



CSPM Playbook



Cloud account Onboarding



- 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)

1 2 3

Cloud Account Details Label & Tag Set Up Connectivity

Select your Cloud Account

AWS GCP Azure

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



1 2 3

Cloud Account Details Label & Tag Set Up Connectivity

Connection Method *

Access Keys - Terraform Script (Recommended)

Label ⓘ *

AWSP12

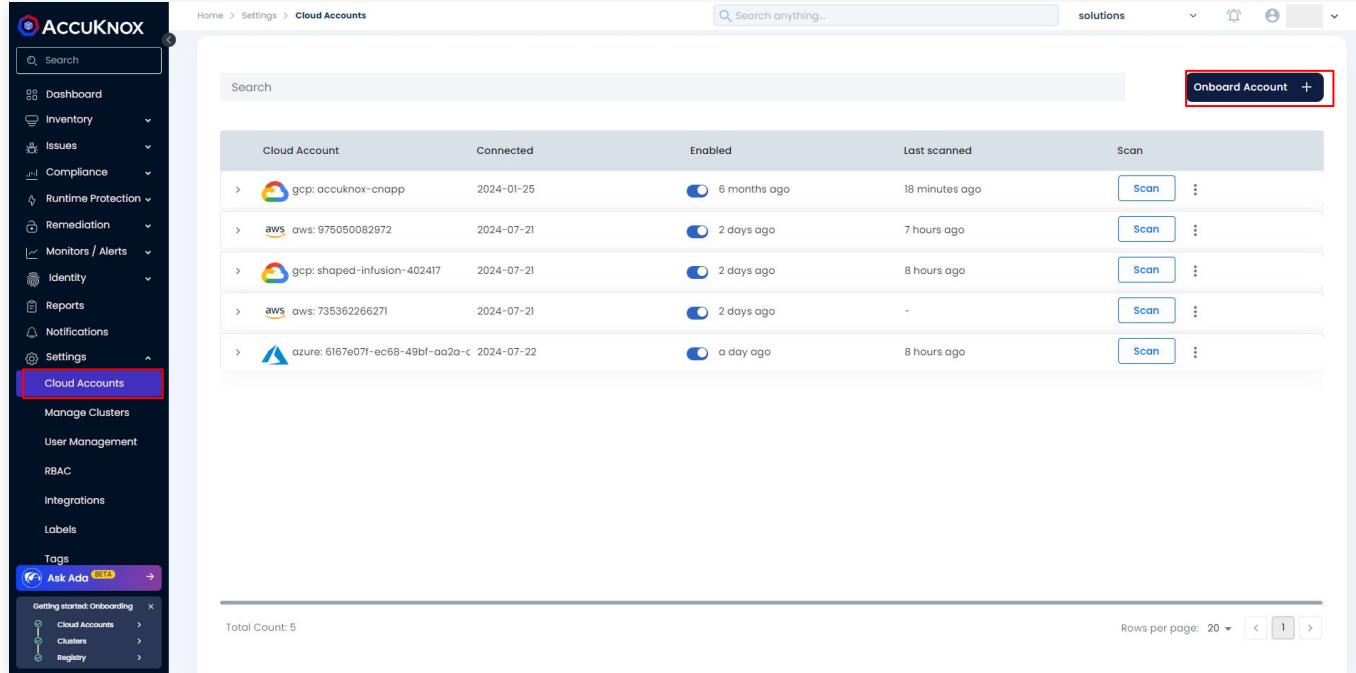
Tag ⓘ

dev-account

Back Cancel 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 ACCUKNOK platform interface for managing cloud accounts. The left sidebar navigation includes: Dashboard, Inventory, Issues, Compliance, Runtime Protection, Remediation, Monitors / Alerts, Identity, Reports, Notifications, Settings (with Cloud Accounts highlighted), Manage Clusters, User Management, RBAC, Integrations, Labels, Tags, and an Ask Add button. The main content area is titled 'Cloud Accounts' and displays a table of connected accounts. The columns are: Cloud Account, Connected (date), Enabled (switch), Last scanned (date), and Scan (button). The accounts listed are:

Cloud Account	Connected	Enabled	Last scanned	Scan
gcp: accuknox-crapp	2024-01-25	On (blue switch)	6 months ago	Scan
aws: 975050082972	2024-07-21	On (blue switch)	2 days ago	Scan
gcp: shaped-infusion-402417	2024-07-21	On (blue switch)	2 days ago	Scan
aws: 735362266271	2024-07-21	On (blue switch)	-	Scan
azure: 6167e07f-ec68-49bf-aa2a-c	2024-07-22	On (blue switch)	a day ago	Scan

At the top right of the main content area, there is a red box highlighting the 'Onboard Account +' button. The bottom of the page shows a total count of 5 accounts and pagination controls.

Cloud account onboarding



- 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 shows the AccuKnox Cloud Account Onboarding process. It includes:

- Left Sidebar:** Shows navigation options like Dashboard, Inventory, Issues, Compliance, Runtime Protection, Remediation, Monitors / Alerts, Reports, Notifications, Settings, and Cloud Accounts (highlighted).
- Top Progress Bar:** Shows three steps: Cloud Account Details (green checkmark), Label & Tag (green checkmark), and Set Up Connectivity (blue circle).
- Middle Section:** A code editor containing a Terraform script to create IAM users and roles, and an access key. A red box highlights the script area.
- Right Section:** Fields for Access Key ID and Secret Access Key, both with "Enter the" placeholder text. Below them is a "Region" section with a "Select All" checkbox and a list of AWS regions. A red arrow points from the highlighted Terraform script to the "Region" section.
- Bottom Buttons:** Back, Cancel, and a large blue "Connect" button.
- Callout:** A red box with the text "Click on Connect to Onboard your AWS account" points to the "Connect" button.
- Bottom Footer:** Step 4 instructions: "Get the access key and secret key from the file **credentials.txt**, Copy & Paste them below and click connect."

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

Asset	Label	Findings	Last Scan date	Asset Category	Asset type	Monitors	Regions
10.0.0.167(agent-name)	NessusTest	50 63 147 7	2024-07-22	Host_Scan_Host	Host_Scan_Host	0	-
6167e07f-ec68-49bf-aa...	AZURE22JULY	4 20	2024-07-23	Cloud Account	azure_subscription	0	-
3d64034d-3c3e-4959-...	AZURE22JULY		2024-07-23	Management	azure_tenant	0	-
735362266271	None		-	-	-	0	-
750567562417.dkr.ecr.us...	None	7 44 47 8	2023-10-17	Container	Container	0	-
788471067825.dkr.ecr.us...	None	8 37 16 1	2023-10-30	Container	Container	0	-
975050082972	AWS5G	19 40 291	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

Asset details

Asset Name:	975050082972
Parent:	
Label:	AWS5G
Category:	Cloud Account
Last Seen:	Tuesday, July 23, 2024 07:44 AM
Region:	0
Tickets	0

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

Vulnerabilities

Severity	Count
High	1
Low	280
Medium	10
Not_available	10

Risk Assessment - Most Critical Findings



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

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-ngr...	Instance Level SSH Only...	High	Ensures that instances ...	Active
2024-07-23 14:41:15	gke-aryan-cluster-ngr...	Instance Level SSH Only...	High	Ensures that instances ...	Active
2024-07-23 14:41:15	gke-aryan-cluster-ngr...	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-ngr...	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-l7l23l2389-librari...	Root MFA Enabled: global	High	Ensures a multi-factor ...	Active
2024-07-23 07:24:23	root-1-l7l23l2389-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

Risk Assessment - New Findings



- Find the recent most findings

The screenshot shows the AccuKNOX platform interface for managing findings. On the left, a dark sidebar contains navigation links for Dashboard, Inventory, Issues, Findings (which is currently selected), Registry Scan, Compliance, Runtime Protection, Remediation, Monitors / Alerts, Identity, Reports, Notifications, and Settings. At the bottom of the sidebar is a 'Ask Ada' beta feature. The main content area has a header with 'Home > Issues > Findings' and a search bar. Below the header are dropdown menus for 'Cloud Findings' (set to 'Cloud Findings'), 'Asset' (set to 'Asset'), and 'Group by' (set to 'Group by'). To the right of these are 'solutions' and 'Saved Filters' dropdowns, along with icons for edit, delete, and other actions. A large table follows, with columns for 'Last seen', 'Assetname', 'Name', 'Risk factor', and 'Description'. The 'Last seen' column is highlighted with a red box. The table lists several entries, such as Service Account Key Rotation, Instance Default Service Account, Open SSH, Private Access Enabled, Instance Maintenance Behavior, Project Ownership Logging, Flow Logs Enabled, Service Account Key Rotation, Flow Logs Enabled, Autoscale Enabled, and Multiple Subnets. The 'Description' column provides details for each finding. At the bottom of the table, it says 'Total Count: 1869' and shows a page navigation bar with pages 1 through 94.

Last seen	Assetname	Name	Risk factor	Description
2024-07-23 14:41:15	8cc188dc2152527lbc76124e9b566b5b87cafe	Service Account Key Rotation: global	Medium	Ensures that service account keys are rotated within desired number
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
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
2024-07-23 14:41:15	default	Private Access Enabled: asia-south1	Medium	Ensures Private Google Access is enabled for all Subnets
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 V
2024-07-23 14:41:15	accuknox-cnapp	Project Ownership Logging: global	Low	Ensures that logging and log alerts exist for project ownership assignm
2024-07-23 14:41:15	default	Flow Logs Enabled: australia-southeast2	Low	Ensures VPC flow logs are enabled for traffic logging
2024-07-23 14:41:15	f34c689db4c6d402ceff5931ec25d1d3d8771c51	Service Account Key Rotation: global	Medium	Ensures that service account keys are rotated within desired number
2024-07-23 14:41:15	default	Flow Logs Enabled: europe-west9	Low	Ensures VPC flow logs are enabled for traffic logging
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
2024-07-23 14:41:15	default	Multiple Subnets: global	Low	Ensures that VPCs have multiple networks to provide a layered archit

Risk Assessment - Most Impacted Assets across cloud



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

6 issues found across muzammil@accuknox.com X

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

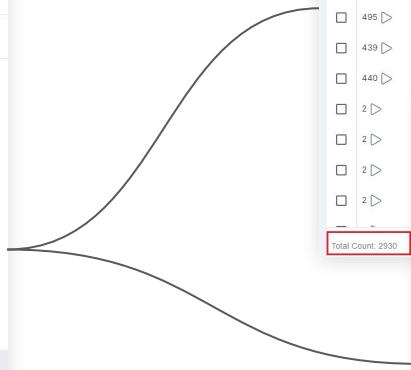
<input type="checkbox"/> Last seen	Asset	Finding	Risk Factor	Description	Status	Location	⋮
2024-07-23 07:24:23	muzammil@accuknox.c...	IAM User Unauthorized t...	Low	Ensures AWS IAM users ...	Active	global	
2024-07-23 07:24:23	muzammil@accuknox.c...	IAM User Has Tags: glob...	Not_available	Ensure that AWS IAM Us...	Active	global	
2024-07-23 07:24:23	muzammil@accuknox.c...	IAM User Account In Use...	Not_available	Ensure that IAM user ac...	Active	global	
2024-07-23 07:24:23	muzammil@accuknox.c...	IAM User Admins: global	Medium	Ensures the number of I...	Active	global	
2024-07-23 07:24:23	muzammil@accuknox.c...	Users Password And Ke...	Low	Detects whether users ...	Active	global	
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

Misconfiguration list for the Onboarded Cloud Account		
Last seen	Finding	
2023-09-13	IAM User Has Tags: global	
2023-09-13	IAM User Without Permissions: global	
2023-09-13	Access Keys Extra: global	
2023-09-13	IAM User Account In Use: global	
2023-09-13	IAM User Account In Use: global	
2023-09-13	IAM User Without Permissions: global	
2023-09-13	IAM User Without Permissions: global	
2023-09-13	IAM User Unauthorized to Edit: global	
2023-09-13	IAM User Has Tags: global	
2023-09-13	IAM Username Matches Regex: global	
2023-09-13	Access Keys Last Used: global	



Ticket Configuration		
Group ids	Last seen	Finding
1	2023-09-13	198.148.116.152 is performing SSH brute force attacks against...
1	2023-09-13	Accelerated Networking Enabled: centralindia
13	2023-09-13	Accelerated Networking Enabled: eastus
1	2023-09-13	Accelerated Networking Enabled: eastus2
495	2023-09-13	Access Keys Extra: global
439	2023-09-13	Access Keys Last Used: global
440	2023-09-13	Access Keys Rotated: global

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

Total Count: 2930

Total Count: 14219

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]

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

Total Count: 1214

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

1

Ticketing Backends

Jira Cloud
priv
Last sync: 2023-09-13
Connected

Jira Cloud
Guru-test
Last sync: 2023-09-13
Connected

2

Jira

Integration Name * Site *

User Email * Token *

Project ID * Issue Summary * Issue Type

Add connector + Test Cancel Save

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

3

ACCUKNOX

Dashboard Inventory Issues Compliance Runtime Protection Remediation

Ticket Summary

Monitors / Logging Reports Notifications Settings

Tickets

Type: Label Type: Data type Type: Status Type: Configuration Type: Priority Type: Date

Project name	Ticket configuration	Ticket Number	Priority	Ticket title	Assets	Status	Comments	Date op
JIRAINTEGRATIONTEST	None	JIRATEST-224	Low	An issue was discovered in the...	0	Opened	0	2023-0
JIRAINTEGRATIONTEST	None	JIRATEST-192	Low	opens: RSA authentication weaknes...	0	Opened	0	2023-0
JIRAINTEGRATIONTEST	None	JIRATEST-198	Low	test - A	0	Opened	0	2023-0
JIRAINTEGRATIONTEST	None	JIRATEST-201	Low	Kernel: A use-after-free due to race between s...	0	Opened	0	2023-0
JIRAINTEGRATIONTEST	None	JIRATEST-195	Medium	systemd: buffer overrun in for...	0	Ongoing	0	2023-0
JIRAINTEGRATIONTEST	None	JIRATEST-199	Medium	test - Avoid	0	Closed	0	2023-0

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

CSPM Compliance Dashboard



Overview of CSPM Compliance Across Multi Cloud

Home > Compliance > CSPM Executive Dashboard

CSPM Executive Dashboard

Total Cloud Accounts

Total Pass V/s Fail Status

Name	Assets Checked	Passed	Warning	Failed	NotAvailable
PCI	2400	2340	2.0%	62	0.7%
HIPAA	2092	2062	2.1%	48	0.3%
CIS1	380	362	17.9%	39	0.0%
CIS2	8	7.5	0.0%	2	0.0%

Executive Compliance Summary

Cloud Accounts	SEP	OCT	Trend
aws 788471067325	0	83	NA
aws 956994857092	85	85	

1-3 of 3 < > Rows per page: 10

Region Based Compliance

Region	Fail	Pass	Warning	Not Available
ap-south-2	0	0	0	4
ap-southeast-4	0	0	0	4
australiacentral	1	212	0	0
australiacentral2	1	212	0	0

1-10 of 58 < > Rows per page: 10

Compliance Summary based on Asset

Assets	Counts	Fail	Pass	Warning	Not Available
ACM	8	0	8	0	0
Active Directory	9	1	8	0	0
Advisor	1	1	0	0	0
API Gateway	26	12	14	0	0
AppFlow	2	0	2	0	0
Application Gate	150	0	150	0	0
App Mesh	6	0	6	0	0

1-50 of 121 < > Rows per page: 50

SLA - Compliance Tickets Age

Month	Count
MAY	~10
JUN	~15
JUL	~12
AUG	~1
SEP	~5
OCT	~8

Compliance Summary



- 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 platform interface. On the left, there's a sidebar with various navigation options like Dashboard, Inventory, Issues, Compliance (which is selected and highlighted in purple), Baselines, CSPM Executive Dashboard, Cloud Assets Summary (also highlighted in purple), Runtime Protection, Remediation, Monitors / Alerts, Identity, Reports, Notifications, and Settings. At the bottom of the sidebar, there's an 'Ask Add' button and a 'Getting started: Onboarding' section with links for Cloud Accounts, Clusters, and Registry.

The main content area is titled 'Cloud Assets Summary'. It has a search bar at the top right and dropdown menus for 'Select Cloud Accounts' and 'Region'. Below that, there are two tabs: 'Compliance' (selected) and 'Detailed View'. The 'Compliance' tab displays a list of '33 Compliance found' under several categories:

- APRA 234 STANDARD**: Controls: 7, 93.4% Compliant. Related Findings: 2.
- AWS CIS Benchmark...**: Controls: 25, 44.6% Compliant. Related Findings: 2.
- AWS CIS Benchmark...**: Controls: 52, 40.7% Compliant. Related Findings: 2.
- AWS CIS Benchmark...**: Controls: 35, 41.7% Compliant. Related Findings: 2.
- AWS Well-Architect...**: Controls: 5, 23.8% Compliant. Related Findings: 2.
- Azure CIS Benchmark...**: Controls: 54, 99.6% Compliant. Related Findings: 2.

Below this list is a table with columns: Control, Assets, Description, Compliance, and Result. The table contains 14 rows of compliance findings, each with a progress bar indicating the percentage of controls met. The 'Result' column uses a color-coded system (red, yellow, green) to show the overall status of each finding.

Control	Assets	Description	Compliance	Result
1.10 Ensure multi-factor authentication (MFA) is enabled for all users	7	Multi-Factor Authentication (MFA) is required for all users	29 %	<div style="width: 29%;"></div> 5 0 0 2
1.11 Do not setup access keys during initial configuration	7	AWS console defaults to no check box	29 %	<div style="width: 29%;"></div> 5 0 0 2
1.12 Ensure credentials unused for 45 days are disabled	7	AWS IAM users can access AWS resources	100 %	<div style="width: 100%;"></div> 0 0 0 7
1.13 Ensure there is only one active account per user	36	Access keys are long-term credentials	86 %	<div style="width: 86%;"></div> 5 0 0 31
1.14 Ensure access keys are rotated every 90 days	38	Access keys consist of an access key ID and a secret access key	68 %	<div style="width: 68%;"></div> 0 12 0 26
1.15 Ensure IAM Users Receive Permissions	36	IAM users are granted access to services	11 %	<div style="width: 11%;"></div> 0 32 0 4
1.16 Ensure IAM policies that allow full access are reviewed regularly	76	IAM policies are the means by which users are granted access to services	13 %	<div style="width: 13%;"></div> 66 0 0 10
1.17 Ensure a support role has been created	0	AWS provides a support center that can be used to troubleshoot issues	0 %	<div style="width: 0%;"></div> 1 0 0 0
1.19 Ensure that all the expired SSL/TLS certificates are replaced	0	To enable HTTPS connections to your website	100 %	<div style="width: 100%;"></div> 0 0 0 1
1.20 Ensure that IAM Access analyzer is enabled	0	Enable IAM Access analyzer for IAM policies	0 %	<div style="width: 0%;"></div> 1 0 0 0
1.4 Ensure no root user account access is granted	1	The root user account is the most privileged account	0 %	<div style="width: 0%;"></div> 1 0 0 0

Total Count: 52

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								
			Asset	Message	Result	Severity	Compliance	Recommended Action	Solution Reference Link		
Multi-Factor Authentication (MFA) ad...	29 %	<div><div style="width: 5%;">5</div><div style="width: 0%;">0</div><div style="width: 0%;">0</div><div style="width: 2%;">2</div></div>	olicies	arn:aws:ia...	Role mana...	FAILED	Low	VAIT +20	Ensure that all IAM roles are scoped to spe...	https://docs.aws.amazon.com/IAM/latest/U...	
AWS console defaults to no check box...	29 %	<div><div style="width: 5%;">5</div><div style="width: 0%;">0</div><div style="width: 0%;">0</div><div style="width: 2%;">2</div></div>	olicies	arn:aws:ia...	Role mana...	FAILED	Low	VAIT +20	Ensure that all IAM roles are scoped to spe...	https://docs.aws.amazon.com/IAM/latest/U...	
AWS IAM users can access AWS resou...	100 %	<div><div style="width: 0%;">0</div><div style="width: 0%;">0</div><div style="width: 0%;">0</div><div style="width: 7%;">7</div></div>	olicies	arn:aws:ia...	Role mana...	FAILED	Low	VAIT +20	Ensure that all IAM roles are scoped to spe...	https://docs.aws.amazon.com/IAM/latest/U...	
Access keys are long-term credential...	86 %	<div><div style="width: 5%;">5</div><div style="width: 0%;">0</div><div style="width: 0%;">0</div><div style="width: 31%;">31</div></div>	olicies	arn:aws:ia...	Role mana...	FAILED	Low	VAIT +20	Ensure that all IAM roles are scoped to spe...	https://docs.aws.amazon.com/IAM/latest/U...	
Access keys consist of an access key ...	68 %	<div><div style="width: 0%;">0</div><div style="width: 12%;">12</div><div style="width: 0%;">0</div><div style="width: 26%;">26</div></div>	olicies	arn:aws:ia...	Role mana...	FAILED	Low	VAIT +20	Ensure that all IAM roles are scoped to spe...	https://docs.aws.amazon.com/IAM/latest/U...	
IAM users are granted access to servi...	11 %	<div><div style="width: 0%;">0</div><div style="width: 32%;">32</div><div style="width: 0%;">0</div><div style="width: 4%;">4</div></div>	olicies	arn:aws:ia...	Role mana...	FAILED	Low	VAIT +20	Ensure that all IAM roles are scoped to spe...	https://docs.aws.amazon.com/IAM/latest/U...	
IAM policies are the means by which ...	13 %	<div><div style="width: 66%;">66</div><div style="width: 0%;">0</div><div style="width: 0%;">0</div><div style="width: 10%;">10</div></div>	olicies	arn:aws:ia...	Role mana...	FAILED	Low	VAIT +20	Ensure that all IAM roles are scoped to spe...	https://docs.aws.amazon.com/IAM/latest/U...	
			<input type="checkbox"/>	iamRolePolicies	arn:aws:ia...	Role mana...	FAILED	Low	VAIT +20	Ensure that all IAM roles are scoped to spe...	https://docs.aws.amazon.com/IAM/latest/U...
			<input type="checkbox"/>	iamRolePolicies	arn:aws:ia...	Role mana...	FAILED	Low	VAIT +20	Ensure that all IAM roles are scoped to spe...	https://docs.aws.amazon.com/IAM/latest/U...
			<input type="checkbox"/>	iamRolePolicies	arn:aws:ia...	Role mana...	FAILED	Low	VAIT +20	Ensure that all IAM roles are scoped to spe...	https://docs.aws.amazon.com/IAM/latest/U...
			<input type="checkbox"/>	iamRolePolicies	arn:aws:ia...	Role inline ...	FAILED	Low	VAIT +20	Ensure that all IAM roles are scoped to spe...	https://docs.aws.amazon.com/IAM/latest/U...
			<input type="checkbox"/>	iamRolePolicies	arn:aws:ia...	Role mana...	FAILED	Low	VAIT +20	Ensure that all IAM roles are scoped to spe...	https://docs.aws.amazon.com/IAM/latest/U...
Total Count: 66											
< 1 2 3 4 >											

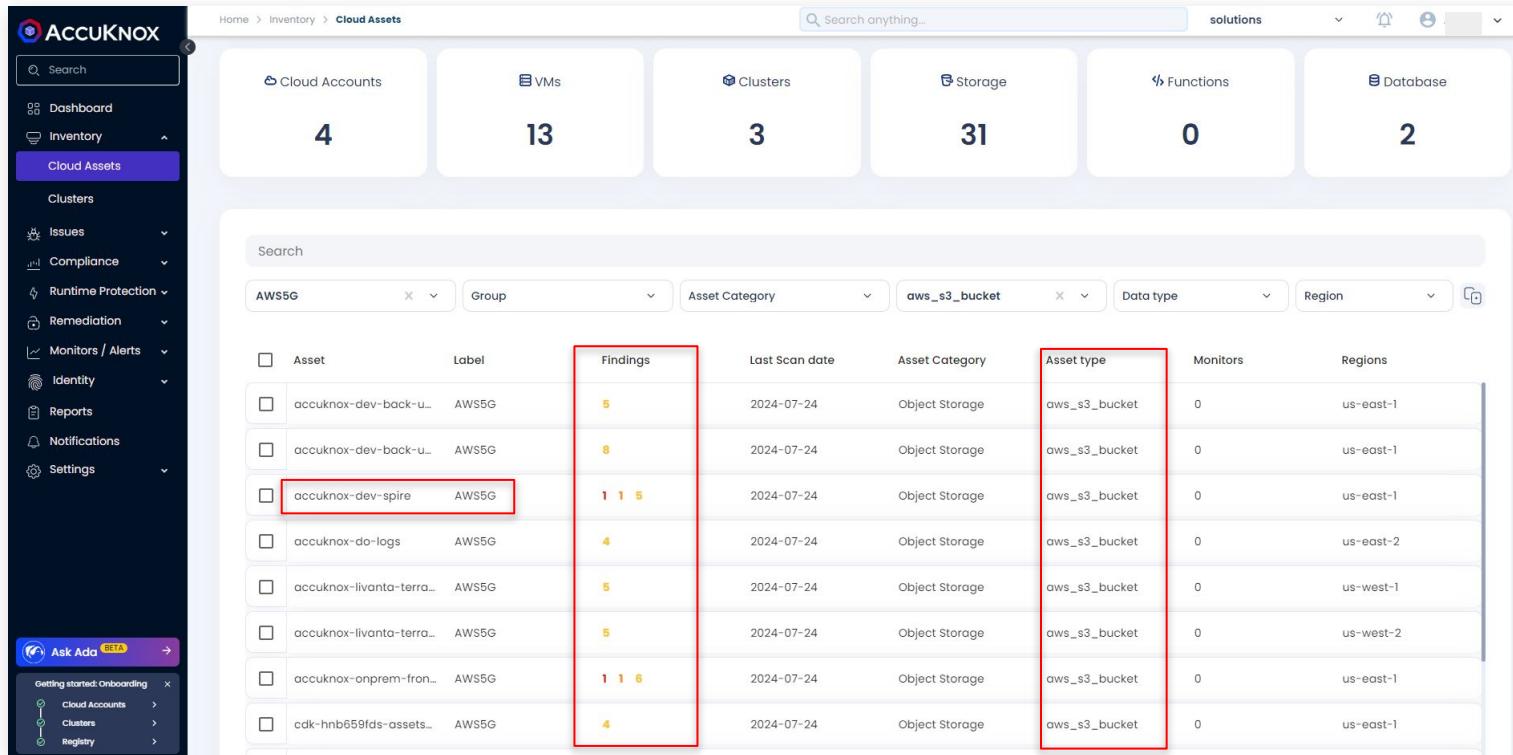


AWS Risk Assessment

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 shows the ACCUKNOKX Cloud Assets dashboard. On the left, there's a sidebar with navigation links like Dashboard, Inventory (selected), Cloud Assets (selected), Clusters, Issues, Compliance, Runtime Protection, Remediation, Monitors / Alerts, Identity, Reports, Notifications, and Settings. At the bottom of the sidebar is an 'Ask Ada' BETA button.

The main area has a header with 'Cloud Accounts' (4), 'VMs' (13), 'Clusters' (3), 'Storage' (31), 'Functions' (0), and 'Database' (2). Below this is a search bar and a filter bar with dropdowns for 'Group', 'Asset Category', 'aws_s3_bucket' (selected), 'Data type', and 'Region'. A 'Search' input field contains 'AWS5G'.

The central part is a table with columns: Asset, Label, Findings, Last Scan date, Asset Category, Asset type, Monitors, and Regions. The 'Findings' column is highlighted with a red border. The 'Asset type' column is also highlighted with a red border. The table lists several AWS5G assets, including 'accuknox-dev-back-u...' (with 5 findings), 'accuknox-dev-back-u...' (with 8 findings), 'accuknox-dev-spire' (with 11 findings, highlighted with a red border), 'accuknox-do-logs' (with 4 findings), 'accuknox-livanta-terra...' (with 5 findings), 'accuknox-livanta-terra...' (with 5 findings), 'accuknox-onprem-fron...' (with 11 findings), and 'cdk-hnb659fds-assets...' (with 4 findings).

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	11	2024-07-24	Object Storage	aws_s3_bucket	0	us-east-1
accuknox-do-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	11	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

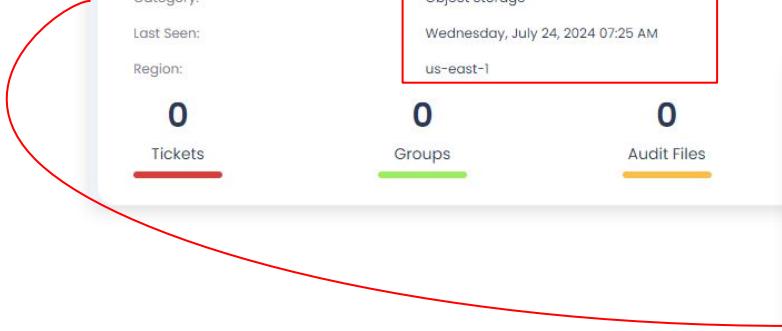
Identify S3 buckets accessible on public networks

- After Identification of S3 bucket with misconfiguration
 - Click on the bucket with misconfiguration(accuknox-dev-spire) to see the detailed view

Asset details

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

0 Tickets 0 Groups 0 Audit Files



Vulnerabilities



Vulnerability Type	Count
High	0
Low	0
Medium	0
Not_available	0

Findings

Search:

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

Last seen	Risk Factor	Finding	Status	Ignored	Exploit Avail...	Tickets	Data Type
2024-07-24	Not_available	S3 Bucket Encryption Enforcement: us-east-1	Active	False	False	0	cloudsploit
2024-07-24	Not_available	S3 Transfer Acceleration Enabled: us-east-1	Active	False	False	0	cloudsploit
2024-07-24	Low	S3 Bucket MFA Delete Status: us-east-1	Active	False	False	0	cloudsploit
2024-07-24	Medium	S3 Bucket All Users Policy: us-east-1	Active	False	False	0	cloudsploit
2024-07-24	High	S3 Bucket Public Access Block: us-east-1	Active	False	False	0	cloudsploit

confidential and proprietary - limited distribution under NDA

17

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 shows the ACCUKNX platform interface. On the left, there's a sidebar with various navigation options like Dashboard, Inventory, Issues, Findings (which is selected), Registry Scan, Compliance, Runtime Protection, Remediation, Monitors / Alerts, Identity, Reports, Notifications, and Settings. At the bottom of the sidebar, there's an 'Ask Ada' beta feature and a 'Getting started: Onboarding' section with links for Cloud Accounts, Clusters, and Registry.

The main area is titled 'Findings' and shows a search bar with 'Cloud Findings' selected and 'ebs' typed in. Below the search bar is a table with columns: Last seen, Assetname (sorted by name), Name, Risk factor, and Description. The table lists several findings, with the last two rows highlighted in red:

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-0365a780f3ba01cc	EBS Encryption Enabled: us-east-1	Medium	Ensures EBS v
2024-07-24 06:43:09	vol-0ab6cfca23b7bf045b	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-0358d385a0d7d1737	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-0126f46c75709670e	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

At the bottom of the table, it says 'Total Count: 17'. To the right of the table, there's a detailed view of the last finding (highlighted in red):

EBS Encryption Enabled: us-west-2 [Medium]

Description	Result	Solution	References	Source Code
Ensures EBS volumes are encrypted at rest				

Details:
Asset: vol-0f38a46063ea738af
Asset Type: aws_ebs_volume
Status: Active
Severity: Medium
Tickets: 0
Notes: Add Comments and Press Ctrl + Enter to Submit

Compliance Frameworks: Coming Soon...

Asset Information:

```
id: "ec903326-45f2-4e63-801b-4fbace8aa00b"
tickets_count: 0
data_type: "aws_ebs_volume"
hash: "8e62285bbdb662564c20936c779735d7"
history: []
date_discovered: "2024-07-24T01:34:13.677058Z"
last_seen: "2024-07-24T01:34:13.677058Z"
data_arn: "arn:aws:ebs:us-west-2:975050082972:volume/vol-0f38..."
data_ctx: {
    stampctx: {
        sdk_version: "5.10.0"
    }
    connection_name: "aws"
}
data_akas: [
    "arn:aws:ebs:us-west-2:975050082972: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

The screenshot shows the ACCUKNOX Cloud Findings interface. The main table lists various findings across different assets and regions. A specific finding for 'Root Hardware MFA: global' is highlighted with a red box. The details pane on the right provides more information about this finding, including its description ('Ensures the root account is using a hardware MFA device'), status ('High'), and a note indicating it's failing since July 21, 2024.

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

Total Count: 41

Root Hardware MFA: global High

Ensures the root account is using a hardware MFA device

Finding for 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_lsm_policy_attachment", "hash": "c24dfdbfb8fc4a284406acc6315652d165", "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 shows the ACCUKNOX platform interface for Cloud Findings. The left sidebar has a red box around the 'Findings' tab. The main search bar has 's3' typed into it, with a red box highlighting the search term. Below the search bar is a table of findings:

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	EIB2FLZPCFTTSD	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	S3 Bucket All Users Policy: us-east-1 [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			

A red box highlights the third row from the top, which corresponds to the finding shown in the details panel below. The details panel includes:

- Description:** Ensures S3 bucket policies do not allow global write, delete, or read permissions
- Finding for:** aws_s3_bucket | kapp.accuknox.com
- Status:** Failing since about 3 day ago, on 21/07/2024
- Last detected:** 24/07/2024
- Compliance Frameworks:** Coming Soon...
- Asset information:** (JSON snippet)

```
{ "id": "d0bf2c80-e6a0-40a4-aaf4-bd2c8cfcc6", "tickets_count": 0, "data_type": "aws_s3_bucket", "hash": "340b07ca2lb25ebdbf85c8a2ab6441e3" }
```

On the right side, there is a sidebar with the following details:

- 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

	Last seen	Assetname	Name	Risk factor	Description		
<input type="checkbox"/>	2024-07-24 07:02:03	rj-gcp	Instance Level SSH Only: us-central	High	Ensures that instances are not configured to... ↳ "data__ctx": { "steampipe": { "sdk_version": "5.10.0" } }, "connection_name": "aws"	Active	us-central
<input type="checkbox"/>	2024-07-24 06:52:26	gke-aryan-cluster-nga452d...	Instance Level SSH Only: us-central	High	Ensures that instances are not configured to... ↳ "data__ctx": { "steampipe": { "sdk_version": "5.10.0" } }, "connection_name": "aws"	Active	us-central
<input type="checkbox"/>	2024-07-24 06:52:26	gke-aryan-cluster-nga452d...	Instance Level SSH Only: us-central	High	Ensures that instances are not configured to... ↳ "data__ctx": { "steampipe": { "sdk_version": "5.10.0" } }, "connection_name": "aws"	Active	us-central
<input type="checkbox"/>	2024-07-24 06:52:26	gke-aryan-cluster-nga452d...	Instance Level SSH Only: us-central	High	Ensures that instances are not configured to... ↳ "data__ctx": { "steampipe": { "sdk_version": "5.10.0" } }, "connection_name": "aws"	Active	us-central
<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 Details + Create Ticket

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

Finding for 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 : "8fdc7a95-0443-4454-8f86-78d831854f35"
tickets_count : 0
data_type : "aws_vpc_security_group"
hash : "c16d6500600efb30443e1947238cec1f8"
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"
```

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 shows the AccuKnox platform interface for identifying IAM-related security misconfigurations. The search bar at the top contains the term "iam". The main table lists findings, with one entry highlighted by a red box:

Last seen	Assetname	Name	Risk
2024-07-24 07:16:51	thiago@5gron.net	IAM User Admins: global	Medium
2024-07-24 07:16:51	sujith.kasireddy@accuknox.co...	IAM User Admins: global	Medium
2024-07-24 07:16:51	rahul@accuknox.com	IAM User Admins: global	Medium
2024-07-24 07:16:51	muzammil@accuknox.com	IAM User Admins: global	Medium
2024-07-24 07:16:51	EKS_User	IAM User Admins: global	Medium
2024-07-24 07:16:51	achref@accuknox.com	IAM User Admins: global	Medium

A detailed view of the first highlighted finding is shown on the right:

IAM User Admins: global [Medium]

Description: Ensures the number of IAM admins in the account are minimized.

Finding for in resource: aws_iam_user | rahul@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 : "81e31335-7bbc-41d2-bfd6-0b67f5b69476"
tickets_count : 0
data_type : "aws_iam_user"
hash : "fca773686527edce63dde8ec292e44e4"
history : []
date_discovered : "2024-07-21T06:52:42.219731Z"
last_seen : "2024-07-24T01:55:12.606470Z"
```

Details panel on the right:

- Asset: rahul@accuknox.com
- Asset Type: aws_iam_user
- Status: Active
- Ignored: No
- Severity: Medium
- Tickets: 0
- Notes: Add Comments and Press Ctrl + Enter to Submit

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 shows the ACCUKNOX platform interface. On the left, there's a sidebar with various navigation options like Dashboard, Inventory, Issues, Findings, Compliance, Runtime Protection, Remediation, Monitors / Alerts, Identity, Reports, Notifications, and Settings. A prominent 'Ask Ada' button is also present. The main area is titled 'Findings' and shows a search bar with the query 'EKS Secrets Encrypted: us-east-1'. Below the search bar, there are tabs for Description, Result, Solution, References, and Source Code. The 'Description' tab is selected, displaying a brief summary: 'Ensures EKS clusters are configured to enable envelope encryption of Kubernetes secrets using KMS.' It lists three findings: one for a resource named 'aws_eks_cluster' (status: failing since 21/07/2024), one failing since about 1 month ago, and one last detected on 16/08/2024. The 'Asset Information' section shows a JSON object with details like ID, ticket count, data type, hash, history, discovery date, last seen date, data ARN, and connection name. On the right, a detailed view of the first finding is shown. This view includes a 'Filter' sidebar with options for Data Type (cloudsploit), Select Fields to filter (Cloud account), Location, Risk Factor (High), Ignored (No), Severity (High), Tickets (0), and Notes (an input field for comments). The 'Cloud account' field in the filter sidebar is highlighted with a red box. The 'Cloud account' field in the notes section is also highlighted with a red box.

How to identify if Insecure HTTP Port open to public?



- To identity 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

The screenshot shows two instances of a finding titled "Open HTTP: us-east-1" with a "High" severity level. Both findings have a red box drawn around the "Asset" field in the "Details" panel.

Findings Details:

- Description:** 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:** A JSON object with fields: id, tickets_count, data_type, hash, history, date_discovered, and last_seen.

Details Panel (Asset Field):

- Asset:** k8s-elb-ae55f3e0b4f134cf68f781e9d48292a5
- Asset Type:** aws_vpc_security_group
- Status:** Active (radio button selected)
- Ignored:** No (checkbox is off)

Second Finding Summary:

- Description:** 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 identity 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.

The screenshot shows the ACCUKNOX platform interface. On the left, there is a detailed view of a finding titled "RDS Public Subnet: us-west-2" with a "High" severity level. The finding details state: "Ensures RDS database instances are not deployed in public subnet." It includes sections for "Description", "Result", "Solution", "References", and "Source Code". Below this, there are sections for "Compliance Frameworks" (Coming Soon...) and "Asset Information" (with a JSON dump of asset data). On the right, a modal dialog titled "Create Ticket" is open, prompting the user to select a ticket configuration. A red box highlights the "+ Create Ticket" button. At the bottom, another instance of the finding is shown with a red box highlighting the "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>" note.

RDS Public Subnet: us-west-2 **High**

Description Result Solution References Source Code

Ensures RDS database instances are not deployed in public subnet.

Finding 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": "3e2a9e62f0bb9c2e0dac6751d12842c", "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.

compliance

Close

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?  AccuKNOX

- 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' menu item highlighted. The main content area displays a finding titled 'CloudTrail Enabled: ap-northeast-1' with a 'High' risk factor. The finding details state: 'Ensures CloudTrail is enabled for all regions within an account'. Below this, sections for 'Compliance Frameworks' and 'Affected Assets' are shown, each with one record. A red box highlights the finding title and risk level. Another red box highlights the 'Solution' section on the right, which provides a link to AWS documentation: <http://docs.aws.amazon.com/awscloudtrail/latest/userguide/getting-started.html>.

Home > Issues > Findings

Finding

CloudTrail Enabled: ap-northeast-1 High

Description

Ensures CloudTrail is enabled for all regions within an account

Count Last seen

2	2024-08-16 08
1	2024-08-16 06
1	2024-08-16 06
1	2024-08-16 07
1	2024-08-16 07
1	2024-08-16 07
1	2024-08-16 07
1	2024-08-16 08

Compliance Frameworks

No compliance found

Affected Assets

<input type="checkbox"/>	Last seen	Asset	Finding	Risk Factor	Description	Status	I
<input type="checkbox"/>	2024-08-16 08:43:45	975050082972	CloudTrail Enabled: ap-...	High	Ensures CloudTrail is en...	Active	ap-...
<input type="checkbox"/>	2024-08-16 06						
<input type="checkbox"/>	2024-08-16 07						
<input type="checkbox"/>	2024-08-16 07						
<input type="checkbox"/>	2024-08-16 08						

Total Records: 62

Solution

Ensure CloudTrail is enabled for all regions and ensure that at least one region monitors global service events, <http://docs.aws.amazon.com/awscloudtrail/latest/userguide/getting-started.html>

Compliance failure for CIS Benchmark



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

The screenshot shows the ACCUKNOX platform interface. On the left, a sidebar menu is visible with various options like Dashboard, Inventory, Issues, Compliance, Baselines, CSPM Executive Dashboard, and Cloud Assets Summary (which is highlighted with a red box). The main content area is titled "Cloud Assets Summary" under "Compliance". A search bar at the top has "aws 975050082972 | AWS5G" entered. Below the search bar, there's a "Region" dropdown. The main view displays "28 Compliance found" across several sections. One section, "AWS CIS Benchmark...", is highlighted with a red box. This section shows "Controls : 52" and "40.7% Compliant". The "Related Findings" link is also highlighted with a red box. To the right, a detailed table lists 14 specific controls from the CIS Benchmark, each with its own row. The columns in the table are "Control", "Assets", "Description", "Compliance", and "Result". The "Compliance" column shows percentages (e.g., 29%, 100%, 86%) and the "Result" column shows a color-coded bar chart (red, yellow, green) indicating the status for each control.

Control	Assets	Description	Compliance	Result
1.10 Ensure multi-factor authentication (MFA) is enabled for all users	7	Multi-Factor Authentication (MFA) is required for user logins	29 %	<div style="width: 29%;"></div> 5 0 0 2
1.11 Do not setup access keys during initial user creation	7	AWS console defaults to no check box for access key creation	29 %	<div style="width: 29%;"></div> 5 0 0 2
1.12 Ensure credentials unused for 45 days or longer are deleted	36	AWS IAM users can access AWS resources using long-term credentials	100 %	<div style="width: 100%;"></div> 0 0 0 7
1.13 Ensure there is only one active access key per user	36	Access keys are long-term credential used for AWS access	86 %	<div style="width: 86%;"></div> 5 0 0 31
1.14 Ensure access keys are rotated every 90 days or less	38	Access keys consist of an access key and secret key	68 %	<div style="width: 68%;"></div> 0 12 0 26
1.15 Ensure IAM Users Receive Permissions Only as Required	36	IAM users are granted access to services based on policies	11 %	<div style="width: 11%;"></div> 0 32 0 4
1.16 Ensure IAM policies that allow full "*" actions are reviewed	76	IAM policies are the means by which users access AWS services	13 %	<div style="width: 13%;"></div> 66 0 0 10
1.17 Ensure a support role has been created to handle support requests	0	AWS provides a support center that can be accessed via email	0 %	<div style="width: 0%;"></div> 1 0 0 0
1.19 Ensure that all the expired SSL/TLS certificates are removed	0	To enable HTTPS connections to your application	100 %	<div style="width: 100%;"></div> 0 0 0 1
1.20 Ensure that IAM Access analyzer is enabled for IAM policies	0	Enable IAM Access analyzer for IAM policies	0 %	<div style="width: 0%;"></div> 1 0 0 0
1.4 Ensure no root user account access key is stored in clear text	1	The root user account is the most privileged account	0 %	<div style="width: 0%;"></div> 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 shows the ACCUKNOX Compliance interface. On the left, a sidebar lists various compliance frameworks: FedRAMP, FERPA, FISMA, General Data Protection, HIPAA (highlighted with a red box), HITRUST CSF, and ISO 27001. The HIPAA section shows 8 controls and 63.6% compliance. The main area displays a table of findings for the HIPAA benchmark, specifically for control 164.312(d) Person or Entity Authentication. The table includes columns for Control, Assets, Description, Compliance, Result, and Severity. Most findings are marked as 'FAILED' with a severity of 'Medium' or 'High'. A filter panel on the right allows users to search by program_name (set to 'HIPAA') and control_name (set to '164.312(d) Person or Entity Authentication').

Control	Assets	Description	Compliance	Result	Severity
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	
164.312(d) Person or Entity Authentication	10	Configure multi-factor authentication ...	0 %	10 0 0 10	High

Filter Clear Filter Apply

Select Fields to filter

control_name

program_name X control_name X

program_name

HIPAA X

control_name

164.312(d) Person or Entity Authentication X

Compliance failure for ISO 27001 Benchmark



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

The screenshot shows the ACCUKNOX Compliance interface. At the top, there's a search bar with 'aws 975050082972 | AWS5G' and a 'Region' dropdown. Below the search bar, the 'Compliance' tab is selected, showing a summary of 28 compliance findings.

Compliance Summary:

- 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

Cloud Asset Summary:

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

Filter: Clear Filter, Apply

Select Fields to filter:
control_name
program_name X control_name X
program_name
ISO 27001
control_name
A.12.2.1 Controls Against Malware

Compliance failure for Mitre AWS Attack Framework



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

Compliance Detailed View

28 Compliance found

Control	Assets	Description	Compliance	Result
Account Manipulation	49	Measures should be put in place to pr...	40 %	6 0 0 4
Brute Force	7	Additional controls should be put in pl...	100 %	7 0 0 0
Create Account	25	Additional controls should be put in pl...	100 %	25 0 0 0
Data from Cloud Storage Object	75	Data in cloud storage objects should be p...	100 %	75 0 0 0
Defacement	2	Disaster recovery plan should be put in p...	100 %	2 0 0 0
Exploit Public-Facing Application	22	Control access to public-facing applications...	100 %	22 0 0 0
Impair Defences	132	Necessary controls should be put in place to...	100 %	132 0 0 0
Implant Container Image	3	Control access to container images...	100 %	3 0 0 0
Modify Cloud Compute Infrastructure	107	Modifications to cloud compute infrastructure...	100 %	107 0 0 0
Network Denial of Service	16	Attackers should not be able to deny service...	100 %	16 0 0 0
Network Scanning	20	Measuring network scanning activity...	100 %	20 0 0 0

Total Count: 14

Mitre AWS Attack Framework Related Findings → Controls: 14 31.9% Compliant

NIST 800-171 Related Findings → Controls: 10 54.7% Compliant

NIST CSF Related Findings → Controls: 38 63.7% Compliant

NIST SP 800-53 Related Findings → Controls: 13 61.5% Compliant

PCI Related Findings → Controls: 8 67.2% Compliant

aws 975050082972 | AWSSG Region Failed Severity

Filter Clear Filter Apply

Select Fields to filter control_name

control_name X

program_name X control_name X

program_name X

Mitre AWS Attack Framework X

control_name X

Impair Defences X

Compliance Detailed View

Plugin	Asset	Message	Result	Severity	Compliance	Recommended Action	Solution Reference Link
iamRolePolicyName	arn:aws:iam::	Role man...	FAILED	Low	VAIT +20	Ensure that all IAM role...	https://docs.aws.amazon.com
iamRolePolicyName	arn:aws:iam::	Role man...	FAILED	Low	VAIT +20	Ensure that all IAM role...	https://docs.aws.amazon.com
iamRolePolicyName	arn:aws:iam::	Role man...	FAILED	Low	VAIT +20	Ensure that all IAM role...	https://docs.aws.amazon.com
iamRolePolicyName	arn:aws:iam::	Role man...	FAILED	Low	VAIT +20	Ensure that all IAM role...	https://docs.aws.amazon.com
iamRolePolicyName	arn:aws:iam::	Role man...	FAILED	Low	VAIT +20	Ensure that all IAM role...	https://docs.aws.amazon.com
iamRolePolicyName	arn:aws:iam::	Role man...	FAILED	Low	VAIT +20	Ensure that all IAM role...	https://docs.aws.amazon.com
iamRolePolicyName	arn:aws:iam::	Role man...	FAILED	Low	VAIT +20	Ensure that all IAM role...	https://docs.aws.amazon.com
iamRolePolicyName	arn:aws:iam::	Role man...	FAILED	Low	VAIT +20	Ensure that all IAM role...	https://docs.aws.amazon.com
iamRolePolicyName	arn:aws:iam::	Role man...	FAILED	Low	VAIT +20	Ensure that all IAM role...	https://docs.aws.amazon.com
iamRolePolicyName	arn:aws:iam::	Role man...	FAILED	Low	VAIT +20	Ensure that all IAM role...	https://docs.aws.amazon.com
iamRolePolicyName	arn:aws:iam::	Role man...	FAILED	Low	VAIT +20	Ensure that all IAM role...	https://docs.aws.amazon.com
iamRolePolicyName	arn:aws:iam::	Role man...	FAILED	Low	VAIT +20	Ensure that all IAM role...	https://docs.aws.amazon.com
iamRolePolicyName	arn:aws:iam::	Role has...	FAILED	Low	VAIT +20	Ensure that all IAM role...	https://docs.aws.amazon.com

Total Count: 67

1 2 3 4 >

Compliance failure for NIST 800 compliance



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

The screenshot shows the ACCUKNOX platform interface. On the left, the navigation bar includes 'Cloud Assets Summary' which is highlighted with a red box. The main content area displays a 'Compliance' section with a summary of '28 Compliance found'. Below this, there is a list of compliance frameworks: LGPD, Mitre AWS Attack Fr..., NIST 800-171 (which is also highlighted with a red box), NIST CSF, NIST SP 800-53, and PCI. The NIST 800-171 section shows 10 controls and 54.7% compliance. To the right is a detailed table of 3.9 controls, each with its assets, description, compliance percentage, and a color-coded result bar (red, yellow, green). The table has columns for Control, Assets, Description, Compliance, and Result.

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 actin...	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

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

The screenshot shows the AccuKnox platform interface. On the left, a finding for 'Root Hardware MFA: global' is displayed with a severity of 'High'. The finding details include: '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', and 'Last detected on 24/07/2024'. Below this are sections for 'Compliance Frameworks' (Coming Soon...) and 'Asset Information' (with JSON data: { "id": "1676061e-b3b1-470a-bda9-cef23a9f394f", "tickets_count": 0, "data_type": "aws_iam_policy_attachment" }). A modal window titled 'Create Ticket' is open in the center, showing a dropdown menu with 'compliancej' selected. The main ticket creation form has fields for 'Ticket Title' (set to 'Root Hardware MFA: global'), 'Ticket Description' (set to 'Ensures the root account is using a hardware MFA device'), and 'Synopsis' (set to 'Impacted Assets: Asset 975050082972, Port global'). The 'Solution' field contains a link: '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'. The 'Plugin Output' field shows the message 'FAILED, Root account is not using an MFA device'. A red box highlights the 'compliancej' dropdown in the modal, and another red box highlights the 'Create Ticket' button in the modal.

Assistive Remediation For AWS 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

The screenshot illustrates the AccuKnox Cloud Assets interface for managing AWS risks. It shows two main panels: a search results table and a detailed view of a specific finding.

Search Results Panel: This panel displays a table of assets found in the 'AWS5G' group. The columns include Asset, Label, Findings, Last Scan date, Asset Category, Asset type, Monitors, and Regions. Two rows are visible, both labeled 'aws_s3_bucket' under Asset Category and 'aws_s3_bucket' under Asset type. The first row has a value of 5 in the 'Findings' column, and the second row has a value of 8. A red box highlights the 'Findings' column header.

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

Detailed View Panel: This panel shows a single finding for an S3 bucket. The top navigation bar includes 'Home', 'Inventory', 'Cloud Assets', and 'Details'. The search bar contains 'compliance'. The right side of the panel features a 'Create a ticket' button with a red box around it, along with other action icons. The bottom part of the panel displays a table of findings with columns: Last seen, Risk Factor, Finding, Status, Ignored, Exploit Avail., Tickets, Data Type, and Last seen. One finding is selected, indicated by a checked checkbox in the 'Ignored' column.

Last seen	Risk Factor	Finding	Status	Ignored	Exploit Avail.	Tickets	Data Type
2024-07-24	NOT_available	S3 Bucket Encryption Enforcement: us-east-1	Active	False	False	0	cloudsploit
2024-07-24	Not_available	S3 Transfer Acceleration Enabled: us-east-1	Active	False	False	0	cloudsploit
2024-07-24	Low	S3 Bucket MFA Delete Status: us-east-1	Active	False	False	0	cloudsploit
2024-07-24	Medium	S3 Bucket All Users Policy: us-east-1	Active	False	False	0	cloudsploit
2024-07-24	High	S3 Bucket Public Access Block: us-east-1	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 shows the AccuKnox platform interface. On the left, the navigation bar includes 'Dashboard', 'Inventory', 'Issues', 'Compliance' (selected), 'Baselines', 'CSPM Executive Dashboard', 'Cloud Assets Summary' (highlighted with a red box), 'Runtime Protection', 'Remediation', 'Monitors / Alerts', 'Identity', 'Reports', 'Notifications', and 'Settings'. An 'Ask Ada' button is also present. The main area displays a 'Cloud Assets Summary' table with columns: Plugin, Asset, Message, and Result. One row is highlighted with a red box and labeled 'FAILED'. To the right, a detailed view for 'iamRolePolicies' is shown. It includes a 'Description' section stating 'Ensures IAM role policies are properly scoped with specific permissions', a 'Message' section stating 'Role managed policy allows actions on all resources', and a 'Solution Reference Link' pointing to https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html. A 'Recommended Actions' section advises ensuring IAM roles are scoped to specific services and API calls. The 'Details' section on the right shows the asset ID 'arn:aws:iam:975050082972:role/aws-service-role/elasticloadbalancing.amazonaws.com/AWSServiceRoleForElasticLoadBalancing', category 'IAM', region 'None', result 'FAILED', severity 'Low', and account 'aws 975050082972'. A '+ Create Ticket' button is also visible.



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**

Home > Inventory > Cloud Assets

Search anything...

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

Cloud Accounts	VMs	Clusters	Storage	Functions	Database
3	9	0	2	0	0

Search

Label Group Asset Category Asset type Monitors Regions

Asset	Label	Findings	Last Scan date	Asset Category	Asset type	Monitors	Regions
[redacted]	AZURE26JUL	1 1 1	2024-08-03	Networking	azure_network_security_group	0	eastus
[redacted]	AZICMA	2 1 2	2024-08-11	Networking	azure_network_security_group	0	eastus
[redacted]	AZICMA	1 1	2024-08-11	Networking	azure_network_security_group	0	eastus
[redacted]	AZICMA	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

Asset details

Asset Name: [REDACTED]
Parent: AZICMA
Label: Networking
Category: Networking
Last Seen: Sunday, August 11, 2024 08:57 AM
Region: --

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

Vulnerabilities

Findings

Search: [REDACTED]

Last seen	Risk Factor	Finding	Status	Ignored	Exploit Available	Tickets	Data Type
2024-08-11	High	Open RDP: eastus	Active	False	False	0	cloudsploit
2024-08-11	Low	Open HTTPS: eastus	Active	False	False	0	cloudsploit
2024-08-11	Medium	NSG Flow Logs Enabled: eastus	Active	False	False	0	cloudsploit
2024-08-11	High	Open HTTP: eastus	Active	False	False	0	cloudsploit
2024-08-11	Low	NSG Log Analytics Enabled: eastus	Active	False	False	0	cloudsploit

Open RDP: eastus

Asset: [REDACTED] Asset Type: azure_network_security_group Location: eastus

Status: Active Ignored: No Tickets: 0 Risk Factor: High

Description: Determine if TCP port [REDACTED] for RDP is open to the public

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 illustrates the ACCUKNOX platform interface for identifying DDoS protection status. On the left, the navigation bar includes links for Home, Dashboard, Inventory, Issues (highlighted), Findings (highlighted), Registry Scan, Compliance, Runtime Protection, Remediation, Monitors / Alerts, Identity, Reports, Notifications, and Settings. A sidebar on the far left shows 'Getting started: Onboarding' with sections for Cloud Accounts, Clusters, and Registry.

The main area shows the 'Issues > Findings' page. The 'Cloud Findings' filter is selected. A search bar contains 'cloudsploit'. A filter sidebar on the right shows 'Cloud type: azure_subscription' highlighted with a red box. The main table lists findings, including:

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]	DDoS Standard Protect...	Low	Ensures that DDoS Stan...	Active

A detailed view of a finding titled 'Public IP Address DDoS Protection: eastus' is shown on the right. The finding details include:

- Description: Ensures that DDoS IP Protection is enabled for Microsoft Azure Public IP Addresses.
- Result: Finding for in resource [REDACTED]
- Solution: Failing since about 5 day ago, on 06/08/2024
- References: Last detected on 11/08/2024
- Source Code: Not available
- Details: Asset type: azure_public_ip, Status: Active, Ignored: No, Severity: Medium, Tickets: 0.
- Notes: Add Comments and Press Ctrl + Enter to Submit.

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 shows the ACCUKNOX platform interface. On the left, there's a sidebar with various navigation options like Dashboard, Inventory, Findings (which is highlighted), Registry Scan, Compliance, Runtime Protection, Remediation, Monitors / Alerts, Identity, Reports, Notifications, and Settings. The main area has a breadcrumb path: Home > Issues > Findings. There are dropdown filters for 'Cloud Findings' (selected), 'Asset' (set to 'Finding'), and a search bar containing 'Finding'. A red box highlights the 'VM disk' search term. Below this is a table of findings:

Count	Last seen	Assetname	Name	Risk factor
11	2024-08-11 08:31:44	[REDACTED]	VM Disk Double Encrypti...	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 Confli...	Low

A red box highlights the row with 'VM Disk Public Access: ...' as High risk. An arrow points from this row to a larger detailed view on the right.

Finding
VM Disk Public Access: eastus High

Description
Ensures that Azure virtual machine disks are not accessible publicly.

Solution
Disable public access for all Azure virtual machine disks.
<https://learn.microsoft.com/en-us/azure/virtual-machines/disks-enable-private-links-for-import-export-portal>

Compliance Frameworks
No compliance found

Affected Assets

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

An arrow points from the 'Affected Assets' table to the text 'All the affected assets by this particular finding.'

Click on any findings to view get more detailed view.

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 illustrates the ACCUKNOX platform interface for identifying an open RDP port in an Azure Network Security Group.

Left Panel (Navigation):

- Home
- Issues > Findings
- Cloud Findings
- RDP
- Last seen
- Assetname
- Name
- Risk factor
- 2024-08-11 08:31:44
- Open RDP: eastus
- High

Right Panel (Details View):

Findings Details:

- Description: Open RDP: eastus
- Result: Determine if TCP port 3389 for RDP is open to the public
- Finding for resource: [redacted]
- Failing since about 1 month ago, on 26/07/2024
- Last detected on 11/08/2024
- Compliance Frameworks: Coming Soon...
- Asset Information: [Redacted asset details]

Notes:

- + Create Ticket
- Users can also add multiple comments here.

Bottom Right Corner:

- Reported: 2024-08-11 20:33:53

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 shows the ACCUKNOX platform interface. On the left, there's a sidebar with various navigation options like Dashboard, Inventory, Issues (which is selected), Findings (highlighted in purple), Registry Scan, Compliance, Runtime Protection, Remediation, Monitors / Alerts, Identity, Reports, Notifications, and Settings. Below the sidebar, there's an 'Onboarding' section with 'Cloud Accounts', 'Clusters', and 'Registry'. The main area has a header with 'Home > Issues > Findings' and a search bar. The 'Cloud Findings' dropdown is set to 'Asset' and the 'Finding' dropdown is set to 'Vault'. A red box highlights the 'Vault' filter. The main table lists findings with columns: Count, Last seen, Assetname, Name, Risk factor, Description, Status, and Location. The first finding is highlighted with a red box. The right side shows a detailed view of this finding, titled 'Recovery Services Vault BYOK Encrypted: centralus'. It includes a 'Description' section with the text 'Ensure that Microsoft Azure Recovery Services Vaults have BYOK encryption enabled.', a 'compliance Frameworks' section stating 'No compliance found', and an 'Affected Assets' table. The affected asset is the same one from the main list, with its details shown in the table. A red box highlights the 'Affected Assets' table.

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	australiacentral
2	2024-08-11 08:31:44	[REDACTED]	Key Vault In Use: austral...	Low	Ensures that Key Vaults ...	Active	australiacentral
2	2024-08-03 06:59:32	[REDACTED]	Key Vault In Use: austral...	Low	Ensures that Key Vaults ...	Active	australiacentral
2	2024-08-11 08:31:44	[REDACTED]	Key Vault In Use: austral...	Low	Ensures that Key Vaults ...	Active	australiacentral
2	2024-08-03 06:59:32	[REDACTED]	Key Vault In Use: brazil..._	Low	Ensures that Key Vaults ...	Active	brazilsouth
2	2024-08-11 08:31:44	[REDACTED]	Key Vault In Use: brazil..._	Low	Ensures that Key Vaults ...	Active	brazilsouth
2	2024-08-03 06:59:32	[REDACTED]	Key Vault In Use: canad..._	Low	Ensures that Key Vaults ...	Active	canadaeast

Total Records: 58

Finding
Recovery Services Vault BYOK Encrypted: centralus

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

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?

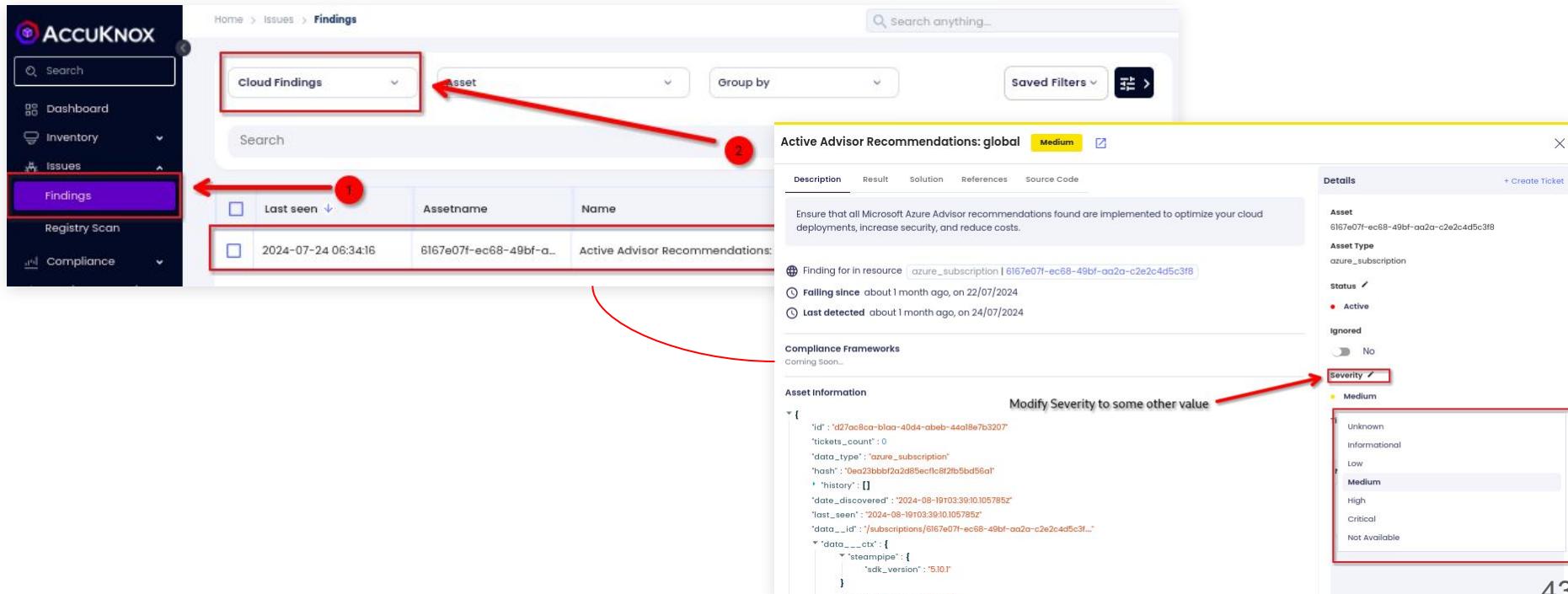


- To identify if the SQL Server Firewall Rule Alerts Monitor is enabled in Azure, please navigate to Issues -> Findings.
 - Select **Cloud Findings** in the findings-type filter.
 - Choose Findings in the group by filter.
 - You can also directly search for the specific Assets/Findings using the Search 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.

Count	Last seen	Assetname	Name	Risk factor	Description
1	2024-07-11 06:34:16	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.



Cloud Findings

Asset

Search anything...

Cloud Findings

Last seen

Assetname

Name

2024-07-24 06:34:16

6167e07f-ec68-49bf-a...

Active Advisor Recommendations: global

Description Result Solution References Source Code

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

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

Last detected: about 1 month ago, on 24/07/2024

Compliance Frameworks

Coming Soon...

Asset Information

Modify Severity to some other value

Severity

Medium

Unknown

Informational

Low

Medium

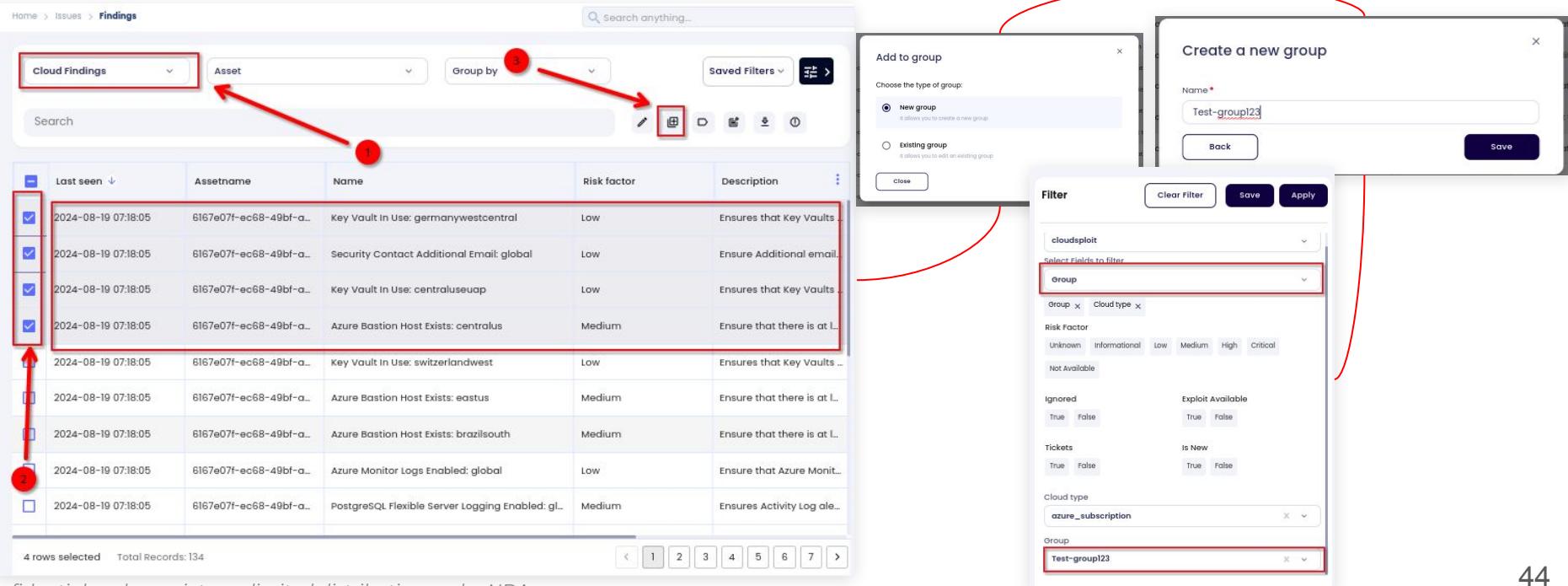
High

Critical

Not Available

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 can filter findings based on the created groups too.

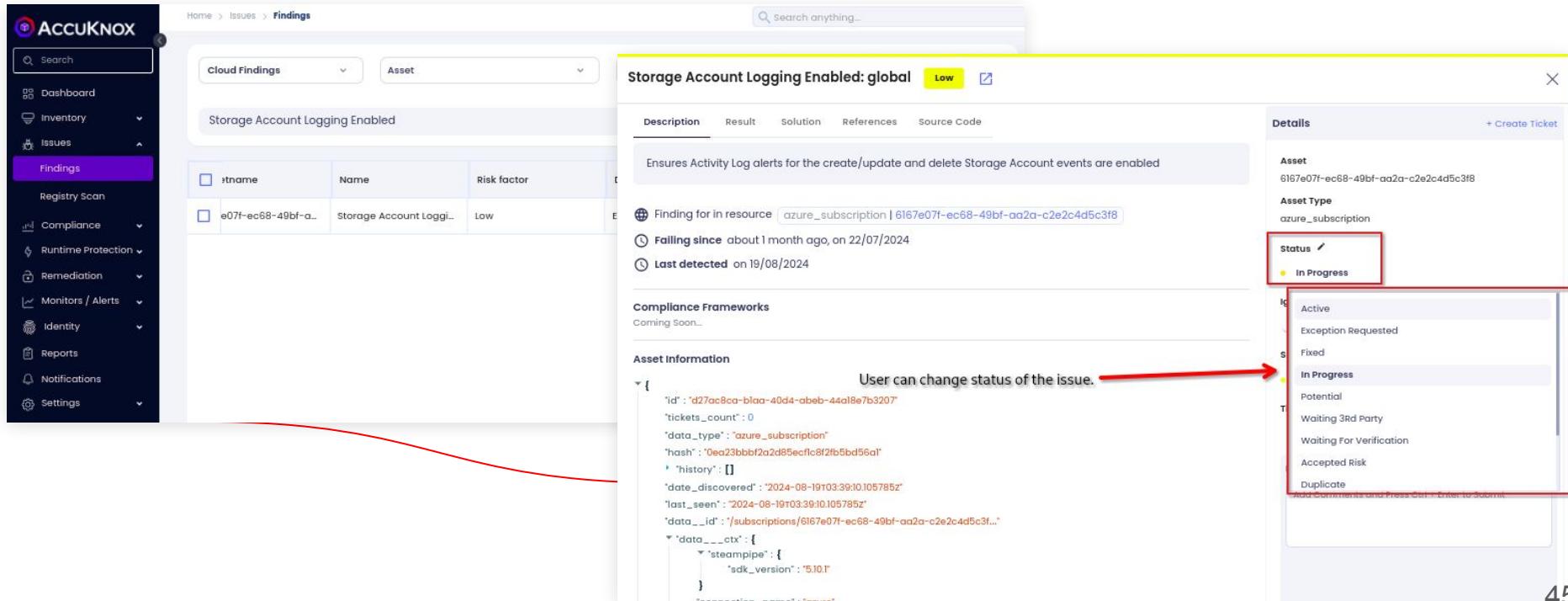


The screenshot illustrates the steps to group findings in the ACCUKNX platform:

- Step 1:** In the "Findings" list view, multiple findings are selected (indicated by red boxes and checkmarks). A red arrow points from the "Cloud Findings" filter dropdown to the selected findings.
- Step 2:** A red arrow points from the "Group by" dropdown menu to the "Group" icon in the toolbar.
- Step 3:** The "Add to group" dialog is open, showing options for "New group" (selected) and "Existing group". A red arrow points from the "New group" radio button to the "Name" input field.
- Step 4:** The "Create a new group" dialog is open, with the name "Test-group123" entered in the "Name" field. A red arrow points from the "Name" input field to the "Save" button.
- Step 5:** The "Filter" dialog is open, showing various filtering options. A red box highlights the "Group" dropdown under the "Select Fields to filter" section. A red arrow points from the "Group" dropdown to the "Group" input field at the bottom of the dialog.
- Step 6:** The "Group" input field in the "Filter" dialog contains the value "Test-group123". A red arrow points from the "Group" input field to the "Group" input field in the "Filter" dialog.

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

- 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 shows the ACCUKNOKX interface. On the left, there's a sidebar with various navigation options like Dashboard, Inventory, Issues, Findings (which is selected), Registry Scan, Compliance, Runtime Protection, Remediation, Monitors / Alerts, Identity, Reports, Notifications, and Settings. The main area shows a 'Findings' page with a search bar and filters for 'Cloud Findings' and 'Asset'. A specific finding titled 'Storage Account Logging Enabled: global' is highlighted with a yellow border. The finding details include a description: 'Ensures Activity Log alerts for the create/update and delete Storage Account events are enabled', a result section with a 'Low' risk factor, and a 'Details' panel on the right. The 'Status' dropdown in the details panel is set to 'In Progress' and is highlighted with a red box. A red arrow points from the text 'User can change status of the issue.' to this dropdown. The status dropdown also lists other options: Active, Exception Requested, Fixed, Potential, In Progress, Waiting For Verification, Accepted Risk, and Duplicate. At the bottom right, there's a note: 'Add comments and press Shift + Enter to submit'.

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 shows the AccuKnox interface with the 'Findings' tab selected. The 'Cloud Findings' filter is applied. A search bar contains the text 'cloudsploit'. The results table lists several findings, with one specific entry highlighted by a red box:

it seen	Assetname	Name	Risk factor	Description
14-08-19 07:18:05	6167e07f-ec68-49bf-a...	Azure Bastion Host Exists: italynorth	Medium	Ensure that there is at ...
14-08-19 07:18:05	6167e07f-ec68-49bf-a...	SQL Server Firewall Rule Alerts Monitor: global	Medium	Ensures Activity Log Ale...
14-08-19 07:18:05	6167e07f-ec68-49bf-a...	Azure Bastion Host Exists: eastus2euop	Medium	Ensure that there is at ...
14-08-19 07:18:05	6167e07f-ec68-49bf-a...	Azure Bastion Host Exists: norwaywest	Medium	Ensure that there is at ...
14-08-19 07:18:05	6167e07f-ec68-49bf-a...	Azure Bastion Host Exists: jbloindicentral	Medium	Ensure that there is at ...
14-08-19 07:18:05	6167e07f-ec68-49bf-a...	Azure Bastion Host Exists: southeastasia	Medium	Ensure that there is at ...
14-08-19 07:18:05	6167e07f-ec68-49bf-a...	Azure Bastion Host Exists: westeurope	Medium	Ensure that there is at ...
14-08-19 07:18:05	6167e07f-ec68-49bf-a...	PostgreSQL Flexible Server Logging Enabled: glo...	Medium	Ensures Activity Log ale...
14-08-19 07:18:05	6167e07f-ec68-49bf-a...	Azure Bastion Host Exists: norwayeast	Medium	Ensure that there is at ...

The right panel displays the details for the highlighted finding:

PostgreSQL Flexible Server Logging Enabled: global [Medium]

Description: Ensures Activity Log alerts for create/update and delete PostgreSQL Flexible Server events are enabled.

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

Filing since: about 1 month ago, on 22/07/2024

Last detected: on 19/08/2024

Compliance Frameworks: Coming Soon...

Asset Information:

```
{ "id": "d270c8ca-blob-40d4-abel-4401be7b3207", "tickets_count": 0, "data_type": "azure_subscription", "hash": "0ea23bb02ad89ecfc8f2fb5bd56a1", "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 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 Cloud type

Risk Factor

Unknown Informational Low Medium High Critical

Not Available

Ignored Exploit Available

True False

Exploit Available True False

Tickets Is New

True False

Exploit Available True False

Cloud type

azure_subscription

Location

global

Home > Issues > Findings Search anything...

Cloud Findings Asset Group by Saved Filters

Search

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

Total Records: 8

47

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 platform interface. On the left, there's a sidebar with various navigation options like Dashboard, Inventory, Issues, Compliance, and Cloud Assets Summary (which is currently selected). The main area is titled "Compliance" and "Cloud Assets Summary". It displays a list of compliance standards with their respective controls and compliance percentages. A red box highlights the "Azure CIS Benchmark" entry, which has 77 controls and 98.5% compliance. To the right, there are two tables: one for "Control" and "Assets" and another for "Description", "Compliance", and "Result". Both tables have rows corresponding to the benchmark controls, with some rows also highlighted by a red border.

Control	Assets	Description	Compliance	Result
1.23 Ensure That No Custom Subscription Policies Are Enabled	0	The principle of least privilege should ...	100 %	0 6 0 1 0
1.5 Ensure Guest Users Are Reviewed on a Regular Basis	0	Azure AD is extended to include Azure ...	100 %	0 0 1 0
2.11 Ensure That Microsoft Defender for Cloud Is Enabled	1	Microsoft Defender for DNS scans all n... Microsoft Defender for Cloud emails t...	0 %	1 0 0 0
2.15 Ensure that Auto Provisioning of New User Accounts Is Enabled	1	Enable automatic provisioning of the ...	0 %	1 0 0 0
2.19 Ensure Additional Email Address Is Enabled	0	Microsoft Defender for Cloud emails t...	0 %	1 0 0 0
2.15 Ensure That Microsoft Defender for SQL Is Enabled	1	Turning on Microsoft Defender for SQL...	0 %	1 6 0 0
2.17 Ensure That Microsoft Defender for Storage Is Enabled	1	Turning on Microsoft Defender for Stor...	0 %	1 0 0 0
2.18 Ensure That Microsoft Defender for Compute Is Enabled	1	Turning on Microsoft Defender for Com...	0 %	1 0 0 0
3.11 Ensure Soft Delete Is Enabled for All Storage Accounts	5	The Azure Storage blobs contain data...	91 %	5 0 52 0
3.15 Ensure the "Minimum TLS Version" Is Set to 1.3 or Higher	5	In some cases, Azure Storage sets the...	98 %	1 0 56 0
3.1 Ensure that Secure Transfer Requirements Are Met	5	Enable data encryption in transit.	98 %	1 6 0 56

Compliance failure for HIPPA Benchmark v2.0.0



- To Identify HIPPA 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 platform's Cloud Assets Summary feature. On the left, a sidebar navigation includes options like Dashboard, Inventory, Issues, Compliance (selected), Baselines, CSPM Executive Dashboard, Cloud Assets Summary (selected), Runtime Protection, Remediation, Monitors / Alerts, Identity, Reports, Notifications, and Settings. A 'Getting started: Onboarding' section lists Cloud Accounts, Clusters, and Registry.

The main area shows a 'Compliance' section with a summary: 25 Compliance found, 88.1% Compliant. Below this, a table lists various compliance frameworks and their controls and compliance percentages:

Control	Assets	Description	Compliance	Result
164.312(a)(1) Access Controls	17	Implement technical policies and pro...	95 %	3 Red, 2 Yellow, 15 Green, 280 Total
164.312(b) Audit Controls	0	Implement hardware, software, and/or...	96 %	2 Red, 5 Yellow, 0 Green, 55 Total
164.312(c) Integrity				
164.312(e)(1) Transmission Security				
164.312(e)(2)(ii) Encryption				

A red box highlights the 'HIPAA' row, which shows 5 controls and 97.6% compliant. Another red box highlights the '164.312(e)(2)(ii) Encryption' row. A red curved arrow points from the 'HIPAA' row towards the detailed view table below.

The detailed view table shows specific findings for storage accounts:

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

On the right, a filter sidebar allows users to search by program_name and result, with 'HIPAA' and 'FAILED' selected. The 'Apply' button is visible at the top right of the filter panel.

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.

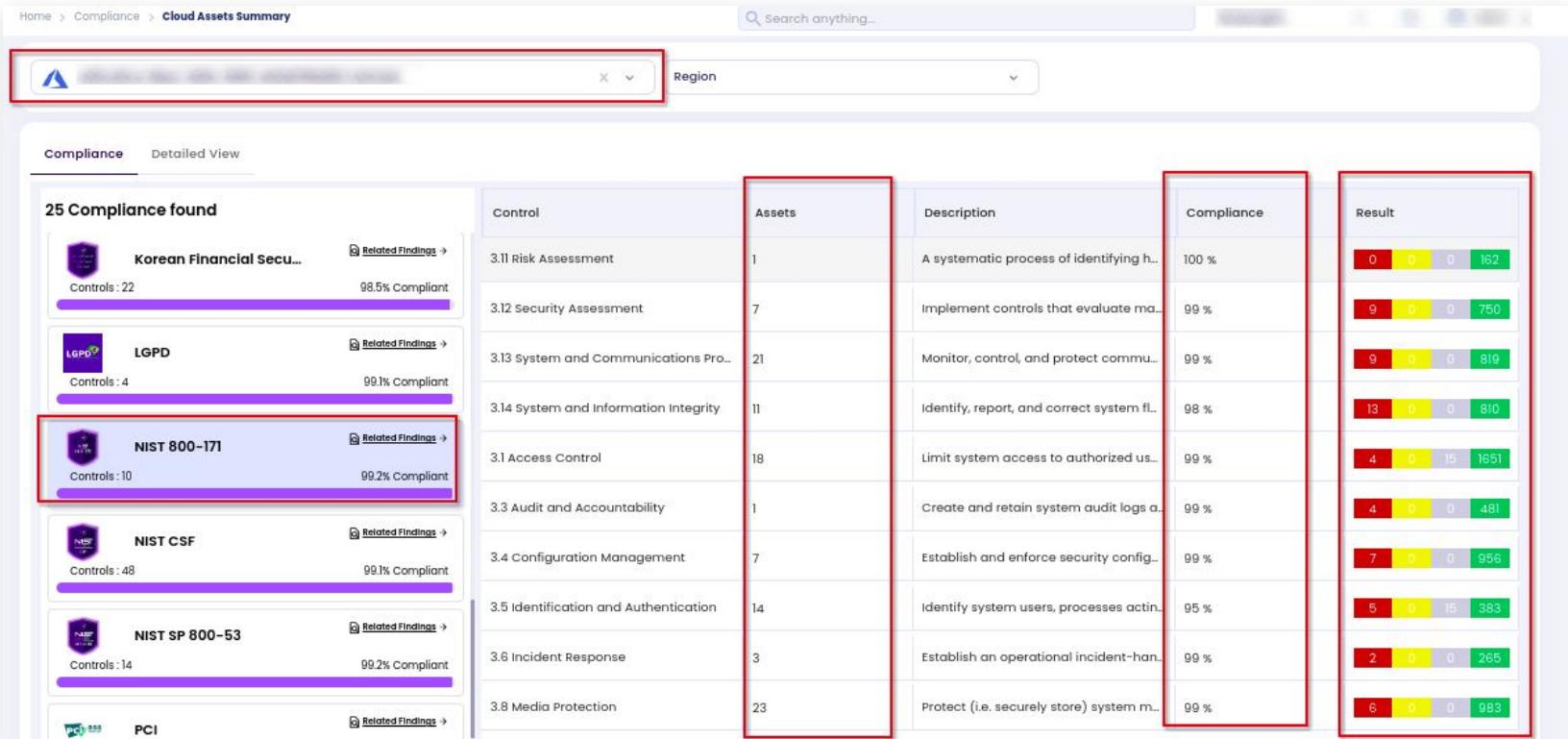
The screenshot shows the ACCUKNOX platform interface for Cloud Assets Summary. On the left, a sidebar lists various compliance frameworks: General Data Protection, HIPAA, HITRUST CSF, ISO 27001, ISO 27017, and ISO 27018. The ISO 27001 section is highlighted with a red box around its 'Related Findings' button. A red arrow points from this button to a callout box containing the text 'To get more detailed view of controls'. The main table displays controls, assets, descriptions, and compliance percentages. One row for 'A.12.4.3 Administrator and Operator Logon Controls' is selected and expanded, showing a detailed view of its findings. This detailed view table includes columns for Plugin, Asset, Message, Result, Severity, Compliance, Recommended Action, and Solution Reference Link. The 'Result' column uses a color-coded scale from green (Passed) to red (Failed).

Control	Assets	Description	Compliance	Result
A.10.1 Policy on the Use of Cryptographic...	17	A policy on the use of cryptographic c...	99 %	5 Passed, 0 Warning, 0 Failed, 497 Info
A.12.1.3 Capacity Management	1	The use of resources shall be monitor...	97 %	1 Passed, 0 Warning, 0 Failed, 97 Info
A.12.2.1 Controls Against Malware	7	Detection, prevention and recovery c...	100	7 Passed, 0 Warning, 0 Failed, 0 Info
A.12.4.1 Event Logging	3	Event logs recording user activities, ex...	97 %	3 Passed, 0 Warning, 0 Failed, 97 Info
A.12.4.2 Protection of Log Information	0	Logging facilities and log information ...	100	0 Passed, 0 Warning, 0 Failed, 100 Info
A.12.4.3 Administrator and Operator Logon Co...	0	System administrator and system operat...	97 %	0 Passed, 0 Warning, 0 Failed, 97 Info
A.12.5.1 Installation of Software on Operati...	0	Procedures shall be implemented to ...	0 %	0 Passed, 0 Warning, 0 Failed, 0 Info
A.12.6.1 Management of Systems Audit Con...	1	Information about technical vulnerab...	100	1 Passed, 0 Warning, 0 Failed, 0 Info
A.12.6.2 Restrictions on Software Installati...	0	Rules governing the installation of sof...	0 %	0 Passed, 0 Warning, 0 Failed, 0 Info
A.12.7.1 Information Systems Audit Con...	1	Audit requirements and activities inv...	99 %	1 Passed, 0 Warning, 0 Failed, 99 Info

Plugin	Asset	Message	Result	Severity	Compliance	Recommended Action	Solution Reference Link
openHadoopNa...	None	No securi...	PASSED	Medium	ISO 27001 +12	Restrict TCP port 8020 to kn...	https://learn.microsoft.com/
scaleSetMultiAz	None	No existin...	PASSED	Low	NIST CSF +6	Multiple zones can only be ...	https://learn.microsoft.com/
identityEnabled	None	No existin...	PASSED	Low	ISO 27001 +13	Enable system or user-assi...	https://learn.microsoft.com/
blobContainersP...	None	No existin...	PASSED	High	ISO 27001 +18	Ensure each blob containe...	https://learn.microsoft.com/
tlsVersionCheck	None	No existin...	PASSED	Low	NIST SP 800-53 +16	Set the minimum TLS versio...	https://azure.microsoft.com/
openTelnet	None	No securi...	PASSED	Medium	SOC 2 TYPE II +13	Restrict TCP port 23 to kno...	https://learn.microsoft.com/
resourceusageL...	/subscrib...	None of t...	PASSED	Low	FISMA +6	Check if resources are clo...	https://learn.microsoft.com/
identityEnabled	None	No existin...	PASSED	Low	ISO 27001 +13	Enable system or user-assi...	https://learn.microsoft.com/
vmDiskDataEncr...	None	No existin...	PASSED	Medium	HITRUST CSF +22	Enable VM Data Disk Encry...	https://learn.microsoft.com/
storageAccount...	None	No storag...	PASSED	High	FISMA +21	Enable the HTTPS-only opti...	https://learn.microsoft.com/

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 shows the ACCUKNOKX Cloud Asset Summary dashboard. At the top, there's a navigation bar with 'Home', 'Compliance', and 'Cloud Assets Summary'. A search bar says 'Search anything...'. Below the navigation is a header with a logo, a close button, and a dropdown for 'Region'. The main area has tabs for 'Compliance' (selected) and 'Detailed View'. A section titled '25 Compliance found' lists several benchmarks with their logos, controls count, and compliance percentage. One row for 'NIST 800-171' is highlighted with a red box. The main table below has columns: 'Control', 'Assets', 'Description', 'Compliance', and 'Result'. Each row in the table also has a red box around it. The 'Compliance' column shows percentages like 100%, 99%, etc. The 'Result' column shows counts of failing, warning, and passing items.

Control	Assets	Description	Compliance	Result
3.11 Risk Assessment	1	A systematic process of identifying h...	100 %	0 0 0 162
3.12 Security Assessment	7	Implement controls that evaluate ma...	99 %	9 0 0 750
3.13 System and Communications Pro...	21	Monitor, control, and protect commu...	99 %	9 0 0 819
3.14 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 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 0 383
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

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.				

Finding for in resource [REDACTED]

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

Last detected on 11/08/2024

Compliance Frameworks
Coming Soon...

Asset Information
[REDACTED]

Create Ticket

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

compliance X ▼

Close

Create Ticket

Home > Issues > Findings > Create Ticket

Ticket 1

Create ticket

Priority: Priority

Ticket Title: PostgreSQL Flexible Server Logging End

Ticket Description: Ensures Activity Log alerts for create/update and delete PostgreSQL Flexible Server events are enabled.

Synopsis

Impacted Assets

Asset	Port
global	

solution

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>

Plugin output

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

The screenshot shows the AccuKnox Cloud Assets interface. At the top, there are navigation links: Home > Inventory > Cloud Assets. A search bar is present above the main content area. The main area has tabs for Cloud Accounts (3), VMs (9), Clusters (0), Storage, Functions, and Database. Below these tabs is a 'Findings' section. The 'Findings' section includes a search bar with 'test-ticket' entered, and filters for Group by, Data Type, Risk Factor, Status, Tickets, and Exploit Available. There is also a 'Create a ticket' button with a circled red border. The main table displays findings for an Azure account labeled 'AZICMA'. The table columns are Asset, Label, Findings, and Last Scan date. The 'Findings' column contains numerical values (e.g., 2, 61, 74, 3, 1) with colored dots (red, yellow, green). A red box highlights the 'Findings' column header, and a red arrow points from the bottom of this box to the 'Findings' column in the table. A red box also highlights the 'Create a ticket' button. The table rows show various findings such as 'Security Policy Alerts Enabled: global', 'Azure Bastion Host Exists: switzerlandn', 'Key Vault In Use: brazilsouth', etc. The last row of the table is highlighted with a red box.

Asset	Label	Findings	Last Scan date
a05cd3ca-8bec-428c-	AZICMA	2 61 74	2024-08-11
7601cf2f-819e-49d1-b4c-	AZICMA		2024-08-11
AzureBackupRG_eastus_	AZICMA	1	2024-08-11
AzureUpdateManager...	AZICMA	1	2024-08-11
AzureAutomationAccou...	AZICMA	3 1	2024-08-11
AZICMA-EnvRD-DG	AZICMA		2024-08-11

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 shows the AccuKnox platform interface. On the left, there's a sidebar with various navigation options like Dashboard, Inventory, Issues, Compliance, Baselines, CSPM Executive Dashboard, and Cloud Assets Summary. The 'Cloud Assets Summary' option is highlighted with a red box. The main content area has a header 'Home > Compliance > Cloud Assets Summary'. Below the header, there's a search bar with a red box around it. The main content is divided into two tabs: 'Compliance' (selected) and 'Detailed View'. Under 'Compliance', there's a table with columns 'Plugin', 'Asset', and 'Message'. One row in the table is highlighted with a red box and corresponds to the 'storageAccountsHttps' finding. The 'Detailed View' tab shows a detailed view of this finding. The finding is titled 'storageAccountsHttps [High]'. It includes a 'Description' section stating 'Ensures HTTPS-only traffic is allowed to storage account endpoints', a 'Finding for in resource' section, and a 'Category: Storage Accounts' section. To the right of the finding details, there's a 'Recommended Actions' section with a button 'Enable the HTTPS-only option for all Storage Accounts.' A 'Details' section and a 'Create Ticket' button are also present. At the bottom of the finding view, there's a 'Compliance Frameworks' section with several icons and a 'Compliance Sub Controls' section with a table of controls and their status.



GCP Risk Assessment

Compliance failure and Misconfiguration

How to identify open SSH port?



- To identify if the SSH port is open to the 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 shows the ACCUKNOX interface. On the left sidebar, the 'Findings' menu item is highlighted with a red box. The main content area displays a finding titled 'Open SSH: global' with a 'High' severity level. A red box highlights the 'Cloud Findings' dropdown in the top navigation bar. The finding details include a description ('Determines if TCP port 22 for SSH is open to the public'), a failing status ('Failing since about 1 month ago, on 21/07/2024'), and a last detected date ('07/08/2024'). It also lists 'Asset Information' and 'Compliance Frameworks' (Coming Soon...). The right side shows the 'Details' tab with asset information like 'default-allow-rdp', asset type 'gcp_compute_firewall', and status 'Active'. A note section at the bottom allows adding comments.

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

The screenshot shows the AccuKnox Cloud Assets dashboard. The left sidebar has a red box around the 'Cloud Assets' option. The main area shows a summary of 4 Cloud Accounts and 23 VMs. A modal window titled 'Asset details' is open for an asset named 'instance-20240802-093858'. The modal includes fields for Asset Name, Parent, Label, Category, Last Seen, and Region. Below these are four metrics: Tickets (0), Groups (0), Audit Files (0), and Monitors (0). To the right is a 'Vulnerabilities' chart with a yellow and red segment. At the bottom, a search bar has '19JUNESS' selected, and a red box highlights the 'Asset Category' dropdown set to 'gcp_compute_instance'. A red arrow points from this dropdown to a table below. The table lists three assets: 'instance-20240802-09...', 'instance-20240805-11...', and 'instance-20240807-08...'. Each row shows a red '1' and a yellow '6' under the 'Findings' column, indicating 6 findings per asset.

Asset	Label	Findings	Last Scan date	Asset Category	Asset type	Monitors	Regions
instance-20240802-09...	19JUNESS	1 6	2024-08-05	Host	gcp_compute_instance	0	us-central1-b
instance-20240805-11...	19JUNESS	1 6	2024-08-07	Host	gcp_compute_instance	0	us-central1-f
instance-20240807-08...	19JUNESS	1 6	2024-08-13	Host	gcp_compute_instance	0	us-central1-a

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 illustrates the AccuKnox interface for identifying compute disk security issues. On the left, the navigation bar highlights the 'Cloud Assets' section. The main dashboard shows summary counts for Cloud Accounts (4), VMs (23), Clusters (4), and Storage (35). A red box and arrow point to the 'Asset Category' dropdown in the search bar, which is set to 'gcp_compute_disk'. The results table lists four findings:

Last seen	Risk Factor	Finding	Status	Ignored	Exploit Avail...	Tickets	Data Type
2024-07-25	Medium	CSEK Encryption Enabled: us-central1	Active	False	False	0	cloudsploit
2024-07-25	Low	Disk MultiAz: us-central1	Active	False	False	0	cloudsploit
2024-07-25	Low	VM Disks CMK Encryption: us-central1	Active	False	False	0	cloudsploit
2024-07-25	Low	Disk Automatic Backup Enabled: us-central1	Active	False	False	0	cloudsploit

A red double-headed arrow connects the highlighted finding in the table back to the 'Findings' section of the dashboard, which displays the same four items.

How to identify publicly exposed ports?



- To identify 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 shows the AccuKNOX interface. On the left, the navigation bar includes 'Findings' (highlighted with a red box). The main panel displays a list of findings under 'Cloud Findings' with a 'High' risk filter applied. One finding is shown in detail:

Description: Determines if all ports are open to the public

Finding for in resource: gcp_compute_firewall | alkow-all

Status: Failing since about 2 day ago, on 05/08/2024

Last detected: 07/08/2024

Compliance Frameworks: Coming Soon...

Asset Information:

```
Id: "57d7970b-823d-48e7-b0e5-380e534b4065"
tickets_count: 0
data_type: "gcp_compute_firewall"
hash: "90ec9d82b973b75087d1476b053327c0"
history: []
date_discovered: "2024-08-05T06:09:25.249658Z"
last_seen: "2024-08-07T01:02:23.421200Z"
data_id: "757010953003227000"
data_ctx: {
  steampipe: {
    sdk_version: "5.10.0"
  }
  connection_name: "gcp"
}
data_alkas: [
  0: "gcp://compute.googleapis.com/projects/shaped-infus...
]
```

Details Panel (Right):

- Asset:** alkow-all
- Asset Type:** gcp_compute_firewall
- Status:** Active
- Ignored:** No
- Severity:** High (highlighted with a red box)
- Tickets:** 0
- Notes:** Add Comments and Press Ctrl + Enter to Submit
- Exploit Available:** True False
- Tickets Is New:** True False
- Location:** Location
- Cloud account:** shaped-infusion-402417 (highlighted with a red box)

Filter Panel (Top Right):

- Data Type: cloudsplint
- Select Fields to filter: misc__cloud_account
- Location: Cloud account
- Risk Factor: Unknown, Informational, Low, Medium, High (highlighted with a red box), Critical
- Not Available
- Ignored: True False
- Exploit Available: True False
- Tickets: True False
- Is New: True False
- Location: Location
- Cloud account: Cloud account

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 shows the ACCUKNOX platform's 'Findings' section. At the top, there is a search bar with dropdowns for 'Cloud Findings', 'Asset', and 'Finding'. A red box highlights the 'Cloud Findings' dropdown. To the right is a 'Filter' panel with tabs for 'Saved Filters' and 'New Filter'. The 'New Filter' tab is active, showing a 'Data Type' dropdown set to 'cloudsploit' and a 'Select Fields to filter' dropdown set to 'misc__cloud_account'. Below these are sections for 'Risk Factor' (with buttons for Unknown, Informational, Low, Medium, High, and Critical, where Medium, High, and Critical are highlighted with a red border), 'Not Available', 'Ignored', 'Exploit Available', 'Tickets', 'Is New', 'Location' (with a dropdown set to 'Location'), and 'Cloud account' (with a dropdown set to 'accuknox-cnapp'). A red box highlights the 'Cloud account' dropdown. At the bottom left, it says 'Total Records: 52'. The main table lists findings with columns: Count, Last seen, Assetname, Name, Risk factor, Description, Status, and Location. Several rows are highlighted with red boxes, particularly the first row and the last two rows.

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-default	CSEK Encryption Enabled: us-central	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-ngl	Instance Automatic Restart Enabled: us-c...	Medium	Ensure that Virtual Machine instances have automatic re...	Active	us-central
5	2024-08-07 07:12:38	gke-ravi-cluster-default	Instance Level SSH Only: us-central	High	Ensures that instances are not configured to allow projec...	Active	us-central
5	2024-07-25 06:56:42	gke-aryan-cluster-ngl	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-c...	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-alb2f5d12b65d4...	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

1 2 3

accuknox-cnapp

60

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

Home > Issues > Findings

Search anything... solutions

Cloud Findings Asset Asset

Search

11 issues found across shaped-infusion-402417
shaped-infusion-402417

Count	Last seen	Assetname	Name	Risk	Asset ID	Asset Type	Asset Category
2	2024-08-19 08:23:45	k8s-fw-a21fb58e851e94...	Open HTTP: global	High	o2790399-c26c-4a8a-b82a-d2f05f92763d	gcp_project	Cloud Account
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	79312cd2456f75b0df32...	Service Account Managed Keys: glob...	Low			
6	2024-08-05 13:23:07	instance-20240802-09...	Disk MultiAz: us-central	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

Assets

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 Loggi...	Low	Ensures that logging an...	Active	global
2024-08-19 08:23:45	shaped-infusion-402417	Storage Permissions Log...	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 shows the AccuKnox platform interface for managing findings. The top navigation bar includes 'Home', 'Issues', and 'Findings'. The search bar contains 'Cloud Findings' and 'Asset'. A red box highlights the 'Finding' input field. The main table lists findings with columns: Count, Last seen, Assetname, Name, Risk factor, Description, Status, and Location. A red box highlights a finding for 'pvc-3435a2da-503d-4...' with a 'Medium' severity level. A modal window for this finding is open, showing details like 'Disk In Use: us-central' and 'Medium'. The modal also displays the finding's description: 'Ensure that there are no unused Compute disks.' Below the table, a summary states 'Total Records: 48'.

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	Ensures		
1	2024-08-19 08:23:45	allow-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

Details [+ Create Ticket](#)

Asset pvc-3435a2da-503d-47ac-b6f5-43cd1a03511d

Asset Type gcp_compute_disk

Status Active

Ignored No

Severity Medium

Tickets 0

Description Disk In Use: us-central

Result Medium

Solution

References

Source Code

Finding for in resource `gcp_compute_disk` | `pvc-3435a2da-503d-47ac-b6f5-43cd1a03511d`

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

Last detected on 19/08/2024

Compliance Frameworks Coming Soon...

Asset Information

`{ "id": "4a701788-4e51-43aa-af81-b5108c7b4179", "tickets_count": 0, "data_type": "gcp_compute_disk" }`

How to identify if service account keys are exposed?



- To identify 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

The screenshot shows the ACCUKNOX platform interface. On the left, the navigation bar includes 'Dashboard', 'Inventory', 'Issues' (selected), 'Findings' (highlighted with a red box), 'Registry Scan', 'Compliance', 'Runtime Protection', 'Remediation', 'Monitors / Alerts', 'Identity', 'Reports', 'Notifications', and 'Settings'. A sidebar at the bottom has sections for 'Getting started: Onboarding', 'Cloud Accounts', 'Clusters', and 'Registry', with a total of 69 records.

The main area displays a 'Findings' table with columns: 'Asset ID', 'Last Seen', 'Status', and 'Actions'. One row is highlighted with a red box, showing 'id': 'a12058931e327bf9c90e653f4f944d879a9cdb6e', 'Last seen': '2024-08-07 07:12:38', 'Status': 'default', and an 'Edit' button.

A modal window titled 'Service Account Key Rotation: global' (Medium risk) is open. It contains tabs for 'Description', 'Result', 'Solution', 'References', and 'Source Code'. The 'Description' tab shows: 'Ensures that service account keys are rotated within desired number of days.' The 'Result' tab lists findings: 'Finding for in resource | gcp_service_account_key | a12058931e327bf9c90e653f4f944d879a9cdb6e', 'Failing since about 1 month ago, on 21/07/2024', and 'Last detected on 07/08/2024'. The 'Asset Information' tab shows JSON data for the asset ID, including fields like 'id', 'tickets_count', 'data_type', 'hash', 'history', 'date_discovered', 'last_seen', 'data__ctx', 'data__akos', and 'data__name'. The 'Details' tab on the right shows asset information: 'Asset' (id: a12058931e327bf9c90e653f4f944d879a9cdb6e), 'Asset Type' (gcp_service_account_key), 'Status' (Active), 'Ignored' (No), and 'Severity' (Medium). The 'Tickets' section shows 0 tickets.

A second modal window titled 'Service Account Key Rotation: global' (Medium risk) is also open, showing the 'Solution' tab (highlighted with a red box). It provides a solution: '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 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 shows the ACCUKNOX platform interface. On the left, there's a sidebar with various navigation options like Dashboard, Inventory, Issues, Findings (which is selected and highlighted with a red box), Registry Scan, Compliance, Runtime Protection, Remediation, Monitors / Alerts, Identity, Reports, Notifications, and Settings. Below the sidebar, there's an 'Ask Ada' AI feature and a 'Getting started: Onboarding' section with links for Cloud Accounts, Clusters, and Registry.

The main area shows a 'Findings' page with a search bar and a filter dropdown set to 'Cloud Findings'. A modal window is open, titled 'Service Account Admin: global' with a 'Medium' risk level. The modal contains the following 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:** (empty)

The modal also includes tabs for Description, Result, Solution, References, and Source Code. The 'Description' tab is active, showing the following text:

Ensure that no service accounts have admin, owner, or write privileges.,
<https://cloud.google.com/iam/docs/overview>

How to identify if RDP port exposed to public?



- To identify if rdp ports are 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**

The screenshot illustrates the process of identifying an exposed RDP port using the ACCUKNOX platform.

Left Panel (Navigation): Shows the main navigation menu with "Findings" selected. Other options include Dashboard, Inventory, Issues, Registry Scan, Compliance, Runtime Protection, Remediation, Monitors / Alerts, Identity, Reports, Notifications, and Settings.

Middle Panel (Findings List): Displays a list of findings under the "Cloud Findings" filter. One finding is highlighted: "Open RDP: global" with a "High" severity level. A red box highlights the "High" severity button. Below the finding, a detailed description states: "Determines if TCP port 3389 for RDP is open to the public".

Right Panel (Details View): Provides detailed information about the finding. It includes:

- Details:** Asset: default-allow-rdp, Asset Type: gcp_compute_firewall, Status: Active, Ignored: No, Severity: High, Tickets: 0.
- Description:** "Failing since about 8 day ago, on 05/08/2024".
- Asset Information:** A JSON snippet showing asset details, including an "id" field and a "data__ctx" field containing a "steampipe" object with a "sdk_version" of "5.10.0".
- Solution:** "Restrict TCP port 3389 to known IP addresses., <https://cloud.google.com/vpc/docs/using-firewalls>".

Filter Bar (Top Right): Includes "Filter", "Clear Filter", "Save", and "Apply" buttons. The "Apply" button is highlighted with a red box.

Filter Sidebar (Right): Allows filtering by Data Type (selected: "cloudsplot"), Select Fields to filter (selected: "Cloud account"), Location (selected: "Cloud account"), Risk Factor (selected: "High" and "Critical"), Ignored (selected: "True" and "False"), Exploit Available (selected: "True" and "False"), Tickets (selected: "True" and "False"), Is New (selected: "True" and "False"), Location (selected: "Location"), Cloud account (selected: "shaped-infusion-402417").

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 shows the ACCUKNOX interface with the following details:

- Left Sidebar:** Includes sections for Dashboard, Inventory, Issues (selected), Findings (highlighted), Registry Scan, Compliance, Runtime Protection, Remediation, Monitors / Alerts, Identity, Reports, Notifications, and Settings.
- Top Navigation:** Home > Issues > Findings.
- Filter Bar:** Shows "Cloud Findings" selected and "Affected Assets" highlighted.
- Findings Table:** A table titled "Affected Assets" showing 13 findings related to "Open HTTP: global".

Finding	Risk Factor	Description	Status	Global
Open HTTP: global	Not_available	Determines if TCP port ...	Active	global
Open HTTP: global	Not_available	Determines if TCP port ...	Active	global
Open HTTP: global	Not_available	Determines if TCP port ...	Active	global
Open HTTP: global	Not_available	Determines if TCP port ...	Active	global
Open HTTP: global	Not_available	Determines if TCP port ...	Active	global
Open HTTP: global	Not_available	Determines if TCP port ...	Active	global
Open HTTP: global	Not_available	Determines if TCP port ...	Active	global
Open HTTP: global	Not_available	Determines if TCP port ...	Active	global
Open HTTP: global	Not_available	Determines if TCP port ...	Active	global
Open HTTP: global	Not_available	Determines if TCP port ...	Active	global
Open HTTP: global	Not_available	Determines if TCP port ...	Active	global
Open HTTP: global	Not_available	Determines if TCP port ...	Active	global
- Details Panel:** Shows a detailed view of one finding, including its description, result, solution, references, and source code.
- Bottom Status:** Total Records: 10 and Total Records: 13.

How to identify if logging is enabled for storage?



- To identify 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 shows the ACCUKNOX platform interface. On the left, there's a sidebar with various navigation options like Dashboard, Inventory, Issues, Findings (which is selected and highlighted in red), Registry Scan, Compliance, Runtime Protection, Remediation, Monitors / Alerts, Identity, Reports, Notifications, and Settings. Below the sidebar, there's an 'Ask Ada' feature and a 'Getting started: Onboarding' section with links for Cloud Accounts, Clusters, and Registry.

The main area shows a search bar with 'storage' entered. A modal window is open for a finding titled 'Storage Permissions Logging: global' (Medium severity). The modal has tabs for Description, Result, Solution, References, and Source Code. The 'Description' tab contains the following text:
Ensures that logging and log alerts exist for storage permission changes
Finding for in resource: gcp_project | accuknox-cnapp
Failing since about 1 month ago, on 20/07/2024
Last detected on 07/08/2024

The 'Asset' section shows the asset is 'accuknox-cnapp' and the 'Asset Type' is 'gcp_project'. The 'Status' is 'Active' and 'Ignored' is set to 'No'. The 'Severity' is 'Medium'. The 'Details' tab shows the following JSON snippet:

```
{
  "id": "80d12595-3a5e-47ac-8cba-c98768101d23",
  "tickets_count": 0,
  "data_type": "gcp_compute_zone",
  "hash": "cb889db755ca8408e259c9f3le2345f4",
  "history": [],
  "date_discovered": "2024-08-07T01:48:38.617075Z",
  "last_seen": "2024-08-07T01:47:20.713477Z",
  "data_id": "2530",
  "data_ctx": {
    "stampeipe": {
      "sdk_version": "5.10.0"
    },
    "connection_name": "gcp"
  },
  "data_aka": [
    {
      "0": "gcp/compute.googleapis.com/projects/accuknox-cna..."
    }
  ]
}
```

The 'Solution' tab contains the following text:
Ensure that log metric and alert for storage permission changes.,
<https://cloud.google.com/logging/docs/logs-based-metrics/>

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



- To identify if instances 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 shows the ACCUKNOX interface with the 'Findings' tab selected. A search bar at the top contains the query 'Instance Level SSH Only: us-central1'. The results table lists several findings, each with a checkbox, last seen timestamp, asset ID, and resource type. One finding is highlighted with a red border:

Asset	Description	Result	Solution	References	Source Code
gke-ravi-cluster-default-pool-adad9155-kdxw	Ensures that instances are not configured to allow project-wide SSH keys	High			
gcp_compute_instance	Finding for in resource gcp_compute_instance gke-ravi-cluster-default-pool-adad9155-kdxw				
gke-ravi-cluster-default-pool-adad9155-kdxw	Failing since about 1 day ago, on 06/08/2024				
gke-ravi-cluster-default-pool-adad9155-kdxw	Last detected on 07/08/2024				
accuknox	Compliance Frameworks Coming Soon...				
accuknox	Asset Information				
accuknox	{ "id": "784870b9-1088-4a5f-8fb7-bebfeb7577d7", "tickets_count": 0, "data_type": "gcp_compute_instance", "hash": "4ff65146e5645bca5d7d00b58a85e2", "history": [], "date_discovered": "2024-08-06T01:40:48.346869Z", "last_seen": "2024-08-07T01:47:20.713477Z", "data_id": 6778012594026671000, "data_ctx": { "steampipe": { "sdk_version": "5.10.0" } }, "connection_name": "gcp", "data_akas": [0: "gcp://compute.googleapis.com/projects/accuknox-cna..."] }				

A modal window for the highlighted finding is open, showing detailed information:

Details	+ Create Ticket
Asset gke-ravi-cluster-default-pool-adad9155-kdxw Asset Type gcp_compute_instance Status Active Ignored No Severity High Tickets	

The bottom section of the page displays a summary of the finding:

Instance Level SSH Only: us-central1 High

Description	Result	Solution	References	Source Code
Ensure project-wide SSH keys are blocked for all instances. https://cloud.google.com/compute/docs/instances/adding-removing-ssh-keys				

Compliance failure for CIS Benchmark



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

The screenshot shows the ACCUKNOX platform interface. On the left, the navigation menu is visible with the 'Cloud Assets Summary' option selected. The main content area displays the 'Compliance' section under 'Cloud Assets Summary'. A search bar at the top right contains the query 'accuknox-cnapp | GCP25JAN'. Below the search bar, there is a 'Region' dropdown set to 'Region'. The 'Compliance' tab is selected, showing a list of 25 found compliances. The 'CIS GCP Benchmark' entry is highlighted with a red box and has its details expanded. This entry includes a 'Related Findings' link, 'Controls: 48', and '80.6% Compliant'. The expanded view shows a table of controls with their descriptions, assets, and compliance percentages. The 'Compliance' column shows values like 100%, 100%, 67%, 0%, etc., and the 'Result' column shows a 4x6 grid of colored squares (red, yellow, green) representing the status for each control. The bottom of the table shows a total of 48 records.

Control	Assets	Description	Compliance	Result
1.1 Ensure that Separation of duties is ...	0	It is recommended that the principle ...	100 %	0 0 0 1
1.1 Ensure that corporate login credentia... l	0	Use corporate login credentials inste...	100 %	0 0 0 1
1.4 Ensure that there are only GCP-ma... naged service accounts	57	User managed service accounts shou...	67 %	19 0 0 38
1.5 Ensure that Service Account has n... o password	4	A service account is a special Google ...	0 %	4 0 0 0
1.6 Ensure that IAM users are not assig... ned to multiple projects	0	It is recommended to assign the Servic...	100 %	0 0 0 1
1.7 Ensure user-managed/external ke... ys are used for service accounts	19	Service Account keys consist of a key ...	26 %	14 0 0 5
1.8 Ensure that Separation of duties is ... is enforced	0	It is recommended that the principle ...	100 %	0 0 0 1
2.10 Ensure that the log metric filter an... d sink is configured correctly	0	It is recommended that a metric filter ...	0 %	1 0 0 0
2.11 Ensure that the log metric filter an... d sink is configured correctly	0	It is recommended that a metric filter ...	100 %	0 0 0 1
2.1 Ensure that Cloud Audit Logging is ... enabled	0	It is recommended that Cloud Audit Logg...	0 %	1 0 0 0
2.2 Ensure that sinks are configured fo... r Cloud Audit Logging	0	It is recommended to create a sink th...	0 %	1 0 0 0

Compliance failure for ISO 27001 Benchmark



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

The screenshot shows the ACCUKNOX platform interface. On the left, a sidebar navigation includes: Dashboard, Inventory, Issues, Compliance (selected), Baselines, CSPM Executive Dashboard, Cloud Assets Summary (selected), Runtime Protection, Remediation, Monitors / Alerts, Identity, Reports, Notifications, Settings, and an Ask Ada BETA button. A Getting started: Onboarding section lists Cloud Accounts, Clusters, and Registry.

The main content area is titled "Cloud Assets Summary" under "Compliance". It displays a summary of 25 found compliances, including ISO 27001, ISO 27017, ISO 27018, Korean Financial Secu..., LGPD, and NIST 800-171. Each entry shows the number of controls and a compliance percentage. The ISO 27001 entry is highlighted with a red border.

A detailed view of the ISO 27001 findings is shown in a table:

Control	Assets	Description	Compliance	Result
A.10.1 Policy on the Use of Cryptograph...	1	A policy on the use of cryptographic c...	97 %	1 0 0 35
A.10.2 Key Management	0	A policy on the use, protection and lif...	100 %	0 0 0 37

Below this, a sub-table for "A.12.2.1 Controls Against Mal" shows multiple rows of findings, each with a red "FAILED" status and "Low" severity. The table has columns: Control, Asset, Message, Result, Severity, Compliance, Recommended Action, and Solution Reference Link.

Control	Asset	Message	Result	Severity	Compliance	Recommended Action	Solution Reference Link
A.12.3.1 Information Backup	flowLogsEnabled	projects/ac...	FAILED	Low	KOREAN FINANCIAL SECU	Enable VPC flow logs for each VPC subnet	https://cloud.google.com/vpc/docs/using-fl
A.12.4.1 Event Logging	vpcNetworkRouteLogging	None	FAILED	Medium	FISMA	Ensure that log metric and alert exist for VP...	https://cloud.google.com/logging/docs/logi
A.12.4.3 Administrator and C	flowLogsEnabled	projects/ac...	FAILED	Low	KOREAN FINANCIAL SECU	Enable VPC flow logs for each VPC subnet	https://cloud.google.com/vpc/docs/using-fl
A.12.7.1 Information Systems	flowLogsEnabled	projects/ac...	FAILED	Low	KOREAN FINANCIAL SECU	Enable VPC flow logs for each VPC subnet	https://cloud.google.com/vpc/docs/using-fl
A.13.1.1 Network Controls	loggingEnabled	projects/ac...	FAILED	Medium	KOREAN FINANCIAL SECU	Enable VPC flow logs for each VPC subnet	https://cloud.google.com/vpc/docs/using-fl
A.13.1.3 Segregation in Netw	flowLogsEnabled	projects/ac...	FAILED	Low	SOC 3	+14 Ensure that logging is enabled on all Kuber...	https://cloud.google.com/monitoring/kuber
A.13.2.1 Information Transfer	flowLogsEnabled	projects/ac...	FAILED	Low	KOREAN FINANCIAL SECU	Enable VPC flow logs for each VPC subnet	https://cloud.google.com/vpc/docs/using-fl
A.13.2.3 Electronic Messagin	flowLogsEnabled	projects/ac...	FAILED	Low	KOREAN FINANCIAL SECU	Enable VPC flow logs for each VPC subnet	https://cloud.google.com/vpc/docs/using-fl
Total Records: 30	flowLogsEnabled	projects/ac...	FAILED	Low	KOREAN FINANCIAL SECU	Enable VPC flow logs for each VPC subnet	https://cloud.google.com/vpc/docs/using-fl
	flowLogsEnabled	projects/ac...	FAILED	Low	KOREAN FINANCIAL SECU	Enable VPC flow logs for each VPC subnet	https://cloud.google.com/vpc/docs/using-fl
	flowLogsEnabled	projects/ac...	FAILED	Low	KOREAN FINANCIAL SECU	Enable VPC flow logs for each VPC subnet	https://cloud.google.com/vpc/docs/using-fl
	flowLogsEnabled	projects/ac...	FAILED	Low	KOREAN FINANCIAL SECU	Enable VPC flow logs for each VPC subnet	https://cloud.google.com/vpc/docs/using-fl

At the bottom of the page, there are navigation links for "Total Records: 49" and page numbers 1, 2, 3, and 70.

Compliance failure for PCI DSS Benchmark



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

The screenshot shows the AccuKnox Compliance interface. On the left, there's a summary of found controls for various frameworks: NIST CSF (81.7% Compliant), NIST SP 800-53 (80.6% Compliant), PCI (95.4% Compliant), and SOC 2 Type II (84.9% Compliant). The PCI section is highlighted with a red box. On the right, a detailed view of the PCI findings is shown. A specific finding for 'storagePermissionsLogging' is highlighted with a red box. The finding details are as follows:

storagePermissionsLogging [Medium]

Description
Ensures that logging and log alerts exist for storage permission changes

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
C.I.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 3.1.4 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 shows the AccuKnox Compliance interface. On the left, there's a sidebar with compliance summaries for various frameworks:

- NIST CSF: Controls: 8, 81.7% Compliant
- NIST SP 800-53: Controls: 32, 80.6% Compliant
- PCI: Controls: 13, 81.3% Compliant
- SOC 2 Type II: Controls: 10, 84.9% Compliant (highlighted with a red box)
- SOC 3: Controls: 5, 9.1% Compliant

The main area is titled "Compliance Detailed View". It shows a table of controls and their associated assets and descriptions. A secondary table on the right provides a detailed view of specific findings, with the "Result" and "Severity" columns highlighted by a red box.

Control	Assets	Description	Compliance	Result	Severity	Compliance	Recommended Action	Solution Reference Link
A1.1	Plugin	Asset	Message	FAILED	Medium	NIST CSF +15	1. Enter the VPC Network service. 2. Enter the...	https://cloud.google.com/vpc/docs/configu
A1.2	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
CC2.1	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
CC5.1	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
CC6.1	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
CC6.2	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
CC6.3	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
CC6.6	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
CC6.7	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
CC7.1	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
	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
	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
	osLoginEnabled	None	OS login is ...	FAILED	Low	IGPD +15	Set enable-oslogin in project-wide metad...	https://cloud.google.com/compute/docs/in

Total Records: 35

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 : "44f30fb...
tickets_count : 0
data_type : "gcp_compute_firewall"

Create Ticket

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

compliance X

Close Create Ticket

+ Create Ticket

Details

Asset: default-allow-ssh
Asset Type: gcp_compute_firewall
Status: Active
Ignored: No
Severity: High
Tickets: 0

Create ticket

Priority: Priority
Ticket Title*: Open SSH: global
Ticket 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

Assistive Remediation For GCP 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

The screenshot illustrates the process of creating a ticket for a selected finding in the AccuKnox platform.

Cloud Assets View: The top section shows a table of assets with columns: Asset, Label, Findings, Last Scan date, Asset Category, Asset type, Monitors, and Regions. A red box highlights the 'Findings' column for the first asset, which contains three yellow numbers (1, 5, 5). A red arrow points from this box down to the 'Findings' card below.

Findings View: The bottom section shows a detailed view of findings. It includes a search bar and various filters: compliance, Group by, Data Type, Risk Factor, Ignored, Status, Tickets, Exploit Available, and Last seen. A red box highlights the 'Create a ticket' button in the top right corner of this card.

Selected Finding: Below the findings card, a table lists specific findings with columns: Last seen, Risk Factor, Finding, Status, Ignored, Exploit Avail..., Tickets, and Data Type. One finding is selected, indicated by a checked checkbox in the first column. This selected finding is also highlighted with a red box.

Last seen	Risk Factor	Finding	Status	Ignored	Exploit Avail...	Tickets	Data Type
2024-08-07	Medium	VPC Network Logging: global	Active	False	False	0	cloudsploit
2024-08-07	Low	OS Login Enabled: global	Active	False	False	0	cloudsploit
2024-08-07	Low	Audit Configuration Logging: global	Active	False	False	0	cloudsploit
2024-08-07	Low	Log Sinks Enabled: global	Active	False	False	0	cloudsploit

Assistive Remediation For GCP 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 shows the Cloud Asset Summary page with a search bar containing "shaped-infusion-402417 | 19JUN". A red box highlights the search bar. Below the search bar, there are tabs for "Compliance" and "Detailed View", with "Detailed View" selected. A table lists various compliance findings, all of which are marked as "FAILED". One specific finding for "serviceAccountManagedKeys" is highlighted with a red box. The details for this finding include:

- Description:** Ensures that service account keys are being managed by Google.
- Category:** projects/shaped-infusion-402417/serviceAccounts/gar-test@shaped-infusion-iam.402417.iam.gserviceaccount.com/keys/eb5de1779baef0397be3e3d16d0d3c1ec0c09d
- Message:** The user service account key is not being managed by Google.
- Solution Reference Link:** <https://cloud.google.com/iam/docs/creating-managing-service-account-keys>
- Compliance Frameworks:** CIS, HITRUST, GDPR, CIS
- Compliance Sub Controls:** 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, 1.4 ENSURE THAT THERE ARE ONLY GCP-MANAGED SERVICE ACCOUNT KEYS FOR EACH SERVICE ACCOUNT

Total Records: 18

This dialog box is titled "serviceAccountManagedKeys" and "Low". It contains the following sections:

- Recommended Actions:** Ensure all user service account keys are being managed by Google.
- Details:** Asset: projects/shaped-infusion-402417/serviceAccounts/gar-test@shaped-infusion-402417.iam.gserviceaccount.com/keys/eb5de1779baef0397be3e3d16d0d3c1ec0c09d. A red box highlights the "+ Create Ticket" button.

Create Ticket

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

testcompliance X v

Close

Create Ticket



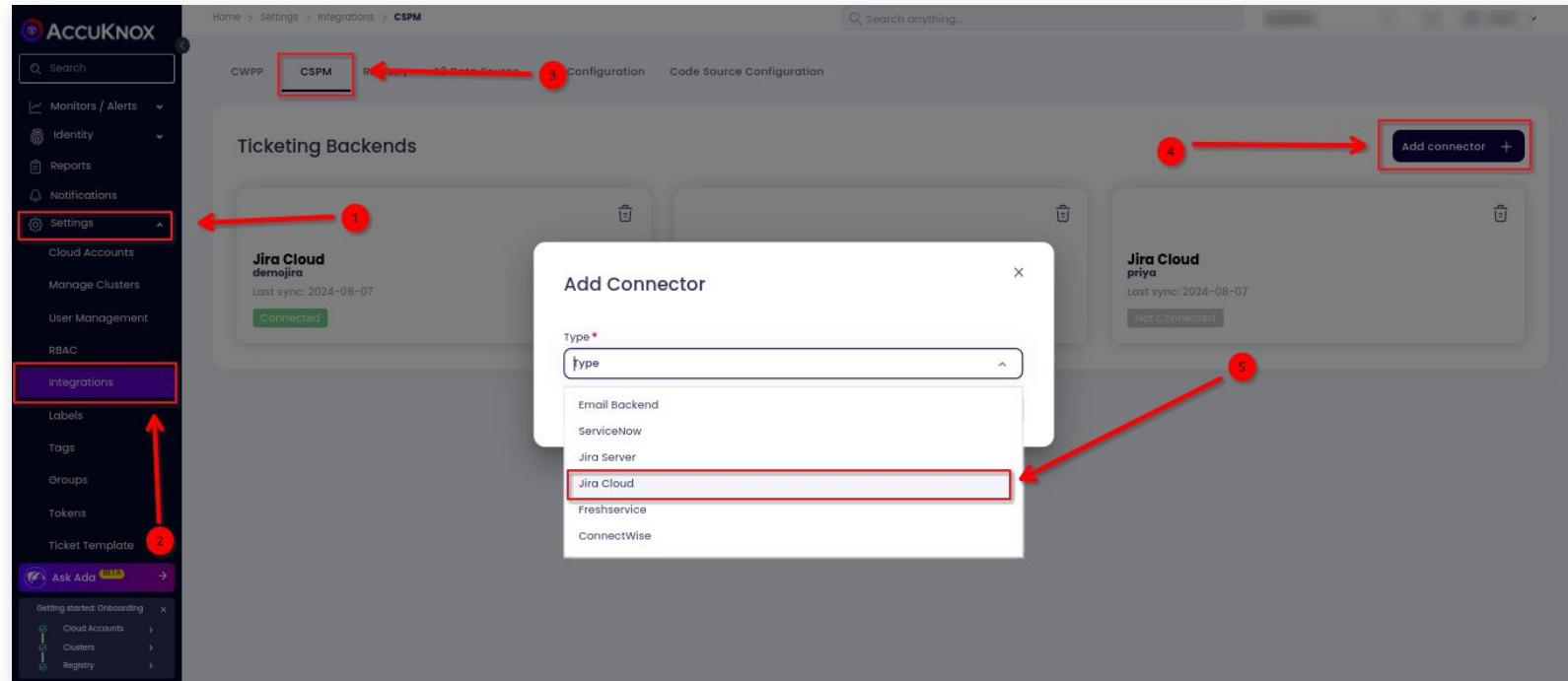
Integrations

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.



How to do CSPM ticketing Integration with Jira Cloud? [2]



- 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., [kRVxxxxxxxxxxxxxx39](#).
- For more detailed steps refer to the Accuknox help [documentation](#).

The screenshot shows a configuration form for integrating CSPM ticketing with Jira Cloud. The form is titled 'Jira Cloud' and includes the following fields:

- Name ***: A text input field.
- Service Desk URL ***: A text input field.
- Email ***: A text input field.
- Secret ***: A text input field.
- Is Jira admin**: A checkbox labeled "Is Jira admin".

At the bottom left is a 'Cancel' button, and at the bottom right is a 'Save' button.

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 shows the AccuKnox web interface with the following steps highlighted:

1. In the left sidebar under "Settings", click on "Integrations".
2. In the main content area, click on the "CSPM" tab.
3. Under "Ticketing Backends", click on the "Add connector" button (marked with a red circle).
4. In the "Add Connector" dialog, select "ServiceNow" from the "Type" dropdown (marked with a red circle).
5. Click the "Next" button in the dialog (marked with a red circle).
6. In the background, the "Ticketing Backends" list shows two entries: "Jira Cloud Test101" (Connected) and "Jira Cloud priya" (Not Connected).

How to do CSPM ticketing Integration with ServiceNow? [2]



- 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](#).

A screenshot of a web-based configuration form for a ServiceNow integration. The form is titled "ServiceNow". It contains four input fields: "Name" (with placeholder "Enter a name for integration"), "ServiceNow URL" (with placeholder "Enter the ServiceNow instance URL"), "Username" (with placeholder "Enter the ServiceNow instance Username"), and "Secret" (with placeholder "Enter the ServiceNow instance Password"). Below the form are two buttons: "Cancel" on the left and "Save" on the right. In the top right corner of the form area, there is a "Help" link with a question mark icon.

Name *	ServiceNow URL *
Enter a name for integration	Enter the ServiceNow instance URL
Username *	Secret *
Enter the ServiceNow instance Username	Enter the ServiceNow instance Password

Cancel Save

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



1

2

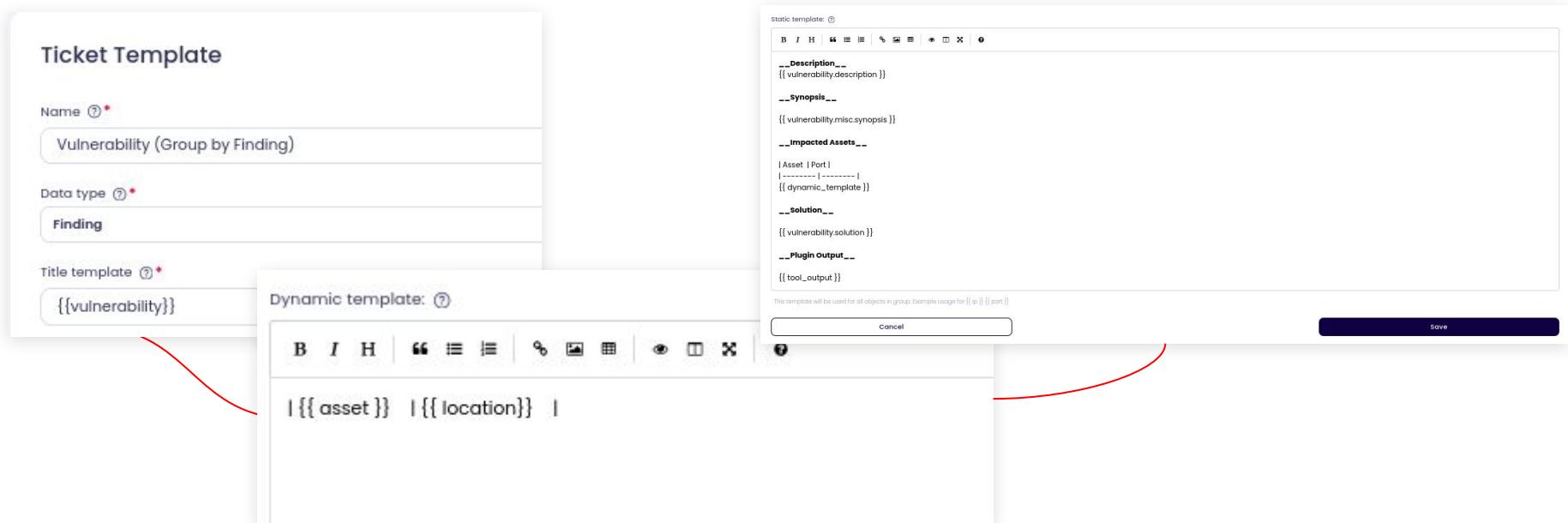
3

List of all templates that is created by user for different kind of tickets.

Name	Type
Datalist Software Template	Data-List
Cloud Scan Misconfiguration	Finding
iac Scan Vulnerability	Finding
Baseline Template	Control
Vulnerability (Group by Finding)	Finding
Compliance Template	Control
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.
 - Name:** Used for easier access to templates in configurations.
 - Data Type:** Associates the template with a selected data type (e.g., vulnerability) for availability on specific pages.
 - Title Template:** Generates ticket titles in the ticketing system by populating variables.
 - Dynamic Template:** Formats and combines data for multiple objects within a group.
 - Static Template:** Applies consistent data (e.g., solution or description) across a group with similar findings.



The screenshot shows the 'Ticket Template' configuration screen. It includes fields for 'Name' (mandatory), 'Data type' (set to 'Finding'), and 'Title template' ({{vulnerability}}). A red arrow points from the 'Title template' field to the 'Dynamic template' dialog window.

The 'Dynamic template' dialog contains a rich text editor toolbar and a code editor area. The code editor contains the following template structure:

```
Static template: ⓘ  
B I H | “ “ ≡ ≡ % % █ █ • • □ □ X X  
_Description_  
{{vulnerability.description}}  
_Synopsis_  
{{vulnerability/misc.synopsis}}  
_Impacted Assets_  
| Asset | Port |  
| ----- | ----- |  
{{dynamic_template}}  
_Solution_  
{{vulnerability.solution}}  
_Plugin output_  
{{tool_output}}
```

A note at the bottom of the dialog says: "This template will be used for all objects in group. Example usage for {{ ip }} {{ port }}". Red arrows point from the 'Save' button and the 'Cancel' button back to their respective counterparts on the main configuration screen.



Reporting

Report Generation



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 platform interface for generating a CSPM report. The left sidebar has a purple 'Reports' button highlighted. The main page shows the 'Reports' section with 'CSPM' selected. A red box highlights the 'Generate CSPM Instantaneous Report' button. A red arrow points from the 'Description*' field to the 'Select Cloud Accounts' dropdown. The 'Select Cloud Account' dropdown is open, showing several cloud accounts: AZURE22JULY, AWS 735362266271, AWS 975050082972 | AWS5G, and Google Cloud shapred-infusion-402417 | 19JUNESS. The 'Generate Report' button is at the bottom right.

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

Report Generation

- 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)

Cloud Account Misconfiguration Report

Compliance report focused on selected Compliance Program with all misconfiguration details will be generated

Select All

APRA 234 STANDARD

CIS AWS CIS Benchmark v1.4.0

CIS AWS CIS Benchmark v1.5.0

CIS AWS CIS Benchmark v2.0.0

Include detailed asset summary

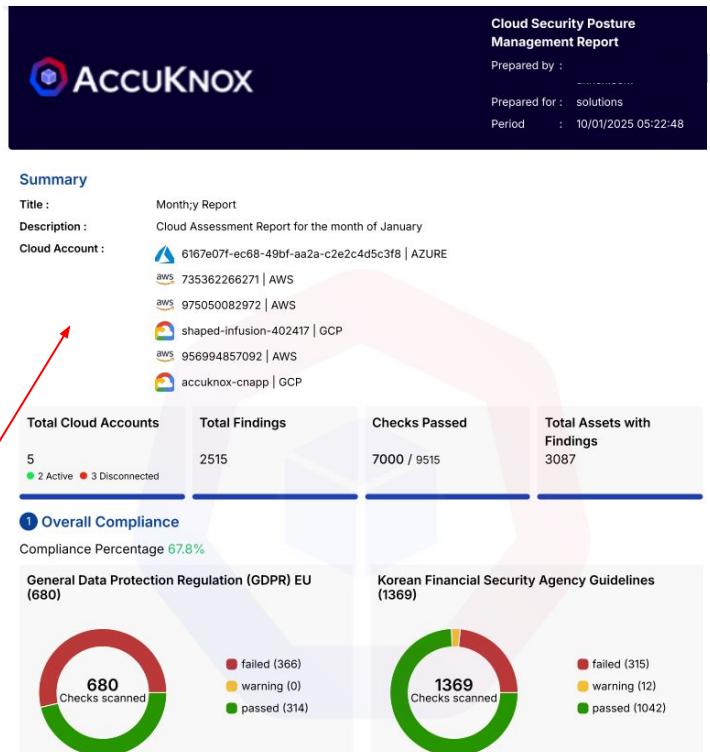
The top 50 misconfigurations will be included. For more details, please check the Cloud Asset Summary Page.

[Cancel](#)

Include detailed ticket summary

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

[Generate Report](#)





CNAPP

(Cloud Native Application Protection Platform)

CNAPP Dashboard with onboarded Cloud, Clusters & Containers

