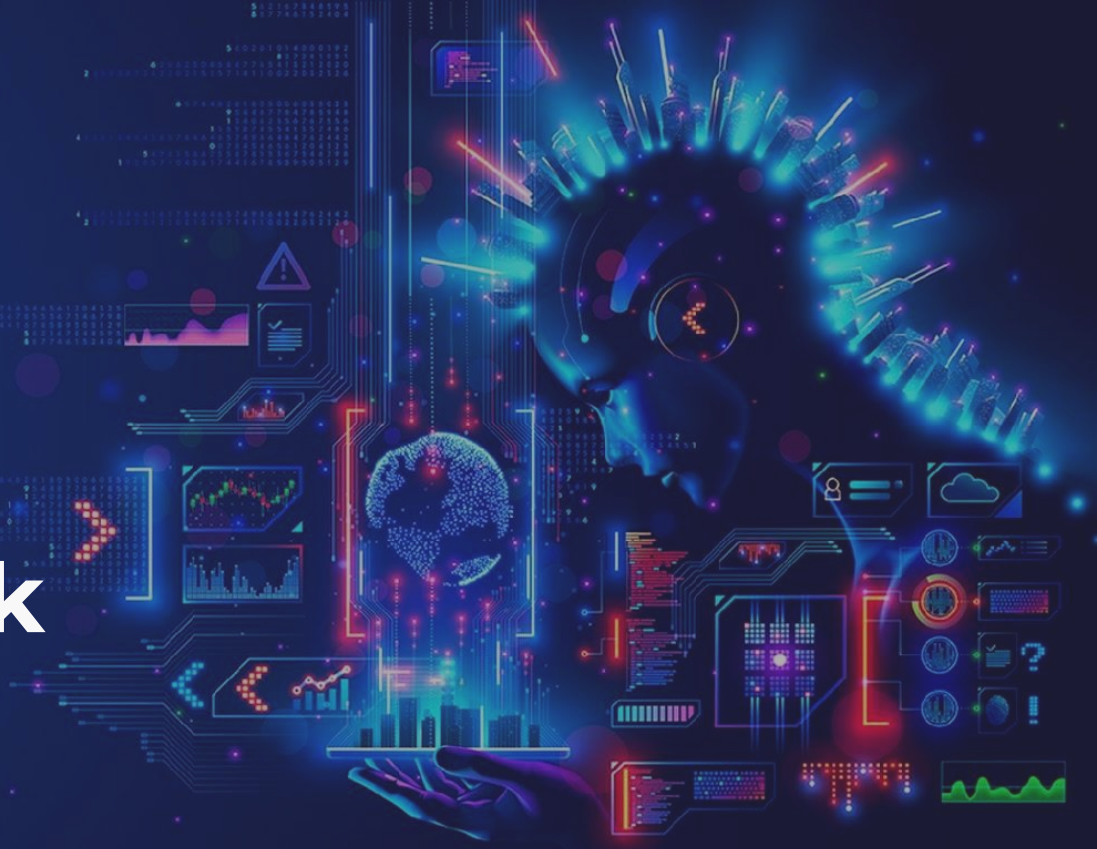
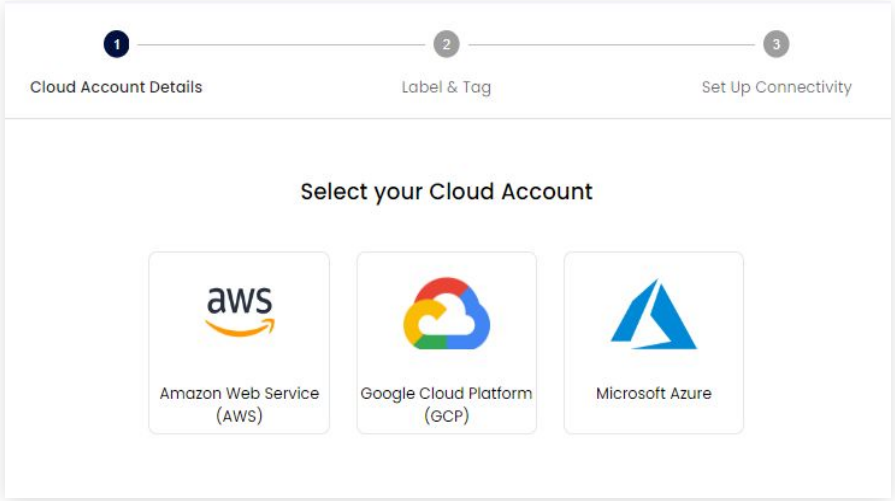
AccuKnox

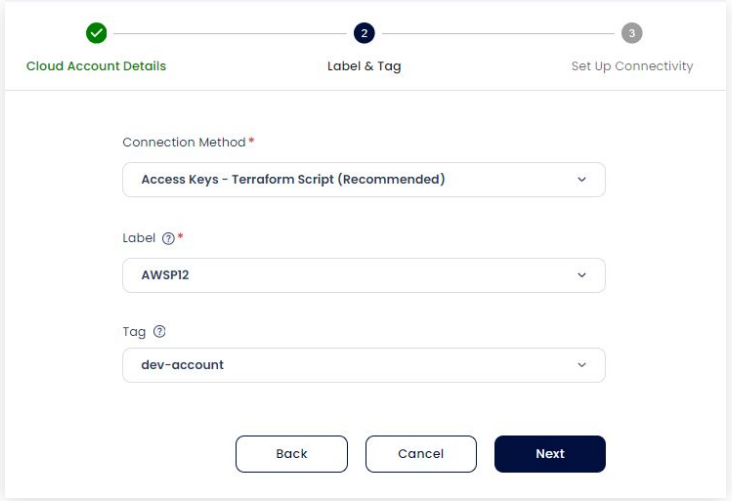
CSPM Playbook



Cloud account Onboarding

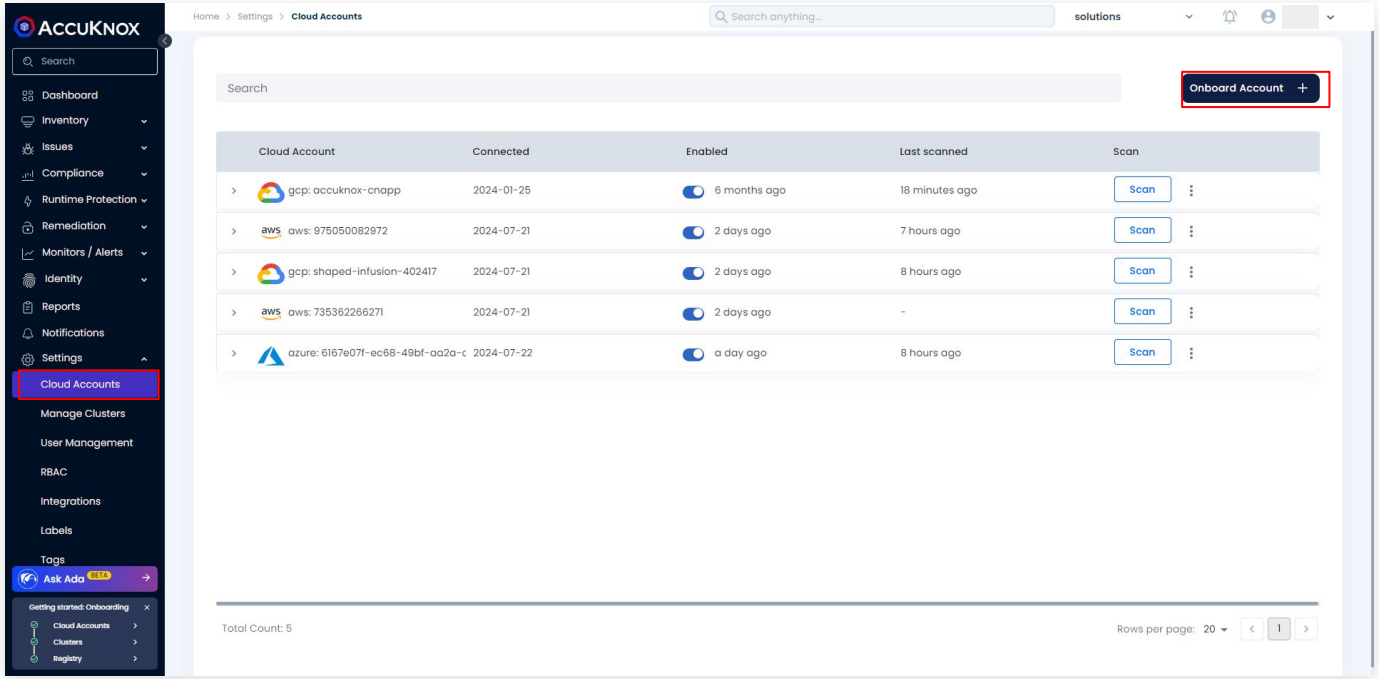
- Choose the Cloud provider (AWS | GCP | Azure)
  - Select AWS
    - Choose connection method -> Access keys
    - Select Label and Tag (It will be used to identify the assets)





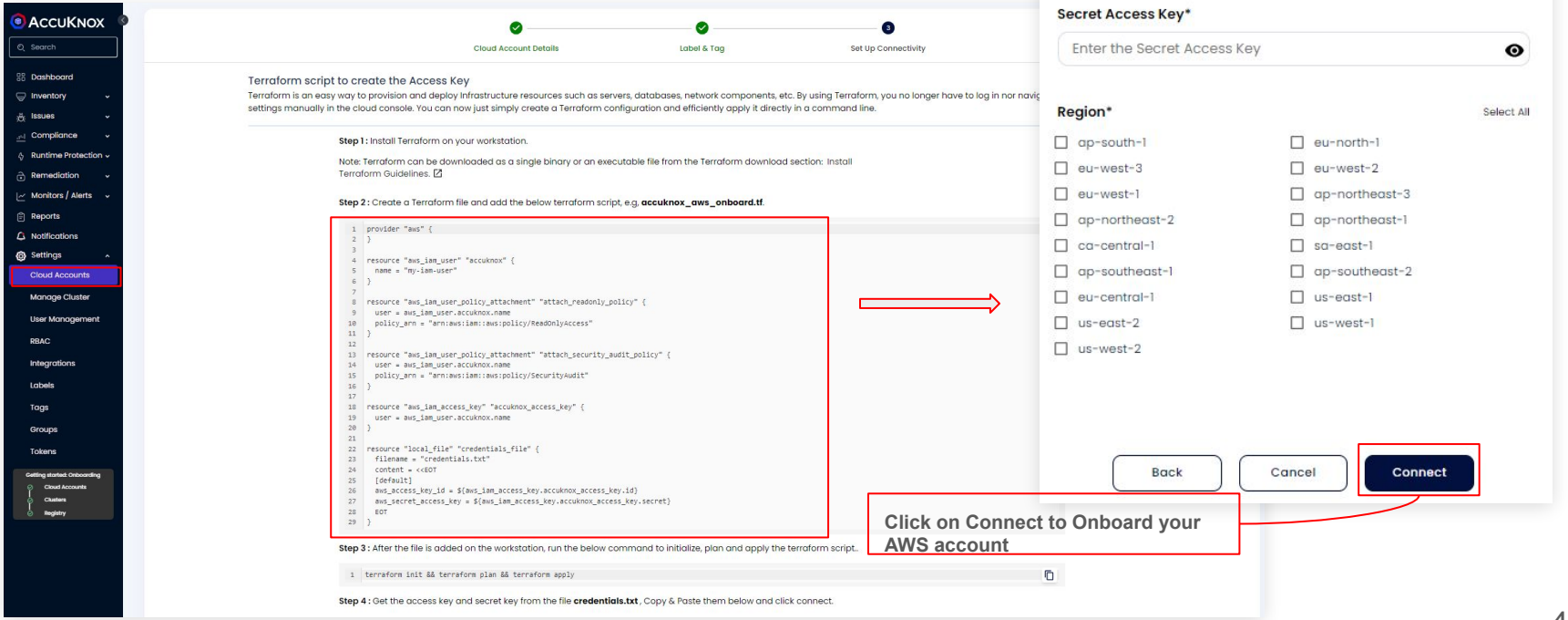
How to onboard Cloud Account?

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



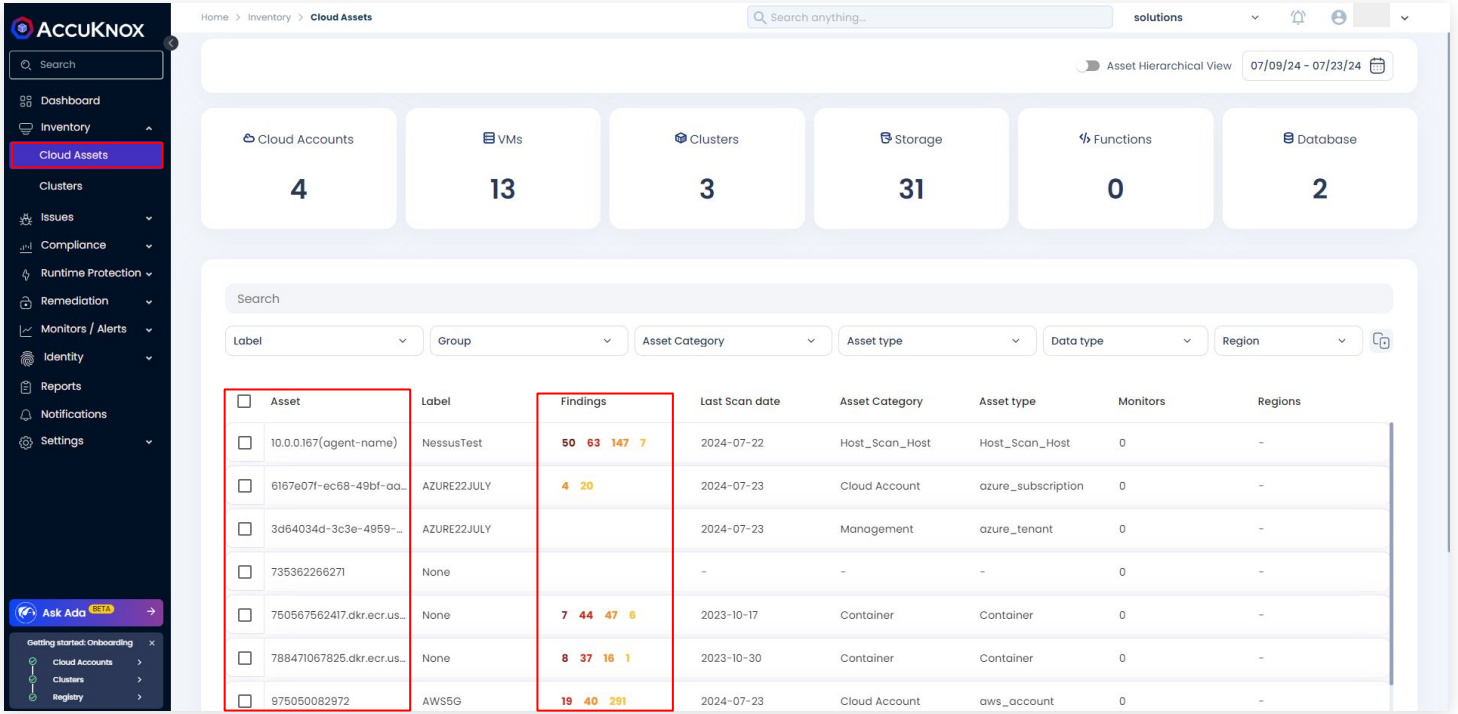
Cloud account onboarding

- 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



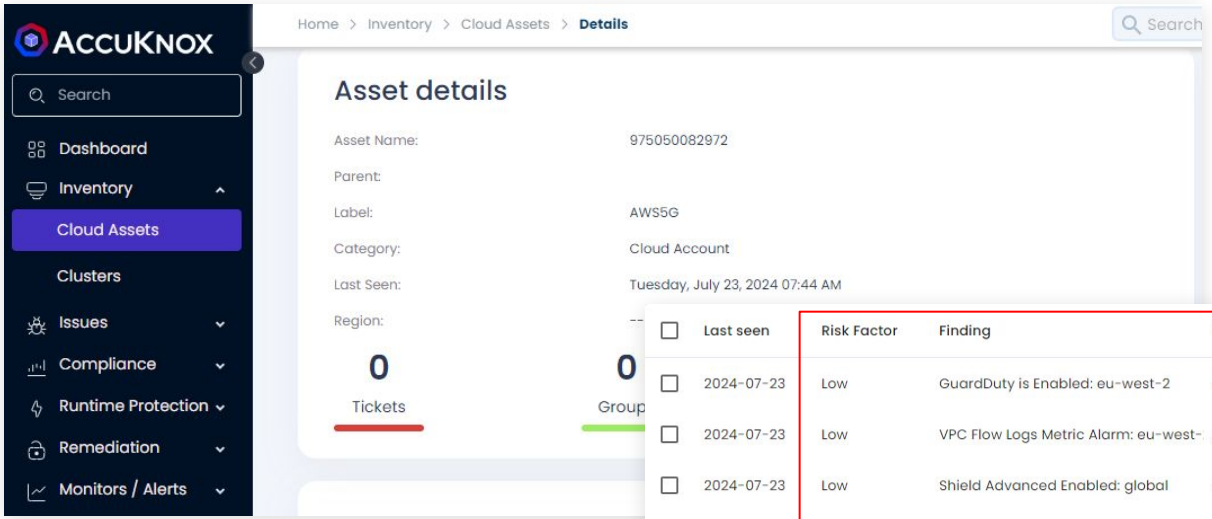
Risk Assessment - Cloud Assets View

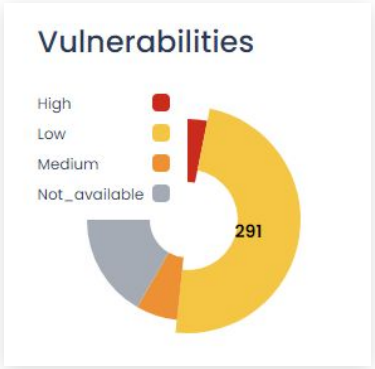
- After Onboarding the cloud account wait for the scan to complete
  - Scan is triggered instantly on account onboarding, but the scan completion might take at-least an hour or more.You will get an email after the successful scan executes.
- Once Scan completed, you should be able to see the cloud assets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



Risk Assessment - Asset Detail View

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

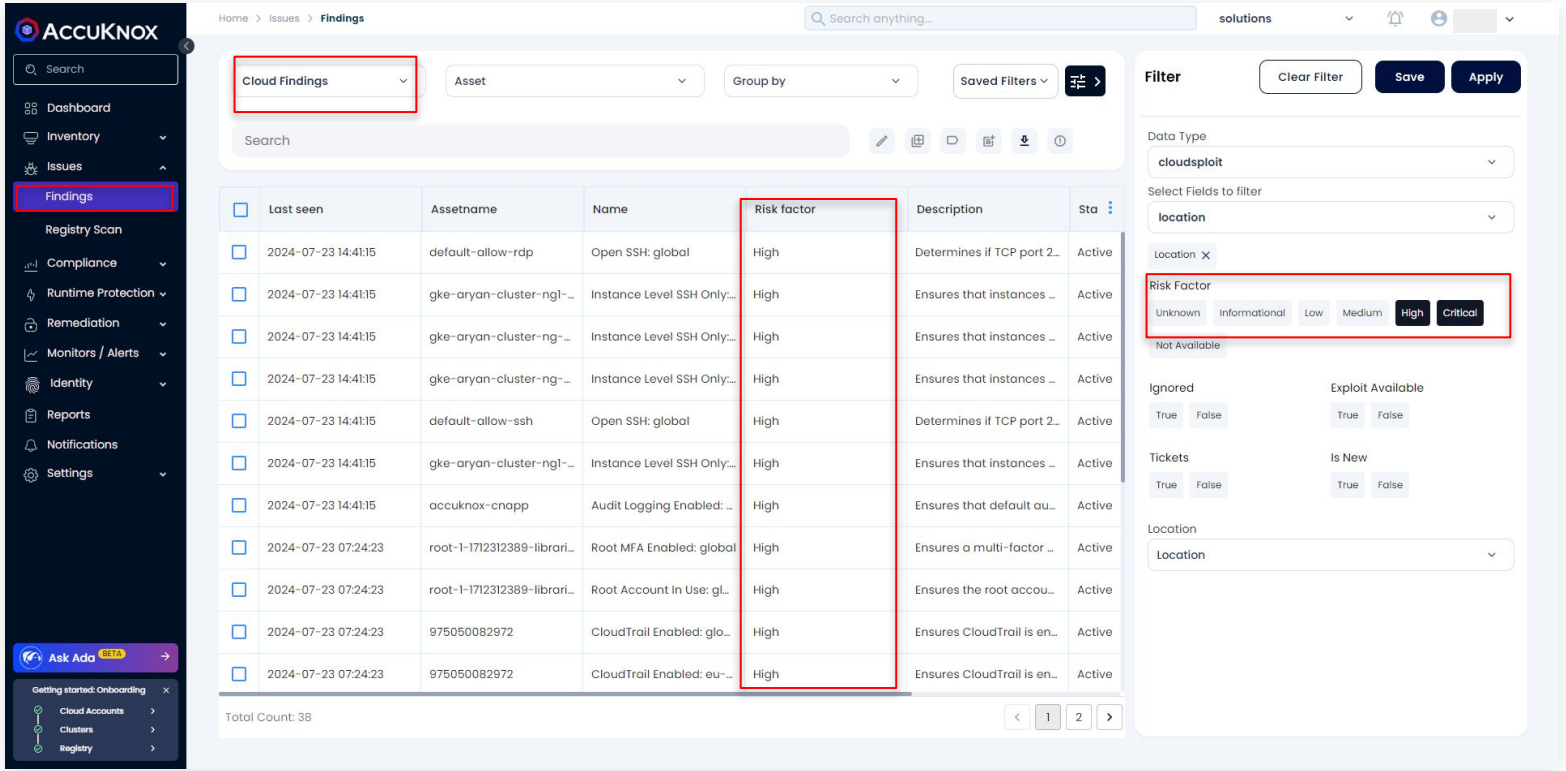




	Last seen	Risk Factor	Finding	Status	Ignored	Exploit Avail...	Tickets	Data Type
	2024-07-23	Low	GuardDuty is Enabled: eu-west-2	Active	False	False	0	cloudsploit
	2024-07-23	Low	VPC Flow Logs Metric Alarm: eu-west-	Active	False	False	0	cloudsploit
	2024-07-23	Low	Shield Advanced Enabled: global	Active	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

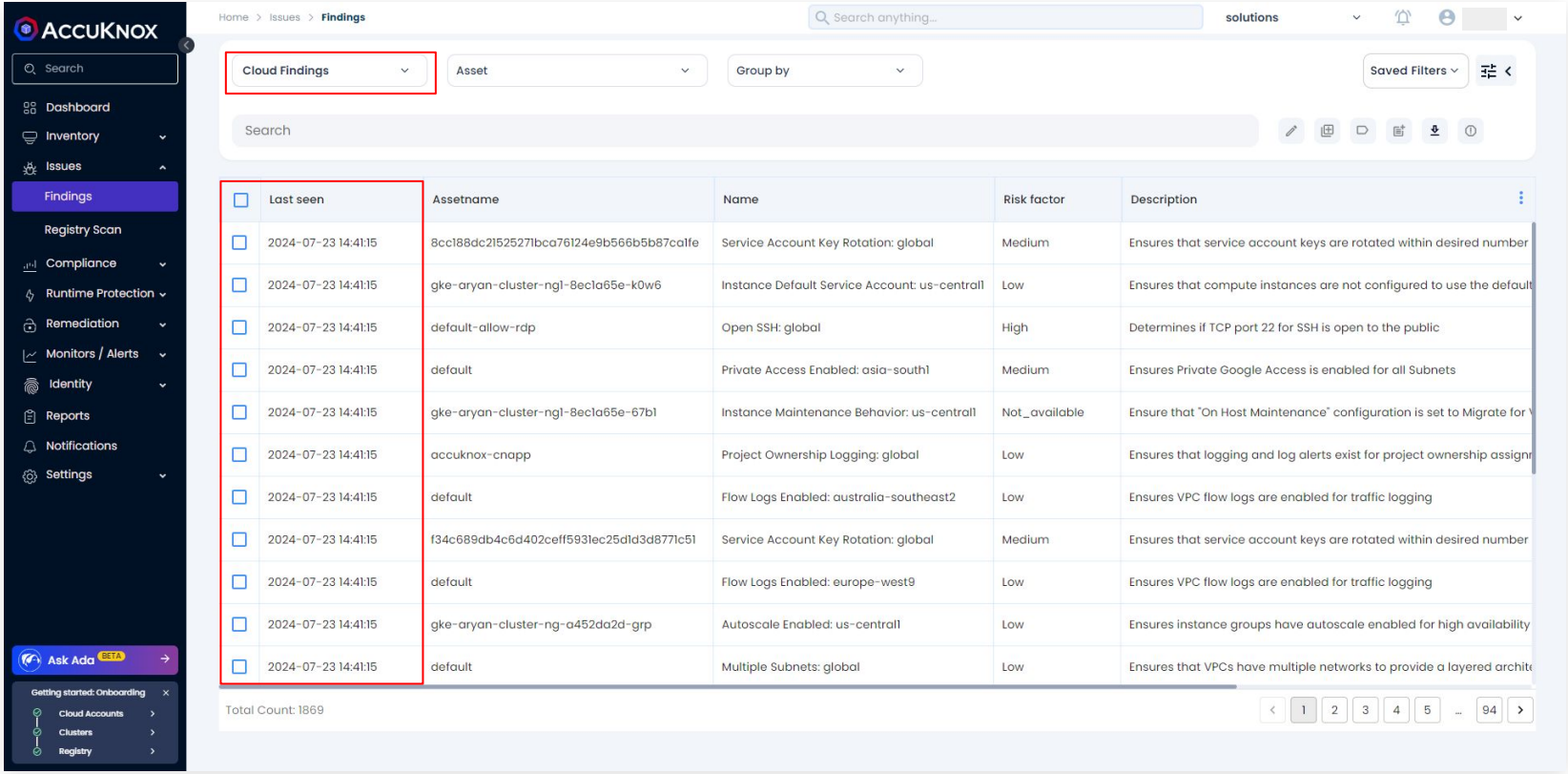
Risk Assessment - Most Critical Findings

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



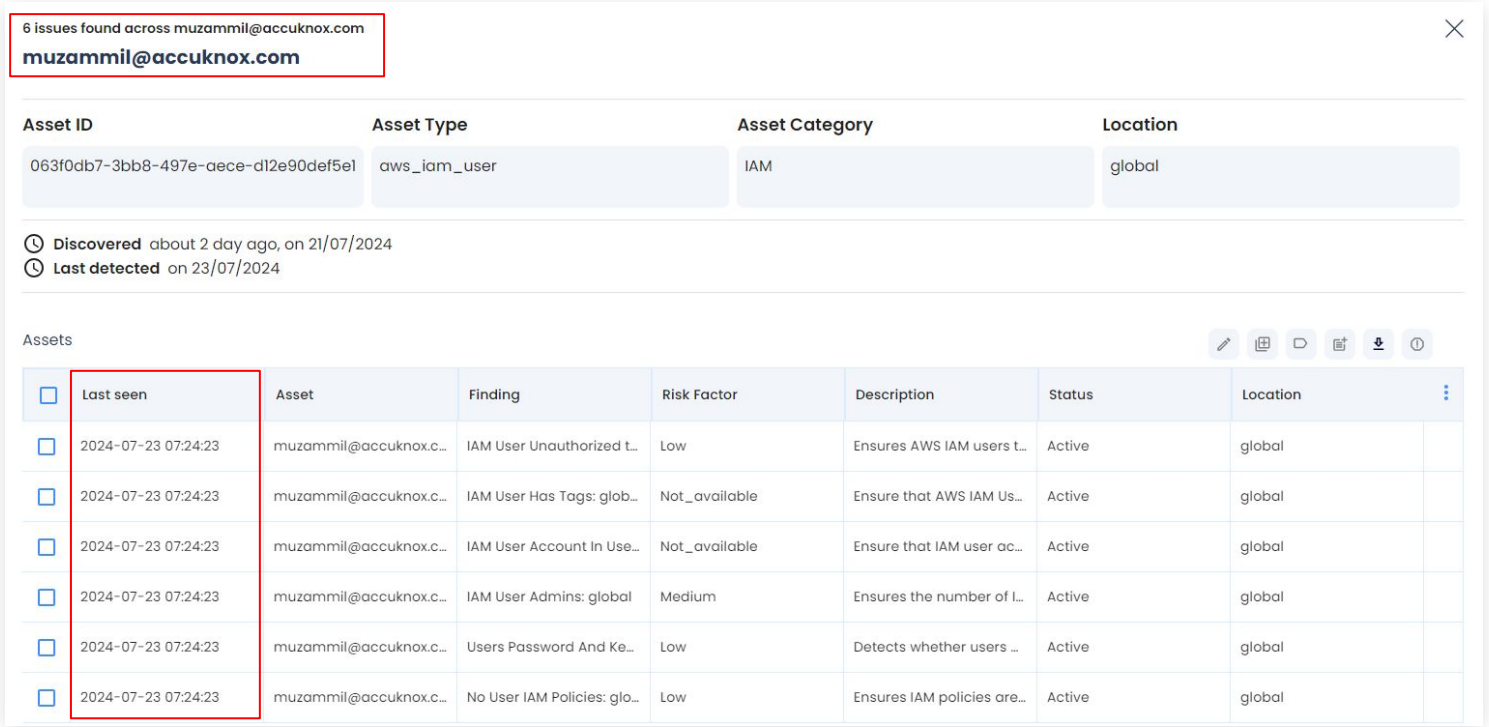
Risk Assessment - New Findings

- Find the recent most findings



Risk Assessment - Most Impacted Assets across cloud

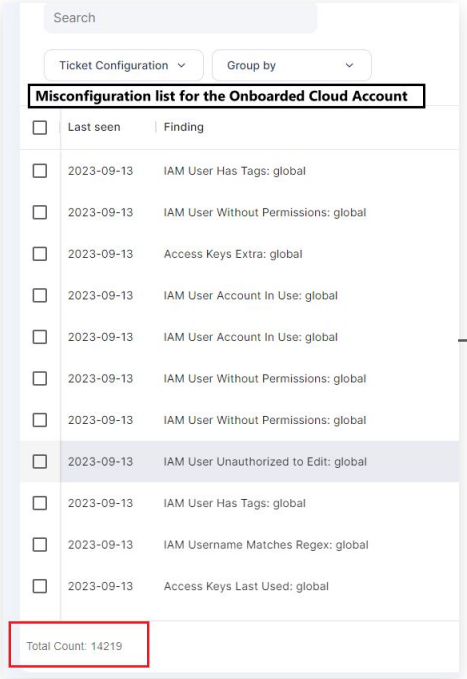
- Find the recent most findings
  - group by assets
  - Click on any of the findings

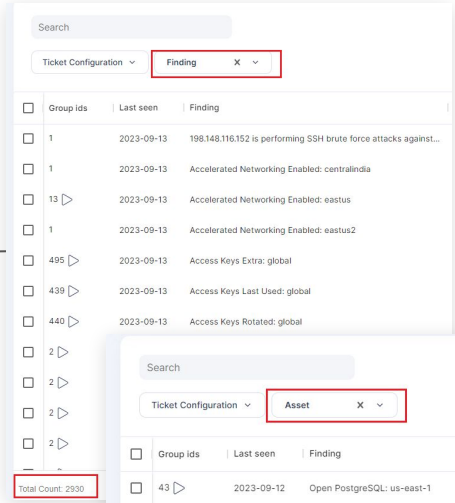


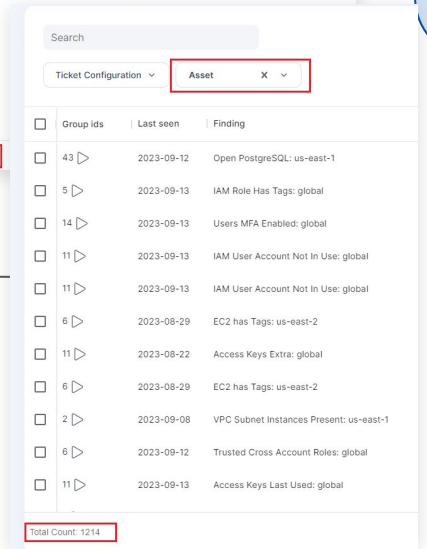
How to Remediate Cloud Misconfigurations?

ACCUKNOX

- 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







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

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

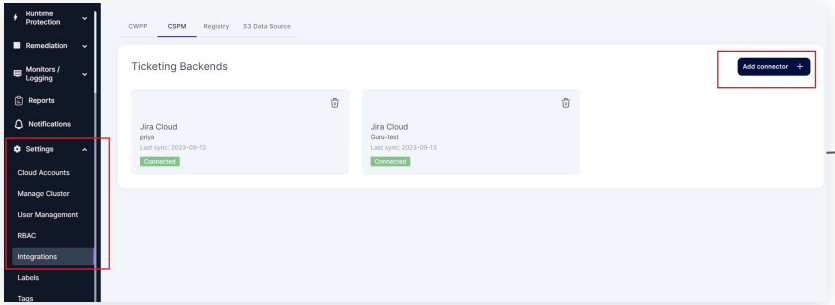
Group by **Assets** for a particular Data-Source (For example - Misconfiguration - Cloudsploit) will showcase ***all the issues associated to a particular Asset*** such as S3bucket, Host, Container etc.

[So that user can focus on Assets of choice]

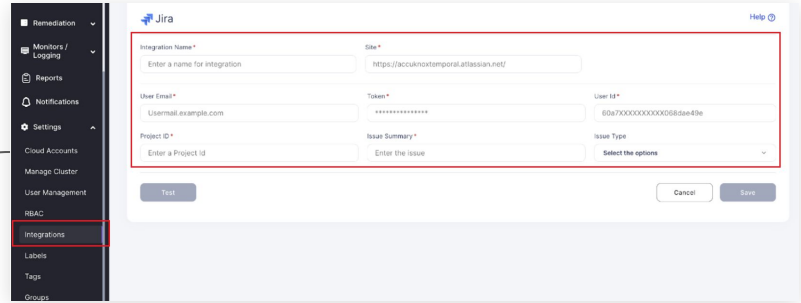
How to set up ticketing tool?

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

1

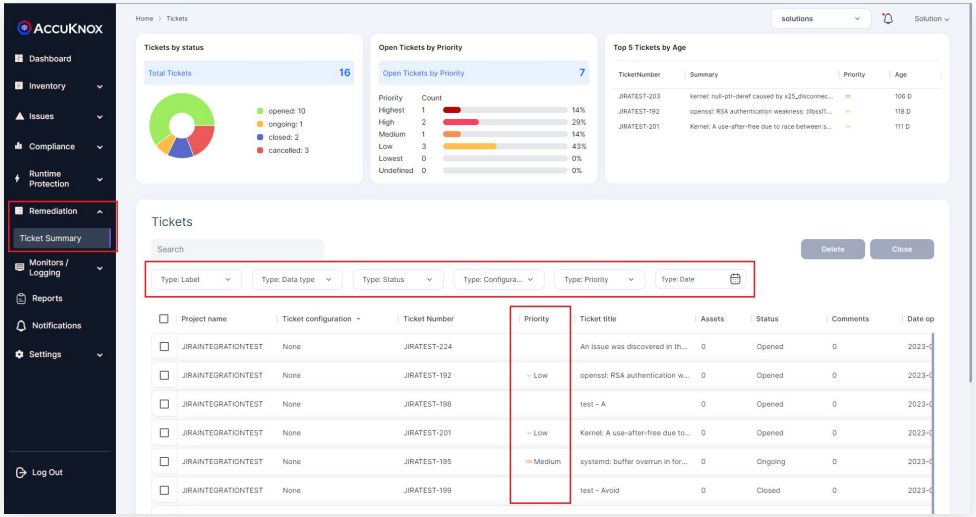


2



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

3

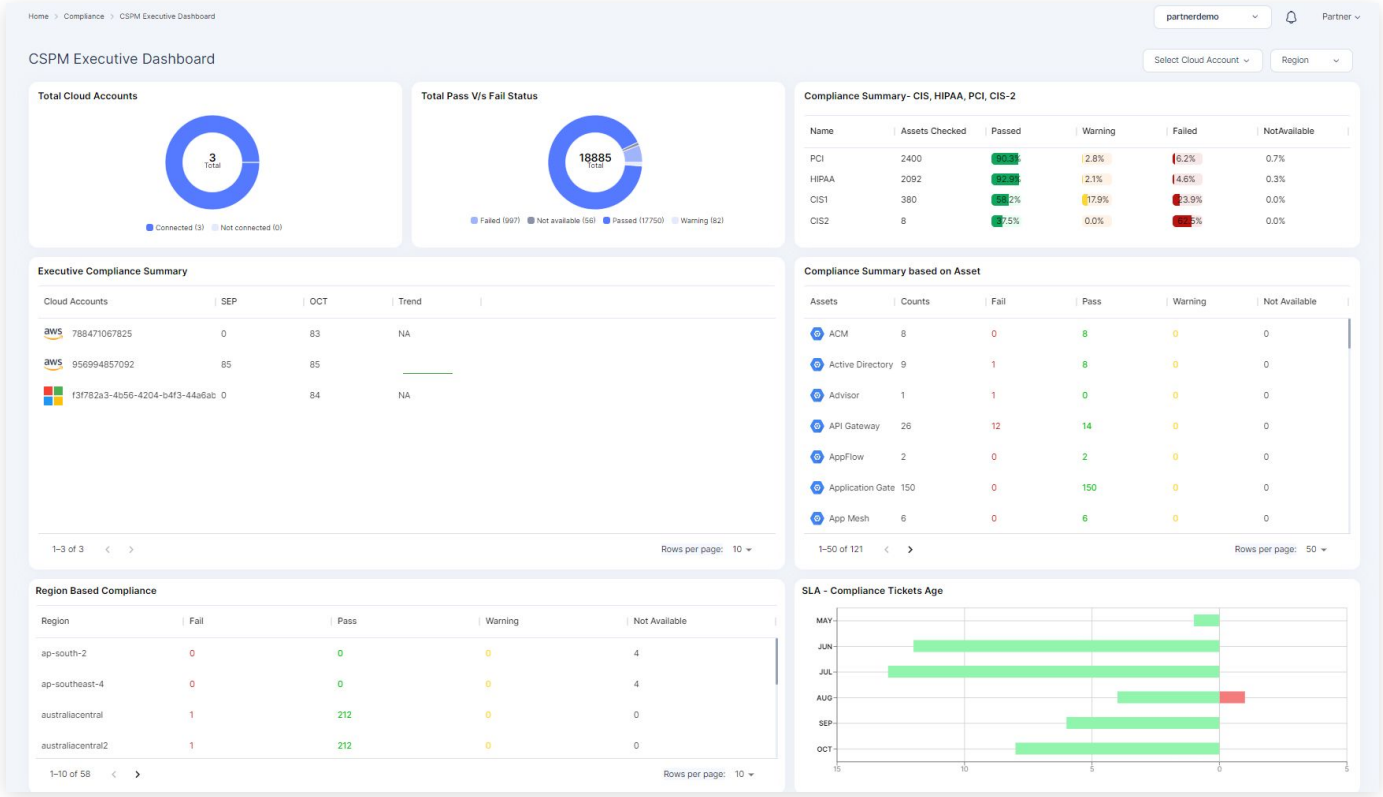


[You need to raise issues from Asset Detail page or Issues >> Vulnerability section to see Ticket Summary]

CSPM Compliance Dashboard

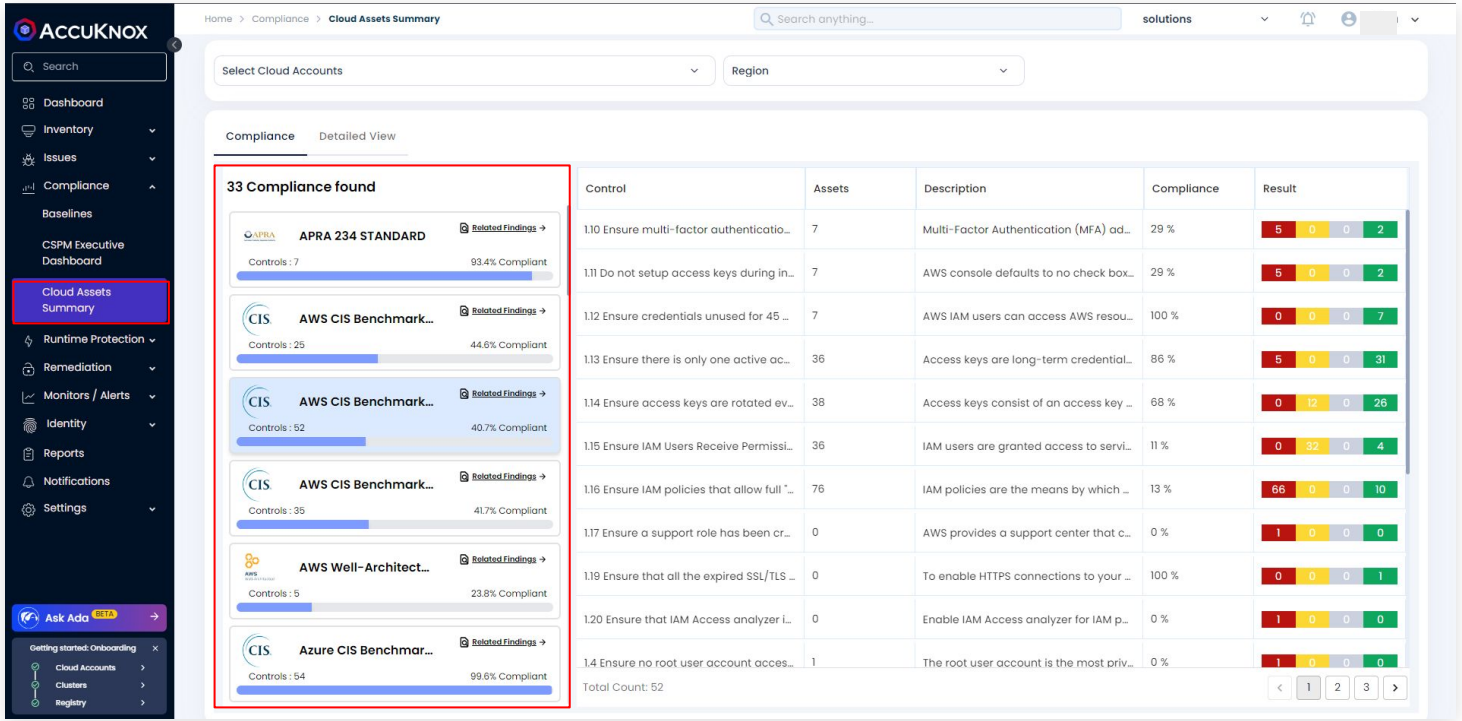
ACCUKNOX

Overview of CSPM Compliance Across Multi Cloud



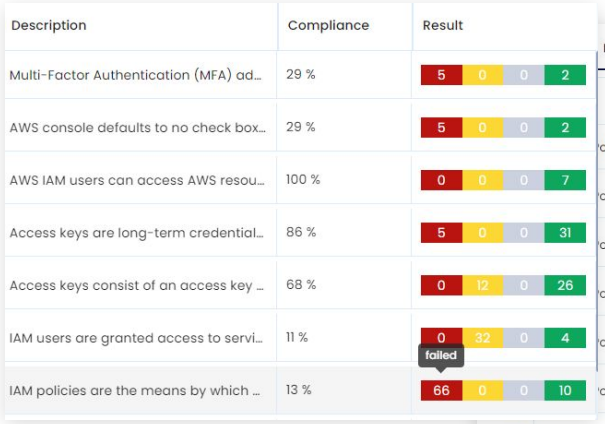
Compliance Summary

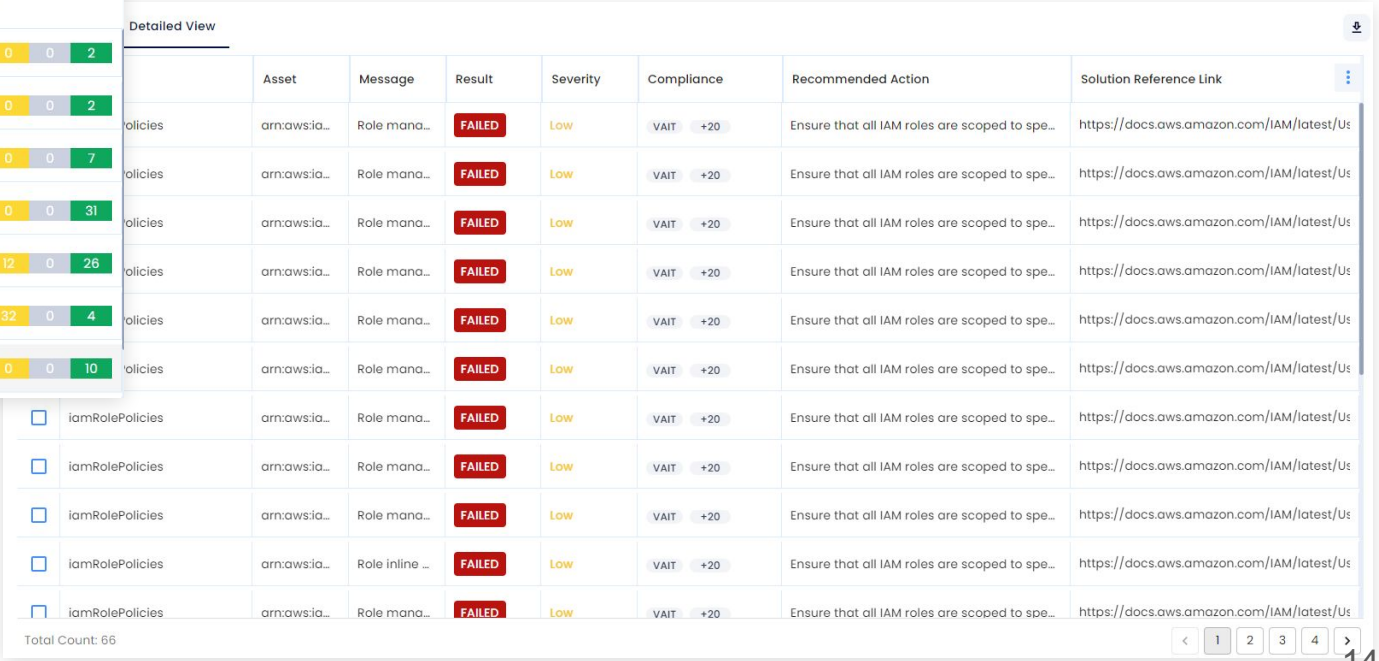
- To see the compliance summary for the cloud account
  - Click on Cloud Asset Summary
  - Choose the Compliance you want to see from the list



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



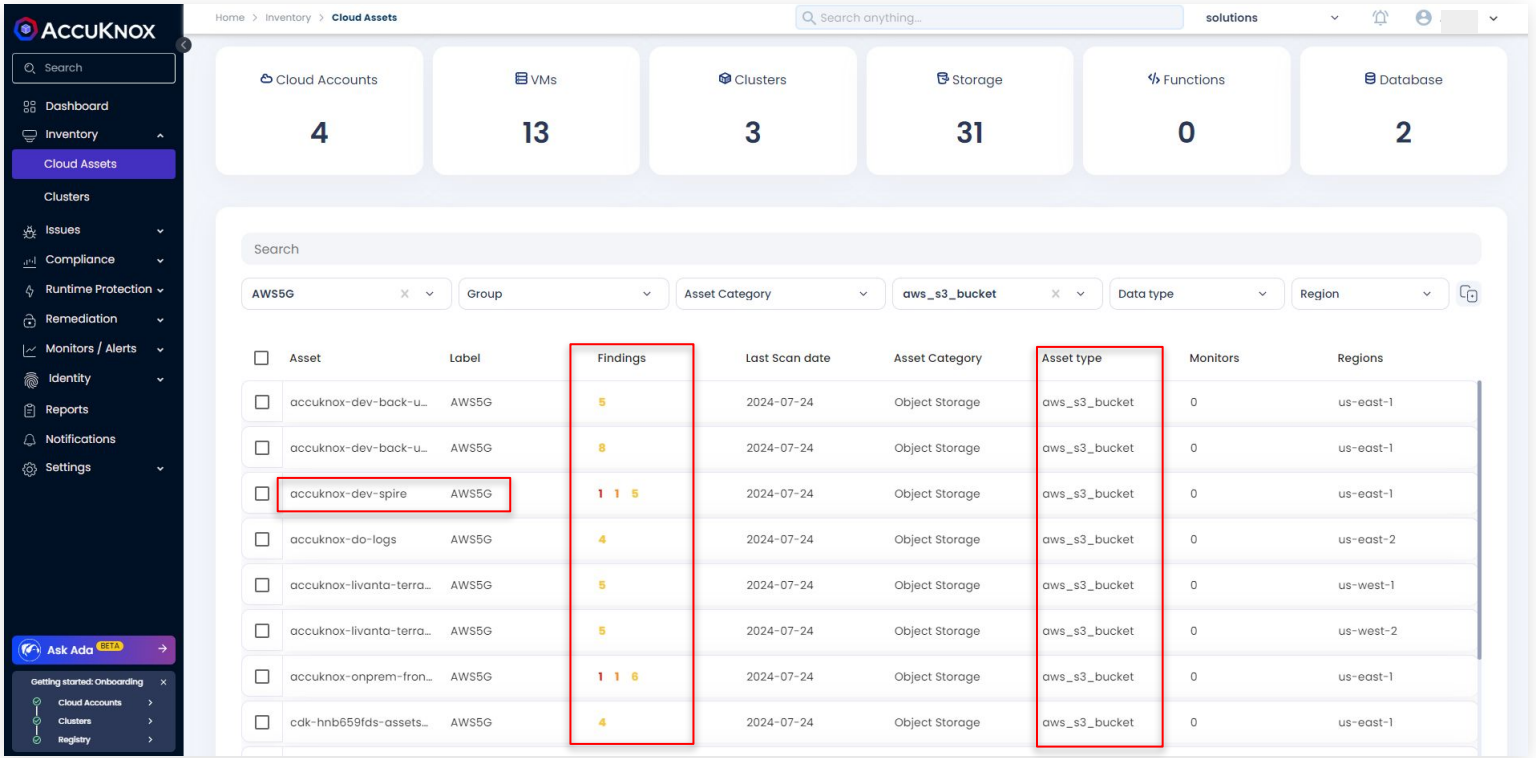


AWS Risk Assessment

Compliance failure and Misconfiguration

How to identify critical S3-buckets?

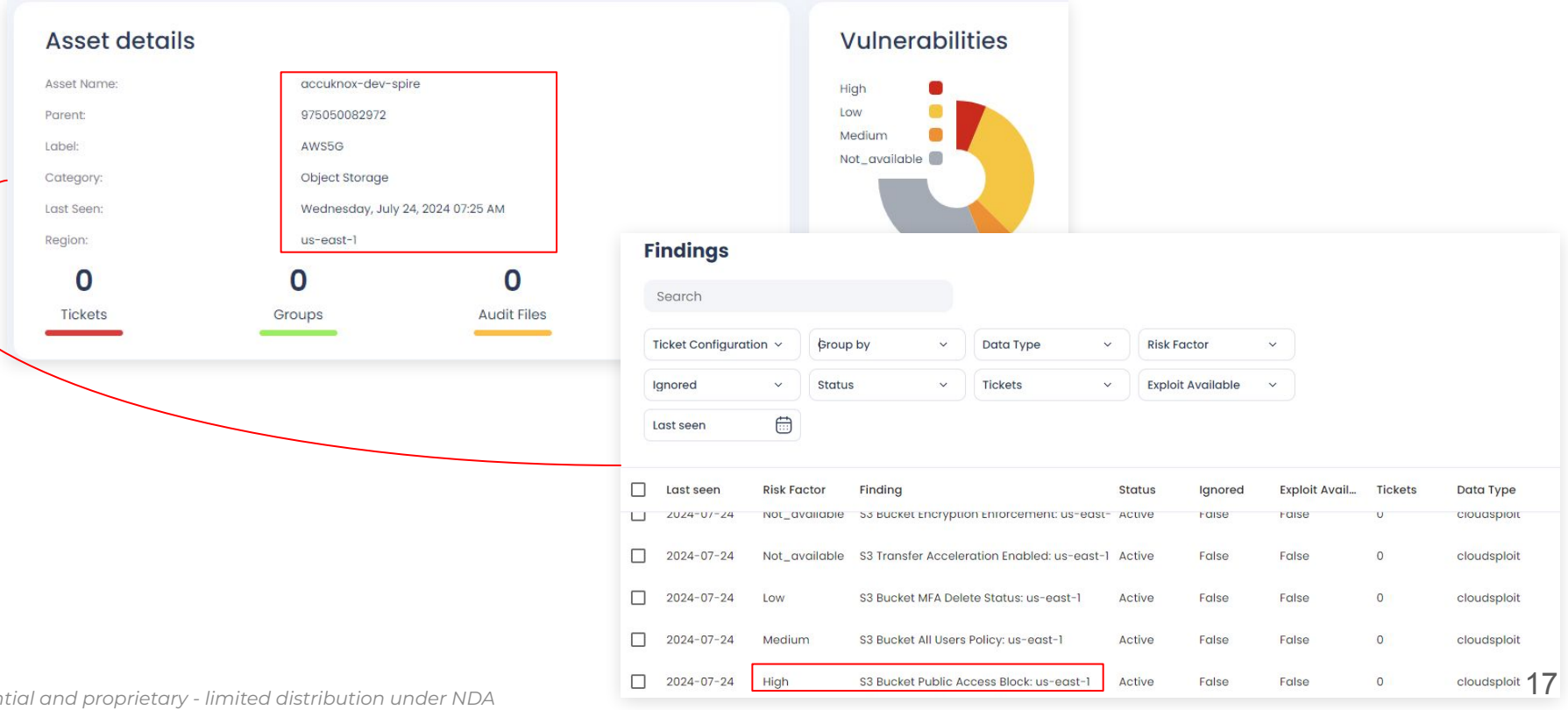
- Go to Inventory >> Assets page and Filter for Asset Type as *s3bucket*
- Look for *S3bucket* with count in *Total Vulnerabilities*



Identify S3 buckets accessible on public networks

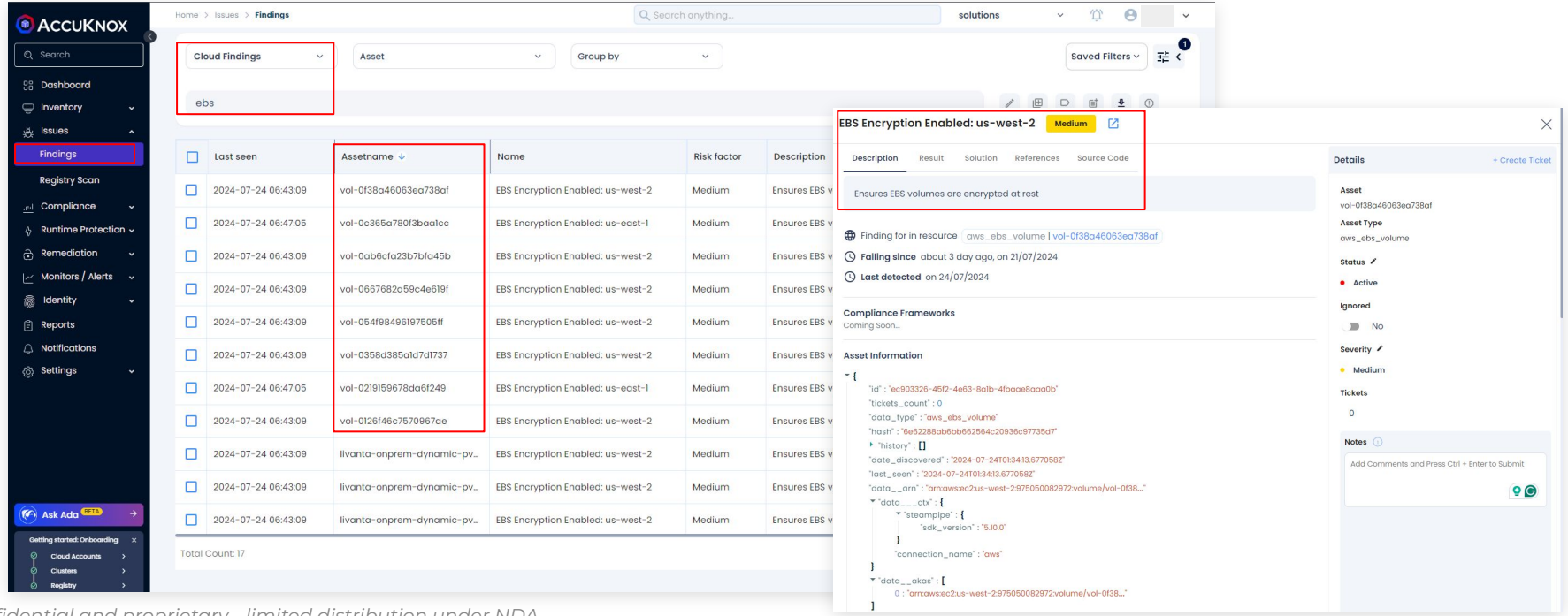
ACCUKNOX

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



How to identify unencrypted EBS Volume?

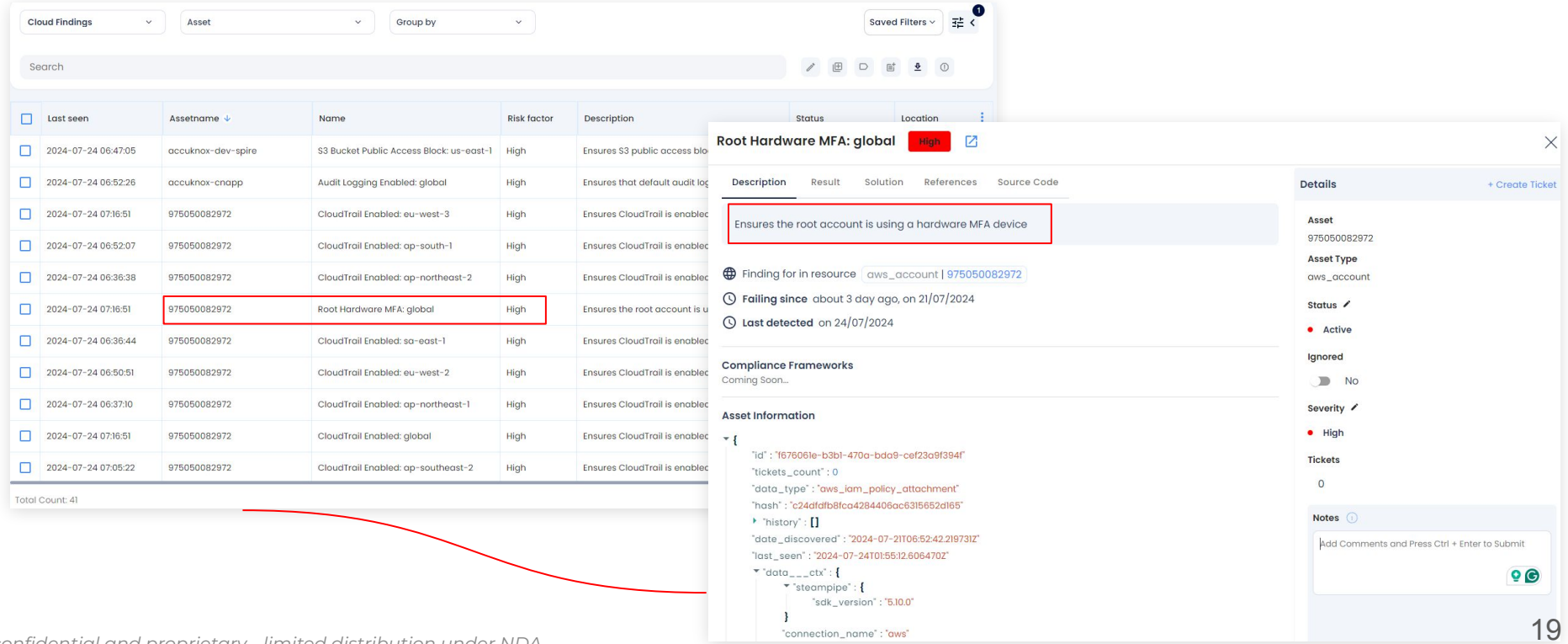
- To identity the unencrypted EBS Volume associated with the Onboarded Cloud Account, Please navigate to Issues -> Findings
  - Apply Cloud Findings in the filter
  - Search for “ebs volume” in the search field



How to identify if root user has enabled MFA?

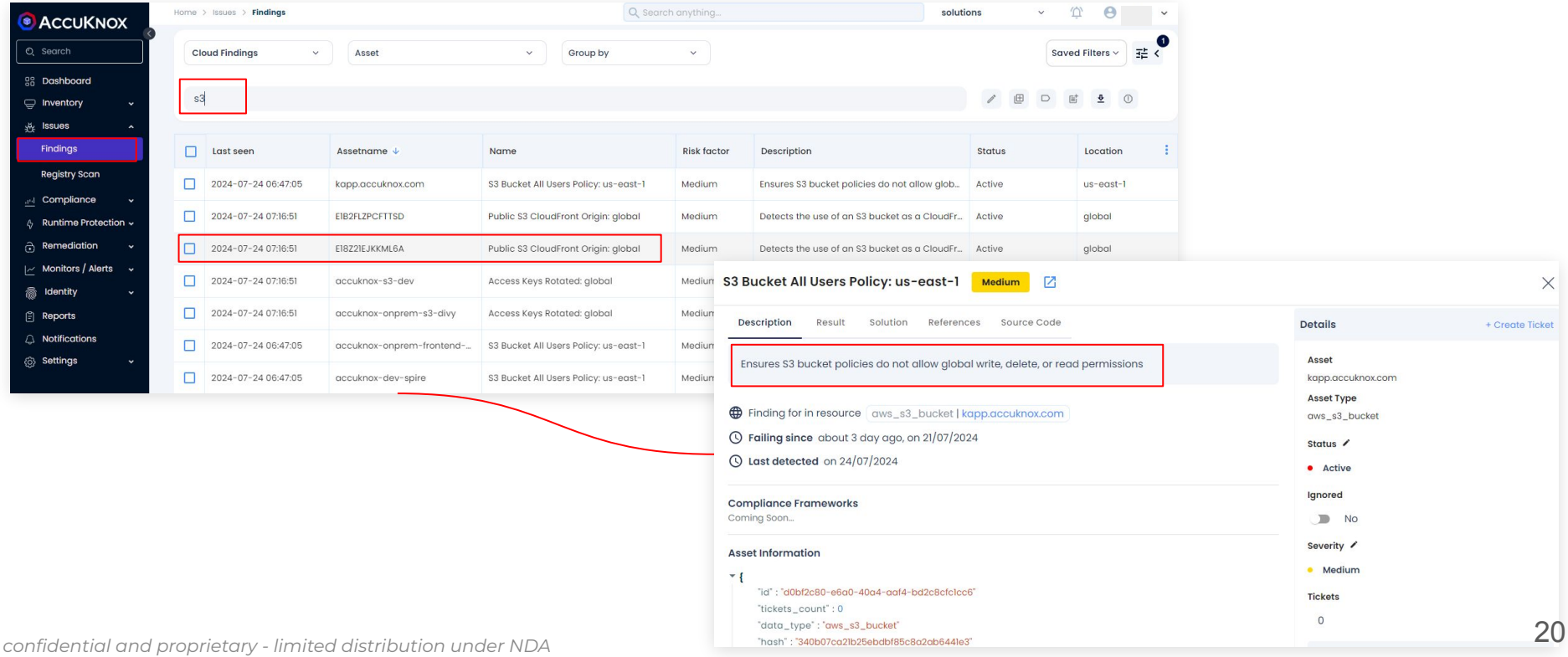
ACCUKNOX

- To identity 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



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

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

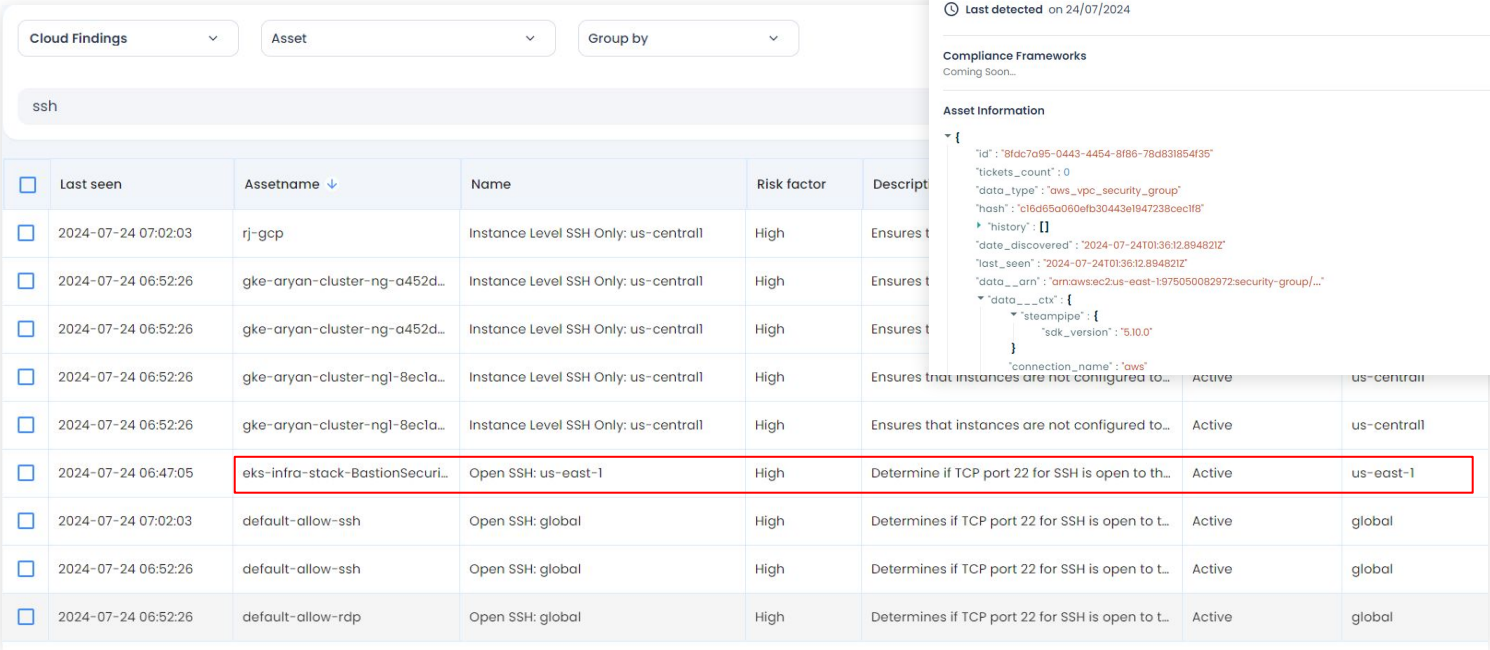


How to find Open SSH?

ACCUKNOX

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

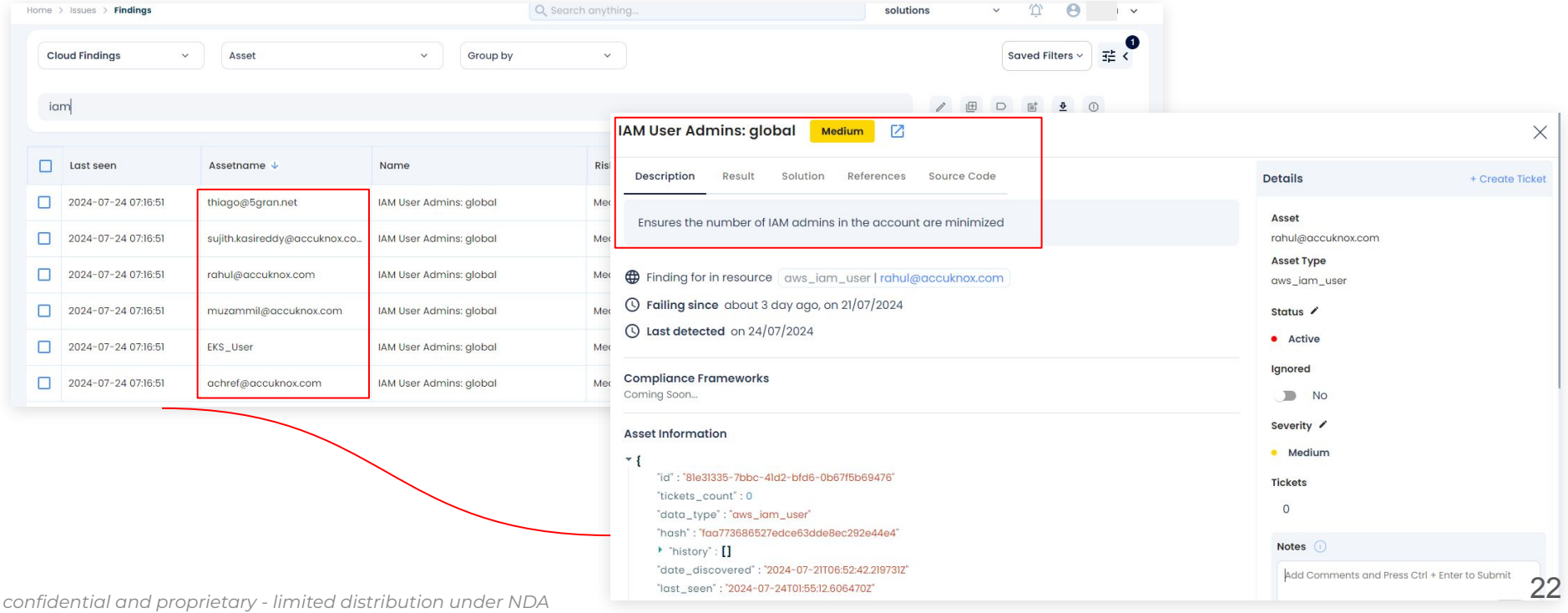


How to Identify IAM related security misconfiguration?

ACCUKNOX

To identify` the critical IAM misconfiguration

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

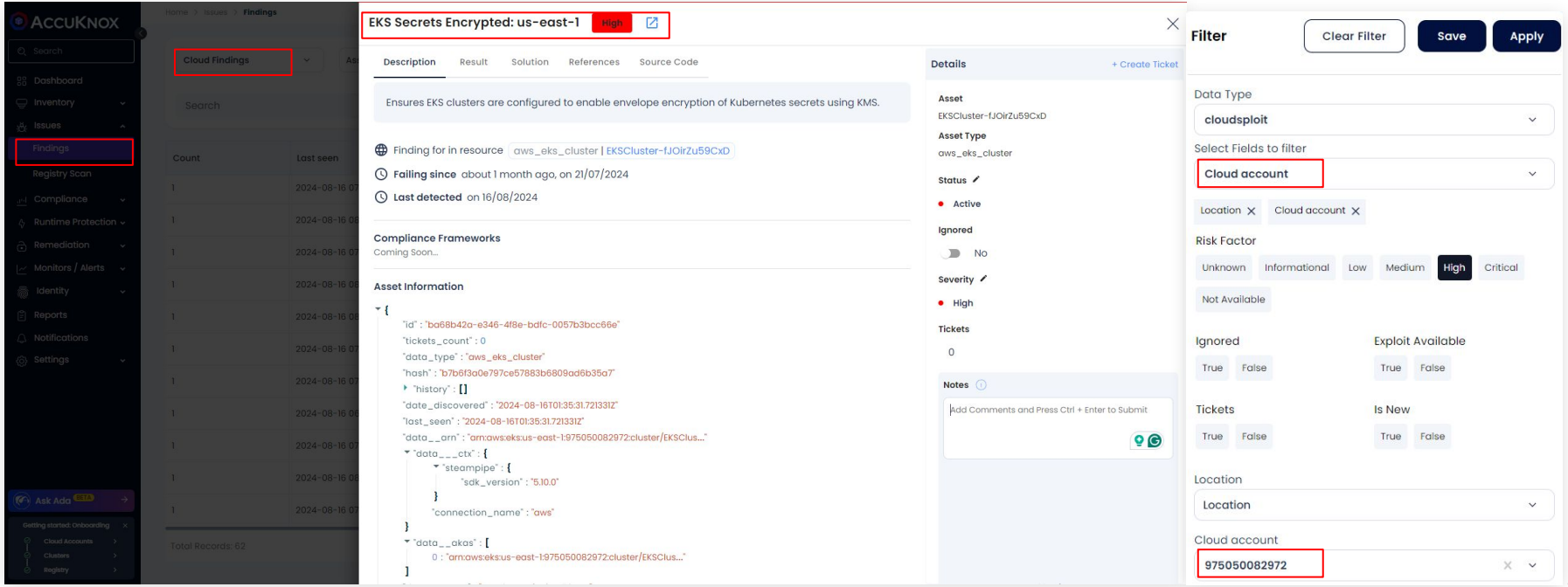


How to Identify if encryption is enabled for EKS secrets?

ACCUKNOX

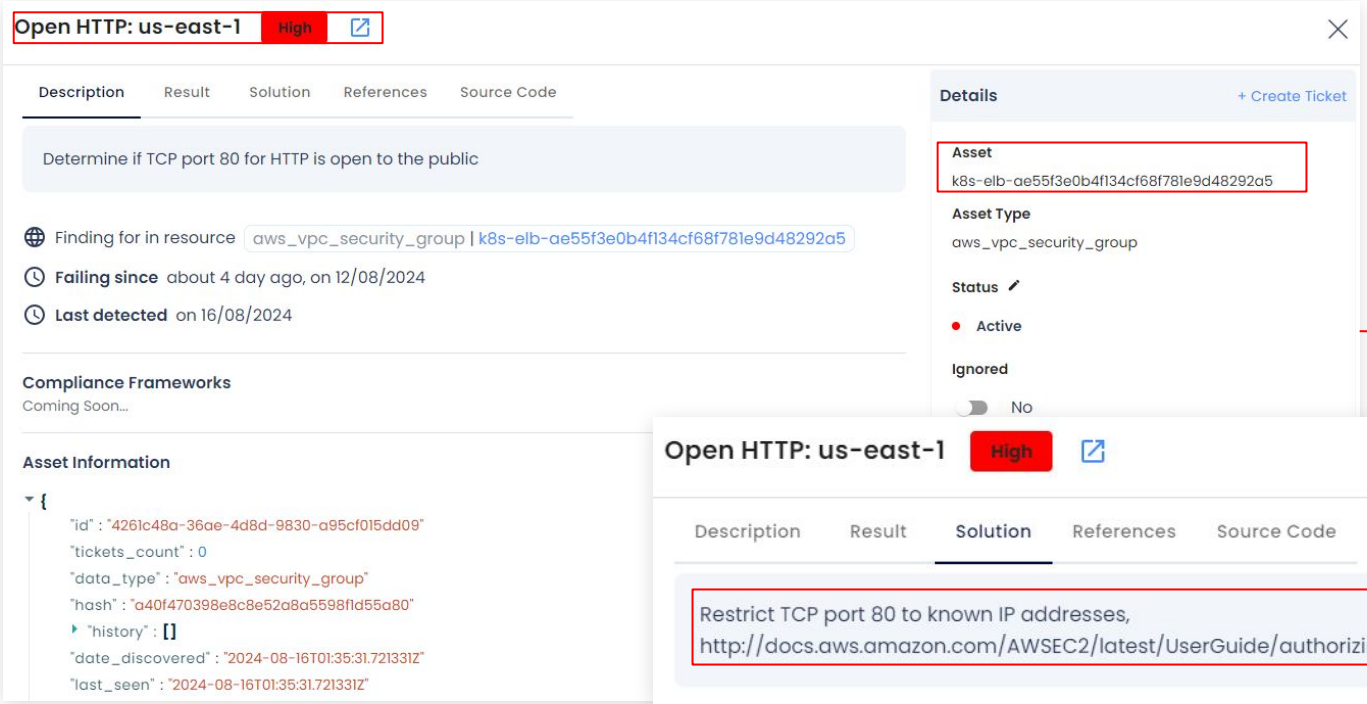
User can identify if encryption is enabled for the EKS secrets by following steps,

- 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.



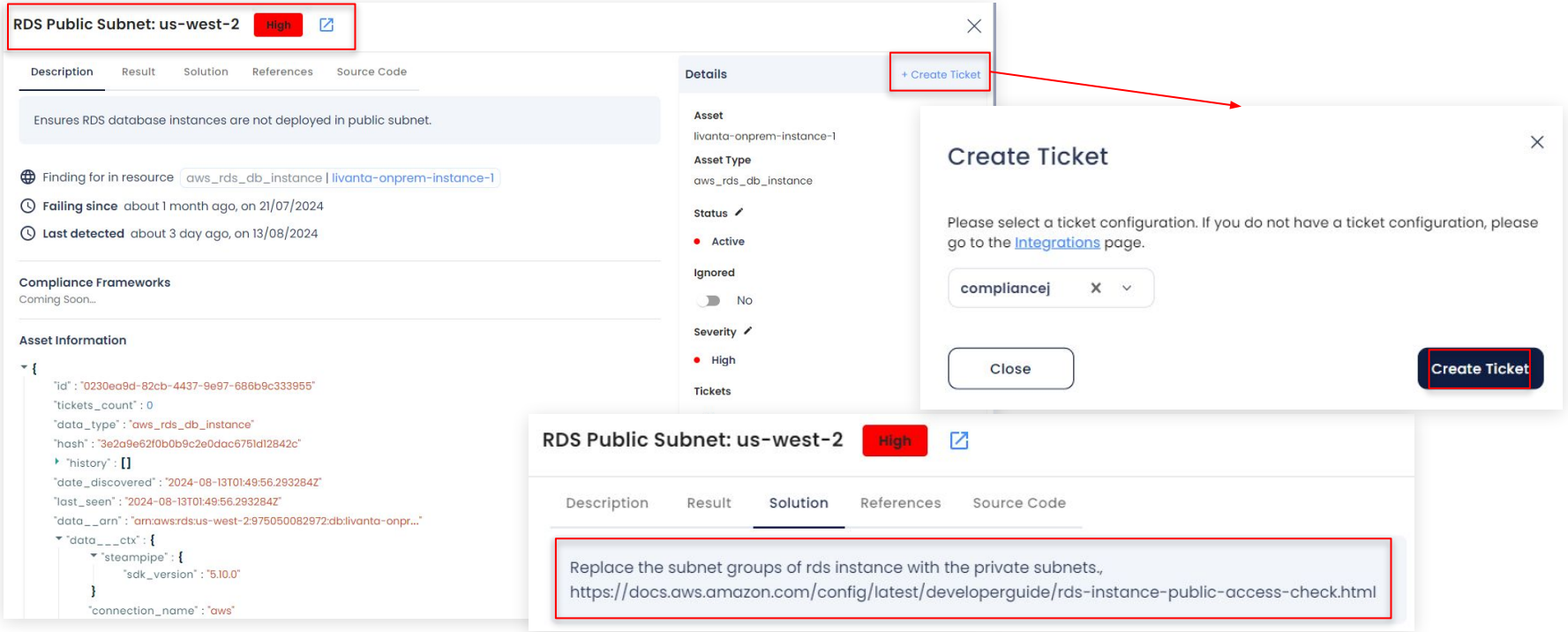
How to identify if Insecure HTTP Port open to public?

- 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



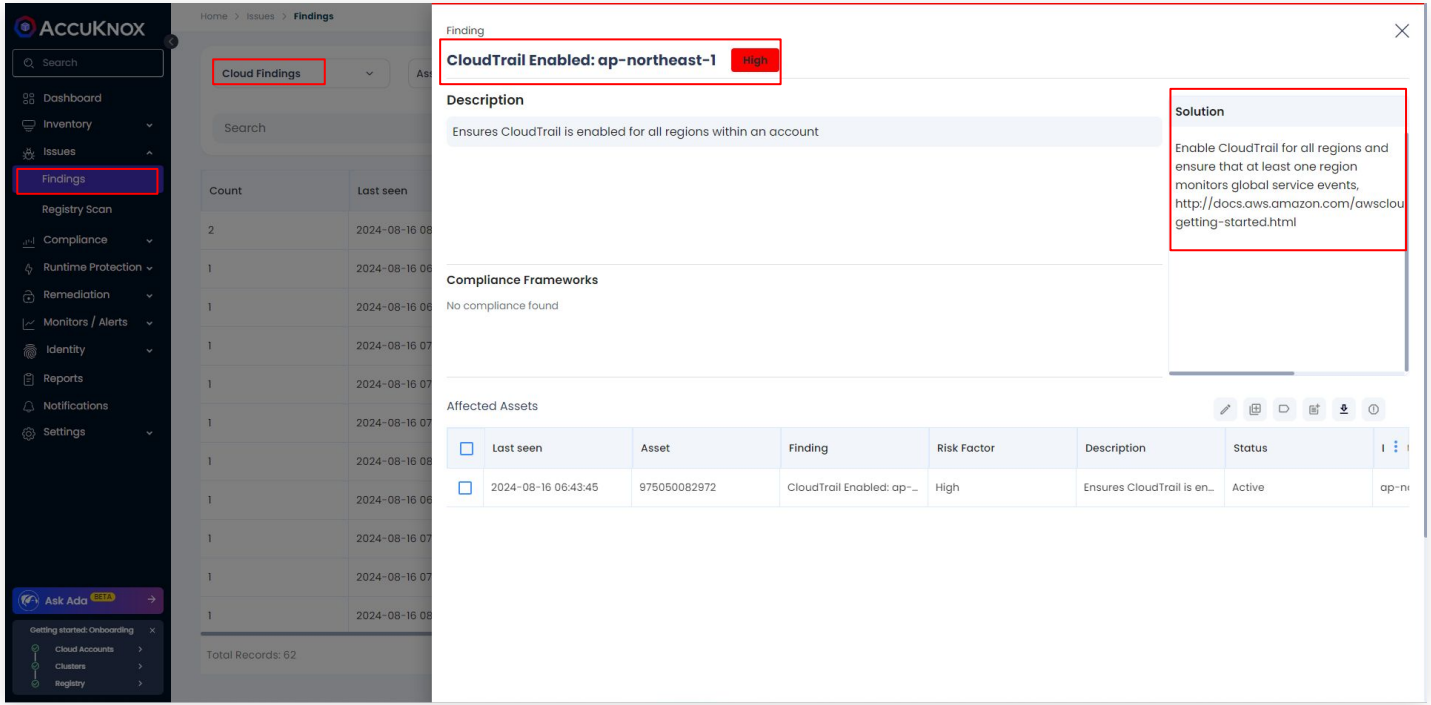
How to identify RDS instances are not deployed in public subnet?

- 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.



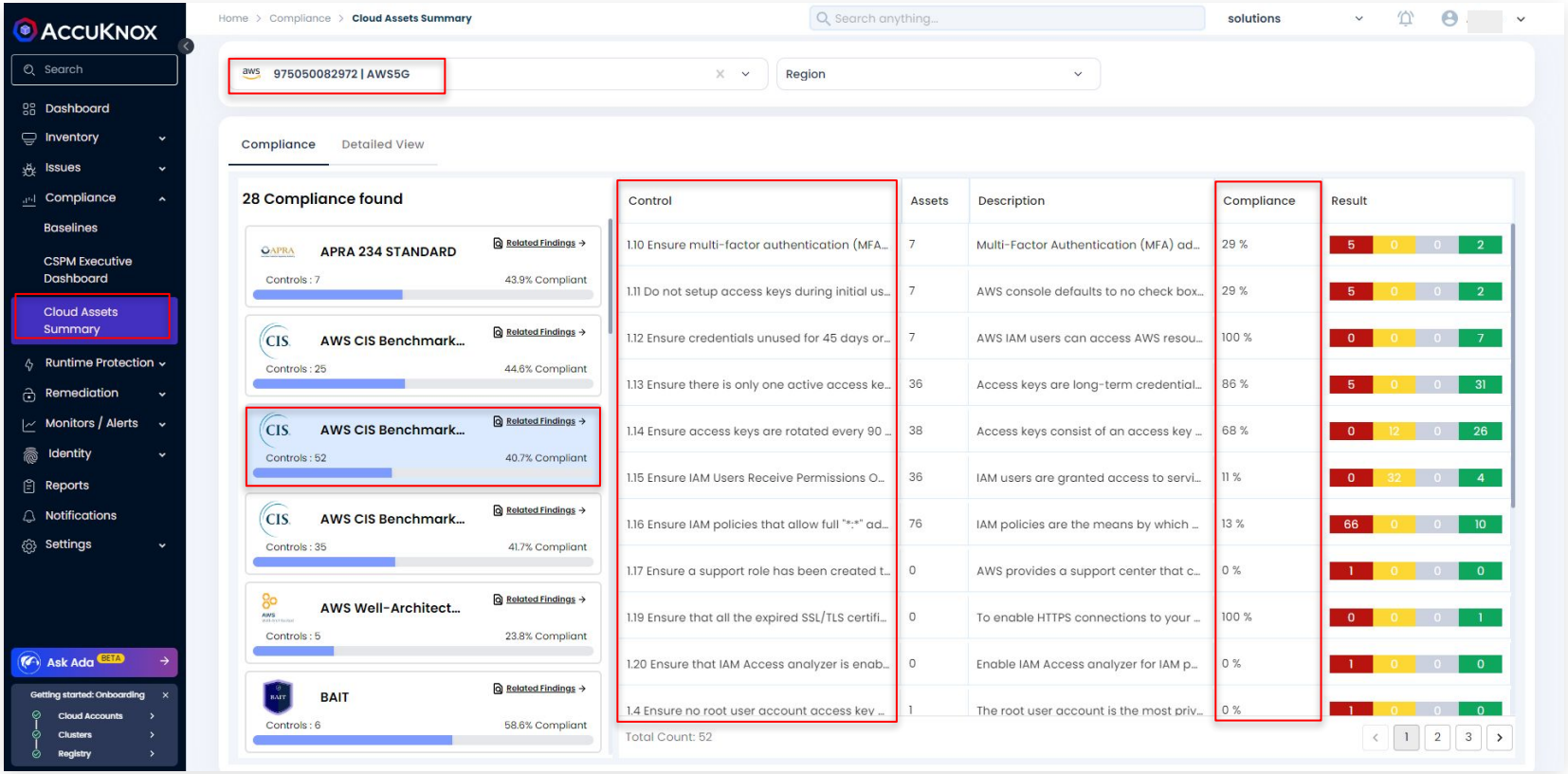
How to identify if cloud trail is enabled for the cloud account?

- To identity 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.



Compliance failure for CIS Benchmark

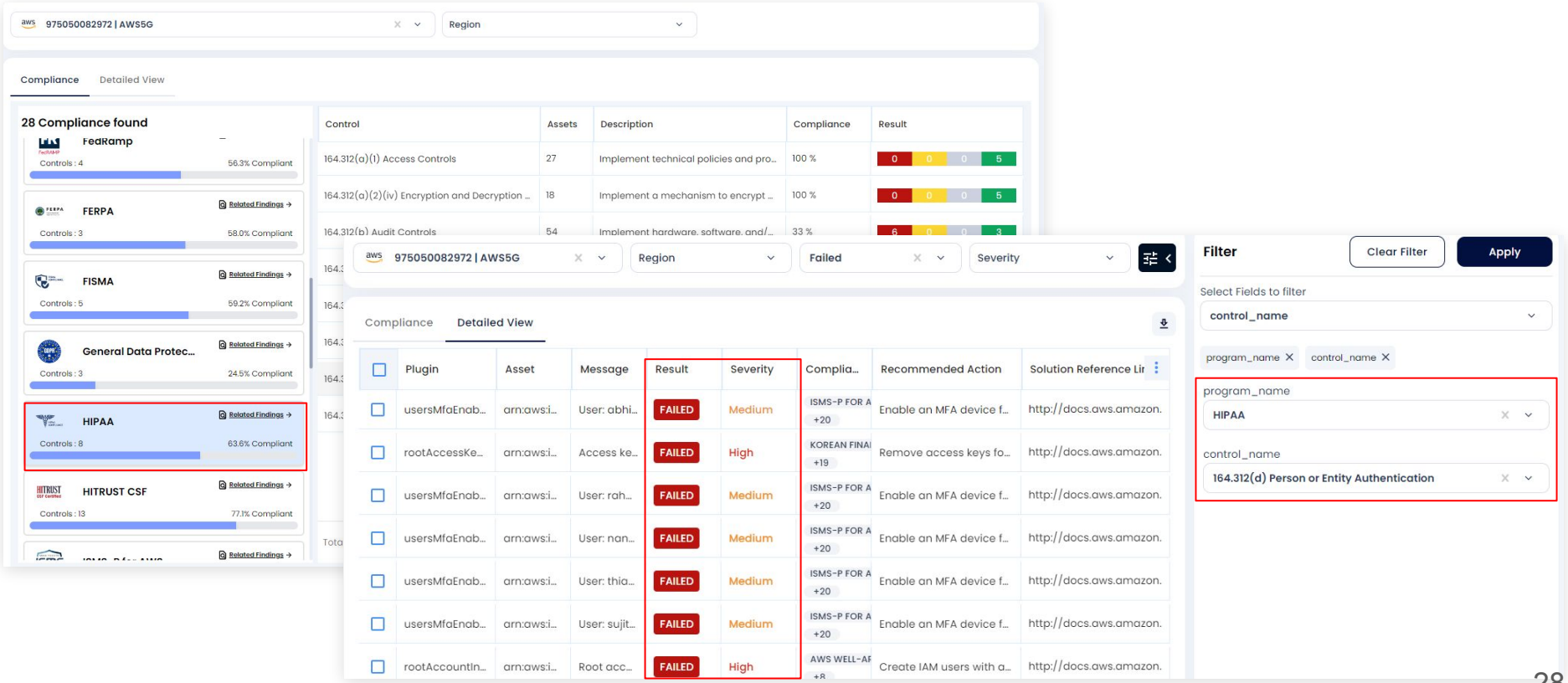
To Identify CIS failed compliance checks > Navigate to Compliance and select Cloud Asset Summary



Compliance failure for HIPAA Benchmark

ACCUKNOX

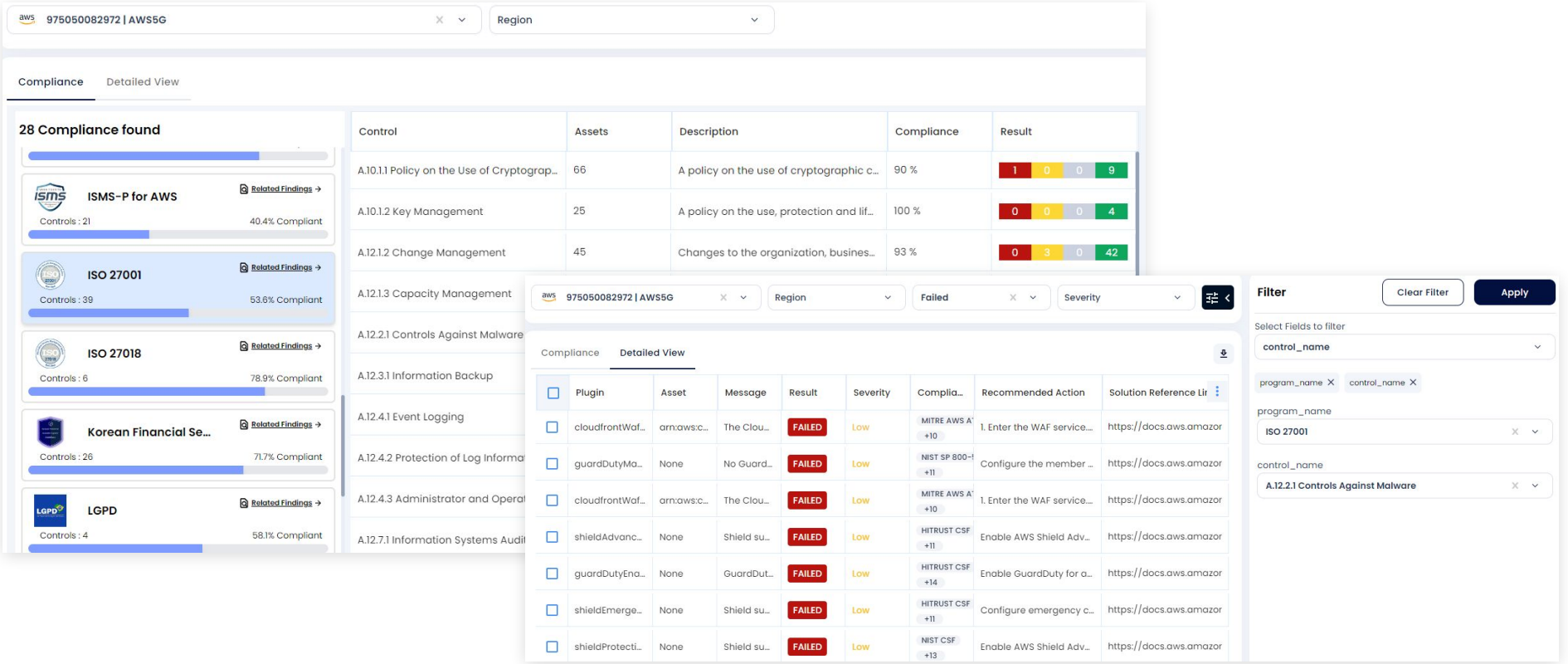
To Identify HIPAA failed compliance checks > Navigate to Compliance and select Cloud Asset Summary



Compliance failure for ISO 27001 Benchmark

ACCUKNOX

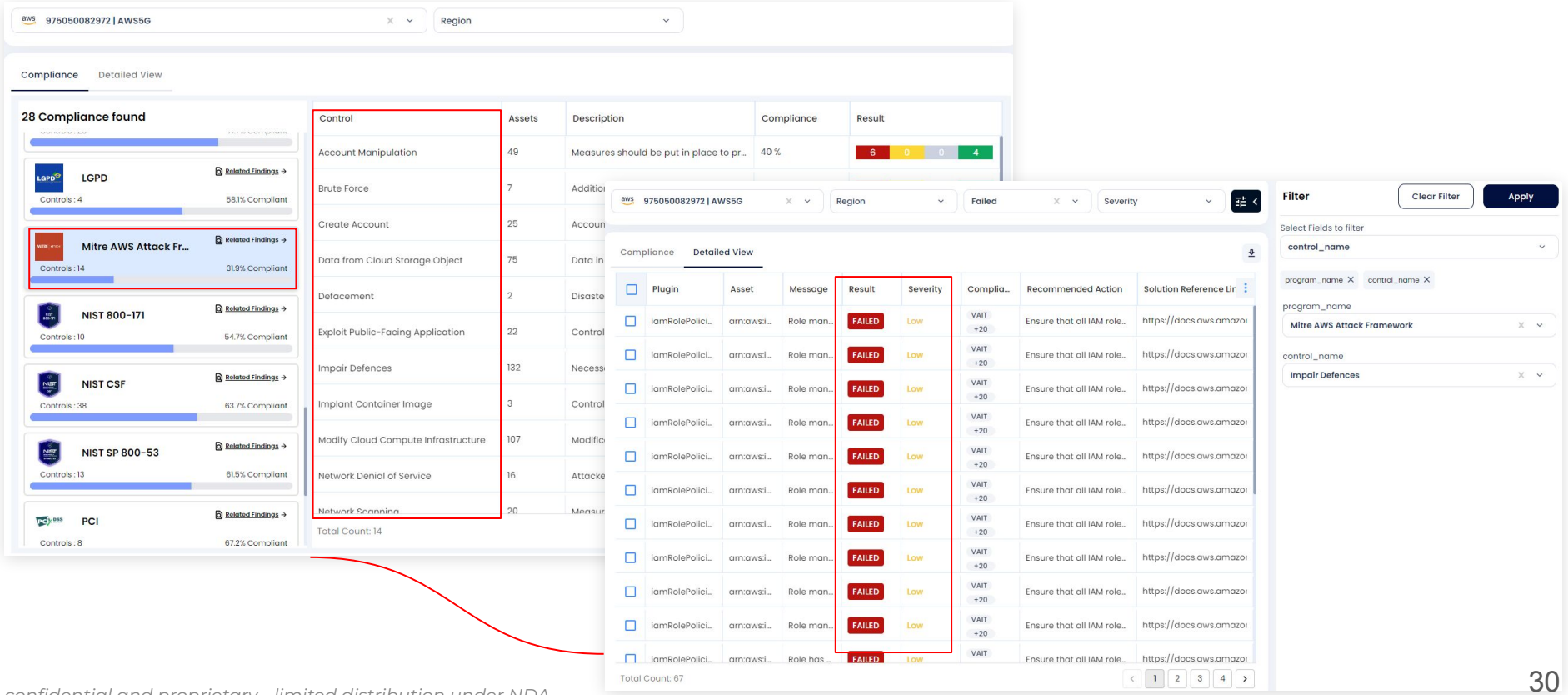
To Identify ISO 27001 failed compliance checks > Navigate to Compliance and select Cloud Asset Summary



Compliance failure for Mitre AWS Attack Framework

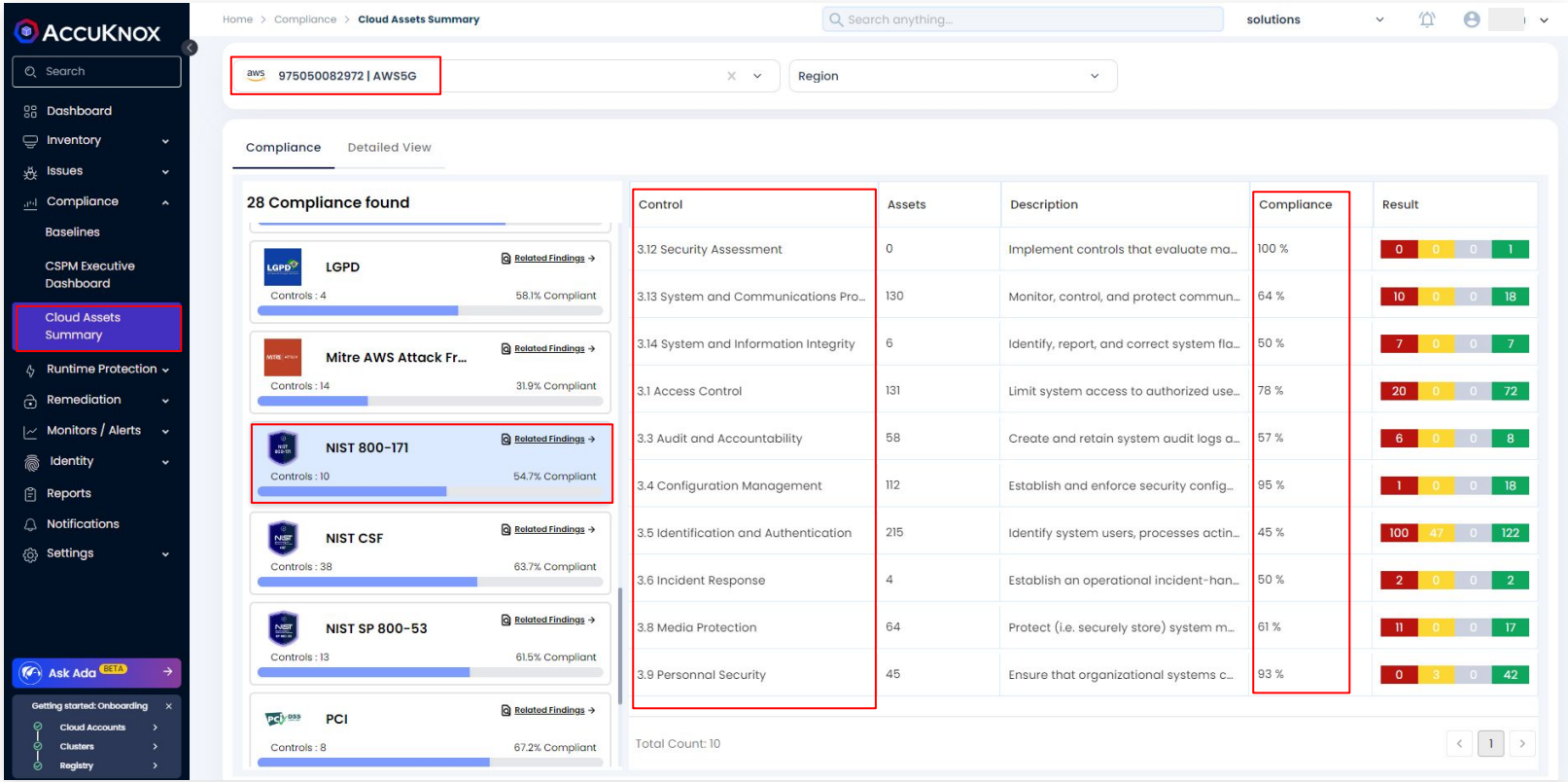
ACCUKNOX

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



Compliance failure for NIST 800 compliance

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



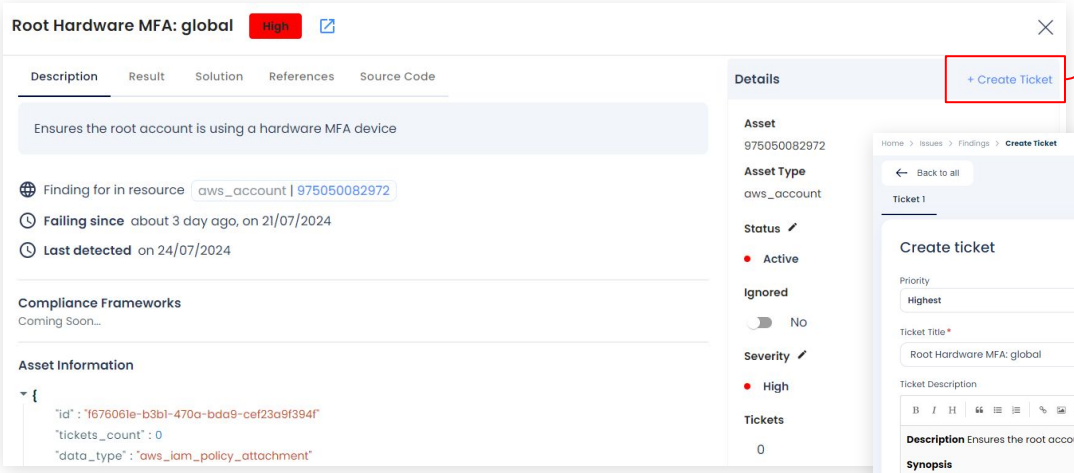
Assistive Remediation For AWS Risks

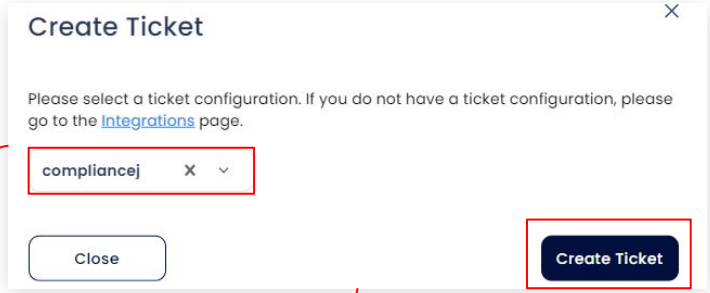
AccuKnox

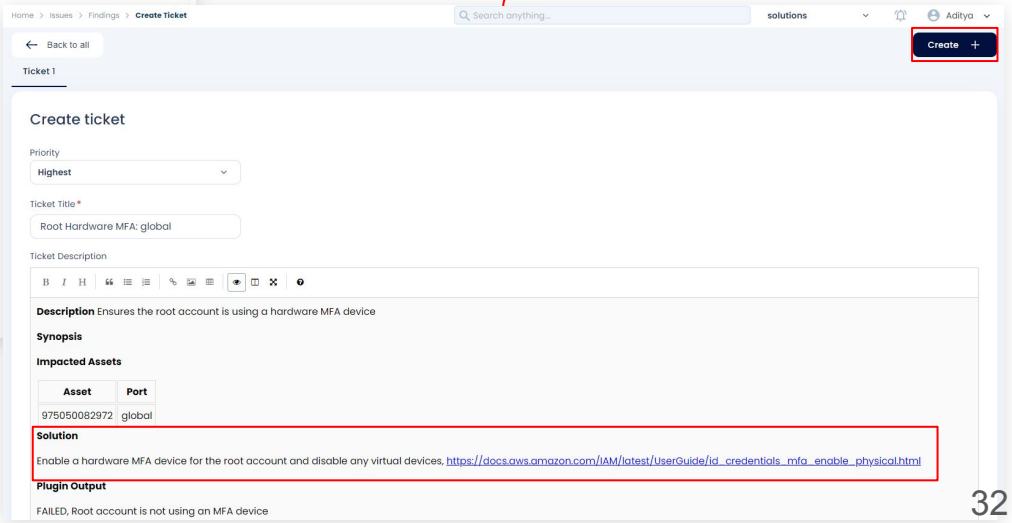
AccuKnox offers solution reference links to assist with the remediation

To Remediate the findings (Approach 1)

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



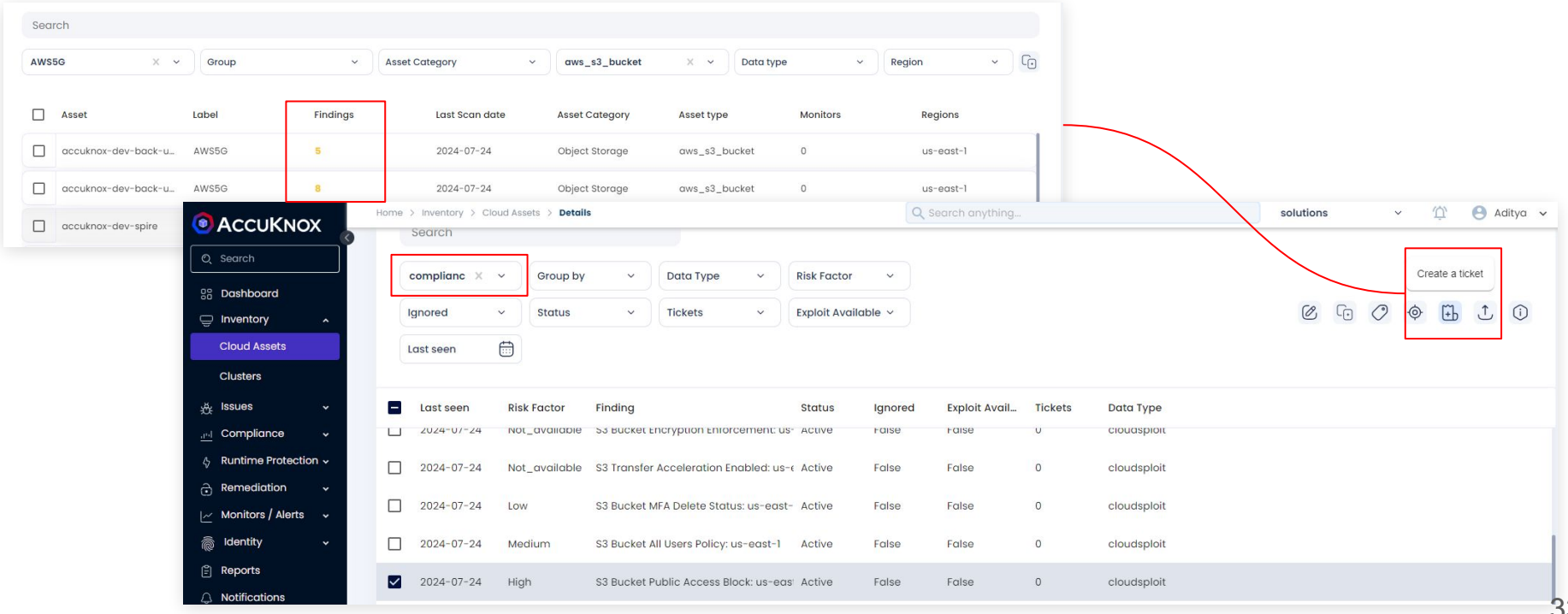




Assistive Remediation For AWS Risks

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

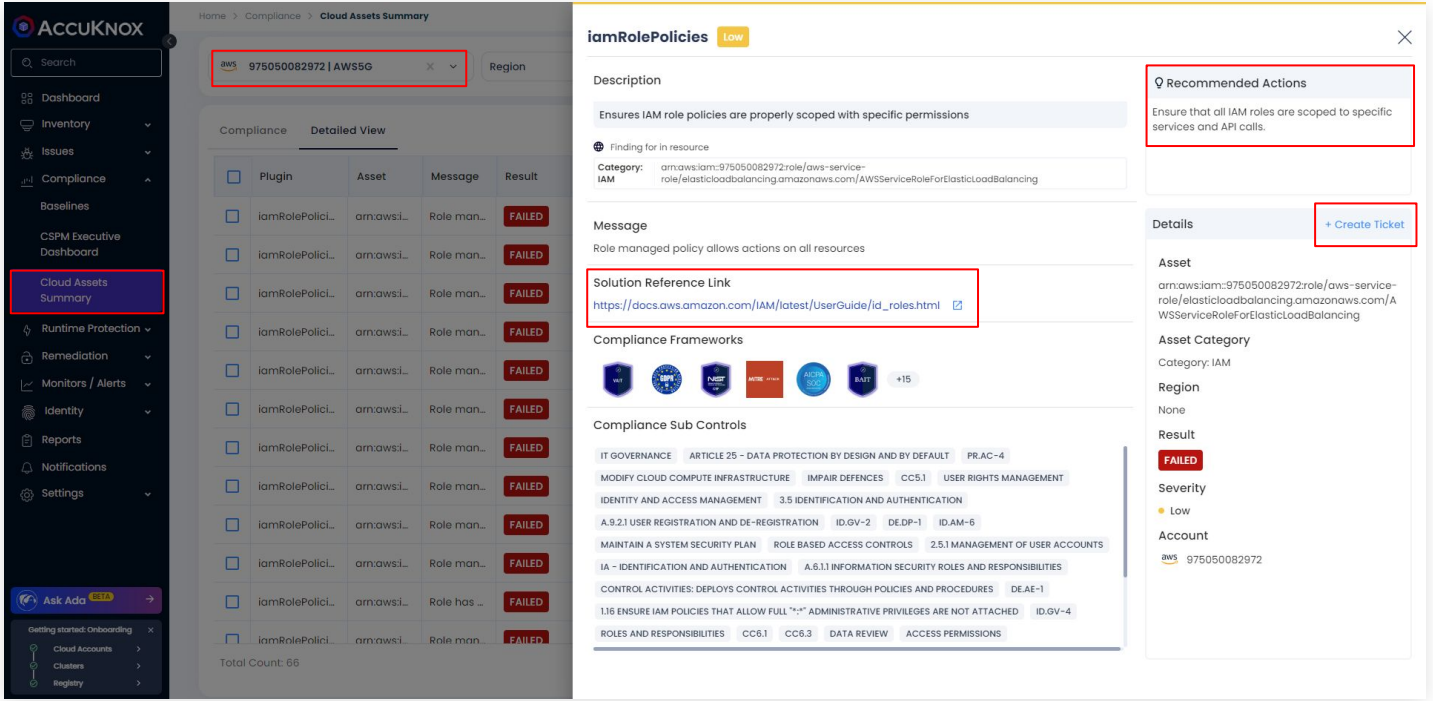


Assistive Remediation For AWS Compliance Failure

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

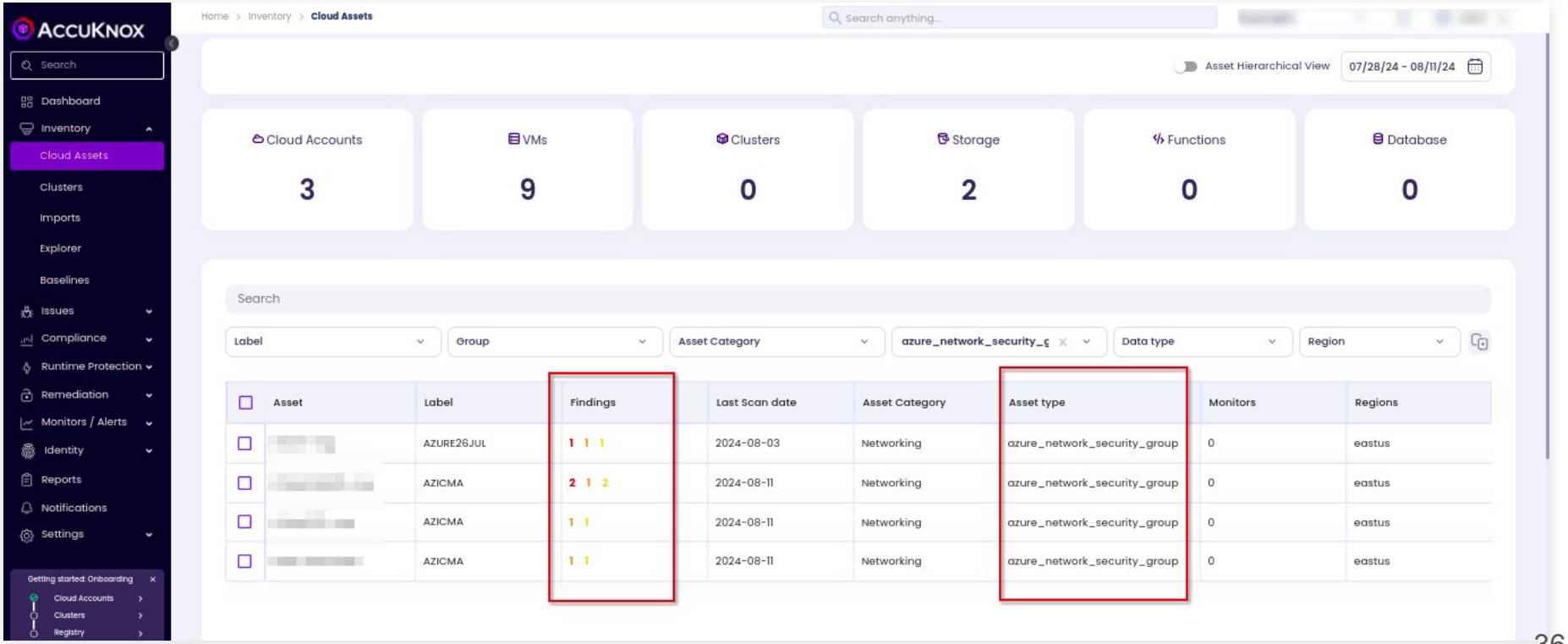


AZURE Misconfigurations

Critical Risks

How to identify all issues in Azure Network security group?

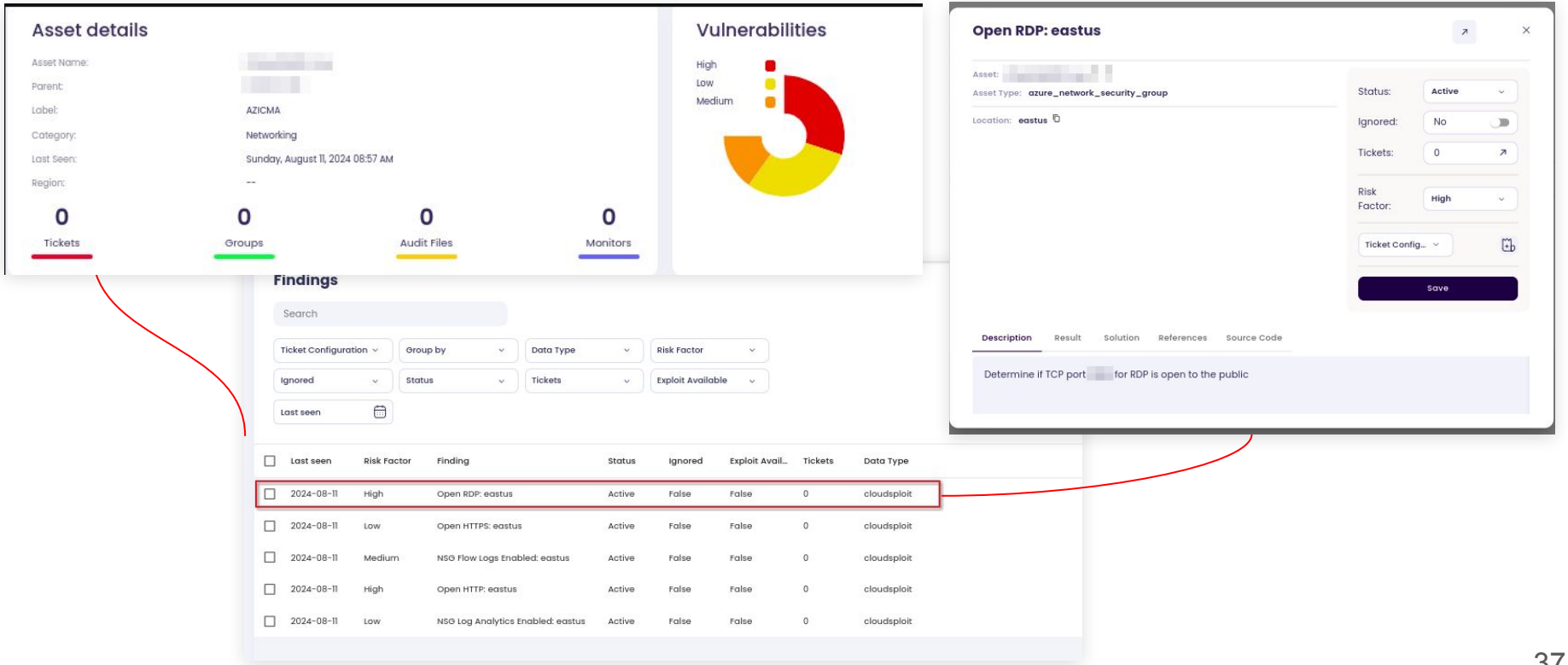
- Go to Inventory >> Assets page and Filter for Asset Type as ***azure_network_security_group***
- Look for ***Azure Network security group*** with count in ***Total Vulnerabilities***



Identify Azure Network security group issues

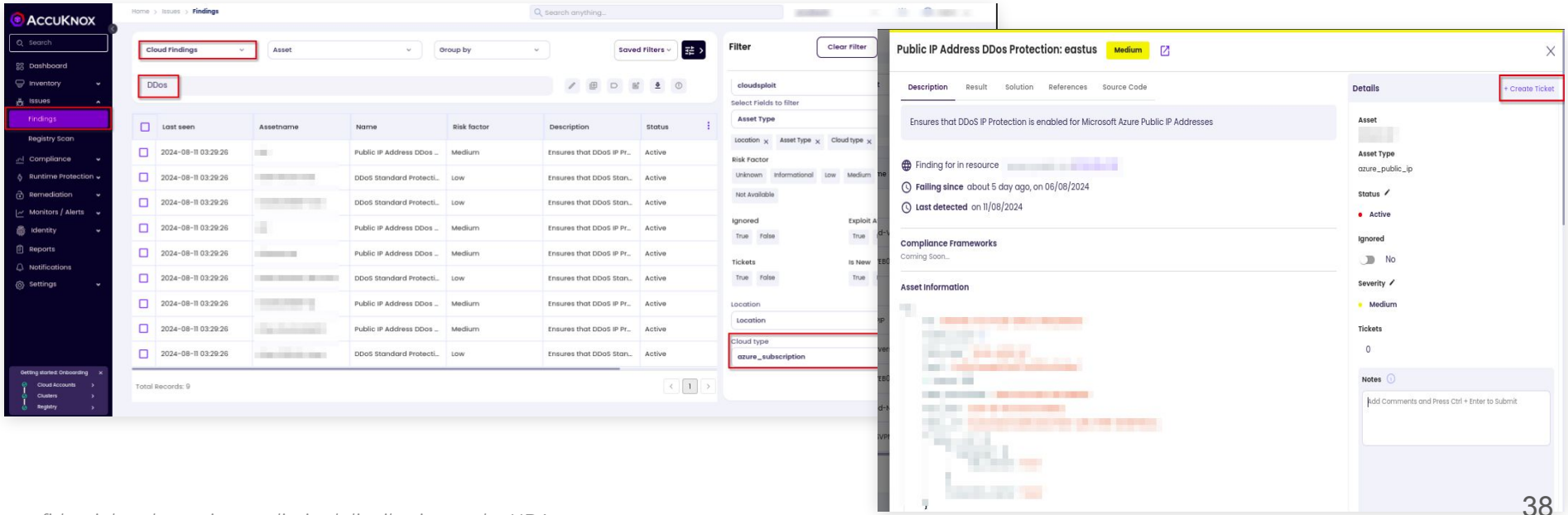
ACCUKNOX

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



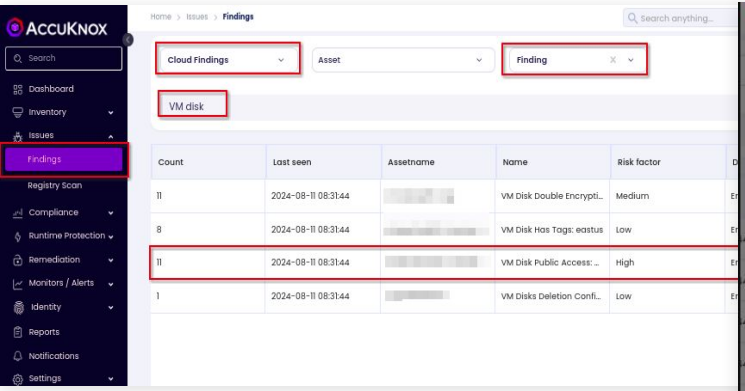
How to Identify if the DDoS protection is enabled?

- 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

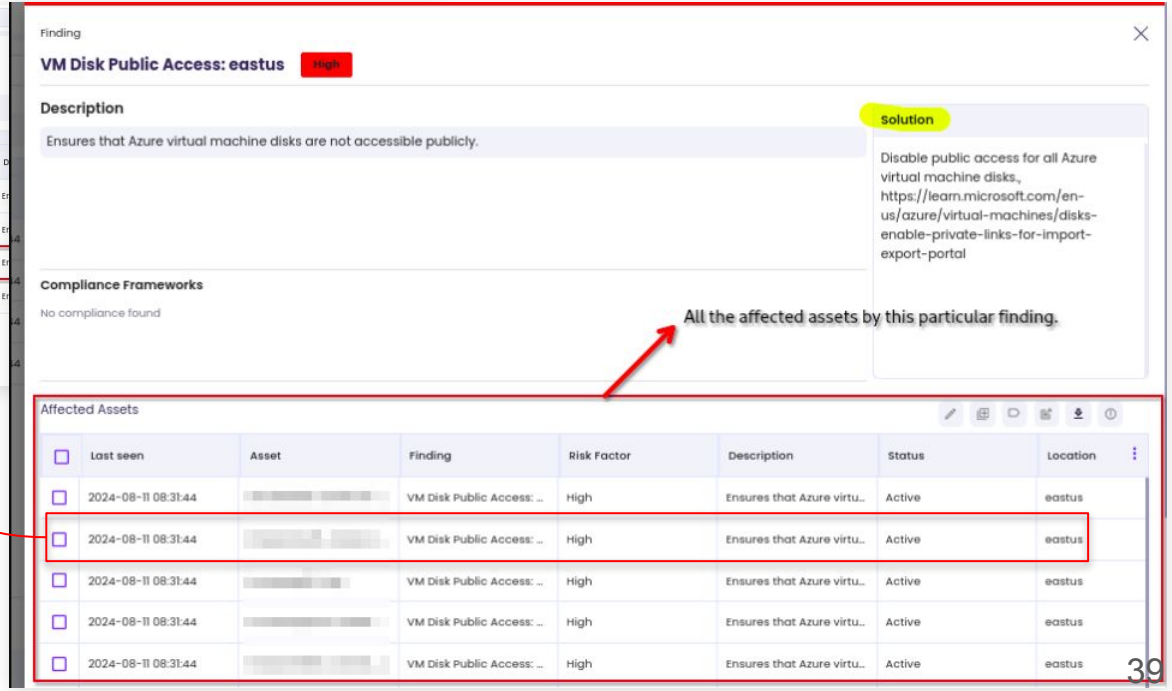


How to Identify if the VM Disks are not publicly accessible?

- 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

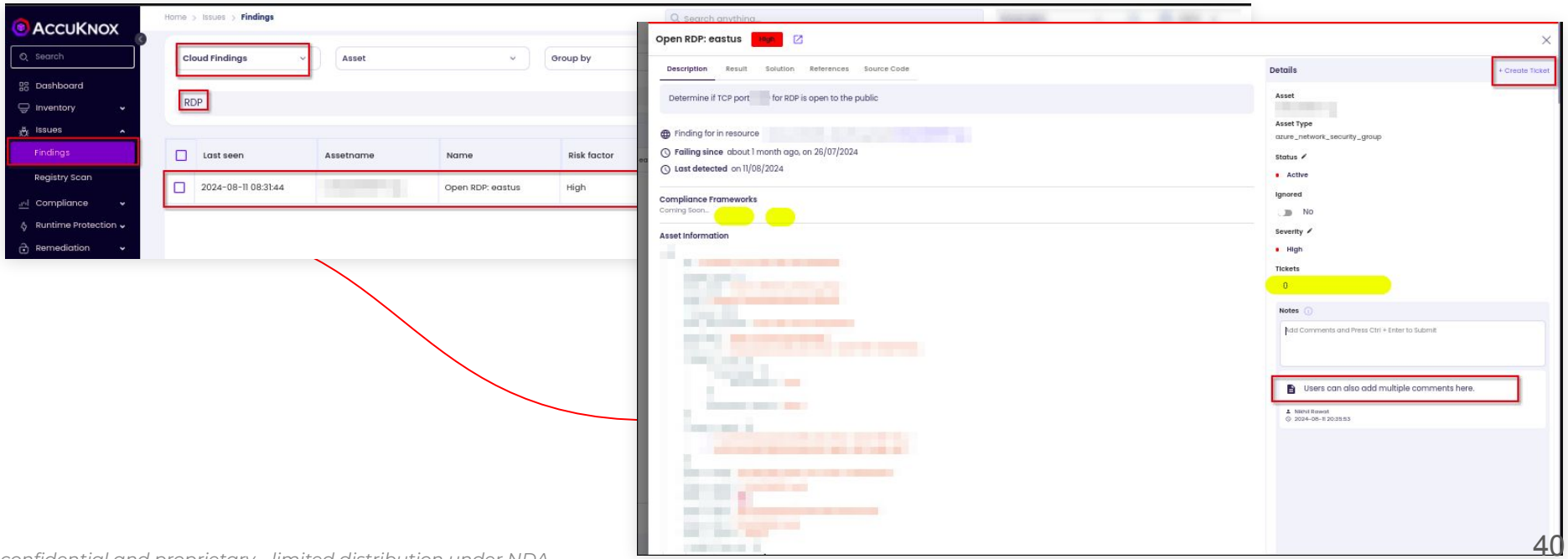


Click on any findings to view get more detailed view.



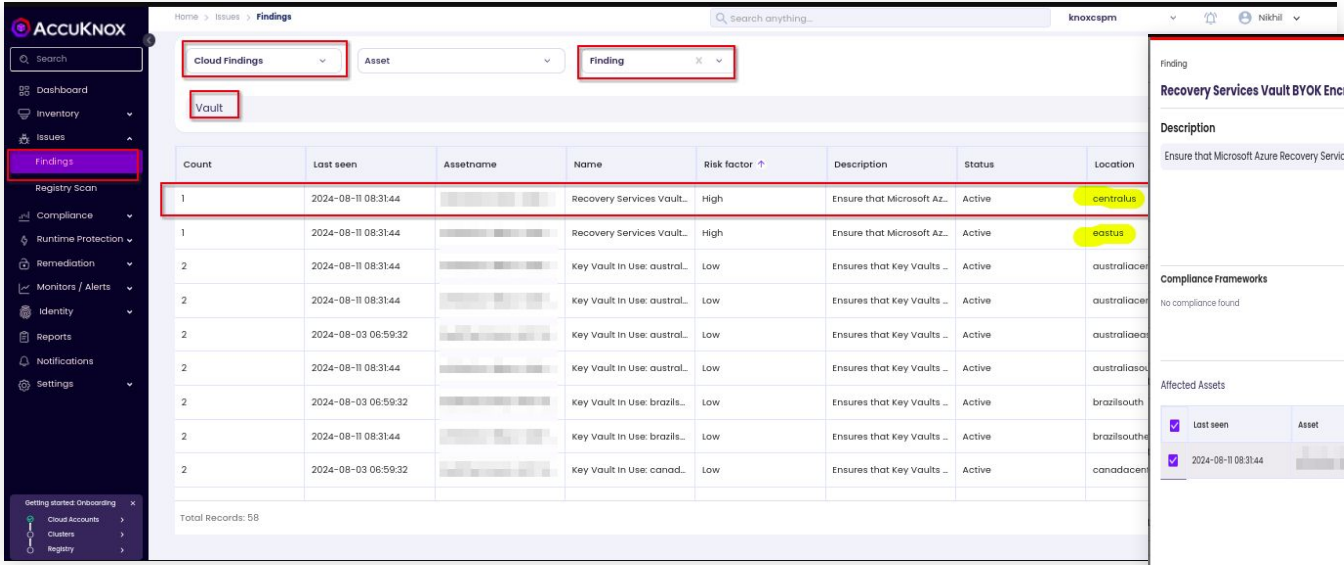
How to Identify if the RDP Port is Open in Azure Network Security Group?

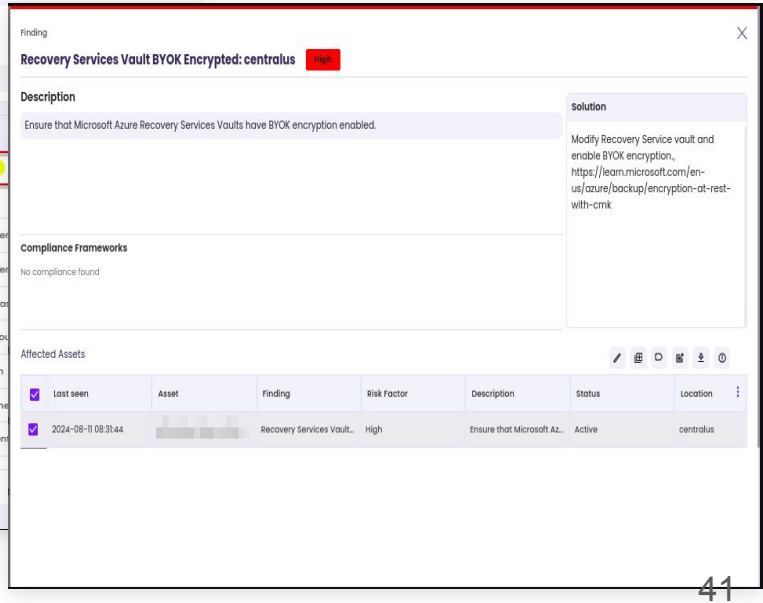
- To identify if the RDP port is open in Azure Network Security Groups, please navigate to Issues -> Findings.
  - Select **Cloud Findings** in the findings-type filter.
  - You can also directly search for the specific Assets/Findings using the Search field.
  - For more detailed information and to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



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

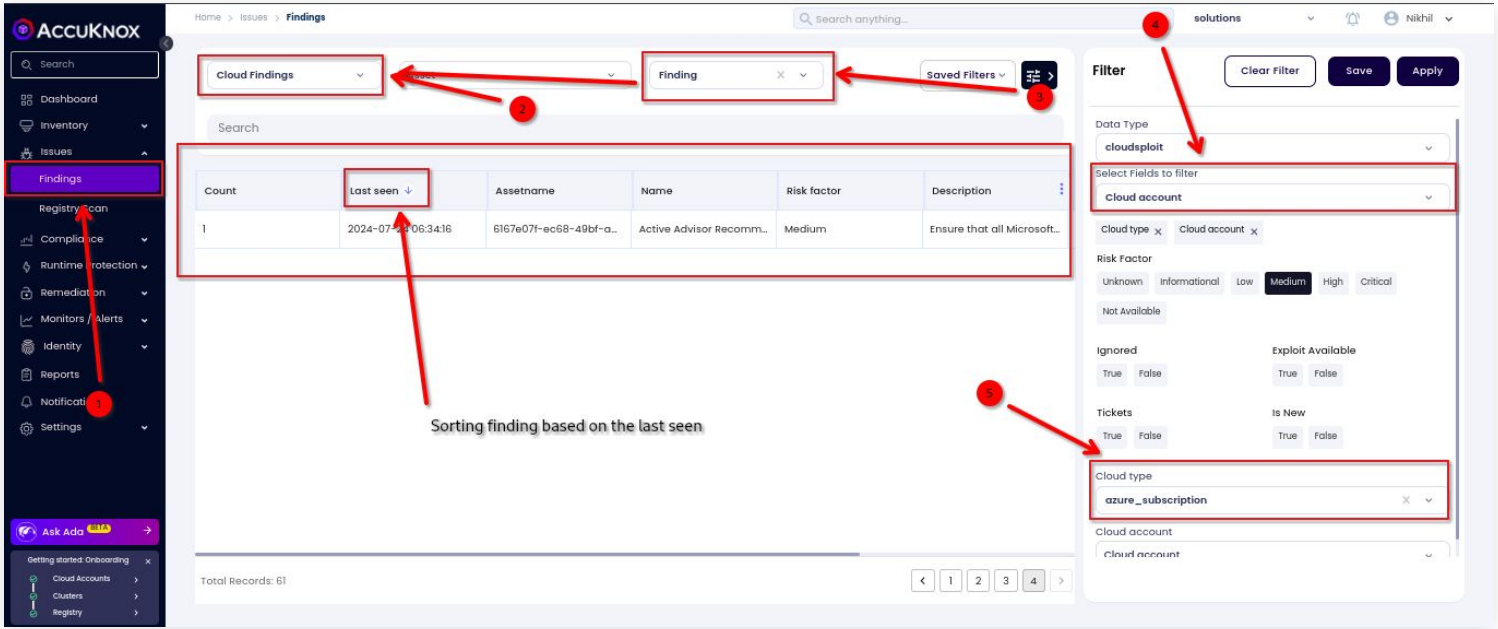
- To identify if the Recovery Services Vault is encrypted with Bring Your Own Key (BYOK) in Azure, please navigate to Issues -> Findings.
  - Select **Cloud Findings** in the findings-type filter.
  - Choose Findings in the group by filter.
  - You can also directly search for the specific Assets/Findings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





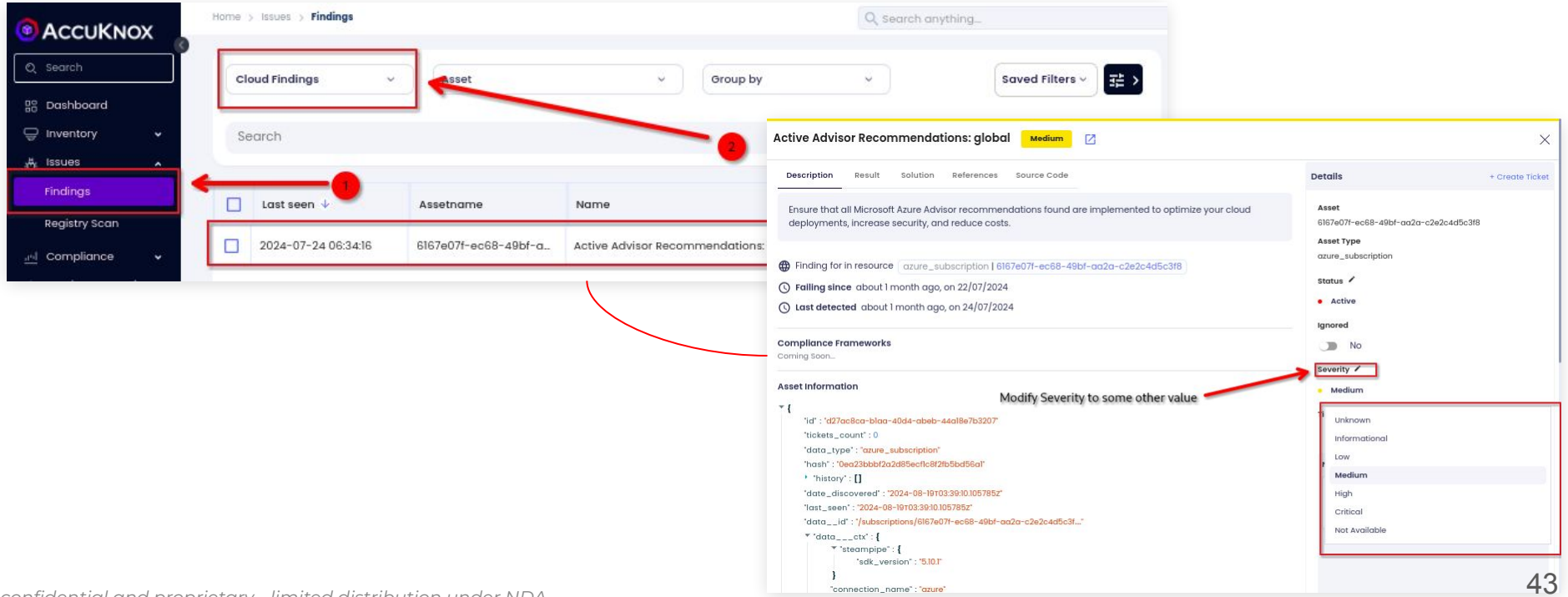
How to Identify if the SQL Server Firewall Rule Alerts Monitor is enabled in Azure?

- 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.



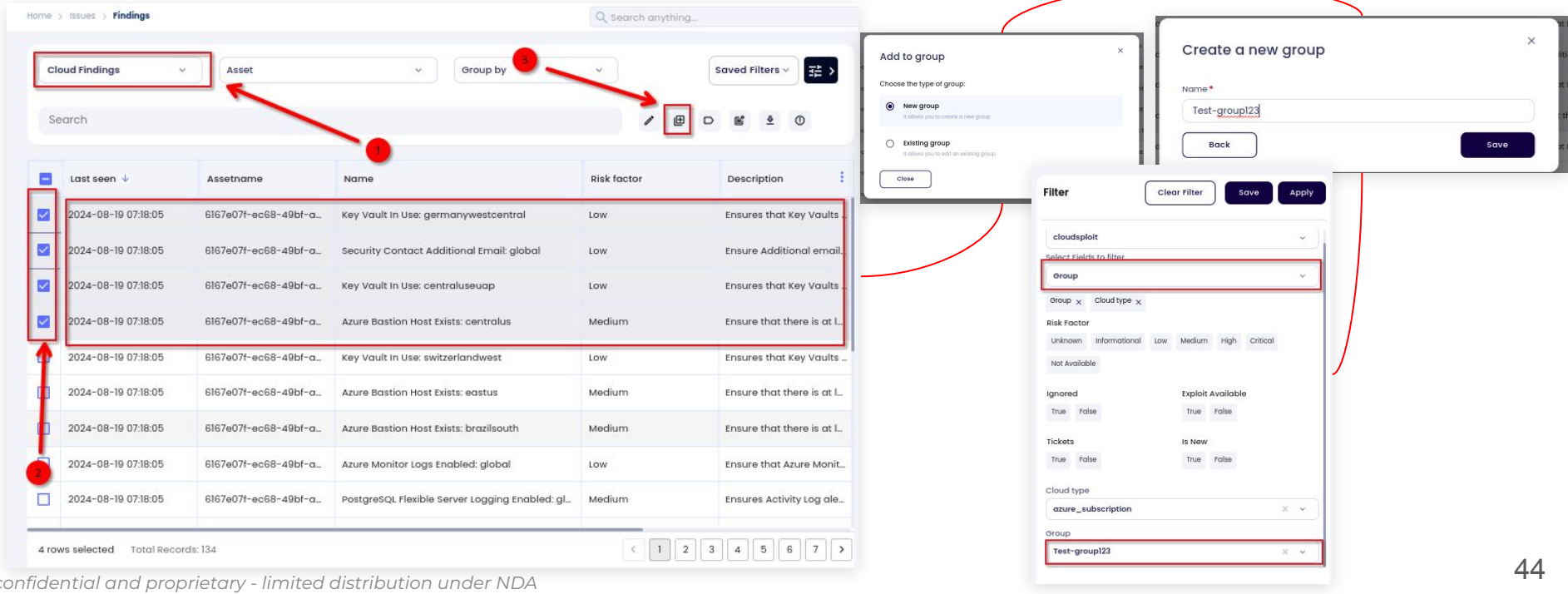
How to Identify if the Microsoft Azure Advisor recommendations are implemented in Azure?

- 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.



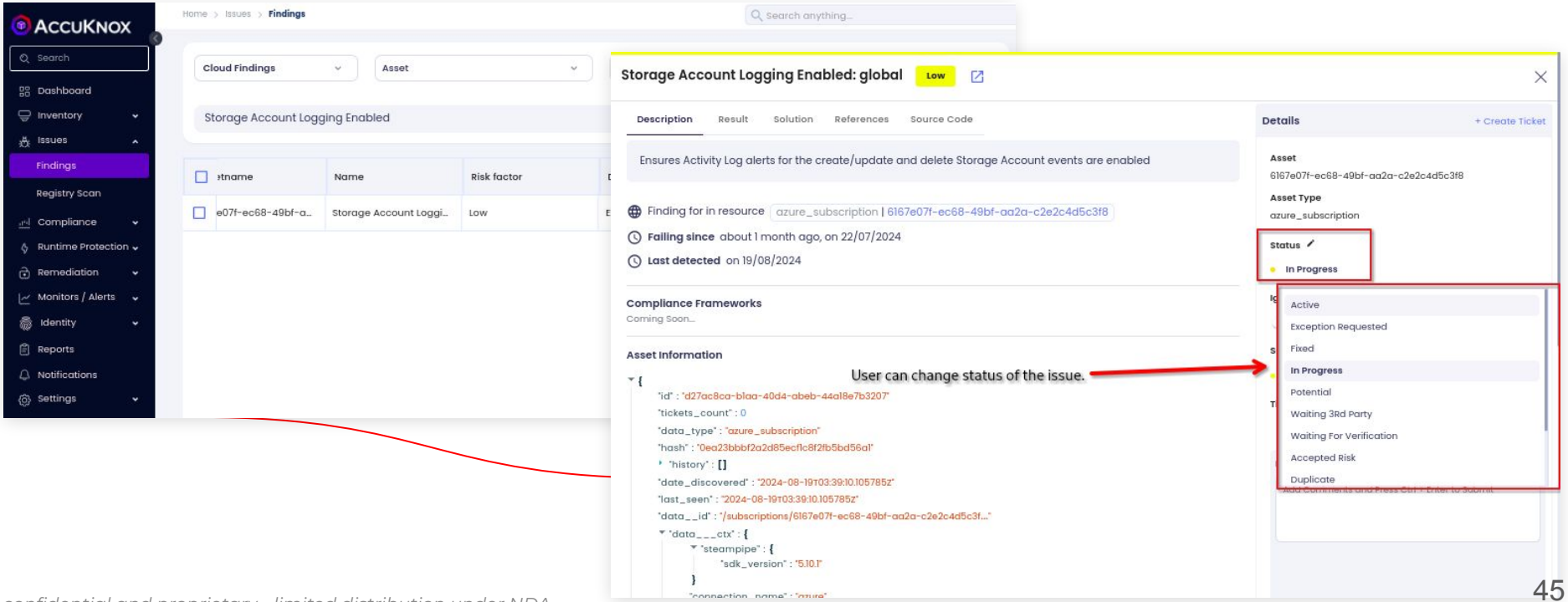
How to Group different findings together in Azure?

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



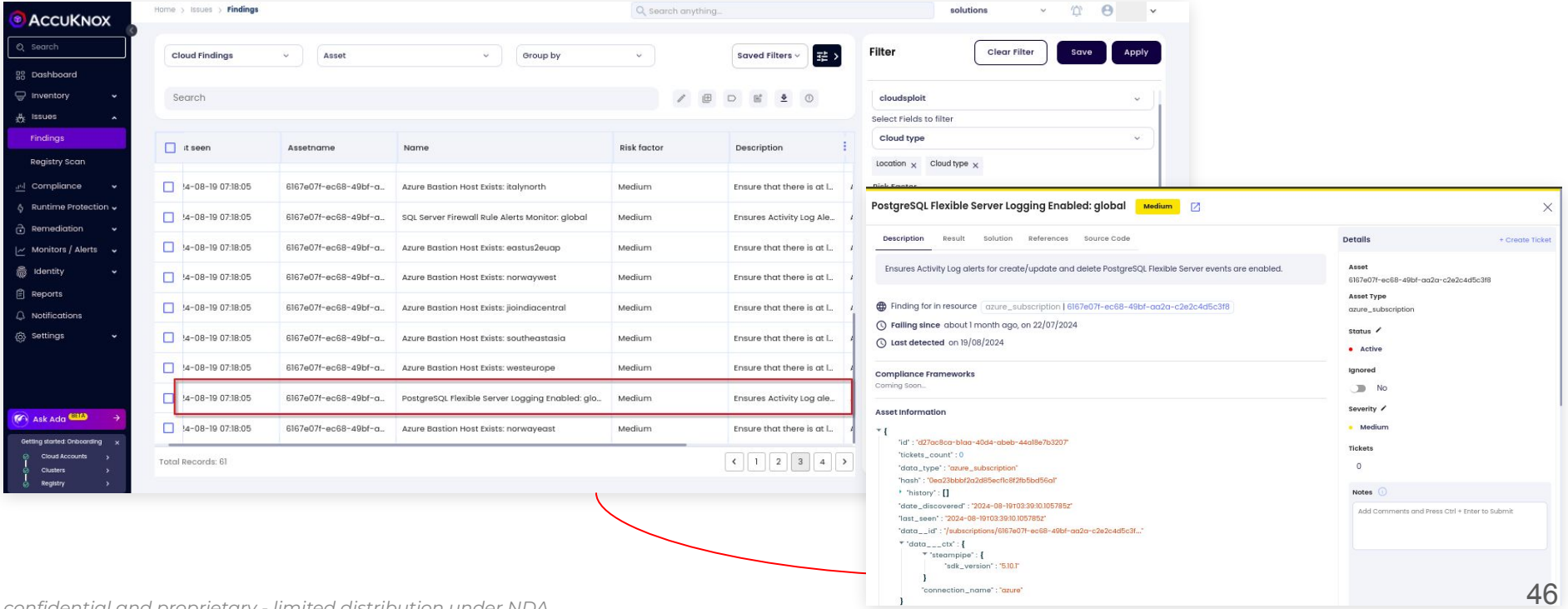
How to Identify if the Storage Account Logging Enabled in Azure?

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



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

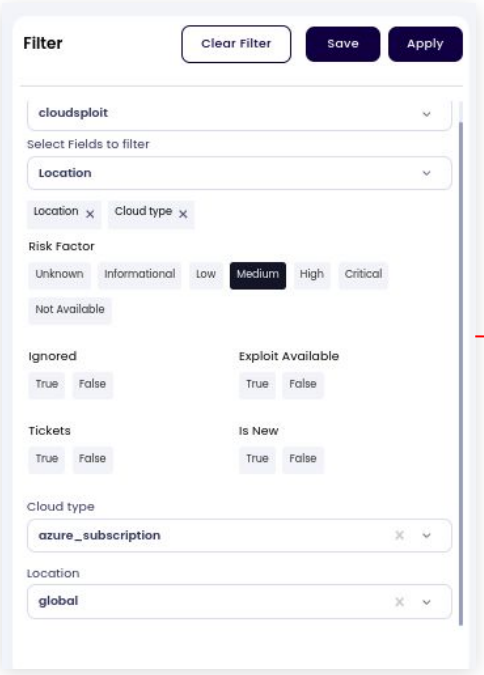
- To identify if the postgreSQL Flexible Server Logging Enabled in Azure, please navigate to Issues -> Findings.
  - Select **Cloud Findings** in the findings-type filter.
  - You can also directly search for the specific Assets/Findings using the Search field.
  - For more detailed information and to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

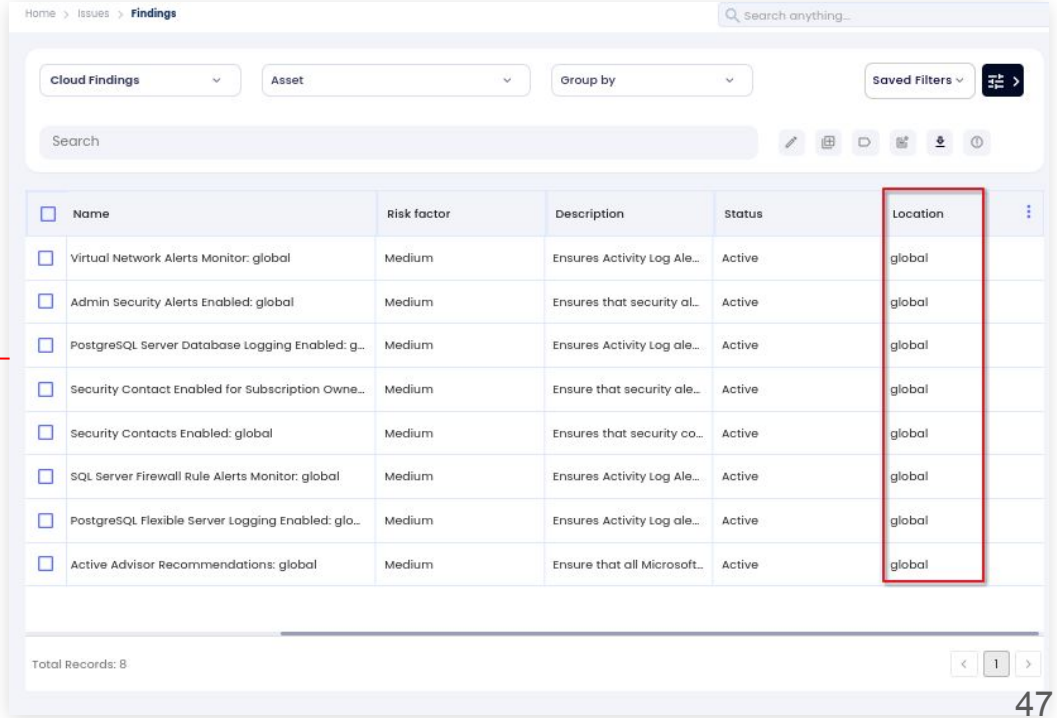


How to Identify all the findings within the Global region in Azure?

ACCUKNOX

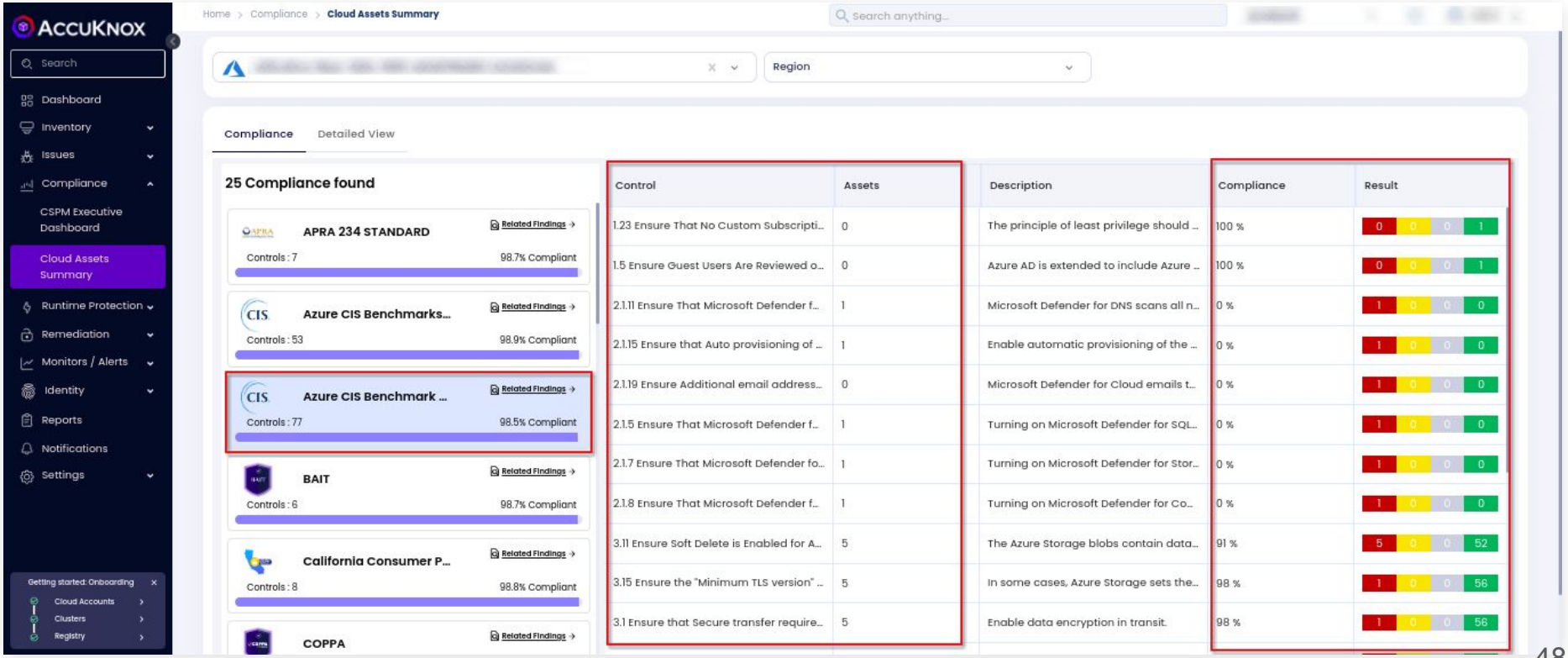
- To identify all the findings within the Global region in Azure, please navigate to Issues -> Findings.
  - Select **Cloud Findings** in the findings-type filter.
  - In the advanced filter add location, then select Global region in location and apply it.
  - For more detailed information and to create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





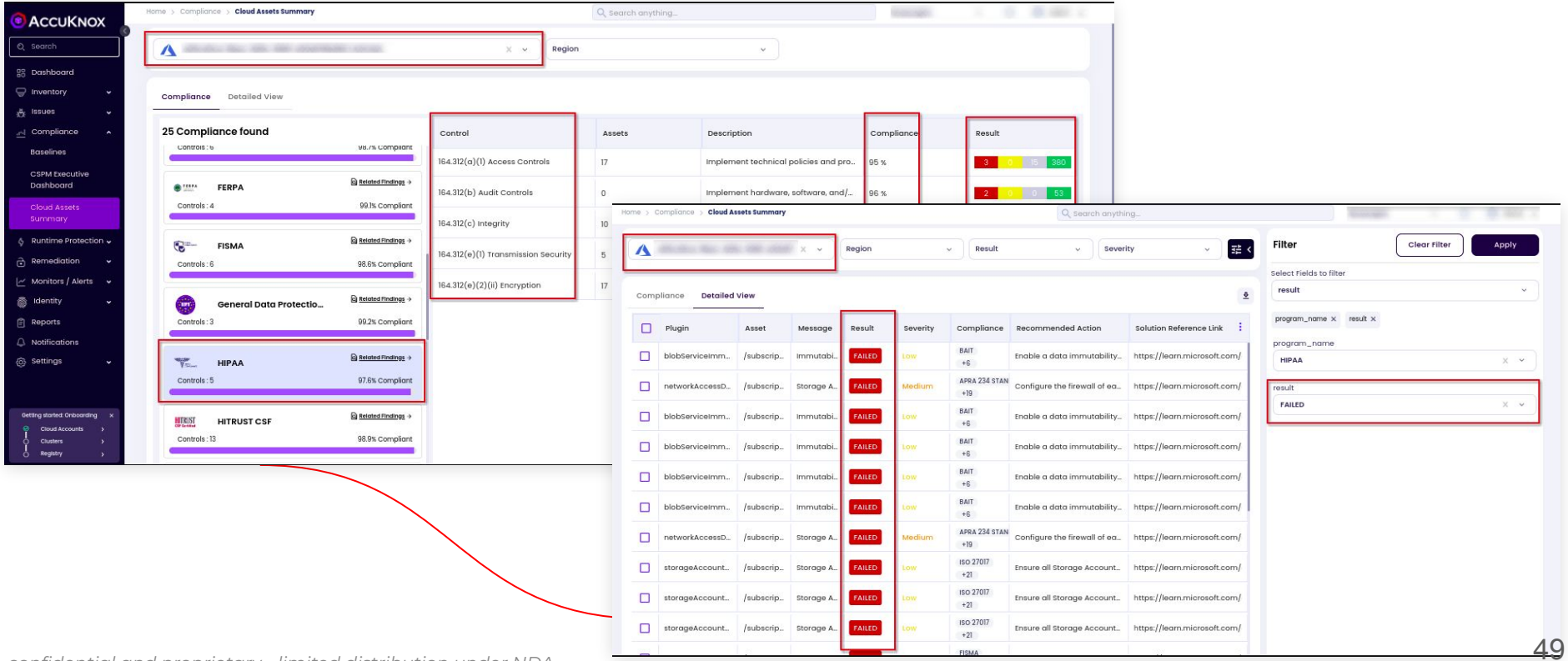
Compliance failure for Azure CIS Benchmark v2.0.0

- 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.



Compliance failure for HIPPA Benchmark v2.0.0

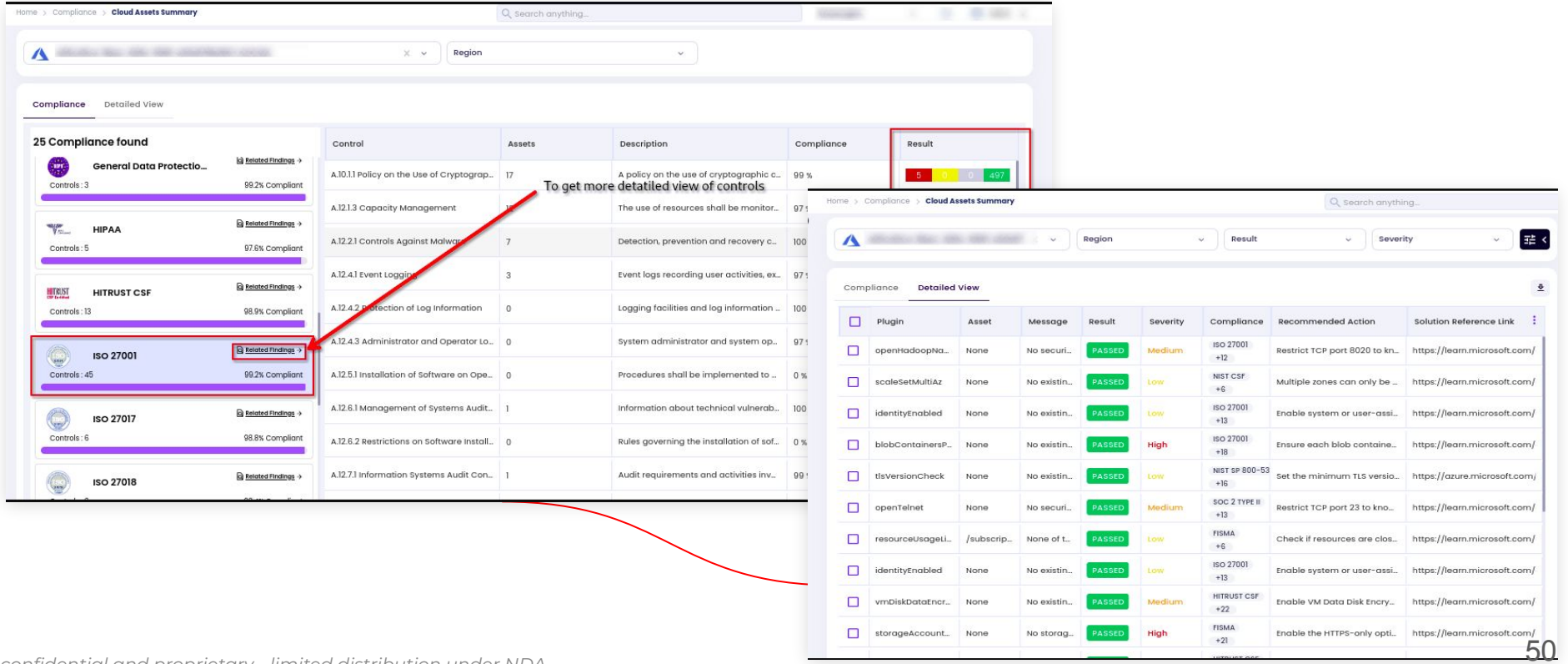
- To Identify HIPPA failed compliance checks > Navigate to Compliance and select Cloud Asset Summary
- After that choose the cloud account for which you want to assess the compliance posture.



Compliance failure for ISO 27001 Benchmark

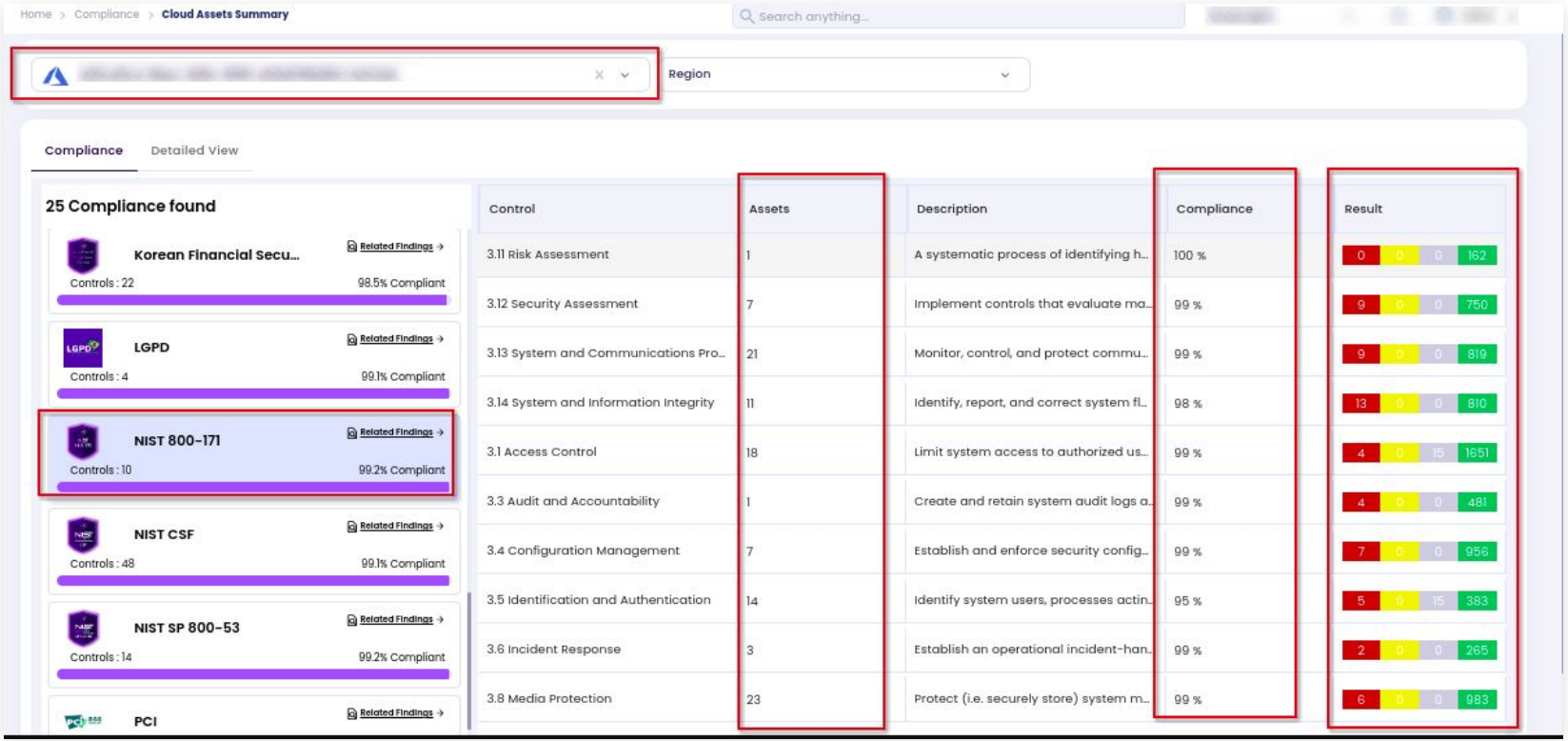
ACCUKNOX

- 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.



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.

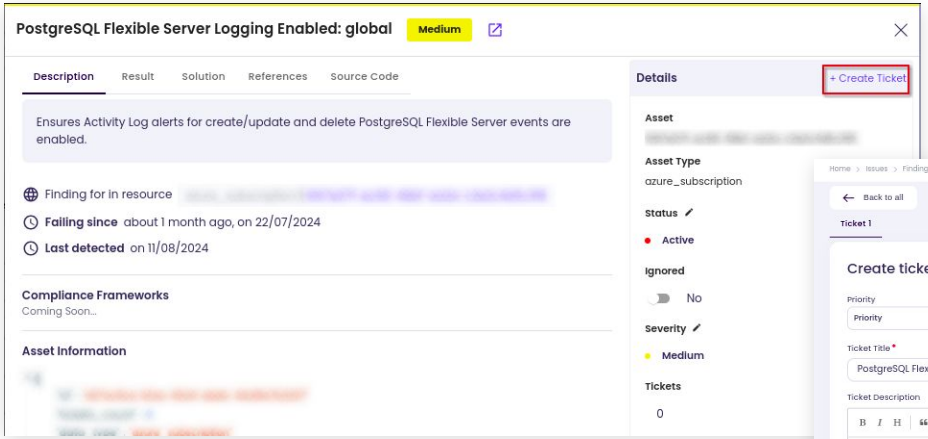


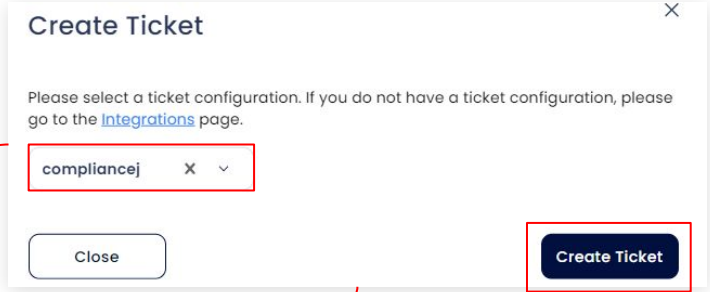
Assistive Remediation For Azure Risks

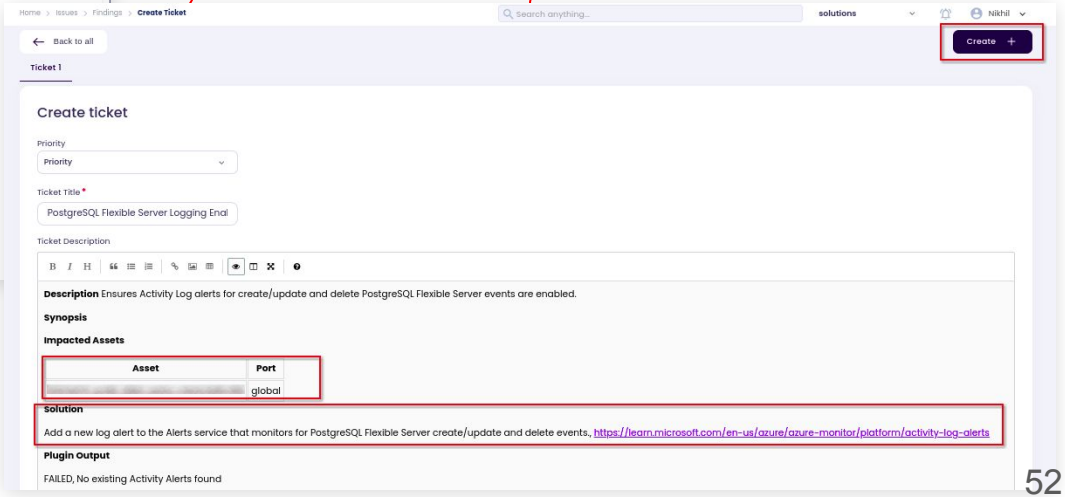
AccuKnox offers solution reference links to assist with the remediation

To Remediate the findings (Approach 1)

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



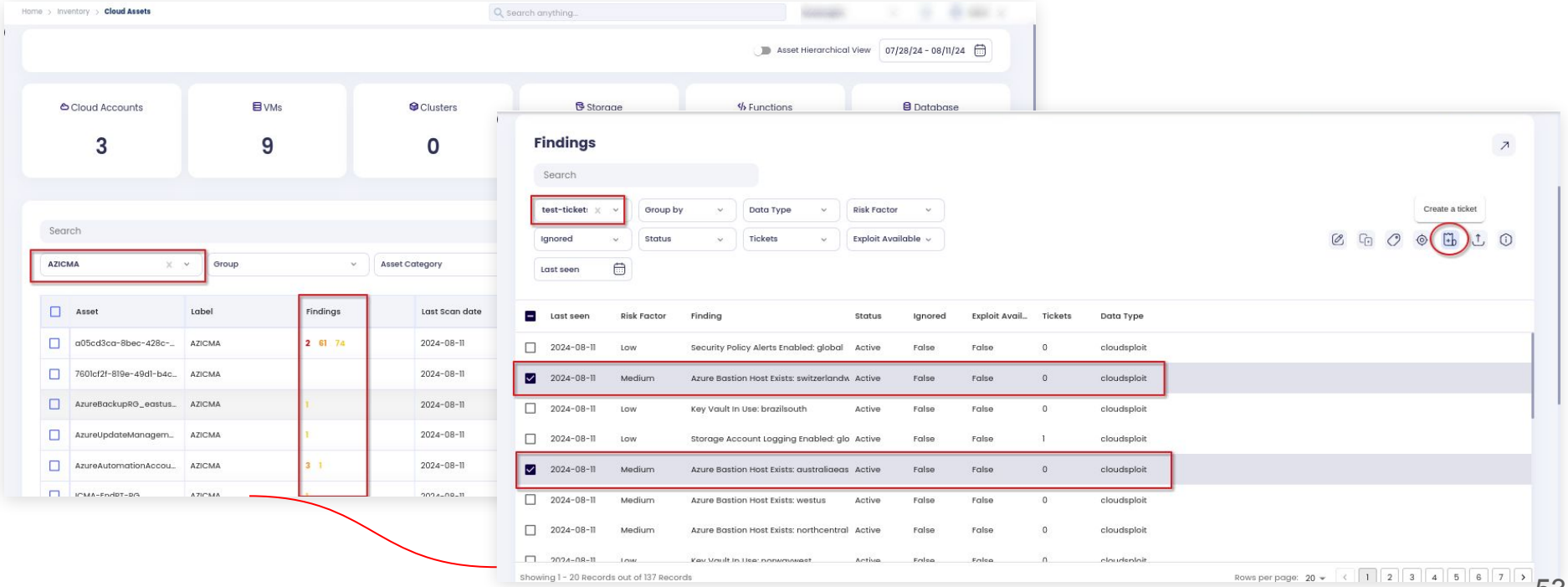




Assistive Remediation For Azure Risks

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

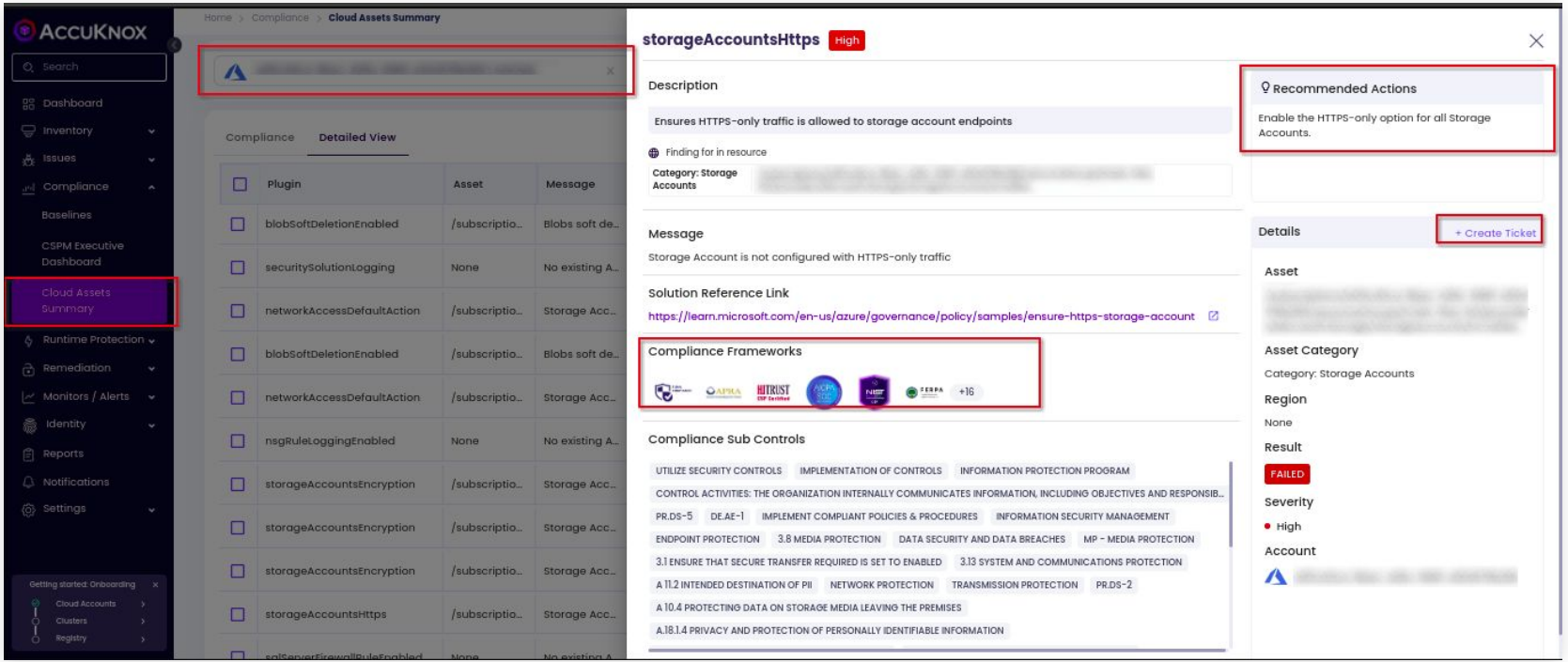


Assistive Remediation For Azure Compliance Failure

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

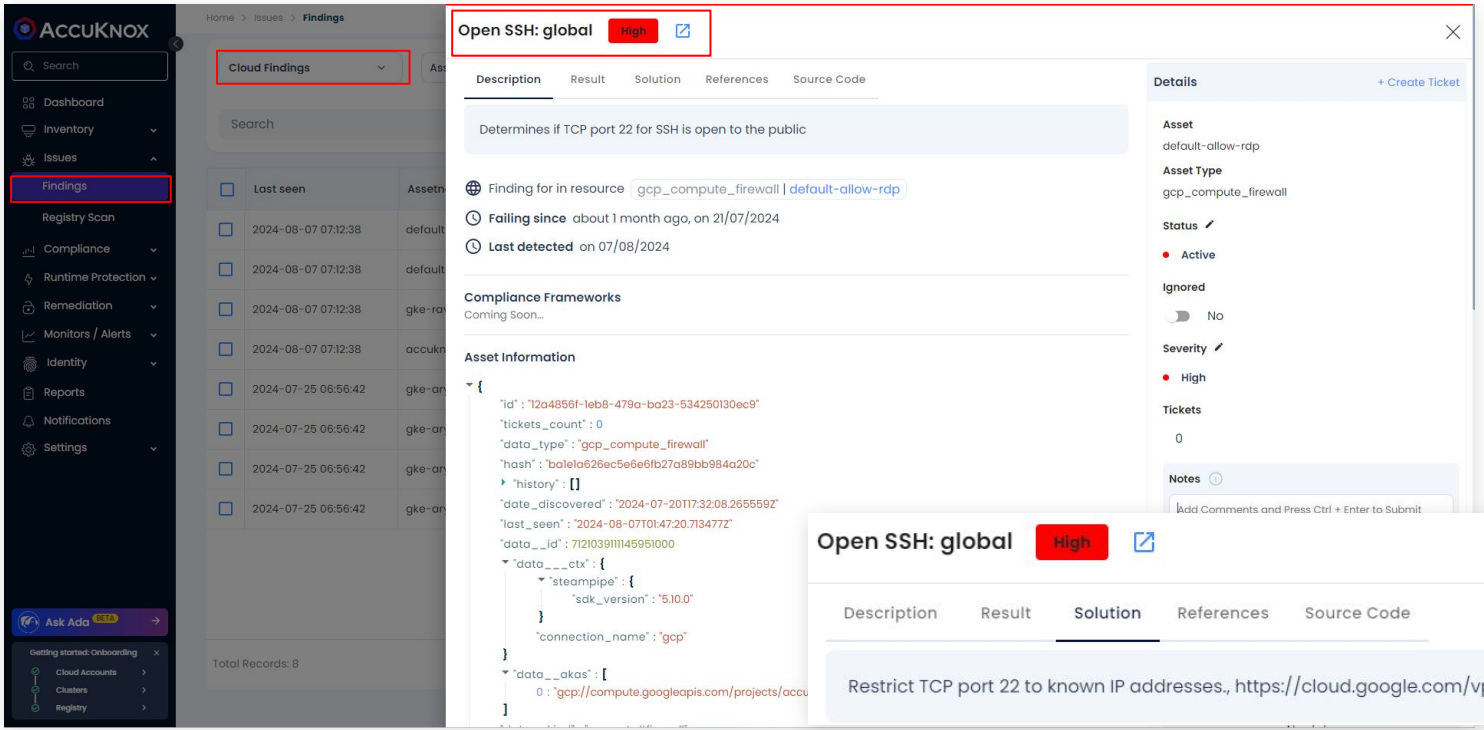


GCP Risk Assessment

Compliance failure and Misconfiguration

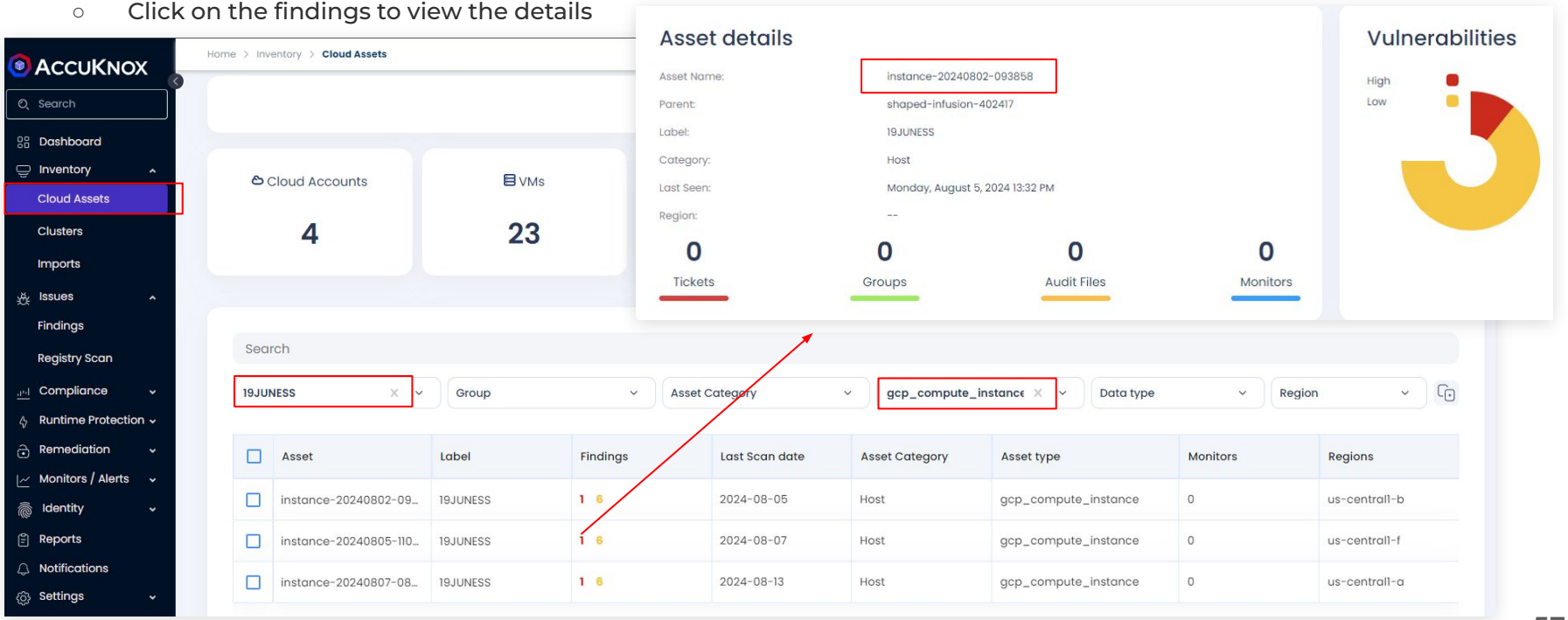
How to identify open SSH port?

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



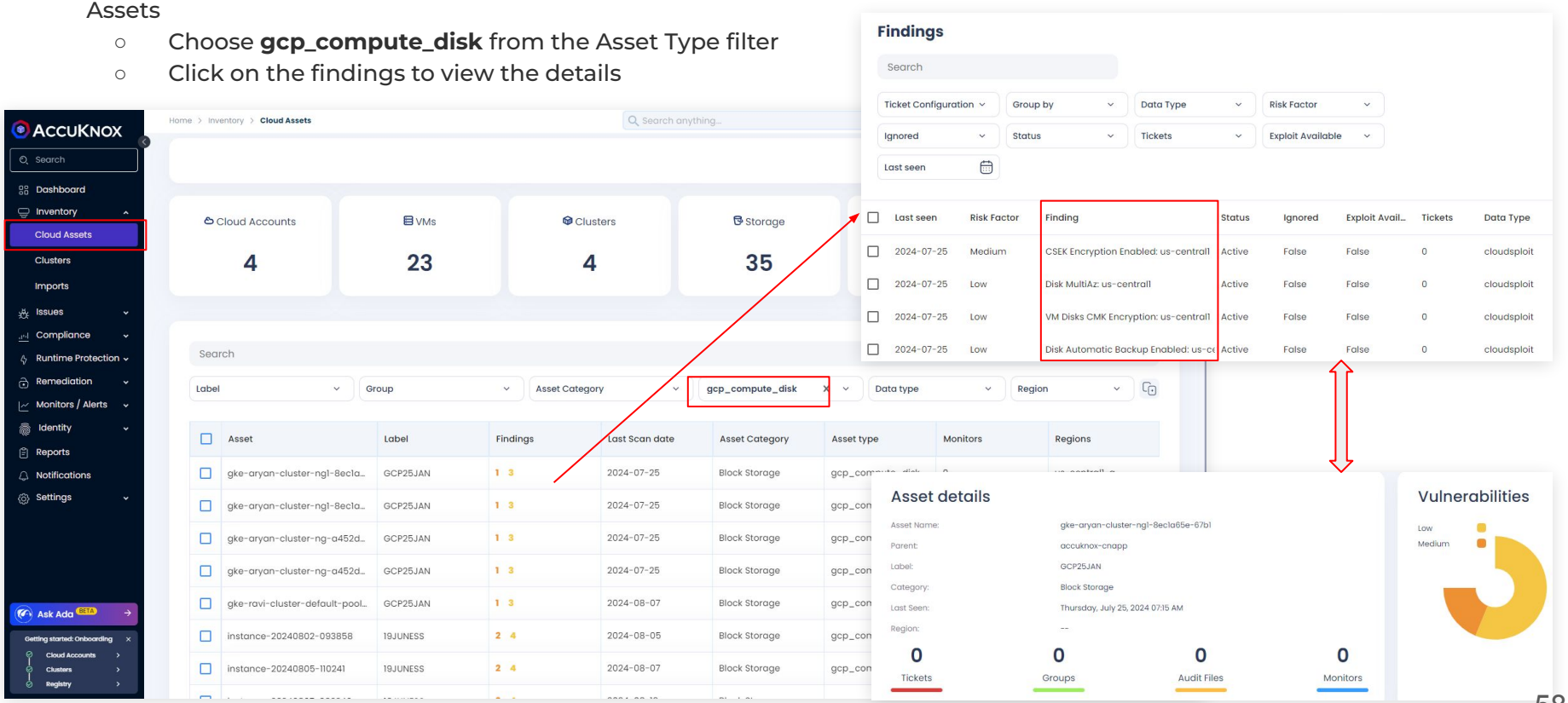
How to identify security issues related to compute instance?

- To identity 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



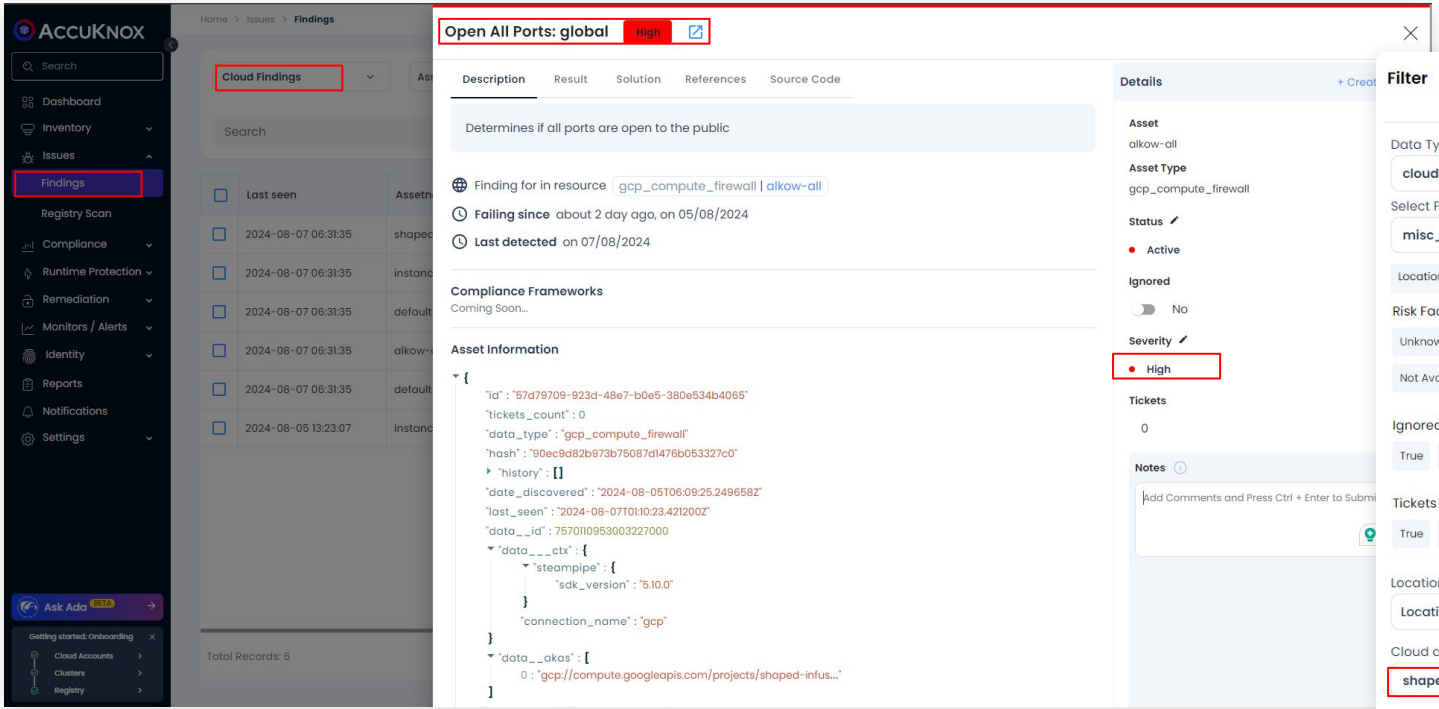
Identify compute disk security issue for all the onboarded GCP account?

- To identity 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



How to identify publicly exposed ports?

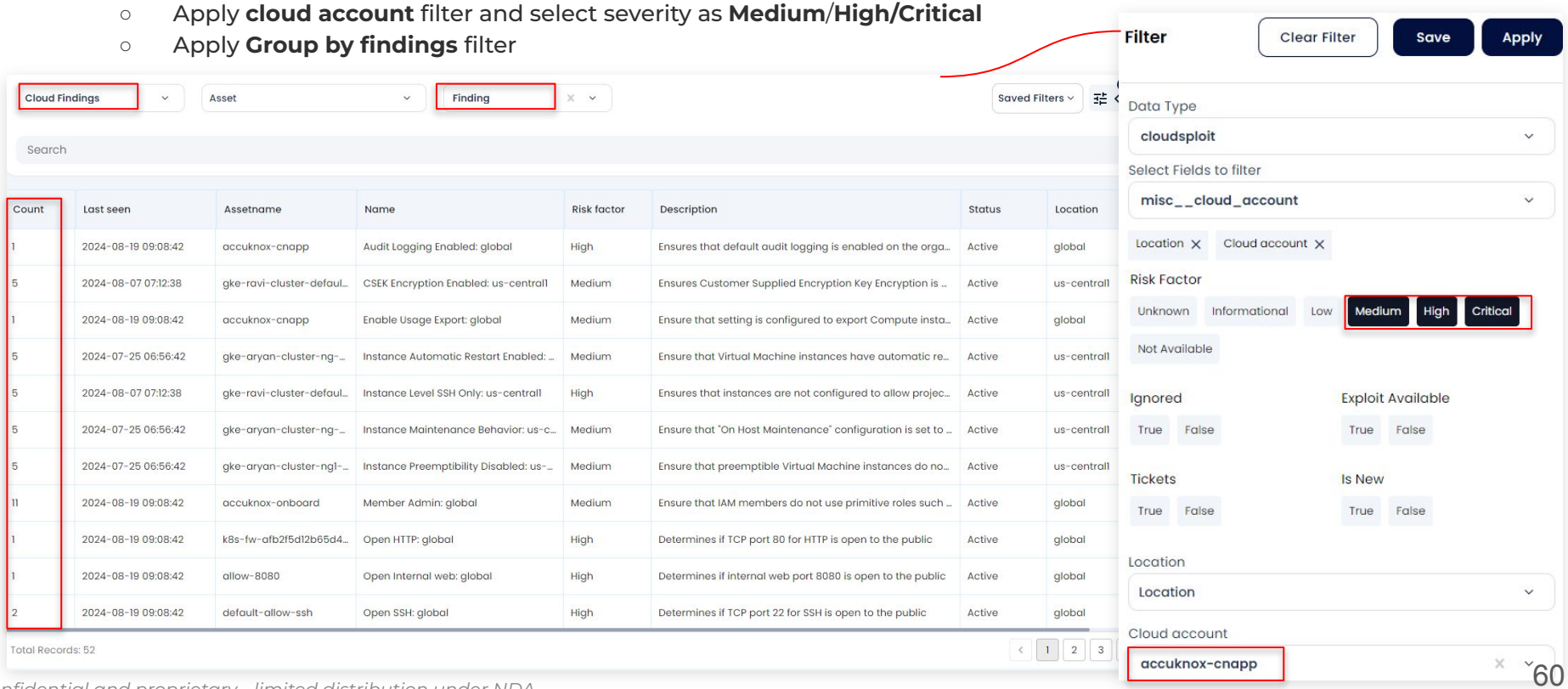
- To identity the if all the ports open to public with the Onboarded Cloud Account, Please navigate to Issues -> Findings
  - Apply **Cloud Findings** in the filter
  - Apply risk factor as “High”
  - Select the filters by cloud account



How to identify unique findings impacting multiple assets?

ACCUKNOX

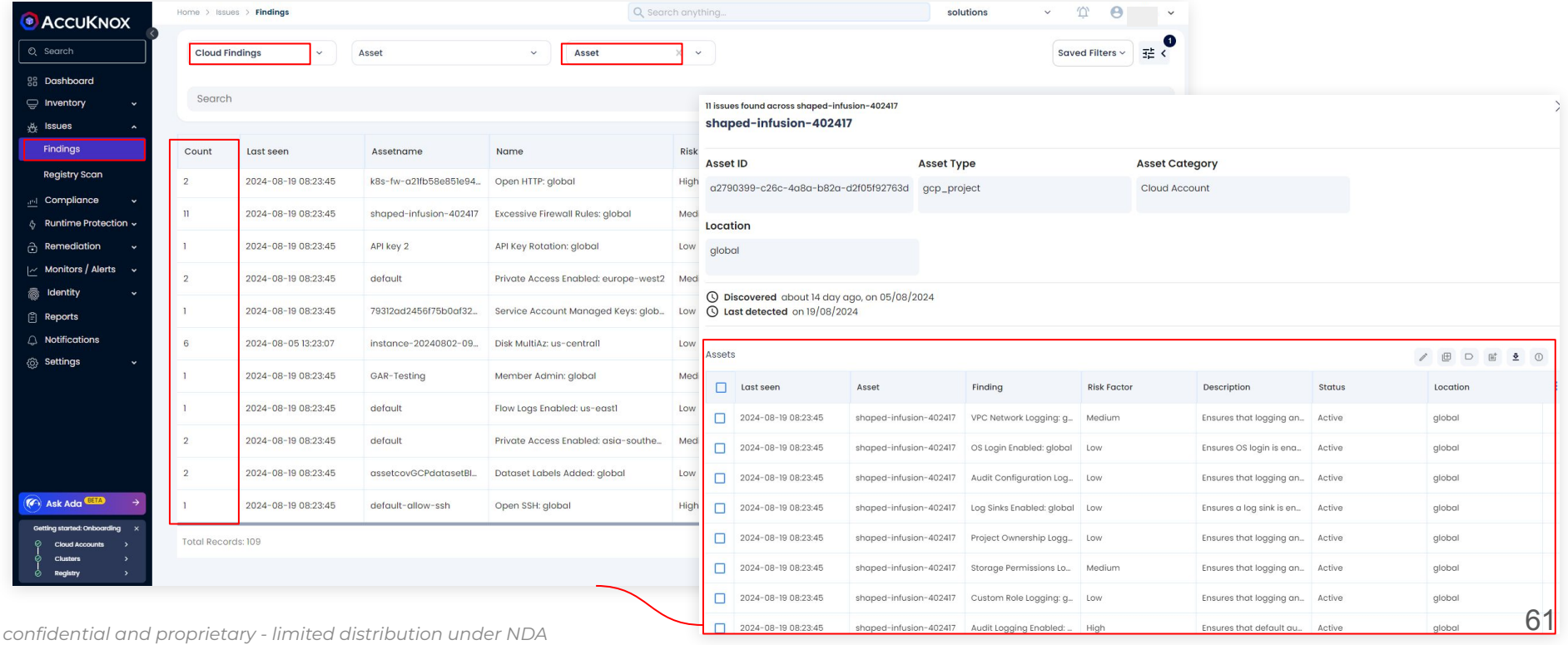
- To identity the unique findings with the Onboarded Cloud Account, Please navigate to Issues -> Findings
  - Apply **Cloud Findings** in the filter
  - Apply **cloud account** filter and select severity as **Medium/High/Critical**
  - Apply **Group by findings** filter



How to identify multiple issues impacting single assets?

ACCUKNOX

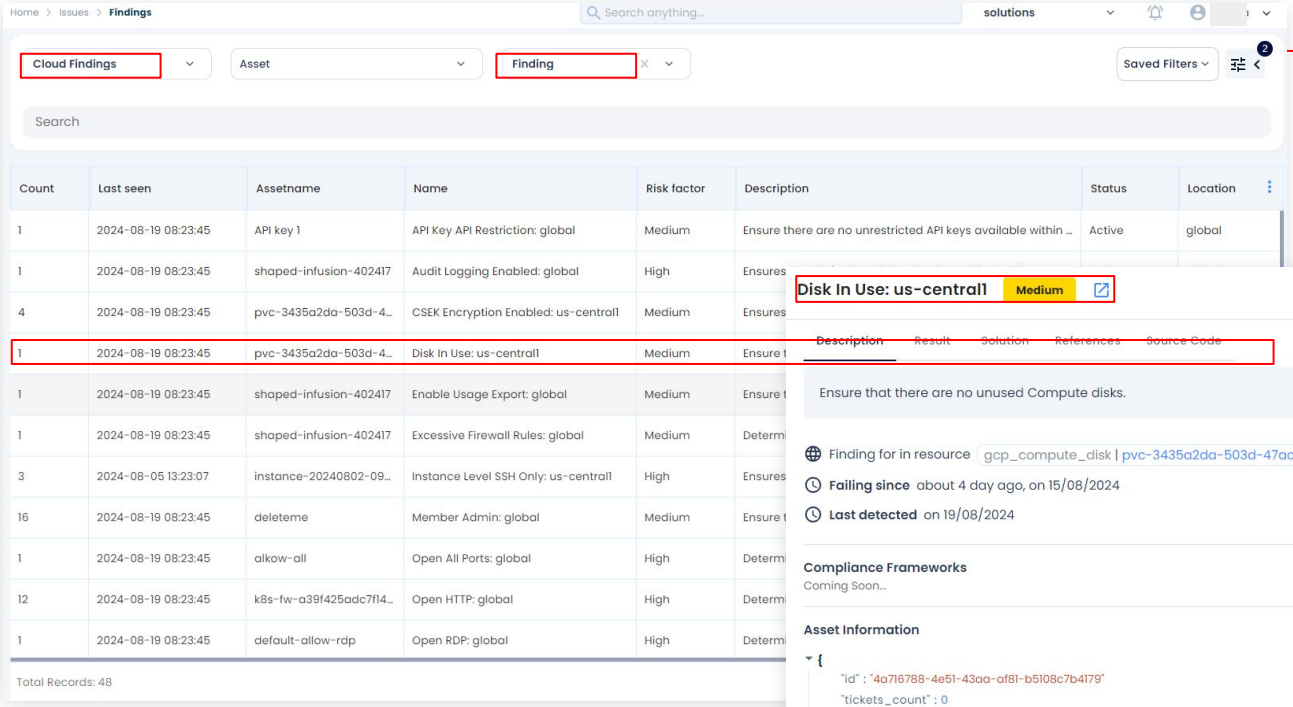
- To identity the unique findings with the Onboarded Cloud Account, Please navigate to Issues -> Findings
  - Apply **Cloud Findings** in the filter
  - Apply **Group by Asset** filter



How to identify unused disk in the onboarded account?

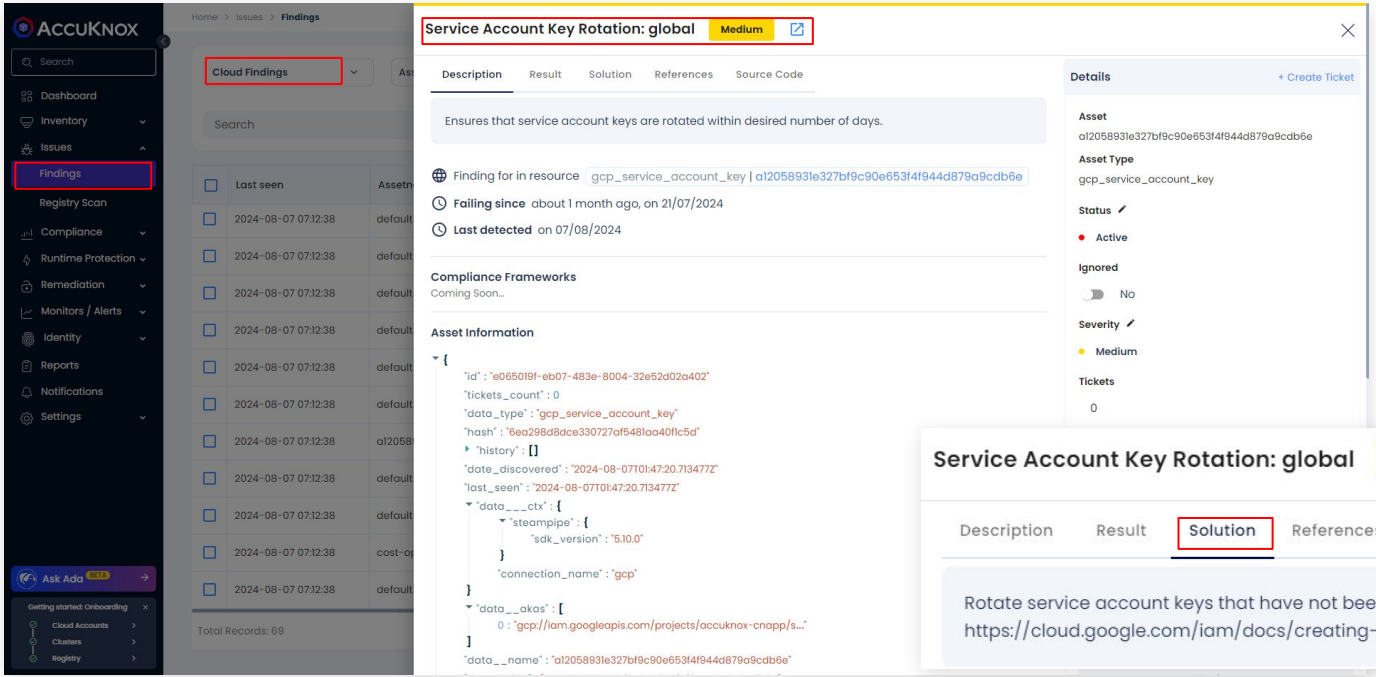
ACCUKNOX

- To identity 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



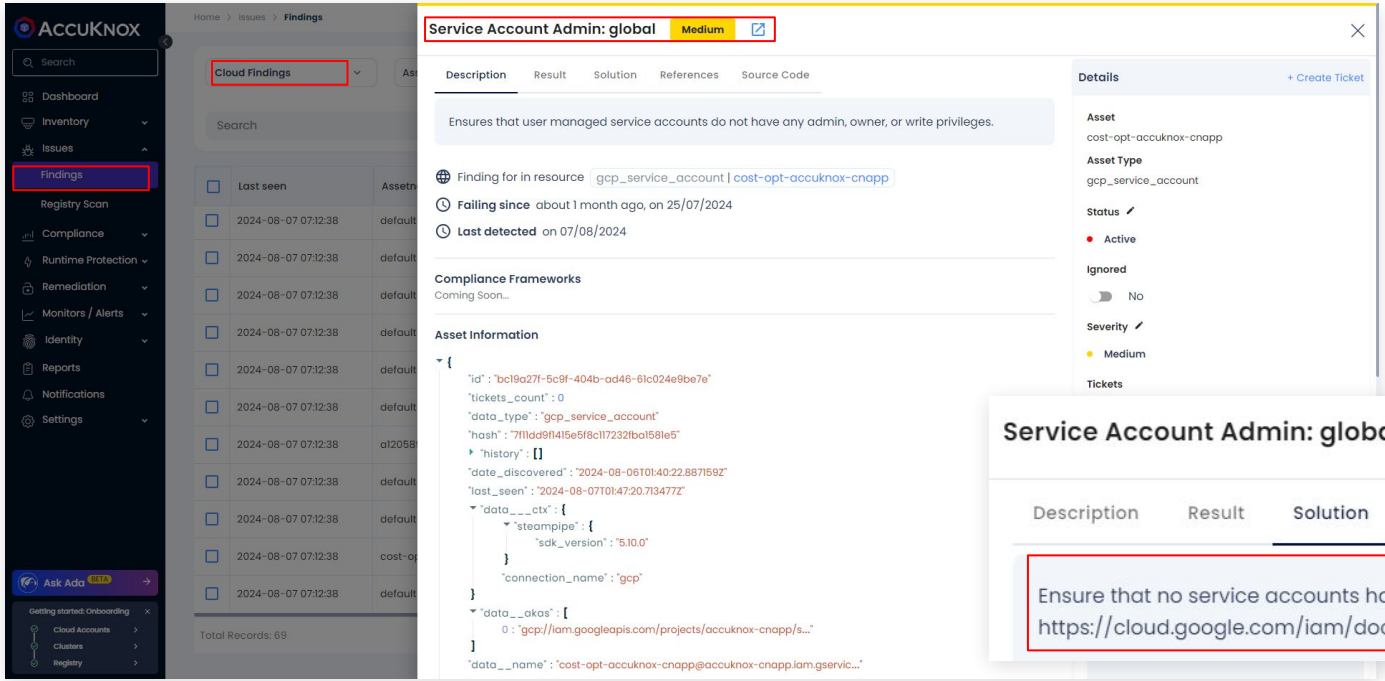
How to identify if service account keys are exposed?

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



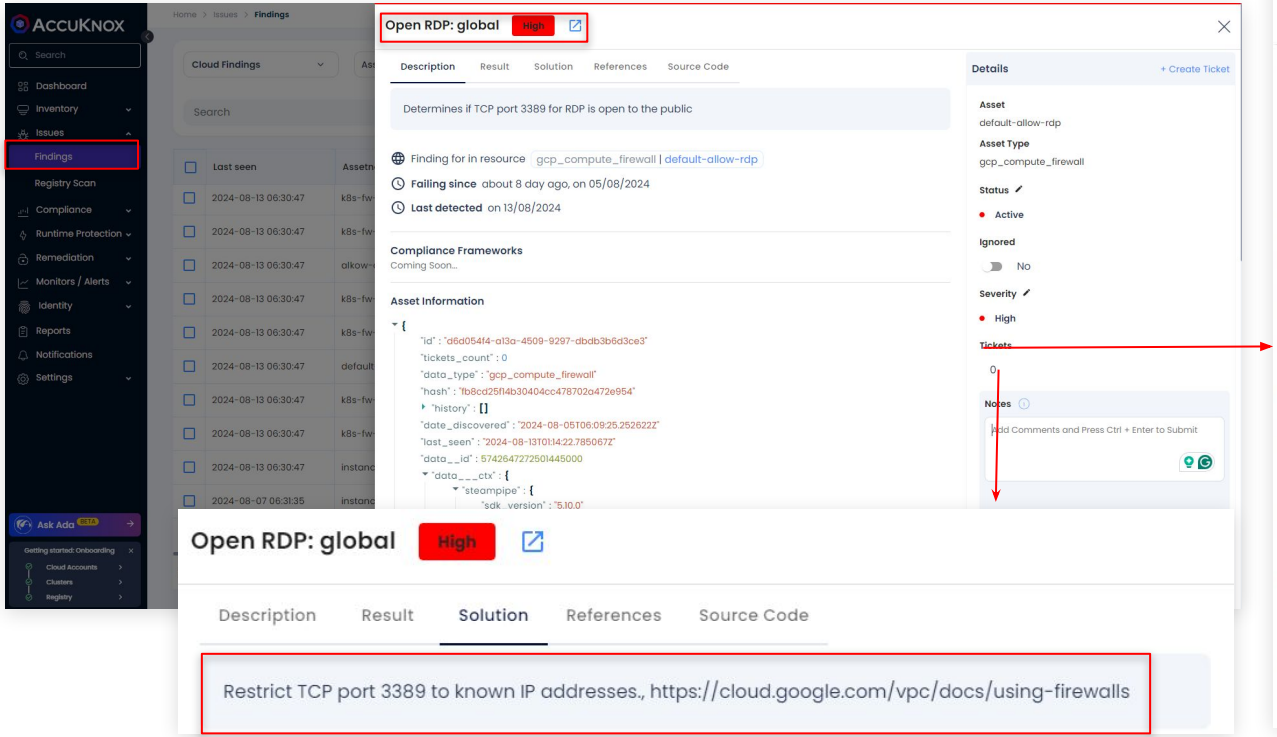
How to identify service accounts with admin privilege?

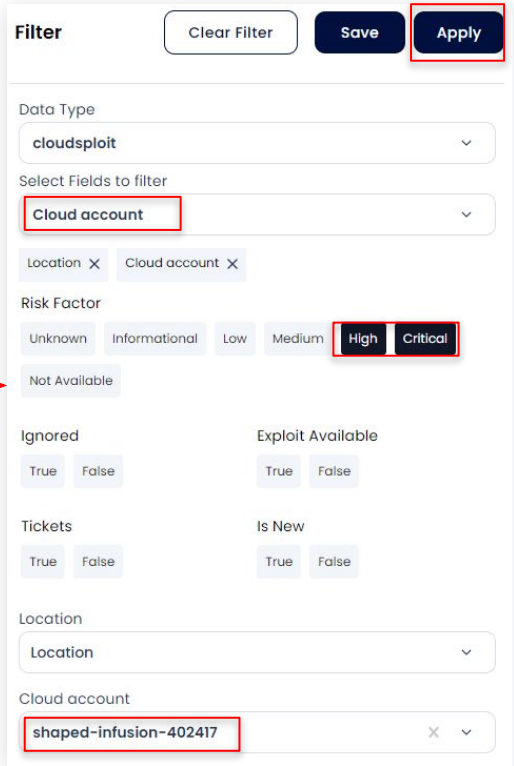
- To identity the if service account keys have admin permissions with the Onboarded Cloud Account, Please navigate to Issues -> Findings
  - Apply **Cloud Findings** in the filter
  - Apply risk factor as “medium”
  - Select the filters by cloud account



How to identify if RDP port exposed to public?

- To identity the 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**

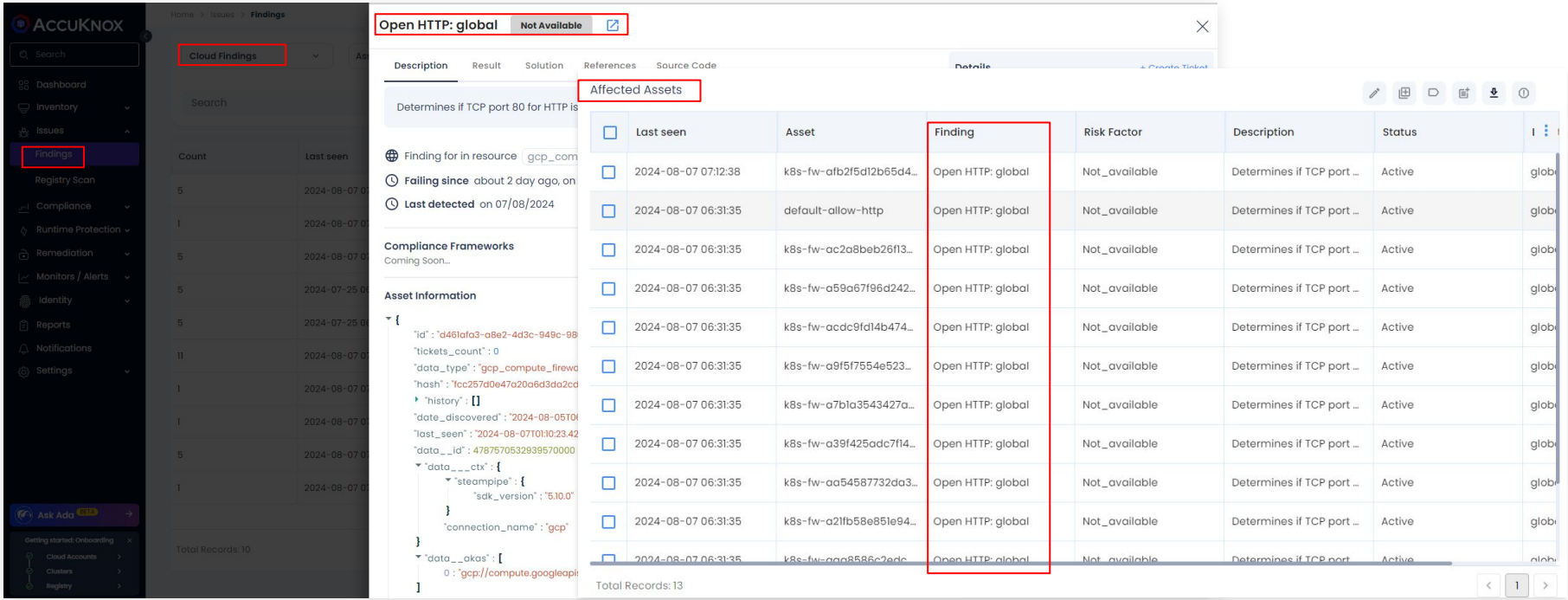




How to identify if Insecure HTTP port are exposed to public?

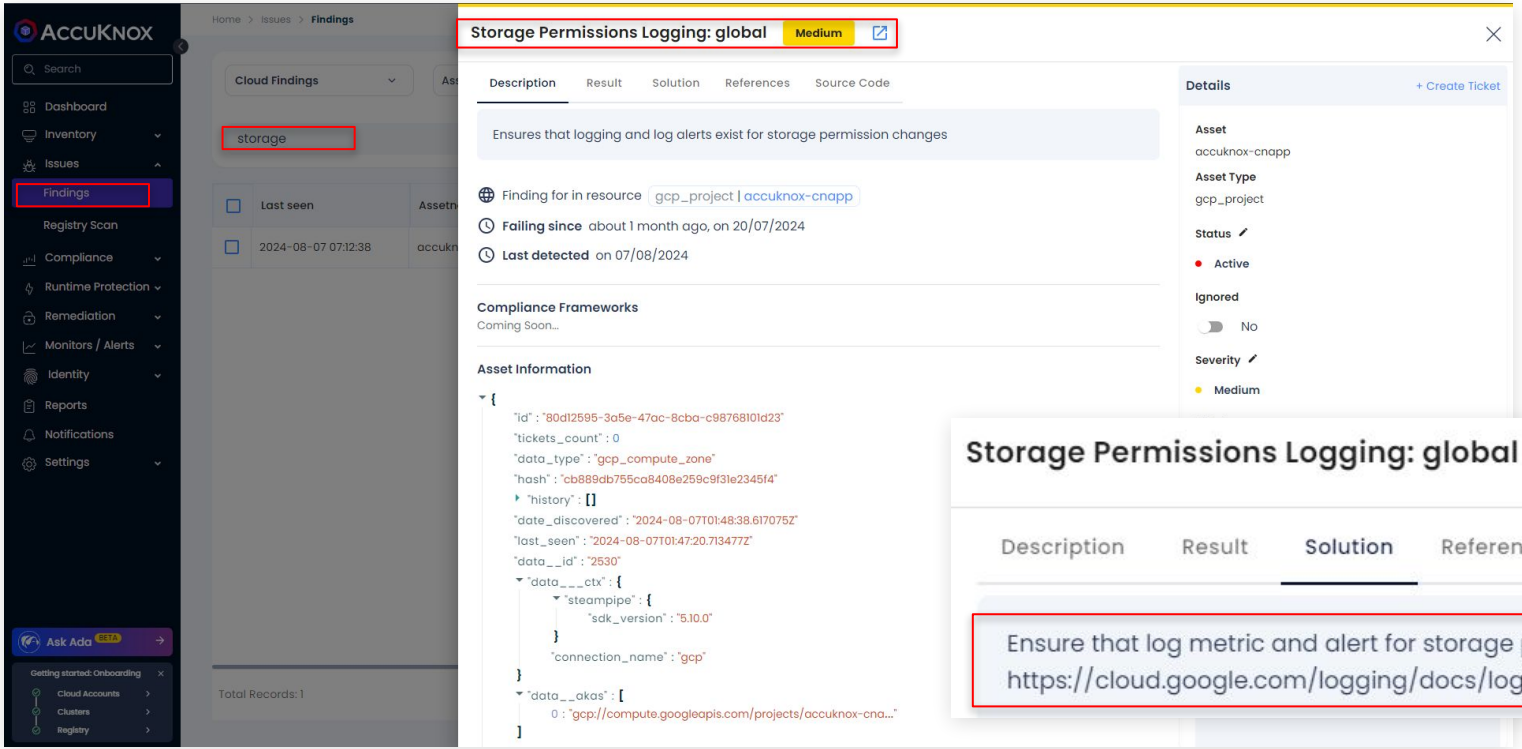
ACCUKNOX

- To identity 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”



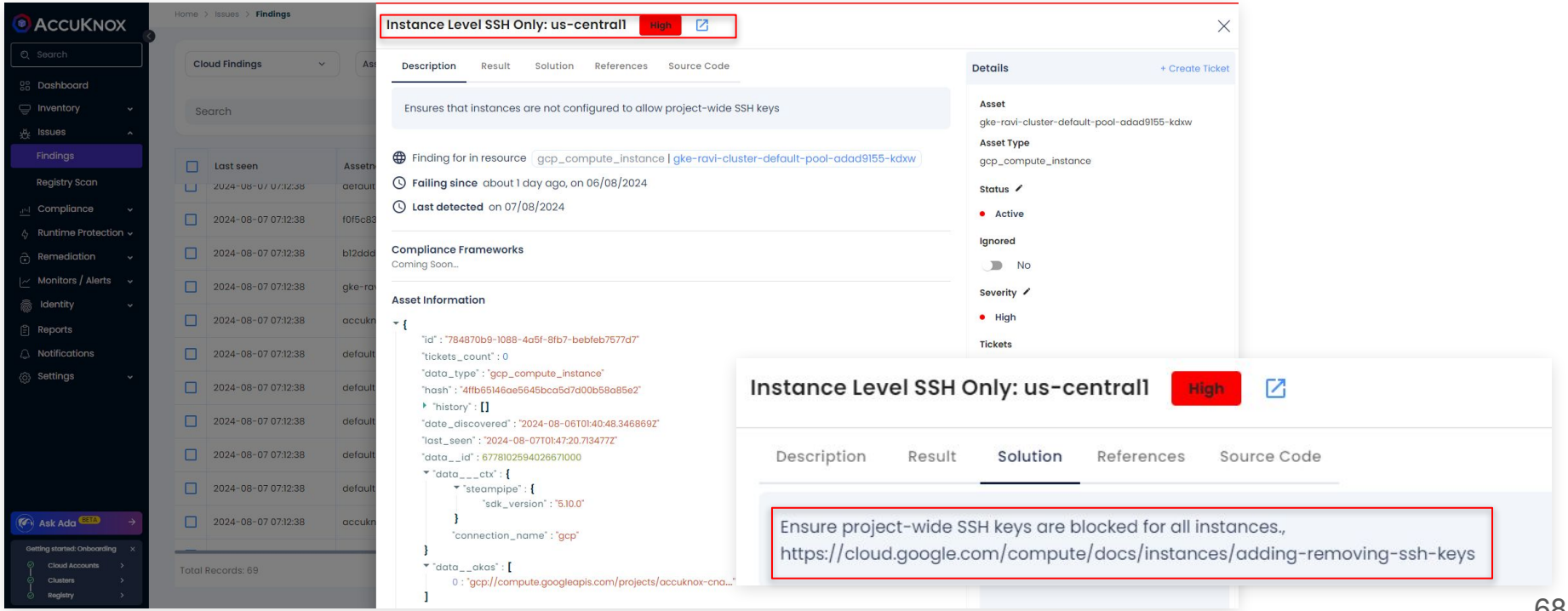
How to identify if logging is enabled for storage?

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



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

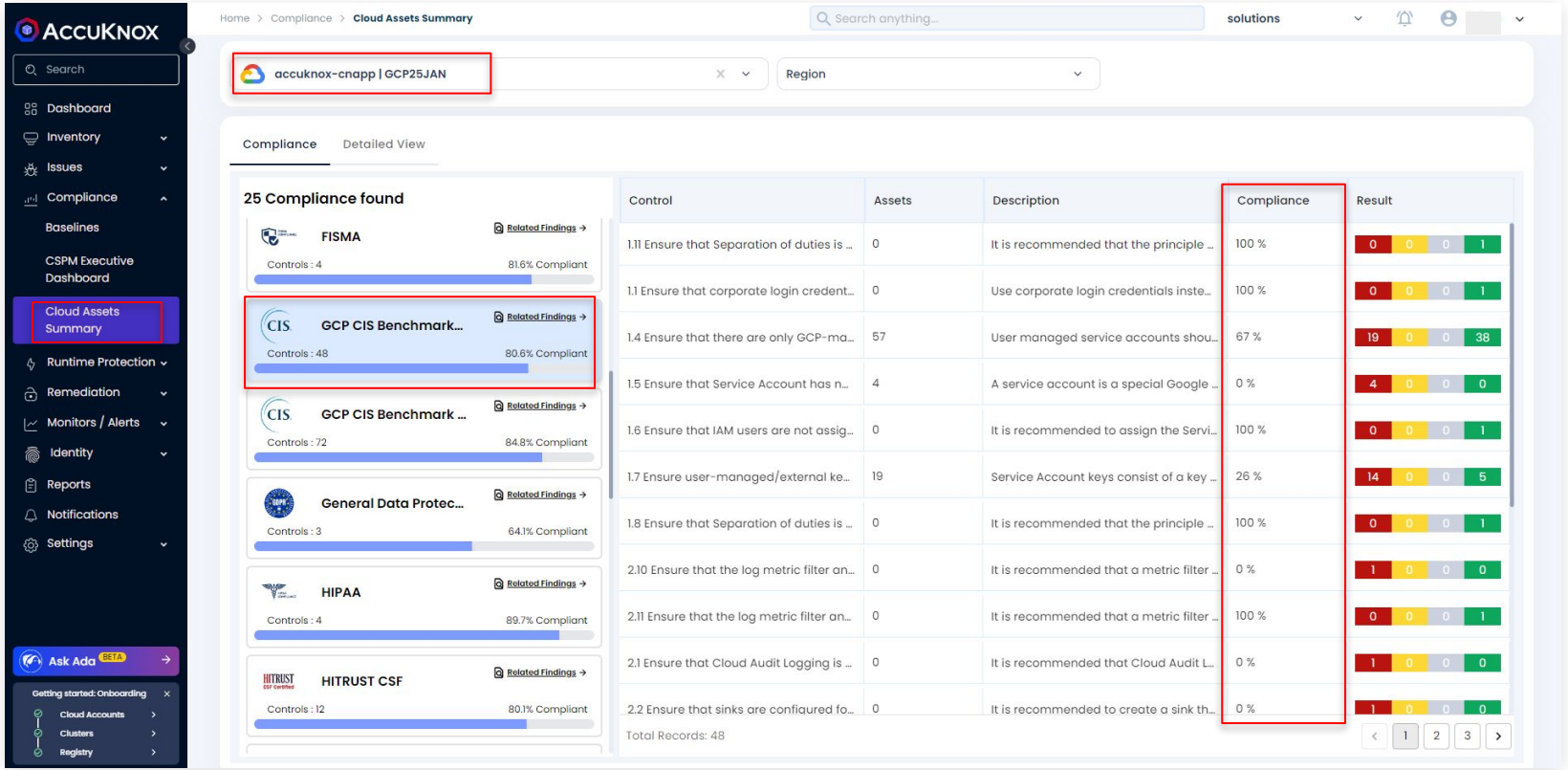
- To identity the if instance are allowed to SSH project-wide with the Onboarded Cloud Account, Please navigate to Issues -> Findings
  - Apply **Cloud Findings** in the filter
  - Search for “SSH”



Compliance failure for CIS Benchmark

ACCUKNOX

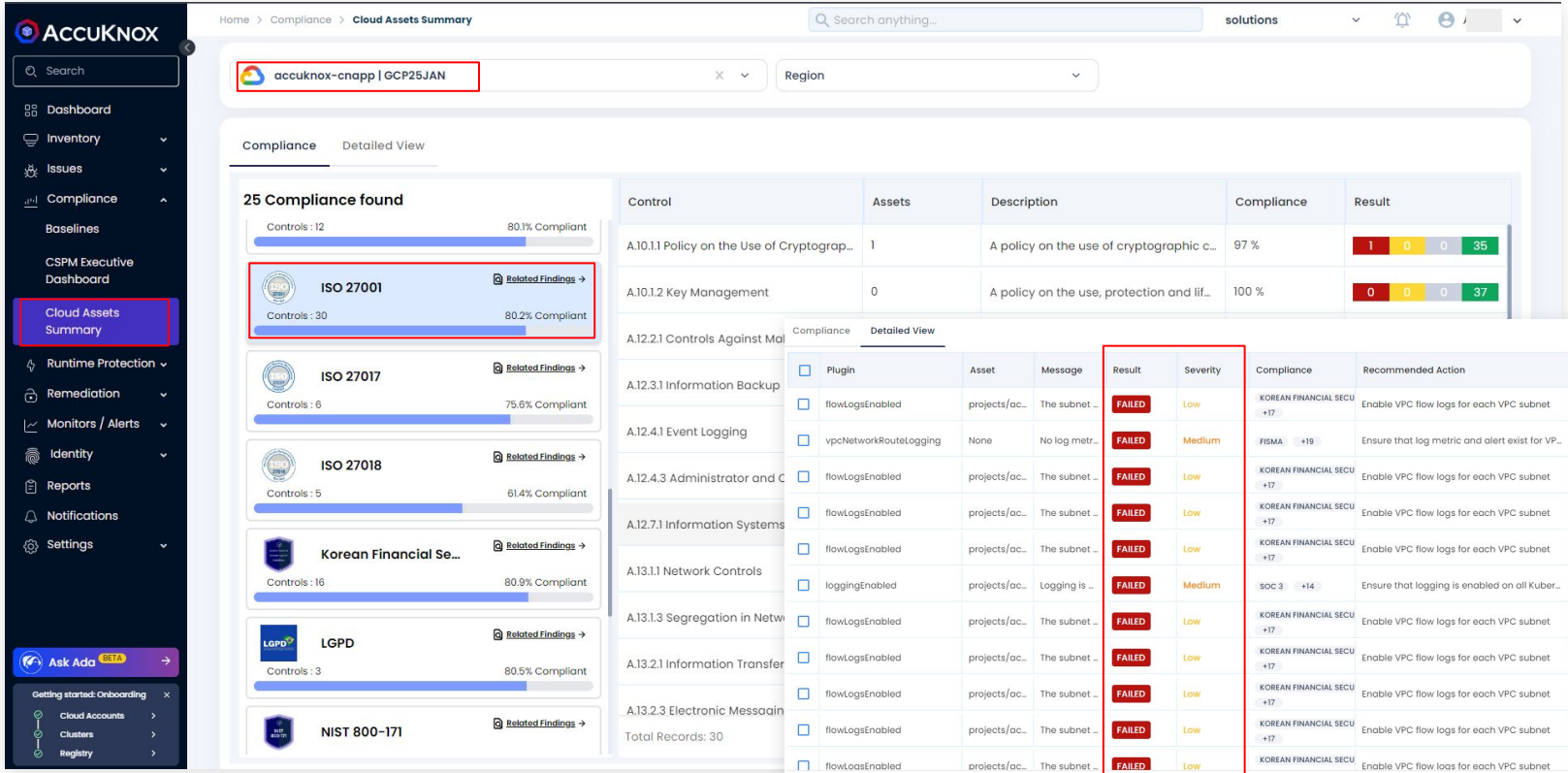
To Identify CIS failed compliance checks > Navigate to Compliance and select Cloud Asset Summary



Compliance failure for ISO 27001 Benchmark

ACCUKNOX

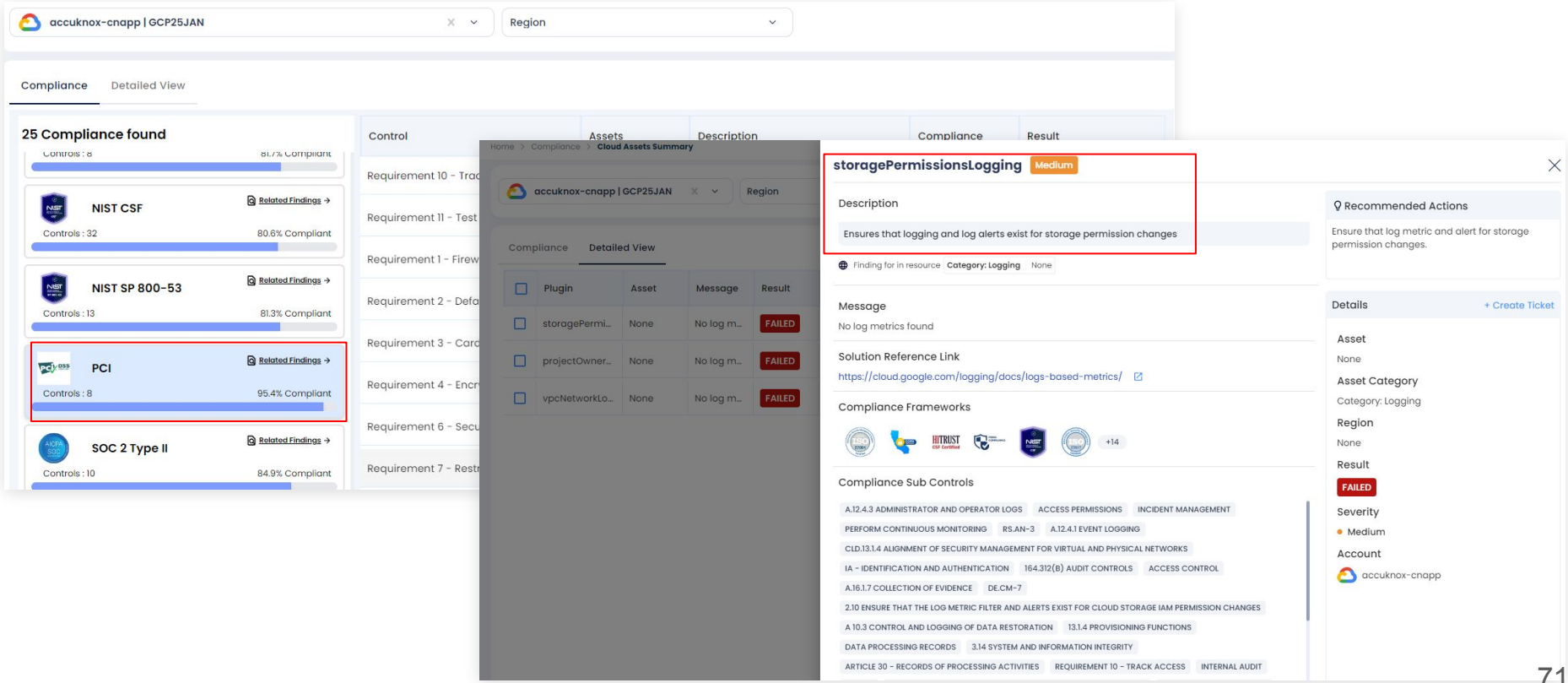
To Identify ISO 27001 failed compliance checks > Navigate to Compliance and select Cloud Asset Summary



Compliance failure for PCI DSS Benchmark

ACCUKNOX

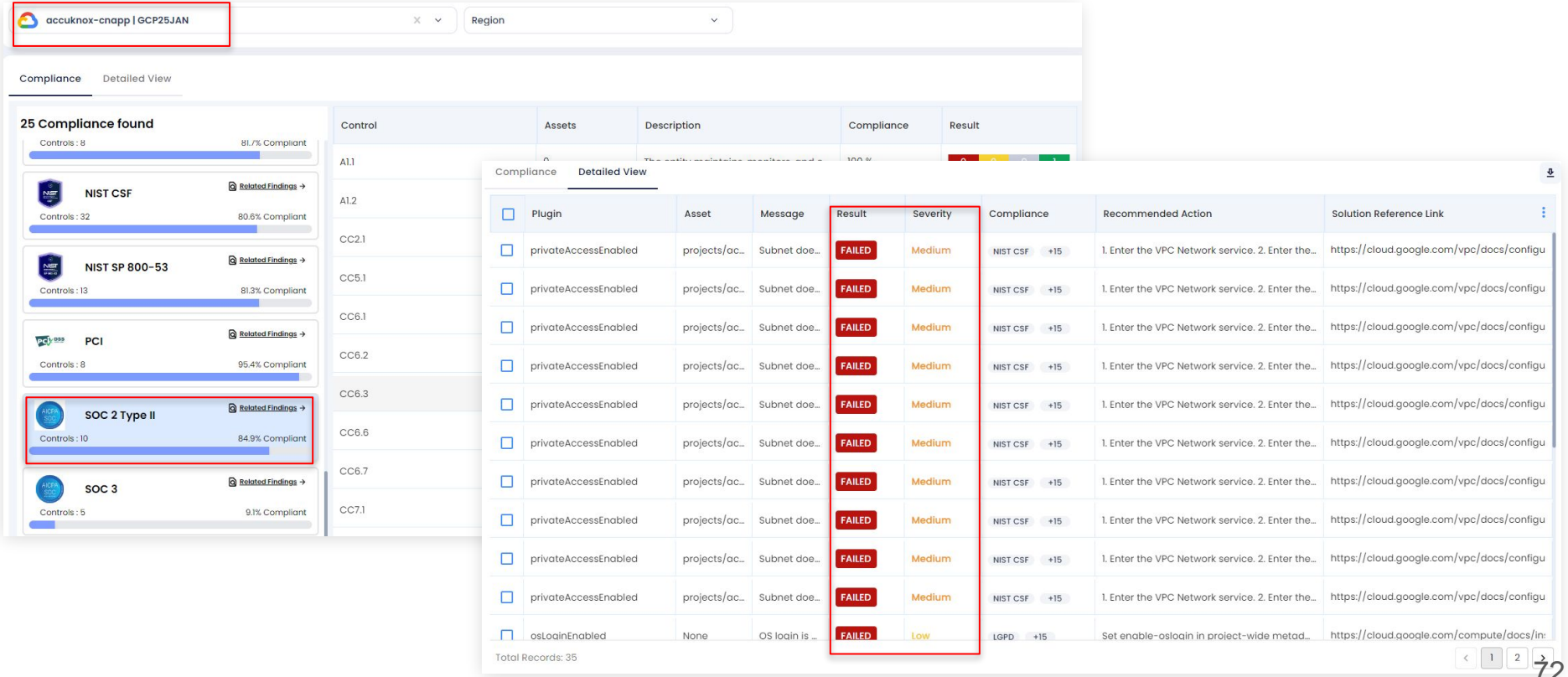
To Identify PCI DSS failed compliance checks > Navigate to Compliance and select Cloud Asset Summary



Compliance failure for SOC 2 Benchmark

ACCUKNOX

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

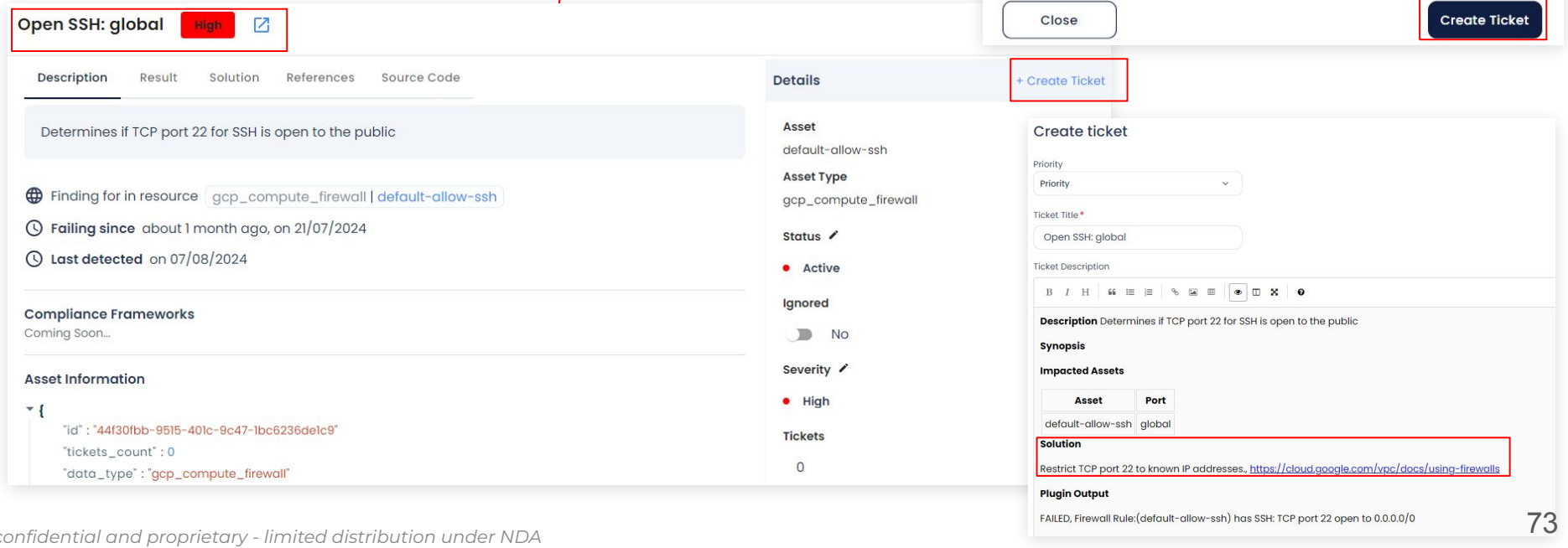


Assistive Remediation For GCP Risks

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

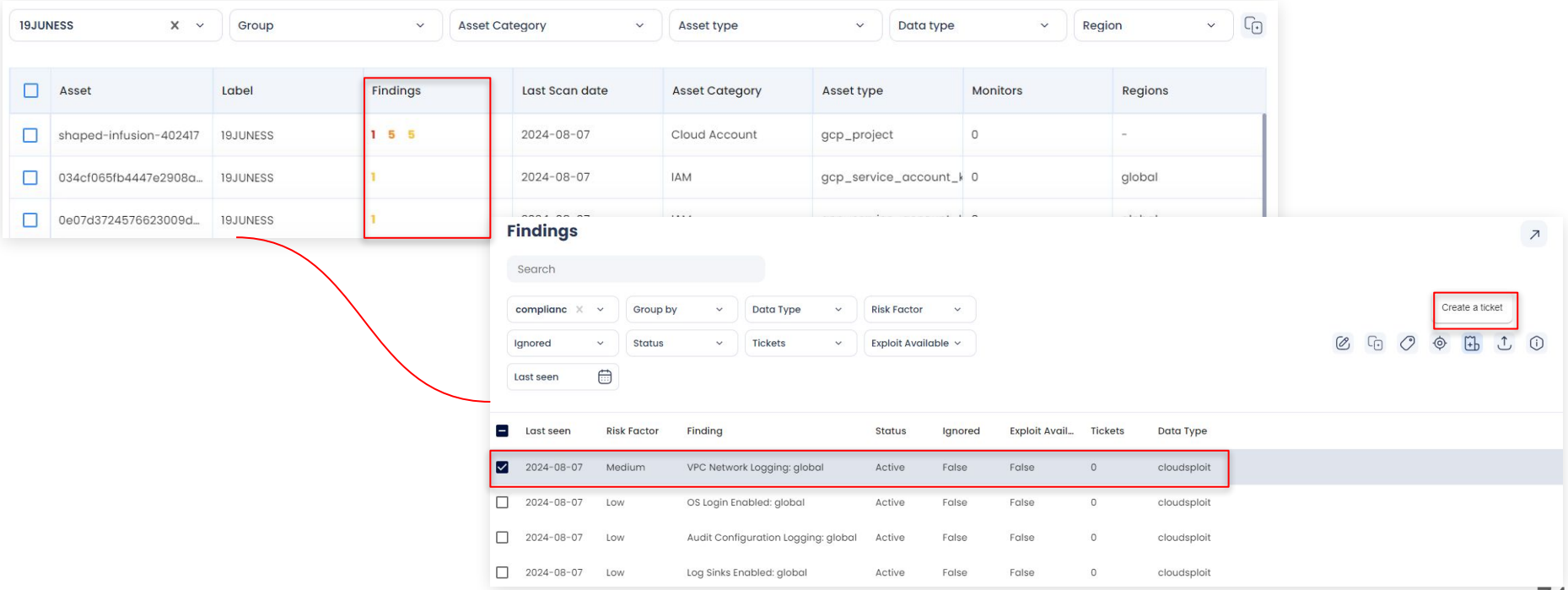


Assistive Remediation For GCP Risks

AccuKnox offers solution reference links to assist with the remediation

To Remediate the findings (Approach 2)

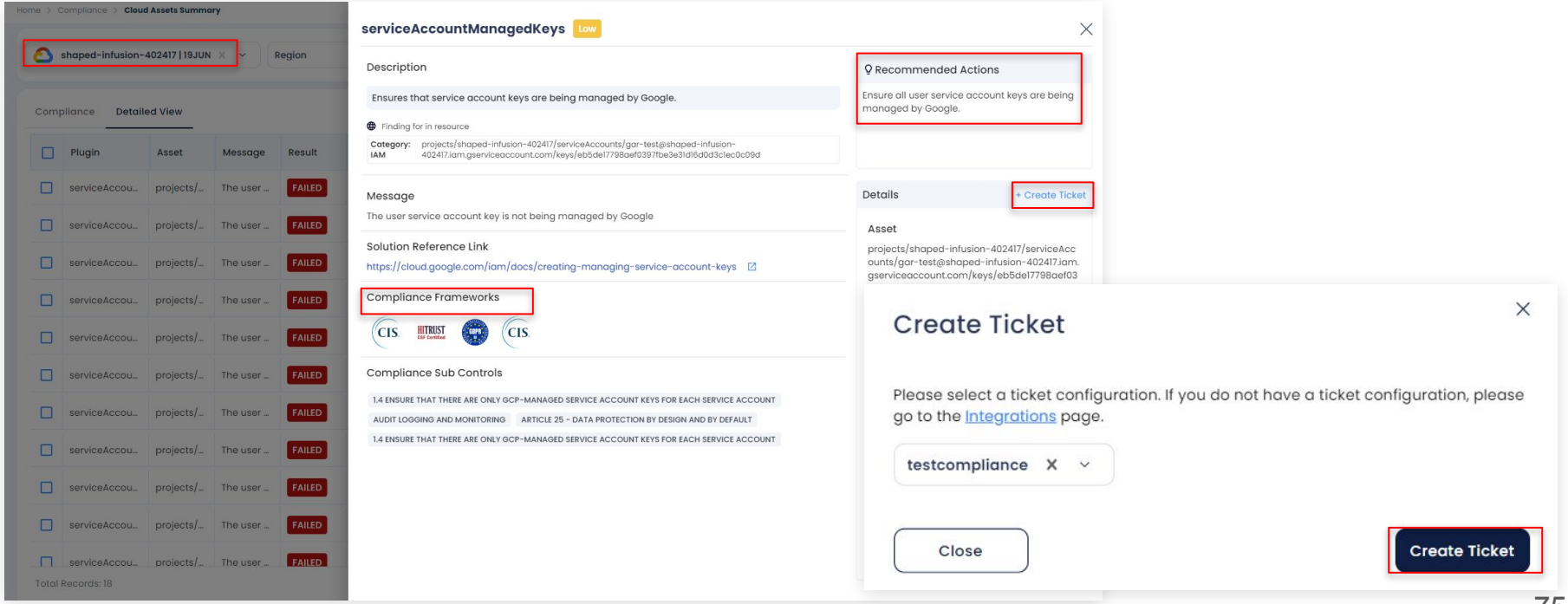
- Navigate to Inventory > Cloud Assets
- Select the finding and create a ticket for it



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

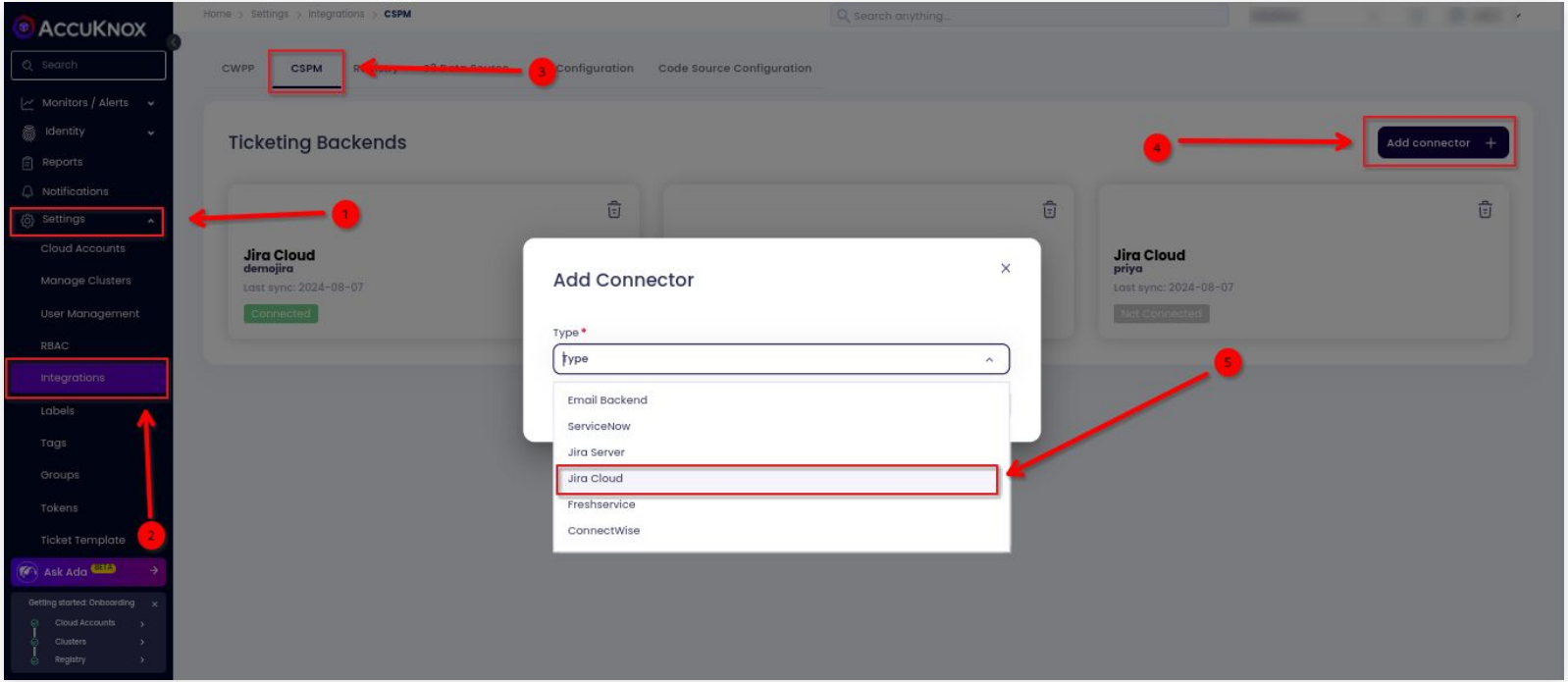


Integrations

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

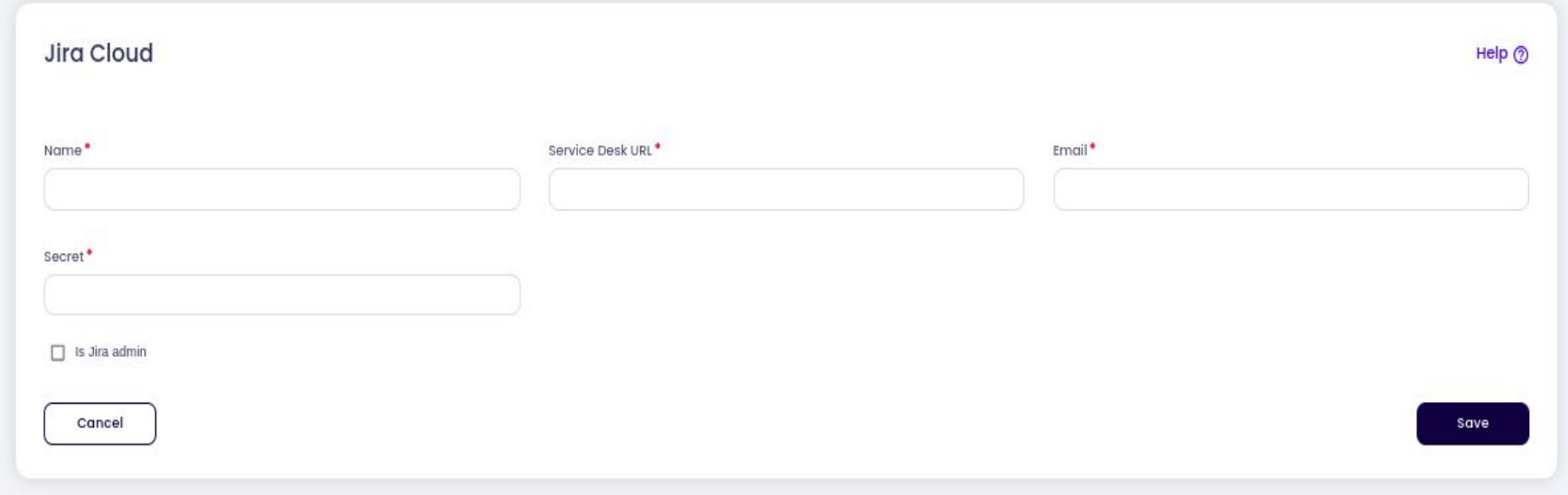
1. Choose Jira Cloud as the connector and Click Next.



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

ACCUKNOX

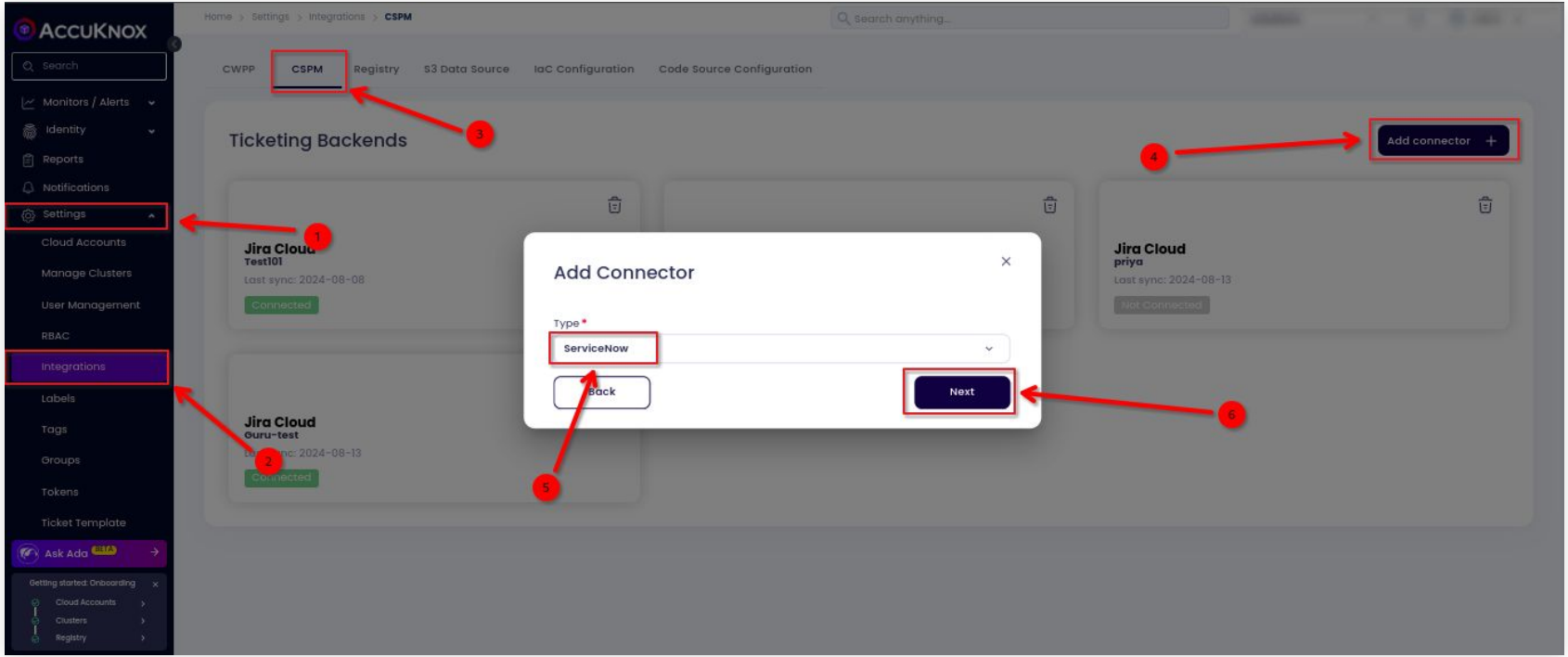
- Fill all the necessary fields and test the connection before saving the integration.
  a. **Integration Name:** Enter the name for the integration. You can set any name. e.g.,Test JIRA
  b. **Service Desk URL:** Enter the site name of your organisation. e.g., https://jiratest.atlassian.net/
  c. **User 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., kRVxxxxxxxxxxxx39.
- For more detailed steps refer to the Accuknox help documentation.



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

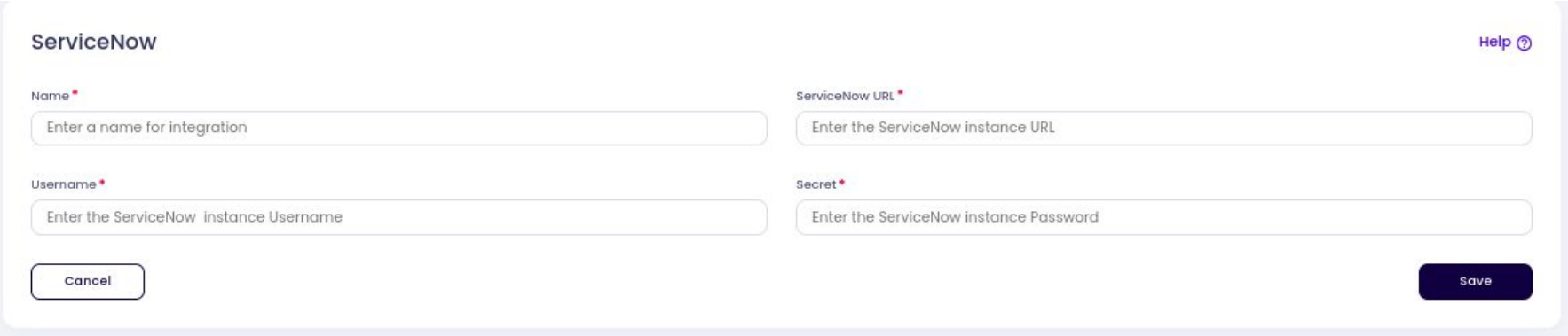
After getting the findings data populated If users want to create tickets for the findings. Then Navigate to Settings->Integrations-> CSPM > Add connector

- Choose ServiceNow as the connector and Click Next.



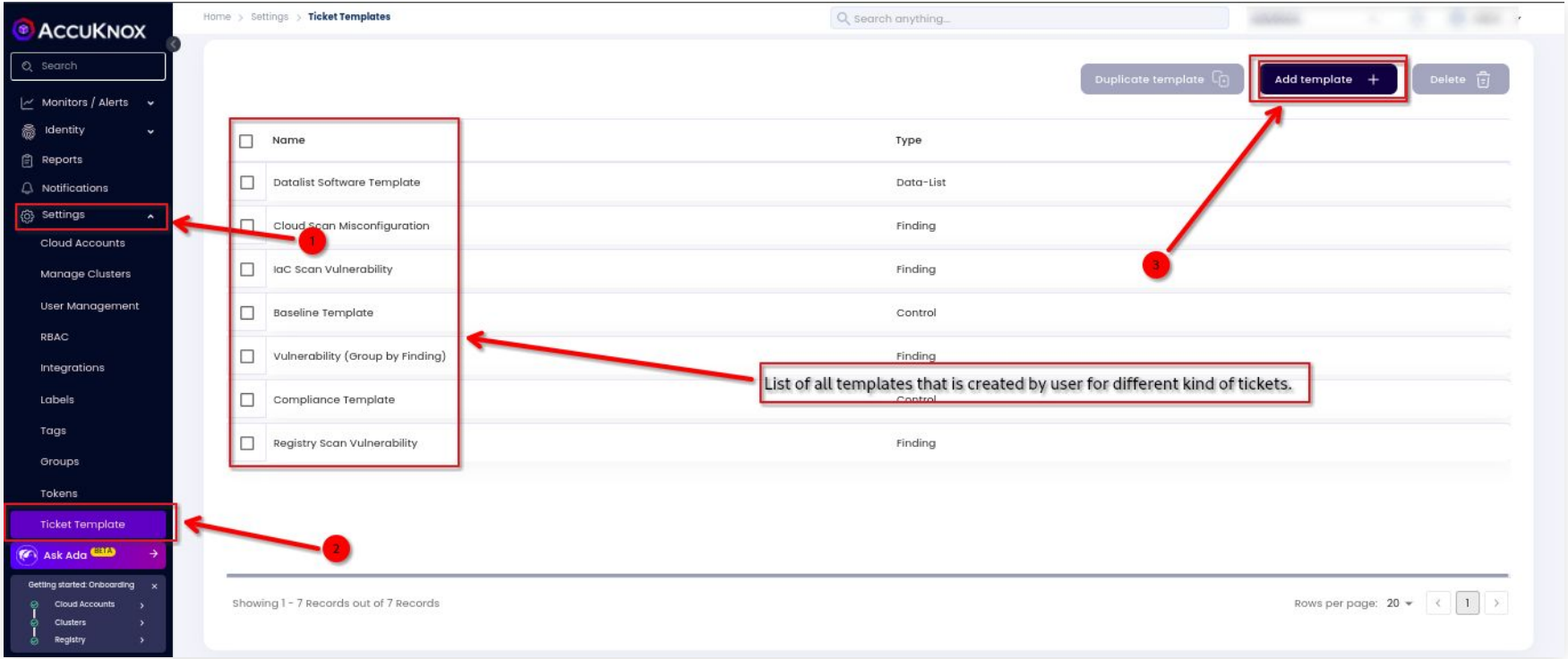
How to do CSPM ticketing Integration with ServiceNow? [2]

- 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.



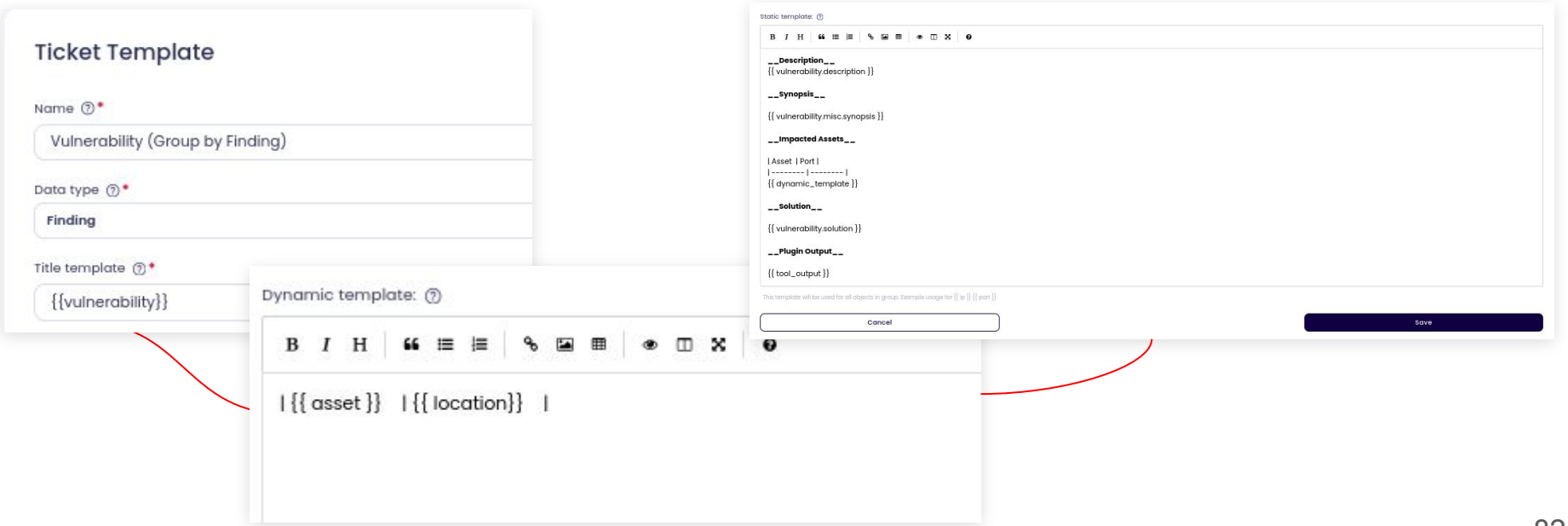
How to create default template for ticket creation? [1]

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



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

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

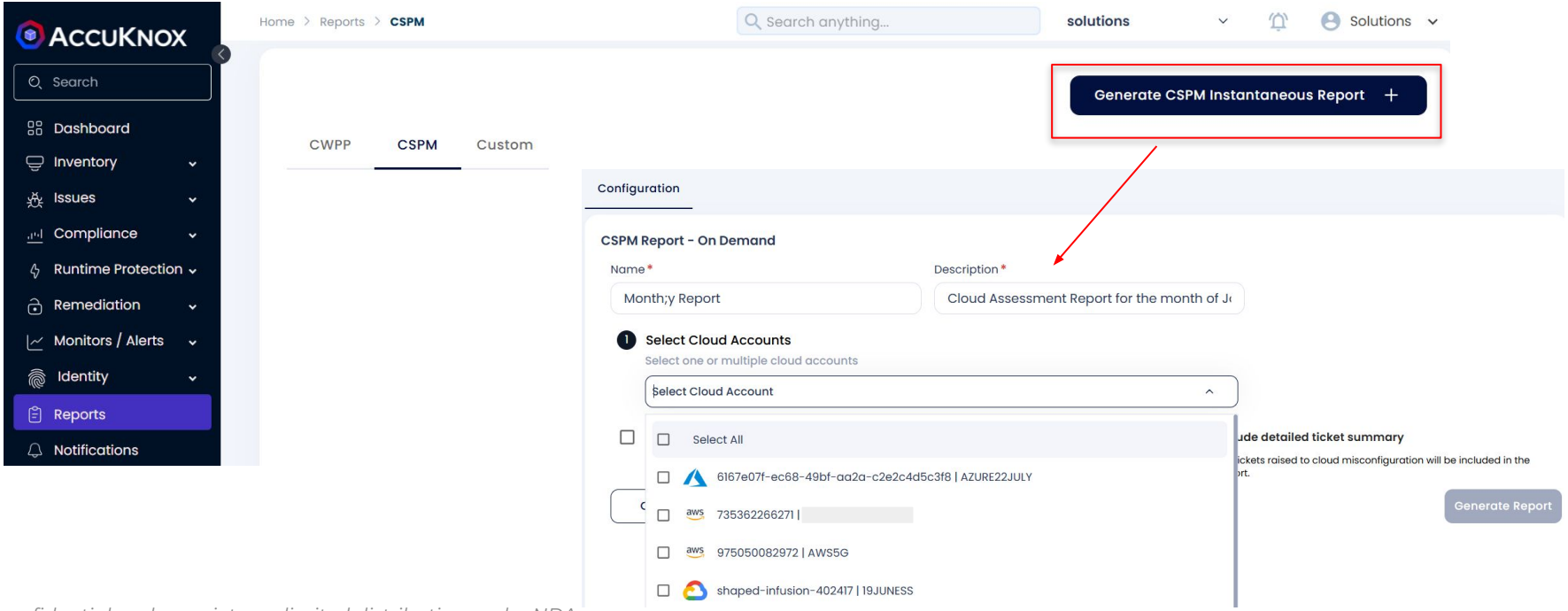


Reporting

Report Generation

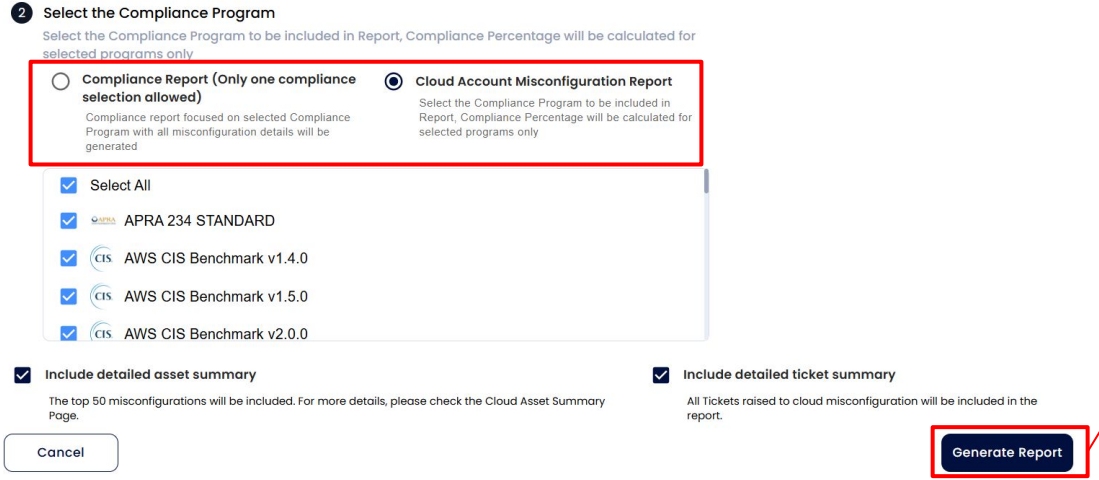
After getting the findings data populated, a report can be generated for all the misconfigurations or a specific compliance across cloud accounts

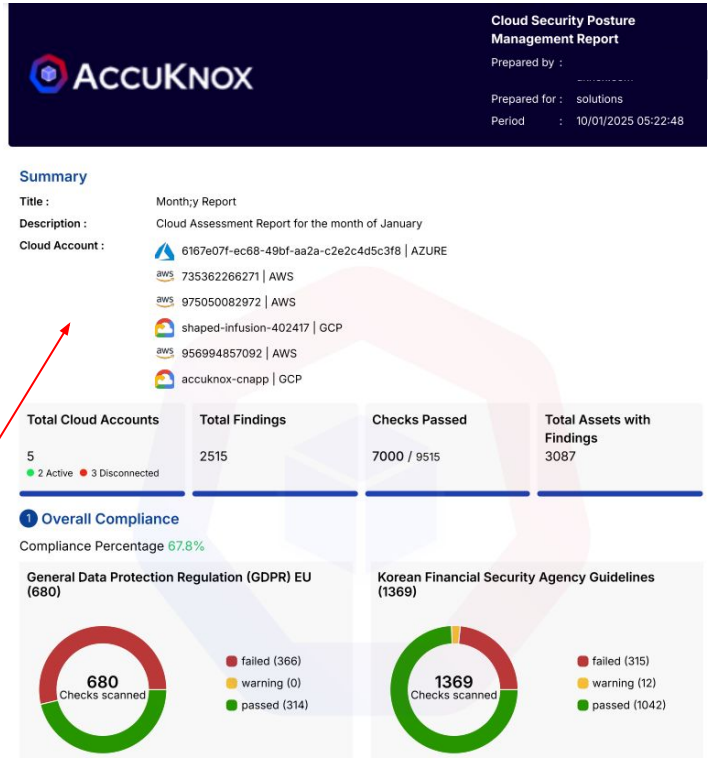
- Navigate to Reports -> CSPM & Select Generate CSPM Instantaneous Report
- Specify, Name, Description and Select the Cloud accounts to report on



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**





CNAPP

(Cloud Native Application Protection Platform)

CNAPP Dashboard with onboarded Cloud, Clusters & Containers