AccuKnox

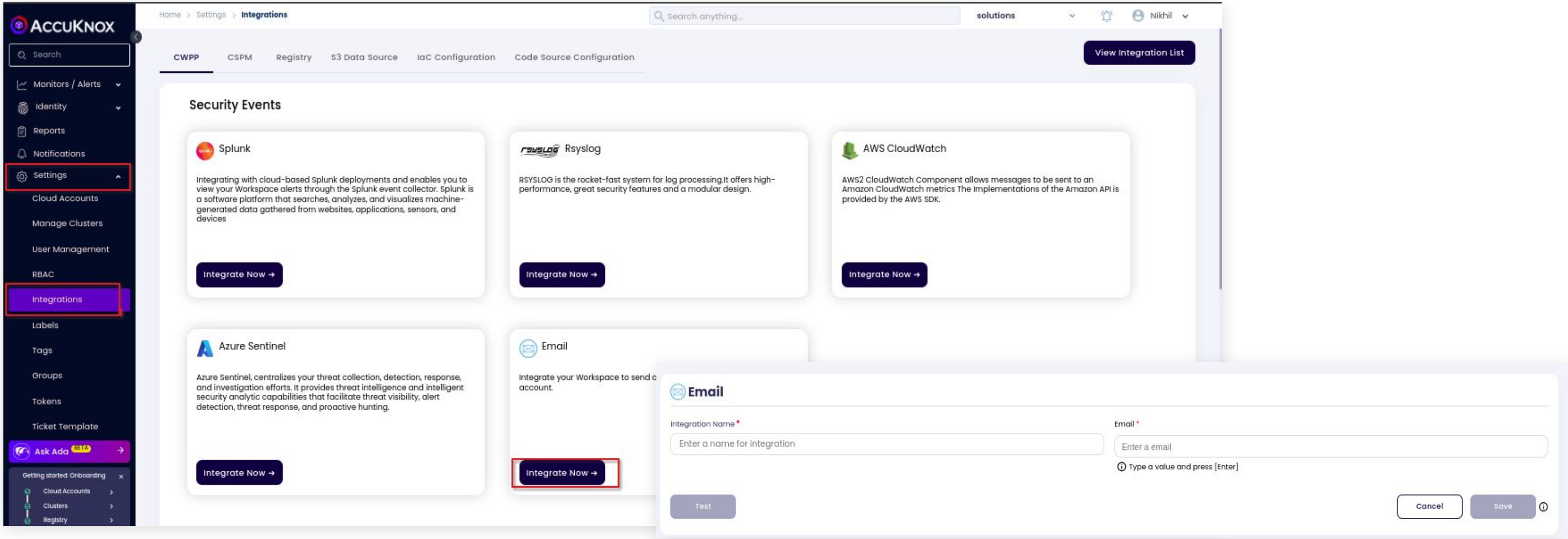
Integration Playbook

Table of Contents

- Email Alerts
- Logs/Telemetry forwarding
  - Splunk
  - Azure Sentinel
- Setting Up Triggers for Forwarding Logs/Alerts
- Ticketing
  - Jira
  - ServiceNow
- Set Up Ticketing
  - Custom Ticket Templates
  - Ticket Configuration Options
- Ticket Creation & Tracking

How to set up Email Alerts for CWPP Security Findings?

1. Go to Settings > Integrations > CWPP > Email (Integrate Now).
2. Fill in the required fields and test the connection before saving.
   a. **Integration Name:** Choose a name.
   b. **User Email:** Enter your email address and press Enter. Multiple emails can be added.



Splunk: Integrating with cloud-based Splunk deployments and enables you to view your Workspace alerts through the Splunk event collector. Splunk is a software platform that searches, analyzes, and visualizes machine-generated data gathered from websites, applications, sensors, and devices

Rsyslog: RSYSLOG is the rocket-fast system for log processing.It offers high-performance, great security features and a modular design.

AWS CloudWatch: AWS2 CloudWatch Component allows messages to be sent to an Amazon CloudWatch metrics The implementations of the Amazon API is provided by the AWS SDK.

Azure Sentinel: Azure Sentinel, centralizes your threat collection, detection, response, and investigation efforts. It provides threat intelligence and intelligent security analytic capabilities that facilitate threat visibility, alert detection, threat response, and proactive hunting.

Email: Integrate your Workspace to send a account.

Email

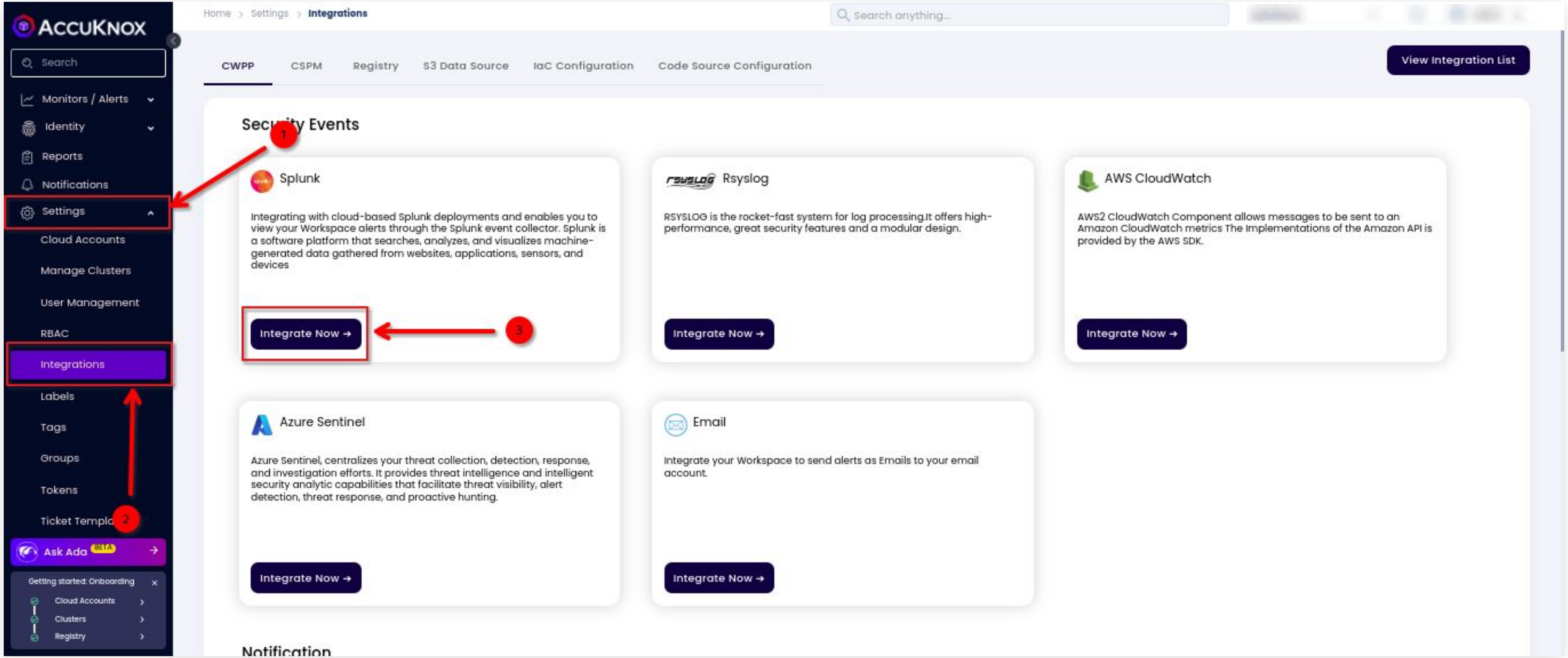
Integration Name *: Enter a name for integration

Email *: Enter a email

Type a value and press [Enter]

How to Set Up Splunk Integration? [1]

After onboarding Cluster and Applying the policies if you want to forward the logs to Splunk. Then Navigate to Settings->Integrations-> Splunk (Integrate Now)



Splunk: Integrating with cloud-based Splunk deployments and enables you to view your Workspace alerts through the Splunk event collector. Splunk is a software platform that searches, analyzes, and visualizes machine-generated data gathered from websites, applications, sensors, and devices

Rsyslog: RSYSLOG is the rocket-fast system for log processing.It offers high-performance, great security features and a modular design.

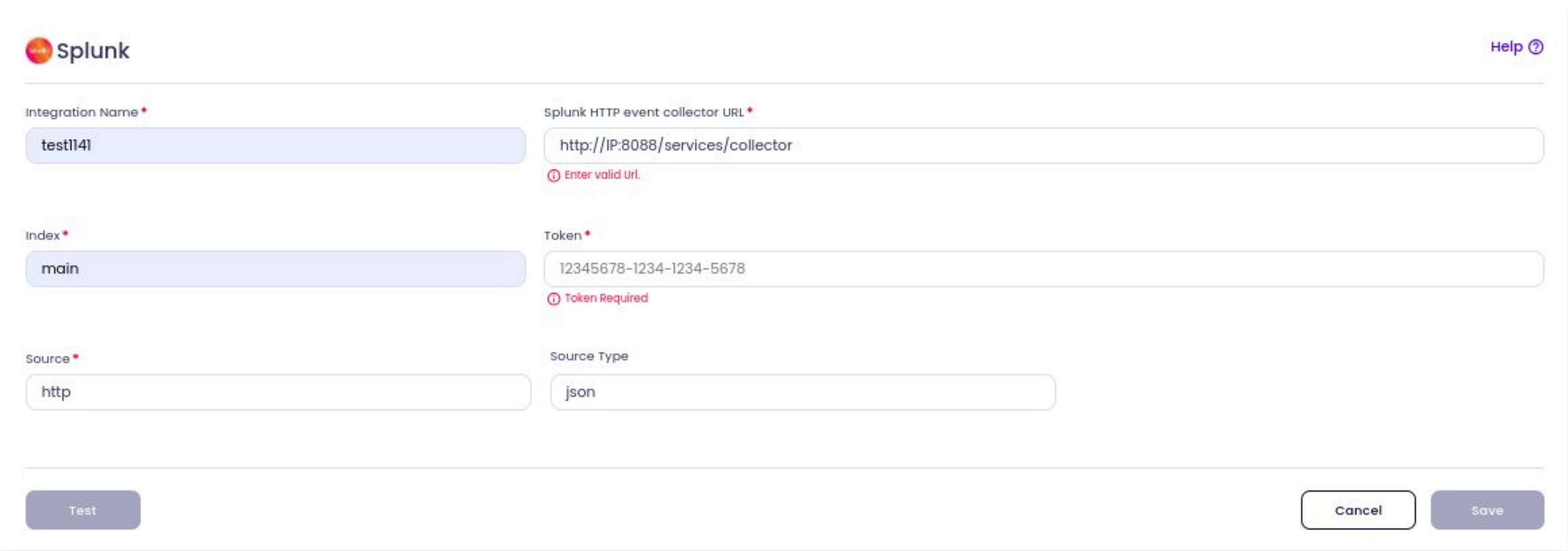
AWS CloudWatch: AWS2 CloudWatch Component allows messages to be sent to an Amazon CloudWatch metrics The implementations of the Amazon API is provided by the AWS SDK.

Azure Sentinel: Azure Sentinel, centralizes your threat collection, detection, response, and investigation efforts. It provides threat intelligence and intelligent security analytic capabilities that facilitate threat visibility, alert detection, threat response, and proactive hunting.

Email: Integrate your Workspace to send alerts as Emails to your email account.

How to Set Up Splunk Integration? [2]

1. Fill all the necessary fields and test the connection before saving the integration.
    - **Integration Name**: Enter any name.
    - **HEC URL**: This is the URL where your Splunk HTTP Event Collector (HEC) is hosted. Enter the full URL, including the protocol (e.g., https://splunk-xxxxxxxxxx.com/services/collector).
    - **Index**: Specify the Splunk index where the data will be stored. The index serves as a container for the incoming data.
    - **Token**: Input the token generated by Splunk for secure communication with the HEC. This token authenticates your requests.
    - **Source**: Indicate the source of the data. This is typically the type of service sending the data (e.g., "http" or "kafka").
    - **Source Type**: Define the format of the incoming data. This helps Splunk interpret the data correctly.
    - **Test**: Before saving, use the "Test" button to send a sample message to Splunk.



Integration Name *: test1141

Splunk HTTP event collector URL *: http://IP:8088/services/collector

ⓘ Enter valid Url.

Index *: main

Token *: 12345678-1234-1234-5678

ⓘ Token Required

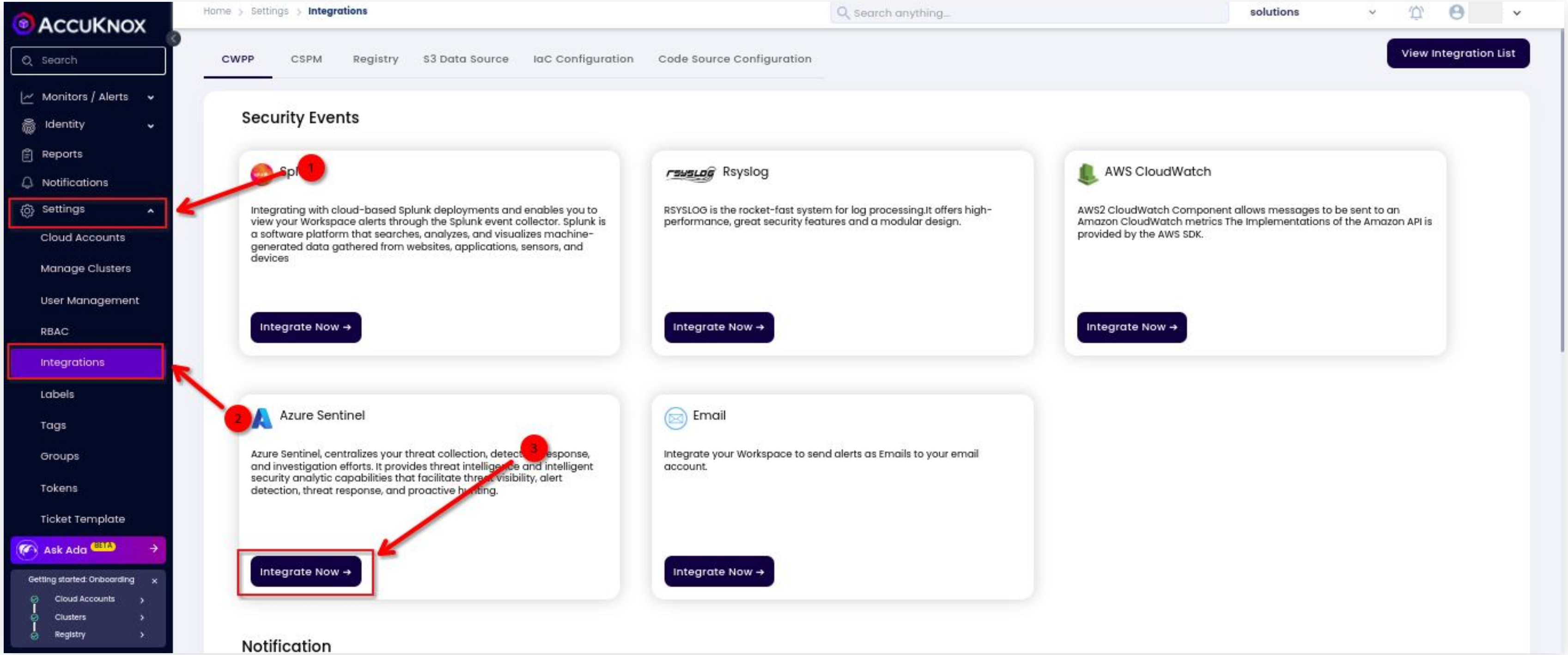
Source *: http

Source Type: json

How to set up Azure Sentinel Integration? [1]

ACCUKNOX

After onboarding Cluster and Applying the policies if you want to forward the logs to SIEM tool. Then Navigate to Settings->Integrations-> Azure Sentinel (Integrate Now)



Security Events

Splunk

Integrating with cloud-based Splunk deployments and enables you to view your Workspace alerts through the Splunk event collector. Splunk is a software platform that searches, analyzes, and visualizes machine-generated data gathered from websites, applications, sensors, and devices

Rsyslog

RSYSLOG is the rocket-fast system for log processing.It offers high-performance, great security features and a modular design.

AWS CloudWatch

AWS2 CloudWatch Component allows messages to be sent to an Amazon CloudWatch metrics The implementations of the Amazon API is provided by the AWS SDK.

Azure Sentinel

Azure Sentinel, centralizes your threat collection, detection, response, and investigation efforts. It provides threat intelligence and intelligent security analytic capabilities that facilitate threat visibility, alert detection, threat response, and proactive hunting.

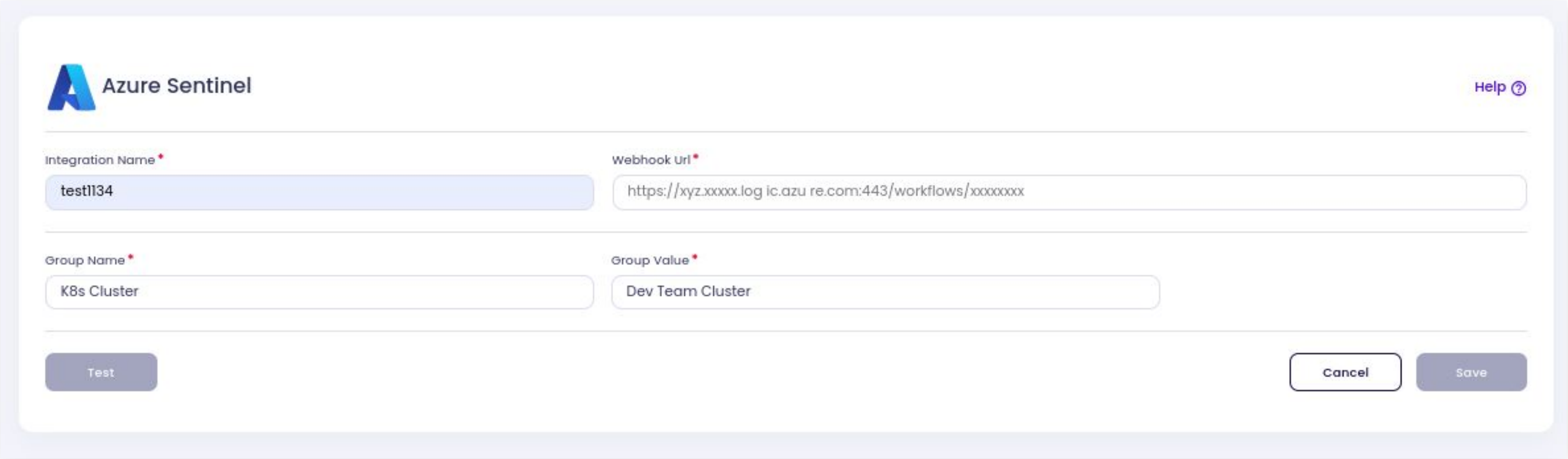
Email

Integrate your Workspace to send alerts as Emails to your email account.

Notification

How to set up Azure Sentinel Integration? [2]

1. 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 of your choice. **Webhook URL:** Enter your Azure Logic App's Webhook URL here.
   b. **Group Name:** You can specify any group name based on your preference, this can be used to filter the events. This works as a key value pair, where key is Group Name and Group Value is the value for the Key Group Name.
2. For more detailed steps refer to the Accuknox help documentation.



Integration Name* test1134

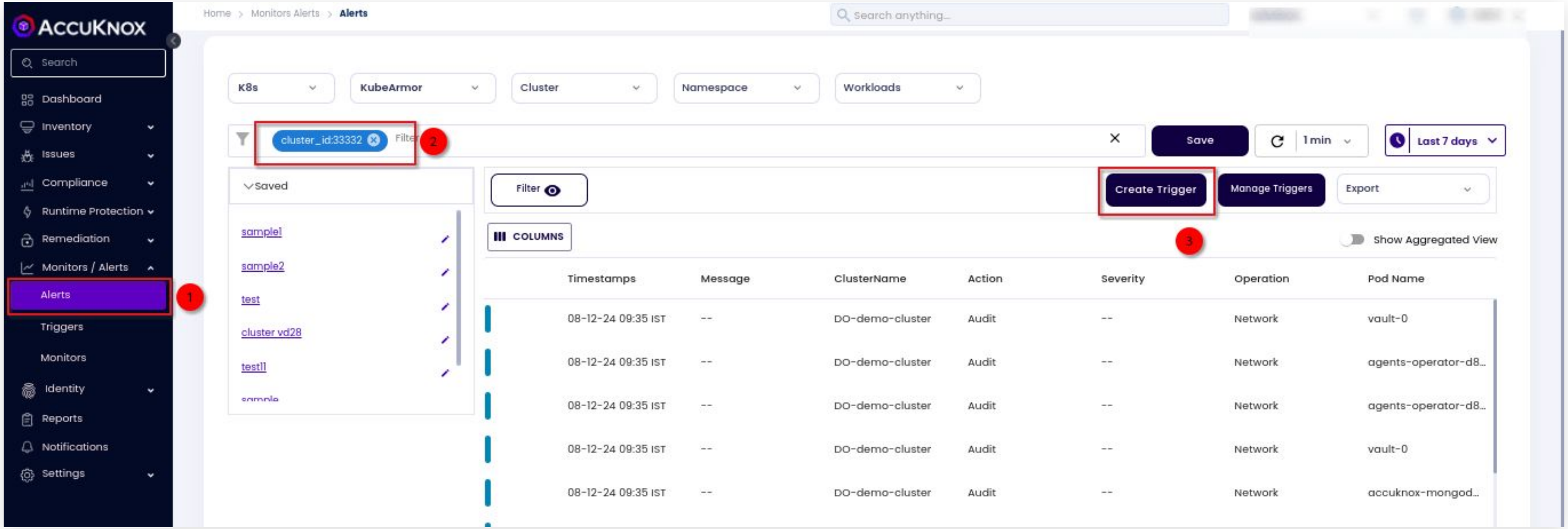
Webhook Url* https://xyz.xxxxx.log ic.azu re.com:443/workflows/xxxxxxxx

Group Name* K8s Cluster

Group Value* Dev Team Cluster

How to Create Triggers for Forwarding Cluster Logs to a Notification Tool? [1]

- Navigate to Monitors/Alerts -> Alerts.
- **Apply the Filter**: Choose the filter criteria that specify the logs you want to forward, ensuring it's set to the specific cluster.
- **Create Trigger**: Click on "Create Trigger" to set up the alert forwarding. Ensure the trigger is configured to capture logs for the desired cluster.



Home > Monitors Alerts > Alerts

cluster_id:33332

1 min

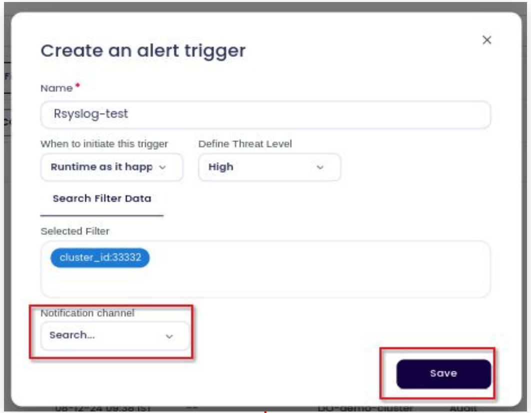
Last 7 days

sample1
sample2
test
cluster vd28
test11
sample

Timestamps	Message	ClusterName	Action	Severity	Operation	Pod Name
08-12-24 09:35 IST	--	DO-demo-cluster	Audit	--	Network	vault-0
08-12-24 09:35 IST	--	DO-demo-cluster	Audit	--	Network	agents-operator-d8...
08-12-24 09:35 IST	--	DO-demo-cluster	Audit	--	Network	agents-operator-d8...
08-12-24 09:35 IST	--	DO-demo-cluster	Audit	--	Network	vault-0
08-12-24 09:35 IST	--	DO-demo-cluster	Audit	--	Network	accuknox-mongod...

How to create triggers to Forward logs for a specific cluster to a notification tool? [2]

- **Trigger Config**: Enter the required details for the trigger configuration.
- **Select Notification Channel**: Choose the appropriate notification channel where alerts should be sent.
- **Click Save**: Finalize and save the trigger.
- Now, all the alerts generated for the specified cluster will be sent to the selected notification channel.



Create an alert trigger

Name *

Rsyslog-test

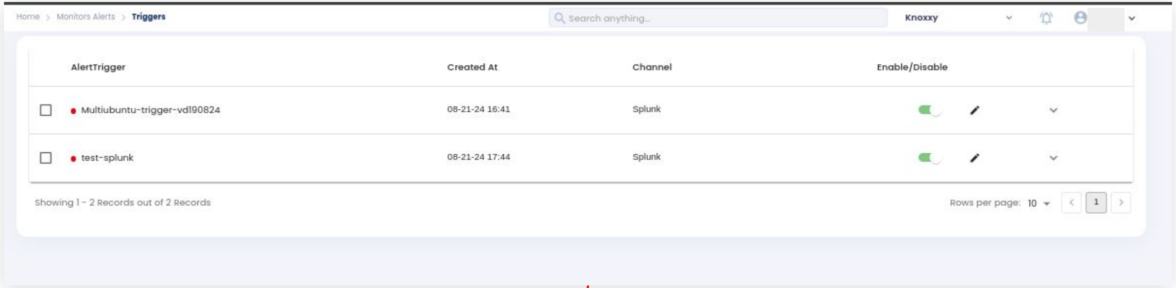
When to initiate this trigger: Runtime as it happ

Define Threat Level: High

Search Filter Data

Selected Filter: cluster_id:33332

Notification channel: Search...

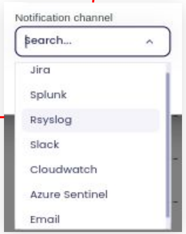


Home > Monitors Alerts > Triggers

	AlertTrigger	Created At	Channel	Enable/Disable
□	Multiubuntu-trigger-vd190824	08-21-24 16:41	Splunk	
□	test-splunk	08-21-24 17:44	Splunk	

Showing 1 - 2 Records out of 2 Records

Rows per page: 10



Notification channel

Search...

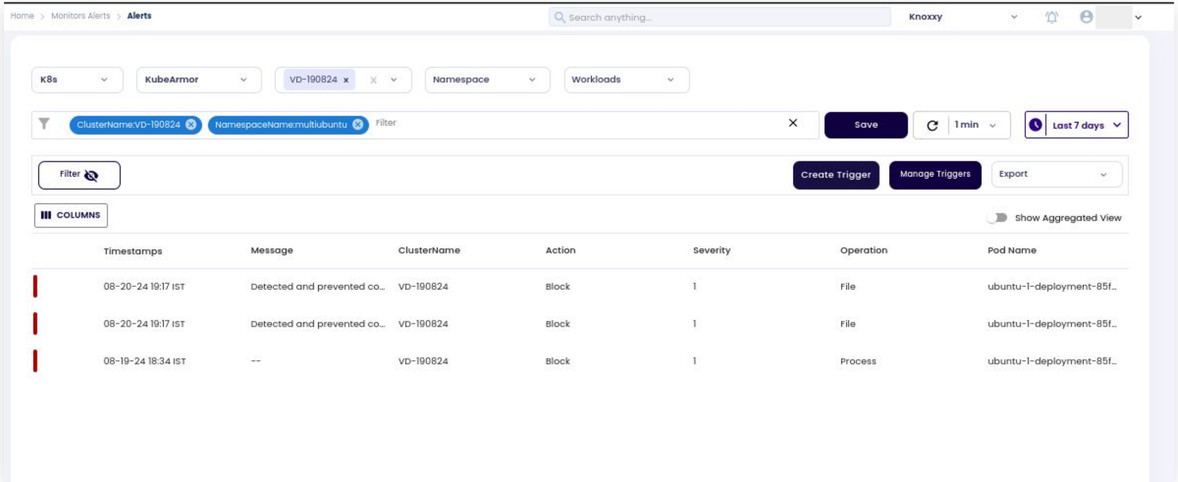
Complete Workflow: Automatically Forward Critical Namespace Alerts to Splunk [1]

1. Integrate Splunk

- **Configure Splunk Integration**

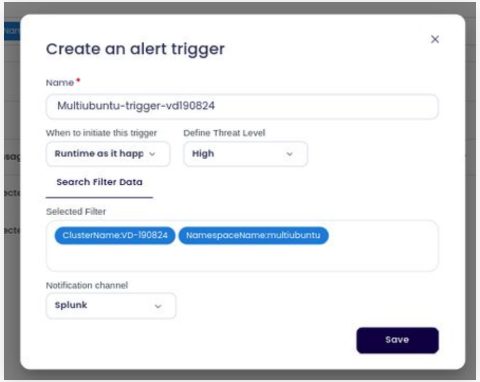
2. Create Triggers

- **Define Alert Trigger:**
  - Go to the alerts section
  - **Add Filter for Namespace:**
    - Set the filter to match your requirements (e.g., namespace:"your-namespace").
  - **Create trigger based on the filter:**
  - **Select Splunk Configuration:**
    - Choose Splunk as the notification channel.



Filter: ClusterName:VD-190824, NamespaceName:multiubuntu

Timestamps	Message	ClusterName	Action	Severity	Operation	Pod Name
08-20-24 19:17 IST	Detected and prevented co...	VD-190824	Block	1	File	ubuntu-1-deployment-85f...
08-20-24 19:17 IST	Detected and prevented co...	VD-190824	Block	1	File	ubuntu-1-deployment-85f...
08-19-24 18:34 IST	--	VD-190824	Block	1	Process	ubuntu-1-deployment-85f...



Create an alert trigger

Name*: Multiubuntu-trigger-vd190824

When to initiate this trigger: Runtime as it happ

Define Threat Level: High

Selected Filter: ClusterName:VD-190824, NamespaceName:multiubuntu

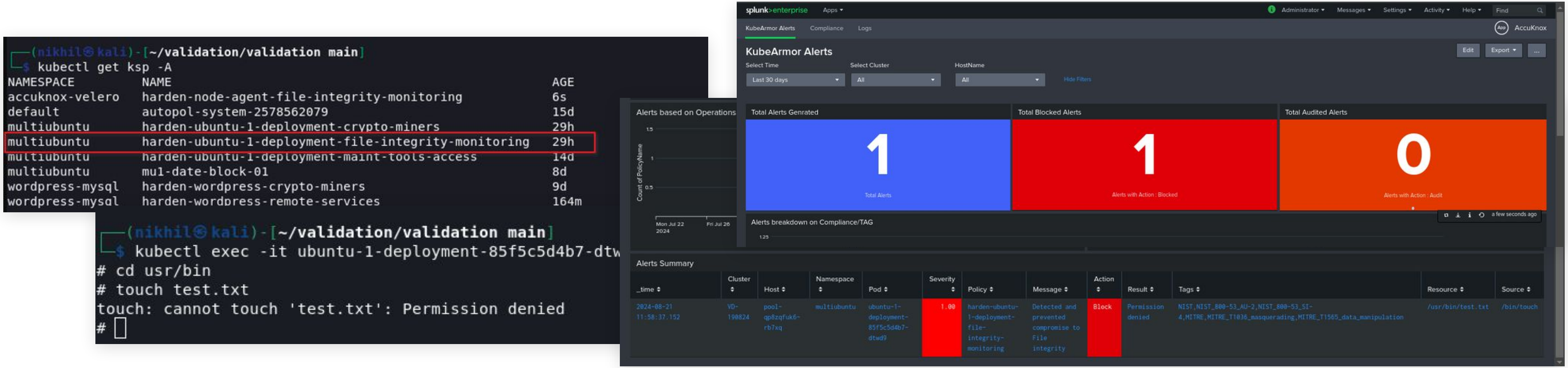
Notification channel: Splunk

confidential and proprietary - limited distribution under NDA

Complete Workflow: Automatically Forward Critical Namespace Alerts to Splunk [2]

3. Test Alert Notification

- **Simulate Policy Violation:**
  - Intentionally violate a policy that you have applied to trigger an alert.
- **Verify Notification:**
  - Check the Splunk dashboard to ensure that the violated alert notification appears as expected.
  - Now, all alerts generated for the specified namespace will be forwarded to Splunk as per the configured trigger.



```
┌──(nikhil㉿kali)-[~/validation/validation main]
└─$ kubectl get ksp -A
NAMESPACE         NAME                                               AGE
accuknox-velero   harden-node-agent-file-integrity-monitoring        6s
default           autopol-system-2578562079                          15d
multiubuntu       harden-ubuntu-1-deployment-crypto-miners           29h
multiubuntu       harden-ubuntu-1-deployment-file-integrity-monitoring   29h
multiubuntu       harden-ubuntu-1-deployment-maint-tools-access      14d
multiubuntu       mul-date-block-01                                  8d
wordpress-mysql   harden-wordpress-crypto-miners                     9d
wordpress-mysql   harden-wordpress-remote-services                   164m
```

```
┌──(nikhil㉿kali)-[~/validation/validation main]
└─$ kubectl exec -it ubuntu-1-deployment-85f5c5d4b7-dtw
# cd usr/bin
# touch test.txt
touch: cannot touch 'test.txt': Permission denied
# 
```

KubeArmor Alerts

Select Time: Last 30 days
Select Cluster: All
HostName: All

Total Alerts Genrated: 1 — Total Alerts

Total Blocked Alerts: 1 — Alerts with Action : Blocked

Total Audited Alerts: 0 — Alerts with Action : Audit

Alerts Summary

_time	Cluster	Host	Namespace	Pod	Severity	Policy	Message	Action	Result	Tags	Resource	Source
2024-08-21 11:58:37.152	VD-190824	pool-qp8zqfuk6-rb7xq	multiubuntu	ubuntu-1-deployment-85f5c5d4b7-dtwd9	1.00	harden-ubuntu-1-deployment-file-integrity-monitoring	Detected and prevented compromise to File integrity	Block	Permission denied	NIST,NIST_800-53_AU-2,NIST_800-53_SI-4,MITRE,MITRE_T1036_masquerading,MITRE_T1565_data_manipulation	/usr/bin/test.txt	/bin/touch

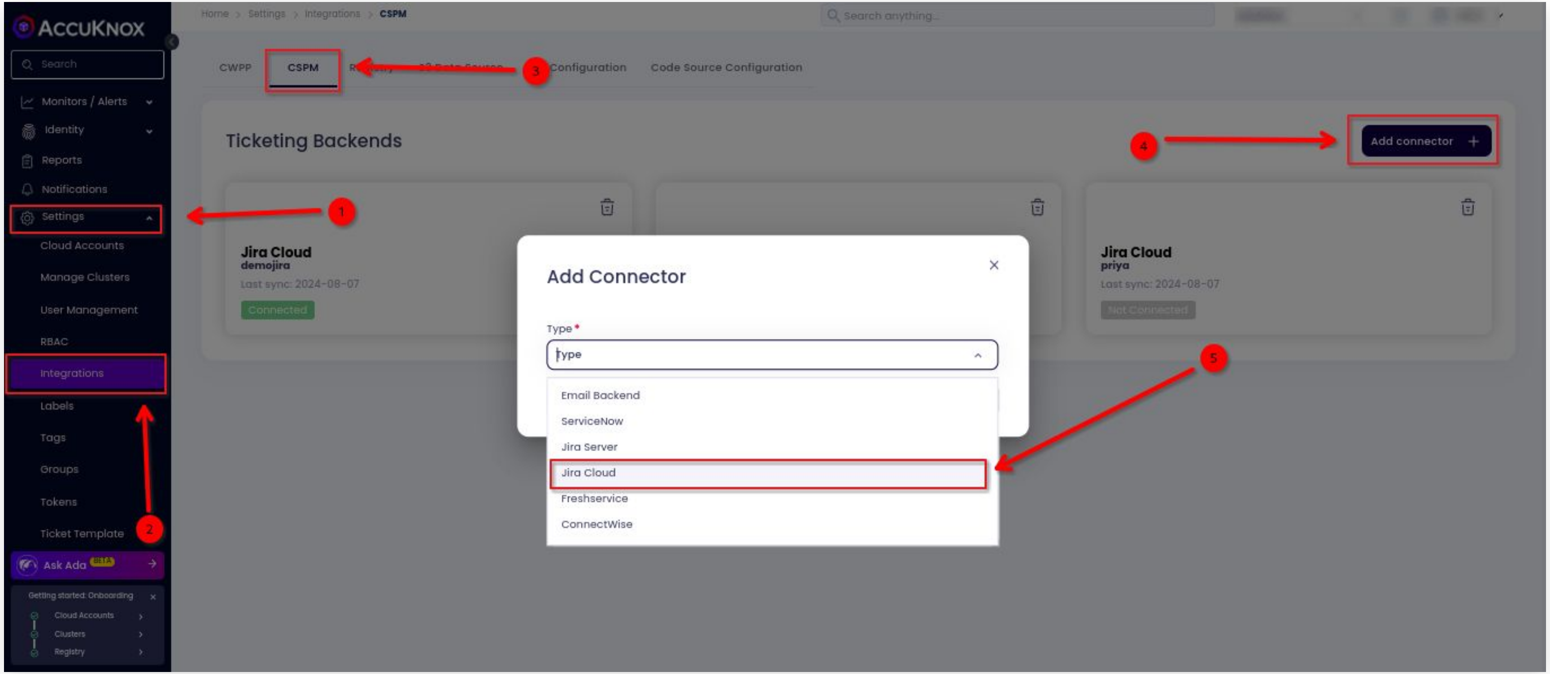
AccuKnox

Ticketing

How to Integrate CSPM Alerts with Jira Cloud for Ticketing? [1]

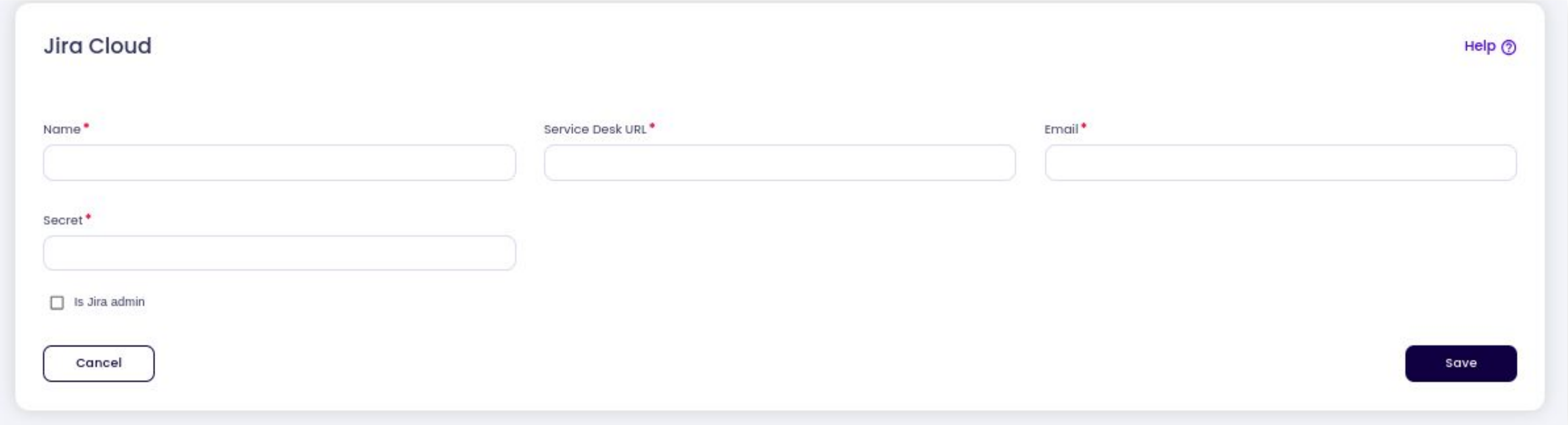
After getting the findings data populated If users want to create tickets for the findings. Then Navigate to Settings->Integrations-> CSPM > Add connector

- Choose Jira Cloud as the connector and Click Next.



How to Integrate CSPM Alerts with Jira Cloud for Ticketing? [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.
  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.
  d. **Token:** Enter the generated Token here from https://id.atlassian.com/manage-profile/security/api-tokens.
- For more detailed steps refer to the Accuknox help documentation.



Jira Cloud

Name *

Service Desk URL *

Email *

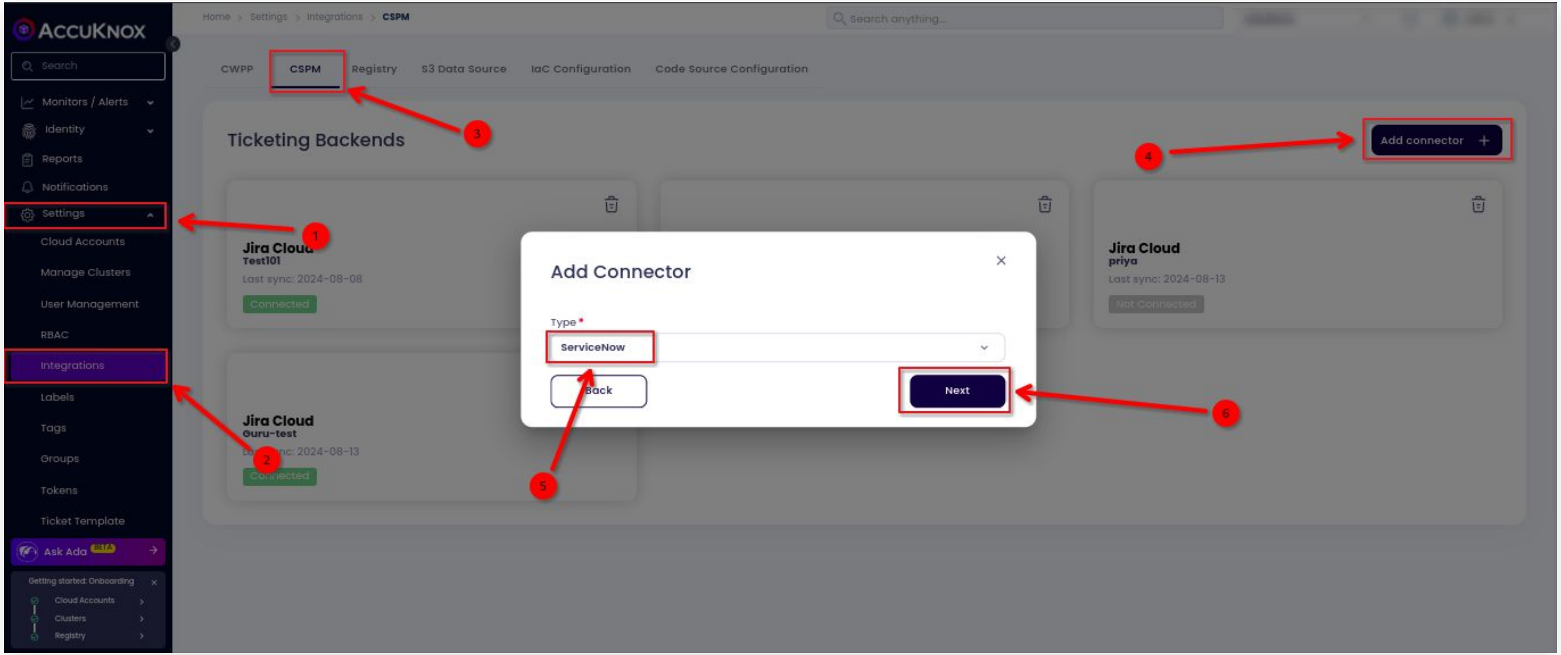
Secret *

☐ Is Jira admin

How to Integrate CSPM Alerts with ServiceNow for Ticketing? [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.



Ticketing Backends

Jira Cloud
Test101
Last sync: 2024-08-08
Connected

Jira Cloud
priya
Last sync: 2024-08-13
Not Connected

Jira Cloud
Guru-test
Last sync: 2024-08-13
Connected

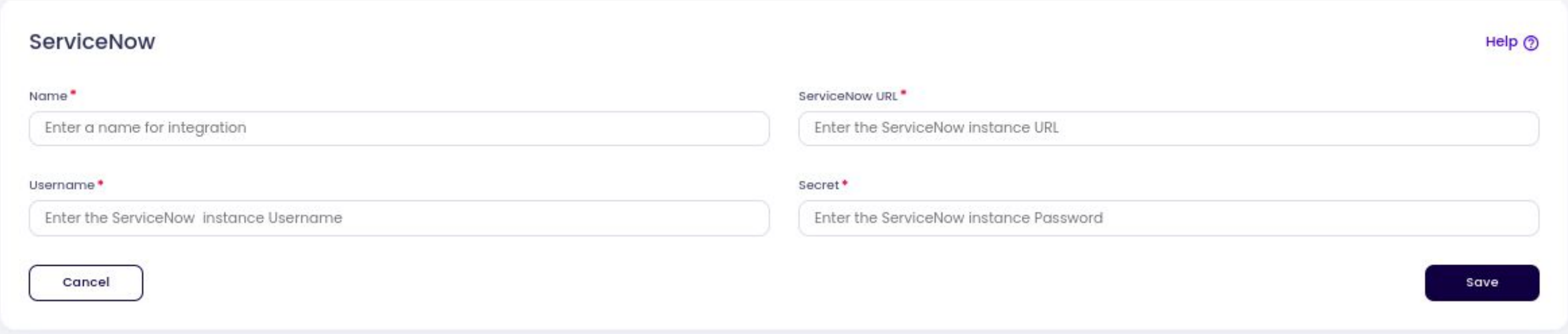
Add Connector

Type *
ServiceNow

How to Integrate CSPM Alerts with ServiceNow for Ticketing? [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.
  b. **ServiceNow URL**: The URL of the ServiceNow instance.
  c. **Instance Username**: The Username associated with the instance.
  d. **Secret**: The current password of the instance.
- For more detailed steps refer to the Accuknox help documentation.



ServiceNow

Name *
Enter a name for integration

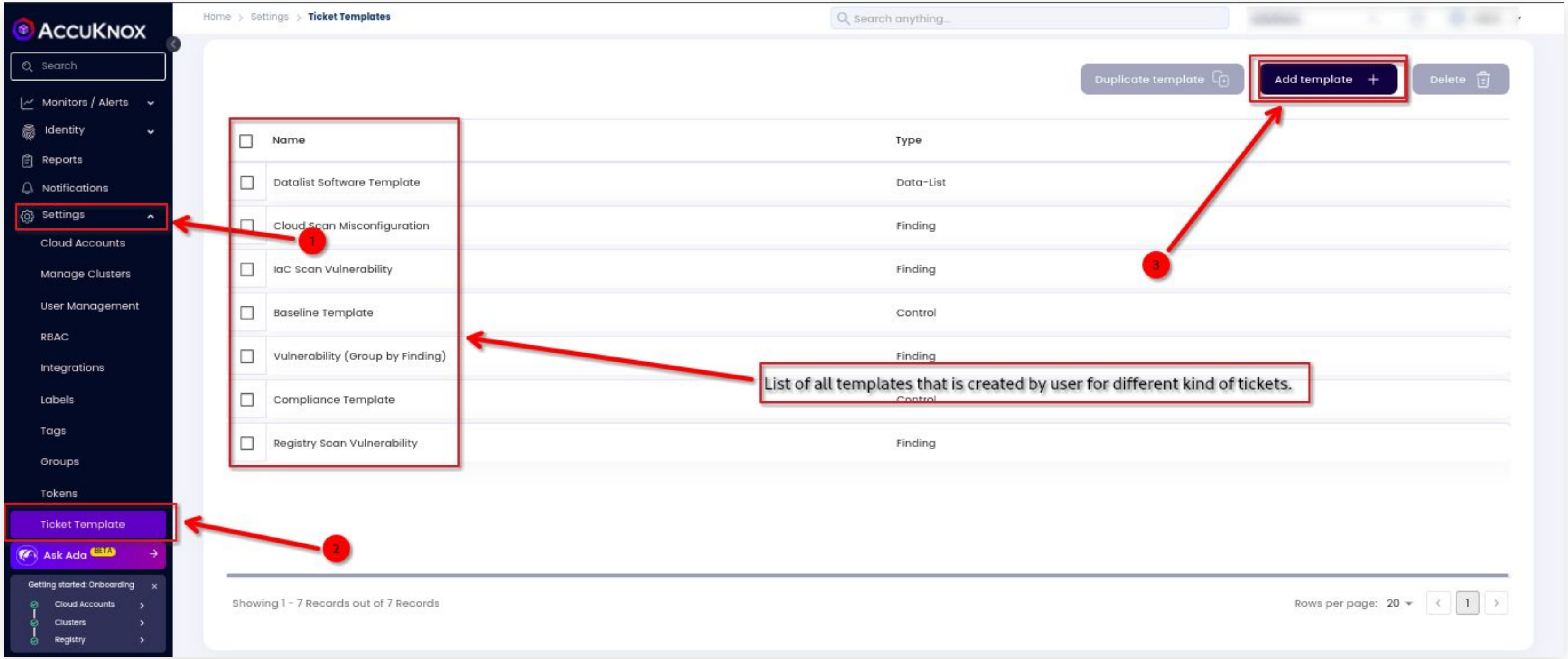
ServiceNow URL *
Enter the ServiceNow instance URL

Username *
Enter the ServiceNow instance Username

Secret *
Enter the ServiceNow instance Password

How to create template for ticket? [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



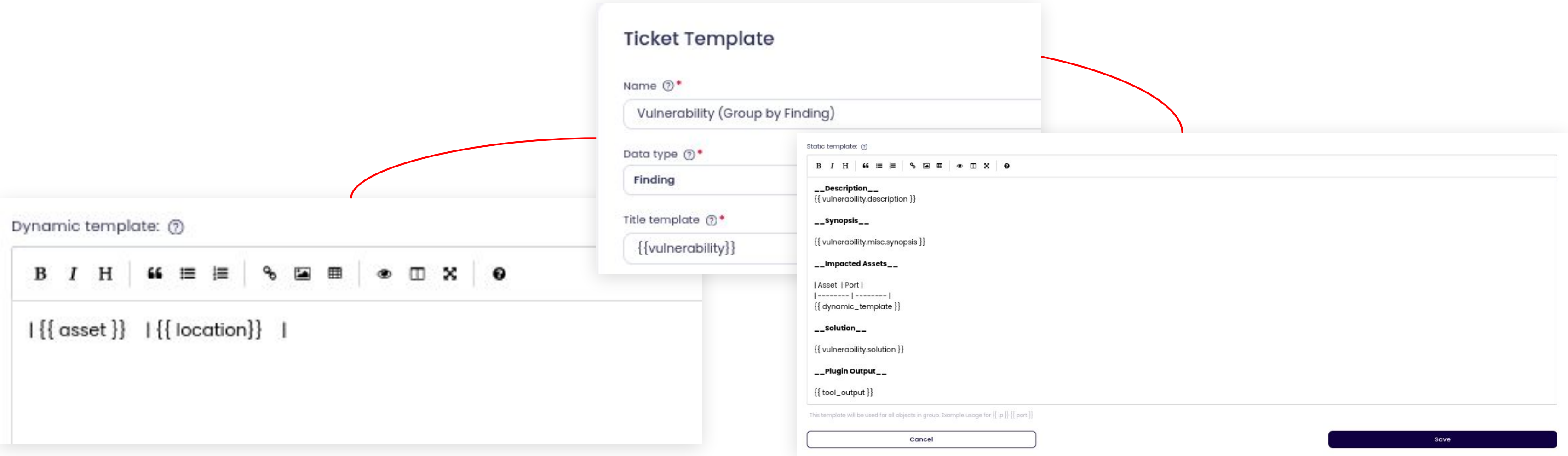
☐ Name	Type
☐ Datalist Software Template	Data-List
☐ Cloud Scan Misconfiguration	Finding
☐ IaC Scan Vulnerability	Finding
☐ Baseline Template	Control
☐ Vulnerability (Group by Finding)	Finding
☐ Compliance Template	Control
☐ Registry Scan Vulnerability	Finding

Showing 1 - 7 Records out of 7 Records

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

How to create template for ticket? [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 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. This would be helpful in case of creating ticket for multiple findings.
  e. **Static Template:** Applies consistent data across a group with similar findings. This template would be helpful for creating ticket for a single finding.



Ticket Template

Name: Vulnerability (Group by Finding)

Data type: Finding

Title template: {{vulnerability}}

Dynamic template:

```
| {{ asset }}   | {{ location}}   |
```

Static template:

```
__Description__
{{ vulnerability.description }}

__Synopsis__

{{ vulnerability.misc.synopsis }}

__Impacted Assets__

| Asset  | Port |
| -------- | -------- |
{{ dynamic_template }}

__Solution__

{{ vulnerability.solution }}

__Plugin Output__

{{ tool_output }}
```

This template will be used for all objects in group. Example usage for {{ ip }} {{ port }}

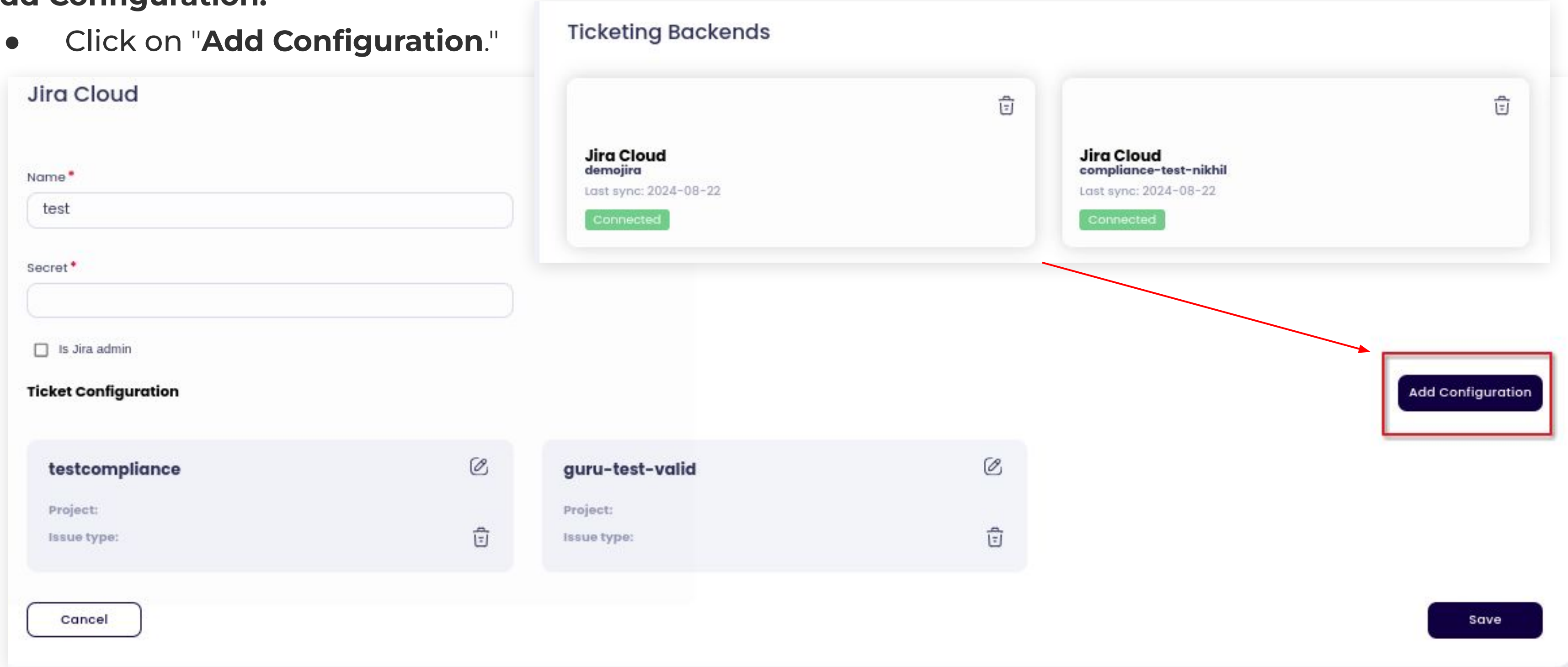
How to Add and Set Up Configuration for Your Ticketing Integration? [1]

To add Configuration Click on the Created Integration:

- Go to the ticket integration you saved.

Add Configuration:

- Click on "**Add Configuration**."



Ticketing Backends

Jira Cloud
demojira
Last sync: 2024-08-22
Connected

Jira Cloud
compliance-test-nikhil
Last sync: 2024-08-22
Connected

Jira Cloud

Name *
test

Secret *

□ Is Jira admin

Ticket Configuration

testcompliance
Project:
Issue type:

guru-test-valid
Project:
Issue type:

confidential and proprietary - limited distribution under NDA

How to Add and Set Up Configuration for Your Ticketing Integration? [2]

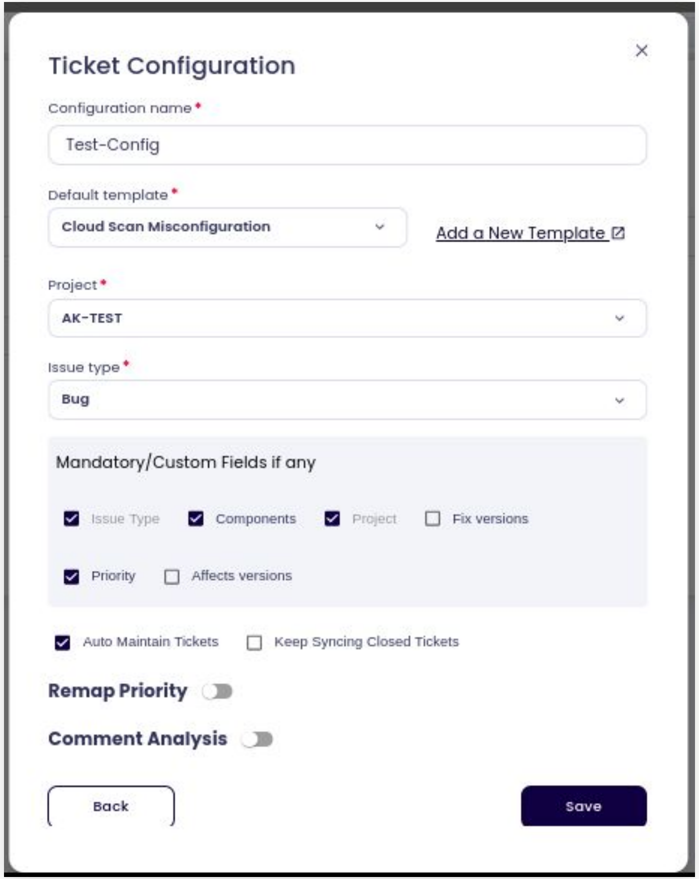
Configuration Details:

- **Name:** Provide a name for the configuration.
- **Default Template:** Select an existing template or create a new one.
- **Project:** Choose the relevant Jira project where you want to create tickets.
- **Issue Type:** Specify the type of issue.

Additional Settings:

- Auto Maintain Tickets: Enable if you want the system to automatically bidirectionally sync the tickets.
- Keep Syncing Closed Tickets: Enable if you want closed tickets to remain synced and updated.
- Custom Fields: Configure any other required custom fields as needed.
- **Remap findings** from the scan result to Jira ticket priorities: Unknown, Informational, Low, Medium, High, Critical, ensuring alignment with your workflow and efficient issue tracking.

This setup finalizes your ServiceNow ticket integration, making it ready for use.



Ticket Configuration

Configuration name *
Test-Config

Default template *
Cloud Scan Misconfiguration

Project *
AK-TEST

Issue type *
Bug

Mandatory/Custom Fields if any

☑ Issue Type ☑ Components ☑ Project ☐ Fix versions

☑ Priority ☐ Affects versions

☑ Auto Maintain Tickets ☐ Keep Syncing Closed Tickets

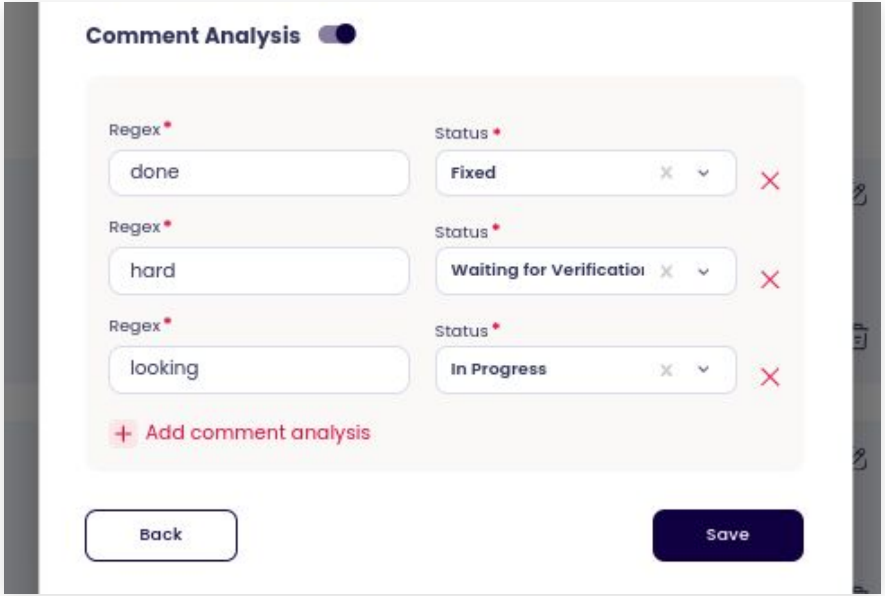
Remap Priority

Comment Analysis

How to Set Up Comment Analysis in Configuration for Your Ticketing Integration?

ACCUKNOX

1. **Toggle on Comment Analysis**
   Enable the comment analysis feature in your ticketing configuration.
2. **Set Up Regex and Status**
   - **Regex:** Enter the regular expression to identify specific comments.
   - **Status Change:** Specify the status you want to apply based on the regex match.
3. **Automatic Issue Management**
   - You can leave comments on tickets for analysis and automatically change issue status based on the comment analysis results.



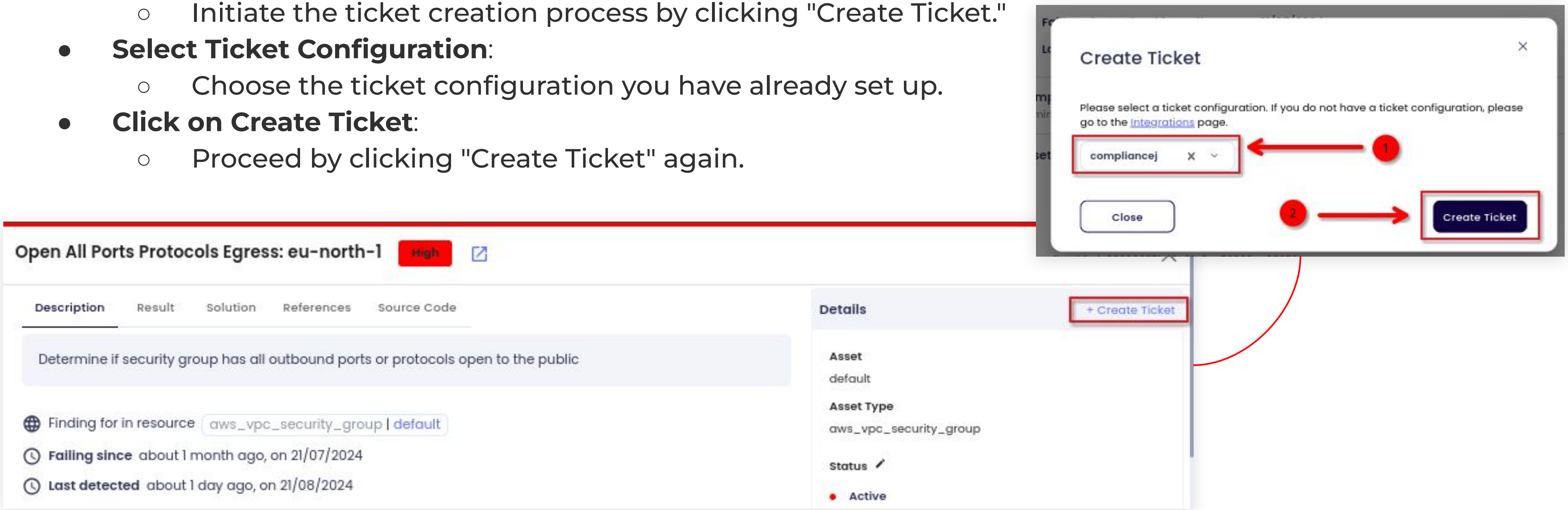
Comment Analysis ●

Regex *	Status *
done	Fixed
hard	Waiting for Verificatio
looking	In Progress

+ Add comment analysis

How to Create a Ticket for Addressing a Finding? [1]

- **Navigate to Issues > Findings**:
  - Go to the "Findings" section under "Issues."
- **Select a Finding**:
  - Click on the specific finding you want to create a ticket for to view more detailed information.
- **Click on Create Ticket**:
  - Initiate the ticket creation process by clicking "Create Ticket."
- **Select Ticket Configuration**:
  - Choose the ticket configuration you have already set up.
- **Click on Create Ticket**:
  - Proceed by clicking "Create Ticket" again.



Create Ticket

Please select a ticket configuration. If you do not have a ticket configuration, please go to the Integrations page.

compliancej

Open All Ports Protocols Egress: eu-north-1

Determine if security group has all outbound ports or protocols open to the public

Finding for in resource aws_vpc_security_group | default

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

Last detected about 1 day ago, on 21/08/2024

Asset
default

Asset Type
aws_vpc_security_group

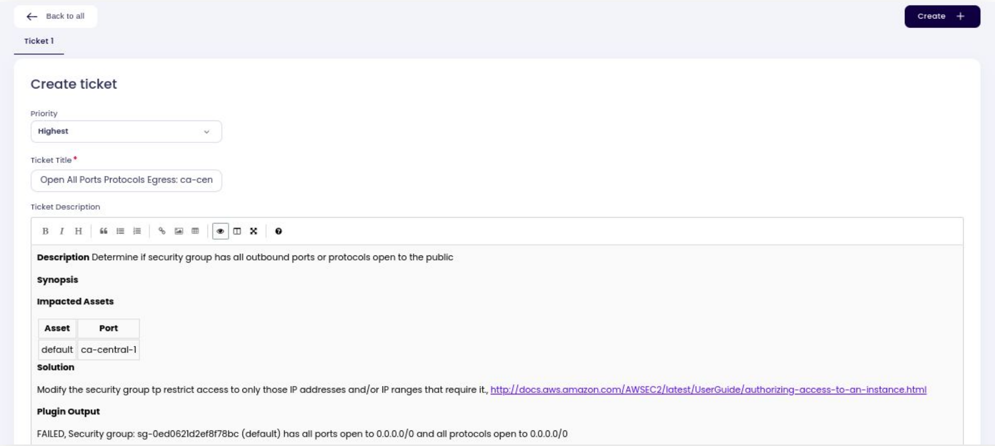
Status
● Active

confidential and proprietary - limited distribution under NDA

How to Create a Ticket for Addressing a Finding? [2]

- Configure Ticket Details:
  - You will be redirected to a new page where you can set the ticket priority, title, and description.
- The description can be automatically generated based on a ticket template you've created, or you can use a predefined ticket template that is available.
- Click Save:
  - Save the ticket by clicking "Save."

Your created ticket will now be available on the ticketing platform.



Create ticket

Priority: Highest

Ticket Title *: Open All Ports Protocols Egress: ca-cen

Ticket Description

Description Determine if security group has all outbound ports or protocols open to the public

Synopsis

Impacted Assets

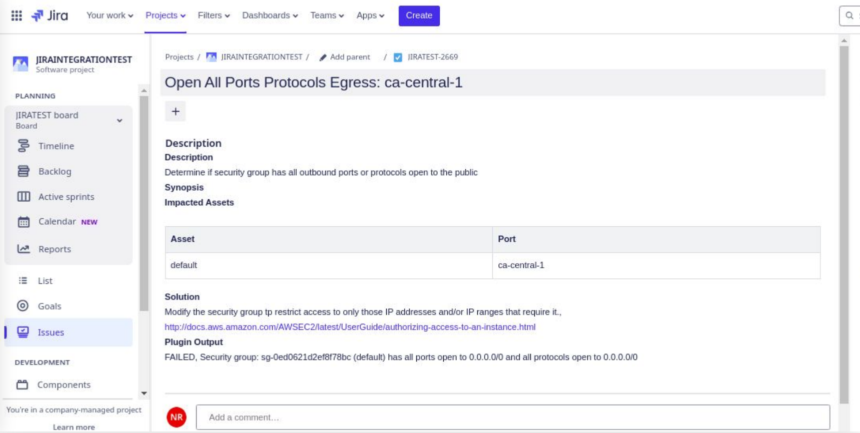
Asset	Port
default	ca-central-1

Solution

Modify the security group tp restrict access to only those IP addresses and/or IP ranges that require it., http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/authorizing-access-to-an-instance.html

Plugin Output

FAILED, Security group: sg-0ed0621d2ef8f78bc (default) has all ports open to 0.0.0.0/0 and all protocols open to 0.0.0.0/0



Open All Ports Protocols Egress: ca-central-1

Description

Description

Determine if security group has all outbound ports or protocols open to the public

Synopsis

Impacted Assets

Asset	Port
default	ca-central-1

Solution

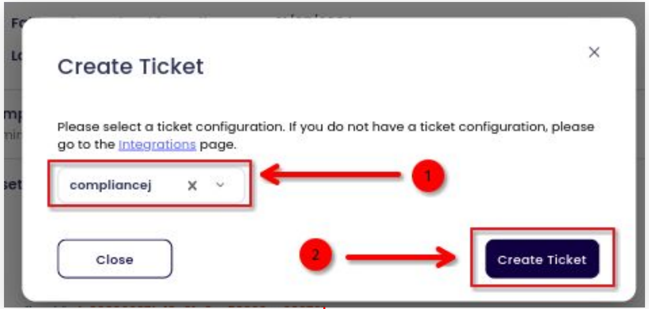
Modify the security group tp restrict access to only those IP addresses and/or IP ranges that require it.,
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/authorizing-access-to-an-instance.html

Plugin Output

FAILED, Security group: sg-0ed0621d2ef8f78bc (default) has all ports open to 0.0.0.0/0 and all protocols open to 0.0.0.0/0

How to create tickets for multiple findings at Once ? [1]

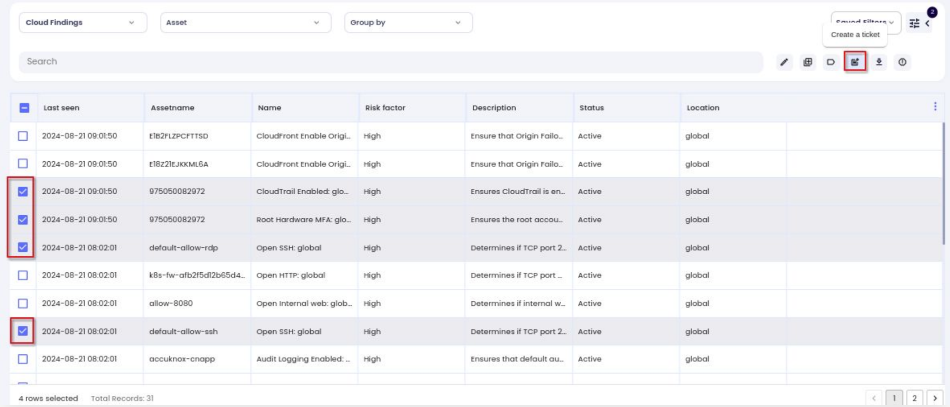
- **Navigate to Issues > Findings**:
  - Go to the "Findings" section under "Issues."
- **Select multiple Finding**:
  - Select multiple findinga you want to create a ticket for.
- **Click on Create Ticket**:
  - Initiate the ticket creation process by clicking "Create Ticket."
- **Select Ticket Configuration**:
  - Choose the ticket configuration you have already set up.
- **Click on Create Ticket**:
  - Proceed by clicking "Create Ticket" again.



Create Ticket

Please select a ticket configuration. If you do not have a ticket configuration, please go to the Integrations page.

compliancej



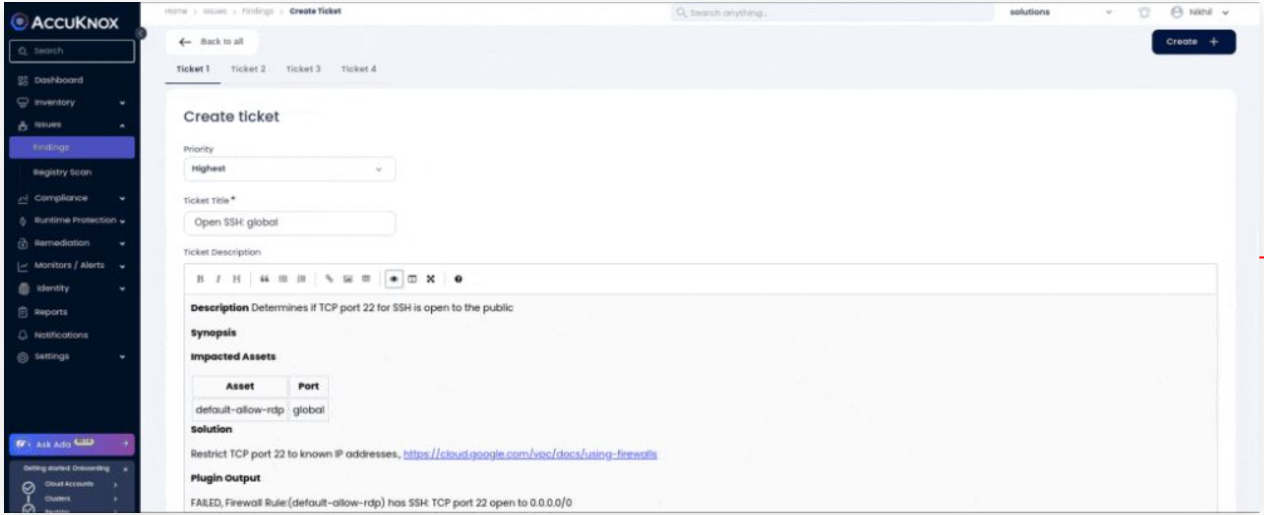
☐	Last seen	Assetname	Name	Risk factor	Description	Status	Location
☐	2024-08-21 09:01:50	E1B2FLZPCFTTSD	CloudFront Enable Origi...	High	Ensure that Origin Failo...	Active	global
☐	2024-08-21 09:01:50	E18Z21EJKKML6A	CloudFront Enable Origi...	High	Ensure that Origin Failo...	Active	global
☑	2024-08-21 09:01:50	975050082972	CloudTrail Enabled: glo...	High	Ensures CloudTrail is en...	Active	global
☑	2024-08-21 09:01:50	975050082972	Root Hardware MFA: glo...	High	Ensures the root accou...	Active	global
☑	2024-08-21 08:02:01	default-allow-rdp	Open SSH: global	High	Determines if TCP port 2...	Active	global
☐	2024-08-21 08:02:01	k8s-fw-afb2f5d12b65d4...	Open HTTP: global	High	Determines if TCP port ...	Active	global
☐	2024-08-21 08:02:01	allow-8080	Open Internal web: glob...	High	Determines if internal w...	Active	global
☑	2024-08-21 08:02:01	default-allow-ssh	Open SSH: global	High	Determines if TCP port 2...	Active	global
☐	2024-08-21 08:02:01	accuknox-cnapp	Audit Logging Enabled: ...	High	Ensures that default au...	Active	global

4 rows selected   Total Records: 31

How to create tickets for multiple findings at Once? [2]

- Configure Ticket Details:
  - You will be redirected to a new page where you can set the ticket priority, title, and description.
- The description can be automatically generated based on a ticket template you've created it, or you can use a predefined ticket template that is available.
- Click Save:
  - Save the ticket by clicking "Save."

Your created ticket will now be available on the ticketing platform.



Create ticket

Priority: Highest

Ticket Title *: Open SSH: global

Ticket Description

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

Synopsis

Impacted Assets

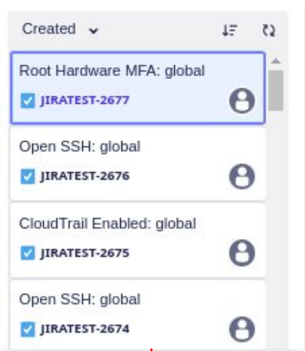
Asset	Port
default-allow-rdp	global

Solution

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

Plugin Output

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



Root Hardware MFA: global
☑ JIRATEST-2677

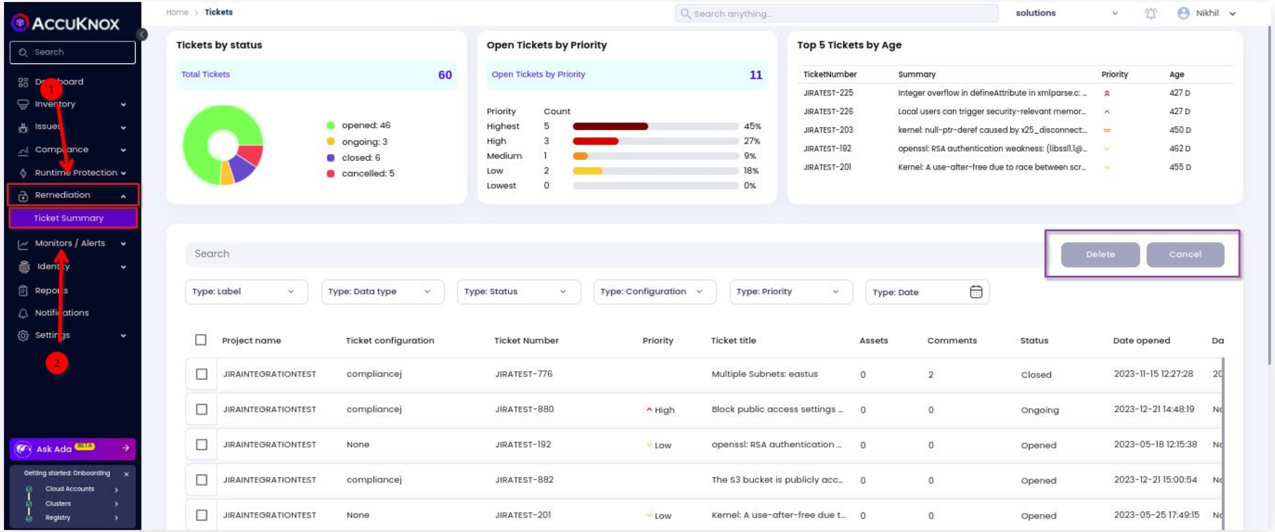
Open SSH: global
☑ JIRATEST-2676

CloudTrail Enabled: global
☑ JIRATEST-2675

Open SSH: global
☑ JIRATEST-2674

How to Track and Manage All Tickets on the Accuknox Platform?

1. **Access the Ticket Summary**
   - Navigate to: Remediation > Ticket Summary
2. **Key Graphs**
   - **Tickets by Status**: See the distribution of tickets across different statuses.
   - **Open Tickets by Priority**: Visualize open tickets sorted by priority level.
   - **Top 5 Tickets by Age**: Identify and review the oldest tickets to address them promptly.
3. **Use Advanced Filters**
   - **Filter Options**: Apply advanced filters to refine and manage ticket data.
4. **Manage Tickets**
   - **Delete or Cancel**: You can directly delete or cancel tickets as needed from the summary view.



Tickets by status

Total Tickets 60

- opened: 46
- ongoing: 3
- closed: 6
- cancelled: 5

Open Tickets by Priority

Open Tickets by Priority 11

Priority	Count	
Highest	5	45%
High	3	27%
Medium	1	9%
Low	2	18%
Lowest	0	0%

Top 5 Tickets by Age

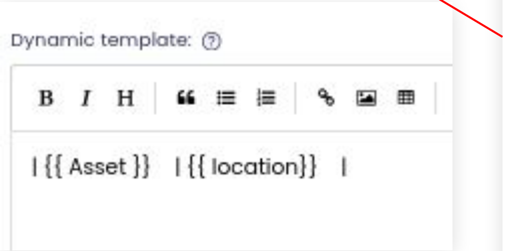
TicketNumber	Summary	Priority	Age
JIRATEST-225	Integer overflow in defineAttribute in xmlparse.c: ...		427 D
JIRATEST-226	Local users can trigger security-relevant memor...		427 D
JIRATEST-203	kernel: null-ptr-deref caused by x25_disconnect:...		450 D
JIRATEST-192	openssl: RSA authentication weakness: (libssl1.1@...		462 D
JIRATEST-201	Kernel: A use-after-free due to race between scr...		455 D

□	Project name	Ticket configuration	Ticket Number	Priority	Ticket title	Assets	Comments	Status	Date opened	Da
□	JIRAINTEGRATIONTEST	compliancej	JIRATEST-776		Multiple Subnets: eastus	0	2	Closed	2023-11-15 12:27:28	20
□	JIRAINTEGRATIONTEST	compliancej	JIRATEST-880	High	Block public access settings ...	0	0	Ongoing	2023-12-21 14:48:19	N
□	JIRAINTEGRATIONTEST	None	JIRATEST-192	Low	openssl: RSA authentication ...	0	0	Opened	2023-05-18 12:15:38	N
□	JIRAINTEGRATIONTEST	compliancej	JIRATEST-882		The S3 bucket is publicly acc...	0	0	Opened	2023-12-21 15:00:54	N
□	JIRAINTEGRATIONTEST	None	JIRATEST-201	Low	Kernel: A use-after-free due t...	0	0	Opened	2023-05-25 17:49:15	N

How to create single ticket for Multiple assets affected by single finding and vice-versa? [1]

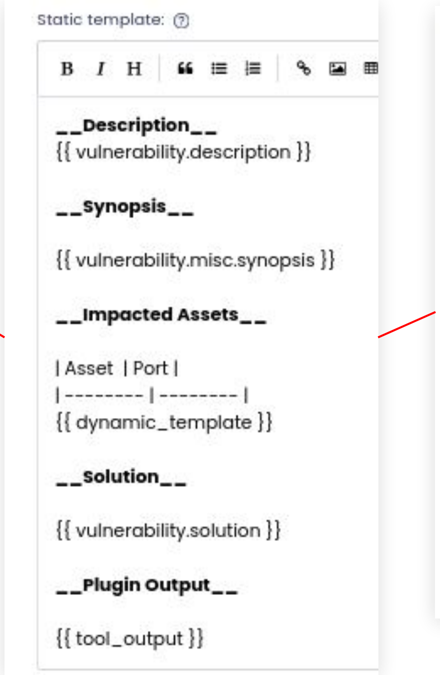
- Create ticket template and link it to the configuration.
- In the findings page add **Group by Findings** filter, click on the finding then select all the **Asset > Create Ticket.**
- Select the config with appropriate ticket template to create ticket

GROUP BY FINDINGS



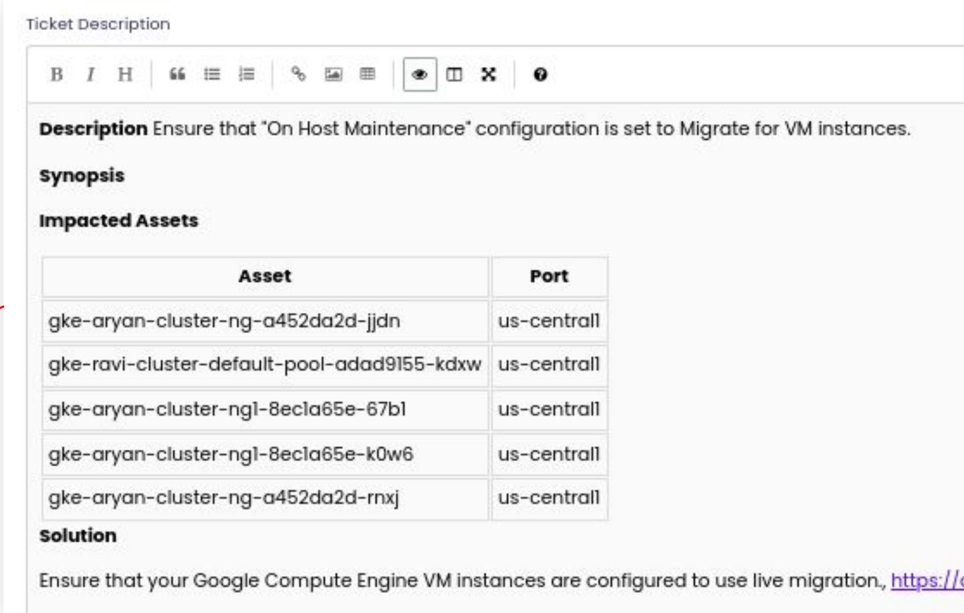
Dynamic template:

```
| {{ Asset }}   | {{ location}}   |
```



Static template:

```
__Description__
{{ vulnerability.description }}

__Synopsis__

{{ vulnerability.misc.synopsis }}

__Impacted Assets__

| Asset  | Port |
| --------- | --------- |
{{ dynamic_template }}

__Solution__

{{ vulnerability.solution }}

__Plugin Output__

{{ tool_output }}
```



Ticket Description

Description Ensure that "On Host Maintenance" configuration is set to Migrate for VM instances.

Synopsis

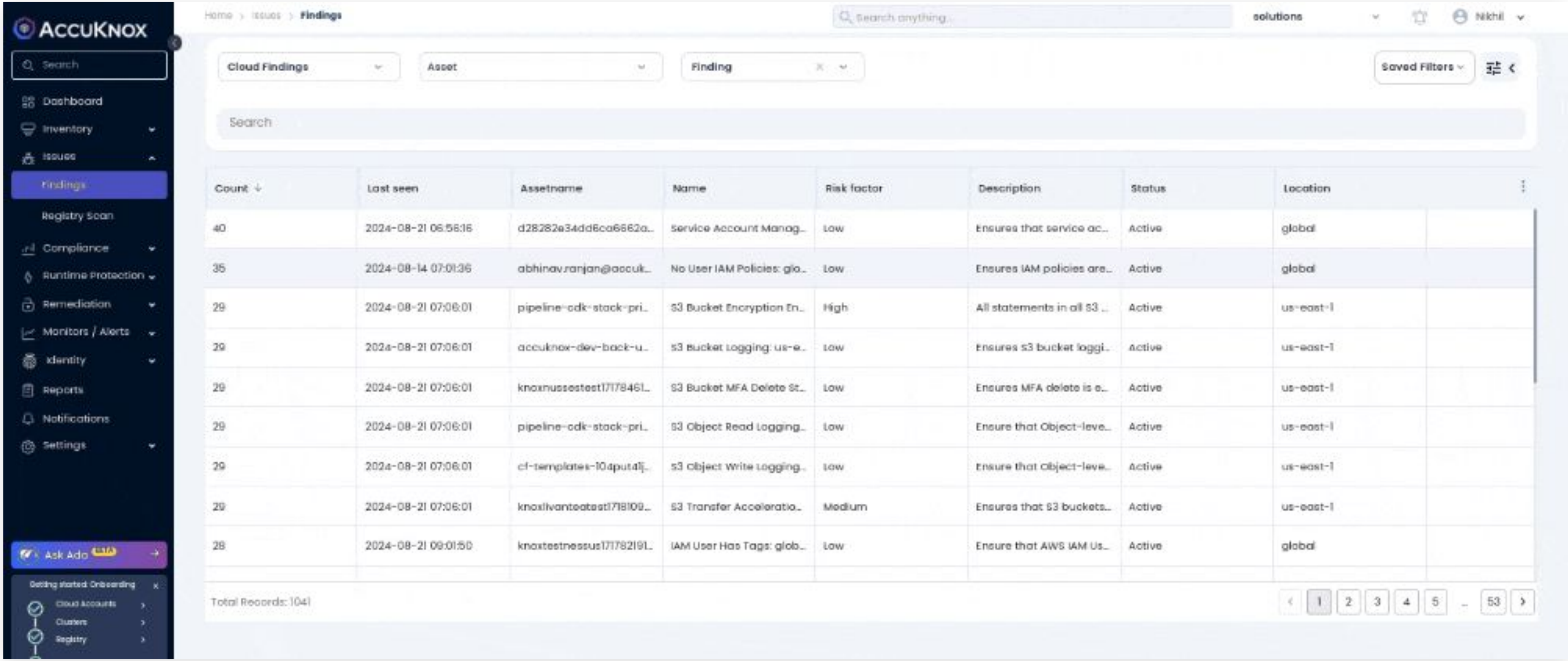
Impacted Assets

Asset	Port
gke-aryan-cluster-ng-a452da2d-jjdn	us-central1
gke-ravi-cluster-default-pool-adad9155-kdxw	us-central1
gke-aryan-cluster-ng1-8ec1a65e-67b1	us-central1
gke-aryan-cluster-ng1-8ec1a65e-k0w6	us-central1
gke-aryan-cluster-ng-a452da2d-rnxj	us-central1

Solution

Ensure that your Google Compute Engine VM instances are configured to use live migration., https://

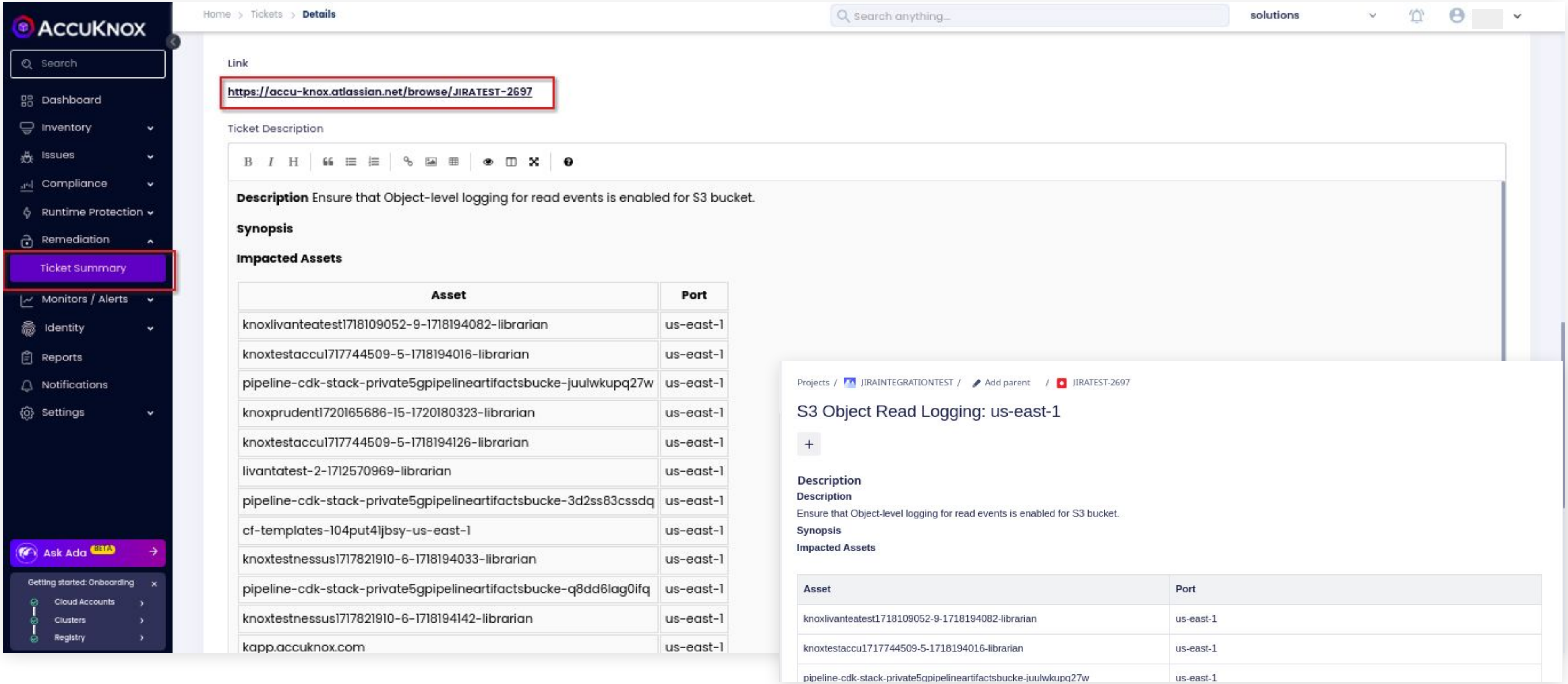
How to create single ticket for Multiple assets affected by single finding and vice-versa? [1a]



Count ↓	Last seen	Assetname	Name	Risk factor	Description	Status	Location
40	2024-08-21 06:56:16	d28282e34dd6ca6662a...	Service Account Manag...	Low	Ensures that service ac...	Active	global
35	2024-08-14 07:01:36	abhinav.ranjan@accuk...	No User IAM Policies: glo...	Low	Ensures IAM policies are...	Active	global
29	2024-08-21 07:06:01	pipeline-cdk-stack-pri...	S3 Bucket Encryption En...	High	All statements in all S3 ...	Active	us-east-1
29	2024-08-21 07:06:01	accuknox-dev-back-u...	S3 Bucket Logging: us-e...	Low	Ensures S3 bucket loggi...	Active	us-east-1
29	2024-08-21 07:06:01	knoxnussestest17178461...	S3 Bucket MFA Delete St...	Low	Ensures MFA delete is e...	Active	us-east-1
29	2024-08-21 07:06:01	pipeline-cdk-stack-pri...	S3 Object Read Logging...	Low	Ensure that Object-leve...	Active	us-east-1
29	2024-08-21 07:06:01	cf-templates-10aput4lj...	S3 Object Write Logging...	Low	Ensure that Object-leve...	Active	us-east-1
29	2024-08-21 07:06:01	knoxlivantestest1718109...	S3 Transfer Acceleratio...	Medium	Ensures that S3 buckets...	Active	us-east-1
28	2024-08-21 09:01:50	knoxtestnessus171782191...	IAM User Has Tags: glob...	Low	Ensure that AWS IAM Us...	Active	global

Total Records: 1041

How to create single ticket for Multiple assets affected by single finding and vice-versa? [1b]



Link

https://accu-knox.atlassian.net/browse/JIRATEST-2697

Ticket Description

Description Ensure that Object-level logging for read events is enabled for S3 bucket.

Synopsis

Impacted Assets

Asset	Port
knoxlivanteatest1718109052-9-1718194082-librarian	us-east-1
knoxtestaccu1717744509-5-1718194016-librarian	us-east-1
pipeline-cdk-stack-private5gpipelineartifactsbucke-juulwkupq27w	us-east-1
knoxprudent1720165686-15-1720180323-librarian	us-east-1
knoxtestaccu1717744509-5-1718194126-librarian	us-east-1
livantatest-2-1712570969-librarian	us-east-1
pipeline-cdk-stack-private5gpipelineartifactsbucke-3d2ss83cssdq	us-east-1
cf-templates-104put41jbsy-us-east-1	us-east-1
knoxtestnessus1717821910-6-1718194033-librarian	us-east-1
pipeline-cdk-stack-private5gpipelineartifactsbucke-q8dd6lag0ifq	us-east-1
knoxtestnessus1717821910-6-1718194142-librarian	us-east-1
kapp.accuknox.com	us-east-1

Projects / JIRAINTEGRATIONTEST / Add parent / JIRATEST-2697

S3 Object Read Logging: us-east-1

+

Description

Description

Ensure that Object-level logging for read events is enabled for S3 bucket.

Synopsis

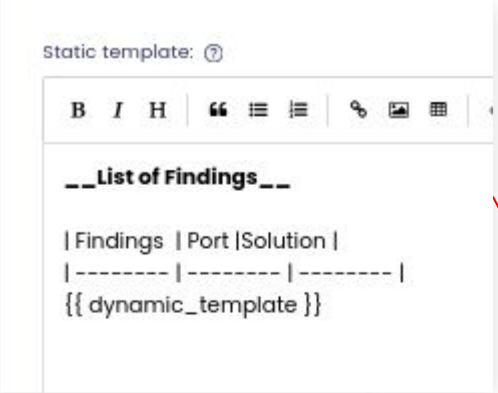
Impacted Assets

Asset	Port
knoxlivanteatest1718109052-9-1718194082-librarian	us-east-1
knoxtestaccu1717744509-5-1718194016-librarian	us-east-1
pipeline-cdk-stack-private5gpipelineartifactsbucke-juulwkupq27w	us-east-1

How to create single ticket for Multiple assets affected by single finding and vice-versa? [2]

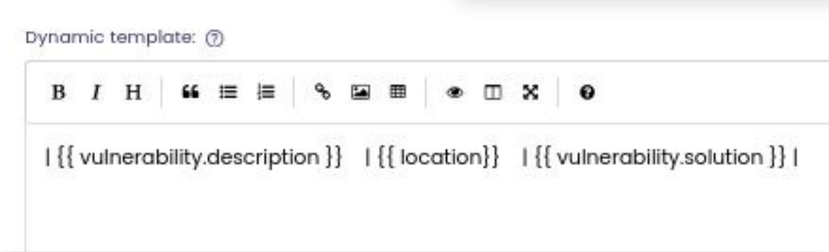
- Create ticket template and link it to the configuration.
- In the findings page add **Group by Findings** filter, click on the finding then select all the **Findings > Create Ticket.**
- Select the config with appropriate ticket template to create ticket

GROUP BY ASSETS



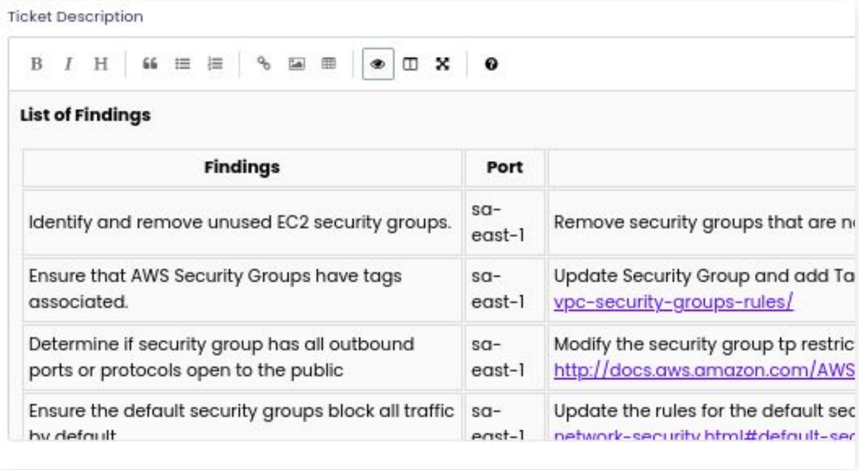
Static template:

```
__List of Findings__

| Findings  | Port |Solution |
| -------- | -------- | -------- |
{{ dynamic_template }}
```



Dynamic template:

```
| {{ vulnerability.description }}  | {{ location}}  | {{ vulnerability.solution }} |
```

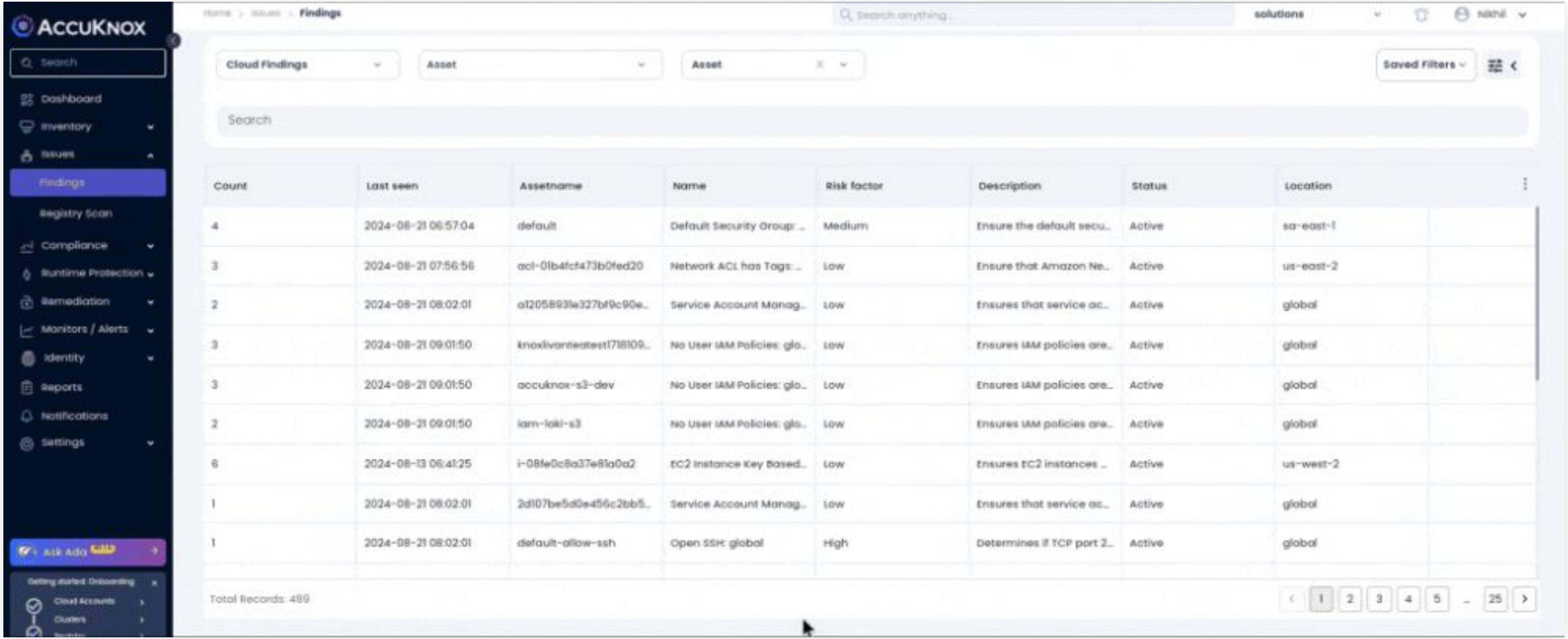


Ticket Description

List of Findings

Findings	Port	
Identify and remove unused EC2 security groups.	sa-east-1	Remove security groups that are n
Ensure that AWS Security Groups have tags associated.	sa-east-1	Update Security Group and add Ta vpc-security-groups-rules/
Determine if security group has all outbound ports or protocols open to the public	sa-east-1	Modify the security group tp restric http://docs.aws.amazon.com/AWS
Ensure the default security groups block all traffic by default	sa-east-1	Update the rules for the default sec network-security.html#default-sec

How to create single ticket for Multiple assets affected by single finding and vice-versa? [2a]



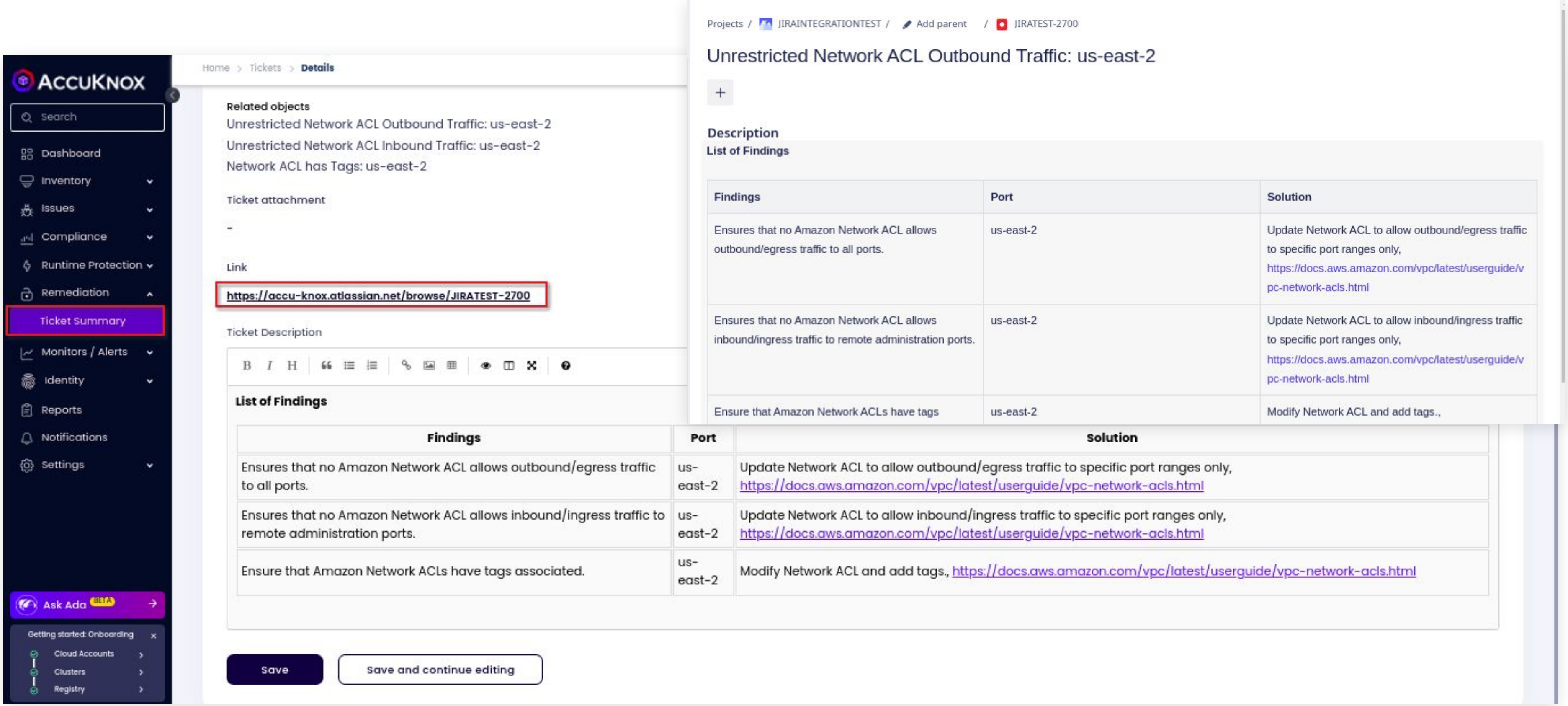
Cloud Findings | Asset | Asset

Count	Last seen	Assetname	Name	Risk factor	Description	Status	Location
4	2024-08-21 06:57:04	default	Default Security Group: ...	Medium	Ensure the default secu...	Active	sa-east-1
3	2024-08-21 07:56:56	acl-01b4fcf473b0fed20	Network ACL has Tags: ...	Low	Ensure that Amazon Ne...	Active	us-east-2
2	2024-08-21 08:02:01	a12058931e327bf9c90e...	Service Account Manag...	Low	Ensures that service ac...	Active	global
3	2024-08-21 09:01:50	knoxlivantestest1718109...	No User IAM Policies: glo...	Low	Ensures IAM policies are...	Active	global
3	2024-08-21 09:01:50	accuknox-s3-dev	No User IAM Policies: glo...	Low	Ensures IAM policies are...	Active	global
2	2024-08-21 09:01:50	iam-loki-s3	No User IAM Policies: glo...	Low	Ensures IAM policies are...	Active	global
6	2024-08-13 06:41:25	i-08fe0c8a37e81a0a2	EC2 Instance Key Based...	Low	Ensures EC2 instances ...	Active	us-west-2
1	2024-08-21 08:02:01	2d107be5d0e456c2bb5...	Service Account Manag...	Low	Ensures that service ac...	Active	global
1	2024-08-21 08:02:01	default-allow-ssh	Open SSH: global	High	Determines if TCP port 2...	Active	global

Total Records: 489

< 1 2 3 4 5 ... 25 >

How to create single ticket for Multiple assets affected by single finding and vice-versa? [2b]



Related objects

Unrestricted Network ACL Outbound Traffic: us-east-2

Unrestricted Network ACL Inbound Traffic: us-east-2

Network ACL has Tags: us-east-2

Ticket attachment

-

Link

https://accu-knox.atlassian.net/browse/JIRATEST-2700

Ticket Description

List of Findings

Findings	Port	Solution
Ensures that no Amazon Network ACL allows outbound/egress traffic to all ports.	us-east-2	Update Network ACL to allow outbound/egress traffic to specific port ranges only, https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html
Ensures that no Amazon Network ACL allows inbound/ingress traffic to remote administration ports.	us-east-2	Update Network ACL to allow inbound/ingress traffic to specific port ranges only, https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html
Ensure that Amazon Network ACLs have tags associated.	us-east-2	Modify Network ACL and add tags., https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html

Save
Save and continue editing
Projects / JIRAINTEGRATIONTEST / Add parent / JIRATEST-2700

Unrestricted Network ACL Outbound Traffic: us-east-2

Description

List of Findings

Findings	Port	Solution
Ensures that no Amazon Network ACL allows outbound/egress traffic to all ports.	us-east-2	Update Network ACL to allow outbound/egress traffic to specific port ranges only, https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html
Ensures that no Amazon Network ACL allows inbound/ingress traffic to remote administration ports.	us-east-2	Update Network ACL to allow inbound/ingress traffic to specific port ranges only, https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html
Ensure that Amazon Network ACLs have tags	us-east-2	Modify Network ACL and add tags.,