

## Prisma Cloud Overview

Prisma Cloud is a comprehensive cloud-native security platform with the industry's broadest security and compliance coverage. It protects cloud-native applications, data, networks, computing, storage, users, and higher-level PaaS services across cloud platforms. Prisma Cloud enables Cloud Security Posture Management (CSPM) and Cloud Workload Protection Platform (CWPP) for comprehensive visibility and threat detection across your organization's hybrid, multi-cloud infrastructure. It dynamically discovers resources as they are deployed and correlates cloud-service-provided data to enable security and compliance insights into your cloud applications and workloads.

**Background:** This example demonstrates how Prisma Cloud can be used to alert on suspicious network traffic, and how to analyze networks in the Prisma Cloud console.

**In this activity, you will:**

- Review out-of-the-box policies, queries, compliance standards, and remediations
- View a Network Alert for suspicious activity.
- Analyze the Network Visualization to trace resources that may have been impacted.
- View the traffic that is reaching your cloud workloads.
- Examine Vulnerabilities that have been detected on your cloud Workload to understand the risk posture.
- View Alert on risky AWS IAM Permissions.
- Analyze the current resource configuration settings.
- Analyze the change history for the IAM configuration settings (show how the resource got to its current state).
- View how Prisma Cloud remediation commands can be leveraged to remediate security findings.

**Note:** This is a standalone activity and is not dependent on other activities.

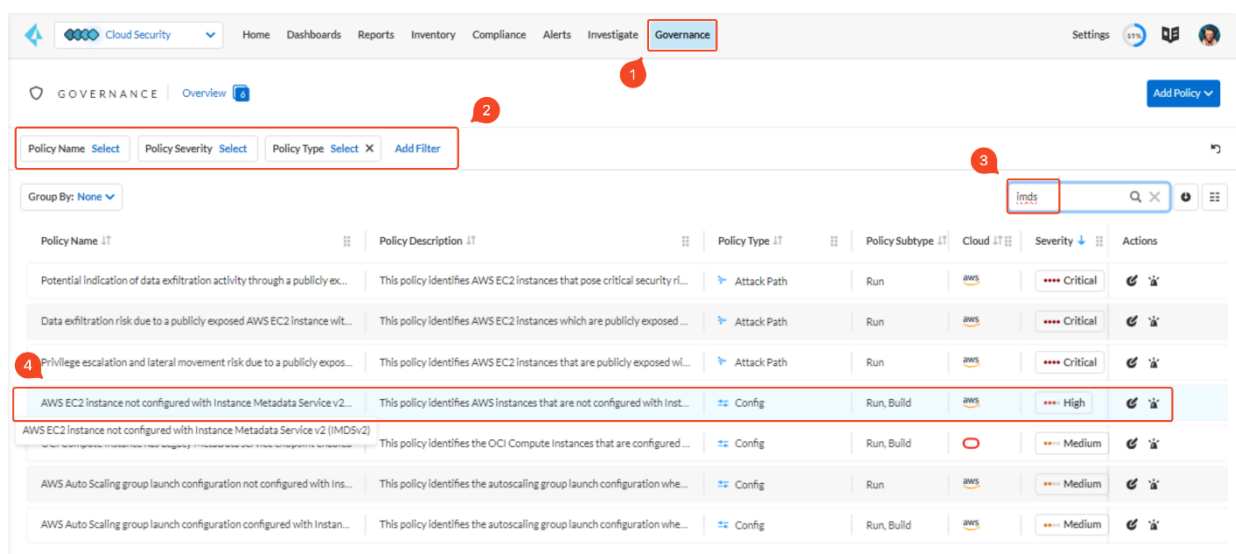
## - Task 1: Looking into Prisma Cloud Governance & Policy

In Prisma Cloud, a policy is a set of one or more constraints or conditions that must be adhered to. Prisma Cloud provides predefined policies for configurations and access controls that adhere to established security best practices such as Otoritas Jasa Keuangan (OJK) 38 POJK.03 206, PCI, GDPR, ISO 27001:2013, NIST, and a larger set of policies that enable you to validate security best practices with an impact beyond regulatory compliance. These Prisma Cloud default policies cannot be modified.

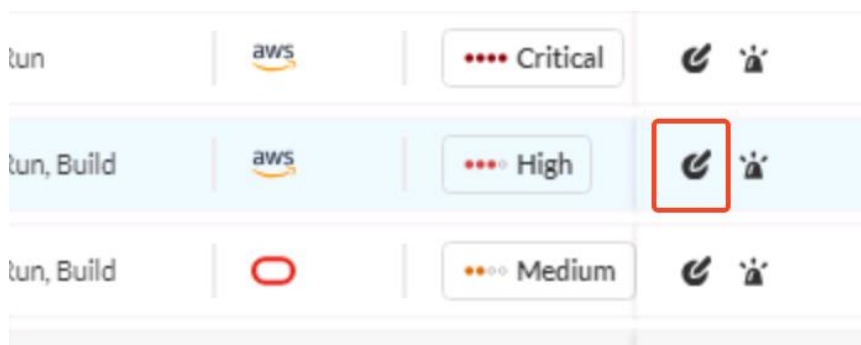
In addition to these predefined policies, you can create custom policies to monitor for violations and enforce your organizational standards. You can use the Default policies as templates to create custom policies. After you set up the policies, any new or existing resources that violate these policies are automatically detected.

Prisma Cloud includes out-of-the-box (OOTB) policies that are part of the Prisma Cloud Recommended Policies Pack.

**Step 1.** In Prisma Cloud Enterprise Edition, click on Governance.



**Step 2.** Make sure the filters are cleared, type in "imds" into the search bar, and click on the Edit icon for the policy "AWS EC2 instance not configured with Instance Metadata Service v2 (IMDSv2)".



**Step 3.** On the popped-out window, run through the policy description, then click Next.

**Step 4:** On the query section, notice that the query has been configured as this is an OOTB policy. Then, click Next.

Standard	Requirement	Section
ISO/IEC 27001:2022	Organisational Controls	A5.10
Secure Controls Framework (SCF) - ...	Network Security	NET-04.10
MITRE ATT&CK v14.0 Cloud IaaS fo...	TA0007	T1580 - Cloud Infrastructure Disco...
RBI Baseline Cyber Security and Re...	Data Leak prevention strategy	15.3
ISO 27002:2022	Organizational controls	5.10
New Zealand Information Security ...	19	19.1
MITRE ATT&CK v10.0	TA0007	T1580 - Cloud Infrastructure Disco...
ISO/IEC 27001:2022	Technological Controls	A8.3
ISO 27002:2022	Technological controls	8.3

**Step 5.** In the remediation section, the recommendation for Remediation has been provided as a manual procedure to remediate if there is a policy violation. CLI command has also been configured, where a CLI command will be provided to remediate the misconfiguration if there is a violation. Click "X" to close the window.

## Prisma Cloud Compliance Overview

The Compliance Overview is a dashboard that provides a snapshot of your overall compliance posture across various compliance standards.

Use the Compliance Dashboard as a tool for risk oversight across all the supported cloud platforms and gauge the effectiveness of the security processes and controls you have implemented to keep your enterprise secure. You can also create compliance reports and run them immediately, or schedule them regularly to measure your compliance over time.

The Compliance Dashboard supports you whether you've spent a lot of time designing and establishing internal regulations and devising the right policies, or you use the built-in regulatory compliance standards available on Prisma Cloud.

You can also find the list of compliance standards that Prisma Cloud supports [here](#)

In this activity, you will:

- Review Compliance Overview in Prisma Cloud Enterprise Edition
- Schedule and generate compliance reports for internal consumption

**Note:** This is a standalone activity and is not dependent on other activities.

**Step 1.** Go to Prisma Cloud Enterprise > Cloud Security > Compliance

**Step 2.** Here you can see a list of compliance standards supported by Prisma Cloud out of the box:

The screenshot shows the 'Compliance' section of the Prisma Cloud interface. The 'Standards' tab is selected, showing a list of compliance standards. The table has columns for Name, Description, Clouds, and Policies Assigned. The data is as of 47 minutes ago.

Name	Description	Clouds	Policies Assigned
CIS v1.0.0 (Alibaba Cloud)	CIS Alibaba Cloud Foundation Benchmark v.1.0.0		19
CIS v1.0.0 (OCI)	CIS Oracle Cloud Infrastructure Foundations Benchmark v.1.0.0		24
CIS v1.1.0 (GKE)	CIS Google Kubernetes Engine Foundation Benchmark v.1.1.0		23
CIS v1.1.0 (OCI)	CIS Oracle Cloud Infrastructure Foundations Benchmark v.1.1.0		23

**Step 3.** Type "NIST" in the search bar in the top right corner to filter the compliance standards. Click on "NIST SP 800-171 Revision 2".

The screenshot shows the 'Compliance' section with the search bar in the top right corner containing the text 'NIST'. The table displays filtered results for NIST standards. The data is as of 50 minutes ago.

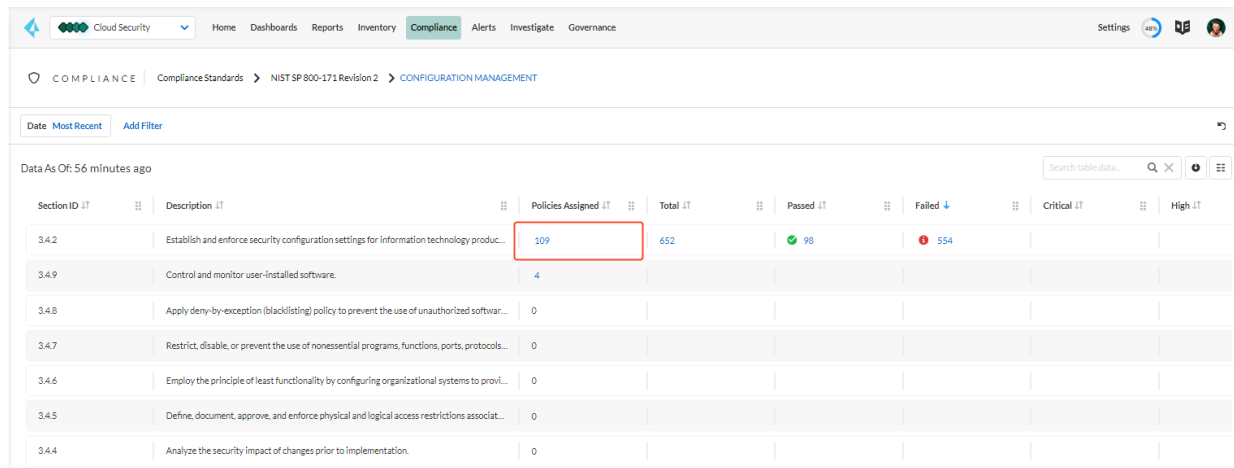
Name	Description	Clouds	Policies Assigned	Total	Passed	Failed
NIST 800-171 Rev1	NIST 800-171 Rev1 Compliance Standard		63	389	119	270
NIST 800-53 Rev5	NIST Special Publication 800-53 Revision 5		312	752	284	468
NIST 800-53 Rev4	NIST 800-53 Rev4 Compliance Standard		374	765	283	482
NIST SP 800-171 Revision 2	NIST Special Publication 800-171 Revision 2		537	1,562	585	977
NIST SP 800-172	NIST Special Publication 800-172		537	1,562	585	977

**Step 4.** On the next page, you can see how the compliance standard is being structured. This is based on the actual compliance requirement, and Prisma Cloud maps the policies according to each section of the compliance requirement. Click on "CONFIGURATION MANAGEMENT".

The screenshot shows the 'Compliance Standards' page for 'NIST SP 800-171 Revision 2'. The 'CONFIGURATION MANAGEMENT' requirement is highlighted. The table displays the structure of the compliance requirement, showing Requirement ID, Description, Policies Assigned, and Total. The data is as of 52 minutes ago.

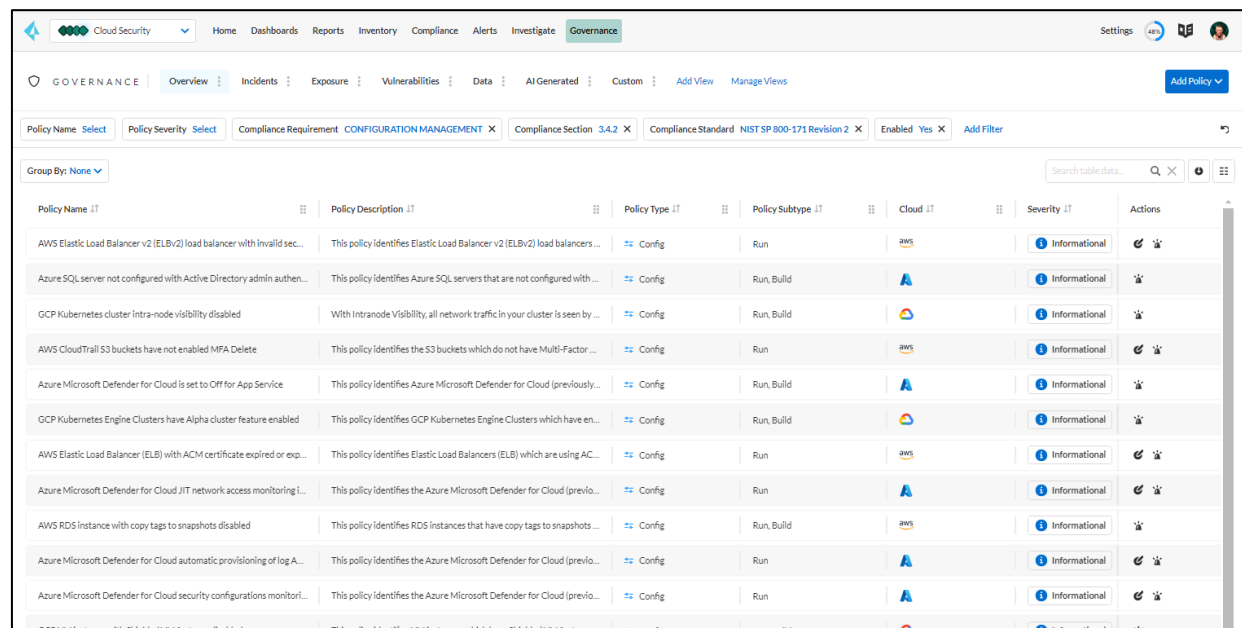
Name	Requirement ID	Description	Policies Assigned	Total
CONFIGURATION MANAGEMENT	3.4	CONFIGURATION MANAGEMENT	113	652
SYSTEM AND COMMUNICATIONS PROTECTION	3.13	SYSTEM AND COMMUNICATIONS PROTECTION	189	537
AUDIT AND ACCOUNTABILITY	3.3	AUDIT AND ACCOUNTABILITY	67	234
SYSTEM AND INFORMATION INTEGRITY	3.14	SYSTEM AND INFORMATION INTEGRITY	127	214
ACCESS CONTROL	3.1	ACCESS CONTROL	82	556
MAINTENANCE	3.7	MAINTENANCE	14	3

**Step 5.** On the next page, you can also see how policies are mapped to each sub-section of the compliance standard. Click on the numbers under **Policies Assigned**, the same row as section 3.4.2.



Section ID	Description	Policies Assigned	Total	Passed	Failed	Critical	High
3.4.2	Establish and enforce security configuration settings for information technology produc...	109	652	98	554		
3.4.9	Control and monitor user-installed software.	4					
3.4.8	Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized softwar...	0					
3.4.7	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols...	0					
3.4.6	Employ the principle of least functionality by configuring organizational systems to provi...	0					
3.4.5	Define, document, approve, and enforce physical and logical access restrictions associat...	0					
3.4.4	Analyze the security impact of changes prior to implementation.	0					

**Step 6.** On the next page, you will be able to see all the policies that are mapped to this particular sub-section. This allows you to understand how all the policies are built into the compliance requirement and how Prisma Cloud can assist organizations with their compliance with certain standards or regulatory requirements.



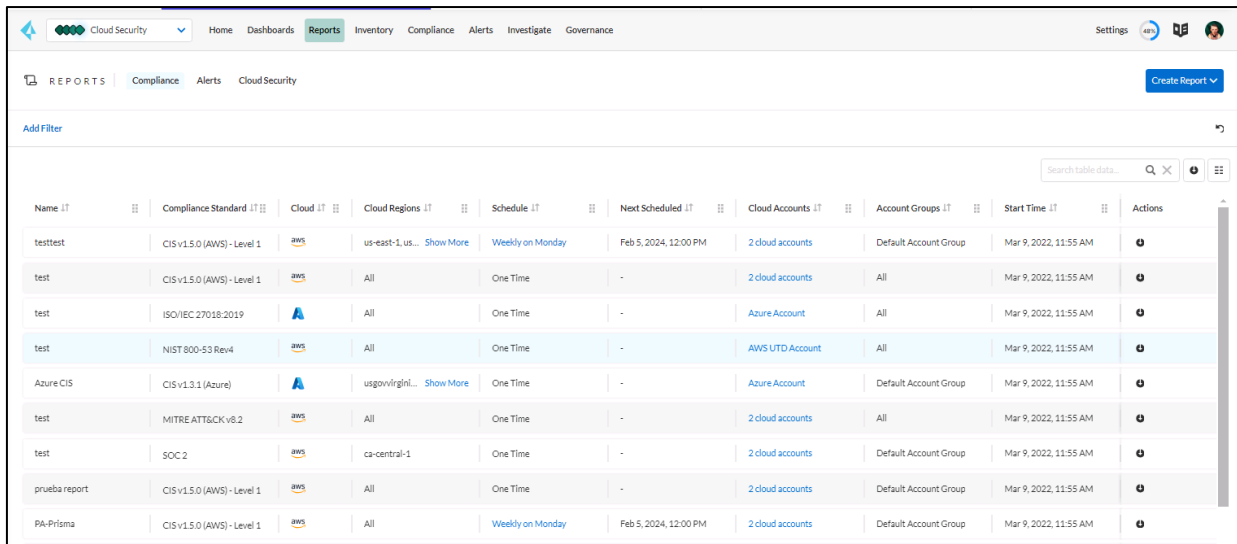
Policy Name	Policy Description	Policy Type	Policy Subtype	Cloud	Severity	Actions
AWS Elastic Load Balancer v2 (ELBv2) load balancer with invalid sec...	This policy identifies Elastic Load Balancer v2 (ELBv2) load balancers ...	Config	Run	AWS	Informational	
Azure SQL server not configured with Active Directory admin authen...	This policy identifies Azure SQL servers that are not configured with ...	Config	Run, Build	Azure	Informational	
GCP Kubernetes cluster intra-node visibility disabled	With Intranode Visibility, all network traffic in your cluster is seen by ...	Config	Run, Build	GCP	Informational	
AWS CloudTrail S3 buckets have not enabled MFA Delete	This policy identifies the S3 buckets which do not have Multi-Factor ...	Config	Run	AWS	Informational	
Azure Microsoft Defender for Cloud is set to Off for App Service	This policy identifies Azure Microsoft Defender for Cloud (previo...	Config	Run, Build	Azure	Informational	
GCP Kubernetes Engine Clusters have Alpha cluster feature enabled	This policy identifies GCP Kubernetes Engine Clusters which have en...	Config	Run, Build	GCP	Informational	
AWS Elastic Load Balancer (ELB) with ACM certificate expired or exp...	This policy identifies Elastic Load Balancers (ELB) which are using AC...	Config	Run	AWS	Informational	
Azure Microsoft Defender for Cloud JIT network access monitoring i...	This policy identifies the Azure Microsoft Defender for Cloud (previ...	Config	Run	Azure	Informational	
AWS RDS instance with copy tags to snapshots disabled	This policy identifies RDS instances that have copy tags to snapshots ...	Config	Run, Build	AWS	Informational	
Azure Microsoft Defender for Cloud automatic provisioning of log A...	This policy identifies the Azure Microsoft Defender for Cloud (previ...	Config	Run	Azure	Informational	
Azure Microsoft Defender for Cloud security configurations monitori...	This policy identifies the Azure Microsoft Defender for Cloud (previ...	Config	Run	Azure	Informational	
GCP VM instances with Shared VM features disabled	This policy identifies VM instances which have Shared VM features...	Config	Run, Build	GCP	Informational	

## Download Compliance Report

**Note:** The lab uses a read-only user, which doesn't have access to generate a compliance report. Therefore, we'll only run through the steps to download a compliance report.

**Step 1.** Go to **Prisma Cloud Enterprise > Cloud Security > Reports**

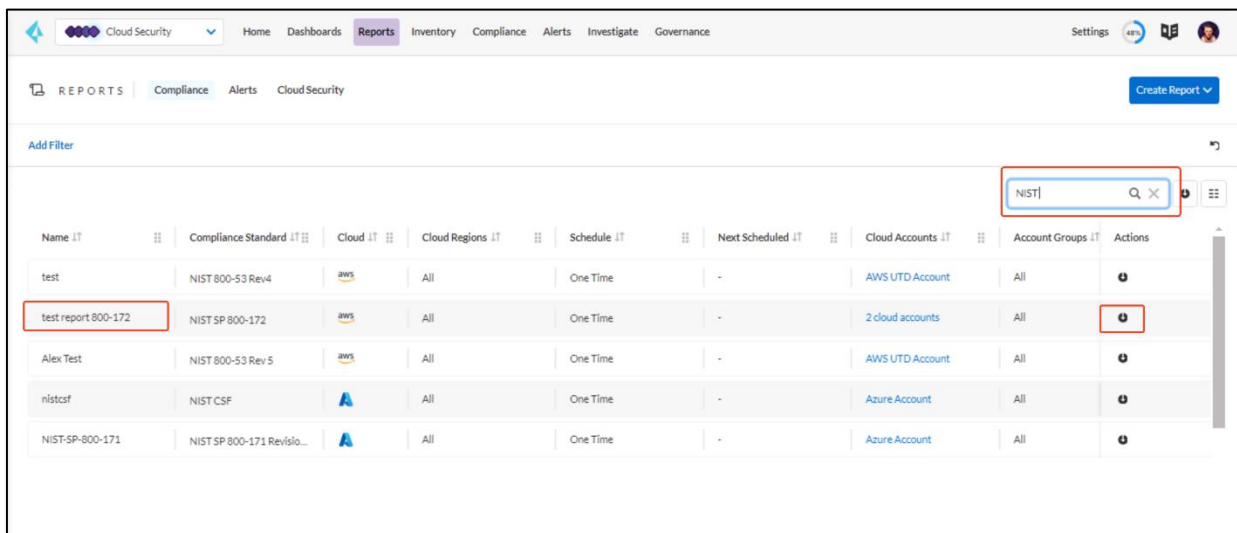
**Step 2.** On this page, you will see all the different reports created by existing users or yourself, either for one-time usage or a regular schedule.



The screenshot shows the Prisma Cloud Reports page. The top navigation bar includes Home, Dashboards, Reports (selected), Inventory, Compliance, Alerts, Investigate, and Governance. Below the navigation bar, there are tabs for REPORTS, Compliance, Alerts, and Cloud Security. A search bar is present with the text "Search table data...". The main table lists various compliance reports with columns for Name, Compliance Standard, Cloud, Cloud Regions, Schedule, Next Scheduled, Cloud Accounts, Account Groups, Start Time, and Actions.

Name	Compliance Standard	Cloud	Cloud Regions	Schedule	Next Scheduled	Cloud Accounts	Account Groups	Start Time	Actions
testtest	CIS v1.5.0 (AWS) - Level 1	aws	us-east-1, us... <a href="#">Show More</a>	Weekly on Monday	Feb 5, 2024, 12:00 PM	2 cloud accounts	Default Account Group	Mar 9, 2022, 11:55 AM	
test	CIS v1.5.0 (AWS) - Level 1	aws	All	One Time	-	2 cloud accounts	All	Mar 9, 2022, 11:55 AM	
test	ISO/IEC 27018:2019	A	All	One Time	-	Azure Account	All	Mar 9, 2022, 11:55 AM	
test	NIST 800-53 Rev4	aws	All	One Time	-	AWS UTD Account	All	Mar 9, 2022, 11:55 AM	
Azure CIS	CIS v1.3.1 (Azure)	A	usgovvirgini... <a href="#">Show More</a>	One Time	-	Azure Account	Default Account Group	Mar 9, 2022, 11:55 AM	
test	MITRE ATT&CK v8.2	aws	All	One Time	-	2 cloud accounts	All	Mar 9, 2022, 11:55 AM	
test	SOC 2	aws	ca-central-1	One Time	-	2 cloud accounts	Default Account Group	Mar 9, 2022, 11:55 AM	
prueba report	CIS v1.5.0 (AWS) - Level 1	aws	All	One Time	-	2 cloud accounts	Default Account Group	Mar 9, 2022, 11:55 AM	
PA-Prisma	CIS v1.5.0 (AWS) - Level 1	aws	All	Weekly on Monday	Feb 5, 2024, 12:00 PM	2 cloud accounts	Default Account Group	Mar 9, 2022, 11:55 AM	

**Step 3.** On the search bar, type "NIST". Click on the **Download** icon in the Action column to download the report.



The screenshot shows the Prisma Cloud Reports page with a search filter applied. The search bar contains the text "NIST". The table lists reports filtered by "NIST". The row for "test report 800-172" is highlighted, and the download icon in the Actions column is circled in red.

Name	Compliance Standard	Cloud	Cloud Regions	Schedule	Next Scheduled	Cloud Accounts	Account Groups	Actions
test	NIST 800-53 Rev4	aws	All	One Time	-	AWS UTD Account	All	
test report 800-172	NIST SP 800-172	aws	All	One Time	-	2 cloud accounts	All	
Alex Test	NIST 800-53 Rev 5	aws	All	One Time	-	AWS UTD Account	All	
nistcsf	NIST CSF	A	All	One Time	-	Azure Account	All	
NIST-SP-800-171	NIST SP 800-171 Revisio...	A	All	One Time	-	Azure Account	All	

**Note:** As you're accessing Prisma Cloud via a full-screen remote desktop, you might not be able to view the downloaded document. For a NIST sample report, refer to a sample document [here](#).

**Note:** You can schedule a compliance report to be sent to specific teams in regular basis (weekly, daily, etc).

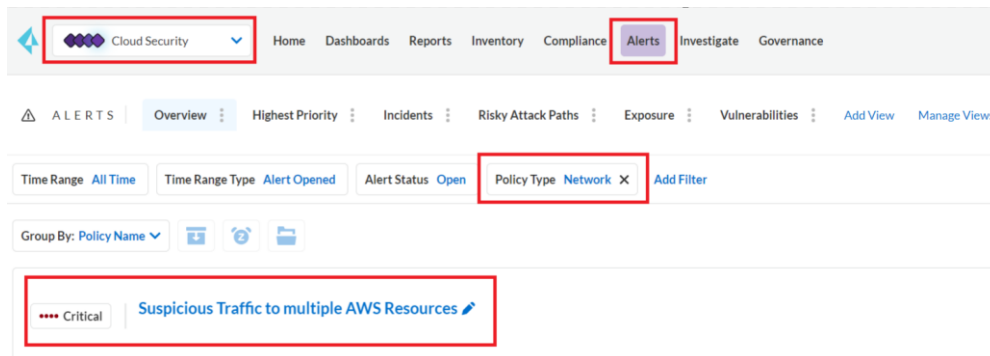
## Task 2: Examine a Network Alert

**Step 1.** In the Prisma Cloud Enterprise Edition console, click the **Alerts** tab and then **Overview**.

**Step 2.** Select the **Reset Filters** icon on the top right corner of the screen to reset all filters and set the **Time Range** to **All Time**.

**Step 3.** Click on the **Add Filter** icon and select the following options and look for the alert **Suspicious Traffic to Multiple AWS Resources**:

- Alert Status = **Open**
- Policy Type = **Network**
- Cloud Account = **AWS UTD Account**



**Step 4.** Here you can see a list of resources causing this alert to fire.

\*\*\* Critical

Suspicious Traffic to multiple AWS Resources

Dismiss

Snooze

Remediate

Reopen

Investigate

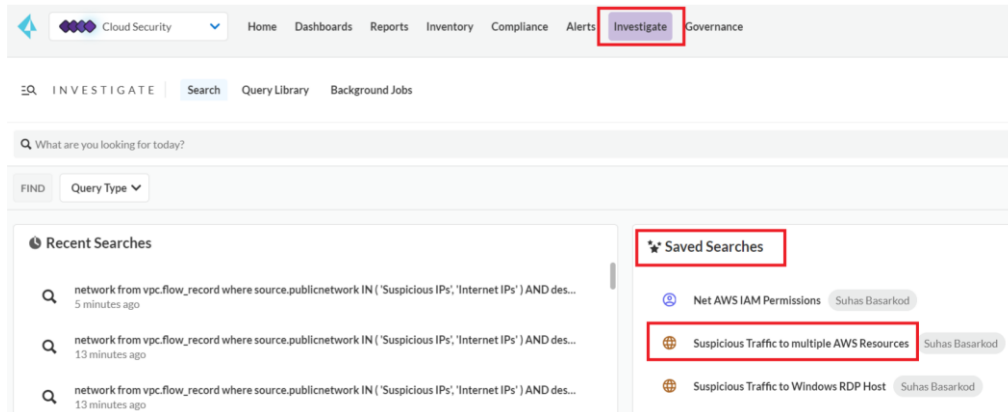
Asset Name		Alert ID		Alert Time		Account ID		Account		Alert Status		Region
PANW-WebServe...		P-52811		12 hours ago		577142504549		AWS Account		open		AWS Virginia
Linux-EC2-1		P-52110		12 hours ago		577142504549		AWS Account		open		AWS Virginia
LinuxBastion		P-52725		12 hours ago		577142504549		AWS Account		open		AWS Virginia
Linux-EC2-2		P-52206		12 hours ago		577142504549		AWS Account		open		AWS Virginia

Load More

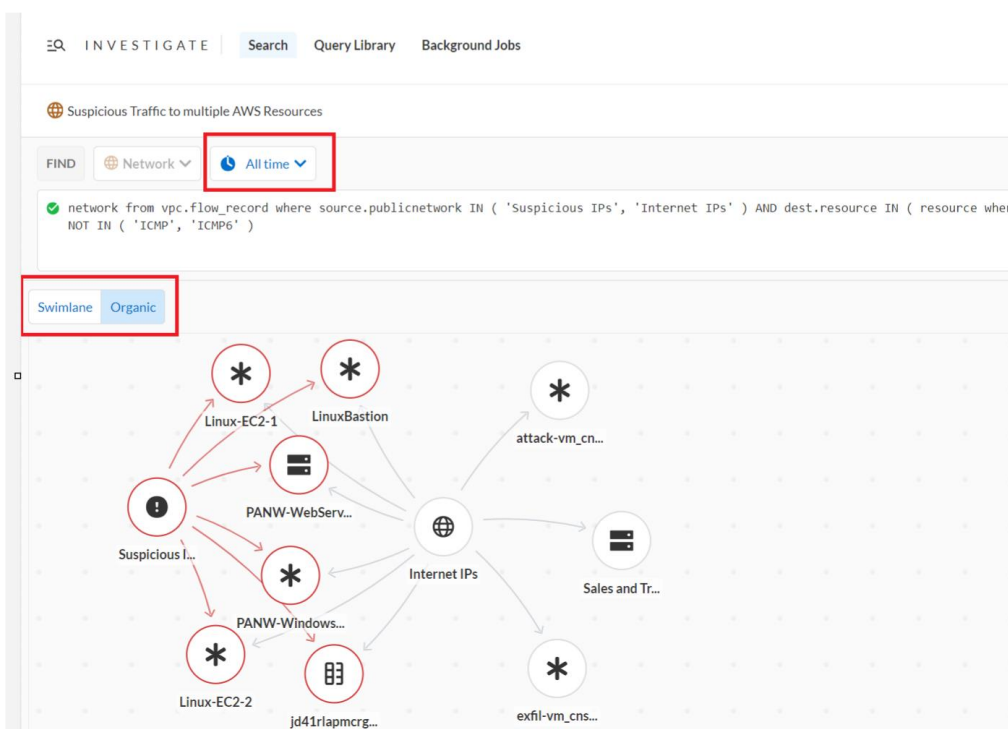
Displaying 1 - 4 of 4 (All records loaded)

### Task 3: Examine the Traffic from Suspicious IPs

**Step 1.** Head over to the **Investigate** window. For your convenience, we have already created a query to list out the resources for the previous alert. To use that, within the **Saved Searches**, select **Suspicious Traffic to multiple AWS Resources**

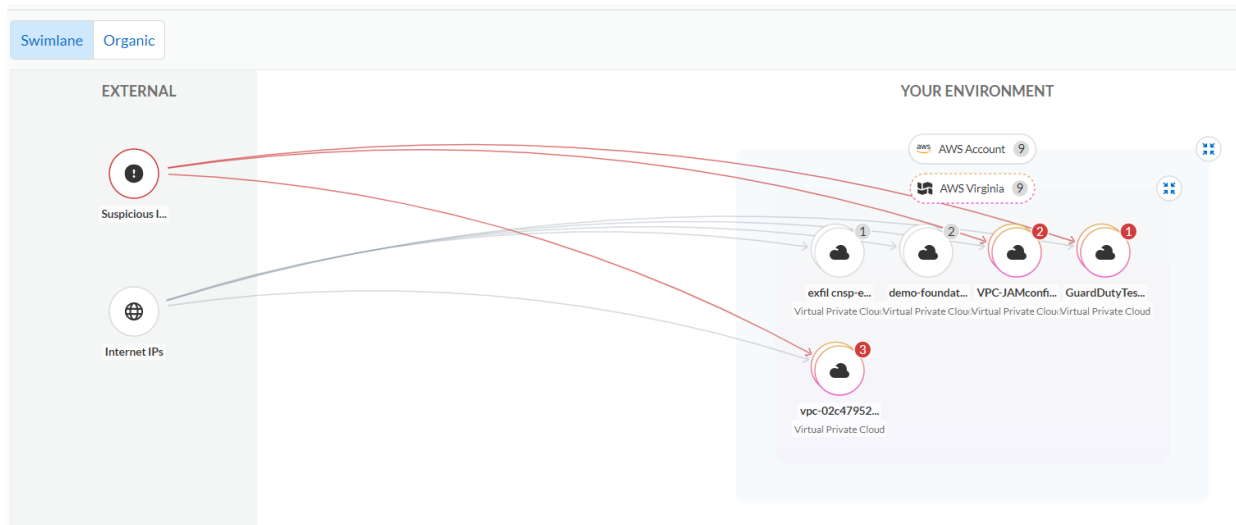


**Step 2.** Make sure to set the time window to **All Time**. Your graph may look a little different as the cloud environment is very dynamic. This shows all the resources that are taking traffic from Suspicious IPs, which are flagged by Prisma Cloud.

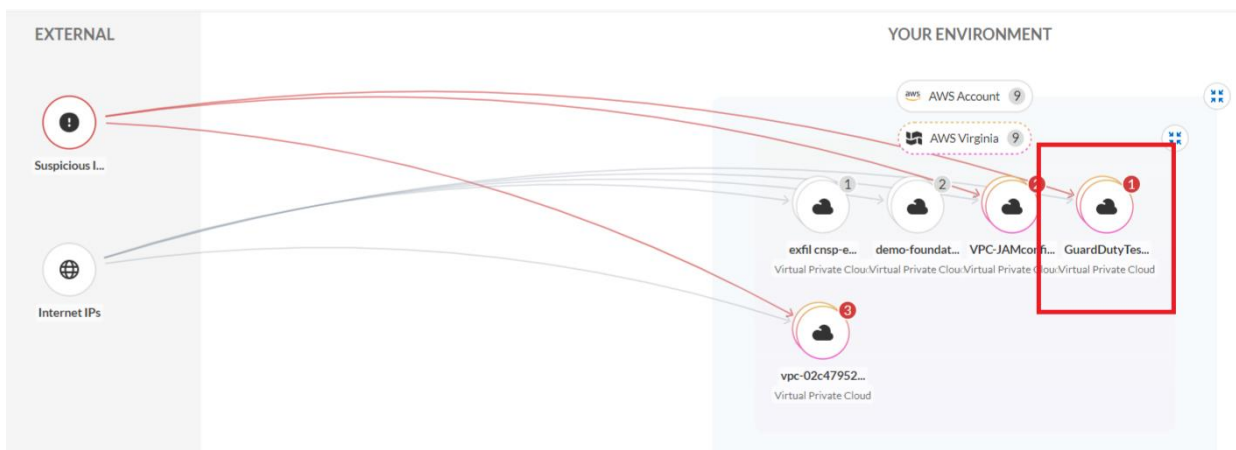




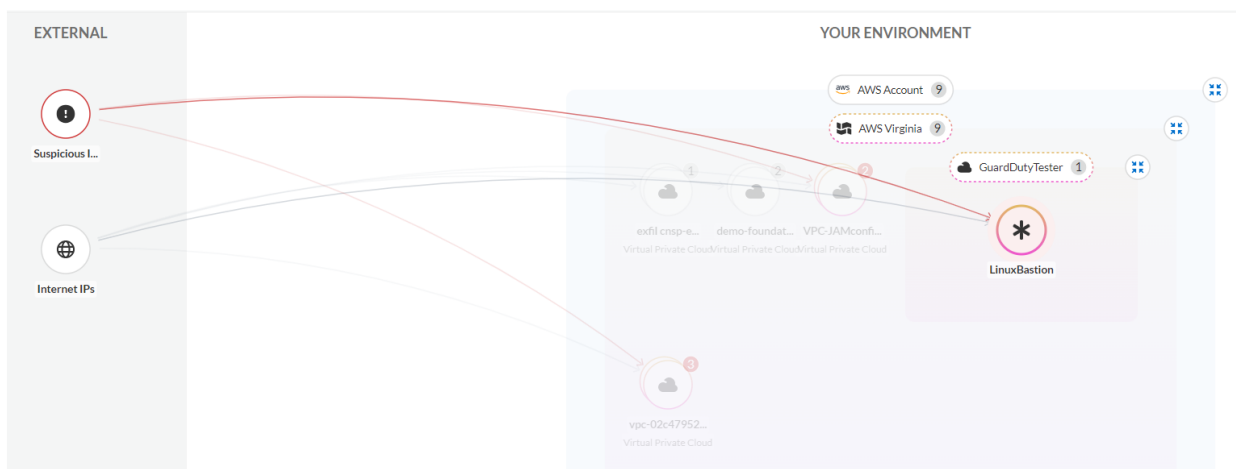
**Step 3.** Toggle between **Swimlane** and **Organic** for different visualizations of the traffic.



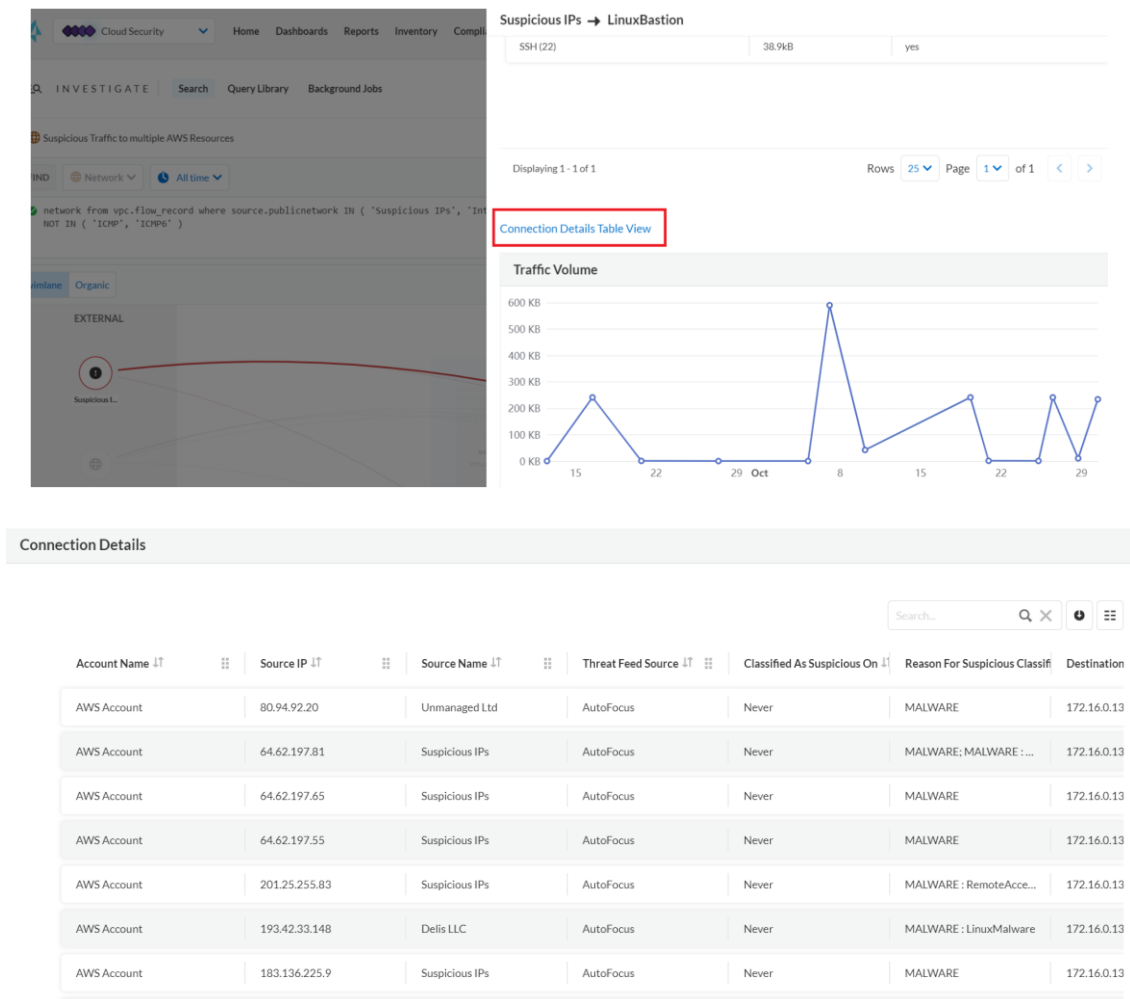
**Step 4.** For the rest of the flow, we will stick with **Swimlane** visualization. Clicking on the **GuardDuty Tester** VPC will expand it and reveal **LinuxBastion** host



**Step 5.** Hover your mouse and click on the line connecting **Suspicious IP** and **Linux Bastion**

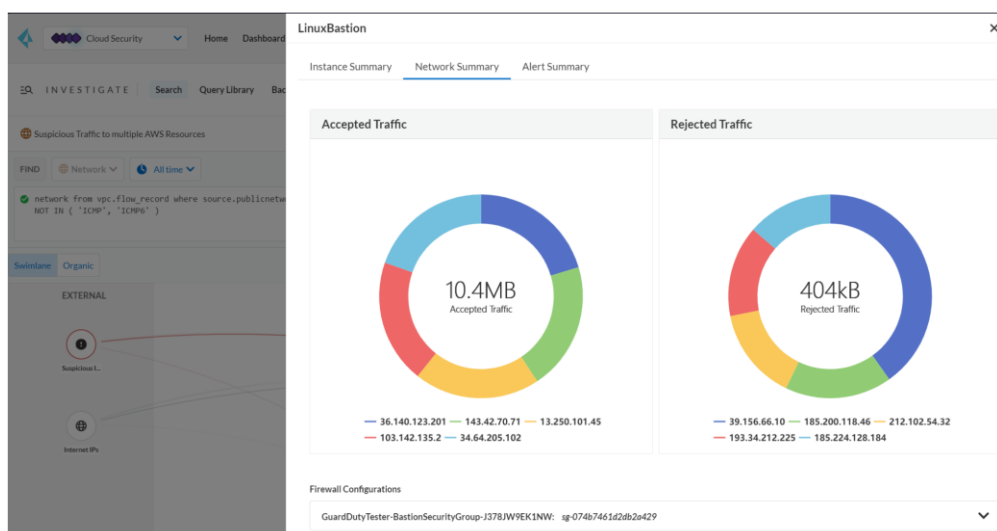


**Step 6.** This will open a sidecar. Click on the **Connection Details Table view** to see the breakdown of the traffic flow between **suspicious IPs** and the **LinuxBastion** host



**Step 7.** Close the **Connection Details** window and the **Suspicious IPs > LinuxBastion** window.

**Step 8.** Click on the **LinuxBastion** host and this will open another window that provides the network summary of that VM.



**Step 9.** Click on the **LinuxBastion** VM, and under the **Instance Summary**, click the value corresponding to **Asset ID** to investigate further the VM. Go to the **Findings** tab at the top of the page to get details.

LinuxBastion ×

[Instance Summary](#)
[Network Summary](#)
[Alert Summary](#)

Asset ID i-03ab3b72a2044dd79

Instance Roles & Groups VM Instance SSH

LinuxBastion View Config ×

EC2 Instance

Findings Types ⓘ

AWS GuardDuty Host
Internet Exposure
Misconfiguration
High Privileged Role
Reconnaissance
+1 more

[Overview](#)
[Attack Paths](#)
[Audit Trail](#)
[Alerts \(13\)](#)
[Findings](#)
[Vulnerabilities \(0\)](#)
[IAM Details](#)
[Relationships](#)
[Objects](#)

You are viewing the most recent data about this asset

Type: All Type(s) Selected
Severity: All Severity Selected
Source: All Source Selected

🔍
✕
🔄
☰

Name ↕	Description ↕	Source ↕	Type ↕	Severity ↑	Actions
AWS EC2 instance that is inte...	This policy identifies AWS EC...	Prisma Cloud	Internet Exposure	High	
AWS EC2 instance not configu...	This policy identifies AWS inst...	Prisma Cloud	Misconfiguration	High	
AWS EC2 instance that is inte...	This policy identifies AWS EC...	Prisma Cloud	Internet Exposure	High	
AWS EC2 with IAM wildcard r...	This policy identifies AWS IA...	Prisma Cloud	High Privileged Role	Medium	

## Task 4: Investigate Risky AWS EC2 IAM Permissions

**Step 1.** Navigate to Prisma Cloud Enterprise Edition console > Cloud Security > Alerts > Overview.

**Step 2.** Select the **Reset Filters** icon on the top right corner of the screen to reset all filters. Use **Add Filter** option to add the specified filters below

**Step 3.** In the filter options, select the following:

- Time Range = **All Time**
- Alert Status = **Open**
- Policy Severity = **High**
- Policy Type = **IAM**
- Policy Name = **AWS EC2 instance with data destruction permissions**

**Step 4.** Navigate to Prisma Cloud Enterprise Edition console > Cloud Security > Alerts > Overview.

The screenshot shows the Prisma Cloud Alerts Overview page. Red boxes and numbers indicate the following elements:

- 1: Cloud Security dropdown menu
- 2: Alerts tab in the top navigation bar
- 3: Overview tab in the sub-navigation bar
- 4: Time Range filter set to All Time
- 5: Alert Status filter set to Open
- 6: Policy Severity filter set to High
- 7: Policy Type filter set to IAM
- 8: Policy Name filter set to AWS EC2 instance with data destruction permissions

The main content area shows a list of alerts, with the first alert highlighted: AWS EC2 instance with data destruction permissions, High severity, Privilege Escalation type.

**Step 5.** Click on the **AWS EC2 instance with data destruction permissions** and Click on the value under the **Asset Name** column to view more information about the resource.

The screenshot shows the details page for the alert 'AWS EC2 instance with data destruction permissions'. It displays a table of alerts with columns: Asset Name, Alert ID, Alert Time, Account ID, Account, Alert Status, and Region. The first row is highlighted, showing the asset name 'i-094838c8bdc105147'.

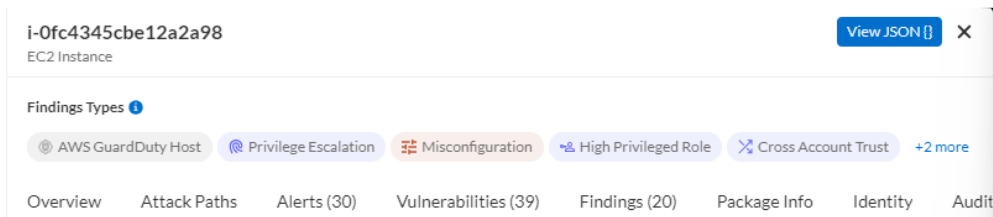
Asset Name	Alert ID	Alert Time	Account ID	Account	Alert Status	Region
i-094838c8bdc105147	I-52710	23 hours ago	577142504549	AWS Account	open	AWS Virginia
i-0c49516a46bc1...	I-52200	23 hours ago	577142504549	AWS Account	open	AWS Virginia

The screenshot shows the details page for the EC2 instance 'i-094838c8bdc105147'. It displays the instance's configuration, including its name, ID, type, cloud type, and service. The instance is an EC2 Instance, running on AWS, and is an Amazon EC2 service.

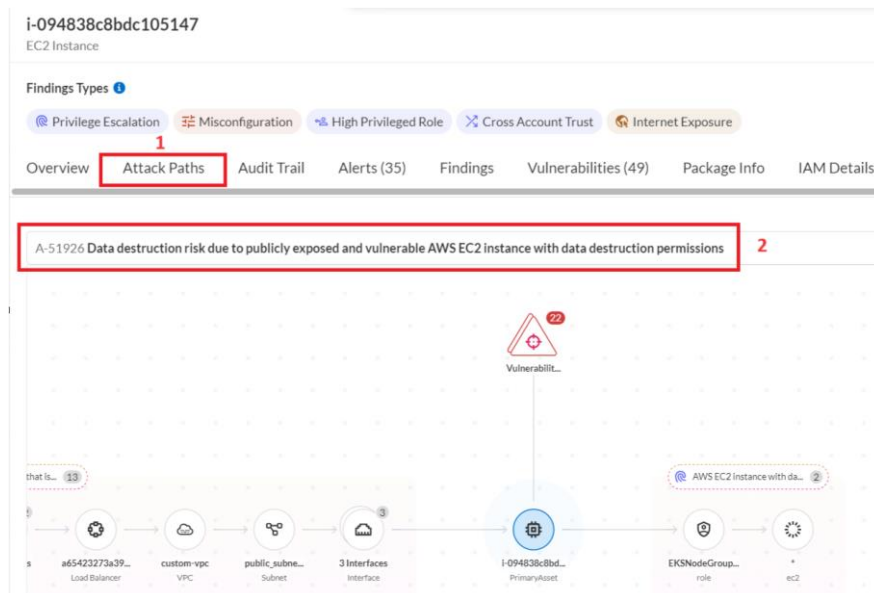
Details	
Name	i-094838c8bdc105147
Asset ID	i-094838c8bdc105147
Asset Type	EC2 Instance
Cloud Type	AWS
Service	Amazon EC2

**Step 6.** In the Resource sidebar, click on the below options to explore further.

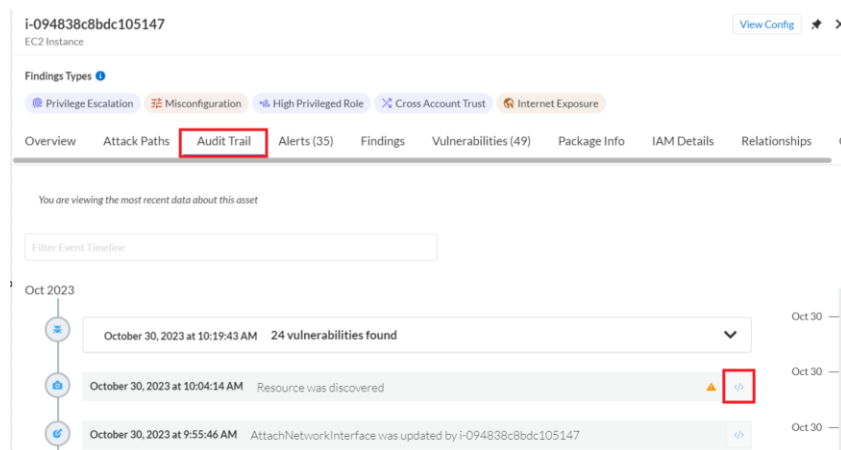
- a) Clicking on **View JSON** will bring up the configuration of the selected resource.



- b) Clicking on **Overview** will provide an overview of the resource. After reviewing, close the pop-up or click **Done**.
- c) Clicking on **Attack Paths** will bring up the attack path graph and highlight where the selected resource fits in the path. Further clicking on the various items within the graph will show relevant information and configuration of the selected item



- d) Clicking on the **Audit Trail** will open up the Audit trail for this resource where you will be able to see the timeline of the configuration changes made on the resource from the time it was discovered by Prisma Cloud. This is continuously monitored by Prisma Cloud and any changes to the configuration are recorded. Click on the **</>** to view the resource configuration



- e) Clicking on **Alerts** will show the various alerts that are open for this specific resource.

i-094838c8bdc105147  
EC2 Instance

Findings Types ⓘ

Privilege Escalation Misconfiguration High Privileged Role Cross Account Trust Internet Exposure

Overview Attack Paths Audit Trail **Alerts (35)** Findings Vulnerabilities (49) Package Info

- f) Clicking on **Findings** will show the various findings about the selected resource and the severity of those findings.

i-094838c8bdc105147  
EC2 Instance

Findings Types ⓘ

Privilege Escalation Misconfiguration High Privileged Role Cross Account Trust Internet Exposure

Overview Attack Paths Audit Trail Alerts (35) **Findings** Vulnerabilities (49) Package Info IAM Details

You are viewing the most recent data about this asset

Type Severity Source

All Type(s) Selected All Severity Selected All Source Selected

Search...

Name ↑	Description ↑	Source ↑	Type ↑	Severity ↑
AWS EC2 instance not configu...	This policy identifies AWS inst...	Prisma Cloud	Misconfiguration	High
AWS EC2 instance with IAM ...	This policy identifies IAM writ...	Prisma Cloud	High Privileged Role	High
AWS EC2 instance with data d...	With access to 's3:DeleteBuck...	Prisma Cloud	Privilege Escalation	High

- g) Clicking on the **Vulnerabilities** will show the various vulnerabilities that were detected for this resource. Further clicking on options such as **Critical & High**, **Exploitable** and **Patchable** will filter the results.

i-094838c8bdc105147  
EC2 Instance

Findings Types ⓘ

Privilege Escalation Misconfiguration High Privileged Role Cross Account Trust Internet Exposure

Overview Attack Paths Audit Trail Alerts (35) Findings **Vulnerabilities (49)** Package Info IAM Details Relationships Obj

You are viewing the most recent data about this asset

52 Total vulnerabilities

31 Critical & High 2 Exploitable 2 Patchable

9.8 Highest CVSS

Vulnerability Severity Critical, High Risk Factors Exploit exists - POC, Exploit exists - in the wild Add Filter

CVE Package 2 CVEs

Search... Sort By: CVSS

9.1 CVE-2022-1996	1 Package	1 patch
7.0 CVE-2023-27561	1 Package	1 patch

h) Feel free to explore the rest of the options and once done, close the window.



**Step 7.** Click on the **AWS EC2 instance with data destruction permissions** and click the corresponding value for the **Alert ID** to see the **Overview** and remediation **Recommendation**.

ALERTS | Overview | Highest Priority | Incidents | Risky Attack Paths | Exposure | Vulnerabilities | Add View | Manage Views

Time Range: All Time | Time Range Type: Alert Opened | Alert Status: Open | Policy Severity: High X | Policy Type: IAM X | Policy Name: AWS EC2 instance with data destruction per... X | Add Filter

Group By: Policy Name

**AWS EC2 instance with data destruction permissions** ✎

High Privilege Escalation

Policy Labels Attack Path Rule

Dismiss Snooze Remediate Reopen Investigate

Asset Name	Alert ID	Alert Time	Account ID	Account	Alert Status	Region
i-094838c8bdc10...	<b>I-52710</b>	23 hours ago	577142504549	AWS Account	open	AWS Virginia
i-0c49516a46bc1...	I-52200	23 hours ago	577142504549	AWS Account	open	AWS Virginia

Load More | Displaying 1 - 2 of 2 (All records loaded)

#### AWS EC2 instance with data destruction permissions

I-52710

Overview Recommendation Alert Rules (1)

Remediation steps:

1. Log in to the AWS console
2. Navigate to the EC2 instance
3. Find the role used by the EC2 instance
4. Navigate to the IAM service
5. Click on Roles
6. Choose the relevant role
7. Under "Permissions policies", find the relevant policy according to the alert details and remove the risky actions

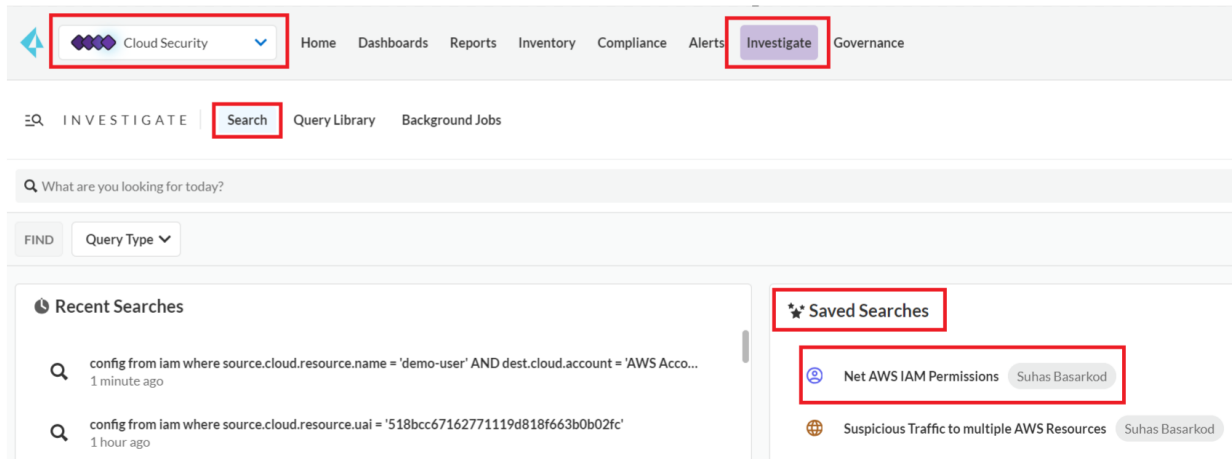
**Step 8.** Once done reviewing, close the window.



## ----- Task 5: Investigate Over Permissive IAM Permissions -----

**Step 1.** In this task, we will find out, with a simple **RQL query**, the net effective permissions of an IAM user to demonstrate the effectiveness of IAM RQL queries in Prisma Cloud.

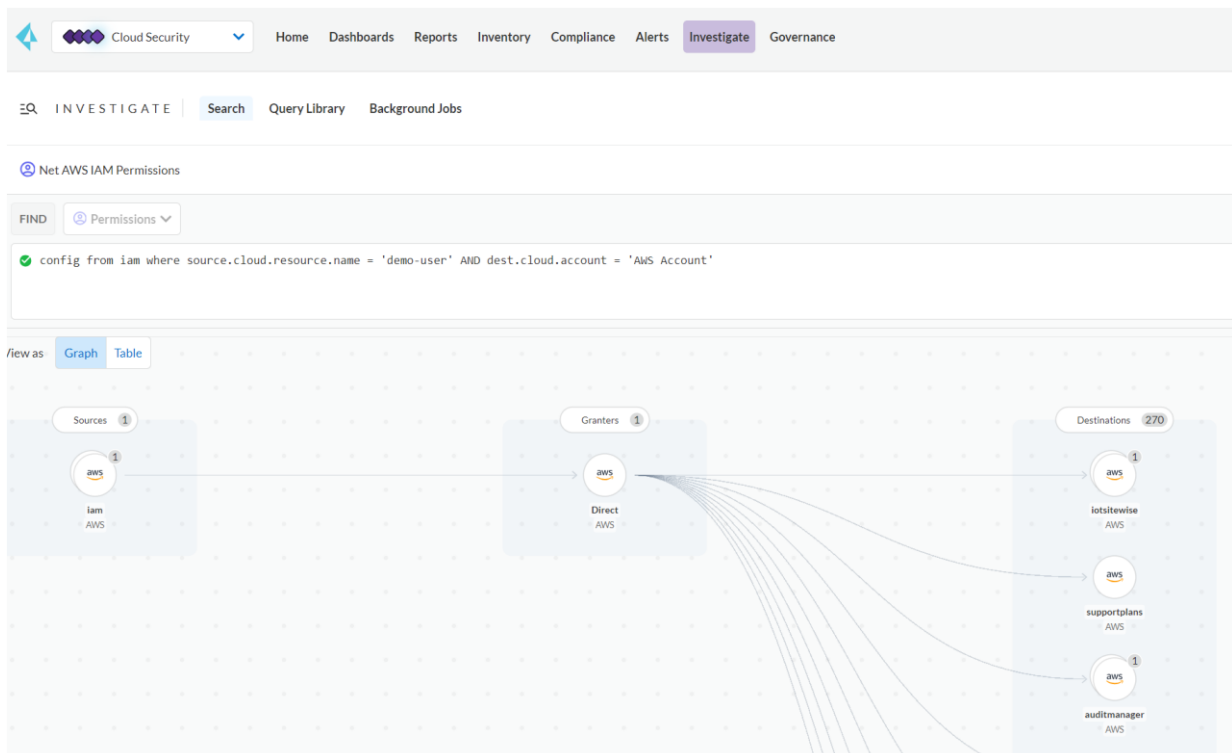
**Step 2.** Navigate to **Prisma Cloud > Cloud Security > Investigate** and select **Net AWS IAM Permissions** from **Saved Searches**



**Step 3.** The RQL query of the selected search query should look like the following:

*config from iam where source.cloud.resource.name = 'demo-user' AND  
dest.cloud.account = 'AWS UTD Account'*

**Step 4.** Click on the **Graph** icon.

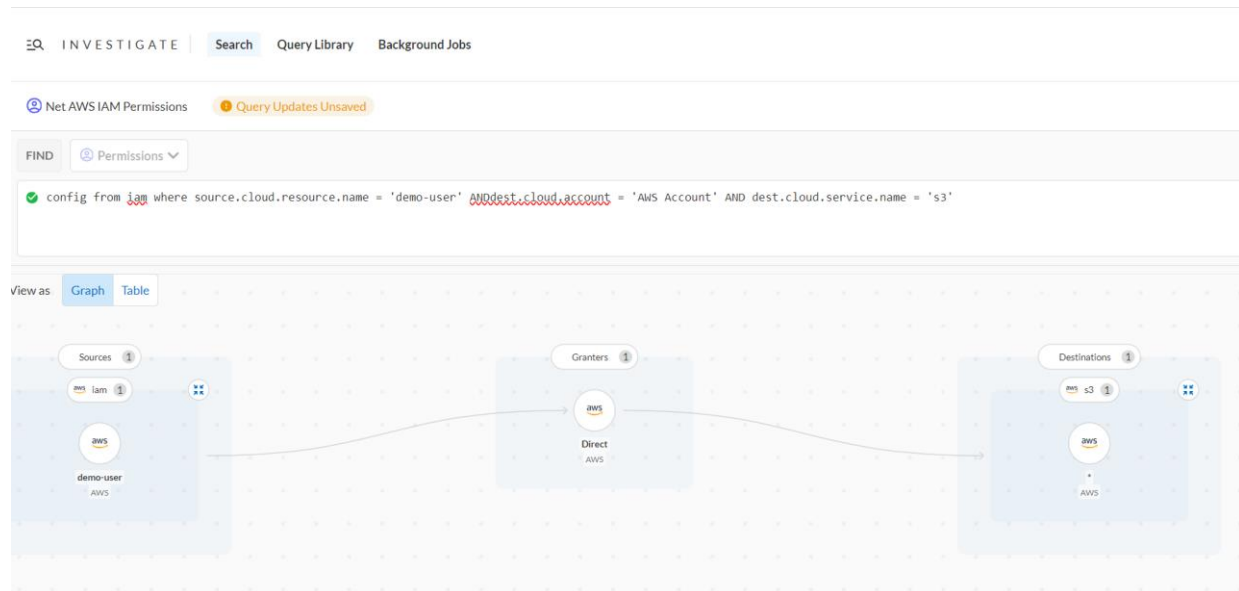




**Step 5.** This graph shows the permissions that the IAM user **demo-user** holds within the specified AWS Account. Feel free to explore the graph further.

**Step 6.** Within the **Destinations** column of the graph, to further narrow down the search to a specific AWS Service such as S3, update the query with the following

*config from iam where source.cloud.resource.name = 'demo-user' AND dest.cloud.account = 'AWS UTD Account' AND dest.cloud.service.name = 's3'*



**Step 7.** From the screenshot, you can see that there's a “\*” (wildcard) permission assigned, which is not a best-practice implementation in a production environment.

**Step 8.** To investigate the permissions of the IAM role used by EKS Node in the previous task, use the below query and explore the **Graph/Table**

*config from iam where dest.cloud.account = 'AWS UTD Account' AND grantedby.cloud.entity.name = 'EKSPNodeGroupRole-cnsp-app4' AND source.cloud.service.name = 'ec2'*