



Introductory Lab Guide

Table of Contents

1. Logistics

2. AWS and Dome9 Setup

- a. Exercise 1.1: Setup lab environment
- b. Exercise 1.2: Connect Dome9 to your new AWS account

3. Security Architecture Review Lab

- a. Exercise 2.1: Review AWS environment
- b. Exercise 2.2: Conduct inventory/asset review
- c. Exercise 2.3: Visualize security architecture
- d. Exercise 2.4: Identify zombie security group
- e. Exercise 2.5: Identify publicly accessible databases (2)

4. Security Posture Management Lab

- a. Exercise 3.1: Enforce security policy
- b. Exercise 3.2: Active protection – Security group level
- c. Exercise 3.2: Active protection – Region level

5. Application Infrastructure Security Lab

- a. Exercise 4.1: Access internal HTTP application via browser
- b. Exercise 4.2: Dynamic access leases

6. Compliance and Governance Lab

- a. Exercise 5.1: Compliance assessment
- b. Exercise 5.2: Custom governance rules

7. Offboarding

Logistics

- **Venue Requirements:** Internet connectivity, desks and chairs, projector with laptop hookup for presentation
- The organizing team is comprised of one speaker and 1-2 technical staff to help out and answer questions
- Participants bring their own laptops and use Dome9's lab AWS accounts
- Participants walk through the labs either individually or in pods of 2-3
- **Format:** 10 minutes upfront presentation, followed by self-directed labs with check-in at the beginning and end of each lab
- **Workshop Duration:** 3.5 hours, including lunch
- **Target Audience:** Technical security users (security engineers, architects, DevOps) who have heard of Dome9 and know what Dome9 offers

AWS and Dome9 Setup

Exercise 1.1: Setup lab environment (Login to your lab AWS account)

The instructor should provide you with an AWS Account for this workshop. Ensure you have an AWS account setup before proceeding.

Exercise Complete!

Exercise 1.2: Connect Dome9 to your new AWS account

Onboard an AWS account

Onboarding an AWS account involves creating policies and attaching it to roles for Dome9 to use. For simplicity, the policies and roles have already been created. Follow these steps to onboard your AWS account to Dome9.

1. On the Dome9 console navigate to **Cloud Inventory** and select Add AWS Account.



2. Select the Dome9 operation mode, **Read-Only** to be used for the account.

Select operation mode

Monitor (Read-Only) Mode

In the Monitor mode, Dome9 Arc can be used for visualization, monitoring and auditing, and will not modify or actively manage your cloud environment.

Available in Monitor (Read-Only) Mode:

- Dome9 Clarity for visualization of network security
- Change notifications
- Audit trail
- Compliance reports
- Alerts
- Policy reports

When to Choose Monitor (Read-Only) Mode:

- You have another source of automation to manage your policies
- You want to manage your security group rules directly, rather than delegating to Dome9

[GET STARTED!](#)

Full-Protection (Read/Write) Mode

In the Full-Protection(Read/Write) Mode, Dome9 Arc can be used to actively manage your security posture and enforce best practices.

Available in Full-Protection (R/W) Mode:

- Dynamic Access Leases - time-limited, on-demand resource access
- Security group management console to edit policies in-place
- Tamper Protection and Region Lock for active enforcement
- Reusable policy objects such as IP Lists and DNS Objects
- Dome9 Clarity for visualization of network security
- Change notifications
- Audit trail
- Compliance reports
- Alerts
- Policy reports

When to Choose Full-Protection (R/W) Mode

- You want to use Dome9 Arc as your system of authority for security management
- You want to use Dome9's active management and enforcement capabilities to maintain a closed-by-default security posture

Note that even when you are using Dome9 **Full-Protection (Read/Write) Mode** you'll still be able to set individual security groups to **Monitor (Read-Only) Mode**

[GET STARTED!](#)



3. Click next again
4. Sign to the AWS console (aws.amazon.com) in a new browser tab or window
(keep the Dome9 console open, as you will be switching between the two in the following steps).
5. Click **Services** and select the **IAM**
6. Select **Policies** and search for Dome9 and you should see two policies created.
Click and review the policy for read only.

Policy name	Type	Used as	Description
Dome9-readonly-policy	Customer managed	None	read only
dome9-write-policy	Customer managed	None	Write policy for Dome9

7. In the AWS console, click **Roles** and “**Create new Role**”
8. Select Role Type: ‘**Another AWS Account**‘, under options mark the ‘**Required External ID**‘ option.
9. Enter the following:
 - AccountId: 634729597623
 - External ID: E+7NvdTUqNKZNoCSQ0L53@64
 - Require MFA: NOT checked

The screenshot shows the AWS Create Role wizard. Step 1: Select type of trusted entity. Step 2: Specify accounts that can use this role. Account ID: 634729597623. Options: Require external ID (Best practice when a third party will assume this role). External ID: E+7NvdTUqNKZNoCSQ0L53. Important note: The console does not support using an external ID with the Switch Role feature. If you select this option, entities in the trusted account must use the API, CLI, or a custom federation proxy to make cross-account iam:AssumeRole calls. Learn more. Step 3: Not visible in the screenshot.

10. **READONLY:** Make sure the following policies are selected:

- **SecurityAudit** (AWS managed policy).
- **AmazonInspectorReadOnlyAccess** (AWS managed policy).
- **dome9_READONLY-policy**, that you created before. You can search for 'dome9' in the filter

11. Set Role Name with your choice ('Dome9-Connect' makes sense) and click on '**Create Role**'

Create role

Review

Provide the required information below and review this role before you create it.

Role name* Dome9-Connect
Use alphanumeric and '+=_,@-' characters. Maximum 64 characters.

Role description

Maximum 1000 characters. Use alphanumeric and '+=_,@-' characters.

Trusted entities The account 634729597623

Policies

- SecurityAudit
- AmazonInspectorReadOnlyAccess
- Dome9_READONLY-policy

Permissions boundary Permissions boundary is not set

* Required Cancel Previous **Create role**

12. Copy the **Role ARN** value, and enter it in the **Role ARN** field in the Dome9 console.

Dome9 Introductory Lab Guide

Summary

Policy Dome9-readonly-policy has been attached for the Dome9-Connect.

Role ARN	arn:aws:iam::371771556915:role/Dome9-Connect
Role description	Dome9 connect Edit
Instance Profile ARNs	
Path	/
Creation time	2018-07-13 14:18 PDT
Maximum CLI/API session duration	1 hour Edit
Give this link to users who can switch roles in the console	
https://signin.aws.amazon.com/switchrole?roleName=Dome9-Connect&account=371771556915	

Permissions **Trust relationships** **Access Advisor** **Revoke sessions**

▼ Permissions policies (3 policies applied)

Attach policies	Add inline policy
Policy name	Policy type
Dome9-readonly-policy	Managed policy
SecurityAudit	AWS managed policy
AmazonInspectorReadOnlyAccess	AWS managed policy

Create IAM Role for Dome9

- Click on 'Roles' and 'Create new Role' ⓘ
- Select: 'Role for Cross-Account Access' and select 'Provide access between your AWS account and a 3rd party AWS account' ⓘ
- Enter ⓘ
 - AccountID: 634729597623
 - External ID: [REDACTED]
 - Require MFA: NOT checked
- Click on the 'Next Step' button
- Select the following policies:
 - 'SecurityAudit' (AWS managed policy) ⓘ
 - 'dome9-readonly-policy' That we created before. You can search for 'dome9' in the filter ⓘ
 - 'dome9-write-policy' That we created before ⓘ
- Click on the 'Next Step' button
- Set Role Name with your choice ('Dome9-Connect' makes sense) and click on 'Create Role' ⓘ
- On the search box look for the "Role name" you set in the previous step, and click on it.
- Copy the **Role ARN** and fill it in the Role ARN field ⓘ
- Click on 'FINISH'

13. Click 'Finish'

14. Review the onboarded cloud account summary.
15. At the end of the onboarding process all the Security Groups will be in **Read Only** mode.

Exercise Complete! You have now connected your Dome9 to your AWS account

Security Architecture Review Lab

Exercise 2.1: Explore AWS Environment

In your AWS account, navigate to **N.Virginia region**. Take a moment to notice anything out of the ordinary. Explore EC2 instances, Security Groups, IAM and other services.
(There are 5 configuration mistakes in the lab, can you find them?)

The screenshot shows the AWS Management Console with the EC2 service selected. The left sidebar lists various AWS services like EC2 Dashboard, Instances, Launch Templates, and Auto Scaling. The main content area is titled 'Resource Groups' and shows a table of security groups. One specific security group, 'sg-a3e455c6', is selected and expanded to show its inbound rules. The table has columns for Name, Group ID, Group Name, VPC ID, and Description. The selected row for 'sg-a3e455c6' has a blue background. Below the table, there's a detailed view of the 'Inbound' tab for the selected security group, showing rules for All TCP, Custom UDP Rule, and Custom TCP Rule.

Name	Group ID	Group Name	VPC ID	Description
sg-60bd2019		Application_Load_Balancer	vpc-89e113ec	Application_Load_Balancer
sg-80e455e5		App1_Servers	vpc-89e113ec	Main Java application
sg-233d9645		App2_ApplicationServers	vpc-89e113ec	no description
sg-4f3c9629		App2_DB	vpc-89e113ec	all DB servers belongs to App2
sg-b50aa0d3		App2_LoadBalancers	vpc-89e113ec	all ELBs that belongs to App2
sg-07359811		App2_Web	vpc-89e113ec	web servers that belongs to application2
sg-9c90eaf		Base SG		SG for basic services
sg-2880x91b		CloudFormer-WebServerS...		Enable HTTPS access via port 443
sg-6291ca81		CloudFormerRoy-WebServe...		Enable HTTPS access via port 443
sg-a3e455c6		Common SG	vpc-89e113ec	shared rules for all instances

Security Group: sg-a3e455c6

Inbound

Type	Protocol	Port Range	Source	Description
All TCP	TCP	0 - 65535	sg-bde455d8 (DB servers)	
Custom UDP Rule	UDP	151 - 162	212.25.105.39/32	
Custom UDP Rule	UDP	151 - 162	212.25.105.40/32	
Custom UDP Rule	UDP	151 - 162	sg-e4e455b1 (LB-Web)	
Custom TCP Rule	TCP	443	4.4.4.4/32	
Custom TCP Rule	TCP	443	50.50.50.50/32	
Custom TCP Rule	TCP	443	100.2.3.4/32	
Custom TCP Rule	TCP	443	4.5.77.88/32	
Custom TCP Rule	TCP	443	9.8.99.88/32	
Custom TCP Rule	TCP	443	77.66.1.2/32	
Custom TCP Rule	TCP	443	5.4.3.3/32	

Exercise Complete! You have now explored your AWS instances and reviewed your security policies in AWS.

Exercise 2.2: Conduct inventory/asset review

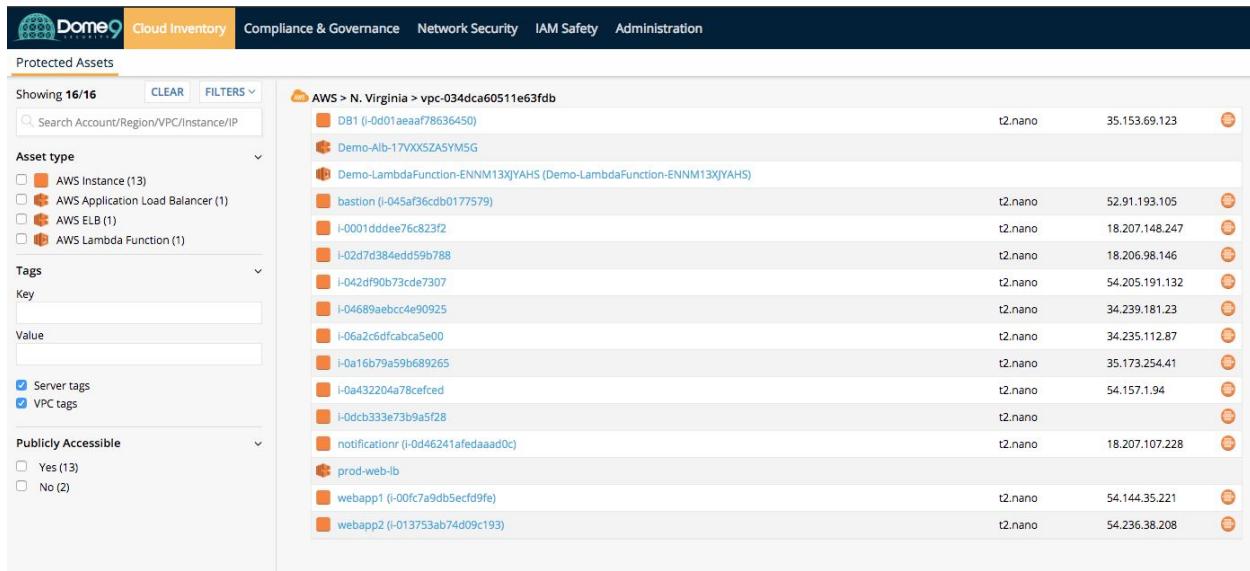
Switch into your Dome9 console for the remaining part of this module

Dome9 presents a single console view of all your assets, on all platforms, from which you can search or filter for specific assets of interest, and see details about their security posture. In this section of the Dome9 console, you can see a summary of all the assets in your VPCs that are protected by Dome9. These assets can include, for example, instances (such as EC2s), RDSs, and load balancers. Dome9 fetches

information about these assets from the cloud platforms (AWS, Azure, Google) and presents it in a console view.

1) View your Protected Assets

The main page shows a list of your assets that are protected by Dome9, organized by region. Filter the list using the filters on the left, or search for assets by name in the search bar.



The screenshot shows the Dome9 Cloud Inventory interface. At the top, there's a navigation bar with links for 'Compliance & Governance', 'Network Security', 'IAM Safety', and 'Administration'. Below the navigation bar, the title 'Protected Assets' is displayed, followed by a subtitle 'Showing 16/16'. There are three buttons: 'CLEAR', 'FILTERS ▾', and a search bar with placeholder text 'Search Account/Region/VPC/Instance/IP'. On the left side, there are several filter dropdowns: 'Asset type' (with options for AWS Instance, AWS Application Load Balancer, AWS ELB, and AWS Lambda Function), 'Tags' (with 'Key' and 'Value' fields), and 'Publicly Accessible' (with 'Yes' and 'No' checkboxes). The main right-hand area displays a table of assets. The columns are 'Asset Type', 'Name', 'Type', and 'IP Address'. The table contains 16 rows, each representing a different asset, such as DB1, Demo-Alb, bastion, and various Lambda functions and web applications. Each row includes a small orange icon representing the asset type and a small orange circle with a number indicating the number of alerts.

Asset Type	Name	Type	IP Address
AWS Instance (13)	DB1 (i-0d01aeaaf78636450)	t2.nano	35.153.69.123
AWS Application Load Balancer (1)	Demo-Alb-17VXX5ZA5YM5G		
AWS ELB (1)	Demo-LambdaFunction-ENNM13XJYAH5 (Demo-LambdaFunction-ENNM13XJYAH5)		
AWS Lambda Function (1)	bastion (i-045af36cdb0177579)	t2.nano	52.91.193.105
	i-0001dddee76c823f2	t2.nano	18.207.148.247
	i-02d7d384edd59b788	t2.nano	18.206.98.146
	i-042df90b73cd7307	t2.nano	54.205.191.132
	i-04689aebcc4e90925	t2.nano	34.239.181.23
	i-06a2c6dfcabca5e00	t2.nano	34.235.112.87
	i-0a16b79a5b689265	t2.nano	35.173.254.41
	i-0a432204a78cefced	t2.nano	54.157.1.94
	i-0dcba333e73b9a5f28	t2.nano	
	notificationr (i-0d46241afedaaad0c)	t2.nano	18.207.107.228
	prod-web-lb		
	webapp1 (i-00fc7a9db5ecfd9fe)	t2.nano	54.144.35.221
	webapp2 (i-013753ab74d09c193)	t2.nano	54.236.38.208

For each asset in the list, the type, and its external IP address (if it has one) are shown.

Click on one of the assets in the list to see more details for it.

2) View your Security Groups

The main page shows a list of all your managed security groups, in all your Dome9 managed accounts, on all cloud providers.

Filter the list using the search box or filter options on the left. You can filter by account, VPC, cloud region, protection method (full, read-only), and the number of instances or alerts.

The screenshot shows the Dome9 Cloud Inventory interface. At the top, there are tabs for Cloud Inventory, Compliance & Governance, Network Security, IAM Safety, and Administration. The Network Security tab is selected. Below the tabs, there's a search bar and a filter section with dropdowns for Region, VPC, and Tags. The main content area displays a table of AWS instances under two regions: N. Virginia and vpc-a39d63d9. The table columns are Instances and Alerts. The N. Virginia region table contains 17 entries, and the vpc-a39d63d9 region table contains 1 entry.

	Instances	Alerts
Demo-AgentServiceSG-1VHM88J7Q2ZOB	2	2
Demo-DBServersSG-NFSU0AAWT5RY	1	0
Demo-DevopSG-13SQSHJNV9JV	0	1
Demo-LambdaSG-1LAMFLCQQ8CJ6	0	0
Demo-MQSG-1UHK4GOBMVPP	1	1
Demo-MonitoringSG-1OE9BZ4APK6R4	1	2
Demo-NotificationServerSG-VPSD01C706WE	1	0
Demo-WebMonitorSG-55MGJUL28QDG	1	1
Demo-WebappSG-SYSUWBJB2BRR	2	1
Demo-appserverSG-169ORD4N0Y8JE	2	1
Demo-default-1AN3SSLBMTN72B	1	0
default	0	0
prod-alb-sg	0	0
prod-bastion-je-sg	1	0
prod-mongo-sg	1	1
prod-webapp-elb-sg	0	0
default	0	0

Exercise Complete! You have now explored your AWS instances and reviewed your inventory within the protected asset view of Dome9.

Exercise 2.3: Visualize security architecture

Dome9 Clarity gives a graphical visualization of the security groups in your cloud environment, and their effects on the cloud assets in the environment. It shows the security groups, traffic sources, and permitted traffic paths in the cloud network. The view is organized logically, according to the level of exposure of the Security Group to the external world. You can use Clarity to analyze your cloud network for security issues such as access to sensitive components from the internet, or to troubleshoot it for connectivity issues such as blocked paths to components.

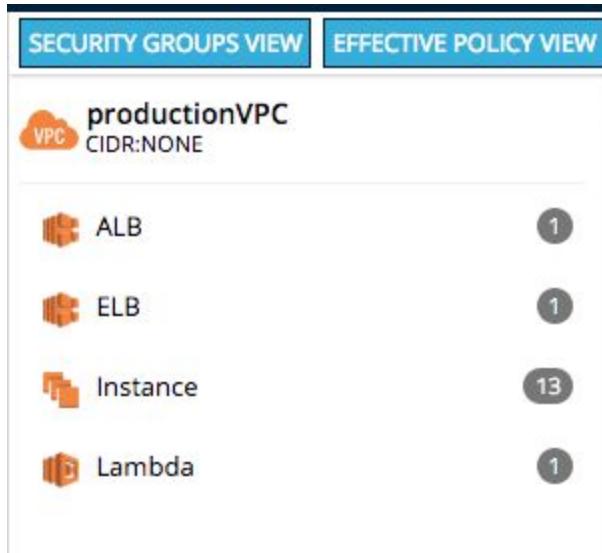
1) Select a cloud environment

Select **Clarity** from the main menu. A list of your cloud accounts is shown on the left.

2) View an environment with the Security Group view

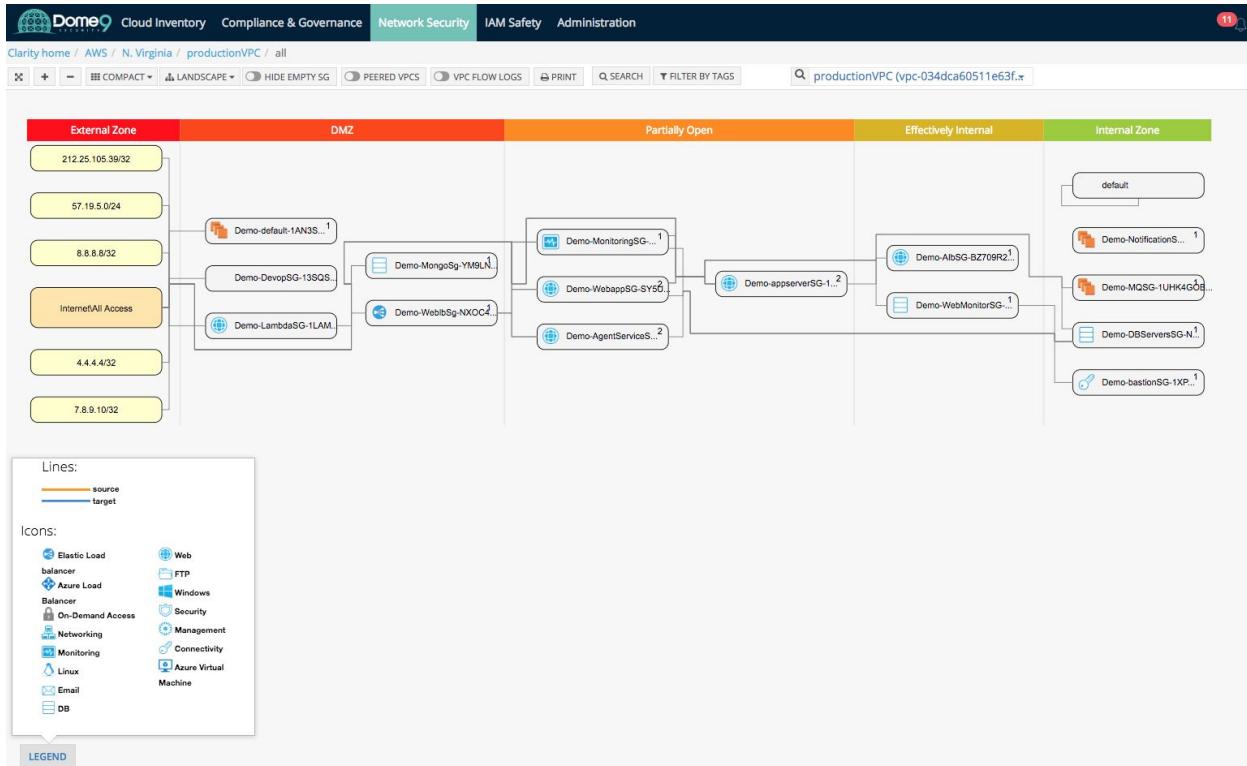
In this step, an environment will be visualized with the Security Group view. This view shows all the Security Groups.

- In Clarity, select a cloud environment in one of your accounts (in the previous section), and then select **Security Groups** from the list in the menu bar on the upper right.

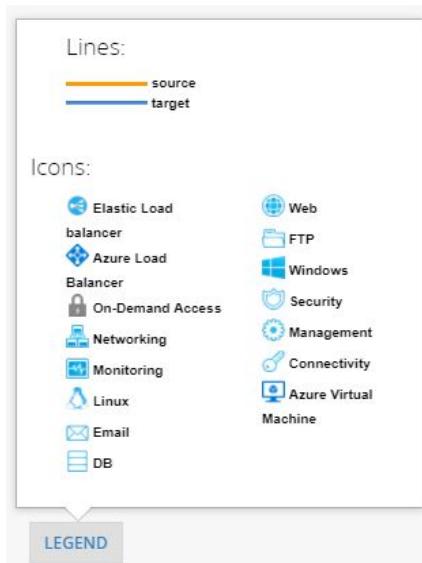


You can tell how the security groups (SG) interact with each other and can now understand whether any internal assets are communicating with the public world based on their inbound and outbound rules. The different swimlanes (which are auto classified by Dome9, so customers don't need to manually create them) represent security groups with various levels of exposure to the public.

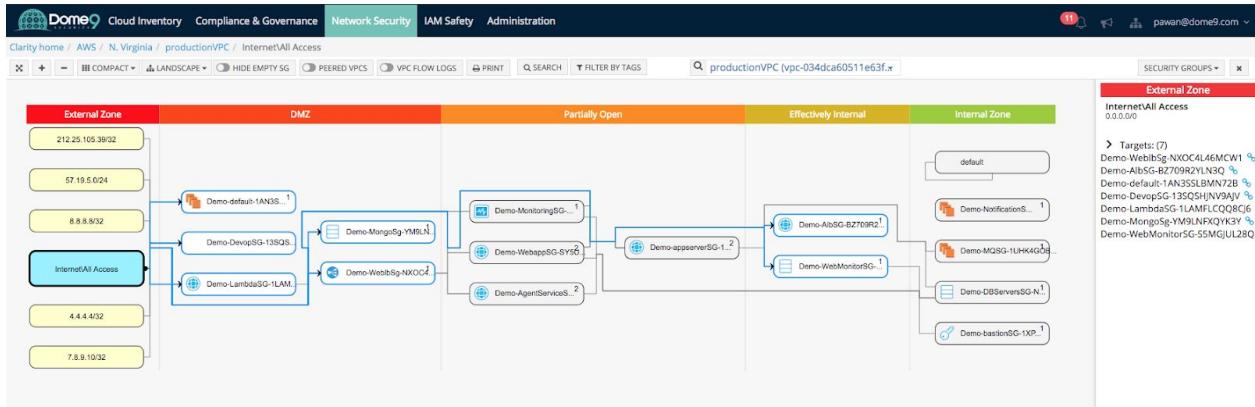
Dome9 Introductory Lab Guide



- b) Click the **Legend** button to show what each icon represents.



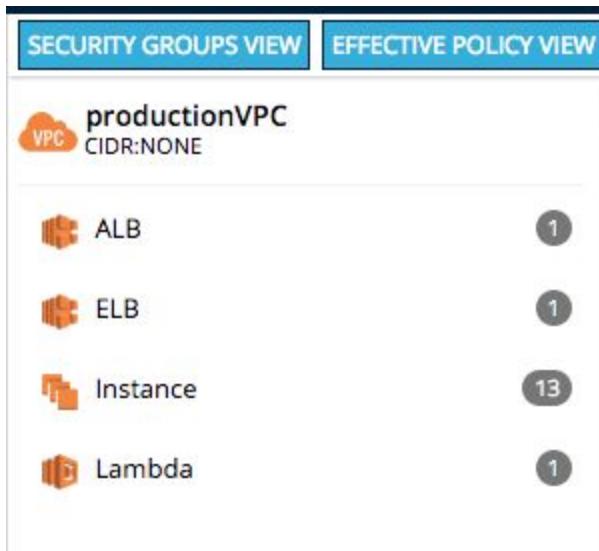
- c) Click on **Internet/All Access** block. The source block is highlighted in the view, and the Security Groups that affect this source are highlighted.



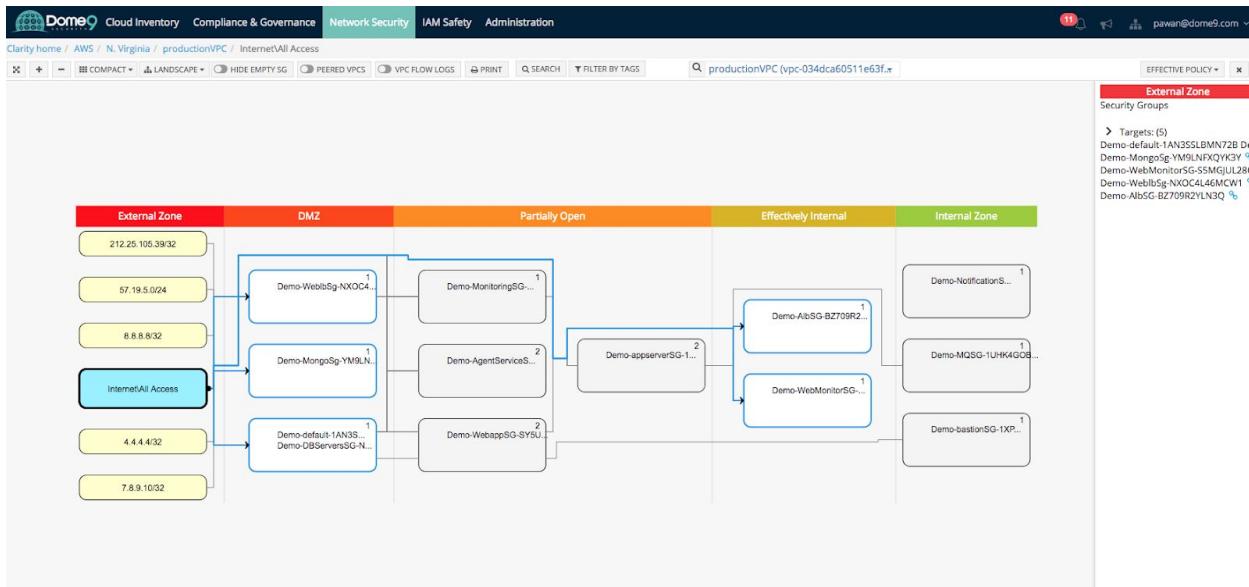
3) View an environment in the Effective Policy view

The Effective Policy view groups Security Groups that affect a common asset, and hides those that do not affect any assets.

- Select **Effective Policy** in the list in the menu bar at the upper right.



- This shows the VPC in the Effective Policy view



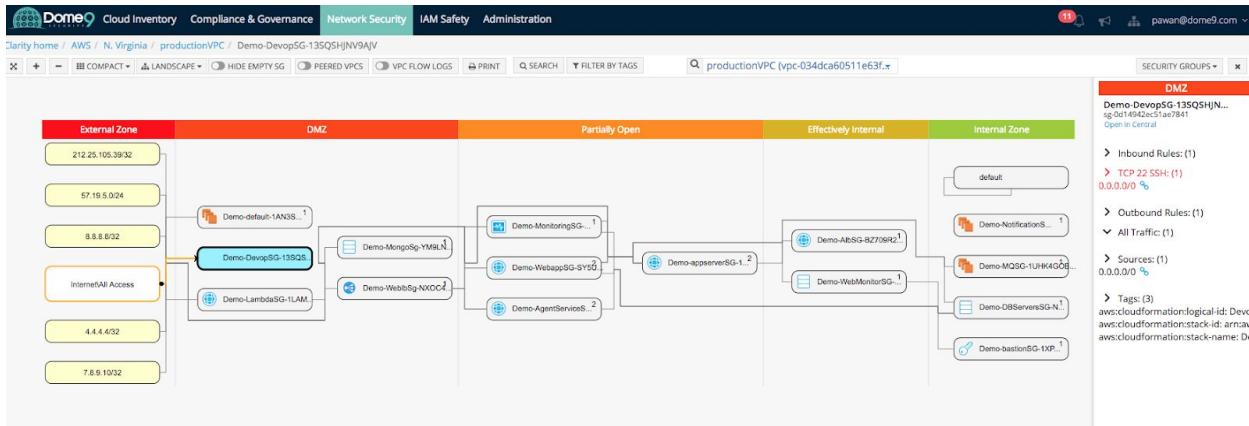
- c) This view also shows the Security Groups and Sources, organized by zone. In this view, however, the Security Groups that affect the same asset are grouped together. Security Groups that affect a number of assets may appear several times in the view. Security Groups that do not affect any assets are hidden.

Exercise Complete! You have visualized your AWS security configurations in the VPC from a logical firewall view (SG view) and instance policy view (effective policy view)

Exercise 2.4: Identify zombie security group

Let's go back into Clarity's security group view. See if you can identify a zombie security group. This is a SG that has no instance attached to it but has an exposed policy (TCP 22 0.0.0.0/0) to the public.

Answer: Don't peek just yet..



This screenshot displays the AWS Security Group details for 'Demo-DevopSG-13SQSHJNV9AJV'. The 'Tags' section shows three tags: 'aws:cloudformation:logical-id' with value 'DevopSG', 'aws:cloudformation:stack-id' with value 'arn:aws:cloudformation:us-east-1:290175429794:stack/Demo/052a6500-95af-11e8-a469-500c286e1a36', and 'aws:cloudformation:stack-name' with value 'Demo'. The 'Inbound Services' table shows one rule: 'SSH' (Protocol/TCP:22, State Open). The 'Outbound Services' section is labeled 'Default'. There are no group members or referencing security groups listed.

This is a low severity issue yet is important to be aware of as it is just one click away from exposing your internal servers. With Clarity you can find such issues and take appropriate actions to fix such misconfigurations.

Exercise Complete! You have now identified the zombie security group exposure

Exercise 2.5: Identify publicly accessible databases

In this section, we will investigate and find 2 different database exposures. Let's jump into Clarity.

Challenge 1: Detect DB Exposure – part 1 (easy)

In Clarity, try to find an exposed DB:

Answer: Here you see that this SG has 0.0.0.0/0 on port 27017 associated with the mongoDB instance. This is a high severity issue as one of your internal DB servers is now wide open. Click on the SG for more details.

The screenshot shows the Dome9 Clarity interface for a VPC. On the left, a network diagram displays various subnets (External Zone, DMZ, Partially Open, Effectively Internal, Internal Zone) and their connections. In the center, a specific security group (Demo-MongoSg-YM9LNFXQYK3Y) is selected. The right panel provides detailed information about this security group, including its inbound and outbound rules, instances, and tags.

Security Group Details:

- Instances:** (1) i-042df90b73cde7307
- Inbound Rules:** (2)
 - TCP 1433 MS-SQL (1)
 - TCP 27017 Custom TCP (27017)
- Outbound Rules:** (1) All Traffic (1)
- Sources:** (2) Demo-LambdaSG-1LAMFLCQQ8CJ6 0.0.0.0/0
- Tags:** (5)
 - env: prod
 - aws:cloudformation:stack-id: arn:aws:cloudformation:us-east-1:290175429794:stack/Demo/052a6500-95af-11e8-a469-500c286e1a36
 - Name: prod-mongo-sg
 - aws:cloudformation:logical-id: MongoSg
 - aws:cloudformation:stack-name: Demo

History: (Last 7 Days) Aug 1, 2018 10:19 AM - 10:24 AM

Group Members:

State	Name	Type	IP Address
Open	(i-042df90b73cde7307)	t2.nano	54.205.191.132 10.10.4.46

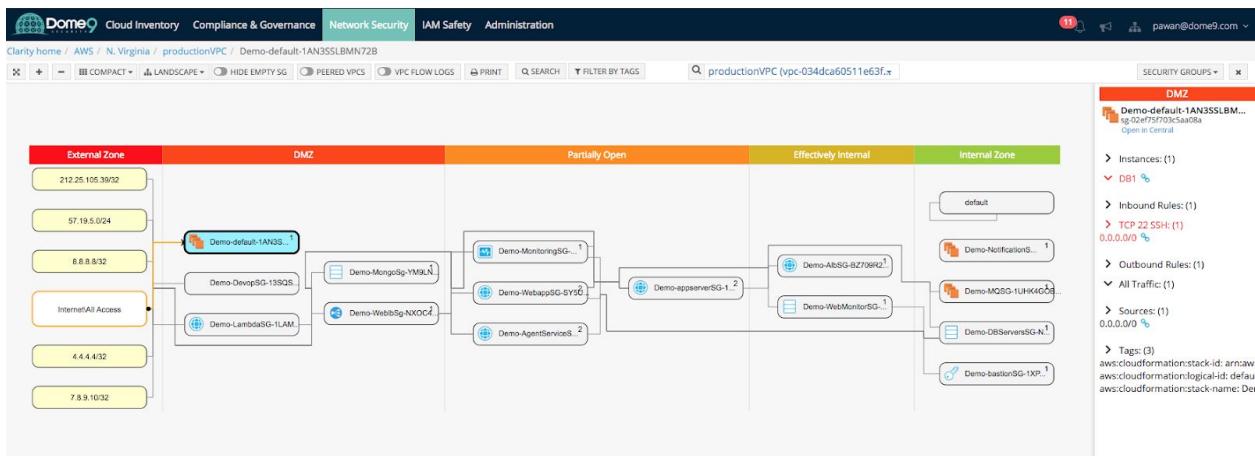
Referencing Security Groups: No referencing

You can see the open port in this view. We will fix these issues in the next lab.

Challenge 2: Detect DB Exposure – part 2 (hard)

Find another exposed DB, this one is a bit tricky.

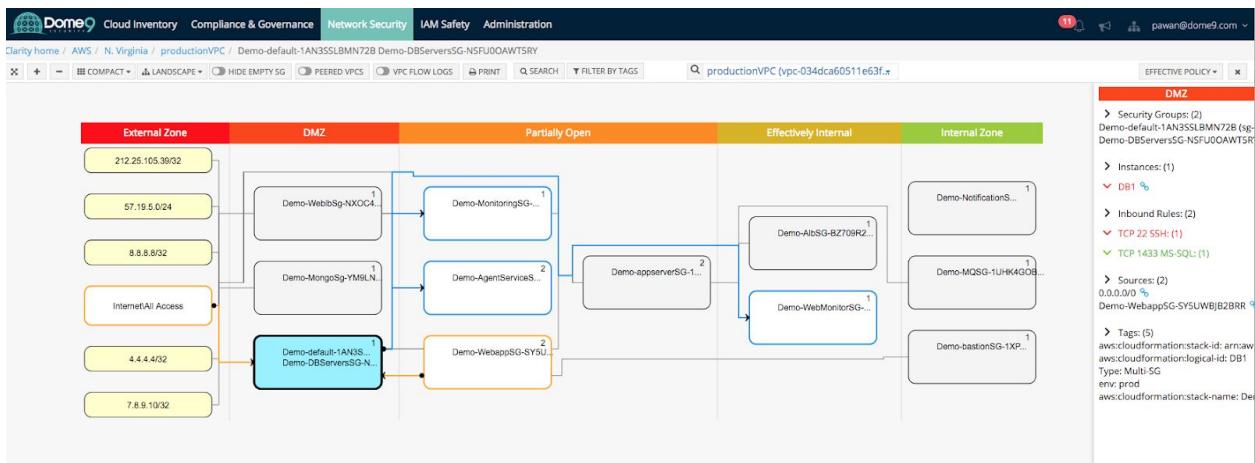
Answer: Click the default SG and hover over the right. Here you see default SG with SSH wide open and that DB1 is associated with this default SG making the database exposed to the public



In the effective policy view below – you can see default SG is in the DMZ zone and has one instance assignment (DB1, which is also part of the DB servers group).

Digging deeper, we realize that even if the rules associated with the security group are correct, an instance can still be assigned to the wrong security group. This is due to a misconfiguration that occurred due to assignment of multiple security groups, and specifically an incorrect default SG to DB1 instance.

The effective policy view brings this to light and tells you what security groups an instance belongs to, and therefore what the effective security policy is. Now it is clear – DB1 is exposed because it belongs to not only the internal DB Servers SG, but also to the Default SG which is in the DMZ.



Exercise Complete! You have now investigated both database exposures in Clarity

Security Posture Management Lab

Exercise 3.1: Enforce security policy

Fix misconfiguration in default security group by deleting the open SSH rule. For the purpose of this lab, lets keep it completely closed.

But first, we need to attach the Dome9-write-policy to the AWS account in order to have write access and make changes.

Go into your **AWS account**, navigate to **IAM**, and click **roles** and select **Dome9-Connect**

Dome9 Introductory Lab Guide

The screenshot shows the AWS IAM Roles page. The left sidebar is collapsed. The main area displays the 'Summary' tab for the 'Dome9-Connect' role. Key details shown include:

- Role ARN:** arn:aws:iam::290175429794:role/Dome9-Connect
- Role description:** Edit
- Instance Profile ARNs:** Edit
- Path:** /
- Creation time:** 2018-08-01 10:24 PDT
- Maximum CLI/API session duration:** 1 hour Edit
- Switch role URL:** <https://signin.aws.amazon.com/switchrole?roleName=Dome9-Connect&account=290175429794>

Below the summary, there are tabs for **Permissions**, **Trust relationships**, **Access Advisor**, and **Revoke sessions**. The **Permissions** tab is selected, showing the attached policies:

- SecurityAudit**: AWS managed policy
- AmazonInspectorReadOnlyAccess**: AWS managed policy
- dome9-readonly-policy**: Managed policy

A blue button labeled **Attach policies** is visible at the bottom left of the permissions section.

Attach the policy

The screenshot shows the 'Attach Permissions' dialog. At the top, it says 'Add permissions to Dome9-Connect' and 'Attach Permissions'. Below that is a 'Create policy' button and a 'Filter policies' dropdown set to 'dome9-wr'. A table lists the available policies:

Policy name	Type	Used as	Description
dome9-write-policy	Customer managed	None	

The 'dome9-write-policy' row has a checked checkbox in the first column. At the bottom right of the dialog are 'Cancel' and 'Attach policy' buttons.

You should have write policy enabled to turn on active protection capabilities in Dome9

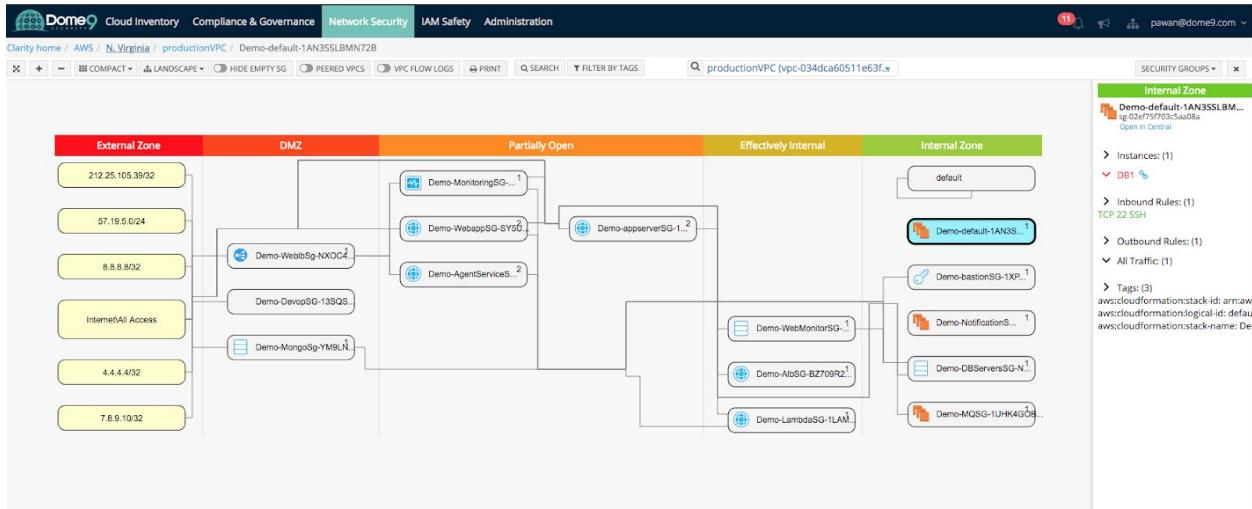
Now back in **Dome9 console** - go to Clarity, click the default SG we saw as the culprit, and turn on full protection mode at the top right in the entity explorer view:

The screenshot shows the Dome9 Cloud Inventory interface. At the top, there are tabs for Cloud Inventory, Compliance & Governance, Network Security, IAM Safety, Administration, and Protection Mode (which has a green checkmark and says 'Protection Mode Changed Successfully'). Below the tabs, the main content area displays the AWS Security Group 'Demo-default-1AN3SSLBMN72B'. It includes sections for Account (AWS), Region (N. Virginia (us_east_1)), VPC (productionVPC (vpc-034dcab60511e63fb)), and Group Description (Default security group). There are also Related Links for Visualize in Clarity, VPC Flow Logs, and Alerts. A History section shows activity from Aug 1, 2018, at 10:19 AM - 10:24 AM. The main configuration area shows Tags, Inbound Services (SSH port 22 is open), Outbound Services (Default), Group Members (DB1 is a member), and a note about Referencing Security Groups.

Fix the issue by closing the SG for now

This screenshot shows the 'Edit Inbound Service' dialog for the security group. It allows configuring an inbound service for SSH on TCP port 22. The 'Port Behavior' is set to 'Open for All'. The 'Allowed Sources' section is set to 'On-Demand' with the note 'Allow On-Demand connections from authorized users (Dynamic-Access)'. There are 'CANCEL' and 'SAVE' buttons at the top right.

You can also check Clarity to see the correct topology below:



Exercise Complete! You have now fixed the misconfigured security group.

Exercise 3.2: Active protection – SG level

Let's try to mess with this by making changes in the AWS console. Make SG change in AWS by going to the default SG.

Dome9 Introductory Lab Guide

The screenshot shows the AWS EC2 Dashboard with the 'Security Groups' section selected. A table lists 17 security groups, each with a checkbox, Name, Group ID, VPC ID, and Description. The 'sg-02ef75f703c5aa08a' row is highlighted. Below the table, a modal window titled 'Security Group: sg-02ef75f703c5aa08a' displays the 'Inbound' tab, which shows no rules. The 'Edit' button is visible.

Name	Group ID	VPC ID	Description
sg-01b79ee69511b6bfd	vpc-034dca60511e63fdb	Monitoring security group	
sg-02b4dba458cc41f67	vpc-034dca60511e63fdb	DB Servers security group	
sg-02ef75f703c5aa08a	vpc-034dca60511e63fdb	Default security group	
sg-0382fe9f809d57409	vpc-034dca60511e63fdb	MQ security group	
sg-04bce6c6c60628e42	vpc-034dca60511e63fdb	Notification server security group	
sg-079430790d9f62542	vpc-034dca60511e63fdb	Agent Service security group	
sg-0a2d3e1098f39a7bf	vpc-034dca60511e63fdb	Agent Service security group	
sg-0a66e77d58bb9d28	vpc-034dca60511e63fdb	default VPC security group	
sg-0bf44ec5380e4a6e	vpc-034dca60511e63fdb	DB Servers security group	
sg-0bf8009d10955602c	vpc-034dca60511e63fdb	WebApp security group	
sg-0d14942ec51ae7841	vpc-034dca60511e63fdb	Devops security group	
sg-0eba43cc935f98779	vpc-034dca60511e63fdb	Lambda Function security group	
sg-a2ca3fe8	vpc-a39d63d9	default	

And now enable 0.0.0.0/0 SSH rule for default SG

The screenshot shows the 'Edit inbound rules' dialog box. The 'Type' dropdown is set to 'SSH'. The 'Protocol' dropdown is set to 'TCP'. The 'Port Range' dropdown is set to '22'. The 'Source' dropdown is set to 'Custom' with '0.0.0.0/0' selected. The 'Description' field contains 'e.g. SSH for Admin Desktop'. At the bottom, there is a note about edits deleting existing rules and a 'Cancel' and 'Save' button.

You should now be able to see the change in Dome9 console. Dome9 also rolls configuration back and adds the user event in the audit trail for further analysis.

You can see the activity trail in the audit log which is extracted context from CloudTrail

Events			
Timestamp	Origin	User / IP Address	Description
2018-07-12 19:07:56	Dome9 Audit	system	Security group tamper detected and handled Security group tamper detected (Group modified). Security group: 'Demo-DBServersSG-1OXTU4VY4ZFT (sg-0bd91e7cf547a00ef)' of 'AWS>us_east_1>vpc-03de4c22bec2c90d3'. Handling method: Dome9 system has overriden the new settings with the approved policy. The following inbound rules were discovered: TCP-22-22: 0.0.0.0/0.

You should see the configuration reversed back to the gold standard configuration

The screenshot shows the AWS CloudFormation console for a security group named 'Demo-default-13LNEK50ZUU60'. The 'Tags' section contains three entries: 'aws:cloudformation:logical-id' with value 'default', 'aws:cloudformation:stack-id' with value 'arn:aws:cloudformation:us-east-1:426895540081:stack/Demo3aae12d0-8637-11e8-94c9-500c20fcfa99', and 'aws:cloudformation:stack-name' with value 'Demo'. The 'Inbound Services' section shows one rule for 'SSH' on 'TCP:22' with 'State' set to 'Closed'. The 'Group Members' section lists an instance named 'DB1' (i-0bda72c518af8bc00) with type 't2.nano' and IP address '18.209.214.249'. The status bar at the bottom indicates 'Showing 2/2'.

You can also confirm it in the AWS console

Name	Group ID	Group Name	VPC ID	Description
sg-01b79ee69511b6bf		Demo-MonitoringSG-10EB9...	vpc-034dca60511e63fdb	Monitoring security group
sg-02b4dba458cc41f67		Demo-WebMonitorSG-S5M...	vpc-034dca60511e63fdb	DB Servers security group
sg-02ef75f703c5aa08a		Demo-default-1AN3SSLBM...	vpc-034dca60511e63fdb	Default security group
sg-0382fe9f809d57409		Demo-MQSG-1UHK4GOBM...	vpc-034dca60511e63fdb	MQ security group
sg-04bce6cc60628e42		Demo-NotificationServerSG...	vpc-034dca60511e63fdb	Notification server security group
sg-079430790d9f62542		Demo-AgentServiceSG-1VH...	vpc-034dca60511e63fdb	Agent Service security group
sg-0a2d3e1098f39a7bf		Demo-appserverSG-1690R...	vpc-034dca60511e63fdb	Agent Service security group
sg-0a66e77d65bb9d28		default	vpc-034dca60511e63fdb	default VPC security group
sg-0b4f44ec5380e4a6e		Demo-DBServersSG-NSFU...	vpc-034dca60511e63fdb	DB Servers security group
sg-0b78009410955602c		Demo-WebappSG-SY5UWB...	vpc-034dca60511e63fdb	WebApp security group
sg-0d14942ec51ae7841		Demo-DevopSG-13SQSHJN...	vpc-034dca60511e63fdb	Devops security group
sg-0eba43cc93598779		Demo-LambdaSG-1LAMFL...	vpc-034dca60511e63fdb	Lambda Function security group
sg-a2ca3fe8		default	vpc-a39d63d9	default VPC security group

Security Group: sg-02ef75f703c5aa08a

Inbound

This security group has no rules

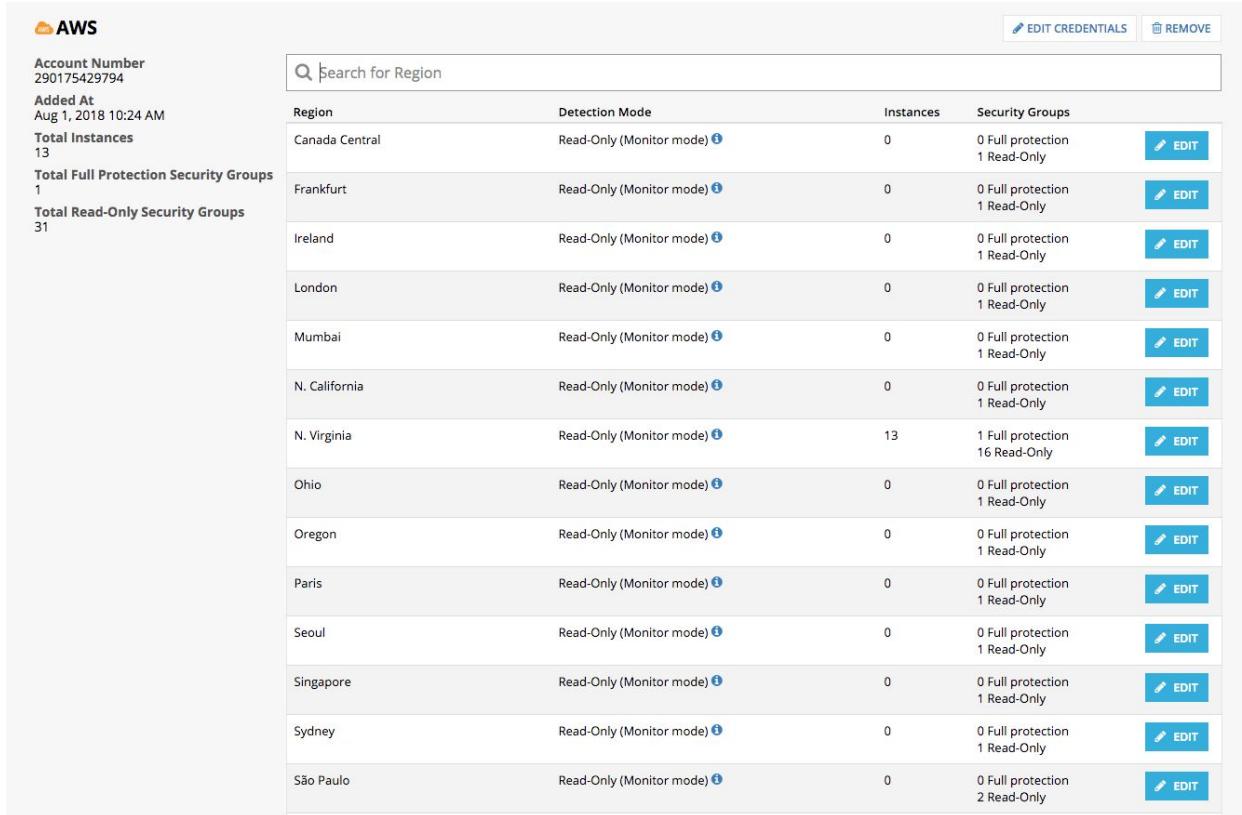
Exercise Complete! You have now enabled enforcement of security policies and eliminate configuration drift at a security group level in AWS

Exercise 3.2: Active protection – Region level

Let's turn on Region Lock first in Dome9 (Lock down Sao Paolo region)

Go to the cloud inventory and select cloud accounts and navigate to Sao Paolo region.

Dome9 Introductory Lab Guide



The screenshot shows the AWS Dome9 Introductory Lab Guide interface. On the left, there's a sidebar with account information: Account Number (290175429794), Added At (Aug 1, 2018 10:24 AM), Total Instances (13), Total Full Protection Security Groups (1), and Total Read-Only Security Groups (31). The main area is a table of AWS regions:

Region	Detection Mode	Instances	Security Groups	Action
Canada Central	Read-Only (Monitor mode) ⓘ	0	0 Full protection 1 Read-Only	<button>EDIT</button>
Frankfurt	Read-Only (Monitor mode) ⓘ	0	0 Full protection 1 Read-Only	<button>EDIT</button>
Ireland	Read-Only (Monitor mode) ⓘ	0	0 Full protection 1 Read-Only	<button>EDIT</button>
London	Read-Only (Monitor mode) ⓘ	0	0 Full protection 1 Read-Only	<button>EDIT</button>
Mumbai	Read-Only (Monitor mode) ⓘ	0	0 Full protection 1 Read-Only	<button>EDIT</button>
N. California	Read-Only (Monitor mode) ⓘ	0	0 Full protection 1 Read-Only	<button>EDIT</button>
N. Virginia	Read-Only (Monitor mode) ⓘ	13	1 Full protection 16 Read-Only	<button>EDIT</button>
Ohio	Read-Only (Monitor mode) ⓘ	0	0 Full protection 1 Read-Only	<button>EDIT</button>
Oregon	Read-Only (Monitor mode) ⓘ	0	0 Full protection 1 Read-Only	<button>EDIT</button>
Paris	Read-Only (Monitor mode) ⓘ	0	0 Full protection 1 Read-Only	<button>EDIT</button>
Seoul	Read-Only (Monitor mode) ⓘ	0	0 Full protection 1 Read-Only	<button>EDIT</button>
Singapore	Read-Only (Monitor mode) ⓘ	0	0 Full protection 1 Read-Only	<button>EDIT</button>
Sydney	Read-Only (Monitor mode) ⓘ	0	0 Full protection 1 Read-Only	<button>EDIT</button>
São Paulo	Read-Only (Monitor mode) ⓘ	0	0 Full protection 2 Read-Only	<button>EDIT</button>

Let's assume this would be an unused foreign region where you would not expect activity happening. You can turn on Region Lock to ensure no changes are made to this region unless it's from within Dome9.

Dome9 Introductory Lab Guide

Edit Region - AWS - São Paulo

Newly Detected Groups Behavior

<input type="checkbox"/> Read-Only (Monitor mode) Newly detected Security Groups and their rules will be imported and will be set as 'Read-Only' Security Groups. These groups will be monitored by Dome9 for changes but can still be changed outside Dome9.	<input type="checkbox"/> Full protection (Dome9 managed) Newly detected Security Groups will be imported with their initial rules to the Dome9 service, and thereafter be treated as Full Protection (Dome9 Managed) Security Groups. Any further security policy changes should be made using the Dome9 console or API. Dome9 Policy Tamper Protection will be added to the Security Group and will be activated after the import.	<input checked="" type="checkbox"/> Region lock Newly detected Security Groups will be imported and will immediately have their rules cleared (deleted) on both ingress and egress. This mode ensures that no network changes will be made to the region, unless they are performed on the Dome9 console.

Note: This will delete all ingress and egress rules from any newly discovered Security Groups. This mode is recommended for highly secured setups that are not allowed to be changed outside of the Dome9 system. This mode is also highly recommended for inactive regions.

São Paulo	select entire region	select entire region																
productionVPC (vpc-09bee5c22c0fd16f5) <table border="1"> <tr> <td><input type="radio"/> Read-Only (Monitor mode) <small>(?)</small></td> <td><input type="radio"/> select all</td> <td><input type="radio"/> Full protection (Dome9 managed) <small>(?)</small></td> <td><input type="radio"/> select all</td> </tr> <tr> <td><input checked="" type="radio"/> permissive-sg (sg-07ed9e3c937021411)</td> <td></td> <td><input type="radio"/></td> <td><input type="radio"/></td> </tr> <tr> <td><input checked="" type="radio"/> default (sg-032df64f273446774)</td> <td><input type="radio"/></td> <td><input type="radio"/></td> <td><input type="radio"/></td> </tr> <tr> <td><input checked="" type="radio"/> Demo-SandBox-bastionSG-2ZQ77PNH4SBA (sg-0170baf9218b4da06)</td> <td><input type="radio"/></td> <td><input type="radio"/></td> <td><input type="radio"/></td> </tr> </table>	<input type="radio"/> Read-Only (Monitor mode) <small>(?)</small>	<input type="radio"/> select all	<input type="radio"/> Full protection (Dome9 managed) <small>(?)</small>	<input type="radio"/> select all	<input checked="" type="radio"/> permissive-sg (sg-07ed9e3c937021411)		<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/> default (sg-032df64f273446774)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/> Demo-SandBox-bastionSG-2ZQ77PNH4SBA (sg-0170baf9218b4da06)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>		
<input type="radio"/> Read-Only (Monitor mode) <small>(?)</small>	<input type="radio"/> select all	<input type="radio"/> Full protection (Dome9 managed) <small>(?)</small>	<input type="radio"/> select all															
<input checked="" type="radio"/> permissive-sg (sg-07ed9e3c937021411)		<input type="radio"/>	<input type="radio"/>															
<input checked="" type="radio"/> default (sg-032df64f273446774)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>															
<input checked="" type="radio"/> Demo-SandBox-bastionSG-2ZQ77PNH4SBA (sg-0170baf9218b4da06)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>															
vpc-c896f0af <table border="1"> <tr> <td><input type="radio"/> Read-Only (Monitor mode) <small>(?)</small></td> <td><input type="radio"/> select all</td> <td><input type="radio"/> Full protection (Dome9 managed) <small>(?)</small></td> <td><input type="radio"/> select all</td> </tr> <tr> <td><input checked="" type="radio"/> default (sg-ff45a086)</td> <td><input type="radio"/></td> <td><input type="radio"/></td> <td><input type="radio"/></td> </tr> <tr> <td><input checked="" type="radio"/> SG1 (sg-0357eeab77f385426)</td> <td><input type="radio"/></td> <td><input type="radio"/></td> <td><input type="radio"/></td> </tr> </table>	<input type="radio"/> Read-Only (Monitor mode) <small>(?)</small>	<input type="radio"/> select all	<input type="radio"/> Full protection (Dome9 managed) <small>(?)</small>	<input type="radio"/> select all	<input checked="" type="radio"/> default (sg-ff45a086)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/> SG1 (sg-0357eeab77f385426)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>						
<input type="radio"/> Read-Only (Monitor mode) <small>(?)</small>	<input type="radio"/> select all	<input type="radio"/> Full protection (Dome9 managed) <small>(?)</small>	<input type="radio"/> select all															
<input checked="" type="radio"/> default (sg-ff45a086)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>															
<input checked="" type="radio"/> SG1 (sg-0357eeab77f385426)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>															

CLOSE **SAVE**

Go to the AWS console and create a new SG in São Paulo

AWS EC2 Dashboard

Create Security Group

Security group name: permissive-sg
 Description: test-sg
 VPC: vpc-09bee5c22c0fd16f5 | productionVPC

Security group rules:

Inbound Outbound

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop

Add Rule

Cancel Create

Go back to Dome9 console, you should see this new SG's inbound/outbound rules deleted.

The screenshot shows the Dome9 Security Groups interface for the 'permissive-sg' security group. The group was created on Jul 12, 2018, at 7:35 PM. It has the following details:

- Account:** AWS
- Region:** São Paulo (sa-east-1)
- VPC:** productionVPC (vpc-09bee5c22c0fd16f5)
- Group Description:** test
- Related Links:**
 - Visualize in Clarity
 - VPC Flow Logs
 - Alerts
- History:** (Last 7 Days) Jul 12, 2018, 7:35 PM
- Group Members:** No members attached
- Referencing Security Groups:** No referencing

You can also confirm it in the AWS console in São Paulo

The screenshot shows the AWS EC2 Dashboard under the 'NETWORK & SECURITY' section, specifically the 'Security Groups' tab. The 'permissive-sg' security group is listed in the table:

Name	Group ID	Group Name	VPC ID	Description
sg-0170ba9218b4d06	Demo-SandBox-bastionSG...	vpc-09bee5c22c0fd16f5	Bastion security group	
sg-032df64f273446774	default	vpc-09bee5c22c0fd16f5	default VPC security group	
sg-0357eeab77f385426	SG1	vpc-c896f0af	launch-wizard-1 created 2018-06-13T15:50:10.469-07:00	
sg-07ed9e3c937021411	permissive-sg	vpc-09bee5c22c0fd16f5	test	
sg-f45a086	default	vpc-c896f0af	default VPC security group	

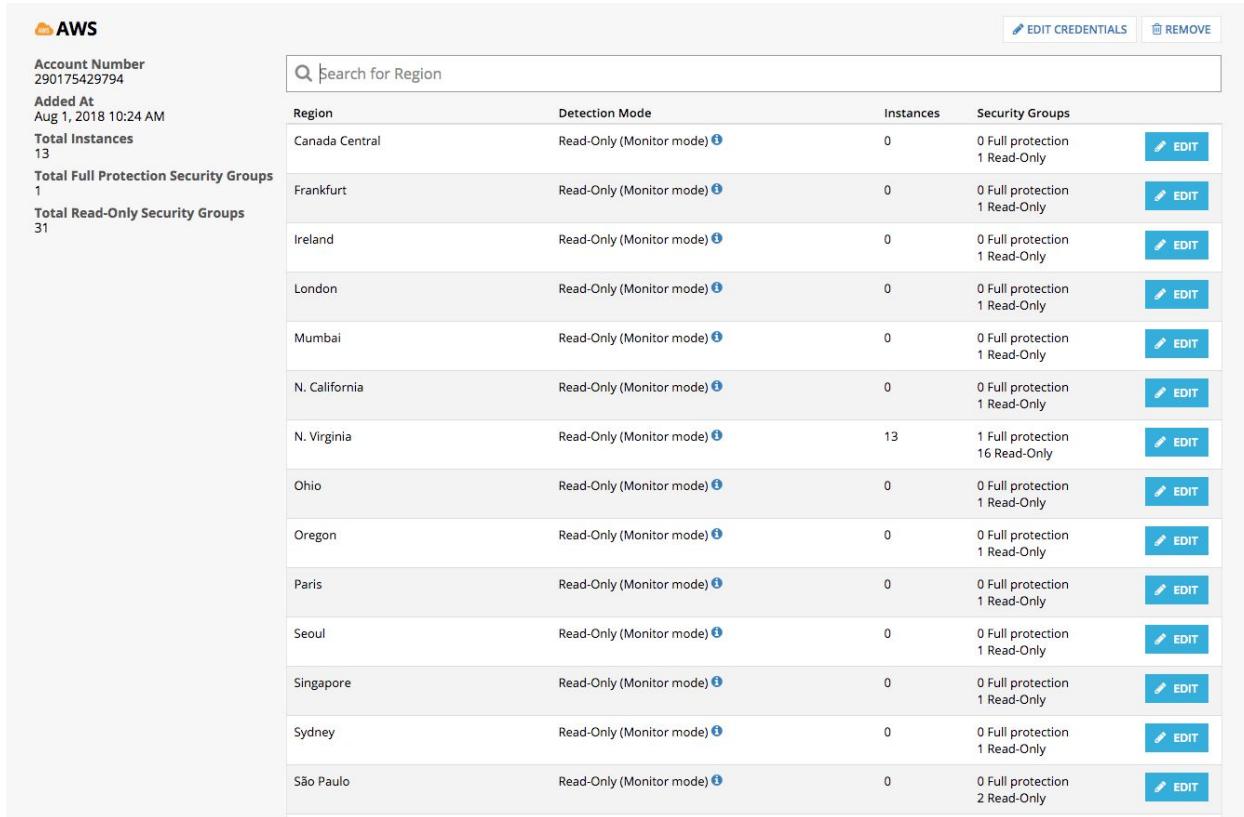
The 'Inbound' tab is selected, and the message 'This security group has no rules' is displayed.

Exercise Complete! You have now enabled enforcement of security policies and eliminate configuration drift at a region level in AWS.

Application Infrastructure Security Lab

Exercise 4.1: Access internal HTTP application via browser

In **Dome9 console** - Make sure you turn on **full protection mode** for **N.Virginia Region** in the cloud accounts.



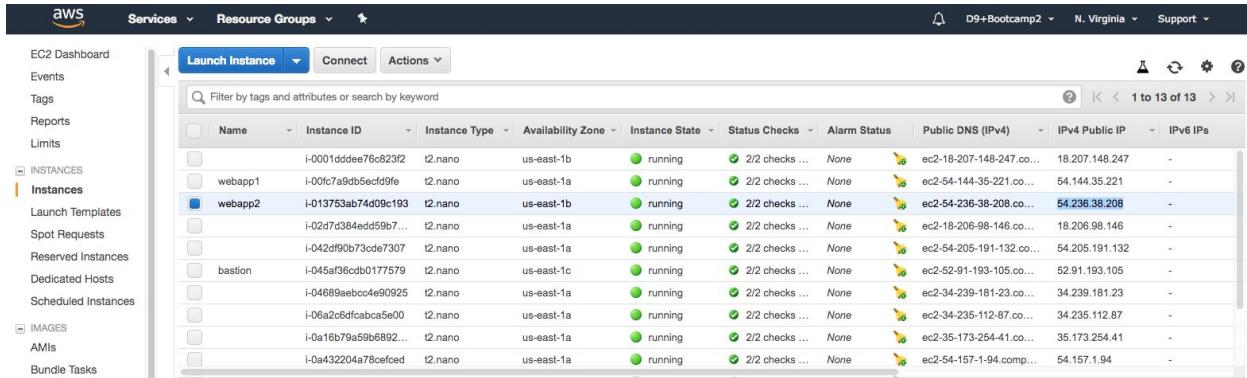
The screenshot shows a table of AWS regions with the following data:

Region	Detection Mode	Instances	Security Groups	
Canada Central	Read-Only (Monitor mode) ⓘ	0	0 Full protection 1 Read-Only	<button>Edit</button>
Frankfurt	Read-Only (Monitor mode) ⓘ	0	0 Full protection 1 Read-Only	<button>Edit</button>
Ireland	Read-Only (Monitor mode) ⓘ	0	0 Full protection 1 Read-Only	<button>Edit</button>
London	Read-Only (Monitor mode) ⓘ	0	0 Full protection 1 Read-Only	<button>Edit</button>
Mumbai	Read-Only (Monitor mode) ⓘ	0	0 Full protection 1 Read-Only	<button>Edit</button>
N. California	Read-Only (Monitor mode) ⓘ	0	0 Full protection 1 Read-Only	<button>Edit</button>
N. Virginia	Read-Only (Monitor mode) ⓘ	13	1 Full protection 16 Read-Only	<button>Edit</button>
Ohio	Read-Only (Monitor mode) ⓘ	0	0 Full protection 1 Read-Only	<button>Edit</button>
Oregon	Read-Only (Monitor mode) ⓘ	0	0 Full protection 1 Read-Only	<button>Edit</button>
Paris	Read-Only (Monitor mode) ⓘ	0	0 Full protection 1 Read-Only	<button>Edit</button>
Seoul	Read-Only (Monitor mode) ⓘ	0	0 Full protection 1 Read-Only	<button>Edit</button>
Singapore	Read-Only (Monitor mode) ⓘ	0	0 Full protection 1 Read-Only	<button>Edit</button>
Sydney	Read-Only (Monitor mode) ⓘ	0	0 Full protection 1 Read-Only	<button>Edit</button>
São Paulo	Read-Only (Monitor mode) ⓘ	0	0 Full protection 2 Read-Only	<button>Edit</button>

This part of the lab shows how you can get on demand access to ports and services using Dome9 Dynamic access feature. For this lab, we have a web server running but access is closed off. Let's try to access it

Navigate to the web application IP, this is the webapp2 IP that you can find from the EC2 console in AWS

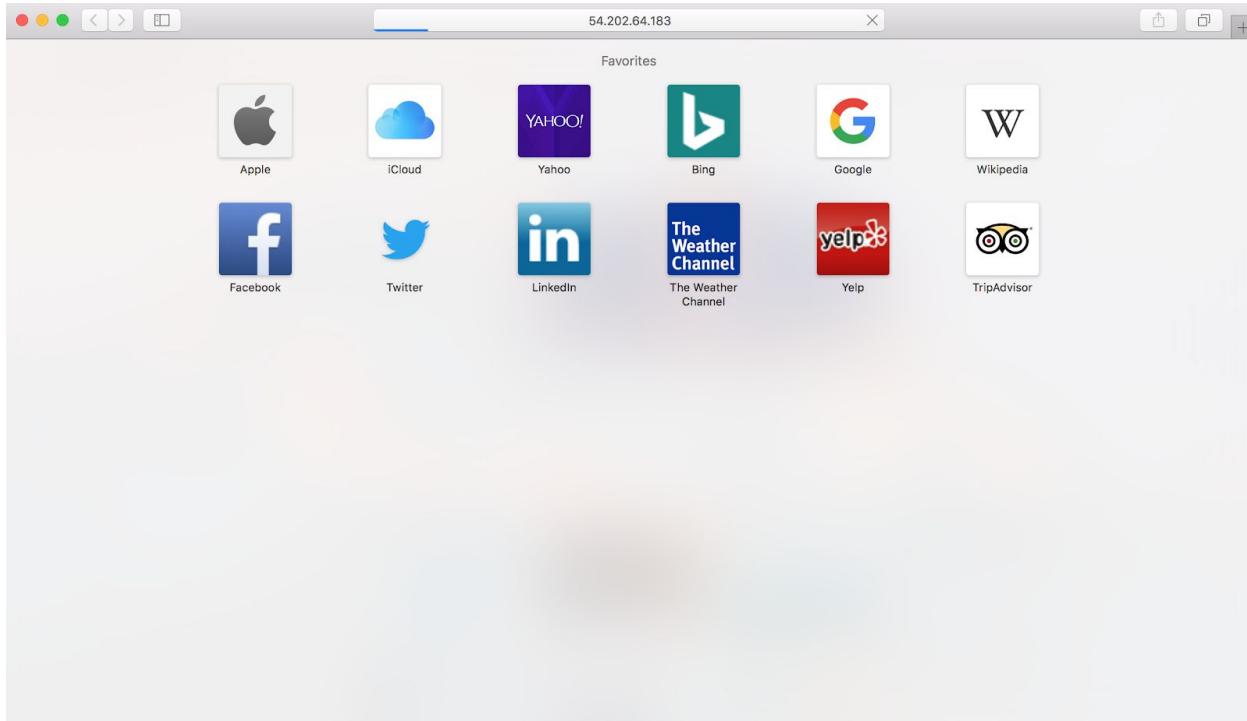
Dome9 Introductory Lab Guide



The screenshot shows the AWS EC2 Dashboard. On the left, there's a sidebar with links like EC2 Dashboard, Events, Tags, Reports, Limits, Instances, Launch Templates, Spot Requests, Reserved Instances, Dedicated Hosts, Scheduled Instances, Images, AMIs, and Bundle Tasks. The main area has tabs for Launch Instance, Connect, and Actions. A search bar at the top says "Filter by tags and attributes or search by keyword". Below it is a table with columns: Name, Instance ID, Instance Type, Availability Zone, Instance State, Status Checks, Alarm Status, Public DNS (IPv4), IPv4 Public IP, and IPv6 IPs. The table lists 13 instances, with one row highlighted in blue for "webapp2". The public IP for "webapp2" is listed as 54.236.38.208.

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP	IPv6 IPs
i-0001ddde76c823f2	t2.nano	us-east-1b	running	2/2 checks ...	None		ec2-18-207-148-247.co...	18.207.148.247	-
webapp1	i-00fc7a9db5e5edcf0fe	t2.nano	us-east-1a	running	2/2 checks ...	None	ec2-54-144-35-221.co...	54.144.35.221	-
webapp2	i-013753ab74d09c193	t2.nano	us-east-1b	running	2/2 checks ...	None	ec2-54-236-38-208.co...	54.236.38.208	-
i-02d7d384ed59b7...	t2.nano	us-east-1a	running	2/2 checks ...	None		ec2-18-206-98-146.co...	18.206.98.146	-
i-042df90b73cd7307	t2.nano	us-east-1a	running	2/2 checks ...	None		ec2-54-205-191-132.co...	54.205.191.132	-
bastion	i-045af36cdb0177579	t2.nano	us-east-1c	running	2/2 checks ...	None	ec2-52-91-193-105.co...	52.91.193.105	-
i-04699aebc04e90925	t2.nano	us-east-1a	running	2/2 checks ...	None		ec2-34-239-181-23.co...	34.239.181.23	-
i-06a2c6dfcabca5e00	t2.nano	us-east-1a	running	2/2 checks ...	None		ec2-34-235-112-87.co...	34.235.112.87	-
i-016b79a59b6892...	t2.nano	us-east-1a	running	2/2 checks ...	None		ec2-35-173-254-41.co...	35.173.254.41	-
i-0a432204a786cefcd	t2.nano	us-east-1a	running	2/2 checks ...	None		ec2-54-157-1-94.comp...	54.157.1.94	-

Navigate to the IP:



You should see nothing pop up. This is because by default, the connection to this web server is blocked. As a best practice, ports and services are closed by default and are opened just on demand to access the service for a pre-defined period of time. Now let's see how that works.

Exercise Complete!

Exercise 4.2: Dynamic access leases

In Dome9 - Navigate to dynamic access in the network security menu bar

The screenshot shows the Dome9 Network Security dashboard. On the left, there's a timeline of events from June 22, including security group tamper detections and assessment runs. The main panel is titled 'Network Security' with a sub-section 'Dynamic Access'. It includes options for IP Addresses, IP Lists, and Flow Logs. A callout box highlights the 'AWS Prod' section, which mentions AWS NIST 800-53 Rev 4 (FEDRAMP). The top right corner shows user information and a notification count of 20.

Click “Get Access” and select webappSG access for http TCP port 80/443, and save it as “Demo”

This screenshot shows the 'Get Access' interface. On the left, there are filters for Active Leases, VPC, Tags, AWS Security Group, Protocol / Port, and more. The main area lists various AWS resources with their security groups and associated ports. For each item, there is a 'GET ACCESS' button. In the bottom right, a modal dialog is open for selecting an access lease. It shows '2 ITEMS SELECTED' (Web (HTTP) and Web (HTTPS)), time options for 1 Hour Access (default), 5 Hours Access, and 10 Hours Access, and a 'SAVE ACCESS GROUP' button. Below the dialog are additional 'GET ACCESS' buttons for other items.

Now you have an active lease, associated with your IP for a period of time (1 hour in this case)



The screenshot shows the Dome9 Cloud Inventory dashboard. The top navigation bar includes links for Cloud Inventory, Compliance & Governance, Network Security, IAM Safety, Administration, and user information (pawan+demo@dome9...). Below the navigation is a search bar and a sidebar with 'Access Groups' and 'Get Access' options.

Active Access Leases:

Service Name	Lease IP	Expires	Created by	Created at (local time)
AWS Stage > Oregon > vpc-0f33b568 > Staging2-WebappSG-1D6XKBF1521N (sg-b7fa47cf)				2018 Jun 22 10:03:24
Web (HTTP)	73.70.208.83/32	in an hour	pawan+demo@dome9.com	

Pending Invitation:

Recipient Name	Security group / Server	Service Name	Created by	Expires	Created At
There are no access lease invitations					

Now jump back to your browser and see if you were able to access the web page.



This concludes the lab on application security hardening and best practices. Let's now move on to the final lab which will cover compliance and governance.

Exercise Complete! You have now successfully opened up the web service for just in time access and thereby followed proper security hardening practice

Compliance and Governance Lab

Exercise 5.1: Compliance assessment

1. Navigate to Compliance Engine Tab

The screenshot shows the Dome9 Cloud Inventory interface. The top navigation bar includes 'Cloud Inventory', 'Compliance & Governance' (which is the active tab), 'Network Security', 'IAM Safety', and 'Administration'. The top right corner shows a notification count of 20, a user icon for 'pawan+demo@dome9...', and a dropdown menu.

Left Sidebar: Shows a timeline of events from June 22:

- 8:57 AM: Security group tamper detected and handled
- 7:56 AM: Security group tamper detected and handled
- 7:04 AM (4 events): Assessment Event
- 8:57 AM: Security group tamper detected and handled
- 5:56 AM: Security group tamper detected and handled
- 4:53 AM: Security group tamper detected and handled
- 4:29 AM (6 events): Assessment Event
- 3:56 AM: Security group tamper detected and handled

Showing 20/81

Compliance & Governance Tab:

AWS Prod: AWS NIST 800-53 Rev 4 (FED...)

CLICK TO RUN

Network:

	SELECT RELEVANT ACCOUNTS AND BUNDLES	SELECT RELEVANT ACCOUNTS AND BUNDLES	SELECT RELEVANT ACCOUNTS AND BUNDLES
150 Default Security Groups with network policies	38 Security Groups with admin ports too exposed to the public internet	31 Security Groups with SSH admin port too exposed to the public internet	10 Instances are not configured within a VPC
58 IAM Users with console password without MFA enabled	0 Accounts without enforced Password Policy	10 IAM Users with Inline IAM Policies applied	27 IAM Users enabled while unused for 90 days or more

IAM:

GCP Accounts: Updated hourly (last updated: 34 minutes ago)

WS Redshift	Azure VM	Azure ELB	GCP VM
0	2	10	3

Network Policy Reports:

2. Explore Compliance Engine page

Dome9 Introductory Lab Guide

The screenshot shows the Dome9 Cloud Inventory interface. The top navigation bar includes links for Cloud Inventory, Compliance & Governance, Network Security, IAM Safety, Administration, and user information (pawan+demo@dome9...). The main menu on the left has options for Policies, Dashboard, Continuous Compliance, Playground, and Assessment History. A 'CLONE BUNDLE' and 'NEW BUNDLE' button are at the top left. On the right, there are buttons for 'SHOW GSL', '+ NEW RULE', 'EDIT JSON', and 'RUN ASSESSMENT'. A message at the top right says 'Dome9 predefined template. In order to edit please CLONE the bundle'. The central area displays a list of bundles, with 'AWS CIS Foundations v. 1.1.0' selected. This bundle page shows a search bar, a validation types section (including IAMUser, CloudTrail, SecurityGroup, IAMPolicy, Region, S3Bucket, KMS, and VPC), and a compliance section. Two specific items are highlighted: 'Avoid the use of the "root" account' (High risk) and 'Enforce Password Policy' (High risk). Each item has a description, remediation steps, and a link to the AWS documentation.

Dome9 Compliance Engine monitors and scans your AWS/Azure/GCP infrastructure to ensure alignment with compliance standards such as PCI-DSS, NIST 800-53, GDPR, CIS etc.

3. Select CIS Benchmarks and run bundle assessment

Select your AWS environment in the cloud account section. Dome9 also provides the option to BYOC (Bring your own CFT) and scan your template before pushing to production.

5. Analyze the report findings

Category	Value
Total Tests	49
Passed (%)	14.29%
Failed (%)	85.71%
Error (%)	0%

Within a few seconds, the Compliance Engine runs an assessment and provides detailed findings in an easy to use dashboard. You can see the number of test cases passed vs failed, as well as test cases segmented geographically, across regions and by test severities.

6. Analyze key test results for Security Group section

Test Case Description	TESTED	RELEVANT	NON COMPLYING
Ensure the default security group restricts all traffic	267	69	61
Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password	29	21	19
Ensure AWS Config is enabled in all regions	15	15	15
Ensure no security groups allow ingress from 0.0.0.0/0 to SSH (TCP:22)	267	267	15
Ensure S3 bucket access logging is enabled on the CloudTrail S3 bucket	56	11	11
Ensure no security groups allow ingress from 0.0.0.0/0 to RDP (TCP:3389)	267	267	11

A few cases you can check on:

1. Ensure password policy on
2. Cloud Trail enabled in all regions
3. VPC flow logs enabled
4. Ensure default security group does not allow 0.0.0.0/0 to SSH

7. Analyze test cases for S3 bucket

1. Ensure bucket is not publically accessible
2. Ensure versioning is turned on

3. Ensure encryption is on.

Exercise Complete! You have now successfully explored CIS best practices, and the test cases associated with this framework.

Exercise 4.2: Custom Governance Rules

Dome9 allows for you to create your own custom rules. Here is how to access the GSL Rule Builder to create your own custom rule:

1. In the Dome9 dashboard, navigate to Compliance & Governance and select 'Compliance Engine'



The screenshot shows the Dome9 dashboard with the 'Compliance & Governance' tab selected. On the left sidebar, under 'Compliance & Governance', the 'Compliance Engine' option is highlighted with a checked checkbox icon. Other options include 'Alerts', 'Policy Reports', 'Audit Trail', 'Compliance Dashboard', 'Compliance Playground', and 'Continuous Compliance'. To the right, there is a main content area titled 'Compliance & Governance' which describes the feature and its purpose.

Compliance & Governance
Use Dome9 broad set of reports to facilitate your cloud security operations.
View alerts on potential misconfigurations, use policy reports to easily detect assets satisfying certain conditions and view a detailed audit trail of changes to your cloud assets as well as Dome9 assets.

- 2.
3. You must create a your own bundle if you'd like to create your own custom GSL rules. You can clone an existing bundle or create a new one. Let's clone the existing Dome9 Best Practices bundle

Dome9 Introductory Lab Guide

4.

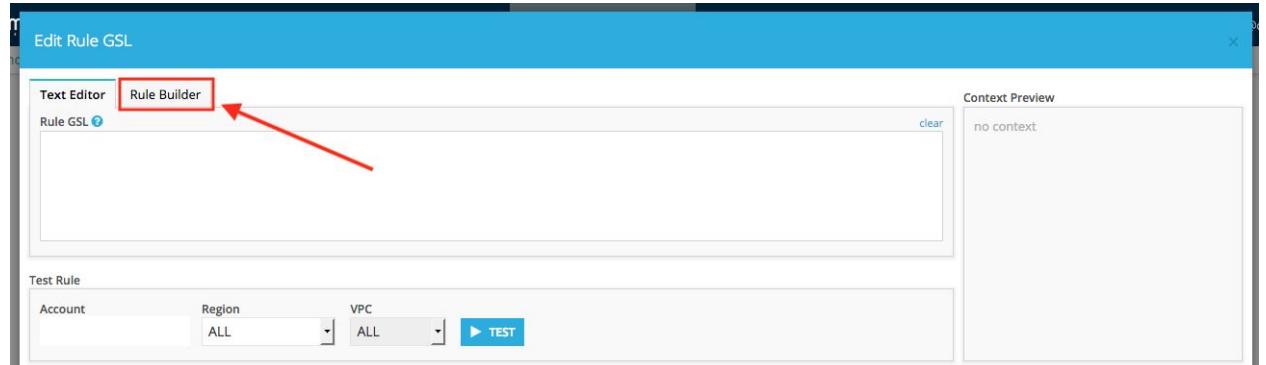
- Now you can create custom rules for your newly created bundle. To create a new rule, select 'New Rule'

6.

- To begin creating your new rule, click in the box that says 'Rule GSL'

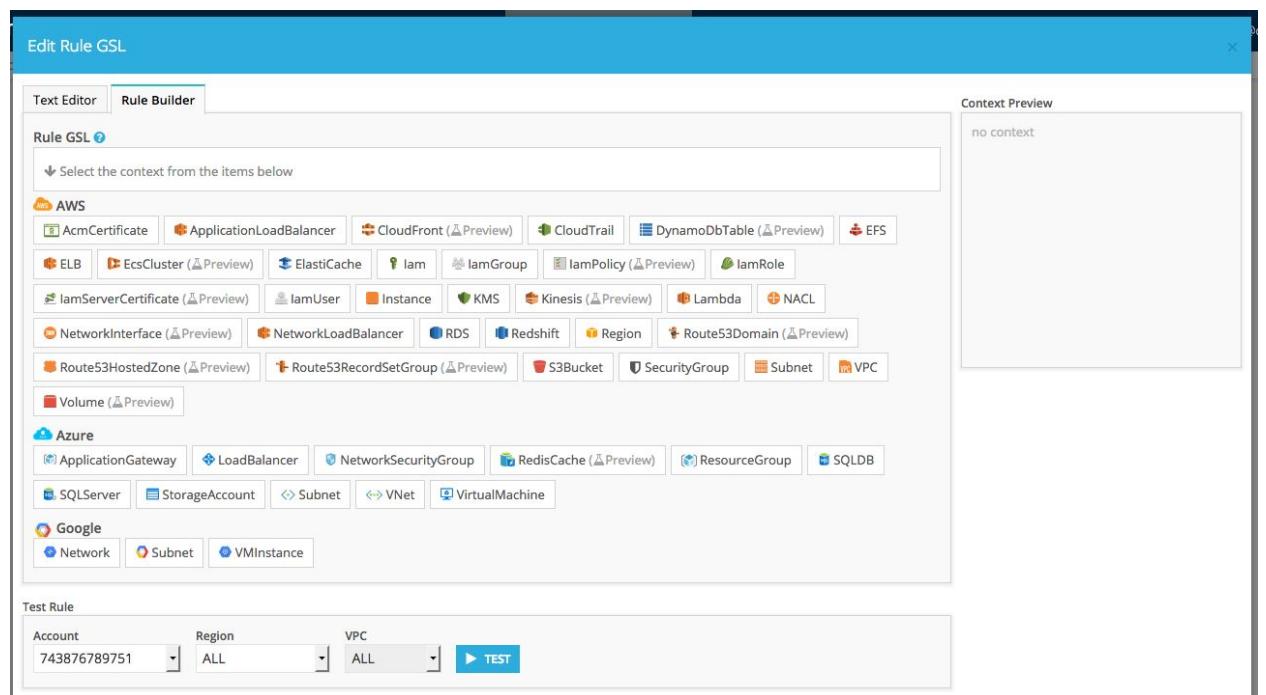
8.

9. Dome9 offers multiple ways for you to create your rules. You can use the Text Editor to create your custom rule, or you can use the Dome9 Rule Builder. To use the Rule Builder, select the tab that says 'Rule Builder'



10.

11. Here is where you can access the Rule Builder to build out your custom GSL rules



Now as part of this exercise, write your custom rule that highlights tagged instances with key value as “PCI”

Once you are done, run the bundle and check your report in the findings view.

Exercise Complete! You have now successfully written custom rules for unique governance policies.

Offboarding

Go to Cloud Inventory, cloud accounts, and remove the existing AWS account from your Dome9 free Trial

The screenshot shows the Dome9 Cloud Inventory interface. At the top, there are tabs for Cloud Inventory, Compliance & Governance, Network Security, IAM Safety, and Administration. The IAM Safety tab is active. In the top right corner, there is a user icon with the name 'pawan@dome9.com'. Below the tabs, there are two main sections: 'Cloud Accounts' and 'AWS'. The 'AWS' section is selected. It displays account details: Account Number (290175429794), Added at (Aug 1, 2018 10:24 AM), Total Instances (13), Total Full Protection Security Groups (18), and Total Read-Only Security Groups (14). To the right of this information is a modal dialog titled 'Remove AWS Cloud Account' with the message 'Are you sure you want to remove 'AWS' cloud account?'. The dialog has 'CANCEL' and 'REMOVE' buttons. Below the modal is a table listing regions, detection modes, instances, and security groups. The table includes rows for Canada Central, Frankfurt, Ireland, London, Mumbai, N. California, N. Virginia, Ohio, Oregon, Paris, Seoul, Singapore, Sydney, and São Paulo. Each row has an 'EDIT' button next to it.

Region	Detection Mode	Instances	Security Groups	EDIT
Canada Central	Read-Only (Monitor mode) ⓘ	0	0 Full protection 1 Read-Only	<button>EDIT</button>
Frankfurt	Read-Only (Monitor mode) ⓘ	0	0 Full protection 1 Read-Only	<button>EDIT</button>
Ireland	Read-Only (Monitor mode) ⓘ	0	0 Full protection 1 Read-Only	<button>EDIT</button>
London	Read-Only (Monitor mode) ⓘ	0	0 Full protection 1 Read-Only	<button>EDIT</button>
Mumbai	Read-Only (Monitor mode) ⓘ	0	0 Full protection 1 Read-Only	<button>EDIT</button>
N. California	Read-Only (Monitor mode) ⓘ	0	0 Full protection 1 Read-Only	<button>EDIT</button>
N. Virginia	Full protection (Dome9 managed) ⓘ	13	16 Full protection 1 Read-Only	<button>EDIT</button>
Ohio	Read-Only (Monitor mode) ⓘ	0	0 Full protection 1 Read-Only	<button>EDIT</button>
Oregon	Read-Only (Monitor mode) ⓘ	0	0 Full protection 1 Read-Only	<button>EDIT</button>
Paris	Read-Only (Monitor mode) ⓘ	0	0 Full protection 1 Read-Only	<button>EDIT</button>
Seoul	Read-Only (Monitor mode) ⓘ	0	0 Full protection 1 Read-Only	<button>EDIT</button>
Singapore	Read-Only (Monitor mode) ⓘ	0	0 Full protection 1 Read-Only	<button>EDIT</button>
Sydney	Read-Only (Monitor mode) ⓘ	0	0 Full protection 1 Read-Only	<button>EDIT</button>
São Paulo	Region lock ⓘ	0	2 Full protection 0 Read-Only	<button>EDIT</button>

Hope you enjoyed this lab! We hope to see you again soon!