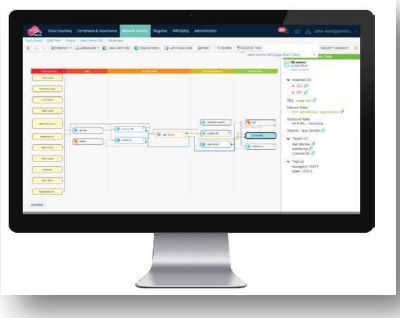
CloudGuard Dome9 Training Lab Guide

Ver. 1.6

Table of Contents

Introduction:

CloudGuard Dome9 is an innovative service that allows enterprises to easily manage the security and compliance of their public cloud environments at any scale across Amazon Web Services (AWS), Microsoft Azure and Google Cloud. CloudGuard Dome9 offers technologies to visualize and assess security posture, detect misconfigurations, model and actively enforce gold standard policies, protect against attacks and insider threats, cloud security intelligence for cloud intrusion detection, and comply with regulatory requirements and best practices. Businesses use CloudGuard Dome9 for faster and more effective cloud security operations, pain-free compliance and governance, and Rugged DevOps practices.



CLOUDGUARD DOME9 HAS PRODUCT CAPABILITIES ACROSS FOUR FUNCTIONAL AREAS:

Security Operations: Visualize assets, assess security posture, fix misconfigurations and threats, manage the cloud firewall, and enforce security from a single source of network authority

Privileged Identity Protection: Protect against compromised credentials and identity theft using a cloud's native IAM capabilities to safeguard access to actions that can have a big impact

Compliance and Governance: Manage the compliance lifecycle for standards such as PCI DSS, from automated data aggregation and assessment to remediation and reporting

Cloud Security Intelligence: CloudGuard Dome9 Magellan is a cloud-native security intelligence technology that delivers cloud intrusion detection, network traffic visualization and user activity analytics

Securing AWS infrastructure with CloudGuard Dome9 Hands-on lab Objectives:

The target of these hands-on lab exercises is to provide you with practical real-life experience with Check Point's CloudGuard Dome9 services on AWS' infrastructure.

The objectives of the hands-on training are:

1. AWS and Dome9 Setup
   This exercise will show you how to prepare your AWS environment via deploying a CloudFormation Template on the AWS account and connecting account to the Dome9 service.

2. Cloud Inventory - Review your Lab Assets
   This exercise will guide you through the Cloud Inventory module.

3. Network Security - Visualize security architecture
   This exercise will guide you through your security configuration, as reflected by the security groups of your cloud accounts.

4. Network Security - Dynamic Access
   This exercise shows how to get on demand access to ports and services using Dome9 Dynamic Access feature.

5. Compliance and Governance
   In this exercise you will become familiar with the Compliance and Governance module.
   You will practice running compliance bundles and create your own queries.

Good Luck

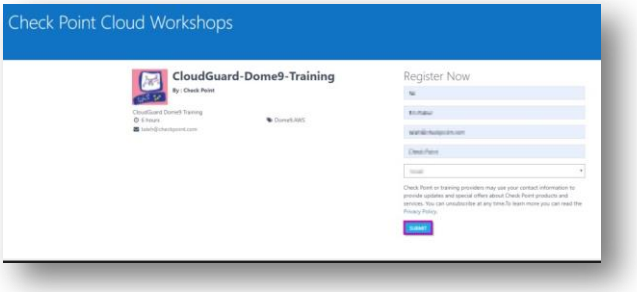
Connecting and setting up the work environment:

Purpose: To become familiar with the console and its options

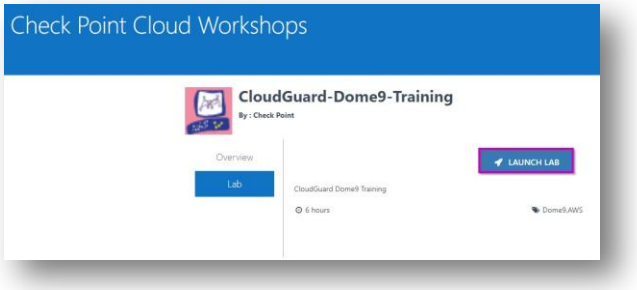
Register and sign-in to AWS

1. Connect to the environment provided to you by the instructor.

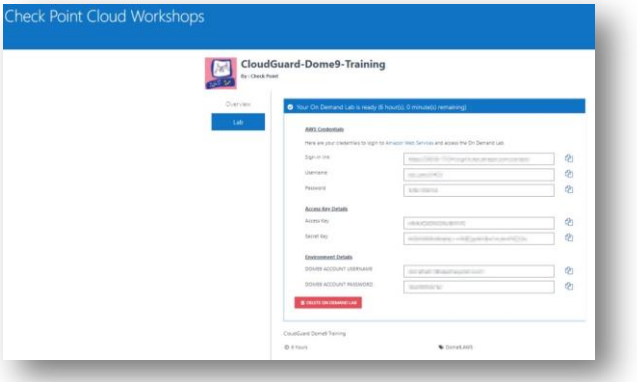
2. Fill in your details for registration and click “Submit”.



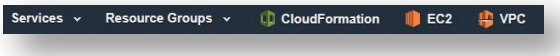
3. On the next screen, Click on “Launch Lab”.



4. You’re On Demand Lab session has started and the session will remain active for several hours (as described on the page). The browser window will show your credentials for this session and the sign-in link (you will also get an email with this information).



5. Browse to the Amazon AWS portal using the provided sign-in link and use the credentials you were provided.
6. At the top of the page click the 
7. Drag to the upper bar the:
    a. CloudFormation
    b. EC2
    c. VPC
8. At the top of the page click the 
9. The upper bar should look like this:



Exercise #1 – AWS and Dome9 Setup

Description

This exercise will guide you through the steps required to deploy resources on your AWS account.

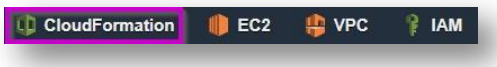
Method

Using the AWS console you will deploy new resources on your AWS account to prepare for the Dome9 lab.

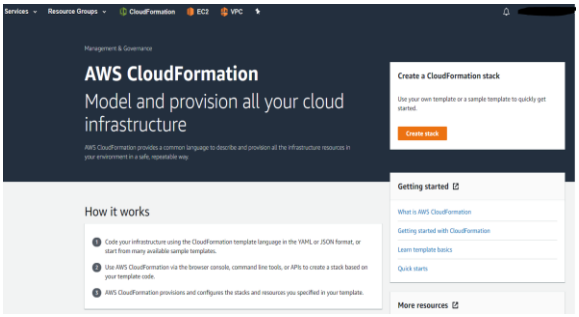
Step 1 *Deploy CloudFormation template*

1. In the top navigation bar in the AWS console, on the top-right, take note of the region in which you'll be creating the VPC (choose the **London** region). Ensure that you continue working in the same region for the rest of the exercises, as you cannot launch an instance into your VPC from a different region.
2. Download the file from the link that is relevant for the one you work in:
    - London: http://tiny.cc/D9CFP-London (CloudFormation).

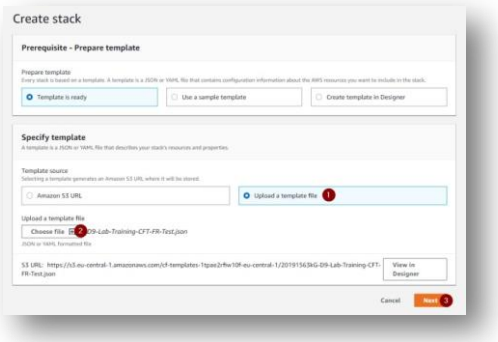
    TIP - If you can't click the link, copy it to your browser
3. Upload the CloudFormation template.
4. At the AWS console, click CloudFormation.



5. In the opened screen, click on the 'create Stack'.

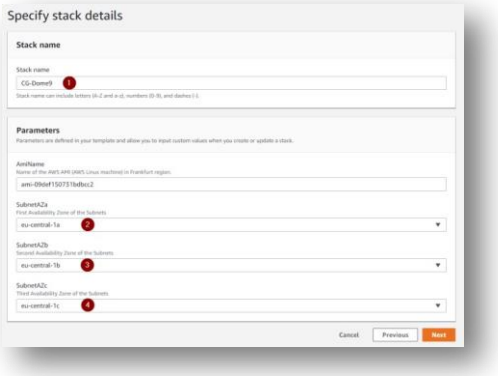


6. Mark the item '**Upload a template'**, and then using the Choose file button add the attached file from section 2 and then click 'Next'.

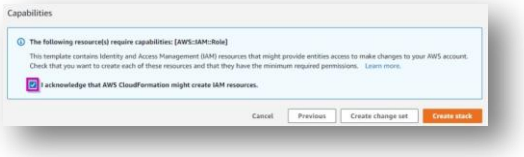


7. Click Next.

8. Fill in a name for your Stack (CG-Dome9 can be a good one) and the 3 availability zones.



6. Click Next
7. Click Next
8. Review the configuration and click the check box.



9. Click Next
10. The template will be deployed.

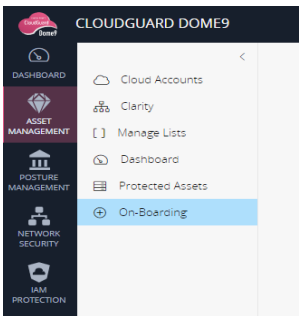
Step 2 *Connect your AWS account to the Dome9 account*

1. On a new browser / tab, connect to the Dome9 portal: **https://secure.dome9.com/v2/login**.

2. Log into the portal with the credentials you got in the email / on the screen.

Top tip: Use the accounts specified in the email / screen. If the AWS training account will be attached to other Dome9 account, the Dome9 account will be deleted automatically as part of the cleanup process.

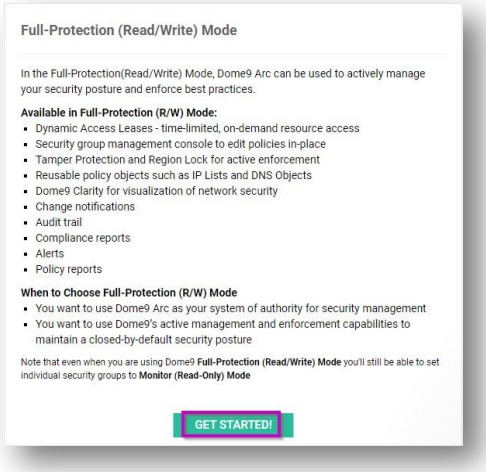
1. At the left~~top~~ bar choose Asset Management~~t~~On-Boarding.



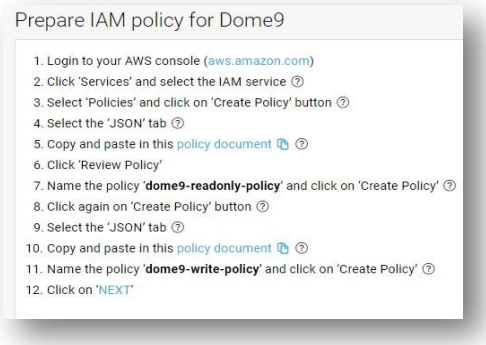
2. Select the "Get started with AWS".

3. Choose Full-Protection mode and click "GET STARTED!".

Commented [KM1]: Why are we choosing Full protection mode ? Is it the recommendation



4. Follow the steps on the screen.



a. Access the AWS console.
b. Click 'Services' and select the IAM service (or use the shortcut you have created).
c. Select 'Policies' and click on the 'Create Policy' button.
d. Select the 'JSON' tab.
e. Copy and paste the policy from the Dome9 portal into the JSON Policy window.

f. Click ‘Review Policy’.

g. Name the policy ‘dome9-readonly-policy’ and click on ‘Create Policy’.

h. Click again on ‘Create Policy’ button.

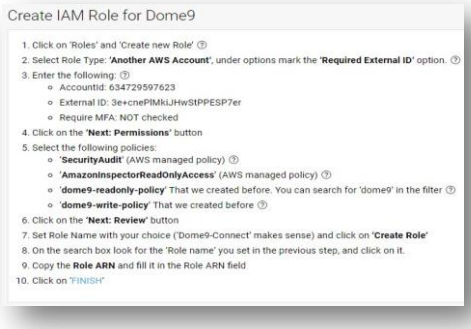
i. Select the ‘JSON’ tab.

j. Copy and paste the policy from the Dome9 portal into the JSON Policy window.

k. Name the policy ‘dome9-write-policy’ and click on ‘Create Policy’.

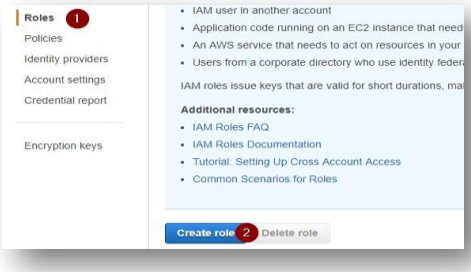
5. Click Next on the Dome9 screen.

6. Follow the steps on the screen.

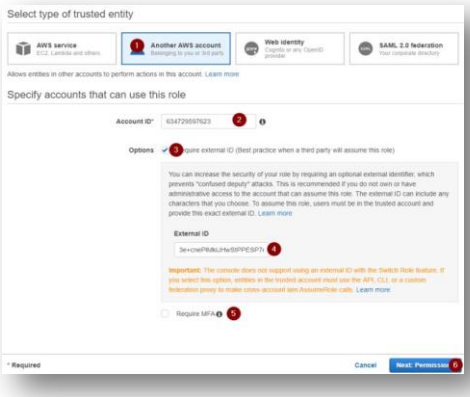


a. Click on ‘Roles’ and ‘Create Role’.

Commented [KM2]: Is there any reference documentation on the permissions set ?



b. Select Role Type: ‘Another AWS Account‘, under options mark the `Required External ID` option.



c. Enter the following:

i. AccountId: copy from the Dome9 screen. ii.

External ID: copy from the Dome9 screen.

iii. Require MFA: NOT checked.

d. Click on the 'Next: Permissions'button.

e. Select the following policies:

i. 'SecurityAudit' (AWS managed policy).

ii. 'AmazonInspectorReadOnlyAccess' (AWS managed policy). iii. 'dome9-readonly-policy' That we created before. You can search for 'dome9' in the filter.

iv. 'dome9-write-policy' That we created before.

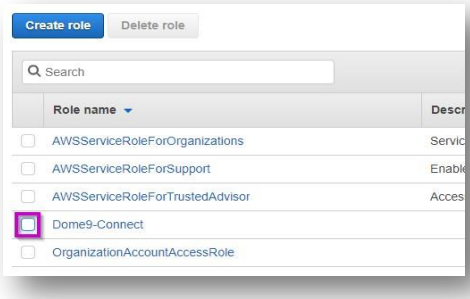
Commented [KM3]: Why do we need both a read only and also a write policy

f. Click on the 'Next: Tags' button.

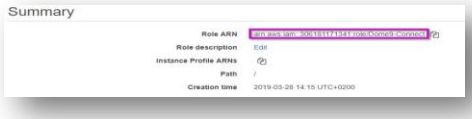
g. Click on the 'Next: Review' button.

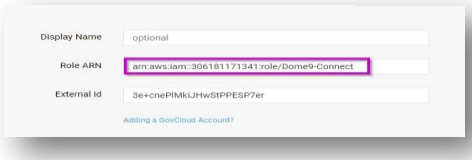
h. Set Role Name 'Dome9-Connect' and click on 'Create Role'.

i. On the search box look for 'Dome9-Connect', and click on it.

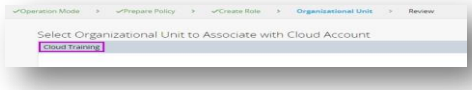


j. Copy the Role ARN and paste it in the Role ARN field on the Dome9 screen.

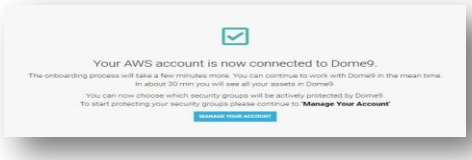




7. Click Next.
8. Select the Cloud Training organizational unit.



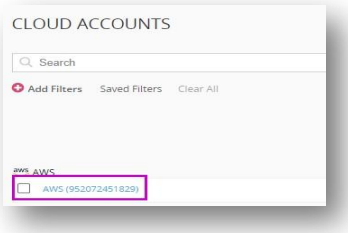
9. Click “Finish”.



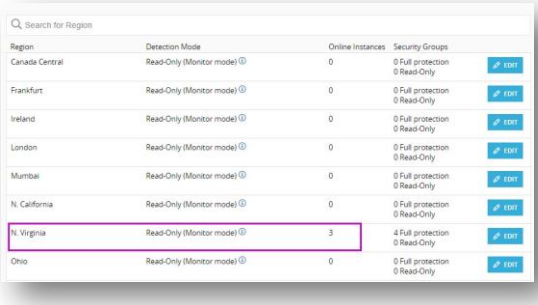
Step 3 *Verify your cloud account is boarded into the Dome9 Account*

1. On the Dome9 console, click on ASSET MANAGEMENT and then Cloud Accounts.

2. Make sure you see the on boarded cloud account.



3. Click on the account to view the account details.



You successfully finished Exercise #1

Exercise #2 – Asset Management - Review your Lab Assets

Purpose: To get familiar with the Cloud Inventory module

Description

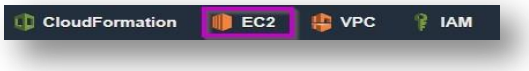
This exercise will guide you through the Cloud Inventory module.

Method

Using the AWS portal you will review the AWS deployed assets and then look at them through the Dome9 console.

Step 1 Review your AWS account assets

1. Open your AWS console and move to the EC2 page.



2. Find out how many instances you have and how many Security Groups you have deployed.

3. Click on the Running Instances link.
4. You have deployed 13 instances based on t2.nano type, look at the list and explore one of the machines to find out the VPC, Subnet, Security Groups, IP's.
5. On the left bar click the Security Groups section.

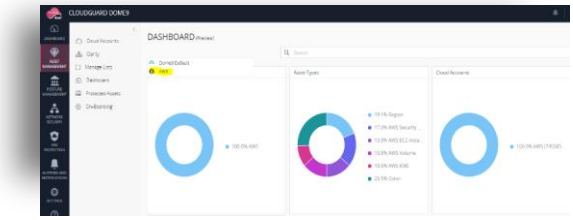
6. You have deployed 16 Security Groups, Explore some of them to find out which inbound and outbound rules have been created.

Step 2 Reviewing the Protected Assets screen

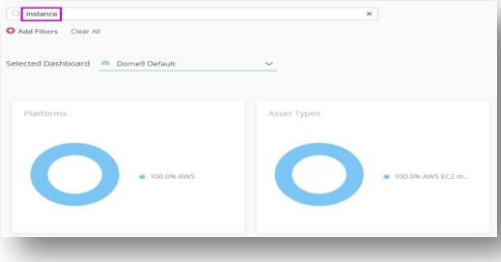
1. Move into the Dome9 console, click on Asset Management and then Protected Assets.

2. Go back to~~At~~ the dashboard, Select~~click on~~ AWS at the drop down~~he~~ left widget

Commented [KM4]: This didn't work



3. Review the list and filter via the upper bar to view only the 'instance' and then look for 'function'.



4. Click on the function to find out the details and security information.
5. Go back into the Protected Assets AWS view and look for machines with public IP.

6. Look for the one without public IP attached and understand why this asset is different.

Commented [KM5]: This has changed in new view I think – looked for function – it didn't work

Commented [KM6]: Found 13 instances on EC2, but protected assets showed 46 – why ? Dome9 showed 9 security groups / AWS shows 16 security groups in my region

You successfully finished Exercise #2

Exercise #3 – Network Security - Visualize security architecture

Purpose: Review the Security Configuration based on the Security Groups

Description

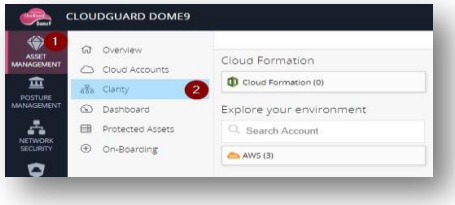
This exercise will guide you through your security configuration, as it is being reflected by the security groups of your cloud accounts.

Method

Using the Dome9 console, you will understand the security group's configuration and identify errors on that area.

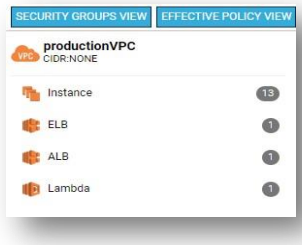
Step 1 Explore Clarity

1. On the CloudGuard Dome9 console, select Asset management and then click on the Clarity module.

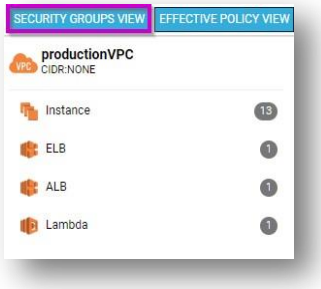


2. Open the AWS account, select the VPC and check how many assets that VPC holds?

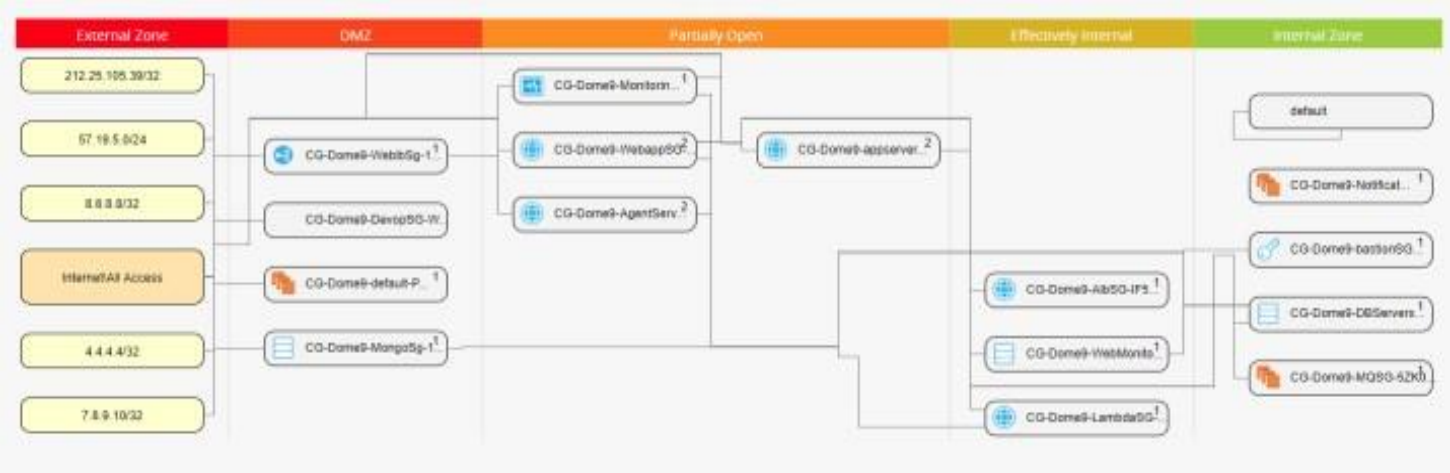
3. Once you choose the VPC you will see (on the right) a bar with the assets and object types that are deployed on the VPC.



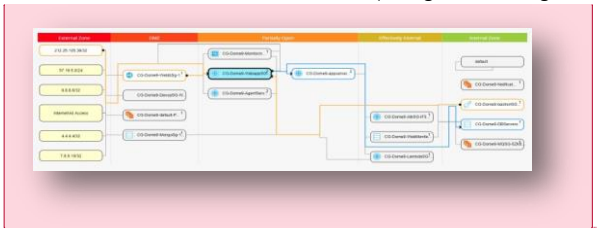
4. On the upper part of that bar click on the SECURITY GROUPS VIEW.



5. In the opened view we see a layout of the existing security groups inside that VPC; the service automatically classifies the security groups according to various levels of exposure to the public internet. On every SG (Security Group) you can see how many assets are deployed inside. The name starts with the CloudFormation name and then the name of the SG.



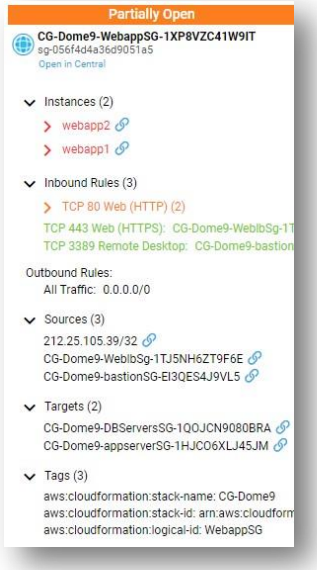
6. Click on the 'CG-Dome9-WebappSG' to find which machines can access the attached instances and which connection are allowed to other machines (Orange lines for ingress and Blue lines for egress)



7. On the bar on the right you will see the information about that SG connections, try to understand which instance is allowed to access the SG machines with remote desktop.

Commented [KM7]: Need to confirm if what I understood is clear

Commented [KM8]: I don't understand why new view is missing this functionality ! customer's loved this



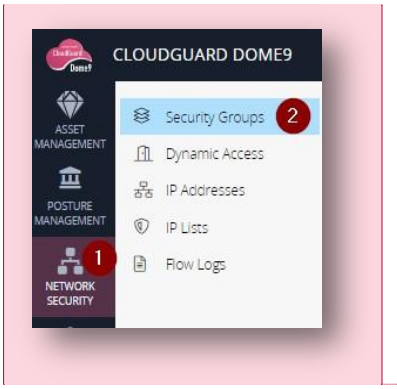
Step 2 Identify zombie security groups

1. A zombie SG is an SG that has no instances attached to it but has an exposed policy to the public internet and thus presents a security issue.
2. Look for an empty SG with connection from the internet.

Commented [KM9]: ssh access over internet

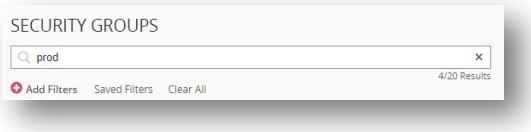
Step 3 *Managing Security Groups*

1. On the CloudGuard Dome9 console select Network Security and then click on Security Groups.



Commented [KM10]: I changed this pic to reflect change

2. This view will present all SG's imported from your cloud accounts.
3. Using the left side bar filter the SG's to those with a Tag value: 'prod'.



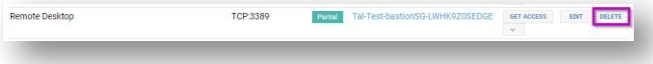
4. From the main Security Group view, choose the 'CG-Dome9-WebappSG' and review the configuration, look at:
    a. Tags
    b. Inbound
    c. outbound services
    d. Group members

5. On the upper bar you can switch between READ ONLY – FULL PROTECTION.

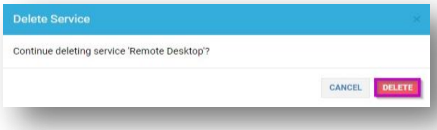
This SG is Tampered protection, the ability to create a baseline and delete all changes to the SG performed from the AWS console (All changes must be performed from the Dome9 Console).

Commented [KM11]: I need to understand the tamper protection in detail

6. Go to the inbound rule and delete the Remote Desktop rule from the rules.



7. Approve the popup by clicking 'DELETE'



8. Go back to the Clarity Security Groups View.
9. Choose the 'CG-Dome9-WebappSG' object and check if the deleted rule still exists

You successfully finished Exercise #3

Exercise #4 – Network Security - Dynamic Access

***Purpose: How to configure temporary access to an* internal web application server via http**

Description

This exercise shows how to get on demand access to ports and services using Dome9's Dynamic Access feature.

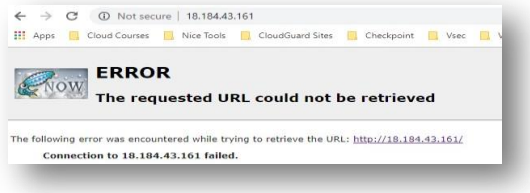
Method

Using the Dome9 console, you can see how that feature is working.

Step 1 Browsing to the Web Server

1. Open the Dome9 console on the protected assets view, search for the external IP address of the webapp2 instance.

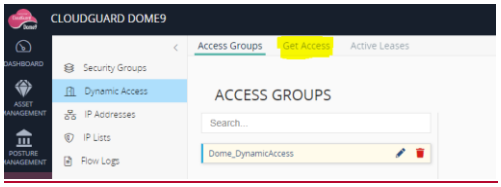
2. Open a new Tab in your browser; try to access the IP address you have found (Http).
3. The session should fail.



Step 2 Request access to the server

1. Select the Network Security section and then click on Dynamic Access.

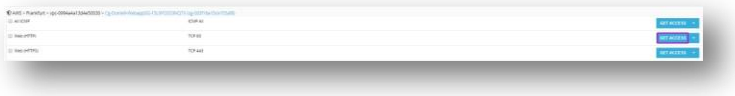
2. Select~~Choose to~~ tab ~~move to~~ 'Get Access'.



Formatted: Indent: Left: 0 cm, Hanging: 0.02 cm, No bullets or numbering

~~2.~~

You will see a number of possible options to allow access to the 'CG-Dome9-WebappSG', check Web (Http) and choose one hour Access.



3. That action will allow access from your machine's IP to that web server using Http.
4. Try to access the same IP address again, now you should get a different screen.

5. Go back to the Dynamic Access screen and ~~move~~ select ~~to~~ the Active Leases screen, you will see the configuration created to allow your access.

You successfully finished Exercise #4

Exercise #5 – Posture Management

Description

In this exercise you will become familiar with the Compliance and Governance module. You will practice running compliance bundles and create your own queries.

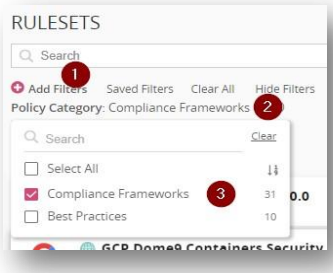
Method

Using Dome9 console, you will view how that feature is working.

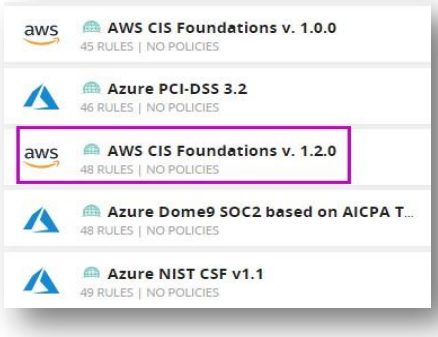
Step 1 running a compliance check

1. On the CloudGuard Dome9 console select Posture Management and then click on Compliance Rulesets.

2. The module has about 1500 compliance rules grouped together in more than 45 bundles.
3. On the upper bar, filter to show only Compliance Frameworks.

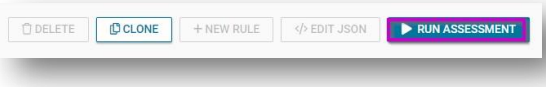


4. ~~Look to figure~~Find -out how many bundles are containing 48 rules.
5. Choose the 'AWS CIS Foundations v. 1.2.0' bundle.

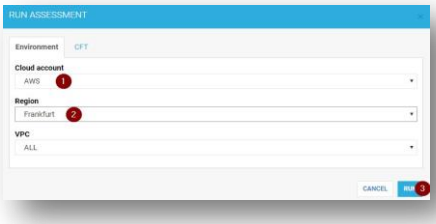


6. The window will display a list of rules for the CIS compliance check.
7. For every rule on the assessment you can view the description and the remediation procedure. Review the different rules, see that every query is written in GSL, and look at the format of the GSL instruction.

8. At the top of the page click on 'RUN ASSESSMENT'.



9. On the opened selection window, choose the account -> region and then run the assessment.



10. Once the report is displayed, find out the score of the test. Which entities have been tested?
11. Search for the rule: Enforce Password Policy, and click to expand the results, find out:
    a. How many assets where tested?
    b. What is the GSL query?
    c. Which account has failed the check?

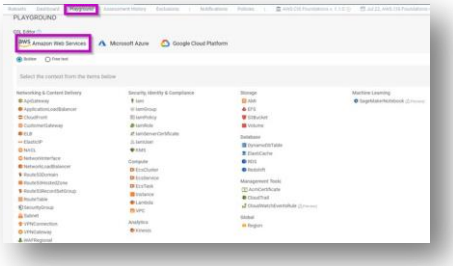
Commented [KM12]: Answer 1 ?

Commented [KM13]: Iam should have passwordPolicy.enabledInAccount=true

Commented [KM14]: (745585221363)

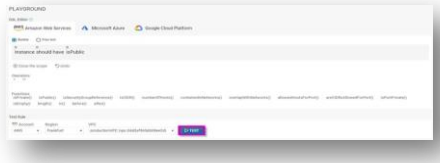
Step 2 Write your own rule

1. ~~On the upper ribbon, choose playground and then click on the rule builder tab~~Go back to Posture Management, Select GSL Builder.

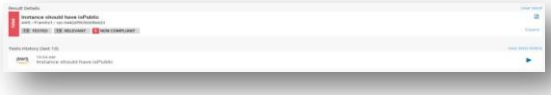


2. Here you can write your own queries before adding them to the bundles.
3. Click on the tiles to compose:
    a. Instance
    b. Should have
    c. IsPublic
    d. =
    e. True/False

~~c.~~4. Test Rule on AWS London VPC ALL
Click on test button.



~~4.~~5. Look at the results of this test and afterwards try to create your own rules using the rule builder.



You successfully finished Exercise #5

You have successfully finished the Dome9 Labs

