Cloud Security Assessment Sample Report

INFOPERCEPT
Sample Report 2020

Infopercept

YOUR DATE HERE

COMPANY NAME
Authored by: Your Name

Contents

Copyright

Disclaimer

By accessing and using this report you agree to the following terms and conditions and all applicable laws, without limitation or qualification, unless otherwise stated, the contents of this document including, but not limited to, the text and images contained herein and their arrangement are the property of Infopercept Consulting Pvt Ltd (Infopercept). Nothing contained in this document shall be construed as conferring by implication, estoppel, or otherwise, any license or right to any copyright, patent, trademark or other proprietary interest of Infopercept or any third party. This document and its contents including, but not limited to, graphic images and documentation may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, without the prior written consent of Infopercept. Any use you make of the information provided, is at your own risk and liability. Infopercept makes no representation about the suitability, reliability, availability, timeliness, and accuracy of the information, products, services, and related graphics contained in this document. All such information products, services, related graphics and other contents are provided 'as is' without warranty of any kind. The relationship between you and Infopercept shall be governed by the laws of the Republic of India without regard to its conflict of law provisions. You and Infopercept agree to submit to the personal and exclusive jurisdiction of the courts located at Mumbai, India. You are responsible for complying with the laws of the jurisdiction and agree that you will not access or use the information in this report, in violation of such laws. You represent that you have the lawful right to submit such information and agree that you will not submit any information unless you are legally entitled to do so.

Section 1 – Scope of Review

1. Primary Production Servers

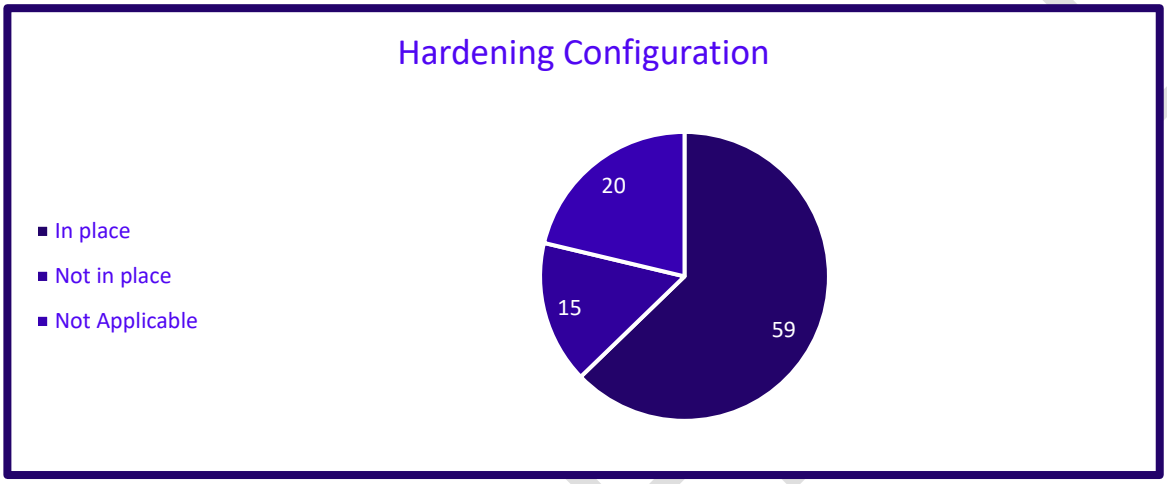
a. Live-ITR-Xyxyx-scraping-server-01
b. Live-REDHAT-1ST - HARDEN OS
c. LIVE-REDHAT-2ND-HARDEN-OS
d. ADMIN-PANEL-INSTANCE
e. ABCD-Live-Production-02
f. CHECK-POINT-GATEWAY-AUTOSCALING ALLBANKS-1
g. CHECK-POINT-GATEWAY-AUTOSCALING ALLBANKS-2
h. CHECK-POINT-VPNGW (ALL BANKS)
i. CHECK-POINT-MGMT (ALL BANKS)
j. CP - 2FA
k. Nginx-LB-Enterprise-Redhat-Production-XXY-XXZ-YYZ-ZZX-XXZ-1
l. Nginx-LB-Enterprise-Redhat-Production-XXY-XXZ-YYZ-ZZX-XXZ-2
m. RDS - PROD-XYZ-V2
n. NEW-TABLEAU-REDHAT-7-LINUX-APRIL-2019
o. NEW-REVERSE PROXY-TABLEAU-WITH LINUX-10-MAY-2019

2. Sub Production Servers

a. SPLUNK-DEPLOYER
b. SPLUNK-INDEXER-1
c. SPLUNK-INDEXER-2
d. SPLUNK-SEARCHHEAD-1
e. SPLUNK-SEARCHHEAD-2
f. Tableau windows server 13-04-2020

Section 2 – Summary

	In place	Not in place	Not Applicable	Percentage
Configuration point	59	15	20	79.72%



Section 3 – AWS Configuration Snapshots for CIS Three tier guidelines

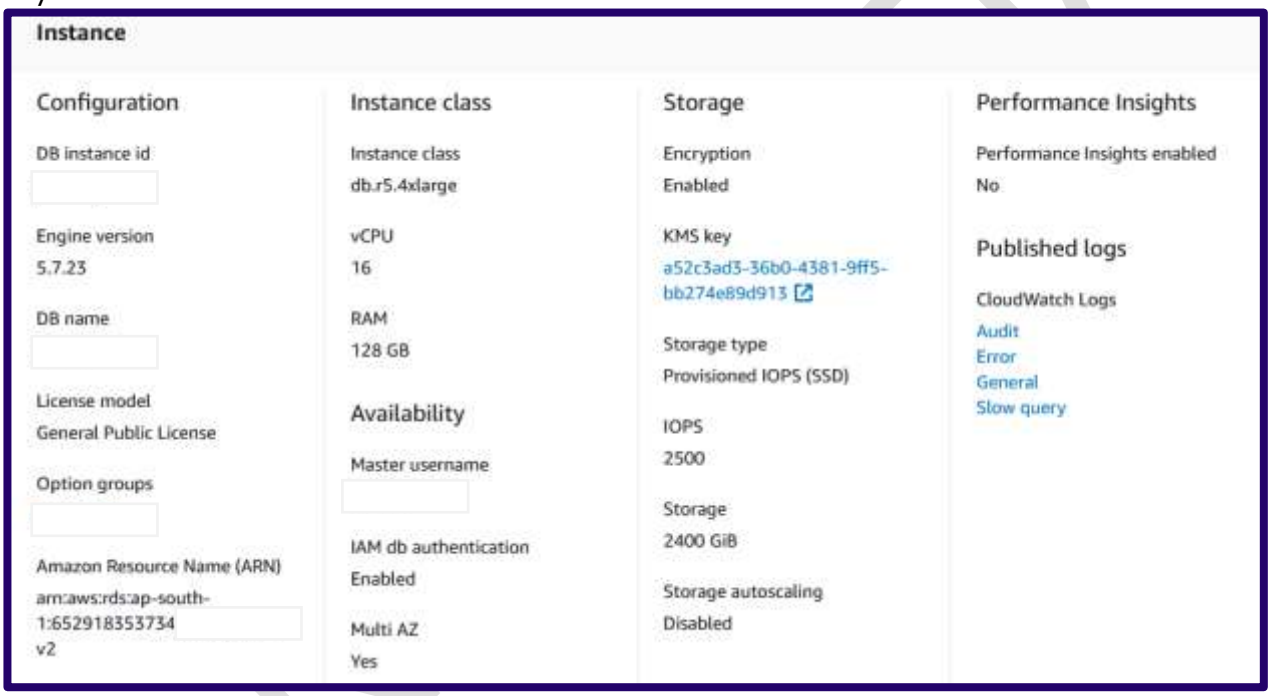
1. Data Protection: -

1.1 Ensure a customer created Customer Master Key (CMK) is created for the Web- tier /
1.2 Ensure a customer created Customer Master Key (CMK) is created for the App-tier /
1.3 Ensure a customer created Customer Master Key (CMK) is created for the Database-Tier

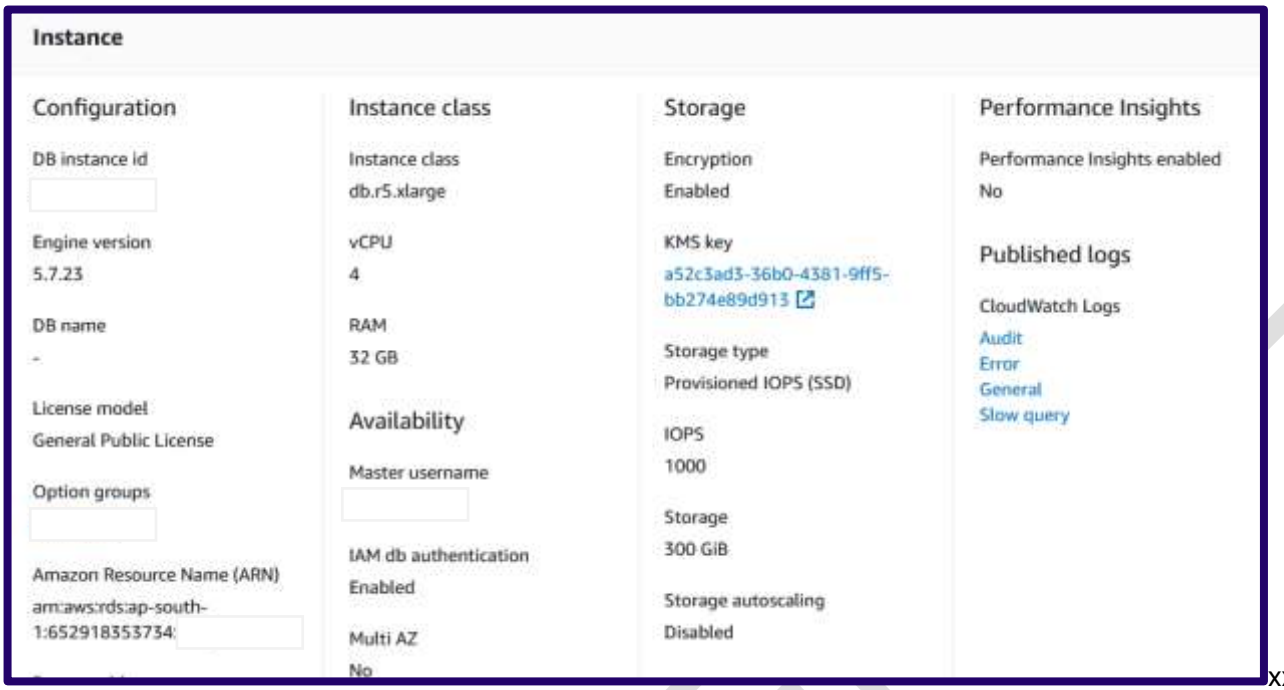
Note: Need to create CMK. Currently we are using AWS default KMS key everywhere.

1.4 Ensure Databases running on RDS have encryption at rest enabled

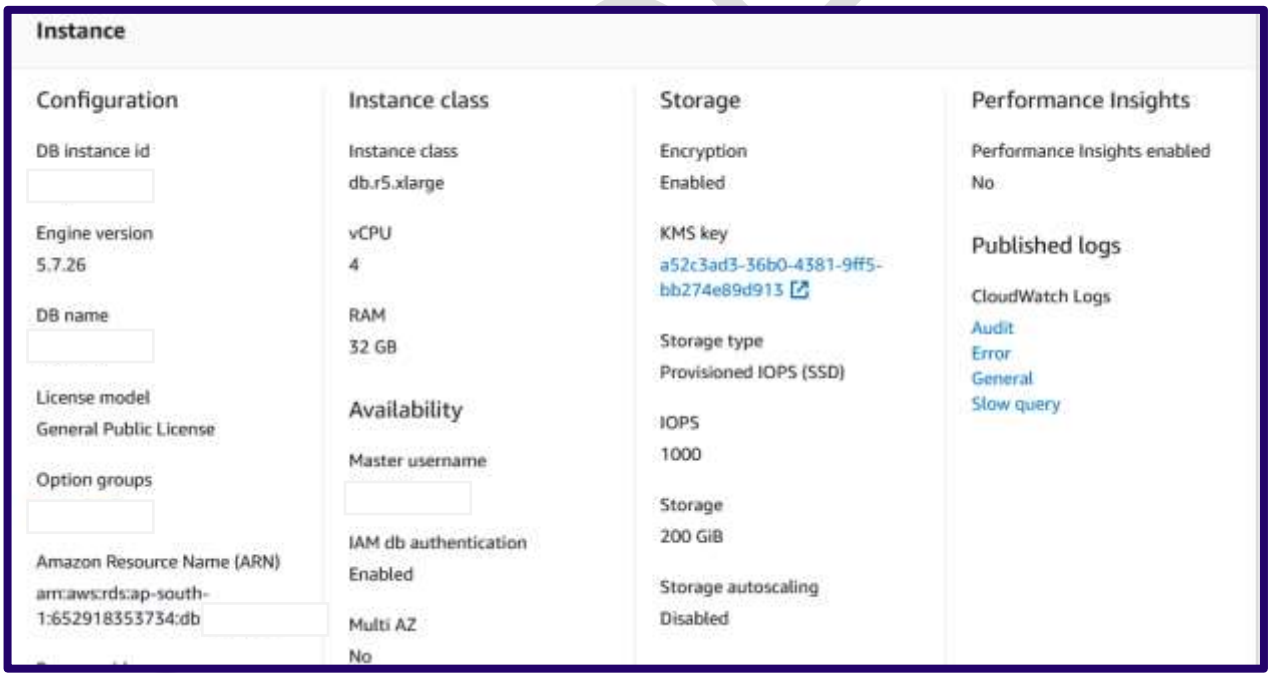
Prod-xyz-v2



Prod-xxy

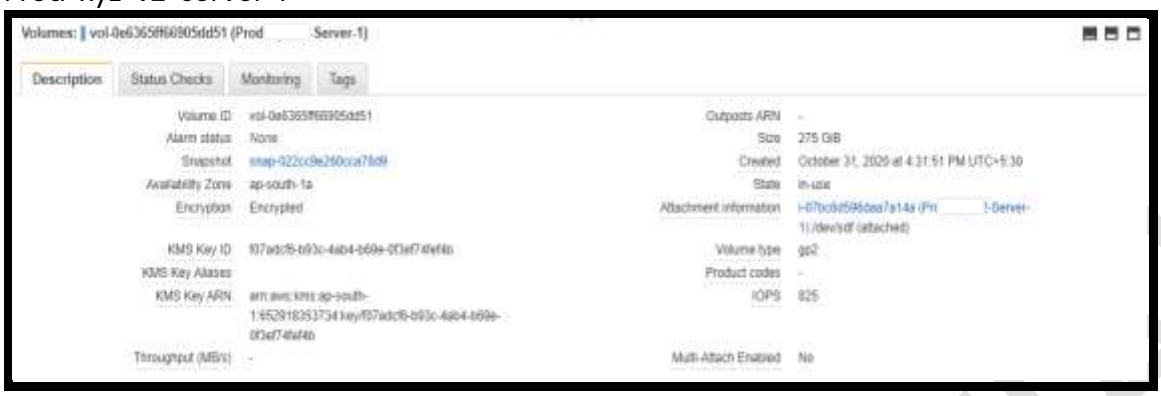


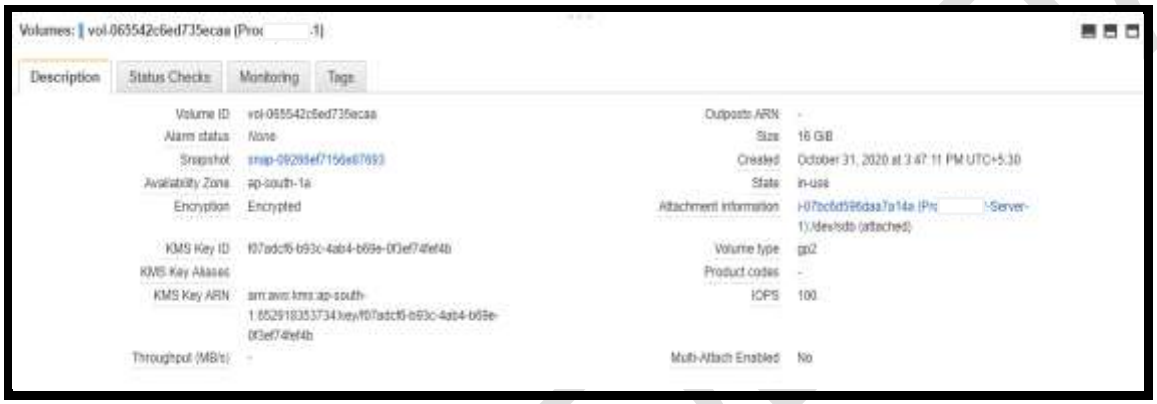
xxz-prod

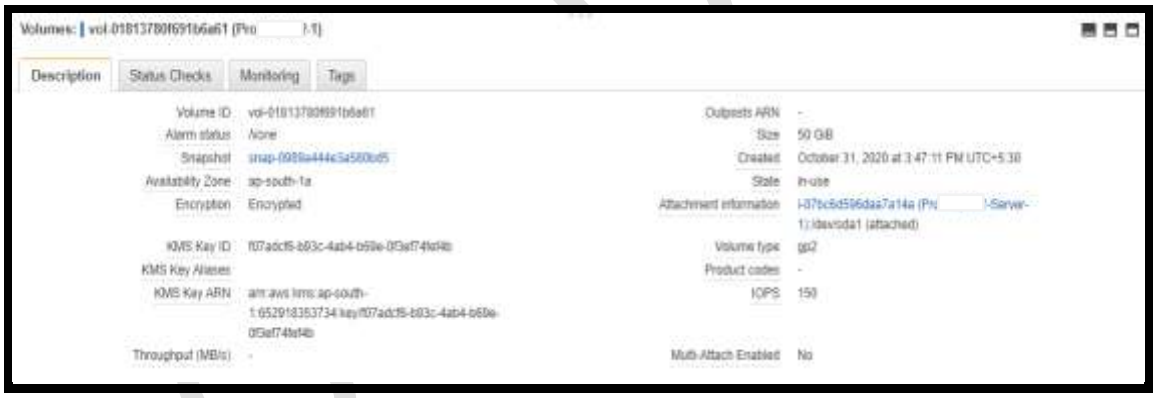


1.5 Ensure all EBS volumes for Web-Tier are encrypted / 1.6 Ensure all EBS volumes for App-Tier are encrypted

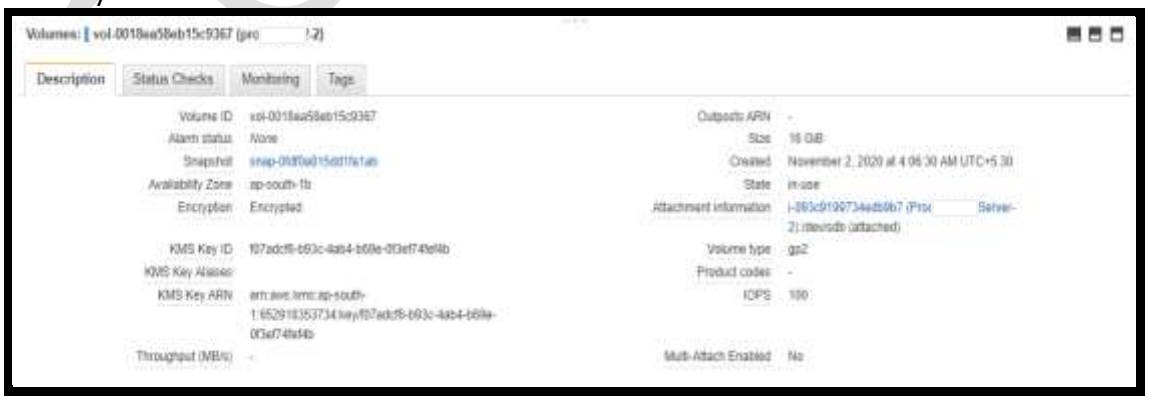
Prod-xyz-v2-server-1

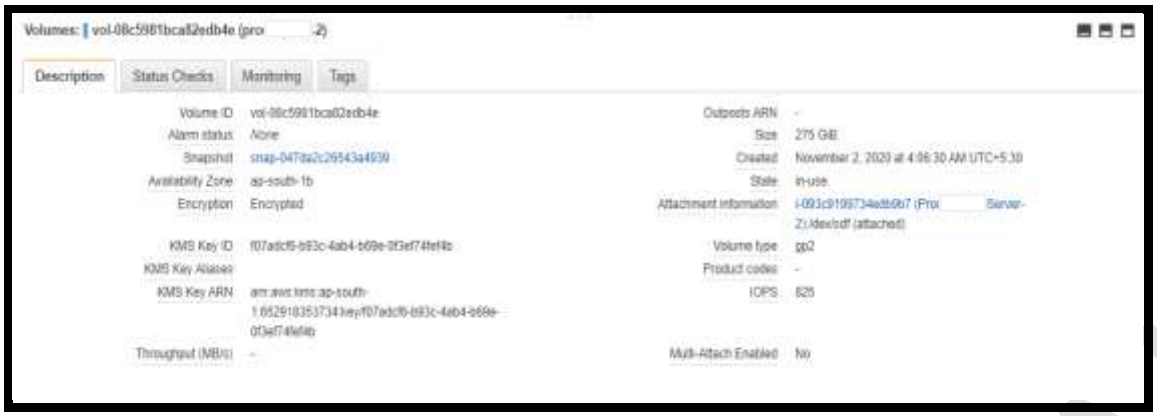


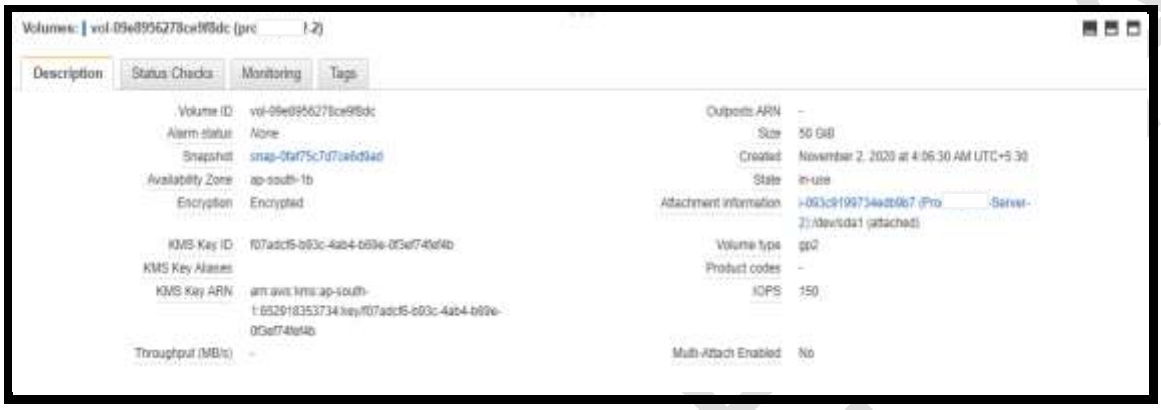




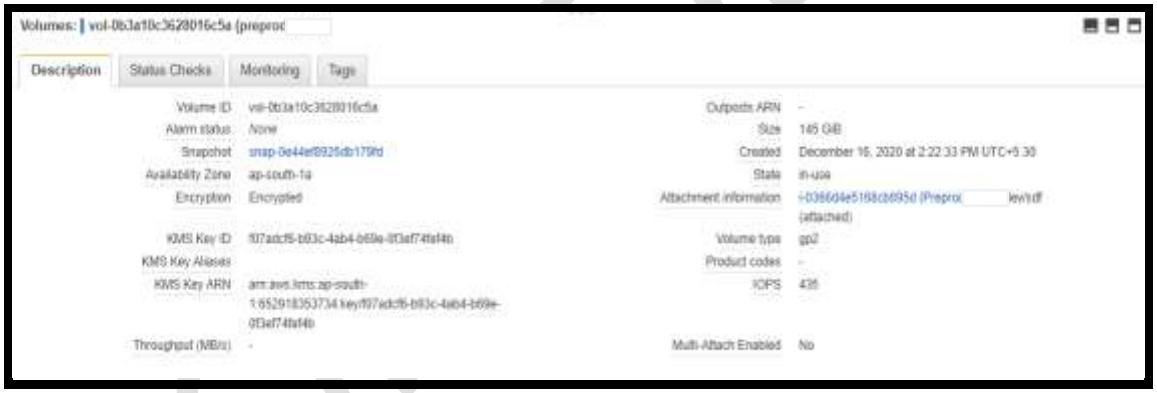
Prod-xyz-v2-2

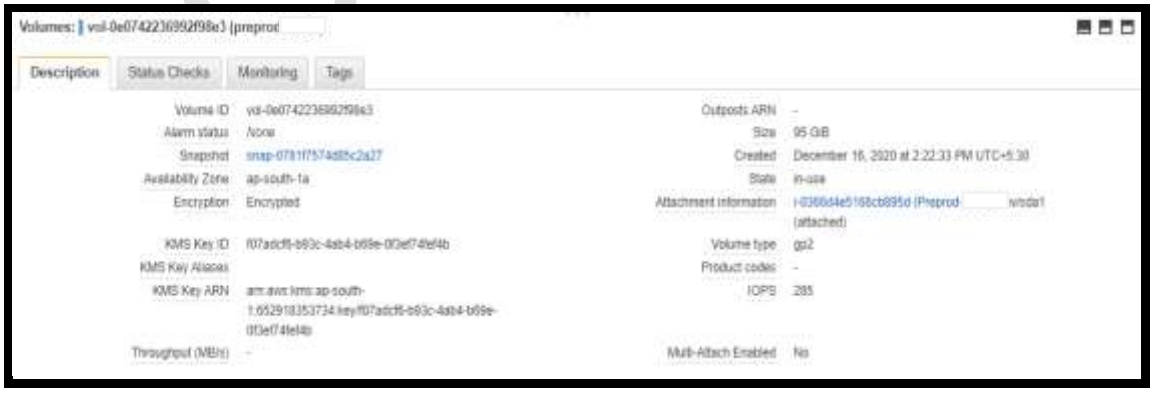


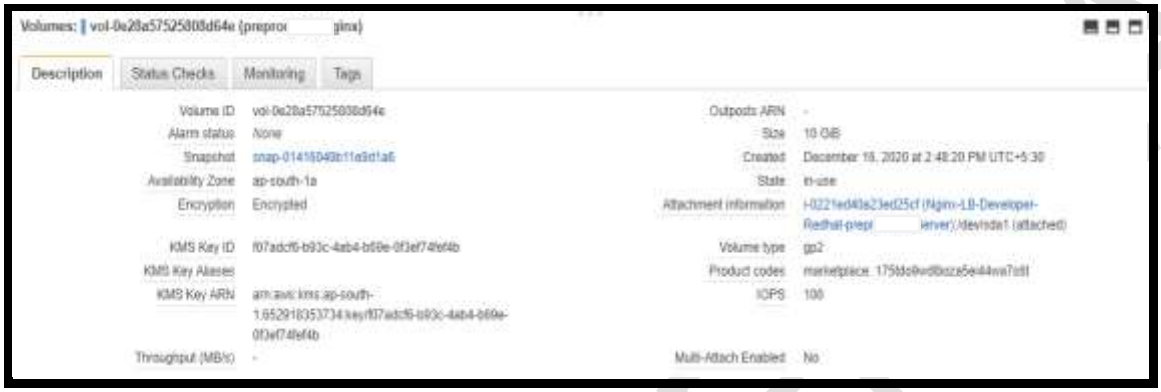




Prod-YYZ-1

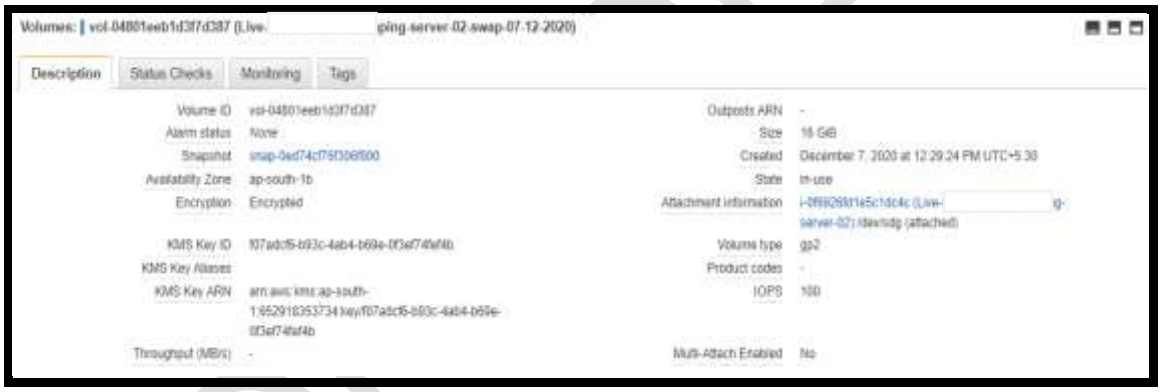




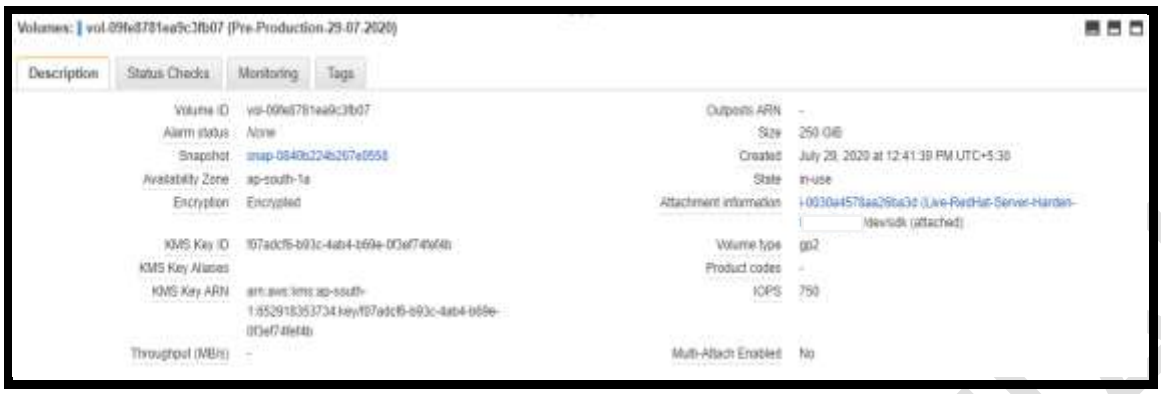


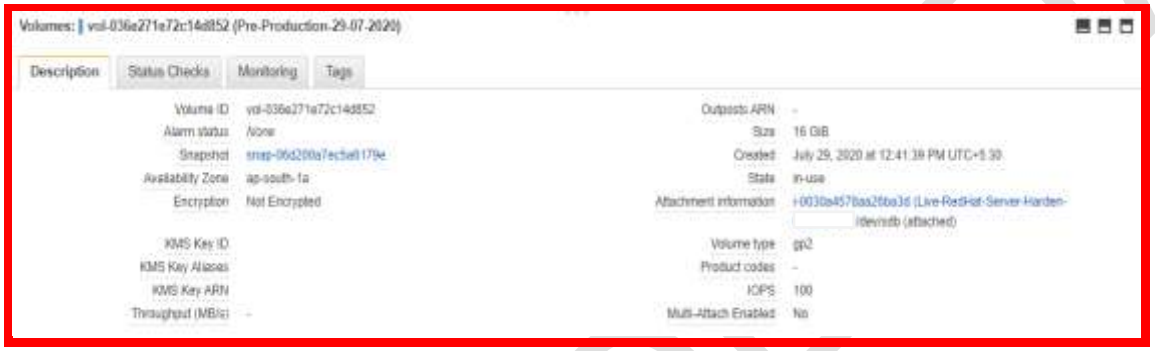
Live-ITR-Xyxyx-scraping-server-01-100GB

Live-ITR-Xyxyx-scraping-server-02-100GB



Pre-Production-29-07-2020

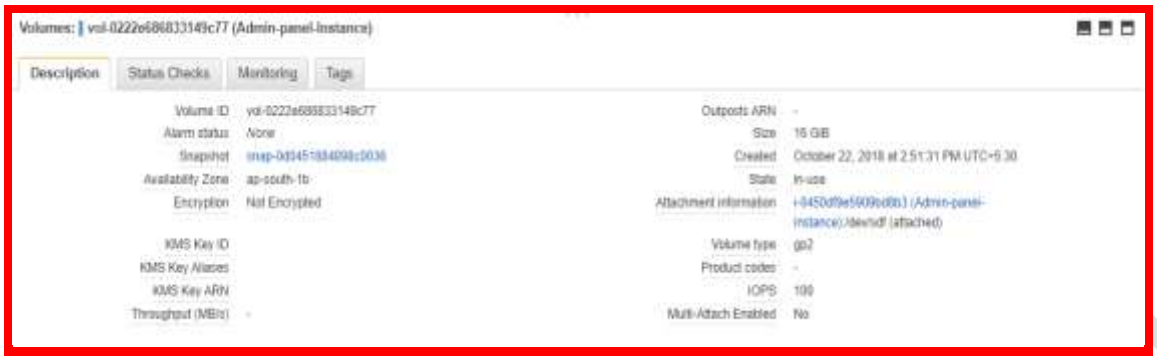




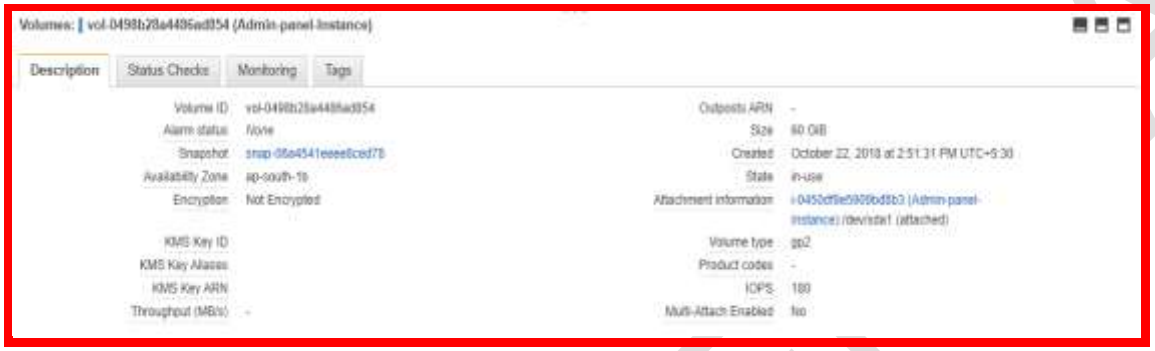
Not Encrypted

Trend-micro-windows

Admin-panel-Instance



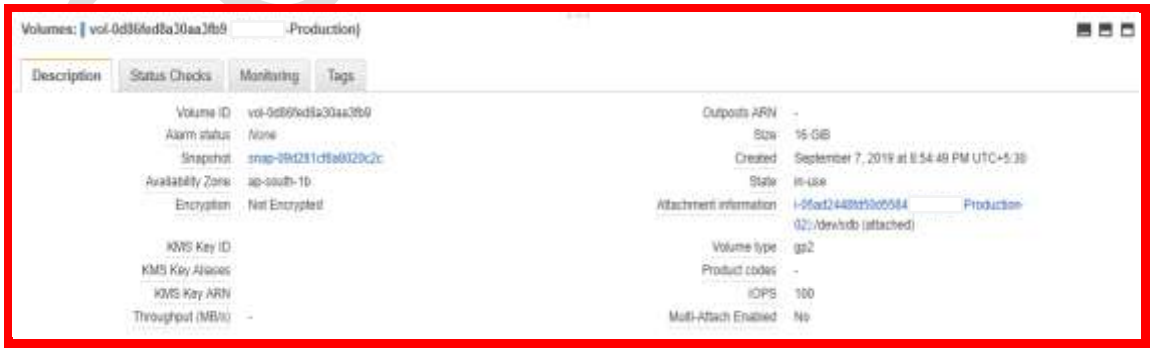
Not Encrypted



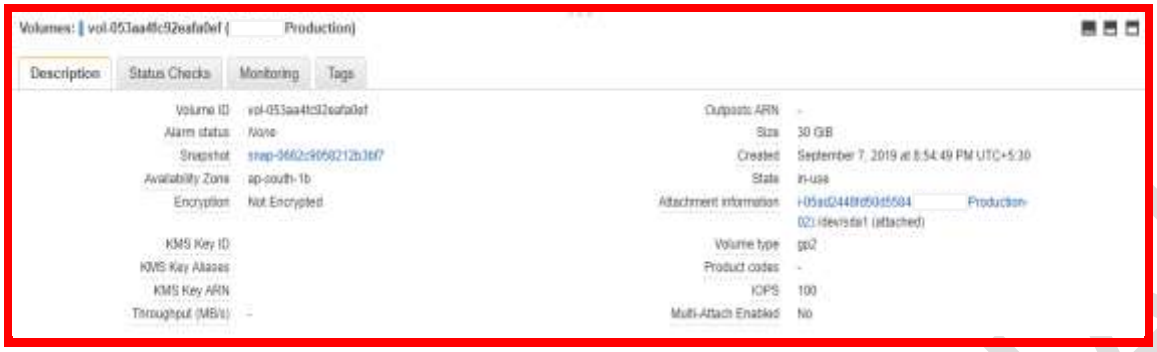
Not Encrypted

Tableau-server-13-04-2020

ABCD-Live-Production

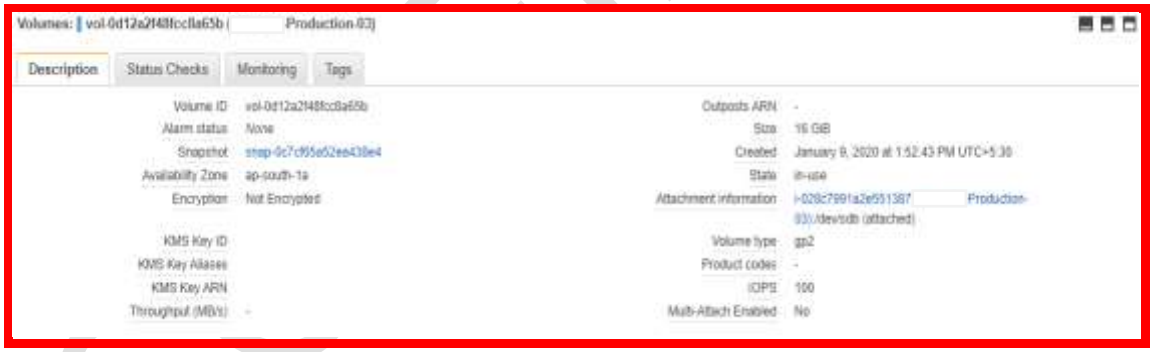


Not Encrypted

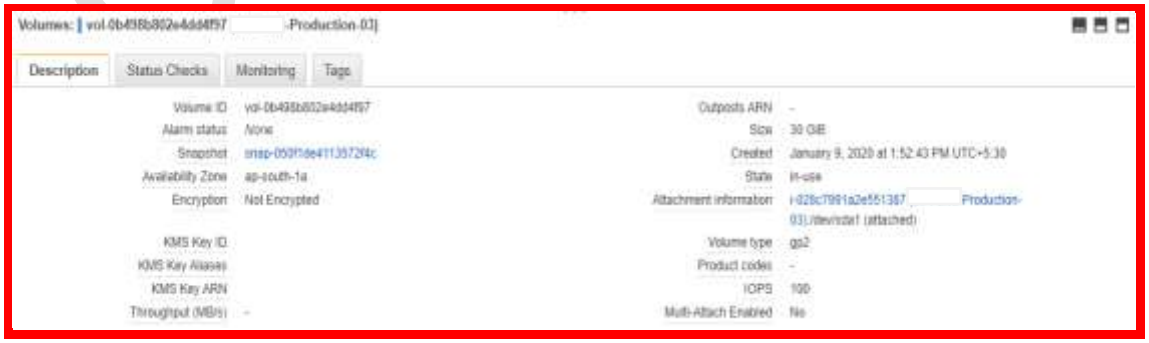


Not Encrypted

ABCD-Live-Production-03



Not Encrypted



Not Encrypted

New Tableau Rev.Proxy Server-10-May-2019

Nginx-LB-Enterprise-Redhat-Production-XXY-XXZ-YYZ-ZZX-XXZ

Nginx-LB-Enterprise-Redhat-Production-XXY-XXZ-YYZ-ZZX-XXZ-BackupServer

1.7 Ensure all customer owned Amazon Machine Images for web-tier are not shared publically

Prod-xyz-v2-server-1-19-12-2020

Prod-xyz-server-2-19-12-2020

ABCD-production-01-11-09-2019

ABCD-production-02-09-01-2020

Live-RedHat-Server-Harden-OS-YYZ-NEW1-21-11-2020

Live-ITR-Xyxyx-scraping-server-01-07-12-2020

Live-ITR-Xyxyx-scraping-server-02

Nginx-LB-Enterprise-Redhat-production-XXY-05-09-2020

Nginx-LB-Enterprise-Redhat-Production-XXY-XXZ-YYZ-ZZX-XXZ-01-11-2020

Linux-Reverse Proxy-Tableau-10-May-2019-14-09-2020

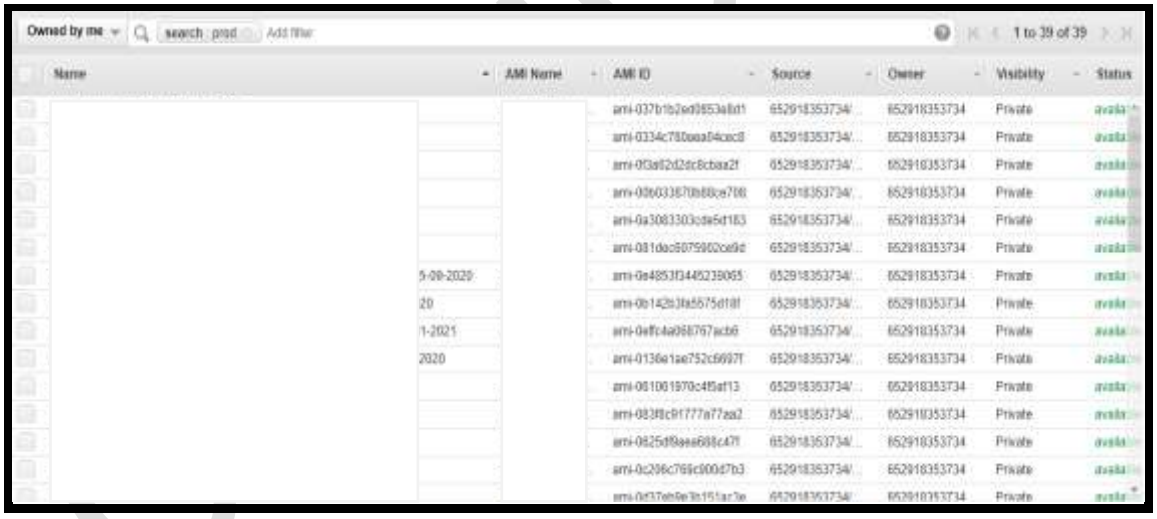
Nginx-LB-Enterprise-Redhat-Production-XXY-ABC-CTI-15-09-2020

Check-Point-Management-ALLBANKS-24-12-2020

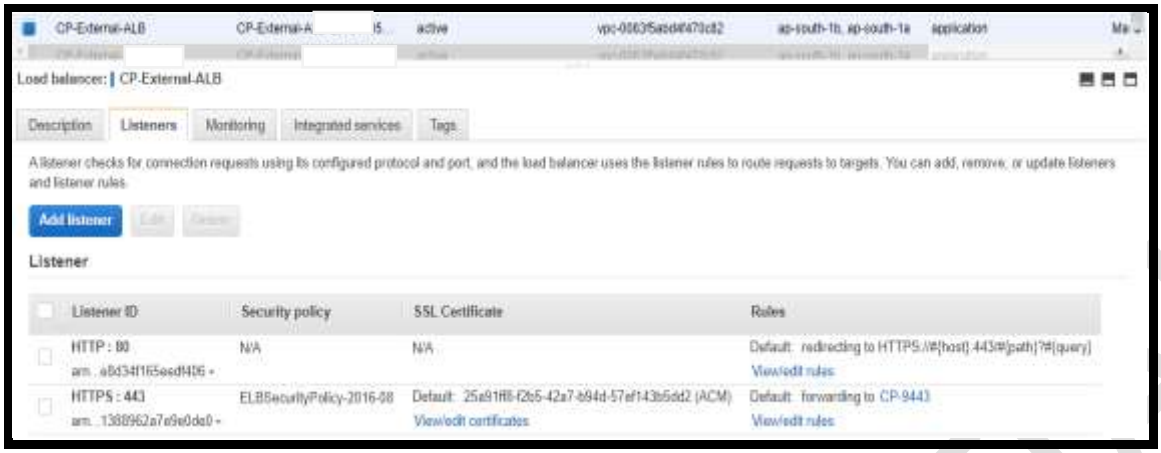
Check-Point-Gateway-VPN-ALLBANKS-24-12-2020

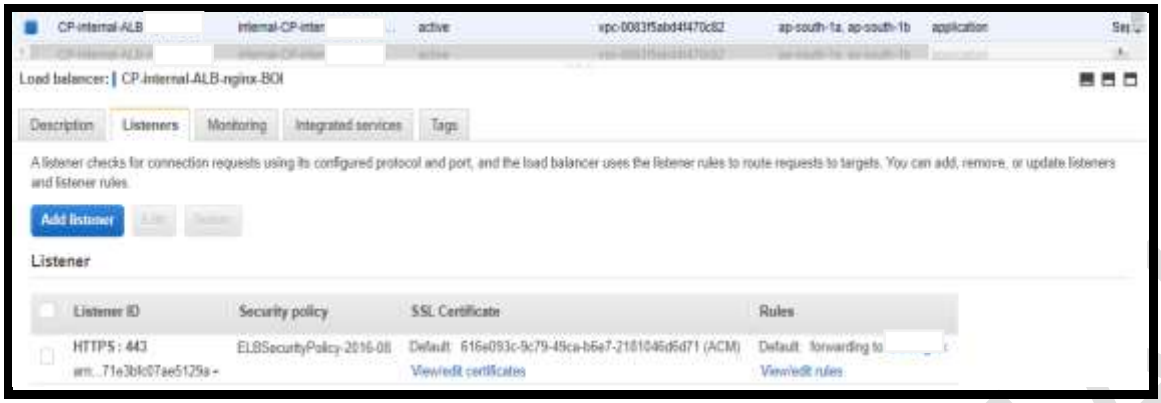
Check-Point-Gateway-AutoScaling-ALLBANKS-24-12-2020

1.8 Ensure all customer owned Amazon Machine Images for Application-tier are not shared publicly

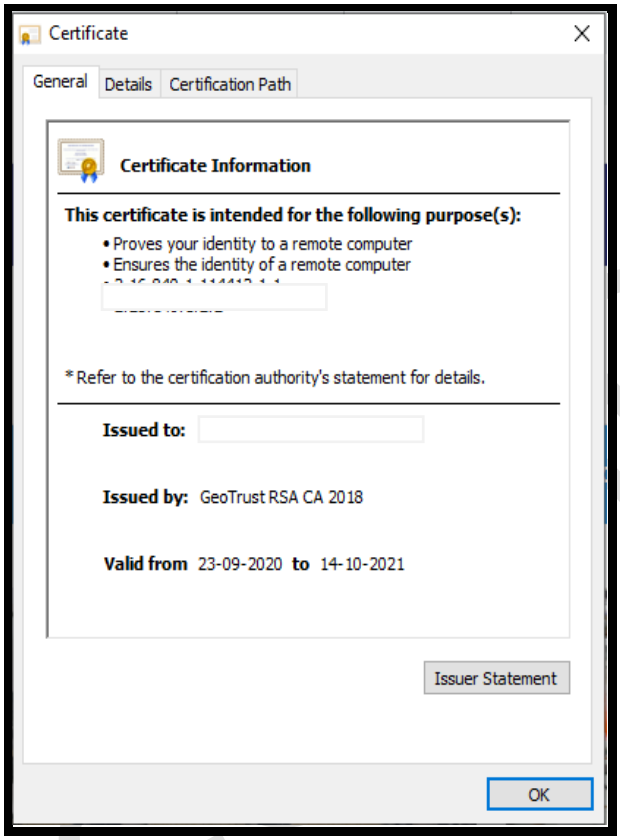


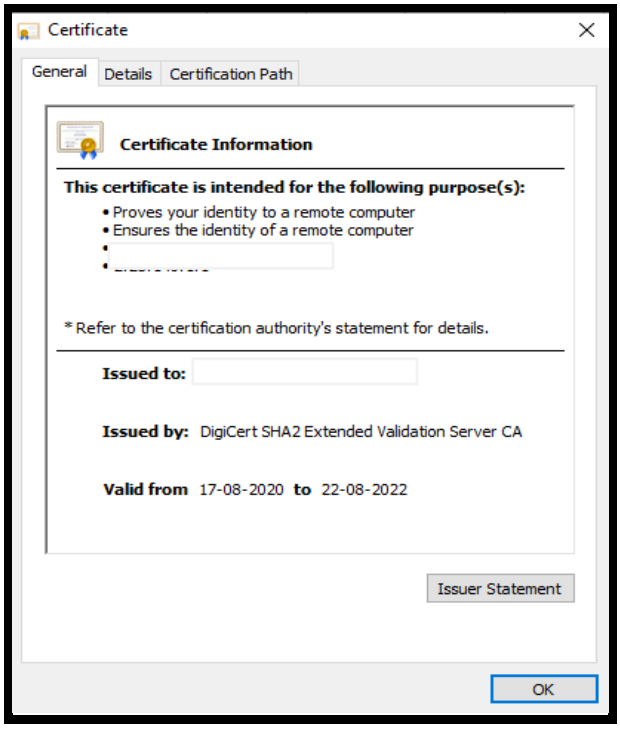
1.9 Ensure Web-tier ELB have SSl/TLS Certificate Attached / 1.10 Ensure web-tier ELB have the latest SSL Security policies configured / 1.11 Ensure web-tier ELB using HTTPS Listener / 1.12 Ensure App-tier ELB have SSL\TLS certificate attached / 1.13 Ensure App-tier ELB have the latest SSL security policies configured / 1.14 Ensure App-tier ELB is using HTTPS listener

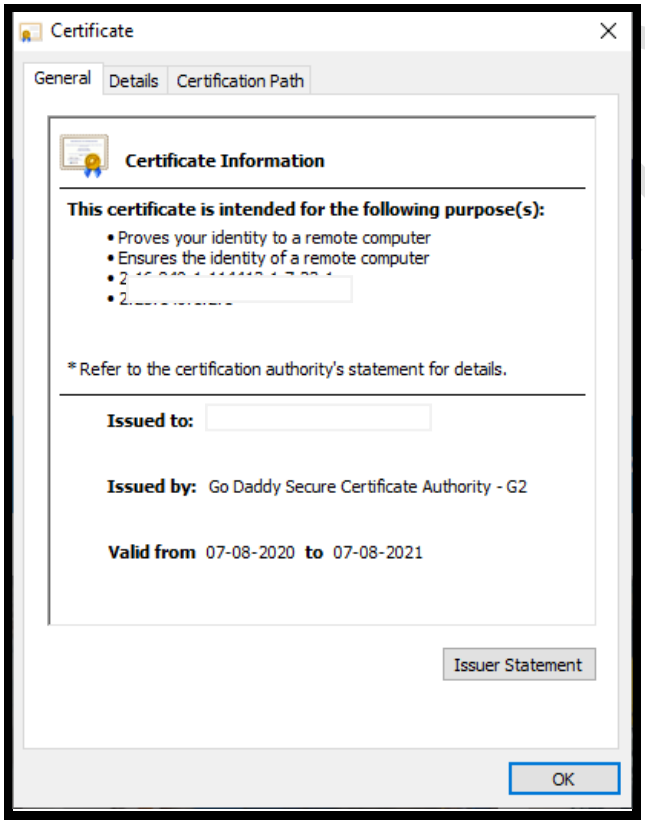


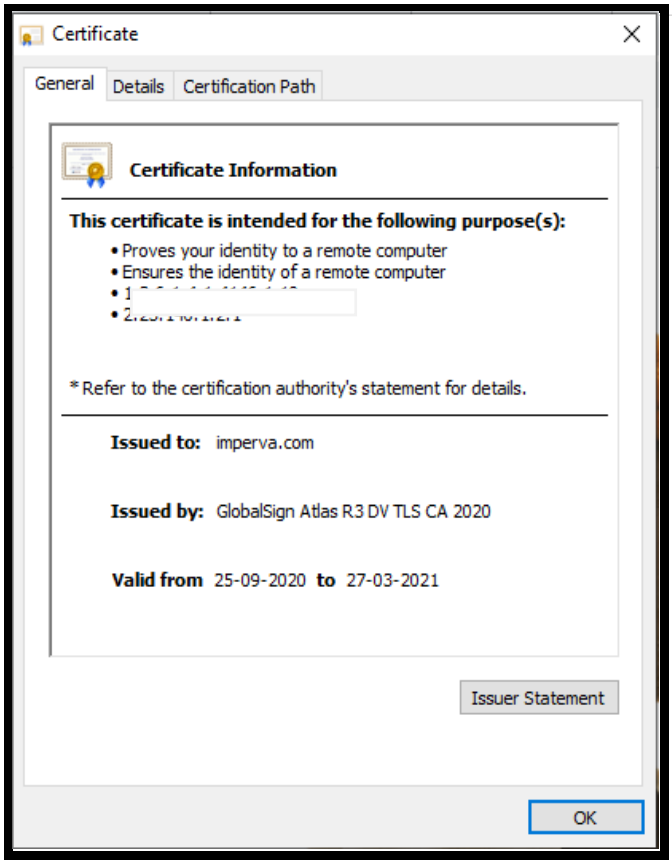


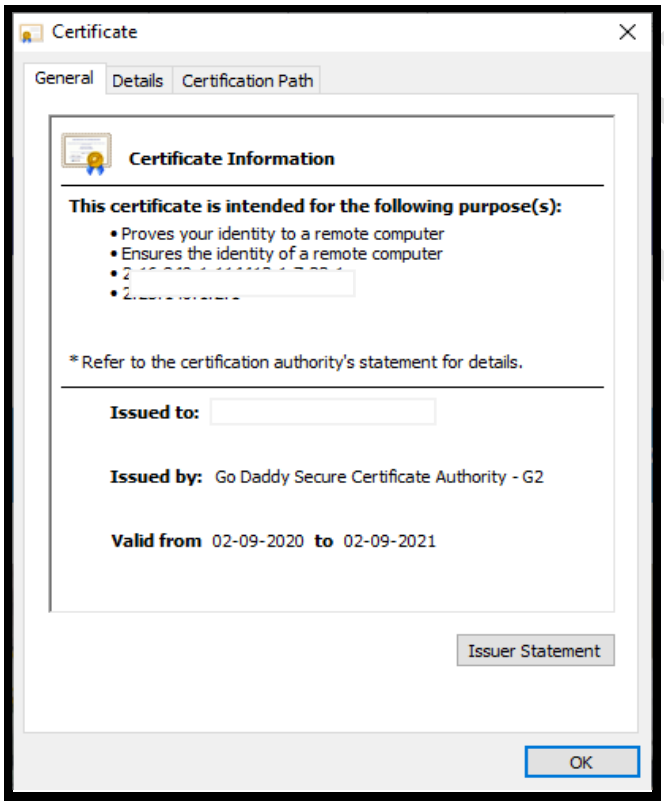
1.15 Ensure all public web-tier SSL\TLS certificates are>30 days from expiration

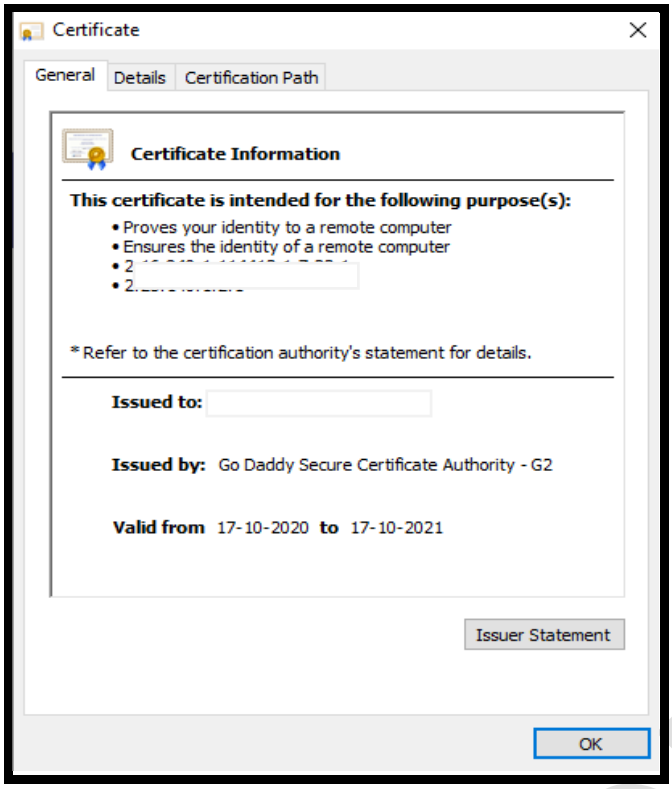


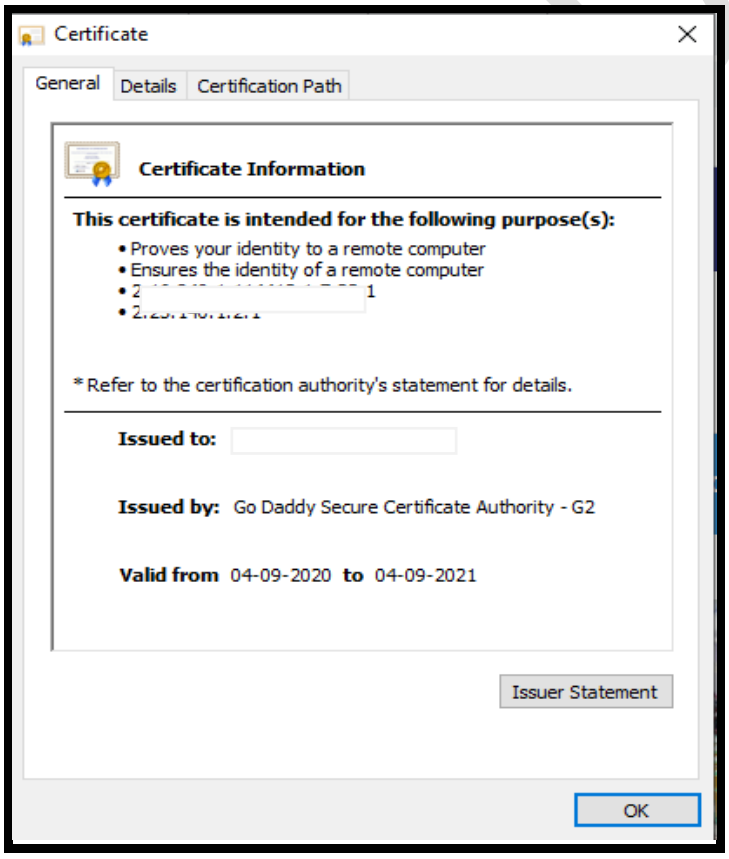

Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Proves your identity to a remote computer
• Ensures the identity of a remote computer
* Refer to the certification authority's statement for details.
Issued to:
Issued by: DigiCert SHA2 Extended Validation Server CA
Valid from 17-08-2020 to 22-08-2022
Issuer Statement
OK

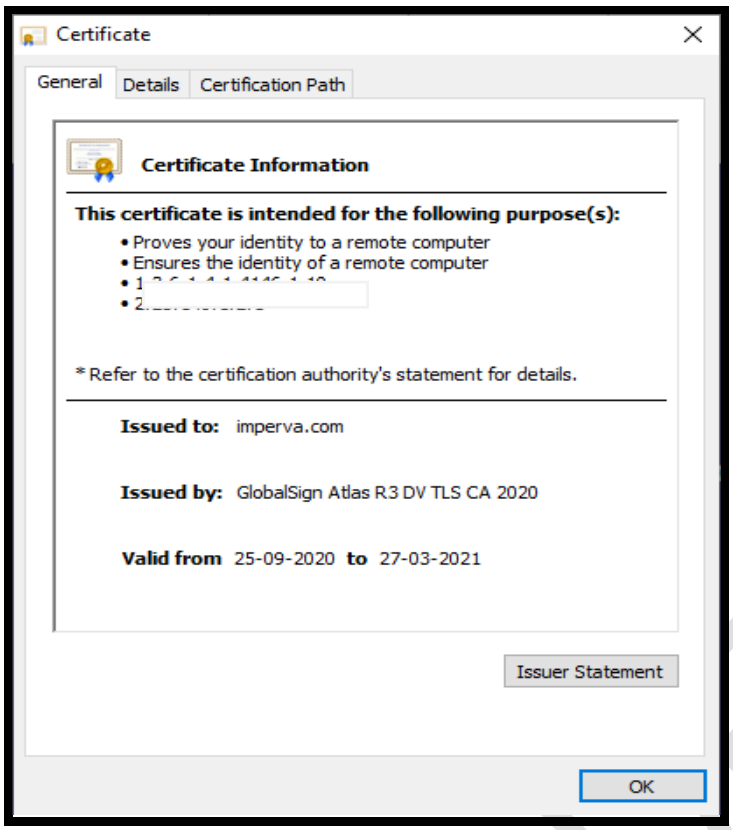

Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Proves your identity to a remote computer
• Ensures the identity of a remote computer
* Refer to the certification authority's statement for details.
Issued to:
Issued by: Go Daddy Secure Certificate Authority - G2
Valid from 07-08-2020 to 07-08-2021
Issuer Statement
OK


Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Proves your identity to a remote computer
• Ensures the identity of a remote computer
• 1
• 2.23.140.1.2.1
* Refer to the certification authority's statement for details.
Issued to: imperva.com
Issued by: GlobalSign Atlas R3 DV TLS CA 2020
Valid from 25-09-2020 to 27-03-2021
Issuer Statement
OK


Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Proves your identity to a remote computer
• Ensures the identity of a remote computer
• 2
• 2
* Refer to the certification authority's statement for details.
Issued to:
Issued by: Go Daddy Secure Certificate Authority - G2
Valid from 02-09-2020 to 02-09-2021
Issuer Statement
OK


Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Proves your identity to a remote computer
• Ensures the identity of a remote computer
• 2
• 2
* Refer to the certification authority's statement for details.
Issued to:
Issued by: Go Daddy Secure Certificate Authority - G2
Valid from 17-10-2020 to 17-10-2021
Issuer Statement
OK


Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Proves your identity to a remote computer
• Ensures the identity of a remote computer
• 2 1
• 2.23.140.1.2.1
* Refer to the certification authority's statement for details.
Issued to:
Issued by: Go Daddy Secure Certificate Authority - G2
Valid from 04-09-2020 to 04-09-2021
Issuer Statement
OK



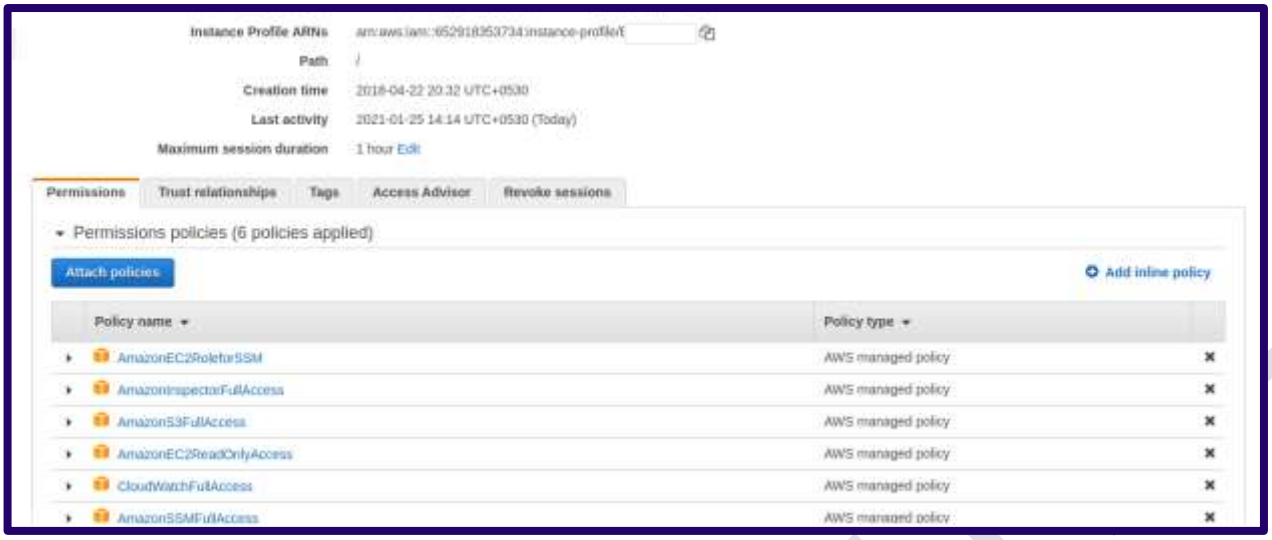
1.16 Ensure all S3 buckets have policy to require server-side and in transit encryption for all objects stored in bucket.

Note: Need to encrypt S3 buckets.

1.17 Ensure CloudFront to Origin connection is configured using TLS1.1+ as the SSL\TLS protocol (NA)

2 Identity and Access Management

2.1 Ensure IAM Policy for EC2 IAM Roles for Web tier is configured /
2.2 Ensure IAM Policy for EC2 IAM Roles for App tier is configured /
2.3 Ensure an IAM Role for Amazon EC2 is created for Web Tier /
2.4 Ensure an IAM Role for Amazon EC2 is created for App Tier



2.5 Ensure AutoScaling Group Launch Configuration for Web Tier is configured to use a customer created Web-Tier IAM Role / 2.6 Ensure AutoScaling Group Launch Configuration for App Tier is configured to use an App-Tier IAM Role. Not Applicable

2.7 Ensure an IAM group for administration purposes is created.

Note: Needs to be configured.

2.8 Ensure an IAM policy that allows admin privileges for all services used is created.

2.9 Ensure SNS Topics do not Allow 'Everyone' To Publish.

```
{
  "Version": "2012-10-17",
  "Id": "__default_policy_ID",
  "Statement": [
    {
      "Sid": "__default_statement_ID",
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": [
        "SNS:GetTopicAttributes",
        "SNS:SetTopicAttributes",
        "SNS:AddPermission",
        "SNS:RemovePermission",
        "SNS:DeleteTopic",
```

```
"Action": [
  "SNS:GetTopicAttributes",
  "SNS:SetTopicAttributes",
  "SNS:AddPermission",
  "SNS:RemovePermission",
  "SNS:DeleteTopic",
  "SNS:Subscribe",
  "SNS:ListSubscriptionsByTopic",
  "SNS:Publish",
  "SNS:Receive"
],
"Resource": "arn:aws:sns:ap-south-1:652918                    ts",
"Condition": {
  "StringEquals": {
    "AWS:SourceOwner": "652918353734"
  }
```

```
    {
      "Sid": "AWSEvents_Prod-Web-EC2-Status-Change_Id69957605406685",
      "Effect": "Allow",
      "Principal": {
        "Service": "events.amazonaws.com"
      },
      "Action": "sns:Publish",
      "Resource": "arn:aws:sns:ap-south-1:6529183537                    ts"
    }
```

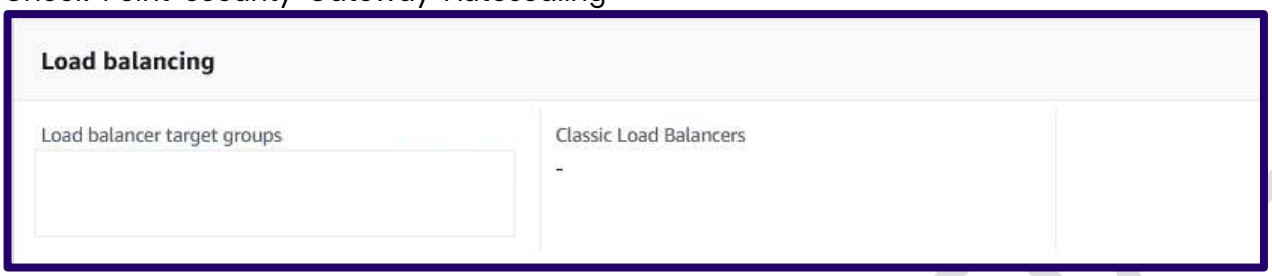
2.10 Ensure SNS Topics do not Allow 'Everyone' To Subscribe

Couldn't create subscription.
Error code: AuthorizationError - Error message: User: arn:aws:iam::652918353734:user/(or is not authorized to perform: SNS:Subscribe on resource: arn:aws:sns:ap-south-1:652918353734 rts

3 Business Continuity

3.1 Ensure each Auto-Scaling Group has an associated Elastic Load Balancer

Check-Point-Security-Gateway-Autoscaling



3.2 Ensure each Auto-Scaling Group is configured for multiple Availability Zones

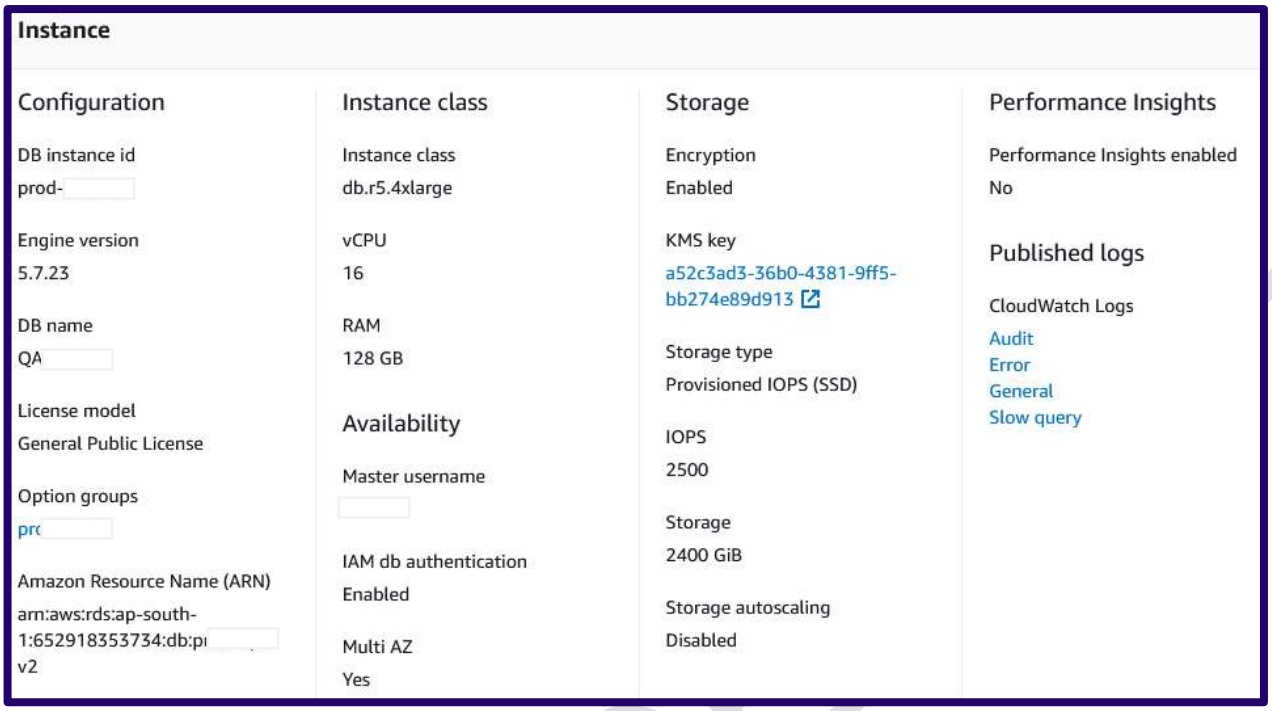
Check-Point-Security-Gateway-Autoscaling

3.3 Ensure Auto-Scaling Launch Configuration for Web-Tier is configured to use an approved Amazon Machine Image / 3.4 Ensure Auto-Scaling Launch Configuration for App-Tier is configured to use an approved Amazon Machine Image

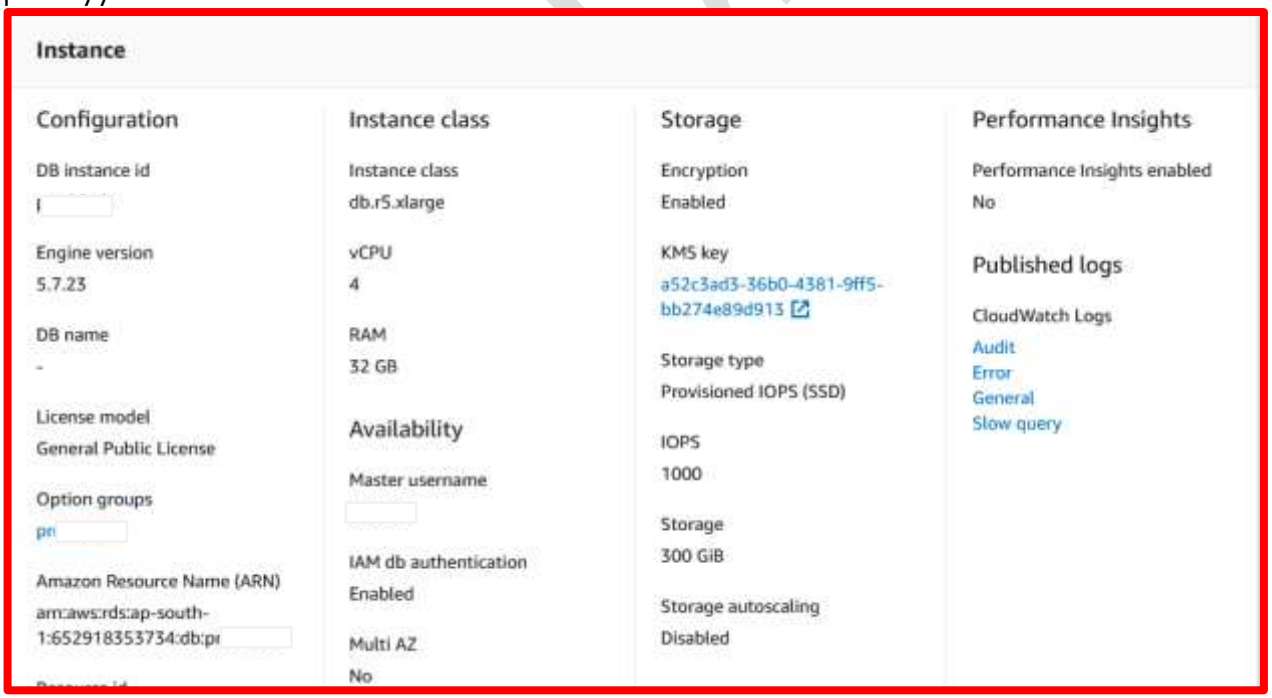
Check-Point-Security-Gateway-Autoscaling

3.5 Ensure Relational Database Service is Multi-AZ Enabled

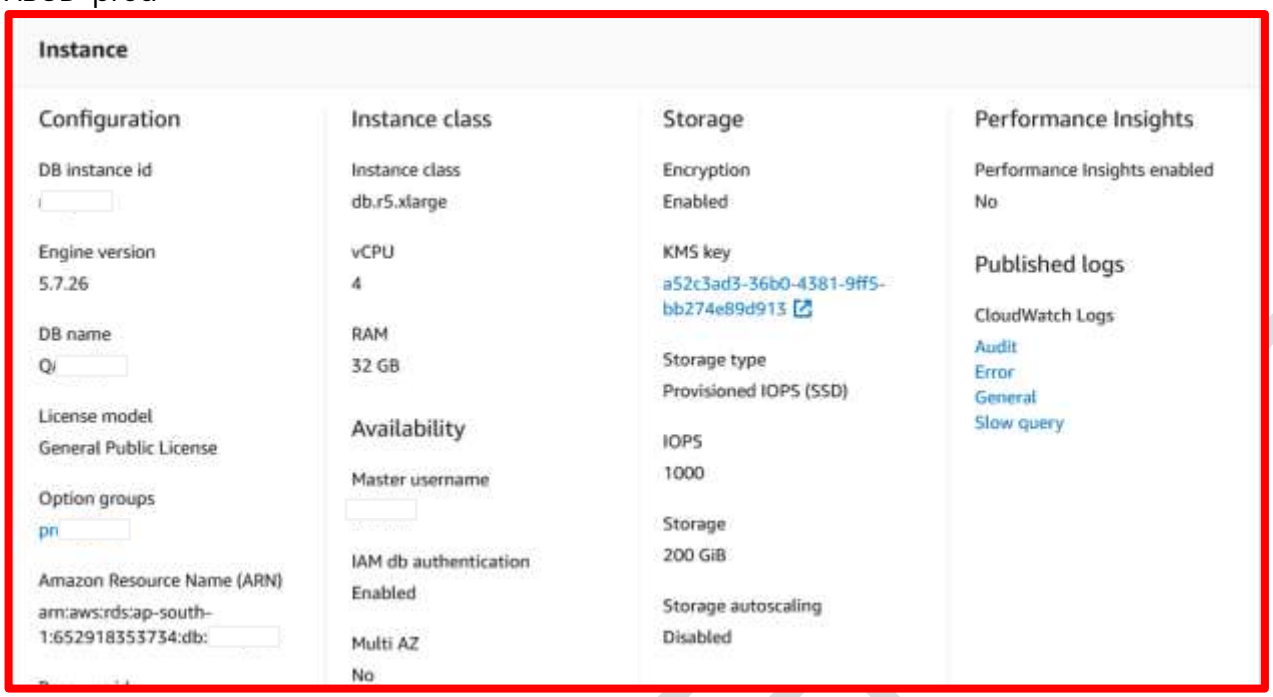
prod-xyz-v2



prod-yyz

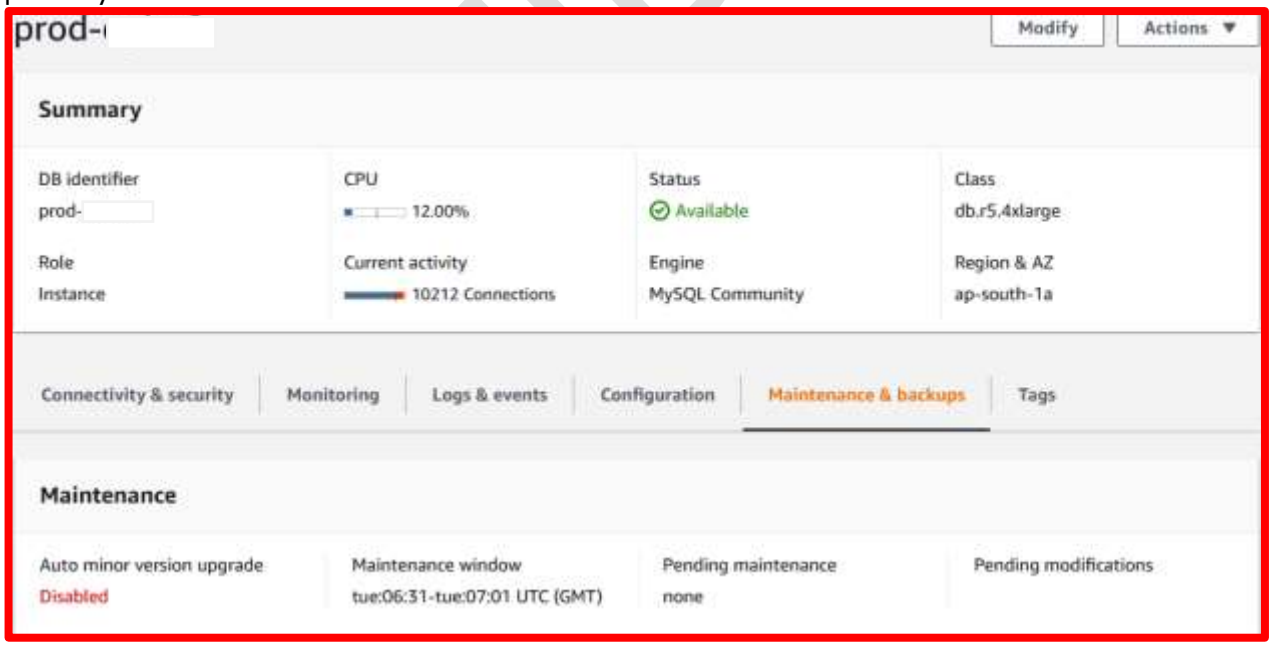


ABCD-prod

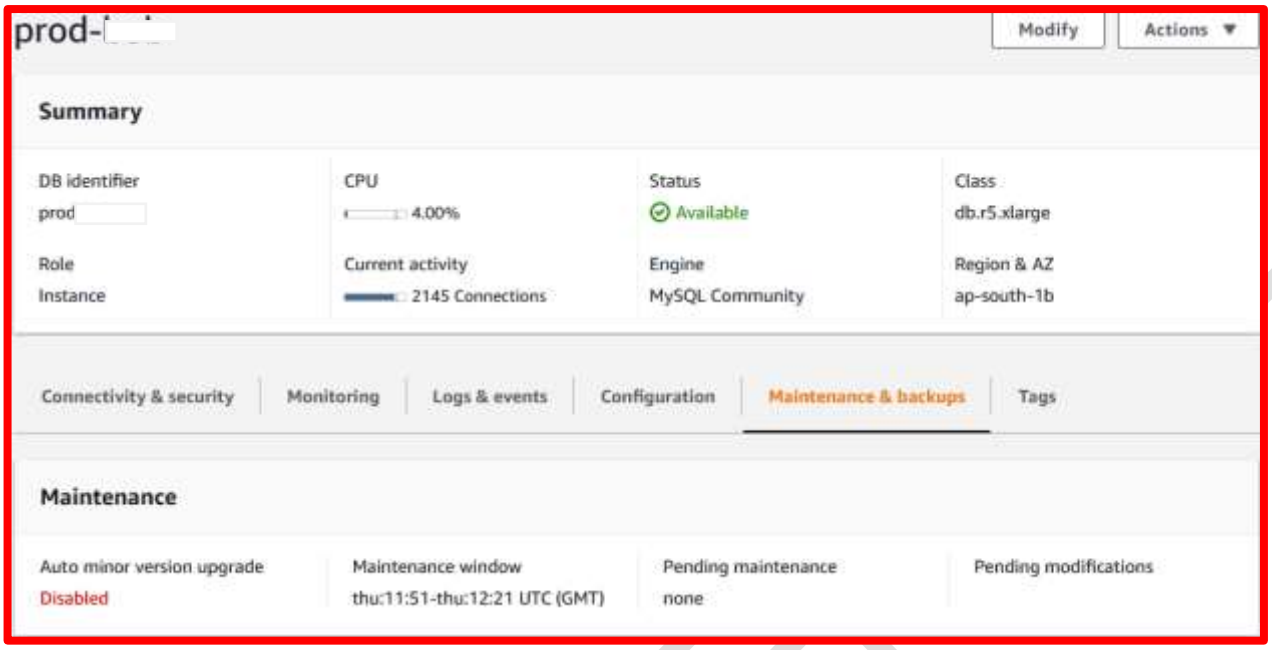


3.6 Ensure Relational Database Service Instances have Auto Minor Version Upgrade Enabled

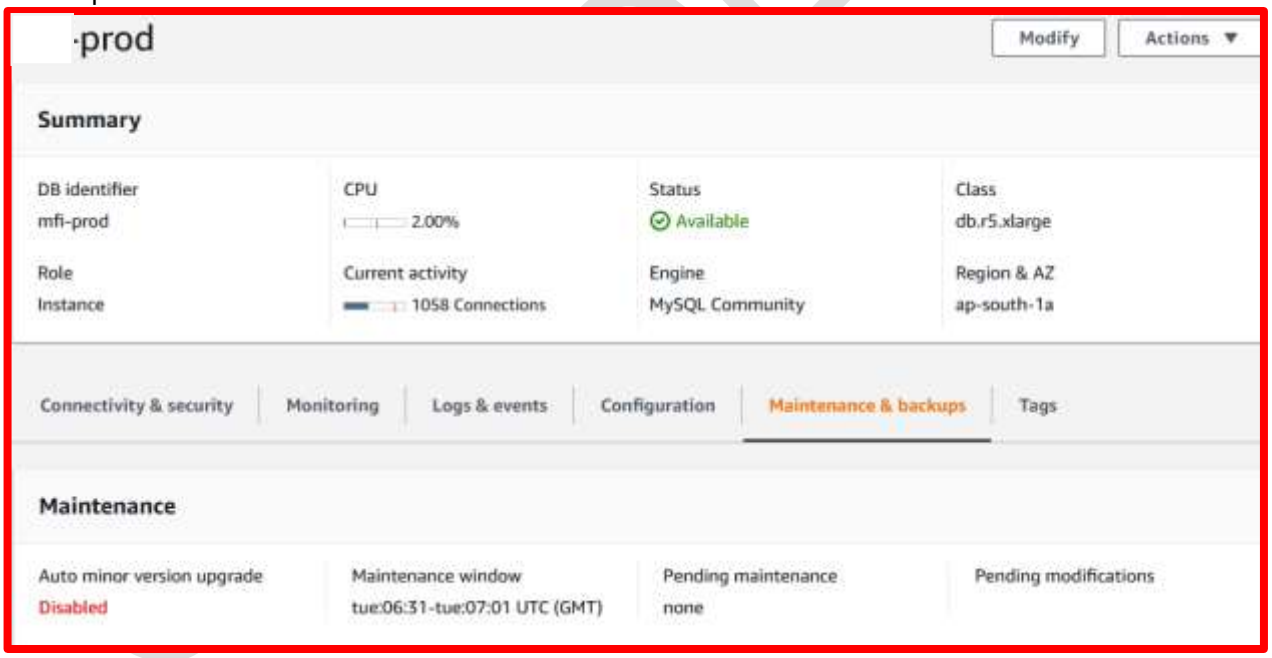
prod-xyz-v2



prod-yyz

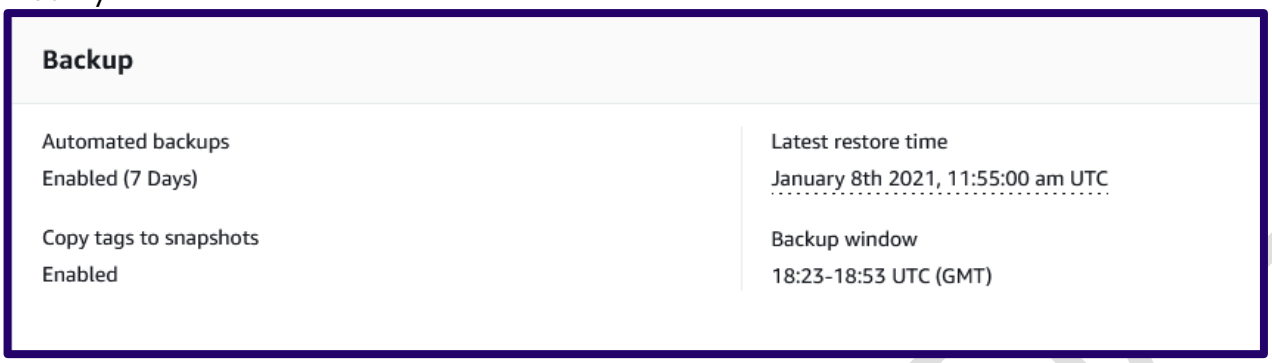


ABCD-prod

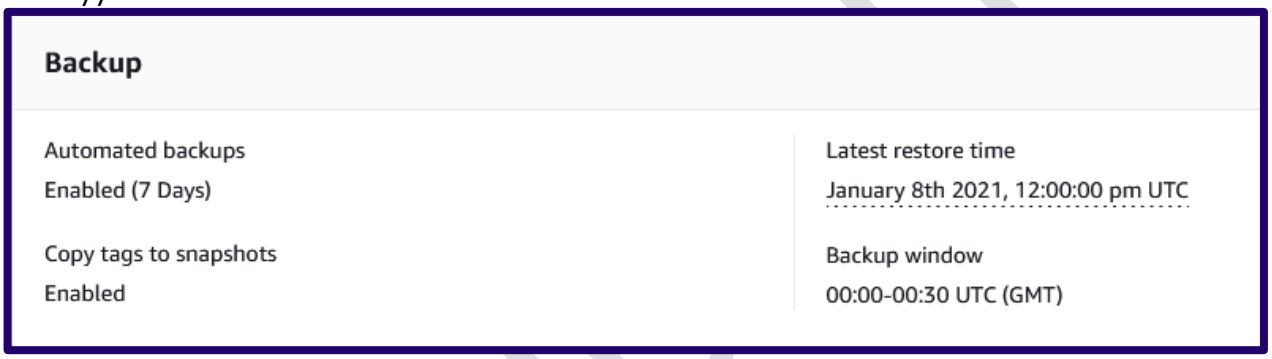


3.8 Ensure Relational Database Service backup retention policy is set

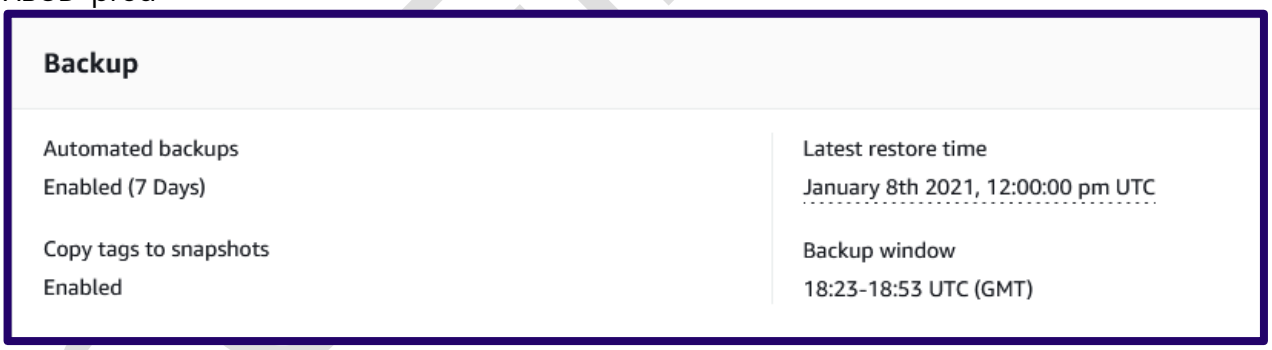
Prod-xyz-v2



Prod-yyz

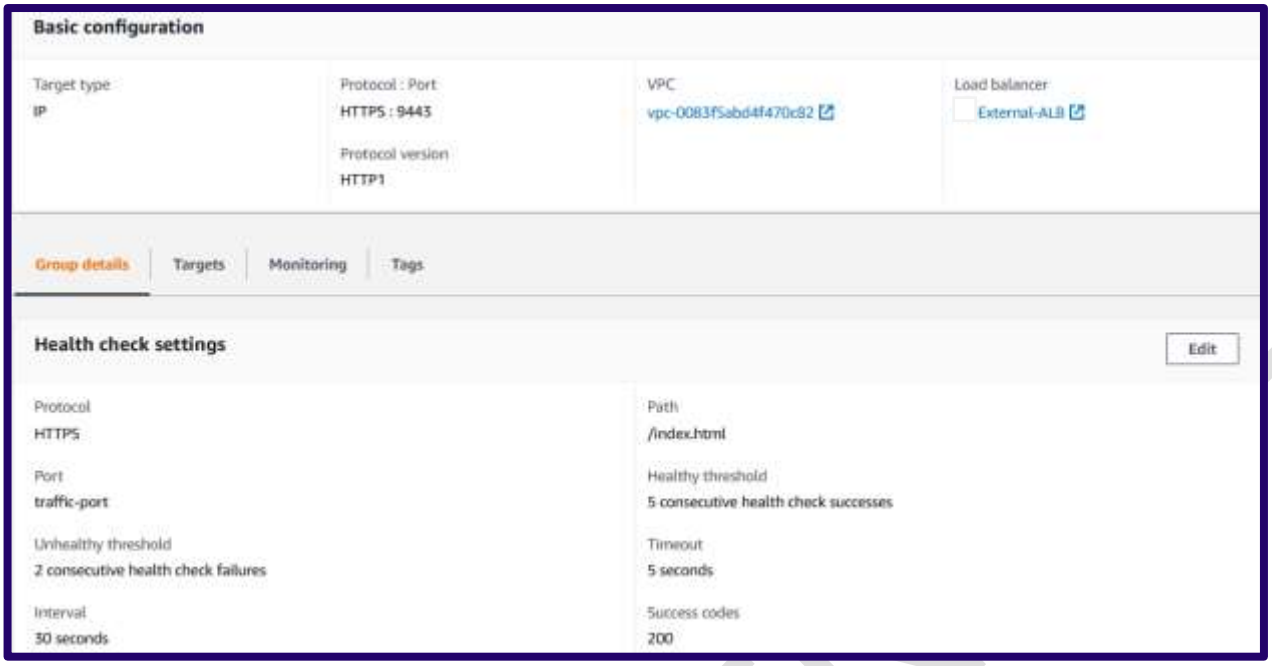


ABCD-prod

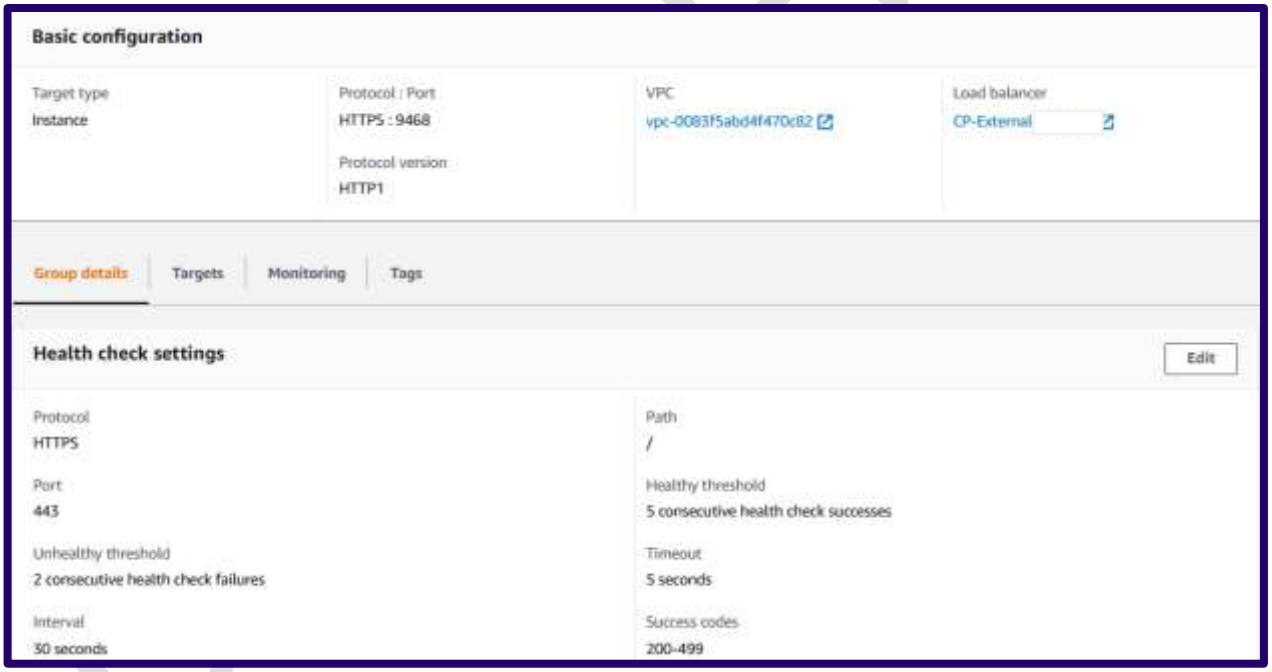


3.9 Ensure Web Tier Elastic Load Balancer has application layer Health Check Configured / 3.10 Ensure APP-Tier Elastic Load Balancer has application layer Health Check Configured

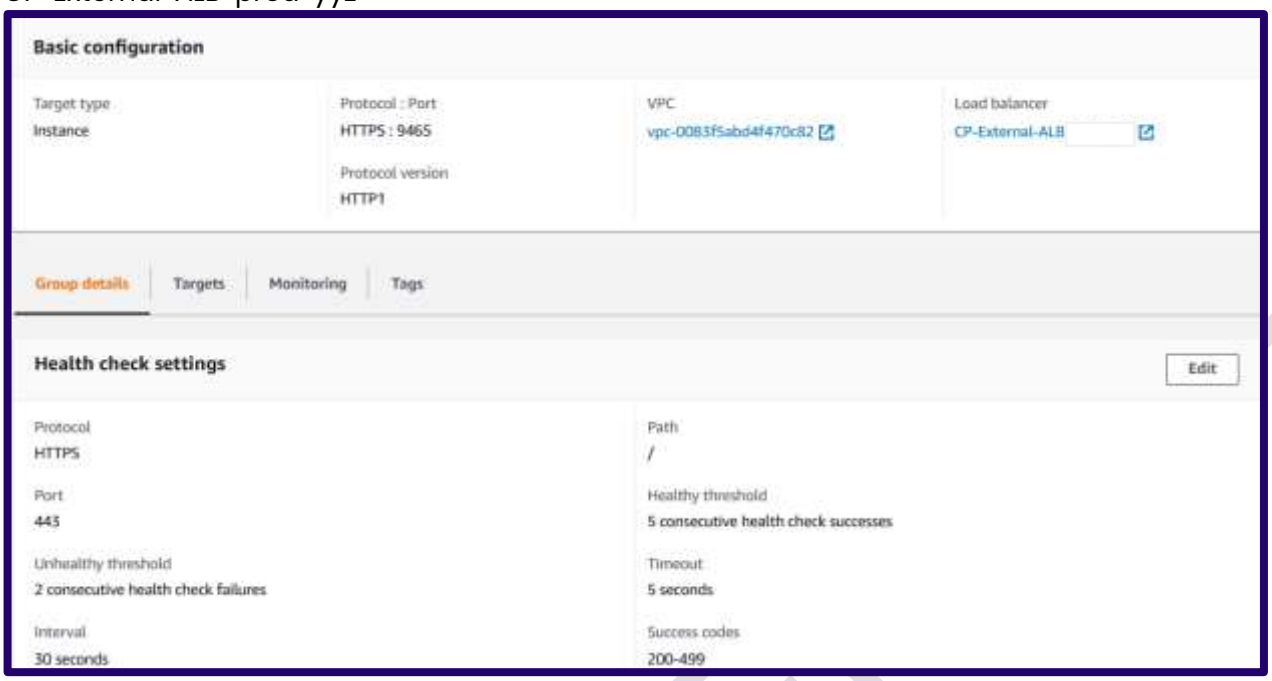
CP-External-ALB



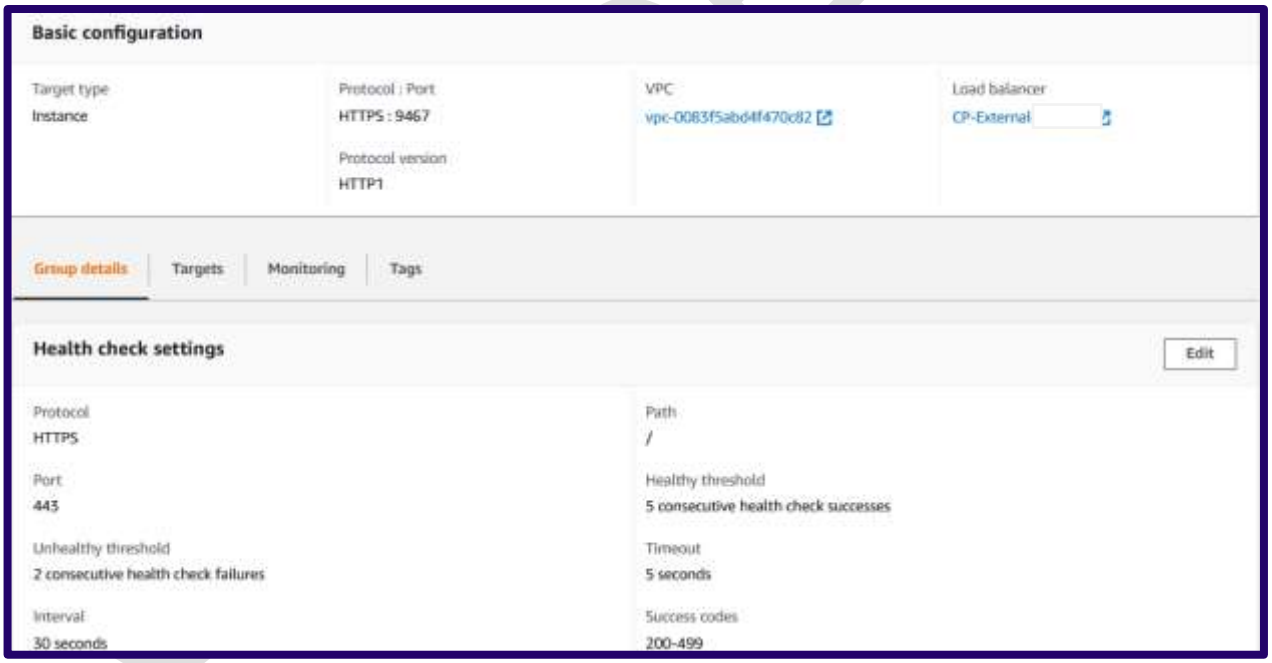
CP-External-ALB-ABC



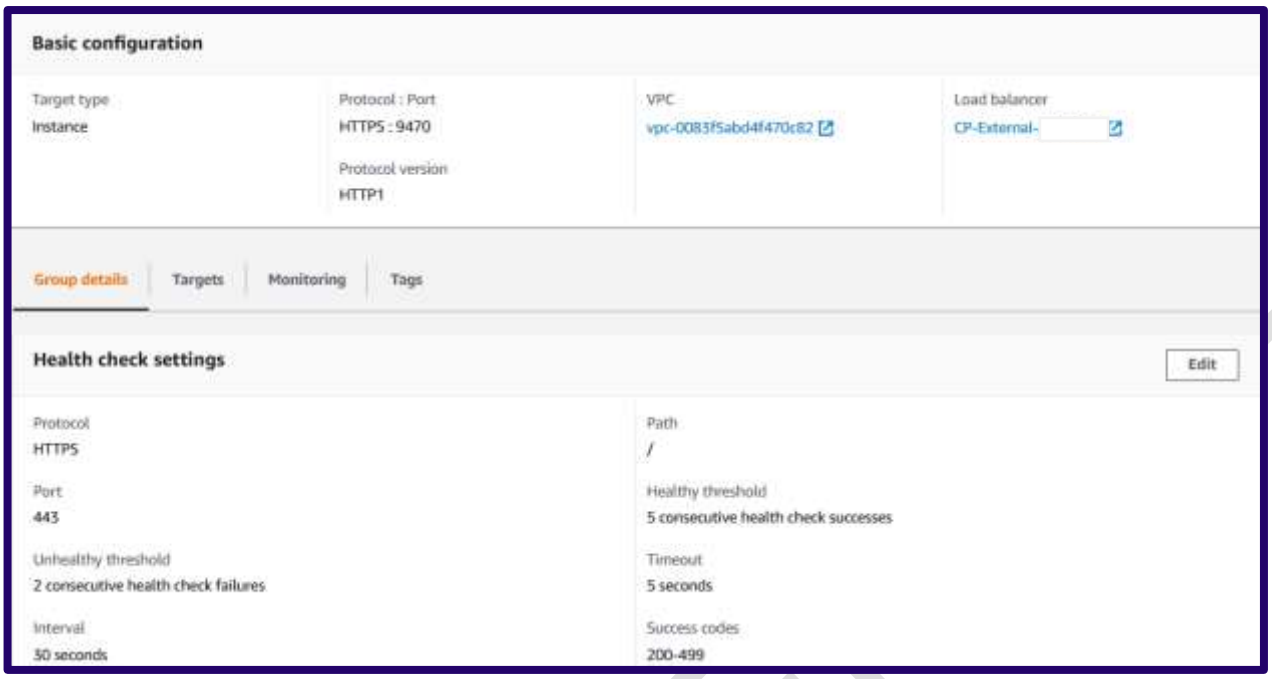
CP-External-ALB-prod-yyz



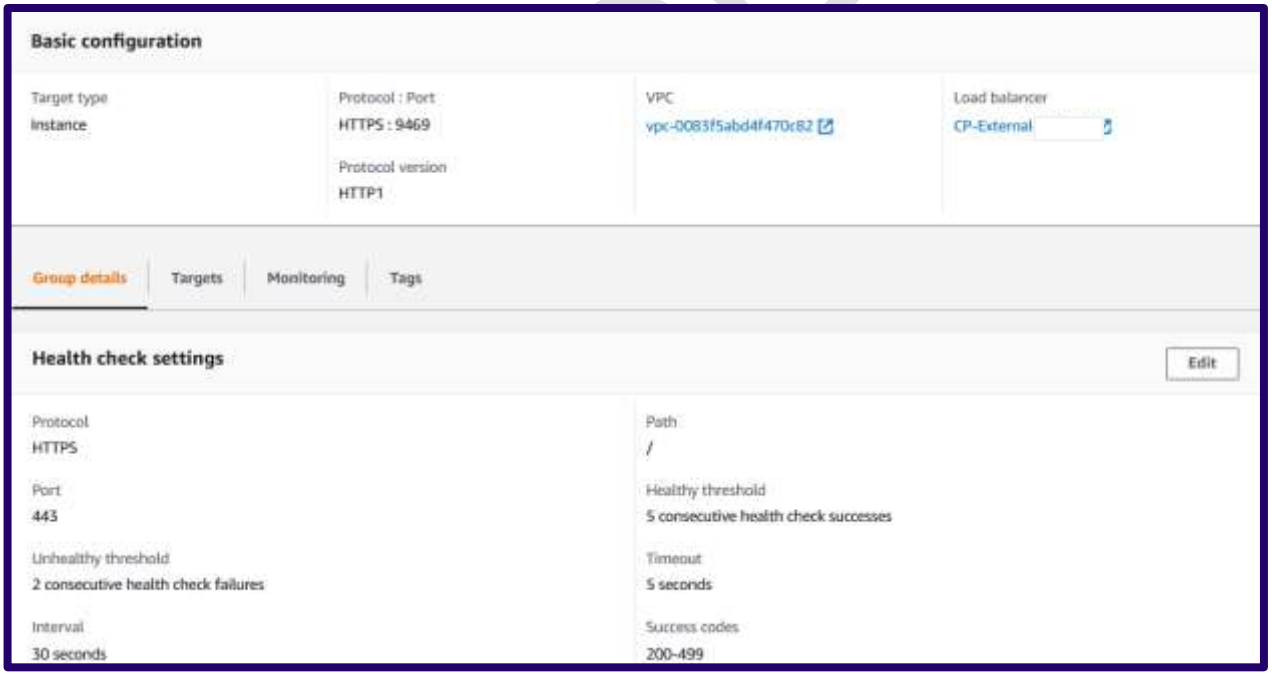
CP-External-ALB-CBI



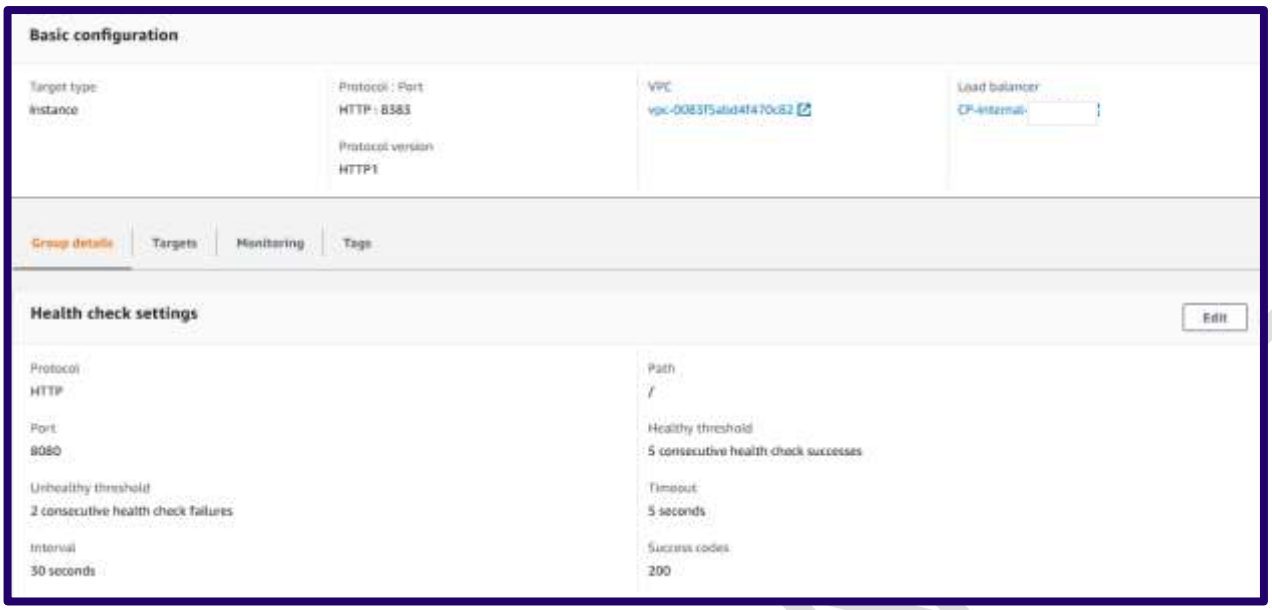
CP-External-ALB-Prod



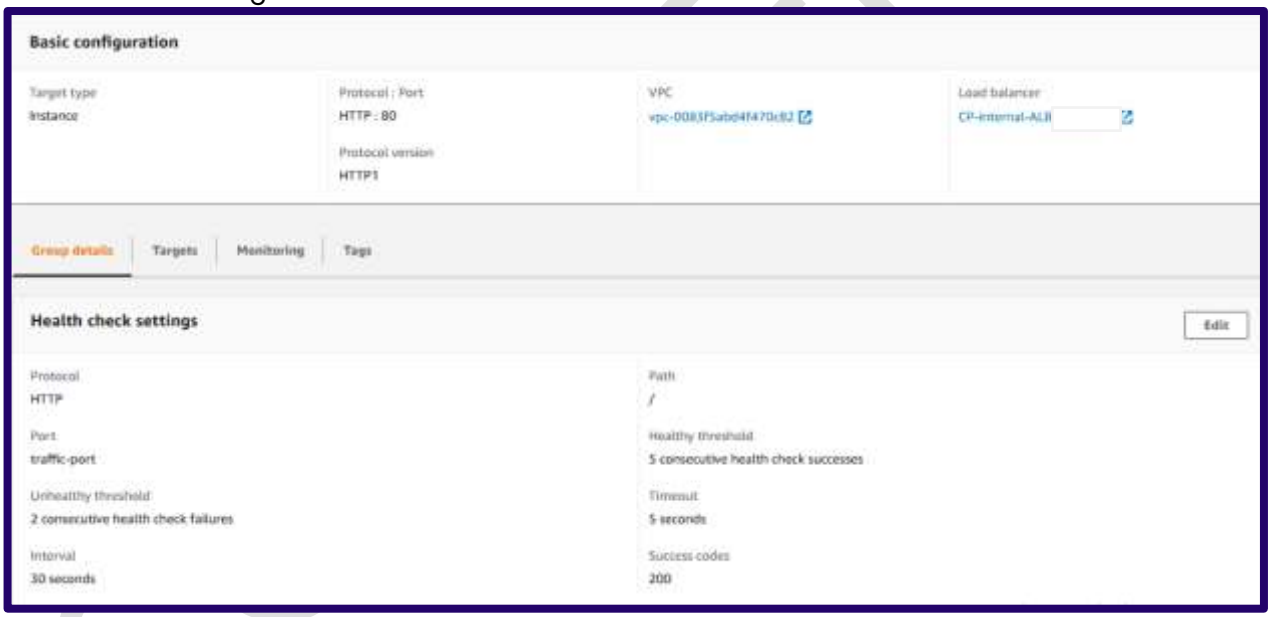
CP-External-ALB-XXY



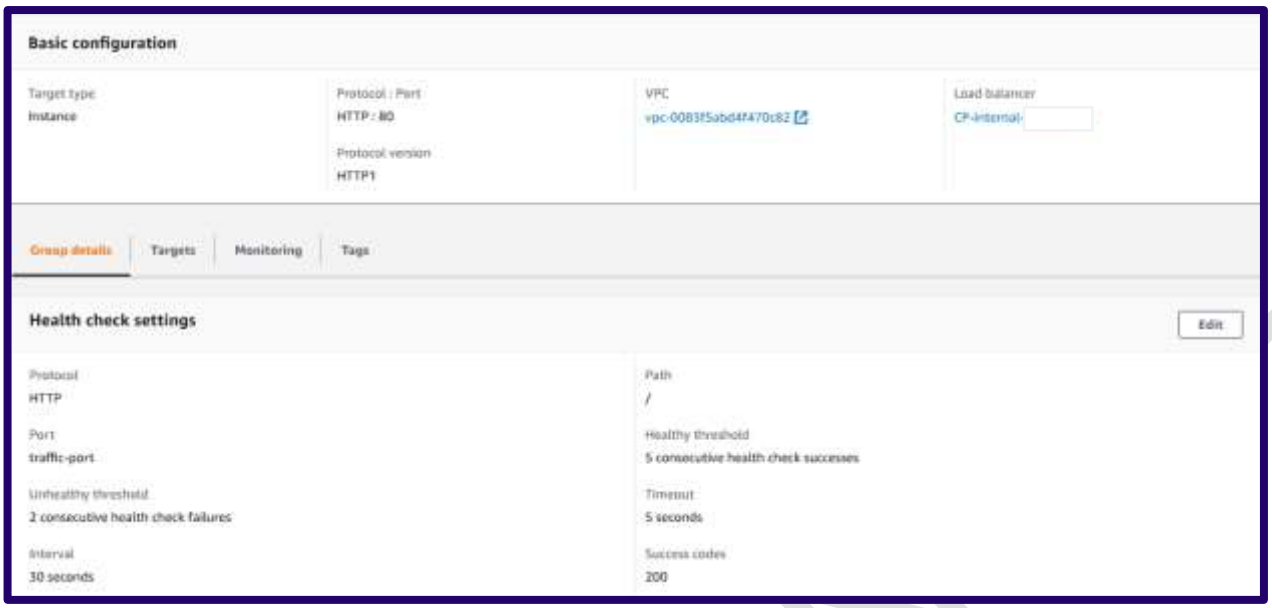
CP-internal-ALB-YYZ



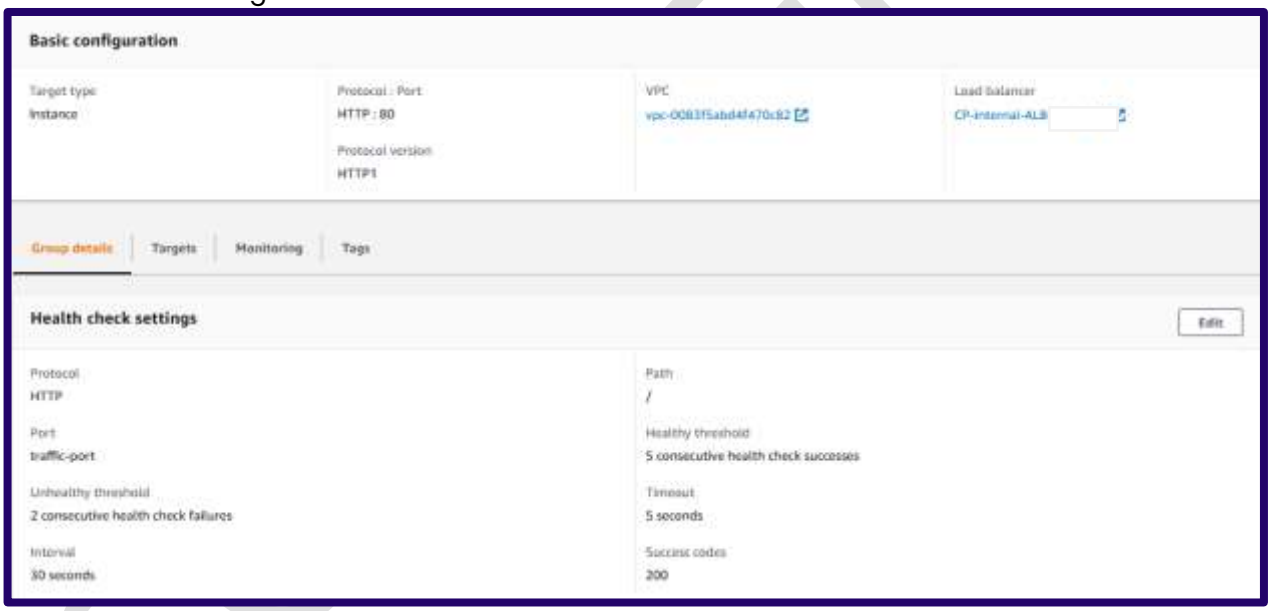
CP-internal-ALB-nginx-ABC



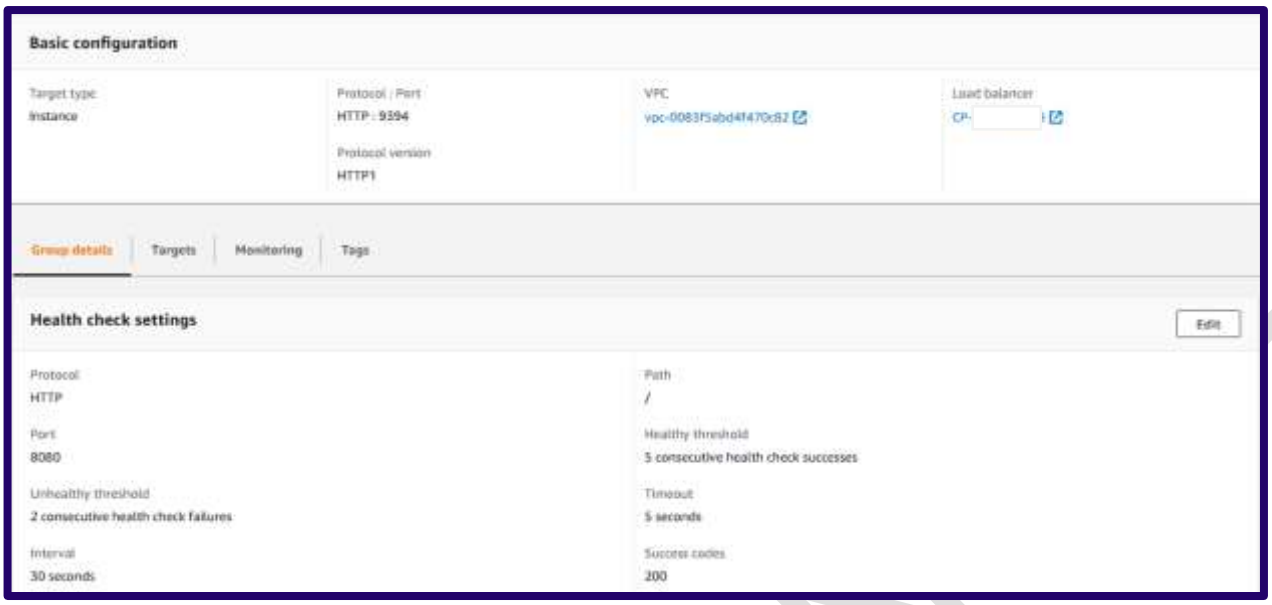
CP-internal-ALB-CI



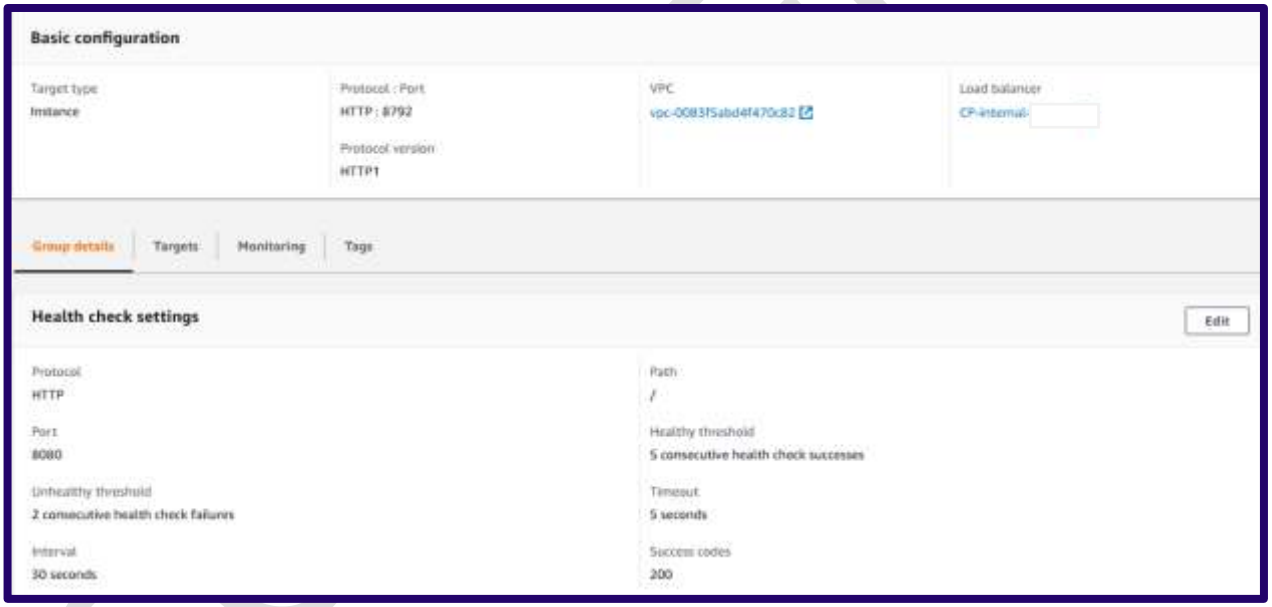
CP-internal-ALB-nginx-XXY



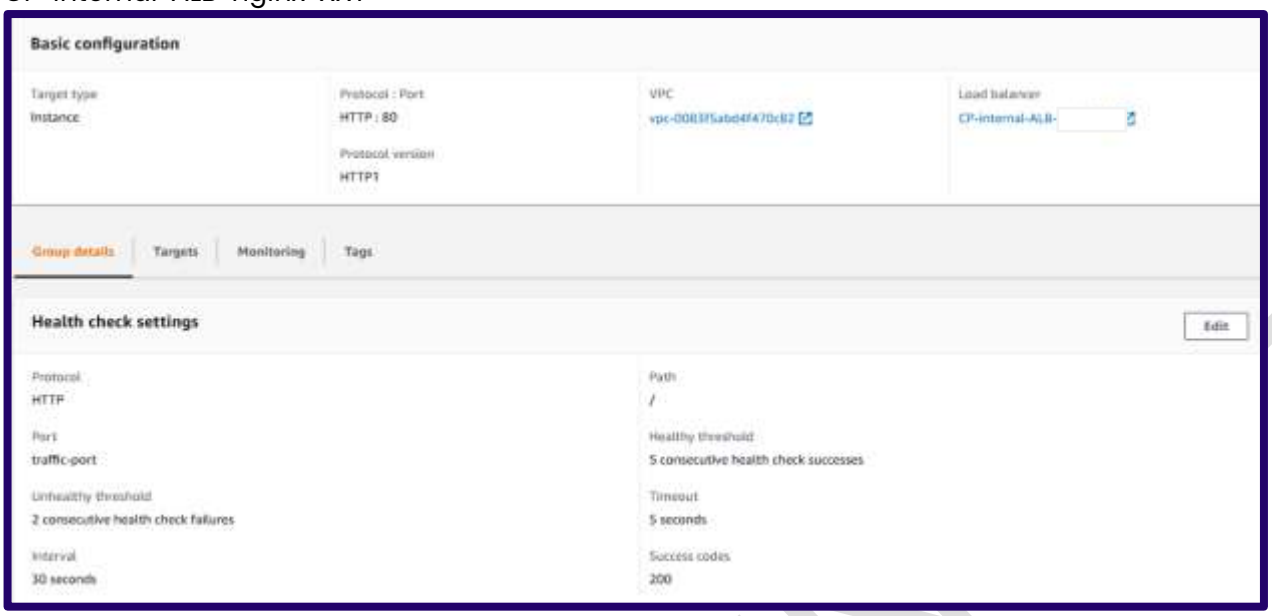
CP-internal-ELB



CP-internal-ALB-XXY



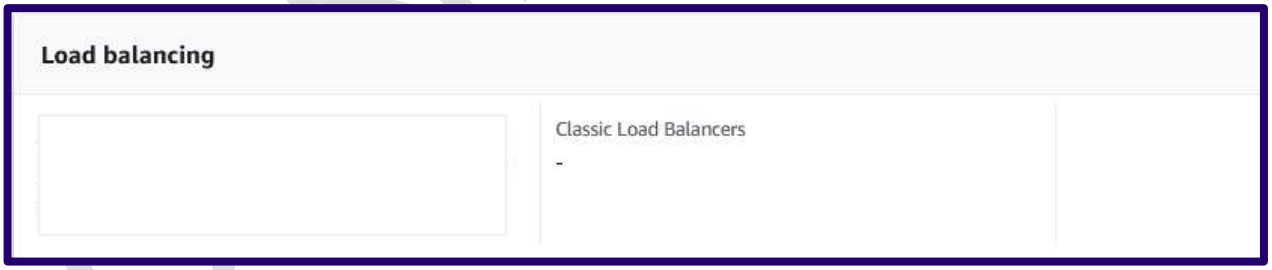
CP-internal-ALB-nginx-XXY



3.11 Ensure S3 Buckets have versioning enabled.

Note: Need to be configured.

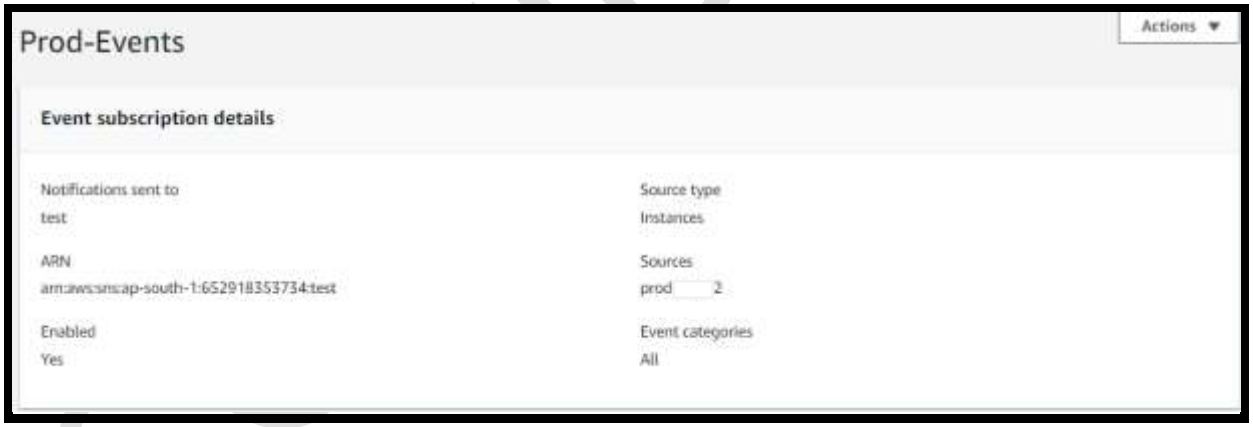
3.12 Configure HTTP to HTTPS redirects with a cloudfront viewer protocol policy: Not Applicable
3.13 Ensure all cloudfront distributions require HTTPS between cloudfront and your web-tier origin: Not Applicable
3.14 Ensure web-tier auto scaling gateway has an associated Elastic load balancer / 3.15 Ensure App-tier auto scaling gateway has an associated Elastic load balancer



4 Event Monitoring and Response

4.1 Ensure a SNS topic is created for sending out notifications from Cloudwatch Alarms and Auto scaling Groups

4.2 Ensure a SNS topic is created for sending out notification from RDS Events /4.3 Ensure RDS events subscription are enabled for instance level events

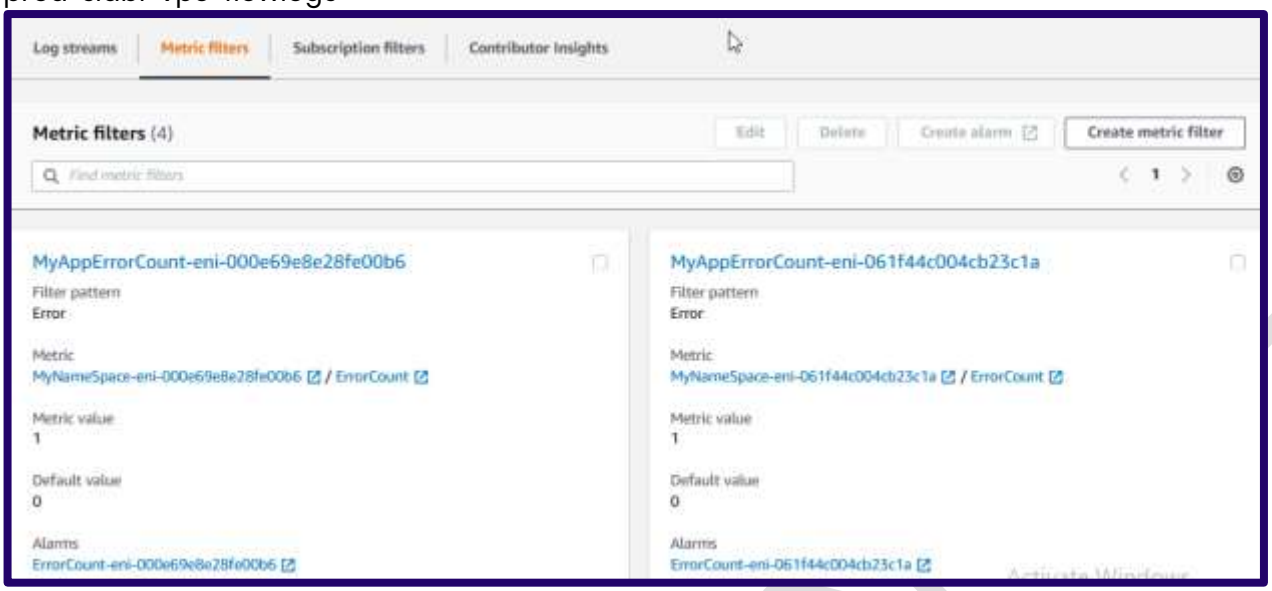


4.4 Ensure RDS events subscription are enabled for DB security groups

Note: Need to be configured.

4.6 Ensure that a log metric filter for the Cloudwatch group assigned to the "VPC Flow Logs" is created /
4.7 Ensure that a CloudtWatch Alarm is created for the "VPC Flow Logs" metric filter, and an Alarm Action is configured

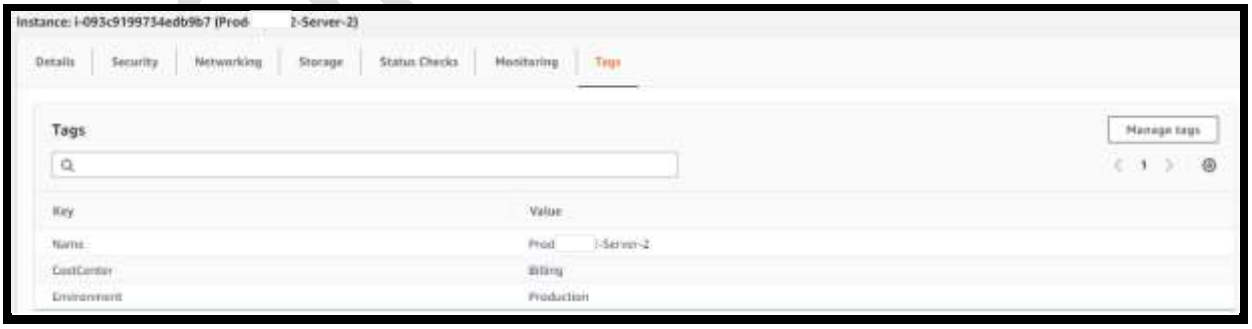
prod-sidbi-vpc-flowlogs

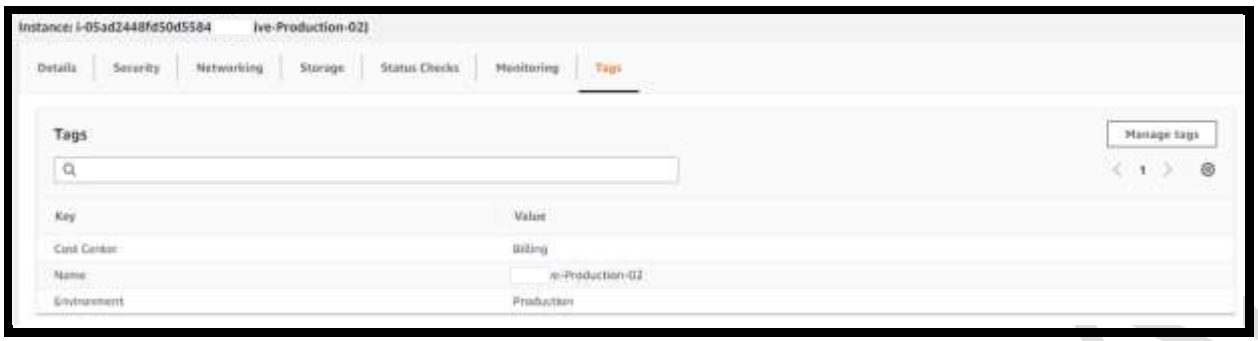


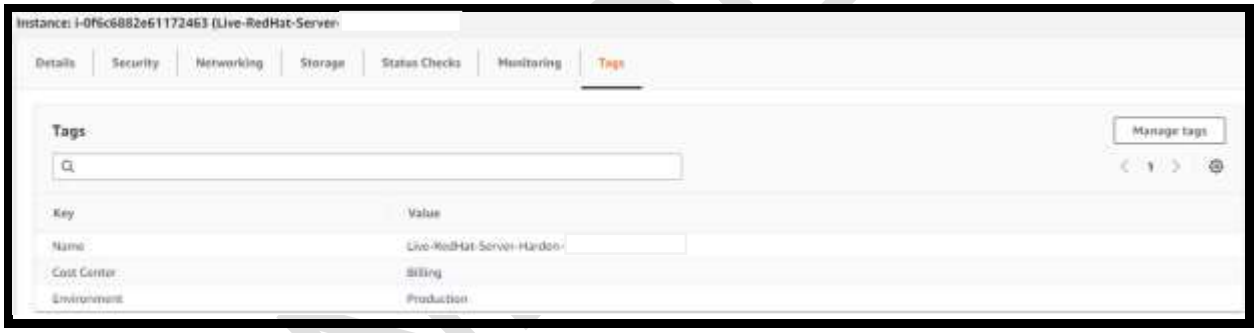
4.8 Ensure Billing Alerts are enabled for increments of X spend: Not Applicable

5 Audit and Logging

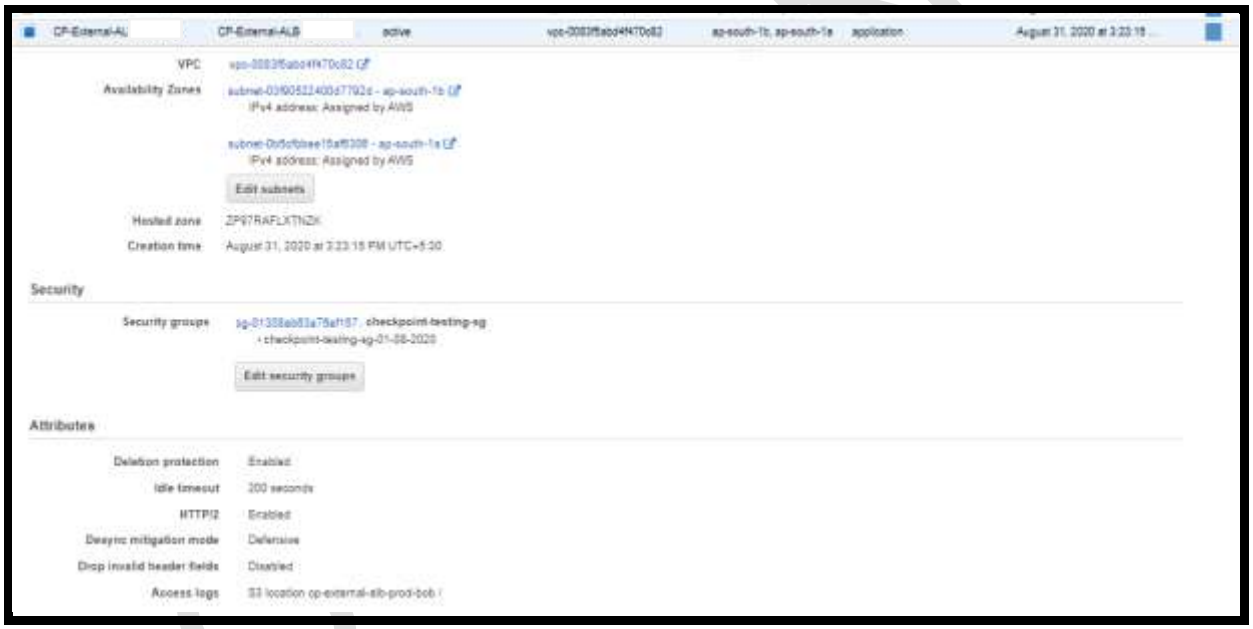
5.1 Ensure all resources are correctly tagged



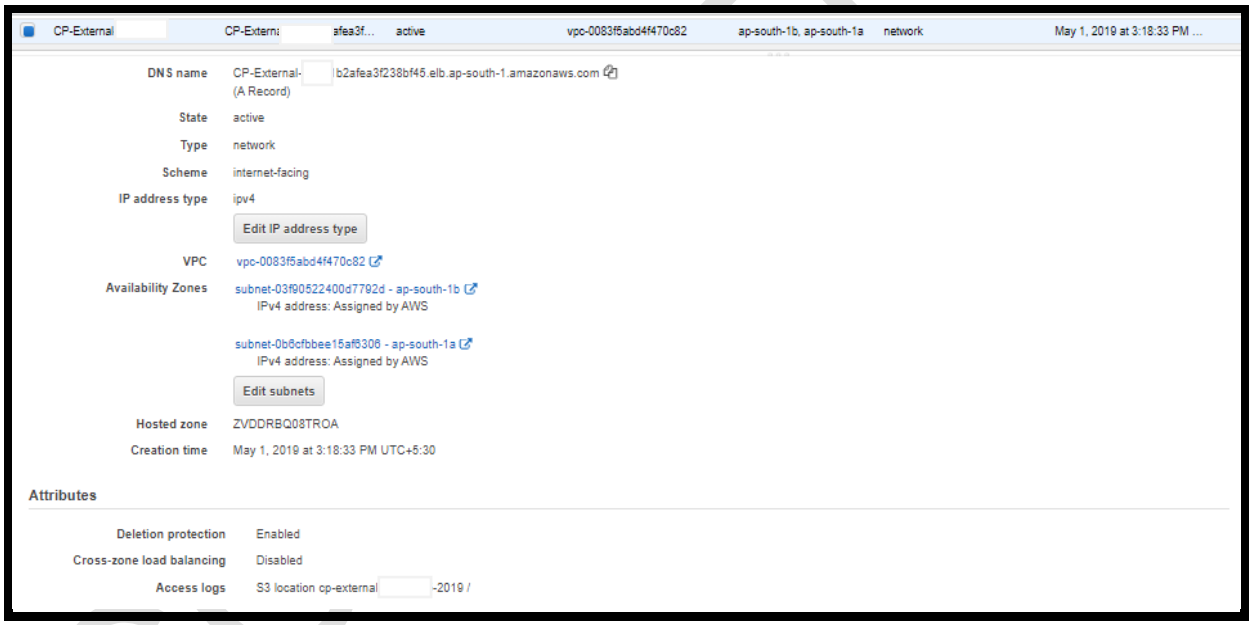




5.2 Ensure AWS Elastic Load Balancer logging is enabled

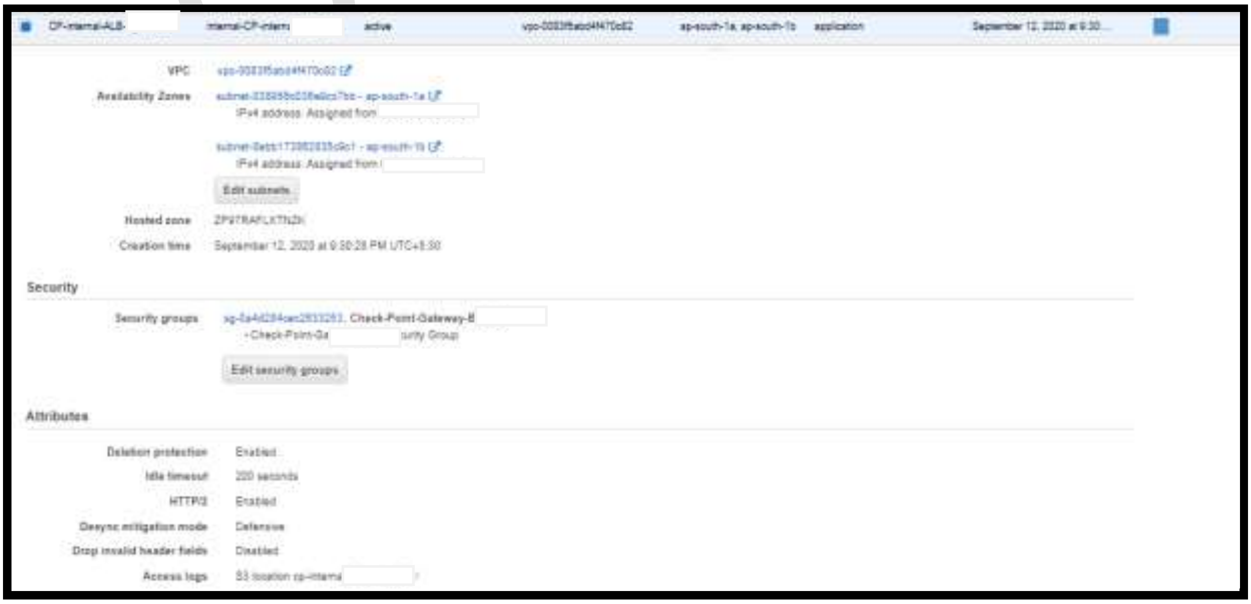



CP-External
active
application
September 12, 2020 at 10:1...
VPC
Availability Zones
IPv4 address: Assigned by AWS
IPv4 address: Assigned by AWS
Edit subnets
Hosted zone
Creation time
Security
Security groups
checkpoint-testing-sg
Edit security groups
Attributes
Deletion protection
Enabled
Idle timeout
Enabled
Desync mitigation mode
Defensive
Drop invalid header fields
Disabled
Access logs

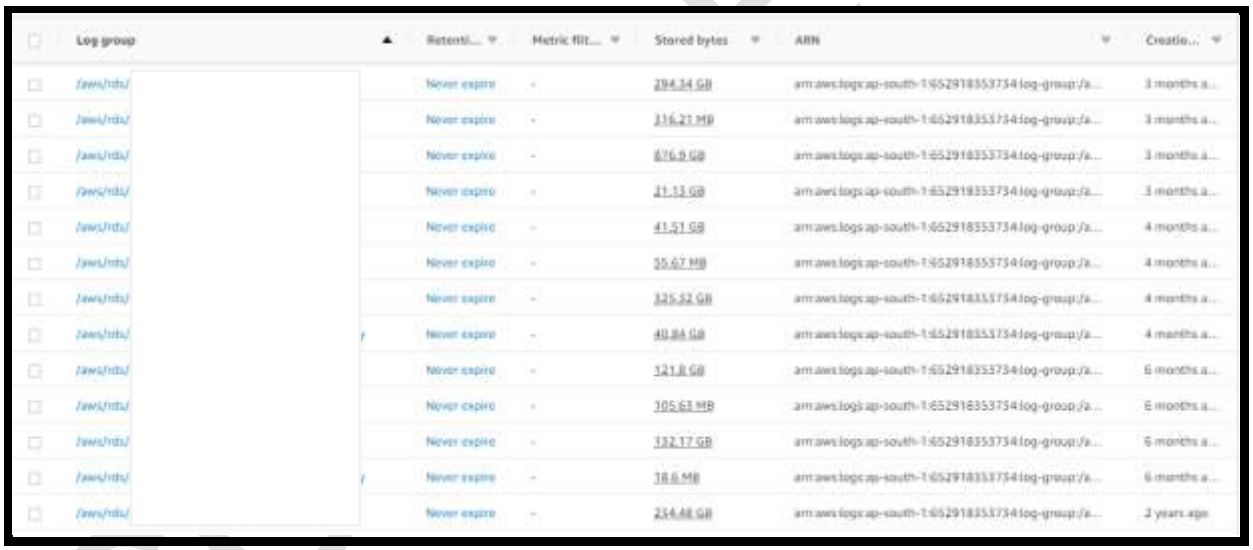

CP-External
active
vpc-0083f5abd4f470c82
ap-south-1b, ap-south-1a
network
May 1, 2019 at 3:18:33 PM ...
DNS name
CP-External-
(A Record)
b2afea3f238bf45.elb.ap-south-1.amazonaws.com
State
active
Type
network
Scheme
internet-facing
IP address type
ipv4
Edit IP address type
VPC
vpc-0083f5abd4f470c82
Availability Zones
subnet-03f90522400d7792d - ap-south-1b
IPv4 address: Assigned by AWS
subnet-0b6cfbbee15af6306 - ap-south-1a
IPv4 address: Assigned by AWS
Edit subnets
Hosted zone
ZVDDRBQ08TROA
Creation time
May 1, 2019 at 3:18:33 PM UTC+5:30
Attributes
Deletion protection
Enabled
Cross-zone load balancing
Disabled
Access logs
S3 location cp-external
-2019 /


active
application
VPC
Availability Zones
Edit subnets
Hosted zone
ZP97RAFLXTNZK
Creation time
September 3, 2020 at 7:55:11 PM UTC+5:30
Security
Security groups
Edit security groups
Attributes
Deletion protection
Enabled
Idle timeout
200 seconds
HTTP/2
Enabled
Desync mitigation mode
Defensive
Drop invalid header fields
Disabled
Access logs

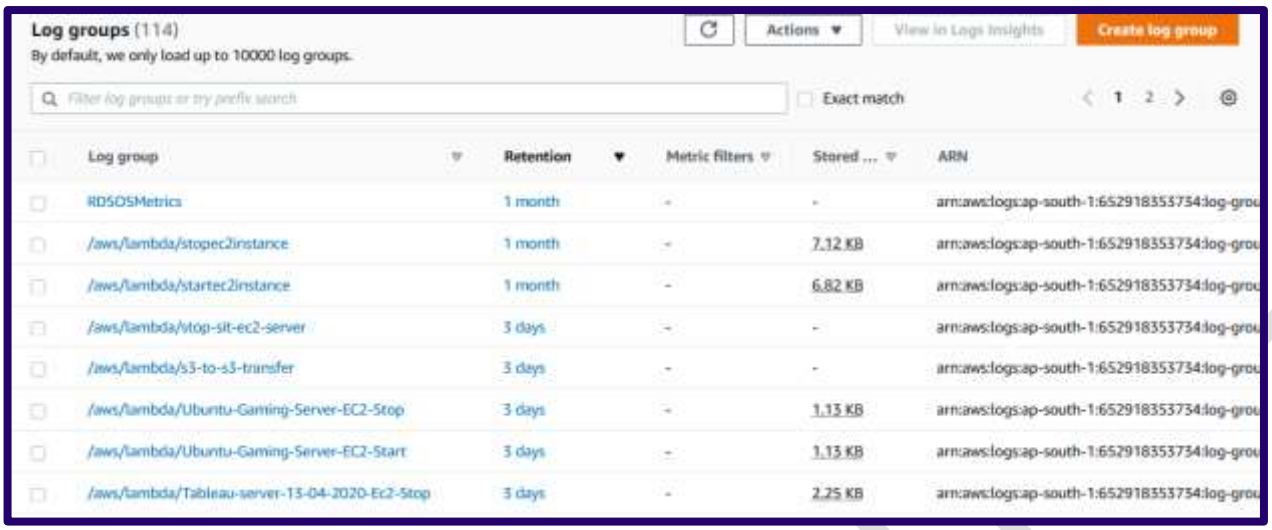

active
application
VPC
Availability Zones
Edit subnets
Hosted zone
ZP97RAFLXTNZK
Creation time
Security
Security groups
Edit security groups
Attributes
Deletion protection
Enabled
Idle timeout
200 seconds
HTTP/2
Enabled
Desync mitigation mode
Defensive
Drop invalid header fields
Disabled
Access logs


active
application
VPC
Availability Zones
Edit subnets
Hosted zone
ZP97RAFLXTNZK
Creation time
Security
Security groups
Edit security groups
Attributes
Deletion protection
Enabled
Idle timeout
200 seconds
HTTP/2
Enabled
Desync mitigation mode
Defensive
Drop invalid header fields
Disabled
Access logs

5.3 Ensure AWS Cloudfront Logging is enabled: Not Applicable
5.4 Ensure Cloudwatch Log Group is created for Web Tier / 5.5 Ensure Cloudwatch Log Group is created for App Tier

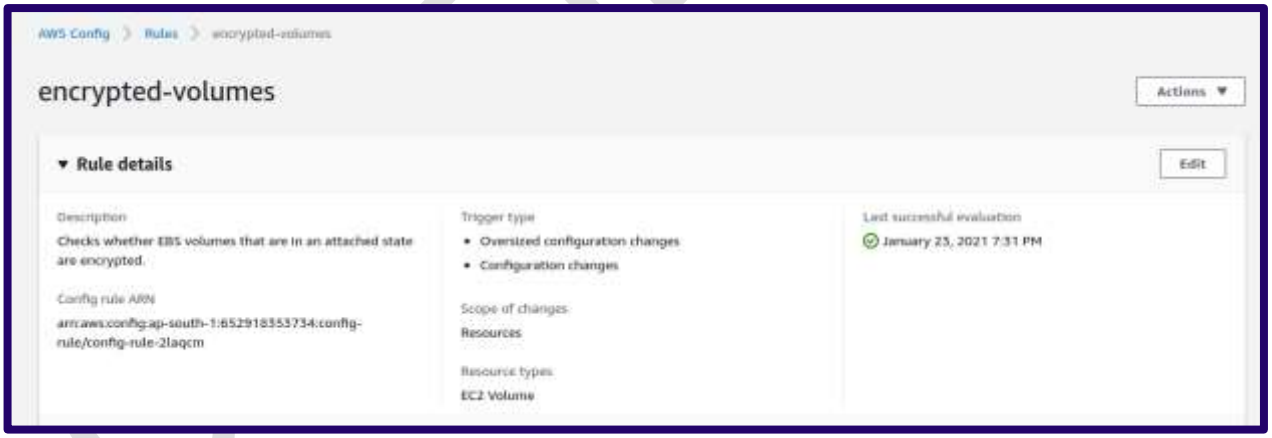


5.6 Ensure Cloudwatch Log Group for Web Tier has a retention period / 5.7 Ensure Cloudwatch Log Group for App Tier has a retention period

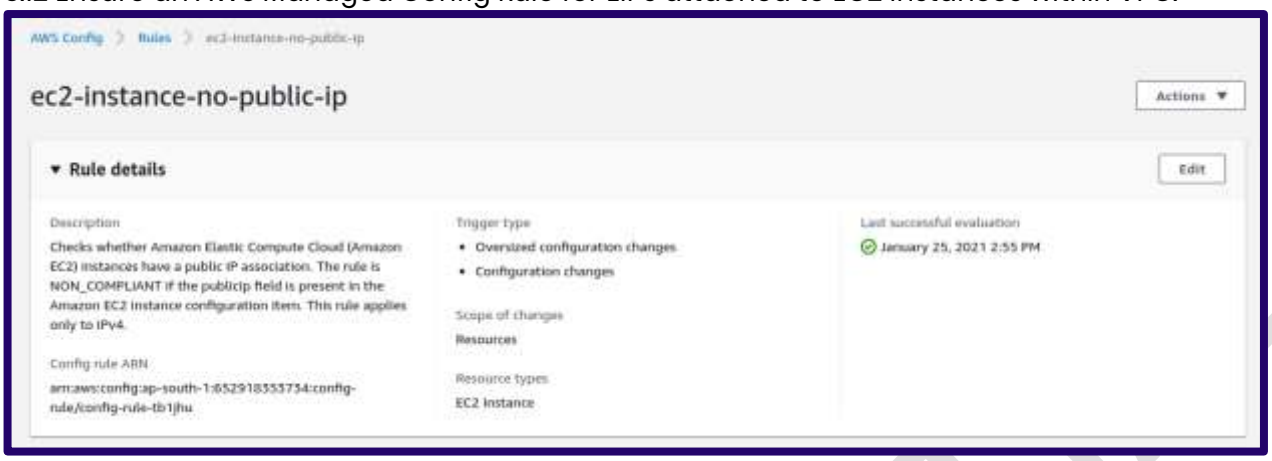


5.8 Ensure an agent for AWS Cloudwatch Logs is installed within AutoScaling Group for Web-Tier: Not Applicable
5.9 Ensure an agent for AWS Cloudwatch Logs is installed within AutoScaling Group for App-Tier: Not Applicable

5.10 Ensure an AWS Managed Config Rule for encrypted volumes is applied to Web Tier / 5.11 Ensure an AWS Managed Config Rule for encrypted volumes is applied to App Tier.



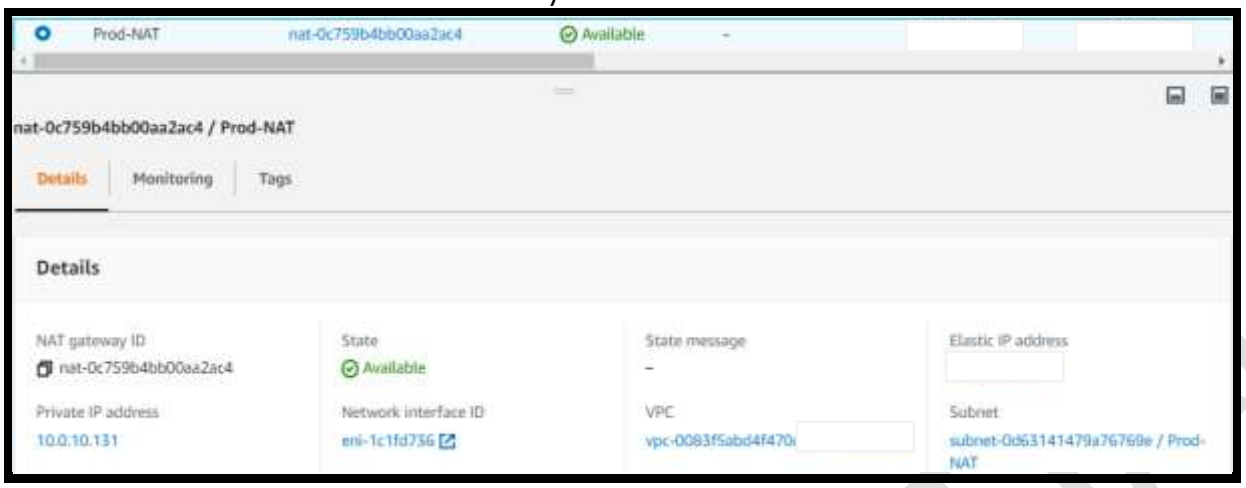
5.12 Ensure an AWS Managed Config Rule for EIPs attached to EC2 instances within VPC.



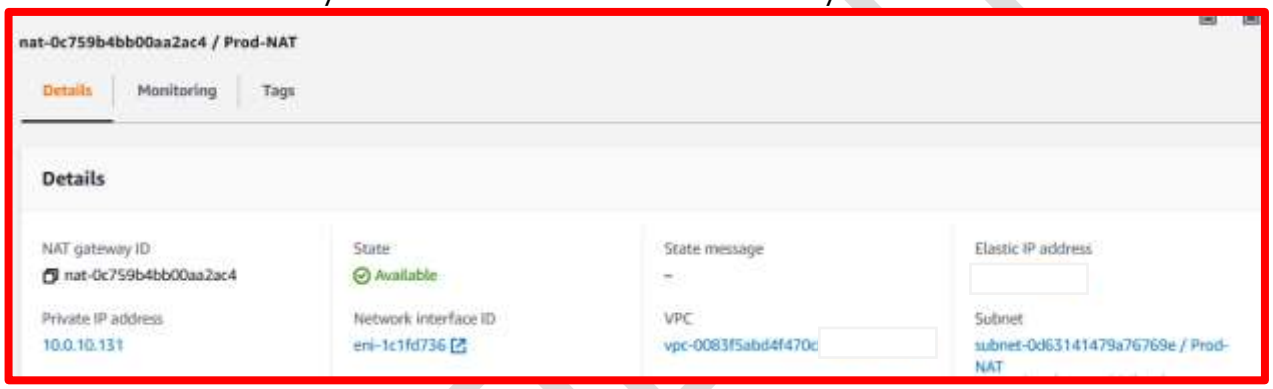
6 Networking

6.1 Ensure Root Domain Alias Record Points to ELB: Not Applicable (pointed to Imperva alias)
6.2 Ensure a DNS alias record for the root domain: Not Applicable
6.3 Use CloudFront Content Distribution Network: Not Applicable
6.4 Ensure Geo-Restriction is enabled within Cloudfront Distribution: Not Applicable
6.5 Ensure subnets for the Web tier ELB are created / 6.6 Ensure subnets for the Web tier are created / 6.7 Ensure subnets for the App tier are created / 6.8 Ensure subnets for the Data tier are created:

6.9 Ensure Elastic IPs for the NAT Gateways are allocated



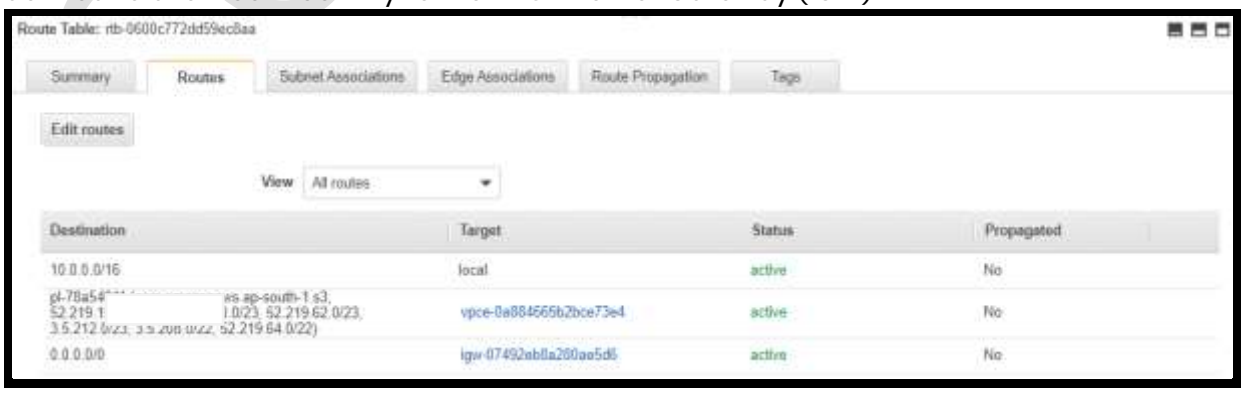
6.10 Ensure NAT Gateways are created in at least 2 Availability Zones



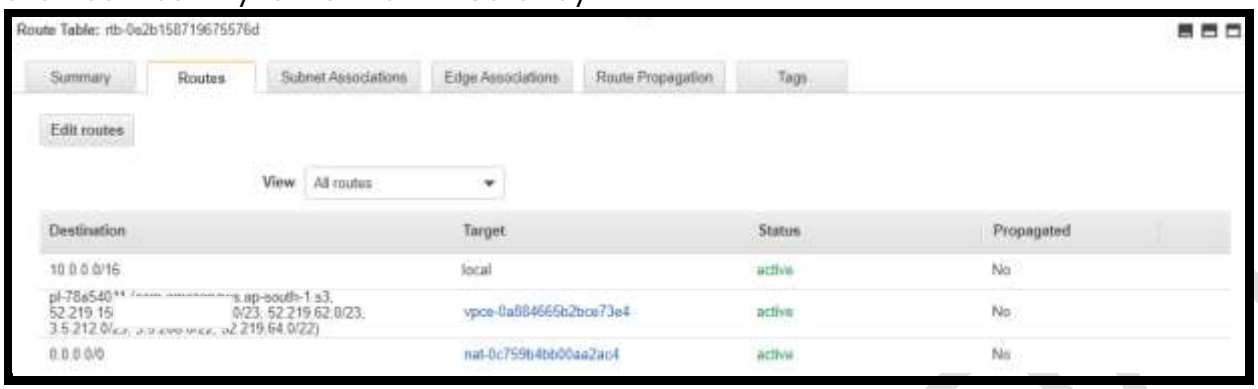
6.11 Ensure a route table for the public subnets is created

6.12 Ensure a route table for the private subnets is created:

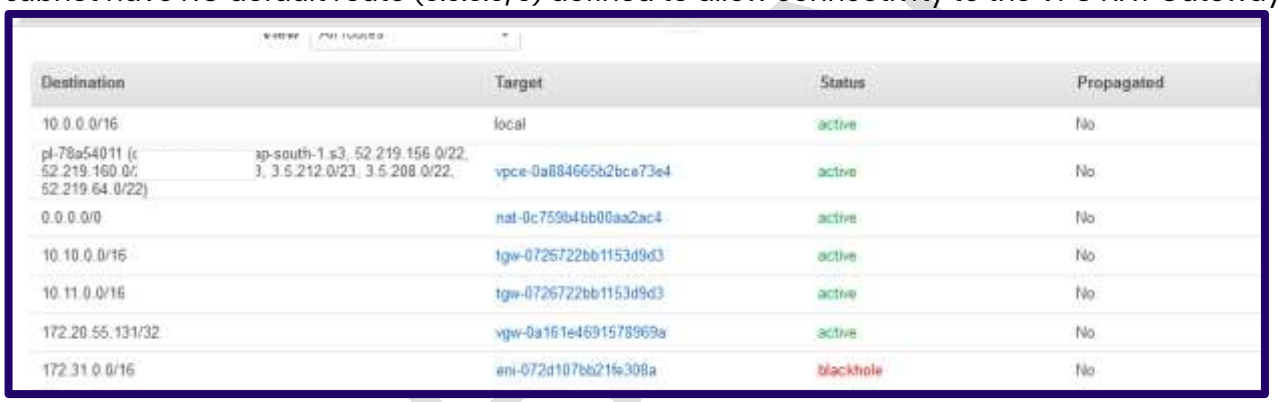
6.13 Ensure Routing Table associated with Web tier ELB subnet have the default route (0.0.0.0/0) defined to allow connectivity to the VPC Internet Gateway (IGW)



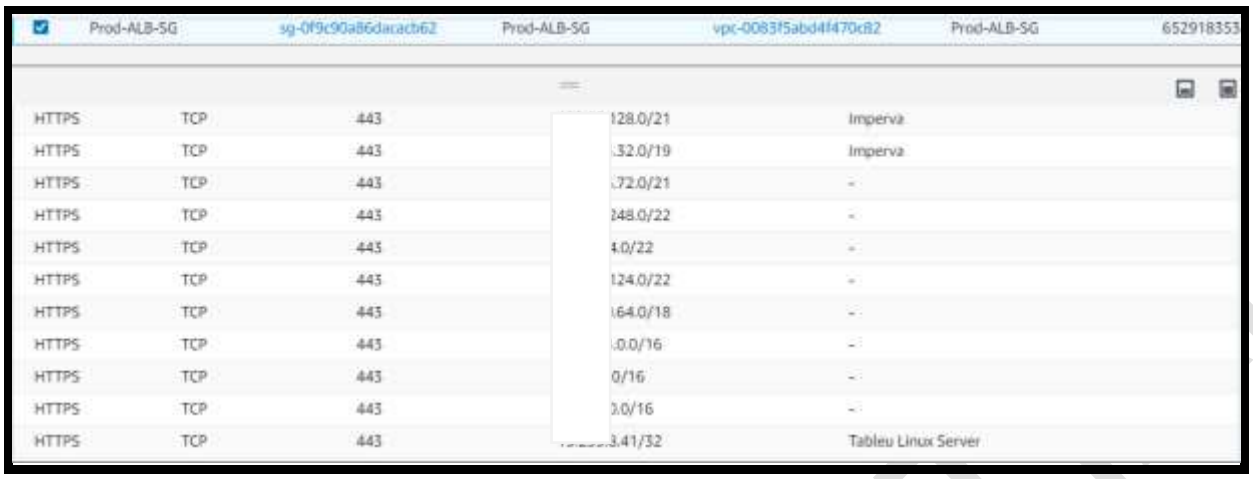
6.14 Ensure Routing Table associated with Web tier subnet have the default route (0.0.0.0/0) defined to allow connectivity to the VPC NAT Gateway



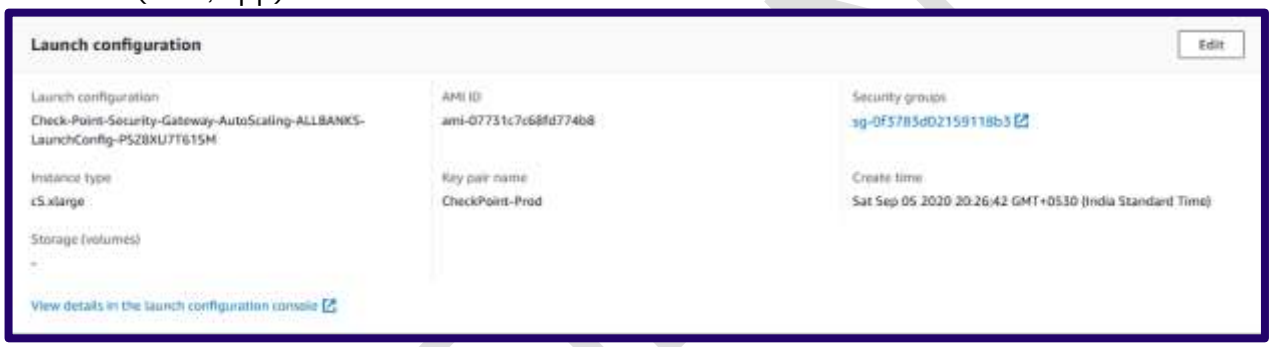
6.15 Ensure Routing Table associated with App tier subnet have the default route (0.0.0.0/0) defined to allow connectivity to the VPC NAT Gateway / 6.16 Ensure Routing Table associated with Data tier subnet have NO default route (0.0.0.0/0) defined to allow connectivity to the VPC NAT Gateway



6.17 Use a Web-Tier ELB Security Group to accept only HTTP/HTTPS



6.18 Ensure Web tier ELB Security Group is not used in the Auto Scaling launch configuration of any other tier (Web, App)



Note – ELB security group is not used in auto scaling launch configuration.

6.19 Create the Web tier Security Group and ensure it allows inbound connections from Web tier ELB Security Group for explicit ports / 6.22 Create the App tier Security Group and ensure it allows inbound connections from App tier ELB Security Group for explicit ports: Not Applicable

6.20 Ensure Web tier Security Group has no inbound rules for CIDR of 0 (Global Allow) / 6.23 Ensure App tier Security Group has no inbound rules for CIDR of 0.

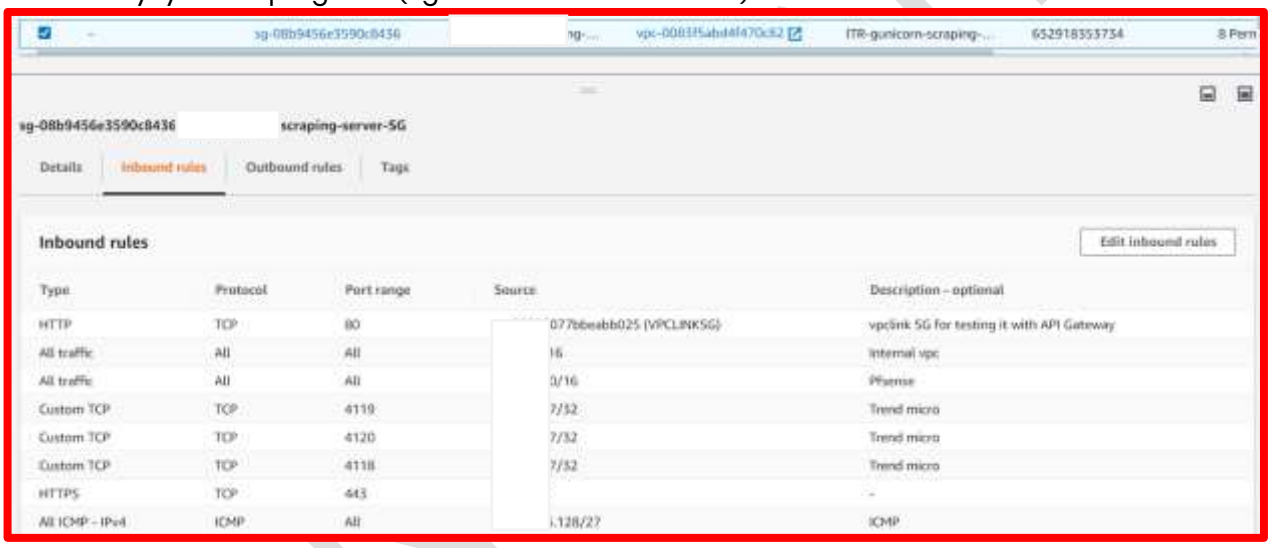
Security Group ID.xlsx

Note: Need to change the inbound rule.

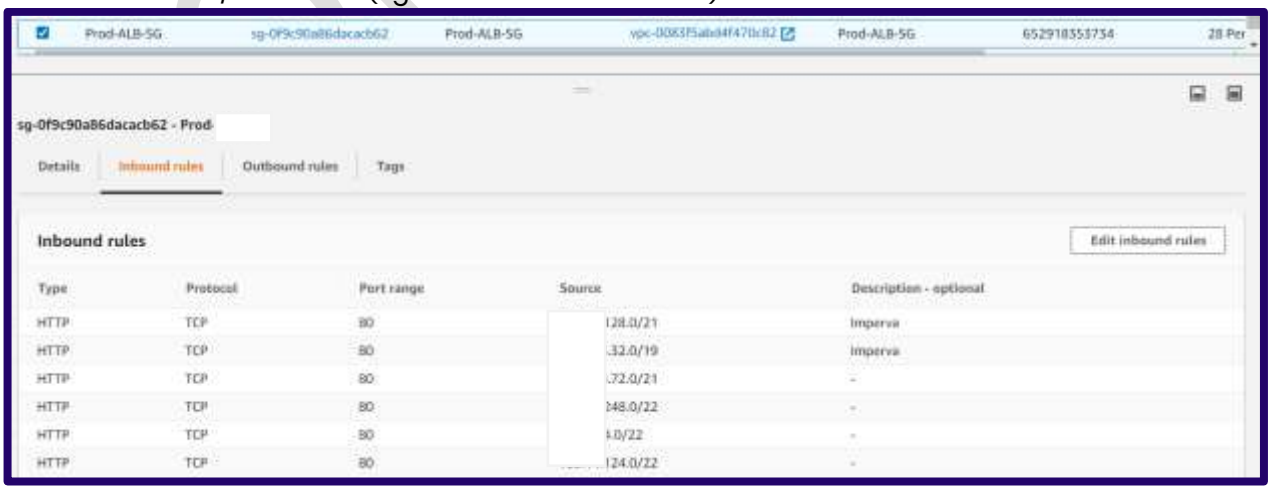
6.21 Create the App tier ELB Security Group and ensure only accepts HTTP/HTTPS

CP-External-ALB (sg-0f6154ad05df248ae)

Live-ITR-Xyxyx-Scraping-ALB (sg-08b9456e3590c8436)



ABCD-Prod-ALB / Prod-ALB (sg-0f9c90a86dacacb62)

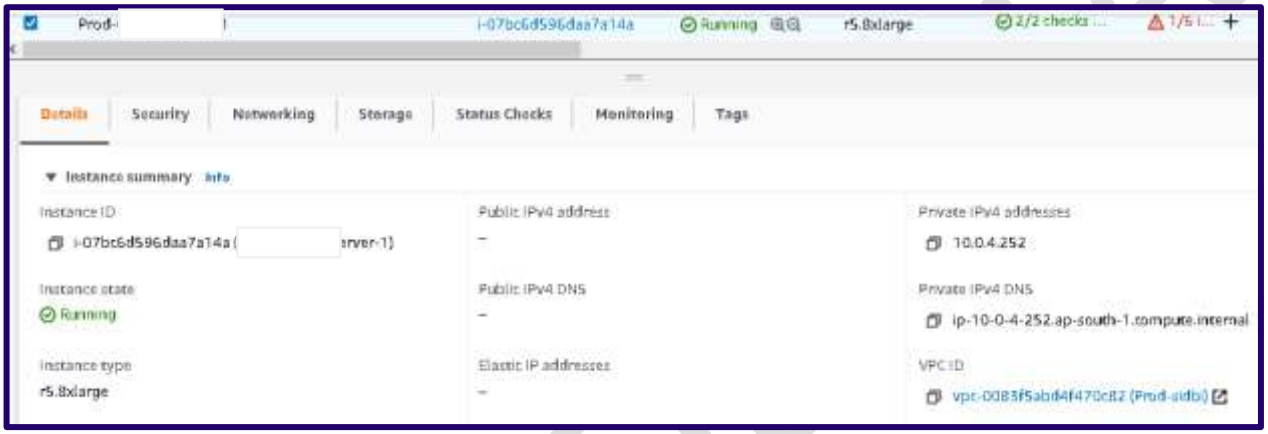


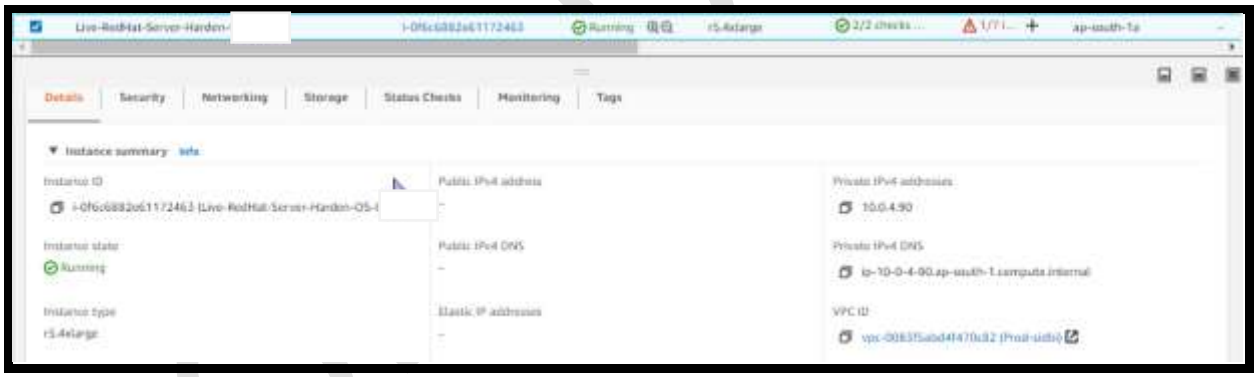
6.24 Create the Data Tier Security Group and ensure it allows inbound connections from App tier Security Group for explicit ports: Not Applicable

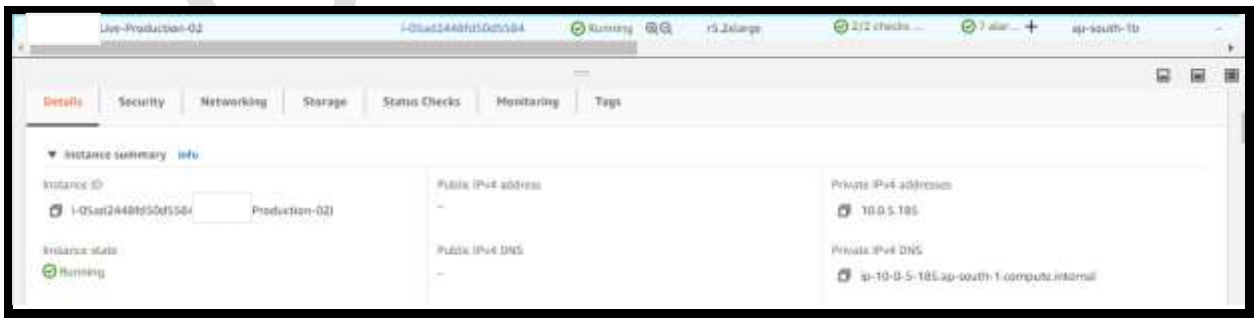
6.25 Ensure Data tier Security Group has no inbound rules for CIDR of 0 (Global Allow): Not Applicable

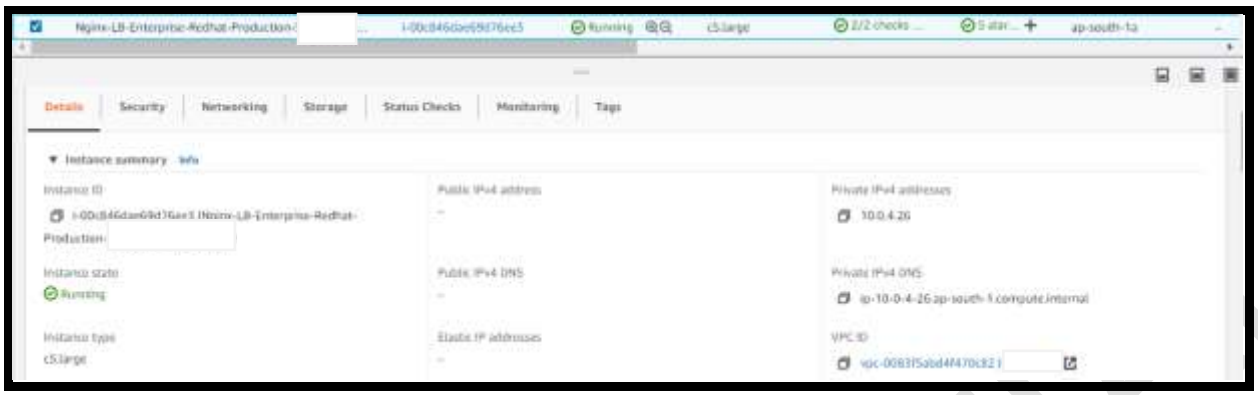
6.26 Ensure the App tier ELB is created as Internal: Not Applicable

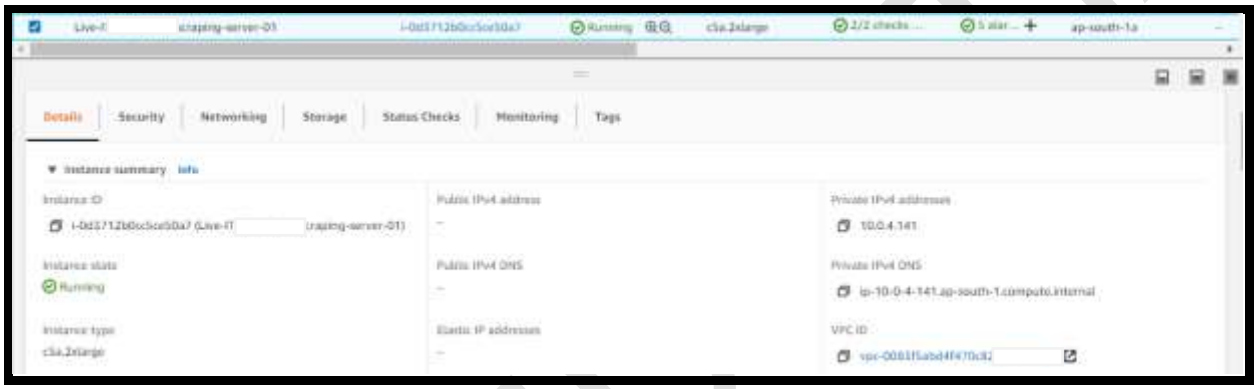
6.27 Ensure EC2 instances within Web Tier have no Elastic / Public IP addresses associated / 6.28 Ensure EC2 instances within App Tier have no Elastic / Public IP addresses associated / 6.29 Ensure EC2 instances within Data Tier have no Elastic / Public IP addresses associated.

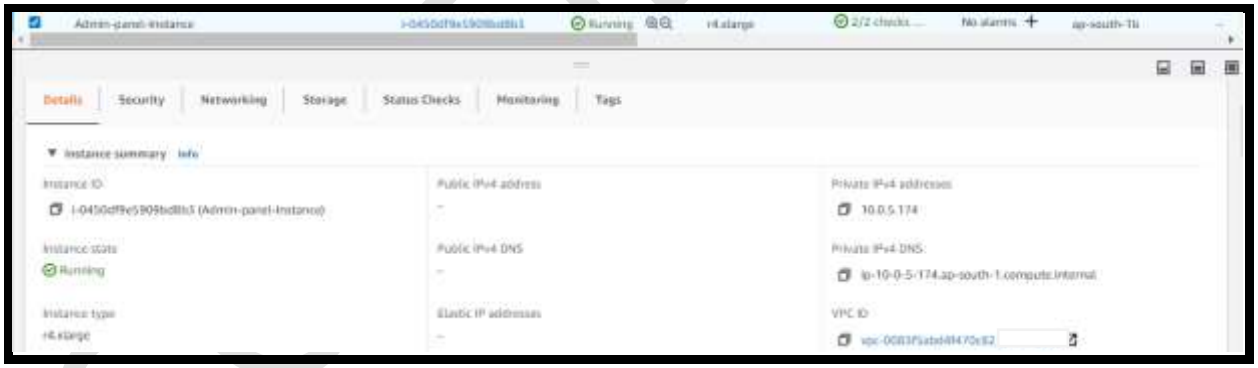




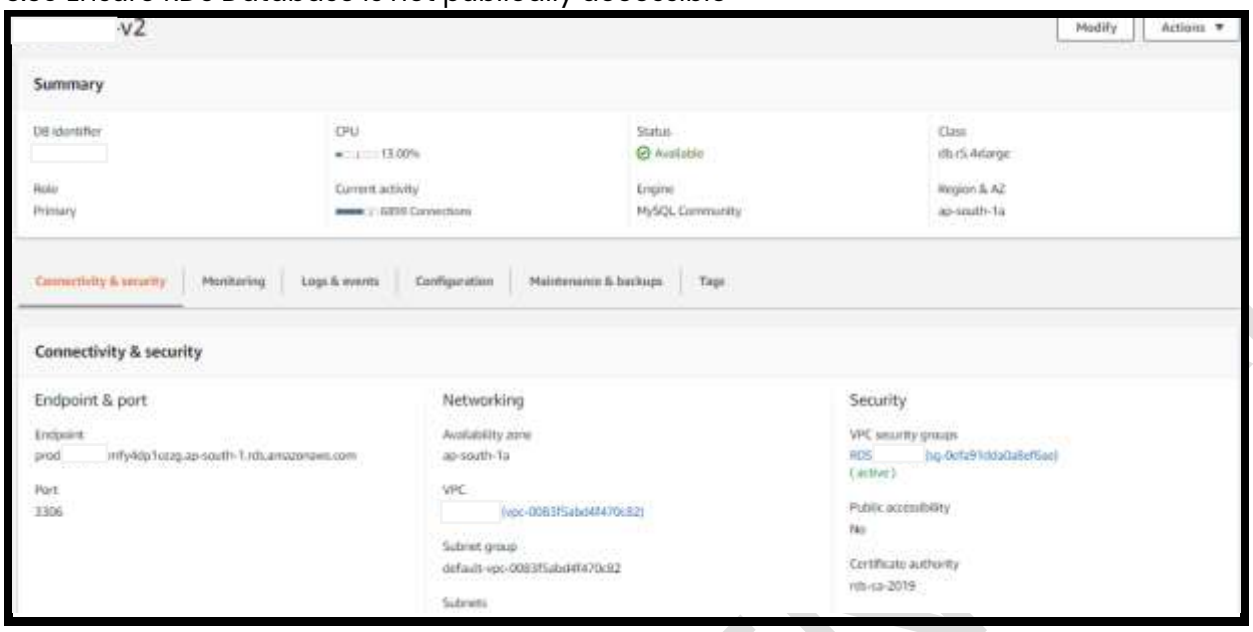


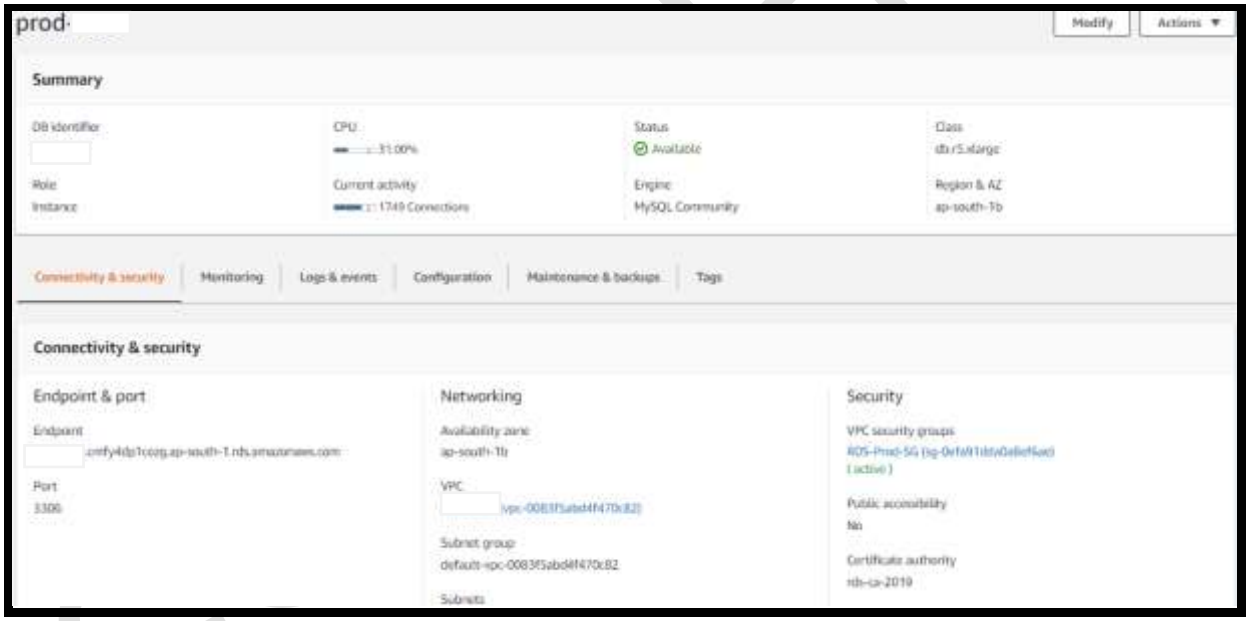


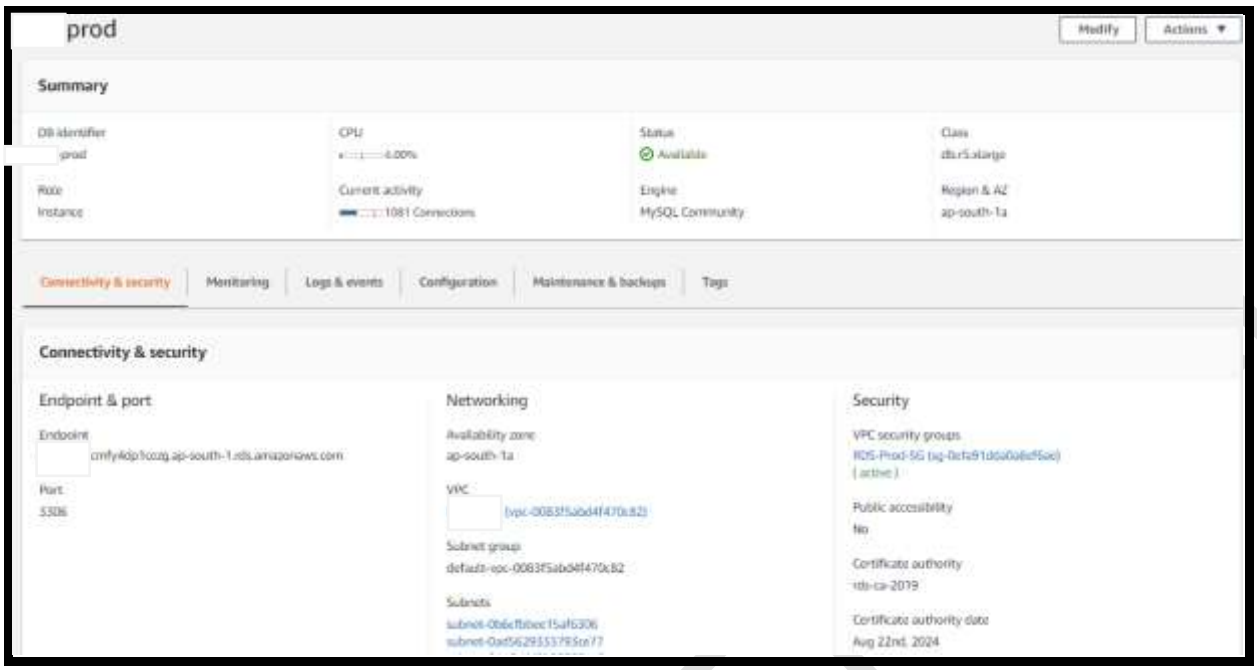




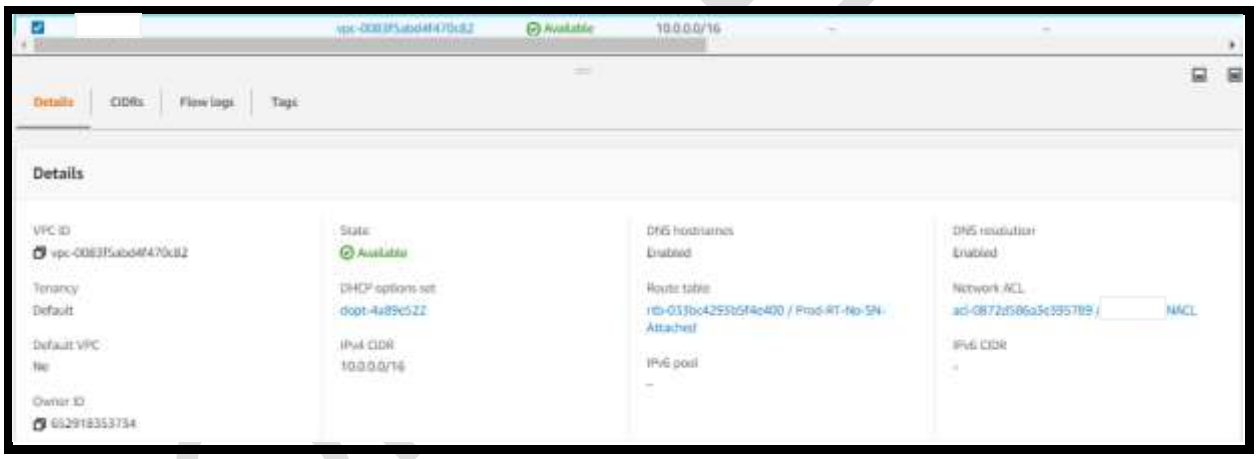
6.30 Ensure RDS Database is not publically accessible







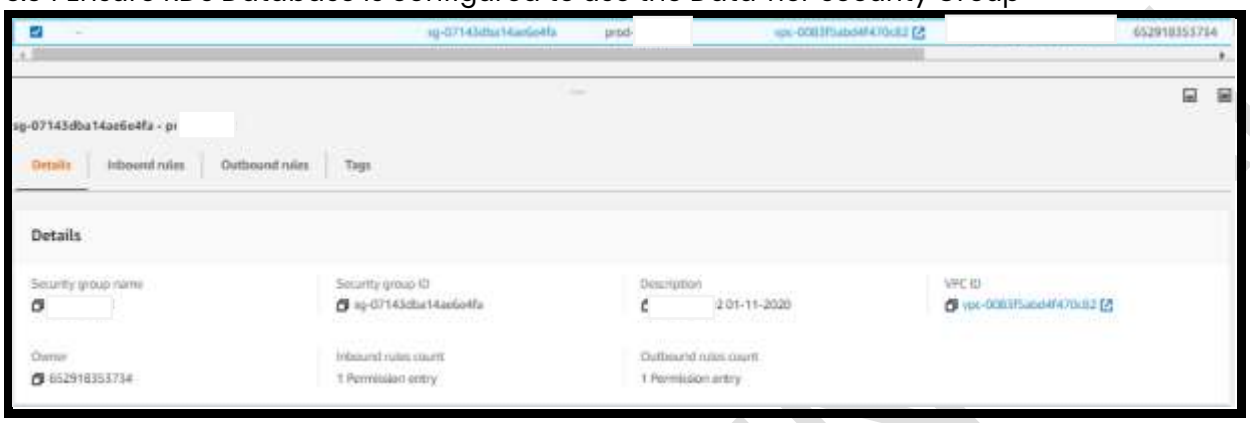
6.31 Don't use the default VPC



6.32 Ensure Auto-Scaling Launch Configuration for Web Tier is configured to use the Web Tier Security Group. Not Applicable

6.33 Ensure Auto-Scaling Launch Configuration for App Tier is configured to use the App Tier Security Group. Not Applicable

6.34 Ensure RDS Database is configured to use the Data Tier Security Group



Section 4 – List of actions required to complete the hardening configuration.

Point		Action Required
1.1,1.2,1.3	Ensure a customer created Customer Master Key (CMK) is created for the Web/App/Database tier	Currently we have default AWS KMS in use, we need to create CMK, which allows for configuration of key rotation and key policy which is applied to the customer created CMK.
1.5,1.6	Ensure all EBS volumes for Web/App Tier are encrypted	Need to encrypt not encrypted EBS volumes.
1.16	Ensure all S3 buckets have policy to require server-side and in transit encryption for all objects stored in bucket.	Need to enable the encryption of S3 buckets.
2.7	Ensure an IAM group for administration purposes is created.	Need to create IAM group for administration purpose so that any user in that group automatically has the permissions that are assigned to the group.
3.5	Ensure Relational Database Service is Multi-AZ Enabled	Need to enable Multi-AZ on RDS service so that it can provide AWS managed high availability of the Database Tier across 2 availability zones within a region through asynchronous replication at the data layer.
3.6	Ensure Relational Database Service Instances have Auto Minor Version Upgrade Enabled	Need to enable Auto Minor Version Upgrade of RDS. It ensures automated patch management is in place on the RDS instance to ensure the database engine has all the latest patches applied.
3.11	Ensure S3 buckets have versioning enabled	Need to enable S3 buckets versioning. It enables us to recover objects from accidental deletion or overwrite.
4.4	Ensure RDS event subscriptions are enabled for DB security groups	Need to enable RDS event subscription for DB security groups. It is designed to provide incident notification of events which may affect the network availability of the RDS instance.
6.10	Ensure NAT Gateways are created in at least 2 Availability Zones	Need to create 2 availability zones for NAT Gateway currently we have 1.
6.20,6.23	Ensure Web tier Security Group has no inbound rules for CIDR of 0 (Global Allow)	Need to change the inbound rule of security groups with same rule.
6.21	Create the App tier ELB Security Group and ensure only accepts HTTP/HTTPS	Need to change the inbound rule of ELB Security Group which accepts from other ports as well.

About Infopercept

Infopercept's vision and core values revolve around making organizations more secure through the core values of Honesty, Transparency and Knowledge, so as to enable them to make better informed decisions about their security practices & goals. With our synergistic vision to combine technical expertise and professional experience, we aim to further establish our place as a one stop shop for our clients and partners' cybersecurity and accreditation needs.

Our specialized core team comprises experienced veterans, technical experts & security enthusiasts having good practical experience & thorough knowledge in the Cybersecurity domain, latest trends, and security innovations; ensuring that you always get the best security approach & solution for your specific business needs exactly the way you want it to be.

Imprint

© Infopercept Consulting Pvt. Ltd. 2021

Publisher

H-1209, Titanium City Center,
Satellite Road,
Ahmedabad – 380 015,
Gujarat, India.

Contact Info

M: +91 9898857117
W: www.infopercept.com
E: sos@infopercept.com

Global Office

United State of America
+1 516 713 5040

United Kingdom
+44 2035002056

Sri Lanka
+94 702 958 909

Kuwait
+965 6099 1177

India
+91 9898857117

Infopercept