



Cloud Security Assessment Sample Report

INFOPERCEPT
Sample Report 2020

YOUR DATE HERE

COMPANY NAME
Authored by: Your Name

 **Infopercept**

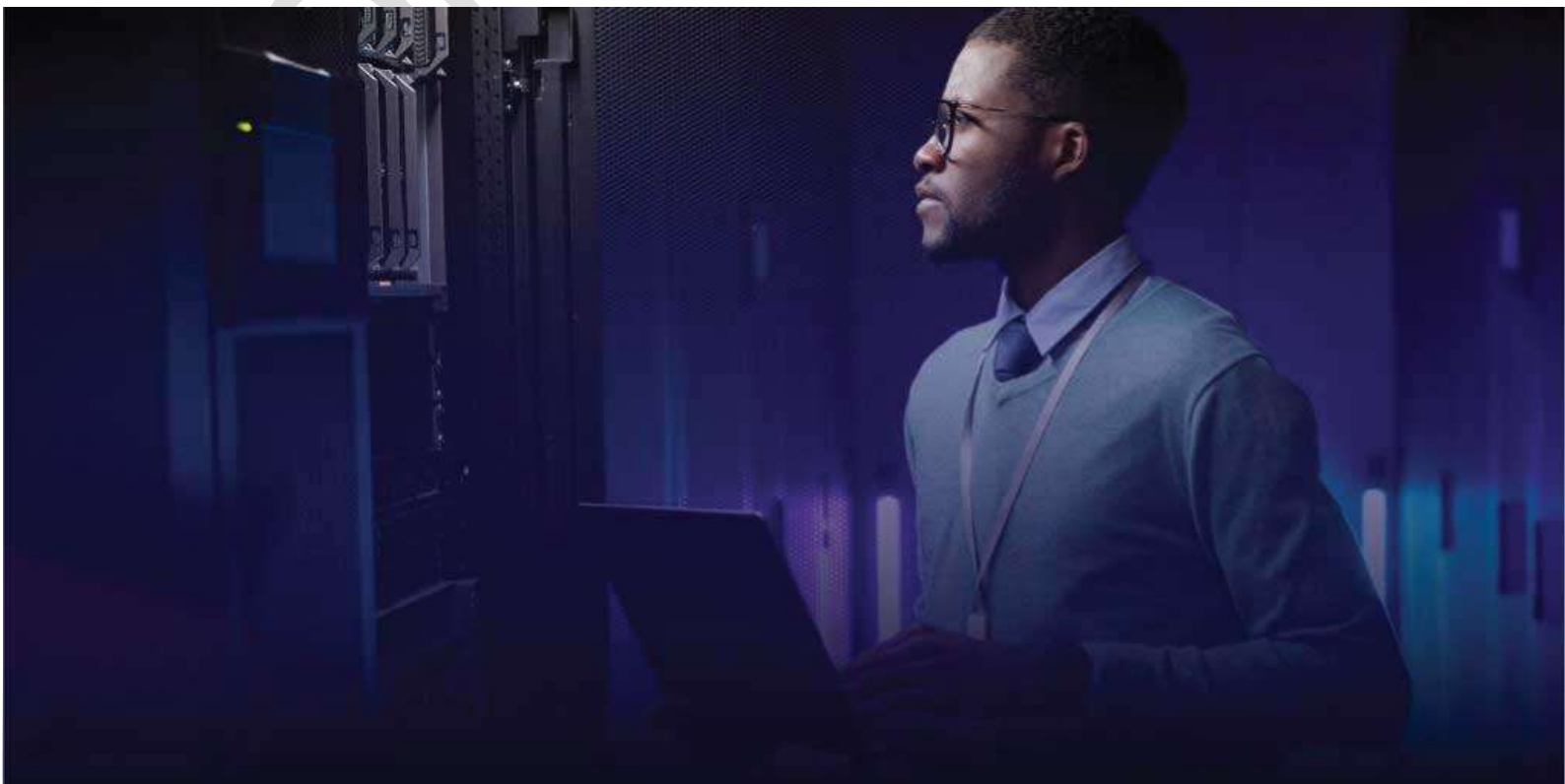
Contents

Disclaimer.....	4
Section 1 – Scope of Review.....	5
1. Primary Production Servers.....	5
2.Sub Production Servers	5
Section 2 – Summary	6
Section 3 – AWS Configuration Snapshots for CIS Three tier guidelines	7
1. Data Protection: -	7
2 Identity and Access Management.....	28
3 Business Continuity	31
4 Event Monitoring and Response	43
5 Audit and Logging	44
6 Networking	53
About Infopercept.....	64

Copyright

The copyright in this work is vested in Infopercept Consulting Pvt. Ltd, and the document is issued in confidence for the purpose for which it is supplied. It must not be reproduced in whole or in part or used for tendering or manufacturing purposes except under agreement or with the consent in writing of Infopercept Consulting Pvt. Ltd. and then only on condition that this notice is included in any such reproduction. No information as to the contents or subject matter of this document or any part thereof arising directly or indirectly there from shall be given orally or in writing or communicated in any manner whatsoever to any third party being an individual firm or company or any employee thereof without the prior consent in writing of Infopercept Consulting Pvt. Ltd.

© Infopercept Consulting Pvt. Ltd. 2021.



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

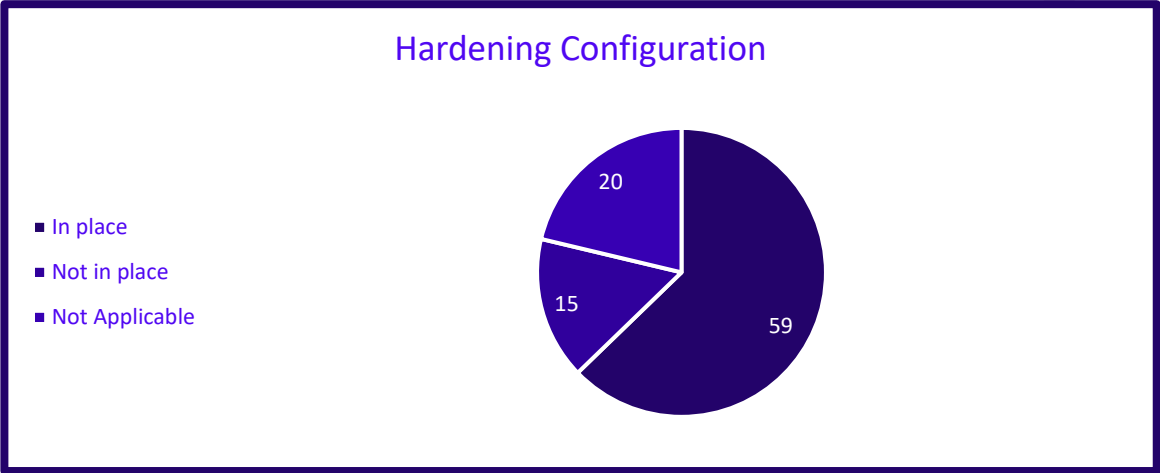
- a. Live-ITR-Xyxyx-scraping-server-01
- b. Live-REDHAT-1ST - HARDEN OS
- c. LIVE-REDHAT-2ND-HARDEN-OS
- d. ADMIN-PANEL-INSTANCE
- e. ABCD-Live-Production-02
- f. CHECK-POINT-GATEWAY-AUTOSCALING ALLBANKS-1
- g. CHECK-POINT-GATEWAY-AUTOSCALING ALLBANKS-2
- h. CHECK-POINT-VPNGW (ALL BANKS)
- i. CHECK-POINT-MGMT (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

Instance			
Configuration	Instance class	Storage	Performance Insights
DB instance id <div></div>	Instance class db.r5.4xlarge	Encryption Enabled	Performance Insights enabled No
Engine version 5.7.23	vCPU 16	KMS key a52c3ad3-36b0-4381-9ff5-bb274e89d913	Published logs
DB name <div></div>	RAM 128 GB	Storage type Provisioned IOPS (SSD)	CloudWatch Logs Audit Error General Slow query
License model General Public License	Availability	IOPS 2500	
Option groups <div></div>	Master username <div></div>	Storage 2400 GiB	
Amazon Resource Name (ARN) arn:aws:rds:ap-south-1:652918353734:v2	IAM db authentication Enabled	Storage autoscaling Disabled	
	Multi AZ Yes		

Prod-xyy

Instance			
Configuration	Instance class	Storage	Performance Insights
DB instance id <input type="text"/>	Instance class db.r5.xlarge	Encryption Enabled	Performance Insights enabled No
Engine version 5.7.23	vCPU 4	KMS key a52c3ad3-36b0-4381-9ff5-bb274e89d913	Published logs
DB name -	RAM 32 GB	Storage type Provisioned IOPS (SSD)	CloudWatch Logs Audit Error General Slow query
License model General Public License	Availability	IOPS 1000	
Option groups <input type="text"/>	Master username <input type="text"/>	Storage 300 GiB	
Amazon Resource Name (ARN) arn:aws:rds:ap-south-1:652918353734: <input type="text"/>	IAM db authentication Enabled	Storage autoscaling Disabled	
	Multi AZ No		

prod

Instance			
Configuration	Instance class	Storage	Performance Insights
DB instance id <input type="text"/>	Instance class db.r5.xlarge	Encryption Enabled	Performance Insights enabled No
Engine version 5.7.26	vCPU 4	KMS key a52c3ad3-36b0-4381-9ff5-bb274e89d913	Published logs
DB name <input type="text"/>	RAM 32 GB	Storage type Provisioned IOPS (SSD)	CloudWatch Logs Audit Error General Slow query
License model General Public License	Availability	IOPS 1000	
Option groups <input type="text"/>	Master username <input type="text"/>	Storage 200 GiB	
Amazon Resource Name (ARN) arn:aws:rds:ap-south-1:652918353734:db- <input type="text"/>	IAM db authentication Enabled	Storage autoscaling Disabled	
	Multi AZ No		

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

Volumes: | vol-0e6365f60905dd51 (Prod-xyz-v2-server-1)

Description	Status Checks	Monitoring	Tags
Volume ID	vol-0e6365f60905dd51	Outposts ARN	-
Alarm status	None	Size	275 GiB
Snapshot	snap-022cc09e260ca78d9	Created	October 31, 2020 at 4:31:51 PM UTC+5:30
Availability Zone	ap-south-1a	State	in-use
Encryption	Encrypted	Attachment information	i-07bc5d595daa7a14a (Prod-xyz-v2-server-1) /dev/sdb (attached)
KMS Key ID	kms-key-03e74ef4b	Volume type	gp2
KMS Key Aliases	arn:aws:kms:ap-south-1:652918353734:key/i07adcf5-b93c-4ab4-b69e-03e74ef4b	Product codes	-
KMS Key ARN	arn:aws:kms:ap-south-1:652918353734:key/i07adcf5-b93c-4ab4-b69e-03e74ef4b	IOPS	825
Throughput (MB/s)	-	Multi-Attach Enabled	No

Volumes: | vol-065542c6ed735eca8 (Prod-xyz-v2-server-1)

Description	Status Checks	Monitoring	Tags
Volume ID	vol-065542c6ed735eca8	Outposts ARN	-
Alarm status	None	Size	16 GiB
Snapshot	snap-09209ef7156e87993	Created	October 31, 2020 at 3:47:11 PM UTC+5:30
Availability Zone	ap-south-1a	State	in-use
Encryption	Encrypted	Attachment information	i-07bc5d595daa7a14a (Prod-xyz-v2-server-1) /dev/sdb (attached)
KMS Key ID	kms-key-03e74ef4b	Volume type	gp2
KMS Key Aliases	arn:aws:kms:ap-south-1:652918353734:key/i07adcf5-b93c-4ab4-b69e-03e74ef4b	Product codes	-
KMS Key ARN	arn:aws:kms:ap-south-1:652918353734:key/i07adcf5-b93c-4ab4-b69e-03e74ef4b	IOPS	100
Throughput (MB/s)	-	Multi-Attach Enabled	No

Volumes: | vol-01813780f91b6a611 (Prod-xyz-v2-server-1)

Description	Status Checks	Monitoring	Tags
Volume ID	vol-01813780f91b6a611	Outposts ARN	-
Alarm status	None	Size	50 GiB
Snapshot	snap-0989a444e5a5800d5	Created	October 31, 2020 at 3:47:11 PM UTC+5:30
Availability Zone	ap-south-1a	State	in-use
Encryption	Encrypted	Attachment information	i-07bc5d595daa7a14a (Prod-xyz-v2-server-1) /dev/sda1 (attached)
KMS Key ID	kms-key-03e74ef4b	Volume type	gp2
KMS Key Aliases	arn:aws:kms:ap-south-1:652918353734:key/i07adcf5-b93c-4ab4-b69e-03e74ef4b	Product codes	-
KMS Key ARN	arn:aws:kms:ap-south-1:652918353734:key/i07adcf5-b93c-4ab4-b69e-03e74ef4b	IOPS	150
Throughput (MB/s)	-	Multi-Attach Enabled	No

Prod-xyz-v2-2

Volumes: | vol-0018a58eb15c93e7 (prod-xyz-v2-2)

Description	Status Checks	Monitoring	Tags
Volume ID	vol-0018a58eb15c93e7	Outposts ARN	-
Alarm status	None	Size	16 GiB
Snapshot	snap-0180a015ed1f1a1a	Created	November 2, 2020 at 4:04:30 AM UTC+5:30
Availability Zone	ap-south-1a	State	in-use
Encryption	Encrypted	Attachment information	i-065cd190734e58b7 (Prod-xyz-v2-server-2) /dev/sdb (attached)
KMS Key ID	kms-key-03e74ef4b	Volume type	gp2
KMS Key Aliases	arn:aws:kms:ap-south-1:652918353734:key/i07adcf5-b93c-4ab4-b69e-03e74ef4b	Product codes	-
KMS Key ARN	arn:aws:kms:ap-south-1:652918353734:key/i07adcf5-b93c-4ab4-b69e-03e74ef4b	IOPS	100
Throughput (MB/s)	-	Multi-Attach Enabled	No

Volumes: | vol-0bc5981bca82ed4e (prod-yyz-1)

Description | Status Checks | Monitoring | Tags

Volume ID	vol-0bc5981bca82ed4e	Outposts ARN	-
Alarm status	None	Size	275 GiB
Snapshot	snap-0478a2c29543a4639	Created	November 2, 2020 at 4:06:30 AM UTC+5:30
Availability Zone	ap-south-1a	State	In-use
Encryption	Encrypted	Attachment information	i-093c9199734ed8607 (Prod-yyz-1/udev/sda1 (attached))
KMS Key ID	fk7adcf5-b93c-4ab4-b69e-03ef74ef4b	Volume type	gp2
KMS Key Aliases		Product codes	-
KMS Key ARN	arn:aws:kms:ap-south-1:652918353734:key/fk7adcf5-b93c-4ab4-b69e-03ef74ef4b	IOPS	620
Throughput (MB/s)	-	Multi-Attach Enabled	No

Volumes: | vol-09e8956278ce1f0dc (prod-yyz-1)

Description | Status Checks | Monitoring | Tags

Volume ID	vol-09e8956278ce1f0dc	Outposts ARN	-
Alarm status	None	Size	50 GiB
Snapshot	snap-0fa75c7d7cebd9ad	Created	November 2, 2020 at 4:06:30 AM UTC+5:30
Availability Zone	ap-south-1a	State	In-use
Encryption	Encrypted	Attachment information	i-093c9199734ed8607 (Prod-yyz-1/udev/sda1 (attached))
KMS Key ID	fk7adcf5-b93c-4ab4-b69e-03ef74ef4b	Volume type	gp2
KMS Key Aliases		Product codes	-
KMS Key ARN	arn:aws:kms:ap-south-1:652918353734:key/fk7adcf5-b93c-4ab4-b69e-03ef74ef4b	IOPS	150
Throughput (MB/s)	-	Multi-Attach Enabled	No

Prod-YYZ-1

Volumes: | vol-0b3a10c3628016c5a (preprod-yyz-1)

Description | Status Checks | Monitoring | Tags

Volume ID	vol-0b3a10c3628016c5a	Outposts ARN	-
Alarm status	None	Size	145 GiB
Snapshot	snap-0e44ae8925db179fd	Created	December 16, 2020 at 2:22:33 PM UTC+5:30
Availability Zone	ap-south-1a	State	In-use
Encryption	Encrypted	Attachment information	i-036694e5168cb895d (Preprod-yyz-1/udev/sda1 (attached))
KMS Key ID	fk7adcf5-b93c-4ab4-b69e-03ef74ef4b	Volume type	gp2
KMS Key Aliases		Product codes	-
KMS Key ARN	arn:aws:kms:ap-south-1:652918353734:key/fk7adcf5-b93c-4ab4-b69e-03ef74ef4b	IOPS	430
Throughput (MB/s)	-	Multi-Attach Enabled	No

Volumes: | vol-0e0742236992f98a3 (preprod-yyz-1)

Description | Status Checks | Monitoring | Tags

Volume ID	vol-0e0742236992f98a3	Outposts ARN	-
Alarm status	None	Size	95 GiB
Snapshot	snap-0781f7574d85c2a27	Created	December 16, 2020 at 2:22:33 PM UTC+5:30
Availability Zone	ap-south-1a	State	In-use
Encryption	Encrypted	Attachment information	i-036694e5168cb895d (Preprod-yyz-1/udev/sda1 (attached))
KMS Key ID	fk7adcf5-b93c-4ab4-b69e-03ef74ef4b	Volume type	gp2
KMS Key Aliases		Product codes	-
KMS Key ARN	arn:aws:kms:ap-south-1:652918353734:key/fk7adcf5-b93c-4ab4-b69e-03ef74ef4b	IOPS	285
Throughput (MB/s)	-	Multi-Attach Enabled	No

Volumes: | vol-06e1b3917421e42c3 (preprod)

Description	Status Checks	Monitoring	Tags
Volume ID	vol-06e1b3917421e42c3	Outposts ARN	-
Alarm status	None	Size	16 GB
Snapshot	snap-0a18b064a87152e	Created	December 16, 2020 at 2:22:33 PM UTC+5:30
Availability Zone	ap-south-1a	State	In-use
Encryption	Encrypted	Attachment information	i-0368d4651682d85d (Preprod-) x86g (attached)
KMS Key ID	07adcf8-b93c-4ab4-b69e-03ef74ef4b	Volume type	gp2
KMS Key Aliases		Product codes	-
KMS Key ARN	arn:aws:kms:ap-south-1:652918353734:key/07adcf8-b93c-4ab4-b69e-03ef74ef4b	IOPS	160
Throughput (MB/s)	-	Multi-Attach Enabled	No

Volumes: | vol-0a28a5752580d64e (preprod ginx)

Description	Status Checks	Monitoring	Tags
Volume ID	vol-0a28a5752580d64e	Outposts ARN	-
Alarm status	None	Size	10 GB
Snapshot	snap-01410d48e11a3d1a6	Created	December 16, 2020 at 2:48:20 PM UTC+5:30
Availability Zone	ap-south-1a	State	In-use
Encryption	Encrypted	Attachment information	i-0221ad40a23ed25cf (Algin-LB-Developer-Redhat-preprod-server)/devsdb1 (attached)
KMS Key ID	07adcf8-b93c-4ab4-b69e-03ef74ef4b	Volume type	gp2
KMS Key Aliases		Product codes	marketplace.1758a9e0b0a2e44a7a8f
KMS Key ARN	arn:aws:kms:ap-south-1:652918353734:key/07adcf8-b93c-4ab4-b69e-03ef74ef4b	IOPS	100
Throughput (MB/s)	-	Multi-Attach Enabled	No

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

Volumes: | vol-0e1afe3e49d12bcd4 (Live-I) ping server 01-100GB)

Description	Status Checks	Monitoring	Tags
Volume ID	vol-0e1afe3e49d12bcd4	Outposts ARN	-
Alarm status	None	Size	100 GB
Snapshot	-	Created	December 15, 2020 at 3:25:38 PM UTC+5:30
Availability Zone	ap-south-1a	State	In-use
Encryption	Encrypted	Attachment information	i-0d3712b0cc50a59a7 (Live-) ig-server-01/devsdb (attached)
KMS Key ID	07adcf8-b93c-4ab4-b69e-03ef74ef4b	Volume type	gp2
KMS Key Aliases		Product codes	-
KMS Key ARN	arn:aws:kms:ap-south-1:652918353734:key/07adcf8-b93c-4ab4-b69e-03ef74ef4b	IOPS	350
Throughput (MB/s)	-	Multi-Attach Enabled	No

Volumes: | vol-0aa9527ac21354c5 (Live-) ping-server-01-encrypted-swap-partition)

Description	Status Checks	Monitoring	Tags
Volume ID	vol-0aa9527ac21354c5	Outposts ARN	-
Alarm status	None	Size	16 GB
Snapshot	snap-260f4ec79b4026f6d	Created	December 7, 2020 at 8:02:56 PM UTC+5:30
Availability Zone	ap-south-1a	State	In-use
Encryption	Encrypted	Attachment information	i-0d3712b0cc50a59a7 (Live-) ig-server-01/devsdb (attached)
KMS Key ID	07adcf8-b93c-4ab4-b69e-03ef74ef4b	Volume type	gp2
KMS Key Aliases		Product codes	-
KMS Key ARN	arn:aws:kms:ap-south-1:652918353734:key/07adcf8-b93c-4ab4-b69e-03ef74ef4b	IOPS	100
Throughput (MB/s)	-	Multi-Attach Enabled	No

Volumes: | vol-0adfa4ff5f139eba (Live: ping-server-01-encrypted-root-partition)

Description	Status Checks	Monitoring	Tags
Volume ID	vol-0adfa4ff5f139eba		
Alarm status	None		
Snapshot	snap-023c33f33e02aa54		
Availability Zone	ap-south-1a		
Encryption	Encrypted		
KMS Key ID	kms-03e74bf4b		
KMS Key ARN	arn:aws:kms:ap-south-1:652918353734:key/kms-03e74bf4b		
Throughput (MB/s)	-		
Outposts ARN	-		
Size	30 GiB		
Created	December 7, 2020 at 8:01:50 PM UTC+5:30		
State	In-use		
Attachment information	i-0d3712b0cc5c50a7 (Live: server-01/devsda1 (attached))		
Volume type	gp2		
Product codes	-		
IOPS	100		
Multi-Attach Enabled	No		

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

Volumes: | vol-0ef623545afcfabab5 (Live: ping-server-02-100GB)

Description	Status Checks	Monitoring	Tags
Volume ID	vol-0ef623545afcfabab5		
Alarm status	None		
Snapshot	-		
Availability Zone	ap-south-1b		
Encryption	Encrypted		
KMS Key ID	kms-03e74bf4b		
KMS Key ARN	arn:aws:kms:ap-south-1:652918353734:key/kms-03e74bf4b		
Throughput (MB/s)	-		
Outposts ARN	-		
Size	100 GiB		
Created	December 15, 2020 at 2:46:36 PM UTC+5:30		
State	In-use		
Attachment information	i-0f992601a5c1d04c (Live: server-02/devsdb (attached))		
Volume type	gp2		
Product codes	-		
IOPS	300		
Multi-Attach Enabled	No		

Volumes: | vol-04801eeb1d3f7d387 (Live: ping-server-02-swap-07-12-2020)

Description	Status Checks	Monitoring	Tags
Volume ID	vol-04801eeb1d3f7d387		
Alarm status	None		
Snapshot	snap-0ed74c78f306f600		
Availability Zone	ap-south-1b		
Encryption	Encrypted		
KMS Key ID	kms-03e74bf4b		
KMS Key ARN	arn:aws:kms:ap-south-1:652918353734:key/kms-03e74bf4b		
Throughput (MB/s)	-		
Outposts ARN	-		
Size	18 GiB		
Created	December 7, 2020 at 12:29:24 PM UTC+5:30		
State	In-use		
Attachment information	i-0f992601a5c1d04c (Live: server-02/devsdb (attached))		
Volume type	gp2		
Product codes	-		
IOPS	100		
Multi-Attach Enabled	No		

Pre-Production-29-07-2020

Volumes: | vol-091e3781ea9c3fb07 (Pre-Production-29-07-2020)

Description	Status Checks	Monitoring	Tags
Volume ID	vol-091e3781ea9c3fb07	Outputs ARN	-
Alarm status	None	Size	250 GiB
Snapshot	snap-0840a24e267e0558	Created	July 29, 2020 at 12:41:39 PM UTC+5:30
Availability Zone	ap-south-1a	State	in-use
Encryption	Encrypted	Attachment information	i-0030a4578aa296a3d (Live-Redhat-Server-Harden- NewIdk (attached))
KMS Key ID	kms-key-007adcf5-b93c-4ab4-b69e-03e774bf4b	Volume type	gp2
KMS Key Alias	arn:aws:kms:ap-south-1:652918353734:key/i07adcf5-b93c-4ab4-b69e-03e774bf4b	Product codes	-
KMS Key ARN	arn:aws:kms:ap-south-1:652918353734:key/i07adcf5-b93c-4ab4-b69e-03e774bf4b	IOPS	750
Throughput (MB/s)	-	Multi-Attach Enabled	No

Volumes: | vol-036e271e72c14d852 (Pre-Production-29-07-2020)

Description	Status Checks	Monitoring	Tags
Volume ID	vol-036e271e72c14d852	Outputs ARN	-
Alarm status	None	Size	16 GiB
Snapshot	snap-06d2f0a7ecdb179e	Created	July 29, 2020 at 12:41:39 PM UTC+5:30
Availability Zone	ap-south-1a	State	in-use
Encryption	Not Encrypted	Attachment information	i-0030a4578aa296a3d (Live-Redhat-Server-Harden- NewIdk (attached))
KMS Key ID	-	Volume type	gp2
KMS Key Alias	-	Product codes	-
KMS Key ARN	-	IOPS	100
Throughput (MB/s)	-	Multi-Attach Enabled	No

Not Encrypted

Trend-micro-windows

Volumes: | vol-00524abb4af48238 (Trend-micro-windows)

Description	Status Checks	Monitoring	Tags
Volume ID	vol-00524abb4af48238	Outputs ARN	-
Alarm status	None	Size	250 GiB
Snapshot	snap-086a7a7ba681252b	Created	September 2, 2020 at 5:11:06 PM UTC+5:30
Availability Zone	ap-south-1b	State	in-use
Encryption	Encrypted	Attachment information	i-033871537a5c89610 (Trend-micro-windows- NewIdk (attached))
KMS Key ID	kms-key-007adcf5-b93c-4ab4-b69e-03e774bf4b	Volume type	gp2
KMS Key Alias	arn:aws:kms:ap-south-1:652918353734:key/i07adcf5-b93c-4ab4-b69e-03e774bf4b	Product codes	-
KMS Key ARN	arn:aws:kms:ap-south-1:652918353734:key/i07adcf5-b93c-4ab4-b69e-03e774bf4b	IOPS	750
Throughput (MB/s)	-	Multi-Attach Enabled	No

Admin-panel-Instance

Volumes: | vol-0a227955afc2c55ed (Admin-panel-Instance)

Description	Status Checks	Monitoring	Tags
Volume ID	vol-0a227955afc2c55ed	Outputs ARN	-
Alarm status	None	Size	150 GiB
Snapshot	snap-052850eab102675	Created	October 22, 2018 at 2:51:32 PM UTC+5:30
Availability Zone	ap-south-1b	State	in-use
Encryption	Encrypted	Attachment information	i-0450d5e9906d8b3 (Admin-panel- InstanceNewIdk (attached))
KMS Key ID	kms-key-007adcf5-b93c-4ab4-b69e-03e774bf4b	Volume type	gp2
KMS Key Alias	arn:aws:kms:ap-south-1:652918353734:key/i07adcf5-b93c-4ab4-b69e-03e774bf4b	Product codes	-
KMS Key ARN	arn:aws:kms:ap-south-1:652918353734:key/i07adcf5-b93c-4ab4-b69e-03e774bf4b	IOPS	450
Throughput (MB/s)	-	Multi-Attach Enabled	No

Volumes: | vol-0222e68633149c77 (Admin-panel-instance)

Description	Status Checks	Monitoring	Tags
Volume ID	vol-0222e68633149c77		
Alarm status	None		
Snapshot	snap-0d3451b34098c5636		
Availability Zone	ap-south-1b		
Encryption	Not Encrypted		
KMS Key ID			
KMS Key Aliases			
KMS Key ARN			
Throughput (MB/s)	-		
Outposts ARN	-		
Size	16 GiB		
Created	October 22, 2018 at 2:51:31 PM UTC+5:30		
State	In-use		
Attachment information	i-0450d9e5909cd0b1 (Admin-panel-instance)/devxsf (attached)		
Volume type	gp2		
Product codes	-		
IOPS	100		
Multi-Attach Enabled	No		

Not Encrypted

Volumes: | vol-0498b78a4495ed354 (Admin-panel-instance)

Description	Status Checks	Monitoring	Tags
Volume ID	vol-0498b78a4495ed354		
Alarm status	None		
Snapshot	snap-05a4541ee68ced7b		
Availability Zone	ap-south-1b		
Encryption	Not Encrypted		
KMS Key ID			
KMS Key Aliases			
KMS Key ARN			
Throughput (MB/s)	-		
Outposts ARN	-		
Size	80 GiB		
Created	October 22, 2018 at 2:51:31 PM UTC+5:30		
State	In-use		
Attachment information	i-0450d9e5909cd0b1 (Admin-panel-instance)/devxsf1 (attached)		
Volume type	gp2		
Product codes	-		
IOPS	100		
Multi-Attach Enabled	No		

Not Encrypted

Tableau-server-13-04-2020

Volumes: | vol-0fb1882b903af7e5 (Tableau-server-13-04-2020)

Description	Status Checks	Monitoring	Tags
Volume ID	vol-0fb1882b903af7e5		
Alarm status	None		
Snapshot	snap-0f0ac7ad28a84e090		
Availability Zone	ap-south-1a		
Encryption	Encrypted		
KMS Key ID	107ad0f6-b93c-4ab4-b69a-03af748f4b		
KMS Key Aliases			
KMS Key ARN	arn:aws:kms:ap-south-1:65291833734:key/107ad0f6-b93c-4ab4-b69a-03af748f4b		
Throughput (MB/s)	-		
Outposts ARN	-		
Size	100 GiB		
Created	April 13, 2020 at 11:05:03 AM UTC+5:30		
State	In-use		
Attachment information	i-04e458d77c2b395d (Tableau-server-13-04-2020)/devxsf1 (attached)		
Volume type	gp2		
Product codes	-		
IOPS	300		
Multi-Attach Enabled	No		

ABCD-Live-Production

Volumes: | vol-0d36ed8a30aa3fb9 (Production)

Description	Status Checks	Monitoring	Tags
Volume ID	vol-0d36ed8a30aa3fb9		
Alarm status	None		
Snapshot	snap-08d211cd8a0329c2c		
Availability Zone	ap-south-1b		
Encryption	Not Encrypted		
KMS Key ID			
KMS Key Aliases			
KMS Key ARN			
Throughput (MB/s)	-		
Outposts ARN	-		
Size	16 GiB		
Created	September 7, 2019 at 8:54:49 PM UTC+5:30		
State	In-use		
Attachment information	i-05ad2448b50c0584 (Production-02)/devxsf (attached)		
Volume type	gp2		
Product codes	-		
IOPS	100		
Multi-Attach Enabled	No		

Not Encrypted

Volumes: | vol-053aa4fc92eaf0ef | Production

Description	Status Checks	Monitoring	Tags
Volume ID	vol-053aa4fc92eaf0ef		
Alarm status	None		
Snapshot	snap-0662c960212b36f7		
Availability Zone	ap-south-1b		
Encryption	Not Encrypted		
KMS Key ID			
KMS Key Alias			
KMS Key ARN			
Throughput (MB/s)	-		
Outposts ARN	-		
Size	30 GiB		
Created	September 7, 2019 at 8:54:49 PM UTC+5:30		
State	In-use		
Attachment information	i-05ad2448f05045504 Production-02:/dev/sda1 (attached)		
Volume type	gp2		
Product codes	-		
IOPS	100		
Multi-Attach Enabled	No		

Not Encrypted

Volumes: | vol-0696130454ed50b5e | Production

Description	Status Checks	Monitoring	Tags
Volume ID	vol-0696130454ed50b5e		
Alarm status	None		
Snapshot	snap-0be10771cd7179e0f		
Availability Zone	ap-south-1b		
Encryption	Encrypted		
KMS Key ID	07adcf8-b93c-4ab4-b89e-0f3ef74ef4e		
KMS Key Alias			
KMS Key ARN	arn:aws:kms:ap-south-1:052918353734:key/07adcf8-b93c-4ab4-b89e-0f3ef74ef4e		
Throughput (MB/s)	-		
Outposts ARN	-		
Size	250 GiB		
Created	September 7, 2019 at 8:54:49 PM UTC+5:30		
State	In-use		
Attachment information	i-05ad2448f05045504 Production-02:/dev/sda1 (attached)		
Volume type	gp2		
Product codes	-		
IOPS	750		
Multi-Attach Enabled	No		

ABCD-Live-Production-03

Volumes: | vol-0d12a2f48fcd8a65b | Production-03

Description	Status Checks	Monitoring	Tags
Volume ID	vol-0d12a2f48fcd8a65b		
Alarm status	None		
Snapshot	snap-0c7d95e52e438e4		
Availability Zone	ap-south-1a		
Encryption	Not Encrypted		
KMS Key ID			
KMS Key Alias			
KMS Key ARN			
Throughput (MB/s)	-		
Outposts ARN	-		
Size	16 GiB		
Created	January 9, 2020 at 1:52:43 PM UTC+5:30		
State	In-use		
Attachment information	i-028c7991a2e551387 Production-03:/dev/sdb (attached)		
Volume type	gp2		
Product codes	-		
IOPS	100		
Multi-Attach Enabled	No		

Not Encrypted

Volumes: | vol-0b498b892e4dd4f97 | Production-03

Description	Status Checks	Monitoring	Tags
Volume ID	vol-0b498b892e4dd4f97		
Alarm status	None		
Snapshot	snap-053f10e411397204c		
Availability Zone	ap-south-1a		
Encryption	Not Encrypted		
KMS Key ID			
KMS Key Alias			
KMS Key ARN			
Throughput (MB/s)	-		
Outposts ARN	-		
Size	30 GiB		
Created	January 9, 2020 at 1:52:43 PM UTC+5:30		
State	In-use		
Attachment information	i-028c7991a2e551387 Production-03:/dev/sda1 (attached)		
Volume type	gp2		
Product codes	-		
IOPS	100		
Multi-Attach Enabled	No		

Not Encrypted

Volumes: | vol-0522d51b4dcb7ea | Production-03 |

Description	Status Checks	Monitoring	Tags
Volume ID	vol-0522d51b4dcb7ea	Outposts ARN	-
Alarm status	None	Size	250 GiB
Snapshot	snap-0501e5821a18d38	Created	January 9, 2020 at 1:52:43 PM UTC-8:30
Availability Zone	ap-southeast-1a	State	In-use
Encryption	Encrypted	Attachment information	i-029c7391a2e551387 Production-03 /dev/sdi (attached)
KMS Key ID	kms-key-007adcf5-b93c-4ab4-b69e-03ef74ef4b	Volume type	gp2
KMS Key Aliases		Product codes	-
KMS Key ARN	arn:aws:kms:ap-south-1:652916353734:key/007adcf5-b93c-4ab4-b69e-03ef74ef4b	IOPS	750
Throughput (MB/s)	-	Multi-Attach Enabled	No

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

Volumes: | vol-04b4b7a2d3860558 | (New Tableau Rev.Proxy Server-10-May-2019-21-05-2021) |

Description	Status Checks	Monitoring	Tags
Volume ID	vol-04b4b7a2d3860558	Outposts ARN	-
Alarm status	None	Size	20 GiB
Snapshot	snap-0a7a90ef2198c743	Created	January 21, 2021 at 10:38:37 PM UTC+8:30
Availability Zone	ap-south-1a	State	In-use
Encryption	Encrypted	Attachment information	i-0c154156a2988571 Linux/RevProxy-Tableau-10-May-2019 /dev/sda1 (attached)
KMS Key ID	kms-key-007adcf5-b93c-4ab4-b69e-03ef74ef4b	Volume type	gp2
KMS Key Aliases		Product codes	marketplace: 98c719b7g5u6c5antaqr1qn
KMS Key ARN	arn:aws:kms:ap-south-1:652916353734:key/007adcf5-b93c-4ab4-b69e-03ef74ef4b	IOPS	100
Throughput (MB/s)	-	Multi-Attach Enabled	No

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

Volumes: | vol-0da96ddda3f94bc2 | (Nginx-LB-Enterprise-Redhat-Production-XXY-XXZ-YYZ-ZZX-XXZ) |

Description	Status Checks	Monitoring	Tags
Volume ID	vol-0da96ddda3f94bc2	Outposts ARN	-
Alarm status	None	Size	20 GiB
Snapshot	snap-0a8650f9647c5d271	Created	September 15, 2020 at 7:18:32 PM UTC+5:30
Availability Zone	ap-south-1a	State	In-use
Encryption	Encrypted	Attachment information	i-00c846d9e09d76ee3 (Nginx-LB-Enterprise-Redhat-Production-XXY-XXZ-YYZ-ZZX-XXZ) /dev/sda1 (attached)
KMS Key ID	kms-key-007adcf5-b93c-4ab4-b69e-03ef74ef4b	Volume type	gp2
KMS Key Aliases		Product codes	marketplace: 98c719b7g5u6c5antaqr1qn
KMS Key ARN	arn:aws:kms:ap-south-1:652916353734:key/007adcf5-b93c-4ab4-b69e-03ef74ef4b	IOPS	100
Throughput (MB/s)	-	Multi-Attach Enabled	No

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

Volumes: | vol-07d9ce49f6c41c00a | (Nginx-LB-Enterprise-Redhat-Production-XXY-XXZ-YYZ-ZZX-XXZ-BackupServer) |

Description	Status Checks	Monitoring	Tags
Volume ID	vol-07d9ce49f6c41c00a	Outposts ARN	-
Alarm status	None	Size	20 GiB
Snapshot	snap-0ee1e077f96a29c2b	Created	September 15, 2020 at 7:24:53 PM UTC+5:30
Availability Zone	ap-south-1b	State	In-use
Encryption	Encrypted	Attachment information	i-071a5f6e7f40980f (Nginx-LB-Enterprise-Redhat-Production-XXY-XXZ-YYZ-ZZX-XXZ-BackupServer) /dev/sda1 (attached)
KMS Key ID	kms-key-007adcf5-b93c-4ab4-b69e-03ef74ef4b	Volume type	gp2
KMS Key Aliases		Product codes	marketplace: 98c719b7g5u6c5antaqr1qn
KMS Key ARN	arn:aws:kms:ap-south-1:652916353734:key/007adcf5-b93c-4ab4-b69e-03ef74ef4b	IOPS	100
Throughput (MB/s)	-	Multi-Attach Enabled	No

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



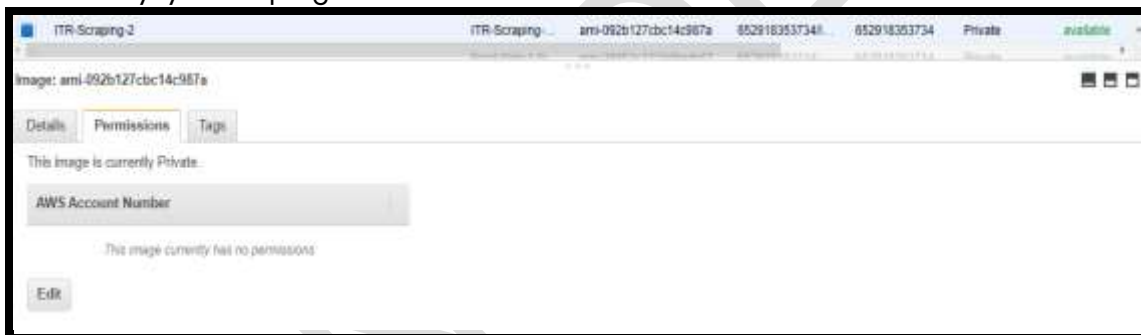
Live-RedHat-Server-Harden-OS-YYZ-NEW1-21-11-2020



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

Name	AMI Name	AMI ID	Source	Owner	Visibility	Status
		ami-037b1b2ed9853a8d1	652918353734/...	652918353734	Private	available
		ami-0334c78d0aa04c0c8	652918353734/...	652918353734	Private	available
		ami-03a012d2c8c0aa2f	652918353734/...	652918353734	Private	available
		ami-036033670b00a700	652918353734/...	652918353734	Private	available
		ami-0a3083303c9e5d183	652918353734/...	652918353734	Private	available
		ami-081da0b075902c0e9	652918353734/...	652918353734	Private	available
5-08-2020		ami-0e4853f344023b005	652918353734/...	652918353734	Private	available
20		ami-0b142b3fa5675d10f	652918353734/...	652918353734	Private	available
1-2021		ami-0e0c4a088767ac06	652918353734/...	652918353734	Private	available
2020		ami-0136e1ae752c66997f	652918353734/...	652918353734	Private	available
		ami-061061970c49eaf13	652918353734/...	652918353734	Private	available
		ami-08308c91777a77aa2	652918353734/...	652918353734	Private	available
		ami-0a25d18aa6688c47f	652918353734/...	652918353734	Private	available
		ami-0c206c769c900d7b3	652918353734/...	652918353734	Private	available
		ami-0c370e0e3e101a70e	652918353734/...	652918353734	Private	available

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

[illegible]

The screenshot shows the 'Listeners' tab in the AWS Management Console for an Amazon CloudFront distribution. The table lists the following listener configuration:

Listener ID	Security policy	SSL Certificate	Rules
HTTPS : 443 arn:aws:acm:us-east-1:123456789012:certificate/12345678-9012-3456-7890-123456789012	ELBSecurityPolicy-2015-08	Default: c5bc269-668e-4e0e-8080-bc91423bf445 (ACM) View/edit certificates	Default: forwarding to CP-External-tg View/edit rules



The screenshot shows the AWS Management Console interface for configuring a Load Balancer. The 'Listeners' tab is active, displaying a table with one listener configuration. The listener is for the 'CP-External' load balancer, using HTTPS on port 443. It is associated with the 'ELBSecurityPolicy-2016-08' security policy and a default SSL certificate. The target is set to 'CP-external-tg'.

Listener ID	Security policy	SSL Certificate	Rules
HTTPS : 443 arn:aws:acm:us-east-1:123456789012:certificate/12345678-1234-5678-9012-345678901234	ELBSecurityPolicy-2016-08	Default: c5bc269-668e-4e0e-8080-bc91423b6445 (ACM) View/edit certificates	Default: forwarding to CP-external-tg View/edit rules

The screenshot shows the 'Listeners' tab of an Amazon ElastiCache Redis instance configuration. The table lists the following listener:

Listener ID	Security policy	SSL Certificate	Rules
<input type="checkbox"/> HTTPS : 443 arn:aws:iam::7405871afdf9686f:role/...	ELBSecurityPolicy-2016-08	Default: c5cbc269-660e-4e0e-8080-bc91423f4445 (ACM) View/edit certificates	Default: forwarding to CP-External-ig-lb View/edit rules

The screenshot displays the 'Listeners' tab for the 'CP-External-ALB-prod' load balancer. A single listener is listed with the following configuration:

Listener ID	Security policy	SSL Certificate	Rules
HTTPS : 443 arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/CP-external-ALB-prod/12345678901234567890123456789012/12345678901234567890123456789012	ELBSecurityPolicy-2016-08	Default: (IAM) View/edit certificates	Default: forwarding to CP-external-tg-tag View/edit rules

Load balancer: CP-External-

Description Listeners Monitoring Integrated services Tags

A listener checks for connection requests using its configured protocol and port, and the load balancer uses the listener rules to route requests to targets. You can add, remove, or update listeners and listener rules.

[Add listener](#) [Edit](#) [Delete](#)

Listener

Listener ID	Security policy	SSL Certificate	Rules
<input type="checkbox"/> HTTPS - 443 arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/CP-External-123456789012/12345678901234567890123456789012/12345678901234567890123456789012	ELBSecurityPolicy-2016-08	Default: c9dbc2b9-668e-4e0e-8000-bc91423b4445 (ACM) View/edit certificates	Default: forwarding to CP-External View/edit rules



The screenshot shows the AWS Management Console interface for configuring a Load Balancer. The 'Listeners' tab is selected, displaying a table with one listener configuration. The listener is for HTTPS on port 443, using the 'ELBSecurityPolicy-2016-08' security policy and the 'Default' SSL certificate. The target group is 'Default' and the target type is 'Instance'.

Listener ID	Security policy	SSL Certificate	Rules
HTTPS : 443 arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/my-load-balancer/50dc6c49-6ba0-40a6-83d0-d6de83c1b351/-	ELBSecurityPolicy-2016-08	Default View/edit certificates	Default: forwarding to View/edit rules

The screenshot displays the AWS Management Console interface for configuring a Load Balancer. The 'Listeners' tab is active, showing a table with one listener configuration. The listener is for HTTPS on port 443, using the 'ELBSecurityPolicy-2016-08' security policy and the 'Default' SSL certificate. The rules are set to 'Default: forwarding to'.

Listener ID	Security policy	SSL Certificate	Rules
HTTPS : 443 arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/elasticloadbalancing:us-east-1:123456789012:listener-arn	ELBSecurityPolicy-2016-08	Default: c9bc269-668e-4e9b-8080-bc91423bf445 (ACM) View/edit certificates	Default: forwarding to View/edit rules

CP-internal-ALB internal-CP-internal active vpc-0083f5abd4470c82 ap-south-1a, ap-south-1b application

Load balancer: CP-internal-ALB-nginx-B01

Description Listeners Monitoring Integrated services Tags

A listener checks for connection requests using its configured protocol and port, and the load balancer uses the listener rules to route requests to targets. You can add, remove, or update listeners and listener rules.

[Add listener](#) [Edit](#) [Delete](#)

Listener

Listener ID	Security policy	SSL Certificate	Rules
HTTPS : 443 arn:aws:elasticloadbalancing:ap-south-1:111111111111:listener/application/CP-internal-ALB/nginx-B01/arn:aws:elasticloadbalancing:ap-south-1:111111111111:listener/application/CP-internal-ALB/nginx-B01	ELBSecurityPolicy-2016-08	Default: 616e093c-9c79-49ca-b6e7-2181046d6d71 (ACM) View/edit certificates	Default: forwarding to arn:aws:elasticloadbalancing:ap-south-1:111111111111:targetgroup/application/CP-internal-ALB/nginx-B01/arn:aws:elasticloadbalancing:ap-south-1:111111111111:targetgroup/application/CP-internal-ALB/nginx-B01 View/edit rules

CP-internal-ALB internal-CP-internal active vpc-0083f5abd4470c82 ap-south-1a, ap-south-1b application

Load balancer: CP-internal

Description Listeners Monitoring Integrated services Tags

A listener checks for connection requests using its configured protocol and port, and the load balancer uses the listener rules to route requests to targets. You can add, remove, or update listeners and listener rules.

[Add listener](#) [Edit](#) [Delete](#)

Listener

Listener ID	Security policy	SSL Certificate	Rules
HTTPS : 443 arn:aws:elasticloadbalancing:ap-south-1:111111111111:listener/application/CP-internal/nginx-B01/arn:aws:elasticloadbalancing:ap-south-1:111111111111:listener/application/CP-internal/nginx-B01	ELBSecurityPolicy-2016-08	Default: c9bc269-668e-4e0e-8080-bc91423b6445 (ACM) View/edit certificates	Default: forwarding to arn:aws:elasticloadbalancing:ap-south-1:111111111111:targetgroup/application/CP-internal/nginx-B01/arn:aws:elasticloadbalancing:ap-south-1:111111111111:targetgroup/application/CP-internal/nginx-B01 View/edit rules

CP-internal-ALB internal-CP-internal active vpc-0083f5abd4470c82 ap-south-1a, ap-south-1b application

Load balancer: CP-internal-ALB

Description Listeners Monitoring Integrated services Tags

A listener checks for connection requests using its configured protocol and port, and the load balancer uses the listener rules to route requests to targets. You can add, remove, or update listeners and listener rules.

[Add listener](#) [Edit](#) [Delete](#)

Listener

Listener ID	Security policy	SSL Certificate	Rules
HTTPS : 443 arn:aws:elasticloadbalancing:ap-south-1:111111111111:listener/application/CP-internal-ALB/nginx-B01/arn:aws:elasticloadbalancing:ap-south-1:111111111111:listener/application/CP-internal-ALB/nginx-B01	ELBSecurityPolicy-2016-08	Default: c9bc269-668e-4e0e-8080-bc91423b6445 (ACM) View/edit certificates	Default: forwarding to arn:aws:elasticloadbalancing:ap-south-1:111111111111:targetgroup/application/CP-internal-ALB/nginx-B01/arn:aws:elasticloadbalancing:ap-south-1:111111111111:targetgroup/application/CP-internal-ALB/nginx-B01 View/edit rules

CP-internal internal-CP-internal active vpc-0083f5abd4470c82 ap-south-1a, ap-south-1b application

Load balancer: CP-internal

Description Listeners Monitoring Integrated services Tags

A listener checks for connection requests using its configured protocol and port, and the load balancer uses the listener rules to route requests to targets. You can add, remove, or update listeners and listener rules.

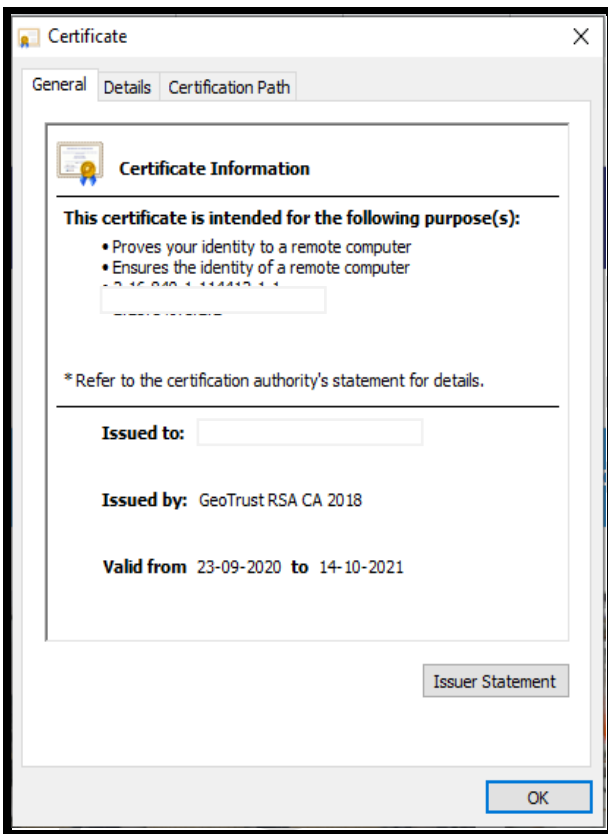
[Add listener](#) [Edit](#) [Delete](#)

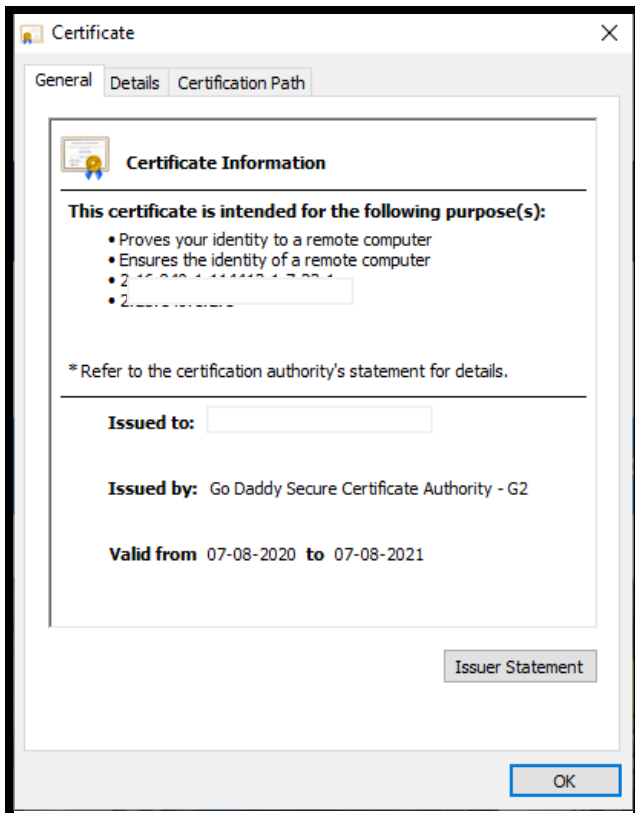
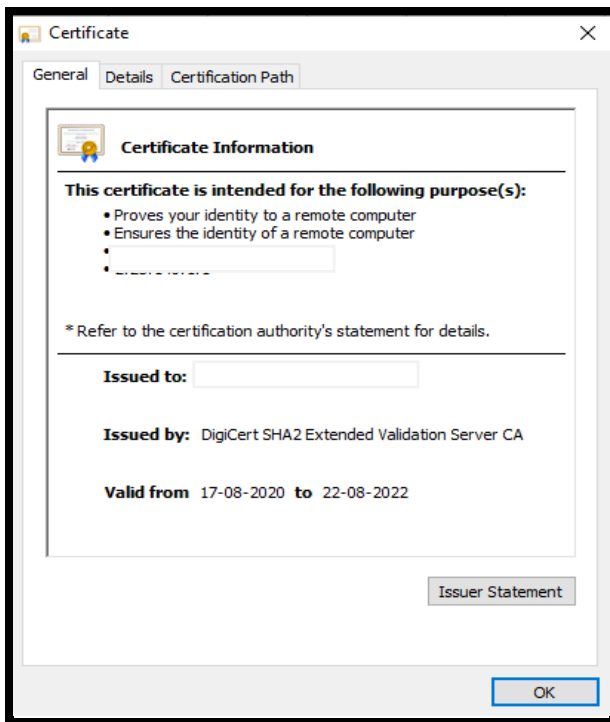
Listener

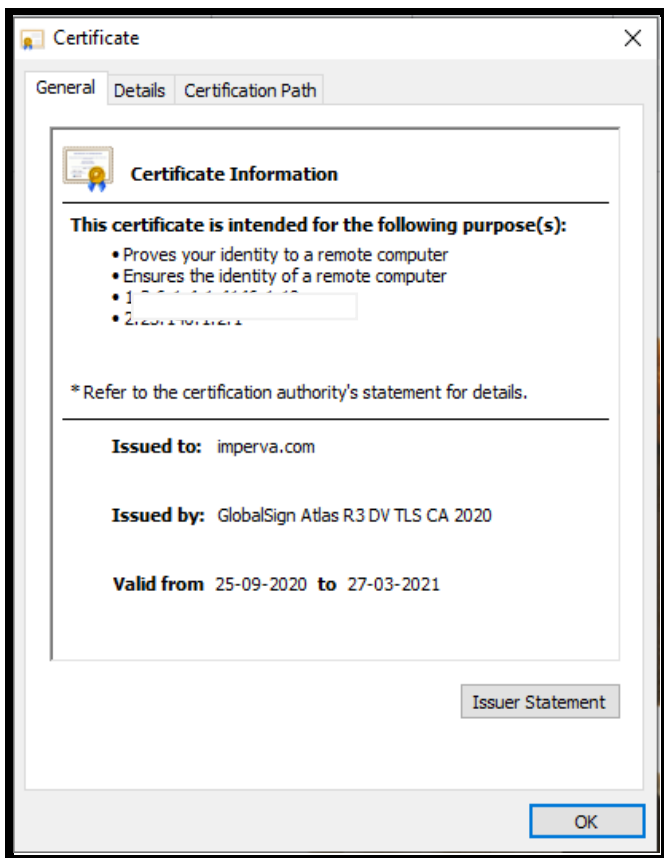
Listener ID	Security policy	SSL Certificate	Rules
HTTPS : 443 arn:aws:elasticloadbalancing:ap-south-1:111111111111:listener/application/CP-internal/nginx-B01/arn:aws:elasticloadbalancing:ap-south-1:111111111111:listener/application/CP-internal/nginx-B01	ELBSecurityPolicy-2016-08	Default: 106f081f-e6b3-458f-b666-17717760d076 (ACM) View/edit certificates	Default: forwarding to arn:aws:elasticloadbalancing:ap-south-1:111111111111:targetgroup/application/CP-internal/nginx-B01/arn:aws:elasticloadbalancing:ap-south-1:111111111111:targetgroup/application/CP-internal/nginx-B01 View/edit rules

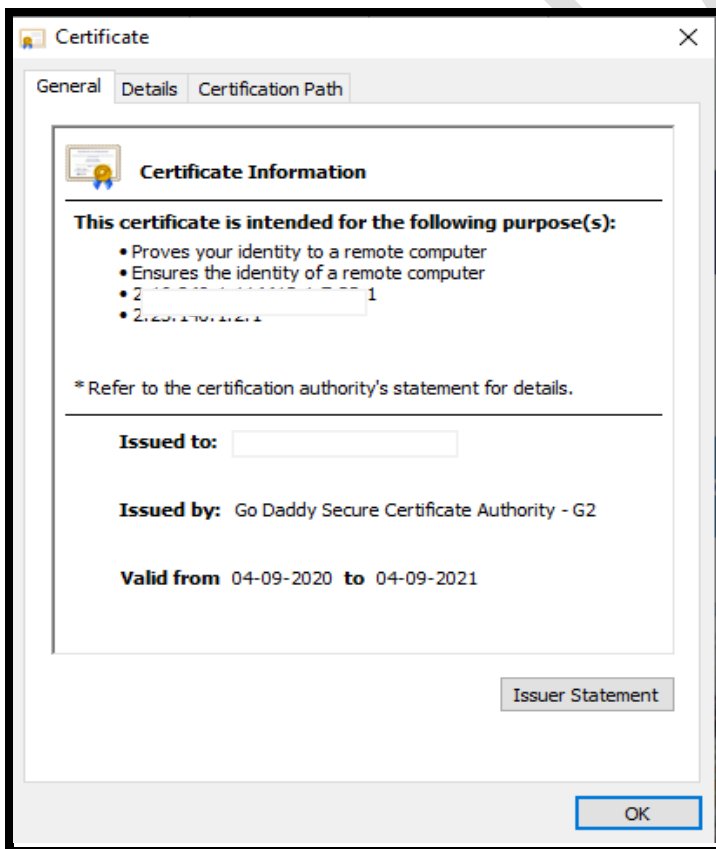


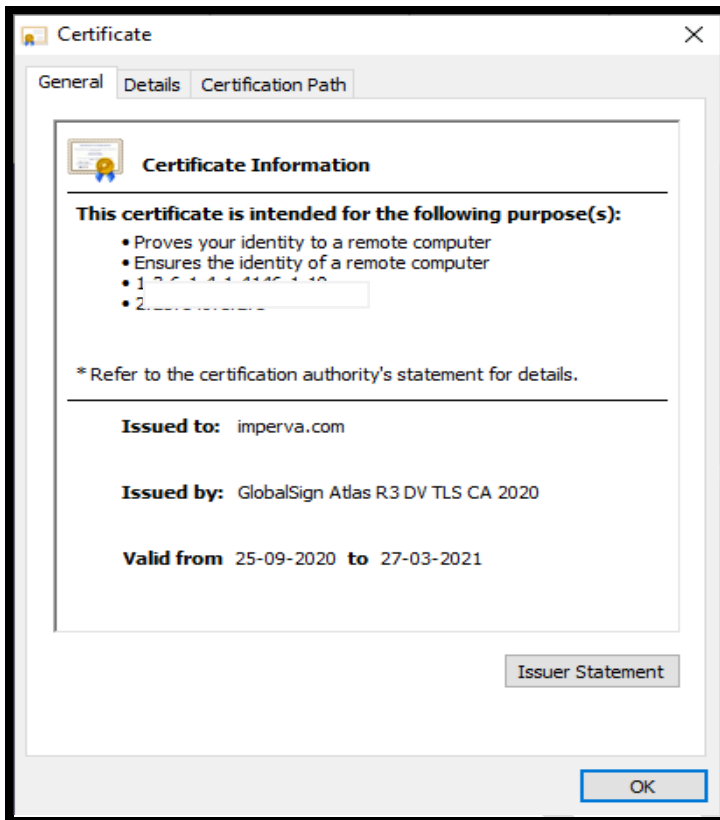
1.15 Ensure all public web-tier SSL/TLS certificates are >30 days from expiration











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)

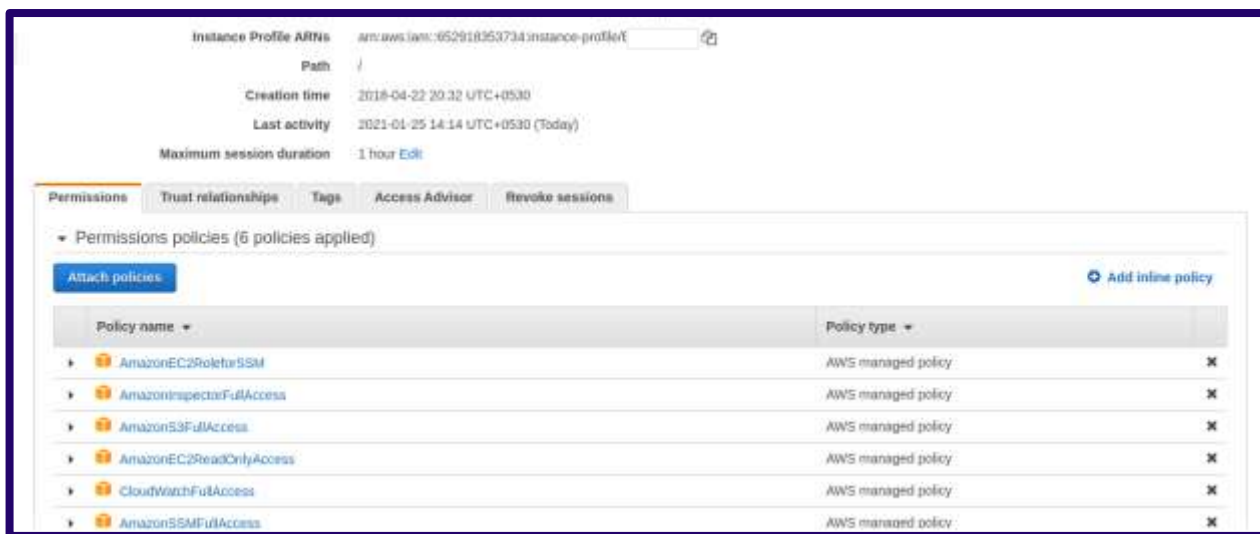
2 Identity and Access Management

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

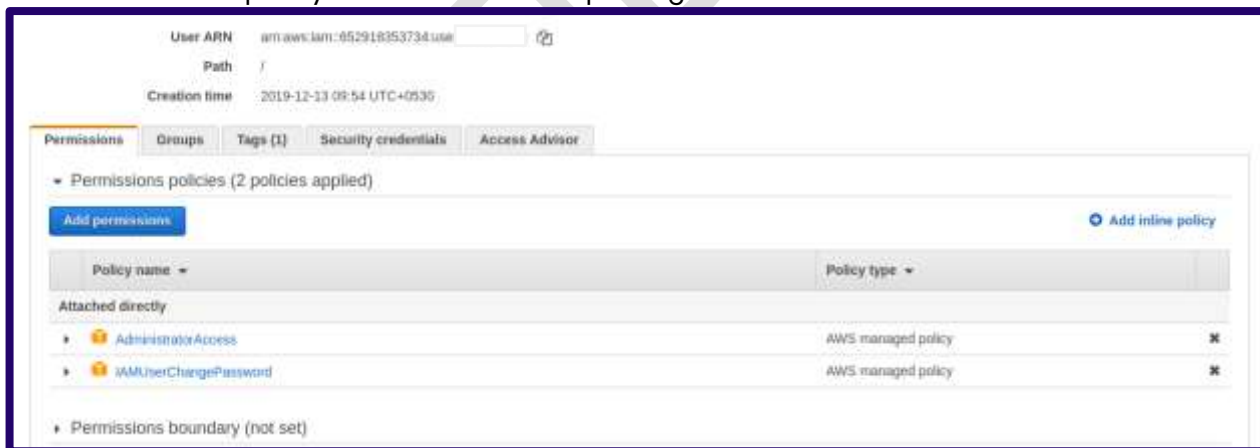


2.5 Ensure AutoScaling Group Launch Configuration for Web Tier is configured to use a customer created Web-Tier IAM Role / 2.6 Ensure AutoScaling Group Launch Configuration for App Tier is configured to use an App-Tier IAM Role. Not Applicable

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-1:652918353734:*****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-1:652918353734:*****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/(redacted) 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

Load balancing

Load balancer target groups

Classic Load Balancers

-

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

Check-Point-Security-Gateway-Autoscaling

Network

Edit

Availability Zones

ap-south-1b, ap-south-1a

Subnet ID

subnet-0ad5629333795ce77, subnet-0772a981ae5939878

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

Launch configuration

Edit

Launch configuration

Check-Point-Security-Gateway-AutoScaling-ALLBANKS-LaunchConfig-PSZ8XU7TG15M

AMI ID

ami-07731e7c68fd774b8

Security groups

[sg-0f3783d02159118b3](#)

Instance type

c5.xlarge

Key pair name


CheckPoint-Prod

Create time


Sat Sep 05 2020 20:26:42 GMT+0530 (India Standard Time)

3.5 Ensure Relational Database Service is Multi-AZ Enabled

prod-xyz-v2

Instance			
Configuration	Instance class	Storage	Performance Insights
DB instance id prod- <input type="text"/>	Instance class db.r5.4xlarge	Encryption Enabled	Performance Insights enabled No
Engine version 5.7.23	vCPU 16	KMS key a52c3ad3-36b0-4381-9ff5-bb274e89d913 	Published logs
DB name QA <input type="text"/>	RAM 128 GB	Storage type Provisioned IOPS (SSD)	CloudWatch Logs
License model General Public License	Availability	IOPS 2500	Audit
Option groups prc <input type="text"/>	Master username <input type="text"/>	Storage 2400 GiB	Error
Amazon Resource Name (ARN) arn:aws:rds:ap-south-1:652918353734:db:pi- <input type="text"/> v2	IAM db authentication Enabled	Storage autoscaling Disabled	General
	Multi AZ Yes		Slow query

prod-yyz

Instance			
Configuration	Instance class	Storage	Performance Insights
DB instance id <input type="text"/>	Instance class db.r5.xlarge	Encryption Enabled	Performance Insights enabled No
Engine version 5.7.23	vCPU 4	KMS key a52c3ad3-36b0-4381-9ff5-bb274e89d913 	Published logs
DB name -	RAM 32 GB	Storage type Provisioned IOPS (SSD)	CloudWatch Logs
License model General Public License	Availability	IOPS 1000	Audit
Option groups prc <input type="text"/>	Master username <input type="text"/>	Storage 300 GiB	Error
Amazon Resource Name (ARN) arn:aws:rds:ap-south-1:652918353734:db:pr- <input type="text"/>	IAM db authentication Enabled	Storage autoscaling Disabled	General
	Multi AZ No		Slow query

ABCD-prod

Instance			
Configuration DB instance id <input type="text" value="i-"/> Engine version 5.7.26 DB name Q/ <input type="text" value=""/> License model General Public License Option groups pn <input type="text" value=""/> Amazon Resource Name (ARN) arn:aws:rds:ap-south-1:652918353734:db:	Instance class Instance class db.r5.xlarge vCPU 4 RAM 32 GiB Availability Master username <input type="text" value=""/> IAM db authentication Enabled Multi AZ No	Storage Encryption Enabled KMS key a52c3ad3-36b0-4381-9ff5-bb274e89d913 🔗 Storage type Provisioned IOPS (SSD) IOPS 1000 Storage 200 GiB Storage autoscaling Disabled	Performance Insights Performance Insights enabled No Published logs CloudWatch Logs Audit Error General Slow query

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

prod-xyz-v2

prod-1

Modify

Actions

Summary

DB identifier prod-1	CPU <div><div></div></div> 12.00%	Status Available	Class db.r5.4xlarge
Role Instance	Current activity <div><div></div></div> 10212 Connections	Engine MySQL Community	Region & AZ ap-south-1a

Connectivity & security

Monitoring

Logs & events

Configuration

Maintenance & backups

Tags

Maintenance

Auto minor version upgrade Disabled	Maintenance window tue:06:31-tue:07:01 UTC (GMT)	Pending maintenance none	Pending modifications
---	---	-----------------------------	-----------------------

prod-yyz

prod-

Modify

Actions ▾

Summary

DB identifier prod	CPU <div></div> 4.00%	Status <div>Available</div>	Class db.r5.xlarge
Role Instance	Current activity <div></div> 2145 Connections	Engine MySQL Community	Region & AZ ap-south-1b

Connectivity & security

Monitoring

Logs & events

Configuration

Maintenance & backups

Tags

Maintenance

Auto minor version upgrade Disabled	Maintenance window thu:11:51-thu:12:21 UTC (GMT)	Pending maintenance none	Pending modifications
--	---	-----------------------------	-----------------------

ABCD-prod

ABCD-prod

Modify

Actions ▾

Summary

DB identifier mfi-prod	CPU <div></div> 2.00%	Status <div>Available</div>	Class db.r5.xlarge
Role Instance	Current activity <div></div> 1058 Connections	Engine MySQL Community	Region & AZ ap-south-1a

Connectivity & security

Monitoring

Logs & events

Configuration

Maintenance & backups

Tags

Maintenance

Auto minor version upgrade Disabled	Maintenance window tue:06:31-tue:07:01 UTC (GMT)	Pending maintenance none	Pending modifications
--	---	-----------------------------	-----------------------

3.8 Ensure Relational Database Service backup retention policy is set

Prod-xyz-v2

Backup	
Automated backups Enabled (7 Days)	Latest restore time January 8th 2021, 11:55:00 am UTC
Copy tags to snapshots Enabled	Backup window 18:23-18:53 UTC (GMT)

Prod-yyz

Backup	
Automated backups Enabled (7 Days)	Latest restore time January 8th 2021, 12:00:00 pm UTC
Copy tags to snapshots Enabled	Backup window 00:00-00:30 UTC (GMT)

ABCD-prod

Backup	
Automated backups Enabled (7 Days)	Latest restore time January 8th 2021, 12:00:00 pm UTC
Copy tags to snapshots Enabled	Backup window 18:23-18:53 UTC (GMT)

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

Basic configuration

Target type IP	Protocol : Port HTTPS : 9443 Protocol version HTTP1	VPC vpc-0083f5abd4f470c82	Load balancer External-ALB
-------------------	--	------------------------------	-------------------------------

Group details

Targets

Monitoring

Tags

Health check settings

Protocol
HTTPS
Port
traffic-port
Unhealthy threshold
2 consecutive health check failures
Interval
30 seconds

Path
/index.html
Healthy threshold
5 consecutive health check successes
Timeout
5 seconds
Success codes
200

Edit

CP-External-ALB-ABC

Basic configuration

Target type Instance	Protocol : Port HTTPS : 9468 Protocol version HTTP1	VPC vpc-0083f5abd4f470c82	Load balancer CP-External
-------------------------	--	------------------------------	------------------------------

Group details

Targets

Monitoring

Tags

Health check settings

Protocol
HTTPS
Port
443
Unhealthy threshold
2 consecutive health check failures
Interval
30 seconds

Path
/
Healthy threshold
5 consecutive health check successes
Timeout
5 seconds
Success codes
200-499

Edit

CP-External-ALB-prod-yyz

Basic configuration

Target type

Instance

Protocol : Port

HTTPS : 9465

Protocol version

HTTP1

VPC

vpc-0083f5abd4ff470c82

Load balancer

CP-External-ALB

Group details

Targets

Monitoring

Tags

Health check settings

Edit

Protocol

HTTPS

Port

443

Unhealthy threshold

2 consecutive health check failures

Interval

30 seconds

Path

/

Healthy threshold

5 consecutive health check successes

Timeout

5 seconds

Success codes

200-499

CP-External-ALB-CBI

Basic configuration

Target type

Instance

Protocol : Port

HTTPS : 9467

Protocol version

HTTP1

VPC

vpc-0083f5abd4ff470c82

Load balancer

CP-External

Group details

Targets

Monitoring

Tags

Health check settings

Edit

Protocol

HTTPS

Port

443

Unhealthy threshold

2 consecutive health check failures

Interval

30 seconds

Path

/

Healthy threshold

5 consecutive health check successes

Timeout

5 seconds

Success codes

200-499

CP-External-ALB-Prod

Basic configuration

Target type

Instance

Protocol : Port

HTTPS : 9470

Protocol version

HTTP1

VPC

vpc-0083f5abd4f470c82

Load balancer

CP-External-

Group details

Targets

Monitoring

Tags

Health check settings

Edit

Protocol

HTTPS

Port

443

Unhealthy threshold

2 consecutive health check failures

Interval

30 seconds

Path

/

Healthy threshold

5 consecutive health check successes

Timeout

5 seconds

Success codes

200-499

CP-External-ALB-XXY

Basic configuration

Target type

Instance

Protocol : Port

HTTPS : 9469

Protocol version

HTTP1

VPC

vpc-0083f5abd4f470c82

Load balancer

CP-External-

Group details

Targets

Monitoring

Tags

Health check settings

Edit

Protocol

HTTPS

Port

443

Unhealthy threshold

2 consecutive health check failures

Interval

30 seconds

Path

/

Healthy threshold

5 consecutive health check successes

Timeout

5 seconds

Success codes

200-499

CP-internal-ALB-YYZ

Basic configuration

Target type

instance

Protocol : Port

HTTP : 8383

Protocol version

HTTP1

VPC

vpc-0083f5abdc4f470c83

Load balancer

CP-internal-

Group details

Targets

Monitoring

Tags

Health check settings

Edit

Protocol

HTTP

Port

8080

Unhealthy threshold

2 consecutive health check failures

Interval

30 seconds

Path

/

Healthy threshold

5 consecutive health check successes

Timeout

5 seconds

Success codes

200

CP-internal-ALB-nginx-ABC

Basic configuration

Target type

instance

Protocol : Port

HTTP : 80

Protocol version

HTTP1

VPC

vpc-0083f5abdc4f470c83

Load balancer

CP-internal-ALB

Group details

Targets

Monitoring

Tags

Health check settings

Edit

Protocol

HTTP

Port

traffic-port

Unhealthy threshold

2 consecutive health check failures

Interval

30 seconds

Path

/

Healthy threshold

5 consecutive health check successes

Timeout

5 seconds

Success codes

200

CP-internal-ALB-CI

Basic configuration

Target type

Instance

Protocol : Port

HTTP : 80

Protocol version

HTTP1

VPC

vpc-0083f5abd4f470c82

Load balancer

CP-internal-

Group details

Targets

Monitoring

Tags

Health check settings

Edit

Protocol

HTTP

Path

/

Port

traffic-port

Healthy threshold

5 consecutive health check successes

Unhealthy threshold

2 consecutive health check failures

Timeout

5 seconds

Interval

30 seconds

Success codes

200

CP-internal-ALB-nginx-XXY

Basic configuration

Target type

Instance

Protocol : Port

HTTP : 80

Protocol version

HTTP1

VPC

vpc-0083f5abd4f470c82

Load balancer

CP-internal-ALB-

Group details

Targets

Monitoring

Tags

Health check settings

Edit

Protocol

HTTP

Path

/

Port

traffic-port

Healthy threshold

5 consecutive health check successes

Unhealthy threshold

2 consecutive health check failures

Timeout

5 seconds

Interval

30 seconds

Success codes

200

CP-internal-ELB

Basic configuration

Target type

Instance

Protocol / Port

HTTP : 9294

Protocol version

HTTP1

VPC

vpc-0083f5abd4f470c82

Load balancer

CP-internal

Group details

Targets

Monitoring

Tags

Health check settings

Edit

Protocol

HTTP

Port

8080

Unhealthy threshold

2 consecutive health check failures

Interval

30 seconds

Path

/

Healthy threshold

5 consecutive health check successes

Timeout

5 seconds

Success codes

200

CP-internal-ALB-XXY

Basic configuration

Target type

Instance

Protocol / Port

HTTP : 8792

Protocol version

HTTP1

VPC

vpc-0083f5abd4f470c82

Load balancer

CP-internal

Group details

Targets

Monitoring

Tags

Health check settings

Edit

Protocol

HTTP

Port

8080

Unhealthy threshold

2 consecutive health check failures

Interval

30 seconds

Path

/

Healthy threshold

5 consecutive health check successes

Timeout

5 seconds

Success codes

200

CP-internal-ALB-nginx-XXY

Basic configuration

Target type

Instance

Protocol : Port

HTTP : 80

Protocol version

HTTP1

VPC

vpc-008375ab04f470c82

Load balancer

CP-internal-A1B-

Group details

Targets

Monitoring

Tags

Health check settings

Edit

Protocol

HTTP

Port

traffic-port

Unhealthy threshold

2 consecutive health check failures

Interval

30 seconds

Path

/

Healthy threshold

5 consecutive health check successes

Timeout

5 seconds

Success codes

200

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

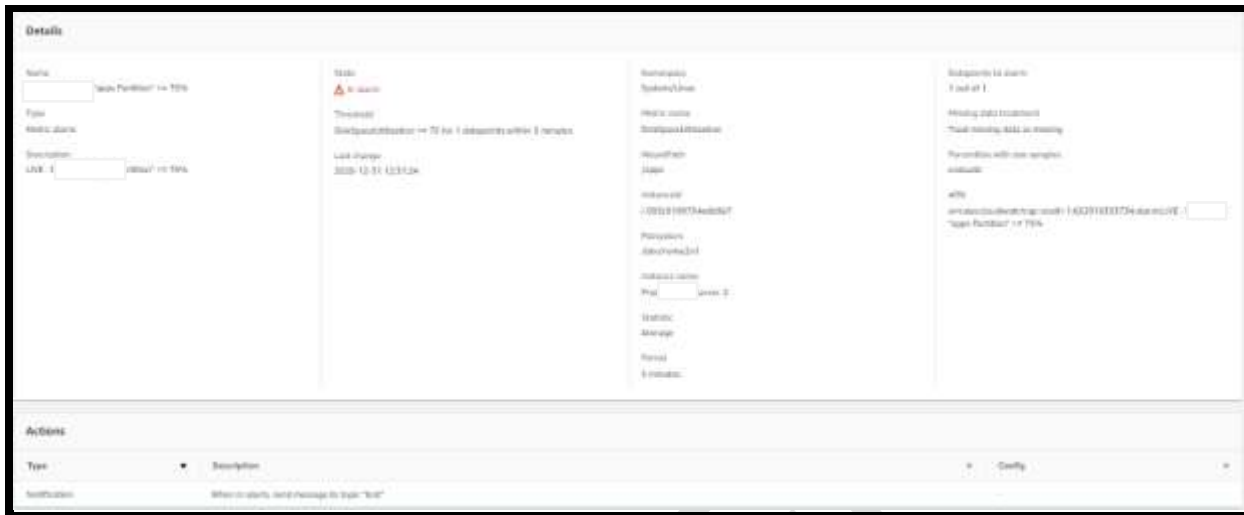
Load balancing

Classic Load Balancers

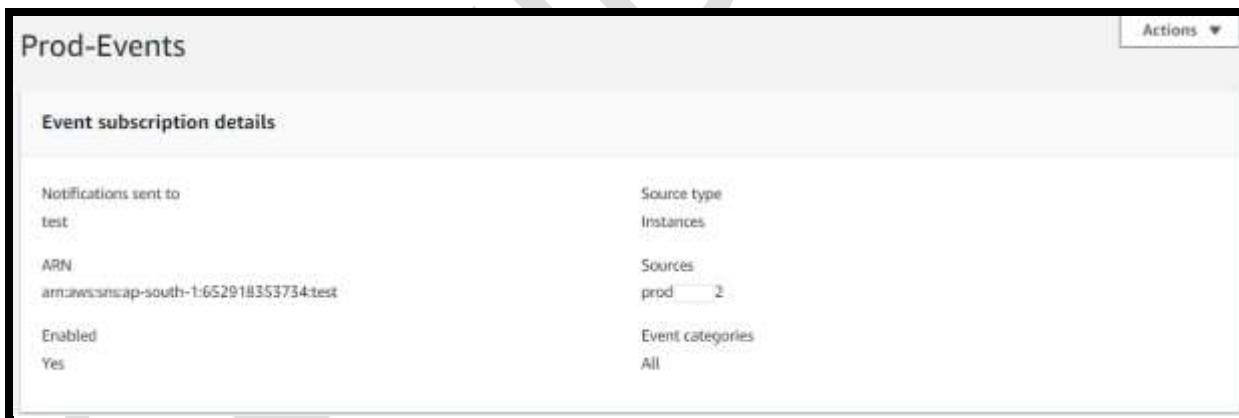
-

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

The screenshot shows the AWS CloudWatch 'Metric filters' page. The 'Metric filters (4)' section is active. Two filters are listed:

- MyAppErrorCount-eni-000e69e8e28fe00b6**: Filter pattern 'Error', Metric 'MyNamespace-eni-000e69e8e28fe00b6 / ErrorCount', Metric value '1', Default value '0', Alarms 'ErrorCount-eni-000e69e8e28fe00b6'.
- MyAppErrorCount-eni-061f44c004cb23c1a**: Filter pattern 'Error', Metric 'MyNamespace-eni-061f44c004cb23c1a / ErrorCount', Metric value '1', Default value '0', Alarms 'ErrorCount-eni-061f44c004cb23c1a'.

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

The screenshot shows the 'Tags' tab for AWS instance 'i-078c6d596das7a14a (Prod-Server-1)'. The tags are:

Key	Value
Name	Prod-Server-1
CostCenter	Billing
Environment	Production

The screenshot shows the 'Tags' tab for AWS instance 'i-093c9199734edb9b7 (Prod-Server-2)'. The tags are:

Key	Value
Name	Prod-Server-2
CostCenter	Billing
Environment	Production

Instance: i-05ad2448fd50d5584 i-ve-Production-02

Details | Security | Networking | Storage | Status Checks | Monitoring | **Tags**

Tags

Manage tags

1

Key	Value
Cost Center	Billing
Name	i-Production-02
Environment	Production

Instance: i-0d1712b0c5ce50a7 i-scraping-server-01

Details | Security | Networking | Storage | Status Checks | Monitoring | **Tags**

Tags

Manage tags

1

Key	Value
Name	i-scraping-server-01
ID	Live
Cost Center	Billing
Environment	Production

Instance: i-0f6c6882e61172463 (Live-RedHat-Server)

Details | Security | Networking | Storage | Status Checks | Monitoring | **Tags**

Tags

Manage tags

1

Key	Value
Name	Live-RedHat-Server-Harden
Cost Center	Billing
Environment	Production

Instance: i-0450df9e5909e8b3 (Admin-panel-Instance)

Details | Security | Networking | Storage | Status Checks | Monitoring | **Tags**

Tags

Manage tags

1

Key	Value
Name	Admin-panel-Instance

Instance: i-00c846dae69d76ee3 (Nginx-LB-Enterprise-Redhat-Production)

Details | Security | Networking | Storage | Status Checks | Monitoring | **Tags**

Tags

Manage tags

1

Key	Value
Environment	Production
Name	Nginx-LB-Enterprise-Redhat-Production
Cost Center	Billing

5.2 Ensure AWS Elastic Load Balancer logging is enabled



The screenshot displays the configuration page for an Elastic Load Balancing (ELB) instance named 'CP-External-ALB'. The instance is in an 'active' state. Key configuration details include:

- VPC:** vpc-3083f5a0a4470a62
- Availability Zones:**
 - subnet-23f052243547782d - ap-south-1a
 - subnet-2a3b3aee15af132b - ap-south-1a
- Hosted zone:** ZP9TRAPLX7N2K
- Creation time:** March 15, 2019 at 11:23:38 PM UTC+5:30
- Security groups:** sg-201f8ad55d1248aa, CP-Prod-External-ELB
- Attributes:**
 - Deletion protection: Enabled
 - Idle timeout: 200 seconds
 - HTTP2: Enabled
 - Deny on mitigation mode: Defensive
 - Drop invalid header fields: Disabled
 - Access logs: S3 location: checkpoint-external-elb-logs



The screenshot displays the configuration page for an Elastic Load Balancing (ELB) instance named 'CP-External-ALB'. The instance is in an 'active' state. Key configuration details include:

- VPC:** vpc-3083f5a0a4470a62
- Availability Zones:**
 - subnet-23f052243547782d - ap-south-1a
 - subnet-2a3b3aee15af132b - ap-south-1a
- Hosted zone:** ZP9TRAPLX7N2K
- Creation time:** September 12, 2020 at 12:04:55 PM UTC+5:30
- Security groups:** sg-2120b8c3a75ef187, checkpoint-testing-sg, checkpoint-testing-sg-01-05-2020
- Attributes:**
 - Deletion protection: Enabled
 - Idle timeout: 200 seconds
 - HTTP2: Enabled
 - Deny on mitigation mode: Defensive
 - Drop invalid header fields: Disabled
 - Access logs: S3 location: cp-external-elb-logs



The screenshot displays the configuration page for an Elastic Load Balancing (ELB) instance named 'CP-External-ALB'. The instance is in an 'active' state. Key configuration details include:

- VPC:** vpc-3083f5a0a4470a62
- Availability Zones:**
 - subnet-23f052243547782d - ap-south-1a
 - subnet-2a3b3aee15af132b - ap-south-1a
- Hosted zone:** ZP9TRAPLX7N2K
- Creation time:** September 10, 2020 at 9:45:37 PM UTC+5:30
- Security groups:** sg-2120b8c3a75ef187, checkpoint-testing-sg, checkpoint-testing-sg-01-05-2020
- Attributes:**
 - Deletion protection: Enabled
 - Idle timeout: 200 seconds
 - HTTP2: Enabled
 - Deny on mitigation mode: Defensive
 - Drop invalid header fields: Disabled
 - Access logs: S3 location: cp-external-elb-logs

CP-External

CP-External

active

vpc-0003f5a04470a82

ap-south-1a, ap-south-1a

application

August 9, 2020 at 11:48:57

VPC: vpc-0003f5a04470a82

Availability Zones: subnet-0098e2240047792d - ap-south-1a
IPv4 address: Assigned by AWS
subnet-0d6cf0bae15af038 - ap-south-1a
IPv4 address: Assigned by AWS
Edit subnets

Hosted zone: ZP67RAFLXTH2K

Creation time: August 9, 2020 at 11:48:57 PM UTC+5:30

Security

Security groups: sg-01308e03a75af187, checkpoint-testing-sg
checkpoint-testing-sg-01-08-2020
Edit security groups

Attributes

Deletion protection: Enabled

Idle timeout: 1200 seconds

HTTP2: Enabled

Default mitigation mode: Defensive

Drop invalid header fields: Disabled

Access logs: S3 location cp-4 -prod/

CP-External-AU

CP-External-AUS

active

vpc-0003f5a04470a82

ap-south-1a, ap-south-1a

application

August 31, 2020 at 2:23:15

VPC: vpc-0003f5a04470a82

Availability Zones: subnet-0098e2240047792d - ap-south-1a
IPv4 address: Assigned by AWS
subnet-0d6cf0bae15af038 - ap-south-1a
IPv4 address: Assigned by AWS
Edit subnets

Hosted zone: ZP67RAFLXTH2K

Creation time: August 31, 2020 at 2:23:15 PM UTC+5:30

Security

Security groups: sg-01308e03a75af187, checkpoint-testing-sg
checkpoint-testing-sg-01-08-2020
Edit security groups

Attributes

Deletion protection: Enabled

Idle timeout: 1200 seconds

HTTP2: Enabled

Default mitigation mode: Defensive

Drop invalid header fields: Disabled

Access logs: S3 location cp-external-aus-prod-bob/

CP-External CP-External 000... active vpc-0083f5abd4f470c82 ap-south-1b, ap-south-1a application September 12, 2020 at 10:1...

VPC vpc-0083f5abd4f470c82 [🔗](#)

Availability Zones

- subnet-03f0522400d7792d - ap-south-1b [🔗](#)
IPv4 address: Assigned by AWS
- subnet-0b8cfbbee15af5308 - ap-south-1a [🔗](#)
IPv4 address: Assigned by AWS

[Edit subnets](#)

Hosted zone ZP8TRAPLXTN2K

Creation time September 12, 2020 at 10:10 PM UTC+5:30

Security

Security groups sg-01308a0f3a75af157, checkpoint-testing-sg, checkpoint-testing-sg-01-08-2020

[Edit security groups](#)

Attributes

Deletion protection	Enabled
Idle timeout	300 seconds
HTTP2	Enabled
Drain mitigation mode	Defense
Drop invalid header fields	Disabled
Access logs	S3 location cp-external-2019 /

CP-External CP-External afea3f... active vpc-0083f5abd4f470c82 ap-south-1b, ap-south-1a network May 1, 2019 at 3:18:33 PM ...

DNS name CP-External-2 b2afea3f238b46.elb.ap-south-1.amazonaws.com [🔗](#)
(A Record)

State active

Type network

Scheme internet-facing

IP address type ipv4

[Edit IP address type](#)

VPC vpc-0083f5abd4f470c82 [🔗](#)

Availability Zones

- subnet-03f0522400d7792d - ap-south-1b [🔗](#)
IPv4 address: Assigned by AWS
- subnet-0b8cfbbee15af5308 - ap-south-1a [🔗](#)
IPv4 address: Assigned by AWS

[Edit subnets](#)

Hosted zone ZVDDR8Q08TROA

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 /

CP-internal-CP-internal-CP-internal active vpc-0003f5e0d4470c82 ap-south-1a, ap-south-1b application September 3, 2020 at 7:55:11 PM UTC+5:30

VPC vpc-0003f5e0d4470c82

Availability Zones

- subnet-03895b0c33e6cc7bc - ap-south-1a
 - IPv4 address: Assigned from CIDR 10.0.20.0/24
- subnet-0e6b1739828395dc1 - ap-south-1b
 - IPv4 address: Assigned from CIDR 10.0.21.0/24

Edit subnets

Hosted zone ZP6T8APLXTH2K

Creation time September 3, 2020 at 7:55:11 PM UTC+5:30

Security

Security groups sg-01ee4075e24e2d0, Check-Point-Gateway
+ Security Gateway for

Edit security groups

Attributes

- Deletion protection Enabled
- Idle timeout 200 seconds
- HTTP2 Enabled
- Drayco mitigation mode Defensive
- Drop invalid header fields Disabled
- Access logs S3 location cp-internal-als-kob/

CP-internal-CP-internal-CP-internal active vpc-0003f5e0d4470c82 ap-south-1a, ap-south-1b application September 4, 2020 at 7:18:23 PM UTC+5:30

VPC vpc-0003f5e0d4470c82

Availability Zones

- subnet-03895b0c33e6cc7bc - ap-south-1a
 - IPv4 address: Assigned from CIDR 10.0.20.0/24
- subnet-0e6b1739828395dc1 - ap-south-1b
 - IPv4 address: 10.0.21.0/24

Edit subnets

Hosted zone ZP6T8APLXTH2K

Creation time September 4, 2020 at 7:18:23 PM UTC+5:30

Security

Security groups sg-0c0b006aa348c95e, Check-Point-Gateway
+ Check-Point-Gateway for central bank of India

Edit security groups

Attributes

- Deletion protection Enabled
- Idle timeout 200 seconds
- HTTP2 Enabled
- Drayco mitigation mode Defensive
- Drop invalid header fields Disabled
- Access logs S3 location checkpoint-naw-in/ (00-0000)

CP-internal-ALB-CP-internal-CP-internal active vpc-0003f5e0d4470c82 ap-south-1a, ap-south-1b application September 12, 2020 at 9:50:28 PM UTC+5:30

VPC vpc-0003f5e0d4470c82

Availability Zones

- subnet-03895b0c33e6cc7bc - ap-south-1a
 - IPv4 address: Assigned from
- subnet-0e6b1739828395dc1 - ap-south-1b
 - IPv4 address: Assigned from

Edit subnets

Hosted zone ZP6T8APLXTH2K

Creation time September 12, 2020 at 9:50:28 PM UTC+5:30

Security

Security groups sg-2a4c294ac2813293, Check-Point-Gateway-B
+ Check-Point-Gateway for Group

Edit security groups

Attributes

- Deletion protection Enabled
- Idle timeout 200 seconds
- HTTP2 Enabled
- Drayco mitigation mode Defensive
- Drop invalid header fields Disabled
- Access logs S3 location cp-internal

CP-internal

Internal-CP-internal active vpc-0003f5a0c447b0d2 ap-south-1a ap-south-1b Application September 15, 2020 at 7:05

VPC vpc-0003f5a0c447b0d2 [\[?\]](#)

Availability Zones

subnet-020555c03b6c17b1 - ap-south-1a [\[?\]](#)
IPv4 address: Assigned from CIDR 10.0.20.0/24

subnet-0a3c172852e25dc1 - ap-south-1b [\[?\]](#)
IPv4 address: Assigned from CIDR 10.0.21.0/24

[Edit subnets](#)

Hosted zone ZP87RAFUKTNQK

Creation time September 15, 2020 at 7:58:38 PM UTC+5:30

Security

Security groups sg-0502a1a0801a71412, Check-Point-Gateway-Auto-Scaling-Permissive [\[?\]](#)
+ Check-Point-Gateway-AutoScaling-Permissive

[Edit security groups](#)

Attributes

Deletion protection Enabled

Idle timeout 1000 seconds

HTTP2 Enabled

Deny on mitigation mode Defensive

Drop invalid header fields Disabled

Access logs S3 location cp-internal-internal- [\[?\]](#)

CP-internal-ALS

Internal-CP-internal active vpc-0003f5a0c447b0d2 ap-south-1a ap-south-1b Application September 12, 2020 at 10:2

VPC vpc-0003f5a0c447b0d2 [\[?\]](#)

Availability Zones

subnet-020555c03b6c17b1 - ap-south-1a [\[?\]](#)
IPv4 address: Assigned from CIDR 10.0.20.0/24

subnet-0a3c172852e25dc1 - ap-south-1b [\[?\]](#)
IPv4 address: Assigned from CIDR 10.0.21.0/24

[Edit subnets](#)

Hosted zone ZP87RAFUKTNQK

Creation time September 12, 2020 at 10:25:31 PM UTC+5:30

Security

Security groups sg-0502a1a0801a71412, Check-Point-Gateway-Auto-Scaling-Permissive SecurityGroups [\[?\]](#)
+ Check-Point-Gateway-AutoScaling-PermissiveSecurityGroups

[Edit security groups](#)

Attributes

Deletion protection Enabled

Idle timeout 300 seconds

HTTP2 Enabled

Deny on mitigation mode Defensive

Drop invalid header fields Disabled

Access logs S3 location cp-internal-als- [\[?\]](#)

CP-internal

Internal-CP-internal active vpc-0003f5a0c447b0d2 ap-south-1a ap-south-1b Application August 9, 2020 at 3:18:17 P...

VPC vpc-0003f5a0c447b0d2 [\[?\]](#)

Availability Zones

subnet-020555c03b6c17b1 - ap-south-1a [\[?\]](#)
IPv4 address: Assigned from CIDR 10.0.20.0/24

subnet-0a3c172852e25dc1 - ap-south-1b [\[?\]](#)
IPv4 address: Assigned from CIDR 10.0.21.0/24

[Edit subnets](#)

Hosted zone ZP87RAFUKTNQK

Creation time August 9, 2020 at 3:18:17 PM UTC+5:30

Security

Security groups sg-0502a1a0801a71412, Check-Point-Gateway-Auto-Scaling-Permissive SecurityGroups [\[?\]](#)
+ Check-Point-Gateway-AutoScaling-PermissiveSecurityGroups

[Edit security groups](#)

Attributes

Deletion protection Enabled

Idle timeout 300 seconds

HTTP2 Enabled

Deny on mitigation mode Defensive

Drop invalid header fields Disabled

Access logs S3 location checkpoint-new-internal- [\[?\]](#)



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

Log group	Retention	Metric filter	Stored bytes	ARN	Creation
/aws/rds/	Never expire	-	294.34 GB	arn:aws:logs:ap-south-1:652918353734:log-group:/a...	3 months a...
/aws/rds/	Never expire	-	216.21 MB	arn:aws:logs:ap-south-1:652918353734:log-group:/a...	3 months a...
/aws/rds/	Never expire	-	676.9 GB	arn:aws:logs:ap-south-1:652918353734:log-group:/a...	3 months a...
/aws/rds/	Never expire	-	41.33 GB	arn:aws:logs:ap-south-1:652918353734:log-group:/a...	3 months a...
/aws/rds/	Never expire	-	41.31 GB	arn:aws:logs:ap-south-1:652918353734:log-group:/a...	4 months a...
/aws/rds/	Never expire	-	25.67 MB	arn:aws:logs:ap-south-1:652918353734:log-group:/a...	4 months a...
/aws/rds/	Never expire	-	325.52 GB	arn:aws:logs:ap-south-1:652918353734:log-group:/a...	4 months a...
/aws/rds/	Never expire	-	40.88 GB	arn:aws:logs:ap-south-1:652918353734:log-group:/a...	4 months a...
/aws/rds/	Never expire	-	321.8 GB	arn:aws:logs:ap-south-1:652918353734:log-group:/a...	6 months a...
/aws/rds/	Never expire	-	105.63 MB	arn:aws:logs:ap-south-1:652918353734:log-group:/a...	6 months a...
/aws/rds/	Never expire	-	132.17 GB	arn:aws:logs:ap-south-1:652918353734:log-group:/a...	6 months a...
/aws/rds/	Never expire	-	18.6 MB	arn:aws:logs:ap-south-1:652918353734:log-group:/a...	6 months a...
/aws/rds/	Never expire	-	234.68 GB	arn:aws:logs:ap-south-1:652918353734:log-group:/a...	2 years ago

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

Log groups (114) Actions View in Logs Insights Create log group

By default, we only load up to 10000 log groups.

Filter log groups or by prefix search Exact match

Log group	Retention	Metric filters	Stored ...	ARN
RDSOSMetrics	1 month	-	-	arn:aws:logs:ap-south-1:652918353734:log-group:RDSOSMetrics
/aws/lambda/stopec2instance	1 month	-	7.12 KB	arn:aws:logs:ap-south-1:652918353734:log-group:/aws/lambda/stopec2instance
/aws/lambda/startec2instance	1 month	-	6.82 KB	arn:aws:logs:ap-south-1:652918353734:log-group:/aws/lambda/startec2instance
/aws/lambda/stop-sit-ec2-server	3 days	-	-	arn:aws:logs:ap-south-1:652918353734:log-group:/aws/lambda/stop-sit-ec2-server
/aws/lambda/s3-to-s3-transfer	3 days	-	-	arn:aws:logs:ap-south-1:652918353734:log-group:/aws/lambda/s3-to-s3-transfer
/aws/lambda/Ubuntu-Gaming-Server-EC2-Stop	3 days	-	1.13 KB	arn:aws:logs:ap-south-1:652918353734:log-group:/aws/lambda/Ubuntu-Gaming-Server-EC2-Stop
/aws/lambda/Ubuntu-Gaming-Server-EC2-Start	3 days	-	1.13 KB	arn:aws:logs:ap-south-1:652918353734:log-group:/aws/lambda/Ubuntu-Gaming-Server-EC2-Start
/aws/lambda/Tableau-server-13-04-2020-Ec2-Stop	3 days	-	2.25 KB	arn:aws:logs:ap-south-1:652918353734:log-group:/aws/lambda/Tableau-server-13-04-2020-Ec2-Stop

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.

AWS Config > Rules > encrypted-volumes

encrypted-volumes Actions

Rule details Edit

<p>Description</p> <p>Checks whether EBS volumes that are in an attached state are encrypted.</p> <p>Config rule ARN</p> <p>arn:aws:config:ap-south-1:652918353734:config-rule/config-rule-2laqcm</p>	<p>Trigger type</p> <ul style="list-style-type: none"> Overized configuration changes Configuration changes <p>Scope of changes:</p> <p>Resources</p> <p>Resource types:</p> <p>EC2 Volume</p>	<p>Last successful evaluation</p> <p>January 25, 2021 7:31 PM</p>
---	--	--

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

The screenshot shows the AWS Config console for the rule 'ec2-instance-no-public-ip'. The rule details include:

- Description:** Checks whether Amazon Elastic Compute Cloud (Amazon EC2) instances have a public IP association. The rule is NON_COMPLIANT if the publicip field is present in the Amazon EC2 Instance configuration item. This rule applies only to IPv4.
- Trigger type:**
 - Over-sized configuration changes
 - Configuration changes
- Scope of changes:** Resources
- Resource types:** EC2 Instance
- Last successful evaluation:** January 25, 2021 2:55 PM
- Config rule ARN:** arn:aws:config:us-east-1:652918333754:config-rule/config-rule-1b1jhu

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

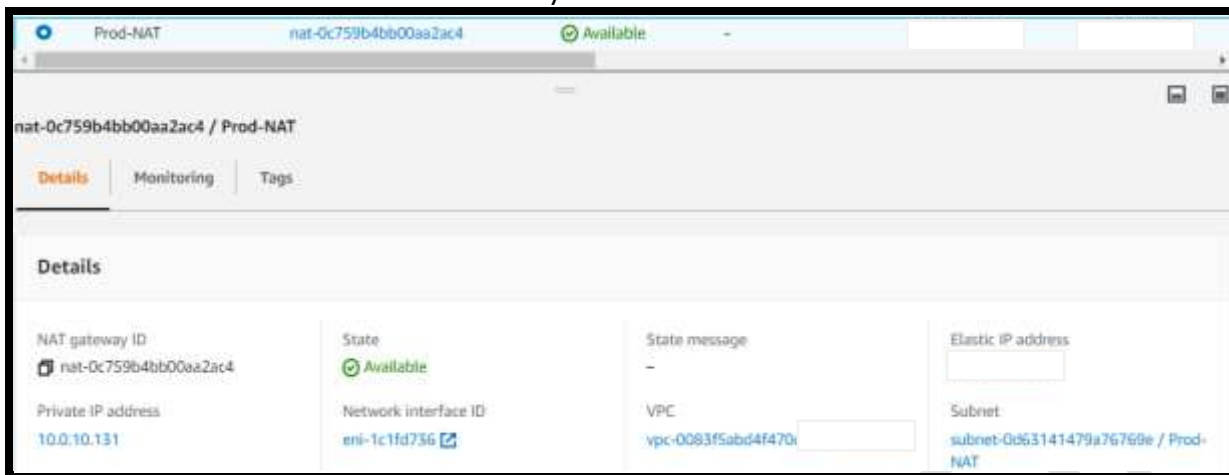
6.5 Ensure subnets for the Web tier ELB are created / 6.6 Ensure subnets for the Web tier are created /

6.7 Ensure subnets for the App tier are created / 6.8 Ensure subnets for the Data tier are created:

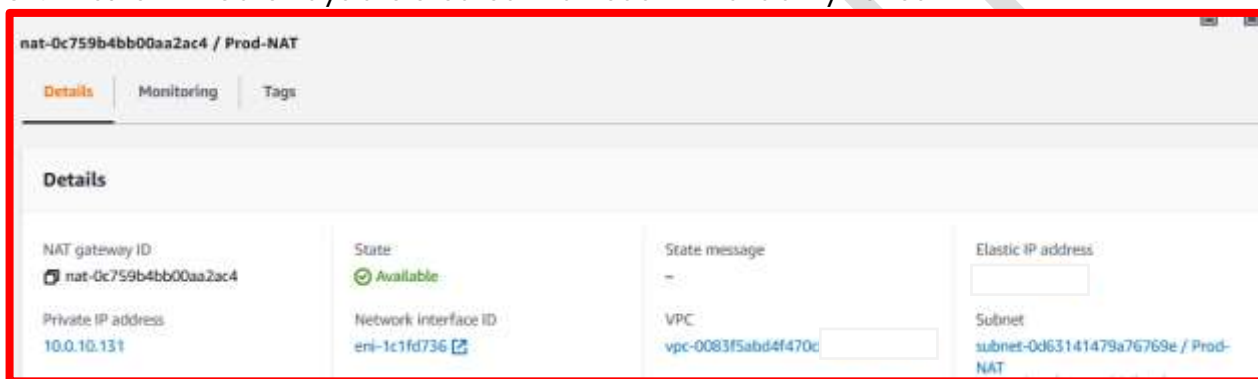
Name	Subnet ID	State	VPC	IPv4 CIDR
SIT-N...	subnet-02ab345ac38a24e99	Available	vpc-0083f5abd4f470c82 Pro...	10.0.19.0/24
SIT-N...	subnet-056e9a2c1d4d9bd08	Available	vpc-0083f5abd4f470c82 Pro...	10.0.25.0/24
Prod-...	subnet-05bdfca7ac13cd12	Available	vpc-0083f5abd4f470c82 Pro...	10.0.11.0/24
Prod-...	subnet-09cd18377afdf884	Available	vpc-0083f5abd4f470c82 Pro...	10.0.9.0/24
Prod-...	subnet-0d9d4f91df3d64cee	Available	vpc-0083f5abd4f470c82 Pro...	10.0.5.0/24
Prod-...	subnet-0146edd9b05583ea5	Available	vpc-0083f5abd4f470c82 Pro...	10.0.4.0/24
Prod-...	subnet-0772a981ae5939878	Available	vpc-0083f5abd4f470c82 Pro...	10.0.3.0/24
Prod-...	subnet-0ad5629333793ce77	Available	vpc-0083f5abd4f470c82 Pro...	10.0.2.0/24

subnet-0d63141479a76769e	Available	vpc-0083f5abd4f470c82 Pro...	10.0.10.0/24
subnet-0ebb175862835c9c1	Available	vpc-0083f5abd4f470c82 Pro...	10.0.21.0/24
subnet-038956c036e9cc7bb	Available	vpc-0083f5abd4f470c82 Pro...	10.0.20.0/24
subnet-03f90522400d7792d	Available	vpc-0083f5abd4f470c82 Pro...	10.0.7.0/24
subnet-0b6cfb0ee15af6306	Available	vpc-0083f5abd4f470c82 Pro...	10.0.6.0/24
subnet-0d3e9e4bae8a0a043	Available	vpc-0083f5abd4f470c82 Pro...	10.0.31.0/24
subnet-0d0f199ee7744eb0b	Available	vpc-0083f5abd4f470c82 Pro...	10.0.30.0/24
subnet-0acffc27060f8d3a7	Available	vpc-0083f5abd4f470c82 Pro...	10.0.33.0/24
subnet-0c8c49fdae20c973f	Available	vpc-0083f5abd4f470c82 Pro...	10.0.32.0/24
subnet-03ce6b19fbfe4b599	Available	vpc-0083f5abd4f470c82 Pro...	10.0.12.0/24

6.9 Ensure Elastic IPs for the NAT Gateways are allocated



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



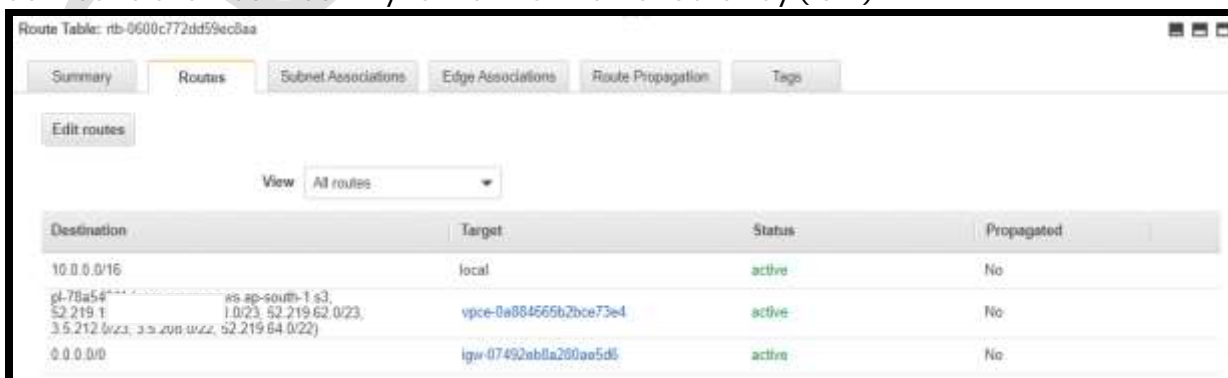
6.11 Ensure a route table for the public subnets is created



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

Route Table: rtb-0a2b15b719675576d

Summary Routes Subnet Associations Edge Associations Route Propagation Tags

Edit routes

View All routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
pl-78a54011 (c 52.219.160.0/ 52.219.64.0/22)	vpce-0a884665b2bce73e4	active	No
0.0.0.0/0	nat-0c759b4bb00aa2ac4	active	No

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

VIEW FILTERS

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
pl-78a54011 (c 52.219.160.0/ 52.219.64.0/22)	vpce-0a884665b2bce73e4	active	No
0.0.0.0/0	nat-0c759b4bb00aa2ac4	active	No
10.10.0.0/16	tgw-0726722bb1153d9d3	active	No
10.11.0.0/16	tgw-0726722bb1153d9d3	active	No
172.20.55.131/32	vgw-0a161e4691578969a	active	No
172.31.0.0/16	eni-072d107bb21fe308a	blackhole	No

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

Prod-ALB-SG sg-0f9c90a86dcaeb62 Prod-ALB-SG vpc-0083f5abd4f470c82 Prod-ALB-SG 652918353

Type	Protocol	Port range	Source	Description - optional
HTTP	TCP	80	28.0/21	Imperva
HTTP	TCP	80	32.0/19	Imperva
HTTP	TCP	80	72.0/21	-
HTTP	TCP	80	48.0/22	-
HTTP	TCP	80	.0/22	-
HTTP	TCP	80	24.0/22	-
HTTP	TCP	80	64.0/18	-
HTTP	TCP	80	0.0/16	-
HTTP	TCP	80	1/16	-
HTTP	TCP	80	0.0.0.0/16	-

Prod-ALB-SG	sg-0f9c90a86dacab62	Prod-ALB-SG	vpc-0083f5abd4f470c82	Prod-ALB-SG	652918353
HTTPS	TCP	443	128.0/21	Imperva	
HTTPS	TCP	443	32.0/19	Imperva	
HTTPS	TCP	443	72.0/21	-	
HTTPS	TCP	443	248.0/22	-	
HTTPS	TCP	443	4.0/22	-	
HTTPS	TCP	443	124.0/22	-	
HTTPS	TCP	443	164.0/18	-	
HTTPS	TCP	443	0.0/16	-	
HTTPS	TCP	443	0/16	-	
HTTPS	TCP	443	3.0/16	-	
HTTPS	TCP	443	3.41/32	Tableau Linux Server	

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

Launch configuration

Launch configuration

Check-Point-Security-Gateway-AutoScaling-ALLBANKS-LaunchConfig-PS28XU7T615M

Instance type

c5.xlarge

Storage (volumes)

View details in the launch configuration console

AMI ID

ami-07731c7c68fd774b8

Key pair name

CheckPoint-Prod

Security groups

sg-0f3785d02159118b3

Create time

Sat Sep 05 2020 20:26:42 GMT+0530 (India Standard Time)

Edit

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.

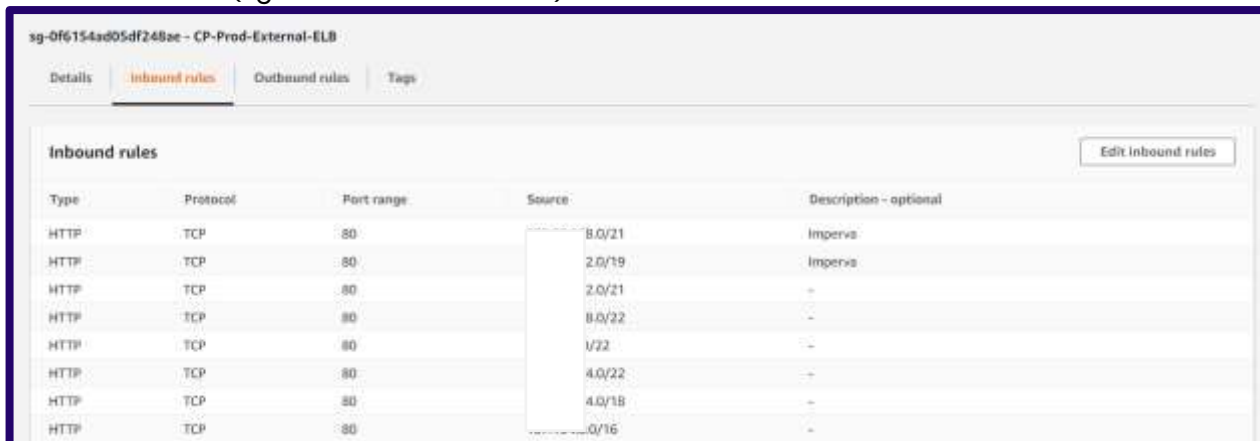


Security Group ID.xlsx

Note: Need to change the inbound rule.

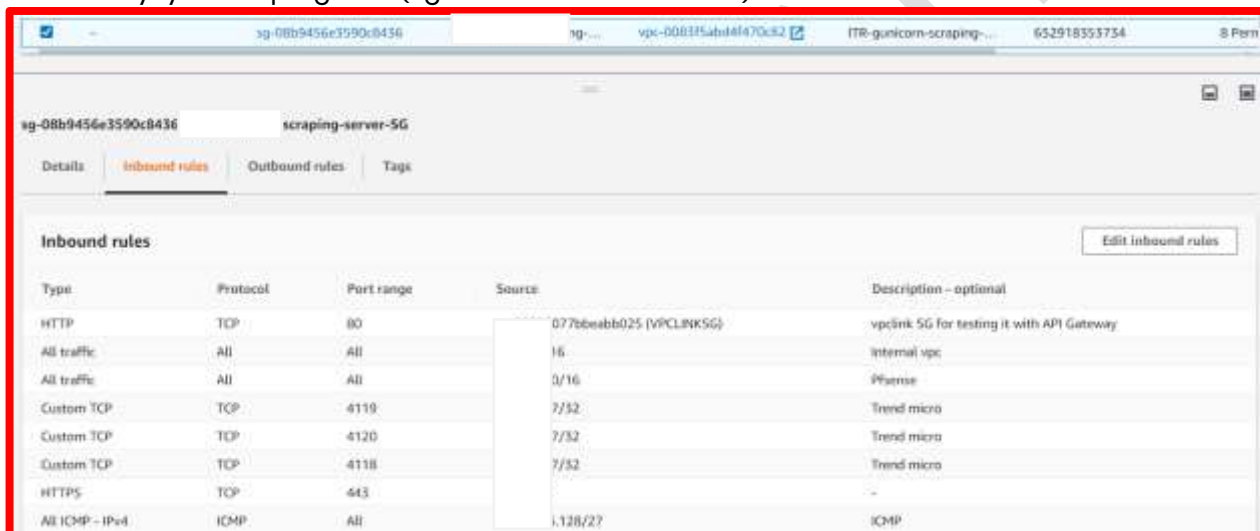
6.21 Create the App tier ELB Security Group and ensure only accepts HTTP/HTTPS

CP-External-ALB (sg-0f6154ad05df248ae)



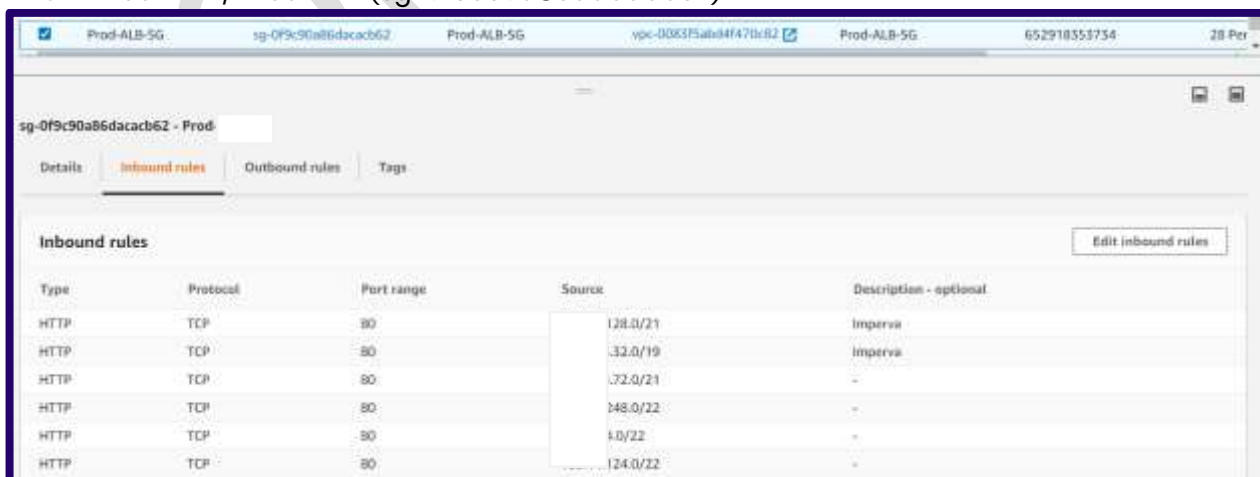
Type	Protocol	Port range	Source	Description - optional
HTTP	TCP	80	8.0/21	Imperva
HTTP	TCP	80	2.0/19	Imperva
HTTP	TCP	80	2.0/21	-
HTTP	TCP	80	8.0/22	-
HTTP	TCP	80	1/22	-
HTTP	TCP	80	4.0/22	-
HTTP	TCP	80	4.0/18	-
HTTP	TCP	80	0/16	-

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



Type	Protocol	Port range	Source	Description - optional
HTTP	TCP	80	077b6beabb025 (VPCLINKSG)	vpc link SG for testing it with API Gateway
All traffic	All	All	16	internal vpc
All traffic	All	All	0/16	IPFense
Custom TCP	TCP	4119	7/32	Trend micro
Custom TCP	TCP	4120	7/32	Trend micro
Custom TCP	TCP	4118	7/32	Trend micro
HTTPS	TCP	443	-	-
All ICMP - IPv4	ICMP	All	1.128/22	ICMP

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



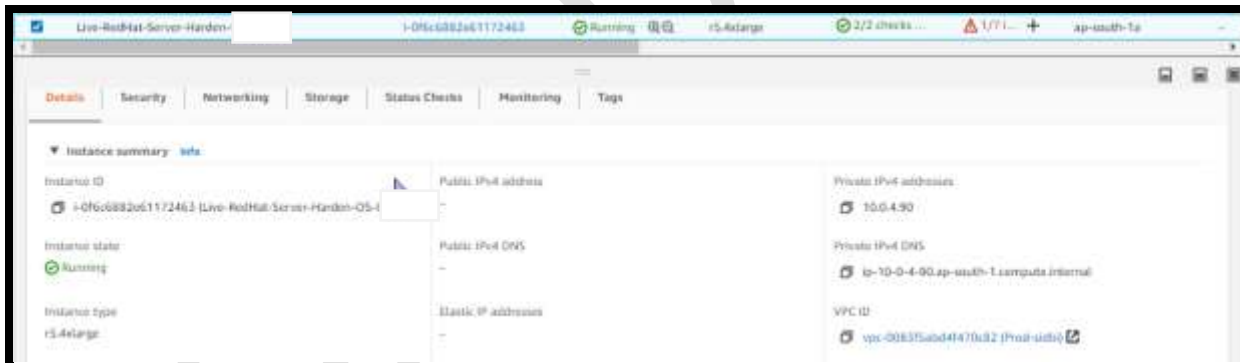
Type	Protocol	Port range	Source	Description - optional
HTTP	TCP	80	128.0/21	Imperva
HTTP	TCP	80	32.0/19	Imperva
HTTP	TCP	80	72.0/21	-
HTTP	TCP	80	148.0/22	-
HTTP	TCP	80	1.0/22	-
HTTP	TCP	80	124.0/22	-

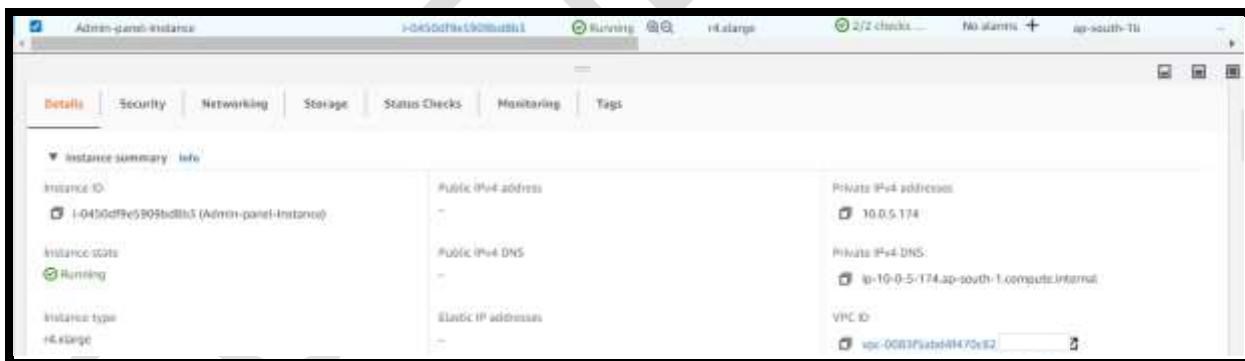
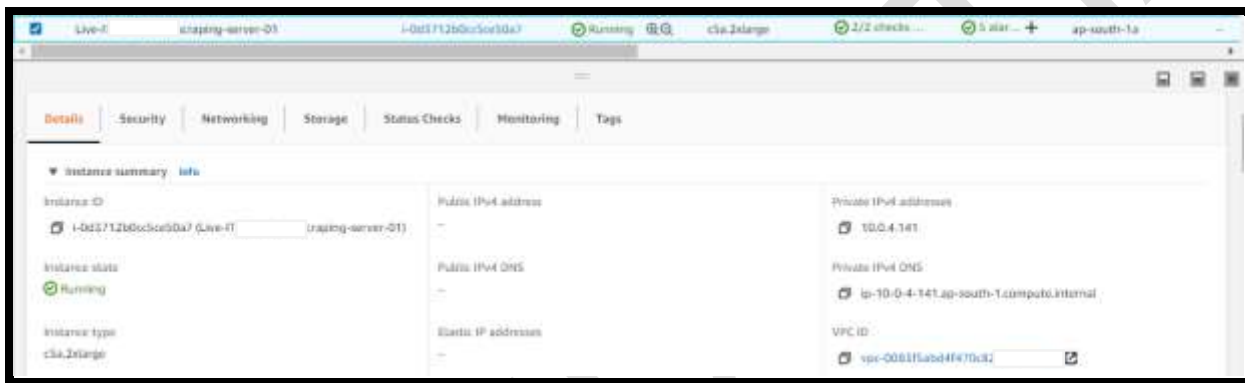
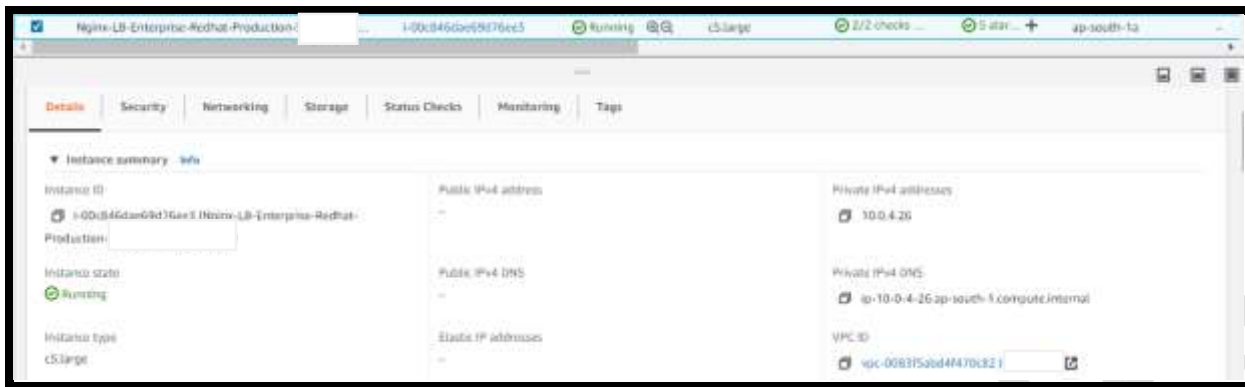
6.24 Create the Data Tier Security Group and ensure it allows inbound connections from App tier Security Group for explicit ports: Not Applicable

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

v2 Modify Actions

Summary

DB identifier prod	CPU 13.00%	Status Available	Class db.r5.4large
Role Primary	Current activity 6299 Connections	Engine MySQL Community	Region & AZ ap-south-1a

Connectivity & security | Monitoring | Logs & events | Configuration | Maintenance & backups | Tags

Connectivity & security

Endpoint & port Endpoint prod-myf4dp1ozqg.ap-south-1.rds.amazonaws.com Port 3306	Networking Availability zone ap-south-1a VPC vpc-0083f5abd4470c82 Subnet group default-vpc-0083f5abd4470c82 Subnets	Security VPC security groups RDS-hg-00f291dd30a8ef5ac (active) Public accessibility No Certificate authority rds-ca-2019
---	---	---

prod Modify Actions

Summary

DB identifier prod	CPU 31.00%	Status Available	Class db.r5.xlarge
Role Instance	Current activity 1749 Connections	Engine MySQL Community	Region & AZ ap-south-1b

Connectivity & security | Monitoring | Logs & events | Configuration | Maintenance & backups | Tags

Connectivity & security

Endpoint & port Endpoint prod-myf4dp1ozqg.ap-south-1.rds.amazonaws.com Port 3306	Networking Availability zone ap-south-1b VPC vpc-0083f5abd4470c82 Subnet group default-vpc-0083f5abd4470c82 Subnets	Security VPC security groups RDS-Prod-SG-hg-00f291dd30a8ef5ac (active) Public accessibility No Certificate authority rds-ca-2019
---	---	---

prod Modify Actions

Summary

DB identifier prod	CPU 4.00%	Status Available	Class db.r5.xlarge
Role	Current activity 1081 Connections	Engine MySQL Community	Region & AZ ap-south-1a

Connectivity & security | Monitoring | Logs & events | Configuration | Maintenance & backups | Tags

Connectivity & security

Endpoint & port Endpoint cmf-kdp-fcczg.ap-south-1.amazonaws.com Port 3306	Networking Availability zone ap-south-1a VPC [vpc-0063f5abd4f470xb2] Subnet group default-epc-0063f5abd4f470xb2 Subnets subnet-0b6c7f8ec15af6306 subnet-0ad5629553795ce77	Security VPC security groups RDS-Prod-SG [sg-0cfa91dd0a0edf50c] (active) Public accessibility No Certificate authority rds-ca-2019 Certificate authority date Aug 22nd, 2024
--	---	---

6.31 Don't use the default VPC

vpc-0063f5abd4f470xb2 Available 10.0.0.0/16

Details | CIDRs | Flow logs | Tags

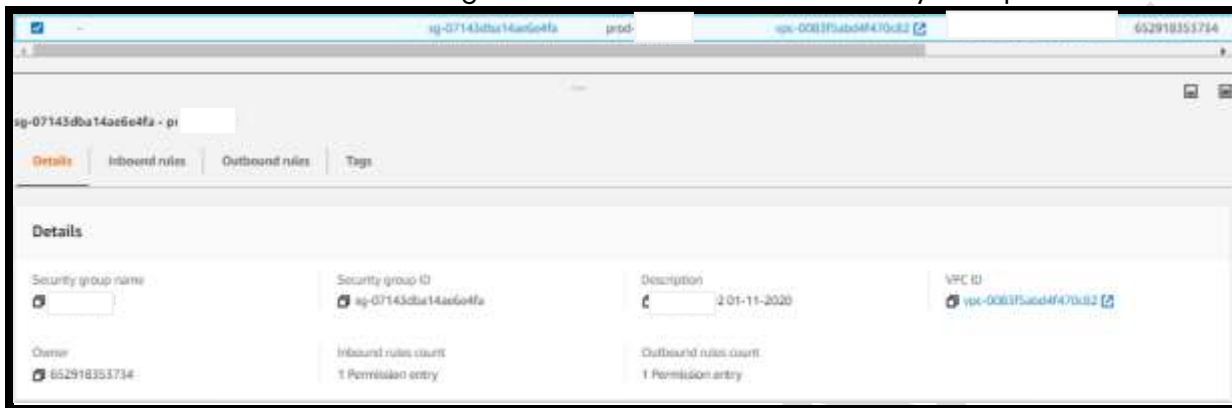
Details

VPC ID vpc-0063f5abd4f470xb2	State Available	DNS hostnames Enabled	DNS resolution Enabled
Tenancy Default	DHCP options set dopt-4a89e522	Route tables rtb-033bc42f5b2f4e400 / Prod-RT-No-5N4 Attached	Network ACL acl-0872d586a5e3957b9 / [] NACL
Default VPC No	IPv4 CIDR 10.0.0.0/16	IPv6 pool -	IPv6 CIDR -
Owner ID 692918353734			

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 of experienced veterans, technical experts & security enthusiasts having good practical experience & thorough knowledge in the Cybersecurity domain, are abreast of the latest trends and security innovations; ensuring that you always get the best security approach & solutions 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 Offices

UNITED STATES OF AMERICA
+1 516 713 5040

UNITED KINGDOM
+44 2035002056

SRI LANKA
+94 702 958 909

KUWAIT
+965 6099 1177

INDIA
+91 9898857117

