

Internal and Confidential

Table of Contents

[Document Control 3](#_Toc164066354)

[1 Purpose 4](#_Toc164066355)

[2 Scope 4](#_Toc164066356)

[3 Roles and Responsibilities 4](#_Toc164066357)

[4 Procedure 4](#_Toc164066358)

[4.1 Cloud Infrastructure Management 4](#_Toc164066359)

[4.1.1 What Cloud Infra Team Does? 4](#_Toc164066360)

[4.1.2 Cloud Infrastructure: 4](#_Toc164066361)

[4.1.3 Infrastructure as code: 5](#_Toc164066362)

[4.1.4 Server configuration management: 5](#_Toc164066363)

[4.1.5 CI/CD: 5](#_Toc164066364)

[4.1.6 Monitoring and alerting: 5](#_Toc164066365)

[4.1.7 Contact 5](#_Toc164066366)

[4.1.8 Tech Stack 5](#_Toc164066367)

[4.1.9 Team Overview 5](#_Toc164066368)

[4.1.10 Wiki 5](#_Toc164066369)

[4.2 Well Architected Review 6](#_Toc164066370)

[4.2.1 Multi-Account setup 6](#_Toc164066371)

[4.2.2 Costs 7](#_Toc164066372)

[4.2.3 Disaster Recovery 7](#_Toc164066373)

[4.2.4 Observability 7](#_Toc164066374)

[4.2.5 Security 7](#_Toc164066375)

[4.2.6 Resource Optimisation 8](#_Toc164066376)

[4.2.7 Databases 8](#_Toc164066377)

[4.2.8 Traffic Management 8](#_Toc164066378)

[4.3 Capacity management 9](#_Toc164066379)

[4.3.1 Autoscaling using AWS Auto Scaling Groups. 9](#_Toc164066380)

[4.3.2 LOAD PREP Dashboard 10](#_Toc164066381)

[4.3.3 Attaching an instance (console) 11](#_Toc164066382)

[4.4 Separation of development, testing and operational environments 12](#_Toc164066383)

[4.4.1 AWS VPC on Console 12](#_Toc164066384)

[4.4.2 Separate VPN Connections for each Environments 13](#_Toc164066385)

[4.4.3 The new QA environments has been created in separate account: 13](#_Toc164066386)

[4.5 Information Backup 14](#_Toc164066387)

[4.5.1 Automatic EBS Backups with Data life cycle manager. 14](#_Toc164066388)

[4.5.2 Volumes are backed up if tag snapshot is set to true. 14](#_Toc164066389)

[4.5.3 OnDemand Backup 15](#_Toc164066390)

[4.5.4 Manual Backup 15](#_Toc164066391)

[4.5.5 Retention Policy: 16](#_Toc164066392)

[4.5.6 Backup Restore 16](#_Toc164066393)

[4.6 Event Logging Procedure 17](#_Toc164066394)

[4.6.1 Following tools are used for even logging. 17](#_Toc164066395)

[4.6.2 Log retentions period: 17](#_Toc164066396)

[4.6.3 GuardDuty Findings: 18](#_Toc164066397)

[4.7 Procedure for Protection of Logs 18](#_Toc164066398)

[4.7.1 Protection of logs in Servers 18](#_Toc164066399)

[4.7.2 Protection of logs in S3 19](#_Toc164066400)

[4.8 Management of Administrator and Operator Logs 19](#_Toc164066401)

[4.8.1 To view CloudTrail events 20](#_Toc164066402)

[4.9 Procedure For Installation Of Software On Operational Systems 20](#_Toc164066403)

[4.9.1 GitHub Repo 20](#_Toc164066404)

[4.9.2 Sample Ansible code. 21](#_Toc164066405)

[4.10 Network Control Management on Cloud Infrastructure 22](#_Toc164066406)

[4.10.1 Network Segregation 22](#_Toc164066407)

[4.10.2 Creating a security group 23](#_Toc164066408)

[4.11 Security of Network Services 23](#_Toc164066409)

[4.11.1 Security Groups Dashboard 23](#_Toc164066410)

[4.11.2 Inbound Security Group 23](#_Toc164066411)

[4.11.3 Outbound Security Group 24](#_Toc164066412)

[4.11.4 GuardDuty 24](#_Toc164066413)

[4.12 Procedure for Disaster Recovery Drill 24](#_Toc164066414)

[4.12.1 POC in case of Disaster 25](#_Toc164066415)

[4.12.2 Check for the Service Availability: External Services 25](#_Toc164066416)

[4.12.3 Check all the alerts in PagerDuty/CloudWatch Monitors 26](#_Toc164066417)

[4.12.4 Executing the Disaster Recovery Drill DR Drill Plan 26](#_Toc164066418)

[4.12.5 Database 26](#_Toc164066419)

[5 Conduct 27](#_Toc164066420)

[6 Exception 27](#_Toc164066421)

[7 Terms/Acronyms 27](#_Toc164066422)

[8 References 27](#_Toc164066423)

[9 Appendix A: Document RACI Matrix 27](#_Toc164066424)

### Document Control

|  |  |
| --- | --- |
| **Document ID** | NDINFRA2024001 |
| **Document Name** | Netradyne Cloud Infrastructure Management Process & Procedure |
| **Document Status** | Released |
| **Document Released Date** | 04-APR-2025 |
| **Document Author** | Sudharsan Sivasankaran |
| **Document Content Contributors** | Sudhansu Kumar, Soham Chatterjee, Rajeev Ghosh |
| **Document Signatory** | Roshan Mathews |
| **Document Owner** | Sudharsan Sivasankaran |
| **Document Version** | V1.0 |
| **Information Classification** | Internal |

**Document Edit History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Additions/Modifications** | **Prepared/Revised By** |
| v1.0 | 04-APR-2024 | Merged 12 different procedural documents into this single Cloud Infrastructure Management Process and Procedure to have single master document for Infra. This will be easy to review and manage. | Sudhansu Kumar |
| V1.1 | 28-Mar-2025 | Review without any change | Kapil Kumar |
|  |  |  |  |
|  |  |  |  |

**Document Review/Approval**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Signatory Name** | **Organization/Signatory Title** | **Comments** |
| 04-APR-2024 | Roshan Mathews | Senior Director-Engineering |  |
| 28-Mar-2025 | Roshan Mathews | Senior Director-Engineering | Updated team — 4.1.9 |
|  |  |  |  |
|  |  |  |  |

**Distribution of Final Document**

|  |  |
| --- | --- |
| **Name** | **Organization/Title** |
| Netradyne Internal |  |
|  |  |
|  |  |

# Purpose

The purpose of Netradyne Capacity Management SOP is to layout the standard operating procedures for Managing Capacity for Netradyne assets.

# Scope

This SOP applies to all NETRADYNE technology assets, facilities, employees, contractors (as provided by law or contract), partners, and visitors, in achieving NETRADYNE missions, programs, projects, and institutional requirements. Frequency of this activity will be twice every year.

# Roles and Responsibilities

Roles and responsibilities specific to this document are included below:

|  |  |
| --- | --- |
| **Role** | **Responsibilities** |
| Owner | * Team or SME responsible for the process area needs to ensure this document is up to date and compliant with governing requirements. * Is the point of contact for the document. * Responsible for initiating and managing document review and the approval process from start to finish including gathering or delegating the collection of content including diagrams, formatting etc. as well as identifying stakeholders to participate in the peer review process. |
| Reviewers/Stakeholders | Representations from teams that can affect or be affected by the document under review (e.g., Operation, Security, Compliance, Quality) |
| Approvers | The Person(s) of authority to validate the document and sign-off on the latest version. Such Person include Document owner, Functional Team Lead, Security Lead, Product Delivery Lead. |
| Document Release | Document Owner/team to work with repository administrator to make release version available. |

# Procedure

## Cloud Infrastructure Management

The purpose of Netradyne Cloud Infrastructure Management Procedure is to layout the standard operating procedures for Managing infra–Critical Processes to be used for Troubleshooting and Compliance reasons.

### What Cloud Infra Team Does?

* Cloud Infrastructure
* Infrastructure as code
* Server configuration management
* CI/CD
* Monitoring and alerting

### Cloud Infrastructure:

Netradyne services are hosted on AWS Cloud. We use AWS services such as EC2, S3, Lambada, Kinesis, IoT, IAM, CloudWatch, VPC.

### Infrastructure as code:

AWS Cloud infra is managed with Terraform and python for automation.

### Server configuration management:

EC2 Instances are configured with the help of Ansible.

### CI/CD:

Cloud Infra Team maintain the build infrastructure which allows the developers to perform continuous integration. Jenkins is used for CI and GitHub as a Source code repository.

### Monitoring and alerting:

CloudWatch metrics are aggregated into Datadog monitoring and the on-call is alerted through PagerDuty.

### Contact

Connect with the Cloud Infra Team:

* on the #infraops channel on Slack. Tag us with @devops or @db there.
* or, on email: [devops@netradyne.com](mailto:devops@netradyne.com) and [dba@netradyne.com](mailto:dba@netradyne.com)

### Tech Stack

* AWS
* Terraform
* Ansible
* Python
* Datadog
* Pagerduty

### Team Overview

* Roshan Mathews
* **DevOps**:
  + Sudharsan Sivasankaran
  + Alok Mohan
  + Soham Chatterjee
  + Pravin Agarwal
  + Rohith Gunda
  + Shrey Saksena
  + Kokileswaran N
  + Rakshith Shivalingaraju
  + Bharath Raja
* **DB**:
  + Boopathi Lakshmanan
  + Gowthaman Sivasankaran
  + Raghunath Dhandapani
  + Nandan Prabhu
  + Ayush Choudhary
* **Infra-Dev**:
  + Rakesh Pelluri
  + Harshith Palakurthy
  + Mallikarjun S Gadiyavar
  + Siddarth Pai

### Wiki

#### Policy

* [Monitoring Policy](https://github.com/netradyne/infrastructure/wiki/Monitoring-Policy)
* [Self-Managed Resources Policy](https://github.com/netradyne/infrastructure/wiki/Self-Managed-Policy)
* [Tags Policy](https://github.com/netradyne/infrastructure/wiki/Tags-Policy)
* [Disaster Recovery Policy](https://github.com/netradyne/infrastructure/wiki/Disaster-Recovery-Policy)

#### What to do when

1. [IDMS is down](https://github.com/netradyne/infrastructure/wiki/IDMS-is-down)
2. [Kibana is down](https://github.com/netradyne/infrastructure/wiki/Kibana-is-down)
3. [AWS EBS service impaired / ALL DBs are crippled](https://github.com/netradyne/infrastructure/wiki/Slow-down-IDMS-ingestion-and-shut-down-console)
4. High disk usage on [metric.0](https://github.com/netradyne/infrastructure/wiki/High-Disk-Usage-on-metric)
5. Responding to Security Incidents
6. If [AWS Root Account is compromised](https://github.com/netradyne/infrastructure/wiki/Compromised-Root-Account)
7. If [AWS Access Keys are compromised](https://github.com/netradyne/infrastructure/wiki/Compromised-Access-Key)
8. If [AWS Certificates are compromised](https://github.com/netradyne/infrastructure/wiki/Compromised-Certificate)

#### DB Tasks

1. [DB on-call checklist](https://github.com/netradyne/infrastructure/wiki/DB-on-call-Check-List)
2. [PostgreSQL disk migration](https://github.com/netradyne/infrastructure/wiki/PostgreSQL-disk-upgrade)
3. [Service Postgres](https://github.com/netradyne/infrastructure/wiki/Service-Postgres)
4. [DB on-call check list](https://github.com/netradyne/infrastructure/wiki/DB-on-call-Check-List)
5. [Rebuild PG replicas using basebackup](https://github.com/netradyne/infrastructure/wiki/Rebuild-PG-replicas)

**·       Database Runbooks**

1. High disk usage on [/dev/xvdf in postgresql.x](https://github.com/netradyne/infrastructure/wiki/High-Disk-Usage-on-postgresql)
2. [Too Many PG Connections?](https://github.com/netradyne/infrastructure/wiki/Clear-Stale-Connections-in-postgresql)
3. [DB Checklist](https://github.com/netradyne/infrastructure/wiki/DB-Checklist)
4. [When to promote slave?](https://github.com/netradyne/infrastructure/wiki/guide-to-decide-slave-promotion)
5. [Postgresql slave promotion](https://github.com/netradyne/infrastructure/wiki/pg-slave-promotion)

#### How do we Create New [Service](https://github.com/netradyne/infrastructure/wiki/Service-Onboarding)

[Inward-Annotation AMI](https://github.com/netradyne/infrastructure/wiki/Building-IPA-AMIs)

* [Redrive Queues](https://github.com/netradyne/infrastructure/wiki/Redrive-queues-using-sqsutils.)
* +/- Employees from company
  + [+ Employees](https://github.com/netradyne/infrastructure/wiki/Employee-Joining-Checklist)
  + [- Employees](https://github.com/netradyne/infrastructure/wiki/Employee-Exit-Checklist)
* [Troubleshoot SSH](https://github.com/netradyne/infrastructure/wiki/Troubleshooting-SSH)
* Deploy [Annotation](https://github.com/netradyne/infrastructure/wiki/annotation)
* [Provide AWS Access/Permissions](https://github.com/netradyne/infrastructure/wiki/Reorganize-IAM-Permissions)
* [Bootstrap consul](https://github.com/netradyne/infrastructure/wiki/Bootstrapping-consul-server-cluster)
* [Tune elasticsearch cron jobs](https://github.com/netradyne/infrastructure/wiki/Elasticsearch-Cron-Jobs)
* [Configure FTP Server](https://github.com/netradyne/infrastructure/wiki/Configure-FTP-Server)

#### Monitoring

* [Improving Monitoring](https://github.com/netradyne/infrastructure/wiki/Measuring-and-fixing-monitoring-gaps)
* [SQS monitoring thresholds](https://github.com/netradyne/infrastructure/wiki/SQS-Monitoring-Thresholds)
* [Service Ownership](https://github.com/netradyne/infrastructure/wiki/Service-Ownership)

#### Notes

* on [Ansible Galaxy](https://github.com/netradyne/infrastructure/wiki/Note-AnsibleGalaxy)

## Well Architected Review

The purpose of Netradyne Well-Architected-Review process is to layout the standard operating procedures for designing AWS Critical Systems and Processes as advised by AWS.

### Multi-Account setup

* Use multiple accounts.
* Use [AWS Organizations](https://aws.amazon.com/organizations/), and [AWS Control Tower](https://aws.amazon.com/controltower/)
* Define [Service Control Policies (SCPs)](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps.html)
* Check out [AWS Landing Zone](https://aws.amazon.com/solutions/implementations/aws-landing-zone/) solution implementation.
* Need to follow up on "few clicks" option of separating out Staging and QA environments from main account
* Check Well-Architected White Papers, especially for the SaaS Lens

### Costs

* Check [AWS Budgets](https://aws.amazon.com/aws-cost-management/aws-budgets/)
* Use this to set expectations per customer, so if breached you know your assumptions are wrong.
* Costs Explorer: we've noticed a 48-hour delay, but ideally the delays should be 24 hours
* Set alerts on forecasted costs.
* on [AWS Marketplace](https://aws.amazon.com/marketplace/) - send a list of essential software we use. "If you're going to make a big purchase, let Vendor/OEM Provider know, to see if we can get a lower private pricing request – for bulk purchases."
* turn on [S3 Intelligent-Tiering](https://aws.amazon.com/about-aws/whats-new/2018/11/s3-intelligent-tiering/) for all buckets — \*strong\* recco from CSP side

### Disaster Recovery

Thought it is recommended that we should copy snapshots across AZs, but it looks like that's not needed.

We need to copy important snapshots across regions if we want to migrate to another region in the case of a disaster.

from the AWS docs: *To make a volume available outside of the Availability Zone, you can create a snapshot and restore that snapshot to a new volume anywhere in that Region. You can copy snapshots to other Regions and then restore them to new volumes there, making it easier to leverage multiple AWS Regions for geographical expansion, data centre migration, and disaster recovery.*

Need to define a Recovery Point Objective (RPO) and a Recovery Time Objective (RTO)

Playbook vs Runbook:

Needs playbook for setting up infra in another AZ if needed.

### Observability

Use something like [AWS X-Ray](https://aws.amazon.com/xray/) or [Splunk SignalFx](https://www.splunk.com/en_us/software/infrastructure-monitoring.html) . Check metrics for dependencies and then fine tune the services.

Enable backup services.

### Security

* Enable EBS encryption
* Encrypt the Database
* Use [Amazon Macie](https://aws.amazon.com/macie/) to protect sensitive data (including PHI, PII)
* Use [AWS Network Firewall](https://aws.amazon.com/network-firewall/)
* We already use [Amazon Guard Duty](https://aws.amazon.com/guardduty/), but we should turn on automated remediation.
* Use [AWS Config](https://aws.amazon.com/config/) — has rules pre-defined.
* For S3 bucket security, turn off world visible S3 buckets
* Use Git tools to scan for access keys checked into repositories.
* Follow [AWS Security Blog](https://aws.amazon.com/blogs/security/)
* Subscribe to AWS security newsletter to be up to date.

### Resource Optimisation

* [Rightsizing recommendations](https://console.aws.amazon.com/cost-management/home?region=us-west-1#/rightsizing) — this is free
* [AWS Compute Optimizer](https://console.aws.amazon.com/compute-optimizer/home?region=us-west-1#/) — this is not free
* [AWS Trusted Advisor](https://aws.amazon.com/premiumsupport/technology/trusted-advisor/) — this is free if we have a business support plan

### Databases

[Amazon Timestream](https://aws.amazon.com/timestream/) — good for IoT and infra-health use cases.

### Traffic Management

* [AWS Wavelength](https://aws.amazon.com/wavelength/) — quickly get onto AWS' 5G network instead of hopping on public internet. Jagan recommended this for live-tracking use-cases.
* [AWS Global Accelerator](https://aws.amazon.com/global-accelerator/) — similar idea.
* [Amazon CloudFront](https://aws.amazon.com/cloudfront/) is cheaper than Data-Transfer-Out and this is good for dynamic content as well.
* Use it to speed up IDMS console, currently only static content is on CloudFront.
* Check costs before enabling this.

A close-up of a computer screen

Description automatically generated

## Capacity management

### Autoscaling using AWS Auto Scaling Groups.

#### Scaling Policies based on Target Response Time.

**A screenshot of a computer

Description automatically generated**

#### Scaling policy based on SQS Queue (Backlog Per Worker)

**A screenshot of a computer

Description automatically generated**

#### Scaling policies logs

**A screenshot of a computer

Description automatically generated**

### A screenshot of a computer Description automatically generatedLOAD PREP Dashboard

Amazon EC2 Auto Scaling provides you with an option to enable automatic scaling for one or more EC2 instances by attaching them to your existing Auto Scaling group. After the instances are attached, they become a part of the Auto Scaling group.

* The instance to attach must meet the following criteria:
* The instance is in the running state.
* The AMI used to launch the instance must still exist.
* The instance is not a member of another Auto Scaling group.
* The instance is launched into one of the Availability Zones defined in your Auto Scaling group.

If the Auto Scaling group has an attached load balancer, the instance and the load balancer must both be in EC2-Classic or the same VPC. If the Auto Scaling group has an attached target group, the instance and the load balancer must both be in the same VPC.

When you attach instances, the desired capacity of the group increases by the number of instances being attached. If the number of instances being attached plus the desired capacity exceeds the maximum size of the group, the request fails.

If you attach an instance to an Auto Scaling group that has an attached load balancer, the instance is registered with the load balancer. If you attach an instance to an Auto Scaling group that has an attached target group, the instance is registered with the target group.

The examples use an Auto Scaling group with the following configuration:

* Auto Scaling group name = my-asg
* Minimum size = 1
* Maximum size = 5
* Desired capacity = 2
* Availability Zone = us-west-2a

### Attaching an instance (console)

You can attach an existing instance to an existing Auto Scaling group, or to a new Auto Scaling group as you create it.

#### To attach an instance to a new Auto Scaling group

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. On the navigation pane, under **INSTANCES**, choose **Instances**, and then select an instance.
3. Choose **Actions**, **Instance settings**, **Attach to Auto Scaling Group**.
4. On the **Attach to Auto Scaling group** page, for **Auto Scaling Group**, enter a name for the group, and then choose **Attach**.

The new Auto Scaling group is created using a new launch configuration with the same name that you specified for the Auto Scaling group. The launch configuration gets its settings (for example, security group and IAM role) from the instance that you attached. The Auto Scaling group gets settings (for example, Availability Zone and subnet) from the instance that you attached and has a desired capacity and maximum size of 1.

* (Optional) To edit the settings for the Auto Scaling group, on the navigation pane, under **AUTO SCALING**, choose **Auto Scaling Groups**. Select the check box next to the new Auto Scaling group, choose the **Edit** button that is above the list of groups, change the settings as needed, and then choose **Update.**

**To attach an instance to an existing Auto Scaling group**

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. (Optional) On the navigation pane, under **AUTO SCALING**, choose **Auto Scaling Groups**. Select the Auto Scaling group and verify that the maximum size of the Auto Scaling group is large enough that you can add another instance. Otherwise, on the **Details** tab, increase the maximum capacity.
3. On the navigation pane, under **INSTANCES**, choose **Instances**, and then select an instance.
4. Choose **Actions**, **Instance settings**, **Attach to Auto Scaling Group**.
5. On the **Attach to Auto Scaling group** page, for **Auto Scaling Group**, select the Auto Scaling group, and then choose **Attach**.
6. An error message will inform you if the instance does not meet the requirements. This could be because the instance is in a different Availability Zone than the Auto Scaling group. Select 'Close' and try again with an instance that meets the criteria.

#### Attaching an instance (AWS CLI)

1. Describe a specific Auto Scaling group using the following [describe-auto-scaling-groups](https://docs.aws.amazon.com/cli/latest/reference/autoscaling/describe-auto-scaling-groups.html) command.
2. AWS autoscaling describe-auto-scaling-groups --auto-scaling-group-names my-asg
3. Attach an instance to the Auto Scaling group using the following [attach-instances](https://docs.aws.amazon.com/cli/latest/reference/autoscaling/attach-instances.html) command.
4. AWS autoscaling attach-instances --instance-ids i-0787762faf1c28619 --auto-scaling-group-name my-asg
5. To verify that the instance is attached, use the following [describe-auto-scaling-groups](https://docs.aws.amazon.com/cli/latest/reference/autoscaling/describe-auto-scaling-groups.html) command.
6. AWS autoscaling describe-auto-scaling-groups --auto-scaling-group-names my-asg

## Separation of development, testing and operational environments

The purpose of Netradyne Separation of development, testing and operational environments is to layout the standard operating procedures for Managing Separate Environment for Netradyne assets.

We have separated our environments into logical networks, each network is isolated from other virtual networks in the AWS Cloud.

Following diagram show the visual representation of Separation of development, testing and operational environments.

A screenshot of a computer

Description automatically generated

### AWS VPC on Console

A screenshot of a computer

Description automatically generated

### Separate VPN Connections for each Environments

A screenshot of a computer

Description automatically generated

### The new QA environments has been created in separate account:

**QA3 – 691101237563**

**QA4 – 949832690386**

**QA5 – 003935485780**

A screenshot of a computer

Description automatically generated

## Information Backup

The purpose of Netradyne INFORMATION BACKUP is to layout the standard operating procedures for Managing Separate copies of Data for High availability and for DR process.

We use AWS EBS volumes as a storage. point-in-time snapshot of an EBS volumes are taken and used as a baseline for new volumes or for data backup.

### Automatic EBS Backups with Data life cycle manager.

**A screenshot of a computer

Description automatically generated**

### Volumes are backed up if tag snapshot is set to true.

**A screenshot of a computer

Description automatically generated**

### OnDemand Backup

We have Jenkins jobs which can backup EBS volume for specific uses cases.

<https://build-production.netradyne.info/job/PostgreSQL-EBS-Snapshot/2814/consoleFull>

### Manual Backup

To create a snapshot using the console

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. Choose Snapshots under Elastic Block Store in the navigation pane.
3. Choose Create Snapshot.
4. For Select resource type, choose Volume.
5. For Volume, select the volume.
6. (Optional) Enter a description for the snapshot.
7. (Optional) Choose Add Tag to add tags to your snapshot. For each tag, provide a tag key and a
8. tag value.
9. Choose Create Snapshot.
10. To create a snapshot using the command line
11. You can use one of the following commands. For more information about these command line
12. interfaces, see Accessing Amazon EC2.

* create-snapshot (AWS CLI)
* New-EC2Snapshot (AWS Tools for Windows PowerShell)

### Retention Policy:

Data life cycle manager is configured to delete daily backups after 3 days.

**A white background with black text

Description automatically generated**

### Backup Restore

You can restore a non-root volume attached to an existing EC2 instance by creating a volume from a snapshot and attaching it to your instance. You can use the console, the AWS CLI, or the API operations to create a volume from an existing snapshot. You can then mount the volume to the instance by using the operating system.

If you are replacing a volume that must use the same mount point, unmount that volume so that you can mount the new volume in its place. To unmount the volume, first stop any processes that are using the volume.

For example, follow these steps to restore a volume to an earlier point-in-time backup

#### by using the console:

1. On the Amazon EC2 console, on the Elastic Block Store menu, choose Snapshots.
2. Search for the snapshot that you want to restore and select it.
3. Choose Actions, and then choose Create Volume.
4. Create the new volume in the same Availability Zone as your EC2 instance.
5. On the Amazon EC2 console, select the instance.
6. In the instance details, make note of the device name that you want to replace in the Root device entry or Block Devices entries.
7. Attach the volume. The process differs for root volumes and non-root volumes.

#### For root volumes:

1. Stop the EC2 instance.
2. On the EC2 Elastic Block Store Volumes menu, select the root volume that you want to replace.
3. Choose Actions, and then choose Detach Volume.
4. On the EC2 Elastic Block Store Volumes menu, select the new volume.
5. Choose Actions, and then choose Attach Volume.
6. Select the instance that you want to attach the volume to and use the same device name that you noted earlier.

#### For non-root volumes:

1. Attach the new volume by choosing it on the EC2 Elastic Block Store Volumes menu and then choosing Actions, Attach Volume. Select the instance that you want to attach it to, and then select an available device name.
2. Using the operating system for the instance, unmount the existing volume, and then mount the new volume in its place.
3. In Linux, you can use the umount command. In Windows, you can use a logical volume manager (LVM) such as the Disk Management system utility.
4. Detach any prior volumes that you may be replacing by choosing it on the EC2 Elastic Block Store Volumes menu and then choosing Actions, Detach Volume.

## Event Logging Procedure

The purpose of Netradyne EVENT LOGGING is to layout the standard operating procedures for Managing logs for Critical Processes to be used for Troubleshooting and Compliance reasons

### Following tools are used for even logging.

#### Application/ Server logs:

Application logs are the server are collected using rsyslog daemon and sent into a centralized rsyslog server then collected logs are enriched using logstash and are indexed into ElasticSearch.

#### Application Exceptions:

exceptions are logged into sentry directly from the code and alert via email and slack channel.

#### Network Security Logs:

GaurdDuty is used for analyzing the AWS VPC flow logs and DNS resolvers logs.

#### AWS Services logs:

All AWS services are configured to write logs to s3 buckets which analyzed with AWS Athena when needed.

### Log retentions period:

* 7 days of logs in Logstash and Kibana
* Logs in s3 are kept 30 days and the archived at glacier.
* A virtual machine which has the s3 path with all the logs as a mountpoint is used to view logs.

**Kibana** - <https://logs-production.netradyne.info/app/kibana>

A screenshot of a computer

Description automatically generated

### GuardDuty Findings:

<https://us-west-1.console.aws.amazon.com/guardduty/home?region=us-west-1#/findings?macros=current>

**GuardDuty 
Findings 
Findings 
Showing 18 of 18 
Suppress Findings 
Create and save a suppression rule to automatically archive findings. 
Saved rules 
Current v Add filter criteria 
O 
O 
O 
O 
o 
O 
O 
Finding type 
Recon:EC2/PortProbeUnprotectedPort 
UnauthorizedAccess:EC2/SSHBruteForce 
Policy:lAMUser/RootCredentialUsage 
Stealth:S3/ServerAccessLoggingDisabled 
Stealth:S3/ServerAccessLoggingDisabled 
Recon:EC2/PortProbeUnprotectedPort 
Recon:EC2/PortProbeUnprotectedPort 
Behavior:EC2/NetworkPortUnusual 
Recon:EC2/PortProbeUnprotectedPort 
Recon:EC2/PortProbeUnprotectedPort 
Resource 
Instance: i- 
Instance: i- 
09db9d76a91 OObd69 
Ofel cc8432153e833 
Root: ASIAVJAW2AD2VRLAJFX2 
terraform: 
terraform: 
Instance: 
Instance: 
Instance: 
Instance: 
Instance: 
AKIAJBPMFJHQKH7ZK32A 
AKIAJBPMFJHQKH7ZK32A 
i-087a1394cOcec4b20 
i-05e3e3a1 bfc33cab2 
i-06f6847ebe227a2bb 
i-01bf805e368738f2f 
i-080a991a1d9525684 
No saved rules 
Last seen 
10 days ago 
13 days ago 
14 days ago 
15 days ago 
18 days ago 
21 days ago 
23 days ago 
a month ago 
a month ago 
a month ago 
Actions v 
Count 
3 
2 
5 
2 
2 
2 **

## Procedure for Protection of Logs

The purpose of Netradyne EVENT LOGGING is to layout the standard operating procedures for Managing logs for Critical Processes to be used for Troubleshooting and Compliance reasons. These logs and its storage need to be protected for data confidentiality Integrity and non-repudiation.

We keep our logs in servers as well as S3.

### Protection of logs in Servers

* All servers are behind VPN.
* We protect our logs with VPN access.  Mount point machine is protected with session manager.
* One should connect to Cisco VPN to check logs of any service for non-production environments (perf, testing, staging, qa, qa2, qa3 ,Devops )
* One should connect to OpenVPN for production logs.

### Protection of logs in S3

* We protect our logs in S3 through bucket policies and IAM permissions.
* We restrict users and AWS resources to access logs from S3 bucket by defining an IAM permission policy.
* Permission policy is attached to IAM users whoever needs to access logs.
* We define read access at bucket level as well as bucket level.

Below screenshot is one such example of IAM permission policy.

A screenshot of a computer

Description automatically generated

In actions section we define the actions (read, list) and in resources sections we define the bucket name and the corresponding objects in the bucket.

Also, we add a bucket policy for s3 bucket where we define cloud trail to collect access events performed on s3 bucket so that we can identify who accessed and what action was performed.

CloudTrail provides the event history of our AWS account activity.

* It helps to identify when access requests are made and identify potential unwarranted access attempts

## Management of Administrator and Operator Logs

All Administrator and operator logs on AWS are stored through **AWS CloudTrail**.

Cloud Trail > 
Event history 
(50+) Info 
Event history 
Read-only 
Event name 
Terminatelnstances 
Updatelnstancelnformation 
Terminatelnstances 
UpdateAutoScalingGroup 
CreateTags 
CreateVolume 
Runlnstances 
UpdateAutoScalingGroup 
UpdateAutoScalingGroup 
Updatelnstancelnformation 
DeregisterlnstancesFromL. .. 
DeregisterlnstancesFromL. .. 
Updatelnstancelnformation 
UpdateAutoScalingGroup 
Download events v 
v 
Q false 
Event time 
December 1 5, 
December 1 5, 
December 1 5, 
December 1 5, 
December 1 5, 
December 1 5, 
December 1 5, 
December 1 5, 
December 1 5, 
December 1 5, 
December 1 5, 
December 1 5, 
December 1 5, 
December 1 5, 
X 
Event source 
30m 
Create Athena table 
2 
2020, 17 
2020, 17 
2020, 17 
2020, 17 
2020, 17 
2020, 17 
2020, 17 
2020, 17 
2020, 17 
2020, 17 
2020, 17 
2020, 17 
2020, 17 
2020, 17 
User name 
AutoScaling 
i-Of42e8bff52ce84fc 
AutoScaling 
jenkins-slave 
i-OcdOd8762622072eb 
i-09460af41 b03f13ee 
AutoScaling 
set_annotation_asg_pro 
jenkins-slave 
i-08253d3b2cd68b714 
AutoScaling 
AutoScaling 
i-Ocf032d153b08b6da 
set_annotation_asg_pro... 
lh 
Resource type 
AWS.. 
AWS.. 
AWS. 
AWS. 
AWS. 
AWS. 
12h 
Custom 
ec2.amazonaws.com 
ssm.amazonaws.com 
ec2.amazonaws.com 
autoscaling.amazonaws.com 
ec2.amazonaws.com 
ec2.amazonaws.com 
ec2.amazonaws.com 
autoscaling.amazonaws.com 
autoscaling.amazonaws.com 
ssm.amazonaws.com 
elasticloadbalancing.amazonaws.c 
elasticloadbalancing.amazonaws.c 
ssm.amazonaws.com 
autoscaling.amazonaws.com 
•:AutoScaling::AutoScaling... 
•:AutoScaling::AutoScaling... 
•:AutoScaling::AutoScaling... 
•:AutoScaling::AutoScaling... 
Resource name 
i-0544c2da8388a86a3 
i-04c8174f19c96c87c 
jenkins-slave-staging 
snap-060c652588770da4f, vol-O... 
vpc-21 fOc744, ami-0490461c57f... 
annotation-us-production 
jenkins-slave-staging 
i-Ocd5367200a319393, i-0492de... 
i-Ocd5367200a319393, i-0492de... 
annotation-us-production 

CloudTrail console to view the last 90 days of recorded API activity and events in an AWS Region. You can also download a file with that information, or a subset of information based on the filter and time range you choose. You can customize your view of Event history by selecting which columns are displayed in the console. You can also look up and filter events by the resource types available for a particular service. You can select up to five events in Event history and compare their details side-by-side.

### To view CloudTrail events

1. Sign in to the AWS Management Console and open the CloudTrail console at <https://console.aws.amazon.com/cloudtrail/home/>.
2. In the navigation pane, choose **Event history**.   
   A filtered list of events appears in the content pane with the latest event first. Scroll down to see more events.
3. To compare events, select up to five events by filling their check boxes in the left margin of the **Event history** table. View details for selected events side-by-side in the **Compare event details** table.

The default view of events in Event history has a filter applied so that it does not display read-only events. To remove this filter, or to apply other filters, change the filter settings. For more information, see [Filtering CloudTrail Events.](https://docs.aws.amazon.com/awscloudtrail/latest/userguide/view-cloudtrail-events-console.html#filtering-cloudtrail-events)

## Procedure For Installation Of Software On Operational Systems

The purpose of Software Installation Management is to layout the standard operating procedures to ensure only authorized personnel are able to make any changes in system configuration or installation of software in production environment.

Ansible is used to configure and install software on our production systems.

### GitHub Repo

>[https://github.com/netradyne/infrastructure/blob/master/tasksconfiguration/app.yml](https://github.com/netradyne/infrastructure/blob/master/tasks-configuration/app.yml)

### Sample Ansible code.

---

- name: Configures CloudApp machine

  vars:

    hosts: app

    device: /dev/xvdf

    data\_directory: /data

    tomcat\_user: tomcat8

    tomcat\_group: tomcat8

  hosts: "{{ hosts }}"

  become: true

  become\_user: root

  vars\_files:

    - "../secrets/{{ environment }}.yml"

  pre\_tasks:

    - name: Ensure data directory exists

      file:

        path: "{{ data\_directory }}"

        mode: 0755

        state: directory

        owner: "root"

        group: "root"

    - name: Create ext4 filesystem on App data disk

      filesystem:

        fstype: ext4

        dev: "{{ device }}"

    - name: Mount the App data disk

      mount:

        name: "{{ data\_directory }}"

        src: "{{ device }}"

        fstype: ext4

        opts: noatime

        state: mounted

    - name: Ensure data directory exists

      file:

        path: "{{ data\_directory }}"

        mode: 0755

        state: directory

        owner: "root"

        group: "root"

  roles:

    - role: ansible-netradyne

    - role: ansible-awscli

## Network Control Management on Cloud Infrastructure

The purpose of Network Control Management is to layout the standard operating procedures to ensure networks are aptly restricted to allow only permissible requests and traffic.

VPC Security Groups are used for controlling networks.

A security group acts as a virtual firewall for the instance to control inbound and outbound traffic with in VPC.

### Network Segregation

Netradyne uses different VPC for segregate networks in different environment such as production, testing and QA.

**us-west-I (N california) 
pROD 
10.100.0.0/16 
Devops 
10.250.0.0/16 
10.230.0.0/16 
Testing 
10.210.0.0/16 
10.240.0.0/16 
Perl 
10.240.0.0/16 
10.250.0.0/16 **

#### Production VPC Configuration

##### Production VPC-external\_22-001

subnet-0e75dae484f22637d vpc-21f0c744 | Production VPC 10.100.8.0/22

##### Production VPC-external-003

subnet-edead3b4 vpc-21f0c744 | Production VPC 10.100.2.0/24

##### Production VPC-external-004

subnet-19bb4b7d vpc-21f0c744 | Production VPC 10.100.3.0/24

##### Production VPC-external-001

subnet-eaead3b3 vpc-21f0c744 | Production VPC 10.100.0.0/24

##### Production VPC-external-002

subnet-1abb4b7e vpc-21f0c744 | Production VPC 10.100.1.0/24

##### Production VPC-external\_22-002

subnet-009802d3a216381eb vpc-21f0c744 | Production VPC 10.100.12.0/22

### Creating a security group

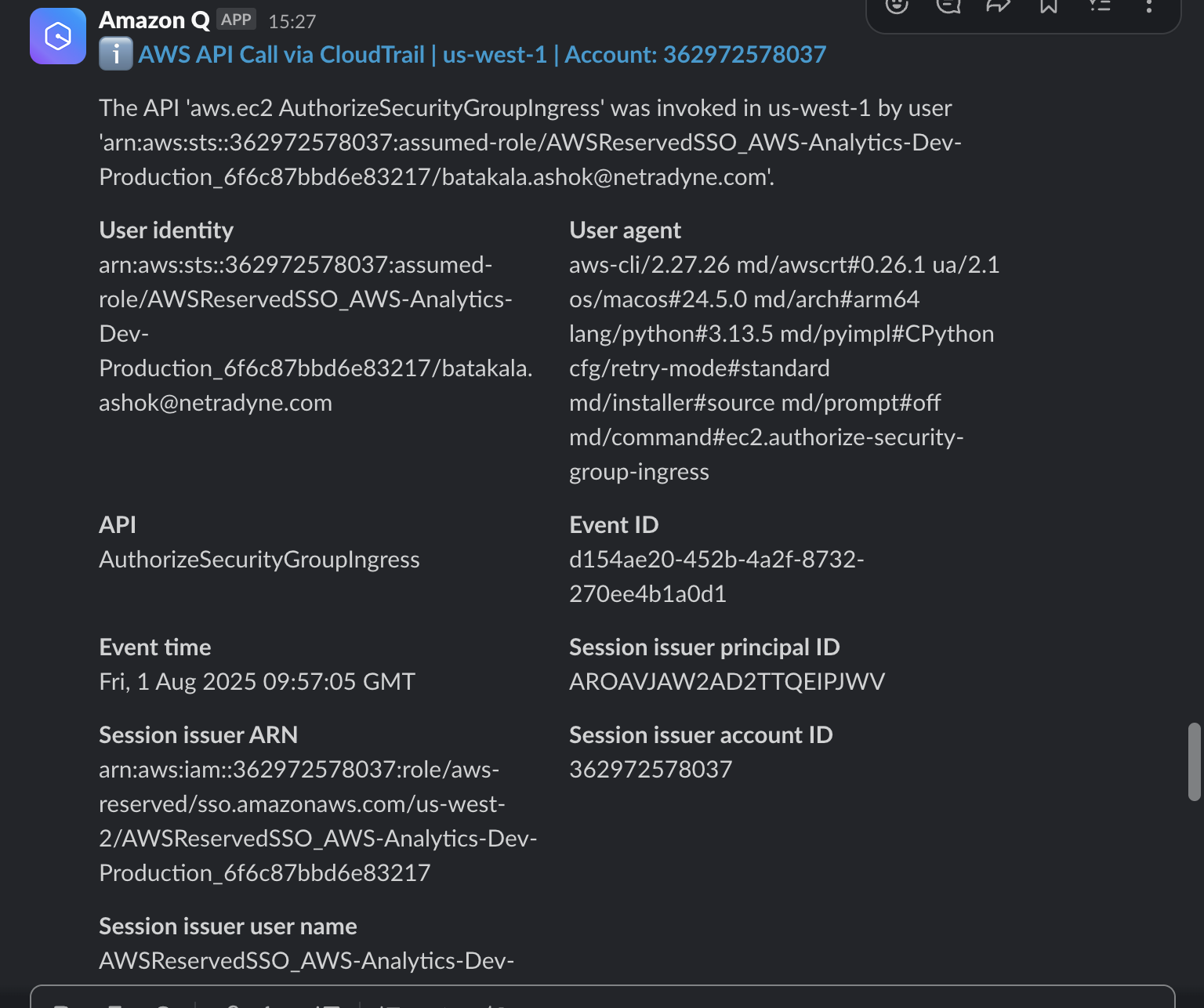
The following procedure creates a security group with no inbound rules, and the default outbound rule.   
To create a security group using the console

1. Open the Amazon VPC console at <https://console.aws.amazon.com/vpc/>.
2. In the navigation pane, choose Security Groups.
3. Choose Create security group.
4. Enter a name for the security group (for example,my-security-group), and then provide a description.
5. From VPC, select the ID of your VPC.
6. (Optional) Add or remove a tag.
7. [Add a tag] Choose Add new tag and do the following:
8. For Key, enter the key name.
9. For Value, enter the key value.
10. [Remove a tag] Choose Remove to the right of the tag’s Key and Value.

## Security of Network Services

All network security is managed by using VPC security groups and network traffic is monitored with AWS Guard Duty and alerts if there is an anomaly found.

All changes to security groups immediately sends a slack notification to all the team members.



### Security Groups Dashboard

A screenshot of a computer

Description automatically generated

### Inbound Security Group

A screenshot of a computer

Description automatically generated

### Outbound Security Group

Description 
Edit 
Type 
Inbound 
Outbound 
Tags 
Protocol 
0) 
Port Range 
This security group has no rules 
0) 
Destination 
Description 

### GuardDuty

GuardDuty 
Findings 
Findings 
Suppress Findings 
Current v Add filter criteria 
Saved rules 
O 
O 
O 
O 
o 
O 
O 
Finding type 
Recon:EC2/PortProbeUnprotectedPort 
UnauthorizedAccess:EC2/SSHBruteForce 
Policy:lAMUser/RootCredentialUsage 
Stealth:S3/ServerAccessLoggingDisabled 
Stealth:S3/ServerAccessLoggingDisabled 
Recon:EC2/PortProbeUnprotectedPort 
Recon:EC2/PortProbeUnprotectedPort 
Behavior:EC2/NetworkPortUnusual 
Recon:EC2/PortProbeUnprotectedPort 
Recon:EC2/PortProbeUnprotectedPort 
Resource 
Instance: i- 
Instance: i- 
09db9d76a91 OObd69 
Ofel cc8432153e833 
Root: ASIAVJAW2AD2VRLAJFX2 
terraform: 
terraform: 
Instance: 
Instance: 
Instance: 
Instance: 
Instance: 
AKIAJBPMFJHQKH7ZK32A 
AKIAJBPMFJHQKH7ZK32A 
i-087a1394cOcec4b20 
i-05e3e3a1 bfc33cab2 
i-06f6847ebe227a2bb 
i-01bf805e368738f2f 
i-080a991a1d9525684 
Showing 
No saved rules 
Last seen 
10 days ago 
13 days ago 
14 days ago 
15 days ago 
18 days ago 
21 days ago 
23 days ago 
a month ago 
a month ago 
a month ago 
18 of 18 
15 
Actions v 
Count 
3 
2 
5 
2 
2 
2 

## Procedure for Disaster Recovery Drill

A disaster recovery drill is a simulated exercise conducted by Netradyne Infra Team to evaluate their preparedness and response capabilities in the event of a disaster. The purpose of such drills is multifold:

**Assessing Preparedness:**

It allows Infra team to evaluate their disaster recovery plans, procedures, and resources to ensure they are comprehensive and effective.

**Identifying Weaknesses:**

By simulating various disaster scenarios, Infra Team can identify weaknesses in their response strategies, infrastructure, communication channels, and personnel readiness.

**Training and Familiarization:**

Conducting drills provides an opportunity for Infra Team Members and other Involved Dept Personnel to become familiar with their roles and responsibilities during a disaster. It also allows them to practice specific actions they would need to take to mitigate the impact of a real disaster.

**Testing Systems and Technology:**

Disaster recovery drills help assess the functionality and reliability of backup systems, data recovery processes, and IT/Cloud infrastructure under stress.

**Improving Response Time:**

By practicing response procedures in a controlled environment, Infra team can streamline their processes and reducing the time it takes to respond to a real disaster.

**Compliance and Regulation:**

Many industries are subject to regulatory requirements related to disaster preparedness and recovery. Conducting regular drills ensures compliance with these regulations and helps Netradyne avoid penalties.

Overall, the purpose of a disaster recovery drill is to enhance Netradyne's resilience and ability to recover quickly and efficiently from a disaster, minimizing disruption to operations and ensuring the safety of employees and stakeholders.

Periodic DR-plan drills are conducted at Netradyne. Summary of DR-plan drills tracked at [JIRA Epic: Disaster recovery checklist](https://netradyne.atlassian.net/browse/INFRA-1242) - INFRA-1242

### POC in case of Disaster

* DevOps POC:
  + Soham Chatterjee [soham.chatterjee@netradyne.com](mailto:soham.chatterjee@netradyne.com)
  + Shrey Saksea shrey.saksena@netradyne.com
  + Alok Mohan [alok.mohan@netradyne.com](mailto:alok.mohan@netradyne.com)
* DB POC:
  + Boopathi Lakshmanan [boopathi.lakshmanan@netradyne.com](mailto:boopathi.lakshmanan@netradyne.com)
  + Rakesh Pelluri [rakesh.pelluri@netradyne.com](mailto:rakesh.pelluri@netradyne.com)
* 2nd level POC:
  + Sudharsan Sivasankaran [sudharsan.sivasankaran@netradyne.com](mailto:sudharsan.sivasankaran@netradyne.com)
  + Roshan Mathews [roshan.mathews@netradyne.com](mailto:roshan.mathews@netradyne.com)

### Check for the Service Availability: External Services

* IDMS
* API
* Partner Assets
* Data Platform

Login to these services and confirm all the features are running in all the external services 

Next Step:

### Check all the alerts in PagerDuty/CloudWatch Monitors

1. Queue based.
2. Latency based

Since services was unavailable and queues and latency will surely increase due to delay in processing. Once everything is fine, we can confirm our services to be up and running.

### Executing the Disaster Recovery Drill DR Drill Plan

We executed the drill with 2 situations:

1. When all the workers get killed by AWS and new workers need to be spawned
2. Spot instances has issue in AWS and we need to scale fixed instances.   
      
   We have deleted all the workers in DevOps environment

* App-console
* app-device
* app-internal
* app-frs
* oath
* partner-assets
* api
* data-platform
* Mapserver
* frs
* stats

Rest is queuing service so there won't be any downtime but there will be delay.   
   
We have now launch template, we can scale up fixed instances immediately without waiting for any infra changes from the code side to make the system up and running.

**We captured the time for all the instances to come up and services to be up.**   
**The system was up in less than 5 mins in both the cases.**

* There is no manual intervention required, since ASG will spawn up new workers and it will load-balance the traffic among the rest of the machines as part of the target group for each service.
* Also, there is mixed instance policy now since we are using launch template instead of launch configuration, so we can manage the capacity rebalancing more quickly compared launch configuration.
* We also have monitors configured for all the services in production and staging environment. In case of delay, we will be notified and can take actions if required.
* Multi AZ: We have setup in 2 availability zones. All the services expect TP runs on both AZ. If 1 AZ have any issue, we can call up workers in the other AZ.

### Database

We did not delete any DB in the drill. In case of disaster, we have slave and can promote to main db anytime. In case of any issue with slave we have regular snapshots, from that we can create the DB.

# Conduct

Compliance Checks to this process are to be performed through various methods, including but not limited to reports, internal/external audits All tests conducted adhere to the controls outlined in both HIPAA and GDPR regulations. Additionally, our workforce receives regular Security Awareness, compliance, and role-based training opportunities. New hires undergo various trainings including security awareness workshops within 90 days of being hired. Furthermore, employees are required to complete mandatory training, including the protection of Personally Identifiable Information (PII), Protected Health Information (PHI), and other sensitive business data, which is monitored continuously. Non-compliance will be escalated to the Netradyne leadership team.

# Exception

Exception to this procedure must be approved through the Netradyne Exception Process.

# Terms/Acronyms

|  |  |
| --- | --- |
| **Term/Acronym** | **Definition** |
| SOP | Standard Operating Procedure |
| TBD | To be disclosed |
| NA | Not Applicable |
| PHI | Protected Health Information |
| PII | Protected Identifiable Information |
| ePHI | Electronic protected health information |
| HIPAA | Health Insurance Portability and Accountability Act |

# References

[Netradyne Information Security Policy & Procedure.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/ISMS%20Published%20Documents/ISMS%202023/Netradyne%20Information%20Security%20Policy%20%26%20Procedure.pdf?csf=1&web=1&e=QDfjvy)

# Appendix A: Document RACI Matrix

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Role/Activity | Document Owner/Functional Area Lead | Document Contributor | ND Leadership | Functional Area Team | InfoSec | All ND Member(s) |
| Ensure document is kept current | A | R | I, C | R, C | C | I |
| Ensure stakeholders are kept informed | A | R | - | R | C | - |
| Ensure document contains all relevant information | A | R | I, C | R, C | C | I |
| Ensure document adheres to document governance policy | A, R | R | I | R, C | R, C | I |
| Provide SME advice | I, R | A, R | I | R, C | I, C | I |
| Gathering and adding document contents | I | A, R | I, C | R, C | C | I |
| Document Approval | A | R | I, R | I | I, R | I |

|  |  |
| --- | --- |
| Key |  |
| R | Responsible |
| A | Accountable |
| C | Consulted |
| I | Informed |