# eMach CTSigma AMI Model Deployment Document.

# Table of Contents

# 1.Introduction

## 1.1 Introduction to the Sigma Product

A cloud ready **Enterprise Data Platform** powered by Intellect's Canvas Technology. eMACH - Sigma enables customization **"out of the box reports** & **on-the-fly-visualization creation"**, thereby enabling all business users to seamlessly access reports & dashboards real-time.

eMACH-Sigma enables creation of reports on-the-fly without the need for technical expertise, testing and deployment by reducing the complexities in designing reports.

**IT and Operations Staff** in organisations who have access to data sources can use **eMACH-Sigma Studio** to define the report configurations. **Report Designers** can use eMACH-Sigma Studio to control how reports are enabled for end-users (Report Consumers).

**eMACH-Sigma Studio enables report designers to build:**

- Simple Data Structures using data source
- Complex Data Structures using Data Builder
- Simple Reports
- Complex Reports sections using Templates
- Complex Reports using Sub-reports

**eMACH-Sigma Studio enables report designers to control:**

- What data or reports can be accessed by end users using Entitlement ● Formats in which the reports can be generated - CSV, DOCX, HTML, PDF, XLS, TXT and XML are supported.
- Maintenance of generated reports
- Execution of EOD reports through REST or online

**Executives and officers** within an organisation or its **customers** can use the **eMACH-Sigma Application** to generate reports for their internal and external audience. They can also perform scheduling to generate BOD/EOD reports. **Report Consumers** can create canned and ad-hoc reports using the eMACH-Sigma application.

**eMACH-Sigma application provides the following features for the end-users:**

- Customizing of reports
- Selecting export formats
- Grouping data
- Applying filters
- Choosing notification or delivery mechanism
- Scheduling reports
- Organizing reports
- Merging multiple reports into single report

To gain a deeper understanding of the **Sigma product**, its features, and various use cases, please refer to the detailed documentation available at the following Confluence link:

What is eMACH-Sigma?

This resource provides comprehensive insights into the product's capabilities, applications, and benefits, helping you explore how it can be effectively utilized to meet your specific requirements.

## 1.2 Introduction about customer deployment and lists of all resources

When a customer subscribes to the product on AWS Marketplace and deploys it using the provided AWS CloudFormation templates, the following resources are automatically provisioned:

### EC2 Instances

- **Application & Database Server Instance**: Launched from the APP & DB AMI, preconfigured with the necessary application and Database stacks.
- **Amazon EBS Volumes**: Attached to the EC2 instances for operating system, application, and database storage.

### Networking & Security

- **Security Groups**: Automatically created to enforce network access control for the application and database instances.
- **IAM Roles & Policies**: Assigned to instances and backup automation services to securely interact with AWS resources.

### Backup Automation (Optional)

If the backup automation CloudFormation template is deployed, the following additional resources are provisioned:

- **AWS Backup Service (Automated via CloudFormation)**
  - The deployment includes a CloudFormation template to set up an **AWS Backup Plan** for EC2 instances.
  - The backup plan, named **SigmaBackupPlan**, automates **daily snapshots** (configurable to run every hour, every 12 hours, or every 24 hours).
  - A **Backup Vault** (**SigmaBackupVault**) is created to store snapshots securely, with a **default retention period of 7 days** (configurable). ○ A **Backup IAM Role** is provisioned to allow AWS Backup to manage instance snapshots.

Once the deployment is complete, customers can access their EC2 instances via SSH or a web-based interface. Additionally, the automated backup solution ensures regular backups of the **APP & DB instance**, providing **disaster recovery and data protection**.

# 1.3 Deployment Options for Sigma Product

The **Sigma Product** is available on **AWS Marketplace** and is deployed using **CloudFormation templates stored in an S3 bucket**. The user guide includes details on the following deployment options:

### 1. Single-AZ Deployment (Standard Option)

- The **Application (APP) and Database (DB) EC2 instances** are launched in the same **Availability Zone (AZ)**.
- This option is cost-effective and suitable for **non-critical workloads** or **development/test environments**.

### 2. Multi-AZ Deployment (High Availability)

- The CloudFormation template provisions EC2 instances across **multiple Availability Zones**, ensuring redundancy and **fault tolerance**.

### 3. Multi-Region Deployment (Disaster Recovery - Optional)

- Customers can manually deploy the CloudFormation template in **multiple AWS Regions** to ensure business continuity.
- **Cross-Region data replication**, such as **S3 replication or AWS Backup cross-region snapshot copies**, can be configured as needed.

### Automated Backup Solution

- A **separate CloudFormation template** is provided to automate the backup of **APP and DB EC2 instance** using **AWS Backup**.
- The backup plan includes:
  - **Configurable backup frequency** (hourly, 12-hour, or daily snapshots).
  - **A Backup Vault** to securely store snapshots.
  - **IAM roles** to manage automated backups efficiently.

Customers can select the most suitable deployment model during CloudFormation stack creation, ensuring **scalability, reliability, and flexibility** based on their operational needs.

## 1.4 Deployment Time Estimation

The deployment of the Sigma APP&DB AMI using the provided CloudFormation template from the S3 bucket is expected to take approximately 5 to 10 minutes. Additionally, once the environment setup and deployment are completed, you may execute the optional CloudFormation template for automating APP & DB EC2 instance backups, which may require an additional 10 minutes.

The total deployment time may vary depending on **instance provisioning speed, network conditions, and AWS service availability**.

## 1.5 Supported AWS Regions

The **Sigma Product AMIs** are currently supported in the following AWS region:

- **ap-southeast-1 (Singapore)**

Customers should ensure that they deploy the AMI in the supported region. If deployment is required in other AWS regions, they can contact the **product support SPOC**. Future regional expansions may be considered based on customer demand.

# 2. Prerequisites and Requirements

## 2.1 Technical Prerequisites and Deployment Requirements

The deployment of the **Sigma Product** requires the following prerequisites:

**1. AWS Infrastructure Requirements**

- **AWS Account** with necessary permissions to deploy EC2 instances and CloudFormation stacks.
- **Amazon EC2 Key Pair** for secure SSH access to instances.

**2. Supported Operating System**

- The **APP&DB AMI** is based on **Ubuntu 24.04 LTS**.
- Customers do not need to install an OS manually as the AMIs come pre-configured.

**3. Instance Requirements**

- **Application &DB Server (APP & DB AMI)**:
    - Default instance type: **t3.xlarge** (configurable during deployment).
    - Minimum **4 vCPUs** and **16 GB RAM** recommended.
    - Pre-configured **MySQL database** with a minimum **200 GB EBS volume**.

**4. Network and Security Requirements**

- **VPC and Subnets**: The instances must be deployed within an existing AWS VPC.
- **Security Groups**:
    - **APP Security Group** allows **SSH (22) and HTTP (8080)** access.
    - **DB Security Group** allows **MySQL (3306) connections** from the APP server.

Customers should review these requirements before deploying the CloudFormation template to ensure a smooth deployment process.

## 2.2 Prerequisite Skills and Knowledge for Deployment

To successfully deploy the Sigma Product using the provided CloudFormation templates, users should have familiarity with the following AWS services and concepts:

**1. AWS Infrastructure & CloudFormation**

- Understanding of AWS EC2, VPCs, Security Groups, and IAM roles.

- Basic knowledge of AWS CloudFormation to launch and manage the deployment stack.

**2. Linux and SSH Access**

- Ability to connect to EC2 instances using SSH with an existing AWS Key Pair.
- Basic Linux command-line knowledge for troubleshooting and application management.

**3. Database Management (For DB Users)**

- Familiarity with MySQL database administration, including connections, configurations, and backups.

**4. AWS Backup and Recovery (Optional)**

- If the optional AWS Backup automation template is deployed, knowledge of AWS Backup policies and snapshot management is helpful.

No programming skills are required, but users should be comfortable navigating the AWS Management Console and running basic CLI commands if needed.

## 2.3 Environment Configuration Requirements

The deployment of the **Sigma Product** requires the following environment configurations:

**1. AWS Account Requirements**

- An active **AWS account** with permissions to launch EC2 instances and create CloudFormation stacks.
- An **existing Key Pair** for SSH access to instances.

**2. Supported Operating System**

- The **APP & DB AMI** are based on **Ubuntu 24.04 LTS**.
- Customers do not need to install an OS manually as the AMIs come pre-configured.

**3. Instance Configuration**

- **Application and DB Server (APP & DB AMI)**
  - Default instance type: **t3.xlarge** (configurable).
  - Minimum **4 vCPUs** and **16 GB RAM** recommended.
  - Preconfigured **MySQL database** with a minimum **100 GB EBS volume**.

**4. Networking & Security**

- The deployment requires an **existing AWS VPC**.
- Security Groups will be automatically created to allow:
  - **SSH access (port 22)** for management.
  - **HTTP access (port 8080)** for the application.
  - **MySQL access (port 3306)** between the application and database.

**5. DNS and Licensing**

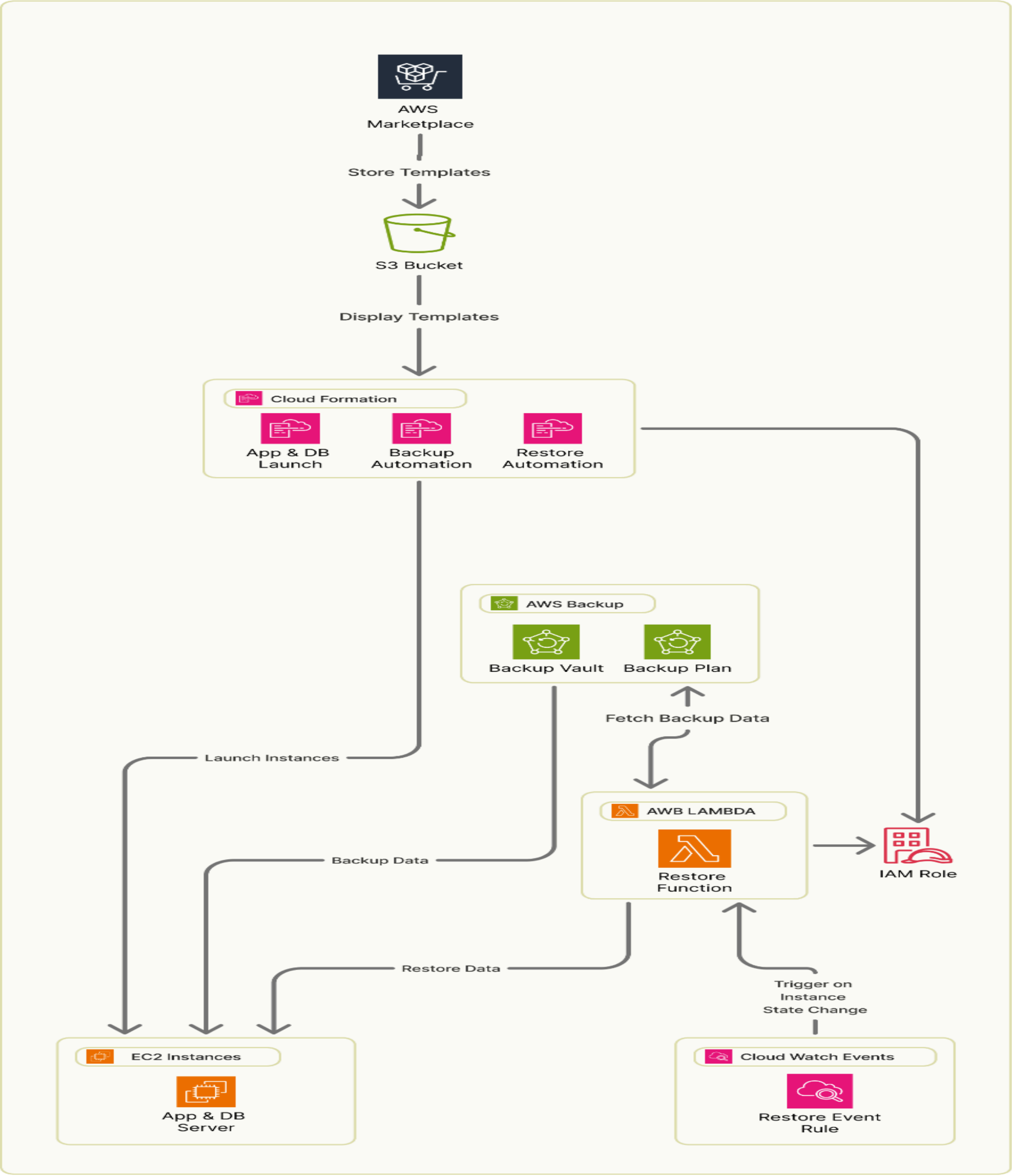
- The AMIs are licensed under **AWS Marketplace terms**, and no additional licensing is needed.

**6. Optional Backup Configuration**

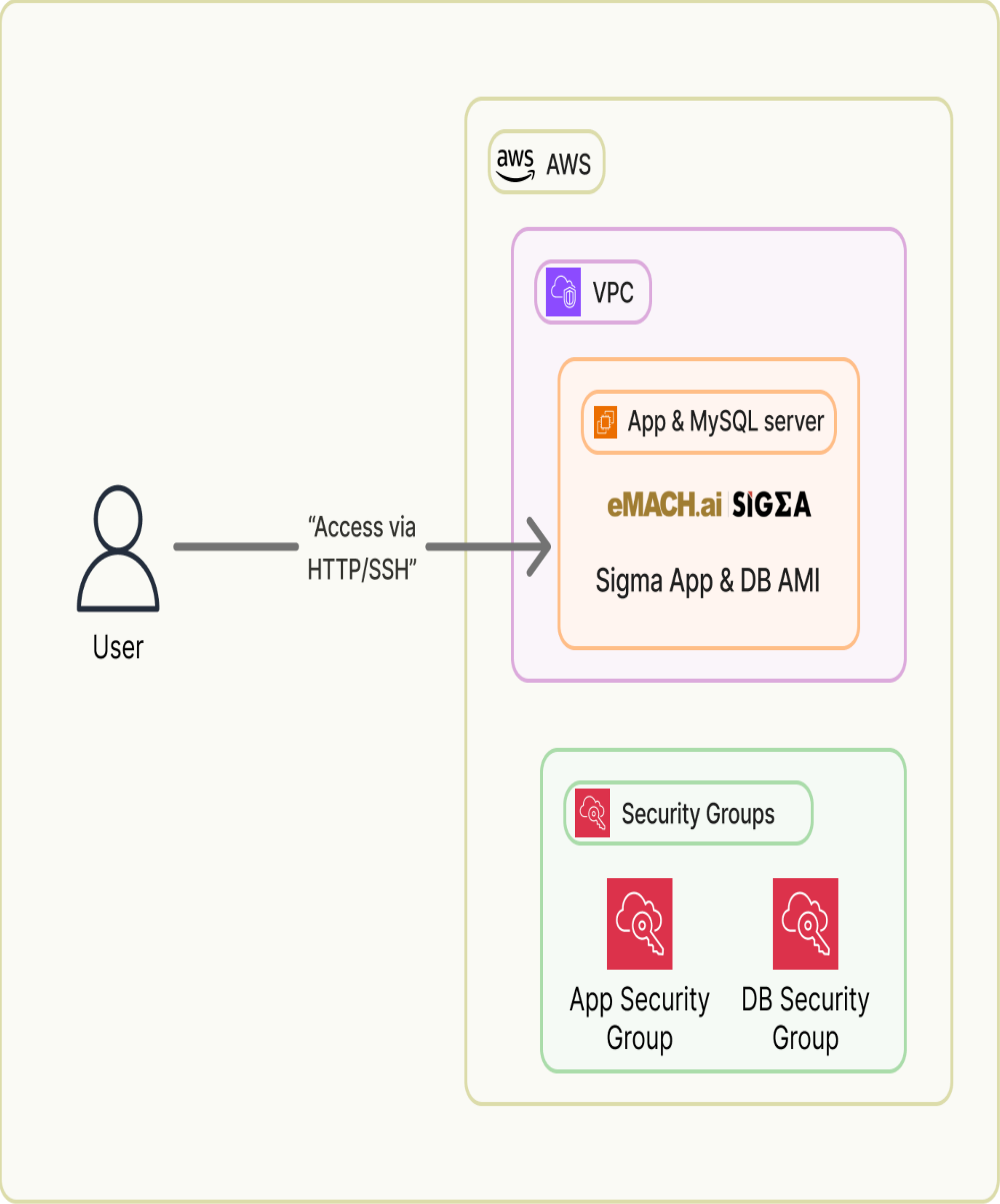
- Customers can deploy an **optional CloudFormation template** to configure **AWS Backup** for automated instance snapshots.

# 3. Architecture Diagram

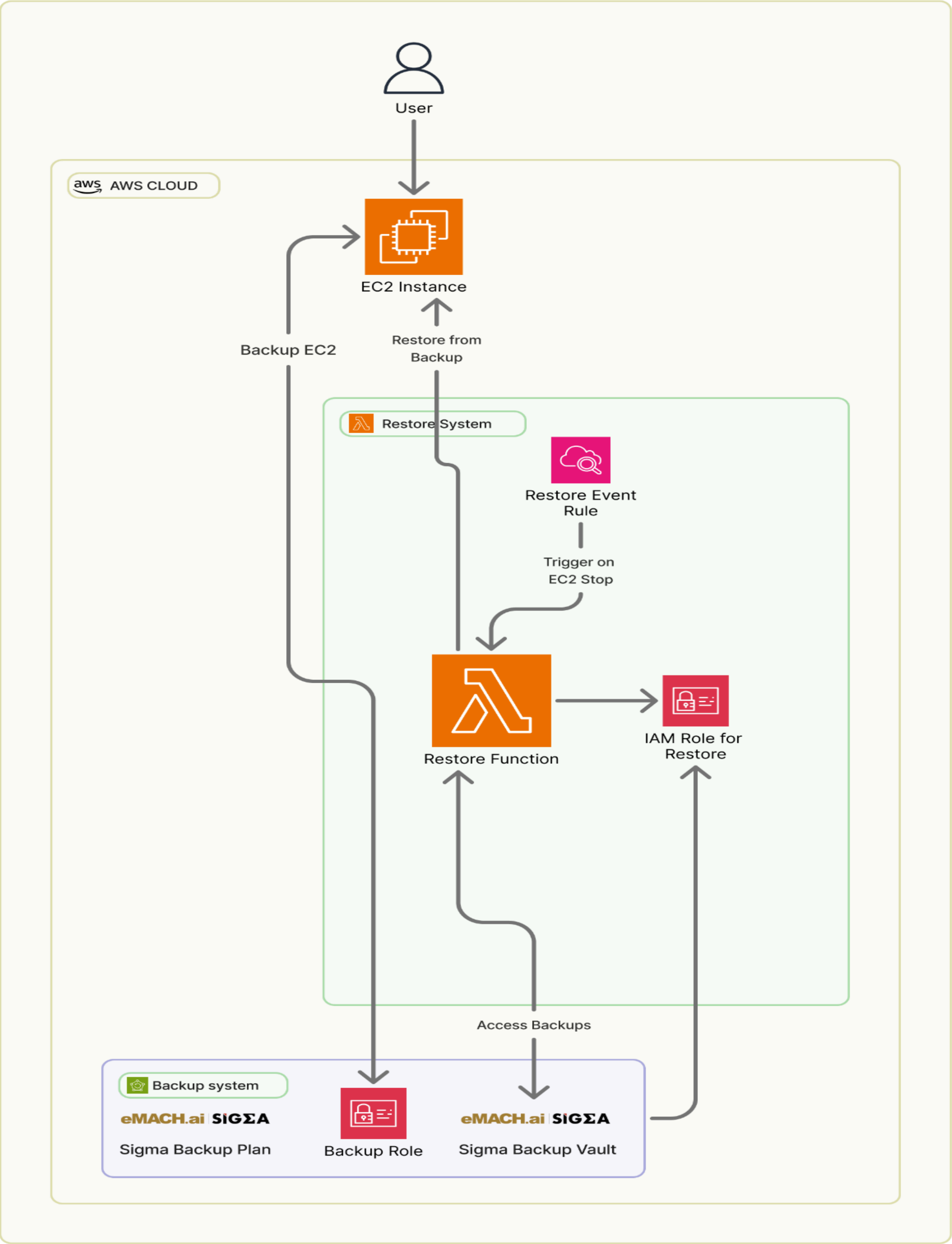
## 3.1 Sigma AMI Overview Architecture Diagram



### 3.2 Sigma AMI deployment Architecture Diagram



## 3.3 Sigma AMI Backup and Recovery Architecture Diagram



# 4. Security

## 4.1 AWS Root Privileges Requirement

The Sigma Product does not require AWS root account privileges for deployment or operation.

- The CloudFormation template provisions the required AWS resources using IAM roles and standard user permissions.
- EC2 instances are launched with least privilege security principles, ensuring they only have access to the necessary AWS services.
- Customers can deploy the application using an AWS IAM user with administrative privileges on EC2, S3, and CloudFormation, without requiring root account access.

This ensures secure deployment while following AWS best practices for IAM and least privilege access.

## 4.2 Policy of Least Privilege in Deployment

The **Sigma Product** deployment guide follows the **principle of least privilege** by ensuring that:

- **IAM permissions** are limited to only the required AWS services.

- The **EC2 instance** (APP & DB) runs with the **minimum necessary permissions**, without administrative or root-level access to AWS resources.

- **Security groups** restrict access to only necessary ports (**SSH (22), HTTP (8080), MySQL (3306)**), ensuring controlled network communication.

- The **optional AWS Backup automation** CloudFormation template uses **IAM roles with scoped permissions** to handle backups securely.
- Customers are advised to **deploy using IAM users with appropriate EC2, CloudFormation, and S3 permissions**, rather than using the AWS root account.

## 4.3 Public Resources in Deployment

The Sigma Product deployment does not create any public resources that expose sensitive data.

- The CloudFormation template does not provision any public S3 buckets or objects with unrestricted access.
- The EC2 instances (APP & DB) are deployed within a VPC, and security groups control access.
- Security Groups allow necessary ports (SSH (22), HTTP (8080), and MySQL (3306)), but customers are advised to modify rules based on their security policies.
- The optional AWS Backup automation does not require public resource access.

### 4.4 IAM Roles and Policies in the CloudFormation Templates

❖ **SigmaApp_AMI_Launch.yaml**

This template provisions the **Application Server and Database Server in a single EC2 instance**.

- **IAM Role Not Required:** This template does not create or require an IAM role.
- **Security Access:** Access is controlled via **Security Groups**, which allow:
  - **Port 22 (SSH)** for administrative access.
  - **Port 8080 (HTTP)** for the application.
  - **Port 3306 (MySQL)** for database connectivity.

❖ **Sigma_Backup_Automation.yaml**

This template provisions **AWS Backup** for automatic EC2 instance snapshots.

- **IAM Role Created:**
  - **Role Name:** `BackupRole`
  - **Purpose:** Grants AWS Backup service permissions to create, manage, and delete EC2 snapshots.
- **Policy Attached:**
  - **Permissions:**
    - `ec2:Describe*` – Allows reading instance details.
    - `ec2:CreateImage` – Enables EC2 snapshot creation.
    - `ec2:DeregisterImage` – Allows removal of old AMIs.
    - `ec2:StopInstances / StartInstances /`

      RebootInstances – Required for backup operations.
    - ec2:CreateTags / DeleteTags – Enables proper backup tagging and cleanup.
- **Security Considerations:**
  - The IAM policy follows **least privilege principles**, allowing only necessary backup operations.

### ❖ Sigma_Recover_Automation.yaml

This template provides **AWS Backup Recovery** and **Lambda-based EC2 instance restoration**.

- **IAM Role Created:**
  - **Role Name:** IAMRoleForRestore
  - **Purpose:** Grants permissions to AWS Backup and Lambda for restoring EC2 instances.
- **Policies Attached:**
  - **Permissions for AWS Backup:**
    - backup:ListBackupJobs – Lists available backups.
    - backup:DescribeBackupJob – Retrieves details about a specific backup.
    - backup:DescribeRestoreJob / backup:StartRestoreJob – Allows restoring EC2 instances.
  - **Permissions for EC2 Management:**
    - ec2:DescribeInstances / DescribeImages / StartInstances / StopInstances / RunInstances – Needed for launching a restored instance.
  - **Permissions for IAM PassRole:**
    - iam:PassRole – Allows the backup process to assume the required IAM role.
- **Security Considerations:**
  - The role is **restricted to backup and restore operations**, ensuring no unnecessary access is granted.

## 4.5 Key Creation and Usage

The Sigma Product deployment guide provides clear instructions on the creation and usage of necessary keys:

- **EC2 Key Pair:**
  - The user must create or use an existing AWS EC2 Key Pair to enable secure SSH access to the deployed APP&DB instance.
  - This key pair is specified in the CloudFormation template parameter (`KeyName`) and is required during deployment.
  - The private key (`.pem` file) is stored locally by the user and should be kept secure, as it is needed for SSH access.
- **AWS Backup Encryption Keys (Optional):**
  - If the optional AWS Backup automation template is deployed, AWS Backup may use AWS-managed encryption keys for data protection. ○ The deployment guide provides guidance on managing encryption settings if needed.

## 4.6 APP & Database Credentials Management

The **APP DB AMI contains pre-configured credentials**, which are securely stored within the instance and **not exposed externally**.
These credentials are necessary for initial setup, and customers are advised to **rotate them after deployment** for enhanced security.

## 4.7 Storage of Customer Data

- Application Data: Stored on the Application Server’s (EC2 - APP AMI) attached Amazon EBS volume.
- Database Data: Stored on the Database Server’s (EC2 - APP DB AMI) attached Amazon EBS volume in the default MySQL data directory (`/var/lib/mysql`). ● Backup Data (Optional): If the AWS Backup automation template is deployed, snapshots of both EC2 instances (APP DB) are stored in AWS Backup Vault.

## 4.8 Data Encryption Configuration

### 1. Amazon Elastic Block Store (EBS) Encryption

- The **Application Server and Database Server (EC2 - APP & DB AMI)** use Amazon EBS for storage.
- **Encryption Mechanism:**
  - **AWS Key Management Service (KMS) encryption** can be enabled for EBS volumes.
  - EBS encryption applies to **both root and attached data volumes**. ○ Snapshots created by AWS Backup are **automatically encrypted** if EBS encryption is enabled.
- **Configuration:**
  - Customers can **enable EBS encryption** in the CloudFormation template or manually in the AWS console.

### 2. Amazon S3 Encryption (For CloudFormation Templates & Backup Storage)

- If customers store application-related data in **Amazon S3**, encryption is recommended.
- **Encryption Options:**
  - **SSE-S3** (Amazon S3 Managed Keys) – Default encryption with Amazon-managed keys.
  - **SSE-KMS** (AWS Key Management Service) – Allows customers to control encryption keys via KMS.
  - **SSE-C** (Customer-Managed Keys) – Customers provide and manage their own encryption keys.
- **Configuration:**
  - Customers can **enable default encryption** at the S3 bucket level in the AWS Management Console.
  - Encryption settings should be **configured in S3 bucket policies**.

### 3. AWS Backup Vault Encryption (For EC2 Instance Backups)

- If the **Sigma_Backup_Automation.yaml** template is used, EC2 instance snapshots are stored in **AWS Backup Vault**.
- **Encryption Mechanism:**
  - AWS Backup **automatically encrypts all stored backups** using **AWS KMS keys**.
  - Customers can choose to **use AWS-managed keys** or **provide their own KMS keys**.

- **Configuration:**
    - Customers can **modify the AWS Backup Vault settings** to specify a **custom KMS key** for encryption.

**4. Linux Unified Key Setup (LUKS) for File System-Level Encryption**

- The **Sigma Product** does not enable **LUKS encryption** by default, but customers can configure **LUKS** manually for additional security.
- **Configuration Steps (Optional):**

## 4.9 Network Configuration in Deployment

The Sigma Product deployment guide includes detailed information on network configuration, covering VPCs, subnets, security groups, network ACLs, and route tables. The provided CloudFormation templates automate the setup of these network components to ensure secure and controlled deployment of the APP and DB instances.

## 4.10 Disabling Instance Metadata Service Version 1 (IMDSv1)

✔ IMDSv1 is disabled by default to prevent unauthorized metadata access.

✔ IMDSv2 is enforced for all EC2 instances deployed by CloudFormation.

# 5. Costs

## 5.1 Billable AWS Services and Cost Details

**1. Mandatory Billable Services**

These services are essential for deploying the application and database:

- **Amazon EC2**: Required for running the **APP & DB instance**. Charged based on **instance type and running hours**.
- **Amazon EBS**: Provides persistent storage for EC2 instances. Billed per **provisioned GB per month**.
- **Amazon VPC**: Ensures secure networking. Basic usage is free, but **NAT Gateway and VPC endpoints incur charges**.

**2. Optional Billable Services**

These services provide additional functionality but are not required for deployment:

- **AWS Backup**: Used for automated EC2 instance snapshots. Billed based on **backup storage and retention period**.
- **Amazon CloudWatch**: Provides logging and monitoring. **Basic monitoring is free**, but **custom metrics and log storage incur charges**.
- **AWS Data Transfer**: Charges apply for **outbound data beyond 1GB/month** or **cross-region transfers**.

**3. Cost Optimization Guidance**

- Customers can **choose smaller EC2 instances** to reduce compute costs.
- **AWS Backup can be disabled** to avoid storage costs.
- **Limiting outbound data transfers** helps minimize additional network charges.

The deployment guide ensures customers understand **expected billing impacts** and how to **optimize costs** when deploying the **Sigma Product**.

# 5.2 The cost model and licensing costs.

**1. AWS Infrastructure Costs**

### Amazon EC2 (Elastic Compute Cloud)

- **Purpose:** Runs the **APP and DB instance** using AMIs.
- **Mandatory/Optional: ✅ Mandatory**
- **Billing Details:**
  - Billed based on **instance type, running hours, and region**.
  - Example: **t3.xlarge costs ~$0.1668/hour** in `ap-southeast-1`.
  - **Stopping instances reduces costs**, but EBS storage is still charged.

### Amazon EBS (Elastic Block Store)

- **Purpose:** Provides storage for EC2 instances.
- **Mandatory/Optional: ✅ Mandatory**
- **Billing Details:**
  - Billed based on **storage provisioned (GB/month)**.
  - Example: **100 GB gp3 volume costs ~$8.00/month** in `ap-southeast-1`.

### Amazon VPC (Virtual Private Cloud)

- **Purpose:** Provides networking for EC2 instances.
- **Mandatory/Optional: ✅ Mandatory**
- **Billing Details:**
  - Free for basic use.
  - **NAT Gateway ($0.045/hour)** and **VPC endpoints ($0.01/GB)** may incur additional costs.

### AWS Backup (Optional)

- **Purpose:** Automates **EC2 backup snapshots**.
- **Mandatory/Optional: ⚡ Optional**
- **Billing Details:**
  - Billed based on **backup storage and retention period**.
  - Example: **$0.05/GB for backup storage** and **$0.01/GB for cross-region copies**.

**2. Licensing Costs**

- The APP and DB AMIs are published under the AWS Marketplace Bring Your Own License (BYOL) model.
- Customers only pay for AWS infrastructure costs and do not incur additional licensing fees for the AMIs.

# 6. Sizing

## 6.1 Provisioning Scripts and Resource Selection Guidance

The **Sigma Product** deployment provides CloudFormation **templates** that automate the provisioning of all required AWS resources, eliminating the need for manual setup.

- The **SigmaApp_AMI_Launch.yaml** CloudFormation template provisions:
  - **Application Server and Database Server (EC2 - APP &DB AMI)**
  - **Security Groups** to control access
  - **Amazon EBS Volumes** for storage
  - **VPC Configuration (if required)**

- The **Sigma_Backup_Automation.yaml** template (optional) provisions:
  - **AWS Backup configuration** for EC2 instance snapshots
  - **Backup Vault and Backup Plans** with configurable retention policies

Additionally, the **deployment guide provides recommendations** on selecting appropriate resource types and sizes based on workload requirements:

- **EC2 Instance Types:**
  - The default instance type is **t3.xlarge**, but customers can choose **t3.medium** or **t3.large** based on performance needs and cost considerations.
- **Database Instance Types:**
  - Default type is **t3.xlarge**, with options to use **t3.medium** for cost efficiency or **r5.large** for high-memory workloads.
- **EBS Storage:**
  - Default volume size is **100GB gp3**, which can be adjusted based on application storage requirements.

The deployment guide ensures that customers can **either use the pre-configured CloudFormation scripts** or **customize resources** based on their specific needs, ensuring **scalability and cost optimization**.

# 7. Deployment Assets

## 7.1 Step-by-Step Deployment Instructions

The **Sigma Product** deployment guide provides **step-by-step instructions** to deploy the application and database on AWS using the **CloudFormation template**.

### 1. Prerequisites

Before deployment, ensure the following:

- An **AWS account** with necessary permissions.
- A **pre-existing EC2 Key Pair** for SSH access.

### 2. Deployment Steps

#### Step 1: Subscribe to the Product on AWS Marketplace

1. Navigate to the **AWS Marketplace** and search for **Sigma Product**.
2. Click on the **Sigma Product listing**.
3. Review the product details, pricing, and supported regions.
4. Click **Continue to Subscribe** and accept the terms.

#### Step 2: Deploy Using CloudFormation

1. Click **Continue to Configuration** and select the appropriate **AWS Region** for deployment.
2. Click **Continue to Launch**, then choose **Launch CloudFormation** as the deployment method.
3. Click **Launch** to open the AWS CloudFormation console.

#### Step 3: Configure the CloudFormation Stack

1. On the **Create Stack** page, ensure the correct template (`SigmaApp_AMI_Launch.yaml`) is pre-loaded.
2. Enter the **Stack Name** (e.g., `SigmaDeployment`).

3. Provide the required **parameters**:
    - **Instance Type** (Default: `t3.xlarge`, but can be customized).
    - **EC2 Key Pair** (To enable SSH access).
    - **VPC and Subnet Selection** (If applicable).
4. Click **Next**.

### Step 4: Set Deployment Options

1. Configure stack options (logging, IAM roles, and tags).
2. Click **Next** and review all settings.
3. Acknowledge the necessary IAM permissions.
4. Click **Create Stack** to start the deployment process.

### Step 5: Monitor Stack Creation

1. Wait for the CloudFormation stack status to change to **CREATE_COMPLETE**.
2. Once completed, navigate to the **Outputs** tab in the CloudFormation console to find:
    - **Application URL** (to access the deployed Sigma Product).
    - **Database Connection Details** (if applicable).

### 3. Accessing the Application

After successful deployment, the application can be accessed using the public IP from the CloudFormation Outputs:

```
SigmaAppURL: http://<Public-IP>:8080/sigma

StudioAppURL: http://<Public-IP>:8080/expertctstudio
```

Use SSH to connect to the instance for further configurations:

```
ssh -i <Your-Key.pem> ec2-user@<Public-IP>
```

### 4. Optional: Enabling Automated Backups

- If **AWS Backup** automation is required, customers can deploy the optional **Sigma_Backup_Automation.yaml** CloudFormation template.
- This template enables **scheduled EC2 instance snapshots** for disaster recovery.

## 7.2 Testing and Troubleshooting Guidance

The **Sigma Product** deployment guide includes **prescriptive guidance** for **testing and troubleshooting** the deployment to ensure smooth operation.

### 1. Post-Deployment Testing

After deploying the CloudFormation template, customers should verify:

**Application Accessibility:** Access the Sigma application using the provided URL which are mentioned in CloudFormation stack output

**Database Connectivity:** Ensure that the **DB server** connectivity by using 3306 port number.

### 2. Common Troubleshooting Scenarios

If issues occur, follow these troubleshooting steps:

**�� Issue: Cannot Access the Application**

- Verify that the **EC2 instance is running** in the AWS console.
- Check the **Security Group settings** to ensure **port 8080 is open**.

**�� Issue: Database Connection Fails**

- Ensure the database **EC2 instance is running**.
- Verify that **port 3306 is open** in the security group.
- Use the **MySQL CLI** to test connectivity.

**�� Issue: CloudFormation Stack Fails to Create**

- Check the **CloudFormation Events tab** for failure reasons.
- Verify **IAM permissions** for CloudFormation execution.

### 3. AWS Backup Validation (Optional)

For customers using **AWS Backup automation**, verify:

- **Backup plans are created** in the AWS Backup console.
- **Snapshots are stored** in the designated Backup Vault.

# 8. Health Check

## 8.1 Assessing and Monitoring Application Health

Customers can verify the application's health by accessing the following URL:

Sigma health check url: http://<Public-IP>:8080/sigma

Studio health check url: http://<Public-IP>:8080/expertctstudio

# 9. Backup and Recovery

## 9.1 Data Stores to be Backed Up

The **Sigma Product** consists of the following data stores:

- **Sigma Application Server (EC2 - APP&DB AMI)**
  - Stores application files and configurations on the attached **Amazon EBS volume**.
- **Sigma Database Server (EC2 - APP&DB AMI)**
  - Stores **MySQL databases** (e.g., `sigma` and `ctstudio`) on the **EBS volume**.
  - The database configuration is stored in **`/var/lib/mysql`**.

To prevent data loss, **EC2 instance (Application & Database servers)** should be included in a backup plan.

## 9.2 Backup Configuration (Automated via AWS Backup)

Customers can use the **optional CloudFormation template** (`Sigma_Backup_Automation.yaml`) to automate EC2 instance backups.

- **Backup Vault**: Stores EC2 snapshots securely.
- **Backup Plan**: Automates scheduled snapshots for APP and DB instances.
- **Backup Frequency** (Configurable in CloudFormation parameters): ○ **Hourly**: `cron(0 */1 * * ? *)`
  - **Every 12 hours**: `cron(0 0/12 * * ? *)`

  - **Daily (Default Setting)**: `cron(0 0 * * ? *)`
- **Retention Period**: Default **7 days** (configurable).

# 10. Routine Maintenance

## 10.1 Credential and Key Rotation

- The deployment guide primarily focuses on using CloudFormation templates to deploy APP& DB AMI to AWS Marketplace, with the templates stored in an S3 bucket.

- Customers should **rotate EC2 key pairs periodically** to enhance security.

- As a result, the deployment guide does not include instructions for rotating such credentials or keys.
- Additionally, an optional CloudFormation template is provided to automate the backup of APP and DB EC2 instances.
- Since there are no cryptographic keys or programmatic credentials involved, no rotation instructions are necessary within the guide.

## 10.2 Software Patches and Upgrades

- The Sigma solution does not require regular software patches or upgrades for the AMI or CloudFormation templates.
- Software patches or upgrades will only be provided if an issue occurs in the Sigma product that requires an update.
- However, as part of the deployment process, we provide detailed instructions for launching the Sigma APP&DB EC2 instance and configuring the necessary security groups.
- Additionally, we offer an optional CloudFormation template to automate the backup of the Sigma APP&DB EC2 instance, ensuring continuous operational integrity.
- If a software patch or upgrade is required due to an issue, please contact the Sigma product support team, who will provide the necessary guidance.

## 10.3 Managing Licenses in Deployment

The Sigma Product does not require a separate software license as it is published on AWS Marketplace using a Bring Your Own License (BYOL) model. Customers are only responsible for the AWS infrastructure costs associated with running the deployed instances.

**1. AWS Licensing Model**

- The APP and DB AMIs are provided without additional software licensing costs.
- Customers are charged only for AWS resources used, including:
    - EC2 instance hours
    - EBS storage
    - Optional AWS Backup service

**2. License Management Considerations**

- No license activation, subscription, or additional licensing fees are required for deploying Sigma Product.
- Customers should review AWS service pricing to estimate operational costs. ● Future enhancements may include integrating AWS License Manager to track license usage if required.

## 10.4 Managing AWS Service Limits

AWS Service Limits Considered in Deployment

Customers deploying the Sigma Product should be aware of the following AWS service quotas:

- EC2 Instance Limits:
    - AWS enforces limits on the number of EC2 instances per region.
    - Customers should check their EC2 quota and request an increase if needed before deployment.
- Amazon EBS Volume Limits:
    - The deployment provisions encrypted EBS volumes for the APP and DB servers.
    - Customers should verify their EBS storage quota to ensure sufficient capacity.
- VPC and Security Group Limits:
    - Each AWS account has a limit on the number of security groups per VPC

and inbound/outbound rules per security group.

    - Customers should confirm they have enough available security group rules for deployment.

# 11. Emergency Maintenance

## 11.1 Handling Fault Conditions

The Sigma Product deployment guide provides clear instructions for handling fault conditions to ensure system reliability and resilience. Fault-handling mechanisms focus on instance availability, connectivity issues, and backup recovery.

**1. Instance Availability and Self-Healing**

- The deployment uses **Amazon EC2 instances** for the **Application Server and Database Server (APP&DB AMI)**.
- Customers can enable **EC2 Auto Recovery** to automatically restart instances if they fail due to hardware issues.
- **Alternative Solution:** Customers can configure **AWS Auto Scaling** for high availability

**2. Connectivity and Network Issue Resolution**

If the **Sigma Application or Database Server becomes unreachable**, customers should check the following:

1️⃣**Security Groups & Network ACLs**

- Ensure **Security Group rules allow inbound traffic** on:
    - **Port 8080 (HTTP) for the application**
    - **Port 3306 (MySQL) for the database**
- Validate **Network ACL settings** do not block required traffic.

2️⃣**Instance Reachability Checks**

Use AWS Systems Manager or SSH to connect to the instance:

Run the following command to check instance status:

**3. Backup and Recovery (Optional AWS Backup Automation)**

- Customers using the **Sigma_Backup_Automation.yaml** template can restore instances using AWS Backup.

**4. Application-Level Fault Handling**

If the application is **not responding**, restart the Tomcat service

**5. Best Practices for Fault Recovery**

✔ **Use AWS CloudWatch** to monitor EC2 instance health and configure alarms.

✔ **Restrict Security Groups and IAM roles** to minimize unauthorized access.
✔ **Test application failover and recovery procedures periodically.**

## 11.2 Recovering the Software

**1. Recovery Process Overview**

- Customers can recover the Application Server and Database Server (APP&DB AMI) using the Sigma Backup and Recovery Automation CloudFormation templates.
- The Sigma_Backup_Automation.yaml template enables automated backups of EC2 instances.
- The Sigma_Recover_Automation.yaml template automates the restoration process in case of failure.

**2. Recovery Using AWS Backup (Automated Method)**

If AWS Backup is enabled, customers can restore EC2 instances as

follows: Step 1: Locate the Latest Backup

1. Navigate to AWS Backup Console → Backup Vaults.
2. Select SigmaBackupVault (created by the backup automation template).
3. Choose the most recent recovery point for the affected instance.

Step 2: Restore the Instance

1. Click Restore Backup and select EC2 as the resource type.
2. Choose the appropriate instance type (e.g., `t3.xlarge`).

3. Click Restore Backup to launch a new EC2 instance from the backup.

### 3. Recovery Using CloudFormation (Automated Failover Method)

The Sigma_Recover_Automation.yaml template can be deployed to restore the latest backup automatically.

Step 1: Deploy the Recovery Automation Template

1. Navigate to AWS CloudFormation Console.
2. Click Create Stack → With New Resources.
3. Upload the `Sigma_Recover_Automation.yaml` template.
4. Provide the required parameters:
   - EC2InstanceId: Instance ID of the affected server.
   - BackupVaultName: `SigmaBackupVault` (default).
   - RestoreInstanceType: Instance type for recovery (e.g., `t3.xlarge`).
5. Click Create Stack to initiate recovery.

Step 2: Monitor Recovery Progress

- The recovery Lambda function (`EC2RestoreLambdaFunction`) triggers the restore process.
- Customers can track the restoration in AWS Backup Console → Restore Jobs.
- Once the restoration is complete, the new instance details can be found in the CloudFormation Outputs section.

### 4. Manual Recovery (If Backup is Not Configured)

If AWS Backup is not enabled, customers must manually launch new instances using the original AMIs:

1. Navigate to AWS EC2 Console → Launch Instance.
2. Select the appropriate AMI ID from the AWS Marketplace.
3. Choose the required instance type (e.g., `t3.xlarge`).
4. Assign the correct VPC, Security Groups, and Key Pair.
5. Click Launch to create a new instance.
6. If necessary, manually restore database backups from external storage (if available).

# 12. Support

## 12.1 Receiving Supports

**1. Support Channels**

Customers can receive support through the following channels:

- AWS Marketplace Support: Customers can raise issues related to the AMI deployment directly through the AWS Marketplace support page.
- Product Documentation: A detailed deployment guide is provided to assist with installation, configuration, and troubleshooting.
- Email Support: Customers can contact the product support team via email at `[Support Email]` for any technical assistance.

**2. Scope of Support**

Support is available for:
✔ CloudFormation template deployment issues
✔ Configuration and setup of EC2 instances
✔ AWS Backup automation and recovery assistance
✔ Network and security group configurations
✔ Application and database connectivity issues

**3. Troubleshooting Steps Before Raising a Ticket**

Before reaching out for support, customers are encouraged to:

1. Review the Deployment Guide for step-by-step setup instructions.

2. Check AWS CloudFormation Stack Events to identify any error messages.

3. Verify Security Groups and IAM Permissions to ensure network connectivity.

4. Check EC2 Instance Logs (`/var/log/userdata.log`) for application-related errors.

**4. Business Hours and Response Time**

- Support is available Monday to Friday, from [Business Hours, e.g., 9 AM - 6 PM UTC].

- The response time for support queries is typically [Response Time, e.g., within 24 hours].

## 12.2 Technical Support Tiers

### 1. Support Tiers

Customers deploying the Sigma Product from AWS Marketplace can access the following levels of support:

- Basic Support (Community & Documentation-Based)
    - Customers can refer to the deployment guide and AWS Marketplace documentation for self-service troubleshooting.
    - Common issues, FAQs, and troubleshooting steps are provided in the deployment guide.
- Standard Support (Email-Based Assistance)
    - Customers can reach out to the support contact (SPOC) for assistance with deployment-related queries.
    - Response time varies based on the severity of the issue.
- Premium Support (Dedicated Assistance - Optional)
    - For customers requiring dedicated support, a separate support package can be arranged.
    - Includes personalized assistance for troubleshooting, best practices, and performance optimization.

### 2. Service Level Agreements (SLAs)

- Response Time SLA:
    - General inquiries: Response within 48 hours.
    - Deployment issues: Response within 24 hours.
    - Critical issues impacting availability: Response within 12 hours.
- Uptime & Availability:
    - The product itself does not include an SLA for infrastructure uptime, as it runs on customer-managed AWS resources.
    - Customers are advised to configure AWS Backup and recovery automation for high availability.

### 3. Escalation Process

- If an issue requires escalation, customers can contact the support SPOC via the email provided in the AWS Marketplace listing.
- For AWS infrastructure-related issues, customers should raise a support ticket with AWS Support.