架构方案

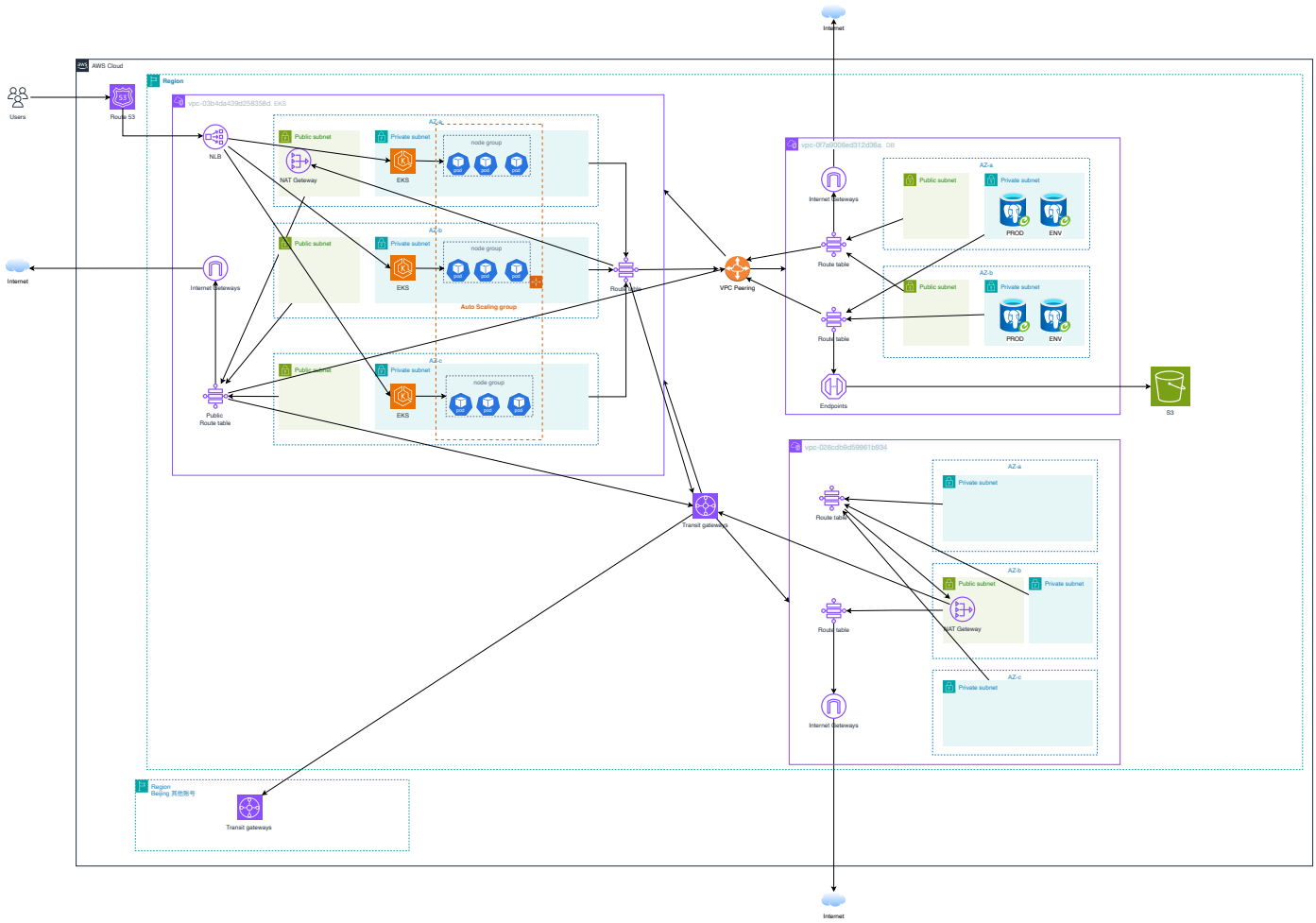
1. 引言

1.1 项目背景

本项目旨在利用AWS的云服务，构建一个支持现代应用程序的高可用和可扩展的Mendix平台。

1.2 目标与范围

1.2.1 平台网络现状



1.2.2 目标

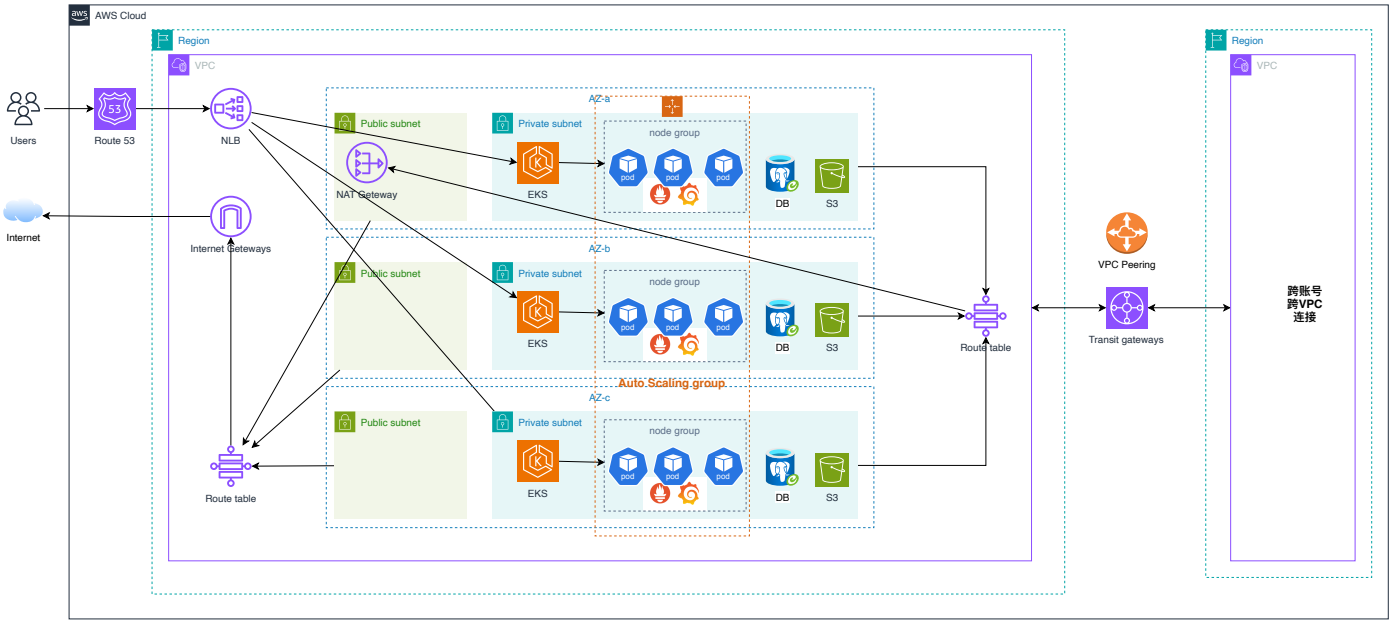
- **高可用性**：确保系统在任何情况下都能提供持续的服务，最大限度地减少停机时间。
- **可扩展性**：根据业务需求，动态调整资源以满足性能要求。
- **安全性**：保护数据和应用程序免受未经授权的访问和潜在的安全威胁。
- **易管理维护**：同一平台VPC管理、路由表网络配置。

1.2.3 范围

- **基础设施搭建**：构建基于AWS的云基础设施，包括计算、存储和网络资源。
- **应用部署**：使用Kubernetes进行应用的容器化和编排，确保灵活的部署和管理。
- **安全措施**：实施全面的安全策略，包括数据加密、访问控制和合规性管理。
- **监控与管理**：建立监控和日志系统，确保系统的可见性和可管理性。

2. 架构概述

2.1总体架构图



- **VPC**：包含公共和私有子网
- **负载均衡器**：Network Load Balancer
- **通信组件**： VPC Peering、Transit Gateways
- **计算资源**：Kubernetes集群
- **存储**：Amazon S3、EBS、RDS
- **安全组件**：IAM、KMS、Secrets Manager
- **监控与日志**：CloudWatch、Prometheus、Grafana、CloudTrail

2.2 基于现有架构调整方案1

2.2.1 方案说明

在现有账号下创建一套新的架构，再将旧架构的服务迁移至新的架构。

2.2.2 方案优势

- Route 53 无需配置DNS解析
- tgw网关 无需创建配置

2.3 基于新账号调整方案2

2.3.1 方案说明

在新账号下创建平台架构，再将旧账号的服务、数据迁移至新的架构。

2.2.2 方案优势

- 易管理、安全隔离、不影响现有系统

2.4 方案对比

比较维度	基于现有架构调整方案1	基于新账号调整方案2	备注
Route 53 创建	不需要	需要	
VPC 创建	需要	需要	
子网创建	需要	需要	
路由表、nat网关、igw网关 创建	需要	需要	
tgw网关 创建	不需要	需要	
EKS 创建	需要	需要	
EKS服务迁移	需要	需要	
EKS服务文件迁移	需要	需要	
节点组创建	需要	需要	
Load balance	需要	需要	
数据库创建	需要	需要	数据库不能更改vpc
数据库迁移	需要	需要	
安全组创建	需要	需要	控制网络访问白名单

2.5 结论

综上对比，需要创建的资源区别并不大，建议使用新账号进行平台创建。可以更好管理服务资源及进行安全隔离，同时不影响现有系统的运行。

2.6 设计原则

2.6.1 高可用性

- 部署在多个可用区，确保服务的连续性和可靠性。

- 使用自动故障转移和负载均衡来减少单点故障。

2.6.2 可扩展性

- 利用自动扩展组根据流量动态调整资源。
- 采用容器化技术，实现快速部署和扩展。

2.6.3安全性

- 实施最小权限原则，使用IAM进行细粒度访问控制。
- 加密静态和传输中的数据，确保数据安全。

2.6.4成本效益

- 使用按需资源和预留实例相结合的策略，优化成本。
- 定期审计资源使用情况，避免浪费。

2.6.5 可管理性

- 通过CloudWatch和CloudTrail进行全面的监控和日志记录。
- 提供自动化的备份和恢复解决方案。

2.6.6 灵活性

- 采用微服务架构，支持快速迭代和更新。
- 利用CI/CD管道实现持续集成和部署。

3. 网络架构

3.1 VPC设计

- **VPC**：创建一个隔离的虚拟网络环境，提供完整的控制权和安全性。
- **CIDR块**：选择适当的CIDR范围（如10.0.0.0/16），确保足够的IP地址空间。

3.2子网配置

- **公共子网**：
  - 部署需要互联网访问的资源，如负载均衡器。
  - 配置弹性IP以便于外部访问。
- **私有子网**：
  - 部署内部资源，如应用服务器和数据库。
  - 通过NAT网关访问外部互联网。

3.3 NAT网关和互联网访问

- **NAT网关**：
  - 部署在公共子网中，允许私有子网中的资源安全地访问互联网。
  - 提供高可用性和自动故障转移。
- **互联网网关**：
  - 附加到VPC，允许公共子网中的资源直接访问互联网。

3.4 路由配置

- **公共子网路由表**：
  - 配置默认路由指向互联网网关，支持外部访问。
- **私有子网路由表**：
  - 配置默认路由指向NAT网关，确保安全的互联网访问。
- **安全组和网络ACL**：
  - 使用安全组控制入站和出站流量，确保资源安全。
  - 网络ACL提供额外的流量过滤层，增强安全性。

4. 计算资源

4.1Kubernetes集群

- **EKS（Amazon Elastic Kubernetes Service）**：
  - 托管的Kubernetes服务，简化集群管理。
  - 部署在多个可用区，确保高可用性。
  - 支持自动化的集群升级和修补。
- **节点组**：
  - 使用EC2实例作为工作节点。
  - 配置节点组策略以适应不同的工作负载。

4.2自动扩展组（Auto Scaling Group）

- **自动扩展**：
  - 根据流量和负载自动调整节点数量。
  - 使用CloudWatch指标触发扩展和缩减策略。
- **策略配置**：
  - 设置最小和最大实例数量，确保资源充足。
  - 配置扩展冷却时间，避免频繁扩展和缩减。

4.3负载均衡（Network Load Balancer）

- **NLB**：

    - 提供高性能的流量分发，支持TCP和UDP协议。
    - 自动处理来自多个可用区的流量，增强可靠性。
- **配置**：
    - 将NLB与Kubernetes服务集成，实现流量的自动分发。
    - 配置健康检查，确保仅将流量发送到健康的实例。

5. 存储解决方案

5.1Amazon S3

- **用途**：
    - 用于存储静态文件、备份和日志。
    - 提供高可用性和持久性。
- **特性**：
    - 支持版本控制和生命周期管理。
    - 提供加密和访问控制，确保数据安全。

5.2 Amazon EBS

- **用途**：
    - 为EC2实例提供持久块存储。
    - 适用于需要低延迟的数据存储，如数据库。
- **特性**：
    - 支持快照备份和加密。
    - 提供不同的性能级别，适应多种工作负载。

5.3 Amazon RDS

- **用途**：
    - 提供托管的关系型数据库服务。
    - 支持多种数据库引擎，如 MySQL、PostgreSQL、Oracle。
- **特性**：
    - 自动备份和故障转移，确保高可用性。
    - 支持多可用区部署和加密，增强数据安全性。

6. 容器与镜像管理

6.1 Amazon ECR

用途：

- 托管Docker容器镜像，支持版本控制。
- 与EKS无缝集成，简化镜像部署。

特性：

- 提供安全的镜像存储和传输，支持加密。
- 支持基于IAM的访问控制。

6.2 CI/CD 集成

工具选择：

- 使用AWS CodePipeline、Jenkins或GitLab CI等工具进行持续集成和部署。

流程：

- 自动化构建、测试和部署流程。
- 代码提交后触发流水线，自动构建镜像并推送到ECR。
- 部署更新的镜像到EKS集群，确保快速迭代和发布。

最佳实践：

- 使用Blue/Green或Canary部署策略，降低发布风险。
- 配置自动回滚机制，确保在失败时快速恢复。

7. 安全管理

7.1访问控制（IAM）

用途：

- 管理用户和服务的访问权限。
- 实现细粒度的权限控制。

特性：

- 使用角色和策略，限制资源访问。
- 定期审计和更新权限，确保最小权限原则。

7.2数据加密（AWS KMS）

用途：

- 提供数据加密服务，保护静态和传输中的数据。

特性：

- 集成到S3、EBS、RDS等服务中。
- 管理加密密钥的生命周期和访问权限。

7.3密钥管理（Secrets Manager）

用途：

- 安全存储和管理敏感信息，如数据库凭证和API密钥。

特性：

- 支持自动轮换密钥，减少人为错误。
- 提供访问控制和审计日志，增强安全性。

7.4安全组和网络ACL

用途：

- 控制VPC内外的网络流量。

特性：

- 安全组：状态化防火墙，基于实例级别。
- 网络ACL：无状态防火墙，基于子网级别，提供额外的流量控制。

最佳实践：

- 定义明确的入站和出站规则。
- 定期审查和更新规则，确保符合安全需求。

8. 监控与日志

8.1 CloudWatch监控

用途：

- 提供实时监控和告警功能，跟踪资源使用情况。

特性：

- 收集和分析指标，如CPU使用率、内存、网络流量等。
- 设置自定义告警，及时响应异常情况。

最佳实践：

- 配置仪表板，集中查看关键指标。
- 使用CloudWatch Logs Insights进行日志分析。

8.2日志管理 CloudTrail

用途：

- 记录AWS账户中的API调用和活动。

特性：

- 提供审计和合规性支持。
- 帮助检测潜在的安全威胁。

8.3ELK（Elasticsearch, Logstash, Kibana）

用途：

- 实现集中化日志收集、存储和分析。

特性：

- Elasticsearch：高效存储和搜索日志数据。
- Logstash：灵活的数据处理和传输。
- Kibana：可视化和分析日志数据。

最佳实践：

- 设置日志索引策略，优化存储和性能。
- 创建可视化报表，帮助快速定位问题。

9. 成本管理

9.1成本优化策略

按需和预留实例结合使用：

- 根据工作负载需求，灵活使用按需和预留实例。
- 预留实例可用于长期稳定的工作负载，降低成本。

使用Auto Scaling：

- 自动调整实例数量以应对流量波动，避免资源浪费。

选择合适的存储类型：

- 根据数据访问频率选择合适的存储类型，如S3标准、S3智能分层等。

利用Spot实例：

- 对于非关键任务，使用Spot实例以降低计算成本。

优化数据传输：

- 减少跨区域数据传输，利用CloudFront等服务缓存内容。

9.2预算与监控

设置预算：

- 使用AWS Budgets设定和跟踪预算，及时发现超支风险。

成本和使用情况报告：

- 定期查看AWS Cost Explorer，分析使用情况和成本趋势。

启用成本分配标签：

- 使用标签对资源进行分类，便于成本分摊和分析。

自动化成本警报：

- 配置成本警报，自动通知相关人员，防止预算超支。

通过这些策略和工具，确保资源使用的高效性和成本的可控性。

10. 灾备与高可用

10.1多可用区设计

- **跨可用区部署**：
  - 在多个可用区中部署应用和数据库，确保高可用性。
  - 使用负载均衡器（如ALB或NLB）分发流量，避免单点故障。
- **自动故障转移**：
  - 配置自动故障转移机制，确保在一个可用区故障时，应用能继续运行。

10.2备份与恢复策略

- **定期备份**：
  - 使用AWS Backup或快照功能定期备份数据和配置。
  - 对关键数据和应用状态进行每日或每周备份。
- **版本控制和存档**：
  - 对重要文件和数据库启用版本控制，防止数据丢失。
  - 将长期备份存储在Amazon S3 Glacier，降低存储成本。
- **恢复演练**：
  - 定期进行恢复演练，确保备份可用且恢复流程高效。
- **灾难恢复计划**：
  - 制定详细的灾难恢复计划，包括RTO（恢复时间目标）和RPO（恢复点目标）。
  - 使用AWS Elastic Disaster Recovery等服务，实现快速恢复。

通过这些策略，确保系统在灾难情况下仍能保持高可用性和数据完整性。

11. 结论

11.1风险评估

- **技术风险**：
  - 系统故障：多可用区部署和自动故障转移可降低风险。
  - 数据丢失：定期备份和版本控制可确保数据安全。
- **成本风险**：
  - 超出预算：通过成本优化和监控工具进行管理。
- **安全风险**：

- 数据泄露：使用加密和访问控制措施保护数据。

11.2后续步骤

- **持续监控和优化**：
  - 定期评估系统性能和成本，进行优化调整。
- **安全审计**：
  - 定期进行安全审计，确保符合最佳实践。

12. 运维支持

#	Priority	Response Time	Solved Time
1	P1 (24*7)	30 mins	4 hour
2	P2 (24*7)	1 hour	6 hour
3	P3 (5*8)	2 hour	2 work days
4	P4 (5*8)	4 hour	3 work days

Level	Incident Impact	Typical Incidents
P1	System downtime or critical failure causes system to be unavailable	System aborted (cannot save work in progress) System functional failure results in data loss or system unavailability System functional failure causes system failure System failure causes critical task application to restart
P2	System performance is severely damaged, but the system is still working	Applications fail frequently without causing data loss Serious but predictable failures in the management system System performance is severely degraded
P3	System is operating normally and has only limited impact	System partial configuration modification
P4	Need information or support for product features, installation and configuration	System permissions issue Some conceptual answers System management issues

附录

术语表

- **VPC**：虚拟私有云，用于隔离网络资源。
- **NAT网关**：用于私有子网的互联网访问。
- **NLB**：网络负载均衡器，分发流量。
- **RDS**：关系数据库服务，提供托管数据库。
- **KMS**：密钥管理服务，用于数据加密。
- **Auto Scaling**：自动调整资源以匹配需求。
- **Route Tables**：路由表，控制流量从子网传递到其它子网或网络目标。

参考资料

1. AWS官方文档：AWS 文档
2. AWS架构最佳实践：AWS Well-Architected Framework

3. AWS成本管理指南：AWS Cost Management