

18 基于 Keycloak 的身份和访问控制系统

Keycloak on Amazon Web Services

行业：通用

技术：身份安全



1. 总体介绍

- 方案背景** 随着云计算的需求越来越强烈，客户需要高可用的身份管理系统来进行统一的身份管理、访问控制、鉴权和登录，帮助客户在 Amazon Web Services 上把已经建立好的用户 (user) 或身份 (identity) 带上云端来使用，并兼顾安全与管理的便利，让客户加速创新进入市场。
- 适用客户** 所有需要在云上进行身份管理的客户。
- 适用场景** 当客户期望快速构建身份管理系统，而 Amazon Cognito User Pool 或其他第三方产品无法满足客户需求时，即可使用该方案。
- 客户痛点** 在部分区域（如北京、宁夏、香港）尚未提供 Amazon Cognito User Pool 或 Amazon SSO 功能，客户无法进行身份管理；同时，客户对于身份管理系统运行在第三方网站存在安全顾虑，更不希望自己从头搭建一套身份管理系统，日后将面临运维的痛苦。

2. 客户价值

- (1) 安全：所有初始用户密码全部自动产生，并且存放在 Amazon Secrets Manager，由 IAM 控管。
- (2) 灵活部署：该方案同时提供 Amazon CloudFormation 与 CDK 两种部署方式。除了选择 Amazon CloudFormation 一键部署外，熟悉 CDK 的客户可依据项目提供的库进行二次开发、定制，或直接 CDK 部署。
- (3) 易于管理：所有服务全是无服务器架构，包括 Amazon Fargate 和 Amazon Aurora，客户不需要管理或维护任何一台 Amazon EC2 实例。
- (4) 高可用：所有服务全部采用冗余设计，不存在单点或单可用区故障导致服务中断的问题。
- (5) 完整覆盖：最大范围地满足客户的目标覆盖区域，可支持中国区域和全球区域。

3. 解决方案概要

- 方案概要** 该方案帮助客户快速在 Amazon Web Services 上构建高可用架构的 Keycloak 集群，以实现标准化的身份与访问控制系统。
- 方案特点** Keycloak 是一款开源的身份与访问控制软件，提供单点登录 (SSO) 功能，支持 OpenID Connect、OAuth 2.0、SAML 2.0 标准协议。Keycloak 提供可自定义的用户界面，用于登录、注册和账户管理等。客户可将其集成到现有的 LDAP 和 Azure Active Directory 服务器中，还可以将身份验证委派给第三方身份提供商。
- 部署前提** 无部署前提条件。客户没有任何基础（身份管理或者开发基础），也能快速搭建出演示或 POC 系统进行展示和验证。
- 客户资源/能力评估** 受场景和集成等因素影响，生产系统会相对复杂。使用托管服务搭建 POC 系统，工作量为 1~2 人天。对于其他场景则要根据实际情况具体分析。
- 成本因素** 该方案的运行成本主要来自三方面：ECS Fargate 计算服务、RDS 数据库服务、数据传输出站。以 Oregon 区为例：
- [案例 1]
- ECS Fargate: Linux x86, 利用率 24h/day, 2 tasks, 短暂存储量 (20 GB), 8GB Mem, 4 vcpu = 288.30 USD
- RDS MySQL: db.r5.large, 100GB gp2 磁盘, 利用率 24hr/day = 373.40 USD
- 数据传输出站: 500GB/月 = 45.00 USD
- 总计: 706.70 USD/月
- [案例 2]
- ECS Fargate: Linux x86, 利用率 24h/day, 2 tasks, 短暂存储量 (20 GB), 8GB Mem, 4 vcpu = 288.30

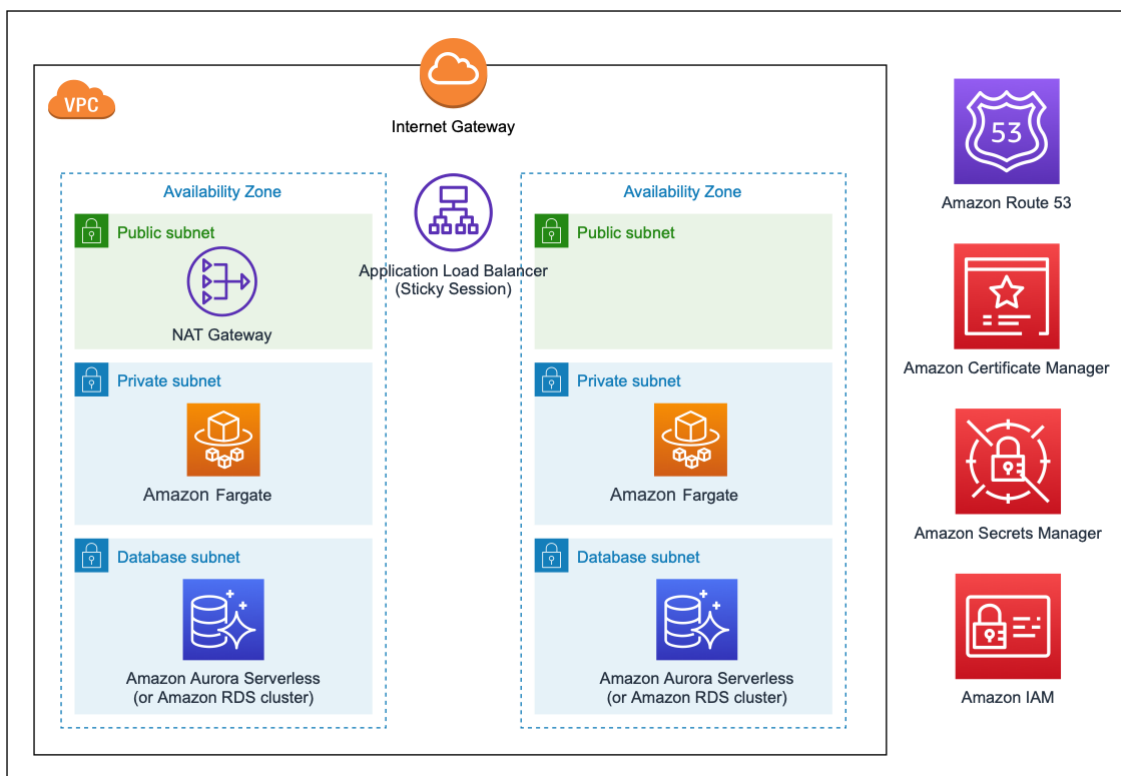
USD

Aurora Serverless MySQL: $4 * 24\text{hr} * 30\text{day} = 2880 \text{ ACU/月}$, 100GB 存储, baseline 30 rps, peek 100 rps, peek duration 60 每月 = 201.80 USD

数据传输出站: 500GB/月 = 45.00 USD

总计: 535.10 USD/月

4. 架构图



主要服务: Amazon Aurora、Amazon Certificate Manager (ACM)、Amazon Fargate、Amazon RDS、Amazon Route 53、Amazon Secrets Manager

5. 资源和帮助

官网 (中国) » <https://www.amazonaws.cn/solutions/keycloak-on-aws/>

部署手册 » https://s3.cn-north-1.amazonaws.com.cn/aws-dam-prod/china/Solutions/Keycloak_on_AWS/Deployment_guide_keycloak.pdf

GitHub » <https://github.com/aws-samples/keycloak-on-aws>

GitHub (CDK) » <https://github.com/aws-samples/cdk-keycloak>

PartnerCast: 构建与应用基于 Keycloak 的身份和访问控制系统 »

<https://explore.skillbuilder.aws/learn/course/internal/view/elearning/12925/aws-partnercast-gou-jian-yu-ying-yong-ji-yukeycloak-de-shen-fen-he-fang-wen-kong-zhi-xi-tong-technical>

YouTube 视频 (中文) » <https://www.youtube.com/watch?v=MO3oINUUOAI>

Keycloak 官网 » <https://www.keycloak.org/>

Active Directory 介绍 » <https://azure.microsoft.com/en-us/services/active-directory>

Twitter » <https://twitter.com/pahudnet/status/1372740745241583618/>

Campaign ID » SLV8-SIC-Mgmt-Ops-IAM-Keycloak on AWS

产品经理 施乔 (qiaoshi@amazon.com)

项目负责人 魏昌浩 (wch@amazon.com)

推广负责人 张濮 (puzhang@amazon.com)

SO8021 