

# 01-Install

2022年11月13日 10:45

<https://developer.hashicorp.com/terraform/downloads>



## Install Terraform

Install or update to v1.3.4 (latest version) of Terraform to get started.

### Operating System

1.3.4 (latest)

macOS **Windows** Linux FreeBSD OpenBSD Solaris

### Binary download for Windows

386

Version: 1.3.4

Download

AMD64

Version: 1.3.4

Download

设置path

Vs code下载HashiCorp Terraform

Aws config设置

init, Plan, apply, destroy

cmd中terraform --version确认

# 02-Provide main

2022年11月13日 11:02

```
terraform {
  required_providers {
    aws = {
      source = "hashicorp/aws"
      version = "4.39.0"
    }
  }
}

# Configure the AWS Provider
provider "aws" {
  region = "ap-northeast-1"
}
```

编辑main.tf

```
resource "aws_vpc" "kggvpc" {
  cidr_block      = "10.0.0.0/16"
  instance_tenancy = "default"
  tags = {
    Name = "teat vpc"
  }
}


resource "aws_subnet" "kgg" {
  vpc_id      = aws_vpc.kggvpc.id
  cidr_block = "10.0.1.0/24"
  tags = {
    Name = "test sb"
  }
}
```

执行terraform init #第一次需要预设值provide

执行terraform plan #模拟执行

## 03-variable変量

2022年11月13日 11:26

 variable.tf

```
variable "env" {  
    type = string  
    description = "xxx"  
    default = "prd"
```

```
}
```

```
variable "owner" {  
    type = string  
    description = "xxx"  
    default = "kgg"
```

```
}
```

# 04-data

2022年11月13日

12:03

引用资源模块

# 05-output

2022年11月13日 12:04

## ヒアリングシート

（お客様の要件です。お客様の要求に基づいて、グループで検討して、ヒアリングシートを作成）

パラシー：ヒアリングシートを参照して、グループ会議で検討して、決めます。

（VPC、SB、RTB、ACL [#元に存在](#)、IAMポリシー [#お客様の要求に基づいて](#)、S3権限 [あげて](#) リストとGETなど、[アタッチします。](#)、インスタンス、S3、EBS、ロードバランサーなど）

## OS構築設計書

（外部設計書参考して、修正しました。）

## 単体試験と結合試験の仕様書

## 本番環境各種の申請書

（IPアドレス [#EC2構築](#)、本番admin [#構築のため](#)、監視申請 [#WEBSAM申請](#)）

## 手順書

（）

# 考点

2022年10月12日 10:55

cloudfront 比 elb 便宜

专用子网=vpc端点

删除+轮换=secrets

DAX = 缓解查询压力，例如新闻

aws glacier（冰川）= 长期存储

FSx = 文件存储

特权限 + IAM角色

Amazon glacier 长期存储关键数据，可用vault  
lock锁定保存时间

DMS = 易于迁徙

beanstalk = 易于管理，计算代码

snowball = 75tb

ec2展示组 单个可用区的实例

http get post = query (查询)

EIP最大 = 5

AWS Import/Export

s3导入导出，其他只能导入

s3标准 = 24小时

高度可伸缩数据库 = 不能部署在实例上

OLTP = RDS 实例 只读副本

kubernetes = 弹性容器服务 (google)

capacity optimized

容量 优化



ebs 单个实例存储

key pair = ec2 cloudfront

ses邮件

awap = 交换

启动和停止 = 竞价型实例

s3存储桶配置 = aws config

EMR = 大数据,分析日志文件

HPC（高性能）= 集群

配额监控 = lambda

certificate manager 凭证 管理

hadoop java框架

DDOS缓解攻击 = shield advanced 盾 先进

memory内存 利用率 = cloud watch需要手动设置

存储会话状态数据 = DynamoDB + ElastiCache

重复邮件通知的原因 = web程序处理完之后, SQS队列的消息不会被删除

保护后端不受峰值流量影响 = 节流限制和结果缓存

transfer转移

acceleration加速度

放置组是单个可用区实例的逻辑分组

cloudfront边缘位置是数据中心

解耦架构 = 计算架构, 计算组件或者层级能独立执行

AWS STS短期访问令牌, 临时安全凭证

SQS+LAMBDA = S3通知目标,

AWS IoT Core = 设备, 程序交互

opsWork = 管理配置服务

# ElastiCache for Redis

2022年10月19日 10:46

Amazon ElastiCache（弹性缓存）是一种 Web 服务，可让用户在云中轻松设置、管理和扩展分布式内存数据存储或缓存环境。它可以提供高性能、可扩展且具有成本效益的缓存解决方案。同时，它可以帮助消除与部署和管理分布式缓存环境相关的复杂性。

托管，高可用的内存缓存

高性能，数据复制

快照，复制，亚毫秒级

# AURORA极光

2022年10月19日 10:49

Amazon Aurora (Aurora) 是一个与 MySQL 和 PostgreSQL **兼容**的完全托管的**关系数据库**引擎。

在某些工作负载条件下, Aurora 最多可以将 MySQL 吞吐量增加 **5 倍**, 将 PostgreSQL 的吞吐量增加 **3 倍**, 而无需对大多数现有应用程序进行更改。

Aurora 集群卷可增大到最大大小 128TB

**不用instance就可以托管运行**

高吞吐, 自动扩展, **acd三个区, 跨区域复制, 容错**

故障转移

pro < 5秒

rto (恢复) < 1分钟

# S3

2022年10月19日 11:00

S3 生命周期 - 配置生命周期策略以管理您的对象，并在其整个生命周期内经济高效地存储。

S3 对象锁定 - 可以在固定的时间段内或无限期地阻止删除或覆盖 Amazon S3 对象。

S3 复制 - 将对象及其各自的元数据和对象标签复制到同一或不同的 AWS 区域 目标存储桶中的一个或多个目标存储桶，以减少延迟、合规性、安全性和其他使用案例。

S3 分批操作 - 通过单个 S3 API 请求或在 Amazon S3 控制台中单击几次，大规模管理数十亿个对象。

standard（标准）

glacier（冰川） 长期保存 检索要1-5分钟

glacier Deep Archive（深度冰川） 更加便宜

检索要12小时

s3 transfer acceleration（转移，加速）

s3 standard-Infrequent Access（标准不频繁 访问）

提取快，便宜，但是不能经常访问

s3 one zone-Infrequent Access

一个区 不频繁访问 (更便宜)

MFA 防止删除

# cloud front

2022年10月19日 11:05

Amazon CloudFront 是一项加快将静态和动态 Web 内容（例如 .html、.css、.js 和图像文件）分发给用户的速度的 Web 服务

CloudFront 通过[全球数据中心](#)（称作[边缘站点](#)）网络传输内容。

[加快响应时间](#)

数据传输比s3便宜（下载）

无服务器

可以拒绝被阻止的国家访问

| [将Amazon CloudFront与指向本地服务器的自定义来源一起使用](#)



# cloud trail

2022年10月19日 11:13

AWS CloudTrail 可帮助您对 AWS 账户进行操作和风险审核、监管和合规性检查。用户、角色或 AWS 服务执行的操作将记录为 CloudTrail 中的事件。事件包括在 AWS Management Console、AWS Command Line Interface 和 AWS 开发工具包和 API 中执行的操作。

创建时，将在AWS账户上启用 CloudTrail。当您的 AWS 账户中发生活动时，该活动将记录在 CloudTrail 事件中。您可以通过转到 Event history(事件历史记录)轻松查看 CloudTrail 控制台中的近期事件。要持续记录 AWS 账户中的活动和事件，请创建跟踪。

## 日志文件

## Dynamo DAX

2022年10月19日 11:17

Amazon DynamoDB 是一种全托管 NoSQL 数据库服务

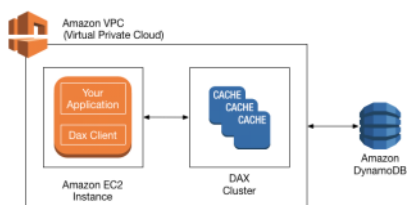
可增减，原子更新

快（毫秒微秒）

适合频繁更改数据

### DAX

Amazon DynamoDB Accelerator (DAX) 设计在(Amazon VPC) 环境中运行。可以在虚拟网络中启动一个 DAX 集群, 使用 Amazon VPC 安全组控制对该集群的访问。



高可用 内存缓解

Amazon FSx 完全托管式的 Windows 文件服务器

文件系统、备份和文件共享

高性能存储

企业应用程序并将其转移到AWS Cloud.

SMB协议 win 共享打印机、文件访问、串行端口以及网络上的节点之间的其他通信协议

# ROUTE53

2022年10月19日 11:38

- **简单路由策略** - 对于为您的域执行给定功能的单一资源（例如为 example.com 网站提供内容的 Web 服务器），可以使用该策略。在私有托管区域中，可以使用简单的路由创建记录。
- **故障转移路由策略** - 如果您想要配置主动-被动故障转移，则可以使用该策略。在私有托管区域中，可以使用失效转移路由创建记录。
- **地理位置路由策略** - 如果您想要根据用户的位置来路由流量，则可以使用该策略。在私有托管区域中，可以使用地理位置路由创建记录。
- **地理位置临近度路由策略** - 用于根据资源的位置来路由流量，以及（可选）将流量从一个位置中的资源转移到另一个位置中的资源。
- **延迟路由策略** - 如果您的资源位于多个 AWS 区域，并且您想要将流量路由到提供最佳延迟的区域，则可以使用该策略。在私有托管区域中，可以使用延迟路由创建记录。
- **基于 IP 的路由策略** - 如果您希望根据用户的位置来路由流量，并且获得流量来源的 IP 地址，则可以使用该策略。
- **多值应答路由策略** - 如果您想要让 Route 53 用随机选择的正常记录（最多八条）响应 DNS 查询，则可以使用该策略。在私有托管区域中，可以使用多值应答路由创建记录。
- **加权路由策略** - 用于按照您指定的比例将流量路由到多个资源。在私有托管区域中，可以使用加权路由创建记录。

# direct connect DX

2022年10月19日 12:14

direct connect  
直接 连接

AWS Direct Connect 是AWS提供的一种云服务解决方案, 通过该功能可以使企业网络与现有的AWS Direct Connect Locatio之间建立专用网络连接。





# Storage Gateway

2022年10月19日 13:00

是一项混合云存储服务，  
可让您从本地访问几乎不受限制的云存储。

低延迟

不中断



# Data Sync

2022年10月19日 14:19

迁移数据（快速，加密）

保护数据（安全）

归档保存（直接移动到glacier）

本地与aws无缝混合移动

# Amazon Kinesis Data Streams

2022年10月19日 14:37

是一项无服务器串流数据服务,  
可简化任何规模的数据流捕获、处理和存储



# Snowball

2022年10月19日 14:41

通过 Snowball 将 PB 级数据迁移到 AWS

对于需要多个设备的任务，请使用 Snow 的大型数据迁移管理器跟踪设备的阶段。

# SQS队列

2022年10月19日 16:33

Amazon Simple QS (Amazon SQS) 提供了安全、持久且可用的托管队列，用于存储在计算机之间传输的消息

访问存储待处理消息的消息队列

FIFO精确处理

可以设置多个队列，根据优先策略来排队

消息队列基本知识

在现代云架构中，应用程序被分解为多个规模较小且更易于开发、部署和维护的独立构建块。消息队列可为这些分布式应用程序提供通信和协调。消息队列可以显著简化分离应用程序的编码，同时提高性能、可靠性和可扩展性。

貼り付け元 <<https://aws.amazon.com/cn/message-queue/>>

# EFS

2022年10月20日 11:47

efs生命周期，根据文件空闲天数进行移动

POSIX标准

vpc内部

# VPN

2022年10月20日 14:34

VPN 连接：本地设备和 VPC 之间的安全连接

aws云资源连接到本地数据中心

## 虚拟专用网关

虚拟私有网关是站点到站点 VPN 连接在 Amazon 一端的 VPN 集中器。您可以创建虚拟私有网关，并将其附加到要从中创建站点到站点 VPN 连接的 VPC。



## SITE TO SITE VPN

按照以下步骤创建为 AWS 云 WAN 创建 Site-to-Site VPN 连接。

### 创建 AWS 云 WAN Site-to-Site VPN 连接

1. 通过以下网址打开 Amazon VPC 控制台：<https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 **Site-to-Site VPN 连接**。
3. 选择 **Create VPN connection** (创建 VPN 连接)。
4. (可选) 在 **Name tag** (名称标签) 文本框中输入连接名称。
5. 对于 **Target gateway type** (目标网关类型)，请选择 **Not associated** (未关联)。
6. 对于 **Customer gateway** (客户网关)，执行以下操作之一：
  - 要使用现有的客户网关，请选择 **Existing** (现有)，然后选择要使用的客户网关 ID。
  - 要创建客户网关，请选择 **New** (新建)。
    - 对于 **IP address** (IP 地址)，请输入静态公有 IP 地址。对于 **Certificate ARN** (证书 ARN)，请选择私有证书的 ARN (如果使用基于证书的身份验证)。对于 **BGP ASN**，输入您的客户网关的边界网关协议 (BGP) 自治系统编号 (ASN)。参阅 [站点到站点 VPN 连接的客户网关选项](#) 了解更多信息。
7. 对于 **Routing options** (路由选项)，选择是使用 **Dynamic** (动态) 还是 **Static** (静态)。
8. 对于 **Tunnel inside IP version** (隧道内部 IP 版本)，请选择是使用 **IPv4** 还是 **IPv6**。
9. (可选) 对于 **Enable acceleration** (启用加速)，选中复选框可启用加速。有关更多信息，请参阅[加速站点到站点 VPN 连接](#)。  
如果您启用加速，我们将创建两个加速器以供您的 VPN 连接使用。将收取额外费用。
10. (可选) 对于 **Local IPv4 network CIDR** (本地 IPv4 网络 CIDR)，指定客户网关 (本地部署) 端上允许通过 VPN 隧道进行通信的 IPv4 CIDR 范围。默认为 0.0.0.0/0。  
对于 **Remote IPv4 network CIDR** (远程 IPv4 网络 CIDR)，请指定 AWS 端上允许通过 VPN 隧道进行通信的 IPv4 CIDR 范围。默认为 0.0.0.0/0。  
如果您为 **Tunnel inside IP version** (隧道内部 IP 版本) 指定了 **IPv6**，请指定客户网关端和 AWS 端上允许通过 VPN 隧道进行通信的 IPv6 CIDR 范围。这两个范围的默认值均为 ::/0。
11. (可选) 对于 **隧道选项**，您可以选择为每个隧道指定以下信息：
  - 隧道内的 IPv4 地址范围 169.254.0.0/16 内的大小为 /30 的 IPv4 CIDR 块。
  - 如果为 **隧道内 IP 版本** 指定了 **IPv6**，则应指定隧道内 IPv6 地址范围 fd00::/8 内的 /126 IPv6 CIDR 块。
  - IKE 预共享密钥 (PSK)。支持以下版本：IKEv1 或 IKEv2。
  - 高级隧道信息，包括以下内容：
    - IKE 协商阶段 1 和 2 的加密算法
    - IKE 协商阶段 1 和 2 的完整性算法
    - IKE 协商阶段 1 和 2 的 Diffie-Hellman 组
    - IKE 版本
    - 阶段 1 和 2 生命周期
    - 更改密钥容许时间
    - 更改密钥模糊值
    - 回放窗口大小
    - 失效对端检测间隔
    - 失效对端检测超时操作
    - 启动操作有关这些选项的详细信息，请参阅 [站点到站点 VPN 连接的隧道选项](#)。
12. 选择 **Create VPN connection** (创建 VPN 连接)。  
**使用命令行或 API 创建 Site-to-Site VPN 连接**
  - [CreateVpnConnection](#) (Amazon EC2 查询 API)
  - [create-vpn-connection](#) (AWS CLI)

貼り付け元 <[https://docs.aws.amazon.com/zh\\_cn/vpn/latest/s2svpn/create-cwan-vpn-attachment.html](https://docs.aws.amazon.com/zh_cn/vpn/latest/s2svpn/create-cwan-vpn-attachment.html)>



# Route53

2022年10月20日 16:53

Amazon Route 53 是一种可用性高、可扩展性强的域名系统 (DNS) Web 服务。您可以使用 Route 53 以任意组合执行三个主要功能：域注册、DNS 路由和运行状况检查。

貼り付け元 <[https://docs.aws.amazon.com/zh\\_cn/Route53/latest/DeveloperGuide/Welcome.html](https://docs.aws.amazon.com/zh_cn/Route53/latest/DeveloperGuide/Welcome.html)>

地理临近策略



# kinesis

2022年10月21日 10:52

实时轻松收集、处理和分析视频和数据流

貼り付け元 <[https://aws.amazon.com/cn/kinesis/?nc1=h\\_ls](https://aws.amazon.com/cn/kinesis/?nc1=h_ls)>

# 数据流

2022年10月21日 10:58

各种各样的饮料原料（Producer）被送进饮料厂，原料各有作用，于是这些饮料原料通过一个自动化分拣机（Kafka）送进了不同的分拣篓（Topic），随即这些原料按照配比从分拣篓中取出被送上饮料厂里的运输车（consumer），再由运输车将原料送上流水线

（Streaming），经过流水线加工、装瓶、封盖等操作后，一些半成品被送进分拣机再次进行分拣等操作，一部分成品装箱后送往仓库（数据库）等待处理，另一部分成品则直接装进卡车，送给客户（输出）。我们的Kafka与Streaming与工厂流水线有相似之处也有不同之处。Kafka与饮料厂的分拣系统基本相似，但不同在于Kafka分类后的数据是按照时间先后的顺序排列好的，会组成一个消息队列，时间在前的数据会先进入下一轮处理。接下来是Streaming流处理，这个在某些方面还真的和流水线很像。首先它是一种处理，也就是对数据流的分析和加工。其次，数据流在某种意义上和流水线上的商品确实很像，而Streaming就像固定在流水线上的机器，对流经过它的数据流做着快速地处理。

-----  
©著作权归作者所有：来自51CTO博客作者mob604756fd5175的原创作品，请联系作者获取转载授权，否则将追究法律责任

白话大数据 | 流处理技术Streaming是什么？

[https://blog.51cto.com/u\\_15127640/2774713](https://blog.51cto.com/u_15127640/2774713)

# ElasticCache

2022年10月21日 16:33

内存数据库

执行快，复制数据提高可用性

弹性缓存

可以设置查询的负载和响应时间

# AWS Shield

2022年10月25日 14:42

AWS Shield（**护盾**）是一种托管式分布式**拒绝服务 (DDoS) 防护服务**，可以**保护**在 AWS 上运行的**应用程序**。AWS Shield 提供**持续检测**和**自动内联缓解功能**，能够尽可能**缩短应用程序的停机时间和延迟**，因此您不需要**联系 AWS Support 来获得 DDoS 防护**。AWS Shield 有两个**层级**，分别为 Standard 和 Advanced。

## AWS Shield Advanced

**护盾**      **高度**

# API凭证

2022年11月8日 11:00

利用KMS来存储加密敏感信息

# macie

2022年11月10日 11:44

是一个安全服务，，可以发现，分类，保护S3中的敏感数据

# aws MQ

2022年11月10日 12:10

支持API协议, 传递代码

# Iambda

2022年11月11日 11:03

无需服务器

按照运算时间计费

快速运行任何程序和代码



# 英语

2022年11月14日 11:13

infrequent 不经常

acceleration 加速

global 全球

kinesis 运动

setp 步骤

data pump 数据泵

function 函数

encryption 加密

management 管理

secrets 秘密，隐藏

associate 联合

enhanced 增强

monitoring 监视

event 最终

cluster 集群

snapshots 快照

replicas 副本

lifecycle manager

# API gateway

2022年11月14日 11:36

API 是一个接口，应用可通过它轻松使用来自另一个应用的功能或数据

用于创建、发布、维护、监控和保护任意规模的 REST、HTTP 和 WebSocket API

支持有状态（WebSocket）和无状态（HTTP 和 REST）API。

# AWS Fargate

2022年11月14日 11:49

AWS Fargate 是一种适用于容器的无服务器计算引擎，可与Amazon Elastic Container Service (ECS) 和Amazon Elastic Kubernetes Service (EKS) 一起使用。通过AWS Fargate 可以轻松专注于构建应用程序。

# storage gateway

2022年11月16日 11:01

低延迟访问 检索数据

使用标准文件存储协议

本地存储空间不足的话，可以与aws存储链接起来

提供三种存储方式

卷网关 volume

文件网关 file

磁带网关 tape

# AWS fargate

2022年11月16日 11:47

## 适用于容器的计算引擎（无服务器）

# RDS 只读副本

2022年11月16日 11:58

弹性拓展

异步复制

# AWS CloudTrail

2022年11月17日 16:24

可以对aws账户，运营审计，治理，风险审计。

可以记录，监控并保留用户的操作。

默认设置：使用S3服务器端加密（SSE）

# AWS EMR

2022年11月17日 16:27

(Amazon Elastic MapReduce)

用来分析日志文件，大量数据



## 交互式查询服务

使用标准SQL在S3中分析，导出数据

## 处理实时流数据

不丢失，持久，按照顺序，不重复

EBS

2022年11月18日 14:14

## 最低延迟服务

# MFA

2022年11月18日 17:24

txt认证

时间一次性认证 (TOTP)

第二种身份认证

# 综合

2022年11月21日 10:52

源访问身份（OAI）

metadata详细数据

redshift

2022年11月21日 10:59

数据库分析

高性能

大规模

排列

大量（海量）数据集，超快分析，查询

复制大型数据集（数百个万文件）

数据迁移

自动化加速

通过Internet, Direct Connect

## 服务器访问日志

记录对其 S3 存储桶的每个请求访问，包括请求者、存储桶名称、请求时间、请求操作、引用者、周转时间和错误代码信息。

。



# EFA

2022年11月21日 11:41

## Elastic Fabric Adapter 弹性结构适配器

是一种网络设备，与EC2链接加速高性能计算（HPC）和机器学习

# AWS Shield

2022年11月21日 11:46

AWS Shield（护盾）是一种托管式分布式拒绝服务 (DDoS) 防护服务，可以保护在 AWS 上运行的应用程序。

AWS Shield 提供持续检测和自动内联缓解功能，能够尽可能缩短应用程序的停机时间和延迟，因此您不需要联系 AWS Support 来获得 DDoS 防护。AWS Shield 有两个层级，分别为 Standard 和 Advanced。

AWS Shield Advanced

护盾 高度

## 配置管理服务

提供Chef和Puppet的托管实例

邮件默认保留期限4天

Receive Message Wait Time Seconds 大于零是长轮询

Receive Message Wait Time Seconds 等于零是短轮询

FIFO 先进先出，严格按照顺序（只处理一次）

标准 尽量按照信息顺序发送，可能无法按照顺序发送  
（最少处理一次）

特定顺序 FIFO

不会丢失 标准SQS

# workspace

2022年11月21日 14:18

workspace（工作区）  
虚拟桌面

完全托管的提取，转换和加载（ETL）的服务  
可以让客户轻松进行数据分析

## 管理和存储会话数据

# Dynamo

2022年11月30日 星期三 8:35

TTL生存时间

不会用到的数据。时间戳到期后。会从表中删除数据。免费使用的



Q28 : 高度动态批处理作业，无状态，定时启动停止，60分钟以上完成，可扩展并且具有成本效益  
A实施EC2 Spot实例

Q29 : ec2实例上运行应用程序，SQS读取数据并处理，消息量不可预测，断断续续。要求持续处理不停机，最经济高效的方案。  
C使用预留实例作为基准容量，并使用spot instances处理额外容量

Q30 : API根据价格自动查询税务计算，假期中会有大量计算，会导致响应变慢。有什么可扩展的弹性方案。  
使用接受项目名称的RESTAPI gateway，传递给lambda运算。

Q31 : 具有pubsb prisb的VPC，三个az各有一个pub pri子网internet网关给pub用。pri sb需要访问Internet允许ec2实例 下载更新  
创建三个nat网关，每个AZ中的PUB一个，非vpc流量转到AZ中的NAT网关的私有路由表。

Q32 : elb后面的ec2实例启动web应用程序，第三方服务用于DNS。检测和防御大规模DDoS攻击。  
启用 AWS Shield Advanced并将ELB分配给他

Q33 : 在两个ec2上托管了web应用程序，用公司自己的SSL证书，但是SSL加密和解密导致服务器达到计算能力上线。如何提高应用程序性能  
将SSL证书导入ACM，使用ACM证书的HTTPS侦听器创建ALB

Q34 : 可搜索的项目存储库有超过1000万行的RDS数据库表，存在2TB的SSD上每天的数据更新需要十秒以上，数据库性能的瓶颈怎么解决。  
将存储类型更改为Provisioned IOPS SSD (io1)

Q35 : 大量大小5MB的文件，存在S3中，要求文件存储四年后才能删除，因为是关键数据需要能够立即访问前30天经常访问，之后很少访问。  
创建S3生命周期策略，30天内存在S3标准，之后存在S3标准-不频繁（IA），四年后删除。

Q36 : S3存储机密数据，静态加密，密钥每年轮换，什么运行效率最高。  
自动轮换功能的KMS客户主密钥的CMK进行服务器端加密

Q37 : 本地数据库MySQL移动到AWS，最大程度减少数据丢失，存储在最少两个节点。  
创建启用多可用区的MySQL数据库，以同步复制数据

Q38 : 汽车销售网站，列表存在RDS数据库中，汽车出售时，需要从网站删除列表，并将数据发送到多个目标系统。  
订阅RDS时间通知，并将SNS主体散出到多个SQS，使用lambda更新。

Q39 : 构建可扩展的密钥管理基础架构，支持应用程序中加密数据，怎么减少运营负担。  
AWS KMS

Aurora兼容PostgreSQL  
fargate无服务器的容器计算引擎

Q40 : 本地运行应用容器化的应用程序，并且链接了Linux的PostgreSQL运行，怎么减少运营开销。  
PostgreSQL数据库迁移到Aurora、使用ECS迁移要在AWS fargate上的应用程序

Q41 : 一个高峰是为数十万用户提供服务，需要实时共享详细信息给几个内部应用程序，检索前，还要删除敏感数据  
将交易数据流传到Amazon Kinesis Data Streams用lambda删除数据，存在DynamoDB中，其他应用程序可以使用kinesis

Q42 : 允许特权用户访问S3对象，怎么防止S3上的数据丢失。  
在S3存储桶上启用版本控制，使用MEADelete要求多重身份验证来删除对象。

Q43 : 只有在私网中的ec2才能访问RDS  
创建一个安全组，允许私网中的ec2安全组进入，附加到RDS数据库实例中

Q44 :

Q45 :

Q46 :

Q47 :

Q48 :

Q49 :

Q50 :

Q51 :

Q52 :

# spot instance

2022年11月16日 11:37

## spot instance

aws云的备用计算容量，比按需实例便宜  
最便宜

# 预留 instance

2022年11月16日 12:00

reserved instance

稳定可预测的应用程序用预留更划算

# ec2重启

2022年11月16日 12:03

实例的底层主机更改

实例的内存会清空数据

# 按需 instance

2022年11月18日 14:19

direct 直接

connect 连接

certificate 证书

directory 目录

Saving 节省

Requester 请求者

Dynamic 动态

transcriber 转录

# ボリューム修正

2022年11月17日 14:18

错误ec2のボリューム（A）给他スナップショット  
用スナップショット启动一个新的ボリューム（B）  
把ボリューム（B）追加到一个新的ec2上，新ec2の原本的ボリューム就那么放着

然后新的ec2再启动

进入teraterm执行以下命令

```
mkdir /yangshike  
mount /dev/xvdf /yangshike  
ll /yangshike/  
mount -t xfs -o nouuid /dev/xvdf1 /yangshike/  
ll /yangshike/
```

里面修改就行了  
改好了直接退出

把新的ec2上のボリューム（B）デタッチ

把错误的ec2上のデタッチ（A）给デタッチ

修改好的ボリューム（B）アタッチ到错误的ec2上，路径名**注意是/dev/xvda**



# Site-to-site

2022年12月6日 星期二 12:29