AWS 启动安全基准 (AWS SSB)

# AWS 规范性指导

# AWS 规范性指导: AWS 启动安全基准 (AWS SSB)

# Table of Contents

# AWS Startup Security Baseline（AWS SSB）

Jay Michael，Amazon Web Services（AWS）

2023 年 5 月（文档历史记录）

AWS Startup Security Baseline（SSB）是一套控制措施，为企业在不降低敏捷性的前提下，在 AWS 上安全构建奠定了最低基础。这些控制构成了安全状况的基础，重点是保护凭证、启用日志记录和可见性、管理联系信息以及实现基本数据边界。

本指南中的控制在设计时考虑了早期初创企业，让他们无需花费大量精力即可降低最常见的安全风险。许多初创企业都是从一个 AWS 账户 开始他们的 AWS Cloud 旅程的。随着组织的发展，他们开始迁移到多账户架构。本指南中的指导是针对单账户架构设计的，但它可以帮助您建立安全控制，让您在过渡到多账户架构时轻松迁移或修改。

AWS SSB 中的控制分为两类：账户和工作负载。账户控制有助于保护您的 AWS 账户。它包括有关设置用户访问、策略和权限的建议，以及如何监控您的账户中是否存在未经授权或潜在恶意活动的建议。工作负载控制有助于保护云中的资源和代码，比如应用程序、后端进程和数据。它包括加密和减小访问范围等建议。

> **Note**
>
> 本指南中推荐的某些控制会替代初始设置时配置的默认值，而大多数控制则会配置新的设置和策略。绝不应将本文档视为包含所有可用的控制措施。

## 目标受众

本指南最适合处于发展初期、人员和运营规模较小的初创企业。

对于处在运营和发展后期阶段的初创企业或其他企业，仍然可以从对照其当前做法来审查这些控制措施中获得重要价值。如果发现任何差距，可以实施本指南中的单个控制，然后评估它们是否适合作为长期解决方案。

> **Note**
>
> 本指南中推荐的控制本质上是基础性的。对于处在后期规模或成熟阶段的初创企业或其他企业，应酌情增加额外的控制措施。

# 基础框架和安全责任

AWS Well-Architected Framework 可帮助云架构师为各种应用程序和工作负载构建安全、高性能、弹性和高效的基础架构。AWS Startup Security Baseline 与 AWS Well-Architected Framework 的安全支柱一致。安全支柱介绍了如何利用云技术来保护数据、系统和资产，从而改善您的安全状况。这有助于您遵循最新 AWS 建议，从而满足您的业务和监管要求。

您可以使用 AWS 账户中的 AWS Well-Architected Tool，评测自己对架构完善的最佳实践的遵守情况。

安全性和合规性是 AWS 与客户共同的责任。责任共担模式通常是说，AWS 负责云的安全（即保护 AWS Cloud 中提供的所有服务的基础设施），而您负责云中的安全（由您选择的 AWS Cloud 服务决定）。在责任共担模式中，实施本文档中的安全控制是您作为客户的责任之一。

# 保护您的账户

本节中的控件和建议有助于保护您的 AWS 账户安全。它强调使用 AWS Identity and Access Management (IAM) 用户、用户组和角色（也称为委托人）进行人员和机器访问，限制根用户的使用，并要求进行多因素身份验证。在本节中，您确认 AWS 拥有与您的账户活动和状态相关的联系信息。您还可以设置监控服务，例如 AWS Trusted Advisor Amazon 和 GuardDuty AWS Budgets，这样您就可以收到账户活动通知，并且可以在活动未经授权或意外时快速做出响应。

本节包含以下主题：



## ACCT.01 - 将账户级别的联系人设置为有效的电子邮件通讯组列表

为您的 AWS 账户设置主要联系人和备用联系人时，请使用电子邮件通讯组列表而不是个人的电子邮件地址。使用电子邮件通讯组列表可以确保组织中的人员进出时保留所有权和可访问性。为账单、操作和安全通知设置备用联系人，并相应地使用相应的电子邮件通讯组列表。 AWS 使用这些电子邮件地址与您联系，因此请务必保留对它们的访问权限。

若要编辑您的账户名称、对用户密码或用户电子邮件地址进行根处理

1. 在 https://console.aws.amazon.com/billing/home?#/account 上登录到“账单和成本管理”控制台中的账户设置页面
2. 在账户设置页面上的账户设置旁，选择编辑。

3. 在要更新的字段旁，选择编辑。
4. 输入您的更改后，选择保存更改。
5. 完成所有更改后，选择完成。

若要编辑您的联系信息

1. 在账户设置页面上的联系信息下方，选择编辑。
2. 对于要更改的字段，输入更新后的信息，然后选择更新。

若要添加、更新或删除备用联系人

1. 在账户设置页面上的备用联系人下方，选择编辑。
2. 对于要更改的字段，输入更新后的信息，然后选择更新。

## ACCT.02 - 限制使用根用户

root 用户是在您注册 AWS 账户时创建的，该用户对该账户拥有完全的所有权权限和权限，且无法更改。仅将根用户用于需要它的特定任务 有关更多信息，请参阅需要根用户凭证的任务（AWS Account Management）。使用其他类型的 IAM 身份（如具有 IAM 角色的联合用户）执行账户中的所有其他操作。有关更多信息，请参阅 AWS security credentials（IAM 文档）。

若要限制使用根用户

1. 需要对根用户进行多重身份验证（MFA），如 ACCT.05 - 需要多重身份验证（MFA）才能登录 中所述。
2. 创建管理用户，这样就不必使用根用户执行日常任务。有关配置用户访问权限的更多信息，请参阅 ACCT.03 - 为每个用户配置控制台访问权限。

## ACCT.03 - 为每个用户配置控制台访问权限

作为最佳实践， AWS 建议使用临时证书来授予对 AWS 账户 和资源的访问权限。临时凭证的使用期限有限，因此，在不需要这些凭证时不必轮换或明确撤销它们。有关更多信息，请参阅 Temporary security credentials（IAM 文档）。

对于人类用户， AWS 建议使用集中式身份提供商 (IdP) 提供的联合身份，例如 Okta、Active Directory 或 Ping Identity。 AWS IAM Identity Center联合用户允许您在单一的中心位置定义身份，并且用户可

以安全地向多个应用程序和网站进行身份验证 AWS，包括仅使用一组凭证。有关更多信息，请参阅中的联合身份 AWS和 IAM 身份中心（AWS 网站）。

> **Note**
>
> 身份联合验证会使从单账户架构到多账户架构的过渡变得复杂。初创企业通常会推迟实施身份联合验证，直到他们建立一个在 AWS Organizations中管理的多账户架构。

若要设置身份联合验证

1. 如果您使用的是 IAM Identity Center，请参阅 Getting started（IAM Identity Center 文档）。

   如果您使用的是外部或第三方 IdP，请参阅 Creating IAM identity providers（IAM 文档）。
2. 确保您的 IdP 强制执行多重身份验证（MFA）。
3. 根据 ACCT.04 - 分配权限 应用权限。

对于未准备好配置身份联合验证的初创企业，可以直接在 IAM 中创建用户。这不是推荐的安全最佳实践，因为这些是永不过期的长期凭证。但这是初创企业在运营初期的常见做法，防止在运营准备就绪过渡到多账户架构时遇到困难。

作为基线，您可以为需要访问 AWS Management Console的每个人创建一个 IAM 用户。如果您配置 IAM 用户，请勿在用户之间共享凭证，并定期轮换长期凭证。

> **Warning**
>
> IAM 用户拥有长期证书，这会带来安全风险。为帮助减轻这种风险，我们建议仅向这些用户提供执行任务所需的权限，并在不再需要这些用户时将其移除。

若要创建 IAM 用户

1. 创建 IAM 用户（IAM 文档）。
2. 根据 ACCT.04 - 分配权限 应用权限。

# ACCT.04 - 分配权限

通过将策略分配给 IAM 身份（用户组或角色）来配置账户中的用户权限。您可以自定义权限，也可以附加AWS 托管策略，这些策略是独立策略，旨在为许多常见用例提供权限。 AWS 如果您自定义权限，请遵循授予最低权限的安全最佳实践。最低权限是授予每个用户执行任务所需的最低权限集的做法。

如果您使用联合身份，用户将通过外部身份提供者承担 IAM 角色访问账户。IAM 角色定义了允许经过贵组织的 IdP 身份验证的用户在其中执行的操作。 AWS您可以将自定义或 AWS 托管策略应用于此角色来配置权限。

若要为联合身份分配权限

- 如果您使用的是 IAM Identity Center，请参阅 Use IAM policies in permission sets（IAM Identity Center 文档）。

  如果您使用的是外部或第三方 IdP，请参阅 Adding IAM identity permissions（IAM 文档）。

如果您使用的是 IAM 用户，则可以使用用户组或角色来管理多个 IAM 用户的权限。我们建议初创企业使用用户组，因为它们更容易管理，也不容易出现可能会给账户带来安全风险的配置错误。根据用户的工作职能将用户分配到用户组。用户组的示例包括应用程序、数据、网络和开发运营 (DevOps) 工程师。您还可以根据决策权限将用户类型划分为较小的用户组，比如高级或非高级工程师。

若要分配 IAM 用户权限

1. 创建 IAM 用户组（IAM 文档）。
2. 将@@ AWS 托管策略附加到 IAM 用户组（IAM 文档）。

# ACCT.05 - 需要多重身份验证（MFA）才能登录

有了 MFA，用户就有了一个可以生成身份验证质询响应的设备。需要每个用户的凭证和设备生成的响应才能完成登录过程。作为安全最佳实践，请启用 MFA 进行 AWS 账户 访问，尤其是针对账户根用户和 IAM 用户等长期证书。

若要为根用户设置 MFA

1. 登录到 a AWS Management Console t https://console.aws.amazon.com/。
2. 在导航栏的右侧，选择您的账户名称，然后选择我的安全凭证。

3. 如有必要，选择继续使用安全凭证。
4. 展开多重身份验证（MFA）部分。
5. 选择激活 MFA。
6. 按照向导说明相应地配置您的 MFA 设备。有关更多信息，请参阅 Enabling MFA devices for users in AWS（IAM 文档）。

若要在 IAM Identity Center 设置 MFA

- 启用 MFA（IAM Identity Center 文档）

若要为自己的 IAM 用户设置 MFA

1. 利用您的登录凭证，在 https://console.aws.amazon.com/iam 上登录到 IAM 控制台。
2. 在右上角的导航栏中，选择您的用户名，然后选择我的安全凭证。
3. 在 AWS IAM 凭证选项卡的多重身份验证部分中，选择管理 MFA 设备。

若要为其他 IAM 用户设置 MFA

1. 登录 AWS Management Console 并打开 IAM 控制台，网址为https://console.aws.amazon.com/iam。
2. 在导航窗格中，选择用户。
3. 选择要为其启用 MFA 的用户的名称，然后选择安全凭证选项卡。
4. 在分配的 MFA 设备旁边，选择管理。
5. 按照向导说明相应地配置您的 MFA 设备。有关更多信息，请参阅 Enabling MFA devices for users in AWS（IAM 文档）。

## ACCT.06 - 强制执行密码策略

用户 AWS Management Console 通过提供登录凭证登录，建议使用 MFA。要求密码遵循强密码策略，以防止通过暴力破解或社交工程发现。

有关强密码的最新建议的更多信息，请参阅 Center for Internet Security（CIS）网站上的 Password Policy Guide。

对于 IAM 用户，您可以在自定义 IAM 密码策略中配置密码要求。有关更多信息，请参阅 Setting an account password policy（IAM 文档）。

若要创建自定义密码策略

1. 登录 AWS Management Console 并打开 IAM 控制台，网址为https://console.aws.amazon.com/iam。
2. 在导航窗格中，选择账户设置。
3. 在密码策略部分，选择更改密码策略。
4. 选择您要应用于密码策略的选项，然后选择保存更改。

## ACCT.07 — 将 CloudTrail 日志传送到受保护的 S3 存储桶

您的 AWS 账户中的用户、角色和服务所执行的操作将作为事件记录在中 AWS CloudTrail。CloudTrail 默认情况下处于启用状态，在 CloudTrail 控制台中，您可以访问 90 天的事件历史记录信息。要查看、搜索、下载、存档、分析和响应 AWS 基础架构中的账户活动，请参阅使用 CloudTrail事件历史记录查看事件（CloudTrail 文档）。

要将 CloudTrail 历史记录保留超过 90 天以及其他数据，您可以创建一个新的跟踪，将所有事件类型的日志文件传输到亚马逊简单存储服务 (Amazon S3) 存储桶。在 CloudTrail 控制台中创建跟踪时，即创建多区域跟踪。

创建将所有 AWS 区域 人的日志传输到 S3 存储桶的跟踪

1. 创建跟踪（CloudTrail 文档）。在选择日志事件页面上，执行以下操作：
   a. 对于 API 活动，同时选择读取和写入。
   b. 对于预生产环境，选择排除 AWS KMS 事件。这会将所有 AWS Key Management Service (AWS KMS) 事件排除在您的跟踪之外。 AWS KMS 读取诸如`Encrypt`、`Decrypt`、和之类的操作`GenerateDataKey`可以生成大量事件。

      对于生产环境，选择记录写入管理事件，并清除排除 AWS KMS 事件复选框。这不包括高容量 AWS KMS 读取事件，但仍会记录相关的写入事件`Disable`，例如`Delete`、和。`ScheduleKey`这些是生产环境推荐的最低 AWS KMS 日志记录设置。
2. 新的跟踪将显示在跟踪页面上。大约 15 分钟后，将 CloudTrail 发布日志文件，显示在您的账户中进行的 AWS 应用程序编程接口 (API) 调用。您可以在指定的 S3 存储桶中查看日志文件。

为了帮助保护存储 CloudTrail 日志文件的 S3 存储桶

1. 查看您存储日志文件的所有存储桶的 Amazon S3 存储桶策略（CloudTrail 文档），并根据需要进行调整以删除任何不必要的访问权限。
2. 作为安全最佳实践，务必手动将 `aws:SourceArn` 条件键添加到存储桶策略。有关更多信息，请参阅创建或更新用于存储组织跟踪日志文件的 Amazon S3 存储桶（CloudTrail 文档）。
3. 启用 MFA 删除（Amazon S3 文档）。

## ACCT.08 - 防止公开访问私有 S3 存储桶

默认情况下，只有的根用户 AWS 账户 和 IAM 委托人（如果使用）才有权读取和写入该委托人创建的 Amazon S3 存储桶。使用基于身份的策略向其他 IAM 主体授予访问权限，并且可以使用存储桶策略强制执行访问条件。您可以创建存储桶策略，授予对存储桶（公有存储桶）的公开访问权限。

在 2023 年 4 月 28 日当天或之后创建的存储桶默认启用阻止公开访问设置。对于在此日期之前创建的存储桶，用户可能会错误配置存储桶策略，无意中将访问权限授予公众。您可以为每个存储桶启用阻止公开访问设置来防止这种配置错误。如果您没有公有 S3 存储桶的当前或将来的用例，请在 AWS 账户级别启用此设置。此设置会阻止允许公开访问的策略。

若要阻止公开访问 S3 存储桶

- 为 S3 存储桶配置阻止公开访问设置（Amazon S3 文档）。

AWS Trusted Advisor 为允许公众进行列表或读取访问的 S3 存储桶生成黄色查找结果，并对允许公开上传或删除的存储桶生成红色查找结果。作为基线，遵循控制 ACCT.12 - 使用 Trusted Advisor监控和解决高风险问题 来识别和纠正配置错误的存储桶。Amazon S3 控制台中还显示了可公开访问的 S3 存储桶。

## ACCT.09 - 删除未使用的 VPC、子网和安全组

若要减少出现安全问题的机会，请删除或关闭任何未使用的资源。在新 AWS 账户中，默认情况下会在每个账户中自动创建虚拟私有云 (VPC) AWS 区域，这使您能够在公有子网中分配公有 IP 地址。但如果不需要这些 VPC，就会产生资源意外暴露的风险。

如果未使用默认 VPC，请删除所有区域中的默认 VPC，而不仅仅是可能部署工作负载的区域中的默认 VPC。删除 VPC 还会删除其组件，如子网和安全组。

> **Note**
>
> 您可以在 https://console.aws.amazon.com/ec2globalview/home 的 Amazon EC2 全局视图控制台上查看所有区域和 VPC。有关更多信息，请参阅 List and filter resources across Regions using Amazon EC2 Global View（Amazon EC2 文档）。

若要删除未使用的默认 VPC

1. 删除 VPC（Amazon VPC 文档）。
2. 根据需要对其他区域中的 VPC 重复此操作。

## ACCT.10 — 配置 AWS Budgets 以监控您的支出

AWS Budgets 启用对每月成本和使用情况的监控，并在预计成本超过目标阈值时发出通知。预测的成本通知可以提供意外活动的指示，除了其他监控系统（例如 AWS Trusted Advisor 和 Amazon GuardDuty）之外，还可以提供额外的防御。监控和了解您的 AWS 成本也是良好运营卫生的一部分。

要在中设置预算 AWS Budgets

- 创建成本预算（AWS Budgets 文档）。

## ACCT.11-启用和回复通知 GuardDuty

Amazon GuardDuty 是一项威胁检测服务，可持续监控恶意或未经授权的行为，以帮助保护您的 AWS 账户、工作负载和数据。当它检测到意外和潜在的恶意活动时，会 GuardDuty 提供详细的安全调查结果，以便进行可见性和补救。 GuardDuty 可以检测到诸如加密货币挖矿活动、来自 Tor 客户端和中继的访问、意外行为以及 IAM 凭证受损等威胁。启用 GuardDuty 并响应调查结果，以阻止 AWS 环境中潜在的恶意行为或未经授权的行为。有关中查找结果的更多信息 GuardDuty，请参阅查找类型（GuardDuty 文档）。

您可以使用 Amazon Ev CloudWatch ents 在 GuardDuty 创建调查结果或发现更改时设置自动通知。首先，您要设置一个 Amazon Simple Notification Service（Amazon SNS）主题，并向该主题添加端点或电子邮件地址。然后，您为 GuardDuty 发现设置事件， CloudWatch 事件规则会通知 Amazon SNS 主题中的终端节点。

启用 GuardDuty 和 GuardDuty 通知

1. 启用 Amazon GuardDuty（GuardDuty 文档）。
2. 创建 CloudWatch 事件规则以通知您 GuardDuty 调查结果（GuardDuty文档）。

# ACCT.12 - 使用 Trusted Advisor监控和解决高风险问题

AWS Trusted Advisor 被动扫描您的 AWS 基础架构，以发现与安全、性能、成本和可靠性相关的高风险或高影响问题。它提供了有关受影响资源和修复建议的详细信息。有关检查和说明的完整列表，请参阅AWS Trusted Advisor 支票参考（Trusted Advisor 文档）。

定期审查 Trusted Advisor 调查结果，并在必要时对问题进行补救。如果您有 B AWS usiness Support 或 Enterprise Support 计划，则可以订阅每周调查结果电子邮件。有关更多信息，请参阅 Set up notification preferences（AWS Support 文档）。

要在中查看问题 Trusted Advisor

- 根据查看支票类别（AWS Support 文档）中的说明查看每个支票类别。至少，我们建议您查看建议执行操作问题（红色显示）。

# 保护工作负载

本节中的控制和建议可帮助您在构建工作负载时保护在 AWS 中运行的工作负载。它们强调管理应用程序密钥和访问范围的安全实践，尽量减少私有资源的访问路由，使用加密来保护传输中数据和静态数据。

本节包含以下主题：



## WKLD.01 - 使用 IAM 角色获取计算环境权限

在 AWS Identity and Access Management（IAM）中，角色表示个人或服务在可配置的一段时间内可以承担的一组权限。使用角色无需存储或管理长期凭证，从而大大降低了意外使用的几率。在支持的情况下，将 IAM 角色直接分配给 Amazon Elastic Compute Cloud（Amazon EC2）实例、AWS Fargate 任务和服务、AWS Lambda 函数以及其他 AWS 计算服务。使用 AWS SDK 并在这些计算环境中运行的应用程序会自动使用 IAM 角色凭证进行身份验证。

有关对每个服务使用 IAM 角色的方法和说明，请参阅适用于该服务的 AWS 文档。例如，请参阅以下文档：

- 适用于 Amazon EC2 的 IAM 角色（Amazon EC2 文档）
- 适用于任务的 IAM 角色（Amazon Elastic Container Service 文档）
- Lambda 执行角色（Lambda 文档）

## WKLD.02 - 使用基于资源的策略权限限制凭证使用范围

策略是可以定义权限或指定访问条件的对象。主要有两种托管策略：

- 基于身份的策略附加到主体，并定义主体在 AWS 环境中的权限。
- 基于资源的政策附加到资源，如 Amazon Simple Storage Service（Amazon S3）存储桶或虚拟私有云（VPC）端点。这些策略指定了允许哪些主体访问、支持的操作以及必须满足的任何其他条件。

要允许主体访问以对资源执行操作，必须在其基于身份的策略中授予权限，并满足基于资源的策略的条件。有关更多信息，请参阅基于身份的策略和基于资源的策略（IAM 文档）。

基于资源的策略的建议条件包括：

- 使用 `aws:PrincipalOrgID` 条件来限制只能访问指定组织中的主体（在 AWS Organizations 中定义）。
- 分别使用 `aws:SourceVpc` 或 `aws:SourceVpce` 条件来限制访问来自特定 VPC 或 VPC 端点的流量。
- 使用 `aws:SourceIp` 条件根据源 IP 地址允许或拒绝流量。

以下是基于资源的策略示例，该策略使用 `aws:PrincipalOrgID` 条件仅允许 **<o-xxxxxxxxxxx>** 组织中的主体访问 **<bucket-name>** S3 存储桶：

```
{
   "Version":"2012-10-17",
   "Statement":[
     {
       "Sid":"AllowFromOrganization",
       "Effect":"Allow",
       "Principal":"*",
       "Action":"s3:*",
       "Resource":"arn:aws:s3:::<bucket-name>/*",
       "Condition": {
         "StringEquals": {"aws:PrincipalOrgID":"<o-xxxxxxxxxxx>"}
       }
```

```
      }
    ]
}
```

# WKLD.03 - 使用临时密钥或密钥管理服务

应用程序密钥主要由凭证组成，如密钥对、访问令牌、数字证书和登录凭证。应用程序使用这些密钥来访问它所依赖的其他服务，如数据库。为了保护这些密钥，我们建议它们要么是临时的（在请求时生成，持续时间很短，比如 IAM 角色），要么是从密钥管理服务中检索的。这样可以防止通过不太安全的机制（比如保存在静态配置文件中）意外泄露。这也使得将应用程序代码从开发环境提升到生产环境变得更加容易。

对于密钥管理服务，我们建议使用 Parameter Store、AWS Systems Manager 功能和 AWS Secrets Manager 的组合：

- 使用 Parameter Store 管理密钥和其他参数，这些都是单独的键值对、基于字符串、总长度较短且访问频繁。您可以使用 AWS Key Management Service（AWS KMS）密钥加密密钥。在 Parameter Store 的标准层中存储参数不收取任何费用。有关参数层的更多信息，请参阅“管理参数层”（Systems Manager 文档）。
- 使用 Secrets Manager 存储文档形式（如多个相关的键值对）、超过 4 KB（如数字证书）或需要自动轮换的密钥。

您可以使用 Parameter Store API 检索存储在 Secrets Manager 中的密钥。这样，当您同时使用这两种服务时，就可以将应用程序中的代码标准化。

若要在 Parameter Store 中管理密钥

1. 创建对称的 AWS KMS 密钥（AWS KMS 文档）。
2. 创建 SecureString 参数（Systems Manager 文档）。Parameter Store 中的密钥使用 `SecureString` 数据类型。
3. 在您的应用程序中，使用适合您的编程语言的 AWS SDK 从 Parameter Store 检索参数。有关 Java 示例，请参阅 GetParameter.java（AWS 代码示例目录）。

若要在 Secrets Manager 中管理密钥

1. 创建密钥（Secrets Manager 文档）。
2. 在代码中从 AWS Secrets Manager 检索密钥（Secrets Manager 文档）。

请务必阅读使用 AWS Secrets Manager 客户端缓存库来提高使用密钥的可用性并减少延迟（AWS 博客文章）。使用已实施最佳实践的客户端 SDK 应将加速和简化 Secrets Manager 的使用和集成。

## WKLD.04 - 防止应用程序密钥泄露

在本地开发过程中，应用程序密钥可以存储在本地配置或代码文件中，并意外签入源代码存储库。托管在公有服务提供商的不安全存储库可能会遭到未经授权的访问，随后这些密钥被发现。使用可用工具防止密钥被签入。将检查密钥是否泄露作为手动代码审查流程的一部分。

一些可以防止应用程序密钥签入源代码存储库的常见工具有：

- Gitleaks（GitHub 存储库）
- Whispers（GitHub 存储库）
- detect-secrets（GitHub 存储库）
- git-secrets（GitHub 存储库）
- TruffleHog（GitHub 存储库）

## WKLD.05 - 检测和修复密钥泄露

在 WKLD.03 - 使用临时密钥或密钥管理服务 和 WKLD.04 - 防止应用程序密钥泄露 中，采取措施保护密钥。在这种控制中，您可以部署解决方案，检测密钥是否绕过这些预防措施，然后进行相应的修复。

Amazon CodeGuru Reviewer 会检测源代码中的应用程序密钥，并提供一种机制来修复和发布在 Secrets Manager 中检测到的密钥。还将提供用于从 Secrets Manager 检索密钥的应用程序代码。执行成本效益分析，确定该解决方案是否适合您的业务。替代方案是，WKLD.04 - 防止应用程序密钥泄露 中的一些开源解决方案提供了对现有密钥的检测能力。

若要设置 CodeGuru Reviewer 与 Secrets Manager 的集成

- 使用 CodeGuru Reviewer 识别硬编码密钥并使用 AWS Secrets Manager 保护这些密钥（AWS 博客文章和指导性演练）。

# WKLD.06 - 使用 Systems Manager 代替 SSH 或 RDP

就本身而言，具有指向互联网网关的默认路由的公有子网比没有指向互联网的路由的私有子网存在更大的安全风险。您可以在私有子网中运行 EC2 实例，使用 Session Manager 的 AWS Systems Manager 功能通过 AWS Command Line Interface（AWS CLI）或 AWS Management Console 远程访问实例。然后，您可以使用 AWS CLI 或控制台启动通过安全隧道连接到实例的会话，这样就无需管理用于 Secure Shell（SSH）或 Windows 远程桌面协议（RDP）的其他凭证。

使用 Session Manager，而不是在公有子网中运行 EC2 实例、运行跳转盒或运行堡垒主机。

若要设置 Session Manager

1. 确保 EC2 实例使用的是最新的操作系统亚马逊机器映像（AMI），比如 Amazon Linux 2 或 Ubuntu。AMI 上已预安装 AWS Systems Manager 代理（SSM 代理）。
2. 确保实例可通过互联网网关或 VPC 端点连接到这些地址（将 **<region>** 替换为相应的 AWS 区域）：
    a. Ec2messages.<region>.amazonaws.com
    b. ssm.<region>.amazonaws.com
    c. ssmmessages.<region>.amazonaws.com
3. 将 AWS 托管策略 `AmazonSSMManagedInstanceCore` 附加到与您的实例关联的 IAM 角色。

有关更多信息，请参阅设置 Session Manager（Systems Manager 文档）。

若要启动会话

- 启动会话（Systems Manager 文档）。

# WKLD.07 - 记录包含敏感数据的 S3 存储桶的数据事件

默认情况下，AWS CloudTrail 会捕获管理事件，即在账户中创建、修改或删除资源的事件。这些管理事件不会捕获对 Amazon Simple Storage Service 存储桶中单个对象的读取或写入操作。在安全事件发生期间，必须在单个记录或对象级别捕获未经授权的数据访问或使用。使用 CloudTrail 记录用来存储敏感或业务关键型数据的任何 S3 存储桶的数据事件，以便进行检测和审计。

> **Note**
>
> 记录数据事件将收取额外费用。有关更多信息，请参阅 AWS CloudTrail 定价。

若要记录跟踪的数据事件

1. 登录 AWS Management Console，并在 https://console.aws.amazon.com/cloudtrail/ 上打开 CloudTrail 控制台
2. 在导航窗格中，选择跟踪，然后选择跟踪名称。
3. 在一般详细信息中，选择“编辑”以更改以下设置。您无法更改跟踪的名称。
    a. 在数据事件中，选择编辑。
    b. 对于数据事件源，选择 S3。
    c. 对于所有当前和将来的 S3 存储桶，清除读取和写入。
    d. 在单个存储桶选择中，浏览要在其上记录数据事件的存储桶。您可以在此窗口中选择多个存储桶。选择添加存储桶，记录更多存储桶的数据事件。选择记录读取事件（如 `GetObject`）、写入事件（如 `PutObject`）或同时记录两者。
    e. 选择更新跟踪。

## WKLD.08 - 加密 Amazon EBS 卷

强制将 Amazon Elastic Block Store（Amazon EBS）卷加密作为您的 AWS 账户中的默认行为 加密卷的每秒进行读写操作的次数（IOPS）性能与未加密卷相同，对延迟的影响极小。这样可以防止以后出于合规或其他原因而重建卷。有关更多信息，请参阅关于 Amazon EBS 加密的必知最佳实践（AWS 博客文章）。

若要加密 Amazon EBS 卷

- 默认启用加密（Amazon EC2 文档）。

## WKLD.09 - 加密 Amazon RDS 数据库

类似于 WKLD.08 - 加密 Amazon EBS 卷，启用 Amazon Relational Database Service（Amazon RDS）数据库加密。这种加密在底层卷级别执行，IOPS 性能与未加密卷相同，对延迟的影响极小。有关更多信息，请参阅加密 Amazon RDS 资源概述（Amazon RDS 文档）。

若要加密 RDS 数据库实例

- 加密数据库实例（Amazon RDS 文档）。

# WKLD.10 - 将私有资源部署到私有子网

将不需要直接访问互联网的资源（如 EC2 实例、数据库、队列、缓存或其他基础设施）部署到 VPC 私有子网。私有子网的路由表中没有声明到附加互联网网关的路由，因此无法接收互联网流量。来自私有子网、发往互联网的流量必须通过托管的 AWS NAT 网关或在公有子网中运行 NAT 进程的 EC2 实例进行网络地址转换（NATI）。有关网络隔离的更多信息，请参阅 Amazon VPC 中的基础设施安全性（Amazon VPS 文档）。

创建私有资源和子网时，请遵循以下实践：

- 创建私有子网时，禁用自动分配公有 IPv4 地址。
- 创建私有 EC2 实例时，禁用自动分配公有 IP。如果实例因为配置错误而无意中部署到公有子网中，这样可以防止分配公有 IP。

必要时，您可以在资源配置中为其指定子网。您可以使用模块化和可扩展 VPC 架构快速入门（AWS 快速入门）来部署遵循最佳实践的 VPC。

# WKLD.11 – 使用安全组限制网络访问

使用安全组控制到 EC2 实例、RDS 数据库和其他受支持资源的流量。安全组充当虚拟防火墙，可应用于任何一组相关资源，以便一致地定义允许入站和出站流量的规则。除了基于 IP 地址和端口的规则之外，安全组还支持允许来自其他安全组关联资源的流量的规则。例如，数据库安全组可以设置规则，仅允许来自应用程序服务器安全组的流量。

默认情况下，安全组允许所有出站流量，但不允许入站流量。可以删除出站流量规则，也可以配置添加的其他规则，来限制出站流量和允许入站流量。如果安全组没有出站规则，则不允许来自您的实例的出站流量。有关更多信息，请参阅使用安全组控制到资源的流量（Amazon VPC 文档）。

在以下示例中，有三个安全组，用于控制从应用程序负载均衡器到连接到 Amazon RDS for MySQL 数据库的 EC2 实例的流量。

| 安全组 | 入站规则 | 出站规则 |
| --- | --- | --- |
| 应用程序负载均衡器安全组 | 描述：允许来自任何位置的 HTTPS 流量<br><br>类型：HTTPS<br><br>来源：Anywhere-IPv4（0.0.0.0/0） | 描述：允许所有流量到达任何位置<br><br>类型：所有流量<br><br>目标：Anywhere-IPv4（0.0.0.0/0） |
| EC2 实例安全组 | 描述：允许来自应用程序负载均衡器的 HTTP 流量<br><br>类型：HTTP<br><br>来源：应用程序负载均衡器安全组 | 描述：允许所有流量到达任何位置<br><br>类型：所有流量<br><br>目标：Anywhere-IPv4（0.0.0.0/0） |
| RDS 数据库安全组 | 描述：允许来自 EC2 实例的 MySQL 流量<br><br>类型：MySQL<br><br>来源：EC2 实例安全组 | 无出站规则 |

# WKLD.12 - 使用 VPC 端点访问支持的服务

在 VPC 中，需要访问 AWS 或其他外部服务的资源需要一个到互联网（`0.0.0.0/0`）或目标服务的公有 IP 地址的路由。使用 VPC 端点启用从 VPC 到受支持 AWS 或其他服务的私有 IP 路由，以避免使用互联网网关、NAT 设备、虚拟专用网络（VPN）连接或 AWS Direct Connect 连接。

VPC 端点支持附加策略和安全组，以进一步控制对服务的访问。例如，您可以为 Amazon DynamoDB 编写 VPC 端点策略，只允许对 VPC 中的所有资源执行项目级操作，并阻止执行表级操作，无论其自身的权限策略如何。您还可以编写 S3 存储桶策略，仅允许来自特定 VPC 端点的请求，拒绝所有其他外部访问。VPC 端点还可以设置安全组规则，例如，只允许访问与特定应用程序安全组关联的 EC2 实例，比如 Web 应用程序的业务逻辑层。

VPC 端点有多种类型。您可以使用 VPC 接口端点访问大多数服务。使用网关端点访问 DynamoDB。Amazon S3 支持网关端点和接口端点。对于包含在单个 AWS 账户和区域中的工作负

载，建议使用网关端点，并且不收取额外费用。如果需要更具可扩展性的访问，例如，从其他 VPC、本地网络或不同的 AWS 区域 访问 S3 存储桶，则建议使用接口端点。接口端点会产生每小时正常运行时间费用和每 GB 数据处理费用，这两项费用均低于通过 AWS NAT 网关向 `0.0.0.0/0` 发送数据的相应费用。

有关使用 VPC 端点的更多信息，请参阅以下资源：

- 有关在 Amazon S3 的网关和接口端点之间进行选择的更多信息，请参阅为 Amazon S3 选择 VPC 端点策略（AWS 博客文章）。
- 创建接口端点（Amazon VPC 文档）。
- 创建网关端点（Amazon VPC 文档）。
- 有关限制访问特定 VPC 或 VPC 端点的 S3 存储桶策略示例，请参阅限制访问特定 VPC（Amazon S3 文档）。
- 有关限制操作的 DynamoDB 端点策略示例，请参阅 DynamoDB 端点策略（Amazon VPS 文档）

## WKLD.13 - 所有公有 Web 端点都需要使用 HTTPS

需要使用 HTTPS 为您的 Web 端点提供额外的可信度，允许您的端点使用证书来证明其身份，并确认您的端点和连接的客户端之间的所有流量均已加密。对于公共网站，这还能带来提高搜索引擎排名的额外好处。

很多 AWS 服务都为您的资源提供了公有 Web 端点，比如 AWS Elastic Beanstalk、Amazon CloudFront、Amazon API Gateway、Elastic Load Balancing 和 AWS Amplify。有关这些服务如何要求使用 HTTPS 的说明，请参阅以下内容：

- Elastic Beanstalk（Elastic Beanstalk 文档）
- CloudFront（CloudFront 文档）
- 应用程序负载均衡器（AWS 知识中心）
- 经典负载均衡器（AWS 知识中心）
- Amplify（Amplify 文档）

Amazon S3 上托管的静态网站不支持 HTTPS。若要对这些网站要求 HTTPS，您可以使用 CloudFront。无需公开访问通过 CloudFront 提供内容的 S3 存储桶。

若要使用 CloudFront 为 Amazon S3 上托管的静态网站提供服务

1. 使用 CloudFront 为 Amazon S3 上托管的静态网站提供服务（AWS 知识中心）。
2. 如果您要配置对公有 S3 存储桶的访问，需要在查看器和 CloudFront 之间使用 HTTPS（CloudFront 文档）。

   如果您要配置对私有 S3 存储桶的访问，使用来源访问身份限制对 Amazon S3 内容的访问（CloudFront 文档）。

此外，将 HTTPS 端点配置为需要现代传输层安全性（TLS）协议和密码，除非需要与旧协议兼容。例如，使用 `ELBSecurityPolicy-FS-1-2-Res-2020-10` 或适用于应用程序负载均衡器 HTTPS 侦听器的最新策略，而不是默认的 `ELBSecurityPolicy-2016-08`。最新的策略至少需要 TLS 1.2、向前保密以及与现代 Web 浏览器兼容的强密码。

有关 HTTPS 公有端点的可用安全策略的更多信息，请参阅：

- 适用于经典负载均衡器的预定义 SSL 安全策略（Elastic Load Balancing 文档）
- 适用于应用程序负载均衡器的安全策略（Elastic Load Balancing 文档）
- 查看器和 CloudFront 之间支持的协议和密码（CloudFront 文档）

## WKLD.14 - 对公有端点使用边缘保护服务

与其直接从 EC2 实例或容器等计算服务提供流量，不如使用边缘保护服务。这将在来自互联网的传入流量和服务该流量的资源之间建立额外的安全层。这些服务可以在流量到达内部资源之前过滤不需要的流量，强制加密，应用路由或其他规则，如负载均衡。

可提供公有端点保护的 AWS 服务包括 AWS WAF、CloudFront、Elastic Load Balancing、API Gateway 和 Amplify Hosting。在公有子网中运行基于 VPC 的服务（如 Elastic Load Balancing），作为在私有子网中运行的 Web 服务资源的代理。

CloudFront、API Gateway 和 Amazon Route 53 可免费提供第 3 层和第 4 层分布式拒绝服务（DDoS）攻击防护，AWS WAF 可抵御第 7 层攻击。

有关如何开始使用这些服务的说明，请参阅以下内容：

- AWS WAF 入门（AWS 网站）
- Amazon CloudFront 入门（CloudFront 文档）
- Elastic Load Balancing 入门（Elastic Load Balancing 文档）

- API Gateway 入门（API Gateway 文档）
- Amplify Hosting 入门（Amplify 文档）

# WKLD.15 - 在模板中定义安全控制，并使用 CI/CD 实践进行部署

基础设施即代码（IaC）是在模板和代码中定义所有 AWS 服务资源和配置的做法，这些模板和代码是使用持续集成和持续交付（CI/CD）管道部署的，而这些管道与用来部署软件应用程序的管道相同。IaC 服务（如 AWS CloudFormation）支持基于 IAM 身份和基于资源的策略，并支持 AWS 安全服务（如 Amazon GuardDuty、AWS WAF 和 Amazon VPC）。捕获这些构件作为 IaC 模板，将模板提交到源代码存储库，然后使用 CI/CD 管道进行部署。

除非另有要求，否则在同一存储库中使用应用程序代码提交应用程序权限策略，并在单独的代码存储库和部署管道中管理常规资源策略和安全服务配置。

有关 AWS 上的 IaC 入门的更多信息，请参阅 AWS Cloud Development Kit (AWS CDK) 文档。

# 贡献者

本文档的贡献者包括：

- Jay Michael，首席解决方案架构师
- Cole Calistra，首席解决方案架构师
- Justin Plock，首席解决方案架构师
- Faisal Farooq，解决方案架构师
- Michael Nguyen，高级解决方案架构师
- Ritik Khatwani，高级解决方案架构师
- Paul Hawkins，首席信息安全官（CISO）办公室负责人

特别感谢下列在指导和审查方面提供帮助的人员：

- Robert Put
- Mike Sullivan
- Bob Lee III

# 文档历史记录

下表介绍了本指南的一些重要更改。如果您希望收到有关未来更新的通知，可以订阅 RSS 源。

| 变更 | 说明 | 日期 |
| --- | --- | --- |
| Amazon S3 存储桶设置 | 我们更新了 ACCT.08 – 阻止公开访问私有 S3 存储桶部分，以反映 2023 年 4 月 28 日之后创建的 Amazon S3 存储桶默认启用阻止公开访问设置。 | 2023 年 5 月 18 日 |
| IAM 安全最佳实践 | 我们更新了本指南，以便与最新的 AWS Identity and Access Management（IAM）最佳实践保持一致。有关更多信息，请参阅 IAM 文档中的安全最佳实践。 | 2023 年 2 月 1 日 |
| IAM 角色 | 我们在 WKLD.01 – 使用 IAM 角色获取计算环境权限部分中提供了 AWS 服务 文档的额外链接。 | 2022 年 9 月 22 日 |
| 密码策略 | 我们更新了有关强密码的建议，采用了 Center for Internet Security（CIS）的最新指南。 | 2022 年 5 月 10 日 |
| 初次发布 | — | 2022 年 4 月 13 日 |

# AWS 规范性指导词汇表

以下是 AWS 规范性指导提供的策略、指南和模式中的常用术语。若要推荐词条，请使用术语表末尾的提供反馈链接。

## 数字

7 R

将应用程序迁移到云中的 7 种常见迁移策略。这些策略以 Gartner 于 2011 年确定的 5 R 为基础，包括以下内容：

- 重构/重新架构 - 充分利用云原生功能来提高敏捷性、性能和可扩展性，以迁移应用程序并修改其架构。这通常涉及到移植操作系统和数据库。示例：将本地 Oracle 数据库迁移到 Amazon Aurora PostgreSQL 兼容版。
- 更换平台 - 将应用程序迁移到云中，并进行一定程度的优化，以利用云功能。示例：将您的本地 Oracle 数据库迁移到 AWS 云端适用于 Oracle 的亚马逊关系数据库服务 (Amazon RDS)。
- 重新购买 - 转换到其他产品，通常是从传统许可转向 SaaS 模式。示例：将客户关系管理（CRM）系统迁移到 Salesforce.com。
- 更换主机（直接迁移）- 将应用程序迁移到云中，无需进行任何更改即可利用云功能。示例：将您的本地 Oracle 数据库迁移到 AWS 云中 EC2 实例上的 Oracle。
- 重新定位（虚拟机监控器级直接迁移）：将基础设施迁移到云中，无需购买新硬件、重写应用程序或修改现有操作。此迁移场景特定于 VMware Cloud on AWS，它支持虚拟机 (VM) 兼容性和本地环境与之间的工作负载可移植性。 AWS在将基础设施迁移到 VMware Cloud on AWS时，您可以在本地数据中心使用 VMware Cloud Foundation 技术。示例：将托管 Oracle 数据库的虚拟机管理程序重新部署到 VMware Cloud 上。 AWS
- 保留（重访）- 将应用程序保留在源环境中。其中可能包括需要进行重大重构的应用程序，并且您希望将工作推迟到以后，以及您希望保留的遗留应用程序，因为迁移它们没有商业上的理由。
- 停用 - 停用或删除源环境中不再需要的应用程序。

## A

ABAC

请参阅基于属性的访问控制。

抽象服务

参见托管服务。

酸

参见原子性、一致性、隔离性、耐久性。

主动-主动迁移

一种数据库迁移方法，在这种方法中，源数据库和目标数据库保持同步（通过使用双向复制工具或双写操作），两个数据库都在迁移期间处理来自连接应用程序的事务。这种方法支持小批量、可控的迁移，而不需要一次性割接。与主动-被动迁移相比，它更灵活，但需要更多的工作。

主动-被动迁移

一种数据库迁移方法，在这种方法中，源数据库和目标数据库保持同步，但在将数据复制到目标数据库时，只有源数据库处理来自连接应用程序的事务。目标数据库在迁移期间不接受任何事务。

聚合函数

一个 SQL 函数，它对一组行进行操作并计算该组的单个返回值。聚合函数的示例包括SUM和MAX。

AI

参见人工智能。

AIOps

参见人工智能操作。

匿名化

永久删除数据集中个人信息的过程。匿名化可以帮助保护个人隐私。匿名化数据不再被视为个人数据。

反模式

一种用于解决反复出现的问题的常用解决方案，而在这类问题中，此解决方案适得其反、无效或不如替代方案有效。

应用程序控制

一种安全方法，仅允许使用经批准的应用程序，以帮助保护系统免受恶意软件的侵害。

应用程序组合

有关组织使用的每个应用程序的详细信息的集合，包括构建和维护该应用程序的成本及其业务价值。这些信息是产品组合发现和分析过程的关键，有助于识别需要进行迁移、现代化和优化的应用程序并确定其优先级。

人工智能（AI）

计算机科学领域致力于使用计算技术执行通常与人类相关的认知功能，例如学习、解决问题和识别模式。有关更多信息，请参阅什么是人工智能？

人工智能运营（AIOps）

使用机器学习技术解决运营问题、减少运营事故和人为干预以及提高服务质量的过程。有关如何在 AWS 迁移策略中使用 AIOps 的更多信息，请参阅运营集成指南。

非对称加密

一种加密算法，使用一对密钥，一个公钥用于加密，一个私钥用于解密。您可以共享公钥，因为它不用于解密，但对私钥的访问应受到严格限制。

原子性、一致性、隔离性、持久性（ACID）

一组软件属性，即使在出现错误、电源故障或其他问题的情况下，也能保证数据库的数据有效性和操作可靠性。

基于属性的访问权限控制（ABAC）

根据用户属性（如部门、工作角色和团队名称）创建精细访问权限的做法。有关更多信息，请参阅 AWS Identity and Access Management (I AM) 文档 AWS中的 AB AC。

权威数据源

存储主要数据版本的位置，被认为是最可靠的信息源。您可以将数据从权威数据源复制到其他位置，以便处理或修改数据，例如对数据进行匿名化、编辑或假名化。

可用区

中的一个不同位置 AWS 区域 ，不受其他可用区域故障的影响，并向同一区域中的其他可用区提供低成本、低延迟的网络连接。

AWS 云采用框架 (AWS CAF)

该框架包含指导方针和最佳实践 AWS ，可帮助组织制定高效且有效的计划，以成功迁移到云端。AWS CAF将指导分为六个重点领域，称为视角：业务、人员、治理、平台、安全和运营。业务、人员和治理角度侧重于业务技能和流程；平台、安全和运营角度侧重于技术技能和流程。例如，人员角度针对的是负责人力资源（HR）、人员配置职能和人员管理的利益相关者。从这个角度来看，AWS CAF 为人员发展、培训和沟通提供了指导，以帮助组织为成功采用云做好准备。有关更多信息，请参阅 AWS CAF 网站和 AWS CAF 白皮书。

AWS 工作负载资格框架 (AWS WQF)

一种评估数据库迁移工作负载、推荐迁移策略和提供工作估算的工具。 AWS WQF 包含在 AWS Schema Conversion Tool (AWS SCT) 中。它用来分析数据库架构和代码对象、应用程序代码、依赖关系和性能特征，并提供评测报告。

# B

坏机器人

旨在破坏个人或组织或对其造成伤害的机器人。

BCP

参见业务连续性计划。

行为图

一段时间内资源行为和交互的统一交互式视图。您可以使用 Amazon Detective 的行为图来检查失败的登录尝试、可疑的 API 调用和类似的操作。有关更多信息，请参阅 Detective 文档中的行为图中的数据。

大端序系统

一个先存储最高有效字节的系统。另请参见字节顺序。

二进制分类

一种预测二进制结果（两个可能的类别之一）的过程。例如，您的 ML 模型可能需要预测诸如“该电子邮件是否为垃圾邮件？”或“这个产品是书还是汽车？”之类的问题

bloom 筛选条件

一种概率性、内存高效的数据结构，用于测试元素是否为集合的成员。

蓝/绿部署

一种部署策略，您可以创建两个独立但完全相同的环境。在一个环境中运行当前的应用程序版本（蓝色），在另一个环境中运行新的应用程序版本（绿色）。此策略可帮助您在影响最小的情况下快速回滚。

自动程序

一种通过互联网运行自动任务并模拟人类活动或互动的软件应用程序。有些机器人是有用或有益的，例如在互联网上索引信息的网络爬虫。其他一些被称为恶意机器人的机器人旨在破坏个人或组织或对其造成伤害。

僵尸网络

被恶意软件感染并受单方（称为机器人牧民或机器人操作员）控制的机器人网络。僵尸网络是最著名的扩展机器人及其影响力的机制。

分支

代码存储库的一个包含区域。在存储库中创建的第一个分支是主分支。您可以从现有分支创建新分支，然后在新分支中开发功能或修复错误。为构建功能而创建的分支通常称为功能分支。当功能可以发布时，将功能分支合并回主分支。有关更多信息，请参阅关于分支（GitHub 文档）。

破碎的玻璃通道

在特殊情况下，通过批准的流程，用户 AWS 账户 可以快速访问他们通常没有访问权限的内容。有关更多信息，请参阅 Well -Architected 指南中的 “实施破碎玻璃程序” 指示 AWS 器。

棕地策略

您环境中的现有基础设施。在为系统架构采用棕地策略时，您需要围绕当前系统和基础设施的限制来设计架构。如果您正在扩展现有基础设施，则可以将棕地策略和全新策略混合。

缓冲区缓存

存储最常访问的数据的内存区域。

业务能力

企业如何创造价值（例如，销售、客户服务或营销）。微服务架构和开发决策可以由业务能力驱动。有关更多信息，请参阅在 AWS上运行容器化微服务白皮书中的围绕业务能力进行组织部分。

业务连续性计划（BCP）

一项计划，旨在应对大规模迁移等破坏性事件对运营的潜在影响，并使企业能够快速恢复运营。

# C

CAF

参见AWS 云采用框架。

金丝雀部署

向最终用户缓慢而渐进地发布版本。当您确信时，可以部署新版本并全部替换当前版本。

CCoE

参见云卓越中心。

CDC

参见变更数据捕获。

更改数据捕获（CDC）

跟踪数据来源（如数据库表）的更改并记录有关更改的元数据的过程。您可以将 CDC 用于各种目的，例如审计或复制目标系统中的更改以保持同步。

混沌工程

故意引入故障或破坏性事件来测试系统的弹性。您可以使用 AWS Fault Injection Service (AWS FIS) 来执行实验，对您的 AWS 工作负载施加压力并评估其响应。

CI/CD

查看持续集成和持续交付。

分类

一种有助于生成预测的分类流程。分类问题的 ML 模型预测离散值。离散值始终彼此不同。例如，一个模型可能需要评估图像中是否有汽车。

客户端加密

在目标 AWS 服务 收到数据之前，对数据进行本地加密。

云卓越中心（CCoE）

一个多学科团队，负责推动整个组织的云采用工作，包括开发云最佳实践、调动资源、制定迁移时间表、领导组织完成大规模转型。有关更多信息，请参阅 AWS 云企业战略博客上的 CCoE 帖子。

云计算

通常用于远程数据存储和 IoT 设备管理的云技术。云计算通常与边缘计算技术相关。

云运营模型

在 IT 组织中，一种用于构建、完善和优化一个或多个云环境的运营模型。有关更多信息，请参阅构建您的云运营模型。

云采用阶段

组织迁移到 AWS 云端时通常要经历的四个阶段：

- 项目 - 出于概念验证和学习目的，开展一些与云相关的项目
- 基础 - 进行基础投资以扩大云采用率（例如，创建登录区、定义 CCoE、建立运营模型）
- 迁移 - 迁移单个应用程序

- 重塑 - 优化产品和服务，在云中创新

Stephen Orban 在 “云企业战略” 博客文章《云优先之旅和采用阶段》中定义了 AWS 这些阶段。有关它们与 AWS 迁移策略的关系的信息，请参阅迁移准备指南。

CMDB

参见配置管理数据库。

代码存储库

通过版本控制过程存储和更新源代码和其他资产（如文档、示例和脚本）的位置。常见的云存储库包括 GitHub 或 AWS CodeCommit。每个版本的代码都称为一个分支。在微服务结构中，每个存储库都专门用于一个功能。单个 CI/CD 管道可以使用多个存储库。

冷缓存

一种空的、填充不足或包含过时或不相关数据的缓冲区缓存。这会影响性能，因为数据库实例必须从主内存或磁盘读取，这比从缓冲区缓存读取要慢。

冷数据

很少访问的数据，且通常是历史数据。查询此类数据时，通常可以接受慢速查询。将这些数据转移到性能较低且成本更低的存储层或类别可以降低成本。

计算机视觉 (CV)

人工智能领域，使用机器学习来分析和提取数字图像和视频等视觉格式的信息。例如， AWS Panorama 提供将 CV 添加到本地摄像机网络的设备，而 Amazon 则为 CV SageMaker 提供图像处理算法。

配置偏差

对于工作负载，配置会从预期状态发生变化。这可能会导致工作负载变得不合规，而且通常是渐进的，不是故意的。

配置管理数据库（CMDB）

一种存储库，用于存储和管理有关数据库及其 IT 环境的信息，包括硬件和软件组件及其配置。您通常在迁移的产品组合发现和分析阶段使用来自 CMDB 的数据。

合规性包

一系列 AWS Config 规则和补救措施，您可以汇编这些规则和补救措施，以自定义合规性和安全性检查。您可以使用 YAML 模板将一致性包作为单个实体部署在 AWS 账户 和区域或整个组织中。有关更多信息，请参阅 AWS Config 文档中的一致性包。

持续集成和持续交付（CI/CD）

自动执行软件发布过程的源代码、构建、测试、暂存和生产阶段的过程。CI/CD 通常被描述为管道。CI/CD 可以帮助您实现流程自动化、提高工作效率、改善代码质量并加快交付速度。有关更多信息，请参阅持续交付的优势。CD 也可以表示持续部署。有关更多信息，请参阅持续交付与持续部署。

CV

参见计算机视觉。

# D

静态数据

网络中静止的数据，例如存储中的数据。

数据分类

根据网络中数据的关键性和敏感性对其进行识别和分类的过程。它是任何网络安全风险管理策略的关键组成部分，因为它可以帮助您确定对数据的适当保护和保留控制。数据分类是 Well-Architecte AWS d Framework 中安全支柱的一个组成部分。有关详细信息，请参阅数据分类。

数据漂移

生产数据与用来训练机器学习模型的数据之间的有意义差异，或者输入数据随时间推移的有意义变化。数据漂移可能降低机器学习模型预测的整体质量、准确性和公平性。

传输中数据

在网络中主动移动的数据，例如在网络资源之间移动的数据。

数据网格

一种架构框架，可提供分布式、去中心化的数据所有权以及集中式管理和治理。

数据最少化

仅收集并处理绝对必要数据的原则。在中进行数据最小化 AWS Cloud 可以降低隐私风险、成本和分析碳足迹。

数据边界

AWS 环境中的一组预防性防护措施，可帮助确保只有可信身份才能访问来自预期网络的可信资源。有关更多信息，请参阅在上构建数据边界。 AWS

数据预处理

将原始数据转换为 ML 模型易于解析的格式。预处理数据可能意味着删除某些列或行，并处理缺失、不一致或重复的值。

数据溯源

在数据的整个生命周期跟踪其来源和历史的过程，例如数据如何生成、传输和存储。

数据主体

正在收集和处理其数据的个人。

数据仓库

一种支持商业智能（例如分析）的数据管理系统。数据仓库通常包含大量历史数据，通常用于查询和分析。

数据库定义语言（DDL）

在数据库中创建或修改表和对象结构的语句或命令。

数据库操作语言（DML）

在数据库中修改（插入、更新和删除）信息的语句或命令。

DDL

参见数据库定义语言。

深度融合

组合多个深度学习模型进行预测。您可以使用深度融合来获得更准确的预测或估算预测中的不确定性。

深度学习

一个 ML 子字段使用多层人工神经网络来识别输入数据和感兴趣的目标变量之间的映射。

defense-in-depth

一种信息安全方法，经过深思熟虑，在整个计算机网络中分层实施一系列安全机制和控制措施，以保护网络及其中数据的机密性、完整性和可用性。当你采用这种策略时 AWS，你会在 AWS Organizations 结构的不同层面添加多个控件来帮助保护资源。例如，一种 defense-in-depth 方法可以结合多因素身份验证、网络分段和加密。

委托管理员

在中 AWS Organizations，兼容的服务可以注册 AWS 成员帐户来管理组织的帐户并管理该服务的权限。此账户被称为该服务的委托管理员。有关更多信息和兼容服务列表，请参阅 AWS Organizations 文档中使用 AWS Organizations的服务。

部署

使应用程序、新功能或代码修复在目标环境中可用的过程。部署涉及在代码库中实现更改，然后在应用程序的环境中构建和运行该代码库。

开发环境

参见环境。

侦测性控制

一种安全控制，在事件发生后进行检测、记录日志和发出警报。这些控制是第二道防线，提醒您注意绕过现有预防性控制的安全事件。有关更多信息，请参阅在 AWS上实施安全控制中的侦测性控制。

开发价值流映射 (DVSM)

用于识别对软件开发生命周期中的速度和质量产生不利影响的限制因素并确定其优先级的流程。DVSM 扩展了最初为精益生产实践设计的价值流映射流程。其重点关注在软件开发过程中创造和转移价值所需的步骤和团队。

数字孪生

真实世界系统的虚拟再现，如建筑物、工厂、工业设备或生产线。数字孪生支持预测性维护、远程监控和生产优化。

维度表

在星型架构中，一种较小的表，其中包含事实表中定量数据的数据属性。维度表属性通常是文本字段或行为类似于文本的离散数字。这些属性通常用于查询约束、筛选和结果集标注。

灾难

阻止工作负载或系统在其主要部署位置实现其业务目标的事件。这些事件可能是自然灾害、技术故障或人为操作的结果，例如无意的配置错误或恶意软件攻击。

灾难恢复 (DR)

您用来最大限度地减少灾难造成的停机时间和数据丢失的策略和流程。有关更多信息，请参阅 Well-Architected Fr ame AWS work 中的 “工作负载灾难恢复：云端 AWS 恢复”。

DML

参见数据库操作语言。

领域驱动设计

一种开发复杂软件系统的方法，通过将其组件连接到每个组件所服务的不断发展的领域或核心业务目标。Eric Evans 在其著作领域驱动设计：软件核心复杂性应对之道（Boston: Addison-Wesley Professional, 2003）中介绍了这一概念。有关如何将领域驱动设计与 strangler fig 模式结合使用的信息，请参阅使用容器和 Amazon API Gateway 逐步将原有的 Microsoft ASP.NET（ASMX）Web 服务现代化。

DR

参见灾难恢复。

漂移检测

跟踪与基准配置的偏差。例如，您可以使用 AWS CloudFormation 来检测系统资源中的偏差，也可以使用 AWS Control Tower 来检测着陆区中可能影响监管要求合规性的变化。

DVSM

参见开发价值流映射。

# E

EDA

参见探索性数据分析。

边缘计算

该技术可提高位于 IoT 网络边缘的智能设备的计算能力。与云计算相比，边缘计算可以减少通信延迟并缩短响应时间。

加密

一种将人类可读的纯文本数据转换为密文的计算过程。

加密密钥

由加密算法生成的随机位的加密字符串。密钥的长度可能有所不同，而且每个密钥都设计为不可预测且唯一。

字节顺序

字节在计算机内存中的存储顺序。大端序系统先存储最高有效字节。小端序系统先存储最低有效字节。

端点

参见服务端点。

端点服务

一种可以在虚拟私有云（VPC）中托管，与其他用户共享的服务。您可以使用其他 AWS 账户 或 AWS Identity and Access Management (IAM) 委托人创建终端节点服务， AWS PrivateLink 并向其授予权限。这些账户或主体可通过创建接口 VPC 端点来私密地连接到您的端点服务。有关更多信息，请参阅 Amazon Virtual Private Cloud（Amazon VPC）文档中的创建端点服务。

企业资源规划 (ERP)

一种自动化和管理企业关键业务流程（例如会计、MES 和项目管理）的系统。

信封加密

用另一个加密密钥对加密密钥进行加密的过程。有关更多信息，请参阅 AWS Key Management Service (AWS KMS) 文档中的信封加密。

environment

正在运行的应用程序的实例。以下是云计算中常见的环境类型：

- 开发环境 — 正在运行的应用程序的实例，只有负责维护应用程序的核心团队才能使用。开发环境用于测试更改，然后再将其提升到上层环境。这类环境有时称为测试环境。
- 下层环境 — 应用程序的所有开发环境，比如用于初始构建和测试的环境。
- 生产环境 — 最终用户可以访问的正在运行的应用程序的实例。在 CI/CD 管道中，生产环境是最后一个部署环境。
- 上层环境 — 除核心开发团队以外的用户可以访问的所有环境。这可能包括生产环境、预生产环境和用户验收测试环境。

epic

在敏捷方法学中，有助于组织工作和确定优先级的功能类别。epics 提供了对需求和实施任务的总体描述。例如， AWS CAF 安全史诗包括身份和访问管理、侦探控制、基础设施安全、数据保护和事件响应。有关 AWS 迁移策略中 epics 的更多信息，请参阅计划实施指南。

ERP

参见企业资源规划。

探索性数据分析（EDA）

分析数据集以了解其主要特征的过程。您收集或汇总数据，并进行初步调查，以发现模式、检测异常并检查假定情况。EDA 通过计算汇总统计数据和创建数据可视化得以执行。

# F

事实表

星形架构中的中心表。它存储有关业务运营的定量数据。通常，事实表包含两种类型的列：包含度量的列和包含维度表外键的列。

失败得很快

一种使用频繁和增量测试来缩短开发生命周期的理念。这是敏捷方法的关键部分。

故障隔离边界

在中 AWS Cloud，诸如可用区 AWS 区域、控制平面或数据平面之类的边界，它限制了故障的影响并有助于提高工作负载的弹性。有关更多信息，请参阅AWS 故障隔离边界。

功能分支

参见分支。

特征

您用来进行预测的输入数据。例如，在制造环境中，特征可能是定期从生产线捕获的图像。

特征重要性

特征对于模型预测的重要性。这通常表示为数值分数，可以通过各种技术进行计算，例如 Shapley 加法解释（SHAP）和积分梯度。有关更多信息，请参阅机器学习模型的可解释性：AWS。

功能转换

为 ML 流程优化数据，包括使用其他来源丰富数据、扩展值或从单个数据字段中提取多组信息。这使得 ML 模型能从数据中获益。例如，如果您将“2021-05-27 00:15:37”日期分解为“2021”、“五月”、“星期四”和“15”，则可以帮助学习与不同数据成分相关的算法学习精细模式。

FGAC

请参阅精细的访问控制。

精细访问控制 (FGAC)

使用多个条件允许或拒绝访问请求。

快闪迁移

一种数据库迁移方法，它使用连续的数据复制，通过更改数据捕获在尽可能短的时间内迁移数据，而不是使用分阶段的方法。目标是将停机时间降至最低。

# G

地理封锁

请参阅地理限制。

地理限制（地理阻止）

在 Amazon 中 CloudFront，一种阻止特定国家/地区的用户访问内容分发的选项。您可以使用允许列表或阻止列表来指定已批准和已禁止的国家/地区。有关更多信息，请参阅 CloudFront 文档中的限制内容的地理分布。

GitFlow 工作流程

一种方法，在这种方法中，下层和上层环境在源代码存储库中使用不同的分支。Gitflow 工作流程被认为是传统的，而基于主干的工作流程是现代的首选方法。

全新策略

在新环境中缺少现有基础设施。在对系统架构采用全新策略时，您可以选择所有新技术，而不受对现有基础设施（也称为棕地）兼容性的限制。如果您正在扩展现有基础设施，则可以将棕地策略和全新策略混合。

防护机制

一种高级规则，用于跨组织单位（OU）管理资源、策略和合规性。预防性防护机制会执行策略以确保符合合规性标准。它们是使用服务控制策略和 IAM 权限边界实现的。侦测性防护机制会检测策略违规和合规性问题，并生成警报以进行修复。它们通过使用 AWS Config、、Amazon、 AWS Security Hub GuardDuty AWS Trusted Advisor、Amazon Inspector 和自定义 AWS Lambda 支票来实现。

# H

HA

参见高可用性。

异构数据库迁移

将源数据库迁移到使用不同数据库引擎的目标数据库（例如，从 Oracle 迁移到 Amazon Aurora）。异构迁移通常是重新架构工作的一部分，而转换架构可能是一项复杂的任务。AWS 提供了 AWS SCT 来帮助实现架构转换。

高可用性 (HA)

在遇到挑战或灾难时，工作负载无需干预即可连续运行的能力。HA 系统旨在自动进行故障转移、持续提供良好性能，并以最小的性能影响处理不同负载和故障。

历史数据库现代化

一种用于实现运营技术 (OT) 系统现代化和升级以更好满足制造业需求的方法。历史数据库是一种用于收集和存储工厂中各种来源数据的数据库。

同构数据库迁移

将源数据库迁移到共享同一数据库引擎的目标数据库（例如，从 Microsoft SQL Server 迁移到 Amazon RDS for SQL Server）。同构迁移通常是更换主机或更换平台工作的一部分。您可以使用本机数据库实用程序来迁移架构。

热数据

经常访问的数据，例如实时数据或近期的转化数据。这些数据通常需要高性能存储层或存储类别才能提供快速的查询响应。

修补程序

针对生产环境中关键问题的紧急修复。由于其紧迫性，修补程序通常是在典型的 DevOps 发布工作流程之外进行的。

hypercare 周期

割接之后，迁移团队立即管理和监控云中迁移的应用程序以解决任何问题的时间段。通常，这个周期持续 1-4 天。在 hypercare 周期结束时，迁移团队通常会将应用程序的责任移交给云运营团队。

## I

IaC

参见基础架构即代码。

基于身份的策略

附加到一个或多个 IAM 委托人的策略，用于定义他们在 AWS Cloud 环境中的权限。

空闲应用程序

90 天内平均 CPU 和内存使用率在 5% 到 20% 之间的应用程序。在迁移项目中，通常会停用这些应用程序或将其保留在本地。

IIoT

参见工业物联网。

不可变的基础架构

一种为生产工作负载部署新基础架构，而不是更新、修补或修改现有基础架构的模型。不可变基础架构本质上比可变基础架构更一致、更可靠、更可预测。有关更多信息，请参阅 Well-Architected Framework 中的使用不可变基础架构 AWS 部署最佳实践。

入站（入口）VPC

在 AWS 多账户架构中，一种接受、检查和路由来自应用程序外部的网络连接的 VPC。AWS 安全参考架构建议使用入站、出站和检查 VPC 设置网络账户，保护应用程序与广泛的互联网之间的双向接口。

增量迁移

一种割接策略，在这种策略中，您可以将应用程序分成小部分进行迁移，而不是一次性完整割接。例如，您最初可能只将几个微服务或用户迁移到新系统。在确认一切正常后，您可以逐步迁移其他微服务或用户，直到停用遗留系统。这种策略降低了大规模迁移带来的风险。

工业 4.0

该术语由克劳斯·施瓦布（Klaus Schwab）于2016年推出，指的是通过连接、实时数据、自动化、分析和人工智能/机器学习的进步实现制造流程的现代化。

基础设施

应用程序环境中包含的所有资源和资产。

基础设施即代码（IaC）

通过一组配置文件预置和管理应用程序基础设施的过程。IaC 旨在帮助您集中管理基础设施、实现资源标准化和快速扩展，使新环境具有可重复性、可靠性和一致性。

工业物联网（IIoT）

在工业领域使用联网的传感器和设备，例如制造业、能源、汽车、医疗保健、生命科学和农业。有关更多信息，请参阅制定工业物联网（IIoT）数字化转型策略。

检查 VPC

在 AWS 多账户架构中，一种集中式 VPC，用于管理 VPC（相同或不同 AWS 区域）、互联网和本地网络之间的网络流量检查。AWS 安全参考架构建议使用入站、出站和检查 VPC 设置网络账户，保护应用程序与广泛的互联网之间的双向接口。

物联网（IoT）

由带有嵌入式传感器或处理器的连接物理对象组成的网络，这些传感器或处理器通过互联网或本地通信网络与其他设备和系统进行通信。有关更多信息，请参阅什么是 IoT？

可解释性

它是机器学习模型的一种特征，描述了人类可以理解模型的预测如何取决于其输入的程度。有关更多信息，请参阅使用 AWS 实现机器学习模型的可解释性。

IoT

参见物联网。

IT 信息库（ITIL）

提供 IT 服务并使这些服务符合业务要求的一套最佳实践。ITIL 是 ITSM 的基础。

IT 服务管理（ITSM）

为组织设计、实施、管理和支持 IT 服务的相关活动。有关将云运营与 ITSM 工具集成的信息，请参阅运营集成指南。

ITIL

请参阅 IT 信息库。

ITSM

请参阅 IT 服务管理。

# L

基于标签的访问控制 (LBAC)

强制访问控制 (MAC) 的一种实施方式，其中明确为用户和数据本身分配了安全标签值。用户安全标签和数据安全标签之间的交集决定了用户可以看到哪些行和列。

登录区

landing zone 是一个架构精良的多账户 AWS 环境，具有可扩展性和安全性。这是一个起点，您的组织可以从这里放心地在安全和基础设施环境中快速启动和部署工作负载和应用程序。有关登录区的更多信息，请参阅设置安全且可扩展的多账户 AWS 环境。

大规模迁移

迁移 300 台或更多服务器。

LBAC

参见基于标签的访问控制。

最低权限

授予执行任务所需的最低权限的最佳安全实践。有关更多信息，请参阅 IAM 文档中的应用最低权限许可。

直接迁移

见 7 R。

小端序系统

一个先存储最低有效字节的系统。另请参见字节顺序。

下层环境

参见环境。

# M

机器学习（ML）

一种使用算法和技术进行模式识别和学习的人工智能。ML 对记录的数据（例如物联网（IoT）数据）进行分析和学习，以生成基于模式的统计模型。有关更多信息，请参阅机器学习。

主分支

参见分支。

恶意软件

旨在危害计算机安全或隐私的软件。恶意软件可能会破坏计算机系统、泄露敏感信息或获得未经授权的访问。恶意软件的示例包括病毒、蠕虫、勒索软件、特洛伊木马、间谍软件和键盘记录器。

托管服务

AWS 服务 它 AWS 运行基础设施层、操作系统和平台，您可以访问端点来存储和检索数据。亚马逊简单存储服务 (Amazon S3) Service 和 Amazon DynamoDB 就是托管服务的示例。这些服务也称为抽象服务。

制造执行系统 (MES)

一种软件系统，用于跟踪、监控、记录和控制在车间将原材料转化为成品的生产过程。

MAP

参见迁移加速计划。

机制

一个完整的过程，在此过程中，您可以创建工具，推动工具的采用，然后检查结果以进行调整。机制是一种在运行过程中自我增强和改进的循环。有关更多信息，请参阅在 Well-Architect AWS ed 框架中构建机制。

成员账户

AWS 账户 除属于组织中的管理账户之外的所有账户 AWS Organizations。一个账户一次只能是一个组织的成员。

MES

参见制造执行系统。

消息队列遥测传输 (MQTT)

一种基于发布/订阅模式的轻量级 machine-to-machine (M2M) 通信协议，适用于资源受限的物联网设备。

微服务

一种小型独立服务，通过明确定义的 API 进行通信，通常由小型独立团队拥有。例如，保险系统可能包括映射到业务能力（如销售或营销）或子域（如购买、理赔或分析）的微服务。微服务的好处包括敏捷、灵活扩展、易于部署、可重复使用的代码和恢复能力。有关更多信息，请参阅使用 AWS 无服务器服务集成微服务。

微服务架构

一种使用独立组件构建应用程序的方法，这些组件将每个应用程序进程作为微服务运行。这些微服务使用轻量级 API 通过明确定义的接口进行通信。该架构中的每个微服务都可以更新、部署和扩展，以满足对应用程序特定功能的需求。有关更多信息，请参阅在上实现微服务。 AWS

迁移加速计划（MAP）

AWS 该计划提供咨询支持、培训和服务，以帮助组织为迁移到云奠定坚实的运营基础，并帮助抵消迁移的初始成本。MAP 提供了一种以系统的方式执行遗留迁移的迁移方法，以及一套用于自动执行和加速常见迁移场景的工具。

大规模迁移

将大部分应用程序组合分波迁移到云中的过程，在每一波中以更快的速度迁移更多应用程序。本阶段使用从早期阶段获得的最佳实践和经验教训，实施由团队、工具和流程组成的迁移工厂，通过自动化和敏捷交付简化工作负载的迁移。这是 AWS 迁移策略的第三阶段。

迁移工厂

跨职能团队，通过自动化、敏捷的方法简化工作负载迁移。迁移工厂团队通常包括运营、业务分析师和所有者、迁移工程师、开发 DevOps 人员和冲刺专业人员。20% 到 50% 的企业应用程序组合由可通过工厂方法优化的重复模式组成。有关更多信息，请参阅本内容集中有关迁移工厂的讨论和云迁移工厂指南。

迁移元数据

有关完成迁移所需的应用程序和服务器的信息。每种迁移模式都需要一套不同的迁移元数据。迁移元数据的示例包括目标子网、安全组和 AWS 账户。

迁移模式

一种可重复的迁移任务，详细列出了迁移策略、迁移目标以及所使用的迁移应用程序或服务。示例：使用 AWS 应用程序迁移服务重新托管向 Amazon EC2 的迁移。

迁移组合评测（MPA）

一种在线工具，可提供信息，用于验证迁移到 AWS 云端的业务案例。MPA 提供了详细的组合评测（服务器规模调整、定价、TCO 比较、迁移成本分析）以及迁移计划（应用程序数据分析和数据收集、应用程序分组、迁移优先级排序和波次规划）。所有 AWS 顾问和 APN 合作伙伴顾问均可免费使用 MPA 工具（需要登录）。

迁移准备情况评测（MRA）

使用 AWS CAF 深入了解组织的云就绪状态、确定优势和劣势以及制定行动计划以缩小已发现差距的过程。有关更多信息，请参阅迁移准备指南。MRA 是 AWS 迁移策略的第一阶段。

迁移策略

用于将工作负载迁移到 AWS 云端的方法。有关更多信息，请参阅此词汇表中的 7 R 条目和动员组织以加快大规模迁移。

ML

参见机器学习。

现代化

将过时的（原有的或单体）应用程序及其基础设施转变为云中敏捷、弹性和高度可用的系统，以降低成本、提高效率和利用创新。有关更多信息，请参阅中的应用程序现代化策略。 AWS Cloud

现代化准备情况评估

一种评估方式，有助于确定组织应用程序的现代化准备情况；确定收益、风险和依赖关系；确定组织能够在多大程度上支持这些应用程序的未来状态。评估结果是目标架构的蓝图、详细说明现代化进程发展阶段和里程碑的路线图以及解决已发现差距的行动计划。有关详细信息，请参阅在 AWS 云中评估应用程序的现代化准备情况。

单体应用程序（单体式）

作为具有紧密耦合进程的单个服务运行的应用程序。单体应用程序有几个缺点。如果某个应用程序功能的需求激增，则必须扩展整个架构。随着代码库的增长，添加或改进单体应用程序的功能也会变得更加复杂。若要解决这些问题，可以使用微服务架构。有关更多信息，请参阅将单体分解为微服务。

MPA

参见迁移组合评估。

MQTT

请参阅消息队列遥测传输。

多分类器

一种帮助为多个类别生成预测（预测两个以上结果之一）的过程。例如，ML 模型可能会询问“这个产品是书、汽车还是手机？”或“此客户最感兴趣什么类别的产品？”

可变基础架构

一种用于更新和修改现有生产工作负载基础架构的模型。为了提高一致性、可靠性和可预测性，Well-Architect AWS ed Framework 建议使用不可变基础设施作为最佳实践。

# O

OAC

请参阅源站访问控制。

OAI

参见源访问身份。

OCM

参见组织变更管理。

离线迁移

一种迁移方法，在这种方法中，源工作负载会在迁移过程中停止运行。这种方法会延长停机时间，通常用于小型非关键工作负载。

OI

参见运营集成。

OLA

参见运营层协议。

在线迁移

一种迁移方法，在这种方法中，源工作负载无需离线即可复制到目标系统。在迁移过程中，连接工作负载的应用程序可以继续运行。这种方法的停机时间为零或最短，通常用于关键生产工作负载。

OPC-UA

参见开放流程通信-统一架构。

开放流程通信-统一架构 (OPC-UA)

一种用于工业自动化的 machine-to-machine （M2M）通信协议。OPC-UA 提供了数据加密、身份验证和授权方案的互操作性标准。

运营级别协议（OLA）

一项协议，阐明了 IT 职能部门承诺相互交付的内容，以支持服务水平协议（SLA）。

运营准备情况审查 (ORR)

一份问题清单和相关的最佳实践，可帮助您理解、评估、预防或缩小事件和可能的故障的范围。有关更多信息，请参阅 Well-Architecte AWS d Frame work 中的运营准备情况评估 (ORR)。

操作技术 (OT)

与物理环境配合使用以控制工业运营、设备和基础设施的硬件和软件系统。在制造业中，OT 和信息技术 (IT) 系统的集成是工业 4.0 转型的重点。

运营整合（OI）

在云中实现运营现代化的过程，包括就绪计划、自动化和集成。有关更多信息，请参阅运营整合指南。

组织跟踪

由 AWS CloudTrail 此创建的跟踪记录组织 AWS 账户 中所有人的所有事件 AWS Organizations。该跟踪是在每个 AWS 账户 中创建的，属于组织的一部分，并跟踪每个账户的活动。有关更多信息，请参阅 CloudTrail文档中的为组织创建跟踪。

组织变革管理（OCM）

一个从人员、文化和领导力角度管理重大、颠覆性业务转型的框架。OCM 通过加快变革采用、解决过渡问题以及推动文化和组织变革，帮助组织为新系统和战略做好准备和过渡。在 AWS 迁移策略中，该框架被称为人员加速，因为云采用项目需要变更的速度。有关更多信息，请参阅 OCM 指南。

来源访问控制（OAC）

中 CloudFront，一个增强的选项，用于限制访问以保护您的亚马逊简单存储服务 (Amazon S3) 内容。OAC 全部支持所有 S3 存储桶 AWS 区域、使用 AWS KMS (SSE-KMS) 进行服务器端加密，以及对 S3 存储桶的动态PUT和DELETE请求。

来源访问身份（OAI）

在中 CloudFront，一个用于限制访问权限以保护您的 Amazon S3 内容的选项。当您使用 OAI 时，CloudFront 会创建一个 Amazon S3 可以对其进行身份验证的委托人。经过身份验证的委托人只能通过特定 CloudFront 分配访问 S3 存储桶中的内容。另请参阅 OAC，其中提供了更精细和增强的访问控制。

或者

参见运营准备情况审查。

OT

参见运营技术。

出站（出口）VPC

在 AWS 多账户架构中，一种处理从应用程序内部启动的网络连接的 VPC。AWS 安全参考架构建议使用入站、出站和检查 VPC 设置网络账户，保护应用程序与广泛的互联网之间的双向接口。

# P

权限边界

附加到 IAM 主体的 IAM 管理策略，用于设置用户或角色可以拥有的最大权限。有关更多信息，请参阅 IAM 文档中的权限边界。

个人身份信息 (PII)

直接查看其他相关数据或与之配对时可用于合理推断个人身份的信息。PII 的示例包括姓名、地址和联系信息。

PII

查看个人身份信息。

playbook

一套预定义的步骤，用于捕获与迁移相关的工作，例如在云中交付核心运营功能。playbook 可以采用脚本、自动化运行手册的形式，也可以是操作现代化环境所需的流程或步骤的摘要。

PLC

参见可编程逻辑控制器。

PLM

参见产品生命周期管理。

策略

一个对象，可以在中定义权限（参见基于身份的策略）、指定访问条件（参见基于资源的策略）或定义组织中所有账户的最大权限 AWS Organizations （参见服务控制策略）。

多语言持久性

根据数据访问模式和其他要求，独立选择微服务的数据存储技术。如果您的微服务采用相同的数据存储技术，它们可能会遇到实现难题或性能不佳。如果微服务使用最适合其需求的数据存储，则可以更轻松地实现微服务，并获得更好的性能和可扩展性。有关更多信息，请参阅在微服务中实现数据持久性。

组合评测

一个发现、分析和确定应用程序组合优先级以规划迁移的过程。有关更多信息，请参阅评估迁移准备情况。

谓词

返回`true`或的查询条件`false`，通常位于子`WHERE`句中。

谓词下推

一种数据库查询优化技术，可在传输前筛选查询中的数据。这减少了必须从关系数据库检索和处理的数据量，并提高了查询性能。

预防性控制

一种安全控制，旨在防止事件发生。这些控制是第一道防线，帮助防止未经授权的访问或对网络的意外更改。有关更多信息，请参阅在 AWS上实施安全控制中的预防性控制。

主体

中 AWS 可以执行操作和访问资源的实体。此实体通常是 IAM 角色的根用户或用户。 AWS 账户有关更多信息，请参阅 IAM 文档中角色术语和概念中的主体。

隐私设计

一种贯穿整个工程化过程考虑隐私的系统工程方法。

私有托管区

私有托管区就是一个容器，其中包含的信息说明您希望 Amazon Route 53 如何响应一个或多个 VPC 中的某个域及其子域的 DNS 查询。有关更多信息，请参阅 Route 53 文档中的私有托管区的使用。

主动控制

一种安全控制措施，旨在防止部署不合规的资源。这些控件会在资源配置之前对其进行扫描。如果资源与控件不兼容，则不会对其进行配置。有关更多信息，请参阅 AWS Control Tower 文档中的控制参考指南，并参见在上实施安全控制中的主动控制 AWS。

产品生命周期管理 (PLM)

在产品的整个生命周期中，从设计、开发和上市，到成长和成熟，再到衰落和移除，对产品进行数据和流程的管理。

生产环境

参见环境。

可编程逻辑控制器 (PLC)

在制造业中，一种高度可靠、适应性强的计算机，用于监控机器并实现制造过程自动化。

假名化

用占位符值替换数据集中个人标识符的过程。假名化可以帮助保护个人隐私。假名化数据仍被视为个人数据。

发布/订阅（发布/订阅）

一种支持微服务间异步通信的模式，以提高可扩展性和响应能力。例如，在基于微服务的 MES 中，微服务可以将事件消息发布到其他微服务可以订阅的频道。系统可以在不更改发布服务的情况下添加新的微服务。

# Q

查询计划

一系列步骤，例如指令，用于访问 SQL 关系数据库系统中的数据。

查询计划回归

当数据库服务优化程序选择的最佳计划不如数据库环境发生特定变化之前时。这可能是由统计数据、约束、环境设置、查询参数绑定更改和数据库引擎更新造成的。

# R

RACI 矩阵

参见负责任、负责、咨询、知情（RACI）。

勒索软件

一种恶意软件，旨在阻止对计算机系统或数据的访问，直到付款为止。

RASCI 矩阵

参见负责任、负责、咨询、知情（RACI）。

RCAC

请参阅行和列访问控制。

只读副本

用于只读目的的数据库副本。您可以将查询路由到只读副本，以减轻主数据库的负载。

重新架构师

见 7 R。

恢复点目标 (RPO)

自上一个数据恢复点以来可接受的最长时间。这决定了从上一个恢复点到服务中断之间可接受的数据丢失情况。

恢复时间目标 (RTO)

服务中断和服务恢复之间可接受的最大延迟。

重构

见 7 R。

区域

地理区域内的 AWS 资源集合。每一个 AWS 区域 都相互隔离，彼此独立，以提供容错、稳定性和弹性。有关更多信息，请参阅指定 AWS 区域 您的账户可以使用的账户。

回归

一种预测数值的 ML 技术。例如，要解决“这套房子的售价是多少？”的问题 ML 模型可以使用线性回归模型，根据房屋的已知事实（如建筑面积）来预测房屋的销售价格。

重新托管

见 7 R。

版本

在部署过程中，推动生产环境变更的行为。

搬迁

见 7 R。

更换平台

见 7 R。

回购

见 7 R。

故障恢复能力

应用程序抵御中断或从中断中恢复的能力。在中规划弹性时，高可用性和灾难恢复是常见的考虑因素。 AWS Cloud有关更多信息，请参阅AWS Cloud 弹性。

基于资源的策略

一种附加到资源的策略，例如 AmazonS3 存储桶、端点或加密密钥。此类策略指定了允许哪些主体访问、支持的操作以及必须满足的任何其他条件。

责任、问责、咨询和知情（RACI）矩阵

定义参与迁移活动和云运营的所有各方的角色和责任的矩阵。矩阵名称源自矩阵中定义的责任类型：负责 (R)、问责 (A)、咨询 (C) 和知情 (I)。支持 (S) 类型是可选的。如果包括支持，则该矩阵称为 RASCI 矩阵，如果将其排除在外，则称为 RACI 矩阵。

响应性控制

一种安全控制，旨在推动对不良事件或偏离安全基线的情况进行修复。有关更多信息，请参阅在AWS上实施安全控制中的响应性控制。

保留

见 7 R。

退休

见 7 R。

旋转

定期更新密钥以使攻击者更难访问凭据的过程。

行列访问控制 (RCAC)

使用已定义访问规则的基本、灵活的 SQL 表达式。RCAC 由行权限和列掩码组成。

RPO

参见恢复点目标。

RTO

参见恢复时间目标。

运行手册

执行特定任务所需的一套手动或自动程序。它们通常是为了简化重复性操作或高错误率的程序而设计的。

# S

SAML 2.0

许多身份提供商 (IdPs) 使用的开放标准。此功能支持联合单点登录 (SSO)，因此用户无需在 IAM 中为组织中的所有人创建用户即可登录 AWS Management Console 或调用 AWS API 操作。有关基于 SAML 2.0 的联合身份验证的更多信息，请参阅 IAM 文档中的关于基于 SAML 2.0 的联合身份验证。

SCADA

参见监督控制和数据采集。

SCP

参见服务控制政策。

secret

在中 AWS Secrets Manager，您以加密形式存储的机密或受限信息，例如密码或用户凭证。它由密钥值及其元数据组成。密钥值可以是二进制、单个字符串或多个字符串。有关更多信息，请参阅 Sec rets Manager 文档中的密钥。

安全控制

一种技术或管理防护机制，可防止、检测或降低威胁行为体利用安全漏洞的能力。安全控制主要有四种类型：预防性、侦测、响应式和主动式。

安全加固

缩小攻击面，使其更能抵御攻击的过程。这可能包括删除不再需要的资源、实施授予最低权限的最佳安全实践或停用配置文件中不必要的功能等操作。

安全信息和事件管理（SIEM）系统

结合了安全信息管理（SIM）和安全事件管理（SEM）系统的工具和服务。SIEM 系统会收集、监控和分析来自服务器、网络、设备和其他来源的数据，以检测威胁和安全漏洞，并生成警报。

安全响应自动化

一种预定义和编程的操作，旨在自动响应或修复安全事件。这些自动化可作为侦探或响应式安全控制措施，帮助您实施 AWS 安全最佳实践。自动响应操作的示例包括修改 VPC 安全组、修补 Amazon EC2 实例或轮换证书。

服务器端加密

由接收数据的人在目的地对数据 AWS 服务 进行加密。

服务控制策略（SCP）

一种策略，用于集中控制 AWS Organizations的组织中所有账户的权限。SCP 为管理员可以委托给用户或角色的操作定义了防护机制或设定了限制。您可以将 SCP 用作允许列表或拒绝列表，指定允许或禁止哪些服务或操作。有关更多信息，请参阅 AWS Organizations 文档中的服务控制策略。

服务端点

的入口点的 URL AWS 服务。您可以使用端点，通过编程方式连接到目标服务。有关更多信息，请参阅 AWS 一般参考 中的 AWS 服务 端点。

服务水平协议（SLA）

一份协议，阐明了 IT 团队承诺向客户交付的内容，比如服务正常运行时间和性能。

服务级别指示器 (SLI)

对服务性能方面的衡量，例如其错误率、可用性或吞吐量。

服务级别目标 (SLO)

代表服务运行状况的目标指标，由服务级别指标衡量。

责任共担模式

描述您在云安全与合规方面共同承担 AWS 的责任的模型。 AWS 负责云的安全，而您则负责云中的安全。有关更多信息，请参阅责任共担模式。

暹粒

参见安全信息和事件管理系统。

单点故障 (SPOF)

应用程序的单个关键组件出现故障，可能会中断系统。

SLA

参见服务级别协议。

SLI

参见服务级别指标。

SLO

参见服务级别目标。

split-and-seed 模型

一种扩展和加速现代化项目的模式。随着新功能和产品发布的定义，核心团队会拆分以创建新的产品团队。这有助于扩展组织的能力和服务，提高开发人员的工作效率，支持快速创新。有关更多信息，请参阅中的分阶段实现应用程序现代化的方法。 AWS Cloud

恶作剧

参见单点故障。

星型架构

一种数据库组织结构，它使用一个大型事实表来存储交易数据或测量数据，并使用一个或多个较小的维度表来存储数据属性。此结构专为在数据仓库中使用或用于商业智能目的而设计。

strangler fig 模式

一种通过逐步重写和替换系统功能直至可以停用原有的系统来实现单体系统现代化的方法。这种模式用无花果藤作为类比，这种藤蔓成长为一棵树，最终战胜并取代了宿主。该模式是由 Martin Fowler 提出的，作为重写单体系统时管理风险的一种方法。有关如何应用此模式的示例，请参阅使用容器和 Amazon API Gateway 逐步将原有的 Microsoft ASP.NET（ASMX）Web 服务现代化。

子网

您的 VPC 内的一个 IP 地址范围。子网必须位于单个可用区中。

监控和数据采集 (SCADA)

在制造业中，一种使用硬件和软件来监控有形资产和生产操作的系统。

对称加密

一种加密算法，它使用相同的密钥来加密和解密数据。

综合测试

以模拟用户交互的方式测试系统，以检测潜在问题或监控性能。你可以使用 Amazon S CloudWatch ynthetics 来创建这些测试。

# T

tags

键值对，用作组织资源的元数据。 AWS 标签可帮助您管理、识别、组织、搜索和筛选资源。有关更多信息，请参阅标记您的 AWS 资源。

目标变量

您在监督式 ML 中尝试预测的值。这也被称为结果变量。例如，在制造环境中，目标变量可能是产品缺陷。

任务列表

一种通过运行手册用于跟踪进度的工具。任务列表包含运行手册的概述和要完成的常规任务列表。对于每项常规任务，它包括预计所需时间、所有者和进度。

测试环境

参见环境。

训练

为您的 ML 模型提供学习数据。训练数据必须包含正确答案。学习算法在训练数据中查找将输入数据属性映射到目标（您希望预测的答案）的模式。然后输出捕获这些模式的 ML 模型。然后，您可以使用 ML 模型对不知道目标的新数据进行预测。

中转网关

中转网关是网络中转中心，您可用它来互连 VPC 和本地网络。有关更多信息，请参阅 AWS Transit Gateway 文档中的什么是公交网关。

基于中继的工作流程

一种方法，开发人员在功能分支中本地构建和测试功能，然后将这些更改合并到主分支中。然后，按顺序将主分支构建到开发、预生产和生产环境。

可信访问权限

向您指定的服务授予权限，该服务可以代表您在其账户中执行任务。 AWS Organizations 当需要服务相关的角色时，受信任的服务会在每个账户中创建一个角色，为您执行管理任务。有关更多信息，请参阅 AWS Organizations 文档中的AWS Organizations 与其他 AWS 服务一起使用。

优化

更改训练过程的各个方面，以提高 ML 模型的准确性。例如，您可以通过生成标签集、添加标签，并在不同的设置下多次重复这些步骤来优化模型，从而训练 ML 模型。

双披萨团队

一个小 DevOps 团队，你可以用两个披萨来喂食。双披萨团队的规模可确保在软件开发过程中充分协作。

# U

不确定性

这一概念指的是不精确、不完整或未知的信息，这些信息可能会破坏预测式 ML 模型的可靠性。不确定性有两种类型：认知不确定性是由有限的、不完整的数据造成的，而偶然不确定性是由数据中固有的噪声和随机性导致的。有关更多信息，请参阅量化深度学习系统中的不确定性指南。

无差别任务

也称为繁重工作，即创建和运行应用程序所必需的工作，但不能为最终用户提供直接价值或竞争优势。无差别任务的示例包括采购、维护和容量规划。

上层环境

参见环境。

# V

vacuum 操作

一种数据库维护操作，包括在增量更新后进行清理，以回收存储空间并提高性能。

版本控制

跟踪更改的过程和工具，例如存储库中源代码的更改。

VPC 对等连接

两个 VPC 之间的连接，允许您使用私有 IP 地址路由流量。有关更多信息，请参阅 Amazon VPC 文档中的什么是 VPC 对等连接。

漏洞

损害系统安全的软件缺陷或硬件缺陷。

# W

热缓存

一种包含经常访问的当前相关数据的缓冲区缓存。数据库实例可以从缓冲区缓存读取，这比从主内存或磁盘读取要快。

暖数据

不常访问的数据。查询此类数据时，通常可以接受中速查询。

窗口函数

一个 SQL 函数，用于对一组以某种方式与当前记录相关的行进行计算。窗口函数对于处理任务很有用，例如计算移动平均线或根据当前行的相对位置访问行的值。

工作负载

一系列资源和代码，它们可以提供商业价值，如面向客户的应用程序或后端过程。

工作流

迁移项目中负责一组特定任务的职能小组。每个工作流都是独立的，但支持项目中的其他工作流。例如，组合工作流负责确定应用程序的优先级、波次规划和收集迁移元数据。组合工作流将这些资产交付给迁移工作流，然后迁移服务器和应用程序。

蠕虫

参见一次写入，多读。

WQF

请参阅 AWS 工作负载资格框架。

一次写入，多次读取 (WORM)

一种存储模型，它可以一次写入数据并防止数据被删除或修改。授权用户可以根据需要多次读取数据，但他们无法对其进行更改。这种数据存储基础架构被认为是不可变的。

# Z

零日漏洞利用

一种利用未修补漏洞的攻击，通常是恶意软件。

零日漏洞

生产系统中不可避免的缺陷或漏洞。威胁主体可能利用这种类型的漏洞攻击系统。开发人员经常因攻击而意识到该漏洞。

僵尸应用程序

平均 CPU 和内存使用率低于 5% 的应用程序。在迁移项目中，通常会停用这些应用程序。

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。