自动驾驶数据框架（ADDF）安全和操作指南

AWS 规范性指导

AWS 规范性指导: 自动驾驶数据框架（ADDF）安全和操作指南

Table of Contents

简介 1
目标受众 1
目标业务成果 1
架构和术语 2
ADDF 术语 2
ADDF 架构 3
责任共担模式 7
AWS 责任 8
ADDF 核心团队责任 8
ADDF 用户责任 9
一般 AWS 账户 责任 10
特定于 ADDF 的责任 10
安全审查流程 11
AWS 定期进行安全审查 11
开源安全审查和贡献 11
内置安全功能 12
ADDF 模块代码的最低权限 12
基础设施即代码 12
IaC 自动安全检查 13
AWS CDK 部署角色的自定义最低权限策略 13
模块部署规范文件的最低权限策略 14
数据加密 14
使用 Secrets Manager 存储凭证 14
SeedFarmer 和 CodeSeeder 的安全审查 14
针对 CodeSeeder AWS CodeBuild 角色的权限边界支持 15
AWS 多账户架构 15
多账户部署的最低权限许可 15
安全设置和操作 18
定义您的 ADDF 架构 18
在 PoC 环境中运行 ADDF 18
在生产环境中运行 ADDF 19
初始设置 22
自定义 ADDF 部署框架代码 22
在 ADDF 中编写自定义模块 23

重复部署 ADDF 23
重复进行安全审计 23
ADDF 更新 23
停用 24
后续步骤 25
资源 26
AWS 文档 26
开源资源 26
注意事项 27
文档历史记录 28
术语表 29
..... 29
A 29
B 32
C 33
D 36
E 39
F 41
G 42
H 42
I 43
L 45
M 46
O 49
P 52
Q 54
R 54
S 57
T 59
U 61
V 61
W 61
Z 62
..... lxiii

自动驾驶数据框架（ADDF）安全和操作指南

Andreas Falkenberg、Junjie Tang、Torsten Reitemeyer 和 Srinivas Reddy Cheruku，Amazon Web Services（AWS）

2022 年 11 月（文档历史记录）

自动驾驶数据框架（ADDF）是一个开源项目，旨在为想要实现高级驾驶辅助系统（ADAS）常见任务的汽车团队提供可重复使用的模块化代码构件，例如，配置集中式数据存储、数据处理管道、可视化机制、搜索界面、模拟工作负载、分析界面和预构建的控制面板。通过 ADDF，您可以共享、修改或创建完全可自定义的模块，从而减少创建和部署这些解决方案所需的工作量。

本指南旨在帮助您了解在 AWS Cloud 中安全部署和操作 ADDF 的最佳实践。本指南讨论了以下主题：

- 架构和术语 - 查看一般架构、工作流程和重要术语。
- 责任共担模式 - 了解您在确保 ADDF 部署和云资源安全方面的 AWS 角色和作用。
- 安全审查流程 - 由于 ADDF 是一个开源项目，查看 AWS 和贡献者如何完成安全审查。
- 内置安全功能 - 查看如何将安全最佳实践和功能内置到 ADDF 开源项目及其部署框架中。
- 安全设置和操作 - 了解如何在 AWS Cloud 中部署和操作 ADDF。

目标受众

本指南适用于负责评测、部署、自定义和操作 ADDF 的开发运营（DevOps）团队、基础设施工程师、管理员、IT 安全人员和事件响应团队。您可以将本指南中的建议应用于概念验证或生产环境。

本指南假定您之前不了解 ADDF。我们建议您在阅读 ADDF 自述文件（GitHub）之后再继续。

目标业务成果

本指南旨在帮助您在开发和生产环境中更加自信、安全地设置和操作 ADDF。

ADDF 架构和术语

在理解本指南中的安全和操作主题之前，务必先对自动驾驶数据框架（ADDF）的术语、组件和架构有一个深入的了解。本节包含以下主题：

- ADDF 术语
- ADDF 架构

ADDF 术语

ADDF 的主要术语如下所示：

- ADDF 模块 - 模块是指在高级驾驶辅助系统（ADAS）中实现常见任务的基础设施即代码（IaC）。常见任务包括配置集中式数据存储、数据处理管道、可视化机制、搜索界面、模拟工作负载、分析界面和预构建的控制面板。您可以根据自己的需求创建模块，也可以重复使用或自定义现有模块。

  您可以使用 AWS Cloud Development Kit (AWS CDK) 定义 ADDF 模块，也可以使用任何常见的 IaC 框架，比如 Hashicorp Terraform 或 AWS CloudFormation 来实现 ADDF 模块。一个模块有一组输入参数。输入参数可能取决于其他模块的输出值。ADDF 模块是 ADDF 目标 AWS 账户 最小的部署单元。
- ADDF 部署清单文件 - 该文件定义了独立 ADDF 模块的编排。编排是指模块的部署顺序。在 ADDF 部署清单文件中，您可以使用 ADDF 群组将相关模块分组在一起。在此文件中，您还可以定义 ADDF 工具链 AWS 账户、ADDF 目标 AWS 账户 和目标 AWS 区域。
- ADDF 部署框架 - 该框架根据 ADDF 部署清单文件中定义的编排将 ADDF 模块部署到 ADDF 目标 AWS 账户 中。ADDF 部署框架是使用以下 AWS 开源项目实现的：
  - SeedFarmer（GitHub）- SeedFarmer 是用于 ADDF 部署的 CLI 工具。它用来管理每个模块状态，准备和打包模块代码，为 ADDF 部署角色创建最低权限策略，并提供 CodeSeeder 用于部署的语义指令。您可以直接与 SeedFarmer 交互以运行 ADDF 部署，也可以将其集成到持续集成和持续部署（CI/CD）管道中。
  - CodeSeeder（GitHub）- CodeSeeder 通过 AWS CodeBuild 作业将任意基础设施部署为代码包。SeedFarmer 会自动编排和运行 CodeSeeder。只有 SeedFarmer 直接与 CodeSeeder 交互。

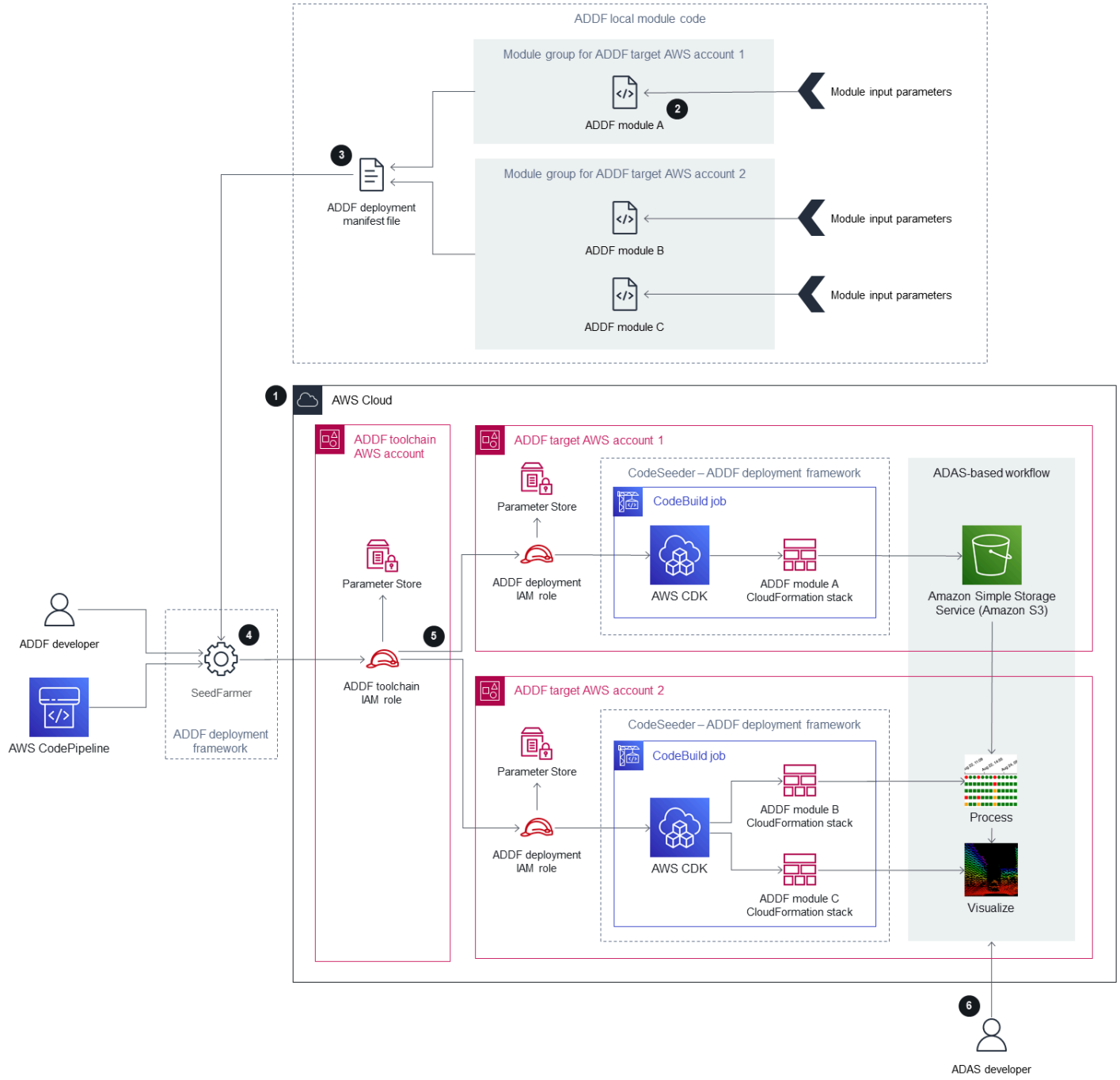
  ADDF 部署框架用来支持单账户和多账户架构中的部署。根据贵组织的需求，您可以决定需要单账户架构还是多账户架构。
- ADDF 工具链 AWS 账户 - 该账户根据 ADDF 部署清单文件中的定义编排和管理模块到 ADDF 目标 AWS 账户 的部署。一个 ADDF 部署只能有一个 ADDF 工具链 AWS 账户。在单账户架构

中，ADDF 工具链 AWS 账户 也是 ADDF 目标 AWS 账户。该账户包含一个 AWS Identity and Access Management（IAM）角色，称为 ADDF 工具链 IAM 角色，该角色由 SeedFarmer 在 ADDF 部署过程中承担。在本指南中，我们将 ADDF 工具链 AWS 账户 称为工具链账户。

- ADDF 目标 AWS 账户 - 这些是您在其中部署 ADDF 模块的目标账户。您可以拥有一个或多个目标账户。这些账户包含 ADDF 部署清单文件及其映射模块中描述的资源和应用程序逻辑。在单账户架构中，ADDF 目标 AWS 账户 也是 ADDF 工具链 AWS 账户。每个 ADDF 目标账户都包含一个 IAM 角色，称为 ADDF 部署 IAM 角色，该角色由 CodeSeeder 在部署过程中承担。在本指南中，我们将 ADDF 目标 AWS 账户 称为目标账户。
- ADDF 实例 - 当您在云中部署 ADDF 和模块时（如 ADDF 部署清单文件中所定义），它将成为 ADDF 实例。一个 ADDF 实例可以采用单账户或多账户架构，您可以部署多个 ADDF 实例。有关为您的用例选择实例数量和设计账户架构的更多信息，请参阅 定义您的 ADDF 架构。

ADDF 架构

下图显示了 AWS Cloud 中 ADDF 实例的高级架构。它显示了一个多账户架构，包括一个专用工具链账户和两个目标账户。本指南讨论了使用 ADDF 将资源部署到目标账户的端到端流程。



1. 创建并引导 ADDF AWS 账户。

   若要正常运行，必须将每个账户引导至 ADDF 和 AWS CDK。如果这是新的 ADDF 部署，或者您要添加新的目标账户，请执行以下操作：

   a. 在工具链账户和每个目标账户中引导 AWS CDK。有关说明，请参阅引导程序（AWS CDK 文档）。ADDF 使用 AWS CDK 来部署基础设施。

b. 在工具链账户和每个目标账户中引导 ADDF。有关说明，请参阅 ADDF 部署指南中的引导 AWS 账户。这将设置 SeedFarmer 和 CodeSeeder 所需的所有特定于 ADDF 的 IAM 角色。

> **Note**
>
> 只有在最初部署 ADDF 或添加新的目标账户时，才需要执行此步骤。该步骤不属于向已建立的 ADDF 实例重复部署 ADDF 的过程。

2. 创建或自定义 ADDF 模块。

   根据您要解决的特定问题创建或自定义 ADDF 模块。您的模块应代表一个独立的任务或一组任务。根据需要定义模块的输入参数，并将模块输出值用作其他模块的输入参数。

3. 在 ADDF 部署清单文件中定义模块编排。

   在 ADDF 清单文件中，将模块整理成组，并定义部署顺序和模块之间的依赖关系。在此文件中，您还可以为每个 ADDF 组及其模块指定单个工具链账户和目标账户（包括 AWS 区域）。

4. 评估 ADDF 部署清单文件并确定部署范围。

   ADDF 开发人员或 CI/CD 管道（如 AWS CodePipeline）通过调用 CLI 工具 SeedFarmer 开始对 ADDF 部署清单文件进行评估。若要开始评估：

   - SeedFarmer 使用 ADDF 部署清单文件作为评估的输入参数。
   - 若要承担 ADDF 工具链 IAM 角色，SeedFarmer 需使用步骤 1 中在 ADDF 引导过程中定义的相同且有效的 IAM 角色或用户凭证。

   如果 SeedFarmer 没有正确的凭证来承担 ADDF 工具链 IAM 角色，或者无法访问 ADDF 部署清单文件，则评估不会开始。

   如果 SeedFarmer 可以开始评估，它将在工具链账户中承担 ADDF 工具链 IAM 角色。SeedFarmer 可以从那里访问任何目标账户，只需在该账户中承担 ADDF 部署 IAM 角色。然后，SeedFarmer 会尝试读取工具链账户和目标账户中的任何 ADDF 元数据。将出现以下情况之一：

   - 如果没有 ADDF 元数据可以读取，则表明这是一个新的 ADDF 实例。SeedFarmer 确定部署范围是整个 ADDF 部署清单文件及其内容。
   - 如果存在 ADDF 元数据，SeedFarmer 会将 ADDF 部署清单文件及其内容与目标账户中现有已部署构件的 MD5 哈希值进行比较。如果检测到可部署的更改，该过程将继续。如果未检测到可部署的更改，该过程将结束。

5. 将范围内 ADDF 模块部署到目标账户。

根据 ADDF 部署清单文件和上一步的评估结果，CodeSeeder 现在有一个有序的部署列表要运行。根据该有序列表，CodeSeeder 会在每个相关目标账户中承担 ADDF 部署 IAM 角色。然后，它在 AWS CodeBuild 作业中运行 CodeSeeder，为 ADDF 模块创建或更新单个 IaC 部署（如 AWS CDK 应用程序）。默认情况下，ADDF 将 AWS CDK 用作其 IaC 框架，但也支持其他常见的 IaC 框架。为每个目标账户完成此过程后，您将拥有一个完全部署的、跨账户的、基于 ADAS 的端到端工作流，正如您在 ADDF 部署清单文件中定义的那样。

如果您使用单账户架构，则工具链账户和目标账户是同一个账户，并且一个账户具有上述所有功能。

6. 使用 ADDF 部署的基础设施。

ADAS 开发人员可以根据您的用例定义使用已部署的基于 ADAS 的工作流。

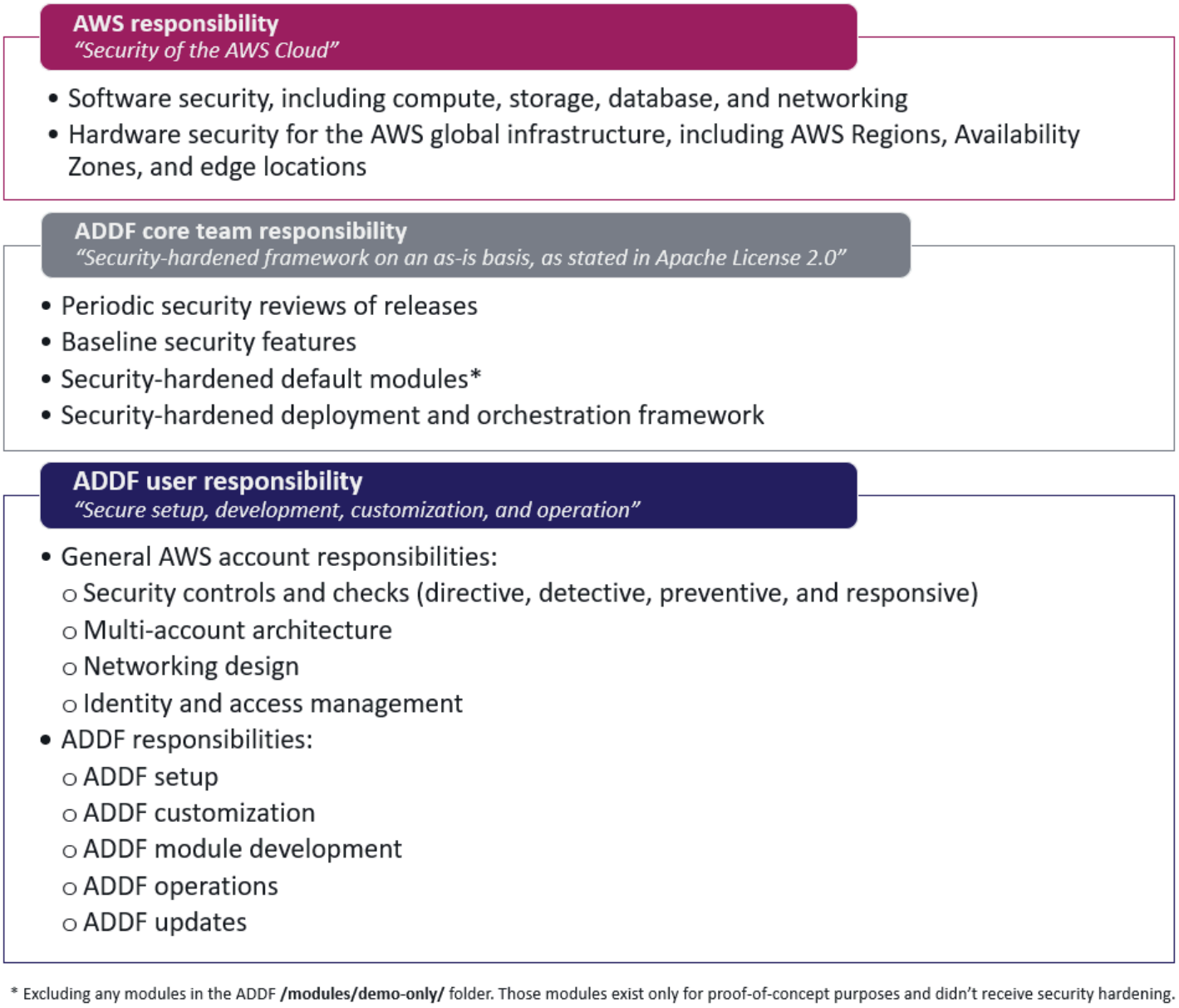
该工作流描述了 ADDF 多账户环境的单个实例的架构。根据您的开发、部署和操作模型，我们建议您在多阶段环境中运行多个 ADDF 实例。典型设置可能包括专用的 ADDF 实例，其中包含专用于每个部署阶段的 AWS 账户，比如开发、测试和生产分支。您也可以在同一 AWS 区域 的相同单账户或多账户环境中运行多个 ADDF 实例，假设您为每个 ADDF 实例创建了唯一的资源命名空间。有关更多信息，请参阅 定义您的 ADDF 架构。

ADDF 责任共担模式

适用于 AWS 服务 的责任共担模式也适用于自动驾驶数据框架（ADDF）。如下图所示，下列实体共同承担保护 ADDF 的责任：

- AWS - 云基础设施提供者提供 AWS 服务。
- ADDF 核心团队 - ADDF 核心团队是在 ADDF 存储库（GitHub）中发布 ADDF 版本的实体。
- ADDF 用户 - ADDF 用户包括但不限于：
  - ADDF 开发人员 - 任何更改、自定义或创建新 ADDF 模块代码的人。
  - ADDF 操作员 - 任何设置和操作 ADDF 实例的人。
  - ADAS 开发人员 - ADDF 部署的资源的最终用户或使用者。例如，ADAS 开发人员可以查询作为 ADDF 部署的一部分创建的可视化前端。

下图总结了 AWS、ADDF 核心团队和 ADDF 用户之间的共同责任。



AWS 责任

AWS 负责保护运行 AWS Cloud 中提供的所有服务的基础设施，正如 AWS 责任共担模式中定义的那样。该基础设施由运行 AWS Cloud 服务的硬件、软件、网络和设施组成。

ADDF 核心团队责任

根据 Apache 许可证 2.0（GitHub），ADDF 核心团队努力打造了一个本身安全的框架。ADDF 核心团队负责以下工作：

- 定期对版本进行安全审查
- 基线安全功能
- 安全加固的默认模块（不包括 /modules/demo-only/ 文件夹中的任何模块。这些模块仅用于概念验证，不会进行安全加固）。
- 安全加固的部署和编排框架

这些安全责任仅延伸到 GitHub 存储库中提供的框架，无需进行任何修改或自定义。这包括所有 ADDF 模块，modules/demo-only/ 文件夹中的 ADDF 模块除外。该文件夹中的 ADDF 模块未经过安全加固，不应部署在生产环境或任何包含敏感或受保护数据的环境中。包含这些模块是为了展示系统功能，您可以将它们作为创建自己的自定义安全加固模块的基础。

> **Note**
>
> ADDF 作为一个框架按原样交付。如 Apache 许可证 2.0（GitHub）中所述，它不附带任何责任和保证。您应自行对 ADDF 进行安全评测，验证其是否符合贵组织的特定安全要求。

ADDF 用户责任

只有以安全的方式设置、自定义和操作 ADDF 时，ADDF 及其模块才是安全的。ADDF 用户对以下方面的安全负全部责任：

- 一般 AWS 账户 责任：
  - 安全控制和检查（指令性、侦测性、预防性和响应性）
  - 多账户架构
  - 网络设计
  - 身份和访问管理
- 特定于 ADDF 的责任：
  - ADDF 设置
  - ADDF 自定义
  - ADDF 模块开发
  - ADDF 操作
  - ADDF 更新

一般 AWS 账户 责任

在将任何 ADDF 相关的资源部署到 AWS 账户 之前，应根据 AWS Well-Architected Framework 中的最佳实践配置 AWS 账户。这包括指导性、检测性、预防性和响应性安全控制。您应该制定详细的缓解流程，以防出现任何安全违规或事件。贵组织的策略应涵盖集中管理身份、访问权限和网络的要求。通常，这些要求和服务由专门的登录区团队处理。

特定于 ADDF 的责任

安全设置 ADDF

ADDF 用户的责任始于根据 ADDF 文档对 ADDF 进行安全设置。我们强烈建议您按照 ADDF 部署指南（GitHub）中的说明操作。有关安全设置 ADDF 的更多信息，请参阅 定义您的 ADDF 架构 和 初始设置。

安全自定义 ADDF

如果对 ADDF 核心功能（如 CodeSeeder、SeedFarmer 和 ADDF 核心模块）进行任何自定义，ADDF 用户对这些更改承担全部责任。有关更多信息，请参阅 自定义 ADDF 部署框架代码。

安全开发 ADDF 模块

ADDF 用户对使用 ADDF 部署的任何自定义模块负全部责任。此外，ADDF 用户负责对 ADDF 提供的模块进行任何代码更改。有关更多信息，请参阅 在 ADDF 中编写自定义模块。

安全更新和操作 ADDF

随着框架的演变，ADDF 会收到功能和安全更新。ADDF 用户负责定期检查发布到 GitHub 存储库的更新，并长期安全操作 ADDF。有关更多信息，请参阅 重复部署 ADDF、重复进行安全审计、ADDF 更新 和 停用。

ADDF 安全审查流程

自动驾驶数据框架（ADDF）在构建时充分考虑了安全性。在向公众发布之前，AWS 对 ADDF 进行了初步的内部安全审查，解决了所有已发现的安全问题。AWS 和开源社区都对框架的持续安全审查做出了贡献。

AWS 定期进行安全审查

ADDF 由 AWS 拥有的 awslabs GitHub 组织发布。AWS 会定期对该组织的代码进行自动和手动安全审查，充分验证安全性。根据 AWS 政策，AWS 不会披露有关安全审查频率、方法或所用工具的信息。此外，AWS 不会发布任何关于 ADDF 的内部审计报告。不过，任何已发现的安全调查结果都将通过拉取请求紧急修复和发布。

> **Note**
>
> ADDF 作为一个框架“按原样”交付，不附带任何明示或暗示的保证或条件，包括但不限于所有权、非侵权、适销性或特定用途适用性的任何保证或条件，正如 Apache 许可证 2.0（GitHub）所规定的。您应自行对 ADDF 进行安全评测，验证其是否符合贵组织的特定安全要求，正如 Apache 许可证 2.0 中规定的那样，您自行负责确定使用或重新分发 ADDF 的适当性，并承担您在该许可证下的行为或权限相关的任何风险。

开源安全审查和贡献

ADDF 是一个开源项目，每个人都可以做出贡献。我们邀请所有用户对自己的框架进行安全审查，并报告调查结果的任何安全问题。如果您在代码中发现问题，请遵循安全问题通知（ADDF 文档）中的指南。

ADDF 内置安全功能

自动驾驶数据框架（ADDF）具有各种内置安全功能。默认情况下，这些功能旨在帮助您建立安全框架，并帮助贵组织满足常见的企业安全要求。

以下是内置安全功能：

- ADDF 模块代码的最低权限
- 基础设施即代码
- IaC 自动安全检查
- AWS CDK 部署角色的自定义最低权限策略
- 模块部署规范文件的最低权限策略
- 数据加密
- 使用 Secrets Manager 存储凭证
- SeedFarmer 和 CodeSeeder 的安全审查
- 针对 CodeSeeder AWS CodeBuild 角色的权限边界支持
- AWS 多账户架构
- 多账户部署的最低权限许可

ADDF 模块代码的最低权限

最低权限是授予执行任务所需的最低权限的安全最佳实践。有关更多信息，请参阅应用最低权限许可。ADDF 提供的模块在其代码和部署的资源中严格遵循最低权限原则，如下所示：

- 为 ADDF 模块生成的所有 AWS Identity and Access Management（IAM）policy 都具有用例所需的最低权限。
- AWS 服务 是根据最低权限原则配置和部署的。ADDF 提供的模块仅使用特定用例所需的服务和服务功能。

基础设施即代码

ADDF 作为一个框架，用于将 ADDF 模块部署为基础设施即代码（IaC）。IaC 消除了手动部署过程，有助于防止手动过程可能导致的错误和配置错误。

ADDF 旨在使用任何常见的 IaC 框架来编排和部署模块。这包括但不限于：

- AWS Cloud Development Kit (AWS CDK)
- AWS CloudFormation
- Hashicorp Terraform

您可以使用不同的 IaC 框架来编写不同的模块，然后使用 ADDF 来部署它们。

ADDF 模块使用的默认 IaC 框架是 AWS CDK。AWS CDK 是一种面向对象的高级抽象，可以用它来强制性定义 AWS 资源。默认情况下，AWS CDK 已针对各种服务和场景强制执行安全最佳实践。使用 AWS CDK 降低了安全配置错误的风险。

IaC 自动安全检查

开源 cdk-nag 实用工具（GitHub）已集成到 ADDF 中。该实用工具会自动检查基于 AWS CDK 的 ADDF 模块是否符合一般和安全最佳实践。cdk-nag 实用工具使用规则和规则包来检测和报告违反最佳实践的代码。有关规则和完整列表的更多信息，请参阅 cdk-nag 规则（GitHub）。

AWS CDK 部署角色的自定义最低权限策略

ADDF 广泛使用 AWS CDK v2。您需要将所有 ADDF AWS 账户 引导至 AWS CDK。有关更多信息，请参阅引导程序（AWS CDK 文档）。

默认情况下，AWS CDK 将宽松的 AdministratorAccess AWS 管理策略分配给在引导账户中创建的 AWS CDK 部署角色。该角色的完整名称是 `cdk-[CDK_QUALIFIER]-cfn-exec-role-[AWS_ACCOUNT_ID]-[REGION]`。AWS CDK 使用该角色将资源部署到引导的 AWS 账户 中，作为 AWS CDK 部署过程的一部分。

根据贵组织的安全需求，`AdministratorAccess` 策略可能过于宽松。作为 AWS CDK 引导过程的一部分，您可以根据需要自定义策略和权限。您可以使用 `--cloudformation-execution-policies` 参数通过新定义的策略重新引导账户，来更改策略。有关更多信息，请参阅自定义引导程序（AWS CDK 文档）。

> **Note**
>
> 此安全功能并非 ADDF 所特有，但在本节中列出它是因为其可以提高 ADDF 部署的整体安全性。

模块部署规范文件的最低权限策略

每个模块都包含一个名为 deployspec.yaml 的部署规范文件。该文件定义了模块的部署说明。CodeSeeder 通过 AWS CodeBuild 用它在目标账户中部署定义的模块。CodeSeeder 按照部署规范文件中的说明，为 CodeBuild 分配一个默认服务角色来部署资源。该服务角色是根据最低权限原则设计的。它包括部署 AWS CDK 应用程序所需的所有权限，因为所有 ADDF 提供的模块都是作为 AWS CDK 应用程序创建的。

但是，如果需要在 AWS CDK 外部运行任何 stage 命令，则需要创建自定义 IAM policy，而非使用 CodeBuild 的默认服务角色。例如，如果您使用的是 AWS CDK 以外的 IaC 部署框架（如 Terraform），则需要创建一个 IAM policy，为特定框架运行授予足够的权限。另一个需要专用 IAM policy 的场景是，在 `install`、`pre_build`、`build` 或 `post_build` stage 命令中包含对其他 AWS 服务 的直接 AWS Command Line Interface（AWS CLI）调用时。例如，如果您的模块包含用于将文件上传到 S3 存储桶的 Amazon Simple Storage Service（Amazon S3）命令，则需要自定义策略。自定义 IAM policy 为 AWS CDK 部署以外的任何 AWS 命令提供精细控制。有关自定义 IAM policy 的示例，请参阅 ModuleStack（SeedFarmer 文档）。为 ADDF 模块创建自定义 IAM policy 时，确保应用最低权限许可。

数据加密

ADDF 会存储和处理潜在的敏感数据。为了保护这些数据，SeedFarmer、CodeSeeder 和 ADDF 提供的模块会对所有使用的 AWS 服务 进行静态数据和传输中数据加密（除非 `demo-only` 文件夹中的模块另有明确说明）。

使用 Secrets Manager 存储凭证

ADDF 会处理不同服务的各种密钥，例如 Docker Hub、JupyterHub 和 Amazon Redshift。ADDF 使用 AWS Secrets Manager 存储任何 ADDF 相关的密钥。这可以帮助您从源代码中删除敏感数据。

Secrets Manager 密钥仅存储在目标账户中，以满足该账户正常运行的需要。默认情况下，工具链账户不包含任何密钥。

SeedFarmer 和 CodeSeeder 的安全审查

SeedFarmer 和 CodeSeeder（GitHub 存储库）用于部署 ADDF 及其 ADDF 模块。这些开源项目经历了与 ADDF 相同的定期 AWS 内部安全审查过程，如 ADDF 安全审查流程 中所述。

针对 CodeSeeder AWS CodeBuild 角色的权限边界支持

IAM 权限边界是一种常见的安全机制，它定义了基于身份的策略可授予 IAM 实体的最大权限。SeedFarmer 和 CodeSeeder 支持每个目标账户的 IAM 权限边界附件。当 CodeSeeder 部署模块时，权限边界会限制 CodeBuild 使用的任何服务角色的最大权限。IAM 权限边界必须由安全团队在 ADDF 外部创建。IAM 权限边界策略附件作为 ADDF 部署清单文件 deployment.yaml 中的一个属性被接受。有关更多信息，请参阅 权限边界支持（SeedFarmer 文档）。

工作流程如下所示：

1. 您的安全团队根据您的安全需求定义和创建 IAM 权限边界。IAM 权限边界必须在每个 ADDF AWS 账户 中单独创建 输出是权限边界策略 Amazon 资源名称（ARN）列表。
2. 安全团队与您的 ADDF 开发团队共享策略 ARN 列表。
3. ADDF 开发人员团队将策略 ARN 列表集成到清单文件中。有关此集成的示例，请参阅 sample-permissionboundary.yaml（GitHub）和部署清单（SeedFarmer 文档）。
4. 成功部署后，权限边界将附加到 CodeBuild 用于部署模块的所有服务角色。
5. 安全团队会根据需要监控是否应用权限边界。

AWS 多账户架构

正如 AWS Well-Architected Framework 的安全支柱中所定义的那样，最佳做法是根据组织的需求将资源和工作负载分成多个 AWS 账户。这是因为 AWS 账户 充当隔离边界。有关更多信息，请参阅 AWS 账户 管理和分离。这一概念的实现称为多账户架构。与单账户架构相比，设计合理的 AWS 多账户架构可提供工作负载分类，在发生安全漏洞时减小影响范围。

ADDF 原生支持 AWS 多账户架构。您可以根据组织的安全和职责分离要求，将您的 ADDF 模块分发到多个 AWS 账户 中。您可以将 ADDF 部署到单个 AWS 账户，并结合工具链和目标账户功能。或者，您可以为 ADDF 模块或模块组创建单独的目标账户。

您需要考虑的唯一限制是，ADDF 模块代表每个 AWS 账户 的最小部署单元。

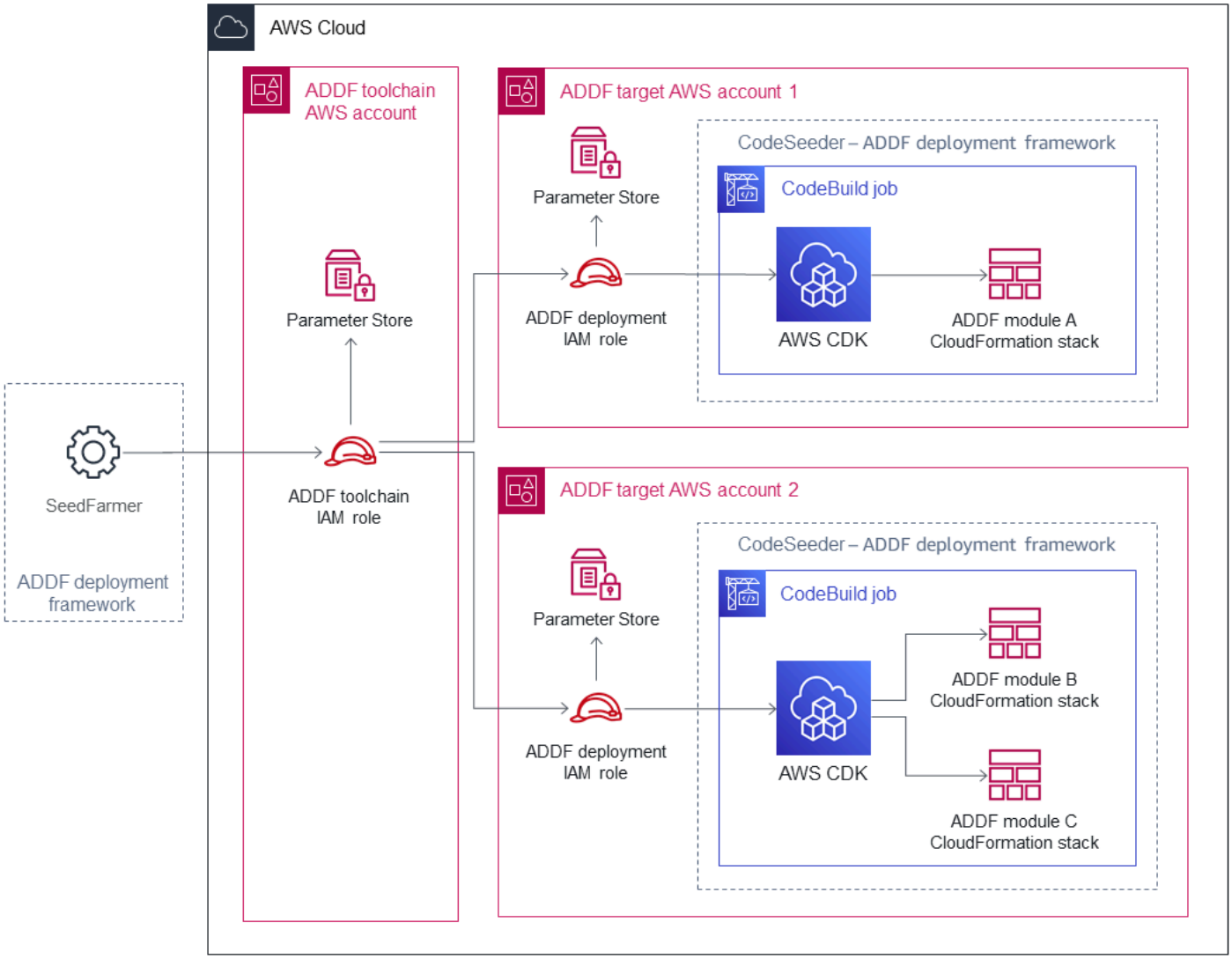
对于生产环境，建议您使用由一个工具链账户和至少一个目标账户组成的多账户架构。有关更多信息，请参阅 ADDF 架构。

多账户部署的最低权限许可

如果您使用多账户架构，SeedFarmer 需要访问目标账户才能执行以下三个操作：

1. 将 ADDF 模块元数据写入工具链账户和目标账户。
2. 从工具链账户和目标账户读取当前的 ADDF 模块元数据。
3. 在目标账户中启动 AWS CodeBuild 作业，以便部署或更新模块。

下图显示了跨账户关系，包括承担特定于 ADDF 的 AWS Identity and Access Management（IAM）角色的操作。



这些跨账户操作是使用明确定义的 assume-role 操作实现的。

- ADDF 工具链 IAM 角色部署在工具链账户中。SeedFarmer 承担了这一角色。该角色具有执行 `iam:AssumeRole` 操作的权限，并且可以在每个目标账户中承担 ADDF 部署 IAM 角色。此外，ADDF 工具链 IAM 角色还可以执行本地 AWS Systems Manager Parameter Store 操作。

- ADDF 部署 IAM 角色部署在每个目标账户中。只能使用 ADDF 工具链 IAM 角色从工具链账户承担此角色。该角色拥有运行本地 AWS Systems Manager Parameter Store 操作的权限，以及通过 CodeSeeder 运行启动和描述 CodeBuild 作业的 AWS CodeBuild 操作的权限。

这些特定于 ADDF 的 IAM 角色是作为 ADDF 引导过程的一部分创建的。有关更多信息，请参阅 ADDF 部署指南（GitHub）中的引导 AWS 账户。

所有跨账户权限都是根据最低权限原则设置的。如果一个目标账户遭到入侵，对另一个 ADDF AWS 账户 的影响很小或没有影响。

对于 ADDF 的单账户架构，角色关系保持不变。只是折叠成一个 AWS 账户。

ADDF 安全设置和操作

自动驾驶数据框架（ADDF）应被视为一款自定义的软件，需要组织中专门的 DevOps 和安全团队持续维护和管理。本节介绍了与安全相关的常见任务，这些任务可帮助您在 ADDF 的整个生命周期中设置和操作 ADDF。

本节包含以下任务：

- 定义您的 ADDF 架构
- 初始设置
- 自定义 ADDF 部署框架代码
- 在 ADDF 中编写自定义模块
- 重复部署 ADDF
- 重复进行安全审计
- ADDF 更新
- 停用

定义您的 ADDF 架构

ADDF 实例的安全性取决于其部署的 AWS 账户 环境。这个 AWS 账户 环境的设计必须满足特定用例的安全和操作需求。例如，在概念验证（PoC）环境中设置 ADDF 实例的安全和操作相关任务和注意事项与在生产环境中设置 ADDF 的任务和注意事项不同。

在 PoC 环境中运行 ADDF

如果您要在 PoC 环境中使用 ADDF，我们建议您为 ADDF 创建一个不包含任何其他工作负载的专用 AWS 账户 环境。这有助于在您探索 ADDF 及其功能时确保您的账户安全。这种方法的优点如下：

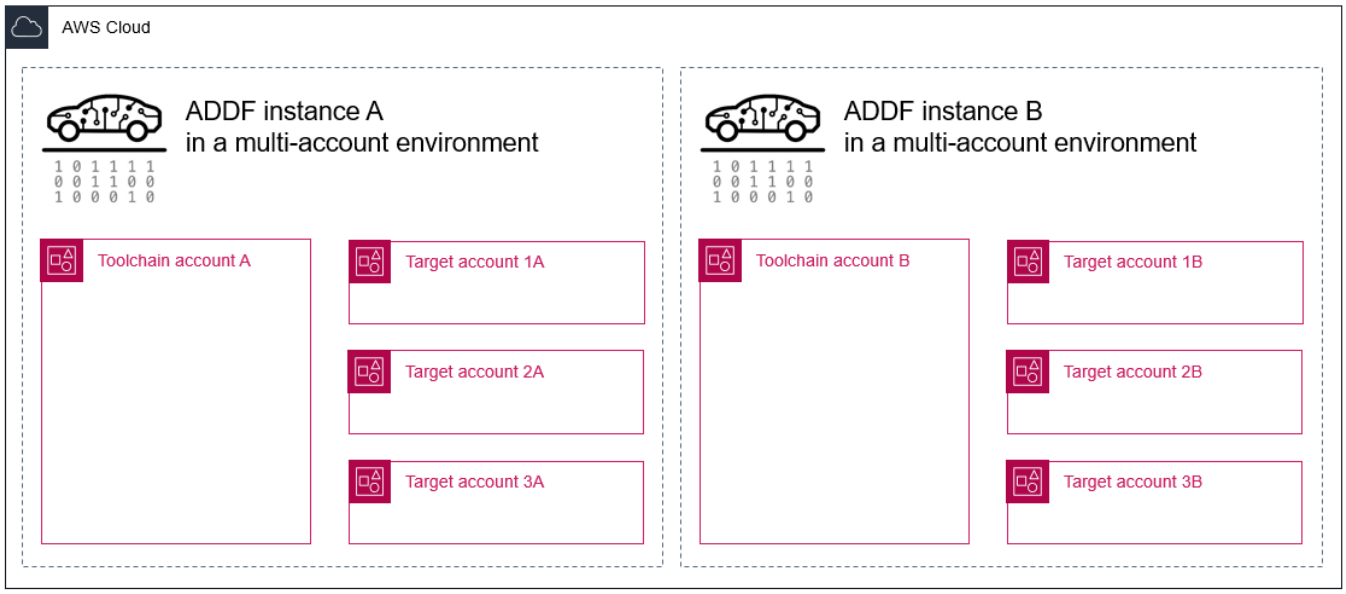
- 如果出现严重的 ADDF 配置错误，不会对其他工作负载产生不利影响。
- 不存在任何其他可能对 ADDF 设置产生不利影响的工作负载配置错误的风险。

即使对于 PoC 环境，我们仍然建议您尽可能遵循 在生产环境中运行 ADDF 中列出的最佳实践。

在生产环境中运行 ADDF

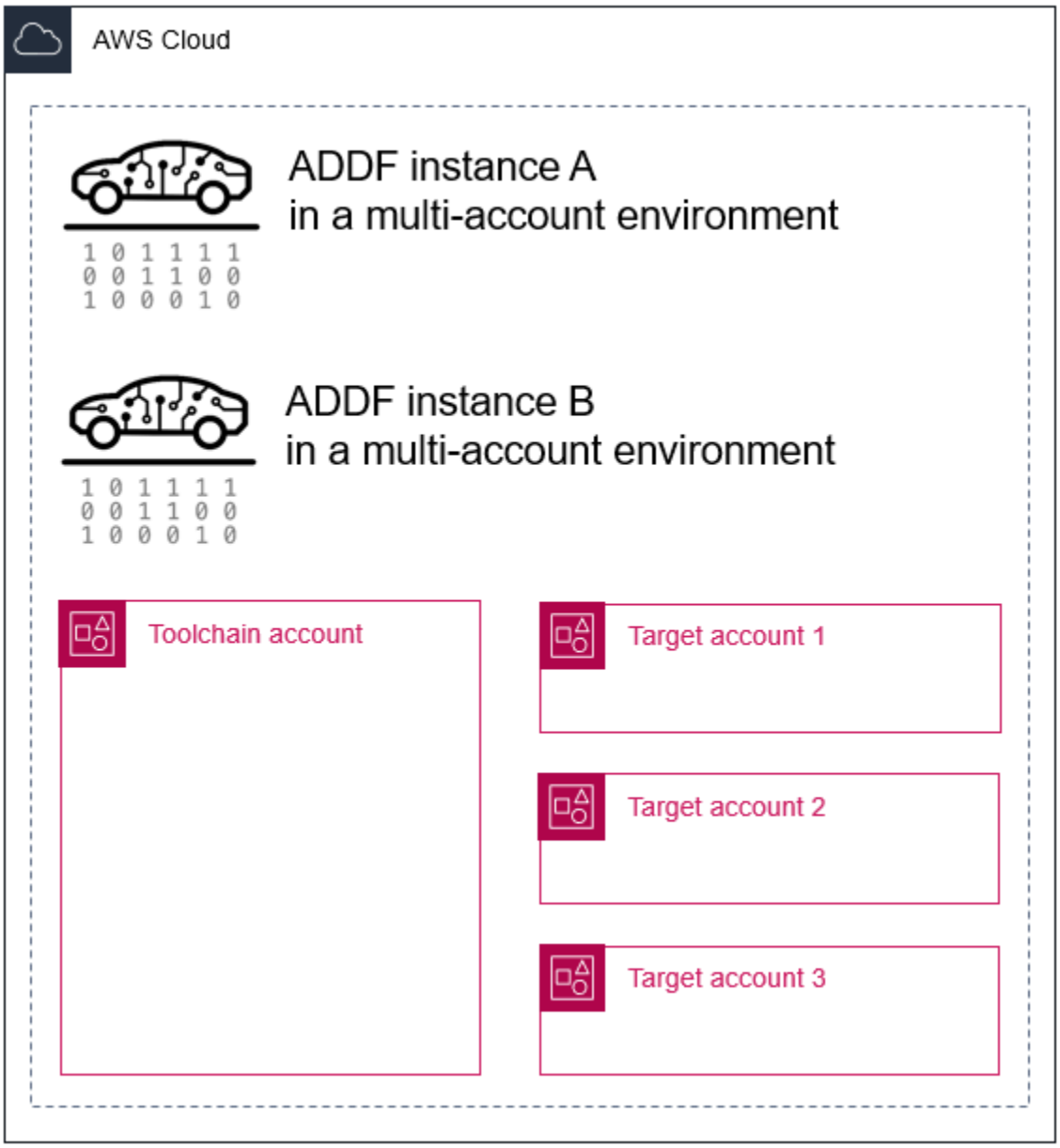
如果您要在企业生产环境中使用 ADDF，我们强烈建议您考虑组织的安全最佳实践，并相应地实施 ADDF。除了组织的安全最佳实践外，我们还建议您实施以下措施：

- 组建一支长期、专注的 ADDF DevOps 团队 - ADDF 应被视为一款自定义的软件。它需要一个专门的 DevOps 团队持续维护和管理。在开始在生产环境中运行 ADDF 之前，应确定一个具有足够规模和能力的 DevOps 团队，并投入全部资源，直到 ADDF 部署的生命周期结束。
- 使用多账户架构 - 每个 ADDF 实例都应部署在自己专用的 AWS 多账户环境中，没有任何其他不相关的工作负载。正如 AWS 账户管理和分离（AWS Well-Architected Framework）中所定义的那样，最佳做法是根据组织的要求将资源和工作负载分成多个 AWS 账户。这是因为 AWS 账户 充当隔离边界。与单账户架构相比，设计合理的 AWS 多账户架构可提供工作负载分类，在发生安全漏洞时减小影响范围。使用多账户架构还有助于您的账户保持在 AWS 服务 限额内。根据组织的安全和职责分离要求，将您的 ADDF 模块分发到多个 AWS 账户 中。
- 部署多个 ADDF 实例 - 根据需要设置任意数量的单独 ADDF 实例，以便根据组织的软件开发流程正确开发、测试和部署 ADDF 模块。在设置多个 ADDF 实例时，可使用以下方法之一：
  - 不同 AWS 多账户环境中的多个 ADDF 实例 - 您可以使用单独的 AWS 账户 来隔离不同的 ADDF 实例。例如，如果您的组织有专门的开发、测试和生产阶段，则可以为每个阶段创建单独的 ADDF 实例和专用账户。这样做有很多好处，比如降低错误跨阶段传播的风险，帮助您实施审批流程，以及限制用户只能访问某些环境。下图显示了在单独的多账户环境中部署的两个 ADDF 实例。



  - 同一 AWS 多账户环境中的多个 ADDF 实例 – 您可以创建共享同一 AWS 多账户环境的多个 ADDF 实例。这实际上是在同一 AWS 账户 中创建独立的分支。例如，如果不同的开发人员并行工作，则开发人员可以在同一 AWS 账户 中创建专用的 ADDF 实例。这有助于开发人员在独立的分支中

进行开发和测试。如果使用这种方法，对于每个 ADDF 实例，ADDF 资源必须具有唯一的资源名称。默认情况下，ADDF 预提供的模块支持此功能。只要不超过 AWS 服务 限额，就可以使用这种方法。下图显示了在共享的多账户环境中部署的两个 ADDF 实例。



- 同一 AWS 单账户环境中的多个 ADDF 实例 – 此架构与前面的示例非常相似。不同之处在于，多个 ADDF 实例部署在单账户环境中，而不是多账户环境中。此架构适合非常简单的 ADDF 用例，这些用例的范围非常有限，而且多个开发人员同时在不同的分支上工作。

由于 SeedFarmer 是控制 ADDF 实例部署的单一工具，因此您可以构建适合贵组织部署策略和 CI/CD 流程的任何环境和账户架构。

- 根据组织的安全要求自定义 AWS Cloud Development Kit (AWS CDK) 引导过程 – 默认情况下，AWS CDK 在引导过程中分配 AdministratorAccess AWS 托管策略。此策略授予完全管理权限。如果此策略对于贵组织的安全要求而言过于宽松，您可以自定义应用哪些策略。有关更多信息，请参阅 AWS CDK 部署角色的自定义最低权限策略。
- 在 IAM 中设置访问权限时遵循最佳实践 – 建立结构化 AWS Identity and Access Management（IAM）访问解决方案，允许您的用户访问 ADDF AWS 账户。ADDF 框架的设计遵循最低权限原则。您的 IAM 访问模式还应遵循最低权限原则，应符合贵组织的要求，并遵守 IAM 安全最佳实践（IAM 文档）。
- 根据组织的最佳实践设置网络 - ADDF 包含一个可选的网络 AWS CloudFormation 堆栈，用于创建基本的公有或私有虚拟私有云（VPC）。根据组织的配置，此 VPC 可能会将资源直接公开到互联网。我们建议您遵循组织的最佳网络实践，创建一个自定义的安全加固网络模块。
- 在 AWS 账户 级别上部署安全预防、检测和缓解措施 - AWS 提供各种安全服务，如 Amazon GuardDuty、AWS Security Hub、Amazon Detective 和 AWS Config。在 ADDF AWS 账户 中启用

这些服务，并集成组织的安全预防、检测、缓解和事件处理流程。我们建议您遵循安全、身份和合规性最佳实践（AWS 架构中心）以及该服务文档中包含的任何特定于服务的建议。有关更多信息，请参阅 AWS 安全性文档。

ADDF 未涉及这些主题，因为实施和配置细节在很大程度上取决于贵组织的具体要求和流程。这些主题主要由贵组织负责阐述。通常，管理 AWS 登录区的团队会帮助您规划和实施 ADDF 环境。

初始设置

根据 ADDF 部署指南（GitHub）设置 ADDF。任何部署的起点都是自动驾驶数据框架 Git Hub 存储库中的 `/manifest` 文件夹。`/manifest/example-dev` 文件夹包含一个用于演示的示例部署。以本示例为起点，设计您自己的部署。在该目录中，有一个名为 deployment.yaml 的 ADDF 部署清单文件。它包含 SeedFarmer 在 AWS Cloud 中管理、部署或删除 ADDF 及其资源的所有信息。您可以在专用文件中创建 ADDF 模块组。core-modules.yaml 是核心模块组的一个示例，它包含 ADDF 提供的所有核心模块。总之，deployment.yaml 文件包含对将部署到其目标账户的组和模块的所有引用，并指定部署顺序。

为了实现安全和合规的配置，尤其是在非概念验证环境中，我们建议您查看要部署的每个模块的源代码。根据安全加固最佳实践，您应该只部署预期用例所需的模块。

> **Note**
>
> `modules/demo-only/` 文件夹中的 ADDF 模块未经过安全加固，不应部署在生产环境或任何包含敏感或受保护数据的环境中。包含这些模块是为了展示系统功能，您可以将它们作为创建自己的自定义安全加固模块的基础。

自定义 ADDF 部署框架代码

ADDF 部署框架及其编排和部署逻辑可以完全自定义，以满足任何要求。但是，出于以下原因，我们建议您不要自定义或尽量减少更改：

- 保持上游兼容性 - 上游兼容性使更新 ADDF 以获取最新功能和安全更新变得更容易。更改框架会破坏与 SeedFarmer、CodeSeeder 和任何 ADDF 核心模块的原生向后兼容性。
- 安全后果 - 更改 ADDF 部署框架可能是一项复杂的任务，会带来意想不到的安全后果。在最坏的情况下，框架更改可能会产生安全漏洞。

在可能的情况下，构建和自定义自己的模块代码，而不是修改 ADDF 部署框架和 ADDF 核心模块代码。

> **Note**
>
> 如果您认为 ADDF 部署框架的特定部分需要改进或进一步加强安全性，请通过拉取请求将您的更改提交到 ADDF 存储库。有关更多信息，请参阅 开源安全审查和贡献。

在 ADDF 中编写自定义模块

创建新的 ADDF 模块或扩展现有模块是 ADDF 的核心概念。在创建或自定义模块时，我们建议您遵循一般 AWS 安全最佳实践和组织的安全编码最佳实践。此外，我们建议您根据组织的安全要求进行初步和定期的内部或外部技术安全审查，以进一步降低出现安全问题的风险。

重复部署 ADDF

按照 ADDF 部署指南（GitHub）中的说明部署 ADDF 及其模块。为了支持在目标账户中添加、更新或移除资源的重复 ADDF 部署，SeedFarmer 使用存储在工具链和目标账户 Parameter Store 中的 MD5 哈希值，将当前部署的基础设施与本地代码库清单文件中定义的基础设施进行比较。

这种方法遵循了 GitOps 范式，其中您的源存储库（操作 SeedFarmer 的本地代码库）是可信来源，而明确声明的基础设施是您的部署的预期结果。有关 GitOps 的更多信息，请参阅什么是 GitOps（GitLab 网站）。

重复进行安全审计

像组织中的任何其他软件一样，将 ADDF 和自定义 ADDF 模块代码集成到安全风险管理、安全审查和安全审计周期中。

ADDF 更新

作为其持续开发工作的一部分，ADDF会定期收到更新。这包括功能更新以及与安全相关的改进和修复。我们建议您定期检查新的框架版本，并及时应用更新。有关更多信息，请参阅更新 ADDF 的步骤（ADDF 文档）。

停用

如果不再需要 ADDF，从您的 AWS 账户 中删除 ADDF 及其所有相关资源。任何无人值守和未使用的基础设施都会产生不必要的成本，带来潜在的安全风险。有关更多信息，请参阅销毁 ADDF 的步骤（ADDF 文档）。

后续步骤

本指南回顾了在您的 AWS Cloud 环境中部署自动驾驶数据框架（ADDF）时的安全和操作最佳实践和注意事项。本指南介绍了 ADDF 用户、ADDF 核心团队和 AWS 之间的责任共担模式，让您了解您在安全设置和操作 ADDF 方面的角色和责任。它还包括在 ADDF 生命周期中安全操作 ADDF 的建议，包括针对特定环境的建议。

我们建议您熟悉 资源 一节中的资源。准备就绪后，您可以根据 ADDF 部署指南（GitHub）中的说明设置 ADDF。

在设置和操作 ADDF 时，如果您认为部署框架需要改进或进一步加强安全性，请通过拉取请求将您的更改提交到 ADDF 存储库。有关更多信息，请参阅 开源安全审查和贡献。

资源

AWS 文档

- 在 AWS 上使用 ADDF 开发和部署自定义工作流程（AWS 博客文章）
- AWS 安全服务文档
- IAM 安全最佳实践
- AWS 账户管理和分离
- AWS CDK 引导程序
- AWS 责任共担模式
- AWS Well-Architected Framework

开源资源

- ADDF 存储库（GitHub）
- ADDF 部署指南（GitHub）
- CodeSeeder 存储库（GitHub）
- SeedFarmer 存储库（GitHub）

注意事项

客户有责任对本文档中的信息进行单独评测。本文档：（a）仅供参考，（b）代表当前的 AWS 产品和实践，如有更改，恕不另行通知，以及（c）不构成 AWS 及其附属公司、供应商或许可方的任何承诺或保证。AWS 产品或服务“按原样”提供，不附带任何明示或暗示的保证、陈述或条件。

AWS 对其客户承担的责任和义务受 AWS 协议制约，本文档不是 AWS 与客户直接协议的一部分，也不构成对该协议的修改。

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
初次发布	—	2022 年 11 月 15 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：将您的本地 Oracle 数据库迁移到兼容 Amazon Aurora PostgreSQL 的版本。
- 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：在中将您的本地 Oracle 数据库迁移到适用于 Oracle 的亚马逊关系数据库服务 (Amazon RDS) AWS Cloud。
- 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：将您的客户关系管理 (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：在中的 EC2 实例上将您的本地 Oracle 数据库迁移到 Oracle AWS Cloud。
- 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。您可以将服务器从本地平台迁移到同一平台的云服务。示例：将Microsoft Hyper-V应用程序迁移到 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。当你有信心时，你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 Cloud 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

组织迁移到以下阶段时通常会经历四个阶段 AWS Cloud：

- 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 AWS Cloud 企业战略博客的博客文章《云优先之旅和采用阶段》中定义了这些阶段。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中的信息。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，用于验证迁移到的业务案例。 AWS Cloud 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的方法 AWS Cloud。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。有关更多信息，请参阅中的评估应用程序的现代化准备情况 AWS Cloud。

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）

在中 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。这些控件会在资源置备之前对其进行扫描。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 Secret s Manager 密钥中有什么？ 在 Secrets Manager 文档中。

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

在目的地对数据进行加密，由接收数据 AWS 服务 的人加密。

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

标签

键值对，充当用于组织资源的元数据。 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。