为以下各项实施最低特权权限策略 AWS CloudFormation

AWS 规范性指导

AWS 规范性指导: 为以下各项实施最低特权权限策略 AWS CloudFormation

Table of Contents

简介 1
什么是最低权限？ 1
目标业务成果 2
目标受众 2
使用访问策略 3
CloudFormation 使用权限 4
基于身份的策略 5
最佳实践 5
示例策略 6
服务角色 9
实现 CloudFormation 服务角色的最低权限 10
配置服务角色 10
向 IAM 委托人授予使用 CloudFormation 服务角色的权限 11
为 CloudFormation 服务角色配置信任策略 13
将服务角色与堆栈关联 13
堆栈策略 13
配置堆栈策略 14
设置和覆盖堆栈策略 14
限制和要求堆栈策略 14
预调配的资源权限 18
示例：Amazon S3 存储桶 18
最佳实践 21
后续步骤 22
资源 23
CloudFormation 文档 23
IAM 文档 23
其他 AWS 参考 23
文档历史记录 24
术语表 25
..... 25
A 25
B 28
C 30
D 32

E 36
F 37
G 39
H 40
我 41
L 43
M 44
O 48
P 50
Q 52
R 52
S 55
T 58
U 59
V 60
W 60
Z 61
..... lxii

为以下各项实施最低权限策略 AWS CloudFormation

Nima Fotouhi 和 Moumita Saha，Amazon Web Services（AWS）

2023 年 5 月（文档历史记录）

AWS CloudFormation是一项基础设施即代码 (IaC) 服务，可通过配置 AWS 资源来帮助您扩展云基础架构的开发。它还可以帮助您在 AWS 账户 和的整个生命周期中管理这些资源 AWS 区域。在中 CloudFormation，您可以定义模板，这些模板充当一组资源的蓝图。然后，您可以通过创建和部署堆栈来预调配这些资源，堆栈是一组作为单个单元管理的相关资源。您还可以使用 CloudFormation 部署堆栈集，堆栈集是一组堆栈，您可以通过单个操作跨多个账户创建、更新和 AWS 区域 删除这些堆栈。本指南概述了如何为通过配置的资源实现最低权限 AWS CloudFormation 和资源。CloudFormation

您可以通过执行以下任一操作来部署 CloudFormation 堆栈或堆栈集：

- 通过 AWS Identity and Access Management (IAM) 委托人直接访问 AWS 环境并部署 CloudFormation 堆栈。
- 将 CloudFormation 堆栈推送到部署管道中，然后通过管道启动堆栈部署。管道通过 IAM 委托人访问 AWS 环境并部署堆栈。此方法是推荐的最佳实践。

对于这两种方法，部署 CloudFormation 堆栈都需要权限。例如，假设一个用户计划使用 CloudFormation 创建亚马逊弹性计算云 (Amazon EC2) 实例。该实例需要一个 IAM 实例配置文件才能访问其他实例 AWS 服务。用于部署 CloudFormation 堆栈的 IAM 委托人需要以下权限：

- 访问权限 CloudFormation
- 在中创建堆栈的权限 CloudFormation
- 在 Amazon EC2 中创建实例的权限
- 创建所需的 IAM 实例配置文件的权限

什么是最低权限？

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。最低权限原则是 Well-Architecte AWS d Framework 中安全支柱的一部分。当您实施此最佳实践时，它可以帮助保护您的 AWS 环境免受权限升级风险，减少攻击面，提高数据安全性，并防止用户错误（例如错误配置或错误删除资源）。

要对您的 AWS 资源实施最低权限，您可以在 AWS Identity and Access Management (IAM) 中配置策略，例如基于身份的策略。这些策略定义权限和指定访问条件。Organi AWS zations 可能从托管策略开始，但随后他们通常会创建自定义策略，将权限范围限制为工作负载或用例所需的操作。

该 CloudFormation 服务的最低权限是一个重要的安全考虑因素。由于与之交互的用户和开发人员 CloudFormation 可以大规模快速创建、修改或删除资源，因此最小权限尤为重要。但是，CloudFormation 需要在中创建、更新和修改资源所需的权限 AWS 账户。您必须在操作权限需求 CloudFormation 与最低权限原则之间取得平衡。

在应用最小权限原则时 CloudFormation，需要考虑以下几点：

- CloudFormation 服务权限 — 哪些用户需要访问权限 CloudFormation，他们需要什么级别的访问权限，以及他们可以采取哪些操作来创建、更新或删除堆栈？
- 资源配置权限-用户可以通过哪些资源进行预配 CloudFormation？
- 已配置资源的权限-如何为通过配置的资源配置最低权限权限？ CloudFormation

目标业务成果

通过遵循本指南中的最佳实践和建议，您可以：

- 确定组织中哪些用户需要访问权限 CloudFormation，然后为这些用户配置最低权限权限。
- 使用堆栈策略来帮助保护 CloudFormation 堆栈免受意外更新的影响。
- 为 CloudFormation 用户和资源配置最低权限以帮助防止权限升级和混乱的代理问题。
- AWS CloudFormation 用于配置具有最低权限的 AWS 资源。这有助于您的组织保持更稳健的安全状况。
- 主动减少调查和缓解安全事件所需的时间、精力和金钱。

目标受众

本指南适用于通过使用管理和配置资源的云基础设施架构 DevOps 师、工程师和站点可靠性工程师 (SREs) CloudFormation。

使用访问策略授予权限 AWS

您可以 AWS 通过创建基于身份的策略并将其关联到 AWS Identity and Access Management (IAM) 委托人（例如角色或用户），以及创建基于资源的策略并将其附加到资源来管理中的访问权限。 AWS AWS 每当提出请求时，都会评估这些策略。策略中的权限确定是允许还是拒绝请求。

要了解如何在策略中配置最低权限访问权限，您需要了解不同类型的策略、策略的元素和结构及如何评估策略。本指南仅关注基于身份的策略和基于资源的策略。但是， AWS 提供了其他类型的策略，例如服务控制策略 (SCPs)、权限边界和会话策略。每种类型的策略在您的中实现最低权限的过程中都起着作用。 AWS 账户有关更多信息，请参阅 IAM 文档中的策略和权限和应用最低权限许可。

配置要使用的最低权限权限 CloudFormation

本章介绍配置访问和使用 AWS CloudFormation 服务的权限的选项。

当用户或服务通过配置 AWS 资源时 CloudFormation，第一步是通过 AWS Identity and Access Management (IAM) 委托人调用该 CloudFormation 服务。此 IAM 委托人必须拥有创建 CloudFormation 堆栈的权限。接下来，IAM 委托人使用以下方法之一通过以下方式配置资源 CloudFormation：

- 如果 IAM 委托人未将堆栈操作传递给 CloudFormation 服务角色，则 CloudFormation 使用 IAM 委托人的证书执行堆栈操作。这是默认值。因此，除了执行 CloudFormation 堆栈操作的权限外，IAM 委托人还需要配置他们将要使用的 CloudFormation 模板中定义的资源的权限。例如，如果 IAM 委托人无权创建亚马逊弹性计算云 (Amazon EC2) 实例，那么他们就无法创建 CloudFormation 预配置 Amazon EC2 实例的堆栈。
- 如果 IAM 委托人将堆栈操作传递给 CloudFormation 服务角色，则 CloudFormation 使用该服务角色执行堆栈操作并在 CloudFormation 模板中配置资源。此 CloudFormation 服务角色的定义应具有代表 IAM 委托人置备的权限。 AWS 服务 这种方法可避免向 IAM 委托人直接授予预置 CloudFormation 模板中定义的 AWS 资源的权限。IAM 委托人需要 CloudFormation 堆栈创建权限，并 CloudFormation 使用服务角色的策略而不是 IAM 委托人的策略进行调用。

通过使用服务角色方法和最小权限原则，您可以标准化 AWS 环境中的资源配置，并要求用户通过 CloudFormation IaC 配置资源。由于附加到 IAM 委托人的策略不包含直接配置 AWS 资源的权限，因此用户必须使用 CloudFormation 来配置资源。

本章概述了用于配置和管理对 CloudFormation 服务和 CloudFormation 堆栈的访问的以下机制：

- 基于身份的策略 CloudFormation— 使用此类策略来配置哪些 IAM 委托人可以访问 CloudFormation 以及他们可以执行哪些操作。 CloudFormation
- 的服务角色 CloudFormation— 创建一个服务角色， CloudFormation 允许代表部署堆栈的 IAM 委托人创建、更新或删除堆栈资源。服务角色在 IAM 中创建，且可以与一个或多个堆栈关联。
- CloudFormation 堆栈策略：使用此类策略来确定何时可以更新堆栈。此类策略有助于防止堆栈资源被意外更新或删除。堆栈策略已创建并与中的 CloudFormation堆栈相关联。

基于身份的策略 CloudFormation

考虑需要访问的用户类型 AWS CloudFormation，并考虑这些用户需要执行哪些操作 CloudFormation。您可以通过基于身份的策略配置用户权限，这些策略将关联到 AWS Identity and Access Management (IAM) 委托人，例如角色或用户。

配置基于身份的策略时，`Effect`、`Action` 和 `Resource` 元素是必需的。您也可以选择定义 `Condition` 元素。有关这些元素的更多信息，请参阅 IAM JSON 策略元素参考。

本节包含以下主题：

- 为最低权限访问配置基于身份的策略的最佳实践 CloudFormation
- 基于身份的策略示例 CloudFormation

为最低权限访问配置基于身份的策略的最佳实践 CloudFormation

- 对于需要访问权限的 IAM 委托人 CloudFormation，您必须在操作权限需求 CloudFormation 与最低权限原则之间取得平衡。为了帮助您遵循最低权限原则，我们建议您为 IAM 主体定义基于身份的特定操作，以便该主体能够执行以下操作：
  - 创建、更新和删除堆 CloudFormation 栈。
  - 传递一个或多个具有部署 CloudFormation 模板中定义的资源所需权限的服务角色。这 CloudFormation 允许代入服务角色并代表 IAM 委托人配置堆栈中的资源。
- 权限升级是指具有访问权限的用户能够提升其权限级别并危及安全性。最低权限是一种重要的最佳实践，可帮助防止权限升级。由于 CloudFormation 支持配置 IAM 资源类型（例如策略和角色），因此 IAM 委托人可以通过以下方式 CloudFormation 提升其权限：
  - 使用 CloudFormation 堆栈为 IAM 委托人配置高特权权限、策略或证书 — 为了防止这种情况，我们建议使用权限护栏来限制 IAM 委托人的访问级别。权限护栏设置基于身份的策略可以授予 IAM 主体的最大权限。这有助于防止故意和无意的权限升级。您可以使用以下策略类型作为权限护栏：
    - 权限边界定义基于身份的策略可以授予 IAM 主体的最大权限。有关更多信息，请参阅 IAM 实体的权限边界。
    - 在中 AWS Organizations，您可以使用服务控制策略 (SCPs) 来定义组织级别的最大可用权限。SCPs 仅影响 IAM 角色和由组织中的账户管理的用户。您可以附加 SCPs 到帐户、组织单位或组织根目录。有关更多信息，请参阅 SCP 对权限的影响。
  - 创建提供广泛权限的 CloudFormation 服务角色 — 为防止出现这种情况，我们建议您在基于身份的策略中添加以下精细权限，以供将使用的 IAM 委托人使用： CloudFormation

- 使用`cloudformation:RoleARN`条件键控制 IAM 委托人可以使用哪些 CloudFormation 服务角色。
- 仅允许对 IAM 委托人需要传递的特定 CloudFormation服务角色执行`iam:PassRole`操作。

有关更多信息，请参阅本指南中的向 IAM 委托人授予使用 CloudFormation 服务角色的权限。

- 使用权限护栏（例如权限边界和）限制权限 SCPs，并使用基于身份或基于资源的策略来授予权限。

基于身份的策略示例 CloudFormation

本节包含基于身份的策略示例，这些策略演示了如何授予和拒绝权限。 CloudFormation您可以使用这些示例策略开始设计自己的策略，这些策略遵循最低权限原则。

有关 CloudFormation 特定操作和条件的列表，请参阅和条件的操作、资源 AWS CloudFormation 和AWS CloudFormation 条件键。有关可与条件结合使用的资源类型列表，请参阅 AWS 资源和属性类型参考。

本节包含以下示例策略：

- 允许查看访问权限
- 允许基于模板创建堆栈
- 拒绝更新或删除堆栈

允许查看访问权限

查看访问权限是权限最低的访问类型。 CloudFormation这种策略可能适合那些想要查看所有CloudFormation堆栈的 IAM 委托人。 AWS 账户以下示例策略授予查看账户中任何 CloudFormation 堆栈详细信息的权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources"
      ],
```

```
      "Resource": "*"
    }
  ]
}
```

允许基于模板创建堆栈

以下示例策略允许 IAM 委托人仅使用存储在特定亚马逊简单存储服务 (Amazon S3) 存储桶中的 CloudFormation 模板来创建堆栈。此存储桶名称为 `my-CFN-templates`。您可以将批准的模板上传到此存储桶。策略中的 `cloudformation:TemplateUrl` 条件键可防止 IAM 主体使用任何其他模板来创建堆栈。

> **Important**
>
> 允许 IAM 主体对此 S3 存储桶具有只读访问权限。这有助于防止 IAM 主体添加、删除或修改已批准的模板。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:CreateStack"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "cloudformation:TemplateUrl": "https:// my-CFN-templates.s3.amazonaws.com/*"
        }
      }
    }
  ]
}
```

拒绝更新或删除堆栈

为了帮助保护配置关键业务 AWS 资源的特定 CloudFormation 堆栈，您可以限制该特定堆栈的更新和删除操作。您只能允许少数指定的 IAM 主体执行这些操作，而拒绝环境中的任何其他 IAM 主体执行这

些操作。以下策略声明拒绝更新或删除特定 AWS 区域 和中的特定 CloudFormation 堆栈的权限 AWS 账户。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "cloudformation:DeleteStack",
        "cloudformation:UpdateStack"
      ],
      "Resource": "arn:aws:cloudformation:us-east-1:123456789012:stack/
MyProductionStack/<stack_ID>"
    }
  ]
}
```

此策略声明拒绝更新或删除MyProductionStack CloudFormation 堆栈的权限，该堆栈位于us-east-1 AWS 区域 和中123456789012 AWS 账户。您可以在 CloudFormation 控制台中查看堆栈 ID。以下是如何根据使用案例修改此语句的 Resource 元素的一些示例：

- 您可以在此策略的Resource元素 IDs 中添加多个 CloudFormation 堆栈。
- 您可以使用arn:aws:cloudformation:us-east-1:123456789012:stack/*防止 IAM 委托人更新或删除123456789012账户中us-east-1 AWS 区域 和中的任何堆栈。

重要的一步是决定哪个策略应包含此声明。您可以将此声明添加到以下策略：

- 附加到 IAM 委托人的基于身份的策略 — 将声明置于此策略中会限制特定的 IAM 委托人创建或删除特定堆栈。 CloudFormation
- 附加到 IAM 主体的权限边界：将声明放在此策略中会创建权限护栏。它限制多个 IAM 委托人创建或删除特定 CloudFormation 堆栈，但不限制环境中的所有委托人。
- 附加到账户、组织单位或组织的 SCP：将声明放入此策略中会创建权限护栏。它限制目标账户、组织单位或组织中的所有 IAM 委托人创建或删除特定 CloudFormation堆栈。

  但是，如果您不允许至少一个 IAM 委托人（特权委托人）更新或删除 CloudFormation 堆栈，则在必要时将无法对通过此堆栈配置的资源进行任何更改。用户或开发管线（推荐）可以代入此特权主体。如果您想将限制部署为 SCP，那么我们建议改用以下策略声明。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "cloudformation:DeleteStack",
        "cloudformation:UpdateStack"
      ],
      "Resource": "arn:aws:cloudformation:us-east-1:123456789012:stack/
MyProductionStack/<stack_ID>",
      "Condition": {
        "ArnNotLike": {
          "aws:PrincipalARN": [
            "<ARN of the allowed privilege IAM principal>"
          ]
        }
      }
    }
  ]
}
```

在此语句中，Condition 元素定义了从 SCP 中排除的 IAM 主体。此语句拒绝任何 IAM 委托人更新或删除 CloudFormation 堆栈的权限，除非 IAM 委托人的 ARN 与元素中的 ARN 相匹配。Conditionaws:PrincipalARN 条件键接受一个列表，这意味着您可以根据环境需要，从限制中排除多个 IAM 主体。有关防止修改 CloudFormation 资源的类似 SCP，请参阅 SCP-CLOUDFORMATION-1 (GitHub)。

的服务角色 CloudFormation

服务角色是允许 AWS CloudFormation 创建、更新或删除堆栈资源的 AWS Identity and Access Management (IAM) 角色。如果您不提供服务角色，则 CloudFormation使用 IAM 委托人的证书执行堆栈操作。如果您为创建服务角色 CloudFormation 并在创建堆栈期间指定服务角色，则 CloudFormation 使用该服务角色的证书来执行操作，而不是 IAM 委托人的证书。

使用服务角色时，附加到 IAM 委托人的基于身份的策略不需要配置模板中定义的所有 AWS 资源的权限。 CloudFormation如果您还没有准备好通过开发管道为关键业务运营配置 AWS 资源（ AWS 推荐的最佳实践），那么使用服务角色可以为中的资源管理增加一层额外的保护 AWS。此方法的优点：

- 您组织中的 IAM 委托人遵循最低权限模式，防止他们在您的环境中手动创建或更改 AWS 资源。
- 要创建、更新或删除 AWS 资源，IAM 委托人必须使用 CloudFormation。这通过基础设施即代码实现了资源预调配的标准化。

例如，要创建包含 Amazon Elastic Compute Cloud（Amazon EC2）实例的堆栈，IAM 主体需要有权通过基于身份的策略创建 EC2 实例。相反， CloudFormation 可以代入一个有权代表委托人创建 EC2 实例的服务角色。通过此方法，IAM 主体可以创建堆栈，且您无需为 IAM 主体授予他们不应该定期访问的服务的过于宽泛的权限。

要使用服务角色创建 CloudFormation 堆栈，IAM 委托人必须拥有将服务角色传递给的权限 CloudFormation，并且该服务角色的信任策略必须 CloudFormation 允许代入该角色。

本节包含以下主题：

- 实现 CloudFormation 服务角色的最低权限
- 配置服务角色
- 向 IAM 委托人授予使用 CloudFormation 服务角色的权限
- 为 CloudFormation 服务角色配置信任策略
- 将服务角色与堆栈关联

实现 CloudFormation 服务角色的最低权限

在服务角色中，您可以定义一个权限策略，该策略明确指定服务可以执行哪些操作。这些操作可能与 IAM 主体可以执行的操作不同。我们建议您从 CloudFormation 模板向后移动，创建符合最低权限原则的服务角色。

正确界定 IAM 主体的基于身份的策略范围以仅传递特定的服务角色，并将服务角色的信任策略范围限定为仅允许特定的主体代入该角色，这有助于防止可能通过服务角色进行权限升级。

配置服务角色

> **Note**
>
> 服务角色是在 IAM 中配置的。要创建服务角色，您必须拥有相应的权限。有权创建角色和附加任何策略的 IAM 委托人可以提升自己的权限。 AWS 建议 AWS 服务 为每个用例分别创建一个服务角色。为用例创建 CloudFormation 服务角色后，您可以允许用户仅将已批准的服务角色

传递给 CloudFormation。有关允许用户创建服务角色的基于身份的策略示例，请参阅 IAM 文档中的服务角色权限。

有关如何创建服务角色的说明，请参阅创建向委派权限的角色 AWS 服务。指定 CloudFormation (`cloudformation.amazonaws.com`) 作为可代入此角色的服务。这可以防止 IAM 主体自己代入角色或将其传递给其他服务。配置服务角色时，`Effect`、`Action` 和 `Resource` 元素是必需的。您也可以选择定义 `Condition` 元素。

有关这些元素的更多信息，请参阅 IAM JSON 策略元素参考。有关操作、资源和条件键的完整列表，请参阅 Actions, resources, and condition keys for Identity And Access Management。

向 IAM 委托人授予使用 CloudFormation 服务角色的权限

要使用 CloudFormation 服务角色 CloudFormation 通过配置资源，IAM 委托人必须具有传递服务角色的权限。通过在主体的权限中指定角色的 ARN，您可以将 IAM 主体的权限限制为仅传递某些角色。有关更多信息，请参阅 IAM 文档中的向用户授予权限以将角色传递给 AWS 服务。

以下基于 IAM 身份的策略声明允许主体传递 `cfnroles` 路径中的角色，包括服务角色。主体无法传递不同路径中的角色。

```
{
"Sid": "AllowPassingAppRoles",
"Effect": "Allow",
"Action": "iam:PassRole",
"Resource": "arn:aws:iam::<account ID>:role/cfnroles/*"
}
```

将委托人限制为某些角色的另一种方法是使用 CloudFormation 服务角色名称的前缀。以下策略声明允许 IAM 主体仅传递带有 `CFN-` 前缀的角色。

```
{
"Sid": "AllowPassingAppRoles",
"Effect": "Allow",
"Action": "iam:PassRole",
"Resource": "arn:aws:iam::<account ID>:role/CFN-*"
}
```

除了之前的策略声明外，您还可以使用 `cloudformation:RoleARN` 条件键在基于身份的策略中提供进一步的精细控制，以实现最低权限的访问。以下政策声明仅允许 IAM 委托人创建、更新和删除

堆栈，前提是堆栈传递了特定的 CloudFormation 服务角色。作为变体，您可以在条件键中定义多个 CloudFormation服务角色。 ARNs

```
{
  "Sid": "RestrictCloudFormationAccess",
  "Effect": "Allow",
  "Action": [
    "cloudformation:CreateStack",
    "cloudformation:DeleteStack",
    "cloudformation:UpdateStack"
  ],
  "Resource": "arn:aws:iam::<account ID>:role/CFN-*",
  "Condition": {
    "StringEquals": {
      "cloudformation:RoleArn": [
        "<ARN of the specific CloudFormation service role>"
      ]
    }
  }
}
```

此外，您还可以使用`cloudformation:RoleARN`条件键限制 IAM 委托人为堆栈操作传递高权限 CloudFormation 服务角色。唯一需要更改的是条件运算符，从 `StringEquals` 改为 `StringNotEquals`。

```
{
  "Sid": "RestrictCloudFormationAccess",
  "Effect": "Allow",
  "Action": [
    "cloudformation:CreateStack",
    "cloudformation:DeleteStack",
    "cloudformation:UpdateStack"
  ],
  "Resource": "arn:aws:iam::<account ID>:role/CFN-*",
  "Condition": {
    "StringNotEquals": {
      "cloudformation:RoleArn": [
        "<ARN of a privilege CloudFormation service role>"
      ]
    }
  }
}
```

为 CloudFormation 服务角色配置信任策略

角色信任策略是附加到 IAM 角色的必需的基于资源的策略。信任策略定义哪些 IAM 主体可以代入此角色。在信任策略中，您可以指定用户、角色、账户或服务作为主体。为防止 IAM 委托人将的服务角色传递 CloudFormation 给其他服务，您可以在角色的信任策略中指定 CloudFormation 为委托人。

以下信任策略仅允许 CloudFormation 服务担任服务角色。

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Principal": {
      "Service": "cloudformation.amazonaws.com"
    },
    "Action": "sts:AssumeRole"
  }
}
```

将服务角色与堆栈关联

创建服务角色后，您可以在创建堆栈时将其与堆栈关联。有关更多信息，请参阅配置堆栈选项。在指定服务角色之前，确保 IAM 主体具有传递该角色的权限。有关更多信息，请参阅 向 IAM 委托人授予使用 CloudFormation 服务角色的权限。

CloudFormation 堆栈策略

堆栈策略有助于防止堆栈资源在堆栈更新过程中被意外更新或删除。堆栈策略是一个 JSON 文档，该文档定义可对指定资源执行的更新操作。默认情况下，任何具有`cloudformation:UpdateStack`权限的 IAM 委托人都可以更新 AWS CloudFormation 堆栈中的所有资源。更新可能会导致中断，也可能会完全删除和替换资源。您可以使用堆栈策略来帮助配置最低权限许可。堆栈策略可以提供额外的保护层。

默认情况下，堆栈策略有助于保护堆栈中的所有资源。但是，堆栈策略的主要好处是它们为堆 CloudFormation 栈中部署的每个 AWS 资源提供了精细的控制。您可以使用堆栈策略来帮助仅保护堆栈中的特定资源，并允许更新或删除同一堆栈中的其他资源。要允许对特定资源进行更新，您可在堆栈策略中包含针对这些资源的显式 `Allow` 语句。

堆栈策略为它们所连接的 CloudFormation 堆栈提供预防性控制。每个堆栈只能有一个堆栈策略，但您可以使用该堆栈策略来帮助保护该堆栈内的所有资源。您可以将堆栈策略应用于多个堆栈。

例如，假设您有一个管线，该管线生成敏感构件并将其临时存储在 Amazon Simple Storage Service（Amazon S3）存储桶中以供进一步处理。S3 存储桶由配置 CloudFormation，并且所有必要的安全控制措施都已到位。如果没有堆栈策略，开发者可能会有意或无意地将管线构件的目标更改为不太安全的 S3 存储桶，并暴露敏感数据。如果您对堆栈应用了堆栈策略，则它会阻止授权用户执行不必要的更新或删除操作。

本节包含以下主题：

- 配置堆栈策略
- 设置和覆盖堆栈策略
- 限制和要求堆栈策略

配置堆栈策略

配置堆栈策略时，`Effect`、`Action`、`Principal` 和 `Resource` 元素是必需的。您也可以选择定义 `Condition` 元素。

在创建堆栈策略时，默认情况下，它会阻止对堆栈中的所有资源进行更新。您可以自定义堆栈策略以定义明确允许哪些操作。如果要反转策略，您可以定义一个允许所有操作的 `Allow` 语句，然后指定显式 `Deny` 语句来阻止仅对特定资源的操作。如需参考，请参阅 CloudFormation 文档中的堆栈策略示例。

有关使用这些元素创建自定义堆栈策略的更多信息以及更多示例策略，请参阅 CloudFormation 文档中的定义堆栈策略和更多示例堆栈策略。

设置和覆盖堆栈策略

创建堆栈策略后，将其与堆栈关联。如果要将堆栈策略分配给现有堆栈，则必须使用 AWS Command Line Interface (AWS CLI)。但是，如果您在创建堆栈时分配策略，则可以使用 CloudFormation控制台或 AWS CLI。有关说明，请参阅 CloudFormation 文档中的设置堆栈策略。

当您确实想允许用户更新或删除堆栈中的资源时，您需要暂时覆盖堆栈策略。此覆盖允许您对该堆栈中的受保护资源执行原本被拒绝的操作。有关说明，请参阅 CloudFormation 文档中的更新受保护资源。

限制和要求堆栈策略

作为最低权限许可的最佳实践，请考虑要求 IAM 主体分配堆栈策略并限制 IAM 主体可以分配的堆栈策略。许多 IAM 主体不应有权为自己的堆栈创建和分配自定义堆栈策略。

创建堆栈策略后，我们建议您将这些策略上传到 S3 存储桶。然后，您可以使用 `cloudformation:StackPolicyUrl` 条件键并在 S3 存储桶中提供堆栈策略的 URL，来引用这些堆栈策略。

授予附加堆栈策略的权限

作为最低权限权限的最佳实践，可以考虑限制 IAM 委托人可以附加到堆栈的堆栈策略。CloudFormation 在 IAM 主体的基于身份的策略中，您可以指定 IAM 主体有权分配哪些堆栈策略。这可防止 IAM 主体附加任何堆栈策略，从而降低配置错误的风险。

例如，一个组织可能拥有不同的团队，每个团队都有不同的要求。因此，每个团队都会为其团队特定的 CloudFormation 堆栈制定堆栈策略。在共享环境中，如果所有团队都将其堆栈策略存储在同一 S3 存储桶中，则团队成员可能会附加一个可用但不适用于其团队堆栈的 CloudFormation 堆栈策略。为避免这种情况，您可以定义一个策略声明，允许 IAM 主体仅附加特定的堆栈策略。

以下示例策略允许 IAM 主体附加存储在 S3 存储桶中特定于团队的文件夹中的堆栈策略。您可以在此存储桶中存储已批准的堆栈策略。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:SetStackPolicy"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "cloudformation:StackPolicyUrl": "<Bucket URL>/<Team folder>/*"
        }
      }
    }
  ]
}
```

此策略声明不要求 IAM 主体为每个堆栈分配堆栈策略。即使 IAM 主体有权使用特定的堆栈策略创建堆栈，他们也可以选择创建没有堆栈策略的堆栈。

需要堆栈策略

为确保所有 IAM 主体为其堆栈分配堆栈策略，您可以将服务控制策略（SCP）或权限边界定义为预防性护栏。

以下示例策略显示了如何配置要求 IAM 主体在创建堆栈时分配堆栈策略的 SCP。如果 IAM 主体未附加堆栈策略，则无法创建堆栈。此外，此策略可防止具有堆栈更新权限的 IAM 主体在更新期间删除堆栈策略。该策略使用 `cloudformation:StackPolicyUrl` 条件键限制 `cloudformation:UpdateStack` 操作。

```
        {
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack"
      ],
      "Resource": "*",
      "Condition": {
        "Null": {
          "cloudformation:StackPolicyUrl": "true"
        }
      }
    }
  ]
}
```

通过将此策略声明包含在 SCP 而不是权限边界中，您可以将护栏应用于组织中的所有账户。这可以执行以下操作：

1. 减少将策略单独附加到 AWS 账户中的多个 IAM 主体的工作量。权限边界只能直接附加到 IAM 主体。
2. 减少为不同 AWS 账户创建和管理多个权限边界副本的工作量。这样可以降低在多个相同权限边界中出现配置错误的风险。

> **Note**
>
> SCPs 权限边界是权限防护栏，用于定义账户或组织中 IAM 委托人的最大可用权限。这些策略不会向 IAM 主体授予任何权限。如果您想要标准化您的账户或组织中的所有 IAM 主体分配堆栈策略的要求，则需要同时使用权限护栏和基于身份的策略。

为通过置备的资源配置最低权限权限 CloudFormation

AWS CloudFormation 允许您配置许多不同类型的 AWS 资源。预调配的资源需要自己的一组权限才能按预期运行，并配置谁有权访问这些资源。上一章回顾了配置访问和使用 CloudFormation 服务的权限的选项。本章介绍如何将最低权限原则应用于通过 CloudFormation置备的资源。

在本指南中，几乎不可能查看可通过 CloudFormation配置的每类 AWS 资源的安全建议和最佳实践。如果您对某项特定服务有疑问，我们建议您查看该服务的文档。大多数 AWS 服务 文档都包含安全部分以及有关使用该服务所需权限的信息。有关 AWS 服务 文档的完整列表，请参阅 AWS 文档。

以下是与服务无关的高级步骤，您可以采取这些步骤来创建符合最低权限原则的 CloudFormation模板：

1. 准备一份您计划使用配置的资源清单 CloudFormation。
2. 请参阅 AWS 文档了解相关服务，并查看有关安全性和访问管理的章节。这将帮助您了解特定于服务的要求和建议。
3. 使用您在前面的步骤中收集的信息来设计 CloudFormation 模板和关联策略，这些策略仅允许所需的权限而拒绝所有其他权限。

接下来，本指南将介绍如何使用真实用例在 CloudFormation 模板中应用最低权限原则的示例。

示例：用于存储管线构件的 Amazon S3 存储桶。

此示例将创建一个用于存储 AWS CodeBuild 项目构件的 Amazon Simple Storage Service（Amazon S3）存储桶。AWS CodePipeline 使用这些存储的构件。您可以通过服务角色 CodePipeline 允许 CodeBuild 和访问此 S3 存储桶，并使用 Amazon S3 存储桶策略控制该访问权限。以下是本示例中使用的资源名称：

- `Deployfiles_build`是 CodeBuild 项目的名称。
- `Deployment-Pipeline`是中管道的名称 CodePipeline。

定义 Amazon S3 存储桶

首先，在 CloudFormation 模板中定义 S3 存储桶，该存储桶是一个 YAML 格式的文本文件。

```
amzn-s3-demo-bucket:
```

```
  Type: AWS::S3::Bucket
  Properties:
    PublicAccessBlockConfiguration:
        BlockPublicAcls: true
        BlockPublicPolicy: true
        IgnorePublicAcls: true
        RestrictPublicBuckets: true
```

定义 Amazon S3 存储桶策略

接下来，在 CloudFormation 模板中创建仅允许Deployfiles_build项目和Deployment-Pipeline管道访问存储桶的存储桶策略。

```
MyBucketPolicy:
  Type: AWS::S3::BucketPolicy
  Properties:
    Bucket: !Ref amzn-s3-demo-bucket
    PolicyDocument:
      Version: "2012-10-17"
      Statement:
      - Sid: "S3ArtifactRepoAccess"
        Effect: Allow
        Action:
          - ‘s3:GetObject'
          - ‘s3:GetObjectVersion'
          - ‘s3:PutObject'
          - ‘s3:GetBucketVersioning'
        Resource:
          - !Sub ‘arn:aws:s3:::${amzn-s3-demo-bucket}'
          - !Sub ‘arn:aws:s3:::${amzn-s3-demo-bucket}/*'
        Principal:
          Service:
            - codebuild.amazonaws.com
            - codepipeline.amazonaws.com
        Condition:
          StringLike:
            ‘aws:SourceArn':
              - !Sub ‘arn:aws:codebuild:${AWS::Region}:${AWS::AccountId}:project/
Deployfiles_build'
              - !Sub ‘arn:aws:codepipeline:${AWS::Region}:${AWS::AccountId}:Deployment-
Pipeline'
              - !Sub ‘arn:aws:codepipeline:${AWS::Region}:${AWS::AccountId}:Deployment-
Pipeline/*'
```

请注意有关该存储桶策略的以下详细信息：

- 该 Resource 元素列出了两种不同类型的资源，它们使用以下 Amazon 资源名称（ARN）格式：
  - S3 对象的 ARN 格式为 arn:$*<Partition>*:s3:::$*<BucketName>*/$*<ObjectName>*。
  - S3 存储桶 ARN 的格式为 arn:$*<Partition>*:s3:::$*<BucketName>*。

  s3:GetObject、s3:GetObjectVersion 和 s3:PutObject 需要 S3 对象资源类型，且 s3:GetBucketVersioning 需要 S3 存储桶资源类型。有关每个操作所需的资源类型的更多信息，请参阅 Amazon S3 的操作、资源和条件键。
- 该 Principal 元素列出了允许执行语句中定义的 Amazon S3 操作的实体。在这种情况下，只允许 CodeBuild 和 CodePipeline 执行这些操作。
- 该Condition元素进一步限制了对 S3 存储桶的访问权限，因此只有Deployfiles_build CodeBuild 项目、Deployment-Pipeline CodePipeline 管道和管道操作才能访问该存储桶。

创建服务角色

尽管存储桶策略控制对存储桶的访问权限，但它不授予访问 CodeBuild 和 CodePipeline 访问存储桶的权限。要授予访问权限，您需要为每项服务创建一个服务角色，并在每个服务中添加以下语句。服务角色用于 CodeBuild 并 CodePipeline 允许服务访问 S3 存储桶及其对象。

```
Sid: "ViewAccessToS3ArtifactRepo"
Effect: Allow
Action:
  - ‘s3:GetObject'
  - ‘s3:GetObjectVersion'
  - ‘s3:PutObject'
  - ‘s3:GetBucketVersioning'
Resource:
  - !Sub ‘arn:aws:s3:::${BuildArtifactsBucket}'
  - !Sub ‘arn:aws:s3:::${BuildArtifactsBucket}/*'
```

最低权限权限的最佳实践 AWS CloudFormation

本指南回顾了不同的方法和某些类型的策略，您可以使用这些方法和策略来配置对资源的最低权限访问权限 AWS CloudFormation 和通过其配置的资源。 CloudFormation本指南重点介绍 CloudFormation 通过 IAM 委托人、服务角色和堆栈策略配置访问权限。随附的建议和最佳实践旨在帮助保护您的账户和堆栈资源免受授权用户的意外操作以及可能利用过度权限的恶意操作者的侵害。

以下是本指南中介绍的最佳实践的摘要。这些最佳实践可以帮助您在配置使用权限 CloudFormation 和通过 CloudFormation以下方式配置资源时遵守最低权限原则：

- 确定用户和团队需要什么级别的访问权限才能使用该 CloudFormation 服务，并仅授予所需的最低访问权限。例如，向实习生和审计员授予查看权限，且不允许这些类型的用户创建、更新或删除堆栈。
- 对于需要通过 CloudFormation 堆栈配置多种类型 AWS 资源的 IAM 委托人，可以考虑使用服务角色 CloudFormation 来允许代表委托人配置资源，而不是配置对委托人基于身份的策略 AWS 服务 中的资源的访问权限。
- 在 IAM 委托人的基于身份的策略中，使用`cloudformation:RoleARN`条件键来控制可以传递哪些 CloudFormation 服务角色。
- 为帮助防止权限升级，请执行以下操作：
  - 严格监控所有有权访问该 CloudFormation 服务的 IAM 委托人及其访问级别。
  - 严格监控哪些用户可以访问这些 IAM 主体。
  - 监控可以向其传递特权服务角色的 IAM 委托人的活动。 CloudFormation虽然他们可能无权通过基于身份的策略创建 IAM 资源，但他们可以传递的服务角色可以创建 IAM 资源。
- 只要创建具有重要资源的堆栈，就要指定堆栈策略。这可以帮助保护关键堆栈资源免受可能导致这些资源中断或替换的意外更新。
- 有关通过配置的资源 CloudFormation，请参阅该服务的访问管理建议和安全最佳实践。
- 为了补充本指南中针对基于身份的策略和基于资源的策略的建议，可以考虑对最低权限权限实施额外的安全控制，例如服务控制策略 () SCPs 和权限边界。有关更多信息，请参阅 后续步骤。

该 CloudFormation 文档包含其他最佳实践和安全最佳实践，可帮助您 CloudFormation 更有效、更安全地使用。此外，请参阅本指南中的为最低权限访问配置基于身份的策略的最佳实践 CloudFormation。

后续步骤

您可以使用本指南中的信息和示例，开始在您的组织中应用最低权限原则。我们建议您查看资源一节中的其他资源，其中包含可帮助您优化策略的文档参考和工具。

本指南旨在帮助您开始实施 AWS CloudFormation 的最低权限访问。但是，还有其他类型的策略可以帮助您在组织中加强最低权限原则。根据您的环境和业务需求，您可能要实施本指南中未讨论的额外控件。下一步以及有关更多信息，我们建议您查看以下与最低权限和配置访问和权限相关的主题：

- IAM 实体的权限边界
- 服务控制策略（SCP）
- 用于跨账户访问的角色
- 联合身份
- 查看 IAM 的上次访问信息

以下工具可以帮助您监控 CloudFormation 的最低权限访问和权限：

- AWS Identity and Access Management Access Analyzer
- 您可以使用 AWS Identity and Access Management（IAM）控制台中的访问权限推荐功能选项卡，来识别 IAM 身份的过度权限。有关示例，请参阅 Tighten S3 permissions for your IAM users and roles using access history of S3 actions（AWS 博客文章）。
- 您可以使用检查工具 [例如 cfn-policy-validator（GitHub）]，来帮助识别过多的权限。

在您熟悉创建和管理 CloudFormation 权限后，建议您使用持续集成和持续交付（CI/CD）管线来部署您的 CloudFormation 模板。这降低了人为错误的风险，并加快了部署过程。

资源

AWS CloudFormation 文档

- 使用 AWS Identity and Access Management控制访问权限
- AWS 资源和属性类型参考
- 设置 AWS CloudFormation 堆栈选项
- AWS CloudFormation 服务角色

AWS Identity and Access Management （ IAM 文档 ）

- IAM 中的策略和权限
- IAM JSON 策略元素参考
- 策略评估逻辑
- 与 IAM 配合使用的AWS 服务
- 创建角色以向某人委派权限 AWS 服务
- 混淆代理人问题
- IAM 安全最佳实操

其他 AWS 参考

- AWS 服务的操作、资源和条件键（服务授权参考）
- 授予最低权限访问权限（AWS Well-Architected 框架）
- 编写最低权限 IAM 策略的技巧（AWS 博客文章）

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
重大更新	我们对指引和策略声明样本进行了重大修订和完善，以解决常见的组织使用案例。	2023 年 5 月 5 日
初次发布	—	2023 年 3 月 9 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：

- Refactor/re-architect — 充分利用云原生功能来提高敏捷性、性能和可扩展性，从而移动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 数据库迁移到亚马逊 Aurora PostgreSQL-Compatible 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：将本地 Oracle 数据库迁移到 AWS Cloud中的 Amazon Relational Database Service（Amazon RDS）for Oracle。
- 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。
- 重新托管（直接迁移）：将应用程序迁移到云，无需进行任何更改即可利用云功能。示例：将本地 Oracle 数据库迁移到 AWS Cloud中 EC2 实例上的 Oracle。
- 重新放置（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。您将服务器从本地平台迁移到同一平台的云服务中。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

A2A () Agent-to-Agent

一种支持任务委托和状态转移的代理到代理协作的状态协议。

ABAC

请参阅基于属性的访问控制。

抽象服务

请参阅托管服务。

ACID

请参阅原子性、一致性、隔离性、持久性。

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。它比主动-被动迁移更灵活，但工作量更大。

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。

座席

一种能够使用工具自主推理、计划和采取行动来实现目标的人工智能系统。

特工行动

在生产环境中大规模构建、测试、部署和运行 AI 代理的操作实践。

聚合函数

一种 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

请参阅人工智能。

AIOps

请参阅人工智能运营。

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。

权威数据来源

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来源复制到其他位置，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

恶意机器人

一种旨在扰乱或伤害个人或组织的机器人。

BCP

请参阅业务连续性计划。

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。另请参阅字节顺序。

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。

blue/green 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应用程序版本（蓝色），在另一个环境中运行新应用程序版本（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交互的软件应用程序。有些机器人是有用或有益的，例如在互联网上索引信息的 Web 爬网程序。还有一些被称为恶意机器人的机器人，其目的是扰乱或伤害个人或组织。

僵尸网络

被恶意软件感染并受单方（称为僵尸网络控制者或僵尸网络操作者）控制的僵尸网络。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）。

紧急（break-glass）访问

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，请参阅指南中的 “实施破碎玻璃程序” AWS Well-Architected 指示器。

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

请参阅 AWS 云采用框架。

金丝雀部署

缓慢而渐进地向最终用户发布版本。当您确信无误后，即可部署新版本，并完全替换当前版本。

CCoE

请参阅云卓越中心。

CDC

请参阅更改数据捕获。

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韧性。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

请参阅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。

公民开发者

使用无code/low代码平台创建 AI 应用程序但没有专业技术技能的企业用户。

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。云计算通常连接到边缘计算技术。

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 Cloud中时通常会经历四个阶段：

- 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
- Re-invention — 优化产品和服务，在云端进行创新

Stephen Orban在 AWS Cloud 企业战略博客的博客文章《走向之旅 Cloud-First 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

请参阅配置管理数据库。

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 Bitbucket Cloud。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）

一种 AI 领域，它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，Amazon SageMaker AI 为 CV 提供了图像处理算法。

配置偏移

对于工作负载而言，一种偏离预期状态的配置更改。这可能会导致工作负载变得不合规，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、提高生产力、提高代码质量和更快地交付。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

请参阅计算机视觉。

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《 AWS Well-Architected 框架》中安全支柱的组成部分。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

请参阅数据库定义语言。

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。

深度防御

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，深度防御方法可能将多因素身份验证、网络分段和加密结合起来。

委派管理员

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

请参阅环境。

侦测性控制

一种安全控制，在事件发生后进行检测、记录日志和发出提醒。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

星型架构中的一种较小的表，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）

您用来最大程度地减少由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《工作负载灾难恢复 AWS： AWS Well-Architected 框架中的云端恢复》。

DML

请参阅数据库操作语言。

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。埃里克·埃文斯（Eric Evans）在他的《Domain-Driven 设计：解决软件核心的复杂性》（波士顿： Addison-Wesley 专业版，2003年）一书中介绍了这个概念。有关如何使用带有 strangler fig 模式的域驱动设计的信息，请参阅使用容器和 Amazon API Gateway 逐步实现传统微软 ASP.NET (ASMX) 网络服务的现代化。

DR

请参阅灾难恢复。

偏差检测

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

请参阅开发价值流映射。

E

EDA

请参阅探索性数据分析。

EDI

请参阅电子数据交换。

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。与云计算比较时，边缘计算可以减少通信延迟并缩短响应时间。

电子数据交换（EDI）

组织之间业务文件的自动交换。有关更多信息，请参阅什么是电子数据交换。

加密

一种将人类可读的纯文本数据转换为加密文字的计算流程。

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。 Big-endian 系统首先存储最重要的字节。 Little-endian 系统首先存储最低有效字节。

端点

请参阅服务端点。

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。

环境

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

请参阅企业资源规划。

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

星型架构中的中心表。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。

快速失效机制

一种使用频繁且增量式的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

请参阅分支。

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。

少样本提示

在要求 LLM 执行类似任务之前，先向其提供少量示例，以演示任务和预期输出。这种技术是情境学习的应用，模型可以从提示中嵌入的示例（镜头）中学习。 Few-shot 对于需要特定格式、推理或领域知识的任务，提示可能非常有效。另请参阅零样本提示。

FGAC

请参阅精细访问控制。

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，通过更改数据捕获使用连续数据复制，在极短的时间内迁移数据，而非使用分阶段方法。目标是将停机时间降至最低。

FM

请参阅基础模型。

基础模型（FM）

一个大型深度学习神经网络，它已使用海量的通用和未标注数据集进行训练。FM 能够执行各种常规任务，例如理解语言、生成文本和图像以及使用自然语言进行对话。有关更多信息，请参阅什么是基础模型。

FM 网关

一种集中式中介，用于控制和规范对基础模型的访问。也称为 LLM 网关。

G

生成式人工智能

AI 模型的一个子集，这些模型已经过大量数据训练，可以使用简单的文本提示来创建新的内容和构件，例如图像、视频、文本和音频。有关更多信息，请参阅什么是生成式人工智能。

地理阻止

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工作流程，而基于中继的工作流程则是现代的、首选的方法。

黄金映像

系统或软件的快照，用作部署该系统或软件的新实例的模板。例如，在制造业中，黄金映像可用于在多个设备上预调配软件，并有助于提高设备制造操作的速度、可扩展性和生产效率。

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。侦测性护栏会检测策略违规和合规性问题，并生成提醒以进行修复。它们通过使用 AWS Config、、Amazon、 AWS Security Hub CSPM GuardDuty AWS Trusted Advisor、Amazon Inspector 和自定义 AWS Lambda 支票来实现。

护栏 (AI)

用于过滤、验证和限制代理输入和输出的安全机制，有助于确保负责任和安全的 AI 行为。

H

HA

请参阅高可用性。

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。

保留数据

从用于训练机器学习模型的数据集中保留的一部分标注的历史数据。通过将模型预测与保留数据进行比较，您可以使用保留数据来评估模型性能。

人机在圈 (HitL)

一种工作流程模式，其中代理执行在关键决策点暂停以供人工审查和批准。

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。

我

IaC

请参阅基础设施即代码。

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

请参阅工业物联网。

不可变基础设施

一种模型，可为生产工作负载部署新的基础设施，而不是更新、修补或修改现有基础设施。不可变基础设施本质上比可变基础设施更一致、更可靠、更可预测。有关更多信息，请参阅框架中的使用不可变基础架构部署最佳实践。 AWS Well-Architected

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）在2016年推出，指的是通过连接性、实时数据、自动化、分析和的进步实现制造流程的现代化。 AI/ML

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调配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，请参阅机器学习模型的可解释性 AWS。

物联网

请参阅物联网。

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。

大语言模型（LLM）

一种基于大量数据进行预训练的深度学习 AI 模型。LLM 可以执行多项任务，例如回答问题、总结文档、将文本翻译成其他语言以及完成句子。有关更多信息，请参阅什么是 LLM。

大规模迁移

迁移 300 台或更多服务器。

LBAC

请参阅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

请参阅 7 R。

小端序系统

一个先存储最低有效字节的系统。另请参阅字节顺序。

LLM

请参阅大型语言模型。

下层环境

请参阅环境。

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

请参阅分支。

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权限。恶意软件的示例包括病毒、蠕虫、勒索软件、木马、间谍软件和键盘记录器。

托管式服务

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。Amazon Simple Storage Service（Amazon S3）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

请参阅迁移加速计划。

MCP

参见模型上下文协议。

模型上下文协议（MCP）

一种用于代理与工具通信的无状态协议。

MCP 服务器

一种通过模型上下文协议公开一个或多个工具的服务。

机制

一个完整的过程，您可以在其中创建工具，推动工具的采用，然后检查结果以进行调整。机制是一种在运作过程中自我强化和改善的循环。有关更多信息，请参阅在 AWS Well-Architected 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

请参阅制造执行系统。

消息队列遥测传输（MQTT）

一种基于publish/subscribe模式的轻量级机器对机器 (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

Cross-functional 通过自动化、敏捷的方法简化工作负载迁移的团队。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，提供了用于验证迁移到 AWS Cloud的业务案例的信息。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

将工作负载迁移到 AWS Cloud的方法。有关更多信息，请参见术语表中的 7 R 词条，以及动员您的组织以加快大规模迁移。

ML

请参阅机器学习。

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，请参阅在 AWS Cloud中实现应用程序现代化的策略。

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，请参阅在 AWS Cloud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

请参阅迁移组合评测。

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？”

可变基础设施

一种用于更新和修改生产工作负载的现有基础设施的模型。为了提高一致性、可靠性和可预测性，该 AWS Well-Architected 框架建议使用不可变基础设施作为最佳实践。

O

OAC

请参阅来源访问控制。

OAI

请参阅来源访问身份。

OCM

请参阅组织变革管理。

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

请参阅运营集成。

OLA

请参阅运营级别协议。

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

请参阅开放流程通信 – 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机器对机器 (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）

一份问题核对清单和关联的最佳实践，可帮助您了解、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 AWS Well-Architected 框架中的运营准备情况审查 (ORR)。

运营技术（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 转型的关键重点。

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。

ORR

请参阅运营准备情况审查。

OT

请参阅运营技术。

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

请参阅个人身份信息。

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

请参阅可编程逻辑控制器。

PLM

请参阅产品生命周期管理。

policy

一个对象，可以定义权限（请参阅基于身份的策略）、指定访问条件（请参阅基于资源的策略）或定义 AWS Organizations 的组织中所有账户的最大权限（请参阅服务控制策略）。

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。

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 `false` 的查询条件，通常位于 `WHERE` 子句中。

谓词下推

一种数据库查询优化技术，可在传输之前筛选查询中的数据。这将减少从关系数据库检索和处理的数据量，并提高查询性能。

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

一种在整个开发过程中都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，旨在防止部署不合规资源。这些控制会在资源预置之前对其进行扫描。如果资源与控制不兼容，则不会预置它。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）

对产品在其整个生命周期内的数据和流程的管理，从设计、开发和发布，到增长和成熟，再到衰退和淘汰。

生产环境

请参阅环境。

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。

提示串接

使用一个 LLM 提示的输出作为下一个提示的输入，以生成更好的响应。该技术用于将复杂的任务分解为子任务，或者迭代地完善或扩展初步响应。它有助于提高模型响应的准确性和相关性，并允许获得更精细的个性化结果。

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。

publish/subscribe (pub/sub)

一种支持微服务间异步通信的模式，可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

一系列用于访问 SQL 关系数据库系统中的数据的步骤，类似于指令。

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

请参阅责任、问责、咨询和知情（RACI）。

RAG

请参阅检索增强生成。

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

请参阅责任、问责、咨询和知情（RACI）。

RCAC

请参阅行列访问控制。

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

请参阅 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

请参阅 7 R。

Region

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，请参阅指定您的账户可以使用的 AWS 区域。

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

请参阅 7 R。

版本

在部署过程中，推动生产环境变更的行为。

重新放置

请参阅 7 R。

更换平台

请参阅 7 R。

重新购买

请参阅 7 R。

韧性

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

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

请参阅 7 R。

停用

请参阅 7 R。

检索增强生成（RAG）

一种生成式人工智能技术，其中 LLM 在生成响应之前引用其训练数据来源之外的权威数据来源。例如，RAG 模型可以对组织的知识库或自定义数据执行语义搜索。有关更多信息，请参阅什么是 RAG。

轮换

定期更新密钥以使攻击者更难访问凭证的过程。

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

请参阅恢复点目标。

RTO

请参阅恢复时间目标。

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 管理控制台 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

请参阅监督控制和数据采集。

SCP

请参阅服务控制策略。

机密密钥

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 Secrets Manager 文档中的什么是 Amazon Secrets Manager 密钥？。

安全设计

一种在整个开发过程中都考虑安全的系统工程方法。

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。安全控制有以下四种类型：预防性、检测性、响应性和主动性。

安全固化

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

一种预定义的程序化操作，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 实例或轮换凭证。

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。

服务水平指示器（SLI）

对服务性能方面的衡量，例如错误率、可用性或吞吐量。

服务水平目标（SLO）

代表服务运行状况的目标指标，由服务水平指示器衡量。

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。

暗影人工智能

在组织内受管控渠道之外构建或使用的未经授权的 AI 应用程序。

SIEM

请参阅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

请参阅服务水平协议。

SLI

请参阅服务水平指示器。

SLO

请参阅服务水平目标。

split-and-seed 模式

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，请参阅在 AWS Cloud中实现应用程序现代化的分阶段方法。

SPOF

请参阅单点故障。

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事务数据或测量数据，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 逐步实现传统微软 ASP.NET (ASMX) 网络服务的现代化。

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。

监督控制和数据采集（SCADA）

在制造业中，一种使用硬件和软件来监控实物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。

系统提示

一种为 LLM 提供上下文、说明或准则以指导其行为的技术。系统提示有助于设置上下文并制定与用户交互的规则。

T

标签

Key-value 对充当用于组织 AWS 资源的元数据。标签有助于您管理、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

请参阅环境。

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。

工具

代理可以调用以在外部系统中执行操作的函数或 API。

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。

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

请参阅环境。

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

一种对与当前记录有某种关联的一组行执行计算的 SQL 函数。窗口函数对于处理任务很有用，例如计算移动平均值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。

WORM

请参阅一次写入多次读取。

WQF

请参阅 AWS 工作负载资格鉴定框架。

一次写入多次读取（WORM）

一种存储模型，可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，但无法对其进行更改。此数据存储基础设施被认为不可变。

Z

零日漏洞利用

一种利用零日漏洞的攻击，通常为恶意软件。

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。

零样本提示

为 LLM 提供执行任务的说明，但没有可以帮助指导的示例（样本）。LLM 必须使用预先训练的知识来处理任务。零样本提示的有效性取决于任务的复杂性和提示的质量。另请参阅少样本提示。

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。