正在过渡到多个 AWS 账户

AWS 规范性指导

AWS 规范性指导: 正在过渡到多个 AWS 账户

Table of Contents

简介 1
目标受众 2
目标业务成果 3
单账户架构示例 3
基础框架 5
AWS Well-Architected Framework 5
Cloud Foundation on AWS 5
身份管理和访问控制 6
设置组织 6
最佳实操 7
创建登录区 7
最佳实操 7
添加组织单位 8
最佳实操 9
添加初始用户 9
最佳实操 9
管理成员账户 10
邀请您先前存在的账户 11
在 AWS Control Tower 中自定义 VPC 设置 12
定义范围界定标准 12
管理权限和访问权限 14
工程文化方面的注意事项 14
创建权限集 15
账单权限集 15
开发人员权限集 15
生产权限集 17
创建权限边界 18
管理个人的权限 22
网络连接 23
连接 VPC 23
连接应用程序 23
最佳实践 24
集中式出口 24
保护出口流量的最佳实践 25

分散式入口 26
安全事件响应 29
Amazon GuardDuty 29
最佳实践 29
Amazon Macie 30
最佳实践 30
AWS Security Hub 30
最佳实践 31
备份 32
账户迁移 33
资源迁移 34
AWS AppConfig 35
AWS Certificate Manager 35
Amazon CloudFront 35
AWS CodeArtifact 35
Amazon DynamoDB 35
Amazon EBS 36
Amazon EC2 36
Amazon ECR 36
Amazon EFS 36
亚马逊 ElastiCache (RedisOSS) 37
AWS Elastic Beanstalk 37
弹性 IP 地址 37
AWS Lambda 37
Amazon Lightsail 37
Amazon Neptune 38
亚马逊 OpenSearch 服务 38
Amazon RDS 38
Amazon Redshift 38
Amazon Route 53 38
Amazon S3 39
Amazon SageMaker 39
AWS WAF 39
账单注意事项 40
结论 41
贡献者 42

资源 43
AWS Prescriptive Guidance 43
AWS 博客文章 43
AWS 白皮书 43
AWS 代码示例 43
文档历史记录 44
术语表 46
..... 46
A 46
B 49
C 50
D 53
E 56
F 58
G 59
H 60
I 61
L 63
M 63
O 67
P 69
Q 71
R 71
S 74
T 77
U 78
V 78
W 79
Z 80
..... lxxxi

过渡到多个 AWS 账户

亚马逊 Web Services（贡献者）

2024 年 5 月（文件历史记录）

许多公司都是从使用单一的 Amazon Web Services（AWS）账户开始自己的旅程。公司内的多个角色使用此账户来运营业务。工程师开发代码，部署到开发和测试环境，并推动对生产环境的更改。产品经理查询数据来源，以收集对业务绩效的见解。销售团队在生产环境中进行演示，以吸引新客户。财务团队正在通过 AWS Billing 控制台监控云支出。

当所有这些不同的角色都使用单个角色时 AWS 账户，可能很难强制执行应用最低权限的安全最佳实践，这意味着您只授予完成工作所需的最低权限。在初创企业发展的某个阶段，有人会提出这样的问题：我们所有的工程师都需要访问生产环境吗？ 答案几乎总是不；但是许多公司都在努力解决如何在不减缓业务的情况下将现有的单账户环境转变为多账户环境的问题。

本指南包含最佳实践，可帮助您从单账户环境过渡到多账户环境。其中探讨了您需要做出的有关账户迁移、用户管理、联网、安全和架构的各项决策。本文旨在帮助您在业务和日常运营中以最小的停机时间或无停机时间取得成功。本指南重点介绍从单 AWS 账户 账户环境过渡到多账户环境时的以下功能：

- 身份管理和访问控制
- 管理权限和访问权限
- 网络连接
- 安全事件响应
- 备份
- 账户迁移
- 资源迁移
- 账单注意事项

有关各项功能的更多信息，请参阅 Cloud Foundation on AWS。

本指南与与本主题相关的现有资源保持一致，包括AWS 启动安全基准 (AWS SSB)、《使用多个账户组织 AWS 环境》白皮书、《AWS 安全参考架构》(AWS SRA) 和《建立云基础 AWS白皮书》。您可以继续使用这些资源，获取本指南中未介绍的更具体的指导。

目标受众

本指南最适合想要或需要过渡到多 AWS 账户的公司。对于初创企业来说，当你找到了产品与市场的契合度，筹集了一轮资金，并开始雇用不同的工程学科，例如基础设施、开发运营（DevOps）或安全时，通常会出现这种需求。

即使您的公司还没有准备好进行这种过渡，您仍然可以使用本指南来了解过渡期间需要做出的决策，并着手做好准备。

过渡到多账户架构的目标业务成果

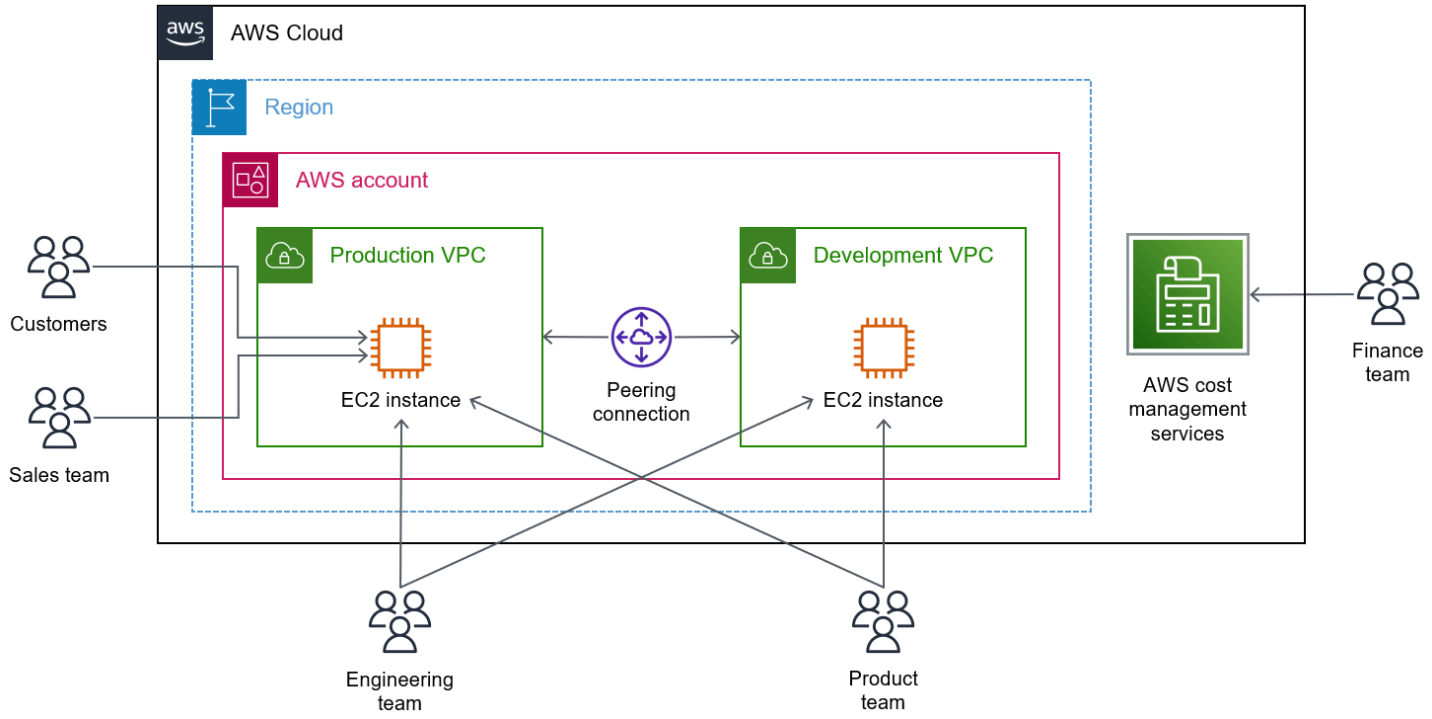
过渡到多账户架构通常是由对以下一项或多项好处的业务需求所驱动：

- 根据业务目的或所有权对工作负载进行分组
- 按环境应用不同的安全控制
- 限制对敏感数据的访问
- 促进创新和敏捷性
- 限制不良事件的影响范围
- 支持多种 IT 运营模式
- 管理成本
- 分配 AWS 服务 限额和 API 请求速率限制

有关多账户架构的多重好处的更多信息，请参阅使用多个账户整理您的 AWS 环境（AWS 白皮书）和建立架构完善的环境的指导方针（AWS Control Tower 文档）。

单账户架构示例

作为起点，初创企业或小型公司通常使用单 AWS 区域，并有两个通过 VPC 对等连接的虚拟私有云（VPC）。每个 VPC 都包含计算资源，例如 Amazon Elastic Compute Cloud（Amazon EC2）实例。工程团队直接在开发 VPC 中开发代码。产品团队审查更改，之后工程团队手动将更改提升到生产 VPC。财务团队可以访问 AWS 账户，这样他们就可以查看 AWS Billing and Cost Management 控制台。



以下是公司在这种环境下可能遇到的挑战的几个示例：

- 一名工程师误以为正在访问开发数据库，却删除了生产数据。
- 当生产部署花费的时间超过预期时，销售演示受到了影响。
- 在对开发代码进行负载测试时，生产 VPC 速度变慢，并生成有关节流的错误消息。
- 财务团队无法区分生产环境和开发环境的成本。
- 首席执行官担心，一些新雇用的离岸承包商可以通过生产 VPC 访问客户数据。
- 财务团队不能禁止访问可能导致高成本的特定 AWS 服务。

采用多账户策略通过使用分离式 AWS 账户 将工作负载和访问权限分开，从而解决了所有这些挑战。

有关过渡到多账户架构的基础框架和安全责任

本指南中的信息和最佳实践旨在与有关基础设施和安全的现有 AWS 建议相辅相成。当从单 AWS 账户过渡到多 AWS 账户 时，请务必确保您的新多账户架构与 AWS Well-Architected Framework 和 Cloud Foundation 原则保持一致。这可以帮助您构建和运营一个专门针对安全性、性能和弹性而设计的环境，同时遵守治理要求和 AWS 最佳实践。

AWS Well-Architected Framework

AWS Well-Architected Framework 可帮助您为各种应用程序和工作负载构建安全、高性能、弹性和高效的基础设施。本指南与此框架的卓越运营、安全性以及可靠性支柱保持一致。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。

Cloud Foundation on AWS

构建您的 Cloud Foundation on AWS（AWS 白皮书）提供的指导可帮助您量身定制 AWS 满足您业务需求的环境。您可以使用基于容量的方法，创建一个用于部署、运营和管理工作负载的环境。您还可以增强各项功能，以便随着需求的变化而扩展环境，进而将更多工作负载部署到云。有关 AWS 定义的 30 项功能的更多信息，请参阅功能。本指南包括按预期顺序实现初始功能的最佳实践。

您可以根据自己的运营和治理需求采用和实现各种功能。随着业务需求日臻完善，可将基于容量的方法用作一种机制，以验证您的云环境是否已准备好支持您的工作负载并根据需要进行扩展。这种方法使您能够信心百倍地为构建者和业务建立云环境。

用于过渡到多账户架构的身份管理和访问控制

过渡到多账户架构的第一步是在组织内设置新的账户结构。然后，您可以添加用户并配置他们对账户的访问权限。本节介绍管理用户访问多 AWS 账户 的权限的方法。

本节包含以下任务：

- 设置组织
- 创建登录区
- 添加组织单位
- 添加初始用户
- 管理成员账户

设置组织

当有多个 AWS 账户 时，您可以在 AWS Organizations 中通过组织以逻辑方式管理这些账户。AWS Organizations 中的账户是标准 AWS 账户，其中包含您的 AWS 资源以及可以访问这些资源的身份。组织是供合并您的 AWS 账户 的实体，以便可以将这些账户作为单个单位进行管理。

当您使用账户创建组织时，该账户将变为管理账户（也称为付款人账户或根账户）代表该组织。一个组织只能有一个管理账户。当为组织添加额外 AWS 账户 时，这些账户会变成成员账户。

> **Note**
>
> 每个 AWS 账户 还有一个叫做根用户的单一实体。您可以使用在创建账户时使用的电子邮件地址和密码以根用户身份登录。但是，我们强烈建议您不要使用根用户来执行日常任务，即使是管理任务。有关更多信息，请参阅 AWS 账户 根用户。

您可以以树状分层结构组织账户，该结构包括组织根账户、组织单元（OU）账户和成员账户。根是您组织中所有账户的父容器。一个组织单位（OU）是根中账户的一个容器。一个 OU 可以包含其他 OU 或成员账户。一个 OU 只有一个父级，而每个账户都只能是一个 OU 的成员。有关更多信息，请参阅术语和概念（AWS Organizations 文档）。

服务控制策略（SCP）指定用户和角色可以使用的服务和操作。SCP 类似于 AWS Identity and Access Management（IAM）权限策略，不同的是前者不授予任何权限。相反，SCP 定义最大权限。当您将策

略附加到层次结构中的一个节点时，该策略将应用于该节点中的所有 OU 和账户。例如，如果您将策略应用于根目录，该策略将应用于组织中所有 OU 和账户；如果您将策略应用于 OU，该策略将仅应用于 OU 和目标 OU 中的账户。

您可以使用 AWS Organizations 控制台集中查看和管理组织内所有账户。使用组织的好处之一是，您可以收到一份整合账单，其中显示与管理账户和成员账户相关的所有费用。有关更多信息，请参阅整合账单（AWS Organizations 文档）。

最佳实操

- 不要使用现有 AWS 账户 创建组织。用一个新账户开始，该账户将成为组织的管理账户。组织的管理账户中可以执行特权操作，SCP 不适用于管理账户。因此，管理账户中包含的云资源和数据应仅限于必须在管理账户中管理的云资源和数据。
- 将管理账户的访问权限限制为仅需要配置新 AWS 账户 并管理组织的个人才可访问。
- 使用 SCP 定义根账户、组织单位账户和成员账户的最大权限。SCP 不能直接应用于管理账户。
- 遵守 AWS Organizations 的最佳实践（AWS Organizations文档）。

创建登录区

登录区是一个架构完善的多账户 AWS 环境，这是您可以从中部署工作负载和应用程序的起点。它为开始使用多账户架构、身份和访问管理、治理、数据安全、网络设计和日志记录提供了基准。AWS Control Tower 是一项通过提供自动化防护机制来简化多账户环境维护和治理的服务。通常，您需要预置一个AWS Control Tower登录区来管理跨所有 AWS 区域 的环境。AWS Control Tower 通过编排账户中的其他 AWS 服务 来运作。有关更多信息，请参阅当您设置登录区时会发生什么（AWS Control Tower 文档）。

当使用 AWS Control Tower 设置登录区时，您可以标识三个共享账户：管理账户、日志存档账户和审计账户。有关更多信息，请参阅共享账户有哪些（AWS Control Tower 文档）。对于管理账户，您必须使用未托管任何工作负载的现有账户来设置登录区。对于日志存档账户和审计账户，您可以选择重复使用现有 AWS 账户，或者 AWS Control Tower 可以为您创建它们。

有关如何设置 AWS Control Tower 登录区的说明，请参阅入门指南（AWS Control Tower 文档）。

最佳实操

- 遵守多账户策略的设计原则中的安全最佳实践（AWS 白皮书）。
- 遵守有关 AWS Control Tower 管理员的最佳实践（AWS Control Tower 文档）。

- 在 AWS 区域 中创建登录区，托管您的大部分工作负载。

> **Important**
>
> 如果您在部署登录区后决定更改此区域，则需要 AWS Support 的帮助，而且必须停用登录区。不建议采用这种做法。

- 在确定 AWS Control Tower 将管理哪些区域时，请仅选择您希望立即部署工作负载的区域。您可以更改这些区域，也可以稍后添加更多区域。如果 AWS Control Tower 管理一个区域，则它将在该区域部署检测性防护机制作为 AWS Config 规则。
- 在确定了 AWS Control Tower 将管理哪些区域之后，拒绝访问所有未受管理的区域。这有助于确保您的工作负载和开发人员只能使用经过批准的 AWS 区域。这是作为组织的服务控制策略（SCP）来实现。有关更多信息，请参阅 Configure the AWS 区域 deny control（AWS Control Tower 文档）。
- 在 AWS Control Tower 中设置登录区时，我们建议重命名以下 OU 和账户：
  - 我们建议重命名安全 OU 为 Security_Prod，表示此 OU 将用于与生产安全相关的 AWS 账户。
  - 我们建议允许 AWS Control Tower 创建其他 OU，然后将其从沙盒重命名为工作负载。在下一节中，您将在工作负载 OU 中创建其他 OU，用它来整理您的 AWS 账户。
  - 我们建议将集中日志记录AWS 账户从日志存档重命名为 log-archive-prod。
  - 我们建议将审计账户从审计重命名为 security-tooling-prod。
- 为了帮助防止欺诈，AWS 需要 AWS 账户 具有使用历史记录才能添加到 AWS Control Tower 登录区。如果您使用的是新 AWS 账户，且新账户中没有任何使用历史记录，则可以不使用 AWS 免费套餐启动 Amazon Elastic Compute Cloud（Amazon EC2）实例。让实例运行几分钟，然后将其终止。

添加组织单位

建立适当的组织结构对于设置多账户环境至关重要。由于您使用服务控制策略（SCP）来定义组织单位及其中的账户的最大权限，因此从管理、权限和财务报告的角度来看，您的组织结构必须合乎逻辑。有关组织的结构，包括组织单位（OU）的更多信息，请参阅术语和概念（AWS Organizations 文档）。

在本节中，您将通过创建嵌套的 OU 来自定义登录区，以帮助细分和构建环境，例如生产环境和非生产环境。这些推荐的最佳做法旨在细分您的登录区，将生产资源与非生产资源分开，将基础设施与工作负载分开。

有关如何创建 OU 的更多信息，请参阅管理组织单位（AWS Organizations 文档）。

最佳实操

- 在您于 创建登录区 中创建的工作负载中，创建以下嵌套的 OU：
  - Prod：将此 OU 用于存储和访问生产数据的 AWS 账户，包括客户数据。
  - NonProd：将此 OU 用于存储非生产数据的 AWS 账户，例如开发、暂存或测试环境。

在组织根账户下，创建一个 Infrastructure_Prod OU。使用此 OU 托管集中式网络账户。

添加初始用户

有两种方法向用户授予对 AWS 账户 的访问权限：

- IAM 身份，例如：用户、组和角色
- 身份联合验证，例如使用 AWS IAM Identity Center

在小型公司和单账户环境中，管理员通常会在有新人加入公司时创建 IAM 用户。与 IAM 用户关联的访问密钥和私密密钥凭证称为长期凭证，因为它们不会过期。但是，这并不是推荐的安全最佳实践，因为如果攻击者破解了这些凭证，则您必须为用户生成一组新的凭证。访问 AWS 账户 的另一种方式是通过 IAM 角色。您也可以使用 AWS Security Token Service（AWS STS）临时请求短期凭证，它将在一段可配置的时间后过期。

您可以通过 IAM Identity Center 管理用户对 AWS 账户 的访问权限。您可以为每位员工或承包商创建个人用户账户，他们可以管理自己的密码和多重身份验证（MFA）解决方案，也可以对他们进行分组以管理访问权限。配置 MFA 时，您可以使用软件令牌（例如：身份验证器应用程序），也可以使用硬件令牌（例如：YubiKey 设备）。

IAM Identity Center 还支持来自外部身份提供者（IdP）的联合身份验证，例如 Okta、JumpCloud 和 Ping Identity。有关更多信息，请参阅支持的身份提供者（IAM Identity Center documentation 文档）。您可以通过与外部 IdP 联合，跨应用程序管理用户身份验证，然后使用 IAM Identity Center 向特定 AWS 账户 授予访问权限。

最佳实操

- 遵循配置用户访问权限的安全最佳实践（IAM 文档）。
- 按组而不是个人用户管理账户访问权限。在 IAM Identity Center 中，创建代表您的每项业务职能的新组。例如，您可以为工程、财务、销售和产品管理等部门创建组。

- 通常，将需要访问所有 AWS 账户 的人（通常只有只读访问权限）以及需要访问单个 AWS 账户 的人分开来定义组。我们建议您对组使用以下命名惯例，以便于识别 AWS 账户 以及与该组关联的权限。

  `<prefix>-<account name>-<permission set>`

- 例如，对于组 `AWS-A-dev-nonprod-DeveloperAccess`，`AWS-A` 是一个前缀，表示对单个账户的访问权限，`dev-nonprod` 是账户的名称，`DeveloperAccess` 是分配给该组的权限集。对于组 `AWS-O-BillingAccess`，`AWS-O` 前缀表示具有对整个组织的访问权限，`BillingAccess` 表示该组的权限集。在本例中，由于组有权访问整个组织，因此组名中没有显示账户名。
- 如果您将 IAM Identity Center 与外部基于 SAML 的 IdP 一起使用，并且希望要求 MFA，则可以使用基于属性的访问权限控制（ABAC）将身份验证方法从 IdP 传递到 IAM Identity Center。这些属性通过 SAML 断言发送。有关更多信息，请参阅启用和配置访问控制的属性（IAM Identity Center 文档）。

  许多 IdP（例如：Microsoft Azure Active Directory 和 Okta）都可以使用身份验证方法参考（`amr`）在 SAML 断言中声明将用户的 MFA 状态传递给 IAM Identity Center。用于断言 MFA 状态的声明及其格式因 IdP 而异。有关更多信息，请参阅您的 IdP 的相应文档。

  之后您可以在 IAM Identity Center 中创建权限集策略来确定哪些人可以访问您的 AWS 资源。当您启用 ABAC 并指定属性时，IAM Identity Center 会将经过身份验证的用户的属性值传递到 IAM，以便在策略评估中使用。有关更多信息，请参阅为 ABAC 创建权限策略（IAM Identity Center 文档）。如以下示例所示，您可以使用 `aws:PrincipalTag` 条件键为 MFA 创建访问控制规则。

```
"Condition": {
  "StringLike": { "aws:PrincipalTag/amr": "mfa" }
}
```

管理成员账户

在本节中，您需要邀请您先前存在的账户加入组织，并开始在组织中创建新账户。此过程的一个重要部分是定义用于确定是否需要配置新账户的标准。

本节包含以下任务：

- 邀请您先前存在的账户
- 在 AWS Control Tower 中自定义 VPC 设置
- 定义范围界定标准

邀请您先前存在的账户

在 AWS Organizations 内，您可以邀请贵公司先前存在的账户加入您的新组织。只有组织中的管理账户可以邀请其他账户加入。当受邀账户的管理员接受时，该账户会立即加入组织，组织的管理账户将承担新成员账户产生的所有费用。有关更多信息，请参阅邀请 AWS 账户 加入您的组织和接受或拒绝来自组织的邀请（AWS Organizations 文档）。

> **Note**
>
> 只有当某个账户当前不在其他组织中时，您才能邀请该账户加入组织。如果某个账户是现有组织的成员，则您必须将其从组织中删除。如果某个账户是错误创建的另一个组织的管理账户，则必须删除该组织。

> **Important**
>
> 如果您需要访问先前存在的账户中的任何历史成本或使用情况信息，则可以使用 AWS 成本和使用情况报告 将该信息导出到 Amazon Simple Storage Service（Amazon S3）存储桶。请在接受加入组织的邀请之前执行此操作。在账户加入组织后，您将无法访问该账户的历史数据。有关更多信息，请参阅为成本和使用情况报告设置 Amazon S3 存储桶（AWS 成本和使用情况报告 文档）。

最佳实践

- 我们建议您将先前存在的账户（可能包含生产工作负载）添加到您在 添加组织单位 中创建的工作负载 > Prod 组织单位。
- 默认情况下，组织的管理账户对受邀加入该组织的成员账户没有管理访问权限。如果您希望管理账户具有管理控制权，您必须在成员账户中创建 OrganizationAccountAccessRole IAM 角色，并将权限授予管理账户以担任该角色。有关更多信息，请参阅在受邀成员账户中创建 OrganizationAccountAccessRole（AWS Organizations 文档）。
- 对于您邀请加入该组织的先前存在的账户，请查看针对成员账户的最佳实践（AWS Organizations 文档），并确认该账户遵守这些建议。

在 AWS Control Tower 中自定义 VPC 设置

我们建议您在 AWS Control Tower 中通过 Account Factory 配置新的 AWS 账户。您可以使用 Account Factory，使用 AWS Control Tower 与 Amazon EventBridge 集成，在账户创建后立即在 AWS 账户 中配置资源。

当您设置新 AWS 账户 时，默认虚拟私有云（VPC）会自动配置。但是，当您通过 Account Factory 设置新账户时，AWS Control Tower 会自动配置额外的 VPC。有关更多信息，请参阅 AWS Control Tower 的概述和 VPC（AWS Control Tower 文档）。这意味着，默认情况下，AWS Control Tower 在每个新账户中配置两个默认 VPC。

公司通常希望对其账户中的 VPC 拥有更多控制权。许多人更倾向使用其他服务（例如：AWS CloudFormation、Hashicorp Terraform 或 Pulumi）来设置和管理 VPC。您应自定义 Account Factory 设置，以防止创建由 AWS Control Tower 配置的其他 VPC。有关说明，请参阅配置 Amazon VPC 设置（AWS Control Tower 文档），并应用以下设置：

1. 禁用可通过互联网访问的子网选项。
2. 对于私有子网的最大数量，选择 0。
3. 在创建 VPC 的区域，清除所有区域。
4. 在可用区，选择 3。

最佳实践

- 删除每个新账户中自动配置的默认 VPC。这可以防止用户在未明确创建专用 VPC 的情况下在账户中启动公有 EC2 实例。有关更多信息，请参阅删除默认子网和默认 VPC（Amazon Virtual Private Cloud 文档）。您也可以配置适用于 Terraform 的 AWS Control Tower Account Factory（AFT），自动删除新创建账户中的默认 VPC。
- 将名为 dev-nonprod 的新 AWS 账户 部署到工作负载 > NonProd 组织单位。在您的开发环境中使用此账户。有关说明，请参阅使用 AWS Service Catalog 部署 Account Factory 账户（AWS Control Tower 文档）。

定义范围界定标准

您需要选择贵公司在决定是否配置新 AWS 账户 时将使用的标准。您可以决定为每个业务部门配置账户，也可以决定根据环境（例如生产、测试或 QA）配置账户。每家公司都应对自己的 AWS 账户 规模大小有自己的要求。通常，在决定如何调整账户规模时，您需要评估以下三个因素：

- 平衡服务限额：服务限额是 AWS 账户 内每个 AWS 服务 在资源、操作和项目数量方面的最大值。如果许多工作负载共享同一个账户，而一个工作负载占用了大部分或全部服务限额，则可能会对同一账户中的另一个工作负载产生负面影响。如果是这样，您可能需要将这些工作负载分到不同的账户中。有关更多信息，请参阅 AWS 服务 限额（AWS 一般参考）。
- 成本报告：将工作负载隔离到单独的账户中，方便您在成本和使用情况报告中查看账户级别的成本。当为多个工作负载使用同一个账户时，可以使用标签来帮助管理和识别资源。有关标记的更多信息，请参阅标记 AWS 资源（AWS 一般参考）。
- 控制访问权限：当工作负载共享账户时，您需要考虑如何配置 IAM policy，以限制对账户资源的访问权限，确保用户无法访问不需要的工作负载。作为替代方案，您可以在 IAM Identity Center 中使用多个账户和权限集，管理对个人账户的访问权限。

最佳实践

- 遵循适合您的 AWS Control Tower 登录区的 AWS 多账户策略中的安全最佳实践（AWS Control Tower 文档）。
- 制定有效的标记策略，帮助您识别和管理 AWS 资源。您可使用标签，按用途、业务部门、环境或其他标准对资源进行分类。有关更多信息，请参阅有关标记的最佳实践（AWS 一般参考 文档）。
- 不要让账户负载过多的工作负载。如果工作负载的需求超过服务限额，则可能导致出现性能问题。您可以将相互竞争的工作负载分成不同的 AWS 账户；或者您可以申请增加服务限额。有关更多信息，请参阅请求增加限额（《服务限额》文档）。

管理多账户架构的权限和访问权限

本节包含以下主题：

- 工程文化方面的注意事项
- 创建权限集
- 创建权限边界
- 管理个人的权限

工程文化方面的注意事项

AWS Well-Architected Framework 的支柱之一是卓越运营。团队必须明白运营模式，以及他们在实现业务成果方面所起的作用。当团队知晓自己的职责，能够承担责任，并知道如何做出决策时，才能专注于实现共同的目标。

由于处于早期阶段的公司发展迅速，因此团队中的每个人都扮演着多个角色。这些用户拥有对 AWS 账户 的高权限访问权限的情况并不少见。随着公司的发展，他们通常希望遵循最低权限的原则，并且仅授予用户完成工作所需的权限。为了帮助限制范围，您可以使用 AWS Identity and Access Management Access Analyzer 查看用户或 IAM 角色实际使用了哪些权限，从而方便您移除任何多余的权限。

要决定贵公司中哪些人有权限创建 IAM 角色可能很困难。这通常是提升权限的途经。提升权限是指用户可以扩展自己的权限或访问权限范围。例如，如果用户的权限有限但可以创建新的 IAM 角色，则该用户可以通过创建并担任已应用 `AdministratorAccess` 托管策略的新 IAM 角色来提升其权限。

一些公司将 IAM 角色配置限制为由可信人员组成的集中式团队。这种方法的缺点是，该团队很快会产生瓶颈，因为几乎所有 AWS 服务 都需要一个 IAM 角色才能运行。作为替代方案，您可以使用权限边界仅向开发、测试、启动和管理您的云基础设施的用户授予 IAM 访问权限。有关示例策略，请参阅权限边界示例（GitHub）。

开发运营（DevOps）团队，也称为平台团队，通常需要在多个内部开发团队的自助服务功能和应用程序的运行稳定性之间取得平衡。在工作场所培养一种弘扬自主性、精通能力和目标的工程文化可以帮助激励团队。工程师们希望以自我指导的方式完成工作，而不必依赖他人为自己做事。如果 DevOps 团队能够实施自助服务解决方案，则还可以减少其他人依赖他们完成工作的时间。

创建权限集

您可以在 AWS IAM Identity Center 中使用权限集管理 AWS 账户 访问权限。一个权限集是一个模板，可帮助您将一个或多个 IAM policy 部署到多个 AWS 账户。当您将权限集分配给 AWS 账户 时，IAM Identity Center 会创建一个 IAM 角色，并将您的 IAM policy 附加到该角色。有关更多信息，请参阅创建并管理权限集（IAM Identity Center 文档）。

AWS 建议创建与企业中不同角色对应的权限集。

例如，您可以创建以下权限集：

- 账单权限集
- 开发人员权限集
- 生产权限集

以下权限集是来自 AWS CloudFormation 模板的片段。您不妨使用此代码作为起点，并根据您的业务对其进行自定义。有关 CloudFormation 模板的更多信息，请参阅了解模板基础知识（CloudFormation 文档）。

账单权限集

财务团队使用 BillingAccessPermissionSet 查看 AWS Billing 控制台控制面板和每个账户中的 AWS Cost Explorer。

```
BillingAccessPermissionSet:
  Type: "AWS::SSO::PermissionSet"
  Properties:
    Description: Access to Billing and Cost Explorer
    InstanceArn: !Sub "arn:${AWS::Partition}:sso:::instance/ssoins-instanceId"
    ManagedPolicies:
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/job-function/Billing"
    Name: BillingAccess
    SessionDuration: PT8H
    RelayStateType: https://console.aws.amazon.com/billing/home
```

开发人员权限集

工程团队使用 DeveloperAccessPermissionSet 访问非生产账户。

```
DeveloperAccessPermissionSet:
```

```
  Type: "AWS::SSO::PermissionSet"
  Properties:
    Description: Access to provision resources through CloudFormation
    InlinePolicy: !Sub |-
      {
        "Version": "2012-10-17",
        "Statement": [
          {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:${AWS::Partition}:iam::*:role/CloudFormationRole",
            "Condition": {
              "StringEquals": {
                "aws:ResourceAccount": "${!aws:PrincipalAccount}",
                "iam:PassedToService": "cloudformation.${AWS::URLSuffix}"
              }
            }
          },
          {
            "Effect": "Allow",
            "Action": [
              "cloudformation:ContinueUpdateRollback",
              "cloudformation:CreateChangeSet",
              "cloudformation:CreateStack",
              "cloudformation:DeleteStack",
              "cloudformation:RollbackStack",
              "cloudformation:UpdateStack"
            ],
            "Resource": "arn:${AWS::Partition}:cloudformation:*:*:stack/app/*",
            "Condition": {
              "ArnLike": {
                "cloudformation:RoleArn": "arn:${AWS::Partition}:iam::${!
aws:PrincipalAccount}:role/CloudFormationRole"
              },
              "Null": {
                "cloudformation:ImportResourceTypes": true
              }
            }
          },
          {
            "Effect": "Allow",
            "Action": [
              "cloudformation:CancelUpdateStack",
              "cloudformation:DeleteChangeSet",
```

```
              "cloudformation:DetectStackDrift",
              "cloudformation:DetectStackResourceDrift",
              "cloudformation:ExecuteChangeSet",
              "cloudformation:TagResource",
              "cloudformation:UntagResource",
              "cloudformation:UpdateTerminationProtection"
            ],
            "Resource": "arn:${AWS::Partition}:cloudformation:*:*:stack/app/*"
          },
          {
           "Effect": "Allow",
            "Action": [
              "cloudformation:CreateUploadBucket",
              "cloudformation:ValidateTemplate",
              "cloudformation:EstimateTemplateCost"
            ],
            "Resource": "*"
          }
        ]
      }
    InstanceArn: !Sub "arn:${AWS::Partition}:sso:::instance/ssoins-instanceId"
    ManagedPolicies:
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/AWSServiceCatalogEndUserFullAccess"
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/AWSProtonDeveloperAccess"
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/AWSBillingReadOnlyAccess"
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/AWSSupportAccess"
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/ReadOnlyAccess"
    Name: DeveloperAccess
    SessionDuration: PT8H
```

生产权限集

工程团队使用 ProductionPermissionSet 访问生产账户。此权限集具有有限的、仅限查看的访问权限。

```
ProductionPermissionSet:
  Type: "AWS::SSO::PermissionSet"
  Properties:
    Description: Access to production accounts
    InlinePolicy: !Sub |-
      {
        "Version": "2012-10-17",
        "Statement": [
          {
```

```
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:${AWS::Partition}:iam::*:role/CloudFormationRole",
            "Condition": {
              "StringEquals": {
                "aws:ResourceAccount": "${!aws:PrincipalAccount}",
                "iam:PassedToService": "cloudformation.${AWS::URLSuffix}"
              }
            }
          },
          {
            "Effect": "Allow",
            "Action": "cloudformation:ContinueUpdateRollback",
            "Resource": "arn:${AWS::Partition}:cloudformation:*:*:stack/app/*",
            "Condition": {
              "ArnLike": {
                "cloudformation:RoleArn": "arn:${AWS::Partition}:iam::${!
aws:PrincipalAccount}:role/CloudFormationRole"
              }
            }
          },
          {
            "Effect": "Allow",
            "Action": "cloudformation:CancelUpdateStack",
            "Resource": "arn:${AWS::Partition}:cloudformation:*:*:stack/app/*"
          }
        ]
      }
    InstanceArn: !Sub "arn:${AWS::Partition}:sso:::instance/ssoins-instanceId"
    ManagedPolicies:
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/AWSBillingReadOnlyAccess"
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/AWSSupportAccess"
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/job-function/ViewOnlyAccess"
    Name: ProductionAccess
    SessionDuration: PT2H
```

创建权限边界

部署权限集后，您可以建立权限边界。此权限边界是一种机制，仅向开发、测试、启动和管理您的云基础设施的用户授予 IAM 访问权限。这些用户只能执行策略和权限边界允许的操作。

您可以使用 AWS CloudFormation 模板定义权限边界，然后使用 CloudFormation StackSets 将模板部署到多个账户中。这有助于您通过单一操作在整个组织中建立和维护标准化策略。有关更多信息和说明，请参阅使用 AWS CloudFormation StackSets（CloudFormation 文档）。

以下 CloudFormation 模板预置了一个 IAM 角色，并创建了一个充当权限边界的 IAM policy。您可以使用堆栈集将此模板部署到组织中的所有成员账户。

```
CloudFormationRole:
  Type: "AWS::IAM::Role"
  Properties:
    AssumeRolePolicyDocument:
      Version: "2012-10-17"
      Statement:
        Effect: Allow
        Principal:
          Service: !Sub "cloudformation.${AWS::URLSuffix}"
        Action: "sts:AssumeRole"
        Condition:
          StringEquals:
            "aws:SourceAccount": !Ref "AWS::AccountId"
    Description: !Sub "DO NOT DELETE - Used by CloudFormation. Created by
 CloudFormation ${AWS::StackId}"
    ManagedPolicyArns:
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/AdministratorAccess"
    PermissionsBoundary: !Ref DeveloperBoundary
    RoleName: CloudFormationRole

DeveloperBoundary:
  Type: "AWS::IAM::ManagedPolicy"
  Properties:
    Description: Permission boundary for developers
    ManagedPolicyName: PermissionsBoundary
    PolicyDocument:
      Version: "2012-10-17"
      Statement:
        - Sid: AllowModifyIamRolesWithBoundary
          Effect: Allow
          Action:
            - "iam:AttachRolePolicy"
            - "iam:CreateRole"
            - "iam:DeleteRolePolicy"
            - "iam:DetachRolePolicy"
            - "iam:PutRolePermissionsBoundary"
```

```
            - "iam:PutRolePolicy"
          Resource: !Sub "arn:${AWS::Partition}:iam::${AWS::AccountId}:role/app/*"
          Condition:
            ArnEquals:
              "iam:PermissionsBoundary": !Sub "arn:${AWS::Partition}:iam::
${AWS::AccountId}:policy/PermissionsBoundary"
        - Sid: AllowModifyIamRoles
          Effect: Allow
          Action:
            - "iam:DeleteRole"
            - "iam:TagRole"
            - "iam:UntagRole"
            - "iam:UpdateAssumeRolePolicy"
            - "iam:UpdateRole"
            - "iam:UpdateRoleDescription"
          Resource: !Sub "arn:${AWS::Partition}:iam::${AWS::AccountId}:role/app/*"
        - Sid: OverlyPermissiveAllowedServices
          Effect: Allow
          Action:
            - "lambda:*"
            - "apigateway:*"
            - "events:*"
            - "s3:*"
            - "logs:*"
          Resource: "*"
```

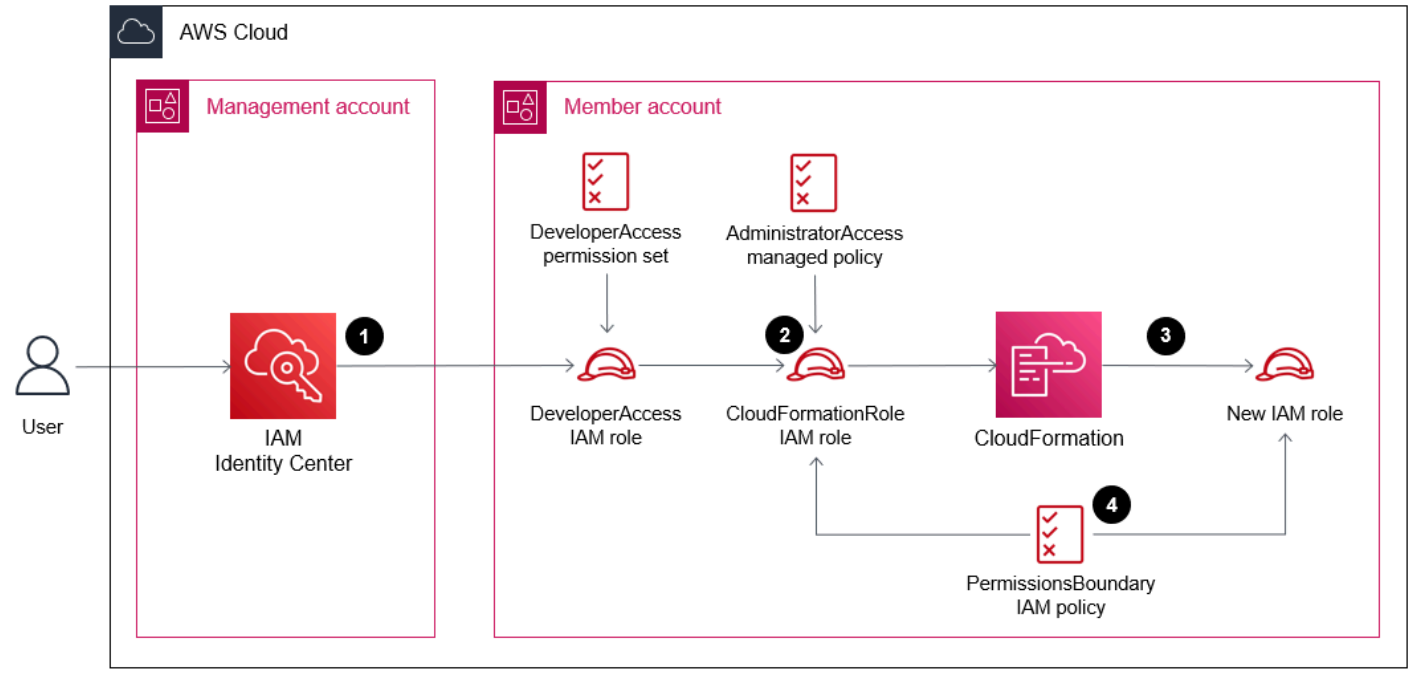
CloudFormationRole 角色、PermissionsBoundary 策略以及 DeveloperAccess 权限集协同工作，以授予以下权限：

- 通过 ReadOnlyAccess AWS 托管策略，用户对大多数 AWS 服务 都具有只读访问权限。
- 用户可以通过 AWSSupportAccess AWS 托管策略访问未解决的支持案例。
- 用户通过 AWSBillingReadOnlyAccess AWS 托管策略对 AWS Billing 控制面板仪表板拥有只读访问权限。
- 用户可以通过 AWSProtonDeveloperAccess AWS 托管策略从 AWS Proton 中预置新环境。
- 用户可以通过 AWSServiceCatalogEndUserFullAccess AWS 托管策略从 Service Catalog 中预置产品。
- 用户可以通过内联策略验证和估算任何 CloudFormation 模板的成本。
- 用户可以通过使用 CloudFormationRole IAM 角色创建、更新或删除任何以 app/ 开头的 CloudFormation 堆栈。

- 用户可以使用 CloudFormation 创建、更新或删除以 app/ 开头的 IAM 角色。PermissionsBoundary IAM policy 可防止用户提升其权限。
- 用户只能通过使用 CloudFormation 预置 AWS Lambda、Amazon EventBridge、Amazon CloudWatch、Amazon Simple Storage Service（Amazon S3）和 Amazon API Gateway 资源。

下图显示了授权用户（例如开发人员）如何使用本指南中介绍的权限集、IAM 角色和权限边界在成员账户中创建新的 IAM 角色：

1. 用户在 IAM Identity Center 中进行身份验证，并承担 DeveloperAccess IAM 角色。
2. 用户启动 `cloudformation:CreateStack` 操作，并承担 CloudFormationRole IAM 角色。
3. 用户启动 `iam:CreateRole` 操作，并使用 CloudFormation 创建新的 IAM 角色。
4. 为新 IAM 角色应用 PermissionsBoundary IAM policy。



CloudFormationRole 角色已附加 AdministratorAccess 托管策略，但由于 PermissionsBoundary IAM policy，CloudFormationRole 角色的有效权限变为等于 PermissionsBoundary 策略。PermissionsBoundary 策略在允许 `iam:CreateRole` 操作时会引用自身，这确保只有在应用权限边界时才能创建角色。

管理个人的权限

您可以使用权限集、权限边界和 CloudFormationRole IAM 角色，限制需要直接分配给各个主体的权限数量。这有助于您随着公司的发展而管理访问权限，并帮助您应用授予最低权限的安全最佳实践。

您也可以使用服务相关角色，它向 AWS 服务授予权限，代表您预置资源。您可以向服务授予权限，而不是向 IAM 主体（用户、用户组或角色）授予权限。例如，用于 AWS Proton 和 AWS Service Catalog 的服务相关角色允许您预置自己的模板、资源和环境，而无需向 IAM 主体分配权限。有关更多信息，请参阅使用 IAM 的 AWS 服务 和使用服务相关角色（IAM 文档）。

另一种最佳实践是限制个人对 AWS Management Console 的访问权限数量。您可以限制对控制台的访问，要求个人使用基础设施即代码（IaC）技术预置资源，例如 AWS CloudFormation、HashiCorp Terraform 或 Pulumi。您可以通过 IaC 管理基础设施，跟踪资源随时间推移而发生的变化，并引入批准变更的机制，例如 GitHub 提取请求。

多账户架构的网络连接

连接 VPC

许多公司在 Amazon Virtual Private Cloud（Amazon VPC）中使用 VPC 对等来连接开发和生产 VPC。您可以使用 VPC 对等连接并使用私有 IP 寻址，在两个 VPC 之间路由流量。连接的 VPC 可以是不同 AWS 账户 的，也可以是不同 AWS 区域的。有关更多信息，请参阅什么是 VPC 对等连接（Amazon VPC 文档）。随着公司的发展和 VPC 数量的增加，维护所有 VPC 之间的对等连接可能会成为维护负担。您可能还会受到每个 VPC 的最大 VPC 对等连接数量的限制。有关更多信息，请参阅 VPC 对等连接限额（Amazon VPC 文档）。

如果您有多个开发、测试和暂存环境，这些环境跨多个托管非生产数据 AWS 账户，则可能需要在所有这些 VPC 之间提供网络连接，但不允许对生产环境进行任何访问。此时可以使用 AWS Transit Gateway 跨多个账户连接多个 VPC。您可以将路由表分开，以防止开发 VPC 通过充当集中式路由器的中转网关与生产 VPC 通信。有关更多信息，请参阅集中式路由器（Transit Gateway 文档）。

Transit Gateway 还支持与其他中转网关进行对等连接，包括位于不同 AWS 账户 或 AWS 区域中的中转网关。由于 Transit Gateway 是一项完全托管式、高度可用的服务，因此您只需为每个区域预置一个中转网关。

有关更多信息和详细的网络架构，请参阅构建可扩展且安全的多 vPC AWS 网络基础架构（AWS 白皮书）。

连接应用程序

如果您需要在同一环境（例如生产）AWS 账户 中不同应用程序之间建立通信，则可以使用以下选项之一：

- 如果您想开放对多个 IP 地址和端口的广泛访问，VPC 对等或 AWS Transit Gateway 可以在网络级别提供连接。
- AWS PrivateLink 在 VPC 的私有子网中创建端点，并将这些端点注册为 Amazon Route 53 Resolver 中的 DNS 条目。通过使用 DNS，应用程序可以解析端点，并连接到注册的服务，而无需在 VPC 中使用 NAT 网关或互联网网关。
- Amazon VPC Lattice 跨多个账户和 VPC 关联服务（例如应用程序），并将它们收集到服务网络中。VPC 中与服务网络关联的客户端可以向与服务网络关联的所有其他服务发送请求，无论他们是否在同一个账户中。VPC Lattice 与 AWS Resource Access Manager (AWS RAM) 集成，因此您可

以与其他账户或通过 AWS Organizations其他账户共享资源。只能将一个 VPC 与一个服务网络相关联。此解决方案不需要使用 VPC 对等或 AWS Transit Gateway 跨账户通信。

网络连接最佳实践

- 创建 AWS 账户 用于集中式联网的。将此账户命名为 n etwork-prod，并将其用于 AWS Transit Gateway Amazon VPC IP 地址管理器 (IPAM)。将此账户添加到 Infrastructure_Prod 组织单位。
- 使用 AWS Resource Access Manager（AWS RAM）与组织其他成员共享中转网关、VPC Lattice 服务网络和 IPAM 池。这样，您组织 AWS 账户 中的任何人都可以与这些服务进行交互。
- 您可以使用 IPAM 池集中管理 IPv4 和 IPv6 地址分配，从而允许最终用户使用 AWS Service Catalog 自行预置 VPC。这可以帮助您适当调整 VPC 的大小，并防止 IP 地址空间重叠。
- 对绑定到互联网的流量使用集中式出口方法，对从互联网进入您环境的流量使用分散式入口方法。有关更多信息，请参阅 集中式出口 和 分散式入口。

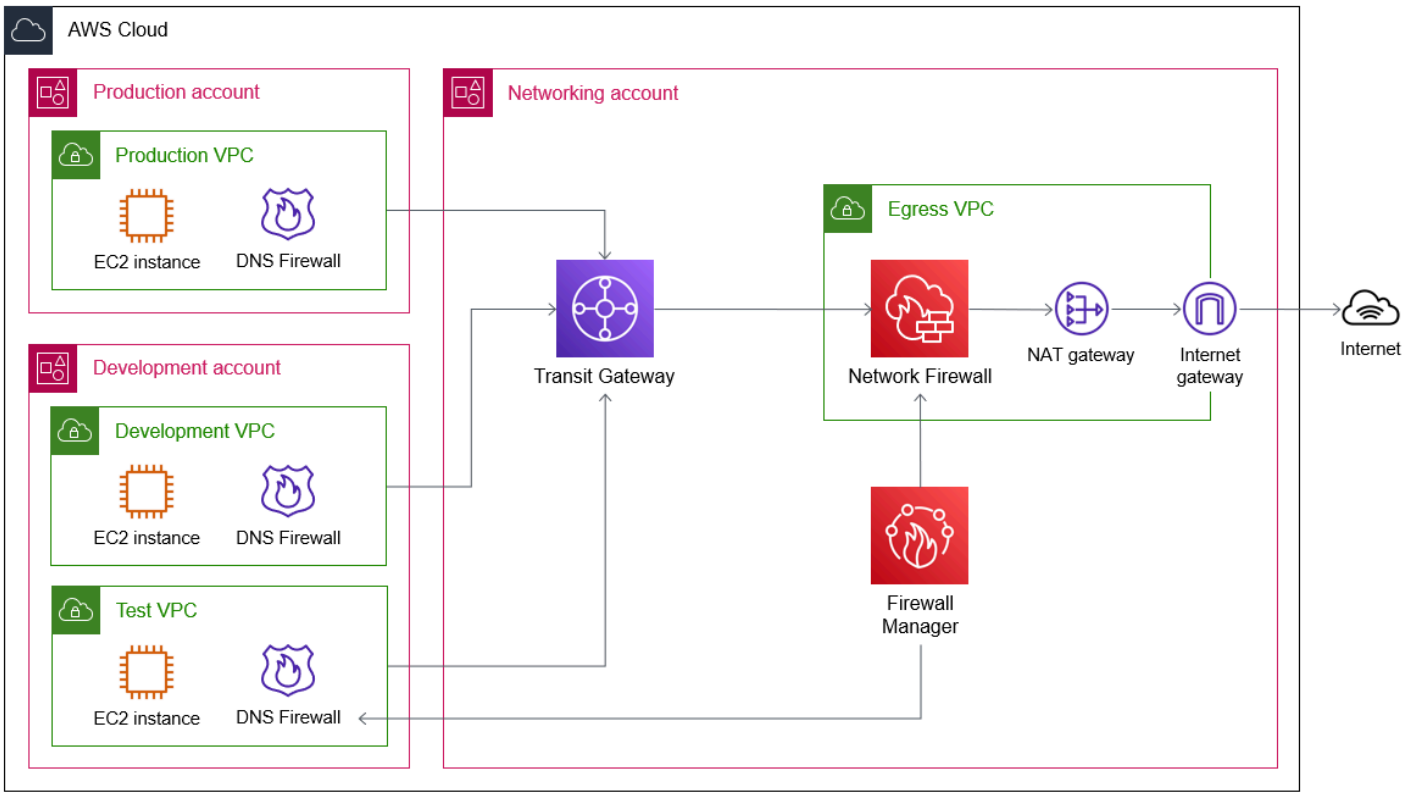
集中式出口

集中式出口是一种对所有发往互联网的网络流量使用单一的通用检查点的原则。在此检查点，您可以仅允许流量进入指定域，或者只允许流量通过指定的端口或协议。集中式出口还可以帮助您降低成本，因为无需在每个 VPC 中部署 NAT 网关即可访问互联网。从安全角度来看，这是有益的，因为它限制了暴露给外部可访问的恶意资源（例如：恶意软件命令和控制（C&C）基础设施）。有关集中出站的更多信息和架构选项，请参阅集中式互联网出口（AWS 白皮书）。

您可以使用 AWS Network Firewall，它是一种有状态的托管式网络防火墙和入侵检测和防护服务，作为出口流量的中心检查点。您可以在专用 VPC 中为出口流量设置此防火墙。Network Firewall 支持有状态规则，您可以使用这些规则来限制对特定域的互联网访问。有关更多信息，请参阅域筛选（Network Firewall 文档）。

您也可以使用 Amazon Route 53 Resolver DNS 防火墙限制特定域的出口流量，主要是为了防止未经授权的数据外泄。在 DNS 防火墙规则中，您可以应用域列表（Route 53 文档），允许或拒绝对指定域的访问。您可以使用 AWS 托管域列表，其中包含与恶意活动或其他潜在威胁相关的域名，也可以创建自定义域列表。您可以创建 DNS 防火墙规则组，然后将其应用于您的 VPC。出站 DNS 请求在 VPC 中通过 Resolver 进行域名解析，DNS 防火墙根据应用于 VPC 的规则组对请求进行筛选。发送到 Resolver 的递归 DNS 请求不会流经中转网关和 Network Firewall 路径。Route 53 Resolver 和 DNS 防火墙应被视为 VPC 之外的独立出口路径。

下图显示了集中式出口的示例架构。在网络通信开始之前，DNS 请求会发送到 Route 53 Resolver，DNS 防火墙允许或拒绝解析用于通信的 IP 地址。发往互联网的流量将路由到集中式网络账户中的中转网关。中转网关将流量转发到 Network Firewall 进行检查。如果防火墙策略允许出口流量，则流量会通过 NAT 网关、互联网网关路由到互联网。您可以使用 AWS Firewall Manager 在多账户基础架构中集中管理 DNS 防火墙规则组和 Network Firewall 策略。



保护出口流量的最佳实践

- 从仅日志记录模式（Route 53 文档）开始。确认合法流量不受影响后，请更改为屏蔽模式。
- 使用网络访问控制列表的AWS Firewall Manager 策略或使用，阻止进入互联网的 DNS 流量 AWS Network Firewall。所有 DNS 查询都应通过 Route 53 解析器进行路由，在那里你可以使用 Amazon GuardDuty （如果启用）对其进行监控，并使用 R oute 53 解析器 DNS 防火墙（如果启用）对其进行过滤。有关更多信息，请参阅解析 VPC 和您的网络之间的 DNS 查询（Route 53 文档）。
- 在 DNS 防火墙和 Network Firewall 中使用 AWS 托管的域列表（Route 53 文档）。
- 考虑屏蔽高风险、未使用的顶级域名，例如：.info、.top、.xyz 或某些国家/地区代码域名。
- 考虑屏蔽高风险、未使用的端口，例如：端口 1389、4444、3333、445、135、139 或 53。
- 首先，您可以使用包含 AWS 托管规则的拒绝列表。然后，你可以随着时间的推移努力实现允许名单模型。例如，与其在允许列表中仅包含严格的完全限定域名的列表，不如先使用一些通配符，例如 *

.example.com。您甚至可以只允许您期望的顶级域名，而屏蔽所有其他域名。然后，随着时间的推移，也要缩小范围。

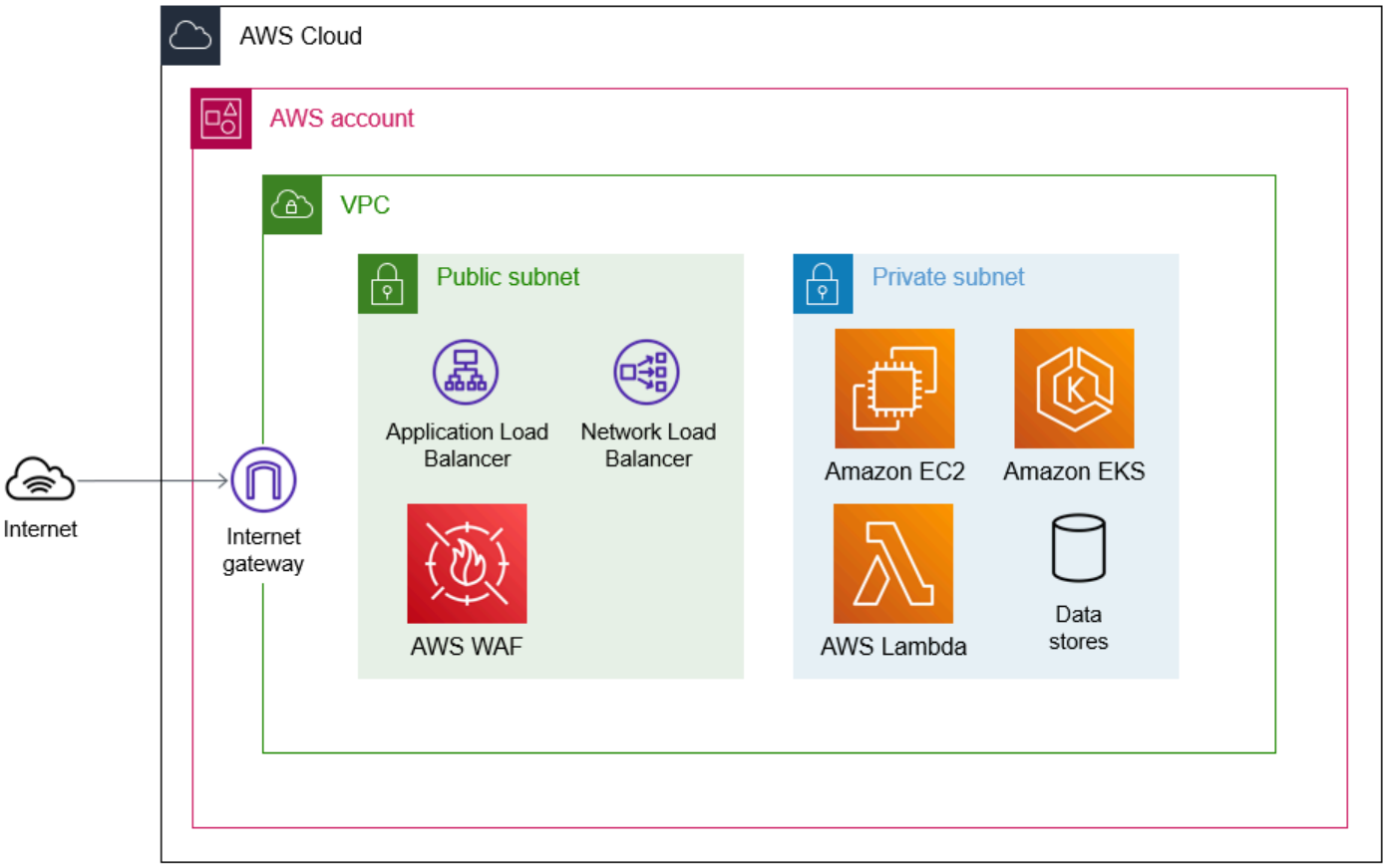
- 使用 Route 53 配置文件（Route 53 文档）在许多 VPC 和不同的 VPC 中应用与 DNS 相关的 Route 53 配置。 AWS 账户
- 定义处理这些最佳做法的异常情况的流程。

分散式入口

分散式入口是一种在个人账户级别定义来自互联网的流量如何到达该账户中的工作负载的原则。在多账户架构中，分散式入口的好处之一是，每个账户都可以使用最合适的入口服务或资源来处理其工作负载，例如应用程序负载均衡器、Amazon API Gateway 或网络负载均衡器。

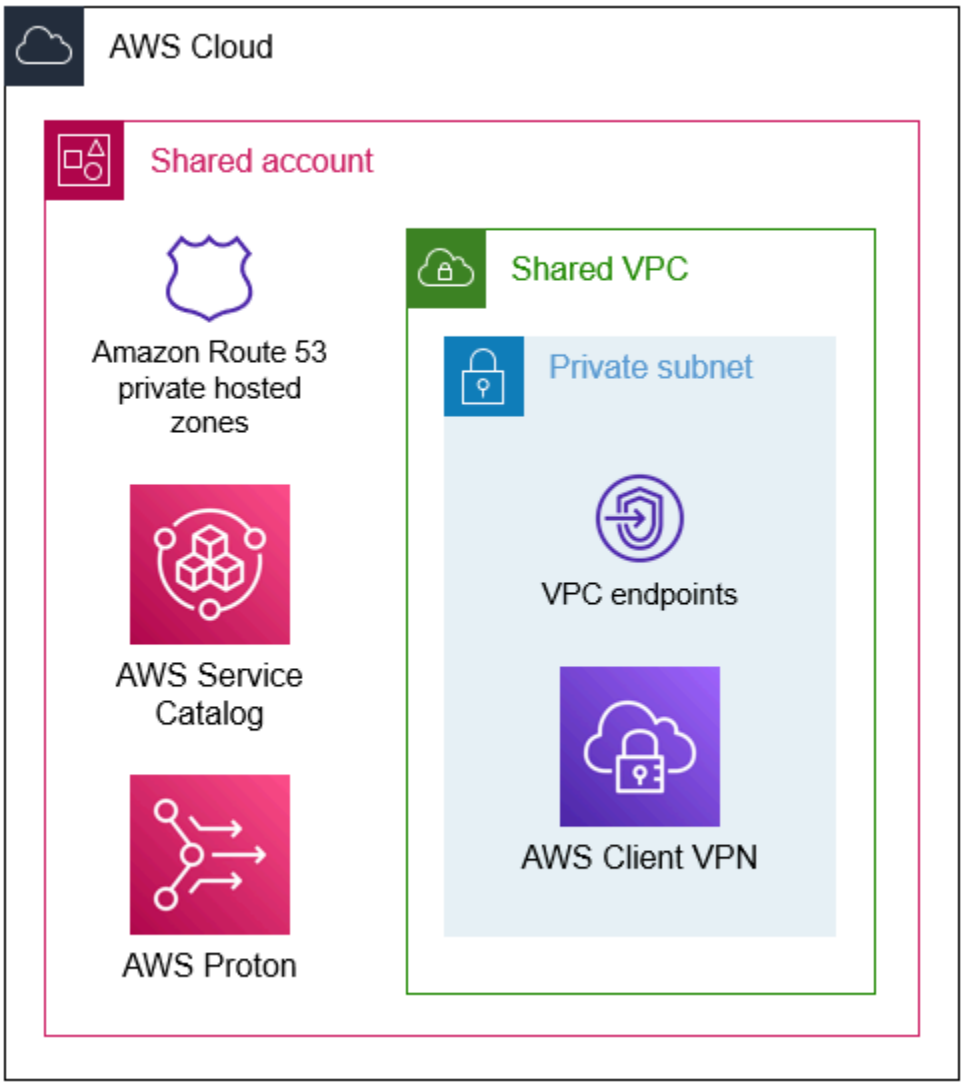
尽管分散式入口意味着您必须单独管理每个账户，但您可以通过 AWS Firewall Manager 集中管理和维护您的配置。Firewall Manager 支持诸如 AWS WAF 和 Amazon VPC 安全组等保护。您可以关联 AWS WAF 到 Application Load Balancer、Amazon CloudFront、API Gateway 或 AWS AppSync。如果您使用的是出口 VPC 和中转网关（如 集中式出口 中所述），则每个分支 VPC 包含公有和私有子网。但是，无需部署 NAT 网关，因为流量会通过网络账户中的出口 VPC 路由。

下图显示了一个个人的示例 AWS 账户 ，该个人拥有一个 VPC，其中包含可访问互联网的工作负载。来自互联网的流量通过互联网网关访问 VPC，然后到达公有子网中托管的负载均衡和安全服务。（公有子网包含一条指向互联网网关的默认路由）。将负载均衡器部署到公有子网中，并附加 AWS WAF 访问控制列表 (ACL)，以帮助防范恶意流量，例如跨站点脚本。将托管应用程序的工作负载部署到私有子网，它们无法直接访问互联网，互联网也无法访问它们。



如果您的组织中有很多 VPC，则可能需要通过在专用和共享 AWS 账户中创建接口 VPC 端点或私有托管区而共享共同的 AWS 服务 。有关更多信息，请参阅AWS 服务 使用接口 VPC 终端节点访问和（AWS PrivateLink 文档）和使用私有托管区域（Route 53 文档）。

下图显示了一个托管 AWS 账户 可在组织内共享的资源的示例。VPC 端点可通过在专用 VPC 中创建，以实现跨账户共享。在创建 VPC 端点时，您可以选择使用 AWS 管理端点的 DNS 条目。要共享端点，请清除此选项，然后在单独的 Route 53 私有托管区（PHZ）中创建 DNS 条目。然后，您可以将 PHZ 与组织中的所有 VPC 关联，以便对 VPC 端点进行集中化 DNS 解析。您还需要确保中转网关路由表中包含共享 VPC 到其他 VPC 的路由。有关更多信息，请参阅集中访问接口 VPC 终端节点（AWS 白皮书）。



共享 AWS 账户 也是托管 AWS Service Catalog 投资组合的好地方。产品组合是您要在其上部署的 IT 服务的集合 AWS，该产品组合包含这些服务的配置信息。您可以在共享账户中创建产品组合，将其共享给组织，然后每个成员账户将产品组合导入自己的区域 Service Catalog 实例。有关更多信息，请参阅与 AWS Organizations共享（Service Catalog 文档）。

同样 AWS Proton，使用，您可以使用共享账户来集中管理您的环境和服务模板，然后设置与组织成员账户的账户连接。有关更多信息，请参阅环境帐户连接（AWS Proton 文档）。

多账户架构的安全事件响应

当你过渡到多人时 AWS 账户，重要的是要保持对组织内可能发生的安全事件的可见性。在 身份管理和访问控制 中，您使用了 AWS Control Tower 来设置登录区。在该设置过程中， AWS 账户 为了安全起见， AWS Control Tower 指定为。您应将安全服务的管理委托给该security-tooling-prod帐户，并使用此帐户集中管理这些服务。

本指南回顾了如何使用以下内容 AWS 服务 来帮助保护您 AWS 账户 和组织：

- Amazon GuardDuty
- Amazon Macie
- AWS Security Hub

Amazon GuardDuty

Amazon GuardDuty 是一项持续的安全监控服务，用于分析数据源，例如 AWS CloudTrail 事件日志。有关支持的数据源的完整列表，请参阅 Amazon 如何 GuardDuty 使用其数据源（GuardDuty 文档）。它使用威胁情报源（例如，恶意 IP 地址和域的列表）和机器学习来标识您 AWS 环境中意外和未经授权的恶意活动。

GuardDuty 与一起使用时 AWS Organizations，组织中的管理账户可以将组织中的任何账户指定为 GuardDuty 委派管理员。委派的 GuardDuty 管理员将成为该地区的管理员帐户。 GuardDuty 在:中自动启用AWS 区域，并且委派的管理员账户有权 GuardDuty 为该区域内组织中的所有账户启用和管理。有关更多信息，请参阅使用管理 GuardDuty 账户 AWS Organizations（GuardDuty 文档）。

GuardDuty 是一项区域服务。这意味着您必须在要监控 GuardDuty 的每个区域中启用。

最佳实践

- GuardDuty 在所有支持中启用 AWS 区域。 GuardDuty 可以生成有关未经授权或异常活动的调查结果，即使在您未积极使用的区域也是如此。的 GuardDuty 定价基于所分析事件的数量。即使在您不操作工作负载的地区，启用 GuardDuty 也是一种有效且具有成本效益的检测工具，可以提醒您注意潜在的恶意活动。有关可用区域的更多信息，请参阅 Amazon GuardDuty 服务终端节点 (AWS 一般参考)。 GuardDuty
- 在每个区域内，委托您的组织管理security-tooling-prod GuardDuty 账户。有关更多信息，请参阅指定 GuardDuty 委派管理员（GuardDuty 文档）。

- 配置 GuardDuty 为在将新 AWS 账户 成员添加到组织时自动注册。有关更多信息，请参阅 AWS Organizations（GuardDuty 文档）管理账户中的步骤 3-自动添加新的组织账户作为成员。

Amazon Macie

Amazon Macie 是一个完全托管式数据安全和数据隐私服务，它使用机器学习和模式匹配来帮助您发现、监控并帮助您保护 Amazon Simple Storage Service（Amazon S3）中的敏感数据。您可以从 Amazon Relational Database Service（Amazon RDS）和 Amazon DynamoDB 的 S3 存储桶导出数据，然后使用 Macie 扫描数据。

当您将 Macie 与一起使用时 AWS Organizations，组织中的管理帐户可以将组织中的任何帐户指定为 Macie 管理员帐户。管理员账户可以为组织中的成员账户启用和管理 Macie，可以访问 Amazon S3 清单数据，还可以为账户运行敏感数据发现任务。有关更多信息，请参阅使用 AWS Organizations管理账户（Macie 文档）。

Macie 是一项区域性服务。这意味着您必须在需要监控的每个区域中启用 Macie，并且 Macie 管理员账户只能管理同一区域内的成员账户。

最佳实践

- 遵循将 Macie 与 AWS Organizations搭配使用时的注意事项和建议（Macie 文档）。
- 在每个区域内，委托该security-tooling-prod账户为您的组织管理 Macie。要集中管理多个 Macie 账户 AWS 区域，管理账户必须登录到组织当前使用或将要使用 Macie 的每个区域，然后在每个区域中指定 Macie 管理员账户。然后，Macie 管理员账户可以在每个区域中配置组织。有关更多信息，请参阅整合和配置组织（Macie 文档）。
- Macie 提供每月免费套餐，可供执行敏感数据发现任务。如果您在 Amazon S3 中存储了敏感数据，请使用 Macie 来分析您的 S3 存储桶，这是每月免费套餐的一部分。如果超过免费套餐，您的账户就会开始产生敏感数据发现费用。

AWS Security Hub

AWS Security Hub为您提供中安全状态的全面视图 AWS。您可以使用它根据安全行业标准和最佳实践检查您的环境。Security Hub 从您的 AWS 账户所有服务（包括 GuardDuty 和 Macie）以及支持的第三方合作伙伴产品中收集安全数据。Security Hub 帮助您分析安全趋势并确定最高优先级的安全问题。Security Hub 提供各种安全标准，您可以启用这些标准来对每个 AWS 账户执行合规性检查。

当您将 Security Hub 与一起使用时 AWS Organizations，组织中的管理帐户可以将组织中的任何帐户指定为 Security Hub 管理员帐户。然后，Security Hub 管理员账户可以启用并管理组织中的其他成员账户。有关更多信息，请参阅使用 AWS Organizations 管理账户（Security Hub 文档）。

Security Hub 是一项区域性服务。这意味着您必须在要分析的每个区域中启用 Security Hub AWS Organizations，并且必须为每个区域定义委派的管理员。

最佳实践

- 遵循先决条件和建议（Security Hub 文档）。
- 在每个区域内，委托该security-tooling-prod账户为您的组织管理 Security Hub。有关更多信息，请参阅指定 Security Hub 管理员账户（Security Hub 文档）。
- 将 Security Hub 配置为在新员工加入组织 AWS 账户 时自动注册。
- 启用 AWS 基础安全最佳实践标准（Security Hub 文档），来检测资源何时偏离安全最佳实践。
- 启用跨区域聚合（Security Hub 文档），以便您可以查看和管理来自单一区域的所有 Security Hub 调查发现。

为多账户架构配置备份

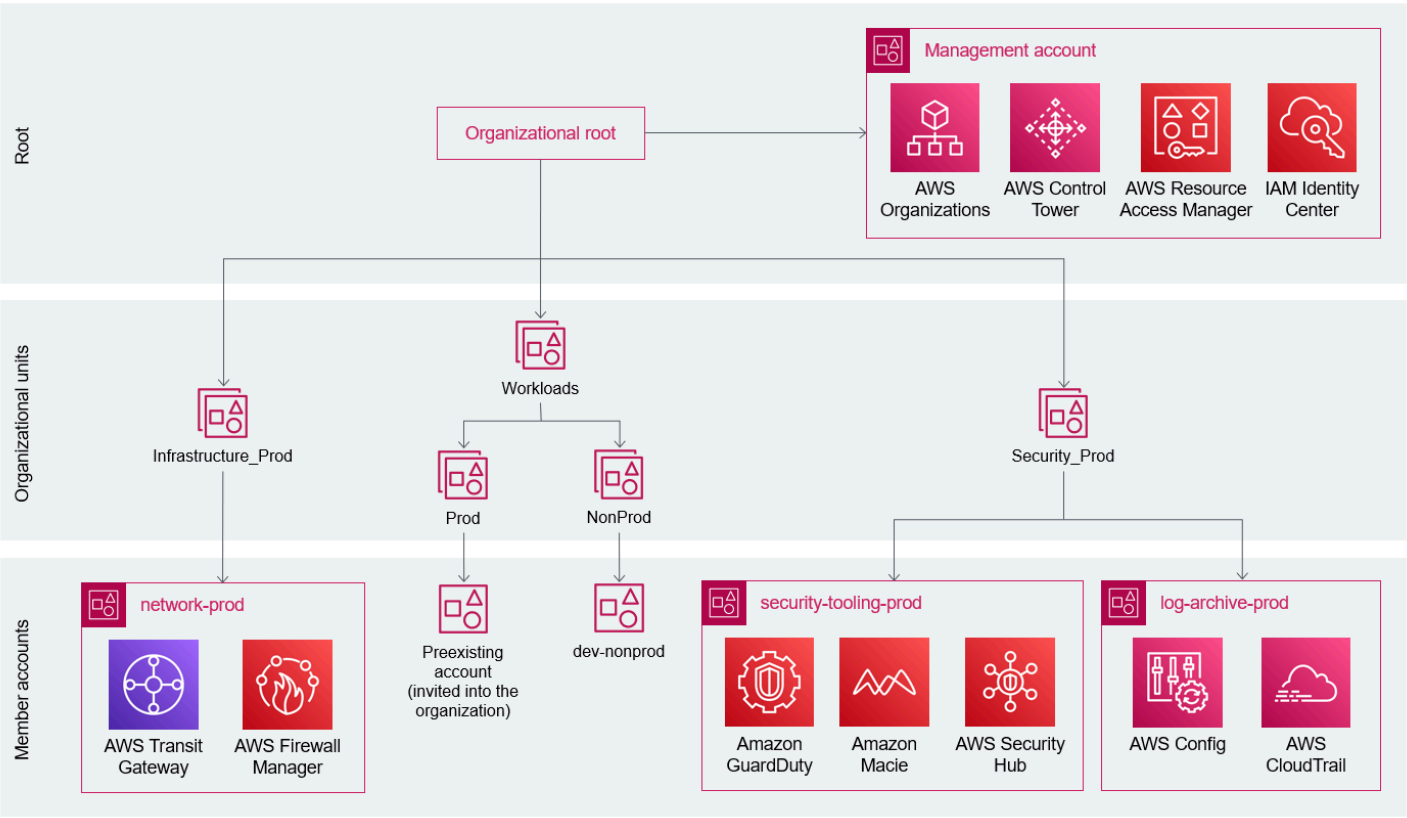
全面的备份战略是公司数据保护计划的重要组成部分，可以承受、恢复和降低因安全事件而可能持续产生的任何影响。备份策略可帮助您将资源标准化，并为组织中的所有账户的资源实施备份策略。在备份策略中，您可以为资源配置和部署备份计划。有关更多信息，请参阅备份策略（AWS Organizations 文档）。有关更多信息，请参阅 AWS 中针对保护备份排名前 10 的安全最佳实践（AWS Prescriptive Guidance）。

过渡到多账户架构时的账户迁移

在 邀请您先前存在的账户，您邀请您之前存在的账户加入工作负载 > 产品组织单位。此账户现在作为您组织的一部分进行管理。

您还在工作负载 > 非产品组织单位中配置了一个新的 dev-nonprod 账户。现在，团队成员应该能够通过 AWS IAM Identity Center 访问相应的账户。移除 AWS Identity and Access Management（IAM）中的任何个人用户账户。

如果您遵循了本指南中的建议，那么贵组织现在具有以下结构。



如果先前存在的账户中正在运行工作负载，则可以根据您在 定义范围界定标准 中确定的标准，将这些工作负载迁移到独立账户。将任何非生产工作负载迁移到新的工作负载 dev-nonprod 组织单位，并将生产工作负载迁移到 network-prod 账户。有关迁移常用 AWS 资源的更多信息，请参阅本指南的以下部分 资源迁移。

在 AWS 账户之间复制或迁移资源

从单账户架构迁移 AWS 账户 到多账户架构后，生产和非生产工作负载通常在先前存在的账户中运行。将这些资源迁移到专用生产和非生产账户或组织单位可以帮助您管理这些工作负载的访问和联网。以下是将公共 AWS 资源迁移到其他资源的一些选项 AWS 账户。

本节重点介绍在 AWS 账户之间复制数据的策略。您应该努力使您的工作负载尽可能保持无状态，从而避免需要在账户之间复制计算资源。通过基础设施即代码（IaC）管理资源也很有好处，这样您就可以在单独的 AWS 账户中重新预置环境。

本节回顾了迁移以下数据资源的选项：

- AWS AppConfig 配置和环境
- AWS Certificate Manager 证书
- 亚马逊配 CloudFront 送
- AWS CodeArtifact 域和存储库
- Amazon DynamoDB 表
- Amazon EBS 交易量
- Amazon EC2 实例或 AMIs
- 亚马逊ECR注册表
- Amazon EFS 文件系统
- 亚马逊 ElastiCache (RedisOSS) 集群
- AWS Elastic Beanstalk 环境
- 弹性 IP 地址
- AWS Lambda 图层
- Amazon Lightsail 实例
- Amazon Neptune 集群
- 亚马逊 OpenSearch 服务域名
- 亚马逊RDS快照
- Amazon Redshift 集群
- Amazon Route 53 域名和托管区
- Amazon S3 存储桶

- 亚马逊 SageMaker 模型
- AWS WAF 网页 ACLs

AWS AppConfig 配置和环境

AWS AppConfig 不支持将其配置直接复制到另一个配置 AWS 账户。但是，最佳做法是将 AWS AppConfig 配置和环境与托管环境 AWS 账户 的配置和环境分开管理。有关更多信息，请参阅使用进行跨账户配置 AWS AppConfig（AWS 博客文章）。

AWS Certificate Manager 证书

您无法直接将 AWS Certificate Manager (ACM) 证书从一个账户导出到另一个账户，因为用于加密证书私钥的 AWS Key Management Service (AWS KMS) 密钥对每个 AWS 区域 和账户都是唯一的。但是，您可以跨多个账户和区域同时预置具有相同域名的多个证书。ACM支持使用DNS（推荐）或电子邮件验证域名所有权。当您使用DNS验证并创建新证书时，ACM会为证书上的每个域生成唯一的CNAME记录。每个账户的CNAME记录都是唯一的，必须在 72 小时内将其添加到 Amazon Route 53 托管区域或DNS提供商，才能正确验证证书。

亚马逊配 CloudFront 送

Amazon CloudFront 不支持将分发从一个迁移 AWS 账户 到另一个分配 AWS 账户。但是，CloudFront 确实支持将备用域名（也称为 a）从一个CNAME发行版迁移到另一个发行版。有关更多信息，请参阅为我的 CloudFront分配设置CNAME别名时如何解决CNAMEAlreadyExists错误（AWS 知识中心）。

AWS CodeArtifact 域和存储库

尽管一个组织可以有多个域，但建议使用一个包含所有已发布构件的生产域。这可以帮助开发团队在整个组织中查找和共享软件包。拥有 AWS 账户 该域的账户可以不同于拥有与该域关联的任何存储库的账户。您可以在存储库之间复制软件包，但它们必须属于同一个域。有关更多信息，请参阅在存储库之间复制软件包（CodeArtifact 文档）。

Amazon DynamoDB 表

您可以使用以下服务之一将 Amazon DynamoDB 表迁移到其他 AWS 账户：

- AWS Backup
- DynamoDB 导入和导出到 Amazon S3
- 亚马逊 S3 和 AWS Glue
- AWS Data Pipeline
- Amazon EMR

有关更多信息，请参阅如何将我的 Amazon DynamoDB 表从 AWS 账户 一个表迁移到另一个表AWS（知识中心）。

Amazon EBS 交易量

您可以为现有的 Amazon Elastic Block Store (AmazonEBS) 卷拍摄快照，与目标账户共享快照，然后在目标账户中创建该卷的副本。这可以有效地将卷从一个账户迁移到另一个账户。有关更多信息，请参阅如何与其他人共享加密的 Amazon EBS 快照或卷 AWS 账户（AWS 知识中心）。

Amazon EC2 实例或 AMIs

无法将现有的亚马逊弹性计算云 (AmazonEC2) 实例或亚马逊系统映像 (AMIs) 直接转移到其他实例 AWS 账户。相反，您可以在源账户AMI中创建自定义，AMI与目标账户共享，从目标账户AMI中共享的EC2实例启动新实例，然后取消注册共享AMI账户。有关更多信息，请参阅如何将 Amazon EC2 实例或其他实例转移AMI到其他实例 AWS 账户（AWS 知识中心）。

亚马逊ECR注册表

Amazon 弹性容器注册表 (AmazonECR) 支持跨账户和跨区域复制。您可以在源注册表上配置复制，在目标注册表上配置注册表权限策略。有关更多信息，请参阅配置跨账户复制（Amazon ECR 文档）和允许源账户的根用户复制所有存储库（Amazon ECR 文档）。

Amazon EFS 文件系统

对于 Amazon Elastic File Syste AWS DataSync m (AmazonEFS)，您可以使用将数据从源文件系统复制到另一个文件系统的目标文件系统 AWS 账户。必须在与源文件系统相同 AWS 区域 且 AWS 账户与源文件系统相同的环境中创建 DataSync 代理。有关更多信息，请参阅将数据从云文件系统传输到另一个云文件系统（DataSync文档）。在不同的 Amazon EFS 文件系统之间进行复制时 AWS 账户，我

们建议您使用NFS（源）到EFS（目标）的传输。有关更多信息和说明，请参阅创建从 Amazon 传输数据的任务 EFS（DataSync 文档）。

亚马逊 ElastiCache (RedisOSS) 集群

您可以使用 Amazon ElastiCache (RedisOSS) 数据库集群的备份将其迁移到其他账户。有关更多信息，请参阅迁移我的 ElastiCache (RedisOSS) 集群的最佳实践（AWS 知识中心）。

AWS Elastic Beanstalk 环境

对于 AWS Elastic Beanstalk，您可以使用保存的配置（Elastic Beanstalk 文档）将环境迁移到其他环境。 AWS 账户有关更多信息，请参阅如何将我的 Elastic Beanstalk 环境 AWS 账户 从一个环境迁移 AWS 账户到AWS 另一个环境（知识中心）。

弹性 IP 地址

您可以在相同地址之间 AWS 账户 传输弹性 IP 地址 AWS 区域。有关更多信息，请参阅传输弹性 IP 地址（Amazon VPC 文档）。

AWS Lambda 图层

默认情况下，您创建的 AWS Lambda 图层对您来说是私有的 AWS 账户。但是，您可以选择与其他人共享图层 AWS 账户 或将其公开。要复制图层，需要将其重新置备到另一个 AWS 账户图层。有关更多信息，请参阅配置层权限（Lambda 文档）。

Amazon Lightsail 实例

您可以创建 Amazon Lightsail 实例的快照，然后将快照导出到亚马逊系统映像 (AMI) 和亚马逊EBS卷的加密快照。有关更多信息，请参阅将亚马逊 Lightsail 快照导出到亚马逊（L EC2 ightsail 文档）。默认情况下，快照使用在 AWS Key Management Service (AWS KMS) 中创建的AWS托管密钥进行加密。但是，这种类型的KMS密钥不能在两者之间共享 AWS 账户。相反，您可以使用客户管理的密钥手动加密副本，该密钥可以从目标账户中使用。AMI有关更多信息，请参阅允许其他账户中的用户使用KMS密钥（AWS KMS 文档）。然后，您可以AMI与目标共享复制的实例， AWS 账户 并从复制的EC2实例中启动 Lightsail 的新实例。AMI有关更多信息，请参阅使用新的启动实例向导启动实例（Amazon EC2 文档）。

Amazon Neptune 集群

您可以将 Amazon Neptune 数据库集群的自动快照复制到另一个 AWS 账户。有关更多信息，请参阅复制数据库（DB）集群快照（Neptune 文档）。

还可以与最多 20 个AWS 账户 共享手动快照，直接从快照中恢复数据库集群。有关更多信息，请参阅共享数据库集群快照（Neptune 文档）。

亚马逊 OpenSearch 服务域名

要在 Amazon S OpenSearch ervice 域之间复制数据，您可以使用 Amazon S3 创建源域的快照，然后将快照还原到其他域中的目标域中 AWS 账户。有关更多信息，请参阅如何从另一个 Amazon S OpenSearch ervice 域名恢复数据 AWS 账户（AWS 知识中心）。

如果两者之间有网络连接 AWS 账户，则还可以使用 Service 中的 OpenSearch 跨集群复制（OpenSearch 服务文档）功能。

亚马逊RDS快照

对于 Amazon Relational Database Service (AmazonRDS)，您可以将数据库实例或集群的手动快照共享给最多 20 个AWS 账户。您可以从共享快照还原数据库实例或数据库集群。有关更多信息，请参阅如何与其他人共享手动的 Amazon RDS 数据库快照或 Aurora 数据库集群快照 AWS 账户（AWS 知识中心）。

您还可以使用 AWS Database Migration Service (AWS DMS) 在不同账户的数据库实例之间配置连续复制。但是，这需要账户之间的网络连接，例如对等互VPC连或传输网关。

Amazon Redshift 集群

要将 Amazon Redshift 集群迁移到其他集群 AWS 账户，请在源账户中创建该集群的手动快照，与目标账户共享该快照 AWS 账户，然后从快照中恢复集群。有关更多信息，请参阅如何将 Amazon Redshift 预配置的集群复制到另一个集群 AWS 账户（AWS 知识中心）。

Amazon Route 53 域名和托管区

您可以在 AWS 账户之间转移 Amazon Route 53 域。有关更多信息，请参阅将域转移到其他 AWS 账户（Route 53 文档）。

您也可以将 Route 53 托管区域迁移到其他托管区域 AWS 账户。有关何时建议或要求执行此操作的更多信息，请参阅将托管区迁移到其他 AWS 账户（Route 53 文档）。迁移托管区时，可以在目标 AWS 账户中重新创建托管区。有关说明，请参阅将托管区迁移到其他 AWS 账户（Route 53 文档）。

Amazon S3 存储桶

您可以使用亚马逊简单存储服务 (Amazon S3) Semple Storage Service 同区域复制在同一区域的 S3 存储桶之间复制对象。AWS有关更多信息，请参阅复制对象（Amazon S3 文档）。请注意以下几点：

- 将副本所有权更改 AWS 账户 为拥有目标存储桶的。有关说明，请参阅更改副本拥有者（Amazon S3 文档）。
- 更新存储桶所有者条件以反映目标存储桶的 AWS 账户 ID。有关更多信息，请参阅使用存储桶拥有者条件验证存储桶所有权（Amazon S3 文档）。
- 自 2023 年 4 月起，已为新创建的存储桶启用存储桶所有者强制设置，从而使存储桶访问控制列表 (ACLs) 和对象ACLs失效。有关更多信息，请参阅 Amazon S3 安全变更即将到来（AWS 博客文章）。
- 可以使用 S3 批量复制（Amazon S3 文档）复制配置复制之前存在的对象。

亚马逊 SageMaker 模型

SageMaker 训练期间，模型存储在 Amazon S3 存储桶中。通过从目标账户授予对 S3 存储桶的访问权限，可以将存储在源账户中的模型部署到目标账户。有关更多信息，请参阅如何将 Amazon SageMaker 模型部署到其他 AWS 账户（AWS 知识中心）。

AWS WAF 网页 ACLs

AWS WAF Web 访问控制列表 (WebACLs) 必须与其关联的资源（例如亚马逊 CloudFront 分配、应用程序负载均衡器、Amazon G API ateway 和 AWS AppSync GraphQLAPIs）位于同一个账户 RESTAPIs中。您可以使用 AWS Firewall Manager 集中管理整个组织内 AWS Organizations 和ACLs 跨地区的 AWS WAF Web。有关更多信息，请参阅开始使用 AWS Firewall ManagerAWS WAF 策略（Firewall Manager 文档）。

过渡到多账户架构时的计费注意事项

如果您使用AWS Organizations过渡到多个AWS 账户，则可以使用整合账单功能（AWS Organizations 文档）。此功能提供一张合并账单，显示多个账户的费用。

以下是向多个账户过渡的最佳计费实践和建议：

- 如果您需要访问历史账单数据，在接受加入组织的邀请之前，请创建成本和使用情况报告（AWS 成本和使用情况报告文档），将账户的历史账单数据导出到 Amazon Simple Storage Service (Amazon S3) 存储桶。在您接受加入组织的邀请后，将无法再访问该账户的历史账单数据。
- 如果您需要合并两个组织（例如合并或收购），则可以使用客户评估 AWS Organizations（AWS解决方案库）来评估每个组织中基于资源的政策，并在合并之前确定任何潜在问题。

结论

如果没有采用策略，从单 AWS 账户 过渡到多个账户一开始可能会让人感到不知所措。通过实施多账户策略，可以解决公司在使用单 AWS 账户 时面临的许多挑战：

- 将生产数据误认为是开发数据：您可以使用 AWS IAM Identity Center 搭配单独的权限集生产和非生产组织单位，授予不同的权限和访问权限。只有具有高权限的用户才能访问生产数据库，并且该访问权限应在有限的时间内进行审计。
- 影响其他业务运营的生产部署：您可以使用多个账户和多个环境将利益相关者分开。例如，您可以在非生产账户中创建一个专用的销售演示环境，这样就可以在不进行演示时规划部署和发布。
- 测试开发工作负载时生产工作负载性能降低：每个 AWS 账户 具有管理每项服务的独立服务限额。通过使用多个账户，您可以限制一个环境影响另一个环境的范围。
- 区分生产成本和开发成本：组织的整合账单将所有费用在 AWS 账户 等级汇总，这样财务团队就可以了解与非生产环境（例如开发、测试和演示环境）相比，生产成本是多少。您还可以使用标签和标记策略来区分账户内的成本。
- 限制对敏感数据的访问：IAM Identity Center 允许您为与特定账户关联的一群人设置单独的访问策略。
- 控制成本：您可以通过在多账户架构中使用服务控制策略（SCP），禁止访问可能会给您的组织带来高昂成本的特定 AWS 服务。SCP 可以拒绝对特定服务的所有访问权限，也可以将服务的使用限制为特定类型，例如限制可以创建的 Amazon Elastic Compute Cloud（Amazon EC2）实例的类型。

贡献者

本文档的贡献者包括：

- 贾斯汀·普洛克，首席解决方案架构师， AWS （主要作者）
- 艾米丽·阿瑙托维奇，首席建筑师 AWS
- Jason DiDomenico，高级解决方案架构师， AWS
- Michael Leighty，高级安全专家解决方案架构师， AWS
- Jesse Lepich，高级安全专家解决方案架构师， AWS
- 首席解决方案架构师 Rodney Lester AWS
- 以色列洛佩兹·莫里亚诺，解决方案架构师， AWS
- 乔治·罗尔斯顿，高级解决方案架构师， AWS
- 亚历克斯·托雷斯，高级解决方案架构师， AWS
- 首席解决方案架构师戴夫·沃克 AWS

资源

AWS Prescriptive Guidance

- AWS Startup Security Baseline（AWS SSB）
- AWS Security Reference Architecture（AWS SRA）
- 保护 AWS 中备份的 10 大最佳实践

AWS 博客文章

- 设置 IAM 用户和 IAM 角色如何帮助您的初创企业保持安全
- 如何让构建者创建 IAM 资源，同时提高组织的安全性和敏捷性

AWS 白皮书

- 使用多个账户整理您的 AWS 环境
- 在 AWS 上建立您的云基础
- 构建可扩展的安全多 VPC AWS 网络基础设施

AWS 代码示例

- 使用 AWS Control Tower 自动设置安全服务（GitHub）

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
集中式出口最佳实践	我们更新了保护出口流量的最佳实践。	2024年5月6日
组织最佳实践	我们更新了在 AWS Organizations中创建组织的最佳实践。	2023 年 12 月 4 日
计费注意事项	我们添加了计费注意事项部分。	2023 年 9 月 20 日
资源迁移、应用程序连接和 Amazon VPC Lattice	我们增加了资源迁移和连接应用程序部分。我们还增加了有关新 AWS 服务 Amazon Virtual Private Cloud（Amazon VPC）的信息。	2023 年 4 月 27 日
账户历史记录和 ABAC	我们修改了 “创建着陆区” 部分，添加了有关如何确保新版 AWS 账户 有使用历史记录的信息，以便您可以将其添加到 AWS Control Tower 着陆区。我们还修改了添加初始用户部分，以增加有关如何使用基于属性的访问权限控制（ABAC），将身份验证方法从外部基于 SAML 的 IdP 传递到 AWS IAM Identity Center的信息。	2023 年 1 月 6 日
出口流量联网	我们修订了集中式出口部分，添加了有关使用 Amazon Route 53 Resolver DNS 防火	2022 年 10 月 13 日

	墙将出口流量限制到特定域名的相关信息。	
出口流量的安全性	我们增加了保护出口流量的最佳实践。	2022 年 10 月 6 日
权限边界	我们改进了权限边界的定义。在资源部分，我们增加了一个新链接，以供获取有关此主题的更多信息。	2022 年 9 月 22 日
初次发布	—	2022 年 9 月 6 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SQL兼容 Amazon Aurora Postgre 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：将您的本地 Oracle 数据库迁移到适用于 Oracle 的 Amazon Relational Database Service (AmazonRDS) 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。

ACID

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

对一组行进行操作并计算该组的单个返回值的SQL函数。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？

人工智能操作 (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 AIOps AWS 迁移策略中使用的更多信息，请参阅操作集成指南。

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、耐久性 () 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，ABAC请参阅 AWS Identity and Access Management (IAM) 文档 AWS中的。

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。您可以在 Amazon Detective 中使用行为图来检查登录尝试失败、可疑API呼叫和类似操作。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

请参阅变更数据捕获。

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CDC用于各种用途，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，创建着陆区、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)

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， 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。您通常使用来自投资组合CMDB中的迁移发现和分析阶段的数据。

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，以自定义您的合规性和安全性检查。您可以使用YAML模板将合规包作为单个实体部署在 AWS 账户 和区域中，也可以跨组织部署。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，其中包含事实表中有关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。有关如何使用带有 strangler fig 模式的域驱动设计的信息，请参阅对旧版 Microsoft 进行现代化改造。ASP NET(ASMX) 通过使用容器和 Amazon API Gateway 逐步提供网络服务。

DR

参见灾难恢复。

漂移检测

跟踪与基线配置的偏差。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

您可以托管在虚拟私有云 (VPC) 中以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。这些账户或委托人可以通过创建接口终端节点私密连接到您的终VPC端节点服务。有关更多信息，请参阅 Amazon Vir tual Private Cloud (AmazonVPC) 文档中的创建终端节点服务。

企业资源规划 (ERP)

一种自动化和管理企业关键业务流程（例如会计和项目管理）的系统。MES

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是通过计算汇总统计数据和创建数据可视化来执行的。

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。这通常表示为数字分数，可以通过各种技术进行计算，例如 Shapley Additive Explantions (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。

精细的访问控制 () 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

一项高级规则，可帮助管理各组织单位的资源、策略和合规性 (OUs)。预防性防护机制会执行策略以确保符合合规性标准。它们通过使用服务控制策略和IAM权限边界来实现。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

将您的源数据库迁移到共享相同数据库引擎的目标数据库（例如，将 Microsoft SQL Server 迁移到 Amazon fo RDS r 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

一种在 90 天内平均使用率CPU和内存使用率介于 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VPC，接受、检查和路由来自应用程序外部的网络连接。AWS 安全参考架构建议设置您的网络帐户，包括入站、出站和检查，VPCs以保护您的应用程序与更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，请参阅构建工业物联网 (IIoT) 数字化转型战略。

检查 VPC

在 AWS 多账户架构中，VPC一种集中式管理VPCs（相同或不同 AWS 区域）、互联网和本地网络之间的网络流量的检查。AWS 安全参考架构建议设置您的网络帐户，包括入站、出站和检查，VPCs以保护您的应用程序与更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，请参阅使用机器学习模型的可解释性AWS。

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为... 提供了基础ITSM。

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。有关将云操作与ITSM工具集成的信息，请参阅操作集成指南。

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) 的实现，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

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，请参阅文档中的应用最低权限权限。IAM

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

一种小型的独立服务，通过明确的定义进行通信APIs，通常由小型的独立团队拥有。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通过定义明确的接口进行通信。APIs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

Migration Acceleration P MAP rog

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包括一种以有条不紊的方式执行遗留迁移的迁移方法，以及一组用于自动化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、开发人员和从事冲刺工作的 DevOps 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：EC2使用 AWS 应用程序迁移服务重新托管向 Amazon 的迁移。

迁移组合评估 (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提供详细的产品组合评估（服务器规模调整、定价、TCO比较、迁移成本分析）以及迁移规划（应用程序数据分析和数据收集、应用程序分组、迁移优先级划分和波浪规划）。所有 AWS 顾问和APN合作伙伴顾问均可免费使用该MPA工具（需要登录）。

迁移准备情况评估 (MRA)

使用以下方法获取有关组织云就绪状态的见解、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 AWS CAF。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，并参阅调动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 提供数据加密、身份验证和授权方案的互操作性标准。

运营层协议 () OLA

一项协议，阐明 IT 职能部门承诺相互提供哪些服务，以支持服务级别协议 () SLA。

操作准备情况审查 (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 ORRwork 中的运营准备情况评估 ()。

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

由此创建的跟踪 AWS CloudTrail ，用于记录组织 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并过渡到新系统和战略。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。

源站访问控制 (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) 的服务器端加密以及对 S3 存储桶的动态PUT和DELETE请求。

源站访问身份 (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。使用时OAI，CloudFront 会创建 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，它提供了更精细和更增强的访问控制。

ORR

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VPC，用于处理从应用程序内部启动的网络连接。AWS 安全参考架构建议设置您的网络帐户，包括入站、出站和检查，VPCs以保护您的应用程序与更广泛的互联网之间的双向接口。

P

权限边界

附加到IAM委托人的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。的示例PII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。该实体通常是 AWS 账户、IAM角色或用户的 root 用户。有关更多信息，请参见IAM文档中的角色承担者术语和概念。

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

一个容器，其中包含有关您希望 Amazon Route 53 如何响应对一个或多个VPCs域名及其子域名的DNS查询的信息。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，在基于微服务的微服务中MES，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

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

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。

负责、负责、咨询、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。

行和列访问控制 (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

SAML2.0

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)，因此用户无需为组织中的IAM所有人创建用户即可登录 AWS Management Console 或调用 AWS API操作。有关SAML基于 2.0 的联合身份验证的更多信息，请参阅文档中的关于SAML基于 2.0 的联合。IAM

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，由接收方 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。SCPs定义防护措施或限制管理员可以委托给用户或角色的操作。您可以使用SCPs允许列表或拒绝列表来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

URL的入口点的 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。

服务级别协议 () 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。

SIEM

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

SPOF

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，请参阅对旧版 Microsoft ASP 进行现代化改造。 NET(ASMX) 通过使用容器和 Amazon API Gateway 逐步提供网络服务。

子网

您的 IP 地址范围VPC。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

一个网络传输中心，可用于将您的网络VPCs和本地网络互连。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凝视

两者之间的连接VPCs，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对等互连。

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

一种对一组以某种方式与当前记录相关的行进行计算的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。

WORM

参见一次写入，多读。

WQF

参见AWS工作负载资格框架。

写一次，读多次 (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

平均值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。