为预签名者建立护栏并进行监控 URLs

AWS 规范性指导

AWS 规范性指导: 为预签名者建立护栏并进行监控 URLs

Table of Contents

建立防护栏并监控预签名 URL

Ryan Baker，亚马逊 Web Services (AWS)

2024 年 7 月（文件历史记录）

安全是所有公司最关心的问题，也是 AWS Well-Architected Framework 的关键支柱。作为一名安全工程师，你需要实施符合组织控制要求的管理护栏。在 Well-A AWS rchitected Framework 中，护栏定义了限制活动的边界。

本指南提供了使用预签名 URL 的背景信息和最佳实践，这些网址用于亚马逊简单存储服务 (Amazon S3) Service 对象。预签名 URL 允许有权访问有效凭证的用户或应用程序生成预先签名的请求，并在定义的到期时间之前被接受。预签名 URL 的一个常见用例是通过共享这些请求来扩展对对象或资源的访问权限。共享的预签名请求由有权执行特定请求的系统或用户生成，然后可以发送给其他系统或用户以扩展执行相同请求的能力。

在本指南中，您将学习：

- 预签名 URL 的概念
- 预签名 URL 的用例
- 推荐和可选的护栏
- 监控选项
- 如何 AWS 服务 使用预签名 URL 的示例

目标受众

本指南适用于负责在 AWS Cloud中实施安全控制的架构师和安全工程师。

目标

作为一名安全工程师，你需要了解解决方案构建者是如何实现安全性的，以及最终用户拥有的访问权限类型。本指南涵盖一种访问类型，即预签名 URL，通常用于 Amazon S3。预签名 URL 为构建者提供了有效桥接身份验证机制的选项。

在 Amazon S3 中，预签名 URL 代表一种独特的请求类别。安全工程师可以监控和管理这些请求，以确保仅在适当和必要的情况下使用这些请求。本指南的目的是帮助安全工程师提供此类高级监督。

阅读本指南后，您应该了解什么是预签名 URL，通常何时使用它，以及使用它的动机。

先决条件

如果您的公司尚未按照在 AWS 上实施安全控制指南中所述定义安全策略、控制目标或标准，我们建议您在继续阅读本指南之前完成这些监管任务。

在开始之前，您还应该熟悉控制和监控方面的推荐和可选最佳实践。有关更多信息，请参阅：

- 服务控制策略（AWS Organizations 文档）
- 亚马逊 S3 的存储桶策略（亚马逊 S3 文档）
- 使用服务器访问日志记录请求（Amazon S3 文档）
- 使用 AWS CloudTrail（亚马逊 S3 文档）记录亚马逊 S3 API 调用

预签名 URL 概述

预签名网址是一种由 AWS Identity and Access Management (IAM) 服务识别的 HTTP 请求。这种类型的请求与所有其他 AWS 请求的区别在于 X-Amz-Ex pires 查询参数。与其他经过身份验证的请求一样，预签名 URL 请求也包含签名。对于预签名 URL 请求，此签名将传入。`X-Amz-Signature`签名使用签名版本 4 加密操作对所有其他请求参数进行编码。

> **注意**
>
> - Signature 版本 2 目前正在被弃用，但某些 AWS 区域版本仍支持该版本。本指南适用于签名版本 4 签名。
> - 接收服务可以处理未签名的标头，但根据最佳实践，对该选项的支持有限且有针对性。除非另有说明，否则假设所有标头都必须经过签名才能被接受。

该`X-Amz-Expires`参数允许将签名视为有效，但与编码的日期时间偏差更大。 签名有效性的其他方面仍在评估中。 签名凭证（如果是临时证书）在处理签名时不得过期。 签名证书必须附加到在处理时拥有足够授权的 IAM 委托人。

预签名 URL 是预签名请求的子集

预签名 URL 并不是将来签署请求的唯一方法。Amazon S3 还支持 POST 请求，这些请求通常也是预先签名的。 预签名的 POST 签名允许上传符合已签名政策且该政策中包含有效期的上传。

请求的签名可能是 future 日期，尽管这种情况并不常见。 只要底层凭证有效，签名算法就不会禁止将来的约会。 但是，这些请求要等到有效的计时窗口才能成功处理，这使得对于大多数用例来说，future dating 是不切实际的。

预签名请求允许什么？

预签名的请求只能允许用于签署请求的凭据所允许的操作。如果凭证隐式或显式拒绝预签名请求指定的操作，则预签名请求在发送时将被拒绝。这适用于以下情况：

- 与凭证关联的会话策略
- 与与证书关联的委托人关联的策略
- 影响会话或委托人的资源策略
- 影响会话或主体的服务控制策略

使用预签名请求的动机

作为一名安全工程师，您应该了解促使解决方案构建者使用预签名 URL 的原因。 了解什么是必要的，哪些是可选的，将有助于你与解决方案构建者沟通。动机可能包括以下几点：

- 支持非 IAM 身份验证机制，同时受益于 Amazon S3 的可扩展性。核心动机是直接与 Amazon S3 通信，以便从该服务提供的内置可扩展性中受益。如果没有这种直接通信，解决方案就需要支持重新传输传入的字节PutObject和GetObject调用的负载。根据总负载，此要求增加了解决方案构建者可能希望避免的扩展挑战。

  其他直接与 Amazon S3 通信的方式，例如在 AWS Security Token Service (AWS STS) 中使用临时凭证或在 URL 之外使用签名版本 4 签名，可能不适合您的用例。Amazon S3 通过 AWS 证书识别用户，而预签名的请求则假定通过证书以外的 AWS 机制进行身份识别。通过预签名的请求，可以弥合这种差异，同时保持数据的直接通信。
- 受益于浏览器对网址的本机理解。浏览器可以理解 URL，而 AWS STS 凭据和签名版本 4 的签名却无法理解。这在与基于浏览器的解决方案集成时非常有用。替代解决方案需要更多的代码，将占用更多内存来存储大文件，恶意软件和病毒扫描程序等扩展程序可能会以不同的方式对待。

与临时 AWS STS 证书的比较

临时证书与预签名请求类似。 它们都过期，允许限制访问范围，并且通常用于将非 IAM 证书与需要 AWS 证书的使用联系起来。

您可以将临时 AWS STS 凭证的范围严格限定为单个 S3 对象和操作，但这可能会导致扩展方面的挑战，因为 AWS STS API 有限制。（有关更多信息，请参阅 AWS re: Post AWS STS网站上的 “如何解决 IAM 的 API 限制或 “超出速率” 错误的文章。）此外，生成的每个凭证都需要一个 AWS STS API 调用，这会增加延迟和可能影响弹性的新依赖关系。 临时 AWS STS 凭证的最短到期时间也为 15 分钟，而预签名的请求可以支持更短的持续时间。（如果条件合适，60 秒是可行的。）

与仅限签名的解决方案的比较

预签名请求中唯一固有的秘密部分是其签名版本 4 签名。 如果客户知道请求的其他详细信息并且获得了与这些详细信息相匹配的有效签名，则它可以发送有效的请求。如果没有有效的签名，则不能。

预签名 URL 和仅限签名的解决方案在密码学上是相似的。但是，仅限签名的解决方案具有实际优势，例如能够使用 HTTP 标头而不是查询字符串参数来传输签名（请参阅日志交互和缓解措施部分）。 管理员还应考虑到，查询字符串通常被视为元数据，而标头则不太常被当作元数据对待。

另一方面， AWS SDK 对直接生成和使用签名的支持较少。构建仅限签名的解决方案需要更多的自定义代码。从实际角度来看，为了安全起见，使用库代替自定义代码是一种一般的最佳做法，因此仅限签名的解决方案的代码需要额外的审查。

仅限签名的解决方案不使用`X-Amz-Expires`查询字符串，也没有提供明确的有效期。IAM 管理没有明确到期时间的签名的隐式有效期。这些隐含的时期并未公布。它们通常不会更改，但是在管理时考虑到了安全性，因此您不应该依赖有效期。 在明确控制到期日期和让 IAM 管理到期日之间需要权衡。

作为管理员，您可能更喜欢仅限签名的解决方案。但是，从实际意义上讲，您需要支持已构建的解决方案。

识别预签名的请求

识别使用预签名 URL 的请求

Amazon S3 提供了两种用于在请求级别监控使用情况的内置机制：Amazon S3 服务器访问日志和 AWS CloudTrail 数据事件。 这两种机制都可以识别预签名 URL 的使用情况。

要筛选日志以了解预签名 URL 的使用情况，您可以使用身份验证类型。有关服务器访问日志，请查看 “身份验证类型” 字段，在 Amazon Athena 表中定义该字段时，该字段通常命名为 authty pe。对于 CloudTrail，AuthenticationMethod在`additionalEventData`实地考察。在这两种情况下，使用预签名 URL 的请求的字段值均为`QueryString`，而`AuthHeader`大多数其他请求的字段值均为。

`QueryString`用法并不总是与预签名 URL 相关联。要将搜索限制为仅使用预签名 URL，请查找包含查询字符串参数`X-Amz-Expires`的请求。对于服务器访问日志，请检查 Request-URI 并查找查询字符串中`X-Amz-Expires`包含参数的请求。 对于 CloudTrail，检查`requestParameters`元素中是否有`X-Amz-Expires`元素。

```
{"Records": [{…, "requestParameters": {…, "X-Amz-Expires": "300"}}, …]}
```

以下 Athena 查询将应用此过滤器：

```
SELECT * FROM {athena-table} WHERE
  authtype = 'QueryString' AND
  request_uri LIKE '%X-Amz-Expires=%';
```

对于 AWS CloudTrail Lake，以下查询将应用此过滤器：

```
SELECT * FROM {data-store-event-id} WHERE
  additionalEventData['AuthenticationMethod'] = 'QueryString' AND
  requestParameters['X-Amz-Expires'] IS NOT NULL
```

识别其他类型的预签名请求

在 Amazon S3 服务器访问日志中`HtmlForm`，POST 请求还具有唯一的身份验证类型，以及 CloudTrail。 这种身份验证类型不太常见，因此在您的环境中可能找不到这些请求。

以下 Athena 查询将过滤器应用于：`HtmlForm`

```
SELECT * FROM {athena-table} WHERE
  authtype = 'HtmlForm';
```

对于 CloudTrail Lake，以下查询将应用过滤器：

```
SELECT * FROM {data-store-event-id} WHERE
  additionalEventData['AuthenticationMethod'] = 'HtmlForm'
```

识别请求模式

您可以使用上一节中讨论的技术来查找预签名的请求。但是，为了使这些数据有用，你需要找到模式。您的查询的简单TOP 10结果可能会提供见解，但如果这还不够，请使用下表中的分组选项。

分组选项	服务器访问日志	CloudTrail湖	描述
用户代理	`GROUP BY useragent`	`GROUP BY userAgent`	此分组选项可帮助您找到请求的来源和目的。用户代理由用户提供，作为身份验证或授权机制不可靠。但是，如果你正在寻找模式，它可能会揭示很多信息，因为大多数客户使用的是至少部分人类可读的唯一字符串。
请求者	`GROUP BY requester`	`GROUP BY userIdentity['arn']`	此分组选项有助于查找签署请求的 IAM 委托人。如果您的目标是阻止这些请求或为现有请求创建例外，则这些查询可为此目的提供足够的信息。当您按照 IAM 最佳实践使用角色时，该角色会有一个明确标识

分组选项	服务器访问日志	CloudTrail湖	描述
			的所有者，您可以使用该信息来了解更多信息。

分组选项	服务器访问日志	CloudTrail湖	描述
来源 IP 地址	`GROUP BY remoteip`	`GROUP BY sourceIPAddress`	此选项按到达 Amazon S3 之前的最后一个网络转换跳点进行分组。 • 如果流量通过 NAT 网关，则这将是 NAT 网关地址。 • 如果流量通过互联网网关，则这将是将流量发送到互联网网关的公有 IP 地址。 • 如果流量来自外部 AWS，则这将是与来源关联的公共互联网地址。 • 如果它通过网关虚拟私有云 (VPC) 终端节点，则这将是 VPC 中实例的 IP 地址。 • 如果它通过公共虚拟接口 (VIF)，则这将是请求者或任何中介（例如代理服务器或防火墙）仅暴露其 IP 地址的本地 IP。

分组选项	服务器访问日志	CloudTrail湖	描述
			• 如果它通过接口 VPC 终端节点，则可能是 VPC 中实例的 IP 地址。它也可以是来自其他 VPC 或本地网络的 IP 地址。与公共 VIF 一样，这可能是任何中介的 IP 地址。 如果您的目标是实施网络控制，则这些数据非常有用。您可能需要将此选项与诸如`endpoint`（用于服务器访问日志）或`vpcEndpointId`（对于 CloudTrail Lake）之类的数据结合使用以明确来源，因为不同的网络可能会重复私有 IP 地址。
S3 存储桶名称	`GROUP BY bucket_name`	`GROUP BY requestParameters['bucketName']`	此分组选项有助于查找已收到请求的存储桶。这可以帮助您确定是否需要例外。

使用预签名请求的最佳实践

本节讨论安全工程师应考虑的使用预签名请求的最佳实践。指导方针包括：

- 基础最佳实践，即每个组织都应遵循的实践。
- 额外的护栏，这是你应该考虑的做法，但可能会决定部分实施或有例外情况实施。它们旨在提供额外的控制和深度防御，但应与整体复杂性保持平衡。
- 记录互动，这可能是由分担责任模式中属于您或您的客户责任一部分的设备或服务引起的。本节包括限制可通过日志访问的信息的预防措施。

基础最佳实践

有效控制其他 AWS API 请求的一般最佳做法也适用于预签名请求。本节回顾了两种最相关的做法：最低权限和数据边界。这些做法创造了其他实践所扩展的控制深度。

应用最小权限原则

限制使用预签名请求的第一步是总体上限制对 Amazon S3 的访问。预签名 URL 无法提供对未授予为预签名 URL 生成签名的委托人的资源的访问权限。它也不能以未授予该委托人的方式提供对资源的访问权限。因此，应用最佳实践来授予这些校长最少的特权是一种有效的保护措施。

创建预签名 URL 的过程是一种基于已发布的签名生成标准（签名版本 4）的算法操作。因此，不可能限制预签名的 URLs生成。但是，为了保持相关性，预签名 URL 必须有效并提供对资源的访问权限，因此预签名 URL 的有效性也是一个有效的保护措施。

有关最低权限的更多信息，请参阅 Well-Architecte AWS d Framework 的 “安全” 支柱中的授予最低权限访问权限。

实现数据边界

最低权限的扩展是维护与组织需求一致的数据边界。预签名 URLs与数据边界兼容。 与其他请求一样，预签名 URL 请求的有效性是在请求时评估的。如果网络、资源、角色会话和主体的属性发生变化，则在接收请求时使用接收请求的方法对其进行评估。

例如，假设在亚马逊 Elastic Kubernetes Service（Amazon EKS）容器中运行的服务签署了请求。该请求随后由连接到互联网的用户的个人计算机系统发送。在本例中，aws: SourceIp 条件评估的是来自用户个人系统的请求的可见公有 IP 地址，而不是 Amazon EKS 容器中服务的 IP 地址。

同样，如果委托人或资源的标签在发送请求之前发生了变化，则通过 aws: /tag-key 和 aws: /tag-ke PrincipalTagy 和 aws: /tag-key 条件将更新后的值（不是原始值）应用于请求。ResourceTag

额外的护栏

当解决方案构建者和用户适当地使用预签名的请求时，它们为用户提供了一种安全的数据访问机制。此外，生成预签名请求的功能并不能为委托人提供他们尚未拥有的访问权限。

在这种情况下，是否需要额外的控制措施？ 采取额外控制措施的理由不是基于拒绝访问的需求，而是为了提供监控、批准使用情况和设定界限以及降低用户错误风险的能力。通过这种方式，您可以帮助确保使用是适当和必要的。

以下护栏可帮助您实现这一目标。在启用这些控件之前，您可能需要通过识别预签名的请求来确定现有使用情况。这种识别可以帮助您为护栏对现有使用情况的影响做好准备，或者在需要时计划例外情况。

s3: SignatureAge 的护栏

预签名请求的一个决定性特征是它们描述了过期时间。请求的签名包含日期。对于预签名，此日期作为`X-Amz-Date`查询字符串参数传输 URLs，对于预签名 POST，则作为日期或 x-amz-date标题传输。

Amazon S3 提供了一个名为 s3: SignatureAge 的条件密钥，您可以使用它来限制从签名日期到请求的有效到期之间的最长时间。这种情况永远不会延长有效期，但可以缩短有效期。

在以下策略中，`s3:signatureAge`条件键将预签名请求的有效期限制为 15 分钟。以下示例均使用 15 分钟将有效期限制在与标准签名支持的类似时间范围内。

该策略的第二条声明拒绝任何签名版本 2 的访问权限。此版本的签名协议已被弃用，但某些 AWS 区域版本仍受支持。我们建议您在将其完全弃用之前明确屏蔽它。

您可以将以下策略应用为 AWS Organizations 服务控制策略 (SCP)。只要签名生成和使用之间的时间少于 15 分钟，用户仍然可以使用预签名请求并部署依赖于这些请求的解决方案。根据实现的不同，此限制可能不会产生任何影响，也可能导致解决方案无法使用，或者可能导致偶尔出现故障，可以重试。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyPresignedOver15Minutes",
      "Effect": "Deny",
      "Action": "s3:*",
```

```
      "Resource": "*",
      "Condition": {
        "NumericGreaterThan": {
          "s3:signatureAge": "900000"
        }
      }
    },
    {
      "Sid": "DenySignatureVersion2",
      "Effect": "Deny",
      "Action": "s3:*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
           "s3:signatureversion": "AWS"
        }
      }
    }
  ]
}
```

异常

如果解决方案需要更长的时间才能到期，因此受到上述政策的影响，我们建议您提供一种批准例外情况的方法。为避免枚举 SCP 中的异常，请使用 a ws: PrincipalTag，如以下策略所示，以可扩展的方式管理异常。其他 AWS 示例，例如 AWS 数据边界策略示例，则使用此策略。

如果您通过使用实现异常策略aws:PrincipalTag，则必须控制对委托人设置标签的访问权限。这种类型的标签可以直接来自委托人，也可以由 SCP 控制，如控制可以设置哪些标签值的示例。这种类型的标签也可以来自会话标签，这些标签由身份提供商 (IdP) 设置或在使用时设置。 AWS STS控制访问权限aws:PrincipalTag是一个复杂的话题。但是，具有使用基于属性的访问控制 (ABAC) 经验的组织将具有相应的经验和控制能力，可以aws:PrincipalTag针对此用例进行适当的使用。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyPresignedOver15Minutes",
      "Effect": "Deny",
      "Action": "s3:*",
      "Resource": "*",
      "Condition": {
```

```
        "NumericGreaterThan": {
          "s3:signatureAge": "900000"
        },
--- Example exception ---
        "StringNotEquals": {
          "aws:PrincipalTag/long-presigned-allowed": "true"
        }
--- Example exception end ---
      }
    }
  ]
}
```

存储桶策略

您可以使用策略将存储桶策略应用于所有或选定的存储桶，如下例所示。与 SCP 不同，存储桶策略还针对服务委托人的使用情况。附录 A 没有记录预签名请求的任何预期服务主体使用情况，但是如果您想实施控制以证明该限制，则以下策略将提供该控制权。此外，与 SCP 不同，存储桶策略可以应用于管理账户中的委托人。基于 ABAC 的异常在存储桶策略中的作用方式与 SCP 相同。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyPresignedOver15Minutes",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::{bucket-name}/*",
      "Condition": {
        "NumericGreaterThan": {
          "s3:signatureAge": "900000"
        },
--- Example exception ---
        "StringNotEquals": {
          "aws:PrincipalTag/long-presigned-allowed": "true"
        }
--- Example exception end ---
      }
    }
  ]
}
```

s3: authType 的护栏

预签名 URLs 使用查询字符串身份验证，预签名 POSTs 始终使用 P OST 身份验证。Amazon S3 支持通过 s3: authType 条件密钥根据身份验证类型拒绝请求。 REST-QUERY-STRING是查询字符串的s3:authType值，POST也是 POST 的s3:authType值。

您可以作为 SCP 应用以下策略。该策略用于仅s3:authType允许基于标头的身份验证。它还配置了一种向单个用户或角色提供例外情况的方法。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyNonHeaderAuth",
      "Effect": "Deny",
      "Action": "s3:*",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "s3:authType": "REST-HEADER",
          "aws:PrincipalTag/non-header-auth-allowed": "true"
        }
      }
    }
  ]
}
```

根据身份验证类型拒绝请求会影响使用被拒绝身份验证类型的任何解决方案或功能。例如，拒绝REST-QUERY-STRING会阻止用户从 Amazon S3 控制台进行上传或下载。如果您希望用户使用 Amazon S3 控制台，请不要使用此护栏，也不要将用户作为例外。另一方面，如果您不希望用户使用 Amazon S3 控制台，则可以拒绝REST-QUERY-STRING用户使用。

也许您已经拒绝用户直接访问 Amazon S3 资源。在这种情况下，身份验证类型的护栏是多余的。但是，s3:authType拒绝语句提供了 defense-in-depth实用性，因为拒绝直接访问的实现通常跨越许多控制语句，有些则有例外。

用于工作负载的角色通常不需要访问查询字符串或POST身份验证。支持旨在使用预签名请求的服务的角色除外。您可以为这些角色创建特定的例外情况。

您还可以使用诸如以下的策略将存储桶策略应用于所有或选定的存储桶：

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyNonHeaderAuth",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::{bucket-name}/*",
      "Condition": {
        "StringNotEquals": {
          "s3:authType": "REST-HEADER",
          "aws:PrincipalTag/non-header-auth-allowed": "true"
        }
      }
    }
  ]
}
```

此存储桶策略的效果是拒绝使用CopyObject和UploadPartCopy APIs 制作跨区域副本。Amazon S3 复制不会受到影响，因为它不依赖这些 APIs。

如果您想使用诸如上述策略之类的存储桶策略，但仍支持跨区域CopyObject或 UploadPartCopyAPI，请添加`aws:ViaAWSService`类似于以下内容的条件：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyNonHeaderAuth",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::{bucket-name}/*",
      "Condition": {
        "StringNotEquals": {
          "s3:authType": "REST-HEADER",
          "aws:PrincipalTag/non-header-auth-allowed": "true"
        },
        "Bool": {
          "aws:ViaAWSService": "false"
        },
      }
    }
```

```
  ]
}
```

将预先签名的护栏和其他护栏的例外情况结合起来

如果您不打算对您的用户和角色普遍使用护栏，则可能需要将其应用于其他常见护栏的例外情况，这样这些例外就不支持预签名的请求。

如果您有网络限制，但允许外部合作伙伴例外情况或特殊用例，则应在应用这些例外情况时屏蔽查询字符串或POST身份验证，除非明确标识为必填项。

s3: SignatureAge 的限制

管理员会发现，s3:signatureAge更全面地了解其含义很有用。每个已签署的请求都包括X-Amz-Date，它应注明当前时间。此值由客户端和请求签名者填写。 AWS 拒绝它认为时间无效的请求。但是，签名者可以在 future 的时间内提前生成签名。如果请求提前发送得太早，Amazon S3 会拒绝指定未来时间的请求。但是，如果请求直到签名后才发送，则签名可能会更早生成，然后再发送。

s3:signatureAge仅对预签名X-Amz-Date请求限制签名的最大年限。 超过指定年龄的申请将被拒绝，即使保单到期X-Amz-Expires或POST保单本来会宣布其有效。 s3:signatureAge不会更改不包含明确到期日期的请求的有效期。它也无法控制客户端用于签名的值。X-Amz-Date

如果系统时钟错误，或者客户故意将日期设置为未来日期，则签名时间可能不是生成签名的时间。 这限制了解决方案s3:signatureAge可以控制的程度。使用生成签名的当前时间的解决方案会受到预期的限制：签名在中指定的毫秒数内保持有效。s3:signatureAge 不使用当前时间的解决方案会有不同的限制。一个限制是，用于签署签名的证书必须仍然有效。作为管理员，您可以控制所颁发的临时证书的最大有效期。 您可以允许证书的有效期最长 36 小时，也可以将有效期限制在 15 分钟以内。 临时证书的到期时间不取决于的值X-Amz-Date。

永久凭证没有此限制。 仅使用临时证书是最佳做法，您可以明确撤销任何永久证书，这也会使基于该凭证的所有签名失效。

尽管s3:signatureAge以毫秒为单位，但将其设置为小于 60 秒是不切实际的，即使您的时钟同步良好，使用延迟也很低。 低于 60 秒的设置存在拒绝有效请求的风险。如果您预计签名生成和请求提交之间会出现延迟，或者时钟同步出现问题，则应在管理中考虑这些问题s3:signatureAge。

大规模定位存储桶

SCPs 可以aws:PrincipalTag用来为用户设置例外。您不能在存储桶上使用标签来控制访问权限 aws:ResourceTag —— 只有对象标签用于访问控制。向要应用此控件的每个对象添加标签通常无法扩展。

适合许多用例的解决方案是在账户级别应用策略和例外情况，方法是更改 SCP 适用的账户，或者使用 aws: ResourceAccount、aws: 或 a w s: ResourceOrg ID。ResourceOrgPaths例如，可以将 SCP 应用于一组生产帐户。

另一种解决方案是使用自定义 AWS Config 规则来实现侦探控件或响应式控件。目标是让每个存储桶都包含带有适当护栏的存储桶策略。除了测试存储桶策略的内容外，如果存储桶使用特定值标记，则自定义 AWS Config 规则还可以从存储桶中检索标签，并从规则中排除该存储桶。如果该规则未通过合规性检查，则它可以将存储桶标记为不合规，也可以调用补救措施将护栏添加到存储桶的策略中。

> **Note**
>
> 您不能将请求的标签内容限制为PutBucketTagging。要控制存储桶的标记方式，必须限制对PutBucketTagging和的访问权限DeleteBucketTagging。

记录交互和缓解措施

预签名 URL 包含签名，可在到期前的一段时间内用于执行其签名的特定 API 操作。应将其视为临时访问凭证。签名应仅对需要知道的各方保密。在大多数环境中，这是发送请求的客户端和接收请求的服务器。作为直接 HTTPS 会话的一部分发送签名会保持其私有性，因为只有 HTTPS 会话的参与者才能看到传输签名的 URI。

对于预签名 URLs，签名作为X-Amz-Signature查询字符串参数传输。查询字符串参数是 URI 的组成部分。风险在于客户端可能会用它记录 URI 和签名。客户端可以访问整个 HTTP 请求，并且可以记录请求的任何部分、数据和标头（包括身份验证标头）。但是，按照惯例，这种情况并不常见。URI 日志记录更为常见，在访问日志等情况下是必需的。在登录之前，客户端应使用密文或屏蔽来删除签名。URIs

在某些环境中，用户允许中介（代理）查看其 HTTPS 会话。启用代理需要对客户端系统的高级特权访问权限，因为它们需要配置和可信证书。在客户端中间环境的本地环境中安装代理配置和可信证书允许非常高的权限级别。为此，应严格控制与此类中介机构的接触。

中介的目的通常是屏蔽不需要的出口，并跟踪其他出口。因此，此类中介机构通常会记录请求。尽管中介机构可以像客户端一样记录任何内容、标题和数据（所有这些都非常敏感），但他们更常见的是记录URIs，例如包含X-Amz-Signature查询字符串参数的内容。

缓解措施

我们建议 URI 日志记录可以删除X-Amz-Signature查询字符串参数，编辑整个查询字符串，或者将信息视为高度机密信息，就像直接访问中间服务器一样。尽管强烈建议使用这些保护措施，但只要泄露延迟足够长的时间以至于签名 URLs 到期，预签名过期这一事实就可以降低日志泄露的风险。

Amazon S3 还会看到签名，并且必须对其进行适当的处理。Amazon S3 服务器访问日志包含请求URIX-Amz-Signature，但建议对其进行编辑。在记录 Amazon S3 CloudTrail 的数据事件时，情况也是如此。 您可以使用自定义数据标识符将 CloudWatch Amazon Logs 配置为屏蔽数据。

以下正则表达式与 URI 中显示的相匹配：X-Amz-Signature

```
X-Amz-Signature=[a-f0-9]{64}
```

以下正则表达式添加了分组模式，以更具体地标识要替换的文本：

```
(?:X-Amz-Signature=)([a-f0-9]{64})
```

如果您有如下访问日志条目：

```
X-Amz-Signature=733255ef022bec3f2a8701cd61d4b371f3f28c9f193a1f02279211d48d5193d7
```

第一个正则表达式将访问日志条目转换为：

```
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

第二个正则表达式在支持非捕获组的系统上，将访问日志条目转换为：

```
X-Amz-Signature=XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

常见问题解答

一个预签名的请求可以多次使用吗？ 这是安全风险吗？

是的，预签名请求中的签名可以多次使用。这是否构成安全风险是一个上下文问题。其他访问 AWS 服务的方法也允许重复。具有 AWS 凭据的用户或工作负载可以向发送多个请求 AWS 服务，其中任何一个请求都可能是重复的。

如果您的用例需要执行一次且仅执行一次，则应实施其他机制来强制执行一次性使用。一次性使用不是预签名请求的功能。作为一名安全工程师，您应该查看用例和实现，但在许多情况下，多次使用符合可接受的用途。

目标用户以外的其他人能否使用预签名请求？

预签名请求中的签名可以由任何拥有该签名的人发送。只有当它通过其他形式的验证（例如数据边界控制）时，它才会被接受。如果签名已过期、签名证书已过期，或者签名凭证无法访问所请求的资源，则请求将被拒绝。

其他使用进行身份验证的方法也是如此。 AWS 服务不当共享的凭据允许不当访问。核心最佳做法是仅与目标受众共享凭证和签名。如果您无法相信目标受众会保护私人数据的安全而不与他人共享，那么这将破坏任何形式的身份验证。

授权用户能否使用预签名的请求来泄露数据？

保护数据需要采取强有力的行动。在维护数据边界的同时允许出于预期目的进行访问需要一种全面的方法。 最低权限访问、数据边界控制以及仅使用临时访问凭证是适用于保护数据的一般最佳做法。适当使用这些控件还会限制用户通过他们生成的预签名请求执行操作的能力。

这是因为预签名请求提供的访问权限是授予用于签署请求的凭据的访问权限的子集。在这种情况下，适用于访问数据的最佳做法通常适用于预签名的请求，但是预签名的请求不会创建对数据的新访问权限。

- 最大到期时间仅限于签名证书的到期。 如果签名凭证被撤销，则基于凭证的签名将不再有效。
- 如果与签名证书关联的 IAM 委托人的权限不包括执行与预签名请求相关的操作，则调用预签名请求会导致 “访问被拒绝” 响应。 响应取决于调用时权限的当前状态，这与生成预签名请求签名的时间无关。

- 委托人的属性是根据与签名凭证关联的委托人进行评估的。
- 根据与签名凭证关联的角色会话来评估角色会话的@@ 属性。
- 与普通请求一样，网络的属性是根据请求的接收方式来评估的。

在这种情况下，对与预签名请求相关的风险的审查仅限于使用与用户凭证不同的凭据签署的区域，并且提供的访问权限不是用户主体的一部分。此检查应应用于服务设计、工作负载或代表用户生成签名的解决方案，而不是预签名的请求功能本身。

如果我怀疑预签名 URL 是以未经授权的方式共享的，我能否拒绝该网址的访问？

是。这需要使 URL 签名时使用的凭据失效。有多种方法可以做到这一点：

- 移除证书所属的 IAM 委托人的权限。如果该 IAM 委托人不再有权访问该 URL 所签名的资源和操作，则该 URL 将无法执行该操作。这会影响该 IAM 委托人的所有匹配使用。
- 如果用于签名 URL 的证书是临时 AWS STS 证书，则可以撤消在特定时间之前为 IAM 委托人颁发的临时证书的会话权限。根据用例，可能还有其他有效会话在正常到期时间之前失效，但新会话不会受到影响。撤消会话权限还会使使用与这些会话关联的凭据签名的任何 URL 失效，但是与新会话关联的新 URL 不会受到影响。
- 如果用于签名 URL 的凭证是永久凭证，请停用访问密钥。这会影响与这些凭证相关的所有用法。

资源

Amazon S3 文档

- 对@@ 请求进行身份验证（AWS 签名版本 4）
- 对@@ 请求进行身份验证：使用查询参数（AWS 签名版本 4）
- 对@@ 请求进行身份验证：使用 POST 进行基于浏览器的上传（AWS 签名版本 4）
- Amazon S3 签名版本 4 身份验证特定策略密钥
- 使用预签名 URL

其他参考资料

- 在 AWS 上构建数据边界（AWS 白皮书）
- SEC03-BP02 授予最低权限访问权限（架构AWS 良好的框架，安全支柱）
- SEC03-BP05 为您的组织定义权限护栏（架构AWS 良好的框架、安全支柱）

附录 A：如何 AWS 服务 使用预签名 URLs

本附录提供有关使用预签名的 AWS 服务 URLs信息和功能。此信息有两个用途：

- 为实施控制措施的安全工程师提供有关这些控制措施可能产生的影响的信息。
- 让人们意识到这种风险可能与URL记录交互相关的情况。

> **Important**
>
> 本附录未提供预签名的URLs完整列表 AWS 服务 或其用法。它也不涵盖定制解决方案或第三方解决方案。

Amazon S3 控制台

主体：控制台用户

默认到期时间：5 分钟

> **免责声明**
>
> 本节记录了 Amazon S3 控制台的当前行为。 AWS 控制台行为如有更改，恕不另行通知。

Amazon S3 控制台支持下载和上传对象。 下载使用过期时间为 300 秒（5 分钟）的预签名 URL。 由向URL的请求生成`https://<bucket-region>.console.aws.amazon.com/s3/batchOpsServlet-proxy`。

该请求是在用户单击下载按钮时启动的，因此在出现明确的下载请求之前，URL不会提前生成或发送给客户端。

上传内容类似，唯一的不同是控制台发送两个请求：`OPTIONS`作为飞行前CORS检查，和。`PUT` 两个请求都使用相同的签名。

用于签名的凭证是与当前登录的用户关联的临时证书。 有关获取这些临时证书的方法的详细信息不在本指南的讨论范围之内。

Amazon S3 Object Lambda

负责人：接入点呼叫者

默认过期时间：61 秒

Amazon S3 对象 Lambda 使用 AWS Lambda 函数自动处理和转换从亚马逊 S3 检索的数据。当 S3 Object Lambda 调用函数时，会为该函数提供一个预签名 URL (`inputS3Url`)，它可以使用该预签名 () 从支持的接入点下载原始对象。

这些预签名URLs是为支持的 Amazon S3 接入点签名的，该接入点是在您配置 S3 对象 Lambda 时提供的。（这与对象 Lambda 接入点不同。）不是使用绑定到 Lambda 函数的角色，而是使用原始调用者的身份进行签名，并且该用户的权限将在使用时生效URL。URL如果中有签名的标头URL，那么 Lambda 函数必须在对 Amazon S3 的调用中包含这些标头。

返回的预签名的URL过期时间为 61 秒（比 S3 Object Lambda 函数的最大持续时间多一秒）。生成的URL只能与支持的接入点一起使用。S3 对象 Lambda 接入点的调用者需要有权访问该接入点。您可以使用条件限制对 S3 对象 Lambda 上下文的访问权限。`"aws:CalledVia": ["s3-object-lambda.amazonaws.com"]`当该条件附加到支持的接入点或存储桶时，用户无法直接访问支持的接入点或存储桶。

这种方法的价值在于，无需向 Lambda 函数授予对您的 S3 存储桶或访问点的访问权限。与 Lambda 函数关联的角色需要权限 WriteGetObjectResponse，但不需要权限。GetObject

当 S3 对象 Lambda 生成预签名时URLs，它不会添加网络限制，因此URL可以在 Lambda 函数之外使用。但是，对 S3 对象 Lambda 的调用者施加的任何限制仍然适用。例如，如果您的 Lambda 函数在中运行，VPC并且您限制调用者使用VPC终端节点，则任何拥有预签名的人都需要URL能够通过该终端节点发送该函数。VPC 此限制也适用于SourceIp和VpcSourceIp。

> **Note**
>
> 要在中使用 S3 对象 Lambda 函数VPC，VPC必须有通往公共 S3 终端节点的路径才能调用。WriteGetObjectResponse 这并不表示使用VPC终端节点的要求不适用于从存储桶检索数据的请求。

AWS Lambda 跨区域 CopyObject

校长：AWS 内部

默认到期时间：3600 秒

当您使用CopyObject或UploadPartCopyAPI进行复制时 AWS 区域，Amazon S3 在URLs内部使用预签名。它们APIs可以直接从命令中调用，SDKs也可以从 AWS CLI 命令`aws s3api copy-object`和中调用`aws s3api upload-part`。它们APIs不用于 Amazon S3 复制，但是当源 AWS CLI `aws s3 cp`和目标是 S3 存储桶时，和`aws s3 sync`命令会使用它们。它们还得到各种`TransferManager`实现的支持 AWS SDKs。

AWS Lambda GetFunction

校长： AWS 内部

默认到期时间：10 分钟

AWS Lambda 在生成部署到 Lambda 容器的资产之前，将用户版本存储在 Lambda 团队拥有的 S3 存储桶中。 要访问函数的代码时，可以调用GetFunctionAPI。 API响应为`Code.Location`，其中包含有效期为 10 分钟的预签名URL（此到期时间是当前行为，不是已发布的合同）。 如果您不想要代码，则可以使用GetFunctionConfigurationGetFunctionConcurrency、和的组合ListTags来检索返回的其他数据`GetFunction`。

返回的URL不是使用当前登录用户的证书签名的，而是由 Lambda 代表用户签名的。因此，应用于当前登录的用户或该用户的临时会话凭证的条件密钥（例如`aws:SourceIP`）不适用于生成的URL。无论条件键GetFunction仅应用于用户或会话的所有用法，还是应用于用户或会话的所有AWSAPI用法，都是如此。

Lambda 控制台还使用GetFunction并返回预签名URL。 控制台使用与当前登录用户关联的临时凭证进行呼叫GetFunction。有关获取这些临时证书的详细信息不在本文档的讨论范围之内。

Amazon ECR

校长： AWS 内部

默认到期时间：1 小时

Amazon Elastic Container Registry (AmazonECR) 提供了URL，它会返回有效期为一小时的预签名，并支持从亚马逊ECR图像下载单个图层。GetDownloadUrlForLayerAPI但是，此操作由 Amazon ECR 代理使用，用户通常不使用此操作来拉取和推送图像。

Amazon Redshift Spectrum

校长：角色已传递给CREATEEXTERNALSCHEMA直接 `IAM_ROLE`

默认到期时间：1 小时

Amazon Redshift Spectrum 在内部使用URLs预签名，禁止限制存储桶和亚马逊 Redshift 角色的组合，以限制预签名。URLs 您可以使用 16 分钟的`s3:signatureAge`值，但值过低是不可靠的。您可以使用的最小值取决于查询的时间和大小。尽管小于 16 分钟的值适用于许多场景，但它需要测试。可以而且应该将该角色限制为仅供Redshift Spectrum使用，而Redshift Spectrum不会透露URLs其生成的内容，从而减轻了降低过期值的典型理由。

亚马逊 A SageMaker I Studio

亚马逊 SageMaker AI Studio 支持两个API操作：CreatePresignedDomainUrl和CreatePresignedNotebookInstanceUrl。但是，它们APIs与签名版本 4 的预签名URL功能无关。它们会APIsURL创建使用`authToken`参数的，但它们不支持任何标准的 Signature 版本 4 查询参数。

`authToken`是一种不同的机制，但与预签名URLs有相似之处。它作为查询字符串参数发送，并支持 5 分钟的过期时间。

SageMaker AI 支持网络限制。如果您对操作设置了限制，则该`sagemaker:CreatePresignedDomainUrl`操作既适用于调用 CreatePresignedDomainUrl，也适用于生成的操作的使用URL。如果从有效的网络生成，然后由无效网络发送，则生成该网络的API调用将URL成功，但发送该URL请求的请求将失败。URL`sagemaker:CreatePresignedNotebookInstanceUrl`动作也是如此。CreatePresignedNotebookInstanceUrl

有关更多信息，请参阅 A SageMaker I 文档。

附录 B：预签名 URL 的控件如何影响 AWS 服务

本附录描述了使用预签名 URL（如附录 A 中所述）与本指南前面所述的控件之间的交互。 AWS 服务

s3: SignatureAge 的护栏

Amazon S3 控制台不会因为`s3:signatureAge`条件密钥设置的最长 5 分钟到期时间而中断。 当您选择 “下载” 按钮时，Amazon S3 控制台会生成预签名 URL，并应用自己的 5 分钟到期时间。短于 2 分钟的最大持续时间可能会导致基于时钟同步和延迟的随机故障。

Amazon S3 Object Lambda 使用的过期时间为 61 秒，因此将条件设置`s3:signatureAge`为 61 秒或更长时间不会造成任何中断。较短的持续时间可能不太可靠，并可能导致间歇性故障。

Amazon S3 跨区域CopyObject不会因为最长 5 分钟的过期时间而中断。但是，较短的持续时间可能会导致基于时钟同步和延迟的随机故障。

在中 AWS Lambda，GetFunction提供指向客户账户之外对象的 URL，因此客户政策不会影响生成的网址。

亚马逊 Redshift Spectrum 已经过测试`s3:signatureAge`，条件为 16 分钟。但是，较短的持续时间可能会导致中断。

不使用网络限制时 s3: authType 的护栏

Amazon S3 控制台通常会受到`s3:authType`护栏的影响。 控制台根据本地网络配置路由到 Amazon S3。 如果本地网络以网络限制允许的方式路由到 Amazon S3，则 Amazon S3 控制台仍然可以运行。但是，如果以不允许的方式通过代理或公共互联网进行路由，则使用将被阻止。 但是，阻止使用可能是该政策的目的。

如果 Lambda 函数未连接到相应的 VPC，则 Amazon S3 对象 Lambda 会受到影响。 在此配置中，VPC 必须具有 NAT 网关，不是为了访问 S3 存储桶，而是为了调用WriteGetObjectResponse。

如果将此保护措施应用于存储桶策略，而没有建议的例外情况（何时**`aws:viaAWSService`**为真），则会中断 Amazon S3 跨区域CopyObject。

除非使用增强型 VPC 路由`s3:authType`，否则 Amazon Redshift Spectrum 会受到护栏的影响。目前，Redshift Spectrum 仅支持无服务器集群的增强型 VPC 路由，不支持已配置集群的增强型 VPC 路由。

文档历史记录

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

变更	说明	日期
初次发布	—	2024年7月23日

AWS 规范性指导词汇表

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

数字

7 R

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

- 重构/重新架构 - 充分利用云原生功能来提高敏捷性、性能和可扩展性，以迁移应用程序并修改其架构。这通常涉及到移植操作系统和数据库。示例：将您的本地 Oracle 数据库迁移到兼容 Amazon Aurora PostgreSQL 的版本。
- 更换平台 - 将应用程序迁移到云中，并进行一定程度的优化，以利用云功能。示例：在中将您的本地 Oracle 数据库迁移到适用于 Oracle 的亚马逊关系数据库服务 (Amazon RDS) AWS Cloud。
- 重新购买 - 转换到其他产品，通常是从传统许可转向 SaaS 模式。示例：将您的客户关系管理 (CRM) 系统迁移到 Salesforce.com。
- 更换主机（直接迁移）- 将应用程序迁移到云中，无需进行任何更改即可利用云功能。示例：在中的 EC2 实例上将您的本地 Oracle 数据库迁移到 Oracle AWS Cloud。
- 重新定位（虚拟机监控器级直接迁移）：将基础设施迁移到云中，无需购买新硬件、重写应用程序或修改现有操作。您可以将服务器从本地平台迁移到同一平台的云服务。示例：将Microsoft Hyper-V应用程序迁移到 AWS。
- 保留（重访）- 将应用程序保留在源环境中。其中可能包括需要进行重大重构的应用程序，并且您希望将工作推迟到以后，以及您希望保留的遗留应用程序，因为迁移它们没有商业上的理由。
- 停用 - 停用或删除源环境中不再需要的应用程序。

A

ABAC

请参阅基于属性的访问控制。

抽象服务

参见托管服务。

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

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

AI

参见人工智能。

AIOps

参见人工智能操作。

匿名化

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

反模式

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

应用程序控制

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

应用程序组合

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

人工智能（AI）

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

人工智能操作 (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、持久性（ACID）

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

基于属性的访问权限控制（ABAC）

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

权威数据源

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

可用区

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

AWS 云采用框架 (AWS CAF)

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

AWS 工作负载资格框架 (AWS WQF)

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

B

坏机器人

旨在破坏个人或组织或对其造成伤害的机器人。

BCP

参见业务连续性计划。

行为图

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

大端序系统

一个先存储最高有效字节的系统。另请参见字节顺序。

二进制分类

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

bloom 筛选条件

一种概率性、内存高效的数据结构，用于测试元素是否为集合的成员。

蓝/绿部署

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

自动程序

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

僵尸网络

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

分支

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

破碎的玻璃通道

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

棕地策略

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

缓冲区缓存

存储最常访问的数据的内存区域。

业务能力

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

业务连续性计划（BCP）

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

C

CAF

参见AWS 云采用框架。

金丝雀部署

向最终用户缓慢而渐进地发布版本。当你有信心时，你可以部署新版本并全部替换当前版本。

CCoE

参见云卓越中心。

CDC

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。您可以将 CDC 用于各种目的，例如审计或复制目标系统中的更改以保持同步。

混沌工程

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

CI/CD

查看持续集成和持续交付。

分类

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

客户端加密

在目标 AWS 服务 收到数据之前，对数据进行本地加密。

云卓越中心 (CCoE)

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

云计算

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

云运营模型

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

云采用阶段

组织迁移到以下阶段时通常会经历四个阶段 AWS Cloud：

- 项目 - 出于概念验证和学习目的，开展一些与云相关的项目
- 基础 — 进行基础投资以扩大云采用率（例如，创建着陆区、定义 CCo E、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)

人工智能领域，使用机器学习来分析和提取数字图像和视频等视觉格式的信息。例如，Amazon SageMaker AI 为 CV 提供了图像处理算法。

配置偏差

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

配置管理数据库（CMDB）

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

合规性包

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

持续集成和持续交付（CI/CD）

自动执行软件发布过程的源代码、构建、测试、暂存和生产阶段的过程。 CI/CD is commonly described as a pipeline. 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

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。

后

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。有关如何将领域驱动设计与 strangler fig 模式结合使用的信息，请参阅使用容器和 Amazon API Gateway 逐步将原有的 Microsoft ASP.NET（ASMX）Web 服务现代化。

DR

参见灾难恢复。

漂移检测

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

DVSM

参见开发价值流映射。

E

EDA

参见探索性数据分析。

EDI

参见电子数据交换。

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。与云计算相比，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)

组织之间自动交换业务文档。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密文的计算过程。

加密密钥

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

字节顺序

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

端点

参见服务端点。

端点服务

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

企业资源规划 (ERP)

一种自动化和管理企业关键业务流程（例如会计、MES 和项目管理）的系统。

信封加密

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

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

参见企业资源规划。

探索性数据分析（EDA）

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

F

事实表

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

失败得很快

一种使用频繁和增量测试来缩短开发生命周期的理念。这是敏捷方法的关键部分。

故障隔离边界

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

功能分支

参见分支。

特征

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

特征重要性

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

少量提示

在要求法学硕士执行类似任务之前，向其提供少量示例，以演示该任务和所需的输出。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。对于需要特定格式、推理或领域知识的任务，Few-shot 提示可能非常有效。另请参见零镜头提示。

FGAC

请参阅精细的访问控制。

精细访问控制 (FGAC)

使用多个条件允许或拒绝访问请求。

快闪迁移

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

FM

参见基础模型。

基础模型 (FM)

一个大型深度学习神经网络，一直在广义和未标记数据的大量数据集上进行训练。 FMs 能够执行各种各样的一般任务，例如理解语言、生成文本和图像以及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。

G

生成式人工智能

人工智能模型的子集，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工件，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 AI。

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。

金色影像

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配置软件，并有助于提高设备制造运营的速度、可扩展性和生产力。

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。它们是使用服务控制策略和 IAM 权限边界实现的。侦测性防护机制会检测策略违规和合规性问题，并生成警报以进行修复。它们通过使用 AWS Config、、Amazon、 AWS Security Hub GuardDuty AWS Trusted Advisor、Amazon Inspector 和自定义 AWS Lambda 支票来实现。

H

HA

参见高可用性。

异构数据库迁移

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

高可用性 (HA)

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

历史数据库现代化

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

抵制数据

从用于训练机器学习模型的数据集中扣留的一部分带有标签的历史数据。通过将模型预测与抵制数据进行比较，您可以使用抵制数据来评估模型性能。

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

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

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

IIoT

参见工业物联网。

不可变的基础架构

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

入站（入口）VPC

在 AWS 多账户架构中，一种接受、检查和路由来自应用程序外部的网络连接的 VPC。AWS 安全参考架构建议设置您的网络帐户，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，请参阅制定工业物联网 (IIoT) 数字化转型战略。

检查 VPC

在 AWS 多账户架构中，一种集中式 VPC，用于管理对 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 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。

大型语言模型 (LLM)

一种基于大量数据进行预训练的深度学习 AI 模型。法学硕士可以执行多项任务，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 LLMs。

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

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。

LLM

参见大型语言模型。

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

迁移加速计划（MAP）

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

大规模迁移

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

迁移工厂

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

迁移元数据

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

迁移模式

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

迁移组合评测（MPA）

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

迁移准备情况评测（MRA）

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

迁移策略

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

ML

参见机器学习。

现代化

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

现代化准备情况评估

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

单体应用程序（单体式）

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

MPA

参见迁移组合评估。

MQTT

请参阅消息队列遥测传输。

多分类器

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

可变基础架构

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

O

OAC

请参阅源站访问控制。

OAI

参见源访问身份。

OCM

参见组织变更管理。

离线迁移

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

OI

参见运营集成。

OLA

参见运营层协议。

在线迁移

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

OPC-UA

参见开放流程通信-统一架构。

开放流程通信-统一架构 (OPC-UA)

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

运营级别协议（OLA）

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

运营准备情况审查 (ORR)

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

操作技术 (OT)

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

运营整合（OI）

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

组织跟踪

由此创建的跟踪 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

参见运营准备情况审查。

OT

参见运营技术。

出站（出口）VPC

在 AWS 多账户架构中，一种处理从应用程序内部启动的网络连接的 VPC。AWS 安全参考架构建议设置您的网络帐户，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 主体的 IAM 管理策略，用于设置用户或角色可以拥有的最大权限。有关更多信息，请参阅 IAM 文档中的权限边界。

个人身份信息 (PII)

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

PII

查看个人身份信息。

playbook

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

PLC

参见可编程逻辑控制器。

PLM

参见产品生命周期管理。

policy

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

多语言持久性

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

组合评测

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

谓词

返回`true`或的查询条件`false`，通常位于子`WHERE`句中。

谓词下推

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

预防性控制

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

主体

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

通过设计保护隐私

一种在整个开发过程中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 如何响应针对一个或多个 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。

提示链接

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

Q

查询计划

一系列步骤，例如指令，用于访问 SQL 关系数据库系统中的数据。

查询计划回归

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

R

RACI 矩阵

参见 “负责任、负责、咨询、知情”（RACI）。

RAG

请参见检索增强生成。

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

参见 “负责任、负责、咨询、知情”（RACI）。

RCAC

请参阅行和列访问控制。

只读副本

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

重新架构师

见 7 R。

恢复点目标 (RPO)

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

恢复时间目标 (RTO)

服务中断和服务恢复之间可接受的最大延迟。

重构

见 7 R。

区域

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

回归

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

重新托管

见 7 R。

版本

在部署过程中，推动生产环境变更的行为。

搬迁

见 7 R。

更换平台

见 7 R。

回购

见 7 R。

故障恢复能力

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

基于资源的策略

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

责任、问责、咨询和知情（RACI）矩阵

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

响应性控制

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

保留

见 7 R。

退休

见 7 R。

检索增强生成（RAG）

一种生成式人工智能技术，其中法学硕士在生成响应之前引用其训练数据源之外的权威数据源。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据的过程。

行列访问控制 (RCAC)

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

RPO

参见恢复点目标。

RTO

参见恢复时间目标。

运行手册

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

S

SAML 2.0

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

SCADA

参见监督控制和数据采集。

SCP

参见服务控制政策。

secret

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

安全性源于设计

一种在整个开发过程中考虑安全性的系统工程方法。

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。安全控制主要有四种类型：预防性、侦测、响应式和主动式。

安全加固

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

安全信息和事件管理（SIEM）系统

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

安全响应自动化

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

服务器端加密

在目的地对数据进行加密，由接收方 AWS 服务 进行加密。

服务控制策略（SCP）

一种策略，用于集中控制组织中所有账户的权限 AWS Organizations。 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

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

服务水平协议（SLA）

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

服务级别指示器 (SLI)

对服务性能方面的衡量，例如其错误率、可用性或吞吐量。

服务级别目标 (SLO)

代表服务运行状况的目标指标，由服务级别指标衡量。

责任共担模式

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

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

恶作剧

参见单点故障。

星型架构

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

strangler fig 模式

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

子网

您的 VPC 内的一个 IP 地址范围。子网必须位于单个可用区中。

监控和数据采集 (SCADA)

在制造业中，一种使用硬件和软件来监控有形资产和生产操作的系统。

对称加密

一种加密算法，它使用相同的密钥来加密和解密数据。

综合测试

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

系统提示符

一种向法学硕士提供上下文、说明或指导方针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

tags

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 对等连接

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 对等连接。

漏洞

损害系统安全的软件缺陷或硬件缺陷。

W

热缓存

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

暖数据

不常访问的数据。查询此类数据时，通常可以接受中速查询。

窗口函数

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

工作负载

一系列资源和代码，它们可以提供商业价值，如面向客户的应用程序或后端过程。

工作流

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

蠕虫

参见一次写入，多读。

WQF

参见AWS 工作负载资格框架。

一次写入，多次读取 (WORM)

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

Z

零日漏洞利用

一种利用未修补漏洞的攻击，通常是恶意软件。

零日漏洞

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

零镜头提示

向法学硕士提供执行任务的说明，但没有示例（镜头）可以帮助指导任务。法学硕士必须使用其预先训练的知识来处理任务。零镜头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 few-shot 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。