实施指南

AWS 上的工作负载发现

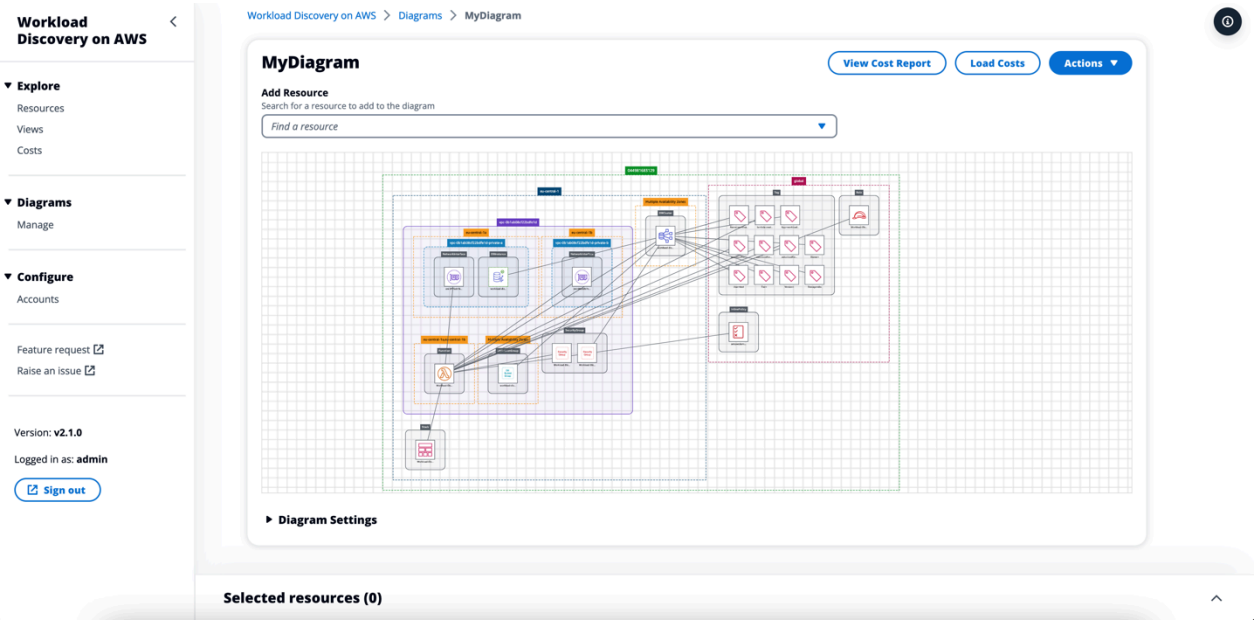
AWS 上的工作负载发现: 实施指南

Table of Contents

部署可视化工具，自动生成 AWS 云工作负载架构图

监控您的 Amazon Web Services (AWS) 云工作负载是保持运营健康和效率的关键。但是，跟踪 AWS 资源及其之间的关系可能是一项挑战。AWS 上的 Workload Discovery 是一种可视化工具，可自动生成您在 AWS 上的工作负载架构图。您可以使用此解决方案根据来自 AWS 的实时数据构建、自定义和共享详细的工作负载可视化效果。

该解决方案的工作原理是维护您的账户和地区的 AWS 资源清单，映射它们之间的关系，然后在 Web 用户界面 (Web UI) 中显示这些资源。对资源进行更改时，AWS 上的 Workload Discovery 通过在 AWS 管理控制台中提供指向该资源的链接来节省您的时间。



AWS 上的 “工作负载发现” 生成的示例架构图

本实施指南描述了在 AWS 云中在 AWS 上部署工作负载发现的架构注意事项和配置步骤。它包括指向 A WS CloudFormation 模板的链接，该模板使用安全性和可用性方面的 AWS 最佳实践启动和配置部署此解决方案所需的 AWS 服务。

在其环境中实施 Workload Discovery on AWS 解决方案的目标受众包括解决方案架构师、业务决策者、 DevOps 工程师、数据科学家和云专业人员。

使用以下导航表可快速找到这些问题的答案：

如果您想. . .	阅读. . .
了解运行此解决方案的成本。	成本

如果您想. . .	阅读. . .
在美国东部（弗吉尼亚北部）地区运行此解决方案的估计费用为每月 425.19 美元。	
了解此解决方案的安全注意事项。	安全性
了解如何为此解决方案规划限额。	配额
了解哪些 AWS 区域支持此解决方案。	支持的 AWS 区域
查看或下载此解决方案中包含的 AWS CloudFormation 模板，以自动部署该解决方案的基础设施资源（“堆栈”）。	AWS CloudFormation 模板
访问源代码。	GitHub 存储库

功能和优势

AWS 上的工作负载发现提供以下功能：

使用近乎实时的数据构建架构图

AWS 上的 Workload Discovery 每 15 分钟扫描一次您的账户，以确保您创建的图表准确且最新地呈现您的工作负载。

一站式查看来自多个账户和地区的资源

该解决方案在一个集中的图表数据库中维护您的 AWS 账户和地区的 AWS 资源清单，使您能够在单个 UI 中探索多个账户和区域及其相互关系。

AWS Organitions

在 AWS Organizations 中部署解决方案时，AWS 上的 Workload Discovery 将自动发现您组织中所有支持的资源。在此配置中，无需直接管理账户特定 CloudFormation 模板的部署，即可让这些账户可供发现。

整理工作负载中的成本数据

启用后，成本功能允许您按成本搜索账户中的资源，并将找到的资源添加到图表中。您也可以将成本数据添加到已有的逻辑示意图中。

导出到 diagrams.net（以前是 draw.io）

AWS 上的 Workload Discovery 可以导出您的图表，以便您可以使用此第三方绘图软件对其进行进一步注释。

与 AWS Service Catalog AppRegistry 和应用程序管理器集成，这是 AWS Systems Manager 的一项功能

此解决方案包括一个 S ervice Catalog AppRegistry 资源，用于在 Service Catalog 和 Applicat AppRegistry ion Manager 中将解决方案的 CloudFormation 模板及其底层资源注册为应用程序。通过这种集成，您可以集中管理解决方案的资源并启用应用程序搜索、报告和管理操作。

使用案例

设计和安全审查

使用此解决方案生成架构图，以验证工作负载的实现是否与建议的设计相匹配。

探索和记录现有工作负载

创建架构图以探索几乎没有文档或在没有基础架构即代码的情况下手动部署的工作负载。

可视化成本

为您的架构图生成一份成本报告，其中包含估计成本的概述。

概念和定义

本节介绍重要概念并定义此解决方案特有的术语：

资源

一种 AWS 资源，例如亚马逊简单存储服务 (Amazon S3) 存储桶或 AWS Lambda 函数。

关系

两个资源之间的链接，例如 AWS 身份和访问管理 (IAM) 角色和关联的 AWS Lambda 函数。

资源类型

资源的分类类别。始终遵循 CloudFormation 命名惯例，例如`AWS::Lambda::Function`。

discovery

该解决方案启动的流程，用于映射您的 AWS 账户和区域中的资源及其关系。

账户发现模式

发现账户并将其添加到解决方案中的方法：要么通过 AWS UI 上的工作负载发现进行自我管理，要么委托给 AWS Organizations。

> **Note**
>
> 有关 AWS 术语的一般参考，请参阅 AWS 术语表。

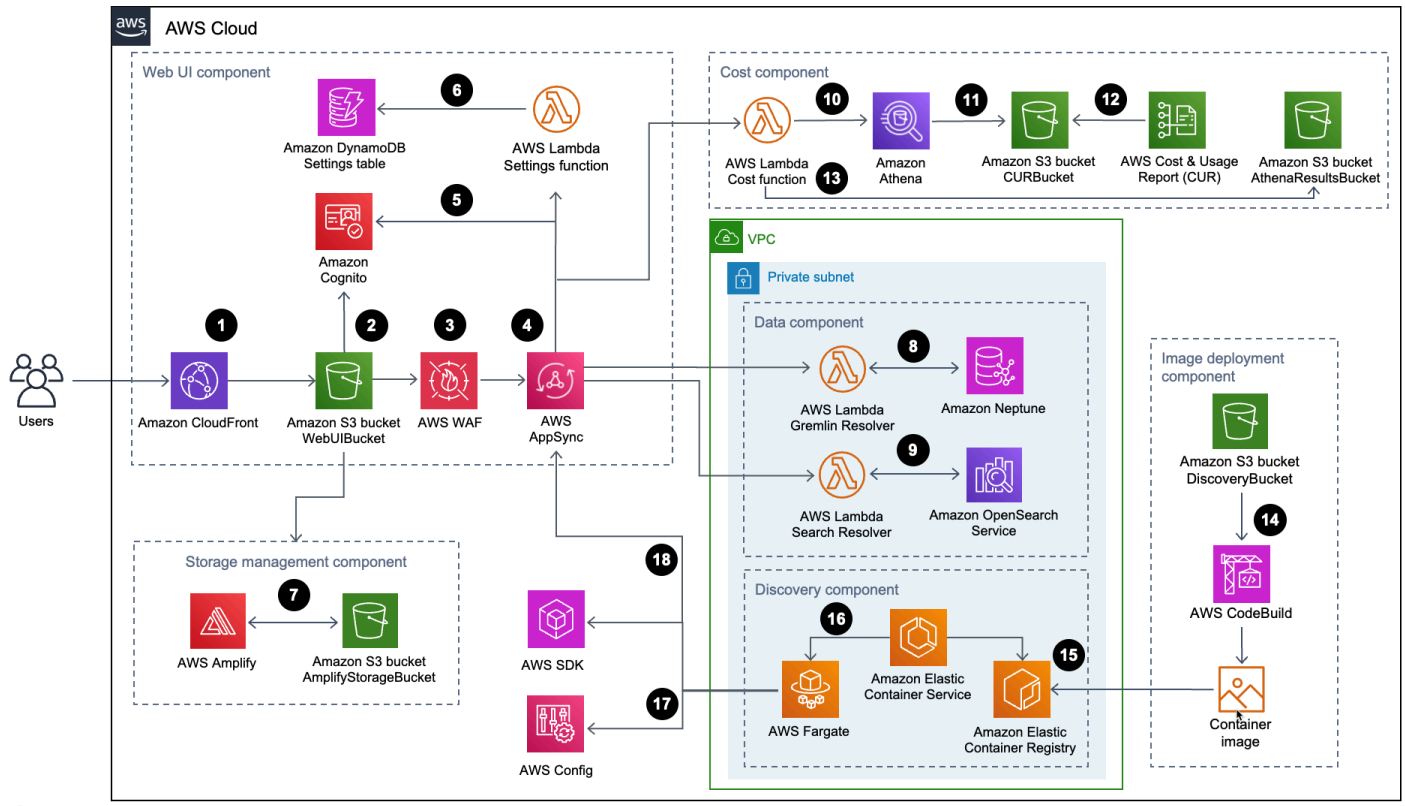
架构概述

本节提供了此解决方案所部署组件的参考实施架构图。

架构图

使用默认参数部署此解决方案将在 AWS 云中构建以下环境。

在 AWS 架构上发现工作负载



使用 AWS CloudFormation 模板部署的解决方案组件的高级流程如下：

1. HTTP Strict-Transport-Security (HSTS) 为来自亚马逊 CloudFront分配的每个响应添加安全标头。
2. 亚马逊简单存储服务 (Amazon S3) 存储桶托管与亚马逊一起分发的 Web UI CloudFront。Amazon Cognito 对用户访问网页用户界面的身份进行身份验证。
3. AWS WAF 保护 AppSync API 免受常见漏洞和机器人攻击，这些漏洞和机器人可能会影响可用性、危及安全性或消耗过多资源。
4. AWS AppSync 终端节点允许 Web UI 组件请求资源关系数据、查询成本、导入新的 AWS 区域和更新首选项。AWS AppSync 还允许发现组件在解决方案的数据库中存储永久数据。

5. AWS AppSync 使用 Amaz on Cognito 配置的 JSON 网络令牌 (JWTs) 对每个请求进行身份验证。
6. SettingsAWS Lambda 函数将导入的区域和其他配置保留到亚马逊 Dynam oD B 中。
7. 该解决方案将 AWS A mplify 和 Amazon S3 存储桶部署为存储管理组件，用于存储用户首选项和保存的架构图。
8. 数据组件使用 Gremlin Resolver AWS Lambda 函数查询和返回来自亚马逊 Neptun e 数据库的数据。
9. 数据组件使用 Search Resolver Lambda 函数查询资源数据并将其保存到亚马逊 OpenSearch 服务域中。
10. CostLambda 函数使用亚马逊 Athena 查询 AWS 成本和使用量报告 (AWS CUR)，以便向网页用户界面提供估计的成本数据。
11. 亚马逊 Athena 在 AWS CUR 上运行查询。
12. AWS CUR 将报告传送到CostAndUsageReportBucket亚马逊 S3 存储桶。
13. CostLambda 函数将亚马逊 Athena 的结果存储在亚马逊 S3 存储桶中。AthenaResultsBucket
14. AWS 在映像部署组件中 CodeBuild构建发现组件容器镜像。
15. 亚马逊弹性容器注册表 (Amazon ECR) 包含映像部署组件提供的 Docker 镜像。
16. 亚马逊弹性容器服务 (Amazon EC S) 管理 AWS Fargate 任务并提供运行该任务所需的配置。AWS Fargate 每 15 分钟运行一次容器任务，以刷新库存和资源数据。
17. AWS Config 和 AWS SDK 调用可帮助发现组件维护来自导入区域的资源数据清单，然后将其结果存储在数据组件中。
18. AWS Fargate 任务将 AWS Config 和 AWS 开发工具包调用结果保存在亚马逊 Neptune 数据库和带有 API API 调用的 OpenSearch 亚马逊服务域中。 AppSync

AWS Well-Architected 设计注意事项

该解决方案采用 AWS Well-Architected Fram ework 中的最佳实践，可帮助客户在云中设计和运行可靠、安全、高效且经济实惠的工作负载。

本节介绍 Well-Architected Framework 的设计原则和最佳实践如何使该解决方案受益。

卓越运营

我们使用卓越运营支柱的原则和最佳实践设计了此解决方案，以使该解决方案受益。

- 资源定义为基础架构，即使用代码 CloudFormation。

- 该解决方案将指标推送 CloudWatch 到亚马逊，以提供基础设施、Lambda 函数、Amazon ECS 任务、AWS S3 存储桶和其他解决方案组件的可观察性。

安全性

我们使用安全支柱的原则和最佳实践设计了此解决方案，以使该解决方案受益。

- Amazon Cognito 对网页用户界面应用程序用户进行身份验证和授权。
- 该解决方案使用的所有角色都遵循最低权限访问权限。换句话说，它们仅包含服务正常运行所需的最低权限。
- 静态数据和传输数据使用存储在专用密钥管理存储库 AWS Key Management Servic e (AWS KMS) 中的密钥进行加密。
- 凭证的有效期很短，并且遵循严格的密码策略。
- AWS AppSync 安全 GraphQL 指令可以精细控制前端和后端可以调用的操作。
- 在适用的情况下，日志记录、跟踪和版本控制处于开启状态。
- 如果适用，自动修补（次要版本）和快照创建功能已开启。
- 默认情况下，网络访问是私有的，亚马逊虚拟私有云（Amazon VPC）终端节点在可用时处于开启状态。

可靠性

我们使用可靠性支柱的原则和最佳实践设计了此解决方案，以使该解决方案受益。

- 该解决方案尽可能使用 AWS 无服务器服务来确保高可用性并从服务故障中恢复。
- 所有计算处理都使用 Lambda 函数或 AWS Fargate 上的 Amazon ECS。
- 所有自定义代码都使用 AWS 开发工具包，并且请求在客户端受到限制，以防止达到 API 速率配额。

性能效率

我们使用性能效率支柱的原则和最佳实践设计了此解决方案，以使该解决方案受益。

- 该解决方案尽可能使用 AWS 无服务器架构。这消除了管理物理服务器的运营负担。
- 该解决方案可以在支持本解决方案中使用的 AWS 服务的任何区域启动，例如：AWS Lambda、Amazon Neptune、AWS、Amazon S3 和 AppSync Amazon Cognito。

- 在支持的区域，Amazon Neptune 无服务器允许您运行和即时扩展图形工作负载，而无需管理和优化数据库容量。
- 该解决方案自始至终都使用托管服务，以减轻资源配置和管理的运营负担。

成本优化

我们使用成本优化支柱的原则和最佳实践来设计此解决方案，以使该解决方案受益。

- AWS Fargate 上的 AWS ECS 使用 Lambda 函数专门用于计算，并且仅根据使用量收费。
- Amazon DynamoDB 可按需扩展容量，因此您只需为使用的容量付费。

可持续性

我们使用可持续发展支柱的原则和最佳实践设计了该解决方案，以使该解决方案受益。

- 该解决方案尽可能使用托管和无服务器服务，以最大限度地减少后端服务对环境的影响。

架构详情

本节介绍构成此解决方案的组件和 AWS 服务，以及这些组件如何协同工作的架构详情。

身份验证机制

AWS 上的工作负载发现使用 A mazon Cognito 用户池进行用户界面和 AWS AppSync 身份验证。经过身份验证后，Amazon Cognito 会向网页用户界面提供一个 JSON 网络令牌 (JWT)，所有后续的 API 请求都将提供该令牌。如果未提供有效的 JWT，则 API 请求将失败并返回 HTTP 403 禁止响应。

支持的资源

有关 AWS 上的 Workload Discovery 可以在您的账户和区域中发现的 AWS 资源类型列表，请参阅支持的资源。

AWS 上的工作负载发现架构图管理

您可以使用 Web 用户界面将工作负载发现保存在 AWS 架构图上，可以在其中执行创建、读取、更新和删除 (CRUD) 操作。AWS Amplify 存储 API 允许 AWS 上的工作负载发现将架构图存储在 Amazon S3 存储桶中。有两个级别的权限可用：

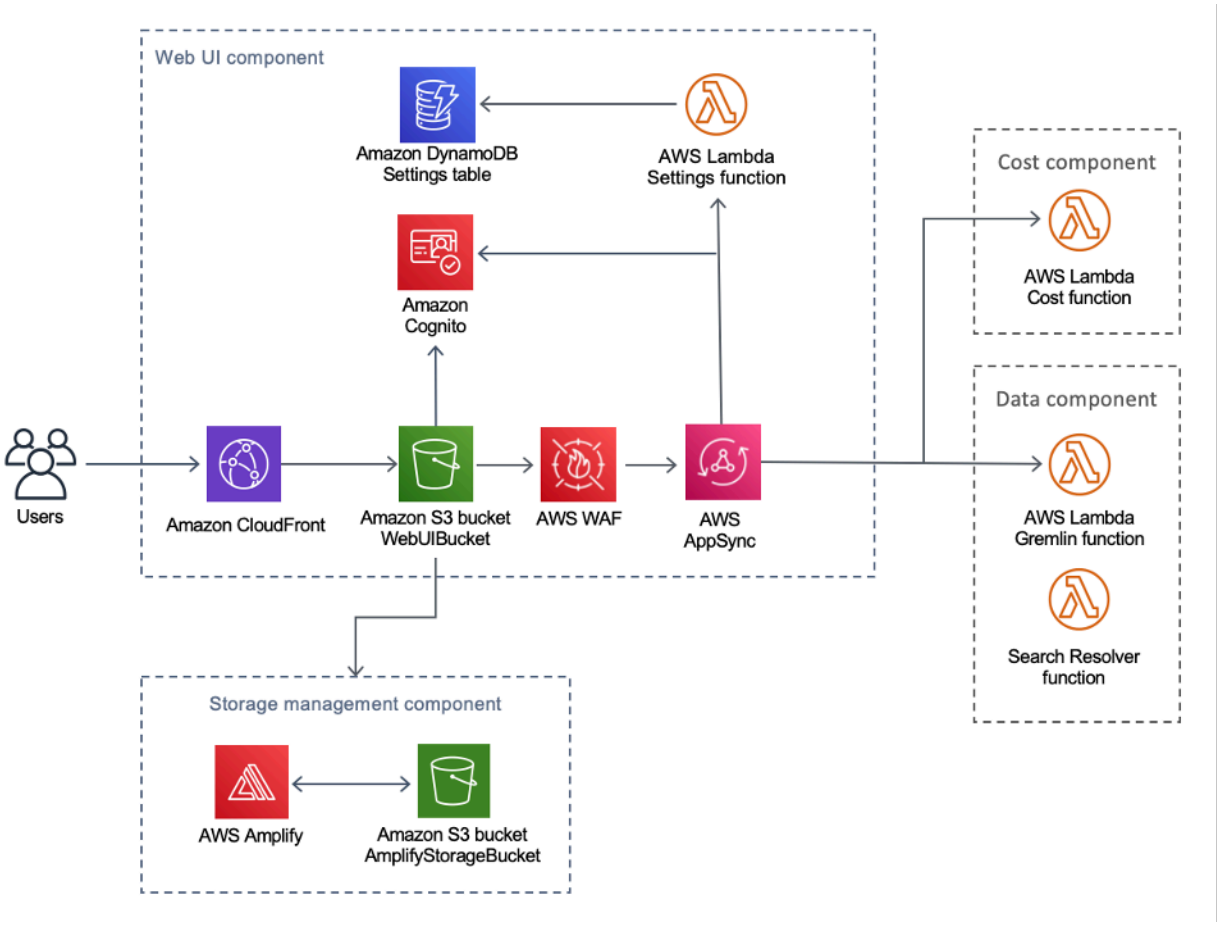
- 所有用户-允许在部署中的 AWS 用户上的 AWS 用户的工作负载发现可见 AWS 架构图上的工作负载发现。用户可以下载和编辑这些图表。
- 您-允许 AWS 架构图上的工作负载发现仅对创建者可见。其他用户将无法查看它们。

Web 用户界面和存储管理

我们使用 React 开发了网页用户界面。Web UI 提供了前端控制台，允许用户在 AWS 上与 Workload Discovery 进行交互。

Amazon 配置 CloudFront为向网页用户界面的每个 HTTP 请求附加安全标头。这提供了额外的安全层，可以抵御跨站点脚本 (XSS) 等攻击。

在 AWS Web 用户界面和存储管理组件上发现工作负载

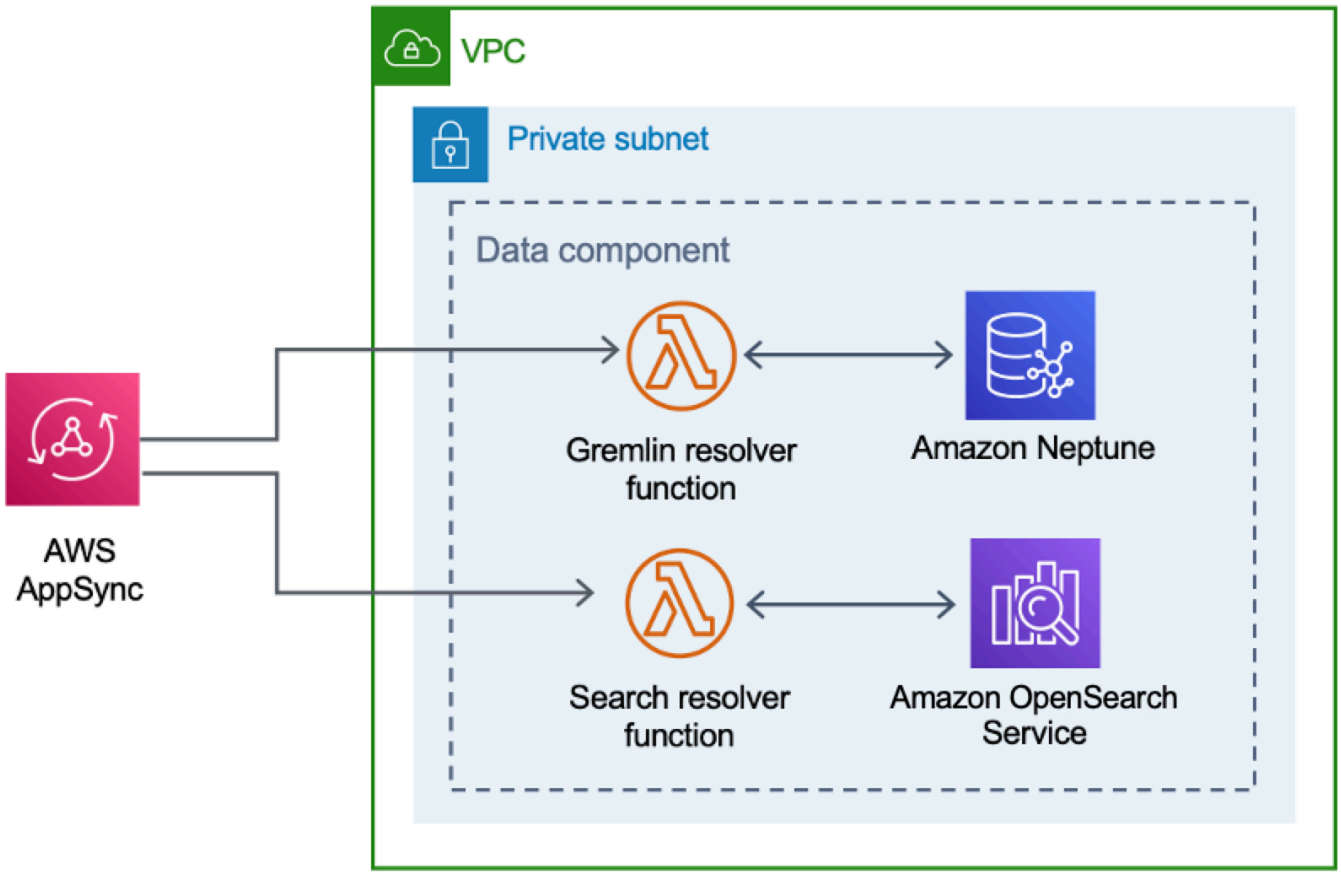


网页用户界面资源托管在 `WebUIBucket` Amazon S3 存储桶中并由亚马逊分发 CloudFront。AWS Amplify 提供了一个抽象层，用于简化与 AWS 和 A AppSync mazon S3 的集成。

该解决方案使用 AWS AppSync 来促进与 AWS 上工作负载发现中可用的各种配置的交互，包括管理导入的区域。AWS AppSync 利用 `Settings` AWS Lambda 函数来处理诸如导入新账户或区域之类的请求。

数据组件

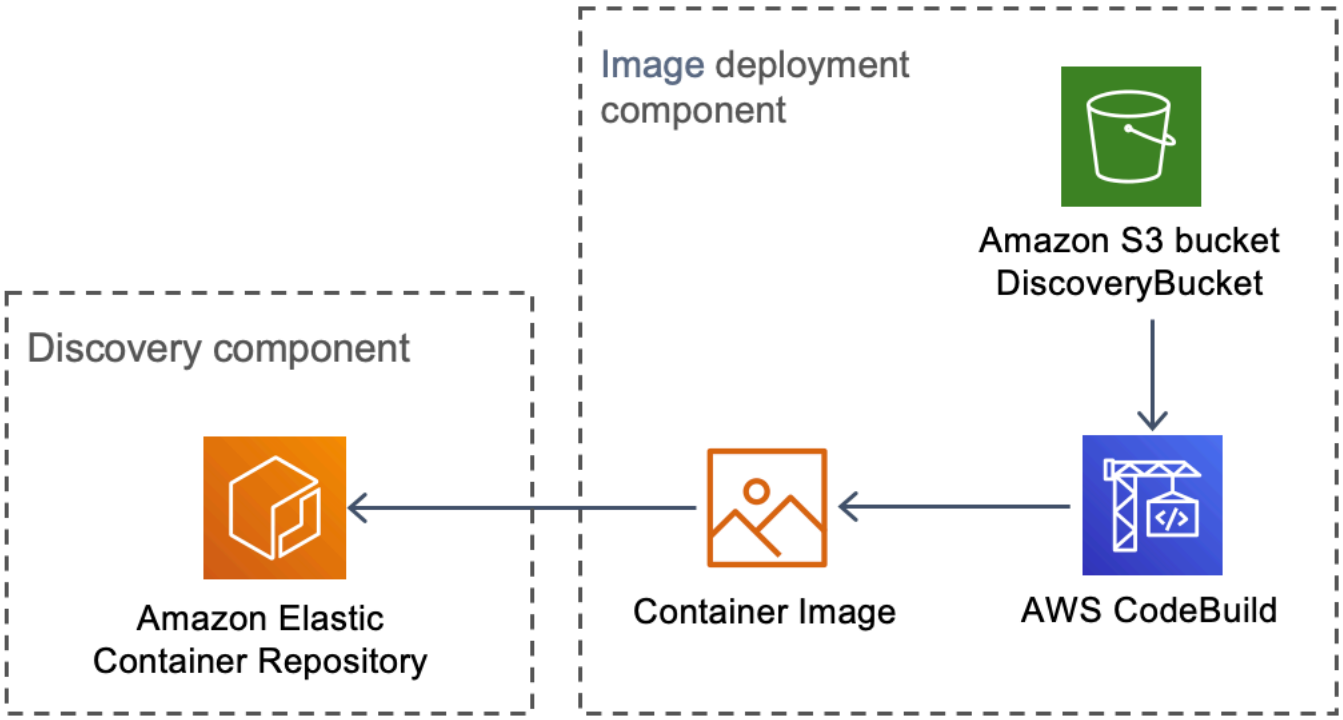
AWS 数据组件上的工作负载发现



网页界面向 API 发送请求， AppSync API 会调用或 `Gremlin Resolver` Lambda 函数`Search Resolver`。这些函数处理请求并查询 Amazon Neptune 或 OpenSearch 服务以检索有关所提供资源的数据。AWS AppSync 还支持从 AWS CUR 请求估算成本数据。

发现组件向 AppSync API 发送请求，要求读取并保存 Amazon Neptune 和 OpenSearch 服务数据库中的数据。API 在发现组件中接收来自 AWS Fargate 任务的请求。然后，使用提供数据库访问权限的 IAM 角色对 API 进行身份验证。

映像部署组件



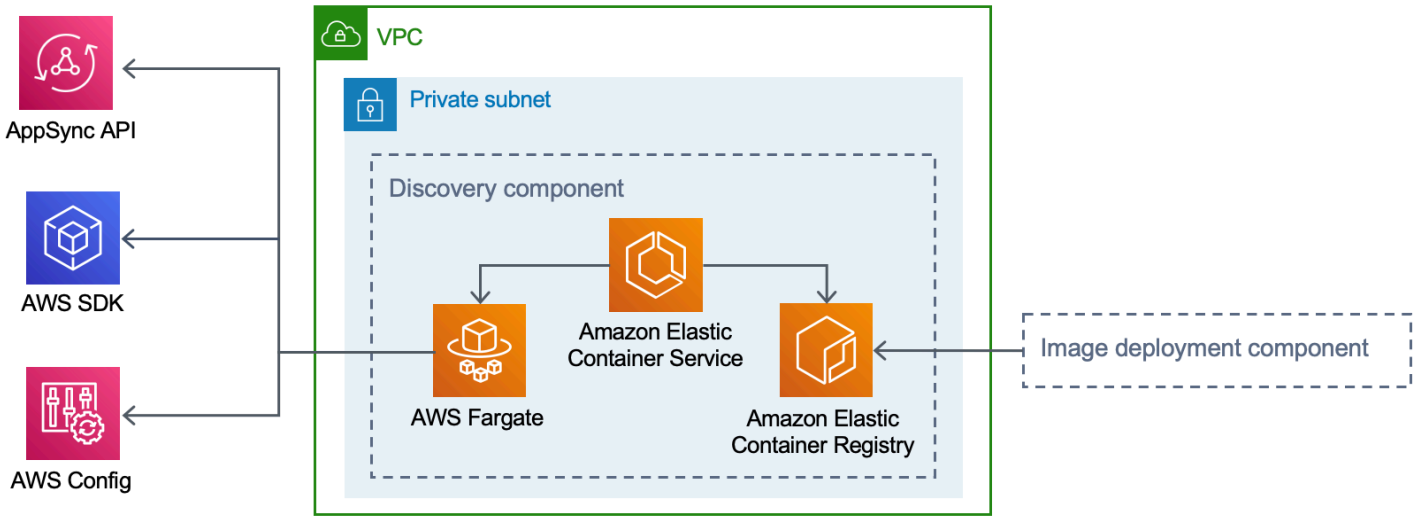
AWS 映像部署组件上的工作负载发现

映像部署组件构建发现组件使用的容器镜像。`DiscoveryBucket`和 Amazon S3 存储桶托管的代码可在部署时由构建容器映像并将其上传到 Amazon ECR 的 AWS CodeBuild 任务下载。

发现组件

发现组件是 AWS 架构上工作负载发现的主要数据收集元素。它负责查询 AWS Config 并进行描述 API 调用，以维护资源库存及其彼此之间的关系。

AWS 发现组件上的工作负载发现



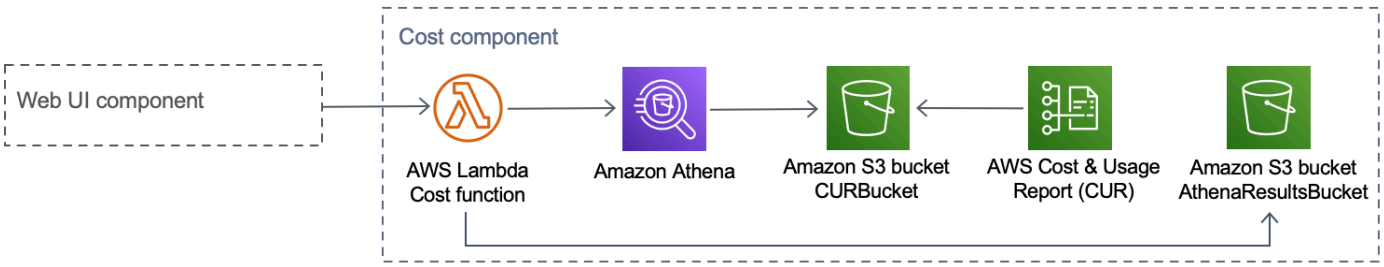
此解决方案将 Amazon ECS 配置为使用从 Amazon ECR 下载的容器映像运行 AWS Fargate 任务。AWS Fargate 任务计划每隔 15 分钟运行一次。收集的资源关系数据将插入到 Amazon Neptune 图表数据库和亚马逊 OpenSearch 服务中。

发现组件工作流程包括以下三个步骤：

1. Amazon ECS 每隔 15 分钟调用 AWS Fargate 任务。
2. Fargate 任务从 AWS Config、AWS API 描述调用和亚马逊 Neptune 数据库收集资源数据。
3. Fargate 任务计算 Amazon Neptune 数据库中存在的内容与从 AWS Config 收到的内容和描述调用之间的差异。
4. Fargate 任务向 AppSync API 发送请求，要求保留在 Amazon Neptune 和亚马逊服务中发现的对资源和 OpenSearch 关系的更改。

成本部分

AWS 上的工作负载发现成本组件



您可以在 AWS 账单和成本管理以及成本管理中创建 AWS CUR。这会将一个 Par q uet 格式的文件发布到 `CostAndUsageReportBucket` Amazon S3 存储桶。Web 用户界面向调用 Cost Lambda 函数的 AWS AppSync 终端节点发出请求。该函数向 Amazon Athena 发送预定义的查询，这些查询会从 AWS CUR 返回预估的成本信息。

由于 AWS CUR 的大小，来自亚马逊 Athena 的响应可能非常大。该解决方案将结果存储在 `AthenaResultsBucket` Amazon S3 存储桶中，并将结果分页回网页用户界面。在此存储桶上配置的生命周期策略会删除超过七天的项目。

此解决方案中的 AWS 服务

AWS 服务	描述
AWS AppSync	核心。此解决方案用于提供 Web 用户界面使用的 AppSync 无服务器 GraphQL API。
Amazon CloudFront	核心。此解决方案 CloudFront 使用 Amazon S3 存储桶作为源。这会限制对 Amazon S3 存储桶的访问，使其不可公开访问，并阻止从该存储桶直接访问。
AWS Config	核心。该解决方案使用 AWS Config 作为解决方案发现的资源和关系的主要数据源。
亚马逊 OpenSearch 服务	核心。该解决方案使用 Amazon S OpenSearch ervice 进行应用程序监控、日志分析和可观察性。
Amazon DynamoDB	核心。此解决方案使用 DynamoDB 来存储解决方案的配置数据。
亚马逊弹性容器服务 (ECS)	核心。此解决方案使用 Amazon ECS 来协调任务的运行，以发现您的 AWS 账户中的资源和关系。
AWS Fargate	核心。该解决方案使用亚马逊 ECS 上的 AWS Fargate 作为发现任务的计算层。

AWS 服务	描述
AWS Lambda	核心。此解决方案使用无服务器 Lambda 函数以及 Node.js 和 Python 运行时来处理 API 调用。
Amazon Neptune	核心。此解决方案使用 Neptune 作为解决方案发现的资源和关系的主数据存储。
Amazon Simple Storage Service	核心。此解决方案使用 Amazon S3 进行前端和后端存储。
Amazon CloudWatch	支持。该解决方案 CloudWatch 用于在自动案例中收集和可视化实时日志、指标和事件数据。此外，您还可以监控已部署解决方案的资源使用情况和性能问题。
AWS CodeBuild	支持。此解决方案 CodeBuild 用于构建包含发现任务代码的 Docker 容器，并将前端的资产部署到 Amazon S3。
Amazon Cognito	支持。此解决方案使用 Cognito 用户池对用户进行身份验证和授权，以访问解决方案 Web UI。
AWS Systems Manager	支持。该解决方案使用 AWS Systems Manager 来提供应用程序级资源监控，并可视化资源操作和成本数据。
Amazon Virtual Private Cloud	支持。此解决方案使用 VPC 在中启动 Neptune 和 OpenSearch 数据库。
AWS WAF	支持。此解决方案使用 AWS WAF 保护 AppSync API 免受常见漏洞和机器人攻击，这些漏洞和机器人可能会影响可用性、危及安全性或消耗过多资源。
Amazon Athena	可选。如果启用了成本功能，则此解决方案使用 Athena 来查询成本和使用情况报告。

规划您的部署

本节介绍部署解决方案之前的区域、成本、安全性和其他注意事项。

支持的 AWS 区域

该解决方案使用 Amazon Cognito 服务，但该服务目前并非在所有 AWS 区域都可用。要了解按地区划分的 AWS 服务的最新可用性，请参阅 AWS 区域服务列表。

AWS 上的工作负载发现功能可在以下 AWS 区域中使用：

区域名称	
美国东部（弗吉尼亚州北部）	加拿大（中部）
美国东部（俄亥俄州）	欧洲地区（伦敦）
美国西部（俄勒冈州）	欧洲地区（法兰克福）
亚太地区（孟买）	欧洲地区（爱尔兰）
亚太地区（首尔）	欧洲地区（巴黎）
亚太地区（新加坡）	欧洲地区（斯德哥尔摩）
亚太地区（悉尼）	南美洲（圣保罗）
亚太地区（东京）	

AWS 上的工作负载发现功能不适用于以下 AWS 区域：

区域名称	服务不可用
AWS GovCloud （美国东部）	AWS AppSync
AWS GovCloud （美国西部）	AWS AppSync
中国（北京）	Amazon Cognito

区域名称	服务不可用
中国（宁夏）	Amazon Cognito

成本

运行此解决方案时预配置 AWS 服务的费用由您承担。从本次修订开始，在美国东部（弗吉尼亚北部）地区使用单实例部署选项运行此解决方案的成本约为每小时 0.58 美元或每月 425.19 美元。

> **Note**
>
> 在 AWS 云中在 AWS 上运行工作负载发现的成本取决于您选择的部署配置。以下示例提供了美国东部（弗吉尼亚北部）地区单实例和多实例部署配置的成本明细。下表示例中列出的 AWS 服务按月计费。

我们建议通过 AWS Cost Explorer 创建预算，以帮助管理成本。价格可能会发生变化。有关完整详情，请参阅本解决方案中使用的每项 AWS 服务的定价网页。

成本表示例

选项 1：单实例部署（默认）

使用 AWS CloudFormation 模板部署此解决方案时，修改OpensearchMultiAz参数以No部署 OpenSearch 服务域的单个实例，然后将CreateNeptuneReplica参数修改为为 Neptune 数据存储No部署单个实例。单实例部署选项的成本较低，但在可用区出现故障时，它会降低 AWS 上工作负载发现的可用性。

AWS 服务	实例类型	每小时成本 [美元]	每月费用 [美元]
Amazon Neptune	`db.r5.large`	0.348 美元	254.04 美元
亚马逊 OpenSearch 服务	`m6g.large .search`	0.128 美元	93.44 美元
亚马逊 VPC（NAT 网关）	不适用	0.090 USD	65.7 美元

AWS 服务	实例类型	每小时成本 [美元]	每月费用 [美元]
AWS Config	不适用	每项资源 0.003 美元	每项资源 0.003 美元
亚马逊 ECS（AWS Fargate 任务）	不适用	0.02 美元	12.01 美元
Total		0.586 美元	425.19 美元

选项 2：多实例部署

使用 AWS CloudFormation 模板部署此解决方案时，修改OpensearchMultiAz参数以在 OpenSearch 服务域的两个可用区中Yes部署两个实例，并将CreateNeptuneReplica参数修改为在 Neptune 数据存储的两个可用区中Yes部署两个实例。多实例部署选项的运行成本会更高，但在可用区出现故障时，它可以提高 AWS 上工作负载发现的可用性。

AWS 服务	实例类型	每小时成本	每月费用 [美元]
Amazon Neptune	`db.r5.large`	0.696 美元	508.08 美元
亚马逊 OpenSearch 服务	`m6g.large.search`	0.256 美元	186.88 美元
亚马逊 VPC（NAT 网关）	不适用	0.090 USD	65.7 美元
AWS Config	不适用	每项资源 0.003 美元	每项资源 0.003 美元
亚马逊 ECS（AWS Fargate 任务）	不适用	0.02 美元	12.01 美元
Total		1.062	772.67 美元

- 您的最终费用取决于 AWS Config 检测到的资源数量。除了表中提供的金额外，还会为每个记录的资源项目支出 0.003 美元。

> **Important**
>
> Amazon Neptune 和亚马逊 OpenSearch 服务的费用会有所不同，具体取决于您选择的实例类型。

安全性

当您在 AWS 基础设施上构建系统时，安全责任由您和 AWS 共同承担。这种分担责任模式减轻了您的运营负担，因为 AWS 运营、管理和控制包括主机操作系统、虚拟化层和服务运行设施的物理安全在内的组件。有关 AWS 安全的更多信息，请访问 AWS 安全中心。

资源访问权限

IAM 角色

IAM 角色允许客户向 AWS 云上的服务和用户分配精细的访问策略和权限。需要多个角色才能在 AWS 上运行工作负载发现和发现 AWS 账户中的资源。

Amazon Cognito

Amazon Cognito 用于使用短期的强凭证对访问进行身份验证，该证书允许访问 AWS 上工作负载发现所需的组件。

网络访问

Amazon VPC

AWS 上的工作负载发现部署在 Amazon VPC 中，并根据最佳实践进行配置，以提供安全性和高可用性。有关更多详细信息，请参阅您的 VPC 安全最佳实践。VPC 终端节点允许在服务之间进行非互联网传输，并在可用时进行配置。

安全组用于控制和隔离在 AWS 上运行 Workload Discovery 所需的组件之间的网络流量。

我们建议您在部署启动并运行后查看安全组并根据需要进一步限制访问权限。

Amazon CloudFront

此解决方案部署了托管在亚马逊分发的 Amazon S3 存储桶中的 Web 控制台用户界面。 CloudFront通过使用源访问身份功能，只能通过访问此 Amazon S3 存储桶的内容 CloudFront。有关更多信息，请参阅《亚马逊 CloudFront 开发者指南》中的限制对 Amazon S3 来源的访问。

CloudFront 激活其他安全缓解措施，将 HTTP 安全标头附加到每个查看者响应中。有关更多详细信息，请参阅在 CloudFront 响应中添加或删除 HTTP 标头。

此解决方案使用默认 CloudFront 证书，其支持的最低安全协议为 TLS v1.0。要强制使用 TLS v1.2 或 TLS v1.3，必须使用自定义 SSL 证书而不是默认 CloudFront 证书。有关更多信息，请参阅如何将我的 CloudFront 发行版配置为使用 SSL/TLS 证书。

应用程序配置

AWS AppSync

AWS GraphQL 上的工作负载发现 APIs 功能由 AWS AppSync 根据 GraphQL 规范提供请求验证。此外，身份验证和授权是使用 IAM 和 Amazon Cognito 实现的，当用户在网页用户界面中成功进行身份验证时，它们使用 Amazon Cognito 提供的 JWT。

AWS Lambda

默认情况下，Lambda 函数使用最新稳定版本的语言运行时进行配置。不记录任何敏感数据或机密。服务交互是以最低要求的权限进行的。定义这些权限的角色不会在函数之间共享。

亚马逊 OpenSearch 服务

Amazon S OpenSearch ervice 域配置了访问策略，该策略限制访问权限，以阻止向 OpenSearch 服务集群发出的任何未签名请求。这仅限于单个 Lambda 函数。

OpenSearch 服务集群是在激活 node-to-node加密的情况下构建的，以便在现有 OpenSearch 服务安全功能之上再增加一层数据保护。

限额

服务限额（也称为限制）是您的 AWS 账户使用的服务资源或操作的最大数量。

此解决方案中 AWS 服务的配额

请确保此解决方案中实施的每项服务都有足够的限额。有关更多信息，请参阅 AWS 服务限额。

使用以下链接转到该服务的页面。要在不切换页面的情况下查看文档中所有 AWS 服务的服务配额，请改为查看 PDF 中服务终端节点和配额页面中的信息。

Amplify	Amazon ECR
Athena	Lambda
CloudFront	OpenSearch 服务
Cognito	Neptune
Config	Amazon S3
Amazon ECS	

AWS CloudFormation 配额

您的 AWS 账户有 AWS CloudFormation 配额，在此解决方案中启动堆栈时应注意这些配额。通过了解这些限额，可以避免阻碍成功部署此解决方案的限制错误。有关更多信息，请参阅 AWS CloudFormation 用户指南中的 AWS CloudFormation 配额。

AWS Lambda 配额

您的账户的 AWS Lambda 并发执行配额为 1000。如果在有其他工作负载运行和使用 Lambda 的账户中使用该解决方案，则将此配额设置为适当的值。此值是可调整的；有关更多信息，请参阅 AWS Lambda 用户指南中的 A WS Lambda 配额。

> **Note**
>
> 此解决方案需要并发执行配额中的 150 个执行才能在部署该解决方案的账户中可用。如果该账户中可用的执行次数少于 150 个，则 CloudFormation 部署将失败。

Amazon VPC 配额

您的 AWS 账户可以包含五个 VPCs 和两个 Elastic IPs (EIPs)。如果在其他 VPCs 或的账户中使用该解决方案 EIPs，则可能会使您无法成功部署此解决方案。如果您面临达到此配额的风险，则可以按照启动堆栈部分中的步骤提供自己的 VPC 进行部署。有关更多信息，请参阅亚马逊 VPC 用户指南中的亚马逊 VPC 配额。

选择部署账户

如果您要在 AWS 上将 Workload Discovery 部署到 AWS 组织，则该解决方案必须安装在已启用多区域 AWS Config 功能的委托管理员账户中。StackSets

如果您不使用 AWS Organizations，我们建议您将 AWS 上的工作负载发现部署到专门为此解决方案创建的 AWS 专用 AWS 账户中。这种方法意味着 AWS 上的 Workload Discovery 与您的现有工作负载隔离，并提供单一位置来配置解决方案，例如添加用户和导入新区域。跟踪运行解决方案时产生的成本也更容易。

在 AWS 上部署 Workload Discovery 后，您可以从已配置的任何账户中导入区域。

部署解决方案

该解决方案使用 AWS CloudFormation 模板和堆栈来自动部署。该 CloudFormation 模板指定了此解决方案中包含的 AWS 资源及其属性。 CloudFormation 堆栈预置模板中描述的资源。

部署流程概述

> **Note**
>
> 如果您之前在 AWS 上部署了 Workload Discovery，并且想要升级到最新版本，请参阅更新解决方案。

按照本节中的 step-by-step说明配置解决方案并将其部署到您的账户。

部署时间：大约 30 分钟

在启动解决方案之前，请查看本指南中讨论的成本、架构、网络安全和其他注意事项。

> **Important**
>
> 此解决方案包含向 AWS 发送匿名运营指标的选项。我们使用这些数据来更好地了解客户如何使用此解决方案以及相关服务和产品。AWS 拥有通过本次调查收集的数据。数据收集受 AWS 隐私声明的约束。

先决条件

收集部署参数详细信息

在 AWS 上部署工作负载发现之前，请查看亚马逊 OpenSearch 服务相关角色和 AWS Config 的配置详细信息。

验证你是否有 AWSServiceRoleForAmazonOpenSearchService 角色

该部署在亚马逊虚拟私有云（亚马逊 VPC）内创建亚马逊 OpenSearch 服务集群。该模板使用服务相关角色来创建 OpenSearch 服务集群。但是，如果您的账户中已经创建了该角色，请使用现有角色。

要检查您是否已经拥有此角色，请执行以下操作：

1. 登录您计划部署此解决方案的账户的 Identity and Access Managem ent 控制台。
2. 在 Search (搜索) 框中，输入 `AWSServiceRoleForAmazonOpenSearchService`。
3. 如果您的搜索返回了角色，请在启动堆栈时选择No该CreateOpensearchServiceRole参数。

验证 AWS Config 是否已设置

AWS 上的工作负载发现使用 AWS Config 来收集大部分资源配置。部署解决方案或导入新区域时，必须确认 AWS Config 是否已设置好并按预期运行。该AlreadyHaveConfigSetup CloudFormation 参数会通知 AWS 上的工作负载发现是否要设置 AWS Config。

以下代码段摘自 A WS CLI 命令参考。在您打算在 AWS 上部署工作负载发现或导入 AWS 上的工作负载发现的区域中运行该命令。

输入以下命令：

```
aws configservice get-status
```

如果您收到与输出相似的响应，则说明该区域正在运行配置记录器和传送渠道。`Yes`为AlreadyHaveConfigSetup CloudFormation 参数选择。

输出：

```
Configuration Recorders:

name: default
recorder: ON
last status: SUCCESS

Delivery Channels:

name: default
last stream delivery status: SUCCESS
last history delivery status: SUCCESS
last snapshot delivery status: SUCCESS
```

如果您正在配置 AWS CloudFormation StackSets，则必须将此区域包含在已配置 AWS Config 的批次区域中。

在您的账户中验证您的 AWS Config 详细信息

部署将尝试设置 AWS Config。如果您已经在计划在 AWS 上部署或通过 Workload Discovery 发现的账户中使用了 AWS Config，请在部署此解决方案时选择相关参数。此外，要成功部署，请确保您没有限制 AWS Config 扫描的资源。

要检查您当前的 AWS Config 配置，请执行以下操作：

1. 登录 AWS Config 控制台。
2. 选择 “设置”，并确保选中 “记录该区域支持的所有资源” 和 “包括全局资源” 复选框。

验证您的 VPC 配置

如果部署到现有 VPC，请验证您的私有子网是否可以将请求路由到 AWS 服务。

如果您选择在现有 VPC 中部署解决方案，则必须确保 AWS Lambda 上的工作负载发现功能和在您的 VPC 私有子网中运行的 Amazon ECS 任务可以连接到其他 AWS 服务。启用此功能的标准方法是使用 NAT 网关。您可以列出账户中的 NAT 网关，如以下代码示例所示。

```
aws ec2 describe-route-tables --filters Name=association.subnet-id,Values=<private-subnet-id1>,<private-subnet-id2> --query 'RouteTables[].Routes[].NatGatewayId'
```

输出：

```
[
    "nat-1111111111111111",
    "nat-2222222222222222"
]
```

> **Note**
>
> 如果返回的结果少于两个，则子网的 NAT 网关数量不正确。

如果您的 VPC 没有 NAT 网关，则必须对其进行预配置，或者确保为 AWS 部分列出的所有 AWS 服务提供 VPC 终端 APIs节点。

AWS CloudFormation 模板

此解决方案使用 AWS 在 AWS CloudFormation 云中的 AWS 上自动部署工作负载发现。它包括以下 CloudFormation 模板，您可以在部署前下载该模板：

View template

workload-discovery-on-aws.template-使用此模板启动解决方案和所有关联组件。默认配置部署了本解决方案部分的 AWS 服务中的核心和支持解决方案，但您可以自定义模板以满足您的特定需求。

> **Note**
>
> 您可以自定义模板以满足您的特定需求；但是，您所做的任何更改都可能影响升级过程。

启动 堆栈

此自动化 AWS CloudFormation 模板在 AWS 云中的 AWS 上部署工作负载发现。在启动堆栈之前，您必须收集部署参数的详细信息。有关详细信息，请参阅先决条件。

部署时间：大约 30 分钟

1. 登录 A WS 管理控制台并选择按钮启动 `workload-discovery-on-aws.template` AWS CloudFormation 模板。

   Launch solution

2. 默认情况下，该模板在美国东部（弗吉尼亚州北部）区域启动。要在不同的 AWS 区域启动该解决方案，请使用控制台导航栏中的区域选择器。

   > **Note**
   >
   > 此解决方案使用的服务并非在所有 AWS 区域都可用。有关支持的 AWS 区域列表，请参阅支持的 AWS 区域。

3. 在创建堆栈页面上，确认 Amazon S3 URL 文本框中的模板 URL 是否正确，然后选择下一步。
4. 在指定堆栈详细信息页面上，为您的解决方案堆栈分配一个名称。有关命名字符限制的信息，请参阅 A WS Identity and A ccess Management 用户指南中的 IAM 和 AWS STS 配额。

5. 在“参数”下，查看此解决方案模板的参数并根据需要对其进行修改。该解决方案使用以下默认值。

参数	默认值	描述
AdminUserEmailAddress	*<Requires input>*	用于创建第一个用户的电子邮件地址。临时证书将发送到此电子邮件地址。
AlreadyHaveConfigSetup	No	确认您是否已经在部署账户中设置了 AWS Config。有关详细信息，请参阅先决条件。
AthenaWorkgroup	`primary`	启用成本功能后，将用于发出 Athena 查询的工作组。
ApiAllowListedRanges	`0.0.0.0/1,128.0.0.0/1`	以逗号分隔的列表 CIDRs ，用于管理 AppSync GraphQL API 的访问权限。要允许整个互联网，请使用 0.0.0.0/1,128.0.0.0/1。如果将访问限制为特定网关 CIDRs，则还必须包括允许在其私有子网中运行的发现进程 ECS 任务访问互联网的 NAT 网关的 IP 地址（以及子网掩码 /32）。注意：此允许列表不控制对WebUI的访问，仅控制GraphQL API的访问权限。
CreateNeptuneReplica	No	选择是否在单独的可用区中为 Neptune 创建只读副本。选择Yes可以提高弹性，但会增加此解决方案的成本。
CreateOpenSearchServiceRole	`Yes`	确认您是否已经拥有亚马逊 OpenSearch 服务的服务相关角色。有关详细信息，请参阅先决条件。

参数	默认值	描述
NeptuneInstanceClass	db.r5.large	用于托管 Amazon Neptune 数据库的实例类型。您在此处选择的内容会影响运行此解决方案的成本。
OpensearchInstanceType	m6g.large.search	用于您的 OpenSearch 服务数据节点的实例类型。您的选择会影响解决方案的运行成本。
OpensearchMultiAz	No	选择是否创建跨越多个可用区的 OpenSearch 服务集群。选择Yes可以提高弹性，但会增加此解决方案的成本。
CrossAccountDiscovery	SELF_MANAGED	选择是 AWS 上的 Workload Discovery 还是 AWS Organizations 管理账户 该值可以是 SELF_MANAGED 或 AWS_ORGANIZATIONS 。
OrganizationUnitId	<Optional input>	根组织单位 ID。此参数仅在设置CrossAccountDiscovery为时使用AWS_ORGANIZATIONS 。
AccountType	DELEGATED_ADMIN	在 AWS 上安装工作负载发现的 AWS Organizations 账户类型。此参数仅在设置CrossAccountDiscovery为时使用AWS_ORGANIZATIONS 。有关详细信息，请参阅选择部署帐户。

参数	默认值	描述
ConfigAggregatorName	<Optional input>	要使用的 AWS 组织范围的 Config 聚合器。您必须在与该聚合器相同的账户和区域中安装该解决方案。如果将此参数留空，则将创建一个新的聚合器。此参数仅在设置CrossAccountDiscovery为时使用AWS;_ORGANIZATIONS 。
CpuUnits	1 vCPU	CPUs 要为运行发现过程的 Fargate 任务分配的数量。
内存	2048	为运行发现过程的 Fargate 任务分配的内存量。
DiscoveryTaskFrequency	15mins	每次运行发现进程 ECS 任务之间的时间间隔。
最小值NCUs	1	要在 Neptune 集群上设置的最小海王星容量单位 (NCUs)（必须小于或等于最大容量单位）。NCUs如果 DBInstance 类型为，则为必填项db.serverless 。
最大值NCUs	128	NCUs 要在 Neptune 集群上设置的最大值（必须大于或等于最小值 NCUs）。如果 DBInstance 类型为，则为必填项db.serverless 。
VpcId	<Optional input>	供解决方案使用的现有 VPC 的 ID。如果将此参数留空，则将配置一个新的 VPC。

参数	默认值	描述
VpcCidrBlock	<Optional input>	VpcId参数所引用的 VPC 的 VPC 网段。只有在设置了该VpcId参数时才会使用此参数。
PrivateSubnet0	<Optional input>	您要使用的私有子网。只有在设置了该VpcId参数时才会使用此参数。
PrivateSubnet1	<Optional input>	您要使用的私有子网。只有在设置了该VpcId参数时才会使用此参数。
UsesCustomIdentity	No	确认您是否将使用自定义身份提供商，例如 SAML 或 OIDC。
CognitoCustomDomain	<Optional input>	托管应用程序注册和登录页面的 Amazon Cognito 自定义域名的域名前缀。如果您不使用自定义 IdP，请留空，否则必须仅包含小写字母、数字和连字符。
CognitoAttributeMapping	<Optional input>	将 IdP 属性映射到标准和自定义 Cognito 用户池属性。如果您未使用自定义 IdP，请留空，否则必须是有效的 JSON 字符串。
IdentityType	<Optional input>	要使用的身份提供商的类型（`GoogleSAML`、或`OIDC`）。如果您没有使用自定义 IdP，请留空。

参数	默认值	描述
ProviderName	<Optional input>	身份提供者的名称。如果您没有使用自定义 IdP，请留空。
GoogleClientId	<Optional input>	要使用的谷歌客户端 ID。参数仅在设置IdentityType为时使用Google。
GoogleClientSecret	<Optional input>	要使用的谷歌客户端密钥。参数仅在设置IdentityType为时使用Google。
SAMLMetadataURL	<Optional input>	SAML 身份提供商的元数据 URL。参数仅在设置IdentityType为 SAML 时使用。
OIDCClientId	<Optional input>	要使用的 OIDC 客户端 ID。参数仅在设置IdentityType为时使用OIDC。
OIDCClient密钥	<Optional input>	要使用的 OIDC 客户端密钥。参数仅在设置IdentityType为时使用OIDC。
OIDCIssuerURL	<Optional input>	要使用的 OIDC 发行人网址。参数仅在设置IdentityType为时使用OIDC。
OIDCAttributeRequestMethod	GET	要使用的 OIDC 属性请求方法。必须为GET或POST（请参阅 OIDC 提供商或使用默认值）。参数仅在设置IdentityType为时使用OIDC。

6. 选择 Next(下一步)。
7. 在 配置堆栈选项 页面上，请选择 下一步。
8. 在 “查看并创建” 页面上，查看并确认设置。选中确认模板创建 IAM 资源并需要某些功能的复选框。

9. 选择提交以部署堆栈。

您可以在 AWS CloudFormation 控制台的 “状态” 列中查看堆栈的状态。您将在大约 30 分钟后收到 “创建_完成” 状态。

> **Note**
>
> 如果删除，此堆栈将移除所有资源。如果堆栈已更新，它将保留 Amazon Cognito 用户池，以确保配置的用户不会丢失。

部署后配置任务

成功部署 AWS 上的工作负载发现后，完成以下部署后配置任务。

在 Amazon Cognito 中开启高级安全

要启用 Amazon Cognito 的高级安全功能，请按照《Amazon Cog nit o 开发者指南》中关于向用户池添加高级安全功能的说明进行操作。

> **Note**
>
> 在 Amazon Cognito 中激活高级安全功能需要支付额外费用。

创建亚马逊 Cognito 用户

AWS 上的工作负载发现使用 Amazon Cognito 来管理所有用户和身份验证。它会在部署期间为您创建一个用户，并通过 AdminUserEmailAddress 参数中提供的地址发送一封包含临时证书的电子邮件。

要创建其他用户，请执行以下操作：

1. 登录 AWS Cognito 控制台。
2. 选择管理用户池。
3. 选择 WDCognitoUserPool- *<ID-string>*。
4. 在导航窗格的 “常规设置” 下，选择 “用户和群组”。
5. 在用户选项卡上，选择创建用户。
6. 在创建用户框中，为所有必填字段输入值。

表单字段	必填？	描述
用户名	是	您将用于登录 AWS 上的工作负载发现的用户名。
发送邀请	是（仅限电子邮件）	选中后，会发送通知以提醒您输入临时密码。选择 “仅限电

表单字段	必填？	描述
		子邮件”。如果选择短信（默认），则会显示一条错误消息，但用户仍处于创建状态。
临时密码	是	输入临时密码。当用户首次登录 AWS 上的 Workload Discovery 时，他们必须更改此设置。
电话号码	否	输入国际格式的电话号码，例如\+44。确保将电话号码标记为已验证？ 复选框已选中。
电子邮件	是	输入有效的电子邮件地址。确保将电子邮件标记为已验证？复选框已选中。

7. 选择创建用户。

重复此过程，根据需要创建任意数量的用户。

> **Note**
>
> 每个用户对发现的资源都具有相同的访问权限。我们建议在 AWS 上为包含敏感工作负载或数据的账户单独配置工作负载发现部署。这使您可以将访问权限限制为只有需要访问权限的用户。

登录 AWS 上的 “工作负载发现”

成功部署解决方案后，确定提供解决方案网页用户界面的 Amazon CloudFront 分发的 URL。

1. 登录 A WS CloudFormation 控制台。
2. 选择 View ne sted 以显示构成部署的嵌套堆栈。根据您的偏好，嵌套堆栈可能已经显示出来。
3. 在 AWS 堆栈上选择主工作负载发现。
4. 选择 “输出” 选项卡，然后在 “值” 列中选择与WebUiUrl密钥关联的 URL。

5. 在 “登录到” 屏幕上，输入您通过电子邮件收到的登录凭据。然后采取以下行动：
   a. 按照提示更改您的密码。
   b. 使用发送到您的电子邮件的验证码完成账户恢复。

导入区域

> **Note**
>
> 以下部分仅适用于解决方案的帐户发现模式为自我管理的情况。有关在 AWS Organizations 模式下如何发现账户的信息，请参阅 AWS Organizations 账户发现模式部分。

导入区域需要部署特定的基础设施。该基础设施由全球和区域资源组成：

全局-在一个账户中部署一次的资源，并在导入的每个区域重复使用的资源。

- 一个 IAM 角色 (WorkloadDiscoveryRole)

区域-在导入的每个区域中部署的资源。

- AWS Config 交付渠道
- 适用于 AWS Config 的 Amazon S3 存储桶
- 一个 IAM 角色 (ConfigRole)

部署此基础架构有两个选项：

- AWS CloudFormation StackSets （推荐）
- AWS CloudFormation

导入区域

这些步骤将指导您完成导入区域和部署 AWS CloudFormation 模板的过程。

1. 在 AWS 上登录 “工作负载发现”。有关 URL，请参阅登录 AWS 上的工作负载发现。
2. 在导航菜单中，选择账户。

3. 选择 Import（导入）。
4. 选择导入方法：
   a. 使用 CSV 文件@@ 添加账户和区域。
   b. 使用表单@@ 添加账户和区域。

CSV 文件

按以下格式提供包含要导入的区域的逗号分隔值 (CSV) 文件。

```
"accountId","accountName","region"
123456789012,"test-account-1",eu-west-2
123456789013,"test-account-2",eu-west-1
123456789013,"test-account-2",eu-west-2
123456789014,"test-account-3",eu-west-3
```

1. 选择 “上传 CSV”。
2. 找到并打开您的 CSV 文件。
3. 查看 “区域” 表，然后选择 “导入”。
4. 在模式对话框中，下载全球资源模板和区域资源模板。
5. 在相关账户中部署 CloudFormation 模板（请参阅部署 AWS CloudFormation 模板部分）。
6. 部署全球和区域资源模板后，选中两个复选框以确认安装已完成，然后选择导入。

表单

使用以下表单提供要导入的区域：

1. 在账户 ID 中，输入 12 位数的账户 ID 或选择现有的账户 ID。
2. 在账户名称中，输入账户名称或在选择现有账户 ID 时使用预先填充的值。
3. 选择要导入的区域。
4. 选择 “添加” 以填充下方 “区域” 表中的 “区域”。
5. 查看 “区域” 表，然后选择 “导入”。
6. 在模式对话框中，下载全球资源模板和区域资源模板。
7. 在相关账户中部署 CloudFormation 模板（请参阅部署 AWS CloudFormation 模板部分）。
8. 部署全球和区域资源模板后，选中两个复选框以确认安装已完成，然后选择导入。

部署 AWS CloudFormation 模板

每个账户必须部署一次全球资源。从包含已导入 AWS 工作负载发现中的区域的账户导入区域时，请勿部署此模板。如果已导入区域，请按照部署堆栈中的说明配置区域资源。

CloudFormation StackSets 用于跨账户配置全球资源

> **Important**
>
> 首先，完成要在目标账户 StackSets 中激活堆栈集操作的先决条件。

1. 使用管理员账户登录 AWS CloudFormation 控制台。
2. 从导航菜单中选择StackSets。
3. 选择创建 StackSet。
4. 在 “选择模板” 页面的 “权限” 下：
   a. 如果您使用的是 AWS Organizations，请选择服务托管权限或自助服务权限。有关详细信息，请参阅在 AWS 组织 StackSets 中使用。
   b. 如果您不使用 AWS Organizations，请输入执行 StackSets 先决步骤时使用的 IAM 运行角色名称。有关详细信息，请参阅授予自我管理权限。
5. 在 “指定模板” 下，选择 “上传模板文件”。选择`global-resources.template`文件（之前通过 CSV 文件或表单导入区域时下载的），然后选择 “下一步”。
6. 在 “指定 StackSet 详细信息” 页面上，为您指定一个名称 StackSet。有关命名字符限制的信息，请参阅 A WS Identity and A ccess Management 用户指南中的 IAM 和 AWS STS 配额。
7. 在 “参数” 下，查看此解决方案模板的参数并根据需要进行修改。该解决方案使用以下默认值。

字段名称	默认值	描述
AccountId	部署账户 ID	原始部署账户的账户 ID。您必须将此值保留为默认值。

1. 选择下一步。
2. 在 “配置 StackSet 选项” 页面上，选择 “下一步”。

3. 在 “设置部署选项” 页面的 “帐户” 下，在 “账号” 框中输入 IDs 用于部署账户角色的帐户。
4. 在 “指定区域” 下，选择要安装堆栈的区域。
5. 在 “部署选项” 下，选择 “并行”，然后选择 “下一步”。
6. 在查看页面上，选中确认 AWS CloudFormation 可能使用自定义名称创建 IAM 资源的复选框。
7. 选择提交。

用于 CloudFormation StackSets 提供区域资源

> **Important**
>
> 首先，完成要在目标账户 StackSets 中激活堆栈集操作的先决条件。
> 如果您有一些区域安装了 AWS Config，而有些区域未安装，则必须执行两个 StackSet 操作，一个用于安装了 AWS Config 的区域，另一个针对未安装了 AWS Config 的区域。

1. 使用管理员账户登录 AWS CloudFormation 控制台。
2. 从导航菜单中选择StackSets。
3. 选择创建 StackSet。
4. 在 “选择模板” 页面的 “权限” 下：
   a. 如果您使用的是 AWS Organizations，请选择服务托管权限或自助服务权限。有关详细信息，请参阅在 AWS 组织 StackSets 中使用。
   b. 如果您不使用 AWS Organizations，请输入执行 StackSets 先决步骤时使用的 IAM 运行角色名称。有关详细信息，请参阅授予自我管理权限。
5. 在 “指定模板” 下，选择 “上传模板文件”。选择`regional-resources.template`文件（之前通过 CSV 文件或表单导入区域时下载的），然后选择 “下一步”。
6. 在 “指定 StackSet 详细信息” 页面上，为您指定一个名称 StackSet。有关命名字符限制的信息，请参阅 A WS Identity and A ccess Management 用户指南中的 IAM 和 AWS STS 配额。
7. 在 “参数” 下，查看此解决方案模板的参数并根据需要进行修改。该解决方案使用以下默认值。

字段名称	默认值	描述
AccountId	部署账户 ID	原始部署账户的账户 ID。您必须将此值保留为默认值。

字段名称	默认值	描述
AggregationRegion	部署区域	最初部署到的区域。您必须将此值保留为默认值。
AlreadyHaveConfigSetup	No	确认该区域是否已经安装了 AWS Config。如果该区域已经安装了 AWS Config，则设置为 “是”。

1. 选择下一步。
2. 在 “配置 StackSet 选项” 页面上，选择 “下一步”。
3. 在 “设置部署选项” 页面的 “帐户” 下，在 “账号 IDs ” 框中输入要将账户角色部署到的账户。
4. 在 “指定区域” 下，选择要安装堆栈的区域。这将在步骤 6 中输入的所有账户中将堆栈安装到这些区域。
5. 在 “部署选项” 下，选择 “并行”，然后选择 “下一步”。
6. 在查看页面上，选中确认 AWS CloudFormation 可能使用自定义名称创建 IAM 资源的复选框。
7. 选择提交。

使用部署堆栈以配置全球资源 CloudFormation

每个账户必须部署一次全球资源。从包含已导入 AWS 工作负载发现中的区域的账户导入区域时，请勿部署此模板。

1. 登录 A WS CloudFormation 控制台。
2. 选择 “创建堆栈”，然后选择 “使用新资源（标准）”。
3. 在创建堆栈页面的指定模板部分，选择上传模板文件。
4. 选择 “选择文件” 并选择（之前通过 CSV `global-resources.template` 文件或表单导入区域时下载的文件），然后选择 “下一步”。
5. 在指定堆栈详细信息页面上，为您的解决方案堆栈分配一个名称。有关命名字符限制的信息，请参阅 _A WS Identity and Access Management _用户指南中的 IAM 和 AWS STS 配额。
6. 在 “参数” 下，查看此解决方案模板的参数并根据需要进行修改。该解决方案使用以下默认值。

字段名称	默认值	描述
堆栈名称	`workload-discovery`	此 AWS CloudFormation 堆栈的名称。
AccountId	部署账户 ID	原始部署账户的账户 ID。您必须将此值保留为默认值。

1. 选择下一步。
2. 选中确认 AWS CloudFormation 可能使用自定义名称创建 IAM 资源的复选框。
3. 选择创建堆栈。

将在下一个发现过程中扫描新的区域，该过程每隔 15 分钟，例如：
15:00、15:15、15:30、15:30、15:45。

使用部署堆栈以配置区域资源 CloudFormation

1. 登录 A WS CloudFormation 控制台。
2. 选择 “创建堆栈”，然后选择 “使用新资源（标准）”。
3. 在创建堆栈页面的指定模板部分，选择上传模板文件。
4. 选择 “选择文件” 并选择`regional-resources.template`文件（之前通过 CSV 文件或表单导入区域时已下载），然后选择 “下一步”。
5. 在指定堆栈详细信息页面上，为您的解决方案堆栈分配一个名称。有关命名字符限制的信息，请参阅 A WS Identity and A ccess Management 用户指南中的 IAM 和 AWS STS 配额。
6. 在 “参数” 下，查看此解决方案模板的参数并根据需要进行修改。该解决方案使用以下默认值。

字段名称	默认值	描述
AccountId	解决方案部署账户 ID	原始部署账户的账户 ID。必须保留为默认值。
AggregationRegion	解决方案部署区域	最初部署到的区域。必须保留为默认值。

字段名称	默认值	描述
AlreadyHaveConfigSetup	No	确认该区域是否已经安装了 AWS Config。Yes如果该区域已经安装了 AWS Config，则设置为。

1. 选择下一步。
2. 选中确认 AWS CloudFormation 可能使用自定义名称创建 IAM 资源的复选框。
3. 选择创建堆栈。

将在下一个发现过程中扫描新的区域，该过程每隔 15 分钟，例如 15:00、15:15、15:30、15:30、15:45。

验证区域是否已正确导入

1. 登录解决方案的 Web 用户界面（如果页面已加载，则刷新页面）。有关 URL，请参阅登录 AWS 上的工作负载发现。
2. 在左侧导航面板的 “设置” 下，选择 “导入的区域”。

区域、账户名和账户 ID 显示在表格中。“上次扫描” 列显示该区域最后发现的资源。

> **Note**
>
> 如果 “上次扫描” 列的空白时间超过 30 分钟，请参阅调试发现组件。

设置成本功能

成本功能需要手动设置 AWS 成本和使用率报告 (CUR)。按照以下说明，您将：

1. 设置预定的 CUR。
2. 设置 Amazon S3 复制（当 CURs 在部署账户之外时）

在部署账户中创建 AWS 成本和使用率报告

1. 登录您要从中收集成本数据的账户的账单控制台。
2. 在导航菜单的 “账单” 下，选择 “成本和使用情况报告”。
3. 选择 “创建报告”。
4. `workload-discovery-cost-and-usage-`*`<your-workload-discovery-deployment-account-ID>`*用作报告名称。

> **Note**
>
> 您必须遵循此命名约定，因为将部署少量基础架构以方便查询 CURs。

5. 选中 “包括资源” IDs 复选框。

> **Note**
>
> 您必须选中 “包括资源 IDs” 框才能查看成本数据。此 ID 必须与 AWS 上的 Workload Discovery 发现的资源相匹配。

6. 选择下一步。
7. 在配送选项页面上，选择配置 0
8. 选择用于存储 CUR 的 *`<stack-name>`* `-s3buc-costandusagereportbucket-` *`<ID-string>`* Amazon S3 存储桶。选择下一步。
9. 查看政策，选中确认框，然后选择保存。
10. 将报告前缀路径设置为`aws-perspective`。
11. 选择 “每日” 作为时间粒度。
12. 在 “为其启用报告数据集成” 下，选择 Amazon Athena。
13. 选择下一步。
14. 选择 “查看并完成”。

要验证报告的设置是否正确，请检查 Amazon S3 存储桶中是否有测试文件。

> **Note**
>
> 报告最多可能需要 24 小时才能上传到您的存储桶。

在外部账户中创建 AWS 成本和使用率报告

1. 登录您要从中收集成本数据的账户的账单控制台。
2. 在导航菜单的 “成本管理” 下，选择 “成本和使用情况报告”。
3. 选择 “创建报告”。
4. `workload-discovery-cost-and-usage-<your-external-account-ID>`用作报告名称。

> **Note**
>
> 您必须遵循此命名约定，因为将部署少量基础架构以方便查询 CURs。

5. 选中 “包括资源 IDs” 复选框。

> **Note**
>
> 您必须选中 “包括资源 IDs” 框才能查看成本数据。需要此 ID 才能与 AWS 上的 Workload Discovery 发现的资源相匹配。

6. 选择下一步。
7. 在配送选项页面上，选择配置 0
8. 创建一个新的 Amazon S3 存储桶来存储 CURs.
9. 查看政策，选中确认框，然后选择保存。
10. 将报告前缀路径设置为`aws-perspective`。
11. 选择 “每日” 作为时间粒度。
12. 在 “为其启用报告数据集成” 下，选择 Amazon Athena。
13. 选择下一步。
14. 选择 “查看并完成”。要验证报告的设置是否正确，请检查 Amazon S3 存储桶中是否有测试文件。

> **Note**
>
> 报告最多可能需要 24 小时才能上传到您的存储桶。

接下来，设置部署帐户的复制。

设置复制

设置复制到部署期间创建的 Amazon S3 存储桶中。Amazon S3 存储桶采用以下格式：*<stack-name>*-s3buc-costandusagereportbucket-*<ID-string>*。这允许解决方案使用 Amazon Athena 查询存储桶。

1. 在 A mazon S3 控制台中登录包含需要复制的已创建 CUR 的 AWS 账户。
2. 选择在配置 CUR 时创建的 Amazon S3 存储桶。有关更多信息，请查看创建和安排 AWS 成本和使用率报告的第 8 步。
3. 选择管理选项卡。
4. 在复制规则下，选择创建复制规则。
5. 在复制规则配置下的复制规则名称框中，输入描述性规则 ID。
6. 在源存储桶下，选择应用于存储桶中的所有对象以配置规则范围。
7. 在目标下，配置以下内容：
   a. 选择在其他账户中指定存储桶。
   b. 输入账户 ID。
   c. 输入在 AWS 上部署工作负载发现期间创建的存储桶名称的值。您可以按照定位部署资源中的说明进行操作，使用您在首次在 AWS 上部署 Workload Discovery 时指定的逻辑 ID `CostAndUsageReportBucket` 和堆栈名称来找到这一点。
   d. 选中 “将对象所有权更改为目标存储桶所有者” 复选框。
8. 在 IAM 角色下，选择创建新角色。

> **Note**
>
> 复制角色可能已经存在。您可以选择它并确保它具有所需的 S3 复制角色操作。

9. 选择保存。
10. 登录安装了 CUR 的 AWS 管理控制台，导航到 S3 服务页面并选择 `CostAndUsageReportBucket` S3 存储桶。有关详细信息，请参阅查找部署资源。
11. 选择 “管理” 选项卡。
12. 在 “复制规则” 下，从 “操作” 下拉菜单中选择 “接收复制的对象”。
13. 在源存储桶账户设置下：
    a. 输入源存储桶账户 ID。
    b. 选择 “生成策略”。

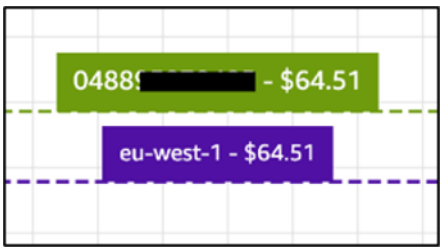
c. 在 “策略” 下，选择 “查看存储桶策略”。

d. 选择包含将对象所有权更改为目标存储桶所有者的权限。

e. 选择 “应用设置”。这使它可以向其复制对象。有关 S3 存储桶策略的示例，请参阅成本存储桶复制策略。

> **Note**
>
> CURs 从多个 AWS 账户进行复制时。您需要确保目标存储桶（在 AWS 上的工作负载发现账户中）的存储桶策略包含您在每个账户中使用的每个 IAM 角色的 ARN。有关更多详细信息，请参阅成本桶复制政策。

当报告存入账户时，成本数据会显示在边界框和各个资源上。



编辑 S3 存储桶生命周期策略

在部署期间，该解决方案在两个存储桶上配置生命周期策略：

- `CostAndUsageReportBucket`
- `AccessLogsBucket`

> **Important**
>
> 这些生命周期策略会在 90 天后从这些存储桶中删除数据。您可以根据自己的任何内部策略编辑生命周期。

监控解决方案

此解决方案使用 MyApplic ations CloudWatch AppInsights，并允许您在 AWS 部署中监控工作负载发现。

myApplications

MyApplications 是 Console Home 的扩展，可帮助您管理和监控在 AWS 上的应用程序的成本、运行状况、安全状况和性能。您可以从 AWS 管理控制台中的一个视图访问账户中的所有应用程序、所有应用程序的关键指标，以及来自多个服务控制台的成本、安全和运营指标的概述和见解。

要在 AWS 上查看 “我的应用程序” 控制面板以发现工作负载，请执行以下操作：

1. 登录 A WS 管理控制台。
2. 在左侧边栏中，选择 myApplications。
3. 在搜索栏`workload-discovery`中键入以查找应用程序。
4. 选择应用程序。

CloudWatch AppInsights

CloudWatch Application Insights 通过识别和设置应用程序资源和技术堆栈中的关键指标、日志和警报，帮助您监控应用程序。它会持续监控指标和日志，以检测和关联异常和错误。为了帮助进行故障排除，它会为检测到的问题创建自动化控制面板，其中包含关联的指标异常情况和日志错误，以及可指出潜在根本原因的其他洞察。

要在 AWS 上查看工作负载发现 CloudWatch AppInsights 控制面板，请执行以下操作：

1. 登录 CloudWatch 控制台。
2. 在左侧边栏中，选择见解、应用程序见解。
3. 选择 “应用程序” 选项卡。
4. 在搜索栏`workload-discovery`中键入即可找到控制面板。
5. 选择仪表板。
6. 选择应用程序。

更新此解决方案

> **Important**
>
> 不支持在 AWS 上将 Workload Discovery 从 v1.x.x 更新到 v2.x.x。我们建议您在安装 v2.x.x 之前卸载此解决方案的 v1.x.x。

要从 2.x.x 部署进行更新，请按照以下步骤操作。

1. 下载该解决方案的 AWS CloudFormation 模板。
2. 登录 A WS CloudFormation 控制台。
3. 使用部署期间提供的名称选择堆栈，然后选择 Update。
4. 在更新堆栈页面上，选择替换当前模板，然后选择上传模板文件，然后上传在步骤 1 中下载的文件。
5. 选择下一步。
6. 在指定堆栈详细信息页面的参数下，查看参数并根据需要对其进行修改。
7. 选择下一步。
8. 在配置堆栈选项页面的堆栈故障选项下，确保将置备失败时的行为单选按钮设置为回滚所有堆栈资源。
9. 选择 Next(下一步)。
10. 在 Review 页面上，审核并确认设置。选中确认模板创建 IAM 资源并需要某些功能的复选框。
11. 选择更新堆栈以部署堆栈。

> **Note**
>
> 如果您在自行管理的账户发现模式下部署了解决方案，则必须按照导入区域部分中的步骤更新部署的全球资源。

故障排除

已知问题解决方案提供了缓解已知错误的说明。如果这些说明无法解决您的问题，请参阅 “联系 AWS Supp ort” 部分，了解如何针对此解决方案提出 AWS Support 案例的说明。

已知问题解决方案

在 AWS 上部署 Workload Discovery 期间和部署后阶段，可能会出现几个常见的配置错误：

> **Note**
>
> 为了便于排除故障，我们建议在 AWS CloudFormation 模板中禁用 “失败时回滚” 功能。您还可以在 AWS 上的工作负载发现部署后配置文档中找到其他疑难解答帮助。

Config 交付渠道错误

问题：部署主 AWS CloudFormation 模板时出现以下错误：

```
Failed to put delivery channel '<stack-name>-DiscoveryImport-<ID-string>-
DeliveryChannel-<ID-string>' because the maximum number of delivery channels:
 1 is reached. (Service: AmazonConfig; Status Code: 400; Error Code:
 MaxNumberOfDeliveryChannelsExceededException; Request ID: 4edc54bc-8c85-4925-
b99d-7ef9c73215b3; Proxy: null)
```

原因：正在将解决方案部署到已启用 AWS Config 的区域。

解决方案：按照先决条件部分中的说明进行操作，将 CloudFormation 参数AlreadyHaveConfigSetup设置为`Yes`，部署解决方案。

部署到现有 VPC 时，搜索解析器堆栈部署超时

问题：置备自定义资源以在 OpenSearch 群集中创建索引的嵌套堆栈超时，并出现以下错误：

```
Embedded stack arn:aws:cloudformation:<region>::stack/<stack-name>-
SearchResolversStack-<ID-string>/<guid> was not successfullycreated: Stack creation
 time exceeded the specified timeout
```

原因：作为 CloudFormation 参数提供的私有子网无法路由到 S3（自定义资源必须使用预签名 URL 将其执行结果写入 S3 存储桶）。这通常有两个原因：

1. 私有子网没有关联的 NAT 网关，因此无法访问互联网。
2. 私有子网使用 VPC 终端节点而不是 NAT 网关，并且 S3 网关终端节点配置不正确。

解决方案：

1. 根据文档，在 VPC 中配置 NAT 网关，允许在私有子网中运行的任务访问互联网，使用 CloudFormation 或 AWS CLI。
2. 确保已根据文档更新了 S3 VPC 终端节点的子网路由表。

导入账户后未发现资源

问题：账户已通过 Web UI 导入，但在发现过程运行后似乎未发现任何资源。

原因：最可能的原因如下，

1. 当CrossAccountDiscovery CloudFormation 参数设置为时`SELF_MANAGED`，全球资源 CloudFormation 模板尚未部署。
2. 当CrossAccountDiscovery CloudFormation 参数设置为`AWS_ORGANIZATIONS`：未发现一个或多个帐户，且角色状态列中有 “未部署” 条目时。这意味着使用自动部署全球资源模板时存在问题 StackSets。
3. 发现进程 ECS 任务内存不足。导入大量账户或资源时会发生这种情况。用户界面中的 “上次发现” 列的值将大于DiscoveryTaskFrequency CloudFormation 参数中指定的值（默认值为 15 分钟），并且 ECS 控制台中将出现内存不足错误。

解决方案：

1. 根据文档，在所需的账户中部署全球资源模板。
2. 前往WdGlobalResources StackSet 已部署 Workload Discovery 的区域，检查部署失败的堆栈实例中的错误。
3. CloudFormation 将 Memory 参数更新为更大的值：从 double 开始并不断增加，直到错误停止。

> **Note**
>
> 只有特定的 CPU 单位和内存值组合才有效，因此您可能还必须更新CpuUnits CloudFormation 参数。完整的组合列表在 ECS 文档中列出。

在特定账户中仅发现非 AWS 配置资源

问题：解决方案发现的唯一资源类型是 “支持的资源” 部分表格中列出的资源类型。

原因：此问题最常见的原因是，

1. 当CrossAccountDiscovery CloudFormation 参数设置为时SELF_MANAGED，区域资源 CloudFormation 模板尚未部署到要发现的每个账户的区域。
2. 当该CrossAccountDiscovery CloudFormation 参数设置为时SELF_MANAGED，区域资源 CloudFormation 模板已部署在多个未启用 Config 但 CloudFormation 参数AlreadyHaveConfigSetup被错误设置为的账户所在的区域。Yes
3. 当CrossAccountDiscovery CloudFormation 参数设置为时AWS_ORGANIZATIONS，AWS Config 不会在要发现的每个账户的区域中启用。在AWS_ORGANIZATIONS模式下，您负责根据组织的政策启用 Config。

解决方案：

1. 根据文档，在所需账户中部署区域资源模板。
2. 删除之前部署的区域资源堆栈（否则 AWS Config 将处于不一致状态），然后在 CloudFormation 参数AlreadyHaveConfigSetup设置为No的情况下重新部署。
3. 在要发现的每个账户所在的区域启用 AWS Config。

联系 AWS Support

如果您有 AWS 开发者支持、AWS 商业支持或 AWS 企业支持，则可以使用支持中心获取有关此解决方案的专家帮助。以下部分提供了说明。

创建案例

1. 登录 Su pport Center。

2. 选择创建案例。

我们能帮上什么忙？

1. 选择 “技术”。
2. 对于 “服务”，选择 “解决方案”。
3. 在 “类别” 中，选择 “其他解决方案”。
4. 在 “严重性” 中，选择与您的用例最匹配的选项。
5. 当您输入 “服务”、“类别” 和 “严重性” 时，界面会填充常见疑难解答问题的链接。如果您无法通过这些链接解决问题，请选择下一步：其他信息。

其他信息

1. 在 “主题” 中，输入总结您的问题或问题的文本。
2. 在描述中，详细描述问题。
3. 选择 “附加文件”。
4. 附上 AWS Support 处理请求所需的信息。

帮助我们更快地解决您的问题

1. 输入所需的信息。
2. 选择下一步：立即解决或联系我们。

立即解决或联系我们

1. 查看 “立即解决” 解决方案。
2. 如果您无法使用这些解决方案解决问题，请选择 “联系我们”，输入所需信息，然后选择 “提交”。

卸载此解决方案

要卸载该解决方案，请使用 AWS 管理控制台或 AWS 命令行界面 (AWS CLI) Line CLI。首先，停止 Amazon ECS 集群中所有正在运行的任务。否则，堆栈删除可能会失败。

使用 AWS 管理控制台

1. 登录 A WS CloudFormation 控制台。
2. 使用部署期间提供的名称选择堆栈。
3. 选择删除堆栈。

使用 AWS 命令行界面

确定 AWS CLI 在您的环境中是否可用。有关安装说明，请参阅 AWS CLI 用户指南中的 AWS 命令行界面是什么。

确认 AWS CLI 可用后，运行以下命令：

```
$ aws cloudformation delete-stack --stack-name <customer-defined-stack-name>
```

开发人员指南

本节提供解决方案的源代码和其他自定义设置。

源代码

访问 AWS GitHub 存储库上的 Workload Discovery，下载此解决方案的模板和脚本，并与其他人共享您的自定义设置。

查找部署资源

按照以下步骤查找部署到您账户中的资源。

1. 登录 A WS CloudFormation 控制台。
2. 选择您在其中部署解决方案的区域。

   根据此帐户的使用情况，它可能包含用于不同工作负载的多个堆栈。将有一个主堆栈，其名称与部署期间提供的名称相同，其下方会有多个嵌套堆栈。
3. 选择每个堆栈以访问使用该模板部署的资源。
4. 选择 “资源” 选项卡，然后选择相关资源的 “物理 ID” 链接，即可在其相应的服务控制台中查看该资源。

   如果您知道资源的逻辑 ID，也可以使用表格上方的搜索栏进行搜索。

支持的资源

该解决方案支持 AWS Config 支持的所有资源类型，如下所示。下表包含 AWS 上的 Workload Discovery 发现的 AWS Config 不支持的支持资源。相关的 AWS 文档清单中提供了详细信息。

资源类型	源	描述
AWS::APIGateway::Authorizer	SDK	获取授权者
AWS::ApiGateway::Resource	SDK	获取资源

资源类型	源	描述
AWS::ApiGateway::Method	SDK	获取方法
AWS::Cognito::UserPool	SDK	describeUserPool
AWS::ECS::Task	SDK	describe-tasks
AWS::EKS::Nodegroup	SDK	描述 NodeGroup
AWS::DynamoDB::Stream	SDK	describeSt
AWS:: IAM:: 政策 AWSManaged	SDK	getAccountAuthorization详细信息
AWS::ElasticLoadBalancingV2 ::TargetGroup	SDK	describeTargetGroups
AWS::EC2::Spot	SDK	describeSpotInstance请求
AWS::EC2::SpotFleet	SDK	describeSpotFleet请求

AWS Organiations 账户发现模式

当 AWS 上的工作负载发现部署在 AWS 组织中时，账户的发现不再通过解决方案的 Web 用户界面进行管理。在这种情况下，您无需管理 CloudFormation 模板的部署即可发现账户。

相反，该解决方案使用 AWS 组织范围内的 AWS Config 聚合器来发现组织中所有启用了 AWS Config 的账户中的资源。

对于 AWS Config 不支持的资源类型，该解决方案使用 AWS 在组织中的每个账户中自动部署一个 IA CloudFormation StackSets M 角色。此角色允许发现过程在组织的所有账户中调用 SDK 来发现这些补充资源。

此配置 StackSet 为在添加到组织的所有新账户中自动部署该角色，并从从组织中删除的所有账户中删除该角色。

> **Note**
>
> 无法将堆栈实例部署 StackSet 到管理账户。如果您希望 Workload Discovery 发现此账户，则必须使用 CloudFormation 部署堆栈以配置全球资源 CloudFormation部分中描述的标准 AWS 部署方法部署全球资源模板。

亚马逊 S3 复制角色操作

用于执行复制的 IAM 角色需要具有以下操作：

s3：ReplicateObject
s3：ReplicateDelete
s3：ReplicateTags
s3：ObjectOwnerOverrideToBucketOwner
s3：ListBucket
s3：GetReplicationConfiguration
s3：GetObjectVersionForReplication
s3：GetObjectVersionAcl
s3：GetObjectVersionTagging
s3：GetObjectRetention
s3：GetObjectLegalHold

要验证角色是否具有复制角色的操作，请执行以下操作：

1. 在 S3 复制向导中复制角色名称的名称。
2. 使用您要设置复制的账户登录 IAM 控制台。
3. 将角色名称粘贴到 “搜索 IAM” 框中。
4. 从列表中选择最上面的项目。这是将要使用的 IAM 角色。

5. 在权限策略下，展开托管策略。
6. 确保该策略具有上表中详述的操作。

S3 存储桶策略

以下是 S3 存储桶策略的示例，该策略允许 CURs 上传到存储桶，同时允许外部账户将对象复制到存储桶。您需要将每个外部 AWS 账户的 IAM 角色添加到此策略中，以授予进行复制的权限。

```
   {
      "Version":"2012-10-17",
      "Id":"",
      "Statement":[
          {
            "Sid":"Set permissions for objects"
            "Effect":"Allow",
            "Principal":{
                "AWS":"arn-of-role-selected-in-replication-setup-in-source-account"
          },
      "Action":["s3:ReplicateObject",
      "s3:ReplicateDelete"],
"s3:ObjectOwnerOverrideToBucketOwner",
        "Resource":"arn:aws:s3:::destination-bucket-name/*"
      },
      {
          "Sid":"Set permissions on bucket",
          "Effect":"Allow",
          "Principal":{
                "AWS":"arn-of-role-selected-in-replication-setup-in-source-account"
      },

      "Action":["s3:GetBucketVersioning",
"s3:PutBucketVersioning"],
        "Resource":"arn:aws:s3:::destination-bucket-name "
      },
      {
          "Sid": "Stmt1335892150622",
          "Effect": "Allow",
          "Principal": {
              "Service": "billingreports.amazonaws.com"
          },
          "Action": [
              "s3:GetBucketAcl",
```

```
            "s3:GetBucketPolicy"
         ],
        "Resource": "arn:aws:s3:::destination-bucket-name"
    },
    {

        "Sid": "Stmt1335892526596",
        "Effect": "Allow",
        "Principal": {
            "Service": "billingreports.amazonaws.com"
        },
        "Action": "s3:PutObject",
        "Resource": "arn:aws:s3:::destination-bucket-name/*"

      }
  ]
}
```

AWS APIs

如先决条件中所述，如果您要将解决方案部署到现有 VPC，则必须可以从您的私有子网访问以下服务。

API Gateway

- GetAuthorizers
- GetIntegration
- GetMethod
- GetResources
- GetRestApis

Cognito

- DescribeUserPool

配置

- BatchGetAggregateResourceConfig

- DescribeConfigurationAggregators
- ListAggregateDiscoveredResources
- SelectAggregateResourceConfig

DynamoDB Streams

- DescribeStream

Amazon EC2

- DescribeInstances
- DescribeSpotFleetRequests
- DescribeSpotInstanceRequests
- DescribeTransitGatewayAttachments

亚马逊 Elastic Load Balancer

- DescribeLoadBalancers
- DescribeListeners
- DescribeTargetGroups
- DescribeTargetHealth

Amazon Elastic Kubernetes Service

- DescribeNodegroup
- ListNodegroups

IAM

- GetAccountAuthorizationDetails
- ListPolicies

Lambda

- GetFunction
- GetFunctionConfiguration
- ListEventSourceMappings

OpenSearch 服务

- DescribeDomains
- ListDomainNames

组织

- ListAccounts
- ListAccountsForParent
- ListOrganizationalUnitsForParent
- ListRoots

Amazon Simple Notification Service

- ListSubscriptions

Amazon Security Token Service

- AssumeRole

参考

本节包含有关用于收集该解决方案的独特指标的可选功能的信息，以及为该解决方案做出贡献的构建者列表。

匿名数据收集

此解决方案包含向 AWS 发送匿名运营指标的选项。我们使用这些数据来更好地了解客户如何使用此解决方案以及相关服务和产品。激活后，它将收集以下信息并发送到 AWS：

- 解决方案 ID-AWS 解决方案标识符
- 唯一 ID (UUID)-为每个部署随机生成的唯一标识符
- 时间戳-数据收集时间戳
- 已启用成本功能-有关用户是否在使用成本功能的信息
- 账户数量-用户在部署中加入的账户数量
- 逻辑示意图数量-每次部署中创建的逻辑示意图数量
- 资源数量-在所有已登录账户中发现的资源数量

通过本次调查收集的数据归AWS所有。数据收集受 隐私声明的约束。要选择退出此功能，请在启动 AWS CloudFormation 模板之前完成以下步骤。

1. 将 AWS CloudFormation 模板下载到您的本地硬盘。
2. 使用文本编辑器打开 AWS CloudFormation 模板。
3. 从以下地址修改 AWS CloudFormation 模板映射部分：

```
Mappings:
  Solution:
    Metrics:
      CollectAnonymizedUsageMetrics: 'true'
```

更改为：

```
Mappings:
  Solution:
    Metrics:
```

```
      CollectAnonymizedUsageMetrics: 'false'
```

1. 登录 A WS CloudFormation 控制台。
2. 选择创建堆栈。
3. 在创建堆栈页面的指定模板部分，选择上传模板文件。
4. 在上传模板文件下，选择选择文件，然后从本地驱动器中选择编辑过的模板。
5. 选择 “下一步”，然后按照启动堆栈中的步骤进行操作。

贡献者

- Mohsan Jaffery
- 马修·鲍尔
- Stefano Vozza
- 康纳·柯克帕特里克
- Chris Deigan
- 尼克·李
- Tim Mekari

修订

出版日期：二零二零年九月。有关更新，请参阅存储库中的 changelog.md 文件。 GitHub

请参阅存储库中的 changelog.md 文件。 GitHub

版权声明

客户有责任对本文档中的信息进行单独评测。本文档：(a) 仅供参考，(b) 代表当前的 AWS 产品和实践，如有更改，恕不另行通知，以及 (c) AWS 及其关联公司、供应商或许可方未做出任何承诺或保证。AWS 产品或服务 “按原样” 提供，不附带任何形式的担保、陈述或条件，无论是明示还是暗示。AWS 对其客户承担的责任和义务受 AWS 协议制约，本文档不是 AWS 与客户直接协议的一部分，也不构成对该协议的修改。

该解决方案根据 Apache 许可证（版本 2.0）的条款进行许可。

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。