實作指南

AWS 上的工作負載探索

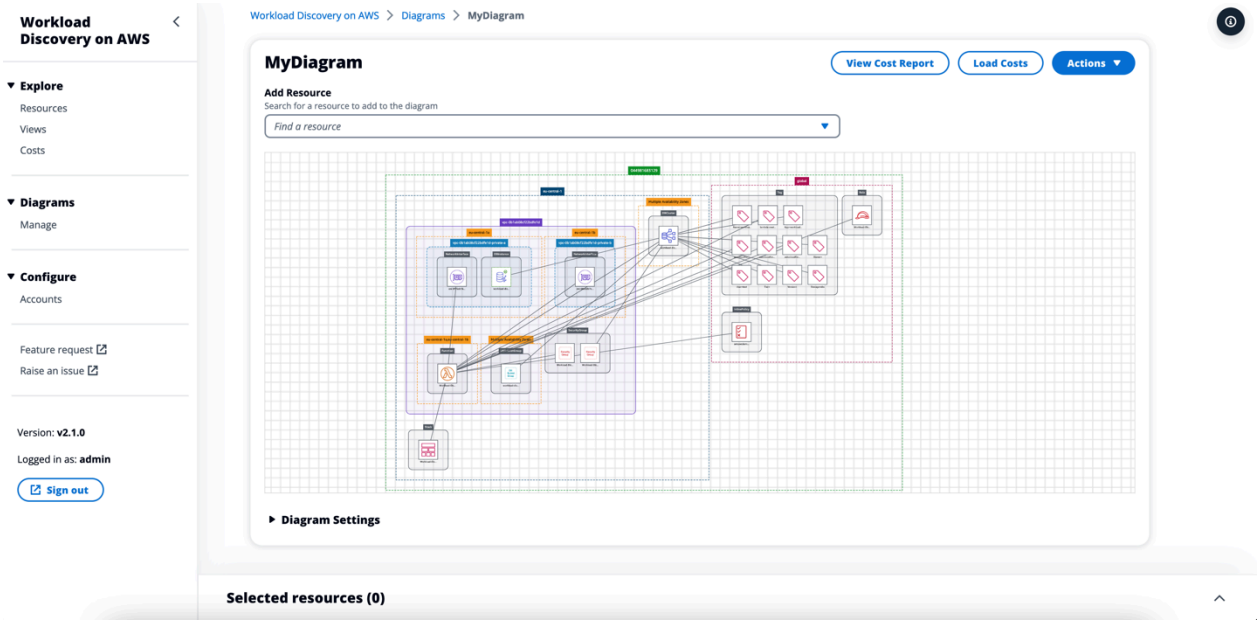
AWS 上的工作負載探索: 實作指南

Table of Contents

部署可自動產生 AWS 雲端工作負載架構圖的視覺化工具

監控 Amazon Web Services (AWS) 雲端工作負載是維護營運運作狀態和效率的關鍵。不過，追蹤 AWS 資源及其之間的關係可能是一項挑戰。AWS 上的工作負載探索是一種視覺化工具，可在 AWS 上自動產生工作負載的架構圖。您可以使用此解決方案，根據 AWS 的即時資料來建置、自訂和共用詳細的工作負載視覺化。

此解決方案的運作方式是維護您帳戶和區域的 AWS 資源庫存、它們之間的映射關係，以及在 Web 使用者介面 (Web UI) 中顯示它們。變更資源時，AWS 上的工作負載探索會在 AWS 管理主控台中提供資源的連結，以節省時間。



AWS 上工作負載探索產生的架構圖範例

此實作指南說明在 AWS 雲端中部署工作負載探索的架構考量和組態步驟。它包含 AWS CloudFormation 範本的連結，該範本會使用 AWS 安全與可用性最佳實務，啟動並設定部署此解決方案所需的 AWS 服務。

在其環境中實作 AWS 解決方案上工作負載探索的目標對象包括解決方案架構師、商業決策者、DevOps 工程師、資料科學家和雲端專業人員。

使用此導覽表快速找到這些問題的答案：

如果您想要 . . .	讀取 . . .
了解執行此解決方案的成本。	成本

如果您想要 . . .	讀取 . . .
在美國東部（維吉尼亞北部）區域執行此解決方案的估計成本為每月 425.19 USD。	
了解此解決方案的安全考量。	安全性
了解如何規劃此解決方案的配額。	配額
了解哪些 AWS 區域支援此解決方案。	支援的 AWS 區域
檢視或下載此解決方案中包含的 AWS CloudFormation 範本，以自動部署此解決方案的基礎設施資源（「堆疊」）。	AWS CloudFormation 範本
存取原始碼。	GitHub 儲存庫

功能和優勢

AWS 上的工作負載探索提供下列功能：

使用近乎即時的資料建置架構圖

AWS 上的工作負載探索會每 15 分鐘掃描一次您的帳戶，以確保您建立的圖表是工作負載的準確且最新表示。

在一個位置檢視來自多個帳戶和區域的資源

解決方案會在集中式圖形資料庫中維護您 AWS 帳戶和區域中的 AWS 資源庫存，讓您可以在單一 UI 中探索多個帳戶和區域及其彼此之間的關係。

AWS Organizations 整合

使用 AWS Organizations 部署解決方案時，AWS 上的工作負載探索會自動探索組織中所有支援的資源。在此組態中，不需要直接管理帳戶特定 CloudFormation 範本的部署，即可讓這些帳戶可供探索。

整理工作負載的成本資料

啟用時，成本功能可讓您依成本搜尋帳戶中的資源，並將找到的資源新增至圖表。您也可以將成本資料新增至現有的圖表。

匯出至 diagrams.net （ 先前為 draw.io)

AWS 上的工作負載探索可以匯出圖表，以便您可以使用此第三方繪製軟體進一步註釋圖表。

與 AWS Service Catalog AppRegistry 和 Application Manager 整合，AWS Systems Manager 的功能

此解決方案包含 Service Catalog AppRegistry 資源，可將解決方案的 CloudFormation 範本及其基礎資源註冊為 Service Catalog AppRegistry 和 Application Manager 中的應用程式。透過此整合，您可以集中管理解決方案的資源，並啟用應用程式搜尋、報告和管理動作。

使用案例

設計和安全性審查

使用此解決方案來產生架構圖表，以驗證工作負載的實作是否符合提議的設計。

探索並記錄現有的工作負載

建立架構圖，以探索存在很少文件或手動部署而沒有基礎設施做為程式碼的工作負載。

視覺化成本

為您的架構圖產生成本報告，其中包含預估成本的概觀。

概念和定義

本節說明關鍵概念並定義此解決方案特有的術語：

資源

AWS 資源，例如 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 AWS Lambda 函數。

關係

兩個資源之間的連結，例如 AWS Identity and Access Management (IAM) 角色和相關聯的 AWS Lambda 函數。

資源類型

資源的分類類別。一律遵循 CloudFormation 命名慣例，例如 `AWS::Lambda::Function`。

探索

解決方案啟動的程序，以映射您 AWS 帳戶和區域中的資源及其關係。

帳戶探索模式

探索帳戶並將其新增至解決方案的方法：透過 AWS 使用者介面上的工作負載探索自我管理，或委派給 AWS Organizations。

> **Note**
>
> 如需 AWS 術語的一般參考，請參閱 AWS 詞彙表。

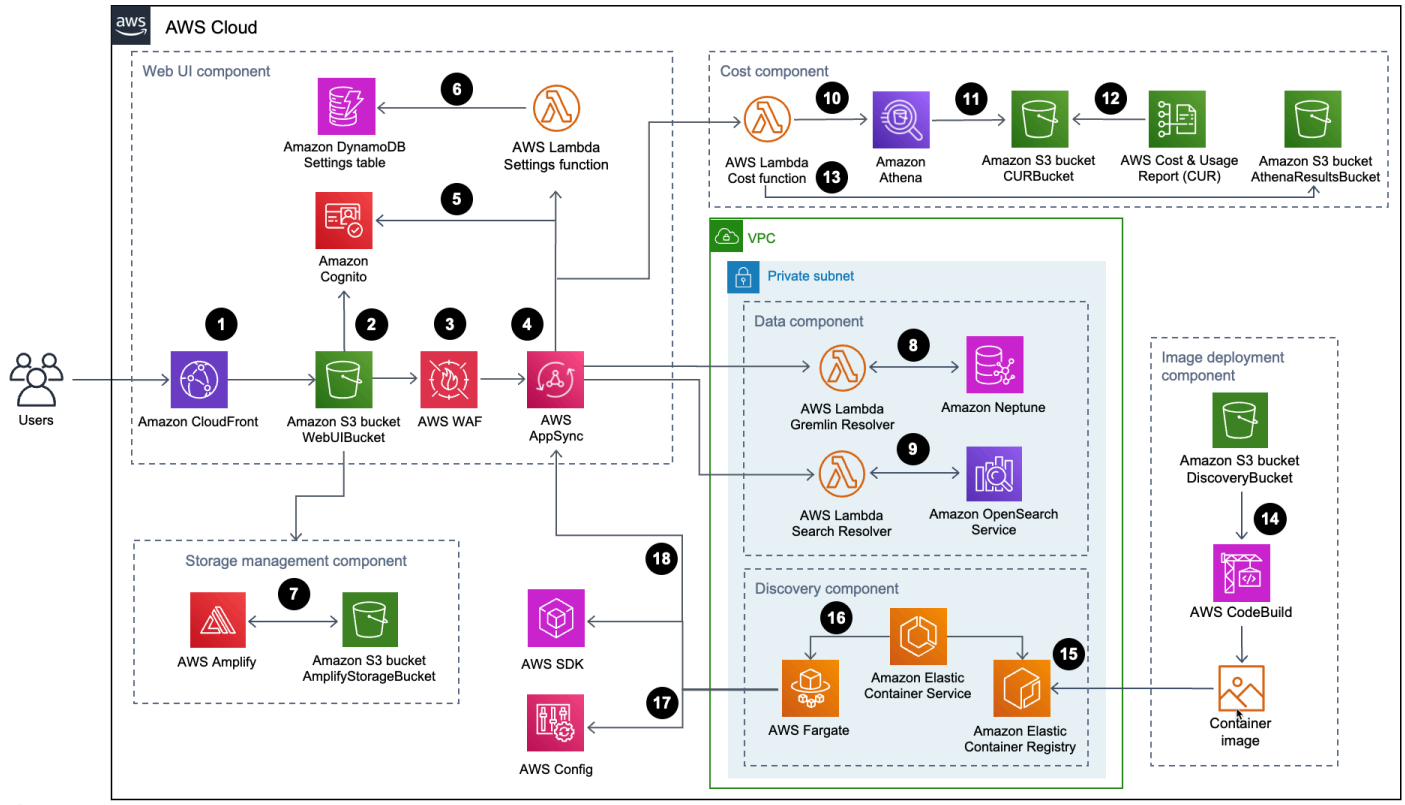
架構概觀

本節提供使用此解決方案部署之元件的參考實作架構圖。

架構圖

使用預設參數部署此解決方案會在 AWS 雲端中建置下列環境。

AWS 架構上的工作負載探索



使用 AWS CloudFormation 範本部署之解決方案元件的高階程序流程如下：

1. HTTP Strict-Transport-Security (HSTS) 會將安全標頭新增至來自 Amazon CloudFront 分發的每個回應。
2. Amazon Simple Storage Service (Amazon S3) 儲存貯體託管與 Amazon CloudFront 一起分佈的 Web UI。Amazon Cognito 會驗證使用者對 Web UI 的存取。
3. AWS WAF 可保護 AppSync API，避免可能影響可用性、危及安全性或消耗過多資源的常見漏洞和機器人。

4. AWS AppSync 端點允許 Web UI 元件請求資源關係資料、查詢成本、匯入新的 AWS 區域和更新偏好設定。AWS AppSync 也允許探索元件將持久性資料存放在解決方案的資料庫中。
5. AWS AppSync 使用 Amazon Cognito 佈建的 JSON Web Token (JWTs) 來驗證每個請求。
6. `Settings` AWS Lambda 函數會保留匯入至 Amazon DynamoDB 的區域和其他組態。
7. 解決方案會部署 AWS Amplify 和 Amazon S3 儲存貯體做為儲存管理元件，以存放使用者偏好設定和儲存的架構圖。
8. 資料元件使用 `Gremlin Resolver` AWS Lambda 函數從 Amazon Neptune 資料庫查詢和傳回資料。
9. 資料元件使用 `Search Resolver` Lambda 函數來查詢資源資料並將其保留到 Amazon OpenSearch Service 網域。
10. `Cost` Lambda 函數使用 Amazon Athena 查詢 AWS 成本和用量報告 (AWS CUR)，以提供預估的成本資料給 Web 使用者介面。
11. Amazon Athena 會在 AWS CUR 上執行查詢。
12. AWS CUR 會將報告交付至 `CostAndUsageReportBucket` Amazon S3 儲存貯體。
13. `Cost` Lambda 函數會將 Amazon Athena 結果存放在 `AthenaResultsBucket` Amazon S3 儲存貯體中。
14. AWS CodeBuild 會在映像部署元件中建置探索元件容器映像。
15. Amazon Elastic Container Registry (Amazon ECR) 包含映像部署元件提供的 Docker 映像。
16. Amazon Elastic Container Service (Amazon ECS) 會管理 AWS Fargate 任務，並提供執行任務所需的組態。AWS Fargate 每 15 分鐘執行一次容器任務，以重新整理庫存和資源資料。
17. AWS Config 和 AWS 開發套件呼叫可協助探索元件維護匯入區域的資源資料庫存，然後將其結果存放在資料元件中。
18. AWS Fargate 任務會將 AWS Config 和 AWS 開發套件呼叫的結果保留在 Amazon Neptune 資料庫和 Amazon OpenSearch Service 網域中，並搭配對 AppSync API 的 API 呼叫。

AWS Well-Architected 設計考量事項

此解決方案使用 AWS Well-Architected Framework 的最佳實務，協助客戶在雲端設計及操作可靠、安全、有效率且符合成本效益的工作負載。

本節說明 Well-Architected Framework 的設計原則和最佳實務如何讓此解決方案受益。

卓越營運

我們利用卓越營運支柱的原則和最佳實務來建構此解決方案，以受益於此解決方案。

- 使用 CloudFormation 將定義為基礎設施的 資源定義為程式碼。
- 解決方案會將指標推送至 Amazon CloudWatch，以提供可觀測性的基礎設施、Lambda 函數、Amazon ECS 任務、AWS S3 儲存貯體，以及其餘的解決方案元件。

安全

我們利用安全支柱的原則和最佳實務來建構此解決方案，以受益於此解決方案。

- Amazon Cognito 會驗證並授權 Web UI 應用程式使用者。
- 解決方案使用的所有角色都遵循最低權限存取。換句話說，它們只包含所需的最低許可，以便服務可以正常運作。
- 靜態資料和傳輸資料會使用存放在 AWS Key Management Service (AWS KMS) 中的金鑰加密，這是專用金鑰管理存放區。
- 登入資料有短暫的過期時間，並遵循強式密碼政策。
- AWS AppSync 安全性 GraphQL 指令可精細控制前端和後端可叫用的操作。
- 記錄、追蹤和版本控制會在適用時開啟。
- 自動修補 (次要版本) 和快照建立會在適用時開啟。
- 根據預設，網路存取是私有的，Amazon Amazon Virtual Private Cloud (Amazon VPC) 端點會在可用時開啟。

可靠性

我們利用可靠性支柱的原則和最佳實務來建構此解決方案，以受益於此解決方案。

- 解決方案會盡可能使用 AWS 無伺服器服務，以確保高可用性和從服務故障中復原。
- 所有運算處理都使用 Lambda 函數或 AWS Fargate 上的 Amazon ECS。
- 所有自訂程式碼都使用 AWS 開發套件，並在用戶端調節請求，以防止達到 API 速率配額。

效能效率

我們使用效能效率支柱的原則和最佳實務來建構此解決方案，以受益於此解決方案。

- 解決方案盡可能使用 AWS 無伺服器架構。這可免除管理實體伺服器的操作負擔。
- 該解決方案可以在支援此解決方案中使用的 AWS 服務的任何區域中啟動，例如：AWS Lambda、Amazon Neptune、AWS AppSync、Amazon S3 和 Amazon Cognito。
- 在支援的區域中，Amazon Neptune 無伺服器可讓您執行並立即擴展圖形工作負載，而不需要管理和最佳化資料庫容量。
- 解決方案使用全局的受管服務，以減少資源佈建和管理的操作負擔。

成本最佳化

我們利用成本最佳化支柱的原則和最佳實務來建構此解決方案，以受益於此解決方案。

- AWS Fargate 上的 AWS ECS 只會使用 Lambda 函數進行運算，而且只會根據使用量收費。
- Amazon DynamoDB 會隨需擴展容量，因此您只需支付使用的容量。

永續性

我們使用永續性支柱的原則和最佳實務來建構此解決方案，以受益於此解決方案。

- 解決方案會盡可能使用受管和無伺服器服務，將後端服務對環境的影響降至最低。

架構詳細資訊

本節說明構成此解決方案的元件和 AWS 服務，以及這些元件如何一起運作的架構詳細資訊。

身分驗證機制

AWS 上的工作負載探索會使用 Amazon Cognito 使用者集區進行 UI 和 AWS AppSync 身分驗證。驗證後，Amazon Cognito 會提供 JSON Web Token (JWT) 給 Web UI，該 UI 將隨所有後續 API 請求一起提供。如果未提供有效的 JWT，API 請求將會失敗並傳回 HTTP 403 禁止的回應。

支援的資源

如需 AWS 上工作負載探索可在您的帳戶和區域中探索的 AWS 資源類型清單，請參閱支援的資源。

AWS 架構圖管理上的工作負載探索

您可以使用 Web UI 在 AWS 架構圖上儲存工作負載探索，其中可以執行建立、讀取、更新和刪除 (CRUD) 操作。AWS Amplify 儲存 API 可讓 AWS 上的工作負載探索將架構圖存放在 Amazon S3 儲存貯體中。有兩種層級的許可可用：

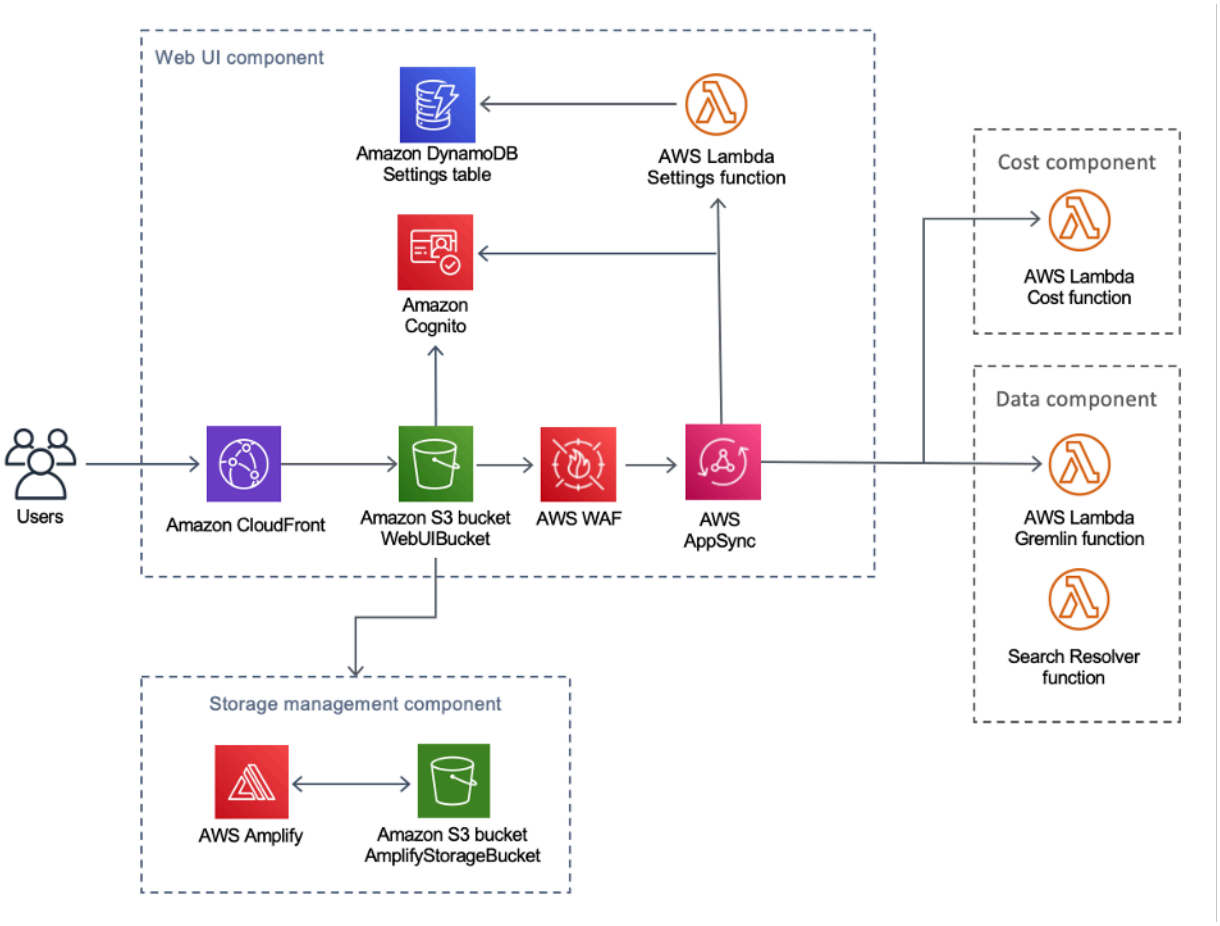
- 所有使用者 - 允許部署中 AWS 使用者的工作負載探索可見 AWS 架構圖上的工作負載探索。使用者可以下載和編輯這些圖表。
- 您 - 允許只有建立者才能看見 AWS 架構圖上的工作負載探索。其他使用者將無法檢視這些使用者。

Web UI 和儲存體管理

我們使用 React 開發 Web UI。Web UI 提供前端主控台，允許使用者與 AWS 上的工作負載探索互動。

Amazon CloudFront 設定為將安全標頭附加到 Web UI 的每個 HTTP 請求。這提供了多一層的安全性，可防範跨網站指令碼 (XSS) 等攻擊。

AWS Web UI 上的工作負載探索和儲存管理元件

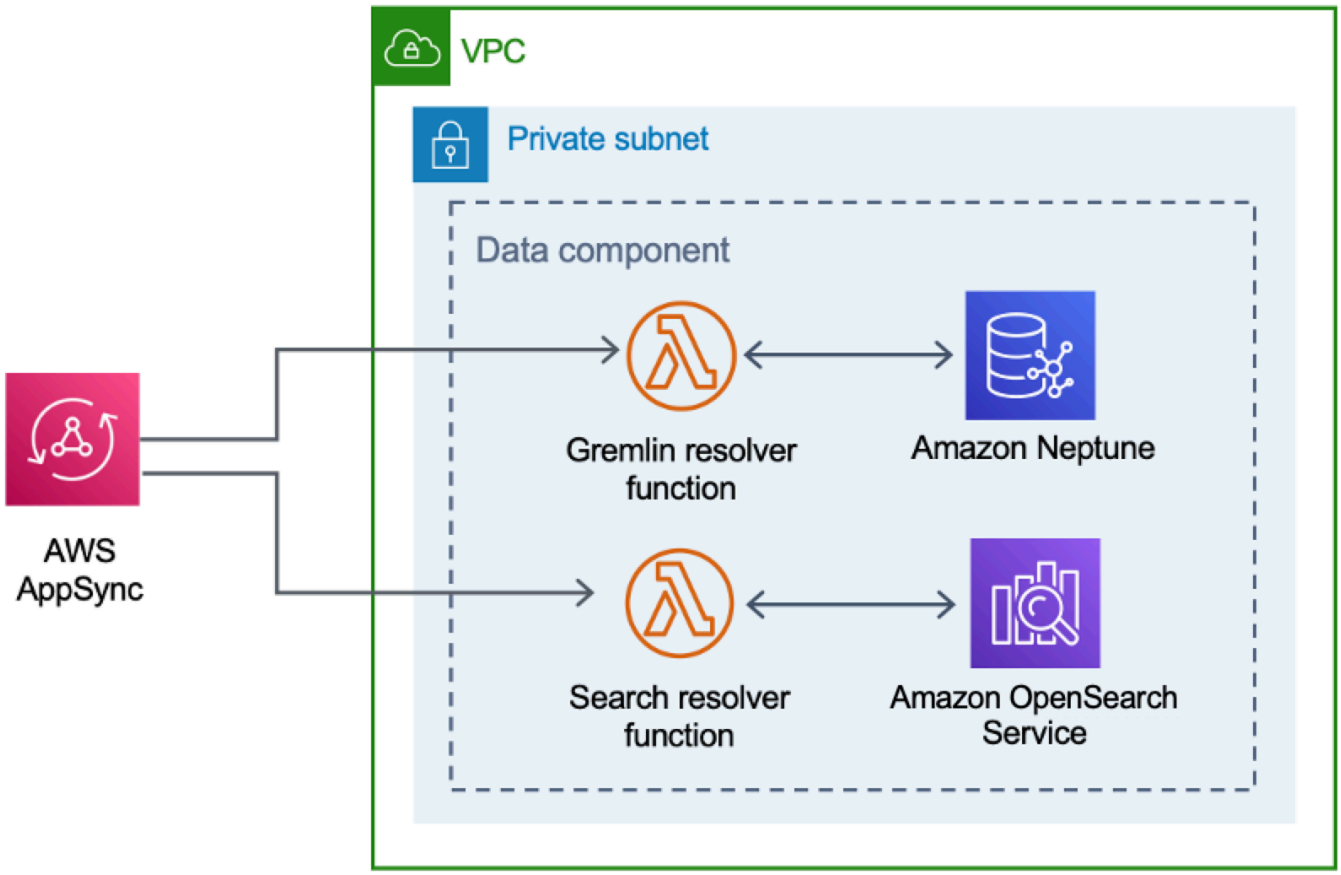


Web UI 資源託管在 `WebUIBucket` Amazon S3 儲存貯體中，並由 Amazon CloudFront 分發。AWS Amplify 提供抽象層，可簡化與 AWS AppSync 和 Amazon S3 的整合。

此解決方案使用 AWS AppSync 來促進與 AWS 上工作負載探索可用的各種組態的互動，包括管理匯入的區域。AWS AppSync 利用 `Settings` AWS Lambda 函數來處理請求，例如匯入新帳戶或區域。

資料元件

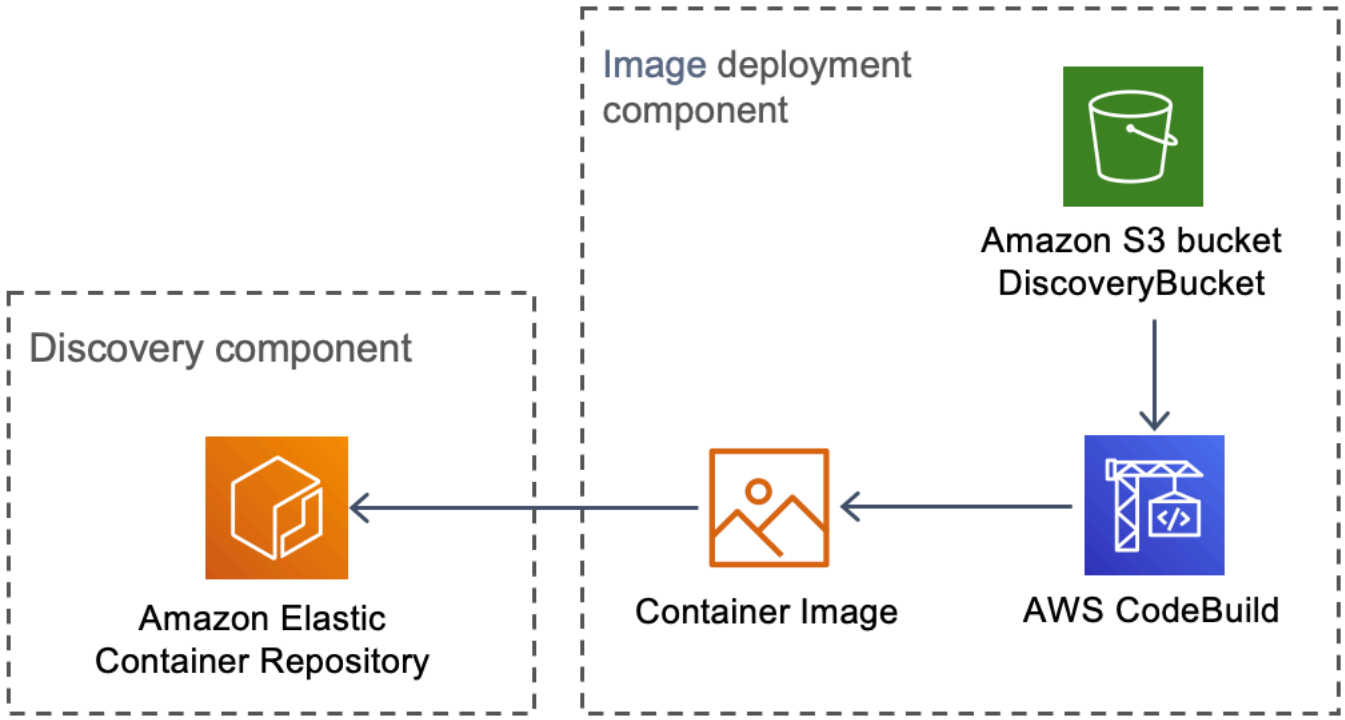
AWS 資料元件上的工作負載探索



Web UI 會將請求傳送至 AppSync API，該 API 會叫用 `Gremlin Resolver`或 `Search Resolver` Lambda 函數。這些函數會處理請求並查詢 Amazon Neptune 或 OpenSearch Service，以擷取所提供資源的資料。AWS AppSync 也支援來自 AWS CUR 的預估成本資料請求。

探索元件會將請求傳送至 AppSync API，以讀取和保留 Amazon Neptune 和 OpenSearch Service 資料庫中的資料。API 接收來自探索元件中 AWS Fargate 任務的請求。然後，API 會使用提供資料庫存取權的 IAM 角色進行身分驗證。

映像部署元件



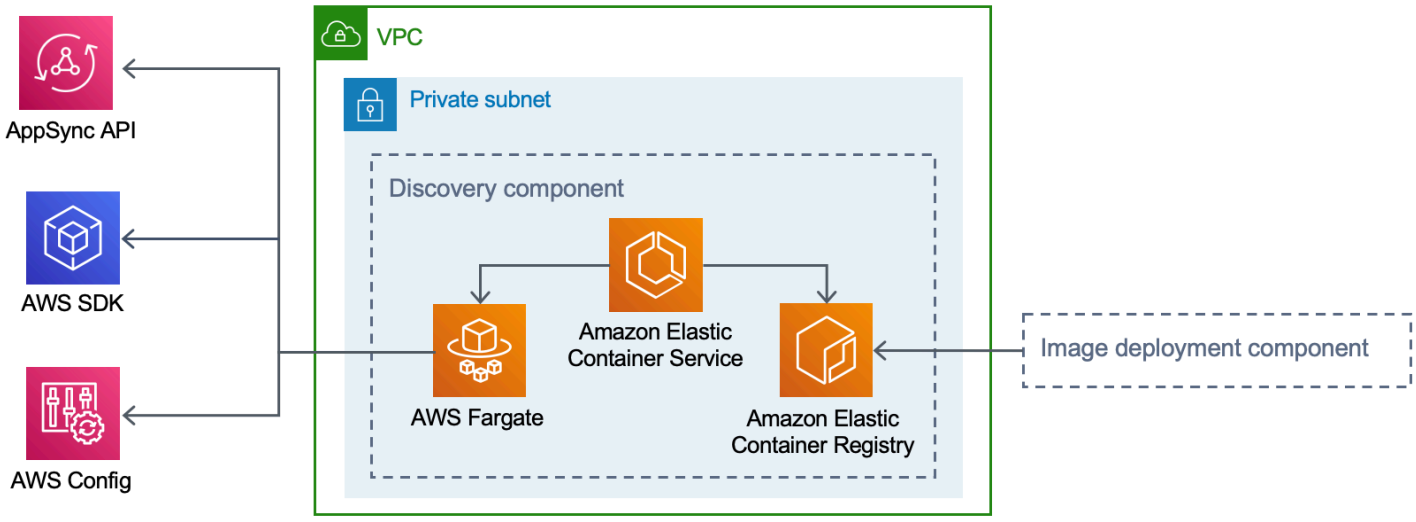
AWS 映像部署元件上的工作負載探索

映像部署元件會建置探索元件使用的容器映像。`DiscoveryBucket` 和 Amazon S3 儲存貯體託管可在部署時由建置容器映像並將其上傳至 Amazon ECR 的 AWS CodeBuild 任務下載的程式碼。

探索元件

探索元件是 AWS 架構上工作負載探索的主要資料收集元素。它負責查詢 AWS Config 並進行描述 API 呼叫，以維護資源庫存及其彼此之間的關係。

AWS 探索元件上的工作負載探索



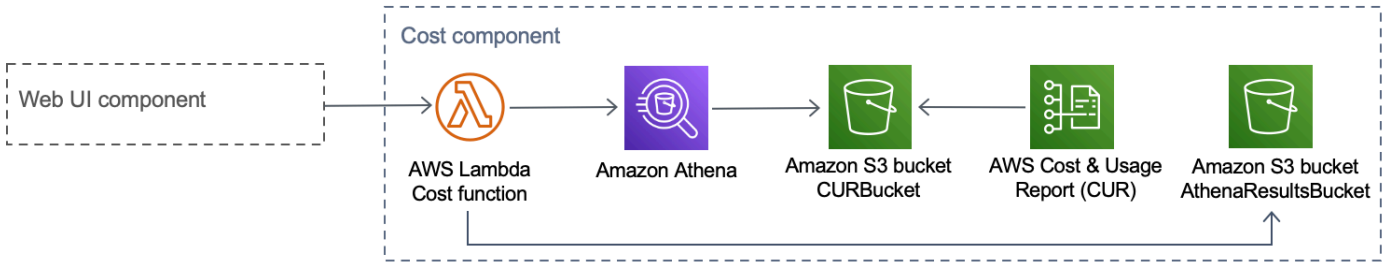
此解決方案會將 Amazon ECS 設定為使用從 Amazon ECR 下載的容器映像來執行 AWS Fargate 任務。AWS Fargate 任務排程以 15 分鐘的間隔執行。所收集的資源關係資料會插入 Amazon Neptune 圖形資料庫和 Amazon OpenSearch Service。

探索元件工作流程包含下列三個步驟：

1. Amazon ECS 每隔 15 分鐘叫用 AWS Fargate 任務。
2. Fargate 任務會從 AWS Config、AWS API 描述呼叫，以及從 Amazon Neptune 資料庫收集資源資料。
3. Fargate 任務會計算 Amazon Neptune 資料庫中存在的內容，以及從 AWS Config 收到的內容和描述呼叫之間的差異。
4. Fargate 任務會將請求傳送至 AppSync API，以將發現的資源和關係的變更保留在 Amazon Neptune 和 Amazon OpenSearch Service 中。

成本元件

AWS 成本元件上的工作負載探索



您可以在 AWS Billing and Cost Management and Cost Management 中建立 AWS CUR。這會將 Parquet 格式的檔案發佈至 `CostAndUsageReportBucket` Amazon S3 儲存貯體。Web UI 向叫用 Cost Lambda 函數的 AWS AppSync 端點提出請求。函數會將預先定義的查詢傳送至 Amazon Athena，從 AWS CUR 傳回預估成本資訊。

由於 AWS CUR 的大小，來自 Amazon Athena 的回應可能會非常大。解決方案會將結果存放在 `AthenaResultsBucket` Amazon S3 儲存貯體中，並將結果分頁回 Web UI。在此儲存貯體上設定的生命週期政策會移除超過七天的項目。

此解決方案中的 AWS 服務

AWS 服務	描述
AWS AppSync	核心。此解決方案使用 AppSync 提供 Web UI 使用的無伺服器 GraphQL API。
Amazon CloudFront	核心。此解決方案使用 CloudFront 搭配 Amazon S3 儲存貯體做為原始伺服器。這會限制對 Amazon S3 儲存貯體的存取，使其無法公開存取，並防止從儲存貯體直接存取。
AWS Config	核心。解決方案使用 AWS Config 做為解決方案探索的資源和關係的主要資料來源。
Amazon OpenSearch Service	核心。解決方案使用 Amazon OpenSearch Service 進行應用程式監控、日誌分析和可觀測性。
Amazon DynamoDB	核心。此解決方案使用 DynamoDB 來存放解決方案的組態資料。

AWS 服務	描述
Amazon Elastic Container Service (ECS)	核心。此解決方案使用 Amazon ECS 來協調執行任務，以探索 AWS 帳戶中的資源和關係。
AWS Fargate	核心。此解決方案使用 Amazon ECS 上的 AWS Fargate 作為探索任務的運算層。
AWS Lambda	核心。此解決方案使用無伺服器 Lambda 函數搭配 Node.js 和 Python 執行時間來處理 API 呼叫。
Amazon Neptune	核心。此解決方案使用 Neptune 作為解決方案探索的資源和關係的主要資料存放區。
Amazon Simple Storage Service	核心。此解決方案使用 Amazon S3 進行前端和後端儲存。
Amazon CloudWatch	支援。此解決方案使用 CloudWatch 在自動化案例中收集和視覺化即時日誌、指標和事件資料。此外，您可以監控已部署解決方案的資源用量和效能問題。
AWS CodeBuild	支援。此解決方案使用 CodeBuild 建置包含探索任務程式碼的 Docker 容器，並將前端的資產部署至 Amazon S3。
Amazon Cognito	支援。此解決方案使用 Cognito 使用者集區來驗證和授權使用者存取解決方案 Web UI。
AWS Systems Manager	支援。此解決方案使用 AWS Systems Manager 來提供資源操作和成本資料的應用程式層級資源監控和視覺化。
Amazon Virtual Private Cloud	支援。此解決方案使用 VPC 在 中啟動 Neptune 和 OpenSearch 資料庫。

AWS 服務	描述
AWS WAF	支援。此解決方案使用 AWS WAF 保護 AppSync API 免受可能影響可用性、危及安全性或消耗過多資源的常見漏洞和機器人影響。
Amazon Athena	「選用」。如果成本功能已啟用，此解決方案會使用 Athena 查詢成本和用量報告。

規劃您的部署

本節說明部署解決方案之前的區域、成本、安全性和其他考量事項。

支援的 AWS 區域

此解決方案使用 Amazon Cognito 服務，目前並非所有 AWS 區域都提供此服務。如需各區域 AWS 服務的最新可用性，請參閱 AWS 區域服務清單。

AWS 上的工作負載探索可在下列 AWS 區域使用：

區域名稱	
美國東部 (維吉尼亞北部)	加拿大 (中部)
美國東部 (俄亥俄)	歐洲 (倫敦)
美國西部 (奧勒岡)	歐洲 (法蘭克福)
亞太區域 (孟買)	歐洲 (愛爾蘭)
亞太區域 (首爾)	Europe (Paris)
亞太區域 (新加坡)	歐洲 (斯德哥爾摩)
亞太區域 (悉尼)	南美洲 (聖保羅)
亞太區域 (東京)	

AWS 上的工作負載探索不適用於下列 AWS 區域：

區域名稱	無法使用的服務
AWS GovCloud (US-East)	AWS AppSync
AWS GovCloud (US-West)	AWS AppSync
中國 (北京)	Amazon Cognito

區域名稱	無法使用的服務
中國 (寧夏)	Amazon Cognito

成本

您需負責支付執行此解決方案時佈建的 AWS 服務的費用。截至此修訂，在美國東部（維吉尼亞北部）區域使用單一執行個體部署選項執行此解決方案的成本約為每小時 0.58 美元或每月 425.19 美元。

> **Note**
>
> 在 AWS 雲端的 AWS 上執行工作負載探索的成本取決於您選擇的部署組態。下列範例提供美國東部（維吉尼亞北部）區域中單一執行個體和多個執行個體部署組態的成本明細。下列範例資料表中列出的 AWS 服務會每月計費。

我們建議您透過 AWS Cost Explorer 建立預算，以協助管理成本。價格可能變動。如需完整詳細資訊，請參閱此解決方案中使用的每個 AWS 服務的定價網頁。

成本表範例

選項 1：單一執行個體部署（預設）

使用 AWS CloudFormation 範本部署此解決方案時，請修改 OpensearchMultiAz 參數以No部署 OpenSearch Service 網域的單一執行個體，並修改 CreateNeptuneReplica 參數以部署 Neptune No 資料存放區的單一執行個體。單一執行個體部署選項的成本較低，但可減少在可用區域故障時 AWS 上工作負載探索的可用性。

AWS 服務	執行個體類型	每小時成本 【USD】	每月成本 【USD】
Amazon Neptune	`db.r5.large`	0.348 美元	254.04 美元
Amazon OpenSearch Service	`m6g.large .search`	0.128 美元	93.44 美元
Amazon VPC (NAT Gateway)	N/A	0.090 USD	65.7 美元

AWS 服務	執行個體類型	每小時成本 【USD】	每月成本 【USD】
AWS Config	N/A	每個資源 0.003 美元	每個資源 0.003 美元
Amazon ECS (AWS Fargate 任務)	N/A	0.02 美元	12.01 美元
總計		0.586 美元	425.19 美元

選項 2：多個執行個體部署

使用 AWS CloudFormation 範本部署此解決方案時，請修改 OpensearchMultiAz 參數以將兩個執行個體Yes部署在 OpenSearch Service 網域的兩個可用區域中，並修改 CreateNeptuneReplica 參數以將兩個執行個體部署在 Neptune Yes 資料存放區的兩個可用區域中。多個執行個體部署選項的執行成本較高，但在可用區域故障時，會增加 AWS 上工作負載探索的可用性。

AWS 服務	執行個體類型	每小時成本	每月成本 【USD】
Amazon Neptune	`db.r5.large`	0.696 美元	508.08 美元
Amazon OpenSearch Service	`m6g.large .search`	0.256 美元	186.88 美元
Amazon VPC (NAT Gateway)	N/A	0.090 USD	65.7 美元
AWS Config	N/A	每個資源 0.003 美元	每個資源 0.003 美元
Amazon ECS (AWS Fargate 任務)	N/A	0.02 美元	12.01 美元
總計		1.062 美元	772.67 美元

- 您的最終成本取決於 AWS Config 偵測到的資源數量。 除了表格中提供的金額之外，還會產生每個記錄的資源項目 0.003 USD。

> **Important**
>
> Amazon Neptune 和 Amazon OpenSearch Service 的成本會因您選擇的執行個體類型而異。

安全

當您在 AWS 基礎設施上建置系統時，您與 AWS 之間會共同承擔安全責任。此共同責任模型可減少您的營運負擔，因為 AWS 會操作、管理和控制元件，包括主機作業系統、虛擬化層，以及服務營運所在設施的實體安全性。如需 AWS 安全性的詳細資訊，請造訪 AWS 安全中心。

資源存取

IAM 角色

IAM 角色可讓客戶將精細存取政策和許可指派給 AWS 雲端上的服務和使用者。在 AWS 上執行工作負載探索和探索 AWS 帳戶中的資源需要多個角色。

Amazon Cognito

Amazon Cognito 用於使用短期、強大的登入資料來驗證存取權，以授予 AWS 上工作負載探索所需的元件存取權。

網路存取

Amazon VPC

AWS 上的工作負載探索部署在 Amazon VPC 中，並根據最佳實務進行設定，以提供安全性和高可用性。如需其他詳細資訊，請參閱 VPC 的安全最佳實務。VPC 端點允許服務之間的非網際網路傳輸，並在可用時設定。

安全群組用於控制和隔離在 AWS 上執行工作負載探索所需的元件之間的網路流量。

我們建議您檢閱安全群組，並在部署啟動並執行後視需要進一步限制存取。

Amazon CloudFront

此解決方案會部署託管在由 Amazon CloudFront 分佈的 Amazon S3 儲存貯體中的 Web 主控台 UI。Amazon CloudFront 透過使用原始存取身分功能，只能透過 CloudFront 存取此 Amazon S3 儲存貯體

的內容。如需詳細資訊，請參閱《Amazon CloudFront 開發人員指南》中的限制對 Amazon S3 原始伺服器的存取。 Amazon CloudFront

CloudFront 會啟用其他安全緩解措施，將 HTTP 安全標頭附加到每個檢視器回應。如需其他詳細資訊，請參閱在 CloudFront 回應中新增或移除 HTTP 標頭。

此解決方案使用預設 CloudFront 憑證，該憑證具有 TLS v1.0 的最低支援安全通訊協定。若要強制使用 TLS v1.2 或 TLS v1.3，您必須使用自訂 SSL 憑證，而非預設 CloudFront 憑證。如需詳細資訊，請參閱如何將 CloudFront 分佈設定為使用 SSL/TLS 憑證。

應用程式組態

AWS AppSync

AWS GraphQL APIs 上的工作負載探索具有 AWS AppSync 根據 GraphQL 規格提供的請求驗證。此外，身分驗證和授權是使用 IAM 和 Amazon Cognito 實作，當使用者在 Web UI 中成功驗證時，會使用 Amazon Cognito 提供的 JWT。

AWS Lambda

根據預設，Lambda 函數會設定為最新穩定版本的語言執行時間。不會記錄任何敏感資料或秘密。服務互動是以最低必要權限執行。定義這些權限的角色不會在函數之間共用。

Amazon OpenSearch Service

Amazon OpenSearch Service 網域設定了存取政策，限制存取以停止對 OpenSearch Service 叢集提出的任何未簽署請求。這僅限於單一 Lambda 函數。

OpenSearch Service 叢集建置時已啟用node-to-node加密，可在現有的 OpenSearch Service 安全功能上新增額外的資料保護層。

配額

服務配額 (也稱為限制) 是您 AWS 帳戶的服務資源或操作數目最大值。

此解決方案中 AWS 服務的配額

請確定您有足夠的配額，可用於此解決方案中實作的每個服務。如需詳細資訊，請參閱 AWS 服務配額。

使用以下連結前往該服務的 頁面。若要檢視文件中所有 AWS 服務的服務配額，而不切換頁面，請改為檢視 PDF 中服務端點和配額頁面中的資訊。

Amplify	Amazon ECR
Athena	Lambda
CloudFront	OpenSearch Service
Cognito	Neptune
Config	Amazon Simple Storage Service (Amazon S3)
Amazon ECS	

AWS CloudFormation 配額

您的 AWS 帳戶具有 AWS CloudFormation 配額，在此解決方案中啟動堆疊時，您應該注意這些配額。透過了解這些配額，您可以避免限制會阻止您成功部署此解決方案的錯誤。如需詳細資訊，請參閱《AWS CloudFormation 使用者指南》中的 中的 AWS CloudFormation 配額。 AWS CloudFormation

AWS Lambda 配額

您的帳戶的 AWS Lambda 並行執行配額為 1000。如果解決方案用於執行和使用 Lambda 的其他工作負載的帳戶，請將此配額設定為適當的值。此值可調整；如需詳細資訊，請參閱AWS Lambda 使用者指南》中的 AWS Lambda 配額。 AWS Lambda

> **Note**
>
> 此解決方案需要 150 個來自並行執行配額的執行，才能在部署解決方案的帳戶中使用。如果該帳戶中可用的執行少於 150 個，CloudFormation 部署將會失敗。

Amazon VPC 配額

您的 AWS 帳戶可以包含五個 VPCs和兩個彈性 IPs(EIPs)。如果在具有其他 VPCs 帳戶中使用該解決方案，這可能會阻止您成功部署此解決方案。 EIPs 如果您有達到此配額的風險，您可以在遵循啟動堆疊區段中的步驟時提供自己的 VPC 以進行部署。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的 Amazon VPC 配額。 https://docs.aws.amazon.com/vpc/latest/userguide/amazon-vpc-limits.html

選擇部署帳戶

如果您要將 AWS 上的工作負載探索部署至 AWS 組織，則必須在已啟用 StackSets 和多區域 AWS Config 功能的委派管理員帳戶中安裝解決方案。

如果您不是使用 AWS Organizations，我們建議您將 AWS 上的工作負載探索部署到專門為此解決方案建立的專用 AWS 帳戶。此方法表示 AWS 上的工作負載探索與您現有的工作負載隔離，並提供單一位置來設定解決方案，例如新增使用者和匯入新區域。追蹤執行 解決方案時產生的成本也比較容易。

部署 AWS 上的工作負載探索之後，您就可以從已佈建的任何帳戶匯入區域。

部署解決方案

此解決方案使用 AWS CloudFormation 範本和堆疊來自動化其部署。CloudFormation 範本會指定此解決方案中包含的 AWS 資源及其屬性。CloudFormation 堆疊會佈建範本中描述的資源。

部署程序概觀

> **Note**
>
> 如果您之前在 AWS 上部署了工作負載探索，並想要升級至最新版本，請參閱更新解決方案。

遵循本節中的step-by-step說明，設定解決方案並將其部署至您的帳戶。

部署時間：約 30 分鐘

啟動解決方案之前，請檢閱本指南中討論的成本、架構、網路安全和其他考量事項。

> **Important**
>
> 此解決方案包含將匿名操作指標傳送至 AWS 的選項。我們使用這些資料更好地了解客戶使用此解決方案、相關服務和產品的方式。AWS 擁有透過此問卷收集的資料。資料收集受 AWS 隱私權聲明約束。

先決條件

收集部署參數詳細資訊

在 AWS 上部署工作負載探索之前，請檢閱 Amazon OpenSearch Service 服務連結角色和 AWS Config 的組態詳細資訊。

驗證您是否具有 AWSServiceRoleForAmazonOpenSearchService 角色

部署會在 Amazon Virtual Private Cloud (Amazon VPC) 內建立 Amazon OpenSearch Service 叢集。範本使用服務連結角色來建立 OpenSearch Service 叢集。不過，如果您已在帳戶中建立角色，請使用現有的角色。

若要檢查您是否已經有此角色：

1. 針對您計劃部署此解決方案的帳戶，登入 Identity and Access Management (IAM) 主控台。
2. 在 Search (搜尋) 方塊中，輸入 AWSServiceRoleForAmazonOpenSearchService。
3. 如果您的搜尋傳回角色，請在啟動堆疊時No為 CreateOpensearchServiceRole 參數選取 。

確認已設定 AWS Config

AWS 上的工作負載探索使用 AWS Config 來收集大部分的資源組態。部署解決方案或匯入新區域時，您必須確認 AWS Config 是否已設定並如預期運作。AlreadyHaveConfigSetup CloudFormation 參數會通知 AWS 上的工作負載探索是否設定 AWS Config。

下列程式碼片段取自 AWS CLI 命令參考。在您打算在 AWS 上部署工作負載探索的區域中執行 命令，或匯入 AWS 上的工作負載探索。

輸入以下命令：

```
aws configservice get-status
```

如果您收到類似輸出的回應，則在該區域中會執行組態記錄器和交付通道。Yes 針對 AlreadyHaveConfigSetup CloudFormation 參數選取 。

輸出：

```
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
```

如果您正在設定 AWS CloudFormation StackSets，則必須在已設定 AWS Config 的區域批次中包含此區域。

驗證帳戶中的 AWS Config 詳細資訊

部署將嘗試設定 AWS Config。如果您已在計劃部署至 或讓 AWS 上的工作負載探索可探索的帳戶中使用 AWS Config，請在部署此解決方案時選取相關參數。此外，為了成功部署，請確定您未限制 AWS Config 掃描的資源。

若要檢查您目前的 AWS Config 組態：

1. 登入 AWS Config 主控台。
2. 選擇設定，並確保已選取記錄此區域支援的所有資源和包含全域資源方塊。

驗證 VPC 組態

如果部署到現有的 VPC，請確認您的私有子網路可以將請求路由到 AWS 服務。

如果您選擇在現有 VPC 中部署解決方案的選項，則必須確保 AWS Lambda 函數上的工作負載探索和 VPC 私有子網路中執行的 Amazon ECS 任務可以連接到其他 AWS 服務。啟用此項目的標準方法是使用 NAT 閘道。您可以列出帳戶中的 NAT 閘道，如下列程式碼範例所示。

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

輸出：

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

> **Note**
>
> 如果傳回的結果少於兩個，子網路沒有正確數量的 NAT 閘道。

如果您的 VPC 沒有 NAT 閘道，則必須佈建它們，或確定您擁有 AWS APIs區段中列出的所有 AWS 服務的 VPC 端點。

AWS CloudFormation 範本

此解決方案使用 AWS CloudFormation，在 AWS 雲端中自動部署 AWS 上的工作負載探索。它包含下列 CloudFormation 範本，您可以在部署前下載：

View template

workload-discovery-on-aws.template - 使用此範本啟動解決方案和所有相關聯的元件。預設組態會部署此解決方案區段中 AWS 服務的核心和支援解決方案，但您可以自訂範本以符合您的特定需求。

> **Note**
>
> 您可以自訂範本以符合您的特定需求；不過，您所做的任何變更都可能會影響升級程序。

啟動 堆疊

此自動化 AWS CloudFormation 範本會在 AWS 雲端的 AWS 上部署工作負載探索。您必須先收集部署參數詳細資訊，才能啟動堆疊。如需詳細資訊，請參閱先決條件。

部署時間：約 30 分鐘

1. 登入 AWS 管理主控台，然後選取按鈕以啟動 `workload-discovery-on-aws.template` AWS CloudFormation 範本。

   Launch solution

2. 根據預設，範本會在美國東部（維吉尼亞北部）區域啟動。若要在不同 AWS 區域中啟動解決方案，請使用主控台導覽列中的區域選擇器。

   > **Note**
   >
   > 此解決方案使用並非所有 AWS 區域都提供的服務。如需支援的 AWS 區域清單，請參閱支援的 AWS 區域。

3. 在建立堆疊頁面上，確認 Amazon S3 URL 文字方塊中的範本 URL 正確，然後選擇下一步。

4. 在指定堆疊詳細資訊頁面上，為您的解決方案堆疊指派名稱。如需有關命名字元限制的資訊，請參閱《AWS Identity and Access Management 使用者指南》中的 IAM 和 AWS STS 配額。 AWS Identity and Access Management
5. 在參數下，檢閱此解決方案範本的參數，並視需要修改。此解決方案使用下列預設值。

參數	預設	描述
AdminUserEmailAddress	####	用來建立第一個使用者的電子郵件地址。臨時登入資料將傳送至此電子郵件地址。
AlreadyHaveConfigSetup	No	確認您是否已在部署帳戶中設定 AWS Config。如需詳細資訊，請參閱先決條件。
AthenaWorkgroup	primary	成本功能啟用時，將用於發出 Athena 查詢的工作群組。
ApiAllowListedRanges	0.0.0.0/1,128.0.0.0/1	逗號分隔的 CIDRs 清單，用於管理 AppSync GraphQL API 的存取。若要允許整個網際網路，請使用 0.0.0.0/1，128.0.0.0/1。如果限制對特定 CIDRs存取，您還必須包含 NAT 閘道的 IP 地址（和 /32 的子網路遮罩），允許探索處理在其私有子網路中執行的 ECS 任務來存取網際網路。注意：此允許清單不會管理對 WebUI 的存取，只有 GraphQL API。
CreateNeptuneReplica	No	選擇是否要在個別可用區域中為 Neptune 建立僅供讀取複本。選擇 可Yes改善彈性，但會增加此解決方案的成本。

參數	預設	描述
CreateOpenSearchServiceRole	Yes	確認您是否已擁有 Amazon OpenSearch Service 的服務連結角色。如需詳細資訊，請參閱先決條件。
NeptuneInstanceClass	db.r5.large	用來託管 Amazon Neptune 資料庫的執行個體類型。您在此處選取的項目會影響執行此解決方案的成本。
OpensearchInstanceType	m6g.large.search	用於 OpenSearch Service 資料節點的執行個體類型。您的選擇會影響執行解決方案的成本。
OpensearchMultiAz	No	選擇是否要建立跨越多個可用區域的 OpenSearch Service 叢集。選擇 可Yes改善彈性，但會增加此解決方案的成本。
CrossAccountDiscovery	SELF_MANAGED	選擇 AWS 或 AWS Organizations 上的工作負載探索是否管理帳戶的匯入。此值可以為 SELF_MANAGED 或 AWS_ORGANIZATIONS 。
OrganizationUnitId	< 選用輸入 >	根組織單位 ID。只有在 CrossAccountDiscovery 設定為 時，才會使用此參數 AWS_ORGANIZATIONS 。

參數	預設	描述
AccountType	DELEGATED_ADMIN	要在 AWS 上安裝工作負載探索的 AWS Organizations 帳戶類型。只有在 CrossAccountDiscovery 設定為 時，才會使用此參數AWS_ORGANIZATIONS 。如需詳細資訊，請參閱選擇部署帳戶。
ConfigAggregatorName	< 選用輸入 >	要使用的 AWS Organization-wide Config 彙總工具。您必須在與此彙總工具相同的帳戶和區域中安裝解決方案。如果您將此參數保留空白，則會建立新的彙總工具。只有在 CrossAccountDiscovery 設定為 時，才會使用此參數AWS;_ORGANIZATIONS 。
CpuUnits	1 vCPU	探索程序執行的 Fargate 任務所配置的 CPUs 數量。
記憶體	2048	探索程序執行的 Fargate 任務所配置的記憶體量。
DiscoveryTaskFrequency	15mins	探索程序 ECS 任務每次執行之間的時間間隔。
MinNCUs	1	要在 Neptune 叢集上設定的 Neptune 容量單位下限 (NCUs) （必須小於或等於 MaxNCUs)。如果 DBInstance 類型為 ，則為必要項目db.serverless 。

參數	預設	描述
MaxNCUs	128	要在 Neptune 叢集上設定的 NCUs 上限（必須大於或等於 MinNCUs)。如果 DBInstance 類型為 ，則為必要項目`db.serverless` 。
VpcId	< 選用輸入 >	解決方案使用的現有 VPC ID。如果您將此參數保留空白，則會佈建新的 VPC。
VpcCidrBlock	< 選用輸入 >	VpcId 參數所參考之 VPC 的 VPC CIDR 區塊。只有在設定 VpcId 參數時，才會使用此參數。
PrivateSubnet0	< 選用輸入 >	您要使用的私有子網路。只有在設定 VpcId 參數時，才會使用此參數。
PrivateSubnet1	< 選用輸入 >	您要使用的私有子網路。只有在設定 VpcId 參數時，才會使用此參數。
UsesCustomIdentity	No	確認您是否將使用自訂身分提供者，例如 SAML 或 OIDC。
CognitoCustomDomain	< 選用輸入 >	託管應用程式註冊和登入頁面的 Amazon Cognito 自訂網域的網域字首。如果您未使用自訂 IdP，請保留空白，否則只能包含小寫字母、數字和連字號。

參數	預設	描述
CognitoAttributeMapping	< 選用輸入 >	IdP 屬性與標準和自訂 Cognito 使用者集區屬性的映射。如果您未使用自訂 IdP，請保留空白，否則必須是有效的 JSON 字串。
IdentityType	< 選用輸入 >	要使用的身分提供者類型 (Google、 SAML或 OIDC)。如果您未使用自訂 IdP，請保留空白。
ProviderName	< 選用輸入 >	身分提供者的名稱。如果您未使用自訂 IdP，請保留空白。
GoogleClientId	< 選用輸入 >	要使用的 Google 用戶端 ID。參數僅在 IdentityType 設定為時使用Google。
GoogleClientSecret	< 選用輸入 >	要使用的 Google 用戶端秘密。只有在 IdentityType 設定為 時使用參數Google。
SAMLMetadataURL	< 選用輸入 >	SAML 身分提供者的中繼資料 URL。只有在 IdentityType 設定為 SAML 時使用參數。
OIDCClientId	< 選用輸入 >	要使用的 OIDC 用戶端 ID。參數僅在 IdentityType 設定為時使用OIDC。
OIDCClientSecret	< 選用輸入 >	要使用的 OIDC 用戶端秘密。只有在 IdentityType 設定為 時使用參數OIDC。

參數	預設	描述
OIDCIssuerURL	< 選用輸入 >	要使用的 OIDC 發行者 URL。只有在 IdentityType 設定為 時使用參數OIDC。
OIDCAttributeRequestMethod	GET	要使用的 OIDC 屬性請求方法。必須是 GET或 POST (請參閱 OIDC 提供者或使用預設值) 。參數僅在 IdentityType 設定為 時使用OIDC。

6. 選擇下一步。
7. 在 Configure stack options (設定堆疊選項) 頁面，選擇 Next (下一步)。
8. 在檢閱和建立頁面上，檢閱並確認設定。選取確認範本建立 IAM 資源並需要特定功能的方塊。
9. 選擇提交以部署堆疊。

您可以在狀態欄中的 AWS CloudFormation 主控台中檢視堆疊的狀態。您應該會在大約 30 分鐘內收到 CREATE_COMPLETE 狀態。

> **Note**
>
> 如果刪除，此堆疊會移除所有資源。如果堆疊已更新，則會保留 Amazon Cognito 使用者集區，以確保設定的 使用者不會遺失。

部署後組態任務

在 AWS 上工作負載探索成功部署後，請完成下列部署後組態任務。

在 Amazon Cognito 中開啟進階安全性

若要開啟 Amazon Cognito 的進階安全功能，請遵循《Amazon Cognito 開發人員指南》中將進階安全新增至使用者集區的指示。

> **Note**
>
> 在 Amazon Cognito 中啟用進階安全性需額外付費。

建立 Amazon Cognito 使用者

AWS 上的工作負載探索使用 Amazon Cognito 來管理所有使用者和身分驗證。它會在部署期間為您建立使用者，並使用暫時登入資料，透過 AdminUserEmailAddress 參數中提供的地址傳送電子郵件。

若要建立其他使用者：

1. 登入 AWS Cognito 主控台。
2. 選擇 Manage User Pools (管理使用者集區)。
3. 選擇 WDCognitoUserPool- *<ID-string>*。
4. 在導覽窗格的一般設定下，選擇使用者和群組。
5. 在使用者索引標籤上，選擇建立使用者。
6. 在建立使用者方塊中，輸入所有必要欄位的值。

表單欄位	是否為必要？	描述
使用者名稱	是	您將用來登入 AWS 上工作負載探索的使用者名稱。
傳送邀請	是（僅限電子郵件）	選取時，會傳送通知，做為臨時密碼的提醒。僅選取電子

表單欄位	是否為必要？	描述
		郵件。如果您選取 SMS （預設），則會顯示錯誤訊息，但仍會建立使用者。
臨時密碼	是	輸入臨時密碼。使用者第一次登入 AWS 上的工作負載探索時，必須變更此項目。
電話號碼	否	輸入國際格式的電話號碼，例如 \+44。確定已選取將電話號碼標記為已驗證？方塊。
電子郵件	是	輸入有效的電子郵件地址。確定已選取將電子郵件標記為已驗證？方塊。

7. 選擇 Create user (建立使用者)。

重複此程序，視需要建立任意數量的使用者。

> **Note**
>
> 每個使用者將擁有相同層級的探索資源存取權。我們建議為包含敏感工作負載或資料的帳戶，在 AWS 上佈建工作負載探索的個別部署。這可讓您將存取限制為僅需要的使用者。

登入 AWS 上的工作負載探索

成功部署解決方案後，請判斷提供解決方案 Web UI 的 Amazon CloudFront 分佈 URL。

1. 登入 AWS CloudFormation 主控台。
2. 選擇檢視巢狀以顯示組成部署的巢狀堆疊。根據您的偏好設定，可能已顯示巢狀堆疊。
3. 選取 AWS 堆疊上的主要工作負載探索。
4. 選取輸出索引標籤，然後在與 WebUiUrl 金鑰相關聯的值欄中選擇 URL。
5. 在登入畫面上，輸入您透過電子郵件收到的登入憑證。然後採取下列動作：

a. 依照提示變更您的密碼。

b. 使用傳送至您電子郵件的驗證碼來完成帳戶復原。

匯入區域

> **Note**
>
> 以下章節僅適用於解決方案的帳戶探索模式為自我管理的情況。如需帳戶探索如何在 AWS Organizations 模式下運作的詳細資訊，請參閱 AWS Organizations 帳戶探索模式一節。

匯入區域需要部署特定基礎設施。此基礎設施包含全球和區域資源：

全域 – 在帳戶中部署一次，並針對每個匯入的區域重複使用的資源。

- IAM 角色 (WorkloadDiscoveryRole)

區域 – 在每個匯入的區域中部署的資源。

- AWS Config 交付管道
- 適用於 AWS Config 的 Amazon S3 儲存貯體 AWS Config
- IAM 角色 (ConfigRole)

部署此基礎設施有兩種選項：

- AWS CloudFormation StackSets （建議）
- AWS CloudFormation

匯入區域

這些步驟會引導您匯入區域和部署 AWS CloudFormation 範本。

1. 登入以在 AWS 上探索工作負載。如需 URL，請參閱登入 AWS 上的工作負載探索。
2. 在導覽功能表中，選取帳戶。
3. 選擇匯入。

4. 選取匯入方法：
   a. 使用 CSV 檔案新增帳戶和區域。
   b. 使用表單新增帳戶和區域。

CSV 檔案

提供逗號分隔值 (CSV) 檔案，其中包含以下列格式匯入的區域。

```
"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. 選取上傳 CSV。
2. 尋找並開啟 CSV 檔案。
3. 檢閱 Regionstable，然後選取匯入。
4. 在模態對話方塊中，下載全域資源範本和區域資源範本。
5. 在相關帳戶中部署 CloudFormation 範本（請參閱部署 AWS CloudFormation 範本一節）。
6. 部署全域和區域資源範本後，選取兩個方塊以確認安裝完成，然後選擇匯入。

表格

使用表單提供要匯入的區域：

1. 針對帳戶 ID，輸入 12 位數的帳戶 ID 或選取現有的帳戶 ID。
2. 在帳戶名稱中，輸入帳戶名稱，或在選取現有帳戶 ID 時使用預先填入的值。
3. 選取要匯入的區域。
4. 選取新增以填入下方 區域表中的區域。
5. 檢閱區域資料表，然後選取匯入。
6. 在模態對話方塊中，下載全域資源範本和區域資源範本。
7. 在相關帳戶中部署 CloudFormation 範本（請參閱部署 AWS CloudFormation 範本一節）。
8. 部署全域和區域資源範本後，選取兩個方塊以確認安裝完成，然後選擇匯入。

部署 AWS CloudFormation 範本

每個帳戶必須部署全域資源一次。從包含已匯入 AWS 上工作負載探索的區域的帳戶匯入區域時，請勿部署此範本。如果區域已匯入，請遵循部署堆疊中的指示來佈建區域資源。

使用 CloudFormation StackSets 跨帳戶佈建全域資源

> **Important**
>
> 首先，完成堆疊集操作的先決條件，以在目標帳戶中啟用 StackSets。

1. 在管理員帳戶中，登入 AWS CloudFormation 主控台。
2. 從導覽功能表中，選取 StackSets。
3. 選擇 Create StackSet (建立 StackSet)。
4. 在選擇範本頁面的許可下：
   a. 如果您使用的是 AWS Organizations，請選擇服務受管許可或自助服務許可。如需詳細資訊，請參閱在 AWS 組織中使用 StackSets。
   b. 如果您不是使用 AWS Organizations，請輸入在遵循 StackSets 先決條件步驟時使用的 IAM 執行角色名稱。如需詳細資訊，請參閱授予自我管理許可。
5. 在指定範本下，選取上傳範本檔案。選擇`global-resources.template`檔案（當您透過 CSV 檔案或表單匯入區域時稍早下載），然後選擇下一步。
6. 在指定 StackSet 詳細資訊頁面上，將名稱指派給您的 StackSet。如需有關命名字元限制的資訊，請參閱《AWS Identity and Access Management 使用者指南》中的 IAM 和 AWS STS 配額。 AWS Identity and Access Management
7. 在參數下，檢閱此解決方案範本的參數，並視需要修改。此解決方案使用下列預設值。

欄位名稱	預設	描述
AccountId	部署帳戶 ID	原始部署帳戶的帳戶 ID。您必須將此值保留為預設值。

1. 選擇下一步。
2. 在設定 StackSet 選項頁面上，選擇下一步。

3. 在設定部署選項頁面的帳戶下，於帳號方塊中輸入用於部署帳戶角色的帳戶 IDs。
4. 在指定區域下，選取要安裝堆疊的區域。
5. 在部署選項下，選取平行，然後選擇下一步。
6. 在檢閱頁面上，勾選確認 AWS CloudFormation 可能會使用自訂名稱建立 IAM 資源的方塊。
7. 選擇提交。

使用 CloudFormation StackSets 佈建區域資源

> **Important**
>
> 首先，完成堆疊集操作的先決條件，以在目標帳戶中啟用 StackSets。
> 如果您已安裝 AWS Config 的某些區域，但有些沒有，則必須執行兩個 StackSet 操作，一個用於已安裝 AWS Config 的區域，另一個用於沒有 AWS Config 的區域。

1. 在管理員帳戶中，登入 AWS CloudFormation 主控台。
2. 從導覽功能表中，選取 StackSets。
3. 選擇 Create StackSet (建立 StackSet)。
4. 在選擇範本頁面的許可下：
   a. 如果您使用的是 AWS Organizations，請選擇服務受管許可或自助服務許可。如需詳細資訊，請參閱在 AWS 組織中使用 StackSets。
   b. 如果您不是使用 AWS Organizations，請輸入在遵循 StackSets 先決條件步驟時使用的 IAM 執行角色名稱。如需詳細資訊，請參閱授予自我管理許可。
5. 在指定範本下，選取上傳範本檔案。選擇 `regional-resources.template` 檔案（當您透過 CSV 檔案或表單匯入區域時，稍早下載），然後選擇下一步。
6. 在指定 StackSet 詳細資訊頁面上，將名稱指派給您的 StackSet。如需有關命名字元限制的資訊，請參閱《AWS Identity and Access Management 使用者指南》中的 IAM 和 AWS STS 配額。 AWS Identity and Access Management
7. 在參數下，檢閱此解決方案範本的參數，並視需要修改它們。此解決方案使用下列預設值。

欄位名稱	預設	描述
AccountId	部署帳戶 ID	原始部署帳戶的帳戶 ID。您必須將此值保留為預設值。
AggregationRegion	部署區域	最初部署到 的區域。您必須將此值保留為預設值。
AlreadyHaveConfigSetup	No	確認區域是否已安裝 AWS Config。如果此區域已安裝 AWS Config，則設定為是。

1. 選擇下一步。
2. 在設定 StackSet 選項頁面上，選擇下一步。
3. 在設定部署選項頁面的帳戶下，於帳號方塊中輸入要部署帳戶角色的帳戶 IDs。
4. 在指定區域下，選取要安裝堆疊的區域。這會在步驟 6 中輸入的所有帳戶中的這些區域中安裝堆疊。
5. 在部署選項下，選取平行，然後選擇下一步。
6. 在檢閱頁面上，勾選確認 AWS CloudFormation 可能會使用自訂名稱建立 IAM 資源的方塊。
7. 選擇提交。

使用 CloudFormation 部署堆疊以佈建全域資源

每個帳戶必須部署全域資源一次。從包含已匯入 AWS 上工作負載探索的區域的帳戶匯入區域時，請勿部署此範本。

1. 登入 AWS CloudFormation 主控台。
2. 選擇建立堆疊，然後選取使用新資源 （標準）。
3. 在建立堆疊頁面的指定範本區段中，選取上傳範本檔案。
4. 選擇選擇檔案，然後選擇`global-resources.template`檔案 （透過 CSV 檔案或表單匯入區域時稍早下載），然後選擇下一步。
5. 在指定堆疊詳細資訊頁面上，為您的解決方案堆疊指派名稱。如需有關命名字元限制的資訊，請參閱《_AWS Identity and Access Management_User Guide》中的 IAM 和 AWS STS 配額。

6. 在參數下，檢閱此解決方案範本的參數，並視需要加以修改。此解決方案使用下列預設值。

欄位名稱	預設	描述
Stack name (堆疊名稱)	`workload-discovery`	此 AWS CloudFormation 堆疊的名稱。
AccountId	部署帳戶 ID	原始部署帳戶的帳戶 ID。您必須將此值保留為預設值。

1. 選擇下一步。
2. 選取方塊，確認 AWS CloudFormation 可能會使用自訂名稱建立 IAM 資源。
3. 選擇建立堆疊。

新區域將在下一個探索程序中掃描，每隔 15 分鐘執行，例如：15：00、15：15、15：30、15：45。

使用 CloudFormation 部署堆疊以佈建區域資源

1. 登入 AWS CloudFormation 主控台。
2. 選擇建立堆疊，然後選取使用新資源 （標準）。
3. 在建立堆疊頁面的指定範本區段中，選取上傳範本檔案。
4. 選擇選擇檔案，然後選擇`regional-resources.template`檔案 （當您透過 CSV 檔案或表單匯入區域時，稍早下載），然後選擇下一步。
5. 在指定堆疊詳細資訊頁面上，為您的解決方案堆疊指派名稱。如需有關命名字元限制的資訊，請參閱《AWS Identity and Access Management 使用者指南》中的 IAM 和 AWS STS 配額。 AWS Identity and Access Management
6. 在參數下，檢閱此解決方案範本的參數，並視需要修改它們。此解決方案使用下列預設值。

欄位名稱	預設	描述
AccountId	解決方案部署帳戶 ID	原始部署帳戶的帳戶 ID。必須保留為預設值。

欄位名稱	預設	描述
AggregationRegion	解決方案部署區域	最初部署到 的區域。必須保留為預設值。
AlreadyHaveConfigSetup	No	確認區域是否已安裝 AWS Config。Yes 如果此區域已安裝 AWS Config，則設定為 。

1. 選擇下一步。
2. 選取方塊，確認 AWS CloudFormation 可能會使用自訂名稱建立 IAM 資源。
3. 選擇建立堆疊。

新區域將在下一個探索程序期間掃描，該程序每隔 15 分鐘執行，例如 15：00、15：15、15：30、15：45。

確認區域已正確匯入

1. 登入解決方案的 Web UI （或重新整理已載入的頁面）。如需 URL，請參閱登入 AWS 上的工作負載探索。
2. 在左側導覽面板的設定下，選取匯入的區域。

區域、帳戶名稱和帳戶 ID 會顯示在表格中。上次掃描資料欄會顯示該區域中上次探索的資源。

> **Note**
>
> 如果上次掃描的資料欄保留空白超過 30 分鐘，請參閱偵錯探索元件。

設定成本功能

成本功能需要手動設定 AWS 成本和用量報告 (CUR)。遵循以下指示，您將：

1. 設定排程的 CUR。
2. 設定 Amazon S3 複寫 （當 CURs部署帳戶外時）

在部署帳戶中建立 AWS 成本和用量報告

1. 登入您想要從中收集成本資料的 帳戶的帳單主控台。
2. 在導覽選單的帳單下，選取成本與用量報告。
3. 選擇建立報告。
4. 使用 `workload-discovery-cost-and-usage-` *`<your-workload-discovery-deployment-account-ID>`* 做為報告名稱。

> **Note**
>
> 您必須遵循此命名慣例，因為會部署少量的基礎設施，以促進 CURs的查詢。

5. 選取包含資源 IDs方塊。

> **Note**
>
> 您必須選取包含資源 IDs方塊以檢視成本資料。此 ID 必須與 AWS 上工作負載探索探索探索發現的資源相符。

6. 選擇下一步。
7. 在交付選項頁面上，選擇設定 -0-
8. 選取 *`<stack-name>`* `-s3buc-costandusagereportbucket-` *`<ID-string>`* Amazon S3 儲存貯體以存放 CUR。選擇下一步。
9. 檢閱政策，選取確認方塊，然後選擇儲存。
10. 將報告字首路徑設定為 `aws-perspective`。
11. 選取每日以取得時間精細程度。
12. 在啟用 的報告資料整合下，選取 Amazon Athena。
13. 選擇下一步。
14. 選擇檢閱並完成。

若要驗證報告是否已正確設定，請檢查測試檔案的 Amazon S3 儲存貯體。

> **Note**
>
> 最多可能需要 24 小時才會將報告上傳至您的儲存貯體。

在外部帳戶中建立 AWS 成本和用量報告

1. 登入您想要從中收集成本資料的 帳戶的帳單主控台。
2. 在導覽功能表中，於成本管理下，選取成本與用量報告。
3. 選擇建立報告。
4. 使用 `workload-discovery-cost-and-usage-` *<your-external-account-ID>* 做為報告名稱。

> **Note**
>
> 您必須遵循此命名慣例，因為會部署少量的基礎設施，以促進 CURs的查詢。

5. 勾選包含資源 IDs方塊。

> **Note**
>
> 您必須選取包含資源 IDs方塊以檢視成本資料。需要此 ID 才能與 AWS 上工作負載探索探索探索發現的資源相符。

6. 選擇下一步。
7. 在交付選項頁面上，選擇設定 -0-
8. 建立新的 Amazon S3 儲存貯體以存放 CURs。
9. 檢閱政策，選取確認方塊，然後選擇儲存。
10. 將報告字首路徑設定為 `aws-perspective`。
11. 選取每日以取得時間精細程度。
12. 在啟用 的報告資料整合下，選取 Amazon Athena。
13. 選擇下一步。
14. 選擇檢閱並完成。若要驗證報告是否已正確設定，請檢查測試檔案的 Amazon S3 儲存貯體。

> **Note**
>
> 最多可能需要 24 小時才會將報告上傳至您的儲存貯體。

接著，設定複寫到部署帳戶。

設定複寫

設定複寫至部署期間建立的 Amazon S3 儲存貯體。Amazon S3 儲存貯體遵循下列格式：*<stack-name>* -s3buc-costandusagereportbucket- *<ID-string>*。這可讓解決方案使用 Amazon Athena 查詢儲存貯體。

1. 在 Amazon S3 主控台中登入 AWS 帳戶，其中包含需要複寫的建立 CUR。
2. 選取設定 CUR 時建立的 Amazon S3 儲存貯體。如需詳細資訊，請參閱建立的步驟 8，並排程 AWS 成本和用量報告。
3. 選擇 Management (管理) 標籤，
4. 在複寫規則下，選擇建立複寫規則。
5. 在複寫規則組態下，於複寫規則名稱方塊中，輸入描述性規則 ID。
6. 在來源儲存貯體下，選取套用至儲存貯體中的所有物件，以設定規則範圍。
7. 在目的地下，設定下列項目：
   a. 選取指定另一個帳戶中的儲存貯體。
   b. 輸入帳戶 ID。
   c. 輸入在 AWS 上部署工作負載探索期間所建立之儲存貯體名稱的值。您可以依照在 AWS 上第一次部署工作負載探索時指定的邏輯 ID 和堆疊名稱，尋找部署資源中的指示來找到。CostAndUsageReportBucket
   d. 選取將物件擁有權變更為目的地儲存貯體擁有者的方塊。
8. 在 IAM 角色下，選擇建立新角色。

> **Note**
>
> 複寫角色可能已存在。您可以選取它，並確保它具有必要的 S3 複寫角色動作。

9. 選擇儲存。
10. 登入安裝 CUR 的 AWS 管理主控台，導覽至 S3 服務頁面，然後選取 CostAndUsageReportBucket S3 儲存貯體。如需詳細資訊，請參閱尋找部署資源。
11. 選取管理索引標籤。
12. 在複寫規則下，從動作下拉式功能表中，選取接收複寫的物件。
13. 在來源儲存貯體帳戶設定下：
    a. 輸入來源儲存貯體帳戶 ID。
    b. 選擇產生政策。

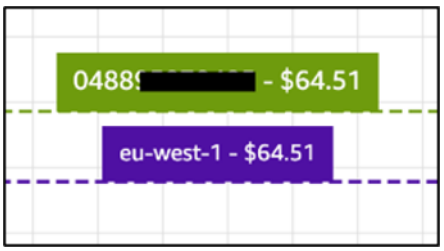
c. 在政策下，選取檢視儲存貯體政策。

d. 選取包含許可，將物件擁有權變更為目的地儲存貯體擁有者。

e. 選擇套用設定。這可讓它存取複製物件。如需範例 S3 儲存貯體政策，請參閱成本儲存貯體複寫政策。

> **Note**
>
> 從多個 AWS 帳戶複寫 CURs 時。您需要確保目的地儲存貯體上的儲存貯體政策（在 AWS 帳戶上的工作負載探索內）具有您從每個帳戶使用的每個 IAM 角色的 ARN。如需詳細資訊，請參閱 成本儲存貯體複寫政策。

當報告在帳戶中時，成本資料會顯示在週框方塊和個別資源上。



編輯 S3 儲存貯體生命週期政策

在部署期間，解決方案會在兩個儲存貯體上設定生命週期政策：

- `CostAndUsageReportBucket`
- `AccessLogsBucket`

> **Important**
>
> 這些生命週期政策會在 90 天後從這些儲存貯體中刪除資料。您可以編輯生命週期，以符合您擁有的任何內部政策。

監控解決方案

此解決方案使用 myApplications 和 CloudWatch AppInsights，可讓您監控 AWS 部署上的工作負載探索。

myApplications

myApplications 是 Console Home 的延伸，可協助您管理和監控 AWS 上應用程式的成本、運作狀態、安全狀態和效能。您可以從 AWS 管理主控台的單一檢視中存取帳戶中的所有應用程式、所有應用程式的關鍵指標，以及來自多個服務主控台的成本、安全性和操作指標和洞見概觀。

若要檢視 AWS 上工作負載探索的 myApplications 儀表板：

1. 登入 AWS 管理主控台。
2. 在左側邊欄中，選擇 myApplications。
3. 在搜尋列`workload-discovery`中輸入 以尋找應用程式。
4. 選取應用程式。

CloudWatch AppInsights

CloudWatch Application Insights 透過識別和設定應用程式資源的關鍵指標、日誌和警示，協助您監控應用程式，而技術 stack.lt 會持續監控指標和日誌，以偵測並關聯異常和錯誤。為協助進行故障診斷，它會建立已偵測到問題的自動化儀表板，包括關聯的指標異常和日誌錯誤以及其他洞見，指出可能的根本原因。

若要檢視 AWS 上工作負載探索的 CloudWatch AppInsights 儀表板：

1. 登入 CloudWatch 主控台。
2. 在左側邊欄中，選擇 Insights、Application Insights。
3. 選取應用程式索引標籤。
4. 在搜尋列`workload-discovery`中輸入 以尋找儀表板。
5. 選取儀表板。
6. 選取應用程式。

更新解決方案

> **Important**
>
> 不支援在 AWS 上將工作負載探索從 v1.x.x 更新至 v2.x.x。建議您先解除安裝此解決方案的 v1.x.x，再安裝 v2.x.x。

若要從 2.x.x 部署更新，請依照下列步驟進行。

1. 下載解決方案的 AWS CloudFormation 範本。
2. 登入 AWS CloudFormation 主控台。
3. 選取具有部署期間所提供名稱的堆疊，然後選擇更新。
4. 在更新堆疊頁面上，選取取代目前範本，然後選取上傳範本檔案，然後上傳在步驟 1 中下載的檔案。
5. 選擇下一步。
6. 在指定堆疊詳細資訊頁面的參數下，檢閱參數並視需要修改。
7. 選擇下一步。
8. 在設定堆疊選項頁面的堆疊失敗選項下，確保佈建失敗時的行為選項按鈕設定為轉返所有堆疊資源。
9. 選擇下一步。
10. 在檢視 頁面上，檢視和確認的設定。選取確認範本建立 IAM 資源並需要特定功能的方塊。
11. 選擇更新堆疊以部署堆疊。

> **Note**
>
> 如果您以自我管理帳戶探索模式部署解決方案，則必須在遵循匯入區域區段中的步驟時更新部署的全域資源。

疑難排解

已知問題解決提供減輕已知錯誤的指示。如果這些指示無法解決您的問題，請參閱聯絡 AWS Support 一節，以取得為此解決方案開啟 AWS Support 案例的說明。

已知問題解決方案

在 AWS 上部署工作負載探索期間以及在部署後階段，可能會發生幾個常見的組態錯誤：

> **Note**
>
> 為了協助您更輕鬆地進行故障診斷，建議您在 AWS CloudFormation 範本中停用轉返失敗功能。您也可以在 AWS 部署後工作負載探索組態文件中找到其他故障診斷說明。

Config 交付管道錯誤

問題：部署主要 AWS CloudFormation 範本時發生下列錯誤：

```
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：解決方案正在部署到已啟用 AWS Config 的區域。

解決方案：遵循先決條件一節中的指示，並將 CloudFormation 參數 AlreadyHaveConfigSetup 設定為來部署解決方案Yes。

將部署至現有 VPC 時搜尋解析程式堆疊部署逾時

問題：佈建自訂資源以在 OpenSearch 叢集中建立索引的巢狀堆疊逾時，並顯示下列錯誤：

```
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：以 CloudFormation 參數提供的私有子網路無法路由至 S3（自訂資源必須使用預先簽章的 URL 將執行結果寫入 S3 儲存貯體）。這通常有兩個原因：

1. 私有子網路沒有與其相關聯的 NAT 閘道，因此無法存取網際網路。
2. 私有子網路使用 VPC 端點而非 NAT 閘道，而且 S3 閘道端點未正確設定。

解決方法：

1. 在 VPC 中佈建 NAT 閘道，以允許在私有子網路中執行的任務存取網際網路，可根據文件使用 CloudFormation 或 AWS CLI。
2. 確定子網路的路由表已根據文件更新 S3 VPC 端點。

匯入帳戶後未發現的資源

問題：帳戶已透過 Web UI 匯入，但在探索程序執行後似乎沒有發現任何資源。

原因：最可能的原因如下：

1. 當 CrossAccountDiscovery CloudFormation 參數設定為 時`SELF_MANAGED`，尚未部署全域資源 CloudFormation 範本。
2. 當 CrossAccountDiscovery CloudFormation 參數設定為 時`AWS_ORGANIZATIONS`：未探索一或多個帳戶，且角色狀態欄具有未部署的項目。這表示使用 StackSets 自動部署全域資源範本時發生問題。
3. 探索程序 ECS 任務記憶體不足。匯入大量帳戶或資源時會發生這種情況。UI 中的上次探索欄的值會大於 DiscoveryTaskFrequency CloudFormation 參數中指定的值（預設值為 15 分鐘），而且 ECS 主控台中會出現記憶體不足錯誤。

解決方法：

1. 根據文件，在所需帳戶中部署全域資源範本。
2. 前往已部署工作負載探索之區域中的 WdGlobalResources StackSet，並檢查已部署失敗之堆疊執行個體中的錯誤。
3. 將 Memory CloudFormation 參數更新為較大的值：從雙數開始，並持續增加直到錯誤停止為止。

> **Note**
>
> 只有特定 CPU 單位和記憶體值組合有效，因此您可能也必須更新 CpuUnits CloudFormation 參數。組合的完整清單會列在 ECS 文件中。

在特定帳戶中僅探索非 AWS Config 資源

問題：解決方案探索的唯一資源類型是支援資源區段中 資料表中列出的類型。

原因：此問題最常見的原因是，

1. 當 CrossAccountDiscovery CloudFormation 參數設定為 時SELF_MANAGED，CloudFormation 範本尚未部署在每個要探索之帳戶的區域中。
2. 當 CrossAccountDiscovery CloudFormation 參數設定為 時SELF_MANAGED，CloudFormation 範本已部署在許多未啟用 Config 但 CloudFormation 參數 AlreadyHaveConfigSetup 錯誤設定為 的帳戶區域中Yes。
3. 當 CrossAccountDiscovery CloudFormation 參數設定為 時AWS_ORGANIZATIONS，不會在每個要探索的帳戶區域中啟用 AWS Config。在 AWS_ORGANIZATIONS模式下，您有責任根據組織的政策啟用 Config。

解決方法：

1. 根據文件，在所需帳戶中部署區域資源範本。
2. 刪除先前部署的區域資源堆疊（否則 AWS Config 將處於不一致狀態），並使用設定為 的 CloudFormation 參數AlreadyHaveConfigSetup部署No。
3. 在要探索的每個帳戶區域中啟用 AWS Config。

聯絡 AWS Support

如果您有 AWS 開發人員支援、AWS Business Support 或 AWS Enterprise Support，您可以使用 支援中心來取得此解決方案的專家協助。以下章節將提供說明。

建立案例

1. 登入支援中心。

2. 選擇建立案例。

如何提供協助？

1. 選擇技術。
2. 針對服務，選取解決方案。
3. 針對類別，選取其他解決方案。
4. 針對嚴重性，選取最符合您使用案例的選項。
5. 當您輸入服務、類別和嚴重性時，界面會填入常見故障診斷問題的連結。如果您無法使用這些連結來解決問題，請選擇下一步：其他資訊。

其他資訊

1. 針對主旨，輸入摘要您的問題的文字。
2. 針對描述，詳細說明問題。
3. 選擇連接檔案。
4. 連接 AWS Support 處理請求所需的資訊。

協助我們更快解決您的案例

1. 輸入請求的資訊。
2. 選擇下一步驟：立即解決或聯絡我們。

立即解決或聯絡我們

1. 檢閱立即解決解決方案。
2. 如果您無法解決這些解決方案的問題，請選擇聯絡我們，輸入請求的資訊，然後選擇提交。

解除安裝解決方案

若要解除安裝解決方案，請使用 AWS 管理主控台或 AWS 命令列界面 (AWS CLI)。首先，停止 Amazon ECS 叢集中的所有執行中任務。否則，堆疊刪除可能會失敗。

使用 AWS 管理主控台

1. 登入 AWS CloudFormation 主控台。
2. 使用部署期間提供的名稱選取堆疊。
3. 選擇刪除堆疊。

使用 AWS 命令列界面

判斷您的環境中是否提供 AWS CLI。如需安裝說明，請參閱《AWS CLI 使用者指南》中的什麼是 AWS 命令列界面。

確認 AWS CLI 可用後，請執行下列命令：

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

開發人員指南

本節提供解決方案的原始程式碼和其他自訂項目。

來源碼

請造訪 AWS GitHub 上的工作負載探索儲存庫，下載此解決方案的範本和指令碼，並與他人共用您的自訂項目。

尋找部署資源

請依照下列步驟來尋找部署至您 帳戶的資源。

1. 登入 AWS CloudFormation 主控台。
2. 選取您部署解決方案的區域。

   根據此帳戶的使用情況，它可能包含多個堆疊，用於不同的工作負載。主要堆疊在部署期間會提供名稱，並在其下提供多個巢狀堆疊。
3. 選取每個堆疊以存取使用該範本部署的資源。
4. 選取資源索引標籤，然後選擇相關資源的實體 ID 連結，以在其各自的服務主控台中檢視資源。

   如果您知道資源的邏輯 ID，也可以使用資料表上方的搜尋列進行搜尋。

支援的資源

解決方案支援 AWS Config 支援的所有資源類型，如此處所列。下表包含 AWS 上工作負載探索發現 AWS Config 不支援的支援資源。詳細資訊提供於對應的 AWS 文件清單中。

資源類型	來源	描述
AWS::APIGateway::Authorizer	SDK	getAuthorizers
AWS::ApiGateway::Resource	SDK	getResource
AWS::ApiGateway::Method	SDK	getMethod
AWS::Cognito::UserPool	SDK	describeUserPool

資源類型	來源	描述
AWS::ECS::Task	SDK	describe-tasks
AWS::EKS::Nodegroup	SDK	describeNodegroup
AWS::DynamoDB::Stream	SDK	describeStream
AWS::IAM::AWSManagedPolicy	SDK	getAccountAuthorizationDetails
AWS::ElasticLoadBalancingV2::TargetGroup	SDK	describeTargetGroups
AWS::EC2::Spot	SDK	describeSpotInstanceRequests
AWS::EC2::SpotFleet	SDK	describeSpotFleetRequests

AWS Organizations 帳戶探索模式

當 AWS 上的工作負載探索部署在 AWS 組織中時，帳戶探索不再透過解決方案的 Web UI 進行管理。在這種情況下，您不需要管理 CloudFormation 範本的部署來探索帳戶。

反之，解決方案會使用 AWS Organization-wide AWS Config 彙總工具來探索組織中已啟用 AWS Config 的所有帳戶中的資源。

對於 AWS Config 不支援的資源類型，解決方案會使用 AWS CloudFormation StackSets 在組織中的每個帳戶中自動部署 IAM 角色。此角色允許探索程序在所有組織的帳戶中進行 SDK 呼叫，以探索這些補充資源。

此 StackSet 已設定為在新增至組織的任何新帳戶中自動部署角色，並從組織移除的任何帳戶中刪除角色。

> **Note**
>
> StackSet 無法將堆疊執行個體部署至 管理帳戶。如果您希望 Workload Discovery 探索此帳戶，則必須使用部署堆疊中描述的標準 AWS CloudFormation 部署方法部署全域資源範本，以使用 CloudFormation 佈建全域資源區段。 CloudFormation

Amazon S3 複寫角色動作

用於執行複寫的 IAM 角色需要有下列動作：

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

若要驗證角色具有複寫角色動作：

1. 在 S3 複寫精靈中複製角色名稱的名稱。
2. 在您設定複寫的帳戶內登入 IAM 主控台。
3. 將角色的名稱貼到搜尋 IAM 方塊中。
4. 從清單中選取最上方項目。這是將使用的 IAM 角色。
5. 在許可政策下，展開 受管政策。
6. 確保政策具有上表中詳述的動作。

S3 儲存貯體政策

以下是 S3 儲存貯體政策的範例，該政策允許將 CURs上傳到儲存貯體，以及允許外部帳戶將物件複寫到其中的許可。您需要從每個外部 AWS 帳戶將 IAM 角色新增至此政策，以授予執行複寫的許可。

```
   {
      "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 API

如先決條件所述，如果您要將解決方案部署到現有的 VPC，則必須從私有子網路存取下列服務。

API Gateway

- GetAuthorizers
- GetIntegration
- GetMethod
- GetResources
- GetRestApis

Cognito

- DescribeUserPool

Config

- BatchGetAggregateResourceConfig
- DescribeConfigurationAggregators
- ListAggregateDiscoveredResources
- SelectAggregateResourceConfig

DynamoDB Streams

- DescribeStream

Amazon EC2

- DescribeInstances
- DescribeSpotFleetRequests
- DescribeSpotInstanceRequests
- DescribeTransitGatewayAttachments

Amazon Elastic Load Balancer

- DescribeLoadBalancers
- DescribeListeners
- DescribeTargetGroups
- DescribeTargetHealth

Amazon Elastic Kubernetes Service

- DescribeNodegroup
- ListNodegroups

IAM

- GetAccountAuthorizationDetails
- ListPolicies

Lambda

- GetFunction
- GetFunctionConfiguration
- ListEventSourceMappings

OpenSearch Service

- DescribeDomains
- ListDomainNames

組織

- ListAccounts
- ListAccountsForParent
- ListOrganizationalUnitsForParent
- ListRoots

Amazon Simple Notification Service

- ListSubscriptions

Amazon Security Token Service

- AssumeRole

參考資料

本節包含收集此解決方案唯一指標之選用功能的相關資訊，以及有助於此解決方案的建置器清單。

匿名資料收集

此解決方案包含將匿名操作指標傳送至 AWS 的選項。我們使用這些資料更好地了解客戶使用此解決方案、相關服務和產品的方式。啟用時，會收集下列資訊並傳送至 AWS：

- 解決方案 ID - AWS 解決方案識別符
- 唯一 ID (UUID) - 每個部署隨機產生的唯一識別符
- 時間戳記 - 資料收集時間戳記
- 已啟用成本功能 - 有關使用者是否使用成本功能的資訊
- 帳戶數量 - 使用者在其部署中加入的帳戶數量
- 圖表數量 - 每個部署中建立的圖表數量
- 資源數量 - 在所有加入的帳戶中發現的資源數量

AWS 擁有透過此問卷收集的資料。資料收集受 隱私權聲明的約束。若要選擇退出此功能，請先完成下列步驟，再啟動 AWS CloudFormation 範本。

1. 將 AWS CloudFormation 範本下載到您的本機硬碟。
2. 使用文字編輯器開啟 AWS CloudFormation 範本。
3. 從以下位置修改 AWS CloudFormation 範本映射區段：

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

至:

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

```
      CollectAnonymizedUsageMetrics: 'false'
```

1. 登入 AWS CloudFormation 主控台。
2. 選取建立堆疊。
3. 在建立堆疊頁面上，指定範本區段，選取上傳範本檔案。
4. 在上傳範本檔案下，選擇選擇檔案，然後從本機磁碟機中選取編輯過的範本。
5. 選擇下一步，然後遵循啟動堆疊中的步驟。

貢獻者

- Mohsan Jaffery
- Matthew 球
- Stefano Vozza
- Connor Kirkpatrick
- Chris Deigan
- 李尼克
- Tim Mekari

修訂

發佈日期：2020 年 9 月。如需更新，請參閱 GitHub 儲存庫中的 CHANGELOG.md 檔案。

請參閱 GitHub 儲存庫中的 CHANGELOG.md 檔案。

注意

客戶有責任對本文件中的資訊進行自己的獨立評定。本文件：(a) 僅供參考，(b) 代表目前的 AWS 產品產品和實務，這些產品和實務如有變更，恕不另行通知，且 (c) 不會從 AWS 及其附屬公司、供應商或授權方建立任何承諾或保證。AWS 產品或服務「原樣」提供，不做任何明示或暗示的保證、表示或條件。AWS 對其客戶的責任與義務應由 AWS 協議管轄，本文並非 AWS 與其客戶之間的任何協議的一部分，也並非上述協議的修改。

解決方案是根據 Apache License 2.0 版的條款進行授權。

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。