aws

使用者指南

Amazon DevOps 大師

Amazon DevOps 大師: 使用者指南

Table of Contents

什麼是 Amazon DevOps 大師？

歡迎使用 Amazon DevOps 大師用戶指南。

DevOpsGuru 是一項完全受控的作業服務，可讓開發人員和營運商輕鬆改善其應用程式的效能和可用性。 DevOpsGuru 可讓您卸載與識別作業問題相關的管理工作，以便快速實作建議以改善應用程式。 DevOpsGuru 創建反應式見解，您可以用來改善您的應用程序。它也會建立主動洞察，協助您避免 future 可能影響應用程式的操作問題。

DevOpsGuru 應用機器學習來分析您的操作數據和應用程序指標和事件，以識別偏離正常操作模式的行為。當 DevOps Guru 偵測到操作問題或風險時，您會收到通知。 DevOpsGuru 針對每個問題提供智慧型建議，以解決目前和預測的 future 營運問題。

若要開始使用，請參閱 我如何開始使用 DevOps大師？

DevOps大師如何工作？

DevOpsGuru 工作流程會在您設定涵蓋範圍和通知時開始。設置 DevOps Guru 後，它將開始分析您的操作數據。當它偵測到異常行為時，它會建立一個洞察，其中包含與問題相關的建議和指標、記錄群組和事件清單。對於每個見解， DevOpsGuru 都會通知您。如果您啟用 AWS Systems Manager OpsCenter， OpsItem 就會建立一個，讓您可以使用 Systems Manager OpsCenter 來追蹤和管理尋址您的見解。每個洞察都包含與異常行為相關的建議、指標、記錄群組和事件。在洞察中使用信息來幫助您了解和解決異常行為。

高階 DevOps大師工作流程如需三個高階工作流程步驟的詳細資訊，請參閱。請參閱詳細的工 DevOps作流程以了解更詳細的 DevOps Guru 工作流程，包括它如何與其他 AWS 服務互動。

主題

- 高階 DevOps大師工作流程
- 詳細的工 DevOps作流程

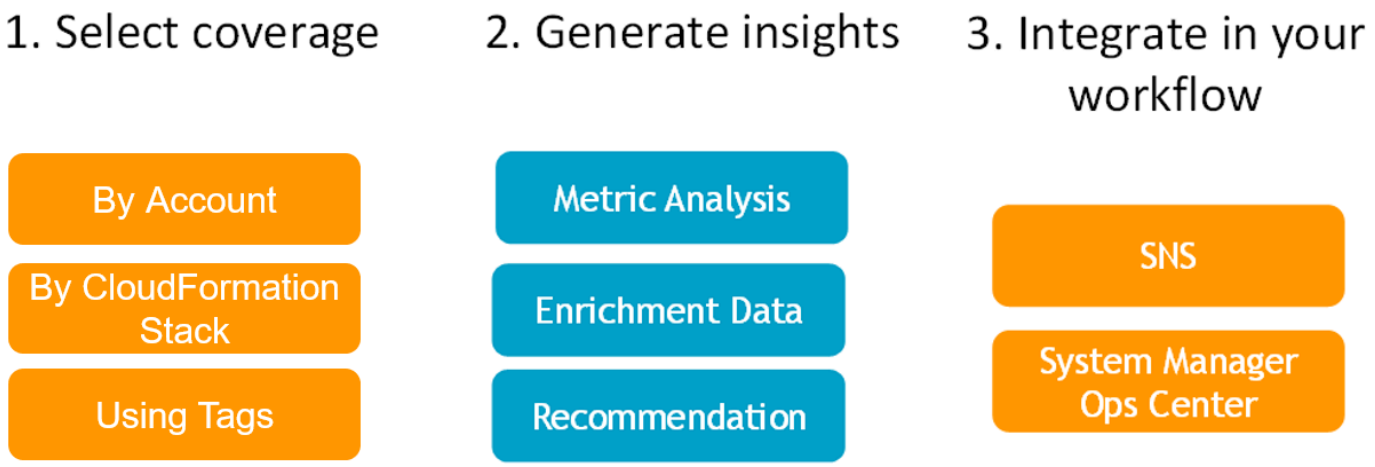
高階 DevOps大師工作流程

Amazon DevOps 大師工作流程可分為三個高階步驟。

1. 告知您 AWS 帳戶中要分析哪些 AWS 資源，以指定 DevOps Guru 涵蓋範圍。

2. DevOpsGuru 開始分析 Amazon CloudWatch 指標和其他操作資料 AWS CloudTrail，找出您可以修正以改善營運的問題。
3. DevOpsGuru 通過向您發送每個重要 G DevOps uru 事件的通知，以確保您了解見解和重要信息。

您還可以配置 DevOps Guru 創建一個 OpsItem 在， AWS Systems Manager OpsCenter 以幫助您跟踪您的見解。下圖顯示此高階工作流程。



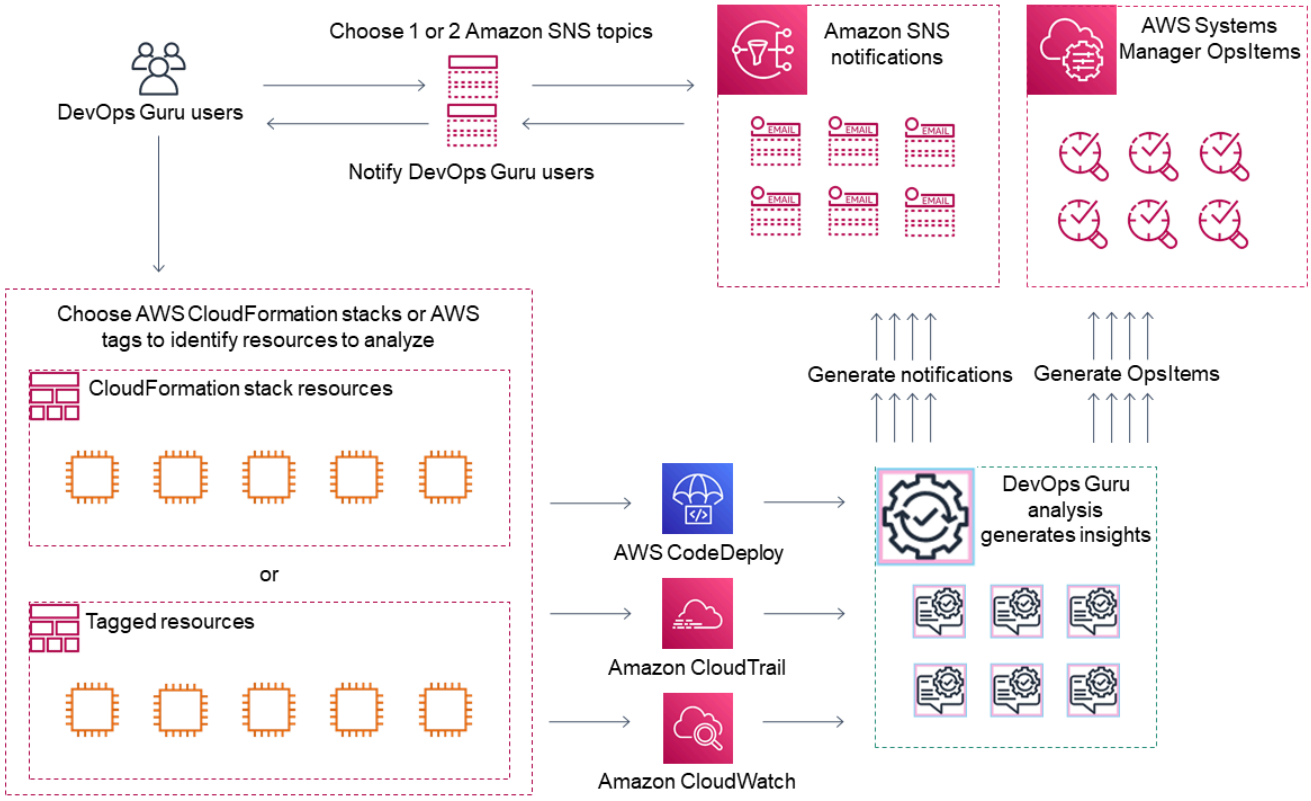
1. 在第一步中，您可以通過指定 AWS 帳戶中的哪些 AWS 資源進行分析來選擇承保範圍。DevOpsGuru 可以涵蓋或分析 AWS 帳戶中的所有資源，或者您可以使用 AWS CloudFormation 堆疊或 AWS 標籤來指定帳戶中要分析的資源子集。請確定您指定的資源組成您的業務關鍵應用程式、工作負載和微服務。如需有關支援服務和資源的詳細資訊，請參閱 Amazon DevOps Guru 定價。
2. 在第二個步驟中， DevOpsGuru 會分析資源以產生見解。這是一個持續的過程。您可以在 DevOps Guru 控制台中查看見解並查看其包含的建議和相關信息。DevOpsGuru 分析以下數據以查找問題並創建見解。
   - 您的 AWS 資源發出的個別 Amazon CloudWatch 指標。當發現問題時， DevOpsGuru 會一起收集這些指標。
   - 記錄來自 Amazon 日 CloudWatch 誌群組的異常情況。如果您啟用記錄異常偵測，則 DevOps Guru 會在發生問題時顯示相關的記錄異常。
   - DevOpsGuru 從 AWS CloudTrail 管理日誌中提取豐富資料，以查找與收集的指標相關的事件。這些事件可以是資源部署事件和組態變更。
   - 如果您使用 AWS CodeDeploy， DevOpsGuru 會分析部署事件以協助產生深入分析資訊。分析所有類型部 CodeDeploy 署的事件 (現場部署伺服器、Amazon EC2 伺服器、Lambda 或 Amazon EC2)。

- 當 DevOps Guru 找到特定模式時，它會產生一個或多個建議，以幫助緩解或修復已識別的問題。這些建議是在一個見解中收集的。深入解析也包含與問題相關的量度和事件清單。您可以使用見解資料來解決和瞭解已識別的問題。

3. 在第三個步驟中， DevOpsGuru 將洞察通知整合到您的工作流程中，以協助您管理問題並快速解決問題。
   - 在您 AWS 帳戶中產生的見解會發佈到 DevOps Guru 設定期間選擇的 Amazon 簡單通知服務 (Amazon SNS) 主題。這是創建見解後立即通知您的方式。如需詳細資訊，請參閱 更新您的通知DevOps老師。
   - 如果您 AWS Systems Manager 在 DevOps Guru 設定期間啟用，每個見解都會建立對應的資訊， OpsItem 以協助您追蹤和管理發現的問題。如需詳細資訊，請參閱 更新中AWS Systems Manager整合於DevOps老師。

詳細的工 DevOps作流程

DevOps大師工作流程與多種 AWS 服務集成, 包括 Amazon CloudWatch AWS CloudTrail, Amazon 簡單通知服務, 和 AWS Systems Manager. 下圖顯示詳細的工作流程，其中包括它如何與其他 AWS 服務搭配使用。



此圖表顯示 DevOps Guru 涵蓋範圍是由 AWS CloudFormation 堆疊中定義或使用 AWS 標籤的 AWS 資源所指定的案例。如果沒有選擇堆疊或標籤，則 DevOps Guru 涵蓋範圍會分析您帳戶中的所有 AWS 資源。如需詳細資訊，請參閱 使用定義應用程式AWS資源 及 確定覆蓋範圍DevOps大師。

1. 在安裝期間，您可以指定一個或兩個 Amazon SNS 主題，這些主題用於通知您有關重要的 DevOps Guru 事件，例如在建立洞察時。接下來，您可以指定定義您要分析的資源的 AWS CloudFormation 堆疊。您也可以啟用 Systems Manager 產生每個深入 OpsItem 分析資訊，以協助您管理深入解析。
2. DevOpsGuru 設定完成後，它會開始分析從您的資源和與 CloudWatch 指標相關的資 AWS CloudTrail 料發出的 CloudWatch指標、記錄群組和事件。如果您的作業包括 CodeDeploy 部署，DevOpsGuru 也會分析部署事件。

   DevOpsGuru 會在識別分析資料中的異常行為時，建立深入分析資料。每個見解都包含一或多個建議、用於產生深入解析的指標清單、相關記錄群組的清單，以及用來產生深入解析的事件清單。使用此資訊來解決識別的問題。
3. 建立每個深入解析之後， DevOpsGuru 會使用 Amazon SNS 主題或 DevOps Guru 設定期間指定的主題傳送通知。如果您啟用 DevOps Guru OpsItem 在 Systems Manager 器中生成一個 OpsCenter，那麼每個洞察也會觸發一個新的 Systems Manager 器OpsItem。您可以使用 Systems Manager 來管理您的見解 OpsItems。

我如何開始使用 DevOps大師？

建議您完成下列步驟：

1. 閱讀中的資訊，進一步瞭解 DevOps Guru DevOps大師概念。
2. 依照中的步驟設定您的 AWS 帳戶 AWS CLI、和管理使用者設置 Amazon DevOps 大師。
3. 按照中的說明使用 DevOps Guru 開始使用 DevOps大師。

如何停止產生 DevOps Guru 費用？

若要停用 Amazon DevOps Guru，以免因分析您 AWS 帳戶和區域中的資源而產生費用，請更新您的涵蓋範圍設定，使其不會分析資源。若要這樣做，請依照中的步驟執行，更新您的AWS分析涵蓋範圍DevOps老師並在步驟 4 中選擇「無」。您必須針對 DevOps Guru 分析資源的每個 AWS 帳戶和區域執行此操作。

> **Note**
>
> 如果您更新涵蓋範圍以停止分析資源，如果您查看 DevOps Guru 過去產生的現有見解，則可能會繼續產生小額費用。這些費用與用於擷取和顯示見解資訊的 API 呼叫相關聯。如需詳細資訊，請參閱 Amazon DevOps 大師定價。

DevOps大師概念

下列概念對於了解 Amazon DevOps Guru 的運作方式相當重要。

主題

異常

異常表示 DevOps Guru 檢測到的一個或多個意外或不尋常的相關指標。 DevOpsGuru 使用機器學習來分析與資源相關的指標和操作AWS資料，從而產生異常。您可以在設定 Amazon DevOps 大師時指定要分析的AWS資源。如需詳細資訊，請參閱設置 Amazon DevOps 大師。

Insight

深入分析是指在您設定 DevOps Guru 時指定的AWS資源分析期間所建立的異常狀況集合。每個洞察都包含觀察、建議和分析資料，您可以用來改善營運績效。有兩種類型的深入解析：

- 反應式：反應式洞察會在發生異常行為時識別出現。它包含具有建議、相關指標和事件的異常情況，可協助您立即瞭解並解決問題。
- 主動：主動洞察可讓您在異常行為發生之前了解異常行為。它包含異常和建議，以幫助您在預測問題發生之前解決問題。

指標標標標標標標

透過分析 Amazon 傳回的指標 CloudWatch 和AWS資源發出的操作事件，產生構成洞察的異常情況。您可以檢視可建立洞察力的指標和作業事件，協助您更瞭解應用程式中的問題。

日誌群組標標標標標標標記錄

當您啟用記錄異常偵測時，相關的記錄群組會顯示在 DevOps Guru 主控台的 Guru 深入解析頁面上。DevOps記錄群組可讓您瞭解有關資源執行和存取方式的重要診斷資訊。

記錄異常代表在記錄群組中發現的類似異常記錄事件的叢集。 DevOpsGuru 中可能顯示的異常記錄事件範例包括關鍵字異常、格式異常、HTTP 程式碼異常等。

您可以使用日誌異常來診斷操作問題的根本原因。 DevOpsGuru 還在洞察建議中引用日誌行，以為推薦的解決方案提供更多上下文。

> **Note**
>
> DevOpsGuru 與亞馬遜合作 CloudWatch 以啟用日誌異常檢測。當您啟用記錄異常偵測時， DevOpsGuru 會將標記新增至您的 CloudWatch 記錄群組。當您關閉記錄異常偵測時，DevOpsGuru 會從您的 CloudWatch 記錄群組中移除標記。
> 此外，管理員應確保只有具備檢視 CloudWatch 記錄檔權限的使用者才有檢視異常 CloudWatch 記錄的權限。建議您使用 IAM 政策，以便您允許或拒絕存取`ListAnomalousLogs`營運。如需詳細資訊，請參閱 DevOpsGuru Identity and Access Management。

建議

每個深入解析都提供建議，協助您改善應用程式的效能。建議包含以下內容：

- 建議動作的說明，以解決構成洞察之異常情況。
- DevOpsGuru 在其中發現異常行為的分析指標的列表。每個測量結果都包括產生與測量結果相關聯之資源的AWS CloudFormation堆疊名稱、資源名稱，以及與資源關聯的AWS服務名稱。
- 與洞察相關聯之異常量度相關的事件清單。每個相關事件都包含產生與事件相關聯之資源的AWS CloudFormation堆疊名稱、產生事件的資源名稱，以及與事件相關聯的AWS服務名稱。
- 與深入解析相關聯之異常行為相關的記錄群組清單。每個記錄群組都包含範例記錄訊息、報告的記錄異常類型的相關資訊、記錄異常發生的時間，以及檢視記錄行的連結 CloudWatch。

DevOps大師覆蓋

DevOpsGuru 為許多不同的 AWS 服務解決並創建見解。 DevOpsGuru 針對每項為其建立見解的服務，DevOps都會顯示各種分析指標和產生的見解。

反應式見解的範例使用案例：

服務名稱	使用案例	範例	指標
AWS Lambda	偵測由各種根本原因 (例如冷啟動、請求增加、下游節流或程式碼部署) 所造成的 Lambda 函數延遲或持續時間異常。建議快速減輕的方法。	程式碼部署： Amazon API Gateway 延遲會受到最近 Lambda 程式碼部署後 Lambda 延遲增加的影響。下游節流：操作員減少 DynamoDB 讀取單元的容量，導致重試次數增加。這會導致節流。冷啟動：Lambda 函數佈建不足，因此提出請求時，Lambda 需要更長的時間。	持續時間 限流

主動見解的範例使用案例：

服務名稱	使用案例	指標
Amazon DynamoDB	DynamoDB 表格讀取使用的容量有達到資料表限制的風險。建議的動作：如果您使用佈建的容量模式，請使用 auto 動擴展主動管理表格的輸送量容量，或事先購買表格的預留容量。切換到隨需容量模式以按讀取請求付費，只需為使用的內容付費。檢測時間：6 天	ConsumedReadCapacityUnits

服務範圍清單

對於某些服務，DevOpsGuru 創建反應式見解。反應式洞察會在發生異常行為時有效識別。它包含具有建議、相關指標和事件的異常情況，可協助您立即瞭解並解決問題。

對於某些服務，DevOpsGuru 創建主動的見解。主動洞察可讓您在異常行為發生之前了解異常行為。它包含異常和建議，以幫助您在預測問題發生之前解決問題。

DevOpsGuru 為以下服務創建反應式見解：

- Amazon API Gateway
- Amazon CloudFront
- Amazon DynamoDB
- Amazon EC2

> **Note**
>
> DevOpsGuru 監控是在 Auto Scaling 群組層級，而非單一執行個體層級。

- Amazon ECS
- Amazon EKS
- AWS Elastic Beanstalk
- Elastic Load Balancing
- Amazon Kinesis
- AWS Lambda
- Amazon OpenSearch Service
- Amazon RDS
- Amazon Redshift
- Amazon Route 53
- Amazon S3
- Amazon SageMaker
- AWS Step Functions
- Amazon SNS
- Amazon SQS

- Amazon SWF
- Amazon VPC

DevOpsGuru 為以下服務創建主動見解：

- Amazon DynamoDB
- Amazon Kinesis
- AWS Lambda
- Amazon RDS
- Amazon SQS

設置 Amazon DevOps 大師

完成本節中的任務以首次設定 Amazon DevOps 大師。如果您已經擁有 AWS 帳戶、知道要分析哪個帳 AWS 戶或多個帳戶，並擁有 Amazon 簡單通知服務主題可用於深入分析通知，則可以跳到開始使用 DevOps大師。

或者，您可以使用的 AWS Systems Manager「快速設定」功能來設定 DevOps Guru 並快速設定其選項。您可以使用「快速設定」為獨立帳戶或組織設定 DevOps Guru。若要使用「Systems Manager」中的「快速設定」來設定組織的 DevOps Guru，您必須具備下列先決條件：

- 一個組織與 AWS Organizations. 如需詳細資訊，請參閱《AWS Organizations 使用指南》中的AWS Organizations 術語和概念。
- 兩個或兩個以上的組織單位 (OU)。
- 每個 OU 中的一或多個目標 AWS 帳戶。
- 一個管理員帳戶，具有管理目標帳戶的權限。

若要瞭解如何使用快速設定來設定 DevOps Guru，請參閱使用AWS Systems Manager 者指南中的使用快速設定來設定 DevOps G uru。

使用以下步驟在沒有快速設置的情況下設置 DevOps Guru。

- 步驟 1 — 註冊 AWS
- 步驟 2 — 確定DevOps大師的覆蓋範圍
- 步驟 3 — 識別您的 Amazon SNS 通知主題

步驟 1 — 註冊 AWS

註冊一個 AWS 帳戶

如果您沒有 AWS 帳戶，請完成以下步驟來建立一個。

若要註冊成為 AWS 帳戶

1. 開啟 https://portal.aws.amazon.com/billing/signup。
2. 請遵循線上指示進行。

部分註冊程序需接收來電，並在電話鍵盤輸入驗證碼。

當您註冊時 AWS 帳戶，會建立AWS 帳戶根使用者一個。根使用者有權存取該帳戶中的所有 AWS 服務 和資源。安全性最佳做法是將管理存取權指派給使用者，並僅使用 root 使用者來執行需要 root 使用者存取權的工作。

AWS 註冊過程完成後，會向您發送確認電子郵件。您可以隨時登錄 https://aws.amazon.com/ 並選擇我的帳戶，以檢視您目前的帳戶活動並管理帳戶。

建立具有管理權限的使用者

註冊後，請保護您的 AWS 帳戶 AWS 帳戶根使用者 AWS IAM Identity Center、啟用和建立系統管理使用者，這樣您就不會將 root 使用者用於日常工作。

保護您的 AWS 帳戶根使用者

1. 選擇 Root 使用者並輸入您的 AWS 帳戶 電子郵件地址，以帳戶擁有者身分登入。AWS Management Console在下一頁中，輸入您的密碼。

   如需使用根使用者登入的說明，請參閱 AWS 登入 使用者指南中的以根使用者身分登入。
2. 若要在您的根使用者帳戶上啟用多重要素驗證 (MFA)。

   如需指示，請參閱《IAM 使用者指南》中的為 AWS 帳戶 根使用者啟用虛擬 MFA 裝置 (主控台)。

建立具有管理權限的使用者

1. 啟用 IAM Identity Center。

   如需指示，請參閱 AWS IAM Identity Center 使用者指南中的啟用 AWS IAM Identity Center。
2. 在 IAM 身分中心中，將管理存取權授予使用者。

   若要取得有關使用 IAM Identity Center 目錄 做為身分識別來源的自學課程，請參閱《使用指南》IAM Identity Center 目錄中的「以預設值設定使用AWS IAM Identity Center 者存取」。

以具有管理權限的使用者身分登入

- 若要使用您的 IAM Identity Center 使用者簽署，請使用建立 IAM Identity Center 使用者時傳送至您電子郵件地址的簽署 URL。

如需使用 IAM 身分中心使用者登入的說明，請參閱使用AWS 登入 者指南中的登入 AWS 存取入口網站。

指派存取權給其他使用者

1. 在 IAM 身分中心中，建立遵循套用最低權限許可的最佳做法的權限集。

   如需指示，請參閱《AWS IAM Identity Center 使用指南》中的「建立權限集」。
2. 將使用者指派給群組，然後將單一登入存取權指派給群組。

   如需指示，請參閱《AWS IAM Identity Center 使用指南》中的「新增群組」。

步驟 2 — 確定DevOps大師的覆蓋範圍

您的邊界涵蓋範圍決定 Amazon DevOps Guru 針對異常行為分析的 AWS 資源。我們建議您將資源分組到操作應用程式中。資源界限中的所有資源都應包含一或多個應用程式。如果您有一個操作解決方案，那麼您的覆蓋範圍應包括其所有資源。如果您有多個應用程式，請選擇組成每個解決方案的資源，並使用 AWS CloudFormation 堆疊或 AWS 標籤將它們分組在一起。Guru 會分析您指定的所有合併資源，無論是定義一個或多個應用程式，都會由 DevOps Guru 進行分析，並組成其涵蓋範圍界限。

使用下列其中一種方法來指定作業解決方案中的資源。

- 選擇讓您的 AWS 地區和帳戶定義您的保險範圍。使用此選項， DevOps Guru 會分析您帳戶和區域中的所有資源。如果您只將帳戶用於一個應用程序，這是一個不錯的選擇。
- 使用 AWS CloudFormation 堆疊來定義作業應用程式中的資源。 AWS CloudFormation 範本會為您定義並產生您的資源。指定在設定 DevOps Guru 時建立應用程式資源的堆疊。你可以隨時更新堆疊。您選擇的堆疊中的所有資源都會定義邊界涵蓋範圍。如需詳細資訊，請參閱 使用AWS CloudFormation堆棧以識別您的資源 DevOpsGuru。
- 使用 AWS 標籤指定應用程式中的 AWS 資源。 DevOpsGuru 僅分析包含您選擇的標籤的資源。這些資源構成了你的界限。

  標 AWS 籤由標籤鍵和標籤值組成。您可以指定一個標籤鍵，並且可以使用該鍵指定一個或多個值。針對其中一個應用程式中的所有資源使用一個值。如果您有多個應用程式，請為所有應用程式使用具有相同索引鍵的標籤，並使用標籤值將資源分組到應用程式中。所有帶有您選擇的標籤的資源都構成了 DevOps Guru 的覆蓋範圍邊界。如需詳細資訊，請參閱 使用標籤識別 DevOps Guru 應用程式中的資源。

如果您的邊界涵蓋範圍包含組成多個應用程式的資源，您可以使用標籤來篩選深入解析，以便一次檢視一個應用程式。如需詳細資訊，請參閱中的步驟 4 檢視DevOps大師洞察。

如需詳細資訊，請參閱 使用定義應用程式AWS資源。如需有關支援服務和資源的詳細資訊，請參閱 Amazon DevOps Guru 定價。

步驟 3 — 識別您的 Amazon SNS 通知主題

您可以使用一或兩個 Amazon SNS 主題來產生有關重要 DevOps Guru 事件的通知，例如在建立洞察時。這樣可以確保您盡快了解 DevOps Guru 發現的問題。設置 DevOps Guru 時，請準備好主題。使用 DevOps Guru 主控台設定 G DevOps uru 時，您可以使用其名稱或其 Amazon 資源名稱 (ARN) 來指定通知主題。如需詳細資訊，請參閱啟用 DevOps Guru。您可以使用 Amazon SNS 主控台來檢視每個主題的名稱和 ARN。如果您沒有主題，可以在 DevOps使用 Guru 主控台啟用 DevOps Guru 時建立主題。如需詳細資訊，請參閱 Amazon 簡單通知服務開發人員指南中的建立主題。

新增至您的 Amazon SNS 主題的許可

Amazon SNS 主題是包含 AWS Identity and Access Management (IAM) 資源政策的資源。當您在此指定主題時， DevOpsGuru 會將下列權限附加至其資源策略。

```
{
    "Sid": "DevOpsGuru-added-SNS-topic-permissions",
    "Effect": "Allow",
    "Principal": {
        "Service": "region-id.devops-guru.amazonaws.com"
    },
    "Action": "sns:Publish",
    "Resource": "arn:aws:sns:region-id:topic-owner-account-id:my-topic-name",
    "Condition" : {
      "StringEquals" : {
        "AWS:SourceArn": "arn:aws:devops-guru:region-id:topic-owner-account-
id:channel/devops-guru-channel-id",
        "AWS:SourceAccount": "topic-owner-account-id"
    }
  }
}
```

DevOpsGuru 使用主題發佈通知需要這些權限。如果您不想擁有該主題的這些權限，則可以安全地將其移除，並且該主題將繼續像您選擇之前的那樣運作。不過，如果移除這些附加的權限，DevOpsGuru 就無法使用主題來產生通知。

估算 Amazon DevOps 大師資源分析成本

您可以估算 Amazon DevOps 大師分析 AWS 資源的每月成本。您需為指定資源涵蓋範圍內每個作用中 AWS 資源的分析時數付費。如果資源在一小時內產生指標、事件或記錄，就會處於作用中狀態。

DevOps Guru 會掃描您選取的資源，以建立每月成本估算。您可以檢視資源、每小時計費價格，以及預估的每月費用。成本估算器會假設為預設值，已分析的使用中資源會 100% 使用時間。您可以根據您的預估使用量變更每個已分析服務的這個百分比，以建立更新的每月費用估算。此預估是用於分析資源的成本，不包含與 DevOps Guru API 呼叫相關的成本。

您可以一次建立一個成本估算。產生成本預估所需的時間，取決於您在建立成本預估時指定的資源數目。當您指定一些資源時，可能需要 1 到 2 個小時才能完成。當您指定大量資源時，最多可能需要 4 小時才能完成。您的實際成本會有所不同，而且取決於分析的使用中資源所使用的時間百分比。

> **Note**
>
> 對於成本估算，您只能指定一個AWS CloudFormation堆疊。對於實際涵蓋範圍邊界，您最多可以指定 1000 個堆疊。

若要建立每月資源分析成本預估

1. 在以下位置打開 Amazon DevOps 大師控制台 https://console.aws.amazon.com/devops-guru/。
2. 在導覽窗格中選擇 [成本估算器]。
3. 如果您尚未啟用 DevOps Guru，則必須建立 IAM 角色。在出現的「為 DevOps Guru 建立 IAM 角色」快顯視窗中，選擇「同意」以建立 IAM 角色。這可讓 DevOps Guru 在您選擇開始成本估算分析或開始使用 DevOps Guru 時，為您建立 IAM 服務連結角色。如此一來， DevOpsGuru 就擁有建立成本估算所需的權限。如果您已啟用 DevOps Guru，表示角色已建立，且不會顯示此選項。
4. 選擇您要用來建立估算值的資源。

   - 如果您要估算 DevOps Guru 分析一個AWS CloudFormation堆疊所定義之資源的成本，請執行下列動作。

     1. 在當前區域中選擇CloudFormation 堆棧。
     2. 在 [選擇 CloudFormation 堆疊] 中，選擇AWS帳戶中的AWS CloudFormation堆疊名稱。您也可以輸入堆疊的名稱以快速找到它。如需使用和檢視堆疊的詳細資訊，請參閱《AWS CloudFormation使用指南》中的「使用堆疊」。

3. (選擇性) 如果您使用目前未分析的AWS CloudFormation堆疊，請選擇啟用資源分析，讓 DevOps Guru 開始分析其資源。如果您尚未啟用 DevOps Guru 或您已經在分析堆疊中的資源，則無法使用此選項。

- 如果您要估算 DevOps Guru 使用標籤分析資源的成本，請執行以下操作。
  1. 選擇目前區域中AWS資源的標籤
  2. 在標籤鍵中選擇標籤的密鑰
  3. 在「標記值」中，選擇 (所有值) 或選擇一個值。
- 如果您要估算 DevOps Guru 分析您AWS帳戶和區域中資源的成本，請選擇目前區域中的AWS帳戶。

5. 選擇估算每月費用。
6. (選擇性) 在作用中資源使用率百分比欄中，輸入一或多個 AWS 服務的更新百分比值。預設的有效資源使用率百分比為 100%。這表示 DevOps Guru 透過計算分析資源一小時的成本來產生 AWS 服務的估算值，然後推斷超過 30 天，總共 720 小時。如果服務的使用中時間少於 100%，您可以根據預估的使用量更新百分比，以獲得更準確的估計值。例如，如果您將服務的有效資源使用率更新為 75%，則分析其資源的一小時成本會推斷超過 (720 x 0.75) 小時或 540 小時。

如果您的估計金額為零，則您選擇的資源可能不包含 DevOps Guru 所支援的資源。如需有關支援服務和資源的詳細資訊，請參閱 Amazon DevOps Guru 定價。

開始使用 DevOps大師

在本節中，您將學習如何開始使用 Amazon DevOps Guru，以便分析應用程式的操作資料和指標，以產生洞察。

主題

步驟 1：設定

在開始之前，請先執行中的步驟來準備設置 Amazon DevOps 大師。

步驟 2：啟用DevOps大師

若要將 Amazon DevOps Guru 設定為第一次使用，您必須選擇設定 DevOps大師的方式。您可以監控整個組織的應用程式，也可以監視目前帳戶中的應用程式。

您可以監控整個組織的應用程式，或僅針對目前帳戶啟用 DevOps Guru。以下程序概述了根據您的需求設置 DevOps Guru 的不同方法。

監控整個組織的帳戶

如果您選擇監控整個組織的應用程式，請登入您的組織管理帳戶。您可以選擇性地將組織成員帳戶設定為委派的管理員。您一次只能有一個委派管理員，稍後可以修改管理員設定。您設定的管理帳戶和委派的系統管理員帳戶都可以存取組織中所有帳戶的所有深入解析。

您可以使用主控台為組織新增跨帳戶支援，也可以使用 AWS CLI 來執行此操作。

與 DevOps Guru 控制台一起上載

您可以使用主控台新增對整個組織帳戶的支援。

使用主控台可讓 DevOps Guru 檢視彙總見解

1. 在以下位置打開 Amazon DevOps 大師控制台 https://console.aws.amazon.com/devops-guru/。
2. 選擇「監視整個組織的應用程式」作為設定類型。

3. 選擇您要作為委派管理員使用的帳戶。然後，選擇 [註冊委派管理員]。這可讓您存取任何已啟用 DevOps Guru 的帳戶的整合檢視。委派的系統管理員擁有整個組織中所有 DevOps Guru 深入解析和指標的整合檢視。您可以使用 SSM 快速設定或 AWS CloudFormation 堆疊集來啟用其他帳戶。要了解有關快速設置的更多信息，請參閱使用快速設置配置 DevOps Guru。若要進一步了解如何設定堆疊組合，請參閱使用AWS CloudFormation者指南中的使用堆疊和步驟 2 — 確定DevOps大師的覆蓋範圍. 和使用AWS CloudFormation堆棧以識別您的資源 DevOpsGuru。

透過 AWS CLI 進行板載

您可以使用 AWS CLI 來啟用 DevOps Guru 檢視彙總見解。執行下列命令。

```
aws iam create-service-linked-role --aws-service-name devops-guru.amazonaws.com --
description "My service-linked role to support DevOps Guru"

aws organizations enable-aws-service-access --service-principal devops-
guru.amazonaws.com

aws organizations register-delegated-administrator --account-id >ACCOUNT_ID< --service-
principal devops-guru.amazonaws.com
```

下表描述了這些命令。

Command	描述
`create-service-linked-role`	授與 DevOps Guru 收集組織相關資訊的權限。如果此步驟不成功，請勿繼續。
`enable-aws-service-access`	登陸您的組織到 DevOps大師。
`register-delegated-administrator`	允許訪問成員帳戶以查看見解。

監控您目前的帳戶

如果您選擇監控目前 AWS 帳戶中的應用程式，請選擇要涵蓋或分析帳戶和區域中的哪些 AWS 資源，並指定一或兩個 Amazon 簡單通知服務主題，這些主題在建立洞察時用來通知您。您可以稍後視需要更新這些設定。

使 DevOps Guru 能夠監控您當前 AWS 帳戶中的應用程序

1. 在以下位置打開 Amazon DevOps 大師控制台 https://console.aws.amazon.com/devops-guru/。
2. 選擇當前 AWS 帳戶中的監視應用程序作為設置類型。
3. 在 DevOpsGuru 分析涵蓋範圍中，選擇下列其中一項。

   - 分析當前 AWS 帳戶中的所有 AWS 資源： DevOpsGuru 分析您帳戶中的所有 AWS 資源。
   - 選擇要稍後分析的 AWS 資源：稍後再選擇分析界限。如需詳細資訊，請參閱 確定覆蓋範圍 DevOps大師 及 更新您的AWS分析涵蓋範圍 DevOps老師。

   DevOpsGuru 可以分析與其支持的 AWS 帳戶相關聯的任何資源。如需有關支援服務和資源的詳細資訊，請參閱 Amazon DevOps Guru 定價。
4. 您最多可以新增兩個主題。 DevOpsGuru 使用主題或主題來通知您有關 DevOps Guru 重要事件的資訊，例如建立新的見解。如果您現在未指定主題，可以稍後透過在導覽窗格中選擇 [設定] 來新增主題。

   a. 在指定 Amazon SNS 主題中，選擇要使用的主題。
   b. 若要新增 Amazon SNS 主題，請執行下列其中一個動作。

      - 選擇使用電子郵件產生新的 SNS 主題。然後，從指定電子郵件地址中，輸入您要接收通知的電子郵件地址。若要輸入其他電子郵件地址，請選擇 [新增電子郵件]。
      - 選擇「使用現有的 SNS 主題」。然後，從選擇 AWS 帳戶中的主題中，選擇您要使用的主題。
      - 選擇「使用現有的 SNS 主題 ARN」，從其他帳戶指定現有的主題。然後，在輸入主題的 ARN 中，輸入主題 ARN。ARN 是該主題的 Amazon 資源名稱。您可以在不同的帳戶中指定主題。如果您在其他帳號中使用某個主題，則必須將資源策略新增至該主題。如需詳細資訊，請參閱 Amazon SNS 主題的許可。
5. 選擇 啟用 。

若要將 Amazon DevOps Guru 設定為第一次使用，您必須選擇要涵蓋或分析帳戶和區域中的哪些 AWS 資源，並指定一或兩個 Amazon 簡單通知服務主題，這些主題在建立洞察時用來通知您。您可以稍後視需要更新這些設定。

步驟 3：指定您的 DevOps Guru 資源涵蓋範圍

如果您選擇稍後在啟用 DevOps Guru 時指定 AWS 資源，則需要在 AWS 帳戶中選擇 AWS CloudFormation 堆疊，以建立您要分析的資源。 AWS CloudFormation 堆疊是您以單一單元形式管理的 AWS 資源集合。您可以使用一或多個堆疊來包含執行作業應用程式所需的所有資源，然後加以指定，以便 DevOps Guru 對其進行分析。如果您未指定堆疊，則 DevOps Guru 會分析您帳戶中的所有 AWS 資源。如需詳細資訊，請參閱《AWS CloudFormation 使用指南》中的〈使用堆疊〉和〈〉和確定覆蓋範圍DevOps大師使用AWS CloudFormation堆棧以識別您的資源 DevOpsGuru。

> **Note**
>
> 如需有關支援服務和資源的詳細資訊，請參閱 Amazon DevOps Guru 定價。

指定 DevOps Guru 資源涵蓋率

1. 在以下位置打開 Amazon DevOps 大師控制台 https://console.aws.amazon.com/devops-guru/。
2. 展開導覽窗格中的 [設定]。
3. 在 [分析資源] 中，選擇 [編輯分析的資源
4. 選擇下列其中一個保障選項。

   - 如果您希望 DevOps Guru 分析您帳戶和區域中所有支援的資源，請選擇 [所有 AWS 帳號資源]。如果您選擇此選項，您的 AWS 帳戶就是您的資源分析涵蓋範圍界限。您帳戶中每個堆疊中的所有資源都會分組到他們自己的應用程式中。任何不在堆疊中的剩餘資源都會分組到它們自己的應用程式中。
   - 如果您希望 DevOps Guru 分析您選擇CloudFormation 的堆疊中的資源，請選擇「堆疊」，然後選擇下列其中一個選項。
     - 所有資源 — 分析帳戶中堆疊的所有資源。每個堆疊中的資源會分組到它們自己的應用程式中。不會分析您帳戶中未在堆疊中的任何資源。
     - 選取堆疊 — 選取您要 DevOps Guru 分析的堆疊。您選取的每個堆疊中的資源會分組到它們自己的應用程式中。您可以在「尋找堆疊」中輸入堆疊的名稱，以快速找到特定堆疊。您最多可以選擇 1,000 個堆疊。

     如需詳細資訊，請參閱 使用AWS CloudFormation堆棧以識別您的資源 DevOpsGuru。
   - 如果您希望 DevOps Guru 分析包含您選擇之標籤的所有資源，請選擇「標籤」。選擇按鍵，然後選擇下列其中一個選項。

- 所有帳戶資源 — 分析目前區域和帳戶中的所有 AWS 資源。具有所選標籤鍵的資源會依標籤值分組 (如果有的話)。沒有此標籤鍵的資源會分別分組和分析。
- 選擇特定標籤值 — 分析所有包含含有您選擇鍵之標籤的資源。 DevOpsGuru 根據標籤的值將您的資源分組到應用程序中。

  標籤的密鑰必須以前綴開頭devops-guru-。此前綴不區分大小寫。例如，有效的金鑰為DevOps-Guru-Production-Applications。如需詳細資訊，請參閱 使用標籤識別 DevOps Guru 應用程式中的資源。

- 如果您不希望 DevOps Guru 分析任何資源，請選擇「無」。此選項會停用 DevOps Guru，以便您停止因資源分析而產生費用。

5. 選擇 Save (儲存)。

啟用 DevOps Guru 分析AWS服務

亞馬遜DevOps大師可以分析它支持的任何AWS資源的性能。當它發現異常行為時，它會生成一個洞察力，其中包含有關該行為以及如何解決它的詳細信息。如需有關支援服務和資源的詳細資訊，請參閱 Amazon DevOps Guru 定價。

DevOpsGuru 使用 Amazon CloudWatch 指標、AWS CloudTrail事件等來協助分析資源。它支持的大多數資源都會自動生成 DevOps Guru 分析所需的指標。不過，有些AWS服務需要額外的動作才能產生所需的指標。對於某些服務，啟用這些指標可為現有 DevOps Guru 涵蓋範圍提供額外的分析。對於其他人，除非您啟用這些量度，否則無法進行分析。如需詳細資訊，請參閱 確定覆蓋範圍DevOps大師 及 更新您的AWS分析涵蓋範圍 DevOps老師。

需要針對 DevOps Guru 分析採取行動的服務

- Amazon 彈性容器服務 — 若要產生其他指標以改善其資源的 DevOps Guru 涵蓋範圍，請按照在 Amazon ECS 上設定容器見解中的步驟進行操作。這樣做可能會產生亞馬遜CloudWatch費用。
- 亞馬遜彈性 Kubernetes 服務 — 若要產生指標以供 DevOps Guru 分析，請按照在 Amazon EKS 和 Kubernetes 上設定容器洞見中的步驟進行操作。DevOps在設置這些指標的生成之前，大師不會分析任何 Amazon EKS 資源。這樣做可能會產生亞馬遜CloudWatch費用。
- Amazon 簡單儲存服務 — 若要產生指標供 DevOps Guru 分析，您必須啟用請求指標。請依照建立值區中所有物件的CloudWatch指標組態中的步驟進行。DevOps在設置這些指標的生成之前，Guru不會分析任何 Amazon S3 資源。這樣做可能會產生CloudWatch和亞馬遜 S3 費用。

如需詳細資訊，請參閱 Amazon CloudWatch 定價。

使用深入解析DevOps老師

亞馬遜DevOps大師生成一個洞察力當它檢測到操作應用程序中的異常行為時。DevOps大師分析了指標，事件等AWS您在設定時指定的資源DevOps大師。每個見解都包含一個或多個建議，供您採取以緩解此問題。它也包含量度清單、記錄群組清單，以及用來識別異常行為的事件清單。

有兩種洞察力類型。

- 反應性見解提供您可以採取的建議來解決目前正在發生的問題。
- 主動洞察有解決問題的建議DevOps大師預測將在未來發生。

主題

檢視DevOps大師洞察

您可以使用AWS Management Console。

檢視您的DevOps大師洞察

1. 打開亞馬遜DevOps大師控制台在https://console.aws.amazon.com/devops-guru/。
2. 開啟導覽窗格，然後選擇洞察力。
3. 在「」反應性選項卡中，您可以看到被動見解的列表。在「」主動選項卡中，您可以看到主動見解的列表。
4. (選擇性) 使用下列一或多個篩選器尋找您要尋找的深入解析。
   - 選擇合適的反應性或者主動選項卡，具體取決於您正在尋找的洞察力的類型。
   - 選擇篩選見解，然後選擇選項以指定篩選。您可以新增狀態、嚴重性、資源和標籤篩選器的組合。使用一個AWS標籤篩選器可檢視僅由具有特定標籤的資源所產生的見解。如需進一步了解，請參閱 使用標籤識別 DevOps Guru 應用程式中的資源。

> **Note**
>
> DevOpsGuru 可以分析以下資源，但無法使用標籤篩選其見解。
>
> - 亞馬遜 API 閘道路徑和路由
> - 亞馬遜串流
> - 亞馬遜 EC2 自動擴展組執行個體
> - AWS Elastic Beanstalk 環境
> - 亞馬遜紅移節點

- 選擇或指定時間範圍，以依據深入解析建立時間進行篩選。
  - 12 小時顯示過去 12 小時內建立的見解。
  - 1D顯示過去一天所建立的見解。
  - 1 瓦特顯示在過去一周創建的見解。
  - 1 米顯示在過去一個月創建的見解。
  - 自訂可讓您指定其他時間範圍。您可以用來篩選見解的最長時間範圍為 180 天。

5. 若要檢視有關分析的詳細資料，請選擇其名稱。

了解中的見解DevOps大師控制台

使用亞馬遜DevOpsGuru 主控台可在您的見解中檢視有用的資訊，以協助您診斷並解決異常行為。何時DevOps大師分析您的資源並找到相關的亞馬遜CloudWatch度量，AWS CloudTrail事件和指示異常行為的操作數據，它創建了一個洞察力，其中包含解決問題的建議以及有關相關指標和事件的信息。使用深入解析資料DevOps 專家中的最佳實踐解決檢測到的操作問題DevOps大師。

若要檢視深入分析，請依照中的步驟執行檢視見解找到一個，然後選擇它的名稱。分析頁面包含下列詳細資料。

洞察概述

您可以使用此區段取得深入解析的高階概觀。您可以查看見解的狀態 (持續中或者封閉），多少AWS CloudFormation堆疊會受到影響、深入解析開始、結束和上次更新的時間，以及相關的作業項目 (如果有的話)。

如果洞察分組在堆疊層級，然後您可以選擇受影響的堆疊數量以查看其名稱。建立洞察的異常行為發生在受影響堆疊所建立的資源中。如果洞察分組在帳戶層級，則數字為零或不顯示。

如需詳細資訊，請參閱了解異常行為如何歸類為見解。

洞見名稱

洞察的名稱取決於它是否被分組在堆疊層級或帳戶層級。

- 堆疊層級洞察力名稱包括包含資源及其異常行為的堆疊名稱。
- 帳戶級別見解名稱不包含堆疊名稱。

如需詳細資訊，請參閱了解異常行為如何歸類為見解。

彙總指標

選擇合適的彙總指標索引標籤可檢視與深入解析相關的量度。在表格中，每一列代表一個測量結果。你可以看到哪個AWS CloudFormation棧創建了發出指標，資源名稱及其類型的資源。並非所有測量結果都與AWS CloudFormation堆棧或有一個名稱。

當同時存在多個資源異常時，時間軸檢視會彙總資源，並在單一時間軸中顯示其異常指標，以便於分析。時間軸上的紅線表示量度發出不尋常值時的時間範圍。若要放大，請使用滑鼠選擇特定的時間範圍。您也可以使用放大鏡圖示來放大和縮小。

在時間軸中選擇紅線以檢視詳細資訊。在打開的窗口中，您可以：

- 選擇在中檢視CloudWatch以查看量度在CloudWatch控制台。如需詳細資訊，請參閱統計和尺寸在亞馬遜CloudWatch使用者指南。
- 將滑鼠游標暫留在圖表上，即可檢視異常量度資料及發生時間的詳細資料。
- 選擇帶有向下箭頭的框以下載圖形的 PNG 圖像。

图形异常

選擇合適的图形异常索引標籤可檢視每個洞察異常的詳細圖表。每個異常都會顯示一個磚，其中包含相關量度中偵測到的異常行為的詳細資訊。您可以調查並查看資源級別和每個統計數據的異常情況。圖表會依量度名稱分組。在每個動態磚中，您可以在時間軸中選擇要縮放的特定時間範圍。您也可以使用放大鏡圖示來放大和縮小，或選擇以小時、天或週為單位的預先定義持續時間 (1 小時,3 小時,12 小時,1D,3D,1 瓦特，或2 瓦特).

選擇檢視所有統計資料和維度以查看有關異常的詳細信息。在打開的窗口中，您可以：

- 選擇在中檢視CloudWatch以查看量度在CloudWatch控制台。

- 將滑鼠游標暫留在圖表上，即可檢視異常量度資料及發生時間的詳細資料。
- 選擇統計或者尺寸以自訂圖形的顯示。如需詳細資訊，請參閱統計和尺寸在亞馬遜CloudWatch使用者指南。

日誌群組

當您啟用記錄異常偵測時，DevOps大師標籤您的CloudWatch記錄群組讓您可以檢視與見解相關的記錄群組。在記錄群組在見解詳細資訊頁面的區段中，表格中的每一列代表一個記錄群組，並列出相關的資源。

當同時有多個異常記錄群組時，時間軸檢視會彙總它們，並將它們顯示在單一時間軸中，以便於分析。時間軸上的紫色線條表示記錄群組發生記錄異常時的時間範圍。

選擇時間軸中的紫色線條，以檢視日誌異常資訊的範例，例如關鍵字例外和數值偏差。選擇檢視記錄群組詳情以檢視記錄異常。在打開的窗口中，您可以：

- 檢視記錄異常和相關事件的圖表。
- 將滑鼠游標暫留在圖表上，即可檢視異常記錄資料及其發生時間的詳細資料。
- 透過範例訊息、預訂頻率、相關建議和發生時間，詳細檢視記錄異常。
- 點擊查看詳細信息CloudWatch以檢視記錄異常中的記錄行。

相關活動

在相關活動，檢視AWS CloudTrail與您的見解有關的事件。使用這些事件來協助瞭解、診斷和解決異常行為的根本原因。

建議

在建議，您可以檢視可能有助於解決潛在問題的建議。何時DevOps大師檢測異常行為，它試圖創建建議。深入解析可能包含一個、多個或零個建議。

了解異常行為如何歸類為見解

洞察力分組在堆疊層級或帳戶層級。如果針對位於AWS CloudFormation堆棧，那麼它是一個堆疊層級洞察力。否則，它是一個帳戶層級洞察力。

堆疊的分組方式取決於您在 Amazon 中設定資源分析涵蓋範圍的方式DevOps大師。

如果您的承保範圍由AWS CloudFormation堆疊

系統會分析您選擇的堆疊中包含的所有資源，而所有偵測到的見解都會分組在堆疊層級。

如果您的保障範圍是您目前的AWS帳戶和地區

系統會分析您帳戶和區域中的所有資源，並且有三種可能的分組案例可用於偵測到的見解。

- 從不屬於堆疊一部分的資源產生的見解會分組在帳戶層級。
- 從資源產生的深入解析，該資源位於前 10,000 個已分析堆疊中的其中一個，會分組在堆疊層級。
- 從不在前 10,000 個已分析堆疊之一的資源產生的深入分析資訊會分組在帳戶層級。例如，針對分析的 10,000 個堆疊中的資源產生的深入解析會分組在帳戶層級。

如需詳細資訊，請參閱確定覆蓋範圍DevOps大師。

了解洞察嚴重性

洞察力可以有三種嚴重性之一，高,中等，或低。一個洞察力是由亞馬遜創造DevOps在檢測到相關異常並為每個異常分配嚴重性之後，Guru。DevOpsGuru 將異常分配的嚴重性為高,中等，或低使用領域知識和多年的集體經驗。洞察力的嚴重性取決於建立洞察力的最嚴重的異常情況。

- 如果產生洞察力的所有異常的嚴重性為低，那麼洞察力的嚴重性是低。
- 如果產生洞察力的所有異常的最高嚴重性為中等，那麼洞察力的嚴重性是中等。產生洞察力的一些異常的嚴重性可能是低。
- 如果產生洞察力的所有異常的最高嚴重性為高，那麼洞察力的嚴重性是高。產生洞察力的一些異常的嚴重性可能是低或者中等。

使用 DevOps Guru 監視資料庫

DevOps大師提供了在操作數據庫顯著價值 AWS. 通過利用其機器學習算法， DevOpsGuru 可以幫助優化數據庫性能，提高可靠性並減少營運開銷。使用者指南的這一節提供這些資料庫功能的高階概觀，包括不同資料 AWS 庫服務的特定 DevOps Guru 使用案例。

DevOps大師可以為關聯式資料庫 (例如 Amazon RDS 和 Amazon Redshift. 它也可以提供非關聯式或 NoSQL 資料庫的見解，例如 Amazon DynamoDB 和. Amazon ElastiCache

主題

使用 DevOps Guru 監視關聯資料庫

DevOpsGuru 從兩個主要資料來源提取，以尋找關聯式資料庫中的洞察和異常情況。對於 Amazon RDS 和 Amazon Redshift， CloudWatch 系統會針對所有執行個體類型分析提供指標。對於 Amazon RDS，也會擷取下列引擎類型的 Performance Insights 資料：RDS 版、Aurora 和 Aurora MySQL。

監控 Amazon RDS 中的數據庫操作

本節包含有關 DevOps Guru for RDS 中監控的使用案例和指標的特定資訊，包括來自 CloudWatch 付費指標和 Performance Insights 的資料。如需有關 DevOps Guru for RDS 的詳細資訊，包括關鍵概念、組態和權益，請參閱the section called “使用 RDS 的 DevOps大師中的異常”。

使用來自付費指標的 CloudWatch 數據監控 RDS

DevOpsGuru 能夠通過導入默認 CloudWatch 指標（例如 CPU 使用率和讀寫操作延遲）來監控每種類型的 RDS 實例。由於預設會提供這些指標，因此當您使用 DevOps Guru 監控 RDS 執行個體時，無需進一步設定即可取得見解。 DevOpsGuru 會根據歷史模式自動建立這些指標的基準，並將它們與即時資料進行比較，以偵測資料庫中的異常和潛在問題。

下表顯示來自供貨指標的 Amazon RDS 潛在 CloudWatch 被動洞察清單。

AWS 由 DevOps大師監控的資源	DevOps大師識別的場景	CloudWatch 監控的指標
Amazon RDS（所有執行個體類型）	CPU 或記憶體達到限制	資料庫載入, DBLOADCPU
RDS for PostgreSQL	高複寫插槽延遲	OldestReplicationSlotLag

DevOpsGuru 監控的來自 Amazon RDS 執行個體的其他 CloudWatch 銷售指標：

- CPUUtilization
- DatabaseConnections
- DiskQueueDepth
- 失敗的 SQL ServerAgentJobsCount
- ReadLatency
- ReadThroughput
- ReplicaLag
- WriteLatency

使用 Performance Insights 見中的資料監控 RDS

對於某些類型的 Amazon RDS 執行個體 (例如 Aurora PostgreSQL、Aurora MySQL 和 RDS 版 PostgreSQL)，您可以確保在這些執行個體上啟用效能洞見，從 DevOps大師監控中釋放更多功能。

DevOpsGuru 為各種情況提供了反應式見解，包括以下情況：

DevOpsGuru 識別以生成反應式洞察的場景
鎖定爭用問題
缺少索引
應用程序池配置錯誤
次優的 JDBC 默認值

DevOpsGuru 為各種情況提供主動洞察，包括以下情況：

AWS 由 DevOps大師監控的資源	DevOpsGuru 識別以產生主動洞察的場景
Aurora MySQL	InnoDB 歷史記錄列表越來越大，這可能會導致性能下降，例如冗長的數據庫關閉時間
Aurora MySQL	在磁碟上建立的暫存資料表增加，可能會影響資料庫效能
適用於 PostgreSQL 的 RDS	在事務中閒置時間過長的連接，保持鎖定，阻止其他查詢以及防止真空（包括 auto真空）清理死行的潛在影響

監視資料庫作業 Amazon Redshift

DevOpsGuru 能夠通過導入默認 CloudWatch 指標來監視您的 Amazon Redshift 資源，包括 CPU 使用率和使用的磁盤空間百分比。由於預設會提供這些指標，因此 DevOps Guru 不需要進一步設定即可自動監控您的 Amazon Redshift 資源。 DevOpsGuru 會根據歷史模式為這些指標建立基準，並將它們與即時資料進行比較以偵測異常。

DevOps大師識別的場景	CloudWatch 監控的指標
偵測由叢集工作負載、偏斜和未排序的資料或領導節點工作等因素造成的 Amazon Redshift 執行個體高 CPU 使用率	CPUUtilization
偵測 Amazon Redshift 執行個體是否因為查詢處理、散發和排序索引鍵、維護作業或標記區塊的問題而導致磁碟空間不足	PercentageDiskSpaceUsed

DevOpsGuru 監控 Amazon Redshift 執行個體的其他 CloudWatch 供應指標：

- DatabaseConnections
- HealthStatus
- MaintenanceMode

- NumExceededSchemaQuotas
- PercentageQuotaUsed
- QueryDuration
- QueryRuntimeBreakdown
- ReadIOPS
- ReadLatency
- WLM QueueLength
- WLM QueueWaitTime
- WLM QueryDuration
- WriteLatency

使用 RDS 的 DevOps大師中的異常

DevOpsGuru 會針對支援的AWS資源 (包括 Amazon RDS 引擎) 偵測、分析並提供建議。對於已開啟 Performance Insights 的 Amazon Aurora 和 RDS for PostgreSQL 資料庫執行個體，適用於 RDS 的 DevOps大師會針對效能問題提供詳細的資料庫特定分析，並建議修正動作。

主題

- RDS 大 DevOps師概述
- 為 RDS 啟用 DevOps大師
- 分析 Amazon RDS 中的異常

RDS 大 DevOps師概述

接下來，您可以找到 DevOps Guru for RDS 的主要優點和功能的摘要。如需深入解析和異常情況的背景，請參閱 DevOps大師概念。

主題

- RDS 大 DevOps師的好處
- 資料庫效能調整的關鍵概念
- RDS DevOps 大師的關鍵概念
- RDS 的 DevOps大師如何工作
- 支援資料庫引擎

RDS 大 DevOps師的好處

如果您負責 Amazon RDS 資料庫，您可能不知道正在發生影響該資料庫的事件或回歸。得知問題時，您可能不知道為何發生或如何處理。您可以遵循 DevOps Guru for RDS 的建議，而不是向資料庫管理員 (DBA) 尋求協助或依賴第三方工具。

您可以從 RDS 的 DevOps大師的詳細分析中獲得以下優勢：

快速診斷

DevOpsRDS 大師持續監視和分析資料庫遙測。Performance Insights、增強型監控和 Amazon 會 CloudWatch 收集資料庫執行個體的遙測資料。 DevOpsGuru for RDS 使用統計和機器學習技術來挖掘這些數據並檢測異常。若要進一步了解 Amazon Aurora 資料庫的遙測資料，請參閱使用 Amazon Aurora 上的 Performance Insights 來監控資料庫負載和 Amazon Aurora 使用者指南中的使用增強型監控來監控作業系統。若要進一步了解其他 Amazon RDS 資料庫的遙測資料，請參閱使用 Amazon 關聯式資料庫服務的 Performance Insights 來監控資料庫負載和 Amazon RDS 使用者指南中的增強型監控來監控作業系統指標。

快速解決

每個異常都指出效能問題，並建議調查途徑或更正行動。例如，RDS 版 DevOps Guru 可能會建議您調查特定的等待事件。或者，可能建議您調整應用程式集區設定，以限制資料庫連線的數目。採用這些建議，解決效能問題會比手動疑難排解更快。

主動式洞察

DevOpsGuru for RDS 使用資源中的指標來檢測潛在問題的行為，然後再成為更大的問題。例如，它可以偵測連線到資料庫的工作階段何時未執行使用中工作，而且可能會封鎖資料庫資源。DevOps然後，Guru 提供建議以幫助您在問題變得更大的問題之前解決問題。

Amazon 工程師和機器學習的深厚知識

為了偵測效能問題並協助您解決瓶頸，適用於 RDS 的 DevOps Guru 仰賴機器學習 (ML) 和進階統計分析。Amazon 資料庫工程師為開發 RDS 的 DevOps Guru 做出了貢獻，其中包含了管理數十萬個資料庫的多年。通過利用這個集體知識， DevOpsGuru for RDS 可以教你最佳實踐。

資料庫效能調整的關鍵概念

DevOpsRDS 大師假設您熟悉幾個關鍵的效能概念。若要進一步了解這些概念，請參閱 Amazon Aurora 使用者指南中的效能洞見概觀或 Amazon RDS 使用者指南中的 Performance Insights 概觀。

主題

- 指標
- 問題偵測
- 資料庫負載
- 等待事件

指標

指標代表按時間順序排列的資料集點。您可以將指標視為要監控的變數，且資料點代表該變數隨著時間的值。Amazon RDS 可即時為資料庫和執行資料庫執行個體所在的作業系統 (OS) 提供指標。您可以在 Amazon RDS 主控台上檢視 Amazon RDS 資料庫執行個體的所有系統指標和處理資訊。 DevOpsRDS 的 Guru 監視器，並為其中一些指標提供見解。如需詳細資訊，請參閱在 Amazon Aurora 叢集中監控指標或在 Amazon 關聯式資 Amazon Relational Database Service 執行個體中監控指標。

問題偵測

DevOpsGuru for RDS 使用數據庫和操作系統（OS）指標來檢測關鍵的數據庫性能問題，無論這些問題是即將發生還是持續發生。RDS 問題檢測的工作 DevOps原理有兩種主要方法：

- 使用臨界值
- 使用異常

偵測臨界值的問題

臨界值是評估監督測量結果時所依據的邊界值。您可以將臨界值視為量度圖表上的水平線，分隔正常行為與潛在有問題的行為。 DevOpsGuru for RDS 會透過分析指定資源可能有問題的層級來監控特定指標並建立閾值。 DevOps然後，當新的指標值在指定時間段內一致地跨過指定的閾值時， DevOpsGuru for RDS 會在 Guru 主控台中建立見解。這些見解包含防止 future 資料庫效能影響的建議。

例如， DevOpsGuru for RDS 可能會在 15 分鐘內使用磁碟監控暫存資料表的數目，並在每秒使用磁碟的暫存資料表速率異常高時建立深入解析。提高磁碟上臨時資料表使用量層級可能會影響資料庫效能。DevOpsGuru for RDS 可協助您採取糾正措施來預防問題，在這種情況變得關鍵之前公開這種情況。

偵測異常問題

雖然閾值提供了一種簡單而有效的方法來檢測數據庫問題，但在某些情況下它們是不夠的。考慮因為已知的處理程序 (例如每日報告工作)，因此量度值會尖峰並定期進入潛在有問題的行為的情況。由於預計會出現這種峰值，因此為每個人創建見解和通知將適得其反，並可能導致警報疲勞。

不過，仍然需要偵測非常不尋常的尖峰，因為指標遠高於其餘或持續時間更長，可能代表真正的資料庫效能問題。為了解決此問題， DevOpsGuru for RDS 會監控某些指標，以偵測指標的行為何時變得非常不尋常或異常。 DevOpsGuru 然後在洞察中報告這些異常情況。

例如， DevOpsGuru for RDS 可能會在資料庫負載不僅很高時建立洞察，而且也明顯偏離其通常的行為，這表示資料庫作業的重大意外速度降低。 DevOpsGuru for RDS 只辨識異常的資料庫負載尖峰，讓您專注於真正重要的問題。

資料庫負載

資料庫調整的關鍵概念是資料庫負載 (DB 載入) 量度。數據庫負載表示數據庫在任何給定時間的繁忙程度。數據庫負載的增加意味著數據庫活動的增加。

資料庫工作階段代表應用程式與關聯式資料庫的對話。使用中的工作階段是執行資料庫要求程序中的工作階段。工作階段處於作用中是指工作階段正在 CPU 上執行，或等待資源變成可用以繼續執行。例如，作用中的工作階段可能等待分頁讀入記憶體中，然後從分頁讀取資料時耗用 CPU。

Performance Insights 中的量DBLoad度是以平均作用中工作階段 (AAS) 來衡量。若要計算 AAS，Performance Insights 每秒會抽樣使用中工作階段的數目。針對特定期間，AAS 是作用中階段作業的總數除以抽樣總數。AAS 值為 2 表示平均而言，在任何給定時間，請求中有 2 個工作階段都處於作用中狀態。

倉庫中的活動可比喻為資料庫負載。假設倉庫僱用 100 名工人。如果有 1 份訂單進來，則 1 名工人履行訂單，其他工人閒置。如果有 100 個或更多的訂單進來，則所有 100 名員工同時履行訂單。如果您定期抽樣特定時段內有多少作用中的工人，則可以算出平均的作用中工人數目。計算結果指出平均隨時都有 N 名工人忙於履行訂單。如果昨天平均 50 名工人，今天平均 75 名工人，則表示倉庫中的活動程度上升。同樣地，資料庫負載會隨著工作階段活動增加而提高。

若要進一步了解，請參閱 Amazon Aurora 使用者指南中的資料庫負載或 Amazon RDS 使用者指南中的資料庫負載。

等待事件

wait 事件是一種資料庫檢測類型，會告訴您資料庫工作階段正在等待哪些資源，以便繼續進行。當 Performance Insights 計算作用中工作階段以計算資料庫負載時，它也會記錄造成作用中工作階段等待的等待事件。此技術可讓 Performance Insights 顯示哪些等待事件會導致資料庫負載。

每個使用中的工作階段都在 CPU 上執行或等待中。例如，工作階段會在搜尋記憶體、執行計算或執行程序程式碼時消耗 CPU。當工作階段不消耗 CPU 時，它們可能正在等待讀取資料檔案或將記錄寫入。工作階段等待資源越久，在 CPU 上執行的時間就越短。

當您調整資料庫時，您通常會嘗試尋找工作階段正在等待的資源。例如，兩個或三個等待事件可能佔資料庫負載的 90%。此量值表示作用中工作階段平均花最多時間等待少量資源。如果您能找出這些等待的原因，則可以嘗試解決問題。

以倉庫工人的比喻為例。進來的訂單是買一本書。工人可能延遲履行訂單。例如，不同的工作人員目前可能正在重新進貨架，或者可能無法使用手推車。或者，用來輸入訂單狀態的系統可能很慢。工人等待的時間越長，訂單履行所需的時間就越長。等待是倉儲工作流程的自然組成部分，但如果等待時間過長，生產力會降低。同樣地，重複或冗長的工作階段等待會降低資料庫效能。

如需有關 Amazon Aurora 中等待事件的詳細資訊，請參閱亞馬 Amazon Aurora Aurora 使用者指南中的使用等待事件進行調整 Aurora Postgre SQL 和使用等待事件進行調整。

如需有關其他 Amazon RDS 資料庫中等待事件的詳細資訊，請參閱 Amazon RDS 使用者指南中的 PostgreSQL 用等待事件進行調整。

RDS DevOps 大師的關鍵概念

DevOpsGuru 在偵測到操作應用程式中的異常或有問題的行為時，會產生洞察力。洞察包含一或多個資源的異常情況。異常表示 DevOps Guru 檢測到的一個或多個意外或不尋常的相關指標。

洞察的嚴重性為高、中或低。洞察嚴重性取決於建立洞察力的最嚴重異常情況。例如，如果洞察 AWS-ECS_ MemoryUtilization _and_ else 包含一個嚴重性低的異常，另一個具有高嚴重性的異常，則洞察的整體嚴重性很高。

如果 Amazon RDS 資料庫執行個體已開啟 Performance Insights，則 DevOps Guru for RDS 會針對這些執行個體的異常情況提供詳細的分析和建議。為了識別異常情況，RDS 的 DevOps Guru 開發了資料庫度量值的基準。 DevOps然後，Guru for RDS 會比較目前的測量結果值與歷史基準線。

主題

- 主動式洞察
- 反應式洞察
- 建議

主動式洞察

主動洞察可讓您在異常行為發生前了解該行為。它包含具有建議和相關指標的異常情況，可幫助您在問題變得更大的問題之前解決問題。

每個主動分析頁面都提供有關一個異常的詳細資料。

反應式洞察

反應式洞察會在發生異常行為時有效識別。它包含具有建議、相關指標和事件的異常情況，可協助您立即瞭解並解決問題。

因果異常

因果異常是反應式洞察中最高等級的異常。它會在 DevOps Guru 主控台的異常詳細資料頁面上顯示為主要量度。 數據庫負載（數據庫負載）是 RDS DevOps 大師的因果異常。例如，深入解析 AWS-ECS_ MemoryUtilization _and_其它可能有數個度量異常，其中一個是資源 AWS/RDS 的資料庫載入 (資料庫負載)。

透過深入分析，多個 Amazon RDS 資料庫執行個體可能會發生異常的資料庫負載 (資料庫負載)。每個資料庫執行個體的異常嚴重性可能會有所不同。例如，一個資料庫執行個體的嚴重性可能很高，而其他資料庫執行個體的嚴重性則較低。主控台預設為嚴重性最高的異常狀況。

情境異常

情境異常是資料庫負載內的研究結果，與反應式洞察相關。它會顯示在 DevOps Guru 主控台中異常詳細資料頁面的「相關量度」區段中。每個情境異常都描述了需要調查的特定 Amazon RDS 效能問題。例如，因果異常可以包括下列內容異常：

- 超出 CPU 容量 — CPU 執行佇列或 CPU 使用率高於正常狀態。
- 資料庫記憶體不足 — 處理序沒有足夠的記憶體。
- 資料庫連線激增 — 資料庫連線數目高於正常值。

建議

每個見解都至少有一個建議的動作。下列範例是由 DevOps大師針對 RDS 產生的建議：

- 調整 SQL ID *## _OF_ID* 以減少 CPU 使用率，或升級執行個體類型以增加 CPU 容量。
- 檢閱目前資料庫連線的相關尖峰。請考慮調整應用程式集區設定值，以避免頻繁動態配置新的資料庫連線。
- 尋找執行過多記憶體作業的 SQL 陳述式，例如記憶體內排序或大型聯結。
- 調查下列 SQL 識別碼的大量 I/O 使用量：*## _OF_* ID。
- 檢查是否有建立大量暫存資料的陳述式，例如執行大型排序或使用大型暫存資料表的陳述式。
- 檢查應用程式以瞭解造成資料庫工作負載增加的原因。
- 請考慮啟用 MySQL 效能結構描述。

- 檢查長時間運行的事務，並以提交或回滾結束它們。
- 設定 idle_in_transaction_session_timeout 參數，以結束任何處於「交易閒置」狀態超過指定時間的工作階段。

RDS 的 DevOps大師如何工作

DevOpsGuru for RDS 會收集指標資料、對其進行分析，然後在儀表板中發佈異常。

主題

- 數據收集和分析
- 異常出版

數據收集和分析

DevOpsRDS 專家會從 Amazon RDS Performance Insights 收集有關您的 Amazon RDS 資料庫的資料。此功能可監控 Amazon RDS 資料庫執行個體、收集指標，並讓您在圖表中探索指標。最重要的效能測量結果是DBLoad。 DevOpsGuru for RDS 消耗 Performance Insights 指標並對其進行分析以檢測異常。如需效能洞見的詳細資訊，請參閱 Amazon Aurora 使用者指南中的使用 Amazon Aurora 上的 Performance Insights 來監控資料庫負載，或在 Amazon RDS 使用者指南中使用 Amazon RDS 上的 Performance Insights 來監控資料庫負載。

DevOpsGuru for RDS 使用機器學習和進階統計分析來分析從 Performance Insights 收集的資料。如果 RDS 的 DevOps Guru 發現效能問題，它會繼續進行下一個步驟。

異常出版

資料庫效能問題 (例如高資料庫負載) 可能會降低資料庫的服務品質。當 DevOps Guru 偵測到 RDS 資料庫中的問題時，它會在儀表板中發佈深入解析。深入解析包含資源 AW S/RDS 的異常狀況。

如果您的執行個體開啟了 Performance Insights，則異常狀況會包含問題的詳細分析。 DevOpsRDS 版 Guru 也建議您執行調查或特定的更正動作。例如，建議可能是調查特定的高負載 SQL 陳述式、考慮增加 CPU 容量，或是關閉 idle-in-transaction 工作階段。

支援資料庫引擎

DevOpsRDS 大師支援下列資料庫引擎：

與 MySQL 相容性的 Amazon Aurora

若要進一步了解此引擎，請參閱 Amazon Aurora 使用者指南中的使用 Amazon Aurora MySQL。

與 PostgreSQL 相容的 Amazon Aurora

若要進一步了解此引擎，請參閱 Amazon Aurora 使用者指南中的使用 Amazon Aurora PostgreSQL。

Amazon RDS for PostgreSQL 性

若要進一步了解此引擎，請參閱 Amazon RDS 使用者指南Amazon RDS for PostgreSQL中的。

DevOpsGuru 報告異常並為其他數據庫引擎提供基本分析。 DevOpsRDS 專家僅針對 Amazon Aurora 和適用於 PostgreSQL 執行個體的 RDS 提供詳細的分析和建議。

為 RDS 啟用 DevOps大師

啟用 DevOps Guru for RDS 時，您可以讓 DevOps Guru 分析資料庫執行個體等資源中的異常。Amazon RDS 可讓您輕鬆探索並啟用 RDS 資料庫執行個體或資料庫叢集的建議功能。為了實現這一目標，RDS 會對其他服務（例如 Amazon EC2， DevOps大師和 IAM）進行 API 調用。RDS 主控台進行這些 API 呼叫時，請AWS CloudTrail記錄它們以取得可見性。

若要允許 DevOps大師發佈 Amazon RDS 資料庫的見解，請完成以下各節中的任務。

主題

- 為您的 Amazon RDS 資料庫執行個體啟用 Performance Insights
- 設定 RDS DevOps 專用的存取原則
- 將 Amazon RDS 資料庫執行個體新增至您的 DevOps大師範圍

為您的 Amazon RDS 資料庫執行個體啟用 Performance Insights

若要讓 DevOps Guru for RDS 分析資料庫執行個體上的異常，請確定已開啟 Performance Insights。如果未開啟資料庫執行個體的 Performance Insights，則 DevOps Guru for RDS 會在下列位置通知您：

儀表板

如果您依資源類型檢視見解，RDS 圖標會提醒您未開啟 Performance Insights。選擇連結以在 Amazon RDS 主控台中開啟 Performance Insights。

深入分析

在頁面底部的「建議」區段中，選擇「啟用 Amazon RDS Performance Insights」。

設定

在「服務：Amazon RDS」區段中，選擇連結以在 Amazon RDS 主控台中開啟 Performance Insights。

如需詳細資訊，請參閱 Amazon Aurora 使用者指南中的開啟和關閉 Performance Insights，或在 Amazon RDS 使用者指南中的開啟和關閉效能洞見。

設定 RDS DevOps 專用的存取原則

若要讓使用者存取 RDS 的 DevOps Guru，他們必須具有下列其中一個原則的權限：

- AWS 受管政策 `AmazonRDSFullAccess`
- 允許以下動作的客戶受管政策：
  - `pi:GetResourceMetrics`
  - `pi:DescribeDimensionKeys`
  - `pi:GetDimensionKeyDetails`

如需詳細資訊，請參閱 Amazon Aurora 使用者指南中的設定效能洞見的存取政策或 Amazon RDS 使用者指南中的設定 Performance Insights 的存取政策。

將 Amazon RDS 資料庫執行個體新增至您的 DevOps大師範圍

您可以在 DevOps大師主控台或 Amazon RDS 主控台中設定 DevOps大師來監控您的 Amazon RDS 資料庫。

在 DevOps Guru 控制台中，您有以下選項：

- 在帳戶層級開啟 DevOps Guru。此為預設值。當您選擇此選項時， DevOpsGuru 會分析AWS 區域和中所有支援的AWS資源AWS 帳戶，包括 Amazon RDS 資料庫。
- 指定 RDS DevOps 專家的AWS CloudFormation堆疊。

  如需詳細資訊，請參閱 使用AWS CloudFormation堆棧以識別您的資源 DevOpsGuru。
- 標記您的 Amazon RDS 資源。

  標籤是您指派給AWS資源的自訂屬性標籤。使用標籤來識別組成應用程式的AWS資源。然後，您可以按標籤篩選見解，以便僅檢視應用程式建立的見解。若只要檢視應用程式中 Amazon RDS 資源產生的見解，請新增一個值，例如 `Devops-guru-rds` Amazon RDS 資源標籤。如需詳細資訊，請參閱 使用標籤識別 DevOps Guru 應用程式中的資源。

> **Note**
>
> 標記 Amazon RDS 資源時，您必須標記資料庫執行個體，而不是叢集。

若要從 Amazon RDS 主控台啟用 DevOps大師監控，請參閱 RDS 主控台中的開啟 DevOps 大師。請注意，若要從 Amazon RDS 主控台啟用 DevOps大師，您必須使用標籤。如需標籤的詳細資訊，請參閱the section called “使用標籤識別應用程式中的資源”。

分析 Amazon RDS 中的異常

當 DevOps Guru for RDS 在儀表板中發佈效能異常時，您通常會執行下列步驟：

1. 在 DevOps Guru 儀表板中檢視深入分析資訊。 DevOpsRDS 大師報告被動和主動的見解。

   如需詳細資訊，請參閱 檢視見解。
2. 檢視 AWS/ RDS 資源的異常狀況。

   如需詳細資訊，請參閱 檢視反應異常 及 檢視主動異常。
3. 回應 DevOps大師的 RDS 建議。

   如需詳細資訊，請參閱 回應建議。
4. 監視資料庫執行個體的健康狀態，以確保已解決的效能問題不會再發生。

   如需詳細資訊，請參閱 Amazon Aurora 使用者指南中的監控 Amazon Aurora 資料庫叢集中的指標和 Amazon RDS 使用者指南中的 Amazon RDS 執行個體中的監控指標。

檢視見解

存取 DevOps Guru 主控台中的「見解」頁面，以尋找被動式和主動式見解。您可以從清單中選擇深入分析，以檢視指標、建議和深入解析的詳細資訊頁面。

若要檢視深入分析

1. 在 https://console.aws.amazon.com/devops-guru/ 打開 Amazon DevOps 大師控制台。
2. 開啟瀏覽窗格，然後選擇 [深入解析]。
3. 選擇「被動」索引標籤以檢視被動式見解，或選擇「主動」以檢視主動式見解。
4. 選擇深入解析的名稱，並依狀態和嚴重性排列優先順序。

詳細分析頁面隨即出現。

檢視反應異常

在深入分析中，您可以檢視 Amazon RDS 資源的異常情況。在反應式分析頁面的「彙總量度」區段中，您可以檢視具有對應時間表的異常清單。還有一些區段會顯示與異常相關的記錄群組和事件的相關資訊。反應洞察中的因果異常，每個都有一個對應的頁面，其中包含有關異常的詳細信息。

檢視 RDS 反應異常的詳細分析

在此階段，請向下鑽研異常情況，以取得適用於 Amazon RDS 資料庫執行個體的詳細分析和建議。

詳細分析僅適用於已開啟 Performance Insights 的 Amazon RDS 資料庫執行個體。

若要向下鑽研至異常詳細資訊頁面

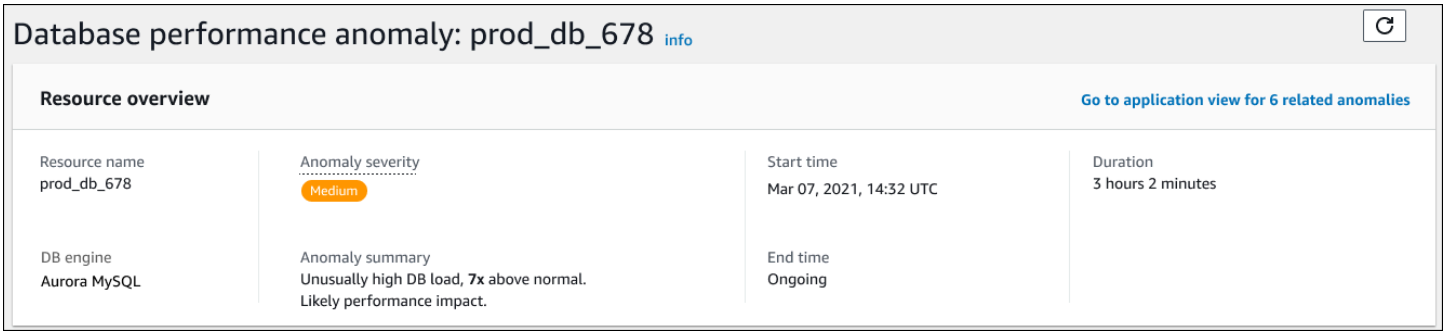
1. 在深入解析頁面上，尋找具有資源類型 AWS/ RDS 的彙總指標。
2. 請選擇 View Details (查看詳細資訊)。

   「異常詳細資訊」頁面隨即出現。標題以資料庫效能異常開頭，並顯示資源的名稱。無論何時發生異常，控制台都預設為嚴重性最高的異常。
3. (選擇性) 如果有多個資源受到影響，請從頁面頂端的清單中選擇不同的資源。

接下來，您可以找到詳細資訊頁面元件的說明。

資源概觀

詳細資訊頁面的頂端區段是資源概觀。本節概述 Amazon RDS 資料庫執行個體所經歷的效能異常情況。

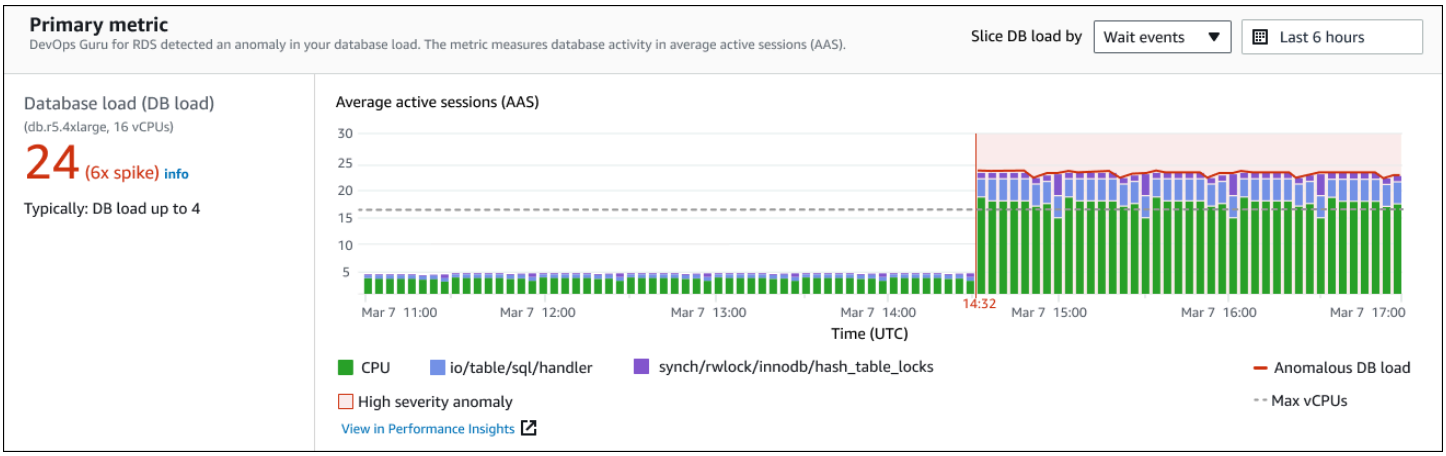


此區段包含下列欄位：

- 資源名稱 — 發生異常的資料庫執行個體名稱。在此範例中，資源的名稱為
- 資料庫引擎 — 發生異常的資料庫執行個體名稱。在這個例子中，引擎是 Aurora MySQL。
- 異常嚴重性 — 異常對執行個體造成負面影響的衡量方式。可能的嚴重性為「高」、「中」和「低」。
- 異常摘要 — 問題的簡短摘要。典型的摘要是非常高的 DB 負載。
- 開始時間和結束時間 — 異常開始和結束的時間。如果結束時間是持續的，則異常仍在發生。
- 持續時間 — 異常行為的持續時間。在此範例中，異常狀況正在進行，並且已經發生了 3 小時又 2 分鐘。

主要量度

「主要量度」區段會摘要顯示偶然異常，也就是深入解析中的最上層異常。您可以將因果異常視為資料庫執行個體所遇到的一般問題。



左側面板提供有關此問題的更多詳細資訊。在此範例中，摘要包括下列資訊：

- 資料庫負載 (DB 載入) — 將異常分類為資料庫載入問題。「Performance Insights」中的對應度量為DBLoad。此指標也會發佈至 Amazon CloudWatch。
- 資料庫執行個體類別 — 資料庫執行個體類別。此範例中的 vCPUs 數目為 16，對應於「平均作用中階段作業 (AAS)」圖表中的虛線。
- 24 (6 倍尖峰) — 資料庫負載，以洞察報告的時間間隔內的平均作用中工作階段 (AAS) 來測量。因此，在異常期間的任何指定時間，資料庫上平均有 24 個工作階段處於作用中狀態。資料庫負載是此執行個體一般資料庫負載的 6 倍。
- 通常：資料庫負載最多 4 — 在一般工作負載期間，資料庫負載的基準線 (以 AAS 測量)。值 4 表示在一般作業期間，資料庫在任何指定時間平均有 4 個或更少的作業階段作用中。

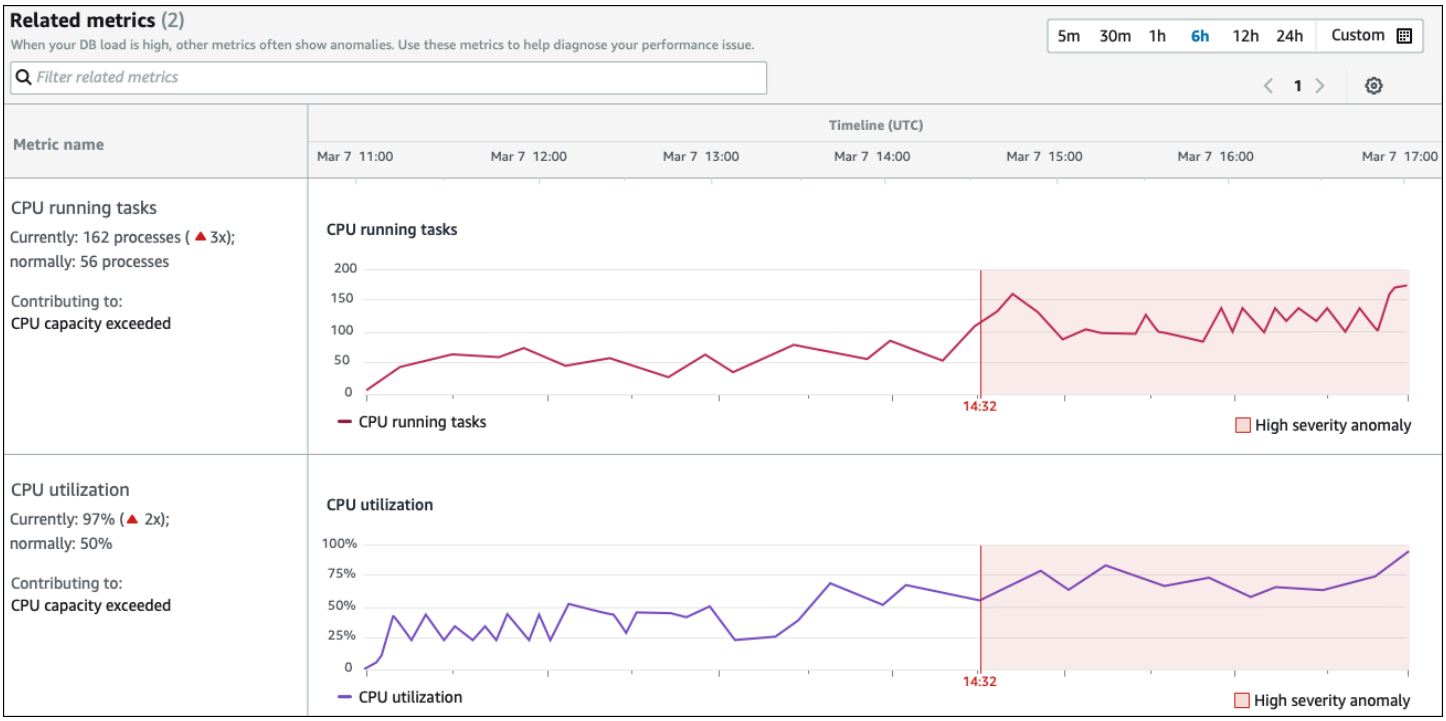
根據預設，負載圖表會由等待事件切割。這表示對於圖表中的每個長條，最大的彩色區域代表對總資料庫負載最大貢獻的等待事件。此圖表顯示問題開始的時間 (以紅色顯示)。將注意力集中在佔用欄中最多空間的等待事件上：

- CPU
- IO:wait/io/sql/table/handler

對於此 Aurora MySQL 資料庫，先前的等待事件顯示得超過正常情況。若要了解如何使用 Amazon Aurora 中的等待事件調整效能，請參閱亞馬 Amazon Aurora Aurora 使用者指南中的使用等待事件進行調整以及使用 Aurora Postgre SQL MySQL 的等待事件進行調整。若要了解如何使用 RDS 版 PostgreSQL 中的等待事件調整效能，請參閱 Amazon RDS 使用者指南中的使用等待事件進行調整。

相關指標

「相關量度」區段會列出上下文異常，這些異常是因果異常中的特定發現項目。這些發現項目提供有關效能問題的其他資訊。



「相關測量結果」表格有兩個資料欄：測量結果名稱和時間軸 (UTC)。表格中的每一列都對應一個特定的量度。

每一列的第一欄包含下列資訊：

- ## — 測量結果的名稱。第一列會將測量結果識別為 CPU 執行中的作業。

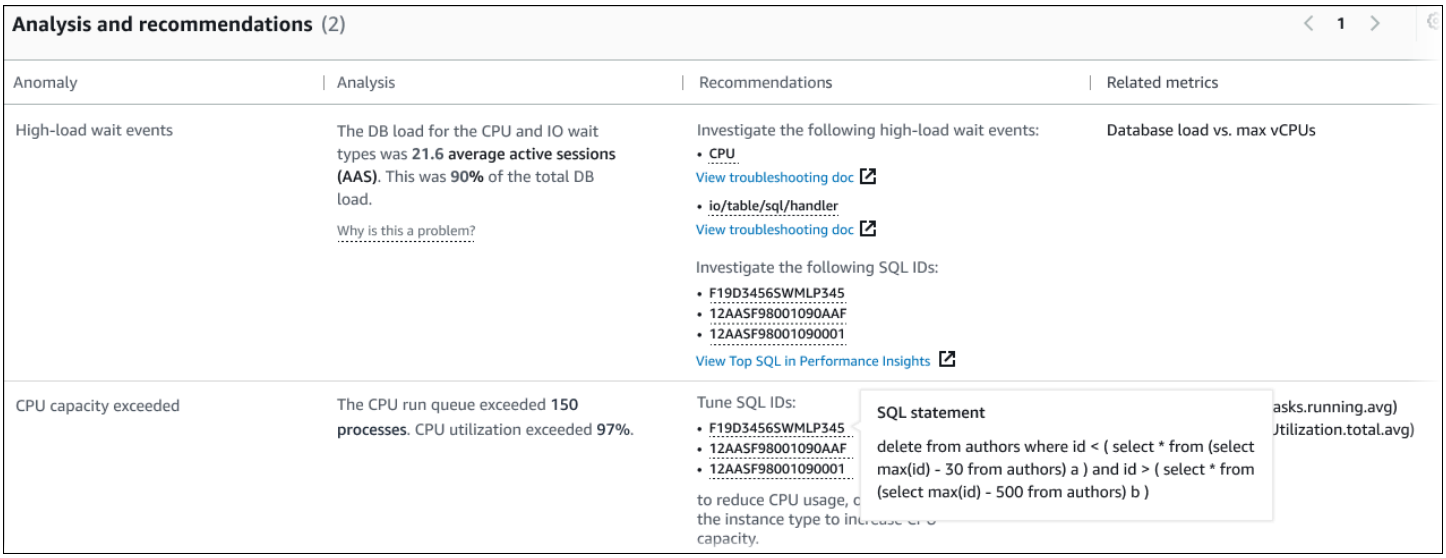
- 目前 — 測量結果的目前值。在第一行中，當前值為 162 進程（3x）。
- 一般 — 此資料庫正常運作時，此測量結果的基準線。 DevOpsRDS 的大師將基準計算為歷史記錄的第 95 個百分位數值。第一列表示 56 個處理序通常在 CPU 上執行。
- 貢獻給 — 與此測量結果相關聯的發現項目。在第一列中，CPU 執行中的工作量度與超過異常的 CPU 容量相關聯。

「時間軸」欄會顯示量度的折線圖。陰影區域會顯示當 DevOps Guru for RDS 將發現項目指定為高嚴重性時的時間間隔。

分析和建議

因果異常描述了整體問題，上下文異常描述了需要調查的特定發現。每個發現項目都會對應至一組相關量度。

在下列 [分析和建議] 區段的範例中，高資料庫負載異常有兩個發現項目。



資料表包含以下資料行：

- 異常 — 此上下文異常的一般描述。在此範例中，第一個異常是高負載等待事件，第二個是超過 CPU 容量。
- 分析 — 異常情況的詳細說明。

  在第一個異常情況中，三種等待類型有助於 90% 的 DB 負載。在第二個異常情況下，CPU 執行佇列超過 150，這表示在任何指定時間，超過 150 個工作階段正在等待 CPU 時間。CPU 使用率超過 97%，這意味著在問題發生期間，CPU 忙碌了 97% 的時間。因此，CPU 幾乎持續佔用，而平均 150 個工作階段等待在 CPU 上執行。

- 建議 — 建議的使用者對異常的回應。

  在第一個異常情況下，RDS 的 DevOps Guru 建議您調查等待事件cpu和io/table/sql/handler. 若要了解如何根據這些事件調整資料庫效能，請參閱 Amazon Aurora 使用者指南中的 CPU 和 io/表格/sql/處理程式。

  在第二個異常狀況中，RDS DevOps 專用的 Guru 建議您調整三個 SQL 敘述句，以減少 CPU 耗用量。您可以將鼠標懸停在鏈接上以查看 SQL 文本。
- 相關指標 — 為您提供異常特定測量值的指標。如需有關這些指標的詳細資訊，請參閱 Amazon Aurora 使用者指南中的 Amazon Aurora 指標參考或 Amazon RDS 使用者指南中的 Amazon RDS 指標參考。

  在第一個異常狀況中，RDS 的 DevOps Guru 建議將資料庫負載與執行個體的最大 CPU 進行比較。在第二個異常情況下，建議查看 CPU 執行佇列、CPU 使用率和 SQL 執行速率。

檢視主動異常

在深入解析中，您可以檢視 Amazon RDS 資源的異常情況。每個主動洞察都提供有關一個主動異常的詳細資訊。在主動式分析頁面上，您可以檢視洞察概觀、異常情況的詳細指標，以及預防 future 問題的建議。若要檢視主動異常情況，請前往主動洞察頁面。

洞察概述

「洞察概觀」區段提供有關為何建立見解的詳細資料。它會顯示洞察的嚴重性，以及異常情況的描述，以及異常發生的時間範圍。它還列出了 DevOps Guru 檢測到的受影響服務和應用程序的數量。

指標

「量度」區段提供異常的圖形。每個圖形都會顯示由資源的基準行為決定的臨界值，以及從異常發生時報告的指標資料。

彙總資源的建議

本節建議您在報告的問題成為更大問題之前可以採取的措施來緩解這些問題。您可以執行的動作會顯示在「建議的自訂變更」欄中。這些建議背後的基本原理在 DevOps Guru 為什麼推薦這一點？ 欄。如需如何回應建議的詳細資訊，請參閱the section called “回應建議”。

回應建議

建議是洞察力中最重要的部分。在分析的這個階段，您採取行動來解決效能問題。通常，您需要執行以下步驟：

1. 決定報告的效能問題是否表示真正的問題。

   在某些情況下，可能會出現問題並且是良性的。例如，如果您使測試資料庫受到極端的資料庫負載，則 DevOps Guru for RDS 會將負載報告為效能異常。但是，您不需要補救此異常，因為這是測試的預期結果。

   如果您判斷問題需要回應，請前往下一個步驟。

2. 決定是否實作建議。

   在建議表格中，會有一欄顯示建議的動作。對於反應式見解，這是反應性異常詳細資料頁面上的「我們建議什麼」欄。如需主動見解，這是主動式分析頁面上的「建議自訂變更」欄。

   DevOpsRDS 的 Guru 提供涵蓋數個潛在問題情況的建議清單。檢閱此清單之後，請判斷哪些建議與您目前的狀況更相關，並考慮套用它。如果建議符合您的情況，請前往下一個步驟。如果沒有，請跳過剩下的步驟，並使用手動技術解決問題。

3. 執行建議的動作。

   DevOpsRDS 專家建議您執行下列其中一項作業：

   - 執行特定的更正動作。

     例如，RDS 的 DevOps Guru 可能會建議您升級 CPU 容量、調整應用程式集區設定或啟用效能結構描述。

   - 調查問題的原因。

     一般而言，RDS 專用的 DevOps Guru 建議您調查特定的 SQL 陳述式或等待事件。例如，建議可能是調查等待事件`io/table/sql/handler`。在 Amazon Aurora 使用者指南中的使用等待事件進行微調 Aurora Postgre SQL 或使用等待事件進行調整中列出的等待事件，或在 Amazon Aurora RDS 使用者指南中的使用等待事件進行調整中查 PostgreSQL 列出的等待事件。然後執行建議的動作。

     > **Important**
     >
     > 建議您先在測試執行個體上測試任何變更，然後再修改生產執行個體。如此就可以了解變更的影響。

使用 Guru 監視非關聯式資料 DevOps庫

DevOpsGuru 能夠為您的非關聯式或 NoSQL 資料庫產生見解，協助您根據最佳做法保持資源設定。例如， DevOpsGuru 可以根據現有流量預測 future 需求，幫助您保持容量規劃的最佳狀態。DevOpsGuru 可以識別您使用的資源是否比您設定的少，並根據您的歷史使用情況提供改善應用程式可用性的建議。這可以幫助您減少不必要的成本。

除了容量規劃之外， DevOpsGuru 還可以偵測並協助您疑難排解操作問題，例如節流、交易衝突、條件式檢查失敗以及 SDK 參數的改進區域。資料庫通常與多個服務和資源相連， DevOpsGuru 可以使用基於標記或 AWS CloudFormation 彙總的群組來關聯您的應用程式結構以進行分析。異常可能涉及多個資源，這些資源都受到相同解決方案的影響。 DevOpsGuru 能夠跨不同的資源指標，配置，日誌和事件進行關聯。例如， DevOpsGuru 可以分析並關聯 Lambda 函數的資料，這些函數可能正在從資料 Amazon DynamoDB 表讀取或寫入資料。透過這種方式， DevOpsGuru 監控多個相關資源，以偵測異常情況，並為您的資料庫解決方案提供有用的見解。

監視資料庫作業 Amazon DynamoDB

下表顯示 DevOps Guru 監控的範例案例和見解 Amazon DynamoDB。

Amazon DynamoDB 使用案例	範例	指標
偵測由於大量讀取 AccountProvisionedReadCapacityUtilization 和 AccountProvisioned WriteCapacityUtilization寫入要求而導致的大量使用和正在使用。	Amazon DynamoDB 讀取或寫入要求的資料表消耗容量已達到資料表層級限制。	AccountProvisioned ReadCapacityUtilization, AccountProvisionedWriteCapacityUtilization
偵測由提供的條件運算式不符合資料庫預期的 Amazon DynamoDB 要求所造成的條件檢查失敗。	條件式檢查失敗是由資料表中的錯誤資料、嚴格條件運算式或競爭條件所造成。	ConditionalCheckFailedRequests

監視資料庫作業 Amazon ElastiCache

下表顯示 DevOps Guru 監控的範例案例和見解 Amazon ElastiCache。

DevOps大師識別的場景	CloudWatch 監控的指標
偵測 Amazon ElastiCache 叢集是否因叢集需求不斷變化而達到 Redis 或 Memcached 的運算限制。	CPU 利用率, EngineCPUUtilization, 驅逐

整合 CodeGuru Profiler

本章節將概要概要說明 Amazon DevOps Guru 如何與 Amazon CodeGuru Proventer。您可以從 CodeGuru 將 Profiler 作為 DevOps Guru 控台中的洞察。

Amazon DevOps Guru 與亞馬遜集成 CodeGuru 配置文件的 EventBridge 受管規則。 CodeGuru ProventBridge 會將事件傳送到 EventBridge。託管規則路由隨默認事件總線發送的事件。來自的每個入站事件 CodeGuru 分析器是一個主動的異常報告。如需詳細資訊，請參閱「」使用 EventBridge CodeGuru Profiler。

DevOps 專家通過 EventBridge 支持入站事件。事件表示 DevOps Guru 確定的建議中有變更的事件。CodeGuru Profiler 每 24 小時發送一次檢測信號事件，以顯示事件的連續性。活動攜帶 CodeGuru Profiler 推薦信息以及您計算資源的元數據。有關事件生命週期的信息，請參閱亞馬遜 EventBridge 活動。

當您設置 DevOps 專家時，DevOps 專家將創建 EventBridge 從另一個服務路由事件的帳戶中的託管規則。此規則將路由到 DevOps Guru。當存在入站事件時，會發送通知。

事件總線接收來自 DevOps Guru 等源的事件，並將其路由到與該事件總線關聯的規則。如需事件總線的詳細資訊，請參事件匯流排。

如需某些參數的詳細資訊，請參Amazon EventBridge 事件。

要接收 CodeGuru 分析器見解 DevOps 專家，您必須具備以下內容。

- 必須啟用 CodeGuru Profiler。有關啟用 CodeGuru 分析器，請參閱設定 CodeGuru Profiler。
- 必須啟用 DevOps 大師。有關啟用 DevOps 專家的信息，請參閱啟用 DevOps Guru。
- 相同的資源必須在同一個地區監控 CodeGuru 分析器和 DevOps 專家。

使用定義應用程式AWS資源

亞馬遜 DevOpsGuru 將涵蓋範圍邊界中的資源分組，以指定分析哪些資源以獲得營運見解。資源按資源分組AWS CloudFormation堆棧或帶有標籤的資源。您可以在設定時選擇堆疊或標籤 DevOpsGuru。您也可以稍後更新堆疊或標記。建議您將資源群組視為應用程式。例如，您在一個堆疊中可能定義了一個監視應用程式所使用的所有資源。或者，您可以將相同的標籤添加到您在數據庫應用程序中使用的所有資源。定義哪些資源的邊界DevOpsGuru 分析。集合中的所有資源都在此邊界內。您帳戶中不在資源集合中的任何資源都不在界限之外，不會進行分析。如需所支援服務和資源的詳細資訊，請參閱亞馬遜 DevOpsGuru 定價。

您可以定義涵蓋範圍界限，其中包含應用程式中的資源有三種方式。

- 指定所有支援AWS您的資源AWS帳戶和區域。這使您的帳戶和區域成為您的資源邊界。有了這個選項， DevOpsGuru 會分析您帳戶和區域中所有受支援的資源。在一個堆棧中的所有資源都被分組到一個應用程序中。任何不在堆疊中的資源都會分組到它們自己的應用程式中。
- 使用AWS CloudFormation堆疊以指定應用程式中的資源。堆棧包含使用生成的資源AWS CloudFormation。在 中 DevOps大師，您在帳戶中選擇堆棧。您選擇的每個堆疊中的資源會分組到一個應用程式中。堆棧中的所有資源均由以下方式進行分析 DevOps大師的見解。
- 使用AWS標記，指定您應用程式中的資源。同時AWS標籤包含鍵和一個值。在 中 DevOps大師，選擇一個標籤鍵並選擇性地選擇一個或多個值與那個配對鍵。您可以使用值將您的資源分組到應用程式中。

如需詳細資訊，請參閱更新您的AWS分析涵蓋範圍 DevOps老師。

主題

- 使用標籤識別 DevOps Guru 應用程式中的資源
- 使用AWS CloudFormation堆棧以識別您的資源 DevOpsGuru

使用標籤識別 DevOps Guru 應用程式中的資源

您可以使用標籤來識別 Amazon DevOps Guru 分析的AWS資源，並指定要分組哪些資源，以便使用選取的標籤金鑰和標籤值進行監控。您可以在設定 DevOps Guru 或從 [分析的資源] 頁面中選擇 [編輯分析的資源] 時編輯這些組態。選取「標籤」之後，您可以選擇以「devops-Guru」開頭的特定標籤金鑰。若要分析帳號中的所有資源，並使用標籤值將資源分組，請選取所有帳號資源。若要使用標籤值來指定 DevOps Guru 要分析的資源，請選取選擇特定的標籤值。

> **Note**
>
> 選取「所有帳號資源」且不存在任何標籤值時，不含標籤索引鍵的資源會分組並分別進行分析。

您可以使用標籤的金鑰來識別資源，然後使用具有該金鑰的值，將資源分組到應用程式中。例如，您可以使用金鑰標記資源devops-guru-applications，然後針對每個應用程式使用不同值的金鑰。您可以使用標籤鍵-值配對 devops-guru-applications/databasedevops-guru-applications/cicd，devops-guru-applications/monitoring以及識別帳戶中的三個應用程式。每個應用程序都由包含相同標籤鍵值對的相關資源組成。您可以使用標籤所屬的AWS服務將標籤新增至資源。如需詳細資訊，請參閱 新增AWS標籤至AWS資源。

將標籤新增至應用程式中的資源後，您可以透過產生這些資源的標籤來篩選見解。如需如何使用標籤篩選見解的詳細資訊，請參閱檢視DevOps大師洞察。

如需有關支援服務和資源的詳細資訊，請參閱 Amazon DevOps Guru 定價。

主題

- 什麼是AWS標籤？
- 使用標籤定義 DevOps Guru 應用程序
- 與 DevOps大師一起使用標籤
- 新增AWS標籤至AWS資源

什麼是AWS標籤？

標籤可協助您識別和整理 AWS 資源。許多 AWS 服務支援標記，因此您可以對來自不同服務的資源指派相同的標籤，指示資源是相關的。例如，您可以將指派給 AWS Lambda 函數的相同標籤指派給 Amazon DynamoDB 資料表資源。如需使用標籤的詳細資訊，請參閱標記最佳實務白皮書。

每個 AWS 標籤都有兩個部分。

- 標籤鍵 (例如，CostCenter、Environment、Project 或 Secret)。標籤鍵區分大小寫。
- 一個名為標籤值 (例如，111122223333、Production 或團隊名稱) 的選用欄位。忽略標籤值基本上等同於使用空字串。與標籤鍵相同，標籤值會區分大小寫。

這些合稱為鍵值對。

使用標籤定義 DevOps Guru 應用程序

若要使用標籤定義 Amazon DevOps Guru 應用程式，請將該標籤新增至組成應用程式的帳戶AWS資源。您的標籤包含一個鍵和一個值。我們建議您為 DevOps Guru 分析的每個具有相同金鑰的AWS資源新增標籤。在標籤中使用不同的值，將資源分組到您的應用程式中。例如，您可devops-guru-analysis-boundary以將帶有索引鍵的標籤指派給涵蓋範圍邊界中的所有AWS資源。使用不同的值搭配該金鑰來識別您帳戶中的應用程式。您可以monitoring針對三個應用程式使用database、和值containers。如需詳細資訊，請參閱 更新您的AWS分析涵蓋範圍 DevOps老師。

如果您使用AWS標籤來指定要分析的資源，則只能使用一個鍵的標籤。您可以將標籤的密鑰與任何值配對。使用此值將包含金鑰的資源分組到作業應用程式中。

> **Important**
>
> 用於定義資源涵蓋範圍的標籤中鍵的字串必須以字首 Devops-guru- 開頭。標籤鍵可以是 DevOps-Guru-deployment-application 或 devops-guru-rds-application。建立鍵時，您可任意選擇鍵中字元的大小寫。建立鍵後，區分大小寫。例如， DevOpsGuru 使用一個名為的密鑰devops-guru-rds和一個名為的密鑰DevOps-Guru-RDS，這些鍵充當兩個不同的密鑰。應用程式中可能的鍵/值對可以是 Devops-Guru-production-application/RDS 或 Devops-Guru-production-application/containers。

與 DevOps大師一起使用標籤

指定標AWS籤以識別您希望 Amazon DevOps Guru 分析的AWS資源，或指定標籤值以識別要分組的資源。這些資源是您的資源涵蓋範圍邊界。您可以選擇一個鍵和零個或多個值。

若要選擇您的標籤

1. 在以下位置打開 Amazon DevOps 大師控制台 https://console.aws.amazon.com/devops-guru/。
2. 開啟導覽窗格，然後展開 [設定]。
3. 在已分析的資源中，選擇編輯。
4. 如果您希望 DevOps Guru 分析包含您選擇之標籤的所有資源，請選擇「標籤」。選擇按鍵，然後選擇下列其中一個選項。
   - 所有帳號資源 — 分析目前區域和帳號中的所有AWS資源。具有所選標籤鍵的資源會依標籤值分組 (如果有的話)。沒有此標籤鍵的資源會分別分組和分析。

- 選擇特定標籤值 — 分析所有包含含有您選擇鍵之標籤的資源。 DevOpsGuru 根據標籤的值將您的資源分組到應用程序中。

  標籤的密鑰必須以前綴開頭devops-guru-。此前綴不區分大小寫。例如，有效的金鑰為DevOps-Guru-Production-Applications。

5. 選擇儲存。

新增AWS標籤至AWS資源

當您指定標AWS籤以識別您希望 DevOps Guru 分析的AWS資源時，請選擇與其相關聯的資源的標籤。您可以使用每個資源所屬的AWS服務或使用AWS標籤編輯器，將標籤新增至資源。

- 若要使用資源的服務管理標籤，請使用資源所屬服務的主控台或 SDK。AWS Command Line Interface例如，您可以標記 Amazon Kinesis 串流資源或 Amazon CloudFront 分發資源。這些是具有可標記資源的兩個服務範例。DevOpsGuru 可以分析支持標籤的大多數資源。如需詳細資訊，請參閱 Amazon Kinesis 開發人員指南中的標記串流和 Amazon 開發人 CloudFront 員指南中的標記分佈。若要瞭解如何將標籤新增至其他類型的資源，請參閱其所屬AWS服務的使用者指南或開發人員指南。

  > **Note**
  >
  > 標記 Amazon RDS 資源時，您必須標記資料庫執行個體，而不是叢集。

- 您可以使用AWS標籤編輯器，依地區中的資源和特定AWS服務中的資源來管理標籤。如需詳細資訊，請參閱《AWS資源群組和標籤使用指南》中的標籤編輯器。

當您將標籤新增至資源時，您只能新增金鑰，也可以加入索引鍵和值。例如，您可以使 DevOps 用屬於應用程式一部分devops-guru-的所有資源建立索引鍵的標籤。您也可以新增包含金鑰devops-guru-和值的標籤RDS，然後將該金鑰-值配對僅新增至應用程式中的 Amazon RDS 資源。如果您想要在主控台中檢視僅從應用程式中的 Amazon RDS 資源產生的見解，此功能非常有用。

使用AWS CloudFormation堆棧以識別您的資源 DevOpsGuru

您可以使用AWS CloudFormation堆疊以指定哪些AWS您想要的資源 DevOps大師來分析。堆疊是以下方案的集合AWS作為單一單元進行管理的資源。您選擇的堆棧中的資源組成了您的 DevOpsGuru。針對您選擇的每個堆疊，會分析其支援資源中的作業資料，找出異常行為。然後將這些問題分為相關的異

常情況，以創建見解。每個洞察都包含一個或多個建議，以幫助您解決這些問題。您可以指定的堆疊數目上限為 1000。如需詳細資訊，請參閱《》使用堆疊在AWS CloudFormation使用者指南和更新您的AWS分析涵蓋範圍 DevOps老師。

選擇堆疊後， DevOps大師立即開始分析您添加到它的任何資源。如果您從堆疊中移除資源，則不會再對其進行分析。

如果您選擇擁有 DevOpsGuru 分析您帳戶中所有支持的資源（這意味著您的AWS帳戶和區域是您的DevOps大師覆蓋邊界），然後 DevOpsGuru 會針對您帳戶中所有受支援的資源 (包括堆疊中的資源) 分析並建立見解。從不在堆疊中的資源中的異常建立的洞察會分組在帳戶層級。如果洞察是從堆疊中的資源中的異常建立的，則會將其分組在堆疊層級。如需詳細資訊，請參閱 了解異常行為如何歸類為見解。

選擇堆疊 DevOpsGuru

指定您希望 Amazon 的資源 DevOps大師通過選擇分析AWS CloudFormation創建它們的堆棧。您可以使用AWS Management Console或軟體開發套件。

主題

- 選擇堆疊 DevOps大師分析（控制台）
- 選擇堆疊 DevOps大師分析（DevOpsGuru)

選擇堆疊 DevOps大師分析（控制台）

您可以添加AWS CloudFormation堆疊使用主控台。

若要選擇包含要分析之資源的堆疊

1. Open Open Open Open DevOpsGuruhttps://console.aws.amazon.com/devops-guru/。
2. 開啟導覽窗格，然後選擇設定。
3. 在 中DevOpsGuru，選擇Manage (管理)。
4. 選擇CloudFormation 堆疊如果你想 DevOpsGuru 分析您所選堆疊中的資源，然後選擇以下其中一個選項。

   - 所有資源— 分析了帳戶中堆棧中的所有資源。每個堆疊中的資源會分組到它們自己的應用程式中。不會分析您帳戶中未在堆疊中的任何資源。

- 選取堆疊— 選擇您想要設定的堆疊 DevOps大師來分析。您選取的每個堆疊中的資源會分組到它們自己的應用程式中。您可以在以下位置輸入堆疊名稱尋找堆疊以快速找到特定的堆疊。您可以選擇最多 1,000 個堆疊。

5. 選擇 Save (儲存)。

選擇堆疊 DevOps大師分析（DevOpsGuru)

若要指定AWS CloudFormation使用亞馬遜堆棧 DevOps大師 SDK，使用`UpdateResourceCollection`方法。如需詳細資訊，請參閱《》UpdateResourceCollection在亞馬遜 DevOpsGuru Guru。

與 Amazon 合作 EventBridge

Amazon DevOps Guru 與 Amazon EventBridge 整合，可通知您有關見解和對應洞察更新的特定事件。來自 AWS 服務的事件會以近乎即時 EventBridge 的方式傳送到。您可編寫簡單的規則，來指示您在意的事件，以及當事件符合規則時所要自動執行的動作。可自動啟動的動作包括下列範例：

- 調用函數 AWS Lambda
- 調用 Amazon 彈性計算雲運行命令
- 將事件轉傳至 Amazon Kinesis Data Streams
- 激活 Step Functions 狀態機
- 通知 Amazon SNS 或 Amazon SQS

您可以選取下列任何預先定義的模式來篩選事件，或建立自訂模式規則以在支援的 AWS 資源中啟動動作。

- DevOps 大師新洞察開放
- DevOps 大師新異常協會
- DevOps 大師洞察嚴重性升級
- DevOps 創建大師新推薦
- DevOps 大師洞察關閉

DevOps大師的活動

以下是 DevOps Guru 的範例事件。盡可能發出事件。要了解有關事件模式的更多信息，請參閱開始使用 Amazon EventBridge 或 Amazon EventBridge 事件模式。

DevOpsGuru新洞察開放活動

當 DevOps 大師打開一個新的洞察力，它發送以下事件。

```
{
    "version" : "0",
    "id" : "08108845-ef90-00b8-1ad6-2ee5570ac6c4",
    "detail-type" : "DevOps Guru New Insight Open",
    "source" : "aws.devops-guru",
    "account" : "123456789012",
```

```
    "time" : "2021-11-01T17:06:10Z",
    "region" : "us-east-1",
    "resources" : [ ],
    "detail" : {
      "insightSeverity" : "high",
      "insightDescription" : "ApiGateway 5XXError Anomalous In Stack TestStack",
      "insightType" : "REACTIVE",
      "anomalies" : [
        {
          "startTime" : "1635786000000",
          "id" : "AL41JDFFQPYlZlXD8cpREkAAAAF83HGGgC9TmTr9lbfJ7sCiISlWMeFCbHY_XXXX",
          "sourceDetails" : [
            {
              "dataSource" : "CW_METRICS",
              "dataIdentifiers" : {
                "period" : "60",
                "stat" : "Average",
                "unit" : "None",
                "name" : "5XXError",
                "namespace" : "AWS/ApiGateway",
                "dimensions" : [
                  {
                    "name" : "ApiName",
                    "value" : "Test API Service"
                  },
                  {
                    "name" : "Stage",
                    "value" : "prod"
                  }
                ]
              }
            }
          ]
        }
      ],
      "accountId" : "123456789012",
      "messageType" : "NEW_INSIGHT",
      "insightUrl" : "https://us-east-1.console.aws.amazon.com/devops-guru/#/insight/
reactive/AIYH6JxdbgkcG0xJmypiL4MAAAAAAAAAL0SLEjkxiNProXWcsTJbLU07EZ7XXXX",
      "startTime" : "1635786120000",
      "insightId" : "AIYH6JxdbgkcG0xJmypiL4MAAAAAAAAAL0SLEjkxiNProXWcsTJbLU07EZ7XXXX",
      "region" : "us-east-1"
    }
```

```
  },
```

高嚴重性的自訂範例事件模式新洞察

規則使用事件模式以選擇事件並將事件路由到目標。以下是 DevOps Guru 事件模式的範例。

```
{
  "source": [
    "aws.devops-guru"
  ],
  "detail-type": [
    "DevOps Guru New Insight Open"
  ],
  "detail": {
    "insightSeverity": [
         "high"
         ]
  }
}
```

更新中 DevOps大師設置

您可以更新以下亞馬遜 DevOps大師設置：

- 您的 DevOps大師覆蓋範圍。這會決定要分析您帳戶中的哪些資源。
- 您的通知。這決定了使用哪些 Amazon 簡單通知服務主題來通知您重要事項 DevOps大師事件。
- 增強見解的功能。這包括日誌異常偵測、加密和您的AWS Systems Manager整合設定。這決定了是否 DevOpsGuru 顯示日誌數據，您是否使用額外的安全密鑰，以及是否 OpsItem 在系統管理器中創建 OpsCenter 對於每一個新的見解。

主題

更新您的管理帳戶設定

您可以配置 DevOps大師為您的組織中的帳戶。如果您尚未註冊委派的系統管理員，您可以選擇註冊委派管理員。如需註冊委派管理員的詳細資訊，請參閱啟用DevOps老師。

更新您的AWS分析涵蓋範圍 DevOps老師

您可以更新哪個AWS您帳戶中的資源 DevOps大師分析。若要執行此操作，請瀏覽至分析資源在控制台中頁面，然後選擇編輯。如需詳細資訊，請參閱檢視分析的資源。

更新您的通知 DevOps老師

設置亞馬遜簡單通知服務主題，用於通知您有關重要亞馬遜的信息 DevOps大師事件。您可以從已存在於您的主題名稱清單中進行選擇AWS帳戶中，輸入新主題的名稱 DevOps大師在您的帳戶中創建，或

輸入任何現有主題的亞馬遜資源名稱（ARN）AWS您所在地區的帳戶。如果您指定的 ARN 不在您的帳戶中的主題，您必須授予權限DevOps大師可以通過向其添加 IAM 策略來訪問該主題。如需詳細資訊，請參閱Amazon SNS 主題的許可。您最多可以指定兩個主題。

DevOpsGuru 會傳送下列更新的通知：

- 創建了一個新的見解。
- 一個新的異常被添加到洞察。
- 深入解析的嚴重性已從Low或者Medium至High。
- 深入解析的狀態會從持續變更為已解決。
- 對於洞察力的建議被確定。

DevOps如果選擇了 Guru 還會發送通知AWS CloudFormation當您嘗試將資源添加到您的堆棧或標籤密鑰無效 DevOps大師帳戶。

您可以選擇接收有關問題的各種更新的 Amazon SNS 通知，或只有在問題已開啟、關閉或嚴重性變更時才接收 Amazon SNS 通知。根據預設，您會收到所有更新的通知。

若要更新通知，請先瀏覽至通知頁面，然後選擇是否要新增、移除或更新 Amazon SNS 通知主題的組態。

主題

- 導覽至「」中的「通知設定」 DevOps大師控制台
- 將亞馬遜 SNS 通知主題添加到 DevOps大師控制台
- 移除中的亞馬遜 SNS 通知主題 DevOps大師控制台
- 更新亞馬遜 SNS 通知組態
- 新增至您的亞馬遜 SNS 主題的許可

導覽至「」中的「通知設定」 DevOps大師控制台

若要更新通知，您必須先瀏覽至通知設定區段。

瀏覽至通知設定區段

1. 打開亞馬遜 DevOps大師控制台https://console.aws.amazon.com/devops-guru/。
2. 在導覽窗格中選擇 Settings (設定)。

「設定」頁面包括通知一節，其中包含已設定 Amazon SNS 主題的相關資訊。

將亞馬遜 SNS 通知主題添加到 DevOps大師控制台

若要新增亞馬遜 SNS 通知主題 DevOps大師控制台

1. the section called “導覽至「」中的「通知設定」 DevOps大師控制台”.
2. 選擇 Add notification (新增通知)。
3. 若要新增 Amazon SNS 主題，請執行下列其中一個動作。
   - 選擇使用電子郵件產生新的 SNS 主題。然後，從指定電子郵件地址」下方，輸入您要接收通知的電子郵件地址。若要輸入其他電子郵件地址，請選擇新增電子郵件。
   - 選擇使用現有的 SNS 主題。然後，從選擇您的主題AWS帳戶」下方，選擇您要使用的主題。
   - 選擇使用現有 SNS 主題 ARN 從其他帳戶指定現有主題。然後，在輸入主題的 ARN」中，輸入主題 ARN。ARN 是該主題的亞馬遜資源名稱。您可以在不同的帳戶中指定主題。如果您在其他帳號中使用某個主題，則必須將資源策略新增至該主題。如需詳細資訊，請參閱Amazon SNS 主題的許可。
4. 選擇 Save (儲存)。

移除中的亞馬遜 SNS 通知主題 DevOps大師控制台

若要移除中的亞馬遜 SNS 主題 DevOps大師控制台

1. the section called “導覽至「」中的「通知設定」 DevOps大師控制台”.
2. 選擇選擇現有主題。
3. 從下拉式功能表中，選取您要移除的主題。
4. 選擇 Remove (移除)。
5. 選擇 儲存 。

更新亞馬遜 SNS 通知組態

亞馬遜 SNS 通知主題有兩種類型的通知組態 DevOps大師。您可以選擇接收所有嚴重性等級的通知，也可以選擇僅接收通知高和中等嚴重性等級。您也可以選擇接收各種更新或僅接收某些類型更新的通知。

當您選擇接收有關該問題的各種更新的 Amazon SNS 通知時， DevOpsGuru 會傳送下列更新的通知：

- 創建了一個新的見解。
- 一個新的異常被添加到洞察。
- 深入解析的嚴重性已從Low或者Medium至High。
- 深入解析的狀態會從持續變更為已解決。
- 對於洞察力的建議被確定。

默認情況下，您只會收到高和中等嚴重性等級通知，您會收到各種更新的通知。

更新亞馬遜 SNS 通知主題的通知組態

1. the section called “導覽至「」中的「通知設定」 DevOps大師控制台”.
2. 選擇選擇現有主題。
3. 從下拉式功能表中，選取您要進行更新的主題。
4. 選擇所有嚴重性等級接收具有「高」、「中」和「低」嚴重性等級的通知，或選擇只有高和中接收具有「高」和「中」嚴重性等級的通知。
5. 選擇通知我有關洞察力的所有更新，或選擇洞察力已開啟或關閉，或嚴重性層級從「低」或「中」變更為「高」時通知我。
6. 選擇 儲存 。

新增至您的亞馬遜 SNS 主題的許可

亞馬遜 SNS 主題是包含AWS Identity and Access Management(IAM) 資源政策。當您在此指定主題時， DevOpsGuru 會將下列權限附加至其資源策略。

```
{
    "Sid": "DevOpsGuru-added-SNS-topic-permissions",
    "Effect": "Allow",
    "Principal": {
        "Service": "region-id.devops-guru.amazonaws.com"
    },
    "Action": "sns:Publish",
    "Resource": "arn:aws:sns:region-id:topic-owner-account-id:my-topic-name",
    "Condition" : {
      "StringEquals" : {
```

```
        "AWS:SourceArn": "arn:aws:devops-guru:region-id:topic-owner-account-
id:channel/devops-guru-channel-id",
        "AWS:SourceAccount": "topic-owner-account-id"
    }
  }
}
```

這些權限是必需的 DevOps大師使用主題發布通知。如果您不想擁有該主題的這些權限，則可以安全地將其移除，並且該主題將繼續像您選擇之前的那樣運作。但是，如果刪除了這些附加的權限，DevOpsGuru 無法使用主題來產生通知。

過濾您的 DevOps大師通知

您可以過濾 DevOps通過大師通知the section called “更新亞馬遜 SNS 通知組態”或透過使用亞馬遜 SNS 訂閱篩選政策。

主題

- 使用 Amazon SNS 訂閱篩選政策篩選通知
- 亞馬遜過濾亞馬遜 SNS 通知示例 DevOps老師

使用 Amazon SNS 訂閱篩選政策篩選通知

您可以建立亞馬遜簡單通知服務 (Amazon SNS) 訂閱篩選政策，以減少從亞馬遜收到的通知數量 DevOps大師。

使用篩選策略來指定您接收的通知類型。您可以使用下列關鍵字篩選 Amazon SNS 訊息。

- NEW_INSIGHT— 在創建新的見解時收到通知。
- CLOSED_INSIGHT— 當現有的見解已關閉時收到通知。
- NEW_RECOMMENDATION— 從洞察力建立新建議時收到通知。
- NEW_ASSOCIATION— 從洞察中檢測到新異常時收到通知。
- CLOSED_ASSOCIATION— 當現有異常關閉時收到通知。
- SEVERITY_UPGRADED— 在洞察的嚴重性升級時收到通知

如需如何建立 Amazon SNS 訂閱篩選器政策的相關資訊，請參閱亞馬遜 SNS 訂閱篩選政策在Amazon 簡易通知服務開發人員指南。在您的篩選政策中，您可以使用政策指定其中一個關鍵

字MessageType。例如，篩選器中會出現以下內容，該篩選器指定 Amazon SNS 主題僅在從洞察中偵測到新異常時才會傳送通知。

```
{
  "MessageType":["NEW_ ASSOCIATION"]
}
```

亞馬遜過濾亞馬遜 SNS 通知示例 DevOps老師

以下是來自 Amazon SNS 主題的 Amazon 簡單通知服務 (Amazon SNS) 通知範例，其中包含篩選政策。其MessageType設定為NEW_ASSOCIATION，因此只有在從洞察中偵測到新異常時，才會傳送通知。

```
{
      "accountId": "123456789012",
      "region": "us-east-1",
      "messageType": "NEW_ASSOCIATION",
      "insightId": "ADyf4FvaVNDzu9MA2-IgFDkAAAAAAAAAEGpJd5sjicgauU2wmAlnWUyyI2hiO5it",
      "insightName": "Repeated Insight: Anomalous increase in Lambda
 ApigwLambdaDdbStack-22-Function duration due to increased number of invocations",
      "insightUrl": "https://us-east-1.console.aws.amazon.com/devops-guru/insight/
reactive/ADyf4FvaVNDzu9MA2-IgFDkAAAAAAAAAEGpJd5sjicgauU2wmAlnWUyyI2hiO5it",
      "insightType": "REACTIVE",
      "insightDescription": "At March 29, 2023 22:02 GMT, Lambda function
 ApigwLambdaDdbStack-22-Function had\n an increased duration anomaly possibly caused by
 the Lambda function invocation increase. DevOps Guru has detected this is a repeated
 insight. DevOps Guru treats repeated insights as 'Low Severity'.",
      "startTime": 1628767500000,
      "startTimeISO": "2023-03-29T22:00:00Z",
      "anomalies": [
        {
          "id": "AG2n8ljW74BoI1CHu-m_oAgAAAF7Ohu24N4Yro69ZSdUtn_alzPH7VTpaL30JXiF",
          "startTime": 1628767500000,
          "startTimeISO": "2023-03-29T22:00:00Z",
          "openTime": 1680127740000,
          "openTimeISO": "2023-03-29T22:09:00Z",
          "sourceDetails": [
            {
              "dataSource": "CW_METRICS",
              "dataIdentifiers": {
                "namespace": "AWS/SQS",
                "name": "ApproximateAgeOfOldestMessage",
```

```
                "stat": "Maximum",
                "unit": "None",
                "period": "60",
                "dimensions": "{\"QueueName\":\"FindingNotificationsDLQ\"}"
              }
            }
          ],
          "associatedResourceArns":[
           "arn:aws:sns:us-east-1:123456789012:DevOpsGuru-insights-sns"
          ]
        }
      ],
      "resourceCollection":{
      "cloudFormation":{
         "stackNames":[
            "CapstoneNotificationPublisherEcsApplicationInfrastructure"
          ]
        }
      }
}
```

更新中AWS Systems Manager整合於DevOps老師

您可以啟用建立 OpsItem 對於每一個新的見解AWS Systems Manager OpsCenter。OpsCenter 是一個集中式系統，您可以在其中檢視、調查和檢閱作業工作項目 (OpsItems). 該 OpsItems 因為您的見解可以幫助您管理解決觸發每個洞察力創建的異常行為的工作。如需詳細資訊，請參閱AWS Systems Manager OpsCenter和使用 OpsItem在AWS Systems Manager使用者指南。

> **Note**
>
> 如果您更改標籤字段的鍵或值 OpsItem，然後 DevOps大師無法更新 OpsItem。例如，如果您變更的標籤 OpsItem 從`"aws:RequestTag/DevOps-GuruInsightSsmOpsItemRelated": "true"`然後到別的東西 DevOps大師無法更新 OpsItem。

管理您的系統管理員整合

1. 打開亞馬遜 DevOps大師控制台https://console.aws.amazon.com/devops-guru/。
2. 在導覽窗格中選擇 Settings (設定)。

3. 在AWS Systems Manager整合，選取啟用 DevOps創建一個大師AWS OpstItem 在 OpsCenter 對於每個洞察力有一個 OpsItem 為每一個新的見解創建。取消選擇它以停止 OpsItem為每一個新的見解創建。

我們會向您收取費用 OpsItems 在您的帳戶中創建。如需詳細資訊，請參閱 AWS Systems Manager 定價。

更新記錄異常偵測DevOps老師

管理記錄異常偵測設定

1. 打開亞馬遜 DevOps大師控制台https://console.aws.amazon.com/devops-guru/。
2. 在導覽窗格中選擇 Settings (設定)。
3. 在記錄異常偵測，選取通過授予啟用日誌異常檢測 DevOps顯示與深入解析相關聯的記錄資料的 Guru 權限。有DevOpsGuru 顯示與見解相關的日誌資料。

更新中的加密設定DevOps老師

您可以更新要使用的加密設定AWS擁有的金鑰或AWS KMS客戶管理的金鑰。切換到管理的新客戶時AWS KMS來自管理的現有客戶的鑰匙AWS KMS鑰匙， DevOpsGuru 會使用新金鑰自動開始加密新擷取的中繼資料。歷史數據將與先前配置的客戶管理保持加密AWS KMS索引鍵。

> **Note**
>
> 如果您撤銷授予，或者禁用或刪除以前AWS KMS鑰匙， DevOpsGuru 將無法訪問此密鑰加密的任何數據，您可能會看到`AccessDeniedException`執行讀取操作時。

管理您的加密設定

1. 打開亞馬遜 DevOps大師控制台https://console.aws.amazon.com/devops-guru/。
2. 在導覽窗格中選擇 Settings (設定)。
3. 在加密區段中，選擇編輯加密。
4. 選取您要用來保護資料的加密類型。您可以使用預設值AWS擁有的金鑰、選擇現有的客戶管理金鑰，或建立新的客戶管理金鑰AWS KMS索引鍵。

5. 選擇 儲存 。

加密是其中一個重要組成部分 DevOps 大師安全。如需詳細資訊，請參閱 the section called “資料保護”。

查看通知

DevOpsGuru 中有不同類型的通知。

主題

此頁面上的段落會顯示每種通知類型的範例。

新洞察力

新見解的通知包含下列資訊：


```
{
   "accountId":"123456789101",
   "region":"eu-west-1",
   "messageType":"NEW_INSIGHT",
   "insightId":"a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
   "insightName": "Repeated Insight: ApiGateway 5XXError Anomalous In Application
 CanaryCommonResources-123456789101-LogAnomaly-4",
   "insightUrl":"https://eu-west-1.console.aws.amazon.com/devops-guru/insight/reactive/
a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
   "insightType":"REACTIVE",
   "insightDescription":"DevOps Guru has detected this is a repeated insight. DevOps
 Guru treats repeated insights as 'Low Severity'.",
   "insightSeverity":"medium",
   "startTime": 1680148920000,
   "startTimeISO": "2023-03-30T04:02:00Z",
   "anomalies":[
      {
         "id":"a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
         "startTime": 1680148800000,
         "startTimeISO": "2023-03-30T04:00:00Z",
```

```
         "openTime": 1680148920000,
         "openTimeISO": "2023-03-30T04:02:00Z",
         "sourceDetails":[
            {
               "dataSource":"CW_METRICS",
               "dataIdentifiers":{
                  "name":"ApproximateAgeOfOldestMessage",
                  "namespace":"AWS/SQS",
                  "period":"60",
                  "stat":"Maximum",
                  "unit":"None",
                  "dimensions":"{\"QueueName\":\"SampleQueue\"}"
               }
            }
         ],
         "associatedResourceArns":[
            "arn:aws:sqs:eu-west-1:123456789101:SampleQueue"
         ]
      }
   ],
   "resourceCollection":{
        "cloudFormation":{
            "stackNames":[
                "SampleApplication"
            ]
        },
   }
}
```

封閉洞察力

封閉式見解的通知包含下列資訊：

```
{
"accountId":"123456789101",
   "region":"us-east-1",
   "messageType":"CLOSED_INSIGHT",
   "insightId":"a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
   "insightName": "DynamoDB table writes are under utilized in mock-stack",
   "insightUrl":"https://us-east-1.console.aws.amazon.com/devops-guru/insight/
proactive/a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
   "insightType":"PROACTIVE",
   "insightDescription":"DynamoDB table writes are under utilized",
```

```
    "insightSeverity":"medium",
    "startTime": 1670612400000,
    "startTimeISO": "2022-12-09T19:00:00Z",
    "endTime": 1679994000000,
    "endTimeISO": "2023-03-28T09:00:00Z",
    "anomalies":[
       {
          "id":"a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa",
          "startTime": 1665428400000,
          "startTimeISO": "2022-10-10T19:00:00Z",
          "endTime": 1679986800000,
          "endTimeISO": "2023-03-28T07:00:00Z",
          "openTime": 1670612400000,
          "openTimeISO": "2022-12-09T19:00:00Z",
          "closeTime": 1679994000000,
          "closeTimeISO": "2023-03-28T09:00:00Z",
          "description":"Empty receives while messages are available",
          "anomalyResources":[
             {
                "type":"AWS::SQS::Queue",
                "name":"SampleQueue"
             }
          ],
          "sourceDetails":[
             {
                "dataSource":"CW_METRICS",
                "dataIdentifiers":{
                "name":"NumberOfEmptyReceives",
                   "namespace":"AWS/SQS",
                   "period":"60",
                   "stat":"Sum",
                   "unit":"COUNT",
                   "dimensions":"{\"QueueName\":\"SampleQueue\"}"
                }
             }
           ],
         "associatedResourceArn": [
             "arn:aws:sqs:us-east-1:123456789101:SampleQueue"
         ]
       }
    ],
    "resourceCollection":{
         "cloudFormation":{
             "stackNames":[
```

```
                "SampleApplication"
            ]
        }
    }
}
```

新關聯

新關聯的通知包含下列資訊：

```
{
"accountId":"123456789101",
   "region":"eu-west-1",
   "messageType":"NEW_ASSOCIATION",
   "insightId":"a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
   "insightName": "Repeated Insight: Anomalous increase in Lambda
 ApigwLambdaDdbStack-22-GetOneFunction duration due to increased number of
 invocations",
   "insightUrl":"https://eu-west-1.console.aws.amazon.com/devops-guru/insight/reactive/
a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
   "insightType":"REACTIVE",
   "insightDescription":"At March 29, 2023 22:02 GMT, Lambda function
 ApigwLambdaDdbStack-22-GetOneFunction had\nan increased duration anomaly possibly
 caused by the Lambda function invocation increase. DevOps Guru has detected this is a
 repeated insight. DevOps Guru treats repeated insights as 'Low Severity'.",
   "insightSeverity":"medium",
   "startTime": 1680127200000,
   "startTimeISO": "2023-03-29T22:00:00Z",
   "anomalies":[
      {
         "id":"a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
         "startTime":1672945500000,
         "startTimeISO": "2023-03-29T22:00:00Z",
         "openTime": 1680127740000,
         "openTimeISO": "2023-03-29T22:09:00Z",
         "sourceDetails":[
            {
               "dataSource":"CW_METRICS",
               "dataIdentifiers":{
               "namespace":"AWS/SQS",
                  "name":"ApproximateAgeOfOldestMessage",
                  "stat":"Maximum",
                  "unit":"None",
```

```
                  "period":"60",
                  "dimensions":"{\"QueueName\":\"SampleQueue\"}"
               }
            }
         ],
         "associatedResourceArns":[
            "arn:aws:sqs:eu-west-1:123456789101:SampleQueue"
         ]
      }
   ],
   "resourceCollection":{
        "cloudFormation":{
            "stackNames":[
                "SampleApplication"
            ]
        }
   }
}
```

新推薦

新建議的通知包含下列資訊：

```
{
   "accountId":"123456789101",
   "region":"us-east-1",
   "messageType":"NEW_RECOMMENDATION",
   "insightId":"a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
   "insightName": "Recreation of AWS SDK Service Clients",
   "insightUrl":"https://us-east-1.console.aws.amazon.com/devops-guru/insight/
proactive/a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
   "insightType":"PROACTIVE",
   "insightDescription": "Usually for a given service you can create one [AWS SDK
 service client](https://docs.aws.amazon.com/sdk-for-java/v1/developer-guide/creating-
clients.html) and reuse that client across your entire service.\n\nWhen instead you
 create a new AWS SDK service client for each call (e.g. for DynamoDB) it\u0027s
 generally a waste of CPU time.",
   "insightSeverity":"medium",
   "startTime": 1680125893576,
   "startTimeISO": "2023-03-29T21:38:13.576Z",
   "recommendations":[
      {
         "name":"Tune Availability Zones of your Lambda Function",
```

```
        "description":"Based on your configurations, we recommend that you set
 SampleFunction to be deployed in at least 3 Availability Zones to maintain Multi
 Availability Zone Redundancy.",
        "reason":"Lambda Function SampleFunction is currently only deployed to 2
 unique Availability zones in a region with 7 total Availability zones.",
        "link":"https://docs.aws.amazon.com/lambda/latest/dg/configuration-vpc.html",
        "relatedAnomalies":[
           {
              "sourceDetails":{
                   "cloudWatchMetrics":null
              },
              "resources":[
                 {
                    "name":"SampleFunction",
                    "type":"AWS::Lambda::Function"
                 }
              ],
              "associatedResourceArns": [
                 "arn:aws:lambda:arn:123456789101:SampleFunction"
              ]
           }
        ]
     }
  ],
  "resourceCollection": {
       "cloudFormation": {
       "stackNames":[
           "SampleApplication"
        ]
     }
  }
}
```

嚴重性升級

嚴重性升級的通知包含下列資訊：

```
{
"accountId":"123456789101",
   "region":"eu-west-1",
   "messageType":"SEVERITY_UPGRADED",
   "insightId":"a1b2c3d4-5678-90ab-cdef-EXAMPLEbbbbb",
```

```
   "insightName": "Repeated Insight: ApiGateway 5XXError Anomalous In Application
 CanaryCommonResources-123456789101-LogAnomaly-11",
   "insightUrl":"https://eu-west-1.console.aws.amazon.com/devops-guru/insight/reactive/
a1b2c3d4-5678-90ab-cdef-EXAMPLEbbbbb",
   "insightType":"REACTIVE",
   "insightDescription": "DevOps Guru has detected this is a repeated insight. DevOps
 Guru will treat future occurrences of this insight as 'Low Severity' for the next 7
 days.",
   "insightSeverity":"high",
   "startTime": 1680127320000,
   "startTimeISO": "2023-03-29T22:02:00Z",
   "resourceCollection":{
        "cloudFormation":{
            "stackNames":[
                "SampleApplication"
            ]
        }
   }
}
```

資源驗證失敗

您可以使用AWS CloudFormation堆疊和AWS標籤來篩選和識別您希望 DevOps Guru 分析的AWS資源。當您為 DevOps Guru 選擇無效的堆疊或標籤來識別資源時，DevOpsGuru 會建立SELECTED_RESOURCE_FILTER_VALIDATION_FAILURE通知。當您指定的標籤或堆疊名稱沒有與其相關聯的資源時，就會發生這種情況。若要充分利用 DevOps Guru 篩選方法，請選擇堆疊和標籤與其相關聯的資源。

```
{
    "accountId":"123456789101",
    "region":"eu-west-1",
    "messageType":"SELECTED_RESOURCE_FILTER_VALIDATION_FAILURE",
    "ResourceFilterType": "Tags",
    "InvalidResourceNames": [
         "Devops-Guru-tag-key-tag-value"
    ],
    "awsInsightSource": "aws.devopsguru"
}
```

檢視分析者的資源DevOps老師

DevOpsGuru 提供了資源名稱和他們的應用程序邊界的列表使用`ListMonitoredResources`動作。這些信息是從亞馬遜收集CloudWatch,AWS CloudTrail和其他AWS服務使用DevOps大師服務連結角色。

請注意，即使使用者沒有明確的權限來存取其他服務的 API，例如AWS Lambda或亞馬遜 RDS，DevOpsGuru 仍然提供該服務的資源列表，只要`ListMonitoredResources`允許執行動作。

主題

更新您的AWS分析涵蓋範圍DevOps老師

您可以更新哪個AWS您帳戶中的資源DevOps大師分析。經過分析的資源構成了您的DevOps大師覆蓋邊界。當您指定邊界時，您的資源會分組在應用程式中。您有四個邊界保障選項。

- 選擇擁有DevOpsGuru 會分析您帳戶中所有支援的資源。您帳戶中堆疊中的所有資源都會分組到應用程式中。如果您的帳戶中有多個堆疊，則每個堆疊中的資源會組成自己的應用程式。如果您帳戶中的任何資源不在堆疊中，則會將這些資源分組到自己的應用程式中。
- 透過選擇指定資源AWS CloudFormation定義這些資源的堆疊。如果你這樣做，DevOpsGuru 會分析您選擇的堆疊中指定的每個資源。如果您帳號中的資源未由您選擇的堆疊定義，則不會對其進行分析。如需詳細資訊，請參閱使用堆疊在AWS CloudFormation使用者指南和確定覆蓋範圍DevOps大師。
- 使用指定資源AWS標籤。DevOpsGuru 會分析您帳戶和區域中的所有資源，或包含您選擇的標籤鍵的所有資源。資源會根據選取的標籤值進行分組。如需詳細資訊，請參閱使用標籤識別 DevOps Guru 應用程式中的資源。
- 指定不分析任何資源，這樣就不會產生資源分析的費用。

> **Note**
>
> 如果您更新涵蓋範圍以停止分析資源，如果您查看由下列項目產生的現有見解，則可能會繼續產生小額費用。DevOps大師在過去。這些費用與用於擷取和顯示見解資訊的 API 呼叫相關聯。如需詳細資訊，請參閱亞馬遜DevOps大師定價。

DevOpsGuru 支援與支援服務相關聯的所有資源。如需有關支援服務和資源的詳細資訊，請參閱亞馬遜DevOps大師定價。

若要管理您的DevOps大師分析覆蓋

1. 打開亞馬遜DevOps大師控制台https://console.aws.amazon.com/devops-guru/。
2. 展開分析資源在導航窗格中。
3. 選擇 編輯 。
4. 選擇下列其中一個保障選項。

   - 選擇所有帳號資源如果你想DevOps大師來分析你的所有支持的資源AWS帳戶和地區。如果您選擇此選項，AWS帳號是您的資源分析涵蓋範圍界限。您帳戶中每個堆疊中的所有資源都會分組到他們自己的應用程式中。任何不在堆疊中的剩餘資源都會分組到它們自己的應用程式中。
   - 選擇CloudFormation堆疊如果你想DevOps大師分析您選擇的堆棧中的資源，然後選擇以下選項之一。
     - 所有資源— 分析了帳戶中堆棧中的所有資源。每個堆疊中的資源會分組到它們自己的應用程式中。不會分析您帳戶中未在堆疊中的任何資源。
     - 選取堆疊— 選擇你想要的堆棧DevOps大師來分析。您選取的每個堆疊中的資源會分組到它們自己的應用程式中。您可以在以下位置輸入堆疊名稱尋找堆疊以快速找到特定的堆疊。您最多可以選擇 1,000 個堆疊。

     如需詳細資訊，請參閱使用AWS CloudFormation堆棧以識別您的資源 DevOpsGuru。
   - 選擇标签如果你想DevOps大師分析包含您選擇的標籤的所有資源。選擇一個鍵，然後選擇下列其中一個選項。
     - 所有帳號資源— 分析目前區域和帳戶中的所有 AWS 資源。具有所選標籤鍵的資源會依標籤值分組 (如果有的話)。沒有此標籤鍵的資源會分別分組和分析。
     - 選擇特定標籤值— 包含標籤的所有資源鍵系統會分析您選擇的內容 DevOpsGuru 通過您的標籤將您的資源分組到應用程序中值。

     標籤的鍵必須以前綴開頭`devops-guru-`。此前綴不區分大小寫。例如，一個有效的鍵是`DevOps-Guru-Production-Applications`。如需詳細資訊，請參閱使用標籤識別 DevOps Guru 應用程式中的資源。
   - 選擇无如果你不想DevOps大師來分析任何資源。此選項禁用DevOpsGuru 這樣您就可以停止從資源分析產生費用。
5. 選擇 儲存 。

移除使用者的分析資源檢視

即使使用者沒有明確的權限，可以存取其他服務 (例如 Lambda 或 Amazon RDS) 的 API，DevOpsGuru 仍然提供該服務的資源列表，只要`ListMonitoredResources`允許執行動作。若要變更此行為，您可以更新AWS拒絕此動作的 IAM 政策。

```
{
            "Sid": "DenyListMonitoredResources",
            "Effect": "Deny",
            "Action": [
                "devops-guru:ListMonitoredResources"
            ]
}
```

DevOps 專家中的最佳實踐

以下最佳實踐可幫助您瞭解、診斷和修復 Amazon DevOps 專家檢測到的異常行為。使用的最佳實務了解中的見解DevOps大師控制台來解決 DevOps 專家檢測到的操作問題。

- 在見解的時間線視圖中，首先查看突出顯示的指標。它們往往是問題的關鍵指標。
- 使用 Amazon CloudWatch 查看在第一個突出顯示的指標之前發生的指標，以確定行為何時以及如何更改行為。這可以幫助您診斷並解決問題。
- 有關 Amazon RDS 資源，請查看 Performance Insights 指標。通過將計數器度量與數據庫負載相關聯，您可以獲取有關性能問題的詳細信息。如需詳細資訊，請參閱「」使用 DevOps Gurufor 亞馬遜 RDS 分析性能異常。
- 同一指標的多個維度通常可能是異常的。查看圖形視圖中的尺寸，以更深入地瞭解問題。
- 請查看深入見解的事件部分，瞭解在創建洞察時發生的部署或基礎架構事件。瞭解發生見解異常行為時發生的事件可以幫助您理解和診斷問題。
- 在您的操作系統中查找與線索洞察同時發生的票證。
- 在洞察中，請閱讀建議並訪問建議中的鏈接。這些通常具有故障排除步驟，可幫助您快速診斷和解決問題。
- 除非您已經解決了問題，否則不要忽略已解決的見解。每天一次，看看新的見解，即使它們已經解決。嘗試瞭解儘可能多的見解背後的根本原因，你可以。尋找一種可能是系統性問題標誌的模式。如果一個系統性問題得不到解決，將來可能造成更嚴重的問題。現在修復暫時性問題可以幫助防止未來更嚴重的事件。

Amazon DevOps 大師中的安全

雲安全 AWS 是最高的優先級。身為 AWS 客戶，您可以從資料中心和網路架構中獲益，這些架構是為了滿足對安全性最敏感的組織的需求而建置的。

安全是 AWS 與您之間共同的責任。共同責任模型將其描述為雲端的安全性和雲端中的安全性：

- 雲端的安全性 — AWS 負責保護在 AWS 雲端中執行 AWS 服務的基礎架構。 AWS 還為您提供可以安全使用的服務。若要了解適用於 Amazon DevOps Guru 的合規計劃，請參閱合規計劃的 AWS 服務範圍內的合規計劃 。
- 雲端中的安全性 — 您的責任取決於您使用的 AWS 服務。您也必須對其他因素負責，包括資料的機密性、您公司的要求和適用法律和法規。

本文檔可幫助您了解如何在使用 DevOps Guru 時應用共同的責任模型。下列主題說明如何設定 DevOps Guru 以符合您的安全性和合規性目標。您也會學到如何使用其他 AWS 服務，協助您監控和保護您的 DevOps Guru 資源。

主題

- Amazon DevOps 大師中的數據保護
- Amazon DevOps 大師的 Identity and Access Management
- 記錄和監控 DevOps大師
- DevOps大師和介面 VPC 端點 ()AWS PrivateLink
- DevOpsGuru 的基礎架構安全
- Amazon DevOps 大師的韌性

Amazon DevOps 大師中的數據保護

AWS 共同責任模型適用於 Amazon DevOps Guru 中的資料保護。如此模型中所述， AWS 負責保護執行所有 AWS 雲端. 您負責維護在此基礎設施上託管內容的控制權。您也同時負責所使用 AWS 服務 的安全組態和管理任務。如需資料隱私權的詳細資訊，請參閱資料隱私權常見問答集。如需有關歐洲資料保護的相關資訊，請參閱 AWS 安全性部落格上的 AWS 共同的責任模型和 GDPR 部落格文章。

基於資料保護目的，我們建議您使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 保護 AWS 帳戶 登入資料並設定個別使用者。如此一來，每個使用者都只會獲得授與完成其任務所必須的許可。我們也建議您採用下列方式保護資料：

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源進行通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用設定 API 和使用者活動記錄 AWS CloudTrail。
- 使用 AWS 加密解決方案以及其中的所有默認安全控制 AWS 服務。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果您在透過命令列介面或 API 存取時需要經 AWS 過 FIPS 140-2 驗證的加密模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的更多相關資訊，請參閱聯邦資訊處理標準 (FIPS) 140-2 概觀。

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的文字欄位中，例如名稱欄位。這包括當您 AWS 服務 使用控制台，API 或 AWS SDK 與 DevOps Guru 或其他人一起工作時。 AWS CLI您在標籤或自由格式文字欄位中輸入的任何資料都可能用於計費或診斷日誌。如果您提供外部伺服器的 URL，我們強烈建議請勿在驗證您對該伺服器請求的 URL 中包含憑證資訊。

DevOps大師中的數據加密

加密是 DevOps Guru 安全性的重要組成部分。某些加密 (例如傳輸中的資料) 是預設提供的，不需要您執行任何動作。其他加密，例如靜態資料，您可以在建立專案或建置時進行設定。

- 傳輸中的資料加密：客戶與 DevOps Guru 之間以及 Guru 與其下游相依性之間 DevOps的所有通訊均使用 TLS 保護，並使用簽名版本 4 簽署程序進行驗證。所有 DevOps Guru 端點都使用由 AWS Private Certificate Authority. 如需詳細資訊，請參閱簽章版本 4 簽署程序和什麼是 ACM PCA。
- 靜態資料加密：對於 DevOps Guru 分析的所有 AWS 資源，Amazon CloudWatch 指標和資料、資源 ID 和 AWS CloudTrail 事件均使用 Amazon S3、Amazon DynamoDB 和 Amazon Kinesis 存放。如果 AWS CloudFormation 堆棧用於定義分析的資源，則也會收集堆棧數據。 DevOps大師使用 Amazon S3、DynamoDB 和 Kinesis 的資料保留政策。Kinesis 中儲存的資料最多可保留一年，並視原則設定而定。存放在 Amazon S3 和 DynamoDB 中的資料會存放一年。

  存放的資料會使用 Amazon S3、DynamoDB 和 Kinesis 的 data-at-rest 加密功能進行加密。

  客戶受管金鑰： DevOpsGuru 支援加密客戶內容和敏感中繼資料，例如使用客戶管理金鑰 CloudWatch 記錄檔產生的異常狀況。此功能可讓您選擇新增自我管理的安全層，協助您符合組織的法規遵循與法規要求。如需在 DevOps Guru 設定中啟用客戶管理金鑰的相關資訊，請參閱the section called “更新加密”。

  您可以完全控制此層加密，因此能執行以下任務：

  - 建立和維護金鑰政策

- 建立和維護 IAM 政策和授予操作
- 啟用和停用金鑰政策
- 輪換金鑰密碼編譯資料
- 新增標籤
- 建立金鑰別名
- 安排金鑰供刪除

如需詳細資訊，請參閱 AWS Key Management Service 開發人員指南中的客戶管理金鑰。

> **Note**
>
> DevOpsGuru 使用 AWS 擁有的金鑰自動啟用靜態加密，以免費保護敏感的中繼資料。但是，使用客戶管理的金鑰需要 AWS KMS 支付費用。如需有關定價的詳細資訊，請參閱定 AWS Key Management Service 價。

DevOps大師如何使用贈款 AWS KMS

DevOpsGuru 需要授權才能使用您的客戶管理密鑰。

當您選擇使用客戶管理的金鑰啟用加密時， DevOpsGuru 會將 CreateGrant 要求傳送至，以代表您建立授權 AWS KMS。中的贈款 AWS KMS 用於授予 DevOps Guru 對客戶帳戶中 AWS KMS 密鑰的訪問權限。

DevOpsGuru 需要授權，才能使用您的客戶管理密鑰進行以下內部操作：

- 傳送 DescribeKey AWS KMS 要求，以確認建立追蹤器或地理圍欄集合時所輸入的對稱客戶受管 KMS 金鑰 ID 是否有效。
- 傳送 GenerateDataKey 要求 AWS KMS 以產生由客戶管理金鑰加密的資料金鑰。
- 發送解密請求 AWS KMS 以解密加密的數據密鑰，以便將其用於加密您的數據。

您可以隨時撤銷授予的存取權，或移除服務對客戶受管金鑰的存取權。如果您這樣做， DevOpsGuru 將無法存取客戶管理金鑰加密的任何資料，這會影響依賴該資料的作業。例如，如果您嘗試取得 DevOps Guru 無法存取的加密記錄異常資訊，則作業會傳回錯 AccessDeniedException 誤。

在 DevOps Guru 中監控您的加密金鑰

當您將 AWS KMS 客戶受管金鑰與 DevOps Guru 資源搭配使用時，您可以使用 AWS CloudTrail 或 CloudWatch Logs 來追蹤 DevOps Guru 傳送的要求 AWS KMS。

建立客戶受管金鑰

您可以使用 AWS Management Console 或 AWS KMS API 建立對稱的客戶管理金鑰。

若要建立對稱的客戶受管金鑰，請參閱建立對稱加密 KMS 金鑰。

金鑰政策

金鑰政策會控制客戶受管金鑰的存取權限。每個客戶受管金鑰都必須只有一個金鑰政策，其中包含決定誰可以使用金鑰及其使用方式的陳述式。在建立客戶受管金鑰時，可以指定金鑰政策。如需詳細資訊，請參閱 AWS Key Management Service 開發人員指南 AWS KMS中的驗證和存取控制。

若要將您的客戶管理金鑰與 DevOps Guru 資源搭配使用，必須在金鑰政策中允許下列 API 作業：

- `kms:CreateGrant`：新增客戶受管金鑰的授權。授予對指定 AWS KMS 金鑰的控制權限，允許存取權授與 DevOps Guru 所需的作業。如需使用授權的詳細資訊，請參閱開 AWS Key Management Service 發人員指南。

這允許 DevOps Guru 執行以下操作：

- 呼叫生成 GenerateDataKey 加密的數據密鑰並將其存儲，因為數據密鑰不會立即用於加密。
- 呼叫解密以使用已儲存的加密資料金鑰存取加密資料。
- 設定退休本金以允許服務。 RetireGrant
- 使用 kms：DescribeKey 提供客戶管理的金鑰詳細資料，以允許 DevOps Guru 驗證金鑰。

下列陳述式包含您可以為 DevOps Guru 新增的政策陳述式範例：

```
"Statement" : [
  {
    "Sid" : "Allow access to principals authorized to use DevOps Guru",
    "Effect" : "Allow",
    "Principal" : {
      "AWS" : "*"
    },
```

```
      "Action" : [
        "kms:DescribeKey",
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "kms:ViaService" : "devops-guru.Region.amazonaws.com",
          "kms:CallerAccount" : "111122223333"
        }
    },
    {
      "Sid": "Allow access for key administrators",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
       },
      "Action" : [
        "kms:*"
       ],
      "Resource": "arn:aws:kms:region:111122223333:key/key_ID"
    },
    {
      "Sid" : "Allow read-only access to key metadata to the account",
      "Effect" : "Allow",
      "Principal" : {
        "AWS" : "arn:aws:iam::111122223333:root"
      },
      "Action" : [
        "kms:Describe*",
        "kms:Get*",
        "kms:List*"
      ],
      "Resource" : "*"
    }
  ]
```

流量隱私權

您可以將 DevOps Guru 設定為使用介面 VPC 端點，以改善資源分析和洞察產生的安全性。若要執行此動作，您不需要網際網路閘道、NAT 裝置或虛擬私有閘道。它也不需要配置 PrivateLink，雖然這是建議的。如需詳細資訊，請參閱 DevOps大師和介面 VPC 端點 ()AWS PrivateLink。如需PrivateLink和 VPC 端點的詳細資訊，請參閱AWS PrivateLink和透過 PrivateLink存取 AWS 服務。

Amazon DevOps 大師的 Identity and Access Management

AWS Identity and Access Management (IAM) 可協助管理員安全地控制 AWS 資源存取權。 AWS 服務 IAM 管理員控制哪些人可以驗證 (登入) 和授權 (具有權限) 以使用 DevOps Guru 資源。您可以使用 IAM AWS 服務 ，無需額外付費。

主題

物件

您的使用方式 AWS Identity and Access Management (IAM) 會有所不同，具體取決於您在 DevOps Guru 中所做的工作。

服務使用者 — 如果您使用 DevOps Guru 服務執行工作，則管理員會為您提供所需的認證和權限。當您使用更多 DevOps Guru 功能來完成工作時，您可能需要其他權限。了解存取許可的管理方式可協助您向管理員請求正確的許可。如果您無法存取 DevOps Guru 中的功能，請參閱疑難排解 Amazon DevOps Guru 身分和存取權。

服務管理員 — 如果您負責公司的 DevOps Guru 資源，則可能擁有 DevOps Guru 的完整存取權。決定您的服務使用者應該存取哪些 DevOps Guru 功能和資源是您的工作。接著，您必須將請求提交給您的 IAM 管理員，來變更您服務使用者的許可。檢閱此頁面上的資訊，了解 IAM 的基本概念。若要進一步瞭解貴公司如何將 IAM 與 DevOps Guru 搭配使用，請參閱Amazon DevOps 大師如何與 IAM 合作。

IAM 管理員 — 如果您是 IAM 管理員，可能需要瞭解如何撰寫政策以管理 DevOps Guru 存取權的詳細資訊。若要檢視您可以在 IAM 中使用的 DevOps Guru 身分型政策範例，請參閱。Amazon 大師基於身份的政策 DevOps

使用身分驗證

驗證是您 AWS 使用身分認證登入的方式。您必須以 IAM 使用者身分或假設 IAM 角色進行驗證 (登入 AWS)。 AWS 帳戶根使用者

您可以使用透過 AWS 身分識別來源提供的認證，以聯合身分識別身分登入。 AWS IAM Identity Center (IAM 身分中心) 使用者、貴公司的單一登入身分驗證，以及您的 Google 或 Facebook 登入資料都是聯合身分識別的範例。您以聯合身分登入時，您的管理員先前已設定使用 IAM 角色的聯合身分。當您使 AWS 用同盟存取時，您會間接擔任角色。

根據您的使用者類型，您可以登入 AWS Management Console 或 AWS 存取入口網站。如需有關登入的詳細資訊 AWS，請參閱《AWS 登入 使用指南》 AWS 帳戶中的如何登入您的。

如果您 AWS 以程式設計方式存取，請 AWS 提供軟體開發套件 (SDK) 和命令列介面 (CLI)，以使用您的認證以加密方式簽署要求。如果您不使用 AWS 工具，則必須自行簽署要求。如需使用建議的方法自行簽署請求的詳細資訊，請參閱 IAM 使用者指南中的簽署 AWS API 請求。

無論您使用何種身分驗證方法，您可能都需要提供額外的安全性資訊。例如， AWS 建議您使用多重要素驗證 (MFA) 來增加帳戶的安全性。如需更多資訊，請參閱 AWS IAM Identity Center 使用者指南中的多重要素驗證和 IAM 使用者指南中的在 AWS中使用多重要素驗證 (MFA)。

AWS 帳戶 根使用者

當您建立時 AWS 帳戶，您會從一個登入身分開始，該身分可完整存取該帳戶中的所有資源 AWS 服務和資源。此身分稱為 AWS 帳戶 root 使用者，可透過使用您用來建立帳戶的電子郵件地址和密碼登入來存取。強烈建議您不要以根使用者處理日常任務。保護您的根使用者憑證，並將其用來執行只能由根使用者執行的任務。如需這些任務的完整清單，了解需以根使用者登入的任務，請參閱 IAM 使用者指南中的需要根使用者憑證的任務。

聯合身分

最佳作法是要求人類使用者 (包括需要系統管理員存取權的使用者) 使用與身分識別提供者的同盟，才能使用臨時認證 AWS 服務 來存取。

聯合身分識別是來自企業使用者目錄的使用者、Web 身分識別提供者、Identi ty Center 目錄，或使用透過身分識別來源提供的認證進行存取 AWS 服務 的任何使用者。 AWS Directory Service同盟身分存取時 AWS 帳戶，他們會假設角色，而角色則提供臨時認證。

對於集中式存取權管理，我們建議您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中建立使用者和群組，也可以連線並同步到自己身分識別來源中的一組使用者和群組，以便在所有應用程式 AWS 帳戶 和應用程式中使用。如需 IAM Identity Center 的相關資訊，請參閱 AWS IAM Identity Center 使用者指南中的什麼是 IAM Identity Center？。

IAM 使用者和群組

IAM 使用者是您內部的身分，具 AWS 帳戶 有單一人員或應用程式的特定許可。建議您盡可能依賴暫時憑證，而不是擁有建立長期憑證 (例如密碼和存取金鑰) 的 IAM 使用者。但是如果特定使用案例需要擁有長期憑證的 IAM 使用者，建議您輪換存取金鑰。如需更多資訊，請參閱 IAM 使用者指南中的為需要長期憑證的使用案例定期輪換存取金鑰。

IAM 群組是一種指定 IAM 使用者集合的身分。您無法以群組身分簽署。您可以使用群組來一次為多名使用者指定許可。群組可讓管理大量使用者許可的程序變得更為容易。例如，您可以擁有一個名為 IAMAdmins 的群組，並給予該群組管理 IAM 資源的許可。

使用者與角色不同。使用者只會與單一人員或應用程式建立關聯，但角色的目的是在由任何需要它的人員取得。使用者擁有永久的長期憑證，但角色僅提供暫時憑證。如需進一步了解，請參閱 IAM 使用者指南中的建立 IAM 使用者 (而非角色) 的時機。

IAM 角色

IAM 角色是您 AWS 帳戶 內部具有特定許可的身分。它類似 IAM 使用者，但不與特定的人員相關聯。您可以切換角色，在中暫時擔任 IAM 角色。 AWS Management Console 您可以透過呼叫 AWS CLI 或 AWS API 作業或使用自訂 URL 來擔任角色。如需使用角色的方法更多相關資訊，請參閱 IAM 使用者指南中的使用 IAM 角色。

使用暫時憑證的 IAM 角色在下列情況中非常有用：

- 聯合身分使用者存取 – 若要向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並獲授予由角色定義的許可。如需有關聯合角色的相關資訊，請參閱 IAM 使用者指南中的為第三方身分提供者建立角色。如果您使用 IAM Identity Center，則需要設定許可集。為控制身分驗證後可以存取的內容，IAM Identity Center 將許可集與 IAM 中的角色相關聯。如需有關許可集的資訊，請參閱 AWS IAM Identity Center 使用者指南中的許可集。
- 暫時 IAM 使用者許可 – IAM 使用者或角色可以擔任 IAM 角色來暫時針對特定任務採用不同的許可。
- 跨帳戶存取權 – 您可以使用 IAM 角色，允許不同帳戶中的某人 (信任的委託人) 存取您帳戶中的資源。角色是授予跨帳戶存取權的主要方式。但是，對於某些策略 AWS 服務，您可以將策略直接附加到資源（而不是使用角色作為代理）。若要了解跨帳戶存取權角色和資源型政策間的差異，請參閱 IAM 使用者指南中的 IAM 角色與資源類型政策的差異。

- 跨服務訪問 — 有些 AWS 服務 使用其他 AWS 服務功能。例如，當您在服務中進行呼叫時，該服務通常會在 Amazon EC2 中執行應用程式或將物件儲存在 Amazon Simple Storage Service (Amazon S3) 中。服務可能會使用呼叫主體的許可、使用服務角色或使用服務連結角色來執行此作業。
  - 轉寄存取工作階段 (FAS) — 當您使用 IAM 使用者或角色在中執行動作時 AWS，您會被視為主體。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 會使用主體呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。只有當服務收到需要與其 AWS 服務 他資源互動才能完成的請求時，才會發出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的政策詳細資訊，請參閱《轉發存取工作階段》。
  - 服務角色 – 服務角色是服務擔任的 IAM 角色，可代表您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需更多資訊，請參閱 IAM 使用者指南中的建立角色以委派許可給 AWS 服務。
  - 服務連結角色 — 服務連結角色是連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。
- 在 Amazon EC2 上執行的應用程式 — 您可以使用 IAM 角色來管理在 EC2 執行個體上執行的應用程式以及發出 AWS CLI 或 AWS API 請求的臨時登入資料。這是在 EC2 執行個體內儲存存取金鑰的較好方式。若要將 AWS 角色指派給 EC2 執行個體並提供給其所有應用程式，請建立連接至執行個體的執行個體設定檔。執行個體設定檔包含該角色，並且可讓 EC2 執行個體上執行的程式取得暫時憑證。如需更多資訊，請參閱 IAM 使用者指南中的利用 IAM 角色來授予許可給 Amazon EC2 執行個體上執行的應用程式。

若要了解是否要使用 IAM 角色或 IAM 使用者，請參閱 IAM 使用者指南中的建立 IAM 角色 (而非使用者) 的時機。

使用政策管理存取權

您可以透 AWS 過建立原則並將其附加至 AWS 身分識別或資源來控制中的存取。原則是一個物件 AWS ，當與身分識別或資源相關聯時，會定義其權限。 AWS 當主參與者 (使用者、root 使用者或角色工作階段) 提出要求時，評估這些原則。政策中的許可決定是否允許或拒絕請求。大多數原則會 AWS 以 JSON 文件的形式儲存在中。如需 JSON 政策文件結構和內容的更多相關資訊，請參閱 IAM 使用者指南中的 JSON 政策概觀。

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

預設情況下，使用者和角色沒有許可。若要授予使用者對其所需資源執行動作的許可，IAM 管理員可以建立 IAM 政策。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

IAM 政策定義該動作的許可，無論您使用何種方法來執行操作。例如，假設您有一個允許 `iam:GetRole` 動作的政策。具有該原則的使用者可以從 AWS Management Console AWS CLI、或 AWS API 取得角色資訊。

身分型政策

身分型政策是可以附加到身分 (例如 IAM 使用者、使用者群組或角色) 的 JSON 許可政策文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。若要了解如何建立身分類型政策，請參閱 IAM 使用者指南中的建立 IAM 政策。

身分型政策可進一步分類成內嵌政策或受管政策。內嵌政策會直接內嵌到單一使用者、群組或角色。受管理的策略是獨立策略，您可以將其附加到您的 AWS 帳戶. 受管政策包括 AWS 受管政策和客戶管理的策略。若要了解如何在受管政策及內嵌政策間選擇，請參閱 IAM 使用者指南中的在受管政策和內嵌政策間選擇。

資源型政策

資源型政策是連接到資源的 JSON 政策文件。資源型政策的最常見範例是 IAM 角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定主體。主參與者可以包括帳戶、使用者、角色、同盟使用者或。 AWS 服務

資源型政策是位於該服務中的內嵌政策。您無法在以資源為基礎的政策中使用 IAM 的 AWS 受管政策。

存取控制清單 (ACL)

存取控制清單 (ACL) 可控制哪些委託人 (帳戶成員、使用者或角色) 擁有存取某資源的許可。ACL 類似於資源型政策，但它們不使用 JSON 政策文件格式。

Amazon S3 和 Amazon VPC 是支援 ACL 的服務範例。 AWS WAF若要進一步了解 ACL，請參閱 Amazon Simple Storage Service 開發人員指南中的存取控制清單 (ACL) 概觀。

其他政策類型

AWS 支援其他較不常見的原則類型。這些政策類型可設定較常見政策類型授予您的最大許可。

- 許可界限 – 許可範圍是一種進階功能，可供您設定身分型政策能授予 IAM 實體 (IAM 使用者或角色) 的最大許可。您可以為實體設定許可界限。所產生的許可會是實體的身分型政策和其許可界限的交集。會在 `Principal` 欄位中指定使用者或角色的資源型政策則不會受到許可界限限制。所有這類政

策中的明確拒絕都會覆寫該允許。如需許可範圍的更多相關資訊，請參閱 IAM 使用者指南中的 IAM 實體許可範圍。

- 服務控制策略（SCP）— SCP 是 JSON 策略，用於指定中組織或組織單位（OU）的最大權限。AWS Organizations AWS Organizations 是一種用於分組和集中管理您企業擁 AWS 帳戶 有的多個服務。若您啟用組織中的所有功能，您可以將服務控制政策 (SCP) 套用到任何或所有帳戶。SCP 限制成員帳戶中實體的權限，包括每個 AWS 帳戶根使用者帳戶。如需組織和 SCP 的更多相關資訊，請參閱 AWS Organizations 使用者指南中的 SCP 運作方式。
- 工作階段政策 – 工作階段政策是一種進階政策，您可以在透過編寫程式的方式建立角色或聯合使用者的暫時工作階段時，作為參數傳遞。所產生工作階段的許可會是使用者或角色的身分型政策和工作階段政策的交集。許可也可以來自資源型政策。所有這類政策中的明確拒絕都會覆寫該允許。如需更多資訊，請參閱 IAM 使用者指南中的工作階段政策。

多種政策類型

將多種政策類型套用到請求時，其結果形成的許可會更為複雜、更加難以理解。要了解如何在涉及多個政策類型時 AWS 確定是否允許請求，請參閱《IAM 使用者指南》中的政策評估邏輯。

DevOpsGuru 更新 AWS 受管理政策和服務連結角色

檢視有關 DevOps Guru AWS 受管理政策的更新和服務連結角色的詳細資料，因為此服務開始追蹤這些變更。如需有關此頁面變更的自動警示，請訂閱 DevOps Guru 上的 RSS 摘要亞馬遜DevOps大師文檔歷史。

變更	描述	日期
AmazonDevOpsGuruConsoleFullAccess – 更新現有政策。	受AmazonDevOpsGuruFullAccess 管政策現在支援 Amazon SNS 訂閱。	2023 年 8 月 9 日
AmazonDevOpsGuruReadOnlyAccess – 更新現有政策	受AmazonDevOpsGuruReadOnlyAccess 管政策現在支援 Amazon SNS 訂閱清單的唯讀存取。	2023 年 8 月 9 日
AmazonDevOpsGuruServiceRolePolicy – 更新現有政策。	AWSServiceRoleForDevOpsGuru 服務連結角色	2023 年 1 月 11 日

變更	描述	日期
	現在支援存取 REST API 上的 API Gateway GET 動作。	
AmazonDevOpsGuruServiceRolePolicy – 更新現有政策。	服AWSServiceRoleForDevOpsGuru 務連結角色現在支援多個 Amazon 簡單儲存服務和 Service Quotas 動作。	2022 年 10 月 19 日
AmazonDevOpsGuruFullAccess – 更新現有政策	AmazonDevOpsGuruFullAccess 受管政策 現在支援存取 CloudWatch FilterLogEvents 動作。	2022 年 8 月 30 日
AmazonDevOpsGuruConsoleFullAccess – 更新現有政策	受AmazonDevOpsGuruConsoleFullAccess 管理的原則現在支援存取 CloudWatchFilterLogEvents 動作。	2022 年 8 月 30 日
AmazonDevOpsGuruReadOnlyAccess – 更新現有政策	受AmazonDevOpsGuruReadOnlyAccess 管理的原則現在支援 CloudWatch FilterLogEvents 動作的唯讀存取權。	2022 年 8 月 30 日
AmazonDevOpsGuruServiceRolePolicy – 更新現有政策。	AWSServiceRoleForDevOpsGuru 服務連結角色現在支援記 CloudWatch 錄檔動作FilterLogEvents DescribeLogGroups 、和DescribeLogStreams 。	2022 年 7 月 12 日
DevOpsGuru 的身分識別型原則 — 新的受管原則。	已新增AmazonDevOpsGuruConsoleFullAccess 原則。	2021 年 12 月 16 日

變更	描述	日期
AmazonDevOpsGuruServiceRolePolicy – 更新現有政策。	AWSServiceRoleForDevOpsGuru 服務連結角色現在支援 Performance Insights DescribeMetricsKeys 和 Amazon RDS DescribeDBInstances 動作。	2021 年 12 月 1 日
AmazonDevOpsGuruReadOnlyAccess – 更新現有政策	受AmazonDevOpsGuruReadOnlyAccess 管政策現在支援 Amazon RDS DescribeDBInstances 動作的唯讀存取。	2021 年 12 月 1 日
AmazonDevOpsGuruFullAccess – 更新現有政策	受AmazonDevOpsGuruFullAccess 管政策現在支援存取 Amazon RDS DescribeDBInstances 動作。	2021 年 12 月 1 日
Amazon 大師基於身份的政策 DevOps-添加了新策略。	AWSServiceRoleForDevOpsGuru 服務連結角色現在支援存取 Amazon RDS DescribeDBInstances 和 Performance Insights GetResourceMetrics 動作。 受AmazonDevOpsGuruOrganizationsAccess 管理的原則可讓您存取組織內的 DevOps Guru。	2021 年 11 月 16 日
AmazonDevOpsGuruServiceRolePolicy – 更新現有政策。	AWSServiceRoleForDevOpsGuru 服務連結角色現在支援 AWS Organizations。	2021 年 11 月 4 日

變更	描述	日期
AmazonDevOpsGuruServiceRolePolicy – 更新現有政策。	AWSServiceRoleForDevOpsGuru 服務連結角色現在包含ssm:CreateOpsItem 和ssm:AddTagsToResource 動作的新條件。	2021 年 10 月 11 日
Guru 的 DevOps服務連結角色權限 – 更新現有政策。	AWSServiceRoleForDevOpsGuru 服務連結角色現在包含ssm:CreateOpsItem 和ssm:AddTagsToResource 動作的新條件。	2021 年 6 月 14 日
AmazonDevOpsGuruReadOnlyAccess – 更新現有政策	受AmazonDevOpsGuruReadOnlyAccess 管理的政策現在允許對 AWS Identity and Access Management GetRole和 DevOps Guru DescribeFeedback 動作的唯讀存取。	2021 年 6 月 14 日
AmazonDevOpsGuruReadOnlyAccess – 更新現有政策	受AmazonDevOpsGuruReadOnlyAccess 管理的原則現在允許對 DevOps Guru GetCostEstimation 和StartCostEstimation 動作的唯讀存取。	2021 年 4 月 27 日

變更	描述	日期
AmazonDevOpsGuruServiceRolePolicy – 更新現有政策。	該AWSServiceRoleForDevOpsGuru 角色現在允許存取 AWS Systems Manager AddTagsToResource 和 Amazon EC2 Auto Scaling DescribeAutoScalingGroups 動作。	2021 年 4 月 27 日
DevOps大師開始跟踪更改	DevOpsGuru 開始追蹤其 AWS 受管理政策的變更。	2020 年 12 月 10 日

Amazon DevOps 大師如何與 IAM 合作

在您使用 IAM 管理 DevOps Guru 的存取權限之前，請先了解哪些 IAM 功能可與 DevOps Guru 搭配使用。

您可以與 Amazon DevOps 大師一起使用的 IAM 功能

IAM 功能	DevOps大師支持
身分型政策	是
資源型政策	否
政策動作	是
政策資源	是
政策條件索引鍵	是
ACL	否
ABAC(政策中的標籤)	否
臨時憑證	是

IAM 功能	DevOps大師支持
主體許可	是
服務角色	否
服務連結角色	是

若要深入瞭解 DevOps Guru 和其他 AWS 服務如何使用大多數 IAM 功能，請參閱 IAM 使用者指南中的搭配 IAM 使用的AWS 服務。

Guru 的基於身份識別的政策 DevOps

支援身分型政策	是

身分型政策是可以連接到身分 (例如 IAM 使用者、使用者群組或角色) 的 JSON 許可政策文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。若要了解如何建立身分類型政策，請參閱《IAM 使用者指南》中的建立 IAM 政策。

使用 IAM 身分型政策，您可以指定允許或拒絕的動作和資源，以及在何種條件下允許或拒絕動作。您無法在身分型政策中指定主體，因為這會套用至連接的使用者或角色。如要了解您在 JSON 政策中使用的所有元素，請參閱《IAM 使用者指南》中的 IAM JSON 政策元素參考。

Guru 的基於身份的政策示例 DevOps

若要檢視 DevOps Guru 身分型原則的範例，請參閱。Amazon 大師基於身份的政策 DevOps

在 DevOps大師內基於資源的策略

支援以資源基礎的政策	否

資源型政策是附加到資源的 JSON 政策文件。資源型政策的最常見範例是 IAM 角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定主體。主參與者可以包括帳戶、使用者、角色、同盟使用者或。 AWS 服務

若要啟用跨帳戶存取，您可以指定在其他帳戶內的所有帳戶或 IAM 實體，作為資源型政策的主體。新增跨帳戶主體至資源型政策，只是建立信任關係的一半。當主體和資源位於不同時 AWS 帳戶，受信任帳戶中的 IAM 管理員也必須授與主體實體 (使用者或角色) 權限，才能存取資源。其透過將身分型政策連接到實體來授與許可。不過，如果資源型政策會為相同帳戶中的主體授予存取，這時就不需要額外的身分型政策。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 角色與資源型政策有何差異。

DevOps大師的政策行動

支援政策動作	是

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼条件下可以對什麼資源執行哪些動作。

JSON 政策的 `Action` 元素描述您可以用來允許或拒絕政策中存取的動作。原則動作通常與關聯的 AWS API 作業具有相同的名稱。有一些例外狀況，例如沒有相符的 API 操作的僅限許可動作。也有一些作業需要政策中的多個動作。這些額外的動作稱為相依動作。

政策會使用動作來授予執行相關聯動作的許可。

若要查看 DevOps Guru 動作清單，請參閱服務授權參考中的 Amazon DevOps Guru 定義的動作。

DevOpsGuru 中的策略操作在操作之前使用以下前綴：

```
aws
```

若要在單一陳述式中指定多個動作，請用逗號分隔。

```
"Action": [
      "aws:action1",
      "aws:action2"
         ]
```

若要檢視 DevOps Guru 身分型原則的範例，請參閱。Amazon 大師基於身份的政策 DevOps

DevOps大師的政策資源

支援政策資源	是

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Resource JSON 政策元素可指定要套用動作的物件。陳述式必須包含 Resource 或 NotResource 元素。最佳實務是使用其 Amazon Resource Name (ARN) 來指定資源。您可以針對支援特定資源類型的動作 (稱為資源層級許可) 來這麼做。

對於不支援資源層級許可的動作 (例如列出操作)，請使用萬用字元 (*) 來表示陳述式適用於所有資源。

```
"Resource": "*"
```

若要查看 DevOps Guru 資源類型及其 ARN 的清單，請參閱服務授權參考中的 Amazon DevOps Guru 定義的資源。若要了解可以使用哪些動作指定每個資源的 ARN，請參閱 Amazon DevOps Guru 定義的動作。

若要檢視 DevOps Guru 身分型原則的範例，請參閱。Amazon 大師基於身份的政策 DevOps

DevOpsGuru 的政策條件金鑰

支援服務特定政策條件金鑰	是

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Condition 元素 (或 Condition 區塊) 可讓您指定使陳述式生效的條件。Condition 元素是選用項目。您可以建立使用條件運算子的條件運算式 (例如等於或小於)，來比對政策中的條件和請求中的值。

若您在陳述式中指定多個 Condition 元素，或是在單一 Condition 元素中指定多個索引鍵， AWS 會使用邏輯 AND 操作評估他們。如果您為單一條件索引鍵指定多個值，請使用邏輯OR運算來 AWS 評估條件。必須符合所有條件，才會授與陳述式的許可。

您也可以在指定條件時使用預留位置變數。例如，您可以只在使用者使用其 IAM 使用者名稱標記時，將存取資源的許可授予該 IAM 使用者。如需更多資訊，請參閱 IAM 使用者指南中的 IAM 政策元素：變數和標籤。

AWS 支援全域條件金鑰和服務特定條件金鑰。若要查看所有 AWS 全域條件金鑰，請參閱《IAM 使用者指南》中的AWS 全域條件內容金鑰。

若要查看 DevOps Guru 條件金鑰清單，請參閱服務授權參考中的 Amazon DevOps Guru 的條件金鑰。若要了解可以使用條件金鑰的動作和資源，請參閱 Amazon DevOps Guru 定義的動作。

若要檢視 DevOps Guru 身分型原則的範例，請參閱。Amazon 大師基於身份的政策 DevOps

大師中DevOps的訪問控制列表（ACL）

支援 ACL	否

存取控制清單 (ACL) 可控制哪些主體 (帳戶成員、使用者或角色) 擁有存取某資源的許可。ACL 類似於資源型政策，但它們不使用 JSON 政策文件格式。

基於屬性的訪問控制（ABAC）與 Guru DevOps

支援 ABAC (政策中的標籤)	否

屬性型存取控制 (ABAC) 是一種授權策略，可根據屬性來定義許可。在中 AWS，這些屬性稱為標籤。您可以將標籤附加到 IAM 實體 (使用者或角色) 和許多 AWS 資源。為實體和資源加上標籤是 ABAC 的第一步。您接著要設計 ABAC 政策，允許在主體的標籤與其嘗試存取的資源標籤相符時操作。

ABAC 在成長快速的環境中相當有幫助，並能在政策管理變得繁瑣時提供協助。

若要根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件金鑰，在政策的條件元素中，提供標籤資訊。

如果服務支援每個資源類型的全部三個條件金鑰，則對該服務而言，值為 Yes。如果服務僅支援某些資源類型的全部三個條件金鑰，則值為 Partial。

如需 ABAC 的詳細資訊，請參閱《IAM 使用者指南》中的什麼是 ABAC?。如要查看含有設定 ABAC 步驟的教學課程，請參閱《IAM 使用者指南》中的使用屬性型存取控制 (ABAC)。

使用 DevOps Guru 的臨時登入資料

支援臨時憑證	是

當您使用臨時憑據登錄時，某些 AWS 服務 不起作用。如需其他資訊，包括哪些 AWS 服務 與臨時登入資料搭配AWS 服務 使用，請參閱 IAM 使用者指南中的 IAM。

如果您使用除了使用者名稱和密碼以外的任何方法登入，則您正在 AWS Management Console 使用臨時認證。例如，當您 AWS 使用公司的單一登入 (SSO) 連結存取時，該程序會自動建立暫時認證。當您以使用者身分登入主控台，然後切換角色時，也會自動建立臨時憑證。如需切換角色的詳細資訊，請參閱《IAM 使用者指南》中的切換至角色 (主控台)。

您可以使用 AWS CLI 或 AWS API 手動建立臨時登入資料。然後，您可以使用這些臨時登入資料來存取 AWS。 AWS 建議您動態產生臨時登入資料，而不是使用長期存取金鑰。如需詳細資訊，請參閱 IAM 中的暫時性安全憑證。

Guru 的 DevOps跨服務主體權限

支援轉寄存取工作階段 (FAS)	是

當您使用 IAM 使用者或角色在中執行動作時 AWS，您會被視為主體。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 會使用主體呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。只有當服務收到需要與其 AWS 服務 他資源互動才能完成的請求時，才會發出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的政策詳細資訊，請參閱《轉發存取工作階段》。

DevOpsGuru 的服務角色

支援服務角色	否

服務角色是服務擔任的 IAM 角色，可代您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需更多資訊，請參閱 IAM 使用者指南中的建立角色以委派許可給 AWS 服務。

> **Warning**
>
> 變更服務角色的權限可能會中斷 DevOps Guru 功能。只有在 DevOps Guru 提供指引時才編輯服務角色。

Guru 的 DevOps服務連結角色

支援服務連結角色	是

服務連結角色是一種連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

如需建立或管理服務連結角色的詳細資訊，請參閱可搭配 IAM 運作的AWS 服務。在表格中尋找服務，其中包含服務連結角色欄中的 Yes。選擇是連結，以檢視該服務的服務連結角色文件。

Amazon 大師基於身份的政策 DevOps

依預設，使用者和角色沒有建立或修改 DevOps Guru 資源的權限。他們也無法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或 AWS API 來執行工作。若要授予使用者對其所需資源執行動作的許可，IAM 管理員可以建立 IAM 政策。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

若要了解如何使用這些範例 JSON 政策文件建立 IAM 身分型政策，請參閱《IAM 使用者指南》中的建立 IAM 政策。

有關 DevOps Guru 定義的動作和資源類型的詳細資訊，包括每種資源類型的 ARN 格式，請參閱服務授權參考中的 Amazon DevOps Guru 的動作、資源和條件金鑰。

主題

- 政策最佳實務
- 使用大 DevOps師控制台
- 允許使用者檢視他們自己的許可
- 適用於DevOps大師的 AWS 受管 (預先定義) 政策

政策最佳實務

以身分識別為基礎的原則會決定某人是否可以建立、存取或刪除您帳戶中的 DevOps Guru 資源。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管原則並邁向最低權限權限 — 若要開始授與使用者和工作負載的權限，請使用可授與許多常見使用案例權限的AWS 受管理原則。它們可用在您的 AWS 帳戶. 建議您透過定義特定於您使用案例的 AWS 客戶管理政策，進一步降低使用權限。如需更多資訊，請參閱 IAM 使用者指南中的 AWS 受管政策或任務職能的AWS 受管政策。
- 套用最低許可許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的權限。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的更多相關資訊，請參閱 IAM 使用者指南中的 IAM 中的政策和許可。

- 使用 IAM 政策中的條件進一步限制存取權 – 您可以將條件新增至政策，以限制動作和資源的存取。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。您也可以使用條件來授與對服務動作的存取權 (如透過特定) 使用這些動作 AWS 服務，例如 AWS CloudFormation。如需更多資訊，請參閱 IAM 使用者指南中的 IAM JSON 政策元素：條件。
- 使用 IAM Access Analyzer 驗證 IAM 政策，確保許可安全且可正常運作 – IAM Access Analyzer 驗證新政策和現有政策，確保這些政策遵從 IAM 政策語言 (JSON) 和 IAM 最佳實務。IAM Access Analyzer 提供 100 多項政策檢查及切實可行的建議，可協助您編寫安全且實用的政策。如需更多資訊，請參閱 IAM 使用者指南中的 IAM Access Analyzer 政策驗證。
- 需要多因素身份驗證 (MFA) — 如果您的案例需要 IAM 使用者或根使用者 AWS 帳戶，請開啟 MFA 以獲得額外的安全性。若要在呼叫 API 作業時請求 MFA，請將 MFA 條件新增至您的政策。如需更多資訊，請參閱 IAM 使用者指南中的設定 MFA 保護的 API 存取。

如需 IAM 中最佳實務的相關資訊，請參閱 IAM 使用者指南中的 IAM 安全最佳實務。

使用大 DevOps師控制台

若要存取 Amazon DevOps Guru 主控台，您必須擁有最少一組許可。這些權限必須允許您列出並檢視您的 AWS 帳戶. DevOps 如果您建立比最基本必要許可更嚴格的身分型政策，則對於具有該政策的實體 (使用者或角色) 而言，主控台就無法如預期運作。

您不需要為僅對 AWS CLI 或 AWS API 進行呼叫的使用者允許最低主控台權限。反之，只需允許存取符合他們嘗試執行之 API 操作的動作就可以了。

若要確保使用者和角色仍可使用 DevOps Guru 主控台，請同時將 DevOps Guru `AmazonDevOpsGuruReadOnlyAccess` 或`AmazonDevOpsGuruFullAccess` AWS 受管理的原則附加至實體。如需詳細資訊，請參閱《IAM 使用者指南》中的新增許可到使用者。

允許使用者檢視他們自己的許可

此範例會示範如何建立政策，允許 IAM 使用者檢視附加到他們使用者身分的內嵌及受管政策。此原則包含在主控台上或以程式設計方式使用 AWS CLI 或 AWS API 完成此動作的權限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
```

```
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

適用於DevOps大師的 AWS 受管 (預先定義) 政策

AWS 透過提供由建立和管理的獨立 IAM 政策來解決許多常見使用案例 AWS。這些 AWS受管理的政策會為常見使用案例授與必要的權限，因此您可以避免調查需要哪些權限。如需詳細資訊，請參閱《IAM 使用者指南》中的 AWS Managed Policies (AWS 受管政策)。

若要建立和管理 DevOps Guru 服務角色，您還必須附加名為`IAMFullAccess`的 AWS受管理原則。

您也可以建立自己的自訂 IAM 政策，以允許 DevOps Guru 動作和資源的許可。您可以將這些自訂政策連接至需要這些許可的使用者或群組。

下列 AWS受管理的原則 (您可以附加至帳戶中的使用者) 是 DevOps Guru 所特有的。

主題

- AmazonDevOpsGuruFullAccess
- AmazonDevOpsGuruConsoleFullAccess
- AmazonDevOpsGuruReadOnlyAccess

- AmazonDevOpsGuruOrganizationsAccess

AmazonDevOpsGuruFullAccess

AmazonDevOpsGuruFullAccess— 提供對 DevOps Guru 的完整存取權，包括建立 Amazon SNS 主題、存取 Amazon CloudWatch 指標和存取 AWS CloudFormation 堆疊的許可。僅將其套用至您要授予 Guru 完全控制權的系統管理層級使用者。 DevOps

此原AmazonDevOpsGuruFullAccess則包含下列陳述式。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DevOpsGuruFullAccess",
            "Effect": "Allow",
            "Action": [
                "devops-guru:*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CloudFormationListStacksAccess",
            "Effect": "Allow",
            "Action": [
                "cloudformation:DescribeStacks",
                "cloudformation:ListStacks"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CloudWatchGetMetricDataAccess",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:GetMetricData"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SnsListTopicsAccess",
            "Effect": "Allow",
            "Action": [
                "sns:ListTopics",
```

```
                "sns:ListSubscriptionsByTopic"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SnsTopicOperations",
            "Effect": "Allow",
            "Action": [
                "sns:CreateTopic",
                "sns:GetTopicAttributes",
                "sns:SetTopicAttributes",
                "sns:Subscribe",
                "sns:Publish"
            ],
            "Resource": "arn:aws:sns:*:*:DevOps-Guru-*"
        },
        {
            "Sid": "DevOpsGuruSlrCreation",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/devops-
guru.amazonaws.com/AWSServiceRoleForDevOpsGuru",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "devops-guru.amazonaws.com"
                }
            }
        },
        {
            "Sid": "DevOpsGuruSlrDeletion",
            "Effect": "Allow",
            "Action": [
                "iam:DeleteServiceLinkedRole",
                "iam:GetServiceLinkedRoleDeletionStatus"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/devops-
guru.amazonaws.com/AWSServiceRoleForDevOpsGuru"
        },
        {
            "Sid": "RDSDescribeDBInstancesAccess",
            "Effect": "Allow",
            "Action": [
                "rds:DescribeDBInstances"
            ],
```

```
            "Resource": "*"
        },
        {
          "Sid": "CloudWatchLogsFilterLogEventsAccess",
          "Effect": "Allow",
          "Action": [
              "logs:FilterLogEvents"
          ],
          "Resource": "arn:aws:logs:*:*:log-group:*",
          "Condition": {
              "StringEquals": {
                  "aws:ResourceTag/DevOps-Guru-Analysis": "true"
              }
          }
        }
    ]
}
```

AmazonDevOpsGuruConsoleFullAccess

AmazonDevOpsGuruConsoleFullAccess— 提供對 DevOps Guru 的完整存取權，包括建立 Amazon SNS 主題、存取 Amazon CloudWatch 指標和存取 AWS CloudFormation 堆疊的許可。此政策具有其他效能洞見許可，因此您可以在主控台中檢視與異常 Amazon RDS Aurora 資料庫執行個體相關的詳細分析。僅將其套用至您要授予 Guru 完全控制權的系統管理層級使用者。 DevOps

此原AmazonDevOpsGuruConsoleFullAccess則包含下列陳述式。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DevOpsGuruFullAccess",
            "Effect": "Allow",
            "Action": [
                "devops-guru:*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CloudFormationListStacksAccess",
            "Effect": "Allow",
            "Action": [
                "cloudformation:DescribeStacks",
```

```
                "cloudformation:ListStacks"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CloudWatchGetMetricDataAccess",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:GetMetricData"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SnsListTopicsAccess",
            "Effect": "Allow",
            "Action": [
                "sns:ListTopics",
                "sns:ListSubscriptionsByTopic"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SnsTopicOperations",
            "Effect": "Allow",
            "Action": [
                "sns:CreateTopic",
                "sns:GetTopicAttributes",
                "sns:SetTopicAttributes",
                "sns:Subscribe",
                "sns:Publish"
            ],
            "Resource": "arn:aws:sns:*:*:DevOps-Guru-*"
        },
        {
            "Sid": "DevOpsGuruSlrCreation",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/devops-
guru.amazonaws.com/AWSServiceRoleForDevOpsGuru",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "devops-guru.amazonaws.com"
                }
            }
```

```
        },
        {
            "Sid": "DevOpsGuruSlrDeletion",
            "Effect": "Allow",
            "Action": [
                "iam:DeleteServiceLinkedRole",
                "iam:GetServiceLinkedRoleDeletionStatus"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/devops-
guru.amazonaws.com/AWSServiceRoleForDevOpsGuru"
        },
        {
            "Sid": "RDSDescribeDBInstancesAccess",
            "Effect": "Allow",
            "Action": [
                "rds:DescribeDBInstances"
            ],
            "Resource": "*"
        },
        {
            "Sid": "PerformanceInsightsMetricsDataAccess",
            "Effect": "Allow",
            "Action": [
                "pi:GetResourceMetrics",
                "pi:DescribeDimensionKeys"
            ],
            "Resource": "*"
        },
        {
          "Sid": "CloudWatchLogsFilterLogEventsAccess",
          "Effect": "Allow",
          "Action": [
              "logs:FilterLogEvents"
          ],
          "Resource": "arn:aws:logs:*:*:log-group:*",
          "Condition": {
              "StringEquals": {
                  "aws:ResourceTag/DevOps-Guru-Analysis": "true"
              }
          }
        }
    ]
}
```

AmazonDevOpsGuruReadOnlyAccess

AmazonDevOpsGuruReadOnlyAccess— 授予對 DevOps Guru 和其他 AWS 服務中相關資源的唯讀存取權。將此政策套用至您想要授予檢視見解的能力，但不能對 DevOps Guru 的分析涵蓋範圍界限、Amazon SNS 主題或 Systems Manager OpsCenter 整合進行任何更新的使用者。

此原AmazonDevOpsGuruReadOnlyAccess則包含下列陳述式。

```
{
"Version": "2012-10-17",
"Statement": [
    {
        "Sid": "DevOpsGuruReadOnlyAccess",
        "Effect": "Allow",
        "Action": [
            "devops-guru:DescribeAccountHealth",
            "devops-guru:DescribeAccountOverview",
            "devops-guru:DescribeAnomaly",
            "devops-guru:DescribeEventSourcesConfig",
            "devops-guru:DescribeFeedback",
            "devops-guru:DescribeInsight",
            "devops-guru:DescribeResourceCollectionHealth",
            "devops-guru:DescribeServiceIntegration",
            "devops-guru:GetCostEstimation",
            "devops-guru:GetResourceCollection",
            "devops-guru:ListAnomaliesForInsight",
            "devops-guru:ListEvents",
            "devops-guru:ListInsights",
            "devops-guru:ListAnomalousLogGroups",
            "devops-guru:ListMonitoredResources",
            "devops-guru:ListNotificationChannels",
            "devops-guru:ListRecommendations",
            "devops-guru:SearchInsights",
            "devops-guru:StartCostEstimation"
        ],
        "Resource": "*"
    },
    {
        "Sid": "CloudFormationListStacksAccess",
        "Effect": "Allow",
        "Action": [
            "cloudformation:DescribeStacks",
```

```
                "cloudformation:ListStacks"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetRole"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/devops-
guru.amazonaws.com/AWSServiceRoleForDevOpsGuru"
        },
        {
            "Sid": "CloudWatchGetMetricDataAccess",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:GetMetricData"
            ],
            "Resource": "*"
        },
        {
            "Sid": "RDSDescribeDBInstancesAccess",
            "Effect": "Allow",
            "Action": [
                "rds:DescribeDBInstances"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SnsListTopicsAccess",
            "Effect": "Allow",
            "Action": [
                "sns:ListTopics",
                "sns:ListSubscriptionsByTopic"
            ],
            "Resource": "*"
        },
        {
          "Sid": "CloudWatchLogsFilterLogEventsAccess",
          "Effect": "Allow",
          "Action": [
              "logs:FilterLogEvents"
          ],
          "Resource": "arn:aws:logs:*:*:log-group:*",
```

```
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/DevOps-Guru-Analysis": "true"
                }
            }
        }
    ]
}
```

AmazonDevOpsGuruOrganizationsAccess

AmazonDevOpsGuruOrganizationsAccess— 可讓組 Organizations 管理員存取組織內的 DevOps Guru 多帳戶檢視。將此原則套用至您要授與組織內 DevOps Guru 完整存取權的組織管理員層級使用者。您可以在組織的管理帳戶和 DevOps Guru 委派的系統管理員帳戶中套用此原則。您可以套用AmazonDevOpsGuruReadOnlyAccess或附AmazonDevOpsGuruFullAccess加此原則，以提供 DevOps Guru 的唯讀或完整存取權。

此原AmazonDevOpsGuruOrganizationsAccess則包含下列陳述式。

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "AmazonDevOpsGuruOrganizationsAccess",
   "Effect": "Allow",
   "Action": [
    "devops-guru:DescribeOrganizationHealth",
    "devops-guru:DescribeOrganizationResourceCollectionHealth",
    "devops-guru:DescribeOrganizationOverview",
    "devops-guru:ListOrganizationInsights",
    "devops-guru:SearchOrganizationInsights"
   ],
   "Resource": "*"
  },
  {
   "Sid": "OrganizationsDataAccess",
   "Effect": "Allow",
   "Action": [
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "organizations:ListAWSServiceAccessForOrganization",
    "organizations:ListAccounts",
    "organizations:ListChildren",
```

```
     "organizations:ListOrganizationalUnitsForParent",
     "organizations:ListRoots"
    ],
    "Resource": "arn:aws:organizations::*:"
   },
   {
    "Sid": "OrganizationsAdminDataAccess",
    "Effect": "Allow",
    "Action": [
     "organizations:DeregisterDelegatedAdministrator",
     "organizations:RegisterDelegatedAdministrator",
     "organizations:ListDelegatedAdministrators",
     "organizations:EnableAWSServiceAccess",
     "organizations:DisableAWSServiceAccess"
    ],
    "Resource": "*",
    "Condition": {
     "StringEquals": {
      "organizations:ServicePrincipal": [
       "devops-guru.amazonaws.com"
      ]
     }
    }
   }
  ]
}
```

針 DevOps對 Guru 使用服務連結角色

Amazon DevOps 大師使用 AWS Identity and Access Management (IAM) 服務連結角色。服務連結角色是直接連結至 DevOps Guru 的唯一 IAM 角色類型。服務連結角色由 DevOps Guru 預先定義 AWS CloudTrail，並包含服務代表您呼叫 Amazon CloudWatch 和 AWS Organizations 所需的所有許可。AWS CodeDeploy AWS X-Ray

服務連結角色可讓您輕鬆設定 DevOps Guru，因為您不必手動新增必要的權限。 DevOpsGuru 定義了其服務鏈接角色的權限，除非另有定義，否則只有 DevOps Guru 可以擔任其角色。定義的許可包括信任政策和許可政策，且該許可政策無法附加至其他 IAM 實體。

您必須先刪除角色的相關資源，才能刪除服務連結角色。這樣可以保護您的 DevOps Guru 資源，因為您無法無意中刪除訪問資源的權限。

Guru 的 DevOps服務連結角色權限

DevOpsGuru 使用名為AWSServiceRoleForDevOpsGuru的服務連結角色。這是具有範圍權限的 AWS 受管理策略， DevOpsGuru 需要在您的帳戶中運行。

AWSServiceRoleForDevOpsGuru 服務連結角色信任下列服務來擔任此角色：

- devops-guru.amazonaws.com

角色權限原則AmazonDevOpsGuruServiceRolePolicy可讓 DevOps Guru 在指定的資源上完成下列動作。

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "autoscaling:DescribeAutoScalingGroups",
    "cloudtrail:LookupEvents",
    "cloudwatch:GetMetricData",
    "cloudwatch:ListMetrics",
    "cloudwatch:DescribeAnomalyDetectors",
    "cloudwatch:DescribeAlarms",
    "cloudwatch:ListDashboards",
    "cloudwatch:GetDashboard",
    "cloudformation:GetTemplate",
    "cloudformation:ListStacks",
    "cloudformation:ListStackResources",
    "cloudformation:DescribeStacks",
    "cloudformation:ListImports",
    "codedeploy:BatchGetDeployments",
    "codedeploy:GetDeploymentGroup",
    "codedeploy:ListDeployments",
    "config:DescribeConfigurationRecorderStatus",
    "config:GetResourceConfigHistory",
    "events:ListRuleNamesByTarget",
    "xray:GetServiceGraph",
    "organizations:ListRoots",
    "organizations:ListChildren",
    "organizations:ListDelegatedAdministrators",
    "pi:GetResourceMetrics",
```

```
        "tag:GetResources",
        "lambda:GetFunction",
        "lambda:GetFunctionConcurrency",
        "lambda:GetAccountSettings",
        "lambda:ListProvisionedConcurrencyConfigs",
        "lambda:ListAliases",
        "lambda:ListEventSourceMappings",
        "lambda:GetPolicy",
        "ec2:DescribeSubnets",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "sqs:GetQueueAttributes",
        "kinesis:DescribeStream",
        "kinesis:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeStream",
        "dynamodb:ListStreams",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "rds:DescribeOptionGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBInstanceAutomatedBackups",
        "rds:DescribeAccountAttributes",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "s3:GetBucketNotification",
        "s3:GetBucketPolicy",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketTagging",
        "s3:GetBucketWebsite",
        "s3:GetIntelligentTieringConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetReplicationConfiguration",
        "s3:ListAllMyBuckets",
        "s3:ListStorageLensConfigurations",
        "servicequotas:GetServiceQuota",
        "servicequotas:ListRequestedServiceQuotaChangeHistory",
        "servicequotas:ListServiceQuotas"
    ],
    "Resource": "*"
```

```
  },
  {
   "Sid": "AllowPutTargetsOnASpecificRule",
   "Effect": "Allow",
   "Action": [
    "events:PutTargets",
    "events:PutRule"
   ],
   "Resource": "arn:aws:events:*:*:rule/DevOps-Guru-managed-*"
  },
  {
   "Sid": "AllowCreateOpsItem",
   "Effect": "Allow",
   "Action": [
    "ssm:CreateOpsItem"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AllowAddTagsToOpsItem",
   "Effect": "Allow",
   "Action": [
    "ssm:AddTagsToResource"
   ],
   "Resource": "arn:aws:ssm:*:*:opsitem/*"
  },
  {
   "Sid": "AllowAccessOpsItem",
   "Effect": "Allow",
   "Action": [
    "ssm:GetOpsItem",
    "ssm:UpdateOpsItem"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "aws:ResourceTag/DevOps-GuruInsightSsmOpsItemRelated": "true"
    }
   }
  },
  {
   "Sid": "AllowCreateManagedRule",
   "Effect": "Allow",
   "Action": "events:PutRule",
```

```
    "Resource": "arn:aws:events:*:*:rule/DevOpsGuruManagedRule*"
   },
   {
    "Sid": "AllowAccessManagedRule",
    "Effect": "Allow",
    "Action": [
     "events:DescribeRule",
     "events:ListTargetsByRule"
    ],
    "Resource": "arn:aws:events:*:*:rule/DevOpsGuruManagedRule*"
   },
   {
    "Sid": "AllowOtherOperationsOnManagedRule",
    "Effect": "Allow",
    "Action": [
     "events:DeleteRule",
     "events:EnableRule",
     "events:DisableRule",
     "events:PutTargets",
     "events:RemoveTargets"
    ],
    "Resource": "arn:aws:events:*:*:rule/DevOpsGuruManagedRule*",
    "Condition": {
     "StringEquals": {
      "events:ManagedBy": "devops-guru.amazonaws.com"
     }
    }
   },
   {
    "Sid": "AllowTagBasedFilterLogEvents",
    "Effect": "Allow",
    "Action": [
     "logs:FilterLogEvents"
    ],
    "Resource": "arn:aws:logs:*:*:log-group:*",
    "Condition": {
     "StringEquals": {
      "aws:ResourceTag/DevOps-Guru-Analysis": "true"
     }
    }
   },
   {
    "Sid": "AllowAPIGatewayGetIntegrations",
    "Effect": "Allow",
```

```
    "Action": "apigateway:GET",
    "Resource": [
     "arn:aws:apigateway:*::/restapis/??????????",
     "arn:aws:apigateway:*::/restapis/*/resources",
     "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration"
    ]
   }
  ]
}
```

為 DevOps Guru 建立服務連結角色

您不需要手動建立一個服務連結角色。當您在 AWS Management Console、或 AWS API 中建立深入解析時 AWS CLI， DevOpsGuru 會為您建立服務連結角色。

> **Important**
>
> 如果您在使用此角色支援的功能的其他服務中完成動作，則此服務連結角色可能會出現在您的帳戶中；例如，如果您從 AWS CodeCommit中將 DevOps Guru 新增至儲存庫，則該角色可能會出現。

編輯 Guru 的服務連結角色 DevOps

DevOpsGuru 不允許您編輯`AWSServiceRoleForDevOpsGuru`服務連結角色。因為有各種實體可能會參考服務連結角色，所以您無法在建立角色之後變更角色名稱。然而，您可使用 IAM 來編輯角色描述。如需更多資訊，請參閱 IAM 使用者指南中的編輯服務連結角色。

刪除 Guru 的服務連結角色 DevOps

若您不再使用需要服務連結角色的功能或服務，我們建議您刪除該角色。如此一來，您就沒有未主動監控或維護的未使用實體。但是，您必須先取消與所有儲存庫的關聯，才能手動刪除它。

> **Note**
>
> 當您嘗試刪除資源時，如果 DevOps Guru 服務正在使用此角色，則刪除可能會失敗。若此情況發生，請等待數分鐘後並再次嘗試操作。

使用 IAM 手動刪除服務連結角色

使用 IAM 主控台或 AWS API 刪除AWSServiceRoleForDevOpsGuru服務連結角色。 AWS CLI如需詳細資訊，請參閱《IAM 使用者指南》中的刪除服務連結角色。

Amazon DevOps 大師許可參考

您可以在 DevOps Guru 政策中使用 AWS寬條件金鑰來表示條件。如需清單，請參閱 IAM 使用者指南中的 IAM JSON 政策元素參考。

您可以在政策的 Action 欄位中指定動作。若要指定動作，請使用 devops-guru: 字首，後面接著 API 操作名稱 (例如 devops-guru:SearchInsights 和 devops-guru:ListAnomalies)。若要在單一陳述式中指定多個動作，請用逗號加以分隔 (例如 "Action": ["devops-guru:SearchInsights", "devops-guru:ListAnomalies"])。

使用萬用字元

您可以在政策Resource欄位中指定 Amazon 資源名稱 (ARN) (含或不含萬用字元 (*) 作為資源值。您可以使用萬用字元指定多個動作或資源。例如，devops-guru:*指定所有 DevOps Guru 動作，並devops-guru:List*指定以該字開頭的所有 DevOps Guru 動作List。下列範例會參考具有以通用唯一識別碼 (UUID) 開頭的所有見解。12345

```
arn:aws:devops-guru:us-east-2:123456789012:insight:12345*
```

當您設定使用身分驗證和撰寫可附加至 IAM 身分 (身分型政策) 的許可政策時，您可以使用下表做為參考。

DevOps大師 API 操作和操作所需的權限

AddNotificationChannel

動作：devops-guru:AddNotificationChannel

需要從 DevOps Guru 添加通知通道。當 DevOps Guru 產生包含有關如何改善操作資訊的見解時，會使用通知通道通知您。

資源：*

RemoveNotificationChannel

devops-guru:RemoveNotificationChannel

需要從 DevOps Guru 中刪除通知通道。當 DevOps Guru 產生包含有關如何改善操作資訊的見解時，會使用通知通道通知您。

資源：*

ListNotificationChannels

動作：devops-guru:ListNotificationChannels

需要返回為 DevOps Guru 配置的通知通道列表。每個通知通道都用於在 DevOps Guru 產生包含有關如何改進操作的信息的見解時通知您。支援的一種通知類型是 Amazon 簡易通知服務。

資源：*

UpdateResourceCollectionFilter

動作：devops-guru:UpdateResourceCollectionFilter

需要更新堆疊清單，這些 AWS CloudFormation 堆疊清單用於指定 DevOps Guru 分析您帳戶中的哪些 AWS 資源。分析會產生包含建議、作業指標和作業事件的見解，讓您可以用來改善營運效能。此方法也會建立您使用所需的 IAM 角色 CodeGuru OpsAdvisor。

資源：*

GetResourceCollectionFilter

動作：devops-guru:GetResourceCollectionFilter

需要返回堆棧列表，這些 AWS CloudFormation 堆棧用於指定 DevOps Guru 分析您帳戶中的哪些 AWS 資源。分析會產生包含建議、作業指標和作業事件的見解，讓您可以用來改善營運效能。

資源：*

ListInsights

動作：devops-guru:ListInsights

傳回 AWS 帳戶中的深入解析清單所需。您可以指定依據開始時間、狀態 (ongoing或any) 和類型 (reactive或predictive) 傳回的深入解析。

資源：*

DescribeInsight

動作：devops-guru:DescribeInsight

必須傳回您使用其 ID 指定之深入解析的詳細資料。

資源：*

SearchInsights

動作：devops-guru:SearchInsights

傳回 AWS 帳戶中的深入解析清單所需。您可以指定依據開始時間、篩選器和類型 (reactive或predictive) 傳回的深入解析。

資源：*

ListAnomalies

動作：devops-guru:ListAnomalies

傳回屬於您使用其 ID 指定之洞察的異常清單所需。

資源：*

DescribeAnomaly

動作：devops-guru:DescribeAnomaly

必須傳回您使用其 ID 指定之異常的詳細資料。

資源：*

ListEvents

動作：devops-guru:ListEvents

傳回由 DevOps Guru 評估之資源所發出的事件清單所需。您可以使用篩選器來指定要傳回的事件。

資源：*

ListRecommendations

動作：devops-guru:ListRecommendations

傳回指定見解建議的清單所需。每個建議都包含量度清單，以及與建議相關的事件清單。

資源：*

DescribeAccountHealth

動作：devops-guru:DescribeAccountHealth

需要傳回開放式反應式見解的數量、開放式預測見解的數量，以及您 AWS 帳戶中分析的指標數量。使用這些數字來衡量您 AWS 帳戶中操作的健康狀態。

資源：*

DescribeAccountOverview

動作：devops-guru:DescribeAccountOverview

必須傳回某個時間範圍內發生的下列事項：建立的開放式反應式深入解析數量、建立的開放式預測見解數量，以及所有已關閉之被動式深入解析的平均復原時間 (MTTR)。

資源：*

DescribeResourceCollectionHealthOverview

動作：devops-guru:DescribeResourceCollectionHealthOverview

傳回 Guru 中 DevOps指定之每個 AWS CloudFormation 堆疊之所有深入解析的開放式預測見解、開放式反應式深入解析和平均復原時間 (MTTR) 數量所需。

資源：*

DescribeIntegratedService

動作：devops-guru:DescribeIntegratedService

必須傳回可與 DevOps Guru 整合之服務的整合狀態。可以與 DevOps Guru 集成的一個服務是 AWS Systems Manager，可用於 OpsItem 為每個生成的見解創建一個。

資源：*

UpdateIntegratedServiceConfig

動作：devops-guru:UpdateIntegratedServiceConfig

需要啟用或停用與可與 DevOps Guru 整合的服務整合。可以與 DevOps Guru 集成的一個服務是 Systems Manager，可用於 OpsItem 為每個生成的見解創建一個。

資源：*

Amazon SNS 主題的許可

只有當您想要將 Amazon DevOps Guru 設定為將通知傳遞給另一個 AWS 帳戶擁有的 Amazon SNS 主題時，才使用本主題中的資訊。

若要讓 DevOps Guru 將通知傳送到不同帳戶擁有的 Amazon SNS 主題，您必須將政策附加到 Amazon SNS 主題，以授予 DevOps Guru 傳送通知給該主題的權限。如果您將 DevOps Guru 設定為 DevOps向您使用 Guru 的相同帳戶所擁有的 Amazon SNS 主題傳遞通知，則 DevOps Guru 會為您新增政策至主題。

在您附加原則以設定其他帳戶中 Amazon SNS 主題的許可後，您可以在 DevOps Guru 中新增 Amazon SNS 主題。您也可以使用通知管道更新 Amazon SNS 政策，以使其更安全。

> **Note**
>
> DevOpsGuru 目前僅支持同一地區的跨帳戶訪問。

主題

在另一個帳戶中設定 Amazon SNS 主題的許可

將許可新增為 IAM 角色

若要在使用 IAM 角色登入後使用其他帳戶的 Amazon SNS 主題，您必須將政策附加到要使用的 Amazon SNS 主題。若要在使用 IAM 角色時從另一個帳戶將政策附加到 Amazon SNS 主題，您需要具有該帳戶資源的下列許可，做為 IAM 角色的一部分：

- SNS: CreateTopic
- SNS: GetTopicAttributes
- SNS: SetTopicAttributes
- sns:Publish

將下列政策附加到您要使用的 Amazon SNS 主題。對於`Resource`密鑰，*`topic-owner-account-id`*是主題所有者的帳戶 ID，*`topic-sender-account-id`*是設置 DevOps Guru 的用戶的帳戶 ID，並且*`devops-guru-role`*是涉及的個別用戶的 IAM 角色。您必須以適當的值取代*`## ID`* (例如，`us-west-2`) 和。*`my-topic-name`*

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "EnableDevOpsGuruServicePrincipal",
            "Action": "sns:Publish",
            "Effect": "Allow",
            "Resource": "arn:aws:sns:region-id:topic-owner-account-id:my-topic-name",
            "Principal": {
                "Service": "region-id.devops-guru.amazonaws.com"
            },
            "Condition": {
                "StringEquals": {
                    "AWS:SourceAccount": "topic-sender-account-id"
                }
            }
        },
        {
            "Sid": "EnableAccountPrincipal",
            "Action": "sns:Publish",
            "Effect": "Allow",
            "Resource": "arn:aws:sns:region-id:topic-owner-account-id:my-topic-name",
            "Principal": {
                "AWS": ["arn:aws:iam::topic-sender-account-id:role/devops-guru-role"]
            }
        }
    ]
}
```

以 IAM 使用者身分新增許可

若要使用其他帳戶中的 Amazon SNS 主題做為 IAM 使用者，請將下列政策附加到您要使用的 Amazon SNS 主題。對於Resource金鑰，*topic-owner-account-id*是主題擁有者的帳戶 ID、*topic-sender-account-id*設定 DevOps Guru 的使用者帳戶 ID，以及*devops-guru-user-name*是涉及的個別 IAM 使用者。您必須以適當的值取代*## ID* (例如，us-west-2) 和。*my-topic-name*

> **Note**
>
> 建議您盡可能依賴暫時憑證，而不是擁有建立長期憑證 (例如密碼和存取金鑰) 的 IAM 使用者。如需 IAM 中最佳實務的相關資訊，請參閱 IAM 使用者指南中的 IAM 安全最佳實務。

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "EnableDevOpsGuruServicePrincipal",
            "Action": "sns:Publish",
            "Effect": "Allow",
            "Resource": "arn:aws:sns:region-id:topic-owner-account-id:my-topic-name",
            "Principal": {
                "Service": "region-id.devops-guru.amazonaws.com"
            },
            "Condition": {
                "StringEquals": {
                    "AWS:SourceAccount": "topic-sender-account-id"
                }
            }
        },
        {
            "Sid": "EnableAccountPrincipal",
            "Action": "sns:Publish",
            "Effect": "Allow",
            "Resource": "arn:aws:sns:region-id:topic-owner-account-id:my-topic-name",
            "Principal": {
                "AWS": ["arn:aws:iam::topic-sender-account-id:user/devops-guru-user-
name"]
            }
        }
    ]
}
```

從另一個帳戶添加 Amazon SNS 主題

在其他帳戶中設定 Amazon SNS 主題的許可後，您可以將該 Amazon SNS 主題新增至您的 DevOps Guru 通知設定。您可以使用 AWS CLI 或 DevOps Guru 主控台新增 Amazon SNS 主題。

- 使用主控台時，您必須選取 [使用 SNS 主題 ARN] 選項來指定現有主題，才能使用其他帳戶的主題。
- 使用 AWS CLI 作業時 add-notification-channel，您必須在`NotificationChannelConfig`物件`TopicArn`內指定。

使用主控台從其他帳戶新增 Amazon SNS 主題

1. 在 https://console.aws.amazon.com/devops-guru/ 打開 Amazon DevOps 大師控制台。
2. 開啟功能窗格，然後選擇 [設定]。
3. 前往「通知」區段，然後選擇 「編輯」。
4. 選擇新增 SNS 主題。
5. 選擇「使用 SNS 主題 ARN」以指定現有主題。
6. 輸入您要使用的 Amazon SNS 主題的 ARN。您應該已經為此主題設定權限，方法是將原則附加至該主題。
7. (選擇性) 選擇 [通知設定] 以編輯通知頻率設定。
8. 選擇儲存。

將 Amazon SNS 主題新增至通知設定後， DevOpsGuru 會使用該主題通知您重要事件，例如建立新的深入分析時。

使用通知管道更新您的 Amazon SNS 政策 (建議使用)

新增主題後，建議您僅為包含您主題的 DevOps Guru 通知通道指定權限，以使原則更安全。

使用通知管道更新您的 Amazon SNS 主題政策 (建議使用)

1. 在您要從中傳送通知的帳戶中執行 `list-notification-channels` DevOps Guru AWS CLI 命令。

```
aws devops-guru list-notification-channels
```

2. 在`list-notification-channels`回應中，記下包含您的 Amazon SNS 主題 ARN 的通道識別碼。通道識別碼是一個 GUID。

   例如，在下列回應中，具有 ARN `arn:aws:sns:`*region-id*`:`*111122223333*`:`*topic-name* 之主題的通道識別碼為 *e89be5f7-989d-4c4c-b1fe-e7145037e531*

```
{
  "Channels": [
    {
      "Id": "e89be5f7-989d-4c4c-b1fe-e7145037e531",
      "Config": {
      "Sns": {
```

```
            "TopicArn": "arn:aws:sns:region-id:111122223333:topic-name"
          },
        "Filters": {
            "MessageTypes": ["CLOSED_INSIGHT", "NEW_INSIGHT", "SEVERITY_UPGRADED"],
            "Severities": ["HIGH", "MEDIUM"]
          }
        }
      }
    ]
}
```

3. 使用中的主題擁有者 ID 移至您在其他帳戶中建立的策略the section called “在另一個帳戶中設定 Amazon SNS 主題的許可”。在原則Condition陳述式中，新增指定SourceArn. ARN 包含您的地區 ID (例如us-east-1)、主題寄件者的 AWS 帳號，以及您記下的頻道 ID。

   您更新的Condition陳述式如下所示。

```
"Condition" : {
  "StringEquals" : {
    "AWS:SourceArn": "arn:aws:devops-guru:us-
east-1:111122223333:channel/e89be5f7-989d-4c4c-b1fe-e7145037e531",
    "AWS:SourceAccount": "111122223333"
   }
 }
```

如果AddNotificationChannel無法新增 SNS 主題，請檢查您的 IAM 政策是否具有下列許可。

```
{
     "Version": "2012-10-17",
     "Statement": [{
           "Sid": "DevOpsGuruTopicPermissions",
           "Effect": "Allow",
           "Action": [
                 "sns:CreateTopic",
                 "sns:GetTopicAttributes",
                 "sns:SetTopicAttributes",
                 "sns:Publish"
           ],
           "Resource": "arn:aws:sns:region-id:account-id:my-topic-name"
     }]
}
```

AWS KMS加密 Amazon SNS 主題的許可

您指定的 Amazon SNS 主題可能已由加密 AWS Key Management Service。若要允許 DevOps Guru 使用加密主題，您必須先建立， AWS KMS key 然後將下列陳述式新增至 KMS 金鑰的原則。如需詳細資訊，請參閱使用 AWS KMS 加密發佈到 Amazon SNS 的訊息、AWS KMS 使用者指南中的金鑰識別碼 (KeyId) 和 Amazon 簡單通知服務開發人員指南中的資料加密。

```
{
  "Version": "2012-10-17",
  "Id": "your-kms-key-policy",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "region-id.devops-guru.amazonaws.com"
      },
      "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
      ],
      "Resource": "*"
    }
  ]
}
```

> **Note**
>
> DevOpsGuru 目前支援在單一帳戶中使用的加密主題。目前不支援跨多個帳戶使用加密主題。

疑難排解 Amazon DevOps Guru 身分和存取權

使用下列資訊可協助您診斷並修正使用 DevOps Guru 和 IAM 時可能會遇到的常見問題。

主題

- 我沒有授權在 DevOps Guru 中執行操作
- 我想讓使用者以程式設計方式存取
- 我沒有授權執行 iam：PassRole

- 我想允許我 AWS 帳戶以外的人訪問我的 DevOps Guru 資源

我沒有授權在 DevOps Guru 中執行操作

如果 AWS Management Console 告訴您您沒有執行動作的授權，則您必須聯絡您的管理員以尋求協助。

當使用者mateojackson嘗試使用主控台來檢視虛構*my-example-widget*資源的詳細資料，但沒有虛構的aws:*GetWidget*權限時，就會發生下列範例錯誤。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 aws:GetWidget on resource: my-example-widget
```

在此情況下，Mateo 會請求管理員更新他的政策，允許他使用 *my-example-widget* 動作存取 aws:*GetWidget* 資源。

我想讓使用者以程式設計方式存取

如果使用者想要與 AWS 之外的 AWS Management Console. 授與程式設計存 AWS取權的方式取決於正在存取的使用者類型。

若要授與使用者程式設計存取權，請選擇下列其中一個選項。

哪個使用者需要程式設計存取權？	到	By
人力身分 (IAM Identity Center 中管理的使用者)	使用臨時登入資料來簽署對 AWS CLI、 AWS SDK 或 AWS API 的程式設計要求。	請依照您要使用的介面所提供的指示操作。 • 如需詳細資訊 AWS CLI，請參閱《使 AWS CLI 用AWS Command Line Interface者指南》 AWS IAM Identity Center中的〈配置使用〉。 • 如需 AWS SDK、工具和 AWS API，請參閱 AWS SDK 和工具參考指南中的 IAM 身分中心身分驗證。

哪個使用者需要程式設計存取權？	到	By
IAM	使用臨時登入資料來簽署對 AWS CLI、 AWS SDK 或 AWS API 的程式設計要求。	遵循《IAM 使用者指南》中的〈將臨時登入資料搭配 AWS 資源使用〉中的指示
IAM	(不建議使用) 使用長期認證來簽署對 AWS CLI、 AWS SDK 或 AWS API 的程式設計要求。	請依照您要使用的介面所提供的指示操作。 • 如需相關資訊 AWS CLI，請參閱使用指南中的使用 IAM 使用者登入資料進行驗證。AWS Command Line Interface • 對於 AWS SDK 和工具，請參閱 AWS SDK 和工具參考指南中的使用長期憑據進行身份驗證。 • 如需 AWS API，請參閱 IAM 使用者指南中的管理 IAM 使用者的存取金鑰。

我沒有授權執行 iam：PassRole

如果您收到未獲授權執行`iam:PassRole`動作的錯誤訊息，您必須更新原則，才能將角色傳遞給 DevOps Guru。

有些 AWS 服務 允許您將現有角色傳遞給該服務，而不是建立新的服務角色或服務連結角色。如需執行此作業，您必須擁有將角色傳遞至該服務的許可。

當名為的 IAM 使用者`marymajor`嘗試使用主控台在 DevOps Guru 中執行動作時，就會發生下列範例錯誤。但是，動作請求服務具備服務角色授予的許可。Mary 沒有將角色傳遞至該服務的許可。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

在這種情況下，Mary 的政策必須更新，允許她執行 `iam:PassRole` 動作。

如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的簽署憑證。

我想允許我 AWS 帳戶以外的人訪問我的 DevOps Guru 資源

您可以建立一個角色，讓其他帳戶中的使用者或您組織外部的人員存取您的資源。您可以指定要允許哪些信任物件取得該角色。針對支援基於資源的政策或存取控制清單 (ACL) 的服務，您可以使用那些政策來授予人員存取您的資源的許可。

如需進一步了解，請參閱以下內容：

- 若要瞭解 DevOps Guru 是否支援這些功能，請參閱Amazon DevOps 大師如何與 IAM 合作。
- 若要了解如何提供對您所擁有資源 AWS 帳戶 的存取權，請參閱 IAM 使用者指南中您擁有的另一 AWS 帳戶 個 IAM 使用者提供存取權限。
- 若要了解如何將資源存取權提供給第三方 AWS 帳戶，請參閱 IAM 使用者指南中的提供第三方 AWS 帳戶 擁有的存取權。
- 若要了解如何透過聯合身分提供存取權，請參閱 IAM 使用者指南中的將存取權提供給在外部進行身分驗證的使用者 (聯合身分)。
- 若要了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱 IAM 使用者指南中的 IAM 角色與資源型政策的差異。

記錄和監控 DevOps大師

監控是維持 DevOps Guru 和其他 AWS 解決方案的可靠性、可用性和效能的重要組成部分。AWS 提供下列監控工具來觀看 DevOps Guru、在發生錯誤時報告，並在適當時採取自動動作：

- Amazon 會即時 CloudWatch監控您的 AWS 資源和執行 AWS 的應用程式。您可以收集和追蹤指標、建立自訂儀板表，以及設定警示，在特定指標達到您指定的閾值時通知您或採取動作。例如，您可以 CloudWatch 追蹤 Amazon EC2 執行個體的 CPU 使用率或其他指標，並在需要時自動啟動新執行個體。如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南。
- AWS CloudTrail擷取您帳戶或代表您 AWS 帳戶發出的 API 呼叫和相關事件，並將日誌檔傳送到您指定的 Amazon S3 儲存貯體。您可以找出哪些使用者和帳戶呼叫 AWS、發出呼叫的來源 IP 地址，以及呼叫的發生時間。如需詳細資訊，請參閱 AWS CloudTrail 使用者指南。

主題

- 監控 DevOps大師與 Amazon CloudWatch
- 記錄 Amazon DevOps 大師 API 調用 AWS CloudTrail

監控 DevOps大師與 Amazon CloudWatch

您可以使用監視 DevOps Guru CloudWatch，它會收集原始數據並將其處理為可讀的近實時指標。這些統計資料會保留 15 個月，以便您存取歷史資訊，並更清楚 Web 應用程式或服務的執行效能。您也可以設定警報監看特定閾值，在達到閾值發出通知或採取動作。如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南。

對於 DevOps Guru，您可以跟踪 G DevOps uru 使用情況的見解和指標的指標。您可能需要留意大量的建立項目，Insights以協助您判斷作業解決方案是否發生異常行為。或者，您可能希望觀察 DevOps Guru 的使用情況以幫助跟踪您的成本。

DevOpsGuru 服務會在AWS/DevOps-Guru命名空間中報告下列度量。

主題

- 洞察指標
- DevOps大師使用量度

洞察指標

您可以使 CloudWatch 用追蹤指標，以顯示 AWS 帳戶中建立了多少見解。您可以指定要追蹤的Type維度proactive或reactive深入解析。如果要追蹤所有見解，請勿指定維度。

指標

指標	描述
Insight	在帳戶中建立的見解數 AWS 目。 有效尺寸：Type 有效統計資料：樣本計數、總和 單位：計數

DevOpsGuru Insight 量度支援下列維度。

Dimensions (尺寸)

維度	描述
Type	這是洞察力的類型。如果您要追蹤所有深入解析，請勿指定Insights量度的維度。有效值為：proactive 、reactive。

DevOps大師使用量度

您可以使用 CloudWatch 來跟踪您的 Amazon DevOps 大師使用情況。

指標

指標	描述
CallCount	以下其中一種 DevOps Guru 方法進行的呼叫次數。 • ListInsights • ListAnomaliesForInsight • ListRecommendations • ListEvents • SearchInsights • DescribeInsight • DescribeAnomaly 有效尺寸:Service、Class、Type、Resource 有效統計資料：樣本計數、總和 單位：計數

DevOpsGuru 使用量度支援下列維度。

Dimensions (尺寸)

維度	描述
`Service`	這是包含資源的 AWS 服務名稱。例如，對於 DevOps Guru，這個值是`DevOps-Guru` 。
`Class`	這是要追蹤的資源類別。 DevOpsGuru 將此維度與值一起使用`None`。
`Type`	這是要追蹤的資源類型。 DevOpsGuru 將此維度與值一起使用`API`。
`Resource`	這是大 DevOps師操作的名稱。有效值為：`ListInsights` 、`ListAnomaliesForInsight` 、`ListRecommendations` 、`ListEvents` 、、`SearchInsights` 、`DescribeInsight` 、`DescribeAnomaly` 。

記錄 Amazon DevOps 大師 API 調用 AWS CloudTrail

Amazon DevOps Guru 與這項服務整合在一起 AWS CloudTrail，可提供 G DevOps uru 中使用者、角色或 AWS 服務所採取的動作記錄。 CloudTrail 捕獲DevOps大師的 API 調用作為事件。擷取的呼叫包括來自 DevOps Guru 主控台的呼叫，以及對 DevOps Guru API 作業的程式碼呼叫。如果您建立追蹤，您可以啟用持續交付 CloudTrail 事件到 Amazon S3 儲存貯體，包括 DevOps Guru 的事件。如果您未設定追蹤，您仍然可以在 [事件歷程記錄] 中檢視 CloudTrail 主控台中最近的事件。使用收集的信息 CloudTrail，您可以確定向 DevOps Guru 提出的請求，提出請求的 IP 地址，提出請求的人員，提出請求的時間以及其他詳細信息。

若要進一步了解 CloudTrail，請參閱使AWS CloudTrail 用者指南。

DevOps大師信息 CloudTrail

CloudTrail 在您創建 AWS 帳戶時，您的帳戶已啟用。當活動在 DevOps Guru 中發生時，該活動會與事件歷史記錄中的其他 AWS 服務 CloudTrail 事件一起記錄在事件中。您可以在帳戶中查看，搜索和下載最近的事 AWS 件。如需詳細資訊，請參閱使用 CloudTrail 事件歷程記錄檢視事件。

如需 AWS 帳戶中持續記錄事件 (包括 DevOps Guru 的活動)，請建立追蹤。追蹤可 CloudTrail 將日誌檔交付到 Amazon S3 儲存貯體。根據預設，當您在主控台建立追蹤記錄時，追蹤記錄會套用到所有 AWS 區域。追蹤記錄來自 AWS 分區中所有區域的事件，並將日誌檔傳送到您指定的 Amazon S3 儲存貯體。此外，您還可以設定其他 AWS 服務，以進一步分析 CloudTrail 記錄中收集的事件資料並採取行動。如需詳細資訊，請參閱下列內容：

- 建立追蹤的概觀
- CloudTrail 支援的服務與整合
- 設定 Amazon SNS 通知 CloudTrail
- 從多個區域接收 CloudTrail 日誌文件並從多個帳戶接收 CloudTrail 日誌文件

DevOpsGuru 支持將其所有操作記錄為 CloudTrail 日誌文件中的事件。如需詳細資訊，請參閱 DevOpsGuru API 參考中的動作。

每一筆事件或日誌專案都會包含產生請求者的資訊。身分資訊可協助您判斷下列事項：

- 該請求是否使用根或使用者憑證提出。
- 提出該請求時，是否使用了特定角色或聯合身分使用者的暫時安全憑證。
- 請求是否由其他 AWS 服務提出。

如需詳細資訊，請參閱CloudTrail 使 userIdentity 元素。

了解 DevOps Guru 日誌文件條目

追蹤是一種組態，可讓事件以日誌檔的形式傳遞到您指定的 Amazon S3 儲存貯體。 CloudTrail 記錄檔包含一或多個記錄項目。事件代表來自任何來源的單一請求，包括有關請求的操作，動作的日期和時間，請求參數等信息。 CloudTrail 日誌文件不是公共 API 調用的有序堆棧跟踪，因此它們不會以任何特定順序顯示。

下列範例顯示示範`UpdateResourceCollection`動作的 CloudTrail 記錄項目。

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AAAAAAAAAEXAMPLE:TestSession",
    "arn": "arn:aws:sts::123456789012:assumed-role/TestRole/TestSession",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
```

```
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/TestRole",
        "accountId": "123456789012",
        "userName": "sample-user-name"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2020-12-03T15:29:51Z"
      }
    }
  },
  "eventTime": "2020-12-01T16:14:31Z",
  "eventSource": "devops-guru.amazonaws.com",
  "eventName": "UpdateResourceCollection",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "sample-ip-address",
  "userAgent": "aws-internal/3 aws-sdk-java/1.11.901
 Linux/4.9.217-0.3.ac.206.84.332.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.275-b01
 java/1.8.0_275 vendor/Oracle_Corporation",
  "requestParameters": {
    "Action": "REMOVE",
    "ResourceCollection": {
      "CloudFormation": {
        "StackNames": [
          "*"
        ]
      }
    }
  },
  "responseElements": null,
  "requestID": " cb8c167e-EXAMPLE ",
  "eventID": " e3c6f4ce-EXAMPLE ",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012"
}
```

DevOps大師和介面 VPC 端點 ()AWS PrivateLink

當您呼叫 Amazon DevOps 大師 API 時，可以使用 VPC 人雲端端點。當您使用 VPC 端點時，API 呼叫會更加安全，因為它們包含在您的 VPC 中且無法存取網際網路。如需詳細資訊，請參閱 Amazon DevOps 大師 API 參考中的動作。

您可以透過建立介面 VPC 端點，在 VPC 和 DevOps Guru 之間建立私人連線。介面端點採用這項技術 AWS PrivateLink，可讓您在沒有網際網路閘道、NAT 裝置、VPN 連線或 AWS Direct Connect 連線的情況下私有存取 DevOps Guru API。VPC 中的執行個體不需要公用 IP 位址即可與 DevOps Guru API 進行通訊。您的 VPC 和 DevOps Guru 之間的流量不會離開 Amazon 網路。

每個介面端點都是由您子網路中的一或多個彈性網路介面表示。

如需詳細資訊，請參閱 Amazon VPC 使用者指南中的介面虛擬私人雲端端點 (AWS PrivateLink)。

DevOps大師 VPC 端點的注意事項

在為 DevOps Guru 設定介面 VPC 端點之前，請務必先檢閱 Amazon VPC 使用者指南中的介面端點屬性和限制。

DevOps大師支援從您的 VPC 呼叫其所有 API 動作。

為 DevOps Guru 建立介面 VPC 端點

您可以使用 Amazon VPC 主控台或 AWS Command Line Interface (AWS CLI) 為 DevOps Guru 服務建立 VPC 端點。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的建立介面端點。

使用下列服務名稱為 DevOps Guru 建立 VPC 端點：

- com.amazonaws.*region*.devops-guru

如果您為端點啟用私有 DNS，則可以使用該區域的預設 DNS 名稱向 DevOps Guru 發出 API 要求，例如`devops-guru.us-east-1.amazonaws.com`。

如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的透過介面端點存取服務。

為 Guru 建立 VPC 端點原則 DevOps

您可以將端點政策附加到 VPC 端點，以控制對 DevOps Guru 的存取。此政策會指定下列資訊：

- 可執行動作的主體。

- 可執行的動作。
- 可供執行動作的資源。

如需詳細資訊，請參閱 Amazon VPC 使用者指南中的使用 VPC 端點控制對服務的存取。

範例： DevOpsGuru 動作的 VPC 端點原則

以下是 DevOps Guru 的端點策略示例。連接至端點時，此策略會授與所有資源上所有主體列出之 DevOps Guru 動作的存取權。

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "devops-guru:AddNotificationChannel",
            "devops-guru:ListInsights",
            "devops-guru:ListRecommendations"
         ],
         "Resource":"*"
      }
   ]
}
```

DevOpsGuru 的基礎架構安全

作為一項受管服務，Amazon DevOps Guru 受到 AWS 全球網路安全的保護。有關 AWS 安全服務以及如何 AWS 保護基礎結構的詳細資訊，請參閱AWS 雲端安全 若要使用基礎架構安全性的最佳做法來設計您的 AWS 環境，請參閱安全性支柱架構良 AWS 好的架構中的基礎結構保護。

您可以使用 AWS 已發佈的 API 呼叫透過網路存取 DevOps Guru。使用者端必須支援下列專案：

- Transport Layer Security (TLS)。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 具備完美轉送私密(PFS)的密碼套件，例如 DHE (Ephemeral Diffie-Hellman)或 ECDHE (Elliptic Curve Ephemeral Diffie-Hellman)。現代系統(如 Java 7 和更新版本)大多會支援這些模式。

此外，請求必須使用存取金鑰 ID 和與 IAM 主體相關聯的私密存取金鑰來簽署。或者，您可以透過 AWS Security Token Service (AWS STS) 來產生暫時安全憑證來簽署請求。

Amazon DevOps 大師的韌性

AWS 全球基礎架構是圍繞區 AWS 域和可用區域建立的。 AWS 區域提供多個實體分離和隔離的可用區域，這些區域透過低延遲、高輸送量和高度備援的網路連線。 DevOpsGuru 在多個可用區域中運作，並將人工因素資料和中繼資料存放在 Amazon S3 和 Amazon DynamoDB 中。您的加密資料會以冗餘方式儲存在多個設施和每個設施中的多個裝置，因此具有高可用性和高度耐用性。

如需區域和可用區域的相關 AWS 資訊，請參閱AWS 全域基礎結構。

亞馬遜的配額和限制DevOps老師

下表列出了亞馬遜當前的配額DevOps大師。此配額適用於每個受支援項目AWS每個區域AWS帳戶。

通知

您可以一次指定的最大 Amazon 簡單通知服務主題數量	2

AWS CloudFormation 堆疊

最大數量AWS CloudFormation您可以指定的堆疊	1000

DevOps大師資源監視限制

資源描述	限制	可以提高
監控亞馬遜簡單佇列服務 (Amazon SQS) 佇列的預設限制	100*	是 **

* 對於新的DevOps在 2023 年 6 月 29 日當天或之後建立的大師帳戶，以及在同一日期有效且 Amazon SQS 佇列少於 100 個的現有帳戶。

** 要求更改此限制，請聯繫AWS Support在https://aws.amazon.com/contact-us。您可以要求亞馬遜 SQS 佇列監控限制為 100、500、1,000、5,000 或 10,000。

DevOps用於建立、部署和管理 API 的大師配額

下列固定配額適用於在中建立、部署和管理 APIDevOps大師, 使用AWS CLI、API 閘道主控台或 API 閘道 REST API 及其開發套件。

對於所有的列表DevOps大師 API，請參閱亞馬遜DevOps大師行動。

預設配額	可以提高	
每個帳戶每 1 秒 20 個請求	是	

亞馬遜DevOps大師文檔歷史

下表說明此版本的文件DevOps大師。

- API 版本：最新
- 最新的文檔更新：2023年8月9 日

變更	描述	日期
受管理政策更新	Amazon SNS 訂閱和訂閱清單存取權已新增至AmazonDevOpsGuruConsoleFullAccess 政策。訂閱清單存取權也已新增至AmazonDevOpsGuruReadOnlyAccess 政策。如需詳細資訊，請參閱亞馬遜的基於身份的政策DevOps老師。	2023年8月9 日
客戶管理的加密金鑰	DevOpsGuru 現在支持使用客戶託管密鑰進行加密AWS KMS。如需詳細資訊，請參閱資料保護DevOps老師。	2023 年 7 月 5 日
DevOpsRDS 大師支援 RDS	DevOpsRDS 專家可以檢測 PostgreSQL 數據庫中的性能瓶頸和其他見解。如需詳細資訊，請參閱的好處DevOpsRDS的大師。	2023 年 3 月 30 日
DevOpsRDS 大師支持主動洞察	DevOpsGuru for RDS 發佈主動式見解及建議，協助您在 Aurora 資料庫中解決問題，避免問題變得更大。如需詳細資訊，請參閱使用中的異常DevOpsRDS 的大師。	2023 年 2 月 28 日

分析資源頁面	一個新的一頁DevOpsGuru 控制台列出了您帳戶中分析的資源DevOps大師。如需詳細資訊，請參閱檢視分析者的資源DevOps老師。	2022 年 10 月 20 日
新的通知組態設定	您現在可以選擇是否要接收所有通知，還是只接收特定嚴重性和事件的通知。如需詳細資訊，請參閱更新亞馬遜 SNS 通知組態。	2022 年 9 月 30 日
記錄受管理原則之外的異常分析	AWS受管理的政策DevOps大師已在 IAM 控制台中更新，以支持對CloudWatch行動`FilterLogEvents` 。如需詳細資訊，請參閱DevOps大師更新AWS受管理的策略和服務連結角色。	2022 年 8 月 30 日
新增日誌異常分析	您可以在中檢視與見解相關的記錄群組詳細資訊DevOps大師控制台。還有一個擴展的服務鏈接角色可用於描述CloudWatch日誌和流。如需詳細資訊，請參閱了解中的見解DevOps大師控制台和DevOps大師更新AWS受管理的策略和服務連結角色。	2022 年 7 月 12 日
CodeGuru效能分析工具整合	DevOps大師現在與亞馬遜集成CodeGuru使用效能分析工具EventBridge受管規則。每個傳入事件CodeGuru效能分析工具是主動的異常報告。如需詳細資訊，請參閱與整合CodeGuru效能分析工具。	2022 年 3 月 7 日

服務連結角色和受管政策更新	IAM 主控台提供的擴充政策。這些更改允許DevOps大師支持與亞馬遜關係數據庫服務（亞馬遜 RDS）的增強集成。如需詳細資訊，請參閱使用服務連結角色和AWS的管理 (預先定義) 策略DevOps老師。	2021 年 12 月 21 日
添加了新的受管策略	該AmazonDevOpsGuruConsoleFullAccess 已新增策略。如需詳細資訊，請參閱亞馬遜的基於身份的政策DevOps老師。	2021 年 12 月 6 日
支援定義您的應用程式AWS標籤	您現在可以使用AWS標籤以識別您想要的資源DevOpsGuru可以在主控台中分析、識別應用程式中的資源，並篩選見解。如需詳細資訊，請參閱使用標籤識別應用程式中的資源。	2021 年 12 月 1 日
服務連結角色和受管政策更新	IAM 主控台提供的擴充政策。這些更改允許DevOps大師支持與亞馬遜關係數據庫服務（亞馬遜 RDS）的增強集成。如需詳細資訊，請參閱使用服務連結角色和AWS的管理 (預先定義) 策略DevOps老師。	2021 年 12 月 1 日
亞馬遜 RDS 支持	DevOpsGuru 現在為您的應用程式中的 Amazon 關聯式資料庫服務 (Amazon RDS) 資源提供全面的分析和見解。如需詳細資訊，請參閱使用中的異常DevOps亞馬遜 RDS 的大師。	2021 年 12 月 1 日

亞馬遜EventBridge整合	DevOps大師現在集成了Event Bridge通知您某些與您有關的事件DevOps大師見解。如需詳細資訊，請參閱使用 EventBridge。	2021 年 11 月 18 日
AWS已新增受管原則	新AWS已新增受管理原則。該AmazonDevOpsGuruOrganizationsAccess 原則提供存取DevOps組織內的大師。如需詳細資訊，請參閱以身分為基礎的原則。	2021 年 11 月 16 日
服務連結角色原則更新	IAM 主控台提供的擴充政策。變更允許DevOps大師支持多帳戶視圖。如需詳細資訊，請參閱使用服務連結角色。	2021 年 11 月 4 日
跨帳戶支援	您現在可以檢視組織中多個帳戶的深入解析和指標。如需詳細資訊，請參閱什麼是亞馬遜DevOps老師。	2021 年 11 月 4 日
一般可用性版本	亞馬遜DevOps大師現已正式推出 (GA)。	2021 年 5 月 4 日
新主題	您現在可以產生的每月成本估算DevOps大師來分析你的資源。如需詳細資訊，請參閱估計你的亞馬遜DevOps大師成本。	2021 年 4 月 27 日
VPC 端點支援	您現在可以使用 VPC 端點來提高資源分析和洞察產生的安全性。如需詳細資訊，請參閱DevOps大師和接口 VPC 端點 (AWS PrivateLink)。	2021 年 4 月 15 日

新主題	有關如何監視的新主題DevOps大師與亞馬遜CloudWatch已新增。如需詳細資訊，請參閱監控DevOps大師與亞馬遜CloudWatch。	2020 年 12 月 11 日
預覽版	這是預覽版的亞馬遜DevOps大師用戶指南。	2020 年 12 月 1 日

AWS 詞彙表

如需最新的 AWS 術語，請參閱《AWS 詞彙表 參考》中的 AWS 詞彙表。

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。