aws

使用者指南

Amazon DevOps Guru

Amazon DevOps Guru: 使用者指南

Table of Contents

什麼是 Amazon DevOps Guru？

歡迎使用 Amazon DevOps Guru 使用者指南。

DevOps Guru 是一種全受管操作服務，可讓開發人員和操作員輕鬆改善其應用程式的效能和可用性。DevOps Guru 可讓您卸載與識別操作問題相關聯的管理任務，以便快速實作建議以改善應用程式。DevOps Guru 會建立反應式洞見，您現在可以用來改善您的應用程式。它也會建立主動洞見，協助您避免未來可能影響應用程式的營運問題。

DevOps Guru 會套用機器學習來分析您的操作資料和應用程式指標和事件，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。對於每個問題，DevOps Guru 都會提供智慧型建議，以解決目前和預測的未來營運問題。

若要開始使用，請參閱 如何開始使用 DevOps Guru？

DevOps Guru 如何運作？

DevOps Guru 工作流程會在您設定其涵蓋範圍和通知時開始。設定 DevOps Guru 之後，它會開始分析您的營運資料。當偵測到異常行為時，它會建立洞見，其中包含與問題相關的指標、日誌群組和事件的建議和清單。對於每個洞見，DevOps Guru 都會通知您。如果您 enabled AWS Systems Manager OpsCenter，則會建立 OpsItem，以便您可以使用 Systems Manager OpsCenter 來追蹤和管理解決您的洞見。每個洞見都包含與異常行為相關的建議、指標、日誌群組和事件。使用洞見中的資訊來協助您了解並解決異常行為。

高階 DevOps Guru 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 DevOps Guru 工作流程 以了解更詳細的 DevOps Guru 工作流程，包括其與其他 AWS 服務的互動方式。

主題

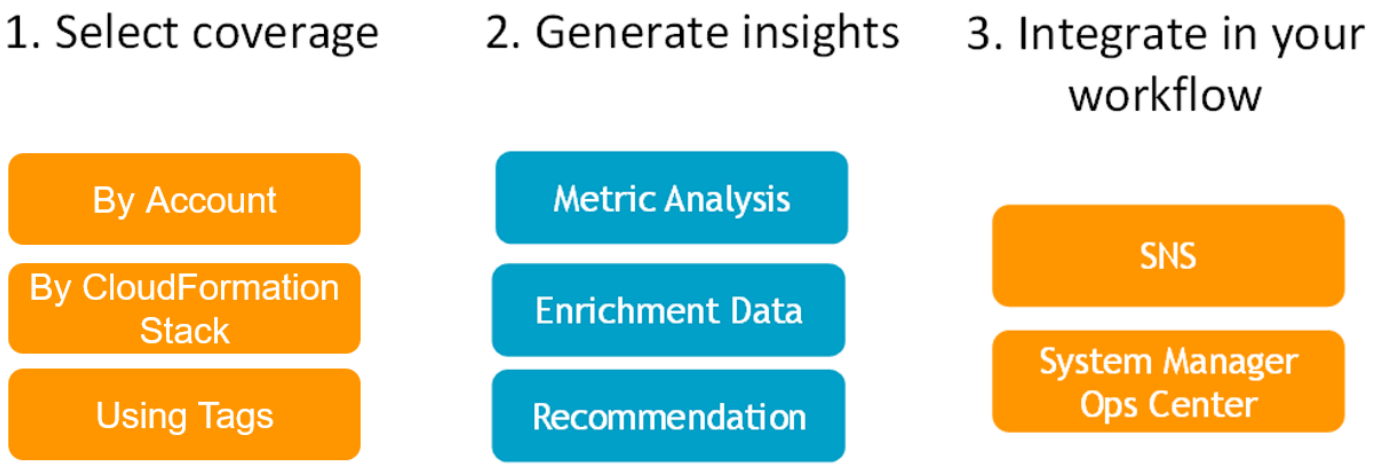
高階 DevOps Guru 工作流程

Amazon DevOps Guru 工作流程可以分為三個高階步驟。

1. 告訴 DevOps Guru 涵蓋範圍，您帳戶中要分析 AWS 的資源 AWS 。

2. DevOps Guru 會開始分析 Amazon CloudWatch 指標和其他操作資料 AWS CloudTrail，以識別您可以修正以改善操作的問題。
3. DevOps Guru 會傳送每個重要 DevOps Guru 事件的通知給您，以確保您了解洞見和重要資訊。

您也可以設定 DevOps Guru 建立 OpsItem in AWS Systems Manager OpsCenter，以協助您追蹤洞見。下圖顯示此高階工作流程。



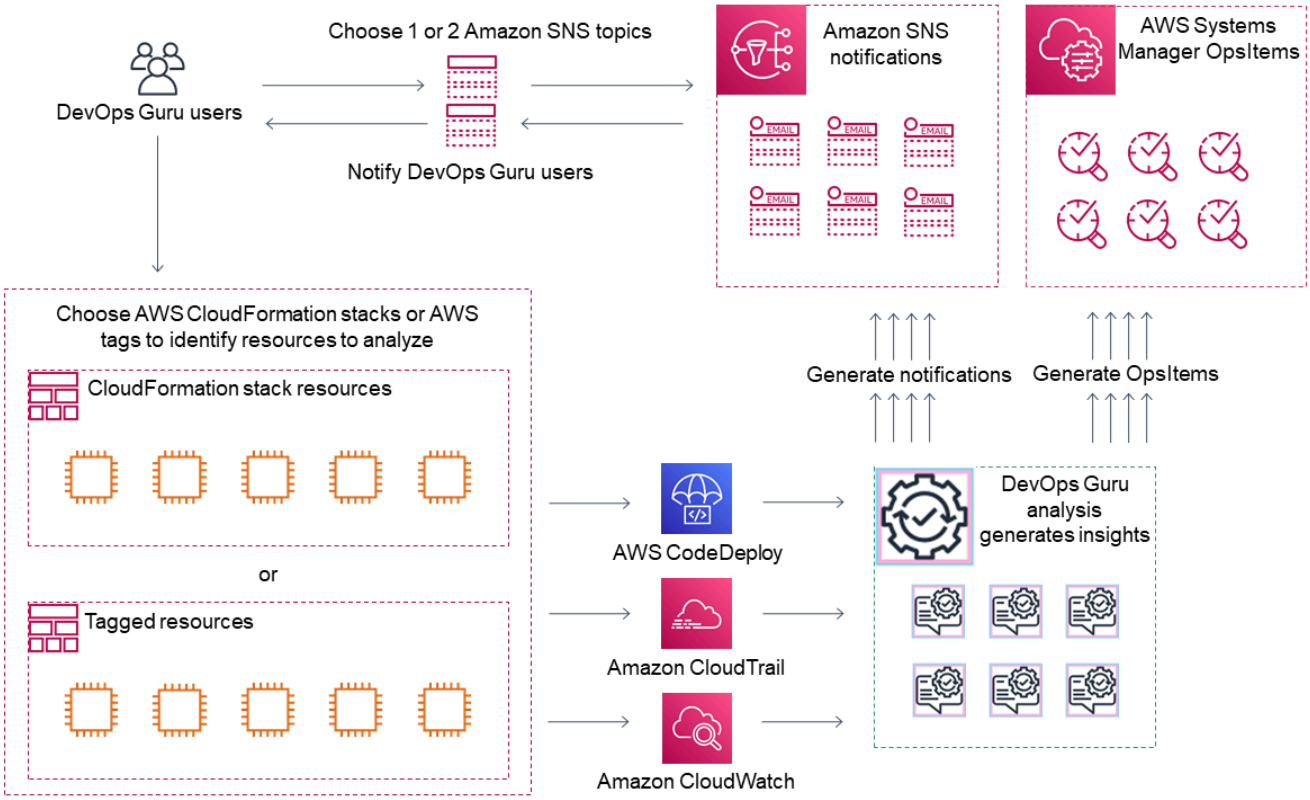
1. 在第一個步驟中，您可以透過指定要分析 AWS 帳戶中的資源 AWS 來選擇涵蓋範圍。DevOps Guru 可以涵蓋或分析 AWS 帳戶中的所有資源，也可以使用 AWS CloudFormation 堆疊或 AWS 標籤來指定帳戶中要分析的資源子集。請確定您指定的資源構成了業務關鍵應用程式、工作負載和微服務。如需支援服務和資源的詳細資訊，請參閱 Amazon DevOps Guru 定價。
2. 在第二個步驟中，DevOps Guru 會分析資源以產生洞見。這是持續進行的程序。您可以檢視洞見，並查看它們在 DevOps Guru 主控台中包含的建議和相關資訊。DevOps Guru 會分析下列資料，以尋找問題並建立洞見。
   - AWS 資源發出的個別 Amazon CloudWatch 指標。發現問題時，DevOps Guru 會一起收集這些指標。
   - 來自 Amazon CloudWatch 日誌群組的日誌異常。如果您啟用日誌異常偵測，DevOps Guru 會在發生問題時顯示相關的日誌異常。
   - DevOps Guru 會從 AWS CloudTrail 管理日誌提取擴充資料，以尋找與收集指標相關的事件。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，DevOps Guru 會分析部署事件，以協助產生洞見。會分析所有 CodeDeploy 部署類型 （內部部署伺服器、Amazon EC2 伺服器、Lambda 或 Amazon EC2) 的事件。

- 當 DevOps Guru 找到特定模式時，會產生一或多個建議，以協助緩解或修正已識別的問題。建議收集在一個洞見中。洞見也包含與問題相關的指標和事件清單。您可以使用洞見資料來解決和了解已識別的問題。

3. 在第三個步驟中，DevOps Guru 會將洞見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。
   - AWS 帳戶中產生的洞見會發佈至 DevOps Guru 設定期間選擇的 Amazon Simple Notification Service (Amazon SNS) 主題。這是建立洞見後立即通知您的方式。如需詳細資訊，請參閱在 DevOps Guru 中更新您的通知。
   - 如果您在 DevOps Guru 設定 AWS Systems Manager 期間啟用 ，每個洞見都會建立對應的 OpsItem，以協助您追蹤和管理發現的問題。如需詳細資訊，請參閱在 DevOps Guru 中更新 AWS Systems Manager 整合。

詳細 DevOps Guru 工作流程

DevOps Guru 工作流程與數個 AWS 服務整合，包括 Amazon CloudWatch、 AWS CloudTrail、Amazon Simple Notification Service 和 AWS Systems Manager。下圖顯示詳細的工作流程，其中包含它如何與其他 AWS 服務搭配使用。



此圖表顯示 DevOps Guru 涵蓋範圍是由 AWS CloudFormation 堆疊中或使用 AWS 標籤定義的 AWS 資源所指定的案例。如果未選擇堆疊或標籤，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 AWS 資源定義應用程式及判斷 DevOps Guru 的涵蓋範圍。

1. 在設定期間，您可以指定一或兩個 Amazon SNS 主題，用於通知您重要的 DevOps Guru 事件，例如在建立洞見時。接下來，您可以指定定義要分析之資源的 AWS CloudFormation 堆疊。您也可以讓 Systems Manager 為每個洞見產生 OpsItem，以協助您管理您的洞見。
2. 設定 DevOps Guru 之後，它會開始分析從與 CloudWatch 指標相關的資源和 AWS CloudTrail 資料發出的 CloudWatch 指標、日誌群組和事件。如果您的操作包含 CodeDeploy 部署，DevOps Guru 也會分析部署事件。

   DevOps Guru 會在識別分析資料中的異常異常行為時建立洞見。每個洞見都包含一或多個建議、用於產生洞見的指標清單、相關日誌群組清單，以及用於產生洞見的事件清單。使用此資訊來解決已識別的問題。
3. 建立每個洞見後，DevOps Guru 會使用 Amazon SNS 主題或在 DevOps Guru 設定期間指定的主題傳送通知。如果您讓 DevOps Guru 在 Systems Manager OpsCenter 中產生 OpsItem，則每個洞見也會觸發新的 Systems Manager OpsItem。 OpsCenter 您可以使用 Systems Manager 來管理您的洞見 OpsItems。

如何開始使用 DevOps Guru？

建議您完成下列步驟：

1. 閱讀 中的資訊，進一步了解 DevOps GuruDevOps Guru 概念。
2. 遵循中的步驟來設定 AWS 您的帳戶 AWS CLI、 和管理使用者設定 Amazon DevOps Guru。
3. 依照 中的指示使用 DevOps GuruDevOps Guru 入門。

如何停止產生 DevOps Guru 費用？

若要停用 Amazon DevOps Guru，使其不會因分析 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，請遵循中的步驟在 DevOps Guru 中更新您的 AWS 分析涵蓋範圍，然後在步驟 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，則如果您過去檢閱 DevOps Guru 產生的現有洞見，可能會繼續產生小額費用。這些費用與用於擷取和顯示洞見資訊的 API 呼叫相關聯。如需詳細資訊，請參閱 Amazon DevOps Guru 定價。

DevOps Guru 概念

下列概念對於了解 Amazon DevOps Guru 的運作方式非常重要。

主題

異常

異常表示 DevOps Guru 偵測到的一個或多個未預期或不尋常的相關指標。DevOps Guru 會使用機器學習來分析與您 AWS 資源相關的指標和操作資料，進而產生異常。您可以在設定 Amazon DevOps Guru 時指定要分析 AWS 的資源。如需詳細資訊，請參閱設定 Amazon DevOps Guru。

Insight

洞見是在分析您在設定 DevOps Guru 時指定的資源時建立的 AWS 異常集合。每個洞見都包含觀察、建議和分析資料，您可以用來改善營運效能。有兩種類型的洞見：

- 被動：被動洞察會在異常行為發生時加以識別。它包含具有建議、相關指標和事件的異常，以協助您立即了解並解決問題。
- 主動：主動洞察可讓您在異常行為發生之前知道。它包含具有建議的異常，可協助您在預測問題發生之前解決問題。

指標和操作事件

構成洞見的異常是透過分析 Amazon CloudWatch 傳回的指標和 AWS 資源發出的操作事件所產生。您可以檢視建立洞見的指標和操作事件，以協助您進一步了解應用程式中的問題。

日誌群組和日誌異常

當您啟用日誌異常偵測時，相關的日誌群組會顯示在 DevOps Guru 主控台的 DevOps Guru 洞見頁面上。日誌群組可讓您了解資源如何執行和存取的重要診斷資訊。

日誌異常代表在日誌群組中找到的類似異常日誌事件叢集。DevOps Guru 中可能顯示的異常日誌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。DevOps Guru 也會在洞見建議中參考日誌行，以提供建議解決方案的更多內容。

> **Note**
>
> DevOps Guru 可與 Amazon CloudWatch 搭配使用，以啟用日誌異常偵測。當您啟用日誌異常偵測時，DevOps Guru 會將標籤新增至 CloudWatch 日誌群組。當您關閉日誌異常偵測時，DevOps Guru 會從 CloudWatch 日誌群組中移除標籤。
> 此外，管理員應確保只有具有檢視 CloudWatch 日誌許可的使用者才具有檢視異常 CloudWatch 日誌的許可。我們建議您使用 IAM 政策來允許或拒絕對 `ListAnomalousLogs`操作的存取。如需詳細資訊，請參閱 DevOps Guru 的 Identity and Access Management。

建議

每個洞見都提供建議，協助您改善應用程式的效能。建議包括下列項目：

- 建議動作的描述，以解決構成洞見的異常情況。
- DevOps Guru 發現異常行為的已分析指標清單。每個指標都包含產生與指標相關聯資源的 CloudFormation 堆疊名稱、資源名稱，以及與資源相關聯的 AWS 服務名稱。
- 與洞見相關聯的異常指標相關的事件清單。每個相關事件都包含產生與事件相關聯資源的 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。
- 與洞見相關聯的異常行為相關的日誌群組清單。每個日誌群組都包含範例日誌訊息、報告日誌異常類型的相關資訊、日誌異常發生的時間，以及在 CloudWatch 上檢視日誌行的連結。

DevOps Guru 涵蓋範圍

DevOps Guru 會處理並建立許多不同 AWS 服務的洞見。對於 DevOps Guru 建立洞見的每個服務，DevOps Guru 會顯示各種分析指標和產生的洞見。

反應式洞見的範例使用案例：

服務名稱	使用案例	範例	指標
AWS Lambda	偵測各種根本原因導致的 Lambda 函數延遲或持續時間異常，例如冷啟動、請求增加、下游限流或程式碼部署。建議快速緩解的方法。	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。下游限流：運算子減少 DynamoDB 讀取單位的容量，導致重試次數增加。這會導致限流。冷啟動：Lambda 函數佈建不足，因此 Lambda 在提出請求時需要更長的時間。	持續時間 限流

主動洞察的範例使用案例：

服務名稱	使用案例	指標
Amazon DynamoDB	DynamoDB 資料表讀取耗用容量有達到資料表限制的風險。建議動作：如果您使用佈建容量模式，請使用自動擴展主動管理資料表的輸送量容量，或事先購買資料表的預留容量。切換到隨需容量模式，以按讀取請求付費，僅按使用量付費。偵測時間：6 天	ConsumedReadCapacityUnits

服務涵蓋範圍清單

對於某些服務，DevOps Guru 會建立反應式洞見。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，以協助您立即了解並解決問題。

對於某些服務，DevOps Guru 會建立主動洞察。主動洞察可讓您在異常行為發生之前知道。它包含具有建議的異常，可協助您在預測問題發生之前解決問題。

DevOps Guru 會為下列服務建立反應式洞見：

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

> **Note**
>
> DevOps Guru 監控位於 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 AI
- AWS Step Functions
- Amazon SNS
- Amazon SQS

- Amazon SWF
- Amazon VPC

DevOps Guru 會為下列服務建立主動洞見：

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

設定 Amazon DevOps Guru

完成本節中的任務，以首次設定 Amazon DevOps Guru。如果您已經有 AWS 帳戶、知道要分析哪些 AWS 帳戶，並具有用於洞見通知的 Amazon Simple Notification Service 主題，您可以直接跳到 DevOps Guru 入門。

或者，您可以使用 的快速設定功能 AWS Systems Manager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。若要在 Systems Manager 中使用快速設定為組織設定 DevOps Guru，您必須具備下列先決條件：

- 使用 的組織 AWS Organizations。如需詳細資訊，請參閱AWS Organizations 《 使用者指南》中的AWS Organizations 術語和概念。
- 兩個或多個組織單位 OUs)。
- 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。

若要了解如何使用快速設定設定 DevOps Guru，請參閱AWS Systems Manager 《 使用者指南》中的使用快速設定設定 DevOps Guru。

使用下列步驟來設定 DevOps Guru，無需快速設定。

- 步驟 1 – 註冊 AWS
- 步驟 2 – 判斷 DevOps Guru 的涵蓋範圍
- 步驟 3 – 識別您的 Amazon SNS 通知主題

步驟 1 – 註冊 AWS

註冊 AWS 帳戶

如果您沒有 AWS 帳戶，請完成下列步驟來建立一個。

註冊 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或簡訊，並在電話鍵盤輸入驗證碼。

當您註冊 時 AWS 帳戶，AWS 帳戶根使用者會建立 。根使用者有權存取該帳戶中的所有 AWS 服務 和資源。作為安全最佳實務，請將管理存取權指派給使用者，並且僅使用根使用者來執行需要根使用者存取權的任務。

AWS 會在註冊程序完成後傳送確認電子郵件給您。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。

建立具有管理存取權的使用者

註冊 後 AWS 帳戶，請保護 AWS 帳戶根使用者、啟用 AWS IAM Identity Center和建立管理使用者，以免將根使用者用於日常任務。

保護您的 AWS 帳戶根使用者

1. 選擇根使用者並輸入 AWS 帳戶 您的電子郵件地址，以帳戶擁有者AWS 管理主控台身分登入 。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)。

   如需說明，請參閱《IAM 使用者指南》中的為您的 AWS 帳戶 根使用者 （ 主控台 ） 啟用虛擬 MFA 裝置。

建立具有管理存取權的使用者

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 Identity Center 中，將管理存取權授予使用者。

   如需使用 IAM Identity Center 目錄 做為身分來源的教學課程，請參閱AWS IAM Identity Center 《 使用者指南》中的使用預設值設定使用者存取 IAM Identity Center 目錄。

以具有管理存取權的使用者身分登入

- 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 Identity Center 使用者登入的說明，請參閱AWS 登入 《 使用者指南》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 Identity Center 中，建立一個許可集來遵循套用最低權限的最佳實務。

   如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的建立許可集。
2. 將使用者指派至群組，然後對該群組指派單一登入存取權。

   如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的新增群組。

步驟 2 – 判斷 DevOps Guru 的涵蓋範圍

您的界限涵蓋範圍會決定 Amazon DevOps Guru 針對異常行為所分析 AWS 的資源。建議您將資源分組到營運應用程式中。資源界限中的所有資源都應該包含一或多個應用程式。如果您有一個操作解決方案，則涵蓋範圍界限應該包含其所有資源。如果您有多個應用程式，請選擇構成每個解決方案的資源，並使用 CloudFormation 堆疊或 AWS 標籤將其分組在一起。無論您指定的所有合併資源定義一或多個應用程式，DevOps Guru 都會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 操作解決方案中的資源。

- 選擇讓您的 AWS 區域和帳戶定義您的涵蓋範圍界限。使用此選項，DevOps Guru 會分析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式，這是不錯的選擇。
- 使用 CloudFormation 堆疊來定義營運應用程式中的資源。 CloudFormation 範本會為您定義和產生資源。當您設定 DevOps Guru 時，請指定建立應用程式資源的堆疊。您可以隨時更新堆疊。您選擇的堆疊中的所有資源都會定義您的界限涵蓋範圍。如需詳細資訊，請參閱使用 CloudFormation 堆疊來識別 DevOps Guru 應用程式中的資源。
- 使用 AWS 標籤來指定應用程式中 AWS 的資源。DevOps Guru 只會分析包含您選擇的標籤的資源。這些資源構成您的界限。

  AWS 標籤由標籤索引鍵和標籤值組成。您可以指定一個標籤索引鍵，也可以指定一或多個使用該索引鍵的值。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，請針對所有應用程式使用具有相同索引鍵的標籤，並使用標籤的值將資源分組到您的應用程式中。所有具有您選擇構成 DevOps Guru 涵蓋範圍之標籤的資源。如需詳細資訊，請參閱使用標籤來識別 DevOps Guru 應用程式中的資源。

如果您的界限涵蓋範圍包含由多個應用程式組成的資源，您可以使用 標籤來篩選您的洞見，以一次依一個應用程式檢視這些洞見。如需詳細資訊，請參閱 中的步驟 4檢視 DevOps Guru 洞見。

如需詳細資訊，請參閱使用 AWS 資源定義應用程式。如需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 主題來產生重要 DevOps Guru 事件的通知，例如建立洞見的時間。這可確保您知道 DevOps Guru 盡快發現的問題。當您設定 DevOps Guru 時，請準備好您的主題。當您使用 DevOps Guru 主控台設定 DevOps Guru 時，您可以使用其名稱或其 Amazon Resource Name (ARN) 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，則可以在使用 DevOps Guru 主控台啟用 DevOps Guru 時建立主題。如需詳細資訊，請參閱《Amazon Simple Notification Service 開發人員指南》中的建立主題。

新增到 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。當您在此處指定主題時，DevOps Guru 會將下列許可附加至其資源政策。

```
{
    "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"
    }
  }
}
```

DevOps Guru 需要這些許可才能使用主題發佈通知。如果您不想對主題擁有這些許可，您可以安全地移除這些許可，而且主題會繼續像您選擇主題之前一樣運作。不過，如果移除這些附加的許可，DevOps Guru 就無法使用 主題來產生通知。

預估 Amazon DevOpsGuru 資源分析成本

您可以預估 Amazon DevOpsGuru 的每月成本，以分析您的 AWS 資源。您需為指定資源涵蓋範圍中每個作用中 AWS 資源所分析的時數支付費用。如果資源在一小時內產生指標、事件或日誌，則會處於作用中狀態。

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，以及估計的每月費用。成本估算器預設會 100% 的時間使用分析的作用中資源。您可以根據預估用量變更每個分析服務的此百分比，以建立更新的每月成本估算。預估是分析 資源的成本，不包含與 DevOpsGuru API 呼叫相關聯的成本。

您可以一次建立一個成本估算。產生成本估算所需的時間取決於您在建立成本估算時指定的資源數量。當您指定幾個資源時，可能需要 1 到 2 小時才能完成。當您指定許多資源時，最多可能需要 4 小時才能完成。您的實際成本會有所不同，取決於分析的作用中資源的使用時間百分比。

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

建立每月資源分析成本估算

1. 在 https://console.aws.amazon.com/devops-guru/ : // 開啟 Amazon DevOpsGuru 主控台。
2. 在導覽窗格中選擇成本估算器。
3. 如果您尚未啟用 DevOpsGuru，則必須建立 IAM 角色。在顯示的為 DevOpsGuru 建立 IAM 角色快顯視窗中，選擇同意以建立 IAM 角色。這可讓 DevOpsGuru 在您選擇開始成本估算分析或開始使用 DevOpsGuru 時，為您建立 IAM 服務連結角色。如此一來，DevOpsGuru 便擁有建立成本估算所需的許可。如果您已啟用 DevOpsGuru，則角色已建立，此選項不會顯示。
4. 選擇您要用來建立估算的資源。

   - 如果您想要預估 DevOpsGuru 分析一個 CloudFormation 堆疊定義的資源的成本，請執行下列動作。

     1. 選擇目前區域中的 CloudFormation 堆疊。
     2. 在選擇 CloudFormation 堆疊中，選擇您 AWS 帳戶中的 CloudFormation 堆疊名稱。您也可以輸入堆疊的名稱，以快速找到堆疊。如需有關使用 和檢視堆疊的資訊，請參閱CloudFormation 《 使用者指南》中的使用 堆疊。

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

- 如果您想要預估 DevOpsGuru 使用標籤分析資源的成本，請執行下列動作。
  1. 在目前區域中 AWS 的資源上選擇標籤
  2. 在標籤金鑰中選擇標籤的金鑰
  3. 在標籤值中選擇（所有值）或選擇一個值。
- 如果您想要預估 DevOpsGuru 分析 AWS 帳戶和區域中資源的成本，請選擇AWS 目前區域中的帳戶。

5. 選擇預估每月成本。
6. （選用）在作用中資源使用率 % 欄中，輸入一或多個 AWS 服務的更新百分比值。預設作用中資源使用率 % 為 100%。這表示 DevOps Guru 會計算分析其資源一小時的成本，然後推斷超過 30 天，總共 720 小時，以產生 AWS 服務的預估值。如果服務在不到 100% 的時間內處於作用中狀態，您可以根據預估用量更新百分比，以獲得更準確的預估。例如，如果您將服務的作用中資源使用率更新為 75%，則分析其資源的一小時成本會推斷為 (720 x 0.75) 小時或 540 小時。

如果您的預估值為零美元，則您選擇的資源可能不包含 DevOpsGuru 支援的資源。如需支援服務和資源的詳細資訊，請參閱 Amazon DevOpsGuru 定價。

DevOps Guru 入門

在本節中，您將了解如何開始使用 Amazon DevOps Guru，以便分析應用程式的營運資料和指標以產生洞見。

主題

步驟 1：設定

開始之前，請執行 中的步驟來準備 設定 Amazon DevOps Guru。

步驟 2：啟用 DevOps Guru

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

您可以在整個組織中監控應用程式，或僅為目前的帳戶啟用 DevOps Guru。下列程序概述了根據您的需求設定 DevOps Guru 的不同方式。

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管理員帳戶都可以存取組織中所有帳戶的所有洞見。

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

使用 DevOps Guru 主控台加入

您可以使用 主控台，為整個組織的帳戶新增支援。

使用 主控台讓 DevOps Guru 檢視彙總的洞見

1. 開啟位於 https：//https://console.aws.amazon.com/devops-guru/ 的 Amazon DevOps Guru 主控台。

2. 選擇監控整個組織的應用程式做為設定類型。
3. 選擇您要用作委派管理員的帳戶。然後，選擇註冊委派管理員。這可讓您存取已啟用 DevOps Guru 的任何帳戶的合併檢視。委派管理員具有整個組織所有 DevOps Guru 洞察和指標的合併檢視。您可以使用 SSM 快速設定或 AWS CloudFormation 堆疊集啟用其他帳戶。若要進一步了解快速設定，請參閱使用快速設定設定 DevOps Guru。若要進一步了解如何使用堆疊集進行設定，請參閱CloudFormation 《 使用者指南》中的使用堆疊，以及 步驟 2 – 判斷 DevOps Guru 的涵蓋範圍和 使用 CloudFormation 堆疊來識別 DevOps Guru 應用程式中的資源。

使用 CLI AWS 加入

您可以使用 AWS CLI 讓 DevOps Guru 檢視彙總的洞見。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
```

下表說明 命令。

命令	Description
`create-service-linked-role`	授予 DevOps Guru 收集組織相關資訊的許可。如果此步驟不成功，請勿繼續。
`enable-aws-service-access`	將您的組織加入 DevOps Guru。
`register-delegated-administrator`	提供成員帳戶的存取權，以檢視洞見。

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，請選擇您的帳戶和區域中涵蓋或分析 AWS 的資源，並指定一或兩個用於在建立洞見時通知您的 Amazon Simple Notification Service 主題。您可以視需要稍後更新這些設定。

讓 DevOps Guru 監控目前 AWS 帳戶中的應用程式

1. 開啟位於 https：//https://console.aws.amazon.com/devops-guru/ 的 Amazon DevOps Guru 主控台。
2. 選擇監控目前 AWS 帳戶中的應用程式做為設定類型。
3. 在 DevOps Guru 分析涵蓋範圍內，選擇下列其中一項。

   - 分析目前 AWS 帳戶中的所有 AWS 資源：DevOps Guru 會分析您帳戶中的所有 AWS 資源。
   - 選擇 AWS 資源以供稍後分析：您稍後選擇分析界限。如需詳細資訊，請參閱判斷 DevOps Guru 的涵蓋範圍及在 DevOps Guru 中更新您的 AWS 分析涵蓋範圍。

   DevOps Guru 可以分析與其支援 AWS 的帳戶相關聯的任何資源。如需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。DevOps Guru 使用 主題來通知您重要的 DevOps Guru 事件，例如建立新的洞見。如果您現在未指定主題，您可以稍後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，請執行下列其中一項操作。

      - 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，從另一個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 是主題的 Amazon Resource Name。您可以在不同的帳戶中指定主題。如果您在另一個帳戶中使用主題，則必須將資源政策新增至主題。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，您必須選擇帳戶和區域中涵蓋或分析的資源 AWS ，並指定一或兩個用於在建立洞見時通知您的 Amazon Simple Notification Service 主題。您可以視需要稍後更新這些設定。

步驟 3：指定您的 DevOps Guru 資源涵蓋範圍

如果您在稍後啟用 DevOps Guru 時選擇指定 AWS 資源，則需要選擇 AWS 帳戶中建立您要分析之資源的 CloudFormation 堆疊。 CloudFormation 堆疊是您以單一單位管理的一組 AWS 資源。您可以使用一或多個堆疊來包含執行營運應用程式所需的所有資源，然後指定這些資源，以便 DevOps Guru 分析這些資源。如果您未指定堆疊，DevOps Guru 會分析您帳戶中的所有 AWS 資源。如需詳細資訊，請參閱CloudFormation 《 使用者指南》中的使用堆疊，以及 判斷 DevOps Guru 的涵蓋範圍和 使用 CloudFormation 堆疊來識別 DevOps Guru 應用程式中的資源。

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

指定 DevOps Guru 資源涵蓋範圍

1. 開啟位於 https：//https://console.aws.amazon.com/devops-guru/ 的 Amazon DevOps Guru 主控台。
2. 在導覽窗格中展開設定。
3. 在分析的資源中，選擇編輯分析的資源。
4. 選擇下列其中一個涵蓋範圍選項。

   - 如果您希望 DevOps Guru 分析帳戶和區域中所有支援的資源，請選擇所有 AWS 帳戶資源。如果您選擇此選項， AWS 您的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自己的應用程式中。
   - 如果您希望 DevOps Guru 分析所選堆疊中的資源，請選擇 CloudFormation 堆疊，然後選擇下列其中一個選項。
     - 所有資源 – 分析您帳戶中堆疊中的所有資源。每個堆疊中的資源會分組到自己的應用程式中。不會分析您帳戶中任何不在堆疊中的資源。
     - 選取堆疊 – 選取您希望 DevOps Guru 分析的堆疊。您選取的每個堆疊中的資源會分組到自己的應用程式。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。您最多可以選取 1，000 個堆疊。

如需詳細資訊，請參閱使用 CloudFormation 堆疊來識別 DevOps Guru 應用程式中的資源。

- 如果您希望 DevOps Guru 分析包含您選擇的標籤的所有資源，請選擇標籤。選擇金鑰，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。具有所選標籤索引鍵的資源會依標籤值分組，如果有的話。沒有此標籤索引鍵的資源會個別分組和分析。
  - 選擇特定標籤值 – 會分析包含具有所選索引鍵之標籤的所有資源。DevOps Guru 會根據標籤的值將您的資源分組到應用程式中。

  如需詳細資訊，請參閱使用標籤來識別 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，讓您停止因資源分析而產生費用。

5. 選擇儲存。

啟用 DevOpsGuru 分析 AWS 的服務

Amazon DevOpsGuru 可以分析其支援的任何 AWS 資源的效能。當它找到異常行為時，會產生有關行為以及如何解決該行為的詳細資訊的洞見。如需支援服務和資源的詳細資訊，請參閱 Amazon DevOpsGuru 定價。

DevOpsGuru 使用 Amazon CloudWatch 指標、 AWS CloudTrail 事件等協助分析資源。其支援的大多數資源會自動產生 DevOpsGuru 分析所需的指標。不過，有些 AWS 服務需要額外的動作來產生所需的指標。對於某些服務，啟用這些指標可為現有的 DevOpsGuru 涵蓋範圍提供額外的分析。對於其他人，在您啟用這些指標之前，無法進行分析。如需詳細資訊，請參閱 判斷 DevOps Guru 的涵蓋範圍 和 在 DevOps Guru 中更新您的 AWS 分析涵蓋範圍。

需要 DevOpsGuru 分析動作的服務

- Amazon Elastic Container Service – 若要產生可改善 DevOpsGuru 資源涵蓋範圍的其他指標，請遵循在 Amazon ECS 上設定容器洞見的步驟。這樣做可能會產生 Amazon CloudWatch 費用。
- Amazon Elastic Kubernetes Service – 若要為 DevOpsGuru 產生要分析的指標，請遵循在 Amazon EKS 和 Kubernetes 上設定容器洞見的步驟。DevOpsGuru 在設定這些指標之前，不會分析任何 Amazon EKS 資源。這樣做可能會產生 Amazon CloudWatch 費用。
- Amazon Simple Storage Service – 若要產生 DevOpsGuru 分析的指標，您必須啟用請求指標。請遵循為儲存貯體中的所有物件建立 CloudWatch 指標組態中的步驟。DevOpsGuru 在設定這些指標之前，不會分析任何 Amazon S3 資源。這樣做可能會產生 CloudWatch 和 Amazon S3 費用。

如需詳細資訊，請參閱 Amazon CloudWatch 定價。

在 DevOps Guru 中使用洞見

當 Amazon DevOps Guru 在營運應用程式中偵測到異常行為時，會產生洞見。DevOps Guru 會分析您在設定 DevOps Guru 時所指定 AWS 資源中的指標、事件等。每個洞見都包含一或多個建議，供您採取以減輕問題。它還包含指標清單、日誌群組清單，以及用於識別異常行為的事件清單。

有兩種洞見類型。

- 被動洞察有您可以採取的建議，以解決目前正在發生的問題。
- 主動洞察的建議可解決 DevOps Guru 預測未來將發生的問題。

主題

檢視 DevOps Guru 洞見

您可以使用 檢視您的洞見 AWS 管理主控台。

檢視您的 DevOps Guru 洞見

1. 開啟位於 https：//https://console.aws.amazon.com/devops-guru/ 的 Amazon DevOps Guru 主控台。
2. 開啟導覽窗格，然後選擇 Insights。
3. 在被動索引標籤上，您可以看到被動洞察的清單。在主動標籤上，您可以看到主動洞察的清單。
4. （選用）使用下列一或多個篩選條件來尋找您要尋找的洞見。
   - 根據您要尋找的洞見類型，選擇被動或主動索引標籤。
   - 選擇篩選條件洞察，然後選擇一個選項來指定篩選條件。您可以新增狀態、嚴重性、資源和標籤篩選條件的組合。使用 AWS 標籤篩選條件，僅檢視具有特定標籤的資源所產生的洞見。如需詳細資訊，請參閱 使用標籤來識別 DevOps Guru 應用程式中的資源。

> **Note**
>
> DevOps Guru 可以分析下列資源，但無法使用標籤篩選其洞見。
>
> - Amazon API Gateway 路徑和路由
> - Amazon DynamoDB Streams
> - Amazon EC2 Auto Scaling 群組執行個體
> - AWS Elastic Beanstalk 環境
> - Amazon Redshift 節點

- 選擇要依洞見建立時間篩選的時間範圍。
  - 12 小時顯示過去 12 小時內建立的洞見。
  - 1d 顯示過去一天建立的洞見。
  - 1w 顯示過去一週建立的洞見。
  - 1m 顯示上個月建立的洞見。
  - 自訂可讓您指定另一個時間範圍。您可用來篩選洞見的時間範圍上限為 180 天。

5. 若要檢視洞見的詳細資訊，請選擇其名稱。

了解 DevOps Guru 主控台中的洞見

使用 Amazon DevOps Guru 主控台檢視洞見中的實用資訊，以協助您診斷和解決異常行為。當 DevOps Guru 分析您的資源，並尋找指出異常行為的相關 Amazon CloudWatch 指標、 AWS CloudTrail 事件和操作資料時，它會建立洞見，其中包含解決相關指標和事件的問題和資訊的建議。搭配 使用洞見資料DevOpsGuru 的最佳實務，以解決 DevOps Guru 偵測到的操作問題。

若要檢視洞見，請依照 中的步驟檢視洞見尋找洞見，然後選擇其名稱。洞見頁面包含下列詳細資訊。

Insight 概觀

使用本節來取得洞見的高階概觀。您可以查看洞見的狀態 (進行中或已關閉)、受影響的 CloudFormation 堆疊數量、洞見開始、結束和上次更新的時間，以及如果有的話的相關操作項目。

如果洞見在堆疊層級分組，您可以選擇受影響的堆疊數量來查看其名稱。建立洞見的異常行為發生在受影響堆疊建立的資源中。如果洞見在帳戶層級分組，則數字為零或不會顯示。

如需詳細資訊，請參閱了解異常行為如何分組為洞見。

洞見名稱

洞見的名稱取決於是在堆疊層級或帳戶層級進行分組。

- 堆疊層級洞見名稱包含堆疊的名稱，其中包含具有異常行為的資源。
- 帳戶層級洞見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分組為洞見。

彙總指標

選擇彙總指標索引標籤，以檢視與洞見相關的指標。在表格中，每一列代表一個指標。您可以查看哪個 CloudFormation 堆疊建立了發出指標的資源、資源的名稱及其類型。並非所有指標都與 CloudFormation 堆疊相關聯或具有名稱。

當同時有多個資源異常時，時間軸檢視會彙總資源，並在單一時間軸中呈現其異常指標，以便於分析。時間軸上的紅線表示指標發出異常值的時間範圍。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。在開啟的視窗中，您可以：

- 選擇在 CloudWatch 中檢視，即可在 CloudWatch 主控台中查看指標的外觀。如需詳細資訊，請參閱《Amazon CloudWatch 使用者指南》中的統計資料和維度。
- 將滑鼠游標暫留在圖表上，以檢視異常指標資料的詳細資訊，以及何時發生。
- 選擇具有向下箭頭的方塊，以下載圖形的 PNG 影像。

圖形異常

選擇圖形異常索引標籤，以檢視每個洞見的異常的詳細圖形。每個異常都會出現一個圖磚，其中包含相關指標中偵測到的異常行為的詳細資訊。您可以調查並查看資源層級和每個統計資料的異常。圖形會依指標名稱分組。在每個圖磚中，您可以選擇時間軸中要縮放的特定時間範圍。您也可以使用放大和縮小放大鏡圖示，或以小時、天或週為單位選擇預先定義的持續時間 (1H、3H、12H、1D、3D、1W 或 2W)。

選擇檢視所有統計資料和維度，以查看異常的詳細資訊。在開啟的視窗中，您可以：

- 選擇在 CloudWatch 中檢視，即可在 CloudWatch 主控台中查看指標的外觀。
- 將滑鼠游標暫留在圖表上，以檢視異常指標資料的詳細資訊，以及何時發生。
- 選擇統計資料或維度來自訂圖形的顯示。如需詳細資訊，請參閱《Amazon CloudWatch 使用者指南》中的統計資料和維度。

日誌群組

當您啟用日誌異常偵測時，DevOps Guru 會標記您的 CloudWatch 日誌群組，以便您可以檢視與洞見相關的日誌群組。在洞見詳細資訊頁面上的日誌群組區段中，資料表中的每一列代表一個日誌群組並列出相關資源。

當同時有多個異常日誌群組時，時間軸檢視會彙總它們，並以單一時間軸呈現它們，以便於分析。時間軸上的紫色線條表示日誌群組遇到日誌異常的時間範圍。

在時間軸中選擇紫色行，以檢視日誌異常資訊的範例，例如關鍵字例外狀況和數值偏差。選擇檢視日誌群組詳細資訊以檢視日誌異常。在開啟的視窗中，您可以：

- 檢視日誌異常和相關事件的圖表。
- 將滑鼠游標暫留在圖表上，以檢視異常日誌資料的詳細資訊，以及日誌資料發生的時間。
- 詳細檢視日誌異常，其中包含範例訊息、發生頻率、相關建議和發生時間。
- 按一下在 CloudWatch 中檢視詳細資訊，以檢視日誌異常中的日誌行。

相關事件

在相關事件中，檢視與您的洞見相關的 AWS CloudTrail 事件。使用這些事件來協助了解、診斷和解決異常行為的根本原因。

建議

在建議中，您可以檢視可能有助於解決基礎問題的建議。當 DevOps Guru 偵測到異常行為時，它會嘗試建立建議。洞見可能包含一個、多個或零個建議。

了解異常行為如何分組為洞見

洞見會在堆疊層級或帳戶層級分組。如果為堆疊中的 AWS CloudFormation 資源產生洞見，則它是堆疊層級洞見。否則，它是帳戶層級洞見。

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

如果您的涵蓋範圍是由 CloudFormation 堆疊定義

您選擇的堆疊中包含的所有資源都會進行分析，所有偵測到的洞見都會在堆疊層級分組。

如果您的涵蓋範圍是您目前的 AWS 帳戶和區域

分析您帳戶和區域中的所有資源，偵測到的洞見有三種可能的分組案例。

- 從不屬於堆疊的資源產生的洞見會在帳戶層級分組。

- 從前 10，000 個已分析堆疊之一的資源產生的洞見會在堆疊層級分組。
- 從不在前 10，000 個分析堆疊之一的資源產生的洞見會在帳戶層級分組。例如，針對第 10，001 個分析堆疊中資源產生的洞見會在帳戶層級分組。

如需詳細資訊，請參閱判斷 DevOps Guru 的涵蓋範圍。

了解洞見嚴重性

洞見可以有三種嚴重性之一：高、中或低。Amazon DevOps Guru 在偵測到相關異常並為每個異常指派嚴重性之後，會建立洞見。DevOps Guru 會使用網域知識和多年的集體經驗，將高、中或低嚴重性指派給異常狀況。洞見的嚴重性取決於有助於建立洞見的最嚴重異常。

- 如果產生洞見的所有異常的嚴重性很低，則洞見的嚴重性很低。
- 如果產生洞見的所有異常的最高嚴重性為中等，則洞見的嚴重性為中等。產生洞見的一些異常的嚴重性可能很低。
- 如果產生洞見的所有異常的最高嚴重性都很高，則洞見的嚴重性很高。產生洞見的一些異常的嚴重性可能很低或中等。

使用 DevOps Guru 監控資料庫

DevOps Guru 為 上的操作資料庫提供了顯著的值 AWS。透過利用其機器學習演算法，DevOps Guru 可協助最佳化資料庫效能、改善可靠性，並減少營運開銷。使用者指南的本節提供這些資料庫功能的高階概觀，包括不同 AWS 資料庫服務的特定 DevOps Guru 使用案例。

DevOps Guru 可以提供關聯式資料庫的洞見，例如 Amazon RDS 和 Amazon Redshift。它也可以為 Amazon DynamoDB 和 等非關聯式或 NoSQL 資料庫提供洞見 Amazon ElastiCache。

主題

使用 DevOps Guru 監控關聯式資料庫

DevOps Guru 從兩個主要資料來源提取，以尋找關聯式資料庫中的洞見和異常。對於 Amazon RDS 和 Amazon Redshift，CloudWatch 提供的指標會針對所有執行個體類型進行分析。對於 Amazon RDS，績效詳情資料也會擷取下列引擎類型：RDS for PostgreSQL、Aurora PostgreSQL 和 Aurora MySQL。

在 Amazon RDS 中監控資料庫操作

本節包含 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 vended 指標和績效詳情的資料。如需 DevOps Guru for RDS 的詳細資訊，包括關鍵概念、組態和優點，請參閱 the section called “在 DevOps Guru for RDS 中使用異常”。

使用來自 CloudWatch vended 指標的資料監控 RDS

DevOps Guru 能夠透過擷取預設 CloudWatch 指標來監控每種類型的 RDS 執行個體，例如 CPU 使用率和讀取和寫入操作延遲。由於這些指標預設為 ，因此當您使用 DevOps Guru 監控 RDS 執行個體時，不需要進一步的組態即可取得洞見。DevOps Guru 會根據歷史模式自動建立這些指標的基準，並將其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 CloudWatch 提供之指標中 Amazon RDS 的潛在被動洞察清單。

AWS DevOps Guru 監控的資源	DevOps Guru 識別的案例	監控的 CloudWatch 指標
Amazon RDS （所有執行個體類型）	CPU 或記憶體達到限制	DBLoad、DBLoadCPU
RDS for PostgreSQL	高複寫槽延遲	OldestReplicationSlotLag

DevOps Guru 監控的 Amazon RDS 執行個體的其他 CloudWatch 已提供指標：

- CPUUtilization
- DatabaseConnections
- DiskQueueDepth
- FailedSQLServerAgentJobsCount
- ReadLatency
- ReadThroughput
- ReplicaLag
- WriteLatency

使用績效詳情中的資料監控 RDS

對於某些類型的 Amazon RDS 執行個體，例如 Aurora PostgreSQL、Aurora MySQL 和 RDS for PostgreSQL，您可以透過確保在這些執行個體上啟用績效詳情，從 DevOps Guru 監控中釋放更多功能。

DevOps Guru 提供各種情況的被動洞察，包括下列案例：

DevOps Guru 識別來產生被動洞見的案例
鎖定爭用問題
缺少索引
應用程式集區的設定錯誤
次佳 JDBC 預設值

DevOps Guru 為各種情況提供主動洞察，包括下列案例：

AWS DevOps Guru 監控的資源	DevOps Guru 識別來產生主動洞見的案例
Aurora MySQL	InnoDB 歷史記錄清單太大，可能導致效能降低，例如資料庫關閉時間過長
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
RDS for PostgreSQL、Aurora PostgreSQL	在交易中閒置太久、保留鎖定、封鎖其他查詢以及防止清空（包括自動清空）清除無效資料列的潛在影響的連線

在 中監控資料庫操作 Amazon Redshift

DevOps Guru 能夠透過擷取預設 CloudWatch 指標來監控您的 Amazon Redshift 資源，包括 CPU 使用率和使用的磁碟空間百分比。由於這些指標是預設提供，DevOps Guru 不需要進一步的組態即可自動監控您的 Amazon Redshift 資源。DevOps Guru 會根據歷史模式建立這些指標的基準，並將其與即時資料進行比較，以偵測異常。

DevOps Guru 識別的案例	監控的 CloudWatch 指標
偵測叢集工作負載、扭曲和未排序資料或領導節點任務等因素所造成的 Amazon Redshift 執行個體高 CPU 使用率	CPUUtilization
偵測 Amazon Redshift 執行個體何時因為查詢處理、分佈和排序金鑰、維護操作或 tombstone 區塊的問題而用盡磁碟空間	PercentageDiskSpaceUsed

DevOps Guru 監控之 Amazon Redshift 執行個體的其他 CloudWatch 提供指標：

- DatabaseConnections
- HealthStatus
- MaintenanceMode

- NumExceededSchemaQuotas
- PercentageQuotaUsed
- QueryDuration
- QueryRuntimeBreakdown
- ReadIOPS
- ReadLatency
- WLMQueueLength
- WLMQueueWaitTime
- WLMQueryDuration
- WriteLatency

在 DevOps Guru for RDS 中使用異常

DevOps Guru 會偵測、分析支援 AWS 的資源並提供建議，包括 Amazon RDS 引擎。對於開啟績效詳情的 Amazon Aurora 和 RDS for PostgreSQL 資料庫執行個體，DevOps Guru for RDS 會提供效能問題的詳細資料庫特定分析，並建議修正動作。

主題

DevOps Guru for RDS 概觀

您可以在下面找到 DevOps Guru for RDS 的主要優點和功能的摘要。如需洞察和異常的背景，請參閱 DevOps Guru 概念。

主題

DevOps Guru for RDS 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迴歸。得知問題時，您可能不知道為何發生或如何處理。您不需要轉向資料庫管理員 (DBA) 求助，或依賴第三方工具，您可以遵循 DevOps Guru for RDS 的建議。

您可以從 DevOps Guru for RDS 的詳細分析中獲得下列好處：

快速診斷

DevOps Guru for RDS 持續監控並分析資料庫遙測。績效詳情、增強型監控和 Amazon CloudWatch 會收集資料庫執行個體的遙測資料。DevOps Guru for RDS 使用統計和機器學習技術來挖掘此資料並偵測異常。若要進一步了解 Amazon Aurora 資料庫的遙測資料，請參閱《Amazon Aurora 使用者指南》中的使用績效詳情監控資料庫負載和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《Amazon RDS 使用者指南》中的在 Amazon Relational Database Service 上使用 Performance Insights 監控資料庫負載，以及使用增強型監控監控作業系統指標。

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，DevOps Guru for RDS 可能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

DevOps Guru for RDS 會使用資源中的指標，在潛在問題行為變得更嚴重之前進行偵測。例如，它可以偵測連線到資料庫的工作階段何時未執行作用中工作，並且可能會封鎖資料庫資源。DevOps Guru 會接著提供建議，協助您在問題變得更嚴重之前加以解決。

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，DevOps Guru for RDS 依賴機器學習 (ML) 和進階統計分析。Amazon 資料庫工程師以多年來管理數十萬個資料庫的底蘊，努力發展 DevOps Guru for RDS 的研究結果。憑藉此共同知識，DevOps Guru for RDS 可以教導您最佳實務。

資料庫效能調校的重要概念

DevOps Guru for RDS 假設您熟悉幾個關鍵效能概念。若要進一步了解這些概念，請參閱《Amazon Aurora 使用者指南》中的績效詳情概觀或《Amazon RDS 使用者指南》中的績效詳情概觀。

主題

- 指標
- 問題偵測
- 資料庫載入
- 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 即時為資料庫和資料庫執行個體執行所在的作業系統 (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程序資訊。DevOps Guru for RDS 會監控並提供某些這些指標的洞見。如需詳細資訊，請參閱監控 Amazon Aurora 叢集中的指標或監控 Amazon Relational Database Service 執行個體中的指標。

問題偵測

DevOps Guru for RDS 採用資料庫和作業系統 (OS) 指標來偵測關鍵資料庫效能問題，無論這些問題是即將發生還是持續發生。DevOps Guru for RDS 問題偵測有 2 種主要運作方式：

- 使用閾值
- 使用異常

偵測閾值的問題

閾值是評估受監控指標的邊界值。您可以將閾值視為指標圖表上的水平線，將正常行為與潛在有問題的行為分開。DevOps Guru for RDS 會監控特定指標，並透過分析特定資源被視為可能有問題的層級來建立閾值。然後，DevOps Guru for RDS 會在 DevOps Guru 主控台中，當新的指標值在指定期間內超過指定的閾值時，建立洞見。洞見包含防止未來資料庫效能影響的建議。

例如，DevOps Guru for RDS 可能會在 15 分鐘內監控使用磁碟的暫存資料表數量，並在使用每秒磁碟的暫存資料表速率異常高時建立洞見。增加磁碟上暫存資料表用量層級可能會影響資料庫效能。DevOps Guru for RDS 會在此情況變得嚴重之前公開，協助您採取修正動作來預防問題。

偵測異常問題

雖然閾值提供簡單且有效的方法來偵測資料庫問題，但在某些情況下，它們還不夠。假設因為已知的程序，例如每日報告任務，指標值會定期激增並交叉進入潛在有問題的行為。由於這種峰值是預期的，因此為每個峰值建立洞見和通知會具有反效果，並可能導致警示疲勞。

不過，仍然需要偵測高度不尋常的峰值，因為遠高於其餘的指標或持續更長的指標可能代表實際的資料庫效能問題。為了解決這個問題，DevOps Guru for RDS 會監控特定指標，以偵測指標的行為何時變得高度異常或異常。DevOps Guru 接著會在洞見中報告這些異常。

例如，DevOps Guru for RDS 可能會在資料庫負載不高時建立洞見，也大幅偏離其一般行為，這表示資料庫操作的重大意外變慢。透過僅識別異常資料庫負載峰值，DevOps Guru for RDS 可讓您專注於真正重要的問題。

資料庫載入

資料庫調校的關鍵概念是資料庫負載（資料庫負載）指標。資料庫負載代表資料庫在任何指定時間的忙碌程度。資料庫負載增加表示資料庫活動增加。

資料庫工作階段代表應用程式與關聯式資料庫的對話。作用中工作階段是正在執行資料庫請求的工作階段。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 中的指標是以平均作用中工作階段 DBLoad (AAS) 測量。 為了計算 AAS，績效詳情會取樣每秒作用中工作階段的數量。在特定期間內，ASS 是作用中工作階段的總數除以範例總數。AAS 值 2 表示平均而言，2 個工作階段在任何指定時間在請求中處於作用中狀態。

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 100 個或更多訂單進來，所有 100 個工作者都會同時履行訂單。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

等待事件是一種資料庫檢測，會告訴您資料庫工作階段正在等待哪個資源，以便繼續。當績效詳情計算作用中工作階段以計算資料庫負載時，也會記錄導致作用中工作階段等待的等待事件。此技術可讓 Performance Insights 顯示哪些等待事件導致資料庫載入。

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耗用 CPU。當工作階段未使用 CPU 時，他們可能會等待資料檔案讀取或日誌寫入。工作階段等待資源越久，在 CPU 上執行的時間就越短。

當您調校資料庫時，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。如果您可以找出這些等待的原因，您可以嘗試解決問題。

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，不同的工作者目前可能正在重新存放架子，或無法使用手拉車。或者，用來輸入訂單狀態的系統可能很慢。工作者等待的時間越長，訂單完成的時間就越長。等待是倉儲工作流程的自然部分，但如果等待時間過長，生產力就會降低。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 Amazon Aurora 中等待事件的詳細資訊，請參閱《Amazon Aurora 使用者指南》中的使用 Aurora PostgreSQL 的等待事件進行調校和使用 Aurora MySQL 的等待事件進行調校。

如需其他 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》中的使用 RDS for PostgreSQL 的等待事件進行調校。

DevOps Guru for RDS 的重要概念

當 DevOps Guru 在營運應用程式中偵測到異常或有問題的行為時，會產生洞見。洞見包含一或多個資源的異常。異常表示 DevOps Guru 偵測到的一個或多個未預期或不尋常的相關指標。

洞見的嚴重性為高、中或低。洞見嚴重性取決於有助於建立洞見的最嚴重異常。例如，如果洞見 AWS-ECS_MemoryUtilization_and_others 包含一個低嚴重性的異常，以及另一個高嚴重性的異常，洞見的整體嚴重性很高。

如果 Amazon RDS 資料庫執行個體已開啟績效詳情，DevOps Guru for RDS 會在這些執行個體的異常中提供詳細的分析和建議。為了識別異常，DevOps Guru for RDS 開發資料庫指標值的基準。DevOps Guru for RDS 接著會將目前的指標值與歷史基準進行比較。

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，協助您在問題變得更大之前解決問題。

每個主動洞察頁面都會提供有關一個異常的詳細資訊。

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，以協助您立即了解並解決問題。

因果異常

因果異常是反應式洞察中最高等級的異常。它在 DevOps Guru 主控台的異常詳細資訊頁面上顯示為主要指標。資料庫負載（資料庫負載）是 DevOps Guru for RDS 的因果異常。例如，洞見 AWS-ECS_MemoryUtilization_and_others 可能有數個指標異常，其中一個是資源 AWS/RDS 的資料庫負載（資料庫負載）。

在洞見中，多個 Amazon RDS 資料庫執行個體可能發生異常資料庫載入（資料庫載入）。每個資料庫執行個體的異常嚴重性可能不同。例如，一個資料庫執行個體的嚴重性可能很高，其他資料庫執行個體的嚴重性則很低。主控台預設為具有最高嚴重性的異常。

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訊頁面的相關指標區段中。每個情境異常都會描述需要調查的特定 Amazon RDS 效能問題。例如，因果異常可包含下列情境異常：

- 超過 CPU 容量 – CPU 執行佇列或 CPU 使用率高於正常。
- 資料庫記憶體不足 – 程序沒有足夠的記憶體。
- 資料庫連線峰值 – 資料庫連線的數量高於正常。

建議

每個洞見至少有一個建議的動作。下列範例是由 DevOps Guru for RDS 產生的建議：

- 調校 SQL IDs *list_of_IDs* 以減少 CPU 用量，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關聯尖峰。請考慮調校應用程式集區設定，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操作的 SQL 陳述式，例如記憶體內排序或大型聯結。
- 調查下列 SQL IDs的繁重 I/O 用量：*list_of_IDs*。
- 檢查建立大量暫存資料的陳述式，例如執行大量排序或使用大型暫存資料表的陳述式。
- 檢查應用程式以查看導致資料庫工作負載增加的原因。
- 考慮啟用 MySQL 效能結構描述。

- 檢查是否有長時間執行的交易，並以遞交或轉返結束交易。
- 設定 idle_in_transaction_session_timeout 參數，以結束超過指定時間處於「交易」狀態的任何工作階段。

DevOps Guru for RDS 的運作方式

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

主題

- 資料收集和分析
- 異常發佈

資料收集和分析

DevOps Guru for RDS 會從 Amazon RDS Performance Insights 收集 Amazon RDS 資料庫的資料。此功能會監控 Amazon RDS 資料庫執行個體、收集指標，並可讓您探索圖表中的指標。最重要的效能指標是 DBLoad。DevOps Guru for RDS 會耗用績效詳情指標，並加以分析以偵測異常。如需績效詳情的詳細資訊，請參閱《Amazon Aurora 使用者指南》中的使用績效詳情監控資料庫負載，或《Amazon RDS 使用者指南》中的使用績效詳情監控資料庫負載。

DevOps Guru for RDS 使用機器學習和進階統計分析來分析從績效詳情收集的資料。如果 DevOps Guru for RDS 發現效能問題，則會繼續進行下一個步驟。

異常發佈

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 在 RDS 資料庫中偵測到問題時，它會在儀表板中發佈洞見。洞見包含資源 AWS/RDS 的異常。

如果您的執行個體已開啟績效詳情，則異常狀況會包含問題的詳細分析。DevOps Guru for RDS 也建議您執行調查或特定修正動作。例如，建議可能是調查特定高負載 SQL 陳述式、考慮增加 CPU 容量，或關閉idle-in-transaction工作階段。

支援的資料庫引擎

下列資料庫引擎支援 DevOps Guru for RDS：

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 相容性

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 。

DevOps Guru 會報告異常並提供其他資料庫引擎的基本分析。DevOps Guru for RDS 僅針對 Amazon Aurora 和 RDS for PostgreSQL 執行個體提供詳細的分析和建議。

啟用 DevOps Guru for RDS

當您啟用 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 可讓您輕鬆探索和啟用 RDS 資料庫執行個體或資料庫叢集的建議功能。為了達成此目的，RDS 會呼叫其他 服務，例如 Amazon EC2、DevOps Guru 和 IAM。當 RDS 主控台進行這些 API 呼叫時， 會 AWS CloudTrail 記錄這些呼叫以供查看。

若要允許 DevOps Guru 發佈 Amazon RDS 資料庫的洞見，請完成以下章節中的任務。

主題

- 為您的 Amazon RDS 資料庫執行個體開啟績效詳情
- 設定 DevOps Guru for RDS 的存取政策
- 將 Amazon RDS 資料庫執行個體新增至 DevOps Guru 涵蓋範圍

為您的 Amazon RDS 資料庫執行個體開啟績效詳情

若要讓 DevOps Guru for RDS 分析資料庫執行個體上的異常，請確定績效詳情已開啟。如果資料庫執行個體的績效詳情未開啟，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洞見，RDS 圖標會提醒您未開啟績效詳情。選擇連結以在 Amazon RDS 主控台中開啟績效詳情。

洞見

在頁面底部的建議區段中，選擇啟用 Amazon RDS 績效詳情。

設定

在服務：Amazon RDS 區段中，選擇連結以在 Amazon RDS 主控台中開啟績效詳情。

如需詳細資訊，請參閱《Amazon Aurora 使用者指南》中的開啟和關閉績效詳情，或《Amazon RDS 使用者指南》中的開啟和關閉績效詳情。

設定 DevOps Guru for RDS 的存取政策

若要讓使用者存取 DevOps Guru for RDS，他們必須具有下列任一政策的許可：

- 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》中的設定績效詳情的存取政策，或《Amazon RDS 使用者指南》中的設定績效詳情的存取政策。

將 Amazon RDS 資料庫執行個體新增至 DevOps Guru 涵蓋範圍

您可以設定 DevOps Guru 在 DevOps Guru 主控台或 Amazon RDS 主控台中監控 Amazon RDS 資料庫。

在 DevOps Guru 主控台中，您有下列選項：

- 在帳戶層級開啟 DevOps Guru。這是預設值。當您選擇此選項時，DevOps Guru 會分析 AWS 區域和 中的所有支援 AWS 資源 AWS 帳戶，包括 Amazon RDS 資料庫。
- 為 DevOps Guru for RDS 指定 AWS CloudFormation 堆疊。

  如需詳細資訊，請參閱使用 CloudFormation 堆疊來識別 DevOps Guru 應用程式中的資源。
- 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您應用程式 AWS 的資源。然後，您可以依標籤篩選洞見，僅檢視應用程式建立的洞見。若要僅檢視應用程式中 Amazon RDS 資源所產生的洞見，請將 等值新增至`Devops-guru-rds`您的 Amazon RDS 資源標籤。如需詳細資訊，請參閱使用標籤來識別 DevOps Guru 應用程式中的資源。

> **Note**
>
> 當您標記 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 Guru 監控，請參閱 RDS 主控台中的開啟 DevOps Guru。請注意，若要從 Amazon RDS 主控台啟用 DevOps Guru，您必須使用標籤。如需標籤的詳細資訊，請參閱the section called “使用標籤來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 儀表板中檢視洞見。DevOps Guru for RDS 會報告被動和主動洞察。

   如需詳細資訊，請參閱檢視洞見。
2. 檢視 AWS/RDS 資源的異常。

   如需詳細資訊，請參閱檢視被動異常及檢視主動異常。
3. 回應 DevOps Guru 以取得 RDS 建議。

   如需詳細資訊，請參閱回應建議。
4. 監控資料庫執行個體的運作狀態，以確保已解決的效能問題不會再次發生。

   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，以及《Amazon RDS 使用者指南》中的監控 Amazon RDS 執行個體中的指標。

檢視洞見

存取 DevOps Guru 主控台中的洞見頁面，尋找被動和主動的洞見。您可以從清單中選擇洞見，以檢視指標、建議和洞見詳細資訊的詳細頁面。

檢視洞見

1. 開啟位於 https：//https://console.aws.amazon.com/devops-guru/ 的 Amazon DevOps Guru 主控台。
2. 開啟導覽窗格，然後選擇 Insights。
3. 選擇被動索引標籤來檢視被動洞察，或選擇主動來檢視主動洞察。

4. 選擇洞見的名稱，依狀態和嚴重性排定優先順序。

   詳細的洞見頁面隨即出現。

檢視被動異常

在洞見中，您可以檢視 Amazon RDS 資源的異常。在被動洞察頁面上，在彙總指標區段中，您可以檢視具有對應時間軸的異常清單。也有部分顯示與異常相關的日誌群組和事件資訊。被動洞察中的因果異常各有對應的頁面，其中包含異常的詳細資訊。

檢視 RDS 反應異常的詳細分析

在此階段，深入探討異常狀況，以取得 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績效詳情的 Amazon RDS 資料庫執行個體。

向下切入異常詳細資訊頁面

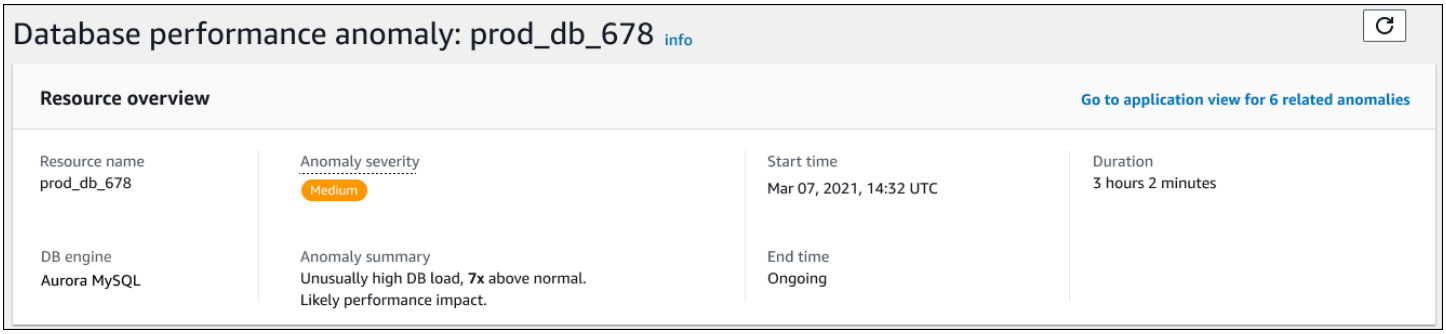
1. 在洞見頁面上，尋找資源類型為 AWS/RDS 的彙總指標。
2. 請選擇檢視詳細資料。

   出現異常詳細資訊頁面。標題開頭為資料庫效能異常，以及資源顯示的名稱。無論異常何時發生，主控台都會預設為嚴重性最高的異常。
3. （選用）如果多個資源受到影響，請從頁面頂端的清單中選擇不同的資源。

您可以在下面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。本節摘要說明 Amazon RDS 資料庫執行個體遇到的效能異常情況。

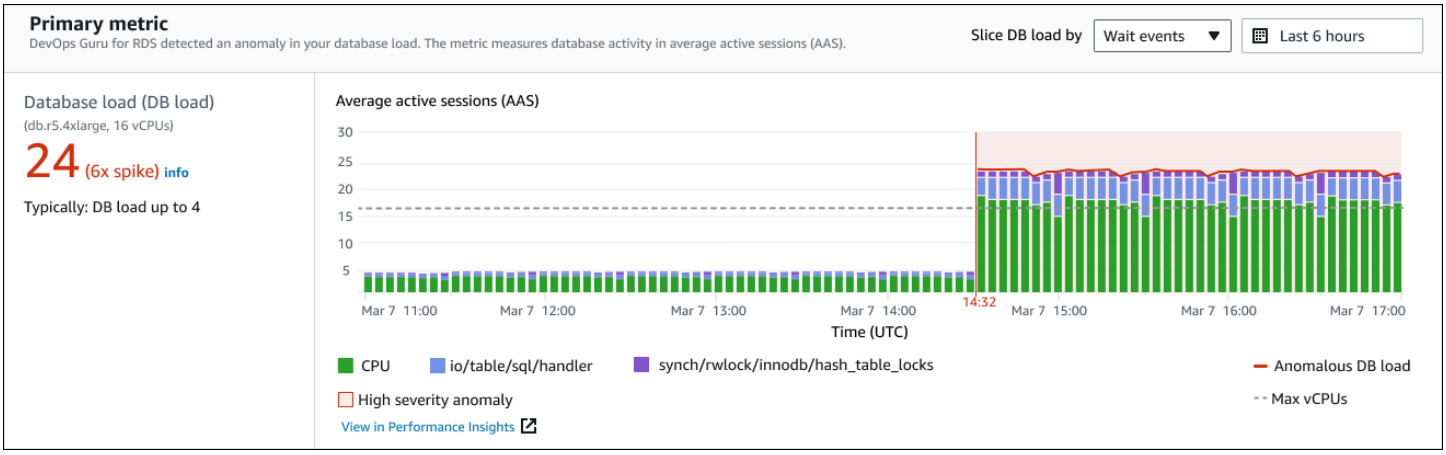


本節包含下列欄位：

- 資源名稱 – 遇到異常的資料庫執行個體名稱。在此範例中，資源名為 prod_db_678。
- 資料庫引擎 – 遇到異常的資料庫執行個體名稱。在此範例中，引擎為 Aurora MySQL。
- 異常嚴重性 – 異常對執行個體的負面影響度量。可能的嚴重性為高、中和低。
- 異常摘要 – 問題的簡短摘要。典型的摘要是異常高的資料庫負載。
- 開始時間和結束時間 – 異常開始和結束的時間。如果結束時間為進行中，表示仍發生異常。
- 持續時間 – 異常行為的持續時間。在此範例中，異常持續發生 3 小時又 2 分鐘。

主要指標

主要指標區段摘要說明意外異常，這是洞見中最上層的異常。您可以將因果異常視為資料庫執行個體遇到的一般問題。



左側面板提供有關問題的更多詳細資訊。在此範例中，摘要包含下列資訊：

- 資料庫載入 （資料庫載入） – 異常分類為資料庫載入問題。績效詳情中的對應指標為 DBLoad。此指標也會發佈至 Amazon CloudWatch。
- db.r5.4xlarge – 資料庫執行個體類別。vCPUs 的數量，在此範例中為 16，對應至平均作用中工作階段 (AAS) 圖表中的虛線。
- 24 (6 倍峰值） – 資料庫負載，在洞見中報告的時間間隔內以平均作用中工作階段 (AAS) 測量。因此，在異常期間的任何指定時間，資料庫中平均有 24 個工作階段處於作用中狀態。資料庫負載是此執行個體正常資料庫負載的 6 倍。
- 一般而言：資料庫負載最多 4 – 在一般工作負載期間，以 AAS 測量的資料庫負載基準。值 4 表示在正常操作期間，資料庫上在任何指定時間平均有 4 個或更少的工作階段處於作用中狀態。

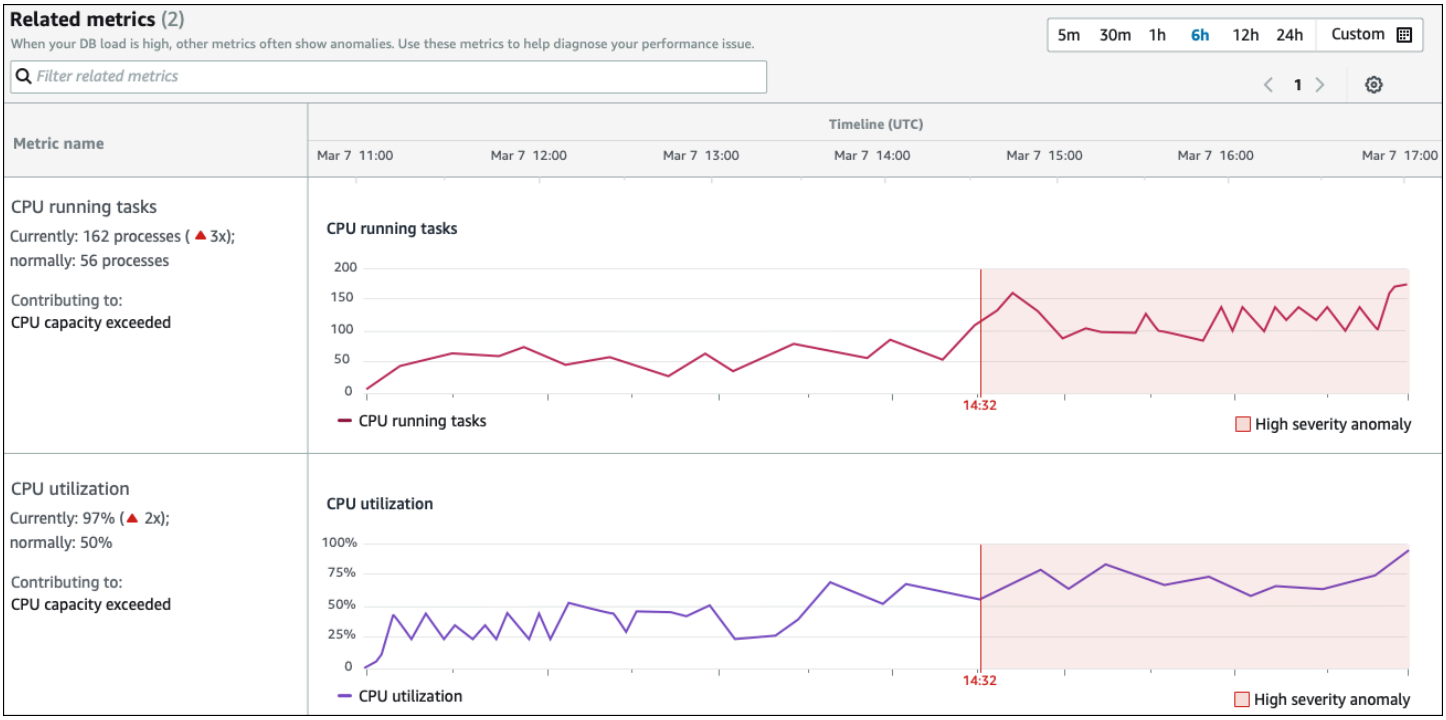
根據預設，負載圖表會依等待事件進行分割。這表示圖表中每個長條的最大彩色區域代表對總資料庫負載貢獻最大的等待事件。圖表顯示問題開始的時間（紅色）。將您的注意力集中在長條中佔用最多空間的等待事件上：

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

此 Aurora MySQL 資料庫出現的上述等待事件超過正常值。若要了解如何使用 Amazon Aurora 中的等待事件調校效能，請參閱《Amazon Aurora 使用者指南》中的使用 Aurora MySQL 的等待事件調校和使用 Aurora PostgreSQL 的等待事件調校。若要了解如何使用 RDS for PostgreSQL 中的等待事件來調校效能，請參閱《Amazon RDS 使用者指南》中的使用 RDS for PostgreSQL 的等待事件進行調校。

相關指標

相關指標區段列出情境異常，這是因果異常中的特定問題清單。這些調查結果提供有關效能問題的其他資訊。



相關指標資料表有兩個資料欄：指標名稱和時間軸 (UTC)。資料表中的每一列都對應至特定指標。

每一列的第一欄包含下列資訊：

- ## – 指標的名稱。第一列會將指標識別為 CPU 執行中的任務。

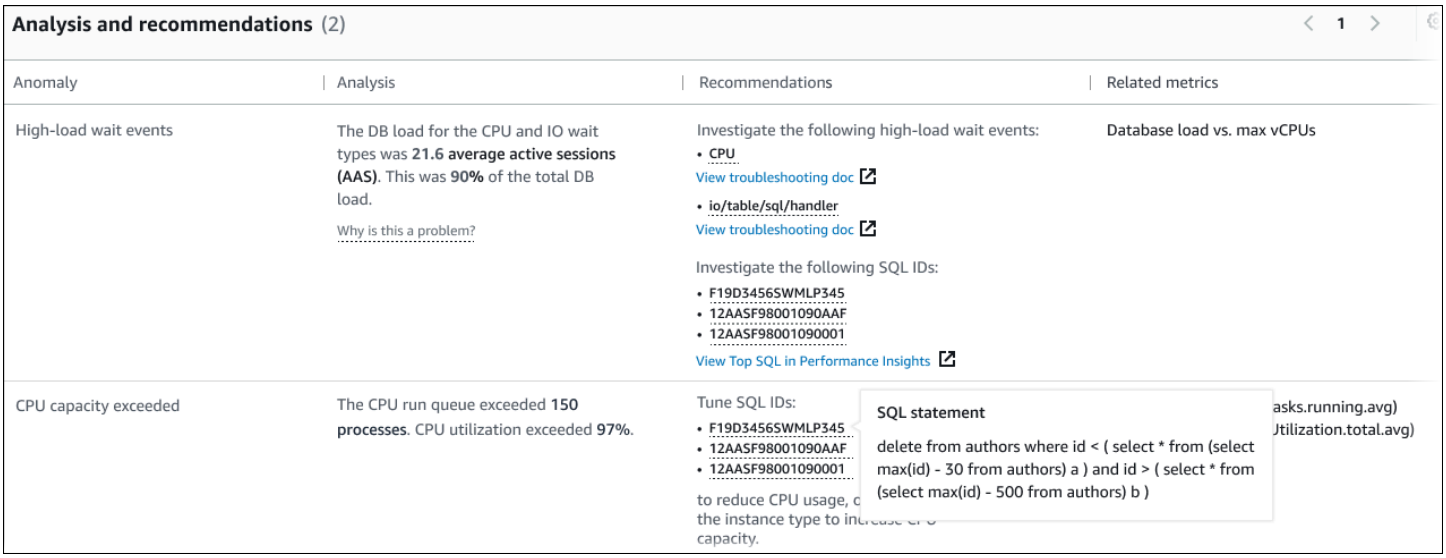
- 目前 – 指標的目前值。在第一列中，目前值為 162 個處理程序 (3x)。
- 正常 – 此資料庫正常運作時，此指標的基準。DevOps Guru for RDS 會將基準計算為 1 週內的第 95 個百分位數值。第一列指出 56 個程序通常在 CPU 上執行。
- 貢獻至 - 與此指標相關聯的調查結果。在第一列中，CPU 執行中的任務指標與超過異常的 CPU 容量相關聯。

時間軸欄會顯示指標的折線圖。陰影區域會顯示 DevOps Guru for RDS 將調查結果指定為高嚴重性時的時間間隔。

分析和建議

雖然因果異常描述了整體問題，但情境異常描述了需要調查的特定調查結果。每個調查結果對應於一組相關指標。

在分析和建議區段的下列範例中，高資料庫負載異常有兩個問題清單。



資料表包含以下資料行：

- 異常 – 此情境異常的一般描述。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 – 異常的詳細說明。

  在第一個異常中，三種等待類型會導致 90% 的資料庫負載。在第二個異常中，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%，這表示在問題發生期間，CPU 有 97% 的時間忙碌。因此，CPU 幾乎持續佔用，而平均有 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。

  在第一個異常中，DevOps Guru for RDS 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/table/sql/handler。

  在第二個異常中，DevOps Guru for RDS 建議您透過調校三個 SQL 陳述式來減少 CPU 使用量。您可以將滑鼠游標暫留在連結上以查看 SQL 文字。
- 相關指標 – 為您提供異常特定測量的指標。如需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。

  在第一個異常中，DevOps Guru for RDS 建議將資料庫負載與執行個體的最大 CPU 進行比較。在第二個異常中，建議查看 CPU 執行佇列、CPU 使用率和 SQL 執行率。

檢視主動異常

在洞見中，您可以檢視 Amazon RDS 資源的異常。每個主動洞察都提供有關一種主動異常的詳細資訊。在主動洞察頁面上，您可以檢視洞察概觀、有關異常的詳細指標，以及防止未來問題的建議。若要檢視主動異常，請前往主動洞察頁面。

Insight 概觀

Insight 概觀區段提供有關為何建立洞見的詳細資訊。它會顯示洞見的嚴重性，以及異常的描述，以及異常發生的時間範圍。它還列出了 DevOps Guru 偵測到的受影響服務和應用程式的數量。

指標

指標區段提供異常的圖形。每個圖形會顯示由資源的基準行為決定的閾值，以及從異常時回報的指標資料。

彙總資源的建議

本節建議您可以在問題變成更大的問題之前，採取哪些動作來緩解回報的問題。您可以採取的動作會顯示在建議的自訂變更欄中。DevOps DevOps Guru 建議此行的原因如下：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

建議是洞見中最重要的部分。在此階段的分析中，您會採取行動來解決效能問題。一般而言，您會採取下列步驟：

1. 判斷報告的效能問題是否表示實際問題。

   在某些情況下，問題可能是預期且良性的。例如，如果您讓測試資料庫承受極端資料庫負載，DevOps Guru for RDS 會將負載報告為效能異常。不過，您不需要修正此異常，因為這是您測試的預期結果。

   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，資料欄會顯示建議的動作。對於被動洞察，這是我們建議在被動異常詳細資訊頁面上的資料欄。對於主動洞察，這是主動洞察頁面上的建議自訂變更欄。

   DevOps Guru for RDS 提供涵蓋多種潛在有問題案例的建議清單。檢閱此清單後，請判斷哪個建議與您目前的情況更相關，並考慮套用該建議。如果建議適用於您的情況，請前往下一個步驟。如果沒有，請略過剩餘的步驟，並使用手動技術對問題進行疑難排解。

3. 執行建議的動作。

   DevOps Guru for RDS 建議您執行下列其中一項操作：

   - 執行特定的修正動作。

     例如，DevOps Guru for RDS 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，DevOps Guru for RDS 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`。請參閱《Amazon Aurora 使用者指南》中的使用 Aurora PostgreSQL 的等待事件調校或使用 Aurora MySQL 的等待事件調校中列出的等待事件，或《Amazon RDS 使用者指南》中的使用 RDS for PostgreSQL 的等待事件調校中列出的等待事件。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 DevOps Guru 監控非關聯式資料庫

DevOps Guru 能夠為非關聯式或 NoSQL 資料庫產生洞見，協助您根據最佳實務設定資源。例如，DevOps Guru 可根據現有流量預測未來需求，協助您掌握容量規劃。DevOps Guru 可以識別您是否使用的資源少於您設定的資源，並根據您的歷史用量提供改善應用程式可用性的建議。這可協助您降低不必要的成本。

除了容量規劃之外，DevOps Guru 還會偵測並協助您疑難排解操作問題，例如限流、交易衝突、條件式檢查失敗，以及 SDK 參數的改善領域。資料庫通常與多個 服務和資源連接，DevOps Guru CloudFormation 可以根據標記或彙總來關聯您的應用程式結構，以便使用群組進行分析。異常可能涉及受相同解決方案影響的多個資源。DevOps Guru 能夠在不同的資源指標、組態、日誌和事件之間相互關聯。例如，DevOps Guru 可以分析和關聯來自 Lambda 函數的資料，這些函數可能正在從 Amazon DynamoDB 資料表讀取或寫入資料。以這種方式，DevOps Guru 會監控多個相關資源來偵測異常，並為您的資料庫解決方案提供有用的洞見。

在 中監控資料庫操作 Amazon DynamoDB

下表顯示 DevOps Guru 監控的範例案例和洞見 Amazon DynamoDB。

Amazon DynamoDB 使用案例	範例	指標
由於大量的讀取和寫入請求，偵測何時使用大量的 AccountProvisioned ReadCapacityUtilization 和 AccountProvisionedWriteCapacityUtilization。	Amazon DynamoDB 讀取或寫入請求的資料表消耗容量達到資料表層級限制。	AccountProvisioned ReadCapacityUtilization、 AccountProvisionedWriteCapacityUtilization
偵測所提供條件表達式與資料庫中預期不相符之 Amazon DynamoDB 請求中的條件式檢查失敗。	條件式檢查失敗是由資料表中的錯誤資料、嚴格的條件表達式或競爭條件所造成。	ConditionalCheckFailedRequests

在 中監控資料庫操作 Amazon ElastiCache

下表顯示 DevOps Guru 監控的範例案例和洞見 Amazon ElastiCache。

DevOps Guru 識別的案例	監控的 CloudWatch 指標
偵測 Amazon ElastiCache 叢集何時因為叢集上不斷變化的需求而達到 Redis 或 Memcached 的運算限制。	CPUUtilization、En EngineCPUUtilization、Evictions

與 CodeGuru Profiler 整合

本節提供 Amazon DevOpsGuru 如何與 Amazon CodeGuru Profiler 整合的概觀。您可以在 DevOps CodeGuru Guru主控台中，將 CodeGuru Profiler 的建議檢視為洞見。

Amazon DevOpsGuru 與 Amazon CodeGuru Profiler 整合了 EventBridge 受管規則。CodeGuru Profiler 會將事件傳送至 EventBridge。受管規則會路由使用預設事件匯流排傳送的事件。CodeGuru Profiler 的每個傳入事件都是主動異常報告。如需詳細資訊，請參閱使用 EventBridge 搭配 CodeGuru Profiler。

DevOpsGuru 支援使用 EventBridge 的傳入事件。事件表示 DevOpsGuru 已識別的建議有所變更。CodeGuru Profiler 每 24 小時傳送一次活動訊號事件，以顯示事件的連續性。事件附帶 CodeGuru Profiler 建議資訊，以及運算資源的中繼資料。如需事件生命週期的資訊，請參閱 Amazon EventBridge Events。

當您設定 DevOpsGuru 時，DevOps 會在您的帳戶中建立 EventBridge 受管規則，以從其他服務路由事件。此規則路由至 DevOpsGuru。發生傳入事件時，會傳送通知。

事件匯流排會從 DevOpsGuru 等來源接收事件，並將其路由到與該事件匯流排相關聯的規則。如需事件匯流排的詳細資訊，請參閱事件匯流排。

如需某些參數的資訊，請參閱 Amazon EventBridge 事件。

若要在 DevOps Guru中接收 CodeGuru Profiler 洞見，您必須具備下列項目。

- CodeGuru Profiler 必須啟用。如需啟用 CodeGuru Profiler 的資訊，請參閱設定 CodeGuru Profiler。
- 必須啟用 DevOpsGuru。如需啟用 DevOpsGuru 的資訊，請參閱啟用 DevOpsGuru。
- 在 CodeGuru Profiler 和 DevOpsGuru 的相同區域中，必須監控相同的資源。

使用 AWS 資源定義應用程式

Amazon DevOps Guru 會將涵蓋範圍內的資源分組，以指定其分析哪些資源以取得營運洞見。資源會依 CloudFormation 堆疊中的資源或具有標籤的資源分組。您可以在設定 DevOps Guru 時選擇堆疊或標籤。您也可以稍後更新堆疊或標籤。我們建議您將資源群組視為應用程式。例如，您可能擁有用於在一個堆疊中定義之監控應用程式的所有資源。或者，您可以將相同的標籤新增至您在資料庫應用程式中使用的所有資源。定義 DevOps Guru 分析哪些資源的邊界。集合中的所有資源都在此界限內。您帳戶中任何不在資源集合中的資源都超出界限，不會進行分析。如需支援服務和資源的詳細資訊，請參閱 Amazon DevOps Guru 定價。

您可以用三種方式定義涵蓋範圍，其中包含應用程式中的資源。

- 指定 AWS 帳戶和區域中所有支援 AWS 的資源。這會使您的帳戶和區域成為您的資源界限。使用此選項，DevOps Guru 會分析帳戶和區域中每個支援的資源。在一個堆疊中的所有資源都會分組到應用程式中。任何不在堆疊中的資源都會分組到自己的應用程式中。
- 使用 CloudFormation 堆疊來指定應用程式中的資源。堆疊包含使用 產生的資源 CloudFormation。在 DevOps Guru 中，您可以選擇帳戶中的堆疊。您在每個堆疊中選擇的資源會分組到應用程式中。DevOps Guru 會分析堆疊中的所有資源以取得洞見。
- 使用 AWS 標籤來指定應用程式中的資源。 AWS 標籤包含索引鍵和值。在 DevOps Guru 中，選擇一個標籤索引鍵，並選擇性地選擇與該索引鍵配對的一或多個值。您可以使用這些值將資源分組到應用程式中。

如需詳細資訊，請參閱在 DevOps Guru 中更新您的 AWS 分析涵蓋範圍。

主題

- 使用標籤來識別 DevOps Guru 應用程式中的資源
- 使用 CloudFormation 堆疊來識別 DevOps Guru 應用程式中的資源

使用標籤來識別 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 AWS 的資源，並指定要分組以使用選取的標籤索引鍵和標籤值進行監控的資源。您可以在設定 DevOps Guru 或從分析資源頁面選擇編輯分析的資源時編輯這些組態。選取標籤後，您可以選擇您希望 Amazon DevOps Guru 監控的特定標籤金鑰。若要分析帳戶中的所有資源，並使用標籤值將資源分組，請選取所有帳戶資源。若要使用標籤值指定 DevOps Guru 分析的資源，請選取選擇特定標籤值。

> **Note**
>
> 選取所有帳戶資源且沒有標籤值時，沒有標籤索引鍵的資源會分別分組和分析。

您可以使用標籤的金鑰來識別資源，然後使用該金鑰的值，將資源分組到您的應用程式中。例如，您可以使用索引鍵 標記資源devops-guru-applications，然後針對每個應用程式使用具有不同值的索引鍵。您可以使用標籤鍵/值對 devops-guru-applications/database、 devops-guru-applications/cicd和 devops-guru-applications/monitoring 來識別您帳戶中的三個應用程式。每個應用程式都由包含相同標籤鍵值對的相關資源組成。您可以使用其所屬 AWS 的服務，將標籤新增至資源。如需詳細資訊，請參閱將 AWS 標籤新增至 AWS 資源。

將標籤新增至應用程式中的資源後，您可以依產生它們的資源上的標籤來篩選洞見。如需如何使用標籤篩選洞見的詳細資訊，請參閱 檢視 DevOps Guru 洞見。

如需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 應用程式
- 搭配 DevOps Guru 使用標籤
- 將 AWS 標籤新增至 AWS 資源

什麼是 AWS 標籤？

標籤可協助您識別和組織 AWS 資源。許多 AWS 服務支援標記，因此您可以將相同的標籤指派給來自不同 服務的資源，以指出資源相關。例如，您可以將相同的標籤指派給指派給 AWS Lambda 函數的 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 應用程式

若要使用標籤定義 Amazon DevOps Guru 應用程式，請將該標籤新增至您帳戶中構成您應用程式 AWS 的資源。您的標籤包含索引鍵和值。我們建議您將標籤新增至 DevOps Guru 分析且具有相同金鑰的每個 AWS 資源。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，您可以將具有 金鑰的標籤指派給涵蓋範圍界限中的所有`devops-guru-analysis-boundary` AWS 資源。使用該索引鍵使用不同的值來識別您帳戶中的應用程式。您可以針對三個應用程式使用值 `database`、`containers`和 `monitoring` 。如需詳細資訊，請參閱在 DevOps Guru 中更新您的 AWS 分析涵蓋範圍。

如果您使用 AWS 標籤來指定要分析的資源，則只能使用一個索引鍵的標籤。您可以將標籤的金鑰與任何值配對。使用 值將包含金鑰的資源分組到操作應用程式中。

> **Important**
>
> 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，DevOps Guru 使用名為 `devops-guru-rds` 的鍵和名為 `DevOps-Guru-RDS` 的鍵，這兩個鍵作為兩種不同的鍵使用。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`。

搭配 DevOps Guru 使用標籤

指定識別您希望 Amazon DevOps Guru 分析之 AWS 資源的 AWS 標籤，或指定識別要分組之資源的標籤值。這些資源是您的資源涵蓋範圍。您可以選擇一個索引鍵和零或多個值。

選擇您的標籤

1. 開啟位於 https：//https://console.aws.amazon.com/devops-guru/ 的 Amazon DevOps Guru 主控台。
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 分析包含您選擇的標籤的所有資源，請選擇標籤。選擇金鑰，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。具有所選標籤索引鍵的資源會依標籤值分組，如果有的話。沒有此標籤索引鍵的資源會個別分組和分析。

- 選擇特定標籤值 – 系統會分析包含具有所選索引鍵之標籤的所有資源。DevOps Guru 會根據標籤的值將您的資源分組到應用程式中。

5. 選擇儲存。

將 AWS 標籤新增至 AWS 資源

當您指定識別您希望 DevOps Guru 分析之 AWS 資源的 AWS 標籤時，請選擇具有與其相關聯資源的標籤。您可以使用每個資源所屬 AWS 的服務，或使用標籤編輯器，將 AWS 標籤新增至資源。

- 若要使用資源的服務管理標籤，請使用 主控台 AWS Command Line Interface或資源所屬服務的 SDK。例如，您可以標記 Amazon Kinesis 串流資源或 Amazon CloudFront 分發資源。這些是具有可標記之資源的兩個 服務範例。DevOps Guru 可以分析的大多數資源都支援標籤。如需詳細資訊，請參閱《Amazon Kinesis 開發人員指南》中的標記您的串流和《Amazon CloudFront 開發人員指南》中的標記分佈。若要了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**
  >
  > 當您標記 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，依區域中的資源和特定 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者指南》中的標籤編輯器。

當您將標籤新增至資源時，您只能新增金鑰或金鑰和值。例如，您可以devops-guru-為 DevOps 應用程式中的所有資源建立具有 金鑰的標籤。您也可以使用索引鍵 devops-guru-和值 來新增標籤RDS，然後將該索引鍵/值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 資源產生的洞見，這會很有用。

使用 CloudFormation 堆疊來識別 DevOps Guru 應用程式中的資源

您可以使用 AWS CloudFormation 堆疊來指定您希望 DevOps Guru 分析 AWS 的資源。堆疊是以單一單位管理的一組 AWS 資源。您選擇的堆疊中的資源構成您的 DevOps Guru 涵蓋範圍界限。對於您選擇的每個堆疊，會分析其支援資源中的操作資料是否有異常行為。然後，這些問題會分組為相關的異常，以建立洞見。每個洞見都包含一或多個建議，以協助您解決這些問題。您可以指定的堆疊數目上限為 1000。如需詳細資訊，請參閱AWS CloudFormation 《 使用者指南》中的使用堆疊和 在 DevOps Guru 中更新您的 AWS 分析涵蓋範圍。

選擇堆疊後，DevOps Guru 會立即開始分析您新增至堆疊的任何資源。如果您從堆疊移除資源，則不會再分析該資源。

如果您選擇讓 DevOps Guru 分析您帳戶中的所有支援資源（這表示 AWS 您的帳戶和區域是您的 DevOps Guru 涵蓋範圍界限），則 DevOps Guru 會分析並建立帳戶中每個支援資源的洞見，包括堆疊中的資源。從不在堆疊中的資源異常建立的洞見會在帳戶層級分組。如果從堆疊中資源的異常建立洞見，則會在堆疊層級將其分組。如需詳細資訊，請參閱了解異常行為如何分組為洞見。

選擇堆疊供 DevOps Guru 分析

選擇建立資源的 CloudFormation 堆疊，指定您希望 Amazon DevOps Guru 分析的資源。您可以使用 AWS 管理主控台 或 SDK 來執行此操作。

主題

選擇要分析的 DevOps Guru 堆疊（主控台）

您可以使用 主控台新增 AWS CloudFormation 堆疊。

選擇包含要分析之資源的堆疊

1. 開啟位於 https：//https://console.aws.amazon.com/devops-guru/ 的 Amazon DevOps Guru 主控台。
2. 開啟導覽窗格，然後選擇設定。
3. 在 DevOps Guru 分析涵蓋範圍內，選擇管理。
4. 如果您希望 DevOps Guru 分析所選堆疊中的資源，請選擇 CloudFormation 堆疊，然後選擇下列其中一個選項。
   - 所有資源 – 分析您帳戶中堆疊中的所有資源。每個堆疊中的資源都會分組到自己的應用程式中。不會分析您帳戶中任何不在堆疊中的資源。
   - 選取堆疊 – 選取您希望 DevOps Guru 分析的堆疊。您選取的每個堆疊中的資源會分組到自己的應用程式。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。您最多可以選取 1，000 個堆疊。
5. 選擇儲存。

選擇要分析的 DevOps Guru 堆疊 (DevOps Guru SDK)

若要使用 Amazon DevOps Guru SDK 指定 CloudFormation 堆疊，請使用 `UpdateResourceCollection`方法。如需詳細資訊，請參閱《Amazon DevOps Guru API 參考》中的 UpdateResourceCollection。

使用 Amazon EventBridge

Amazon DevOps Guru 與 Amazon EventBridge 整合，以通知您有關洞見和對應洞見更新的特定事件。來自 AWS 服務的事件會以近乎即時的方式交付至 EventBridge。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：

- 叫用 AWS Lambda 函數
- 叫用 Amazon Elastic Compute Cloud 執行命令
- 將事件轉傳至 Amazon Kinesis Data Streams
- 啟用 Step Functions 狀態機器
- 通知 Amazon SNS 或 Amazon SQS

您可以選擇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 AWS 的資源中啟動動作。

- DevOps Guru New Insight Open
- DevOps Guru 新異常關聯
- DevOps Guru Insight 嚴重性已升級
- 已建立 DevOps Guru 新建議
- DevOps Guru Insight 已關閉

DevOps Guru 的事件

以下是 DevOps Guru 的範例事件。盡可能發出事件。若要進一步了解事件模式，請參閱 Amazon EventBridge 或 Amazon EventBridge 事件模式入門。

DevOps Guru New Insight 公開事件

DevOps Guru 開啟新的洞見時，會傳送下列事件。

```
{
    "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"
    }
```

```
  },
```

適用於高嚴重性新 Insight 的自訂範例事件模式

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 DevOps Guru 設定

您可以更新下列 Amazon DevOps Guru 設定：

- 您的 DevOps Guru 涵蓋範圍。這會決定分析您帳戶中的哪些資源。
- 您的通知。這會決定使用哪些 Amazon Simple Notification Service 主題來通知您重要的 DevOps Guru 事件。
- 增強洞察功能。這包括日誌異常偵測、加密和 AWS Systems Manager 整合設定。這可判斷 DevOps Guru 是否顯示日誌資料、您是否使用其他安全金鑰，以及是否針對每個新洞見在 Systems Manager OpsCenter 中建立 OpsItem。 OpsCenter

主題

更新您的管理帳戶設定

您可以為組織中的帳戶設定 DevOps Guru。如果您尚未註冊委派管理員，您可以選擇註冊委派管理員來執行此操作。如需註冊委派管理員的詳細資訊，請參閱啟用 DevOps Guru。

在 DevOps Guru 中更新您的 AWS 分析涵蓋範圍

您可以更新帳戶中 DevOps Guru 分析 AWS 的資源。若要這樣做，請導覽至 主控台中的已分析資源頁面，然後選擇編輯。如需詳細資訊，請參閱檢視分析的資源。

在 DevOps Guru 中更新您的通知

設定用於通知您重要 Amazon DevOps Guru 事件的 Amazon Simple Notification Service 主題。您可以從 AWS 帳戶中已存在的主題名稱清單中選擇，輸入 DevOps Guru 在您帳戶中建立的新主題名稱，或

輸入您區域中任何 AWS 帳戶中現有主題的 Amazon Resource Name (ARN)。如果您指定不在帳戶中的主題 ARN，則必須將 IAM 政策新增至該主題，以授予 DevOps Guru 存取該主題的許可。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。

DevOps Guru 會傳送下列更新的通知：

- 建立新的洞見。
- 新的異常會新增至洞見。
- 洞見的嚴重性會從 Low或 升級Medium到 High。
- 洞見的狀態會從進行中變更為已解決。
- 已識別洞見的建議。

當您嘗試將資源新增至 DevOps Guru 帳戶時，如果選取的 CloudFormation 堆疊或標籤金鑰無效，DevOps Guru 也會傳送通知。

您可以選擇針對問題的所有更新類型接收 Amazon SNS 通知，或只在問題開啟、關閉或嚴重性變更時接收 Amazon SNS 通知。根據預設，您會收到所有更新的通知。

若要更新您的通知，請先導覽至通知頁面，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 DevOps Guru 主控台中的通知設定
- 在 DevOps Guru 主控台中新增 Amazon SNS 通知主題
- 在 DevOps Guru 主控台中移除 Amazon SNS 通知主題
- 更新 Amazon SNS 通知組態
- 新增到 Amazon SNS 主題的許可

導覽至 DevOps Guru 主控台中的通知設定

若要更新通知，您必須先導覽至通知設定區段。

導覽至通知設定區段

1. 開啟位於 https：//https://console.aws.amazon.com/devops-guru/ 的 Amazon DevOps Guru 主控台。
2. 在導覽窗格中選擇 Settings (設定)。

設定頁面包含通知區段，其中包含已設定 Amazon SNS 主題的相關資訊。

在 DevOps Guru 主控台中新增 Amazon SNS 通知主題

在 DevOps Guru 主控台中新增 Amazon SNS 通知主題

1. the section called “導覽至 DevOps Guru 主控台中的通知設定”.
2. 選擇 Add notification (新增通知)。
3. 若要新增 Amazon SNS 主題，請執行下列其中一項操作。
   - 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，從另一個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 是主題的 Amazon Resource Name。您可以在不同的帳戶中指定主題。如果您在另一個帳戶中使用主題，則必須將資源政策新增至主題。如需詳細資訊，請參閱Amazon SNS 主題的許可。
4. 選擇 Save (儲存)。

在 DevOps Guru 主控台中移除 Amazon SNS 通知主題

在 DevOps Guru 主控台中移除 Amazon SNS 主題

1. the section called “導覽至 DevOps Guru 主控台中的通知設定”.
2. 選擇選取現有主題。
3. 從下拉式選單中，選取要移除的主題。
4. 選擇移除。
5. 選擇儲存。

更新 Amazon SNS 通知組態

DevOps Guru 中的 Amazon SNS 通知主題有兩種類型的通知組態。您可以選擇接收所有嚴重性等級的通知，或僅接收具有高嚴重性等級和中嚴重性等級的通知。您也可以選擇接收所有更新類型的通知，或只接收某些類型的更新。

當您選擇接收所有類型問題更新的 Amazon SNS 通知時，DevOps Guru 會傳送下列更新的通知：

- 建立新的洞見。
- 新的異常會新增至洞見。
- 洞見的嚴重性會從 Low或 升級Medium到 High。
- 洞見的狀態會從進行中變更為已解決。
- 已識別洞見的建議。

根據預設，您只會收到高和中嚴重性等級通知，而且會收到所有更新類型的通知。

更新 Amazon SNS 通知主題的通知組態

1. the section called “導覽至 DevOps Guru 主控台中的通知設定”.
2. 選擇選取現有主題。
3. 從下拉式選單中，選取您要進行更新的主題。
4. 選擇所有嚴重性等級以接收高、中和低嚴重性等級的通知，或選擇僅高和中以接收高和中嚴重性等級的通知。
5. 選擇在洞見的所有更新時通知我，或選擇在洞見開啟或關閉時通知我，或嚴重性等級從低或中變更為高。
6. 選擇儲存。

新增到 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。當您在此處指定主題時，DevOps Guru 會將下列許可附加至其資源政策。

```
{
    "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"
    }
  }
}
```

DevOps Guru 需要這些許可才能使用主題發佈通知。如果您不想對主題擁有這些許可，您可以安全地移除這些許可，而且主題會繼續像在選擇主題之前一樣運作。不過，如果移除這些附加的許可，DevOps Guru 就無法使用 主題來產生通知。

篩選 DevOps Guru 通知

您可以使用 Amazon SNS 訂閱篩選條件政策，透過 the section called “更新 Amazon SNS 通知組態”或 來篩選 DevOps Guru 通知。

主題

- 使用 Amazon SNS 訂閱篩選條件政策篩選通知
- Amazon DevOps Guru 的篩選 Amazon SNS 通知範例

使用 Amazon SNS 訂閱篩選條件政策篩選通知

您可以建立 Amazon Simple Notification Service (Amazon SNS) 訂閱篩選條件政策，以減少從 Amazon DevOps Guru 收到的通知數量。

使用篩選條件政策來指定您收到的通知類型。您可以使用下列關鍵字篩選 Amazon SNS 訊息。

- `NEW_INSIGHT` — 建立新的洞見時收到通知。
- `CLOSED_INSIGHT` — 在現有洞見關閉時收到通知。
- `NEW_RECOMMENDATION` — 從洞見建立新建議時收到通知。
- `NEW_ASSOCIATION` — 從洞見偵測到新的異常時收到通知。
- `CLOSED_ASSOCIATION` — 在現有異常關閉時收到通知。
- `SEVERITY_UPGRADED` — 升級洞見嚴重性時收到通知

如需有關如何建立 Amazon SNS 訂閱篩選條件政策的資訊，請參閱《Amazon Simple Notification Service 開發人員指南》中的 Amazon SNS 訂閱篩選條件政策。在篩選政策中，您可以使用政策的 指

定其中一個關鍵字MessageType。例如，以下會出現在篩選條件中，指定 Amazon SNS 主題只會在從洞見偵測到新的異常時傳送通知。

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

Amazon DevOps Guru 的篩選 Amazon SNS 通知範例

以下是來自具有篩選條件政策之 Amazon SNS 主題的 Amazon SNS) 通知範例。其MessageType設定為 NEW_ASSOCIATION，因此只有在從洞見偵測到新的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"
          ]
        }
      }
}
```

在 DevOps Guru 中更新 AWS Systems Manager 整合

您可以為每個 in AWS Systems Manager OpsCenter 的新洞見啟用 OpsItem 的建立。OpsCenter 是一種集中式系統，您可以在其中檢視、調查和檢閱操作工作項目 (OpsItems)。洞見的 OpsItems 可協助您管理工作，以解決觸發每個洞見建立的異常行為。如需詳細資訊，請參閱AWS Systems Manager《 使用者指南》中的 AWS Systems Manager OpsCenter 和使用 OpsItem。

> **Note**
>
> 如果您變更 OpsItem 標籤欄位的索引鍵或值，則 DevOps Guru 無法更新該 OpsItem。例如，如果您將 OpsItem 的標籤從 `"aws:RequestTag/DevOps-GuruInsightSsmOpsItemRelated": "true"` 變更為其他項目，則 DevOps Guru 無法更新該 OpsItem。

管理您的 Systems Manager 整合

1. 開啟位於 https：//https://console.aws.amazon.com/devops-guru/ 的 Amazon DevOps Guru 主控台。
2. 在導覽窗格中選擇 Settings (設定)。

3. 在AWS Systems Manager 整合中，針對每個洞見，選取啟用 DevOps Guru 在 OpsCenter 中建立 an AWS OpstItem，以為每個新洞見建立 OpsItem。取消選取以停止為每個新洞見建立 OpsItem。

您需要為帳戶中建立OpsItems 付費。如需詳細資訊，請參閱 AWS Systems Manager 定價。

在 DevOps Guru 中更新日誌異常偵測

管理日誌異常偵測設定

1. 開啟位於 https：//https://console.aws.amazon.com/devops-guru/ 的 Amazon DevOps Guru 主控台。
2. 在導覽窗格中選擇 Settings (設定)。
3. 在日誌異常偵測中，透過授予 DevOps Guru 許可來顯示與洞見相關聯的日誌資料，選取啟用日誌異常偵測。 可讓 DevOps Guru 顯示與洞見相關的日誌資料。

在 DevOps Guru 中更新加密設定

您可以更新加密設定，以使用 AWS 擁有的金鑰或 AWS KMS 客戶受管金鑰。從現有客戶受管 AWS KMS 金鑰切換到新客戶受管 AWS KMS 金鑰時，DevOps Guru 會自動開始使用新金鑰來加密新擷取的中繼資料。歷史資料將使用先前設定的客戶受管 AWS KMS 金鑰保持加密。

> **Note**
>
> 如果您撤銷授予，或停用或刪除先前的 AWS KMS 金鑰，DevOps Guru 將無法存取此金鑰加密的任何資料，而且您可能會在執行讀取操作`AccessDeniedException`時看到 。

管理加密設定

1. 開啟位於 https：//https://console.aws.amazon.com/devops-guru/ 的 Amazon DevOps Guru 主控台。
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. 選取您想要用來保護資料的熵類型。您可以使用預設 AWS 擁有的金鑰、選擇現有的客戶受管金鑰，或建立新的客戶受管 AWS KMS 金鑰。

5. 選擇儲存。

加密是 DevOps Guru 安全性的重要部分。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

本頁的各節顯示每種通知類型的範例。

新洞見

新洞見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"
            ]
        },
   }
}
```

已關閉洞見

已關閉洞見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"
            ]
        }
   }
}
```

新建議

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"
        ]
     }
  }
}
```

嚴重性已升級

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 CloudFormation 堆疊和 AWS 標籤來篩選和識別您希望 DevOpsGuru 分析 AWS 的資源。當您為 DevOpsGuru 選擇無效的堆疊或標籤以識別資源時，DevOps 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 DevOpsGuru 篩選方法，請選擇具有相關資源的堆疊和標籤。

```
{
    "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 DevOpsGuru 分析的資源

DevOpsGuru 提供資源名稱清單，以及其使用 `ListMonitoredResources`動作進行分析的應用程式邊界。此資訊是從 Amazon CloudWatch AWS CloudTrail和其他使用 DevOpsGuru AWS 服務連結角色的服務收集而來。

請注意，即使使用者沒有明確許可來存取其他服務的 APIs，例如 AWS Lambda 或 Amazon RDS，只要動作`ListMonitoredResources`允許，DevOps 仍會提供該服務的資源清單。

主題

在 DevOpsGuru 中更新您的 AWS 分析涵蓋範圍

您可以更新您帳戶中 DevOpsGuru 分析 AWS 的資源。分析的資源構成您的 DevOpsGuru 涵蓋範圍界限。當您指定界限時，您的資源會分組在應用程式中。您有四個界限涵蓋範圍選項。

- 選擇讓 DevOpsGuru 分析您帳戶中所有支援的資源。您帳戶中所有堆疊中的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都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，它們會分組到自己的應用程式中。
- 選擇定義這些資源的 AWS CloudFormation 堆疊來指定資源。如果您這樣做，DevOps 會分析您選擇的堆疊中指定的每個資源。如果您選擇的堆疊未定義您帳戶中的資源，則不會進行分析。如需詳細資訊，請參閱CloudFormation 《 使用者指南》中的使用堆疊和》判斷 DevOps Guru 的涵蓋範圍。
- 使用 AWS 標籤指定資源。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金鑰的所有資源。資源會根據選取的標籤值分組。如需詳細資訊，請參閱使用標籤來識別 DevOps Guru 應用程式中的資源。
- 指定 來不分析資源，以便停止因資源分析產生費用。

> **Note**
>
> 如果您更新您的涵蓋範圍以停止分析資源，則如果您過去檢閱 DevOpsGuru 產生的現有洞見，可能會繼續產生小額費用。這些費用與用於擷取和顯示洞見資訊的 API 呼叫相關聯。如需詳細資訊，請參閱 Amazon DevOpsGuru 定價。

DevOpsGuru 支援與支援的服務相關聯的所有資源。如需支援服務和資源的詳細資訊，請參閱 Amazon DevOpsGuru 定價。

管理您的 DevOpsGuru 分析涵蓋範圍

1. 在 https://console.aws.amazon.com/devops-guru/ ：// 開啟 Amazon DevOpsGuru 主控台。
2. 在導覽窗格中展開已分析的資源。
3. 選擇編輯。
4. 選擇下列其中一個涵蓋範圍選項。

   - 如果您希望 DevOpsGuru 分析帳戶和區域中所有支援的資源，請選擇所有 AWS 帳戶資源。如果您選擇此選項， AWS 您的帳戶即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自己的應用程式中。
   - 如果您希望 DevOpsGuru 分析您選擇的堆疊中的資源，請選擇 CloudFormation 堆疊，然後選擇下列其中一個選項。
     - 所有資源 – 分析您帳戶中堆疊中的所有資源。每個堆疊中的資源都會分組到自己的應用程式。不會分析您帳戶中任何不在堆疊中的資源。
     - 選取堆疊 – 選取您希望 DevOpsGuru 分析的堆疊。您選取的每個堆疊中的資源會分組到自己的應用程式。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 CloudFormation 堆疊來識別 DevOps Guru 應用程式中的資源。
   - 如果您希望 DevOpsGuru 分析包含您選擇的標籤的所有資源，請選擇標籤。選擇金鑰，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。具有所選標籤索引鍵的資源會依標籤值分組，如果有的話。沒有此標籤索引鍵的資源會個別分組和分析。
     - 選擇特定的標籤值 – 系統會分析包含具有所選索引鍵之標籤的所有資源。DevOpsGuru 會根據標籤的值將您的資源分組到應用程式中。

     如需詳細資訊，請參閱使用標籤來識別 DevOps Guru 應用程式中的資源。
   - 如果您不希望 DevOpsGuru 分析任何資源，請選擇無。此選項會停用 DevOpsGuru，讓您停止因資源分析而產生費用。
5. 選擇 Save (儲存)。

移除使用者的分析資源檢視

即使使用者沒有存取 Lambda 或 Amazon RDS 等其他服務 APIs明確許可，只要動作`ListMonitoredResources`允許，DevOps 仍會提供該服務的資源清單。若要變更此行為，您可以更新您的 AWS IAM 政策以拒絕此動作。

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

DevOpsGuru 的最佳實務

下列最佳實務可協助您了解、診斷和修正 Amazon DevOpsGuru 偵測到的異常行為。搭配 使用最佳實務了解 DevOps Guru 主控台中的洞見，解決 DevOpsGuru 偵測到的操作問題。

- 在洞見的時間軸檢視中，先查看反白顯示的指標。它們通常是問題的關鍵指標。
- 使用 Amazon CloudWatch 來檢視在洞見中第一個反白指標之前發生的指標，以準確指出行為變更的時間和方式。這可協助您診斷和修正問題。
- 對於 Amazon RDS 資源，請查看績效詳情指標。透過將計數器指標與資料庫負載建立關聯，您可以取得效能問題的詳細資訊。如需詳細資訊，請參閱使用 DevOpsGurufor Amazon RDS 分析效能異常。
- 相同指標的多個維度通常可能是異常的。查看圖形檢視中的維度，以更深入了解問題。
- 請查看 部署洞見中的事件區段，或是建立洞見時所發生的基礎設施事件。了解當洞見發生異常行為時，發生哪些事件可協助您了解並診斷問題。
- 在作業系統中尋找與線索洞見大約同時發生的票證。
- 在洞見中，閱讀建議並瀏覽建議中的連結。這些通常具有故障診斷步驟，可協助您快速診斷和解決問題。
- 除非您已解決問題，否則請勿忽略已解決的洞見。每天查看一次新的洞見，即使它們已解決。盡量了解洞察背後的根本原因。尋找可能是系統問題跡象的模式。如果系統性問題未解決，未來可能會導致更嚴重的問題。現在修正暫時性問題有助於防止未來更嚴重的事件。

Amazon DevOps Guru 的安全性

的雲端安全性 AWS 是最高優先順序。身為 AWS 客戶，您可以受益於資料中心和網路架構，這些架構是為了符合最安全敏感組織的需求而建置。

安全性是 AWS 與您之間的共同責任。共同責任模式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 Cloud 中執行 AWS 服務的基礎設施。 AWS 也為您提供可安全使用的服務。作為AWS 合規計畫的一部分，第三方稽核人員會定期測試和驗證我們安全的有效性。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。
- 雲端的安全性 – 您的責任取決於您使用 AWS 的服務。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。

本文件可協助您了解如何在使用 DevOps Guru 時套用共同責任模型。下列主題說明如何設定 DevOps Guru 以符合您的安全與合規目標。您也會了解如何使用其他 AWS 服務來協助您監控和保護 DevOps Guru 資源。

主題

Amazon DevOps Guru 中的資料保護

AWS 共同責任模型適用於 Amazon DevOps Guru 中的資料保護。如此模型所述， AWS 負責保護執行所有 的全域基礎設施 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 共同責任模型和 GDPR 部落格文章。

基於資料保護目的，我們建議您保護 AWS 帳戶 登入資料，並使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 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。如需有關使用 CloudTrail 追蹤擷取 AWS 活動的資訊，請參閱AWS CloudTrail 《 使用者指南》中的使用 CloudTrail 追蹤。
- 使用 AWS 加密解決方案，以及其中的所有預設安全控制 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 AWS 透過命令列界面或 API 存取 時需要 FIPS 140-3 驗證的密碼編譯模組，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) 140-3。

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。這包括當您使用 DevOps Guru 或使用主控台、API AWS CLI或 AWS SDKs的其他 AWS 服務 時。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 Guru 中的資料加密

加密是 DevOps Guru 安全性的重要部分。有些加密，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設定 。

- 資料傳輸中加密：客戶與 DevOps Guru 之間，以及 DevOps Guru 與其下游相依性之間的所有通訊都會使用 TLS 進行保護，並使用 Signature 第 4 版簽署程序進行驗證。所有 DevOps Guru 端點都使用 管理的憑證 AWS 私有憑證授權單位。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 IDs 和 AWS CloudTrail 事件會使用 Amazon S3、Amazon DynamoDB 和 Amazon Kinesis 儲存。如果使用 CloudFormation 堆疊來定義分析的資源，則也會收集堆疊資料。DevOps Guru 使用 Amazon S3、DynamoDB 和 Kinesis 的資料保留政策。存放在 Kinesis 中的資料最多可保留一年，並取決於政策集。存放在 Amazon S3 和 DynamoDB 中的資料會儲存一年。

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

  客戶受管金鑰：DevOps Guru 支援加密客戶內容和敏感中繼資料，例如使用客戶受管金鑰從 CloudWatch Logs 產生的日誌異常。此功能可讓您選擇新增自我管理的安全層，以協助您符合組

織的合規和法規要求。如需在 DevOps Guru 設定中啟用客戶受管金鑰的資訊，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》中的客戶受管金鑰。

> **Note**
>
> DevOps Guru 會使用 AWS 擁有的金鑰自動啟用靜態加密，以免費保護敏感中繼資料。不過，使用客戶受管金鑰會產生 AWS KMS 費用。如需定價的詳細資訊，請參閱 AWS Key Management Service 定價。

DevOps Guru 如何在 中使用授予 AWS KMS

DevOps Guru 需要授予才能使用客戶受管金鑰。

當您選擇使用客戶受管金鑰啟用加密時，DevOps Guru 會透過傳送 CreateGrant 請求至 來代表您建立授權 AWS KMS。中的授予 AWS KMS 用於授予 DevOps Guru 存取客戶帳戶中的 AWS KMS 金鑰。

DevOps Guru 需要授予 ，才能將客戶受管金鑰用於下列內部操作：

- 傳送 DescribeKey 請求至 AWS KMS ，以驗證在建立追蹤器或地理圍欄集合時輸入的對稱客戶受管 KMS 金鑰 ID 是否有效。
- 將 GenerateDataKey 請求傳送至 AWS KMS ，以產生由客戶受管金鑰加密的資料金鑰。
- 將 Decrypt 請求傳送至 AWS KMS 以解密加密的資料金鑰，以便用來加密您的資料。

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。如果您這麼做，DevOps Guru 將無法存取客戶受管金鑰加密的任何資料，這會影響依賴該資料的操作。例如，如果您嘗試取得 DevOps Guru 無法存取的加密日誌異常資訊，則操作會傳回 AccessDeniedException 錯誤。

在 DevOps Guru 中監控您的加密金鑰

當您搭配 DevOps Guru 資源使用 AWS KMS 客戶受管金鑰時，您可以使用 AWS CloudTrail 或 CloudWatch Logs 來追蹤 DevOps Guru 傳送的請求 AWS KMS。

建立客戶自管金鑰

您可以使用 AWS 管理主控台 或 AWS KMS APIs 來建立對稱客戶受管金鑰。

若要建立對稱客戶受管金鑰，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》中的 的身分驗證和存取控制 AWS KMS。

若要將客戶受管金鑰與 DevOps Guru 資源搭配使用，必須在金鑰政策中允許下列 API 操作：

- `kms:CreateGrant`：新增客戶受管金鑰的授權。授予控制對指定 AWS KMS 金鑰的存取，以允許存取授予 DevOps Guru 所需的操作。如需使用授予的詳細資訊，請參閱 AWS Key Management Service 開發人員指南。

這可讓 DevOps Guru 執行下列動作：

- 呼叫 GenerateDataKey 以產生加密的資料金鑰並將其存放，因為不會立即使用資料金鑰進行加密。
- 呼叫 Decrypt 以使用儲存的加密資料金鑰來存取加密的資料。
- 設定淘汰委託人，以允許向 RetireGrant 提供服務。
- 使用 kms:DescribeKey 提供客戶受管金鑰詳細資訊，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見產生的安全性。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。您也不需要設定 PrivateLink，不過這是建議的行為。如需詳細資訊，請參閱DevOps Guru 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 Guru 的 Identity and Access Management

AWS Identity and Access Management (IAM) 是一種 AWS 服務 ，可協助管理員安全地控制對 AWS 資源的存取。IAM 管理員可控制誰可以進行身分驗證 （登入） 和授權 （具有許可），以使用 DevOps Guru 資源。IAM 是您可以免費使用 AWS 服務 的 。

主題

- 目標對象
- 使用身分驗證
- 使用政策管理存取權
- DevOps Guru 更新 AWS 受管政策和服務連結角色
- Amazon DevOps Guru 如何與 IAM 搭配使用
- Amazon DevOps Guru 的身分型政策
- 使用 DevOps Guru 的服務連結角色
- Amazon DevOps Guru 許可參考
- Amazon SNS 主題的許可
- AWS KMS加密 Amazon SNS 主題的許可
- 對 Amazon DevOps Guru 身分和存取進行故障診斷

目標對象

使用方式 AWS Identity and Access Management (IAM) 會根據您的角色而有所不同：

- 服務使用者 — 若無法存取某些功能，請向管理員申請所需許可 (請參閱 對 Amazon DevOps Guru 身分和存取進行故障診斷)

- 服務管理員 — 負責設定使用者存取權並提交相關許可請求 (請參閱 Amazon DevOps Guru 如何與 IAM 搭配使用)
- IAM 管理員 — 撰寫政策以管理存取控制 (請參閱 Amazon DevOps Guru 的身分型政策)

使用身分驗證

身分驗證是您 AWS 使用身分憑證登入 的方式。您必須以 AWS 帳戶根使用者、IAM 使用者或擔任 IAM 角色身分進行身分驗證。

您可以使用身分來源的登入資料，例如 AWS IAM Identity Center (IAM Identity Center)、單一登入身分驗證或 Google/Facebook 登入資料，以聯合身分的形式登入。如需有關登入的詳細資訊，請參閱《AWS 登入 使用者指南》中的如何登入您的 AWS 帳戶。

對於程式設計存取， AWS 提供 SDK 和 CLI 以密碼編譯方式簽署請求。如需詳細資訊，請參閱《IAM 使用者指南》中的 API 請求的AWS 第 4 版簽署程序。

AWS 帳戶 根使用者

當您建立 時 AWS 帳戶，您會從一個名為 AWS 帳戶 theroot 使用者的登入身分開始，該身分可完整存取所有 AWS 服務 和 資源。強烈建議不要使用根使用者來執行日常任務。有關需要根使用者憑證的任務，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

最佳實務是要求人類使用者使用聯合身分提供者，以 AWS 服務 使用臨時憑證存取 。

聯合身分是來自您的企業目錄、Web 身分提供者的使用者，或使用來自身分來源的 AWS 服務 憑證存取 Directory Service 的使用者。聯合身分會擔任角色，而該角色會提供臨時憑證。

若需集中化管理存取權限，建議使用 AWS IAM Identity Center。如需詳細資訊，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https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users.html是一種身分具備單人或應用程式的特定許可權。建議以臨時憑證取代具備長期憑證的 IAM 使用者。如需詳細資訊，請參閱《IAM 使用者指南》中的要求人類使用者使用聯合身分提供者，以 AWS 使用臨時憑證存取 。

IAM 群組會指定 IAM 使用者集合，使管理大量使用者的許可權更加輕鬆。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 使用者的使用案例。

IAM 角色

IAM 角色https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html的身分具有特定許可權，其可以提供臨時憑證。您可以透過從使用者切換到 IAM 角色（主控台）或呼叫 AWS CLI 或 AWS API 操作來擔任角色。如需詳細資訊，請參閱《IAM 使用者指南》中的擔任角色的方法。

IAM 角色適用於聯合身分使用者存取、臨時 IAM 使用者許可、跨帳戶存取權與跨服務存取，以及在 Amazon EC2 執行的應用程式。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 中的快帳戶資源存取。

使用政策管理存取權

您可以透過建立政策並將其連接到身分或資源 AWS 來控制 AWS 中的存取。政策定義與身分或資源相關聯的許可。當委託人提出請求時 AWS ， 會評估這些政策。大多數政策會以 JSON 文件 AWS 形式存放在 中。如需進一步了解 JSON 政策文件，請參閱《IAM 使用者指南》中的 JSON 政策概觀。

管理員會使用政策，透過定義哪些主體可在哪些條件下對哪些資源執行動作，以指定可存取的範圍。

預設情況下，使用者和角色沒有許可。IAM 管理員會建立 IAM 政策並將其新增至角色，供使用者後續擔任。IAM 政策定義動作的許可，無論採用何種方式執行。

身分型政策

身分型政策是附加至身分 (使用者、使用者群組或角色) 的 JSON 許可政策文件。這類政策控制身分可對哪些資源執行哪些動作，以及適用的條件。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的透過客戶管理政策定義自訂 IAM 許可。

身分型政策可分為內嵌政策 (直接內嵌於單一身分) 與受管政策 (可附加至多個身分的獨立政策)。如需了解如何在受管政策及內嵌政策之間做選擇，請參閱《IAM 使用者指南》中的在受管政策與內嵌政策之間選擇。

資源型政策

資源型政策是附加到資源的 JSON 政策文件。範例包括 IAM 角色信任政策與 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。您必須在資源型政策中指定主體。

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來自 IAM 的 AWS 受管政策。

其他政策類型

AWS 支援其他政策類型，可設定更多常見政策類型授予的最大許可：

- 許可界限 — 設定身分型政策可授與 IAM 實體的最大許可。如需詳細資訊，請參閱《 IAM 使用者指南》中的 IAM 實體許可界限。
- 服務控制政策 (SCP) — 為 AWS Organizations中的組織或組織單位指定最大許可。如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的服務控制政策。
- 資源控制政策 (RCP) — 設定您帳戶中資源可用許可的上限。如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的資源控制政策 (RCP)。
- 工作階段政策 — 在以程式設計方式為角色或聯合身分使用者建立臨時工作階段時，以參數形式傳遞的進階政策。如需詳細資訊，請參《IAM 使用者指南》中的工作階段政策。

多種政策類型

當多種類型的政策適用於請求時，產生的許可會更複雜而無法理解。若要了解如何 AWS 決定是否在涉及多個政策類型時允許請求，請參閱《IAM 使用者指南》中的政策評估邏輯。

DevOps Guru 更新 AWS 受管政策和服務連結角色

檢視自 DevOps Guru 開始追蹤這些變更以來， AWS 受管政策和服務連結角色更新的詳細資訊。如需此頁面變更的自動提醒，請訂閱 DevOps Guru 上的 RSS 摘要Amazon DevOpsGuru 文件歷史記錄。

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

變更	描述	Date
	現在支援存取 REST API 上的 APIs Gateway GET 動作。	
AmazonDevOpsGuruServiceRolePolicy – 更新至現有政策。	AWSServiceRoleForDevOpsGuru 服務連結角色現在支援數個 Amazon Simple Storage Service 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	AmazonDevOpsGuruConsoleFullAccess 受管政策現在支援存取 CloudWatch FilterLogEvents 動作。	2022 年 8 月 30 日
AmazonDevOpsGuruReadOnlyAccess – 更新現有政策	AmazonDevOpsGuruReadOnlyAccess 受管政策現在支援 CloudWatch FilterLogEvents 動作的唯讀存取。	2022 年 8 月 30 日
AmazonDevOpsGuruServiceRolePolicy – 更新至現有政策。	AWSServiceRoleForDevOpsGuru 服務連結角色現在支援 CloudWatch 日誌動作 FilterLogEvents 、DescribeLogGroups 和 DescribeLogStreams 。	2022 年 7 月 12 日
DevOps Guru 的身分型政策 – 新的受管政策。	政策AmazonDevOpsGuruConsoleFullAccess 已新增。	2021 年 12 月 16 日

變更	描述	Date
AmazonDevOpsGuruServiceRolePolicy – 更新至現有政策。	AWSServiceRoleForDevOpsGuru 服務連結角色現在支援績效詳情 DescribeMetricsKeys 和 Amazon RDS DescribeDBInstances 動作。	2021 年 12 月 1 日
AmazonDevOpsGuruReadOnlyAccess – 更新現有政策	AmazonDevOpsGuruReadOnlyAccess 受管政策現在支援 Amazon RDS DescribeDBInstances 動作的唯讀存取。	2021 年 12 月 1 日
AmazonDevOpsGuruFullAccess – 更新現有政策	AmazonDevOpsGuruFullAccess 受管政策現在支援存取 Amazon RDS DescribeDBInstances 動作。	2021 年 12 月 1 日
Amazon DevOps Guru 的身分型政策 – 已新增新政策。	AWSServiceRoleForDevOpsGuru 服務連結角色現在支援存取 Amazon RDS DescribeDBInstances 和績效詳情GetResourceMetrics 動作。 AmazonDevOpsGuruOrganizationsAccess 受管政策提供組織內 DevOps Guru 的存取權。	2021 年 11 月 16 日
AmazonDevOpsGuruServiceRolePolicy – 更新至現有政策。	AWSServiceRoleForDevOpsGuru 服務連結角色現在支援 AWS Organizations。	2021 年 11 月 4 日

變更	描述	Date
AmazonDevOpsGuruServiceRolePolicy – 更新至現有政策。	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
DevOps Guru 的服務連結角色許可 – 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	AmazonDevOpsGuruReadOnlyAccess 受管政策現在允許唯讀存取 AWS Identity and Access Management GetRole和 DevOps Guru DescribeFeedback 動作。	2021 年 6 月 14 日
AmazonDevOpsGuruReadOnlyAccess – 更新現有政策	AmazonDevOpsGuruReadOnlyAccess 受管政策現在允許唯讀存取 DevOps Guru GetCostEstimation 和 StartCostEstimation 動作。	2021 年 4 月 27 日
AmazonDevOpsGuruServiceRolePolicy – 更新至現有政策。	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

變更	描述	Date
DevOps Guru 開始追蹤變更	DevOps Guru 開始追蹤其 AWS 受管政策的變更。	2020 年 12 月 10 日

Amazon DevOps Guru 如何與 IAM 搭配使用

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

您可以搭配 Amazon DevOps Guru 使用的 IAM 功能

IAM 功能	DevOps Guru 支援
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
主體許可	是
服務角色	否
服務連結角色	是

若要全面了解 DevOps Guru 和其他 AWS 服務如何與大多數 IAM 功能搭配使用，請參閱《IAM 使用者指南》中的AWS 與 IAM 搭配使用的 服務。

DevOps Guru 的身分型政策

支援身分型政策：是

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。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的透過客戶管理政策定義自訂 IAM 許可。

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。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。

DevOps Guru 的身分型政策範例

若要檢視 DevOps Guru 身分型政策的範例，請參閱 Amazon DevOps Guru 的身分型政策。

DevOps Guru 中的資源型政策

支援資源型政策：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。委託人可以包含帳戶、使用者、角色、聯合身分使用者或 AWS 服務。

如需啟用跨帳戶存取權，您可以在其他帳戶內指定所有帳戶或 IAM 實體作為資源型政策的主體。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 中的快帳戶資源存取。

DevOps Guru 的政策動作

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。

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。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。

DevOps Guru 中的政策動作在動作之前使用以下字首：

```
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 身分型政策的範例，請參閱 Amazon DevOps Guru 的身分型政策。

DevOps Guru 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。最佳實務是使用其 Amazon Resource Name (ARN) 來指定資源。若動作不支援資源層級許可，使用萬用字元 (*) 表示該陳述式適用於所有資源。

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

若要查看 DevOps Guru 資源類型及其 ARNs，請參閱《服務授權參考》中的 Amazon DevOps Guru 定義的資源。若要了解您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 身分型政策的範例，請參閱 Amazon DevOps Guru 的身分型政策。

DevOps Guru 的政策條件索引鍵

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` 元素會根據定義的條件，指定陳述式的執行時機。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。若要查看所有 AWS 全域條件索引鍵，請參閱《IAM 使用者指南》中的AWS 全域條件內容索引鍵。

若要查看 DevOps Guru 條件索引鍵的清單，請參閱《服務授權參考》中的 Amazon DevOps Guru 的條件索引鍵。若要了解您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 身分型政策的範例，請參閱 Amazon DevOps Guru 的身分型政策。

DevOps Guru 中的存取控制清單 (ACLs)

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。

使用 DevOps Guru 的屬性型存取控制 (ABAC)

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，依據稱為標籤的屬性來定義許可。您可以將標籤連接至 IAM 實體 AWS 和資源，然後設計 ABAC 政策，以便在主體的標籤符合資源上的標籤時允許操作。

如需根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件索引鍵，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》中的使用 ABAC 授權定義許可。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)。

搭配 DevOps Guru 使用暫時登入資料

支援臨時憑證：是

臨時登入資料提供對 AWS 資源的短期存取，並在您使用聯合或切換角色時自動建立。 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 使用者指南》中的 IAM 中的臨時安全憑證與可與 IAM 搭配運作的AWS 服務。

DevOps Guru 的跨服務主體許可

支援轉寄存取工作階段 (FAS)：是

轉送存取工作階段 (FAS) 使用呼叫 的委託人許可 AWS 服務，並結合 AWS 服務 請求向下游服務提出請求。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。

DevOps Guru 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。如需詳細資訊，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**
>
> 變更服務角色的許可可能會中斷 DevOps Guru 功能。只有在 DevOps Guru 提供指引時，才能編輯服務角色。

DevOps Guru 的服務連結角色

支援服務連結角色：是

服務連結角色是連結至 的一種服務角色 AWS 服務。服務可以擔任代表您執行動作的角色。服務連結角色會出現在您的 中 AWS 帳戶 ，並由服務擁有。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。在資料表中尋找服務，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 DevOps Guru 的身分型政策

根據預設，使用者和角色沒有建立或修改 DevOps Guru 資源的許可。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。

如需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 (主控台)。

如需 DevOps Guru 定義之動作和資源類型的詳細資訊，包括每種資源類型的 ARNs 格式，請參閱《服務授權參考》中的 Amazon DevOps Guru 的動作、資源和條件索引鍵。

主題

政策最佳實務

身分型政策會判斷您帳戶中的某個人員是否可以建立、存取或刪除 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 受管政策並邁向最低權限許可 – 若要開始將許可授予您的使用者和工作負載，請使用將許可授予許多常見使用案例的 AWS 受管政策。它們可在您的 中使用 AWS 帳戶。我們建議您定義特定於使用案例 AWS 的客戶受管政策，以進一步減少許可。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。
- 套用最低權限許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的許可。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。如果透過特定 例如 使用服務動作 AWS 服務，您也可以使用條件來授予其存取權 CloudFormation。如需詳細資訊，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，可協助您撰寫安全且實用的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的使用 IAM Access Analyzer 驗證政策。
- 需要多重要素驗證 (MFA) – 如果您的案例需要 IAM 使用者或 中的根使用者 AWS 帳戶，請開啟 MFA 以提高安全性。如需在呼叫 API 操作時請求 MFA，請將 MFA 條件新增至您的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的透過 MFA 的安全 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 DevOps Guru 主控台

若要存取 Amazon DevOps Guru 主控台，您必須擁有一組最低許可。這些許可必須允許您列出和檢視中 DevOps Guru 資源的詳細資訊 AWS 帳戶。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。

對於僅呼叫 AWS CLI 或 AWS API 的使用者，您不需要允許最低主控台許可。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。

為了確保使用者和角色仍然可以使用 DevOps Guru 主控台，也請將 DevOps Guru `AmazonDevOpsGuruReadOnlyAccess`或 `AmazonDevOpsGuruFullAccess` AWS 受管政策連接到實體。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。此政策包含在主控台或使用 或 AWS CLI AWS API 以程式設計方式完成此動作的許可。

```
{
    "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": "*"
        }
    ]
}
```

DevOps Guru 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，解決許多常見的使用案例 AWS。這些 AWS受管政策會授予常見使用案例的必要許可，因此您可以避免調查需要哪些許可。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，您還必須連接名為 的 AWS受管政策`IAMFullAccess`。

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受管政策是 DevOps Guru 特有的，您可以連接到您帳戶中的使用者。

主題

- AmazonDevOpsGuruFullAccess
- AmazonDevOpsGuruConsoleFullAccess
- AmazonDevOpsGuruReadOnlyAccess
- AmazonDevOpsGuruOrganizationsAccess

AmazonDevOpsGuruFullAccess

`AmazonDevOpsGuruFullAccess` – 提供 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。僅將此套用至您要授予 DevOps Guru 完整控制權的管理層級使用者。

`AmazonDevOpsGuruFullAccess` 政策包含下列陳述式。

JSON

```
{
    "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 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。此政策具有額外的效能洞見許可，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。僅將此套用至您要授予 DevOps Guru 完整控制權的管理層級使用者。

AmazonDevOpsGuruConsoleFullAccess 政策包含下列陳述式。

JSON

```
{
    "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 DevOps Guru 和其他 AWS 服務中相關資源的唯讀存取權。將此政策套用到您要授予檢視洞見能力的使用者，但不對 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。

AmazonDevOpsGuruReadOnlyAccess 政策包含下列陳述式。

JSON

```
{
"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 – 為 Organizations 管理員提供組織內 DevOps Guru 多帳戶檢視的存取權。將此政策套用到組織的管理員層級使用者，您要為其授予組織內 DevOps Guru 的完整存取權。您可以在組織的管理帳戶和 DevOps Guru 的委派管理員帳戶中套用此政策。除了此政策AmazonDevOpsGuruFullAccess之外，您還可以套用 AmazonDevOpsGuruReadOnlyAccess 或 ，以提供 DevOps Guru 的唯讀或完整存取權。

AmazonDevOpsGuruOrganizationsAccess 政策包含下列陳述式。

使用 DevOps Guru 的服務連結角色

Amazon DevOps Guru 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。服務連結角色是由 DevOps Guru 預先定義，並包含服務代表您呼叫 AWS CloudTrail、Amazon CloudWatch AWS CodeDeploy、 AWS X-Ray、 和 AWS Organizations 所需的所有許可。

服務連結角色可讓您更輕鬆地設定 DevOps Guru，因為您不必手動新增必要的許可。DevOps Guru 定義其服務連結角色的許可，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。這可保護您的 DevOps Guru 資源，因為您不會不小心移除存取資源的許可。

DevOps Guru 的服務連結角色許可

DevOps Guru 使用名為 的服務連結角色AWSServiceRoleForDevOpsGuru。這是 AWS 受管政策，具有 DevOps Guru 在您的 帳戶中執行所需的範圍許可。

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

- devops-guru.amazonaws.com

角色許可政策AmazonDevOpsGuruServiceRolePolicy允許 DevOps Guru 對指定的資源完成下列動作。

JSON

```
{
 "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

您不需要手動建立服務連結角色，當您在 AWS 管理主控台、 AWS CLI或 AWS API 中建立洞見時，DevOps Guru 會為您建立服務連結角色。

> **Important**
>
> 如果您在另一個使用此角色支援之功能的 服務中完成動作，則此服務連結角色會出現在您的帳戶中；例如，如果您從 將 DevOps Guru 新增至儲存庫，則它可能會顯示 AWS CodeCommit。

編輯 DevOps Guru 的服務連結角色

DevOps Guru 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。如需詳細資訊，請參閱《IAM 使用者指南》中的編輯服務連結角色。

刪除 DevOps Guru 的服務連結角色

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。不過，您必須先取消與所有儲存庫的關聯，才能手動將其刪除。

> **Note**
>
> 如果您嘗試刪除資源時 DevOps Guru 服務正在使用 角色，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 AWS CLI、 或 AWS API 來刪除`AWSServiceRoleForDevOpsGuru`服務連結角色。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 Guru 許可參考

您可以在 DevOps Guru 政策中使用 AWS整體條件金鑰來表達條件。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

您可以指定含或不含萬用字元 (*) 的 Amazon Resource Name (ARN)，做為政策Resource欄位中的資源值。您可以使用萬用字元指定多個動作或資源。例如， 會devops-guru:*指定所有 DevOps Guru 動作，並devops-guru:List*指定以字詞 開頭的所有 DevOps Guru 動作List。下列範例是指具有以 開頭的通用唯一識別符 (UUID) 的所有洞見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連接到 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 Guru API 操作和動作的必要許可

AddNotificationChannel

動作：devops-guru:AddNotificationChannel

從 DevOps Guru 新增通知管道時需要。當 DevOps Guru 產生洞見，其中包含如何改善操作的相關資訊時，會使用通知管道通知您。

資源：*

RemoveNotificationChannel

devops-guru:RemoveNotificationChannel

從 DevOps Guru 移除通知管道時需要。當 DevOps Guru 產生洞見，其中包含如何改善操作的相關資訊時，會使用通知管道通知您。

資源：*

ListNotificationChannels

動作：devops-guru:ListNotificationChannels

傳回為 DevOps Guru 設定的通知通道清單時需要。當 DevOps Guru 產生洞見，其中包含如何改善操作的相關資訊時，每個通知管道都會用來通知您。支援的通知類型是 Amazon Simple Notification Service。

資源：*

UpdateResourceCollectionFilter

動作：devops-guru:UpdateResourceCollectionFilter

更新用於指定 DevOps Guru 分析帳戶中哪些 AWS 資源的 CloudFormation 堆疊清單時需要。分析會產生洞見，其中包括建議、操作指標和操作事件，您可以用來改善操作的效能。此方法也會建立您使用 CodeGuru OpsAdvisor 所需的 IAM 角色。

資源：*

GetResourceCollectionFilter

動作：devops-guru:GetResourceCollectionFilter

傳回用於指定 DevOps Guru 分析帳戶中哪些 AWS 資源的 AWS CloudFormation 堆疊清單時需要。分析會產生洞見，其中包括建議、操作指標和操作事件，您可以用來改善操作的效能。

資源：*

ListInsights

動作：devops-guru:ListInsights

傳回您 AWS 帳戶中的洞見清單時需要。您可以指定依開始時間、狀態 (ongoing 或 any) 和類型 (reactive 或) 傳回哪些洞見predictive。

資源：*

DescribeInsight

動作：devops-guru:DescribeInsight

傳回您使用其 ID 指定之洞見的詳細資訊時需要。

資源：*

SearchInsights

動作：devops-guru:SearchInsights

傳回您 AWS 帳戶中的洞見清單時需要。您可以指定依開始時間、篩選條件和類型 (reactive 或) 傳回哪些洞見predictive。

資源：*

`ListAnomalies`

動作：devops-guru:ListAnomalies

傳回屬於您使用其 ID 指定之洞見的異常清單時需要。

資源：*

`DescribeAnomaly`

動作：devops-guru:DescribeAnomaly

傳回您使用其 ID 指定之異常的詳細資訊時需要。

資源：*

`ListEvents`

動作：devops-guru:ListEvents

傳回 DevOps Guru 評估之資源發出的事件清單時需要。您可以使用篩選條件來指定傳回哪些事件。

資源：*

`ListRecommendations`

動作：devops-guru:ListRecommendations

傳回指定洞見的建議清單時需要。每個建議都包含指標清單，以及與建議相關的事件清單。

資源：*

`DescribeAccountHealth`

動作：devops-guru:DescribeAccountHealth

傳回開放被動洞察的數量、開放預測洞察的數量，以及 AWS 帳戶中分析的指標數量時需要。使用這些數字來衡量您 AWS 帳戶中操作的運作狀態。

資源：*

`DescribeAccountOverview`

動作：devops-guru:DescribeAccountOverview

傳回在某個時間範圍內發生的下列項目時需要：已建立的開放式被動洞察數量、已建立的開放式預測洞察數量，以及已關閉的所有被動洞察的平均復原時間 (MTTR)。

資源：*

`DescribeResourceCollectionHealthOverview`

動作：`devops-guru:DescribeResourceCollectionHealthOverview`

傳回 DevOps Guru 中指定之每個 CloudFormation 堆疊的所有洞見的開放式預測洞見、開放式反應洞見和平均復原時間 (MTTR) 時需要。

資源：*

`DescribeIntegratedService`

動作：`devops-guru:DescribeIntegratedService`

傳回可與 DevOps Guru 整合之服務的整合狀態時需要。可以與 DevOps Guru 整合的一項服務是 AWS Systems Manager，可用於為每個產生的洞見建立 OpsItem。

資源：*

`UpdateIntegratedServiceConfig`

動作：`devops-guru:UpdateIntegratedServiceConfig`

啟用或停用與可與 DevOps Guru 整合之服務的整合時需要。一個可與 DevOps Guru 整合的服務是 Systems Manager，可用於為每個產生的洞見建立 OpsItem。

資源：*

Amazon SNS 主題的許可

只有當您想要設定 Amazon DevOps Guru 傳送通知給另一個 AWS 帳戶擁有的 Amazon SNS 主題時，才使用此主題中的資訊。

若要讓 DevOps Guru 將通知交付至不同帳戶擁有的 Amazon SNS 主題，您必須將政策連接至 Amazon SNS 主題，以授予 DevOps Guru 傳送通知的許可。如果您設定 DevOps Guru 將通知傳送到您用於 DevOps Guru 的相同帳戶所擁有的 Amazon SNS 主題，則 DevOps Guru 會為您新增政策至主題。

連接政策以設定另一個帳戶中 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，使其更安全。

> **Note**
>
> DevOps Guru 目前僅支援相同區域中的跨帳戶存取。

主題

在另一個帳戶中設定 Amazon SNS 主題的許可

新增許可做為 IAM 角色

若要在使用 IAM 角色登入後從另一個帳戶使用 Amazon SNS 主題，您必須將政策連接至您要使用的 Amazon SNS 主題。若要在使用 IAM 角色時從另一個帳戶將政策連接至 Amazon SNS 主題，您需要擁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

將下列政策連接至您要使用的 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`* 是設定 DevOps Guru 的使用者的帳戶 ID，而 *`devops-guru-role`* 是涉及的個別使用者的 IAM 角色。您必須將適當的值取代為 *`region-id`*（例如 `us-west-2`) 和 *`my-topic-name`*。

以 IAM 使用者身分新增許可

若要從另一個帳戶使用 Amazon SNS 主題做為 IAM 使用者，請將下列政策連接至您要使用的 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`* 是設定 DevOps Guru 的使用者的帳戶 ID，而 *`devops-guru-user-name`* 是

涉及的個別 IAM 使用者。您必須將適當的值取代為 *region-id* （例如 us-west-2) 和 *my-topic-name*。

> **Note**
>
> 建議您盡可能依賴臨時憑證，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。

從另一個帳戶新增 Amazon SNS 主題

在另一個帳戶中設定 Amazon SNS 主題的許可後，您可以將該 Amazon SNS 主題新增至 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 選項 使用 SNS 主題 ARN 來指定現有主題，才能使用來自另一個帳戶的主題。
- 當您使用 AWS CLI 操作 add-notification-channel 時，您必須在 `NotificationChannelConfig` 物件`TopicArn`中指定 。

使用主控台從另一個帳戶新增 Amazon SNS 主題

1. 開啟位於 https：//https://console.aws.amazon.com/devops-guru/ 的 Amazon DevOps Guru 主控台。
2. 開啟導覽窗格，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 來指定現有的主題。
6. 輸入您要使用的 Amazon SNS 主題 ARN。您應該已透過連接政策來設定此主題的許可。
7. （選用）選擇通知組態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，DevOps Guru 會使用該主題來通知您重要事件，例如建立新洞見的時間。

使用通知管道更新您的 Amazon SNS 政策 （建議）

新增主題後，建議您僅指定包含主題的 DevOps Guru 通知管道的許可，讓您的政策更安全。

使用通知管道更新您的 Amazon SNS 主題政策 （建議）

1. 在您要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 Amazon SNS 主題 ARN 的頻道 ID。頻道 ID 是 guid。

   例如，在下列回應中，具有 ARN 之 主題的頻道 ID `arn:aws:sns:`*region-id*`:`*111122223333*`:`*topic-name*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. 前往您在另一個帳戶中使用 中的主題擁有者 ID 建立的政策the section called “在另一個帳戶中設定 Amazon SNS 主題的許可”。在政策的 `Condition`陳述式中，新增指定 的行`SourceArn`。ARN 包含您的區域 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。

AWS KMS加密 Amazon SNS 主題的許可

您指定的 Amazon SNS 主題可能由 加密 AWS Key Management Service。若要允許 DevOps Guru 使用加密的主題，您必須先建立 ， AWS KMS key 然後將下列陳述式新增至 KMS 金鑰的政策。如需詳細資訊，請參閱AWS KMS 《 使用者指南》中的使用 AWS KMS 加密發佈至 Amazon SNS 的訊息、金鑰識別符 (KeyId)，以及《Amazon Simple Notification Service 開發人員指南》中的資料加密。

> **Note**
>
> DevOps Guru 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。

對 Amazon DevOps Guru 身分和存取進行故障診斷

使用以下資訊來協助您診斷和修正使用 DevOps Guru 和 IAM 時可能遇到的常見問題。

主題

- 我無權在 DevOps Guru 中執行動作
- 我想要提供使用者程式設計存取權
- 我未獲得執行 iam:PassRole 的授權
- 我想要允許 AWS 帳戶外的人員存取我的 DevOps Guru 資源

我無權在 DevOps Guru 中執行動作

如果 AWS 管理主控台 告訴您無權執行 動作，則必須聯絡您的管理員尋求協助。

當使用者mateojackson嘗試使用主控台檢視虛構*my-example-widget*資源的詳細資訊，但沒有虛構aws:*GetWidget*許可時，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。

我想要提供使用者程式設計存取權

如果使用者想要與 AWS 外部互動，則需要程式設計存取 AWS 管理主控台。授予程式設計存取權的方式取決於正在存取的使用者類型 AWS。

若要授予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	根據
IAM	（建議）使用主控台登入資料做為臨時登入資料，以簽署對 AWS CLI、 AWS SDKs程式設計請求。 AWS APIs	請依照您要使用的介面所提供的指示操作。 • 如需 AWS CLI，請參閱AWS Command Line Interface 《使用者指南》中的登入以進行 AWS 本機開發。 • AWS SDKs請參閱 AWS SDKs和工具參考指南中的登入以進行 AWS 本機開發。
人力資源身分 (IAM Identity Center 中管理的使用者)	使用暫時登入資料簽署對 AWS CLI、 AWS SDKs程式設計請求。 AWS APIs	請依照您要使用的介面所提供的指示操作。 • 如需 AWS CLI，請參閱AWS Command Line Interface 《使用者指南》中的設定 AWS CLI 要使用 AWS IAM Identity Center的 。 • AWS SDKs、工具和 AWS APIs，請參閱 AWS SDKs

哪個使用者需要程式設計存取權？	到	根據
		和工具參考指南中的 IAM Identity Center 身分驗證。
IAM	使用暫時登入資料簽署對 AWS CLI、 AWS SDKs程式設計請求。 AWS APIs	遵循《IAM 使用者指南》中將臨時登入資料與 AWS 資源搭配使用的指示。
IAM	(不建議使用) 使用長期憑證簽署對 AWS CLI、 AWS SDKs 或 AWS APIs程式設計請求。	請依照您要使用的介面所提供的指示操作。 • 如需 AWS CLI，請參閱AWS Command Line Interface 《 使用者指南》中的使用 IAM 使用者憑證進行身分驗證。 • AWS SDKs和工具，請參閱 AWS SDKs和工具參考指南中的使用長期憑證進行身分驗證。 • 對於 AWS APIs，請參閱《 IAM 使用者指南》中的管理 IAM 使用者的存取金鑰。

我未獲得執行 iam:PassRole 的授權

如果您收到錯誤，告知您無權執行 `iam:PassRole`動作，您的政策必須更新，以允許您將角色傳遞給 DevOps Guru。

有些 AWS 服務 可讓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 `marymajor` 使用者嘗試使用主控台在 DevOps Guru 中執行動作時，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 沒有將角色傳遞給服務的許可。

```
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。

我想要允許 AWS 帳戶外的人員存取我的 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：

- 若要了解 DevOps Guru 是否支援這些功能，請參閱 Amazon DevOps Guru 如何與 IAM 搭配使用。
- 若要了解如何 AWS 帳戶 在您擁有的 資源之間提供存取權，請參閱《IAM 使用者指南》中的在您擁有 AWS 帳戶 的另一個 IAM 使用者中提供存取權。
- 若要了解如何將資源的存取權提供給第三方 AWS 帳戶，請參閱《IAM 使用者指南》中的將存取權提供給第三方 AWS 帳戶 擁有。
- 如需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)。
- 如需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 中的跨帳戶資源存取。

記錄和監控 DevOps Guru

監控是維護 DevOps Guru 和其他 AWS 解決方案可靠性、可用性和效能的重要部分。AWS 提供下列監控工具來監看 DevOps Guru、在發生錯誤時回報，以及適時採取自動動作：

- Amazon CloudWatch AWS 會即時監控您的 AWS 資源和您在 上執行的應用程式。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，您可以讓 CloudWatch 追蹤 CPU 使用量或其他 Amazon EC2 執行個體指標，並在需要時自動啟動新的執行個體。如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南。
- AWS CloudTrail 會擷取由您的帳戶或代表 AWS 您的帳戶發出的 API 呼叫和相關事件，並將日誌檔案交付至您指定的 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 位址，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

使用 Amazon CloudWatch 監控 DevOps Guru

您可以使用 CloudWatch 監控 DevOps Guru，這會收集原始資料並將其處理為可讀且近乎即時的指標。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。如需更多資訊，請參閱 Amazon CloudWatch 使用者指南。

對於 DevOps Guru，您可以追蹤 指標以取得 DevOps Guru 用量的洞見和指標。您可能想要觀察建立的大量 `Insights`，以協助您判斷營運解決方案是否發生異常行為。或者，您可能想要監看 DevOps Guru 用量，以協助追蹤您的成本。

DevOps Guru 服務會在 `AWS/DevOps-Guru` 命名空間中報告下列指標。

主題

Insight 指標

您可以使用 CloudWatch 追蹤指標，向您顯示您的帳戶 AWS 中建立了多少洞見。您可以指定要追蹤的`Type`維度`proactive`或`reactive`洞見。如果您想要追蹤所有洞見，請勿指定維度。

指標

指標	Description
`Insight`	在 AWS 帳戶中建立的洞見數量。 有效維度：`Type` 有效統計資料：範例計數、總和 單位：Count

DevOps Guru Insight 指標支援下列維度。

Dimensions (尺寸)

維度	Description
Type	這是洞見的類型。如果您想要追蹤所有洞見，請勿指定Insights指標的維度。有效值為：proactive 、reactive。

DevOps Guru 用量指標

您可以使用 CloudWatch 來追蹤 Amazon DevOps Guru 用量。

指標

指標	Description
CallCount	下列其中一個 DevOps Guru 方法進行的呼叫數量。 • ListInsights • ListAnomaliesForInsight • ListRecommendations • ListEvents • SearchInsights • DescribeInsight • DescribeAnomaly 有效維度：Service、Class、Type、 Resource

指標	Description
	有效統計資料：範例計數、總和 單位：Count

DevOps Guru 用量指標支援下列維度。

Dimensions (尺寸)

維度	Description
`Service`	這是包含 資源的 AWS 服務名稱。例如，對於 DevOps Guru，此值為 `DevOps-Guru` 。
`Class`	這是追蹤的資源類別。DevOps Guru 使用此維度與值 `None`。
`Type`	這是追蹤的資源類型。DevOps Guru 使用此維度與值 `API`。
`Resource`	這是 DevOps Guru 操作的名稱。有效值為：`ListInsights` 、`ListAnomaliesForInsight` 、`ListRecommendations` 、`ListEvents` 、`SearchInsights` 、`DescribeInsight` 、`DescribeAnomaly` 。

使用 記錄 Amazon DevOps Guru API 呼叫 AWS CloudTrail

Amazon DevOps Guru 已與 整合 AWS CloudTrail，此服務提供由使用者、角色或 DevOps Guru 中的 AWS 服務所採取之動作的記錄。CloudTrail 會將 DevOps Guru 的 API 呼叫擷取為事件。擷取的呼叫包括來自 DevOps Guru 主控台的呼叫，以及對 DevOps Guru API 操作的程式碼呼叫。如果您建立追蹤，則可以將 CloudTrail 事件持續交付至 Amazon S3 儲存貯體，包括 DevOps Guru 的事件。即使您未設定追蹤，依然可以透過 CloudTrail 主控台中的事件歷史記錄檢視最新事件。您可以使用 CloudTrail 所收集的資訊，判斷向 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，以及其他詳細資訊。

若要進一步了解 CloudTrail，請參閱「AWS CloudTrail 使用者指南」。

CloudTrail 中的 DevOps Guru 資訊

當您建立 AWS 帳戶時，會在您的帳戶上啟用 CloudTrail。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 服務事件一起記錄在 CloudTrail 事件中。您可以在 AWS 帳戶中檢視、搜尋和下載最近的事件。如需詳細資訊，請參閱「使用 CloudTrail 事件歷史記錄檢視事件」。

若要持續記錄您 AWS 帳戶中的事件，包括 DevOps Guru 的事件，請建立追蹤。線索能讓 CloudTrail 將日誌檔案交付至 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。線索會記錄 AWS 分割區中所有區域的事件，並將日誌檔案傳送到您指定的 Amazon S3 儲存貯體。此外，您可以設定其他 AWS 服務，以進一步分析和處理 CloudTrail 日誌中所收集的事件資料。如需詳細資訊，請參閱下列內容：

- 建立追蹤的概觀
- CloudTrail 支援的服務和整合
- 設定 CloudTrail 的 Amazon SNS 通知
- 接收多個區域的 CloudTrail 日誌檔案和接收多個帳戶的 CloudTrail 日誌檔案

DevOps Guru 支援將其所有動作記錄為 CloudTrail 日誌檔案中的事件。如需詳細資訊，請參閱 DevOps Guru 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 userIdentity 元素。

了解 DevOps Guru 日誌檔案項目

追蹤是一種組態，能讓事件以日誌檔案的形式交付到您指定的 Amazon S3 儲存貯體。CloudTrail 日誌檔案包含一或多個日誌專案。一個事件為任何來源提出的單一請求，並包含請求動作、請求的日期和時間、請求參數等資訊。CloudTrail 日誌檔並非依公有 API 呼叫的堆疊追蹤排序，因此不會以任何特定順序出現。

以下範例顯示的是展示 `UpdateResourceCollection` 動作的 CloudTrail 日誌項目。

```
{
```

```
  "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 Guru 和介面 VPC 端點 (AWS PrivateLink)

您可以在呼叫 Amazon DevOps Guru APIs時使用 VPC 端點。當您使用 VPC 端點時，您的 API 呼叫會更安全，因為它們包含在 VPC 中且無法存取網際網路。如需詳細資訊，請參閱《Amazon DevOps Guru API 參考》中的動作。

您可以透過建立介面 VPC 端點，在 VPC 和 DevOps Guru 之間建立私有連線。介面端點採用 AWS PrivateLink技術，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，私下存取 DevOps Guru APIs。VPC 中的執行個體不需要公有 IP 地址，即可與 DevOps Guru APIs通訊。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》中的界面 VPC 端點 (AWS PrivateLink)。

DevOps Guru VPC 端點的考量事項

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

DevOps Guru 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 () 為 DevOps Guru 服務建立 VPC 端點AWS CLI。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，您可以使用區域的預設 DNS 名稱向 DevOps Guru 提出 API 請求，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 DevOps Guru 建立 VPC 端點政策

您可以將端點政策連接至控制 DevOps Guru 存取的 VPC 端點。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：DevOps Guru 動作的 VPC 端點政策

以下是 DevOps Guru 的端點政策範例。連接到端點時，此政策會授予所有資源上所有主體的所列 DevOps Guru 動作的存取權。

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

DevOps Guru 中的基礎設施安全

Amazon DevOps Guru 是受管服務，受到 AWS 全球網路安全的保護。如需 AWS 安全服務以及如何 AWS 保護基礎設施的資訊，請參閱AWS 雲端安全。若要使用基礎設施安全的最佳實務設計您的 AWS 環境，請參閱安全支柱 AWS Well-Architected Framework 中的基礎設施保護。

您可以使用 AWS 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。

Amazon DevOps Guru 中的彈性

AWS 全球基礎設施是以 AWS 區域和可用區域為基礎建置。 AWS 區域提供多個分開且隔離的實際可用區域，並以低延遲、高輸送量和高度備援聯網功能相互連結。DevOps Guru 在多個可用區域中操作，並將成品資料和中繼資料存放在 Amazon S3 和 Amazon DynamoDB 中。您的加密資料會以備援方式存放在多個設施和每個設施中的多個裝置，使其具有高可用性和高耐用性。

如需 AWS 區域和可用區域的詳細資訊，請參閱 AWS 全球基礎設施。

Amazon DevOps Guru 的配額和限制

下表列出 Amazon DevOps Guru 中的目前配額。此配額適用於每個 AWS 帳戶的每個支援 AWS 區域。

通知

您可以一次指定的 Amazon Simple Notification Service 主題數目上限	2

CloudFormation 堆疊

您可以指定的 AWS CloudFormation 堆疊數量上限	1000

DevOps Guru 資源監控限制

資源描述	限制	可以提高
監控 Amazon Simple Queue Service (Amazon SQS) 佇列的預設限制	100*	是**

*適用於在 2023 年 6 月 29 日當天或之後建立的新 DevOps Guru 帳戶，以及截至相同日期且具有少於 100 個 Amazon SQS 佇列的現有帳戶。

**若要請求變更此限制，請聯絡 支援 https：//https://aws.amazon.com/contact-us。您可以請求 Amazon SQS 佇列監控限制為 100、500、1，000、5，000 或 10，000。

用於建立、部署和管理 API 的 DevOps Guru 配額

下列固定配額適用於使用、API Gateway 主控台或 API Gateway REST API 及其 SDKs 在 DevOps Guru 中建立 AWS CLI、部署和管理 API。

如需所有 DevOps Guru APIs的清單，請參閱 Amazon DevOps Guru 動作。

預設配額	可以提高	
每個帳戶每 1 秒 20 個請求	是	

Amazon DevOpsGuru 文件歷史記錄

下表說明此 DevOpsGuru 版本的文件。

- API 版本：最新
- 文件最近更新時間：2023 年 8 月 9 日

變更	描述	日期
受管政策更新	Amazon SNS 訂閱和訂閱清單存取已新增至`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 Amazon DevOps Guru 的身分型政策。	2023 年 8 月 9 日
客戶受管加密金鑰	DevOpsGuru 現在支援使用的客戶受管金鑰加密 AWS KMS。如需詳細資訊，請參閱 DevOpsGuru 中的資料保護。	2023 年 7 月 5 日
DevOpsGuru for RDS 支援 RDS PostgreSQL	適用於 RDS 的 DevOpsGuru 可以偵測 PostgreSQL 資料庫中的效能瓶頸和其他洞見。如需詳細資訊，請參閱 DevOpsGuru for RDS 的優點。	2023 年 3 月 30 日
DevOpsGuru for RDS 支援主動洞察	DevOpsGuru for RDS 發佈主動洞察與建議，協助您解決 Aurora 資料庫的問題，以免問題變得更嚴重。如需詳細資	2023 年 2 月 28 日

	訊，請參閱在 DevOpsGuru for RDS 中使用異常。	
分析的資源頁面	DevOpsGuru 主控台中的新頁面會列出您帳戶中由 DevOpsGuru 分析的資源。如需詳細資訊，請參閱檢視 DevOpsGuru 分析的資源。	2022 年 10 月 20 日
新的通知組態設定	您現在可以選擇是否接收所有通知，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 Amazon Amazon SNS 通知組態。	2022 年 9 月 30 日
將日誌異常分析新增至受管政策	AWS DevOpsGuru 的 受管政策已在 IAM 主控台中更新，以支援對 CloudWatch 動作 的存取`FilterLogEvents` 。如需詳細資訊，請參閱 DevOpsGuru 對 AWS 受管政策和服務連結角色的更新。	2022 年 8 月 30 日
已新增日誌異常分析	您可以在 DevOpsGuru 主控台中檢視與洞見相關的日誌群組詳細資訊。還有擴展的服務連結角色，可用於描述 CloudWatch 日誌和串流。如需詳細資訊，請參閱 DevOpsGuru 主控台中的了解洞見，以及 DevOpsGuru 對 AWS 受管政策和服務連結角色的更新。	2022 年 7 月 12 日

CodeGuru Profiler 整合	DevOpsGuru 現在與 Amazon CodeGuru Profiler 整合了 EventBridge 受管規則。CodeGuru Profiler 的每個傳入事件都是主動異常報告。如需詳細資訊，請參閱與 CodeGuru Profiler 整合。	2022 年 3 月 7 日
服務連結角色和受管政策更新	IAM 主控台中可用的擴展政策。這些變更可讓 DevOpsGuru 支援與 Amazon Relational Database Service (Amazon RDS) 的增強整合。如需詳細資訊，請參閱使用 DevOpsGuru 的服務連結角色AWS 和受管（預先定義）政策 DevOps。	2021 年 12 月 21 日
已新增新的受管政策	`AmazonDevOpsGuruConsoleFullAccess` 政策已新增。如需詳細資訊，請參閱 Amazon DevOps Guru 的身分型政策。	2021 年 12 月 6 日
支援使用 AWS 標籤定義您的應用程式	您現在可以使用 AWS 標籤來識別您希望 DevOpsGuru 分析的資源、識別應用程式中的資源，以及在主控台中篩選洞見。如需詳細資訊，請參閱使用標籤來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 主控台中可用的擴展政策。這些變更可讓 DevOpsGuru 支援與 Amazon Relational Database Service (Amazon RDS) 的增強整合。如需詳細資訊，請參閱使用 DevOpsGuru 的服務連結角色AWS 和受管（預先定義）政策 DevOps。	2021 年 12 月 1 日
Amazon RDS 支援	DevOpsGuru 現在為您的應用程式中的 Amazon Relational Database Service (Amazon RDS) 資源提供全面的分析和洞見。如需詳細資訊，請參閱在 DevOpsGuru for Amazon RDS 中使用異常。	2021 年 12 月 1 日
Amazon EventBridge 整合	DevOpsGuru 現在與 EventBridge 整合，以通知您與 DevOpsGuru 洞察相關的特定事件。如需詳細資訊，請參閱使用 EventBridge。	2021 年 11 月 18 日
AWS 已新增 受管政策	新增了新的 AWS 受管政策。此`AmazonDevOpsGuruOrganizationsAccess` 政策提供組織內 DevOps Guru 的存取權。如需詳細資訊，請參閱身分型政策。	2021 年 11 月 16 日
服務連結角色政策更新	IAM 主控台中可用的擴展政策。此變更可讓 DevOpsGuru 支援多帳戶檢視。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洞見和指標。如需詳細資訊，請參閱什麼是 Amazon DevOpsGuru。	2021 年 11 月 4 日
一般可用性版本	Amazon DevOpsGuru 現已正式推出 (GA)。	2021 年 5 月 4 日
新主題	您現在可以為 DevOpsGuru 產生每月成本估算，以分析您的資源。如需詳細資訊，請參閱估算 Amazon DevOpsGuru 成本。	2021 年 4 月 27 日
VPC 端點支援	您現在可以使用 VPC 端點來改善資源分析和洞見產生的安全性。如需詳細資訊，請參閱DevOpsGuru 和界面 VPC 端點 (AWS PrivateLink)。	2021 年 4 月 15 日
新主題	已新增如何使用 Amazon CloudWatch 監控 DevOpsGuru 的新主題。如需詳細資訊，請參閱使用 Amazon CloudWatch 監控 DevOpsGuru。	2020 年 12 月 11 日
預覽版本	這是 Amazon DevOpsGuru 使用者指南的預覽版本。	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。