aws

使用者指南

Amazon Macie

Amazon Macie: 使用者指南

Table of Contents

什麼是 Amazon Macie？

Amazon Macie 是一種資料安全服務，透過使用機器學習和模式比對來探索敏感資料、提供資料安全風險的可見性，以及啟用自動保護以防範這些風險。

為了協助您管理組織 Amazon Simple Storage Service (Amazon S3) 資料資產的安全狀態，Macie 會提供 S3 一般用途儲存貯體的清單，並自動評估和監控儲存貯體的安全性和存取控制。如果 Macie 偵測到您資料的安全性或隱私權存在潛在問題，例如變成可公開存取的儲存貯體，Macie 會視需要產生調查結果來檢閱並修補此問題。

Macie 也會自動化敏感資料的探索和報告，讓您更好地瞭解組織在 Amazon S3 中存放的資料。若要偵測敏感資料，您可以使用 Macie 提供的內建條件和技術，您定義的自訂條件，或兩者的組合。如果 Macie 偵測到 S3 物件中的敏感資料，Macie 會產生一個發現項目，通知您找到的敏感資料。

除了發現結果之外，Macie 還提供統計資料和資訊，可深入瞭解 Amazon S3 資料的安全狀態，以及敏感資料可能存放在資料資產中的位置。統計資料和資訊可指導您決策，對特定 S3 儲存貯體和物件執行更深入的調查。您可以使用 Amazon Macie 主控台或 Amazon Macie API 來檢閱和分析發現項目、統計資料和其他資訊。您也可以利用與 Amazon 的 Macie 整合， EventBridge 並使用其他服務、應用程式和系統 AWS Security Hub 來監控、處理和補救發現結果。

主題

Amazon Macie 的特點

以下是 Amazon Macie 可協助您探索、監控和保護 Amazon S3 中敏感資料的一些關鍵方法。

自動探索敏感資料

使用 Macie，您可以透過兩種方式自動探索和報告敏感資料：將 Macie 設定為執行自動化的敏感資料探索，以及建立和執行敏感資料探索工作。如果 Macie 偵測到 S3 物件中的敏感資料，就會為您建立敏感資料尋找。此發現項目提供 Macie 偵測到之敏感資料的詳細報告。

自動化敏感資料探索可讓您廣泛掌握敏感資料在 Amazon S3 資料資產中的位置。使用此選項，Macie 會持續評估您的 S3 儲存貯體庫存，並使用取樣技術從儲存貯體中識別和選取代表性的 S3 物件。然後，Macie 會擷取並分析選取的物件，檢查它們是否有敏感資料。

敏感資料探索工作提供更深入、更具針對性的分析。使用此選項，您可以定義分析的廣度和深度 — 要分析的 S3 儲存貯體、取樣深度，以及從 S3 物件屬性衍生的自訂準則。您也可以將工作設定為僅執行一次以進行隨選分析和評估，或定期分析、評估和監視定期執行一次。

這兩個選項都可協助您建立和維護組織存放在 Amazon S3 中的資料以及該資料的任何安全或合規風險的全面檢視。

探索各種敏感資料類型

若要使用 Macie 探索敏感資料，您可以使用內建的準則和技術 (例如機器學習和模式比對) 來分析 S3 儲存貯體中的物件。這些標準和技術 (稱為受管資料識別碼) 可以偵測許多國家和地區不斷增加的敏感資料類型清單，包括多種類型的個人識別資訊 (PII)、財務資訊和憑證資料。

您也可以使用自訂資料識別碼。自訂資料識別碼是您定義用來偵測機密資料的一組準則 (regex)，定義要比對的文字模式 (可選擇性地定義字元序列和細化結果的鄰近規則)。使用此類識別碼，您可以偵測反映特定案例、智慧財產權或專屬資料的敏感資料。您可以補充 Macie 提供的受管理資料識別碼。

若要微調分析，您也可以使用允許清單。允許清單定義您希望 Macie 在 S3 物件中忽略的特定文字和文字模式。這些通常是您特定案例或環境的敏感資料例外狀況，例如組織的公開代表姓名、組織的公用電話號碼或組織用於測試的範例資料。

評估和監控資料以確保安全性和存取控制

當您啟用 Macie 時，Macie 會自動產生並開始維護 S3 一般用途儲存貯體的完整庫存。Macie 還開始評估和監視存儲桶的安全性和訪問控制。如果 Macie 偵測到值區的安全性或隱私權存在潛在問題，就會為您建立原則搜尋結果。

除了特定發現項目之外，儀表板還提供 Amazon S3 資料彙總統計資料的快照。這包括關鍵指標的統計資料，例如可公開存取或與其他人共用的值區數目 AWS 帳戶。您可以向下鑽研每個統計資料以檢閱支援資料。

Macie 也會針對庫存中的個別 S3 儲存貯體提供詳細資訊和統計資料。資料包括值區公開存取和加密設定的劃分，以及 Macie 可分析以偵測值區中敏感資料的物件大小和數量。您可以瀏覽庫存，或按特定字段對庫存進行排序和過濾。

審查和分析發現

在 Macie 中，發現項目是 Macie 在 S3 物件中偵測到的敏感資料的詳細報告，或 S3 一般用途儲存貯體的安全性或隱私權的潛在問題。每個發現項目都會提供嚴重性等級、受影響資源的相關資訊，以及其他詳細資訊，例如 Macie 偵測到資料或問題的時間和方式。

若要檢閱、分析和管理發現項目，您可以使用 Amazon Macie 主控台上的「發現項目」頁面。這些頁面列出您的發現項目，並提供個別發現項目的詳細資訊 它們還提供了多個選項，用於分組，過濾，排序和抑制發現項目。您也可以使用 Amazon Macie API 來查詢、擷取和隱藏發現項目。如果您使用 API，您可以將資料傳遞至其他應用程式、服務或系統，以進行更深入的分析、長期儲存或報告。

監控和處理與其他服務和系統的發現

為了支援與其他服務和系統的整合，Macie 將調查結果發佈給 Amazon EventBridge 作為尋找事件。 EventBridge 是一種無伺服器事件匯流排服務，可將發現項目資料路由到 AWS Lambda 功能和 Amazon Simple Notification Service (Amazon SNS) 主題等目標。有了 EventBridge，您可以在現有的安全性和合規性工作流程中，以近乎即時的方式監控和處理發現項目。

您可以設定 Macie 也將發現項目發佈至 AWS Security Hub。Security Hub 是一項服務，可提供您 AWS 環境中安全性狀態的全面檢視，並協助您根據安全性產業標準和最佳做法來檢查環境。使用 Security Hub，您可以更輕鬆地監視和處理發現項目，作為對組織中的安全性狀態進行更廣泛分析的一部分 AWS。您也可以彙總多個發現項目 AWS 區域，然後監視並處理來自單一「區域」的彙總發現項目資料。

集中管理多個 Macie 帳戶

如果您的 AWS 環境有多個帳戶，您可以集中管理環境中帳戶的 Macie。您可以通過兩種方式執行此操作，通過將 Macie 與 Macie 集成 AWS Organizations 或通過在 Macie 中發送和接受會員邀請來完成此操作。

在多帳戶配置中，指定的 Macie 管理員可以執行某些任務，並訪問屬於同一組織成員的帳戶的某些 Macie 設置，數據和資源。任務包括檢閱成員帳戶所擁有之 S3 儲存貯體的相關資訊、檢閱這些儲存貯體的政策發現項目，以及檢查值區中是否有敏感資料。如果帳戶透過關聯 AWS Organizations，Macie 管理員也可以為組織中的成員帳戶啟用 Macie。

以程式設計方式開發和管

除了 Amazon Macie 控制台外，您還可以使用亞馬遜 Macie API 與 Macie 進行交互。Amazon Macie API 可讓您以程式設計方式存取 Macie 帳戶設定、資料和資源。

若要以程式設計方式與 Macie 互動，您可以將 HTTPS 要求直接傳送至 Macie，或使用目前版本的 AWS 命令列工具或 SDK。 AWS AWS 提供包含各種語言和平台的程式庫和範例程式碼 (例如 Java PowerShell、Go、Python、C++ 和 .NET) 的工具和 SDK。

訪問 Amazon Macie

Amazon Macie 是在大多數 AWS 區域可用. 如需目前可使用 Macie 的區域清單，請參閱. AWS 一般參考 如需管理您的帳戶 AWS 區域 的相關資訊 AWS 帳戶，請參閱AWS Account Management 參考指南中的「指定 AWS 區域 您的帳戶可以使用的項目」。

在每個區域中，您可以使用以下任何一種方式與 Macie 合作。

AWS Management Console

這 AWS Management Console 是一個基於瀏覽器的介面，您可以使用它來建立和管理 AWS 資源。作為該主控台的一部分，Amazon Macie 主控台可讓您存取 Macie 帳戶、資料和資源。您可以使用 Macie 主控台來執行任何 Macie 工作 — 檢閱 S3 儲存貯體的統計資料和其他資訊、建立和執行敏感資料探索任務、檢閱和分析發現項目等。

AWS 命令行工具

使用 AWS 命令行工具，您可以在系統的命令行中發出命令以執行 Macie 任務和 AWS 任務。使用命令行可以比使用控制台更快，更方便。若您想要建構執行 任務的指令碼，命令列工具也非常實用。

AWS 提供兩組指令行工具： AWS Command Line Interface (AWS CLI) 和 AWS Tools for PowerShell. 若要取得有關安裝和使用的資訊 AWS CLI，請參閱《使AWS Command Line Interface 用指南》。若要取得有關安裝和使用的「工具」的資訊 PowerShell，請參閱《使AWS Tools for PowerShell 用指南》。

AWS 開發套件

AWS 提供包含各種程式設計語言和平台 (例如 Java、Go、Python、C++ 和 .NET) 的程式庫和範例程式碼的開發套件。SDK 提供方便、程式化的方式存取 Macie 和其他功能。 AWS 服務他們還處理諸如密碼編譯簽名請求，管理錯誤以及自動重試請求等任務。如需安裝和使用 AWS SDK 的詳細資訊，請參閱建置在其上 AWS的工具。

Amazon Macie 休息 API

Amazon Macie REST API 為您提供對 Macie 帳戶、資料和資源的全面程式設計存取。使用此 API，您可以將 HTTPS 請求直接發送到馬西。但是，與 AWS 命令行工具和 SDK 不同，使用此

API 需要您的應用程序處理低級別的詳細信息，例如生成散列以簽署請求。如需有關此 API 的資訊，請參閱 Amazon Macie API 參考資料。

Amazon Macie 的定價

與其他 AWS 產品一樣，使用 Amazon Macie 沒有合約或最低承諾。

Macie 定價以多種維度為基礎，包括評估和監控 S3 儲存貯體的安全性和存取控制、監控 S3 物件以自動化敏感資料探索，以及分析 S3 物件以探索和報告物件中的敏感資料。如需詳細資訊，請參閱 Amazon Macie 定價。

為了幫助您了解和預測使用 Macie 的成本，Macie 會為您的帳戶提供估計的使用費用。您可以在 Amazon Macie 控制台上查看這些估計值，並使用 Amazon Macie API 訪問它們。視您使用服務的方式而定，搭配使用其他 AWS 服務 功能時可能會產生額外費用，例如從 Amazon S3 擷取儲存貯體資料，以及使用客戶管理解密物件 AWS KMS keys 以進行分析。

當您第一次啟用 Macie 時，系統會自動註冊您 AWS 帳戶 的 Macie 30 天免費試用版。這包括在中作為組織一部分啟用的個別帳戶 AWS Organizations。在免費試用期間，在適用項目中使用 Macie AWS 區域 來評估和監控 S3 儲存貯體的安全性和存取控制無須付費。根據您的帳戶設定，免費試用還包括針對 Amazon S3 資料執行自動化敏感資料探索。免費試用不包括執行敏感資料探索任務來探索和報告 S3 物件中的敏感資料。

為了幫助您了解並預測免費試用期結束後使用 Macie 的成本，Macie 會根據您在試用期間使用 Macie 的情況，為您提供估計的使用費用。您的使用量資料也會指出免費試用期結束前剩餘的時間長度。您可以在 Amazon Macie 主控台上查看此資料，並使用 Amazon Macie API 進行存取。

相關服務

為了在中進一步保護您的資料、工作負載和應用程式 AWS，請考慮將以下 AWS 服務 內容與 Amazon Macie 結合使用。

AWS Security Hub

AWS Security Hub 可讓您全面檢視 AWS 資源的安全狀態，並協助您根據安全性產業標準和最佳實務來檢查 AWS 環境。部分原因是從多個 AWS 服務 (包括 Macie) 和支援的 AWS 合作夥伴網路 (APN) 產品中使用、彙總、組織和優先順序排列您的安全發現結果。Security Hub 可協助您分析安全性趨勢，並識別 AWS 環境中最優先順序的安全性問題。

若要進一步了解資訊 Security Hub，請參閱使AWS Security Hub 用者指南。若要瞭解如何一起使用 Macie 和 Security Hub，請參閱Amazon Macie 與集成 AWS Security Hub。

Amazon GuardDuty

Amazon GuardDuty 是一種安全監控服務，可分析和處理特定類型的 AWS 日誌，例如 Amazon S3 的 AWS CloudTrail 資料事件日誌和 CloudTrail 管理事件日誌。它使用威脅情報摘要，例如惡意 IP 位址和網域的清單，以及機器學習來識別您 AWS 環境中未預期和潛在未經授權的惡意活動。

若要進一步了解 GuardDuty，請參閱 Amazon GuardDuty 使用者指南。

若要深入了解其他 AWS 安全性服務，請參閱上的安全性、身分識別和合規性 AWS。

開始使用 Amazon Macie

本教程介紹了 Amazon Macie。您將學習如何為您 AWS 帳戶啟用麥西。您還將學習如何評估 Amazon Simple Storage Service (Amazon S3) 安全狀態，以及設定關鍵設定和資源，以探索和報告 S3 儲存貯體中的敏感資料。

任務

- 開始之前
- 步驟 1：啟用 Amazon Macie
- 步驟 2：設定敏感資料探索結果的儲存庫
- 步驟 3：探索範例發現項目
- 步驟 4：建立工作以探索敏感資料
- 步驟 5：查看您的發現

開始之前

當您註冊 Amazon Web Services（AWS），您的帳戶將自動註冊為所有人 AWS 服務，包括 Amazon Macie。不過，若要啟用和使用 Macie，您必須先設定許可，以便存取 Amazon Macie 主控台和 API 操作。您或您的管理 AWS 員可以使用 AWS Identity and Access Management (IAM) 將名為的 AWS 受管政策附加`AmazonMacieFullAccess`到您的 IAM 身分。如需進一步了解，請參閱AWS亞馬遜馬西的受管政策。

步驟 1：啟用 Amazon Macie

設定所需的許可後，您 Amazon Macie 您 AWS 帳戶的. 請按照以下步驟為您的帳戶啟用 Macie。

啟用馬西

1. 在以下位置打開 Amazon Macie 控制台 https://console.aws.amazon.com/macie/。
2. 使用頁面右上角的選取 AWS 區域 器，選取您要在其中啟用並使用 Macie 的「區域」。
3. 在 Amazon Macie 頁面上，選擇開始使用。
4. (選擇性) 當您啟用 Macie 時，Macie 會自動建立服務連結角色，授 AWS 服務 與 Macie 代表您呼叫其他 AWS 資源所需的權限。若要檢閱此角色的權限原則，請選擇 [在主控台上檢視角色權限]。若要進一步瞭解此角色，請參閱Amazon Macie 的服務連結角色。

5. 選擇 Enable Macie (啟用 Macie)。

在幾分鐘內，Macie 會自動產生並開始維護目前區域中 S3 一般用途儲存貯體的完整清查。Macie 還開始評估和監視存儲桶的安全性和訪問控制。如需進一步了解，請參閱Macie 如何監控 Amazon S3 數據安全。

根據您的帳戶設定，Macie 也會開始為 S3 儲存貯體執行自動化敏感資料探索。Macie 會開始持續識別、選取和分析值區中的代表物件，並檢查物件中是否有敏感資料。隨著分析的進展，Macie 會提供統計數據和其他結果，您可以查看這些結果，通常在為您的帳戶啟用 Macie 的 48 小時內。您可以為您的帳戶設定自動化敏感資料探索設定，以量身打造分析。如需進一步了解，請參閱自動化敏感資料探索如何運作。

若要檢閱 Amazon S3 資料的彙總統計資料，請在主控台的導覽窗格中選擇「摘要」。若要檢閱有關庫存中個別 S3 儲存貯體的詳細資訊，請在導覽窗格中選擇 S3 儲存貯體。若要顯示值區的明細，請選擇值區。詳細資料面板會顯示統計資料和其他資訊，以深入瞭解值區資料的安全性、隱私權和敏感性。若要瞭解這些詳細資訊，請參閱檢閱您的 S3 儲存貯體庫存。

步驟 2：設定敏感資料探索結果的儲存庫

使用 Amazon Macie，您可以透過兩種方式探索 S3 儲存貯體中的敏感資料：將 Macie 設定為執行自動化敏感資料探索，以及執行敏感資料探索任務。敏感資料探索任務是您建立的工作，用於分析 S3 儲存貯體中的物件，以判斷物件是否包含敏感資料。

Macie 會為您執行敏感資料探索任務或執行自動化敏感資料探索時分析的每個 S3 物件建立記錄。這些記錄稱為敏感資料探索結果，記錄有關個別物件分析的詳細資料。Macie 也會為因錯誤或問題而無法分析的物件建立敏感資料探索結果。敏感資料探索結果為您提供分析記錄，這些記錄對於資料隱私權和保護稽核或調查有幫助。

Macie 只會儲存您的敏感資料探索結果 90 天。若要存取結果並啟用它們的長期儲存和保留，請將 Macie 設定為將結果存放在 S3 儲存貯體中。您應該在啟用 Macie 後的 30 天內執行此操作。執行此操作之後，儲存貯體可做為所有敏感資料探索結果的確定長期存放庫。

若要瞭解如何設定此儲存庫，請參閱儲存及保留敏感資料探索結果。

步驟 3：探索範例發現項目

在 Amazon Macie 中，發現項目分為兩類：政策發現和敏感資料發現項目。當 S3 一般用途儲存貯體的政策或設定以降低儲存貯體和儲存貯體物件的安全性或隱私權的方式變更時，Macie 會建立政策尋

找。Macie 會在偵測到 S3 物件中的敏感資料時建立敏感資料尋找。在每個類別中，有多種類型的發現項目。

若要探索並瞭解 Macie 提供的不同類別和發現項目類型，請選擇性地建立並檢閱發現項目範例。範例發現項目會使用範例資料和預留位置值來示範 Macie 可能包含在每一種發現項目類型中的資訊種類。

請依照下列步驟建立和檢閱發現項目範例。

若要建立和檢閱發現項目範例

1. 在以下位置打開 Amazon Macie 控制台 https://console.aws.amazon.com/macie/。
2. 在導覽窗格中，選擇設定。
3. 在範例發現項目下，選擇產生範例發現項目 Macie 會為 Macie 支援的每種類型的發現項目產生一個範例搜尋結果。
4. 在導覽窗格中，選擇調查結果。「發現項目」頁面會顯示目前帳戶的發現項目 AWS 區域。這包括您在上一個步驟中建立的發現項目範例。
5. 在「發現項目」頁面上，找出類型以 [SAMPLE] 開頭的發現項目。
6. 若要檢閱特定範例發現項目的詳細資訊，請選擇發現項目。詳細資料面板會顯示發現項目的詳細資料。

若要瞭解每種尋找項目類型，請參閱問題清單類型。若要深入瞭解如何建立和檢閱範例發現項目，請參閱使用範例發現項目。

步驟 4：建立工作以探索敏感資料

若要探索並報告 S3 儲存貯體中的機密資料，您可以執行敏感資料探索任務。敏感資料探索任務是您建立的工作，用於分析 S3 儲存貯體中的物件，以判斷物件是否包含敏感資料。與自動化敏感資料探索不同，您可以定義分析的廣度和深度。您也可以指定執行工作的頻率 (一次或按排程定期執行)。

請依照下列步驟建立工作，並在建立工作後立即執行一次，並使用預設設定。若要瞭解如何建立定期執行或使用自訂設定的工作，請參閱建立敏感資料探索任務。

建立敏感資料探索工作

1. 在以下位置打開 Amazon Macie 控制台 https://console.aws.amazon.com/macie/。
2. 在導覽窗格中，選擇 Jobs (任務)。
3. 選擇建立作業。

4. 在 [選擇 S3 儲存貯體] 步驟中，選擇 [選取特定儲存貯體 然後，在表格中，針對您要分析任務的每個 S3 儲存貯體選取核取方塊。

   此表格提供目前 S3 一般用途儲存貯體的完整清查 AWS 區域。若要更輕鬆地尋找特定值區，請在表格上方的篩選方塊中輸入篩選條件。您也可以選擇表格中的欄標題來排序表格。

5. 完成選取值區後，請選擇「下一步」。
6. 對於 [檢閱 S3 儲存貯體] 步驟，請檢閱並驗證您的儲存貯體選項，然後選擇 [下一步]。
7. 在 [精簡範圍] 步驟中，選擇 [一次性工作]，然後選擇 [下一步]。
8. 在 [選取受管理的資料識別碼] 步驟中，選擇 [建議 選擇性地複查我們針對工作建議的受管理資料識別碼表格，然後選擇 [下一步]。

   受管資料識別碼是一組內建準則和技術，用來偵測特定類型的敏感資料，例如特定國家或地區的信用卡號碼、 AWS 秘密存取金鑰或護照號碼。如需進一步了解，請參閱使用受管資料識別符。

9. 在「選取自訂資料識別碼」步驟中，選擇「下一步」

   自訂資料識別碼是您定義用來偵測機密資料的一組準則 (regex)，定義要比對的文字模式 (可選擇性地定義字元序列和細化結果的鄰近規則)。如需進一步了解，請參閱建置自訂資料識別符。

10. 在 [選取允許清單] 步驟中，選擇 [下一步]。

    在 Macie 中，允許清單指定您希望 Macie 在檢查 S3 物件中是否有敏感資料時忽略的文字或文字模式。這些通常是特定案例或環境的敏感資料例外狀況。如需進一步了解，請參閱使用允許清單定義敏感資料例外。

11. 在 [輸入一般設定] 步驟中，輸入工作的名稱，並選擇性地輸入工作的描述。然後選擇下一步。
12. 對於 [檢閱] 和 [建立] 步驟，檢閱工作的組態設定，並確認其正確無誤。

    您也可以檢閱執行工作的總估計成本 (以美元為單位)。預估值可協助您決定是否在儲存工作之前調整工作的設定。如需進一步了解，請參閱預測敏感資料探索任務的成本。

13. 完成檢閱和驗證工作設定後，請選擇 [送出]。

馬西立即開始運行作業。若要瞭解如何監視工作，請參閱檢查敏感資料探索工作的狀態。

步驟 5：查看您的發現

Amazon Macie 會自動監控 S3 一般用途儲存貯體的安全性和存取控制，並建立政策發現結果，以報告儲存貯體安全性或隱私權的潛在問題。如果您執行敏感資料探索工作或將 Macie 設定為執行自動化敏

感資料探索，Macie 會建立敏感資料發現項目，以報告在 S3 物件中偵測到的敏感資料。若要深入瞭解發現項目，請參閱分析發現。

請依照下列步驟檢閱您的發現項目。

若要檢閱您的發現

1. 在以下位置打開 Amazon Macie 控制台 https://console.aws.amazon.com/macie/。
2. 在導覽窗格中，選擇調查結果。「發現項目」頁面會顯示目前帳戶的發現項目 AWS 區域。
3. (選擇性) 若要依特定條件篩選發現項目，請在表格上方的篩選方塊中輸入條件。
4. 若要複查特定發現項目的詳細資訊，請選擇發現項目。詳細資料面板會顯示發現項目的詳細資料。

若要深入瞭解，包括如何分組和篩選發現項目，請參閱檢閱問題清單。

Amazon Macie 概念和術語

在 Amazon Macie 中，我們以通用 AWS 概念和術語為基礎，並使用這些額外術語。

帳戶

一種標準 AWS 帳戶 ，其中包含您的 AWS 資源以及可存取這些資源的身分識別。

要使用 Macie，請使用您的 AWS 帳戶 憑據登錄，選擇要 AWS 區域 在其中使用 Macie，然後在該區 AWS 帳戶 域中啟用 Macie。 AWS 如需詳細資訊，請參閱 開始使用 Amazon Macie。

Macie 有三種類型的帳戶：

- 管理員帳戶 — 這種類型的帳戶可管理組織的 Macie 帳戶。組織是一組 Macie 帳戶，它們彼此相關聯，並以特定 AWS 區域帳戶群組的形式集中管理。
- 成員帳戶 — 此類型的帳戶與組織的 Macie 管理員帳戶相關聯並管理。
- 獨立帳戶 — 此類型的帳戶既不是管理員，也不是成員帳戶。它不是組織的一部分。

您可以通過兩種方式將 Macie 帳戶添加到組織：通過將 Macie 與集成 AWS Organizations 或通過發送和接受 Macie 成員邀請。如需詳細資訊，請參閱 管理多個 帳戶。

管理員帳戶

在 Macie 中，管理組織的 Macie 帳戶的帳戶。組織是一組 Macie 帳戶，它們彼此相關聯，並以特定 AWS 區域帳戶群組的形式集中管理。

Macie 管理員帳戶的使用者可以存取其組織中所有帳戶的 Amazon 簡單儲存服務 (Amazon S3) 庫存資料、政策發現項目，以及特定 Macie 設定和資源。他們還可以執行自動化敏感資料探索並執行敏感資料探索任務，以偵測帳戶所擁有的 S3 儲存貯體中的敏感資料。視帳戶被指定為管理員帳戶的方式而定，他們也可以針對其組織中的其他帳號執行其他任務。

如需詳細資訊，請參閱 管理多個 帳戶。

允許清單

在 Macie 中，允許清單指定您希望 Macie 在檢查 S3 物件中是否有敏感資料時忽略的文字或文字模式。

您可以在 Macie 中建立兩種類型的允許清單：列出特定字詞和其他類型要忽略的字元序列的純文字檔案，或是定義要忽略的文字模式的規則運算式 (regex)。如果物件包含的文字符合允許清單中的項目或模式，Macie 不會在敏感資料發現項目、統計資料和其他類型的結果中報告文字，即使該文字符合受管理資料識別碼或自訂資料識別碼的準則。

如需詳細資訊，請參閱 使用允許清單定義敏感資料例外。

自動化敏感資料探索

Macie 持續執行的一系列自動化分析活動，以識別和選取 S3 儲存貯體中的代表物件，並檢查選取的物件是否存在敏感資料。

隨著分析的進展，Macie 會產生它找到的敏感數據（敏感數據發現）和它執行的分析（敏感數據發現結果）的記錄。Macie 也會更新提供有關 Amazon S3 資料的統計資料和其他資訊。

如需詳細資訊，請參閱 執行自動化敏感資料探索。

AWS 安全性搜尋結果格式 (ASFF)

發佈至或產生之發現項目內容的標準化 JSON 格式 AWS Security Hub。ASFF 包含有關安全問題來源、受影響的資源，以及發現項目狀態的詳細資訊。

若要取得有關 ASFF 的資訊，請參閱《AWS Security Hub 使用指南》中的「AWS 安全性尋找格式 (ASFF)」。如需將 Macie 發現項目發佈至 Security Hub 的相關資訊，請參閱Amazon Macie 與集成 AWS Security Hub。

可分類的位元組或大小

在 Macie 提供的 S3 儲存貯體統計資料中，S3 儲存貯體中所有可分類物件的總儲存大小。

如果值區已啟用版本控制，則此值會根據值區中每個可分類物件的最新版本儲存大小為基礎。如果物件是壓縮檔案，這個值不會反映檔案解壓縮後檔案內容的實際大小。

如需詳細資訊，請參閱 檢閱您的 S3 儲存貯體庫存 及 評估您的 Amazon S3 安全狀態。

可分類的物件

Macie 可以分析以偵測敏感資料的 S3 物件。

計算 S3 儲存貯體統計資料時，Macie 會根據物件的儲存類別和副檔名判斷物件是否可分類。如果物件使用受支援的 Amazon S3 儲存類別，且具有支援檔案或儲存格式的副檔名，則可分類該物件。

如需詳細資訊，請參閱 檢閱您的 S3 儲存貯體庫存 及 評估您的 Amazon S3 安全狀態。

針對敏感資料探索，Macie 會根據物件的儲存類別、副檔名和內容，判斷物件是否可分類。如果物件使用支援的 Amazon S3 儲存類別，其副檔名為支援的檔案或儲存格式，則可進行分類，而 Macie 驗證可從物件擷取和分析資料。

如需詳細資訊，請參閱 探索敏感資料 及 預測和監控成本。

自訂資料識別碼

您定義用來偵測機密資料的一組準則。

此條件包含規則運算式 (Regex)，此表達式定義要比對的文字模式，以及可選擇的字元序列和精簡結果之鄰近性規則。字元序列可以是：

- 關鍵字，其為單詞或片語，必須位於符合 Regex 的文本附近，或者
- 忽略單詞，其為要從結果中排除的單詞或片語。

除了偵測準則之外，您還可以為自訂資料識別碼所產生的敏感資料發現項目定義自訂嚴重性設定。

如需詳細資訊，請參閱 建置自訂資料識別符。

篩選規則

您建立並儲存的一組屬性篩選條件，以便在 Amazon Macie 主控台上分析發現項目。篩選規則可協助您對具有特定特性的發現項目執行一致的分析，例如報告特定類型敏感資料的所有高嚴重性發現項目。

如需詳細資訊，請參閱 建立及管理發現項目的篩選規則。

問題清單

Macie 在 S3 物件中發現的敏感資料的詳細報告，或 S3 一般用途儲存貯體的安全性或隱私權潛在問題。每個發現項目都會提供詳細資訊，例如嚴重性等級、受影響資源的相關資訊，以及 Macie 何時找到資料或問題。

Macie 會產生兩類發現項目：針對 Macie 在 S3 物件中偵測到的敏感資料發現的敏感資料，以及針對 Macie 透過 S3 儲存貯體的安全性和存取控制設定偵測到的潛在問題的政策發現項目。在每個類別中，都有特定類型的發現項目。

如需詳細資訊，請參閱 Amazon Macie 發現的類型。

尋找事件

一種 Amazon EventBridge 事件，其中包含敏感資料發現或政策發現的詳細資訊。

Macie 會自動將敏感資料發現和政策發現 EventBridge作為事件發佈到 Amazon。事件是符合事件結構 EventBridge 描述的 JSON 物件。 AWS 您可以使用這些事件，藉由使用其他應用程式、服務和系統來監視、處理和處理發現項目。

如需詳細資訊，請參閱 Amazon Macie 與亞馬遜集成 EventBridge 及 Amazon Macie 發現的亞馬遜 EventBridge 事件模式。

job

查看敏感性資料探索工作。

受管資料識別碼

一組內置準則和技術，旨在檢測特定類型的敏感數據。敏感資料的範例包括特定國家或地區的信用卡號碼、 AWS 秘密存取金鑰或護照號碼。這些識別碼可以偵測許多國家和地區不斷增加的敏感資料類型清單。

如需詳細資訊，請參閱 使用受管資料識別符。

成員帳戶

由組織的指定 Macie 管理員帳戶管理的 Macie 帳戶。組織是一組 Macie 帳戶，它們彼此相關聯，並以特定 AWS 區域帳戶群組的形式集中管理。

一個帳戶可以通過兩種方式成為會員帳戶：通過將 Macie 與帳戶的組織集成在一起， AWS Organizations 或者通過接受 Macie 會員邀請來成為會員帳戶。

如果您有會員帳戶，您的 Macie 管理員可以存取您帳戶的 Amazon S3 庫存資料、政策發現項目，以及特定 Macie 設定和資源。您的管理員也可以執行自動化敏感資料探索，並執行敏感資料探索任務，以

偵測 S3 儲存貯體中的敏感資料。他們還可以為您的帳戶執行其他任務，具體取決於您的帳戶成為會員帳戶的方式。

如需詳細資訊，請參閱 管理多個 帳戶。

組織

一組 Macie 帳戶，這些帳戶彼此關聯並集中管理為特定 AWS 區域帳戶中的一組相關帳戶。

每個組織都包含一個指定的 Macie 管理員帳戶和一個或多個關聯的成員帳戶。管理員帳戶可以訪問某些 Macie 設置，數據和成員帳戶的資源。您可以通過兩種方式創建組織：通過將 Macie 與集成 AWS Organizations 或通過在 Macie 中發送和接受會員邀請來創建組織。

如需詳細資訊，請參閱 管理多個 帳戶。

政策發現

S3 一般用途儲存貯體之安全性和存取控制設定的潛在政策違規或問題的詳細報告。詳細資訊包括嚴重性等級、受影響資源的相關資訊，以及 Macie 發現問題的時間。

當 S3 一般用途儲存貯體的政策或設定以降低儲存貯體和儲存貯體物件的安全性或隱私權的方式變更時，Macie 會產生政策發現項目。Macie 會產生這些發現項目，做為 Amazon S3 資料持續監控活動的一部分。Macie 可以產生數種類型的原則發現項目。

如需詳細資訊，請參閱 Amazon Macie 發現的類型 及 監控數據安全性和隱私。

樣本發現

使用範例資料和預留位置值來示範發現項目可能包含的資訊種類的發現項目。

如需詳細資訊，請參閱 使用範例發現項目。

敏感資料尋找

Macie 在 S3 物件中找到的敏感資料的詳細報告。詳細資料包括嚴重性等級、受影響資源的相關資訊、Macie 找到的敏感資料的類型和出現次數，以及 Macie 何時找到敏感資料。

如果 Macie 偵測到 S3 物件中的敏感資料，當您執行敏感資料探索任務或執行自動化敏感資料探索時，Macie 會產生敏感資料發現項目。Macie 可以生成幾種類型的敏感數據發現。

如需詳細資訊，請參閱 Amazon Macie 發現的類型 及 探索敏感資料。

敏感資料探索工作

也稱為工作，Macie 執行的一系列自動化處理和分析任務，以偵測和報告 S3 物件中的敏感資料。建立工作時，您可以指定要執行工作的頻率，並定義工作分析的範圍和性質。

當工作執行時，Macie 會產生找到的敏感資料 (敏感資料發現項目) 及其執行的分析 (敏感資料探索結果) 的記錄。Macie 還將日誌記錄數據發佈到 Amazon CloudWatch 日誌。

如需詳細資訊，請參閱 執行敏感資料探索任務。

敏感資料探索結果

記錄 Macie 在 S3 物件上執行的分析詳細資料的記錄，以判斷物件是否包含敏感資料。Macie 會產生這些記錄並將其寫入 JSON 行 (.jsonl) 檔案，這些檔案會加密並儲存在您指定的 S3 儲存貯體中。這些記錄遵循標準化的結構描述。

當您執行敏感資料探索工作或 Macie 執行自動化敏感資料探索時，Macie 會為包含在分析範圍內的每個物件建立敏感資料探索結果。其中包含：

- Macie 在中尋找敏感資料的物件，因此也會產生敏感資料發現項目。
- Macie 在中找不到敏感數據的對象，因此不會產生敏感數據發現。
- Macie 因權限設定或使用不支援的檔案或儲存格式等錯誤或問題而無法分析的物件。

如需詳細資訊，請參閱 儲存及保留敏感資料探索結果。

獨立帳戶

組織中既不是系統管理員也不是成員帳戶的 Macie 帳戶。該帳戶不是組織的一部分。

抑制尋找

由抑制規則自動封存的發現項目。也就是說，Macie 會自動將尋找項目的狀態變更為封存，因為當 Macie 產生搜尋結果時，發現項目符合抑制規則的準則。

如需詳細資訊，請參閱 隱藏問題清單。

抑制規則

您建立並儲存以自動封存 (隱藏) 發現項目的一組以屬性為基礎的篩選條件。抑制規則在您已檢閱過一類發現項目且不想再次收到通知的情況下很有幫助。

如果您使用抑制規則隱藏發現項目，Macie 會繼續產生符合規則條件的發現項目。但是，Macie 會自動將發現項目的狀態變更為已封存。這意味著發現結果默認情況下不會出現在 Amazon Macie 控制台上，並且 Macie 不會將它們發佈到其他。 AWS 服務

如需詳細資訊，請參閱 隱藏問題清單。

未分類的位元組或大小

在 Macie 提供的 S3 儲存貯體統計資料中，S3 儲存貯體中所有未分類物件的總儲存大小。

如果值區已啟用版本控制，則此值會根據值區中每個未分類物件的最新版本儲存大小為基礎。如果物件是壓縮檔案，這個值不會反映檔案解壓縮後檔案內容的實際大小。

如需詳細資訊，請參閱 檢閱您的 S3 儲存貯體庫存 及 評估您的 Amazon S3 安全狀態。

未分類的物件

Macie 無法分析以偵測敏感資料的 S3 物件。

計算 S3 儲存貯體統計資料時，Macie 會根據物件的儲存類別和副檔名，判斷物件是否未分類。如果物件未使用支援的 Amazon S3 儲存類別，或者沒有支援的檔案或儲存格式的副檔名，則該物件將無法分類。

如需詳細資訊，請參閱 檢閱您的 S3 儲存貯體庫存 及 評估您的 Amazon S3 安全狀態。

針對敏感資料探索，Macie 會根據物件的儲存類別、副檔名和內容，判斷物件是否可以取消分類。如果物件不使用支援的 Amazon S3 儲存類別、沒有支援的檔案或儲存格式的副檔名，或 Macie 無法從物件擷取和分析資料，則物件無法分類。例如，物件是格式錯誤的檔案。

如需更多詳細資訊，請參閱 探索敏感資料 及 預測和監控成本。

使用 Amazon Macie 監控數據安全和隱私

當您為您啟用 Amazon Macie 時 AWS 帳戶，Macie 會自動產生並開始維護目前 Amazon Simple Storage Service (Amazon S3) 一般用途儲存貯體的完整庫存。 AWS 區域 Macie 還開始評估和監視存儲桶的安全性和訪問控制。如果 Macie 偵測到會降低儲存貯體安全性或隱私權的事件，Macie 會建立一個政策發現項目，供您視需要檢閱和修正。

若要評估和監控 S3 儲存貯體是否存在敏感資料，您可以建立和執行敏感資料探索任務。敏感資料探索任務可以每天、每週或每月對值區物件執行累加分析。如果 Macie 偵測到 S3 物件中的敏感資料，Macie 會建立一個敏感資料尋找項目，通知您找到的敏感資料。根據您的帳戶設定，您也可以將 Macie 設定為執行自動化的敏感資料探索。自動化敏感資料探索使用取樣技術持續識別、選取和分析值區中的代表性物件。如需這兩個選項的更多資訊，請參閱探索敏感資料。

Macie 也能持續掌握 Amazon S3 資料的安全性和隱私權。若要評估資料的安全狀態並決定採取行動的位置，您可以使用主控台上的「摘要」儀表板。儀表板提供 Amazon S3 資料彙總統計資料的快照。統計資料包括關鍵安全指標的資料，例如可公開存取或與其他人共用的一般用途值區數目 AWS 帳戶。儀表板也會顯示您帳戶的彙總發現項目資料群組，例如，前 7 天發現項目最多的 1-5 個值區的名稱。您可以向下鑽研每個統計資料，以檢閱其支援資料。若要以程式設計方式查詢統計資料，請使用 Amazon Macie API 的GetBucketStatistics作業。

為了進行更深入的分析和評估，Macie 會針對庫存中的個別 S3 儲存貯體提供詳細資訊和統計資料。這包括每個值區的公開存取和加密設定的細分，以及 Macie 可以分析以偵測值區中敏感資料的物件大小和數量。詳細目錄也會指出您是否設定敏感資料探索工作或自動化敏感資料探索，以分析值區中的物件。如果有，它會指出最近發生該分析的時間。您可以使用 Amazon Macie 主控台或亞馬 Amazon Macie API 的DescribeBuckets操作來瀏覽、排序和篩選庫存。

如果您是組織的 Macie 管理員，則可以存取成員帳戶所擁有之 S3 儲存貯體的統計資料和其他資料。您也可以存取 Macie 為值區產生的原則發現項目，並檢查值區中是否有機密資料。這表示您可以使用 Macie 評估和監控組織 Amazon S3 資料資產的整體安全狀態。如需更多詳細資訊，請參閱 管理多個帳戶。

主題

- Amazon Macie 如何監控 Amazon S3 數據安全
- 使用亞馬遜 Macie 評估您的 Amazon S3 安全狀態
- 使用亞馬遜 Macie 分析您的 Amazon S3 安全狀態
- 允許 Amazon Macie 訪問 S3 存儲桶和對象

Amazon Macie 如何監控 Amazon S3 數據安全

當您為您的帳戶啟用 Amazon Macie 時 AWS 帳戶，Macie 會在當前帳戶中為您的帳戶創建一個 AWS Identity and Access Management （ IAM ）服務鏈接角色。 AWS 區域此角色的權限原則允許 Macie 代表您呼叫其他 AWS 資源 AWS 服務 並監視資源。透過使用此角色，Macie 會產生並維護該區域中 Amazon Simple Storage Service (Amazon S3) 一般用途儲存貯體的完整庫存。Macie 還監視和評估存儲桶的安全性和訪問控制。

如果您是組織的 Macie 管理員，則庫存會包含您帳戶和組織中成員帳戶之 S3 儲存貯體的統計資料和其他相關資料。有了這些資料，您可以使用 Macie 監控和評估組織在 Amazon S3 資料資產中的安全狀態。如需詳細資訊，請參閱 管理多個 帳戶。

主題

關鍵元件

Amazon Macie 結合使用功能和技術來提供和維護 S3 一般用途儲存貯體的庫存資料，並監控和評估儲存貯體的安全性和存取控制。

收集中繼資料並計算統計

為了產生和維護儲存貯體庫存的中繼資料和統計資料，Macie 會直接從 Amazon S3 擷取儲存貯體和物件中繼資料。對於每個值區，中繼資料包括：

- 值區的一般資訊，例如儲存貯體的名稱、Amazon 資源名稱 (ARN)、建立日期、加密設定、標籤，以及擁有 AWS 帳戶 該值區的帳戶 ID。
- 套用至值區的帳戶層級權限設定，例如帳戶的封鎖公開存取設定。
- 值區的值區層級權限設定，例如值區的封鎖公用存取設定，以及衍生自值區政策或存取控制清單 (ACL) 的設定。
- 值區的共用存取權和複寫設定，包括儲存貯體資料是否已複製到組織中，或與其共 AWS 帳戶 用非屬於您組織的儲存貯體資料。
- 值區中物件的物件計數和設定，例如值區中的物件數目，以及依加密類型、檔案類型和儲存區類別劃分物件計數的劃分。

Macie 直接向您提供此信息。Macie 也會使用這些資訊來計算統計資料，並針對您的存貨中儲存貯體庫存的整體和個別值區的安全性和隱私性提供評估。例如，您可以找到詳細目錄中值區的總儲存大小和數量、這些值區中的總儲存大小和物件數量，以及 Macie 可分析以偵測值區中機密資料的總儲存大小和物件數量。

依預設，中繼資料和統計資料包括由於不完整的分段上傳而存在的任何物件零件的資料。如果您手動重新整理特定值區的物件中繼資料，Macie 會整體重新計算值區和值區詳細目錄的統計資料，並從重新計算的值中排除物件零件的資料。Macie 下次從 Amazon S3 擷取儲存貯體和物件中繼資料做為每日重新整理週期的一部分時，Macie 會更新您的庫存資料，並再次納入物件零件的資料。如需 Macie 何時擷取值區和物件中繼資料的詳細資訊，請參閱數據刷新。

重要的是要注意，Macie 無法分析對象部分來檢測敏感數據。Amazon S3 必須先將零件組裝成一個或多個物件，以便 Macie 進行分析。如需有關分段上傳和物件零件的資訊，包括如何使用生命週期規則自動刪除零件，請參閱 Amazon Simple Storage Service 使用者指南中的使用多部分上傳來上傳和複製物件。若要識別包含物件組件的儲存貯體，您可以參考 Amazon S3 儲存鏡頭中不完整的分段上傳指標。如需詳細資訊，請參閱 Amazon 簡單儲存服務使用者指南中的評估儲存活動和使用情況。

監控存儲桶安全性和隱私

為協助確保庫存中儲存貯體層級資料的準確性，Macie 會監控並分析 Amazon S3 資料可能發生的某些AWS CloudTrail事件。如果發生相關事件，Macie 會更新適當的庫存資料。

例如，如果您為值區啟用封鎖公開存取設定，Macie 會更新值區公開存取設定的所有相關資料。同樣地，如果您新增或更新值區的儲存貯體政策，Macie 會分析該政策並更新庫存中的相關資料。

Macie 會監控並分析下列 CloudTrail 事件的資料：

- 帳戶層級事件 — 以及 DeletePublicAccessBlock PutPublicAccessBlock
- 值區層級事件 —CreateBucket,, DeleteAccountPublicAccessBlock, DeleteBucket,,DeleteBucketEncryption, DeleteBucketPolicy, DeleteBucketPublicAccessBlock,DeleteBucketReplication,, DeleteBucketTagging, PutAccountPublicAccessBlock,PutBucketAcl, PutBucketEncryption,, PutBucketPolicyPutBucketPublicAccessBlock, PutBucketReplication 和 PutBucketTagging PutBucketVersioning

您無法啟用監視其他 CloudTrail 事件，也無法停用任何先前事件的監視。如需前述事件對應作業的詳細資訊，請參閱 Amazon 簡單儲存服務 API 參考。

> **Tip**
>
> 若要監控物件層級事件，建議您使用 Amazon 的 Amazon S3 保護功能。 GuardDuty此功能可監控物件層級 Amazon S3 資料事件，並分析這些事件是否有惡意和可疑活動。有關更多信息，請參閱 Amazon GuardDuty 用戶指南 GuardDuty中的 Amazon S3 保護。

評估值區安全性和存取控制

為了評估值區層級的安全性和存取控制，Macie 會使用自動化的邏輯型推理來分析套用至值區的資源型政策。Macie 也會分析套用至值區的帳戶和值區層級權限設定。此分析會考量值區政策、值區層級 ACL，以及帳戶和值區的封鎖公用存取設定。

對於資源為基礎的政策，馬西使用櫸樹。Zelkova 是一種自動推理引擎，可將 AWS Identity and Access Management （ IAM ）策略轉換為邏輯語句，並針對決策問題運行一套通用和專門的邏輯求解器（可滿足性模塊理論）。Macie 將 Zelkova 重複套用到具有日益特定查詢的策略，以表徵該策略允許的行為類別。要了解有關 Zelkova 使用求解器的性質的更多信息，請參閱滿足性模塊理論。

> **Important**
>
> 若要針對儲存貯體執行上述工作，儲存貯體必須是 S3 一般用途儲存貯體。Macie 不會監控或分析 S3 目錄儲存貯體。
> 此外，必須允許 Macie 存取儲存貯體。如果值區的權限設定阻止 Macie 擷取值區或值區物件的中繼資料，Macie 只能提供值區的一部分資訊，例如值區的名稱和建立日期。Macie 無法為存儲桶執行任何其他任務。如需詳細資訊，請參閱 允許 Macie 存取 S3 儲存貯體和物件。

數據刷新

當您為您啟用 Amazon Macie 時 AWS 帳戶，Macie 會直接從 Amazon S3 擷取 S3 一般用途儲存貯體和物件的中繼資料。之後，Macie 會每天自動從 Amazon S3 擷取儲存貯體和物件中繼資料，作為每日重新整理週期的一部分。

當發生以下任何情況時，Macie 也會直接從 Amazon S3 擷取儲存貯體中繼資料：

- 您可以在 Amazon Macie 主控台上選擇重新整理庫存資料（  ）。
  您可以每五分鐘重新整理一次資料的頻率。

- 您以程式設計方式將DescribeBuckets請求提交至 Amazon Macie API，但在前五分鐘內尚未提交DescribeBuckets請求。
- 馬西檢測到相關 AWS CloudTrail 事件。

如果您選擇手動重新整理特定值區的最新物件中繼資料，Macie 也可以擷取該值區的最新物件中繼資料。如果您最近建立了值區，或在過去 24 小時內對值區的物件進行了重大變更，這會很有幫助。若要手動重新整理儲存貯體的物件中繼資料，請在主控台 S3 儲存貯體頁面上的「儲存貯體詳細資料」面板的「物件統計資料」區段中選擇 refresh ()。此功能適用於儲存 30,000 個或更少物件的值區。

每次 Macie 擷取值區或物件中繼資料時，Macie 都會自動更新您詳細目錄中的所有相關資料。如果 Macie 偵測到會影響儲存貯體安全性或隱私權的差異，Macie 會立即開始評估和分析變更。分析完成後，Macie 會更新庫存中的相關資料。如果任何差異會降低儲存貯體的安全性或隱私權，Macie 也會建立適當的政策調查結果，供您視需要檢閱和修正。

若要判斷 Macie 最近擷取帳戶的值區或物件中繼資料的時間，您可以參考主控台上的 [上次更新] 欄位。此欄位會出現在摘要儀表板、S3 儲存貯體頁面上，以及 S3 儲存貯體頁面上的儲存貯體詳細資料面板中。(如果您使用 Amazon Macie API 查詢庫存資料，則`lastUpdated`欄位會提供此資訊。) 如果您是組織的 Macie 管理員，「上次更新」欄位會指出 Macie 擷取組織中帳戶資料的最早日期和時間。

在特定情況下，在極少數情況下，延遲和其他問題可能會導致 Macie 無法擷取值區和物件中繼資料。它們也可能會延遲 Macie 收到有關儲存貯體清單變更的通知，或是個別值區的權限設定和政策。例如， CloudTrail 事件的傳遞問題可能會導致延遲。如果發生這種情況，Macie 會在下次執行 24 小時內的每日重新整理時分析新的和更新的資料。

其他考量

當您使用 Amazon Macie 監控和評估 Amazon S3 資料的安全狀態時，請牢記以下事項：

- 庫存資料僅適用於目前中的 S3 一般用途儲存貯體 AWS 區域。若要存取其他區域的資料，請在每個額外的區域中啟用並使用 Macie。
- 如果您是組織的 Macie 管理員，只有在目前區域中為該帳戶啟用 Macie 時，才能存取該成員帳戶的庫存資料。
- 如果值區的權限設定阻止 Macie 擷取值區或值區物件的相關資訊，Macie 就無法評估和監控值區資料的安全性和隱私權，也無法提供值區的詳細資訊。

  為了幫助您識別出現這種情況的存儲桶，Macie 執行以下操作：

- 在值區清單中，Macie 會顯示值區的警告圖示
  (⚠)。
  對於值區的詳細資訊，Macie 只會顯示欄位和資料的子集：擁有 AWS 帳戶 該值區的帳戶 ID、值區名稱、Amazon 資源名稱 (ARN)、建立日期和區域；以及 Macie 最近擷取值區的值區和物件中繼資料作為每日重新整理週期的一部分的日期和時間。如果您使用 Amazon Macie API 查詢庫存資料，Macie 會提供值區的錯誤代碼和訊息，且儲存貯體大部分屬性的值為空值。
- 在「摘要」儀表板上，值區的值為「公開存取」、「加密」和「共用」統計資料的值為「未知」。(如果您使用 Amazon Macie API 查詢統計資料，則值區的值unknown為這些統計資料。) 此外，Macie 會在計算「儲存體」和「物件」統計資料的資料時排除值區。

  若要調查問題，請檢閱 Amazon S3 中儲存貯體的政策和許可設定。例如，值區可能具有限制性的值區政策。如需詳細資訊，請參閱 允許 Macie 存取 S3 儲存貯體和物件。

- 有關存取和權限的資料僅限於帳戶和儲存貯體層級的設定。它不會反映決定存取值區中特定物件的物件層級設定。例如，如果值區中的特定物件啟用了公開存取權，Macie 就不會報告該值區或值區的物件是可公開存取的。

  若要監控物件層級操作並識別潛在的安全風險，建議您使用 Amazon 的 Amazon S3 保護功能。GuardDuty此功能可監控物件層級 Amazon S3 資料事件，並分析這些事件是否有惡意和可疑活動。有關更多信息，請參閱 Amazon GuardDuty 用戶指南 GuardDuty中的 Amazon S3 保護。

- 如果您手動重新整理特定值區的物件中繼資料，Macie 會暫時回報未知的加密統計資料套用至物件。下次 Macie 執行每日資料重新整理時 (24 小時內)，Macie 會重新評估物件的加密中繼資料，並再次回報統計資料的量化資料。
- 如果您手動重新整理特定值區的物件中繼資料，Macie 會暫時排除值區所包含之任何物件零件的資料，這是因為分段上傳不完整。下次 Macie 執行每日資料重新整理時 (24 小時內)，Macie 會重新計算值區物件的計數和儲存大小值，並在這些計算中包含零件的資料。
- 在極少數情況下，Macie 可能無法判斷值區是否可公開存取或共用，或需要伺服器端加密新物件。例如，暫時性問題可能會導致 Macie 無法擷取和分析必要的資料。或者，Macie 可能無法完全判斷一或多個原則陳述式是否授與外部實體的存取權。在這些情況下，Macie 會針對庫存中的相關統計資料和欄位報告「未知」。若要調查這些案例，請檢閱 Amazon S3 中儲存貯體的政策和許可設定。

另請注意，只有在您為帳戶啟用 Macie 之後，儲存貯體的安全性或隱私權降低時，Macie 才會產生政策發現項目。例如，如果您在啟用 Macie 之後停用儲存貯體的封鎖公用存取設定，Macie 會產生原則：儲存貯體的 IAMUS BlockPublicAccessDisabled ER/S3 尋找。但是，如果在啟用 Macie 時停用儲存貯體的封鎖公用存取設定，而且繼續停用這些設定，Macie 就不會產生原則：儲存貯體的 IAMUser BlockPublicAccessDisabled /S3 尋找。

此外，當 Macie 評估值區的安全性和隱私權時，它不會檢查存取記錄，也不會分析帳戶的使用者、角色和其他相關設定。相反，Macie 會分析並報告指出潛在安全風險的關鍵設定的資料。例如，如果政策發現指出存儲桶可以公開訪問，則不一定表示外部實體訪問該值區。同樣地，如果發現原則指出儲存貯體已與組織 AWS 帳戶 外部人員共用，Macie 就不會嘗試判斷此存取權是否有意且安全。相反地，這些發現指出外部實體可能存取值區的資料，這可能是意外的安全性風險。

使用亞馬遜 Macie 評估您的 Amazon S3 安全狀態

若要評估 Amazon Simple Storage Service (Amazon S3) 資料的整體安全狀態，並確定採取行動的位置，您可以使用 Amazon Macie 主控台上的摘要儀表板。

摘要儀表板提供目前 Amazon S3 資料彙總統計資料的快照 AWS 區域。統計資料包括關鍵安全指標的資料，例如可公開存取或與其他人共用的一般用途值區數目 AWS 帳戶。儀表板也會顯示您帳戶的彙總發現項目資料群組，例如過去 7 天內發現次數最多的發現項目類型。如果您是組織的 Macie 管理員，則儀表板會提供組織中所有帳戶的彙總統計資料和資料。您可以選擇按帳戶過濾數據。

若要執行更深入的分析，您可以向下鑽研並檢閱儀表板上個別項目的支援資料。您也可以使用 Amazon Macie 主控台檢閱和分析 S3 儲存貯體庫存，或使用 Amazon Macie API 的DescribeBuckets操作以程式設計方式查詢和分析庫存資料。

主題

- 顯示「摘要」儀表板
- 瞭解「摘要」控制面板的元件
- 了解摘要儀表板上的資料安全統計資料

顯示「摘要」儀表板

在 Amazon Macie 主控台上，摘要儀表板提供目前 Amazon S3 資料彙總統計資料和發現項目 AWS 區域資料的快照。如果您偏好以程式設計方式查詢統計資料，可以使用 Amazon Macie API 的GetBucketStatistics操作。

顯示「摘要」控制面板

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 在導覽窗格中，選擇摘要。Macie 會顯示「摘要」控制面板。
3. 若要判斷 Macie 最近何時從 Amazon S3 擷取您帳戶的儲存貯體或物件中繼資料，請參閱儀表板頂端的「上次更新」欄位。如需詳細資訊，請參閱 數據刷新。

4. 若要向下鑽研並複查儀表板上項目的支援資料，請選擇該項目。

如果您是組織的 Macie 管理員，儀表板會顯示組織中帳戶和成員帳戶的彙總統計資料和資料。若要篩選儀表板並僅顯示特定帳戶的資料，請在儀表板上方的 [帳戶] 方塊中輸入帳戶的 ID。

瞭解「摘要」控制面板的元件

在「摘要」儀表板上，統計資料和資料分為數個區段。在儀表板頂端，您會找到彙總統計資料，這些統計資料會指出 Amazon S3 中存放的資料量，以及 Amazon Macie 可以分析多少資料以偵測敏感資料。您也可以參閱「上次更新」欄位，以確定 Macie 最近何時從 Amazon S3 擷取帳戶的儲存貯體或物件中繼資料。其他部分提供統計資料和最近的發現資料，可協助您評估目前 Amazon S3 資料的安全性、隱私權和敏感度 AWS 區域。

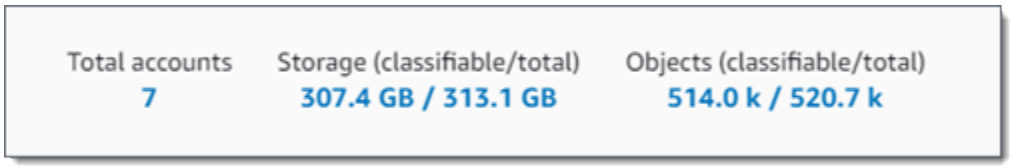
統計資料和資料分為下列各節：

儲存和敏感資料探索 | 自動化探索和涵蓋範圍問題 | 資料安全 | 排名前 S3 儲存貯體 | 最熱門的尋找類型 | 政策發現

複查每個區段時，選擇性地選擇要向下追溯並複查支援資料的料號。另請注意，儀表板不包含 S3 目錄儲存貯體的資料，僅包含一般用途儲存貯體的資料。Macie 不會監視或分析目錄值區。

儲存和敏感資料探索

儀表板頂端的統計資料會指出您在 Amazon S3 中存放的資料量，以及 Macie 可以分析多少資料以偵測敏感資料。例如：



在本節中：

- 帳戶總數 — 如果您是組織的 Macie 管理員，或者您擁有獨立的 Macie 帳戶，則會顯示此欄位。它會指出您值區庫存中 AWS 帳戶 該時段的總數。如果您是 Macie 管理員，這是您為組織管理的 Macie 帳戶總數。如果您有獨立的 Macie 帳戶，則此值為 1。

  S3 儲存貯體總數 — 如果您的 Macie 帳戶是組織的成員，則會顯示此欄位。它會指出詳細目錄中一般用途值區的總數，包括不儲存任何物件的值區。
- 儲存空間 — 這些指標提供值區詳細目錄中物件儲存大小的相關資訊：

- 可分類 — Macie 可以在值區中分析的所有物件的總儲存大小。
- 總計 — 值區中所有物件的總儲存空間大小，包括 Macie 無法分析的物件。

如果有任何物件是壓縮檔案，這些值在解壓縮後不會反映這些檔案的實際大小。如果已啟用任何值區的版本控制，則這些值會以這些值區中每個物件最新版本的儲存大小為基礎。

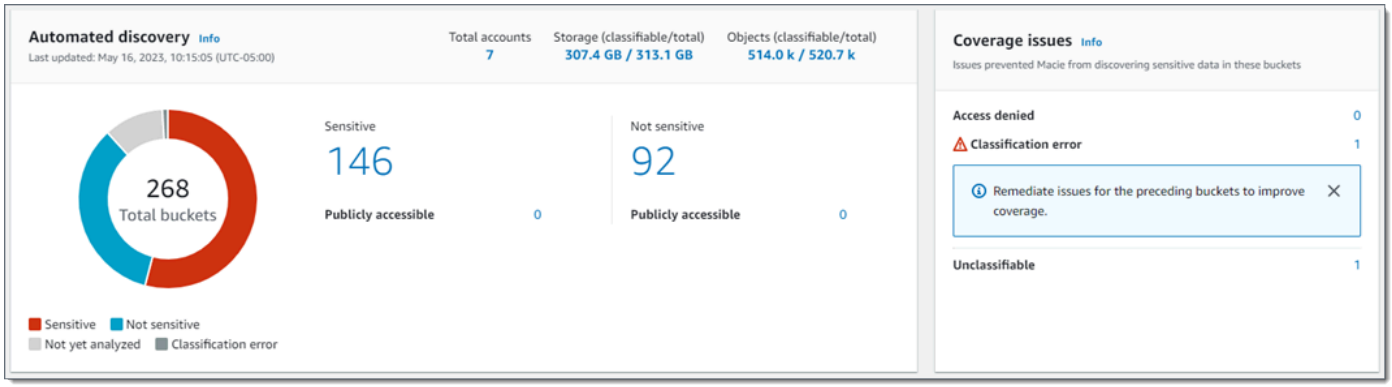
- 物件 — 這些指標提供值區詳細目錄中物件數目的相關資訊：
  - 可分類 — Macie 可以在值區中分析的物件總數。
  - 「總計」— 值區中的物件總數，包括 Macie 無法分析的物件。

在上述統計資料中，如果資料和物件使用支援的 Amazon S3 儲存類別，且具有支援的檔案或儲存格式的副檔名，則資料和物件可分類。您可以通過使用 Macie 檢測對象中的敏感數據。如需詳細資訊，請參閱 支援的儲存類別和格式。

請注意，「儲存體」和「物件」統計資料不會包含 Macie 不允許存取之值區中物件的相關資料。例如，值區中具有限制性值區政策的物件。若要識別發生這種情況的儲存貯體，您可以使用 S3 儲存貯體表格來檢閱儲存貯體庫存。如果值區名稱旁邊出現警告圖示 (⚠)，表示不允許 Macie 存取值區。

自動化探索與涵蓋問題

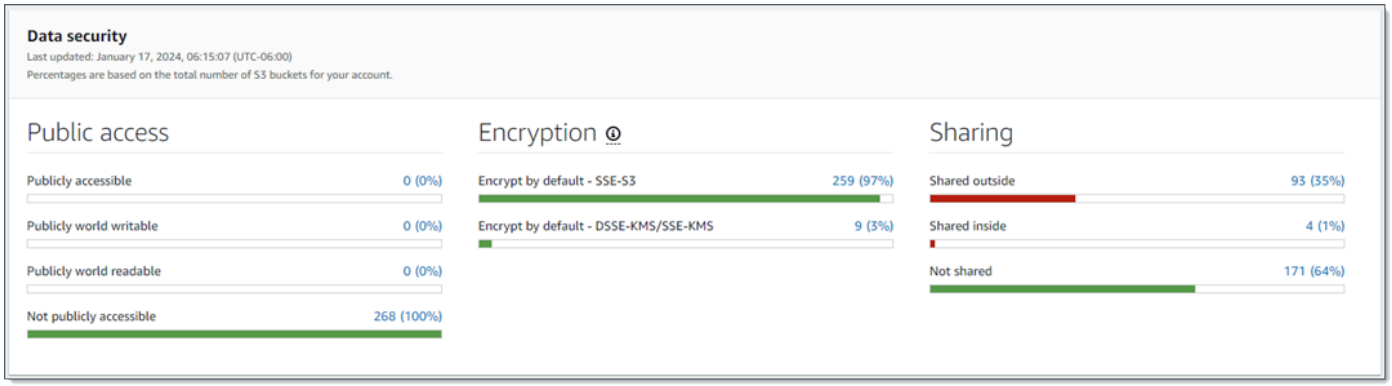
如果啟用了自動化敏感資料探索，這些區段會顯示在儀表板上。這些區段中的統計資料會擷取 Macie 迄今為止針對 Amazon S3 資料執行的自動化敏感資料探索活動的狀態和結果。例如：



如需這些統計值的詳細資訊，請參閱在摘要儀表板上檢閱彙總的資料敏感度統計。

資料安全

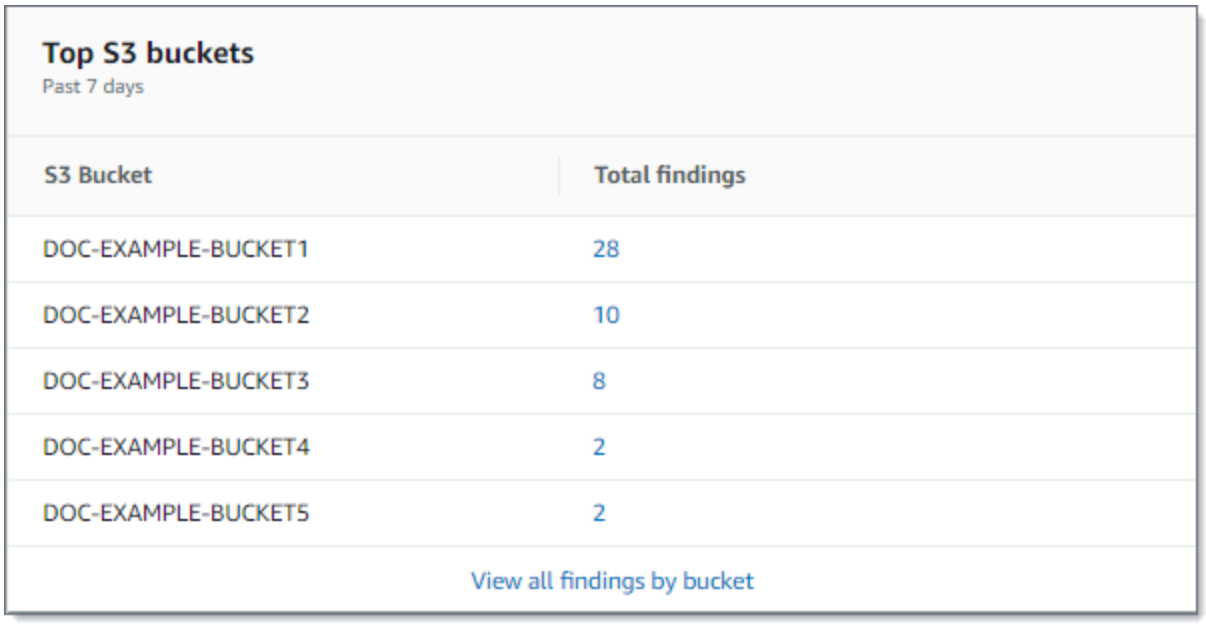
本節提供指出 Amazon S3 資料潛在安全和隱私權風險的統計資料。例如：



如需這些統計值的詳細資訊，請參閱了解摘要儀表板上的資料安全統計資料。

前 S3 儲存貯體

本節列出在過去七天內產生任何類型最多發現項目的 S3 儲存貯體 (最多五個儲存貯體)。它也會指出 Macie 為每個值區建立的發現項目數目。例如：

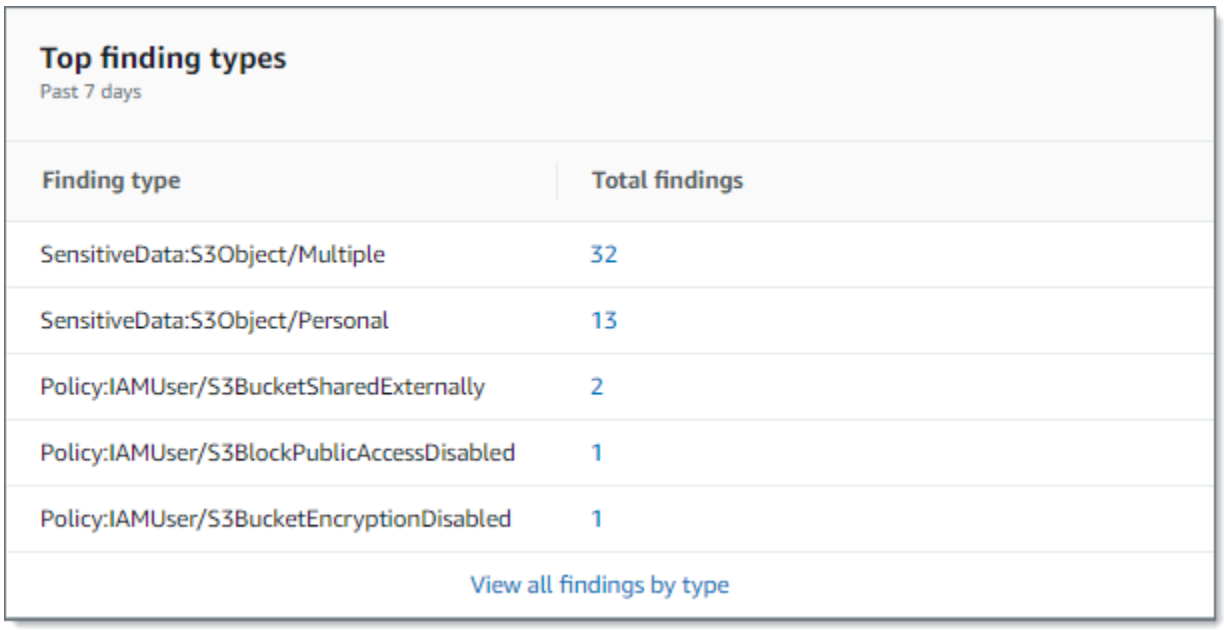


若要顯示並選擇性地向下追溯過去 7 天內某時段的所有搜尋結果，請在「搜尋結果總計」欄位中選擇值。若要顯示所有時段的目前搜尋結果 (依時段分組)，請選擇「依時段檢視所有搜尋結果」。

如果 Macie 在過去七天內未建立任何發現項目，則此區段為空白。或者，在前七天內建立的所有發現項目都會受到抑制規則所抑制。

尋找項目類型

本節列出過去 7 天內發現次數最多的發現項目類型 (最多五種發現項目類型)。它還表示 Macie 為每個類型創建的發現項目的數量。例如：



若要顯示並選擇性地向下追溯過去 7 天內特定型態的所有發現項目，請在「發現項目總計」欄位中選擇值。若要顯示所有目前發現項目 (依搜尋結果型態分組)，請選擇依型態檢視所有發現項

如果 Macie 在過去七天內未建立任何發現項目，則此區段為空白。或者，在前七天內建立的所有發現項目都會受到抑制規則所抑制。

政策結果

本節列出 Macie 最近建立或更新的原則發現項目，最多十個發現項目。例如：

若要顯示特定發現項目的明細，請選擇搜尋結果。

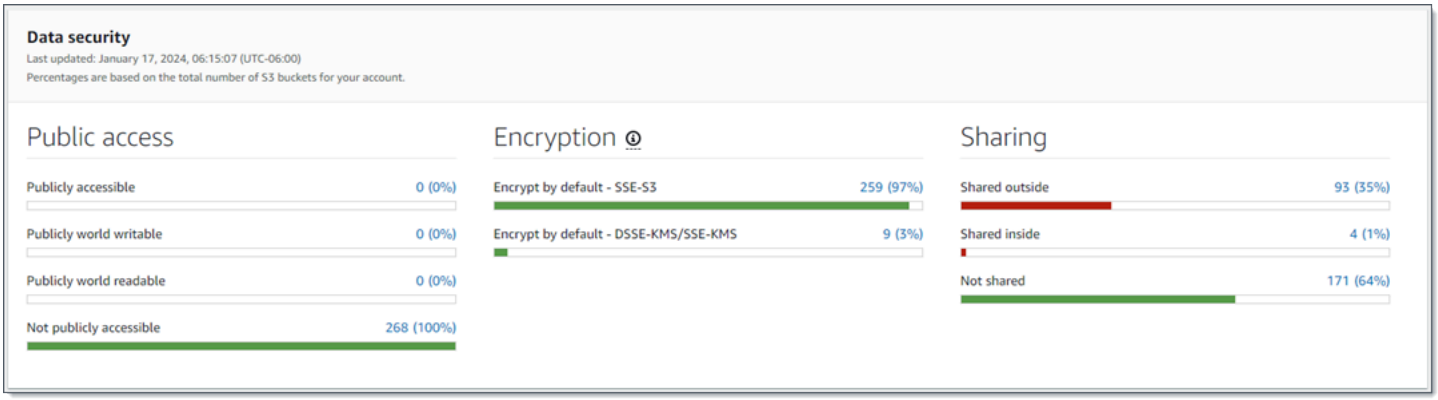
如果 Macie 在過去七天內未建立或更新任何原則發現項目，則此區段為空白。或者，在過去七天內建立或更新的所有原則發現項目，都會受到抑制規則的抑制。

了解摘要儀表板上的資料安全統計資料

摘要儀表板的資料安全部分提供統計資料，可協助您識別和調查目前 Amazon S3 資料的潛在安全和隱私權風險 AWS 區域。例如，您可以使用此資料來識別可公開存取或與其他人共用的一般用途值區 AWS 帳戶。

如果您的 Macie 帳戶是組織的成員，則本節頂端的儲存和敏感資料探索統計資料會指出您在 Amazon S3 中存放的資料量，以及 Macie 可以分析多少資料以偵測敏感資料。

對於任何類型的 Macie 帳戶，其他統計資料分為三個區域，如下圖所示。



複查每個區域時，選擇性地選擇要向下追溯並複查支援資料的料號。另請注意，統計資料不包含 S3 目錄儲存貯體的資料，僅包含一般用途儲存貯體的資料。Macie 不會監視或分析目錄值區。

各區域的個別統計資料如下。

公用存取

這些統計資料指出有多少 S3 儲存貯體可公開存取或不可公開存取：

- 可公開存取 — 允許一般大眾對值區具有讀取或寫入存取權的值區的數量和百分比。
- 可公開寫入的世界 — 允許一般大眾對存儲桶具有寫入權限的存儲桶的數量和百分比。
- 公開的世界可讀 — 允許一般大眾對存儲桶具有讀取權限的存儲桶的數量和百分比。
- 不可公開存取 — 不允許一般大眾對值區具有讀取或寫入存取權限的值區的數量和百分比。

若要計算每個百分比，Macie 會將適用時段數除以時段存貨中的時段總數。

為了決定此區段中的值，Macie 會分析每個值區的帳戶層次與時段層次設定組合：帳戶的區塊公用存取設定、值區的區塊公用存取設定、值區的值區政策，以及值區的存取控制清單 (ACL)。如需這些設定的相關資訊，請參閱 Amazon S3 中的身分和存取管理和 Amazon S3 儲存的公開存取和 Amazon S3 儲存使用者指南中的封鎖對 Amazon S3 儲存的公開存取。

在某些情況下，「公用存取」區段也會顯示「未知」的值。如果出現這些值，Macie 就無法評估指定數量和值區百分比的公用存取設定。例如，暫時性問題或值區的權限設定會導致 Macie 無法擷取必要的資料。或者 Macie 無法完全判斷一或多個原則陳述式是否允許外部實體存取值區。

加密

這些統計資料指出有多少 S3 儲存貯體設定為將特定類型的伺服器端加密套用至新增至儲存貯體的物件：

- 預設加密 — SSE-S3 — 其預設加密設定設定設定為使用 Amazon S3 受管金鑰加密新物件的儲存貯體數量和百分比。對於這些值區，新物件會使用 SSE-S3 加密自動加密。
- 預設情況下加密 — DSSE-KMS/SSE-KMS — 值區的數量和百分比 AWS KMS key，其預設加密設定已設定為使用或客戶管理的金鑰來加密新物件。 AWS 受管金鑰 對於這些值區，新物件會使用 DSSE-KMS 或 SSE-KMS 加密自動加密。

若要計算每個百分比，Macie 會將適用時段數除以時段存貨中的時段總數。

為了確定本節中的值，Macie 會分析每個值區的預設加密設定。自 2023 年 1 月 5 日起，Amazon S3 會自動使用 Amazon S3 受管金鑰 (SSE-S3) 套用伺服器端加密，作為新增至儲存貯體之物件的基礎加密層級。您可以選擇性地設定值區的預設加密設定，改為使用金鑰 (SSE-KMS) 的伺服器端加密，或使用金 AWS KMS 鑰 (DSSE-KMS) 進行雙層伺服器端加密。 AWS KMS 如需有關預設加密設定和選項的資訊，請參閱 Amazon 簡單儲存體服務使用者指南中的設定 S3 儲存貯體的預設伺服器端加密行為。

在某些情況下，「加密」區段也會顯示「未知」的值。如果出現這些值，Macie 就無法評估指定數目和值區百分比的預設加密設定。例如，暫時性問題或值區的權限設定會導致 Macie 無法擷取必要的資料。

分享

這些統計資料指出有多少 S3 儲存貯體與其他 AWS 帳戶 Amazon CloudFront 原始存取身分 (OAI) 或來源存取控制 (OAC) 共用或 CloudFront未與其他儲存貯體共用：

- 外部共用 — 與下列一或多個或下列任何組合共用的值區數量和百分比： CloudFront OAI、CloudFront OAC 或不在同一組織中的帳戶。
- 共用內部 — 與相同組織中一或多個帳號共用的值區數量和百分比。這些值區不會與 CloudFront OAI 或 OAC 共用。
- 未共用 — 未與其他帳戶、 CloudFront OAI 或 CloudFront OAC 共用的值區數量和百分比。

若要計算每個百分比，Macie 會將適用時段數除以時段存貨中的時段總數。

為了判斷值區是否與其他值區共用 AWS 帳戶，Macie 會分析每個值區的值區政策和 ACL。此外，組織被定義為一組 Macie 帳戶，透過 AWS Organizations 或透過 Macie 邀請集中管理為一組相關帳戶。如需 Amazon S3 共用儲存貯體選項的相關資訊，請參閱 Amazon 簡單儲存服務使用者指南中的 Amazon S3 中的身分和存取管理。

> **Note**
>
> 在某些情況下，Macie 可能會錯誤地報告與不在同一個組織中 AWS 帳戶 的值區共用的值區。如果 Macie 無法完全評估儲存貯體政策中的元素與政策`Principal`元素中的特定AWS 全域條件內容金鑰或 Amazon S3 條件金鑰之間的關係，就會發生這種情況。`Condition`適用的條件鍵為：`aws:PrincipalAccount`、`aws:PrincipalArn`、`aws:PrincipalOrgID`、`aws:Principal`和`s3:DataAccessPointArn`。
>
> 若要判斷是否適用於個別值區，請在資料面板上選擇「共用的外部統計資料」。在顯示的表格中，記下每個值區的名稱。然後使用 Amazon S3 檢閱每個儲存貯體的政策，並判斷共用存取設定是否有意且安全。

若要判斷值區是否與 CloudFront OAI 或 OAC 共用，Macie 會分析每個儲存貯體的儲存貯體政策。CloudFront OAI 或 OAC 可讓使用者透過一或多個指 CloudFront定的發行版存取值區的物件。如需 CloudFront OAI 和 OAC 的相關資訊，請參閱 Amazon 開發人員指南中的限制對 Amazon S3 來源的存取。 CloudFront

在某些情況下，「共用」區段也會顯示「未知」的值。如果出現這些值，Macie 就無法判斷指定的值區數目和百分比是否與其他帳戶、 CloudFront OAI 或 CloudFront OAC 共用。例如，暫時性問題或值區的權限設定會導致 Macie 無法擷取必要的資料。或者 Macie 無法完全評估桶的政策或 ACL。

使用亞馬遜 Macie 分析您的 Amazon S3 安全狀態

為了協助您執行深入分析並評估 Amazon Simple Storage Service (Amazon S3) 資料的安全狀態，Amazon Macie 會在您使用 Macie 的每個 AWS 區域 位置維護 S3 一般用途儲存貯體的完整清單。若要瞭解 Macie 如何為您維護此庫存，請參閱Macie 如何監控 Amazon S3 數據安全。如果您是組織的 Macie 管理員，則庫存會包含您的成員帳戶所擁有的 S3 儲存貯體的資料。

透過使用此庫存，您可以檢閱 Amazon S3 資料資產，並檢查適用於個別 S3 儲存貯體的關鍵安全設定和指標的詳細資料和統計資料。例如，您可以存取每個值區的公開存取和加密設定的劃分，以及 Macie 可以分析以偵測每個值區中敏感資料的物件大小和數量。您也可以決定是否設定敏感資料探索工作或自

動化敏感資料探索，以分析值區中的物件。如果有，您的庫存資料會指出最近進行該分析的時間。如果啟用自動化敏感資料探索，您也可以使用庫存來檢閱 Macie 迄今為止針對 Amazon S3 資料執行的自動化敏感資料探索活動的結果。如需詳細資訊，請參閱 探索敏感資料。

您可以使用 Amazon Macie 主控台上的 S3 儲存貯體頁面瀏覽和篩選庫存資料。您也可以使用 Amazon Macie API 的DescribeBuckets操作，以程式設計方式存取庫存資料。

主題

- 使用 Amazon Macie 查看您的 S3 儲存貯體庫存
- 使用 Amazon Macie 篩選 S3 儲存貯體庫存

使用 Amazon Macie 查看您的 S3 儲存貯體庫存

在 Amazon Macie 主控台上，S3 儲存貯體頁面針對目 AWS 區域前 Amazon Simple Storage Service (Amazon S3) 資料的安全性和隱私權提供詳細的見解。使用此頁面，您可以檢閱和分析區域中 S3 一般用途儲存貯體的完整清查，並檢閱個別儲存貯體的詳細資訊和統計資料。如果您是組織的 Macie 管理員，您的庫存會包含成員帳戶所擁有的 S3 儲存貯體的詳細資料和統計資料。

S3 儲存貯體頁面也會指出 Macie 最近從 Amazon S3 擷取您帳戶的儲存貯體或物件中繼資料的時間。您可以在頁面頂端的「上次更新」欄位中找到此資訊。如果您是組織的 Macie 管理員，此欄位會指出 Macie 擷取組織中帳戶資料的最早日期和時間。如需詳細資訊，請參閱 數據刷新。

請注意，庫存資料和統計資料不包含 S3 目錄儲存貯體的相關資料，只包含一般用途儲存貯體。Macie 不會監視或分析目錄值區。此外，大多數庫存資料僅限於 Macie 允許您帳戶存取的儲存貯體。如果值區的權限設定阻止 Macie 擷取值區或值區物件的相關資訊，Macie 只能提供值區相關資訊的子集。如果特定值區發生這種情況，Macie 會在值區庫存中顯示該值區的警告圖示 (⚠) 和訊息。對於值區的詳細資訊，Macie 僅顯示欄位和資料的子集：擁有 AWS 帳戶 該值區的帳戶 ID、值區的名稱、Amazon 資源名稱 (ARN)、建立日期和區域；以及 Macie 最近擷取值區的值區和物件中繼資料作為每日重新整理週期的一部分時。若要調查問題，請檢閱 Amazon S3 中儲存貯體的政策和許可設定。例如，值區可能具有限制性的值區政策。如需詳細資訊，請參閱 允許 Macie 存取 S3 儲存貯體和物件。

如果您偏好以程式設計方式存取和查詢庫存資料，可以使用 Amazon Macie API 的DescribeBuckets操作。

主題

- 檢閱您的 S3 儲存貯體庫存

- 檢閱 S3 儲存貯體的詳細資訊

檢閱您的 S3 儲存貯體庫存

Amazon Macie 主控台上的 S3 儲存貯體頁面提供目前 AWS 區域 S3 一般用途儲存貯體的相關資訊。在此頁面上，表格會顯示詳細目錄中每個儲存貯體的摘要資訊。若要自訂檢視，您可以排序和篩選表格。如果您在表格中選擇值區，詳細資料面板會顯示值區的其他相關資訊。這包括設置和指標的詳細信息和統計信息，可提供值區數據的安全性和隱私性的洞察力。您可以選擇性地將資料從表格匯出至逗號分隔值 (CSV) 檔案。

如果啟用了自動化敏感資料探索功能，您也可以選擇使用互動式熱圖來檢閱庫存。該地圖提供 Amazon S3 資料資產中資料敏感度的視覺化呈現。它捕獲 Macie 迄今為止執行的自動化敏感數據發現活動的結果。若要瞭解此地圖，請參閱使用 S3 儲存貯體對應視覺化資料敏感度。

若要檢閱您的 S3 儲存貯體庫存

1. 在以下位置打開 Amazon Macie 控制台 https://console.aws.amazon.com/macie/。
2. 在導覽窗格中，選擇 S3 儲存貯體。S3 儲存貯體頁面會顯示儲存貯體庫存。如果頁面顯示庫存的互動式地圖，請選擇頁面頂端的 table
   ()。
   然後，Macie 會顯示庫存中的值區數量以及值區表格。

   如果啟用了自動化敏感資料探索，預設檢視不會顯示目前從自動探索中排除的值區的資料。若要顯示此資料，請在篩選器方塊下方的 [由自動探索篩選器權杖監視] 中選擇 [X]。
3. 在頁面頂端，選擇性地選擇重新整理
   ()
   以從 Amazon S3 擷取最新的儲存貯體中繼資料。

   如果資訊圖示
   ()
   出現在任何值區名稱旁，我們建議您這麼做。此圖示表示儲存貯體是在過去 24 小時內建立的，可能是在 Macie 上次從 Amazon S3 擷取儲存貯體和物件中繼資料作為每日重新整理週期的一部分之後。
4. 在 S3 儲存貯體頁面上，使用表格來檢閱庫存中每個儲存貯體的相關資訊子集：

   - 靈敏度 — 值區目前的靈敏度分數。只有在啟用自動敏感資料探索時，才會顯示此欄。如需有關 Macie 定義之敏感度分數範圍的資訊，請參閱S3 儲存貯體的靈敏度評分。

- 「值區」— 值區的名稱。
- 帳號 — 擁有值區 AWS 帳戶 的帳號 ID。
- 可分類的物件 — Macie 可以分析以偵測值區中敏感資料的物件總數。
- 可分類大小 — Macie 可以分析以偵測值區中敏感資料的所有物件的總儲存大小。

  請注意，這個值不會反映任何壓縮物件解壓縮後的實際大小。此外，如果值區已啟用版本控制，則此值會根據值區中每個物件最新版本的儲存大小而定。
- 依工作監控 — 是否將任何敏感資料探索工作設定為每日、每週或每月定期分析值區中的物件。

  如果此欄位的值為「是」，則時段會明確納入週期性工單中，或符合過去 24 小時內週期性工單條件的時段。此外，其中至少有一個工作的狀態為「未取消」。Macie 每天都會更新此數據。
- 最新工作執行 — 如果將任何一次性或定期敏感資料探索工作配置為分析值區中的物件，則此欄位會指出其中一個工作開始執行的最近日期和時間。否則，此欄位中會出現一個破折號 (—)。

在上述資料中，如果物件使用支援的 Amazon S3 儲存類別，且物件具有支援檔案或儲存格式的副檔名，則物件即可分類。您可以通過使用 Macie 檢測對象中的敏感數據。如需詳細資訊，請參閱支援的儲存類別和格式。

5. 若要使用表格分析庫存，請執行下列任一項作業：

- 若要依特定欄位對表格進行排序，請選擇欄位的欄標題。若要變更排序順序，請再次選擇欄標題。
- 若要篩選表格並僅顯示具有特定欄位值的值區，請將游標置於篩選方塊中，然後新增欄位的篩選條件。若要進一步細化結果，請新增其他欄位的篩選條件。如需詳細資訊，請參閱 篩選 S3 儲存貯體庫存。

6. 若要檢閱特定值區的詳細資料和統計資料，請在表格中選擇值區的名稱，然後參閱詳細資料面板。

> **Tip**
>
> 您可以在值區詳細資料面板中樞紐分析和向下鑽研許多欄位。若要顯示欄位具有相同值的值區，請在欄位中選擇。若要顯示具有欄位其他值的值區，請在欄位中選擇。

7. 若要將資料從表格匯出至 CSV 檔案，請選取要匯出之每一列的核取方塊，或選取選取欄標題中的核取方塊以選取所有列。然後選擇頁面頂端的「匯出為 CSV」。您最多可以從表格中匯出 50,000 列。

檢閱 S3 儲存貯體的詳細資訊

在 Amazon Macie 主控台上，您可以使用 S3 儲存貯體頁面上的詳細資料面板來檢閱 S3 儲存貯體庫存中每個一般用途儲存貯體的統計資料和其他資訊。這包括設置和指標的詳細信息和統計信息，可提供值區數據安全性和隱私性的洞察力。

例如，您可以檢閱 S3 儲存貯體的公開存取設定細分，並判斷儲存貯體是設定為複寫物件還是與其他 AWS 帳戶儲存貯體共用。您也可以判斷是否設定任何敏感資料探索工作來檢查儲存貯體中是否有敏感資料。如果有，您可以存取最近執行之工作的詳細資訊，並選擇性地顯示工作產生的任何發現項目。

如果啟用自動化敏感資料探索，您也可以使用詳細資料面板來檢閱敏感資料探索統計資料以及個別 S3 儲存貯體的其他相關資訊。此面板會擷取 Macie 迄今為止針對值區執行的自動化敏感資料探索活動的結果。若要瞭解這些詳細資訊，請參閱複查個別 S3 儲存貯體的資料敏感度詳細。

若要檢閱 S3 儲存貯體的詳細資訊

1. 在以下位置打開 Amazon Macie 控制台 https://console.aws.amazon.com/macie/。
2. 在導覽窗格中，選擇 S3 儲存貯體。S3 儲存貯體頁面會顯示儲存貯體庫存。

   如果啟用了自動化敏感資料探索，預設檢視不會顯示目前從自動探索中排除的值區的資料。若要顯示此資料，請在篩選器方塊下方的 [由自動探索篩選器權杖監視] 中選擇 [X]。
3. 在頁面頂端，選擇性地選擇重新整理
   ()
   以從 Amazon S3 擷取最新的儲存貯體中繼資料。
4. 選擇您要複查其明細的時段。詳細資料面板會顯示值區的統計資料和其他相關資訊。

在詳細資料面板中，統計資料和資訊會組織成下列主要區段：

概觀 | 對象統計信息 | 服務器端加密 | 敏感數據發現 | 公共訪問 | 複製 | 標籤

當您複查每個區段中的資訊時，您可以選擇性地對某些欄位進行樞
紐分析和向下鑽研。若要顯示欄位具有相同值的值區，
請 在

欄位中選擇。若要顯示具有欄位其他值的值區，
請 在
欄位中選擇。

概觀

本節提供值區的一般資訊，例如值區的名稱、建立值區的時間，以及擁有 AWS 帳戶 該值區的帳號 ID。特別注意的是，「上次更新」欄位會指出 Macie 最近從 Amazon S3 擷取儲存貯體或儲存貯體物件的中繼資料的時間。

共用存取權欄位會指出儲存貯體是否與另一個儲存貯體共用 AWS 帳戶、Amazon CloudFront 原始存取身分 (OAI) 或 CloudFront 來源存取控制 (OAC)：

- 外部 — 值區會與下列一或多項或下列任何組合共用： CloudFront OAI、CloudFront OAC 或組織外部 (不屬於) 組織的帳戶。
- 內部 — 值區會與一或多個屬於您組織內部 (部分) 的帳戶共用。它不會與 CloudFront OAI 或 OAC 共用。
- 未共用 — 值區不會與其他帳戶、 CloudFront OAI 或 CloudFront OAC 共用。
- 未知 — Macie 無法評估值區的共用存取設定。

為了判斷值區是否與另一個值區共用 AWS 帳戶，Macie 會分析值區的儲存貯體政策和存取控制清單 (ACL)。分析僅限於值區層級設定。它不會反映值區中共用特定物件的任何物件層級設定。此外，組織被定義為一組 Macie 帳戶，透過 AWS Organizations 或透過 Macie 邀請集中管理為一組相關帳戶。若要了解 Amazon S3 共用儲存貯體的選項，請參閱 Amazon 簡單儲存服務使用者指南中的 Amazon S3 中的身分和存取管理。

> **Note**
>
> 在某些情況下，Macie 可能會錯誤地指出儲存貯體與組 AWS 帳戶 織外部 (不屬於) 的值區共用。如果 Macie 無法完全評估儲存貯體政策中的元素與政策`Principal`元素中的特定AWS 全域條件內容金鑰或 Amazon S3 條件金鑰之間的關係，就會發生這種情況。`Condition`適用的條件鍵為：`aws:PrincipalAccount`、`aws:PrincipalArn`、`aws:PrincipalOrgID`、`aws:PrincipalOrgP`和`s3:DataAccessPointArn`。我們建議您檢閱值區的政策，以判斷此存取是否有意且安全。

若要判斷值區是否與 CloudFront OAI 或 OAC 共用，Macie 會分析值區的值區政策。 CloudFront OAI 或 OAC 可讓使用者透過一或多個指 CloudFront 定的發行版存取值區的物件。若要了解 CloudFront OAI 和 OAC，請參閱 Amazon 開發人員指南中的限制對 Amazon S3 來源的存取。 CloudFront

[概觀] 區段也包含 [最新的自動化探索執行] 欄位。此欄位指出 Macie 最近在執行自動化敏感資料探索時分析值區中物件的時間。如果尚未進行此分析，則此欄位中會出現破折號 (—)。

物件統計

本節提供值區中物件的相關資訊，從值區中的物件總數開始 (總計計數)、所有這些物件的總儲存大小 (儲存大小總計)，以及所有壓縮物件 (.gz、.gzip 或 .zip) 檔案的總儲存大小 (壓縮大小總計)。本節中的其他統計資料可協助您評估 Macie 可以分析多少資料以偵測值區中的敏感資料。

如果您最近建立了值區，或在過去 24 小時內對值區的物件進行了重大變更，請選擇重新整理
()
來擷取值區物件的最新中繼資料。Macie 會顯示資訊圖示
()
來協助您判斷是否發生這種情況。如果值區儲存 30,000 個或更少的物件，則可使用重新整理選項。

檢閱本節中的統計資料時，請記住下列事項：

- 如果值區已啟用版本控制，則大小值會根據值區中每個物件最新版本的儲存大小為基礎。
- 如果值區儲存壓縮物件，則大小值在解壓縮後不會反映這些物件的實際大小。
- 如果您重新整理值區的物件中繼資料，Macie 會暫時回報未知的加密統計資料套用至物件。Macie 會在 24 小時內執行值區和物件中繼資料的下一次每日重新整理時，重新評估和更新這些統計資料的資料。
- 根據預設，物件計數和大小值會包含值區因上傳不完整而包含之任何物件零件的資料。如果您重新整理值區的物件中繼資料，Macie 會從重新計算的值中排除物件零件的資料。當 Macie 執行值區和物件中繼資料的下一次每日重新整理時 (在 24 小時內)，Macie 會重新計算並更新這些統計資料的值，並在值中再次包含物件部分的資料。

  請注意，Macie 無法分析物件部分來偵測敏感資料。Amazon S3 必須先將零件組裝成一個或多個物件，以便 Macie 進行分析。如需有關分段上傳和物件零件的資訊，包括如何使用生命週期規則自動刪除零件，請參閱 Amazon Simple Storage Service 使用者指南中的使用多部分上傳來上傳和複製物件。若要識別包含物件組件的儲存貯體，您可以參考 Amazon S3 儲存鏡頭中不完整的分段上傳指標。如需詳細資訊，請參閱 Amazon 簡單儲存服務使用者指南中的評估儲存活動和使用情況。

物件統計資料的組織方式如下。

可分類的物件

本節指出 Macie 可以分析以偵測敏感資料的物件總數，以及這些物件的總儲存大小。這些物件使用支援的 Amazon S3 儲存類別，並具有支援檔案或儲存格式的副檔名。您可以通過使用 Macie 檢測對象中的敏感數據。如需詳細資訊，請參閱 支援的儲存類別和格式。

未分類的物件

本節指出 Macie 無法分析以偵測敏感資料的物件總數，以及這些物件的儲存空間總大小。這些物件不使用支援的 Amazon S3 儲存類別，或者它們沒有支援的檔案或儲存格式的副檔名。

無法分類的物件：儲存類別

本節提供 Macie 無法分析的物件數量和儲存大小明細，因為物件不使用支援的 Amazon S3 儲存類別。

無法分類的物件：檔案類型

本節提供 Macie 無法分析之物件的數量和儲存大小明細，因為物件沒有支援的檔案或儲存格式的副檔名。

各加密類型的物件

本節提供使用 Amazon S3 支援之每種加密類型的物件數目明細：

- 客戶提供 — 使用客戶提供的金鑰加密的物件數目。這些物件使用 SSE-C 加密。
- AWS KMS Managed — 使用客戶管理金鑰 AWS 受管金鑰 或客戶管理金鑰加密的物件數目。AWS KMS key這些物件會使用 DSSE-KMS 或 SSE-KMS 加密。
- Amazon S3 受管 — 使用 Amazon S3 受管金鑰加密的物件數量。這些物件使用 SSE-S3 加密。
- [無加密] — 未加密或使用用戶端加密的物件數目。(如果物件使用用戶端加密加密，Macie 就無法存取和報告該物件的加密資料。)
- 未知 — Macie 目前沒有加密中繼資料的物件數目。如果您最近選擇手動重新整理值區物件的中繼資料，通常會發生這種情況。Macie 會在 24 小時內執行值區和物件中繼資料的下一次每日重新整理時，更新加密統計資料。

如需每種受支援加密類型的相關資訊，請參閱 Amazon 簡單儲存服務使用者指南中的使用加密保護資料。

伺服器端加密

本節提供值區伺服器端加密設定的深入資訊。

值區政策所需的加密欄位會指出將物件新增至值區時，值區的政策是否需要對物件進行伺服器端加密：

- 否 — 值區沒有值區政策，或儲存貯體的政策不需要新物件的伺服器端加密。如果存在值區政策，則不需要要PutObject求包含有效的伺服器端加密標頭。
- 是 — 值區的政策需要新物件的伺服器端加密。 PutObject值區的要求必須包含有效的伺服器端加密標頭。否則，Amazon S3 會拒絕要求。
- 未知 — Macie 無法評估值區的政策，以判斷是否需要新物件的伺服器端加密。

對於此評估，有效的伺服器端加密標頭為：`x-amz-server-side-encryption`值為`AES256`或`aws:kms`，且`x-amz-server-side-encryption-customer-algorithm`值為`AES256`。如需使用儲存貯體政策要求伺服器端加密新物件的相關資訊，請參閱 Amazon 簡單儲存服務使用者指南中的使用伺服器端加密保護資料。

預設加密欄位會指出儲存貯體設定為預設套用哪個伺服器端加密演算法至新增至值區的物件：

- AES256 — 儲存貯體的預設加密設定已設定為使用 Amazon S3 受管金鑰加密新物件。新物件會使用 SSE-S3 加密自動加密。
- aw:kms — 值區的預設加密設定是設定為使用 AWS KMS key、 AWS 受管金鑰 或客戶管理的金鑰來加密新物件。新物件會使用 SSE-KMS 加密自動加密。此AWS KMS key欄位會顯示所使用金鑰的 Amazon 資源名稱 (ARN) 或唯一識別碼 (金鑰 ID)。
- aws: kms: dsse — 值區的預設加密設定已設定為使用 (或客戶管理的金鑰) 來加 AWS KMS key密新物件。 AWS 受管金鑰 新物件會使用 DSSE-KMS 加密自動加密。此AWS KMS key欄位會顯示所使用金鑰的 ARN 或金鑰識別碼。
- 無 — 值區的預設加密設定不會為新物件指定伺服器端加密行為。

自 2023 年 1 月 5 日起，Amazon S3 會自動使用 Amazon S3 受管金鑰 (SSE-S3) 套用伺服器端加密，作為新增至儲存貯體之物件的基礎加密層級。您可以選擇性地設定值區的預設加密設定，改為使用金鑰 (SSE-KMS) 的伺服器端加密，或使用金 AWS KMS 鑰 (DSSE-KMS) 進行雙層伺服器端加密。 AWS KMS 如需有關預設加密設定和選項的資訊，請參閱 Amazon 簡單儲存體服務使用者指南中的設定 S3 儲存貯體的預設伺服器端加密行為。

敏感性資料探索

本節指出是否將任何敏感資料探索工作設定為每日、每週或每月定期分析值區中的物件。如果「由工單主動監督」欄位的值為「是」，則該時段會明確納入週期性工單中，或符合過去 24 小時內週期性工單之條件的時段。此外，其中至少有一個工作的狀態為「未取消」。Macie 每天都會更新此數據。

如果將任何類型的敏感資料探索工作 (定期工作或一次性工作) 設定為檢查值區，則 [最新作業] 欄位會提供最近開始執行之工作的唯一識別碼。[最近的工作執行] 欄位會指出該工作開始執行的時間。

> **Tip**
>
> 若要顯示工作產生的所有機密資料發現項目，請選擇「最新工作」欄位中的連結。在出現的工作詳細資料面板中，選擇面板頂端的 [顯示結果]，然後選擇 [顯示發現項目]。

公用存取

本節指出儲存貯體是否可公開存取。它也會提供各種帳戶層級和儲存貯體層級設定的明細，以判斷是否發生這種情況。[有效權限] 欄位會指出這些設定的累計結果：

- 不公開 — 值區不可公開存取。
- 公開 — 值區可公開存取。
- 未知 — Macie 無法評估值區的所有公開存取設定。

請注意，此資料僅限於帳戶和儲存貯體層級的設定。它不會反映允許公開存取值區中特定物件的物件層級設定。

若要了解用於管理儲存貯體和儲存貯體資料的公有存取權限的 Amazon S3 設定，請參閱 Amazon S3 中的身分和存取管理和 Amazon S3 儲存的公有存取權限，以及 Amazon 簡單儲存服務使用者指南中的封鎖公開存取。

複寫

在此段落中，「已複製」欄位會指出值區是否設定為將物件複製到其他值區。如果此欄位的值為 [是]，則會為值區配置並啟用一或多個複製規則。接著，本節也會列出擁有目標值區 AWS 帳戶 之每個帳號 ID。

「外部複製」欄位會指出值區是否設定為 AWS 帳戶 將物件複製到組織外部 (非屬於) 的值區。組織是一組 Macie 帳戶，可透過 AWS Organizations 或透過 Macie 邀請集中管理為一組相關帳戶。如果此欄位的值為 [是]，則會針對值區設定並啟用複製規則，且規則會設定為將物件複製到外部所擁有的值區 AWS 帳戶。

> **Note**
>
> 在特定情況下，Macie 可能會錯誤地指出值區已設定為將物件複製到外部 AWS 帳戶所擁有的值區。如果在 Macie 從 Amazon S3 擷取儲存貯體和物件中繼資料作為每日重新整理週期的一部分之後，目標儲存貯體是在前 24 小時內建立的，則可能會發生這種 AWS 區域 情況。

若要使用 Macie 調查問題，請選擇重新整理
()
從 Amazon S3 擷取最新的儲存貯體中繼資料。然後檢閱本節中的帳號 ID 清單。如需更深入的調查，請使用 Amazon S3 檢閱儲存貯體的複寫規則。

若要了解 Amazon S3 複寫儲存貯體物件的選項和設定，請參閱 Amazon 簡單儲存服務使用者指南中的複寫物件。

標籤

如果標籤與值區相關聯，此區段就會出現在面板中，並列出這些標籤。標籤是您可以定義並指派給特定類型 AWS 資源 (包括 S3 儲存貯體) 的標籤。每個標籤都包含必要的標籤鍵和一個可選的標籤值。

若要了解如何標記儲存貯體，請參閱 Amazon 簡單儲存服務使用者指南中的使用成本分配 S3 儲存貯體標籤。

使用 Amazon Macie 篩選 S3 儲存貯體庫存

若要識別並專注於具有特定特性的儲存貯體，您可以在 Amazon Macie 主控台上篩選 S3 儲存貯體庫存，以及使用 Amazon Macie API 以程式設計方式提交的查詢中篩選 S3 儲存貯體庫存。建立篩選器時，您可以使用特定的值區屬性來定義條件，以便在檢視表或查詢結果中包含或排除值區。值區屬性是儲存貯體特定中繼資料的欄位。

在 Macie 中，過濾器由一個或多個條件組成。每個條件，也稱為準則，由三個部分組成：

- 以屬性為基礎的欄位，例如「值區名稱」、「標籤索引鍵」或「在工作中定義」。
- 運算子，例如等於或不等於。
- 一或多個值。值的類型和數目取決於您選擇的欄位和運算子。

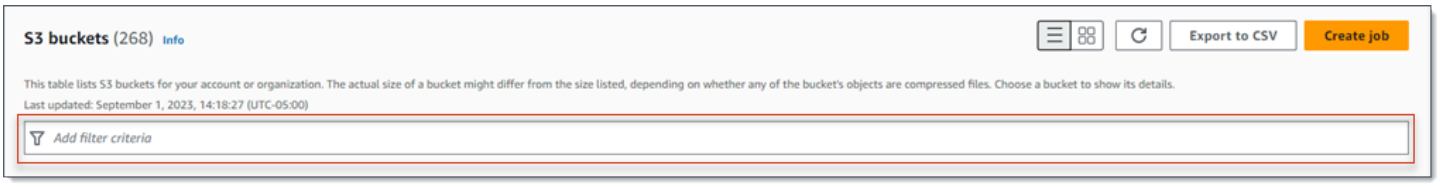
定義和套用篩選條件的方式取決於您使用的是 Amazon Macie 主控台還是 Amazon Macie API。

主題

- 在 Amazon Macie 控制台上過濾庫存
- 使用 Amazon Macie API 以程式設計方式篩選庫存

在 Amazon Macie 控制台上過濾庫存

如果您使用 Amazon Macie 主控台篩選 S3 儲存貯體庫存，Macie 會提供選項來協助您針對個別條件選擇欄位、操作員和值。您可以使用 S3 儲存貯體頁面上的篩選方塊存取這些選項，如下圖所示。

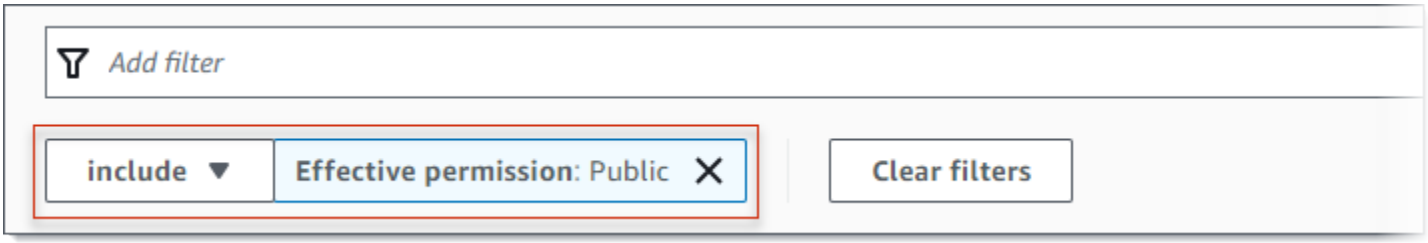


當您將游標置於篩選方塊中時，Macie 會顯示您可以在篩選條件中使用的欄位清單。欄位依邏輯類別組織。例如，「一般欄位」 類別包含儲存 S3 儲存貯體一般資訊的欄位。公開存取類別包含欄位，這些欄位會儲存可套用至值區之各種公用存取設定類型的相關資料。欄位會在每個類別中按字母順序排序。

若要新增條件，請先從清單中選擇欄位。若要尋找欄位，請瀏覽完整清單，或輸入部分欄位名稱以縮小欄位清單。

根據您選擇的欄位，Macie 會顯示不同的選項。這些選項會反映您所選欄位的類型和性質。例如，如果您選擇「共用存取」欄位，Macie 會顯示可供選擇的值清單。如果您選擇「儲存貯體名稱」欄位，Macie 會顯示一個文字方塊，您可以在其中輸入 S3 儲存貯體的名稱。無論您選擇哪個欄位，Macie 都會引導您完成以下步驟，以新增條件，其中包含欄位的必要設定。

在您新增條件之後，Macie 會套用條件的條件，並在篩選方塊下方的篩選條件 Token 中顯示條件，如下圖所示。



在此範例中，條件設定為包含可公開存取的所有值區，並排除所有其他值區。它返回桶，其中有效權限字段的值等於公共。

當您新增更多條件時，Macie 會套用其準則，並將其顯示在篩選方塊下方。如果您新增多個條件，Macie 會使用 AND 邏輯來連接條件並評估篩選準則。這表示 S3 儲存貯體只有在符合篩選條件中的所有條件時才符合篩選條件。您可以隨時參考篩選方塊下方的區域，以決定您套用的條件。

使用主控台篩選庫存

1. 在以下位置打開 Amazon Macie 控制台 https://console.aws.amazon.com/macie/。

2. 在導覽窗格中，選擇 S3 儲存貯體。S3 儲存貯體頁面會顯示儲存貯體庫存。

   如果啟用了自動化敏感資料探索，預設檢視不會顯示目前從自動探索中排除的值區的資料。如果您是組織的 Macie 管理員，它也不會顯示目前已停用自動探索功能的帳戶資料。若要顯示此資料，請在篩選器方塊下方的 [由自動探索篩選器權杖監視] 中選擇 [X]。

3. 在頁面頂端，選擇性地選擇重新整理

   ()

   以從 Amazon S3 擷取最新的儲存貯體中繼資料。

4. 將游標置於篩選方塊中，然後選擇要用於條件的欄位。

5. 為欄位選擇或輸入適當的值類型，並牢記下列秘訣。

   日期、時間和時間範圍

   對於日期和時間，請使用「從」(From) 和「到」(To) 方塊定義包含的時間範圍：

   - 若要定義固定時間範圍，請使用「從」(From) 和「到」(To) 方塊，分別指定範圍中的第一個日期和時間，以及最後一個日期和時間。
   - 若要定義從特定日期和時間開始並在目前時間結束的相對時間範圍，請在「從」(From) 方塊中輸入開始日期和時間，並刪除「至」(To) 方塊中的任何文字。
   - 若要定義在特定日期和時間結束的相對時間範圍，請在 [收件者] 方塊中輸入結束日期和時間，並刪除 [從] 方塊中的任何文字。

   請注意，時間值使用 24 小時標記法。如果您使用日期選擇器來選擇日期，您可以直接在「從」(From) 和「到」(To) 方塊中輸入文字來精簡值。

   數字和數值範圍

   對於數值，請使用「從」(From) 和「到」(To) 方塊來輸入定義包含數值範圍的整數：

   - 若要定義固定的數值範圍，請使用「從」(From) 和「到」(To) 方塊，分別指定範圍中的最小和最高數字。
   - 若要定義僅限於一個特定值的固定數值範圍，請在「從」(From) 和「到」(To) 方塊中輸入值。例如，若只要包含剛好存放 15 個物件的 S3 儲存貯體，請**15**在 [從] 和 [到] 方塊中輸入。
   - 若要定義從特定數字開始的相對數值範圍，請在「從」(From) 方塊中輸入數字，並且不要在「到」方塊中輸入任何文字。
   - 若要定義結束於特定數字的相對數值範圍，請在「至」方塊中輸入數字，並且不要在「從」方塊中輸入任何文字。

文字 (字串) 值

對於此類型的值，請為欄位輸入完整、有效的值。值是區分大小寫的。

請注意，您不能在這種類型的值中使用部分值或萬用字元。唯一的例外是「值區名稱」欄位。對於該欄位，您可以指定前置字元，而不是完整的值區名稱。例如，若要尋找名稱以 My-S3 開頭的所有 S3 儲存貯體，請輸入儲**my-S3**存貯體名稱欄位的篩選器值。如果您輸入任何其他值，例如**My-s3**或**my***，Macie 將不會傳回值區。

6. 為欄位新增值後，請選擇「套用」。Macie 會套用篩選條件，並在篩選器方塊下方的篩選器 Token 中顯示條件。
7. 針對您要新增的每個其他條件重複步驟 4 到 6。
8. 若要移除條件，請在條件的篩選器 Token 中選擇 X。
9. 若要變更條件，請在條件的篩選器 Token 中選擇 X 來移除條件。然後重複步驟 4 到 6，以使用正確的設定新增條件。

使用 Amazon Macie API 以程式設計方式篩選庫存

若要以程式設計方式篩選 S3 儲存貯體庫存，請在使用 Amazon Macie API DescribeBuckets操作提交的查詢中指定篩選條件。此操作返回對象的數組。每個物件都包含符合篩選準則之值區的統計資料和其他資訊。

若要在查詢中指定篩選條件，請在請求中包含篩選條件對映。對於每個條件，請為欄位指定欄位、運算子以及一或多個值。值的類型和數目取決於您選擇的欄位和運算子。如需可在條件下使用的欄位、運算子和值類型的相關資訊，請參閱 Amazon Macie API 參考中的 Amazon S3 資料來源。

下列範例說明如何在使用 AWS Command Line Interface (AWS CLI) 提交的查詢中指定篩選條件。您也可以使用目前版本的其他 AWS 命令列工具或 AWS SDK，或直接將 HTTPS 要求傳送至 Macie 來執行此操作。如需 AWS 工具和 SDK 的相關資訊，請參閱要建置的工具。 AWS

範例

- 範例 1：依時段名稱搜尋時段
- 範例 2：尋找可公開存取的值區
- 範例 3：尋找儲存未加密物件的值區
- 範例 4：尋找未受工作監控的值區
- 範例 5：搜尋將資料複製到外部帳戶的值區
- 範例 6：根據多重條件搜尋時段

這些示例使用描述桶命令。如果範例成功執行，Macie 會傳回buckets陣列。陣列會針對目前儲存貯體中的每個值區包含一個物件， AWS 區域 且符合篩選準則。如需此輸出的範例，請展開下一節。

buckets數組的例子

在此範例中，buckets陣列提供兩個值區的詳細資訊，這兩個值區符合查詢中指定的篩選準則。


```
{
    "buckets": [
        {
            "accountId": "123456789012",
            "allowsUnencryptedObjectUploads": "FALSE",
            "automatedDiscoveryMonitoringStatus": "MONITORED",
            "bucketArn": "arn:aws:s3:::DOC-EXAMPLE-BUCKET1",
            "bucketCreatedAt": "2020-05-18T19:54:00+00:00",
            "bucketName": "DOC-EXAMPLE-BUCKET1",
            "classifiableObjectCount": 13,
            "classifiableSizeInBytes": 1592088,
            "jobDetails": {
                "isDefinedInJob": "TRUE",
                "isMonitoredByJob": "TRUE",
                "lastJobId": "08c81dc4a2f3377fae45c9ddaexample",
                "lastJobRunTime": "2024-05-26T14:55:30.270000+00:00"
            },
            "lastAutomatedDiscoveryTime": "2024-06-07T19:11:25.364000+00:00",
            "lastUpdated": "2024-06-12T07:33:06.337000+00:00",
            "objectCount": 13,
            "objectCountByEncryptionType": {
                "customerManaged": 0,
                "kmsManaged": 2,
                "s3Managed": 7,
                "unencrypted": 4,
                "unknown": 0
            },
            "publicAccess": {
                "effectivePermission": "NOT_PUBLIC",
                "permissionConfiguration": {
                    "accountLevelPermissions": {
                        "blockPublicAccess": {
                            "blockPublicAcls": true,
                            "blockPublicPolicy": true,
                            "ignorePublicAcls": true,
                            "restrictPublicBuckets": true
                        }
```

```
                    },
                    "bucketLevelPermissions": {
                        "accessControlList": {
                            "allowsPublicReadAccess": false,
                            "allowsPublicWriteAccess": false
                        },
                        "blockPublicAccess": {
                            "blockPublicAcls": true,
                            "blockPublicPolicy": true,
                            "ignorePublicAcls": true,
                            "restrictPublicBuckets": true
                        },
                        "bucketPolicy": {
                            "allowsPublicReadAccess": false,
                            "allowsPublicWriteAccess": false
                        }
                    }
                },
                "region": "us-east-1",
                "replicationDetails": {
                    "replicated": false,
                    "replicatedExternally": false,
                    "replicationAccounts": []
                },
                "sensitivityScore": 78,
                "serverSideEncryption": {
                    "kmsMasterKeyId": null,
                    "type": "NONE"
                },
                "sharedAccess": "NOT_SHARED",
                "sizeInBytes": 4549746,
                "sizeInBytesCompressed": 0,
                "tags": [
                    {
                        "key": "Division",
                        "value": "HR"
                    },
                    {
                        "key": "Team",
                        "value": "Recruiting"
                    }
                ],
                "unclassifiableObjectCount": {
```

```
                "fileType": 0,
                "storageClass": 0,
                "total": 0
            },
            "unclassifiableObjectSizeInBytes": {
                "fileType": 0,
                "storageClass": 0,
                "total": 0
            },
            "versioning": true
        },
        {
            "accountId": "123456789012",
            "allowsUnencryptedObjectUploads": "TRUE",
            "automatedDiscoveryMonitoringStatus": "MONITORED",
            "bucketArn": "arn:aws:s3:::DOC-EXAMPLE-BUCKET2",
            "bucketCreatedAt": "2020-11-25T18:24:38+00:00",
            "bucketName": "DOC-EXAMPLE-BUCKET2",
            "classifiableObjectCount": 8,
            "classifiableSizeInBytes": 133810,
            "jobDetails": {
                "isDefinedInJob": "TRUE",
                "isMonitoredByJob": "FALSE",
                "lastJobId": "188d4f6044d621771ef7d65f2example",
                "lastJobRunTime": "2024-04-09T19:37:11.511000+00:00"
            },
            "lastAutomatedDiscoveryTime": "2024-06-07T19:11:25.364000+00:00",
            "lastUpdated": "2024-06-12T07:33:06.337000+00:00",
            "objectCount": 8,
            "objectCountByEncryptionType": {
                "customerManaged": 0,
                "kmsManaged": 0,
                "s3Managed": 8,
                "unencrypted": 0,
                "unknown": 0
            },
            "publicAccess": {
                "effectivePermission": "NOT_PUBLIC",
                "permissionConfiguration": {
                    "accountLevelPermissions": {
                        "blockPublicAccess": {
                            "blockPublicAcls": true,
                            "blockPublicPolicy": true,
                            "ignorePublicAcls": true,
```

```
                        "restrictPublicBuckets": true
                    }
                },
                "bucketLevelPermissions": {
                    "accessControlList": {
                        "allowsPublicReadAccess": false,
                        "allowsPublicWriteAccess": false
                    },
                    "blockPublicAccess": {
                        "blockPublicAcls": true,
                        "blockPublicPolicy": true,
                        "ignorePublicAcls": true,
                        "restrictPublicBuckets": true
                    },
                    "bucketPolicy": {
                        "allowsPublicReadAccess": false,
                        "allowsPublicWriteAccess": false
                    }
                }
            },
            "region": "us-east-1",
            "replicationDetails": {
                "replicated": false,
                "replicatedExternally": false,
                "replicationAccounts": []
            },
            "sensitivityScore": 95,
            "serverSideEncryption": {
                "kmsMasterKeyId": null,
                "type": "AES256"
            },
            "sharedAccess": "EXTERNAL",
            "sizeInBytes": 175978,
            "sizeInBytesCompressed": 0,
            "tags": [
                {
                    "key": "Division",
                    "value": "HR"
                },
                {
                    "key": "Team",
                    "value": "Recruiting"
                }
```

```
            ],
            "unclassifiableObjectCount": {
                "fileType": 3,
                "storageClass": 0,
                "total": 3
            },
            "unclassifiableObjectSizeInBytes": {
                "fileType": 2999826,
                "storageClass": 0,
                "total": 2999826
            },
            "versioning": true
        }
    ]
}
```

如果沒有值區符合篩選條件，Macie 會傳回空buckets陣列。

```
{
    "buckets": []
}
```

範例 1：依時段名稱搜尋時段

此範例使用 describe- bucket 命令來查詢名稱以 My-S3 開頭且位於目前值區的所有值區的中繼資料。AWS 區域

若為 Linux、macOS 或 Unix：

```
$ aws macie2 describe-buckets --criteria '{"bucketName":{"prefix":"my-S3"}}'
```

對於 Microsoft 視窗：

```
C:\> aws macie2 describe-buckets --criteria={\"bucketName\":{\"prefix\":\"my-S3\"}}
```

其中：

- 儲存貯 *bucketName* 指定值區名稱欄位的 JSON 名稱。
- *prefix* 指定前綴運算符。
- *## S3* 是值區名稱欄位的值。

範例 2：尋找可公開存取的值區

此範例使用 describe- bucket 命令來查詢目前儲存貯體的中繼資料，AWS 區域 並且根據權限設定的組合，可公開存取。

若為 Linux、macOS 或 Unix：

```
$ aws macie2 describe-buckets --criteria '{"publicAccess.effectivePermission":{"eq":["PUBLIC"]}}'
```

對於 Microsoft 視窗：

```
C:\> aws macie2 describe-buckets --criteria={\"publicAccess.effectivePermission\":{\"eq\":[\"PUBLIC\"]}}
```

其中：

- *####. ####### [####]* 欄位的 JSON 名稱。
- *eq* 指定等於運算符。
- *PUB* LIC 是 [有效權限] 欄位的列舉值。

範例 3：尋找儲存未加密物件的值區

此範例使用 describe- bucket 命令來查詢目前儲存貯體的中繼資料，AWS 區域 並儲存未加密物件。

若為 Linux、macOS 或 Unix：

```
$ aws macie2 describe-buckets --criteria '{"objectCountByEncryptionType.unencrypted":{"gte":1}}'
```

對於 Microsoft 視窗：

```
C:\> aws macie2 describe-buckets --criteria={\"objectCountByEncryptionType.unencrypted\":{\"gte\":1}}
```

其中：

- *objectCountByEncryptionType##### [###] ### JSON ###*

- *gte* 指定大於或等於運算符。
- *1* 是「無加密」欄位中包含相對數值範圍內的最低值。

範例 4：尋找未受工作監控的值區

此範例會使用 describe-bucket 命令，查詢目前儲存貯體的中繼資料， AWS 區域 而這些值區與任何週期性敏感資料探索工作都沒有關聯。

若為 Linux、macOS 或 Unix：

```
$ aws macie2 describe-buckets --criteria '{"jobDetails.isMonitoredByJob":{"eq":
["FALSE"]}}'
```

對於 Microsoft 視窗：

```
C:\> aws macie2 describe-buckets --criteria={\"jobDetails.isMonitoredByJob\":{\"eq\":
[\"FALSE\"]}}
```

其中：

- *####### isMonitoredBy#Job*」指定「由工作主動監視」欄位的 JSON 名稱。
- *eq* 指定等於運算符。
- *FALSE* 是「由工作主動監視」欄位的列舉值。

範例 5：搜尋將資料複製到外部帳戶的值區

此範例使用 describe- bucket 命令來查詢目前值區中的中繼資料， AWS 區域 並設定為將物件複製到不屬於您組織 AWS 帳戶 的值區。

若為 Linux、macOS 或 Unix：

```
$ aws macie2 describe-buckets --criteria '{"replicationDetails.replicatedExternally":
{"eq":["true"]}}'
```

對於 Microsoft 視窗：

```
C:\> aws macie2 describe-buckets --
criteria={\"replicationDetails.replicatedExternally\":{\"eq\":[\"true\"]}}
```

其中：

- *################ [##*複寫] 欄位的 JSON 名稱。
- *eq* 指定等於運算符。
- *true* 指定「外部複製」欄位的布林值。

範例 6：根據多重條件搜尋時段

此範例使用 describe-bucket 命令來查詢目前值區中 AWS 區域 且符合下列準則的中繼資料：根據權限設定的組合可公開存取；儲存未加密的物件；而且不會與任何定期性敏感資料探索工作相關聯。

對於 Linux、macOS 或 Unix，請使用反斜線 (\) 行接續字元來提高可讀性：

```
$ aws macie2 describe-buckets \
--criteria '{"publicAccess.effectivePermission":{"eq":
["PUBLIC"]},"objectCountByEncryptionType.unencrypted":
{"gte":1},"jobDetails.isMonitoredByJob":{"eq":["FALSE"]}}'
```

對於 Microsoft Windows，使用脫字符號（^）行繼續字符來提高可讀性：

```
C:\> aws macie2 describe-buckets ^
--criteria={\"publicAccess.effectivePermission\":{\"eq\":
[\"PUBLIC\"]},\"objectCountByEncryptionType.unencrypted\":{\"gte\":1},
\"jobDetails.isMonitoredByJob\":{\"eq\":[\"FALSE\"]}}
```

其中：

- *####. ####### [#####]* 欄位的 JSON 名稱，以及：
  - *eq* 指定等於運算符。
  - *PUB* LIC 是 [有效權限] 欄位的列舉值。
- *objectCountByEncryptionType###*指定 [無加密] 欄位的 JSON 名稱，並且：
  - *gte* 指定大於或等於運算符。
  - *1* 是「無加密」欄位中包含相對數值範圍內的最低值。
- *####### isMonitoredBy#Job*」指定「由工作主動監視」欄位的 JSON 名稱，以及：
  - *eq* 指定等於運算符。
  - *FALSE* 是「由工作主動監視」欄位的列舉值。

允許 Amazon Macie 訪問 S3 存儲桶和對象

當您為您啟用 Amazon Macie 時 AWS 帳戶，Macie 會創建一個服務鏈接角色，該角色授予 Macie 代表您調用 Amazon Simple Storage Service (Amazon S3) 和其他 AWS 服務 所需的許可。服務連結角色可簡化設定程序， AWS 服務 因為您不需要手動新增服務的權限，即可代表您完成動作。若要深入瞭解此類型的角色，請參閱使用AWS Identity and Access Management 者指南中的使用服務連結角色。

Macie 服務連結角色 (AWSServiceRoleForAmazonMacie) 的許可政策允許 Macie 執行動作，其中包括擷取 S3 儲存貯體和物件的相關資訊，以及從值區擷取物件。如果您是組織的 Macie 系統管理員，此原則也會允許 Macie 代表您針對組織中的成員帳戶執行這些動作。

Macie 會使用這些權限來執行下列工作：

- 產生並維護 S3 一般用途儲存貯體的庫存
- 提供值區中值區和物件的統計資料和其他資料
- 監控和評估存儲桶的安全性和訪問控制
- 分析值區中的物件以偵測敏感資料

在大多數情況下，Macie 具有執行這些任務所需的權限。但是，如果 S3 儲存貯體有限制性的儲存貯體政策，則該政策可能會阻止 Macie 執行部分或全部工作。

儲存貯體政策是以資源為基礎的 AWS Identity and Access Management (IAM) 政策，可指定主體 (使用者、帳戶、服務或其他實體) 可在 S3 儲存貯體上執行的動作，以及主體可以執行這些動作的條件。動作和條件可套用至值區層級作業，例如擷取值區的相關資訊，以及物件層級作業 (例如從值區擷取物件)。

儲存貯體政策通常會使用明確或Deny陳述式和條件來授予Allow或限制存取權。例如，值區政策可能包含拒絕存取值區的Allow或Deny陳述式，除非使用特定來源 IP 地址、Amazon Virtual Private Cloud 端 (Amazon VPC) 端點或 VPC 來存取儲存貯體。如需使用儲存貯體政策授予或限制儲存貯體存取權的詳細資訊，請參閱 Amazon 簡單儲存服務使用者指南中的儲存貯體政策和使用者政策以及 Amazon S3 如何授權請求。

如果值區政策使用明確Allow陳述式，政策不會阻止 Macie 擷取值區和值區物件的相關資訊，或從值區擷取物件。這是因為 Macie 服務連結角色的權限原則中的Allow陳述式會授與這些權限。

不過，如果值區政策使用具有一或多個條件的明確Deny陳述式，Macie 可能無法擷取值區或值區物件的相關資訊，或擷取值區的物件。例如，如果值區政策明確拒絕來自特定 IP 位址以外的所有來源的存

取，當您執行敏感資料探索工作時，Macie 就不會被允許分析值區的物件。這是因為限制性值區政策優先於 Macie 服務連`Allow`結角色的權限原則中的陳述式。

若要允許 Macie 存取具有限制性儲存貯體政策的 S3 儲存貯體，您可以將 Macie 服務連結角色 (`AWSServiceRoleForAmazonMacie`) 的條件新增至儲存貯體政策。此條件可以排除 Macie 服務連結角色，使其不符合原則中的`Deny`限制。它可以使用 Macie 服務連結角色的`aws:PrincipalArn`全域條件內容金鑰和 Amazon 資源名稱 (ARN) 來執行此操作。

下列程序會引導您完成此程序，並提供範例。

若要將 Macie 服務連結角色新增至值區政策

1. 登入 AWS Management Console 並開啟 Amazon S3 主控台，網址為 https://console.aws.amazon.com/s3/。
2. 在導覽窗格中，選擇 儲存貯體。
3. 選擇您要允許 Macie 存取的 S3 儲存貯體。
4. 在 Permissions (許可) 索引標籤上，Bucket policy (儲存貯體政策) 下，選擇 Edit (編輯)。
5. 在值區政策編輯器中，識別限制存取權的每個`Deny`陳述式，並防止 Macie 存取值區或值區的物件。
6. 在每個`Deny`陳述式中，新增使用`aws:PrincipalArn`全域條件內容索引鍵的條件，並為您的. AWS 帳戶

   條件金鑰的值應該是`arn:aws:iam::`*`123456789012`*`:role/aws-service-role/macie.amazonaws.com/AWSServiceRoleForAmazonMacie`，其中 *`123456789012`* 是您的帳戶識別碼。 AWS 帳戶

將此新增至值區政策的位置取決於原則目前包含的結構、元素和條件。若要了解支援的結構和元素，請參閱 Amazon 簡單儲存服務使用者指南中的 Amazon S3 中的政策和許可。

以下是儲存貯體政策的範例，該政策使用明確的`Deny`陳述式限制存取名為 DOC/EXAMPLE- BUCKET 的 S3 儲存貯體。使用目前的政策，只能從 ID 為`vpce-1a2b3c4d`的 VPC 端點存取儲存貯體。拒絕來自所有其他 VPC 端點的存取，包括來自 AWS Management Console 和 Macie 的存取。

```
{
   "Version": "2012-10-17",
   "Id": "Policy1415115example",
   "Statement": [
      {
```

```
         "Sid": "Access from specific VPCE only",
         "Effect": "Deny",
         "Principal": "*",
         "Action": "s3:*",
         "Resource": [
            "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
            "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
         ],
         "Condition": {
            "StringNotEquals": {
               "aws:SourceVpce": "vpce-1a2b3c4d"
            }
         }
      }
   ]
}
```

若要變更此政策並允許 Macie 存取 S3 儲存貯體和儲存貯體的物件，我們可以新增使用條件運算子和aws:PrincipalArn全域StringNotLike條件內容索引鍵的條件。此額外條件會將 Macie 服務連結角色排除在符合限制之Deny外。

```
{
   "Version": "2012-10-17",
   "Id":" Policy1415115example ",
   "Statement": [
      {
         "Sid": "Access from specific VPCE and Macie only",
         "Effect": "Deny",
         "Principal": "*",
         "Action": "s3:*",
         "Resource": [
            "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
            "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
         ],
         "Condition": {
            "StringNotEquals": {
               "aws:SourceVpce": "vpce-1a2b3c4d"
            },
            "StringNotLike": {
               "aws:PrincipalArn": "arn:aws:iam::123456789012:role/aws-service-role/
macie.amazonaws.com/AWSServiceRoleForAmazonMacie"
            }
         }
```

```
      }
   ]
}
```

在上述範例中，StringNotLike條件運算子會使用aws:PrincipalArn條件內容索引鍵來指定 Macie 服務連結角色的 ARN，其中：

- 123456789012是允許使用 Macie 擷取值區和值區物件的相關資訊，以及從值區擷取物件的帳戶 ID。 AWS 帳戶
- macie.amazonaws.com是 Macie 服務主體的識別碼。
- AWSServiceRoleForAmazonMacie是 Macie 服務連結角色的名稱。

我們使用StringNotLike運算子，因為原則已經使用StringNotEquals運算子。政策只能使用一次StringNotEquals運算子。

如需管理 Amazon S3 資源存取權的其他政策範例和詳細資訊，請參閱 Amazon 簡單儲存服務使用者指南中的 Amazon S3 中的身分和存取管理。

使用 Amazon Macie 探索敏感資料

使用 Amazon Macie，您可以自動探索、記錄和報告 Amazon Simple Storage Service (Amazon S3) 資料資產中的敏感資料。您可以透過兩種方式執行此操作：將 Macie 設定為執行自動化敏感資料探索，以及建立和執行敏感資料探索工作。

自動化敏感資料探索

自動化敏感資料探索可讓您廣泛掌握敏感資料在 Amazon S3 資料資產中的位置。使用此選項，Macie 會每天評估您的 S3 儲存貯體庫存，並使用取樣技術從儲存貯體中識別和選取具代表性的 S3 物件。然後，Macie 會擷取並分析選取的物件，檢查它們是否有敏感資料。如需詳細資訊，請參閱 執行自動化敏感資料探索。

敏感性資料探索工作

敏感資料探索工作提供更深入、更具針對性的分析。使用此選項，您可以定義分析的廣度和深度 — 您選取的特定 S3 儲存貯體或符合特定準則的儲存貯體。您也可以選擇選項 (例如從 S3 物件屬性衍生的自訂準則) 來縮小分析範圍。此外，您可以將工作設定為僅執行一次以進行隨選分析和評估，或定期分析、評估和監視定期執行一次。如需詳細資訊，請參閱 執行敏感資料探索任務。

透過自動化敏感資料探索或敏感資料探索任務，您可以使用 Macie 提供的受管資料識別碼、您定義的自訂資料識別碼或兩者的組合來分析 S3 物件。您也可以使用允許清單來微調分析。

受管資料識別碼

受管理資料識別碼是內建的準則和技術，用來偵測特定類型的敏感資料，例如特定國家或地區的信用卡號碼、 AWS 秘密存取金鑰或護照號碼。他們可以偵測許多國家和地區的大量敏感資料類型清單，包括多種類型的憑證資料、財務資訊和個人識別資訊 (PII)。如需詳細資訊，請參閱 使用受管資料識別符。

自訂資料識別碼

自訂資料識別碼定義偵測敏感資料的自訂準則。每個自訂資料識別碼都會指定一個規則運算式 (regex)，該運算式會定義要比對的文字模式，以及可選擇性的字元序列和細化結果的鄰近規則。您可以使用它們來偵測反映您特定案例、智慧財產或專屬資料的敏感資料，例如員工 ID、客戶帳號或內部資料分類。如需詳細資訊，請參閱 建置自訂資料識別符。

允許清單

在 Macie 中，允許清單指定 S3 物件中要忽略的文字和文字模式，通常是針對特定案例或環境的敏感資料例外狀況，例如組織的公用名稱或電話號碼，或組織用於測試的範例資料。如果 Macie 在允

許清單中找到符合項目或模式的文字，Macie 也不會報告該文字出現的情況，即使該文字符合受管理資料識別碼或自訂資料識別碼的準則。如需詳細資訊，請參閱 使用允許清單定義敏感資料例外。

當 Macie 分析 S3 物件時，Macie 會從 Amazon S3 擷取物件的最新版本，然後檢查物件的內容是否有敏感資料。如果符合以下條件，Macie 可以分析物件：

- 物件使用支援的檔案或儲存格式，並使用支援的儲存類別存放在 S3 一般用途儲存貯體中。如需詳細資訊，請參閱 支援的儲存類別和格式。
- 如果物件已加密，則會使用 Macie 可存取且允許使用的金鑰加密物件。如需詳細資訊，請參閱 分析加密的 S3 物件。
- 如果物件儲存在具有限制性值區政策的值區中，則此政策允許 Macie 存取值區中的物件。如需詳細資訊，請參閱 允許 Macie 存取 S3 儲存貯體和物件。

為了協助您符合資料安全性和隱私權要求，Macie 會產生所找到的敏感資料及其執行的分析記錄，包括敏感資料發現和敏感資料探索結果。敏感資料發現是 Macie 在 S3 物件中找到的敏感資料的詳細報告。敏感資料探索結果是記錄物件分析之相關詳細資料的報告。每種類型的記錄都遵循標準化的結構描述，可協助您視需要使用其他應用程式、服務和系統來查詢、監視和處理這些記錄。

> **Tip**
>
> 雖然 Macie 已針對 Amazon S3 進行了最佳化，但您可以使用它來探索目前存放在其他地方的資源中的敏感資料。您可以暫時或永久地將資料移至 Amazon S3 來執行此操作。例如，將 Amazon Relational Database Service 服務或 Amazon Aurora 快照以 Apache 實木複合格式匯出到 Amazon S3。或將亞馬遜動態資料表匯出至 Amazon S3。然後，您可以建立任務來分析 Amazon S3 中的資料。

主題

- 在亞馬遜 Macie 中使用受管資料識別碼
- 在亞馬遜 Macie 中構建自定義數據標識符
- 使用 Amazon Macie 允許清單定義敏感資料例外
- 使用 Amazon Macie 執行自動化敏感資料探索
- 在 Amazon Macie 中執行敏感性資料探索任務
- 使用亞馬遜 Macie 分析加密的 Amazon S3 對象
- 使用 Amazon Macie 儲存和保留敏感資料探索結果

- Amazon Macie 支援的儲存類別和格式

在亞馬遜 Macie 中使用受管資料識別碼

Amazon Macie 使用各種標準和技術 (包括機器學習和模式比對) 來偵測 Amazon 簡單儲存服務 (Amazon S3) 物件中的敏感資料。這些標準和技術，統稱為受管資料識別碼，可偵測許多國家和地區不斷增加的敏感資料類型清單，包括多種類型的憑證資料、財務資訊、個人健康資訊 (PHI) 和個人識別資訊 (PII)。每個受管理的資料識別碼都是為了偵測特定類型的敏感資料而設計，例如：AWS特定國家或地區的秘密存取金鑰、信用卡號碼或護照號碼。

Macie 可以使用託管數據標識符來檢測以下類別的敏感數據：

- 認證，用於認證資料，例如私密金鑰和AWS秘密存取金鑰。
- 財務資訊，用於財務資料，例如信用卡號碼和銀行帳號。
- PHI 的個人資訊，例如健康保險和醫療識別號碼，以及 PII，例如駕駛執照識別號碼和護照號碼。

在每個類別中，Macie 可以檢測多種類型的敏感數據。本節中的主題列出並說明每種類型以及偵測它的任何相關需求。對於每種類型，它們也會指出專為偵測資料而設計之受管理資料識別符的唯一識別符 (ID)。當你建立敏感資料探索工作或者設定自動化敏感資料探索設定，您可以使用這些 ID 來指定要 Macie 在分析 S3 物件時使用的受管資料識別碼。

如需我們針對工作建議的受管資料識別碼清單，請參閱建議用於敏感資料探索工作的受管資料識別。如需我們建議並預設用於自動化敏感資料探索的受管資料識別碼清單，請參閱自動化敏感資料探索的預設設定。

主題

- Amazon Macie 受管資料識別碼的關鍵字需求
- 快速參考：Amazon Macie 受管資料識別碼
- 詳細參考資料：Amazon Macie 受管資料識別碼

Amazon Macie 受管資料識別碼的關鍵字需求

若要使用受管資料識別碼偵測特定類型的敏感資料，Amazon Macie 要求在資料附近使用關鍵字。如果特定類型的資料是這種情況，本節的後續主題會指出該資料的關鍵字需求。

如果關鍵字必須與特定類型的資料相鄰，則關鍵字通常必須在 30 個字元以內 (包含在內) 資料。其他鄰近要求會根據 Amazon 簡單儲存服務 (Amazon S3) 物件的檔案類型或儲存格式而有所不同。

結構化的單欄式資料

對於單欄資料，關鍵字必須是相同值的一部分，或是儲存值的欄或欄位名稱。這是適用於微軟 Excel 工作簿，CSV 文件和 TSV 文件。

例如，如果欄位的值同時包含兩者SSN以及使用美國社會安全號碼（SSN）語法的九位數字，Macie 可以檢測字段中的 SSN。同樣，如果列的名稱包含SSN，Macie 可以偵測資料行中的每個 SSN。Macie 將該列中的值視為靠近關鍵字SSN。

結構化、以記錄為基礎的資料

對於基於記錄的數據，關鍵字必須是相同值的一部分，或者在存儲值的字段或數組的路徑中的元素名稱。這是阿帕奇阿夫羅對象容器，阿帕奇實木複合地板文件，JSON 文件和 JSON 行文件是如此。

例如，如果欄位的值同時包含兩者證書和使用的語法的字符序列AWS密鑰訪問密鑰，Macie 可以在現場檢測密鑰。同樣，如果字段的路徑是`$.credentials.aws.key`，馬西可以檢測到AWS該字段中的秘密訪問密鑰。Macie 將字段中的值視為靠近關鍵字證書。

非結構化資料

Adobe 可移植文檔格式文件，微軟 Word 文檔，電子郵件消息和非二進制文本文件除 CSV，JSON 行和 TSV 文件以外沒有任何其他鄰近要求。關鍵字通常必須在資料的 30 個字元內 (包含在內)。這包括這些類型檔案中的任何結構化資料，例如資料表。

關鍵字不區分大小寫。此外，如果關鍵字包含空格，Macie 會自動比對不包含空格或包含底線 (_) 或連字號 (-) 而非空格的關鍵字變體。在某些情況下，Macie 也會展開或縮寫關鍵字，以解決關鍵字的常見變化。

如需關鍵字如何提供上下文並協助 Macie 偵測特定類型敏感資料的示範，請觀看下列影片：亞馬遜 Macie 如何使用關鍵字發現敏感數據。

快速參考：Amazon Macie 受管資料識別碼

在 Amazon Macie 中，受管資料識別碼是一組內建準則和技術，用來偵測特定類型的敏感資料，例如特定國家或地區的信用卡號碼、 AWS 秘密存取金鑰或護照號碼。這些識別碼可偵測許多國家和地區不斷增加的敏感資料類型清單，包括多種類型的憑證資料、財務資訊、個人健康資訊 (PHI) 和個人識別資訊 (PII)。

下表列出 Macie 目前提供的所有受管理資料識別碼，並依機密資料類型進行組織。它會針對每種類型提供下列資訊：

- 敏感資料類別 — 指定敏感資料的一般類別，包括以下類型：身份證明資料 (例如私密金鑰)；財務資訊 (例如信用卡號碼和銀行帳戶號碼)；個人資訊：個人健康資訊 (例如健康保險和醫療識別號碼) 的 PHI；以及個人資訊：個人識別資訊 (例如駕駛執照識別號碼) 的 PII護照號碼。
- 受管理的資料識別碼 ID — 為設計用來偵測資料的一或多個受管理資料識別碼指定唯一識別碼 (ID)。當您建立敏感資料探索工作或設定自動化敏感資料探索設定時，您可以使用這些 ID 來指定您希望 Macie 在分析資料時使用的受管理資料識別碼。如需我們針對工作建議的受管資料識別碼清單，請參閱建議用於敏感資料探索工作的受管資料識別。如需我們建議用於自動化敏感資料探索的受管資料識別碼清單，請參閱自動化敏感資料探索的預設設定。
- 需要關鍵字 — 指定偵測是否需要關鍵字與資料相鄰。如需 Macie 在分析資料時如何使用關鍵字的詳細資訊，請參閱關鍵字要求。
- 國家和地區 — 指定適用的受管資料識別碼所設計的國家或地區。如果受管資料識別碼並非針對特定國家或地區設計，則此值為 A ny。

若要檢閱特定敏感資料類型之受管理資料識別碼的其他詳細資訊，請選擇類型。

敏感資料類型	敏感資料類別	受管資料識別符 ID	必要的關鍵字	國家和地區
AWS 私密存取金鑰	登入資料	AWS_CREDENTIALS	是	任何
銀行帳戶號碼	財務資訊	BANK_ACCOUNT_NUMBER（適用於加拿大和美國）	是	加拿大、美國
基本銀行帳戶號碼	財務資訊	取決於國家或地區： FRANCE_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, ITALY_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER	是	法國、德國、義大利、西班牙、英國
出生日期	個人資料：個人資料	DATE_OF_BIRTH	是	任何

敏感資料類型	敏感資料類別	受管資料識別符 ID	必要的關鍵字	國家和地區
信用卡到期日	財務資訊	CREDIT_CARD_EXPIRATION	是	任何
信用卡磁條數據	財務資訊	CREDIT_CARD_MAGNETIC_STRIPE	是	任何
信用卡號碼	財務資訊	CREDIT_CARD_NUMBER(適用於鄰近關鍵字的信用卡號碼)、CREDIT_CARD_NUMBER_(NO_KEYWORD) (適用於不在關鍵字附近的信用卡號碼)	各有不同	任何
信用卡驗證碼	財務資訊	CREDIT_CARD_SECURITY_CODE	是	任何

敏感資料類型	敏感資料類別	受管資料識別符 ID	必要的關鍵字	國家和地區
駕照識別號碼	個人資料：個人資料	取決於國家或地區： AUSTRALIA_DRIVERS_LICENSE, AUSTRIA_DRIVERS_LICENSE, BELGIUM_DRIVERS_LICENSE, BULGARIA_DRIVERS_LICENSE, CANADA_DRIVERS_LICENSE, CROATIA_DRIVERS_LICENSE, CYPRUS_DRIVERS_LICENSE, CZECHIA_DRIVERS_LICENSE, DENMARK_DRIVERS_LICENSE, DRIVERS_LICENSE (for the US), ESTONIA_DRIVERS_LICENSE, FINLAND_DRIVERS_LICENSE, FRANCE_DRIVERS_LICENSE, GERMANY_DRIVERS_LICENSE, GREECE_DRIVERS_LICENSE, HUNGARY_DRIVERS_LICENSE, INDIA_DRIVERS_LICENSE, IRELAND_DRIVERS_LICENSE, ITALY_DRIVERS_LICENSE, LATVIA_DRIVERS_LICENSE, LITHUANIA_DRIVERS_LICENSE, LUXEMBOURG_DRIVERS_LICENSE, MALTA_DRIVERS_LICENSE, NETHERLANDS_DRIVERS_LICENSE, POLAND_DRIVERS_LICENSE, PORTUGAL_DRIVERS_LICENSE, ROMANIA_DRIVERS_LICENSE, SLOVAKIA_DRIVERS_LICENSE, SLOVENIA_DRIVERS_LICENSE, SPAIN_DRIVERS_LICE	是	澳大利亞，奧地利，比利時，保加利亞，加拿大，克羅地亞，塞浦路斯，捷克共和國，丹麥，愛沙尼亞，芬蘭，法國，德國，希臘，匈牙利，印度，愛爾蘭，意大利，拉脫維亞，立陶宛，盧森堡，馬耳他，荷蘭，波蘭，葡萄牙，羅馬尼亞，斯洛伐克，斯洛文尼亞，西班牙，瑞典，英國，美國

敏感資料類型	敏感資料類別	受管資料識別符 ID	必要的關鍵字	國家和地區
		NSE, SWEDEN_DRIVERS_LICENSE, UK_DRIVERS_LICENSE		
毒品執法局 (DEA) 註冊號碼	個人資料：PHI	US_DRUG_ENFORCEMENT_AGENCY_NUMBER	是	美國
選民名冊號碼	個人資料：個人資料	UK_ELECTORAL_ROLL_NUMBER	是	英國
全名	個人資料：個人資料	NAME	否	任何，如果名稱使用拉丁字元集
全球定位系統 (GPS) 座標	個人資料：個人資料	LATITUDE_LONGITUDE	是	任何，如果坐標靠近英文關鍵字
谷歌雲 API 密鑰	登入資料	GCP_API_KEY	是	任何
Health 保險索償編號	個人資料：PHI	USA_HEALTH_INSURANCE_CLAIM_NUMBER	是	美國
健康保險或醫療識別號碼	個人資料：PHI	取決於國家或地區： CANADA_HEALTH_NUMBER, EUROPEAN_HEALTH_INSURANCE_CARD_NUMBER, FINLAND_EUROPEAN_HEALTH_INSURANCE_NUMBER, FRANCE_HEALTH_INSURANCE_NUMBER, UK_NHS_NUMBER, USA_MEDICARE_BENEFICIARY_IDENTIFIER	是	加拿大、歐盟、芬蘭、法國、英國、美國

敏感資料類型	敏感資料類別	受管資料識別符 ID	必要的關鍵字	國家和地區
醫療保健通用程序編碼系統 (HCPCS) 代碼	個人資料：PHI	USA_HEALTHCARE_PROCEDURE_CODE	是	美國
HTTP 基本授權標頭	登入資料	HTTP_BASIC_AUTH_HEADER	否	任何
餅乾	個人資料：個人資料	HTTP_COOKIE	否	任何

敏感資料類型	敏感資料類別	受管資料識別符 ID	必要的關鍵字	國家和地區
國際銀行帳戶號碼	財務資訊	取決於國家或地區： ALBANIA_BANK_ACCOUNT_NUMBER, ANDORRA_BANK_ACCOUNT_NUMBER, BOSNIA_AND_HERZEGOVINA_BANK_ACCOUNT_NUMBER, BRAZIL_BANK_ACCOUNT_NUMBER, BULGARIA_BANK_ACCOUNT_NUMBER, COSTA_RICA_BANK_ACCOUNT_NUMBER, CROATIA_BANK_ACCOUNT_NUMBER, CYPRUS_BANK_ACCOUNT_NUMBER, CZECH_REPUBLIC_BANK_ACCOUNT_NUMBER, DENMARK_BANK_ACCOUNT_NUMBER, DOMINICAN_REPUBLIC_BANK_ACCOUNT_NUMBER, EGYPT_BANK_ACCOUNT_NUMBER, ESTONIA_BANK_ACCOUNT_NUMBER, FAROE_ISLANDS_BANK_ACCOUNT_NUMBER, FINLAND_BANK_ACCOUNT_NUMBER, FRANCE_BANK_ACCOUNT_NUMBER, GEORGIA_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, GREECE_BANK_ACCOUNT_NUMBER, GREENLAND_BANK_ACCOUNT_NUMBER, HUNGARY_BANK_ACCOUNT_NUMBER, ICELAND_BANK_ACCOUNT_NUMBER, IRELAND_BANK_ACCOUNT_NUMBER, ITALY_BANK_ACCOUNT_NUMBER,	否	阿爾巴尼亞、安道爾、波斯尼亞和黑塞哥維那、巴西、保加利亞、哥斯達黎加、克羅地亞、塞浦路斯、捷克共和國、丹麥、多明尼加共和國、埃及、愛爾蘭、埃及、愛爾蘭、埃及、立陶宛、馬耳他、毛里塔尼亞、毛里塔尼亞、毛里塔尼亞、匈牙利、冰島、愛爾蘭、意大利、約旦、科索沃、列支敦士登、立陶宛、馬耳他、毛里塔尼亞、毛里塔尼亞、毛里塔尼

敏感資料類型	敏感資料類別	受管資料識別符 ID	必要的關鍵字	國家和地區
		JORDAN_BANK_ACCOUNT_NUMBER, KOSOVO_BANK_ACCOUNT_NUMBER, LIECHTENSTEIN_BANK_ACCOUNT_NUMBER, LITHUANIA_BANK_ACCOUNT_NUMBER, MALTA_BANK_ACCOUNT_NUMBER, MAURITANIA_BANK_ACCOUNT_NUMBER, MAURITIUS_BANK_ACCOUNT_NUMBER, MONACO_BANK_ACCOUNT_NUMBER, MONTENEGRO_BANK_ACCOUNT_NUMBER, NETHERLANDS_BANK_ACCOUNT_NUMBER, NORTH_MACEDONIA_BANK_ACCOUNT_NUMBER, POLAND_BANK_ACCOUNT_NUMBER, PORTUGAL_BANK_ACCOUNT_NUMBER, SAN_MARINO_BANK_ACCOUNT_NUMBER, SENEGAL_BANK_ACCOUNT_NUMBER, SERBIA_BANK_ACCOUNT_NUMBER, SLOVAKIA_BANK_ACCOUNT_NUMBER, SLOVENIA_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, SWEDEN_BANK_ACCOUNT_NUMBER, SWITZERLAND_BANK_ACCOUNT_NUMBER, TIMOR_LESTE_BANK_ACCOUNT_NUMBER, TUNISIA_BANK_ACCOUNT_NUMBER, TURKIYE_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER, UKRAINE_BANK_ACCOUNT_NUMBER, UNITED_ARAB_EMIRAT		亞、摩納哥、匈牙利、冰島、愛爾蘭、意大利、約旦、科索沃、列支敦士登、, 斯洛文尼亞, 西班牙, 瑞典, 瑞士, 東帝汶, 突尼斯, 土耳其, 英國, 烏克蘭, 阿拉伯聯合酋長國, 英屬維爾京群島

敏感資料類型	敏感資料類別	受管資料識別符 ID	必要的關鍵字	國家和地區
		ES_BANK_ACCOUNT_NUMBER, VIRGIN_ISLANDS_BANK_ACCOUNT_NUMBER（適用於英屬維爾京群島）		
網絡令牌	登入資料	JSON_WEB_TOKEN	否	任何
郵寄地址	個人資料：個人資料	ADDRESS，BRAZIL_CEP_CODE（巴西郵政編碼）	各有不同	澳大利亞，巴西，加拿大，法國，德國，意大利，西班牙，英國，美國
美国国家药品法典	個人資料：PHI	USA_NATIONAL_DRUG_CODE	是	美國
國家身分證號碼	個人資料：個人資料	取決於國家或地區： BRAZIL_RG_NUMBER, FRANCE_NATIONAL_IDENTIFICATION_NUMBER, GERMANY_NATIONAL_IDENTIFICATION_NUMBER, INDIA_AADHAAR_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_DNI_NUMBER	是	巴西，法國，德國，印度，意大利，西班牙
國民保險號碼 (NINO)	個人資料：個人資料	UK_NATIONAL_INSURANCE_NUMBER	是	英國
國家供應商識別碼 (NPI)	個人資料：PHI	USA_NATIONAL_PROVIDER_IDENTIFIER	是	美國
OpenSSH 私密金鑰	登入資料	OPENSSH_PRIVATE_KEY	否	任何

敏感資料類型	敏感資料類別	受管資料識別符 ID	必要的關鍵字	國家和地區
護照號碼	個人資料：個人資料	取決於國家或地區： CANADA_PASSPORT_NUMBER, FRANCE_PASSPORT_NUMBER, GERMANY_PASSPORT_NUMBER, ITALY_PASSPORT_NUMBER, SPAIN_PASSPORT_NUMBER, UK_PASSPORT_NUMBER, USA_PASSPORT_NUMBER	是	加拿大、法國、德國、義大利、西班牙、英國、美國
永久居留號碼	個人資料：個人資料	CANADA_NATIONAL_IDENTIFICATION_NUMBER	是	加拿大
PGP 私密金鑰	登入資料	PGP_PRIVATE_KEY	否	任何
電話號碼	個人資料：個人資料	取決於國家或地區： BRAZIL_PHONE_NUMBER, FRANCE_PHONE_NUMBER, GERMANY_PHONE_NUMBER, ITALY_PHONE_NUMBER, PHONE_NUMBER (for Canada and the US), SPAIN_PHONE_NUMBER, UK_PHONE_NUMBER	各有不同	巴西、加拿大、法國、德國、義大利、西班牙、英國、美國
公開金鑰加密標準 (PKCS) 私密金鑰	登入資料	PKCS	否	任何
PuTTY 私密金鑰	登入資料	PUTTY_PRIVATE_KEY	否	任何
社會保險號碼 (SIN)	個人資料：個人資料	CANADA_SOCIAL_INSURANCE_NUMBER	是	加拿大

敏感資料類型	敏感資料類別	受管資料識別符 ID	必要的關鍵字	國家和地區
社會安全號碼 (SSN)	個人資料：個人資料	視乎國家或地區而定：SPAIN_SOCIAL_SECURITY_NUMBERUSA_SOCIAL_SECURITY_NUMBER	是	西班牙、美國
the section called “條紋 API 金鑰”	登入資料	STRIPE_CREDENTIALS	否	任何
納稅識別號碼或參考號碼	個人資料：個人資料	取決於國家或地區： AUSTRALIA_TAX_FILE_NUMBER, BRAZIL_CNPJ_NUMBER, BRAZIL_CPF_NUMBER, FRANCE_TAX_IDENTIFICATION_NUMBER, GERMANY_TAX_IDENTIFICATION_NUMBER, INDIA_PERMANENT_ACCOUNT_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_NIE_NUMBER, SPAIN_NIF_NUMBER, SPAIN_TAX_IDENTIFICATION_NUMBER, UK_TAX_IDENTIFICATION_NUMBER, USA_INDIVIDUAL_TAX_IDENTIFICATION_NUMBER	是	澳大利亞，巴西，法國，德國，印度，意大利，西班牙，英國，美國
唯一裝置識別碼 (UDI)	個人資料：PHI	MEDICAL_DEVICE_UDI	是	美國

敏感資料類型	敏感資料類別	受管資料識別符 ID	必要的關鍵字	國家和地區
車輛識別號碼 (VIN)	個人資料：個人資料	VEHICLE_IDENTIFICATION_NUMBER	是	任何，如果 VIN 接近以下其中一種語言的關鍵字：英語，法語，德語，立陶宛語，波蘭語，葡萄牙語，羅馬尼亞語或西班牙語

詳細參考資料：Amazon Macie 受管資料識別碼

在 Amazon Macie 中，受管資料識別碼是專為偵測特定類型敏感資料而設計的內建準則和技術。他們可以偵測許多國家和地區的大量敏感資料類型清單，包括多種類型的憑證資料、財務資訊和個人資訊。每個受管資料識別碼都是設計來偵測特定類型的敏感資料，例如特定國家或地區的 AWS 秘密存取金鑰、信用卡號碼或護照號碼。

Macie 可以使用受管理的資料識別碼來偵測多種類別的敏感資料。在每個類別中，Macie 可以檢測多種類型的敏感數據。本節中的主題列出並說明每種類型以及偵測資料的任何相關需求。如需有關特定敏感資料類型之受管理資料識別碼的詳細資訊，您可以依類別瀏覽主題：

- 認證 — 用於認證資料，例如私密金鑰和 AWS 秘密存取金鑰。
- 財務資訊 — 適用於財務資料，例如信用卡號碼和銀行帳號。
- 個人信息：PHI — 用於個人健康信息（PHI），例如健康保險和醫療識別號碼。
- 個人資訊：PII — 用於個人識別資訊 (PII)，例如駕駛執照識別號碼和護照號碼。

或者，您可以從下表中選擇特定類型的敏感數據。此表格會列出 Macie 目前提供的所有受管理資料識別碼，並依機密資料類型進行組織。此表也會摘要說明偵測每種類型的相關需求。

敏感資料類型	敏感資料類別	受管資料識別符 ID	必要的關鍵字	國家和地區
AWS 私密存取金鑰	登入資料	AWS_CREDENTIALS	是	任何
銀行帳戶號碼	財務資訊	BANK_ACCOUNT_NUMBER（適用於加拿大和美國）	是	加拿大、美國
基本銀行帳戶號碼	財務資訊	取決於國家或地區： FRANCE_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, ITALY_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER	是	法國、德國、義大利、西班牙、英國
出生日期	個人資料：個人資料	DATE_OF_BIRTH	是	任何
信用卡到期日	財務資訊	CREDIT_CARD_EXPIRATION	是	任何
信用卡磁條數據	財務資訊	CREDIT_CARD_MAGNETIC_STRIPE	是	任何
信用卡號碼	財務資訊	CREDIT_CARD_NUMBER(適用於鄰近關鍵字的信用卡號碼)、CREDIT_CARD_NUMBER_(NO_KEYWORD) (適用於不在關鍵字附近的信用卡號碼)	各有不同	任何
信用卡驗證碼	財務資訊	CREDIT_CARD_SECURITY_CODE	是	任何
駕照識別號碼	個人資料：個人資料	取決於國家或地區： AUSTRALIA_DRIVERS_LICENSE, AUSTRIA_DRIVERS_LICENSE,	是	澳大利亞，奧地利，比利時，保加利亞，加

敏感資料類型	敏感資料類別	受管資料識別符 ID	必要的關鍵字	國家和地區
		BELGIUM_DRIVERS_LICENSE, BULGARIA_DRIVERS_LICENSE, CANADA_DRIVERS_LICENSE, CROATIA_DRIVERS_LICENSE, CYPRUS_DRIVERS_LICENSE, CZECHIA_DRIVERS_LICENSE, DENMARK_DRIVERS_LICENSE, DRIVERS_LICENSE (for the US), ESTONIA_DRIVERS_LICENSE, FINLAND_DRIVERS_LICENSE, FRANCE_DRIVERS_LICENSE, GERMANY_DRIVERS_LICENSE, GREECE_DRIVERS_LICENSE, HUNGARY_DRIVERS_LICENSE, INDIA_DRIVERS_LICENSE, IRELAND_DRIVERS_LICENSE, ITALY_DRIVERS_LICENSE, LATVIA_DRIVERS_LICENSE, LITHUANIA_DRIVERS_LICENSE, LUXEMBOURG_DRIVERS_LICENSE, MALTA_DRIVERS_LICENSE, NETHERLANDS_DRIVERS_LICENSE, POLAND_DRIVERS_LICENSE, PORTUGAL_DRIVERS_LICENSE, ROMANIA_DRIVERS_LICENSE, SLOVAKIA_DRIVERS_LICENSE, SLOVENIA_DRIVERS_LICENSE, SPAIN_DRIVERS_LICENSE, SWEDEN_DRIVERS_LICENSE, UK_DRIVERS_LICENSE		拿大，克羅地亞，塞浦路斯，捷克共和國，丹麥，愛沙尼亞，芬蘭，法國，德國，希臘，匈牙利，印度，愛爾蘭，意大利，拉脫維亞，立陶宛，盧森堡，馬耳他，荷蘭，波蘭，葡萄牙，羅馬尼亞，斯洛伐克，斯洛文尼亞，西班牙，瑞典，英國，美國
毒品執法局 (DEA) 註冊號碼	個人資料：PHI	US_DRUG_ENFORCEMENT_AGENCY_NUMBER	是	美國

敏感資料類型	敏感資料類別	受管資料識別符 ID	必要的關鍵字	國家和地區
選民名冊號碼	個人資料：個人資料	UK_ELECTORAL_ROLL_NUMBER	是	英國
全名	個人資料：個人資料	NAME	否	任何，如果名稱使用拉丁字元集
全球定位系統 (GPS) 座標	個人資料：個人資料	LATITUDE_LONGITUDE	是	任何，如果坐標靠近英文關鍵字
谷歌雲 API 密鑰	登入資料	GCP_API_KEY	是	任何
Health 保險索償編號	個人資料：PHI	USA_HEALTH_INSURANCE_CLAIM_NUMBER	是	美國
健康保險或醫療識別號碼	個人資料：PHI	取決於國家或地區： CANADA_HEALTH_NUMBER, EUROPEAN_HEALTH_INSURANCE_CARD_NUMBER, FINLAND_EUROPEAN_HEALTH_INSURANCE_NUMBER, FRANCE_HEALTH_INSURANCE_NUMBER, UK_NHS_NUMBER, USA_MEDICARE_BENEFICIARY_IDENTIFIER	是	加拿大、歐盟、芬蘭、法國、英國、美國
醫療保健通用程序編碼系統 (HCPCS) 代碼	個人資料：PHI	USA_HEALTHCARE_PROCEDURE_CODE	是	美國
HTTP 基本授權標頭	登入資料	HTTP_BASIC_AUTH_HEADER	否	任何

敏感資料類型	敏感資料類別	受管資料識別符 ID	必要的關鍵字	國家和地區
餅乾	個人資料：個人資料	HTTP_COOKIE	否	任何

敏感資料類型	敏感資料類別	受管資料識別符 ID	必要的關鍵字	國家和地區
國際銀行帳戶號碼	財務資訊	取決於國家或地區： ALBANIA_BANK_ACCOUNT_NUMBER, ANDORRA_BANK_ACCOUNT_NUMBER, BOSNIA_AND_HERZEGOVINA_BANK_ACCOUNT_NUMBER, BRAZIL_BANK_ACCOUNT_NUMBER, BULGARIA_BANK_ACCOUNT_NUMBER, COSTA_RICA_BANK_ACCOUNT_NUMBER, CROATIA_BANK_ACCOUNT_NUMBER, CYPRUS_BANK_ACCOUNT_NUMBER, CZECH_REPUBLIC_BANK_ACCOUNT_NUMBER, DENMARK_BANK_ACCOUNT_NUMBER, DOMINICAN_REPUBLIC_BANK_ACCOUNT_NUMBER, EGYPT_BANK_ACCOUNT_NUMBER, ESTONIA_BANK_ACCOUNT_NUMBER, FAROE_ISLANDS_BANK_ACCOUNT_NUMBER, FINLAND_BANK_ACCOUNT_NUMBER, FRANCE_BANK_ACCOUNT_NUMBER, GEORGIA_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, GREECE_BANK_ACCOUNT_NUMBER, GREENLAND_BANK_ACCOUNT_NUMBER, HUNGARY_BANK_ACCOUNT_NUMBER, ICELAND_BANK_ACCOUNT_NUMBER, IRELAND_BANK_ACCOUNT_NUMBER, ITALY_BANK_ACCOUNT_NUMBER,	否	阿爾巴尼亞、安道爾、波斯尼亞和黑塞哥維那、巴西、保加利亞、哥斯達黎加、克羅地亞、塞浦路斯、捷克共和國、丹麥、多明尼加共和國、埃及、愛爾蘭、埃及、愛爾蘭、埃及、立陶宛、馬耳他、毛里塔尼亞、毛里塔尼亞、毛里塔尼亞、匈牙利、冰島、愛爾蘭、意大利、約旦、科索沃、列支敦士登、立陶宛、馬耳他、毛里塔尼亞、毛里塔尼亞、毛里塔尼

敏感資料類型	敏感資料類別	受管資料識別符 ID	必要的關鍵字	國家和地區
		JORDAN_BANK_ACCOUNT_NUMBER, KOSOVO_BANK_ACCOUNT_NUMBER, LIECHTENSTEIN_BANK_ACCOUNT_NUMBER, LITHUANIA_BANK_ACCOUNT_NUMBER, MALTA_BANK_ACCOUNT_NUMBER, MAURITANIA_BANK_ACCOUNT_NUMBER, MAURITIUS_BANK_ACCOUNT_NUMBER, MONACO_BANK_ACCOUNT_NUMBER, MONTENEGRO_BANK_ACCOUNT_NUMBER, NETHERLANDS_BANK_ACCOUNT_NUMBER, NORTH_MACEDONIA_BANK_ACCOUNT_NUMBER, POLAND_BANK_ACCOUNT_NUMBER, PORTUGAL_BANK_ACCOUNT_NUMBER, SAN_MARINO_BANK_ACCOUNT_NUMBER, SENEGAL_BANK_ACCOUNT_NUMBER, SERBIA_BANK_ACCOUNT_NUMBER, SLOVAKIA_BANK_ACCOUNT_NUMBER, SLOVENIA_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, SWEDEN_BANK_ACCOUNT_NUMBER, SWITZERLAND_BANK_ACCOUNT_NUMBER, TIMOR_LESTE_BANK_ACCOUNT_NUMBER, TUNISIA_BANK_ACCOUNT_NUMBER, TURKIYE_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER, UKRAINE_BANK_ACCOUNT_NUMBER, UNITED_ARAB_EMIRAT		亞、摩納哥、匈牙利、冰島、愛爾蘭、意大利、約旦、科索沃、列支敦士登、, 斯洛文尼亞, 西班牙, 瑞典, 瑞士, 東帝汶, 突尼斯, 土耳其, 英國, 烏克蘭, 阿拉伯聯合酋長國, 英屬維爾京群島

敏感資料類型	敏感資料類別	受管資料識別符 ID	必要的關鍵字	國家和地區
		ES_BANK_ACCOUNT_NUMBER, VIRGIN_ISLANDS_BANK_ACCOUNT_NUMBER（適用於英屬維爾京群島）		
網絡令牌	登入資料	JSON_WEB_TOKEN	否	任何
郵寄地址	個人資料：個人資料	ADDRESS，BRAZIL_CEP_CODE（巴西郵政編碼）	各有不同	澳大利亞，巴西，加拿大，法國，德國，意大利，西班牙，英國，美國
美国国家药品法典	個人資料：PHI	USA_NATIONAL_DRUG_CODE	是	美國
國家身分證號碼	個人資料：個人資料	取決於國家或地區： BRAZIL_RG_NUMBER, FRANCE_NATIONAL_IDENTIFICATION_NUMBER, GERMANY_NATIONAL_IDENTIFICATION_NUMBER, INDIA_AADHAAR_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_DNI_NUMBER	是	巴西，法國，德國，印度，意大利，西班牙
國民保險號碼 (NINO)	個人資料：個人資料	UK_NATIONAL_INSURANCE_NUMBER	是	英國
國家供應商識別碼 (NPI)	個人資料：PHI	USA_NATIONAL_PROVIDER_IDENTIFIER	是	美國
OpenSSH 私密金鑰	登入資料	OPENSSH_PRIVATE_KEY	否	任何

敏感資料類型	敏感資料類別	受管資料識別符 ID	必要的關鍵字	國家和地區
護照號碼	個人資料：個人資料	取決於國家或地區： CANADA_PASSPORT_NUMBER, FRANCE_PASSPORT_NUMBER, GERMANY_PASSPORT_NUMBER, ITALY_PASSPORT_NUMBER, SPAIN_PASSPORT_NUMBER, UK_PASSPORT_NUMBER, USA_PASSPORT_NUMBER	是	加拿大、法國、德國、義大利、西班牙、英國、美國
永久居留號碼	個人資料：個人資料	CANADA_NATIONAL_IDENTIFICATION_NUMBER	是	加拿大
PGP 私密金鑰	登入資料	PGP_PRIVATE_KEY	否	任何
電話號碼	個人資料：個人資料	取決於國家或地區： BRAZIL_PHONE_NUMBER, FRANCE_PHONE_NUMBER, GERMANY_PHONE_NUMBER, ITALY_PHONE_NUMBER, PHONE_NUMBER (for Canada and the US), SPAIN_PHONE_NUMBER, UK_PHONE_NUMBER	各有不同	巴西、加拿大、法國、德國、義大利、西班牙、英國、美國
公開金鑰加密標準 (PKCS) 私密金鑰	登入資料	PKCS	否	任何
PuTTY 私密金鑰	登入資料	PUTTY_PRIVATE_KEY	否	任何
社會保險號碼 (SIN)	個人資料：個人資料	CANADA_SOCIAL_INSURANCE_NUMBER	是	加拿大

敏感資料類型	敏感資料類別	受管資料識別符 ID	必要的關鍵字	國家和地區
社會安全號碼 (SSN)	個人資料：個人資料	視乎國家或地區而定：SPAIN_SOCIAL_SECURITY_NUMBERUSA_SOCIAL_SECURITY_NUMBER	是	西班牙、美國
the section called “條紋 API 金鑰”	登入資料	STRIPE_CREDENTIALS	否	任何
納稅識別號碼或參考號碼	個人資料：個人資料	取決於國家或地區： AUSTRALIA_TAX_FILE_NUMBER, BRAZIL_CNPJ_NUMBER, BRAZIL_CPF_NUMBER, FRANCE_TAX_IDENTIFICATION_NUMBER, GERMANY_TAX_IDENTIFICATION_NUMBER, INDIA_PERMANENT_ACCOUNT_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_NIE_NUMBER, SPAIN_NIF_NUMBER, SPAIN_TAX_IDENTIFICATION_NUMBER, UK_TAX_IDENTIFICATION_NUMBER, USA_INDIVIDUAL_TAX_IDENTIFICATION_NUMBER	是	澳大利亞，巴西，法國，德國，印度，意大利，西班牙，英國，美國
唯一裝置識別碼 (UDI)	個人資料：PHI	MEDICAL_DEVICE_UDI	是	美國

敏感資料類型	敏感資料類別	受管資料識別符 ID	必要的關鍵字	國家和地區
車輛識別號碼 (VIN)	個人資料：個人資料	VEHICLE_IDENTIFICATION_NUMBER	是	任何，如果 VIN 接近以下其中一種語言的關鍵字：英語，法語，德語，立陶宛語，波蘭語，葡萄牙語，羅馬尼亞語或西班牙語

認證資料的受管理資料識別碼

Amazon Macie 可以使用受管資料識別碼偵測多種類型的敏感登入資料資料。此頁面上的主題會指定每個類型，並提供有關設計用來偵測資料之受管理資料識別碼的資訊。每個主題都提供下列資訊：

- 受管理的資料識別碼 ID — 指定專為偵測資料而設計的受管理資料識別碼的唯一識別碼 (ID)。當您建立敏感資料探索工作或設定自動化敏感資料探索設定時，您可以使用此 ID 來指定您是否希望 Macie 在分析資料時使用受管理資料識別碼。
- 支援的國家和地區 — 指出適用的受管資料識別碼適用於哪些國家或地區。如果受管資料識別碼並非針對特定國家或地區設計，則此值為 A ny。
- 需要關鍵字 — 指定偵測是否需要關鍵字與資料相鄰。如果需要關鍵字，主題也會提供必要關鍵字的範例。如需 Macie 在分析資料時如何使用關鍵字的詳細資訊，請參閱關鍵字要求。
- 註解 — 提供任何相關詳細資訊，這些詳細資料可能會影響您選擇的受管理資料識別碼，或是您對報告的敏感資料發生次數 詳細資料包括支援的標準、語法需求和例外等資訊。

主題會依機密資料類型按字母順序列出。

敏感資料類型

- AWS 私密存取金鑰

- 谷歌雲 API 密鑰
- HTTP 基本授權標頭
- 網絡令牌
- OpenSSH 私密金鑰
- PGP 私密金鑰
- 公開金鑰加密標準 (PKCS) 私密金鑰
- PuTTY 私密金鑰
- 條紋 API 金鑰

AWS 私密存取金鑰

受管理的資料識別碼 ID：AWS_CREDENTIALS

支持的國家和地區：任何

需要關鍵字：是。關鍵字包括：aws_secret_access_key, credentials, secret access key, secret key, set-awscredential

備註：Macie 不會報告下列字元序列的出現次數，這些序列通常用作虛構範例：和。`je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY` `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`

谷歌雲 API 密鑰

受管理的資料識別碼 ID：GCP_API_KEY

支持的國家和地區：任何

需要關鍵字：是。關鍵字包括：G_PLACES_KEY, GCP api key, GCP key, google cloud key, google-api-key, google-cloud-apikeys, GOOGLEKEY, X-goog-api-key

註解:Macie 只能偵測谷歌雲 API 金鑰的字串 (`keyString`) 元件。Support 務不包括偵測 GCP API 金鑰的 ID 或顯示名稱元件。

HTTP 基本授權標頭

受管理的資料識別碼 ID：HTTP_BASIC_AUTH_HEADER

支持的國家和地區：任何

需要關鍵字：否

備註：偵測需要完整的標頭，包括欄位名稱和驗證配置指示詞，如 RFC 76 17 所指定。例如：`Authorization: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==` 和 `Proxy-Authorization: Basic dGVzdDoxMjPCow==`。

網絡令牌

受管理的資料識別碼 ID：JSON_WEB_TOKEN

支持的國家和地區：任何

需要關鍵字：否

備註：馬西可以偵測符合 RFC 7519 針對 JSON 網頁簽章 (JWS) 結構所指定之要求的 JSON 網頁權杖 (JWT)。令牌可以簽名或無符號。

OpenSSH 私密金鑰

受管理的資料識別碼 ID：OPENSSH_PRIVATE_KEY

支持的國家和地區：任何

需要關鍵字：否

評論：無

PGP 私密金鑰

受管理的資料識別碼 ID：PGP_PRIVATE_KEY

支持的國家和地區：任何

需要關鍵字：否

評論：無

公開金鑰加密標準 (PKCS) 私密金鑰

受管理的資料識別碼 ID：PKCS

支持的國家和地區：任何

需要關鍵字：否

評論：無

PuTTY 私密金鑰

受管理的資料識別碼 ID：PUTTY_PRIVATE_KEY

支持的國家和地區：任何

需要關鍵字：否

備註:Macie 可以偵測 PuTTY 私密金鑰，這些私密金鑰使用下列標準標頭和標頭序列：PuTTY-User-Key-FileEncryption、Comment、、Public-LinesPrivate-Lines、和。Private-MAC標頭值可以包含英數字元、連字號 (-) 和換行符號 (\n或\r)。 Public-Lines和Private-Lines值也可以包含正斜線 (/)、加號 (+) 和等號 (=)。 Private-MAC值也可以包含加號 (+)。Support 不包括偵測含有其他字元的標頭值的私密金鑰，例如空格或底線 (_)。Support 也不包括偵測包含自訂標頭的私密金鑰。

條紋 API 金鑰

受管理的資料識別碼 ID：STRIPE_CREDENTIALS

支持的國家和地區：任何

需要關鍵字：否

備註：Macie 不會報告下列字元序列的出現次數，這些字元序列通常用於 Stripe 程式碼範例中：sk_test_4eC39HqLyjWDarjtT1zdp7dc和pk_test_TYooMQauvdEDq54NiTphI7jx.

財務資訊的受管理資料識別碼

Amazon Macie 可以使用受管資料識別碼偵測多種類型的敏感財務資訊。此頁面上的主題會列出每個類型，並提供有關設計用來偵測資料之受管理資料識別碼的資訊。每個主題都提供下列資訊：

- 受管理的資料識別碼 ID — 為設計用來偵測資料的一或多個受管理資料識別碼指定唯一識別碼 (ID)。當您建立敏感資料探索工作或設定自動化敏感資料探索設定時，您可以使用這些 ID 來指定您希望 Macie 在分析資料時使用的受管理資料識別碼。
- 支援的國家和地區 — 指出適用的受管資料識別碼適用於哪些國家或地區。如果受管資料識別碼並非針對特定國家或地區設計，則此值為 A ny。
- 需要關鍵字 — 指定偵測是否需要關鍵字與資料相鄰。如果需要關鍵字，主題也會提供必要關鍵字的範例。如需 Macie 在分析資料時如何使用關鍵字的詳細資訊，請參閱關鍵字要求。
- 註解 — 提供任何相關詳細資訊，這些詳細資料可能會影響您選擇的受管理資料識別碼，或是您對報告的敏感資料發生次數 詳細資料包括支援的標準、語法需求和例外等資訊。

主題會依機密資料類型按字母順序列出。

敏感資料類型

- 銀行帳戶號碼
- 基本銀行帳戶號碼
- 信用卡到期日
- 信用卡磁條數據
- 信用卡號碼
- 信用卡驗證碼
- 國際銀行帳戶號碼

銀行帳戶號碼

Macie 可以偵測由 9—17 位數序列組成且不包含任何空格的加拿大和美國銀行帳戶號碼。

受管理的資料識別碼 ID：BANK_ACCOUNT_NUMBER

支援的國家和地區：加拿大、美國

需要關鍵字：是。關鍵字包括：bank account, bank acct, checking account, checking acct, deposit account, deposit acct, savings account, savings acct, chequing account, chequing acct

備註：此受管資料識別碼專為偵測加拿大和美國的銀行帳戶號碼而設計。這些國家/地區不使用 ISO 13616 規定的 ISO 國際標準為銀行帳戶編號所定義的基本銀行帳戶號碼 (BBAN) 或國際銀行帳戶號碼 (IBAN) 格式。若要偵測其他國家和地區的銀行帳戶號碼，請使用專為這些格式設計的受管資料識別碼。如需詳細資訊，請參閱 基本銀行帳戶號碼 及 國際銀行帳戶號碼。

基本銀行帳戶號碼

Macie 可以檢測符合 ISO 13616 規定的 ISO 國際銀行帳戶編號標準定義的 BBAN 結構的基本銀行帳戶號碼（BBAN）。這包括不包含空格，或使用空格或連字號分隔符號的 BBAN，例如、和。`NWBK60161331926819` `NWBK 6016 1331 9268 19` `NWBK-6016-1331-9268-19`

受管資料識別碼 ID：視國家或地區而定，FRANCE_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, ITALY_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER

支持的國家和地區：法國，德國，意大利，西班牙，英國

需要關鍵字：是。下表列出 Macie 在特定國家和地區辨識的關鍵字。

國家/地區或區域	關鍵字
法國	account code, account number, accountno#, accountnumber#, bban, code bancaire, compte bancaire, customer account id, customer account number, customer bank account id, iban, numéro de compte
德國	account code, account number, accountno #, accountnumber#, bankleitzahl, bban, customer account id, customer account number, customer bank account id, geheimzahl, iban, kartennummer, kontonummer, kreditkartennummer, sepa
義大利	account code, account number, accountno #, accountnumber#, bban, codice bancario, conto bancario, customer account id, customer account number, customer bank account id, iban, numero di conto
西班牙	account code, account number, accountno #, accountnumber#, bban, código cuenta, código cuenta bancaria, cuenta cliente id, customer account ID, customer account number, customer bank account id, iban, número cuenta bancaria cliente, número cuenta cliente
英國	account code, account number, accountno #, accountnumber#, bban, customer account id, customer account number, customer bank account id, iban, sepa

備註：這些受管資料識別碼也可以偵測符合 ISO 13616 標準的國際銀行帳戶號碼 (IBAN)。如需詳細資訊，請參閱 國際銀行帳戶號碼。UK (UK_BANK_ACCOUNT_NUMBER) 的受管資料識別碼也可以偵測英國的國內銀行帳戶號碼，例如。`60-16-13 31926819`

信用卡到期日

受管理的資料識別碼 ID：CREDIT_CARD_EXPIRATION

支持的國家和地區：任何

需要關鍵字：是。關鍵字包括：exp d, exp m, exp y, expiration, expiry

註釋：Support 包括大多數日期格式，例如所有數字以及數字和月份名稱的組合。日期元件可以用斜線 (/)、連字號 (-) 或適用的關鍵字分隔。例如，Macie 可以偵測日期，例如02/2602/2026、Feb 2026、26-Feb、和expY=2026, expM=02。

信用卡磁條數據

受管理的資料識別碼 ID：CREDIT_CARD_MAGNETIC_STRIPE

支持的國家和地區：任何

需要關鍵字：是。關鍵字包括：card data, iso7813, mag, magstripe, stripe, swipe

備註:Support 包括音軌 1 和 2。

信用卡號碼

受管理資料識別碼 ID：CREDIT_CARD_NUMBER適用於與關鍵字相鄰的信CREDIT_CARD_NUMBER_(NO_KEYWORD)用卡號碼，不在關鍵字附近的信用卡號碼

支持的國家和地區：任何

所需關鍵字：不同 CREDIT_CARD_NUMBER受管理的資料識別碼需要關鍵字。關鍵字包括：account number, american express, amex, bank card, c card, card, cc #, ccn, check card, cred card, credit, credit card, credit cards, credit no, credit num, dankort, debit, debit card, debit no, debit num, diners club, discover, electron, japanese card bureau, jcb, mastercard, mc, pan, payment account number, payment card number, pcn, pmnt #, pmnt card, pmnt no, pmnt number, union pay, visa. CREDIT_CARD_NUMBER_(NO_KEYWORD)受管理的資料識別碼不需要關鍵字。

註釋：檢測要求數據是一個 13—19 位數字序列，該序列符合 Luhn 檢查公式，並為以下任何類型的信用卡使用標準卡號前綴：美國運通卡，Dankort，晚餐俱樂部，發現，電子，日本卡局（JCB），萬事達卡和 Visa。 UnionPay

Macie 不會報告信用卡發卡機構已保留供公開測試之用的下列順序：1220000000000003,,,,,,2222405343248877,,2222990905257051,2223007648726984,,2223577125200828282828210

5204230080000017520474000990001 4、5420923878724339、5454545454545454、5455330760076009244561。

信用卡驗證碼

受管理的資料識別碼 ID：CREDIT_CARD_SECURITY_CODE

支持的國家和地區：任何

需要關鍵字：是。關鍵字包括：card id, card identification code, card identification number, card security code, card validation code, card validation number, card verification data, card verification value, cvc, cvc2, cvv, cvv2, elo verification code

評論：沒有

國際銀行帳戶號碼

Macie 可以檢測到由多達 34 個字母數字字符組成的國際銀行帳戶號碼（IBAN），包括國家/地區代碼等元素。更具體地說，Macie 可以檢測符合 ISO 13616 規定的 ISO 國際銀行帳戶編號標準的 IBAN。這包括不包含空格，或使用空格或連字號分隔符號的 IBAN，例如，、和。GB29NWBK60161331926819 GB29 NWBK 6016 1331 9268 19 GB29-NWBK-6016-1331-9268-19檢測包括基於模數 97 方案的驗證檢查。

受管資料識別碼 ID：視國家或地區而定 ALBANIA_BANK_ACCOUNT_NUMBER, ANDORRA_BANK_ACCOUNT_NUMBER, BOSNIA_AND_HERZEGOVINA_BANK_ACCOUNT_NUMBER, BRAZIL_BANK_ACCOUNT_NUMBER, BULGARIA_BANK_ACCOUNT_NUMBER, COSTA_RICA_BANK_ACCOUNT_NUMBER, CROATIA_BANK_ACCOUNT_NUMBER, CYPRUS_BANK_ACCOUNT_NUMBER, CZECH_REPUBLIC_BANK_ACCOUNT_NUMBER, DENMARK_BANK_ACCOUNT_NUMBER, DOMINICAN_REPUBLIC_BANK_ACCOUNT_NUMBER, EGYPT_BANK_ACCOUNT_NUMBER, ESTONIA_BANK_ACCOUNT_NUMBER, FAROE_ISLANDS_BANK_ACCOUNT_NUMBER, FINLAND_BANK_ACCOUNT_NUMBER, FRANCE_BANK_ACCOUNT_NUMBER, GEORGIA_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, GREECE_BANK_ACCOUNT_NUMBER, GREENLAND_BANK_ACCOUNT_NUMBER, HUNGARY_BANK_ACCOUNT_NUMBER, ICELAND_BANK_ACCOUNT_NUMBER, IRELAND_BANK_ACCOUNT_NUMBER, ITALY_BANK_ACCOUNT_NUMBER, JORDAN_BANK_ACCOUNT_NUMBER, KOSOVO_BANK_ACCOUNT_NUMBER, LIECHTENSTEIN_BANK_ACCOUNT_NUMBER, LITHUANIA_BANK_ACCOUNT_NUMBER, MALTA_BANK_ACCOUNT_NUMBER, MAURITANIA_BANK_ACCOUNT_NUMBER, MAURITIUS_BANK_ACCOUNT_NUMBER,

MONACO_BANK_ACCOUNT_NUMBER, MONTENEGRO_BANK_ACCOUNT_NUMBER, NETHERLANDS_BANK_ACCOUNT_NUMBER, NORTH_MACEDONIA_BANK_ACCOUNT_NUMBER, POLAND_BANK_ACCOUNT_NUMBER, PORTUGAL_BANK_ACCOUNT_NUMBER, SAN_MARINO_BANK_ACCOUNT_NUMBER, SENEGAL_BANK_ACCOUNT_NUMBER, SERBIA_BANK_ACCOUNT_NUMBER, SLOVAKIA_BANK_ACCOUNT_NUMBER, SLOVENIA_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, SWEDEN_BANK_ACCOUNT_NUMBER, SWITZERLAND_BANK_ACCOUNT_NUMBER, TIMOR_LESTE_BANK_ACCOUNT_NUMBER, TUNISIA_BANK_ACCOUNT_NUMBER, TURKIYE_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER, UKRAINE_BANK_ACCOUNT_NUMBER, UNITED_ARAB_EMIRATES_BANK_ACCOUNT_NUMBER, VIRGIN_ISLANDS_BANK_ACCOUNT_NUMBER (適用於英屬維京群島)

支持的國家和地區：阿爾巴尼亞，安道爾，波斯尼亞-黑塞哥維那，巴西，保加利亞，哥斯達黎加，克羅地亞，捷克共和國，丹麥，多米尼加共和國，埃及，愛爾蘭，埃及，埃及，愛爾蘭，意大利，約旦，科索沃，列支敦士登，芬蘭，法國，格魯吉亞，德國，希臘，格陵蘭，匈牙利，冰島，愛爾蘭，意大利，約旦，科索沃，列支敦士登，立陶宛，馬耳他，毛里塔尼亞，毛里塔尼亞，毛里塔尼亞，毛里塔尼亞，匈牙利，冰島，愛爾蘭塞內加爾, 塞爾維亞, 斯洛伐克, 斯洛文尼亞, 西班牙, 瑞典, 瑞士, 東帝汶, 突尼斯, 土耳其, 英國, 烏克蘭, 阿拉伯聯合阿聯酋航空、維爾京群島 (英屬)

需要關鍵字：否

備註：法國、德國、義大利、西班牙和英國的受管資料識別碼也可以偵測符合 ISO 13616 標準所定義之 BBAN 結構的基本銀行帳戶號碼 (BBAN) (如果字元序列與關鍵字相近)。如需更多詳細資訊，請參閱基本銀行帳戶號碼。

個人健康資訊 (PHI) 的受管理資料識別碼

Amazon Macie 可以使用受管資料識別碼偵測多種類型的敏感個人健康資訊 (PHI)。此頁面上的主題會指定每個類型，並提供有關設計用來偵測資料之受管理資料識別碼的資訊。每個主題都提供下列資訊：

- 受管理的資料識別碼 ID — 指定專為偵測資料而設計的受管理資料識別碼的唯一識別碼 (ID)。當您建立敏感資料探索工作或設定自動化敏感資料探索設定時，您可以使用此 ID 來指定您是否希望 Macie 在分析資料時使用受管理資料識別碼。
- 支援的國家和地區 — 指出適用的受管資料識別碼適用於哪些國家或地區。如果受管資料識別碼並非針對特定國家或地區設計，則此值為 A ny。
- 需要關鍵字 — 指定偵測是否需要關鍵字與資料相鄰。如果需要關鍵字，主題也會提供必要關鍵字的範例。如需 Macie 在分析資料時如何使用關鍵字的詳細資訊，請參閱關鍵字要求。

- 註解 — 提供任何相關詳細資訊，這些詳細資料可能會影響您選擇的受管理資料識別碼，或是您對報告的敏感資料發生次數 詳細資料包括支援的標準、語法需求和例外等資訊。

主題會依機密資料類型按字母順序列出。

敏感資料類型

- 毒品執法局 (DEA) 註冊號碼
- Health 保險索償編號
- 健康保險或醫療識別號碼
- 醫療保健通用程序編碼系統 (HCPCS) 代碼
- 美国国家药品法典
- 國家供應商識別碼 (NPI)
- 唯一裝置識別碼 (UDI)

毒品執法局 (DEA) 註冊號碼

受管理的資料識別碼 ID：US_DRUG_ENFORCEMENT_AGENCY_NUMBER

支援的國家和地區：美國

需要關鍵字：是。關鍵字包括：dea number, dea registration

評論：沒有

Health 保險索償編號

受管理的資料識別碼 ID：USA_HEALTH_INSURANCE_CLAIM_NUMBER

支援的國家和地區：美國

需要關鍵字：是。關鍵字包括：health insurance claim number, hic no, hic no., hic number, hic#, hicn, hicn#., hicno#

評論：沒有

健康保險或醫療識別號碼

Support 務包括歐盟和芬蘭的歐洲 Health 保險卡號碼、法國的 Health 保險號碼、美國的 Medicare 受益人識別碼、英國的 NHS 號碼，以及加拿大的個人健康號碼。

受管資料識別碼 ID：視國家或地區而定，CANADA_HEALTH_NUMBER, EUROPEAN_HEALTH_INSURANCE_CARD_NUMBER, FINLAND_EUROPEAN_HEALTH_INSURANCE_NUMBER, FRANCE_HEALTH_INSURANCE_NUMBER, UK_NHS_NUMBER, USA_MEDICARE_BENEFICIARY_IDENTIFIER

支持的國家和地區：加拿大，歐盟，芬蘭，法國，英國，美國

需要關鍵字：是。下表列出 Macie 在特定國家和地區辨識的關鍵字。

國家/地區或區域	關鍵字
加拿大	canada healthcare number, msp number, personal healthcare number, phn, soins de santé
歐盟	assicurazione sanitaria numero, carta assicurazione numero, carte d’assurance maladie, carte européenne d'assurance maladie, ceam, ehic, ehic#, finlandehicnumber#, gesundheitskarte, hälsokort, health card, health card number, health insurance card, health insurance number, insurance card number, krankenversicherungskarte, krankenversicherungsnummer, medical account number, numero conto medico, numéro d’assurance maladie, numéro de carte d’assurance, numéro de compte medical, número de cuenta médica, número de seguro de salud, número de tarjeta de seguro, sairaanhoitokortin, sairausva kuutuskortti, sairausvakuutusnumero, sjukförsäkring nummer, sjukförsäkringskort, suomi ehic-numero, tarjeta de salud, terveyskortti, tessera sanitaria assicurazione numero, versicherungsnummer
芬蘭	ehic, ehic#, finland health insurance card, finlandehicnumber#, finska sjukförsäkringskor

國家/地區或區域	關鍵字
	t, hälsokort, health card, health card number, health insurance card, health insurance number, sairaanhoitokortin, sairaanhoitokortin , sairausvakuutuskortti, sairausvakuutusnum ero, sjukförsäkring nummer, sjukförsäkringskor t, suomen sairausvakuutuskortti, suomi ehic-numero, terveyskortti
法國	carte d'assuré social, carte vitale, insurance card
英國	national health service, NHS
美國	mbi, medicare beneficiary

評論：沒有

醫療保健通用程序編碼系統 (HCPCS) 代碼

受管理的資料識別碼 ID：USA_HEALTHCARE_PROCEDURE_CODE

支援的國家和地區：美國

需要關鍵字：是。關鍵字包括：current procedural terminology, hcpcs, healthcare common procedure coding system

評論：沒有

美国国家药品法典

受管理的資料識別碼 ID：USA_NATIONAL_DRUG_CODE

支援的國家和地區：美國

需要關鍵字：是。關鍵字包括：national drug code, ndc

評論：沒有

國家供應商識別碼 (NPI)

受管理的資料識別碼 ID：USA_NATIONAL_PROVIDER_IDENTIFIER

支援的國家和地區：美國

需要關鍵字：是。關鍵字包括：hipaa, n.p.i, national provider, npi

評論：沒有

唯一裝置識別碼 (UDI)

受管理的資料識別碼 ID：MEDICAL_DEVICE_UDI

支援的國家和地區：美國

需要關鍵字：是。關鍵字包括：blood, blood bag, dev id, device id, device identifier, gs1, hibcc, iccbba, med, udi, unique device id, unique device identifier

備註：Macie 可偵測符合美國食品和藥物管理局核准格式的唯一裝置識別碼 (UDIS)。這包括由 GS1、中央銀行和 ICCBBA 定義的標準格式。ICCBA 支援適用於 ISBT 標準。

個人識別資訊 (PII) 的受管理資料識別碼

Amazon Macie 可以使用受管資料識別碼偵測多種類型的敏感個人識別資訊 (PII)。此頁面上的主題會列出每個類型，並提供有關設計用來偵測資料之受管理資料識別碼的資訊。每個主題都提供下列資訊：

- 受管理的資料識別碼 ID — 為設計用來偵測資料的一或多個受管理資料識別碼指定唯一識別碼 (ID)。當您建立敏感資料探索工作或設定自動化敏感資料探索設定時，您可以使用這些 ID 來指定您希望 Macie 在分析資料時使用的受管理資料識別碼。
- 支援的國家和地區 — 指出適用的受管資料識別碼適用於哪些國家或地區。如果受管資料識別碼並非針對特定國家或地區設計，則此值為 A ny。
- 需要關鍵字 — 指定偵測是否需要關鍵字與資料相鄰。如果需要關鍵字，主題也會提供必要關鍵字的範例。如需 Macie 在分析資料時如何使用關鍵字的詳細資訊，請參閱關鍵字要求。
- 註解 — 提供任何相關詳細資訊，這些詳細資料可能會影響您選擇的受管理資料識別碼，或是您對報告的敏感資料發生次數 詳細資料包括支援的標準、語法需求和例外等資訊。

主題會依機密資料類型按字母順序列出。

敏感資料類型

- 出生日期
- 駕照識別號碼

- 選民名冊號碼
- 全名
- 全球定位系統 (GPS) 座標
- 餅乾
- 郵寄地址
- 國家身分證號碼
- 國民保險號碼 (NINO)
- 護照號碼
- 永久居留號碼
- 電話號碼
- 社會保險號碼 (SIN)
- 社會安全號碼 (SSN)
- 納稅識別號碼或參考號碼
- 車輛識別號碼 (VIN)

出生日期

受管理的資料識別碼 ID：DATE_OF_BIRTH

支持的國家和地區：任何

需要關鍵字：是。關鍵字包括：bday, b-day, birth date, birthday, date of birth, dob

註釋：Support 包括大多數日期格式，例如所有數字以及數字和月份名稱的組合。您可以用空格、斜線 (/) 或連字號 (-) 分隔日期組成部分。

駕照識別號碼

受管資料識別碼 ID：視國家或地區而定，AUSTRALIA_DRIVERS_LICENSE, AUSTRIA_DRIVERS_LICENSE, BELGIUM_DRIVERS_LICENSE, BULGARIA_DRIVERS_LICENSE, CANADA_DRIVERS_LICENSE, CROATIA_DRIVERS_LICENSE, CYPRUS_DRIVERS_LICENSE, CZECHIA_DRIVERS_LICENSE, DENMARK_DRIVERS_LICENSE, DRIVERS_LICENSE (for the US), ESTONIA_DRIVERS_LICENSE, FINLAND_DRIVERS_LICENSE, FRANCE_DRIVERS_LICENSE, GERMANY_DRIVERS_LICENSE, GREECE_DRIVERS_LICENSE,

HUNGARY_DRIVERS_LICENSE, INDIA_DRIVERS_LICENSE, IRELAND_DRIVERS_LICENSE, ITALY_DRIVERS_LICENSE, LATVIA_DRIVERS_LICENSE, LITHUANIA_DRIVERS_LICENSE, LUXEMBOURG_DRIVERS_LICENSE, MALTA_DRIVERS_LICENSE, NETHERLANDS_DRIVERS_LICENSE, POLAND_DRIVERS_LICENSE, PORTUGAL_DRIVERS_LICENSE, ROMANIA_DRIVERS_LICENSE, SLOVAKIA_DRIVERS_LICENSE, SLOVENIA_DRIVERS_LICENSE, SPAIN_DRIVERS_LICENSE, SWEDEN_DRIVERS_LICENSE, UK_DRIVERS_LICENSE

支持的國家和地區：澳大利亞，奧地利，比利時，保加利亞，加拿大，克羅地亞，塞浦路斯，捷克共和國，丹麥，愛爾蘭，愛爾蘭，愛爾蘭，拉脫維亞，立陶宛，盧森堡，馬耳他，荷蘭，波蘭，葡萄牙，羅馬尼亞，斯洛伐克，斯洛文尼亞，西班牙，瑞典，英國，美國

需要關鍵字：是。下表列出 Macie 在特定國家和地區辨識的關鍵字。

國家/地區或區域	關鍵字
澳洲	dl#, dl:, dlno#, driver licence, driver license, driver permit, drivers lic., drivers licence, driver's licence, drivers license, driver's license, drivers permit, driver's permit, drivers permit number, driving licence, driving license, driving permit
奧地利	führerschein, fuhrerschein, führerschein republik österreich, fuhrerschein republik osterreich
比利時	fuehrerschein, fuehrerschein- nr, fuehrerschheinnummer, fuhrerschein, führerschein, fuhrerschein- nr, führerschein- nr, fuhrerscheinnummer, führerscheinnummer, numéro permis conduire, permis de conduire, rijbewijs, rijbewijsnummer
保加利亞	превозно средство, свидетелство за управление на моторно, свидетелство за управление на мпс, сумпс, шофьорска книжка

國家/地區或區域	關鍵字
加拿大	dl#, dl:, dlno#, driver licence, driver licences, driver license, driver licenses, driver permit, drivers lic., drivers licence, driver's licence, drivers licences, driver's licences, drivers license, driver's license, drivers licenses, driver's licenses, drivers permit, driver's permit, drivers permit number, driving licence, driving license, driving permit, permis de conduire
克羅埃西亞	vozačka dozvola
賽普勒斯	άδεια οδήγησης
捷克	číslo licence, číslo licence řidiče, číslo řidičskéh o průkazu, ovladače lic., povolení k jízdě, povolení řidiče, řidiči povolení, řidičský prúkaz, řidičský průkaz
丹麥	kørekort, kørekortnummer
愛沙尼亞	juhi litsentsi number, juhiloa number, juhiluba, juhiluba number
芬蘭	ajokortin numero, ajokortti, förare lic., körkort, körkort nummer, kuljettaja lic., permis de conduire
法國	permis de conduire
德國	fuehrerschein, fuehrerschein- nr, fuehrersc heinnummer, fuhrerschein, führerschein, fuhrerschein- nr, führerschein- nr, fuhrersch einnummer, führerscheinnummer
希臘	δεια οδήγησης, adeia odigisis

國家/地區或區域	關鍵字
匈牙利	illesztőprogramok lic, jogosítvány, jogsi, licencszám, vezető engedély, vezetői engedély
印度	driver licence, driver licences, driver license, driver licenses, drivers lic., drivers licence, driver's licence, drivers licences, driver's licences, drivers license, driver's license, drivers licenses, driver's licenses, driving licence, driving license
愛爾蘭	ceadúnas tiomána
義大利	patente di guida, patente di guida numero, patente guida, patente guida numero
拉脫維亞	autovadītāja apliecība, licences numurs, vadītāja apliecība, vadītāja apliecības numurs, vadītāja atļauja, vadītāja licences numurs, vadītāji lic.
立陶宛	vairuotojo pažymėjimas
盧森堡	fahrerlaubnis, führerschäin
馬爾他	liċenzja tas-sewqan
荷蘭	permis de conduire, rijbewijs, rijbewijsnummer
波蘭	numer licencyjny, prawo jazdy, zezwolenie na prowadzenie
葡萄牙	carta de condução, carteira de habilitação, carteira de motorist, carteira habilitação, carteira motorist, licença condução, licença de condução, número de licença, número licença, permissão condução, permissão de condução

國家/地區或區域	關鍵字
羅馬尼亞	numărul permisului de conducere, permis de conducere
斯洛伐克	číslo licencie, číslo vodičského preukazu, ovládače lic., povolenia vodičov, povolenie jazdu, povolenie na jazdu, povolenie vodiča, vodičský preukaz
斯洛維尼亞	vozniško dovoljenje
西班牙	carnet conducer, el carnet de conducer, licencia conducer, licencia de manejo, número carnet conducer, número de carnet de conducer, número de permiso conducer, número de permiso de conducer, número licencia conducer, número permiso conducer, permiso conducción, permiso conducer, permiso de conducción
瑞典	ajokortin numero, dlno# ajokortti, drivere lic., förare lic., körkort, körkort nummer, körkortsn ummer, kuljettajat lic.
英國	dl#, dl:, dlno#, driver licence, driver licences, driver license, driver licenses, driver permit, drivers lic., drivers licence, driver's licence, drivers licences, driver's licences, drivers license, driver's license, drivers licenses, driver's licenses, drivers permit, driver's permit, drivers permit number, driving licence, driving license, driving permit

國家/地區或區域	關鍵字
美國	dl#, dl:, dlno#, driver licence, driver licences, driver license, driver licenses, driver permit, drivers lic., drivers licence, driver's licence, drivers licences, driver's licences, drivers license, driver's license, drivers licenses, driver's licenses, drivers permit, driver's permit, drivers permit number, driving licence, driving license, driving permit

評論：沒有

選民名冊號碼

受管理的資料識別碼 ID：UK_ELECTORAL_ROLL_NUMBER

支持的國家和地區：英國

需要關鍵字：是。關鍵字包括：electoral #, electoral number, electoral roll #, electoral roll no., electoral roll number, electoralrollno

評論：沒有

全名

受管理的資料識別碼 ID：NAME

支持的國家和地區：任何

需要關鍵字：否

註釋:馬西只能檢測全名。支援僅限於拉丁字元集。

全球定位系統 (GPS) 座標

受管理的資料識別碼 ID：LATITUDE_LONGITUDE

支援的國家和地區：任何 (如果座標靠近英文關鍵字)。

需要關鍵字：是。關鍵字包括：coordinate, coordinates, lat long, latitude longitude, position

註釋：如果經緯度坐標存儲為一對，並且它們是十進制度（DD）格式，Macie 可以檢測 GPS 坐標。41.948614,-87.655311Support 不包括以下方式檢測坐標：十進制分鐘（DDM）格式41°56.9168'N 87°39.3187'W，例如度，分，秒（DMS）格式。41°56'55.0104"N 87°39'19.1196"W

餅乾

受管理的資料識別碼 ID：HTTP_COOKIE

支持的國家和地區：任何

需要關鍵字：否

備註：偵測需要完整Cookie或Set-Cookie標頭。標頭可以包含一個或多個名稱-值對，例如：Set-Cookie: id=TWlrZQ和。Cookie: session=3948; lang=en

郵寄地址

託管數據標識符 ID：ADDRESS（適用於澳大利亞，加拿大，法國，德國，意大利，西班牙，英國和美國），BRAZIL_CEP_CODE（適用於巴西郵政局）

支持的國家和地區：澳大利亞，巴西，加拿大，法國，德國，意大利，西班牙，英國，美國

所需關鍵字：不同 ADDRESS受管理資料識別碼不需要關鍵字。BRAZIL_CEP_CODE受管理的資料識別碼需要關鍵字。關鍵字包括：cep, código de endereçamento postal, codigo de endereçamento postal, código postal, codigo postal

備註：雖然ADDRESS受管理的資料識別碼不需要關鍵字，但偵測功能需要在支援的國家或地區中包含城市或地區的名稱，以及對應的郵遞區號或郵遞區號。受BRAZIL_CEP_CODE管理的資料識別碼只能偵測地址的郵政編碼 (CEP) 部分。

國家身分證號碼

Support 務包括印度的 Aadhaar 號碼、義大利的 Codice Fiscale 號碼、西班牙身份證明文件 (DNI) 識別碼、法國國家統計與經濟研究所 (INSEE) 代碼、德國國民身分證號碼，以及巴西的格拉爾登記 (RG) 號碼。

受管資料識別碼 ID：視國家或地區而定，BRAZIL_RG_NUMBER, FRANCE_NATIONAL_IDENTIFICATION_NUMBER, GERMANY_NATIONAL_IDENTIFICATION_NUMBER, INDIA_AADHAAR_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_DNI_NUMBER

支持的國家和地區：巴西，法國，德國，印度，意大利，西班牙

需要關鍵字：是。下表列出 Macie 在特定國家和地區辨識的關鍵字。

國家/地區或區域	關鍵字
巴西	registro geral, rg
法國	assurance sociale, carte nationale d’identit é, cni, code sécurité sociale, French social security number, fssn#, insee, insurance number, national id number, nationalid#, numéro d'assurance, sécurité sociale, sécurité sociale non., sécurité sociale numéro, social, social security, social security number, socialsecuritynumber, ss#, ssn, ssn#
德國	ausweisnummer, id number, identification number, identity number, insurance number, personal id, personalausweis
印度	aadhaar, aadhar, adhaar, uidai
義大利	codice fiscal, dati anagrafici, ehic, health card, health insurance card, p. iva, partita i.v.a., personal data, tax code, tessera sanitaria
西班牙	dni, dni#, dninúmero#, documento nacional de identidad, identidad único, identidadúnico#, insurance number, national identification number, national identity, nationalid#, nationali dno#, número nacional identidad, personal identification number, personal identity no, unique identity number, uniqueid#

評論：沒有

國民保險號碼 (NINO)

受管理的資料識別碼 ID：UK_NATIONAL_INSURANCE_NUMBER

支持的國家和地區：英國

需要關鍵字：是。關鍵字包括：insurance no., insurance number, insurance#, national insurance number, nationalinsurance#, nationalinsurancenumber, nin, nino

評論：沒有

護照號碼

受管資料識別碼 ID：視國家或地區而定，CANADA_PASSPORT_NUMBER, FRANCE_PASSPORT_NUMBER, GERMANY_PASSPORT_NUMBER, ITALY_PASSPORT_NUMBER, SPAIN_PASSPORT_NUMBER, UK_PASSPORT_NUMBER, USA_PASSPORT_NUMBER

支持的國家和地區：加拿大，法國，德國，意大利，西班牙，英國，美國

需要關鍵字：是。下表列出 Macie 在特定國家和地區辨識的關鍵字。

國家/地區或區域	關鍵字
加拿大	passeport, passeport#, passport, passport#, passportno, passportno#
法國	numéro de passeport, passeport, passeport #, passeport n °, passeport non
德國	ausstellungsdatum, ausstellungsort, geburtsdatum, passport, passports, reisepass, reisepass–nr, reisepassnummer
義大利	italian passport number, numéro passeport , numéro passeport italien, passaporto, passaporto italiana, passaporto numero, passport number, repubblica italiana passaporto
西班牙	españa pasaporte, libreta pasaporte, número pasaporte, pasaporte, passport, passport book, passport no, passport number, spain passport

國家/地區或區域	關鍵字
英國	passeport #, passeport n °, passeport non, passeportn °, passport #, passport no, passport number, passport#, passportid
美國	passport, travel document

評論：沒有

永久居留號碼

受管理的資料識別碼 ID：CANADA_NATIONAL_IDENTIFICATION_NUMBER

支援的國家和地區：加拿大

需要關鍵字：是。關鍵字包括：carte résident permanent, numéro carte résident permanent, numéro résident permanent, permanent resident card, permanent resident card number, permanent resident no, permanent resident no., permanent resident number, pr no, pr no., pr non, pr number, résident permanent no., résident permanent non

評論：沒有

電話號碼

受管資料識別碼 ID：視國家或地區而定，BRAZIL_PHONE_NUMBER, FRANCE_PHONE_NUMBER, GERMANY_PHONE_NUMBER, ITALY_PHONE_NUMBER, PHONE_NUMBER (for Canada and the US), SPAIN_PHONE_NUMBER, UK_PHONE_NUMBER

支持的國家和地區：巴西，加拿大，法國，德國，意大利，西班牙，英國，美國

所需關鍵字：不同 如果關鍵字與資料相鄰，則該號碼不必包含國家/地區代碼。關鍵字包括：cell, contact, fax, fax number, mobile, phone, phone number, tel, telephone, telephone number. 對於巴西，關鍵字還包括：cel, celular, fone, móvel, número residencial, numero residencial, telefone。如果關鍵字不在資料附近，則該數字必須包含國家/地區代碼。

備註：對於美國，支援包括免付費電話號碼。

社會保險號碼 (SIN)

受管理的資料識別碼 ID：CANADA_SOCIAL_INSURANCE_NUMBER

支援的國家和地區：加拿大

需要關鍵字：是。關鍵字包括：canadian id, numéro d'assurance sociale, sin, social insurance number

評論：沒有

社會安全號碼 (SSN)

受管資料識別碼 ID：視國家或地區而定 SPAIN_SOCIAL_SECURITY_NUMBER，USA_SOCIAL_SECURITY_NUMBER

支援的國家和地區：西班牙、美國

需要關鍵字：是。西班牙的關鍵字包括：número de la seguridad social, social security no., social security number, socialsecurityno#, ssn, ssn#。對於美國，關鍵字包括：social security, ss#, ssn。

評論：沒有

納稅識別號碼或參考號碼

Support 包括：西班牙的 CIF，NIE 和 NIF 號碼；巴西的 CNPJ 和 CPF 號碼；意大利的科德斯·菲斯卡號碼；美國的 ITIN；印度的 PAN；德國的代碼識別數字；澳大利亞的 TFN；法國的 TINS；英國的 TRN 和 UTR 號碼。

受管資料識別碼 ID：視國家或地區而定，AUSTRALIA_TAX_FILE_NUMBER, BRAZIL_CNPJ_NUMBER, BRAZIL_CPF_NUMBER, FRANCE_TAX_IDENTIFICATION_NUMBER, GERMANY_TAX_IDENTIFICATION_NUMBER, INDIA_PERMANENT_ACCOUNT_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_NIE_NUMBER, SPAIN_NIF_NUMBER, SPAIN_TAX_IDENTIFICATION_NUMBER, UK_TAX_IDENTIFICATION_NUMBER, USA_INDIVIDUAL_TAX_IDENTIFICATION_NUMBER

支持的國家和地區：澳大利亞，巴西，法國，德國，印度，意大利，西班牙，英國，美國

需要關鍵字：是。下表列出 Macie 在特定國家和地區辨識的關鍵字。

國家/地區或區域	關鍵字
澳洲	tax file number, tfn
巴西	cadastro de pessoa física, cadastro de pessoa fisica, cadastro de pessoas físicas, cadastro de pessoas fisicas, cadastro nacional da pessoa

國家/地區或區域	關鍵字
	jurídica, cadastro nacional da pessoa juridica, cnpj, cpf
法國	numéro d'identification fiscal, tax id, tax identification number, tax number, tin, tin#
德國	identifikationsnummer, steuer id, steueridentifikationsnummer, steuernummer, tax id, tax identification number, tax number
印度	e-pan, pan card, pan number, permanent account number
義大利	codice fiscal, dati anagrafici, ehic, health card, health insurance card, p. iva, partita i.v.a., personal data, tax code, tessera sanitaria
西班牙	cif, cif número, cifnúmero#, nie, nif, número de contribuyente, número de identidad de extranjero, número de identificación fiscal, número de impuesto corporativo, personal tax number, tax id, tax identification number, tax number, tin, tin#
英國	paye, tax id, tax id no., tax id number, tax identification, tax identification#, tax no., tax number, tax reference, tax#, taxid#, temporary reference number, tin, trn, unique tax reference, unique taxpayer reference, utr
美國	i.t.i.n., 個人納稅人識別號碼, 個人納稅識別號碼

評論：沒有

車輛識別號碼 (VIN)

受管理的資料識別碼 ID：VEHICLE_IDENTIFICATION_NUMBER

支援的國家和地區：任何，如果 VIN 接近以下其中一種語言的關鍵字：英文、法文、德文、立陶宛文、波蘭文、葡萄牙文、羅馬尼亞文或西班牙文。

需要關鍵字：是。關鍵字包括：Fahrgestellnummer, niv, numarul de identificare, numarul seriei de sasiu, numer VIN, Número de Identificação do Veículo, Número de Identificación de Automóviles, numéro d'identification du véhicule, vehicle identification number, vin, VIN numeris

備註:Macie 可以偵測包含 17 個字元序列的 VIN，並符合 ISO 3779 和 3780 標準。這些標準是專為全球使用而設計的。

在亞馬遜 Macie 中構建自定義數據標識符

一個自訂資料識別碼這是您定義用來偵測 Amazon 簡單儲存服務 (Amazon S3) 物件中敏感資料的一組準則。此條件包含規則運算式 (Regex)，此表達式定義要比對的文字模式，以及可選擇的字元序列和精簡結果之鄰近性規則。

使用自訂資料識別碼，您可以定義偵測準則，以反映組織的特定案例、智慧財產或專屬資料，例如員工 ID、客戶帳戶號碼或內部資料分類。如果您設定敏感資料探索工作或者自動化敏感資料探索若要使用這些識別碼，您可以以補充受管資料識別碼亞馬遜麥西提供。

除了偵測準則之外，您還可以為自訂資料識別碼所產生的敏感資料發現項目定義自訂嚴重性設定。默認情況下，馬西分配中等自訂資料識別碼所產生之所有發現項目的嚴重性 — 嚴重性不會根據符合自訂資料識別碼偵測準則的文字出現次數而變更。透過定義自訂嚴重性設定，您可以根據符合條件的文字出現次數，指定要指派的嚴重性。

主題

- 定義自訂資料識別碼的偵測標準
- 定義尋找自訂資料識別碼的嚴重性設定
- 建立自訂資料識別碼
- 自訂資料識別碼中的正則表達

定義自訂資料識別碼的偵測標準

建立自訂資料識別碼時，您可以指定規則運算式 (正規則)，定義要在 S3 物件中比對的文字模式。Macie 支持由提供的正則表達式模式語法的子集Perl 兼容的正則表達式（PCRE）庫。如需詳細資訊，請參閱正則表達式本節後面。

您也可以指定字元序列 (例如單字和片語)，以及鄰近規則來精簡結果。

關鍵字

這些是特定的字符序列，必須在與正則表達式模式匹配的文本附近。鄰近需求會根據 S3 物件的儲存格式或檔案類型而有所不同：

- 對於結構化的單欄式資料，如果文字符合 regex 模式，且關鍵字位於儲存文字的欄位或欄名稱中，或者文字的前面和位於相同欄位或儲存格值中關鍵字的最大符合距離之內，則 Macie 會包含結果。這是適用於微軟 Excel 工作簿，CSV 文件和 TSV 文件。
- 對於結構化、以記錄為基礎的資料，如果文字符合 regex 模式，且文字位於關鍵字的最大比對距離內，Macie 會包含結果。關鍵字可以位於儲存文字之欄位或陣列路徑中的元素名稱中，也可以位於儲存文字的欄位或陣列中的相同值之前並成為相同值的一部分。這是阿帕奇阿夫羅對象容器，阿帕奇實木複合地板文件，JSON 文件和 JSON 行文件是如此。
- 對於非結構化資料，如果文字符合 regex 模式，且文字的前面加上關鍵字的最大比對距離之內，Macie 就會包含一個結果。對於 Adobe 可移植文檔格式文件，微軟 Word 文檔，電子郵件消息和非二進制文本文件，CSV，JSON 行和 TSV 文件以外的非二進制文本文件是如此。這包括這些類型檔案中的任何結構化資料，例如資料表。

您可以指定多達 50 個關鍵字。每個關鍵字可包含 3—90 個 UTF-8 字元。關鍵字不區分大小寫。

最大匹配距離

這是一個基於字符的關鍵字鄰近規則。Macie 會使用此設定來判斷關鍵字是否在符合正則運算式模式的文字之前。此設定會定義在 complete 關鍵字結尾與符合 regex 模式的文字結尾之間可以存在的最大字元數。如果文字符合 regex 模式，發生在至少一個 complete 關鍵字之後，並且出現在關鍵字的指定距離內，Macie 會將其包含在結果中。否則，Macie 將其從結果中排除。

您可以指定 1-300 個字元的距離。預設距離為 50 個字元。為了獲得最佳結果，此距離應該大於正則表達式設計用於檢測的文本字符的最小字符數。如果只有部分文字在關鍵字的最大比對距離內，Macie 就不會將其包含在結果中。

忽略單字

這些是要從結果中排除的特定字符序列。如果文本與正則表達式模式匹配，但它包含忽略單詞，Macie 不會將其包含在結果中。

您最多可以指定 10 個忽略單字。每個忽略單字可包含 4—90 個 UTF-8 字元。忽略單詞需區分大小寫。

例如，許多公司都有員工 ID 的特定語法。一種這樣的語法可能是：一個大寫字母，表示員工是否是全職（F) 或兼職 (P) 員工，其次是連字號 (-)，後面接著識別員工的八位數序列。例子是：F-12345678，對於全職員工，以及P-87654321，對於兼職員工。

如果您建立自訂資料識別碼來偵測使用此語法的員工 ID，您可以使用下列 regex：[A-Z]-\d{8}。要優化分析並避免誤報，您還可以配置自定義數據標識符以使用關鍵字僱員和員工識別碼和 20 個字符的最大匹配距離。使用這些條件，結果僅在文本出現在關鍵字之後時才包含匹配 regex 的文本僱員或者員工識別碼並且所有文本都在其中一個關鍵字的 20 個字符內出現。

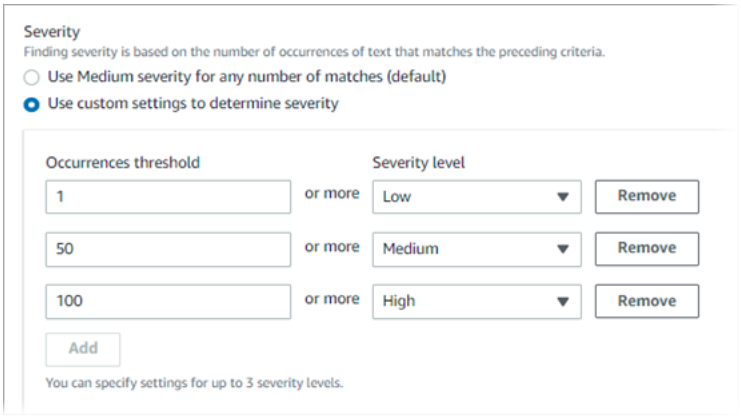
如需瞭解關鍵字如何協助您尋找敏感資料並避免誤判的示範，請觀看下列影片：亞馬遜 Macie 如何使用關鍵字發現敏感數據。

定義尋找自訂資料識別碼的嚴重性設定

建立自訂資料識別碼時，您也可以為識別碼產生的敏感資料發現項目定義自訂嚴重性設定。默認情況下，馬西分配中等自訂資料識別碼所產生之所有發現項目的嚴重性 — 如果 S3 物件包含至少一次符合自訂資料識別碼偵測準則的文字，Macie 會自動指派中等結果發現項目的嚴重性。

使用自訂嚴重性設定，您可以根據符合自訂資料識別碼偵測準則的文字出現次數，指定要指派的嚴重性。要做到這一點，你定義事件臨界值最多三個嚴重性等級：低（最不嚴重），中等，以及高（最嚴重）。一個發生次數閾是 S3 物件中必須存在的最小相符項目，才能產生具有指定嚴重性的發現項目。如果您指定一個以上的臨界值，臨界值必須按嚴重性遞增順序排列，低至高。

例如，下圖顯示自訂資料識別碼的嚴重性設定，該識別碼指定了三個發生次數臨界值，Macie 支援的每個嚴重性層級各一個。



下表指出自訂資料識別碼所產生之發現項目的嚴重性。

發生次數閾	嚴重性等級	結果
1	低	如果 S3 物件包含 1-49 次符合偵測準則的文字，則結果發現項目的嚴重性為低。

發生次數閾	嚴重性等級	結果
50	中型	如果 S3 物件包含 50—99 次符合偵測準則的文字，則結果發現項目的嚴重性為中等。
100	高	如果 S3 物件包含 100 個或更多符合偵測準則的文字，則結果發現項目的嚴重性為高。

您也可以使用嚴重性設定來指定是否要建立完全發現項目。如果 S3 物件包含的出現次數少於最低出現次數閾值，Macie 不會建立發現項目。

建立自訂資料識別碼

請依照下列步驟使用 Amazon Macie 主控台建立自訂資料識別碼。要以程式設計方式建立自訂資料識別碼，請使用CreateCustomDataIdentifier亞馬遜梅西 API 的操作。

若要建立自訂資料識別碼

1. 打開亞馬遜 Macie 控制台https://console.aws.amazon.com/macie/。
2. 在導覽窗格中的設定，選擇自訂資料識別碼。
3. 選擇 建立 。
4. 對於名稱」中，輸入自訂資料識別碼的名稱。該名稱最多可包含 128 個字元。

   避免在名稱中包含任何敏感數據。您帳戶的其他使用者可能可以看到該名稱，具體取決於允許他們在 Macie 中執行的動作。
5. (選擇性) 對於描述」中，輸入自訂資料識別碼的簡短描述。該描述最多可包含 512 個字元。

   避免在說明中包含任何敏感資料。您帳戶的其他使用者可能可以看到說明，具體取決於允許他們在 Macie 中執行的動作。
6. 對於規則運算式，輸入規則運算式 (正規則)，定義要比對的文字模式。正則表達式可以包含多達 512 個字符。若要瞭解支援的語法和條件約束，請參閱正則表達式本節後面。
7. (選擇性) 對於關鍵字中，輸入最多 50 個字元序列 (以逗號分隔)，以定義必須與 regex 模式相符之文字相鄰的特定文字。每個關鍵字可包含 3—90 個 UTF-8 字元。關鍵字不區分大小寫。

只有當文字符合 regex 模式且文字位於其中一個關鍵字的最大匹配距離內時，Macie 才會在結果中包含一個出現位置，如前面的主題。

8. (選擇性) 對於忽略單字中，輸入最多 10 個字元序列 (以逗號分隔)，以定義要從結果中排除的特定文字。每個忽略單字可包含 4—90 個 UTF-8 字元。忽略單詞需區分大小寫。

   如果文本與正則表達式模式匹配，但它包含以下忽略單詞之一，Macie 將從結果中排除出現的事件。

9. (選擇性) 對於最大匹配距離」下方，輸入關鍵字結尾與符合 regex 模式的文字結尾之間可以存在的最大字元數。距離可以是 1 至 300 個字元。預設距離為 50 個字元。

   只有當文字符合 regex 模式且文字位於 complete 關鍵字的這個距離內時，Macie 才會在結果中包含一個出現項，如前面的主題。

10. 對於嚴重性，選擇您希望 Macie 如何為自訂資料識別碼產生的敏感資料發現項目指派嚴重性：

    - 若要自動指定中等所有發現項目的嚴重性，選擇針對任意數目的相符項目使用中等嚴重性 (預設)。使用此選項，Macie 會自動指定中等如果受影響的 S3 物件包含一或多個符合偵測準則的文字，則發現項目的嚴重性。
    - 若要根據您指定的發生次數臨界值指派嚴重性，請選擇使用自訂設定判斷嚴重性。然後使用發生次數閾和嚴重性等級用於指定 S3 物件中必須存在的相符項目下限，才能產生具有所選嚴重性的發現項目。

      例如，若要指派高針對報告符合偵測準則的文字出現 100 個或更多次的發現項目的嚴重性，請輸入**100**在發生次數閾框，然後選擇高從嚴重性等級列表。

      您可以指定多達三個發生次數臨界值，Macie 支援的每個嚴重性層級各一個：低(對於最不嚴重),中等，或高（對於最嚴重的）。如果您指定多個臨界值，則臨界值必須按嚴重性遞增順序排列，低至高。如果 S3 物件包含的出現次數少於最低指定閾值，Macie 不會建立發現項目。

11. (選擇性) 對於标签，選擇新增標籤，然後輸入最多 50 個標籤，以指派給自訂資料識別碼。

    一個標籤是您定義並指定給某些類型的標籤AWS資源。每個標籤都包含必要的標籤鍵和一個可選的標籤值。標籤可協助您以不同的方式識別、分類及管理資源，例如依用途、擁有者、環境或其他條件。如需進一步了解，請參閱 標記亞馬遜麥西資源。

12. (選擇性) 對於評估」中，最多可輸入 1,000 個字元範例資料方塊中，然後選擇測試以測試偵測標準。Macie 會評估範例資料，並報告符合條件的文字出現次數。您可以根據需要重複此步驟多次，以優化和最佳化條件。

> **Note**
>
> 我們強烈建議您在儲存自訂資料識別碼之前，先測試並調整偵測準則。由於敏感資料探索任務會使用自訂資料識別碼，因此您無法在儲存自訂資料識別碼之後編輯該資料識別碼。這有助於確保您擁有不可變的敏感資料發現歷史記錄，以及您執行的資料隱私權和保護稽核或調查的探索結果。

13. 完成後，請選擇 Submit (提交)。

Macie 測試設置並驗證它是否可以編譯正則表達式。如果任何設置或正則表達式存在問題，則會發生錯誤並指出問題的性質。解決任何問題後，您可以儲存自訂資料識別碼。

自訂資料識別碼中的正則表達

Macie 支持由提供的正則表達式模式語法的子集Perl 兼容的正則表達式（PCRE）庫。在 PCRE 程式庫所提供的結構中，Macie 不支援下列樣式元素：

- 反向引用
- 擷取群組
- 條件式模式
- 內嵌程式碼
- 全域模式旗標，例如`/i`,`/m`，以及`/x`
- 遞歸模式
- 正面和負面的後視和前瞻零寬度斷言，例如`?=`,`?!`,`?<=`，以及`?<!`

要為自定義數據標識符創建有效的正則表達式模式，請注意以下提示和建議：

- 壁虎— 使用錨（^或者$) 僅當您預期圖樣出現在檔案的開頭或結尾，而不是行的開頭或結尾時。
- 有界重复— 出於性能原因，Macie 限制了有界重複組的大小。例如，`\d{100,1000}`不會在馬西編譯。若要近似此功能，您可以使用開放式重複，例如`\d{100,}`。
- 不區分大小寫— 若要使圖案的某些部分不區分大小寫，您可以使用`(?i)`構造而不是`/i`標誌。
- 性能— 無需手動優化前綴或替代。例如，變更`/hello|hi|hey/`至`/h(?:ello|i|ey)/`不會提高性能。
- 萬用字元— 出於性能原因，Macie 限制了重複通配符的數量。例如，`a*b*a*`不會在馬西編譯。

為了防止格式錯誤或長時間執行的運算式，Macie 會根據範例文字集合自動測試 regex 模式。

使用 Amazon Macie 允許清單定義敏感資料例外

您可以使用 Amazon Macie 中的允許清單，您可以定義 Macie 在檢查 Amazon Simple Storage Service (Amazon S3) 物件中忽略這些文字和文字模式。這些通常是針對特定案例或環境的敏感資料例外狀況。如果資料符合受管理資料中的文字或文字模式，則即使資料符合受管理資料的條件，Macie 也不會報告資料。透過使用允許清單，您可以精簡 Amazon S3 資料的分析並降低噪音。

您可以在 Macie 中建立和使用兩種類型的允許清單：

- 預先定義的文字 — 對於此類型的清單，您可以指定要忽略的特定字元序列，例如組織的公眾代表姓名、特定電話號碼或組織用於測試的特定範例資料。如果您使用這種類型的清單，Macie 會忽略與清單中項目完全相符之文字。

  如果您想要指定不敏感，不太可能更改，並且不一定依循常見模式的字元序列，這種類型的允許清單非常有用。
- 規則運算式 — 對於這種類型的清單，您可以指定定義要忽略的文字模式的規則運算式 (regex)，例如組織的公用電話號碼、組織網域的電子郵件地址，或組織用於測試的樣本資料。如果您使用這種類型的清單，Macie 會忽略與清單定義的模式完全相符之文字。

  如果您想要指定不敏感但多變，或可能更改且依循常見模式的文本，這種類型的允許清單非常有用。

建立允許清單後，您可以建立並設定敏感資料探索工作以使用該清單，或將其新增至自動化敏感資料探索設定。然後，Macie 在分析數據時使用該列表。如果 Macie 在允許清單中找到符合項目或模式的文字，Macie 就不會在敏感資料發現項目、統計資料和其他類型的結果中報告該文字出現。

您可以在目前可用 Macie 的所有 AWS 區域 中建立並使用允許清單，亞太區域 (大阪) 區域除外。

主題

- 允許 Amazon Macie 中的列表選項和要求
- 在 Amazon Macie 中創建和管理允許列表

允許 Amazon Macie 中的列表選項和要求

在 Amazon Macie 中，您可以使用允許清單來指定當 Macie 檢查 Amazon Simple Storage Service (Amazon S3) 物件是否有敏感資料時，要忽略的文字或文字模式。Macie 為兩種類型的允許清單 (預先定義的文字和規則運算式) 提供選項。

如果您希望 Macie 忽略您認為不敏感的特定字詞、片語和其他類型的字元序列，預先定義的文字清單非常有用。範例包括貴組織的公開代表姓名、特定電話號碼或貴組織用於測試的特定範例資料。如果 Macie 找到符合受管理或自訂資料識別碼準則的文字，而且該文字也符合允許清單中的項目，Macie 就不會在敏感資料發現項目、統計資料和其他類型的結果中報告該文字出現。

如果您希望 Macie 忽略變化或可能發生變化的文本，同時也堅持常見模式，則正則表達式（regex）非常有用。正則表達式指定要忽略的文本模式。範例包括組織的公用電話號碼、組織網域的電子郵件地址，或是組織用於測試的樣本資料。如果 Macie 找到符合受管理或自訂資料識別碼準則的文字，而且該文字也符合允許清單中的規則運算式模式，Macie 就不會在敏感資料發現項目、統計資料和其他類型的結果中報告該文字出現。

除了亞太區域 (大阪) 區域外，您可以 AWS 區域 在 Macie 目前提供的所有區域中建立和使用這兩種類型的允許清單。建立和管理允許清單時，請記住下列選項和需求。另外請注意，不支持郵件地址的允許列表條目和正則表達式模式。

主題

預先定義文字清單的選項和需求

對於這種類型的允許清單，您可以提供以行分隔的純文字檔案，其中列出要忽略的特定字元序列。清單項目通常是您認為不敏感、不太可能變更且不一定遵循特定模式的字詞、片語和其他類型的字元序列。如果您使用這種類型的清單，Amazon Macie 不會報告與清單中項目完全相符的文字出現次數。Macie 會將每個清單項目視為字串常值。

若要使用這種類型的允許清單，請先在文字編輯器中建立清單並將其儲存為純文字檔案。然後將列表上傳到 S3 通用存儲桶。此外，請確定值區和物件的儲存空間和加密設定允許 Macie 擷取和解密清單。然後在 Macie 中創建和配置列表的設置。

在 Macie 中設定設定之後，我們建議您使用一組適用於您帳戶或組織的代表性資料來測試允許清單。若要測試清單，除了通常用於分析資料的受管理資料識別碼和自訂資料識別碼之外，您還可以建立一次性工作，並將工作設定為使用清單。然後，您可以檢視工作的結果，包括敏感資料發現項目、敏感資料探索結果，或兩者兼而有之。如果工作的結果與預期的結果不同，您可以變更並測試清單，直到結果符合您預期的結果為止。

完成設定並測試允許清單之後，您可以建立並設定其他工作以使用該清單，或將其新增至帳戶的自動化敏感資料探索設定。當這些任務開始執行或下一個自動化探索分析週期開始時，Macie 會從 Amazon S3 擷取最新版本的清單，並將其存放在暫存記憶體中。然後，當 Macie 檢查 S3 物件是否存在敏感資料時，會使用此清單的暫存副本。當工作完成執行或分析週期完成時，Macie 會從記憶體中永久刪除其清單複本。該列表不會在 Macie 中持續存在。只有清單的設定會保留在 Macie 中。

> **Important**
>
> 由於預先定義的文字清單不會保留在 Macie 中，因此定期檢查允許清單的狀態非常重要。如果 Macie 無法擷取或剖析您設定工作或自動探索要使用的清單，Macie 就不會使用該清單。這可能會產生非預期的結果，例如針對您在清單中指定的文字找到敏感資料。

主題

- 語法要求
- 儲存需求
- 加密/解密要求
- 設計考量和建議

語法要求

當您建立此類型的允許清單時，請注意清單檔案的下列需求：

- 清單必須儲存為純文字 (`text/plain`) 檔案，例如 .txt、.text 或 .plain 檔案。
- 清單必須使用分行符號來分隔個別項目。例如：

```
Akua Mansa
John Doe
Martha Rivera
425-555-0100
425-555-0101
```

```
425-555-0102
```

Macie 會將每一行視為清單中的單一不同項目。該文件還可以包含空行以提高可讀性。Macie 會在剖析檔案時跳過空白行。

- 每個項目可包含 1-90 UTF 至 8 個字元。
- 每個項目必須完全相符，才能忽略文字。Macie 不支援在項目中使用萬用字元或部分值。Macie 會將每個項目視為字串常值。相符的項目不區分大小寫。
- 檔案可以包含 1 至 10 萬個項目。
- 檔案的總儲存空間大小不得超過 35 MB。

儲存需求

在 Amazon S3 中新增和管理允許清單時，請注意下列儲存需求和建議：

- 區域支援 — 允許清單必須儲存在與您的 Macie 帳戶相 AWS 區域 同的儲存貯體中。如果 Macie 儲存在不同地區，則無法存取允許清單。
- 值區擁有權 — 允許清單必須儲存在您的 AWS 帳戶. 如果您希望其他帳戶使用相同的允許清單，請考慮建立 Amazon S3 複寫規則，將清單複寫到這些帳戶擁有的儲存貯體。如需複寫 S3 物件的相關資訊，請參閱 Amazon 簡單儲存服務使用者指南中的複寫物件。

  此外，您的 AWS Identity and Access Management (IAM) 身分必須具有儲存清單的值區和物件的讀取權限。否則，您將無法建立或更新清單的設定，或使用 Macie 檢查清單狀態。
- 儲存類型和類別 — 允許清單必須儲存在一般用途值區中，而非目錄值區中。此外，必須使用下列其中一種儲存類別來存放：低冗餘 (RRS)、S3 Glacier 即時擷取、S3 智慧型分層、S3 單區域 — IA、S3 標準或 S3 標準 — IA。
- 儲存貯體政策 — 如果您將允許清單儲存在具有限制值區政策的值區中，請確定該政策允許 Macie 擷取清單。若要這麼做，您可以將 Macie 服務連結角色的條件新增至值區政策。如需詳細資訊，請參閱 允許 Macie 存取 S3 儲存貯體和物件。

  此外，還要確保該政策允許您的 IAM 身分對存儲桶具有讀取權限。否則，您將無法建立或更新清單的設定，或使用 Macie 檢查清單狀態。
- 物件路徑 — 如果您在 Amazon S3 中存放多個允許清單，則每個清單的物件路徑必須是唯一的。換句話說，每個允許清單必須單獨存放為其自己的 S3 物件。
- 版本控制 — 當您將允許清單新增至值區時，我們建議您同時啟用值區的版本控制。然後，您可以使用日期和時間值，將清單的版本與使用清單的敏感資料探索工作和自動化敏感資料探索週期的結果建立關聯。這可以幫助您進行數據隱私和保護審核或調查。

- 物件鎖定 — 若要防止允許清單在一段時間內或無限期遭到刪除或覆寫，您可以針對儲存清單的值區啟用物件鎖定。啟用此設定並不會阻止 Macie 存取清單。如需此設定的相關資訊，請參閱 Amazon 簡單儲存服務使用者指南中的使用 S3 物件鎖定。

加密/解密要求

如果您在 Amazon S3 中加密允許清單，Macie 服務連結角色的許可政策通常會授予 Macie 解密清單所需的許可。但是，這取決於所使用的加密類型：

- 如果使用具有 Amazon S3 受管金鑰 (SSE-S3) 的伺服器端加密清單加密，Macie 可以解密清單。您的 Macie 帳戶的服務連結角色會授予 Macie 所需的權限。
- 如果使用伺服器端加密與 AWS 受管理 AWS KMS key (DSSE-KMS 或 SSE-KMS) 加密清單，Macie 可以解密清單。您的 Macie 帳戶的服務連結角色會授予 Macie 所需的權限。
- 如果使用伺服器端加密與客戶管理 AWS KMS key (DSSE-KMS 或 SSE-KMS) 加密清單，則只有當您允許 Macie 使用金鑰時，Macie 才能解密清單。若要了解如何操作，請參閱 允許 Macie 使用客戶管理 AWS KMS key。

> **Note**
>
> 您可以使用外部金鑰存放區 AWS KMS key 中管理的客戶來加密清單。但是，與完全在其中管理的密鑰相比，密鑰可能會慢且不太可靠 AWS KMS。如果延遲或可用性問題導致 Macie 無法解密清單，Macie 在分析 S3 物件時不會使用該清單。這可能會產生非預期的結果，例如針對您在清單中指定的文字找到敏感資料。若要降低此風險，請考慮將清單存放在設定為使用金鑰做為 S3 儲存貯體金鑰的 S3 儲存貯體中。
>
> 如需在外部金鑰存放區使用 KMS 金鑰的詳細資訊，請參閱AWS Key Management Service 開發人員指南中的外部金鑰存放區。如需使用 S3 儲存貯體金鑰的相關資訊，請參閱 Amazon 簡單儲存服務使用者指南中的使用 Amazon S3 儲存貯體金鑰降低 SSE-KMS 的成本。

- 如果使用伺服器端加密使用客戶提供的金鑰 (SSE-C) 或用戶端加密來加密清單，Macie 就無法解密清單。請考慮改用 SSE-S3、DSSE-公司或 SSE-KMS 加密。

如果使用 AWS 受管 KMS 金鑰或客戶受管 KMS 金鑰加密清單，您的 AWS Identity and Access Management (IAM) 身分也必須允許使用金鑰。否則，您將無法建立或更新清單的設定，或使用 Macie 檢查清單狀態。若要瞭解如何檢查或變更 KMS 金鑰的權限，請參閱AWS Key Management Service 開發人員指南 AWS KMS中的金鑰政策。

如需 Amazon S3 資料加密選項的詳細資訊，請參閱 Amazon 簡單儲存服務使用者指南中的使用加密保護資料。

設計考量和建議

一般而言，Macie 會將允許清單中的每個項目視為字串常值。也就是說，Macie 會忽略與允許列表中完全匹配完全匹配的文本的每個出現。相符的項目不區分大小寫。

但是，Macie 使用這些條目作為更大的數據提取和分析框架的一部分。該框架包括機器學習和模式匹配功能，這些功能會因素維度，例如語法和語法變化，在許多情況下還包括關鍵字鄰近性。此架構也會考量 S3 物件的檔案類型或儲存格式。因此，在新增和管理允許清單中的項目時，請記住下列考量和建議。

準備不同的檔案類型和儲存格式

對於非結構化資料 (例如 Adobe 可攜式文件格式 (.pdf) 檔案中的文字，Macie 會忽略完全符合允許清單中完整項目的文字，包括跨越多行或多頁的文字。

對於結構化資料 (例如 CSV 檔案中的單欄資料或 JSON 檔案中以記錄為基礎的資料)，如果所有文字都儲存在單一欄位、儲存格或陣列中，Macie 會忽略完全符合允許清單中完全符合完整項目的文字。此要求不適用於儲存在其他非結構化檔案中的結構化資料，例如 .pdf 檔案中的資料表。

例如，請考慮 CSV 檔案中的下列內容：

```
Name,Account ID
Akua Mansa,111111111111
John Doe,222222222222
```

如果Akua Mansa和John Doe是允許清單中的項目，Macie 會忽略 CSV 檔案中的這些名稱。每個清單項目的完整文字儲存在單一Name欄位中。

相反地，請考慮包含下列欄和欄位的 CSV 檔案：

```
First Name,Last Name,Account ID
Akua,Mansa,111111111111
John,Doe,222222222222
```

如果Akua Mansa和John Doe是允許清單中的項目，Macie 不會忽略 CSV 檔案中的這些名稱。CSV 檔案中的欄位都不包含允許清單中項目的完整文字。

包括常見的變化

新增數值資料、適當名詞、字詞和英數字元序列的常見變化項目。例如，如果您加入的名稱或片語在單字之間只包含一個空格，也會加入在字詞之間包含兩個空格的變體。同樣地，新增包含和不包含特殊字元的字詞和片語，並考慮包含常見的語法和語意變化。

例如，對於美國電話號碼 425-555-0100，您可以將下列項目新增至允許清單：

```
425-555-0100
425.555.0100
(425) 555-0100
+1-425-555-0100
```

對於日期 2022 年 2 月 1 日在跨國情境中，您可以新增包含英文和法文常用語法變化的項目，包括含有和不包含特殊字元的變體：

```
February 1, 2022
1 février 2022
1 fevrier 2022
Feb 01, 2022
1 fév 2022
1 fev 2022
02/01/2022
01/02/2022
```

對於人員的姓名，請包含您不認為敏感的各種形式的名稱項目。例如，包括：名字後面接著姓氏；姓氏後跟名字，名字和姓氏以一個空格分隔；名字和姓氏以兩個空格分隔；以及暱稱。

例如，對於瑪莎·里維拉的名稱，您可以添加：

```
Martha Rivera
Martha  Rivera
Rivera, Martha
Rivera,  Martha
Rivera Martha
Rivera  Martha
```

如果您想要忽略包含許多零件之特定名稱的變體，請建立使用規則運算式的允許清單。例如，對於名稱博士. 瑪莎·利達里維拉, 博士, 你可以使用下面的正則表達式:. `^(Dr. )?Martha\s(Lyda|L\.)?\s?Rivera,?( PhD)?$`

允許清單中規則運算式的選項和需求

對於這種類型的允許清單，您可以指定定義要忽略的文字模式的規則運算式 (regex)，例如組織的公用電話號碼、組織網域的電子郵件地址，或組織用於測試的樣本資料。正則表達式為您不認為敏感的特定類型數據定義了一種常見模式。如果您使用這種類型的允許清單，Amazon Macie 不會報告完全符合指定模式的文字出現次數。與指定要忽略的預先定義文字的允許清單不同，您可以在 Macie 中建立並儲存正則運算式和所有其他清單設定。

當您建立或更新此類型的允許清單時，您可以在儲存清單之前，使用範例資料測試清單的 regex。我們建議您使用多組範例資料來執行此操作。如果您創建了一個過於通用的正則表達式，Macie 可能會忽略您認為敏感的文本的出現情況。如果正則表達式太具體，Macie 可能不會忽略您不認為敏感的文本的出現次數。為了防止格式錯誤或長時間執行的運算式，Macie 也會根據範例文字集合自動編譯和測試 regex，並通知您需要解決的問題。

對於進一步的測試，我們建議您也使用一組適用於您帳戶或組織的代表性資料來測試清單的正則表達式。若要這麼做，您可以建立一次性工作，並將工作設定為使用清單，以及通常用於分析資料的受管理資料識別碼和自訂資料識別碼。然後，您可以檢視工作的結果，包括敏感資料發現項目、敏感資料探索結果，或兩者兼而有之。如果工作的結果與您所期望的不同，則可以更改並測試正則表達式，直到結果達到您所期望的結果。

設定並測試允許清單之後，您可以建立並設定其他工作以使用該清單，或將其新增至帳戶的自動化敏感資料探索設定。當這些工作執行或 Macie 為您的帳戶執行自動探索時，Macie 會使用最新版本的清單正則運算式來分析資料。

主題

- 語法支援與建議
- 範例

語法支援與建議

允許清單可以指定包含多達 512 個字元的規則運算式 (regex)。Macie 支持 Perl 兼容正則表達式（PCRE）庫提供的正則表達式模式語法的子集。在 PCRE 程式庫所提供的結構中，Macie 不支援下列樣式元素：

- 反向引用
- 擷取群組
- 條件式模式
- 內嵌程式碼

- 全域模式旗標/i，例如/m、和 /x
- 遞歸模式
- 正面和負向後視和前瞻零寬度斷言，例如，，和 ?= ?! ?<= ?<!

要為允許列表創建有效的正則表達式模式，還請注意以下提示和建議：

- 錨點 — 只有當您希望模式出現在檔案的開頭^或結尾，而不是行的開頭或結尾時，才使用錨點(或$)。
- 有界重複-出於性能原因，Macie 限制了有界重複組的大小。例如，不\d{100,1000}會在 Macie 中編譯。若要近似此功能，您可以使用開放式重複，例如\d{100,}。
- 大小寫不區分大小寫 — 若要使部分模式不區分大小寫，您可以使用(?i)建構來代替旗標/i。
- 效能 — 無需手動最佳化前置字元或替代項目。例如，變更/hello|hi|hey/為不/h(?:ello|i|ey)/會改善效能。
- 萬用字元 — 基於效能原因，Macie 會限制重複萬用字元的數目。例如，不a*b*a*會在 Macie 中編譯。
- 交替 — 若要在單一允許清單中指定多個模式，您可以使用交替運算子 (|) 來連接模式。如果你這樣做，Macie 使用 OR 邏輯來組合模式並形成一個新的模式。例如，如果您指定(apple|orange)，Macie 會將蘋果和橘色識別為相符項目，並忽略兩個字詞的出現次數。如果串連模式，請務必將串連運算式的整體長度限制為 512 個或更少的字元。

最後，當您開發正則表達式時，請將其設計為適應不同的文件類型和存儲格式。Macie 使用正則表達式作為更大的數據提取和分析框架的一部分。架構會考量 S3 物件的檔案類型或儲存格式。對於結構化資料 (例如 CSV 檔案中的單欄資料或 JSON 檔案中以記錄為基礎的資料)，只有當所有文字都儲存在單一欄位、儲存格或陣列中時，Macie 才會忽略完全符合模式的文字。此要求不適用於儲存在其他非結構化檔案中的結構化資料，例如 Adobe 可攜式文件格式 (.pdf) 檔案中的表格。對於非結構化資料 (例如 .pdf 檔案中的文字)，Macie 會忽略完全符合模式的文字，包括跨越多行或多頁的文字。

範例

下列範例會示範一些常見案例的有效正則運算式模式。

電子郵件地址

如果您使用自訂資料識別碼來偵測電子郵件地址，則可以忽略您不認為機密的電子郵件地址，例如組織的電子郵件地址。

若要忽略特定第二層和頂層網域的電子郵件地址，您可以使用下列模式：

```
[a-zA-Z0-9_.+\\-]+@example\.com
```

其中##是第二級域的名稱，而 *com* 是頂級域名。在這種情況下，馬西匹配並忽略地址，如 johndoe@example.com 和 john.doe@example.com。

若要忽略任何一般頂層網域 (gTLD) 中特定網域的電子郵件地址，例如 .com 或 .gov，您可以使用下列模式：

```
[a-zA-Z0-9_.+\\-]+@example\.[a-zA-Z]{2,}
```

其中##是域的名稱。在這種情況下，馬西匹配並忽略地址，例如 johndoe@example.com，john.doe@example.gov 和。johndoe@example.edu

若要忽略任何一個國家/地區代碼頂級網域 (ccTLD) 中特定網域的電子郵件地址，例如加拿大的 .ca 或澳洲的 .au，您可以使用以下模式：

```
[a-zA-Z0-9_.+\\-]+@example\.(ca|au)
```

其中##是域的名稱，*ca* 和 *au* 是要忽略的特定 ccTLDs 域名。在這種情況下，馬西匹配並忽略地址，如 johndoe@example.ca 和 john.doe@example.au。

若要忽略特定網域和 gTLD 的電子郵件地址，並包含第三層和第四層網域，您可以使用以下模式：

```
[a-zA-Z0-9_.+\\-]+@([a-zA-Z0-9-]+\.)?[a-zA-Z0-9-]+\.example\.com
```

其中，##域名，*com* 是 gTLD 名。在這種情況下，馬西匹配並忽略地址，如 johndoe@www.example.com 和 john.doe@www.team.example.com。

電話號碼

Macie 提供託管數據標識符，可以檢測多個國家和地區的電話號碼。若要忽略某些電話號碼，例如組織的免付費號碼或公用電話號碼，您可以使用下列模式。

若要忽略免付費電話，使用 800 區碼並格式化為 (800) ##-#### 的美國電話號碼：

```
^\(?800\)?[ -]?\d{3}[ -]?\d{4}$
```

若要忽略免付費電話，使用 888 區號並格式化為 (888) ##-##### 的美國電話號碼：

```
^\(?888\)?[ -]?\d{3}[ -]?\d{4}$
```

若要忽略 10 位數字，包含 33 個國家/地區代碼的法文電話號碼並格式化為 +33 ## ## ## ## ##：

```
^\+33 \d( \d\d){4}$
```

若要忽略使用特定區域和交換代碼的美國和加拿大電話號碼，請不要包含國碼，並且格式為 (###) ###-####：

```
^\(?123\)?[ -]?555[ -]?\d{4}$
```

其中 *123* 是區號，*555* 是交換代碼。

若要忽略使用特定區域和交換代碼的美國和加拿大電話號碼，請加入國碼，並格式化為 +1 (###) ###-#-###：

```
^\+1\(?123\)?[ -]?555[ -]?\d{4}$
```

其中 *123* 是區號，*555* 是交換代碼。

在 Amazon Macie 中創建和管理允許列表

在 Amazon Macie 中，允許清單定義了您希望 Macie 在檢查 Amazon Simple Storage Service (Amazon S3) 物件中是否有敏感資料時忽略的特定文字或文字模式。如果文字與允許清單中的項目或模式相符，Macie 不會在敏感資料發現項目、統計資料或其他類型的結果中報告文字，即使該文字符合受管理資料識別碼或自訂資料識別碼的準則。

您可以在 Macie 中建立和管理下列類型的允許清單。

預定義文字

使用這種類型的清單來指定不敏感、不太可能變更且不一定遵循一般模式的字元序列的字詞、片語和其他類型的字元序列。範例包括貴組織的公開代表姓名、特定電話號碼，以及貴組織用於測試的特定範例資料。如果您使用這種類型的清單，Macie 會忽略與清單中項目完全相符的文字。

對於這種類型的清單，您可以建立以行分隔的純文字檔案，其中列出要忽略的特定文字。然後，您將檔案儲存在 S3 儲存貯體中，並設定 Macie 的設定，以存取儲存貯體中的清單。然後，您可以建立並設定敏感資料探索工作以使用清單，或將清單新增至您帳戶的自動化敏感資料探索設定。當每個任務開始執行或下一個自動探索分析週期開始時，Macie 會從 Amazon S3 擷取最新版本的清單。然後，當 Macie 檢查 S3 物件是否存在敏感資料時，會使用該清單版本。如果 Macie 找到與清單中項目完全相符的文字，Macie 就不會將該出現的文字報告為敏感資料。

Regular expression (常規表達式)

使用這種類型的列表來指定定義要忽略的文本模式的正則表達式（regex）。範例包括組織的公用電話號碼、組織網域的電子郵件地址，以及組織用於測試的樣本資料。如果您使用這種類型的列表，Macie 會忽略完全符合列表定義的正則表達式模式的文本。

對於這種類型的列表，您可以創建一個正則表達式，該正則表達式定義不敏感但變化或可能發生變化的文本的常見模式。與預定義文本列表不同，您可以在 Macie 中創建並存儲正則表達式和所有其他列表設置。然後，您可以建立並設定敏感資料探索工作以使用清單，或將清單新增至您帳戶的自動化敏感資料探索設定。當這些工作執行或 Macie 為您的帳戶執行自動探索時，Macie 會使用最新版本的清單正則運算式來分析資料。如果 Macie 找到完全符合清單所定義模式的文字，Macie 就不會將出現的文字報告為敏感資料。

如需每種清單類型的詳細需求、建議和範例，請參閱允許清單選項和需求。您可以在每個支援的帳戶中建立多達 10 個允許清單 AWS 區域，最多五個指定預先定義文字的允許清單，以及最多五個指定規則運算式的允許清單。除了亞太區域（大阪）地區以外，您可以 AWS 區域 在 Macie 目前所有可用的地方創建和使用允許列表。

若要建立和管理允許清單，您可以使用 Amazon Macie 主控台或 Amazon Macie API。下列主題說明如何進行。對於 API，主題包括如何使用 AWS Command Line Interface (AWS CLI) 執行這些工作的範例。您也可以使用目前版本的其他 AWS 命令列工具或 AWS SDK，或直接將 HTTPS 要求傳送至 Macie 來執行這些工作。如需 AWS 工具和 SDK 的相關資訊，請參閱要建置的工具。 AWS

主題

- 建立允許清單
- 檢查允許清單的狀態
- 變更允許清單
- 刪除允許清單

建立允許清單

在 Amazon Macie 中建立允許清單的方式取決於您要建立的清單類型。允許列表可以是列出要忽略的預定義文本的文件，也可以是定義要忽略的文本模式的正則表達式（regex）。選擇您要建立之清單類型的區段。

預定義文字

在 Macie 中建立此類型的允許清單之前，請先執行下列步驟：

1. 透過使用文字編輯器，建立以行分隔的純文字檔案，其中列出要忽略的特定文字，例如 .txt、.text 或 .plain 檔案。如需詳細資訊，請參閱 預先定義文字清單的語法需求。
2. 將檔案上傳到 S3 一般用途儲存貯體，並記下儲存貯體和物件的名稱。在 Macie 中進行設定時，您需要輸入這些名稱。

3. 確定 S3 儲存貯體和物件的設定允許您和 Macie 從儲存貯體擷取清單。如需詳細資訊，請參閱 預先定義文字清單的儲存需求。
4. 如果您已加密 S3 物件，請確定已使用允許您和 Macie 使用的金鑰加密該物件。如需詳細資訊，請參閱 預定義文本列表的加密/解密要求。

完成這些步驟後，您就可以在 Macie 中設定清單的設定了。您可以使用亞馬遜 Macie 控制台或亞馬 Amazon Macie API 來配置設置。

Console

請依照下列步驟使用 Amazon Macie 主控台設定允許清單的設定。

在 Macie 中設定允許清單設定

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 在功能窗格的 [設定] 下，選擇 [允許清單]。
3. 在 [允許清單] 頁面上，選擇 [建立]。
4. 在選取清單類型下，選擇預先定義的文字。
5. 在 [清單設定] 下，使用下列選項輸入允許清單的其他設定：

   - 在「名稱」中，輸入清單的名稱。該名稱最多可包含 128 個字元。
   - 在「說明」中，選擇性地輸入清單的簡短描述。該描述最多可包含 512 個字元。
   - 對於 S3 儲存貯體名稱，請輸入存放清單的儲存貯體名稱。

     在 Amazon S3 中，您可以在儲存貯體屬性的「名稱」欄位中找到此值。此值區分大小寫。此外，輸入名稱時請勿使用萬用字元或部分值。
   - 對於 S3 物件名稱，請輸入存放清單的 S3 物件名稱。

     在 Amazon S3 中，您可以在物件屬性的「金鑰」欄位中找到此值。例如，如果名稱包含路徑，請務必在輸入名稱時包含完整路徑**allowlists/macie/mylist.txt**。此值區分大小寫。此外，輸入名稱時請勿使用萬用字元或部分值。
6. (選擇性) 在「標籤」下，選擇「新增標籤」，然後輸入最多 50 個標籤以指派給允許清單。

   標籤是您定義並指派給特定 AWS 資源類型的標籤。每個標籤都包含必要的標籤鍵和一個可選的標籤值。標籤可協助您以不同的方式識別、分類及管理資源，例如依用途、擁有者、環境或其他條件。如需進一步了解，請參閱標記亞馬遜麥西資源。
7. 當您完成時，請選擇建立。

馬西測試列表的設置。Macie 還驗證它是否可以從 Amazon S3 檢索列表和解析列表的內容。如果發生錯誤，Macie 會顯示描述錯誤的訊息。如需可協助您疑難排解錯誤的詳細資訊，請參閱預先定義文字清單的選項和需求。解決任何錯誤後，您可以儲存清單的設定。

API

若要以程式設計方式設定允許清單設定，請使用 Amazon Macie API 的CreateAllowList操作，並為所需參數指定適當的值。

對於`criteria`參數，請使用`s3WordsList`物件來指定 S3 儲存貯體 (`bucketName`) 的名稱和存放清單的 S3 物件 (`objectKey`) 名稱。若要判斷儲存貯體名稱，請參閱 Amazon S3 中的`Name`欄位。若要判斷物件名稱，請參閱 Amazon S3 中的`Key`欄位。請注意，這些值區分大小寫。此外，當您指定這些名稱時，請勿使用萬用字元或部分值。

若要使用配置設定 AWS CLI，請執行命create-allow-list令並為所需參數指定適當的值。下列範例說明如何針對存放在名為 *DOC/EXAMPLE-* BUCKET 的 S3 儲存貯體中的允許清單進行設定。儲存清單的 S3 物件的名稱為 *allowlists/macie/mylist.txt*。

此範例已針對 Linux、macOS 或 Unix 格式化，並使用反斜線 (\) 行接續字元來改善可讀性。

```
$ aws macie2 create-allow-list \
--criteria '{"s3WordsList":{"bucketName":"DOC-EXAMPLE-
BUCKET","objectKey":"allowlists/macie/mylist.txt"}}' \
--name my_allow_list \
--description "Lists public phone numbers and names for Example Corp."
```

此範例針對 Microsoft Windows 進行格式化，並使用脫字符號 (^) 行接續字元來提高可讀性。

```
C:\> aws macie2 create-allow-list ^
--criteria={\"s3WordsList\":{\"bucketName\":\"DOC-EXAMPLE-BUCKET\",\"objectKey\":
\"allowlists/macie/mylist.txt\"}} ^
--name my_allow_list ^
--description "Lists public phone numbers and names for Example Corp."
```

當您提交請求時，Macie 會測試列表的設置。Macie 還驗證它是否可以從 Amazon S3 檢索列表和解析列表的內容。如果發生錯誤，您的要求會失敗，而 Macie 會傳回描述錯誤的訊息。如需可協助您疑難排解錯誤的詳細資訊，請參閱預先定義文字清單的選項和需求。

如果 Macie 可以擷取和剖析清單，您的要求就會成功，而且您會收到類似下列內容的輸出。

```
{
```

```
    "arn": "arn:aws:macie2:us-west-2:123456789012:allow-list/
nkr81bmtu2542yyexample",
    "id": "nkr81bmtu2542yyexample"
}
```

其中arn是建立之允許清單的 Amazon 資源名稱 (ARN)，id是清單的唯一識別碼。

儲存清單設定後，您可以建立並設定敏感資料探索工作以使用清單，或將清單新增至自動化的敏感資料探索設定。每當這些任務開始執行或自動探索分析週期開始時，Macie 都會從 Amazon S3 擷取最新版本的清單。然後，Macie 會在分析資料時使用該清單版本。

Regular expression (常規表達式)

當您建立指定規則運算式 (regex) 的允許清單時，您可以直接在 Macie 中定義正則運算式和所有其他清單設定。Macie 支持 Perl 兼容正則表達式（PCRE）庫提供的正則表達式模式語法的子集。如需詳細資訊，請參閱 語法支援與建議。

您可以通過使用亞馬遜 Macie 控制台或亞馬 Amazon Macie API 創建這種類型的列表。

Console

請依照下列步驟使用 Amazon Macie 主控台建立允許清單。

建立允許清單

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 在功能窗格的 [設定] 下，選擇 [允許清單]。
3. 在 [允許清單] 頁面上，選擇 [建立]。
4. 在 [選取清單類型] 下，選擇 [規則運算式]。
5. 在 [清單設定] 下，使用下列選項輸入允許清單的其他設定：
   - 在「名稱」中，輸入清單的名稱。該名稱最多可包含 128 個字元。
   - 在「說明」中，選擇性地輸入清單的簡短描述。該描述最多可包含 512 個字元。
   - 針對規則運算式，請輸入定義要忽略之文字模式的 regex。正則表達式可以包含多達 512 個字符。
6. (選擇性) 對於「評估」，請在「範例資料」方塊中輸入最多 1,000 個字元，然後選擇「測試」來測試正則運算式。Macie 會評估範例資料，並報告符合正則運算式的文字出現次數。您可以根據需要重複此步驟，以優化和優化正則表達式。

> **Note**
>
> 我們建議您使用多組樣本數據來測試和優化正則表達式。如果您創建了一個過於通用的正則表達式，Macie 可能會忽略您認為敏感的文本的出現情況。如果正則表達式太具體，Macie 可能不會忽略您不認為敏感的文本的出現次數。

7. (選擇性) 在「標籤」下，選擇「新增標籤」，然後輸入最多 50 個標籤以指派給允許清單。

   標籤是您定義並指派給特定 AWS 資源類型的標籤。每個標籤都包含必要的標籤鍵和一個可選的標籤值。標籤可協助您以不同的方式識別、分類及管理資源，例如依用途、擁有者、環境或其他條件。如需進一步了解，請參閱標記亞馬遜麥西資源。

8. 當您完成時，請選擇建立。

馬西測試列表的設置。Macie 還測試正則表達式以驗證它是否可以編譯表達式。如果發生錯誤，Macie 會顯示描述錯誤的訊息。如需可協助您疑難排解錯誤的詳細資訊，請參閱允許清單中規則運算式的選項和需求。解決任何錯誤後，您可以儲存允許清單。

API

在 Macie 中建立這種類型的允許清單之前，我們建議您使用多組範例資料來測試和調整規則運算式。如果您創建了一個過於通用的正則表達式，Macie 可能會忽略您認為敏感的文本的出現情況。如果正則表達式太具體，Macie 可能不會忽略您不認為敏感的文本的出現次數。

若要使用 Macie 測試運算式，您可以使用 Amazon Macie API 的TestCustomDataIdentifier作業，或執行命令。 AWS CLItest-custom-data-identifierMacie 會使用相同的基礎程式碼來編譯允許清單和自訂資料識別碼的運算式。如果您以這種方式測試表示式，請務必僅為`regex`和`sampleText`參數指定值。否則，您將收到不正確的結果。

當您準備好建立此類型的允許清單時，請使用 Amazon Macie API 的CreateAllowList作業，並為所需參數指定適當的值。對於`criteria`參數，請使用`regex`欄位來指定定義要忽略之文字模式的規則運算式。該運算式最多可包含 512 個字元。

若要使用建立此類型的清單 AWS CLI，請執行create-allow-list命令並為所需參數指定適當的值。下列範例會建立名為 *my_allow_* list 的允許清單。正則表達式旨在忽略自定義數據標識符否則可能檢測到該`example.com`域的所有電子郵件地址。

此範例已針對 Linux、macOS 或 Unix 格式化，並使用反斜線 (\) 行接續字元來改善可讀性。

```
$ aws macie2 create-allow-list \
```

```
--criteria '{"regex":"[a-z]@example.com"}' \
--name my_allow_list \
--description "Ignores all email addresses for Example Corp."
```

此範例針對 Microsoft Windows 進行格式化，並使用脫字符號 (^) 行接續字元來提高可讀性。

```
C:\> aws macie2 create-allow-list ^
--criteria={\"regex\":\"[a-z]@example.com\"} ^
--name my_allow_list ^
--description "Ignores all email addresses for Example Corp."
```

當您提交請求時，Macie 會測試列表的設置。Macie 還測試正則表達式以驗證它是否可以編譯表達式。如果發生錯誤，請求會失敗，Macie 會傳回描述錯誤的訊息。如需可協助您疑難排解錯誤的詳細資訊，請參閱允許清單中規則運算式的選項和需求。

如果 Macie 可以編譯運算式，請求就會成功，而且您會收到類似下列內容的輸出：

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:allow-list/
km2d4y22hp6rv05example",
    "id": "km2d4y22hp6rv05example"
}
```

其中`arn`是建立之允許清單的 Amazon 資源名稱 (ARN)，`id`是清單的唯一識別碼。

儲存清單後，您可以建立並設定敏感資料探索工作以使用該清單，或將其新增至自動化的敏感資料探索設定。當這些工作執行或 Macie 為您的帳戶執行自動探索時，Macie 會使用最新版本的清單正則運算式來分析資料。

檢查允許清單的狀態

定期檢查允許清單的狀態很重要。否則，錯誤可能會導致 Amazon Macie 產生非預期的分析結果，例如針對您在允許清單中指定的文字發現的敏感資料。

如果您將敏感資料探索工作設定為使用允許清單，且 Macie 在工作開始執行時無法存取或使用該清單，則工作會繼續執行。但是，Macie 在分析 S3 物件時不會使用清單。同樣地，如果自動化敏感資料探索的分析週期開始，而 Macie 無法存取或使用指定的允許清單，則分析會繼續進行，但 Macie 不會使用該清單。

指定正則表達式（regex）的允許列表不太可能發生錯誤。這部分是因為 Macie 會在您創建或更新列表的設置時自動測試正則表達式。此外，您可以將正則表達式和所有其他列表設置存儲在 Macie 中。

不過，指定預先定義文字的允許清單可能會發生錯誤，部分原因是您將清單存放在 Amazon S3 而非 Macie。錯誤的常見原因是：

- S3 儲存貯體或物件已刪除。
- S3 儲存貯體或物件已重新命名，而且 Macie 中的清單設定不會指定新名稱。
- S3 儲存貯體的許可設定已變更，而 Macie 會失去儲存貯體和物件的存取權。
- S3 儲存貯體的加密設定已變更，Macie 無法解密儲存清單的物件。
- 加密金鑰的政策已變更，而 Macie 會失去對金鑰的存取權。Macie 無法解密存儲列表的 S3 對象。

> **Important**
>
> 由於這些錯誤會影響您的分析結果，因此建議您定期檢查允許清單的狀態。如果您變更存放允許清單的 S3 儲存貯體的許可或加密設定，或變更用於加密清單的 AWS Key Management Service (AWS KMS) 金鑰的政策，我們也建議您這麼做。

您可以使用亞馬遜 Macie 主控台或亞馬 Amazon Macie API 來檢查允許清單的狀態。如需可協助您疑難排解發生錯誤的詳細資訊，請參閱預先定義文字清單的選項和需求。

Console

請按照以下步驟使用 Amazon Macie 主控台檢查允許清單的狀態。

檢查允許清單的狀態

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 在功能窗格的 [設定] 下，選擇 [允許清單]。
3. 在 [允許清單] 頁面上，選擇 [重新整理]
   ()。Ma
   會測試所有允許清單的設定，並更新 [狀態] 欄位以指出每個清單的目前狀態。

   如果清單指定規則運算式，則其狀態通常為 OK。這意味著馬西可以編譯表達式。如果清單指定了預先定義的文字，其狀態可以是下列任一值。

   OK (確定)

   Macie 可以檢索和解析列表的內容。

存取遭拒

Macie 不允許訪問存儲列表的 S3 對象。Amazon S3 拒絕了檢索對象的請求。如果物件是由受管理的 Macie 不允許使用的客戶進行加密 AWS KMS key ，則清單也可以具有此狀態。

若要解決此錯誤，請檢閱值區政策以及值區和物件的其他權限設定。確保 Macie 被允許訪問和檢索對象。如果物件使用客戶管理的 AWS KMS 金鑰加密，請同時檢閱金鑰政策，並確保允許 Macie 使用金鑰。

錯誤

當 Macie 嘗試擷取或剖析清單的內容時，就會發生暫時性或內部錯誤。如果允許清單使用 Amazon S3 和 Macie 無法存取或使用的加密金鑰加密，則允許清單也可能具有此狀態。

若要解決此錯誤，請等待幾分鐘，然後再次選擇 refresh
()。
如果狀態繼續為「錯誤」，請檢查 S3 物件的加密設定。確保使用 Amazon S3 和 Macie 可以存取和使用的金鑰對物件進行加密。

對象是空的

Macie 可以從 Amazon S3 檢索列表，但列表不包含任何內容。

若要解決此錯誤，請從 Amazon S3 下載物件，並確保其中包含正確的項目。如果輸入正確，請在 Macie 中檢閱清單的設定。請確定指定的值區和物件名稱正確無誤。

找不到物件

該列表在 Amazon S3 中不存在。

若要解決此錯誤，請在 Macie 中檢閱清單的設定。請確定指定的值區和物件名稱正確無誤。

超過配額

馬西可以在 Amazon S3 訪問列表。不過，清單中的項目數目或清單的儲存大小超過允許清單的配額。

若要解決此錯誤，請將清單分成多個檔案。請確定每個檔案包含少於 100,000 個項目。另外，請確保每個文件的大小小於 35 MB。然後，將每個文件上傳到 Amazon S3。完成後，

請在 Macie 中為每個檔案設定允許清單設定。在每個支援的預先定義文字中，您可以有多達五個清單 AWS 區域。

節流

Amazon S3 限制了請求以檢索列表。

若要解決此錯誤，請等待幾分鐘，然後再次選擇 refresh
()。

拒絕使用者存取

Amazon S3 拒絕了檢索對象的請求。如果指定的對象存在，則不允許您訪問它，或者使用您不允許使用的密 AWS KMS 鑰對其進行加密。

若要解決此錯誤，請與您的 AWS 管理員合作，確定清單的設定指定了正確的值區和物件名稱，並且您具有值區和物件的讀取權限。如果物件已加密，也請確保此物件使用允許您使用的金鑰加密。

4. 若要檢閱特定清單的設定和狀態，請選擇清單名稱。

API

若要以程式設計方式檢查允許清單的狀態，請使用 Amazon Macie API 的GetAllowList作業，或針對 AWS CLI執行命get-allow-list令。

對於id參數，請為您要檢查其狀態的允許清單指定唯一識別碼。要獲取此標識符，您可以使用該ListAllowLists操作。此ListAllowLists作業會擷取有關您帳戶之所有允許清單的資訊。如果您使用的是 AWS CLI，您可以執行命list-allow-lists令來擷取此資訊。

當您提交GetAllowList要求時，Macie 會測試允許清單的所有設定。如果設置指定了正則表達式（regex），Macie 會驗證它是否可以編譯表達式。如果設定指定了預先定義的文字清單，Macie 會驗證它是否可以擷取和剖析清單。

然後 Macie 會傳回提供允許清單詳細資訊的`GetAllowListResponse`物件。在`GetAllowListResponse`物件中，`status`物件會指示清單的目前狀態：狀態碼 (`code`)，以及清單狀態碼的簡短描述 (`description`)。

如果允許列表指定了正則表達式，則狀態代碼通常是`OK`並且沒有關聯的描述。這意味著馬西成功地編譯了表達式。

如果允許清單指定預先定義的文字，狀態碼會根據測試結果而有所不同：

- 如果 Macie 成功擷取並剖析清單，則狀態碼為0K且沒有關聯的描述。
- 如果發生錯誤導致 Macie 無法擷取或剖析清單，狀態碼和說明會指出發生錯誤的性質。

如需可能的狀態碼清單和每個狀態碼的說明，請參閱 Amazon Macie API 參考AllowListStatus中的。

變更允許清單

建立允許清單後，您可以在 Amazon Macie 中變更清單的大部分設定。例如，您可以變更清單的名稱和說明，也可以新增和編輯清單的標籤。唯一無法變更的設定是清單類型。例如，如果現有的允許清單指定規則運算式，則無法將其類型變更為預先定義的文字。

如果允許清單指定預先定義的文字，您也可以變更清單中的項目。若要這麼做，請更新包含項目的檔案，然後將檔案的新版本上傳到 Amazon S3。下次 Macie 準備使用清單時，Macie 會從 Amazon S3 擷取檔案的最新版本。上傳新檔案時，請確保將其存放在相同的 S3 儲存貯體和物件中。或者，如果您變更值區或物件的名稱，請務必在 Macie 中更新清單的設定。

您可以使用亞馬遜 Macie 主控台或亞馬 Amazon Macie API 來變更允許清單的設定。

Console

請依照下列步驟使用 Amazon Macie 主控台變更允許清單的設定。

變更允許清單

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 在功能窗格的 [設定] 下，選擇 [允許清單]。
3. 在 [允許清單] 頁面上，選擇您要變更的允許清單名稱。允許清單頁面隨即開啟，並顯示清單的目前設定。
4. 若要指派或編輯允許清單的標籤，請在「標籤」區段中選擇「管理標籤」。然後視需要變更標籤。完成後，請選擇儲存。
5. 若要變更允許清單的其他設定，請在 [清單設定] 區段中選擇 [編輯]。然後變更您想要的設定：
   - 名稱 — 輸入清單的新名稱。該名稱最多可包含 128 個字元。
   - 描述 — 輸入清單的新描述。該描述最多可包含 512 個字元。
   - 如果允許清單指定預先定義的文字：
     - S3 儲存貯體名稱 — 輸入目前存放清單的儲存貯體名稱。

在 Amazon S3 中，您可以在儲存貯體屬性的「名稱」欄位中找到此值。此值區分大小寫。此外，輸入名稱時請勿使用萬用字元或部分值。

- S3 物件名稱 — 輸入目前存放清單的 S3 物件名稱。

  在 Amazon S3 中，您可以在物件屬性的「金鑰」欄位中找到此值。例如，如果名稱包含路徑，請務必在輸入名稱時包含完整路徑**allowlists/macie/mylist.txt**。此值區分大小寫。此外，輸入名稱時請勿使用萬用字元或部分值。

- 如果允許清單指定規則運算式 (regex)，請在「規則運算式」方塊中輸入新的 regex。正則表達式可以包含多達 512 個字符。

  輸入新的正則表達式後，可以選擇對其進行測試。若要這麼做，請在 [範例資料] 方塊中輸入最多 1,000 個字元，然後選擇 [測試]。Macie 會評估範例資料，並報告符合正則運算式的文字出現次數。在儲存變更之前，您可以根據需要重複此步驟，以精簡和最佳化正則表達式。

完成變更設定後，請選擇 [儲存]。

馬西測試列表的設置。對於預先定義的文字清單，Macie 也會驗證它是否可以從 Amazon S3 擷取清單並剖析清單的內容。對於正則表達式，Macie 還驗證它是否可以編譯表達式。如果發生錯誤，Macie 會顯示描述錯誤的訊息。如需可協助您疑難排解錯誤的詳細資訊，請參閱允許清單選項和需求。解決任何錯誤後，您可以儲存變更。

API

若要以程式設計方式變更允許清單，請使用 Amazon Macie API 的UpdateAllowList作業，或針對 AWS CLI執行命update-allow-list令。在您的請求中，使用支援的參數為您要變更的每個設定指定一個新值。請注意，`criteria`、`id`、和`name`參數是必需的。如果您不想變更必要參數的值，請指定參數的目前值。

例如，下列命令會變更現有允許清單的名稱和描述。此範例已針對 Microsoft Windows 進行格式化，並使用脫字元 (^) 行接續字元來提高可讀性。

```
C:\> aws macie2 update-allow-list ^
--id km2d4y22hp6rv05example ^
--name my_allow_list-email ^
--criteria={\"regex\":\"[a-z]@example.com\"} ^
--description "Ignores all email addresses for the example.com domain"
```

其中：

- *km2d4y22hp6* rv05 範例是該清單的唯一識別碼。
- *my_allow_list-########*的新名稱。
- *[a-z] @example .com* 是列表的標準，一個正則表達式。
- *## example.com ##########*是清單的新描述。

當您提交請求時，Macie 會測試列表的設置。如果清單指定了預先定義的文字，這包括驗證 Macie 可以從 Amazon S3 擷取清單並剖析清單的內容。如果列表指定了正則表達式，這包括驗證 Macie 是否可以編譯表達式。

如果 Macie 測試設定時發生錯誤，您的要求會失敗，而 Macie 會傳回描述錯誤的訊息。如需可協助您疑難排解錯誤的詳細資訊，請參閱允許清單選項和需求。如果要求因其他原因而失敗，Macie 會傳回 HTTP 4 xx 或 500 回應，指出作業失敗的原因。

如果您的請求成功，Macie 會更新列表的設置，並且您會收到類似以下內容的輸出。

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:allow-list/
km2d4y22hp6rv05example",
    "id": "km2d4y22hp6rv05example"
}
```

其中`arn`是已更新之允許清單的 Amazon 資源名稱 (ARN)，`id`是清單的唯一識別碼。

刪除允許清單

當您在 Amazon Macie 中刪除允許清單時，會永久刪除清單的所有設定。刪除這些設定後無法復原。如果設定指定您存放在 Amazon S3 中的預先定義文字清單，Macie 不會刪除存放清單的 S3 物件。只會刪除 Macie 中的設定。

如果您將敏感資料探查工作設定為使用允許清單，並隨後刪除該清單，則工作將會依排程執行。不過，您的工作結果 (包括敏感資料發現項目和敏感資料探索結果) 都可能會報告您先前在允許清單中指定的文字。同樣地，如果您將自動化敏感資料探索設定為使用清單，並隨後刪除清單，則會繼續進行每日分析週期。不過，敏感資料發現項目、統計資料或其他類型的結果可能會報告您先前在允許清單中指定的文字。

刪除允許清單之前，建議您先檢閱工作清單，以識別使用該清單且排定在 future 執行的工作。在詳細目錄中，詳細資料面板會指出工作是否設定為使用任何允許清單，如果有，則指出哪些允許清單。此外，請檢查您的自動化敏感資料探索設定。您可能會判斷最好是變更清單，而不是刪除清單。

當您嘗試刪除允許清單時，Macie 會檢查所有工作的設定，作為額外的保護措施。如果您將工作設定為使用清單，且這些工作的狀態為「完成」或「已取消」以外的狀態，除非您提供其他確認，否則 Macie 不會刪除該清單。

您可以使用亞馬遜 Macie 主控台或亞馬 Amazon Macie API 刪除允許清單。

Console

請依照下列步驟使用 Amazon Macie 主控台刪除允許清單。

刪除允許清單

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 在功能窗格的 [設定] 下，選擇 [允許清單]。
3. 在 [允許清單] 頁面上，選取要刪除之允許清單的核取方塊。
4. 在操作功能表上，選擇刪除。
5. 出現確認提示時，請輸入 **delete**，然後選擇 Delete (刪除)。

API

若要以程式設計方式刪除允許清單，請使用 Amazon Macie API 的DeleteAllowList作業。對於`id`參數，請為允許清單指定要刪除的唯一識別碼。您可以通過使用ListAllowLists操作獲取此標識符。此ListAllowLists作業會擷取有關您帳戶之所有允許清單的資訊。如果您使用的是 AWS CLI，您可以執行命list-allow-lists令來擷取此資訊。

對於`ignoreJobChecks`參數，請指定是否強制刪除清單，即使將敏感資料探索工作設定為使用清單：

- 如果您指定`false`，Macie 會檢查所有狀態為`COMPLETE`或`CANCELLED`以外的工作的設定。如果這些工作均未設定為使用清單，Macie 會永久刪除該清單。如果這些工作中有任何設定為使用清單，Macie 會拒絕您的要求，並傳回 HTTP 400 (`ValidationException`) 錯誤訊息。錯誤訊息會指出最多 200 個工作的適用工作數目。
- 如果您指定`true`，Macie 會永久刪除清單，而不檢查任何工作的設定。

若要使用刪除允許清單 AWS CLI，請執行delete-allow-list命令。例如：

```
C:\> aws macie2 delete-allow-list --id nkr81bmtu2542yyexample --ignore-job-checks
 false
```

其中 *nkr81bmtu2542 ###*是允許清單刪除的唯一識別碼。

如果您的請求成功，馬西會返回一個空的 HTTP 200 響應。否則，馬西會傳回 HTTP 4 xx 或 500 回應，指出作業失敗的原因。

如果允許清單指定了預先定義的文字，您可以選擇性地刪除存放清單的 S3 物件。但是，保留此物件有助於確保您擁有不可變的敏感資料發現歷史記錄，以及資料隱私權和保護稽核或調查的探索結果。

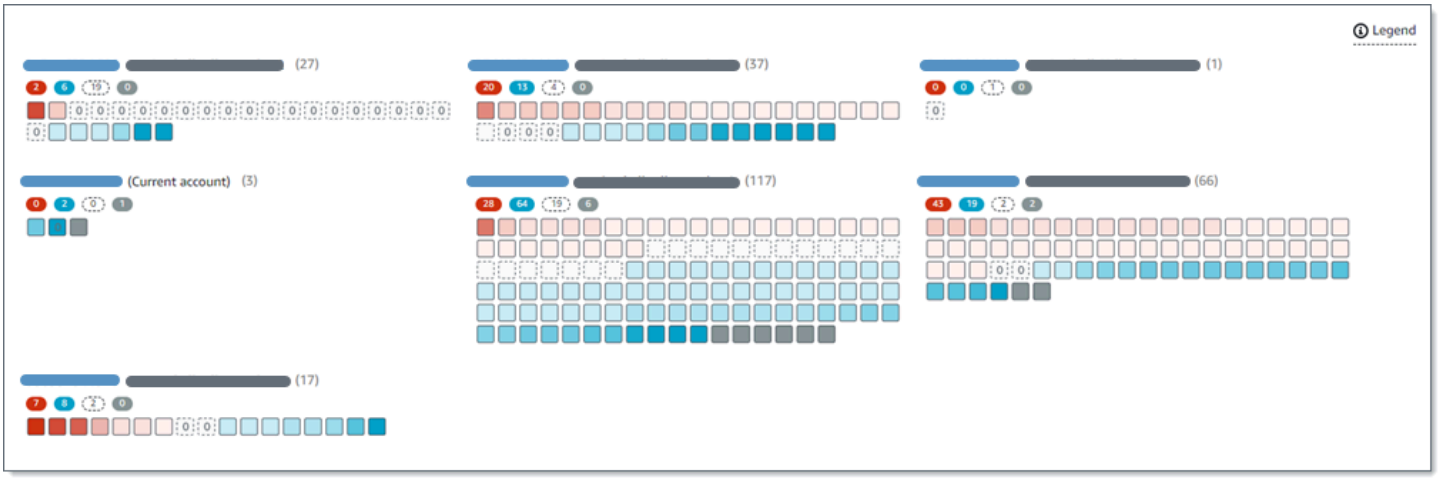
使用 Amazon Macie 執行自動化敏感資料探索

若要廣泛瞭解敏感資料可能存放在 Amazon Simple Storage Service (Amazon S3) 資料資產中的位置，請設定 Amazon Macie 為您的帳戶或組織執行自動化敏感資料探索。透過自動化的敏感資料探索功能，Macie 會持續評估您的 S3 儲存貯體庫存，並使用取樣技術來識別和選取儲存貯體中代表性的 S3 物件。然後，Macie 會擷取並分析選取的物件，檢查它們是否有敏感資料。

根據預設，Macie 會從所有 S3 一般用途儲存貯體中選取並分析物件。如果您是組織的 Macie 管理員，這會包含您的成員帳戶所擁有的值區中的物件。您可以排除特定的值區 (例如，通常儲存記錄資料的值區) 來調整分析範圍。 AWS 如果您是 Macie 管理員，則另一個選項是針對組織中的個別帳戶啟用或停用自動化敏感資料探索功能。 case-by-case

您可以調整分析以專注於特定類型的敏感資料。根據預設，Macie 會使用我們建議用於自動化敏感資料探索的一組受管資料識別碼來分析 S3 物件。若要自訂分析，請設定 Macie 使用 Macie 提供的特定受管理資料識別碼、您定義的自訂資料識別碼，或兩者的組合。您也可以將 Macie 配置為使用您指定的允許清單來精簡分析。

隨著分析每天進行，Macie 會產生找到的敏感資料及其執行的分析記錄：敏感資料發現項目，報告 Macie 在個別 S3 物件中找到的敏感資料，以及敏感資料探索結果，記錄有關個別 S3 物件分析的詳細資料。Macie 也會更新提供有關 Amazon S3 資料的統計資料、庫存資料和其他資訊。例如，主控台上的互動式熱圖可提供資料資產中資料敏感度的視覺化呈現方式：



這些功能旨在協助您評估 Amazon S3 資料資產中的資料敏感度，並深入研究和評估個別帳戶、儲存貯體和物件。它們還可以透過執行敏感資料探索工作，協助您判斷在何處執行更深入、更即時的分析。結合 Macie 提供有關 Amazon S3 資料安全性和隱私權的資訊，您也可以使用這些功能來識別可能需要立即修復的案例，例如 Macie 在其中找到敏感資料的可公開存取儲存貯體。

若要設定和管理自動化敏感資料探索，您的帳戶必須是組織的 Macie 管理員帳戶或獨立 Macie 帳戶。

主題

自動化敏感資料探索如何運作

當您為您的帳戶啟用 Amazon Macie 時 AWS 帳戶，Macie 會在當前帳戶中為您的帳戶創建一個 AWS Identity and Access Management （IAM）服務鏈接角色。 AWS 區域此角色的權限原則允許 Macie 代表您呼叫其他 AWS 資源 AWS 服務 並監視資源。透過使用此角色，Macie 會產生並維護區域中 Amazon Simple Storage Service (Amazon S3) 一般用途儲存貯體的完整庫存。詳細目錄包含儲存貯體中每個 S3 儲存貯體和物件的相關資訊。如果您是某個組織的 Macie 管理員，則您的庫存管理員會包含您會員帳戶所擁有的值區的相關資訊。如需詳細資訊，請參閱 管理多個 帳戶。

如果您啟用自動化敏感資料探索，Macie 會每天評估您的庫存資料，以識別符合自動探索資格的 S3 物件。作為評估的一部分，Macie 還選擇了代表性對象的樣本進行分析。然後，Macie 會擷取並分析每個所選物件的最新版本，並檢查其中是否有敏感資料。

隨著分析每天進行，Macie 會更新提供有關 Amazon S3 資料的統計資料、庫存資料和其他資訊。Macie 還會產生它找到的敏感數據和它執行的分析的記錄。產生的資料可讓您深入了解 Macie 在 Amazon S3 資料資產中發現敏感資料的位置，這些資料可橫跨 Macie 為您帳戶監控和分析的所有 S3 一般用途儲存貯體。這些資料可協助您評估 Amazon S3 資料的安全性和隱私權、判斷在何處執行更深入的調查，以及識別需要修復的案例。

如需自動化敏感資料探索如何運作的簡短示範，請觀看以下影片：Amazon Macie 自動化資料探索概觀。

若要設定和管理自動化敏感資料探索，您的帳戶必須是組織的 Macie 管理員帳戶或獨立 Macie 帳戶。如果您的帳戶是組織的一部分，則只有組織的 Macie 管理員可以啟用或停用組織中帳戶的自動敏感資料探索。此外，只有 Macie 管理員可以設定和管理帳戶的自動化敏感資料探索設定。

主題

關鍵元件

Amazon Macie 使用功能和技術的組合來執行自動化的敏感資料探索。這些功能與 Macie 提供的功能搭配使用，協助您監控 Amazon S3 資料的安全性和存取控制。

選取要分析的 S3 物件

Macie 每天都會評估您的 Amazon S3 庫存資料，藉由自動化敏感資料探索來識別符合分析資格的 S3 物件。如果您是組織的 Macie 管理員，則評估預設會包含您的成員帳戶所擁有的 S3 儲存貯體的資料。

作為評估的一部分，Macie 使用取樣技術來選取要分析的具有代表性的 S3 物件。這些技術定義了具有類似中繼資料且可能具有類似內容的物件群組。這些群組是以儲存貯體名稱、字首、儲存區類別、副檔名和上次修改日期等維度為基礎。然後，Macie 會從每個群組中選取一組代表性的範例，從 Amazon S3 擷取每個所選物件的最新版本，並分析每個選取的物件以判斷物件是否包含敏感資料。分析完成後，Macie 會捨棄其物件複本。

採樣策略會優先考慮分散式分析。一般而言，它會使用廣度優先的方法來處理 Amazon S3 資料資產。每天，系統會根據 Amazon S3 資料資產中所有可分類物件的總儲存大小，從盡可能多的一般用途儲存貯體中選取一組代表性的 S3 物件。例如，如果 Macie 已經分析並發現某個值區中物件中的敏感資料，但尚未分析另一個值區中的物件，則後一個值區的分析優先順序較高。使用這種方法，您可以更快地獲得對 Amazon S3 資料敏感度的廣泛洞察。根據資料資產的大小，分析結果可能會在 48 小時內開始顯示。

取樣策略也會優先分析最近建立或變更的不同類型 S3 物件和物件。不能保證任何單個對象樣本是確定性的。因此，分析各種物件集可以對 S3 儲存貯體可能包含的敏感資料類型和數量產生更好的洞察力。此外，設定新物件或最近變更物件的優先順序，有助於分析適應值區庫存的變更。例如，如果在先前的分析之後建立或變更了物件，則這些物件對於後續分析的優先順序較高。相反地，如果物件先前已經過分析，而且自該分析之後沒有變更，Macie 就不會再次分析該物件。此方法可協助您為個別 S3 儲存貯體建立敏感度基準。然後，隨著帳戶的持續增量分析進展，您對個別時段的敏感度評估可能會以可預測的速率變得越來越深入和詳細。

定義分析範圍

根據預設，Macie 會在評估您的庫存資料並選取要分析的 S3 物件時，包含所有 S3 一般用途儲存貯體，這些儲存貯體會為您的帳戶監控和分析。如果您是組織的 Macie 管理員，這包括您的成員帳戶所擁有的值區。

您可以透過排除特定的 S3 儲存貯體來調整分析範圍。例如，您可能希望排除通常存儲日誌 AWS 記錄數據的存儲桶，例如 AWS CloudTrail 事件日誌。若要排除值區，您可以變更帳戶或儲存貯體的自動化敏感資料探索設定。如果您這樣做，Macie 會在下一個每日評估和分析週期開始時開始排除值區。您可以從分析中排除多達 1,000 個值區。如果您排除 S3 儲存貯體，之後可以再次包含它。若要這麼做，請再次變更帳戶或值區的設定。然後，Macie 在下一個每日評估和分析週期開始時開始包括存儲桶。

如果您是組織的 Macie 系統管理員，也可以啟用或停用組織中個別帳戶的自動敏感資料探索功能。如果您停用帳戶的自動探索，Macie 會排除該帳戶擁有的所有 S3 儲存貯體。如果您之後重新啟用帳戶的自動探索，Macie 會再次開始包含值區。

判斷要偵測和報告的敏感資料類型

根據預設，Macie 會使用我們建議用於自動化敏感資料探索的一組受管資料識別碼來檢查 S3 物件。如需這些受管資料識別碼的清單，請參閱自動化敏感資料探索的預設設定。

您可以調整分析以專注於特定類型的敏感資料。若要這麼做，請使用下列任一方式變更帳戶的自動敏感資料探索設定：

- 新增或移除受管資料識別碼 — 受管資料識別碼是一組內建準則和技術，用來偵測特定類型的敏感資料，例如特定國家或地區的信用卡號碼、 AWS 秘密存取金鑰或護照號碼。如需詳細資訊，請參閱 使用受管資料識別符。
- 新增或移除自訂資料識別碼 — 自訂資料識別碼是您定義用來偵測敏感資料的一組準則。使用自訂資料識別碼，您可以偵測反映組織特定案例、智慧財產或專屬資料的敏感資料，例如員工 ID、客戶帳號或內部資料分類。如需詳細資訊，請參閱 建置自訂資料識別符。
- 新增或移除允許清單 — 在 Macie 中，允許清單會指定您希望 Macie 在 S3 物件中忽略的文字或文字模式。這些通常是您特定案例或環境的敏感資料例外狀況，例如組織的公用名稱或電話號碼，或是組織用於測試的範例資料。如需詳細資訊，請參閱 使用允許清單定義敏感資料例外。

如果您變更設定，Macie 會在下一個每日分析週期開始時套用您的變更。如果您是組織的 Macie 管理員，當 Macie 分析組織中其他帳戶的 S3 物件時，會使用您帳戶的設定。

您也可以調整儲存貯體層級設定，以決定是否要在值區敏感度的評估中包含特定類型的機密資料。如要瞭解如何作業，請參閱管理個別 S3 儲存貯體的自動化敏感資料探索。

計算敏感度分數

根據預設，Macie 會針對您的帳戶監控和分析的每個 S3 一般用途儲存貯體自動計算敏感度分數。如果您是組織的 Macie 管理員，這包括您的成員帳戶所擁有的值區。

在 Macie 中，敏感度分數是兩個主要維度交集的量化測量方法：Macie 在值區中找到的敏感資料量，以及 Macie 在值區中分析的資料量。值區的靈敏度分數會決定 Macie 指派給值區的敏感度標籤。敏感度標籤是值區靈敏度分數的定性表示法，例如「敏感」、「不敏感」和「尚未分析」。如需有關 Macie 定義之敏感度分數和標籤範圍的詳細資訊，請參閱S3 儲存貯體的靈敏度評分。

> **Important**
>
> S3 儲存貯體的敏感度分數和標籤並不暗示或以其他方式表示儲存貯體或儲存貯體的物件對您的組織可能具有的重要性或重要性。相反，它們旨在提供可幫助您識別和監控潛在安全風險的參考點。

當您一開始啟用自動化敏感資料探索時，Macie 會自動為每個 S3 儲存貯體指派 50 的敏感度分數和尚未分析的標籤。例外情況是空值區。空值區是不儲存任何物件的值區，或是值區的所有物件都包含零 (0) 個位元組的資料。如果儲存貯體是這種情況，Macie 會將分數 1 指派給值區，並將「不敏感」標籤指派給值區。

隨著自動化敏感資料探索的進展，Macie 會更新敏感度分數和標籤，以反映分析結果。例如：

- 如果 Macie 在物件中找不到敏感資料，Macie 會降低值區的敏感度分數，並視需要更新值區的敏感度標籤。
- 如果 Macie 在物件中找到敏感資料，Macie 會增加值區的敏感度分數，並視需要更新值區的敏感度標籤。
- 如果 Macie 在隨後變更的物件中找到敏感資料，Macie 會從值區的敏感度評分中移除物件的敏感性資料偵測，並視需要更新值區的敏感性標籤。
- 如果 Macie 在隨後刪除的物件中找到敏感資料，Macie 會從值區的敏感度分數中移除物件的敏感性資料偵測，並視需要更新值區的敏感性標籤。

您可以在儲存貯體分數中包含或排除特定類型的敏感資料，以調整個別 S3 儲存貯體的敏感度評分設定。您也可以手動將最高分數 (100) 指派給值區，以覆寫值區的計算得分。如果您指派最高分數，則值區會標示為「敏感」。如需詳細資訊，請參閱 管理個別 S3 儲存貯體的自動化探索。

產生中繼資料、統計資料和結果

當您啟用自動化敏感資料探索時，Macie 會產生並開始維護其他有關 S3 一般用途儲存貯體的其他庫存資料、統計資料和其他資訊，這些資訊會監控並分析您的帳戶。如果您是組織的 Macie 管理員，預設會包含您的成員帳戶所擁有的值區。

其他資訊會擷取 Macie 迄今為止執行的自動化敏感資料探索活動的結果。它還補充了 Macie 提供有關 Amazon S3 資料的其他資訊，例如個別儲存貯體的公用存取和共用存取設定。其他資訊包括：

- 彙總的資料敏感性統計資料，例如 Macie 在其中找到敏感資料的儲存貯體總數，以及可公開存取的值區數量。
- 以互動式視覺化方式呈現 Amazon S3 資料資產的資料敏感度。
- 指出分析目前狀態的值區層級詳細資訊。例如，Macie 在值區中分析過的物件清單、Macie 在值區中找到的敏感資料類型，以及 Macie 找到的每種敏感資料類型的出現次數。

這些資訊還包括統計資料和詳細資料，可協助您評估和監控 Amazon S3 資料的涵蓋範圍。您可以檢查儲存貯體庫存中整體資料資產和個別 S3 儲存貯體的分析狀態。您也可以找出阻止 Macie 分析特定值區中物件的問題。如果修復問題，您可以在後續的分析週期中增加 Amazon S3 資料的涵蓋範圍。如需詳細資訊，請參閱 評估自動化敏感資料探索範圍。

Macie 會在執行自動化敏感資料探索時自動重新計算和更新此資訊。例如，如果 Macie 在 S3 物件中發現隨後變更或刪除的機密資料，Macie 會更新適用儲存貯體的中繼資料：從分析物件清單中移除該物件；移除 Macie 在物件中找到的敏感度資料；如果分數是自動計算的，則重新計算敏感度分數；並視需要更新敏感度標籤以反映新的分數。

除了中繼資料和統計資料之外，Macie 還會產生所找到的敏感資料及其執行的分析記錄：敏感資料發現項目、報告 Macie 在個別 S3 物件中找到的敏感資料，以及敏感資料探索結果，記錄有關個別 S3 物件分析的詳細資料。

如需詳細資訊，請參閱 檢閱自動化的敏感資料探索統計資料和。

考量事項

當您設定和使用 Amazon Macie 為 Amazon S3 資料執行自動化敏感資料探索時，請記住以下事項：

- 您的自動探索設定僅適用於目前的 AWS 區域。因此，產生的分析和資料僅適用於目前區域中的 S3 一般用途儲存貯體和物件。若要在其他區域中執行自動化探索並存取產生的資料，請在每個額外的區域中啟用和設定自動化探索。
- 如果您是組織的 Macie 管理員：
  - 只有當目前區域中的帳戶啟用 Macie 時，您才能為成員帳戶執行自動探索。此外，您必須為該區域中的帳戶啟用自動探索功能。成員無法為自己的帳戶啟用自動探索功能。
  - 如果您為成員帳戶啟用自動探索功能，Macie 會在分析成員帳戶的資料時，使用您的管理員帳戶的自動探索設定。適用的設定包括：要從分析中排除的 S3 儲存貯體清單、受管資料識別碼、自訂資料識別碼，以及允許在分析 S3 物件時使用的清單。會員無法為自己的帳戶設定這些設定。
  - 成員無法存取 S3 儲存貯體的自動探索設定。例如，成員無法針對自己擁有的值區調整靈敏度評分設定。只有 Macie 管理員可以存取這些設定。
  - 成員無法存取 Macie 直接為其 S3 儲存貯體提供的敏感資料探索統計資料和其他結果。例如，成員無法使用 Macie 檢閱其 S3 儲存貯體的敏感度分數，或存取自動探索為其 S3 物件產生的發現項目。只有 Macie 管理員可以通過使用 Macie 訪問這些數據。
- 如果 S3 儲存貯體的許可設定阻止 Macie 擷取或存取儲存貯體或儲存貯體物件的相關資訊，Macie 就無法執行儲存貯體的自動探索。Macie 只能提供值區的相關資訊子集，例如擁有 AWS 帳戶 該值區的帳戶 ID、值區的名稱，以及 Macie 最近擷取值區的值區和物件中繼資料作為每日重新整理週期的一部分。在您的值區庫存中，這些值區的敏感度分數為 50，而且尚未分析其敏感度標籤。

  若要快速識別出現這種情況的 S3 儲存貯體，請參閱您的自動探索涵蓋範圍資料。如需詳細資訊，請參閱 評估自動化敏感資料探索範圍。若要調查特定儲存貯體的問題，請檢閱 Amazon S3 中儲存貯體的政策和許可設定。例如，值區可能具有限制性的值區政策。如需詳細資訊，請參閱 允許 Macie 存取 S3 儲存貯體和物件。
- 若要符合選取和分析的資格，S3 物件必須存放在一般用途儲存貯體中，且必須可分類。可分類的物件使用支援的 Amazon S3 儲存類別，且其副檔名為支援的檔案或儲存格式。如需詳細資訊，請參閱 支援的儲存類別和格式。

- 如果 S3 物件已加密，Macie 只有在使用 Macie 可存取且允許使用的金鑰加密時，才能對其進行分析。如需詳細資訊，請參閱 分析加密的 S3 物件。若要識別加密設定阻止 Macie 分析值區中一或多個物件的案例，請參閱您的自動探索涵蓋範圍資料。如需更多詳細資訊，請參閱 評估自動化敏感資料探索範圍。

設定自動化敏感資料探索

透過自動化敏感資料探索功能，Amazon Macie 會持續從 Amazon 簡單儲存服務 (Amazon S3) 一般用途儲存貯體中選取範例物件，並分析物件以判斷它們是否包含敏感資料。如果您是組織的 Macie 管理員，預設情況下會包含您成員帳戶所擁有的 S3 儲存貯體中的物件。隨著分析的進展，Macie 會更新提供有關 Amazon S3 資料的統計資料、庫存資料和其他資訊。Macie 還會產生它找到的敏感數據和它執行的分析的記錄。

若要設定和管理自動化敏感資料探索，您的帳戶必須是組織的 Macie 管理員帳戶或獨立 Macie 帳戶。如果您的帳戶是組織的一部分，則只有組織的 Macie 管理員可以啟用或停用組織中帳戶的自動敏感資料探索。此外，只有 Macie 管理員可以為帳戶設定自動化敏感資料探索設定。如果您擁有成員帳戶，並希望 Macie 為 S3 儲存貯體執行自動化敏感資料探索，請聯絡您的 Macie 管理員。

主題

- 開始之前
- 組織的組態選項
- 啟用自動化敏感資料探索
- 設定自動化敏感資料探索設定
- 停用自動化敏感資料探索

啟用、設定或停用自動化敏感資料探索時，您的變更只會套用至目前的 AWS 區域。若要在其他區域中進行相同的變更，請在每個額外的「區域」中重複適用的步驟。

開始之前

啟用或設定自動化敏感資料探索之前，請先完成下列工作，以確保您擁有所需的資源和權限。

任務

- 設定機密資料探索結果的儲存庫
- 驗證您的權限

如果您已啟用並設定自動化敏感資料探索，而且只想變更設定或停用，則這些工作為選擇性工作。

設定機密資料探索結果的儲存庫

Amazon Macie 執行自動化敏感資料探索時，會為選取用於分析的每個 Amazon Simple Storage Service (Amazon S3) 物件建立分析記錄。這些記錄稱為敏感資料探索結果，記錄有關個別 S3 物件分析的詳細資料。這包括 Macie 無法在其中找到敏感資料的物件，以及 Macie 因錯誤或權限設定等問題而無法分析的物件。如果 Macie 在物件中找到敏感資料，則敏感資料探索結果會包含 Macie 找到的敏感資料的相關資訊。敏感資料探索結果為您提供分析記錄，這些記錄對於資料隱私權和保護稽核或調查有幫助。

Macie 只會儲存您的敏感資料探索結果 90 天。若要存取結果並啟用它們的長期儲存和保留，請將 Macie 設定為將結果存放在 S3 儲存貯體中。儲存貯體可作為所有敏感資料探索結果的確定長期存放庫。

若要確認您已設定此儲存庫，請在 Amazon Macie 主控台的導覽窗格中選擇「探索結果」。如果您希望以編程方式執行此GetClassificationExportConfiguration操作，請使用 Amazon Macie API 的操作。若要進一步瞭解敏感資料探索結果以及如何設定此存放庫，請參閱儲存及保留敏感資料探索結果。

如果您已設定存放庫，當您第一次啟用自動化敏感資料探索時，Macie 會`automated-sensitive-data-discovery`在儲存庫中建立名為的資料夾。此資料夾儲存 Macie 在為您的帳戶或組織執行自動探索時所建立的敏感資料探索結果。

驗證您的權限

若要驗證您的許可，請使用 AWS Identity and Access Management (IAM) 檢閱附加到 IAM 身分的 IAM 政策。然後將這些策略中的資訊與下列必須允許您執行的動作清單進行比較：

- `macie2:GetMacieSession`
- `macie2:UpdateAutomatedDiscoveryConfiguration`
- `macie2:ListClassificationScopes`
- `macie2:UpdateClassificationScope`
- `macie2:ListSensitivityInspectionTemplates`
- `macie2:UpdateSensitivityInspectionTemplate`

第一個動作允許您訪問您的 Amazon Macie 帳戶。第二個動作可讓您啟用或停用帳戶或組織的自動敏感資料探索功能。對於組織，它也可讓您針對組織中的帳戶自動啟用自動化敏感資料探索功能。其餘動作可讓您識別和變更組態設定。

如果您計劃使用 Amazon Macie 主控台檢閱或變更組態設定，請確認您是否允許執行下列動作：

- `macie2:GetAutomatedDiscoveryConfiguration`
- `macie2:GetClassificationScope`
- `macie2:GetSensitivityInspectionTemplate`

這些動作可讓您擷取目前的組態設定，以及帳戶或組織的自動化敏感資料探索狀態。如果您計劃以程式設計方式變更組態設定，則可選擇執行這些動作的權限。

如果您是組織的 Macie 管理員，您也必須被允許執行下列動作：

- `macie2:ListAutomatedDiscoveryAccounts`
- `macie2:BatchUpdateAutomatedDiscoveryAccounts`

第一個動作可讓您擷取組織中個別帳戶的自動化敏感資料探索狀態。第二個動作可讓您啟用或停用組織中個別帳戶的自動敏感資料探索功能。

如果您不允許執行必要的動作，請向 AWS 管理員尋求協助。

組織的組態選項

如果帳戶屬於集中管理多個 Amazon Macie 帳戶的組織，該組織的 Macie 管理員會為組織中的帳戶設定和管理自動化敏感資料探索。這包括定義 Macie 對帳戶執行的分析範圍和性質的設定。會員無法存取自己帳戶的這些設定。

如果您是組織的 Macie 管理員，您可以透過數種方式定義分析範圍：

- 自動啟用帳戶的自動敏感資料探索 — 當您啟用自動敏感資料探索時，您可以指定是否針對所有現有帳戶和新成員帳戶自動啟用此功能，僅針對新成員帳戶啟用，或不啟用任何帳戶。如果您為新成員帳戶自動啟用此功能，則當該帳戶在 Macie 中加入您的組織時，任何後續加入組織的帳戶都會啟用此功能。如果已為帳戶啟用此功能，Macie 會包含該帳戶擁有的 S3 儲存貯體。如果某個帳戶已停用此功能，Macie 會排除該帳戶擁有的儲存貯體。
- 選擇性地啟用帳戶的自動敏感資料探索 — 使用此選項，您可以 case-by-case 根據個別帳戶啟用或停用自動化敏感資料探索。如果您為帳戶啟用此功能，Macie 會包含該帳戶擁有的 S3 儲存貯體。如果您未啟用或停用帳戶的帳戶，Macie 會排除該帳戶擁有的值區。
- 從自動化敏感資料探索中排除特定 S3 儲存貯體 — 如果您為一或多個帳戶啟用自動化敏感資料探索功能，則可以排除該帳戶擁有的特定 S3 儲存貯體。然後，Macie 會在為您的組織執行自動化探索時

略過值區。若要排除特定值區，請將它們新增至管理員帳戶組態設定中的值區例外清單。您可以為您的組織排除多達 1,000 個值區。

根據預設，組織中所有新帳戶和現有帳戶都會自動啟用自動敏感資料探索功能。此外，Macie 還包含帳戶擁有的所有 S3 儲存貯體。如果您保留預設設定，Macie 會針對管理員帳戶監控和分析的所有值區執行自動探索，其中包括您的成員帳戶所擁有的所有值區。

身為 Macie 管理員，您也可以定義 Macie 為您的組織執行的分析本質。您可以透過為管理員帳戶設定其他設定 (受管資料識別碼、自訂資料識別碼、自訂資料識別碼，並允許您希望 Macie 在分析 S3 物件時使用的清單)。當 Macie 分析組織中其他帳戶的 S3 物件時，會使用管理員帳戶的設定。

啟用自動化敏感資料探索

當您啟用自動化敏感資料探索時，Amazon Macie 會開始評估您的 Amazon S3 庫存資料，並針對目前 AWS 區域帳戶執行其他自動化探索活動。如果您是組織的 Macie 管理員，預設情況下會包含您的成員帳戶所擁有的 S3 儲存貯體。根據 Amazon S3 資料資產的大小，敏感資料探索統計資料和其他結果可能會在 48 小時內開始顯示。

若要為帳戶或組織啟用自動化敏感資料探索功能，您可以使用 Amazon Macie 主控台或 Amazon Macie API。要使用控制台啟用它，請按照下列步驟操作。若要以程式設計方式啟用，請針對組織中的個別帳戶使用下列 Amazon Macie API 操作：BatchUpdateAutomatedDiscoveryAccounts針對組織中的個別帳戶 UpdateAutomatedDiscoveryConfiguration，或組織使用 Macie 管理員帳戶或獨立的 Macie 帳戶。

啟用自動化敏感資料探索

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 使用頁面右上角的選取 AWS 區域 器，選取您要在其中啟用自動化敏感資料探索的區域。
3. 在功能窗格的 [設定] 下，選擇 [自動敏感資料探索]。
4. 如果您有獨立的 Macie 帳戶，請在「狀態」區段中選擇「啟用」。
5. 如果您是組織的 Macie 管理員，請在「狀態」區段中選擇一個選項，以指定要啟用自動敏感資料探索的帳戶：

   - 若要為組織中的所有帳號啟用此功能，請選擇 [啟用]。在出現的對話方塊中，選擇 [我的組織]。若要針對隨後加入組織的帳戶自動啟用此功能，請選取 [針對新帳戶自動啟用]。完成後，請選擇 [啟用]。

- 若只要針對特定成員帳戶啟用此功能，請選擇 [管理帳戶]。然後，在 [帳戶] 頁面上的表格中，針對您要為其啟用的每個帳戶選取核取方塊。完成後，請在 [動作] 功能表上選擇 [啟用自動敏感資料探索]。
- 若只要針對您的 Macie 管理員帳戶啟用此功能，請選擇「啟用」。在出現的對話方塊中，選擇「我的帳戶」，然後清除「為新帳戶自動啟用」。完成後，請選擇 [啟用]。

若要隨後檢查或變更組織中個別帳戶的自動敏感資料探索狀態，請在功能窗格中選擇 [帳戶]。在 [帳戶] 頁面上，表格中的 [自動化敏感資料探索] 欄位會指出帳戶目前自動探索的狀態。若要變更帳號的狀態，請選取該帳戶，然後使用 [動作] 功能表啟用以停用帳戶的自動探索。

啟用自動化敏感資料探索之後，請檢閱並設定您的設定，以精簡 Macie 執行的分析。

設定自動化敏感資料探索設定

如果您為帳戶或組織啟用自動化敏感資料探索，則可以調整自動探索設定，以精簡 Amazon Macie 執行的分析。這些設定會指定要從分析中排除的 S3 儲存貯體。它們也會指定要偵測和報告之敏感資料的類型和出現次數，例如受管資料識別碼、自訂資料識別碼，以及在分析 S3 物件時使用的允許清單。

根據預設，Macie 會針對您的帳戶監控和分析的所有 S3 一般用途儲存貯體執行自動化的敏感資料探索。如果您是組織的 Macie 管理員，這包括您的成員帳戶所擁有的值區。您可以從分析中排除特定值區。例如，您可以排除通常儲存 AWS 記錄資料的值區，例如 AWS CloudTrail 事件記錄檔。如果排除值區，之後可以再次包含該值區。

此外，Macie 僅使用我們建議用於自動化敏感資料探索的一組受管資料識別碼來分析 S3 物件。Macie 不會使用自訂資料識別碼或允許您定義的清單。若要自訂分析，您可以設定 Macie 使用特定的受管理資料識別碼、自訂資料識別碼和允許清單。

以下各節提供有關每種設定類型的其他資訊。他們還說明如何使用 Amazon Macie 控制台更改設置。選擇一個部分以了解更多信息。若要以程式設計方式檢閱或變更設定，您可以使用 Amazon Macie API 的下列操作：UpdateClassificationScope指定要從分析中排除的 S3 儲存貯體，以及UpdateSensitivityInspectionTemplate指定要使用的受管資料識別碼、自訂資料識別碼和允許清單。

如果您變更設定，Macie 會在下一個評估和分析週期開始進行自動化敏感資料探索時套用您的變更，通常在 24 小時內。

排除或包含 S3 儲存貯體

根據預設，Macie 會針對您的帳戶監控和分析的所有 S3 一般用途儲存貯體執行自動化的敏感資料探索。如果您是組織的 Macie 管理員，這包括您的成員帳戶所擁有的值區。

若要精簡範圍，您可以從分析中排除多達 1,000 個 S3 儲存貯體。如果您排除值區，Macie 會在執行自動化敏感資料探索時停止選取和分析值區中的物件。值區的現有敏感資料探索統計資料和詳細資料會持續存在，例如儲存貯體目前的敏感度分數維持不變。排除值區之後，您可以隨後再次包含該值區。

排除或包含特定 S3 儲存貯體

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 使用頁面右上角的選取 AWS 區域 器，選取要在自動探索分析中排除或包含特定 S3 儲存貯體的區域。
3. 在功能窗格的 [設定] 下，選擇 [自動敏感資料探索]。

   自動化敏感資料探索頁面隨即出現，並顯示您目前的設定。在該頁面上，S3 儲存貯體區段會列出目前排除的 S3 儲存貯體，或指示目前已包含所有儲存貯體。
4. 在 S3 儲存貯體區段中，選擇編輯。
5. 執行以下任意一項：

   - 若要排除一或多個 S3 儲存貯體，請選擇 [將儲存貯體新增至排除清單]。然後，在 S3 儲存貯體表格中，針對要排除的每個儲存貯體選取核取方塊。此表格會列出目前「區域」中您帳戶或組織的所有一般用途時段。
   - 若要包含先前排除的一或多個 S3 儲存貯體，請從排除清單中選擇 [移除儲存貯體]。然後，在 S3 儲存貯體表格中，針對要包含的每個儲存貯體選取核取方塊。此表格列出目前從自動探索分析中排除的所有值區。

   若要更輕鬆地尋找特定值區，請在表格上方的搜尋方塊中輸入搜尋條件。您也可以選擇欄標題來排序表格。
6. 完成選取值區後，請根據您在前面步驟中選擇的選項，選擇「新增」或「移除」。

新增或移除受管資料識別碼

受管資料識別碼是一組內建準則和技術，用來偵測特定類型的敏感資料，例如特定國家或地區的信用卡號碼、 AWS 秘密存取金鑰或護照號碼。根據預設，Macie 會使用我們建議用於自動化敏感資料探索的一組受管資料識別碼來分析 S3 物件。若要檢閱這些識別碼的清單，請參閱自動化敏感資料探索的預設設定。

您可以自訂分析以專注於特定類型的敏感資料：

- 為您希望 Macie 偵測和報告的敏感資料類型新增受管理的資料識別碼，以及

- 移除您不希望 Macie 偵測和報告之敏感資料類型的受管理資料識別碼。

如果您移除受管資料識別碼，您的變更不會影響 S3 儲存貯體的現有敏感資料探索統計資料和詳細資料。例如，如果您移除 AWS 秘密存取金鑰的受管理資料識別碼，而 Macie 先前在值區中偵測到該類型的資料，Macie 會繼續回報值區的這些偵測。

> **Tip**
>
> 您可以將其偵測從特定儲存貯體的敏感度分數中排除，而不會移除會影響所有 S3 儲存貯體後續分析的受管資料識別碼。如需詳細資訊，請參閱 管理個別 S3 儲存貯體的自動化敏感資料探索。

新增或移除受管理的資料識別碼

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 使用頁面右上角的選取 AWS 區域 器，選取您要在其中新增或移除自動化探索分析中的受管理資料識別碼的區域。
3. 在功能窗格的 [設定] 下，選擇 [自動敏感資料探索]。

   自動化敏感資料探索頁面隨即出現，並顯示您目前的設定。在該頁面上，「受管理的資料識別碼」區段會顯示您目前的設定，並分為兩個索引標籤：

   - 新增至預設值 — 此索引標籤會列出您新增的受管理資料識別碼。Macie 除了預設集合中且您尚未移除的識別碼之外，還會使用這些識別碼。
   - 已從預設移除 — 此索引標籤會列出您移除的受管理資料識別碼。Macie 不會使用這些識別碼。
4. 在「受管理的資料識別碼」區段中，選擇編輯。
5. 執行下列任何一項：

   - 若要新增一或多個受管理資料識別碼，請選擇 [新增至預設值] 索引標籤。然後，在表格中，選取要新增的每個受管理資料識別碼的核取方塊。如果已選取核取方塊，表示您已新增該識別碼。
   - 若要移除一或多個受管理的資料識別碼，請選擇 [從預設移除] 索引標籤。然後，在表格中，選取要移除的每個受管理資料識別碼的核取方塊。如果已選取核取方塊，表示您已移除該識別碼。

   在每個索引標籤上，表格會顯示 Macie 目前提供的所有受管理資料識別碼的清單。在資料表中，第一欄會指定每個受管理資料識別碼的 ID。ID 描述識別碼用來偵測的敏感資料類型，例如美國護

照號碼的 USA_PASSPORT_NUMBER。若要更輕鬆地尋找特定的受管理資料識別碼，請在表格上方的搜尋方塊中輸入搜尋條件。您也可以選擇欄標題來排序表格。如需每個識別碼的詳細資訊，請參閱使用受管資料識別符。

6. 完成後，請選擇儲存。

新增或移除自訂資料識別碼

自訂資料識別碼是您定義用來偵測機密資料的一組準則。此條件包含規則運算式 (Regex)，此表達式定義要比對的文字模式，以及可選擇的字元序列和精簡結果之鄰近性規則。如需進一步了解，請參閱建置自訂資料識別符。

根據預設，Amazon Macie 在執行自動化敏感資料探索時不會使用自訂資料識別碼。如果您希望 Macie 使用特定的自訂資料識別碼，您可以將它們加入分析中。然後，Macie 會使用自訂資料識別碼，以及您設定 Macie 要使用的任何受管理資料識別碼。

如果您新增自訂資料識別碼，您可以隨後將其移除。您的變更不會影響 S3 儲存貯體的現有敏感資料探索統計資料和詳細資料。也就是說，如果您移除先前針對值區產生偵測的自訂資料識別碼，Macie 會繼續回報值區的這些偵測。不過，不要移除會影響所有值區後續分析的識別碼，而是考慮將其偵測從特定值區的敏感度評分中排除。如需詳細資訊，請參閱 管理個別 S3 儲存貯體的自動化敏感資料探索。

若要新增或移除自訂資料識別碼

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 使用頁面右上角的選取 AWS 區域 器，選取您要從自動化探索分析新增或移除自訂資料識別碼的區域。
3. 在功能窗格的 [設定] 下，選擇 [自動敏感資料探索]。

   自動化敏感資料探索頁面隨即出現，並顯示您目前的設定。在該頁面上，[自訂資料識別碼] 區段會列出您新增的自訂資料識別碼，或表示您尚未選取任何自訂資料識別碼。
4. 在 [自訂資料識別碼] 區段中，選擇 [編輯]。
5. 執行下列任何一項：

   - 若要新增一或多個自訂資料識別碼，請選取要新增的每個自訂資料識別碼的核取方塊。如果已選取核取方塊，表示您已新增該識別碼。
   - 若要移除一或多個自訂資料識別碼，請清除要移除的每個自訂資料識別碼的核取方塊。如果核取方塊已經清除，Macie 目前不會使用該識別碼。

> **Tip**
>
> 若要在新增或移除自訂資料識別碼之前檢閱或測試自訂資料識別碼的設定，請選擇識別碼名稱旁邊的連結圖示 ( )。Macie 打開一個頁面，顯示標識符的設置。若要使用範例資料測試識別碼，請在該頁面的 [範例資料] 方塊中輸入最多 1,000 個字元的文字。然後選擇測試。Macie 評估樣本數據並報告匹配的數量。

6. 完成後，請選擇儲存。

新增或移除允許清單

在 Amazon Macie 中，允許清單會定義您希望 Macie 在檢查 S3 物件中是否有敏感資料時忽略的特定文字或文字模式。如果文字符合允許清單中的項目或模式，Macie 就不會報告該文字。即使文字符合受管理或自訂資料識別碼的準則，也會發生這種情況。如需進一步了解，請參閱使用允許清單定義敏感資料例外。

根據預設，Macie 在執行自動化敏感資料探索時不會使用允許清單。如果您希望 Macie 使用特定的允許清單，您可以將它們加入到分析中。如果您新增允許清單，您可以隨後將其移除。

新增或移除允許清單

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 使用頁面右上角的選取 AWS 區域 器，選取您要從自動探索分析新增或移除允許清單的區域。
3. 在功能窗格的 [設定] 下，選擇 [自動敏感資料探索]。

   自動化敏感資料探索頁面隨即出現，並顯示您目前的設定。在該頁面上，[允許清單] 區段會指定您已新增的允許清單，或表示您尚未選取任何允許清單。
4. 在 [允許清單] 區段中，選擇 [編輯]。
5. 執行下列任何一項：

   - 若要新增一或多個允許清單，請選取要新增的每個允許清單的核取方塊。如果已選取核取方塊，表示您已新增該清單。
   - 若要移除一或多個允許清單，請清除每個要移除之允許清單的核取方塊。如果核取方塊已經清除，Macie 目前不會使用該清單。

> **Tip**
>
> 若要在新增或移除允許清單之前檢閱允許清單的設定，請選擇清單名稱旁邊的連結圖示 ()。Macie 會開啟顯示清單設定的頁面。如果清單指定規則運算式 (regex)，您也可以使用此頁面來測試使用範例資料的 regex。若要這麼做，請在 [範例資料] 方塊中輸入最多 1,000 個字元的文字，然後選擇 [測試]。Macie 評估樣本數據並報告匹配的數量。

6. 完成後，請選擇儲存。

停用自動化敏感資料探索

您可以隨時停用帳戶或組織的自動敏感資料探索功能。如果您這麼做，Macie 會在後續評估和分析週期開始之前 (通常在 48 小時內) 停止執行帳戶或組織的所有自動化探索活動。其他效果有所不同：

- 如果您為組織中的某個帳戶停用此功能，您可以繼續存取 Macie 產生並直接提供的所有統計資料、庫存資料和其他資訊，同時為該帳戶執行自動探索。您也可以再次為帳戶啟用自動探索。然後，Macie 會繼續該帳戶的所有自動探索活動。
- 如果您為組織或獨立的 Macie 帳戶停用此功能，您將無法存取 Macie 產生並直接提供的所有統計資料、庫存資料及其他資訊，同時為您的組織或帳戶執行自動化探索。例如，您的 S3 儲存貯體庫存不再包含敏感度視覺效果或分析統計資料。您可以隨後再次啟用它。然後，Macie 會為您的組織或帳戶恢復所有自動探索活動。如果您在 30 天內重新啟用它，您將重新存取 Macie 先前產生並在執行自動化探索時直接提供的所有資料和資訊的存取權。如果您未在 30 天內重新啟用，Macie 會永久刪除此資料和資訊。

在為您的組織或帳戶執行自動化敏感資料探索時，您可以繼續存取 Macie 產生的敏感資料發現項目。瑪西存儲 90 天的發現。此外，您存放或發佈到其他資料會 AWS 服務 保持完整且不受影響，例如敏感資料探索會導致 Amazon S3 中的資料以及在 Amazon 中尋找事件 EventBridge。

若要停用自動化敏感資料探索，您可以使用 Amazon Macie 主控台或 Amazon Macie API。要使用控制台禁用它，請按照下列步驟操作。若要以程式設計方式停用此功能，請針對組織中的個別帳戶使用下列 Amazon Macie API 操作：BatchUpdateAutomatedDiscoveryAccounts針對組織中的個別帳戶 UpdateAutomatedDiscoveryConfiguration，或組織使用 Macie 管理員帳戶或獨立的 Macie 帳戶。

停用自動化敏感資料探索

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 使用頁面右上角的選取 AWS 區域 器，選取您要停用自動化敏感資料探索的區域。
3. 在功能窗格的 [設定] 下，選擇 [自動敏感資料探索]。
4. 如果您是組織的 Macie 管理員，請在「狀態」區段中選擇一個選項，以指定要停用自動化敏感資料探索功能的帳戶：
   - 若只要針對特定成員帳戶停用此功能，請選擇 [管理帳戶]。然後，在 [帳戶] 頁面上的表格中，針對您要停用它的每個帳戶選取核取方塊。完成後，請在 [動作] 功能表上選擇 [停用自動化敏感資料探索]。
   - 若只要針對您的 Macie 管理員帳戶停用此功能，請選擇「停用」。在出現的對話方塊中，選擇 [我的帳戶]，然後選擇 [停用]。
   - 若要針對組織和組織整體中的所有帳戶停用此功能，請選擇 [停用]。在出現的對話方塊中，選擇 [我的組織]，然後選擇 [停用]。
5. 如果您有獨立的 Macie 帳戶，請在「狀態」區段中選擇「停用」。

管理個別 S3 儲存貯體的自動化敏感資料探索

在檢閱和評估自動化敏感資料探索統計資料和結果時，您可以調整個別 Amazon Simple Storage Service (Amazon S3) 儲存貯體的敏感度評分和其他設定。透過調整這些設定，您可以微調整整體 Amazon S3 資料資產和其中特定儲存貯體的敏感度評估。您也可以擷取針對特定值區執行的調查結果。

您可以透過下列方式調整 S3 儲存貯體的自動化敏感資料探索設定。

指派敏感度分數

根據預設，Amazon Macie 會自動計算值區的敏感度分數。分數主要取決於 Macie 在值區中找到的敏感資料量，以及 Macie 在值區中分析的資料量。如需詳細資訊，請參閱 S3 儲存貯體的靈敏度評分。

您可以覆寫值區的計算得分，並手動指派最高分數 (100)，這也會將「敏感」標籤套用至值區。如果您這麼做，Macie 會繼續執行值區的自動化探索。但是，後續分析不會影響存儲桶的分數。若要再次自動計算分數，請再次變更設定。

在敏感度分數中排除或包含特定敏感資料類型

如果自動計算，值區的敏感度分數部分取決於 Macie 在值區中找到的敏感資料量。這主要衍生自 Macie 在值區中找到的敏感資料類型的性質和數量，以及每種類型的出現次數。根據預設，Macie 會在計算值區的敏感度分數時，包含所有類型敏感資料的出現次數。

您可以在值區分數中排除或包含特定類型的敏感資料，以調整計算。例如，如果 Macie 偵測到值區中的郵寄地址，而您認為這是可接受的，您可以從值區的分數中排除所有出現的郵寄地址。如果您排除敏感資料類型，Macie 會繼續檢查儲存貯體是否有該類型的資料，並報告找到的事件。但是，這些事件不會影響值區的計算得分。若要在計算的存放區中再次包含敏感資料類型，請再次變更設定。

在後續分析中排除或包含值區

根據預設，Macie 會針對您的帳戶監控和分析的所有一般用途儲存貯體執行自動化探索。如果您是組織的 Macie 管理員，預設設定會包含您的成員帳戶所擁有的值區。您可以從分析中排除特定值區。例如，您可以排除通常儲存 AWS 記錄資料的值區，例如 AWS CloudTrail 事件記錄檔。

如果您排除儲存貯體，則該值區的現有敏感資料探索統計資料和詳細資料會持續存在，例如，值區目前的敏感度分數維持不變。不過，Macie 會在執行自動化探索時停止分析值區中的物件。排除值區之後，您可以隨後再次包含該值區。

如果您變更會影響 S3 儲存貯體敏感度分數的設定，Macie 會立即開始重新計算並更新其提供有關 Amazon S3 資料的相關統計資料和資訊。例如，如果您將最高分數指派給值區，Macie 會在您帳戶或組織的彙總統計資料中遞增敏感值區的計數。

請依照下列步驟使用 Amazon Macie 主控台變更設定。若要以程式設計方式變更設定，您可以使用 Amazon Macie API 的下列操作：UpdateResourceProfile將敏感度分數指派給值區；UpdateResourceProfileDetections排除或隨後在值區的分數中包含敏感資料類型；以及在後續分析中排除或包含儲存貯體。UpdateClassificationScope

變更 S3 儲存貯體的自動化敏感資料探索設定

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 在導覽窗格中，選擇 S3 儲存貯體。S3 儲存貯體頁面會顯示儲存貯體庫存。

   依預設，頁面不會顯示目前從分析中排除的值區的資料。如果您是組織的 Macie 管理員，它也不會顯示目前已停用自動化敏感資料探索功能的帳戶資料。若要顯示此資料，請在篩選器方塊下方的 [由自動探索篩選器權杖監視] 中選擇 [X]。

3. 選擇您要變更其設定的 S3 儲存貯體。您可以使用表格檢視
()
或互動式 map
()
來選擇值區。
4. 在詳細資料面板中，執行下列任一項作業:

   - 若要覆寫已計算的分數並手動指派敏感度分數給值區，請開啟「指派最高分數」
   ()。
   這會將值區的分數變更為 100，並將「敏感」標籤套用至值區。

   若要指定 Macie 自動計算的分數，請關閉指派最高分數
   ()。
   - 若要將值區排除在後續分析之外，請開啟「從自動探索中排除」
   ()。

   如果先前已將值區排除在分析之外，請關閉「從自動探索排除」
   ()
   以再次包含該值區。
   - 若要在值區的敏感度分數中排除或包含特定類型敏感資料的出現情況，請選擇「敏感度」標籤。在「偵測」表格中，選取要排除或包含之機密資料類型的核取方塊。然後，在「動作」功能表上，選擇「從評分中排除」以排除類型，或選擇「包含在分數中」以包含類型。

     在資料表中，「機密資料類型」欄位會指定偵測到資料的受管理資料識別碼的唯一識別碼 (ID)，或偵測到資料的自訂資料識別碼名稱。受管資料識別碼的 ID 描述識別碼設計用來偵測的敏感資料類型，例如，美國護照號碼的 USA_PASSPORT_NUMBER。如需每個受管資料識別碼的詳細資訊，請參閱使用受管資料識別符。

如果您變更了影響 S3 儲存貯體敏感度分數的設定，Macie 會立即開始重新計算並更新相關的敏感資料探索統計資料以及儲存貯體的其他相關資訊。

評估自動化敏感資料探索範圍

隨著您的帳戶或組織進行自動化敏感資料探索，Amazon Macie 會提供統計資料和詳細資料，協助您評估和監控 Amazon Simple Storage Service (Amazon S3) 資料資產的涵蓋範圍。有了這些資料，您可以檢查整體資料資產和儲存貯體庫存中個別 S3 儲存貯體的自動化敏感資料探索狀態。您也可以找出阻

止 Macie 分析特定值區中物件的問題。如果修復問題，您可以在後續分析週期中增加 Amazon S3 資料的涵蓋範圍。

涵蓋範圍資料提供目前 S3 一般用途儲存貯體的自動化敏感資料探索目前狀態的快照 AWS 區域。如果您是組織的 Macie 管理員，這包括您的成員帳戶所擁有的值區。對於每個值區，資料會指出當 Macie 嘗試分析值區中的物件時是否發生問題。如果發生問題，資料會指出每個問題的性質，以及 (在某些情況下) 發生次數。資料會隨著自動化敏感資料探索每天進行而更新。如果 Macie 在每日分析週期中分析或嘗試分析值區中的一或多個物件，Macie 會更新涵蓋範圍和其他資料以反映結果。

針對特定類型的問題，您可以檢閱所有 S3 一般用途儲存貯體的彙總資料，並選擇性地向下展開以取得每個儲存貯體的其他詳細資訊。例如，涵蓋範圍資料可協助您快速識別 Macie 不允許存取您帳戶的所有值區。涵蓋範圍資料也會報告所發生的物件層級問題。這些稱為分類錯誤的問題，使得 Macie 無法分析值區中的特定物件。例如，您可以判斷 Macie 無法在值區中分析多少物件，因為物件是使用不再可用的 AWS Key Management Service (AWS KMS) 金鑰加密物件。

如果您使用 Amazon Macie 主控台檢閱涵蓋範圍資料，您的資料檢視會包含修復每種類型問題的指引。本節的後續主題也提供每種類型的修正指引。

主題

檢閱自動化敏感資料探索範圍資料

若要檢閱和評估自動化敏感資料探索涵蓋範圍，您可以使用 Amazon Macie 主控台或 Amazon Macie API。主控台和 API 都會提供資料，指出目前 Amazon 簡單儲存服務 (Amazon S3) 一般用途儲存貯體的目前分析狀態 AWS 區域。資料包括有關在分析中造成間隙的問題的資訊：

- 梅西不允許訪問的桶。Macie 無法分析這些值區中的任何物件，因為值區的權限設定會阻止 Macie 存取值區和值區的物件。

- 不儲存任何可分類物件的值區。Macie 無法分析這些儲存貯體中的任何物件，因為所有物件都使用 Macie 不支援的 Amazon S3 儲存類別，或者它們具有 Macie 不支援的檔案或儲存格式的副檔名。
- 由於物件層級分類錯誤，Macie 尚未能夠分析的值區。Macie 試圖分析這些值區中的一或多個物件。不過，由於物件層級權限設定、物件內容或配額有問題，Macie 無法分析物件。

涵蓋範圍資料會隨著每天進行自動化敏感資料探索而更新。如果您是組織的 Macie 管理員，資料會包含您的成員帳戶所擁有之 S3 儲存貯體的資訊。

> **Note**
>
> 涵蓋範圍資料不會明確包含您已建立和執行之敏感資料探索工作的結果。不過，修正影響自動化敏感資料探索結果的涵蓋範圍問題也可能會增加您隨後執行的敏感資料探索工作的涵蓋範圍。若要評估工作的涵蓋範圍，請檢閱工作的統計資料和結果。如果工作的記錄事件或其他結果指出涵蓋範圍問題，本節稍後的補救指引可協助您解決部分問題。

檢閱自動化敏感資料探索涵蓋範圍資料

您可以使用 Amazon Macie 主控台或 Amazon Macie API 來檢閱您帳戶或組織的涵蓋範圍資料。在主控台上，單一頁面提供所有 S3 一般用途儲存貯體的涵蓋範圍資料的統一檢視，包括最近針對每個儲存貯體發生的問題彙總。此頁面也提供依問題類型複查資料群組的選項。若要追蹤特定值區的問題調查，您可以將頁面中的資料匯出為逗號分隔值 (CSV) 檔案。

Console

請遵循下列步驟，使用 Amazon Macie 主控台檢閱自動化敏感資料探索涵蓋範圍資料。

檢視涵蓋範圍資料

1. 在以下位置打開 Amazon Macie 控制台 https://console.aws.amazon.com/macie/。
2. 在瀏覽窗格中，選擇 [資源涵蓋範圍]。
3. 在 [資源涵蓋範圍] 頁面上，選擇您要複查之涵蓋範圍資料類型的索引標籤：

   - 全部 — 列出 Macie 為您的帳戶監控和分析的所有值區。

     針對每個值區，「問題」欄位會指出問題是否導致 Macie 無法分析值區中的物件。如果此欄位的值為 None，表示 Macie 已分析至少一個值區的物件，或者 Macie 尚未嘗試分析值區的任何物件。如果發生問題，此欄位會指出問題的性質以及如何修正問題。對於物件層級的分類錯誤，它也可能會指出錯誤的發生次數 (括弧內)。

- 拒絕存取 — 列出 Macie 不允許存取的儲存貯體。這些值區的權限設定會阻止 Macie 存取值區和值區的物件。因此，Macie 無法分析這些值區中的任何物件。
- 分類錯誤 — 列出由於物件層級分類錯誤而尚未分析的值區 — 物件層級權限設定、物件內容或配額的問題。

  針對每個值區，「問題」欄位會指出發生的每種錯誤類型的性質，並防止 Macie 分析值區中的物件。它也會指出如何修復每種類型的錯誤。根據錯誤的不同，它也可能會指出錯誤的發生次數 (在括號中)。
- 未分類 — 列出 Macie 無法分析的值區，因為它們不儲存任何可分類的物件。這些儲存貯體中的所有物件均使用不受支援的 Amazon S3 儲存類別，或具有不支援檔案或儲存格式的副檔名。因此，Macie 無法分析這些值區中的任何物件。

4. 若要向下鑽研並複查值區的支援資料，請選擇值區的名稱。然後，請參閱值區詳細資料面板，以取得值區的統計資料和其他相關資訊。
5. 若要將表格匯出為 CSV 檔案，請選擇頁面頂端的「匯出為 CSV」。產生的 CSV 檔案包含表格中每個值區的中繼資料子集，最多可容納 50,000 個值區。該文件包括一個覆蓋問題字段。此欄位的值會指出問題是否阻止 Macie 分析值區中的物件，以及問題的性質 (若有)。

API

若要以程式設計方式檢閱涵蓋範圍資料，請在使用 Amazon Macie API DescribeBuckets操作提交的查詢中指定篩選條件。此操作返回對象的數組。每個物件都包含符合篩選準則的 S3 一般用途儲存貯體的統計資料和其他資訊。

在篩選條件中，包含您要檢閱之涵蓋範圍資料類型的條件：

- 若要識別因為值區的權限設定而不允許 Macie 存取的值區，請加入欄位值等於的條件。`errorCode` `ACCESS_DENIED`
- 若要識別 Macie 允許存取且尚未分析的值區，請包含欄位值等於`50`且`sensitivityScore`欄位值不相等`ACCESS_DENIED`的`errorCode`條件。
- 若要識別 Macie 無法分析的值區，因為所有值區的物件都使用不支援的儲存區類別或格式，請包含`classifiableSizeInBytes`欄位值等於`0`且`sizeInBytes`欄位值大於的條件。`0`
- 若要識別 Macie 已分析至少一個物件的值區，請包含`sensitivityScore`欄位值落在 1—99 範圍內但不等於的條件。`50`若要同時包含您手動指派最高分數的值區，範圍應為 1-100。
- 若要識別 Macie 因物件層級分類錯誤而尚未分析的值區，請加入`sensitivityScore`欄位值等於的條件。`-1`然後若要複查特定值區所發生之類型和錯誤數目的明細，請使用此GetResourceProfile作業。

如果您使用的是 AWS Command Line Interface (AWS CLI)，請在您提交的查詢中指定篩選條件，方法是執行 describe- bucket 命令。若要檢閱特定 S3 儲存貯體發生的類型和錯誤數目的明細 (如果有的話)，請執行get-resource-profile命令。

例如，下列 AWS CLI 命令會使用篩選準則擷取由於儲存貯體的權限設定而不允許 Macie 存取的所有 S3 儲存貯體的詳細資料。

此範例是針對 Linux、macOS 或 Unix 進行格式化：

```
$ aws macie2 describe-buckets --criteria '{"errorCode":{"eq":["ACCESS_DENIED"]}}'
```

這個例子被格式化為 Microsoft 視窗：

```
C:\> aws macie2 describe-buckets --criteria={\"errorCode\":{\"eq\":[\"ACCESS_DENIED
\"]}}
```

如果您的請求成功，Macie 返回一個數組buckets。陣列針對目前儲存貯體中的每個 S3 儲存貯體包含一個物件， AWS 區域 且符合篩選準則。

如果沒有 S3 儲存貯體符合篩選條件，Macie 會傳回空buckets陣列。

```
{
    "buckets": []
}
```

如需有關在查詢中指定篩選條件的詳細資訊，包括一般條件的範例，請參閱篩選 S3 儲存貯體庫存。

修正自動化敏感資料探索的涵蓋範圍問題

Amazon Macie 報告了幾種類型的問題，這些問題可減少 Amazon Simple Storage Service (Amazon S3) 資料的自動化敏感資料探索涵蓋範圍。下列資訊可協助您調查並修正這些問題。

問題類型和詳細資料

- 存取遭拒
- 分類錯誤：無效的內容
- 分類錯誤：無效的加密

- 分類錯誤:無效的 KMS 金鑰
- 分類錯誤：權限被拒
- 未分類

> **Tip**
>
> 若要調查 S3 儲存貯體的物件層級分類錯誤，請先檢閱儲存貯體的物件範例清單。此清單會指出 Macie 在值區中分析或嘗試分析哪些物件，最多 100 個物件。
> 若要檢閱 Amazon Macie 主控台上的清單，請在 S3 儲存貯體頁面上選擇儲存貯體，然後選擇儲存貯體詳細資料面板中的物件範例索引標籤。若要以程式設計方式檢閱清單，請使用 Amazon Macie API 的ListResourceProfileArtifacts作業。如果物件的分析狀況為「略過」(SKIPPED)，則該物件可能已導致錯誤。

存取遭拒

此問題表示 S3 儲存貯體的許可設定會阻止 Macie 存取儲存貯體和儲存貯體的物件。Macie 無法擷取和分析值區中的任何物件。

詳細資訊

造成此類問題的最常見原因是限制性值區政策。儲存貯體政策是以資源為基礎的 AWS Identity and Access Management (IAM) 政策，可指定主體 (使用者、帳戶、服務或其他實體) 可在 S3 儲存貯體上執行的動作，以及主體可以執行這些動作的條件。限制性值區政策會使用明確的`Allow`或`Deny`陳述式，根據特定條件授予或限制儲存貯體資料的存取權。例如，值區政策可能包含拒絕存取值區的`Allow`或`Deny`陳述式，除非使用特定來源 IP 位址存取值區。

如果 S3 儲存貯體政策包含具有一或多個條件的明確`Deny`陳述式，可能不允許 Macie 擷取和分析儲存貯體的物件以偵測敏感資料。Macie 只能提供值區相關資訊的子集，例如值區的名稱和建立日期。

補救指引

若要修復此問題，請更新 S3 儲存貯體的儲存貯體政策。請確定政策允許 Macie 存取值區和值區的物件。若要允許此存取，請將 Macie 服務連結角色 (`AWSServiceRoleForAmazonMacie`) 的條件新增至原則。此條件應排除 Macie 服務連結角色，使其不符合原則中的`Deny`限制。它可以使用您帳戶的 Macie 服務連結角色的`aws:PrincipalArn`全域條件內容金鑰和 Amazon 資源名稱 (ARN) 來執行此操作。

如果您更新儲存貯體政策且 Macie 取得 S3 儲存貯體的存取權，Macie 會偵測變更。發生這種情況時，Macie 將更新統計資料、庫存資料和其他提供的 Amazon S3 資料相關資訊。此外，在後續的分析週期中，值區的物件將成為較高的分析優先順序。

其他參考

如需更新 S3 儲存貯體政策以允許 Macie 存取儲存貯體的詳細資訊，請參閱允許 Amazon Macie 訪問 S3 存儲桶和對象。如需使用儲存貯體政策控制儲存貯體存取的相關資訊，請參閱 Amazon 簡單儲存服務使用者指南中的儲存貯體政策和使用者政策以及 Amazon S3 如何授權請求。

分類錯誤：無效的內容

如果 Macie 嘗試分析 S3 儲存貯體中的物件，且物件格式錯誤，或物件包含超出敏感資料探索配額的內容，就會發生這種類型的分類錯誤。馬西不能分析對象。

詳細資訊

這個錯誤通常是因為 S3 物件是格式錯誤或損毀的檔案。因此，Macie 無法剖析和分析檔案中的所有資料。

如果 S3 物件的分析超出個別檔案的敏感資料探索配額，也會發生此錯誤。例如，物件的儲存大小超過該類型檔案的大小配額。

對於任何一種情況，Macie 都無法完成對 S3 物件的分析，且物件的分析狀態為略過 (SKIPPED)。

補救指引

若要調查此錯誤，請下載 S3 物件並檢查檔案的格式和內容。同時針對敏感資料探索的 Macie 配額來評估檔案內容。

如果您未修復此錯誤，Macie 會嘗試分析 S3 儲存貯體中的其他物件。如果 Macie 成功分析另一個物件，Macie 會更新涵蓋範圍資料及其提供關於值區的其他資訊。

其他參考

如需敏感資料探索配額的清單，包括特定檔案類型的配額，請參閱Amazon Macie 配額。如需 Macie 如何更新敏感度分數及其提供有關 S3 儲存貯體的其他資訊的詳細資訊，請參閱自動化敏感資料探索如何運作。

分類錯誤：無效的加密

如果 Macie 嘗試分析 S3 儲存貯體中的物件，並使用客戶提供的金鑰對物件進行加密，就會發生這種類型的分類錯誤。物件使用 SSE-C 加密，這表示 Macie 無法擷取和分析物件。

詳細資訊

Amazon S3 支援 S3 物件的多個加密選項。對於大多數這些選項，Macie 可以使用您帳戶的 Macie 服務連結角色來解密物件。但是，這取決於所使用的加密類型。

若要讓 Macie 解密 S3 物件，物件必須使用 Macie 可以存取且可以使用的金鑰加密。如果物件使用客戶提供的金鑰加密，Macie 就無法提供必要的金鑰材料來從 Amazon S3 擷取物件。因此，Macie 無法分析物件，且物件的分析狀態為「略過」(SKIPPED)。

補救指引

若要修復此錯誤，請使用 Amazon S3 受管金鑰或 AWS Key Management Service (AWS KMS) 金鑰加密 S3 物件。如果您偏好使用金 AWS KMS 鑰，金鑰可以是 AWS 受管理的 KMS 金鑰，也可以是 Macie 允許使用的客戶管理 KMS 金鑰。

若要使用 Macie 可存取和使用的金鑰加密現有 S3 物件，您可以變更物件的加密設定。若要使用 Macie 可存取和使用的金鑰加密新物件，請變更 S3 儲存貯體的預設加密設定。此外，請確保儲存貯體的政策不需要使用客戶提供的金鑰加密新物件。

如果您未修復此錯誤，Macie 會嘗試分析 S3 儲存貯體中的其他物件。如果 Macie 成功分析另一個物件，Macie 會更新涵蓋範圍資料及其提供關於值區的其他資訊。

其他參考

如需使用 Macie 分析加密 S3 物件的需求和選項的相關資訊，請參閱使用亞馬遜 Macie 分析加密的 Amazon S3 對象。如需 S3 儲存貯體加密選項和設定的相關資訊，請參閱 Amazon Simple Storage 服務使用者指南中的使用加密保護資料和為 S3 儲存貯體設定預設伺服器端加密行為。

分類錯誤:無效的 KMS 金鑰

如果 Macie 嘗試分析 S3 儲存貯體中的物件，並使用不再可用的 AWS Key Management Service (AWS KMS) 金鑰加密物件，就會發生這種類型的分類錯誤。Macie 無法擷取和分析物件。

詳細資訊

AWS KMS 提供停用和刪除客戶管理的選項 AWS KMS keys。如果 S3 物件使用已停用、排定刪除或刪除的 KMS 金鑰加密，Macie 就無法擷取和解密該物件。因此，Macie 無法分析物件，且物件的分析狀態為「略過」(SKIPPED)。若要讓 Macie 分析加密的物件，物件必須使用 Macie 可以存取且可以使用的金鑰加密。

補救指引

若要修正此錯誤，請根據金鑰的目前狀態 AWS KMS key，重新啟用或取消適用項目的排程刪除。如果已刪除適用的金鑰，則無法修正此錯誤。

若要判斷哪個 AWS KMS key 是用來加密 S3 物件，您可以先使用 Macie 檢閱 S3 儲存貯體的伺服器端加密設定。如果儲存貯體的預設加密設定已設定為使用 KMS 金鑰，則儲存貯體的詳細資料會指出使用哪個金鑰。然後，您可以檢查該密鑰的狀態。或者，您可以使用 Amazon S3 檢閱儲存貯體和儲存貯體中個別物件的加密設定。

如果您未修復此錯誤，Macie 會嘗試分析 S3 儲存貯體中的其他物件。如果 Macie 成功分析另一個物件，Macie 會更新涵蓋範圍資料及其提供關於值區的其他資訊。

其他參考

如需使用 Macie 檢閱 S3 儲存貯體的伺服器端加密設定的相關資訊，請參閱檢閱 S3 儲存貯體的詳細資訊。如需有關重新啟用或取消排程刪除的資訊 AWS KMS key，請參閱開發人員指南中的啟用和停用金鑰以及排程和取消金鑰刪除。AWS Key Management Service

分類錯誤：權限被拒

如果 Macie 嘗試分析 S3 儲存貯體中的物件，而因為物件的權限設定或用於加密物件的金鑰的權限設定，Macie 無法擷取或解密該物件，就會發生這種類型的分類錯誤。Macie 無法擷取和分析物件。

詳細資訊

此錯誤通常是因為 S3 物件使用不允許 Macie 使用的客戶管理 AWS Key Management Service (AWS KMS) 金鑰加密。如果使用客戶管理的物件加密 AWS KMS key，則該金鑰的政策必須允許 Macie 使用金鑰解密資料。

如果 Amazon S3 許可設定阻止 Macie 擷取 S3 物件，也可能發生此錯誤。S3 儲存貯體的儲存貯體政策可能會限制對特定儲存貯體物件的存取，或只允許特定主體 (使用者、帳戶、服務或其他實體) 存取物件。或者物件的存取控制清單 (ACL) 可能會限制物件的存取權。因此，Macie 可能無法存取物件。

對於上述任何一種情況，Macie 都無法擷取和分析物件，且該物件的分析狀態為「略過」(SKIPPED)。

補救指引

若要修復此錯誤，請判斷 S3 物件是否透過受管 AWS KMS key的客戶加密。如果是，請確定金鑰的原則允許 Macie 服務連結角色 (AWSServiceRoleForAmazonMacie) 使用金鑰解密資料。允許

此存取的方式取決於擁有該物件的帳戶是否 AWS KMS key 也擁有存放該物件的 S3 儲存貯體。如果相同的帳戶擁有 KMS 金鑰和儲存貯體，則該帳戶的使用者必須更新金鑰的政策。如果一個帳戶擁有 KMS 金鑰，而另一個帳戶擁有該儲存貯體，則擁有該金鑰的帳戶的使用者必須允許跨帳戶存取金鑰。

> **Tip**
>
> 您可以自動產生 Macie 需要存取的所 AWS KMS keys 有受管理客戶清單，以分析您帳戶的 S3 儲存貯體中的物件。若要執行此操作，請執行 AWS KMS 權限分析器指令碼，該指令碼可從 Amazon Macie 指令碼存放庫取 GitHub得。該腳本還可以生成 AWS Command Line Interface (AWS CLI) 命令的其他腳本。您可以選擇性地執行這些命令，為您指定的 KMS 金鑰更新必要的組態設定和原則。

如果 Macie 已被允許使用適用的， AWS KMS key 或者 S3 物件未使用客戶管理的 KMS 金鑰加密，請確定儲存貯體的政策允許 Macie 存取物件。同時驗證物件的 ACL 是否允許 Macie 讀取物件的資料和中繼資料。

對於值區政策，您可以將 Macie 服務連結角色的條件新增至原則，以允許此存取。此條件應排除 Macie 服務連結角色，使其不符合原則中的`Deny`限制。它可以使用您帳戶的 Macie 服務連結角色的`aws:PrincipalArn`全域條件內容金鑰和 Amazon 資源名稱 (ARN) 來執行此操作。

對於物件 ACL，您可以與物件擁有者合作，將您新增 AWS 帳戶 為具有物件權限的受權者，以允許此存取`READ`權。然後，Macie 可以針對您的帳戶使用服務連結角色來擷取和分析物件。此外，也請考慮變更值區的「物件擁有權」設定。您可以使用這些設定來停用值區中所有物件的 ACL，並將擁有權權限授與擁有值區的帳戶。

如果您未修復此錯誤，Macie 會嘗試分析 S3 儲存貯體中的其他物件。如果 Macie 成功分析另一個物件，Macie 會更新涵蓋範圍資料及其提供關於值區的其他資訊。

其他參考

有關允許 Macie 與受管理的客戶解密數據的更多信息 AWS KMS key，請參閱允許 Amazon Macie 使用客戶管理 AWS KMS key。如需更新 S3 儲存貯體政策以允許 Macie 存取儲存貯體的詳細資訊，請參閱允許 Amazon Macie 訪問 S3 存儲桶和對象。

如需更新金鑰原則的詳細資訊，請參閱AWS Key Management Service 開發人員指南中的變更金鑰政策。如需使用受管客戶 AWS KMS keys 來加密 S3 物件的相關資訊，請參閱 Amazon 簡單儲存服務使用者指南中的以 AWS KMS 金鑰使用伺服器端加密。

如需使用儲存貯體政策控制 S3 儲存貯體存取的相關資訊，請參閱 Amazon 簡單儲存服務使用者指南中的儲存貯體政策和使用者政策以及 Amazon S3 如何授權請求。如需使用 ACL 或物件擁有權設定來控制 S3 物件存取的相關資訊，請參閱 Amazon 簡單儲存服務使用者指南中的使用 ACL 管理存取和控制物件擁有權和停用儲存貯體的 ACL。

未分類

此問題表示 S3 儲存貯體中的所有物件均使用不支援的 Amazon S3 儲存類別或不支援的檔案或儲存格式來存放。Macie 無法分析值區中的任何物件。

詳細資訊

為了符合選擇和分析的資格，S3 物件必須使用 Macie 支援的 Amazon S3 儲存類別。物件還必須具有 Macie 支援的檔案或儲存格式的副檔名。如果物件不符合這些準則，則會將物件視為不可分類的物件。Macie 不會嘗試擷取或分析未分類物件中的資料。

如果 S3 儲存貯體中的所有物件都是未分類的物件，則整個儲存貯體就是不可分類的儲存貯體。Macie 無法為值區執行自動化敏感資料探索。

補救指引

若要解決此問題，請檢閱生命週期組態規則和其他設定，以判斷哪些儲存類別用於在 S3 儲存貯體中存放物件。請考慮調整這些設定，以使用 Macie 支援的儲存空間類別。您也可以變更值區中現有物件的儲存空間類別。

同時評估 S3 儲存貯體中現有物件的檔案和儲存格式。若要分析物件，請考慮將資料暫時或永久移植到使用支援格式的新物件。

如果將物件新增至 S3 儲存貯體，且物件使用支援的儲存類別和格式，Macie 會在下次評估儲存貯體庫存時偵測到物件。發生這種情況時，Macie 將停止報告儲存貯體未分類的統計資料、涵蓋範圍資料以及其提供有關 Amazon S3 資料的其他資訊。此外，在後續的分析週期中，新物件將具有較高的分析優先順序。

其他參考

如需 Amazon S3 儲存類別以及 Macie 支援的檔案和儲存格式的相關資訊，請參閱Amazon Macie 支援的儲存類別和格式。如需 Amazon S3 提供的生命週期組態規則和儲存類別選項的詳細資訊，請參閱 Amazon 簡單儲存服務使用者指南中的管理儲存生命週期和使用 Amazon S3 儲存類別。

檢閱自動化的敏感資料探索統計資料和

如果啟用自動化敏感資料探索，Amazon Macie 會自動產生並維護其他有關 Amazon Simple Storage Service (Amazon S3) 一般用途儲存貯體的其他庫存資料、統計資料和其他資訊，這些資訊會監控和分析您的帳戶。如果您是組織的 Macie 管理員，預設情況下會包含您的成員帳戶所擁有的 S3 儲存貯體。

其他資訊會擷取 Macie 迄今為止執行的自動化敏感資料探索活動的結果。它還補充了 Macie 提供有關 Amazon S3 資料的其他資訊，例如個別 S3 儲存貯體的公用存取和加密設定。除了中繼資料和統計資料之外，Macie 還會產生所找到的敏感資料及其執行的分析記錄，包括敏感資料發現項目和敏感資料探索結果。

隨著自動化敏感資料探索每天都在進行，下列功能和資料可協助您檢閱和評估結果：

- 摘要儀表板 — 提供 Amazon S3 資料資產的彙總統計資料。統計資料包括關鍵指標的資料，例如 Macie 在其中找到敏感資料的儲存貯體總數，以及可公開存取的值區數量。他們也會報告影響 Amazon S3 資料涵蓋範圍的問題。
- S3 儲存貯體熱圖 — 提供跨資料資產的資料敏感度的互動式視覺化呈現方式，依據分組 AWS 帳戶。對於每個帳戶，對映都包含彙總的敏感度統計資料，並使用顏色來指示帳戶擁有之每個值區的目前敏感度分數。該地圖還使用符號來幫助您識別可公開訪問，Macie 無法分析的存儲桶等。
- S3 儲存貯體表 — 提供庫存中每個 S3 儲存貯體的摘要資訊。對於每個值區，資料表包含值區目前的敏感度評分、Macie 可以在值區中分析的物件數目，以及您是否設定任何敏感資料探索工作來定期分析值區中的物件。您可以將資料從表格匯出為逗號分隔值 (CSV) 檔案。
- 詳細資料面板 — 提供您在熱圖或表格中選擇的 S3 儲存貯體的詳細資料和統計資料。詳細資料包括 Macie 已在值區中分析過的物件清單，以及 Macie 在值區中找到的敏感資料類型和出現次數的明細資料。您也可以使用面板來管理值區的自動探索設定。
- 敏感資料發現項目 — 提供 Macie 在個別 S3 物件中找到之敏感資料的詳細報告。詳細資料包括 Macie 何時發現敏感資料，以及 Macie 找到的敏感資料的類型和出現次數。詳細資料也包括受影響 S3 儲存貯體和物件的相關資訊，包括儲存貯體的公開存取設定，以及物件最近變更的時間。
- 敏感資料探索結果 — 提供 Macie 針對個別 S3 物件執行的分析記錄。這包括 Macie 無法在其中找到敏感資料的物件，以及 Macie 因問題或錯誤而無法分析的物件。如果 Macie 在物件中找到敏感資料，則敏感資料探索結果會提供 Macie 找到之敏感資料的相關資訊。

使用此資料，您可以評估整個 Amazon S3 資料資產的資料敏感度，並向下鑽研以評估和調查個別 S3 儲存貯體和物件。結合 Macie 提供的有關 Amazon S3 資料安全性和隱私權的資訊，您也可以識別可能需要立即修復的案例，例如 Macie 在其中找到敏感資料的可公開存取儲存貯體。

其他資料可協助您評估和監控 Amazon S3 資料資產的涵蓋範圍。透過涵蓋範圍資料，您可以檢查整體資料資產和儲存貯體庫存中個別 S3 儲存貯體的分析狀態。您也可以找出阻止 Macie 分析特定值區中物件的問題。如果修復問題，您可以在後續的分析週期中增加 Amazon S3 資料的涵蓋範圍。如需詳細資訊，請參閱 評估自動化敏感資料探索範圍。

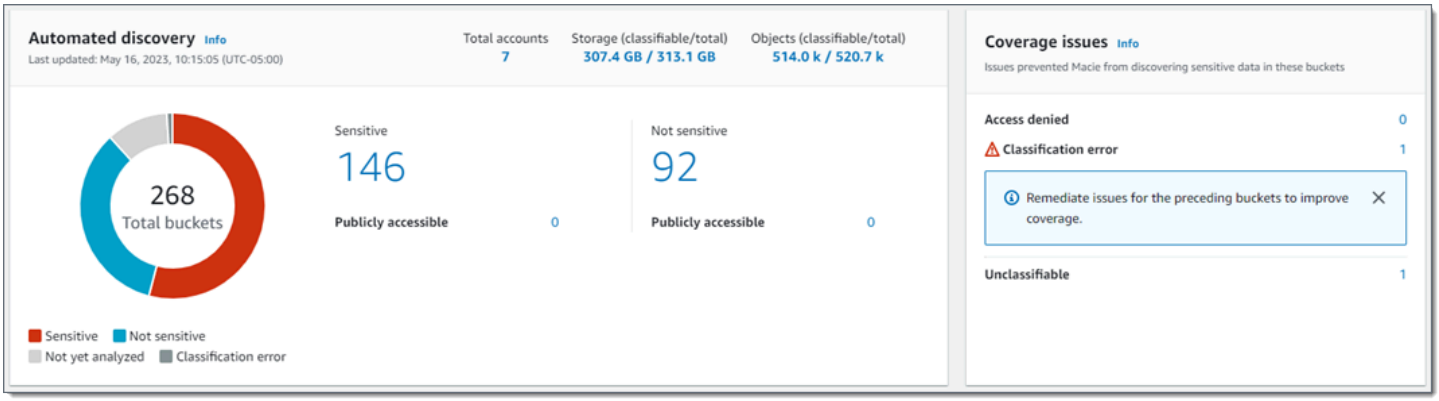
主題

在摘要儀表板上檢閱彙總的資料敏感度統計

在 Amazon Macie 主控台上，摘要儀表板可為您目前的 Amazon Simple Storage Service (Amazon S3) 資料提供彙總統計資料和發現項目 AWS 區域資料的快照。它旨在協助您評估 Amazon S3 資料的整體安全狀態。

儀表板統計資料包括關鍵安全指標的資料，例如可公開存取或與其他人共用的 S3 一般用途儲存貯體數量 AWS 帳戶。儀表板也會顯示您帳戶的彙總發現項目資料群組，例如，在過去七天內產生最多發現項目的值區。如果您是組織的 Macie 管理員，則儀表板會提供組織中所有帳戶的彙總統計資料和資料。您可以選擇按帳戶過濾數據。

如果啟用自動化敏感資料探索，「摘要」儀表板會包含自動探索統計資料。統計資料會擷取 Macie 迄今為止針對 Amazon S3 資料執行的自動化敏感資料探索活動的狀態和結果。例如：



「自動化探索」段落中的統計資料提供目前狀態和自動化敏感資料探索活動結果的快照。資料不包含您已建立和執行之敏感資料探索工作的結果。

涵蓋範圍問題區段中的統計資料會指出問題是否會阻止 Macie 分析個別 S3 儲存貯體中的物件。這些統計資料不會明確包含您已建立和執行之敏感資料探索工作的資料。不過，修正影響自動化敏感資料探索結果的涵蓋範圍問題，也可能會增加您隨後執行之工作的涵蓋範圍。

主題

- 顯示「摘要」儀表板
- 了解摘要儀表板上的自動敏感資料探索統計資料

顯示「摘要」儀表板

請依照下列步驟在 Amazon Macie 主控台上顯示「摘要」儀表板。如果您偏好以程式設計方式查詢統計資料，可以使用 Amazon Macie API 的GetBucketStatistics操作。

顯示「摘要」控制面板

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 在導覽窗格中，選擇摘要。Macie 會顯示「摘要」控制面板。
3. 若要向下鑽研並複查儀表板上項目的支援資料，請選擇該項目。

如果您是組織的 Macie 管理員，儀表板會顯示組織中帳戶和成員帳戶的彙總統計資料和資料。若要篩選儀表板並僅顯示特定帳戶的資料，請在儀表板上方的 [帳戶] 方塊中輸入帳戶的 ID。

了解摘要儀表板上的自動敏感資料探索統計資料

Amazon Macie 主控台上的摘要儀表板包含彙總統計資料，可協助您監控 Amazon S3 資料的自動化敏感資料探索。它提供目前 Amazon S3 資料的目前狀態和分析結果的快照 AWS 區域。

例如，您可以使用儀表板統計資料快速判斷 Amazon Macie 在中找到敏感資料的 S3 儲存貯體數量，以及可公開存取的儲存貯體數量。您也可以評估 Amazon S3 資料的涵蓋範圍，並找出阻止 Macie 分析個別 S3 儲存貯體中物件的問題。

在儀表板上，自動化敏感資料探索統計資料主要分為下列區段：

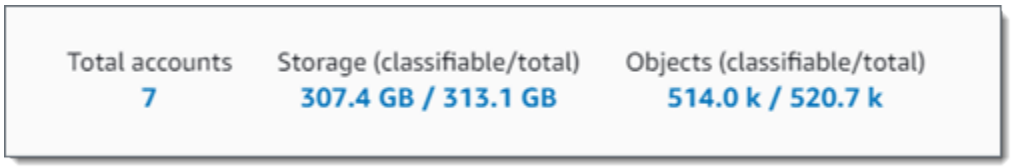
- 儲存和敏感資料探索
- 自動化探索
- 覆蓋問題

複查每個區段時，選擇性地選擇要向下追溯並複查支援資料的料號。另請注意，儀表板不包含 S3 目錄儲存貯體的資料，僅包含一般用途儲存貯體的資料。Macie 不會監視或分析目錄值區。

每個部分的個別統計數據如下。如需「摘要」儀表板其他區段中統計資料的相關資訊，請參閱瞭解「摘要」控制面板的元件。

儲存和敏感資料探索

在「自動化探索」區段的頂端，您會找到統計資料，指出您在 Amazon S3 中存放多少資料，以及 Macie 可以分析多少資料以偵測敏感資料。例如：



在本節中：

- 帳戶總計 — 值區庫存中 AWS 帳戶 該時段的總數。如果您是組織的 Macie 管理員，這是您為組織管理的 Macie 帳戶總數。如果您有獨立的 Macie 帳戶，則此值為 1。
- 儲存空間 — 這些指標提供值區詳細目錄中物件儲存大小的相關資訊：
  - 可分類 — Macie 可以在值區中分析的所有物件的總儲存大小。
  - 總計 — 值區中所有物件的總儲存空間大小，包括 Macie 無法分析的物件。

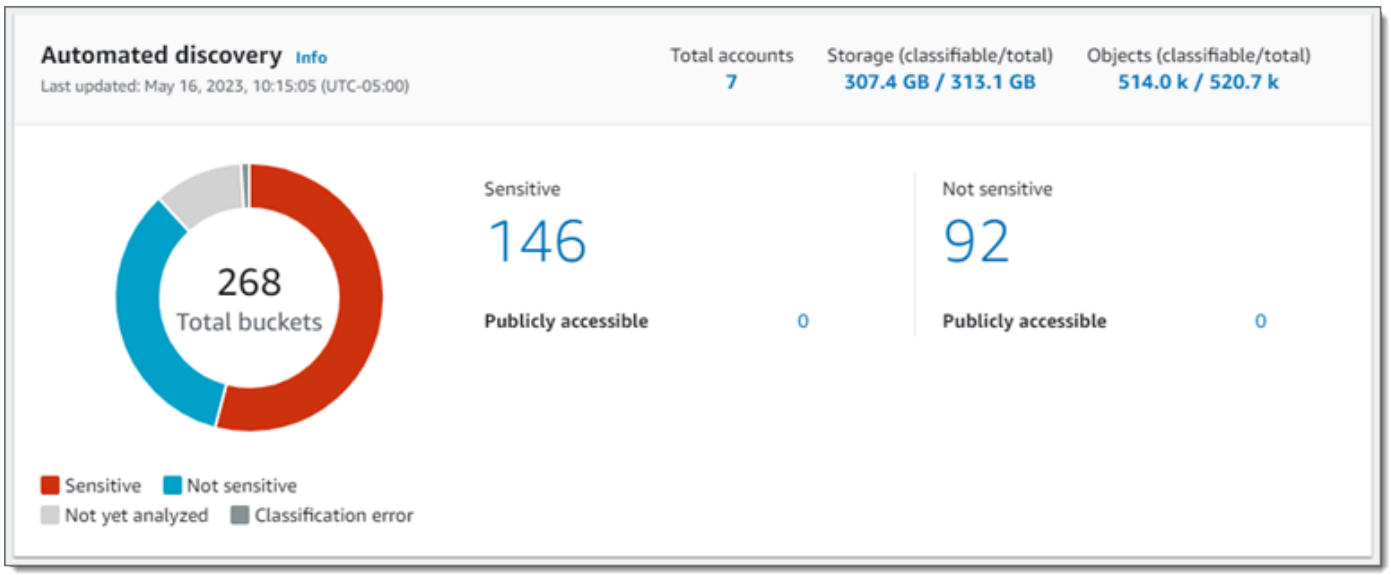
  如果有任何物件是壓縮檔案，這些值在解壓縮後不會反映這些檔案的實際大小。如果已啟用任何值區的版本控制，則這些值會以這些值區中每個物件最新版本的儲存大小為基礎。
- 物件 — 這些指標提供值區詳細目錄中物件數目的相關資訊：
  - 可分類 — Macie 可以在值區中分析的物件總數。
  - 「總計」— 值區中的物件總數，包括 Macie 無法分析的物件。

在上述統計資料中，如果資料和物件使用支援的 Amazon S3 儲存類別，且具有支援的檔案或儲存格式的副檔名，則資料和物件將可分類。您可以通過使用 Macie 檢測對象中的敏感數據。如需詳細資訊，請參閱 支援的儲存類別和格式。

請注意，「儲存體」和「物件」統計資料不會包含 Macie 不允許存取之值區中物件的相關資料。若要識別發生這種情況的值區，請在儀表板的「涵蓋範圍問題」區段中選擇「拒絕存取」統計資料。

自動化探索

這些統計資料主要擷取 Macie 迄今為止針對 Amazon S3 資料執行的自動化敏感資料探索活動的狀態和結果。例如：



本節中的個別統計資料如下。

總桶數

環圈圖會指出時段存貨中的時段總數。圖表會根據每個時段目前的敏感度評分，將值區分組為不同類別：

- 敏感度 (紅色) — 敏感度分數介於 51 到 100 之間的儲存貯體總數。
- 不敏感 (藍色) — 敏感度分數範圍介於 1 到 49 之間的值區總數。
- 尚未分析 (淺灰色) — 敏感度分數為 50 的儲存貯體總數。
- 分類錯誤 (深灰色) — 敏感度分數為 -1 的值區總數。

如需有關 Macie 定義之敏感度分數和標籤範圍的詳細資訊，請參閱S3 儲存貯體的靈敏度評分。

若要檢閱群組的其他統計資料，請將游標暫留在群組上：

- 「桶」— 值區的總數。
- 可公開存取 — 允許一般大眾對儲存貯體具有讀取或寫入存取權的值區總數。
- 可分類位元組 — Macie 可以在值區中分析的所有物件的總儲存大小。這些物件使用支援的 Amazon S3 儲存類別，且具有支援檔案或儲存格式的副檔名。如需詳細資訊，請參閱 支援的儲存類別和格式。
- 位元組總計 — 所有值區的總儲存大小。

在上述統計資料中，儲存區大小值是以值區中每個物件最新版本的儲存體大小為基礎。如果有任何物件是壓縮檔案，這些值在解壓縮後不會反映這些檔案的實際大小。

敏感

此區域指出目前具有 51 到 100 之間的敏感度分數的值區總數。在此群組中，「公開存取」表示也允許一般大眾對值區具有讀取或寫入存取權的值區總數。

不敏感

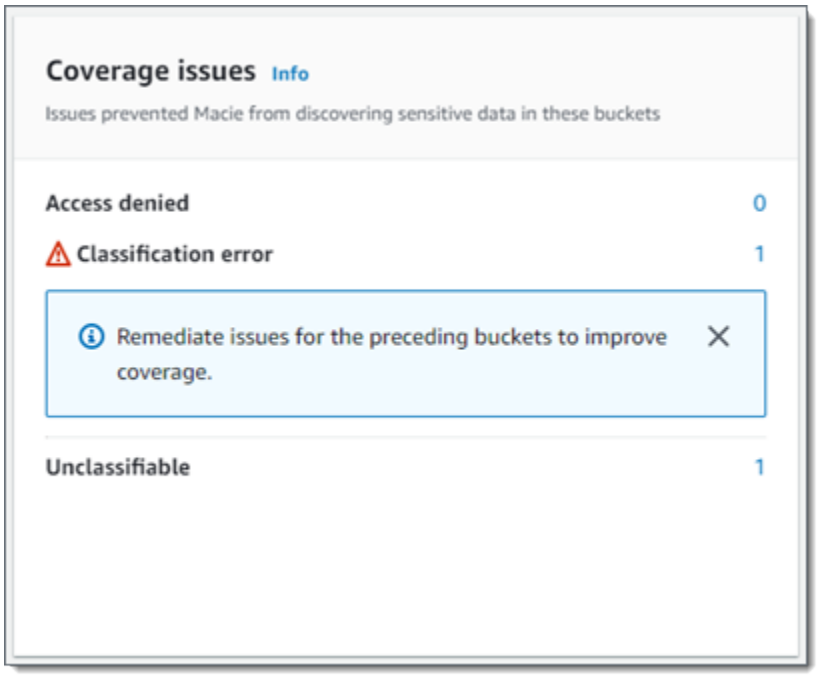
此區域指出目前具有 1 到 49 之間敏感度分數的值區總數。在此群組中，「公開存取」表示也允許一般大眾對值區具有讀取或寫入存取權的值區總數。

為了決定並計算可公開存取的統計資料值，Macie 會分析每個值區的帳戶層級和值區層級設定組合，例如帳戶和值區的區塊公開存取設定，以及值區的值區政策。如需詳細資訊，請參閱 Macie 如何監控 Amazon S3 數據安全。

請注意，[自動化探索] 區段中的統計資料不包含您已建立和執行之敏感資料探索工作的結果。

覆蓋問題

這些統計資料指出某些類型的問題是否會阻止 Macie 分析個別 S3 儲存貯體中的物件。例如：



在本節中：

- 拒絕存取 — Macie 不允許存取的儲存貯體總數。Macie 無法分析這些值區中的任何物件。值區的權限設定會阻止 Macie 存取值區和值區的物件。
- 分類錯誤 — 由於物件層級分類錯誤，Macie 尚未分析的值區總數。Macie 試圖分析這些值區中的一或多個物件。不過，由於物件層級權限設定、物件內容或配額有問題，Macie 無法分析物件。

- 未分類 — 不儲存任何可分類物件的值區總數。Macie 無法分析這些值區中的任何物件。所有物件都使用 Macie 不支援的 Amazon S3 儲存類別，或者它們具有 Macie 不支援的檔案或儲存格式的副檔名。

選擇統計值以顯示其他詳細資訊，以及適用的修正指引。如果您修復存取問題和分類錯誤，可以在後續分析週期中增加 Amazon S3 資料的涵蓋範圍。如需詳細資訊，請參閱 評估自動化敏感資料探索範圍。

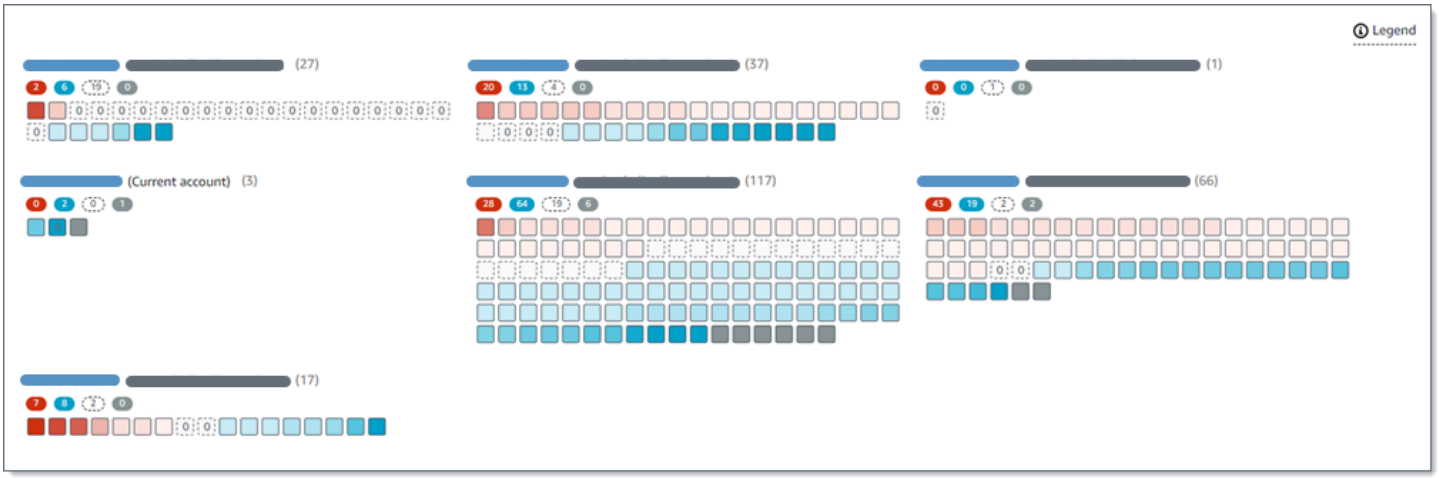
請注意，[覆蓋範圍問題] 區段中的統計資料不會明確包含您已建立和執行之敏感資料探索工作的資料。不過，修正影響自動化敏感資料探索結果的涵蓋範圍問題，也可能會增加您隨後執行之工作的涵蓋範圍。

如需有關「摘要」控制面板其他區段的資訊，請參閱瞭解「摘要」控制面板的元件。

使用 S3 儲存貯體對應視覺化資料敏感度

在 Amazon Macie 主控台上，S3 儲存貯體熱圖提供跨 Amazon Simple Storage Service (Amazon S3) 資料資產的資料敏感度的互動式視覺化表示。它會擷取 Macie 迄今為止針對目 AWS 區域前 Amazon S3 資料執行的自動化敏感資料探索活動的結果。

如果您是組織的 Macie 管理員，則地圖會包含您的成員帳戶所擁有的 S3 儲存貯體的結果。資料會依帳戶 ID 分組， AWS 帳戶 並依帳戶 ID 排序。例如：



地圖的每一頁顯示最多 99 個帳戶或 1,000 個儲存貯體的資料，具體取決於組織或 Amazon S3 資料資產的大小。

若要顯示地圖，請在主控台的導覽窗格中選擇 S3 儲存貯體。然後選擇頁面頂端的 map ()。

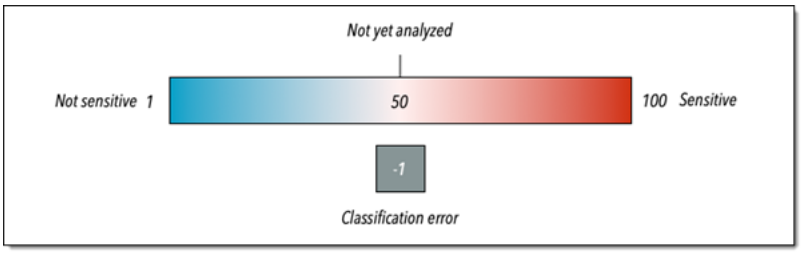
只有當您的帳戶或組織目前已啟用自動敏感資料探索功能時，才能使用對應。它不包含您已建立和執行之敏感資料探索工作的結果。

主題

- 解譯 S3 儲存貯體對應中的資料
- 與 S3 存儲桶映射進行交互

解譯 S3 儲存貯體對應中的資料

在 S3 儲存貯體對應中，每個方形代表儲存貯體庫存中的 S3 一般用途儲存貯體。正方形的顏色代表值區目前的敏感度分數，用來測量兩個主要維度的交集：Macie 在值區中找到的敏感資料量，以及 Macie 在值區中分析的資料量。色彩的色調強度代表值區分數落在資料敏感度值範圍內的位置，如下圖所示。



一般而言，您可以解譯顏色和色相強度，如下所示：

- 藍色 — 如果值區的電流靈敏度分數介於 1 到 49 之間，則值區的方形為藍色，且值區的靈敏度標籤不敏感。藍色色調的強度反映了 Macie 在值區中分析的唯一物件數，相對於值區中唯一物件的總數。較暗的色調表示靈敏度分數較低。
- 無顏色 — 如果值區目前的靈敏度分數為 50，表示桶的方形不會著色，且尚未分析值區的靈敏度標籤。此外，正方形有一個虛線邊框。
- 紅色 — 如果值區的電流靈敏度分數介於 51 到 100 之間，則值區的方形為紅色，而值區的靈敏度標籤為「敏感」。紅色色調的強度反映了 Macie 在存儲桶中找到的敏感數據量。較暗的色調表示靈敏度分數越高。
- 灰色 — 如果值區目前的靈敏度分數為 -1，則值區的方形為深灰色，而值區的靈敏度標籤為分類錯誤。色調強度不會有所不同。

如需有關 Macie 定義之敏感度分數和標籤範圍的詳細資訊，請參閱S3 儲存貯體的靈敏度評分。

在地圖中，S3 存儲桶的正方形也可能包含一個符號。符號表示可能會影響您評估值區敏感度的錯誤、問題或其他類型的考慮因素。符號也可以表示儲存貯體安全性存在潛在問題，例如，值區可公開存取。下表列出了 Macie 用來通知您這些情況的符號。

符號	定義	描述
	存取遭拒	Macie 不允許存取值區或值區的物件。因此，Macie 無法分析值區中的任何物件。 這個問題通常是因為值區具有限制性的值區政策。如需如何解決此問題的詳細資訊，請參閱允許 Macie 存取 S3 儲存貯體和物件。
	可公開存取	公眾對存儲桶具有讀取或寫入訪問權限。 為了做出此決定，Macie 會分析每個值區的帳戶層次與時段層次設定組合，例如帳戶與值區的區塊公用存取設定，以及值區的值區政策。如需詳細資訊，請參閱 Macie 如何監控 Amazon S3 數據安全。
	未分類	Macie 無法分析值區中的任何物件。儲存貯體的所有物件都使用 Macie 不支援的 Amazon S3 儲存類別，或者它們具有 Macie 不支援的檔案或儲存格式的副檔名。 若要讓 Macie 分析物件，物件必須使用支援的儲存類別，並具有支援檔案或儲存格式的副檔名。如需詳細資訊，請參閱支援的儲存類別和格式。
	零位元組	值區不會儲存任何物件供 Macie 進行分析。值區是空

符號	定義	描述
		的，或值區中的所有物件都包含零 (0) 個位元組的資料。

與 S3 存儲桶映射進行交互

檢閱 S3 儲存貯體對應時，您可以透過不同的方式與其互動，以顯示和評估個別帳戶和儲存貯體的其他資料和詳細資料。請依照下列步驟在 Amazon Macie 主控台上顯示地圖，並使用其提供的各種功能。

若要與 S3 儲存貯體對應互動

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 在導覽窗格中，選擇 S3 儲存貯體。S3 儲存貯體頁面會顯示儲存貯體庫存的地圖。如果頁面以表格格式顯示您的庫存，請選擇頁面頂端的 map ()。

   根據預設，地圖不會顯示目前從自動化敏感資料探索中排除的值區的資料。如果您是組織的 Macie 管理員，它也不會顯示目前已停用自動化敏感資料探索功能的帳戶資料。若要顯示此資料，請在篩選器方塊下方的 [由自動探索篩選器權杖監視] 中選擇 [X]。
3. 在頁面頂端，選擇性地選擇重新整理 () 以從 Amazon S3 擷取最新的儲存貯體中繼資料。
4. 在 S3 儲存貯體對應中，執行下列任一項作業：

   - 要確定有多少個桶具有特定的靈敏度標籤，請參閱 AWS 帳戶 ID 下方的彩色徽章。徽章會顯示彙總值區計數，並依敏感度標籤細分。

     例如，紅色標記會報告帳戶擁有且具有敏感標籤的值區總數。這些值區的靈敏度分數介於 51 到 100 之間。藍色標記會報告帳戶擁有且具有「不敏感」標籤的值區總數。這些值區的靈敏度分數範圍介於 1 到 49 之間。
   - 若要檢視值區的相關資訊子集，請將滑鼠游標暫留在值區的正方形上。彈出式視窗會顯示值區的名稱和目前的敏感度分數。

     酥料餅也會顯示 Macie 可以在值區中分析的物件總數，以及這些物件最新版本的總儲存大小。這些物件是可分類的。他們使用支援的 Amazon S3 儲存類別，且具有支援檔案或儲存格式的副檔名。如需詳細資訊，請參閱 支援的儲存類別和格式。

- 若要篩選地圖並僅顯示具有特定欄位值的值區，請將游標置於篩選方塊中，然後為欄位新增篩選條件。Macie 會套用條件的條件，並在篩選方塊下方顯示條件。若要進一步細化結果，請新增其他欄位的篩選條件。如需詳細資訊，請參閱 篩選 S3 儲存貯體庫存。
- 若要向下追溯並僅顯示特定帳戶所擁有的值區，請選擇該帳戶的帳戶 ID。Macie 打開一個新選項卡，該選項卡僅過濾和顯示該帳戶的數據。

5. 若要檢閱特定值區的所有敏感資料探索統計資料和其他資訊，請選擇值區的方塊，然後參閱詳細資料面板。如需這些詳細資訊，請參閱複查個別 S3 儲存貯體的資料敏感度詳細。

> **Tip**
>
> 在面板的「值區詳細資訊」標籤上，您可以對許多欄位進行樞紐分析和向下鑽研。若要顯示欄位具有相同值的值區，請在欄位中選擇。若要顯示具有欄位其他值的值區，請在欄位中選擇。

使用 S3 儲存貯體表評估資料敏感度

在 Amazon Macie 主控台上，S3 儲存貯體表會顯示目前 AWS 區域每個 Amazon Simple Storage Service (Amazon S3) 一般用途儲存貯體的摘要資訊。如果您是某個組織的 Macie 管理員，這包括您的成員帳戶所擁有的值區的相關資訊。如果您偏好以程式設計方式存取資料，可以使用 Amazon Macie API 的DescribeBuckets操作。

在主控台上，您可以排序和篩選表格以自訂檢視。您也可以將資料從表格匯出至逗號分隔值 (CSV) 檔案。如果您在表格中選擇 S3 儲存貯體，詳細資料面板會顯示有關儲存貯體的其他資訊。這包括設置和指標的詳細信息和統計信息，可提供值區數據的安全性和隱私性的洞察力。如果啟用了自動化敏感資料探索，它也會包含擷取 Macie 迄今為止為儲存貯體執行的自動化探索活動結果的資料。除了檢閱這些詳細資料之外，您還可以使用面板來調整值區的自動探索設定。如要瞭解如何作業，請參閱管理個別 S3 儲存貯體的自動化敏感資料探索。

使用 S3 儲存貯體表評估資料敏感度

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 在導覽窗格中，選擇 S3 儲存貯體。S3 儲存貯體頁面會顯示儲存貯體庫存。

根據預設，頁面不會顯示目前從自動化敏感資料探索中排除的值區的資料。如果您是組織的 Macie 管理員，它也不會顯示目前已停用自動化敏感資料探索功能的帳戶資料。若要顯示此資料，請在篩選器方塊下方的 [由自動探索篩選器權杖監視] 中選擇 [X]。

3. 選擇頁面頂端的表格

   ()。Ma

   會顯示庫存中的值區數量，以及值區表格。

4. 若要從 Amazon S3 擷取最新的儲存貯體中繼資料，請選擇頁面頂端的重新整理

   ()。

   如果資訊圖示

   ()

   出現在任何值區名稱旁，我們建議您這麼做。此圖示表示儲存貯體是在過去 24 小時內建立的，可能是在 Macie 上次從 Amazon S3 擷取儲存貯體和物件中繼資料作為每日重新整理週期的一部分之後。

5. 在 S3 儲存貯體表格中，檢閱有關庫存中每個儲存貯體的摘要資訊：

   - 靈敏度 — 值區目前的靈敏度分數。如需有關 Macie 定義之敏感度分數範圍的資訊，請參閱S3 儲存貯體的靈敏度評分。
   - 「值區」— 值區的名稱。
   - 帳號 — 擁有值區 AWS 帳戶 的帳號 ID。
   - 可分類的物件 — Macie 可以分析以偵測值區中敏感資料的物件總數。
   - 可分類大小 — Macie 可以分析以偵測值區中敏感資料的所有物件的總儲存大小。

     這個值不會反映任何壓縮物件解壓縮之後的實際大小。此外，如果值區已啟用版本控制，則此值會根據值區中每個物件最新版本的儲存大小而定。
   - 依工作監控 — 是否將任何敏感資料探索工作設定為每日、每週或每月定期分析值區中的物件。

     如果此欄位的值為「是」，則時段會明確納入週期性工單中，或符合過去 24 小時內週期性工單之條件的時段。此外，其中至少有一個工作的狀態為「未取消」。Macie 每天都會更新此數據。
   - 最新工作執行 — 如果將任何一次性或定期敏感資料探索工作配置為分析值區中的物件，則此欄位會指出其中一個工作開始執行的最近日期和時間。否則，此欄位中會出現一個破折號 (—)。

在上述資料中，如果物件使用支援的 Amazon S3 儲存類別，且物件具有支援檔案或儲存格式的副檔名，則物件即可分類。您可以通過使用 Macie 檢測對象中的敏感數據。如需詳細資訊，請參閱支援的儲存類別和格式。

6. 若要使用表格分析庫存，請執行下列任一項作業：

   - 若要依特定欄位對表格進行排序，請選擇欄位的欄標題。若要變更排序順序，請再次選擇欄標題。
   - 若要篩選表格並僅顯示具有特定欄位值的值區，請將游標置於篩選方塊中，然後新增欄位的篩選條件。Macie 會套用條件的條件，並在篩選方塊下方顯示條件。若要進一步細化結果，請新增其他欄位的篩選條件。如需詳細資訊，請參閱 篩選 S3 儲存貯體庫存。
   - 若要檢閱特定值區的敏感資料探索統計資料和其他資訊，請在表格中選擇值區的名稱，然後參閱詳細資料面板。如需這些詳細資訊，請參閱檢閱 S3 儲存貯體詳情。

   > **Tip**
   >
   > 在面板的「值區詳細資訊」標籤上，您可以對許多欄位進行樞紐分析和向下鑽研。若要顯示欄位具有相同值的值區，請在欄位中選擇。若要顯示具有欄位其他值的值區，請在欄位中選擇。

7. 若要將資料從表格匯出至 CSV 檔案，請選取要匯出之每一列的核取方塊，或選取選取欄標題中的核取方塊以選取所有列。然後選擇頁面頂端的「匯出為 CSV」。您最多可以從表格中匯出 50,000 列。
8. 若要對一或多個時段中的物件執行更深入、更即時的分析，請勾選每個值區的核取方塊，然後選擇 [建立工作]。如需詳細資訊，請參閱 建立敏感資料探索任務。

複查個別 S3 儲存貯體的資料敏感度詳細

在 Amazon Macie 主控台上，您可以使用 S3 儲存貯體頁面上的詳細資料面板來檢閱 Macie 監控和分析您帳戶的每個 Amazon Simple Storage Service (Amazon S3) 一般用途儲存貯體的相關統計資料和其他資訊。如果您是組織的 Macie 管理員，這包括您的成員帳戶所擁有的值區。

統計資料和資訊包括詳細資訊，可深入瞭解 S3 儲存貯體資料的安全性和隱私權。如果啟用了自動化敏感資料探索，它們也會擷取 Macie 迄今為止針對值區執行的自動化探索活動的結果。例如，您可以找到 Macie 在值區中分析過的物件清單，以及 Macie 在值區中找到的敏感資料類型和出現次數的明細資料。請注意，資料不包含您已建立和執行之敏感資料探索工作的結果。

Macie 在執行自動化敏感資料探索時，會自動重新計算和更新這些統計資料和詳細資料。例如：

- 如果 Macie 在 S3 物件中找不到敏感資料，Macie 會降低儲存貯體的敏感度分數，並視需要更新儲存貯體的敏感度標籤。Macie 也會將物件新增至值區中分析的物件清單中。
- 如果 Macie 在 S3 物件中找到敏感資料，Macie 會將這些發生次數新增至 Macie 在儲存貯體中找到的敏感資料類型劃分中。Macie 也會提高儲存貯體的靈敏度分數，並視需要更新值區的靈敏度標籤。此外，Macie 會將物件新增至值區中分析的物件清單中。這些工作除了為物件建立敏感資料尋找項目之外。
- 如果 Macie 在 S3 物件中發現隨後變更或刪除的敏感資料，Macie 會從儲存貯體的敏感資料類型劃分中移除該物件的敏感資料。Macie 也會降低值區的靈敏度分數，並視需要更新值區的靈敏度標籤。此外，Macie 會從值區中分析的物件清單中移除該物件。
- 如果 Macie 嘗試分析 S3 物件，但出現問題或錯誤導致 Macie 無法分析，Macie 會將該物件新增至儲存貯體中分析的物件清單，並指出無法分析該物件。

除了檢閱統計資料和詳細資料之外，您還可以使用面板調整 S3 儲存貯體的自動化敏感資料探索設定。例如，您可以在值區的分數中包含或排除特定類型的敏感資料。如需詳細資訊，請參閱 管理個別 S3 儲存貯體的自動化探索。

若要檢閱 S3 儲存貯體的資料敏感度詳細資料

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 在導覽窗格中，選擇 S3 儲存貯體。S3 儲存貯體頁面會顯示儲存貯體庫存的互動式地圖。選擇性地選擇頁面頂端的表格
   ()，
   以表格形式顯示您的存貨。

   根據預設，頁面不會顯示目前從自動化敏感資料探索中排除的值區的資料。如果您是組織的 Macie 管理員，它也不會顯示目前已停用自動化敏感資料探索功能的帳戶資料。若要顯示此資料，請在篩選器方塊下方的 [由自動探索篩選器權杖監視] 中選擇 [X]。
3. 在 S3 儲存貯體對應或表格中，選擇您要檢閱其詳細資訊的 S3 儲存貯體。詳細資料面板會顯示值區的統計資料和其他相關資訊。

面板頂端會顯示值區的一般資訊：值區的名稱，以及擁有 AWS 帳戶 該值區的帳號 ID。它還提供了用於變更值區的某些自動化敏感資料探索設定的選項。值區的其他設定和資訊分為下列索引標籤：

- 靈敏度
- 鏟斗細節
- 物件範例
- 敏感性資料探索

每個標籤上的個別設定和資訊如下。

靈敏度

此標籤顯示值區目前的靈敏度分數，範圍從 -1 到 100。如需有關 Macie 定義之敏感度分數範圍的資訊，請參閱S3 儲存貯體的靈敏度評分。

此索引標籤也會提供 Macie 在值區物件中找到的敏感資料類型明細，以及每種類型的出現次數：

- 敏感資料類型 — 偵測到資料的受管理資料識別碼的唯一識別碼 (ID)，或偵測到資料的自訂資料識別碼的名稱。

  受管資料識別碼的 ID 描述識別碼設計用來偵測的敏感資料類型，例如，美國護照號碼的 USA_PASSPORT_NUMBER。如需每個受管資料識別碼的詳細資訊，請參閱使用受管資料識別符。
- 計數 — 受管理或自訂資料識別碼偵測到的資料出現次數總數。
- 評分狀態 — 指定資料的出現次數是否包含在值區的敏感度分數之外。

  如果您已將 Macie 設定為自動計算值區的分數，您可以在值區分數中包含或排除特定類型的敏感資料來調整計算：勾選要包含或排除的資料識別碼核取方塊，然後在「動作」功能表中選擇您要的選項。如需詳細資訊，請參閱 管理個別 S3 儲存貯體的自動化探索。

如果 Macie 在值區目前儲存的物件中找不到敏感資料，本節會顯示「找不到偵測」訊息。

請注意，「敏感度」索引標籤不包含 Macie 分析並隨後變更或刪除之物件的資料。如果在 Macie 分析物件後從值區中變更或刪除物件，Macie 會自動重新計算並更新適當的統計資料和資料，以排除物件。

鏟斗細節

此索引標籤提供值區設定的詳細資訊，包括資料安全性和隱私權設定。例如，您可以檢閱值區的公開存取設定細分，並判斷值區是否複製物件或與其他人共用。 AWS 帳戶

特別注意的是，「上次更新」欄位會指出 Macie 最近從 Amazon S3 擷取儲存貯體或儲存貯體物件的中繼資料的時間。[最新的自動化探索執行] 欄位會指出 Macie 最近在執行自動探索時分析值區中物件的時間。如果尚未進行此分析，則此欄位中會出現破折號 (—)。

此索引標籤也提供物件層級統計資料，協助您評估 Macie 可以在值區中分析多少資料量。它也會指出是否設定任何敏感資料探索工作來分析值區中的物件。如果有，您可以存取最近執行之工作的詳細資訊，然後選擇性地顯示工作產生的任何發現項目。

如需有關此標籤上資訊的其他詳細資訊，請參閱檢閱 S3 儲存貯體的詳細資訊。

物件範例

此標籤列出 Macie 在為值區執行自動化敏感資料探索時選取進行分析的物件。選擇性地選擇物件的名稱以開啟 Amazon S3 主控台並顯示物件的屬性。

此清單包含多達 100 個物件的資料。系統會根據「物件敏感度」欄位的值填入清單：「敏感」，接著是「不敏感」，接著是 Macie 無法分析的物件。

在清單中，物件敏感度欄位會指出 Macie 是否在物件中找到敏感資料：

- 敏感 — Macie 在物件中找到至少一次出現的敏感資料。
- 不敏感 — Macie 在物件中找不到敏感資料。
- — (破折號) — 由於問題或錯誤，Macie 無法完成對物件的分析。

「分類結果」欄位會指出 Macie 是否能夠分析物件：

- 完成 — Macie 完成了對物件的分析。
- 部分 — 由於問題或錯誤，Macie 僅分析了對象中的數據子集。例如，物件是一個封存檔案，其中包含不支援格式的檔案。
- 略過 — 由於問題或錯誤，Macie 無法分析物件中的任何資料。例如，物件會使用 Macie 不允許使用的金鑰加密。

請注意，此清單不包含在 Macie 分析或嘗試分析後變更或刪除的物件。如果隨後變更或刪除物件，Macie 會自動從清單中移除物件。

敏感性資料探索

此索引標籤提供儲存貯體的彙總自動化敏感資料探索統計資料：

- 分析的位元組 — Macie 在值區中分析的資料總量 (以位元組為單位)。
- 可分類位元組 — Macie 可以在值區中分析的所有物件的儲存大小總計 (位元組)。這些物件使用支援的 Amazon S3 儲存類別，且具有支援檔案或儲存格式的副檔名。如需詳細資訊，請參閱 支援的儲存類別和格式。

- 偵測總數 — Macie 在值區中找到的敏感資料出現次數總數。這包括目前由值區的敏感度評分設定所抑制的發生次數。

「物件分析」圖表會指出 Macie 在值區中分析過的物件總數。它還提供了 Macie 在其中找到或未找到敏感數據的對象數量的可視化表示。圖表下方的圖例顯示了這些結果的細目：

- 敏感物件 (紅色) — Macie 在其中找到至少一次出現的機密資料的物件總數。
- 非敏感物件 (藍色) — Macie 未在其中找到敏感資料的物件總數。
- 略過的物件 (深灰色) — Macie 因問題或錯誤而無法分析的物件總數。

圖表圖例下方的區域提供了因為發生某些類型的權限問題或密碼編譯錯誤而無法分析物件的情況的明細資訊：

- 略過：無效的加密 — 使用客戶提供的金鑰加密的物件總數。馬西不能訪問這些密鑰。
- 略過：無效的 KMS — 使用 AWS Key Management Service (AWS KMS) 金鑰加密且無法再使用的物件總數。這些物件會使用 AWS KMS keys 已停用、排定刪除或刪除的物件加密。馬西不能使用這些按鍵。
- 略過：權限被拒絕 — 由於物件的權限設定，或是用來加密物件之金鑰的權限設定，所以 Macie 無法存取的物件總數。

如需有關可能發生的這些問題和其他類型的問題和錯誤的詳細資訊，請參閱修正自動化敏感資料探索的涵蓋範圍問題。如果您修復問題和錯誤，則可以在後續分析週期中增加值區資料的涵蓋範圍。

敏感資料探索索引標籤上的統計資料不包含 Macie 分析或嘗試分析物件之後變更或刪除的資料。如果在 Macie 分析或嘗試分析物件後從值區中變更或刪除物件，Macie 會自動重新計算這些統計資料以排除這些物件。

分析自動化探索所產生的敏感資料發現

在執行自動化敏感資料探索時，Amazon Macie 會為尋找敏感資料的每個 Amazon Simple Storage Service (Amazon S3) 物件建立敏感資料尋找。敏感資料發現是 Macie 在 S3 物件中找到的敏感資料的詳細報告。每個敏感資料發現都會提供嚴重性等級和詳細資料，例如：

- Macie 發現敏感數據的日期和時間。
- Macie 發現的敏感數據的類別和類型。
- Macie 找到的每種敏感資料類型的出現次數。
- Macie 如何發現敏感數據，自動化敏感數據發現或敏感數據發現任務。
- 名稱、公用存取設定、加密類型，以及受影響 S3 儲存貯體和物件的其他相關資訊。

視受影響的 S3 物件的檔案類型或儲存格式而定，詳細資料也可能包括 Macie 找到多達 15 次出現之敏感資料的位置。敏感數據發現不包括 Macie 發現的敏感數據。相反地，它會提供資訊，供您視需要用於進一步調查和補救。

Macie 會將您的敏感資料發現儲存 90 天。您可以通過使用 Amazon Macie 控制台或 Amazon Macie API 訪問它們。您也可以使用其他應用程式、服務和系統來監視和處理發現項目。如需詳細資訊，請參閱 分析發現。

分析自動化敏感資料探索所產生的發現項目

若要識別和分析 Macie 在執行自動化敏感資料探索時所建立的發現項目，您可以篩選發現項目。透過篩選器，您可以使用發現項目的特定屬性來建立發現項目的自訂檢視和查詢。您可以使用 Amazon Macie 主控台篩選發現項目，或使用 Amazon Macie API 以程式設計方式提交查詢。

Console

請遵循下列步驟，使用 Amazon Macie 主控台識別和分析發現結果。

分析自動化探索產生的發現項目

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 在導覽窗格中，選擇調查結果。
3. (選擇性) 若要顯示抑制規則所抑制的發現項目，請變更「發現項目」狀態設定。選擇「全部」以顯示隱藏與未抑制的搜尋結果，或選擇「已存檔」以僅顯示隱藏的搜尋結果。若要再次隱藏隱藏的發現項目，請選擇目前。
4. 將光標放在「過濾條件」框中。在顯示的欄位清單中，選擇「原點類型」。

   此欄位指定 Macie 如何找到產生尋找、自動化敏感資料探索或敏感資料探索工作的敏感資料。若要在篩選欄位清單中尋找此欄位，您可以瀏覽完整清單，或輸入部分欄位名稱以縮小欄位清單。
5. 選取 [自動 _ 敏感資料探索] 做為欄位的值，然後選擇 [套用]。Macie 會套用篩選條件，並將條件新增至 [篩選條件] 方塊中的篩選器權杖。
6. (選擇性) 若要精簡結果，請為其他欄位新增篩選條件 — 例如，針對建立發現項目時的時間範圍建立、受影響儲存貯體名稱的 S3 儲存貯體名稱，或針對偵測到並產生發現項目的敏感性資料偵測類型的敏感性資料偵測類型。如需詳細資訊，請參閱 篩選問題清單。

如果您隨後想要再次使用這組條件，您可以將其儲存為篩選規則。若要這麼做，請在 [篩選條件] 方塊中選擇 [儲存規則]。然後輸入規則的名稱和描述 (選擇性)。完成後，請選擇儲存。

API

若要以程式設計方式識別和分析發現項目，請在使用 Amazon Macie API ListFindings或GetFindingStatistics操作提交的查詢中指定篩選條件。此ListFindings作業會傳回尋找 ID 的陣列，每個符合篩選準則的發現項目都有一個 ID。然後，您可以使用這些 ID 來擷取每個發現項目的詳細資訊。此GetFindingStatistics作業會傳回符合篩選準則之所有發現項目的彙總統計資料，並依您在要求中指定的欄位分組。如需有關以程式設計方式篩選發現項目的詳細篩選問題清單資

在篩選條件中，包括originType欄位的條件。此欄位指定 Macie 如何找到產生尋找、自動化敏感資料探索或敏感資料探索工作的敏感資料。此欄位的值是AUTOMATED_SENSITIVE_DATA_DISCOVERY否在執行自動化探索時產生了發現項目。

若要識別並使用 AWS Command Line Interface (AWS CLI) 分析發現項目，請執行清單發現項目或get-finding-statistics命令。下列範例會使用list-findings命令來擷取目前自動化敏感資料探索所產生之所有高嚴重性發現項目的尋找項目 AWS 區域 ID。

對於 Linux、macOS 或 Unix，請使用反斜線 (\) 行接續字元來提高可讀性：

```
$ aws macie2 list-findings \
--finding-criteria '{"criterion":{"classificationDetails.originType":{"eq":
["AUTOMATED_SENSITIVE_DATA_DISCOVERY"]},"severity.description":{"eq":["High"]}}}'
```

對於 Microsoft Windows，使用脫字符號（^）行繼續字符來提高可讀性：

```
C:\> aws macie2 list-findings ^
--finding-criteria={\"criterion\":{\"classificationDetails.originType\":{\"eq
\":[\"AUTOMATED_SENSITIVE_DATA_DISCOVERY\"]},\"severity.description\":{\"eq\":
[\"High\"]}}}
```

其中：

- classificationDetails.originType指定原始類型欄位的 JSON 名稱，以及：
  - eq指定等於運算子。
  - AUTOMATED_SENSITIVE_DATA_DISCOVERY是欄位的列舉值。
- *severity.description*指定嚴重性欄位的 JSON 名稱，並且：
  - *eq*指定等於運算子。
  - *High*是欄位的列舉值。

如果命令運行成功，Macie 返回一個findingIds數組。陣列會列出符合篩選準則之每個發現項目的唯一識別碼，如下列範例所示。

```
{
    "findingIds": [
        "1f1c2d74db5d8caa76859ec52example",
        "6cfa9ac820dd6d55cad30d851example",
        "702a6fd8750e567d1a3a63138example",
        "826e94e2a820312f9f964cf60example",
        "274511c3fdcd87010a19a3a42example"
    ]
}
```

如果沒有發現符合篩選條件，Macie 會傳回空findingIds陣列。

```
{
    "findingIds": []
}
```

存取自動化探索產生的敏感資料探索結果

Amazon Macie 會在執行自動化敏感資料探索時，為選擇用於分析的每個 Amazon 簡單儲存服務 (Amazon S3) 物件建立分析記錄。這些記錄稱為敏感資料探索結果，記錄 Macie 在個別 S3 物件上執行之分析的詳細資料。這包括 Macie 在其中找不到敏感資料的物件，以及 Macie 因權限設定或使用不支援的檔案或儲存格式等錯誤或問題而無法分析的物件。

如果 Macie 在 S3 物件中找到敏感資料，敏感資料探索結果會提供 Macie 找到之敏感資料的相關資訊。這些資訊包含敏感資料尋找項目所提供的相同類型詳細資料。它還提供了其他信息，例如 Macie 發現的每種類型敏感數據的多達 1,000 次出現的位置。例如：

- 在 Microsoft Excel 活頁簿、CSV 檔案或 TSV 檔案中的儲存格或欄位的欄和列號
- JSON 或 JSON 行檔案中欄位或陣列的路徑
- CSV、JSON、JSON 行或 TSV 檔案以外的非二進位文字檔案中的行號，例如 HTML、TXT 或 XML 檔案
- Adobe 可攜式文件格式 (PDF) 檔案中頁面的頁碼
- 記錄索引和路徑在一個 Apache 的 Avro 對象容器或 Apache 實木複合地板文件中的記錄字段

如果受影響的 S3 物件是封存檔案 (例如 .tar 或 .zip 檔案)，敏感資料探索結果也會針對 Macie 從封存中擷取的個別檔案中出現的敏感資料提供詳細位置資料。Macie 不會在封存檔案的敏感資料發現項目中包含此資訊。若要報告位置資料，敏感資料探索結果會使用標準化的 JSON 結構定義。

敏感資料探索結果不包含 Macie 找到的敏感資料。相反，它為您提供了一個分析記錄，可以幫助您進行數據隱私和保護審核或調查。

Macie 會將您的敏感資料探索結果儲存 90 天。您無法直接在 Amazon Macie 控制台或使用 Amazon Macie API 訪問它們。相反，您可以將 Macie 設定為加密並將其存放在 S3 儲存貯體中。儲存貯體可作為所有敏感資料探索結果的明確長期存放庫。然後，您可以選擇性地存取和查詢該儲存庫中的結果。

若要判斷此儲存庫適用於您帳戶的位置，請在 Amazon Macie 主控台的導覽窗格中選擇「探索結果」。要以編程方式執行此GetClassificationExportConfiguration操作，請使用 Amazon Macie API 的操作。如果您尚未為您的帳戶設定此儲存庫，請參閱儲存及保留敏感資料探索結果以瞭解如何進行。

將 Macie 設定為將敏感資料探索結果儲存在 S3 儲存貯體之後，Macie 會將結果寫入 JSON 行 (.jsonl) 檔案，並將這些檔案加密並以 GNU Zip (.gz) 檔案的形式新增至儲存貯體。對於自動化敏感資料探索，Macie 會將檔案新增至值區`automated-sensitive-data-discovery`中名為的資料夾。

如同敏感資料發現項目的情況一樣，敏感資料探索結果會遵循標準化結構描述。這可協助您選擇性地使用其他應用程式、服務和系統來查詢、監控和處理這些項目。

> **Tip**
>
> 有關如何查詢和使用敏感資料探索結果來分析和報告潛在資料安全風險的詳細說明範例，請參閱安全部落格上的如何使用 Amazon Athena 和 Amazon QuickSight 部落格文章查詢和視覺化 Macie 敏感資料探索結果。AWS
> 如需可用來分析敏感資料探索結果的 Athena 查詢範例，請造訪上 GitHub的 Amazon Macie 結果分析儲存庫。此儲存庫也提供設定 Athena 擷取和解密結果的指示，以及建立結果表格的指令碼。

S3 儲存貯體的靈敏度評分

如果啟用自動化敏感資料探索，Amazon Macie 會自動計算和指派敏感度分數給每個 Amazon Simple Storage Service (Amazon S3) 一般用途儲存貯體，以監控和分析帳戶或組織。敏感度分數是 S3 儲存貯體可能包含之敏感資料量的量化表示。根據該分數，Macie 也會為每個值區指派一個敏感度標籤。敏感度標籤是值區靈敏度分數的定性表示。這些值可作為參考點，用於確定敏感資料可能存放在 Amazon S3 資料資產中的位置，以及識別和監控該資料的潛在安全風險。

根據預設，S3 儲存貯體的敏感度分數和標籤會反映 Macie 迄今為止為儲存貯體執行的自動化敏感資料探索活動的結果。它們不會反映您已建立和執行的敏感資料探索工作的結果。此外，分數和標籤都不會暗示或以其他方式表示值區或值區的物件對您的組織可能具有的重要性或重要性。不過，您可以手動將最高分數 (100) 指派給值區，以覆寫值區的計算得分，同時也會將「敏感」標籤指派給值區。

主題

靈敏度評分尺寸和範圍

如果由 Amazon Macie 計算，S3 儲存貯體的靈敏度分數是兩個主要維度交集的量化度量：

- Macie 在值區中找到的敏感資料量。這主要衍生自 Macie 在值區中找到的敏感資料類型的性質和數量，以及每種類型的出現次數。
- Macie 在值區中分析的資料量。這主要衍生自 Macie 在值區中分析的唯一物件數量 (相對於值區中的唯一物件總數)。

S3 儲存貯體的靈敏度分數也會決定 Macie 指派給儲存貯體的敏感度標籤。敏感度標籤是評分的定性表示法，例如「敏感」或「不敏感」。在 Amazon Macie 主控台上，值區的敏感度分數也會決定 Macie 在資料視覺效果中用來表示值區的顏色，如下圖所示。

敏感度分數範圍介於 -1 到 100 之間，如下表所述。若要評估 S3 儲存貯體分數的輸入，您可以參考敏感資料探索統計資料以及 Macie 提供有關儲存貯體的其他詳細資料。

靈敏度分數	敏感性標籤	其他資訊
-1	分類錯誤	由於物件層級分類錯誤（物件層級權限設定、物件內容或配額有問題），Macie 尚未成功分析值區的任何物件。

靈敏度分數	敏感性標籤	其他資訊
		當 Macie 嘗試分析值區中的一或多個物件時，發生錯誤。例如，物件是格式錯誤的檔案，或是物件使用 Macie 無法存取或不允許使用的金鑰加密。值區的涵蓋範圍資料可協助您調查和修正錯誤。如需詳細資訊，請參閱 評估自動化敏感資料探索範圍。 Macie 將繼續嘗試分析存儲桶中的對象。如果 Macie 成功分析物件，Macie 會更新值區的敏感度分數和標籤，以反映分析結果。
1-49	不敏感	在此範圍內，較高的分數（例如 49）表示 Macie 分析了值區中相對較少的物件。較低的分數 (例如 1) 表示 Macie 分析了值區中的許多物件 (相對於值區中的物件總數)，並偵測到這些物件中敏感資料的類型和出現次數相對較少。 分數為 1 也可以表示值區未儲存任何物件，或儲存貯體中的所有物件都包含零 (0) 個位元組的資料。值區詳細資料中的物件統計資料可協助您判斷是否發生這種情況。如需詳細資訊，請參閱 檢閱 S3 儲存貯體詳情。

靈敏度分數	敏感性標籤	其他資訊
50	尚未分析	Macie 尚未嘗試分析或分析值區的任何物件。 當初始啟用自動探索或將值區新增至帳戶的儲存貯體詳細目錄時，Macie 會自動指派此分數。在組織中，如果從未針對擁有值區的帳戶啟用自動探索功能，值區也可以具有此分數。 50 分也表示值區的權限設定會阻止 Macie 存取值區或值區的物件。這通常是因為值區政策有限制。值區的詳細資料可協助您判斷是否發生這種情況，因為 Macie 只能提供值區相關資訊的子集。如需如何解決此問題的詳細資訊，請參閱允許 Macie 存取 S3 儲存貯體和物件。
51-99	敏感	在此範圍內，較高的分數 (例如 99) 表示 Macie 已經分析了值區中的許多物件 (相對於值區中的物件總數)，並偵測到這些物件中多種類型和機密資料的出現次數。較低的分數 (例如 51) 表示 Macie 已經分析了值區中的中等數目物件 (相對於值區中的物件總數)，並偵測到這些物件中至少一些類型和出現的機密資料。

靈敏度分數	敏感性標籤	其他資訊
100	敏感	分數已手動指派給值區，並覆寫計算得分。Macie 不會將此分數指派給值區。

監控敏感度分數

一開始為帳戶啟用自動敏感資料探索時，Amazon Macie 會自動為帳戶擁有的每個 S3 儲存貯體指派 50 的敏感度分數。當值區新增至帳戶的值區庫存時，Macie 也會將此分數指派給值區。根據該分數，尚未分析每個值區的敏感度標籤。例外情況是一個空值區，它是一個不存儲任何對象的存儲桶，或者存儲桶中的所有對象包含零（0）個字節的數據。如果值區是這種情況，Macie 會將分數指派給值區 1，且值區的靈敏度標籤不敏感。

隨著自動化敏感資料探索每天進行，Macie 會更新 S3 儲存貯體的敏感度分數和標籤，以反映其分析結果。例如：

- 如果 Macie 在物件中找不到敏感資料，Macie 會降低值區的敏感度分數，並視需要更新值區的敏感度標籤。
- 如果 Macie 在物件中找到敏感資料，Macie 會增加值區的敏感度分數，並視需要更新值區的敏感度標籤。
- 如果 Macie 在隨後變更的物件中找到敏感資料，Macie 會從值區的敏感度評分中移除物件的敏感性資料偵測，並視需要更新值區的敏感性標籤。
- 如果 Macie 在隨後刪除的物件中找到敏感資料，Macie 會從值區的敏感度分數中移除物件的敏感性資料偵測，並視需要更新值區的敏感性標籤。
- 如果將物件新增至先前為空的值區，而 Macie 在物件中找到敏感資料，Macie 會增加值區的敏感度分數，並視需要更新值區的敏感度標籤。
- 如果值區的權限設定讓 Macie 無法擷取或存取值區或值區物件的相關資訊，Macie 會將值區的敏感度分數變更為 50，並將值區的敏感度標籤變更為「尚未分析」。

分析結果可在啟用帳戶的自動敏感資料探索後 48 小時內開始顯示。

如果您是組織的 Macie 管理員，或者您擁有獨立的 Macie 帳戶，則可以調整組織或帳戶的敏感度評分設定：

- 若要調整後續分析所有 S3 儲存貯體的設定，請變更帳戶的自動化敏感資料探索設定。您可以開始包含或排除特定受管資料識別碼、自訂資料識別碼或允許清單。您也可以排除特定值區。如需詳細資訊，請參閱 設定自動化探索。
- 若要調整個別 S3 儲存貯體的設定，請變更每個儲存貯體的自動化敏感資料探索設定。您可以在值區的分數中包含或排除特定類型的敏感資料。您也可以指定是否要將自動計算的分數指派給值區。如需詳細資訊，請參閱 管理個別 S3 儲存貯體的自動化探索。

如果停用自動化敏感資料探索，對現有敏感度評分和標籤的影響會有所不同。如果您為組織中的成員帳戶停用此功能，則該帳戶擁有的 S3 儲存貯體會持續存在現有的分數和標籤。如果您針對整個組織或獨立的 Macie 帳戶停用此功能，則現有評分和標籤只會保留 30 天。在 30 天後，Macie 會重設組織或帳戶擁有之所有時段的評分與標籤。如果值區儲存物件，Macie 會將分數變更為 50，並將尚未分析的標籤指派給值區。如果值區為空，Macie 會將分數變更為 1，並將「不敏感」標籤指派給值區。此重設之後，Macie 會停止更新值區的敏感度分數和標籤，除非您再次為組織或帳戶啟用自動化敏感資料探索功能。

自動化敏感資料探索的預設設定

如果啟用了自動化敏感資料探索，Amazon Macie 會自動從所有 Amazon 簡單儲存服務 (Amazon S3) 一般用途儲存貯體中選取並分析樣本物件，以監控和分析您的帳戶。如果您是組織的 Macie 管理員，預設情況下會包含您的成員帳戶所擁有的 S3 儲存貯體。

若要精簡分析範圍，您可以從自動化敏感資料探索中排除特定 S3 儲存貯體。您可以透過兩種方式執行此操作：變更帳戶的設定，以及變更個別值區的設定。如果您是 Macie 管理員，您也可以啟用或停用組織中個別帳戶的自動敏感資料探索功能。如需詳細資訊，請參閱 設定自動化敏感資料探索。

根據預設，Macie 僅使用我們建議用於自動化敏感資料探索的一組受管資料識別碼來分析 S3 物件。Macie 不會使用任何自訂資料識別碼或允許您定義的清單。若要自訂分析，您可以設定 Macie 使用特定的受管理資料識別碼、自訂資料識別碼和允許清單。您可以透過變更帳戶的設定來執行此操作。如需詳細資訊，請參閱 設定自動化敏感資料探索。

主題

- 自動化敏感資料探索的預設受管資料識別碼
- 自動化敏感資料探索的預設設定更新

自動化敏感資料探索的預設受管資料識別碼

根據預設，Amazon Macie 僅使用我們建議用於自動化敏感資料探索的一組受管資料識別碼來分析 S3 物件。這組預設的受管理資料識別碼是設計來偵測敏感資料的常見類別和類型。根據我們的研究，它可以檢測敏感數據的一般類別和類型，同時通過降低噪音優化您的自動化發現結果。

預設設定為動態設定。隨著我們發佈新的受管資料識別碼，如果這些識別碼可能會進一步最佳化您的自動化敏感資料探索結果，我們會將它們新增至預設集。隨著時間的推移，我們也可能會在集合中新增或移除現有的受管理資料識別碼。移除受管資料識別碼不會影響 S3 儲存貯體的現有敏感資料探索統計資料和詳細資料。例如，如果我們移除 Macie 先前在值區中偵測到的敏感資料類型的受管理資料識別碼，Macie 會繼續回報值區的這些偵測。如果我們在預設集合中新增或移除受管理資料識別碼，我們會更新此頁面以指出變更的性質和時間。如需有關這些變更的自動警示，您可以訂閱 Macie 文件歷史記錄頁面上的 RSS 摘要。

下列主題列出目前位於預設集合中的受管理資料識別碼，依機密資料類別和類型進行組織。它們會為集合中的每個受管理資料識別碼指定唯一識別碼 (ID)。此 ID 描述受管資料識別碼用來偵測的敏感資料類型，例如：針`PGP_PRIVATE_KEY`對 PGP 私密金鑰和`USA_PASSPORT_NUMBER`美國護照號碼。如果您變更帳戶的自動化敏感資料探索設定，您可以使用此 ID 明確排除受管理資料識別碼，不再進行後續分析。

主題

- 登入資料
- 財務資訊
- 個人身分識別資訊 (PII)

如需有關特定受管理資料識別碼的詳細資訊，或 Macie 目前提供之所有受管理資料識別碼的完整清單，請參閱使用受管資料識別符。

登入資料

為了偵測 S3 物件中登入資料資料的發生次數，Macie 預設會使用下列受管資料識別碼。

敏感資料類型	受管資料識別符 ID
AWS 秘密訪問密鑰	`AWS_CREDENTIALS`
HTTP 基本授權標頭	`HTTP_BASIC_AUTH_HEADER`

敏感資料類型	受管資料識別符 ID
OpenSSH 私密金鑰	OPENSSH_PRIVATE_KEY
PGP 私密金鑰	PGP_PRIVATE_KEY
公開金鑰加密標準 (PKCS) 私密金鑰	PKCS
PuTTY 私密金鑰	PUTTY_PRIVATE_KEY

財務資訊

為了偵測 S3 物件中財務資訊的發生次數，Macie 預設會使用下列受管資料識別碼。

敏感資料類型	受管資料識別符 ID
信用卡磁條數據	CREDIT_CARD_MAGNETIC_STRIPE
信用卡號碼	CREDIT_CARD_NUMBER (適用於鄰近關鍵字的信用卡號碼)

個人身分識別資訊 (PII)

為了偵測 S3 物件中個人識別資訊 (PII) 的發生次數，Macie 預設會使用下列受管資料識別碼。

敏感資料類型	受管資料識別符 ID
駕照識別號碼	CANADA_DRIVERS_LICENSE, DRIVERS_LICENSE (適用於美國), UK_DRIVERS_LICENSE
選民名冊號碼	UK_ELECTORAL_ROLL_NUMBER
國家身分證號碼	FRANCE_NATIONAL_IDENTIFICATION_NUMBER, GERMANY_NATIONAL_IDENTIFICATION_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_DNI_NUMBER

敏感資料類型	受管資料識別符 ID
國民保險號碼 (NINO)	UK_NATIONAL_INSURANCE_NUMBER
護照號碼	CANADA_PASSPORT_NUMBER, FRANCE_PASSPORT_NUMBER, GERMANY_PASSPORT_NUMBER, ITALY_PASSPORT_NUMBER, SPAIN_PASSPORT_NUMBER, UK_PASSPORT_NUMBER, USA_PASSPORT_NUMBER
社會保險號碼 (SIN)	CANADA_SOCIAL_INSURANCE_NUMBER
社會安全號碼 (SSN)	SPAIN_SOCIAL_SECURITY_NUMBER, USA_SOCIAL_SECURITY_NUMBER
納稅識別號碼或參考號碼	AUSTRALIA_TAX_FILE_NUMBER, BRAZIL_CPF_NUMBER, FRANCE_TAX_IDENTIFICATION_NUMBER, GERMANY_TAX_IDENTIFICATION_NUMBER, SPAIN_NIE_NUMBER, SPAIN_NIF_NUMBER, SPAIN_TAX_IDENTIFICATION_NUMBER, USA_INDIVIDUAL_TAX_IDENTIFICATION_NUMBER

自動化敏感資料探索的預設設定更新

下表說明 Amazon Macie 預設用於自動化敏感資料探索的設定變更。如需有關這些變更的自動警示，請訂閱 Macie 文件歷史記錄頁面上的 RSS 摘要。

變更	描述	日期
實作一組新的動態預設受管資料識別碼	新的自動化敏感資料探索組態現在以動態預設的受管資料識別碼集為基礎。如果您在此日期或之後首次啟用自動化敏感	2023 年 8 月 2 日

變更	描述	日期
	資料探索，則您的組態會以動態集為基礎。 如果您在此日期之前第一次啟用自動化敏感資料探索，則您的組態會根據一組不同的受管理資料識別碼。如需詳細資訊，請參閱此表格後面的附註。	
一般可用性	初始發行自動化敏感資料探索。	2022 年 11 月 28 日

如果您最初在 2023 年 8 月 2 日之前啟用了自動化敏感資料探索，則您的組態不是以動態預設受管資料識別碼集合為基礎。而是以我們為初始發行自動化敏感資料探索所定義的一組靜態受管理資料識別碼為基礎，如下表所列。

若要判斷最初啟用自動敏感資料探索的時間，請在 Amazon Macie 主控台的導覽窗格中選擇「自動化敏感資料探索」，然後參閱「狀態」區段中的啟用日期。若要以程式設計方式執行此GetAutomatedDiscoveryConfiguration作業，請使用 Amazon Macie API 的作業，並參考`firstEnabledAt`欄位的值。如果日期早於 2023 年 8 月 2 日，且您想要開始使用動態的預設受管理資料識別碼集，請聯絡以 AWS Support 尋求協助。

下表列出靜態集合中的所有受管理資料識別碼。資料表會先依機密資料類別排序，然後依機密資料類型排序。如需特定受管資料識別碼的詳細資訊，請參閱使用受管資料識別符。

敏感資料類別	敏感資料類型	受管資料識別符 ID
登入資料	AWS 秘密訪問密鑰	`AWS_CREDENTIALS`
登入資料	HTTP 基本授權標頭	`HTTP_BASIC_AUTH_HEADER`
登入資料	OpenSSH 私密金鑰	`OPENSSH_PRIVATE_KEY`
登入資料	PGP 私密金鑰	`PGP_PRIVATE_KEY`

敏感資料類別	敏感資料類型	受管資料識別符 ID
登入資料	公開金鑰加密標準 (PKCS) 私密金鑰	PKCS
登入資料	PuTTY 私密金鑰	PUTTY_PRIVATE_KEY
財務資訊	銀行帳戶號碼	BANK_ACCOUNT_NUMBER (適用於加拿大及美國的銀行帳戶號碼)、FRANCE_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, ITALY_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER
財務資訊	信用卡到期日	CREDIT_CARD_EXPIRATION
財務資訊	信用卡磁條數據	CREDIT_CARD_MAGNETIC_STRIPE
財務資訊	信用卡號碼	CREDIT_CARD_NUMBER (適用於鄰近關鍵字的信用卡號碼)
財務資訊	信用卡驗證碼	CREDIT_CARD_SECURITY_CODE
個人信息：個人健康信息（PHI）	緝毒署 (DEA) 註冊號碼	US_DRUG_ENFORCEMENT_AGENCY_NUMBER
個人資料：PHI	健康保險索償編碼 (HICN)	USA_HEALTH_INSURANCE_CLAIM_NUMBER

敏感資料類別	敏感資料類型	受管資料識別符 ID
個人資料：PHI	健康保險或醫療識別號碼	CANADA_HEALTH_NUMBER, EUROPEAN_HEALTH_INSURANCE_CARD_NUMBER, FINLAND_EUROPEAN_HEALTH_INSURANCE_NUMBER, FRANCE_HEALTH_INSURANCE_NUMBER, UK_NHS_NUMBER, USA_MEDICARE_BENEFICIARY_IDENTIFIER
個人資料：PHI	醫療保健通用程序編碼系統 (HCPCS) 代碼	USA_HEALTHCARE_PROCEDURE_CODE
個人資料：PHI	國家藥物法規 (NDC)	USA_NATIONAL_DRUG_CODE
個人資料：PHI	國家提供者識別符 (NPI)	USA_NATIONAL_PROVIDER_IDENTIFIER
個人資料：PHI	唯一裝置識別碼 (UDI)	MEDICAL_DEVICE_UDI
個人資訊：個人識別資訊 (PII)	出生日期	DATE_OF_BIRTH

敏感資料類別	敏感資料類型	受管資料識別符 ID
個人資料：個人資料	駕照識別號碼	AUSTRALIA_DRIVERS_LICENSE, AUSTRIA_DRIVERS_LICENSE, BELGIUM_DRIVERS_LICENSE, BULGARIA_DRIVERS_LICENSE, CANADA_DRIVERS_LICENSE, CROATIA_DRIVERS_LICENSE, CYPRUS_DRIVERS_LICENSE, CZECHIA_DRIVERS_LICENSE, DENMARK_DRIVERS_LICENSE, DRIVERS_LICENSE (適用於美國), ESTONIA_DRIVERS_LICENSE, FINLAND_DRIVERS_LICENSE, FRANCE_DRIVERS_LICENSE, GERMANY_DRIVERS_LICENSE, GREECE_DRIVERS_LICENSE, HUNGARY_DRIVERS_LICENSE, IRELAND_DRIVERS_LICENSE, ITALY_DRIVERS_LICENSE, LATVIA_DRIVERS_LICENSE, LITHUANIA_DRIVERS_LICENSE, LUXEMBOURG_DRIVERS_LICENSE, MALTA_DRIVERS_LICENSE, NETHERLANDS_DRIVER

敏感資料類別	敏感資料類型	受管資料識別符 ID
		S_LICENSE, POLAND_DRIVERS_LICENSE, PORTUGAL_DRIVERS_LICENSE, ROMANIA_DRIVERS_LICENSE, SLOVAKIA_DRIVERS_LICENSE, SLOVENIA_DRIVERS_LICENSE, SPAIN_DRIVERS_LICENSE, SWEDEN_DRIVERS_LICENSE, UK_DRIVERS_LICENSE
個人資料：個人資料	選民名冊號碼	UK_ELECTORAL_ROLL_NUMBER
個人資料：個人資料	全名	NAME
個人資料：個人資料	全球定位系統 (GPS) 座標	LATITUDE_LONGITUDE
個人資料：個人資料	郵寄地址	ADDRESS, BRAZIL_CEP_CODE
個人資料：個人資料	國家身分證號碼	BRAZIL_RG_NUMBER, FRANCE_NATIONAL_IDENTIFICATION_NUMBER, GERMANY_NATIONAL_IDENTIFICATION_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_DNI_NUMBER
個人資料：個人資料	國民保險號碼 (NINO)	UK_NATIONAL_INSURANCE_NUMBER

敏感資料類別	敏感資料類型	受管資料識別符 ID
個人資料：個人資料	護照號碼	CANADA_PASSPORT_NUMBER, FRANCE_PASSPORT_NUMBER, GERMANY_PASSPORT_NUMBER, ITALY_PASSPORT_NUMBER, SPAIN_PASSPORT_NUMBER, UK_PASSPORT_NUMBER, USA_PASSPORT_NUMBER
個人資料：個人資料	永久居留號碼	CANADA_NATIONAL_IDENTIFICATION_NUMBER
個人資料：個人資料	電話號碼	BRAZIL_PHONE_NUMBER, FRANCE_PHONE_NUMBER, GERMANY_PHONE_NUMBER, ITALY_PHONE_NUMBER, PHONE_NUMBER （適用於加拿大和美國）, SPAIN_PHONE_NUMBER, UK_PHONE_NUMBER
個人資料：個人資料	社會保險號碼 (SIN)	CANADA_SOCIAL_INSURANCE_NUMBER
個人資料：個人資料	社會安全號碼 (SSN)	SPAIN_SOCIAL_SECURITY_NUMBER, USA_SOCIAL_SECURITY_NUMBER

敏感資料類別	敏感資料類型	受管資料識別符 ID
個人資料：個人資料	納稅識別號碼或參考號碼	AUSTRALIA_TAX_FILE_NUMBER, BRAZIL_CNPJ_NUMBER, BRAZIL_CPF_NUMBER, FRANCE_TAX_IDENTIFICATION_NUMBER, GERMANY_TAX_IDENTIFICATION_NUMBER, SPAIN_NIE_NUMBER, SPAIN_NIF_NUMBER, SPAIN_TAX_IDENTIFICATION_NUMBER, UK_TAX_IDENTIFICATION_NUMBER, USA_INDIVIDUAL_TAX_IDENTIFICATION_NUMBER
個人資料：個人資料	車輛識別碼 (VIN)	VEHICLE_IDENTIFICATION_NUMBER

在 Amazon Macie 中執行敏感性資料探索任務

使用 Amazon Macie，您可以建立和執行敏感資料探索任務，在 Amazon Simple Storage Service (Amazon S3) 一般用途儲存貯體中自動探索、記錄和報告敏感資料。敏感資料探索任務是 Macie 執行的一系列自動化處理和分析任務，以偵測和報告 Amazon S3 物件中的敏感資料。每項工作都會提供 Macie 找到的敏感資料以及 Macie 執行的分析的詳細報告。透過建立和執行任務，您可以建立和維護組織存放在 Amazon S3 中的資料以及該資料的任何安全或合規風險的全面檢視。

為了協助您符合資料安全性和隱私權要求，Macie 提供了數個選項來排程和定義工作範圍。您可以將工作設定為僅執行一次隨選分析和評估，或定期分析、評估和監視定期執行一次。您也可以定義任務分析的廣度和深度，也就是您選取的特定 S3 儲存貯體或符合特定條件的儲存貯體。您可以選擇性地選擇性地細化該分析的範圍。這些選項包括從 S3 物件屬性衍生的自訂包含和排除條件，例如標籤、首碼，以及上次修改物件的時間。

對於每項工作，您也可以指定要 Macie 偵測和報告的敏感資料類型。您可以將工作設定為使用 Macie 提供的受管理資料識別碼、您定義的自訂資料識別碼，或兩者的組合。透過為工作選取特定的受管理和自訂資料識別碼，您可以自訂分析以專注於特定類型的敏感資料。若要微調分析，您也可以將工作設定為使用您定義的允許清單。允許清單指定您希望 Macie 忽略的文字和文字模式，通常是組織特定案例或環境的敏感資料例外狀況。

每項工作都會產生 Macie 找到的敏感資料以及 Macie 執行的分析記錄 — 敏感資料發現和敏感資料探索結果。敏感資料發現是 Macie 在 S3 物件中找到的敏感資料的詳細報告。敏感資料探索結果是記錄 S3 物件分析詳細資料的記錄。Macie 會為您設定要分析的工作的每個物件建立敏感資料探索結果。這包括 Macie 無法在其中找到敏感資料，因此不會產生敏感資料發現項目的物件，以及 Macie 因錯誤或問題而無法分析的物件。每種類型的記錄都遵循標準化的結構描述，可協助您查詢、監視和處理記錄，以符合您的安全性和合規性需求。

主題

敏感資料探索工作的範圍選項

使用敏感資料探索任務時，您可以定義 Amazon Macie 分析的 Amazon 簡單儲存服務 (Amazon S3) 資料範圍，以偵測和報告敏感資料。為了協助您執行此操作，Macie 提供了數個工作特定選項，您可以在建立和設定工作時選擇這些選項。

範圍選項

- S3 儲存貯體
- 初始執行：現有 S3 物件
- 採樣深度
- S3 物件條件

S3 儲存貯體

建立敏感資料探索任務時，您可以指定哪些 S3 儲存貯體存放您希望 Macie 在任務執行時分析的物件。您可以透過兩種方式執行此操作：從儲存貯體庫存中選取特定的 S3 儲存貯體，或指定從 S3 儲存貯體屬性衍生的自訂條件。

選取特定 S3 儲存貯體

使用此選項，您可以明確選取要分析的每個 S3 儲存貯體。然後，當工作執行時，它只會分析您選取的值區中的物件。如果您將工作設定為每天、每週或每月定期執行，則工作會在每次執行時分析相同值區中的物件。

對於您想要對特定資料集執行目標分析的情況，此組態非常有用。它可讓您精確且可預測的控制工作分析的值區。

指定 S3 儲存貯體條件

使用此選項，您可以定義執行階段準則，以決定要分析哪些 S3 儲存貯體。此條件包含一或多個衍生自值區屬性的條件，例如公用存取設定和標籤。工作執行時，會識別符合您準則的值區，然後分析這些值區中的物件。如果您將工作設定為定期執行，則每次執行工作時都會執行此作業。因此，工作可能會在每次執行時分析不同值區中的物件，具體取決於值區詳細目錄的變更以及您定義的條件。

對於您希望分析範圍動態適應值區庫存變更的情況，此組態非常有用。如果您將工作設定為使用值區條件並定期執行，工作會自動識別符合條件的新值區，並檢查這些值區中是否有機密資料。

本節中的主題提供有關每個選項的其他詳細資訊。

主題

選取特定 S3 儲存貯體

如果您選擇明確選取要分析任務的每個 S3 儲存貯體，Macie 會為您提供目前 AWS 區域一般用途儲存貯體的完整清查。然後，您可以複查庫存並選取所需的時段。若要瞭解 Macie 如何為您產生和維護此庫存，請參閱Macie 如何監控 Amazon S3 數據安全。

如果您是組織的 Macie 管理員，則資產管理員會包含組織中成員帳戶所擁有的值區。您可以選取多達 1,000 個這些值區，跨越多達 1,000 個帳戶。

為了協助您選擇值區，詳細目錄會提供每個值區的詳細資料和統計資料。這包括任務可以在每個儲存貯體中分析的資料量 — 可分類的物件是使用支援的 Amazon S3 儲存類別的物件，且具有支援檔案或儲存格式的副檔名。詳細目錄也會指出是否已將任何現有工作設定為分析值區中的物件。這些詳細資料可協助您估計工作的廣度，並精簡值區選擇。

在庫存表格中：

- 敏感度 — 如果啟用了自動化敏感資料探索，則指出值區目前的敏感度分數。
- 可分類的物件 — 指出工作可在值區中分析的物件總數。
- 可分類大小 — 指出工作可在值區中分析之所有物件的儲存大小總計。

  如果值區儲存壓縮物件，這個值並不會反映這些物件解壓縮後的實際大小。如果儲存貯體已啟用版本控制，則此值會根據值區中每個物件最新版本的儲存大小而定。
- 依工作監視 — 指出是否已將任何現有工作設定為每日、每週或每月定期分析值區中的物件。

  如果此欄位的值為「是」，則時段會明確納入週期性工單中，或符合過去 24 小時內週期性工單條件的時段。此外，其中至少有一個工作的狀態為「未取消」。Macie 每天更新此數據。
- 最新工作執行 — 如果將現有的週期性或一次性工作配置為分析值區中的物件，則此欄位會指出其中一個工作開始執行的最近日期與時間。否則，此欄位中會出現一個破折號 (—)。

如果資訊圖示
(ⓘ)
出現在表格中的任何儲存貯體名稱旁，建議您從 Amazon S3 擷取最新的儲存貯體中繼資料。若要這麼做，請選擇表格上方的重新整理
(↻)。
資訊圖示表示儲存貯體是在過去 24 小時內建立的，可能是在 Macie 上次從 Amazon S3 擷取儲存貯體和物件中繼資料作為每日重新整理週期的一部分之後建立。如需詳細資訊，請參閱 數據刷新。

如果表格中值區名稱旁邊出現警告圖示
(⚠)，
表示不允許 Macie 存取值區或值區的物件。這表示工作將無法分析值區中的物件。若要調查問題，請檢閱 Amazon S3 中儲存貯體的政策和許可設定。例如，值區可能具有限制性的值區政策。如需詳細資訊，請參閱 允許 Macie 存取 S3 儲存貯體和物件。

若要自訂您的庫存檢視並更輕鬆地尋找特定值區，您可以在篩選方塊中輸入篩選條件來篩選表格。下表提供一些範例。

若要顯示所有值區...	套用此篩選器...
由特定帳戶擁有	帳戶 ID = 帳戶*# 12 #####*
可公開存取	有效許可 = 公開
不包括在任何定期工作中	主動監控工作 = 假
不包含在任何定期或一次性工作中	在工作中定義 = 假
擁有特定的標籤金鑰 *	標籤鍵 = *###*
具有特定的標籤值 *	標籤值 = *###*
儲存未加密的物件 (或使用用戶端加密的物件)	加密的物件計數為「無加密」，「從」= 1

* 標籤鍵和值區分大小寫。此外，您必須在篩選器中為這些欄位指定完整、有效的值。您不能指定部分值或使用萬用字元。

若要顯示值區的詳細資訊，請選擇值區的名稱並參閱詳細資料面板。從那裡，您還可以：

- 透過選擇欄位的放大鏡，對某些欄位進行樞紐分析和深入研究。選擇 顯示具有相同值的值區，或選擇 顯示具有其他值的值區。
- 擷取值區中物件的最新中繼資料。如果您最近建立了值區，或在過去 24 小時內對值區的物件進行了重大變更，這會很有幫助。若要擷取資料，請在面板的「物件統計資料」區段中選擇 refresh ()。此選項適用於儲存 30,000 個或更少物件的值區。

指定 S3 儲存貯體條件

如果您選擇指定工作的儲存貯體條件，Macie 會提供用於定義和測試條件的選項。這些是決定要分析哪些 S3 儲存貯體存放物件的執行階段準則。每次工作執行時，都會識別符合您準則的一般用途值區，然後分析適當值區中的物件。如果您是組織的 Macie 管理員，這包括組織中成員帳戶所擁有的值區。

定義時段條件

儲存貯體條件包含從 S3 儲存貯體屬性衍生的一或多個條件。每個條件 (也稱為準則) 由下列部分組成：

- 以屬性為基礎的欄位，例如「帳戶 ID」或「有效」權限。
- 一個運算符，無論是等於（eq）或不等於（neq）。
- 一或多個值。
- 包含或排除陳述式，指出要分析 (包含) 或略過 (排除) 符合條件的值區。

如果您為欄位指定多個值，Macie 會使用 OR 邏輯來聯結這些值。如果您為準則指定多個條件，Macie 會使用 AND 邏輯來連接這些條件。此外，排除條件的優先順序高於包含條件。例如，如果您包含可公開存取的值區，並排除具有特定標籤的值區，則工作會分析任何可公開存取的值區中的物件，除非值區具有其中一個指定的標記。

您可以為 S3 儲存貯體定義從下列任何屬性欄位衍生的條件。

帳戶 ID

擁有值區的 AWS 帳戶 唯一識別碼 (ID)。若要為此欄位指定多個值，請輸入每個帳戶的 ID，並以逗號分隔每個項目。

請注意，Macie 不支援此欄位使用萬用字元或部分值。

儲存貯體名稱

值區的名稱。此欄位與 Amazon Amazon S3 中的「名稱」欄位相關，而不是 Amazon 資源名稱 (ARN) 欄位。若要為此欄位指定多個值，請輸入每個值區的名稱，並以逗號分隔每個項目。

請注意，值區分大小寫。此外，Macie 不支援此欄位使用萬用字元或部分值。

有效許可

指定值區是否可公開存取。您可以為此欄位選擇下列一或多個值：

- 不公開 — 一般大眾沒有值區的讀取或寫入權限。
- 公用 — 一般大眾擁有值區的讀取或寫入存取權。
- 未知 — Macie 無法評估值區的公開存取設定。

為了決定值區的此值，Macie 會分析值區的帳戶層次與時段層次設定組合：帳戶的區塊公用存取設定、值區的區塊公用存取設定、值區的值區塊公開存取設定、值區的值區政策，以及值區的存取控制清單 (ACL)。

共用存取

指定儲存貯體是與另一個儲存貯體共用 AWS 帳戶、Amazon CloudFront 原始存取身分 (OAI) 還是 CloudFront 來源存取控制 (OAC)。您可以為此欄位選擇下列一或多個值：

- 外部 — 值區會與下列一或多項或下列任何組合共用： CloudFront OAI、CloudFront OAC 或組織外部 (不屬於) 組織的帳戶。
- 內部 — 值區會與一或多個屬於您組織內部 (部分) 的帳戶共用。它不會與 CloudFront OAI 或 OAC 共用。
- 未共用 — 值區不會與其他帳戶、 CloudFront OAI 或 CloudFront OAC 共用。
- 未知 — Macie 無法評估值區的共用存取設定。

為了判斷某個值區是否與另一個值區共用 AWS 帳戶，Macie 會分析值區政策和值區的 ACL。此外，組織被定義為一組 Macie 帳戶，透過 AWS Organizations 或透過 Macie 邀請集中管理為一組相關帳戶。如需 Amazon S3 共用儲存貯體選項的相關資訊，請參閱 Amazon 簡單儲存服務使用者指南中的 Amazon S3 中的身分和存取管理。

若要判斷值區是否與 CloudFront OAI 或 OAC 共用，Macie 會分析值區的值區政策。 CloudFront OAI 或 OAC 可讓使用者透過一或多個指 CloudFront定的發行版存取值區的物件。如需 CloudFront OAI 和 OAC 的相關資訊，請參閱 Amazon 開發人員指南中的限制對 Amazon S3 來源的存取。 CloudFront

Tags (標籤)

與值區相關聯的標籤。標籤是您可以定義並指派給特定類型 AWS 資源 (包括 S3 儲存貯體) 的標籤。每個標籤都包含必要的標籤鍵和一個可選的標籤值。如需標記 S3 儲存貯體的相關資訊，請參閱 Amazon 簡單儲存服務使用者指南中的使用成本分配 S3 儲存貯體標籤。

對於敏感資料探索工作，您可以使用這種類型的條件來包含或排除具有特定標籤鍵、特定標籤值或特定標籤鍵和標籤值 (以配對形式) 的值區。例如：

- 如果您指定**`Project`**為標籤鍵，但未指定條件的任何標籤值，則任何具有 Project 標籤鍵的值區都會符合條件的準則，而不論與該標籤鍵相關聯的標籤值為何。
- 如果您將**`Development`**和指定**`Test`**為標籤值，但未為條件指定任何標籤鍵，則任何具有**`Development`**或**`Test`**標籤值的值區都會符合條件的準則，而不論與這些標籤值相關聯的標籤鍵為何。

若要在條件中指定多個標籤鍵，請在「金鑰」欄位中輸入每個標籤鍵，並以逗號分隔每個項目。若要在條件中指定多個標籤值，請在「值」欄位中輸入每個標籤值，並以逗號分隔每個項目。

請注意，標籤鍵和值是區分大小寫的。此外，Macie 不支援在標籤條件中使用萬用字元或部分值。

測試桶標準

定義值區條件時，您可以透過預覽結果來測試和細化條件。若要這麼做，請展開主控台上顯示在條件下方的 [預覽條件結果] 區段。本節顯示目前符合條件的 S3 一般用途儲存貯體的表格。

此表格也提供任務在每個儲存貯體中可分析的資料量深入分析 — 可分類的物件是使用受支援的 Amazon S3 儲存類別，且具有支援檔案或儲存格式副檔名的物件。此表格也會指出是否已將任何現有工作設定為定期分析值區中的物件。

在資料表中：

- 敏感度 — 如果啟用了自動化敏感資料探索，則指出值區目前的敏感度分數。
- 可分類的物件 — 指出工作可在值區中分析的物件總數。
- 可分類大小 — 指出工作可在值區中分析之所有物件的儲存大小總計。

  如果值區儲存壓縮物件，這個值並不會反映這些物件解壓縮後的實際大小。如果值區已啟用版本控制，則此值會根據值區中每個物件最新版本的儲存大小而定。
- 依工作監視 — 指出是否已將任何現有工作設定為每日、每週或每月定期分析值區中的物件。

  如果此欄位的值為「是」，則時段會明確納入週期性工單中，或符合過去 24 小時內週期性工單條件的時段。此外，其中至少有一個工作的狀態為「未取消」。Macie 每天更新此數據。

如果值區名稱旁邊出現警告圖示 (⚠)，表示不允許 Macie 存取值區或值區的物件。這表示工作將無法分析值區中的物件。若要調查問題，請檢閱 Amazon S3 中儲存貯體的政策和許可設定。例如，值區可能具有限制性的值區政策。如需詳細資訊，請參閱 允許 Macie 存取 S3 儲存貯體和物件。

若要精簡工作的值區條件，請使用篩選選項來新增、變更或移除條件中的條件。然後 Macie 會更新表格以反映您的變更。

初始執行：現有 S3 物件

您可以使用敏感資料探索任務，對 S3 儲存貯體中的物件執行持續的增量分析。如果您將工作設定為定期執行，Macie 會自動執行此動作 — 每次執行都只會分析在上次執行之後建立或變更的物件。使用「包括現有物件」選項，您可以選擇第一個增量的起點：

- 若要在完成建立工作後立即分析所有現有物件，請選取此選項的核取方塊。

- 若只要等待並分析建立工作之後以及第一次執行之前所建立或變更的物件，請清除此選項的核取方塊。

  清除此核取方塊對於您已經分析資料且想要定期繼續分析資料的情況很有幫助。例如，如果您之前使用其他服務或應用程式來分類資料，而您最近開始使用 Macie，您可以使用此選項來確保繼續探索和分類您的資料，而不會產生不必要的成本或複製分類資料。

每次後續執行週期性工作，都只會自動分析在前一次執行之後建立或變更的物件。

對於定期和一次性工作，您也可以將工作配置為僅分析那些在特定時間之前或之後或在特定時間範圍內建立或變更的物件。若要執行此操作，請新增使用物件上次修改日期的物件條件。

採樣深度

使用此選項，您可以指定要敏感資料探索任務分析的合格 S3 物件百分比。符合條件的物件是指以下物件：使用支援的 Amazon S3 儲存類別、支援的檔案或儲存格式具有副檔名，以及符合您為任務指定的其他準則。

如果此值小於 100%，Macie 會隨機選取合格的物件進行分析，最多可達指定的百分比，並分析這些物件中的所有資料。例如，如果您將工作設定為分析 10,000 個物件，並指定 20% 的取樣深度，Macie 會在工作執行時分析大約 2,000 個隨機選取的合格物件。

減少工作的取樣深度可以降低成本並減少工作的持續時間。對於物件中的資料高度一致，而您想要判斷 S3 儲存貯體 (而非每個物件) 是否存放敏感資料的情況，這很有幫助。

請注意，此選項會控制分析物件的百分比，而不是分析的位元組百分比。如果您輸入的取樣深度小於 100%，Macie 會分析每個選取物件中的所有資料，而非每個所選物件中資料的該百分比。

S3 物件條件

若要微調敏感資料探索任務的範圍，您也可以定義自訂條件，以決定 Macie 在任務分析中包含或排除哪些 S3 物件。這些準則包含從 S3 物件屬性衍生的一或多個條件。這些條件適用於您設定要分析任務的所有 S3 儲存貯體中的物件。如果值區儲存了物件的多個版本，則這些條件會套用至物件的最新版本。

如果您將多個條件定義為物件準則，Macie 會使用 AND 邏輯來連接條件。此外，排除條件的優先順序高於包含條件。例如，如果您包括副檔名為 .pdf 的物件，並排除大於 5 MB 的物件，則工作會分析任何具有 .pdf 副檔名的物件，除非該物件大於 5 MB。

您可以定義從 S3 物件的下列任何屬性衍生出來的條件。

副檔名

這與 S3 物件的副檔名相關。您可以使用此類型的條件，根據檔案類型包括或排除物件。若要針對多種類型的檔案執行此動作，請輸入每個類型的副檔名，並以逗號分隔每個項目，例如：。**docx,pdf,xlsx**如果您輸入多個副檔名作為條件的值，Macie 會使用 OR 邏輯來結合這些值。

請注意，值區分大小寫。此外，Macie 不支援在此類型條件中使用部分值或萬用字元。

如需有關 Macie 可以分析的檔案類型的資訊，請參閱支援的檔案和儲存格式。

上次修改

這與 Amazon S3 中的「上次修改」欄位相關。在 Amazon S3 中，此欄位會儲存建立或上次變更 S3 物件的日期和時間，以最新的日期和時間為準。

對於敏感性資料探索工作，此條件可以是特定日期、特定日期和時間或獨佔時間範圍：

- 若要分析在特定日期或日期和時間之後上次修改的物件，請在「從」欄位中輸入值。
- 若要分析上次在特定日期或日期和時間之前修改的物件，請在「至」(To) 欄位中輸入值。
- 若要分析特定時間範圍內上次修改的物件，請使用「從」欄位輸入時間範圍內第一個日期或日期與時間的值。使用「至」欄位可輸入時間範圍內上次日期或日期與時間的值。
- 若要分析某一天內隨時修改的物件，請在「起始日期」欄位中輸入日期。在「終止日期」欄位中輸入下一天的日期。然後確認兩個時間欄位都是空白的。（Macie 將空白時間字段視為`00:00:00`。）例如，若要分析在 2023 年 8 月 9 日變更的物件，請**2023/08/09**在「起始日期」欄位**2023/08/10**中輸入「結束日期」欄位，並且不要在任一時間欄位中輸入值。

以國際標準時間 (UTC) 輸入任何時間值，並使用 24 小時標記法。

字首

這與 Amazon S3 中的關鍵字段相關。在 Amazon S3 中，此欄位存放 S3 物件的名稱，包括物件的前置詞。前綴類似於存儲桶中的目錄路徑。它可讓您將類似物件分組在值區中，就像您可能會將類似檔案一起儲存在檔案系統上的資料夾中。如需 Amazon S3 中物件前置詞和資料夾的相關資訊，請參閱 Amazon 簡單儲存服務使用者指南中的使用資料夾組織 Amazon S3 主控台中的物件。

您可以使用這種類型的條件來包含或排除其索引鍵 (名稱) 以特定值開頭的物件。例如，若要排除其索引鍵開頭**AWSLogs**為的所有物件 AWSLogs，請輸入「首碼」條件的值，然後選擇「排除」。

如果您輸入多個字首作為條件的值，Macie 會使用 OR 邏輯來結合這些值。例如，如果您輸入 **AWSLogs1** and **AWSLogs2** 做為條件的值，則索引鍵以 AWSLogs1 或 AWSLogs2 開頭的任何物件都會符合條件的準則。

當您輸入「首碼」條件的值時，請記住下列事項：

- 值是區分大小寫的。
- Macie 不支援在這些值中使用萬用字元。
- 在 Amazon S3 中，物件的金鑰不包含存放物件的儲存貯體名稱。因此，請勿在這些值中指定值區名稱。
- 如果字首包含分隔符號，請在值中包含分隔符號。例如，輸入**AWSLogs/eventlogs**以定義其索引鍵開頭為 AWSLogs/event logs 的所有物件的條件。Macie 支援預設的 Amazon S3 分隔符號，也就是斜線 (/) 和自訂分隔符號。

另請注意，只有當物件的索引鍵完全符合您輸入的值 (從物件索引鍵中的第一個字元開始) 時，物件才符合條件的準則。此外，Macie 會將條件套用至物件的完整 Key 值，包括物件的檔案名稱。

例如，如果物件的索引鍵是 AWSLogs/eventlogs/testlog.csv，而您針對條件輸入下列任一值，則該物件就會符合條件的準則：

- **AWSLogs**
- **AWSLogs/event**
- **AWSLogs/eventlogs/**
- **AWSLogs/eventlogs/testlog**
- **AWSLogs/eventlogs/testlog.csv**

但是，如果您輸入***eventlogs***，則該對象與條件不匹配-條件的值不包括鍵的第一部分/。AWSLogs同樣地，如果您輸入**awslogs**，則由於大小寫差異，物件與準則不符。

儲存體大小

這與 Amazon S3 中的大小字段相關。在 Amazon S3 中，此欄位會指出 S3 物件的總儲存大小。如果物件是壓縮檔案，這個值不會反映檔案解壓縮後的實際大小。

您可以使用此類型的條件來包括或排除小於特定大小、大於特定大小或落在特定大小範圍內的物件。Macie 會將這種類型的條件套用至所有類型的物件，包括壓縮檔案或封存檔案，以及它們所包含的檔案。如需每種支援格式之大小限制的相關資訊，請參閱。Amazon Macie 配額

Tags (標籤)

與 S3 物件相關聯的標籤。標籤是您可以定義並指派給特定類型 AWS 資源 (包括 S3 物件) 的標籤。每個標籤都包含必要的標籤鍵和一個可選的標籤值。如需標記 S3 物件的相關資訊，請參閱 Amazon 簡單儲存服務使用者指南中的使用標籤對儲存進行分類。

對於敏感性資料探索工作，您可以使用此類型的條件來包含或排除具有特定標籤的物件。這可以是特定的標籤鍵，也可以是特定的標籤鍵和標籤值 (作為一對)。如果您指定多個標籤作為條件的值，Macie 會使用 OR 邏輯來連接這些值。例如，如果您指定**Project1**和**Project2**做為條件的標籤關鍵字，則任何具有 Project1 或 Projec t2 標籤鍵的物件都會符合條件的準則。

請注意，標籤鍵和值是區分大小寫的。此外，Macie 不支援在此類型的條件中使用部分值或萬用字元。

建立敏感資料探索任務

使用 Amazon Macie，您可以建立和執行敏感資料探索任務，在 Amazon Simple Storage Service (Amazon S3) 一般用途儲存貯體中自動探索、記錄和報告敏感資料。敏感資料探索任務是 Macie 執行的一系列自動化處理和分析任務，以偵測和報告 Amazon S3 物件中的敏感資料。隨著分析的進行，Macie 會提供所找到之敏感資料及其執行分析的詳細報告：敏感資料發現項目、報告 Macie 在個別 S3 物件中找到的敏感資料，以及敏感資料探索結果，記錄有關個別 S3 物件分析的詳細資料。如需詳細資訊，請參閱 複查工作統計資料和結果。

建立任務時，首先要指定哪些 S3 儲存貯體存放物件，這些物件會在任務執行時進行分析，也就是您選取的特定儲存貯體或符合特定準則的值區。然後，您可以指定執行工作的頻率 — 一次，或定期每天、每週或每月執行一次。您也可以選擇選項來精簡工作的分析範圍。這些選項包括從 S3 物件屬性衍生而來的自訂準則，例如標籤、首碼，以及上次修改物件的時間。

定義工作的排程和範圍之後，您可以指定要使用的受管理資料識別碼和自訂資料識別碼：

- 受管資料識別碼是一組內建準則和技術，用來偵測特定類型的敏感資料，例如特定國家或地區的信用卡號碼、 AWS 秘密存取金鑰或護照號碼。這些識別碼可以偵測許多國家和地區不斷增加的敏感資料類型清單，包括多種類型的憑證資料、財務資訊和個人識別資訊 (PII)。如需詳細資訊，請參閱 使用受管資料識別符。
- 自訂資料識別碼是您定義用來偵測機密資料的一組準則。使用自訂資料識別碼，您可以偵測反映組織特定案例、智慧財產或專屬資料的敏感資料，例如員工 ID、客戶帳號或內部資料分類。您可以補充 Macie 提供的受管理資料識別碼。如需詳細資訊，請參閱 建置自訂資料識別符。

然後，您可以選擇性地選取允許使用清單。允許清單會指定您希望 Macie 忽略的文字或文字模式，通常是針對特定案例或環境的敏感資料例外狀況，例如組織的公用名稱或電話號碼，或組織用於測試的範例資料。如需詳細資訊，請參閱 使用允許清單定義敏感資料例外。

完成選擇這些選項後，您就可以輸入工作的一般設定，例如工作的名稱和描述。然後，您可以檢閱並儲存工作。

任務

開始之前

在建立工作之前，最好先採取下列步驟：

- 確認您已為敏感資料探索結果設定存放庫。若要這樣做，請在 Amazon Macie 主控台的導覽窗格中選擇「探索結果」。若要瞭解這些設定，請參閱儲存及保留敏感資料探索結果。
- 建立您要工作使用的任何自訂資料識別碼。如要瞭解如何作業，請參閱建置自訂資料識別符。
- 建立您希望工作使用的任何允許清單。如要瞭解如何作業，請參閱建立和管理允許清單。
- 如果您要分析已加密的 S3 物件，請確定 Macie 可以存取和使用適當的加密金鑰。如需詳細資訊，請參閱 分析加密的 S3 物件。
- 如果您想要分析具有限制性儲存貯體政策的 S3 儲存貯體中的物件，請確定允許 Macie 存取這些物件。如需詳細資訊，請參閱 允許 Macie 存取 S3 儲存貯體和物件。

如果您在建立工作之前執行這些操作，您可以簡化工作的建立，並協助確保工作能夠分析您想要的資料。

步驟 1：選擇 S3 儲存貯體

建立任務時，第一個步驟是指定哪些 S3 儲存貯體存放您希望 Macie 在任務執行時分析的物件。對於此步驟，您有兩個選擇：

- 選取特定儲存貯體 — 使用此選項，您可以明確選取要分析的每個 S3 儲存貯體。然後，當工作執行時，它只會分析您選取的值區中的物件。

- 指定儲存貯體準則 — 使用此選項，您可以定義執行時期準則，以決定要分析哪些 S3 儲存貯體。條件包含從值區屬性衍生的一或多個條件。然後，當工作執行時，它會識別符合您準則的值區，並分析這些值區中的物件。

如需這些選項的詳細資訊，請參閱 任務的範圍選項。

以下各節提供選擇和配置每個選項的指示。選擇所需選項的區段。

選取特定時段

如果您選擇明確選取要分析的每個 S3 儲存貯體，Macie 會提供您目前 AWS 區域一般用途儲存貯體的完整清查。然後，您可以使用此庫存來選取工單的一或多個時段。若要瞭解此清單，請參閱選取特定 S3 儲存貯體。

如果您是組織的 Macie 管理員，則資產管理員會包含組織中成員帳戶所擁有的值區。您可以選取多達 1,000 個這些值區，跨越多達 1,000 個帳戶。

若要為任務選取特定的 S3 儲存貯體

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 在導覽窗格中，選擇 Jobs (任務)。
3. 選擇建立作業。
4. 在 [選擇 S3 儲存貯體] 頁面上，選擇選取特定儲存貯體。Macie 會顯示目前區域中您帳戶的所有一般用途值區的表格。
5. 在「選取 S3 儲存貯體」 區段中，選擇性地選擇重新整理
   ()
   以從 Amazon S3 擷取最新的儲存貯體中繼資料。

   如果資訊圖示
   ()
   出現在任何值區名稱旁，我們建議您這麼做。此圖示表示儲存貯體是在過去 24 小時內建立的，可能是在 Macie 上次從 Amazon S3 擷取儲存貯體和物件中繼資料作為每日重新整理週期的一部分之後。
6. 在表格中，選取您要分析工作的每個值區的核取方塊。

> **Tip**
>
> - 若要更輕鬆地尋找特定值區，請在表格上方的篩選方塊中輸入篩選條件。您也可以選擇欄標題來排序表格。
> - 若要判斷您是否已將工作設定為定期分析值區中的物件，請參閱按工作監視欄位。如果欄位中出現「是」，則該時段會明確納入週期性工單中，或符合過去 24 小時內週期性工單條件的時段。此外，其中至少有一個工作的狀態為「未取消」。Macie 每天都會更新此數據。
> - 若要判斷值區中現有的週期性工作或一次性工作最近分析過的物件時間，請參閱「最新工作執行」欄位。如需有關該工作的其他資訊，請參閱值區的詳細資訊。
> - 若要顯示值區的詳細資訊，請選擇值區的名稱。除了工作相關資訊之外，詳細資料面板還提供值區的統計資料和其他資訊，例如值區的公開存取設定。若要進一步瞭解此資料，請參閱檢閱您的 S3 儲存貯體庫存。

7. 完成選取值區後，請選擇「下一步」。

在下一個步驟中，您將檢閱並確認您的選取項目。

指定值區條件

如果您選擇指定決定要分析哪些 S3 儲存貯體的執行階段條件，Macie 會提供選項來協助您針對條件中的個別條件選擇欄位、運算子和值。若要進一步了解這些選項，請參閱指定 S3 儲存貯體條件。

若要指定工作的 S3 儲存貯體條件

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 在導覽窗格中，選擇 Jobs (任務)。
3. 選擇建立作業。
4. 在 [選擇 S3 儲存貯體] 頁面上，選擇 [指定儲存貯體條件
5. 在「指定值區條件」下，執行下列動作，將條件新增至條件：
   a. 將游標置於篩選方塊中，然後選擇要用於條件的值區內容。
   b. 在第一個方塊中，選擇條件的運算子，「等於」或「不等於」。
   c. 在下一個方塊中，輸入性質的一個或多個值。

根據值區屬性的類型和性質，Macie 會顯示輸入值的不同選項。例如，如果您選擇「有效」權限屬性，Macie 會顯示可供選擇的值清單。如果您選擇「帳戶 ID」屬性，Macie 會顯示一個文字方塊，您可以在其中輸入一或多個 AWS 帳戶 ID。若要在文字方塊中輸入多個值，請輸入每個值，並以逗號分隔每個項目。

d. 選擇套用。Macie 會新增條件，並將其顯示在篩選方塊下方。

   默認情況下，馬西添加了一個包括語句的條件。這表示工作已設定為分析 (包含) 值區中符合條件的物件。若要略過 (排除) 符合條件的值區，請針對條件選擇「包含」，然後選擇「排除」。

e. 針對您要新增至條件的每個其他條件重複上述步驟。

6. 若要測試您的條件，請展開「預覽條件結果」區段。此段落顯示目前符合條件的一般用途值區表格。
7. 若要精簡您的條件，請執行下列任一項作業：

   - 若要移除條件，請選擇「X」做為條件。
   - 若要變更條件，請為條件選擇 X 來移除條件。然後新增具有正確設定的條件。
   - 若要移除所有條件，請選擇 [清除篩選]。

   Macie 會更新條件結果表格，以反映您的變更。
8. 完成指定值區條件後，請選擇「下一步」。

在下一個步驟中，您將檢閱並驗證您的條件。

步驟 2：查看您的 S3 儲存貯體選擇或條件

對於此步驟，請確認您在上述步驟中選擇了正確的設定：

- 檢閱儲存貯體選項-如果您為工作選取了特定的 S3 儲存貯體，請檢閱值區表，並視需要變更儲存貯體選項。此表格提供了工作分析的預計範圍和成本的深入分析。資料是根據目前儲存在值區中的物件大小和類型而定。

  在表格中，「預估成本」欄位會指出分析 S3 儲存貯體中物件的總估計成本 (以美元為單位)。每個估計值都會反映工作將在值區中分析之未壓縮資料的預估數量。如果有任何物件是壓縮檔案或封存檔案，估計值會假設檔案使用 3:1 的壓縮比率，且工作可以分析所有擷取的檔案。如需詳細資訊，請參閱 預測和監控工作成本。

- 複查您的時段條件-如果您已指定工單的時段條件，請複查條件中的每個條件。若要變更條件，請選擇「上一步」，然後使用前述步驟中的篩選選項輸入正確的條件。完成後，請選擇下一步。

完成檢閱和驗證設定後，請選擇 [下一步]。

步驟 3：定義排程並細化範圍

在此步驟中，指定您希望執行工作的頻率 — 一次，或每日、每週或每月定期執行一次。也可以選擇各種選項來細化工作的分析範圍。若要瞭解這些選項，請參閱任務的範圍選項。

若要定義排程並精簡工作範圍，請執行下列步驟：

1. 在 [精簡範圍] 頁面上，指定您要執行工作的頻率：

   - 若只要執行一次工作，請在完成建立工作之後立即選擇「一次性工作」。
   - 若要定期執行工作，請選擇 [排定的工作]。在「更新頻率」中，選擇要每天、每週還是每月執行工作。然後使用「包含現有物件」選項來定義工作第一次執行的範圍：
     - 選取此核取方塊可在完成建立工作後立即分析所有現有物件。每次後續執行都只會分析在前一次執行之後建立或變更的物件。
     - 清除此勾選方塊可略過對所有既有物件的分析。工作的第一次執行只會分析在您完成建立工作後以及第一次執行開始之前所建立或變更的物件。每次後續執行都只會分析在前一次執行之後建立或變更的物件。

       清除此核取方塊對於您已經分析資料且想要定期繼續分析資料的情況很有幫助。例如，如果您之前使用其他服務或應用程式來分類資料，而您最近開始使用 Macie，您可以使用此選項來確保繼續探索和分類您的資料，而不會產生不必要的成本或複製分類資料。
2. (選擇性) 若要指定要工作分析的物件百分比，請在「取樣深度」方塊中輸入百分比。

   如果此值小於 100%，Macie 會根據指定的百分比隨機選取要分析的物件，並分析這些物件中的所有資料。預設值為 100%。
3. (選擇性) 若要新增決定哪些 S3 物件要包含或從任務分析中排除的特定條件，請展開 [其他設定] 區段，然後輸入準則。這些準則由從物件性質導出的個別條件組成：

   - 若要分析 (包括) 符合特定條件的物件，請輸入條件類型和值，然後選擇「包含」。
   - 若要略過 (排除) 符合特定條件的物件，請輸入條件類型和值，然後選擇「排除」。

   針對您想要的每個包含或排除條件重複此步驟。

如果您輸入多個條件，任何排除條件的優先順序都會高於包含條件。例如，如果您包含副檔名為 .pdf 的物件，並排除大於 5 MB 的物件，則工作會分析任何具有 .pdf 副檔名的物件，除非該物件大於 5 MB。

4. 完成後，請選擇下一步。

步驟 4：選取受管理的資料識別碼

在此步驟中，指定工作分析 S3 物件時要使用的受管資料識別碼。您有兩種選擇：

- 使用建議的設定-使用此選項，任務會使用我們針對任務建議的一組受管資料識別碼來分析 S3 物件。此集合旨在檢測敏感數據的常見類別和類型。若要檢閱集合中目前的受管理資料識別碼清單，請參閱建議用於工作的受管資料識別。每當我們在集合中新增或移除受管理的資料識別碼時，我們都會更新該清單。
- 使用自訂設定-使用此選項，任務會使用您選取的受管資料識別碼來分析 S3 物件。這可以是目前可用的全部或僅部分受管理資料識別碼。您也可以將工作設定為不使用任何受管理的資料識別碼。作業只能使用您在下一個步驟中選取的自訂資料識別碼。若要檢閱目前可用的受管理資料識別碼清單，請參閱快速參考：Amazon Macie 受管資料識別碼。每次我們發布新的託管數據標識符時，我們都會更新該列表。

當您選擇其中一個選項時，Macie 會顯示受管理資料識別碼的表格。在資料表中，敏感資料類型欄位會指定受管理資料識別碼的唯一識別碼 (ID)。此識別碼描述了受管資料識別碼用來偵測的敏感資料類型，例如：美國護照號碼的 USA_PASSPORT_NUMBER，信用卡號為信用卡號碼，PGP 私密金鑰的 PGP_ PRIVATE_KEY。若要更快速地尋找特定識別碼，您可以依敏感資料類別或類型來排序和篩選表格。

若要選取工作的受管理資料識別碼

1. 在 [選取受管資料識別碼] 頁面的 [受管理的資料識別碼選項] 下，執行下列其中一個動作：

   - 若要使用我們針對工作建議的一組受管理資料識別碼，請選擇 [建議]。

     如果您選擇此選項，並將工作設定為執行一次以上，則每次執行會在執行開始時自動使用建議集合中的所有受管理資料識別碼。這包括我們釋放並新增至集合的新受管理資料識別碼。它會排除我們從集合中移除且不再建議用於工作的受管資料識別碼。

   - 若只要使用您選取的特定受管理資料識別碼，請選擇 [自訂]，然後選擇 [使用特定受管資料識別碼]。然後，在表格中，選取您要工作使用的每個受管理資料識別碼的核取方塊。

如果您選擇此選項，並將工作設定為執行一次以上，則每次執行都只會使用您選取的受管理資料識別碼。換句話說，工作每次執行時都會使用這些相同的受管理資料識別碼。

- 若要使用 Macie 目前提供的所有受管理資料識別碼，請選擇 [自訂]，然後選擇 [使用特定的受管理資料識別碼]。然後，在表格中，選取選取欄標題中的核取方塊，以選取所有列。

  如果您選擇此選項，並將工作設定為執行一次以上，則每次執行都只會使用您選取的受管理資料識別碼。換句話說，工作每次執行時都會使用這些相同的受管理資料識別碼。

- 若要不使用任何受管理的資料識別碼並僅使用自訂資料識別碼，請選擇 [自訂]，然後選擇 [不使用任何受管理的資料識別碼]。然後，在下一步中，選取要使用的自訂資料識別碼。

2. 完成後，請選擇下一步。

步驟 5：選擇自定義數據標識符

在此步驟中，請選取任務在分析 S3 物件時要使用的任何自訂資料識別碼。除了設定工作使用的任何受管理資料識別碼之外，工作還會使用選取的識別碼。若要進一步瞭解自訂資料識別碼，請參閱建置自訂資料識別符。

若要選取工作的自訂資料識別碼

1. 在 [選取自訂資料識別碼] 頁面上，選取您要工作使用的每個自訂資料識別碼的核取方塊。您最多可以選取 30 個自訂資料識別碼。

   > **Tip**
   >
   > 若要在選取自訂資料識別碼之前檢閱或測試自訂資料識別碼的設定，請選擇識別碼名稱旁邊的連結圖示
   > ( )。Macie
   > 打開一個頁面，顯示標識符的設置。
   > 您也可以使用此頁面來測試使用範例資料的識別碼。若要這麼做，請在 [範例資料] 方塊中輸入最多 1,000 個字元的文字，然後選擇 [測試]。Macie 會使用識別碼來評估範例資料，然後報告相符項目的數目。

2. 完成選取自訂資料識別碼後，請選擇 [下一步]。

步驟 6：選擇允許列表

在此步驟中，選取任何您希望工作在分析 S3 物件時使用的允許清單。若要深入瞭解允許清單，請參閱使用允許清單定義敏感資料例外。

若要選取工作的允許清單

1. 在 [選取允許清單] 頁面上，針對您要工作使用的每個允許清單選取核取方塊。您可以選擇多達 10 個列表。

   > **Tip**
   >
   > 若要在選取允許清單之前檢閱該清單的設定，請選擇清單名稱旁邊的連結圖示 ( )。Macie 會開啟顯示清單設定的頁面。
   > 如果清單指定規則運算式 (regex)，您也可以使用此頁面來測試使用範例資料的 regex。若要這麼做，請在 [範例資料] 方塊中輸入最多 1,000 個字元的文字，然後選擇 [測試]。Macie 使用正則表達式評估樣本數據，然後報告匹配的數量。

2. 完成選取允許清單後，請選擇 [下一步]。

步驟 7：輸入常規設置

對於此步驟，請指定工作的名稱，並選擇性地指定描述。您也可以為工作指派標籤。標籤是您定義並指派給特定 AWS 資源類型的標籤。每個標籤都包含必要的標籤鍵和一個可選的標籤值。標籤可協助您以不同的方式識別、分類及管理資源，例如依用途、擁有者、環境或其他條件。如需進一步了解，請參閱標記亞馬遜麥西資源。

輸入工作的一般設定

1. 在 [輸入一般設定] 頁面上，於 [Job 名稱] 方塊中輸入工作的名稱。該名稱最多可包含 500 個字元。
2. (選擇性) 在「Job 說明」中，輸入工作的簡短描述。該描述最多可包含 200 個字元。
3. (選擇性) 針對「標籤」，選擇「新增標記」，然後輸入最多 50 個標籤以指派給工作。
4. 完成後，請選擇下一步。

步驟 8：檢閱並建立

在最後一個步驟中，檢閱工作的組態設定，並確認設定正確無誤。這是一個重要的步驟。建立工作後，您無法變更任何這些設定。這有助於確保您擁有不可變的敏感資料發現歷史記錄，以及您執行的資料隱私權和保護稽核或調查的探索結果。

根據工作的設定，您也可以檢閱執行作業的總估計成本 (以美元計) 一次。如果您為工作選取了特定的 S3 儲存貯體，則預估會根據您選取的儲存貯體中的物件大小和類型，以及該工作可以分析的資料量。如果您為工作指定了值區條件，則預估會根據目前符合準則的 500 個值區中的物件大小和類型，以及該工作可以分析的資料量。若要瞭解此估計值，請參閱預測和監控工作成本。

若要檢閱和建立工作

1. 在 [檢閱並建立] 頁面上，檢閱每個設定並確認其正確無誤。若要變更設定，請在包含設定的區段中選擇 [編輯]，然後輸入正確的設定。您也可以使用導覽索引標籤移至包含設定的頁面。
2. 完成驗證設定後，請選擇送出以建立並儲存工作。Macie 會檢查設置並通知您要解決的任何問題。

> **Note**
>
> 如果您尚未為敏感資料探索結果設定儲存庫，Macie 會顯示警告，且不會儲存工作。若要解決此問題，請選擇 [儲存區域中的機密資料探查結果] 區段中的 [設定] 然後輸入存放庫的組態設定。如要瞭解如何作業，請參閱儲存及保留敏感資料探索結果。輸入設定值後，請返回「複查並建立」頁面，然後在頁面的「敏感資料探索結果的儲存區域」段落中選擇 refresh ( )。
>
> 雖然我們不建議這樣做，但您可以暫時覆寫存放庫需求並儲存工作。如果這樣做，您可能會遺失工作中的探索結果 — Macie 只會保留 90 天的結果。若要暫時取代需求，請選取取代選項的勾選方塊。

3. 如果 Macie 通知您要解決的問題，請解決問題，然後再次選擇「送出」以建立並儲存工作。

如果您設定工作執行一次、每天執行一次，或在一週或每月的目前日期執行，Macie 會在您儲存工作後立即開始執行工作。否則，Macie 會準備在星期或每月的指定日期執行工作。若要監視工作，您可以檢查工作的狀態。

複查敏感資料探索工作的統計資料和結果

當您執行敏感資料探索任務時，Amazon Macie 會自動計算並報告該任務的特定統計資料。例如，Macie 會報告任務已執行的次數，以及任務目前執行期間尚未處理的 Amazon 簡單儲存服務 (Amazon S3) 物件的大約數目。Macie 也會為工作產生數種類型的結果：記錄事件、敏感資料發現項目，以及敏感資料探索結果。

主題

敏感資料探索工作的結果類型

隨著敏感資料探索任務的進行，Amazon Macie 會產生下列類型的任務結果。

記錄事件

這是工作執行時發生的事件記錄。Macie 會自動記錄特定事件的資料並將其發佈到 Amazon CloudWatch 日誌。這些記錄檔中的資料會提供工作進度或狀態變更的記錄，例如工作開始或停止執行的確切日期和時間。資料也會提供工作執行時發生之任何帳戶或儲存貯體層級錯誤的詳細資料。

記錄事件可協助您監視工作，並解決任何造成工作無法分析所需資料的問題。如果任務使用執行時期條件來判斷要分析哪些 S3 儲存貯體，則記錄事件也可協助您判斷任務執行時是否以及哪些 S3 儲存貯體符合準則。

您可以使用 Amazon CloudWatch 主控台或 Amazon CloudWatch 日誌 API 存取日誌事件。為了協助您導覽至任務的日誌事件，Amazon Macie 主控台會提供指向這些事件的連結。如需詳細資訊，請參閱 監控任務。

敏感資料尋找

這是 Macie 在 S3 物件中找到的敏感資料的報告。每個發現項目都提供嚴重性等級和詳細資料，例如：

- Macie 發現敏感數據的日期和時間。
- Macie 發現的敏感數據的類別和類型。
- Macie 找到的每種敏感資料類型的出現次數。

- 產生尋找項目之工作的唯一識別碼。
- 名稱、公用存取設定、加密類型，以及受影響 S3 儲存貯體和物件的其他相關資訊。

視受影響的 S3 物件的檔案類型或儲存格式而定，詳細資料也可能包含 Macie 找到多達 15 次出現之敏感資料的位置。若要報告位置資料，敏感資料發現項目會使用標準化 JSON 結構定義。

敏感數據發現不包括 Macie 發現的敏感數據。相反地，它會提供資訊，供您視需要用於進一步調查和補救。

Macie 將敏感數據發現存儲 90 天。您可以通過使用 Amazon Macie 控制台或 Amazon Macie API 訪問它們。您還可以使用其他應用程序，服務和系統來監視和處理它們。如需詳細資訊，請參閱 分析發現。

敏感資料探索結果

這是記錄 S3 物件分析詳細資料的記錄。Macie 會自動為您設定要分析的工作的每個物件建立敏感資料探索結果。這包括 Macie 無法在其中找到敏感資料，因此不會產生敏感資料發現項目的物件，以及 Macie 因權限設定或使用不支援的檔案或儲存格式等錯誤或問題而無法分析的物件。

如果 Macie 在 S3 物件中找到敏感資料，則敏感資料探索結果會包含來自對應敏感資料發現項目的資料。它也會提供其他資訊，例如 Macie 在物件中找到的每種敏感資料類型多達 1,000 次出現的位置。例如：

- 在 Microsoft Excel 活頁簿、CSV 檔案或 TSV 檔案中的儲存格或欄位的欄和列號
- JSON 或 JSON 行檔案中欄位或陣列的路徑
- CSV、JSON、JSON 行或 TSV 檔案以外的非二進位文字檔案中的行號，例如 HTML、TXT 或 XML 檔案
- Adobe 可攜式文件格式 (PDF) 檔案中頁面的頁碼
- 記錄索引和路徑在一個 Apache 的 Avro 對象容器或 Apache 實木複合地板文件中的記錄字段

如果受影響的 S3 物件是封存檔案 (例如 .tar 或 .zip 檔案)，敏感資料探索結果也會針對 Macie 從封存中擷取的個別檔案中出現的敏感資料提供詳細位置資料。Macie 不會在封存檔案的敏感資料發現項目中包含此資訊。若要報告位置資料，敏感資料探索結果會使用標準化的 JSON 結構定義。

敏感資料探索結果不包含 Macie 找到的敏感資料。相反，它為您提供了一個分析記錄，可以幫助您進行數據隱私和保護審核或調查。

Macie 會將您的敏感資料探索結果儲存 90 天。您無法直接在 Amazon Macie 控制台或使用 Amazon Macie API 訪問它們。相反地，您可以將 Macie 設定為加密並將它們存放在 S3 儲存貯體

中。儲存貯體可作為所有敏感資料探索結果的確定長期存放庫。然後，您可以選擇性地存取和查詢該儲存庫中的結果。若要瞭解如何進行這些設定，請參閱儲存及保留敏感資料探索結果。

設定完設定之後，Macie 會將您的敏感資料探索結果寫入 JSON 行 (.jsonl) 檔案，並將這些檔案加密並新增至 S3 儲存貯體，做為 GNU Zip (.gz) 檔案。為了協助您瀏覽至搜尋結果，Amazon Macie 主控台會提供這些結果的連結。

敏感資料發現項目和敏感資料探索結果都遵循標準化結構描述。這可協助您選擇性地使用其他應用程式、服務和系統來查詢、監控和處理這些項目。

> **Tip**
>
> 有關如何查詢和使用敏感資料探索結果來分析和報告潛在資料安全風險的詳細說明範例，請參閱安全部落格上的如何使用 Amazon Athena 和 Amazon QuickSight 部落格文章查詢和視覺化 Macie 敏感資料探索結果。AWS
> 如需可用來分析敏感資料探索結果的 Amazon Athena 查詢範例，請造訪上 GitHub的 Amazon Macie 結果分析儲存庫。此儲存庫也提供設定 Athena 擷取和解密結果的指示，以及建立結果表格的指令碼。

複查敏感性資料探索工作的統計資料和結果

若要檢閱個別敏感資料探索任務的處理統計資料和結果，您可以使用 Amazon Macie 主控台或 Amazon Macie API。請依照下列步驟，使用主控台檢閱工作的統計資料和結果。

若要以程式設計方式存取任務的處理統計資料，請使用 Amazon Macie API 的DescribeClassificationJob操作。若要以程式設計方式存取任務產生的發現項目，請使用 Amazon Macie API 的ListFindings操作，並在欄位的篩選條件中指定任務的唯一識別碼。`classificationDetails.jobId`如要瞭解如何作業，請參閱建立並將篩選套用至發現項目。然後，您可以使用此GetFindings作業擷取發現項目的詳細資訊。

若要複查工作的統計資料和結果

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 在導覽窗格中，選擇 Jobs (任務)。
3. 在「工作」頁面上，選擇您要複查其統計值和結果的工作名稱。詳細資料面板會顯示工作的統計資料、設定和其他相關資訊。
4. 在詳細資料面板中，執行下列任一項作業:

- 若要檢閱工作的處理統計資料，請參閱小組的「統計資料」一節。此段落顯示統計資料，例如工作執行的次數，以及工作目前執行期間尚未處理的大約物件數目。
- 若要檢閱工作的記錄事件，請選擇面板頂端的 [顯示結果]，然後選擇 [顯示 CloudWatch 記錄檔]。Macie 打開 Amazon CloudWatch 控制台，並顯示 Macie 為任務發布的日誌事件表。
- 若要檢閱工作產生的所有敏感資料發現項目，請選擇面板頂端的 [顯示結果]，然後選擇 [顯示發現項目]。Macie 會開啟「發現項目」頁面，並顯示工作中的所有發現項目。若要檢閱特定發現項目的詳細資料，請選擇發現項目，然後參閱詳細資料面板。

  > **Tip**
  >
  > 在尋找詳細資料面板中，您可以使用詳細結果位置欄位中的連結導覽至 Amazon S3 中對應的敏感資料探索結果：
  >
  > - 如果發現項目適用於大型封存檔或壓縮檔，則連結會顯示包含檔案探查結果的資料夾。如果封存檔或壓縮檔產生超過 100 個探索結果，則該檔案或壓縮檔案會很大。
  > - 如果發現項目適用於小型歸檔或壓縮檔，則連結會顯示包含檔案探查結果的檔案。如果存檔或壓縮檔產生 100 個或更少的探索結果，則封存檔或壓縮檔案很小。
  > - 如果發現項目適用於其他類型的檔案，則連結會顯示包含檔案探查結果的檔案。

- 若要檢閱工作產生的所有敏感資料探索結果，請選擇面板頂端的 [顯示結果]，然後選擇 [顯示分類]。Macie 會開啟 Amazon S3 主控台，並顯示包含任務所有探索結果的資料夾。您必須將 Macie 設定為將敏感資料探索結果儲存在 S3 儲存貯體中，才能使用此選項。

使用 Amazon CloudWatch 日誌監控敏感資料探索任務

除了監視敏感性資料探索工作的整體狀態之外，您還可以監視和分析工作進行時發生的特定事件。您可以使用 Amazon Macie 自動發佈到 Amazon CloudWatch 日誌的近乎即時的日誌記錄資料來執行此操作。這些記錄檔中的資料會提供工作進度或狀態變更的記錄，例如工作開始執行、暫停或完成執行的確切日期和時間。

記錄檔資料也會提供工作執行時所發生之任何帳戶或儲存貯體層級錯誤的詳細資料。例如，如果 S3 儲存貯體的許可設定阻止工作分析儲存貯體中的物件，Macie 會記錄事件。此事件會指出錯誤發生的時間，並識別受影響的值區和擁有值區的帳戶。這些事件類型的資料可協助您識別、調查和解決錯誤，這些錯誤會阻止 Macie 分析您想要的資料。

使用 Amazon CloudWatch Logs，您可以監控、存放和存取來自多個系統、應用程式和 AWS 服務 Macie 在內的日誌檔。您也可以查詢和分析記錄檔資料，並設定「 CloudWatch 記錄檔」以在發生特定

事件或達到臨界值時通知您。 CloudWatch 日誌還提供存檔日誌資料和將資料匯出到 Amazon S3 的功能。若要進一步了解CloudWatch 日誌，請參閱 Amazon CloudWatch 日誌使用者指南。

主題

記錄如何處理敏感資料探索工作

當您開始執行敏感資料探索任務時，Macie 會自動在 Amazon CloudWatch Logs 中建立和設定適當的資源，以記錄目前所有任務的事件。AWS 區域然後，Macie 會在工作執行時自動將事件資料發佈至這些資源。您帳戶之 Macie 服務連結角色的權限原則可讓 Macie 代表您執行這些工作。您不需要採取任何步驟即可在 CloudWatch 記錄檔中建立或設定資源，或記錄工作的事件資料。

在 CloudWatch 記錄檔中，記錄會組織到記錄群組中。每個記錄群組都包含記錄資料流。每個記錄資料流都包含記錄事件。這些資源的一般用途如下：

- 記錄群組是共用相同保留、監視和存取控制設定的記錄串流集合，例如收集所有敏感資料探索工作的記錄檔。
- 記錄串流是共用相同來源的一系列記錄事件，例如，個別的敏感資料探索工作。
- 記錄事件是應用程式或資源所記錄的活動記錄，例如 Macie 針對特定敏感資料探索工作記錄並發佈的個別事件。

Macie 會將所有敏感資料探索工作的事件發佈至一個記錄群組，而每項工作在該記錄群組中都有唯一的記錄資料流。記錄群組具有下列前置詞和名稱：

```
/aws/macie/classificationjobs
```

如果此記錄群組已存在，Macie 會使用它來儲存工作的記錄事件。如果您的組織使用自動化設定 (例如，針對工作AWS CloudFormation事件使用預先定義的記錄保留期間、加密設定、標籤、指標篩選器等來建立記錄群組)，這會很有幫助。

如果此記錄群組不存在，Macie 會使用 CloudWatch Logs 用於新記錄群組的預設設定來建立該群組。這些設定包括永不過期的記錄保留期，這表示 CloudWatch 記錄檔會無限期儲存記錄檔。若要變更日誌

群組的保留期，您可以使用 Amazon CloudWatch 主控台或 Amazon CloudWatch 日誌 API。要了解如何操作，請參閱 Amazon CloudWatch 日誌使用者指南中的使用日誌群組和日誌串流。

在此記錄群組中，Macie 會在工作第一次執行時，為您執行的每個工作建立唯一的記錄資料流。記錄資料流的名稱是工作的唯一識別碼，例如85a55dc0fa6ed0be5939d0408example，格式如下。

```
/aws/macie/classificationjobs/85a55dc0fa6ed0be5939d0408example
```

每個記錄資料流都包含 Macie 記錄並針對對應工作發佈的所有記錄事件。對於週期性工作，這包括所有工作執行的事件。如果您刪除定期工作的記錄資料流，Macie 會在下次執行工作時再次建立串流。如果您刪除一次性工作的記錄串流，則無法還原該工作。

請注意，根據預設，您的所有工作都會啟用記錄功能。您無法停用它，或以其他方式阻止 Macie 將工作事件發佈至 CloudWatch 記錄檔。如果您不想儲存記錄檔，可以將記錄群組的保留期限縮短至最短一天。在保留期結束時， CloudWatch 記錄檔會自動從記錄群組中刪除過期的事件資料。

檢閱敏感資料探索工作的記錄

您可以使用 Amazon CloudWatch 主控台或 Amazon 日誌 API 來檢閱敏感資料探索任務的 CloudWatch 日誌。控制台和 API 都提供了旨在幫助您查看和分析日誌數據的功能。您可以使用這些功能來處理工作的記錄串流和事件，就像處理記錄中任何其他類型的CloudWatch 記錄資料一樣。

例如，您可以搜尋和篩選彙總資料，以識別在特定時間範圍內針對所有工作發生的特定事件類型。或者，您也可以針對特定工作發生的所有事件執行目標檢閱。 CloudWatch 記錄檔也提供用於監視記錄資料、定義指標篩選器以及建立自訂警示的選項。

> **Tip**
>
> 若要使用 Amazon Macie 主控台導覽至特定任務的日誌事件，請執行以下操作：在「作業」頁面上，選擇任務的名稱。在詳細資料面板頂端，選擇 [顯示結果]，然後選擇 [顯示 CloudWatch 記錄檔]。Macie 會開啟 Amazon CloudWatch 主控台，並顯示任務的日誌事件表格。

若要檢閱任務的日誌 (Amazon CloudWatch 主控台)

1. 請在以下位置開啟 CloudWatch 主控台。 https://console.aws.amazon.com/cloudwatch/
2. 使用頁面右上角的選取AWS 區域器，選取您執行要檢閱記錄之工作的區域。
3. 在導覽窗格中，選擇 Logs (日誌)，然後選擇 Log groups (日誌群組)。

4. 在 [記錄群組] 頁面上，選擇 /aws/maci/ 分類工作記錄群組。 CloudWatch 記錄檔會顯示您已執行之工作的記錄資料流表格。每個作業都有一個唯一的資料流。每個串流的名稱都會與作業的唯一識別碼相關聯。
5. 在「記錄串流」下，執行下列其中一個動作：

   - 若要檢閱特定工作的記錄事件，請選擇該工作的記錄資料流。若要更輕鬆地尋找串流，請在表格上方的篩選方塊中輸入工作的唯一識別碼。選擇記錄資料流之後，「 CloudWatch 記錄」會顯示工作的記錄事件表格。
   - 若要檢閱所有工作的記錄事件，請選擇 [搜尋所有記錄資料流]。 CloudWatch 記錄檔會顯示所有工作的記錄事件表格。
6. (選擇性) 在表格上方的篩選方塊中，輸入字詞、片語或值，以指定要檢閱之特定事件的特性。如需詳細資訊，請參閱 Amazon CloudWatch Logs 使用者指南中的使用篩選模式搜尋日誌資料。
7. 若要檢閱特定記錄事件的詳細資訊，請選擇事件列中的向右箭號 ( )。 CloudWatch 記錄檔會以 JSON 格式顯示事件的詳細資料。

當您熟悉記錄事件中的資料時，也可以執行工作，例如建立將記錄資料轉換為數值指標的 CloudWatch 指標篩選器，以及建立自訂警示，讓您更容易識別並回應特定記錄事件。如需詳細資訊，請參閱 Amazon CloudWatch 日誌使用者指南。

敏感資料探索工作的記錄事件結構描述

敏感資料探索任務的每個日誌事件都是符合 Amazon CloudWatch Logs 事件結構描述且包含一組標準欄位的 JSON 物件。某些類型的事件具有其他欄位，可提供對該類型事件特別有用的資訊。例如，帳戶層級錯誤的事件包括受影響的帳號 ID。AWS 帳戶值區層級錯誤的事件包括受影響 S3 儲存貯體的名稱。如需 Macie 發佈至 CloudWatch 記錄檔的工作事件的詳細清單，請參閱工作的記錄事件類型。

下列範例顯示敏感資料探索工作的記錄事件結構描述。在此範例中，事件報告 Macie 無法分析 S3 儲存貯體中的任何物件，因為 Amazon S3 拒絕存取儲存貯體。

```
{
    "adminAccountId": "123456789012",
    "jobId": "85a55dc0fa6ed0be5939d0408example",
    "eventType": "BUCKET_ACCESS_DENIED",
    "occurredAt": "2021-04-14T17:11:30.574809Z",
    "description": "Macie doesn't have permission to access the affected S3 bucket.",
    "jobName": "My_Macie_Job",
    "operation": "ListObjectsV2",
```

```
    "runDate": "2021-04-14T17:08:30.345809Z",
    "affectedAccount": "111122223333",
    "affectedResource": {
        "type": "S3_BUCKET_NAME",
        "value": "DOC-EXAMPLE-BUCKET"
    }
}
```

在上述範例中，Macie 嘗試使用 Amazon S3 API 的 ListObjectsV2 操作來列出儲存貯體中的物件。當 Macie 將請求發送到 Amazon S3 時，Amazon S3 拒絕訪問存儲桶。

下列欄位適用於敏感資料探索工作的所有記錄事件：

- `adminAccountId`— 建立工作之AWS 帳戶唯一識別元。
- `jobId`— 工作的唯一識別元。
- `eventType`— 發生的事件類型。如需可能值的完整清單和每個值的描述，請參閱工作的記錄事件類型。
- `occurredAt`— 事件發生時的日期和時間，以國際標準時間 (UTC) 和延伸的 ISO 8601 格式表示。
- `description`— 事件的簡要說明。
- `jobName`— 工作的自訂名稱。

視事件的類型和性質而定，記錄事件也可以包含下列欄位：

- `affectedAccount`— 擁有受影響資源之AWS 帳戶唯一識別碼。
- `affectedResource`— 提供有關受影響資源之詳細資訊的物件。在物件中，`type`欄位會指定儲存資源相關中繼資料的欄位。該`value`字段指定字段的值（`type`）。
- `operation`— Macie 嘗試執行並導致錯誤的操作。
- `runDate`— 適用的工作或工作執行開始時的日期和時間，以國際標準時間 (UTC) 和延伸的 ISO 8601 格式顯示。

敏感資料探索工作的記錄事件類型

Macie 發佈三種事件類別的記錄事件：

- Job 狀態事件，記錄工作或工作執行的狀態或進度的變更。
- 帳戶層級錯誤事件，記錄了使 Macie 無法分析特定 Amazon S3 資料的錯誤。AWS 帳戶
- 儲存貯體層級錯誤事件，會記錄阻止 Macie 分析特定 S3 儲存貯體中資料的錯誤。

本節中的主題列出並說明 Macie 針對每個類別發佈的事件類型。

主題

Job 狀態事件

工作狀態事件會記錄工作或工作執行狀態或進度的變更。對於定期工作，Macie 會記錄並發佈整體工作和個別工作執行的這些事件。如需決定工作整體狀態的資訊，請參閱檢查敏感資料探索工作的狀態。

下列範例使用範例資料來顯示工作狀態事件中欄位的結構和性質。在此範例中，SCHEDULED_RUN_COMPLETED事件表示定期工作的排程執行已完成執行。此次運行於 2021 年 4 月 14 日 (世界標準時間下午 5 時 9 分 30 分) 開始，如欄位所示runDate。此次活動已於 2021 年 4 月 14 日 (世界標準時間下午 17 時 30 分) 結束，如欄位所示occurredAt。

```
{
    "adminAccountId": "123456789012",
    "jobId": "ffad0e71455f38a4c7c220f3cexample",
    "eventType": "SCHEDULED_RUN_COMPLETED",
    "occurredAt": "2021-04-14T17:16:30.574809Z",
    "description": "The scheduled job run finished running.",
    "jobName": "My_Daily_Macie_Job",
    "runDate": "2021-04-14T17:09:30.574809Z"
}
```

下表列出並說明 Macie 記錄並發佈至 CloudWatch 「記錄檔」的工作狀態事件類型。「事件類型」(Event type) 欄會指出每個事件出現在事件欄eventType位中時的名稱。「描述」欄提供事件顯示在事件欄description位中時的簡短描述。其他資訊提供有關事件套用之工作類型的資訊。表格會先依照事件可能發生的一般時間先順序排序，然後依事件類型以字母遞增順序排序。

事件類型	描述	其他資訊
已建立工作	工作已建立。	適用於一次性與定期工作。
一次工作已開始	工作開始執行。	僅適用於一次性工作。

事件類型	描述	其他資訊
已排程 _ 執行 (_R) 已啟動	排定的工作執行已開始執行。	僅適用於週期性工作。為了記錄一次性工作的開始，Macie 會發佈一個 ONE_TIME_JOB_START 事件，而不是這種類型的事件。
儲存格符合條件	受影響的值區符合為工作指定的值區條件。	適用於使用執行時期儲存貯體條件來決定要分析哪些 S3 儲存貯體的一次性和週期性工作。 `affectedResource` 物件會指定符合條件且包含在工作分析中的值區名稱。
非值區匹配條件	工作已開始執行，但目前沒有任何值區符合工作指定的值區條件。工作未分析任何資料。	適用於使用執行時期儲存貯體條件來決定要分析哪些 S3 儲存貯體的一次性和週期性工作。
已排程 (_R) 執行完成	排定的工作執行已完成執行。	僅適用於週期性工作。若要記錄一次性工作的完成，Macie 會發佈 JOB_COMPLETED 事件，而不是這種類型的事件。
由使用者暫停工作	使用者已暫停工作。	套用至暫時停止 (已暫停) 的一次性和定期工作。
由使用者履歷的工作	使用者已繼續工作。	適用於暫時停止 (暫停) 並隨後繼續的一次性和定期工作。

事件類型	描述	其他資訊
工作暫停由澳門服務支付	這項工作被梅西暫停了。完成工作將超過受影響帳戶的每月配額。	適用於 Macie 暫時停止 (已暫停) 的一次性和定期工作。 當工作或工作執行的其他處理超過工作分析資料之一或多個帳戶的每月敏感資料探索配額時，Macie 會自動暫停工作。若要避免此問題，請考慮增加受影響帳戶的配額。
工作簡歷由澳門服務 _ 報價解除	這份工作被馬西恢復了。受影響帳戶的每月服務配額已解除。	適用於 Macie 暫時停止 (暫停) 並隨後繼續的一次性和定期工作。 如果 Macie 自動暫停一次性工作，Macie 會在隨後的月份開始時自動繼續工作，或增加所有受影響帳戶的每月敏感資料探索配額 (以先發生者為準)。如果 Macie 自動暫停定期工作，Macie 會在排定下一次執行開始或後續月份開始 (以先發生者為準) 時自動繼續工作。

事件類型	描述	其他資訊
工作 (_ 取消)	工作已取消。	適用於您永久停止 (已取消) 的一次性和定期工作，或針對一次性工作，在 30 天內暫停和未恢復的工作。 如果您暫停或停用 Macie，此類型的事件也會套用至您暫停或停用 Macie 時處於作用中或暫停狀態的工作。AWS 區域如果您暫停或禁用 Macie 在該地區，Macie 會自動取消您的作業。
工作 (_完成)	工作已完成執行。	僅適用於一次性工作。若要記錄定期工作的工作執行完成，Macie 會發佈排程 _RUN_COMPLEED 事件，而非此類型的事件。

帳戶層級錯誤事件

帳戶層級錯誤事件會記錄錯誤，導致 Macie 無法分析特定儲存貯體所擁有的 S3 儲存貯體中的物件。AWS 帳戶每個事件中的`affectedAccount`欄位都會指定該帳戶的帳戶 ID。

下列範例使用範例資料來顯示帳戶層級錯誤事件中欄位的結構和性質。在此範例中，`ACCOUNT_ACCESS_DENIED`事件表示 Macie 無法分析帳戶`444455556666`擁有的任何 S3 儲存貯體中的物件。

```
{
    "adminAccountId": "123456789012",
    "jobId": "85a55dc0fa6ed0be5939d0408example",
    "eventType": "ACCOUNT_ACCESS_DENIED",
    "occurredAt": "2021-04-14T17:08:30.585709Z",
    "description": "Macie doesn’t have permission to access S3 bucket data for the
 affected account.",
```

```
    "jobName": "My_Macie_Job",
    "operation": "ListBuckets",
    "runDate": "2021-04-14T17:05:27.574809Z",
    "affectedAccount": "444455556666"
}
```

下表列出並說明 Macie 記錄並發佈至記錄的帳戶層級錯誤事件類型。 CloudWatch 「事件類型」(Event type) 欄會指出每個事件出現在事件欄`eventType`位中時的名稱。「描述」欄提供事件顯示在事件欄`description`位中時的簡短描述。「其他資訊」欄提供調查或解決發生錯誤的任何適用提示。該表按事件類型按字母升序排序。

事件類型	描述	其他資訊
帳戶訪問被拒絕	Macie 沒有存取受影響帳戶的 S3 儲存貯體資料的權限。	這通常是因為帳戶所擁有的值區具有限制性的值區政策。如需如何解決此問題的詳細資訊，請參閱允許 Macie 存取 S3 儲存貯體和物件。 事件中`operation` 欄位的值可協助您判斷哪些許可設定阻止 Macie 存取帳戶的 S3 資料。此欄位表示 Macie 在發生錯誤時嘗試執行的 Amazon S3 作業。
帳戶停用	工作略過受影響帳號所擁有的資源。該帳戶已禁用馬西。	要解決此問題，請重新啟用相同帳戶的 Macie。AWS 區域
已解除關聯的帳戶	工作略過受影響帳號所擁有的資源。該帳戶不再與您的 Macie 管理員帳戶作為成員帳戶關聯。	如果您身為組織的 Macie 管理員，將工作設定為分析關聯成員帳戶的資料，且該成員帳戶隨後從您的組織中移除，就會發生這種情況。 若要解決此問題，請將受影響的帳戶與您的 Macie 管理員帳

事件類型	描述	其他資訊
		戶重新建立關聯，做為成員帳戶。如需詳細資訊，請參閱管理多個 帳戶。
帳戶隔離 (_)	工作略過受影響帳號所擁有的資源。AWS 帳戶被隔離了。	–
帳戶區域已停用	工作略過受影響帳號所擁有的資源。在目前中AWS 帳戶沒有作用中AWS 區域。	–
帳戶 (_ 暫停)	工作已取消或略過受影響帳號所擁有的資源。梅西被暫停的帳戶。	如果指定的帳戶是您自己的帳戶，Macie 會自動取消作業，當您暫停 Macie 在同一地區。若要解決此問題，請重新啟用該地區中的 Macie。 如果指定的帳戶是會員帳戶，請在同一地區重新啟用該帳戶的 Macie。
帳戶終止	工作略過受影響帳號所擁有的資源。AWS 帳戶已終止。	–

值區層級錯誤事件

儲存貯體層級錯誤事件會記錄錯誤，導致 Macie 無法分析特定 S3 儲存貯體中的物件。每個事件中的`affectedAccount`欄位都會指定擁有值區的帳戶 ID。AWS 帳戶每個事`affectedResource`件中的物件都會指定值區的名稱。

下列範例會使用範例資料來顯示儲存貯體層級錯誤事件中欄位的結構和性質。在此範例中，`BUCKET_ACCESS_DENIED`事件表示 Macie 無法分析名為`DOC-EXAMPLE-BUCKET`的 S3 儲存貯體中的任何物件。當 Macie 嘗試使用 Amazon S3 API 的 ListObjectsV2 操作列出儲存貯體中的物件時，Amazon S3 拒絕存取儲存貯體。

```
{
    "adminAccountId": "123456789012",
    "jobId": "85a55dc0fa6ed0be5939d0408example",
    "eventType": "BUCKET_ACCESS_DENIED",
    "occurredAt": "2021-04-14T17:11:30.574809Z",
    "description": "Macie doesn't have permission to access the affected S3 bucket.",
    "jobName": "My_Macie_Job",
    "operation": "ListObjectsV2",
    "runDate": "2021-04-14T17:09:30.685209Z",
    "affectedAccount": "111122223333",
    "affectedResource": {
        "type": "S3_BUCKET_NAME",
        "value": "DOC-EXAMPLE-BUCKET"
    }
}
```

下表列出並說明 Macie 記錄並發佈至「記錄檔」的儲存貯體層級錯誤事件類型。 CloudWatch 「事件類型」(Event type) 欄會指出每個事件出現在事件欄`eventType`位中時的名稱。「描述」欄提供事件顯示在事件欄`description`位中時的簡短描述。「其他資訊」欄提供調查或解決發生錯誤的任何適用提示。該表按事件類型按字母升序排序。

事件類型	描述	其他資訊
存取被拒絕	Macie 沒有存取受影響的 S3 儲存貯體的權限。	這通常是因為值區具有限制性的值區政策。如需如何解決此問題的詳細資訊，請參閱允許 Macie 存取 S3 儲存貯體和物件。 事件中`operation` 欄位的值可協助您判斷哪些權限設定阻止 Macie 存取值區。此欄位表示 Macie 在發生錯誤時嘗試執行的 Amazon S3 作業。
桶 _ 詳細資料 _ 不可用	暫時性問題導致 Macie 無法擷取值區和值區物件的詳細資料。	如果暫時性問題導致 Macie 無法擷取分析值區物件所需的值區和物件中繼資料，就會發生

事件類型	描述	其他資訊
		此問題。例如，當 Macie 嘗試驗證是否允許存取儲存貯體時，就會發生 Amazon S3 例外狀況。 若要解決一次性工作的問題，請考慮建立並執行新的一次性工作來分析值區中的物件。對於排定的工作，Macie 會在下一次工作執行期間嘗試再次擷取中繼資料。
儲存貯體不存在	受影響的 S3 儲存貯體不再存在。	這通常是因為已刪除值區而發生。
區域不同區域	受影響的 S3 儲存貯體已移至其他儲存貯體AWS 區域。	–
儲存桶所有者 _ 已變更	受影響 S3 儲存貯體的擁有者已變更。Macie 已經沒有存取桶的權限了。	如果儲存貯體的擁有權已移轉至不屬於您組織的值區，通常會發生這種情況。AWS 帳戶事件中的`affectedAccount` 欄位會指出先前擁有該值區之帳戶的帳戶 ID。

管理敏感性資料探索工作

為了協助您管理敏感資料探索任務，Amazon Macie 會提供每個 AWS 區域任務的完整清查。使用此清查，您可以將工作作為單一集合管理，並存取個別作業的組態設定、狀態和處理統計資料。您也可以存取敏感資料發現項目，以及每項工作產生的其他結果。

除了這些工作之外，您還可以建立個別工作的自訂變體：複製現有工作、調整複本的設定，然後將複本儲存為新工作。如果您想要以相同的方式分析不同的資料集，或以不同的方式分析相同的資料集，這可

能很有幫助。或者您想要調整現有工作的組態設定 — 取消現有工作、複製它，然後調整複本並將其儲存為新工作。

主題

檢閱敏感資料探索工作的清查

Amazon Macie 主控台上的「工作」頁面提供目 AWS 區域前帳戶所有敏感資料探索任務的相關資訊。此表格會針對每個工作顯示摘要資訊，其中包括：工作目前的狀態、工作是否按排程定期執行；以及工作是否分析特定數量的 S3 儲存貯體，還是分析符合執行階段準則的 S3 儲存貯體。如果您在表格中選擇工作，詳細資料面板會顯示組態設定和其他有關該工作的資訊。

若要檢視您的工作庫存

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 在導覽窗格中，選擇 Jobs (任務)。「工作」(Jobs) 頁面隨即開啟，並顯示詳細目錄中的工作數目，以及這些工作的表格。
3. 若要更快找到特定工作，請執行下列任一項作業：

   - 若要依特定欄位對表格進行排序，請選擇欄位的欄標題。若要變更排序順序，請再次選擇欄標題。
   - 若只要顯示具有特定欄位值的工作，請將游標置於篩選方塊中。在出現的功能表中，選擇要用於篩選的欄位，然後輸入篩選的值。接著選擇 Apply (套用)。
   - 若要隱藏具有特定欄位值的工作，請將游標置於篩選方塊中。在出現的功能表中，選擇要用於篩選的欄位，然後輸入篩選的值。接著選擇 Apply (套用)。在篩選方塊中，選擇篩選條件的等於圖示 (●)。這將過濾器的運算符從 equals 更改為不等於 ( )

- 若要移除篩選，請選擇要移除的篩選器的移除篩選圖示 ()。

4. 若要檢閱特定工作的組態設定和其他詳細資料，請在表格中選擇工作的名稱，然後參閱詳細資料面板。

檢閱敏感資料探查工作的組態設定

在 Amazon Macie 主控台上，您可以使用「任務」頁面上的詳細資料面板來檢閱組態設定和有關個別敏感資料探索任務的其他資訊。例如，您可以檢閱工作設定用來分析的 S3 儲存貯體清單，以及任務用來分析這些值區中物件的受管資料識別碼。

> **Note**
>
> 您無法變更現有工作的任何組態設定。這有助於確保您擁有不可變的敏感資料發現歷史記錄，以及您執行的資料隱私權和保護稽核或調查的探索結果。如果要變更現有工作，請取消該工作。然後複製工作，將副本設定為使用所需的設定，然後將副本儲存為新工作。
> 如果您這樣做，您也應該採取措施，以確保新工作不會再以相同的方式分析現有資料。若要這麼做，請記下您取消現有工作的日期和時間。然後將新工作的範圍設定為僅包含取消原始工作後建立或變更的物件。例如，使用物件條件來新增「上次修改」排除條件，以指定您取消原始工作的日期和時間。

檢閱工作的組態設定

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 在導覽窗格中，選擇 Jobs (任務)。
3. 在「工作」頁面上，選擇您要檢閱其設定的工作名稱。詳細資料面板會顯示組態設定和工作的其他相關資訊。根據工作的設定，面板包含下列區段。

一般資訊

本節提供有關工作的一般資訊 — 例如，任務的 Amazon 資源名稱 (ARN)、工作最近開始執行的時間，以及任務的目前狀態。如果您暫停工作，此區段也會指出您暫停工作的時間，以及工作或最新工作執行的時間到期或未繼續工作的時間到期。

統計

此段落顯示工作的處理統計資料 — 例如，工作已執行的次數，以及工作目前執行期間尚未處理的大約物件數目。

Scope (範圍)

此段落指出工作執行的頻率。它也會顯示精簡任務範圍的設定，例如取樣深度，以及任何在任務分析中包含或排除 S3 物件的物件標準。

S3 儲存貯體

如果將工作設定為分析您在建立工作時明確選取的值區，則此區段會顯示在面板中。這表示設定為分析資料的 AWS 帳戶 工作編號。它也會指出工作設定要分析的值區數目，以及這些值區的名稱 (依帳戶分組)。

若要以 JSON 格式顯示帳戶和值區的完整清單，請在「總值區」欄位中選擇數字。

S3 儲存貯體條件

如果工作使用執行階段準則來決定要分析的值區，此區段就會顯示在面板中。它會列出工作設定為使用的準則。

若要以 JSON 格式顯示條件，請選擇 [詳細資料]，然後在出現的視窗中選擇 [條件] 索引標籤。

若要複查目前符合條件的時段表格，請選擇「明細」，然後在出現的視窗中選擇「比對時段」頁標。選擇性地選擇重新整理 () 以擷取最新資料。

> **Tip**
>
> 如果工作已經執行，您也可以決定工作執行時是否有任何值區符合條件，以及這些值區的名稱 (若有)。若要這麼做，請檢閱工作的記錄事件：選擇面板頂端的 [顯示結果]，然後選擇 [顯示 CloudWatch 記錄檔]。Macie 會開啟 Amazon CloudWatch 主控台，並顯示任務的日誌事件表格。這些`BUCKET_MATCHED_THE_CRITERIA`事件包括符合條件且包含在工作分析中的每個值區的事件。如需詳細資訊，請參閱 監控任務。

自訂資料識別碼

如果工作設定為使用一或多個自訂資料識別碼，此區段就會顯示在面板中。它會指定這些自訂資料識別碼的名稱。

允許清單

如果工作設定為使用一或多個允許清單，此區段就會顯示在面板中。它指定這些列表的名稱。若要檢閱清單的設定和狀態，請選擇清單名稱旁邊的連結圖示 ( )。

受管資料識別碼

此段落指出工作設定要使用的受管理資料識別碼。這是由工作的受管理資料識別碼選擇類型決定：

- 建議 — 工作執行時，使用建議集中的受管理資料識別碼。
- 包括所選項目 — 僅使用「選取項目」區段中列出的受管理資料識別碼。
- 包含全部 — 使用工作執行時可用的所有受管資料識別碼。
- 排除選取項目 — 使用工作執行時可用的所有受管理資料識別碼，但「選取項目」段落中列出的 ID 除外。
- 全部排除 — 不使用任何受管理的資料識別碼。僅使用指定的自訂資料識別碼。

若要檢閱 JSON 格式的這些設定，請選擇 [詳細資料]。

Tags (標籤)

如果標籤與工作相關聯，則此區段會顯示在面板中。它會列出這些標籤。

標籤是您定義並指派給特定 AWS 資源類型的標籤。每個標籤都包含必要的標籤鍵和一個可選的標籤值。標籤可協助您以不同的方式識別、分類及管理資源，例如依用途、擁有者、環境或其他條件。如需進一步了解，請參閱標記亞馬遜麥西資源。

4. 若要檢閱並以 JSON 格式儲存工作的設定，請在面板頂端選擇工作的唯一識別碼 (J ob ID)，然後選擇 [下載]。

檢查敏感資料探索工作的狀態

建立敏感資料探查工作時，其初始狀態為「作用中」(執行中) 或「作用中」(閒置)，視工作的類型和排程而定。然後工作會經過其他狀態，您可以在工作進行時監視這些狀態。

> **Tip**
>
> 除了監視工作的整體狀態之外，您還可以監視工作進行時發生的特定事件。您可以使用 Macie 自動發佈到 Amazon CloudWatch 日誌的記錄資料來執行此操作。這些記錄檔中的資料會提供工作狀態變更的記錄，以及工作執行時發生之任何帳戶或儲存貯體層級錯誤的詳細資料。如需詳細資訊，請參閱 監控任務。

檢查 工作的狀態

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 在導覽窗格中，選擇 Jobs (任務)。
3. 在「工作」頁面上，找出您要檢查其狀態的工作。「狀態」(Status) 欄位會指出工作的目前狀態。

作用中 (閒置)

對於定期工作，上一次執行已完成，且下一個排定的執行正在擱置中。此值不適用於一次性工作。

作用中 (執行中)

對於一次性工作，工作目前正在進行中。對於定期工作，已排程的執行正在進行中。

已取消

對於任何類型的工作，工作都會永久停止 (已取消)。

如果您明確取消工作，或者如果是一次性工作，則您暫停工作而未在 30 天內恢復工作，則該工作將具有此狀態。如果您先前在目 AWS 區域前暫停 Macie，工作也可以具有此狀態。

完成

對於一次性工作，工作已成功執行，現在已完成。此值不適用於週期性工作。每次執行成功完成時，週期性工作的狀態會變更為「作用中 (閒置)」。

暫停（由馬西）

對於任何類型的工作，Macie 已暫時停止 (暫停) 工作。

如果工作完成或工作執行會超過您帳戶的每月敏感資料探索配額，則工作會具有此狀態。發生這種情況時，Macie 會自動暫停工作。Macie 會在下一個日曆月份開始時自動恢復工作（並且帳戶的每月配額已重設），或者您增加帳戶的配額。

如果您是組織的 Macie 系統管理員，並將工作設定為分析成員帳戶的資料，則如果工作完成或工作執行會超過成員帳戶的每月敏感資料探索配額，則該工作也會有此狀態。

如果工作正在執行，且合格物件的分析達到成員帳戶的此配額，則工作將停止分析該帳戶所擁有的物件。當工作完成分析所有其他未達配額的帳戶的物件時，Macie 會自動暫停工作。如果這是一次性工作，Macie 會在下一個日曆月開始時自動恢復工作，或增加所有受影響帳戶的配額，以先發生者為準。如果是定期工作，Macie 會在排定下一次執行開始或下一個行事曆月份開始 (以先發生者為準) 時自動繼續工作。如果排定的執行在下個行事曆月份開始之前開始，或是受影響帳戶的配額增加，則工作不會分析帳戶擁有的物件。

已暫停 (依使用者)

對於任何類型的工作，您都會暫時停止 (暫停) 工作。

如果您暫停一次性工作，但未在 30 天內繼續工作，則工作會過期，而 Macie 會取消。如果您在定期工作正在執行時暫停工作，但未在 30 天內繼續執行，則工作的執行會過期，而 Macie 會取消執行。若要檢查暫停工作或工作執行的到期日，請在表格中選擇工作的名稱，然後參考詳細資料面板中「狀態詳細資料」區段中的「過期」欄位。

如果工作已取消或暫停，您可以參考工作的詳細資料，以判斷工作是否開始執行，或者針對定期工作，在取消或暫停之前至少執行一次。若要這麼做，請在表格中選擇工作名稱，然後參考詳細資料面板。在面板中，[執行次數] 欄位會指出工作已執行的次數。「上次執行時間」欄位會指出工作開始執行的最近日期和時間。

根據工作的目前狀態，您可以選擇性地暫停、繼續或取消工作。

暫停、繼續或取消敏感資料探索工作

建立敏感資料探索工作後，您可以暫時將其暫停或永久取消。當您暫停正在執行的工作時，Macie 會立即開始暫停該工作的所有處理工作。當您取消正在執行的工作時，Macie 會立即開始停止該工作的所有處理工作。取消工作後，您無法繼續或重新啟動工作。

如果暫停一次性工作，您可以在 30 天內恢復工作。當您繼續工作時，Macie 會立即從您暫停工作的位置繼續處理，MacIE 不會從頭開始重新啟動工作。如果您沒有在暫停工作的 30 天內恢復一次性工作，則工作會過期，而 Macie 會取消它。

如果您暫停定期工作，您可以隨時繼續工作。如果您繼續定期工作，且工作在暫停時處於閒置狀態，Macie 會根據您在建立工作時選擇的排程和其他組態設定繼續工作。如果您繼續定期工作，而當您暫停工作時該工作仍在進行中，Macie 恢復工作的方式取決於您何時繼續工作：

- 如果您在暫停工作的 30 天內繼續工作，Macie 會立即從您暫停工作的點繼續最新排定的執行 — MacIE 不會從頭開始重新啟動執行。
- 如果您沒有在暫停工作的 30 天內繼續工作，則最新排程的執行會過期，而 Macie 會取消所有剩餘的處理工作以進行執行。當您隨後繼續工作時，Macie 會根據您在建立工作時選擇的排程和其他組態設定繼續工作。

為了協助您判斷暫停的工作或工作執行何時到期，Macie 會在工作暫停時將到期日新增至工作的詳細資料。若要檢查此日期，請在「工作」頁面的表格中選擇工作名稱，然後參考詳細資料面板中「狀態詳細資料」區段中的「過期」欄位。此外，我們會在工作或工作執行到期前大約七天通知您。當工作或作業執行到期且被取消時，我們會再次通知您。為了通知您，我們會將電子郵件發送到與您相關聯的電子郵件地址 AWS 帳戶。我們還為您的帳戶創建 AWS Health CloudWatch 活動和 Amazon 活動。

暫停、繼續或取消工作

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 在導覽窗格中，選擇 Jobs (任務)。
3. 在 [工作] 頁面上，選取您要暫停、繼續或取消之工作的核取方塊，然後在 [動作] 功能表上執行下列其中一項作業：
   - 若要暫停工作，請選擇 [暫停]。只有當工作的目前狀態為作用中 (閒置)、作用中 (執行中) 或已暫停 (由 Macie) 時，才能使用此選項。
   - 若要繼續工作，請選擇 [繼續]。只有當工作的目前狀態為「已暫停」(依使用者) 時，才能使用此選項。
   - 若要永久取消工作，請選擇「取消」。如果選擇此選項，則隨後將無法繼續或重新啟動工作。

複製敏感資料探索工作

若要快速建立與現有工作類似的新敏感資料探索工作，您可以建立工作的副本、編輯副本的設定，然後將副本儲存為新工作。如果您想要建立現有工作的自訂變體，這會很有幫助。或者您想要透過取消工作，然後複製、變更和儲存設定為新工作來調整現有工作的組態設定。

複製工作

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 在導覽窗格中，選擇 Jobs (任務)。
3. 選取要複製之工作的核取方塊。

4. 在 [動作] 功能表上，選擇 [複製到新的]。
5. 完成主控台上的步驟，以檢閱和調整工作副本的設定。針對「精簡範圍」 步驟，請考慮選擇可防止工作再次以相同方式分析現有資料的選項：

   - 對於一次性工作，請使用物件條件來僅包含在特定時間之後建立或變更的物件。例如，如果您要建立已取消的工作副本，請新增 [上次修改] 條件，指定取消現有工作的日期和時間。
   - 對於定期工作，請清除「包括現有物件」核取方塊。如果您這麼做，第一次工作執行只會分析建立工作之後和工作第一次執行之前所建立或變更的物件。您也可以使用物件條件來排除上次在特定日期和時間之前修改的物件。

   如需此步驟和其他步驟的其他詳細資訊，請參閱建立敏感資料探索任務。
6. 完成時，請選擇送出，將複本儲存為新工作。

預測和監控敏感資料探索任務的成本

Amazon Macie 定價部分取決於您透過執行敏感資料探索任務分析的資料量。若要預測和監視執行敏感資料探索工作的估計成本，您可以檢閱 Macie 在建立工作時和開始執行作業時所提供的成本預估值。

要查看和監視您的實際成本，您可以使用AWS Billing and Cost Management。 AWS Billing and Cost Management提供的功能可協助您追蹤和分析成本AWS 服務，以及管理帳戶或組織的預算。它還提供了可幫助您根據歷史數據預測使用成本的功能。若要進一步了解 ，請參閱 AWS Billing 使用者指南。

如需有關 Macie 定價的資訊，請參閱 Amazon Macie 定價。

主題

- 預測敏感資料探索任務的成本
- 監控敏感資料探索任務的預估成本

預測敏感資料探索任務的成本

建立敏感資料探索任務時，Amazon Macie 可以計算並顯示任務建立程序中兩個關鍵步驟的估計成本：當您檢閱為任務選取的 S3 儲存貯體表格 (步驟 2) 以及檢閱任務的所有設定時 (步驟 8)。這些預估值可協助您決定是否在儲存工作之前調整工作的設定。預估值的可用性和性質取決於您為工作選擇的設定。

複查個別時段的預估成本 (步驟 2)

如果您明確選取要分析之工作的個別值區，則可以複查分析每個值區中物件的預估成本。當您複查儲存貯體選項時，Macie 會在工作建立程序的步驟 2 中顯示這些預估值。在此步驟的表格中，顯示執行任務一次的預估成本總計 (以美元計算)。

每個估計值都會根據目前儲存在值區中的物件大小和類型，反映工作將在值區中分析的未壓縮資料預計數量。該估計還反映了當前AWS 區域的 Macie 定價。

值區的成本估算中只會包含可分類的物件。可分類物件是 S3 物件，使用支援的 Amazon S3 儲存類別，且具有支援檔案或儲存格式的副檔名。如果有任何可分類的物件為壓縮檔案或封存檔案，估計值會假設檔案使用 3:1 的壓縮比率，且工作可以分析所有擷取的檔案。

複查工作的估計總成本 (步驟 8)

如果您建立一次性任務，或是建立並設定定期工作以包含現有 S3 物件，Macie 會在任務建立程序的最後一個步驟中計算並顯示該工作的預估總成本。您可以在檢閱並確認為工作選取的所有設定時，檢閱此預估值。

此預估成員會指出在目前區域執行任務一次的預估成本總計 (以美元計算)。估計值會反映工作將分析之未壓縮資料的預估量。它是根據目前儲存在您為工作明確選取的值區中的物件大小和類型，或最多 500 個目前符合您為工作指定的值區條件的值區條件的值區 (視工作的設定而定) 為基礎。

請注意，此估計不會反映您選取用來調整和縮小工作範圍的任何選項，例如較低的取樣深度，或從任務中排除特定 S3 物件的條件。它也不會反映您每月的敏感資料探索配額，這可能會限制工作分析的範圍和成本，或是可能適用於您帳戶的任何折扣。

除了工作的總估計成本之外，估算還提供彙總資料，以深入瞭解工作的預計範圍和成本：

- 大小值會指出任務可以分析和無法分析之物件的總儲存大小。
- 物件計數值會指出任務可以分析和無法分析的物件總數。

在這些值中，可分類物件是 S3 物件，它使用支援的 Amazon S3 儲存類別，且具有支援檔案或儲存格式的副檔名。只有可分類的物件才會包含在成本估算中。「不可分類的物件」是指未使用支援的儲存類別，或是沒有支援檔案或儲存格式之副檔名的物件。這些物件不會包含在成本估算中。

估計值會針對壓縮或封存檔案的 S3 物件提供其他彙總資料。壓縮值表示使用支援的 Amazon S3 儲存類別，並具有受支援類型的壓縮或存檔檔案副檔名之物件的總儲存大小。未壓縮值會根據指定的壓縮比例，指出解壓縮這些物件的約略大小。由於 Macie 分析壓縮文件和歸檔文件的方式，此數據是相關的。

當 Macie 分析壓縮檔案或封存檔案時，會同時檢查完整檔案和檔案內容。為了檢查檔案的內容，Macie 會將檔案解壓縮，然後檢查每個使用支援格式的解壓縮檔案。因此，工作分析的實際資料量取決於：

- 檔案是否使用壓縮，如果使用壓縮，則使用壓縮比率。
- 解壓縮檔案的數量、大小和格式。

默認情況下，Macie 在計算工作的成本估算時會假設以下內容：

- 所有壓縮檔案和封存檔案都使用 3:1 的壓縮比例。
- 所有解壓縮的文件都使用支持的文件或存儲格式。

這些假設可能會對工作將分析的資料範圍產生較大的大小估計，因此可能會產生較高的工作成本預估。

您可以根據不同的壓縮比率重新計算工作的估計總成本。若要執行此操作，請從 [估計成本] 區段的 [選擇估計的壓縮比率] 清單中選擇比率。然後，Macie 會更新估計值以符合您的選擇。

如需 Amazon ie 計算預估成本的詳細資訊，請參閱瞭解估計使用成本的計算方式。

監控敏感資料探索任務的預估成本

如果您已經在執行敏感資料探索任務，Amazon Macie 主控台上的「使用情況」頁面可協助您監控這些任務的預估成本。此頁面顯示您目前AWS 區域的預估成本 (以美元計算)。如需有關 Macie 如何計算這些估計值的資訊，請參閱瞭解估計使用成本的計算方式。

檢閱執行工作的估計成本

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 使用頁面右上角的選AWS 區域擇器，選擇要檢閱預估成本的區域。
3. 在導覽窗格中，選擇使用法。
4. 在 [使用量] 頁面上，請參閱您帳戶的預估費用明細。敏感性資料探索工作項目會報告您目前為止在目前「區域」目前為止在目前月份執行的工作預估總成本。

   如果您是組織的 Macie 管理員，則「預估費用」區段會顯示您組織目前「區域」當月的整體預估成本。若要顯示針對特定帳戶執行任務的預估成本總計，請在表格中選擇帳戶。然後，「預估成本」區段會顯示帳戶的預估成本明細，包括執行作業的預估成本。若要顯示不同帳戶的此資料，請在表格中選擇帳戶。若要清除您的帳戶選擇，請選擇帳戶 ID 旁邊的 X。

若要檢閱和監控您的實際成本，請使用AWS Billing and Cost Management。

建議用於敏感資料探索工作的受管資料識別

若要最佳化敏感性資料探索工作的結果，您可以將個別工作設定為自動使用我們針對工作建議的一組受管資料識別碼。一個受管資料識別碼是一組內建準則和技術，用來偵測特定類型的敏感資料，例如，AWS特定國家或地區的秘密存取金鑰、信用卡號碼或護照號碼。

建議的受管資料識別碼集是設計來偵測敏感資料的常見類別和類型。根據我們的研究，它可以檢測敏感數據的一般類別和類型，同時還可以通過降低噪音來優化您的工作結果。當我們發佈新的受管資料識別碼時，如果這些識別碼可能會進一步最佳化您的工作結果，我們會將它們新增至此集。隨著時間的推移，我們也可能會在集合中新增或移除現有的受管理資料識別碼。如果我們在建議的資料集中新增或移除受管理的資料識別碼，我們會更新此頁面以指出變更的性質和時間。如需有關這些變更的自動警示，您可以訂閱馬西文件歷史頁面。

建立敏感資料探索任務時，您可以指定任務用來分析 Amazon 簡單儲存服務 (Amazon S3) 儲存貯體中的物件的受管資料識別碼。若要將工作設定為使用建議的一組受管理資料識別碼，請選擇推薦建立工作時的選項。然後，工作會在工作開始執行時，自動使用建議集合中的所有受管理資料識別碼。如果您將工作設定為執行多次，則每次執行都會在執行開始時自動使用建議集合中的所有受管理資料識別碼。

下列主題列出目前位於建議集中的受管理資料識別碼，依機密資料類別和類型進行組織。它們會為集合中的每個受管理資料識別碼指定唯一識別碼 (ID)。此 ID 描述受管理資料識別碼用來偵測的機密資料類型，例如：`PGP_PRIVATE_KEY`適用於 PGP 私密金鑰和`USA_PASSPORT_NUMBER`美國護照號碼。

主題

- 憑證
- 財務資訊
- 個人身分識別資訊 (PII)
- 更新推薦集

如需有關特定受管理資料識別碼的詳細資訊，或 Macie 目前提供的所有受管理資料識別碼的完整清單，請參閱使用受管資料識別符。

憑證

若要偵測 S3 物件中登入資料資料的發生次數，建議的集合會使用下列受管資料識別碼。

敏感資料類型	受管資料識別符 ID
AWS 私密存取金鑰	`AWS_CREDENTIALS`

敏感資料類型	受管資料識別符 ID
HTTP 基本授權標頭	HTTP_BASIC_AUTH_HEADER
OpenSSH 私密金鑰	OPENSSH_PRIVATE_KEY
PGP 私密金鑰	PGP_PRIVATE_KEY
公開金鑰加密標準 (PKCS) 私密金鑰	PKCS
PuTTY 私密金鑰	PUTTY_PRIVATE_KEY

財務資訊

若要偵測 S3 物件中財務資訊的發生次數，建議的集合會使用下列受管資料識別碼。

敏感資料類型	受管資料識別符 ID
信用卡磁條數據	CREDIT_CARD_MAGNETIC_STRIPE
信用卡號碼	CREDIT_CARD_NUMBER (適用於鄰近關鍵字的信用卡號碼)

個人身分識別資訊 (PII)

若要偵測 S3 物件中個人識別資訊 (PII) 的發生次數，建議的集合使用下列受管資料識別碼。

敏感資料類型	受管資料識別符 ID
駕照識別號碼	CANADA_DRIVERS_LICENSE, DRIVERS_LICENSE (適用於美國),UK_DRIVERS_LICENSE
選民名冊號碼	UK_ELECTORAL_ROLL_NUMBER
國家身分證號碼	FRANCE_NATIONAL_IDENTIFICATION_NUMBER, GERMANY_NATIONAL_IDENTIFICATION_NUMBER, ITALY_NAT

敏感資料類型	受管資料識別符 ID
	IONAL_IDENTIFICATION_NUMBER, SPAIN_DNI_NUMBER
國民保險號碼 (NINO)	UK_NATIONAL_INSURANCE_NUMBER
護照號碼	CANADA_PASSPORT_NUMBER, FRANCE_PASSPORT_NUMBER, GERMANY_PASSPORT_NUMBER, ITALY_PASSPORT_NUMBER, SPAIN_PASSPORT_NUMBER, UK_PASSPORT_NUMBER, USA_PASSPORT_NUMBER
社會保險號碼 (SIN)	CANADA_SOCIAL_INSURANCE_NUMBER
社會安全號碼 (SSN)	SPAIN_SOCIAL_SECURITY_NUMBER, USA_SOCIAL_SECURITY_NUMBER
納稅識別號碼或參考號碼	AUSTRALIA_TAX_FILE_NUMBER, BRAZIL_CPF_NUMBER, FRANCE_TAX_IDENTIFICATION_NUMBER, GERMANY_TAX_IDENTIFICATION_NUMBER, SPAIN_NIE_NUMBER, SPAIN_NIF_NUMBER, SPAIN_TAX_IDENTIFICATION_NUMBER, USA_INDIVIDUAL_TAX_IDENTIFICATION_NUMBER

更新推薦集

下表說明我們針對敏感資料探索工作建議的一組受管資料識別碼變更。如需有關這些變更的自動警示，請訂閱上的 RSS 摘要馬西文件歷史頁面。

變更	描述	日期
一般可用性	推薦集的初始版本。	2023 年 6 月 27 日

使用亞馬遜 Macie 分析加密的 Amazon S3 對象

當您為您啟用 Amazon Macie 時 AWS 帳戶，Macie 會創建一個服務鏈接角色，該角色授予 Macie 代表您調用 Amazon Simple Storage Service (Amazon S3) 和其他 AWS 服務 所需的許可。服務連結角色可簡化設定程序， AWS 服務 因為您不需要手動新增服務的權限，即可代表您完成動作。若要深入瞭解此類型的角色，請參閱使用AWS Identity and Access Management 者指南中的使用服務連結角色。

Macie 服務連結角色 (`AWSServiceRoleForAmazonMacie`) 的許可政策允許 Macie 執行動作，其中包括擷取 S3 儲存貯體和物件的相關資訊，以及擷取和分析 S3 儲存貯體中的物件。如果您的帳戶是組織的 Macie 管理員帳戶，則該策略也允許 Macie 代表您針對組織中的成員帳戶執行這些動作。

如果 S3 物件已加密，Macie 服務連結角色的許可政策通常會授與 Macie 解密物件所需的許可。但是，這取決於所使用的加密類型。它還可以取決於是否允許 Macie 使用適當的加密密鑰。

主題

Amazon S3 物件的加密選項

Amazon S3 支援 S3 物件的多個加密選項。對於大多數這些選項，Amazon Macie 可以使用您帳戶的 Macie 服務連結角色來解密物件。不過，這取決於用來加密物件的加密類型。

使用 Amazon S3 受管金鑰 (SSE-S3) 的伺服器端加密

如果使用具有 Amazon S3 受管金鑰 (SSE-S3) 的伺服器端加密物件加密，Macie 可以解密該物件。

若要了解此類加密類型，請參閱 Amazon 簡單儲存服務使用者指南中的 Amazon S3 受管金鑰使用伺服器端加密。

伺服器端加密與 AWS KMS keys (DSSE-KMS 和 SSE-KMS)

如果物件使用雙層伺服器端加密或使用 AWS 受管理 AWS KMS key (DSSE-KMS 或 SSE-KMS) 的伺服器端加密，Macie 可以解密該物件。

如果物件使用雙層伺服器端加密或伺服器端加密與客戶管理 AWS KMS key (DSSE-KMS 或 SSE-KMS) 加密，Macie 只有在您允許 Macie 使用金鑰時才能解密物件。對於使用完全在內部管理的 KMS 金鑰 AWS KMS 和外部金鑰存放區中的 KMS 金鑰加密的物件，就是這種情況。如果不允許 Macie 使用適用的 KMS 金鑰，Macie 只能儲存和報告物件的中繼資料。

若要了解這些類型的加密，請參閱 Amazon 簡單儲存服務使用者指南 AWS KMS keys中的使用雙層伺服器端加密 AWS KMS keys和搭配使用伺服器端加密。

> **Tip**
>
> 您可以自動產生 Macie 需要存取的所 AWS KMS keys 有受管客戶清單，以分析您帳戶的 S3 儲存貯體中的物件。若要執行此操作，請執行 AWS KMS 權限分析器指令碼，該指令碼可從 Amazon Macie 指令碼存放庫取 GitHub得。該腳本還可以生成 AWS Command Line Interface (AWS CLI) 命令的其他腳本。您可以選擇性地執行這些命令，為您指定的 KMS 金鑰更新必要的組態設定和原則。

使用客戶提供的金鑰 (SSE-C) 進行伺服器端加密

如果使用伺服器端加密使用客戶提供的金鑰 (SSE-C) 加密物件，Macie 就無法解密該物件。Macie 只能儲存和報告物件的中繼資料。

若要了解此類加密類型，請參閱 Amazon 簡單儲存服務使用者指南中的使用伺服器端加密與客戶提供的金鑰搭配使用。

用戶端加密

如果物件使用用戶端加密加密，Macie 就無法解密該物件。Macie 只能儲存和報告物件的中繼資料。例如，Macie 可以報告物件的大小以及與物件相關聯的標籤。

若要了解 Amazon S3 中的此類加密類型，請參閱 Amazon 簡單儲存服務使用者指南中的使用用戶端加密保護資料。

您可以在 Macie 中篩選儲存貯體庫存，以判斷哪些 S3 儲存貯體存放使用特定類型加密的物件。您也可以決定哪些值區在儲存新物件時，預設會使用特定類型的伺服器端加密。下表提供篩選器範例，您可以套用至儲存貯體庫存以尋找此資訊。

若要顯示值區...	套用此篩選器...
儲存使用 SSE-C 加密的物件	依加密方式的物件計數是由客戶提供，且從 = 1
儲存使用 DSSE-KMS 加密或 SSE-KMS 加密的物件	透過加密AWS KMS 管理的物件計數，且從 = 1

若要顯示值區...	套用此篩選器...
儲存使用 SSE-S3 加密的物件	加密的物件計數是由 Amazon S3 管理的，且從 = 1
儲存使用用戶端加密 (或未加密) 的物件	加密的物件計數為「無加密」，「從」= 1
依預設，使用 DSSE-KMS 加密來加密新物件	預設加密 = AW S: kms: DSE
依預設，使用 SSE-KMS 加密來加密新物件	預設加密 = aw s: 公里
預設情況下，使用 SSE-S3 加密加密新物件	預設加密 = AES256

如果儲存貯體設定為預設使用 DSSE-KMS 或 SSE-KMS 加密來加密新物件，您也可以判斷使用哪一個物件。 AWS KMS key 若要這麼做，請在 S3 儲存貯體頁面上選擇儲存貯體。在值區詳細資料面板的伺服器端加密下，請參閱AWS KMS key欄位。此欄位顯示金鑰的 Amazon 資源名稱 (ARN) 或唯一識別碼 (金鑰 ID)。

允許 Amazon Macie 使用客戶管理 AWS KMS key

如果 Amazon S3 物件使用雙層伺服器端加密或使用客戶受管 AWS KMS key (DSSE-KMS 或 SSE-KMS) 的伺服器端加密，Amazon Macie 只有在允許使用金鑰的情況下才能解密物件。如何提供此存取權取決於擁有金鑰的帳戶是否也擁有存放物件的 S3 儲存貯體：

- 如果相同的帳戶擁有 AWS KMS key 和值區，則該帳戶的使用者必須更新金鑰的政策。
- 如果一個帳戶擁有該帳戶， AWS KMS key 而另一個帳戶擁有該值區，則擁有該金鑰的帳戶的使用者必須允許跨帳戶存取金鑰。

本主題說明如何執行這些工作，並提供兩種案例的範例。若要深入瞭解如何允許存取受管理的客戶 AWS KMS keys，請參閱AWS Key Management Service 開發人員指南 AWS KMS中的驗證和存取控制。

允許相同帳戶存取客戶管理的金鑰

如果同一帳戶同時擁有 S3 儲存貯體，則該帳戶的使用者必須在金鑰的政策中新增陳述式。 AWS KMS key 其他陳述式必須允許帳戶的 Macie 服務連結角色使用金鑰來解密資料。如需更新金鑰原則的詳細資訊，請參閱AWS Key Management Service 開發人員指南中的變更金鑰政策。

在聲明中：

- `Principal`元素必須為擁有 AWS KMS key 和 S3 儲存貯體的帳戶指定 Macie 服務連結角色的 Amazon 資源名稱 (ARN)。

  如果帳戶處於選擇加入 AWS 區域，ARN 還必須包含該地區的適當區域代碼。例如，如果帳戶位於中東 (巴林) 區域，其區域代碼為 me-south-1，則必須指定`Principal``arn:aws:iam::`*123456789012*`:role/aws-service-role/macie.me-south-1.amazonaws.com/AWSServiceRoleForAmazonMacie`元素，其中 *123456789012* 是帳戶的帳戶識別碼。如需目前提供 Macie 的區域的區域代碼清單，請參閱. AWS 一般參考
- `Action`陣列必須指定`kms:Decrypt`動作。這是必須允許 Macie 執行的唯一 AWS KMS 動作，才能解密使用金鑰加密的 S3 物件。

以下是要新增至策略的陳述式範例 AWS KMS key。

```
{
    "Sid": "Allow the Macie service-linked role to use the key",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::123456789012:role/aws-service-role/macie.amazonaws.com/
AWSServiceRoleForAmazonMacie"
    },
    "Action": [
        "kms:Decrypt"
    ],
    "Resource": "*"
}
```

在上述範例中：

- `Principal`元素中的`AWS`欄位會指定帳戶之 Macie 服務連結角色 (`AWSServiceRoleForAmazonMacie`) 的 ARN。它可讓 Macie 服務連結角色執行原則陳述式所指定的動作。 *123456789012* 是一個帳戶識別碼範例。將此值取代為擁有 KMS 金鑰和 S3 儲存貯體之帳戶的帳戶識別碼。
- `Action`陣列會指定允許 Macie 服務連結角色使用 KMS 金鑰執行的動作 — 解密使用金鑰加密的加密文字。

將此陳述式新增至金鑰原則的位置取決於原則目前包含的結構和元素。當您新增陳述式時，請確定語法有效。金鑰政策使用 JSON 格式。這表示您也必須在陳述式之前或之後加上逗號，視您將陳述式新增至原則的位置而定。

允許跨帳戶存取客戶管理的金鑰

如果一個帳戶擁有 AWS KMS key （金鑰擁有者），而另一個帳戶擁有 S3 儲存貯體（儲存貯體擁有者），則金鑰擁有者必須向儲存貯體擁有者提供 KMS 金鑰的跨帳戶存取權。為此，密鑰所有者首先確保密鑰的策略允許存儲桶所有者同時使用密鑰並為密鑰創建授予。然後值區擁有者會建立金鑰的授權。授權是一種原則工具，可讓 AWS 主體在符合授權指定的條件時，在密碼編譯作業中使用 KMS 金鑰。在此情況下，授權會將相關權限委派給值區擁有者帳戶的 Macie 服務連結角色。

如需更新金鑰原則的詳細資訊，請參閱AWS Key Management Service 開發人員指南中的變更金鑰政策。若要進一步了解撥款，請參閱AWS Key Management Service 開發人員指南 AWS KMS中的贈款。

步驟 1：更新金鑰原則

在金鑰原則中，金鑰擁有者應確定原則包含兩個陳述式：

- 第一個陳述式允許儲存貯體擁有者使用金鑰來解密資料。
- 第二個陳述式可讓儲存貯體擁有者為其 (值區擁有者) 帳戶建立 Macie 服務連結角色的授權。

在第一個陳述式中，`Principal`元素必須指定值區擁有者帳戶的 ARN。`Action`陣列必須指定`kms:Decrypt`動作。這是唯一必須允許 Macie 執行的 AWS KMS 動作，才能解密使用金鑰加密的物件。以下是政策中此陳述式的範例 AWS KMS key。

```
{
    "Sid": "Allow account 111122223333 to use the key",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
    },
    "Action": [
        "kms:Decrypt"
    ],
    "Resource": "*"
}
```

在上述範例中：

- `Principal`元素中的`AWS`欄位會指定值區擁有者帳戶的 ARN (*11112* 2223333)。它可讓儲存貯體擁有者執行政策陳述式所指定的動作。 *111122223333* 是一個帳戶識別碼範例。將此值取代為值區擁有者帳戶的帳戶 ID。

- Action陣列指定允許儲存貯體擁有者使用 KMS 金鑰執行的動作 — 解密使用金鑰加密的加密文字。

金鑰政策中的第二個陳述式可讓儲存貯體擁有者為其帳戶建立 Macie 服務連結角色的授權。在此陳述式中，Principal元素必須指定值區擁有者帳戶的 ARN。Action陣列必須指定kms:CreateGrant動作。Condition元素可以篩選對陳述式中指定kms:CreateGrant動作的存取。以下是政策中此陳述式的範例 AWS KMS key。

```
{
    "Sid": "Allow account 111122223333 to create a grant",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
    },
    "Action": [
        "kms:CreateGrant"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:GranteePrincipal": "arn:aws:iam::111122223333:role/aws-service-role/
macie.amazonaws.com/AWSServiceRoleForAmazonMacie"
        }
    }
}
```

在上述範例中：

- Principal元素中的AWS欄位會指定值區擁有者帳戶的 ARN (*11112* 2223333)。它可讓儲存貯體擁有者執行政策陳述式所指定的動作。 *111122223333* 是一個帳戶識別碼範例。將此值取代為值區擁有者帳戶的帳戶 ID。
- Action陣列指定允許儲存貯體擁有者對 KMS 金鑰執行的動作 — 建立金鑰的授權。
- Condition元素會使用StringEquals條件運算子和kms:GranteePrincipal條件索引鍵來篩選對原則陳述式所指定動作的存取。在這種情況下，值區擁有者只能為指定的人建立授權GranteePrincipal，也就是其帳戶之 Macie 服務連結角色的 ARN。在該 ARN 中，*111122223333* 是一個示例帳戶識別碼。將此值取代為值區擁有者帳戶的帳戶 ID。

  如果值區擁有者的帳戶屬於選擇加入 AWS 區域，請同時在 Macie 服務連結角色的 ARN 中加入適當的區域代碼。例如，如果帳戶位於中東 (巴林) 區域，其區域代碼為 me-south-1，請macie.me-

south-1.amazonaws.com在 ARN 中取macie.amazonaws.com代。如需目前提供 Macie 的區域的區域代碼清單，請參閱. AWS 一般參考

索引鍵擁有者將這些陳述式新增至金鑰原則的位置取決於原則目前包含的結構和元素。當密鑰所有者添加語句時，他們應該確保語法有效。金鑰政策使用 JSON 格式。這表示金鑰擁有者也必須在每個陳述式之前或之後加上逗號，視使用者將陳述式新增至原則的位置而定。

步驟 2：建立授權

在金鑰擁有者視需要更新金鑰政策之後，值區擁有者必須為金鑰建立授權。授權會將相關權限委派給其 (值區擁有者) 帳戶的 Macie 服務連結角色。值區擁有者建立授權之前，應先確認自己是否有權針對其帳戶執行kms:CreateGrant動作。此動作可讓他們將授權新增至現有、受管理的客戶 AWS KMS key。

若要建立授權，值區擁有者可以使用 AWS Key Management Service API 的CreateGrant作業。值區擁有者建立授權時，應為必要參數指定下列值：

- KeyId— KMS 金鑰的 ARN。若要跨帳戶存取 KMS 金鑰，此值必須是 ARN。它不能是金鑰識別碼。
- GranteePrincipal— 其帳戶的 Macie 服務連結角色 (AWSServiceRoleForAmazonMacie) 的 ARN。這個值應該是arn:aws:iam::*111122223333*:role/aws-service-role/macie.amazonaws.com/AWSServiceRoleForAmazonMacie，其中 *111122223333* 是值區擁有者帳戶的帳戶識別碼。

  如果他們的帳戶位於選擇加入的地區，ARN 必須包含適當的區域代碼。例如，如果他們的帳戶位於中東 (巴林) 區域，其區域代碼為 me-south-1，則 ARN 應該arn:aws:iam::*111122223333*:role/aws-service-role/macie.me-south-1.amazonaws.com/AWSServiceRoleForAmazonMacie是，其中 *111122223333* 是值區擁有者帳戶的帳戶識別碼。
- Operations— 解 AWS KMS 密動作 (Decrypt)。這是唯一必須允許 Macie 執行的 AWS KMS 動作，才能解密使用 KMS 金鑰加密的物件。

若要使用 AWS Command Line Interface (AWS CLI) 為客戶管理的 KMS 金鑰建立授權，請執行建立授與命令。下列範例會顯示作法。此範例已針對 Microsoft Windows 進行格式化，並使用脫字元 (^) 行接續字元來提高可讀性。

```
C:\> aws kms create-grant ^
--key-id arn:aws:kms:us-east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab ^
```

```
--grantee-principal arn:aws:iam::111122223333:role/aws-service-role/
macie.amazonaws.com/AWSServiceRoleForAmazonMacie ^
--operations "Decrypt"
```

其中：

- `key-id`指定要套用授權之 KMS 金鑰的 ARN。
- `grantee-principal`針對允許執行授權所指定動作的帳戶，指定 Macie 服務連結角色的 ARN。這個值應該符合金鑰原則中第二個陳述式`kms:GranteePrincipal`條件所指定的 ARN。
- `operations`指定授與允許指定主體執行的動作 — 解密使用 KMS 金鑰加密的加密文字。

如果此命令成功執行，您會收到類似如下的輸出。

```
{
    "GrantToken": "<grant token>",
    "GrantId": "1a2b3c4d2f5e69f440bae30eaec9570bb1fb7358824f9ddfa1aa5a0dab1a59b2"
}
```

其中`GrantToken`是唯一、非秘密、可變長度、base64 編碼的字串，代表已建立的授權，並且`GrantId`是授權的唯一識別碼。

使用 Amazon Macie 儲存和保留敏感資料探索結果

當您執行敏感資料探索任務或 Amazon Macie 執行自動化敏感資料探索時，Macie 會為分析範圍中包含的每個 Amazon 簡單儲存服務 (Amazon S3) 物件建立分析記錄。這些記錄稱為敏感資料探索結果，記錄 Macie 在個別 S3 物件上執行之分析的詳細資料。這包括 Macie 無法在其中偵測敏感資料，因此不會產生發現項目的物件，以及 Macie 因錯誤或問題而無法分析的物件。如果 Macie 偵測到物件中的敏感資料，則記錄會包含來自對應發現項目的資料以及其他資訊。敏感資料探索結果為您提供分析記錄，這些記錄對於資料隱私權和保護稽核或調查有幫助。

Macie 只會儲存您的敏感資料探索結果 90 天。若要存取結果並啟用長期儲存和保留結果，請將 Macie 設定為使用 AWS Key Management Service (AWS KMS) 金鑰加密結果，並將其存放在 S3 儲存貯體中。儲存貯體可作為所有敏感資料探索結果的明確長期存放庫。然後，您可以選擇性地存取和查詢該儲存庫中的結果。

本主題將引導您完成使用 AWS Management Console 來設定敏感資料探查結果存放庫的程序。組態是加密結果的組 AWS KMS key 合、儲存結果的 S3 一般用途儲存貯體，以及指出要使用哪個金鑰和儲

存貯體的 Macie 設定的組合。如果您偏好以程式設計方式設定 Macie 設定，可以使用 Amazon Macie API 的PutClassificationExportConfiguration操作。

當您在 Macie 中設定設定時，您的選擇只會套用至目前 AWS 區域的。如果您是組織的 Macie 管理員，您的選擇僅適用於您的帳戶。它們不適用於任何關聯的成員帳戶。

如果您使用多個 Macie AWS 區域，請為您使用 Macie 的每個區域設定儲存庫設定。您可以選擇性地將多個區域的敏感資料探索結果存放在同一 S3 儲存貯體中。但是，請注意以下要求：

- 若要儲存預設 AWS 啟用的區域 (例如美國東部 (維吉尼亞北部) 區域的結果，您必須在預設啟用的區域中選擇值區。 AWS 帳戶結果無法儲存在選擇加入區域的值區中 (預設為停用的區域)。
- 若要儲存選擇加入區域的結果，例如中東 (巴林) 區域，您必須選擇相同區域中的值區或預設啟用的區域。結果無法儲存在不同選擇加入區域的值區中。

若要確定某個區域是否預設為啟用，請參閱《AWS Identity and Access Management 使用手冊》中的「地區和端點」。除了上述要求之外，還要考慮是否要擷取 Macie 在個別發現項目中報告的敏感資料樣本。若要從受影響的 S3 物件擷取敏感資料樣本，下列所有資源和資料必須儲存在相同的區域：受影響的物件、適用的發現項目，以及對應的敏感資料探索結果。

任務

- 概觀
- 步驟 1：驗證您的權限
- 步驟 2：設定 AWS KMS key
- 步驟 3：選擇 S3 儲存貯體

概觀

Amazon Macie 會自動為每個 Amazon S3 物件建立敏感資料探索結果，這些物件會在您執行敏感資料探索任務或執行自動化敏感資料探索時進行分析或嘗試分析的每個 Amazon S3 物件。其中包含：

- Macie 偵測到敏感資料的物件，因此也會產生敏感資料發現項目。
- Macie 未偵測敏感資料的物件，因此不會產生敏感資料發現項目。
- Macie 因權限設定或使用不支援的檔案或儲存格式等錯誤或問題而無法分析的物件。

如果 Macie 偵測到 S3 物件中的敏感資料，敏感資料探索結果會包含來自對應敏感資料發現的資料。它也會提供其他資訊，例如 Macie 在物件中找到的每種敏感資料類型多達 1,000 次出現的位置。例如：

- 在 Microsoft Excel 活頁簿、CSV 檔案或 TSV 檔案中的儲存格或欄位的欄和列號
- JSON 或 JSON 行檔案中欄位或陣列的路徑
- CSV、JSON、JSON 行或 TSV 檔案以外的非二進位文字檔案中的行號，例如 HTML、TXT 或 XML 檔案
- Adobe 可攜式文件格式 (PDF) 檔案中頁面的頁碼
- 記錄索引和路徑在一個 Apache 的 Avro 對象容器或 Apache 實木複合地板文件中的記錄字段

如果受影響的 S3 物件是封存檔案 (例如 .tar 或 .zip 檔案)，敏感資料探索結果也會針對 Macie 從封存中擷取的個別檔案中出現的敏感資料提供詳細位置資料。Macie 不會在封存檔案的敏感資料發現項目中包含此資訊。若要報告位置資料，敏感資料探索結果會使用標準化的 JSON 結構定義。

敏感資料探索結果不包含 Macie 找到的敏感資料。相反，它提供了一個分析記錄，可以幫助您進行審核或調查。

Macie 會將您的敏感資料探索結果儲存 90 天。您無法直接在 Amazon Macie 控制台或使用 Amazon Macie API 訪問它們。請改為遵循本主題中的步驟，將 Macie 設定為使用您指定的加密結果，並將結果存放在您也指定的 S3 一般用途儲存貯體中。 AWS KMS key 然後，Macie 會將結果寫入 JSON 行 (.jsonl) 檔案，將檔案新增至值區做為 GNU Zip (.gz) 檔案，並使用 SSE-KMS 加密來加密資料。自 2023 年 11 月 8 日起，Macie 也會使用雜湊型訊息驗證碼 (HMAC) 來簽署產生的 S3 物件。 AWS KMS key

將 Macie 設定為將敏感資料探索結果存放在 S3 儲存貯體之後，儲存貯體可做為結果的確定長期存放庫。然後，您可以選擇性地存取和查詢該儲存庫中的結果。

> **Tip**
>
> 有關如何查詢和使用敏感資料探索結果來分析和報告潛在資料安全風險的詳細說明範例，請參閱安全部落格上的如何使用 Amazon Athena 和 Amazon QuickSight 部落格文章查詢和視覺化 Macie 敏感資料探索結果。AWS
> 如需可用來分析敏感資料探索結果的 Amazon Athena 查詢範例，請造訪上 GitHub的 Amazon Macie 結果分析儲存庫。此儲存庫也提供設定 Athena 擷取和解密結果的指示，以及建立結果表格的指令碼。

步驟 1：驗證您的權限

在為敏感性資料探索結果設定存放庫之前，請確認您具有加密和儲存結果所需的權限。若要驗證您的許可，請使用 AWS Identity and Access Management (IAM) 檢閱附加到 IAM 身分的 IAM 政策。然後將這些原則中的資訊與下列動作清單進行比較，您必須執行這些動作才能設定存放庫。

Amazon Macie

若為 Macie，請確認您已被允許執行下列動作：

`macie2:PutClassificationExportConfiguration`

此動作可讓您在 Macie 中新增或變更存放庫設定。

Amazon Simple Storage Service (Amazon S3)

對於 Amazon S3，請確認您是否允許執行下列動作：

- `s3:CreateBucket`
- `s3:GetBucketLocation`
- `s3:ListAllMyBuckets`
- `s3:PutBucketAcl`
- `s3:PutBucketPolicy`
- `s3:PutBucketPublicAccessBlock`
- `s3:PutObject`

這些動作可讓您存取和設定可做為存放庫的 S3 一般用途儲存貯體。

AWS KMS

若要使用 Amazon Macie 主控台新增或變更儲存庫設定，請確認您可以執行下列 AWS KMS 動作：

- `kms:DescribeKey`
- `kms:ListAliases`

這些動作可讓您擷取和顯示您帳戶 AWS KMS keys 的相關資訊。然後，您可以選擇其中一個金鑰來加密敏感資料探索結果。

如果您計劃建立新資料 AWS KMS key 來加密資料，您還需要被允許執行下列動作：`kms:CreateKey`、`kms:GetKeyPolicy`和`kms:PutKeyPolicy`。

如果您無法執行必要的動作，請先向 AWS 管理員尋求協助，然後再繼續進行下一個步驟。

步驟 2：設定 AWS KMS key

驗證您的權限後，請決定 AWS KMS key 您希望 Macie 使用哪一個來加密您的敏感資料探索結果。金鑰必須是客戶管理的對稱加密 KMS 金鑰，與您要存放結果的 S3 儲存貯體相同 AWS 區域 。

該密鑰可以是您自己帳戶 AWS KMS key 中的現有密鑰，也可以 AWS KMS key 是另一個帳戶擁有的現有密鑰。如果您想要使用新的 KMS 金鑰，請先建立金鑰，然後再繼續。如果您想要使用其他帳戶擁有的現有金鑰，請取得該金鑰的 Amazon 資源名稱 (ARN)。當您在 Macie 中設定儲存庫設定時，您需要輸入此 ARN。如需建立和檢閱 KMS 金鑰設定的詳細資訊，請參閱AWS Key Management Service 開發人員指南中的管理金鑰。

> **Note**
>
> 金鑰可以是外部金鑰存放區 AWS KMS key 中的金鑰。但是，與完全在其中管理的密鑰相比，密鑰可能會慢且不太可靠 AWS KMS。您可以將敏感資料探索存放在設定為使用金鑰做為 S3 儲存貯體金鑰的 S3 儲存貯體，藉此降低此風險。這樣可以減少加密敏感資料探索結果所必須提出的 AWS KMS 要求數量。
>
> 如需在外部金鑰存放區使用 KMS 金鑰的詳細資訊，請參閱AWS Key Management Service 開發人員指南中的外部金鑰存放區。如需使用 S3 儲存貯體金鑰的相關資訊，請參閱 Amazon 簡單儲存服務使用者指南中的使用 Amazon S3 儲存貯體金鑰降低 SSE-KMS 的成本。

在您決定要 Macie 使用哪個 KMS 金鑰之後，請授與 Macie 使用金鑰的權限。否則，Macie 將無法在存儲庫中加密或存儲您的結果。若要授予 Macie 使用金鑰的權限，請更新金鑰的金鑰原則。如需有關金鑰原則和管理 KMS 金鑰存取權的詳細資訊，請參閱AWS Key Management Service 開發人員指南 AWS KMS中的金鑰政策。

若要更新金鑰原則

1. 請在以下位置開啟 AWS KMS 主控台。 https://console.aws.amazon.com/kms
2. 若要變更 AWS 區域，請使用頁面右上角的「地區」選取器。
3. 選擇您希望 Macie 用來加密敏感資料探索結果的金鑰。
4. 在金鑰原則索引標籤上，選擇編輯。
5. 將下列陳述式複製到剪貼簿，然後將其新增至原則：

```
{
    "Sid": "Allow Macie to use the key",
    "Effect": "Allow",
```

```
    "Principal": {
        "Service": "macie.amazonaws.com"
    },
    "Action": [
        "kms:GenerateDataKey",
        "kms:Encrypt"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "111122223333"
         },
         "ArnLike": {
             "aws:SourceArn": [
                 "arn:aws:macie2:Region:111122223333:export-configuration:*",
                 "arn:aws:macie2:Region:111122223333:classification-job/*"
             ]
         }
    }
}
```

> **Note**
>
> 當您將陳述式新增至政策時，請確定語法有效。策略使用 JSON 格式。這表示您也需要在陳述式之前或之後加上逗號，視您將陳述式新增至原則的位置而定。如果您將陳述式新增為最後一個陳述式，請在前述陳述式的右大括號後加上逗號。如果您將它新增為第一個陳述式或兩個現有陳述式之間，請在陳述式的右大括號後加上逗號。

6. 使用適合您環境的正確值更新陳述式：

   - 在Condition欄位中，取代預留位置值，其中：
     - *111122223333* 是您的帳戶識別碼。 AWS 帳戶
     - *##*是您正 AWS 區域 在使用 Macie 的，您希望允許 Macie 使用密鑰。

     如果您在多個區域中使用 Macie，並希望允許 Macie 在其他區域中使用密鑰，請為每個額外的區域添加aws:SourceArn條件。例如：

     ```
     "aws:SourceArn": [
         "arn:aws:macie2:us-east-1:111122223333:export-configuration:*",
         "arn:aws:macie2:us-east-1:111122223333:classification-job/*",
         "arn:aws:macie2:us-west-2:111122223333:export-configuration:*",
     ```

```
    "arn:aws:macie2:us-west-2:111122223333:classification-job/*"
]
```

或者，您也可以允許 Macie 在所有區域中使用金鑰。若要這麼做，請以萬用字元 (*) 取代預留位置值。例如：

```
"aws:SourceArn": [
    "arn:aws:macie2:*:111122223333:export-configuration:*",
    "arn:aws:macie2:*:111122223333:classification-job/*"
]
```

- 如果您在選擇加入的區域中使用 Macie，請將適當的區域代碼新增至欄位的`Service`值。例如，如果您在中東 (巴林) 區域中使用 Macie，其中的區域代碼為 me-south-1，請取代為. `macie.amazonaws.com` `macie.me-south-1.amazonaws.com` 如需目前可使用 Macie 的區域清單以及每個區域的 Amazon Macie 域代碼，請參閱. AWS 一般參考

請注意，這些`Condition`欄位使用兩個 IAM 全域條件金鑰：

- aws：SourceAccount— 此條件允許 Macie 僅針對您的帳戶執行指定的操作。更具體地說，它決定哪個帳戶可以針對`aws:SourceArn`條件指定的資源和動作執行指定的動作。

  若要允許 Macie 針對其他帳號執行指定的動作，請將每個額外帳戶的帳號 ID 新增至此條件。例如：

  ```
  "aws:SourceAccount": [111122223333,444455556666]
  ```

- aws：SourceArn-此條件可防 AWS 服務 止其他人執行指定的操作。它還可以防止 Macie 在為您的帳戶執行其他操作時使用密鑰。換句話說，只有在以下情況下，才允許 Macie 使用金鑰加密 S3 物件：物件為敏感資料探索結果，而結果是針對由指定區域中指定帳戶建立的自動化敏感資料探索或敏感資料探索任務。

  若要允許 Macie 針對其他帳號執行指定的動作，請將每個額外帳號的 ARN 新增至此條件。例如：

  ```
  "aws:SourceArn": [
      "arn:aws:macie2:us-east-1:111122223333:export-configuration:*",
      "arn:aws:macie2:us-east-1:111122223333:classification-job/*",
      "arn:aws:macie2:us-east-1:444455556666:export-configuration:*",
      "arn:aws:macie2:us-east-1:444455556666:classification-job/*"
  ```

```
]
```

`aws:SourceAccount`和`aws:SourceArn`條件所指定的帳戶應該符合。

這些條件有助於防止 Macie 在與 AWS KMS交易過程中被用作混淆的副手。雖然我們不建議這樣做，但您可以從陳述式中移除這些條件。

7. 當您完成新增和更新陳述式時，請選擇 [儲存變更]。

步驟 3：選擇 S3 儲存貯體

驗證許可並設定後 AWS KMS key，即可指定要用作敏感資料探索結果的存放庫的 S3 儲存貯體。您有兩種選擇：

- 使用 Macie 建立的新 S3 儲存貯體 — 如果您選擇此選項，Macie 會自動在目前的目前 AWS 區域 為您的探索結果建立新的 S3 通用儲存貯體。Macie 也會將值區政策套用至值區。此政策允許 Macie 將物件新增至值區。它還需要使用 SSE-KMS 加密，使 AWS KMS key 用您指定的對象進行加密。若要檢閱政策，請在指定儲存貯體的名稱和要使用的 KMS 金鑰後，在 Amazon Macie 主控台上選擇「檢視政策」。
- 使用您建立的現有 S3 儲存貯體 — 如果您偏好將探索結果存放在您建立的特定 S3 儲存貯體中，請在繼續之前建立儲存貯體。該桶必須是一個通用的存儲桶。此外，值區的設定和政策必須允許 Macie 將物件新增至值區。本主題說明要檢查的設定以及如何更新原則。它也提供要新增至原則的陳述式範例。

以下各節提供每個選項的指示。選擇所需選項的區段。

使用馬西創建的新 S3 存儲桶

如果您偏好使用 Macie 為您建立的新 S3 儲存貯體，程序的最後一個步驟是在 Macie 中設定儲存庫設定。

若要在 Macie 中設定儲存庫設定

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 在功能窗格的 [設定] 下，選擇 [探索結果]。
3. 在敏感資料探索結果的儲存庫下，選擇 [建立值區]。
4. 在「建立值區」方塊中，輸入值區的名稱。

該名稱在所有 S3 儲存貯體中必須是唯一的。此外，名稱只能由小寫字母、數字、點 (.) 和連字號 (-) 組成。如需其他命名需求，請參閱 Amazon 簡單儲存服務使用者指南中的儲存貯體命名規則。

5. 展開 Advanced (進階) 區段。
6. (選擇性) 若要指定值區中某個位置的路徑中要使用的前置詞，請在資料探索結果前置詞方塊中輸入前置詞。

   當您輸入值時，Macie 會更新方塊下方的範例，以顯示儲存探索結果的值區位置路徑。
7. 在 [封鎖所有公開存取] 中，選擇 [是] 以啟用值區的所有封鎖公開存取設定。

   如需這些設定的相關資訊，請參閱 Amazon 簡單儲存服務使用者指南中的封鎖對 Amazon S3 儲存的公開存取。
8. 在「加密設定」下，指 AWS KMS key 定您希望 Macie 用來加密結果的項目：

   - 若要使用您自己帳戶中的金鑰，請選擇 [從您的帳戶選取金鑰]。然後，在AWS KMS key清單中選擇要使用的金鑰。此清單會顯示您帳戶的客戶管理、對稱加密 KMS 金鑰。
   - 若要使用其他帳號擁有的金鑰，請選擇 [輸入其他帳號金鑰的 ARN]。然後，在 AWS KMS key ARN 方塊中，輸入要使用的金鑰的 Amazon 資源名稱 (ARN)，例如。**`arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`**
9. 完成輸入設定後，請選擇 [儲存]。

   Macie 會測試設定以確認設定是否正確。如果有任何設定不正確，Macie 會顯示錯誤訊息來協助您解決問題。

儲存存放庫設定後，Macie 會將過去 90 天的現有探查結果新增至存放庫。Macie 也開始將新的探索結果新增至儲存庫。

使用您建立的現有 S3 儲存貯體

如果您偏好將敏感資料探索存放在您建立的特定 S3 儲存貯體中，請先建立並設定儲存貯體，然後再在 Macie 中設定設定。建立值區時，請注意下列需求：

- 該桶必須是一個通用的存儲桶。它不能是目錄存儲桶。
- 如果您啟用值區的物件鎖定，就必須停用該功能的預設保留設定。否則，Macie 將無法將您的探索結果新增至值區。如需此設定的相關資訊，請參閱 Amazon 簡單儲存服務使用者指南中的使用 S3 物件鎖定。

- 若要將探索結果儲存在預設為啟用的區域 (例如美國東部 (維吉尼亞北部) 區域，值區必須位於 AWS 帳戶預設為啟用的區域中。結果無法儲存在選擇加入區域的值區中 (預設為停用的區域)。
- 若要儲存選擇加入區域的探索結果，例如中東 (巴林) 區域，值區必須位於預設啟用的相同區域或區域。結果無法儲存在不同選擇加入區域的值區中。

若要確定某個區域是否預設為啟用，請參閱《AWS Identity and Access Management 使用手冊》中的「地區和端點」。

建立值區之後，請更新值區的政策，以允許 Macie 擷取值區的相關資訊，並將物件新增至值區。然後，您可以在 Macie 中配置設置。

若要更新值區的值區政策

1. 前往 https://console.aws.amazon.com/s3/ 開啟的 Amazon Simple Storage Service (Amazon S3) 主控台。
2. 選擇您要儲存探索結果的儲存貯體。
3. 選擇許可索引標籤標籤。
4. 在儲存貯體政策區段中，選擇編輯。
5. 將下列範例原則複製到剪貼簿：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow Macie to use the GetBucketLocation operation",
            "Effect": "Allow",
            "Principal": {
                "Service": "macie.amazonaws.com"
            },
            "Action": "s3:GetBucketLocation",
            "Resource": "arn:aws:s3:::myBucketName",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333"
                },
                "ArnLike": {
                    "aws:SourceArn": [
                        "arn:aws:macie2:Region:111122223333:export-
configuration:*",
                        "arn:aws:macie2:Region:111122223333:classification-job/*"
```

```
                    ]
                }
            }
        },
        {
            "Sid": "Allow Macie to add objects to the bucket",
            "Effect": "Allow",
            "Principal": {
                "Service": "macie.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::myBucketName/[optional prefix/]*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333"
                },
                "ArnLike": {
                    "aws:SourceArn": [
                        "arn:aws:macie2:Region:111122223333:export-
configuration:*",
                        "arn:aws:macie2:Region:111122223333:classification-job/*"
                    ]
                }
            }
        },
        {
            "Sid": "Deny unencrypted object uploads. This is optional",
            "Effect": "Deny",
            "Principal": {
                "Service": "macie.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::myBucketName/[optional prefix/]*",
            "Condition": {
                "StringNotEquals": {
                    "s3:x-amz-server-side-encryption": "aws:kms"
                }
            }
        },
        {
            "Sid": "Deny incorrect encryption headers. This is optional",
            "Effect": "Deny",
            "Principal": {
                "Service": "macie.amazonaws.com"
```

```
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::myBucketName/[optional prefix/]*",
            "Condition": {
                "StringNotEquals": {
                    "s3:x-amz-server-side-encryption-aws-kms-key-id":
 "arn:aws:kms:Region:111122223333:key/KMSKeyId"
                }
            }
        },
        {
            "Sid": "Deny non-HTTPS access",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": "arn:aws:s3:::myBucketName/*",
            "Condition": {
                "Bool": {
                    "aws:SecureTransport": "false"
                }
            }
        }
    ]
}
```

6. 將範例政策貼到 Amazon S3 主控台的儲存貯體政策編輯器中。
7. 使用適用於您環境的正確值更新範例原則：

   - 在拒絕不正確加密標頭的可選語句中：
     - *myBucketName*以值區的名稱取代。
     - 在此StringNotEquals情況下，請將 *ARN: AWS: KMS: ##:1111223333:##/###### Amazon #### (ARN)#######KeyId*索結果。 AWS KMS key
   - 在所有其他語句中，替換佔位符值，其中：
     - *myBucketName*是值區的名稱。
     - *111122223333* 是您的帳戶識別碼。 AWS 帳戶
     - *##*是您正 AWS 區域 在使用 Macie 的位置，並希望允許 Macie 將發現結果添加到存儲桶。

       如果您在多個區域中使用 Macie，並且想要允許 Macie 將結果新增至其他區域的值區，請為每個額外的區域新增aws:SourceArn條件。例如：

```
"aws:SourceArn": [
    "arn:aws:macie2:us-east-1:111122223333:export-configuration:*",
    "arn:aws:macie2:us-east-1:111122223333:classification-job/*",
    "arn:aws:macie2:us-west-2:111122223333:export-configuration:*",
    "arn:aws:macie2:us-west-2:111122223333:classification-job/*"
]
```

或者，您也可以允許 Macie 將結果新增至您使用 Macie 的所有區域的值區。若要這麼做，請以萬用字元 (*) 取代預留位置值。例如：

```
"aws:SourceArn": [
    "arn:aws:macie2:*:111122223333:export-configuration:*",
    "arn:aws:macie2:*:111122223333:classification-job/*"
]
```

- 如果您在選擇加入的區域中使用 Macie，請在每個指定 Macie 服務主體的陳述式中，將適當的區域代碼新增至`Service`欄位值。例如，如果您在中東 (巴林) 區域中使用 Macie，而該區域的區域代碼為 me-south-1，請`macie.me-south-1.amazonaws.com`在每個適用的陳述式中取`macie.amazonaws.com`代為。如需目前可使用 Macie 的區域清單以及每個區域的 Amazon Macie 域代碼，請參閱. AWS 一般參考

請注意，範例政策包含的陳述式可讓 Macie 判斷值區所在的區域 (`GetBucketLocation`)，並將物件新增至值區 (`PutObject`)。這些陳述式定義使用兩個 IAM 全域條件金鑰的條件：

- aws：SourceAccount— 此條件允許 Macie 僅為您的帳戶將敏感數據發現結果添加到存儲桶中。它可以防止 Macie 將其他帳戶的探索結果新增至值區。更具體地說，條件會指定哪個帳戶可以針對條`aws:SourceArn`件指定的資源和動作使用值區。

  若要將其他帳戶的結果儲存在值區中，請將每個額外帳戶的帳戶 ID 新增至此條件。例如：

  ```
  "aws:SourceAccount": [111122223333,444455556666]
  ```

- aws：SourceArn— 此條件會根據要添加到存儲桶的對象的來源限制對存儲桶的訪問。它可以防 AWS 服務 止其他人將物件新增至值區。它也可以防止 Macie 在為您的帳戶執行其他動作時將物件新增至值區。更具體地說，只有在以下情況下，此條件才允許 Macie 將物件新增至值區：物件為敏感資料探索結果，且結果適用於指定區域中指定帳戶所建立的自動化敏感資料探索或敏感資料探索工作。

若要允許 Macie 針對其他帳號執行指定的動作，請將每個額外帳號的 ARN 新增至此條件。例如：

```
"aws:SourceArn": [
    "arn:aws:macie2:us-east-1:111122223333:export-configuration:*",
    "arn:aws:macie2:us-east-1:111122223333:classification-job/*",
    "arn:aws:macie2:us-east-1:444455556666:export-configuration:*",
    "arn:aws:macie2:us-east-1:444455556666:classification-job/*"
]
```

`aws:SourceAccount`和`aws:SourceArn`條件所指定的帳戶應該符合。

這兩種情況都有助於防止 Macie 在與 Amazon S3 進行交易時被用作混淆的副手。雖然我們不建議這樣做，但您可以從值區政策中移除這些條件。

8. 完成值區政策更新後，請選擇 [儲存變更]。

現在，您可以在 Macie 中配置存儲庫設置。

若要在 Macie 中設定儲存庫設定

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 在功能窗格的 [設定] 下，選擇 [探索結果]。
3. 在敏感資料探索結果的儲存庫下，選擇現有儲存貯體。
4. 針對 [選擇值區]，選取您要儲存探索結果的儲存貯體。
5. (選擇性) 若要指定值區中某個位置的路徑中要使用的前置詞，請展開「進階」區段。然後，對於資料探索結果前置詞，輸入要使用的前置詞。

   當您輸入值時，Macie 會更新方塊下方的範例，以顯示儲存探索結果的值區位置路徑。
6. 在「加密設定」下，指 AWS KMS key 定您希望 Macie 用來加密結果的項目：

   - 若要使用您自己帳戶中的金鑰，請選擇 [從您的帳戶選取金鑰]。然後，在AWS KMS key清單中選擇要使用的金鑰。此清單會顯示您帳戶的客戶管理、對稱加密 KMS 金鑰。
   - 若要使用其他帳號擁有的金鑰，請選擇 [輸入其他帳號金鑰的 ARN]。然後，在 AWS KMS key ARN 方塊中，輸入要使用的金鑰的 ARN，例如。**`arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`**
7. 完成輸入設定後，請選擇 [儲存]。

Macie 會測試設定以確認設定是否正確。如果有任何設定不正確，Macie 會顯示錯誤訊息來協助您解決問題。

儲存存放庫設定後，Macie 會將過去 90 天的現有探查結果新增至存放庫。Macie 也開始將新的探索結果新增至儲存庫。

> **Note**
>
> 如果您隨後變更資料探索結果前置詞設定，請同時更新 Amazon S3 中的儲存貯體政策。指定先前路徑的原則陳述式必須指定新路徑。否則，Macie 將不允許將您的探索結果新增至值區。

> **Tip**
>
> 若要降低伺服器端加密成本，請同時將 S3 儲存貯體設定為使用 S3 儲存貯體金鑰，並指 AWS KMS key 定您針對敏感資料探索結果加密所設定的金鑰。使用 S3 儲存貯體金鑰可減少呼叫次數 AWS KMS，進而降低 AWS KMS 請求成本。如果 KMS 金鑰位於外部金鑰存放區中，使用 S3 儲存貯體金鑰也可以將使用金鑰的效能影響降到最低。若要進一步了解，請參閱 Amazon 簡單儲存服務使用者指南中的使用 Amazon S3 儲存貯體金鑰降低 SSE-KMS 的成本。

Amazon Macie 支援的儲存類別和格式

為了協助您發現 Amazon Simple Storage Service (Amazon S3) 資料資產中的敏感資料，Amazon Macie 支援大多數 Amazon S3 儲存類別以及各種檔案和儲存格式。此支援適用於使用受管資料識別碼，以及使用自訂資料識別碼來分析 S3 物件。

若要讓 Macie 分析 S3 物件，物件必須使用支援的儲存類別存放在 Amazon S3 一般用途儲存貯體中。物件也必須使用支援的檔案或儲存格式。本節中的主題列出了 Macie 目前支援的儲存空間類別以及檔案和儲存格式。

> **Tip**
>
> 雖然 Macie 已針對 Amazon S3 進行了最佳化，但您可以使用它來探索目前存放在其他地方的資源中的敏感資料。您可以暫時或永久地將資料移至 Amazon S3 來執行此操作。例如，將 Amazon Relational Database Service 服務或 Amazon Aurora 快照以 Apache 實木複合格式匯

出到 Amazon S3。或將亞馬遜動態資料表匯出至 Amazon S3。然後，您可以建立敏感資料探索任務來分析 Amazon S3 中的資料。

主題

支援的 Amazon S3 儲存類別

針對敏感資料探索，Amazon Macie 支援下列 Amazon S3 儲存類別：

- 低冗餘 (RRS)
- S3 Glacier Instant Retrieval
- S3 智慧型分層
- S3 單區不常存取 (S3 單區域 — IA)
- S3 Standard
- S3 標準 — 不常存取 (S3 標準 — IA)

Macie 不會分析使用其他 Amazon S3 儲存類別的 S3 物件，例如 S3 Glacier Deep Archive 或 S3 快速單區域。此外，Macie 不會分析存放在 S3 目錄儲存貯體中的物件。

如果您設定敏感資料探索任務來分析不使用受支援的 Amazon S3 儲存類別的 S3 物件，Macie 會在任務執行時略過這些物件。Macie 不會嘗試擷取或分析物件中的資料，物件會被視為未分類的物件。未分類的物件是不使用支援的儲存類別或支援的檔案或儲存格式的物件。Macie 只會分析那些使用支援儲存空間類別和支援的檔案或儲存格式的物件。

同樣地，如果您將 Macie 設定為執行自動化敏感資料探索，則無法分類的物件也無法進行選取和分析。Macie 只會選取使用支援的 Amazon S3 儲存類別和受支援的檔案或儲存格式的物件。

若要識別存放未分類物件的 S3 儲存貯體，您可以篩選 S3 儲存貯體庫存。對於詳細目錄中的每個值區，都有一些欄位會報告值區中未分類物件的數量和總儲存大小。

如需 Amazon S3 提供的儲存類別的詳細資訊，請參閱 Amazon 簡單儲存服務使用者指南中的使用 Amazon S3 儲存類別。

支援的檔案和儲存格式

當 Amazon Macie 分析 S3 物件時，Macie 會從 Amazon S3 擷取物件的最新版本，然後對物件的內容執行深入檢查。此檢查會考量資料的檔案或儲存格式。Macie 可以分析許多不同格式的數據，包括常用的壓縮和存檔格式。

當 Macie 分析壓縮檔案或封存檔案中的資料時，Macie 會檢查完整檔案和檔案內容。為了檢查檔案的內容，Macie 會將檔案解壓縮，然後檢查每個使用支援格式的解壓縮檔案。Macie 可以為多達 1,000,000 個文件和 10 個級別的嵌套深度執行此操作。如需適用於敏感資料探索之其他配額的相關資訊，請參閱Amazon Macie 配額。

下表列出並說明 Macie 可分析以偵測敏感資料的檔案類型和儲存格式。對於每個支援的類型，表格也會列出適用的副檔名。

檔案或儲存類型	描述	副檔名
大數據	阿帕奇阿夫羅對象容器和阿帕奇拼花文件	. 阿夫羅,. 鑲木地板
壓縮或存檔	GNU 郵編壓縮檔案，TAR 壓縮檔案和 ZIP 壓縮存檔	.gz,. gzip,. 焦油,. 拉鍊
文件	Adobe 可移植文檔格式文件，Microsoft Excel 工作簿和 Microsoft Word 文檔	. 文件, .docx, .pdf, .xls,
電子郵件	其內容符合 IETF RFC 針對電子郵件訊息所指定之要求的電子郵件檔案，例如 RFC 2822	. 歐姆爾
文字	非二進位文字檔案，例如逗號分隔值 (CSV) 檔案、超文字標記語言 (HTML) 檔案、JavaScript 物件標記 (JSON) 檔案、JSON 行檔案、純文字文件、定位點分隔值 (TSV) 檔案，以及可延伸標記語言 (XML) 檔案	.csv、.htm、.html、.json、.jsonl、.tsv、.txt、.xml 等 (取決於非二進位文字檔案的類型)

Macie 不會分析影像中的資料，也不會分析音訊、視訊和其他類型的多媒體內容。

如果您將敏感資料探索工作設定為分析不使用支援檔案或儲存格式的 S3 物件，Macie 會在任務執行時略過這些物件。Macie 不會嘗試擷取或分析物件中的資料，物件會被視為未分類的物件。未分類的物件是不使用支援的 Amazon S3 儲存類別或支援的檔案或儲存格式的物件。Macie 只會分析那些使用支援儲存空間類別和支援的檔案或儲存格式的物件。

同樣地，如果您將 Macie 設定為執行自動化敏感資料探索，則無法分類的物件也無法進行選取和分析。Macie 只會選取使用支援的 Amazon S3 儲存類別和受支援的檔案或儲存格式的物件。

若要識別存放未分類物件的 S3 儲存貯體，您可以篩選 S3 儲存貯體庫存。對於詳細目錄中的每個值區，都有一些欄位會報告值區中未分類物件的數量和總儲存大小。

分析 Amazon Macie 發現

Amazon Macie 偵測到潛在的政策違規或 Amazon 簡單儲存服務 (Amazon S3) 一般用途儲存貯體的安全性或隱私問題時，或偵測到 S3 物件中的敏感資料時，會產生發現結果。發現是 Macie 發現的潛在問題或敏感數據的詳細報告。每個發現項目都會提供嚴重性等級、受影響資源的相關資訊，以及其他詳細資訊，例如 Macie 發現問題或資料的時間和方式。Macie 會將您的政策和敏感資料調查結果儲存 90 天。

您可以使用下列方式來檢閱、分析及管理發現項目。

Amazon Macie 控制台

Amazon Macie 主控台上的「發現項目」頁面會列出您的發現項目，並提供個別發現項目的詳細資訊。這些頁面也提供分組、篩選和排序發現項目，以及建立和管理隱藏規則的選項。抑制規則可以幫助您簡化發現結果的分析。

Amazon Macie API

使用 Amazon Macie API，您可以使用 AWS 命令列工具或開發 AWS 套件，或直接將 HTTPS 請求傳送至 Macie 來查詢和擷取發現項目資料。若要查詢資料，請向 Amazon Macie API 提交請求，並使用支援的參數來指定要擷取的發現項目。在您提交要求之後，Macie 會以 JSON 回應傳回結果。然後，您可以將結果傳遞給其他服務或應用程式，以進行更深入的分析、長期儲存或報告。如需詳細資訊，請參閱 Amazon Macie API 參考。

Amazon EventBridge

為了進一步支援與其他服務和系統 (例如監控或事件管理系統) 的整合，Macie 將調查結果 EventBridge 作為事件發佈到 Amazon。 EventBridge舊稱為 Amazon E CloudWatch vents，是一種無伺服器事件匯流排服務，可從您自己的應用程式、軟體即服務 (SaaS) 應用程式，以及 Macie AWS 服務 等交付即時資料串流。它可以將該資料路由到 AWS Lambda 功能、Amazon 簡單通知服務主題和 Amazon Kinesis 串流等目標，以進行額外的自動化處理。使用 EventBridge 也有助於確保長期保留發現項目資料。若要進一步了解 EventBridge，請參閱 Amazon EventBridge 使用者指南。

Macie 會自動發布事件以獲 EventBridge 取新的發現。它也會自動發佈事件，以供後續發生的現有策略發現項目。由於發現項目資料的結構為 EventBridge 事件，因此您可以使用其他服務和工具，更輕鬆地監視、分析發現項目並採取行動。例如，您可以使用自動 EventBridge 將特定類型的新發現項目傳送至 AWS Lambda 函式，進而處理資料並傳送至您的安全性事件和事件管理 (SIEM) 系統。如果將 AWS 使用者通知與 Macie 整合，您也可以使用事件，透過您指定的交付管道自動通知

發現結果。若要瞭解如何使用 EventBridge 事件監視和處理發現項目，請參閱Amazon Macie 與亞馬遜集成 EventBridge。

AWS Security Hub

如需組織安全性狀態的其他更廣泛分析，您也可以將發現項目發佈到 AWS Security Hub. Security Hub 是一項服務，可從以 AWS 服務 及支援的安全 AWS Partner Network 性解決方案中收集安全性資料，為您提供 AWS 環境中安全性狀態的全面檢視。Security Hub 也可協助您根據安全性產業標準和最佳做法來檢查您的環境。若要進一步了解資訊 Security Hub，請參閱使AWS Security Hub 用者指南。若要瞭解如何使用 Security Hub 來監視和處理發現項目，請參閱Amazon Macie 與集成 AWS Security Hub。

除了發現項目之外，Macie 還會為 S3 物件建立敏感資料探索結果，這些物件會分析以探索敏感資料。敏感資料探索結果是記錄物件分析之相關詳細資料的報告。這包括 Macie 無法在其中找到敏感資料，因此不會產生發現項目的物件，以及 Macie 因錯誤或問題而無法分析的物件。敏感資料探索結果為您提供分析記錄，這些記錄對於資料隱私權和保護稽核或調查有幫助。您無法直接在 Amazon Macie 主控台或使用 Amazon Macie API 存取敏感資料探索結果。相反地，您可以將 Macie 設定為將結果儲存在 S3 儲存貯體中。然後，您可以選擇性地存取並查詢該值區中的結果。若要瞭解如何設定 Macie 來儲存結果，請參閱儲存及保留敏感資料探索結果。

主題

Amazon Macie 發現的類型

Amazon Macie 產生兩類發現項目：政策發現和敏感資料發現。政策發現是 Amazon 簡單儲存體 (Amazon S3) 一般用途儲存貯體的潛在政策違規或安全性或隱私問題的詳細報告。Macie 會產生原則發現項目，作為其持續活動的一部分，以評估和監視您的一般用途值區，以確保安全性和存取控制。敏感資料發現是 Macie 在 S3 物件中偵測到的敏感資料的詳細報告。Macie 會產生敏感資料發現項目，做為執行敏感資料探索工作或執行自動化敏感資料探索時所執行的活動的一部分。

在每個品類中，都有特定的類型。發現項目的類型可讓您深入瞭解 Macie 找到的問題性質或敏感資料。發現項目的詳細資料會提供嚴重性等級、受影響資源的相關資訊，以及其他資訊，例如 Macie 發現問題或敏感資料的時間和方式。每個發現項目的嚴重性和詳細資料會根據發現項目的類型和性質而有所不同。

主題

> **Tip**
>
> 若要探索並瞭解 Macie 可產生的不同類別和發現項目類型，請建立範例發現項目。範例發現項目會使用範例資料和預留位置值來示範每種發現項目類型可能包含的資訊類型。

政策發現的類型

Amazon Macie 會在 S3 一般用途儲存貯體的政策或設定以降低儲存貯體和儲存貯體物件的安全性或隱私權的方式變更時，產生政策查詢。如需有關 Macie 如何偵測這些變更的資訊，請參閱Macie 如何監控 Amazon S3 數據安全。

只有在您為您啟用 Macie 之後發生變更時，Macie 才會產生原則尋找。 AWS 帳戶例如，如果在啟用 Macie 之後停用 S3 儲存貯體的區塊公用存取設定，Macie 會產生一個政策：儲存貯體的 IAM BlockPublicAccessDisabled USER/S3 尋找。如果在您啟用 Macie 時停用儲存貯體的封鎖公用存取設定，而且繼續停用這些設定，Macie 不會產生原則：儲存貯體的 IAMUS BlockPublicAccessDisabled ER/S3 尋找。

如果 Macie 偵測到現有原則發現的後續發現項目，Macie 會新增有關後續發現項目的詳細資料，並遞增發生次數，以更新現有的發現項目。Macie 會儲存 90 天的政策調查結果。

Macie 可以針對 S3 一般用途儲存貯體產生下列類型的政策發現項目。

Policy:IAMUser/S3BlockPublicAccessDisabled

值區的所有值區層級區塊公開存取設定都已停用。值區的存取權由帳戶的區塊公開存取設定、存取控制清單 (ACL) 以及值區的值區政策所控制。

若要了解 S3 儲存貯體的區塊公開存取設定，請參閱 Amazon 簡單儲存服務使用者指南中的封鎖對 Amazon S3 儲存的公開存取。

Policy:IAMUser/S3BucketEncryptionDisabled

儲存貯體的預設加密設定已重設為預設的 Amazon S3 加密行為，即使用 Amazon S3 受管金鑰自動加密新物件。

自 2023 年 1 月 5 日起，Amazon S3 會自動使用 Amazon S3 受管金鑰 (SSE-S3) 套用伺服器端加密，作為新增至儲存貯體之物件的基礎加密層級。您可以選擇性地設定值區的預設加密設定，改為使用金鑰 (SSE-KMS) 的伺服器端加密，或使用金 AWS KMS 鑰 (DSSE-KMS) 進行雙層伺服器端加密。 AWS KMS 若要了解 S3 儲存貯體的預設加密設定和選項，請參閱 Amazon 簡單儲存貯體使用者指南中的設定 S3 儲存貯體的預設伺服器端加密行為。

如果 Macie 在 2023 年 1 月 5 日之前產生此類型的發現項目，則發現項目表示受影響值區的預設加密設定已停用。這表示值區的設定未指定新物件的預設伺服器端加密行為。Amazon S3 不再支援停用儲存貯體預設加密設定的功能。

Policy:IAMUser/S3BucketPublic

儲存貯體的 ACL 或值區政策已變更，以允許匿名使用者或所有已驗證 AWS Identity and Access Management (IAM) 身分存取。

若要了解 S3 儲存貯體的 ACL 和儲存貯體政策，請參閱 Amazon 簡單儲存服務使用者指南中的 Amazon S3 中的身分和存取管理。

Policy:IAMUser/S3BucketReplicatedExternally

已啟用複寫，並設定為將物件從值區複製到組 AWS 帳戶 織外部 (非組織一部分) 的值區。組織是一組 Macie 帳戶，可透過 AWS Organizations 或透過 Macie 邀請集中管理為一組相關帳戶。

在特定情況下，Macie 可能會針對未設定為將物件複製到外部 AWS 帳戶值區的值區產生這種類型的尋找項目。如果在 Macie 從 Amazon S3 擷取儲存貯體和物件中繼資料作為每日重新整理週期的一部分之後，目標儲存貯體是在前 24 小時內建立的，則可能會發生這種 AWS 區域 情況。若要調查發現項目，請先重新整理庫存資料。然後檢閱值區的詳細資訊。詳細資訊會指出值區是否設定為將物件複製到其他值區。如果值區設定為執行此操作，則詳細資料會包含擁有目標值區之每個帳戶的帳戶 ID。

若要了解 S3 儲存貯體的複寫設定，請參閱 Amazon 簡單儲存服務使用者指南中的複寫物件。

Policy:IAMUser/S3BucketSharedExternally

值區的 ACL 或值區政策已變更，以允許與組織外部 (非屬於) 的值區共用值區。 AWS 帳戶 組織是一組 Macie 帳戶，可透過 AWS Organizations 或透過 Macie 邀請集中管理為一組相關帳戶。

在某些情況下，Macie 可能會針對未與外部 AWS 帳戶共用的儲存貯體產生這種類型的尋找項目。如果 Macie 無法完全評估儲存貯體政策中的元素與政策`Principal`元素中的特定AWS 全域條件內容金鑰或 Amazon S3 條件金鑰之間的關係，就會發生這種情況。`Condition`適用的條件鍵為：`aws:PrincipalAccount`、`aws:PrincipalArn`、`aws:PrincipalOrgID`、`aws:PrincipalOrgPat`和`s3:DataAccessPointArn`。我們建議您檢閱值區的政策，以判斷此存取是否有意且安全。

若要了解 S3 儲存貯體的 ACL 和儲存貯體政策，請參閱 Amazon 簡單儲存服務使用者指南中的 Amazon S3 中的身分和存取管理。

Policy:IAMUser/S3BucketSharedWithCloudFront

儲存貯體的儲存貯體政策已變更為允許與 Amazon CloudFront 原始存取身分 (OAI)、 CloudFront 原始存取控制 (OAC) 或 O CloudFront AI 和 OAC 共用儲存貯體。 CloudFront CloudFront OAI 或 OAC 可讓使用者透過一或多個指 CloudFront定的發行版存取值區的物件。

若要了解 CloudFront OAI 和 OAC，請參閱 Amazon 開發人員指南中的限制對 Amazon S3 來源的存取。 CloudFront

> **Note**
>
> 在某些情況下，Macie 會生成一個策略：IAMUSER/S3 BucketSharedExternally 查找而不是策略：IAMUSER/S3 查找存儲桶。BucketSharedWithCloudFront這些情況是：
>
> - 除了 CloudFront OAI 或 OAC AWS 帳戶 之外，還會與組織外部的值區共用。
> - 儲存貯體的政策會指定 OAI 的規範使用者 ID，而不是 Amazon 資源名稱 (ARN)。 CloudFront
>
> 這會產生值區的嚴重性較高的原則發現項目。

敏感資料發現項目的類型

當 Macie 偵測到 S3 物件中的敏感資料時，會產生敏感資料尋找，而該物件會分析以探索敏感資料。這包括 Macie 在您執行敏感資料探索工作或執行自動化敏感資料探索時所執行的分析。

例如，如果您建立並執行敏感資料探索工作，而 Macie 偵測到 S3 物件中的銀行帳戶號碼，Macie 會為物件產生一個:S3 物件/SensitiveData財務尋找。同樣地，如果 Macie 在自動化敏感資料探索週期中偵測到 S3 物件中所分析的銀行帳戶號碼，Macie 就會為該物件產生 A: SensitiveData S3 物件/財務尋找。

如果 Macie 在後續任務執行或自動化敏感資料探索週期期間偵測到相同 S3 物件中的敏感資料，Macie 會為物件產生新的敏感資料尋找項目。與原則發現項目不同，所有發現的敏感資料都會被視為新的 (唯一)。Macie 存儲敏感數據發現 90 天。

Macie 可以為 S3 物件產生下列類型的敏感資料發現項目。

SensitiveData:S3Object/Credentials

物件包含機密認證資料，例如 AWS 秘密存取金鑰或私密金鑰。

SensitiveData:S3Object/CustomIdentifier

物件包含符合一或多個自訂資料識別碼偵測準則的文字。物件可能包含一種以上的敏感資料類型。

SensitiveData:S3Object/Financial

物件包含敏感的財務資訊，例如銀行帳號或信用卡號碼。

SensitiveData:S3Object/Multiple

物件包含一種以上的敏感資料類別，包括認證資料、財務資訊、個人資訊或符合一或多個自訂資料識別碼偵測準則的文字組合。

SensitiveData:S3Object/Personal

該物件包含敏感的個人資訊 — 個人識別資訊 (PII)，例如護照號碼或駕照識別號碼、個人健康資訊 (PHI)，例如健康保險或醫療識別號碼，或 PII 和 PHI 的組合。

如需 Macie 可以使用內建準則和技術偵測之敏感資料類型的相關資訊，請參閱使用受管資料識別符。如需 Macie 可分析之 S3 物件類型的相關資訊，請參閱支援的儲存類別和格式。

在 Amazon Macie 中使用樣本發現

若要探索並了解 Amazon Macie 可產生的不同類型發現項目，您可以建立範例發現項目。範例發現項目會使用範例資料和預留位置值來示範每種發現項目類型可能包含的資訊類型。

例如，政策：IAMUSER/S3 BucketPublic 範例尋找項目包含虛擬亞馬遜簡單儲存服務 (Amazon S3) 儲存貯體的詳細資料。發現項目的詳細資料包括有關實行者和動作的範例資料，這些動作會變更值區的存取控制清單 (ACL)，並讓值區可公開存取。同樣地，: S3 物件/多個SensitiveData範例尋找項目包含有關虛構 Microsoft Excel 活頁簿的詳細資料。發現項目的詳細資料包括有關工作簿中敏感資料類型和位置的範例資料。

除了熟悉不同發現項目類型可能包含的資訊之外，您還可以使用發現項目範例來測試與其他應用程式、服務和系統的整合。根據您帳戶的抑制規則，Macie 可以將樣本發現 EventBridge 作為事件發佈到 Amazon。透過使用範例發現項目中的範例資料，您可以開發和測試自動化解決方案，以監視和處理這些事件。根據您帳戶的發佈設定，Macie 也可以將範例結果發佈到AWS Security Hub。這表示您也可以使用範例發現項目來開發和測試解決方案，以監視和處理 Security Hub 中的 Macie 發現項目。如需將發現項目發佈至這些服務的相關資訊，請參閱 監控和處理問題清單

主題

建立範例結果

您可以使用亞馬遜 Macie 主控台或亞馬 Amazon Macie API 建立範例發現項目。如果您使用主控台，Macie 會自動為 Macie 支援的每種類型發現項目產生一個範例尋找項目。如果您使用 API，則可以為每個類型建立範例，也可以只為您指定的特定類型建立範例。

Console

請依照下列步驟使用 Amazon Macie 主控台建立範例發現項目。

建立範例發現項目

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 在導覽窗格中，選擇設定。
3. 在範例發現項目下，選擇產生範例發現項目

API

若要以程式設計方式建立範例發現項目，請使用 Amazon Macie API 的CreateSampleFindings作業。當您提交請求時，您可以選擇性地使用`findingTypes`參數來指定要建立的特定型態範例發現項目。若要自動建立所有類型的範例，請勿在要求中包含此參數。

若要使用 AWS Command Line Interface(AWS CLI) 建立範例發現項目，請執行create-sample-findings命令。若要自動建立所有發現項目類型的範例，請勿包含`finding-types`參數。若只要建立特定發現項目類型的範例，請加入此參數，並指定要建立的範例發現項目類型。例如：

```
C:\> aws macie2 create-sample-findings --finding-types "SensitiveData:S3Object/
Multiple" "Policy:IAMUser/S3BucketPublic"
```

```
###S3Object/Multiple SensitiveData################IAMUser/S3 ##########
####BucketPublic
```

如果命令運行成功，Macie 返回一個空的響應。

檢閱範例結果

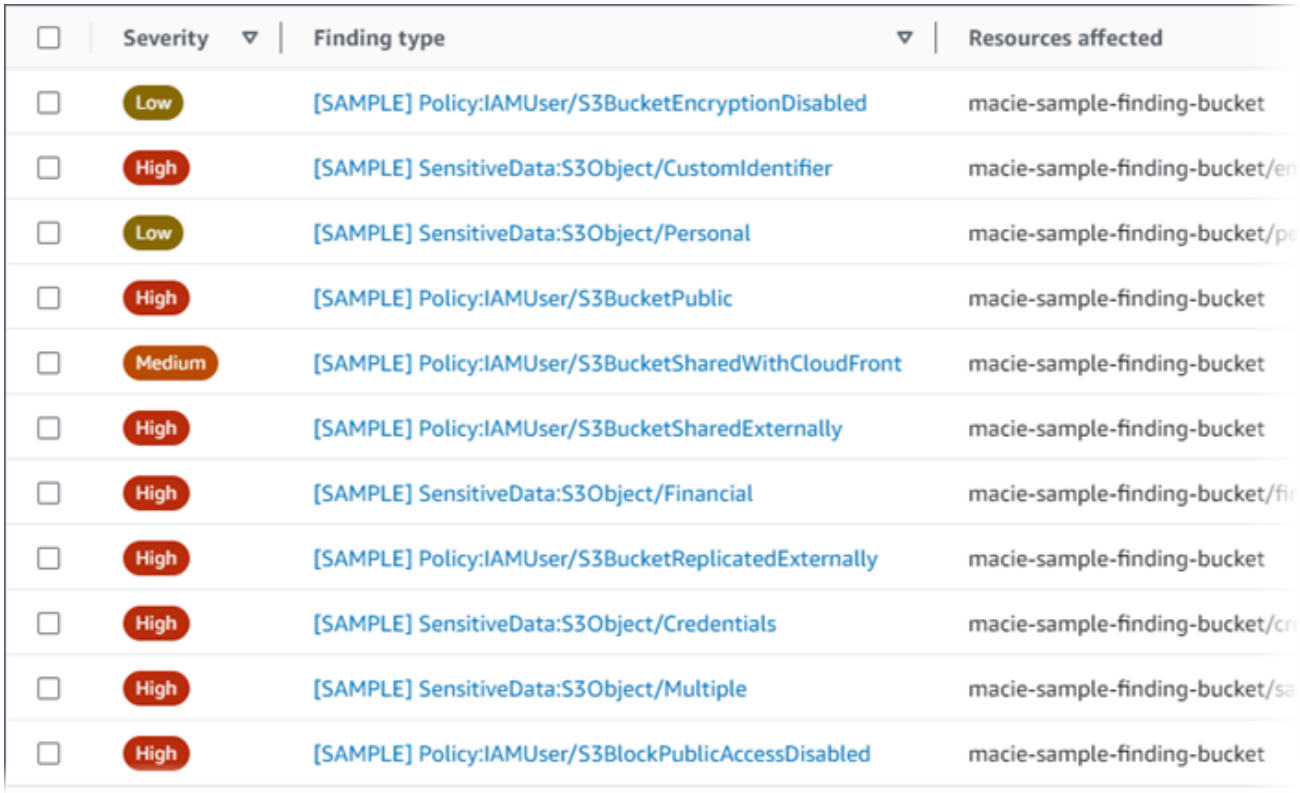
為了協助您識別您所建立的範例發現項目，Macie 會將每個範例發現項目的 [範例] 欄位的值設定為 True。此外，受影響的 S3 儲存貯體的名稱對於所有發現的範例都是相同的：macie-sample-finding-bucket。如果您使用 Amazon Macie 主控台上的「發現項目」頁面來檢閱範例發現項目，Macie 也會在每個範例發現項目的「尋找項目類型」欄位中顯示 [SAMPLE] 前置詞。

Console

請依照下列步驟使用 Amazon Macie 主控台檢閱發現項目範例。

若要檢閱樣本發現

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 在導覽窗格中，選擇調查結果。
3. 在「發現的項目」頁面上，執行下列任一項作業：
   - 在「發現項目類型」欄中，找出類型以 [SAMPLE] 開頭的發現項目，如下圖所示。



- 使用表格上方的「篩選條件」方塊，篩選表格以僅顯示發現項目的範例。若要執行此操作，請將游標放在方塊中。在顯示的欄位清單中，選擇 [範例]。然後選擇「真」，然後選擇「套用」。這會將下列篩選條件新增至表格中：

4. 若要檢閱特定範例發現項目的詳細資料，請選擇發現項目。詳細資料面板會顯示發現項目的資訊。

您也可以將一或多個範例發現項目的詳細資訊下載並儲存為 JSON 檔案。若要這樣做，請選取您要下載並儲存的每個範例發現項目的核取方塊。然後在 「發現項目」頁面頂端的「動作」功能表中選擇「匯出 (JSON)」。在出現的視窗中，選擇 [下載]。如需發現項目可包含之 JSON 欄位的詳細說明，請參閱 Amazon Macie API 參考中的發現項目。

API

若要以程式設計方式檢閱範例發現項目，請先使用 Amazon Macie API 的ListFindings作業來擷取您建立的每個範例發現項目的唯一識別碼 (`findingId`)。然後使用GetFindings作業擷取這些發現項目的詳細資訊。

當您提交ListFindings請求時，您可以指定篩選條件，以便僅在結果中包含發現項目的範例。要做到這一點，添加一個過濾條件，其中的sample字段的值是true。如果您使用的是AWS CLI，請執行清單發現項目命令，並使用finding-criteria參數來指定篩選條件。例如：

```
C:\> aws macie2 list-findings --finding-criteria={\"criterion\":{\"sample\":{\"eq\":[\"true\"]}}}
```

如果您的請求成功，Macie 返回一個數組findingIds。陣列會列出目前帳戶中每個範例發現項目的唯一識別碼AWS 區域。

若要接著擷取範例發現項目的詳細資訊，請在GetFindings要求中指定這些唯一識別碼，或在執行 get- find 命令時指定這些唯一識別碼。AWS CLI

抑制範例發現項目

與其他發現一樣，Macie 將樣本發現存儲 90 天。完成檢閱和試驗範例之後，您可以選擇性地建立隱藏規則來封存它們。如果您這麼做，範例發現項目會依預設停止顯示在主控台上，且其狀態會變更為已封存。

若要使用 Amazon Macie 主控台存檔範例發現項目，請設定規則以在「範例」欄位的值為 True 時存檔發現項目。若要使用 Amazon Macie API 存檔範例發現項目，請設定規則以將發現項目存檔在sample欄位值所在的位true置。

在 Amazon Macie 控制台上查看發現

Amazon Macie 會監控您的 AWS 環境，並在偵測到潛在的政策違規或 Amazon Simple Storage Service (Amazon S3) 一般用途儲存貯體的安全性或隱私問題時產生政策發現。Macie 會在偵測到 S3 物件中的敏感資料時產生敏感資料發現項目。Macie 會將您的政策和敏感資料調查結果儲存 90 天。

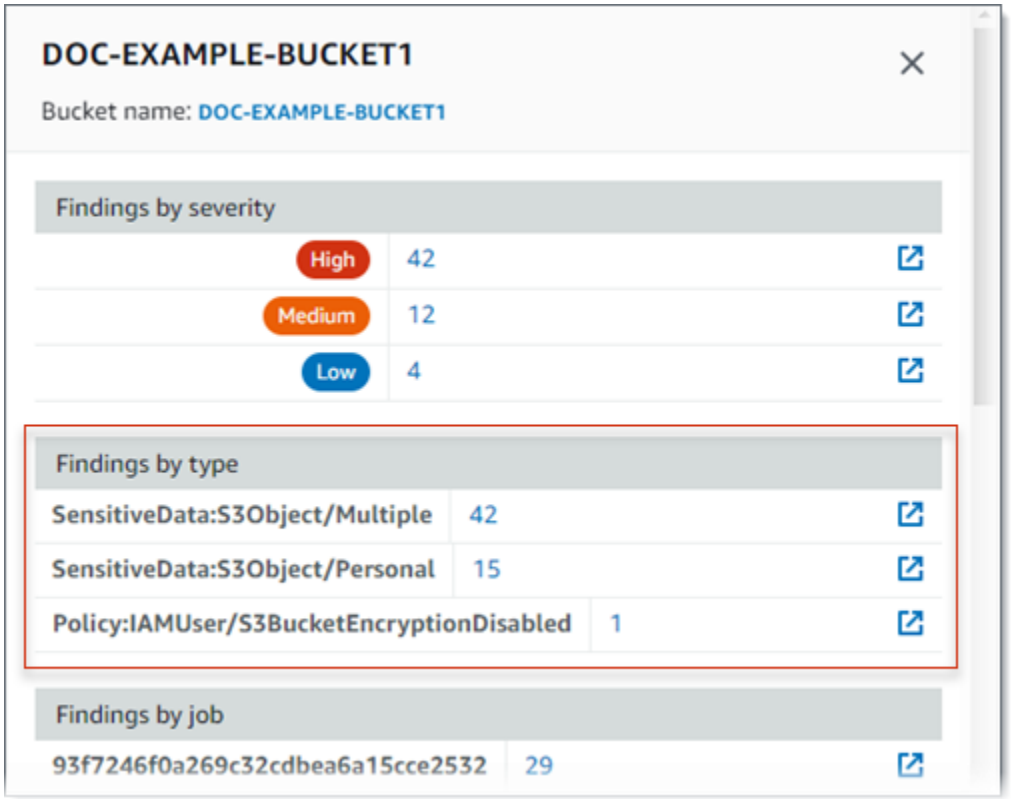
每個發現項目都會指定發現項目類型和嚴重性等 其他詳細資料包括受影響資源的相關資訊，以及 Macie 何時及如何發現此發現項目所回報的機密資料或敏感資料。每個發現項目的嚴重性和詳細資料會根據發現項目的類型和性質而有所不同。

透過使用 Amazon Macie 主控台，您可以檢閱和分析發現項目，以及存取個別發現項目的詳細資訊。您也可以將一或多個發現項目匯出至 JSON 檔案。為了協助您簡化分析，主控台提供了數個選項來建立發現項目的自訂檢視。

使用預先定義的分組

使用特定頁面來檢閱依條件分組的發現項目，例如受影響的 S3 儲存貯體、尋找類型或敏感資料探索工作。您可以使用這些頁面來檢閱每個群組的彙總統計資料，例如按嚴重性分類的發現項目計數。您也可以向下展開以檢閱群組中個別發現項目的詳細資訊，也可以套用篩選條件來精簡分析。

例如，如果您按 S3 儲存貯體將所有發現項目分組，並注意特定儲存貯體發生政策違規，則可以快速判斷儲存貯體是否也有發現的敏感資料。若要這麼做，請在瀏覽窗格 (在 [搜尋結果] 下) 中選擇 [依值區]，然後選擇值區。在出現的詳細資料面板中，「依類型分類的發現項目」區段會列出套用至值區的發現項目類型，如下圖所示。



若要調查特定類型，請選擇類型的編號。Macie 會顯示符合所選類型並套用至 S3 儲存貯體的所有發現項目的表格。若要精簡結果，請篩選表格。

建立並套用篩選

使用特定的發現項目屬性，將某些發現項目納入或排除「發現項目」表 尋找屬性是儲存發現項目的特定資料的欄位，例如尋找類型、嚴重性或受影響 S3 儲存貯體的名稱。如果您篩選資料表，您可以更輕鬆地識別具有特定特性的發現項目。然後，您可以向下鑽研以複查這些發現項目的詳細資訊。

例如，若要檢閱所有敏感資料發現項目，請為「類別」欄位新增篩選條件。若要精簡結果並僅包含特定類型的機密資料尋找項目，請為「尋找項目類型」欄位新增篩選條件。例如：

若要然後複查特定發現項目的詳細資訊，請選擇發現項目。詳細資料面板會顯示發現項目的資訊。

您也可以依特定欄位，以遞增或遞減順序來排序搜尋結果。若要這麼做，請選擇欄位的欄標題。若要變更排序順序，請再次選擇欄標題。

若要在主控台上檢閱發現項目

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 在導覽窗格中，選擇調查結果。「發現項目」頁面會顯示 Macie 在過去 90 天內為您的帳戶建立或更新 AWS 區域 的發現項目。根據預設，這不包括由抑制規則所抑制的發現項目。
3. 若要依預先定義的邏輯群組來樞紐分析並複查發現項目，請在瀏覽窗格 (「搜尋結果」下) 中選擇「依時段」、「依類型」或「依工作」。然後選擇表格中的項目。在詳細資料面板中，選擇要旋轉之欄位的連結。
4. 若要依特定條件篩選發現項目，請使用表格上方的篩選選項：

   - 若要顯示抑制規則所抑制的發現項目，請使用「搜尋結果」狀態功能表。選擇「全部」以顯示隱藏與未抑制的搜尋結果，或選擇「已存檔」以僅顯示隱藏的搜尋結果。若要再次隱藏隱藏的發現項目，請選擇目前。
   - 若只要顯示具有特定屬性的發現項目，請使用篩選條件方塊。將游標置於方塊中，並為屬性新增篩選條件。若要進一步細化結果，請新增其他屬性的條件。若要接著移除條件，請選擇要移除之條件的移除條件圖示 (⊗)。

   如需篩選發現項目的詳細資訊，請參閱建立並將篩選套用至發現項目。
5. 若要依特定欄位排序發現項目，請選擇欄位的欄標題。若要變更排序順序，請再次選擇欄標題。
6. 若要複查特定發現項目的詳細資訊，請選擇發現項目。詳細資料面板會顯示發現項目的資訊。

> **Tip**
>
> 您可以使用詳細資料面板來樞紐和向下鑽研某些欄位。若要顯示欄位具有相同值的發現項目，
> 請 在欄位中選擇。或者
> 選 擇顯示具有欄位其他值的發現項目。
> 對於敏感資料發現，您也可以使用詳細資料面板來調查 Macie 在受影響 S3 物件中找到的敏感資料：
>
> - 若要尋找特定類型敏感資料的出現次數，請在欄位中為該類型的資料選擇數字連結。馬西顯示關於哪裡馬西找到的數據信息（JSON 格式）。如需詳細資訊，請參閱 尋找敏感資料。
> - 若要擷取 Macie 找到的機密資料樣本，請在「顯示範例」欄位中選擇「檢閱」。如需詳細資訊，請參閱 擷取敏感資料範例。
> - 若要瀏覽至對應的機密資料探索結果，請在「詳細結果位置」欄位中選擇連結。Macie 會開啟 Amazon S3 主控台，並顯示包含探索結果的檔案或資料夾。如需詳細資訊，請參閱 儲存及保留敏感資料探索結果。

您也可以將一或多個發現項目的詳細資訊下載並儲存為 JSON 檔案。若要這樣做，請選取您要下載並儲存之每個發現項目的核取方塊。然後在 「發現項目」頁面頂端的「動作」功能表中選擇「匯出 (JSON)」。在出現的視窗中，選擇 [下載]。如需發現項目可包含之 JSON 欄位的詳細說明，請參閱 Amazon Macie API 參考中的發現項目。

Amazon Macie 事件

為了執行目標分析並更有效地分析發現結果，您可以篩選 Amazon Macie 發現項目。使用篩選器，您可以建立發現項目的自訂檢視和查詢，以協助您識別並專注於具有特定特性的發現項目。使用 Amazon Macie 主控台篩選發現項目，或使用 Amazon Macie API 以程式設計方式提交查詢。

當您建立篩選器時，您可以使用發現項目的特定屬性來定義條件，以在檢視表或查詢結果中包含或排除發現項目。發現項目屬性是一個欄位，用於儲存發現項目的特定資料，例如嚴重性、類型或適用於發現項目的 S3 儲存貯體名稱。

Macie 過濾器會包含一或多個條件。每個條件，也稱為準則，由三個部分組成：

- 以屬性為基礎的欄位，例如「嚴重性」或「發現項目」類型。
- 運算子，例如等於或不等於。
- 一或多個值。值的類型和數目取決於您選擇的欄位和運算子。

如果您建立要再次使用的篩選器，可以將其儲存為篩選規則。篩選規則是您建立並儲存的一組篩選條件，以便在 Amazon Macie 主控台上檢閱發現項目時重新套用。

您也可以將篩選儲存為抑制規則。抑制規則是您建立並儲存的一組篩選條件，以自動將符合規則條件的發現項目封存。若要瞭解抑制規則，請參閱隱藏問題清單。

主題

篩選發現項目的基礎

建立篩選器時，請牢記下列功能和準則。另請注意，篩選的結果僅限於前 90 天和目前的AWS 區域。Amazon Macie 只存儲您的發現 90 在每個AWS 區域天.

主題

在篩選條件中使用多個條件

篩選器可以包含一或多個條件。每個條件，也稱為準則，由三個部分組成：

- 以屬性為基礎的欄位，例如「嚴重性」或「發現項目」類型。如需您可以使用的欄位清單，請參閱篩選發現項目的欄位。
- 一個運算符，如等於或不等於。如需可以使用的運算子清單，請參閱在條件下使用運算子。

- 一個或多個值。值的類型和數目取決於您選擇的欄位和運算子。

如果篩選器包含多個條件，Macie 會使用 AND 邏輯來連接條件並評估篩選準則。這表示尋找項目只有在符合篩選條件中的所有條件時才符合篩選準則。

例如，如果您新增條件以僅包含高嚴重性發現項目，並新增另一個條件以僅包含敏感資料發現項目，Macie 就會傳回所有高嚴重度的敏感資料發現項目。換句話說，Macie 會排除所有政策發現項目，以及所有中等嚴重程度和低嚴重度敏感資料發現項目。

您只能在篩選器中使用一次欄位。但是，您可以為許多字段指定多個值。

例如，如果某個條件使用「嚴重性」欄位只包含高嚴重性發現項目，則無法在其他條件中使用「嚴重性」欄位來包含中等嚴重性或低嚴重性發現項目。而是為現有條件指定多個值，或針對現有條件使用不同的運算子。例如，若要包含所有中等嚴重性和高嚴重性發現項目，請新增「嚴重性等於中」、「高」條件或新增「嚴重性」不等於「低」條件。

指定欄位的值

當您為欄位指定值時，該值必須符合欄位的基礎資料類型。根據欄位，您可以指定下列其中一種類型的值。

文本數組（字符串）

指定欄位的文字 (字串) 值清單。每個字串都與欄位的預先定義值或現有值相關聯，例如「嚴重性」欄位的「高」，「尋找項目類型」欄位的:S3Object/FinancialSensitiveData，或 S3 儲存貯體名稱欄位的 S3 儲存貯體名稱。

如果您使用陣列，請注意下列事項：

- 值是區分大小寫的。
- 您無法在值中指定部分值或使用萬用字元。您必須為欄位指定完整、有效的值。

例如，若要篩選名**my-S3-bucket**為 My- S3 儲存貯體的發現項目，請輸入 S3 儲存貯體名稱欄位的值。如果您輸入任何其他值，例如**my-s3-bucket**或**my-S3**，Macie 將不會傳回值區的發現項目。

如需每個欄位的有效值清單，請參閱篩選發現項目的欄位。

您可以在陣列中指定多達 50 個值。指定值的方式取決於您使用的是 Amazon Macie 主控台還是 Amazon Macie API，如中所述。為欄位指定多個值

：布林值

為欄位指定兩個互斥值之一。

如果您使用 Amazon Macie 主控台指定此類型的值，則主控台會提供可供選擇的值清單。如果您使用 Amazon Macie API，請`false`為值指定`true`或。

日期/時間（和時間範圍）

指定欄位的絕對日期和時間。如果您指定這種類型的值，則必須同時指定日期和時間。

在 Amazon Macie 主控台上，日期和時間值會以您當地的時區為單位，並使用 24 小時標記法。在所有其他環境中，這些值均採用國際標準時間 (UTC) 和延伸的 ISO 8601 格式，例如`2020-09-01T14:31:13Z`：世界標準時間 2020 年 9 月 1 日下午 2:31：13。

如果欄位儲存日期/時間值，您可以使用欄位來定義固定或相對時間範圍。例如，您可以只包含在兩個特定日期與時間之間建立的發現項目，或只包含在特定日期與時間之前或之後建立的發現項目。如何定義時間範圍取決於您使用 Amazon Macie 控制台還是 Amazon Macie API：

- 在主控台上，使用日期選擇器或直接在 [從] 和 [到] 方塊中輸入文字。
- 使用 API，透過新增指定範圍中第一個日期和時間的條件來定義固定時間範圍，並新增另一個指定範圍中最後一個日期和時間的條件。如果您這樣做，Macie 會使用 AND 邏輯來加入條件。若要定義相對時間範圍，請新增一個條件來指定範圍中的第一個或最後一個日期和時間。將這些值指定為以毫秒為單位的 Unix 時間戳記，例如，針對 2020 年 11 月 5 日世界標準時`1604616572653`間 22:49：32。

在主控台上，時間範圍包含在內。使用 API 時，時間範圍可以包含或排斥，具體取決於您選擇的運算子。

數字（和數值範圍）

指定欄位的長整數。

如果欄位儲存了數值，您可以使用欄位來定義固定或相對數值範圍。例如，您只能在 S3 物件中包含報告 50-90 次出現敏感資料的發現項目。如何定義數字範圍取決於您使用 Amazon Macie 控制台還是 Amazon Macie API：

- 在主控台上，使用 [從] 和 [到] 方塊來分別輸入範圍內的最小和最高數字。
- 使用 API，透過新增指定範圍中最小數字的條件來定義固定數值範圍，並新增另一個指定範圍中最高數字的條件。如果您這樣做，Macie 會使用 AND 邏輯來加入條件。若要定義相對數值範圍，請新增一個條件，以指定範圍中最低或最高的數字。

在主控台上，數值範圍包含在內。使用 API 時，數值範圍可以包含或排除，具體取決於您選擇的運算子。

文本（字符串）

指定欄位的單一文字 (字串) 值。此字串與欄位的預先定義或現有值相關聯，例如「嚴重性」欄位的「高」、S3 儲存貯體名稱欄位的 S3 儲存貯體名稱，或是「Job ID」欄位敏感資料探索任務的唯一識別碼。

如果您指定單一文字字串，請注意下列事項：

- 值是區分大小寫的。
- 您不能在值中使用部分值或使用萬用字元。您必須為欄位指定完整、有效的值。

例如，若要篩選名**my-S3-bucket**為 My- S3 儲存貯體的發現項目，請輸入 S3 儲存貯體名稱欄位的值。如果您輸入任何其他值，例如**my-s3-bucket**或**my-S3**，Macie 將不會傳回值區的發現項目。

如需每個欄位的有效值清單，請參閱篩選發現項目的欄位。

為欄位指定多個值

對於某些欄位和運算子，您可以為欄位指定多個值。如果您這樣做，Macie 會使用 OR 邏輯來連接這些值並評估篩選條件。這表示如果發現項目具有欄位的任何值，則符合條件。

例如，如果您新增條件以包含「尋找項目類型」欄位的值等於 SensitiveData：SS3 物件/財務，：S3 物件/個人， SensitiveDataMacie 會針對僅包含財務資訊的 S3 物件傳回敏感資料發現項目，以及僅包含個人資訊的 S3 物件。換句話說，Macie 會排除所有政策調查結果。Macie 也會排除包含其他類型敏感資料或多種敏感資料類型之物件的所有敏感資料發現項目。

例外狀況是使用eqExactMatch運算子的條件。對於這個運算子，Macie 會使用 AND 邏輯來連接值並評估篩選條件。這表示只有當搜尋結果具有欄位的所有值且僅具有欄位的值時，才符合條件。若要進一步瞭解此運算子，請參閱在條件下使用運算子。

如何為欄位指定多個值，取決於您使用的是 Amazon Macie API 還是 Amazon Macie 主控台。透過 API，您可以使用列出值的陣列。

在主控台上，您通常會從清單中選擇值。但是，對於某些字段，您必須為每個值添加不同的條件。例如，若要包含 Macie 使用特定自訂資料識別碼偵測到之資料的發現項目，請執行下列動作：

1. 將光標放在過濾條件框中，然後選擇自定義數據標識符名稱字段。輸入自訂資料識別碼的名稱，然後選擇 [套用]。

2. 針對您要為篩選指定的每個其他自訂資料識別碼重複上述步驟。

如需需要執行此操作的欄位清單，請參閱篩選發現項目的欄位。

在條件下使用運算子

您可以在個別條件下使用下列類型的運算子。

等於（eq）

符合 (=) 為欄位指定的任何值。您可以使用 equals 運算子搭配下列類型的值：文字陣列 (字串)、布林值、日期/時間、數字和文字 (字串)。

對於許多欄位，您可以使用此運算子，並為欄位指定多達 50 個值。如果您這樣做，Macie 會使用 OR 邏輯來連接這些值。這表示如果發現項目具有為欄位指定的任何值，則符合條件。

例如：

- 若要包含報告財務資訊、個人資訊或財務與個人資訊的發現項目，請新增使用「機密資料」分類欄位與此運算子的條件，並指定「財務資訊」與「個人資訊」作為欄位的值。
- 若要包含報告信用卡號碼、郵寄地址，或同時報告信用卡號碼和郵寄地址的發現項目，請為「敏感資料偵測類型」欄位新增條件，使用此運算子，CREDIT_CARD_NUMBER並指定和ADDRESS作為欄位的值。

如果您使用 Amazon Macie API 來定義使用此運算子並具有日期/時間值的條件，請將該值指定為以毫秒為單位的 Unix 時間戳記，例如，1604616572653針對 2020 年 11 月 5 日世界標準時間 22:49：32。

等於完全匹配（eqExactMatch）

完全符合為欄位指定的所有值。您可以使用等於完全相符運算子搭配選取的欄位集合。

如果您使用此運算子並為欄位指定多個值，Macie 會使用 AND 邏輯來連接這些值。這表示尋找項目只有在具有為欄位指定的所有值且僅具有欄位的值時，才符合條件。您可以為欄位指定多達 50 個值。

例如：

- 若要包含報告信用卡號碼出現且沒有其他類型敏感資料的發現項目，請為 [敏感資料偵測類型] 欄位新增條件、使用此運算子，並指定CREDIT_CARD_NUMBER為欄位的唯一值。

- 若要包含報告信用卡號碼和郵寄地址 (以及沒有其他類型的機密資料) 的發現項目，請為「敏感資料偵測類型」欄位新增條件，使用此運算子，CREDIT_CARD_NUMBER並指定和ADDRESS作為欄位的值。

由於 Macie 使用 AND 邏輯來聯結欄位的值，因此您無法將此運算子與相同欄位的任何其他運算子結合使用。換句話說，如果您在一個條件中使用等於完全匹配運算符和字段，則必須在使用相同字段的所有其他條件中使用它。

如同其他運算子，您可以在篩選器中的多個條件中使用等於完全相符運算子。如果您這麼做，Macie 會使用 AND 邏輯來連接條件並評估篩選器。這表示只有在搜尋結果具有篩選條件中所有條件所指定的所有值時，才符合篩選準則。

例如，若要包含在特定時間後建立的發現項目、報告信用卡號碼的出現次數，並且不報告任何其他類型的敏感資料，請執行下列動作：

1. 新增使用 [建立於] 欄位的條件、使用大於運算子，並指定篩選器的開始日期和時間。
2. 新增另一個使用 [敏感資料偵測類型] 欄位的條件、使用等於完全相符運算子，並指定CREDIT_CARD_NUMBER為欄位的唯一值。

您可以在下列欄位中使用等於完全相符運算子：

- 自訂資料識別碼 ID (`customDataIdentifiers.detections.arn`)
- 自訂資料識別碼名稱 (`customDataIdentifiers.detections.name`)
- S3 儲存貯體標籤鍵 (`resourcesAffected.s3Bucket.tags.key`)
- S3 儲存貯體標籤值 (`resourcesAffected.s3Bucket.tags.value`)
- S3 物件標籤金鑰 (`resourcesAffected.s3Object.tags.key`)
- S3 物件標籤值 (`resourcesAffected.s3Object.tags.value`)
- 敏感資料偵測類型 (`sensitiveData.detections.type`)
- 敏感資料類別 (`sensitiveData.category`)

在上述清單中，括號名稱會使用點標記法來表示發現項目和 Amazon Macie API 的 JSON 表示法中的欄位名稱。

大於（gt）

大於 (>) 為欄位指定的值。您可以使用具有數字和日期/時間值的大於運算子。

例如，若只要包含報告 S3 物件中出現 90 次以上敏感資料的發現項目，請新增使用敏感資料總計數欄位和此運算子的條件，並將 90 指定為欄位的值。若要在 Amazon Macie 主控台上執行此操

作，請**91**在 [寄件者] 方塊中輸入，不要在 [收件者] 方塊中輸入值，然後選擇 [套用]。主控台包含數值和時間型比較。

如果您使用 Amazon Macie API 定義使用此運算子的時間範圍，則必須將日期/時間值指定為以毫秒為單位的 Unix 時間戳記，例如，1604616572653對於 2020 年 11 月 5 日世界標準時間 22:49：32。

大於或等於（gte）

大於或等於 (>=) 為欄位指定的值。您可以使用具有數字和日期/時間值的大於或等於運算子。

例如，若只要包含報告在 S3 物件中出現 90 或更多機密資料的發現項目，請新增使用敏感資料總計數欄位和此運算子的條件，並將 90 指定為欄位的值。若要在 Amazon Macie 主控台上執行此操作，請**90**在 [寄件者] 方塊中輸入，不要在 [收件者] 方塊中輸入值，然後選擇 [套用]。

如果您使用 Amazon Macie API 定義使用此運算子的時間範圍，則必須將日期/時間值指定為以毫秒為單位的 Unix 時間戳記，例如，1604616572653對於 2020 年 11 月 5 日世界標準時間 22:49：32。

小於（lt）

小於 (<) 為欄位指定的值。您可以使用具有數字和日期/時間值的小於運算子。

例如，若只要包含報告 S3 物件中出現之敏感資料少於 90 次的發現項目，請新增使用敏感資料總計數欄位和此運算子的條件，並將 90 指定為欄位的值。若要在 Amazon Macie 主控台上執行此操作，請**89**在 [收件者] 方塊中輸入，不要在 [寄件者] 方塊中輸入值，然後選擇 [套用]。主控台包含數值和時間型比較。

如果您使用 Amazon Macie API 定義使用此運算子的時間範圍，則必須將日期/時間值指定為以毫秒為單位的 Unix 時間戳記，例如，1604616572653對於 2020 年 11 月 5 日世界標準時間 22:49：32。

小於或等於（lte）

小於或等於 (<=) 為欄位指定的值。您可以使用小於或等於運算子與數字和日期/時間值。

例如，若只要包含報告在 S3 物件中出現 90 或更少之敏感資料的發現項目，請新增使用敏感資料總計數欄位和此運算子的條件，並指定 90 做為欄位的值。若要在 Amazon Macie 主控台上執行此操作，請**90**在 [收件者] 方塊中輸入，不要在 [寄件者] 方塊中輸入值，然後選擇 [套用]。

如果您使用 Amazon Macie API 定義使用此運算子的時間範圍，則必須將日期/時間值指定為以毫秒為單位的 Unix 時間戳記，例如，1604616572653對於 2020 年 11 月 5 日世界標準時間 22:49：32。

不等於（neq）

不符合 (≠) 為欄位指定的任何值。您可以將不等於運算子與下列類型的值搭配使用：文字陣列 (字串)、布林值、日期/時間、數字和文字 (字串)。

對於許多欄位，您可以使用此運算子，並為欄位指定多達 50 個值。如果您這樣做，Macie 會使用 OR 邏輯來連接這些值。這表示如果尋找項目沒有為欄位指定的任何值，就會符合條件。

例如：

- 若要排除報告發生財務資訊、個人資訊或財務與個人資訊的搜尋結果，請新增使用「機密資料」分類欄位與此運算子的條件，並指定「財務資訊」與「個人資訊」作為欄位的值。
- 若要排除報告信用卡號碼出現的發現項目，請為 [敏感資料偵測類型] 欄位新增條件、使用此運算子，並指定CREDIT_CARD_NUMBER為欄位的值。
- 若要排除報告出現信用卡號碼、郵寄地址或信用卡號碼和郵寄地址的發現項目，請為「敏感資料偵測類型」欄位新增條件，使用此運算子，CREDIT_CARD_NUMBER並指定和ADDRESS作為欄位的值。

如果您使用 Amazon Macie API 來定義使用此運算子並具有日期/時間值的條件，請將該值指定為以毫秒為單位的 Unix 時間戳記，例如，1604616572653針對 2020 年 11 月 5 日世界標準時間 22:49：32。

建立並將篩選套用至發現項目

若要識別並專注於具有特定特性的發現項目，您可以在 Amazon Macie 主控台上以及使用 Amazon Macie API 以程式設計方式提交的查詢中篩選發現結果。當您建立篩選器時，您可以使用發現項目的特定屬性來定義條件，以在檢視表或查詢結果中包含或排除發現項目。發現項目屬性是一個欄位，用於儲存發現項目的特定資料，例如嚴重性、類型或適用於發現項目的 S3 儲存貯體名稱。

在 Macie 中，過濾器由一個或多個條件組成。每個條件，也稱為準則，由三個部分組成：

- 以屬性為基礎的欄位，例如「嚴重性」或「發現項目」類型。
- 一個運算符，如等於或不等於。
- 一個或多個值。值的類型和數目取決於您選擇的欄位和運算子。

定義和套用篩選條件的方式取決於您使用的是 Amazon Macie 主控台還是 Amazon Macie API。

主題

- 在 Amazon Macie 控制台上篩選發現的結果
- 使用 Amazon Macie API 以程式設計方式篩選結果

在 Amazon Macie 控制台上篩選發現的結果

如果您使用 Amazon Macie 主控台篩選發現項目，Macie 會提供選項來協助您針對個別條件選擇欄位、運算子和值。您可以使用「發現項目」頁面上的篩選器設定來存取這些選項，如下圖所示。

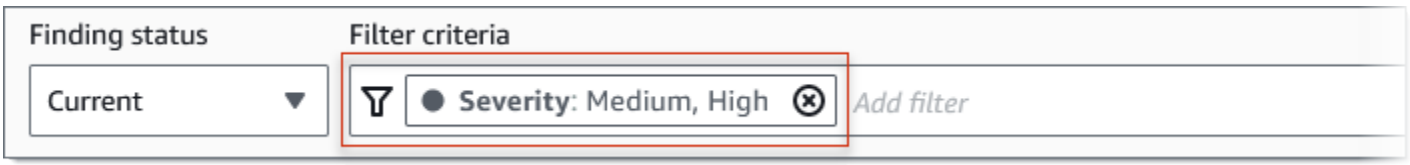
您可以使用「搜尋結果」狀態功能表，指定是否要包含由抑制規則隱藏 (自動封存) 的發現項目。透過使用「篩選條件」方塊，您可以輸入篩選條件。

當您將游標置於 [篩選條件] 方塊中時，Macie 會顯示您可以在篩選條件中使用的欄位清單。這些欄位是依邏輯類別組織的。例如，「一般欄位」 類別包含適用於任何發現項目類型的欄位，而 「分類」欄位類別包含僅適用於敏感資料發現項目的欄位。欄位會在每個類別中按字母順序排序。

若要新增條件，請先從清單中選擇欄位。若要尋找欄位，請瀏覽完整清單，或輸入部分欄位名稱以縮小欄位清單。

根據您選擇的欄位，Macie 會顯示不同的選項。這些選項會反映您所選欄位的類型和性質。例如，如果您選擇「嚴重性」欄位，Macie 會顯示可供選擇的值清單：「低」、「中」和「高」。如果您選擇 S3 儲存貯體名稱欄位，Macie 會顯示一個文字方塊，您可以在其中輸入儲存貯體名稱。無論您選擇哪個欄位，Macie 都會引導您完成以下步驟，以新增條件，其中包含欄位的必要設定。

新增條件之後，Macie 會套用條件的條件，並將條件新增至「篩選條件」方塊中的篩選器標記，如下圖所示。



在此範例中，條件設定為包含所有中等嚴重性和高嚴重性發現項目，並排除所有低嚴重性發現項目。它會傳回「嚴重性」欄位值等於「中」或「高」的發現項目。

> **Tip**
>
> 對於許多欄位，您可以在條件的篩選器權杖中選擇等於圖示 (●)，將條件的運算子從 equals 變更為不等於。如果您這麼做，Macie 會將運算子變更為不等於，並在權杖中顯示不等於圖示 (⊘)。若要再次切換至等於運算子，請選擇「不等於」圖示。

當您新增更多條件時，Macie 會套用其條件，並將其新增至「篩選條件」方塊中的記號。您可以隨時參考此方塊，以確定您已套用哪些條件。若要移除條件，請在條件的記號中選擇移除條件圖示 (⊗)。

若要使用主控台篩選發現項目

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 在導覽窗格中，選擇 Findings (問題清單)。
3. (選擇性) 若要先依預先定義的邏輯群組進行樞紐分析並複查發現項目，請在瀏覽窗格 (在「發現項目」下) 中選擇「依值區」、「依類型」或「依工作」。然後選擇表格中的項目。在詳細資料面板中，選擇要旋轉之欄位的連結。
4. (選擇性) 若要顯示抑制規則所抑制的發現項目，請變更篩選狀態設定。選擇「已存檔」以僅顯示隱藏的搜尋結果，或選擇「全部」以顯示隱藏與未隱藏的搜尋結果。若要隱藏隱藏的發現項目，請選擇目前
5. 若要新增篩選條件：

   a. 將游標置於 [篩選條件] 方塊中，然後選擇要用於條件的欄位。如需有關可使用之欄位的資訊，請參閱篩選發現項目的欄位。

   b. 為欄位輸入適當的值類型。如需不同類型值的詳細資訊，請參閱指定欄位的值。

      文本數組（字符串）

      對於這種類型的值，Macie 通常會提供可供選擇的值清單。如果是這種情況，請選取您要在條件中使用的每個值。

      如果 Macie 未提供值清單，請為欄位輸入完整、有效的值。若要指定欄位的其他值，請選擇「套用」，然後為每個其他值新增其他條件。

請注意，值是區分大小寫的。此外，您不能在值中使用部分值或萬用字元。例如，若要篩選名**my-S3-bucket**為 My- S3 儲存貯體的發現項目，請輸入 S3 儲存貯體名稱欄位的值。如果您輸入任何其他值，例如**my-s3-bucket**或**my-S3**，Macie 將不會傳回值區的發現項目。

：布林值

對於這種類型的值，Macie 會提供可供選擇的值清單。選取您要在條件中使用的值。

日期/時間 (時間範圍)

對於這種類型的值，請使用「從」(From) 和「到」(To) 方塊來定義包含的時間範圍：

- 若要定義固定時間範圍，請使用「從」(From) 和「到」(To) 方塊，分別指定範圍中的第一個日期和時間，以及最後一個日期和時間。
- 若要定義從特定日期和時間開始並在目前時間結束的相對時間範圍，請在「從」(From) 方塊中輸入開始日期和時間，並刪除「至」(To) 方塊中的任何文字。
- 若要定義在特定日期和時間結束的相對時間範圍，請在 [收件者] 方塊中輸入結束日期和時間，並刪除 [從] 方塊中的任何文字。

請注意，時間值使用 24 小時標記法。如果您使用日期選擇器來選擇日期，您可以直接在「從」(From) 和「到」(To) 方塊中輸入文字來精簡值。

數字 (數值範圍)

對於此類型的值，請使用「從」(From) 和「到」(To) 方塊輸入一或多個整數，以定義包含、固定或相對數值範圍。

文字 (字串) 值

對於此類型的值，請為欄位輸入完整、有效的值。

請注意，值是區分大小寫的。此外，您不能在值中使用部分值或萬用字元。例如，若要篩選名**my-S3-bucket**為 My- S3 儲存貯體的發現項目，請輸入 S3 儲存貯體名稱欄位的值。如果您輸入任何其他值，例如**my-s3-bucket**或**my-S3**，Macie 將不會傳回值區的發現項目。

c. 完成新增欄位值後，請選擇「套用」。Macie 會套用篩選條件，並將條件新增至 [篩選條件] 方塊中的篩選器權杖。

6. 針對您要新增的每個其他條件重複步驟 5。
7. 若要移除條件，請在條件的篩選器 Token 中選擇移除條件圖示 ( )。

8. 若要變更條件，請在條件的篩選器 Token 中選擇移除條件圖示 () 來移除條件。然後重複步驟 5 以新增具有正確設定的條件。

如果您隨後想要再次使用這組條件，您可以將該組儲存為篩選規則。若要這麼做，請在 [篩選條件] 方塊中選擇 [儲存規則]。然後輸入規則的名稱和描述 (選擇性)。完成後，請選擇 Save (儲存)。

使用 Amazon Macie API 以程式設計方式篩選結果

若要以程式設計方式篩選發現項目，請在使用 Amazon Macie API ListFindings或GetFindingStatistics操作提交的查詢中指定篩選條件。此ListFindings作業會傳回尋找 ID 的陣列，每個符合篩選準則的發現項目都有一個 ID。此GetFindingStatistics作業會傳回符合篩選準則之所有發現項目的彙總統計資料，並依您在要求中指定的欄位分組。

請注意，ListFindings和GetFindingStatistics作業與您用來隱藏發現項目的作業不同。與隱藏作業 (也會指定篩選條件) 不同，ListFindings與GetFindingStatistics作業只會查詢發現項目資料。它們不會對符合篩選準則的發現項目執行任何動作。若要抑制發現項目，請使用 Amazon Macie API 的CreateFindingsFilter操作。

若要在查詢中指定篩選條件，請在請求中包含篩選條件對映。對於每個條件，請為欄位指定欄位、運算子以及一或多個值。值的類型和數目取決於您選擇的欄位和運算子。如需有關可在條件中使用之欄位、運算子和值類型的資訊，請參閱篩選發現項目的欄位在條件下使用運算子、和指定欄位的值。

下列範例說明如何在使用 AWS Command Line Interface(AWS CLI) 提交的查詢中指定篩選條件。您也可以使用目前版本的其他AWS命令列工具或 AWS SDK，或直接將 HTTPS 要求傳送至 Macie 來執行此操作。如需AWS工具和 SDK 的相關資訊，請參閱要建置的工具。AWS

範例

- 範例 1：根據嚴重性篩選發現項目
- 範例 2：根據敏感資料類別篩選發現項目
- 範例 3：根據固定時間範圍篩選發現項目
- 範例 4：根據抑制狀態篩選搜尋結果
- 範例 5：根據多個欄位和值類型篩選發現項目

這些示例使用列表發現項目命令。如果範例成功執行，Macie 會傳回`findingIds`陣列。陣列會列出符合篩選準則之每個發現項目的唯一識別碼，如下列範例所示。

```
{
    "findingIds": [
        "1f1c2d74db5d8caa76859ec52example",
        "6cfa9ac820dd6d55cad30d851example",
        "702a6fd8750e567d1a3a63138example",
        "826e94e2a820312f9f964cf60example",
        "274511c3fdcd87010a19a3a42example"
    ]
}
```

如果沒有發現符合篩選條件，Macie 會傳回空`findingIds`陣列。

```
{
    "findingIds": []
}
```

範例 1：根據嚴重性篩選發現項目

此範例會使用清單發現項目命令，擷取目前所有高嚴重度和中等嚴重性發現項目的尋找項目 ID。AWS 區域

若為 Linux、macOS 或 Unix：

```
$ aws macie2 list-findings --finding-criteria '{"criterion":{"severity.description":
{"eq":["High","Medium"]}}}'
```

對於 Microsoft 視窗：

```
C:\> aws macie2 list-findings --finding-criteria={\"criterion\":
{\"severity.description\":{\"eq\":[\"High\",\"Medium\"]}}}
```

其中：

- *######*指定嚴重性欄位的 JSON 名稱。
- *eq* 指定等於運算符。
- 「*#*」和「*#*」是「嚴重性」欄位的列舉值陣列。

範例 2：根據敏感資料類別篩選發現項目

此範例使用 list find 命令擷取目前區域中所有敏感資料發現項目的尋找 ID，並報告 S3 物件中財務資訊 (以及沒有其他類別的敏感資料) 的發現情況。

對於 Linux、macOS 或 Unix，請使用反斜線 (\) 行接續字元來提高可讀性：

```
$ aws macie2 list-findings \
--finding-criteria '{"criterion":
{"classificationDetails.result.sensitiveData.category":{"eqExactMatch":
["FINANCIAL_INFORMATION"]}}}'
```

對於 Microsoft Windows，使用脫字符號 (^) 行繼續字符來提高可讀性：

```
C:\> aws macie2 list-findings ^
--finding-criteria={\"criterion\":
{\"classificationDetails.result.sensitiveData.category\":{\"eqExactMatch\":
[\"FINANCIAL_INFORMATION\"]}}}
```

其中：

- *######### ##########* JSON 名稱。
- *eqExactMatch*指定等於精確匹配運算符。
- *####*是敏感資料類別欄位的列舉值。

範例 3：根據固定時間範圍篩選發現項目

此範例會使用清單發現項目命令，擷取目前區域中所有發現項目的尋找 ID，這些項目是在 2020 年 10 月 5 日世界標準時間 07:00 和 2020 年 11 月 5 日世界標準時間 07:00 (包括在內) 之間建立的。

若為 Linux、macOS 或 Unix：

```
$ aws macie2 list-findings --finding-criteria '{"criterion":{"createdAt":
{"gte":1601881200000,"lte":1604559600000}}}'
```

對於 Microsoft 視窗：

```
C:\> aws macie2 list-findings --finding-criteria={\"criterion\":{\"createdAt\":
{\"gte\":1601881200000,\"lte\":1604559600000}}}
```

其中：

- 「*createdAt* 指定「建立於」欄位的 JSON 名稱。
- *gte* 指定大於或等於運算符。
- *1601881200000* 是時間範圍內的第一個日期和時間（以毫秒為單位的 Unix 時間戳記）。
- *LTE* 指定小於或等於運算符。
- *1604559600000* 是時間範圍內的最後一個日期和時間（以毫秒為單位的 Unix 時間戳記）。

範例 4：根據抑制狀態篩選搜尋結果

此範例使用清單發現項目命令，擷取目前「區域」中所有發現項目的尋找項目識別碼，並由抑制規則隱藏 (自動封存)。

若為 Linux、macOS 或 Unix：

```
$ aws macie2 list-findings --finding-criteria '{"criterion":{"archived":{"eq":
["true"]}}}'
```

對於 Microsoft 視窗：

```
C:\> aws macie2 list-findings --finding-criteria={\"criterion\":{\"archived\":{\"eq\":
[\"true\"]}}}
```

其中：

- *######*存欄位的 JSON 名稱。
- *eq* 指定等於運算符。
- *true* 是「已封存」欄位的布林值。

範例 5：根據多個欄位和值類型篩選發現項目

此範例使用清單搜尋結果命令來擷取目前區域中所有敏感資料發現項目的尋找 ID，且符合下列條件：建立於 2020 年 10 月 5 日 07:00 至 2020 年 11 月 5 日世界標準時間 07:00 (獨家)；報告財務資料的發現次數，且 S3 物件中沒有其他類別的敏感資料；並且不會透過抑制規則來抑制 (自動封存)。

對於 Linux、macOS 或 Unix，請使用反斜線 (\) 行接續字元來提高可讀性：

```
$ aws macie2 list-findings \
--finding-criteria '{"criterion":{"createdAt":
{"gt":1601881200000,"lt":1604559600000},"classificationDetails.result.sensitiveData.category":
{"eqExactMatch":["FINANCIAL_INFORMATION"]},"archived":{"eq":["false"]}}}'
```

對於 Microsoft Windows，使用脫字符號（^）行繼續字符來提高可讀性：

```
C:\> aws macie2 list-findings ^
--finding-criteria={\"criterion\":{\"createdAt\":{\"gt\":1601881200000,
\"lt\":1604559600000},\"classificationDetails.result.sensitiveData.category\":
{\"eqExactMatch\":[\"FINANCIAL_INFORMATION\"]},\"archived\":{\"eq\":[\"false\"]}}}
```

其中：

- *createdAt* 會指定 [建立於] 欄位的 JSON 名稱，並且：
  - *gt* 指定大於或等於運算符。
  - *1601881200000* 是時間範圍內的第一個日期和時間（以毫秒為單位的 Unix 時間戳記）。
  - *lt* 指定小於或等於運算符。
  - *1604559600000* 是時間範圍內的最後一個日期和時間（以毫秒為單位的 Unix 時間戳記）。
- *#########. ##################*欄位的 JSON 名稱，並且：
  - *eqExactMatch*指定等於精確匹配運算符。
  - *######*位的列舉值。
- *######*存欄位的 JSON 名稱，以及：
  - *eq* 指定等於運算符。
  - *#*是該字段的布爾值。

建立及管理發現項目的篩選規則

篩選規則是您建立並儲存的一組篩選條件，以便在 Amazon Macie 主控台上檢閱發現項目時再次使用。篩選規則可協助您對具有特定特性的發現項目執行一致的分析。例如，您可以建立一個篩選規則來分析所有包含未加密物件之 S3 儲存貯體的高嚴重性政策發現項目，以及另一個篩選規則，用於分析報告特定類型敏感資料的所有高嚴重性敏感資料發現項目。

請注意，篩選規則與隱藏規則不同。抑制規則是一組過濾條件，您可以建立並儲存，以自動將符合規則條件的發現項目存檔。雖然這兩種類型的規則都會儲存和套用篩選準則，但篩選規則不會對符合規則準

則的發現項目執行任何動作。相反地，篩選規則只會決定在您套用規則後，哪些發現項目會顯示在主控台上。如需有關抑制規則的資訊，請參閱隱藏問題清單。

若要建立和管理篩選規則，您可以使用 Amazon Macie 主控台或 Amazon Macie API。下列主題說明如何進行。對於 API，主題包括如何使用 AWS Command Line Interface(AWS CLI) 執行這些工作的範例。您也可以使用目前版本的其他AWS命令列工具或 AWS SDK，或直接將 HTTPS 要求傳送至 Macie 來執行這些工作。如需AWS工具和 SDK 的相關資訊，請參閱要建置的工具。AWS

主題

- 建立篩選規則
- 套用篩選規則
- 變更篩選規則
- 刪除篩選規則

建立篩選規則

建立篩選規則時，您可以指定篩選準則、名稱以及規則的描述 (選擇性)。您可以使用亞馬遜 Macie 控制台或亞馬 Amazon Macie API 創建一個過濾規則。

Console

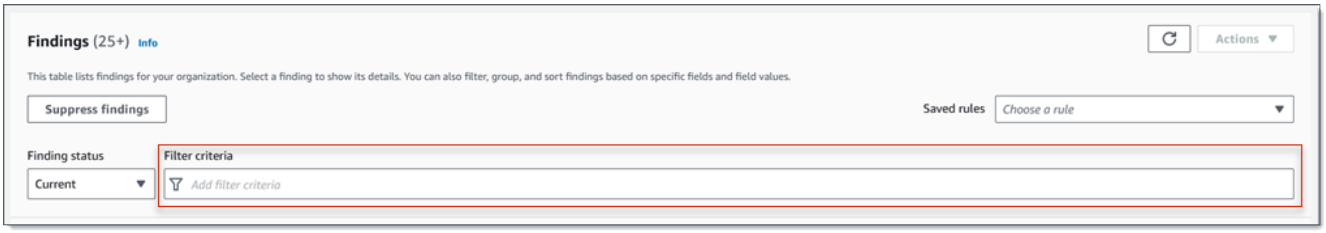
請依照下列步驟使用 Amazon Macie 主控台建立篩選規則。

建立篩選規則

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 在導覽窗格中，選擇 Findings (問題清單)。

> **Tip**
>
> 若要使用現有的篩選規則作為起點，請從「已儲存的規則」清單中選擇規則。
> 您也可以先依預先定義的邏輯群組樞紐和向下鑽研發現項目，藉此簡化規則的建立作業。如果您這麼做，Macie 會自動建立並套用適當的篩選條件，這對於建立規則很有幫助的起點。若要執行此操作，請在導覽窗格 (在「發現項目」下) 中選擇「依時段」、「依類型」或「依工作」，然後選擇表格中的項目。在詳細資料面板中，選擇要旋轉之欄位的連結。

3. 在「篩選準則」方塊中，新增定義規則篩選準則的條件。



若要瞭解如何新增篩選條件，請參閱建立並將篩選套用至發現項目。

4. 完成規則的篩選條件定義後，請在「篩選條件」方塊中選擇「儲存規則」。

5. 在「篩選規則」下，輸入規則的名稱，並選擇性地輸入規則的描述。
6. 選擇 儲存 。

API

若要以程式設計方式建立篩選規則，請使用 Amazon Macie API 的CreateFindingsFilter作業，並為所需參數指定適當的值：

- 對於`action`參數，請指定`NOOP`以確保 Macie 不會隱藏 (自動封存) 符合規則條件的發現項目。
- 對於`criterion`參數，請指定定義規則篩選準則的條件對映。

  在對映中，每個條件都應指定欄位、運算子以及欄位的一或多個值。值的類型和數目取決於您選擇的欄位和運算子。如需有關可在條件中使用之欄位、運算子和值類型的資訊，請參閱篩選發現項目的欄位在條件下使用運算子、和指定欄位的值。

若要使用建立篩選規則AWS CLI，請執行create-findings-filter命令並為所需參數指定適當的值。下列範例會建立篩選規則，此篩選規則會傳回目前所有敏感資料發現項目，以AWS 區域及報告 S3 物件中個人資訊 (且不包含其他類別的敏感資料)。

此範例針對 Linux、macOS 或 Unix 進行格式化，並使用反斜線 (\) 行接續字元來改善可讀性。

```
$ aws macie2 create-findings-filter \
--action NOOP \
```

```
--name my_filter_rule \
--finding-criteria '{"criterion":
{"classificationDetails.result.sensitiveData.category":{"eqExactMatch":
["PERSONAL_INFORMATION"]}}}'
```

此範例針對 Microsoft Windows 進行格式化，並使用脫字符號 (^) 行接續字元來提高可讀性。

```
C:\> aws macie2 create-findings-filter ^
--action NOOP ^
--name my_filter_rule ^
--finding-criteria={\"criterion\":
{\"classificationDetails.result.sensitiveData.category\":{\"eqExactMatch\":
[\"PERSONAL_INFORMATION\"]}}}
```

其中：

- *##########*。
- criterion是規則的篩選條件對映：
  - *#########. ############*欄位的 JSON 名稱。
  - *eqExactMatch*指定等於精確匹配運算符。
  - *####*是敏感資料類別欄位的列舉值。

如果此命令成功執行，您會收到類似如下的輸出。

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/9b2b4508-
aa2f-4940-b347-d1451example",
    "id": "9b2b4508-aa2f-4940-b347-d1451example"
}
```

其中arn是所建立之篩選規則的 Amazon 資源名稱 (ARN)，id是規則的唯一識別碼。

如需篩選準則的其他範例，請參閱使用 Amazon Macie API 以程式設計方式篩選結果。

套用篩選規則

套用篩選規則時，Amazon Macie 會使用規則的準則來決定要在主控台上的發現項目檢視中包含或排除哪些發現項目。Macie 也會顯示準則，以協助您判斷您套用的條件。

請注意，篩選規則是專為搭配 Amazon Macie 主控台使用而設計的。您無法在使用 Amazon Macie API 以程式設計方式提交的查詢中直接使用它們。但是，如果您使用 API 查詢發現項目，則可以使用該GetFindingsFilter操作來擷取規則的篩選準則。然後，您可以將條件添加到查詢中。如需有關在查詢中指定篩選條件的資訊，請參閱建立並將篩選套用至發現項目。

請遵循下列步驟，透過套用篩選規則來篩選主控台上的發現項目。

若要套用篩選規則

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 在導覽窗格中，選擇 Findings (問題清單)。
3. 在「已儲存的規則」清單中，選擇您要套用的篩選規則。Macie 會套用規則的準則，並在「篩選條件」方塊中顯示準則。
4. (選擇性) 若要細化準則，請使用「篩選條件」方塊來新增或移除篩選條件。如果您這麼做，您的變更不會影響規則的設定。除非您明確將它們保存為新規則，否則 Macie 不會保存任何更改。
5. 若要套用不同的篩選規則，請重複步驟 3。

套用篩選規則後，您可以在 [篩選條件] 方塊中選擇 [X]，快速從檢視中移除其所有篩選條件。

變更篩選規則

您可以隨時使用亞馬遜 Macie 主控台或亞馬 Amazon Macie API 來變更篩選規則的設定。您也可以指派和管理規則的標籤。

標籤是您定義並指派給特定AWS資源類型的標籤。每個標籤都包含必要的標籤鍵和一個可選的標籤值。標籤可協助您以不同的方式識別、分類及管理資源，例如依用途、擁有者、環境或其他條件。如需進一步了解，請參閱 標記亞馬遜麥西資源。

Console

請依照下列步驟使用 Amazon Macie 主控台變更現有篩選規則的設定。

變更篩選規則

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 在導覽窗格中，選擇 Findings (問題清單)。
3. 在「已存規則」清單中，選擇您要變更之篩選規則旁邊的編輯圖示 ( )。

4. 執行下列任何一項：

   - 若要變更規則的篩選條件，請使用「篩選條件」方塊來輸入所需準則的條件。如要瞭解如何作業，請參閱 建立並將篩選套用至發現項目。
   - 若要變更規則的名稱，請在「篩選規則」下的「名稱」方塊中輸入新名稱。
   - 若要變更規則的描述，請在「篩選規則」下的「描述」方塊中輸入新描述。
   - 若要指派、檢閱或編輯規則的標籤，請選擇「篩選規則」下的「管理標籤」。然後視需要檢閱並變更標籤。一個規則最多可以有 50 個標籤。

5. 完成變更之後，請選擇 Save (儲存)。

API

若要以程式設計方式變更篩選規則，請使用 Amazon Macie API 的UpdateFindingsFilter作業。當您提交請求時，請使用支援的參數為您要變更的每個設定指定新值。

針對id參數，指定要變更之規則的唯一識別碼。您可以使用ListFindingsFilter操作來擷取帳戶的篩選和抑制規則清單，以取得此識別碼。如果您使用的是AWS CLI，請執行list-findings-filters命令以擷取此清單。

若要使用變更篩選規則AWS CLI，請執行update-findings-filter命令並使用支援的參數為您要變更的每個設定指定新值。例如，下列命令會變更現有篩選規則的名稱。

```
C:\> aws macie2 update-findings-filter --id 9b2b4508-aa2f-4940-b347-d1451example --
name personal_information_only
```

其中：

- *##########*
- *########*新名稱。

如果此命令成功執行，您會收到類似如下的輸出。

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/9b2b4508-
aa2f-4940-b347-d1451example",
    "id": "9b2b4508-aa2f-4940-b347-d1451example"
}
```

其中arn是已變更之規則的 Amazon 資源名稱 (ARN)，id是規則的唯一識別碼。

同樣地，下列範例會將action參數的值從ARCHIVE變更為，將抑制規則轉換為篩選規則NOOP。

```
C:\> aws macie2 update-findings-filter --id 8a1c3508-aa2f-4940-b347-d1451example --
action NOOP
```

其中：

- *############*
- *NOOP* 是 Macie 對符合規則條件的發現項目執行的新動作 — 不執行任何動作 (不要隱藏發現項目)。

如果命令執行成功，您會收到類似下列內容的輸出：

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/8a1c3508-
aa2f-4940-b347-d1451example",
    "id": "8a1c3508-aa2f-4940-b347-d1451example"
}
```

其中arn是已變更之規則的 Amazon 資源名稱 (ARN)，id是規則的唯一識別碼。

刪除篩選規則

您可以隨時使用亞馬遜 Macie 控制台或亞馬 Amazon Macie API 刪除過濾器規則。

Console

請依照下列步驟使用 Amazon Macie 主控台刪除篩選規則。

刪除篩選規則

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 在導覽窗格中，選擇 Findings (問題清單)。
3. 在「已存規則」清單中，選擇您要刪除之篩選規則旁邊的編輯圖示 ( )。
4. 在「篩選規則」下選擇「刪除」。

API

若要以程式設計方式刪除篩選規則，請使用 Amazon Macie API 的DeleteFindingsFilter作業。針對id參數，指定要刪除之篩選規則的唯一識別碼。您可以使用ListFindingsFilter操作來擷取帳戶的篩選和抑制規則清單，以取得此識別碼。如果您使用的是AWS CLI，請執行list-findings-filters命令以擷取此清單。

若要使用刪除篩選規則AWS CLI，請執行delete-findings-filter命令。例如：

```
C:\> aws macie2 delete-findings-filter --id 9b2b4508-aa2f-4940-b347-d1451example
```

其中，*9b2b4508-A2F-4940-b* 347-d1451 範例是要刪除之篩選器規則的唯一識別碼。

如果命令運行成功，馬西返回一個空的 HTTP 200 響應。否則，馬西會傳回 HTTP 4 xx 或 500 回應，指出作業失敗的原因。

篩選發現項目的欄位

為了協助您更有效率地分析發現項目，Amazon Macie 主控台和 Amazon Macie API 可讓您存取數組欄位以篩選發現項目：

- 通用欄位 — 這些欄位儲存適用於任何類型尋找項目的資料。它們與發現項目的一般屬性 (例如嚴重性、尋找項目類型和尋找項目識別碼) 相關聯。
- 受影響的資源欄位 — 這些欄位會儲存有關發現項目套用之資源的資料，例如受影響 S3 儲存貯體或物件的名稱、標籤和加密設定。
- 原則欄位 — 這些欄位會儲存原則發現項目專屬的資料，例如產生尋找項目的動作，以及執行動作的實體。
- 敏感資料分類欄位 — 這些欄位儲存敏感資料發現項目專屬的資料，例如 Macie 在受影響的 S3 物件中找到的敏感資料的類別和類型。

篩選器可以使用任何先前集合中的欄位組合。

本節中的主題列出並說明您可以用來篩選發現項目的個別欄位。如需有關這些欄位的其他詳細資訊，包括欄位之間的任何關係，請參閱 Amazon Macie API 參考中的發現項目。

主題

- 常用欄位
- 受影響資源欄位

- 原則欄位
- 敏感資料分類欄位

常用欄位

下表列出並說明您可以用來根據一般發現項目屬性篩選發現項目的欄位。這些欄位會儲存適用於任何尋找項目類型的資料。

在表格中，「欄位」 欄會指出 Amazon Macie 主控台上欄位的名稱。JSON 欄位資料行使用點標記法來指出發現項目的 JSON 表示法和 Amazon Macie API 中的欄位名稱。「描述」欄提供欄位儲存之資料的簡短描述，並指出篩選器值的任何需求。該表格按字段的字母升序排序，然後按 JSON 字段排序。

欄位	JSON 欄位	描述
帳戶識別碼 *	`accountId`	適用於發現項目AWS 帳戶的唯一識別碼。這通常是擁有受影響資源的帳號。
—	`archived`	Boolean 值，指定是否由抑制規則抑制 (自動封存) 尋找項目。 若要在主控台的篩選器中使用此欄位，請在「尋找項目」狀態功能表上選擇一個選項：「已封存」(僅限隱藏)、「目前」(僅限取消抑制) 或「全部」(抑制和取消抑制)。
類別	`category`	發現項目的類別。 當您將此欄位新增至篩選器時，主控台會提供可供選擇的值清單。在 API 中，對於敏感資料發現項目`CLASSIFICATION` ，有效值為:；以及`POLICY`，用於政策發現項目。

欄位	JSON 欄位	描述
—	`count`	發現項目的出現次數總計。對於敏感資料發現項目，此值一律為1。所有敏感資料發現都被視為是唯一的。 主控台上無法使用此欄位做為篩選選項。透過 API，您可以使用此欄位定義篩選器的數值範圍。
建立於	`createdAt`	Macie 建立搜尋結果的日期和時間。 您可以使用此欄位來定義篩選的時間範圍。
尋找識別碼 *	`id`	發現項目的唯一識別碼。這是 Macie 在創建發現項目時生成並分配給發現的隨機字符串。
尋找類型 *	`type`	尋找的類型 — 例如，或。`SensitiveData:S3Object/Personal` `Policy:IAMUser/S3BucketPublic` 當您將此欄位新增至篩選器時，主控台會提供可供選擇的值清單。如需 API 中有效值的清單，請參閱FindingType亞 Amazon Macie API 參考中的。
區域	`region`	AWS 區域該 Macie 在中創建了發現項目-例如，或。`us-east-1` `ca-central-1`

欄位	JSON 欄位	描述
樣本	`sample`	Boolean 值；指定發現項目是否為範例發現項目。範例發現項目是使用範例資料和預留位置值來示範發現項目可能包含哪些項目的發現項目。 當您將此欄位新增至篩選器時，主控台會提供可供選擇的值清單。
嚴重性	`severity.description`	發現項目嚴重性的定性表示。 當您將此欄位新增至篩選器時，主控台會提供可供選擇的值清單。在 API 中，有效值為：`Low`、`Medium`、和`High`。
更新時間	`updatedAt`	上次更新發現項目的日期和時間。對於敏感資料發現項目，此值與 [建立於] 欄位的值相同。所有敏感數據發現都被視為新的（唯一）。 您可以使用此欄位來定義篩選的時間範圍。

* 若要在主控台上為此欄位指定多個值，請新增使用欄位並為篩選器指定不同值的條件，然後針對每個其他值重複該步驟。要使用 API 執行此操作，請使用列出用於過濾器的值的數組。

受影響資源欄位

下列主題列出並說明您可以根據發現項目套用的資源來篩選發現項目的欄位。主題依資源類型進行組織。

主題

- S3 儲存貯體

- S3 物件

S3 儲存貯體

下表列出並說明可用來根據發現項目套用之 S3 儲存貯體特性篩選發現項目的欄位。

在表格中，「欄位」 欄會指出 Amazon Macie 主控台上欄位的名稱。JSON 欄位資料行使用點標記法來指出發現項目的 JSON 表示法和 Amazon Macie API 中的欄位名稱。較長的 JSON 欄位名稱會使用換行字元序列 (\ n) 來提高可讀性。) 「描述」欄提供欄位儲存之資料的簡短描述，並指出篩選器值的任何需求。該表格按字段的字母升序排序，然後按 JSON 字段排序。

欄位	JSON 欄位	描述
—	`resourcesAffected.s3Bucket.createdAt`	建立受影響值區的日期和時間，或是最近對受影響值區進行的變更 (例如編輯值區政策)。 主控台上無法使用此欄位做為篩選選項。透過 API，您可以使用此欄位來定義篩選器的時間範圍。
S3 儲存貯體預設加密	`resourcesAffected.s3Bucket.defaultServerSideEncryption.encryptionType`	預設會用來加密新增至受影響值區的物件的伺服器端加密演算法。 當您將此欄位新增至篩選器時，主控台會提供可供選擇的值清單。如需 API 的有效值清單，請參閱EncryptionType亞 Amazon Macie API 參考中的。
S3 儲存貯體加密 KMS 金鑰識別碼 *	`resourcesAffected.s3Bucket.defaultSe`	預設用於加密新增至受影響值區的物件的 Amazon 資源名

欄位	JSON 欄位	描述
	`rverSideEncryption.kmsMasterKeyId`	稱 (ARN) 或唯一識別碼 (金鑰 ID)。AWS KMS key
儲存貯體政策所要求的 S3 儲存貯體	`resourcesAffected.s3Bucket.allowsUnencryptedObjectUploads`	指定將物件新增至值區時，受影響值區的儲存貯體政策是否需要對物件進行伺服器端加密。 當您將此欄位新增至篩選器時，主控台會提供可供選擇的值清單。如需 API 的有效值清單，請參閱 Amazon Macie API 參考中的 S3Bucket。
S3 儲存貯體名稱 *	`resourcesAffected.s3Bucket.name`	受影響值區的完整名稱。
S3 儲存貯體擁有者顯示名稱 *	`resourcesAffected.s3Bucket.owner.displayName`	擁有受影響值區之AWS使用者的顯示名稱。
S3 儲存貯體公開存取權限	`resourcesAffected.s3Bucket.publicAccess.effectivePermission`	根據套用至值區的權限設定組合，指定受影響的值區是否可公開存取。 當您將此欄位新增至篩選器時，主控台會提供可供選擇的值清單。如需 API 的有效值清單，請參閱BucketPublicAccess亞 Amazon Macie API 參考中的。

欄位	JSON 欄位	描述
—	resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n accountLevelPermissions.blockPublicAccess.blockPublicAcls	布林值，指定 Amazon S3 是否封鎖受影響儲存貯體和儲存貯體中物件的公開存取控制清單 (ACL)。這是值區的帳戶層級封鎖公開存取設定。 主控台上無法使用此欄位做為篩選選項。
—	resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n accountLevelPermissions.blockPublicAccess.blockPublicPolicy	布林值，指定 Amazon S3 是否封鎖受影響儲存貯體的公有儲存貯體政策。這是值區的帳戶層級封鎖公開存取設定。 主控台上無法使用此欄位做為篩選選項。
—	resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n accountLevelPermissions.blockPublicAccess.ignorePublicAcls	布林值，指定 Amazon S3 是否忽略受影響儲存貯體和儲存貯體中物件的公有 ACL。這是值區的帳戶層級封鎖公開存取設定。 主控台上無法使用此欄位做為篩選選項。

欄位	JSON 欄位	描述
—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n accountLevelPermissions.blockPublicAccess.restrictPublicBuckets`	布林值，指定 Amazon S3 是否限制受影響儲存貯體的公有儲存貯體政策。這是值區的帳戶層級封鎖公開存取設定。 主控台上無法使用此欄位做為篩選選項。
—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n bucketLevelPermissions.accessControlList.allowsPublicReadAccess`	Boolean 值；指定受影響值區的儲存貯體層級 ACL 是否授與具有值區讀取存取權限的一般大眾。 主控台上無法使用此欄位做為篩選選項。
—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n bucketLevelPermissions.accessControlList.allowsPublicWriteAccess`	Boolean 值；指定受影響值區的儲存貯體層級 ACL 是否授與具有值區寫入存取權限的一般大眾。 主控台上無法使用此欄位做為篩選選項。

欄位	JSON 欄位	描述
—	resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n bucketLevelPermissions.blockPublicAccess.blockPublicAcls	布林值，指定 Amazon S3 是否封鎖受影響儲存貯體和儲存貯體中物件的公有 ACL。這是值區的值區層級的區塊公用存取設定。 主控台上無法使用此欄位做為篩選選項。
—	resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n bucketLevelPermissions.blockPublicAccess.blockPublicPolicy	布林值，指定 Amazon S3 是否封鎖受影響儲存貯體的公有儲存貯體政策。這是值區的值區層級的區塊公用存取設定。 主控台上無法使用此欄位做為篩選選項。
—	resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n bucketLevelPermissions.blockPublicAccess.ignorePublicAcls	布林值，指定 Amazon S3 是否忽略受影響儲存貯體和儲存貯體中物件的公有 ACL。這是值區的值區層級的區塊公用存取設定。 主控台上無法使用此欄位做為篩選選項。

欄位	JSON 欄位	描述
—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n bucketLevelPermissions.blockPublicAccess.restrictPublicBuckets`	布林值，指定 Amazon S3 是否限制受影響儲存貯體的公有儲存貯體政策。這是值區的值區層級的區塊公用存取設定。 主控台上無法使用此欄位做為篩選選項。
—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n bucketLevelPermissions.bucketPolicy.allowsPublicReadAccess`	Boolean 值，指定受影響值區的政策是否允許一般大眾擁有值區的讀取權限。 主控台上無法使用此欄位做為篩選選項。
—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n bucketLevelPermissions.bucketPolicy.allowsPublicWriteAccess`	Boolean 值；指定受影響值區的政策是否允許一般大眾擁有值區的寫入存取權。 主控台上無法使用此欄位做為篩選選項。
S3 儲存貯體標籤鍵 *	`resourcesAffected.s3Bucket.tags.key`	與受影響值區相關聯的標籤金鑰。
S3 儲存貯體標籤值 *	`resourcesAffected.s3Bucket.tags.value`	與受影響值區相關聯的標籤值。

* 若要在主控台上為此欄位指定多個值，請新增使用欄位並為篩選器指定不同值的條件，然後針對每個其他值重複該步驟。要使用 API 執行此操作，請使用列出用於過濾器的值的數組。

S3 物件

下表列出並說明可用來根據發現項目套用之 S3 物件特性篩選發現項目的欄位。

在表格中，「欄位」 欄會指出 Amazon Macie 主控台上欄位的名稱。JSON 欄位資料行使用點標記法來指出發現項目的 JSON 表示法和 Amazon Macie API 中的欄位名稱。「描述」欄提供欄位儲存之資料的簡短描述，並指出篩選器值的任何需求。該表格按字段的字母升序排序，然後按 JSON 字段排序。

欄位	JSON 欄位	描述
S3 物件加密 KMS 金鑰識別碼 *	`resourcesAffected.s3Object.serverSideEncryption.kmsMasterKeyId`	用於加密受影響物件的 Amazon 資源名稱 (ARN) 或唯 AWS KMS key一識別碼 (金鑰 ID)。
S3 物件加密類型	`resourcesAffected.s3Object.serverSideEncryption.encryptionType`	用來加密受影響物件的伺服器端加密演算法。 當您將此欄位新增至篩選器時，主控台會提供可供選擇的值清單。如需 API 的有效值清單，請參閱EncryptionType亞 Amazon Macie API 參考中的。
—	`resourcesAffected.s3Object.extension`	受影響物件的副檔名。對於沒有副檔名的物件，請指定""為篩選器的值。 主控台上無法使用此欄位做為篩選選項。

欄位	JSON 欄位	描述
—	`resourcesAffected.s3Object.lastModified`	建立或上次變更受影響物件的日期和時間，以最新日期為準。 主控台上無法使用此欄位做為篩選選項。透過 API，您可以使用此欄位來定義篩選器的時間範圍。
S3 物件金鑰 *	`resourcesAffected.s3Object.key`	受影響物件的全名 (key)，包括物件的前置詞 (如果適用)。
—	`resourcesAffected.s3Object.path`	受影響物件的完整路徑，包括受影響值區的名稱和物件的名稱 (機碼)。 主控台上無法使用此欄位做為篩選選項。
S3 物件公開存取	`resourcesAffected.s3Object.publicAccess`	Boolean 值；根據套用至物件的權限設定組合，指定受影響物件是否可公開存取。 當您將此欄位新增至篩選器時，主控台會提供可供選擇的值清單。
S3 物件標籤金鑰 *	`resourcesAffected.s3Object.tags.key`	與受影響物件相關聯的標籤索引鍵。
S3 物件標籤值 *	`resourcesAffected.s3Object.tags.value`	與受影響物件相關聯的標籤值。

* 若要在主控台上為此欄位指定多個值，請新增使用欄位並為篩選器指定不同值的條件，然後針對每個其他值重複該步驟。要使用 API 執行此操作，請使用列出用於過濾器的值的數組。

原則欄位

下表列出並說明可用來篩選原則發現項目的欄位。這些欄位會儲存原則發現項目特有的資料。

在表格中，「欄位」 欄會指出 Amazon Macie 主控台上欄位的名稱。JSON 欄位資料行使用點標記法來指出發現項目的 JSON 表示法和 Amazon Macie API 中的欄位名稱。較長的 JSON 欄位名稱會使用換行字元序列 (\ n) 來提高可讀性。) 「描述」欄提供欄位儲存之資料的簡短描述，並指出篩選器值的任何需求。該表格按字段的字母升序排序，然後按 JSON 字段排序。

欄位	JSON 欄位	描述
動作類型	`policyDetails.action.actionType`	產生發現項目的動作類型。此欄位的唯一有效值為`AWS_API_CALL` 。
API 呼叫名稱 *	`policyDetails.action.apiCallDetails.api`	最近呼叫並產生尋找的作業名稱，例如，。`PutBucketPublicAccessBlock`
API 服務名稱 *	`policyDetails.action.apiCallDetails.apiServiceName`	提供呼叫並產生尋找之作業的 URL，例如，。AWS 服務`s3.amazonaws.com`
—	`policyDetails.action.apiCallDetails.firstSeen`	呼叫任何作業並產生搜尋結果的第一個日期與時間。 主控台上無法使用此欄位做為篩選選項。透過 API，您可以使用此欄位來定義篩選器的時間範圍。
—	`policyDetails.action.apiCallDetails.lastSeen`	呼叫指定作業 (API 呼叫名稱或`api`) 並產生發現項目的最新日期和時間。 主控台上無法使用此欄位做為篩選選項。透過 API，您可以

欄位	JSON 欄位	描述
		使用此欄位來定義篩選器的時間範圍。
—	`policyDetails.actor.domainDetails.domainName`	用來執行動作之裝置的網域名稱。 主控台上無法使用此欄位做為篩選選項。
知识产权城市 *	`policyDetails.actor.ipAddressDetails.ipCity.name`	用來執行動作之裝置 IP 位址的起始城市名稱。
IP 國家/地區 *	`policyDetails.actor.ipAddressDetails.ipCountry.name`	用來執行動作之裝置 IP 位址的原始國家/地區名稱，例如。`United States`
—	`policyDetails.actor.ipAddressDetails.ipOwner.asn`	自治系統的自治系統編號 (ASN)，其中包含用來執行動作之裝置的 IP 位址。 主控台上無法使用此欄位做為篩選選項。
IP 擁有者出貨預先通知組織 *	`policyDetails.actor.ipAddressDetails.ipOwner.asnOrg`	與自治系統之 ASN 相關聯的組織識別碼，其中包含用來執行動作之裝置的 IP 位址。
IP 擁有者 ISP *	`policyDetails.actor.ipAddressDetails.ipOwner.isp`	擁有用來執行動作之裝置 IP 位址的網際網路服務提供者 (ISP) 名稱。
IP V4 位址 *	`policyDetails.actor.ipAddressDetails.ipAddressV4`	用來執行動作之裝置的網際網路通訊協定第 4 版 (IPv4) 位址。

欄位	JSON 欄位	描述
—	`policyDetails.actor.userIdentity.assumedRole.accessKeyId`	對於使用使用 AWS STS API 作業取得的臨時安全登入資料執行的動`AssumeRole` 作，即識別認證的AWS存取金鑰 ID。 主控台上無法使用此欄位做為篩選選項。
使用者身分假設角色帳號 id *	`policyDetails.actor.userIdentity.assumedRole.accountId`	對於使用使用 AWS STS API 作業取得的臨時安全性認證執行的動`AssumeRole` 作，即擁有用於取得認證之實體的唯一識別碼。AWS 帳戶
使用者識別假定為角色主體 id *	`policyDetails.actor.userIdentity.assumedRole.principalId`	對於使用使用 AWS STS API 作業取得的臨時安全登入資料執行的動`AssumeRole` 作，也就是用來取得認證之實體的唯一識別碼。
使用者身分假設角色工作階段 ARN*	`policyDetails.actor.userIdentity.assumedRole.arn`	對於使用使用 AWS STS API 作業取得的臨時安全登入資料執行的動`AssumeRole` 作，請參閱來源帳戶的 Amazon 資源名稱 (ARN)、IAM 使用者或用來取得登入資料的角色。

—	`policyDetails.actor.userIdentity.assumedRole.sessionContext.\n`
	
	`sessionIssuer.type`
		對於使用使用 AWS STS API 作業取得的臨時安全登入資料執行的動`AssumeRole` 作，臨時安全登入資料的來源 — 例如`RootIAMUser`、、或`Role`。
		
		主控台上無法使用此欄位做為篩選選項。

欄位	JSON 欄位	描述
—	`policyDetails.actor.userIdentity.assumedRole.sessionContext.\n sessionIssuer.userName`	針對使用 AWS STS API 作業取得的臨時安全性認證執行的動`AssumeRole` 作，也就是發出工作階段之使用者或角色的名稱或別名。請注意，如果認證是從沒有別名的根帳戶取得，則此值為 null。 主控台上無法使用此欄位做為篩選選項。
使用者身分識別AWS帳號 ID *	`policyDetails.actor.userIdentity.awsAccount.accountId`	對於使用另一個認證執行的動作AWS 帳戶，即帳戶的唯一識別碼。
使用者身分AWS帳戶主要 ID *	`policyDetails.actor.userIdentity.awsAccount.principalId`	對於使用另一個認證執行的動作AWS 帳戶，即執行動作之實體的唯一識別碼。
呼叫的使用者識別AWS服務	`policyDetails.actor.userIdentity.awsService.invokedBy`	對於屬於服務名稱的帳戶所執行的動作。AWS 服務
—	`policyDetails.actor.userIdentity.federatedUser.accessKeyId`	對於使用使用 AWS STS API 作業取得的臨時安全登入資料執行的動`GetFederationToken` 作，即識別認證的AWS存取金鑰 ID。 主控台上無法使用此欄位做為篩選選項。

欄位	JSON 欄位	描述
使用者身分同盟工作階段 ARN*	`policyDetails.actor.userIdentity.federatedUser.arn`	對於使用使用 AWS STS API `GetFederationToken` 操作（用於獲取憑據的實體的 ARN）獲取的臨時安全憑據執行的操作。
使用者身分識別聯合使用者帳號 id *	`policyDetails.actor.userIdentity.federatedUser.accountId`	對於使用使用 AWS STS API 作業取得的臨時安全性認證執行的動`GetFederationToken` 作，即擁有用於取得認證之實體的唯一識別碼。AWS 帳戶
使用者識別身分同盟使用者主體 id *	`policyDetails.actor.userIdentity.federatedUser.principalId`	對於使用使用 AWS STS API 作業取得的臨時安全登入資料執行的動`GetFederationToken` 作，也就是用來取得認證之實體的唯一識別碼。

—	`policyDetails.actor.userIdentity.federatedUser.sessionContext.\n`
	
	`sessionIssuer.type`
		對於使用使用 AWS STS API 作業取得的臨時安全登入資料執行的動`GetFederationToken` 作，即臨時安全性憑證的來源，例如`Root`、`IAMUser`或。`Role`
		
		主控台上無法使用此欄位做為篩選選項。

欄位	JSON 欄位	描述
—	policyDetails.actor.userIdentity.federatedUser.sessionContext.\n sessionIssuer.userName	針對使用 AWS STS API 作業取得的臨時安全性認證執行的動GetFederationToken 作，也就是發出工作階段之使用者或角色的名稱或別名。請注意，如果認證是從沒有別名的根帳戶取得，則此值為 null。 主控台上無法使用此欄位做為篩選選項。
使用者身分 IAM 帳戶識別碼 *	policyDetails.actor.userIdentity.iamUser.accountId	對於使用 IAM 使用者的登入資料執行的動作，則為與執行 AWS 帳戶該動作的 IAM 使用者相關聯的唯一識別碼。
使用者身分 IAM 主體識別碼 *	policyDetails.actor.userIdentity.iamUser.principalId	對於使用 IAM 使用者登入資料執行的動作，則為執行該動作的 IAM 使用者的唯一識別碼。
使用者身分 IAM 使用者名稱 *	policyDetails.actor.userIdentity.iamUser.userName	對於使用 IAM 使用者登入資料執行的動作，即執行該動作的 IAM 使用者的使用者名稱。
使用者身分根帳號 ID *	policyDetails.actor.userIdentity.root.accountId	針對使用您的認證執行的動作 AWS 帳戶，即帳戶的唯一識別碼。
使用者識別根主體 id *	policyDetails.actor.userIdentity.root.principalId	對於使用您的認證執行的動作 AWS 帳戶，即執行動作之實體的唯一識別元。

欄位	JSON 欄位	描述
使用者身分類型	`policyDetails.actor.userIdentity.type`	執行產生發現項目之動作的實體類型。 當您將此欄位新增至篩選器時，主控台會提供可供選擇的值清單。如需 API 的有效值清單，請參閱UserIdentityType亞 Amazon Macie API 參考中的。

* 若要在主控台上為此欄位指定多個值，請新增使用欄位並為篩選器指定不同值的條件，然後針對每個其他值重複該步驟。要使用 API 執行此操作，請使用列出用於過濾器的值的數組。

敏感資料分類欄位

下表列出並說明可用來篩選機密資料發現項目的欄位。這些欄位會儲存敏感資料發現項目特有的資料。

在表格中，「欄位」 欄會指出 Amazon Macie 主控台上欄位的名稱。JSON 欄位資料行使用點標記法來指出發現項目的 JSON 表示法和 Amazon Macie API 中的欄位名稱。「描述」欄提供欄位儲存之資料的簡短描述，並指出篩選器值的任何需求。該表格按字段的字母升序排序，然後按 JSON 字段排序。

欄位	JSON 欄位	描述
自訂資料識別碼 ID *	`classificationDetails.result.customDataIdentifiers.detections.arn`	偵測資料並產生發現項目的自訂資料識別碼的唯一識別碼。
自訂資料識別碼名稱 *	`classificationDetails.result.customDataIdentifiers.detections.name`	偵測資料並產生尋找項目的自訂資料識別碼名稱。

欄位	JSON 欄位	描述
自訂資料識別碼總數	classificationDetails.result.customDataIdentifiers.detections.count	由自訂資料識別碼偵測並產生發現項目的資料出現次數總數。 您可以使用此欄位來定義篩選的數值範圍。
Job 識別碼 *	classificationDetails.jobId	產生發現項目之機密資料探索工作的唯一識別碼。
原點類型	classificationDetails.originType	Macie 如何找到產生發現項目的敏感資料：AUTOMATED_SENSITIVE_DATA_DISCOVERY 或SENSITIVE_DATA_DISCOVERY_JOB 。
—	classificationDetails.result.mimeType	發現項目適用於 MIME 類型的內容類型，text/csv例如 CSV 檔案或 application/pdf Adobe 可攜式文件格式檔案。 主控台上無法使用此欄位做為篩選選項。
—	classificationDetails.result.sizeClassified	發現項目套用之 S3 物件的儲存大小總計 (以位元組為單位)。 主控台上無法使用此欄位做為篩選選項。透過 API，您可以使用此欄位定義篩選器的數值範圍。

欄位	JSON 欄位	描述
結果狀態碼 *	`classificationDetails.result.status.code`	發現項目的狀態。有效的 值如下： • COMPLETE— Macie 完成了對對象的分析。 • PARTIAL— Macie 只分析了物件中資料的子集。例如，物件是一個封存檔案，其中包含不支援格式的檔案。 • SKIPPED— 馬西不能夠分析對象. 例如，物件是格式錯誤的檔案。
敏感資料類別	`classificationDetails.result.sensitiveData.category`	偵測到並產生發現項目的敏感資料類別。 當您將此欄位新增至篩選器時，主控台會提供可供選擇的值清單。在 API 中，有效值為：CREDENTIALS FINANCIAL_INFORMATION 、和PERSONAL_INFORMATION 。
敏感資料偵測類型	`classificationDetails.result.sensitiveData.detections.type`	偵測到並產生發現項目的敏感資料類型。 當您將此欄位新增至篩選器時，主控台會提供可供選擇的值清單。如需主控台和 API 的有效值清單，請參閱敏感資料偵測類型。

欄位	JSON 欄位	描述
敏感資料總數	`classificationDetails.result.sensitiveData.detections.count`	偵測到並產生發現項目之機密資料的出現次數總計。 您可以使用此欄位來定義篩選的數值範圍。

* 若要在主控台上為此欄位指定多個值，請新增使用欄位並為篩選器指定不同值的條件，然後針對每個其他值重複該步驟。要使用 API 執行此操作，請使用列出用於過濾器的值的數組。

敏感資料偵測類型

下列主題列出您可以在篩選器中為「機密資料偵測類型」欄位指定的值。(此欄位的 JSON 名稱為`classificationDetails.result.sensitiveData.detections.type`。) 這些主題是根據 Macie 可以使用受管理資料識別碼偵測的敏感資料類別進行組織。

類別

- 登入資料
- 財務資訊
- 個人信息：個人健康信息（PHI）
- 個人資訊：個人識別資訊 (PII)

若要深入瞭解特定類型敏感資料的受管理資料識別碼，請參閱詳細參考資料：Amazon Macie 受管資料識別碼。

登入資料

您可以指定下列值來篩選報告 S3 物件中登入資料資料出現的發現項目。

敏感資料類型	過濾器值
AWS 私密存取金鑰	`AWS_CREDENTIALS`
谷歌雲 API 密鑰	`GCP_API_KEY`
HTTP 基本授權標頭	`HTTP_BASIC_AUTH_HEADER`

敏感資料類型	過濾器值
網絡令牌	JSON_WEB_TOKEN
OpenSSH 私密金鑰	OPENSSH_PRIVATE_KEY
PGP 私密金鑰	PGP_PRIVATE_KEY
公開金鑰加密標準 (PKCS) 私密金鑰	PKCS
PuTTY 私密金鑰	PUTTY_PRIVATE_KEY
條紋 API 金鑰	STRIPE_CREDENTIALS

財務資訊

您可以指定下列值來篩選報告 S3 物件中財務資訊出現次數的發現項目。

敏感資料類型	過濾器值
銀行帳戶號碼	BANK_ACCOUNT_NUMBER （適用於加拿大和美國）
基本銀行帳戶號碼	取決於國家或地區：FRANCE_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, ITALY_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER
信用卡到期日	CREDIT_CARD_EXPIRATION
信用卡磁條數據	CREDIT_CARD_MAGNETIC_STRIPE
信用卡號碼	CREDIT_CARD_NUMBER (適用於鄰近關鍵字的信用卡號碼)、CREDIT_CARD_NUMBER_(NO_KEYWORD) (適用於不在關鍵字附近的信用卡號碼)

敏感資料類型	過濾器值
信用卡驗證碼	CREDIT_CARD_SECURITY_CODE

敏感資料類型	過濾器值
國際銀行帳戶號碼	視國家或地區而定：ALBANIA_BANK_ACCOUNT_NUMBER, ANDORRA_BANK_ACCOUNT_NUMBER, BOSNIA_AND_HERZEGOVINA_BANK_ACCOUNT_NUMBER, BRAZIL_BANK_ACCOUNT_NUMBER, BULGARIA_BANK_ACCOUNT_NUMBER, COSTA_RICA_BANK_ACCOUNT_NUMBER, CROATIA_BANK_ACCOUNT_NUMBER, CYPRUS_BANK_ACCOUNT_NUMBER, CZECH_REPUBLIC_BANK_ACCOUNT_NUMBER, DENMARK_BANK_ACCOUNT_NUMBER, DOMINICAN_REPUBLIC_BANK_ACCOUNT_NUMBER, EGYPT_BANK_ACCOUNT_NUMBER, ESTONIA_BANK_ACCOUNT_NUMBER, FAROE_ISLANDS_BANK_ACCOUNT_NUMBER, FINLAND_BANK_ACCOUNT_NUMBER, FRANCE_BANK_ACCOUNT_NUMBER, GEORGIA_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, GREECE_BANK_ACCOUNT_NUMBER, GREENLAND_BANK_ACCOUNT_NUMBER, HUNGARY_BANK_ACCOUNT_NUMBER, ICELAND_BANK_ACCOUNT_NUMBER, IRELAND_BANK_ACCOUNT_NUMBER, ITALY_BANK_ACCOUNT_NUMBER, JORDAN_BANK_ACCOUNT_NUMBER, KOSOVO_BANK_ACCOUNT_NUMBER, LIECHTENSTEIN_BANK_ACCOUNT_NUMBER, LITHUANIA_BANK_ACCOUNT_NUMBER, MALTA_BANK_ACCOUNT_NUMBER, MAURITANIA_BANK_ACCOUNT_NUMBER, MA

敏感資料類型	過濾器值
	URITIUS_BANK_ACCOUNT_NUMBER , MONACO_BANK_ACCOUNT_NUMBER, MONTENEGRO_BANK_ACCOUNT_N UMBER, NETHERLANDS_BANK_AC COUNT_NUMBER, NORTH_MACEDO NIA_BANK_ACCOUNT_NUMBER, P OLAND_BANK_ACCOUNT_NUMBER, PORTUGAL_BANK_ACCOUNT_NUMBER, SAN_MARINO_BANK_ACCOUNT_NUMBER, SENEGAL_BANK_ACCOUNT_NUMBER, SERBIA_BANK_ACCOUNT_NUMBER, SLOVAKIA_BANK_ACCOUNT_NUMBER, SLOVENIA_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, SWEDEN_BANK_ACCOUNT_NUMBER , SWITZERLAND_BANK_ACCOUNT_NU MBER, TIMOR_LESTE_BANK_ACC OUNT_NUMBER, TUNISIA_BANK_ ACCOUNT_NUMBER, TURKIYE_B ANK_ACCOUNT_NUMBER, UK_BAN K_ACCOUNT_NUMBER, UKRAINE_B ANK_ACCOUNT_NUMBER, UNITED _ARAB_EMIRATES_BANK_ACCOUNT _NUMBER, VIRGIN_ISLANDS_BA NK_ACCOUNT_NUMBER （適用於英屬維爾京群島）

個人信息：個人健康信息（PHI）

您可以指定下列值來篩選報告 S3 物件中個人健康資訊 (PHI) 出現的發現項目。

敏感資料類型	過濾器值
毒品執法機構 (DEA) 註冊號碼	US_DRUG_ENFORCEMENT_AGENCY_NUMBER
Health 保險索償編號	USA_HEALTH_INSURANCE_CLAIM_NUMBER
健康保險或醫療識別號碼	取決於國家或地區：CANADA_HEALTH_NUMBER, EUROPEAN_HEALTH_INSURANCE_CARD_NUMBER, FINLAND_EUROPEAN_HEALTH_INSURANCE_NUMBER, FRANCE_HEALTH_INSURANCE_NUMBER, UK_NHS_NUMBER, USA_MEDICARE_BENEFICIARY_IDENTIFIER
醫療保健通用程序編碼系統 (HCPCS) 代碼	USA_HEALTHCARE_PROCEDURE_CODE
美国国家药品法典	USA_NATIONAL_DRUG_CODE
國家供應商識別碼 (NPI)	USA_NATIONAL_PROVIDER_IDENTIFIER
唯一裝置識別碼 (UDI)	MEDICAL_DEVICE_UDI

個人資訊：個人識別資訊 (PII)

您可以指定下列值來篩選報告 S3 物件中個人識別資訊 (PII) 出現的發現項目。

敏感資料類型	過濾器值
出生日期	DATE_OF_BIRTH
駕照識別號碼	取決於國家或地區：AUSTRALIA_DRIVERS_LICENSE, AUSTRIA_DRIVERS_LICENSE, BELGIUM_DRIVERS_LICENSE, BULGARIA_DRIVERS_LICENSE, CANADA_DRIVERS_LICENSE,

敏感資料類型	過濾器值
	CROATIA_DRIVERS_LICENSE, CYPRUS_DRIVERS_LICENSE, CZECHIA_DRIVERS_LICENSE, DENMARK_DRIVERS_LICENSE, DRIVERS_LICENSE （適用於美國），ESTONIA_DRIVERS_LICENSE, FINLAND_DRIVERS_LICENSE, FRANCE_DRIVERS_LICENSE, GERMANY_DRIVERS_LICENSE, GREECE_DRIVERS_LICENSE, HUNGARY_DRIVERS_LICENSE, INDIA_DRIVERS_LICENSE, IRELAND_DRIVERS_LICENSE, ITALY_DRIVERS_LICENSE, LATVIA_DRIVERS_LICENSE, LITHUANIA_DRIVERS_LICENSE, LUXEMBOURG_DRIVERS_LICENSE, MALTA_DRIVERS_LICENSE, NETHERLANDS_DRIVERS_LICENSE, POLAND_DRIVERS_LICENSE, PORTUGAL_DRIVERS_LICENSE, ROMANIA_DRIVERS_LICENSE, SLOVAKIA_DRIVERS_LICENSE, SLOVENIA_DRIVERS_LICENSE, SPAIN_DRIVERS_LICENSE, SWEDEN_DRIVERS_LICENSE, UK_DRIVERS_LICENSE
選民名冊號碼	UK_ELECTORAL_ROLL_NUMBER
全名	NAME
全球定位系統 (GPS) 座標	LATITUDE_LONGITUDE
餅乾	HTTP_COOKIE
郵寄地址	ADDRESS, BRAZIL_CEP_CODE

敏感資料類型	過濾器值
國家身分證號碼	取決於國家或地區：BRAZIL_RG_NUMBER, FRANCE_NATIONAL_IDENTIFICATION_NUMBER, GERMANY_NATIONAL_IDENTIFICATION_NUMBER, INDIA_AADHAAR_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_DNI_NUMBER
國民保險號碼 (NINO)	UK_NATIONAL_INSURANCE_NUMBER
護照號碼	取決於國家或地區：CANADA_PASSPORT_NUMBER, FRANCE_PASSPORT_NUMBER, GERMANY_PASSPORT_NUMBER, ITALY_PASSPORT_NUMBER, SPAIN_PASSPORT_NUMBER, UK_PASSPORT_NUMBER, USA_PASSPORT_NUMBER
永久居留號碼	CANADA_NATIONAL_IDENTIFICATION_NUMBER
電話號碼	取決於國家或地區：BRAZIL_PHONE_NUMBER, FRANCE_PHONE_NUMBER, GERMANY_PHONE_NUMBER, ITALY_PHONE_NUMBER, PHONE_NUMBER （適用於加拿大和美國），SPAIN_PHONE_NUMBER, UK_PHONE_NUMBER
社會保險號碼 (SIN)	CANADA_SOCIAL_INSURANCE_NUMBER
社會安全號碼 (SSN)	取決於國家或地區：SPAIN_SOCIAL_SECURITY_NUMBER, USA_SOCIAL_SECURITY_NUMBER

敏感資料類型	過濾器值
納稅識別號碼或參考號碼	取決於國家或地區：AUSTRALIA_TAX_FILE_NUMBER, BRAZIL_CNPJ_NUMBER, BRAZIL_CPF_NUMBER, FRANCE_TAX_IDENTIFICATION_NUMBER, GERMANY_TAX_IDENTIFICATION_NUMBER, INDIA_PERMANENT_ACCOUNT_NUMBER, SPAIN_NIE_NUMBER, SPAIN_NIF_NUMBER, SPAIN_TAX_IDENTIFICATION_NUMBER, UK_TAX_IDENTIFICATION_NUMBER, USA_INDIVIDUAL_TAX_IDENTIFICATION_NUMBER
車輛識別號碼 (VIN)	VEHICLE_IDENTIFICATION_NUMBER

利用 Amazon Macie 發現調查敏感資料

當您執行敏感資料探索任務或 Amazon Macie 執行自動化敏感資料探索時，Macie 會擷取每次出現在 Amazon Simple Storage Service (Amazon S3) 物件中敏感資料的位置的詳細資料。這包括 Macie 使用受管理資料識別碼偵測的敏感資料，以及符合您設定工作或 Macie 要使用的自訂資料識別碼準則的資料。

透過敏感資料發現，您可以針對 Macie 在個別 S3 物件中找到的多達 15 個敏感資料，檢閱這些詳細資料。這些詳細資料可讓您深入瞭解特定 S3 儲存貯體和物件可能包含的敏感資料類別和類型。它們可協助您找出物件中個別出現的敏感資料，並決定是否要對特定值區和物件執行更深入的調查。

如需其他見解，您可以選擇性地設定並使用 Macie 擷取 Macie 在個別發現項目中報告的敏感資料樣本。這些範例可協助您驗證 Macie 找到的敏感資料的性質。他們也可以協助您針對受影響的 S3 儲存貯體和物件量身打造調查。如果您選擇擷取發現項目的敏感資料樣本，Macie 會使用發現項目中的資料來尋找發現項目所報告之每種敏感資料類型的 1-10 次出現次數。然後，Macie 會從受影響的物件擷取出現的敏感資料，並顯示資料供您檢閱。

如果 S3 物件包含多次出現的敏感資料，則發現項目也可協助您瀏覽至對應的敏感資料探索結果。與敏感資料發現不同，敏感資料探索結果會針對 Macie 在物件中找到的每種敏感資料類型，提供多達 1,000

次出現的詳細位置資料。Macie 會針對敏感資料發現項目和敏感資料探索結果中的位置資料使用相同的結構描述。若要進一步瞭解敏感資料探索結果，請參閱儲存及保留敏感資料探索結果。

本節中的主題說明如何尋找並選擇性地擷取敏感資料發現項目所報告之敏感資料的出現次數。他們也解釋了 Macie 用來報告 Macie 找到之敏感資料個別出現位置的結構描述。

主題

- 使用 Amazon Macie 發現項目尋找敏感資料
- 使用 Amazon Macie 發現項目擷取敏感資料樣本
- 敏感資料位置的 JSON 結構定義

使用 Amazon Macie 發現項目尋找敏感資料

當您執行敏感資料探索任務或 Amazon Macie 執行自動化敏感資料探索時，Macie 會對其分析的每個 Amazon Simple Storage Service (Amazon S3) 物件的最新版本執行深入檢查。對於每個工作執行或分析週期，Macie 也會使用深度優先搜尋演算法，將 Macie 在 S3 物件中找到之特定敏感資料位置的詳細資料填入產生的發現項目。這些事件可以深入了解受影響 S3 儲存貯體和物件可能包含的敏感資料的類別和類型。詳細資料可協助您找出物件中個別出現的敏感資料，並決定是否要對特定值區和物件執行更深入的調查。

透過敏感資料發現，您可以判斷 Macie 在受影響 S3 物件中發現的多達 15 次敏感資料的位置。這包括 Macie 使用受管理資料識別碼偵測到的敏感資料，以及符合您設定工作或 Macie 要使用的自訂資料識別碼準則的資料。

敏感資料發現可提供詳細資料，例如：

- 儲存格或欄位在微軟 Excel 活頁簿、CSV 檔案或 TSV 檔案中的欄和列號。
- JSON 或 JSON 行檔案中欄位或陣列的路徑。
- CSV、JSON、JSON 行或 TSV 檔案以外的非二進位文字檔案中的行號，例如 HTML、TXT 或 XML 檔案。
- Adobe 可攜式文件格式 (PDF) 檔案中頁面的頁碼。
- 記錄索引和路徑在 Apache 的 Avro 對象容器或 Apache 實木複合地板文件中的記錄字段。

您可以使用 Amazon Macie Amazon Macie 您還可以在 Macie 發布給其他AWS 服務亞馬遜 EventBridge和AWS Security Hub. 若要瞭解 Macie 用來報告這些詳細資訊的 JSON 結構，請參閱敏感資料位置的 JSON 結構定義。若要瞭解如何存取 Macie 發佈給其他人的發現項目中的詳細資料AWS 服務，請參閱監控和處理問題清單。

如果 S3 物件包含多次出現的敏感資料，您也可以使用發現項目來導覽至其對應的敏感資料探索結果。與敏感資料發現不同，敏感資料探索結果會針對 Macie 在物件中找到的每種敏感資料類型，提供多達 1,000 次出現的詳細位置資料。如果 S3 物件是封存檔案 (例如 .tar 或 .zip 檔案)，這包括 Macie 從封存中擷取的個別檔案中出現的敏感資料。（Macie 不會在敏感數據發現中包含此信息。）若要進一步瞭解敏感資料探索結果，請參閱儲存及保留敏感資料探索結果。Macie 會針對敏感資料發現項目和敏感資料探索結果中的位置資料使用相同的結構描述。

查找敏感數據的出現

若要尋找敏感資料的發生次數，您可以使用 Amazon Macie 主控台或 Amazon Macie API。下列步驟說明如何使用主控台來尋找敏感資料。

若要以程式設計方式尋找敏感資料，請使用 Amazon Macie API 的GetFindings操作。如果發現項目包含有關特定敏感資料類型之一或多個出現位置的詳細資料，則尋找項目中的`occurrences`物件會提供這些詳細資訊。如需詳細資訊，請參閱敏感資料位置的 JSON 結構定義。

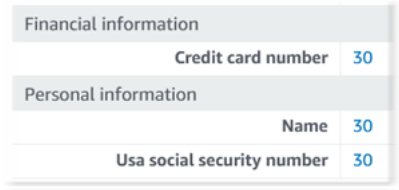
尋找敏感資料的出現次數

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 在導覽窗格中，選擇 Findings (問題清單)。

   > **Tip**
   >
   > 您可以使用「工作」頁面來顯示特定敏感資料探查工作的所有發現項目。若要執行此操作，請在導覽窗格中選擇 [工作]，然後選擇工作名稱。在詳細資料面板頂端，選擇 [顯示結果]，然後選擇 [顯示發現項目]。

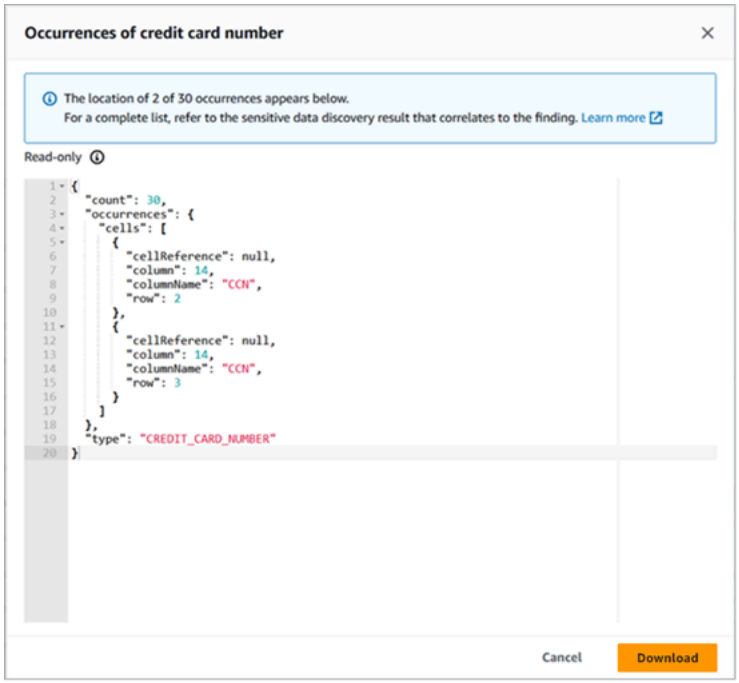
3. 在「發現的項目」頁面上，選擇要尋找之敏感資料的發現項目。詳細資訊面板會顯示問題清單的資訊。
4. 在詳細資料面板中，捲動至「敏感資料」區段。本節提供MacMacMacMacMacMacMacMacMacMacMacMacMacMacMacMacMacMacMacMacMacMacMacMacM它還指出 Macie 發現的每種敏感數據類型的出現次數。

   例如，下圖顯示某個發現項目的一些詳細資料，報告 30 次出現的信用卡號碼、30 次出現的名稱，以及 30 次出現的美國社會安全號碼。



如果發現項目包含有關特定敏感資料類型之一或多個出現位置的詳細資料，則出現次數為連結。選擇顯示詳細資料的連結。馬西打開一個新窗口，並顯示 JSON 格式的詳細信息。

例如，下圖顯示受影響 S3 物件中兩次出現的信用卡號碼位置。



若要將詳細資料儲存為 JSON 檔案，請選擇 [下載]，然後指定檔案的名稱和位置。

5. (選擇性) 若要將所有發現項目的詳細資訊儲存為 JSON 檔案，請在詳細資料面板頂端選擇發現項目的識別碼 (尋找項目 ID)。Macie 打開一個新窗口，並以 JSON 格式顯示所有詳細信息。選擇 [下載]，然後指定檔案的名稱和位置。

若要存取受影響物件中每種敏感資料類型多達 1,000 次出現位置的詳細資料，請參閱發現項目的對應敏感資料探索結果。若要這麼做，請捲動至面板「詳細資料」區段的開頭。然後在「詳細結果位置」欄位中選擇連結。Macie 會開啟 Amazon S3 主控台，並顯示包含對應探索結果的檔案或資料夾。

使用 Amazon Macie 發現項目擷取敏感資料樣本

若要驗證 Amazon Macie 在發現項目中報告的敏感資料本質，您可以選擇性地設定並使用 Macie 來擷取和顯示個別發現項目所報告的敏感資料樣本。這包括 Macie 使用受管理資料識別碼偵測到的敏感資料，以及符合自訂資料識別碼條件的資料。這些範例可協助您針對受影響的 Amazon 簡單儲存服務 (Amazon S3) 物件和儲存貯體量身打造調查。

如果您擷取並顯示尋找項目的敏感資料範例，Macie 會執行下列一般工作：

1. 驗證發現項目是否指定敏感資料個別出現的位置，以及對應敏感資料探索結果的位置。
2. 評估對應的敏感資料探索結果，檢查受影響 S3 物件的中繼資料的有效性，以及物件中出現敏感資料的位置資料。
3. 透過使用敏感資料探索結果中的資料，找出發現項目報告的第 1 至 10 次出現的敏感資料，並從受影響的 S3 物件擷取每個出現的前 1—128 個字元。如果發現項目報告了多種類型的敏感資料，Macie 會針對多達 100 種類型執行此動作。
4. 使用您指定的 AWS Key Management Service (AWS KMS) 金鑰加密擷取的資料。
5. 將加密的資料暫時儲存在快取中，並顯示資料供您檢閱。無論是在傳輸中還是靜態，資料都會隨時加密。
6. 擷取和加密之後不久，會永久刪除快取中的資料，除非暫時需要額外保留才能解決操作問題。

如果您選擇再次擷取和顯示發現項目的敏感資料樣本，Macie 會重複執行這些工作，以尋找、擷取、加密、儲存並最終刪除範例。

Macie 不會針對您的帳戶使用 Macie 服務連結角色來執行這些工作。而是使用您的 AWS Identity and Access Management (IAM) 身分，或允許 Macie 在您的帳戶中擔任 IAM 角色。如果您或角色被允許存取必要的資源和資料，並執行必要的動作，您就可以擷取和顯示發現項目的敏感資料範例。所有必要的動作都會登入AWS CloudTrail。

> **Important**
>
> 建議您使用自訂 IAM 政策來限制對此功能的存取。如需其他存取控制，我們建議您同時建立一個專用AWS KMS key於加密所擷取之敏感資料樣本，並將金鑰限制為只有必須允許擷取和揭露敏感資料樣本的主體使用。
>
> 如需可用來控制此功能存取權的政策建議和範例，請參閱AWS安全部落格上的如何使用 Amazon Macie 預覽 S3 儲存貯體中的敏感資料部落格文章。

本節中的主題說明如何設定及使用 Macie 來擷取和顯示發現項目的敏感資料範例。除了亞太區域（大阪）和以色列（特拉維夫）區域以外，您可以在目前所有提供 Macie 的地AWS 區域方執行這些任務。

主題

擷取含有發現項目之敏感資料範例的組態選項和需求

您可以選擇性地設定和使用 Amazon Macie 擷取和顯示 Macie 在個別發現項目中報告的敏感資料樣本。如果您擷取並揭露用於發現的敏感資料樣本，Macie 會使用對應敏感資料探索結果中的資料，在受影響的 Amazon Simple Storage Service (Amazon S3) 物件中找出敏感資料的出現次數。然後，Macie 會從受影響的物件中擷取這些出現位置的樣本。Macie 會使用您指定的 AWS Key Management Service (AWS KMS) 金鑰加密擷取的資料，將加密的資料暫時儲存在快取中，然後傳回結果中的資料以供尋找結果使用。在擷取和加密之後不久，Macie 會永久刪除快取中的資料，除非暫時需要額外保留才能解決操作問題。

Macie 不會針對您的帳戶使用 Macie 服務連結角色來尋找、擷取、加密或揭露受影響 S3 物件的敏感資料範例。相反地，Macie 會使用您為帳戶設定的設定和資源。在 Macie 中設定設定時，您可以指定如何存取受影響的 S3 物件。您也可以指定AWS KMS key要使用何種方式來加密範例。除了亞太區域（大阪）和以色列（特拉維夫）區域以外，您可以在目前所有 Macie 可用的地AWS 區域方進行設定。

若要存取受影響的 S3 物件並從中擷取敏感資料樣本，您有兩種選擇。您可以將 Macie 設定為使用 AWS Identity and Access Management (IAM) 使用者登入資料或假設 IAM 角色：

- 使用 IAM 使用者登入資料 — 使用此選項，您帳戶的每個使用者都會使用其個別 IAM 身分來尋找、擷取、加密和揭示範例。這表示如果使用者能夠存取必要的資源和資料，並執行必要的動作，就可以擷取和揭露敏感資料範例，以供尋找之用。
- 假設 IAM 角色 — 使用此選項，您可以建立將存取權委派給 Macie 的 IAM 角色。您也可以確定角色的信任和權限原則符合 Macie 擔任該角色的所有需求。然後，當您的帳戶的使用者選擇尋找、擷取、加密和揭露用於尋找的敏感資料範例時，Macie 會擔任該角色。

您可以使用任何類型的 Macie 帳戶 (組織的委派 Macie 管理員帳戶、組織中的 Macie 成員帳戶或獨立的 Macie 帳戶) 來使用任何組態。

下列主題說明可協助您決定如何設定帳戶的設定和資源的選項、需求和考量事項。這包括要附加到 IAM 角色的信任和許可政策。如需可用來擷取和顯示敏感資料樣本的其他建議和政策範例，請參閱AWS安全部落格上的如何使用 Amazon Macie 預覽 S3 儲存貯體中的敏感資料部落格文章。

主題

- 決定要使用哪種存取方法
- 使用 IAM 使用者登入資料存取受影響的 S3 物件
- 假設 IAM 角色存取受影響的 S3 物件
- 設定 IAM 角色以存取受影響的 S3 物件
- 解密受影響的 S3 物件

決定要使用哪種存取方法

判斷哪種組態最適合您的AWS環境時，關鍵的考量是您的環境是否包含多個以組織形式集中管理的 Amazon Macie 帳戶。如果您是組織委派的 Macie 管理員，將 Macie 設定為擔任 IAM 角色，可以簡化從組織中帳戶從受影響 S3 物件擷取敏感資料樣本的程序。使用這種方法，您可以在管理員帳戶中建立 IAM 角色。您也可以在每個適用的成員帳戶中建立 IAM 角色。管理員帳戶中的角色會委派對 Macie 的存取權。成員帳戶中的角色會委派對管理員帳戶中角色的跨帳戶存取權。如果實作，您就可以使用角色鏈結存取成員帳戶的受影響 S3 物件。

還要考慮誰可以直接訪問個別發現項目默認。若要擷取和顯示發現項目的敏感資料範例，使用者必須先具備尋找項目的存取權：

- 敏感資料探索工作 — 只有建立工作的帳戶可以存取工作產生的發現項目。如果您擁有 Macie 管理員帳戶，則可以設定工作來分析 S3 儲存貯體中的物件，以找出組織中任何帳戶的物件。因此，您的工作可以針對您的成員帳戶所擁有的值區中的物件產生發現項目。如果您擁有成員帳戶或獨立的 Macie 帳戶，則可以將工作設定為僅分析您帳戶擁有的值區中的物件。
- 自動化敏感資料探索 — 只有 Macie 管理員帳戶可以存取自動探索為其組織中帳戶產生的發現項目。會員帳戶無法存取這些發現項目。如果您擁有獨立的 Macie 帳戶，則可以存取自動化探索僅針對您自己的帳戶產生的發現項目。

如果您計劃使用 IAM 角色存取受影響的 S3 物件，也請考慮下列事項：

- 若要尋找物件中敏感資料的出現次數，尋找項目的對應敏感資料探索結果必須儲存在使用雜湊型訊息驗證碼 (HMAC) 簽署的 S3 物件中。AWS KMS keyMacie 必須能夠驗證敏感數據發現結果的完整性和真實性。否則，Macie 不會假設 IAM 角色來擷取敏感資料樣本。這是限制帳戶 S3 物件中資料存取的額外防護措施。

- 若要從使用客戶管理的加密物件擷取敏感資料樣本AWS KMS key，必須允許 IAM 角色使用金鑰解密資料。更具體地說，金鑰的原則必須允許角色執行`kms:Decrypt`動作。對於其他類型的伺服器端加密，不需要其他權限或資源即可解密受影響的物件。如需詳細資訊，請參閱解密受影響的 S3 物件。
- 若要從另一個帳戶的物件擷取敏感資料範例，您目前必須是適用AWS 區域帳戶的委派 Macie 管理員。除此之外：
  - 目前必須為適用地區的會員帳戶啟用 Macie。
  - 成員帳戶必須具有 IAM 角色，可將跨帳戶存取權委派給 Macie 管理員帳戶中的 IAM 角色。您的 Macie 管理員帳戶和成員帳戶中角色的名稱必須相同。
  - 成員帳戶中 IAM 角色的信任政策必須包含指定組態正確外部 ID 的條件。此 ID 是一個唯一的英數字串，Macie 會在您設定 Macie 管理員帳戶的設定後自動產生。如需有關在信任策略中使用外部 ID 的詳細資訊，請參閱《使用指南》中的將AWS資源的存取權授予第三方時如何使AWS Identity and Access Management用外部 ID。
  - 如果成員帳戶中的 IAM 角色符合所有 Macie 要求，則該成員帳戶不需要配置和啟用 Macie 設置，即可從其帳戶的對象中檢索敏感數據樣本。Macie 只會在您的 Macie 管理員帳戶中使用設定和 IAM 角色，以及成員帳戶中的 IAM 角色。

> **Tip**
>
> 如果您的帳戶屬於大型組織，請考慮使用AWS CloudFormation範本和堆疊集來佈建和管理組織中成員帳戶的 IAM 角色。若要取得有關建立和使用範本和堆疊集的資訊，請參閱《使AWS CloudFormation用指南》。
>
> 若要檢閱並選擇性地下載可做為起點的 CloudFormation 範本，您可以使用 Amazon Macie 主控台。在主控台的導覽窗格的 [設定] 下，選擇 [顯示範例]。選擇 [編輯]，然後選擇 [檢視成員角色權限和 CloudFormation 範本]。

本節的後續主題提供每種組態類型的其他詳細資料和考量事項。對於 IAM 角色，這包括要附加到角色的信任和許可政策。如果您不確定哪種類型的組態最適合您的環境，請向您的AWS管理員尋求協助。

使用 IAM 使用者登入資料存取受影響的 S3 物件

如果您將 Amazon Macie 設定為使用 IAM 使用者登入資料擷取敏感資料樣本，Macie 帳戶的每個使用者都會使用其 IAM 身分來尋找、擷取、加密和揭示個別發現項目的範例。這表示使用者可以擷取和揭露敏感資料樣本，以便找出其 IAM 身分是否允許存取必要的資源和資料，並執行必要的動作。所有必要的動作都會登入AWS CloudTrail。

若要擷取和顯示特定發現項目的敏感資料樣本，使用者必須被允許存取下列資料和資源：發現項目、對應的敏感資料探索結果、受影響的 S3 儲存貯體以及受影響的 S3 物件。也必須允許他們使用用來加密受影響物件 (如果適用的話)，以及您設定 Macie 用來加密敏感資料樣本的物件。AWS KMS key AWS KMS key如果任何 IAM 政策、資源政策或其他許可設定拒絕必要的存取權，則使用者將無法擷取和揭露發現項目的範例。

若要設定此類型的組態，請完成下列一般工作：

1. 確認您已為敏感資料探索結果設定存放庫。
2. 設定AWS KMS key要用於加密敏感資料樣本。
3. 確認您在 Macie 中設定設定的權限。
4. 配置並啟用 Macie 中的設置。

如需執行這些工作的詳細資訊，請參閱設定 Amazon Macie 以擷取和揭示含有發現項目的敏感資料樣本。

假設 IAM 角色存取受影響的 S3 物件

若要將 Amazon Macie 設定為透過假設 IAM 角色擷取敏感資料樣本，請先建立將存取權委派給 Macie 的 IAM 角色開始。請確定角色的信任和權限原則符合 Macie 擔任該角色的所有需求。當您的 Macie 帳戶的使用者接著選擇擷取並顯示用於尋找的敏感資料樣本時，Macie 會擔任從受影響 S3 物件擷取樣本的角色。只有當使用者選擇擷取並顯示尋找項目的範例時，Macie 才會擔任該角色。為了承擔這個角色，馬西使用AWS Security Token Service（AWS STS）API 的AssumeRole操作。所有必要的動作都會登入AWS CloudTrail。

若要擷取和顯示特定發現項目的敏感資料樣本，必須允許使用者存取發現項目、對應的敏感資料探索結果，以及您設定 Macie 用來加密敏感資料樣本的結果。AWS KMS keyIAM 角色必須允許 Macie 存取受影響的 S3 儲存貯體和受影響的 S3 物件。也必須允許角色使用用來加密受影響物件的角色 (如果適用)。AWS KMS key如果任何 IAM 政策、資源政策或其他許可設定拒絕必要的存取權，則使用者將無法擷取和揭露發現項目的範例。

若要設定此類型的組態，請完成下列一般工作。如果您在組織中擁有成員帳戶，請與您的 Macie 管理員合作，以決定是否以及如何為您的帳戶配置設定和資源。

1. 定義下列項目：
   - 您希望 Macie 假設的 IAM 角色名稱。如果您的帳戶是組織的一部分，委派的 Macie 管理員帳戶和組織中每個適用的成員帳戶的名稱必須相同。否則，Macie 管理員將無法存取適用成員帳戶的受影響 S3 物件。

- 要附加至 IAM 角色的 IAM 許可政策名稱。如果您的帳戶屬於組織，建議您為組織中的每個適用成員帳戶使用相同的策略名稱。這樣可以簡化成員帳戶中的角色佈建和管理作業。

2. 確認您已為敏感資料探索結果設定存放庫。
3. 設定AWS KMS key要用於加密敏感資料樣本。
4. 驗證您建立 IAM 角色的許可，並在 Macie 中設定設定。
5. 如果您是組織的委派 Macie 管理員，或者您擁有獨立的 Macie 帳戶：
   a. 為您的帳戶建立和設定 IAM 角色。請確定角色的信任和權限原則符合 Macie 擔任該角色的所有需求。如需有關這些需求的詳細資訊，請參閱下一個主題。
   b. 配置並啟用 Macie 中的設置。然後 Macie 會產生組態的外部識別碼。如果您是組織的 Macie 管理員，請記下此 ID。每個適用成員帳戶中 IAM 角色的信任政策都必須指定此 ID。
6. 如果您在組織中擁有成員帳戶：
   a. 請向您的 Macie 管理員詢問外部 ID，以便在帳戶中為 IAM 角色的信任政策中指定。同時驗證要建立的 IAM 角色和許可政策的名稱。
   b. 為您的帳戶建立和設定 IAM 角色。請確定角色的信任和權限原則符合 Macie 管理員擔任該角色的所有需求。如需有關這些需求的詳細資訊，請參閱下一個主題。
   c. (選擇性) 如果您想要從自己的帳戶的受影響 S3 物件擷取和顯示敏感資料樣本，請在 Macie 中設定並啟用設定。如果您希望 Macie 假設 IAM 角色擷取範例，請先在帳戶中建立並設定其他 IAM 角色。請確定此額外角色的信任和權限原則符合 Macie 擔任該角色的所有需求。然後在 Macie 中配置設置並指定此附加角色的名稱。如需有關角色原則需求的詳細資訊，請參閱下一個主題。

如需執行這些工作的詳細資訊，請參閱設定 Amazon Macie 以擷取和揭示含有發現項目的敏感資料樣本。

設定 IAM 角色以存取受影響的 S3 物件

若要使用 IAM 角色存取受影響的 S3 物件，請先建立和設定將存取權委派給 Amazon Macie 的角色開始。請確定角色的信任和權限原則符合 Macie 擔任該角色的所有需求。您如何執行此操作取決於您擁有的 Macie 帳戶類型。

以下各節提供有關每種類型 Macie 帳戶附加到 IAM 角色的信任和許可政策的詳細資訊。選擇您擁有的帳戶類型的部分。

> **Note**
>
> 如果您在組織中擁有成員帳戶，則可能需要為您的帳戶建立和設定兩個 IAM 角色：

- 若要允許 Macie 管理員從您帳戶的受影響 S3 物件擷取和揭露敏感資料樣本，請建立並設定管理員帳戶可以擔任的角色。有關這些詳細信息，請選擇 Macie 會員帳戶部分。
- 若要從您自己的帳戶的受影響 S3 物件擷取和揭露敏感資料樣本，請建立並設定 Macie 可以承擔的角色。有關這些詳細信息，請選擇獨立 Macie 帳戶部分。

在您建立和設定 IAM 角色之前，請與您的 Macie 管理員合作，確定帳戶的適當組態。

如需使用 IAM 建立角色的詳細資訊，請參閱使用AWS Identity and Access Management者指南中的使用自訂信任政策建立角色。

瑪西管理員帳戶

如果您是組織的委派 Macie 管理員，請先使用 IAM 政策編輯器建立 IAM 角色的許可政策。該政策應如下。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "RetrieveS3Objects",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "AssumeMacieRevealRoleForCrossAccountAccess",
            "Effect": "Allow",
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": "arn:aws:iam::*:role/IAMRoleName"
        }
    ]
}
```

其中 *IAM RoleName* 是 Macie 從組織帳戶的受影響 S3 物件擷取敏感資料樣本時所承擔的 IAM 角色名稱。將此值取代為您為帳戶建立的角色名稱，並計劃為組織中的適用成員帳戶建立。此名稱必須與您的 Macie 管理員帳戶和每個適用的會員帳戶相同。

> **Note**
>
> 在上述權限原則中，第一個陳述式中的`Resource`元素會使用萬用字元 (*)。這可讓附加的 IAM 實體從組織擁有的所有 S3 儲存貯體擷取物件。若要僅允許特定值區存取此存取權，請將萬用字元取代為每個儲存貯體的 Amazon 資源名稱 (ARN)。例如，若只要允許存取名為值區中的物件 DOC-EXAMPLE-BUCKET，請將元素變更為：
> `"Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"`
> 您也可以針對個別帳戶限制對特定 S3 儲存貯體中物件的存取。若要這麼做，請在每個適用帳戶的 IAM 角色權限政策`Resource`元素中指定儲存貯體 ARN。如需詳細資訊和範例，請參閱AWS Identity and Access Management使用者指南中的 IAM JSON 政策元素：資源。

建立 IAM 角色的許可政策後，請建立並設定角色。如果您使用 IAM 主控台執行此操作，請選擇「自訂信任政策」做為角色的「受信任」實體類型。對於為角色定義受信任實體的信任原則，請指定下列項目。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowMacieReveal",
            "Effect": "Allow",
            "Principal": {
                "Service": "reveal-samples.macie.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "accountID"
                }
            }
        }
    ]
}
```

其中 *account* ID 是您AWS 帳戶的帳號 ID。將此值取代為您的 12 位數帳戶 ID。

在先前的信任策略中：

- `Principal`元素會指定 Macie 從受影響的 S3 物件擷取敏感資料樣本時使用的服務主體。`reveal-samples.macie.amazonaws.com`
- `Action`元素會指定允許服務主體執行的動AssumeRole作，即 AWS Security Token Service (AWS STS) API 的作業。
- 該`Condition`元素定義了使用 aws: SourceAccount 全局條件上下文鍵的條件。此條件決定哪個帳戶可以執行指定的動作。在這種情況下，它允許 Macie 只為指定的帳戶 (*`accountID`*) 承擔角色。該條件有助於防止 Macie 在與AWS STS交易過程中被用作混淆的副手。

定義 IAM 角色的信任政策後，請將許可政策附加到該角色。這應該是您在開始建立角色之前建立的權限原則。然後完成 IAM 中的其餘步驟，以完成角色的建立和設定。完成後，配置並啟用 Macie 中的設置。

馬西會員帳戶

如果您擁有 Macie 成員帳戶，並且想要允許 Macie 管理員從您帳戶的受影響 S3 物件擷取和顯示敏感資料樣本，請先向您的 Macie 管理員詢問下列資訊：

- 要建立的 IAM 角色名稱。您的帳戶和組織的 Macie 管理員帳戶名稱必須相同。
- 要附加至角色的 IAM 許可政策名稱。
- 要在角色信任原則中指定的外部識別碼。此識別碼必須是 Macie 為您的 Macie 管理員設定所產生的外部識別碼。

收到此資訊後，請使用 IAM 政策編輯器建立角色的許可政策。該政策應如下。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "RetrieveS3Objects",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "*"
            ]
        }
```

```
    ]
}
```

上述許可政策允許附加的 IAM 實體從您帳戶的所有 S3 儲存貯體擷取物件。這是因為策略中的`Resource`元素使用萬用字元 (*)。若要僅允許特定值區存取此存取權，請將萬用字元取代為每個儲存貯體的 Amazon 資源名稱 (ARN)。例如，若只要允許存取名為值區中的物件 DOC-EXAMPLE-BUCKET2，請將元素變更為：

```
"Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET2/*"
```

如需詳細資訊和範例，請參閱AWS Identity and Access Management使用者指南中的 IAM JSON 政策元素：資源。

建立 IAM 角色的許可政策後，請建立角色。如果您使用 IAM 主控台建立角色，請選擇「自訂信任政策」做為該角色的受信任實體類型。對於為角色定義受信任實體的信任原則，請指定下列項目。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowMacieAdminRevealRoleForCrossAccountAccess",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::administratorAccountID:role/IAMRoleName"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "sts:ExternalId": "externalID",
                    "aws:PrincipalOrgID": "${aws:ResourceOrgID}"
                }
            }
        }
    ]
}
```

在上述政策中，將預留位置值取代為您AWS環境的正確值，其中：

- *##### ID* 是您 Macie 管理員帳戶的 12 位數帳戶識別碼。
- *IAM RoleName* 是您 Macie 管理員帳戶中的 IAM 角色名稱。它應該是您從 Macie 管理員那裡收到的名稱。

- *## ID* 是您從 Macie 管理員那裡收到的外部識別碼。

一般而言，信任政策可讓您的 Macie 管理員擔任角色，從您帳戶的受影響 S3 物件擷取和揭露敏感資料樣本。`Principal`元素會指定您 Macie 管理員帳戶中某個 IAM 角色的 ARN。這是您的 Macie 管理員用來擷取和顯示組織帳戶之機密資料範例的角色。該`Condition`塊定義了兩個條件，這些條件進一步確定誰可以擔任該角色：

- 第一個條件會指定組織組態專屬的外部 ID。若要進一步了解外部 ID，請參閱《使用AWS Identity and Access Management者指南》中的將AWS資源存取權授予第三方時如何使用外部 ID。
- 第二個條件使用 aws：PrincipalOrgID 全局條件上下文鍵。索引鍵的值是動態變數，代表 AWS Organizations (`${aws:ResourceOrgID}`) 中組織的唯一識別元。條件限制只能存取屬於AWS Organizations中相同組織的帳戶。如果您在 Macie 中接受邀請加入組織，請從原則中移除此條件。

定義 IAM 角色的信任政策後，請將許可政策附加到該角色。這應該是您在開始建立角色之前建立的權限原則。然後完成 IAM 中的其餘步驟，以完成角色的建立和設定。請勿在 Macie 中配置和輸入角色的設置。

獨立的麥西亞帳戶

如果您擁有獨立的 Macie 帳戶或 Macie 成員帳戶，並且想要從自己的帳戶的受影響 S3 物件擷取和揭露敏感資料樣本，請先使用 IAM 政策編輯器為 IAM 角色建立許可政策。該政策應如下。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "RetrieveS3Objects",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

在上述權限原則中，Resource元素會使用萬用字元 (*)。這可讓附加的 IAM 實體從您帳戶的所有 S3 儲存貯體擷取物件。若要僅允許特定值區存取此存取權，請將萬用字元取代為每個儲存貯體的 Amazon 資源名稱 (ARN)。例如，若只要允許存取名為值區中的物件 DOC-EXAMPLE-BUCKET3，請將元素變更為：

```
"Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET3/*"
```

如需詳細資訊和範例，請參閱AWS Identity and Access Management使用者指南中的 IAM JSON 政策元素：資源。

建立 IAM 角色的許可政策後，請建立角色。如果您使用 IAM 主控台建立角色，請選擇「自訂信任政策」做為該角色的受信任實體類型。對於為角色定義受信任實體的信任原則，請指定下列項目。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowMacieReveal",
            "Effect": "Allow",
            "Principal": {
                "Service": "reveal-samples.macie.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "accountID"
                }
            }
        }
    ]
}
```

其中 *account* ID 是您AWS 帳戶的帳號 ID。將此值取代為您的 12 位數帳戶 ID。

在先前的信任策略中：

- Principal元素會指定 Macie 從受影響 S3 物件擷取和顯示敏感資料樣本時使用的服務主體。reveal-samples.macie.amazonaws.com
- Action元素會指定允許服務主體執行的動AssumeRole作，即 AWS Security Token Service (AWS STS) API 的作業。

- 該Condition元素定義了使用 aws: SourceAccount 全局條件上下文鍵的條件。此條件決定哪個帳戶可以執行指定的動作。它允許 Macie 只為指定的帳戶 (*accountID*) 承擔角色。該條件有助於防止 Macie 在與AWS STS交易過程中被用作混淆的副手。

定義 IAM 角色的信任政策後，請將許可政策附加到該角色。這應該是您在開始建立角色之前建立的權限原則。然後完成 IAM 中的其餘步驟，以完成角色的建立和設定。完成後，配置並啟用 Macie 中的設置。

解密受影響的 S3 物件

Amazon S3 支援 S3 物件的多個加密選項。對於大多數這些選項，IAM 使用者或角色不需要其他資源或許可，即可從受影響物件解密和擷取敏感資料樣本。對於使用伺服器端加密搭配 Amazon S3 受管金鑰或受管金鑰加密的物件，就是這種情況AWS KMS key。AWS

但是，如果 S3 物件使用客戶管理加密AWS KMS key，則需要額外的許可才能從物件解密和擷取敏感資料樣本。更具體地說，KMS 金鑰的金鑰政策必須允許 IAM 使用者或角色執行kms:Decrypt動作。否則，會發生錯誤，Macie 不會從物件擷取任何樣本。若要了解如何為 IAM 使用者提供此存取權，請參閱AWS Key Management Service開發人員指南AWS KMS中的身份驗證和存取控制。

如何為 IAM 角色提供此存取權取決於擁有該角色的帳戶是否AWS KMS key也擁有該角色：

- 如果相同的帳戶擁有 KMS 金鑰和角色，則帳戶的使用者必須更新金鑰的原則。
- 如果一個帳戶擁有 KMS 金鑰，而另一個帳戶擁有該角色，則擁有該金鑰的帳戶的使用者必須允許跨帳戶存取金鑰。

本主題說明如何針對您為從 S3 物件擷取敏感資料樣本而建立的 IAM 角色執行這些工作。它也提供這兩種情況的範例。如需有關允許存取其他案例所管理AWS KMS keys之客戶的資訊，請參閱AWS Key Management Service開發人員指南AWS KMS中的驗證與存取控制。

允許相同帳戶存取客戶管理的金鑰

如果同一帳戶同時擁有AWS KMS key和 IAM 角色，則該帳戶的使用者必須在金鑰的政策中新增陳述式。其他陳述式必須允許 IAM 角色使用金鑰來解密資料。如需更新金鑰原則的詳細資訊，請參閱AWS Key Management Service開發人員指南中的變更金鑰政策。

在聲明中：

- 元Principal素必須指定 IAM 角色的 Amazon 資源名稱 (ARN)。

- Action陣列必須指定kms:Decrypt動作。這是唯一必須允許 IAM 角色執行的AWS KMS動作，才能解密使用金鑰加密的物件。

以下是要新增至 KMS 金鑰原則的陳述式範例。

```
{
    "Sid": "Allow the Macie reveal role to use the key",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::123456789012:role/IAMRoleName"
    },
    "Action": [
        "kms:Decrypt"
    ],
    "Resource": "*"
}
```

在上述範例中：

- Principal元素中的AWS欄位會指定帳戶中 IAM 角色的 ARN。它可讓角色執行原則陳述式所指定的動作。*123456789012* 是一個帳戶識別碼範例。將此值取代為擁有角色和 KMS 金鑰之帳戶的帳戶識別碼。*IAM RoleName* 是一個示例名稱。將此值取代為帳戶中 IAM 角色的名稱。
- Action陣列指定允許 IAM 角色使用 KMS 金鑰執行的動作 — 解密使用金鑰加密的加密文字。

將此陳述式新增至金鑰原則的位置取決於原則目前包含的結構和元素。當您新增陳述式時，請確定語法有效。金鑰政策使用 JSON 格式。這表示您也必須在陳述式之前或之後加上逗號，視您將陳述式新增至原則的位置而定。

允許跨帳戶存取客戶管理的金鑰

如果一個帳戶擁有AWS KMS key（金鑰擁有者），而另一個帳戶擁有 IAM 角色（角色擁有者），則金鑰擁有者必須向角色擁有者提供對金鑰的跨帳戶存取權限。要做到這一點的一種方法是通過使用授予. 授權是一種原則工具，可讓AWS主體在符合授權指定的條件時，在密碼編譯作業中使用 KMS 金鑰。若要進一步了解撥款，請參閱AWS Key Management Service開發人員指南AWS KMS中的贈款。

使用這種方法，金鑰擁有者會先確保金鑰的原則允許角色擁有者建立金鑰的授與。然後，角色擁有者會建立金鑰的授權。授權會將相關許可委派給其帳戶中的 IAM 角色。它可讓角色解密使用金鑰加密的 S3 物件。

步驟 1：更新金鑰原則

在金鑰政策中，金鑰擁有者應確保該政策包含允許角色擁有者在其 (角色擁有者) 帳戶中為 IAM 角色建立授與的陳述式。在此陳述式中，Principal元素必須指定角色擁有者帳戶的 ARN。Action陣列必須指定kms:CreateGrant動作。圖Condition塊可以篩選對指定動作的存取。以下是 KMS 金鑰原則中此陳述式的範例。

```
{
    "Sid": "Allow a role in an account to create a grant",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
    },
    "Action": [
        "kms:CreateGrant"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:GranteePrincipal": "arn:aws:iam::111122223333:role/IAMRoleName"
        },
        "ForAllValues:StringEquals": {
            "kms:GrantOperations": "Decrypt"
        }
    }
}
```

在上述範例中：

- Principal元素中的AWS欄位會指定角色擁有者帳戶的 ARN。它允許帳戶執行策略聲明所指定的操作。 *111122223333* 是一個帳戶識別碼範例。將此值取代為角色擁有者帳戶的帳號 ID。
- Action陣列指定允許角色擁有者對 KMS 金鑰執行的動作 — 建立金鑰授權。
- Condition區塊會使用條件運算子和下列條件金鑰來篩選允許角色擁有者對 KMS 金鑰執行之動作的存取：
  - kms: GranteePrincipal — 此條件允許角色擁有者僅為指定的受權者主體 (即其帳戶中 IAM 角色的 ARN) 建立授權。在該 ARN 中，*111122223333* 是一個示例帳戶識別碼。將此值取代為角色擁有者帳戶的帳號 ID。*IAM RoleName* 是一個示例名稱。將此值取代為角色擁有者帳戶中 IAM 角色的名稱。
  - kms: GrantOperations — 此條件允許角色擁有者建立僅授與委派執行AWS KMSDecrypt動作的權限 (解密使用金鑰加密的加密文字)。它可防止角色擁有者建立授與委派權限，以便對 KMS 金鑰

執行其他動作。此Decrypt動作是唯一必須允許 IAM 角色執行的AWS KMS動作，才能解密使用金鑰加密的物件。

金鑰擁有者將此陳述式新增至金鑰原則的位置取決於原則目前包含的結構和元素。當密鑰所有者添加語句時，他們應該確保語法有效。金鑰政策使用 JSON 格式。這表示金鑰擁有者也必須在陳述式之前或之後加上逗號，視使用者將陳述式新增至原則的位置而定。如需更新金鑰原則的詳細資訊，請參閱AWS Key Management Service開發人員指南中的變更金鑰政策。

步驟 2：建立授權

在金鑰擁有者視需要更新金鑰原則之後，角色擁有者會建立金鑰的授與。授權會將相關許可委派給其 (角色擁有者) 帳戶中的 IAM 角色。在角色擁有者建立授權之前，他們應該確認自己已被允許執行kms:CreateGrant動作。此動作可讓他們將授權新增至現有、受管理的客戶AWS KMS key。

若要建立授權，角色擁有者可以使用 AWS Key Management Service API 的CreateGrant作業。當角色擁有者建立授權時，他們應該為必要的參數指定下列值：

- KeyId— KMS 金鑰的 ARN。若要跨帳戶存取 KMS 金鑰，此值必須是 ARN。它不能是金鑰識別碼。
- GranteePrincipal— 其帳戶中 IAM 角色的 ARN。此值應為arn:aws:iam::*111122223333*:role/*IAMRoleName*，其中 *111122223333* 是角色擁有者帳戶的帳戶識別碼，而 *IAM RoleName* 是角色的名稱。
- Operations— 解AWS KMS密動作 (Decrypt)。這是唯一必須允許 IAM 角色執行的AWS KMS動作，才能解密使用 KMS 金鑰加密的物件。

如果角色擁有者正在使用 AWS Command Line Interface (AWS CLI)，他們可以執行 create-grant 命令來建立授權。下列範例會顯示作法。此範例已針對 Microsoft Windows 進行格式化，並使用脫字元 (^) 行接續字元來提高可讀性。

```
C:\> aws kms create-grant ^
--key-id arn:aws:kms:us-east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab ^
--grantee-principal arn:aws:iam::111122223333:role/IAMRoleName ^
--operations "Decrypt"
```

其中：

- key-id指定要套用授權之 KMS 金鑰的 ARN。

- `grantee-principal`指定允許執行授權指定動作的 IAM 角色的 ARN。此值應符合金鑰原則中`kms:GranteePrincipal`條件所指定的 ARN。
- `operations`指定授與允許指定主體執行的動作 — 解密使用金鑰加密的加密文字。

如果此命令成功執行，您會收到類似如下的輸出。

```
{
    "GrantToken": "<grant token>",
    "GrantId": "1a2b3c4d2f5e69f440bae30eaec9570bb1fb7358824f9ddfa1aa5a0dab1a59b2"
}
```

其中`GrantToken`是唯一、非秘密、可變長度、base64 編碼的字串，代表已建立的授權，並且`GrantId`是授權的唯一識別碼。

設定 Amazon Macie 以擷取和揭示含有發現項目的敏感資料樣本

您可以選擇性地設定和使用 Amazon Macie 擷取和揭示 Macie 在個別敏感資料發現項目中報告的敏感資料樣本。這些範例可協助您驗證 Macie 找到的敏感資料的性質。他們還可以協助您針對受影響的 Amazon 簡單儲存服務 (Amazon S3) 物件和儲存貯體量身打造調查。除了亞太區域 (大阪) 和以色列 (特拉維夫) 區域外，您可以擷取並揭露所有 Macie 目前可用的機密資料樣本。AWS 區域

當您擷取並顯示發現項目的敏感資料樣本時，Macie 會使用對應敏感資料探索結果中的資料，找出受影響 S3 物件中敏感資料的出現次數。然後，Macie 會從受影響的物件中擷取這些出現位置的樣本。Macie 會使用您指定的 AWS Key Management Service (AWS KMS) 金鑰加密擷取的資料，將加密的資料暫時儲存在快取中，然後傳回結果中的資料以供尋找結果使用。在擷取和加密之後不久，Macie 會永久刪除快取中的資料，除非暫時需要額外保留才能解決操作問題。

若要擷取和顯示發現項目的敏感資料範例，您必須先設定並啟用 Macie 帳戶的設定。您還需要為您的帳戶配置支持的資源和權限。本節中的主題將引導您完成設定 Macie 以擷取和顯示敏感資料樣本，以及管理帳戶組態狀態的程序。

主題

- 開始之前
- 設定和啟用 Amazon Macie 設定
- 禁用 Amazon Macie 設置

> **Tip**
>
> 如需可用來控制此功能存取權的政策建議和範例，請參閱AWS安全部落格上的如何使用 Amazon Macie 預覽 S3 儲存貯體中的敏感資料部落格文章。

開始之前

在將 Amazon Macie 設定為擷取和顯示發現項目的敏感資料樣本之前，請先完成以下任務，以確保您擁有所需的資源和許可。

任務

- 步驟 1：設定敏感資料探索結果的儲存庫
- 步驟 2：決定如何存取受影響的 S3 物件
- 步驟 3：設定 AWS KMS key
- 步驟 4：驗證您的權限

如果您已將 Macie 設定為擷取和顯示敏感資料範例，而且只想變更您的組態設定，則這些工作是選用的。

步驟 1：設定敏感資料探索結果的儲存庫

當您擷取並顯示發現項目的敏感資料樣本時，Macie 會使用對應敏感資料探索結果中的資料，找出受影響 S3 物件中敏感資料的出現次數。因此，請務必確認您是否為敏感性資料探索結果設定存放庫。否則，Macie 將無法找到您要檢索和顯示的敏感數據樣本。

若要判斷您是否已為帳戶設定此儲存庫，可以使用 Amazon Macie 主控台：在導覽窗格中選擇 [探索結果] (在 [設定] 下)。要以編程方式執行此GetClassificationExportConfiguration操作，請使用 Amazon Macie API 的操作。若要進一步瞭解敏感資料探索結果以及如何設定此存放庫，請參閱儲存及保留敏感資料探索結果。

步驟 2：決定如何存取受影響的 S3 物件

若要存取受影響的 S3 物件並從中擷取敏感資料樣本，您有兩種選擇。您可以將 Macie 設定為使用您的 AWS Identity and Access Management (IAM) 使用者登入資料。或者，您可以將 Macie 設定為可委派存取 Macie 的 IAM 角色。您可以使用任何類型的 Macie 帳戶 (組織的委派 Macie 管理員帳戶、組織中的 Macie 成員帳戶或獨立的 Macie 帳戶) 來使用任何組態。在 Macie 中設定設定之前，請先決定您要

使用的存取方法。如需有關每種方法的選項和需求的詳細資訊，請參閱擷取含有發現項目之敏感資料範例的組態選項和需求。

如果您打算使用 IAM 角色，請先建立並設定角色，然後再在 Macie 中設定設定。此外，請確定角色的信任和權限原則符合 Macie 擔任該角色的所有需求。如果您的帳戶屬於集中管理多個 Macie 帳戶的組織，請與您的 Macie 管理員合作，先決定是否為您的帳戶設定角色以及如何設定角色。

步驟 3：設定 AWS KMS key

當您擷取並顯示發現項目的敏感資料樣本時，Macie 會使用您指定的 AWS Key Management Service (AWS KMS) 金鑰加密範例。因此，您需要決定AWS KMS key要使用哪一個來加密樣本。金鑰可以是您自己帳戶中的現有 KMS 金鑰，也可以是其他帳戶擁有的現有 KMS 金鑰。如果您想要使用其他帳戶擁有的金鑰，請取得該金鑰的 Amazon 資源名稱 (ARN)。當您在 Macie 中輸入組態設定時，您需要指定此 ARN。

KMS 金鑰必須是客戶管理的對稱加密金鑰。它也必須是與您的 Macie 帳戶相同AWS 區域啟用的單一區域金鑰。KMS 金鑰可以位於外部金鑰存放區中。但是，與完全在其中管理的密鑰相比，密鑰可能會慢且不太可靠AWS KMS。如果延遲或可用性問題導致 Macie 無法加密您要擷取和顯示的敏感資料樣本，就會發生錯誤，而且 Macie 不會傳回任何尋找項目的範例。

此外，金鑰的金鑰政策必須允許適當的主體 (IAM 角色、IAM 使用者或AWS 帳戶) 執行下列動作：

- `kms:Decrypt`
- `kms:DescribeKey`
- `kms:GenerateDataKey`

> **Important**
>
> 作為存取控制的額外層，我們建議您建立專用的 KMS 金鑰來加密所擷取的敏感資料樣本，並將金鑰的使用限制為只有必須允許擷取和揭露敏感資料樣本的主體。如果不允許使用者針對金鑰執行上述動作，Macie 會拒絕其擷取和揭露敏感資料樣本的要求。Macie 不會返回任何發現的樣本。

如需建立和設定 KMS 金鑰的詳細資訊，請參閱AWS Key Management Service開發人員指南中的管理金鑰。如需使用金鑰原則管理 KMS 金鑰存取權的詳細資訊，請參閱AWS Key Management Service開發人員指南AWS KMS中的金鑰政策。

步驟 4：驗證您的權限

在 Macie 中設定設定之前，請確認您擁有所需的權限。若要驗證您的許可，請使用 AWS Identity and Access Management (IAM) 檢閱附加到 IAM 身分的 IAM 政策。然後將這些策略中的資訊與下列必須允許您執行的動作清單進行比較。

Amazon Macie

對於 Macie，請確認您是否允許執行下列動作：

- `macie2:GetMacieSession`
- `macie2:UpdateRevealConfiguration`

第一個動作允許您訪問您的 Macie 帳戶。第二個動作可讓您變更用於擷取和顯示敏感資料樣本的組態設定。這包括啟用和停用帳戶的設定。

選擇性地確認您也被允許執行`macie2:GetRevealConfiguration`動作。此動作可讓您擷取目前的組態設定和帳戶組態的目前狀態。

AWS KMS

如果您計劃使用 Amazon Macie 主控台輸入組態設定，請確認您可以執行下列 AWS Key Management Service (AWS KMS) 動作：

- `kms:DescribeKey`
- `kms:ListAliases`

這些動作可讓您擷取您帳戶AWS KMS keys的相關資訊。然後，您可以在輸入設定時選擇其中一個按鍵。

IAM

如果您計劃將 Macie 設定為假設 IAM 角色來擷取和揭露敏感資料範例，請確認您是否可以執行下列 IAM 動作：`iam:PassRole`。此操作允許您將角色傳遞給 Macie，這反過來又允許 Macie 擔任該角色。當您輸入帳戶的組態設定時，Macie 也可以接著驗證該角色是否存在於您的帳戶中，且已正確設定。

如果您不允許執行必要的動作，請向AWS管理員尋求協助。

設定和啟用 Amazon Macie 設定

確認擁有所需的資源和許可後，您可以在 Amazon Macie 中設定設定並啟用帳戶的組態。

如果您的帳戶屬於集中管理多個 Macie 帳戶的組織，請在設定或隨後變更帳戶的設定之前，請注意下列事項：

- 如果您有會員帳戶，請與您的 Macie 管理員合作，以決定是否以及如何為您的帳戶進行設定。您的 Macie 管理員可協助您決定帳戶的正確組態設定。
- 如果您擁有 Macie 管理員帳戶，且變更存取受影響 S3 物件的設定，則您的變更可能會影響組織的其他帳戶和資源。這取決於 Macie 目前是否設定為假設 AWS Identity and Access Management (IAM) 角色來擷取敏感資料樣本。如果是，且您重新設定 Macie 以使用 IAM 使用者登入資料，Macie 會永久刪除 IAM 角色的現有設定 — 角色名稱和組態的外部 ID。如果您的組織隨後選擇再次使用 IAM 角色，則需要在信任政策中為每個適用成員帳戶中的角色指定新的外部 ID。

如需任一帳戶類型的組態選項的詳細資訊，請參閱擷取含有發現項目之敏感資料範例的組態選項和需求。

要在 Macie 中配置設置並為您的帳戶啟用配置，您可以使用 Amazon Macie 控制台或 Amazon Macie API。

Console

請依照下列步驟使用 Amazon Macie 主控台來設定和啟用設定。

若要設定和啟用 Macie 設定

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 使用頁面右上角的選取AWS 區域器，選取您要設定的區域，然後啟用 Macie 擷取和顯示敏感資料樣本。
3. 在導覽窗格的 [設定] 下，選擇 [顯示範例]。
4. 在 Settings (設定) 區段中，選擇 Edit (編輯)。
5. 針對 Status (狀態)，請選擇 Enable (啟用)。
6. 在 Access 下，指定從受影響 S3 物件擷取敏感資料樣本時要使用的存取方法和設定：
   - 若要使用將存取權委派給 Macie 的 IAM 角色，請選擇假設 IAM 角色。如果您選擇此選項，Macie 會假設您AWS 帳戶在. 在 [角色名稱] 方塊中，輸入角色的名稱。
   - 若要使用要求範例的 IAM 使用者登入資料，請選擇「使用 IAM 使用者登入資料」。如果您選擇此選項，您帳戶的每個使用者都會使用其個別的 IAM 身分來擷取範例。
7. 在「加密」下，指AWS KMS key定您要用來加密所擷取之敏感資料樣本的項目：

- 若要使用您自己帳戶中的 KMS 金鑰，請選擇 [從您的帳戶選取金鑰]。然後，在AWS KMS key清單中選擇要使用的金鑰。此清單會顯示您帳戶的現有對稱加密 KMS 金鑰。
- 若要使用其他帳戶擁有的 KMS 金鑰，請選擇 [輸入其他帳戶金鑰的 ARN]。然後，在 AWS KMS keyARN 方塊中，輸入要使用的金鑰的 Amazon 資源名稱 (ARN)，例如。**`arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`**

8. 完成輸入設定後，請選擇 [儲存]。

Macie 測試設置並驗證它們是否正確。如果您將 Macie 設定為擔任 IAM 角色，Macie 也會驗證該角色存在於您的帳戶中，並且信任和許可政策設定正確。如果發生問題，Macie 會顯示描述問題的訊息。

若要解決的問題AWS KMS key，請參閱上一主題中的需求，並指定符合需求的 KMS 金鑰。若要解決 IAM 角色的問題，請先驗證您輸入的角色名稱是否正確。如果名稱正確，請確保角色的策略符合 Macie 擔任該角色的所有要求。如需這些詳細資訊，請參閱設定 IAM 角色以存取受影響的 S3 物件。解決任何問題後，您可以保存並啟用設置。

> **Note**
>
> 如果您是組織的 Macie 管理員，並且將 Macie 設定為擔任 IAM 角色，Macie 會在您儲存帳戶的設定後產生並顯示外部 ID。請注意此識別碼。每個適用成員帳戶中 IAM 角色的信任政策都必須指定此 ID。否則，您將無法從帳戶擁有的 S3 物件擷取敏感資料樣本。

API

若要以程式設計方式設定和啟用設定，請使用 Amazon Macie API 的UpdateRevealConfiguration操作。在您的請求中，為支援的參數指定適當的值：

- 對於`retrievalConfiguration`參數，請指定從受影響 S3 物件擷取敏感資料樣本時要使用的存取方法和設定：
  - 若要採用將存取權委派給 Macie 的 IAM 角色，請`ASSUME_ROLE`為`retrievalMode`參數指定並指定參`roleName`數的角色名稱。如果您指定這些設定，Macie 會假設您AWS 帳戶在.
  - 若要使用要求範例的 IAM 使用者登入資料，請`CALLER_CREDENTIALS`為`retrievalMode`參數指定。如果指定此設定，您帳戶的每個使用者都會使用其個別的 IAM 身分來擷取範例。

> **Important**
>
> 如果您未指定這些參數的值，Macie 會將CALLER_CREDENTIALS存取方法 (retrievalMode) 設定為。如果 Macie 目前設定為使用 IAM 角色擷取範例，Macie 也會永久刪除組態的目前角色名稱和外部 ID。若要保留現有組態的這些設定，請在請求中包含retrievalConfiguration參數，並為這些參數指定目前的設定。若要擷取目前的設定，請使用GetRevealConfiguration作業，或者，如果您使用的是 AWS Command Line Interface (AWS CLI)，請執行get-reveal-configuration命令。

- 針對kmsKeyId參數，指定要AWS KMS key用來加密所擷取之敏感資料樣本的參數：
  - 若要使用您自己帳戶的 KMS 金鑰，請指定金鑰的 Amazon 資源名稱 (ARN)、ID 或別名。如果您指定別名，請包括alias/首碼，例如。alias/ExampleAlias
  - 若要使用其他帳戶擁有的 KMS 金鑰，請指定金鑰的 ARN，例如。arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab或者指定金鑰別名的 ARN — 例如，。arn:aws:kms:us-east-1:111122223333:alias/ExampleAlias
- 對於status參數，請指定ENABLED為您的 Macie 帳戶啟用設定。

在您的要求中，也請確定您指定要AWS 區域在其中啟用並使用組態。

若要使用配置和啟用設定AWS CLI，請執行命update-reveal-configuration令並為支援的參數指定適當的值。例如，如果您AWS CLI在 Microsoft 視窗上使用，請執行下列命令：

```
C:\> aws macie2 update-reveal-configuration ^
--region us-east-1 ^
--configuration={\"kmsKeyId\":\"arn:aws:kms:us-east-1:111122223333:alias/
ExampleAlias\",\"status\":\"ENABLED\"} ^
--retrievalConfiguration={\"retrievalMode\":\"ASSUME_ROLE\",\"roleName\":
\"MacieRevealRole\"}
```

其中：

- *us-east-1* 是要在其中啟用和使用配置的區域。在此範例中，美國東部 (維吉尼亞北部) 區域。
- *ARN: aws: ##:####-1:1111223 ExampleAlias 33: ##*/是要使用的別名的 ARN。AWS KMS key在此範例中，金鑰是由另一個帳戶所擁有。
- ENABLED是組態的狀態。

- *##*是要使用的訪問方法。在此範例中，假設指定的 IAM 角色。
- *MacieRevealRole*是 Macie 在擷取敏感資料樣本時要承擔的 IAM 角色名稱。

上述範例使用脫字元 (^) 行接續字元來改善可讀性。

當您提交請求時，Macie 會測試設定。如果您將 Macie 設定為擔任 IAM 角色，Macie 也會驗證該角色存在於您的帳戶中，並且信任和許可政策設定正確。如果發生問題，表示您的要求失敗，而 Macie 會傳回描述問題的訊息。若要解決的問題AWS KMS key，請參閱上一主題中的需求，並指定符合需求的 KMS 金鑰。若要解決 IAM 角色的問題，請先驗證您指定了正確的角色名稱。如果名稱正確，請確保角色的策略符合 Macie 擔任該角色的所有要求。如需這些詳細資訊，請參閱設定 IAM 角色以存取受影響的 S3 物件。解決問題後，請再次提交您的要求。

如果您的要求成功，Macie 會在指定區域啟用您帳戶的設定，並且您會收到類似下列內容的輸出。

```
{
  "configuration": {
    "kmsKeyId": "arn:aws:kms:us-east-1:111122223333:alias/ExampleAlias",
    "status": "ENABLED"
  },
  "retrievalConfiguration": {
    "externalId": "o2vee30hs31642lexample",
    "retrievalMode": "ASSUME_ROLE",
    "roleName": "MacieRevealRole"
  }
}
```

其中`kmsKeyId`指定用AWS KMS key來加密所擷取的敏感資料樣本，而且`status`是 Macie 帳戶的組態狀態。這`retrievalConfiguration`些值指定擷取樣本時要使用的存取方法和設定。

> **Note**
>
> 如果您是組織的 Macie 管理員，並且已將 Macie 設定為擔任 IAM 角色，請在回應中記下外部 ID (`externalId`)。每個適用成員帳戶中 IAM 角色的信任政策都必須指定此 ID。否則，您將無法從帳戶擁有的受影響 S3 物件擷取敏感資料樣本。

若要隨後檢查帳戶的設定或組態狀態，請使用GetRevealConfiguration作業AWS CLI，或執行命get-reveal-configuration令。

禁用 Amazon Macie 設置

您可以隨時停用 Amazon Macie 帳戶的組態設定。如果停用組態，Macie 會保留指定AWS KMS key要用來加密所擷取之敏感資料樣本的設定。Macie 會永久刪除該組態的 Amazon S3 存取設定。

> **Warning**
>
> 當您停用 Macie 帳戶的組態設定時，也會永久刪除指定如何存取受影響 S3 物件的目前設定。如果 Macie 目前設定為透過假設 AWS Identity and Access Management (IAM) 角色來存取受影響的物件，則包括：角色名稱，以及 Macie 為組態產生的外部 ID。刪除這些設定後無法復原。

若要停用 Macie 帳戶的組態設定，您可以使用 Amazon Macie 主控台或 Amazon Macie API。

Console

請依照下列步驟使用 Amazon Macie 主控台停用帳戶的組態設定。

若要停用馬西埃設定

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 使用頁面右上角的選取AWS 區域器，選取您要停用 Macie 帳戶組態設定的區域。
3. 在導覽窗格的 [設定] 下，選擇 [顯示範例]。
4. 在 Settings (設定) 區段中，選擇 Edit (編輯)。
5. 在「狀態」 中選擇「停用」。
6. 選擇儲存。

API

若要以程式設計方式停用組態設定，請使用 Amazon Macie API 的UpdateRevealConfiguration操作。在您的要求中，請確定AWS 區域您已指定要停用組態的項目。針對 `status` 參數，請指定 `DISABLED`。

若要使用 AWS Command Line Interface (AWS CLI) 停用組態設定，請執行update-reveal-configuration命令。使用`region`參數可指定要在其中停用組態的「區域」。針對 `status` 參數，請指定 `DISABLED`。例如，如果您AWS CLI在 Microsoft 視窗上使用，請執行下列命令：

```
C:\> aws macie2 update-reveal-configuration --region us-east-1 --
configuration={\"status\":\"DISABLED\"}
```

其中：

- *us-east-1* 是要在其中禁用配置的區域。在此範例中，美國東部 (維吉尼亞北部) 區域。
- DISABLED是組態的新狀態。

如果您的要求成功，Macie 會停用指定區域中帳戶的設定，並且您會收到類似下列內容的輸出。

```
{
    "configuration": {
        "status": "DISABLED"
    }
}
```

您status的 Macie 帳戶配置的新狀態在哪裡。

如果 Macie 設定為假設 IAM 角色來擷取敏感資料範例，您可以選擇性地刪除角色和角色的許可政策。當您停用帳戶的組態設定時，Macie 不會刪除這些資源。此外，Macie 不會使用這些資源為您的帳戶執行任何其他任務。若要刪除角色及其許可政策，您可以使用 IAM 主控台或 IAM API。如需詳細資訊，請參閱《使用指南》中的AWS Identity and Access Management〈刪除角色〉。

擷取和揭示含有發現項目的敏感資料樣

透過使用 Amazon Macie，您可以擷取並揭示 Macie 在個別敏感資料發現項目中報告的敏感資料樣本。這包括 Macie 使用受管理資料識別碼偵測到的敏感資料，以及符合自訂資料識別碼條件的資料。這些範例可協助您驗證 Macie 找到的敏感資料的性質。他們還可以協助您針對受影響的 Amazon 簡單儲存服務 (Amazon S3) 物件和儲存貯體量身打造調查。除了亞太區域 (大阪) 和以色列 (特拉維夫) 區域外，您可以擷取並揭露所有 Macie 目前可用的機密資料樣本。 AWS 區域

如果您擷取並顯示發現項目的敏感資料樣本，Macie 會使用對應的敏感資料探索結果中的資料，找出發現項目所報告之敏感資料的前 1 至 10 次出現次出現的情況。然後，Macie 會從受影響的 S3 物件擷取每次出現的前 1-128 個字元。如果發現項目報告了多種類型的敏感資料，Macie 會針對發現項目所報告的最多 100 種敏感資料執行此動作。

當 Macie 從受影響的 S3 物件擷取敏感資料時，Macie 會使用您指定的 AWS Key Management Service (AWS KMS) 金鑰加密資料，將加密的資料暫時儲存在快取中，然後在結果中傳回資料以供尋

找之用。在擷取和加密之後不久，Macie 會永久刪除快取中的資料，除非暫時需要額外保留才能解決操作問題。

如果您選擇再次擷取和顯示發現項目的敏感資料樣本，Macie 會重複尋找、擷取、加密、儲存和最終刪除範例的程序。

如需如何使用 Amazon Macie 主控台擷取和顯示敏感資料樣本的示範，請觀看下列影片：使用 Amazon Macie 擷取和顯示敏感資料樣本。

主題

- 開始之前
- 判斷敏感資料樣本是否可用於尋找項目
- 擷取和顯示用於尋找項目的敏感資料樣本

開始之前

您必須先設定並啟用 Amazon Macie 帳戶的設定，才能擷取和顯示發現項目的敏感資料範例。您還需要與 AWS 管理員合作，以確認您擁有所需的權限和資源。

當您擷取和顯示尋找項目的敏感資料樣本時，Macie 會執行一系列工作來尋找、擷取、加密和顯示範例。Macie 不會針對您的帳戶使用 Macie 服務連結角色來執行這些工作。相反地，您可以使用您的 AWS Identity and Access Management (IAM) 身分，或允許 Macie 在您的帳戶中擔任 IAM 角色。

若要擷取和顯示發現項目的敏感資料樣本，您必須擁有發現項目、對應的敏感資料探索結果，以及您設定 Macie 用來加密敏感資料樣本的存取權。 AWS KMS key 此外，您或 IAM 角色必須被允許存取受影響的 S3 儲存貯體和受影響的 S3 物件。您或角色也必須被允許使用用 AWS KMS key 來加密受影響物件 (如果適用的話)。如果任何 IAM 政策、資源政策或其他許可設定拒絕必要的存取權，就會發生錯誤，而且 Macie 不會傳回發現項目的任何範例。

您還必須被允許執行以下 Macie 操作：

- `macie2:GetMacieSession`
- `macie2:GetFindings`
- `macie2:ListFindings`
- `macie2:GetSensitiveDataOccurrences`

前三個操作允許您訪問您的 Macie 帳戶並檢索發現的詳細信息。最後一個動作可讓您擷取和顯示發現項目的敏感資料範例。

若要使用 Amazon Macie 主控台擷取和顯示敏感資料樣本，您還必須允許執行下列動作：`macie2:GetSensitiveDataOccurrencesAvailability`此動作可讓您判斷個別發現項目是否可使用範例。您不需要執行此動作的權限，即可透過程式設計方式擷取和顯示範例。但是，擁有此權限可以簡化您的樣本擷取作業。

如果您是某個組織的委派 Macie 管理員，並且已將 Macie 設定為假設 IAM 角色來擷取敏感資料範例，則您還必須被允許執行下列動作：`macie2:GetMember`此動作可讓您擷取有關帳戶與受影響帳戶之間關聯的資訊。它可讓 Macie 驗證您目前是受影響帳戶的 Macie 管理員。

如果您不允許執行必要的動作或存取必要的資料和資源，請向 AWS 管理員尋求協助。

判斷敏感資料樣本是否可用於尋找項目

若要擷取和顯示發現項目的敏感資料範例，尋找項目必須符合特定條件。它必須包括特定出現的敏感數據的位置數據。此外，它必須指定有效、對應的敏感資料探索結果的位置。敏感資料探索結果必須儲存在與發現項目 AWS 區域 相同的位置。如果您透過假設 AWS Identity and Access Management (IAM) 角色將 Amazon Macie 設定為存取受影響的 S3 物件，則敏感資料探索結果也必須存放在使用雜湊型訊息驗證碼 (HMAC) 簽署的 S3 物件中。 AWS KMS key

受影響的 S3 物件也需要符合特定條件。物件的 MIME 類型必須是下列其中一種：

- application/avro，對於一個阿帕奇阿夫羅對象容器（.avro）文件
- application/gzip，針對 GNU 壓縮壓縮封存檔 (.gz 或 .gzip) 檔案
- application/json，針對 JSON 或 JSON 行 (.json 或 .jsonl) 檔案
- application/parquet，對於一個阿帕奇鑲木地板（.鑲木地板）文件
- application/vnd.openxmlformats-officedocument.spreadsheetml.sheet，適用於 Microsoft Excel 活頁簿 (.xlsx) 檔案
- application/zip，適用於 ZIP 壓縮封存檔 (.zip) 檔案
- text/csv，適用於 CSV (.csv) 檔案
- text/plain，適用於 CSV、JSON、JSON 行或 TSV 檔案以外的非二進位文字檔
- text/tab-separated-values，針對 TSV (.tsv) 檔案

此外，S3 物件的內容必須與建立發現項目時的內容相同。Macie 檢查對象的實體標籤（ETag），以確定它是否由發現指定的 ETag 匹配。此外，物件的儲存區大小不能超過擷取和顯示敏感資料樣本的適用大小配額。如需適用配額的清單，請參閱Amazon Macie 配額。

如果發現項目和受影響的 S3 物件符合上述條件，則可以使用敏感資料範例來尋找。在嘗試擷取和顯示發現項目的範例之前，您可以選擇性地決定是否適用於特定發現項目的情況。

判斷機密資料範例是否可用於發現項目

您可以使用 Amazon Macie 主控台或 Amazon Macie API 來判斷敏感資料樣本是否可用於尋找項目。

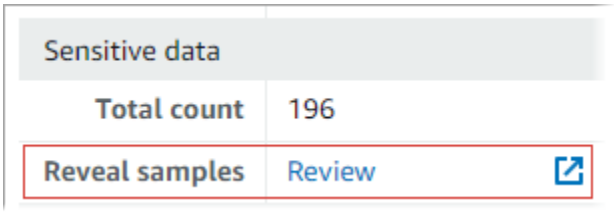
Console

請在 Amazon Macie 主控台上執行下列步驟，以判斷是否有機密資料樣本可供尋找。

若要判斷是否可用於發現項目的範例

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 在導覽窗格中，選擇調查結果。
3. 在「發現的項目」頁面上，選擇發現項目。詳細資料面板會顯示發現項目的資訊。
4. 在詳細資料面板中，捲動至「敏感資料」區段。然後請參閱「顯示範例」欄位。

   如果發現項目可使用敏感資料範例，則欄位中會顯示「檢閱」連結，如下圖所示。



   如果發現項目無法使用敏感資料範例，「顯示範例」欄位會顯示文字，指出下列原因：

   - 不在組織中的帳戶 — 您無法使用 Macie 存取受影響的 S3 物件。受影響的帳戶目前不屬於您組織的一部分。或者該帳戶屬於您組織的一部分，但目前尚未針對該帳戶啟用 Macie。AWS 區域
   - 無效的分類結果 — 發現項目沒有對應的敏感資料探索結果。或者目前無法使用對應的敏感資料探索結果 AWS 區域、格式錯誤或損毀，或使用不支援的儲存格式。Macie 無法驗證要檢索的敏感數據的位置。
   - 無效的結果簽章 — 對應的敏感資料探索結果會儲存在未由 Macie 簽署的 S3 物件中。Macie 無法驗證敏感數據發現結果的完整性和真實性。因此，Macie 無法驗證要檢索的敏感數據的位置。
   - 成員角色過於寬鬆 — 受影響成員帳戶中 IAM 角色的信任或許可政策不符合限制角色存取的 Macie 要求。或者角色的信任原則不會為您的組織指定正確的外部 ID。Macie 不能承擔檢索敏感數據的角色。

- 遺失 GetMember 權限 — 您無法擷取帳戶與受影響帳戶之間關聯的相關資訊。Macie 無法判斷是否允許您以受影響帳戶的委派 Macie 管理員身分存取受影響的 S3 物件。
- 物件超出大小配額 — 受影響 S3 物件的儲存大小超過了從該類型檔案擷取和顯示敏感資料樣本的大小配額。
- 無法使用物件 — 受影響的 S3 物件無法使用。物件已重新命名、移動或刪除，或在 Macie 建立尋找項目之後變更其內容。或者該對象已使用當前禁用 AWS KMS key 的對象進行加密。
- 未簽署結果 — 對應的敏感資料探索結果會儲存在尚未簽署的 S3 物件中。Macie 無法驗證敏感數據發現結果的完整性和真實性。因此，Macie 無法驗證要檢索的敏感數據的位置。
- 角色過於寬鬆 — 您的帳戶設定為使用 IAM 角色 (其信任或許可政策不符合 Macie 限制角色存取權限的要求) 擷取敏感資料的出現次數。Macie 不能承擔檢索敏感數據的角色。
- 不支援的物件類型 — 受影響的 S3 物件使用 Macie 不支援擷取和顯示敏感資料樣本的檔案或儲存格式。受影響 S3 物件的 MIME 類型不是上述清單中的其中一個值。

如果發現項目的敏感資料探索結果發生問題，發現項目的「詳細結果位置」欄位中的資訊可協助您調查問題。此欄位會指定 Amazon S3 中結果的原始路徑。若要調查 IAM 角色的問題，請確保該角色的政策符合 Macie 擔任該角色的所有要求。如需這些詳細資訊，請參閱設定 IAM 角色以存取受影響的 S3 物件。

API

若要以程式設計方式判斷敏感資料樣本是否可用於尋找項目，請使用 Amazon Macie API 的GetSensitiveDataOccurrencesAvailability操作。當您提交請求時，請使用`findingId`參數來指定發現項目的唯一識別碼。要獲取此標識符，您可以使用該ListFindings操作。

如果您使用的是 AWS Command Line Interface (AWS CLI)，請執行 get-sensitive-data-occurrences-availability 命令，並使用`finding-id`參數來指定發現項目的唯一識別碼。要獲取此標識符，您可以運行列表發現項目命令。

如果您的要求成功，而且尋找項目可使用範例，您會收到類似下列的輸出：

```
{
    "code": "AVAILABLE",
    "reasons": []
}
```

如果您的要求成功且尋找項目無法使用範例，則code欄位的值為，UNAVAILABLE而reasons陣列會指定原因。例如：

```
{
    "code": "UNAVAILABLE",
    "reasons": [
        "UNSUPPORTED_OBJECT_TYPE"
    ]
}
```

如果發現項目的敏感資料探索結果發生問題，發現項目classificationDetails.detailedResultsLocation欄位中的資訊可協助您調查問題。此欄位會指定 Amazon S3 中結果的原始路徑。若要調查 IAM 角色的問題，請確保該角色的政策符合 Macie 擔任該角色的所有要求。如需這些詳細資訊，請參閱設定 IAM 角色以存取受影響的 S3 物件。

擷取和顯示用於尋找項目的敏感資料樣本

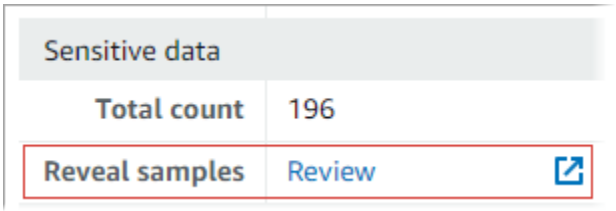
若要擷取和顯示發現項目的敏感資料範例，您可以使用 Amazon Macie 主控台或 Amazon Macie API。

Console

請遵循下列步驟，使用 Amazon Macie 主控台擷取和顯示用於尋找的敏感資料範例。

若要擷取和顯示發現項目的敏感資料範例

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 在導覽窗格中，選擇調查結果。
3. 在「發現的項目」頁面上，選擇發現項目。詳細資料面板會顯示發現項目的資訊。
4. 在詳細資料面板中，捲動至「敏感資料」區段。然後，在「顯示範例」欄位中，選擇「檢閱」：

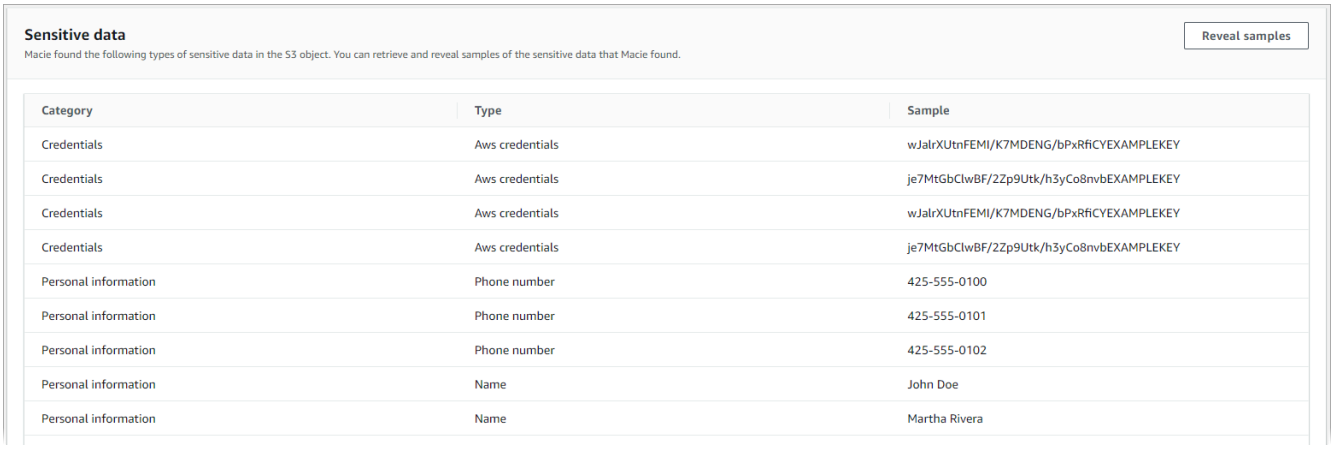


> **Note**
>
> 如果 [顯示範例] 欄位中未顯示 [檢閱] 連結，表示發現項目無法使用敏感資料範例。如需有關為何發生這種情況的詳細資訊，請參閱前面的主題。

選擇複查之後，Macie 會顯示一個頁面，其中摘要發現項目的主要詳細資訊。詳細資料包括 Macie 在受影響的 S3 物件中找到的敏感資料的類別、類型和出現次數。

5. 在頁面的「機密資料」區段中，選擇「顯示範例」。然後，Macie 會擷取並揭示發現項目所報告之前 1-10 次出現之敏感資料的樣本。每個樣本都包含敏感資料出現的前 1—128 個字元。檢索和顯示樣本可能需要幾分鐘的時間。

   如果發現項目報告了多種類型的敏感資料，Macie 會擷取並顯示多達 100 種類型的樣本。例如，下圖顯示了跨越多種類別和敏感資料類型的範例，包括AWS 憑證、美國電話號碼和人員姓名。



   範例會先依機密資料類別組織，然後依機密資料類型進行組織。

API

若要擷取和顯示以程式設計方式尋找的敏感資料範例，請使用 Amazon Macie API 的GetSensitiveDataOccurrences操作。當您提交請求時，請使用`findingId`參數來指定發現項目的唯一識別碼。要獲取此標識符，您可以使用該ListFindings操作。

若要使用 AWS Command Line Interface (AWS CLI) 擷取和顯示敏感資料範例，請執行get-sensitive-data-occurrences命令並使用`finding-id`參數來指定發現項目的唯一識別碼。例如：

```
C:\> aws macie2 get-sensitive-data-occurrences --finding-id
 "1f1c2d74db5d8caa76859ec52example"
```

其中 *1f1c2d74db5d8caa76859ec52* 示例是用於發現項目的唯一標識符。若要使用取得此識別碼 AWS CLI，您可以執行清單發現項目命令。

如果您的要求成功，Macie 會開始處理您的要求，而您會收到類似下列內容的輸出：

```
{
    "status": "PROCESSING"
}
```

處理您的請求可能需要幾分鐘的時間。在幾分鐘內，再次提交您的請求。

如果 Macie 可以尋找、擷取和加密敏感資料樣本，Macie 會傳回地圖中的`sensitiveDataOccurrences`樣本。此對映會指定發現項目報告的敏感資料的 1—100 種類型，並針對每種類型指定 1—10 個範例。每個範例都包含發現項目所報告之敏感資料出現的前 1—128 個字元。

在對映中，每個金鑰都是偵測到敏感資料的受管理資料識別碼的 ID，或偵測到敏感資料的自訂資料識別碼的名稱和唯一識別碼。這些值是指定受管理資料識別碼或自訂資料識別碼的範例。例如，下列回應提供三個人員名稱範例，以及兩個由受管理資料識別碼 (`NAME`和`AWS_CREDENTIALS`分別) 偵測到的 AWS 秘密存取金鑰範例。

```
{
    "sensitiveDataOccurrences": {
        "NAME": [
            {
                "value": "Akua Mansa"
            },
            {
                "value": "John Doe"
            },
            {
                "value": "Martha Rivera"
            }
        ],
        "AWS_CREDENTIALS": [
            {
                "value": "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"
            },
```

```
            {
                "value": "je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY"
            }
        ]
    },
    "status": "SUCCESS"
}
```

如果您的要求成功，但尋找項目無法使用敏感資料範例，您會收到一則UnprocessableEntityException訊息，指出無法使用範例的原因。例如：

```
{
    "message": "An error occurred (UnprocessableEntityException) when calling the
 GetSensitiveDataOccurrences operation: OBJECT_UNAVAILABLE"
}
```

在上述範例中，Macie 嘗試從受影響的 S3 物件擷取樣本，但該物件不再可用。在 Macie 建立尋找項目之後，物件的內容會變更。

如果您的要求成功，但是另一種錯誤類型導致 Macie 無法擷取和顯示發現項目的敏感資料樣本，您會收到類似下列的輸出：

```
{
    "error": "Macie can't retrieve the samples. You're not allowed to access the
 affected S3 object or the object is encrypted with a key that you're not allowed to
 use.",
    "status": "ERROR"
}
```

status欄位的值為ERROR，欄error位說明發生的錯誤。上述主題中的資訊可協助您調查錯誤。

敏感資料位置的 JSON 結構定義

Amazon Macie 使用標準化的 JSON 結構來存放有關在亞馬遜簡單儲存服務 (Amazon S3) 物件中尋找敏感資料之位置的相關資訊。這些結構是由敏感資料發現項目和敏感資料探索結果所使用。對於敏感資料發現項目，這些結構是發現項目 JSON 結構描述的一部分。若要檢閱發現項目的完整 JSON 結構描述，請參閱 Amazon Macie API 參考中的發現項目。若要進一步瞭解敏感資料探索結果，請參閱儲存及保留敏感資料探索結果。

主題

- 敏感資料位置的 JSON 結構描述概觀
- 敏感資料位置的 JSON 結構定義詳細資料和範例

敏感資料位置的 JSON 結構描述概觀

為了報告 Amazon Macie 在受影響 S3 物件中找到的敏感資料的位置，敏感資料發現項目和敏感資料探索結果的 JSON 結構描述包括一個customDataIdentifiers物件和一個sensitiveData物件。customDataIdentifiers物件會提供 Macie 使用自訂資料識別碼偵測到的資料的詳細資料。該sensitiveData對象提供有關 Macie 使用託管數據標識符檢測到的數據的詳細信息。

每個customDataIdentifiers和sensitiveData物件都包含一或多個detections陣列：

- 在customDataIdentifiers物件中，detections陣列會指出哪些自訂資料識別碼偵測到資料並產生尋找項目。對於每個自訂資料識別碼，陣列也會指出識別碼偵測到的資料出現次數。它還可以指示標識符檢測到的數據的位置。
- 在sensitiveData物件中，detections陣列會指出 Macie 使用受管理資料識別碼偵測到的敏感資料類型。對於每種類型的敏感數據，數組還指示數據的出現次數，並且可以指示數據的位置。

對於敏感數據發現，detections數組可以包括 1—15 個occurrences對象。每個occurrences物件都會指定 Macie 偵測到特定類型敏感資料個別出現的位置。

例如，下detections列陣列表示 Macie 在 CSV 檔案中找到的三次出現之敏感資料 (美國社會安全號碼) 的位置。

```
"sensitiveData": [
     {
       "category": "PERSONAL_INFORMATION",
       "detections": [
          {
             "count": 30,
             "occurrences": {
                "cells": [
                   {
                      "cellReference": null,
                      "column": 1,
                      "columnName": "SSN",
                      "row": 2
                   },
                   {
                      "cellReference": null,
```

```
                  "column": 1,
                  "columnName": "SSN",
                  "row": 3
               },
               {
                  "cellReference": null,
                  "column": 1,
                  "columnName": "SSN",
                  "row": 4
               }
            ]
         },
         "type": "USA_SOCIAL_SECURITY_NUMBER"
      }
```

detections陣列中occurrences物件的位置和數目會根據 Macie 在自動化敏感資料探索分析週期或執行敏感資料探索工作期間偵測到的敏感資料的類別、類型和出現次數而有所不同。對於每個分析週期或任務執行，Macie 都會使用深度優先搜尋演算法，將 Macie 在 S3 物件中偵測到的敏感資料 1-15 次出現的位置資料填入產生的發現項目。這些事件表示受影響的 S3 儲存貯體和物件可能包含的敏感資料類別和類型。

occurrences物件可以包含下列任何結構，視受影響的 S3 物件的檔案類型或儲存格式而定：

- cells陣列 — 此陣列適用於微軟 Excel 活頁簿、CSV 檔案和 TSV 檔案。此陣列中的物件會指定 Macie 偵測到敏感資料出現的儲存格或欄位。
- lineRanges陣列 — 此陣列適用於電子郵件訊息 (EML) 檔案，以及 CSV、JSON、JSON 行和 TSV 檔案以外的非二進位文字檔案，例如 HTML、TXT 和 XML 檔案。此陣列中的物件會指定 Macie 偵測到敏感資料中出現的行或包含的行範圍，以及資料在指定一行或多行上的位置。

  在某些情況下，lineRanges陣列中的物件會以另一種陣列類型所支援的檔案類型或儲存格式，指定敏感資料偵測的位置。這些情況包括：偵測其他結構化檔案的非結構化區段，例如檔案中的註解；在 Macie 以純文字分析的格式錯誤檔案中偵測；以及具有 Macie 偵測到敏感資料的一或多個欄名的 CSV 或 TSV 檔案。
- offsetRangesarray-該數組保留供將來使用。如果這個數組存在，它的值為 null。
- pages陣列 — 此陣列適用於 Adobe 可攜式文件格式 (PDF) 檔案。此陣列中的物件會指定 Macie 偵測到敏感資料出現的頁面。
- records陣列 — 此陣列適用於 Apache 的 Avro 物件容器、阿帕奇拼花檔案、JSON 檔案和 JSON 行檔案。對於 Avro 物件容器和 Parquet 檔案，此陣列中的物件會指定記錄索引，以及 Macie 偵測到其中出現敏感資料的記錄中欄位路徑。對於 JSON 和 JSON Lines 檔案，此陣列中的物件會指定

Macie 偵測到敏感資料出現的欄位或陣列的路徑。對於 JSON 行文件，它還指定了包含數據的行的索引。

這些陣列的內容會根據受影響的 S3 物件的檔案類型或儲存格式及其內容而有所不同。

敏感資料位置的 JSON 結構定義詳細資料和範例

Amazon Macie 會針對 JSON 結構的內容進行精心調整，以指出在特定類型檔案和內容中偵測到敏感資料的位置。下列主題說明並提供這些結構的範例。

主題

- 儲存格陣列
- LineRanges陣列
- 頁面陣列
- 記錄陣列

如需可包含在敏感資料尋找項目中之 JSON 結構的完整清單，請參閱 Amazon Macie API 參考中的發現項目。

儲存格陣列

適用於：微軟 Excel 工作簿、CSV 檔案和 TSV 檔

在`cells`陣列中，`Cell`物件會指定 Macie 偵測到敏感資料出現的儲存格或欄位。下表說明`Cell`物件中每個欄位的用途。

欄位	類型	描述
`cellReference`	字串	儲存格的位置，做為絕對儲存格參照，其中包含複本。此欄位僅適用於 Excel 活頁簿。對於 CSV 檔案和 TSV 檔案，此值為空值。
`column`	整數	包含複本之欄的欄編號。對於 Excel 活頁簿，此值與欄識別碼的字母字元相關聯，例如，1對於欄 A、2欄 B 等。

欄位	類型	描述
columnName	字串	包含複本的欄名稱 (如果有的話)。
row	整數	包含出現位置之列的列編號。

下列範例顯示物件的結構，此Cell物件會指定 Macie 在 CSV 檔案中偵測到的敏感資料出現位置。

```
"cells": [
   {
      "cellReference": null,
      "column": 3,
      "columnName": "SSN",
      "row": 5
   }
]
```

在上述範例中，發現項目表示 Macie 偵測到檔案第三欄第五列 (名稱為 SSN) 欄位中的機密資料。

下列範例顯示物件的結構，此Cell物件會指定 Macie 在 Excel 活頁簿中偵測到之敏感資料出現的位置。

```
"cells": [
   {
      "cellReference": "Sheet2!C5",
      "column": 3,
      "columnName": "SSN",
      "row": 5
   }
]
```

在上述範例中，發現項目表示 Macie 偵測到工作簿中名為 Sheet2 的工作表中的敏感資料。在該工作表中，Macie 偵測到第三欄第五列的儲存格中的敏感資料 (欄 C，名為 SSN)。

LineRanges陣列

適用於：電子郵件訊息 (EML) 檔案，以及 CSV、JSON、JSON 行和 TSV 檔案以外的非二進位文字檔案，例如 HTML、TXT 和 XML 檔案

在lineRanges陣列中，Range物件會指定 Macie 偵測到敏感資料出現的行或包含的行範圍，以及資料在指定一行或多行上的位置。

對於物件中其他類型陣列所支援的檔案類型，此occurrences物件通常是空白的。例外情況是：

- 其他結構化檔案的非結構化區段中的資料，例如檔案中的註解。
- Macie 以純文字分析的格式錯誤檔案中的資料。
- CSV 或 TSV 檔案，其中包含一或多個資料行名稱，而 Macie 會在其中偵測到敏感資料。

下表說明lineRanges陣列Range物件中每個欄位的用途。

欄位	類型	描述
end	整數	從檔案開頭到出現位置結束的行數。
start	整數	從檔案開頭到出現位置開始的行數。
startColumn	整數	包含空格且從 1 開始的字元數目，從包含出現位置的第一行開始到出現位置的開頭。start

下列範例顯示Range物件的結構，此物件會指定 Macie 在 TXT 檔案中單行偵測到的敏感資料出現位置。

```
"lineRanges": [
   {
      "end": 1,
      "start": 1,
      "startColumn": 119
   }
]
```

在上述範例中，發現項目表示 Macie 偵測到檔案第一行完全出現的敏感資料 (郵寄地址)。出現的第一個字元是從該行開頭開始的 119 個字元 (含空格)。

下列範例顯示Range物件的結構，該物件指定出現在 TXT 檔案中多行之敏感資料的位置。

```
"lineRanges": [
   {
      "end": 54,
      "start": 51,
      "startColumn": 1
   }
]
```

在上述範例中，發現項目表示 Macie 偵測到跨越檔案第 51 行到 54 行的敏感資料 (郵寄地址)。出現的第一個字符是文件第 51 行的第一個字符。

頁面陣列

適用於：Adobe 可攜式文件格式 (PDF) 檔案

在pages陣列中，Page物件會指定 Macie 偵測到敏感資料出現的頁面。該對象包含一個pageNumber字段。此pageNumber欄位會儲存整數，指定包含具體值之頁面的頁碼。

下列範例顯示物件的結構，此Page物件會指定 Macie 在 PDF 檔案中偵測到的敏感資料出現位置。

```
"pages": [
   {
      "pageNumber": 10
   }
]
```

在上述範例中，發現項目指出檔案的第 10 頁包含具體值。

記錄陣列

適用於：阿帕奇阿夫羅對象容器，阿帕奇實木複合地板文件，JSON 文件和 JSON 行文件

對於 Avro 物件容器或 Parquet 檔案，records陣列中的Record物件會指定記錄索引，以及 Macie 偵測到敏感資料出現的記錄中欄位的路徑。對於 JSON 和 JSON 行檔案，Record物件會指定 Macie 偵測到敏感資料出現之欄位或陣列的路徑。對於 JSON 行文件，它還指定包含出現位置的行的索引。

下表說明Record物件中每個欄位的用途。

欄位	類型	描述
jsonPath	字串	

欄位	類型	描述
		路徑，作為一個 JSONPath 表達式，到出現位置。 對於 Avro 物件容器或實木地板檔案，這是記錄 (`recordIndex`) 中包含出現位置的欄位路徑。對於 JSON 或 JSON 行檔案，這是包含出現位置之欄位或陣列的路徑。如果資料是陣列中的值，路徑也會指出包含出現次數的值。 如果 Macie 偵測到路徑中任何元素名稱中的敏感資料，Macie 就會忽略物件中的`jsonPath`欄位。`Record`如果路徑元素的名稱超過 240 個字元，Macie 會從名稱開頭移除字元來截斷名稱。如果產生的完整路徑超過 250 個字元，Macie 也會從路徑中的第一個元素開始截斷路徑，直到路徑包含 250 個或更少的字元為止。
`recordIndex`	整數	對於 Avro 物件容器或實木地板檔案，記錄索引，從 0 開始，用於包含發生次數的記錄。對於 JSON Lines 檔案，包含出現位置的行索引 (從 0 開始)。此值一律適0用於 JSON 檔案。

下列範例顯示物件的結構，此`Record`物件會指定 Macie 在 Parquet 檔案中偵測到之敏感資料出現的位置。

```
"records": [
   {
      "jsonPath": "$['abcdefghijklmnopqrstuvwxyz']",
      "recordIndex": 7663
   }
]
```

在上述範例中，發現項目表示 Macie 偵測到索引 7663 記錄中的敏感資料 (記錄編號 7664)。在該記錄中，Macie 在名為abcdefghijklmnopqrstuvwxyz的欄位中偵測到敏感資料。記錄中欄位的完整 JSON 路徑為$.abcdefghijklmnopqrstuvwxyz。該字段是根（外層）對象的直接後代。

下列範例也會顯示 Macie 在 Parquet 檔案中偵測到之敏感資料的Record物件結構。但是，在此範例中，Macie 會截斷包含出現位置的欄位名稱，因為名稱超過字元限制。

```
"records": [
   {
      "jsonPath":
 "$['...uvwxyzabcdefghijklmnopqrstuvwxyzabcdefghijklmnopqrstuvwxyzabcdefghijklmnopqrstuvwxyzabc
      "recordIndex": 7663
   }
]
```

在前面的範例中，欄位是根 (外層) 物件的直接子代。

在下列範例中，對於 Macie 在 Parquet 檔案中偵測到的敏感資料，Macie 也會截斷包含該複本之欄位的完整路徑。完整路徑超出字元限制。

```
"records": [
   {
      "jsonPath":
 "$..usssn2.usssn3.usssn4.usssn5.usssn6.usssn7.usssn8.usssn9.usssn10.usssn11.usssn12.usssn13.us
      "recordIndex": 2335
   }
]
```

在上述範例中，發現結果表示 Macie 偵測到索引 2335 記錄中的敏感資料 (記錄編號 2336)。在該記錄中，Macie 在名為abcdefghijklmnopqrstuvwxyz的欄位中偵測到敏感資料。記錄中欄位的完整 JSON 路徑為：

```
$['1234567890']ussn1.usssn2.usssn3.usssn4.usssn5.usssn6.usssn7.usssn8.usssn9.us
```

下列範例顯示物件的結構，此Record物件會指定 Macie 在 JSON 檔案中偵測到的敏感資料出現位置。在此範例中，出現次數是陣列中的特定值。

```
"records": [
   {
      "jsonPath": "$.access.key[2]",
      "recordIndex": 0
   }
]
```

在上述範例中，發現項目表示 Macie 偵測到名為key陣列的第二個值中的敏感資料。陣列是名為的物件的子系access。

下列範例顯示物件的結構，此Record物件會指定 Macie 在 JSON Lines 檔案中偵測到的敏感資料出現位置。

```
"records": [
   {
      "jsonPath": "$.access.key",
      "recordIndex": 3
   }
]
```

在上述範例中，發現項目表示 Macie 偵測到檔案中第三個值 (行) 中的機密資料。在該行中，出現位置位於名為的字段中key，該字段是名為的對象的子項access。

抑制 Amazon Macie 發現

若要簡化發現項目的分析，您可以建立和使用抑制規則。抑制規則是一組以屬性為基礎的篩選條件，用於定義您希望 Amazon Macie 自動存檔發現項目的案例。抑制規則在您已檢閱過一類發現項目且不想再次收到通知的情況下很有幫助。

例如，您可能會決定允許 S3 儲存貯體包含郵寄地址，如果儲存貯體不允許公開存取，而且儲存貯體會以特定物件自動加密新物件AWS KMS key。在此情況下，您可以建立抑制規則，以指定下列欄位的篩選準則：敏感資料偵測類型、S3 儲存貯體公開存取權限和 S3 儲存貯體加密 KMS 金鑰 ID。此規則會隱藏符合篩選準則的 future 發現項目。

如果您使用抑制規則隱藏發現項目，Macie 會繼續為後續出現的機密資料和符合規則條件的潛在策略違規產生發現項目。但是，Macie 會自動將發現項目的狀態變更為已封存。這意味著發現結果默認情況下不會顯示在 Amazon Macie 控制台上，但它們會保留在 Macie 中直到過期。瑪西存儲 90 天的發現。

此外，Macie 不會將抑制的發現 EventBridge 作為事件或發布到亞馬遜。AWS Security Hub不過，Macie 會繼續建立並儲存與您隱藏的敏感資料發現項目相關的敏感資料探索結果。這有助於確保您擁有不可變的敏感資料發現歷史記錄，以進行資料隱私權和保護稽核或您執行的調查。

> **Note**
>
> 如果您的帳戶屬於集中管理多個 Macie 帳戶的組織，則隱藏規則對您的帳戶的運作方式可能會有所不同。這取決於您要隱藏的發現項目類別，以及您是否擁有 Macie 管理員或成員帳戶：
>
> - 策略發現項目 — 只有 Macie 管理員可以隱藏組織帳號的策略發現項目。
>
>   如果您擁有 Macie 管理員帳戶並建立了一個抑制規則，Macie 會將規則套用至組織中所有帳號的策略發現項目，除非您將規則設定為排除特定帳號。如果您有 Macie 成員帳戶，並且想要隱藏帳戶的政策發現，請聯絡您的 Macie 管理員。
> - 敏感資料發現項目 — Macie 管理員和個別成員可以隱藏敏感資料探索工作產生的敏感資料發現項目。Macie 管理員也可以抑制 Macie 在為組織執行自動化敏感資料探索時產生的發現項目。
>
>   只有建立敏感資料探索工作的帳戶才能隱藏或以其他方式存取工作產生的機密資料發現項目。只有組織的 Macie 管理員帳戶可以隱藏或以其他方式存取針對組織中帳戶自動化敏感資料探索產生的發現項目。
>
> 如需有關管理員和成員可執行之工作的詳細資訊，請參閱了解 Amazon Macie 管理員和會員帳戶之間的關係。

若要建立和管理抑制規則，您可以使用 Amazon Macie 主控台或 Amazon Macie API。下列主題說明如何進行。對於 API，主題包括如何使用 AWS Command Line Interface(AWS CLI) 執行這些工作的範例。您也可以使用目前版本的其他AWS命令列工具或 AWS SDK，或直接將 HTTPS 要求傳送至 Macie 來執行這些工作。如需AWS工具和 SDK 的相關資訊，請參閱要建置的工具。AWS

主題

- 建立抑制規則
- 複查抑制的發現
- 變更抑制規則
- 刪除抑制規則

建立抑制規則

建立抑制規則之前，請務必注意，您無法還原 (取消封存) 使用抑制規則所隱藏的發現項目。但是，您可以在 Amazon Macie 主控台上查看抑制的發現項目，並使用 Amazon Macie API 存取抑制的發現結果。

建立抑制規則時，您可以指定篩選準則、名稱以及規則的描述 (選擇性)。您可以使用亞馬遜 Macie 主控台或亞馬 Amazon Macie API 來建立抑制規則。

Console

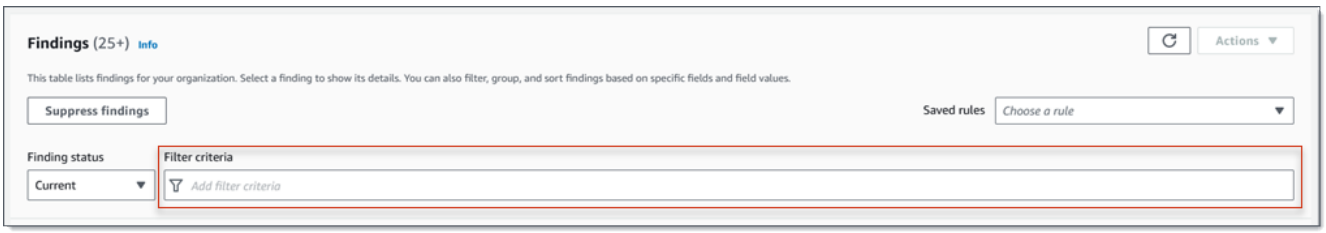
請依照下列步驟使用 Amazon Macie 主控台建立抑制規則。

建立隱藏規則

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 在導覽窗格中，選擇 Findings (問題清單)。

> **Tip**
>
> 若要使用現有的抑制或篩選規則作為起點，請從「已儲存的規則」清單中選擇規則。您也可以先依預先定義的邏輯群組樞紐和向下鑽研發現項目，藉此簡化規則的建立作業。如果您這麼做，Macie 會自動建立並套用適當的篩選條件，這對於建立規則很有幫助的起點。若要執行此操作，請在導覽窗格 (「搜尋結果」下) 中選擇「依時段」、「依類型」或「依工作」，然後選擇表格中的項目。在詳細資料面板中，選擇要旋轉之欄位的連結。

3. 在「篩選條件」方塊中，新增篩選條件，以指定您要規則隱藏之發現項目的屬性。



若要瞭解如何新增篩選條件，請參閱建立並將篩選套用至發現項目。

4. 完成新增規則的篩選條件後，請選擇 [隱藏發現項目]。
5. 在隱藏規則下，輸入規則的名稱，並選擇性地輸入規則的描述。
6. 選擇 儲存 。

API

若要以程式設計方式建立抑制規則，請使用 Amazon Macie API 的CreateFindingsFilter作業，並為所需參數指定適當的值：

- 對於`action`參數，請指定`ARCHIVE`以確保 Macie 隱藏符合規則條件的發現項目。
- 對於`criterion`參數，請指定定義規則篩選準則的條件對映。

  在對映中，每個條件都應指定欄位、運算子以及欄位的一或多個值。值的類型和數目取決於您選擇的欄位和運算子。如需有關可在條件中使用之欄位、運算子和值類型的資訊，請參閱篩選發現項目的欄位在條件下使用運算子、和指定欄位的值。

若要使用建立抑制規則AWS CLI，請執行指create-findings-filter令並為所需參數指定適當的值。下列範例會建立一個隱藏規則，該規則會傳回目前AWS 區域和報告 S3 物件中郵寄地址 (且不包含其他類型的敏感資料) 中的所有敏感資料發現項目。

此範例針對 Linux、macOS 或 Unix 進行格式化，並使用反斜線 (\) 行接續字元來改善可讀性。

```
$ aws macie2 create-findings-filter \
--action ARCHIVE \
--name my_suppression_rule \
--finding-criteria '{"criterion":
{"classificationDetails.result.sensitiveData.detections.type":{"eqExactMatch":
["ADDRESS"]}}}'
```

此範例針對 Microsoft Windows 進行格式化，並使用脫字符號 (^) 行接續字元來提高可讀性。

```
C:\> aws macie2 create-findings-filter ^
--action ARCHIVE ^
--name my_suppression_rule ^
--finding-criteria={\"criterion\":
{\"classificationDetails.result.sensitiveData.detections.type\":{\"eqExactMatch\":
[\"ADDRESS\"]}}}
```

其中：

- 我的`##########`。
- `criterion`是規則的篩選條件對映：
  - `########. #####. ## .type ############### JSON #`稱。

- *eqExactMatch*指定等於精確匹配運算符。
- ADDR@@ *ESS* 是敏感資料偵測類型欄位的列舉值。

如果此命令成功執行，您會收到類似如下的輸出。

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/8a3c5608-
aa2f-4940-b347-d1451example",
    "id": "8a3c5608-aa2f-4940-b347-d1451example"
}
```

其中arn是所建立之抑制規則的 Amazon 資源名稱 (ARN)，id是規則的唯一識別碼。

如需篩選準則的其他範例，請參閱使用 Amazon Macie API 以程式設計方式篩選結果。

複查抑制的發現

默認情況下，Macie 不會在 Amazon Macie 控制台上顯示抑制的發現項目。不過，您可以透過變更篩選器設定，在主控台上檢閱這些發現項目。

在主控台上檢閱隱藏的發現項目

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 在導覽窗格中，選擇 Findings (問題清單)。「發現項目」頁面會顯示 Macie 在過去 90 天內為您的帳戶建立或更新AWS 區域的發現項目。根據預設，這不包括由抑制規則所抑制的發現項目。
3. 針對「搜尋結果」狀態，執行下列其中一項作業
   - 若只要顯示隱藏的發現項目，請選擇已存檔
   - 若要顯示隱藏與未抑制的搜尋結果，請選擇「全部」。
   - 若要再次隱藏隱藏的發現項目，請選擇目前

您也可以使用 Amazon Macie API 存取抑制的發現項目。若要擷取隱藏的發現項目清單，請使用ListFindings作業並包含為archived欄位指定true的篩選條件。如需如何使用執行此操作的範例AWS CLI，請參閱以編程方式過濾。若要接著擷取一或多個隱藏發現項目的詳細資訊，請使用此GetFindings作業，並為每個要擷取的發現項目指定唯一的識別碼。

變更抑制規則

您可以隨時使用亞馬遜 Macie 主控台或亞馬 Amazon Macie API 來變更抑制規則的設定。您也可以指派和管理規則的標籤。

標籤是您定義並指派給特定AWS資源類型的標籤。每個標籤都包含必要的標籤鍵和一個可選的標籤值。標籤可協助您以不同的方式識別、分類及管理資源，例如依用途、擁有者、環境或其他條件。如需進一步了解，請參閱 標記亞馬遜麥西資源。

Console

請遵循下列步驟，使用 Amazon Macie 主控台變更現有抑制規則的設定。

變更抑制規則

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 在導覽窗格中，選擇 Findings (問題清單)。
3. 在「已存規則」清單中，選擇您要變更的隱藏規則旁邊的編輯圖示 ( )。
4. 執行下列任何一項：
   - 若要變更規則的條件，請使用「篩選條件」方塊輸入條件，以指定您要規則隱藏之發現項目屬性的條件。如要瞭解如何作業，請參閱 建立並將篩選套用至發現項目。
   - 若要變更規則的名稱，請在「隱藏規則」下的「名稱」方塊中輸入新名稱。
   - 若要變更規則的描述，請在「隱藏規則」下的「描述」方塊中輸入新描述。
   - 若要指派、檢閱或編輯規則的標籤，請選擇「隱藏規則」下的「管理標籤」。然後視需要檢閱並變更標籤。一個規則最多可以有 50 個標籤。
5. 完成變更之後，請選擇 Save (儲存)。

API

若要以程式設計方式變更抑制規則，請使用 Amazon Macie API 的UpdateFindingsFilter操作。當您提交請求時，請使用支援的參數為您要變更的每個設定指定新值。

針對`id`參數，指定要變更之規則的唯一識別碼。您可以使用ListFindingsFilter操作來擷取帳戶的隱藏和篩選規則清單，以取得此識別碼。如果您使用的是AWS CLI，請執行list-findings-filters命令以擷取此清單。

若要使用變更抑制規則AWS CLI，請執行指update-findings-filter令並使用支援的參數為您要變更的每個設定指定新值。例如，下列指令會變更既有抑制規則的名稱。

```
C:\> aws macie2 update-findings-filter --id 8a3c5608-aa2f-4940-b347-d1451example --
name mailing_addresses_only
```

其中：

- *###########*
- *##########*稱。

如果此命令成功執行，您會收到類似如下的輸出。

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/8a3c5608-
aa2f-4940-b347-d1451example",
    "id": "8a3c5608-aa2f-4940-b347-d1451example"
}
```

其中arn是已變更之規則的 Amazon 資源名稱 (ARN)，id是規則的唯一識別碼。

同樣地，下列範例會將action參數的值從NOOP變更為，將篩選規則轉換為隱藏規則ARCHIVE。

```
C:\> aws macie2 update-findings-filter --id 8a1c3508-aa2f-4940-b347-d1451example --
action ARCHIVE
```

其中：

- *###########*
- *ARCHIVE* 是 Macie 對符合規則條件的發現項目執行的新動作 — 隱藏發現項目。

如果命令執行成功，您會收到類似下列內容的輸出：

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/8a1c3508-
aa2f-4940-b347-d1451example",
    "id": "8a1c3508-aa2f-4940-b347-d1451example"
}
```

其中arn是已變更之規則的 Amazon 資源名稱 (ARN)，id是規則的唯一識別碼。

刪除抑制規則

您可以隨時使用亞馬遜 Macie 主控台或亞馬 Amazon Macie API 刪除抑制規則。如果您刪除抑制規則，Macie 會停止隱藏符合規則準則且不會被其他規則抑制的新發現項目和後續發現項目。但請注意，Macie 可能會繼續隱藏目前正在處理並符合規則條件的發現項目。

刪除抑制規則後，符合規則條件的新發現項目和後續發現項目的狀態為目前 (未封存)。這意味著它們默認顯示在 Amazon Macie 控制台上。此外，Macie 將這些發現 EventBridge 作為事件發布給亞馬遜。根據您帳戶的發佈設定，Macie 也會將發現項目發佈至AWS Security Hub。

Console

請依照下列步驟使用 Amazon Macie 主控台刪除抑制規則。

刪除抑制規則

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 在導覽窗格中，選擇 Findings (問題清單)。
3. 在「已存規則」清單中，選擇您要刪除之隱藏規則旁邊的編輯圖示 ( )。
4. 在「隱藏規則」下選擇「刪除」。

API

若要以程式設計方式刪除抑制規則，請使用 Amazon Macie API 的DeleteFindingsFilter操作。對於id參數，指定要刪除之抑制規則的唯一識別碼。您可以使用ListFindingsFilter操作來擷取帳戶的隱藏和篩選規則清單，以取得此識別碼。如果您使用的是AWS CLI，請執行list-findings-filters命令以擷取此清單。

若要使用刪除抑制規則AWS CLI，請執行delete-findings-filter指令。例如：

```
C:\> aws macie2 delete-findings-filter --id 8a3c5608-aa2f-4940-b347-d1451example
```

其中 *8a3c5608-A2F-4940*-b347-d1451 範例是要刪除之抑制規則的唯一識別碼。

如果命令運行成功，馬西返回一個空的 HTTP 200 響應。否則，馬西會傳回 HTTP 4 xx 或 500 回應，指出作業失敗的原因。

Amazon Macie 調查結果的嚴重性評分

Amazon Macie 產生政策或敏感資料尋找時，會自動為發現項目指派嚴重性。發現項目的嚴重性反映了發現項目的主要特徵，可協助您評估並排定發現項目的優先順序。發現項目的嚴重性並不暗示或以其他方式表示受影響資源對您的組織可能具有的重要性或重要性。

對於政策發現，嚴重性取決於 Amazon Simple Storage Service (Amazon S3) 一般用途儲存貯體的安全性或隱私權潛在問題的性質。對於敏感資料發現項目，嚴重性是根據 Macie 在 S3 物件中發現之敏感資料的性質和出現次數而定。

在 Macie 中，發現項目的嚴重性以兩種方式表示。

嚴重性等級

這是嚴重性的定性表示。嚴重程度範圍從Low最不嚴重程度到High最嚴重程度。

嚴重性等級直接顯示在 Amazon Macie 控制台上。它們也可以在 Macie 主控台、Amazon Macie API 以 JSON 表示形式顯示發現項目，以及與敏感資料發現項目相關的敏感資料探索結果中提供。在查找 Macie 發布給 Amazon 的事件以 EventBridge 及 Macie 發布的調查結果中還包括嚴重性級別。 AWS Security Hub

嚴重性評分

這是嚴重性的數值表示。嚴重性分數範圍介於 1 到 3 之間，並直接對應至嚴重性等級：

嚴重性評分	嚴重性等級
1	低
2	中
3	高

嚴重性分數不會直接顯示在 Amazon Macie 主控台上。但是，它們可以在 Macie 主控台、Amazon Macie API 以 JSON 表示形式顯示發現項目，以及與敏感資料發現項目相關的敏感資料探索結果中提供。在查找 Macie 發布給 Amazon EventBridge 的事件中還包括嚴重性分數。它們不包含在 Macie 發布的調查結果中。 AWS Security Hub

本節中的主題說明 Macie 如何判斷原則發現項目和敏感資料發現的嚴重性。

主題

政策發現的嚴重性評分

政策發現的嚴重性取決於 S3 一般用途儲存貯體的安全性或隱私權潛在問題的性質。下表列出 Macie 指派給每一種策略發現項目類型的嚴重性層級。如需每種類型的描述，請參閱問題清單類型。

調查結果類型	嚴重性等級
Policy:IAMUser/S3BlockPublicAccessDisabled	高
Policy:IAMUser/S3BucketEncryptionDisabled	低
Policy:IAMUser/S3BucketPublic	高
Policy:IAMUser/S3BucketReplicatedExternally	高
Policy:IAMUser/S3BucketSharedExternally	高
Policy:IAMUser/S3BucketSharedWithCloudFront	中

原則發現項目的嚴重性不會根據發現項目的出現次數而變更。

敏感資料發現的嚴重性評分

敏感資料發現的嚴重性是根據 Macie 在 S3 物件中發現之敏感資料的性質和出現次數而定。下列主題說明 Macie 如何判斷每種類型的敏感性資料發現項目的嚴重性：

- SensitiveData:S3Object/Credentials
- SensitiveData:S3Object/CustomIdentifier
- SensitiveData:S3Object/Financial
- SensitiveData:S3Object/Personal
- SensitiveData:S3Object/Multiple

有關 Macie 可以在敏感數據發現項目中檢測和報告的敏感數據類型的詳細信息，請參閱使用受管資料識別符和建置自訂資料識別符。

SensitiveData:S3Object/Credentials

答：S3 物件/認證SensitiveData尋找表示 S3 物件包含敏感登入資料資料。針對此類型的發現項目，Macie 會根據 Macie 在物件中找到之認證資料的類型和出現次數來判斷嚴重性。

下表指出 Macie 指派給報告 S3 物件中登入資料資料出現之發現項目的嚴重性層級。

敏感資料類型	1 次出現	2 至 99 次事件	發生 100 次或更多次
AWS 秘密訪問密鑰	高	高	高
谷歌雲 API 密鑰	高	高	高
HTTP 基本授權標頭	高	高	高
網絡令牌	高	高	高
OpenSSH 私密金鑰	高	高	高
PGP 私密金鑰	高	高	高
公開金鑰加密標準 (PKCS) 私密金鑰	高	高	高
PuTTY 私密金鑰	高	高	高
條紋 API 金鑰	高	高	高

SensitiveData:S3Object/CustomIdentifier

答：S3Object/ SensitiveData發現CustomIdentifier表示 S3 物件包含符合一或多個自訂資料識別碼偵測準則的文字。物件可能包含一種以上的敏感資料類型。

根據預設，Macie 會將「中」嚴重性層級指派給此類型的尋找 — 如果 S3 物件包含至少一個符合自訂資料識別碼偵測條件的文字，Macie 會自動將「中」嚴重性層級指派給發現項目。發現項目的嚴重性不會根據符合自訂資料識別碼準則的文字出現次數而變更。

不過，如果您為產生發現項目的自訂資料識別碼定義了自訂嚴重性設定，則此類型發現項目的嚴重性可能會有所不同。如果是這種情況，Macie 確定嚴重性如下：

- 如果 S3 物件包含的文字只符合一個自訂資料識別碼的偵測準則，Macie 會根據該識別碼的嚴重性設定判斷發現項目的嚴重性。
- 如果 S3 物件包含符合多個自訂資料識別碼偵測準則的文字，Macie 會評估每個自訂資料識別碼的嚴重性設定，判斷哪些設定會產生最高嚴重性，然後為發現項目指派最高嚴重性，以判斷發現項目的嚴重性。

若要檢閱自訂資料識別碼的嚴重性設定，請在 Amazon Macie 主控台的導覽窗格中選擇「自訂資料識別碼」。然後選擇自定義數據標識符的名稱。「嚴重性」區段會顯示設定。如需詳細資訊，請參閱定義尋找自訂資料識別碼的嚴重性設定。

SensitiveData:S3Object/Financial

答：S3 物件/財務SensitiveData發現表示 S3 物件包含敏感財務資訊。針對此類型的發現項目，Macie 會根據 Macie 在物件中找到的財務資訊的類型和出現次數來決定嚴重性。

下表指出 Macie 指派給報告 S3 物件中財務資訊發生次數之發現項目的嚴重性層級。

敏感資料類型	1 次出現	2 至 99 次事件	發生 100 次或更多次
銀行帳戶號碼 [1]	高	高	高
信用卡到期日	低	中	高
信用卡磁條數據	高	高	高
信用卡, 號碼, [2]	高	高	高
信用卡驗證碼	中	高	高

1. 任何銀行帳號類型的嚴重性等級都相同 — 基本銀行帳戶號碼 (BBAN)、國際銀行帳戶號碼 (IBAN) 或加拿大或美國的銀行帳戶號碼。
2. 關鍵字附近或不在關鍵字附近的信用卡號碼，嚴重性等級相同。

如果發現項目報告了物件中的多種財務資訊類型，Macie 會計算 Macie 找到之每種財務資訊類型的嚴重性，判斷哪種類型會產生最高嚴重度，然後將最高嚴重性指定給發現項目，以判斷發現項目的嚴重性。例如，如果 Macie 在物件中偵測到 10 個信用卡到期日 (中嚴重性等級) 和 10 個信用卡號碼 (高嚴重性等級)，Macie 會將「高」嚴重性等級指定給發現項目。

SensitiveData:S3Object/Personal

答：S3 物件/個人SensitiveData發現表示 S3 物件包含敏感的個人資訊，包括個人健康資訊 (PHI)、個人識別資訊 (PII) 或兩者的組合。對於這種類型的發現，Macie 會根據 Macie 在對象中找到的個人信息的類型和出現次數來確定嚴重性。

下表指出 Macie 指派給敏感資料發現項目的嚴重性等級，這些資料發現項目會報告 S3 物件中 PHI 的發現次數。

敏感資料類型	1 次出現	2 至 99 次事件	發生 100 次或更多次
毒品執法機構 (DEA) 註冊號碼	高	高	高
Health 保險索償編號	高	高	高
健康保險或醫療識別號碼	高	高	高
醫療保健通用程序編碼系統 (HCPCS) 代碼	高	高	高
美国国家药品法典	高	高	高
國家供應商識別碼 (NPI)	高	高	高
唯一裝置識別碼 (UDI)	低	中	高

下表指出 Macie 指派給敏感資料發現項目的嚴重性層級，這些資料可報告 S3 物件中 PII 的發現次數。

敏感資料類型	1 次出現	2 至 99 次事件	發生 100 次或更多次
	低	中	高

敏感資料類型	1 次出現	2 至 99 次事件	發生 100 次或更多次
出生日期			
駕照識別號碼	低	中	高
選民名冊號碼	高	高	高
全名	低	中	高
全球定位系統 (GPS) 座標	低	中	中
餅乾	低	中	高
郵寄地址	低	中	高
國家身分證號碼	高	高	高
國民保險號碼 (NINO)	高	高	高
護照號碼	中	高	高
永久居留號碼	高	高	高
電話號碼	低	中	高
社會保險號碼 (SIN)	高	高	高
社會安全號碼 (SSN)	高	高	高
納稅識別號碼或參考號碼	高	高	高
車輛識別號碼 (VIN)	低	低	中

如果發現項目報告了物件中多種類型的 PHI、PII 或同時報告 PHI 和 PII，Macie 會計算每個類型的嚴重性、判斷哪個類型會產生最高嚴重性，然後將最高嚴重性指派給發現項目，以判斷發現項目的嚴重性。

例如，如果 Macie 在物件中偵測到 10 個完整名稱 (「中」嚴重性等級) 和 5 個護照號碼 (「高嚴重性等級」)，Macie 會將「高」嚴重性等級指定給發現項目。同樣地，如果 Macie 在物件中偵測到 10 個完整名稱 (中嚴重性等級) 和 10 個健康保險識別碼 (高嚴重性等級)，Macie 就會將「高」嚴重性等級指定給發現項目。

SensitiveData:S3Object/Multiple

答：S3Object/Multiple SensitiveData發現表示 S3 物件包含跨越多個敏感資料類別的資料，包括憑證資料、財務資訊、個人資訊或符合一或多個自訂資料識別碼偵測準則的任意組合。

針對此類型的發現項目，Macie 會計算 Macie 找到之每種敏感資料類型的嚴重性 (如前述主題所示)，判斷哪個類型會產生最高嚴重性，並將最高嚴重性指派給發現項目，以判斷嚴重性。

例如，如果 Macie 在物件中偵測到 10 個完整名稱 (「中」嚴重性層級) 和 10 個 AWS 秘密存取金鑰 (「高」嚴重性層級)，Macie 會將「高」嚴重性等級指定給發現項目。

監控和處理 Amazon Macie Macie Macie

為了支援與其他應用程式、服務和系統 (例如監控或事件管理系統) 的整合，Amazon Macie 會自動將政策和敏感資料發現EventBridge作為事件發佈到 Amazon。如需組織安全性狀態的其他支援和更廣泛的分析，您可以將 Macie 設定為也將政策和敏感資料發現項目發佈至AWS Security Hub。

Amazon EventBridge

Amazon EventBridge ie ie ie 可從應用程式和服務交付即時資料串流，然後將該資料路由到等AWS Lambda目標。Amazon Kinesis ie ie CloudWatch 使用EventBridge，您可以自動監視和處理特定類型的事件，包括 Macie 針對發現項目發佈的事件。若要進一步了解EventBridge，請參閱 Amazon EventBridge 使用者指南。

如果您將 AWS 使用者通知與 Macie 整合，您也可以使用EventBridge事件自動產生有關 Macie 針對發現項目而發佈的事件的通知。透過使用者通知，您可以建立自訂規則並設定傳遞管道，以接收有關感興趣EventBridge事件的通知。傳送管道包括電子郵件、AWS Chatbot聊天通知和 AWS Console Mobile Application推播通知。您也可以在上的中央位置檢閱通知AWS Management Console。若要進一步了解使用者通知，請參閱 AWS 使用者通知使用者指南。

AWS Security Hub

AWS Security Hub一種安全服務，可供您全面檢視AWS環境中的安全狀態。它可從AWS 服務和支援的AWS Partner Network安全產業業業業業業業標準和最佳實務。它也可協助您分析安全趨勢，並識別最高優先級的安全問題。使用 Security Hub，您可以檢閱 Macie Macie 的清單，作為更廣泛分析組織的安全狀態。您也可以彙總來自多個 AWS 區域 的調查結果，以及監控並處理來自單一區域的彙總調查結果資料。若要進一步了解 Security Hub，請參閱使AWS Security Hub用者指南。

當 Macie 建立尋找項目時，它會自動將尋找項目發佈EventBridge至新事件。根據您為帳戶選擇的發佈設定，Macie 也可以將發現項目發佈到 Security Hub。Macie 會在完成處理發現項目後立即發佈每個新發現項目。如果 Macie 偵測到後續發生的現有原則發現項目，就會發佈發現項目的現有EventBridge事件的更新。根據您的發佈設定，Macie 也可以將更新發佈到 Security Hub。Macie 會使用您在帳戶的發佈設定中指定的發佈頻率，定期發佈這些更新。

主題

- 設定 Amazon Macie 發現項目的發佈設定
- Amazon Macie 與亞馬遜集成 EventBridge
- Amazon Macie 與集成 AWS Security Hub

- Amazon Macie 與 AWS 使用者通知整合
- Amazon Macie 發現的亞馬遜 EventBridge 事件模式

設定 Amazon Macie 發現項目的發佈設定

為了支援與其他應用程式、服務和系統的整合，Amazon Macie 會自動將政策發現結果和敏感資料發現 EventBridge 作為事件發佈到 Amazon。如需有關如何用 EventBridge 來監視和處理發現項目的資訊，請參閱Amazon Macie 與亞馬遜集成 EventBridge。

您可以使用您在帳戶的發行設定 AWS Security Hub 中指定的目的地選項，將 Macie 設定為自動發佈結果。使用這些選項，您可以將 Macie 設定為僅發佈原則發現項目、僅發佈敏感資料發現項目，或將原則和敏感資料發現項目同時發佈至 Security Hub。您也可以設定 Macie 停止將任何發現項目發佈至 Security Hub。如需如何使用 Security Hub 監視和處理發現項目的相關資訊，請參閱Amazon Macie 與集成 AWS Security Hub。

對於政策發現項目，Macie 將發現項目發佈到另一個尋找項目的時間 AWS 服務 取決於發現項目是否為新的，以及您為帳戶指定的發佈頻率。針對敏感資料發現項目，時間永遠是立即的 — Macie 會在處理完尋找項目之後立即發佈敏感資料尋找項目。與政策發現不同，Macie 會將所有敏感資料發現項目視為新的 (唯一)。

請注意，Macie 不會發佈由抑制規則自動封存的原則或敏感資料發現項目。換句話說，Macie 不會將抑制的發現發現發布給其他 AWS 服務人。

主題

- 選擇發現項目的地
- 決定發現項目的發佈頻率
- 變更發現項目的發佈頻率

選擇發現項目的地

除了 Amazon 之外，您還可以將 Amazon Macie 設定為自動將政策和敏感資料發現發現項目發佈到 Amazon EventBridge。 AWS Security Hub 根據預設，Macie 只會將新的和更新的原則發現發現發現發現發佈到 Security Hub 若要變更或延伸預設組態，請調整帳戶的發佈目的地設定。

當您調整目的地設定時，您可以選擇要讓 Macie 發佈到 Security Hub 中心的發現項目類別 — 僅限原則發現項目、只有發現的機密資料，或兩者都發現原則和敏感資料。您也可以選擇停止將任何類別的尋找項目發佈到 Security Hub。

如果您變更目的地設定，您的變更只會套用至目前的目的地設定 AWS 區域。如果您是組織的 Macie 管理員，您的變更只會套用至您的帳戶。它不適用於任何關聯的成員帳戶。如需詳細資訊，請參閱 管理多個 帳戶。

若要選擇發現項目的地的發佈

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 在導覽窗格中，選擇設定。
3. 在「發現項目的發佈」區段的「目的地」下，從下列選項中選擇：

   - 將原則發現項目發現項目發佈至 Security Hub — 選取此核取方塊可開始自動將新的和更新的原則發現項目發佈至 Security Hub 若要停止將新的和更新的原則發現項目發佈到 Security Hub，請清除此核取方塊。

     如果您選取此核取方塊，而且您有現有的原則發現項目，Macie 不會自動將它們發佈到 Security Hub。相反地，Macie 只會在您儲存變更後發佈它所建立或更新的原則發現項目。
   - 將敏感資料發現項目發佈至 Security Hub — 選取此核取方塊可開始自動將新的敏感資料發現項目發佈到 Security Hub。若要停止將新的敏感資料發現項目發佈到 Security Hub，請清除此核取方塊。

     如果您選取此核取方塊，而且您有現有的機密資料發現項目，Macie 不會自動將它們發佈到 Security Hub。相反地，Macie 只會發佈儲存變更後所建立的那些敏感資料發現項目。
4. 選擇 儲存。

如果您選擇將發現項目的任何類別發佈到 Security Hub，請確定您也啟用目前區域中的安全中心，並將其設定為接受來自 Macie 的發現項目。否則，您將無法存取資訊安全中心中的發現項目。若要瞭解如何接受 Security Hub 中的發現項目，請參閱AWS Security Hub 使用者指南中的管理產品整合。

決定發現項目的發佈頻率

在 Amazon Macie 中，每個發現項目都有一個唯一的識別碼。Macie 會使用此識別碼來決定何時將發現項目發佈到另一個 AWS 服務尋找項目：

- 新發現項目 — 當 Macie 建立新的原則或敏感資料發現項目時，會將唯一識別碼指派給發現項目，作為處理發現項目的一部分。Macie 完成處理發現後，立即將發現作為一個新的 Amazon EventBridge 事件發布。根據您帳戶的發佈設定，Macie 也會將發現項目發佈為中 AWS Security Hub的新發現項目。

- 已更新的發現項目 — 當 Macie 偵測到現有原則發現項目的後續發現項目時，會新增有關後續發現項目的詳細資訊，並遞增發生次數，以更新現有發現項目。Macie 也會將這些更新發佈至現有的 EventBridge事件，而且根據您帳戶的發行設定，現有的 Security Hub 發現項目。馬西這樣做只是為了政策調查結果。與原則發現的機密資料不同，都會被視為新的 (唯一)。

  默認情況下，Macie 每 15 分鐘發布一次更新的發現作為週期性發布週期的一部分。這意味著，在最近發布週期之後更新的任何政策調查結果將被保留，並在需要時再次更新，並包含在下一個發布週期中（約 15 分鐘後）。您可以選擇不同的出版頻率來變更此排程。例如，如果您將 Macie 設定為每小時發佈更新的發現項目，而發佈時間為 12:00，則在 12:00 之後發生的任何更新都會在 13:00 發佈。

請注意，這兩種情況都不適用於由隱藏規則自動封存的發現項目。Macie 不會將抑制的發現發現發布給其他 AWS 服務.

變更發現項目的發佈頻率

您可以變更 Amazon Macie 用來將更新發佈到其他 AWS 服務政策發現的現有政策發現項目的排程。默認情況下，Macie 每 15 分鐘發布一次更新的發現。如果您變更此排程，您的變更只會套用至目前的排程 AWS 區域。如果您是組織的 Macie 管理員，您的變更也會套用至區域中所有相關聯的成員帳戶。如需詳細資訊，請參閱 管理多個 帳戶。

若要變更更新發現項目的發佈頻率

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 在導覽窗格中，選擇設定。
3. 在「發現項目的發佈」段落的「更新原則發現項目的更新頻率」下，選擇您希望 Macie 將更新的原則發現項目發佈到其他 AWS 服務人的頻率。
4. 選擇 Save (儲存)。

Amazon Macie 與亞馬遜集成 EventBridge

亞馬遜EventBridge，以前是亞馬遜CloudWatch活動，是一種無服務器事件總線服務。EventBridge從應用程式和服務提供即時資料串流，然後將該資料路由到AWS Lambda函數、Amazon Simple Notification Service (Amazon SNS) 主題和 Amazon Kinesis Streams 等目標。若要進一步了解 EventBridge，請參閱 Amazon EventBridge 使用者指南。

使用EventBridge，您可以自動監視和處理特定類型的事件。這包括 Amazon Macie 針對新政策發現和敏感資料發現自動發佈的事件。這也包括 Macie 為後續發現的現有策略發現項目自動發佈的事件。如需 Macie 如何及何時發佈這些事件的詳細資訊，請參閱設定發現項目的發行設定。

透過使用EventBridge和 Macie 針對發現項目發佈的事件，您可以近乎即時地監視和處理發現項目。然後，您可以使用其他應用程序和服務根據發現採取行動。例如，您可EventBridge以使用將特定類型的新發現項目傳送至AWS Lambda函數。Lambda 函數可能會處理資料並將其傳送至安全事件和事件管理 (SIEM) 系統。如果將 AWS 使用者通知與 Macie 整合，您也可以使用事件，透過您指定的交付管道自動通知發現結果。

除了自動化監控和處理之外，使用的還EventBridge可以長期保留您的發現項目資料。瑪西存儲 90 天的發現。使用時EventBridge，您可以將發現結果資料傳送至您偏好的儲存平台，並且只要您喜歡的時間就可以儲存資料。

> **Note**
>
> 對於長期保留，也請將 Macie 儲存在 S3 儲存貯體中的敏感資料探索結果。敏感資料探索結果是記錄 Macie 對 S3 物件執行分析的詳細資料，以判斷物件是否包含敏感資料。如需進一步了解，請參閱 儲存及保留敏感資料探索結果。

主題

與亞馬遜合作 EventBridge

使用 AmazonEventBridge，您可以建立規則來指定要監控的事件，以及要針對這些事件執行自動動作的目標。目標是EventBridge將事件傳送至的目的地。

若要自動監控和處理發現項目的任務，您可以建立自動偵測 Amazon Macie 尋找事件的EventBridge規則，並將這些事件傳送到另一個應用程式或服務以進行處理或其他動作。您可以自訂規則，以僅傳送符合特定條件的事件。若要執行此操作，請指定衍生自EventBridge 發現項目的事件綱要。

例如，您可以建立一個將特定類型的新問題清單傳送至AWS Lambda函數的規則。然後 Lambda 函數可以執行以下任務：處理資料並將其傳送至 SIEM 系統；自動將特定類型的伺服器端加密套用至 S3 物件；或透過變更物件的存取控制清單 (ACL) 來限制 S3 物件的存取。或者，您可以建立規則，自動將新的高嚴重性發現項目傳送至 Amazon SNS 主題，然後通知您的事件回應團隊有關發現項目的資訊。

除了叫用 Lambda 函數和通知 Amazon SNS 主題外，還EventBridge支援其他類型的目標和動作，例如將事件轉送到 Amazon Kinesis Streams、啟用AWS Step Functions狀態機器，以及叫用執行命令。AWS Systems Manager如需支援目標的相關資訊，請參閱 Amazon EventBridge使用者指南中的 Amazon EventBridge 目標。

為發現項目建立 Amazon EventBridge 規則

下列程序說明如何使用 Amazon EventBridge 主控台和 AWS Command Line Interface(AWS CLI) 為 Amazon Macie 發現項目建立EventBridge規則。此規則會偵測EventBridge使用 Macie 事件的事件，然後將這些事件傳送至AWS Lambda函數進行處理。

AWS Lambda 是一項運算服務，可供您用來執行程式碼，無需佈建或管理伺服器。您封裝程式碼並將其上傳到 AWS Lambda 作為 Lambda 函數。當叫用函數時，AWS Lambda 才會執行函數。函數可由您人工呼叫，可以自動回應事件，或回應應用程式或服務的請求。如需建立和叫用 Lambda 函數的相關資訊，請參閱AWS Lambda開發人員指南。

Console

此程序說明如何使用 Amazon EventBridge 主控台建立自動將所有 Macie 發現事件傳送至 Lambda 函數進行處理的規則。此規則會針對接收到特定事件時執行的規則使用預設設定。如需規則設定的詳細資訊，或瞭解如何建立使用自訂設定的規則，請參閱 Amazon 使用EventBridge者指南中的建立對事件做出反應的規則。

> **Tip**
>
> 您也可以建立使用自訂模式的規則，以便僅對一部分 Macie 事件進行偵測並據其採取行動則。此子集可以 Macie 在尋找事件中包含的特定欄位為基礎。若要瞭解可用欄位，請參閱EventBridge 發現項目的事件綱要。若要了解如何建立此類規則，請參閱 Amazon EventBridge 使用者指南中的事件模式中的內容篩選。

在建立此規則之前，請先建立您希望讓規則作為目標使用的 Lambda 函數。在建立規則時，您需要將此函數指定為該規則的目標。

使用主控台建立事件規則

1. 在以下位置打開亞馬遜EventBridge控制台 https://console.aws.amazon.com/events/。
2. 在導覽窗格的 Events (事件) 下，選擇 Rules (規則)。
3. 在 Rules (規則) 區段中，選擇 Create Rule (建立規則)。

4. 在定義規則詳細資訊頁面，執行下列動作：

   - 對於 Name (名稱)，請輸入規則的名稱。
   - (選用) 對於 Description (描述)，輸入規則的簡短描述。
   - 對於事件匯流排，請確定已選取預設值，並開啟在選取的事件匯流排上啟用規則。
   - 針對 Rule type (規則類型) 選擇 Rule with an event pattern (具有事件模式的規則)。

5. 完成後，請選擇 Next (下一步)。
6. 在建立事件模式頁面，執行下列動作：

   - 對於事件來源，請選擇AWS事件或EventBridge合作夥伴。
   - (選擇性) 對於範例事件，請檢閱 Macie 的範例尋找事件，以瞭解事件可能包含的內容。要做到這一點，選擇AWS事件。然後，針對範例事件，選擇「Macie 尋找」。
   - 對於事件模式，選擇事件模式表單。然後輸入以下設定：
     - 在 Event source (事件來源)，選擇 AWS 服務。
     - 對於 AWS 服務，輸入馬西。
     - 針對「事件類型」，輸入 Macie 搜尋結果。

7. 完成後，請選擇 Next (下一步)。
8. 在選取目標頁面，執行下列動作：

   - 對於 Target types (目標類型)，選擇 AWS 服務。
   - 對於選取目標，輸入 Lambda 函數。然後，對於 Function (函數)，選擇您要傳送尋找事件的 Lambda 函數。
   - 對於 Con figure version/alias (設定版本/別名)，輸入目標 Lambda 函數的版本和別名設定。
   - (選擇性) 對於其他設定，請輸入自訂設定以指定要傳送至 Lambda 函數的事件資料。您也可以指定如何處理未成功傳遞至函數的事件。

9. 完成後，請選擇 Next (下一步)。
10. 在設定標籤頁面上，選用輸入要指派給規則的一或多個標籤。然後選擇 Next (下一步)。
11. 在檢閱和建立頁面，檢閱規則設定並確認它們是否正確。

    若要變更設定，請在包含設定的區段中選擇編輯，然後輸入正確的設定。您也可以使用導覽索引標籤移至包含設定的頁面。

12. 完成驗證設定後，請選擇 [建立規則]。

AWS CLI

此程序說明如何使用建立AWS CLI將所有 Macie 尋找事件傳送至 Lambda 函數進行處理的EventBridge規則。此規則會針對接收到特定事件時執行的規則使用預設設定。在該過程中，這些命令被格式化為微軟視窗。如果是 Linux、macOS 或 Unix，請以反斜線 (\) 取代插入符號 (^) 行接續字元。

在建立此規則之前，請先建立您希望讓規則作為目標使用的 Lambda 函數。在建立函數時，請記住函數的 Amazon 資源名稱 (ARN)。在指定規則的目標時，需要輸入此 ARN。

若要使用建立事件規則 AWS CLI

1. 建立一個規則，以偵測 Macie 發佈至EventBridge的所有發現項目的事件。若要這麼做，請使用 EventBridge put-rule 指令。例如：

```
C:\> aws events put-rule ^
--name MacieFindings ^
--event-pattern "{\"source\":[\"aws.macie\"]}"
```

其中*MacieFindings*是您要用於規則的名稱。

如果命令執行成功，則 EventBridge 會使用規則的 ARN 來回應。請記住 ARN。您需要在步驟 3 輸入此名稱。

> **Tip**
>
> 您也可以建立使用自訂模式的規則，以便僅對一部分 Macie 事件進行偵測並據其採取行動則。此子集可以 Macie 在尋找事件中包含的特定欄位為基礎。若要瞭解可用欄位，請參閱EventBridge 發現項目的事件綱要。若要了解如何建立此類規則，請參閱 Amazon EventBridge 使用者指南中的事件模式中的內容篩選。

2. 指定要用作規則目標的 Lambda 函數。若要執行這項操作，請使用EventBridge放置目標指令。例如：

```
C:\> aws events put-targets ^
--rule MacieFindings ^
--targets Id=1,Arn=arn:aws:lambda:regionalEndpoint:accountID:function:my-findings-function
```

其中*MacieFindings*是您在步驟 1 中為規則指定的名稱，而Arn參數的值為您希望讓規則作為目標使用的函數 ARN。

3. 新增允許規則呼叫目標 Lambda 函數的許可。若要這麼做，請使用 Lambda 新增權限命令。例如：

```
C:\> aws lambda add-permission ^
--function-name my-findings-function ^
--statement-id Sid ^
--action lambda:InvokeFunction ^
--principal events.amazonaws.com ^
--source-arn arn:aws:events:regionalEndpoint:accountId:rule:MacieFindings
```

其中：

- *my-findings-function*是您希望讓規則作為目標使用的 Lambda 函數名稱。
- *Sid* 是您定義來描述 Lambda 函數政策陳述式的陳述式識別符。
- source-arn 是 EventBridge 規則的 ARN。

如果此命令成功執行，您會收到類似如下的輸出：

```
{
  "Statement": "{\"Sid\":\"sid\",
    \"Effect\":\"Allow\",
    \"Principal\":{\"Service\":\"events.amazonaws.com\"},
    \"Action\":\"lambda:InvokeFunction\",
    \"Resource\":\"arn:aws:lambda:us-east-1:111122223333:function:my-findings-
function\",
    \"Condition\":
      {\"ArnLike\":
        {\"AWS:SourceArn\":
         \"arn:aws:events:us-east-1:111122223333:rule/MacieFindings\"}}}"
}
```

Statement 值是陳述式的 JSON 字串版本，且已新增至 Lambda 函數政策。

Amazon Macie 與集成 AWS Security Hub

AWS Security Hub是一項服務，可讓您全面檢視整個AWS環境的安全性狀態，並協助您根據安全性產業標準和最佳實務來檢查您的環境。它部分是通過消耗，聚合，組織和優先級從多個AWS 服務和支持的AWS Partner Network安全解決方案中的發現結果來完成此操作。Security Hub 可協助您分析安全性趨勢，並找出最優先順序的安全性問題。使用 Security Hub，您也可以彙總多個發現項目AWS 區域，然後監視並處理來自單一區域的所有彙總發現項目資料。若要進一步了解資訊 Security Hub，請參閱使AWS Security Hub用者指南。

Amazon Macie 與 Security Hub 集成，這意味著您可以將發現從 Macie 發布到 Security Hub 自動。Security Hub 接著可將這些問題清單納入其安全狀態的分析中。此外，您可以使用 Security Hub 來監視和處理原則和敏感資料發現項目，作為AWS環境中較大、彙總的發現項目資料集的一部分。換句話說，您可以分析 Macie 發現項目，同時對組織的安全性狀態執行更廣泛的分析，並視需要修復發現項目。Security Hub 可降低處理來自多個提供者之大量發現項目的複雜性。此外，它對所有發現都使用標準格式，包括 Macie 的發現結果。使用此格式，即AWS安全性發現格式 (ASFF)，您無需執行耗時的資料轉換工作。

主題

- Amazon Macie 如何發布調查結果 AWS Security Hub
- Amazon Macie 發現的例子 AWS Security Hub
- 啟用和設定AWS Security Hub整合
- 停止發現項目的發佈至 AWS Security Hub

Amazon Macie 如何發布調查結果 AWS Security Hub

在 AWS Security Hub 中，系統會將安全問題作為問題清單來追蹤。有些發現來自 Amazon Macie 或受支援的AWS Partner Network安全解決方案偵測到的問題。AWS 服務Security Hub 也有一組規則，用來偵測安全問題並產生問題清單。

Security Hub 提供工具來管理所有這些來源的發現項目。您可以檢閱和篩選發現項目清單，並檢閱個別發現項目的詳細資訊。若要瞭解如何進行，請參閱AWS Security Hub使用指南中的檢視尋找結果清單和詳細資料 您也可以追蹤問題清單的調查狀態。若要瞭解如何進行，請參閱AWS Security Hub使用者指南中的對發現項目採取行動。

所有 Security Hub 中的問題清單都使用稱為 AWS 安全問題清單格式 (ASFF) 的標準 JSON 格式。ASFF 包含有關問題來源、受影響的資源以及發現項目目前狀態的詳細資訊。請參閱《AWS Security Hub 使用者指南》中的 AWS 安全問題清單格式 (ASFF)。

馬西發布的發現類型

根據您為 Macie 帳戶選擇的發行設定，Macie 可以將它建立的所有發現項目發佈到 Security Hub，包括敏感資料發現項目和原則發現項目。如需有關這些設定及如何變更這些設定的資訊，請參閱設定發現項目的發行設定。根據預設，Macie 只會發佈新的和更新的原則發現項目至 Security Hub。Macie 不會將敏感資料發現項目發佈到 Security Hub。

敏感資料發現

如果您將 Macie 設定為將敏感資料發現項目發佈至 Security Hub，Macie 會自動發佈為您的帳戶建立的每個敏感資料發現項目，並在處理完尋找項目後立即發佈。Macie 會針對未由抑制規則自動封存的所有敏感資料發現項目執行此動作。

如果您是組織的 Macie 管理員，則發佈僅限於您執行之敏感資料探索工作的發現項目，以及 Macie 為您的組織執行的自動化敏感資料探索活動。只有建立工作的帳戶才能發佈工作產生的機密資料發現項目。只有 Macie 管理員帳戶可以發佈自動化敏感資料探索為其組織產生的敏感資料發現項目。

當 Macie 將敏感資料發現項目發佈到 Security Hub 時，它會使用AWS安全性尋找格式 (ASFF)，這是安全性中心中所有發現項目的標準格式。在 ASFF 中，Types欄位會指出發現項目的類型。此欄位使用的分類法與 Macie 中尋找類型分類法略有不同。

下表列出 Macie 可建立之每種類型之敏感資料發現項目的 ASFF 尋找項目類型。

馬西查找類型	ASFF 問題清單類型
SensitiveData:S3Object/Credentials	Sensitive Data Identifications/Passwords/SensitiveData:S3Object-Credentials
SensitiveData:S3Object/CustomIdentifier	Sensitive Data Identifications/PII/SensitiveData:S3Object-CustomIdentifier
SensitiveData:S3Object/Financial	Sensitive Data Identifications/Financial/SensitiveData:S3Object-Financial
SensitiveData:S3Object/Multiple	Sensitive Data Identifications/PII/SensitiveData:S3Object-Multiple

馬西查找類型	ASFF 問題清單類型
SensitiveData:S3Object/Personal	Sensitive Data Identifications/PII/SensitiveData:S3Object-Personal

政策結果

如果您將 Macie 設定為將原則發現項目發佈至 Security Hub，Macie 會自動發佈它建立的每個新原則發現項目，並在完成處理發現項目後立即發佈。如果 Macie 偵測到後續發生的現有原則發現項目，它會使用您為帳戶指定的發佈頻率，自動將更新發佈至 Security Hub 中的現有發現項目。Macie 會針對所有未由抑制規則自動封存的原則發現項目執行這些工作。

如果您是組織的 Macie 系統管理員，則發佈僅限於您帳戶直接擁有之 S3 儲存貯體的政策發現項目。Macie 不會發佈它為組織中的成員帳戶建立或更新的政策發現項目。這有助於確保安全中心中沒有重複的發現項目資料。

與敏感資料發現的情況一樣，Macie 會在將新的和更新的原則發現項目發佈到 AWS Security Hub 時使用安全性尋找格式 (ASFF)。在 ASFF 中，Types欄位使用的分類法與 Macie 中的尋找類型分類法略有不同。

下表列出 Macie 可建立之每一種原則發現項目類型的 ASFF 發現項目類型。如果 Macie 在 2021 年 1 月 28 日或之後在資訊安全中心中建立或更新原則發現項目，則發現項目的 ASFF Types 欄位在「安全性中心」中具有下列其中一個值。

馬西查找類型	ASFF 問題清單類型
Policy:IAMUser/S3BlockPublicAccessDisabled	Software and Configuration Checks/AWS Security Best Practices/Policy:IAMUser-S3BlockPublicAccessDisabled
Policy:IAMUser/S3BucketEncryptionDisabled	Software and Configuration Checks/AWS Security Best Practices/Policy:IAMUser-S3BucketEncryptionDisabled
Policy:IAMUser/S3BucketPublic	Effects/Data Exposure/Policy:IAMUser-S3BucketPublic

馬西查找類型	ASFF 問題清單類型
Policy:IAMUser/S3BucketReplicatedExternally	Software and Configuration Checks/AWS Security Best Practices/Policy:IAMUser-S3BucketReplicatedExternally
Policy:IAMUser/S3BucketSharedExternally	Software and Configuration Checks/AWS Security Best Practices/Policy:IAMUser-S3BucketSharedExternally
Policy:IAMUser/S3BucketSharedWithCloudFront	Software and Configuration Checks/AWS Security Best Practices/Policy:IAMUser-S3BucketSharedWithCloudFront

如果 Macie 在 2021 年 1 月 28 日之前建立或上次更新原則發現項目，則此發現項目具有「安全中心」中「ASFFTypes」欄位的下列其中一個值：

- Policy:IAMUser/S3BlockPublicAccessDisabled
- Policy:IAMUser/S3BucketEncryptionDisabled
- Policy:IAMUser/S3BucketPublic
- Policy:IAMUser/S3BucketReplicatedExternally
- Policy:IAMUser/S3BucketSharedExternally

上述清單中的值會直接對應至 Macie 中「尋找項目類型」(type) 欄位的值。

> **Note**
>
> 當您在 Security Hub 中檢閱和處理原則發現項目時，請注意下列例外狀況：
>
> - 在某些情況下AWS 區域，Macie 早在 2021 年 1 月 25 日就開始使用 ASFF 尋找新的和更新的結果類型。
> - 如果您在 Macie 開始使用您的 ASFF 尋找型態之前，在 Security Hub 中執行原則尋找動作 AWS 區域，則發現項目的 ASFF Types 欄位的值將會是上述清單中其中一個 Macie 尋找型

態。它不會是上一個表格中的 ASFF 尋找項目類型之一。這適用於您使用AWS Security Hub主控台或 AWS Security Hub API BatchUpdateFindings 作業所採取的原則發現項目。

發佈發現項目的延遲

當 Macie 建立新的原則或敏感資料發現項目時，它會在處理完尋找項目之後，立即將發現項目發佈至 Security Hub。

當 Macie 偵測到後續發生的現有原則發現項目時，會將更新發佈至現有的「Security Hub」發現項目。更新的時間取決於您為 Macie 帳戶選擇的發佈頻率。默認情況下，Macie 每 15 分鐘發布一次更新。如需詳細資訊，包括如何變更帳戶的設定，請參閱設定發現項目的發行設定。

當 Security Hub 不可用時重試發行

如果 Security Hub 無法使用，Macie 會建立 Security Hub 尚未收到的發現項目佇列。當系統恢復，Macie 重試發行，直到 Security Hub 收到的發現。

更新 Security Hub 中的現有問題清單

Macie 將原則尋找發現項目發佈至「Security Hub」之後，Macie 會更新發現項目，以反映任何其他發現項目或發現項目活動。馬西這樣做只是為了政策調查結果。與原則發現的機密資料不同，都會被視為新的 (唯一)。

當 Macie 發佈更新至原則發現項目時，Macie 會更新發現項目的「更新時間」(`UpdatedAt`) 欄位的值。您可以使用此值來判斷 Macie 最近何時偵測到後續發生的潛在策略違規或產生發現項目的問題。

如果欄位的現有值不是 ASFF 尋找項目類型，Macie 也可能會更新發現項目的「類型」(`Types`) 欄位的值。這取決於您是否已根據安全中心中的發現採取行動。如果您尚未針對搜尋結果採取行動，Macie 會將欄位的值變更為適當的 ASFF 搜尋結果型態。如果您使用AWS Security Hub控制台或 AWS Security Hub API 的操作對發現進行了BatchUpdateFindings操作，Macie 不會更改字段的值。

Amazon Macie 發現的例子 AWS Security Hub

當 Amazon Macie 將發現項目發佈到時AWS Security Hub，它會使用AWS安全性尋找格式 (ASFF)。這是安全中心中所有發現項目的標準格式。下列範例會使用範例資料來示範 Macie 以此格式發佈至 Security Hub 之發現項目資料的結構和性質：

- 敏感資料尋找範例
- 原則發現項目的範例

在 Security Hub 中尋找敏感資料的範例

下面是一個敏感數據發現 Macie 發佈到 Security Hub 使用 ASFF 的例子。


```
{
    "SchemaVersion": "2018-10-08",
    "Id": "5be50fce24526e670df77bc00example",
    "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/macie",
    "ProductName": "Macie",
    "CompanyName": "Amazon",
    "Region": "us-east-1",
    "GeneratorId": "aws/macie",
    "AwsAccountId": "111122223333",
    "Types":[
        "Sensitive Data Identifications/PII/SensitiveData:S3Object-Personal"
    ],
    "CreatedAt": "2022-05-11T10:23:49.667Z",
    "UpdatedAt": "2022-05-11T10:23:49.667Z",
    "Severity": {
        "Label": "HIGH",
        "Normalized": 70
    },
    "Title": "The S3 object contains personal information.",
    "Description": "The object contains personal information such as first or last
 names, addresses, or identification numbers.",
    "ProductFields": {
        "JobArn": "arn:aws:macie2:us-east-1:111122223333:classification-
job/698e99c283a255bb2c992feceexample",
        "S3Object.Path": "DOC-EXAMPLE-BUCKET1/2022 Sourcing.tsv",
        "S3Object.Extension": "tsv",
        "S3Bucket.effectivePermission": "NOT_PUBLIC",
        "OriginType": "SENSITIVE_DATA_DISCOVERY_JOB",
        "S3Object.PublicAccess": "false",
        "S3Object.Size": "14",
        "S3Object.StorageClass": "STANDARD",
        "S3Bucket.allowsUnencryptedObjectUploads": "TRUE",
        "JobId": "698e99c283a255bb2c992feceexample",
        "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
macie/5be50fce24526e670df77bc00example",
        "aws/securityhub/ProductName": "Macie",
        "aws/securityhub/CompanyName": "Amazon"
    },
    "Resources": [
        {
```

```
            "Type": "AwsS3Bucket",
            "Id": "arn:aws:s3:::DOC-EXAMPLE-BUCKET1",
            "Partition": "aws",
            "Region": "us-east-1",
            "Details": {
                "AwsS3Bucket": {
                    "OwnerId":
 "7009a8971cd538e11f6b6606438875e7c86c5b672f46db45460ddcd08example",
                    "OwnerName": "johndoe",
                    "OwnerAccountId": "444455556666",
                    "CreatedAt": "2020-12-30T18:16:25.000Z",
                    "ServerSideEncryptionConfiguration": {
                        "Rules": [
                            {
                                "ApplyServerSideEncryptionByDefault": {
                                    "SSEAlgorithm": "aws:kms",
                                    "KMSMasterKeyID": "arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
                                }
                            }
                        ]
                    },
                    "PublicAccessBlockConfiguration": {
                        "BlockPublicAcls": true,
                        "BlockPublicPolicy": true,
                        "IgnorePublicAcls": true,
                        "RestrictPublicBuckets": true
                    }
                }
            }
        },
        {
            "Type": "AwsS3Object",
            "Id": "arn:aws:s3:::DOC-EXAMPLE-BUCKET1/2022 Sourcing.tsv",
            "Partition": "aws",
            "Region": "us-east-1",
            "DataClassification": {
                "DetailedResultsLocation": "s3://macie-data-discovery-results/
AWSLogs/111122223333/Macie/us-east-1/
                698e99c283a255bb2c992feceexample/111122223333/32b8485d-4f3a-3aa1-be33-
aa3f0example.jsonl.gz",
                "Result":{
                    "MimeType": "text/tsv",
                    "SizeClassified": 14,
```

```
                    "AdditionalOccurrences": false,
                    "Status": {
                        "Code": "COMPLETE"
                    },
                    "SensitiveData": [
                        {
                            "Category": "PERSONAL_INFORMATION",
                            "Detections": [
                                {
                                    "Count": 1,
                                    "Type": "USA_SOCIAL_SECURITY_NUMBER",
                                    "Occurrences": {
                                        "Cells": [
                                            {
                                                "Column": 10,
                                                "Row": 1,
                                                "ColumnName": "Other"
                                            }
                                        ]
                                    }
                                }
                            ],
                            "TotalCount": 1
                        }
                    ],
                    "CustomDataIdentifiers": {
                        "Detections": [
                        ],
                        "TotalCount": 0
                    }
                }
            },
            "Details": {
                "AwsS3Object": {
                    "LastModified": "2022-04-22T18:16:46.000Z",
                    "ETag": "ebe1ca03ee8d006d457444445example",
                    "VersionId": "SlBC72z5hArgexOJifxw_IN57example",
                    "ServerSideEncryption": "aws:kms",
                    "SSEKMSKeyId": "arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
                }
            }
        }
    ],
```

```
    "WorkflowState": "NEW",
    "Workflow": {
        "Status": "NEW"
    },
    "RecordState": "ACTIVE",
    "FindingProviderFields": {
        "Severity": {
            "Label": "HIGH"
        },
        "Types": [
            "Sensitive Data Identifications/PII/SensitiveData:S3Object-Personal"
        ]
    },
    "Sample": false,
    "ProcessedAt": "2022-05-11T10:23:49.667Z"
}
```

資訊安全中心中的原則尋找範例

以下是 Macie 在 ASFF 中發佈至安全中心的新原則的範例。

```
{
    "SchemaVersion": "2018-10-08",
    "Id": "36ca8ba0-caf1-4fee-875c-37760example",
    "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/macie",
    "ProductName": "Macie",
    "CompanyName": "Amazon",
    "Region": "us-east-1",
    "GeneratorId": "aws/macie",
    "AwsAccountId": "111122223333",
    "Types": [
        "Software and Configuration Checks/AWS Security Best Practices/Policy:IAMUser-
S3BlockPublicAccessDisabled"
    ],
    "CreatedAt": "2022-04-24T09:27:43.313Z",
    "UpdatedAt": "2022-04-24T09:27:43.313Z",
    "Severity": {
        "Label": "HIGH",
        "Normalized": 70
    },
    "Title": "Block Public Access settings are disabled for the S3 bucket",
    "Description": "All Amazon S3 block public access settings are disabled for the
 Amazon S3 bucket. Access to the bucket is
```

```
      controlled only by access control lists (ACLs) or bucket policies.",
    "ProductFields": {
        "S3Bucket.effectivePermission": "NOT_PUBLIC",
        "S3Bucket.allowsUnencryptedObjectUploads": "FALSE",
        "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
macie/36ca8ba0-caf1-4fee-875c-37760example",
        "aws/securityhub/ProductName": "Macie",
        "aws/securityhub/CompanyName": "Amazon"
    },
    "Resources": [
        {
        "Type": "AwsS3Bucket",
        "Id": "arn:aws:s3:::DOC-EXAMPLE-BUCKET2",
        "Partition": "aws",
        "Region": "us-east-1",
        "Tags": {
            "Team": "Recruiting",
            "Division": "HR"
        },
        "Details": {
            "AwsS3Bucket": {
              "OwnerId":
 "7009a8971cd538e11f6b6606438875e7c86c5b672f46db45460ddcd08example",
              "OwnerName": "johndoe",
              "OwnerAccountId": "444455556666",
              "CreatedAt": "2020-11-25T18:24:38.000Z",
              "ServerSideEncryptionConfiguration": {
                "Rules": [
                    {
                    "ApplyServerSideEncryptionByDefault": {
                        "SSEAlgorithm": "aws:kms",
                        "KMSMasterKeyID": "arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
                    }
                  }
                ]
              },
              "PublicAccessBlockConfiguration": {
                "BlockPublicAcls": false,
                "BlockPublicPolicy": false,
                "IgnorePublicAcls": false,
                "RestrictPublicBuckets": false
               }
            }
```

```
          }
        }
    ],
    "WorkflowState": "NEW",
    "Workflow": {
        "Status": "NEW"
    },
    "RecordState": "ACTIVE",
    "FindingProviderFields": {
        "Severity": {
            "Label": "HIGH"
        },
        "Types": [
            "Software and Configuration Checks/AWS Security Best Practices/
Policy:IAMUser-S3BlockPublicAccessDisabled"
        ]
    },
    "Sample": false
}
```

啟用和設定AWS Security Hub整合

若要整合 Amazon Macie 與AWS Security Hub, 啟用 Security Hub 為您AWS 帳戶. 若要瞭解如何進行，請參閱使AWS Security Hub用者指南中的啟用安全性中樞。

當您同時啟用 Macie 和 Security Hub 時，整合會自動啟用。根據預設，Macie 會開始自動將新的和更新的原則發現項目發佈到 Security Hub。您不需要採取其他步驟來設定整合。如果您在啟用整合時有現有的原則發現項目，Macie 不會將它們發佈到 Security Hub。而是，Macie 只會在啟用整合後發佈它所建立或更新的原則發現項目。

您可以選擇性地自訂組態，方法是選擇是否要在 Security Hub 中選擇性地將更新發佈至原則發現項目的更新頻率。您也可以選擇將敏感資料發現項目發佈到 Security Hub。如要了解如何使用，請參閱 設定發現項目的發行設定。

停止發現項目的發佈至 AWS Security Hub

若要停止將發現項目發佈到AWS Security Hub，您可以變更 Amazon Macie 帳戶的發佈設定。如要了解如何使用，請參閱 選擇發現項目的地。您也可以使用安全中心主控台或安全中 Security Hub API 來執行此操作。若要瞭解如何進行，請參閱《AWS Security Hub使用指南》中的 < 停用和啟用整合中的發現項目流程 (主控台) > 或停用整合中的發現項目流程 (Security Hub API、AWS CLI)。

Amazon Macie 與 AWS 使用者通知整合

AWS 使用者通知是一項服務，可做為AWS Management Console.AWS 這包括 Amazon CloudWatch 警示、AWS Support案例和來自其他人的通訊等通知AWS 服務。透過使用者通知，您可以設定自訂規則和交付管道，以接收有關特定類型 Amazon EventBridge 事件的通知。傳送管道包括電子郵件、AWS Chatbot聊天通知和AWS Console Mobile Application推播通知。您也可以在 AWS 使用者通知主控台上查看通知。若要進一步了解使用者通知，請參閱 AWS 使用者通知使用者指南。

Macie 與 AWS 使用者通知整合，這表示您可以設定使用者通知，以通知您 Macie EventBridge 針對政策和敏感資料發現而發佈的事件。如果搜尋結果事件符合您指定的條件，「使用者通知」會產生通知。通知包括關聯發現項目的主要詳細資料，例如發現項目的類型和嚴重性，以及受影響資源的名稱。「使用者通知」也可以將通知傳送至您指定的一或多個傳送管道。您可以根據安全性和合規性工作流程量身打造自己選擇的交付管道。

例如，您可以將「使用者通知」設定為針對特定類型的新高嚴重性發現項目產生通知。您也可以指定AWS Chatbot為這些通知的傳遞管道。接著，「使用者通知」會偵測發現項目的 EventBridge 事件、產生包含發現項目資料的通知，並將通知傳送至AWS Chatbot。 AWS Chatbot然後可能會將通知路由到 Slack 頻道或 Amazon Chime 聊天室，以通知您的事件回應團隊。

主題

使用 AWS 使用者通知

使用 AWS 使用者通知，您可以建立規則以指定要監控和接收通知的 Amazon EventBridge 事件類型。規則定義 EventBridge 事件必須符合才能產生通知的條件。您也可以為規則選擇一或多個傳遞管道。傳遞管道會指定您要接收符合規則條件之事件通知的位置。

如果「使用者通知」偵測到符合規則條件的 EventBridge 事件，則會執行下列一般工作：

1. 從事件中提取數據的子集。
2. 產生包含萃取資料的通知。

3. 將通知傳送至您為該事件類型指定的傳遞通道。

通知的設計和結構已針對傳送至的每個傳遞通道進行最佳化。

若要控制接收通知的頻率或數目，您可以設定規則的彙總設定。如果您啟用這些設定，使用者通知會將多個事件的資料合併為單一通知。您可以選擇快速且頻繁地傳送彙總的事件通知，這些通知可能需要執行高嚴重性的尋找事件。或者減少傳送頻率，以減少接收通知，您可能想要這樣做來處理低嚴重性的尋找事件。如果合併事件資料，您可以使用 AWS 使用者通知主控台深入檢閱每個彙總事件的詳細資訊。從那裡，您也可以在 Amazon Macie 主控台上導覽至每個關聯的搜尋結果。

針對 Amazon Macie 發現項目啟用和設定 AWS 使用者通知

若要讓 AWS 使用者通知產生 Amazon Macie 發現項目的通知，請在使用者通知中為 Macie 建立通知組態。通知組態會指定規則的準則。它也會指定交付管道和其他設定，以監控和傳送符合規則條件之 Amazon EventBridge 事件的相關通知。如需建立通知組態的詳細資訊，請參閱 AWS 使用者通知使用者指南中的 AWS 使用者通知入門。

若要建立 Macie 發現項目的通知組態，請為事件規則選擇下列選項：

- 對於「AWS 服務名稱」，請選擇「瑪西」。
- 針對「事件類型」，選擇「瑪西尋找」。
- 對於「區域」，請選取您使用 Macie 並希望收到發現項目通知的每AWS 區域個區域。

透過此設定，「使用者通知」會監控您的 EventBridge 事件，AWS 帳戶並針對所選區域中的所有 Macie 尋找事件產生通知。事件符合下列條件：

- `source`等於`aws.macie`
- `detail-type`等於`Macie Finding`

事件規則的基礎 JSON 模式為：

```
{
    "source": ["aws.macie"],
    "detail-type": ["Macie Finding"]
}
```

若要精簡規則並僅針對發現項目的子集產生通知，您可以自訂規則的 JSON 模式。若要這麼做，請指定衍生自 Macie 發現項目EventBridge 事件結構描述的其他準則。

如果您建立使用自訂 JSON 模式的規則，您可以為 Macie 發現項目建立多個通知組態。然後，您可以針對特定發現項目類型，為每個組態調整傳遞通道和其他設定，以配合安全性和合規性工作流程。

例如，您可以建立一個規則，在 Macie 產生或更新Policy:IAMUser/S3BucketPublic發現項目時通知您。在這種情況下，規則的模式可能是：

```
{
    "source": ["aws.macie"],
    "detail-type": ["Macie Finding"],
    "detail": {
        "type": ["Policy:IAMUser/S3BucketPublic"]
    }
}
```

您可以建立另一個規則，通知您是否 Macie 針對可公開存取的 S3 儲存貯體產生敏感資料尋找。在這種情況下，規則的模式可能是：

```
{
    "source": ["aws.macie"],
    "detail-type": ["Macie Finding"],
    "detail": {
        "type": [ { "prefix": "SensitiveData" } ],
        "resourcesAffected": {
            "effectivePermission": ["PUBLIC"]
        }
    }
}
```

如果您為 Macie 發現項目建立多個通知組態，最好確保每個組態的規則都是唯一的。否則，您可能會收到個別發現項目的重複通知。

若要進一步了解如何自訂規則的事件模式，請參閱 AWS 使用者通知使用者指南中的使用自訂 JSON 事件模式。

將 AWS 使用者通知欄位對應到 Amazon Macie 尋找欄位

當 AWS 使用者通知產生 Amazon Macie 發現項目的通知時，它會以相應 Amazon EventBridge 事件中欄位子集的資料填入通知。這些欄位提供關聯發現項目的主要詳細資訊，例如發現項目的類型和嚴重性，以及受影響資源的名稱。

如果您在 AWS 使用者通知主控台上檢閱通知，則通知會包含此欄位子集的所有資料。它也提供 Amazon Macie 主控台上相關發現項目的連結。如果您在其他傳送管道中檢閱通知，通知可能只包含部

分欄位的資料。這是因為「使用者通知」會調整其通知的設計和結構，以便與其支援的每種傳遞通道類型搭配使用。

下表列出可能包含在發現項目通知中的欄位。在表格中，「通知」欄位欄描述 (斜體) 或指示通知中欄位的名稱。「發現項目」事件欄位欄使用點標記法來指出尋找項目之 EventBridge 事件中對應 JSON 欄位的名稱。「描述」欄描述儲存在欄位中的資料。

通知欄位	尋找事件欄位	描述
訊息標題	`detail.type`	發現項目的類型。 例如：`Policy:IAMUser/S3BucketPublic` 或 `SensitiveData:S3Object/Financial` 。
摘要	`detail.title`	發現項目的簡短描述。 例如：`The S3 object contains financial information.`
Description (描述)	`detail.description`	發現項目的完整描述。 例如：`The S3 object contains financial information such as bank account numbers or credit card numbers.`
嚴重性	`detail.severity.description`	發現項目嚴重性的定性表示：`Low`、`Medium`、或`High`。
問題清單 ID	`detail.id`	發現項目的唯一識別碼。
已建立	`detail.createdAt`	Macie C存貯體的日期和時間。

通知欄位	尋找事件欄位	描述
Updated	`detail.updatedAt`	Macie C目前更新的日期和時間。 對於敏感資料發現項目，此值與「已建立」(`detail.createdAt`) 欄位的值相同。所有敏感數據發現都被視為新的（唯一）。
影響 S3 儲存貯體	`detail.resourcesAffected.s3Bucket.arn`	受影響 S3 儲存貯體的 Amazon Resource Name (ARN)。
受影響 S3 物件	`detail.resourcesAffected.s3Object.path`	受影響 S3 物件的名稱 (金鑰)，包括儲存物件的儲存貯體名稱，以及物件前置詞 (如果適用)。 此欄位不包含在原則發現項目的通知中。

通知欄位	尋找事件欄位	描述

敏感資料偵測	`detail.classificationDetails.result.sensitiveData.detections...`
	
	及/或
	
	`detail.classificationDetails.result.customDataIdentifiers.detections...`
		這是針對敏感資料尋找的事件中多個欄位的串連。此欄位不包含在原則發現項目的通知中。
		
		如果受管理資料識別碼偵測到敏感資料，則此欄位會指定偵測到的機密資料出現次數 (count) 的類別、類型和次數 ()。例如：`PERSONAL_INFORMATION: USA_SOCIAL_SECURITY_NUMBER 100 occurrences` 。
		
		如果自訂資料識別碼偵測到敏感資料，則此欄位會指定自訂資料識別碼的名稱以及偵測到的機密資料出現次數 (count)。例如：`Employee ID 20 occurrences` 。
		
		如果發現項目報告了多種類型的敏感資料，則通知會包含最多四種類型的資料。資料會先由任何適用的自訂資料識別碼填入，然後由任何適用的受管理資料識別碼填入。

變更 Amazon Macie 發現項目的 AWS 使用者通知設定

您可以隨時變更 Amazon Macie 發現項目的 AWS 使用者通知設定。若要這麼做，請在「使用者通知」中編輯通知設定。要了解如何操作，請參閱 AWS 使用者通知使用者指南中的管理通知組態。

如果您有多個 Macie 發現項目的通知組態，變更一個組態的設定並不會影響其他組態的設定。您可以編輯全部或僅編輯部分組態。

停用 Amazon Macie 發現項目的 AWS 使用者通知

若要停止產生和接收來自 AWS 使用者通知的 Amazon Macie 發現項目的通知，請刪除使用者通知中的通知組態。要了解如何操作，請參閱 AWS 使用者通知使用者指南中的管理通知組態。

如果您有多個 Macie 發現項目的通知設定，刪除一個組態並不會影響您的其他組態。您可以刪除全部或僅刪除部分組態。

Amazon Macie 發現的亞馬遜 EventBridge 事件模式

為了支援與其他應用程式、服務和系統 (例如監控或事件管理系統) 的整合，Amazon Macie 會自動將發現結果 EventBridge 作為事件發佈到 Amazon。 EventBridge舊稱為 Amazon E CloudWatch vents，是一種無伺服器事件匯流排服務，可將應用程式和其他應用程式的即時資料串流交付AWS 服務至 AWS Lambda功能、Amazon 簡單通知服務主題和 Amazon Kinesis 串流等目標。若要進一步了解 EventBridge，請參閱 Amazon EventBridge 使用者指南。

> **Note**
>
> 如果您目前使用 CloudWatch 事件，請注意 EventBridge 和 CloudWatch 事件是相同的基礎服務和 API。但是， EventBridge 包括其他功能，可讓您從軟體即服務 (SaaS) 應用程式和您自己的應用程式接收事件。由於基礎服務和 API 是相同的，因此 Macie 發現項目的事件結構描述也相同。

Macie 會自動發佈所有新發現項目的事件，以及現有原則發現項目的後續發現項目，但由抑制規則自動封存的發現項目除外。這些事件是符合事件 EventBridge 結構描述的 JSON 物AWS件。每個事件都包含特定發現項目的 JSON 表示。由於資料結構為 EventBridge 事件，因此您可以使用其他應用程式、服務和工具，更輕鬆地監視、處理和處理發現項目，並採取行動。如需有關 Macie 如何及何時發佈發現項目事件的詳細資訊，請參閱設定發現項目的發行設定。

主題

- 事件模式
- 原則發現項目的事件範例
- 敏感資料尋找的事件範例

事件模式

下列範例顯示 Amazon Macie 發現項目的亞馬遜 EventBridge 事件結構描述。如需尋找項目事件中可包含之欄位的詳細說明，請參閱 Amazon Macie API 參考中的發現項目。發現項目事件的結構和欄位會與 Amazon Macie API 的尋找物件緊密對應。

```
{
    "version": "0",
    "id": "event ID",
    "detail-type": "Macie Finding",
    "source": "aws.macie",
    "account": "AWS ## ID (string)",
    "time": "event timestamp (string)",
    "region": "AWS ## (string)",
    "resources": [
        <-- ARNs of the resources involved in the event -->
    ],
    "detail": {
        <-- Details of a policy or sensitive data finding -->
    },
    "policyDetails": null, <-- Additional details of a policy finding or null for a
 sensitive data finding -->
    "sample": Boolean,
    "archived": Boolean
}
```

原則發現項目的事件範例

下列範例使用範例資料來示範尋找政策的 Amazon EventBridge 事件中物件和欄位的結構和性質。

在此範例中，事件報告後續發生的現有政策發現：已停用 S3 儲存貯體的區塊公用存取設定。下列欄位和值可協助您判斷是否屬於這種情況：

- `type`欄位設定為`Policy:IAMUser/S3BlockPublicAccessDisabled`。
- `createdAt`和`updatedAt`欄位具有不同的值。這是事件報告後續發現現有策略發現項目的一個指標。如果事件報告了新的發現項目，這些欄位的值會相同。
- 此`count`欄位設定為`2`，表示這是發現項目的第二次出現。
- `category`欄位設定為`POLICY`。

- classificationDetails欄位的值為null，有助於區分原則尋找的此事件與敏感資料發現的事件。對於敏感資料發現項目，此值將是一組物件和欄位，可提供有關如何找到敏感資料的資訊和資訊。

另請注意，該sample字段的值是true。這個值強調這是文件中使用的範例事件。

```
{
    "version": "0",
    "id": "0948ba87-d3b8-c6d4-f2da-732a1example",
    "detail-type": "Macie Finding",
    "source": "aws.macie",
    "account": "123456789012",
    "time": "2021-04-30T23:12:15Z",
    "region":"us-east-1",
    "resources": [],
    "detail": {
        "schemaVersion": "1.0",
        "id": "64b917aa-3843-014c-91d8-937ffexample",
        "accountId": "123456789012",
        "partition": "aws",
        "region": "us-east-1",
        "type": "Policy:IAMUser/S3BlockPublicAccessDisabled",
        "title": "Block public access settings are disabled for the S3 bucket",
        "description": "All bucket-level block public access settings were disabled for
 the S3 bucket. Access to the bucket is controlled by account-level block public access
 settings, access control lists (ACLs), and the bucket's bucket policy.",
        "severity": {
            "score": 3,
            "description": "High"
        },
        "createdAt": "2021-04-29T15:46:02Z",
        "updatedAt": "2021-04-30T23:12:15Z",
        "count": 2,
        "resourcesAffected": {
            "s3Bucket": {
                "arn": "arn:aws:s3:::DOC-EXAMPLE-BUCKET1",
                "name": "DOC-EXAMPLE-BUCKET1",
                "createdAt": "2020-04-03T20:46:56.000Z",
                "owner":{
                    "displayName": "johndoe",
                    "id":
 "7009a8971cd538e11f6b6606438875e7c86c5b672f46db45460ddcd08example"
```

```
                },
                "tags": [
                    {
                        "key": "Division",
                        "value": "HR"
                    },
                    {
                        "key": "Team",
                        "value": "Recruiting"
                    }
                ],
                "defaultServerSideEncryption": {
                    "encryptionType": "aws:kms",
                    "kmsMasterKeyId": "arn:aws:kms:us-
east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab"
                },
                "publicAccess": {
                    "permissionConfiguration": {
                        "bucketLevelPermissions": {
                            "accessControlList": {
                                "allowsPublicReadAccess": false,
                                "allowsPublicWriteAccess": false
                            },
                            "bucketPolicy": {
                                "allowsPublicReadAccess": false,
                                "allowsPublicWriteAccess": false
                            },
                            "blockPublicAccess": {
                                "ignorePublicAcls": false,
                                "restrictPublicBuckets": false,
                                "blockPublicAcls": false,
                                "blockPublicPolicy": false
                            }
                        },
                        "accountLevelPermissions": {
                            "blockPublicAccess": {
                                "ignorePublicAcls": true,
                                "restrictPublicBuckets": true,
                                "blockPublicAcls": true,
                                "blockPublicPolicy": true
                            }
                        }
                    },
                    "effectivePermission": "NOT_PUBLIC"
```

```
                },
                "allowsUnencryptedObjectUploads": "FALSE"
            },
            "s3Object": null
        },
        "category": "POLICY",
        "classificationDetails": null,
        "policyDetails": {
            "action": {
                "actionType": "AWS_API_CALL",
                "apiCallDetails": {
                    "api": "PutBucketPublicAccessBlock",
                    "apiServiceName": "s3.amazonaws.com",
                    "firstSeen": "2021-04-29T15:46:02.401Z",
                    "lastSeen": "2021-04-30T23:12:15.401Z"
                }
            },
            "actor": {
                "userIdentity": {
                    "type": "AssumedRole",
                    "assumedRole": {
                        "principalId": "AROA1234567890EXAMPLE:AssumedRoleSessionName",
                        "arn": "arn:aws:sts::123456789012:assumed-role/RoleToBeAssumed/
MySessionName",
                        "accountId": "111122223333",
                        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
                        "sessionContext": {
                            "attributes": {
                                "mfaAuthenticated": false,
                                "creationDate": "2021-04-29T10:25:43.511Z"
                            },
                            "sessionIssuer": {
                                "type": "Role",
                                "principalId": "AROA1234567890EXAMPLE",
                                "arn": "arn:aws:iam::123456789012:role/
RoleToBeAssumed",
                                "accountId": "123456789012",
                                "userName": "RoleToBeAssumed"
                            }
                        }
                    },
                    "root": null,
                    "iamUser": null,
                    "federatedUser": null,
```

```
                    "awsAccount": null,
                    "awsService": null
                },
                "ipAddressDetails":{
                    "ipAddressV4": "192.0.2.0",
                    "ipOwner": {
                        "asn": "-1",
                        "asnOrg": "ExampleFindingASNOrg",
                        "isp": "ExampleFindingISP",
                        "org": "ExampleFindingORG"
                    },
                    "ipCountry": {
                        "code": "US",
                        "name": "United States"
                    },
                    "ipCity": {
                        "name": "Ashburn"
                    },
                    "ipGeoLocation": {
                        "lat": 39.0481,
                        "lon": -77.4728
                    }
                },
                "domainDetails": null
            }
        },
        "sample": true,
        "archived": false
    }
}
```

敏感資料尋找的事件範例

下列範例使用範例資料來示範針對敏感資料尋找的 Amazon EventBridge 事件中物件和欄位的結構和性質。

在此範例中，事件報告了新的敏感資料發現：Amazon Macie 在 S3 物件中發現了多個類別的敏感資料。下列欄位和值可以協助您判斷是這種情況：

- `type`欄位設定為`SensitiveData:S3Object/Multiple`。
- `createdAt`和`updatedAt`欄位具有相同的值。與原則發現項目不同，這一定是敏感資料發現項目的大小寫。所有敏感數據發現都被視為新的。

- count欄位設定為1，表示這是新發現項目。與原則發現項目不同，這一定是敏感資料發現項目的大小寫。所有敏感數據發現都被認為是唯一的（新的）。
- category欄位設定為CLASSIFICATION。
- policyDetails欄位的值為null，有助於區分發現敏感資料的此事件與原則尋找的事件。對於政策發現，此值將是一組物件和欄位，可提供有關潛在政策違規或 S3 儲存貯體安全性或隱私問題的資訊。

另請注意，該sample字段的值是true。這個值強調這是文件中使用的範例事件。

```
{
    "version": "0",
    "id": "14ddd0b1-7c90-b9e3-8a68-6a408example",
    "detail-type": "Macie Finding",
    "source": "aws.macie",
    "account": "123456789012",
    "time": "2022-04-20T08:19:10Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "schemaVersion": "1.0",
        "id": "4ed45d06-c9b9-4506-ab7f-18a57example",
        "accountId": "123456789012",
        "partition": "aws",
        "region": "us-east-1",
        "type": "SensitiveData:S3Object/Multiple",
        "title": "The S3 object contains multiple categories of sensitive data",
        "description": "The S3 object contains more than one category of sensitive
 data.",
        "severity": {
            "score": 3,
            "description": "High"
        },
        "createdAt": "2022-04-20T18:19:10Z",
        "updatedAt": "2022-04-20T18:19:10Z",
        "count": 1,
        "resourcesAffected": {
            "s3Bucket": {
                "arn": "arn:aws:s3:::DOC-EXAMPLE-BUCKET2",
                "name": "DOC-EXAMPLE-BUCKET2",
                "createdAt": "2020-05-15T20:46:56.000Z",
                "owner": {
```

```
                    "displayName": "johndoe",
                    "id":
 "7009a8971cd538e11f6b6606438875e7c86c5b672f46db45460ddcd08example"
                },
                "tags":[
                    {
                        "key":"Division",
                        "value":"HR"
                    },
                    {
                        "key":"Team",
                        "value":"Recruiting"
                    }
                ],
                "defaultServerSideEncryption": {
                    "encryptionType": "aws:kms",
                    "kmsMasterKeyId": "arn:aws:kms:us-
east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab"
                },
                "publicAccess": {
                    "permissionConfiguration": {
                        "bucketLevelPermissions": {
                            "accessControlList": {
                                "allowsPublicReadAccess": false,
                                "allowsPublicWriteAccess": false
                            },
                            "bucketPolicy":{
                                "allowsPublicReadAccess": false,
                                "allowsPublicWriteAccess": false
                            },
                            "blockPublicAccess": {
                                "ignorePublicAcls": true,
                                "restrictPublicBuckets": true,
                                "blockPublicAcls": true,
                                "blockPublicPolicy": true
                            }
                        },
                        "accountLevelPermissions": {
                            "blockPublicAccess": {
                                "ignorePublicAcls": false,
                                "restrictPublicBuckets": false,
                                "blockPublicAcls": false,
                                "blockPublicPolicy": false
                            }
```

```
                        }
                    },
                    "effectivePermission": "NOT_PUBLIC"
                },
                "allowsUnencryptedObjectUploads": "TRUE"
            },
            "s3Object":{
                "bucketArn": "arn:aws:s3:::DOC-EXAMPLE-BUCKET2",
                "key": "2022 Sourcing.csv",
                "path": "DOC-EXAMPLE-BUCKET2/2022 Sourcing.csv",
                "extension": "csv",
                "lastModified": "2022-04-19T22:08:25.000Z",
                "versionId": "",
                "serverSideEncryption": {
                    "encryptionType": "aws:kms",
                    "kmsMasterKeyId": "arn:aws:kms:us-
east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab"
                },
                "size": 4750,
                "storageClass": "STANDARD",
                "tags":[
                    {
                        "key":"Division",
                        "value":"HR"
                    },
                    {
                        "key":"Team",
                        "value":"Recruiting"
                    }
                ],
                "publicAccess": false,
                "etag": "6bb7fd4fa9d36d6b8fb8882caexample"
            }
        },
        "category": "CLASSIFICATION",
        "classificationDetails": {
            "jobArn": "arn:aws:macie2:us-east-1:123456789012:classification-
job/3ce05dbb7ec5505def334104bexample",
            "jobId": "3ce05dbb7ec5505def334104bexample",
            "result": {
                "status": {
                    "code": "COMPLETE",
                    "reason": null
                },
```

```
                "sizeClassified": 4750,
                "mimeType": "text/csv",
                "additionalOccurrences": true,
                "sensitiveData": [
                    {
                        "category": "PERSONAL_INFORMATION",
                        "totalCount": 65,
                        "detections": [
                            {
                                "type": "USA_SOCIAL_SECURITY_NUMBER",
                                "count": 30,
                                "occurrences": {
                                    "lineRanges": null,
                                    "offsetRanges": null,
                                    "pages": null,
                                    "records": null,
                                    "cells": [
                                        {
                                            "row": 2,
                                            "column": 1,
                                            "columnName": "SSN",
                                            "cellReference": null
                                        },
                                        {
                                            "row": 3,
                                            "column": 1,
                                            "columnName": "SSN",
                                            "cellReference": null
                                        },
                                        {
                                            "row": 4,
                                            "column": 1,
                                            "columnName": "SSN",
                                            "cellReference": null
                                        }
                                    ]
                                }
                            },
                            {
                                "type": "NAME",
                                "count": 35,
                                "occurrences": {
                                    "lineRanges": null,
                                    "offsetRanges": null,
```

```
                            "pages": null,
                            "records": null,
                            "cells": [
                                {
                                    "row": 2,
                                    "column": 3,
                                    "columnName": "Name",
                                    "cellReference": null
                                },
                                {
                                    "row": 3,
                                    "column": 3,
                                    "columnName": "Name",
                                    "cellReference": null
                                }
                            ]
                        }
                    }
                ]
            },
            {
                "category": "FINANCIAL_INFORMATION",
                "totalCount": 30,
                "detections": [
                    {
                        "type": "CREDIT_CARD_NUMBER",
                        "count": 30,
                        "occurrences": {
                            "lineRanges": null,
                            "offsetRanges": null,
                            "pages": null,
                            "records": null,
                            "cells": [
                                {
                                    "row": 2,
                                    "column": 14,
                                    "columnName": "CCN",
                                    "cellReference": null
                                },
                                {
                                    "row": 3,
                                    "column": 14,
                                    "columnName": "CCN",
                                    "cellReference": null
```

```
                                    }
                                ]
                            }
                        }
                    ]
                }
            ],
            "customDataIdentifiers": {
                "totalCount": 0,
                "detections": []
            }
        },
        "detailedResultsLocation": "s3://macie-data-discovery-results/
AWSLogs/123456789012/Macie/us-east-1/3ce05dbb7ec5505def334104bexample/
d48bf16d-0deb-3e49-9d8c-d407cexample.jsonl.gz",
        "originType": "SENSITIVE_DATA_DISCOVERY_JOB"
    },
    "policyDetails": null,
    "sample": true,
    "archived": false
  }
}
```

預測和監控 Amazon Macie 成本

為了協助您預測和監控使用 Amazon Macie 的成本，Macie 會計算並提供帳戶的預估使用費用。透過這些資料，您可以決定是否要調整服務的使用方式或帳戶配額。如果您目前正在參與 Macie 的 30 天免費試用，您可以使用此資料估算免費試用期結束後使用 Macie 的費用。您也可以檢查試用狀態。

您可以在 Amazon Macie 主控台上檢閱預估的使用成本，並使用 Amazon Macie API 以程式設計方式存取這些成本。如果您是組織的 Macie 管理員，則可以檢閱和存取組織的彙總資料，以及組織中帳戶的資料劃分。

除了 Macie 提供的預估使用成本之外，您還可以使用 AWS Billing and Cost Management來查看和監控您的實際成本。 AWS Billing and Cost Management 提供的功能可協助您追蹤和分析成本 AWS 服務，以及管理帳戶或組織的預算。它還提供了可幫助您根據歷史數據預測使用成本的功能。若要進一步了解 ，請參閱 AWS Billing 使用者指南。

主題

了解 Amazon Macie 的估計用量成本計算方式

Amazon Macie 定價是根據以下尺寸。

預防性控制監測

這些成本來自於維護 Amazon 簡單儲存服務 (Amazon S3) 一般用途儲存貯體的庫存，以及評估和監控儲存貯體的安全性和存取控制。如需詳細資訊，請參閱 Macie 如何監控 Amazon S3 數據安全。

我們會根據 Macie 為您的帳戶監控的 S3 一般用途儲存貯體總數向您收費。費用按每天按比例分配。

自動化敏感資料探索的物件監控

這些成本來自監控和評估 S3 儲存貯體庫存，藉由自動化敏感資料探索來識別符合分析資格的 S3 物件。如需詳細資訊，請參閱 自動化敏感資料探索如何運作。

我們會根據 Macie 為您的帳戶監控的一般用途儲存貯體中 S3 物件的總數向您收費。費用按每天按比例分配。

依敏感資料探索工作和自動化敏感資料探索進行物件分析

這些成本來自於分析 S3 物件和報告 Macie 在物件中找到的敏感資料。這包括透過敏感資料探索工作和自動化敏感資料探索進行的分析和報告。如需詳細資訊，請參閱 探索敏感資料。

我們會根據 Macie 在 S3 物件中分析的未壓縮資料量向您收費。Macie 因使用不受支援的 Amazon S3 儲存類別、使用不支援的檔案或儲存格式，或許可設定等原因而無法分析的物件無法收取任何費用。此外，這些費用不會根據您的工作產生的敏感資料發現數量或自動化敏感資料探索而有所不同。

若要管理自動化敏感資料探索的成本，您可以從分析中排除個別 S3 儲存貯體。例如，您可以排除已知符合組織安全性和合規性需求的值區。如果您的帳戶屬於集中管理多個 Macie 帳戶的組織，則另一個選項是選擇性地啟用或停用組織中個別帳戶的自動化敏感資料探索。如需詳細資訊，請參閱設定自動化敏感資料探索。

敏感資料探索工作的費用會受到帳戶每月敏感資料探索配額的限制。預設配額為 5 TB 的資料。) 如果工作正在執行，且符合資格物件的分析達到此配額，Macie 會自動暫停工作，直到下個日曆月份開始，並為您的帳戶重設每月配額，或者您增加帳戶的配額為止。

如果您是組織的 Macie 系統管理員，敏感資料探索工作的費用會受到您分析資料之每個帳戶的每月敏感資料探索配額所限制。成員帳戶的配額定義了您的工作和成員帳戶的工作可以在日曆月分析該帳戶的最大資料量。如果工作正在執行，且合格物件的分析達到成員帳戶的此配額，Macie 就會停止分析帳戶所擁有值區中的物件。當 Macie 完成分析所有其他未達配額的帳戶的物件時，Macie 會自動暫停工作。如果這是一次性工作，Macie 會在下一個日曆月開始時自動恢復工作，或增加所有受影響帳戶的配額，以先發生者為準。如果是定期工作，Macie 會在排定下一次執行開始或下一個行事曆月份開始 (以先發生者為準) 時自動繼續工作。如果排定的執行在下一個日曆月份開始之前開始，或是受影響帳戶的配額增加，Macie 就不會分析帳戶所擁有值區中的物件。

> **Tip**
>
> 如需有關管理或降低敏感資料探索成本的實用秘訣，請參閱AWS 安全部落格上的如何使用 Amazon Macie 降低探查敏感資料的成本部落格文章。

如需使用費用的詳細資訊和範例，請參閱 Amazon Macie 定價。

當您使用 Macie 檢視您的預估使用成本時，請務必瞭解成本估算的計算方式。考慮下列各項：

- 估計值以美元報告， AWS 區域 僅適用於當前。如果您在多個區域中使用 Macie，則不會針對您使用 Macie 的所有區域彙總資料。
- 在控制台上，估計包括當前日曆月份迄今為止。如果您使用 Amazon Macie API 以程式設計方式查詢資料，您可以選擇包含的時間範圍作為預估值。這可以是前 30 天或目前日曆月份的滾動時間範圍。
- 預估值並不反映可能適用於您帳戶的所有折扣。例外情況是從區域數量定價層級獲得的折扣，如 Amazon Macie 定價中所述。如果您的帳戶符合此類 discount 的資格，預估值會反映該 discount。
- 如果您是組織的 Macie 管理員，估算值不會反映組織的使用量合併折扣。如需這些折扣的詳細資訊，請參閱AWS Billing 使用者指南中的大量折扣。
- 對於預防性控制監控，估計是根據適用時間範圍內的平均每日成本。費用是按每天按比例分配的。
- 對於自動化敏感資料探索，整體估計是根據物件監控的平均每日成本 (按比例分配)，以及 Macie 目前在適用時間範圍內分析的未壓縮資料量。如果您是組織的 Macie 管理員，並且為成員帳戶啟用了自動敏感資料探索功能，則這些活動的預估費用會包含在每個適用成員帳戶的預估值中。
- 對於敏感性資料探索工作，估計是根據工作到目前為止在適用時間範圍內分析的未壓縮資料量。如果您是組織的 Macie 系統管理員，而且執行分析成員帳戶資料的工作，則這些工作的預估成本會包含在每個適用成員帳戶的估算中。
- 如果您的帳戶是組織中的成員帳戶，而您的 Macie 管理員會執行自動化敏感資料探索或執行敏感資料探索工作來分析您的資料，則這些活動的預估成本會包含在您帳戶的預估中。
- 估算值不包括您在某些 Macie 功能上使用其他 AWS 服務 功能所產生的費用。例如，使用客戶管理 AWS KMS keys 來解密您要檢查敏感資料的 S3 物件。

另請注意，Macie 提供每月免費方案，供敏感資料探索任務和自動化敏感資料探索分析 S3 物件。每個月最多可分析 1 GB 的資料，以探索和報告 S3 物件中的機密資料。如果在指定月份分析超過 1 GB 的資料，則在前 1 GB 資料之後，您的帳戶就會開始收取敏感資料探索費用。如果在指定月份分析的資料少於 1 GB，則剩餘的配置不會累計到下個月。如果您的帳戶屬於具有合併帳單的組織，則免費方案會套用至您組織分析的合併資料量。換句話說，每個月針對組織中的所有帳戶分析最多 1 GB 的資料無須付費。

查看 Amazon Macie 的估計使用成本

若要查看您目前預估的 Amazon Macie 使用成本，您可以使用 Amazon Macie 主控台或 Amazon Macie API。主控台和 API 都提供 Macie 定價維度的預估成本。如果您目前正在參與 30 天的免費試用期，您可以使用此資料估算免費試用期結束後使用 Macie 的費用。如需有關 Macie 定價維度和注意事項的資訊，請參閱瞭解估計使用成本的計算方式。如需使用費用的詳細資訊和範例，請參閱 Amazon Macie 定價。

在 Macie 中，估計的使用成本以美元報告，並且僅適用於當前 AWS 區域。如果您使用主控台檢閱資料，成本估算是目前的日曆月份 (包括在內)。如果您使用 Amazon Macie API 以程式設計方式查詢資料，您可以指定預估的包含時間範圍，包括前 30 天的滾動時間範圍或目前的日曆月份。

主題

在 Amazon Macie 主控台上查看估計的使用成本

在 Amazon Macie 主控台上，成本估算的組織方式如下：

- 預防性控制監控 — 這是維護 Amazon 簡單儲存服務 (Amazon S3) 一般用途儲存貯體庫存的預估成本，以及評估和監控儲存貯體的安全性和存取控制。
- 敏感資料探索工作 — 這是您執行之敏感資料探索工作的估計成本。
- 自動化敏感資料探索 — 這是執行自動化敏感資料探索的估計成本。這包括監控和評估您的 S3 儲存貯體庫存，以識別符合分析資格的 S3 物件。它還包括分析符合條件的對象，並報告敏感數據統計信息，發現項目和其他類型的結果。若要檢視這些預估值，您的帳戶必須是組織的 Macie 管理員帳戶或獨立的 Macie 帳戶。

請依照下列步驟，使用 Amazon Macie 主控台檢閱估計的使用成本。

在主機上查看預估的使用成本

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 使用頁面右上角的選取 AWS 區域 器，選取您要檢視預估費用的區域。
3. 在導覽窗格中，選擇用量。

如果您擁有獨立的 Macie 帳戶，或者您的帳戶是組織中的成員帳戶，則「使用情況」頁面會顯示您帳戶的預估使用費用明細。

如果您是組織的 Macie 管理員，「使用情況」頁面會列出組織中的帳戶。在資料表中：

- 服務配額 — 作業 — 這是目前每月執行敏感資料探索任務以分析帳戶所擁有儲存貯體中 S3 物件的每月配額。

- 免費試用 — 這些欄位指出帳戶目前是否參與免費試用，以進行預防性控制監視或自動化敏感資料探索。如果帳戶的適用免費試用已結束，則免費試用欄位為空白。
- 總計 — 這是一個帳戶的總估計成本。

「預估成本」區段會顯示組織的預估總成本，以及這些成本的明細。若要檢閱組織中特定帳戶的預估成本明細，請在表格中選擇帳戶。然後，「預估成本」區段會顯示此明細。若要顯示其他帳戶的此資料，請在表格中選擇帳戶。若要清除帳戶選項，請選擇帳戶 ID 旁邊的 X。

使用 Amazon Macie API 查詢估計的用量成本

若要以程式設計方式查詢估計的使用成本，您可以使用 Amazon Macie API 的下列操作：

- GetUsageTotals— 此作業會傳回帳戶的總估計使用費用，並依使用量度分組。如果您是組織的 Macie 管理員，此作業會傳回組織中所有帳戶的彙總成本估算值。若要進一步了解此操作，請參閱 Amazon Macie API 參考中的使用量總計。
- GetUsageStatistics— 此作業會傳回帳戶的使用狀況統計資料和相關資料，依帳戶分組，然後依使用量度分組。資料包含總估計使用費用和目前帳戶配額。如果適用，它還指示您的 30 天免費試用開始於 Macie 和自動化敏感數據發現的時間。如果您是組織的 Macie 管理員，此作業會傳回組織中所有帳戶的資料明細。您可以透過排序和篩選查詢結果來自訂查詢。若要進一步了解此操作，請參閱 Amazon Macie API 參考中的使用量統計資料。

當您使用任一作業時，您可以選擇性地指定資料的包含時間範圍。此時間範圍可以是前 30 天的累計時間範圍 (PAST_30_DAYS)，也可以是目前日曆月份的累計時間範圍 (MONTH_TO_DATE)。如果您未指定時間範圍，Macie 會傳回前 30 天的資料。

下列範例說明如何使用 () 查詢估計的使用成本和統計資AWS Command Line InterfaceAWS CLI料。您也可以使用目前版本的其他 AWS 命令列工具或 AWS SDK，或直接將 HTTPS 要求傳送至 Macie 來查詢資料。如需 AWS 工具和 SDK 的相關資訊，請參閱要建置的工具。 AWS

範例

- 範例 1：查詢預估使用量總成本
- 範例 2：查詢使用量統計資料

範例 1：查詢預估使用量總成本

若要使用查詢預估使用成本總計 AWS CLI，請執行get-usage-totals命令並選擇性地指定資料的時間範圍。例如：

```
C:\> aws macie2 get-usage-totals --time-range MONTH_TO_DATE
```

其中將目前的行事曆月份*MONTH_TO_DATE*指定為資料的時間範圍。

如果此命令成功執行，您會收到類似如下的輸出。

```
{
    "timeRange": "MONTH_TO_DATE",
    "usageTotals": [
        {
            "currency": "USD",
            "estimatedCost": "153.45",
            "type": "SENSITIVE_DATA_DISCOVERY"
        },
        {
            "currency": "USD",
            "estimatedCost": "65.18",
            "type": "AUTOMATED_SENSITIVE_DATA_DISCOVERY"
        },
        {
            "currency": "USD",
            "estimatedCost": "1.51",
            "type": "DATA_INVENTORY_EVALUATION"
        },
        {
            "currency": "USD",
            "estimatedCost": "0.98",
            "type": "AUTOMATED_OBJECT_MONITORING"
        }
    ]
}
```

其中`estimatedCost`是相關使用狀況測量結果的預估使用量成本總計 (`type`)：

- `SENSITIVE_DATA_DISCOVERY`，用於分析具有敏感資料探索任務的 S3 物件。
- `AUTOMATED_SENSITIVE_DATA_DISCOVERY`，用於透過自動化敏感資料探索分析 S3 物件。
- `DATA_INVENTORY_EVALUATION`，用於監控和評估 S3 一般用途儲存貯體，以實現安全性和存取控制。
- `AUTOMATED_OBJECT_MONITORING`，用於評估和監控 S3 儲存貯體庫存，藉由自動化敏感資料探索來識別符合分析資格的 S3 物件。

範例 2：查詢使用量統計資料

若要使用查詢使用統計資料 AWS CLI，請執行get-usage-statistics命令。您可以選擇性地排序、篩選及指定查詢結果的時間範圍。下列範例會擷取過去 30 天之 Macie 管理員帳戶的使用統計資料。結果會依 AWS 帳戶 ID 以遞增順序排序。

對於 Linux、macOS 或 Unix，請使用反斜線 (\) 行接續字元來提高可讀性：

```
$ aws macie2 get-usage-statistics \
--sort-by '{"key":"accountId","orderBy":"ASC"}' \
--time-range PAST_30_DAYS
```

對於 Microsoft Windows，使用脫字符號 (^) 行繼續字符來提高可讀性：

```
C:\> aws macie2 get-usage-statistics ^
--sort-by={\"key\":\"accountId\",\"orderBy\":\"ASC\"} ^
--time-range PAST_30_DAYS
```

其中：

- *accountId* 指定要用來排序結果的欄位。
- *ASC* 是根據指定欄位 (*accountId*) 的值，套用至結果的排序順序。
- *PAST_30_DAYS*將前 30 天指定為資料的時間範圍。

如果命令運行成功，Macie 返回一個records數組。陣列會針對查詢結果中包含的每個帳戶包含一個物件。例如：

```
{
    "records": [
        {
            "accountId": "111122223333",
            "automatedDiscoveryFreeTrialStartDate": "2024-01-28T16:00:00+00:00",
            "freeTrialStartDate": "2020-05-20T12:26:36.917000+00:00",
            "usage": [
                {
                    "currency": "USD",
                    "estimatedCost": "1.51",
                    "type": "DATA_INVENTORY_EVALUATION"
                },
                {
```

```
                    "currency": "USD",
                    "estimatedCost": "65.18",
                    "type": "AUTOMATED_SENSITIVE_DATA_DISCOVERY"
                },
                {
                    "currency": "USD",
                    "estimatedCost": "153.45",
                    "serviceLimit": {
                        "isServiceLimited": false,
                        "unit": "TERABYTES",
                        "value": 50
                    },
                    "type": "SENSITIVE_DATA_DISCOVERY"
                },
                {
                    "currency": "USD",
                    "estimatedCost": "0.98",
                    "type": "AUTOMATED_OBJECT_MONITORING"
                }
            ]
        },
        {
            "accountId": "444455556666",
            "automatedDiscoveryFreeTrialStartDate": "2024-01-28T16:00:00+00:00",
            "freeTrialStartDate": "2020-05-18T16:26:36.917000+00:00",
            "usage": [
                {
                    "currency": "USD",
                    "estimatedCost": "1.58",
                    "type": "DATA_INVENTORY_EVALUATION"
                },
                {
                    "currency": "USD",
                    "estimatedCost": "63.13",
                    "type": "AUTOMATED_SENSITIVE_DATA_DISCOVERY"
                },
                {
                    "currency": "USD",
                    "estimatedCost": "145.12",
                    "serviceLimit": {
                        "isServiceLimited": false,
                        "unit": "TERABYTES",
                        "value": 50
                    },
```

```
                    "type": "SENSITIVE_DATA_DISCOVERY"
                },
                {
                    "currency": "USD",
                    "estimatedCost": "1.02",
                    "type": "AUTOMATED_OBJECT_MONITORING"
                }
            ]
        }
    ],
    "timeRange": "PAST_30_DAYS"
}
```

其中`estimatedCost`是帳戶關聯使用量度 (`type`) 的估計使用量成本總計：

- `DATA_INVENTORY_EVALUATION`，用於監控和評估 S3 一般用途儲存貯體，以實現安全性和存取控制。
- `AUTOMATED_SENSITIVE_DATA_DISCOVERY`，用於透過自動化敏感資料探索分析 S3 物件。
- `SENSITIVE_DATA_DISCOVERY`，用於分析具有敏感資料探索任務的 S3 物件。
- `AUTOMATED_OBJECT_MONITORING`，用於評估和監控帳戶的 S3 儲存貯體庫存，藉由自動化敏感資料探索來識別符合分析資格的 S3 物件。

參加亞 Amazon Macie 免費試用

當您第一次啟用 Amazon Macie 時，您的 Macie AWS 帳戶 會自動註冊 30 天的免費試用版。這包括 AWS Organizations 組織中的個別成員帳戶。

在免費試用期間，在 AWS 區域 以下情況下使用 Macie 不會收取任何費用：

- 執行預防性控制監控 — 這包括產生和維護區域中 Amazon Simple Storage Service (Amazon S3) 一般用途儲存貯體的庫存。它還包括評估和監視存儲桶的安全性和訪問控制。

  如需詳細資訊，請參閱 Macie 如何監控 Amazon S3 數據安全。
- 執行自動化敏感資料探索 — 這包括監控和評估區域中的 S3 儲存貯體庫存，以識別符合分析資格的 S3 物件。它還包括分析符合條件的對象，並報告敏感數據統計信息，發現項目和其他類型的結果。若要設定和管理此功能，您的帳戶必須是組織的 Macie 管理員帳戶或獨立的 Macie 帳戶。如果您是組織的 Macie 管理員，則可以使用此功能來分析成員帳戶所擁有的 S3 儲存貯體中的物件。

  如需詳細資訊，請參閱 自動化敏感資料探索如何運作。

如需目前可使用 Macie 的區域清單，請參閱. AWS 一般參考

免費試用版連續運行 30 天。您無法在啟動後暫停它。免費試用期結束後，執行預防性控制監控的費用將開始累積。執行自動化敏感資料探索的費用也會開始累積。如果您是某個組織的 Macie 管理員，則會根據您組織中的每個帳戶計費。您可以使用 Macie 來檢閱組織中個別帳戶的預估使用費用明細。

> **備註**
>
> 在免費試用期間，您可能會對搭配特定 Macie 功能使用的其他 AWS 服務 功能產生費用，例如，使用 customer Managed AWS KMS keys 解密您要檢查敏感資料的 S3 物件。
> 免費試用不包括敏感資料探索任務對 S3 物件進行分析。如果您建立並執行在免費試用期間分析超過 1 GB 未壓縮資料的敏感資料探索工作，則需要支付費用。Macie 每月提供敏感資料探索的免費方案。 每個月免費分析 S3 物件中最多 1 GB 的未壓縮資料。 在前 1 GB 的資料之後，會產生成本。)

在免費試用期間，您可以查看試用狀態，並查看帳戶的預估使用費用。費用估算是根據您在免費試用期間到目前為止對 Macie 的使用情況進行估算。他們可以幫助您了解試用期結束後的某些使用費用可能是多少。如需有關 Macie 如何計算這些值的詳細資訊，請參閱瞭解估計使用成本的計算方式。

在免費試用期間查看您的狀態和估計費用

請按照以下步驟使用 Amazon Macie 主控台檢查試用狀態並查看估計的使用費用。您也可以使用 Amazon Macie API 的GetUsageStatistics操作，以程式設計方式存取這些資料。

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 使用頁面右上角的選 AWS 區域 擇器，選取您要檢查免費試用狀態和預估使用費用的地區。
3. 在導覽窗格中，選擇用量。

「使用量」頁面會指出免費試用的剩餘天數。它還顯示您的估計使用費用以美元為單位的明細：

- 預防性控制監控 — 這是維護 S3 一般用途儲存貯體的庫存，以及在免費試用期結束後評估和監控儲存貯體的安全性和存取控制的總預計成本。
- 敏感資料探索工作 — 這是您執行的任何敏感資料探索工作的預估總成本。免費試用不包含敏感資料探索工作。

- 自動化敏感資料探索 — 這些是免費試用期結束後執行自動化敏感資料探索的預計成本，依定價維度 (物件監控和物件分析) 細分。若要檢視這些預估值，您的帳戶必須是組織的 Macie 管理員帳戶或獨立的 Macie 帳戶。

如果您是組織的 Macie 管理員，「使用情況」頁面會提供組織中 Macie 帳戶的詳細資料。在資料表中：

- 服務配額 — 作業 — 這是目前每月執行敏感資料探索任務以分析帳戶所擁有儲存貯體中 S3 物件的每月配額。
- 免費試用 — 這些欄位指出帳戶目前是否參與免費試用，以進行預防性控制監視或自動化敏感資料探索。如果帳戶的適用免費試用已結束，則免費試用欄位為空白。
- 總計 — 這是一個帳戶的總估計成本。

「預估成本」區段會顯示組織整體的預估成本。若要檢閱組織中特定帳戶的預估成本明細，請在表格中選擇帳戶。然後，「預估成本」區段會顯示此明細。若要顯示其他帳戶的此資料，請在表格中選擇帳戶。若要清除帳戶選項，請選擇帳戶 ID 旁邊的 X。

> **備註**
>
> 如果帳戶在 Amazon S3 中存放超過 150 TB 的資料，該帳戶用於自動化敏感資料探索的估計和實際成本可能會高於 Macie 在 30 天免費試用期間提供的成本預測。這是因為已註冊免費試用的帳戶分析了 150 GB 的未壓縮資料時，會暫停透過自動化敏感資料探索進行的物件分析。免費試用期結束後，系統會繼續對帳戶進行物件分析。如需協助預測在 Amazon S3 中存放 150 TB 以上資料的帳戶的成本，請聯絡 AWS Support。
>
> 若要在免費試用期結束後管理自動化敏感資料探索的成本，您可以將個別 S3 儲存貯體排除在後續分析之外。如果您是組織的 Macie 系統管理員，則另一個選項是選擇性地啟用或停用組織中個別帳戶的自動化敏感資料探索功能。如需這些選項的資訊，請參閱 設定自動化敏感資料探索。

管理多個 Amazon Macie 帳戶

如果您的AWS環境有多個帳戶，您可以在環境中建立 Amazon Macie 帳戶的關聯，並在 Macie 中以組織的形式集中管理這些帳戶。透過此組態，指定的 Macie 管理員可以評估和監控組織 Amazon Simple Storage Service (Amazon S3) 資料資產的整體安全狀態，並探索組織 S3 儲存貯體中的敏感資料。管理員還可以大規模執行各種帳戶管理和管理任務，例如監控估計的使用成本和評估帳戶配額。

在 Macie 中，組織由指定的 Macie 管理員帳戶和一或多個關聯的成員帳戶組成。您可以通過兩種方式關聯帳戶，通過集成 Macie AWS Organizations 或通過在 Macie 發送和接受會員邀請。我們建議您與 AWS Organizations Macie 整合。

AWS Organizations是一項全球帳戶管理服務，可讓管理AWS員整合並集中管理多個帳戶AWS 帳戶。它提供帳戶管理和合併帳單功能，可支援預算、安全及合規需求。它不收取額外費用AWS 服務，並且與包括 Macie 和 Amazon GuardDuty 在內的多個集成。AWS Security Hub若要進一步了解 ，請參閱 AWS Organizations 使用者指南。

如果您希望在不使用的情況下集中管理多個 Macie 帳戶AWS Organizations，則可以改用會員邀請。如果您傳送邀請且其他帳戶接受邀請，您的帳戶會成為另一個帳戶的 Macie 管理員帳戶。如果您收到並接受邀請，您的帳戶將成為 Macie 成員帳戶，而 Macie 管理員帳戶可以存取和管理您 Macie 帳戶的特定設定、資料和資源。

主題

- 了解 Amazon Macie 管理員和會員帳戶之間的關係
- 管理亞馬遜 Macie 帳戶 AWS Organizations
- 通過邀請管理 Amazon Macie 帳戶

了解 Amazon Macie 管理員和會員帳戶之間的關係

如果您以組織形式集中管理多個 Amazon Macie 帳戶，Macie 管理員可以存取 Amazon Simple Storage Service (Amazon S3) 庫存資料、政策發現項目，以及關聯成員帳戶的特定 Macie 設定和資源。管理員還可以啟用自動化敏感資料探索，並執行敏感資料探索任務，以偵測成員帳戶所擁有的 S3 儲存貯體中的敏感資料。對特定工作的 Support 會因 Macie 管理員帳戶是透過 AWS Organizations 還是邀請與成員帳戶建立關聯而有所不同。

下表提供有關 Macie 管理員和成員帳戶之間關係的詳細資訊。它指示了每種類型的帳戶的默認權限。若要進一步限制對 Macie 功能和作業的存取，您可以使用自訂 AWS Identity and Access Management (IAM) 政策。

在資料表中：

- S@@ elf 表示帳戶無法針對任何關聯的帳戶執行工作。
- 「任何」表示帳戶可針對個別關聯帳戶執行工作。
- 「全部」表示帳戶可以執行工作，且工作適用於所有相關聯的帳戶。

破折號 (—) 表示帳戶無法執行工作。

任務	通過 AWS Organizations		通過邀請	
	管理員	成員	管理員	成員
啟用馬西	任何	–	自我	自我
複查組織的科目存貨 [1]	全部	–	全部	–
新增會員帳戶	任何	–	任何	–
檢閱 S3 儲存貯體的統計資料和中繼	全部	自我	全部	自我
檢討政策發現	全部	自我	全部	自我
隱藏 (封存) 原則發現項目 [2]	全部	–	全部	–
公佈原則發現項目 [3]	自我	自我	自我	自我
設定敏感資料探索結果的存放庫 [4]	自我	自我	自我	自我
建立並使用允許清單	自我	自我	自我	自我

建立和使用自訂資料識別碼	自我	自我	自我	自我
設定自動化敏感資料探索設定	全部	–	全部	–
啟用或停用自動化敏感資料探索	任何	–	任何	–
檢閱自動化敏感資料探索統計資料、資料和結果	全部	–	全部	–
建立並執行敏感性資料探索工作 [5]	任何	自我	任何	自我
檢閱敏感資料探索工作的詳細資料 [6]	自我	自我	自我	自我
檢閱敏感資料發現項目 [7]	自我	自我	自我	自我
隱藏 (封存) 敏感資料發現項目 [7]	自我	自我	自我	自我
發佈敏感資料發現項目 [7]	自我	自我	自我	自我
設定 Macie 以擷取發現項目的敏感資料範例	自我	自我	自我	自我
擷取發現項目的敏感資料範例 [8]	自我	自我	自我	自我
設定發現項目的地的發佈	自我	自我	自我	自我

設定發現項目的發佈頻率	全部	自我	全部	自我
建立範例發現項	自我	自我	自我	自我
檢閱帳戶配額和預估使用成本	全部	自我	全部	自我
暫停馬西 9	任何	–	任何	自我
禁用馬西埃 10	自我	自我	自我	自我
移除 (取消關聯) 成員帳戶	任何	–	任何	–
取消與管理員帳戶的關聯	–	–	–	自我
刪除與其他帳號的關聯 [11]	任何	–	任何	自我

1. 中組織的管理員 AWS Organizations 可以檢閱組織中的所有帳戶，包括尚未啟用 Macie 的帳戶。以邀請為基礎的組織的管理員只能檢閱他們新增至其詳細目錄的帳號。
2. 只有管理員可以隱藏發現的策略。如果管理員建立了抑制規則，Macie 會將規則套用至組織中所有帳號的策略發現項目，除非規則設定為排除特定帳號。如果成員建立了抑制規則，Macie 不會將該規則套用至該成員帳戶的策略發現項目。
3. 只有擁有受影響資源的帳號才能將資源的策略發現項目發佈到 AWS Security Hub。管理員和成員帳戶都會自動將受影響資源的政策發現項目發佈到 Amazon EventBridge。
4. 如果管理員啟用自動化敏感資料探索，或設定工作以分析成員帳戶所擁有的 S3 儲存貯體中的物件，Macie 會將敏感資料探索結果儲存在管理員帳戶的儲存庫中。
5. 成員可以將任務設定為僅在其帳戶擁有的 S3 儲存貯體中分析物件。管理員可以設定工作，以分析其帳戶所擁有的值區或成員帳戶擁有的物件。有關如何套用配額和計算多帳戶作業成本的資訊，請參閱瞭解估計使用成本的計算方式。

6. 只有建立工作的帳戶才能存取工作的詳細資料。這包括 S3 儲存貯體庫存中的工作相關詳細資訊。

7. 只有建立工作的帳戶可以存取、隱藏或發佈工作產生的機密資料發現項目。只有管理員可以存取、隱藏或發佈自動化敏感資料探索產生的機密資料發現項目。

8. 如果敏感資料發現適用於成員帳戶擁有的 S3 物件，則管理員可能可以擷取發現項目所報告之敏感資料的範例。這取決於發現項目的來源，以及管理員帳戶和成員帳戶中的組態設定和資源。如需詳細資訊，請參閱擷取機密資料範例的組態選項和需求。

9. 管理員若要為自己的帳戶暫停 Macie，管理員必須先取消其帳戶與所有成員帳戶的關聯。

10. 若要讓管理員為自己的帳戶停用 Macie，管理員必須先取消其帳戶與所有成員帳戶的關聯，並刪除其帳戶與所有帳戶之間的關聯。中組織的管理員 AWS Organizations 可以透過使用組織的管理帳戶將不同的帳戶指定為管理員帳戶來執行此操作。

    若要讓 AWS Organizations 組織成員停用 Macie，管理員必須先取消成員帳戶與其管理員帳戶的關聯。在以邀請為基礎的組織中，成員可以取消其帳戶與其管理員帳戶的關聯，然後停用 Macie。

11. 中組織的管理員 AWS Organizations 可以在取消帳戶與其管理員帳戶的關聯後刪除與成員帳戶的關聯。帳號會繼續顯示在管理員的帳號詳細目錄中，但其狀態表示該帳號不是成員帳戶。在以邀請為基礎的組織中，管理員和成員可以在取消其帳戶與其他帳戶的關聯後刪除與其他帳戶的關聯。然後，另一個帳戶就會停止出現在其帳戶清單中。

管理亞馬遜 Macie 帳戶 AWS Organizations

如果您使AWS Organizations用集中管理多個項目AWS 帳戶，您可以將 Amazon Macie 與整合AWS Organizations，然後針對組織中的帳戶集中管理 Macie。透過此設定，指定的 Macie 管理員可以啟用和管理多達 10,000 個帳戶的 Macie。管理員還可以存取 Amazon 簡單儲存服務 (Amazon S3) 庫存資料，並在帳戶擁有的 S3 儲存貯體中探索敏感資料。如需有關管理員可執行之工作的詳細資訊，請參閱了解 Amazon Macie 管理員和會員帳戶之間的關係。

若要將 Macie 與整合AWS Organizations，請先將帳戶指定為組織的委派 Macie 管理員帳戶。然後，Macie 管理員會為組織中的其他帳戶啟用 Macie，將這些帳戶新增為 Macie 成員帳戶，並為這些帳戶設定 Macie 設定和資源。

> **Tip**
>
> 如果您已使用邀請將 Macie 管理員帳戶與成員帳戶相關聯，您可以在中指定該帳戶作為組織的委派 Macie 管理員帳戶。AWS Organizations如果您這樣做，所有目前關聯的成員帳戶都會保留成員，您可以使用來充分利用管理帳戶的好處AWS Organizations。如需詳細資訊，請參閱從以邀請為基礎的組織轉換。

本節中的主題說明如何與 Macie 整合，以AWS Organizations及如何管理和管理組織中帳戶的 Macie。

主題

- 搭配使用 Amazon Macie 的注意事項和建議 AWS Organizations
- 在 Amazon Macie 中整合和設定組織
- 查看一個組織的 Amazon Macie 帳戶
- 管理一個組織的 Amazon Macie 成員帳戶
- 為組織指定不同的 Amazon Macie 管理員帳戶
- 禁用 Amazon Macie 集成 AWS Organizations

搭配使用 Amazon Macie 的注意事項和建議 AWS Organizations

在與 Amazon Macie 整合 AWS Organizations 並在 Macie 中設定組織之前，請考慮下列需求和建議。還要確保您了解 Macie 管理員和成員帳戶之間的關係。

主題

- 指定 Macie 管理員帳戶
- 變更或移除 Macie 管理員帳戶的指定
- 添加和刪除馬西成員帳戶
- 從以邀請為基礎的組織轉換

指定 Macie 管理員帳戶

當您決定哪個帳戶應該是組織委派的 Macie 管理員帳戶時，請記住下列事項：

- 一個組織只能有一個委派的 Macie 管理員帳戶。

- 一個帳戶不能同時是 Macie 管理員和會員帳戶。
- 只有組織的 AWS Organizations 管理帳戶可以指定組織的委派 Macie 管理員帳戶。只有管理帳戶可以隨後變更或移除該指定。
- 組織的 AWS Organizations 管理帳戶也可以是組織的委派 Macie 管理員帳戶。但是，我們不建議根據 AWS 安全性最佳實務和最低權限原則進行此配置。出於計費目的而可以訪問管理帳戶的用戶可能與出於信息安全目的而需要訪問 Macie 的用戶不同。

  如果您偏好此設定，您必須在至少一個中為組織的管理帳戶啟用 Macie， AWS 區域 然後才能將帳戶指定為委派的 Macie 管理員帳戶。否則，該帳戶將無法訪問和管理會員帳戶的 Macie 設置和資源。
- 不同的是 AWS Organizations，馬西是一個區域服務。這意味著 Macie 管理員帳戶的指定是區域指定。這也意味著 Macie 管理員和成員帳戶之間的關聯是區域。例如，如果管理帳戶在美國東部 (維吉尼亞北部) 區域指定了 Macie 管理員帳戶，則 Macie 管理員只能管理該區域中的成員帳戶的 Macie。

  若要集中管理多個 Macie 帳戶 AWS 區域，管理帳戶必須登入組織目前使用的每個區域，或將使用 Macie，然後在每個區域中指定 Macie 管理員帳戶。然後，Macie 管理員可以在這些區域中配置組織。如需目前可使用 Macie 的區域清單，請參閱. AWS 一般參考
- 一個帳戶一次只能與一個 Macie 管理員帳戶關聯。如果您的組織在多個區域中使用 Macie，則所有這些區域中指定的 Macie 管理員帳戶必須相同。但是，您組織的管理帳戶必須在每個區域中分別指定管理員帳戶。
- 一個帳戶一次只能是一個組織的委派 Macie 管理員帳戶。如果您在中管理多個組織 AWS Organizations，則必須為每個組織指定不同的 Macie 管理員帳戶。這是由於需 AWS Organizations 求 — 一個帳戶一次只能是一個組織的成員。

如果 Macie 管理員 AWS 帳戶 被暫停、隔離或關閉，所有關聯的 Macie 成員帳戶都會自動移除為 Macie 成員帳戶，但 Macie 會繼續為這些帳戶啟用。如果為一或多個成員帳戶啟用了自動敏感資料探索功能，該帳戶就會停用該功能。這也會停用對 Macie 產生並直接提供的統計資料、庫存資料和其他資訊的存取，同時為帳戶執行自動化探索。若要還原對此資料的存取權，必須在 30 天內發生下列情況：

1. Macie 管理員 AWS 帳戶 已恢復。
2. AWS Organizations 管理帳戶會再次將該帳戶指定為 Macie 管理員帳戶。
3. Macie 管理員會設定組織，並再次針對適當的帳戶啟用自動探索。

在 30 天後，Macie 會永久刪除先前產生並直接提供的資料，同時針對適用的帳戶執行自動探索。

變更或移除 Macie 管理員帳戶的指定

只有組織的 AWS Organizations 管理帳戶可以變更或移除組織委派 Macie 管理員帳戶的指定。

如果管理帳戶變更或移除指定：

- 所有關聯的成員帳戶將被刪除為 Macie 成員帳戶，但 Macie 繼續為帳戶啟用。這些帳戶成為獨立的 Macie 帳戶。要暫停或停止使用 Macie，會員帳戶的用戶必須暫停（暫停）或禁用（停止）該帳戶的 Macie。
- 每個啟用該功能的帳戶都會停用自動化敏感資料探索。這也會停用對 Macie 產生並直接提供的統計資料、庫存資料和其他資訊的存取，同時為每個帳戶執行自動化探索。若要還原此資料的存取權，管理帳戶必須在 30 天內再次指定相同的 Macie 管理員帳戶。此外，Macie 管理員必須再次設定組織，並在 30 天內為每個帳戶重新啟用自動探索功能。30 天后，數據會過期，Macie 將其永久刪除。

添加和刪除馬西成員帳戶

當您新增、移除或管理組織的成員帳戶時，請記住下列事項：

- 一個 Macie 管理員帳戶可以與每個帳戶不超過 10,000 個活躍（已啟用）Macie 成員帳戶相關聯。AWS 區域如果您的組織超過此配額，Macie 管理員將無法新增成員帳戶，直到他們移除區域中必要的現有成員帳戶數量為止。當組織達到此配額時，我們會透過為其帳戶建立 AWS Health 和 Amazon CloudWatch 事件來通知 Macie 管理員。我們也會傳送電子郵件至與他們帳戶相關聯的電子郵件地址。

  如果您是組織的 Macie 管理員，則可以使用 Amazon Macie 主控台上的「帳戶」頁面或 Amazon Macie API 的操作，判斷目前與您的帳戶相關聯的ListMembers作用中成員帳戶數目。如需詳細資訊，請參閱 查看一個組織的 Amazon Macie 帳戶。
- 一個帳戶一次只能與一個 Macie 管理員帳戶關聯。這表示如果某個帳戶已與中組織的 Macie 管理員帳戶相關聯，則該帳戶無法接受來自其他帳戶的 Macie 邀請。 AWS Organizations

  同樣地，如果帳戶已接受邀請，則中組織的 Macie 管理員 AWS Organizations 無法將該帳戶新增為 Macie 成員帳戶。該帳戶必須先取消與其目前、以邀請為基礎的管理員帳戶的關聯。
- 若要將 AWS Organizations 管理帳戶新增為 Macie 成員帳戶，管理帳戶的使用者必須先啟用該帳戶的 Macie。不允許 Macie 管理員為管理帳戶啟用 Macie。
- 如果 Macie 管理員移除了 Macie 成員帳戶：
  - 馬西繼續為該帳戶啟用。該帳戶將成為一個獨立的 Macie 帳戶。要暫停或停止使用 Macie，該帳戶的用戶必須暫停（暫停）或禁用（停止）該帳戶的 Macie。

- 帳戶的自動敏感資料探索功能會停用 (如果已啟用)。這也會停用對 Macie 產生並直接提供的統計資料、庫存資料和其他資訊的存取，同時為帳戶執行自動化探索。
- 成員帳戶無法取消與其 Macie 管理員帳戶的關聯。只有 Macie 管理員可以刪除作為 Macie 成員帳戶的帳戶。

從以邀請為基礎的組織轉換

如果您已使用 Macie 成員資格邀請，將 Macie 管理員帳戶與成員帳戶相關聯，我們建議您將該帳戶指定為中組織的委派 Macie 管理員帳戶。 AWS Organizations這簡化了從以邀請為基礎的組織的轉換。

如果您這麼做，所有目前關聯的成員帳戶都會繼續成為成員。如果某個成員帳戶屬於您組織的一部分 AWS Organizations，帳戶的關聯會自動從「受邀請」變更為 Macie AWS Organizations中的「Via」。如果某個成員帳戶不屬於您組織的一部分 AWS Organizations，則該帳戶的關聯仍然是「按邀請」。在這兩種情況下，帳戶仍會繼續與委派的 Macie 管理員帳戶作為成員帳戶建立關聯。

我們建議使用這種方法，因為一個帳戶無法同時與多個 Macie 管理員帳戶建立關聯。如果您指定不同的帳戶作為中組織的 Macie 管理員帳戶 AWS Organizations，指定的管理員將無法透過邀請來管理已與另一個 Macie 管理員帳戶相關聯的帳戶。每個成員帳戶必須先取消與其目前、以邀請為基礎的管理員帳戶的關聯。然後，您組織的 Macie 管理員 AWS Organizations 可以將帳戶新增為 Macie 成員帳戶，並開始管理帳戶。

在您與 Macie 整合 AWS Organizations 並在 Macie 中設定您的組織之後，您可以選擇性地為組織指定不同的 Macie 管理員帳戶。您也可以繼續使用邀請來關聯和管理不屬於您組織的成員帳戶 AWS Organizations。

在 Amazon Macie 中整合和設定組織

若要開始使用 Amazon Macie AWS Organizations，組織的 AWS Organizations 管理帳戶會將帳戶指定為該組織的委派 Macie 管理員帳戶。這使 Macie 成為中 AWS Organizations的受信任服務。它也會為指定的管理員帳戶啟 AWS 區域 用目前的 Macie，並允許指定的管理員帳戶啟用和管理該區域中組織中其他帳戶的 Macie。如需有關如何授與這些權限的資訊，請參閱《使用指南》 AWS 服務中的「 AWS Organizations 與其他權限搭配AWS Organizations 使用

委派的 Macie 管理員接著會在 Macie 中設定組織，主要是將組織的帳戶新增為「區域」中的 Macie 成員帳戶。然後，管理員可以存取該區域中這些帳戶的特定 Macie 設定、資料和資源。他們還可以執行自動化敏感資料探索和執行敏感資料探索任務，以在帳戶擁有的 Amazon Simple Storage Service (Amazon S3) 儲存貯體中偵測敏感資料。

本主題說明如何為組織指定委派的 Macie 管理員，以及如何將組織的帳戶新增為 Macie 成員帳戶。執行這些工作之前，請確定您瞭解管理員帳戶與成員帳戶之間的關係。檢閱搭 AWS Organizations配使用 Macie 的注意事項和建議也是個好主意。

任務

- 步驟 1：驗證您的權限
- 步驟 2：指定組織的委派 Macie 管理員帳戶
- 步驟 3：自動啟用並新增組織帳戶作為 Macie 成員帳戶
- 步驟 4：啟用並新增現有組織帳戶作為 Macie 成員帳戶

若要整合和設定多個區域中的組織， AWS Organizations 管理帳戶和委派的 Macie 管理員會在每個額外的區域中重複這些步驟。

步驟 1：驗證您的權限

在您為組織指定委派的 Macie 管理員帳戶之前，請確認您 (身為 AWS Organizations 管理帳戶的使用者) 可以執行下列 Macie 動作：`macie2:EnableOrganizationAdminAccount`此動作可讓您使用 Macie 指定組織的委派 Macie 管理員帳戶。

此外，請確認您是否被允許執行下列 AWS Organizations 動作：

- `organizations:DescribeOrganization`
- `organizations:EnableAWSServiceAccess`
- `organizations:ListAWSServiceAccessForOrganization`
- `organizations:RegisterDelegatedAdministrator`

這些動作可讓您：擷取組織的相關資訊、與 Macie 整合、擷取與 AWS Organizations之整合的 AWS 服務 相關資訊 AWS Organizations；以及為您的組織指定委派的 Macie 管理員帳戶。

若要授予這些權限，請在帳戶的 AWS Identity and Access Management (IAM) 政策中包含下列陳述式：

```
{
   "Sid": "Grant permissions to designate a delegated Macie administrator",
   "Effect": "Allow",
   "Action": [
```

```
      "macie2:EnableOrganizationAdminAccount",
      "organizations:DescribeOrganization",
      "organizations:EnableAWSServiceAccess",
      "organizations:ListAWSServiceAccessForOrganization",
      "organizations:RegisterDelegatedAdministrator"
   ],
   "Resource": "*"
}
```

如果您想要將 AWS Organizations 管理帳戶指定為組織委派的 Macie 管理員帳戶，您的帳戶還需要執行下列 IAM 動作的權限：`CreateServiceLinkedRole`此動作可讓您為管理帳戶啟用 Macie。不過，根據 AWS 安全性最佳做法和最低權限原則，我們不建議您這麼做。

如果您決定授予此權限，請在 AWS Organizations 管理帳戶的 IAM 政策中新增下列陳述式：

```
{
   "Sid": "Grant permissions to enable Macie",
   "Effect": "Allow",
   "Action": [
      "iam:CreateServiceLinkedRole"
   ],
   "Resource": "arn:aws:iam::111122223333:role/aws-service-role/macie.amazonaws.com/
AWSServiceRoleForAmazonMacie",
   "Condition": {
      "StringLike": {
         "iam:AWSServiceName": "macie.amazonaws.com"
      }
   }
}
```

在對帳單中，將 *111122223333* 取代為管理帳戶的帳戶識別碼。

如果您想要在選擇加入 AWS 區域 (預設為停用的區域) 中管理 Macie，請同時更新`Resource`元素和條件中 Macie 服務主體的值。`iam:AWSServiceName`此值必須指定「區域」的「地區」代碼。例如，若要管理中東 (巴林) 區域的 Macie，該區域的區域代碼為 me-south-1，請執行以下操作：

- 在`Resource`元素中，替換

  `arn:aws:iam::111122223333:role/aws-service-role/macie.amazonaws.com/AWSServiceRoleForAmazonMacie`

  取代為

```
arn:aws:iam::111122223333:role/aws-service-role/macie.me-
south-1.amazonaws.com/AWSServiceRoleForAmazonMacie
```

其中 *111122223333* 會指定管理帳戶的帳戶識別碼，而 *me-south-1* 會指定區域的地區代碼。

- 在iam:AWSServiceName條件下，取代macie.amazonaws.com為macie.*me-south-1*.amazonaws.com，其中 *me-south-1* 指定「區域」的「區域」代碼。

如需目前可使用 Macie 的區域清單以及每個區域的 Amazon Macie 域代碼，請參閱. AWS 一般參考 如需選擇加入區域的相關資訊，請參閱AWS Account Management 參考指南中的指定 AWS 區域 您的帳戶可以使用的項目。

步驟 2：指定組織的委派 Macie 管理員帳戶

驗證權限後，您 (身為 AWS Organizations 管理帳戶的使用者) 可以為組織指定委派的 Macie 管理員帳戶。

若要指定組織的委派 Macie 管理員帳戶

若要為您的組織指定委派的 Macie 管理員帳戶，您可以使用 Amazon Macie 主控台或 Amazon Macie API。只有 AWS Organizations 管理帳戶的使用者可以執行此工作。

Console

請依照下列步驟使用 Amazon Macie 主控台指定委派的 Macie 管理員帳戶。

若要指定委派的 Macie 管理員帳戶

1. AWS Management Console 使用您的 AWS Organizations 管理帳戶登入。
2. 使用頁面右上角的選取 AWS 區域 器，選取您要在其中指定組織委派 Macie 管理員帳戶的區域。
3. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
4. 根據目前區域中的管理帳戶是否已啟用 Macie，執行下列其中一項作業：
   - 如果未啟用 Macie，請在歡迎頁面上選擇 [開始使用]。
   - 如果已啟用 Macie，請在導覽窗格中選擇 [設定]。
5. 在「委派管理員」下，輸入您要指定為 Macie 管理員帳戶的 12 位數帳號 ID。 AWS 帳戶
6. 選擇委派。

在您要將組織與 Macie 整合的每個其他區域中，重複上述步驟。您必須在這些區域中指定相同的 Macie 管理員帳戶。

API

若要以程式設計方式指定委派的 Macie 管理員帳戶，請使用 Amazon Macie API 的EnableOrganizationAdminAccount操作。若要在多個區域中指定科目，請針對您要將組織與 Macie 整合的每個區域提交指定。您必須在這些區域中指定相同的 Macie 管理員帳戶。

當您提交指定時，請使用必要的`adminAccountId`參數來指定要指定為組織的 AWS 帳戶 Macie 管理員帳戶的 12 位數帳號 ID。同時請務必指定要套用指定的「區域」。

若要使用 AWS Command Line Interface (AWS CLI) 指定 Macie 管理員帳戶，請執行命enable-organization-admin-account令。對於`admin-account-id`參數，請指定 AWS 帳戶 要指定的 12 位數帳戶 ID。使用`region`參數指定要套用指定的「區域」。例如：

```
C:\> aws macie2 enable-organization-admin-account --region us-east-1 --admin-
account-id 111122223333
```

其中 *us-east-1* 是指定套用至的區域 (美國東部 (維吉尼亞北部) 區域)，*111122223333* 是要指定帳戶的帳戶識別碼。

指定組織的 Macie 管理員帳戶後，Macie 管理員即可開始在 Macie 中配置組織。

步驟 3：自動啟用並新增組織帳戶作為 Macie 成員帳戶

根據預設，當帳戶新增至您的組織時，新帳戶不會自動啟用 Macie。 AWS Organizations此外，帳戶不會自動添加為 Macie 成員帳戶。這些帳號會顯示在 Macie 管理員的帳戶清單中。不過，Macie 不一定會為帳戶啟用，而 Macie 管理員也不一定會存取帳戶的 Macie 設定、資料和資源。

如果您是組織的委派 Macie 管理員，您可以變更此組態設定。您可以為組織開啟自動啟用。如果您這麼做，當帳戶新增至您的組織中時，Macie 會自動為新帳戶啟用 AWS Organizations，而這些帳戶會自動與您的 Macie 管理員帳戶關聯為成員帳戶。開啟此設定不會影響組織中的現有帳戶。若要啟用和管理現有帳戶的 Macie，您必須手動將帳戶新增為 Macie 成員帳戶。下一步說明如何執行此操作。

> **備註**
>
> 如果您開啟自動啟用，請注意下列例外狀況：
>
> - 如果新帳戶已與不同的 Macie 管理員帳戶相關聯，Macie 不會自動將該帳戶新增為組織中的成員帳戶。

該帳戶必須先取消與其目前 Macie 管理員帳戶的關聯，才能成為您在 Macie 中組織的一部分。然後，您可以手動添加帳戶。若要識別發生這種情況的科目，您可以複查組織的科目存貨。

- 如果您的組織達到 10,000 Macie 成員帳戶的配額 AWS 區域，Macie 會自動關閉「地區」中的此設定。

  如果發生這種情況，我們會通過為您的 Macie 管理員帳戶創建 AWS Health 和 Amazon CloudWatch 事件通知您。我們也會傳送電子郵件至與該帳戶相關聯的電子郵件地址。如果帳戶總數隨後減少到 10,000 個以下，Macie 會自動再次開啟設定。

自動啟用並新增組織帳戶作為 Macie 成員帳戶

要自動啟用並將新帳戶添加為 Macie 會員帳戶，您可以使用 Amazon Macie 控制台或 Amazon Macie API。只有委派的組織 Macie 管理員可以執行此任務。

Console

若要使用控制台執行此工作，您必須被允許執行下列 AWS Organizations 動作：`organizations:ListAccounts`此動作可讓您擷取並顯示組織中帳號的相關資訊。如果您具有這些權限，請依照下列步驟自動啟用並新增新的組織帳戶作為 Macie 成員帳戶。

若要自動啟用和新增組織帳戶

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 使用頁面右上角的選取 AWS 區域 器，選取您要在其中自動啟用的區域，並將新帳戶新增為 Macie 成員帳戶。
3. 在導覽窗格中，選擇帳戶。
4. 在 [帳戶] 頁面的 [新帳戶] 區段中，選擇 [編輯]。
5. 在 [編輯新帳戶的設定] 對話方塊中，選取 [啟用 Macie]。

   若要同時為新成員帳戶啟用自動敏感資料探索功能，請選取 [啟用自動敏感資料探索]。如果您為帳戶啟用此功能，Macie 會持續從帳戶的 S3 儲存貯體中選取範例物件，並分析物件以判斷它們是否包含敏感資料。如需詳細資訊，請參閱 執行自動化敏感資料探索。
6. 選擇 Save (儲存)。

在您要在 Macie 中配置組織的每個其他區域中，重複上述步驟。

若要隨後變更這些設定，請重複上述步驟，並清除每個設定的核取方塊。

API

若要以程式設計方式自動啟用和新增 Macie 成員帳戶，請使用 Amazon Macie API 的UpdateOrganizationConfiguration操作。當您提交請求時，請將autoEnable參數的值設定為true。(預設值為 false。) 此外，請務必指定要求適用的「地區」。若要在其他區域中自動啟用並新增帳戶，請針對每個額外區域提交要求。

如果您使用 AWS CLI 提交請求，請執行命update-organization-configuration令並指定要自動啟用和新增帳戶的auto-enable參數。例如：

```
$ aws macie2 update-organization-configuration --region us-east-1 --auto-enable
```

其中 *us-east-1* 是自動啟用和新增帳戶的區域，即美國東部 (維吉尼亞北部) 區域。

若要隨後變更此設定並停止自動啟用和新增帳戶，請再次執行相同的命令，並在每個適用的「區域」中使用auto-enable參數而非參數。no-auto-enable

您也可以為新成員帳戶自動啟用自動敏感資料探索功能。如果您為帳戶啟用此功能，Macie 會持續從帳戶的 S3 儲存貯體中選取範例物件，並分析物件以判斷它們是否包含敏感資料。如需詳細資訊，請參閱 執行自動化敏感資料探索。若要為成員帳戶自動啟用此功能，請使用UpdateAutomatedDiscoveryConfiguration作業，或者，如果您正在使用 AWS CLI，請執行update-automated-discovery-configuration命令。

步驟 4：啟用並新增現有組織帳戶作為 Macie 成員帳戶

當您與 Macie 整合時 AWS Organizations，不會為組織中的所有現有帳戶自動啟用 Macie。此外，這些帳戶不會自動與委派的 Macie 管理員帳戶作為 Macie 成員帳戶關聯。因此，在 Macie 中整合和設定組織的最後一個步驟是將現有的組織帳戶新增為 Macie 成員帳戶。當您將現有帳戶添加為 Macie 成員帳戶時，Macie 會自動為該帳戶啟用，並且您（作為委託的 Macie 管理員）可以訪問該帳戶的某些 Macie 設置，數據和資源。

請注意，您無法新增目前與另一個 Macie 管理員帳戶關聯的帳戶。若要新增帳戶，請與帳戶擁有者合作，先取消帳戶與其目前管理員帳戶的關聯。此外，如果該帳戶目前已暫停 Macie，則無法新增現有帳戶。帳戶擁有者必須先重新啟用該帳戶的 Macie。最後，如果您想要將 AWS Organizations 管理帳戶新增為成員帳戶，該帳戶的使用者必須先為該帳戶啟用 Macie。

啟用並新增現有組織帳戶作為 Macie 成員帳戶

若要啟用並將現有的組織帳戶新增為 Macie 成員帳戶，您可以使用 Amazon Macie 主控台或 Amazon Macie API。只有委派的組織 Macie 管理員可以執行此任務。

Console

若要使用控制台執行此工作，您必須被允許執行下列 AWS Organizations 動作：`organizations:ListAccounts`此動作可讓您擷取並顯示組織中帳號的相關資訊。如果您具有這些權限，請按照以下步驟啟用現有帳戶並將其添加為 Macie 成員帳戶。

若要啟用及新增現有的組織帳號

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 使用頁面右上角的選取 AWS 區域 器，選取您要啟用的區域，並將現有帳戶新增為 Macie 成員帳戶。
3. 在導覽窗格中，選擇帳戶。

   「帳戶」頁面隨即開啟，並顯示與您的 Macie 帳戶相關聯的帳戶表格。如果帳戶是中組織的一部分 AWS Organizations，則其「類型」為「通過」 AWS Organizations。如果帳戶已經是 Macie 成員帳戶，則其狀態為已啟用。
4. 在「帳戶」表格中，針對您要新增為 Macie 成員帳戶的每個帳戶選取核取方塊。
5. 在「動作」功能表上，選擇「新增成員」。
6. 確認您要將選取的帳戶新增為成員帳戶。

確認新增所選帳戶之後，帳戶的狀態會變更為 [正在啟用]，然後變更為 [已啟用]。新增成員帳戶後，您也可以為帳戶啟用自動敏感資料探索：在 [帳戶] 表格中，選取每個帳戶的核取方塊以啟用該帳戶，然後選擇 [動作] 功能表上的 [啟用自動敏感資料探索]。如果您為帳戶啟用此功能，Macie 會持續從帳戶的 S3 儲存貯體中選取範例物件，並分析物件以判斷它們是否包含敏感資料。如需詳細資訊，請參閱 執行自動化敏感資料探索。

在您要在 Macie 中配置組織的每個其他區域中，重複上述步驟。

API

若要以程式設計方式啟用並新增一或多個現有帳戶做為 Macie 成員帳戶，請使用 Amazon Macie API 的CreateMember操作。當您提交要求時，請使用支援的參數來指定要啟用和新增的每個 AWS 帳戶 帳戶 ID 和電子郵件地址。同時指定要套用要求的「區域」。若要在其他區域中啟用並新增現有帳戶，請針對每個額外區域提交請求。

若要擷取要啟用和新增的帳戶 ID 和電子郵件地址，您可以選擇性地使用 Amazon Macie API 的ListMembers操作。 AWS 帳戶 此操作提供有關與您的 Macie 帳戶相關聯的帳戶的詳細信息，包括不是 Macie 成員帳戶的帳戶。如果帳戶`relationshipStatus`屬性的值不是`Enabled`，則該帳戶不是 Macie 成員帳戶。

若要使用啟用和新增一或多個現有帳戶 AWS CLI，請執行建立成員命令。使用`region`參數可指定要在其中啟用和新增帳戶的「區域」。使用`account`參數來指定每個 AWS 帳戶 要新增的帳戶 ID 和電子郵件地址。例如：

```
C:\> aws macie2 create-member --region us-east-1 --account={\"accountId\":
\"123456789012\",\"email\":\"janedoe@example.com\"}
```

```
## us-east-1 ############## Macie ####### (#### (######) ##)##account###
########## (123456789012) ####### (janedoe@example.com)#
```

如果您的要求成功，指定帳戶的狀態 (`relationshipStatus`) 會變更為您`Enabled`的帳戶庫存。

若要同時為一或多個帳戶啟用自動化敏感資料探索，請使用該BatchUpdateAutomatedDiscoveryAccounts作業，或者，如果您使用的是 AWS CLI，請執行 batch-update-automated-discovery- account 命令。如果您為帳戶啟用此功能，Macie 會持續從帳戶的 S3 儲存貯體中選取範例物件，並分析物件以判斷它們是否包含敏感資料。如需更多詳細資訊，請參閱 執行自動化敏感資料探索。

查看一個組織的 Amazon Macie 帳戶

在 Amazon Macie 中整合並設定 AWS Organizations組織後，委派的 Macie 管理員可以在 Macie 中存取組織帳戶的清查。身為組織的 Macie 管理員，您可以使用此庫存來複查組織 Macie 帳戶的統計資料和詳細資訊。 AWS 區域您也可以使用它來執行帳戶的某些管理工作。

若要檢視組織的 Macie 帳戶

若要檢閱組織的帳戶，您可以使用 Amazon Macie 主控台或 Amazon Macie API。如果您偏好使用主控台，您必須被允許執行下列 AWS Organizations 動作：`organizations:ListAccounts`。此動作可讓您擷取及顯示屬於中組織之帳號的相關資訊 AWS Organizations。

Console

請依照下列步驟使用 Amazon Macie 主控台檢閱組織的 Macie 帳戶。

若要檢閱您組織的帳戶

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 使用頁面右上角的選取 AWS 區域 器，選取您要檢閱組織帳戶的地區。
3. 在導覽窗格中，選擇帳戶。

「帳戶」頁面會開啟並顯示彙總統計資料，以及目前 AWS 區域與您的 Macie 帳戶相關聯的帳戶表格。

在 [帳戶] 頁面頂端，您會看到下列彙總統計資料。

通過 AWS Organizations

「作用中」會報告透過與您的帳戶相關聯的帳戶總數， AWS Organizations 而且目前為組織中的 Macie 成員帳戶。這些帳戶已啟用 Macie，您是帳戶的 Macie 管理員。

所有報告通過與您的帳戶關聯的帳戶總數 AWS Organizations，包括當前不是 Macie 成員帳戶的帳戶。

通過邀請

活動報告通過 Macie 邀請與您的帳戶相關聯的帳戶總數，目前是 Macie 成員帳戶。這些帳戶不會透過以下方式與您的帳戶相關聯 AWS Organizations。Macie 已為帳戶啟用，您是帳戶的 Macie 管理員，因為他們接受了您的 Macie 會員邀請。

所有報告通過 Macie 邀請與您的帳戶相關聯的帳戶總數，包括尚未回應您的邀請的帳戶。

主動/全部

活動報告的帳戶總數目前是 Macie 成員帳戶為您的帳戶，通過 AWS Organizations 或通過 Macie 邀請。這些帳戶已啟用 Macie，您是帳戶的 Macie 管理員。

所有報告通過 AWS Organizations 或通過 Macie 邀請與您的帳戶關聯的帳戶總數。這包括屬於您組織中 AWS Organizations 且目前不是 Macie 成員帳戶的帳戶，以及任何尚未回應您的 Macie 成員資格邀請的帳戶。

您可以在表格中找到目前區域中每個帳戶的詳細資訊。此表格包含透過 AWS Organizations 或透過 Macie 邀請函與您的 Macie 帳戶相關聯的所有帳戶。

帳戶 ID

的帳戶 ID 和電子郵件地址 AWS 帳戶。

名稱

的帳戶名稱 AWS 帳戶。對於透過 Macie 邀請與您的帳戶相關聯的帳戶，此值通常為 N/A。

類型

該帳戶如何通過 AWS Organizations 或通過 Macie 邀請與您的帳戶關聯。

狀態

您的帳戶與帳戶之間的關係狀態。對於組 AWS Organizations 織中的帳戶 (「類型」為「通過」AWS Organizations)，可能的值為：

- 帳戶已暫停 — AWS 帳戶 已暫停。
- 建立/啟用 — Macie 正在處理啟用帳戶並將帳戶新增為 Macie 成員帳戶的請求。
- 已啟用 — 該帳戶是 Macie 成員帳戶。該帳戶已啟用 Macie，而您是該帳戶的 Macie 管理員。
- 不是成員 — 該帳戶屬於您組織的一部分， AWS Organizations 但不是 Macie 成員帳戶。
- 暫停（已暫停）— 該帳戶是 Macie 成員帳戶，但 Macie 目前已暫停該帳戶。
- 已停用區域 — 帳戶屬於您組織的一部分， AWS Organizations 但目前的 [區域] 已針對停用 AWS 帳戶。
- 已移除 (取消關聯) — 該帳戶先前是 Macie 成員帳戶，但隨後被移除為會員帳戶。您將帳戶與您的 Macie 管理員帳戶取消關聯。馬西繼續為該帳戶啟用。

上次狀態更新

當您或關聯帳戶最近執行了影響您帳戶之間關係的動作時。

自動化敏感資料探索

帳戶目前是否已啟用或停用自動敏感資料探索。

若要依特定欄位對表格進行排序，請選擇欄位的欄標題。若要變更排序順序，請再次選擇欄標題。若要篩選表格，請將游標置於篩選方塊中，然後新增欄位的篩選條件。若要進一步細化結果，請新增其他欄位的篩選條件。

API

若要以程式設計方式檢閱組織的帳戶，請使用 Amazon Macie API 的ListMembers操作，並指定要套用請求的區域。若要複查其他區域中的帳戶，請在每個額外的區域中提交您的請求。

當您提交請求時，請使用`onlyAssociated`參數來指定要包含在回應中的科目。默認情況下，Macie 通過 AWS Organizations 或通過 Macie 邀請返回有關僅指定區域中 Macie 成員帳戶的

那些帳戶的詳細信息。若要擷取與您 Macie 帳戶相關聯的所有帳戶 (包括非成員帳戶的帳戶) 的這些詳細資訊，請在請求中包含`onlyAssociated`參數，並將`false`參數值設定為。

若要使用 AWS Command Line Interface (AWS CLI) 檢閱組織的帳戶，請執行`清單成員`命令。對於`only-associated`參數，請指定是要包含所有關聯帳戶還是僅包含 Macie 成員帳戶。若只要包含成員帳戶，請省略此參數或將參數值設定為`true`。若要包含所有帳戶，請將此值設定為`false`。例如：

```
C:\> aws macie2 list-members --region us-east-1 --only-associated false
```

其中 *us-east-1* 是要求適用的區域，即美國東部 (維吉尼亞北部) 區域。

如果您的請求成功，Macie 返回一個數組`members`。陣列會針`member`對符合要求中指定準則的每個帳戶包含一個物件。在該對象中，該`relationshipStatus`字段指示您的帳戶與指定區域中的其他帳戶之間的關係的當前狀態。對於組 AWS Organizations 織中的帳戶，可能的值為：

- `AccountSuspended`— 已 AWS 帳戶 暫停。
- `Created`— Macie 正在處理啟用帳戶並將帳戶新增為 Macie 成員帳戶的請求。
- `Enabled`— 該帳戶是一個馬西會員帳戶. 該帳戶已啟用 Macie，而您是該帳戶的 Macie 管理員。
- `Paused`— 該帳戶是一個 Macie 成員帳戶，但馬西目前被暫停 (暫停) 該帳戶.
- `RegionDisabled`— 帳戶屬於您組織中的一部分， AWS Organizations 但目前的 [區域] 已針對 AWS 帳戶.
- `Removed`— 該帳戶以前是 Macie 成員帳戶，但隨後被刪除為會員帳戶。您將帳戶與您的 Macie 管理員帳戶取消關聯。馬西繼續為該帳戶啟用。

如需有關`member`物件中其他欄位的資訊，請參閱 Amazon Macie API 參考資料中的`成員`。

管理一個組織的 Amazon Macie 成員帳戶

在 Amazon Macie 中`整合並設定 AWS Organizations`組織後，該組織委派的 Macie 管理員可以存取成員帳戶的特定 Macie 設定、資料和資源。

身為組織的 Macie 管理員，您可以在 Macie 中集中執行特定帳戶管理和管理工作。例如：

- 添加和刪除 Macie 成員帳戶
- 管理個別帳戶的 Macie 狀態，例如啟用或暫停帳戶的 Macie
- 監控個別帳戶和組織整體的 Macie 配額和估計使用成本

您也可以檢閱 Amazon Simple Storage Service (Amazon S3) 庫存資料和 Macie 會員帳戶的政策發現。此外，您還可以在帳戶擁有的 S3 儲存貯體中探索敏感資料。如需可執行之工作的詳細清單，請參閱了解 Amazon Macie 管理員和會員帳戶之間的關係。

根據預設，Macie 可讓您查看組織中所有 Macie 成員帳戶的相關資料和資源。您也可以向下鑽研以檢閱個別帳戶的資料和資源。例如，如果您使用摘要儀表板來評估組織的 Amazon S3 安全狀態，則可以按帳戶篩選資料。同樣地，如果您監控預估的使用成本，則可以存取個別成員帳戶的估計費用明細。

除了管理員和成員帳戶通用的工作之外，您還可以為組織執行各種管理工作。

任務

- 將 Amazon Macie 成員帳戶添加到組織中
- 暫停 Amazon Macie 在組織中的成員帳戶
- 從組織中刪除 Amazon Macie 成員帳戶

身為組織的 Macie 管理員，您可以使用 Amazon Macie 主控台或亞馬 Amazon Macie API 來執行這些任務。如果您偏好使用主控台，您必須被允許執行下列 AWS Organizations 動作：`organizations:ListAccounts`。此動作可讓您擷取及顯示屬於中組織之帳號的相關資訊 AWS Organizations。

將 Amazon Macie 成員帳戶添加到組織中

在某些情況下，您可能需要手動將帳戶新增為 Macie 成員帳戶。對於您先前移除 (取消關聯) 為成員帳戶的帳戶，就會發生這種情況。如果您沒有將 Macie 設定為在 AWS Organizations中將帳戶新增至組織時自動啟用和新增成員帳戶，也會發生這種情況。

當您將帳戶添加為 Macie 會員帳戶時：

- 如果尚未在區域中啟用此帳戶 AWS 區域，則會為目前帳戶啟用 Macie。
- 該帳戶與您的 Macie 管理員帳戶相關聯，作為區域中的成員帳戶。會員帳戶不會收到邀請或其他通知，告知您在帳戶之間建立了這種關係。
- 區域中的帳戶可能會啟用自動化敏感資料探索功能。這取決於您為組織指定的組態設定。如需詳細資訊，請參閱 設定自動化敏感資料探索。

請注意，您無法新增已與其他 Macie 管理員帳戶相關聯的帳戶。該帳戶必須先取消與其當前管理員帳戶的關聯。此外，除非帳戶已啟用 Macie，否則您無法將 AWS Organizations 管理帳戶新增為會員帳戶。若要瞭解其他需求，請參閱搭配使用 Amazon Macie 的注意事項和建議 AWS Organizations。

若要將 Macie 成員帳戶新增至組織

要將一個或多個 Macie 成員帳戶添加到您的組織，您可以使用 Amazon Macie 控制台或 Amazon Macie API。

Console

請依照下列步驟使用 Amazon Macie 主控台新增一或多個 Macie 成員帳戶。

要添加一個馬西成員帳戶

1. 在以下位置打開 Amazon Macie 控制台 https://console.aws.amazon.com/macie/。
2. 使用頁面右上角的選取 AWS 區域 器，選取您要新增成員帳戶的地區。
3. 在導覽窗格中，選擇帳戶。[帳戶] 頁面隨即開啟，並顯示與您帳戶相關聯的帳戶表格。
4. (選擇性) 若要更輕鬆地識別屬於組織中 AWS Organizations 且不是 Macie 成員帳戶的帳戶，請使用「帳戶」表上方的篩選方塊來新增下列篩選條件：

   - 類型 = 組織
   - 狀態 = 不是成員

   若要同時顯示您先前移除且可能想要新增為成員帳戶的帳戶，請同時新增 「狀態 = 已移除」篩選條件。
5. 在「帳戶」表中，針對要新增為成員帳戶的每個帳戶選取核取方塊。
6. 在「動作」功能表上，選擇「新增成員」。
7. 確認您要將選取的帳戶新增為成員帳戶。

確認您的選擇後，所選帳戶的狀態會變更為 [正在啟用]，然後在您的帳戶詳細目錄中變更為 [已啟用]。

在您要新增成員帳戶的每個其他區域中，重複上述步驟。

API

若要以程式設計方式新增一或多個 Macie 成員帳戶，請使用 Amazon Macie API 的CreateMember操作。

當您提交要求時，請使用支援的參數為您要新增的每個帳戶 ID 和電子郵件地址指定 12 位數 AWS 帳戶 的帳戶 ID 和電子郵件地址。同時指定要套用要求的「區域」。若要在其他區域新增帳戶，請在每個額外的區域中提交您的請求。

若要擷取要新增之帳戶的帳戶 ID 和電子郵件地址，您可以將 API ListAccounts作業的輸出與 Amazon Macie AWS Organizations API 的ListMembers操作相互關聯。對於 Macie API 的ListMembers操作，請在請求中包含`onlyAssociated`參數，並將`false`參數的值設置為。如果作業成功，Macie 會傳回`members`陣列，其中提供與指定區域中之 Macie 管理員帳戶相關聯的所有帳戶的詳細資料，包括目前不是成員帳戶的帳戶。請注意陣列中的下列事項：

- 如果帳戶`relationshipStatus`屬性的值不是`Enabled`，則該帳戶與您的帳戶相關聯，但它不是 Macie 成員帳戶。
- 如果某個帳戶未包含在陣列中，但包含在 AWS Organizations API ListAccounts 作業的輸出中，則該帳戶屬於您組織的一部分， AWS Organizations 但與您的帳戶不相關聯，因此不是 Macie 成員帳戶。

若要使用新增成員帳戶 AWS CLI，請執行建立成員命令。使用`region`參數可指定要在其中新增帳戶的「區域」。使用`account`參數指定要新增之每個帳戶的帳戶 ID 和電子郵件地址。例如：

```
C:\> aws macie2 create-member --region us-east-1 --account={\"accountId\":
\"123456789012\",\"email\":\"janedoe@example.com\"}
```

```
## us-east-1 ############### (#### (######) ##)##account#############
(123456789012) ####### (janedoe@example.com)#
```

如果您的要求成功，指定帳戶的狀態 (`relationshipStatus`) 會變更為您`Enabled`的帳戶庫存。

暫停 Amazon Macie 在組織中的成員帳戶

身為中組織的 Macie 管理員 AWS Organizations，您可以針對組織中的成員帳戶暫停 Macie。如果您這樣做，您也可以稍後重新啟用該帳戶的 Macie。

當您暫停 Macie 的會員帳戶時：

- Macie 無法存取目 AWS 區域前帳戶的 Amazon S3 資料，並停止提供有關該帳戶之 Amazon S3 資料的中繼資料。
- Macie 停止執行該地區帳戶的所有活動。這包括監控 S3 儲存貯體的安全性和存取控制、執行自動化敏感資料探索，以及執行目前正在進行的敏感資料探索任務。
- Macie 會取消區域中帳戶建立的所有敏感資料探索工作。工作取消後無法繼續或重新啟動。如果您建立工作來分析該成員帳戶擁有的資料，Macie 不會取消您的工作。相反地，工作會略過帳戶所擁有的資源。

暫停帳戶時，Macie 會保留適用區域中帳戶的 Macie 工作階段識別碼、設定和資源。例如，帳戶的發現項目會保持完整，最多 90 天不受影響。當 Macie 在該地區的帳戶遭到停權時，您的組織不會針對適用地區的帳戶產生 Macie 費用。

若要暫停組織中的成員帳戶的 Macie

要暫停 Macie 組織中的成員帳戶，您可以使用 Amazon Macie 控制台或 Amazon Macie API。

Console

請按照以下步驟使用亞馬遜 Macie 控制台暫停會員帳戶的 Macie。

暫停會員帳戶的 Macie

1. 在以下位置打開 Amazon Macie 控制台 https://console.aws.amazon.com/macie/。
2. 使用頁面右上角的選取 AWS 區域 器，選取您要暫停成員帳戶 Macie 的區域。
3. 在導覽窗格中，選擇帳戶。[帳戶] 頁面隨即開啟，並顯示與您帳戶相關聯的帳戶表格。
4. 在「帳戶」表中，選取您要暫停之帳戶的核取方塊。
5. 在 [動作] 功能表上，選擇 [暫停 Macie]。
6. 確認您要暫停該帳戶的 Macie。

確認停權後，帳戶詳細目錄中的帳戶狀態會變更為「已暫停 (已暫停)」。

在您要暫停帳戶 Macie 的每個其他區域中，重複上述步驟。

API

要以編程方式暫停成員帳戶的 Macie，請使用 Amazon Macie API 的UpdateMemberSession操作。

當您提交請求時，請使用id參數來指定您要暫停 Macie 的 12 位數帳戶 ID。 AWS 帳戶 對於status參數，請指定PAUSED為 Macie 帳戶的新狀態。同時指定要套用要求的「區域」。若要在其他區域暫停帳戶，請在每個額外的區域中提交您的要求。

若要擷取要暫停帳戶的帳戶識別碼，您可以使用 Amazon Macie API 的ListMembers操作。如果您這麼做，請考慮在要求中加入onlyAssociated參數來篩選結果。如果將此參數的值設定為true，Macie 會傳回一個members陣列，該陣列僅提供目前為成員帳戶的帳戶的詳細資訊。

若要使用暫停成員帳戶的 Macie AWS CLI，請執行命update-member-session令。使用region參數可指定要在其中暫停 Macie 的區域，並使用id參數指定 AWS 帳戶 要暫停 Macie 的帳戶 ID。針對 status 參數，請指定 PAUSED。例如：

```
C:\> aws macie2 update-member-session --region us-east-1 --id 123456789012 --status
 PAUSED
```

其中 *us-east-1* 是要暫停 Macie (美國東部 (維吉尼亞北部) 區域) 的區域，*123456789012* 是帳戶暫停 Macie 的帳戶識別碼，而且是該帳戶的新狀態 Macie。PAUSED

如果您的要求成功，Macie 會傳回空白回應，而指定帳戶的狀態會Paused在您的帳戶清單中變更為。

從組織中刪除 Amazon Macie 成員帳戶

如果您想停止訪問會員帳戶的 Macie 設置，數據和資源，則可以刪除該帳戶作為 Macie 成員帳戶。您可以通過取消與 Macie 管理員帳戶的帳戶關聯來完成此操作。請注意，只有您可以為會員帳戶執行此操作。 AWS Organizations 成員帳戶無法取消與其 Macie 管理員帳戶的關聯。

當您移除 Macie 成員帳戶時，Macie 會在目前的帳戶中保持啟用狀態。 AWS 區域但是，該帳戶與您的 Macie 管理員帳戶斷開關聯，並成為獨立的 Macie 帳戶。這表示您無法存取帳戶的所有 Macie 設定、資料和資源，包括帳戶 Amazon S3 資料的中繼資料和政策發現項目。這也表示您無法再使用 Macie 探索帳戶擁有的 S3 儲存貯體中的敏感資料。如果您已建立敏感探索工作來執行此操作，則工作會略過帳戶擁有的值區。如果您為帳戶啟用了自動化敏感資料探索功能，則您和該成員帳戶在執行帳戶的自動化探索時，無法存取 Macie 產生並直接提供的統計資料、庫存資料和其他資訊。

移除 Macie 成員帳戶後，該帳戶會繼續顯示在您的帳戶清單中。Macie 不會通知帳戶擁有者您已移除帳戶。您可以稍後再次將帳戶新增至您的組織。如果您在 30 天內新增帳戶並啟用自動化敏感資料探索功能，您也會重新取得對 Macie 先前產生並直接提供的資料和資訊的存取權，同時為該帳戶執行自動探索。

若要從組織中移除 Macie 成員帳戶

要從您的組織中刪除 Macie 成員帳戶，您可以使用 Amazon Macie 控制台或 Amazon Macie API。

Console

請按照以下步驟使用亞馬遜 Macie 控制台刪除 Macie 成員帳戶。

若要移除馬西成員帳戶

1. 在以下位置打開 Amazon Macie 控制台 https://console.aws.amazon.com/macie/。
2. 使用頁面右上角的選取 AWS 區域 器，選取您要移除成員帳戶的地區。

3. 在導覽窗格中，選擇帳戶。[帳戶] 頁面隨即開啟，並顯示與您帳戶相關聯的帳戶表格。
4. 在「帳戶」表中，選取要移除為成員帳戶之帳戶的核取方塊。
5. 在 [動作] 功能表上，選擇 [取消帳號關聯]。
6. 確認您要移除選取的帳戶作為成員帳戶。

確認您的選擇後，帳戶詳細目錄中的帳戶狀態會變更為「已移除 (已取消關聯)」。

在您要移除成員帳戶的其他每個區域中，重複上述步驟。

API

要以編程方式刪除 Macie 成員帳戶，請使用 Amazon Macie API 的DisassociateMember操作。

當您提交要求時，請使用`id`參數來指定要移除之成員帳戶的 12 位數 AWS 帳戶 ID。同時指定要套用要求的「區域」。若要移除其他區域中的帳戶，請在每個額外的區域中提交您的要求。

若要擷取要移除之成員帳戶的帳戶 ID，您可以使用 Amazon Macie API 的ListMembers操作。如果您這麼做，請考慮在要求中加入`onlyAssociated`參數來篩選結果。如果您將此參數的值設定為`true`，Macie 會傳回一個`members`陣列，該陣列僅提供目前為 Macie 成員帳戶的帳戶的詳細資訊。

若要使用移除 Macie 成員帳戶 AWS CLI，請執行解除關聯成員命令。使用`region`參數可指定要移除帳戶的「區域」。使用`id`參數指定要移除之成員帳戶的帳戶 ID。例如：

```
C:\> aws macie2 disassociate-member --region us-east-1 --id 123456789012
```

其中 *us-east-1* 是要移除帳戶的區域 (美國東部 (維吉尼亞北部) 區域)，而 *123456789012* 是要移除帳戶的帳戶識別碼。

如果您的要求成功，Macie 會傳回空白回應，而指定帳戶的狀態會`Removed`在您的帳戶清單中變更為。

為組織指定不同的 Amazon Macie 管理員帳戶

在 Amazon Macie 中整合並設定 AWS Organizations組織後， AWS Organizations 管理帳戶可以將不同的帳戶指定為組織委派的 Macie 管理員帳戶。

身為組織 AWS Organizations 管理帳戶的使用者，請確認您符合下列權限需求，然後再為組織指定不同的 Macie 管理員帳戶：

- 您必須擁有初始為組織指定 Macie 管理員帳戶所需的相同權限。您也必須被允許執行下列 AWS Organizations 動作：`organizations:DeregisterDelegatedAdministrator`。此額外動作可讓您移除目前的指定。
- 如果您的帳戶目前是 Macie 會員帳戶，則當前的 Macie 管理員必須刪除您作為 Macie 會員帳戶的帳戶。否則，您將無法訪問 Macie 操作來指定不同的管理員帳戶。指定新的管理員帳戶後，新的 Macie 管理員可以再次將您的帳戶新增為 Macie 成員帳戶。

如果您的組織使用多個 Macie AWS 區域，也請務必在組織使用 Macie 的每個區域中變更委派的 Macie 管理員帳戶。所有這些區域中委派的 Macie 管理員帳戶必須相同。如果您在中管理多個組織 AWS Organizations，也請注意，一個帳戶一次只能成為一個組織的委派 Macie 管理員帳戶。若要瞭解其他需求，請參閱搭配使用 Amazon Macie 的注意事項和建議 AWS Organizations。

> **Note**
>
> 當您為組織指定不同的 Macie 管理員帳戶時，您也會停用存取現有的統計資料、庫存資料，以及 Macie 產生並直接提供的其他資訊，同時針對組織中的帳戶執行自動敏感資料探索。新的 Macie 管理員帳戶無法訪問現有數據。如果您變更指定，而新的 Macie 管理員會為帳戶啟用自動探索功能，Macie 會在為帳戶執行自動探索時產生並維護新資料。

為您的組織指定不同的 Macie 管理員帳戶

若要為您的組織指定不同的 Macie 管理員帳戶，您可以使用 Amazon Macie 主控台或 Amazon Macie 和 API 的組合。 AWS Organizations 只有 AWS Organizations 管理帳戶的使用者可以變更其組織的指定。

Console

若要使用 Amazon Macie 主控台變更指定，請依照下列步驟執行。

若要指定不同的 Macie 管理員帳戶

1. AWS Management Console 使用您的 AWS Organizations 管理帳戶登入。
2. 使用頁面右上角的選取 AWS 區域 器，選取您要在其中變更指定的「區域」。
3. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
4. 根據目前區域中的管理帳戶是否已啟用 Macie，執行下列其中一項作業：
   - 如果未啟用 Macie，請在歡迎頁面上選擇 [開始使用]。

- 如果已啟用 Macie，請在導覽窗格中選擇 [設定]。

5. 在委派管理員下，選擇移除。若要變更指定，您必須先移除目前的指定。
6. 確認您要移除目前的指定。
7. 在「委派管理員」下，輸入 AWS 帳戶 要指定為組織新 Macie 管理員帳戶的 12 位數帳號 ID。
8. 選擇委派。

在與 AWS Organizations Macie 整合的每個其他區域中重複上述步驟。

API

若要以程式設計方式變更指定，您可以使用 Amazon Macie API 的兩個操作和 API 的一項作業。AWS Organizations 這是因為您必須在 Macie 和提交新指定 AWS Organizations 之前移除目前的指定。

若要移除目前的指定：

1. 使用馬西 API 的DisableOrganizationAdminAccount操作。針對必要`adminAccountId`參數，指定目前指定為組織之 AWS 帳戶 Macie 管理員帳戶的 12 位數帳號 ID。
2. 使用 AWS Organizations API 的DeregisterDelegatedAdministrator操作。對於`AccountId`參數，請為目前指定為組織的 Macie 管理員帳戶的帳戶指定 12 位數的帳戶 ID。此值應符合您在先前 Macie 要求中指定的帳戶 ID。對於`ServicePrincipal`參數，請指定 Macie 服務主體 (`macie.amazonaws.com`)。

移除目前的指定之後，請使用 Macie API 的EnableOrganizationAdminAccount操作來提交新指定。針對必要`adminAccountId`參數，請指定 12 位數的帳號 ID， AWS 帳戶 以指定為組織的新 Macie 管理員帳戶。

若要使用變更指定 AWS CLI，請執行 Macie API 的命disable-organization-admin-account令和 AWS Organizations API 的deregister-delegated-administrator命令。這些指令會分別移除 Macie 和 AWS Organizations目前的指定。對於`admin-account-id`和`account-id`參數，請指定 AWS 帳戶 要移除的 12 位數帳號 ID 作為目前 Macie 管理員帳戶。使用`region`參數可指定移除套用至的「區域」。例如：

```
C:\> aws macie2 disable-organization-admin-account --region us-east-1 --admin-
account-id 111122223333 && aws organizations deregister-delegated-administrator --
region us-east-1 --account-id 111122223333 --service-principal macie.amazonaws.com
```

其中：

- *us-east-1* 是移除適用於美國東部 (維吉尼亞北部) 區域的區域。
- *111122223333* 是該帳戶的帳戶識別碼，以便以 Macie 系統管理員帳戶身分移除。
- macie.amazonaws.com是馬西埃服務主體。

移除目前的指定之後，請執行 Macie API 的指enable-organization-admin-account令來提交新指定。對於admin-account-id參數，請指定 AWS 帳戶 要指定為組織的新 Macie 管理員帳戶的 12 位數帳號 ID。使用region參數指定要套用指定的「區域」。例如：

```
C:\> aws macie2 enable-organization-admin-account --region us-east-1 --admin-
account-id 444455556666
```

其中 *us-east-1* 是指定套用至的區域 (美國東部 (維吉尼亞北部) 區域)，而 *444455556666* 是要指定為新 Macie 管理員帳戶之帳戶的帳戶識別碼。

禁用 Amazon Macie 集成 AWS Organizations

組 AWS Organizations 織與 Amazon Macie 整合後， AWS Organizations 管理帳戶隨後可以停用整合。身為 AWS Organizations 管理帳戶的使用者，您可以在 AWS Organizations中停用 Macie 的受信任服務存取來執行此操作。

當您停用 Macie 的受信任服務存取時，會發生下列情況：

- Macie 失去了它作為一個值得信賴的服務的地位 AWS Organizations.
- 組織的 Macie 管理員帳戶無法存取所有 Macie 成員帳戶的所有 Macie 設定、資料和資源。 AWS 區域
- 所有 Macie 會員帳戶都成為獨立的 Macie 帳戶。如果已為一或多個區域中的成員帳戶啟用 Macie，Macie 會繼續為這些區域中的帳戶啟用。不過，該帳戶不再與任何地區的 Macie 管理員帳戶相關聯。此外，在為帳戶執行自動化敏感資料探索時，帳戶無法存取 Macie 產生並直接提供的統計資料、庫存資料和其他資訊。

如需停用受信任服務存取之結果的其他資訊，請參閱《使用AWS Organizations 者指南》 AWS 服務中的「 AWS Organizations 與其他」搭配使用。

停用 Macie 的信任服務存取

若要停用受信任的服務存取權，您可以使用 AWS Organizations 主控台或 AWS Organizations API。只有 AWS Organizations 管理帳戶的使用者可以停用 Macie 的受信任服務存取。如需有關所需權限的詳細資訊，請參閱《AWS Organizations 使用指南》中的停用受信任存取所需的權限。

停用信任的服務存取之前，請選擇性地與委派的 Macie 系統管理員合作，讓組織暫停或停用成員帳戶的 Macie，並清除這些帳戶的 Macie 資源。

Console

若要使用 AWS Organizations 主控台停用受信任的服務存取，請依照下列步驟執行。

若要停用受信任的服務存取

1. AWS Management Console 使用您的 AWS Organizations 管理帳戶登入。
2. 開啟主 AWS Organizations 控台，網址為 https://console.aws.amazon.com/organizations/。
3. 在導覽窗格中，選擇服務。
4. 在「整合式服務」下，選擇 Amazon Macie。
5. 選擇停用受信任的存取。
6. 確認您要停用受信任的存取。

API

若要以程式設計方式停用受信任的服務存取，請使用 AWS Organizations API 的停用AWSServiceAccess作業。對於`ServicePrincipal`參數，請指定 Macie 服務主體 (`macie.amazonaws.com`)。

若要使用 AWS Command Line Interface (AWS CLI) 停用受信任的服務存取，請執行 AWS Organizations API 的disable-aws-service-access命令。對於`service-principal`參數，請指定 Macie 服務主體 (`macie.amazonaws.com`)。例如：

```
C:\> aws organizations disable-aws-service-access --service-principal
 macie.amazonaws.com
```

通過邀請管理 Amazon Macie 帳戶

您可以透過兩種方式集中管理多個 Amazon Macie 帳戶，方法是將 Macie 與AWS Organizations會員資格邀請整合。如果您使用會員邀請，指定的 Macie 管理員可以管理多達 1,000 個帳戶的 Macie。管

理員還可以存取 Amazon Simple Storage Service (Amazon S3) 庫存資料，並探索帳戶擁有的 S3 儲存貯體中的敏感資料。如需有關管理員可執行之工作的詳細資訊，請參閱了解 Amazon Macie 管理員和會員帳戶之間的關係。

在基於邀請的組織中，您可以通過在 Macie 中發送和接受會員邀請來相互關聯 Macie 帳戶。如果您傳送邀請，且其他帳戶已接受該邀請，則您會成為另一個帳戶的 Macie 管理員，而另一個帳戶會變成組織中的成員帳戶。如果您收到並接受邀請，您的帳戶將成為會員帳戶，而 Macie 管理員可以存取您帳戶的某些 Macie 設定、資料和資源。

> **Tip**
>
> 如果您在 Macie 中建立以邀請為基礎的組織，您可以隨後轉換為使用。AWS Organizations您也可以同時使用這兩種方法來管理多個 Macie 帳戶。例如，如果您的AWS環境包含測試帳戶，則可以從組織中排除帳戶，AWS Organizations並透過邀請分別管理這些帳戶。

本節中的主題說明如何建立和參與以邀請為基礎的組織，以及如何為組織執行各種管理工作。

主題

- Amazon Macie 中以邀請為基礎的組織的注意事項和建議
- 在 Amazon Macie 中建立和管理以邀請為基礎的組織
- 查看以邀請為基礎的組織的 Amazon Macie 帳戶
- 為以邀請為基礎的組織指定不同的 Amazon Macie 管理員帳戶
- 在 Amazon Macie 的邀請型組織中管理您的會員資格

Amazon Macie 中以邀請為基礎的組織的注意事項和建議

在 Amazon Macie 中建立或開始管理以邀請為基礎的組織之前，請考慮下列需求和建議。還要確保您了解 Macie 管理員和成員帳戶之間的關係。

主題

- 選擇一個 Macie 管理員帳戶
- 發送邀請和管理 Macie 成員帳戶
- 回應及管理會員邀請
- 過渡到 AWS Organizations

選擇一個 Macie 管理員帳戶

當您決定哪個帳戶應該是組織的 Macie 管理員帳戶時，請謹記下列事項：

- 一個組織只能有一個 Macie 管理員帳戶。
- 一個帳戶不能同時是 Macie 管理員和會員帳戶。
- 馬西是一個區域服務。這表示 Macie 管理員帳戶與成員帳戶之間的關聯是區域 — 關聯只存在於中傳送邀請並接受 AWS 區域 的關聯性。例如，如果 Macie 管理員在美國東部 (維吉尼亞北部) 區域傳送邀請，且接受這些邀請，Macie 管理員只能管理該區域中的成員帳戶。
- 若要集中管理多個 Macie 帳戶 AWS 區域，Macie 管理員必須登入組織目前使用或計劃使用 Macie 的每個區域，並將邀請傳送至每個區域中的適當帳戶。如需目前可使用 Macie 的區域清單，請參閱 AWS 一般參考
- 一個會員帳戶一次只能與一個 Macie 管理員帳戶關聯。如果您的組織在多個區域中使用 Macie，這表示這些區域中的 Macie 管理員帳戶必須相同。但是，管理員和成員帳戶必須分別在每個區域中發送和接受邀請。

如果 Macie 管理員 AWS 帳戶 已暫停、隔離或關閉，所有關聯的成員帳戶都會自動移除為成員帳戶，但 Macie 仍會繼續為這些帳戶啟用。這些帳戶成為獨立的 Macie 帳戶。如果為成員帳戶啟用了自動敏感資料探索功能，該帳戶就會停用該帳戶。這也會停用對 Macie 產生並直接提供的統計資料、庫存資料和其他資訊的存取，同時為帳戶執行自動化探索。30 天後，此數據將過期，Macie 將永久刪除它。若要在資料到期前還原對資料的存取權，請還原 Macie 管理員的資料 AWS 帳戶，然後再次使用該帳戶建立和設定組織。

發送邀請和管理 Macie 成員帳戶

身為以邀請為基礎之組織的 Macie 管理員，在傳送邀請和管理組織中的帳戶時，請記住下列事項：

- 如果您傳送邀請，相關資料可能會傳輸到各處 AWS 區域。這是因為 Macie 會使用僅在美國東部 (維吉尼亞北部) 區域運作的電子郵件驗證服務，驗證收件人帳戶的電子郵件地址。
- 您可以傳送邀請至任何作用中的帳戶 AWS 帳戶，包括尚未啟用 Macie 的帳戶。不過，若要接受或拒絕邀請，接收帳戶必須在傳送邀請的地區中啟用 Macie。
- 一個 Macie 管理員帳戶可以與每 AWS 區域個帳戶不超過 1,000 個相關聯。這包括尚未回應邀請的帳戶。如果您的帳戶符合此配額限制，您將無法新增或邀請其他帳戶，除非您移除必要的相關帳戶數目、收到必要的拒絕邀請次數或兩者的組合為止。

若要判斷目前與您的帳戶相關聯的帳戶數目，您可以使用 Amazon Macie 主控台上的「帳戶」頁面或 Amazon Macie API 的ListMembers操作。如需詳細資訊，請參閱 查看以邀請為基礎的組織的 Amazon Macie 帳戶。

- 一個帳戶一次只能與一個 Macie 管理員帳戶關聯。這表示如果某個帳戶已與另一個 Macie 管理員帳戶建立關聯，則該帳戶無法接受您的邀請。該帳戶必須先取消與其當前 Macie 管理員帳戶的關聯。
- 在以邀請為基礎的組織中，成員帳戶可隨時取消與其 Macie 管理員帳戶的關聯。如果發生這種情況，Macie 會繼續為該帳戶啟用，但該帳戶將成為獨立的 Macie 帳戶。如果成員帳戶與您的管理員帳戶斷開關聯，Macie 不會通知您。但是，該帳戶會繼續出現在您的帳戶清單中，並且狀態為「會員已辭職」。
- 如果您從組織中移除成員帳戶，Macie 會繼續為該帳戶啟用。該帳戶將成為一個獨立的 Macie 帳戶。

回應及管理會員邀請

身為邀請的收件者或以邀請為基礎的組織的成員，在回應及管理收到的邀請時，請記住下列事項：

- 在您接受邀請之前，請確定您瞭解 Macie 管理員和成員帳戶之間的關係。
- 您的帳戶一次只能與一個 Macie 管理員帳戶關聯。如果您接受邀請後想要加入其他組織 (透過邀請或透過邀請 AWS Organizations)，您必須先取消帳戶與其目前 Macie 管理員帳戶的關聯。然後，您可以加入其他組織。
- 若要接受或拒絕邀請，您必須在傳送邀請的 AWS 區域 來源中啟用 Macie。傳送邀請的帳戶無法在該地區為您啟用 Macie。拒絕邀請是選擇性的。如果您拒絕邀請，您可以在拒絕邀請後選擇性地區中停用 Macie。
- 如果您是 Macie 管理員，則無法接受成為會員帳戶的邀請 — 帳戶不能同時是 Macie 管理員和成員帳戶。若要成為會員帳戶，您必須先從目前組織中移除所有成員帳戶，以取消帳戶與其所有成員帳戶的關聯。
- 馬西是一個區域服務。如果您接受邀請，您的帳戶與 Macie 管理員帳戶之間的關聯為區域 — 關聯僅存在於中傳送邀請並接受的關聯。 AWS 區域
- 如果您在多個區域中使用 Macie，您帳戶的 Macie 管理員帳戶在所有這些區域中必須相同。不過，Macie 管理員必須在每個地區分別傳送邀請給您，而且您必須在每個地區分別接受邀請。
- 您可以隨時取消帳戶與 Macie 管理員帳戶的關聯。同樣地，您的 Macie 管理員可以隨時從其組織移除您的帳戶。如果任何一種情況：
  - Macie 會繼續為您的帳戶啟用。您的帳戶將成為一個獨立的 Macie 帳戶。

- 如果您的帳戶已啟用自動化敏感資料探索功能，就會停用該帳戶。這也會停用存取現有的統計資料、庫存資料以及 Macie 產生並直接提供的其他資訊，同時為您的帳戶執行自動化探索。您可以再次為您的帳戶啟用自動探索功能。但是，這不會恢復對現有數據的訪問權限。相反地，Macie 會在為您的帳戶執行自動化探索時產生並維護新資料。

過渡到 AWS Organizations

在 Macie 中建立以邀請為基礎的組織之後，您可以轉換為改用。 AWS Organizations 若要簡化轉換，建議您將現有的、以邀請為基礎的管理員帳戶指定為中組織的 Macie 管理員帳戶。 AWS Organizations

如果您這麼做，所有目前關聯的成員帳戶都會繼續成為成員。如果成員帳戶是中組織的一部分 AWS Organizations，則帳戶的關聯會自動從「按邀請」變更為 Macie AWS Organizations中的「Via」。如果成員帳戶不屬於中組織的一部分 AWS Organizations，則該帳戶的關聯仍然是「按邀請」。在這兩種情況下，帳戶仍會繼續與 Macie 管理員帳戶作為成員帳戶關聯。

我們建議使用這種方法，因為一個成員帳戶一次只能與一個 Macie 管理員帳戶建立關聯。如果您指定不同的帳戶作為中組織的 Macie 管理員帳戶 AWS Organizations，指定的管理員將無法透過邀請來管理已與另一個 Macie 管理員帳戶相關聯的帳戶。每個成員帳戶必須先取消與其目前、以邀請為基礎的管理員帳戶的關聯。只有這樣， AWS Organizations 組織的 Macie 管理員才能將成員帳戶新增至其組織，並開始管理該帳戶的 Macie。

在您將 Macie 與 Macie 整合 AWS Organizations 並設定您的組織之後，您可以選擇性地為組織指定不同的 Macie 管理員帳戶。您也可以繼續使用邀請來關聯和管理不屬於您組織的成員帳戶 AWS Organizations。

如需有關將 Macie 與整合的資訊 AWS Organizations，請參閱管理亞馬遜 Macie 帳戶 AWS Organizations。

在 Amazon Macie 中建立和管理以邀請為基礎的組織

若要在 Amazon Macie 中建立以邀請為基礎的組織，請先決定要做為該組織的 Macie 管理員帳戶的帳戶。然後，您可以使用該帳戶來新增成員帳戶 — 您會傳送成員邀請給其他帳戶 AWS 帳戶，邀請這些帳戶以目前的 Macie 成員帳戶的身分加入組織。 AWS 區域若要在多個區域中建立組織，請從其他帳戶目前使用或計劃使用 Macie 的每個區域傳送成員資格邀請。

當帳戶接受邀請時，它會成為與適用區域中的 Macie 管理員帳戶相關聯的 Macie 成員帳戶。然後，Macie 管理員帳戶可以訪問該區域中成員帳戶的某些 Macie 設置，數據和資源。

身為受邀組織的 Macie 管理員，您可以檢閱 Amazon Simple Storage Service (Amazon S3) 庫存資料和成員帳戶的政策發現項目。您也可以啟用自動化敏感資料探索，並執行敏感資料探索任務，以偵測成員帳戶所擁有的 S3 儲存貯體中的敏感資料。如需可執行之工作的詳細清單，請參閱了解 Amazon Macie 管理員和會員帳戶之間的關係。

根據預設，Macie 可讓您檢視整體組織的相關資料和資源。您也可以向下鑽研以複查組織中個別帳戶的資料與資源。例如，如果您使用摘要儀表板來評估組織的 Amazon S3 安全狀態，則可以按帳戶篩選資料。同樣地，如果您監控預估的使用成本，則可以存取個別成員帳戶的估計費用明細。

除了系統管理員和成員帳戶通用的工作之外，您還可以為組織集中執行各種管理工作。在執行這些工作之前，最好先檢閱在 Macie 中管理以邀請為基礎的組織的考量和建議。

任務

- 將 Amazon Macie 成員帳戶添加到以邀請為基礎的組織
- 在基於邀請的組織中暫停 Amazon Macie 的成員帳戶
- 從以邀請為基礎的組織中移除 Amazon Macie 成員帳戶
- 刪除與其他帳戶的關聯

將 Amazon Macie 成員帳戶添加到以邀請為基礎的組織

身為以邀請為基礎之組織的 Macie 管理員，您可以執行兩個主要步驟，將成員帳戶新增至組織：

1. 在 Macie 中將帳戶新增至您的帳戶清單。這會將帳戶與您的帳戶相關聯。
2. 向帳戶發送會員邀請。

當帳戶接受邀請時，該帳戶就會成為您組織中的成員帳戶。

步驟 1：新增帳戶

若要將一個或多個帳戶新增至您的帳戶庫存，您可以使用 Amazon Macie 主控台或 Amazon Macie API。

Console

使用 Amazon Macie 主控台，您可以一次新增一個帳戶，或透過上傳逗號分隔值 (CSV) 檔案同時新增多個帳戶。請依照下列步驟使用主控台新增一或多個帳戶。

若要新增一個帳號

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 使用頁面右上角的選取 AWS 區域 器，選取您要在其中新增帳戶的地區。
3. 在導覽窗格中，選擇帳戶。[帳戶] 頁面隨即開啟，並顯示目前與您帳戶相關聯的帳戶表格。
4. 選擇 Add accounts (新增帳戶)。
5. 在「輸入帳戶詳細資訊」區段中，選擇「新增帳戶」 然後執行下列動作：
   - 在帳戶 ID 中，輸入 AWS 帳戶 要新增的 12 位數帳號 ID。
   - 在「電子郵件地址」中，輸入 AWS 帳戶 要新增的電子郵件地址。
6. 選擇新增。
7. 請選擇頁面最下方的 Next (下一頁)。

Macie 將該帳戶添加到您的帳戶庫存。帳戶類型為 [依邀請]，其狀態為 [已建立]。在您要新增帳戶的每個其他區域中，重複上述步驟。

若要新增多個帳戶

1. 透過使用文字編輯器，建立 CSV 檔案，如下所示：
   a. 將下列標頭新增為檔案的第一行：`Account ID,Email`
   b. 對於每個帳戶，請建立一個新行，其中包含要新增的 12 位數帳號 ID AWS 帳戶 以及該帳戶的電子郵件地址。以逗號分隔項目，例如：`111111111111,janedoe@example.com`

      電子郵件地址必須與相關聯的電子郵件地址相符 AWS 帳戶。
   c. 確認檔案內容的格式如下列範例所示，其中包含三個帳戶的必要標頭和資訊：

```
Account ID,Email
111111111111,janedoe@example.com
222222222222,jorgesouza@example.com
333333333333,lijuan@example.com
```

   d. 將文件保存在計算機上。
2. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
3. 使用頁面右上角的選取 AWS 區域 器，選取您要在其中新增帳戶的地區。
4. 在導覽窗格中，選擇帳戶。[帳戶] 頁面隨即開啟，並顯示目前與您帳戶相關聯的帳戶表格。
5. 選擇 Add accounts (新增帳戶)。

6. 在 [輸入帳戶詳細資料] 區段中，選擇 [上傳清單 (CSV)]。
7. 選擇 [瀏覽]，然後選取您在步驟 1 中建立的 CSV 檔案。
8. 選擇 Add accounts (新增帳戶)。
9. 請選擇頁面最下方的 Next (下一頁)。

Macie 將帳戶添加到您的帳戶庫存。他們的類型為「通過邀請」，其狀態為「已創建」。在您要新增帳戶的每個其他區域中，重複步驟 3 到 8。

API

若要以程式設計方式新增一或多個帳戶，請使用 Amazon Macie API 的CreateMember操作。當您提交要求時，請使用支援的參數，為每個 AWS 帳戶 要新增的帳戶 ID 和電子郵件地址指定 12 位數的帳戶 ID 和電子郵件地址。同時指定要套用要求的「區域」。若要在其他區域中新增帳戶，請在每個額外的區域中提交請求。

若要使用 AWS Command Line Interface (AWS CLI) 新增帳戶，請執行建立成員命令。使用`region`參數可指定要在其中新增帳戶的「區域」。使用`account`參數來指定每個 AWS 帳戶 要新增的帳戶 ID 和電子郵件地址。例如：

```
C:\> aws macie2 create-member --region us-east-1 --account={\"accountId\":
\"111111111111\",\"email\":\"janedoe@example.com\"}
```

```
## us-east-1 ############ (#### (######) ##)##account##################
(111111111111) ####### (janedoe@example.com)#
```

如果您的`Created`請求成功，Macie 會將每個帳戶新增至您的帳戶庫存，其狀態為，您會收到類似下列內容的輸出：

```
{
    "arn": "arn:aws:macie2:us-east-1:123456789012:member/111111111111"
}
```

其中`arn`是為了您的帳戶和您新增的帳戶之間的關聯而建立的資源的 Amazon 資源名稱 (ARN)。在此範例中，`123456789012`是建立關聯之帳戶的帳戶 ID，也`111111111111`是新增之帳戶的帳戶 ID。

步驟 2：向帳戶發送會員邀請

將帳戶新增至帳戶詳細目錄後，您可以邀請該帳戶以 Macie 成員帳戶的身分加入您的組織。要做到這一點，發送會員邀請到該帳戶。當您傳送邀請時，如果帳戶已啟用 Macie，則收件者帳戶的 Amazon Macie 主控台會顯示帳戶徽章和通知。Macie 還為帳戶創建一個 AWS Health 事件。

根據您是使用 Amazon Macie 主控台還是 API 傳送邀請，Macie 也會將邀請傳送至您在新增帳戶時為收件者帳戶指定的電子郵件地址。電子郵件訊息表示您想要成為其帳戶的 Macie 管理員，其中包含您 AWS 帳戶 和收件者的 AWS 帳戶帳戶 ID。訊息也會說明如何存取邀請。您可以選擇性地將自訂文字新增至郵件。

要向一個或多個帳戶發送會員邀請，您可以使用 Amazon Macie 控制台或 Amazon Macie API。

Console

請依照下列步驟使用 Amazon Macie 主控台傳送會員邀請。

傳送會員邀請

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 使用頁面右上角的選取 AWS 區域 器，選取您要傳送邀請的地區。
3. 在導覽窗格中，選擇帳戶。[帳戶] 頁面隨即開啟，並顯示目前與您帳戶相關聯的帳戶表格。
4. 在「帳戶」表格中，針對您要傳送邀請的每個帳戶選取核取方塊。

   > **Tip**
   >
   > 若要更輕鬆地識別您新增且尚未傳送邀請的帳戶，您可以篩選表格。若要執行此操作，請將游標置於表格上方的篩選方塊中，然後選擇 [狀態]。然後選擇「狀態 = 已建立」。

5. 在 [動作] 功能表上，選擇 [邀請]。
6. (選擇性) 在「訊息」方塊中，輸入您要包含在包含邀請的電子郵件訊息中的任何自訂文字。文字最多可包含 80 個英數字元。
7. 選擇 Invite (邀請)。

若要以其他方式傳送邀請 AWS 區域，請在其他每個區域中重複上述步驟。

傳送邀請後，收件者帳戶的狀態會變更為帳號清單中的 [正在進行中的電子郵件驗證]。如果 Macie 可以驗證帳戶的電子郵件地址，該帳戶的狀態隨後會變更為「已邀請」。如果 Macie 無法驗證地

址，則帳戶的狀態變更為電子郵件驗證失敗。如果發生這種情況，請與帳戶擁有者合作以取得正確的電子郵件地址。然後刪除帳戶之間的關聯，再次新增帳戶，然後再次傳送邀請。

當收件者接受邀請時，收件者帳戶的狀態會在您的帳戶庫存中變更為 [已啟用]。如果收件人拒絕邀請，收件人的帳戶就會與您的帳戶中斷連結，並從您的帳戶清單中移除。

API

若要以程式設計方式傳送邀請，請使用 Amazon Macie API 的CreateInvitations操作。當您提交要求時，請使用支援的參數，為每個 AWS 帳戶 要傳送邀請的帳戶指定 12 位數的帳戶 ID。帳戶 ID 必須與您帳戶清單中帳戶的帳戶 ID 相符。否則會發生錯誤。還要指定要從中發送邀請的地區。若要從其他區域傳送邀請，請在每個額外的區域中提交要求。

在您的要求中，您也可以指定是否要以電子郵件訊息的形式傳送邀請，以及是否要在該郵件中包含自訂文字。如果您選擇傳送電子郵件訊息，Macie 會在您將帳戶新增至帳戶清單時，將邀請傳送至您為帳戶指定的電子郵件地址。若要以電子郵件訊息的形式傳送邀請，請省略`disableEmailNotification`參數或將參數值設定為`false`。(預設值為 `false`。) 若要將自訂文字新增至郵件，請使用`message`參數指定要加入的文字。文字最多可包含 80 個英數字元。

若要使用傳送邀請 AWS CLI，請執行建立邀請指令。使用`region`參數可指定要從中傳送邀請的「地區」。使用`account-ids`參數可指定每個 AWS 帳戶 要傳送邀請的帳戶 ID。例如：

```
C:\> aws macie2 create-invitations --region us-east-1 --account-
ids=[\"111111111111\",\"222222222222\",\"333333333333\"]
```

其中 *us-east-1* 是要從美國東部 (維吉尼亞北部) 區域 (美國東部 (維吉尼亞北部) 區域傳送邀請的區域，而`account-ids`參數會指定要傳送邀請的三個帳戶的帳戶 ID。若要以電子郵件訊息的形式傳送邀請，也請加入`no-disable-email-notification`參數，並選擇性地加入`message`參數，以指定要新增至郵件的自訂文字。

傳送邀請後，每個收件者帳戶的狀態都會變更為`EmailVerificationInProgress`。如果 Macie 可以驗證帳戶的電子郵件地址，則該帳戶的狀態隨後會變更為`Invited`。如果 Macie 無法驗證地址，則帳戶的狀態會變更為`EmailVerificationFailed`。如果發生這種情況，請與帳戶擁有者合作以取得正確的地址。然後刪除帳戶之間的關聯，再次新增帳戶，然後再次傳送邀請。

當收件人接受邀請時，收件人帳戶的狀態會`Enabled`在您的帳戶庫存中變更為。如果收件人拒絕邀請，收件人的帳戶就會與您的帳戶中斷連結，並從您的帳戶清單中移除。

在基於邀請的組織中暫停 Amazon Macie 的成員帳戶

身為組織的 Macie 管理員，您可以在組織中個別成員帳戶 AWS 區域 的特定帳戶中暫停 Macie。但請注意，暫停會員帳戶後，您將無法重新啟用 Macie。只有該帳戶的使用者可以隨後重新啟用該帳戶的 Macie。

當您暫停 Macie 的會員帳戶時：

- Macie 會失去對該區域中帳戶 Amazon S3 資料的中繼資料的存取權，並停止提供相關中繼資料。
- Macie 停止執行該地區帳戶的所有活動。這包括監控 S3 儲存貯體的安全性和存取控制、執行自動化敏感資料探索，以及執行目前正在進行的敏感資料探索任務。
- Macie 會取消區域中帳戶建立的所有敏感資料探索工作。工作取消後無法繼續或重新啟動。如果您建立工作來分析成員帳戶所擁有的資料，Macie 不會取消這些工作。相反地，工作會略過帳戶所擁有的資源。

暫停帳戶時，Macie 會保留適用區域中帳戶的 Macie 工作階段識別碼、設定和資源。例如，帳戶的發現項目會保持完整，最多 90 天不受影響。在適用地區使用 Macie 時，該帳戶不會收取任何費用，而 Macie 在該地區的帳戶被停權。

在邀請型組織中暫停成員帳戶的 Macie

若要暫停以邀請為基礎的組織中的成員帳戶 Macie，您可以使用 Amazon Macie 主控台或 Amazon Macie API。

Console

請按照以下步驟使用亞馬遜 Macie 控制台暫停會員帳戶的 Macie。

暫停會員帳戶的 Macie

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 使用頁面右上角的選取 AWS 區域 器，選取您要暫停成員帳戶 Macie 的區域。
3. 在導覽窗格中，選擇帳戶。[帳戶] 頁面隨即開啟，並顯示目前與您帳戶相關聯的帳戶表格。
4. 在「帳戶」表中，選取您要暫停之帳戶的核取方塊。
5. 在 [動作] 功能表上，選擇 [暫停 Macie]。
6. 確認您要暫停所選帳戶的 Macie。

確認停權後，帳戶詳細目錄中的帳戶狀態會變更為「已暫停 (已暫停)」。

在您要暫停帳戶 Macie 的每個其他區域中，重複上述步驟。

API

要以編程方式暫停成員帳戶的 Macie，請使用 Amazon Macie API 的UpdateMemberSession操作。當您提交請求時，請使用id參數來指定您要暫停 Macie AWS 帳戶 的 12 位數帳戶 ID。對於status參數，請指定PAUSED為 Macie 帳戶的新狀態。同時指定要套用要求的「區域」。要在其他區域暫停 Macie，請在每個額外的區域中提交您的請求。

要檢索會員帳戶的帳戶 ID，您可以使用 Amazon Macie API 的ListMembers操作。如果您這麼做，請考慮在要求中加入onlyAssociated參數來篩選結果。如果您將此參數的值設定為true，Macie 會傳回一個members陣列，其中僅提供目前為您管理員帳戶之成員帳戶的帳戶的詳細資訊。

若要使用暫停成員帳戶的 Macie AWS CLI，請執行命update-member-session令。使用region參數可指定要在其中暫停 Macie 的「區域」，並使用id參數指定帳戶的帳戶 ID，以便暫停 Macie。針對 status 參數，請指定 PAUSED。例如：

```
C:\> aws macie2 update-member-session --region us-east-1 --id 123456789012 --status
 PAUSED
```

其中 *us-east-1* 是要暫停 Macie (美國東部 (維吉尼亞北部) 區域) 的區域，*123456789012* 是要暫停 Macie 之帳戶的帳戶識別碼，而且是該帳戶的新狀態 Macie。PAUSED

如果您的要求成功，Macie 會傳回空白回應，而指定帳戶的狀態會Paused在您的帳戶清單中變更為。

從以邀請為基礎的組織中移除 Amazon Macie 成員帳戶

身為 Macie 管理員，您可以從組織中移除成員帳戶。您可以通過取消與 Macie 管理員帳戶的帳戶關聯來完成此操作。

如果您移除成員帳戶，Macie 會繼續啟用該帳戶，且該帳戶會繼續顯示在您的帳戶清單中。但是，該帳戶將成為獨立的 Macie 帳戶。當您移除帳戶時，Macie 不會通知帳戶擁有者。因此，請考慮連絡帳戶擁有者，以確保他們開始管理其帳戶的設定和資源。

當您移除成員帳戶時，您將無法存取該帳戶的所有 Macie 設定、資源和資料。這包括帳戶擁有之 S3 儲存貯體的政策發現項目和中繼資料。此外，您無法再使用 Macie 探索帳戶擁有的 S3 儲存貯體中的敏感資料。如果您已建立敏感資料探索工作來執行此操作，則工作會略過帳戶擁有的值區。如果您為帳戶啟用了自動化敏感資料探索功能，您和帳戶在執行帳戶的自動化探索時，無法存取 Macie 產生並直接提供的統計資料、庫存資料和其他資訊。

移除成員帳戶後，您隨後可以透過傳送新的邀請至該帳戶，將其再次新增至您的組織。如果帳戶接受新邀請，且您在 30 天內為帳戶啟用自動化敏感資料探索功能，您也會重新取得對 Macie 先前產生並直接提供的資料和資訊的存取權，同時為該帳戶執行自動探索。

如果您移除了會員帳號，但不打算再次新增該帳戶，您可以將其從您的帳戶清單中完全移除。如要瞭解如何作業，請參閱刪除與其他帳戶的關聯。

若要從以邀請為基礎的組織中移除成員帳戶

若要從組織中移除成員帳戶，您可以使用 Amazon Macie 主控台或 Amazon Macie API。

Console

請依照下列步驟使用 Amazon Macie 主控台移除會員帳戶。

移除成員帳戶

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 使用頁面右上角的選取 AWS 區域 器，選取您要移除成員帳戶的地區。
3. 在導覽窗格中，選擇帳戶。[帳戶] 頁面隨即開啟，並顯示目前與您帳戶相關聯的帳戶表格。
4. 在「帳戶」表中，選取您要移除之帳戶的核取方塊。
5. 在 [動作] 功能表上，選擇 [取消帳號關聯]。
6. 確認您要移除選取的帳戶作為成員帳戶。

確認您的選擇後，帳戶詳細目錄中的帳戶狀態會變更為「已移除 (已取消關聯)」。

在您要移除成員帳戶的其他每個區域中，重複上述步驟。

API

若要以程式設計方式移除成員帳戶，請使用 Amazon Macie API 的DisassociateMember操作。當您提交要求時，請使用`id`參數來指定要移除之成員帳戶的 12 位數 AWS 帳戶 ID。同時指定要套用要求的「區域」。若要移除其他區域中的帳戶，請在每個額外的區域中提交您的要求。

若要擷取要移除之帳戶的帳戶識別碼，您可以使用 Amazon Macie API 的ListMembers操作。如果您這麼做，請考慮在要求中加入`onlyAssociated`參數來篩選結果。如果您將此參數的值設定為`true`，Macie 會傳回一個`members`陣列，其中僅提供目前為您帳戶成員帳戶之帳戶的帳戶的詳細資訊。

若要使用移除成員帳戶 AWS CLI，請執行取消關聯成員命令。使用`region`參數可指定要在其中移除帳戶的「區域」。使用`id`參數可指定要移除之帳戶的帳戶 ID。例如：

```
C:\> aws macie2 disassociate-member --region us-east-1 --id 123456789012
```

其中 *us-east-1* 是要移除帳戶的區域 (美國東部 (維吉尼亞北部) 區域)，而 *123456789012* 是要移除帳戶的帳戶識別碼。

如果您的要求成功，Macie 會傳回空白回應，而指定帳戶的狀態會Removed在您的帳戶清單中變更為。

刪除與其他帳戶的關聯

將帳戶新增至帳戶詳細目錄後，您可以刪除帳戶與其他帳戶之間的關聯。您可以為庫存中的任何帳戶執行此操作，除了：

- 屬於您組織中的一部分的帳戶 AWS Organizations。這種類型的關聯是通過 AWS Organizations 不 Macie 來控制的。
- 接受加入組織的 Macie 成員資格邀請的成員帳戶。在這種情況下，您必須先移除成員帳戶，才能刪除關聯。

當您刪除關聯時，Macie 會從您的帳戶庫存中移除該帳戶。如果您想要隨後還原關聯性，則必須再次新增該帳戶，就好像它是一個全新的帳戶一樣。

若要刪除與其他帳號的關聯

要刪除您的帳戶和其他帳戶之間的關聯，您可以使用 Amazon Macie 控制台或 Amazon Macie API。

Console

若要使用 Amazon Macie 主控台刪除與其他帳戶的關聯，請按照下列步驟操作。

刪除關聯

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 使用頁面右上角的選取 AWS 區域 器，選取您要刪除關聯的「區域」。
3. 在導覽窗格中，選擇帳戶。[帳戶] 頁面隨即開啟，並顯示目前與您帳戶相關聯的帳戶表格。
4. 在「帳戶」表中，選取您要刪除其關聯之帳戶的核取方塊。
5. 在操作功能表上，選擇刪除。
6. 確認您要刪除選取的關聯。

在您要刪除關聯的每個其他「區域」中重複上述步驟。

API

若要以程式設計方式刪除與其他帳戶的關聯，請使用 Amazon Macie API 的DeleteMember操作。當您提交請求時，請使用id參數來指定要刪除與之關聯的 12 位數帳戶 ID。 AWS 帳戶 同時指定要套用要求的「區域」。若要刪除其他區域中的關聯，請在每個額外的區域中提交您的請求。

若要擷取帳戶的帳戶識別碼，您可以使用 Amazon Macie API 的ListMembers操作。如果這樣做，請在請求中包含onlyAssociated參數，並將參數的值設定為false。如果操作成功，Macie 會返回一個members陣列，其中提供與您的帳戶相關聯的所有帳戶的詳細信息，包括當前不是成員帳戶的帳戶。

若要使用刪除與其他帳戶的關聯 AWS CLI，請執行刪除成員命令。使用region參數可指定要刪除關聯的「區域」，並使用id參數指定帳戶的帳戶 ID。例如：

```
C:\> aws macie2 delete-member --region us-east-1 --id 123456789012
```

其中 *us-east-1* 是要刪除與其他帳戶 (美國東部 (維吉尼亞北部) 區域關聯的區域，而 *1234567890* 12 是帳戶的帳戶識別碼。

如果您的要求成功，Macie 會傳回空白回應，而您的帳戶與其他帳戶之間的關聯也會遭到刪除。先前關聯的帳戶會從您的帳戶清單中移除。

查看以邀請為基礎的組織的 Amazon Macie 帳戶

為了協助您管理組織中的帳戶，Amazon Macie 會在您使用 Macie 的每個 AWS 區域 地方提供與您的 Macie 帳戶相關聯的帳戶清單。身為組織的 Macie 管理員，您可以使用此庫存來複查組織的帳號統計資料和詳細資訊。您還可以使用它來執行成員帳戶的某些管理任務，以及管理您的帳戶與其他帳戶之間的關係狀態。

若要檢閱以邀請為基礎之組織的帳戶

若要檢閱組織中的帳戶，您可以使用 Amazon Macie 主控台或 Amazon Macie API。

Console

請依照下列步驟使用 Amazon Macie 主控台檢閱組織的帳戶。

若要檢閱您組織的帳戶

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。

2. 使用頁面右上角的選取 AWS 區域 器，選取您要檢閱組織帳戶的地區。
3. 在導覽窗格中，選擇帳戶。

「帳戶」頁面會開啟並顯示彙總統計資料，以及目前 AWS 區域與您的 Macie 帳戶相關聯的帳戶表格。

在 [帳戶] 頁面頂端，您會看到下列彙總統計資料。

通過 AWS Organizations

如果您是中某個組織的 Macie 管理員 AWS Organizations，Active 會報告透過與您的帳戶相關聯 AWS Organizations 且目前為組織中的 Macie 成員帳戶的帳戶總數。這些帳戶已啟用 Macie，您是帳戶的 Macie 管理員。

所有報告通過與您的帳戶關聯的帳戶總數 AWS Organizations，包括當前不是 Macie 成員帳戶的帳戶。

通過邀請

作用中報告您邀請型組織中目前為 Macie 成員帳戶的帳戶總數。這些帳戶已啟用 Macie，您是帳戶的 Macie 管理員，因為他們接受了您的成員資格邀請。

所有報告通過 Macie 邀請與您的帳戶相關聯的帳戶總數，包括尚未回應您的邀請的帳戶。

主動/全部

「作用中」會透過 AWS Organizations 或透過邀請，報告目前為您帳戶的 Macie 成員帳戶的帳戶總數。這些帳戶已啟用 Macie，您是帳戶的 Macie 管理員。

所有報告通過 AWS Organizations 或通過邀請與您的帳戶關聯的帳戶總數。這包括尚未接受您的 Macie 會員邀請的帳戶。它還包括與您的帳戶相關聯的帳戶，但目前不是 Macie 會員帳戶的帳戶。 AWS Organizations

您可以在表格中找到目前區域中每個帳戶的詳細資訊。該表包括與您的 Macie 帳戶，通過 Macie 邀請或通過相關聯的所有帳戶。 AWS Organizations

帳戶 ID

的帳戶 ID 和電子郵件地址 AWS 帳戶。

名稱

的帳戶名稱 AWS 帳戶。對於透過邀請與您的帳戶相關聯的帳戶，此值通常為 N/A。

類型

透過邀請或透過邀請方式，將帳戶與您的帳戶建立關聯的方式 AWS Organizations。

狀態

您的帳戶與帳戶之間的關係狀態。對於以邀請為基礎的組織中的帳戶 (「類型」為「依邀請」)，可能的值為：

- 帳戶已暫停 — AWS 帳戶 已暫停。
- 已建立 (邀請) — 您已新增帳號，但尚未傳送會員邀請函給該帳戶。
- 電子郵件驗證失敗 — 您嘗試傳送會員邀請至帳戶，但指定的電子郵件地址對帳戶無效。
- 電子郵件驗證正在進行中 — 您已將會員邀請傳送至帳戶，而 Macie 正在處理要求。
- 已啟用 — 帳戶為成員帳戶。該帳戶已啟用 Macie，您是該帳戶的 Macie 管理員。
- 已邀請 — 您已傳送會員邀請至該帳戶，但該帳戶尚未回應您的邀請。
- 成員已辭職 — 該帳戶之前是會員帳戶。不過，帳戶會取消與您的帳戶關聯，從您的組織辭去。
- 已暫停 (已暫停) — 帳戶是會員帳戶，但 Macie 目前已暫停該帳戶。
- [停用地區] — 目前的 [區域] 已停用 AWS 帳戶。
- 已移除 (取消關聯) — 該帳戶之前是會員帳戶。但是，您將其作為會員帳戶與您的帳戶取消關聯，將其刪除。

上次狀態更新

當您或關聯帳戶最近執行了影響您帳戶之間關係的動作時。

自動化敏感資料探索

帳戶目前是否已啟用或停用自動敏感資料探索。

若要依特定欄位對表格進行排序，請選擇欄位的欄標題。若要變更排序順序，請再次選擇欄標題。若要篩選表格，請將游標置於篩選方塊中，然後新增欄位的篩選條件。若要進一步細化結果，請新增其他欄位的篩選條件。

API

若要以程式設計方式檢閱組織的帳戶，請使用 Amazon Macie API 的ListMembers操作，並指定要套用請求的區域。若要複查其他區域中的詳細資訊，請在每個額外的區域中提交您的請求。

當您提交請求時，請使用`onlyAssociated`參數來指定要包含在回應中的科目。默認情況下，Macie 僅返回有關指定區域中的成員帳戶的詳細信息，通過邀請或通過 AWS Organizations。

若要擷取所有關聯帳戶的詳細資訊，包括非成員帳戶的帳戶，請在請求中包含onlyAssociated參數，並將參數值設定為false。

若要使用 AWS Command Line Interface (AWS CLI) 檢閱組織的帳戶，請執行清單成員命令。對於only-associated參數，指定是要包含所有關聯帳戶還是僅包含成員帳戶。若只要包含成員帳戶，請省略此參數或將參數值設定為true。若要包含所有帳戶，請將此值設定為false。例如：

```
C:\> aws macie2 list-members --region us-east-1 --only-associated false
```

其中 *us-east-1* 是要求適用的區域，即美國東部 (維吉尼亞北部) 區域。

如果您的請求成功，Macie 返回一個數組members。陣列會針member對每個符合要求中指定準則的帳戶包含一個物件。在該對象中，該relationshipStatus字段指示您的帳戶與指定區域中的其他帳戶之間的關聯的當前狀態。對於以邀請為基礎的組織中的帳戶，可能的值為：

- AccountSuspended— 已 AWS 帳戶 暫停。
- Created— 您已新增帳戶，但尚未傳送會員邀請。
- EmailVerificationFailed— 您嘗試向該帳戶發送會員邀請，但指定的電子郵件地址對該帳戶無效。
- EmailVerificationInProgress— 您發送了會員邀請到該帳戶，而 Macie 正在處理該請求。
- Enabled— 該帳戶是一個會員帳戶。該帳戶已啟用 Macie，您是該帳戶的 Macie 管理員。
- Invited— 您發送了會員邀請到該帳戶，但該帳戶尚未回應您的邀請。
- Paused— 該帳戶是會員帳戶，但 Macie 目前已暫停（暫停）該帳戶。
- RegionDisabled— 目前的 [區域] 已停用 AWS 帳戶。
- Removed— 該帳戶以前是會員帳戶。但是，您將其作為會員帳戶與您的帳戶取消關聯，將其刪除。
- Resigned— 該帳戶以前是會員帳戶。不過，帳戶會取消與您的帳戶關聯，從您的組織辭去。

如需有關member物件中其他欄位的資訊，請參閱 Amazon Macie API 參考資料中的成員。

為以邀請為基礎的組織指定不同的 Amazon Macie 管理員帳戶

建立並建立以邀請為基礎的組織後，您可以變更該組織的 Amazon Macie 管理員帳戶。若要這麼做，組織的管理員和成員應該採取下列步驟：

1. 目前的 Macie 管理員可以選擇性地匯出組織使用中成員帳戶的目前庫存。這樣可以幫助您確定應該繼續成為組織一部分的成員帳戶，從而簡化了轉換。
2. 目前的 Macie 管理員會移除目前組織中的所有成員帳戶。這會取消帳戶與目前管理員帳戶的關聯。Macie 繼續為帳戶啟用，但帳戶成為獨立的 Macie 帳戶。

> **Note**
>
> 當目前的 Macie 管理員移除成員帳戶時，Macie 會自動停用帳戶的自動敏感資料探索功能。這也會停用對 Macie 產生並直接提供的統計資料、庫存資料和其他資訊的存取，同時為帳戶執行自動化探索。當轉換至新組織完成時，新的 Macie 管理員將無法存取此資料。

3. 新的 Macie 管理員會將先前的成員帳戶新增至新組織。這會將帳戶與新的管理員帳戶相關聯。
4. 每個成員帳戶都接受加入新組織的邀請。當帳戶接受邀請時，該帳戶就會成為新組織中的作用中成員帳戶。然後，新的 Macie 管理員可以訪問該帳戶的 Macie 設置，數據和資源。如果先前已為帳戶啟用自動化敏感資料探索功能，則不包括 Macie 先前在為帳戶執行自動探索時產生和直接提供的資料。相反地，如果新的 Macie 管理員啟用帳戶的自動探索功能，Macie 會產生並維護帳戶的新資料。

如果您的組織使用多個 Macie AWS 區域，請在這些區域中執行上述步驟。

要導出活躍會員帳戶的當前庫存，當前 Macie 管理員可以使用 Amazon Macie 控制台或 Amazon Macie API。使用主控台，目前的管理員可以將資料匯出為逗號分隔值 (CSV) 檔案。然後，新管理員可以使用主控台上傳 CSV 檔案，並將所有帳戶 (大量) 新增至新組織。

使用主控台匯出成員帳戶資料

1. AWS Management Console 使用目前的 Macie 管理員帳戶登入。
2. 使用頁面右上角的選取 AWS 區域 器，選取您要匯出資料的「區域」。
3. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
4. 在導覽窗格中，選擇帳戶。「帳戶」頁面會開啟，並顯示與目前 Macie 管理員帳戶相關聯的帳戶表格。
5. (選擇性) 若要篩選「帳戶」表，並僅顯示組織中目前作用中 Macie 成員帳戶的帳戶，請使用表格上方的篩選方塊來新增下列篩選條件：
   - 類型 = 邀請
   - 狀態 = 已啟用

6. 在「帳戶」表中，選取要包含在匯出資料中的每個成員帳戶的核取方塊。
7. 選擇「匯出 CSV」。
8. 指定檔案的名稱和位置。

使用 Amazon Macie API，當前的 Macie 管理員可以檢索 JSON 格式的數據。然後，新的 Macie 管理員可以使用該資料來產生帳號 ID 和電子郵件地址清單，以便新增並邀請加入新組織的帳戶。若要擷取 JSON 格式的資料，請使用 Amazon Macie API 的ListMembers操作。如果作業成功，Macie 會傳回一個`members`陣列，其中提供與管理員帳戶相關聯之所有帳戶的詳細資料。如果帳戶是目前、邀請型組織中的作用中 Macie 成員帳戶，則該帳戶的`relationshipStatus`屬性值為，且該屬`invitedAt`性會指定日期`Enabled`和時間。

在 Amazon Macie 的邀請型組織中管理您的會員資格

如果您受邀加入 Amazon Macie 中的組織，您可以選擇性地接受或拒絕邀請。在 Macie 中，組織是一組以相關帳戶的形式集中管理的帳戶。組織由一個指定的 Macie 管理員帳戶和一個或多個關聯的成員帳戶組成。

如果您接受邀請，您的帳戶就會成為組織中的成員帳戶。當您接受邀請時，傳送邀請的帳戶會成為您帳戶的 Macie 管理員帳戶 — 您將帳戶與其他帳戶建立關聯，並啟用帳戶之間的管理員與成員關係。然後，Macie 管理員帳戶可以在適用的情況下訪問您帳戶的某些 Macie 設置，數據和資源。 AWS 區域如需詳細資訊，請參閱 了解 Amazon Macie 管理員和會員帳戶之間的關係。

如果您拒絕邀請，您 Macie 帳戶的目前狀態和設定不會變更。

主題

- 回應組織的會員邀請
- 從 Amazon Macie 管理員帳戶斷開關聯

回應組織的會員邀請

當您收到加入組織的邀請時，Amazon Macie 會透過多種方式通知您。根據預設，Macie 會以電子郵件訊息的形式傳送邀請給您。馬西也創建了一個 AWS Health 事件為您 AWS 帳戶. 如果您已在傳送邀請時使用 Macie，Macie 也會在 Macie 主控台上顯示帳號徽章和通知。 AWS 區域

收到邀請後，您可以選擇性地接受或拒絕邀請。在您回應之前，請注意下列事項：

- 您一次只能成為一個組織的成員。如果您收到多個邀請，則只能接受一個邀請。或者，如果您已經是組織的成員，則必須先取消帳戶與其目前 Macie 管理員帳戶的關聯，才能加入其他組織。

- 如果您在多個地區使用 Macie，您的帳戶必須在所有這些區域中擁有相同的 Macie 管理員帳戶。Macie 管理員必須與每個區域分別傳送邀請給您，而且您必須在每個地區分別接受邀請。
- 若要接受或拒絕邀請，您必須在傳送邀請的地區中啟用 Macie。拒絕邀請是選擇性的。如果您啟用 Macie 拒絕邀請，您可以在拒絕邀請後停用「地區」中的 Macie。這有助於確保您在該地區使用 Macie 時不會產生不必要的費用。
- 如果您的帳戶啟用了自動化敏感資料探索功能，且您接受邀請，您將無法存取 Macie 產生並直接提供的統計資料、庫存資料和其他資訊，同時為您的帳戶執行自動化探索。接受邀請後，您的 Macie 管理員可以為您的帳戶啟用自動探索功能。但是，這不會恢復對現有數據的訪問權限。相反地，Macie 會在為您的帳戶執行自動化探索時產生並維護新資料。

如需其他考量，請參閱回應及管理會員邀請。

若要回應組織的成員資格邀請

若要回應會員邀請，您可以使用 Amazon Macie 主控台或 Amazon Macie API。

Console

請依照下列步驟使用 Amazon Macie 主控台回應會員邀請。

回應會員邀請

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 使用頁面右上角的選取 AWS 區域 器，選取您收到邀請的地區。
3. 如果您尚未在「地區」中啟用 Macie，請選擇「開始使用」，然後選擇「啟用 Mac ie」。您必須先啟用 Macie 才能接受或拒絕邀請。
4. 在導覽窗格中，選擇帳戶。
5. 在「管理員帳戶」下，執行下列其中一個動作：
   - 若要接受邀請，請開啟邀請旁邊的「接受」
     ( )。
     然後根據您之前是否接受其他邀請，選擇「接受邀請」或「更新」。
   - 若要拒絕邀請，請選擇邀請旁邊的 [拒絕邀請]，然後確認您要拒絕邀請。

如果您收到並希望在其他區域中回應邀請，請在其他每個區域中重複上述步驟。

API

若要以程式設計方式回應邀請，請根據您要接受還是拒絕邀請，使用 Amazon Macie API 的或DeclineInvitations操作。AcceptInvitation當您提交請求時，請務必指定邀請的寄件地區。若要在其他地區回應邀請，請在其他每個區域提交您的要求。

在要AcceptInvitation求中，使用administratorAccountId參數來指定傳送邀請的 12 位 AWS 帳戶 數帳戶 ID。使用invitationId參數可指定要接受邀請的唯一 ID。

在DeclineInvitations要求中，使用accountIds參數來指定傳送拒絕邀請的 12 位數帳戶 ID。 AWS 帳戶

要檢索 ID，您可以使用 Amazon Macie API 的ListInvitations操作。如果作業成功，Macie 會傳回一個invitations陣列，其中提供您已收到邀請的詳細資訊，包括傳送每個邀請之帳戶的帳戶 ID，以及每個邀請的唯一 ID。如果邀請函的relationshipStatus屬性值為Invited，表示您尚未回應邀請。

若要使用 AWS Command Line Interface (AWS CLI) 回應邀請，請根據您要接受還是拒絕邀請，執行接受邀請或拒絕邀請命令。使用region參數可指定邀請的寄件地區。例如：

```
C:\> aws macie2 accept-invitation --region us-east-1 --administrator-account-
id 123456789012 --invitation-id d8bdad0e203fd1242e0a4721bexample
```

其中，我們## -1 ######## (######) ########123456789012 ################ d8bdad0e 203 f d 1242e0a4721 比例是接受邀請的唯一識別碼。

如果接受邀請的請求成功，Macie 會傳回空白回應。如果拒絕邀請的請求成功，Macie 會傳回空unprocessedAccounts陣列。

拒絕邀請後，邀請會保留為您的 Macie 帳號的資源。您可以選擇性地使用DeleteInvitations作業或刪除邀 AWS CLI請指令來刪除它。

從 Amazon Macie 管理員帳戶斷開關聯

如果您接受邀請加入 Amazon Macie 中的組織，您隨後可以透過取消帳戶與目前 Macie 管理員帳戶的關聯，從組織辭職。請注意，如果您的帳戶是 AWS Organizations 組織中的成員帳戶，則無法執行此操作。若要從 AWS Organizations 組織辭職，請與您的 Macie 管理員合作，以 Macie 成員帳戶的身分移除您的帳戶。

如果您取消帳戶與其 Macie 管理員帳戶的關聯，Macie 管理員將無法存取您 Macie 帳戶的所有設定、資料和資源。這包括您擁有的 Amazon S3 資料的中繼資料和政策發現項目。這也表示管理員無法再透過執行自動化敏感資料探索或執行敏感資料探索任務來分析您的 Amazon S3 資料。

當您取消帳戶關聯時，Macie 會繼續在適用地區中為您的帳戶啟用。但是，您的帳戶將成為該地區的獨立 Macie 帳戶。您的帳戶狀態會在管理員的帳戶清單中變更為 [成員已辭職]。

取消與 Macie 管理員帳戶的關聯

要取消您的帳戶與其當前 Macie 管理員帳戶的關聯，您可以使用 Amazon Macie 控制台或 Amazon Macie API。

Console

請依照下列步驟，使用 Amazon Macie 主控台取消帳戶與其 Macie 管理員帳戶的關聯。

取消與管理員帳戶的關聯

1. 在以下位置打開 Amazon Macie 亞控制台 https://console.aws.amazon.com/macie/。
2. 使用頁面右上角的選取 AWS 區域 器，選取您要在其中取消帳戶與其管理員帳戶關聯的地區。
3. 在導覽窗格中，選擇帳戶。
4. 在 [系統管理員帳戶] 底下，關閉邀請旁的 [接受]
   ( )，
   然後選擇 [更新]。

帳戶會繼續顯示在 [帳戶] 頁面上。如果您決定重新加入組織，可以使用此頁面再次接受原始邀請。或者，您也可以拒絕並刪除邀請，這也會刪除您帳戶與其他帳戶之間的關聯。若要這麼做，請選擇 [拒絕邀請]。

如果您想要在其他區域中取消帳戶與其 Macie 管理員帳戶的關聯，請在每個其他區域中重複上述步驟。

API

若要以程式設計方式取消帳戶與其 Macie 管理員帳戶的關聯，請使用 Amazon Macie API 的DisassociateFromAdministratorAccount操作。當您提交請求時，請務必指定要求適用的地區。若要取消其他區域中帳戶的關聯，請在每個額外的區域中提交您的要求。

若要使用取消帳戶與其 Macie 管理員帳戶的關聯 AWS CLI，請執行命令。disassociate-from-administrator-account使用`region`參數可指定要在其中取消與帳戶關聯的「區域」。

如果您的要求成功，Macie 會傳回空白回應。

取消與帳號的關聯後，原始邀請函會保留為您 Macie 帳號的資源，除非您將其刪除。如果您決定重新加入組織，您可以使用此資源再次接受原始邀請。或者，您也可以使用DeleteInvitations作業或刪除邀請命 AWS CLI令來刪除邀請。如果您刪除邀請，您也會刪除帳戶與其他帳戶之間的關聯。

Amazon Macie

雲端安全是 AWS 最重視的一環。身為 AWS 的客戶，您將能從資料中心和網路架構中獲益，這些都是專為最重視安全的組織而設計的。

安全是 AWS 與您共同肩負的責任。共同責任模型將其描述為雲端的安全性和雲端中的安全性：

- 雲端本身的安全 – AWS 負責保護在 AWS 雲端 中執行 AWS 服務 的基礎設施。AWS 也提供您可安全使用的服務。第三方稽核人員會定期測試和驗證我們安全性的有效性，作為 AWS 合規計劃的一部分。若要了解適用於 Amazon Macie 的合合計計計，請參閱AWS合規計劃
- 雲端內部的安全：您的責任取決於所使用的 AWS 服務。您也必須對其他因素負責，包括資料的機密性、您公司的要求和適用法律和法規。

本文有助於您了解如何在使用 Macie 下主題 您也將了解如何使用其他AWS 服務，幫幫您監監並保護 Macie 資資資

主題

Amazon Macie 的數據保護

AWS共同責任模型適用於 Amazon Macie 中的資料保護。如此模型所述，AWS 負責保護執行所有 AWS 雲端 的全球基礎設施。您負責維護在此基礎設施上託管內容的控制權。您也必須負責您所使用 AWS 服務 的安全組態和管理任務。如需有關資料隱私權的更多相關資訊，請參閱資料隱私權常見問答集。如需有關歐洲資料保護的相關資訊，請參閱 AWS 安全性部落格上的 AWS 共同的責任模型和 GDPR 部落格文章。

基於資料保護目的，建議您使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 保護 AWS 帳戶 憑證，並設定個人使用者。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 AWS CloudTrail 設定 API 和使用者活動日誌記錄。
- 使用 AWS 加密解決方案，以及 AWS 服務 內的所有預設安全控制項。
- 使用進階的受管安全服務（例如 Amazon Macie），協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果您在透過命令列介面或 API 存取 AWS 時，需要 FIPS 140-2 驗證的加密模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的更多相關資訊，請參閱聯邦資訊處理標準 (FIPS) 140-2 概觀。

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

靜態加密

Amazon Macie 使用AWS加密解決方案安全地存放您的靜態資料。Macie 加密數據，如發現，使用 AWS 受管金鑰從AWS Key Management Service（ ）AWS KMS。

如果您停用 Macie，它會永久刪除它為您儲存或維護的所有資源，例如敏感資料探索工作、自訂資料識別碼和發現項目。

傳輸中加密

Macie 加密之間傳輸中的所有數據。AWS 服務

Amazon Macie 會分析來自 Amazon S3 的資料，並將敏感資料探索結果匯出到 S3 儲存貯體。Macie 從 S3 物件取得所需的資訊之後，就會捨棄這些資訊。

Macie 使用支持的 VPC 端點訪問 Amazon S3。AWS PrivateLink因此，Macie 和 Amazon S3 之間的流量保持在 Amazon 網絡上，並且不會通過公共互聯網。如需詳細資訊，請參閱 AWS PrivateLink。

Amazon Macie 的身份和訪問管理

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

主題

物件

您如何使用 AWS Identity and Access Management （ IAM ），具體取決於您在 Macie 中所做的工作。

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

服務管理員 — 如果您負責公司的 Macie 資源，則可能擁有對 Macie 的完全訪問權限。您的工作就是決定服務使用者應存取哪些 Macie 功能和資源。接著，您必須將請求提交給您的 IAM 管理員，來變更您服務使用者的許可。檢閱此頁面上的資訊，了解 IAM 的基本概念。若要深入瞭解貴公司如何搭配 Macie 使用 IAM，請參閱亞 Amazon Macie 如何與 AWS Identity and Access Management。

IAM 管理員 — 如果您是 IAM 管理員，可能需要瞭解如何撰寫政策來管理 Macie 存取權的詳細資訊。若要檢視可在 IAM 中使用的 Macie 身分型政策範例，請參閱。Amazon Macie 的身分型政策範例

使用身分驗證

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

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

根據您的使用者類型，您可以登入 AWS Management Console 或 AWS 存取入口網站。如需登入的詳細資訊 AWS，請參閱AWS 登入 使用者指南中的如何登入您 AWS 帳戶的。

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

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

AWS 帳戶 根使用者

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

聯合身分

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

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

對於集中式存取權管理，我們建議您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中建立使用者和群組，也可以連線並同步到自己身分識別來源中的一組使用者和群組，以便在所有應用程式 AWS 帳戶 和應用程式中使用。如需 IAM Identity Center 的詳細資訊，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 使用者是您內部的身分，具 AWS 帳戶 有單一人員或應用程式的特定許可。建議您盡可能依賴暫時憑證，而不是擁有建立長期憑證 (例如密碼和存取金鑰) 的 IAM 使用者。但是如果特定使用案例需要擁有長期憑證的 IAM 使用者，建議您輪換存取金鑰。如需更多資訊，請參閱 IAM 使用者指南中的為需要長期憑證的使用案例定期輪換存取金鑰。

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

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

IAM 角色

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

使用暫時憑證的 IAM 角色在下列情況中非常有用：

- 聯合身分使用者存取 — 如需向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並獲授予由角色定義的許可。如需有關聯合角色的相關資訊，請參閱 IAM 使用者指南中的為第三方身分提供者建立角色。如果您使用 IAM Identity Center，則需要設定許可集。為控制身分驗證後可以存取的內容，IAM Identity Center 將許可集與 IAM 中的角色相關聯。如需有關許可集的資訊，請參閱 AWS IAM Identity Center 使用者指南中的許可集。
- 暫時 IAM 使用者許可 – IAM 使用者或角色可以擔任 IAM 角色來暫時針對特定任務採用不同的許可。
- 跨帳戶存取權：您可以使用 IAM 角色，允許不同帳戶中的某人 (信任的主體) 存取您帳戶的資源。角色是授予跨帳戶存取權的主要方式。但是，對於某些策略 AWS 服務，您可以將策略直接附加到資源（而不是使用角色作為代理）。若要了解跨帳戶存取角色和以資源為基礎的政策之間的差異，請參閱 IAM 使用者指南中的 IAM 中的跨帳戶資源存取。
- 跨服務訪問 — 有些 AWS 服務 使用其他 AWS 服務功能。例如，當您在服務中進行呼叫時，該服務通常會在 Amazon EC2 中執行應用程式或將物件儲存在 Amazon Simple Storage Service (Amazon S3) 中。服務可能會使用呼叫主體的許可、使用服務角色或使用服務連結角色來執行此作業。

- 轉寄存取工作階段 (FAS) — 當您使用 IAM 使用者或角色在中執行動作時 AWS，您會被視為主體。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 會使用主體呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。只有當服務收到需要與其 AWS 服務 他資源互動才能完成的請求時，才會發出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的政策詳細資訊，請參閱《轉發存取工作階段》。
- 服務角色 – 服務角色是服務擔任的 IAM 角色，可代表您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需詳細資訊，請參閱 IAM 使用者指南中的建立角色以委派許可給 AWS 服務服務。
- 服務連結角色 — 服務連結角色是連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

- 在 Amazon EC2 上執行的應用程式 — 您可以使用 IAM 角色來管理在 EC2 執行個體上執行的應用程式以及發出 AWS CLI 或 AWS API 請求的臨時登入資料。這是在 EC2 執行個體內儲存存取金鑰的較好方式。若要將 AWS 角色指派給 EC2 執行個體並提供給其所有應用程式，請建立連接至執行個體的執行個體設定檔。執行個體設定檔包含該角色，並且可讓 EC2 執行個體上執行的程式取得暫時憑證。如需詳細資訊，請參閱 IAM 使用者指南中的利用 IAM 角色來授予許可給 Amazon EC2 執行個體上執行的應用程式。

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

使用政策管理存取權

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

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

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

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

身分型政策

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

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

資源型政策

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

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

存取控制清單 (ACL)

存取控制清單 (ACL) 可控制哪些主體 (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。

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

其他政策類型

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

- 許可界限 – 許可範圍是一種進階功能，可供您設定身分型政策能授予 IAM 實體 (IAM 使用者或角色) 的最大許可。您可以為實體設定許可界限。所產生的許可會是實體的身分型政策和其許可界限的交

集。會在 `Principal` 欄位中指定使用者或角色的資源型政策則不會受到許可界限限制。所有這類政策中的明確拒絕都會覆寫該允許。如需許可界限的詳細資訊，請參閱 IAM 使用者指南中的 IAM 實體許可界限。

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

多種政策類型

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

亞 Amazon Macie 如何與 AWS Identity and Access Management

在您使用 AWS Identity and Access Management (IAM) 管理 Amazon Macie 的存取權限之前，請先了解哪些 IAM 功能可與 Macie 搭配使用。

您可以與 Amazon Macie 一起使用的 IAM 功能

IAM 功能	馬西支持
身分型政策	是
資源型政策	否
政策動作	是
政策資源	是
政策條件索引鍵	是
存取控制清單 (ACL)	否

IAM 功能	馬西支持
以屬性為基礎的存取控制 (ABAC) — 策略中的標籤	是
臨時憑證	是
轉送存取工作階段 (FAS)	是
服務角色	否
服務連結角色	是

有關 Macie 和其他如何使 AWS 服務 用大多數 IAM 功能的高級視圖 AWS 服務 ，請參閱 IAM 使用者指南中的 IAM。

Amazon Macie 的基於身份的政策

支援身分型政策	是

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

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

Macie 支援以身分識別為基礎的原則。如需範例，請參閱 Amazon Macie 的身分型政策範例。

Amazon Macie 內基於資源的政策

支援以資源基礎的政策	否

資源型政策是附加到資源的 JSON 政策文件。資源型政策的最常見範例是 IAM 角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源

的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定主體。主參與者可以包括帳戶、使用者、角色、同盟使用者或。 AWS 服務

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

Macie 不支援以資源為基礎的政策。也就是說，您無法將策略直接附加到 Macie 資源。

Amazon Macie 的政策行動

支援政策動作	是

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

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

政策會使用動作來授予執行相關聯動作的許可。

Macie 的原則動作會在動作之前使用下列前置詞：

```
macie2
```

例如，若要授與某人存取 Macie 提供的所有受管資料識別碼相關資訊的權限，這是與 Amazon Macie API `ListManagedDataIdentifiers` 操作相對應的動作，請在其政策中包含`macie2:ListManagedDataIdentifiers`動作：

```
"Action": "macie2:ListManagedDataIdentifiers"
```

若要在單一陳述式中指定多個動作，請用逗號分隔。例如：

```
"Action": [
      "macie2:ListManagedDataIdentifiers",
```

```
      "macie2:ListCustomDataIdentifiers"
]
```

您也可以使用萬用字元 (*) 指定多個動作。例如，若要指定開頭是 List 文字的所有動作，請包含以下動作：

```
"Action": "macie2:List*"
```

但是，根據最佳實務，您應該定義遵循「最低權限」原則的政策。換句話說，您應建立其中只包含執行特定任務所需許可的政策。

如需 Macie 動作的清單，請參閱服務授權參考資料中的 Amazon Macie 定義的動作。如需指定 Macie 動作的策略範例，請參閱Amazon Macie 的身分型政策範例。

Amazon Macie 的政策資源

支援政策資源	是

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

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

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

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

Macie 定義了以下資源類型：

- 允許清單
- 自訂資料識別碼
- 篩選或抑制規則，也稱為發現項目篩選
- 成員帳戶
- 敏感性資料探索工作，也稱為分類工作

您可以使用 ARN 在策略中指定這些類型的資源。

例如，若要為具有工作識別碼為工作識別碼 3ce05dbb7ec5505 def334104 範例的敏感資料探索工作建立原則，您可以使用下列 ARN：

```
"Resource": "arn:aws:macie2:*:*:classification-job/3ce05dbb7ec5505def334104bexample"
```

或者，若要為特定帳戶指定所有敏感資料探索工作，請使用萬用字元 (*)：

```
"Resource": "arn:aws:macie2:*:123456789012:classification-job/*"
```

其中 *123456789012* 是建立工作的帳戶識別碼。 AWS 帳戶 不過，最佳作法是建立遵循最低權限原則的原則。換句話說，您應該建立只包含在特定資源上執行特定工作所需的權限的策略。

某些 Macie 動作可套用至多個資源。例如，`macie2:BatchGetCustomDataIdentifiers`動作可擷取多個自訂資料識別碼的詳細資訊。在這些情況下，主參與者必須具有存取動作適用於之所有資源的權限。若要在單一陳述式中指定多項資源，請使用逗號分隔 ARN：

```
"Resource": [
 "arn:aws:macie2:*:*:custom-data-identifier/12g4aff9-8e22-4f2b-b3fd-3063eexample",
 "arn:aws:macie2:*:*:custom-data-identifier/2d12c96a-8e78-4ca6-b1dc-8fd65example",
 "arn:aws:macie2:*:*:custom-data-identifier/4383a69d-4a1e-4a07-8715-208ddexample"
]
```

如需 Macie 資源類型的清單以及每種資源類型的 ARN 語法，請參閱服務授權參考中 Amazon Macie 定義的資源類型。若要了解您可以針對每種資源類型指定哪些動作，請參閱服務授權參考中的 Amazon Macie 定義的動作。如需指定資源的策略範例，請參閱Amazon Macie 的身分型政策範例。

Amazon Macie 的政策條件密鑰

支援服務特定政策條件金鑰	是

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

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

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

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

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

如需 Macie 條件金鑰的清單，請參閱服務授權參考中的 Amazon Macie 的條件金鑰。若要了解您可以使用條件金鑰的動作和資源，請參閱 Amazon Macie 定義的動作。如需使用條件索引鍵的原則範例，請參閱Amazon Macie 的身分型政策範例。

Amazon Macie 中的訪問控制列表（ACL）

支援 ACL	否

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

Amazon Simple Storage Service (Amazon S3) 是支持 ACL 的 AWS 服務 一個例子。若要進一步了解，請參閱 Amazon 簡單儲存服務使用者指南中的存取控制清單 (ACL) 概觀。

馬西不支援 ACL。也就是說，您無法將 ACL 附加到 Macie 資源。

Amazon Macie 基於屬性的訪問控制（ABAC）

支援 ABAC (政策中的標籤)	是

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

ABAC 在成長快速的環境中相當有幫助，並能在政策管理變得繁瑣時提供協助。

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

您可以將標籤附加至 Macie 資源 — 允許清單、自訂資料識別碼、篩選規則和抑制規則、成員帳戶以及敏感資料探索工作。您也可以透過在策略的Condition元素中提供標籤資訊來控制對這些類型資源的存取。若要取得有關標記 Macie 資源的資訊，請參閱標記亞馬遜麥西資源。如需根據標籤控制資源存取之身分型原則的範例，請參閱。Amazon Macie 的身分型政策範例

使用臨時登入資料與 Amazon Macie

支援臨時憑證	是

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

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

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

馬西支持使用臨時憑據。

Amazon Macie 的轉發訪問會話

支援轉寄存取工作階段 (FAS)	是

當您使用 IAM 使用者或角色在中執行動作時 AWS，您會被視為主體。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 會使用主體呼叫的權限 AWS 服務，並結合要求

AWS 服務 向下游服務發出要求。只有當服務收到需要與其 AWS 服務 他資源互動才能完成的請求時，才會發出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的政策詳細資訊，請參閱《轉發存取工作階段》。

當您執行下列工作 AWS 服務 時，Macie 會向下游發出 FAS 要求：

- 為 S3 儲存貯體中存放的允許清單建立或更新 Macie 設定。
- 檢查 S3 儲存貯體中存放的允許清單狀態。
- 使用 IAM 使用者登入資料從受影響的 S3 物件擷取敏感資料範例。
- 加密使用 IAM 使用者登入資料或 IAM 角色擷取的敏感資料範例。
- 啟用要與之整合的 AWS Organizations Macie。
- 在 AWS Organizations中指定組織的委派 Macie 管理員帳戶。

對於其他任務，Macie 會使用服務連結角色代表您執行動作。如需有關此角色的詳細資訊，請參閱Amazon Macie 的服務連結角色。

Amazon Macie 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 服務服務。

Macie 不會假設或使用服務角色。為了代表您執行動作，Macie 主要使用服務連結角色。如需有關此角色的詳細資訊，請參閱Amazon Macie 的服務連結角色。

Amazon Macie 的服務連結角色

支援服務連結角色	是

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

Macie 會使用服務連結角色代表您執行動作。如需有關此角色的詳細資訊，請參閱Amazon Macie 的服務連結角色。

Amazon Macie 的身分型政策範例

根據預設，使用者和角色不具備建立或修改 Macie 資源的許可。他們也無法使用 AWS Management Console、AWS Command Line Interface (AWS CLI) 或 AWS API 執行任務。若要授予使用者對其所需資源執行動作的許可，IAM 管理員可以建立 IAM 政策。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

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

如需 Macie 所定義之動作和資源類型的詳細資訊，包括每種資源類型的 ARN 格式，請參閱《服務授權參考》中「Amazon Macie 的動作、資源及條件索引鍵」。

建立政策時，請務必解決安全性警告、錯誤、一般警告，以及建議，然後再儲政策，然後再儲政策，然後再儲政策。AWS Identity and Access Management Access AnalyzerIAM Access Analyzer 會比對 IAM 政策文法和最佳實務來執行政策檢查，以驗證政策。這些檢查會產生問題清單並提供可行的建議，協助您撰寫具有功能性且符合安全最佳實務的政策。若要進一步了解如何使用 IAM Access Analyzer 驗證政策，請參閱《IAM 使用者指南》中的 IAM Access Analyzer 政策驗證。若要檢閱 IAM Access Analyzer 可傳回的警告、錯誤和建議清單，請參閱《IAM 使用者指南》中的 IAM Access Analyzer 政策檢查參考。

主題

政策最佳實務

以身分為基礎的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 Macie 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 受管政策並朝向最低權限許可的目標邁進 – 若要開始授予許可給使用者和工作負載，請使用 AWS 受管政策，這些政策會授予許可給許多常用案例。它們可在您的 AWS 帳戶 中使用。我

們建議您定義特定於使用案例的 AWS 客戶管理政策，以便進一步減少許可。如需詳細資訊，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 套用許可的詳細資訊，請參閱 IAM 使用者指南中的 IAM 中的政策和許可。
- 使用 IAM 政策中的條件進一步限制存取權 – 您可以將條件新增至政策，以限制動作和資源的存取。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。您也可以使用條件來授予對服務動作的存取權，前提是透過特定 AWS 服務 (例如 AWS CloudFormation) 使用條件。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，可協助您編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 IAM Access Analyzer 政策驗證。
- 需要多重要素驗證 (MFA) – 如果存在需要 AWS 帳戶中 IAM 使用者或根使用者的情況，請開啟 MFA 提供額外的安全性。若要在呼叫 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 使用者指南中的設定 MFA 保護的 API 存取。

有關 IAM 中最佳實務的詳細資訊，請參閱 IAM 使用者指南中的 IAM 安全最佳實務。

使用 Amazon Macie 控制台

若要存取 Amazon Macie 主控台，您必須擁有最基本的一組許可。這些許可必須允許您列出和檢視您中 Macie 資源的AWS 帳戶詳細資訊 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，您不需要允許其最基本主控台許可。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。

為確保使用者和角色可以使用 Amazon Macie 主控台，請建立 IAM 政策以提供他們主控台存取權。如需詳細資訊，請參閱 IAM 使用者指南 中的 IAM 中的政策和許可。

如果您建立允許使用者或角色使用 Amazon Macie 主控台的政策，請確保該政策允許該`macie2:GetMacieSession`動作。否則，這些使用者或角色將無法存取主控台上的任何 Macie 資源或資料。

此外，也請確定策略允許`macie2:List`對這些使用者或角色在主控台上存取的資源採取適當的動作。否則，他們將無法在控制台上導航到或顯示有關這些資源的詳細信

息。例如，若要使用主控台檢閱敏感資料探索工作的詳細資料，必須允許使用者針對工作和*macie2:DescribeClassificationJob*動作執行macie2:ListClassificationJobs動作。如果不允許使用者執行macie2:ListClassificationJobs動作，使用者將無法在主控台的 [工作] 頁面上顯示工作清單，因此無法選擇工作來顯示其詳細資料。如需詳細資訊包含工作使用的自訂資料識別碼的相關資訊，還必須允許使用者針對自訂資料識別碼執行macie2:BatchGetCustomDataIdentifiers動作。

範例：允許使用者檢閱他們自己的許可

此範例會示範如何建立政策，允許 IAM 使用者檢視連接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上，或是使用 AWS CLI 或 AWS API 透過編寫程式的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": "*"
        }
```

```
    ]
}
```

範例：允許使用者建立敏感資料探索工作

此範例會示範如何建立政策，允許使用者建立政策，允許使用者建立敏感資料探索任務的政策

在此範例中，第一個陳述式會將macie2:CreateClassificationJob權限授與使用者。這些權限可讓使用者建立工作。該聲明還授予macie2:DescribeClassificationJob權限。這些權限可讓使用者存取現有工作的詳細資料。雖然建立工作不需要這些權限，但存取這些詳細資料可協助使用者建立具有唯一組態設定的工作。

範例中的第二個陳述式可讓使用者使用 Amazon Macie 主控台建立、設定和檢閱任務。macie2:ListClassificationJobs權限可讓使用者在主控台的 [工作] 頁面上顯示現有的工作。陳述式中的所有其他權限可讓使用者使用主控台上的 [建立工作] 頁面來設定和建立工作。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CreateAndReviewJobs",
            "Effect": "Allow",
            "Action": [
                "macie2:CreateClassificationJob",
                "macie2:DescribeClassificationJob"
            ],
            "Resource": "arn:aws:macie2:*:*:classification-job/*"
        },
        {
            "Sid": "CreateAndReviewJobsOnConsole",
            "Effect": "Allow",
            "Action": [
                "macie2:ListClassificationJobs",
                "macie2:ListAllowLists",
                "macie2:ListCustomDataIdentifiers",
                "macie2:ListManagedDataIdentifiers",
                "macie2:SearchResources",
                "macie2:DescribeBuckets"
            ],
            "Resource": "*"
        }
    ]
```

```
}
```

範例：允許使用者管理敏感資料探索任務

此範例會示範如何建立政策，允許使用者存取政策，允許使用者存取政策，允許使用者存取其 ID 的詳細資訊3ce05dbb7ec5505def334104bexample。此範例也可讓使用者視需要變更工作狀態。

範例中的第一個陳述式會授macie2:DescribeClassificationJob與使用者和macie2:UpdateClassificationJob權限。這些權限可讓使用者分別擷取工作的詳細資訊並變更工作的狀態。第二個陳述式將macie2:ListClassificationJobs許可授與使用者，讓使用者可以使用 Amazon Macie 主控台上的「作業」頁面存取任務。

```
{
   "Version": "2012-10-17",
   "Statement": [
 {
         "Sid": "ManageOneJob",
         "Effect": "Allow",
         "Action": [
            "macie2:DescribeClassificationJob",
            "macie2:UpdateClassificationJob"
         ],
         "Resource": "arn:aws:macie2:*:*:classification-
job/3ce05dbb7ec5505def334104bexample"
 },
 {
         "Sid": "ListJobsOnConsole",
         "Effect": "Allow",
         "Action": "macie2:ListClassificationJobs",
         "Resource": "*"
 }
   ]
}
```

您也可以允許使用者存取 Macie 針對任務發佈到 Amazon Logs 的記錄資料 (CloudWatch日誌事件)。若要這麼做，您可以新增陳述式，以授與對CloudWatch記錄群組執行 Logs (logs) 動作的權限，並為工作進行串流。例如：

```
"Statement": [
    {
        "Sid": "AccessLogGroupForMacieJobs",
```

```
        "Effect": "Allow",
        "Action": [
            "logs:DescribeLogGroups",
            "logs:DescribeLogStreams"
        ],
        "Resource": "arn:aws:logs:*:*:log-group:aws/macie/classificationjobs"
    },
    {
        "Sid": "AccessLogEventsForOneMacieJob",
        "Effect": "Allow",
        "Action": "logs:GetLogEvents",
        "Resource": [
            "arn:aws:logs:*:*:log-group:aws/macie/classificationjobs/*",
            "arn:aws:logs:*:*:log-group:aws/macie/classificationjobs:log-
stream:3ce05dbb7ec5505def334104bexample"
        ]
    }
]
```

如需管理CloudWatch日誌存取權限的相關資訊，請參閱 Amazon Logs 使用者指南中的管理CloudWatch日CloudWatch誌資源存取許可概觀。

範例：允許使用者檢閱發現

此範例會示範如何建立允許使用者存取政策，允許使用者存取政策，允許使用者存取

在此範例中，macie2:GetFindings和macie2:GetFindingStatistics許可允許使用者使用 Amazon Macie API 或 Amazon Macie 主控台擷取資料。這些macie2:ListFindings許可允許使用者使用 Amazon Macie 主控台上的「摘要」儀表板和「發現項目」頁面來擷取和檢閱資料。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReviewFindings",
            "Effect": "Allow",
            "Action": [
                "macie2:GetFindings",
                "macie2:GetFindingStatistics",
                "macie2:ListFindings"
            ],
            "Resource": "*"
        }
```

```
    ]
}
```

您也可以允許使用者建立和管理發現項目的篩選規則和抑制規則。
若要這麼做，您可能會包含授與下列權限的陳述
式：macie2:CreateFindingsFiltermacie2:GetFindingsFiltermacie2:UpdateFindingsFilte
和macie2:DeleteFindingsFilter。若要允許使用者使用 Amazon Macie 主控台來管理規則，請
同時在政策中包含macie2:ListFindingsFilters許可。例如：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReviewFindings",
            "Effect": "Allow",
            "Action": [
                "macie2:GetFindings",
                "macie2:GetFindingStatistics",
                "macie2:ListFindings"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ManageRules",
            "Effect": "Allow",
            "Action": [
                "macie2:GetFindingsFilter",
                "macie2:UpdateFindingsFilter",
                "macie2:CreateFindingsFilter",
                "macie2:DeleteFindingsFilter"
            ],
            "Resource": "arn:aws:macie2:*:*:findings-filter/*"
        },
        {
            "Sid": "ListRulesOnConsole",
            "Effect": "Allow",
            "Action": "macie2:ListFindingsFilters",
            "Resource": "*"
        }
    ]
}
```

範例：允許使用者根據標籤檢閱自訂資料識別碼

在基於身分的政策中，您可以使用條件，根據標籤控制 Amazon Macie 的存取權。此範例會示範如何建立政策，允許使用者使用 Amazon Macie 主控台或 Amazon Macie 的政策，允許使用者檢視自訂資料識別碼。不過，只在Owner標籤的值是使用者的使用者名稱時，才會授予許可。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReviewCustomDataIdentifiersIfOwner",
            "Effect": "Allow",
            "Action": "macie2:GetCustomDataIdentifier",
            "Resource": "arn:aws:macie2:*:*:custom-data-identifier/*",
            "Condition": {
                "StringEquals": {"aws:ResourceTag/Owner": "${aws:username}"}
            }
        },
        {
            "Sid": "ListCustomDataIdentifiersOnConsoleIfOwner",
            "Effect": "Allow",
            "Action": "macie2:ListCustomDataIdentifiers",
            "Resource": "*",
            "Condition": {
                "StringEquals": {"aws:ResourceTag/Owner": "${aws:username}"}
            }
        }
    ]
}
```

在此範例中，如果具有使用者名稱的使用者richard-roe嘗試檢閱自訂資料識別碼的詳細資料，則必須標記自訂資料識別碼Owner=richard-roe或owner=richard-roe。否則，便會拒絕該使用者存取。條件標籤鍵Owner符合Owner，owner因為條件索引鍵名稱不區分大小寫。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。

Amazon Macie 的服務連結角色

Amazon Macie 使用名為的 AWS Identity and Access Management (IAM) 服務連結角色。AWSServiceRoleForAmazonMacie此服務連結角色是直接連結至 Macie 的 IAM 角色。它是由 Macie 預先定義的，它包括 Macie 需要調用其他 AWS 服務 並代表您監視 AWS 資源所需的所有權限。Macie 會在所有 Macie 可用的 AWS 區域 地方使用此服務連結角色。

服務連結角色可讓設定 Macie 變得更容易，因為您不需要手動新增必要的權限。Macie 定義此服務連結角色的權限，除非另有定義，否則只有 Macie 可以擔任該角色。定義的許可包括信任政策和許可政策，並且該許可政策不能連接到任何其他 IAM 實體。

您必須設定許可，以允許 IAM 實體 (例如使用者或角色) 建立、編輯或刪除服務連結角色。如需詳細資訊，請參閱 IAM 使用者指南中的服務連結角色許可。只有在刪除服務連結角色的相關資源後，才能刪除該角色。這可保護您的資源，避免您不小心移除資源的存取許可。

如需關於支援服務連結角色的其他服務資訊，請參閱可搭配 IAM 運作的AWS 服務，尋找 Service-linked roles (服務連結角色) 欄中顯示為 Yes (是) 的服務。選擇具有連結的 [是]，以檢閱該服務的服務連結角色文件。

主題

- Amazon Macie 的服務連結角色許可
- 創建 Amazon Macie 的服務鏈接角色
- 編輯 Amazon Macie 的服務連結角色
- 刪除 Amazon Macie 的服務鏈接角色
- 支援 AWS 區域 Amazon Macie 服務連結角色

Amazon Macie 的服務連結角色許可

Amazon Macie 使用名為的服務鏈接角色。`AWSServiceRoleForAmazonMacie`此服務連結角色會信任`macie.amazonaws.com`服務擔任該角色。

角色的權限原則 (名`AmazonMacieServiceRolePolicy`為) 可讓 Macie 在指定的資源上執行下列工作：

- 使用 Amazon S3 動作擷取有關 S3 儲存貯體和物件的資訊。
- 使用 Amazon S3 動作擷取 S3 物件。
- 使用 AWS Organizations 動作擷取關聯帳號的相關資訊。
- 使用 Amazon CloudWatch 日誌動作記錄敏感資料探索任務的事件。

角色設定為下列權限原則。

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```
    {
      "Effect": "Allow",
      "Action": [
        "iam:ListAccountAliases",
        "organizations:DescribeAccount",
        "organizations:ListAccounts",
        "s3:GetAccountPublicAccessBlock",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetBucketWebsite",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetReplicationConfiguration",
        "s3:ListBucket",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectTagging"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup"
      ],
      "Resource": [
        "arn:aws:logs:*:*:log-group:/aws/macie/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource": [
```

```
        "arn:aws:logs:*:*:log-group:/aws/macie/*:log-stream:*"
      ]
    }
  ]
}
```

如需有關AmazonMacieServiceRolePolicy策略更新的詳細資訊，請參閱亞馬遜麥西更新AWS受管理政策。如需有關此原則變更的自動警示，請訂閱 Macie 文件歷史記錄頁面上的 RSS 摘要。

您必須設定許可，以允許 IAM 實體 (例如使用者或角色) 建立、編輯或刪除服務連結角色。如需詳細資訊，請參閱 IAM 使用者指南中的服務連結角色許可。

創建 Amazon Macie 的服務鏈接角色

您不需要為 Amazon Macie 手動建立AWSServiceRoleForAmazonMacie服務連結角色。當您為您啟用 Macie 時 AWS 帳戶，Macie 會自動為您建立服務連結角色。

如果您刪除 Macie 服務連結角色，然後需要再次建立角色，則可以使用相同的程序在帳戶中重新建立角色。當您再次啟用 Macie 時，Macie 會再次為您建立服務連結角色。

編輯 Amazon Macie 的服務連結角色

Amazon Macie 不允許您編輯AWSServiceRoleForAmazonMacie服務鏈接的角色。建立服務連結角色之後，您無法變更角色的名稱，因為各種實體可能會參照該角色。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 Amazon Macie 的服務鏈接角色

如果您不再需要使用 Amazon Macie，建議您手動刪除AWSServiceRoleForAmazonMacie服務連結角色。當您停用 Macie 時，Macie 不會為您刪除角色。

在刪除角色之前，您必須在每個啟用 Macie 的 AWS 區域 位置中停用該角色。您也必須手動清理角色的資源。若要刪除角色，您可以使用 IAM 主控台 AWS CLI、或 AWS API。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。

> **Note**
>
> 當您嘗試刪除資源時，如果 Macie 正在使用此AWSServiceRoleForAmazonMacie角色，則刪除可能會失敗。如果發生這種情況，請等待幾分鐘，然後再次嘗試該操作。

如果您刪除AWSServiceRoleForAmazonMacie服務連結角色並需要重新建立，您可以針對您的帳戶啟用 Macie 來重新建立該角色。當您再次啟用 Macie 時，Macie 會再次為您建立服務連結角色。

支援 AWS 區域 Amazon Macie 服務連結角色

Amazon Macie 支持使用AWSServiceRoleForAmazonMacie服務鏈接的角色在所有的 AWS 區域 地方 Macie 是可用的。如需目前可使用 Macie 的區域清單，請參閱. AWS 一般參考

AWS亞馬遜馬西的受管政策

AWS 受管政策是由 AWS 建立和管理的獨立政策。AWS 受管政策的設計在於為許多常見使用案例提供許可，如此您就可以開始將許可指派給使用者、群組和角色。

請記住，AWS 受管政策可能不會授與您特定使用案例的最低權限許可，因為它們可供所有 AWS 客戶使用。我們建議您定義使用案例專屬的客戶管理政策，以便進一步減少許可。

您無法更改 AWS 受管政策中定義的許可。如果 AWS 更新 AWS 受管政策中定義的許可，更新會影響政策連接的所有主體身分 (使用者、群組和角色)。在推出新的 AWS 服務 或有新的 API 操作可供現有服務使用時，AWS 很可能會更新 AWS 受管政策。

如需詳細資訊，請參閱《IAM 使用者指南》https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_managed-vs-inline.html#aws-managed-policies中的 AWS 受管政策。

亞馬遜麥西提供了幾個AWS受管理的策略：AmazonMacieFullAccess政策，AmazonMacieReadOnlyAccess政策，以及AmazonMacieServiceRolePolicy政策。

主題

- AWS 受管政策：AmazonMacieFullAccess
- AWS 受管政策：AmazonMacieReadOnlyAccess
- AWS 受管政策：AmazonMacieServiceRolePolicy
- 亞馬遜麥西更新AWS受管理政策

AWS 受管政策：AmazonMacieFullAccess

您可以附加AmazonMacieFullAccess適用於您的 IAM 實體的政策。

此政策授予允許 IAM 身分的完整管理許可 (主要) 以建立亞馬遜 Macie 服務鏈接角色並為亞馬遜 Macie 執行所有讀取和寫入操作。權限包括變更功能，例如建立、更新和刪除。如果此原則附加至主參與者，則主體可以建立、擷取及存取其帳戶的所有 Macie 資源、資料和設定。

主體必須先將此原則附加至主體，才能為其帳戶啟用 Macie — 主體必須被允許建立 Macie 服務連結角色，才能為其帳戶啟用 Macie。

許可詳細資訊

此政策包含以下許可：

- `macie2`— 允許校長對 Amazon Macie 執行所有讀取和寫入動作。
- `iam`— 允許主參與者建立服務連結角色。該`Resource`元素會指定 Macie 的服務連結角色。該`Condition`元素使用`iam:AWSServiceName` 條件鍵和`StringLike` 條件運算子將權限限制為 Macie 的服務連結角色。
- `pricing`— 允許主參與者擷取其定價資料AWS 帳戶從AWS Billing and Cost Management。當主體建立和設定敏感資料探索工作時，Macie 會使用此資料來計算並顯示預估的成本。

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "macie2:*"
         ],
         "Resource": "*"
      },
      {
         "Effect": "Allow",
         "Action": "iam:CreateServiceLinkedRole",
         "Resource": "arn:aws:iam::*:role/aws-service-role/macie.amazonaws.com/
AWSServiceRoleForAmazonMacie",
         "Condition": {
            "StringLike": {
               "iam:AWSServiceName": "macie.amazonaws.com"
            }
```

```
         }
      },
      {
         "Effect": "Allow",
         "Action": "pricing:GetProducts",
         "Resource": "*"
      }
   ]
}
```

AWS 受管政策：AmazonMacieReadOnlyAccess

您可以附加AmazonMacieReadOnlyAccess適用於您的 IAM 實體的政策。

此政策授予允許 IAM 身分的唯讀許可 (主要) 執行亞馬遜 Macie 的所有讀取操作。權限不包括更改功能，例如創建，更新或刪除。如果此原則附加至主體，主體可以擷取，但無法以其他方式存取其帳戶的所有 Macie 資源、資料和設定。

許可詳細資訊

此政策包含以下許可：

macie2— 允許校長對 Amazon Macie 執行所有讀取動作。

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "macie2:Describe*",
            "macie2:Get*",
            "macie2:List*",
            "macie2:BatchGetCustomDataIdentifiers",
            "macie2:SearchResources"
         ],
         "Resource": "*"
      }
   ]
```

```
}
```

AWS 受管政策：AmazonMacieServiceRolePolicy

您無法將 AmazonMacieServiceRolePolicy 政策附加至 IAM 實體。此原則附加至服務連結角色，可讓 Macie 代表您執行動作。如需詳細資訊，請參閱Amazon Macie 的服務連結角色。

亞馬遜麥西更新AWS受管理政策

檢閱有關更新的詳細資訊AWSAmazon Macie 的受管政策，因為這項服務開始追蹤這些變更。如需有關此頁面變更的自動警示，請訂閱馬西文件歷史頁面。

變更	描述	日期
AmazonMacieReadOnlyAccess-增加了一個新的政策	馬西添加了一個新的政策，AmazonMacieReadOnlyAccess 政策。此原則會授與唯讀權限，讓主體擷取其帳戶的所有 Macie 資源、資料和設定。	2023 年 6 月 15 日
AmazonMacieFullAccess-更新了現有策略	在AmazonMacieFullAccess 政策，馬西更新了 Macie 服務鏈接角色的亞馬遜資源名稱（ARN）（aws-service-role/macie.amazonaws.com/AWSServiceRoleForAmazonMacie ）.	2022 年 6 月 30 日
AmazonMacieServiceRolePolicy-更新了現有策略	馬西刪除動作和資源亞馬遜 Macie 經典從AmazonMacieServiceRolePolicy 政策。亞馬遜 Macie 經典已停產，不再可用。	2022 年 5 月 20 日

變更	描述	日期
	更具體地說，馬西刪除了所有AWS CloudTrail動作。Macie 還刪除了以下資源的所有亞馬遜 S3 操作：`arn:aws:s3:::awsmacie-*` ,`arn:aws:s3:::awsmacietrail-*` ，以及`arn:aws:s3:::*-awsmacietrail-*` 。	
AmazonMacieFullAccess-更新了現有策略	馬西添加了一個AWS Billing and Cost Management(pricing) 行動`AmazonMacieFullAccess` 政策。此動作可讓主參與者擷取其帳戶的定價資料。當主體建立和設定敏感資料探索工作時，Macie會使用此資料來計算並顯示預估的成本。 馬西也刪除了亞馬遜瑪西經典 (`macie`) 來自的動作`AmazonMacieFullAccess` 政策。	2022 年 3 月 7 日
AmazonMacieServiceRolePolicy-更新了現有策略	馬西添加亞馬遜CloudWatch將動作記錄到`AmazonMacieServiceRolePolicy` 政策。這些動作可讓 Macie 將記錄事件發佈至CloudWatch敏感資料探索工作的記錄檔。	2021 年 4 月 13 日
馬西開始跟踪變化	馬西開始跟踪其更改AWS受管理的策略。	2021 年 4 月 13 日

Amazon Macie 身分和存取疑難排解

下列資訊可協助您診斷和修正使用 Amazon Macie 和 AWS Identity and Access Management (IAM) 時可能會遇到的常見問題。

主題

我沒有授權在 Amazon Macie 中執行操作

如果您收到錯誤，告知您未獲授權執行動作，您的政策必須更新，允許您執行動作。

下列範例錯誤會在mateojackson IAM 使用者嘗試使用主控台檢視一個虛構 *my-example-widget* 資源的詳細資訊，但卻無虛構 macie2:*GetWidget* 許可時發生。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 macie2:GetWidget on resource: my-example-widget
```

在此情況下，必須更新 mateojackson 使用者的政策，允許使用 macie2:*GetWidget* 動作存取 *my-example-widget* 資源。

如果您需要協助，請聯絡您的 AWS 系統管理員。您的管理員提供您的簽署憑證。

我想允許我以外的人訪 AWS 帳戶 問我的 Amazon Macie 資源

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

如需進一步了解，請參閱以下內容：

- 若要瞭解 Macie 是否支援這些功能，請參閱亞 Amazon Macie 如何與 AWS Identity and Access Management。
- 若要了解如何提供對您所擁有資源 AWS 帳戶 的存取權，請參閱《IAM 使用者指南》中您擁有的另一 AWS 帳戶 個 IAM 使用者提供存取權限。
- 若要了解如何將資源存取權提供給第三方 AWS 帳戶，請參閱 IAM 使用者指南中的提供第三方 AWS 帳戶 擁有的存取權。

- 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)。
- 若要了解跨帳戶存取使用角色和以資源為基礎的政策之間的差異，請參閱 IAM 使用者指南中的 IAM 中的跨帳戶資源存取。

在 Amazon Macie 中記錄和監控

Amazon Macie 已與整合AWS CloudTrail，這項服務可提供由使用者、角色或其他人在 Macie 中所採取之動作的記錄AWS 服務。這包括來自 Amazon Macie 主控台的動作，以及對 Amazon Macie API 操作的程式設計呼叫。通過使用收集的信息 CloudTrail，您可以確定向 Macie 提出了哪些請求。對於每個請求，您可以識別提出時間、提出請求的 IP 地址、提出請求者，以及其他詳細資料。如需詳細資訊，請參閱 使用日誌記錄 Amazon Macie API 調用 AWS CloudTrail。

Amazon Macie 的合規驗證

若要瞭解 AWS 服務 是否屬於特定規範遵循方案的範圍內，請參閱AWS 服務 遵循規範計劃方案中的，並選擇您感興趣的合規方案。如需一般資訊，請參閱AWS 規範計劃AWS。

您可以使用下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱下載中的報告中的 AWS Artifact。

您在使用時的合規責任取決 AWS 服務 於您資料的敏感性、公司的合規目標以及適用的法律和法規。AWS 提供下列資源以協助遵循法規：

- 安全性與合規性快速入門指南 — 這些部署指南討論架構考量，並提供部署以安全性和合規性 AWS 為重點的基準環境的步驟。
- 在 Amazon Web Services 上架構 HIPAA 安全性與合規性 — 本白皮書說明公司如何使用建立符合 HIPAA 資格的應 AWS 用程式。

> **Note**
>
> 並非所有人 AWS 服務 都符合 HIPAA 資格。如需詳細資訊，請參閱 HIPAA 資格服務參照。

- AWS 合規資源AWS — 此工作簿和指南集合可能適用於您的產業和所在地。
- AWS 客戶合規指南 — 透過合規的角度瞭解共同的責任模式。這份指南總結了在多個架構 (包括美國國家標準技術研究所 (NIST)、支付卡產業安全標準委員會 (PCI) 和國際標準化組織 (ISO)) 中，保 AWS 服務 護指引並對應至安全控制的最佳實務。

- 使用AWS Config 開發人員指南中的規則評估資源 — 此 AWS Config 服務會評估您的資源組態符合內部實務、產業準則和法規的程度。
- AWS Security Hub— 這 AWS 服務 提供了內部安全狀態的全面視圖 AWS。Security Hub 使用安全控制，可評估您的 AWS 資源並檢查您的法規遵循是否符合安全業界標準和最佳實務。如需支援的服務和控制清單，請參閱 Security Hub controls reference。
- Amazon GuardDuty — 透過監控環境中的 AWS 帳戶可疑和惡意活動，藉此 AWS 服務 偵測您的工作負載、容器和資料的潛在威脅。 GuardDuty 可協助您滿足特定合規性架構所要求的入侵偵測需求，例如 PCI DSS 等各種合規性需求。
- AWS Audit Manager— 這 AWS 服務 有助於您持續稽核您的 AWS 使用情況，以簡化您管理風險的方式，以及遵守法規和業界標準的方式。

Amazon Macie 的備援功能

AWS全球基礎設施是以可用區域為中心建置。AWS 區域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網路連線相互連結。透過可用區域，您可以設計與操作的應用程式和資料庫，在可用區域之間自動容錯移轉而不會發生中斷。可用區域的可用性、容錯能力和擴充能力，均較單一或多個資料中心的傳統基礎設施還高。

如需 AWS 區域 與可用區域的詳細資訊，請參閱AWS全球基礎架構。

亞馬遜 Macie 的基礎設施安全

作為一項受管服務，Amazon Macie 受到AWS全球網路安全的保護。如需有關 AWS 安全服務以及 AWS 如何保護基礎設施的詳細資訊，請參閱 AWS 雲端安全。若要使用基礎設施安全性的最佳實務來設計您的 AWS 環境，請參閱安全性支柱 AWS 架構良好的框架中的基礎設施保護。

您可以使用AWS已發佈的 API 呼叫透過網路存取 Macie。用戶端必須支援下列項目：

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

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

Amazon Macie 和 VPC 端點界面 () AWS PrivateLink

如果您使用 Amazon Virtual Private Cloud (Amazon VPC) 託管資AWS源，則可以在 VPC 和 Amazon Macie 之間建立私有連接。Amazon VPC 是您可以用來在您定義的虛擬網路中啟動AWS資源的一種。AWS 服務您可利用 VPC 來控制您的網路設定，例如 IP 地址範圍、子網路、路由表和網路閘道。

要將您的 VPC 連接到 Macie，您可以為 Macie 創建一個接口 VPC 端點。界面端點採用這種技術 AWS PrivateLink，可讓您在沒有網際網路閘道、NAT 裝置、VPN 連線或AWS Direct Connect連線的情況下私有存取 Amazon Macie API。VPC 中的執行個體不需要公有 IP 地址即可與 Amazon Macie API 進行通訊。您的 VPC 和 Macie 之間的流量不會離開亞馬遜網絡。

每個介面端點都由子網路中的一個或多個彈性網路介面表示。如需詳細資訊，請參閱 Amazon VPC AWS 服務 使用者指南中的使用介面 VPC 端點存取。

主題

- Amazon Macie VPC 端點的注意事項
- 為 Amazon Macie 創建一個接口 VPC 端點

Amazon Macie VPC 端點的注意事項

Amazon Macie 支援所有目前可用的 VPC 端點AWS 區域，但亞太區域 (大阪) 和以色列 (特拉維夫) 區域除外。如需目前可使用 Macie 的區域清單，請參閱. AWS 一般參考 此外，Macie 支援從 VPC 呼叫其所有 API 動作。

如果您為 Macie 創建了接口 VPC 端點，請考慮對提供 VPC 支持並與 Macie 集成AWS 服務的其他端點執行相同的操作，例如亞馬遜和. EventBridge AWS Security Hub 然後 Macie 和這些服務可以使用 VPC 端點進行整合。例如，如果您建立適用於 Macie 的 VPC 端點和 Security Hub 的 VPC 端點，Macie 可以在將發現項目發佈到 Security Hub 心時使用其 VPC 端點，而 Security Hub 在收到發現項目時可以使用其 VPC 端點。如需支援 VPC 端點的服務的相關資訊，請參閱 AWS 服務 Amazon VPC 使用者指南AWS PrivateLink中的與整合。

有關其他考量，請參閱 Amazon VPC AWS 服務 使用者指南中的使用界面 VPC 端點存取。

請注意，Macie 不支援 VPC 端點原則。默認情況下，允許通過端點對 Macie 的完全訪問。如需詳細資訊，請參閱 Amazon VPC 使用者指南中的 VPC 端點和 VPC 端點服務的身分識別和存取管理。

為 Amazon Macie 創建一個接口 VPC 端點

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

當您為 Macie 建立 VPC 端點時，請使用下列服務名稱：

- com.amazonaws.*region*.macie2

其中，*##*是適用的區域代碼AWS 區域。

如果您為端點啟用私有 DNS，則可以使用該區域的預設 DNS 名稱 (例如美國東部 (維吉尼亞北部) 區域的`macie2.us-east-1.amazonaws.com`預設 DNS 名稱向 Macie 發出 API 要求。

如需詳細資訊，請參閱 Amazon VPC AWS 服務 使用者指南中的使用介面 VPC 端點存取。

使用日誌記錄 Amazon Macie API 調用 AWS CloudTrail

Amazon Macie 與整合AWS CloudTrail，這是一項服務，可提供使用者、角色或其他使用者在 Macie 中採取的動作記錄。AWS 服務 CloudTrail捕獲馬西的所有 API 調用作為事件。擷取的呼叫包括來自 Amazon Macie 主控台的呼叫，以及對 Amazon Macie API 操作的程式設計呼叫。

如果您建立追蹤，您可以啟用持續交付 CloudTrail 事件到 Amazon Simple Storage Service (Amazon S3) 儲存貯體，包括 Macie 的事件。如果您未設定追蹤，您仍然可以使用AWS CloudTrail主控台上的事件歷程記錄來檢閱最近的事件。使用收集的信息 CloudTrail，您可以確定向 Macie 提出的請求，提出請求的 IP 地址，提出請求的人員，提出請求的時間以及其他詳細信息。

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

主題

- Amazon Macie 信息 AWS CloudTrail
- 了解 Amazon Macie 日誌文件條目

Amazon Macie 信息 AWS CloudTrail

AWS CloudTrail在您建立帳戶AWS 帳戶時啟用。當 Amazon Macie 中發生活動時，該活動會與事件歷史記錄中的其他 CloudTrail 事件一起記錄在AWS事件中。您可以查看，搜索和下載最近的事件AWS 帳戶。若要取得更多資訊，請參閱《使用指南》中的〈AWS CloudTrail使用 CloudTrail 事件歷程〉。

為了持續記錄您的事件AWS 帳戶，包括 Macie 的事件，請創建一個跟踪。追蹤可 CloudTrail 將日誌檔交付到 Amazon Simple Storage Service (Amazon S3) 儲存貯體。根據預設，當您使用AWS CloudTrail主控台建立追蹤時，追蹤會套用至所有項目AWS 區域。該追蹤會記錄來自 AWS 分割區中所有區域的事件，並將日誌檔案交付到您指定的 S3 儲存貯體。此外，您可以設定其他，AWS 服務以進一步分析 CloudTrail 記錄中收集的事件資料並採取行動。如需詳細資訊，請參閱《AWS CloudTrail 使用者指南》中的以下主題：

- 建立 AWS 帳戶 的追蹤
- CloudTrail 支援的服務與整合
- 設定 Amazon SNS 通知 CloudTrail
- 從多個區域接收 CloudTrail 記錄檔
- 從多個帳戶接收 CloudTrail 日誌文件

所有 Macie 動作都會記錄下來， CloudTrail 並記錄在 Amazon Macie API 參考中。例如，呼叫`CreateClassificationJob`、`DescribeBuckets`、和`ListFindings`動作會在 CloudTrail 記錄檔中產生項目。

每一筆事件或日誌項目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：

- 該請求是否透過根或 AWS Identity and Access Management (IAM) 使用者憑證來提出。
- 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。
- 該請求是否由另一項 AWS 服務 服務提出。

如需詳細資訊，請參閱《AWS CloudTrail使用者指南》中的使用者 CloudTrail userIdentity 元素。

了解 Amazon Macie 日誌文件條目

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

下列範例顯示示範 Amazon Macie 動作事件的 CloudTrail 記錄項目。如需有關記錄項目可能包含之資訊的詳細資訊，請參閱《AWS CloudTrail使用指南》中的CloudTrail 記錄事件參考。

範例：列出搜尋結果

下列範例顯示示範 Macie ListFindings動作事件的 CloudTrail 記錄項目。在此範例中，AWS Identity and Access Management(IAM) 使用者 (`Mary_Major`) 使用 Amazon Macie 主控台擷取其帳戶目前政策發現項目的相關資訊子集。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:user/Mary_Major",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Mary_Major",
        "sessionContext":{
            "attributes": {
                "creationdate": "2023-11-14T15:49:57Z",
```

```
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-11-14T16:09:56Z",
    "eventSource": "macie2.amazonaws.com",
    "eventName": "ListFindings",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "198.51.100.1",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/119.0.0.0 Safari/537.36",
    "requestParameters": {
        "sortCriteria": {
            "attributeName": "updatedAt",
            "orderBy": "DESC"
        },
        "findingCriteria": {
            "criterion": {
                "archived": {
                    "eq": [
                        "false"
                    ]
                },
                "category": {
                    "eq": [
                        "POLICY"
                    ]
                }
            }
        },
        "maxResults": 25,
        "nextToken": ""
    },
    "responseElements": null,
    "requestID": "d58af6be-1115-4a41-91f8-ace03example",
    "eventID": "ad97fac5-f7cf-4ff9-9cf2-d0676example",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

範例：擷取發現項目的敏感資料範例

此範例顯示的 CloudTrail 記錄項目會示範擷取和顯示 Macie 在發現項目中報告之敏感資料樣本的事件。在此範例中，IAM 使用者 (JohnDoe) 使用 Amazon Macie 主控台擷取和顯示敏感資料樣本。使用者的 Macie 帳戶設定為假設 IAM 角色 (MacieReveal) 來擷取和揭露敏感資料範例。

下列記錄事件顯示使用者透過執行 Macie GetSensitiveDataOccurrences動作擷取和顯示敏感資料樣本之要求的詳細資料。


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "UU4MH7OYK5ZCOAEXAMPLE:JohnDoe",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/JohnDoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "UU4MH7OYK5ZCOAEXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-12-12T14:40:23Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-12-12T17:04:47Z",
    "eventSource": "macie2.amazonaws.com",
    "eventName": "GetSensitiveDataOccurrences",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "198.51.100.252",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/119.0.0.0 Safari/537.36",
    "requestParameters": {
        "findingId": "3ad9d8cd61c5c390bede45cd2example"
    },
    "responseElements": null,
```

```
    "requestID": "c30cb760-5102-47e7-88d8-ff2e8example",
    "eventID": "baf52d92-f9c3-431a-bfe8-71c81example",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

下一個日誌事件顯示有關 Macie 的詳細信息，然後通過執行（MacieReveal）AssumeRole操作假設指定的 IAM 角色AWS Security Token Service（AWS STS）。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "reveal-samples.macie.amazonaws.com"
    },
    "eventTime": "2023-12-12T17:04:47Z",
    "eventSource": "sts.amazonaws.com",
    "eventName": "AssumeRole",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "reveal-samples.macie.amazonaws.com",
    "userAgent": "reveal-samples.macie.amazonaws.com",
    "requestParameters": {
        "roleArn": "arn:aws:iam::111122223333:role/MacieReveal",
        "roleSessionName": "RevealCrossAccount"
    },
    "responseElements": {
        "credentials": {
            "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
            "sessionToken": "XXYYaz...
EXAMPLE_SESSION_TOKEN
XXyYaZAz",
            "expiration": "Dec 12, 2023, 6:04:47 PM"
        },
        "assumedRoleUser": {
            "assumedRoleId": "AROAXOTKAROCSNEXAMPLE:RevealCrossAccount",
            "arn": "arn:aws:sts::111122223333:assumed-role/MacieReveal/
RevealCrossAccount"
        }
    },
    "requestID": "d905cea8-2dcb-44c1-948e-19419example",
```

```
    "eventID": "74ee4d0c-932d-3332-87aa-8bcf3example",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::IAM::Role",
            "ARN": "arn:aws:iam::111122223333:role/MacieReveal"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

標記亞馬遜麥西資源

標籤是可選的標籤，您可以定義並指派給AWS資源，包括特定類型的 Amazon Macie 資源。標籤可協助您以不同的方式識別、分類及管理資源，例如依用途、擁有者、環境或其他條件。例如，您可以使用標籤來套用原則、分配成本、區分資源版本，或識別支援特定合規性需求或工作流程的資源。

您可以將標籤指派給下列類型的 Macie 資源：允許清單、自訂資料識別碼、發現項目的篩選規則和抑制規則，以及敏感資料探索工作。如果您是組織的 Macie 管理員，也可以為組織中的成員帳戶指派標籤。

主題

標記基本面

資源最多可以擁有 50 個標籤。每個標籤皆包含由您定義的必要「標籤金鑰」與選用「標籤值」。標籤關鍵字是一般標示，可做為更特定標籤值的品類。標籤值是標籤金鑰的描述項。

例如，如果您建立自訂資料識別碼和敏感資料探索工作以分析工作流程中不同點的資料 (一組用於暫存資料，另一組用於生產資料)，則可以為這些資源指派`Stack`標籤索引鍵。此標籤鍵的標籤值可能`Staging`適用於設計用於分析暫存資料的自訂資料識別碼和工作，以及其他`Production`資料。

定義和指派標籤給資源時，請記住下列事項：

- 每個資源的上限為 50 個標籤。
- 對於每個資源，每個標籤鍵必須是唯一的，並且只能有一個標籤值。
- 標籤鍵與值皆區分大小寫。最佳做法是，我們建議您定義策略，以便將標籤資本化，並在資源中一致地實作該策略。
- 一個標籤鍵最多可包含 128 個 UTF-8 字元。一個標籤值最多可包含 256 個 UTF-8 字元。字符可以是字母，數字，空格或以下符號：_。：/= +-@

- 前aws:綴保留供使用AWS。您不能在您定義的任何標籤鍵或值中使用它。此外，您無法變更或移除使用此前置詞的標籤鍵或值。使用此字首的標籤不會計入每個資源 50 個標籤的配額。
- 您指派的任何標籤僅適用於您的標籤，AWS 帳戶且僅適用於您指派標籤的標籤。AWS 區域
- 如果刪除資源，也會刪除指定給該資源的任何標籤。

有關其他限制、提示和最佳做法，請參閱標記AWS資源使用指南。

> **Important**
>
> 請勿在標籤中儲存機密或其他類型的敏感資料。標籤可以從許多人訪問AWS 服務，包括AWS Billing and Cost Management。它們不打算用於敏感數據。

若要新增和管理 Macie 資源的標籤，您可以使用 Amazon Macie 主控台、亞馬遜 Macie API、主AWS Resource Groups控台上的標籤編輯器或標記 API。AWS Resource Groups使用 Macie，您可以在建立資源時將標籤新增至資源。您也可以新增和管理個別現有資源的標籤。使用資源群組，您可以大量新增和管理跨越多個現有資源的標籤AWS 服務，包括 Macie。如需詳細資訊，請參閱標記 AWS 資源使用者指南。

在 IAM 政策中使用標籤

開始標記資源後，您可以在 AWS Identity and Access Management (IAM) 政策中定義以標籤為基礎的資源層級許可。透過這種方式使用標籤，您可以對您中的哪些使用者和角色AWS 帳戶有權建立和標記資源，以及哪些使用者和角色有權更一般地新增、編輯和移除標籤。若要根據標籤控制存取，您可以在 IAM 政策的「條件」元素中使用與標籤相關的條件金鑰。

例如，如果資源的Owner標籤指定了使用者名稱，您可以建立一個政策，允許使用者完全存取所有 Amazon Macie 資源：

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ModifyResourceIfOwner",
            "Effect": "Allow",
            "Action": "macie2:*",
            "Resource": "*",
            "Condition": {
```

```
                "StringEqualsIgnoreCase": {"aws:ResourceTag/Owner": "${aws:username}"}
            }
        }
    ]
}
```

如果您定義標籤型、資源層級許可，則許可會立即生效。這表示您的資源一旦建立就會更安全，而且您可以快速開始強制使用新資源的標籤。您也可以使用資源層級許可，以控制哪些標籤金鑰和值可以與新的和現有的資源相關聯。如需詳細資訊，請參閱 IAM 使用者指南中的使用標籤控制對 AWS 資源的存取。

將標籤添加到亞馬遜 Macie 資源

要將標籤添加到單個亞馬遜 Macie 資源，您可以使用亞馬遜 Macie 控制台或亞馬遜 Macie API。若要同時將標籤新增至多個 Macie 資源，請使用AWS Resource Groups主控台上的「標籤編輯器」或「標記 API」的標AWS Resource Groups記作業。

> **Important**
>
> 將標籤新增至資源可能會影響資源的存取。在將標籤新增至資源之前，請先檢閱任何可能使用標籤來控制資源存取的 AWS Identity and Access Management (IAM) 政策。

Console

建立允許清單、自訂資料識別碼或敏感資料探索任務時，Amazon Macie 主控台會提供將標籤新增至資源的選項。在建立資源時，請遵循主控台上的指示，將標籤新增至這些類型的資源。若要將標籤新增至篩選器或抑制規則或組織中的成員帳號，您必須先建立資源，才能將標籤新增至該資源。

若要使用 Amazon Macie 主控台將一或多個標籤新增至現有資源，請按照下列步驟操作。

若要將標籤新增至資源

1. 在以下位置打開亞馬遜麥西亞控制台 https://console.aws.amazon.com/macie/。
2. 根據您要新增標籤的資源類型，執行下列其中一個動作：

   - 對於允許清單，請在導覽窗格中選擇 [允許清單]。

     然後，在表格中選取清單的核取方塊。然後選擇「動作」功能表上的 「管理標籤」
   - 對於自訂資料識別碼，請在導覽窗格中選擇 [自訂資料識別碼]。

然後，在表格中，選取自訂資料識別碼的核取方塊。然後選擇「動作」功能表上的 「管理標籤」

- 對於篩選或抑制規則，請在導覽窗格中選擇「發現項目」。

  然後，在「儲存的規則」清單中，選擇規則旁邊的編輯圖示 ()。
  然後選擇管理標籤。
- 對於組織中的成員帳戶，請在導覽窗格中選擇 [帳戶]。

  然後，在表格中選取帳戶的核取方塊。然後選擇「動作」功能表上的 「管理標籤」
- 對於敏感性資料探索工作，請在導覽窗格中選擇「工作」。

  然後，在表格中選取工作的核取方塊。然後選擇「動作」功能表上的 「管理標籤」

[管理標籤] 視窗會列出目前指定給資源的所有標籤。

3. 在「管理標籤」視窗中，選擇 「編輯標籤」。
4. 選擇 Add tag (新增標籤)。
5. 在 [金鑰] 方塊中，輸入要新增至資源之標籤的標籤金鑰。然後，在「值」方塊中，選擇性地輸入鍵的標籤值。

   標籤金鑰最多可包含 128 個字元。標籤值最多可包含 256 個字元。字符可以是字母，數字，空格或以下符號：_。：/= +-@
6. (選擇性) 若要將其他標籤新增至資源，請選擇 [新增標籤]，然後重複上述步驟。您最多可以為資源指派 50 個標籤。
7. 完成新增標籤後，請選擇 [儲存]。

API

若要建立資源並以程式設計方式為其新增一或多個標籤，請針對您要建立的資源類型使用適當的`Create`作業：

- 允許清單 — 使用CreateAllowList作業，或者，如果您使用的是 AWS Command Line Interface (AWS CLI)，則執行create-allow-list命令。
- 自訂資料識別碼 — 使用CreateCustomDataIdentifier作業，或者，如果您正在使用AWS CLI，則執行create-custom-data-identifier命令。

- 篩選或抑制規則 — 使用CreateFindingsFilter作業，或者，如果您正在使用AWS CLI，則執行create-findings-filter命令。
- 成員帳戶 — 使用CreateMember作業，或者，如果您正在使用AWS CLI，則執行建立成員命令。
- 敏感資料探索工作 — 使用CreateClassificationJob作業，或者，如果您正在使用AWS CLI，則執行create-classification-job命令。

在您的請求中，使用tags參數來為每個要新增至資源的標籤指定標籤鍵 (keyvalue) 和可選標籤值 ()。該tags參數指定string-to-string標籤鍵及其相關標籤值的映射。

若要將一或多個標籤新增至現有資源，請使用 Amazon Macie API 的TagResource作業，或者，如果您使用的是AWS CLI，請執行標籤資源命令。在您的請求中，指定要新增標籤的資源的 Amazon 資源名稱 (ARN)。使用tags參數可為每個要新增至資源的標籤指定標籤鍵 (keyvalue) 和選擇性標籤值 ()。與Create操作和命令的情況一樣，該tags參數指定標籤鍵及其關聯標籤值的string-to-string映射。

例如，下列AWS CLI命令會將含有Stack標籤值的Production標籤鍵加入至指定的工作。此範例針對 Microsoft Windows 進行格式化，並使用脫字符號 (^) 行接續字元來提高可讀性。

```
C:\> aws macie2 tag-resource ^
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-
job/3ce05dbb7ec5505def334104bexample ^
--tags={\"Stack\":\"Production\"}
```

其中：

- resource-arn指定要加入標籤的工作 ARN。
- *Stack*是要加入至工作之標籤的標籤鍵。
- *Production*是指定標籤鍵的標籤值 (*Stack*)。

在下列範例中，指令會將數個標籤新增至工作：

```
C:\> aws macie2 tag-resource ^
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-
job/3ce05dbb7ec5505def334104bexample ^
--tags={\"Stack\":\"Production\",\"CostCenter\":\"12345\",\"Owner\":\"jane-doe\"}
```

對於tags地圖中的每個標籤，key和參value數都是必需的。不過，value引數的值可以是空字串。如果您不想將標籤值與標籤鍵建立關聯，請不要指定value引數的值。例如，下列AWS CLI命令會加入沒有關聯Owner標籤值的標籤鍵：

```
C:\> aws macie2 tag-resource ^
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-
job/3ce05dbb7ec5505def334104bexample ^
--tags={\"Owner\":\"\"}
```

如果一個標記操作成功，馬西返回一個空的 HTTP 204 響應。否則，馬西會傳回 HTTP 4 xx 或 500 回應，指出作業失敗的原因。

查看亞馬遜 Macie 資源的標籤

您可以使用亞馬遜 Macie 主控台或亞馬遜 Macie API 來檢閱 Amazon Macie 資源的標籤 (標籤金鑰和標籤值)。如果您希望同時針對多個 Macie 資源執行此操作，可以使用AWS Resource Groups主控台上的「標籤編輯器」或「標記 API」的標AWS Resource Groups記作業。

Console

請依照下列步驟使用 Amazon Macie 主控台檢閱資源的標籤。

若要檢閱資源的標籤

1. 在以下位置打開亞馬遜麥西亞控制台 https://console.aws.amazon.com/macie/。
2. 根據您要檢閱其標籤的資源類型，執行下列其中一項作業：

   - 對於允許清單，請在導覽窗格中選擇 [允許清單]。

     然後，在表格中選取清單的核取方塊。然後選擇「動作」功能表上的 「管理標籤」
   - 對於自訂資料識別碼，請在導覽窗格中選擇 [自訂資料識別碼]。

     然後，在表格中，選取自訂資料識別碼的核取方塊。然後選擇「動作」功能表上的 「管理標籤」
   - 對於篩選或抑制規則，請在導覽窗格中選擇「發現項目」。

     然後，在「儲存的規則」清單中，選擇規則旁邊的編輯圖示
     (
)。
     然後選擇管理標籤。

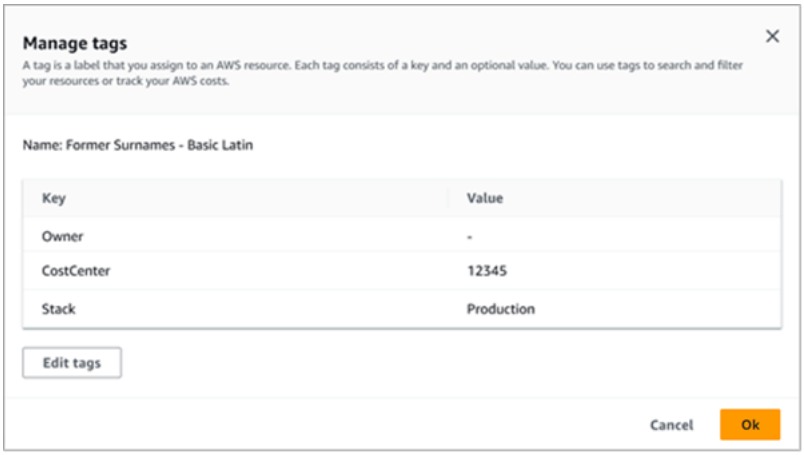
- 對於組織中的成員帳戶，請在導覽窗格中選擇 [帳戶]。

  然後，在表格中選取帳戶的核取方塊。然後選擇「動作」功能表上的 「管理標籤」

- 對於敏感性資料探索工作，請在導覽窗格中選擇「工作」。

  然後，在表格中選取工作的核取方塊。然後選擇「動作」功能表上的 「管理標籤」

[管理標籤] 視窗會列出目前指定給資源的所有標籤。例如，以下影像展示了指派給自訂資料識別碼的標籤。



在此範例中，會將三個標籤指派給自訂資料識別碼：沒有關聯標籤值的擁有者標CostCenter籤鍵；以 12345 作為關聯標籤值的標籤鍵；以及將生產作為關聯標籤值的 Stack 標籤鍵。

3. 完成檢閱標籤後，請選擇「取消」以關閉視窗。

API

若要以程式設計方式擷取和檢閱現有資源的標籤，您可以針對要檢閱標籤的資源類型使用適當的`Get`或`Describe`作業。例如，如果您使用GetCustomDataIdentifier作業或從 AWS Command Line Interface (AWS CLI) 執行get-custom-data-identifier命令，則回應會包含一個`tags`物件。物件會列出目前指派給資源的所有標籤 (包括標籤鍵和標籤值)。

您也可以使用亞馬遜梅西 API 的ListTagsForResource操作。在您的請求中，使用`resourceArn`參數來指定資源的 Amazon 資源名稱 (ARN)。如果您使用的是AWS CLI，請執行list-tags-for-resource命令並使用`resource-arn`參數來指定資源的 ARN。例如：

```
C:\> aws macie2 list-tags-for-resource --resource-arn arn:aws:macie2:us-
east-1:123456789012:classification-job/3ce05dbb7ec5505def334104bexample
```

在前面的範例中，*ARN: AWS: ## 2##### 1:123456789012##### /3ce05dbb7* ec5505def334104 比例是現有敏感資料探索工作的 ARN。

如果作業成功，Macie 會傳回一個tags物件，列出目前指定給資源的所有標籤 (包括標籤鍵和標籤值)。例如：

```
{
    "tags": {
        "Stack": "Production",
        "CostCenter": "12345",
        "Owner": ""
    }
}
```

其中StackCostCenter、和Owner是指派給資源的標籤鍵。 Production是與標籤鍵相關聯的標Stack籤值。 12345是與標籤鍵相關聯的標CostCenter籤值。標Owner籤鍵沒有關聯的標籤值。

若要擷取具有標籤的所有 Macie 資源清單，以及指派給每個資源的所有標籤，請使用標AWS Resource Groups記 API 的GetResources作業。在您的請求中，將ResourceTypeFilters參數的值設定為macie2。若要使用執行此操作AWS CLI，請執行 get-resources 命令，並將resource-type-filters參數的值設定為。macie2例如：

```
C:\> aws resourcegroupstaggingapi get-resources --resource-type-filters "macie2"
```

如果作業成功，資源群組會傳回一個ResourceTagMappingList陣列，其中包含所有具有標籤之 Macie 資源的 ARN，以及指派給這些資源的標籤鍵和值。

編輯亞馬遜 Macie 資源的標籤

若要編輯亞馬遜 Macie 資源的標籤 (標籤金鑰或標籤值)，您可以使用亞馬遜 Macie 主控台或亞馬遜 Macie API。若要同時針對多個 Macie 資源執行此操作，請使用AWS Resource Groups主控台上的「標籤編輯器」或「標記 API」的標AWS Resource Groups記作業。

> **Important**
>
> 編輯資源的標籤可能會影響資源的存取。在編輯資源的標籤金鑰或值之前，請先檢閱任何可能使用標籤來控制資源存取權的 AWS Identity and Access Management (IAM) 政策。

Console

請依照下列步驟使用 Amazon Macie 主控台編輯資源的標籤。

若要編輯資源的標籤

1. 在以下位置打開亞馬遜麥西亞控制台 https://console.aws.amazon.com/macie/。
2. 根據您要編輯其標籤的資源類型，執行下列其中一項作業：

   - 對於允許清單，請在導覽窗格中選擇 [允許清單]。

     然後，在表格中選取清單的核取方塊。然後選擇「動作」功能表上的 「管理標籤」
   - 對於自訂資料識別碼，請在導覽窗格中選擇 [自訂資料識別碼]。

     然後，在表格中，選取自訂資料識別碼的核取方塊。然後選擇「動作」功能表上的 「管理標籤」
   - 對於篩選或抑制規則，請在導覽窗格中選擇「發現項目」。

     然後，在「儲存的規則」清單中，選擇規則旁邊的編輯圖示 (✎)。然後選擇管理標籤。
   - 對於組織中的成員帳戶，請在導覽窗格中選擇 [帳戶]。

     然後，在表格中選取帳戶的核取方塊。然後選擇「動作」功能表上的 「管理標籤」
   - 對於敏感性資料探索工作，請在導覽窗格中選擇「工作」。

     然後，在表格中選取工作的核取方塊。然後選擇「動作」功能表上的 「管理標籤」

   [管理標籤] 視窗會列出目前指定給資源的所有標籤。
3. 在「管理標籤」視窗中，選擇 「編輯標籤」。
4. 執行下列任何一項：

   - 若要將標籤值加入至標籤關鍵字，請在標籤關鍵字旁的「值」方塊中輸入值。
   - 若要變更現有的標籤關鍵字，請選擇標籤旁邊的「移除」。然後選擇「新增標籤」。在出現的「關鍵字」方塊中，輸入新的標籤關鍵字。選擇性地在「值」方塊中輸入關聯的標籤值。
   - 若要變更現有標籤值，請在包含該值的「值」方塊中選擇「X」。然後在「值」方塊中輸入新標籤值。

- 若要移除現有的標籤值，請在包含該值的「值」方塊中選擇「X」。
- 若要移除現有標籤 (包括標籤鍵值和標籤值)，請選擇標籤旁邊的「移除」。

資源最多可以擁有 50 個標籤。標籤金鑰最多可包含 128 個字元。標籤值最多可包含 256 個字元。字符可以是字母，數字，空格或以下符號：_。：/= +-@

5. 編輯完標籤後，請選擇 [儲存]。

API

當您以程式設計方式編輯資源的標籤時，會以新值覆寫現有標籤。因此，編輯標籤的最佳方式取決於您要編輯標籤鍵、標籤值還是兩者。若要編輯標籤關鍵字，請移除目前的標籤並新增標籤。

若只要編輯或移除與標籤金鑰關聯的標籤值，請使用 Amazon Macie API 的TagResource作業覆寫現有值，或者，如果您使用的是 AWS Command Line Interface (AWS CLI)，則執行標籤資源命令。在您的請求中，指定要編輯或移除其標籤值的資源的 Amazon 資源名稱 (ARN)。

若要編輯標籤關鍵字的標籤值，請使用`tags`參數指定要變更其標籤值的標籤鍵，並指定鍵的新標籤值。例如，下列命令會`Production`將指派給指定敏感資料探索工作的`Stack`標籤索引鍵的標籤值從變更`Staging`為。此範例針對 Microsoft Windows 進行格式化，並使用脫字符號 (^) 行接續字元來提高可讀性。

```
C:\> aws macie2 tag-resource ^
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-
job/3ce05dbb7ec5505def334104bexample ^
--tags={\"Stack\":\"Staging\"}
```

其中：

- `resource-arn`指定工作的 ARN。
- *`Stack`*是與要變更的標籤值相關聯的標籤鍵。
- *`Staging`*是指定標籤鍵的新標籤值 (*`Stack`*)。

若要從標籤鍵移除標籤值，請勿在參數中指定`value`引`tags`數的值。例如：

```
C:\> aws macie2 tag-resource ^
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-
job/3ce05dbb7ec5505def334104bexample ^
```

```
--tags={\"Stack\":\"\"}
```

如果操作成功，馬西返回一個空的 HTTP 204 響應。否則，馬西會傳回 HTTP 4 xx 或 500 回應，指出作業失敗的原因。

從亞馬遜 Macie 資源刪除標籤

要從亞馬遜 Macie 資源中刪除標籤，您可以使用亞馬遜 Macie 控制台或亞馬遜 Macie API。若要同時針對多個 Macie 資源執行此操作，請使用AWS Resource Groups主控台上的「標籤編輯器」或「標記 API」的標AWS Resource Groups記作業。

> **Important**
>
> 從資源中移除標籤可能會影響對資源的存取。移除標籤之前，請先檢閱任何可能使用標籤控制資源存取權的 AWS Identity and Access Management (IAM) 政策。

Console

請依照下列步驟使用 Amazon Macie 主控台從資源移除一或多個標籤。

若要從資源中移除標籤

1. 在以下位置打開亞馬遜麥西亞控制台 https://console.aws.amazon.com/macie/。
2. 根據您要從中移除標籤的資源類型，執行下列其中一個動作：
   - 對於允許清單，請在導覽窗格中選擇 [允許清單]。

     然後，在表格中選取清單的核取方塊。然後選擇「動作」功能表上的 「管理標籤」
   - 對於自訂資料識別碼，請在導覽窗格中選擇 [自訂資料識別碼]。

     然後，在表格中，選取自訂資料識別碼的核取方塊。然後選擇「動作」功能表上的 「管理標籤」
   - 對於篩選或抑制規則，請在導覽窗格中選擇「發現項目」。

     然後，在「儲存的規則」清單中，選擇規則旁邊的編輯圖示 ( )。
     然後選擇管理標籤。

- 對於組織中的成員帳戶，請在導覽窗格中選擇 [帳戶]。

  然後，在表格中選取帳戶的核取方塊。然後選擇「動作」功能表上的 「管理標籤」
- 對於敏感性資料探索工作，請在導覽窗格中選擇「工作」。

  然後，在表格中選取工作的核取方塊。然後選擇「動作」功能表上的 「管理標籤」

[管理標籤] 視窗會列出目前指定給資源的所有標籤。

3. 在「管理標籤」視窗中，選擇 「編輯標籤」。
4. 執行下列任何一項：
   - 若只要移除標籤的標籤值，請在包含要移除之值的「值」方塊中選擇「X」。
   - 若要同時移除標籤的標籤鍵和標籤值 (成對)，請選擇要移除的標籤旁邊的「移除」。
5. (選擇性) 若要從資源中移除更多標籤，請針對每個要移除的其他標籤重複上述步驟。
6. 完成移除標籤後，請選擇 [儲存]。

API

若要以程式設計方式從資源中移除一或多個標籤，請使用 Amazon Macie API 的UntagResource操作。在您的請求中，使用`resourceArn`參數指定要從中移除標籤的資源的 Amazon 資源名稱 (ARN)。使用`tagKeys`參數指定要移除之標籤的標籤鍵。若只要從資源中移除特定標籤值 (而非標籤鍵)，請編輯標籤，而不要移除標籤。

如果您使用的是 AWS Command Line Interface (AWS CLI)，請執行 untag-resource 命令，並使用`resource-arn`參數指定要從中移除標籤的資源 ARN。使用`tag-keys`參數指定要移除之標籤的標籤鍵。例如，下列命令會從指定的敏感資料探索工作中移除標`Stack`籤 (標籤索引鍵和標籤值)：

```
C:\> aws macie2 untag-resource ^
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-
job/3ce05dbb7ec5505def334104bexample ^
--tag-keys Stack
```

其中`resource-arn`指定要從中刪除標籤的作業的 ARN，並且`Stack`是要刪除的標籤的標籤鍵。

要從資源中刪除多個標籤，請添加每個額外的標籤鍵作為`tag-keys`參數的引數。例如：

```
C:\> aws macie2 untag-resource ^
```

```
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-
job/3ce05dbb7ec5505def334104bexample ^
--tag-keys Stack Owner
```

其中resource-arn指定要從中刪除標籤的作業的 ARN，並*Stack*且*Owner*是要刪除的標籤的標籤鍵。

如果操作成功，馬西返回一個空的 HTTP 204 響應。否則，馬西會傳回 HTTP 4 xx 或 500 回應，指出作業失敗的原因。

創建 Amazon Macie 資源與 AWS CloudFormation

Amazon Macie C已整合AWS CloudFormation，這項服務可協助您建立AWS資源的模型和設定，以減少建立和管理資源和基礎設施的時間。您可以建立一個範本，描述所有所需的AWS資源 (例如，自訂資料識別碼)，會為您AWS CloudFormation佈建和設定這些資源。

當您使用時AWS CloudFormation，您可以重複使用您的範本，重複、一致的設定您的 Macie C。只需描述一次您的資源，即可重AWS 帳戶複佈建相同資源AWS 區域。

主題

- Amazon Macie Cas和AWS CloudFormation範本
- 進一步了解 AWS CloudFormation

Amazon Macie Cas和AWS CloudFormation範本

若要佈建和配置 Amazon Macie 和相關服務的資源，則必須了解AWS CloudFormation範本。範本是以 JSON 或 YAML 格式化的文本檔案。而您亦可以透過這些範本的說明，了解欲在 AWS CloudFormation 堆疊中佈建的資源。

如果您不熟悉 JSON 或 YAML，則可以使用 AWS CloudFormation Designer。Designer 是一種圖形工具，能讓使用者建立與修改AWS CloudFormation範本。使用 Designer，您可以使用drag-and-drop介面繪製範本資源的圖表，然後使用整合式 JSON 和 YAML 編輯器編輯它們的詳細資訊。如需詳細資訊，請參閱 AWS CloudFormation 使用者指南中的什麼是 AWS CloudFormation Designer？。

您可以為下列類型的 Macie 資源建立AWS CloudFormation範本：

- 允許清單
- 自訂資料識別符
- 發現項目的篩選規則和抑制規則，也稱為發現項目篩選器

如需詳細資訊，包括這些資源類型的 JSON 和 YAML 範本範例，請參閱AWS CloudFormation使用者指南中的 Amazon Macie 資源類型參考資料。

進一步了解 AWS CloudFormation

若要進一步了解AWS CloudFormation，請參閱下列資源：

- AWS CloudFormation
- 《AWS CloudFormation 使用者指南》https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/Welcome.html
- AWS CloudFormation API 參考
- 《AWS CloudFormation 命令列介面使用者指南》https://docs.aws.amazon.com/cloudformation-cli/latest/userguide/what-is-cloudformation-cli.html

暫停或禁用亞馬遜 Macie

您可以暫停或禁用亞馬遜 Macie 在特定AWS 區域通過使用亞馬遜 Macie 控制台或亞馬遜 Macie API。然後，Macie 停止為您在該地區的帳戶執行所有活動。當該地區暫停或停用時，您無需支付使用 Macie 的費用。

如果您暫停或停用 Macie，您可以稍後重新啟用它。

主題

暫停亞馬遜瑪西

如果您暫停 Amazon Macie，Macie 會在適用的情況下保留您帳戶的工作階段識別碼、設定和資源 AWS 區域。例如，您現有的發現項目會保持完整，並保留最多 90 天。但是，當您暫停 Macie 時，它會停止在適用地區為您的帳戶執行所有活動。這包括監控您的 Amazon 簡單儲存服務 (Amazon S3) 資料、執行自動化敏感資料探索，以及執行目前正在進行的任何敏感資料探索任務。Macie 也會取消您在該地區的所有敏感資料探索工作。

暫停 Macie 後，您可以重新啟用它。然後，您可以重新取得適用地區中設定和資源的存取權，Macie 會繼續為您在該地區的帳戶進行活動。這包括更新您帳戶的 S3 儲存貯體庫存，並監控這些儲存貯體，以確保安全性和存取控制。這不包括繼續或重新啟動敏感資料探索工作。取消敏感資料探索工作後，便無法繼續或重新啟動。

本主題說明如何使用 Amazon Macie 主控台暫停 Macie。如果您偏好以程式設計方式執行此操作，可以使用UpdateMacieSession亞馬遜梅西 API 的操作。

> **Note**
>
> 如果您是某個組織的 Macie 管理員，您必須先移除與您帳戶相關聯的所有成員帳戶，然後才能將您的帳戶暫停 Macie。如需詳細資訊，請參閱管理多個 帳戶。

暫停馬西

1. 打開亞馬遜 Macie 控制台https://console.aws.amazon.com/macie/。
2. 通過使用AWS 區域選擇在頁面的右上角，選擇要暫停 Macie 的區域。

3. 在導覽窗格中，選擇 Settings (設定)。
4. 選擇暫停麥西。
5. 當系統提示您確認時，請輸入**Suspend**，然後選擇暫停。

若要在其他區域中暫停 Macie，請在每個額外的區域中重複上述步驟。

禁用亞馬遜麥西

當您禁用亞馬遜 Macie，Macie 停止執行所有活動為您的帳戶在適用AWS 區域。這包括監控您的 Amazon 簡單儲存服務 (Amazon S3) 資料、執行自動化敏感資料探索，以及執行目前正在進行的任何敏感資料探索任務。Macie 也會刪除在適用區域中為您的帳戶儲存或維護的所有現有設定和資源，包括您的發現項目和敏感資料探索工作。您儲存或發佈給其他人的資料AWS 服務保持完整且不受影響 — 例如，敏感資料探索會導致 Amazon S3 並在 Amazon 中尋找事件EventBridge。

> **Warning**
>
> 如果您停用 Macie，您也會永久刪除所有現有的發現項目、敏感資料探索工作、自訂資料識別碼，以及 Macie 在適用區域中為您的帳戶儲存或維護的其他資源。刪除這些資源後無法復原。要保留資源並僅暫停使用 Macie，請暫停 Macie 而不是禁用它。

本主題說明如何使用 Amazon Macie 主控台停用 Macie。如果您偏好以程式設計方式執行此操作，可以使用DisableMacie亞馬遜梅西 API 的操作。

> **Note**
>
> 如果您的帳戶屬於集中管理多個 Macie 帳戶的組織，您必須先執行下列動作，才能停用 Macie：
>
> - 如果您的帳戶是 Macie 會員帳戶，請與您的 Macie 管理員合作，以成員帳戶的身分移除您的帳戶。
> - 如果您的帳戶是 Macie 管理員帳戶，請刪除與您的帳戶相關聯的所有成員帳戶，並刪除您的帳戶與這些帳戶之間的關聯。
>
> 您如何完成上述任務取決於您的 Macie 帳戶是否通過與其他帳戶關聯AWS Organizations或通過邀請。如需詳細資訊，請參閱管理多個 帳戶。

要禁用馬西

1. 打開亞馬遜 Macie 控制台https://console.aws.amazon.com/macie/。
2. 通過使用AWS 區域選擇在頁面的右上角，選擇要禁用 Macie 的區域。
3. 在導覽窗格中，選擇 Settings (設定)。
4. 選擇禁用馬西。
5. 當系統提示您確認時，請輸入**`Disable`**，然後選擇停用。

若要在其他區域中停用 Macie，請在每個額外的區域中重複上述步驟。

Amazon Macie 配額

您的每個配額都AWS 帳戶有特定的預設配額 (先前稱為限制) AWS 服務。這些配額是您帳戶的服務資源或作業數目上限。本主題列出適用於您帳戶的 Amazon Macie 資源和操作的配額。除非另有說明，否則每個配額都適用於您的帳戶AWS 區域。

有些配額可以增加，有些則無法增加。若要要求增加配額，請使用 Service Quotas 主控台。若要瞭解如何要求提高配額，請參閱 Service Quotas 使用者指南中的要求增加配額。如果 Service Quiz 主控台上無法使用配額，請使用上的服務限制增加表單AWS Support Center Console來要求提高配額。

帳戶

- 受邀請的會員帳號：1,000 個
- 會員帳戶數目AWS Organizations：1 萬

問題清單

- 每個帳戶過濾規則和抑制規則：1,000
- 敏感性資料探索工作每次執行的發現項目：滿足 100,000 個閾值後剩餘發現項目的 100,000 + 5%

  此配額僅適用於 Amazon Macie 控制台和 Amazon Macie API。Macie 發佈到 Amazon 的尋找事件數量 EventBridge 或 Macie 為每次執行任務所建立的敏感資料探索結果數量沒有配額。
- 每個敏感數據發現的檢測位置：15
- 從 Amazon S3 物件擷取和揭露敏感資料樣本的請求：每天 100 個

  此配額會每 24 小時於下午 0 時重設一次。
- 要從下列位置擷取和顯示敏感資料樣本的 Amazon S3 物件大小：
  - 阿帕奇阿夫羅對象容器（.avro）文件：70 MB
  - 阿帕奇鑲木地板（.鑲木地板）文件：100 MB
  - CSV 檔案：255 MB
  - GNU 壓縮壓縮存檔（.gz 或 .gzip）文件：90 MB
  - JSON 或 JSON 行 (.json 或 .jsonl) 檔案：25 MB
  - Microsoft Excel 工作簿（.xlsx）文件：20 MB
  - 非二進位文字 (text/plain) 檔案：100 MB
  - TSV (.tsv) 檔案:75 MB

- 壓縮壓縮封存檔 (.zip) 檔案:355 MB

  如果發現項目適用於針對對應敏感資料探索結果產生多個 .gz 檔案的封存檔案，則無法從封存檔中擷取和顯示敏感資料範例。

敏感資料探索

- 每個帳戶按敏感資料探索工作進行的每月分析：5 TB

  此配額僅適用於敏感資料探索工作。若要將配額增加到最多 1,000 TB (1 PB)，請使用 Service Quotas 主控台。若要要求提高超過 1 PB，請使用上的服務限制提高表單AWS Support Center Console。
- 每個帳戶的自訂資料識別碼：10,000 個
- 允許每個帳戶的清單：10、1—5 允許指定預先定義文字的清單和 1—5 允許指定規則運算式的清單

  其他配額適用於指定預先定義文字的允許清單。清單不能包含超過 100,000 個項目，且清單的儲存空間大小不得超過 35 MB。
- 要從自動化敏感資料探索中排除的 S3 儲存貯體：1,000 個

  如果您的帳戶是組織的 Macie 管理員帳戶，則此配額會套用至您的組織。
- 每個敏感資料探索任務的 S3 儲存貯體：1,000 個

  此配額不適用於使用執行時期值區條件來決定要分析哪些值區的工作。只有當您將工作設定為分析您選取的特定值區時，才會套用至工作。如果您的帳戶是組織的 Macie 管理員帳戶，您可以選取多達 1,000 個值區，跨越組織中多達 1,000 個帳戶。
- 每個敏感資料探索工作的自訂資料識別碼：30
- 允許每個敏感性資料探索工作的清單：10、1—5 允許指定預先定義文字的清單和 1—5 允許指定規則運算式的清單
- CreateClassificationJob操作：每秒 0.1 個請求
- 分析個別檔案的時間：10 小時
- 要分析的個別檔案大小：
  - 土坯可攜式文件格式 (.pdf) 檔案:1,024 MB
  - 阿帕奇阿夫羅對象容器（.avro）文件：8 GB
  - 阿帕奇鑲木地板（.鑲木地板）文件:8 GB
  - 電子郵件訊息 (.eml) 檔案：20 GB

  - GNU 壓縮壓縮封存檔 (.gz 或 .gzip) 檔案:8 GB
  - Microsoft Excel 工作簿（.xls 或 .xlsx）文件：512 MB
  - Microsoft Word 文檔（文檔或 .docx）文件：512 MB
  - 非二進位文字檔案：20 GB
  - TAR 封存檔 (.tar) 檔案：20 GB
  - 壓縮壓縮封存檔 (.zip) 檔案:8 GB

  如果檔案大於適用的配額，Macie 就不會分析檔案中的任何資料。
- 提取和分析壓縮或歸檔文件中的數據：
  - 儲存空間大小 (壓縮)：8 GB 的 GNU 壓縮封存檔案 (.gz 或 .gzip) 檔案或 ZIP 壓縮封存檔 (.zip) 檔案；TAR 封存檔 (.tar) 檔案需要 20 GB 的空間
  - 嵌套歸檔深度：10 級
  - 解壓縮的檔案：100 萬
  - 擷取的位元組：整體 10 GB 的未壓縮資料。每個使用支援的檔案類型或儲存格式的解壓縮檔案會有 3 GB 的未壓縮資料。

  如果壓縮檔案或封存檔案的中繼資料指出檔案包含 10 個以上的巢狀層級，或超過儲存大小或擷取位元組的適用配額，Macie 就不會擷取或分析檔案中的任何資料。如果 Macie 開始擷取和分析壓縮檔案或封存檔案中的資料，然後判斷檔案包含超過 1,000,000 個檔案或超過擷取位元組的配額，Macie 會停止分析檔案中的資料，並僅針對已處理的資料建立敏感資料發現項目和探索結果。
- 分析結構化資料中的巢狀元素：每個檔案 256 層

  此配額僅適用於 JSON (.json) 和 JSON 行 (.jsonl) 檔案。如果任一類型檔案的巢狀深度超過此配額，Macie 就不會分析檔案中的任何資料。
- 每個敏感資料探索結果的偵測位置：每種敏感資料偵測類型 1,000 個
- 檢測全名：每個文件 1,000 個，包括存檔文件

  Macie 在檔案中偵測到前 1,000 次出現的全名後，Macie 會停止遞增計數並報告全名的位置資料。
- 偵測郵寄地址：每個檔案 1,000 個，包括封存檔案

  Macie 在檔案中偵測到前 1,000 次出現的郵寄地址之後，Macie 就會停止遞增郵寄地址的計數和報告位置資料。

Amazon Macie 用戶指南的文檔歷史記錄

下表說明自上次發行 Amazon Macie 以來文件的重要變更。如需有關此文件更新的通知，您可以訂閱 RSS 訂閱源。

最新文件更新：2024 年 6 月 14 日

變更	描述	日期
新功能	如果您是組織的委派 Macie 管理員，您現在可以為組織中的個別帳戶啟用或停用自動化敏感資料探索功能。有了這個額外選項，您現在可以透過數種方式定義分析範圍：為所有帳戶啟用自動探索、選擇性地啟用特定帳戶的自動化探索，以及排除特定 S3 儲存貯體。	2024年6月14日
新功能	AWS Security Hub 現在提供安全控制，可檢查 Macie 的狀態，並自動探索帳戶的敏感資料。如果啟用這些控制項，Security Hub 會定期執行安全性檢查，以判斷是否為 AWS 帳戶 (Mac ie.1 控制項) 啟用 Mac ie，以及是否為 Macie 帳戶 (Macie.2 控制項) 啟用自動敏感資料探索。	2024年2月20日
新功能	Macie 現在可以分析使用雙層伺服器端加密 AWS KMS keys (DSSE-KMS) 加密的 Amazon S3 物件。當 Macie 執行自動化敏感資料探索或您執行敏感資料探索工作時，這些物件現在可以進行分析。此外，使用	2024年1月17日

	DSSE-KMS 加密的 S3 儲存貯體和物件現在也包含在 Macie 提供的有關 Amazon S3 資料的統計資料和中繼資料中。	
新功能	現在，您可以將 Macie 設定為在您選擇擷取和顯示 Macie 在發現項目中報告的敏感資料樣本時承擔 AWS Identity and Access Management (IAM) 角色。這些範例可協助您驗證 Macie 找到的敏感資料的性質，並針對受影響的 Amazon S3 物件和儲存貯體量身打造調查。	2023 年 11 月 16 日
新功能	Macie 現在提供託管數據標識符，旨在檢測其他 47 個國家和地區的國際銀行帳戶號碼（IBAN）。現在，您可以使用 Macie 來檢測和報告超過 50 個國家和地區的 IBAN 發生。	2023 年 11 月 1 日
新功能	Macie 現在提供受管資料識別碼，這些識別碼旨在偵測以下類型的敏感資料：Google Cloud API 金鑰、Stripe API 金鑰和 Aadhaar 號碼、永久帳戶號碼 (PAN)，以及印度的駕駛執照識別碼。	2023 年 9 月 25 日

新配額	為了協助您驗證發現項目所報告之敏感資料的性質，我們增加了從 Amazon S3 物件擷取和揭露敏感資料樣本的大小配額。您現在可以從儲存大小超過 10 MB 的 S3 物件擷取和顯示範例。如需新配額的清單，請參閱 Amazon Macie 配額。	2023 年 9 月 7 日
區域可用性	以色列（特拉維夫）地區現已推出 Macie。如需 Macie 目前可用 AWS 區域 位置的完整清單，請參閱. AWS 一般參考	2023 年 8 月 28 日
已更新的功能	我們實作了一組新的動態預設受管資料識別碼，用於自動化敏感資料探索。預設集包括我們建議用於自動化敏感資料探索的受管資料識別碼。它旨在檢測敏感數據的常見類別和類型，同時優化您的自動化敏感數據發現結果。	2023 年 8 月 2 日
已更新的功能	為了協助您找出 Macie 在敏感資料發現項目和敏感資料探索結果中所報告之敏感資料的出現次數，我們將`Record`物件中 JSON 路徑元素名稱的字元限制從 20 變更為 240。這項變更會影響 Apache Avro 物件容器、Apache 拼花檔案、JSON 檔案和 JSON 行檔案的新敏感資料發現項目和探索結果。	2023 年 7 月 24 日

已更新的功能	如果您是中組織的委派 Macie 管理員 AWS Organizations，您現在可以管理組織中多達 10,000 個帳戶的 Macie。	2023 年 6 月 30 日
新功能	您現在可以建立和設定敏感資料探索工作，以自動使用我們針對工作建議的受管理資料識別碼集。這組建議的受管資料識別碼是設計來偵測常見的敏感資料類別和類型，同時最佳化您的工作結果。	2023 年 6 月 28 日
新政策	我們新增了一個新的AWS 受管理原則，即AmazonMacieReadOnlyAccess 原則。此政策授予唯讀許可，允許 IAM 身分 (主體) 擷取其帳戶的所有 Macie 資源、資料和設定。	2023 年 6 月 15 日
新功能	為了協助您評估和監控 Amazon S3 資料的自動化敏感資料探索涵蓋範圍，Macie 主控台現在包含資源涵蓋範圍頁面。此頁面提供所有 S3 儲存貯體的涵蓋範圍統計資料和資料的統一檢視，包括最近針對每個儲存貯體發生的分析問題彙總 (如果有的話)。如果發生問題，頁面也會提供修正指引。	2023 年 5 月 15 日

新功能	Macie 集成了 AWS 使用者通知, 這是一個新 AWS 服務的，充當您的 AWS 通知的中心位置. AWS Management Console使用 使用者通知，您可以設定自訂規則和交付管道，以產生和傳送有關 Macie 針對政策和敏感資料發現的 Amazon EventBridge 事件發佈的通知。	2023 年 5 月 5 日
已更新內容	更新 Macie 針對 S3 儲存貯體預設加密設定提供的統計資料和中繼資料說明。也更新了Policy:IAMUser/S3BucketEncryptionDisabled原則發現項目的描述。Amazon S3 現在會自動使用 Amazon S3 受管金鑰 (SSE-S3) 套用伺服器端加密，作為新增至新儲存貯體和現有儲存貯體之物件的基礎加密層級。如需 Amazon S3 中此變更的相關資訊，請參閱 Amazon 簡單儲存服務使用者指南中的設定 S3 儲存貯體的預設伺服器端加密行為。	2023 年 2 月 27 日

新功能	Macie 現在可以為 S3 儲存貯體產生其他類型的政策發現：Policy:IAMUser/S3BucketSharedWithCloudFront 。這種類型的發現項目表示儲存貯體的政策已變更，以允許儲存貯體與 Amazon CloudFront 原始存取身分 (OAI)、 CloudFront 原始存取控制 (OAC) 或兩者共用。此外，與 CloudFront OAI 或 OAC 共用的儲存貯體現在被視為在 Macie 提供有關 Amazon S3 資料的統計資料和中繼資料中外部共用。	2023 年 2 月 24 日
新功能	Macie 現在支援用於敏感資料探索的 Amazon S3 冰川即時擷取儲存類別。現在，當 Macie 執行自動化敏感資料探索或您執行敏感資料探索任務時，使用此儲存類別的 S3 物件即可進行分析。它們也被視為 Macie 提供有關 Amazon S3 資料的統計資料和中繼資料中的可分類物件。	2022 年 12 月 21 日

新功能	您現在可以設定 Macie 為您的帳戶或組織執行自動化敏感資料探索。透過自動化敏感資料探索功能，Macie 會持續評估您的 Amazon S3 資料，並使用取樣技術來識別、選取和分析 S3 儲存貯體中的代表物件，並檢查物件中的敏感資料。您可以使用 Macie 提供的有關 Amazon S3 資料的統計資料、發現項目和其他資訊來評估分析的結果。	2022 年 11 月 28 日
新功能	您現在可以建立並使用允許清單來指定 Macie 在檢查 Amazon S3 物件中是否有敏感資料時要忽略的文字和文字模式。透過使用允許清單，您可以針對特定案例或環境定義敏感資料例外，例如組織的公開代表姓名、特定電話號碼或組織用於測試的範例資料。	2022 年 8 月 30 日
新功能	若要驗證 Macie 在 S3 物件中找到的敏感資料本質，您現在可以設定並使用 Macie 擷取發現項目所報告之敏感資料的樣本。	2022 年 7 月 26 日
已更新的功能	在AmazonMacieFullAccess政策中，我們更新了 Macie 服務連結角色 () 的 Amazon 資源名稱 (ARN)。`aws-service-role/macie.amazonaws.com/AWSServiceRoleForAmazonMacie`	2022 年 6 月 30 日

已更新的功能	我們已更新AmazonMacieServiceRolePolicy原則，也就是附加至 Macie 服務連結角色 () AWSServiceRoleForAmazonMacie 的原則。該政策不再為 Amazon Macie 經典版指定動作和資源。Amazon Macie 經典已停產，不再可用。	2022 年 5 月 20 日
新功能	Macie 現在會在其發佈至 AWS Security Hub的敏感資料發現項目中包含OriginType 欄位。此OriginType 欄位指定 Macie 如何找到產生發現項目的機密資料。	2022 年 5 月 11 日
已更新內容	說明了關鍵字和最大匹配距離設置如何為自定義數據標識符工作。	2022 年 4 月 22 日
新功能	Macie 現在提供受管理的資料識別碼，這些識別碼旨在偵測 HTTP 基本授權標頭、HTTP Cookie 和 JSON 網頁權杖。	2022 年 4 月 21 日
新內容	新增 Macie 關鍵概念和術語的說明和定義。	2022 年 3 月 16 日

新功能	為了計算並顯示您在建立和設定敏感資料探索工作時的估計成本，Macie 現在會 AWS 帳戶 從中 AWS Billing and Cost Management擷取定價資料。為了支援此功能，我們在AmazonMacieFullAccess政策中新增了 Billing and Cost Management 動作。	2022 年 3 月 7 日
新功能	Macie 現在會在發佈至 AWS Security Hub的發現項目中包含該Sample欄位。此Sample欄位會指定尋找項目是否為範例發現項目。	2022 年 2 月 24 日
新內容	已新增有關使用 Amazon Virtual Private Cloud 在 VPC 和 Macie 之間建立私有連線的資訊。	2022年1月19日
新功能	您現在可以使用 Amazon Macie 主控台來指派和管理自訂資料識別碼的標籤、篩選和抑制發現項目的規則、敏感資料探索任務，以及 (如果您是組織的 Macie 管理員)，則可以使用組織中的成員帳戶。標籤是您選擇性地定義並指派給特定 AWS 資源類型的標籤。	2022 年 1 月 12 日
新內容	已新增有關使用 AWS Identity and Access Management來管理 Macie 存取權的資訊。	2021 年 12 月 20 日

新功能	當您建立自訂資料識別碼時，您現在可以為其產生的敏感資料發現項目定義嚴重性設定。使用這些設定，您可以根據符合自訂資料識別碼偵測準則的文字出現次數，指定要指派給發現項目的嚴重性。	2021 年 11 月 4 日
新功能	若要瞭解 Macie 提供的不同類型發現項目，您可以產生範例發現項目。範例發現項目會使用範例資料和預留位置值來示範 Macie 可能包含在每一種發現項目類型中的資訊種類。	2021 年 10 月 28 日
新功能	Macie 現在會在發佈至 AWS Security Hub的發現項目中包含該OwnerAccountId 欄位。此欄位指定擁有受影響 S3 儲存貯體的帳戶 ID。 AWS 帳戶	2021 年 10 月 27 日
新內容	已新增集中管理多個 Macie 帳戶的相關資訊。您可以通過兩種方式完成此操作，通過將 Macie 與 Macie 集成 AWS Organizations 或通過發送來自 Macie 的會員邀請。	2021 年 10 月 13 日
新功能	S3 儲存貯體庫存現在會指出儲存貯體的許可設定是否阻止 Macie 擷取有關儲存貯體或儲存貯體物件的資訊，以及評估和監控儲存貯體資料的安全性和隱私權。此外，我們更新了對客戶管理金鑰 AWS KMS keys 的參考資料，以反映目前的術語。	2021 年 10 月 5 日

新功能	Macie 現在會將政策和敏感資料發現儲存 90 天，而非 30 天。如果 Macie 在 2021 年 8 月 31 日或之後建立或更新了發現項目，您可以使用 Macie 主控台或 Macie API 存取最多 90 天的發現項目。在某些情況下 AWS 區域，Macie 早在 2021 年 9 月 27 日開始保留 90 天的調查結果。	2021 年 10 月 1 日
新功能	當您建立敏感資料探索任務時，您現在可以指定任務分析 S3 物件時要使用的受管資料識別碼。使用此功能，您可以自訂工作的分析，以專注於特定類型的敏感資料。	2021 年 9 月 17 日
新功能	敏感資料發現現在會提供其他資訊，協助您在 JSON 和 JSON 行檔案中尋找敏感資料。	2021 年 7 月 6 日
已更新的功能	Macie 現在會在發佈至 AWS Security Hub的發現項目中使用`AwsS3Bucket` 資源類型。(Macie 先前將此值設定為`AWS::S3::Bucket` 。) `AwsS3Bucket` 是用於 AWS 安全性發現格式 (ASFF) 中 S3 儲存貯體的資源類型值。	2021 年 6 月 28 日

新功能	當您建立敏感資料探索任務時，您現在可以定義執行階段準則，以決定任務分析哪些 S3 儲存貯體。透過此功能，任務的分析範圍可以根據值區庫存的變更動態調整。	2021年5月15日
新功能	您的 S3 儲存貯體庫存和摘要儀表板現在提供加密中繼資料和統計資料，指出儲存貯體政策是否需要伺服器端加密新物此外，您現在可以針對值區詳細目錄中的個別值區執行物件中繼資料的隨選重新整理。	2021 年 4 月 30 日
新功能	您現在可以使用 Amazon CloudWatch Logs 監控和分析執行敏感資料探索任務時發生的事件。為了支援此功能，我們將 CloudWatch 記錄動作新增至 Macie 服務連結角色的 AWS 受管理原則。	2021 年 4 月 14 日
區域可用性	Macie 現已在 AWS 亞太區域 (大阪) 上市。	2021 年 4 月 5 日
新功能	您現在可以設定 Macie 將敏感資料發現項目發佈到 AWS Security Hub.	2021 年 3 月 22 日
新內容	已新增監控和預測 Macie 成本以及參與免費試用的相關資訊。	2021 年 2 月 26 日
已更新內容	我們用術語管理員帳戶取代了術語主帳戶。系統管理員帳戶可用來集中管理多個帳戶。	2021 年 2 月 12 日

新功能	您現在可以在自訂包含和排除條件中使用 S3 物件前置詞來調整敏感資料探索任務的範圍。	2021 年 2 月 2 日
已更新內容	Macie 現在會遵循「 AWS 安全性發現格式」(ASFF) 的尋找項目類型分類法，將原則發現項目發現項目發佈至。 AWS Security Hub	2021 年 1 月 28 日
新內容	已新增監控 Amazon S3 資料以及評估該資料安全性和隱私權的相關資訊。	2021 年 1 月 8 日
區域可用性	Macie 現已在 AWS 非洲 (開普敦) 地區、 AWS 歐洲 (米蘭) 和 AWS 中東 (巴林) 區域推出。	2020 年 12 月 21 日
新功能	如果您的帳戶是 Macie 管理員帳戶，您現在可以建立並執行敏感資料探索工作，分析組織中多達 1,000 個帳戶的 1,000 個儲存貯體的資料。	2020 年 11 月 25 日
新功能	S3 儲存貯體庫存現在會指出您是否已設定任何一次性或定期敏感資料探索任務來分析儲存貯體中的資料。如果有，它也會提供有關最近執行之工作的詳細資料。	2020 年 11 月 23 日
新內容	新增篩選發現項目的相關資訊	2020 年 11 月 12 日

新功能	敏感資料發現現在會提供其他資訊，協助您在 Apache Avro 物件容器、Apache 實體檔案和 Microsoft Excel 活頁簿中尋找敏感資料。	2020 年 11 月 9 日
新功能	您現在可以使用敏感資料發現項目來尋找 S3 物件中個別出現的敏感資料。	2020 年 10 月 22 日
新功能	您現在可以暫停和繼續敏感性資料探索工作。	2020 年 10 月 16 日
新內容	新增原則發現項目和敏感資料發現項目之嚴重性評分系統的詳細資訊。	2020 年 10 月 6 日
新功能	您現在可以檢視統計資料，指出當您執行敏感資料探索任務時，Macie 可以在個別 S3 儲存貯體中分析多少資料。此外，您現在可以在建立工作時檢視工作的估計成本。	2020 年 9 月 3 日
新內容	已新增設定、執行和管理敏感資料探索工作的相關資訊。	2020 年 8 月 31 日
新功能	受管理資料識別碼現在可以偵測巴西的特定類型的個人識別資訊。	2020 年 7 月 31 日
已更新內容	已新增有關自訂資料識別碼中規則運算式支援語法的資訊。	2020 年 7 月 30 日
已更新內容	已新增受管資料識別碼的關鍵字需求，並增加每個敏感資料探索工作可產生的發現項目數量配額。	2020 年 7 月 17 日

新內容	已新增使用 Amazon 的相關資訊， AWS Security Hub 以 EventBridge 及監控和處理發現項目。這包括發現項目的 EventBridge 事件結構描述，以及原則和敏感資料發現項目的事件範例。	2020 年 6 月 22 日
新內容	已新增有關分析和隱藏發現項目的資訊。	2020 年 6 月 17 日
新內容	已新增設定 Macie 以將詳細探索結果儲存在 S3 儲存貯體中的指示。	2020 年 6 月 2 日
新內容	已新增 Macie 可偵測之敏感資料類型的相關資訊，以及偵測 Amazon S3 物件中敏感資料的加密要求。	2020 年 5 月 28 日
一般可用性	這是 Amazon Macie 使用者指南的初始公開發行版本。	2020 年 5 月 13 日

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。