使用者指南

AWS 驗證存取

AWS 驗證存取: 使用者指南

Table of Contents

什麼是 AWS Verified Access？

使用 AWS Verified Access，您可以提供對應用程式的安全存取，而不需要使用虛擬私人網路 (VPN)。驗證存取會評估每個應用程式要求，並協助確保使用者只有在符合指定的安全性需求時才能存取每個應用程式。

驗證存取權的好處

- 改善安全性狀態 — 傳統安全性模型會評估存取一次，並授與使用者對所有應用程式的存取權。驗證存取會即時評估每個應用程式存取要求。這使得不良行為者難以從一個應用程序轉移到另一個應用程序。
- 與安全性服務整合 — 驗證存取功能與身分識別和裝置管理服務 (包括兩者 AWS 和第三方服務) 整合。使用來自這些服務的資料，驗證存取權會根據一組安全性需求來驗證使用者和裝置的可信度，並判斷使用者是否應該具有應用程式的存取權。
- 改善的使用者體驗 — 已驗證存取權讓使用者無需使用 a VPN 來存取您的應用程式。這有助於減少相VPN關問題引起的支援案例數量。
- 簡化疑難排解與稽核：驗證存取記錄所有存取嘗試，集中掌握應用程式存取權限，協助您快速回應安全性事件和稽核要求。

存取已驗證存取

您可以使用下列任何介面來使用已驗證存取權：

- AWS Management Console— 提供可用於建立和管理已驗證存取資源的 Web 介面。登錄 AWS Management Console 並在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
- AWS Command Line Interface (AWS CLI) — 提供一組廣泛的指令 AWS 服務，包括 AWS Verified Access。在視窗、macOS 和 Linux 上支援。 AWS CLI 若要取得 AWS CLI，請參閱AWS Command Line Interface。
- AWS SDKs— 提供特定語言APIs。會 AWS SDKs處理許多連線詳細資料，例如計算簽章，以及處理要求重試和錯誤。如需詳細資訊，請參閱AWS SDKs。
- 查詢 API — 提供您使用HTTPS要求呼叫的低階API動作。使用查詢API是訪問已驗證訪問的最直接的方法。但是，它會要求您的應用程式處理低階詳細資料，例如產生雜湊來簽署要求和處理錯誤。如需詳細資訊，請參閱 Amazon EC2 API 參考中的已驗證存取動作。

本指南說明如何使用 AWS Management Console 建立、存取和管理已驗證存取資源。

定價

在「已驗證存取」上，每個應用程式都會按小時向您收費，並按照已驗證存取處理的資料量向您收費。如需詳細資訊，請參閱 AWS Verified Access 定價。

驗證存取的運作方式

AWS Verified Access 評估使用者的每個應用程式要求，並根據下列項目允許存取：

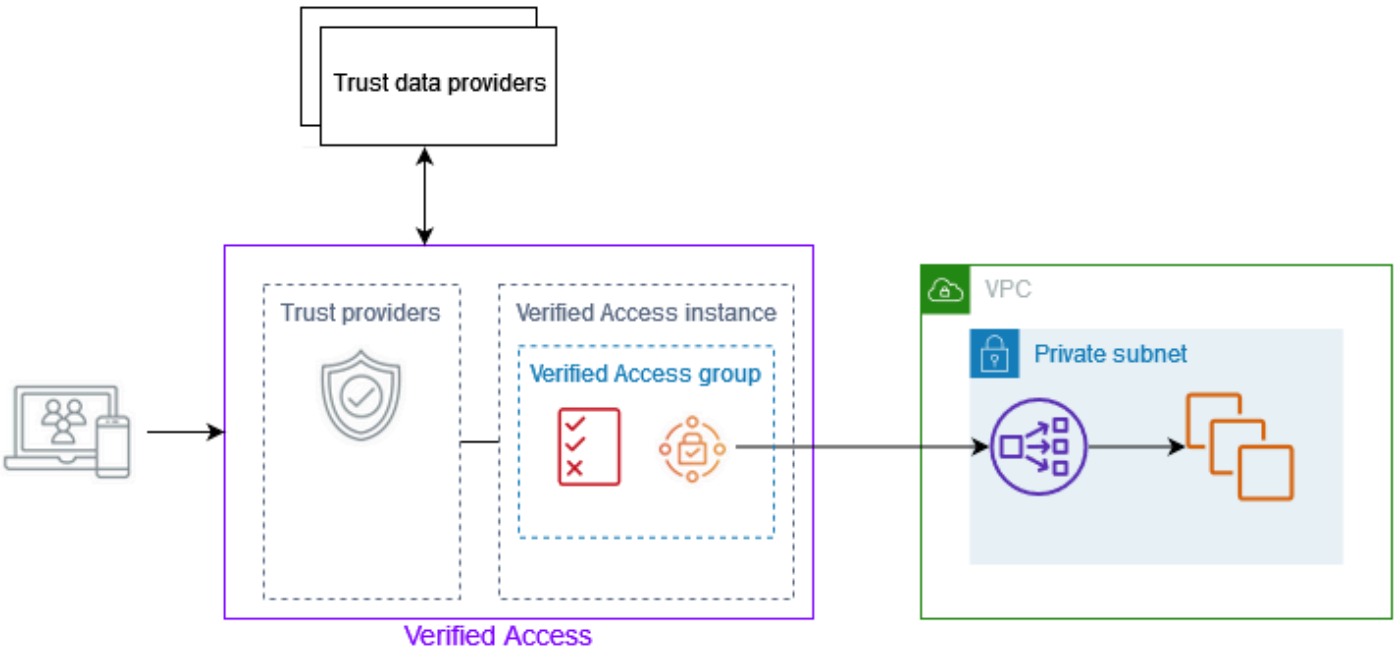
- 您選擇的信任提供商（來自 AWS 或第三方）發送的信任數據。
- 您在已驗證存取權中建立的存取原則。

當使用者嘗試存取應用程式時，「已驗證存取」會從信任提供者取得其資料，並根據您為應用程式設定的原則對其進行評估。只有當使用者符合您指定的安全性需求時，「已驗證存取」才會授與所要求應用程式 預設會拒絕所有應用程式要求，直到定義原則為止。

此外，「驗證存取」會記錄每次存取嘗試，協助您快速回應安全事件和稽核要求。

已驗證存取權的關鍵元件

下圖提供「已驗證存取權」的高階概觀。使用者傳送存取應用程式的要求。「已驗證存取」會根據群組和任何應用程式特定端點原則的存取原則來評估要求。如果允許存取，則會透過端點將要求傳送至應用程式。



- 驗證存取執行個體 — 執行個體會評估應用程式要求，並僅在符合安全性需求時授予存取權。
- 已驗證存取端點 — 每個端點代表一個應用程式。您可以建立負載平衡器端點或網路介面端點。

- 已驗證存取群組 — 已驗證存取端點的集合。建議您針對具有類似安全性需求的應用程式將端點分組，以簡化原則管理。例如，您可以將所有銷售應用程式的端點群組在一起。
- 存取原則 — 一組使用者定義的規則，可決定是否允許或拒絕存取應用程式。您可以指定各種因素的組合，包括使用者身分識別和裝置安全性狀態。您可以為每個「已驗證存取」群組建立群組存取原則，該群組中的所有端點都會繼承該群組。您可以選擇性地建立應用程式特定策略，並將其附加到特定端點。
- 信任提供者 — 管理使用者身分識別或裝置安全性狀態的服務。「驗證存取」適用於 AWS 和第三方信任提供者。您必須將至少一個信任提供者附加至每個已驗證存取執行個體。您可以將單一身分信任提供者和多個裝置信任提供者附加至每個已驗證存取執行個體。
- 信任資料 — 您的信任提供者傳送至已驗證存取權的使用者或裝置的安全性相關資料。也稱為使用者宣告或信任內容。例如，使用者的電子郵件地址或裝置的作業系統版本。「驗證存取」會在收到每個存取應用程式的要求時，根據您的存取原則評估此資料。

教學課程：開始使用已驗證存取

請使用此自學課程來開始使用 AWS Verified Access。您將學習如何建立和設定已驗證存取資源。

作為本教程的一部分，您將將應用程序添加到「已驗證訪問」中。在本教程結束時，特定用戶將能夠通過 Internet 訪問該應用程序，而無需使用VPN。

> **Note**
>
> 本教學課程不會示範與裝置型信任提供者的整合。相反地，我們只與以身分識別為基礎的信任提供者合作。

任務

- 已驗證存取教學課程
- 步驟 1：建立已驗證存取執行個體
- 步驟 2：設定已驗證存取信任提供者
- 步驟 3：將您的信任提供者附加至已驗證存取執行個體
- 步驟 4：建立已驗證的存取群組
- 步驟 5：透過分享您的驗證存取群組 AWS Resource Access Manager
- 步驟 6：建立已驗證存取端點以新增應用程式
- 步驟 7：DNS設定已驗證存取端點的設定
- 步驟 8：測試新增至已驗證存取權的應用程式的連線
- 步驟 9：設定已驗證存取群組層級存取原則
- 步驟 10：重新測試您新增至已驗證存取權的應用程式的連線
- 清除您建立的已驗證存取資源

已驗證存取教學課程

以下是完成此教學課程的先決條件：

- 兩個的可用性 AWS 帳戶。其中一個帳戶代管您的目標應用程式，而「已驗證存取」資源則會在另一個帳戶中建立。

- AWS IAM Identity Center 在您正在 AWS 區域 使用的內容中啟用。然後，您可以使用IAM身分中心做為具有已驗證存取權的信任提供者。如需詳細資訊，請參閱AWS IAM Identity Center 使用指南中的啟用IAM身分識別中心。
- 公用託管網域，以及更新網域DNS記錄所需的權限。
- 在內部負載平衡器後方執行的應用程式 AWS 帳戶。我們將使用的範例應用程式網域名稱為`www.myapp.example.com`。
- 具有建立執行個 AWS Verified Access 體所需之所有權限的IAM政策建立驗證存取執行個體的政策。

步驟 1：建立已驗證存取執行個體

請使用下列程序來建立「已驗證存取權」執行個體。

若要建立已驗證存取權實例

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在 Amazon VPC 導覽窗格中，選擇已驗證存取執行個體，然後選擇建立驗證存取執行個體。
3. (選擇性) 在名稱與說明中，輸入已驗證存取權執行個體的名稱和說明。
4. 若為「信任提供者」，請保留預設選項。
5. (選用) 若要新增標籤，請選擇 Add new tag (新增標籤)，然後輸入標籤的鍵和值。
6. 選擇建立已驗證存取執行個體

步驟 2：設定已驗證存取信任提供者

您可以設置 AWS IAM Identity Center 為您的信任提供商。

建立IAM身分識別中心信任提供者

1. 在 Amazon VPC 導覽窗格中，選擇「已驗證存取信任提供者」，然後選擇「建立驗證存取信任提供者」。
2. (選擇性) 在名稱標籤和說明中，輸入已驗證存取權信任提供者的名稱和說明。
3. 輸入自訂識別碼，以便稍後在使用原則參照名稱的原則規則時使用。例如，您可以輸入**`idc`**。
4. 在 [信任提供者類型] 底下，選取 [使用者信任
5. 在使用者信任提供者類型下，選取IAM身分識別中心
6. (選用) 若要新增標籤，請選擇 Add new tag (新增標籤)，然後輸入標籤的鍵和值。

7. 選擇建立已驗證存取信任提供者。

步驟 3：將您的信任提供者附加至已驗證存取執行個體

現在您已設定信任提供者，您可以將它附加到您先前建立的已驗證存取執行個體。請使用下列程序將信任提供者附加至您的「已驗證存取權」執行個體。

將信任提供者附加至您的執行個體

1. 在 Amazon VPC 導覽窗格中，選擇已驗證存取執行個體。
2. 選取執行個體。
3. 選擇 [動作]、[附加已驗證存取權限信任
4. 針對已驗證存取信任提供者，請選擇您的信任提供者
5. 選擇附加已驗證存取信任提供者。

步驟 4：建立已驗證的存取群組

在此步驟中，您將在步驟 5 中建立要用作端點的群組。

建立已驗證存取群組

1. 在 Amazon VPC 導覽窗格中，選擇 [已驗證存取群組]，然後選擇 [建立已驗證存取群組]。
2. (選擇性) 在名稱標籤和說明中，輸入群組的名稱和說明。
3. 針對已驗證存取執行個體，選擇您的已驗證存取執行
4. 針對「原則」定義，請保留此空白。您將在本教學課程稍後建立策略。
5. (選用) 若要新增標籤，請選擇 Add new tag (新增標籤)，然後輸入標籤的鍵和值。
6. 選擇建立已驗證的存取群組。

步驟 5：透過分享您的驗證存取群組 AWS Resource Access Manager

在此步驟中，您會與目標應用程式執行所 AWS 帳戶 在的群組共用您剛建立的群組。若要共用已驗證存取群組，您必須將其新增至資源共用。如果您沒有資源共用，您必須先建立一個資源共用。

如果您是中組織的一員 AWS Organizations，且已啟用組織內的共用功能，則組織中的取用者會自動授與共用「已驗證存取」群組的存取權。否則，取用者會收到加入資源共用的邀請，並在接受邀請後授與共用「已驗證存取」群組的存取權。

依照《AWS RAM 使用者指南》中建立資源共享的步驟進行。針對 [選取資源類型]，選擇 [已驗證存取權群組]，然後選取 [已驗證存取權] 群組的核取方塊。

如需詳細資訊，請參閱《AWS RAM 使用者指南》中的「入門」。

步驟 6：建立已驗證存取端點以新增應用程式

使用下列程序建立「已驗證存取」端點。此步驟假設您有一個應用程式在 Elastic Load Balancing 的內部負載平衡器後方執行。

建立已驗證存取端點

1. 在 Amazon VPC 導覽窗格中，選擇「已驗證存取端點」，然後選擇「建立已驗證存取端點」。
2. (選擇性) 在名稱標籤和說明中，輸入端點的名稱和說明。
3. 針對已驗證存取群組，選擇您的已驗證存取群組。
4. 有關申請詳細信息，請執行以下操作：
   a. 在應用程式網域中，輸入應用程式的DNS名稱。
   b. 在網域憑證下ARN，選取公用憑TLS證的 Amazon 資源名稱 (ARN)。
5. 如需端點詳細資訊，請執行下列動作：
   a. 針對「附件類型」，選擇VPC。
   b. 對於安全群組，請選取要與端點關聯的安全群組。
   c. 針對端點網域前置詞，輸入自訂識別碼。這會附加在「已驗證存取」產生的DNS名稱之前。在這個例子中，我們可以使用**`my-ava-app`**.
   d. 針對端點類型，選擇負載平衡器。
   e. 針對通訊協定，選取HTTPS或HTTP。這取決於負載平衡器的組態。
   f. 針對 Port (連接埠)，輸入連接埠號碼。這取決於負載平衡器的組態。
   g. 對於負載平衡器 ARN，請選擇您的負載平衡器。
   h. 針對子網路，選取與負載平衡器相關聯的子網路。
6. 對於策略定義，此時請勿輸入策略。我們將在後面的教程中介紹這一點。
7. (選用) 若要新增標籤，請選擇 Add new tag (新增標籤)，然後輸入標籤的鍵和值。

8. 選擇建立已驗證存取端點。

步驟 7：DNS設定已驗證存取端點的設定

在此步驟中，您會將應用程式的網域名稱 (例如 www.myapp.example.com) 對應至已驗證存取端點的網域名稱。若要完成DNS對應，請與您DNS的提供者建立一個規範名稱記錄 (CNAME)。建立記CNAME錄之後，使用者對應用程式的所有要求都會傳送至「已驗證存取」。

取得端點的網域名稱

1. 在 Amazon VPC 導覽窗格中，選擇「已驗證存取端點」。
2. 選取您先前建立的端點。
3. 選擇端點的「詳細資訊」索引標籤。
4. 在端點網域下，複製端點網域。

在本教學課程中，端點的網域名稱將為`my-ava-app.edge-1a2b3c4d5e6f7g.vai-1a2b3c4d5e6f7g.prod.verified-access.us-west-2.amazonaws.com`。

與您的DNS提供商一起創建CNAME記錄：

記錄名稱	Type	Value
我的例子	CNAME	my-ava-app. 邊緣 -1a2b3c4c4d5d5c6f7g. 驗證的訪問. 我們西部-亞馬遜

步驟 8：測試新增至已驗證存取權的應用程式的連線

您現在可以測試應用程式的連線能力。在網頁瀏覽器中輸入應用程式的網域名稱。「已驗證存取」原則的預設行為是拒絕所有要求。由於我們尚未制定允許任何人訪問的策略，因此應拒絕所有請求。

步驟 9：設定已驗證存取群組層級存取原則

使用下列程序修改「已驗證存取」群組，並設定允許連線至應用程式的存取原則。原則的詳細資料將取決於 IAM Identity Center 中設定的使用者和群組。如需有關建立策略的資訊，請參閱驗證存取政策。

修改已驗證存取群組

1. 在 Amazon VPC 導覽窗格中，選擇「已驗證存取群組」。
2. 選擇 群組。
3. 選擇 [動作]、[修改已驗證存取群組原則
4. 輸入策略。
5. 選擇修改已驗證的存取群組原則。

步驟 10：重新測試您新增至已驗證存取權的應用程式的連線

現在您的群組原則已就緒，您可以存取您的應用程式。在網頁瀏覽器中輸入應用程式的網域名稱。該請求應該被允許，並且您應該被重定向到應用程序。

清除您建立的已驗證存取資源

完成測試後，請按照以下步驟刪除已建立的資源。

若要刪除使用此教學課程建立的已驗證存取資源

1. 在 Amazon VPC 導覽窗格中，選擇「已驗證存取端點」。選取要移除的端點。選擇 [動作]、[刪除已驗證存取端點
2. 在功能窗格中，選擇 [已驗證存取群組]。選取您要移除的群組。選擇 [動作]、[刪除已驗證存取群組注意-您可能需要等待幾分鐘，直到端點刪除程序完成。
3. 在 Amazon VPC 導覽窗格中，選擇已驗證存取執行個體。選取您為此自學課程建立的例證。選擇 [動作]、[卸離已驗證存取信任提供 從下拉式清單中選取信任提供者，然後選擇卸離已驗證的存取信任提供者。
4. 在 Amazon VPC 導覽窗格中，選擇「已驗證存取信任提供者」。選取您為此教學課程建立的信任提供者。選擇 [動作]、[刪除已驗證存取信任提供
5. 在 Amazon VPC 導覽窗格中，選擇已驗證存取執行個體。選取您為此自學課程建立的例證。選擇「動作」，「刪除已驗證的存取權

驗證存取執行個

AWS Verified Access 執行個體是可協助您組織信任提供者和已驗證存取群組的 AWS 資源。執行個體會評估應用程式要求，並僅在符合安全性需求時授予存取權。

主題

建立和管理已驗證存取執行個體

您可以使用驗證存取執行個體來組織您的信任提供者和已驗證存取群組。使用下列程序建立「已驗證存取」執行個體，然後將信任提供者附加至「已驗證存取」，或將信任提供者從「已驗證存取」中斷連結。

主題

建立已驗證存取執行個體

請使用下列程序來建立「已驗證存取權」執行個體。

若要建立已驗證存取權實例

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在瀏覽窗格中，選擇 [已驗證存取權執行個體]，然後選擇 [建立已驗證存取權
3. (選擇性) 在名稱與說明中，輸入已驗證存取權執行個體的名稱和說明。
4. (選擇性) 如果您要求「已驗證存取權」FIPS 符合規範，請選擇啟用「聯邦資訊處理標準」(FIPS)。

5. (選擇性) 對於信任提供者，請選擇要附加至「已驗證存取權」執行個體的信任提供者。
6. (選用) 若要新增標籤，請選擇 Add new tag (新增標籤)，然後輸入標籤的鍵和值。
7. 選擇建立已驗證存取執行個體

將信任提供者附加至已驗證存取執行個體

請使用下列程序，將信任提供者附加至「已驗證存取權」執行個體。

將信任提供者附加至已驗證存取執行個體

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在瀏覽窗格中，選擇 [已驗證存取] 執行個體。
3. 選取執行個體。
4. 選擇 [動作]、[附加已驗證存取權限信任
5. 針對「已驗證存取」信任提供者，選擇信任提供者。
6. 選擇附加已驗證存取信任提供者。

從已驗證存取執行個體中分離信任提供者

請使用下列程序，將信任提供者從「已驗證存取」執行個體中斷連結。

從已驗證存取執行個體卸離信任提供者

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在瀏覽窗格中，選擇 [已驗證存取] 執行個體。
3. 選取執行個體。
4. 選擇 [動作]、[卸離已驗證存取信任提供
5. 針對「已驗證存取」信任提供者，選擇信任提供者。
6. 選擇 [卸離已驗證存取信任提供者

刪除已驗證存取執行個體

當您完成「已驗證存取」執行個體時，您可以將其刪除。刪除執行個體之前，您必須先移除任何關聯的信任提供者或已驗證存取群組。

若要刪除已驗證存取權實例

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在瀏覽窗格中，選擇 [已驗證存取] 執行個體。
3. 選取已驗證存取權執行個體。
4. 選擇「動作」，「刪除已驗證的存取權
5. 出現確認提示時，請輸入 **`delete`**，然後選擇 Delete (刪除)。

整合已驗證的存取與 AWS WAF

除了驗證存取強制執行的驗證和授權規則之外，您可能還想要套用周邊保護。這可協助您保護應用程式免於遭受其他威脅。您可以透過整合 AWS WAF 至「已驗證存取」部署來達成此目的。 AWS WAF 是一種 Web 應用程式防火牆，可讓您監控轉寄至受保護 Web 應用程式資源的要求。HTTP如需有關的詳細資訊 AWS WAF，請參閱AWS WAF開AWS WAF 發人員指南中的。

您可以將 AWS WAF Web 存取控制清單 (ACL) AWS WAF 與已驗證存取執行個體建立關聯，以與「已驗證存取」整合。Web ACL 是一種 AWS WAF 資源，可讓您對受保護的資源響應的所有 HTTP (S) Web 請求進行精細控制。正在處理 AWS WAF 關聯或解除關聯要求時，連結至執行個體的任何「已驗證存取」端點的狀態都會顯示為`updating`。請求完成後，狀態會返回`active`。您可以在 AWS Management Console 或中檢視狀態，方法是使用描述端點 AWS CLI。

> **Note**
>
> 您也可以使用主 AWS WAF 控台或完API成此整合。您將需要已驗證存取執行個體的 Amazon 資源名稱 (ARN)。您可以ARN使用以下格式來構造它：`arn:${Partition}:ec2:${Region}:${Account}:verified-access-instance/${VerifiedAccessInstanceId}`。

主題

- IAM將已驗證存取與整合所需的權限 AWS WAF
- 建立 AWS WAF 網頁關聯 ACL
- 檢查 AWS WAF 整合狀態
- 取消網頁的 AWS WAF 關聯 ACL

IAM將已驗證存取與整合所需的權限 AWS WAF

AWS WAF 與已驗證存取整合包含不直接對應於作業的僅授權動作API。這些動作會在「 AWS Identity and Access Management 服務授權參考」中使用指示[permission only]。請參閱服務授權參考EC2中適用於 Amazon 的動作、資源和條件金鑰。

若要使用 WebACL，您的 AWS Identity and Access Management 主體必須具有下列權限。

- ec2:AssociateVerifiedAccessInstanceWebAcl
- ec2:DisassociateVerifiedAccessInstanceWebAcl
- ec2:DescribeVerifiedAccessInstanceWebAclAssociations
- ec2:GetVerifiedAccessInstanceWebAcl

建立 AWS WAF 網頁關聯 ACL

下列步驟示範如何使用將 AWS WAF Web 存取控制清單 (ACL) 與已驗證存取執行個體產生關聯 AWS Management Console。

> **Tip**
>
> 您必須擁有現有的 AWS WAF 網頁ACL才能完成以下程序。如需有關 Web 的詳細資訊，ACLs請參閱AWS WAF 開發人員指南中的 Web 存取控制清單。

將 AWS WAF Web ACL 與已驗證存取執行個體建立關聯

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在瀏覽窗格中，選擇 [已驗證存取] 執行個體。
3. 選取已驗證存取權執行個體。
4. 選取 [整合] 索引標籤。
5. 選擇動作，然後選擇關聯 Web ACL。
6. 對於「網頁」ACL，請選擇現有的網頁ACL，然後選擇「關聯網頁」ACL。

您也可以使用 in AWS Management Console AWS WAF 來完成此工作。如需詳細資訊，請參閱開發人員指AWS WAF 南中的建立網頁ACL與AWS資源的關聯或取消關聯。

檢查 AWS WAF 整合狀態

您可以使用驗證 AWS WAF Web 存取控制清單 (ACL) 是否與已驗證存取執行個體相關聯 AWS Management Console。

若要檢視與已驗證存取權執行個體的 AWS WAF 整合狀態

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在瀏覽窗格中，選擇 [已驗證存取] 執行個體。
3. 選取已驗證存取權執行個體。
4. 選取 [整合] 索引標籤。
5. 檢查「WAF整合狀態」下列出的詳細資訊。如果處於「關聯」狀態，狀態將顯示為「關聯」或「未關聯」，以及 Web ACL 識別碼。

取消網頁的 AWS WAF 關聯 ACL

下列步驟示範如何使用取消 AWS WAF Web 存取控制清單 (ACL) 與已驗證存取執行個體的 AWS Management Console關聯。

取消 AWS WAF 網頁ACL與已驗證存取執行個體的關聯

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在瀏覽窗格中，選擇 [已驗證存取] 執行個體。
3. 選取已驗證存取權執行個體。
4. 選取 [整合] 索引標籤。
5. 選擇「動作」，然後選擇「取消 Web ACL 關聯
6. 選擇 「取消關聯網頁ACL」 以確認。

您也可以使用 in AWS Management Console AWS WAF 來完成此工作。如需詳細資訊，請參閱開發人員指AWS WAF 南中的建立網頁ACL與AWS資源的關聯或取消關聯。

FIPS已驗證存取的合規性

聯邦資訊處理標準 (FIPS) 是美國和加拿大政府的一項標準，針對保護敏感資訊的密碼編譯模組指定安全性需求。 AWS Verified Access 提供設定環境以遵循 140-2 FIPS 出版物的選項。FIPS下列 AWS 區域提供「已驗證存取」的合規性：

- 美國東部 (俄亥俄)
- 美國東部 (維吉尼亞北部)
- 美國西部 (加利佛尼亞北部)
- 美國西部 (奧勒岡)
- 加拿大 (中部)
- AWS GovCloud (US) 西部
- AWS GovCloud (US) 東

此頁面說明如何將新的或現有的「已驗證存取」環境設定為FIPS符合標準。

主題

設定現有的已驗證存取環境以FIPS符合性

如果您有現有的「已驗證存取」環境，並且想要將其設定為FIPS符合標準，則需要刪除並重新建立某些資源，才能啟用合FIPS規性。

若要將現有 AWS Verified Access 環境重新設定為FIPS符合標準，請遵循以下步驟。

1. 刪除原始的「驗證存取」端點、群組和執行個體。您設定的信任提供者可以重複使用。
2. 建立「已驗證存取」執行個體，確保在建立期間啟用「聯邦資訊處理標準」(FIPS)。此外，在建立期間，請從下拉式清單中選取要使用的已驗證存取信任提供者，以附加該提供者。
3. 建立已驗證存取群組。在建立群組期間，您可以將它與剛建立的已驗證存取執行個體建立關聯。
4. 建立一或多個已驗證存取端點。在建立端點期間，您可以將它們與上一個步驟中建立的群組相關聯。

針對FIPS符合性設定新的已驗證存取環境

若要設定FIPS符合規範的新 AWS Verified Access 環境，請遵循下列步驟。

1. 設定信任提供者。根據您的需求，您將需要建立使用者身分信任提供者和 (選擇性) 以裝置為基礎的信任提供者。

2. 建立已驗證存取執行個體，確保在程序期間啟用聯邦資訊處理標準 (FIPS)。此外，在建立期間，請從下拉式清單中選取您在上一個步驟中建立的「已驗證存取」信任提供者。
3. 建立已驗證存取群組。在建立群組期間，您可以將它與剛建立的已驗證存取執行個體建立關聯。
4. 建立一或多個已驗證存取端點。在建立端點期間，您可以將它們與上一個步驟中建立的群組相關聯。

已驗證存取的信任提供者

信任提供者是將使用者和裝置相關資訊傳送至的服務 AWS Verified Access。此資訊稱為信任內容。它可以包括基於用戶身份的屬性，例如「銷售」組織中的電子郵件地址或成員資格，或者設備信息，例如已安裝的安全修補程序或防病毒軟件版本。

「已驗證存取」支援下列類別的信任提供者：

- 使用者身分識別 — 儲存和管理使用者數位身分識別的身分識別提供者 (IdP) 服務。
- 裝置管理 — 適用於筆記型電腦、平板電腦和智慧型手機等裝置的裝置管理系統。

目錄

驗證存取的使用者身分信任提供者

您可以選擇使用 AWS IAM Identity Center 或 OpenID 連接兼容的用戶身份信任提供程序。

目錄

使用IAM身分識別中心做為信任提供者

您可以用 AWS IAM Identity Center 作具有 AWS 已驗證存取權的使用者身分信任提供者。

先決條件和考量事項

- IAM身分識別中心執行個體必須是 AWS Organizations 執行個體。獨立 AWS 帳戶IAM身分識別中心執行個體將無法運作。
- 您的IAM身分識別中心執行個體必須在您要在其中建立已驗證存取信任提供者的相同 AWS 區域中啟用。

如需不同執行個體類型的詳細資訊，請參閱AWS IAM Identity Center 使用指南中的管理 IAM Identity Center 的組織和帳戶執行個體。

建立IAM身分識別中心信任提供者

在您的 AWS 帳戶上啟用IAM身分識別中心後，您可以使用下列程序將IAM身分識別中心設定為已驗證存取權的信任提供者。

建立IAM身分識別中心信任提供者 (AWS 主控台)

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在瀏覽窗格中，選擇 [已驗證存取] 信任提供者，然後選取 [建立已驗證存取信任提供者
3. (選擇性) 在名稱標籤和說明中，輸入信任提供者的名稱和說明。
4. 針對策略參照名稱，請輸入稍後使用原則規則時要使用的識別碼。
5. 在 [信任提供者類型] 底下，選取 [使用者信任
6. 在使用者信任提供者類型下，選取IAM身分識別中心
7. (選用) 若要新增標籤，請選擇 Add new tag (新增標籤)，然後輸入標籤的鍵和值。
8. 選擇建立已驗證存取信任提供者。

若要建立IAM身分識別中心信任提供者 (AWS CLI)

- create-verified-access-trust-提供者（ ）AWS CLI

刪除IAM身分識別中心信任提供者

刪除信任提供者之前，您必須先移除所附加信任提供者的執行個體中的所有端點和群組組態。

刪除IAM身分識別中心信任提供者 (AWS 主控台)

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在功能窗格中，選擇 [已驗證存取] 信任提供者，然後在 [已驗證存取] 信任提供者下選取要刪除的信任提供者。
3. 選擇動作，然後選擇刪除已驗證存取信任提供者
4. 在文字方塊`delete`中輸入以確認刪除。
5. 選擇 刪除 。

若要刪除IAM身分識別中心信任提供者 (AWS CLI)

- delete-verified-access-trust-提供者（ ）AWS CLI

使用 OpenID Connect 信任提供者

AWS Verified Access 支援使用標準 OpenID Connect (OIDC) 方法的身分識別提供者。您可以使用OIDC相容的提供者作為具有已驗證存取權的使用者身分信任 但是，由於潛在OIDC提供程序的廣泛，因 AWS 此無法測試與「已驗證訪問」的每個OIDC集成。

已驗證的`UserInfo Endpoint`存取權取得它從OIDC提供者評估的信任資料。該`Scope`參數用於確定哪些信任數據集將被檢索。收到信任資料之後，系統會針對其評估「已驗證存取」原則。

> **Note**
>
> 在評估「已驗證存取」原則時，「已驗證存取」不會使用OIDC提供者`ID token`傳送的信任資料。只會`UserInfo Endpoint`根據策略評估來自的信任資料。

目錄

建立OIDC信任提供者的先決條件

您需要直接從您的信託提供者服務收集以下信息：

- 發行者
- 授權端點
- 權杖端點
- UserInfo 端點
- 用戶端 ID
- Client secret (用戶端密碼)
- 範圍

建立OIDC信任提供者

請使用下列程序來建立OIDC為您的信任提供者。

若要建立OIDC信任提供者 (AWS 主控台)

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在瀏覽窗格中，選擇 [已驗證存取] 信任提供者，然後選取 [建立已驗證存取信任提供者
3. (選擇性) 在名稱標籤和說明中，輸入信任提供者的名稱和說明。
4. 針對策略參照名稱，請輸入稍後使用原則規則時要使用的識別碼。
5. 在 [信任提供者類型] 底下，選取 [使用者信任
6. 在 [使用者信任提供者類型] 下，選取 [OIDCOpenID Connect]。
7. 針對「發行者」，輸入OIDC發行者的識別碼。
8. 對於授權端點，輸入完整URL的授權端點。
9. 針對 Token 端點，輸入完整URL的權杖端點。
10. 對於使用者端點，請輸入使用者端點URL的完整內容。
11. 輸入用戶端 ID 的 OAuth 2.0 用戶端識別碼。
12. 輸入用戶端密碼的 OAuth 2.0 用戶端密碼。
13. 輸入以身分識別提供者定義的範圍清單，以空格分隔。至少，「OpenID」範圍是必需的範圍。
14. (選用) 若要新增標籤，請選擇 Add new tag (新增標籤)，然後輸入標籤的鍵和值。
15. 選擇建立已驗證存取信任提供者。

> **Note**
>
> 您需要將重新導向新增URI至OIDC提供者的允許清單。您會想要使用「已驗證存取」端點來達到此目`ApplicationDomain`的。您可以在「已驗證存取」端點的「詳細資料」索引標籤下找到 AWS Management Console，或使用 AWS CLI 來描述端點。將以下內容添加到您的OIDC提供商的允許列表中：https：//`ApplicationDomain`/oauth2/IDP

若要建立OIDC信任提供者 (AWS CLI)

- create-verified-access-trust-提供者（ ）AWS CLI

修改OIDC信任提供者

建立信任提供者之後，您可以更新其組態。

若要修改OIDC信任提供者 (AWS 主控台)

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在瀏覽窗格中，選擇 [已驗證存取] 信任提供者，然後在 [已驗證存取] 信任提供者下選取要修改的信任提供者。
3. 選擇動作，然後選擇修改已驗證存取信任提供者
4. 修改您要變更的選項。
5. 選擇修改已驗證的存取信任提供者

若要修改OIDC信任提供者 (AWS CLI)

- modify-verified-access-trust-提供者（ ）AWS CLI

刪除OIDC信任提供者

刪除使用者信任提供者之前，您必須先從信任提供者所附加的執行個體中移除所有端點和群組組態。

刪除OIDC信任提供者 (AWS 主控台)

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在功能窗格中，選擇 [已驗證存取] 信任提供者，然後在 [已驗證存取] 信任提供者下選取要刪除的信任提供者。
3. 選擇動作，然後選擇刪除已驗證存取信任提供者
4. 在文字方塊`delete`中輸入以確認刪除。
5. 選擇 刪除 。

若要刪除OIDC信任提供者 (AWS CLI)

- delete-verified-access-trust-提供者（ ）AWS CLI

已驗證存取權的裝置型信任提供者

您可以使用裝置信任提供者搭配 AWS 已驗證存取權。您可以搭配驗證存取執行個體使用一或多個裝置信任提供者。

目錄

支援裝置信任提供者

下列裝置信任提供者可與「已驗證存取」整合：

- CrowdStrike — 使用 CrowdStrike 和驗證訪問保護私有應用程序
- Jamf — 將已驗證的存取與 Jamf 裝置身分整合
- JumpCloud — 集成 JumpCloud 和 AWS 驗證訪問

建立以裝置為基礎的信任提供者

請依照下列步驟建立並設定裝置信任提供者，以搭配「已驗證存取」使用。

建立已驗證存取裝置信任提供者 (AWS 主控台)

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在瀏覽窗格中，選擇 [已驗證存取] 信任提供者，然後選取 [建立已驗證存取信任提供者
3. (選擇性) 在名稱標籤和說明中，輸入信任提供者的名稱和說明。
4. 輸入稍後使用原則參照名稱的原則規則時要使用的識別碼。
5. 對於信任提供者類型，請選取裝置識別。
6. 對於 [裝置識別類型]，選擇 [Jamf]、CrowdStrike、或JumpCloud。
7. 針對承租人識別碼，輸入承租人應用程式的識別碼。
8. (選擇性) 對於公開簽署金鑰 URL，請輸入裝置信任提供者URL共用的唯一金鑰。(Jamf CrowdStrike 或跳雲端不需要此參數。)

9. 選擇建立已驗證存取信任提供者。

> **Note**
>
> 您需要將重新導向新增URI至OIDC提供者的允許清單。您會想要使用「已驗證存取」端點來達到此目DeviceValidationDomain的。您可以在「已驗證存取」端點的「詳細資料」索引標籤下找到 AWS Management Console，或使用 AWS CLI 來描述端點。將以下內容添加到您的OIDC提供商的允許列表中：https：//DeviceValidationDomain/oauth2/IDP

建立已驗證存取裝置信任提供者 (AWS CLI)

- create-verified-access-trust-提供者（ ）AWS CLI

修改以裝置為基礎的信任提供者

建立信任提供者之後，您可以更新其組態。

修改已驗證存取裝置信任提供者 (AWS 主控台)

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在瀏覽窗格中，選擇 [已驗證存取] 信任提供者。
3. 選取信任提供者。
4. 選擇動作，然後選取修改已驗證的存取信任提供者。
5. 視需要修改描述。
6. (選擇性) 對於公開簽署金鑰 URL，請修改裝置信任提供者URL共用的唯一金鑰。如果您的裝置信任提供者是 Jamf CrowdStrike 或 Jumpcloud，則不需要此參數。)
7. 選擇修改已驗證的存取信任提供者

修改已驗證存取裝置信任提供者 (AWS CLI)

- modify-verified-access-trust-提供者（ ）AWS CLI

刪除以裝置為基礎的信任提供者

完成信任提供者的使用後，您可以將其刪除。

刪除已驗證存取裝置信任提供者 (AWS 主控台)

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在瀏覽窗格中，選擇 [已驗證存取] 信任提供者。
3. 在 [已驗證存取權] 信任提供者下選取您要刪除的信任提供者。
4. 選擇動作，然後選取刪除已驗證的存取信任提供者。
5. 出現確認提示時，請輸入 **`delete`**，然後選擇 Delete (刪除)。

刪除已驗證存取裝置信任提供者 (AWS CLI)

- delete-verified-access-trust-提供者（ ）AWS CLI

已驗證存取群組

AWS Verified Access 群組是「已驗證存取」端點和群組層級「已驗證存取」原則的集合。群組中的每個端點共用「已驗證存取」政策。您可以使用群組將具有一般安全需求的端點聚集在一起。這樣可針對多個應用程式的安全性需求使用一個原則，協助簡化原則管理。

例如，您可以將所有銷售應用程式分組在一起，並設定群組範圍內的存取原則。然後，您可以使用此原則為所有銷售應用程式定義一組通用的最低安全性需求。此方法有助於簡化原則管理。

建立群組時，您必須將群組與「已驗證存取權」執行個體建立關聯。在建立端點的過程中，您會將端點與群組建立關聯。

任務

- 建立已驗證存取群組
- 修改已驗證存取群組原則
- 刪除已驗證的存取群組

建立已驗證存取群組

使用下列程序來建立已驗證的存取群組。

建立已驗證存取群組

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在功能窗格中，選擇 [已驗證的存取群組]，然後選擇 [建立已驗證的存取群組
3. (選擇性) 在名稱標籤和說明中，輸入群組的名稱和說明。
4. 針對已驗證存取執行個體，選取要與群組建立關聯的已驗證存取執行個體。
5. (選擇性) 針對原則定義，輸入要套用至群組的已驗證存取原則。
6. (選用) 若要新增標籤，請選擇 Add new tag (新增標籤)，然後輸入標籤的鍵和值。
7. 選擇建立已驗證的存取群組。

修改已驗證存取群組原則

使用下列程序來修改已驗證的存取群組原則。

修改已驗證存取群組原則

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在瀏覽窗格中，選擇 [已驗證的存取群組]，然後選取您要修改其原則的群組。
3. 選擇動作，然後選擇修改已驗證存取群組原則。
4. (選擇性) 根據您目前的目標，開啟或關閉 [啟用原則]。
5. (選擇性) 針對原則，輸入要套用至群組的已驗證存取原則。
6. 選擇修改已驗證的存取群組原則。

刪除已驗證的存取群組

完成「已驗證存取」群組後，您可以將其刪除。

刪除已驗證存取群組

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在功能窗格中，選擇 [已驗證存取群組]。
3. 選擇 群組。
4. 選擇動作、刪除已驗證的存取群組。
5. 出現確認提示時，請輸入 **`delete`**，然後選擇 Delete (刪除)。

已驗證存取端點

驗證存取端點代表應用程式。每個端點都與一個 Verified Access 群組關聯，並繼承此群組的存取政策。您可以選擇性地將應用程式特定的端點策略附加到每個端點。

目錄

已驗證存取端點類型

以下是可能的「已驗證存取」端點類型：

- 負載平衡器 — 應用程式要求會傳送至負載平衡器，以散發至您的應用程式。
- 網路介面 — 應用程式要求會使用指定的通訊協定和連接埠傳送至網路介面。

驗證存取如何與共用VPCs和子網路搭配使用

以下是有關共用VPC子網路的行為：

- VPC子網路共用支援已驗證的存取端點。參與者可以在共用子網路中建立「已驗證存取」端點。
- 建立端點的參與者將是端點擁有者，也是唯一允許修改端點的一方。將不允許VPC擁有者修改端點。
- 無法在 AWS 本機區域中建立已驗證存取端點，因此無法透過 Local Zones 共用。

如需詳細資訊，請參閱 Amazon VPC 使用者指南中的VPC與其他帳戶共用。

建立已驗證存取的負載平衡器端點

使用下列程序建立已驗證存取的負載平衡器端點。如需有關負載平衡器的詳細資訊，請參閱 E lastic Load Balancing 使用者指南。

要求

- 僅支援IPv4流量。
- 僅支援HTTP和HTTPS通訊協定。
- 負載平衡器必須是應用程式負載平衡器或 Network Load Balancer，且必須是內部負載平衡器。
- 負載平衡器和子網路必須屬於相同的虛擬私有雲 (VPC)。
- HTTPS負載平衡器可以使用自我簽署或公TLS用憑證。
- 您必須為您的應用程式提供網域名稱。這是您的使用者將用來存取應用程式的公用DNS名稱。您也需要提供符合此網域名稱之 CN 的公用SSL憑證。您可以使用建立或匯入憑證 AWS Certificate Manager。

若要建立負載平衡器端點

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在導覽窗格中，選擇「已驗證存取端點」。
3. 選擇建立已驗證存取端點。
4. (選擇性) 在名稱標籤和說明中，輸入端點的名稱和說明。
5. 對於「已驗證存取」群組，請為端點選擇「已驗證存取」群組。
6. 有關申請詳細信息，請執行以下操作：
   a. 在應用程式網域中，輸入應用程式的DNS名稱。
   b. 在 [網域憑證] 下ARN，選擇公用TLS憑證。
7. 如需端點詳細資訊，請執行下列動作：
   a. 對於「附件類型」，請選擇VPC。
   b. 對於「安全性群組」，請選擇端點的安全群組。來自進入負載平衡器之已驗證存取端點的流量將與此安全群組產生關聯。
   c. 對於 Endpoint 網域首碼，請輸入自訂識別碼，以在為端點產生的「已驗證存取」DNS 名稱前面加上。
   d. 針對端點類型，選擇負載平衡器。

e. 在 [通訊協定] 中，選擇HTTPS或HTTP。

f. 在 [連接埠] 下，輸入通訊埠號碼。

g. 對於負載平衡器 ARN，請選擇負載平衡器。

h. 對於子網路，請選擇負載平衡器的子網路。

8. (選擇性) 對於策略定義，請輸入端點的已驗證存取政策。
9. (選用) 若要新增標籤，請選擇 Add new tag (新增標籤)，然後輸入標籤的鍵和值。
10. 選擇建立已驗證存取端點。

建立已驗證存取的網路介面端點

使用下列程序來建立網路介面端點。

要求

- 僅支援IPv4流量。
- 僅支援HTTP和HTTPS通訊協定。
- 網路介面必須屬於與安全性群組相同的虛擬私人雲端 (VPC)。
- 我們使用網絡接口上的私有 IP 轉發流量。
- 您必須為您的應用程式提供網域名稱。這是您的使用者將用來存取應用程式的公用DNS名稱。您也需要提供符合此網域名稱之 CN 的公用SSL憑證。您可以使用建立或匯入憑證 AWS Certificate Manager。

建立網路介面端點

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在導覽窗格中，選擇「已驗證存取端點」。
3. 選擇建立已驗證存取端點。
4. (選擇性) 在名稱標籤和說明中，輸入端點的名稱和說明。
5. 對於「已驗證存取」群組，請為端點選擇「已驗證存取」群組。
6. 有關申請詳細信息，請執行以下操作：

   a. 在應用程式網域中，輸入應用程式的DNS名稱。

   b. 在 [網域憑證] 下ARN，選擇公用TLS憑證。

7. 如需端點詳細資訊，請執行下列動作：

   a. 對於「附件類型」，請選擇VPC。

   b. 對於「安全性群組」，請選擇端點的安全群組。來自進入網路介面之「已驗證存取」端點的流量將與此安全性群組產生關聯。

   c. 對於 Endpoint 網域首碼，請輸入自訂識別碼，以在為端點產生的「已驗證存取」DNS 名稱前面加上。

   d. 選擇 [網路介面] 做為 [端點類型]。

   e. 在 [通訊協定] 中，選擇HTTPS或HTTP。

   f. 在 [連接埠] 下，輸入通訊埠號碼。

   g. 在 [網路介面] 中，選擇網路介面。

8. (選擇性) 對於策略定義，請輸入端點的已驗證存取政策。

9. (選用) 若要新增標籤，請選擇 Add new tag (新增標籤)，然後輸入標籤的鍵和值。

10. 選擇建立已驗證存取端點。

允許來自「已驗證存取」端點的流量

您可以為應用程式設定安全群組，以便允許來自「已驗證存取」端點的流量。您可以透過新增將端點的安全性群組指定為來源的輸入規則來執行此操作。建議您移除任何其他輸入規則，以便應用程式只接收來自「已驗證存取」端點的流量。

我們建議您保留現有的輸出規則。

更新應用程式的安全性群組規則

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。

2. 在導覽窗格中，選擇「已驗證存取端點」。

3. 選擇「已驗證存取」端點，在「詳細資料」索引標籤IDs上找到「安全性」群組，然後複製端點的安全性群組 ID。

4. 在功能窗格中，選擇 [安全性群組]。

5. 選取與目標相關聯之安全性群組的核取方塊，然後選擇 [動作] > [編輯輸入規則]。

6. 若要新增允許來自「已驗證存取」端點的流量的安全性群組規則，請執行下列動作：

   a. 選擇新增規則。

   b. 在「類型」中，選擇「所有流量」或要允許的特定流量。

c. 對於 [來源]，選擇 [自訂]，然後貼上端點安全群組的 ID。

7. (選擇性) 若要求流量僅來自「已驗證存取」端點，請刪除任何其他輸入安全群組規則。
8. 選擇儲存規則。

修改已驗證存取端點

建立已驗證存取端點後，您可以修改其組態。

修改已驗證存取端點

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在導覽窗格中，選擇「已驗證存取端點」。
3. 選取端點。
4. 選擇 [動作]、[修改已驗證存取端點
5. 視需要修改端點詳細資料。
6. 選擇修改已驗證的存取端點。

修改已驗證存取端點策略

建立已驗證存取端點之後，您可以修改其策略。

修改已驗證存取端點策略

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在導覽窗格中，選擇「已驗證存取端點」。
3. 選取您要修改其策略的端點。
4. 選擇「動作」、「修改已驗證存取」端點策
5. (選擇性) 根據您目前的目標，開啟或關閉 [啟用原則]。
6. (選擇性) 針對策略，輸入要套用至端點的已驗證存取政策。
7. 選擇修改已驗證的存取端點策略。

刪除已驗證存取端點

使用「已驗證存取」端點後，您可以將其刪除。

刪除已驗證存取端點

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在導覽窗格中，選擇「已驗證存取端點」。
3. 選取端點。
4. 選擇 [動作]、[刪除已驗證存取端點
5. 出現確認提示時，請輸入 **`delete`**，然後選擇 Delete (刪除)。

信任資料傳送至信任提供者的「驗證存取」

信任資料是 AWS Verified Access 從信任提供者傳送給的資料。信任資料也稱為「使用者宣告」或「信任內容」。資料通常包含使用者或裝置的相關資訊。信任資料的範例包括使用者電子郵件、群組成員資格、裝置作業系統版本、裝置安全性狀態等。傳送的資訊會因信任提供者而有所不同，因此您應該參閱信任提供者的說明文件，以取得完整且更新的信任資料清單。

不過，透過使用「已驗證存取」記錄功能，您也可以查看從信任提供者傳送的信任資料。這在定義允許或拒絕應用程式存取的原則時很有用。如需有關在記錄檔中包含信任內容的資訊，請參閱啟用或停用已驗證存取信任內容。

本節包含範例信任資料和範例，可協助您開始撰寫原則。此處提供的信息僅供說明用途，不作為官方參考。

目錄

已驗證存取信任資料的預設內容

AWS Verified Access 依預設，所有 Cedar 評估都會包含有關目前HTTP要求的一些元素，而不論您設定的信任提供者為何。評估原則時，已驗證存取權會在 Cedar 前後關聯中包含目前HTTP要求的相關資料`context.http_request key`。如果您選擇，您可以撰寫根據資料進行評估的策略。下列JSON結構描述顯示評估中包含的資料。

```
{
     "title": "HTTP Request data included by Verified Access",
     "type": "object",
     "properties": {
         "user_agent": {
             "type": "string",
             "description": "The value of the User-Agent request header"
         },
         "x_forwarded_for": {
```

```
            "type": "string",
            "description": "The value of the X-Forwarded-For request header"
        },
        "http_method": {
            "type": "string",
            "description": "The HTTP Method provided (e.g. GET or POST)"
        },
        "hostname": {
            "type": "string",
            "description": "The value of the Host request header"
        },
        "port": {
           "type": "integer",
           "description": "The value of the verified access endpoint port"
        },
        "client_ip": {
            "type": "string",
            "description": "User ip connecting to the verified access endpoint"
        }
    }
}
```

以下是根據HTTP要求資料進行評估的原則範例。

```
forbid(principal, action, resource) when {
   context.http_request.http_method == "POST"
   && !(context.identity.roles.contains("Administrator"))
};
```

AWS IAM Identity Center 已驗證存取信任資料的上下文

評估原則時，如果您定義 AWS IAM Identity Center 為信任提供者，則會在您在信任提 AWS Verified Access 供者組態上指定為「原則參照名稱」的金鑰下，將信任資料納入 Cedar 內容中。如果您選擇，您可以撰寫根據信任資料進行評估的原則。

> **Note**
>
> 信任提供者的內容金鑰來自您在建立信任提供者時所設定的原則參照名稱。例如，如果您將原則參照名稱設定為「idp123」，則內容索引鍵會是「上下文 .idp123」。建立原則時，請檢查您使用的是正確的內容索引鍵。

下列JSON結構描述顯示評估中包含的資料。

```
{
   "title": "AWS IAM Identity Center context specification",
   "type": "object",
   "properties": {
     "user": {
       "type": "object",
       "properties": {
         "user_id": {
           "type": "string",
           "description": "a unique user id generated by AWS IdC"
         },
         "user_name": {
           "type": "string",
           "description": "username provided in the directory"
         },
         "email": {
           "type": "object",
           "properties": {
             "address": {
               "type": "email",
               "description": "email address associated with the user"
             },
             "verified": {
               "type": "boolean",
               "description": "whether the email address has been verified by AWS IdC"
             }
           }
         }
       }
     },
     "groups": {
       "type": "object",
       "description": "A list of groups the user is a member of",
       "patternProperties": {
         "^[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]
{12}$": {
           "type": "object",
           "description": "The Group ID of the group",
           "properties": {
             "group_name": {
               "type": "string",
               "description": "The customer-provided name of the group"
```

```
            }
          }
        }
      }
    }
  }
}
```

以下是根據提供的信任資料進行評估的策略範例 AWS IAM Identity Center。

```
permit(principal, action, resource) when {
   context.idc.user.email.verified == true
   // User is in the "sales" group with specific ID
   && context.idc.groups has "c242c5b0-6081-1845-6fa8-6e0d9513c107"
};
```

> **Note**
>
> 由於群組名稱可以變更，IAM身分識別中心是指使用其群組 ID 的群組。這有助於避免在變更群組名稱時中斷原則陳述式。

驗證存取信任資料的第三方信任提供者內容

本節說明第三方信任提供者提供給 AWS Verified Access 的信任資料。

> **Note**
>
> 信任提供者的內容金鑰來自您在建立信任提供者時所設定的原則參照名稱。例如，如果您將原則參照名稱設定為「idp123」，則內容索引鍵會是「上下文 .idp123」。建立原則時，請確定您使用的是正確的內容索引鍵。

目錄

瀏覽器擴展

如果您打算將裝置信任內容納入存取原則中，則需要「 AWS 已驗證存取」瀏覽器延伸功能或其他合作夥伴的瀏覽器延伸功能。驗證訪問目前支持谷歌瀏覽器和火狐瀏覽器.

我們目前支援三種裝置信任提供者：Jamf (支援 macOS 裝置) CrowdStrike (支援視窗 11 和視窗 10 裝置)，以及 JumpCloud (支援視窗和 MacOS)。

- 如果您在政策中使用 Jamf 信任資料，您的使用者必須從 Chrome 網路應用程式商店或 Firefox 附加元件網站下載並安裝 AWS Verified Access 瀏覽器延伸功能。
- 如果您在原則中使用CrowdStrike信任資料，則您的使用者必須先安裝AWS Verified Access 原生訊息主機 (直接下載連結)。需要此元件才能從使用者裝置上執行的 CrowdStrike 代理程式取得信任資料。然後，安裝此組件後，用戶必須從 Chrome 網絡應用店或 Firefox 附加組件站點在其設備上安裝 AWS Verified Access 瀏覽器擴展程序。
- 如果您使用的是 JumpCloud，您的使用者必須在其裝置上安裝 Chrome 網路應用程式商店或 Firefox 附加元件網站的 JumpCloud 瀏覽器擴充功能。

Jamf

Jamf 是第三方信任提供者。評估原則時，如果您將 Jamf 定義為信任提供者，則「已驗證存取」會在 Cedar 內容中包含信任資料，在您在信任提供者組態上指定為「原則參照名稱」的金鑰下。如果您選擇，您可以撰寫根據信任資料進行評估的原則。下列JSON結構描述顯示評估中包含的資料。

如需將 Jamf 與已驗證存取權限搭配使用的詳細資訊，請參閱 Jamf 網站上的將AWS已驗證存取與 Jamf 裝置身分整合。

```
{
    "title": "Jamf device data specification",
    "type": "object",
    "properties": {
        "iss": {
            "type": "string",
            "description": "\"Issuer\" - the Jamf customer ID"
        },
        "iat": {
            "type": "integer",
            "description": "\"Issued at Time\" - a unixtime (seconds since epoch) value
 of when the device information data was generated"
        },
```

```
        "exp": {
            "type": "integer",
            "description": "\"Expiration\" - a unixtime (seconds since epoch) value for
 when this device information is no longer valid"
        },
        "sub": {
            "type": "string",
            "description": "\"Subject\" - either the hardware UID or a value generated
 based on device location"
        },
        "groups": {
            "type": "array",
            "description": "Group IDs from UEM connector sync",
            "items": {
                "type": "string"
            }
        },
        "risk": {
            "type": "string",
            "enum": [
                "HIGH",
                "MEDIUM",
                "LOW",
                "SECURE",
                "NOT_APPLICABLE"
            ],
            "description": "a Jamf-reported level of risk associated with the device."
        },
        "osv": {
            "type": "string",
            "description": "The version of the OS that is currently running, in Apple
 version number format (https://support.apple.com/en-us/HT201260)"
        }
    }
}
```

以下是根據 Jamf 提供的信任資料進行評估的策略範例。

```
permit(principal, action, resource) when {
   context.jamf.risk == "LOW"
};
```

Cedar 提供了一個有用的`.contains()`功能來幫助 Jamf 的風險評分等枚舉。

```
permit(principal, action, resource) when {
   ["LOW", "SECURE"].contains(context.jamf.risk)
};
```

CrowdStrike

CrowdStrike 是第三方信任提供者。評估原則時，如果您定義 CrowdStrike 為信任提供者，「已驗證存取」會將信任資料納入 Cedar 前後關聯中，您在信任提供者組態上指定為「原則參照名稱」的金鑰下。如果您選擇，您可以撰寫根據信任資料進行評估的原則。下列JSON結構描述顯示評估中包含的資料。

如需 CrowdStrike 有關使用已驗證存取權的詳細資訊，請參閱使用 CrowdStrike 和 AWS Verified Access在 GitHub 網站上保護私人應用程式。

```
{
  "title": "CrowdStrike device data specification",
  "type": "object",
  "properties": {
    "assessment": {
      "type": "object",
      "description": "Data about CrowdStrike's assessment of the device",
      "properties": {
        "overall": {
          "type": "integer",
          "description": "A single metric, between 1-100, that accounts as a weighted
 average of the OS and and Sensor Config scores"
        },
        "os": {
          "type": "integer",
          "description": "A single metric, between 1-100, that accounts for the OS-
specific settings monitored on the host"
        },
        "sensor_config": {
          "type": "integer",
          "description": "A single metric, between 1-100, that accounts for the
 different sensor policies monitored on the host"
        },
        "version": {
          "type": "string",
          "description": "The version of the scoring algorithm being used"
        }
      }
```

```
    },
    "cid": {
      "type": "string",
      "description": "Customer ID (CID) unique to the customer's environemnt"
    },
    "exp": {
      "type": "integer",
      "description": "unixtime, The expiration time of the token"
    },
    "iat": {
      "type": "integer",
      "description": "unixtime, The issued time of the token"
    },
    "jwk_url": {
      "type": "string",
      "description": "URL that details the JWT signing"
    },
    "platform": {
      "type": "string",
      "enum": ["Windows 10", "Windows 11", "macOS"],
      "description": "Operating system of the endpoint"
    },
    "serial_number": {
      "type": "string",
      "description": "The serial number of the device derived by unique system
 information"
    },
    "sub": {
      "type": "string",
      "description": "Unique CrowdStrike Agent ID (AID) of machine"
    },
    "typ": {
      "type": "string",
      "enum": ["crowdstrike-zta+jwt"],
      "description": "Generic name for this JWT media. Client MUST reject any other
 type"
    }
  }
}
```

以下是根據提供的信任資料進行評估的策略範例 CrowdStrike。

```
permit(principal, action, resource) when {
```

```
    context.crowdstrike.assessment.overall > 50
};
```

JumpCloud

JumpCloud 是第三方信任提供者。評估原則時，如果您定義 JumpCloud 為信任提供者，「已驗證存取」會將信任資料納入 Cedar 前後關聯中，您在信任提供者組態上指定為「原則參照名稱」的金鑰下。如果您選擇，您可以撰寫根據信任資料進行評估的原則。下列JSON結構描述顯示評估中包含的資料。

如需 JumpCloud 有關使用 AWS 已驗證存取權的詳細資訊，請參閱 JumpCloud 網站上的整合 JumpCloud 和 AWS 驗證存取。

```
{
  "title": "JumpCloud device data specification",
  "type": "object",
  "properties": {
    "device": {
      "type": "object",
      "description": "Properties of the device",
      "properties": {
        "is_managed": {
          "type": "boolean",
          "description": "Boolean to indicate if the device is under management"
        }
      }
    },
    "exp": {
      "type": "integer",
      "description": "Expiration. Unixtime of the token's expiration."
    },
    "durt_id": {
      "type": "string",
      "description": "Device User Refresh Token ID. Unique ID that represents the
 device + user."
    },
    "iat": {
      "type": "integer",
      "description": "Issued At. Unixtime of the token's issuance."
    },
    "iss": {
      "type": "string",
```

```
      "description": "Issuer. This will be 'go.jumpcloud.com'"
    },
    "org_id": {
      "type": "string",
      "description": "The JumpCloud Organization ID"
    },
    "sub": {
      "type": "string",
      "description": "Subject. The managed JumpCloud user ID on the device."
    },
    "system": {
      "type": "string",
      "description": "The JumpCloud system ID"
    }
  }
}
```

以下是根據提供的信任內容進行評估的策略範例 JumpCloud。

```
permit(principal, action, resource) when {
   context.jumpcloud.org_id = 'Unique_orgnaization_identifier'
};
```

用戶聲明在已驗證訪問中通過和簽名驗證

AWS Verified Access 執行個體成功驗證使用者之後，會將從 IdP 收到的使用者宣告傳送至「已驗證存取」端點。使用者宣告已簽署，以便應用程式可以驗證簽章，並驗證宣告是由「已驗證存取」傳送的。在此過程中，會新增下列HTTP標頭：

`x-amzn-ava-user-context`

此標頭包含 JSON Web 令牌（JWT）格式的用戶聲明。該JWT格式包括 URL base64 編碼的標頭，有效負載和簽名。驗證訪問使用ES384（使用 SHA -384 哈希算法的ECDSA簽名算法）來生成簽名JWT。

應用程式可以將這些宣告用於個人化或其他使用者特定體驗。應用程式開發人員在使用前，應對身分提供者提供的每個聲明的唯一性等級和驗證進行自我教育。通常，sub聲明是識別給定用戶的最佳方法。

目錄

- 範例：已簽署IAM身JWT分識別中心使用者宣告
- 公有金鑰
- 範例：擷取和解碼 JWT

範例：JWT針對OIDC使用者宣告簽署

以下示例演示了用OIDC戶聲明的標題和有效負載在JWT格式中的外觀。

示例標題：

```
{
"alg": "ES384",
"kid": "12345678-1234-1234-1234-123456789012",
"signer": "arn:aws:ec2:us-east-1:123456789012:verified-access-instance/vai-
abc123xzy321a2b3c",
"iss": "OIDC Issuer URL"
"exp": "expiration" (120 secs)
}
```

承載範例：

```
{
"sub": "xyzsubject",
"email": "xxx@amazon.com",
"email_verified": true,
"groups": [
"Engineering",
"finance"
]
}
```

範例：已簽署IAM身JWT分識別中心使用者宣告

下列範例示範 I IAM dentity Center 使用者宣告的標頭和承載在JWT格式中的外觀。

> **Note**
>
> 對於IAM身分識別中心，宣告中只會包含使用者資訊。

示例標題：

```
{
"alg": "ES384",
"kid": "12345678-1234-1234-1234-123456789012",
"signer": "arn:aws:ec2:us-east-1:123456789012:verified-access-instance/vai-
abc123xzy321a2b3c",
"iss": "arn:aws:ec2:us-east-1:123456789012:verified-access-trust-provider/vatp-
abc123xzy321a2b3c",
"exp": "expiration" (120 secs)
}
```

承載範例：

```
{
"user": {
        "user_id": "f478d4c8-a001-7064-6ea6-12423523",
        "user_name": "test-123",
        "email": {
            "address": "test@amazon.com",
            "verified": false
        }
    }
}
```

公有金鑰

由於已驗證存取執行個體不會加密使用者宣告，因此建議您設定要使用的已驗證存取端點HTTPS。如果您設定要使用的已驗證存取端點HTTP，請務必使用安全群組限制傳輸至端點的流量。

我們建議您在根據宣告進行任何授權之前先驗證簽名。若要取得公開金鑰，請從JWT標頭取得金鑰ID，並使用它從端點查詢公開金鑰。每 AWS 區域 個端點的端點如下所示：

`https://public-keys.prod.verified-access.<region>.amazonaws.com/<key-id>`

範例：擷取和解碼 JWT

下面的代碼示例演示了如何在 Python 3.9 中獲取密鑰 ID，公鑰和有效負載。

```
import jwt
```

```
import requests
import base64
import json

# Step 1: Get the key id from JWT headers (the kid field)
encoded_jwt = headers.dict['x-amzn-ava-user-context']
jwt_headers = encoded_jwt.split('.')[0]
decoded_jwt_headers = base64.b64decode(jwt_headers)
decoded_jwt_headers = decoded_jwt_headers.decode("utf-8")
decoded_json = json.loads(decoded_jwt_headers)
kid = decoded_json['kid']

# Step 2: Get the public key from Regional endpoint
url = 'https://public-keys.prod.verified-access.' + region + '.amazonaws.com/' + kid
req = requests.get(url)
pub_key = req.text

# Step 3: Get the payload
payload = jwt.decode(encoded_jwt, pub_key, algorithms=['ES384'])
```

驗證存取政策

AWS Verified Access 原則可讓您定義存取中託管之應用程式的規則 AWS。它們是用 Cedar 寫的，一種 AWS 政策語言。使用 Cedar，您可以建立原則，根據您設定要與已驗證存取權搭配使用的身分識別或裝置型信任提供者傳送的信任資料進行評估。

如需 Cedar 政策語言的詳細資訊，請參閱 C edar 參考指南。

本節說明已驗證存取原則的結構、其包含的內容、如何定義它們，以及提供一些範例。

目錄

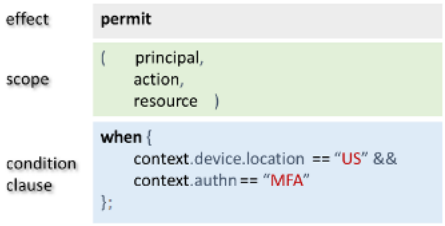
使用已驗證存取權的原則

當您建立「已驗證存取」群組或建立「已驗證存取」端點時，您可以選擇定義「已驗證存取」原則。您可以在不定義「已驗證存取」政策的情況下建立群組或端點，但所有存取要求都會遭到封鎖，直到您定義原則為止。

若要在現有的「已驗證存取」群組或端點建立之後新增或變更其政策，請參閱修改已驗證存取群組原則或修改已驗證存取端點策略。

驗證存取原則陳述式結構

本節說明政 AWS Verified Access 策聲明及其評估方式。您可以在單一「已驗證存取」原則中有多個陳述式。下圖顯示已驗證存取原則的結構。



該策略包含以下部分：

- 效果 — 指定政策陳述式為 `permit` (Allow) 還是 `forbid` (Deny)。
- 範圍 — 指定效果所套用的主參與者、動作及資源。您可以不識別特定主參與者、動作或資源 (如前面範例所示)，讓 Cedar 中的範圍保持未定義。在此情況下，原則會套用至所有可能的主參與者、動作及資源。
- 條件子句 — 指定套用效果的內容。

> **Important**
>
> 針對「已驗證存取」，原則會透過參照條件子句中的信任資料來完整表示。政策範圍必須始終保持未定義。然後，您可以使用條件子句中的身分識別和裝置信任內容來指定存取權。

簡單的政策範例

```
permit(principal,action,resource)
when{
 context.<policy-reference-name>.<attribute> &&
 context.<policy-reference-name>.<attribute2>
};
```

在上述範例中，請注意，您可以使用&&運算子在原則陳述式中使用一個以上的條件子句。Cedar 政策語言賦予您表現力，讓您能夠建立自訂、精細且廣泛的政策聲明。如需額外的範例，請參閱已驗證存取範例原則。

驗證存取原則評估

政策文件是一組或多個政策聲明（`permit`或`forbid`聲明）。如果條件子句 (when陳述式) 為真，則此政策適用。為了讓政策文件允許存取，文件中至少必須套用一個許可政策，且不能套用任何禁止政策。如果不適用許可政策和/或適用一個或多個禁止政策，則保單文件會拒絕訪問。如果您已針對「已驗證

存取」群組和「已驗證存取」端點定義原則文件，則這兩個文件都必須允許存取。如果您尚未定義「已驗證存取」端點的原則文件，則只有「已驗證存取」群組原則需要存取。

> **Note**
>
> AWS Verified Access 在建立原則時驗證語法，但不會驗證您放入條件子句中的資料。

已驗證存取原則的內建運算子

使用各種條件建立 AWS Verified Access 策略的前後關聯時，如中所述驗證存取原則陳述式結構，您可以使用&&運算子來新增其他條件。您還可以使用許多其他內置運營商為您的政策條件添加額外的表達能力。下表包含了所有內置的運算符供參考。

運算子	類型和重載	描述
!	布爾 → 布爾	邏輯不是。
==	任何 → 任何	平等 適用於任何類型的參數，即使類型不匹配。不同類型的值永遠不會彼此相等。
!=	任何 → 任何	不平等；相等的精確反向（見上文）。
<	（長，長）→ 布爾	長整數小於。
<=	（長，長）→ 布爾	長整數 less-than-or-equal-到。
>	（長，長）→ 布爾	長整數大於。
>=	（長，長）→ 布爾	長整數 greater-than-or-equal-到。
in	(實體、實體) → 布林值	層次結構成員資格（反射性：A 中的 A 始終為真）。
	(實體，集合 (實體)) → 布爾值	層次結構成員資格：如果（A 和 B）||（C 中的 A）||...

運算子	類型和重載	描述
		如果集合包含非實體，則 [B，C，...] 中的 A 是真實的。
&&	(布林值、布林值) → 布林值	邏輯和（短路）。
||	(布林值、布林值) → 布林值	邏輯或（短路）。
。存在（ ）	實體 → 布爾	實體存在。
具有	(實體、屬性) → 布林值	中綴運算符。 `e has f`測試記錄或實體是否`e`具有屬性的繫結`f`。`false`如果`e`不存在，或者如果`e`確實存在，但不具有屬性，則返回`f`。屬性可以表示為標識符或字符串文字。
like	（字符串，字符串）→ 布爾	中綴運算符。 `t like p`檢查文字`*`是否`t`符合模式`p`，其中可能包含符合 0 個或多個任何字元的萬用字元。若要符合中的文字星號字元`t`，您可以在中使用特殊逸出字元序列`\*`p。
。包含（ ）	（設置，任意）→ 布爾	設置成員（B 是 A 的元素）。
.containsAll()	（設置，設置）→ 布爾	測試集 A 是否包含集合 B 中的所有元素。
.containsAny()	（設置，設置）→ 布爾	測試集 A 是否包含集合 B 中的任何元素。

已驗證存取政策註解

您可以在 AWS Verified Access 政策中包含註解陳述。註釋被定義為以換行符開頭`//`和終止的行。

下列範例顯示策略中的註解陳述式。

```
// this policy grants access to users in a given domain with trusted devices
permit(principal, action, resource)
when {
  // the user's email address is in the @example.com domain
  context.idc.user.email.address.contains("@example.com")
  // Jamf thinks the user's computer is low risk or secure.
  && ["LOW", "SECURE"].contains(context.jamf.risk)
};
```

驗證的訪問策略邏輯短路

您可能會想要撰寫 AWS Verified Access 原則來評估指定前後關聯中可能存在或可能不存在的資料。如果您在不存在的前後關聯中參照資料，Cedar 將產生錯誤並評估原則以拒絕存取，無論您的意圖為何。例如，這將導致拒絕，因為在此上下文中fake_provider並bogus_key不存在。

```
permit(principal, action, resource) when {
  context.fake_provider.bogus_key > 42
};
```

為了避免這種情況，您可以使用has運算符檢查是否存在密鑰。如果has運算子傳回 false，則會停止對鏈結陳述式的進一步評估，且 Cedar 不會產生嘗試參照不存在的項目的錯誤。

```
permit(principal, action, resource) when {
  context.identity.user has "some_key" && context.identity.user.some_key > 42
};
```

這在指定參考兩個不同信任提供者的原則時最有用。

```
permit(principal, action, resource) when {
  // user is in an allowed group
  context.aws_idc.groups has "c242c5b0-6081-1845-6fa8-6e0d9513c107"
  &&(
    (
      // if CrowdStrike data is present,
      // permit if CrowdStrike's overall assessment is over 50
      context has "crowdstrike" && context.crowdstrike.assessment.overall > 50
    )
    ||
    (
      // if Jamf data is present,
```

```
      // permit if Jamf's risk score is acceptable
      context has "jamf" && ["LOW", "NOT_APPLICABLE", "MEDIUM",
 "SECURE"].contains(context.jamf.risk)
    )
  )
};
```

已驗證存取範例原則

範例 1：建立IAM身分識別中心的原則

> **Note**
>
> 由於群組名稱可以變更，IAM身分識別中心是指使用其群組 ID 的群組。這有助於避免在變更群組名稱時中斷原則陳述式。

下列範例原則只有在使用者屬於finance群組 (其群組識別碼為c242c5b0-6081-1845-6fa8-6e0d9513c107) 且擁有已驗證的電子郵件地址時，才允許存取。

```
permit(principal,action,resource)
when {
    context.<policy-reference-name>.groups has "c242c5b0-6081-1845-6fa8-6e0d9513c107"
    && context.<policy-reference-name>.user.email.verified == true
};
```

範例 1b：將更多條件新增至IAM身分識別中心的原則陳述式

下列範例原則只有在使用者屬於finance群組 (其群組識別碼為c242c5b0-6081-1845-6fa8-6e0d9513c107)、擁有已驗證的電子郵件地址，且 Jamf 裝置風險評分為LOW時，才允許存取。

```
permit(principal,action,resource)
when {
    context.<policy-reference-name>.groups has "c242c5b0-6081-1845-6fa8-6e0d9513c107"
    && context.<policy-reference-name>.user.email.verified == true
    && context.jamf.risk == "LOW"
};
```

範例 2：第三方OIDC供應商的相同政策

下列範例原則只有在使用者來自「財務」群組、擁有已驗證的電子郵件地址，且 Jamf 裝置風險評分為 LOW時，才允許存取。

```
permit(principal,action,resource)
when {
     context.<policy-reference-name>.groups.contains("finance")
     && context.<policy-reference-name>.email_verified == true
     && context.jamf.risk == "LOW"
};
```

範例 3：使用 CrowdStrike

當整體評估分數大於 50 時，下列範例原則允許存取。

```
permit(principal,action,resource)
when {
    context.crwd.assessment.overall > 50
};
```

範例 4：使用特殊字元

下列範例顯示如果內容屬性使用：(分號) (原則語言中的保留字元)，如何撰寫原則。

```
permit(principal, action, resource)
when {
    context.<policy-reference-name>["namespace:groups"].contains("finance")
};
```

範例 5：允許特定 IP 位址

下列範例顯示只允許特定 IP 位址的策略。

```
permit(principal, action, resource)
when {
    context.http_request.client_ip == "192.0.2.1"
};
```

範例 5a：封鎖特定 IP 位址

下列範例顯示將封鎖特定 IP 位址的策略。

```
forbid(principal,action,resource)
when {
ip(context.http_request.client_ip).isInRange(ip("192.0.2.1/32"))
};
```

驗證存取原則助理

「已驗證存取」原則助理是「已驗證存取」主控台中的工具，可用來測試和開發原則。它會在一個畫面上顯示端點策略、群組原則和信任內容，您可以在其中測試和編輯策略。

信任內容格式會因不同的信任提供者而異，有時「已驗證存取」系統管理員可能不知道特定信任提供者使用的確切格式。這就是為什麼將信任內容以及群組和端點政策集中在一個位置以進行測試和開發目的，可能會非常有幫助。

下列各節說明使用原則編輯器的基本概念。

任務

- 步驟 1：指定資源
- 步驟 2：測試和編輯策略
- 步驟 3：檢閱並套用變更

步驟 1：指定資源

在原則助理員的第一頁上，您可以指定要使用的已驗證存取端點。您也將指定使用者 (以電子郵件地址識別)，以及選擇性地指定使用者的名稱和/或裝置識別碼。根據預設，會從指定使用者的「已驗證存取」記錄中擷取最新的授權決定。您可以選擇性地特別選擇最新的允許或拒絕決定。

最後，信任內容、授權決策、端點原則和群組原則都會顯示在下一個畫面上。

開啟原則助理員並指定您的資源

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在瀏覽窗格中，選擇「已驗證存取權」執行個體，然後針對您要使用的執行個體按一下「已驗證存取權」執行個體 ID。
3. 選擇 [啟動原則助理]。
4. 在 [使用者電子郵件地址] 中，輸入使用者的電子郵件地址。
5. 對於「已驗證存取」端點，選取您要編輯和測試策略的端點。

6. (選擇性) 在名稱中，提供使用者的名稱。
7. (選用) 在 [裝置識別碼] 下，提供唯一的裝置識別碼。
8. (選擇性) 針對授權結果，請選擇您要使用的最近授權結果類型。默認情況下，將使用最新的授權結果。
9. 選擇 Next (下一步)。

步驟 2：測試和編輯策略

在此頁面上，您將看到以下資訊以供您使用：

- 您的信任提供者為使用者及 (選擇性) 您在上一個步驟中指定的裝置所傳送的信任內容。
- 在上一個步驟中指定的「已驗證存取」端點的 Cedar 原則。
- 端點所屬之已驗證存取群組的 Cedar 原則。

您可以在此頁面上編輯「已驗證存取」端點和群組的 Cedar 原則，但信任內容是靜態的。您現在可以使用此頁面來檢視 Cedar 原則旁邊的信任內容。

選擇 [測試原則] 按鈕，針對信任內容測試原則，授權結果就會顯示在畫面上。您可以編輯策略並重新測試變更，並視需要重複此程序。

對策略所做的變更感到滿意之後，請選擇 [下一步] 繼續進行原則助理員的下一個畫面。

步驟 3：檢閱並套用變更

在政策助理的最後一頁上，您將看到您對突出顯示的政策所做的更改，以便於查看。您現在可以最後一次檢閱它們，然後選擇 [套用變更] 以確認變更。

您也可以選擇 [上一頁] 返回上一頁，或選擇 [取消] 完全取消原則助理。

驗證存取中的安全性

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

安全是 AWS 與您之間共同承擔的責任。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：

- 雲端安全性 — AWS 負責保護中執行 AWS 服務的基礎架構 AWS 雲端。 AWS 還為您提供可以安全使用的服務。若要瞭解適用於 AWS 已驗證存取權的規範計劃，請參閱規範計劃AWS 服務範圍內的 AWS 服務，遵的服務。
- 雲端中的安全性 — 您的責任取決於您使用的 AWS 服務。您也必須對其他因素負責，包括資料的機密性、您公司的要求和適用法律和法規。

本文件可協助您瞭解如何在使用「已驗證存取權」時套用共同責任模型。下列主題說明如何設定已驗證存取以符合您的安全性和合規性目標。您還將學習如何使用其他 AWS 服務，以幫助您監視和保護「已驗證存取」資源。

目錄

驗證存取權中的資料保護

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

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

- 對每個帳戶使用多重要素驗證 (MFA)。

- 使用SSL/TLS與 AWS 資源溝通。我們需要 TLS 1.2 並推薦 TLS 1.3。
- 使用設定API和使用者活動記錄 AWS CloudTrail。
- 使用 AWS 加密解決方案以及其中的所有默認安全控制 AWS 服務。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果 AWS 透過命令列介面或存取時需要 FIPS 140-3 驗證的密碼編譯模組API，請使用端點。FIPS 如需有關可用FIPS端點的詳細資訊，請參閱聯邦資訊處理標準 (FIPS) 140-3。

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的文字欄位中，例如名稱欄位。這包括當您使用主控台、、API或 AWS 服務 使用「已驗證存取」或其他使用時 AWS SDKs。 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URL給外部伺服器，我們強烈建議您不要在中包含認證資訊，URL以驗證您對該伺服器的要求。

傳輸中加密

「驗證存取」會使用「傳輸層安全性」(TLS) 1.2 或更新版本，透過網際網路加密從使用者傳輸到「已驗證存取」端點的所有資料。

網際網路流量隱私權

您可以配置已驗證的存取權限，以限制對VPC. 對於以使用者為基礎的驗證，您也可以根據存取端點的使用者群組來限制對網路部分的存取。如需詳細資訊，請參閱驗證存取政策。

AWS 已驗證存取權的靜態資料加密

AWS 驗證存取權預設會使用 AWS 擁有的KMS金鑰加密靜態資料。預設情況下，靜態資料加密時，有助於減少保護敏感資料所涉及的營運負荷和複雜性。同時，其可讓您建置符合嚴格加密合規性和法規要求的安全應用程式。以下各節提供「已驗證存取」如何使用KMS金鑰進行靜態資料加密的詳細資料。

目錄

- AWS 已驗證存取加密內容
- 監控您的加密金鑰是否 AWS 已驗證存取

驗證存取權和KMS金鑰

AWS 擁有的金鑰

「已驗證存取」會使用KMS金鑰自動加密個人識別資訊 (PII)。默認情況下會發生這種情況，您無法自己查看，管理，使用或審核AWS擁有密鑰的使用。不過，您不需要採取任何動作或變更任何程式，即可保護加密您資料的金鑰。如需詳細資訊，請參閱《AWS Key Management Service 開發人員指南》中的 AWS 擁有的金鑰。

雖然您無法停用此層加密或選取替代加密類型，但您可以在建立驗證存取資源時選擇客戶管理的金鑰，在現有 AWS 擁有的加密金鑰上新增第二層加密。

客戶受管金鑰

「驗證存取」支援使用您建立和管理的對稱客戶管理金鑰，在現有的預設加密上新增第二層加密。您可以完全控制此層加密，因此能執行以下任務：

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

如需更多資訊，請參閱 AWS Key Management Service 開發人員指南中的客戶受管金鑰。

> **Note**
>
> 驗證存取權會自動啟用使用 AWS 擁有的金鑰進行靜態加密，以免費保護個人識別資料。但是，當您使用客戶管理的金鑰時，將 AWS KMS 收取費用。如需有關定價的詳細資訊，請參閱定AWS Key Management Service 價。

個人身份信息

下表摘要說明「已驗證存取」使用的個人識別資訊 (PII)，以及其加密方式。

資料類型	AWS 擁有的金鑰加密	客戶自管金鑰加密 (選用)
`Trust provider (user-type)` 使用者類型信任提供者包含視PII為 AuthorizationEndpoint的OIDC選項 UserInfoEndpoint ClientId ClientSecret，例如、、、等。	已啟用	已啟用
`Trust provider (device-type)` 設備類型的信任提供程序包含一個 TenantId，這被認為是。PII	已啟用	已啟用
`Group policy` 在建立或修改已驗證存取群組期間提供。包含授權存取要求的規則。可能包含PII諸如用戶名和電子郵件地址等。	已啟用	已啟用
`Endpoint policy` 在建立或修改「已驗證存取」端點期間提供。包含授權存取要求的規則。可能包含PII諸如用戶名和電子郵件地址等。	已啟用	已啟用

AWS 已驗證存取權如何使用授權 AWS KMS

驗證存取權需要授權才能使用您的客戶管理金鑰。

當您建立使用客戶管理金鑰加密的已驗證存取資源時，「已驗證存取」會將CreateGrant請求傳送至以代表您建立授權 AWS KMS。中的授權用 AWS KMS 於授予「已驗證存取權」存取權，讓您能夠存取您帳戶中的客戶管理金鑰。

驗證存取權需要授權才能使用您的客戶管理金鑰進行下列內部作業：

- 發送解密請求 AWS KMS 以解密加密的數據密鑰，以便可以使用它們來解密您的數據。
- 傳送RetireGrant要求 AWS KMS 以刪除授權。

您可以隨時撤銷授予的存取權，或移除服務對客戶受管金鑰的存取權。如果這樣做，「已驗證存取」將無法存取客戶管理金鑰加密的任何資料，這會影響依賴於該資料的作業。

透過驗證存取使用客戶代管金鑰

您可以使用 AWS Management Console、或建立對稱的客戶管理金鑰。 AWS KMS APIs請依照《AWS Key Management Service 開發人員指南》中建立對稱客戶受管金鑰的步驟進行。

重要政策

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

若要將您的客戶管理金鑰與已驗證存取資源搭配使用，金鑰政策中必須允許下列API作業：

- kms:CreateGrant：新增客戶受管金鑰的授權。授與指定KMS金鑰的控制權存取權，允許存取權授與已驗證存取需要的作業。如需有關使用授權的詳細資訊，請參閱開AWS Key Management Service 發人員指南。

  這允許「已驗證存取」執行以下作業：

  - 呼叫 `GenerateDataKeyWithoutPlainText` 以產生加密的資料金鑰並加以儲存，因為資料金鑰不會立即用來加密。
  - 呼叫 `Decrypt` 以使用儲存的加密資料金鑰來存取加密的資料。
  - 設定退休本金以允許服務。`RetireGrant`
- kms:DescribeKey— 提供客戶管理的金鑰詳細資料，以允許已驗證存取權驗證金鑰。
- kms:GenerateDataKey— 允許已驗證的存取權使用金鑰來加密資料。
- kms:Decrypt— 允許驗證訪問解密加密的數據密鑰.

以下是可用於「已驗證存取」的金鑰原則範例。

```
"Statement" : [
    {
      "Sid" : "Allow access to principals authorized to use Verified Access",
      "Effect" : "Allow",
      "Principal" : {
        "AWS" : "*"
      },
      "Action" : [
        "kms:DescribeKey",
        "kms:CreateGrant",
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "kms:ViaService" : "verified-access.region.amazonaws.com",
          "kms:CallerAccount" : "111122223333"
        }
    },
    {
      "Sid": "Allow access for key administrators",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
       },
      "Action" : [
        "kms:*"
       ],
      "Resource": "arn:aws:kms:region:111122223333:key/key_ID"
    },
    {
      "Sid" : "Allow read-only access to key metadata to the account",
      "Effect" : "Allow",
      "Principal" : {
        "AWS" : "arn:aws:iam::111122223333:root"
      },
      "Action" : [
        "kms:Describe*",
        "kms:Get*",
        "kms:List*",
        "kms:RevokeGrant"
```

```
      ],
      "Resource" : "*"
    }
  ]
```

如需有關在政策中指定許可的詳細資訊，請參閱《AWS Key Management Service 開發人員指南》。

如需有關故障診斷金鑰存取的詳細資訊，請參閱《AWS Key Management Service 開發人員指南》。

指定已驗證存取資源的客戶管理金鑰

您可以指定客戶管理的金鑰，為下列資源提供第二層加密：

- 已驗證存取群組
- 驗證存取端點
- 驗證存取信任提供者

使用建立這些資源中的任何資源時 AWS Management Console，您可以在 [其他加密--選用] 區段中指定客戶管理的金鑰。在此程序中，選取 [自訂加密設定 (進階)] 核取方塊，然後輸入您要使用的 AWS KMS 金鑰 ID。這也可以在修改現有資源時或使用 AWS CLI.

> **Note**
>
> 如果用於向上述任何資源新增額外加密的客戶管理金鑰遺失，將無法再存取資源的組態值。不過，您可以使用 AWS Management Console 或 AWS CLI來套用新的客戶管理金鑰並重設組態值來修改資源。

AWS 已驗證存取加密內容

加密內容是一組選用的索引鍵值配對，其中包含有關資料的其他內容資訊。 AWS KMS 使用加密內容作為其他驗證資料，以支援已驗證的加密。當您在加密資料的要求中包含加密內容時，會將加密內容 AWS KMS 繫結至加密的資料。若要解密資料，您必須在請求中包含相同的加密內容。

AWS 已驗證存取加密內容

驗證存取在所有密 AWS KMS 碼編譯作業中使用相同的加密內容，其中金鑰所在，值為資源 Amazon 資源名稱 (ARN)。`aws:verified-access:arn`以下是「已驗證存取」資源的加密內容。

驗證存取信任提供者

```
"encryptionContext": {
    "aws:verified-access:arn":
    "arn:aws:ec2:region:111122223333:VerifiedAccessTrustProviderId"
}
```

已驗證存取群組

```
"encryptionContext": {
    "aws:verified-access:arn":
    "arn:aws:ec2:region:111122223333:VerifiedAccessGroupId"
}
```

驗證存取端點

```
"encryptionContext": {
    "aws:verified-access:arn":
    "arn:aws:ec2:region:111122223333:VerifiedAccessEndpointId"
}
```

如需有關在授權或原則中使用加密內容的詳細資訊，請參閱AWS Key Management Service 開發人員指南中的加密內容。

監控您的加密金鑰是否 AWS 已驗證存取

當您將客戶管理的KMS金鑰與 AWS 已驗證存取資源搭配使用時，您可AWS CloudTrail以使用追蹤已驗證存取權傳送至的要求 AWS KMS。

下列範例是、、、和的 AWS CloudTrail 事件 `CreateGrant` `RetireGrant` `Decrypt` `DescribeKey`，`GenerateDataKey`這些事件會監控「已驗證存取」呼叫的KMS作業，以存取由客戶管理的KMS金鑰加密的資料：

CreateGrant

當您使用客戶受管金鑰來加密資源時，「已驗證存取」會代表您傳送`CreateGrant`要求，以存取您 AWS 帳戶中的金鑰。「已驗證存取」建立的授與特定於與客戶管理金鑰相關聯的資源。

下面的範例事件會記錄 `CreateGrant` 操作：

```
{
    "eventVersion": "1.08",
    "userIdentity": {
```

```
        "type": "AssumedRole",
        "principalId": "AKIAI44QH8DHBEXAMPLE",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AKIAI44QH8DHBEXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-09-11T16:27:12Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "verified-access.amazonaws.com"
    },
    "eventTime": "2023-09-11T16:41:42Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateGrant",
    "awsRegion": "ca-central-1",
    "sourceIPAddress": "verified-access.amazonaws.com",
    "userAgent": "verified-access.amazonaws.com",
    "requestParameters": {
        "operations": [
            "Decrypt",
            "RetireGrant",
            "GenerateDataKey"
        ],
        "keyId": "arn:aws:kms:ca-central-1:111122223333:key/5ed79e7f-88c9-420c-
ae1a-61ee87104dae",
        "constraints": {
            "encryptionContextSubset": {
                "aws:verified-access:arn": "arn:aws:ec2:ca-
central-1:111122223333:verified-access-trust-provider/vatp-0e54f581e2e5c97a2"
            }
        },
        "granteePrincipal": "verified-access.ca-central-1.amazonaws.com",
        "retiringPrincipal": "verified-access.ca-central-1.amazonaws.com"
    },
```

```
    "responseElements": {
        "grantId":
 "e5a050fff9893ba1c43f83fddf61e5f9988f579beaadd6d4ad6d1df07df6048f",
        "keyId": "arn:aws:kms:ca-central-1:111122223333:key/5ed79e7f-88c9-420c-
ae1a-61ee87104dae"
    },
    "requestID": "0faa837e-5c69-4189-9736-3957278e6444",
    "eventID": "1b6dd8b8-cbee-4a83-9b9d-d95fa5f6fd08",
    "readOnly": false,
    "resources": [
        {
            "accountId": "AWS Internal",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:ca-central-1:111122223333:key/5ed79e7f-88c9-420c-
ae1a-61ee87104dae"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

RetireGrant

當您刪除資源時，已驗證的存取權會使用此RetireGrant作業移除授權。

下面的範例事件會記錄 RetireGrant 操作：

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AKIAI44QH8DHBEXAMPLE",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AKIAI44QH8DHBEXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
```

```
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-09-11T16:42:33Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "verified-access.amazonaws.com"
    },
    "eventTime": "2023-09-11T16:47:53Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "RetireGrant",
    "awsRegion": "ca-central-1",
    "sourceIPAddress": "verified-access.amazonaws.com",
    "userAgent": "verified-access.amazonaws.com",
    "requestParameters": null,
    "responseElements": {
        "keyId": "arn:aws:kms:ca-central-1:111122223333:key/5ed79e7f-88c9-420c-
ae1a-61ee87104dae"
    },
    "additionalEventData": {
        "grantId":
 "b35e66f9bacb266cec214fcaa353c9cf750785e28773e61ba6f434d8c5c7632f"
    },
    "requestID": "7d4a31c2-d426-434b-8f86-336532a70462",
    "eventID": "17edc343-f25b-43d4-bbff-150d8fff4cf8",
    "readOnly": false,
    "resources": [
        {
            "accountId": "AWS Internal",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:ca-central-1:111122223333:key/5ed79e7f-88c9-420c-
ae1a-61ee87104dae"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


Decrypt

驗證訪問調用Decrypt操作使用存儲的加密數據密鑰訪問加密的數據。

下面的範例事件會記錄 Decrypt 操作：

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AKIAI44QH8DHBEXAMPLE",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AKIAI44QH8DHBEXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-09-11T17:19:33Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "verified-access.amazonaws.com"
    },
    "eventTime": "2023-09-11T17:47:05Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "ca-central-1",
    "sourceIPAddress": "verified-access.amazonaws.com",
    "userAgent": "verified-access.amazonaws.com",
    "requestParameters": {
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
        "keyId": "arn:aws:kms:ca-
central-1:111122223333:key/380d006e-706a-464b-99c5-68768297114e",
        "encryptionContext": {
            "aws:verified-access:arn": "arn:aws:ec2:ca-
central-1:111122223333:verified-access-trust-provider/vatp-00f20a4e455e9340f",
            "aws-crypto-public-key": "AkK+vi1W/
acBKv7OR8p2DeUrA8EgpTffSrjBqNucODuBYhyZ3hlMuYYJz9x7CwQWZw=="
        }
    },
    "responseElements": null,
```

```
    "requestID": "2e920fd3-f2f6-41b2-a5e7-2c2cb6f853a9",
    "eventID": "3329e0a3-bcfb-44cf-9813-8106d6eee31d",
    "readOnly": true,
    "resources": [
        {
            "accountId": "AWS Internal",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:ca-
central-1:111122223333:key/380d006e-706a-464b-99c5-68768297114e"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

DescribeKey

「已驗證存取」會使用DescribeKey作業來驗證與您的資源相關聯的客戶管理金鑰是否存在於帳戶和區域中。

下面的範例事件會記錄 DescribeKey 操作：

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AKIAI44QH8DHBEXAMPLE",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AKIAI44QH8DHBEXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-09-11T17:19:33Z",
                "mfaAuthenticated": "false"
```

```
            }
        },
        "invokedBy": "verified-access.amazonaws.com"
    },
    "eventTime": "2023-09-11T17:46:48Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "DescribeKey",
    "awsRegion": "ca-central-1",
    "sourceIPAddress": "verified-access.amazonaws.com",
    "userAgent": "verified-access.amazonaws.com",
    "requestParameters": {
        "keyId": "arn:aws:kms:ca-
central-1:111122223333:key/380d006e-706a-464b-99c5-68768297114e"
    },
    "responseElements": null,
    "requestID": "5b127082-6691-48fa-bfb0-4d40e1503636",
    "eventID": "ffcfc2bb-f94b-4c00-b6fb-feac77daff2a",
    "readOnly": true,
    "resources": [
        {
            "accountId": "AWS Internal",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:ca-
central-1:111122223333:key/380d006e-706a-464b-99c5-68768297114e"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

GenerateDataKey

下面的範例事件會記錄 GenerateDataKey 操作：

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AKIAI44QH8DHBEXAMPLE",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
```

```
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AKIAI44QH8DHBEXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-09-11T17:19:33Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "verified-access.amazonaws.com"
    },
    "eventTime": "2023-09-11T17:46:49Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "ca-central-1",
    "sourceIPAddress": "verified-access.amazonaws.com",
    "userAgent": "verified-access.amazonaws.com",
    "requestParameters": {
        "encryptionContext": {
            "aws:verified-access:arn": "arn:aws:ec2:ca-
central-1:111122223333:verified-access-trust-provider/vatp-00f20a4e455e9340f",
            "aws-crypto-public-key": "A/ATGxaYatPUlOtM+l/mfDndkzHUmX5Hav+29IlIm
+JRBKFuXf24ulztmOIsqFQliw=="
        },
        "numberOfBytes": 32,
        "keyId": "arn:aws:kms:ca-
central-1:111122223333:key/380d006e-706a-464b-99c5-68768297114e"
    },
    "responseElements": null,
    "requestID": "06535808-7cce-4ae1-ab40-e3afbf158a43",
    "eventID": "1ce79601-5a5e-412c-90b3-978925036526",
    "readOnly": true,
    "resources": [
        {
            "accountId": "AWS Internal",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:ca-
central-1:111122223333:key/380d006e-706a-464b-99c5-68768297114e"
        }
```

```
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

已驗證存取的身分識別與存取管理

AWS Identity and Access Management (IAM) 可協助系統管理員安全地控制 AWS 資源存取權。 AWS 服務 IAM管理員控制誰可以驗證 (登入) 和授權 (具有權限) 使用已驗證存取資源。IAM是您 AWS 服務可以免費使用的。

主題

- 物件
- 使用身分驗證
- 使用政策管理存取權
- 驗證存取的使用方式 IAM
- 已驗證存取權的身分型原則範例
- 疑難排解驗證存取身分和存取
- 使用服務連結角色進行已驗證存取
- AWS 已驗證存取的受管理原則

物件

根據您在驗證存取權中執行的工作而定， AWS Identity and Access Management (IAM) 的使用方式會有所不同。

服務使用者 — 如果您使用「已驗證存取」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「已驗證存取」功能來完成工作時，您可能需要其他權限。了解存取許可的管理方式可協助您向管理員請求正確的許可。如果您無法存取已驗證存取權中的功能，請參閱疑難排解驗證存取身分和存取。

服務管理員 — 如果您負責公司的「驗證存取」資源，則可能擁有「已驗證存取權」的完整存取權。決定您的服務使用者應存取哪些「已驗證存取」功能和資源是您的工作。然後，您必須向IAM管理員提交

請求，才能變更服務使用者的權限。檢閱此頁面上的資訊，以瞭解的基本概念IAM。若要深入瞭解貴公司如何IAM透過驗證存取權使用，請參閱驗證存取的使用方式 IAM。

IAM系統管理員 — 如果您是IAM系統管理員，您可能想要瞭解如何撰寫原則來管理已驗證存取權的詳細資訊。若要檢視可在中使用的已驗證存取身分型原則範例IAM，請參閱。已驗證存取權的身分型原則範例

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角色來驗證 (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身分識別中心) 使用者、貴公司的單一登入驗證，以及您的 Google 或 Facebook 認證都是聯合身分識別的範例。當您以同盟身分登入時，您的管理員先前會使用IAM角色設定聯合身分識別。當您使 AWS 用同盟存取時，您會間接擔任角色。

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

如果您 AWS 以程式設計方式存取，請 AWS 提供軟體開發套件 (SDK) 和命令列介面 (CLI)，以使用您的認證以密碼編譯方式簽署您的要求。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要求的詳細資訊，請參閱使用IAM者指南中的簽署 AWS API要求。

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。若要深入瞭解，請參閱使用AWS IAM Identity Center 者指南中的多重要素驗證和使用多重要素驗證 (MFA) AWS的使用IAM者指南。

AWS 帳戶 根使用者

當您建立時 AWS 帳戶，您會從一個登入身分開始，該身分可完整存取該帳戶中的所有資源 AWS 服務和資源。此身分稱為 AWS 帳戶 root 使用者，可透過使用您用來建立帳戶的電子郵件地址和密碼登入來存取。強烈建議您不要以根使用者處理日常任務。保護您的根使用者憑證，並將其用來執行只能由根使用者執行的任務。如需需要您以 root 使用者身分登入的完整工作清單，請參閱《使用指南》中的〈需要 root 使用者認證的IAM工作〉。

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，也可以連線並同步處理至您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身分識別中心的相關資訊，請參閱IAM識別中心是什麼？ 在《AWS IAM Identity Center 使用者指南》中。

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權限。在可能的情況下，我們建議您仰賴臨時登入資料，而不要建立具有長期認證 (例如密碼和存取金鑰) 的IAM使用者。不過，如果您的特定使用案例需要使用IAM者的長期認證，建議您輪換存取金鑰。如需詳細資訊，請參閱《使用指南》中的「IAM定期輪換存取金鑰」以瞭解需要長期認證的使用案例。

IAM群組是指定IAM使用者集合的身分識別。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的群組，IAMAdmins並授與該群組管理IAM資源的權限。

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。要了解更多信息，請參閱《IAM用戶指南》中的創建用戶（而不是角色）的IAM時間。

IAM角色

IAM角色是您 AWS 帳戶 中具有特定權限的身份。它類似於用IAM戶，但不與特定人員相關聯。您可以 AWS Management Console 透過切換角色來暫時擔任中的角色。IAM您可以透過呼叫 AWS CLI 或 AWS API作業或使用自訂來擔任角色URL。如需有關使用角色方法的詳細資訊，請參閱《使用指南》中的IAM〈使用IAM角色〉。

IAM具有臨時認證的角色在下列情況下很有用：

- 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。如需聯合角色的相關資訊，請參閱《使用指南》中的〈建立第三方身分識別提供IAM者的角色〉。如果您使用IAM身分識別中心，則需要設定權限集。為了控制身分驗證後可以存取的內IAM容，IAMIdentity Center 會將權限集與中的角色相關聯。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使用者權限 — IAM 使用者或角色可以假定某個IAM角色，暫時取得特定工作的不同權限。
- 跨帳戶存取 — 您可以使用IAM角色允許不同帳戶中的某個人 (受信任的主體) 存取您帳戶中的資源。角色是授予跨帳戶存取權的主要方式。但是，對於某些策略 AWS 服務，您可以將策略直接附加到資源（而不是使用角色作為代理）。若要瞭解跨帳戶存取角色與以資源為基礎的政策之間的差異，請參閱《IAM使用指南》IAM中的〈跨帳號資源存取〉。
- 跨服務訪問 — 有些 AWS 服務 使用其他 AWS 服務功能。例如，當您在服務中撥打電話時，該服務通常會在 Amazon 中執行應用程式EC2或將物件存放在 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) — 當您使用使用IAM者或角色執行中的動作時 AWS，您會被視為主參與者。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會使用主參與者呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。FAS只有當服務收到需要與其他 AWS 服務 資源互動才能完成的請求時，才會發出請求。在此情況下，您必須具有執行這兩個動作的許可。有關提出FAS請求時的策略詳細信息，請參閱轉發訪問會話。
  - 服務角色 — 服務角色是指服務代表您執行動作所代表的IAM角色。IAM管理員可以從中建立、修改和刪除服務角色IAM。如需詳細資訊，請參閱《IAM使用指南》 AWS 服務中的建立角色以將權限委派給
  - 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 (但無法編輯服務連結角色) 的權限。
- 在 Amazon 上執行的應用程式 EC2 — 您可以使用IAM角色來管理在執行個體上EC2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。這比在EC2實例中存儲訪問密鑰更好。若要將 AWS 角色指派給EC2執行個體並讓其所有應用程式都能使用，請建立附加至執行個體的執行個體設定檔。執行個體設定檔包含角色，可讓執行個體上EC2執行的程式取得臨時登入資料。如需詳細資訊，請參閱使用者指南中的使用IAM角色將許可授與在 Amazon EC2 執行個體上執行的應IAM用程式。

要了解是否使用IAM角色還是用IAM戶，請參閱《用戶指南》中的「IAM創建IAM角色的時機（而不是用戶）」。

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。如需有關JSON原則文件結構和內容的詳細資訊，請參閱《IAM使用指南》中的策略概觀。JSON

管理員可以使用 AWS JSON策略來指定誰可以存取什麼內容。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。若要授與使用者對所需資源執行動作的權限，IAM管理員可以建立IAM策略。然後，系統管理員可以將IAM原則新增至角色，使用者可以擔任這些角色。

IAM原則會定義動作的權限，不論您用來執行作業的方法為何。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、或取得角色資訊 AWS API。

身分型政策

以身分識別為基礎的原則是您可以附加至身分識別 (例如使用者、使用IAM者群組或角色) 的JSON權限原則文件。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。若要瞭解如何建立以身分識別為基礎的策略，請參閱《IAM使用指南》中的〈建立IAM策略〉。

身分型政策可進一步分類成內嵌政策或受管政策。內嵌政策會直接內嵌到單一使用者、群組或角色。受管理的策略是獨立策略，您可以將其附加到您的 AWS 帳戶. 受管政策包括 AWS 受管政策和客戶管理的策略。若要了解如何在受管策略或內嵌策略之間進行選擇，請參閱《IAM使用手冊》中的「在受管策略和內嵌策略之間進行選擇」。

資源型政策

以資源為基礎的JSON策略是您附加至資源的政策文件。以資源為基礎的政策範例包括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策略IAM中使用 AWS 受管政策。

存取控制清單 (ACLs)

存取控制清單 (ACLs) 控制哪些主參與者 (帳戶成員、使用者或角色) 具有存取資源的權限。ACLs類似於以資源為基礎的策略，雖然它們不使用JSON政策文件格式。

Amazon S3 和 Amazon VPC 是支持服務的示例ACLs。 AWS WAF若要進一步了解ACLs，請參閱 Amazon 簡單儲存服務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。

- 權限界限 — 權限界限是一項進階功能，您可以在其中設定以身分識別為基礎的原則可授與給IAM實體 (IAM使用者或角色) 的最大權限。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。如需有關權限界限的詳細資訊，請參閱《IAM使用指南》中的IAM實體的權限界限。
- 服務控制策略 (SCPs) — SCPs 是指定中組織或組織單位 (OU) 最大權限的JSON策略 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。如果您啟用組織中的所有功能，則可以將服務控制策略 (SCPs) 套用至您的任何或所有帳戶。SCP限制成員帳戶中實體的權限，包括每個帳戶 AWS 帳戶根使用者。如需有關 Organizations 的詳細資訊SCPs，請參閱AWS Organizations 使用指南中的服務控制原則。
- 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使用指南》中的工作階段原則。

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。若要瞭解如何在涉及多個原則類型時 AWS 決定是否允許要求，請參閱IAM使用指南中的原則評估邏輯。

驗證存取的使用方式 IAM

在您用IAM來管理「已驗證存取權」的存取權之前，請先了解哪些IAM功能可搭配「已驗證存取」使用。

IAM特徵	驗證存取支援
身分型政策	是
資源型政策	否
政策動作	是
政策資源	是
政策條件索引鍵	是

IAM特徵	驗證存取支援
ACLs	否
ABAC(策略中的標籤)	部分
臨時憑證	是
主體許可	是
服務角色	否
服務連結角色	是

若要取得「已驗證存取」和其他 AWS 服務如何與大部分IAM功能搭配使用的高階檢視，請參閱IAM使用者指南IAM中的可使用AWS 服務。

已驗證存取權的基於身分的原則

支援身分型政策：是

以身分識別為基礎的原則是您可以附加至身分識別 (例如使用者、使用IAM者群組或角色) 的JSON權限原則文件。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。若要瞭解如何建立以身分識別為基礎的策略，請參閱《IAM使用指南》中的〈建立IAM策略〉。

使用以IAM身分識別為基礎的策略，您可以指定允許或拒絕的動作和資源，以及允許或拒絕動作的條件。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。若要瞭解可在JSON策略中使用的所有元素，請參閱《使用IAM者指南》中的IAMJSON策略元素參考資料。

已驗證存取權的身分型原則範例

若要檢視已驗證存取身分型原則的範例，請參閱。已驗證存取權的身分型原則範例

已驗證存取內的資源型政策

支援資源型政策：否

以資源為基礎的JSON策略是您附加至資源的政策文件。以資源為基礎的政策範例包括IAM角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條

件下執行的動作。您必須在資源型政策中指定主體。主參與者可以包括帳戶、使用者、角色、同盟使用者或。 AWS 服務

若要啟用跨帳戶存取，您可以在以資源為基礎的策略中指定一個或多個帳戶中的一個或多個帳戶中的IAM實體作為主體。新增跨帳戶主體至資源型政策，只是建立信任關係的一半。當主參與者和資源不同時 AWS 帳戶，受信任帳戶中的IAM管理員也必須授與主參與者實體 (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使用指南》IAM中的〈跨帳號資源存取〉。

已驗證存取權的原則動作

支援政策動作：是

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

JSON策略Action元素描述了您可以用來允許或拒絕策略中存取的動作。策略動作通常與關聯的 AWS API操作具有相同的名稱。有一些例外情況，例如沒有匹配API操作的僅限權限的操作。也有一些作業需要政策中的多個動作。這些額外的動作稱為相依動作。

政策會使用動作來授予執行相關聯動作的許可。

若要查看已驗證存取動作的清單，請參閱服務授權參考EC2中 Amazon 定義的動作。

「已驗證存取」中的原則動作會在動作之前使用下列前置詞：

```
ec2
```

若要在單一陳述式中指定多個動作，請用逗號分隔。

```
"Action": [
    "ec2:action1",
    "ec2:action2"
]
```

若要檢視已驗證存取身分型原則的範例，請參閱。已驗證存取權的身分型原則範例

已驗證存取權的原則資源

支援政策資源：是

管理員可以使用 AWS JSON策略來指定誰可以存取什麼內容。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。

ResourceJSON原則元素會指定要套用動作的一個或多個物件。陳述式必須包含 Resource 或 NotResource 元素。最佳做法是使用其 Amazon 資源名稱 (ARN) 指定資源。您可以針對支援特定資源類型的動作 (稱為資源層級許可) 來這麼做。

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

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

若要查看已驗證存取資源類型及其清單ARNs，請參閱服務授權參考EC2中由 Amazon 定義的資源。若要了解您可以針對每個資源指定ARN哪些動作，請參閱 Amazon 定義的動作EC2。

若要檢視已驗證存取身分型原則的範例，請參閱。已驗證存取權的身分型原則範例

已驗證存取權的原則條件金鑰

支援服務特定政策條件金鑰：是

管理員可以使用 AWS JSON策略來指定誰可以存取什麼內容。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，只有在IAM使用者名稱標記資源時，您才可以授與IAM使用者存取資源的權限。如需詳細資訊，請參閱《IAM使用指南》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 全域條件索引鍵，請參閱《使用指南》中的AWS 全域條件內IAM容索引鍵。

若要查看已驗證存取條件金鑰的清單，請參閱服務授權參考EC2中的 Amazon 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 定義的動作EC2。

若要檢視已驗證存取身分型原則的範例，請參閱。已驗證存取權的身分型原則範例

ACLs在已驗證的存取

支持ACLs：無

存取控制清單 (ACLs) 控制哪些主參與者 (帳戶成員、使用者或角色) 具有存取資源的權限。ACLs類似於以資源為基礎的策略，雖然它們不使用JSON政策文件格式。

ABAC具有已驗證存取

支援 ABAC (策略中的標籤): 部分

以屬性為基礎的存取控制 (ABAC) 是一種授權策略，可根據屬性定義權限。在中 AWS，這些屬性稱為標籤。您可以將標籤附加至IAM實體 (使用者或角色) 和許多 AWS 資源。標記實體和資源是的第一步ABAC。然後，您可以設計ABAC策略，以便在主參與者的標籤與他們嘗試存取的資源上的標籤相符時允許作業。

ABAC在快速成長的環境中很有幫助，並且有助於原則管理變得繁瑣的情況。

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。

如需有關的詳細資訊ABAC，請參閱什麼是ABAC？ 在《IAM使用者指南》中。若要檢視包含設定步驟的自學課程ABAC，請參閱《使用指南》中的〈使用以屬性為基礎的存取控制 (ABAC) IAM 〉。

使用臨時登入資料與驗證存取

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使用 AWS 服務 ，請參閱《IAM使用指南》IAM中的使用方式。

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，該程序會自動建立臨時認證。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。如需有關切換角色的詳細資訊，請參閱《IAM使用者指南》中的〈切換到角色 (主控台)〉。

您可以使用 AWS CLI 或手動建立臨時認證 AWS API。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。

已驗證存取的跨服務主體權限

支援轉寄存取工作階段 (FAS)：是

當您使用使用IAM者或角色在中執行動作時 AWS，您會被視為主參與者。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會使用主參與者呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。FAS只有當服務收到需要與其他 AWS 服務 資源互動才能完成的請求時，才會發出請求。在此情況下，您必須具有執行這兩個動作的許可。有關提出FAS請求時的策略詳細信息，請參閱轉發訪問會話。

已驗證存取權的服務角色

支援服務角色：否

服務角色是服務假定代表您執行動作的IAM角色。IAM管理員可以從中建立、修改和刪除服務角色 IAM。如需詳細資訊，請參閱《IAM使用指南》 AWS 服務中的建立角色以將權限委派給

已驗證存取的服務連結角色

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 (但無法編輯服務連結角色) 的權限。

如需建立或管理已驗證存取服務連結角色的詳細資訊，請參閱使用服務連結角色進行已驗證存取。

已驗證存取權的身分型原則範例

根據預設，使用者和角色沒有建立或修改已驗證存取資源的權限。他們也無法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或執行工作 AWS API。若要授與使用者對所需資源執行動作的權限，IAM管理員可以建立IAM策略。然後，系統管理員可以將IAM原則新增至角色，使用者可以擔任這些角色。

若要瞭解如何使用這些範例原則文件來建立以IAM身分識別為基礎的JSON策略，請參閱使用指南中的IAM建立IAM策略。

如需有關已驗證存取定義的動作和資源類型的詳細資訊，包括每種資源類型的格式，請參閱服務授權參考EC2中的 Amazon 適用的動作、資源和條件金鑰。ARNs

主題

政策最佳實務

以身分識別為基礎的政策會決定某人是否可以在您的帳戶中建立、存取或刪除已驗證存取資源。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管原則並邁向最低權限權限 — 若要開始授與使用者和工作負載的權限，請使用可授與許多常見使用案例權限的AWS 受管理原則。它們可用在您的 AWS 帳戶. 建議您透過定義特定於您使用案例的 AWS 客戶管理政策，進一步降低使用權限。如需詳細資訊，請參閱AWS 《IAM使用指南》中針對工作職能的AWS 受管理策略或受管理的策略。
- 套用最低權限權限 — 當您使用原則設定權限時，IAM只授與執行工作所需的權限。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需有關使用套用權限IAM的詳細資訊，請參閱《使用指南》IAM中的IAM《策略與權限》。
- 使用IAM策略中的條件進一步限制存取 — 您可以在策略中新增條件，以限制對動作和資源的存取。例如，您可以撰寫政策條件，以指定必須使用傳送所有要求SSL。您也可以使用條件來授與對服務動作的存取權 (如透過特定) 使用這些動作 AWS 服務，例如 AWS CloudFormation。如需詳細資訊，請參閱《IAM使用指南》中的IAMJSON策略元素：條件。
- 使用 IAM Access Analyzer 驗證您的原IAM則，以確保安全和功能性的權限 — IAM Access Analyzer會驗證新的和現有的原則，以便原則遵循IAM原則語言 (JSON) 和IAM最佳做法。IAMAccess Analyzer 提供超過 100 項原則檢查和可行的建議，協助您撰寫安全且功能正常的原則。如需詳細資訊，請參閱IAM使IAM用指南中的存取分析器原則驗證。
- 需要多因素驗證 (MFA) — 如果您的案例需要使IAM用者或 root 使用者 AWS 帳戶，請開啟以取得額外MFA的安全性。若要在呼叫API作業MFA時需要，請在原則中新增MFA條件。如需詳細資訊，請參閱《IAM使用指南》中的 < 設定MFA受保護的API存取 > 。

如需有關中最佳作法的詳細資訊IAM，請參閱《IAM使用指南》IAM中的「安全性最佳作法」。

建立驗證存取執行個體的政策

若要建立「已驗證存取」執行個體，IAM主體必須將這個額外的陳述式新增至其IAM原則。

```
{
```

```
    "Effect": "Allow",
    "Action": "verified-access:AllowVerifiedAccess",
    "Resource": "*"
}
```

> **Note**
>
> verified-access:AllowVerifiedAccess是僅限動作的虛擬。API它不支援資源、標籤或條件金鑰型授權。對ec2:CreateVerifiedAccessInstanceAPI動作使用資源、標籤或條件索引鍵型授權。

建立已驗證存取執行個體的範例原則。在此範例中，123456789012是 AWS 帳戶編號，us-east-1是 AWS 區域。

```
{
      "Version": "2012-10-17",
      "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVerifiedAccessInstance",
            "Resource": "arn:aws:ec2:us-east-1:123456789012:verified-access-instance/*"
        },
        {
            "Effect": "Allow",
            "Action": "verified-access:AllowVerifiedAccess",
            "Resource": "*"
        }
    ]
}
```

允許使用者檢視他們自己的許可

此範例顯示如何建立原則，讓使IAM用者檢視附加至其使用者身分識別的內嵌和受管理原則。此原則包含在主控台上或以程式設計方式使用或完成此動作的 AWS CLI 權限 AWS API。

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

疑難排解驗證存取身分和存取

使用下列資訊可協助您診斷及修正使用已驗證存取權和時可能會遇到的常見問題IAM。

問題

- 我沒有在已驗證存取權中執行動作的授權
- 我沒有授權執行 iam：PassRole
- 我想允許我以外的人訪問我 AWS 帳戶 的驗證訪問資源

我沒有在已驗證存取權中執行動作的授權

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。

當使用mateojacksonIAM者嘗試使用主控台來檢視虛構*my-example-widget*資源的詳細資料，但沒有虛構的ec2:*GetWidget*權限時，就會發生下列範例錯誤。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 ec2: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 ec2:*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。

我沒有授權執行 iam：PassRole

如果您收到未獲授權執行iam:PassRole動作的錯誤訊息，則必須更新您的政策，以允許您將角色傳遞給「已驗證的存取權」。

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

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

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

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

如果您需要協助，請聯絡您的 AWS 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問我 AWS 帳戶 的驗證訪問資源

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。對於支援以資源為基礎的政策或存取控制清單 (ACLs) 的服務，您可以使用這些政策授與人員存取您的資源。

如需進一步了解，請參閱以下內容：

- 若要瞭解已驗證存取是否支援這些功能，請參閱驗證存取的使用方式 IAM。
- 若要瞭解如何提供您所擁有資 AWS 帳戶 源的存取權，請參閱《IAM使用指南》中的〈提供存取權給您 AWS 帳戶 所擁有的其他IAM使用者〉。

- 若要瞭解如何將資源存取權提供給第三方 AWS 帳戶，請參閱《IAM使用指南》中的提供第三方 AWS 帳戶 擁有的存取權。
- 若要瞭解如何透過聯合身分識別提供存取權，請參閱使用指南中的提供對外部驗證使用IAM者的存取權 (身分聯合)。
- 若要瞭解針對跨帳號存取使用角色與以資源為基礎的政策之間的差異，請參閱《使用IAM者指南》IAM中的〈跨帳號資源存取〉。

使用服務連結角色進行已驗證存取

AWS Verified Access 使用 AWS Identity and Access Management (IAM) 服務連結角色。服務連結角色是直接連結至已驗證存取權的唯一IAM角色類型。服務連結角色由「已驗證存取」預先定義，並包含服務代表您呼叫其他人所需 AWS 服務 的所有權限。

服務連結角色可讓您更輕鬆地設定已驗證存取，因為您不需要手動新增必要的權限。「已驗證存取」會定義其服務連結角色的權限，除非另有定義，否則只有「已驗證存取」可以擔任其角色。定義的權限包括信任原則和權限原則，而且此權限原則無法附加至任何其他IAM實體。

如需支援服務連結角色之其他服務的相關資訊，請參閱使用的AWS 服務，IAM並在服務連結角色欄中尋找具有是的服務。選擇具有連結的是，以檢視該服務的服務連結角色文件。

已驗證存取權的服務連結角色權限

「已驗證存取」會使用指AWSServiceRoleForVPCVerifiedAccess定的服務連結角色，在您的帳戶中佈建使用服務所需的資源。

服AWSServiceRoleForVPCVerifiedAccess務連結角色會信任下列服務擔任該角色：

- `verified-access.amazonaws.com`

角色權限原則 (名為 AWSVPCVerifiedAccessServiceRolePolicy) 允許「已驗證存取」在指定資源上完成下列動作：

- 針`ec2:CreateNetworkInterface`對所有子網路和安全性群組，以及具有標籤的所有網路介面上執行動作 `VerifiedAccessManaged=true`
- 建立時`ec2:CreateTags`對所有網路介面執行的動作
- `ec2:DeleteNetworkInterface`在具有標籤的所有網路介面上執行動作 `VerifiedAccessManaged=true`

- `ec2:ModifyNetworkInterfaceAttribute`對所有安全群組和具有此標籤的所有網路介面執行動作 `VerifiedAccessManaged=true`

您也可以在中檢視此策略的權限 AWS Management Console AWSVPCVerifiedAccessServiceRolePolicy，或者您可以在《AWS 受管理的AWSVPCVerifiedAccessServiceRolePolicy策略參考指南》中檢視策略。

您必須設定權限，才能允許IAM實體 (例如使用者、群組或角色) 建立、編輯或刪除服務連結角色。如需詳細資訊，請參閱IAM使用指南中的服務連結角色權限。

建立已驗證存取的服務連結角色

您不需要手動建立一個服務連結角色。當您呼叫CreateVerifiedAccessEndpoint AWS Management Console、或「已驗證存取」時 AWS API，會為您建立服務連結角色。 AWS CLI

若您刪除此服務連結角色，之後需要再次建立，您可以在帳戶中使用相同程序重新建立角色。當您再CreateVerifiedAccessEndpoint次撥打電話時，「已驗證存取」會再次為您建立服務連結角色。

編輯已驗證存取權的服務連結角色

「已驗證存取」不允許您編輯AWSServiceRoleForVPCVerifiedAccess服務連結角色。因為有各種實體可能會參考服務連結角色，所以您無法在建立角色之後變更角色名稱。但是，您可以使用編輯角色的描述IAM。如需詳細資訊，請參閱IAM使用指南中的編輯服務連結角色。

刪除已驗證存取權的服務連結角色

您不需要手動刪除AWSServiceRoleForVPCVerifiedAccess角色。當您呼叫DeleteVerifiedAccessEndpoint AWS Management Console AWS CLI、或「已驗證存取」時 AWS API，會清除資源並為您刪除服務連結角色。

若要使用手動刪除服務連結角色 IAM

使用IAM主控台 AWS CLI、或刪除AWSServiceRoleForVPCVerifiedAccess服務連結角色。 AWS API 如需詳細資訊，請參閱IAM使用指南中的刪除服務連結角色。

已驗證存取服務連結角色的支援區域

「已驗證存取」支援在所有可用服務的 AWS 區域 地方使用服務連結角色。如需詳細資訊，請參閱AWS 區域與端點。

AWS 已驗證存取的受管理原則

受 AWS 管理的策略是由建立和管理的獨立策略 AWS。 AWS 受管理的策略旨在為許多常見使用案例提供權限，以便您可以開始將權限指派給使用者、群組和角色。

請記住， AWS 受管理的政策可能不會為您的特定使用案例授與最低權限權限，因為這些權限可供所有 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。

您無法變更受 AWS 管理策略中定義的權限。如果 AWS 更新 AWS 受管理原則中定義的權限，則此更新會影響附加原則的所有主體識別 (使用者、群組和角色)。 AWS 當新的啟動或新API作業可供現有服務使 AWS 服務 用時，最有可能更新 AWS 受管理的策略。

如需詳細資訊，請參閱IAM使用指南中的AWS 受管理策略。

AWS 受管理的策略： AWSVPCVerifiedAccessServiceRolePolicy

此原則附加至服務連結角色，可讓「已驗證存取」代表您執行動作。如需詳細資訊，請參閱使用服務連結角色。若要檢視此策略的權限，您可以AWSVPCVerifiedAccessServiceRolePolicy在中看到 AWS Management Console，或者您可以在《AWS 受管理的AWSVPCVerifiedAccessServiceRolePolicy策略參考指南》中檢視策略。

AWS 受管理策略的已驗證存取更新

檢視有關「已驗證存取」 AWS 受管理原則的詳細資料，因為此服務開始追蹤這些變更。如需有關此頁面變更的自動警示，請訂閱「已驗證存取文件歷史記錄」頁面上的RSS摘要。

變更	描述	日期
AWSVPCVerifiedAccessServiceRolePolicy-政策已更新	已驗證存取已更新其受管理的政策，以在「sid」欄位下包含所有動作的說明。	2023 年 11 月 17 日
AWSVPCVerifiedAccessServiceRolePolicy-政策已更新	已驗證存取已更新其受管理原則，將安全性群組資源新增至`ec2:CreateNetworkInterface` 權限。	2023 年 5 月 31 日
AWSVPCVerifiedAccessServiceRolePolicy – 新政策	已驗證存取新增政策，允許其在您的帳戶中佈建使用服務所需的資源。	2022 年 11 月 29 日

變更	描述	日期
已驗證存取開始追蹤變更	已驗證存取已開始追蹤其 AWS 受管理原則的變更。	2022 年 11 月 29 日

已驗證存取的合規性驗證

AWS Verified Access 可以配置為支持聯邦信息處理標準（FIPS）合規性。如需有關設定已驗證存取FIPS合規性的詳細資訊和詳細資訊，請移至FIPS已驗證存取的合規性。

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 上進行HIPAA安全與合規架構 — 本白皮書說明公司如何使用建立符合資格的應 AWS 用程HIPAA式。

> **Note**
>
> 並非所有 AWS 服務 人都HIPAA符合資格。如需詳細資訊，請參閱合HIPAA格服務參考。

- 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 AWS 服務 與技術研究所 (NIST)、支付卡產業安全標準委員會 () 和國際標準化組織 ()PCI) 中保護安全控制指引的最佳做法，並對應至安全控制措施。ISO
- 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 可協助您因應各種合規性需求 PCIDSS，例如符合特定合規性架構所要求的入侵偵測需求。
- 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。

已驗證存取中的彈性

AWS 全球基礎架構是圍繞 AWS 區域 和可用區域建立的。 AWS 區域 提供多個實體分離和隔離的可用區域，這些區域透過低延遲、高輸送量和高度備援的網路連線。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、容錯能力和擴展能力，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 和可用區域的詳細資訊，請參閱AWS 全域基礎結構。

除了 AWS 全球基礎結構之外，「驗證存取」還提供下列功能，以協助支援您的高可用性需求。

多個子網路提供高可用性

當您建立負載平衡器類型已驗證存取端點時，您可以將多個子網路關聯到該端點。與端點關聯的每個子網路都必須屬於不同的可用區域。透過關聯多個子網路，您可以使用多個可用區域來確保高可用性。

監控 AWS Verified Access

監控是維護的可靠性、可用性和效能的重要組成部分 AWS Verified Access。 AWS 提供下列監視工具來監視「已驗證存取」、在發生錯誤時報告，並在適當時採取自動處理行動：

- 存取記錄 — 擷取有關存取應用程式之請求的詳細資訊。如需詳細資訊，請參閱the section called “驗證存取日誌”。
- AWS CloudTrail— 擷取由您或代表您發出的API呼叫和相關事件， AWS 帳戶 並將日誌檔傳送到您指定的 Amazon S3 儲存貯體。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。如需詳細資訊，請參閱the section called “CloudTrail 日誌”。

驗證存取日誌

AWS Verified Access 評估每個訪問請求後，它會記錄所有訪問嘗試。這可讓您集中掌握應用程式存取權限，並協助您快速回應安全性事件和稽核要求。驗證存取支援開放網路安全架構架構架構 (OCSF) 記錄格式。

啟用記錄時，您必須設定要傳送記錄的目的地。用來設定記錄目的地的IAM主體必須具有特定的權限，才能正常運作記錄。您可以在驗證存取記錄權限本節中看到每個記錄目的地的必要IAM權限。「已驗證存取」支援下列目的地來發佈存取記錄：

- Amazon CloudWatch 日誌日誌群組
- Amazon S3 儲存貯體
- Amazon 數據 Firehose 交付流

目錄

驗證存取記錄版本

默認情況下，驗證訪問日誌系統使用開放網絡安全模式框架（OCSF）版本 0.1。您可以在本OCSF版本 0.1 日誌示例驗證訪問節中看到使用版本 0.1 的範例記錄檔。

最新的記錄版本與 1.0.0-rc. OCSF 2 版相容。關於架構的具體細節可以在這裡找到OCSF架構。您可以在本節中看到使用版本 1.0.0-rc.2 的範例記錄檔。OCSF版本 1.0.0-rc.2 日誌示例驗證的訪問

如果您要升級正在使用的記錄版本，請使用下列程序。

使用主控台升級記錄版本

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在瀏覽窗格中，選擇 [已驗證存取] 執行個體。
3. 選取適當的已驗證存取執行個體。
4. 在驗證存取執行個體記錄組態標籤上，選擇修改已驗證存取執行個體記錄組態。
5. 從「更新記錄檔版本」下拉式清單中選取 ocsf-1.0.0-rc.2。
6. 選擇修改已驗證存取執行處理記錄組態

若要使用升級記錄版本 AWS CLI

使用 modify-verified-access-instance-日誌配置命令。

驗證存取記錄權限

用來設定記錄目的地的IAM主體必須具有特定的權限，才能正常運作記錄。下列各節顯示每個記錄目的地所需的權限。

若要傳送至 CloudWatch 記錄檔：

- `ec2:ModifyVerifiedAccessInstanceLoggingConfiguration`在已驗證存取實例上
- `logs:CreateLogDelivery`、`logs:DeleteLogDelivery`、`logs:GetLogDeliverylogs:ListLog`和所`logs:UpdateLogDelivery`有資源
- `logs:DescribeLogGroupslogs:DescribeResourcePolicies`、和`logs:PutResourcePolicy`在目的地記錄群組上

對於交付到 Amazon S3：

- ec2:ModifyVerifiedAccessInstanceLoggingConfiguration在已驗證存取實例上
- logs:CreateLogDelivery、logs:DeleteLogDelivery、logs:GetLogDeliverylogs:ListLog和所logs:UpdateLogDelivery有資源
- s3:GetBucketPolicy並s3:PutBucketPolicy在目的地桶

運送至 Firehose：

- ec2:ModifyVerifiedAccessInstanceLoggingConfiguration在已驗證存取實例上
- firehose:TagDeliveryStream在所有資源
- iam:CreateServiceLinkedRole在所有資源
- logs:CreateLogDelivery、logs:DeleteLogDelivery、logs:GetLogDeliverylogs:ListLog和所logs:UpdateLogDelivery有資源

啟用或停用已驗證存取記錄

您可以使用本節中的程序來啟用或停用記錄。啟用記錄時，您必須設定要傳送記錄的目的地。用來設定記錄目的地的IAM主體必須具有特定的權限，才能正常運作記錄。您可以在驗證存取記錄權限本節中看到每個記錄目的地的必要IAM權限。

目錄

啟用存取日誌

使用已驗證存取記錄檔

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在瀏覽窗格中，選擇 [已驗證存取] 執行個體。
3. 選取已驗證存取權執行個體。
4. 在驗證存取執行個體記錄組態標籤上，選擇修改已驗證存取執行個體記錄組態。
5. (選擇性) 若要在記錄檔中包含從信任提供者傳送的信任資料，請執行下列動作：

a. 從「更新記錄檔版本」下拉式清單中選取 ocsf-1.0.0-rc.2。
b. 選擇 [包含信任內容]。

6. 執行以下任意一項：
   - 開啟 [傳送至 Amazon CloudWatch 日誌]。選擇目的地記錄群組。
   - 開啟交付至 Amazon S3。輸入目的地值區的名稱、擁有者和字首。
   - 開啟「送到 Firehose。選擇目的地交付串流。
7. 選擇修改已驗證存取執行處理記錄組態

使用啟用已驗證存取記錄 AWS CLI

使用 modify-verified-access-instance-日誌配置命令。

停用存取日誌

您可以隨時停用「已驗證存取」執行個體的存取記錄。停用存取記錄後，您的記錄檔資料會保留在記錄目的地中，直到您將其刪除為止。

使用已驗證存取記錄檔

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在瀏覽窗格中，選擇 [已驗證存取] 執行個體。
3. 選取已驗證存取權執行個體。
4. 在驗證存取執行個體記錄組態標籤上，選擇修改已驗證存取執行個體記錄組態。
5. 關閉記錄傳送。
6. 選擇修改已驗證存取執行處理記錄組態

若要使用停用已驗證存取記錄 AWS CLI

使用 modify-verified-access-instance-日誌配置命令。

啟用或停用已驗證存取信任內容

您可以選擇性地啟用從信任提供者傳送的信任內容，以包含在您的已驗證存取記錄中。這在定義允許或拒絕應用程式存取的原則時很有用。啟用它之後，信任內容會在data欄位下的記錄檔中找到。如果停用信任內容，則data欄位會設定為null。若要將已驗證存取設定為在記錄檔中包含信任內容，請執行下列程序。

> **Note**
>
> 在「已驗證存取」記錄中包含信任內容，需要升級至最新的記錄版本`ocsf-1.0.0-rc.2`。下列程序假設您已啟用記錄。如果不是這樣，請參閱以啟用存取日誌取得完整程序。

目錄

啟用信任內容

使用主控台在已驗證存取記錄檔中包含信任內容

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在瀏覽窗格中，選擇 [已驗證存取] 執行個體。
3. 選取適當的已驗證存取執行個體。
4. 在驗證存取執行個體記錄組態標籤上，選擇修改已驗證存取執行個體記錄組態。
5. 從「更新記錄檔版本」下拉式清單中選取 ocsf-1.0.0-rc.2。
6. 開啟 [包含信任內容]。
7. 選擇修改已驗證存取執行處理記錄組態

若要在已驗證存取記錄中包含信任內容，請使用 AWS CLI

使用 modify-verified-access-instance-日誌配置命令。

停用信任內容

如果您不想再在記錄檔中包含信任內容，可以透過執行下列程序將其移除。

使用主控台從「已驗證存取」記錄檔移除信任內容

1. 在打開 Amazon VPC 控制台https://console.aws.amazon.com/vpc/。
2. 在瀏覽窗格中，選擇 [已驗證存取] 執行個體。
3. 選取適當的已驗證存取執行個體。
4. 在驗證存取執行個體記錄組態標籤上，選擇修改已驗證存取執行個體記錄組態。

5. 關閉「包含信任內容」。
6. 選擇修改已驗證存取執行處理記錄組態

若要從 [已驗證存取] 記錄檔移除信任內容，請使用 AWS CLI

使用 modify-verified-access-instance-日誌配置命令。

OCSF版本 0.1 日誌示例驗證訪問

以下是使用預設記錄OCSF版本 0.1 的範例記錄檔。

範例

- 授與的存取權 OIDC
- 授與OIDC和的存取權 JAMF
- 授與OIDC和的存取權 CrowdStrike
- 由於缺少 cookie 而拒絕訪問
- 政策拒絕存取
- 未知的記錄項目

授與的存取權 OIDC

在此範例記錄項目中，「已驗證存取」允許存取具有OIDC使用者信任提供者的端點。


```
{
    "activity": "Access Granted",
    "activity_id": "1",
    "category_name": "Application Activity",
    "category_uid": "8",
    "class_name": "Access Logs",
    "class_uid": "208001",
    "device": {
        "ip": "10.2.7.68",
        "type": "Unknown",
        "type_id": 0
    },
    "duration": "0.004",
    "end_time": "1668580194344",
    "time": "1668580194344",
    "http_request": {
```

```
        "http_method": "GET",
        "url": {
            "hostname": "hello.app.example.com",
            "path": "/",
            "port": 443,
            "scheme": "https",
            "text": "https://hello.app.example.com:443/"
        },
        "user_agent": "python-requests/2.28.1",
        "version": "HTTP/1.1"
    },
    "http_response": {
        "code": 200
    },
    "identity": {
        "authorizations": [
            {
                "decision": "Allow",
                "policy": {
                    "name": "inline"
                }
            }
        ],
        "idp": {
            "name": "user",
            "uid": "vatp-09bc4cbce2EXAMPLE"
        },
        "user": {
            "email_addr": "johndoe@example.com",
            "name": "Test User Display",
            "uid": "johndoe@example.com",
            "uuid": "00u6wj48lbxTAEXAMPLE"
        }
    },
    "message": "",
    "metadata": {
        "uid": "Root=1-63748362-6408d24241120b942EXAMPLE",
        "logged_time": 1668580281337,
        "version": "0.1",
        "product": {
            "name": "Verified Access",
            "vendor_name": "AWS"
        }
    },
```

```
    "ref_time": "2022-11-16T06:29:54.344948Z",
    "proxy": {
        "ip": "192.168.34.167",
        "port": 443,
        "svc_name": "Verified Access",
        "uid": "vai-002fa341aeEXAMPLE"
    },
    "severity": "Informational",
    "severity_id": "1",
    "src_endpoint": {
        "ip": "172.24.57.68",
        "port": "48234"
    },
    "start_time": "1668580194340",
    "status_code": "100",
    "status_details": "Access Granted",
    "status_id": "1",
    "status": "Success",
    "type_uid": "20800101",
    "type_name": "AccessLogs: Access Granted",
    "unmapped": null
}
```


授與OIDC和的存取權 JAMF

在此範例記錄項目中，「已驗證存取」允許存取同時具有OIDC和JAMF裝置信任提供者的端點。


```
{
    "activity": "Access Granted",
    "activity_id": "1",
    "category_name": "Application Activity",
    "category_uid": "8",
    "class_name": "Access Logs",
    "class_uid": "208001",
    "device": {
        "ip": "10.2.7.68",
        "type": "Unknown",
        "type_id": 0,
        "uid": "41b07859-4222-4f41-f3b9-97dc1EXAMPLE"
    },
    "duration": "0.347",
    "end_time": "1668804944086",
    "time": "1668804944086",
```

```
    "http_request": {
        "http_method": "GET",
        "url": {
            "hostname": "hello.app.example.com",
            "path": "/",
            "port": 443,
            "scheme": "h2",
            "text": "https://hello.app.example.com:443/"
        },
        "user_agent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36",
        "version": "HTTP/2.0"
    },
    "http_response": {
        "code": 304
    },
    "identity": {
        "authorizations": [
            {
                "decision": "Allow",
                "policy": {
                    "name": "inline"
                }
            }
        ],
        "idp": {
            "name": "oidc",
            "uid": "vatp-9778003bc2EXAMPLE"
        },
        "user": {
            "email_addr": "johndoe@example.com",
            "name": "Test User Display",
            "uid": "johndoe@example.com",
            "uuid": "4f040d0f96becEXAMPLE"
        }
    },
    "message": "",
    "metadata": {
        "uid": "Root=1-321318ce-6100d340adf4fb29dEXAMPLE",
        "logged_time": 1668805278555,
        "version": "0.1",
        "product": {
            "name": "Verified Access",
            "vendor_name": "AWS"
```

```
        }
    },
    "ref_time": "2022-11-18T20:55:44.086480Z",
    "proxy": {
        "ip": "10.5.192.96",
        "port": 443,
        "svc_name": "Verified Access",
        "uid": "vai-3598f66575EXAMPLE"
    },
    "severity": "Informational",
    "severity_id": "1",
    "src_endpoint": {
        "ip": "192.168.20.246",
        "port": 61769
    },
    "start_time": "1668804943739",
    "status_code": "100",
    "status_details": "Access Granted",
    "status_id": "1",
    "status": "Success",
    "type_uid": "20800101",
    "type_name": "AccessLogs: Access Granted",
    "unmapped": null
}
```

授與OIDC和的存取權 CrowdStrike

在此範例記錄項目中，「已驗證存取」允許存取同時具有OIDC和 CrowdStrike 裝置信任提供者的端點。

```
{
    "activity": "Access Granted",
    "activity_id": "1",
    "category_name": "Application Activity",
    "category_uid": "8",
    "class_name": "Access Logs",
    "class_uid": "208001",
    "device": {
        "ip": "10.2.173.3",
        "os": {
            "name": "Windows 11",
            "type": "Windows",
            "type_id": 100
```

```
        },
        "type": "Unknown",
        "type_id": 0,
        "uid": "122978434f65093aee5dfbdc0EXAMPLE",
        "hw_info": {
            "serial_number": "751432a1-d504-fd5e-010d-5ed11EXAMPLE"
        }
    },
    "duration": "0.028",
    "end_time": "1668816620842",
    "time": "1668816620842",
    "http_request": {
        "http_method": "GET",
        "url": {
            "hostname": "test.app.example.com",
            "path": "/",
            "port": 443,
            "scheme": "h2",
            "text": "https://test.app.example.com:443/"
        },
        "user_agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36",
        "version": "HTTP/2.0"
    },
    "http_response": {
        "code": 304
    },
    "identity": {
        "authorizations": [
            {
                "decision": "Allow",
                "policy": {
                    "name": "inline"
                }
            }
        ],
        "idp": {
            "name": "oidc",
            "uid": "vatp-506d9753f6EXAMPLE"
        },
        "user": {
            "email_addr": "johndoe@example.com",
            "name": "Test User Display",
            "uid": "johndoe@example.com",
```

```
            "uuid": "23bb45b16a389EXAMPLE"
        }
    },
    "message": "",
    "metadata": {
        "uid": "Root=1-c16c5a65-b641e4056cc6cb0eeEXAMPLE",
        "logged_time": 1668816977134,
        "version": "0.1",
        "product": {
            "name": "Verified Access",
            "vendor_name": "AWS"
        }
    },
    "ref_time": "2022-11-19T00:10:20.842295Z",
    "proxy": {
        "ip": "192.168.144.62",
        "port": 443,
        "svc_name": "Verified Access",
        "uid": "vai-2f80f37e64EXAMPLE"
    },
    "severity": "Informational",
    "severity_id": "1",
    "src_endpoint": {
        "ip": "10.14.173.3",
        "port": 55706
    },
    "start_time": "1668816620814",
    "status_code": "100",
    "status_details": "Access Granted",
    "status_id": "1",
    "status": "Success",
    "type_uid": "20800101",
    "type_name": "AccessLogs: Access Granted",
    "unmapped": null
}
```


由於缺少 cookie 而拒絕訪問

在此範例記錄項目中，「已驗證存取」會因缺少驗證 Cookie 而拒絕存取。


```
{
    "activity": "Access Denied",
    "activity_id": "2",
```

```
    "category_name": "Application Activity",
    "category_uid": "8",
    "class_name": "Access Logs",
    "class_uid": "208001",
    "device": null,
    "duration": "0.0",
    "end_time": "1668593568259",
    "time": "1668593568259",
    "http_request": {
        "http_method": "POST",
        "url": {
            "hostname": "hello.app.example.com",
            "path": "/dns-query",
            "port": 443,
            "scheme": "h2",
            "text": "https://hello.app.example.com:443/dns-query"
        },
        "user_agent": "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML",
        "version": "HTTP/2.0"
    },
    "http_response": {
        "code": 302
    },
    "identity": null,
    "message": "",
    "metadata": {
        "uid": "Root=1-5cf1c832-a565309ce20cc7dafEXAMPLE",
        "logged_time": 1668593776720,
        "version": "0.1",
        "product": {
            "name": "Verified Access",
            "vendor_name": "AWS"
        }
    },
    "ref_time": "2022-11-16T10:12:48.259762Z",
    "proxy": {
        "ip": "192.168.34.167",
        "port": 443,
        "svc_name": "Verified Access",
        "uid": "vai-108ed7a672EXAMPLE"
    },
    "severity": "Informational",
    "severity_id": "1",
    "src_endpoint": {
```

```
        "ip": "10.7.178.16",
        "port": "46246"
    },
    "start_time": "1668593568258",
    "status_code": "200",
    "status_details": "Authentication Denied",
    "status_id": "2",
    "status": "Failure",
    "type_uid": "20800102",
    "type_name": "AccessLogs: Access Denied",
    "unmapped": null
}
```

政策拒絕存取

在此範例記錄項目中，「已驗證存取」會拒絕已驗證的要求，因為存取原則不允許該要求。

```
{
    "activity": "Access Denied",
    "activity_id": "2",
    "category_name": "Application Activity",
    "category_uid": "8",
    "class_name": "Access Logs",
    "class_uid": "208001",
    "device": {
        "ip": "10.4.133.137",
        "type": "Unknown",
        "type_id": 0
    },
    "duration": "0.023",
    "end_time": "1668573630978",
    "time": "1668573630978",
    "http_request": {
        "http_method": "GET",
        "url": {
            "hostname": "hello.app.example.com",
            "path": "/",
            "port": 443,
            "scheme": "h2",
            "text": "https://hello.app.example.com:443/"
        },
        "user_agent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36",
```

```
        "version": "HTTP/2.0"
    },
    "http_response": {
        "code": 401
    },
    "identity": {
        "authorizations": [],
        "idp": {
            "name": "user",
            "uid": "vatp-e048b3e0f8EXAMPLE"
        },
        "user": {
            "email_addr": "johndoe@example.com",
            "name": "Test User Display",
            "uid": "johndoe@example.com",
            "uuid": "0e1281ad3580aEXAMPLE"
        }
    },
    "message": "",
    "metadata": {
        "uid": "Root=1-531a036a-09e95794c7b96aefbEXAMPLE",
        "logged_time": 1668573773753,
        "version": "0.1",
        "product": {
            "name": "Verified Access",
            "vendor_name": "AWS"
        }
    },
    "ref_time": "2022-11-16T04:40:30.978732Z",
    "proxy": {
        "ip": "3.223.34.167",
        "port": 443,
        "svc_name": "Verified Access",
        "uid": "vai-021d5eaed2EXAMPLE"
    },
    "severity": "Informational",
    "severity_id": "1",
    "src_endpoint": {
        "ip": "10.4.133.137",
        "port": "31746"
    },
    "start_time": "1668573630955",
    "status_code": "300",
    "status_details": "Authorization Denied",
```

```
    "status_id": "2",
    "status": "Failure",
    "type_uid": "20800102",
    "type_name": "AccessLogs: Access Denied",
    "unmapped": null
}
```

未知的記錄項目

在此範例記錄項目中，「已驗證存取」無法產生完整的記錄項目，因此會發出未知的記錄項目。這可確保每個請求都出現在訪問日誌中。

```
{
    "activity": "Unknown",
    "activity_id": "0",
    "category_name": "Application Activity",
    "category_uid": "8",
    "class_name": "Access Logs",
    "class_uid": "208001",
    "device": null,
    "duration": "0.004",
    "end_time": "1668580207898",
    "time": "1668580207898",
    "http_request": {
        "http_method": "GET",
        "url": {
            "hostname": "hello.app.example.com",
            "path": "/",
            "port": 443,
            "scheme": "https",
            "text": "https://hello.app.example.com:443/"
        },
        "user_agent": "python-requests/2.28.1",
        "version": "HTTP/1.1"
    },
    "http_response": {
        "code": 200
    },
    "identity": null,
    "message": "",
    "metadata": {
        "uid": "Root=1-435eb955-6b5a1d529343f5adaEXAMPLE",
        "logged_time": 1668580579147,
```

```
        "version": "0.1",
        "product": {
            "name": "Verified Access",
            "vendor_name": "AWS"
        }
    },
    "ref_time": "2022-11-16T06:30:07.898344Z",
    "proxy": {
        "ip": "10.1.34.167",
        "port": 443,
        "svc_name": "Verified Access",
        "uid": "vai-6c32b53b3cEXAMPLE"
    },
    "severity": "Informational",
    "severity_id": "1",
    "src_endpoint": {
        "ip": "172.28.57.68",
        "port": "47220"
    },
    "start_time": "1668580207893",
    "status_code": "000",
    "status_details": "Unknown",
    "status_id": "0",
    "status": "Unknown",
    "type_uid": "20800100",
    "type_name": "AccessLogs: Unknown",
    "unmapped": null
}
```

OCSF版本 1.0.0-rc.2 日誌示例驗證的訪問

以下是使用記錄OCSF版本 1.0.0-rc.2 的範例記錄檔。

目錄

包含信任內容授予的存取權

```
{
    "activity_name": "Access Grant",
```

```
    "activity_id": "1",
    "actor": {
        "authorizations": [{
            "decision": "Allow",
            "policy": {
                "name": "inline"
            }
        }],
        "idp": {
            "name": "user",
            "uid": "vatp-09bc4cbce2EXAMPLE"
        },
        "invoked_by": "",
        "process": {},
        "user": {
            "email_addr": "johndoe@example.com",
            "name": "Test User Display",
            "uid": "johndoe@example.com",
            "uuid": "00u6wj48lbxTAEXAMPLE"
        },
        "session": {}
    },
    "category_name": "Audit Activity",
    "category_uid": "3",
    "class_name": "Access Activity",
    "class_uid": "3006",
    "device": {
        "ip": "10.2.7.68",
        "type": "Unknown",
        "type_id": 0
    },
    "duration": "0.004",
    "end_time": "1668580194344",
    "time": "1668580194344",
    "http_request": {
        "http_method": "GET",
        "url": {
            "hostname": "hello.app.example.com",
            "path": "/",
            "port": 443,
            "scheme": "https",
            "text": "https://hello.app.example.com:443/"
        },
        "user_agent": "python-requests/2.28.1",
```

```
        "version": "HTTP/1.1"
    },
    "http_response": {
        "code": 200
    },
    "message": "",
    "metadata": {
        "uid": "Root=1-63748362-6408d24241120b942EXAMPLE",
        "logged_time": 1668580281337,
        "version": "1.0.0-rc.2",
        "product": {
            "name": "Verified Access",
            "vendor_name": "AWS"
        }
    },
    "ref_time": "2022-11-16T06:29:54.344948Z",
    "proxy": {
        "ip": "192.168.34.167",
        "port": 443,
        "svc_name": "Verified Access",
        "uid": "vai-002fa341aeEXAMPLE"
    },
    "severity": "Informational",
    "severity_id": "1",
    "src_endpoint": {
        "ip": "172.24.57.68",
        "port": "48234"
    },
    "start_time": "1668580194340",
    "status_code": "100",
    "status_detail": "Access Granted",
    "status_id": "1",
    "status": "Success",
    "type_uid": "300601",
    "type_name": "Access Activity: Access Grant",
    "data": {
        "context": {
            "oidc": {
                "family_name": "Last",
                "zoneinfo": "America/Los_Angeles",
                "exp": 1670631145,
                "middle_name": "Middle",
                "given_name": "First",
                "email_verified": true,
```

```
                "name": "Test User Display",
                "updated_at": 1666305953,
                "preferred_username": "johndoe-user@test.com",
                "profile": "http://www.example.com",
                "locale": "US",
                "nickname": "Tester",
                "email": "johndoe-user@test.com"
            },
            "http_request": {
                "x_forwarded_for": "1.1.1.1,2.2.2.2",
                "http_method": "GET",
                "user_agent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36",
                "port": "80",
                "hostname": "hostname.net"
            }
        }
    }
}
```

已忽略信任內容授予的存取權

```
{
    "activity_name": "Access Grant",
    "activity_id": "1",
    "actor": {
        "authorizations": [{
            "decision": "Allow",
            "policy": {
                "name": "inline"
            }
        }],
        "idp": {
            "name": "user",
            "uid": "vatp-09bc4cbce2EXAMPLE"
        },
        "invoked_by": "",
        "process": {},
        "user": {
            "email_addr": "johndoe@example.com",
            "name": "Test User Display",
            "uid": "johndoe@example.com",
            "uuid": "00u6wj48lbxTAEXAMPLE"
```

```
        },
        "session": {}
    },
    "category_name": "Audit Activity",
    "category_uid": "3",
    "class_name": "Access Activity",
    "class_uid": "3006",
    "device": {
        "ip": "10.2.7.68",
        "type": "Unknown",
        "type_id": 0
    },
    "duration": "0.004",
    "end_time": "1668580194344",
    "time": "1668580194344",
    "http_request": {
        "http_method": "GET",
        "url": {
            "hostname": "hello.app.example.com",
            "path": "/",
            "port": 443,
            "scheme": "https",
            "text": "https://hello.app.example.com:443/"
        },
        "user_agent": "python-requests/2.28.1",
        "version": "HTTP/1.1"
    },
    "http_response": {
        "code": 200
    },
    "message": "",
    "metadata": {
        "uid": "Root=1-63748362-6408d24241120b942EXAMPLE",
        "logged_time": 1668580281337,
        "version": "1.0.0-rc.2",
        "product": {
            "name": "Verified Access",
            "vendor_name": "AWS"
        }
    },
    "ref_time": "2022-11-16T06:29:54.344948Z",
    "proxy": {
        "ip": "192.168.34.167",
        "port": 443,
```

```
        "svc_name": "Verified Access",
        "uid": "vai-002fa341aeEXAMPLE"
    },
    "severity": "Informational",
    "severity_id": "1",
    "src_endpoint": {
        "ip": "172.24.57.68",
        "port": "48234"
    },
    "start_time": "1668580194340",
    "status_code": "100",
    "status_detail": "Access Granted",
    "status_id": "1",
    "status": "Success",
    "type_uid": "300601",
    "type_name": "Access Activity: Access Grant",
    "data": null
}
```


使用記錄已驗證存取API呼叫 AWS CloudTrail

AWS 「已驗證存取」與服務整合 AWS CloudTrail，可提供使用者、角色或「已驗證存取」 AWS 服務 中所採取的動作記錄的服務。 CloudTrail 將「已驗證存取」的所有API呼叫擷取為事件。擷取的呼叫包括來自「已驗證存取」主控台的呼叫，以及對已驗證存取API作業的程式碼呼叫 如果您建立追蹤，您可以啟用持續交付 CloudTrail事件到 Amazon S3 儲存貯體，包括已驗證存取的事件。如果您未設定追蹤，您仍然可以在 [事件歷程記錄] 中檢視 CloudTrail 主控台中最近的事件。使用收集的資訊 CloudTrail，您可以判斷向「已驗證存取」提出的要求、提出要求的 IP 位址、提出要求的人員、提出要求的時間，以及其他詳細資訊。

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

已驗證的存取資訊 CloudTrail

CloudTrail 在您創建帳戶 AWS 帳戶 時啟用。當活動發生在已驗證的存取權中時，該活動會與 CloudTrail 事件歷史記錄中的其他 AWS 服務 事件一起記錄在事件中。您可以檢視、搜尋和下載 AWS 帳戶的最新事件。如需詳細資訊，請參閱使用 CloudTrail 事件歷程記錄檢視事件。

如需您 AWS 帳戶的事件的持續記錄 (包括已驗證存取權的事件)，請建立追蹤。追蹤可 CloudTrail 將日誌檔交付到 Amazon S3 儲存貯體。依預設，當您在主控台中建立追蹤時，該追蹤會套用至所有的 AWS 區域。追蹤記錄來自 AWS 分區中所有區域的事件，並將日誌檔傳送到您指定的 Amazon S3 儲

存貯體。此外，您可以設定其他， AWS 服務 以進一步分析 CloudTrail 記錄中收集的事件資料並採取行動。如需詳細資訊，請參閱下列內容：

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

所有已驗證存取動作均由 Amazon 參考記錄， CloudTrail 並記錄在 Amazon EC2 API 參考中。例如，呼叫DeleteVerifiedAccessInstance和ModifyVerifiedAccessInstance動作會CreateVerifiedAccessInstance在 CloudTrail 記錄檔中產生項目。

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

- 要求是以 root 使用者還是 AWS Identity and Access Management (IAM) 使用者認證提出。
- 提出該請求時，是否使用了特定角色或聯合身分使用者的暫時安全憑證。
- 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CloudTrail userIdentity 元素。

瞭解已驗證的存取記錄檔項目

追蹤是一種組態，可讓事件以日誌檔的形式傳遞到您指定的 Amazon S3 儲存貯體。 CloudTrail 記錄檔包含一或多個記錄項目。事件代表來自任何來源的單一請求。它包括請求的動作、動作的日期和時間、請求參數等相關資訊。 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CreateVerifiedAccessInstance動作的 CloudTrail 記錄項目。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAIKK4OOINJWEXAMPLE:jdoe",
        "arn": "arn:aws:iam::123456789012:user/jdoe",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "jdoe"
```

```
    },
    "eventTime": "2022-11-18T20:44:04Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "CreateVerifiedAccessInstance",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "198.51.100.1",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "CreateVerifiedAccessInstanceRequest": {
            "Description": "",
            "ClientToken": "85893b1e-49f6-4d24-97de-280c664edf1b"
        }
    },
    "responseElements": {
        "CreateVerifiedAccessInstanceResponse": {
            "verifiedAccessInstance": {
                "creationTime": "2022-11-18T20:44:04",
                "description": "",
                "verifiedAccessInstanceId": "vai-0d79d91875542c549",
                "verifiedAccessTrustProviderSet": ""
            },
            "requestId": "2eae195d-6bfd-46d7-b46e-a68cb791de09"
        }
    },
    "requestID": "2eae195d-6bfd-46d7-b46e-a68cb791de09",
    "eventID": "297d6529-1144-40f6-abf8-3a76f18d88f0",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

的配額 AWS Verified Access

您的每個配額都 AWS 帳戶 有預設配額 (先前稱為限制) AWS 服務。除非另有說明，否則每個配額都是區域特定規定。

AWS 帳戶層級配額

您 AWS 帳戶 有下列與已驗證存取權相關的配額。

名稱	預設	可調整	描述
驗證存取執行個	5	是	客戶可在目前區域中建立的已驗證存取執行個體數目上限。
已驗證存取群組	10	是	客戶可在目前「區域」中建立的「已驗證存取群組」數目上限。
驗證存取信任提供者	15	是	客戶可在目前區域中建立的「已驗證存取信任提供者」數目上限。
已驗證存取端點	50	是	客戶可在目前區域中建立的「已驗證存取端點」數目上限。

HTTP標頭

以下是HTTP標題的大小限制。

名稱	預設	可調整
請求行	16 K	否
單一標頭	16 K	否
整個回應標頭	32 K	否
整個請求標頭	64 K	否

OIDC索賠大小

以下是OIDC索賠大小限制。

名稱	預設	可調整
OIDC索賠大小	十一公里	否

「已驗證存取權使用者指南」的文件歷

下表說明「已驗證存取權」的文件版本。

變更	描述	日期
AWS 管理策略已更新	更新已驗證存取的 AWS 受管理IAM原則。	2023 年 11 月 17 日
靜態資料加密	AWS 驗證存取權預設會使用 AWS 擁有的KMS金鑰加密靜態資料。	2023 年 9 月 28 日
FIPS合規性 Support	針對FIPS符合性設定已驗證存取。	2023 年 9 月 26 日
增強型日誌	添加日誌記錄功能，可將信任內容添加到日誌中。	2023 年 6 月 19 日
AWS 管理策略已更新	更新已驗證存取的 AWS 受管理IAM原則。	2023 年 5 月 31 日
GA 版本	GA 發行的「已驗證存取使用者指南」。包括AWS WAF 整合。	2023 年 4 月 27 日
預覽版	「已驗證存取權使用者指南」的預覽版	2022 年 11 月 29 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。