aws

使用者指南

Amazon VPC Lattice

Amazon VPC Lattice: 使用者指南

Table of Contents

什麼是 Amazon VPC 格子？

Amazon VPC 萊迪思是一種全受管的應用程式聯網服務，可用來連接、保護和監控應用程式的服務。您可以將 VPC 萊迪斯與單一虛擬私有雲 (VPC) 搭配使用，也可以從一個或多個帳戶跨多個 VPC 使用。

現代應用程序可以由多個小型和模塊化服務組成，這些服務通常稱為微服務。雖然現代化有其優點，但是當您連接這些微服務時，它也會引入網路複雜性和挑戰。例如，如果開發人員分散在不同的團隊中，他們可能會在多個帳戶或 VPC 上建立和部署微服務。

在 VPC 萊迪思中，我們將微服務稱為服務。這是您在 VPC 萊迪思文檔中看到的措辭。

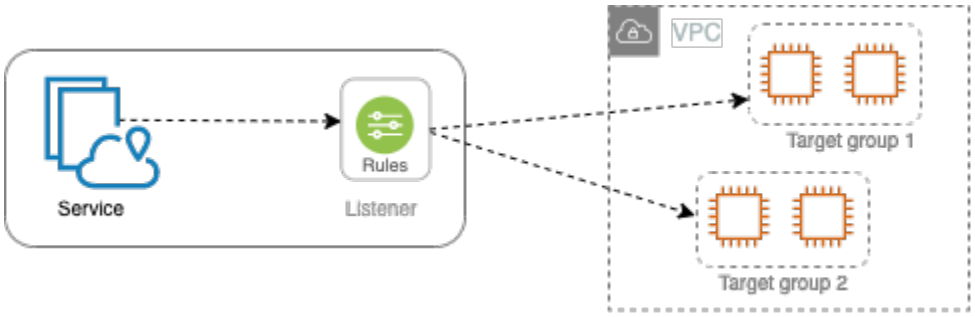
目錄

關鍵元件

若要使用 Amazon VPC 晶格，您應該熟悉其關鍵元件。

服務

可獨立部署的軟體單元，可提供特定工作或功能。服務可以在 EC2 執行個體或 ECS 容器上執行，也可以作為 Lambda 函數在帳戶或虛擬私有雲 (VPC) 中執行。VPC Ladess 服務具有下列元件：目標群組、接聽程式和規則。



目標群組

執行應用程式或服務的資源集合，也稱為目標。目標可以是 EC2 執行個體、IP 地址、Lambda 函數、應用程式負載平衡器或 Kubernetes 網繭。這些類似於 Elastic Load Balancing 提供的目標群組，但它們不可互換。

接聽程式

檢查連線要求，並將它們路由至目標群組中的目標的程序。一個服務最多可以有兩個接聽程式，使用 HTTP 和 HTTPS 通訊協定，以及介於 1 到 65535 之間的通訊埠號碼。

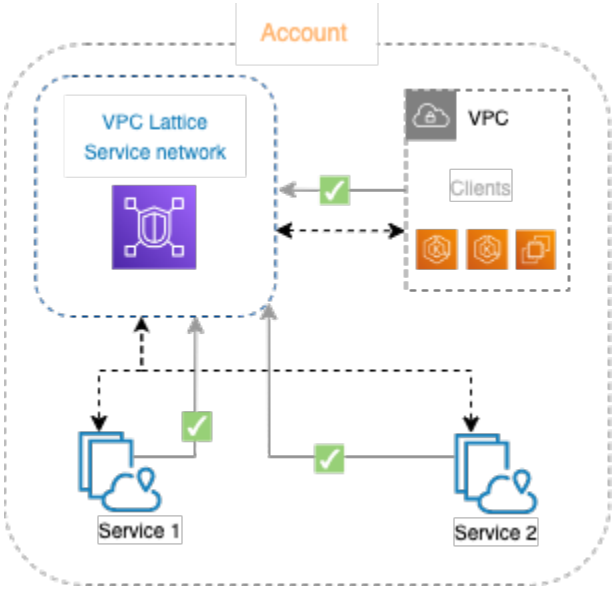
規則

監聽器的預設元件，可將要求轉送至 VPC Licts 目標群組中的目標。每個規則由優先順序、一或多個動作及一或多個條件組成。規則決定接聽程式路由用戶端要求的方式。

服務網絡

服務集合的邏輯界限。用戶端是任何部署在 VPC 中與服務網路相關聯的資源。與相同服務網路相關聯的用戶端和服務只要獲得授權，就可以彼此通訊。

在下圖中，用戶端可以與這兩個服務進行通訊，因為 VPC 和服務與相同的服務網路相關聯。



服務目錄

您擁有或透過 AWS Resource Access Manager (AWS RAM) 與您的帳戶共用的所有 VPC 萊迪思服務的中央登錄檔。

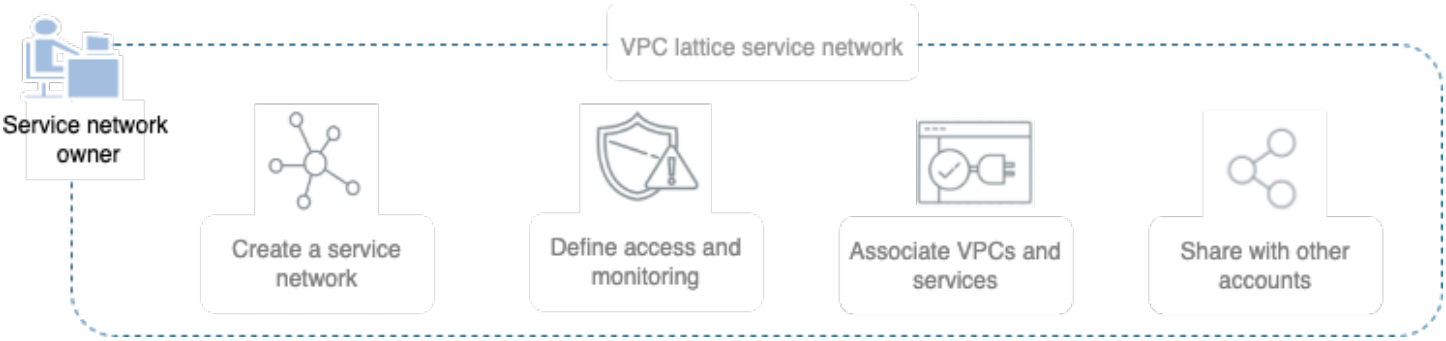
驗證政策

可用於定義服務存取權的精細授權原則。您可以將單獨的身份驗證策略附加到單個服務或服務網絡。例如，您可以建立政策，說明在 EC2 執行個體 auto 調整規模群組上執行的付款服務應如何與中執行的計費服務互動 AWS Lambda。

角色和責任

角色決定誰負責 Amazon VPC 萊格內的資訊設定和流程。通常有兩個角色，服務網路擁有者和服務擁有者，其職責可能會重疊。

服務網路擁有者 — 服務網路擁有者通常是組織中的網路管理員或雲端管理員。服務網路擁有者建立、共用及佈建服務網路。他們還管理誰可以在 VPC 萊迪思內訪問服務網絡或服務。服務網路擁有者可以為與服務網路相關聯的服務定義粗略的存取設定。這些控制項可用來管理使用驗證和授權原則的用戶端與服務之間的通訊。如果服務與服務網路擁有者的帳戶共用，服務網路擁有者也可以將服務與服務網路建立關聯。



服務擁有者 — 服務擁有者通常是組織中的軟體開發人員。服務擁有者可以在 VPC 萊迪思內建立服務、定義路由規則，並將服務與服務網路建立關聯。他們還可以定義精細的訪問設置，這可以限制只對經過身份驗證和授權的服務和客戶端的訪問。

功能

以下是 VPC 萊迪思提供的核心功能。

服務探索

與服務網路相關聯的 VPC 中的所有用戶端和服務都可以與相同服務網路中的其他服務進行通訊。DNS 會透過 VPC 萊迪格端點來引導 client-to-service 和 service-to-service 流量。當客戶端想要向服務發送請求時，它會使用該服務的 DNS 名稱。Route 53 解析器將流量發送到 VPC 萊迪斯，然後識別目的地服務。

連線能力

C lient-to-service 連線是使用 AWS 網路基礎架構內的 VPC 萊迪思資料層建立的。將虛擬私人雲端與服務網路建立關聯時，如果 VPC 中的任何用戶端具有必要的存取權，都可以與服務網路中的服務連線。

可觀測性

VPC 萊迪思會為穿越服務網路的每個要求和回應產生指標和記錄，以協助您監控應用程式並進行疑難排解。根據預設，VPC 萊迪思會在服務擁有者帳戶中發佈指標，並提供開啟記錄功能的選項。如果用戶端也與相同的服務網路相關聯，則服務網路擁有者會收到與服務網路相關聯之所有服務的記錄檔。服務擁有者會收到對其服務發出要求的所有用戶端的記錄檔。

VPC 萊迪思搭配下列工具協助您監控和疑難排解服務： CloudWatch 日誌群組、Firehose 交付串流和 S3 儲存貯體。

安全

VPC 萊迪思提供了一個框架，您可以使用該框架在網絡的多層實施防禦策略。第一層是服務和 VPC 關聯。如果沒有 VPC 和服務關聯，客戶端將無法訪問該服務。第二層可讓使用者將安全群組附加至 VPC 與服務網路之間的關聯。第三層和第四層是可以在服務網路層級和服務層級單獨套用的驗證原則。

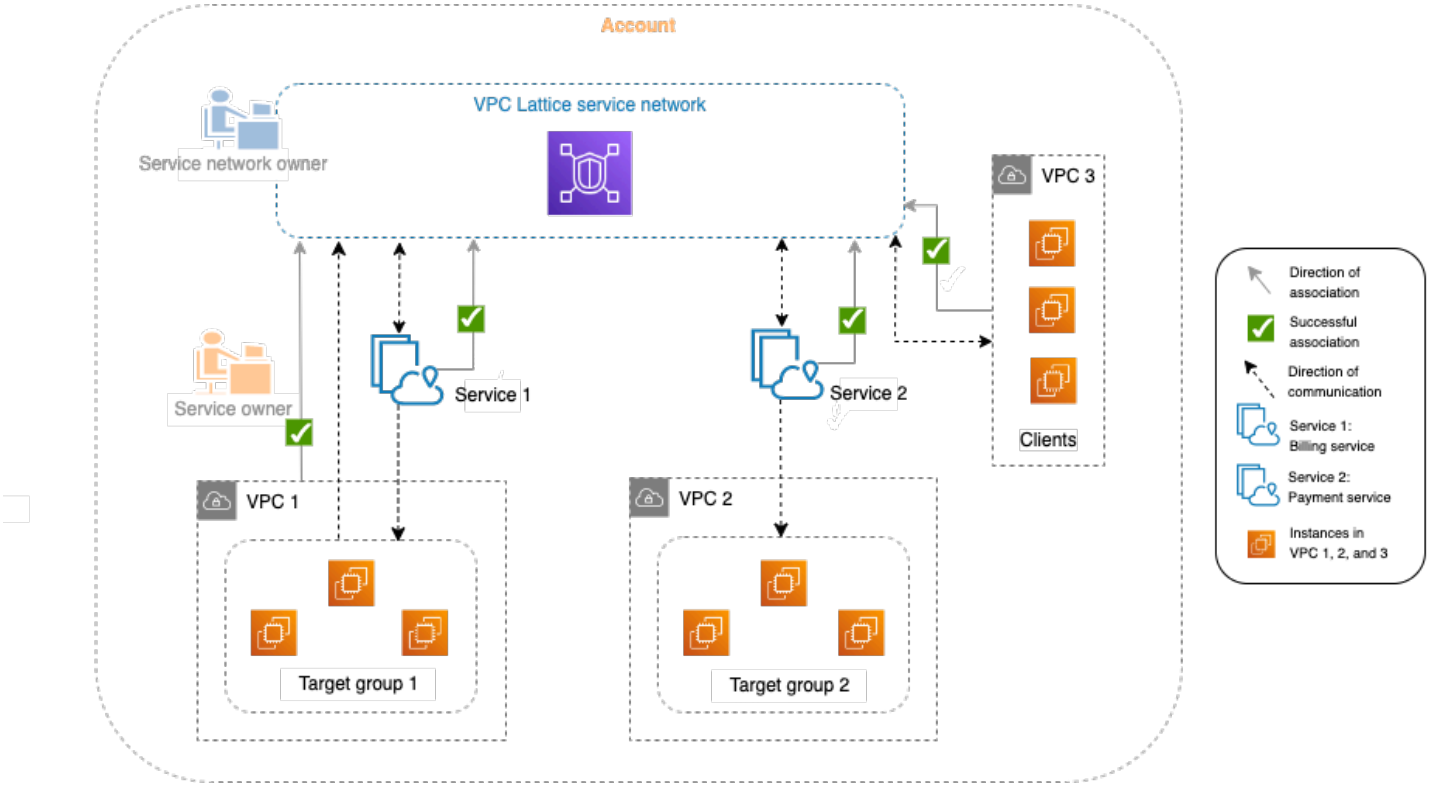
VPC 格子的工作原理

VPC 萊迪思旨在幫助您輕鬆有效地發現，保護，連接和監控其中的所有服務。VPC 萊迪思內的每個元件都會根據服務網路與服務網路的關聯及其存取設定，在服務網路內進行單向或雙向通訊。存取設定包含此通訊所需的驗證和授權原則。

以下摘要描述了 VPC 晶格內部組件之間的通信：

- 與服務網路相關聯的服務可以接收來自 VPC 也與服務網路相關聯的用戶端的要求。
- 只有當用戶端位於與相同服務網路相關聯的 VPC 中時，才能將要求傳送至與服務網路相關聯的服務。周遊 VPC 對等互連或傳輸閘道的用戶端流量將遭拒。
- 用戶端無法將要求傳送至與服務網路相關聯的其他 VPC 中的用戶端。
- VPC 中與服務網路相關聯的服務目標也是用戶端，可以將要求傳送至與服務網路相關聯的其他服務。
- VPC 中與服務網路無關聯的服務目標不是用戶端，也無法將要求傳送至與服務網路相關聯的其他服務。

下列流程圖使用範例案例來說明 VPC 萊迪思內元件之間的資訊流程和通訊方向。有兩個服務與服務網路相關聯。服務和所有三個 VPC 都是在與服務網路相同的帳戶中建立的。這兩個服務都設定為允許來自服務網路的流量。



服務 1 是在 VPC 1 中目標群組 1 註冊的執行個體群組上執行的帳單應用程式。服務 2 是在 VPC 2 中目標群組 2 註冊的一組執行個體上執行的付款應用程式。VPC 3 位於同一帳戶中，並且具有用戶端，但沒有服務。

下列清單依序說明 VPC 萊迪思的典型工作流程。

1. 建立服務網路

服務網路擁有者會建立服務網路。

2. 建立服務

   服務所有者創建各自的服務，服務 1 和服務 2。在建立期間，服務擁有者會新增接聽程式，並定義將要求路由傳送至每個服務的目標群組的規則。

3. 定義製程

   服務擁有者會為每個服務 (目標群組 1 和目標群組 2) 建立目標群組。他們透過指定執行服務的目標資源 (例如執行個體) 來執行此操作。它們也會指定這些目標所在的 VPC。

   在上圖中，從服務指向目標群組的虛線箭頭代表從每個服務流向其各自目標群組的流量。虛線箭頭代表服務與目標群組之間的通訊方向。

4. 將服務與服務網路產生關聯

   服務網絡擁有者或服務擁有者將服務與服務網絡聯繫在一起。關聯會顯示為箭頭，並帶有勾選標記指向服務網路的服務網路。當您將服務與服務網路產生關聯時，該服務會被 VPC 中與服務網路相關聯的其他服務和用戶端進行探索。

   服務與服務網路之間的雙向虛線箭頭代表關聯所產生的雙向通訊。從服務網路到服務的虛線箭頭代表接收來自用戶端要求的服務。相反方向的虛線箭頭 (即從服務到服務網路) 代表透過服務網路回應用戶端要求的服務。

5. 將 VPC 與服務網路建立關聯

   服務網路擁有者將 VPC 1 和 VPC 3 與服務網路相關聯。這些關聯會顯示箭頭，並帶有指向服務網路的核取標記。透過這些關聯，這些 VPC 中的目標會成為用戶端，並且可以向關聯的服務發出要求。VPC 3 和服務網路之間的雙向虛線箭頭代表 VPC 3 中用戶端 (例如執行個體) 與關聯結果的服務網路之間的雙向通訊。同樣地，從目標群組 1 指向服務網路的虛線箭頭代表從屬端向與服務網路相關聯的其他服務發出要求。

   請注意，VPC 2 沒有表示關聯的箭頭或勾選標記。這表示服務網路擁有者或服務擁有者尚未將 VPC 2 與服務網路相關聯。這是因為在此範例中，Service 2 只需要使用相同的要求接收要求並傳送回應。換句話說，服務 2 的目標不是用戶端，也不需要向服務網路中的其他服務發出要求。

存取 VPC 格

您可以使用下列任何介面建立、存取和管理 VPC 萊迪思：

- AWS Management Console— 提供可用於訪問 VPC 格子的 Web 界面。
- AWS Command Line Interface (AWS CLI) — 提供各種 AWS 服務的命令，包括 VPC 格子。在視窗、MacOS 和 Linux 上支援 AWS CLI 此功能。如需 CLI 的詳細資訊，請參閱AWS Command Line Interface。如需 API 的詳細資訊，請參閱 Amazon VPC 萊迪格 API 參考資料。
- 適用於 Kubernetes 的 VPC 點陣控制器 — 管理 Kubernetes 叢集的 VPC 晶格資源。如需將 VPC 點陣與 Kubernetes 搭配使用的詳細資訊，請參閱AWS 閘道 API 控制器使用者指南。
- AWS CloudFormation— 幫助您建模和設置資 AWS 源。如需詳細資訊，請參閱 Amazon VPC 萊迪思資源類型參考資料。

定價

使用 VPC 萊迪思，您需要支付佈建服務的時間、透過每個服務傳輸的資料量以及請求數量。如需詳細資訊，請參閱 Amazon VPC 點陣定價。

設置亞馬遜 VPC 格子

完成本節中的任務以首次設置和啟動 VPC 格子：

任務

- 註冊 AWS
- 建立 IAM 使用者

註冊 AWS

當您註冊 Amazon Web Services 時，系統會自動註冊您AWS 帳戶使用中的所有服務AWS，包括 VPC 萊迪斯。您只需針對所使用的服務付費。

如果您已擁有 AWS 帳戶，請跳至下一項任務。如果您還沒有 AWS 帳戶，請使用下列程序建立新帳戶。

如果您還沒有 AWS 帳戶，請完成下列步驟建立新帳戶。

註冊 AWS 帳戶

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

   部分註冊程序需接收來電，並在電話鍵盤輸入驗證碼。

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

建立 IAM 使用者

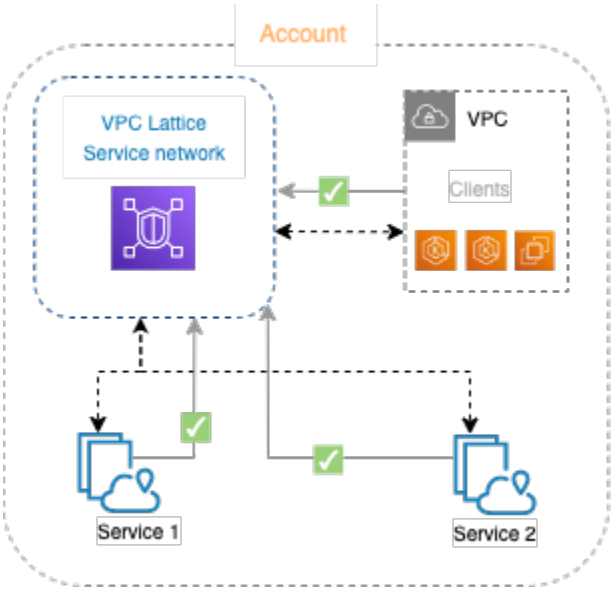
若要建立管理員使用者，請選擇下列其中一個選項。

選擇一種管理管理員的方式	若要	By	您也可以
在 IAM Identity Center (建議)	使用短期憑證存取 AWS。 這與安全性最佳實務一致。有關最佳實務的資訊，請參閱 IAM 使用者指南中的 IAM 安全最佳實務。	請遵循 AWS IAM Identity Center 使用者指南的入門中的說明。	請參閱 AWS Command Line Interface 使用者指南中的設定 AWS CLI 以使用 AWS IAM Identity Center 設定程式設計存取。
在 IAM 中 (不建議使用)	使用長期憑證存取 AWS。	請遵循 IAM 使用者指南中建立您的第一個 IAM 管理員使用者和使用者群組的說明。	請參閱 IAM 使用者指南中的管理 IAM 使用者的存取金鑰，設定程式設計存取。

VPC 格子中的服務網絡

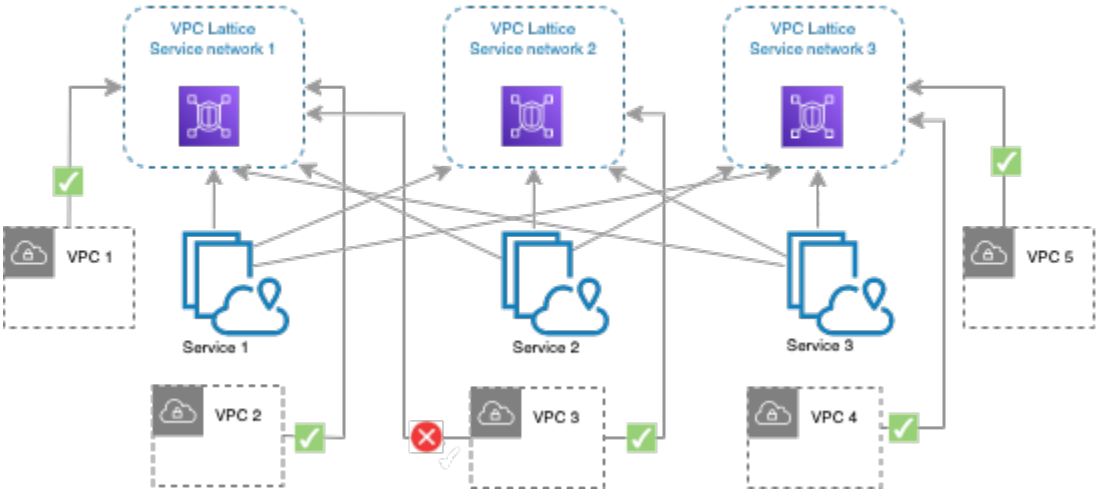
服務網路是服務集合的邏輯界限。與網路相關聯的服務可獲得探索、連線能力、可存取性和觀察性的授權。若要對網路中的服務發出要求，您的服務或用戶端必須位於與服務網路相關聯的 VPC 中。

下圖顯示 Amazon VPC 萊迪思內典型服務網路的關鍵元件。箭頭上的核取標記表示服務和 VPC 與服務網路相關聯。VPC 中與服務網路相關聯的用戶端可以透過服務網路與這兩個服務進行通訊。



您可以將一或多個服務與多個服務網路產生關聯。您也可以將多個 VPC 與一個服務網路建立關聯。但是，每個 VPC 只能與一個服務網路相關聯。

在下圖中，箭頭代表服務與服務網路之間的關聯，以及 VPC 與服務網路之間的關聯。您可以看到多個服務與多個服務網路相關聯，而且多個 VPC 與每個服務網路相關聯。但是，圖表中的紅色 x 標記顯示每個 VPC 與服務網路的關聯不能超過一個。



如需詳細資訊，請參閱 Amazon VPC 格子的配額。

建立服務網路

使用主控台建立服務網路，並選擇性地使用服務、關聯、存取設定和存取記錄來進行設定。

使用主控台建立服務網路

1. 前往 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在功能窗格的 VPC Latters 下，選擇 [服務網路]。
3. 選擇 [建立服務網路]。
4. 在識別碼中，輸入名稱、選用說明和選用標籤。名稱必須介於 3 到 63 個字元之間。您可以使用小寫字母、數字和連字號。名稱必須以字母或數字開頭和結尾。請勿使用連續連字號。說明最多可包含 256 個字元。若要新增標籤，請選擇「新增標籤」，然後指定標籤關鍵字和標籤值。
5. (選擇性) 若要關聯服務，請從「服務關聯」、「服務」中選擇服務。該列表包括您帳戶中的服務，以及從不同帳戶與您共享的任何服務。如果清單中沒有任何服務，您可以選擇 [建立 VPC 萊迪思服務] 來建立服務。

   或者，若要在建立服務網路之後關聯服務，請參閱the section called “管理服務關聯”。
6. (選擇性) 若要關聯 VPC，請選擇「新增 VPC 關聯」。選取要與 VPC 建立關聯的 VPC，然後從安全群組中選取最多五個安全群組。若要建立安全性群組，請選擇 [建立新的安全性群組]。

   或者，若要在建立服務網路之後關聯 VPC，請參閱the section called “管理 VPC 關聯”。

7. 對於網路存取，如果您希望關聯 VPC 中的用戶端存取此服務網路中的服務，則可以保留預設驗證類型「無」。要應用身份驗證策略來控制對服務的訪問，請選擇 AWS IAM 並對身份驗證策略執行以下操作之一：
   - 在輸入欄位中輸入策略。例如，您可以複製和貼上的策略，請選擇策略範例。
   - 選擇套用原則範本，然後選取允許已驗證和未驗證的存取範本。此範本允許來自其他帳戶的用戶端透過簽署要求 (意為已驗證) 或匿名方式 (表示未經驗證) 來存取服務。
   - 選擇套用原則範本，然後選取僅允許已驗證的存取範本。該模板允許來自另一個帳戶的客戶端僅通過簽署請求（意味著已驗證）訪問服務。
8. (選擇性) 若要開啟存取記錄，請選取 [存取記錄] 切換開關，然後指定存取記錄的目的地，如下所示：
   - 選取CloudWatch 記錄群組，然後選擇 CloudWatch 記錄群組。若要建立記錄群組，請在中選擇 [建立記錄群組] CloudWatch。
   - 選取 S3 儲存貯體並輸入 S3 儲存貯體路徑，包括任何前置詞。若要搜尋 S3 儲存貯體，請選擇瀏覽 S3。
   - 選取 Kinesis Data Firehose 傳送串流，然後選擇交付串流。若要建立交付串流，請選擇在 Kinesis 中建立交付串流。
9. (選擇性) 若要與其他帳號共用您的服務網路，請從 AWS RAM 資源共用中選擇資源共用率。若要建立資源共用，請選擇 [在 RAM 主控台中建立資源共用]。
10. 在 [摘要] 區段中檢閱您的組態，然後選擇 [建立服務網路]。

使用建立服務網路 AWS CLI

使用 create-service-network 命令。這個命令只會建立基本的服務網路。若要建立功能完整的服務網路，您還必須使用建立服務關聯、VPC 關聯和存取設定的命令。

管理服務網路的關聯

當您將服務與服務網路產生關聯時，它會讓用戶端 (與服務網路相關聯的 VPC 中的資源) 向服務發出要求。當您將虛擬私人雲端與服務網路建立關聯時，該 VPC 內的所有目標都能成為用戶端，並與服務網路中的其他服務進行通訊。

目錄

管理服務關聯

您可以將位於您帳戶中的服務或從不同帳戶與您共用的服務建立關聯。這是建立服務網路時的選擇性步驟。但是，在您關聯服務之前，服務網路無法完全正常運作。如果服務擁有者的帳戶具有必要的存取權，則可將其服務與服務網路建立關聯。如需詳細資訊，請參閱 VPC 格子的工作原理。

當您刪除服務關聯時，服務將無法再連線至服務網路中的其他服務。

使用主控台管理服務關聯

1. 前往 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在功能窗格的 VPC Latters 下，選擇 [服務網路]。
3. 選取服務網路的名稱，以開啟其詳細資訊頁面。
4. 選擇「服務關聯」頁標。
5. 若要建立關聯，請執行下列動作：
   a. 選擇「建立關聯」。
   b. 從「服務」中選取服務。若要建立服務，請選擇建立 Amazon VPC 萊迪思服務。
   c. (選擇性) 若要新增標籤，請展開「服務關聯標記」，選擇「新增標籤」，然後輸入標籤鍵和標籤值。
   d. 選擇儲存變更。
6. 若要刪除關聯，請選取關聯的核取方塊，然後選擇動作，刪除服務關聯。出現確認提示時，請輸入 **`confirm`**，然後選擇 Delete (刪除)。

若要使用 AWS CLI

使用 create-service-network-service-關聯命令。

若要使用刪除服務關聯 AWS CLI

使用 delete-service-network-service-關聯命令。

管理 VPC 關聯

只有當用戶端位於與服務網路相關聯的 VPC 中時，才能將要求傳送至與服務網路相關聯的服務。周遊 VPC 對等互連或傳輸閘道的用戶端流量將遭拒。

建立服務網路時，關聯 VPC 是可選步驟。但是，在您關聯 VPC 之前，服務網路無法完全運作。如果網路擁有者的帳戶具有必要的存取權，則可以將 VPC 關聯至服務網路。如需詳細資訊，請參閱 VPC 格子的工作原理。

刪除 VPC 關聯時，VPC 中的用戶端將無法再連線到服務網路中的服務。

使用主控台管理 VPC 關聯

1. 前往 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在功能窗格的 VPC Latters 下，選擇 [服務網路]。
3. 選取服務網路的名稱，以開啟其詳細資訊頁面。
4. 選擇 VPC 關聯索引標籤。
5. 若要建立 VPC 關聯，請執行下列動作：
   a. 選擇 [建立 VPC 關聯]。
   b. 選擇新增 VPC 關聯。
   c. 從 VPC 選取 VPC，然後從安全群組中選取最多五個安全群組。若要建立安全性群組，請選擇 [建立新的安全性群組]。
   d. (選擇性) 若要新增標籤，請展開 VPC 關聯標籤，選擇「新增標籤」，然後輸入標籤鍵和標籤值。
   e. 選擇儲存變更。
6. 若要編輯關聯的安全性群組，請選取關聯的核取方塊，然後選擇動作，編輯安全性群組。視需要新增和移除安全性群組。
7. 若要刪除關聯，請選取關聯的核取方塊，然後選擇 [動作] > [刪除 VPC 關聯]。出現確認提示時，請輸入 **`confirm`**，然後選擇 Delete (刪除)。

使用建立 VPC 關聯 AWS CLI

使用 create-service-network-vpc-關聯命令。

若要使用更新 VPC 關聯的安全群組 AWS CLI

使用 update-service-network-vpc-關聯命令。

若要刪除虛 VPC 端關聯 AWS CLI

使用 delete-service-network-vpc-關聯命令。

編輯服務網路的存取設定

存取設定可讓您設定和管理用戶端對服務網路的存取。存取設定包括驗證類型和驗證原則。驗證原則可協助您驗證和授權流向 VPC Lacither 內服務的流量。

您可以在服務網路層級、服務層級或兩者上套用驗證原則。通常，身份驗證策略由網絡所有者或雲管理員應用。他們可以實現課程粒度授權，例如，允許從組織內部進行身份驗證的調用，或允許符合特定條件的匿名 GET 請求。在服務層級，服務擁有者可以套用精細的控制項，這可能會更嚴格。如需詳細資訊，請參閱 使用身份驗證策略控制服務的訪問。

使用主控台新增或更新存取原則

1. 前往 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在功能窗格的 VPC Latters 下，選擇 [服務網路]。
3. 選取服務網路的名稱，以開啟其詳細資訊頁面。
4. 選擇 [存取] 索引標籤以檢查目前的存取設定。
5. 若要更新存取設定，請選擇 [編輯存取設定]。
6. 如果您希望關聯 VPC 中的用戶端存取此服務網路中的服務，請針對驗證類型選擇無。
7. 要將資源策略應用於服務網絡，請為身份驗證類型選擇 AWS IAM，然後對身份驗證策略執行以下操作之一：
   - 在輸入欄位中輸入策略。例如，您可以複製和貼上的策略，請選擇策略範例。
   - 選擇套用原則範本，然後選取允許已驗證和未驗證的存取範本。此範本允許來自其他帳戶的用戶端透過簽署要求 (意為已驗證) 或匿名方式 (表示未經驗證) 來存取服務。
   - 選擇套用原則範本，然後選取僅允許已驗證的存取範本。該模板允許來自另一個帳戶的客戶端僅通過簽署請求（意味著已驗證）訪問服務。
8. 選擇儲存變更。

使用新增或更新存取原則 AWS CLI

使用 put-auth-policy 命令。

編輯服務網路的監督詳細資料

VPC 萊迪思會為每個請求和回應產生指標和日誌，使監控和疑難排解應用程式更有效率。

您可以啟用存取記錄，並指定記錄檔的目標資源。VPC 萊迪思可以將日誌傳送到下列資源：日 CloudWatch 誌群組、Firehose 交付串流和 S3 儲存貯體。

使用主控台啟用存取記錄檔或更新記錄目的地

1. 前往 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在功能窗格的 VPC Latters 下，選擇 [服務網路]。
3. 選取服務網路的名稱，以開啟其詳細資訊頁面。
4. 選擇 Monitoring (監控) 索引標籤。檢查存取記錄以查看是否已啟用存取記錄。
5. 若要啟用或停用存取記錄，請選擇 [編輯存取記錄]，然後開啟或關閉 [存取記錄] 切換開關。
6. 啟用存取記錄檔時，您必須選取傳送目的地類型，然後建立或選擇存取記錄的目的地。您也可以隨時變更送貨目的地。例如：
   - 選取CloudWatch 記錄群組，然後選擇 CloudWatch 記錄群組。若要建立記錄群組，請在中選擇 [建立記錄群組] CloudWatch。
   - 選取 S3 儲存貯體並輸入 S3 儲存貯體路徑，包括任何前置詞。若要搜尋 S3 儲存貯體，請選擇瀏覽 S3。
   - 選取 Kinesis Data Firehose 傳送串流，然後選擇交付串流。若要建立交付串流，請選擇在 Kinesis 中建立交付串流。
7. 選擇儲存變更。

若要啟用存取記錄 AWS CLI

使用 create-access-log-subscription 命令。

若要使用更新記錄目的地 AWS CLI

使用 update-access-log-subscription 命令。

若要停用存取記錄 AWS CLI

使用 delete-access-log-subscription 命令。

管理服務網路的標籤

標籤可協助您以不同的方式分類服務網路，例如，依目的、擁有者或環境。

您可以為每個服務網路新增多個標籤。每個服務網路的標籤金鑰必須是唯一的。如果您新增含有已與服務網路相關聯的金鑰的標籤，則會更新該標籤的值。您可以使用字母、空格、數字 (在 UTF-8 中) 和下列特殊字元之類的字元：+-=。_ : / @。不可使用結尾或前方空格。標籤值區分大小寫。

使用主控台新增或刪除標籤

1. 前往 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在功能窗格的 VPC Latters 下，選擇 [服務網路]。
3. 選取服務網路的名稱，以開啟其詳細資訊頁面。
4. 選擇 Tags (標籤) 索引標籤。
5. 若要新增標籤，請選擇「新增標籤」，然後輸入標籤關鍵字和標籤值。若要新增另一個標籤，請再次選擇「新增標籤」。當您完成新增標籤的作業時，請選擇 Save changes (儲存變更)。
6. 若要刪除標記，請選取標記的核取方塊，然後選擇「刪除」。出現確認提示時，請輸入 **`confirm`**，然後選擇 Delete (刪除)。

若要使用新增或刪除標籤 AWS CLI

使用標籤資源和無標記資源命令。

刪除服務網路

刪除服務網路之前，必須先刪除服務網路與任何服務或 VPC 可能具有的所有關聯。當您刪除服務網路時，我們也會刪除與服務網路相關的所有資源，例如資源原則、驗證原則和存取記錄訂閱。

使用主控台刪除服務網路

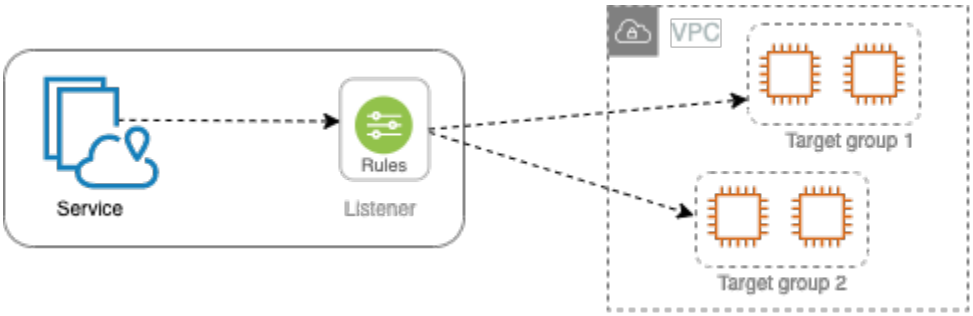
1. 前往 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在功能窗格的 VPC Latters 下，選擇 [服務網路]。
3. 選取服務網路的核取方塊，然後選擇 [動作] > [刪除服務網路]。
4. 出現確認提示時，請輸入 **`confirm`**，然後選擇 Delete (刪除)。

若要刪除服務網路 AWS CLI

使用 delete-service-network 命令。

VPC 格子的服務

VPC Lady 中的服務是可獨立部署的軟體單元，可提供特定工作或功能。服務可以在執行個體、容器上執行，或作為帳戶或虛擬私有雲 (VPC) 內的無伺服器功能執行。服務具有使用規則的監聽器 (稱為監聽器規則)，您可以設定這些規則來協助將流量路由到目標。目標可以是 EC2 執行個體、IP 地址、無伺服器 Lambda 函數、應用程式負載平衡器或 Ku bernetes 網繭。如需詳細資訊，請參閱 VPC 格子中的目標群體。您可以將服務與多個服務網路產生關聯。下圖顯示了 VPC 萊迪思內典型服務的關鍵組成部分。



您可以通過為其提供名稱和描述來創建服務。但是，若要控制和監視服務的流量，請務必加入存取設定和監視詳細資料。若要將流量從您的服務傳送到目標，您必須設定監聽器並設定規則。若要允許流量從服務網路流向您的服務，您必須將服務與服務網路建立關聯。

連線至目標時有閒置逾時和整體連線逾時。閒置連接超時為 1 分鐘，之後我們關閉連接。最長持續時間為 10 分鐘，之後我們不允許通過連接進行新的流，並開始關閉現有流的過程。

任務

- 步驟 1：建立 VPC 格子服務
- 步驟 2：定義製程
- 步驟 3：建立網路關聯
- 步驟 4：檢閱和建立
- 管理 VPC 萊迪思服務的關聯
- 編輯 VPC 萊迪思服務的存取設定
- 編輯 VPC 萊迪思服務的監視詳細資料
- 管理 VPC 萊迪思服務的標籤
- 為 VPC 萊迪思服務設定自訂網域名稱
- 為 VPC 格子攜帶您自己的憑證 (BYOC)
- 刪除服務

步驟 1：建立 VPC 格子服務

建立具有存取設定和監控詳細資料的基本 VPC 萊迪思服務。但是，在您定義其路由組態並將其與服務網路產生關聯之前，該服務才能正常運作。

使用主控台建立基本服務

1. 前往 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在功能窗格的 VPC 格子下，選擇 [服務]。
3. 選擇 Create service (建立服務)。
4. 對於識別碼，請執行下列動作：

   a. 輸入服務的名稱。名稱必須介於 3-63 個字元之間，並使用小寫字母、數字和連字號。它必須以字母或數字開頭和結尾。請勿使用雙連字號。

   b. (選擇性) 輸入服務網路的說明。您可以在建立期間或之後設定或變更說明。說明最多可包含 256 個字元。

5. (選擇性) 若要為您的服務指定自訂網域名稱，請選取指定自訂網域組態，然後輸入自訂網域名稱。您現在可以選擇性地選取相符的憑證。否則，您可以在為服務建立 HTTPS 接聽程式時選取相符的憑證。
6. 對於「服務存取」，如果您希望與服務網路相關聯的 VPC 中的用戶端存取您的服務，請選擇「無」。若要套用驗證政策來控制對服務的存取，請選擇 AWS IAM。若要將資源策略套用至服務，請對 Auth 策略執行下列其中一項操作：
   - 在輸入欄位中輸入策略。例如，您可以複製和貼上的策略，請選擇策略範例。
   - 選擇套用原則範本，然後選取允許已驗證和未驗證的存取範本。此範本允許來自其他帳戶的用戶端透過簽署要求 (意為已驗證) 或匿名方式 (即未經驗證) 來存取服務。
   - 選擇套用原則範本，然後選取僅允許已驗證的存取範本。該模板允許來自另一個帳戶的客戶端僅通過簽署請求（意味著已驗證）訪問服務。
7. (選擇性) 若要啟用存取記錄，請開啟 [存取記錄] 切換開關，並指定存取記錄的目的地，如下所示：
   - 選取CloudWatch 記錄群組，然後選擇一個 CloudWatch 記錄群組。若要建立記錄群組，請在中選擇 [建立記錄群組] CloudWatch。
   - 選取 S3 儲存貯體並輸入 S3 儲存貯體路徑，包括任何前置詞。若要搜尋 S3 儲存貯體，請選擇瀏覽 S3。
   - 選取 Kinesis Data Firehose 傳送串流，然後選擇交付串流。若要建立交付串流，請選擇在 Kinesis 中建立交付串流。

8. (選擇性) 若要與其他帳號共用您的服務，請從 AWS RAM 資源共用中選擇資源共用。若要建立資源共用，請選擇 [在 RAM 主控台中建立資源共用]。
9. 若要檢閱您的組態並建立服務，請選擇 [略過] 以檢閱和建立。否則，請選擇「下一步」以定義服務的路由配置。

步驟 2：定義製程

使用監聽器定義路由組態，讓您的服務可以將流量傳送到您指定的目標。

先決條件

在您可以新增監聽器之前，您必須先建立 VPC 萊迪目標群組。如需詳細資訊，請參閱 the section called “建立目標群組”。

使用主控台定義服務的路由

1. 選擇 Add listener (新增接聽程式)。
2. 對於監聽器名稱，您可以提供自訂監聽器名稱，或使用監聽器的協定和連接埠作為監聽器名稱。您指定的自訂名稱最多可包含 63 個字元，而且帳戶中的每個服務都必須是唯一的。有效字元包括 a-z、0-9 和連字號 (-)。您不能使用連字號作為第一個或最後一個字元，或緊接在其他連字號之後。建立監聽器之後，就無法變更它的名稱。
3. 在「通訊協定：連接埠」中，選擇「HTTP」或「HTTPS」，然後輸入通訊埠號碼。
4. 對於「預設」動作，請選擇要接收流量的 VPC 萊迪目標群組，然後選擇要指派給此目標群組的權重。您指派給目標群組的加權會設定其接收流量的優先順序。例如，如果兩個目標群組的權重相同，則每個目標群組會接收一半的流量。如果您只指定了一個目標群組，則 100% 的流量會傳送到一個目標群組。

   您可以選擇性地為預設動作新增其他目標群組。選擇 [新增動作]，然後選擇另一個目標群組並指定其權重。
5. (選擇性) 若要新增其他規則，請選擇「新增規則」，然後輸入規則的名稱、優先順序、條件和動作。

   您可以為每個規則指定介於 1 到 100 之間的優先順序號碼。接聽程式不能擁有多個優先順序相同的規則。依優先順序評估規則，從最低值到最高值。預設規則最後評估。

   在「條件」中，輸入路徑符合條件的路徑樣式。每個字串的大小上限為 200 個字元。比較不區分大小寫。
6. (選擇性) 若要新增標記，請展開 [監聽程式] 標籤，選擇 [新增標記]，然後輸入標記鍵和標記值。

7. 若要檢閱您的組態並建立服務，請選擇 [略過] 以檢閱和建立。否則，請選擇「下一步」，將您的服務與服務網路產生關聯。

步驟 3：建立網路關聯

將您的服務與服務網路建立關聯，以便用戶端可以與其通訊。

使用主控台將服務與服務網路產生關聯

1. 對於 VPC 萊迪思服務網路，請選擇服務網路。若要建立服務網路，請選擇 [建立 VPC 萊迪思網路]。您可以將您的服務與多個服務網路建立關聯。
2. (選擇性) 若要新增標籤，請展開「服務網路關聯標記」，選擇「新增標籤」，然後輸入標籤機碼和標籤值。
3. 選擇下一步。

步驟 4：檢閱和建立

使用主控台檢閱組態並建立服務

1. 檢閱服務的組態。
2. 如果您需要修改服務組態的任何部分，請選擇「編輯」。
3. 當您完成檢閱或編輯您的組態時，請選擇 [建立 VPC Lady 服務]。
4. 如果您為服務指定了自訂網域名稱，則必須在建立服務之後設定 DNS 路由。如需詳細資訊，請參閱 the section called “設定自訂網域名稱”。

管理 VPC 萊迪思服務的關聯

當您將服務與服務網路產生關聯時，它會讓用戶端 (與服務網路相關聯的 VPC 中的資源) 向此服務發出要求。您可以將帳戶中的服務或從不同帳戶與您共用的服務建立關聯。建立服務時，此步驟為選擇性步驟。不過，在建立之後，除非您將服務與服務網路產生關聯，否則該服務無法與其他服務進行通訊。如果服務擁有者的帳戶具有必要的存取權，則可以將其服務與服務網路建立關聯。如需詳細資訊，請參閱 VPC 格子的工作原理。

使用主控台管理服務網路關聯

1. 前往 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。

2. 在功能窗格的 VPC 格子下，選擇 [服務]。
3. 選取服務名稱以開啟其詳細資訊頁面。
4. 選擇「服務網路關聯」頁標。
5. 若要建立關聯，請執行下列動作：

   a. 選擇「建立關聯」。
   b. 從 VPC 萊迪思服務網絡中選擇一個服務網絡。若要建立服務網路，請選擇 [建立 VPC 萊迪思網路]。
   c. (選擇性) 若要新增標籤，請展開「服務關聯標記」，選擇「新增標籤」，然後輸入標籤鍵和標籤值。
   d. 選擇儲存變更。
6. 若要刪除關聯，請選取關聯的核取方塊，然後選擇動作，刪除網路關聯。出現確認提示時，請輸入 **`confirm`**，然後選擇 Delete (刪除)。

使用建立服務網路關聯 AWS CLI

使用 create-service-network-service-關聯命令。

若要刪除服務網路關聯 AWS CLI

使用 delete-service-network-service-關聯命令。

編輯 VPC 萊迪思服務的存取設定

存取設定可讓您設定和管理用戶端對服務的存取。存取設定包括驗證類型和驗證原則。驗證原則可協助您驗證和授權流向 VPC Racits 內服務的流量。

您可以在服務網路層級、服務層級或兩者上套用驗證原則。在服務層級，服務擁有者可以套用精細的控制項，這可能會更嚴格。通常，身份驗證策略由網絡所有者或雲管理員應用。他們可以實現課程粒度授權，例如，允許從組織內部進行身份驗證的調用，或允許符合特定條件的匿名 GET 請求。如需詳細資訊，請參閱 使用身份驗證策略控制服務的訪問。

使用主控台新增或更新存取原則

1. 前往 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在功能窗格的 VPC 格子下，選擇 [服務]。
3. 選取服務名稱以開啟其詳細資訊頁面。

4. 選擇 [存取] 索引標籤以檢查目前的存取設定。
5. 若要更新存取設定，請選擇 [編輯存取權設定]。
6. 如果您希望關聯服務網路中 VPC 中的用戶端存取您的服務，請針對驗證類型選擇無。
7. 要應用資源策略來控制對服務的訪問，請為身份驗證類型選擇 AWS IAM，然後對身份驗證策略執行以下操作之一：
   - 在輸入欄位中輸入策略。例如，您可以複製和貼上的策略，請選擇策略範例。
   - 選擇套用原則範本，然後選取允許已驗證和未驗證的存取範本。此範本允許來自其他帳戶的用戶端透過簽署要求 (意為已驗證) 或匿名方式 (即未經驗證) 來存取服務。
   - 選擇套用原則範本，然後選取僅允許已驗證的存取範本。該模板允許來自另一個帳戶的客戶端僅通過簽署請求（意味著已驗證）訪問服務。
8. 選擇儲存變更。

若要使用新增或更新存取原則 AWS CLI

使用 put-auth-policy 命令。

編輯 VPC 萊迪思服務的監視詳細資料

VPC 萊迪思會為每個請求和回應產生指標和日誌，使監控和疑難排解應用程式更有效率。

您可以啟用存取記錄，並指定記錄檔的目標資源。VPC 萊迪思可以將日誌傳送到下列資源：日 CloudWatch 誌群組、Firehose 交付串流和 S3 儲存貯體。

使用主控台啟用存取記錄檔或更新記錄目的地

1. 前往 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在功能窗格的 VPC 格子下，選擇 [服務]。
3. 選取服務名稱以開啟其詳細資訊頁面。
4. 選擇監控選項卡，然後選擇日誌。檢查存取記錄以查看是否已啟用存取記錄。
5. 若要啟用或停用存取記錄，請選擇 [編輯存取記錄]，然後開啟或關閉 [存取記錄] 切換開關。
6. 啟用存取記錄檔時，您必須選取傳送目的地類型，然後建立或選擇存取記錄的目的地。您也可以隨時變更送貨目的地。例如：
   - 選取CloudWatch 記錄群組，然後選擇一個 CloudWatch 記錄群組。若要建立記錄群組，請在中選擇 [建立記錄群組] CloudWatch。

- 選取 S3 儲存貯體並輸入 S3 儲存貯體路徑，包括任何前置詞。若要搜尋 S3 儲存貯體，請選擇瀏覽 S3。
- 選取 Kinesis Data Firehose 傳送串流，然後選擇交付串流。若要建立交付串流，請選擇在 Kinesis 中建立交付串流。

7. 選擇儲存變更。

若要啟用存取記錄 AWS CLI

使用 create-access-log-subscription 命令。

若要使用更新記錄目的地 AWS CLI

使用 update-access-log-subscription 命令。

若要停用存取記錄，請使用 AWS CLI

使用 delete-access-log-subscription 命令。

管理 VPC 萊迪思服務的標籤

標籤可協助您以不同的方式對服務進行分類，例如，依目的、擁有者或環境。

您可以為每個服務新增多個標籤。每個服務的標籤金鑰必須是唯一的。如果您新增含有已與服務相關聯的金鑰的標籤，則會更新該標籤的值。您可以使用字母、空格、數字 (在 UTF-8 中) 和下列特殊字元之類的字元：+-=。_ : / @。不可使用結尾或前方空格。標籤值區分大小寫。

使用主控台新增或刪除標籤

1. 前往 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在功能窗格的 VPC 格子下，選擇 [服務]。
3. 選取服務名稱以開啟其詳細資訊頁面。
4. 選擇 Tags (標籤) 索引標籤。
5. 若要新增標籤，請選擇「新增標籤」，然後輸入標籤關鍵字和標籤值。若要新增另一個標籤，請再次選擇「新增標籤」。當您完成新增標籤的作業時，請選擇 Save changes (儲存變更)。
6. 若要刪除標記，請選取標記的核取方塊，然後選擇「刪除」。出現確認提示時，請輸入 **`confirm`**，然後選擇 Delete (刪除)。

若要使用新增或刪除標籤 AWS CLI

使用標籤資源和無標記資源命令。

為 VPC 萊迪思服務設定自訂網域名稱

當您建立新服務時，VPC 萊迪思會為服務產生唯一的完整網域名稱 (FQDN)，例如 ""。*service-name-service_id.partition_id.vpc-lattice-svcs.region.on.aws*但是，這個 VPC 萊迪思生成的域名對於您的用戶來說並不容易記住。

自訂網域名稱是您可以提供給使用者更簡單、更直覺的 URL。如果您希望為您的服務使用自訂網域名稱 (例如，`www.parking.example.com`而不是 VPC Latds 產生的 DNS 名稱)，您可以在建立 VPC 萊迪斯服務時進行設定。當用戶端使用您的自訂網域名稱提出要求時，DNS 伺服器會將其解析為 VPC Lady 產生的網域名稱。但是，只有當您將自訂網域名稱對應至具有 CNAME 記錄的 VPC Latds 產生的網域名稱，以將查詢路由到您的服務時，才會發生這種情況。如需詳細資訊，請參閱 將您的自訂網域名稱與服務建立關聯。

先決條件

- 您必須擁有服務的註冊網域名稱。如果您還沒有註冊網域名稱，可以透過 Amazon Route 53 或任何其他商業註冊商註冊一個網域名稱。
- 若要接收 HTTPS 要求，您必須在中提供您自己的憑證 AWS Certificate Manager。VPC 萊迪思不支援預設憑證做為備用憑證。因此，如果您未提供與自訂網域名稱對應的 SSL/TLS 憑證，則與您自訂網域名稱的所有 HTTPS 連線都會失敗。如需詳細資訊，請參閱 為 VPC 格子攜帶您自己的憑證 (BYOC)。

限制和注意事項

- 您不能擁有一個以上的服務自訂網域名稱。
- 建立服務後，您就無法修改自訂網域名稱。
- 自訂網域名稱對於服務網路而言必須是唯一的。這表示無法使用已存在 (針對其他服務) 在相同服務網路中的自訂網域名稱建立服務。

若要使用 AWS Management Console

1. 前往 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在功能窗格的 VPC 格子下，選擇 [服務]。
3. 選擇「建立服務」。您會導覽至「步驟 1：建立服務」。

4. 在 [自訂網域組態] 區段中，選擇 [指定自訂網域組態]。
5. 輸入您的自訂網域名稱。
6. 若要提供 HTTPS 要求，請在自訂 SSL/TLS 憑證中選取符合您自訂網域名稱的 SS L/TLS 憑證。如果您還沒有憑證，或者現在不想新增憑證，您可以在建立 HTTPS 接聽程式時新增憑證。不過，如果沒有憑證，您的自訂網域名稱將無法提供 HTTPS 要求。如需詳細資訊，請參閱 新增 HTTPS 接聽程式。
7. 當您完成新增所有其他資訊以建立服務之後，請選擇 [建立]。

若要使用 AWS CLI

使用創建服務命令。

```
aws vpc-lattice create-service --name service_name --custom-domain-
name your_custom_domain_name --type https --certificate-arn arn:aws:acm:us-
east-1:123456789012:certificate/12345678-1234-1234-1234-123456789012
```

在上面的命令中--name，輸入服務的名稱。對於--custom-domain-name，輸入您服務的網域名稱，例如，parking.example.com。在 AC --certificate-arn M 中輸入憑證的 ARN。ARN 憑證可在您的帳戶中 AWS Certificate Manager使用。

如果您在 AWS Certificate Manager (ACM) 中沒有自己的 SSL/TLS 憑證，您可以在設定自訂網域名稱之前建立或匯入憑證。不過，只有當您想要使用自訂網域名稱提供 HTTPS 要求時，才需要憑證。如需詳細資訊，請參閱 為 VPC 格子攜帶您自己的憑證 (BYOC)。

將您的自訂網域名稱與服務建立關聯

首先，如果您尚未這樣做，請註冊您的自訂網域名稱。網際網路名稱和數字指派公司 (ICANN) 負責管理網際網路上的網域名稱。您可以使用網域名稱註冊商註冊網域名稱，這是一家 ICANN 認可的組織，專門管理網域名稱的註冊。您的網站註冊商網站將為註冊您的網域名稱提供詳細指示和定價資訊。如需詳細資訊，請參閱下列資源：

- 若要使用 Amazon Route 53 註冊網域名稱，請參閱 Amazon Route 53 開發人員指南中的使用 Route 53 註冊網域名稱。
- 如需這類註冊機構的清單，請參閱認可的註冊機構目錄。

接下來，使用您的 DNS 服務 (例如網域註冊機構) 建立 CNAME 記錄，將查詢路由傳送至您的服務。如需詳細資訊，請參閱您的 DNS 服務文件。或者，您可以使用 Route 53 做為您的 DNS 服務。

如果您使用的是 Route 53，則必須先建立託管區域，其中包含如何為網域路由網際網路流量的相關資訊。建立私有或公用託管區域之後，請建立 CNAME 記錄，例parking.example.com如，將您的自訂網域名稱對應至 VPC Ligess 自動產生的網域名稱，例如。my-service-02031c045478f6ddf1.7d67968.vpc-lattice-svcs.us-west-2.on.aws如果沒有此對應，您的自訂網域名稱將無法在 VPC Latters 中運作。如需詳細資訊，請參閱 Amazon Route 53 開發人員指南中的使用 Amazon Route 53 主控台建立記錄。此外，您可以參考以下步驟來建立託管區域和 CNAME 記錄，以將您的自訂網域名稱對應至 VPC Lagess 端點。

使用 Amazon 路線 53 主控台建立具有 CNAME 記錄的私有或公有託管區域

1. 請在 https://console.aws.amazon.com/route53/ 開啟 Route 53 主控台。
2. 在功能窗格中，選擇 [託管區域]，然後選擇 [建立託管區域]。
3. 對於網域名稱，請選擇您要用來將流量路由到 VPC Lady 服務的託管區域名稱。例如，如果您的自訂網域名稱是 parking.example.com (http://parking.example.com/)，則您託管區域的網域名稱將會是 example.com (http://example.com/)，也稱為頂點網域名稱。然後，您可以為此託管區域建立 CNAME 記錄，將流量路由到您的 VPC Lady 服務。注意：您無法在建立託管區域之後變更它的名稱。
4. 針對「類型」，視需要選擇「私人託管區域」或「公用託管區域」
5. 選擇您的地區，然後為您要與此託管區域建立關聯的 VPC 選取 VPC ID。
6. 視需要新增標記，然後選擇「建立託管區域」。建立之後，您的託管區域會列在託管區域下。
7. 若要在剛建立的託管區域中建立 CNAME 記錄，請選取託管區域，然後選取 [建立記錄]。
8. 在「建立記錄」下指定下列值：

    a. 在「記錄名稱」中，輸入您要用作自訂網域名稱的名稱。如果您想要使用 parking.example.com (http://acme.example.com/) 做為您的自訂網域名稱，請輸入 parking *。這表示您需要輸入子網域名稱，parking但不輸入託管區域名稱 example.com (http://example.com/)。

    b. 選擇 CNAME 做為「記錄類型」。

    c. 保持別名為關閉狀態。

    d. 在「值」中，輸入為您的服務產生網域名稱的 VPC Lady (例如my-service-02031c045478f6ddf1.7d67968.vpc-lattice-svcs.us-west-2.on.aws)。您可以在服務頁面上的 VPC 萊迪斯控制台中找到此自動生成的域名。如果使用 AWS CLI，create-service或list-services命令的輸出將傳回此自動產生的網域名稱。

    e. 對於 TTL (秒)，請接受預設值 300。

f. 對於路由策略，請選擇適用的路由策略。如需詳細資訊，請參閱 Amazon Route 53 開發人員指南中的選擇路由政策。

9. 選擇建立記錄。

變更通常會在 60 秒內傳播至所有 Route 53 伺服器。傳播完成後，您可以使用自訂網域名稱將流量路由到服務。

使用在託管區域中建立別名記錄 AWS CLI

1. 透過執行`get-service`命令，取得您的服務的 VPC Latds 產生的網域名稱 (例如，`my-service-02031c045478f6ddf1.7d67968.vpc-lattice-svcs.us-west-2.on.aws`) 和託管區域 ID。
2. 要設置別名，請使用以下命令。

```
aws route53 change-resource-record-sets --hosted-zone-id hosted-zone-id-for-your-service-domain --change-batch file://~/Desktop/change-set.json
```

對於`change-set.json`檔案，請在下列 JSON 範例中建立內容的 JSON 檔案，並將其儲存在本機電腦上。使用本地計算機中保存的 JSON *##########//#/##/### .JSON* 在上面的命令中。請注意，下列 JSON 中的「類型」可以是 A 或 AAAA 記錄類型。

```
{
    "Comment": "my-service-domain.com alias",
    "Changes": [
        {
            "Action": "CREATE",
            "ResourceRecordSet": {
                "Name": "my-custom-domain-name.com",
                "Type": "alias-record-type",
                "AliasTarget": {
                    "HostedZoneId": "hosted-zone-id-for-your-service-domain",
                    "DNSName": "lattice-generated-domain-name",
                    "EvaluateTargetHealth": true
                }
            }
        }
    ]
}
```

為 VPC 格子攜帶您自己的憑證 (BYOC)

若要提供 HTTPS 要求，您必須在 AWS Certificate Manager (ACM) 中準備好自己的 SSL/TLS 憑證，然後才能設定自訂網域名稱。這些憑證必須具有與服務之自訂網域名稱相符的主體替代名稱 (SAN) 或一般名稱 (CN)。如果 SAN 存在，我們只會在 SAN 清單中檢查相符項目。如果 SAN 不存在，我們會檢查 CN 中的相符項目。

VPC 格子會使用伺服器名稱指示 (SNI) 來提供 HTTPS 要求。DNS 會根據自訂網域名稱和與此網域名稱相符的憑證，將 HTTPS 要求路由傳送至您的 VPC 萊迪思服務。若要在 ACM 中為網域名稱申請 SSL/TLS 憑證，或將憑證匯入 ACM，請參閱使用者指南中的發行與管理憑證和匯入憑證。AWS Certificate Manager 如果您無法在 ACM 中請求或導入自己的證書，請使用 VPC Lady 生成的域名和證書。

VPC 萊迪思每個服務只接受一個自訂憑證。不過，您可以將自訂憑證用於多個自訂網域。這表示您可以對使用自訂網域名稱建立的所有 VPC Lady 服務使用相同的憑證。

若要使用 ACM 主控台檢視憑證，請開啟「憑證」，然後選取您的憑證 ID。您應該會在 [關聯的資源] 下看到與該憑證相關聯的 VPC Lady 服務。

限制及考量

- VPC 格子允許在關聯憑證的主體替代名稱 (SAN) 或一般名稱 (CN) 中深一層的萬用字元比對。例如，如果您使用自訂網域名稱建立服務，`parking.example.com`並將自己的憑證與 SAN 建立關聯`*.example.com`。當要求傳入時`parking.example.com`，VPC 萊迪格會將 SAN 與具有頂點網域的任何網域名稱相符。`example.com`不過，如果您有自訂網域，`parking.different.example.com`且憑證具有 SAN`*.example.com`，則要求會失敗。
- VPC 格子支援一個萬用字元網域比對等級。這表示萬用字元只能用作第一層子網域，而且只能保護一個子網域層級的安全。例如，如果您的憑證的 SAN 是`*.example.com`，則`parking.*.example.com`不受支援。
- VPC 萊迪思每個網域名稱支援一個萬用字元。這意味著這`*.*.example.com`是無效的。如需詳細資訊，請參閱AWS Certificate Manager 使用者指南中的要求公用憑證。
- VPC 晶格僅支援具有 2048 位元 RSA 金鑰的憑證。
- ACM 中的 SSL/TLS 憑證必須與您關聯的 VPC 格子服務位於相同的區域。

保護您憑證的私密金鑰

當您使用 ACM 要求 SSL/TLS 憑證時，ACM 會產生公開/私密 key pair。匯入憑證時，您會產生 key pair。公有金鑰會成為憑證的一部分。為了安全地儲存私密金鑰，ACM 會使用 AWS KMS別名為 aw s/

acm 的 KMS 金鑰建立另一個金鑰。 AWS KMS 使用此金鑰來加密憑證的私密金鑰。如需詳細資訊，請參閱《AWS Certificate Manager 使用指南》AWS Certificate Manager中的〈資料保護〉。

VPC 萊迪思使用 AWS TLS 連線管理員，這是一項只能由人員存取的服務來保護和使用憑證的私密金鑰。 AWS 服務當您使用 ACM 憑證建立 VPC 萊迪思服務時，VPC 萊迪思會將您的憑證與 AWS TLS 連線管理員建立關聯。我們透過 AWS KMS 針對您的 AWS 託管金鑰建立授權來做到這一點。此授權允許 TLS 連線管理員使用 AWS KMS 來解密憑證的私密金鑰。TLS 連線管理員會使用憑證和解密 (純文字) 私密金鑰，與 VPC 萊迪思服務的用戶端建立安全連線 (SSL/TLS 工作階段)。當憑證與 VPC 萊迪思服務中斷關聯時，授權就會被淘汰。如需詳細資訊，請參閱AWS Key Management Service 開發人員指南中的授權。

如需詳細資訊，請參閱 靜態加密。

刪除服務

若要刪除 VPC Lady 服務，您必須先刪除該服務與任何服務網路可能具有的所有關聯。如果您刪除服務，與服務相關的所有資源 (例如資源原則、驗證原則、接聽程式、接聽程式規則和存取記錄訂閱) 也會一併刪除。

使用主控台刪除服務

1. 前往 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在功能窗格的 VPC 格子下，選擇 [服務]。
3. 在 [服務] 頁面上，選取您要刪除的服務，然後選擇 [動作] > [刪除服務]。
4. 出現確認提示時，請選擇刪除。

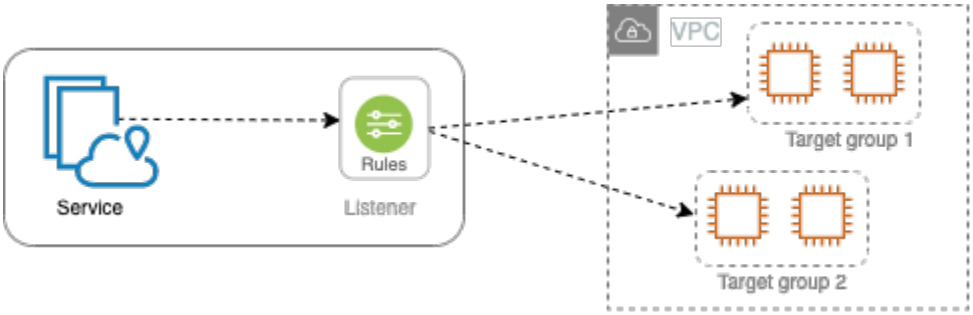
若要使用刪除服務 AWS CLI

使用刪除服務命令。

VPC 格子中的目標群體

VPC Lady 目標群組是執行應用程式或服務的目標或運算資源的集合。目標可以是 EC2 執行個體、IP 地址、Lambda 函數、應用程式負載平衡器或 Kubernetes 網繭。您也可以將現有服務附加到目標群組。如需將 Kubernetes 與 VPC 晶格搭配使用的詳細資訊，請參閱AWS 閘道 API 控制器使用者指南。

每個目標群組會用來將請求轉送到一個或多個註冊的目標。建立監聽器規則時，您可以指定目標群組和條件。規則的條件符合時，會將流量轉送到對應的目標群組。您可以針對不同類型的請求，建立不同的目標群組。例如，為一般要求建立一個目標群組，針對包含特定規則條件 (例如路徑或標頭值) 的要求建立其他目標群組。



您可以針對每個目標群組定義服務的健全狀況檢查設定。除非您在建立目標群組時覆寫這些設定，或是在之後修改設定，否則每個目標群組都會使用預設的運作狀態檢查設定。在監聽器的規則中指定目標群組之後，服務會持續監督向目標群組註冊之所有目標的健全狀況。服務會將要求路由傳送至狀況良好的已註冊目標。

若要在服務接聽程式的規則中指定目標群組，目標群組必須與服務位於相同的帳戶中。

VPC 萊迪思目標群與 Elastic Load Balancing 提供的目標群體類似，但它們不可互換。

目錄

- 虛擬私人雲端格子中的 HTTP 目標
- 作為 VPC 晶格中的目標的 Lambda 函數
- 應用程式負載平衡器做為 VPC 點陣中的目標
- 通訊協定版本
- VPC 格子目標群組的標籤
- 刪除目標群組

建立 VPC 格子目標群組

您會向目標群組註冊您的目標。依預設，VPC Lady 服務會使用您為目標群組指定的連接埠和通訊協定，將要求傳送至已註冊的目標。在透過目標群組來註冊每個目標時，您可以覆寫此埠號。

若要將流量路由到目標群組中的目標，請在建立接聽程式或為接聽程式建立規則時，於動作中指定目標群組。如需詳細資訊，請參閱 您的 VPC 格子服務的接聽程式規則。您可以在多個監聽器中指定相同的目標群組，但這些監聽器必須屬於相同的服務。若要將目標群組與服務搭配使用，您必須確認任何其他服務的監聽器未使用目標群組。

您可以隨時從目標群組新增或移除目標。如需詳細資訊，請參閱 使用 VPC 格子目標群組註冊目標。您也可以修改目標群組的運作狀態檢查設定。如需詳細資訊，請參閱 針對 VPC 萊迪思目標群組進行 Health 狀態檢查。

建立目標群組

您可以建立目標群組，並選擇性地註冊目標，如下所示。

使用主控台來建立目標群組

1. 前往 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在功能窗格的「VPC 格子」下，選擇「目標群組」。
3. 選擇 Create target group (建立目標群組)。
4. 針對 「選擇目標類型」，執行下列任一項作業：
    - 選擇執行個體以依執行處理 ID 註冊目標。
    - 選擇 IP 位址以依 IP 位址註冊目標。
    - 選擇 Lambda 函數以將 Lambda 函數註冊為目標。
    - 選擇 Ap plication Load Balancer，將應用程式負載平衡器註冊為目標。

5. 針對 Target group name (目標群組名稱)，輸入目標群組的名稱。此名稱在每個 AWS 區域中的帳戶必須是唯一的，最多可包含 32 個字元，只能包含英數字元或連字號，且不得以連字號開頭或結尾。
6. 對於通訊協定和連接埠，您可以視需要修改預設值。預設通訊協定為 HTTPS，預設連接埠為 443。

   如果目標類型是 Lambda 函數，則無法指定通訊協定或連接埠。
7. 對於 IP 位址類型，請選擇 IPv4 以使用 IPv4 位址註冊目標，或選擇 IPv6 以使用 IPv6 位址註冊目標。建立目標群組後，您無法變更此設定。

   僅當目標類型為 IP 位址時，此選項才可用。
8. 針對 VPC (VPC) 選擇虛擬私有雲端 (VPC)。

   如果目標類型是 Lambda 函數，則此選項不可用。
9. 對於通訊協定版本，請視需要修改預設值。預設值為 HTTP1。

   如果目標類型是 Lambda 函數，則此選項不可用。
10. 對於 Health 狀態檢查，請視需要修改預設設定。如需詳細資訊，請參閱 針對 VPC 萊迪思目標群組進行 Health 狀態檢查。

    如果目標類型為 Lambda 函數，則無法使用 Health 狀態檢查。
11. 對於 Lambda 事件結構版本，請選擇一個版本。如需詳細資訊，請參閱 the section called “從 VPC 萊迪思服務接收事件”。

    僅當目標類型為 Lambda 函數時，此選項才可用
12. (選擇性) 若要新增標籤，請展開「標籤」，選擇「新增標籤」，然後輸入標籤關鍵字和標籤值。
13. 選擇下一步。
14. 對於註冊目標，您可以略過此步驟或新增目標，如下所示：
    - 如果目標類型為執行個體，請選取執行個體，輸入連接埠，然後選擇包含為以下待定的項目。
    - 如果目標類型是 IP 地址，請執行下列動作：
      a. 針對 [選擇網路]，保留您為目標群組選取的 VPC，或選擇 [其他私人 IP 位址]。
      b. 對於指定 IP 和定義通訊埠，輸入 IP 位址並輸入通訊埠。預設連接埠是目標群組連接埠。
      c. 選擇包含為下方待處理項目。
    - 如果目標類型是 Lambda 函數，請選擇 Lambda 函數。若要建立 Lambda 函數，請選擇 [建立新的 Lambda 函數]。

- 如果目標類型是「Ap plication Load Balancer」，請選擇應用程式負載平衡器。若要建立 Application Load Balancer，請選擇建立 Application Load Balancer。

15. 選擇 Create target group (建立目標群組)。

若要使用建立目標群組 AWS CLI

使用指create-target-group令建立目標群組，並使用「註冊-目標」指令來新增目標。

共用子網路

參與者可以在共用的 VPC 中建立 VPC 萊迪思目標群組。下列規則適用於共用子網路：

- VPC Lady 服務的所有部分 (例如接聽程式、目標群組和目標) 都必須由相同的帳戶建立。它們可以在 VPC Lady 服務擁有者擁有的子網路中建立，也可以與 VPC Lady 服務的擁有者共用。
- 在目標群組註冊的目標必須使用與目標群組相同的帳戶建立。
- 只有 VPC 的擁有者可以將 VPC 與服務網路建立關聯。與服務網路相關聯的共用 VPC 中的參與者資源可以將請求傳送至與服務網路相關聯的服務。不過，系統管理員可以使用安全性群組、網路 ACL 或驗證原則來防止這種情況發生。

如需 VPC 萊迪思可共用資源的詳細資訊，請參閱。分享 VPC 格子資源

使用 VPC 格子目標群組註冊目標

您的服務可作為用戶端的單一聯絡窗口，並將傳入流量分配到其健全的註冊目標。您可以利用一個或多個群組來登錄每個目標。

如果應用程式的需求增加，您可以向一或多個目標群組註冊其他目標，以處理需求。一旦註冊程序完成且目標通過初始健全狀況檢查，服務就會立即開始將要求路由傳送至新註冊的目標。

如果對您應用程式的需求減少，或者您需要為目標提供服務，可以從目標群組取消目標的登錄。取消目標的登錄，會將該目標從目標群組中移除，但不會影響到目標。一旦目標取消註冊，服務就會停止將要求路由傳送至目標。目標會進入 DRAINING 狀態，直到處理中的請求已完成。當您準備讓目標再繼續接收請求時，可以將目標註冊到目標群組。

目標群組的目標類型會決定您向該目標群組註冊目標的方式。如需詳細資訊，請參閱 Target type (目標類型)。

使用下列主控台程序來註冊或取消註冊目標。或者，使用中的註冊-目標和取消註冊- 目標命令。 AWS CLI

目錄

根據執行個體 ID 來登記或取消登記目標

目標執行個體必須位於您為目標群組指定的虛擬私有雲 (VPC) 中。在註冊時，執行個體也必須處於 `running` 狀態。

當您依執行個體 ID 註冊目標時，您可以將服務與 Auto Scaling 群組搭配使用。將目標群組附加到 Auto Scaling 群組並向外擴充之後，Auto Scaling 群組啟動的執行個體會自動向目標群組註冊。如果分離目標群組與 Auto Scaling 群組的連結，會自動從該目標群組中取消註冊執行個體。如需詳細資訊，請參閱 Amazon EC2 Auto Scaling 使用者指南中的使用 VPC 萊迪目標群組將流量路由到您的 Auto Scaling 群組。

使用主控台根據執行個體 ID 來註冊或取消註冊目標

1. 前往 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在功能窗格的「VPC 格子」下，選擇「目標群組」。
3. 選擇目標群組的名稱，以開啟其詳細資訊頁面。
4. 選擇 Targets (目標) 標籤。
5. 若要註冊執行個體，請選擇註冊目標。選取執行個體，輸入執行個體連接埠，然後在下方選擇 [包含為擱置中]。完成新增執行個體時，請選擇 [註冊目標]。
6. 若要取消註冊執行處理，請選取執行處理，然後選擇 [取消註冊]。

根據 IP 地址來登記或取消登記目標

目標 IP 位址必須來自您為目標群組指定的 VPC 的子網路。您無法在同一個 VPC 中註冊其他服務的 IP 位址。您無法註冊 VPC 端點或可公開路由的 IP 位址。

使用主控台根據 IP 地址來註冊或取消註冊目標

1. 前往 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在功能窗格的「VPC 格子」下，選擇「目標群組」。
3. 選擇目標群組的名稱，以開啟其詳細資訊頁面。
4. 選擇 Targets (目標) 標籤。
5. 若要註冊 IP 地址，請選擇註冊目標。為每個 IP 地址選取網路，輸入 IP 地址和連接埠，然後選擇包含為下方待處理項目。完成指定位址後，請選擇 [註冊目標]。
6. 若要取消註冊 IP 地址，請選取 IP 地址，然後選擇取消註冊。

註冊或取消註冊 Lambda 函數

您可以向目標群組註冊單一 Lambda 函數。如果您不再需要將流量傳送到您的 Lambda 函數，則可以將它取消註冊。取消註冊 Lambda 函數之後，傳輸中的請求會失敗，出現 HTTP 5XX 錯誤。建立新的目標群組會比較好，而不是取代目標群組的 Lambda 函數。

使用主控台註冊或取消註冊 Lambda 函數

1. 前往 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在功能窗格的「VPC 格子」下，選擇「目標群組」。
3. 選擇目標群組的名稱，以開啟其詳細資訊頁面。
4. 選擇 Targets (目標) 標籤。
5. 如果沒有註冊 Lambda 函數，請選擇註冊目標。選取 Lambda 函數，然後選擇 [註冊目標]。
6. 若要取消註冊 Lambda 函數，請選擇 Deregister (取消註冊)。當系統提示您確認時，請輸入，**`confirm`**然後選擇「取消註冊」。

註冊或取消註冊 Application Load Balancer

您可以向每個目標群組註冊單一「Application Load Balancer」。如果您不再需要傳送流量至負載平衡器，您可以取消註冊。取消註冊負載平衡器後，執行中要求會失敗，並出現 HTTP 5XX 錯誤。最好建立新的目標群組，而不是取代目標群組的「Application Load Balancer」。

使用主控台註冊或取消註冊應用程式負載平衡器

1. 前往 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。

2. 在功能窗格的「VPC 格子」下，選擇「目標群組」。
3. 選擇目標群組的名稱，以開啟其詳細資訊頁面。
4. 選擇 Targets (目標) 標籤。
5. 如果沒有註冊 Application Load Balancer，請選擇註冊目標。選取應用程式負載平衡器，然後選擇註冊目標。
6. 若要取消註冊應用程式負載平衡器，請選擇取消註冊。當系統提示您確認時，請輸入，**confirm**然後選擇「取消註冊」。

針對 VPC 萊迪思目標群組進行 Health 狀態檢查

您的服務會定期傳送要求至其註冊目標，以測試其狀態。這些測試稱為運作狀況檢查。

每個 VPC 萊迪思服務只會將要求路由傳送至健全的目標。每個服務都會使用註冊目標之目標群組的健全狀況檢查設定值，檢查每個目標的健全狀況檢查設定值。目標註冊後，必須通過一次運作狀態檢查，才算運作狀態良好。完成每次健全狀況檢查之後，服務會關閉為健全狀況檢查建立的連線。

限制和注意事項

- 當目標群組通訊協定版本為 HTTP1 時，依預設會啟用健全狀況檢查。
- 當目標群組通訊協定版本為 HTTP2 時，依預設不會啟用健全狀況檢查。不過，您可以啟用健全狀況檢查，並手動將通訊協定版本設定為 HTTP1 或 HTTP2。
- Health 檢查不支援 gRPC 目標群組通訊協定版本。但是，如果啟用健全狀況檢查，則必須將健全狀況檢查通訊協定版本指定為 HTTP1 或 HTTP2。
- 運作 Health 態檢查不支援 Lambda 目標群組。
- Health 檢查不支援 Application Load Balancer 目標群組。不過，您可以使用 Elastic Load Balancing，為應用程式負載平衡器的目標啟用健康狀態檢查。如需詳細資訊，請參閱《應用程式負載平衡器使用者指南》中的目標群組健全狀況。

運作狀態檢查設定

您需要按下表中的描述為目標群組中的目標設定運作狀態檢查。表中使用的設定名稱是 API 中使用的名稱。此服務會使用指定的連接埠、通訊協定和 ping 路徑，每HealthCheckIntervalSeconds秒傳送健全狀況檢查要求至每個已註冊的目標。每個運作狀態檢查請求是各自獨立，且在整個間隔內持續保持此結果。目標回應所花的時間不影響下次運作狀態檢查請求的間隔。如果健全狀況檢查超過UnhealthyThresholdCount連續的失敗，服務會使目標停止服務。當健全狀況檢查超過HealthyThresholdCount連續成功時，服務會將目標重新啟用。

設定	描述
HealthCheckProtocol	服務在目標上執行健全狀況檢查時使用的通訊協定。可能的通訊協定是 HTTP 和 HTTPS。預設為 HTTP 通訊協定。
HealthCheckPort	服務在目標上執行健全狀況檢查時使用的連接埠。預設值是使用每個目標從服務接收流量的連接埠。
HealthCheckPath	目標上運作狀態檢查的目的地。 如果協議版本是 HTTP1 或 HTTP2，請指定一個有效的 URI（/路徑？ 查詢）。預設為 /.
HealthCheckTimeoutSeconds	以秒為單位的時間量，若目標在此期間內毫無回應即表示運作狀態檢查失敗。範圍為 1-120 秒。如果目標類型為INSTANCE或，則預設值為 5 秒IP。指定 0 可將此設定重設為預設值。
HealthCheckIntervalSeconds	個別目標每次執行運作狀態檢查的大約間隔時間量，以秒為單位。範圍介於 5–300 秒之間。如果目標類型為INSTANCE或，則預設值為 30 秒IP。指定 0 可將此設定重設為預設值。
HealthyThresholdCount	在不健康的目標被視為健康狀況良好之前，所需的連續成功運作狀況檢查次數。範圍介於 2–10 之間。預設值為 5。指定 0 可將此設定重設為預設值。
UnhealthyThresholdCount	在將目標視為運作狀態不良前，必要的連續運作狀態檢查失敗次數。範圍介於 2–10 之間。預設為 2。指定 0 可將此設定重設為預設值。
Matcher	檢查是否收到來自目標的成功回應時所使用的代碼。這些在主控台中稱為成功代碼。 如果通訊協定版本為 HTTP1 或 HTTP2，則可能的值為 200 到 499 之間。您可以指定多個值 (例

設定	描述
	如，"200,202") 或值範圍 (例如，"200-299")。預設值為 200。 目前不支援 gRPC 的 Health 狀態檢查通訊協定版本。不過，如果您的目標群組通訊協定版本是 gRPC，您可以在健全狀況檢查組態中指定 HTTP1 或 HTTP2 通訊協定版本。

檢查目標的運作狀態

您可以檢查已向目標群組註冊的各個目標的運作狀態。

使用主控台檢查目標的運作狀態

1. 前往 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在功能窗格的「VPC 格子」下，選擇「目標群組」。
3. 選擇目標群組的名稱，以開啟其詳細資訊頁面。
4. 在 Targets (目標) 標籤，Health status (運作狀態) 欄指出各目標的狀態。如果狀態為除以外的任何值`Healthy`，則 [Health 全狀況狀態詳細資料] 欄會包含更多資訊。

使用檢查目標的健康狀態 AWS CLI

使用列表目標命令。此命令的輸出包含目標的運作狀態。如果狀態為 `Healthy` 以外的任何值，則輸出也會包含原因代碼。

接收有關狀態不良目標的電子郵件通知

使用 CloudWatch 警示啟動 Lambda 函數，以傳送有關運作狀態不良目標的詳細資訊。

修改健康狀態檢查設定

您可以隨時修改目標群組的運作狀態檢查設定。

使用主控台修改健全狀況檢查設定

1. 前往 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。

2. 在功能窗格的「VPC 格子」下，選擇「目標群組」。
3. 選擇目標群組的名稱，以開啟其詳細資訊頁面。
4. 在健全狀況檢查標籤的 Health 全狀況檢查設定區段中，選擇編輯。
5. 視需要修改健康狀態檢查設定。
6. 選擇儲存變更。

若要使用修改健全狀況檢查設定 AWS CLI

使用 update-target-group 命令。

路由組態

依預設，服務會使用您在建立目標群組時指定的通訊協定和連接埠號碼，將要求路由傳送至其目標。或者，您可以在使用目標群組來登錄目標時，覆寫用來將流量轉傳到目標的連接埠。

目標群組支援下列的通訊協定和連接埠：

- Protocols (通訊協定)：HTTP、HTTPS
- Ports (連接埠)：1-65535

如果目標群組是使用 HTTPS 通訊協定設定或使用 HTTPS 健全狀況檢查，則目標的 TLS 連線會使用監聽器的安全性原則。VPC 萊迪思會使用您在目標上安裝的憑證，與目標建立 TLS 連線。VPC 萊迪思不會驗證這些憑證。因此，您可以使用自我簽署的憑證或已過期的憑證。VPC Ladters 與目標之間的流量會在封包層級進行驗證，因此即使目標上的憑證無效，也不會受到 man-in-the-middle 攻擊或詐騙的風險。

路由演算法

依預設，循環配置資源路由演算法會用來將要求路由到健全狀況良好的目標。

當 VPC 萊迪思服務收到請求時，它會使用以下過程：

1. 以優先順序評估接聽程序的規則，以決定要套用哪個規則。
2. 使用預設循環配置資源演算法，從目標群組中選取規則動作的目標。即使一個目標向多個目標群組註冊，每個目標群組的路由都是獨立運作。

如果目標群組只包含狀況不良的目標，則會將要求路由至所有目標，不論其健全狀況狀態為何。這表示如果所有目標都同時失敗健康狀態檢查，則 VPC Lady 服務會無法開啟。失敗開啟的影響是根據循環配置資源演算法，允許流量傳送至所有目標，無論其健全狀況狀態為何。

Target type (目標類型)

建立目標群組時，您會指定其目標類型，這會決定您對此目標群組註冊目標時指定的目標類型。在建立目標群組之後，您無法變更其目標類型。

下列是可能的目標類型：

`INSTANCE`

以執行個體 ID 來指定目標。

`IP`

目標為 IP 地址。

`LAMBDA`

目標是 Lambda 函數。

`ALB`

目標是 Application Load Balancer。

考量事項

- 當目標類型為時`IP`，您必須從目標群組的 VPC 子網路指定 IP 位址。如果您需要從此 VPC 外部註冊 IP 位址，請建立類型的目標群組，`ALB`並向 Application Load Balancer 註冊 IP 位址。
- 當目標類型為時`IP`，您無法註冊 VPC 端點或可公開路由的 IP 位址。
- 當目標類型為時`LAMBDA`，您可以註冊單個 Lambda 函數。當服務收到 Lambda 函數的要求時，就會叫用 Lambda 函數。如果您想向服務註冊多個 lambda 函數，則需要使用多個目標群組。
- 當目標類型為時`ALB`，您可以將單一內部 Application Load Balancer 註冊為最多兩個 VPC 萊迪思服務的目標。若要這麼做，請將 Application Load Balancer 註冊給兩個不同的 VPC Lady 服務所使用的兩個不同的目標群組。此外，目標 Application Load Balancer 必須至少有一個監聽器，其連接埠與目標群組連接埠相符。
- 若要將 ECS 任務註冊為目標，請使用目`ALB`標類型並為 Amazon ECS 服務註冊應用程式負載平衡器。如需詳細資訊，請參閱 Amazon Elastic Container Service Developer Guide 中的 Service load balancing。

- 若要將 EKS 網繭註冊為目標，請使用AWS 閘道 API 控制器，該控制器會從 Kubernetes 服務取得 IP 位址。

IP 地址類型

當您使用的目標類型建立目標群組時IP，您可以指定目標群組的 IP 位址類型。這會指定負載平衡器用來傳送要求和健全狀況檢查至目標的位址類型。可能的值為 IPv4 和 IPv6。預設值為 IPV4。

考量事項

- 如果您使用的 IP 位址類型建立目標群組IPv6，則您為目標群組指定的 VPC 必須具有 IPv6 位址範圍。
- 您向目標群組註冊的 IP 位址必須與目標群組的 IP 位址類型相符。例如，如果目標群組的 IP 位址類型為，您就無法向目標群組註冊 IPv6 位址IPv4。
- 您向目標群組註冊的 IP 位址必須位於您為目標群組指定之 VPC 的 IP 位址範圍內。

虛擬私人雲端格子中的 HTTP 目標

HTTP 請求和 HTTP 回應使用標頭欄位來傳送有關 HTTP 訊息的資訊。HTTP 標頭會自動新增。標頭欄位是以冒號分隔的名稱值組，以歸位字元 (CR) 和換行 (LF) 分隔。一組以 RFC 2616 定義的標準 HTTP 標頭欄位，訊息標頭。也有應用程式廣泛採用的非標準 HTTP 標頭可用 (而且會自動新增)。例如，有帶有x-forwarded前綴的非標準 HTTP 標頭。

x-forwarded標頭

Amazon VPC 格子添加了以下x-forwarded標題：

`x-forwarded-for`

來源 IP 位址。

`x-forwarded-for-port`

目的地連接埠。

`x-forwarded-for-proto`

連線通訊協定 (http|https)。

呼叫者身份標題

Amazon VPC 格子會新增下列來電者身分標頭：

`x-amz-lattice-identity`

身份信息。如果 AWS 驗證成功，則會顯示下列欄位。

- `principal`— 已驗證的主體。
- `principalOrgID`— 已驗證主參與者的組織 ID。
- `sessionName`— 已驗證工作階段的名稱。

如果使用「任何角色」認證且驗證成功，則會顯示下列欄位。

- `X509Issuer/OU`— 發行者 (OU)。
- `X509SAN/DNS`— 主旨替代名稱 (DNS)。
- `X509SAN/NameCN`— 發行人替代名稱 (名稱 /CN)。
- `X509SAN/URI`— 主旨替代名稱 (URI)。
- `X509Subject/CN`— 主旨名稱 (CN)。

`x-amz-lattice-network`

VPC。格式如下所示。

```
source-vpc=arn:aws:ec2:region:account:vpc/id
```

`x-amz-lattice-target`

目標。格式如下所示。

```
service=arn;service-network=arn;target-group=arn
```

如需 VPC 晶格資源 ARN 的相關資訊，請參閱 Amazon VPC 萊格定義的資源類型。

作為 VPC 晶格中的目標的 Lambda 函數

您可以將 Lambda 函數註冊為 VPC 萊迪目標群組的目標，並設定接聽程式規則，將要求轉送至 Lambda 函數的目標群組。當服務將請求轉送至以 Lambda 函數作為目標的目標群組時，它會叫用您

的 Lambda 函數，並以 JSON 格式將請求的內容傳遞至 Lambda 函數。如需詳細資訊，請參閱AWS Lambda 開發人員指南中的 AWS Lambda 與 Amazon VPC 萊迪思搭配使用。

限制

- Lambda 函數和目標群組必須在相同的帳戶中，且在相同的區域內。
- 您可以傳送至 Lambda 函數的要求主體大小上限為 6 MB。
- Lambda 函數可以傳送的回應 JSON 大小上限為 6 MB。
- 通訊協定必須是 HTTP 或 HTTPS。

準備 Lambda 函數

如果您將 Lambda 函數與 VPC 萊迪斯服務搭配使用，則適用下列建議。

調用 Lambda 函數的許可

當您使用 AWS Management Console 或建立目標群組並註冊 Lambda 函數時 AWS CLI，VPC Ladters 會代表您將必要的權限新增至您的 Lambda 函數政策。

您也可以使用下列 API 呼叫自行新增權限：

```
aws lambda add-permission \
  --function-name lambda-function-arn-with-alias-name \
  --statement-id vpc-lattice \
  --principal vpc-lattice.amazonaws.com \
  --action lambda:InvokeFunction \
  --source-arn target-group-arn
```

Lambda 函數版本控制

您可以為每個目標群組註冊一個 Lambda 函數。若要確保您可以變更 Lambda 函數，並且 VPC 萊迪思服務一律叫用目前版本的 Lambda 函數，請在向 VPC Ladters 服務註冊 Lambda 函數時，建立函數別名並在函數 ARN 中包含別名。如需詳細資訊，請參閱《AWS Lambda 開發人員指南》中的 AWS Lambda 函數版本控制與別名功能和使用別名轉移流量。

為 Lambda 函數建立目標群組

建立目標群組以用於請求路由。如果請求內容符合接聽程式規則與將其轉寄至此目標群組的動作，則 VPC Lady 服務會叫用已註冊的 Lambda 函數。

使用主控台建立目標群組並註冊 Lambda 函數

1. 前往 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在功能窗格的「VPC 格子」下，選擇「目標群組」。
3. 選擇 Create target group (建立目標群組)。
4. 在選取目標類型中，選取 Lambda 函數。
5. 針對 Target group name (目標群組名稱)，輸入目標群組的名稱。
6. 對於 Lambda 事件結構版本，請選擇一個版本。如需詳細資訊，請參閱 the section called “從 VPC 萊迪思服務接收事件”。
7. (選擇性) 若要新增標籤，請展開「標籤」，選擇「新增標籤」，然後輸入標籤關鍵字和標籤值。
8. 選擇下一步。
9. 對於 Lambda function (Lambda 函數)，請執行以下其中一項：
   - 選取現有的 Lambda 函數。
   - 建立新的 Lambda 函數並加以選取。
   - 稍後註冊 Lambda 函數。
10. 選擇 Create target group (建立目標群組)。

使用 AWS CLI建立目標群組和註冊 Lambda 函數

使用create-target-group和註冊目標命令。

從 VPC 萊迪思服務接收事件

VPC 格服務支援透過 HTTP 和 HTTPS 進行請求的 Lambda 叫用。服務會以 JSON 格式傳送事件，並將`X-Forwarded-For`標頭新增至每個要求。

Base64 編碼

如果`content-encoding`標頭存在且內容類型不是下列其中一項，則服務 Base64 會編碼主體：

- `text/*`
- `application/json`
- `application/xml`
- `application/javascript`

如果 content-encoding 標頭不存在，則 Base64 編碼取決於內容類型。對於上述內容類型，服務會依原樣傳送主體，而不使用 Base64 編碼。

事件結構格式

建立或更新類型的目標群組時LAMBDA，您可以指定 Lambda 函數接收的事件結構版本。可能的版本是V1和V2。

Example 範例事件：V2

```
{
    "version": "2.0",
    "path": "/",
    "method": "GET|POST|HEAD|...",
    "headers": {
        "header-key": ["header-value", ...],
        ...
    },
    "queryStringParameters": {
        "key": "value", ...
    },
    "body": "request-body",
    "isBase64Encoded": true|false,
    "requestContext": {
        "serviceNetworkArn": "arn:aws:vpc-
lattice:region:123456789012:servicenetwork/sn-0bf3f2882e9cc805a",
        "serviceArn": "arn:aws:vpc-
lattice:region:123456789012:service/svc-0a40eebed65f8d69c",
        "targetGroupArn": "arn:aws:vpc-
lattice:region:123456789012:targetgroup/tg-6d0ecf831eec9f09",
        "identity": {
            "sourceVpcArn":
 "arn:aws:ec2:region:123456789012:vpc/vpc-0b8276c84697e7339",
            "type": "AWS_IAM",
            "principal": "arn:aws:iam::123456789012:assumed-role/my-role/my-session",
            "principalOrgID": "o-50dc6c495c0c9188",
            "sessionName": "i-0c7de02a688bde9f7",
            "x509IssuerOu": "string",
            "x509SanDns": "string",
            "x509SanNameCn": "string",
            "x509SanUri": "string",
            "x509SubjectCn": "string"
        },
        "region": "region",
```

```
        "timeEpoch": "1690497599177430"
    }
}
```

`body`

請求的本文。僅當通訊協定為 HTTP、HTTPS 或 gRPC 時才會顯示。

`headers`

要求的 HTTP 標頭。僅當通訊協定為 HTTP、HTTPS 或 gRPC 時才會顯示。

`identity`

身份信息。以下是可能的欄位。

- `principal`— 已驗證的主體。只有在 AWS 驗證成功時才會出現。
- `principalOrgID`— 已驗證主參與者的組織 ID。只有在 AWS 驗證成功時才會出現。
- `sessionName`— 已驗證工作階段的名稱。只有在 AWS 驗證成功時才會出現。
- `sourceVpcArn`— 產生請求所在的 VPC 的 ARN。只有在可識別來源 VPC 時才會出現。
- `type`-該值是`AWS_IAM`如果使用了身份驗證策略並且 AWS 身份驗證成功。

如果使用「任何角色」認證且驗證成功，則下列為可能的欄位。

- `x509IssuerOu`— 發行者 (OU)。
- `x509SanDns`— 主旨替代名稱 (DNS)。
- `x509SanNameCn`— 發行人替代名稱 (名稱 /CN)。
- `x509SanUri`— 主旨替代名稱 (URI)。
- `x509SubjectCn`— 主旨名稱 (CN)。

`isBase64Encoded`

指出主體是否為 base64 編碼。只有在通訊協定為 HTTP、HTTPS 或 gRPC，且要求主體還不是字串時，才會顯示此選項。

`method`

請求的 HTTP 方法。僅當通訊協定為 HTTP、HTTPS 或 gRPC 時才會顯示。

`path`

請求的路徑。僅當通訊協定為 HTTP、HTTPS 或 gRPC 時才會顯示。

`queryStringParameters`

HTTP 查詢字串參數。僅當通訊協定為 HTTP、HTTPS 或 gRPC 時才會顯示。

`serviceArn`

接收要求之服務的 ARN。

`serviceNetworkArn`

傳遞要求的服務網路的 ARN。

`targetGroupArn`

接收要求之目標群組的 ARN。

`timeEpoch`

時間，以微秒為單位。

Example 事件範例：V1

```
{
    "raw_path": "/path/to/resource",
    "method": "GET|POST|HEAD|...",
    "headers": {"header-key": "header-value", ... },
    "query_string_parameters": {"key": "value", ...},
    "body": "request-body",
    "is_base64_encoded": true|false
}
```

回應 VPC 格子服務

來自 Lambda 函數的回應必須包含 Base64 編碼狀態、狀態碼、狀態描述和標頭。您可以省略內文。

若要在回應的內文中包含二進位內容，您必須將內容以 Base64 編碼，並將 `isBase64Encoded` 設定為 `true`。該服務解碼內容以檢索二進制內容，並將其發送到 HTTP 響應主體中的客戶端。

VPC 格子服務不接受 hop-by-hop 標頭，例如`Connection`或`Transfer-Encoding`。您可以省略標`Content-Length`頭，因為服務會在傳送回應給用戶端之前先計算標頭。

以下是來自 Lambda 函數的範例回應：

```
{
```

```
    "isBase64Encoded": false,
    "statusCode": 200,
    "statusDescription": "200 OK",
    "headers": {
        "Set-cookie": "cookies",
        "Content-Type": "application/json"
    },
    "body": "Hello from Lambda (optional)"
}
```

多值標頭

根據預設，VPC 萊迪思支援來自用戶端的請求或來自 Lambda 函數的回應，其中包含具有多個值或多次包含相同標頭的標頭。VPC 萊迪思還支持具有相同密鑰的多個值的查詢參數。

對於請求標頭，如果多個參數共享相同的名稱，VPC Lady 會將這兩個值傳遞給目標。下面是一個例子，其中`header 1`是兩個單獨的標題的名稱：

```
header1 = foo
header1 = bar
```

然後 VPC 格子將這兩個值發送到目標：

```
"header1": ["foo", "bar"]
```

對於查詢字串，如果多個參數共用相同的名稱，則最後一個值將獲勝。這表示如果參數共用相同的金鑰名稱，就會_not_ coalesced變成單一值。

下面是一個例子，其中`foo`和`bar`是具有相同名稱的參數值`QS1`：

```
http://www.example.com?&QS1=foo&QS1=bar
```

然後 VPC 格子將最後一個值發送到目標：

```
"QS1": "bar"
```

取消註冊 Lambda 函數

如果您不再需要將流量傳送到您的 Lambda 函數，則可以將它取消註冊。取消註冊 Lambda 函數之後，傳輸中的請求會失敗，出現 HTTP 5XX 錯誤。

若要取代 Lambda 函數，建議您建立新的目標群組、向新目標群組註冊新函數，並更新接聽程式規則以使用新的目標群組，而非現有的目標群組。

若要使用主控台取消註冊 Lambda 函數

1. 前往 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在功能窗格的「VPC 格子」下，選擇「目標群組」。
3. 選擇目標群組的名稱，以開啟其詳細資訊頁面。
4. 在 Targets (目標) 索引標籤上，選擇 Deregister (取消註冊)。
5. 當系統提示您確認時，請輸入，**`confirm`**然後選擇「取消註冊」。

若要使用取消註冊 Lambda 函數 AWS CLI

使用 deregister-targets 命令。

應用程式負載平衡器做為 VPC 點陣中的目標

您可以建立 VPC 萊迪思目標群組、將單一內部 Application Load Balancer 註冊為目標，然後設定 VPC Ladesser 服務以將流量轉送至此目標群組。在這個案例中，Application Load Balancer 會在流量到達時接管路由決策。此組態可讓您將應用程式負載平衡器的第 7 層請求型路由功能與 VPC Ladters 支援的功能結合使用，例如 IAM 身份驗證和授權，以及跨 VPC 和帳戶的連線。

限制

- 您可以將單一內部 Application Load Balancer 註冊為 VPC Lady 目標群組類型ALB中的目標。
- 您可以將 Application Load Balancer 註冊為最多兩個 VPC Lady 目標群組的目標，這些群組由兩個不同的 VPC Lady 服務使用。
- VPC 萊迪思不會為ALB類型目標群組提供健康狀態檢查。不過，您可以針對 Elastic Load Balancing 中的目標，在負載平衡器層級獨立設定健全狀況檢查。如需詳細資訊，請參閱應用程式負載平衡器使用者指南中針對目標群組進行 Health 狀態檢查

必要條件

建立 Application Load Balancer，以向您的 VPC Lady 目標群組註冊為目標。負載平衡器必須符合下列條件：

- 負載平衡器配置為「內部」。

- 應用程式負載平衡器必須與 VPC Lady 目標群組位於相同的帳戶中，且必須處於作用中狀態。
- 應用程式負載平衡器必須與 VPC 萊迪目標群組位於相同的 VPC 中。
- 您可以在應用程式負載平衡器上使用 HTTPS 接聽程式來終止 TLS，但前提是 VPC 萊迪思服務使用與負載平衡器相同的 SSL/TLS 憑證時才能終止 TLS。
- 若要在`X-Forwarded-For`要求標頭中保留 VPC Radis 服務的用戶端 IP，您必須`routing.http.xff_header_processing.mode`將 `Preserve` Application Load Balancer 的屬性設定為。如果值為`Preserve`，負載平衡器會在 HTTP 要求中保留標`X-Forwarded-For`頭，並將其傳送至目標而不進行任何變更。如需詳細資訊，請參閱應用程式負載平衡器使用者指南中的 X-For ward For。

如需詳細資訊，請參閱應用程式負載平衡器使用指南中的建立應用程式負載平衡器。

步驟 1：建立 ALB 類型的目標群組

請使用下列程序來建立目標群組。請注意，VPC 萊迪思不支援 ALB 目標群組的健康狀態檢查。不過，您可以為 Application Load Balancer 的目標群組設定健全狀況檢查。如需詳細資訊，請參閱《應用程式負載平衡器使用者指南》中的目標群組健全狀況。

若要建立目標群組

1. 前往 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在功能窗格的「VPC 格子」下，選擇「目標群組」。
3. 選擇 Create target group (建立目標群組)。
4. 在 [指定目標群組詳細資訊] 頁面的 [基本組態] 下，選擇 [Ap plication Load Balancer] 作為目標類型
5. 針對 Target group name (目標群組名稱)，輸入目標群組的名稱。
6. 對於 Protocol (通訊協定)，請選擇 **HTTP** 或 **HTTPS**。目標群組通訊協定必須符合內部「Application Load Balancer」之監聽器的協定。
7. 在連接埠中，指定目標群組的連接埠。此連接埠必須符合內部 Application Load Balancer 的監聽器連接埠。您也可以在內部 Application Load Balancer 上新增監聽器連接埠，以符合您在此指定的目標群組連接埠。
8. 對於 VPC，請選取您在建立內部 Application Load Balancer 時選取的相同虛擬私人雲端 (VPC)。這應該是包含您的 VPC 格子資源的 VPC。
9. 對於通訊協定版本，請選擇 Application Load Balancer 支援的通訊協定版本。

10. (選擇性) 新增任何必要的標籤。
11. 選擇下一步。

步驟 2：將 Application Load Balancer 註冊為目標

您可以立即或稍後將負載平衡器註冊為目標。

將應用程式負載平衡器註冊為目標

1. 選擇立即註冊。
2. 對於 Ap plication Load Balancer，請選擇您的內部 Application Load Balancer
3. 對於「連接埠」，請保留預設值或視需要指定其他連接埠。此連接埠必須符合應用程式負載平衡器上現有的接聽程式連接埠。如果您在沒有相符連接埠的情況下繼續，流量將無法到達應用程式負載平衡器。
4. 選擇 Create target group (建立目標群組)。

通訊協定版本

根據預設，服務會使用 HTTP/1.1 將要求傳送至目標。您可以使用通訊協定版本，使用 HTTP/2 或 gRPC 將請求傳送至目標。

下表摘要說明請求通訊協定與目標群組通訊協定版本組合的結果。

請求通訊協定	通訊協定版本	結果
HTTP/1.1	HTTP/1.1	Success (成功)
HTTP/2	HTTP/1.1	Success (成功)
gRPC	HTTP/1.1	錯誤
HTTP/1.1	HTTP/2	錯誤
HTTP/2	HTTP/2	Success (成功)
gRPC	HTTP/2	如果目標支援 gRPC，則成功
HTTP/1.1	gRPC	錯誤

請求通訊協定	通訊協定版本	結果
HTTP/2	gRPC	如果是 POST 請求，則成功
gRPC	gRPC	Success (成功)

gRPC 通訊協定版本的考量事項

- 唯一支援的接聽程式通訊協定是 HTTPS。
- 支援的目標類型僅為 `INSTANCE` 和 `IP`。
- 此服務會剖析 gRPC 要求，並根據套件、服務和方法，將 gRPC 呼叫路由至適當的目標群組。
- 您無法使用 Lambda 函數做為目標。

HTTP/2 通訊協定版本的考量事項

- 唯一支援的接聽程式通訊協定是 HTTPS。您可以為目標群組通訊協定選擇 HTTP 或 HTTPS。
- 唯一支援的接聽程式規則是轉寄和固定回應。
- 支援的目標類型僅為 `INSTANCE` 和 `IP`。
- 該服務支持從客戶端流式傳輸。此服務不支援串流至目標。

VPC 格子目標群組的標籤

標籤可幫助您以不同的方式來將目標群組分類，例如，根據目的、擁有者或環境。

您可以在每個目標群組中加入多個標籤。每個目標群組的標籤索引鍵必須是唯一的。如果所新增的標籤，其索引鍵已經和目標群組具有關聯，則此動作會更新該標籤的值。

當您使用完標籤之後，可以將其移除。

限制

- 每一資源標籤數上限：50
- 索引鍵長度上限：127 個 Unicode 字元
- 數值長度上限：255 個 Unicode 字元
- 標籤鍵與值皆區分大小寫。允許的字元包括可用 UTF-8 表示的英文字母、空格和數字，還有以下特殊字元：+ - = . _ : / @。不可使用結尾或前方空格。

- 請勿在標籤名稱或值中使用aws:前置詞，因為它已保留供 AWS 使用。您不可編輯或刪除具此字首的標籤名稱或值。具此字首的標籤，不算在受資源限制的標籤計數內。

使用主控台來更新目標群組的標籤

1. 前往 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在功能窗格的「VPC 格子」下，選擇「目標群組」。
3. 選取目標群組的名稱，以開啟其詳細資訊頁面。
4. 選擇 Tags (標籤) 索引標籤。
5. 若要新增標籤，請選擇「新增標籤」，然後輸入標籤關鍵字和標籤值。若要新增另一個標籤，請再次選擇「新增標籤」。當您完成新增標籤的作業時，請選擇 Save changes (儲存變更)。
6. 若要刪除標記，請選取標記的核取方塊，然後選擇「刪除」。出現確認提示時，請輸入 **confirm**，然後選擇 Delete (刪除)。

若要使用更新目標群組的標記 AWS CLI

使用標籤資源和無標記資源命令。

刪除目標群組

如果沒有任何接聽程式規則的轉送動作參照某目標群組，即可刪除該目標群組。刪除目標群組不會影響透過該目標群組登錄的目標。如果不再需要註冊的 EC2 執行個體，則可以停止或終止它。

使用主控台來刪除目標群組

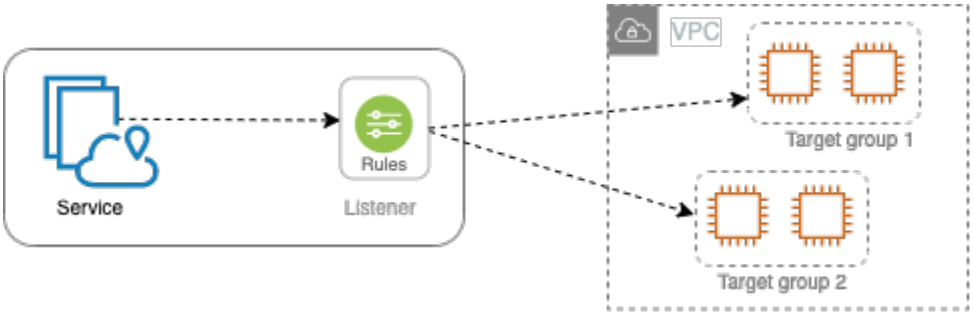
1. 前往 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 [目標群組]。
3. 選取目標群組的核取方塊，然後選擇動作，刪除。
4. 出現確認提示時，請輸入 **confirm**，然後選擇 Delete (刪除)。

若要使用刪除目標群組 AWS CLI

使用 delete-target-group 命令。

適用於 VPC 萊迪思服務的接聽程式

在開始使用 VPC Latters 服務之前，您必須新增一或多個接聽程式。接聽程式是檢查連線請求的程序，必須使用您已設定的通訊協定與連接埠。您為監聽器定義的規則會決定服務如何將要求路由傳送至其註冊目標。



目錄

接聽程式組態

接聽程式支援下列通訊協定與連接埠：

- Protocols (通訊協定)：HTTP、HTTPS
- Ports (連接埠)：1-65535

如果接聽程式通訊協定為 HTTPS，則 VPC 萊迪斯將佈建和管理與 VPC 格子產生的 FQDN 相關聯的 TLS 憑證。VPC 晶格在 HTTP/1.1 和 HTTP/2 上支援 TLS。當您使用 HTTPS 接聽程式設定服務時，VPC 萊迪會使用應用程式層通訊協定交涉 (ALPN) 自動判斷 HTTP 通訊協定。如果不存在 ALPN，則 VPC 晶格預設為 HTTP/1.1。

VPC 晶格可以監聽 HTTP，HTTPS，HTTP/1.1 和 HTTP/2，並在任何這些協議和版本的目標進行通信。我們不要求偵聽器和目標群組通訊協定相符。VPC 萊迪思管理協議和版本之間升級和降級的整個過程。如需詳細資訊，請參閱 通訊協定版本。

VPC 格子不支援 WebSockets。

建立接聽程式

您可以為您的 VPC 萊迪思服務建立接聽程式。建立監聽器時，您必須指定名稱、預設動作和通訊協定。偵聽程式隨附預設規則。您也可以為接聽程式建立其他規則。

使用主控台建立監聽器

- the section called “新增 HTTP 接聽程式 ”
- the section called “新增 HTTPS 接聽程式”
- the section called “新增規則”

使用建立監聽器 AWS CLI

使用建立接聽程式和建立規則命令。

適用於 VPC 晶格服務的 HTTP 接聽程式

接聽程式是檢查連線請求的程序。您可以在建立 VPC 萊迪思服務時定義接聽程式。您可以隨時將接聽程式新增至您的服務。

此頁面中的資訊可協助您建立服務的 HTTP 監聽器。如需為服務建立 HTTPS 接聽程式的相關資訊，請參閱HTTPS 接聽程式。

必要條件

- 若要將轉寄動作新增至預設接聽程式規則，您必須指定可用的 VPC Ladds 目標群組。如需詳細資訊，請參閱 建立 VPC 格子目標群組。
- 您可以在多個監聽器中指定相同的目標群組，但這些監聽器必須屬於相同的服務。若要將目標群組與 VPC Latess 服務搭配使用，您必須確認其未被任何其他 VPC Latters 服務的接聽程式使用。

新增 HTTP 接聽程式

您可以隨時將偵聽程式和規則新增至您的服務。您可以使用協定和連接埠來設定監聽器，以便從屬端與服務之間的連線，以及用於預設監聽器規則的 VPC Ligess 目標群組。如需詳細資訊，請參閱 接聽程式組態。

使用主控台新增 HTTP 接聽程式

1. 前往 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在功能窗格的 VPC 格子下，選擇 [服務]。
3. 選取服務名稱以開啟其詳細資訊頁面。
4. 在「路由」頁籤上，選擇「新增監聽器」。
5. 對於「監聽器名稱」，您可以提供自訂監聽器名稱，或使用監聽器的協定和連接埠作為監聽器名稱。您指定的自訂名稱最多可包含 63 個字元，而且帳戶中的每個服務都必須是唯一的。有效字元包括 a-z、0-9 和連字號 (-)。您不能使用連字號作為第一個或最後一個字元，或緊接在其他連字號之後。您無法在建立名稱之後變更名稱。
6. 在「通訊協定：連接埠」中，選擇 HTTP 並輸入通訊埠號碼。
7. 對於「預設」動作，請選擇要接收流量的 VPC Latters 目標群組，然後選擇要指派給此目標群組的權重。您指派給目標群組的加權會設定其接收流量的優先順序。例如，如果兩個目標群組的權重相同，則每個目標群組會接收一半的流量。如果您只指定了一個目標群組，則 100% 的流量會傳送至一個目標群組。

   您可以選擇性地為預設動作新增其他目標群組。選擇 [新增動作]，然後選擇目標群組並指定其權重。
8. (選擇性) 若要新增其他規則，請選擇「新增規則」，然後輸入規則的名稱、優先順序、條件和動作。

   您可以為每個規則指定介於 1 到 100 之間的優先順序號碼。接聽程式不能擁有多個優先順序相同的規則。依優先順序評估規則，從最低值到最高值。預設規則最後評估。如需詳細資訊，請參閱 接聽程式規則。
9. (選擇性) 若要新增標記，請展開 [監聽程式標籤]，選擇 [新增標記]，然後輸入標籤鍵和標記值。
10. 檢閱您的組態，然後選擇 [新增]。

若要使用 AWS CLI

使用 create- listen 命令建立具有預設規則的監聽器，使用建立規則命令建立其他監聽器規則。

適用於 VPC 格子服務的 HTTPS 接聽程式

接聽程式是檢查連線請求的程序。您可以在建立服務時定義接聽程式。您可以隨時將接聽程式新增至您在 VPC Latds 中的服務。

您可以建立 HTTPS 接聽程式，該接聽程式使用 TLS 1.2 版直接終止與 VPC 萊格的 HTTPS 連線。VPC 萊迪思將佈建和管理與 VPC 格子產生的完整網域名稱 (FQDN) 相關聯的 TLS 憑證。VPC 晶格在 HTTP/1.1 和 HTTP/2 上支援 TLS。當您使用 HTTPS 接聽程式設定服務時，VPC 萊迪思會透過應用程式層通訊協定交涉 (ALPN) 自動判斷 HTTP 通訊協定。如果不存在 ALPN，則 VPC 晶格預設為 HTTP/1.1。

VPC 萊迪思使用多租戶架構，這意味著它可以在同一個端點上託管多個服務。VPC 格子會針對每個用戶端要求使用具有伺服器名稱指示 (SNI) 的 TLS。

VPC 晶格可以監聽 HTTP，HTTPS，HTTP/1.1 和 HTTP/2，並在任何這些協議和版本的目標進行通信。這些監聽器和目標群組組態不需要相符。VPC 萊迪思管理協議和版本之間升級和降級的整個過程。如需詳細資訊，請參閱 通訊協定版本。

此頁面上的資訊可協助您為服務建立 HTTPS 接聽程式。如需為服務建立 HTTP 接聽程式的相關資訊，請參閱監聽程式。

內容

安全政策

VPC 格子使用的安全性原則是 TLSv1.2 通訊協定和 SSL/TLS 加密清單的組合。該協議在客戶端和服務器之間建立了安全連接，並有助於確保客戶端和您在 VPC Latters 中的服務之間傳遞的所有數據都是私有的。隨碼是一項加密演算法，使用加密金鑰來建立編碼的訊息。通訊協定使用多個密碼來加密資料。在連線交涉過程中，用戶端和 VPC Latters 會依偏好順序顯示各自支援的密碼和通訊協定清單。在預設情況下，將針對安全連線選取伺服器清單上符合任何用戶端加密的第一個加密。

VPC 格子會依此偏好順序使用 TLSv1.2 通訊協定和下列 SSL/TLS 密碼：

- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-GCM-SHA256

- ECDHE-ECDSA-AES128-SHA
- ECDHE-RSA-AES128-SHA
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-SHA
- ECDHE-ECDSA-AES256-SHA
- AES128-GCM-SHA256
- AES128-SHA
- AES256-GCM-SHA384
- AES256-SHA

ALPN 政策

應用程式層通訊協定交涉 (ALPN) 是在初始 TLS 握手打招呼訊息時傳送的 TLS 延伸模組。ALPN 使應用程式層能夠協商哪些通訊協定的使用透過安全的連接 (如 HTTP/1 和 HTTP/2) 來進行。

當用戶端啟動 ALPN 連線時，VPC 萊迪思服務會比較用戶端 ALPN 偏好設定清單與其 ALPN 政策。如果用戶端支援來自 ALPN 原則的通訊協定，則 VPC 萊迪思服務會根據 ALPN 政策的偏好設定清單建立連線。否則，本服務將不使用 ALPN。

VPC 萊迪思支援以下 ALPN 政策：

`HTTP2Preferred`

更喜歡 HTTP/2 而不是 HTTP/1.1。ALPN 偏好設定清單為 H2、HTTP /1.1。

新增 HTTPS 接聽程式

您可以使用協定和連接埠來設定監聽器，以便從屬端與服務之間的連線，以及預設監聽器規則的目標群組。如需詳細資訊，請參閱 接聽程式組態。

必要條件

- 若要將轉寄動作新增至預設接聽程式規則，您必須指定可用的 VPC Ladds 目標群組。如需詳細資訊，請參閱 建立 VPC 格子目標群組。

- 您可以在多個監聽器中指定相同的目標群組，但這些監聽器必須屬於相同的 VPC Ligess 服務。若要將目標群組與 VPC Latess 服務搭配使用，您必須確認其未被任何其他 VPC Latters 服務的接聽程式使用。
- 您可以使用 VPC 萊迪思提供的證書或將自己的證書導入到 AWS Certificate Manager. 如需詳細資訊，請參閱 the section called “自攜”。

使用主控台新增 HTTPS 接聽程式

1. 前往 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在功能窗格的 VPC 格子下，選擇 [服務]。
3. 選取服務名稱以開啟其詳細資訊頁面。
4. 在「路由」頁籤上，選擇「新增監聽器」。
5. 對於監聽器名稱，您可以提供自訂監聽器名稱，或使用監聽器的協定和連接埠作為監聽器名稱。您指定的自訂名稱最多可包含 63 個字元，而且帳戶中的每個服務都必須是唯一的。有效字元包括 a-z、0-9 和連字號 (-)。您不能使用連字號作為第一個或最後一個字元，或緊接在其他連字號之後。建立監聽器之後，就無法變更它的名稱。
6. 在「通訊協定：連接埠」中，選擇 HTTPS 並輸入通訊埠號碼。
7. 對於「預設」動作，請選擇要接收流量的 VPC Latters 目標群組，然後選擇要指派給此目標群組的權重。您指派給目標群組的加權會設定其接收流量的優先順序。例如，如果兩個目標群組的權重相同，則每個目標群組會接收一半的流量。如果您只指定了一個目標群組，則 100% 的流量會傳送至一個目標群組。

   您可以選擇性地為預設動作新增其他目標群組。選擇 [新增動作]，然後選擇目標群組並指定其權重。
8. (選擇性) 若要新增其他規則，請選擇「新增規則」，然後輸入規則的名稱、優先順序、條件和動作。

   您可以為每個規則指定介於 1 到 100 之間的優先順序號碼。接聽程式不能擁有多個優先順序相同的規則。依優先順序評估規則，從最低值到最高值。預設規則最後評估。如需詳細資訊，請參閱接聽程式規則。
9. (選擇性) 若要新增標記，請展開 [監聽程式標籤]，選擇 [新增標記]，然後輸入標籤鍵和標記值。
10. 對於 HTTPS 接聽程式憑證設定，如果您在建立服務時未指定自訂網域名稱，則 VPC Ligess 會自動產生 TLS 憑證，以保護流經監聽器的流量安全。

如果您使用自訂網域名稱建立服務，但並未指定相符的憑證，則現在可以從 Custom SSL/TLS 憑證中選擇憑證來執行此操作。否則，您在建立服務時指定的憑證就會被選擇。

11. 檢閱您的組態，然後選擇 [新增]。

若要使用 AWS CLI

使用 create- listen 命令建立具有預設規則的監聽器，使用建立規則命令建立其他監聽器規則。

您的 VPC 格子服務的接聽程式規則

每個接聽程式都有一個預設規則和您可以定義的其他規則。每個規則由優先順序、一或多個動作及一或多個條件組成。您可以隨時新增或編輯規則。

目錄

預設規則

建立接聽程式時，您會定義預設規則的預設動作。預設規則不能有條件。如果沒有符合任何接聽程式規則的條件，則會執行預設規則的動作。

規則優先順序

每個規則具有優先順序。依優先順序評估規則，從最低值到最高值。預設規則最後評估。您可以隨時變更非預設規則的優先順序。您無法變更預設規則的優先順序。

規則動作

VPC 萊迪思服務的接聽程式支援轉寄動作和固定回應動作。

轉送動作

您可以使用forward動作將請求路由到一個或多個 VPC 萊迪目標群組。如果您為一個 forward 動作指定多個目標群組，則必須為每個目標群組指定加權。每個目標群組權重為介於 0 到 999 之間的值。符合加權目標群組之監聽程式規則的請求，會根據其權重分配到這些目標群組。例如，如果您指定兩個目標群組，每個目標群組的權重為 10，則每個目標群組都會收到一半的請求。如果您指定兩個目標群組，一個權重為 10，另一個權重為 20，則權重為 20 的目標群組接收的請求數量是另一個目標群組的兩倍。

固定回應動作

您可以使用 fixed-response 動作來捨棄用戶端請求，並傳回自訂 HTTP 回應。您可以使用此動作來傳回 404 回應碼。

Example 範例固定回應動作 AWS CLI

您可以在建立或更新規則時指定動作。下列動作會傳送具有指定狀態碼的固定回應。

```
"action": {
    "fixedResponse": {
        "statusCode": 404
},
```

規則條件

每個規則條件具有類型和組態資訊。滿足規則的條件時，即會執行它的動作。

以下是規則支援的符合條件：

頭匹配

路由是基於每個請求的 HTTP 標頭。您可以使用 HTTP 標頭條件來設定規則，以根據請求的 HTTP 標頭來路由傳送請求。您可以指定標準或自訂 HTTP 標頭欄位的名稱。標題名稱和匹配評估不區分大小寫。您可以透過開啟區分大小寫來變更此設定。標頭名稱中不支援萬用字元。前綴，確切和包含匹配支持頭匹配。

方法比對

路由是基於每個請求的 HTTP 請求方法。

您可以使用 HTTP 請求方法條件來設定規則，以根據請求的 HTTP 請求方法來路由傳送請求。您可以指定標準或自訂 HTTP 方法。該方法匹配是區分大小寫的。方法名稱必須完全相符。不支援萬用字元。

路徑匹配

路由是以要求 URL 中的路徑模式相符為基礎。

您可以使用路徑條件來定義根據要求中的 URL 路由要求的規則。不支援萬用字元。支持路徑上的前綴和完全匹配。

新增規則

您可以隨時新增監聽程式規則。

使用主控台新增監聽器規則

1. 前往 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在功能窗格的 VPC 格子下，選擇 [服務]。
3. 選取服務名稱以開啟其詳細資訊頁面。
4. 在「路由」頁籤上，選擇「編輯監聽器」。
5. 展開監聽器規則，然後選擇新增規則。
6. 針對 Rule name (規則名稱)，輸入規則的名稱。
7. 在「優先順序」中輸入介於 1 到 100 之間的優先順序。依優先順序評估規則，從最低值到最高值。預設規則最後評估。
8. 在「條件」中，輸入路徑符合條件的路徑樣式。每個字串的大小上限為 200 個字元。比較不區分大小寫。不支援萬用字元。

   若要新增標頭比對或方法比對規則條件，請使用 AWS CLI 或 AWS SDK。
9. 在 [動作] 中，選擇 VPC 格子目標群組。
10. 選擇儲存變更。

若要使用新增規則 AWS CLI

使用「建立規則」指令。

更新規則

您可以隨時更新監聽器規則。您可以修改其優先順序、條件、目標群組以及每個目標群組的權重。您無法修改規則的名稱。

使用主控台更新監聽器規則

1. 前往 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在功能窗格的 VPC 格子下，選擇 [服務]。
3. 選取服務名稱以開啟其詳細資訊頁面。
4. 在「路由」頁籤上，選擇「編輯監聽器」。
5. 視需要修改規則優先順序、條件和動作。
6. 檢閱更新，然後選擇 [儲存變更]。

若要使用更新規則 AWS CLI

使用更新規則命令。

刪除規則

您可以隨時刪除監聽器的非預設規則。您無法刪除接聽程式的預設規則。刪除監聽器時，其所有規則都會被刪除。

使用主控台刪除監聽器規則

1. 前往 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在功能窗格的 VPC 格子下，選擇 [服務]。
3. 選取服務名稱以開啟其詳細資訊頁面。
4. 在「路由」頁籤上，選擇「編輯監聽器」。
5. 尋找規則，然後選擇「移除」。
6. 選擇儲存變更。

若要使用刪除規則 AWS CLI

使用 delete-rule 命令。

更新接聽程式

建立監聽器之後，您可以取代預設動作的目標群組。您也可以將目標群組新增至預設動作，並將權重指派給目標群組。您無法更新監聽器名稱、監聽器通訊協定或監聽器連接埠。

使用主控台更新監聽器

1. 前往 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在功能窗格的 VPC 格子下，選擇 [服務]。
3. 選取服務名稱以開啟其詳細資訊頁面。
4. 在「路由」頁籤上，選擇「編輯監聽器」。
5. 對於「預設」動作，您可以視需要更新目標群組或權重。
6. 若要新增其他目標群組，請選擇 [新增動作]，然後選擇目標群組並指定其權重。
7. 您也可以新增、編輯或刪除監聽器規則。如需詳細資訊，請參閱 接聽程式規則。
8. 檢閱您的更新，然後選擇 [儲存變更]。

使用更新監聽器的預設動作 AWS CLI

使用更新偵聽器命令。

刪除接聽程式

您可隨時刪除接聽程式。刪除監聽器時，其所有規則都會自動刪除。

使用主控台刪除接聽程式

1. 前往 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在功能窗格的 VPC 格子下，選擇 [服務]。
3. 選取服務名稱以開啟其詳細資訊頁面。
4. 在路由索引標籤上，選擇刪除監聽器。
5. 出現確認提示時，請輸入 **`confirm`**，然後選擇 Delete (刪除)。

使用刪除監聽器 AWS CLI

使用 delete-listener 命令。

分享您的 VPC 萊迪思資源

Amazon VPC 萊迪思與 AWS Resource Access Manager (AWS RAM) 整合以啟用資源共用。 AWS RAM是一項服務，可讓您與其他人AWS 帳戶或通過AWS Organizations共享某些 VPC 萊迪思資源。您可以透過 AWS RAM 建立資源共享，以分享您擁有的資源。資源共享指定要分享的資源，以及共用它們的消費者。消費者可以包括：

- 具體在其組織AWS 帳戶內部或外部AWS Organizations。
- 其組織內部的組織單位AWS Organizations。
- 中的整個組織AWS Organizations。

如需有關 AWS RAM 的詳細資訊，請參閱《使用者指南》AWS RAM。

目錄

共用 VPC 格子資源的先決條件

- 要共享資源，您必須在AWS 帳戶. 這表示必須在您的帳戶中配置或佈建資源。您無法共享已與您共享的資源。
- 若要與中的組織或組織單位共用資源AWS Organizations，您必須啟用與共用AWS Organizations。如需詳細資訊，請參閱《AWS RAM使用指南》AWS Organizations中的「啟用資源共用」。

分享 VPC 格子資源

若要共用資源，請先使用建立資源共用AWS Resource Access Manager。資源共用指定要共用的資源、共用資源的用戶，以及主參與者可以執行的動作。

當您與其他帳戶共用您擁有的 VPC 萊迪思資源時AWS 帳戶，您可以讓這些帳戶將其資源與您帳戶中的資源建立關聯。當您針對共用資源建立關聯時，我們會在資源擁有者帳戶中產生 Amazon 資源名稱

(ARN)，並在建立關聯的帳戶中產生一個 ARN。如此一來，資源擁有者和建立關聯的帳號都可以刪除關聯。

如果您是組織的一員，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獲得共用資源的存取權。否則，取用者會收到加入資源共用的邀請，並在接受邀請後授予共用資源的存取權。

考量事項

- 您可以共用兩種類型的 VPC 萊迪思資源：服務網路和服務。
- 您可以與任AWS 帳戶何人共享您的 VPC 萊迪思資源。
- 您無法與個別 IAM 使用者和角色共用您的 VPC 萊迪思資源。
- VPC 萊迪思同時支援服務網路和服務的客戶管理權限。

使用 VPC 萊迪思主控台共用您擁有的資源

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在功能窗格的 VPC Latts 下，選擇 [服務] 或 [服務網路]。
3. 選擇要開啟其詳細資料頁面的資源名稱，然後從 [共用] 索引標籤中選擇 [共用服務] 或 [共用服務網路]。
4. 從「資AWS RAM源共用」中選擇資源共用。若要建立資源共用，請選擇 [在 RAM 主控台中建立資源共用]。
5. 選擇共用服務或共用服務網路。

使用AWS RAM主控台共用您擁有的資源

請使用《使用AWS RAM者指南》中所述的建立資源共用中所述的程序。

若要共用您所擁有的資源，請使用 AWS CLI

使用 associate-resource-share 命令。

停止共用 VPC 格子資源

若要停止共用您擁有的 VPC Laters 資源，您必須將其從資源共用中移除。停止共用資源後，現有的關聯仍會持續存在。不允許與先前共用資源的新關聯。當資源擁有者或關聯擁有者刪除關聯時，會從這兩個帳號中刪除該關聯。如果帳號擁有者想要離開資源共用，則必須要求資源共用的擁有者移除該帳號。

若要停止共用您使用 VPC 萊迪思主控台所擁有的資源

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在功能窗格的 VPC Latts 下，選擇 [服務] 或 [服務網路]。
3. 選擇要開啟其詳細資訊頁面的資源名稱。
4. 在 [共用] 索引標籤上，選取資源共用的核取方塊，然後選擇 [移除]。

若要停止使用AWS RAM主控台共用您擁有的資源

請參閱《AWS RAM使用指南》中的更新資源共用。

若要停止共用您所擁有的資源，請使用 AWS CLI

使用 disassociate-resource-share 命令。

職責和權限

使用共用 VPC 萊迪思資源時，下列職責與權限適用。

資源擁有者

- 服務網路擁有者無法修改取用者所建立的服務。
- 服務網路擁有者無法刪除取用者所建立的服務。
- 服務網路擁有者可以描述服務網路的所有服務關聯。
- 服務網路擁有者可以取消與服務網路相關聯的任何服務的關聯，無論是誰建立關聯。
- 服務網路擁有者可以描述服務網路的所有 VPC 關聯。
- 服務網路擁有者可以取消消用戶與服務網路相關聯的任何 VPC 的關聯。
- 服務擁有者可以描述與服務的所有網路關聯。
- 服務擁有者可以取消服務與其相關聯之任何服務網路的關聯。
- 只有建立關聯的帳戶可以更新服務網路與 VPC 之間的關聯。

資源消費者

- 消費者無法刪除他們未建立的服務。
- 消費者只能取消與服務網路相關聯之服務的關聯。

- 消費者和網路擁有者可以描述服務網路與服務之間的所有關聯。
- 消費者無法擷取他們不擁有的服務的服務資訊。
- 消費者可以描述與共享服務網絡的所有服務關聯。
- 消費者可以將服務與共享服務網絡相關聯。
- 消費者可以看到與共用服務網路的所有 VPC 關聯。
- 取用者可以將 VPC 與共用服務網路建立關聯。
- 取用者只能取消與服務網路相關聯的 VPC 的關聯。
- 共用服務的消費者無法將服務與他們不擁有的服務網路產生關聯。
- 共用服務網路的使用者無法關聯他們不擁有的 VPC 或服務。
- 消費者可以描述與他們共享的服務或服務網絡。
- 如果兩個資源都與他們共享，則消費者無法關聯兩個資源。

跨帳戶事件

當資源擁有者和取用者對共用資源執行動作時，這些動作會記錄為中AWS CloudTrail的跨帳號事件。

`CreateServiceNetworkServiceAssociationBySharee`

當資源取用者呼叫共用資源時，傳送給資源CreateServiceNetworkServiceAssociation擁有者。如果呼叫者擁有服務，則會將事件傳送給服務網路的擁有者。如果呼叫者擁有服務網路，則會將事件傳送給服務的擁有者。

`CreateServiceNetworkVpcAssociationBySharee`

當資源消費者CreateServiceNetworkVpcAssociation使用共用服務網路呼叫時，傳送給資源擁有者。

`DeleteServiceNetworkServiceAssociationByOwner`

當資源擁有者DeleteServiceNetworkServiceAssociation使用共用資源呼叫時，傳送給關聯擁有者。如果呼叫者擁有服務，則會將事件傳送給服務網路關聯的擁有者。如果呼叫者擁有服務網路，則會將事件傳送給服務關聯的擁有者。

`DeleteServiceNetworkServiceAssociationBySharee`

當資源取用者呼叫共用資源時，傳送給資源DeleteServiceNetworkServiceAssociation擁有者。如果呼叫者擁有服務，則會將事件傳送給服務網路的擁有者。如果呼叫者擁有服務網路，則會將事件傳送給服務的擁有者。

`DeleteServiceNetworkVpcAssociationByOwner`

當資源擁有者DeleteServiceNetworkVpcAssociation使用共用服務網路呼叫時，傳送給關聯擁有者。

`DeleteServiceNetworkVpcAssociationBySharee`

當資源消費者DeleteServiceNetworkVpcAssociation使用共用服務網路呼叫時，傳送給資源擁有者。

`GetServiceBySharee`

當資源取用者呼叫共用服務時，傳送給資源GetService擁有者。

`GetServiceNetworkBySharee`

當資源消費者GetServiceNetwork使用共用服務網路呼叫時，傳送給資源擁有者。

`GetServiceNetworkServiceAssociationBySharee`

當資源取用者呼叫共用資源時，傳送給資源GetServiceNetworkServiceAssociation擁有者。如果呼叫者擁有服務，則會將事件傳送給服務網路的擁有者。如果呼叫者擁有服務網路，則會將事件傳送給服務的擁有者。

`GetServiceNetworkVpcAssociationBySharee`

當資源消費者GetServiceNetworkVpcAssociation使用共用服務網路呼叫時，傳送給資源擁有者。

以下是事件的範例項`CreateServiceNetworkServiceAssociationBySharee`目。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown"
    },
    "eventTime": "2023-04-27T17:12:46Z",
    "eventSource": "vpc-lattice.amazonaws.com",
    "eventName": "CreateServiceNetworkServiceAssociationBySharee",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "vpc-lattice.amazonaws.com",
    "userAgent": "ec2.amazonaws.com",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "callerAccountId": "111122223333"
```

```
    },
    "requestID": "ddabb0a7-70c6-4f70-a6c9-00cbe8a6a18b",
    "eventID": "bd03cdca-7edd-4d50-b9c9-eaa89f4a47cd",
    "readOnly": false,
    "resources": [
        {
            "accountId": "123456789012",
            "type": "AWS::VpcLattice::ServiceNetworkServiceAssociation",
            "ARN": "arn:aws:vpc-
lattice:region:123456789012:servicenetworkserviceassociation/snsa-0d5ea7bc72EXAMPLE"
        }
    ],
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

Amazon VPC 格子中的安全性

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。

您負責維護在此基礎設施上託管內容的控制權。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。若要了解適用於 Amazon VPC 萊迪思的合規計劃，請參閱合規計劃AWS 服務範圍內的合規計劃AWS服務。
- 雲端安全性 — 您必須負責維持對此基礎架構上託管之內容的控制權。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 VPC 萊迪思時應用共同的責任模型。以下主題說明如何設定 VPC 萊迪思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 服務來幫助您監控和保護您的 VPC 萊迪思資源。

目錄

管理您服務的存取

根據預設，VPC 萊迪思是安全的，因為您必須明確了解哪些服務可以提供存取 VPC 以及使用哪些 VPC。對於多帳戶案例，您可以使AWS Resource Access Manager用跨帳戶界限共用資源。VPC 萊迪思提供了一個架構，可讓您在網路的多層實作defense-in-depth策略。

- 第一層 — 服務和 VPC 與服務網路的關聯。如果 VPC 或特定服務未與服務網路相關聯，則 VPC 中的用戶端將無法存取該服務。

- 第二層 — 為服務網路選購的網路層級安全性保護，例如安全群組和網路 ACL。透過使用這些功能，您可以允許存取 VPC 中的特定資源群組，而不是 VPC 中的所有資源。
- 第三層 — 可選的 VPC 格子身份驗證策略。您可以將身份驗證策略應用於服務網絡和個別服務。通常，服務網絡上的身份驗證策略由網絡或雲管理員操作，並且他們實施粗粒度授權。例如，僅允許來自中特定組織的已驗證請求 AWS Organizations。對於服務級別的身份驗證策略，通常服務所有者設置了精細的控件，這可能比在服務網絡級別應用的粗粒度授權更具限制性。

存取控制的方法

- 驗證政策
- 安全群組
- 網路 ACL

使用身份驗證策略控制服務的訪問

VPC 萊迪思身份驗證政策是您附加到服務網路或服務的 IAM 政策文件，用於控制指定的主體是否可以存取一組服務或特定服務。您可以將一個身份驗證策略附加到要控制訪問的每個服務網絡或服務。

驗證政策與 IAM 身分型政策不同。IAM 身分型政策會附加至 IAM 使用者、群組或角色，並定義這些身分可對哪些資源執行的動作。驗證政策附加到服務和服務網絡。為了授權成功，身份驗證策略和基於身份的策略都需要具有明確的 allow 語句。如需詳細資訊，請參閱 授權如何運作。

您可以使用 AWS CLI 和主控台來檢視、新增、更新或移除服務和服務網路上的驗證原則。使用時 AWS CLI，請記住您的命令會在為您的設定檔所 AWS 區域 設定的中執行。如果您想在不同區域中執行命令，則可變更設定檔的預設區域，或搭配 `--region` 參數使用命令。

目錄

要開始使用身份驗證策略，請按照以下步驟創建適用於服務網絡的身份驗證策略。對於不希望應用於其他服務的限制性更嚴格的權限，您可以選擇性地在單個服務上設置身份驗證策略。

使用驗證政策管理服務網路的存取

下列 AWS CLI 工作說明如何使用驗證原則來管理服務網路的存取。如需使用主控台的指示，請參閱VPC 格子中的服務網絡。

任務

- 將身份驗證策略添加到服務網絡
- 變更服務網路的驗證類型
- 從服務網絡中刪除身份驗證策略

將身份驗證策略添加到服務網絡

請按照本節中的步驟使 AWS CLI 用：

- 使用 IAM 在服務網路上啟用存取控制。
- 將身份驗證策略添加到服務網絡。如果未添加身份驗證策略，則所有流量都將收到拒絕訪問錯誤。

啟用存取控制並將驗證原則新增至新的服務網路

1. 若要在服務網路上啟用存取控制，以便它可以使用驗證原則，請使用create-service-network指令搭配--auth-type選項和值AWS_IAM。

   ```
   aws vpc-lattice create-service-network --name Name --auth-type AWS_IAM [--
   tags TagSpecification]
   ```

   如果成功，此命令傳回的輸出會類似如下。

   ```
   {
      "arn": "arn",
      "authType": "AWS_IAM",
      "id": "sn-0123456789abcdef0",
      "name": "Name"
   }
   ```

2. 使用命put-auth-policy令，指定要在其中添加身份驗證策略和要添加的身份驗證策略的服務網絡的ID。

例如，使用以下命令為具有 ID 的服務網絡創建身份驗證策略*sn-0123456789abcdef0*。

```
aws vpc-lattice put-auth-policy --resource-identifier sn-0123456789abcdef0 --
policy file://policy.json
```

使用 JSON 建立原則定義。如需詳細資訊，請參閱 身份驗證策略中的常見元素。

如果成功，此命令傳回的輸出會類似如下。

```
{
   "policy": "policy",
   "state": "Active"
}
```

啟用存取控制並將驗證原則新增至現有服務網路

1. 若要在服務網路上啟用存取控制，以便它可以使用驗證原則，請使用update-service-network指令搭配--auth-type選項和值AWS_IAM。

```
aws vpc-lattice update-service-network --service-network-
identifier sn-0123456789abcdef0 --auth-type AWS_IAM
```

如果成功，此命令傳回的輸出會類似如下。

```
{
   "arn": "arn",
   "authType": "AWS_IAM",
   "id": "sn-0123456789abcdef0",
   "name": "Name"
}
```

2. 使用命put-auth-policy令，指定要在其中添加身份驗證策略和要添加的身份驗證策略的服務網絡的ID。

```
aws vpc-lattice put-auth-policy --resource-identifier sn-0123456789abcdef0 --
policy file://policy.json
```

使用 JSON 建立原則定義。如需詳細資訊，請參閱 身份驗證策略中的常見元素。

如果成功，此命令傳回的輸出會類似如下。

```
{
   "policy": "policy",
   "state": "Active"
}
```

變更服務網路的驗證類型

若要停用服務網路的驗證原則

將指update-service-network令與--auth-type選項和值搭配使用NONE。

```
aws vpc-lattice update-service-network --service-network-
identifier sn-0123456789abcdef0 --auth-type NONE
```

如果您稍後需要再次啟用身份驗證策略，請運行此命令並為該--auth-type選項AWS_IAM指定。

從服務網絡中刪除身份驗證策略

從服務網路移除驗證政策

使用 delete-auth-policy 命令。

```
aws vpc-lattice delete-auth-policy --resource-identifier sn-0123456789abcdef0
```

如果您在將服務網絡的身份驗證類型更改為之前刪除身份驗證策略，則請求將失敗NONE。

使用身份驗證策略管理對服務的訪問

下列 AWS CLI 工作說明如何使用驗證原則來管理服務的存取權。如需使用主控台的指示，請參閱VPC格子的服務。

任務

- 將身份驗證策略添加到服務
- 更改服務的身份驗證類型
- 從服務中刪除身份驗證策略

將身份驗證策略添加到服務

請依照下列步驟使 AWS CLI 用：

- 使用 IAM 對服務啟用存取控制。
- 將身份驗證策略添加到服務。如果未添加身份驗證策略，則所有流量都將收到拒絕訪問錯誤。

啟用存取控制並將驗證原則新增至新服務

1. 若要對服務啟用存取控制，以便它可以使用驗證原則，請使用create-service指令搭配--auth-type選項和值AWS_IAM。

```
aws vpc-lattice create-service --name Name --auth-type AWS_IAM [--
tags TagSpecification]
```

如果成功，此命令傳回的輸出會類似如下。

```
{
   "arn": "arn",
   "authType": "AWS_IAM",
   "dnsEntry": {
      ...
   },
   "id": "svc-0123456789abcdef0",
   "name": "Name",
   "status": "CREATE_IN_PROGRESS"
}
```

2. 使用命put-auth-policy令，指定要在其中添加身份驗證策略和要添加的身份驗證策略的服務的 ID。

例如，使用下列命令為識別碼 *svc-* 0123456789abcdef0 的服務建立驗證原則。

```
aws vpc-lattice put-auth-policy --resource-identifier svc-0123456789abcdef0 --
policy file://policy.json
```

使用 JSON 建立原則定義。如需詳細資訊，請參閱 身份驗證策略中的常見元素。

如果成功，此命令傳回的輸出會類似如下。

```
{
```

```
   "policy": "policy",
   "state": "Active"
}
```

啟用存取控制並將驗證原則新增至現有服務

1. 若要對服務啟用存取控制，以便它可以使用驗證原則，請使用update-service指令搭配--auth-type選項和值AWS_IAM。

```
aws vpc-lattice update-service --service-identifier svc-0123456789abcdef0 --auth-
type AWS_IAM
```

如果成功，此命令傳回的輸出會類似如下。

```
{
   "arn": "arn",
   "authType": "AWS_IAM",
   "id": "svc-0123456789abcdef0",
   "name": "Name"
}
```

2. 使用命put-auth-policy令，指定要在其中添加身份驗證策略和要添加的身份驗證策略的服務的 ID。

```
aws vpc-lattice put-auth-policy --resource-identifier svc-0123456789abcdef0 --
policy file://policy.json
```

使用 JSON 建立原則定義。如需詳細資訊，請參閱 身份驗證策略中的常見元素。

如果成功，此命令傳回的輸出會類似如下。

```
{
   "policy": "policy",
   "state": "Active"
}
```

更改服務的身份驗證類型

若要停用服務的驗證原則

將指update-service令與--auth-type選項和值搭配使用NONE。

```
aws vpc-lattice update-service --service-identifier svc-0123456789abcdef0 --auth-type
 NONE
```

如果您稍後需要再次啟用身份驗證策略，請運行此命令並為該--auth-type選項AWS_IAM指定。

從服務中刪除身份驗證策略

從服務中刪除身份驗證策略

使用 delete-auth-policy 命令。

```
aws vpc-lattice delete-auth-policy --resource-identifier svc-0123456789abcdef0
```

如果您在將服務的 auth 類型更改為之前刪除了身份驗證策略，則請求將失敗NONE。

如果您啟用需要對服務進行身份驗證請求的身份驗證策略，則對該服務的任何請求都必須包含使用簽名版本 4（SIGv4）計算的有效請求簽名。如需詳細資訊，請參閱 簽章版本 4 驗證要求的範例。

身份驗證策略中的常見元素

VPC 萊迪思驗證政策使用與 IAM 政策相同的語法來指定。如需詳細資訊，請參閱 IAM 使用指南中的以身分識別為基礎的政策和以資源為基礎的政策。

身份驗證策略包含以下元素：

- 主體 — 允許存取陳述式中動作與資源的人員或應用程式。在驗證政策中，主體是身為此權限接收者的 IAM 實體。主體會驗證為 IAM 實體，以便向特定資源或資源群組發出請求，就像服務網路中的服務一樣。

  您必須在資源型政策中指定主體。主參與者可以包括帳戶、使用者、角色、同盟使用者或 AWS 服務。如需詳細資訊，請參閱 IAM 使用者指南中的 AWS JSON 政策元素：主體。
- 效果 — 指定主參與者要求特定動作時的效果。可以是 Allow 或 Deny。根據預設，當您使用 IAM 對服務或服務網路啟用存取控制時，主體沒有向服務或服務網路發出請求的權限。Allow因此，明確的會覆寫預設值。
- 動作 — VPC 格子支援一個動作。vpc-lattice-svcs:Invoke此權限允許指定的主體對Resources元素中指定的資源執行要求。
- 資源 — 受動作影響的服務。
- 條件 — 條件是選擇性的。您可以使用它們來控制政策的生效時間。

建立和管理身份驗證政策時，您可能需要使用 IAM 政策產生器。

需求

JSON 中的策略不得包含換行符或空行。

身份驗證策略的資源格式

您可以通過創建使用具有模式的匹配<serviceARN>/<path>模式的身份驗證策略來限制對特定資源的Resource訪問，如以下示例所示。

身份驗證策略的資源示例

通訊協定	範例
HTTP	• "Resource": "arn:aws:vpc-lattice:us-west-2:1234567890:service/svc-0123456789abcdef0/rates" • "Resource": "*/rates" • "Resource": "*/*"
gRPC	• "Resource": "arn:aws:vpc-lattice:us-west-2:1234567890:service/svc-0123456789abcdef0/api.parking/GetRates" • "Resource": "arn:aws:vpc-lattice:us-west-2:1234567890:service/svc-0123456789abcdef0/api.parking/*" • "Resource": "arn:aws:vpc-lattice:us-west-2:1234567890:service/svc-0123456789abcdef0/*"

使用下列 Amazon 資源名稱 (ARN) 資源格式<serviceARN>：

```
arn:aws:vpc-lattice:region:account-id:service/service-id
```

例如：

```
"Resource": "arn:aws:vpc-lattice:us-west-2:123456789012:service/svc-0123456789abcdef0"
```

可以在身份驗證策略中使用的條件密鑰

訪問可以通過身份驗證策略的條件元素中的條件鍵進一步控制。根據通訊協定以及要求是使用簽章版本 4 (SIGv4) 還是匿名簽署，這些條件金鑰可供評估。如需詳細資訊，請參閱服務授權參考中的 Amazon VPC 萊迪思服務的條件金鑰。

需求

條件金鑰名稱有區分大小寫。

身份驗證策略的條件密鑰

條件索引鍵	描述	範例	可用於匿名（未經身份驗證的）呼叫者？	適用於 gRPC 嗎？
vpc-lattice-svcs:Port	根據要求的服務連接埠篩選存取	80	是	是
vpc-lattice-svcs:RequestMethod	依請求的方法來篩選存取權	GET	是	總是張貼
vpc-lattice-svcs:RequestHeader/ *header-name* : *value*	依請求標頭中的標頭名稱/值對來篩選存取權	content-type: application/json	是	是
vpc-lattice-svcs:RequestQueryString/ *key-name*: *value*	依請求 URL 中的查詢字串鍵值對來篩選存取權	quux: [corge, grault]	是	否
vpc-lattice-svcs:ServiceNetworkArn	篩選接收要求之服務之服務網路的 ARN 存取	arn:aws:vpc-lattice:us-west	是	是

條件索引鍵	描述	範例	可用於匿名（未經身份驗證的）呼叫者？	適用於 gRPC 嗎？
		-2:123456789012:servicenetwork/sn-0123456789abcdef0		
vpc-lattice-svcs:ServiceArn	透過接收要求之服務的 ARN 篩選存取	arn:aws:vpc-lattice:us-west-2:123456789012:service/svc-0123456789abcdef0	是	是
vpc-lattice-svcs:SourceVpc	依提出請求的 VPC 來篩選存取權	vpc-1a2b3c4d	是	是
vpc-lattice-svcs:SourceVpcOwnerAccount	依提出請求的 VPC 所屬帳戶來篩選存取權	123456789012	是	是

AWS 也提供可用來控制存取的其他條件索引鍵，例如`aws:PrincipalOrgID`全域條件索引鍵。若要查看所有 AWS 全域條件金鑰，請參閱《IAM 使用者指南》中的AWS 全域條件內容金鑰。

匿名 (未驗證) 主體

匿名主體是指未使用簽章版本 4 (SIGv4) 簽署 AWS 要求的來電者，且位於連線至服務網路的 VPC 內。如果身份驗證策略允許，匿名主體可以向服務網絡中的服務發出未經驗證的請求。

驗證政策示例

以下是需要經過驗證的主體提出要求的範例驗證原則。

所有範例均使用「us-west-2地區」，並包含虛擬帳號 ID。

範例 1：限制特定 AWS 組織對服務的存取

以下身份驗證策略示例授予任何經過身份驗證的請求的權限，以訪問該策略適用的服務網絡中的任何服務。但是，請求必須來自屬於條件中指定 AWS 組織的主參與者。

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": "*",
         "Action": "vpc-lattice-svcs:Invoke",
         "Resource": "*",
         "Condition": {
            "StringEquals": {
               "aws:PrincipalOrgID": [
                  "o-123456example"
               ]
            }
         }
      }
   ]
}
```

範例 2：依特定 IAM 角色限制對服務的存取

以下身份驗證策略示例授予任何使用 IAM 角色rates-client在Resource元素中指定的服務上發出 HTTP GET 請求的身份驗證請求的許可。Resource元素中的資源與附加策略的服務相同。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect": "Allow",
         "Principal": {
            "AWS": [
```

```
                "arn:aws:iam::123456789012:role/rates-client"
            ]
         },
         "Action": "vpc-lattice-svcs:Invoke",
         "Resource": [
            "arn:aws:vpc-lattice:us-west-2:123456789012:service/svc-0123456789abcdef0/
*"
         ],
         "Condition": {
            "StringEquals": {
               "vpc-lattice-svcs:RequestMethod": "GET"
            }
         }
      }
   ]
}
```

範例 3：透過特定 VPC 中已驗證的主體限制對服務的存取

以下身份驗證策略示例僅允許來自 VPC ID 為的 VPC 中主體的已驗證請求。*vpc-1a2b3c4d*

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": "*",
         "Action": "vpc-lattice-svcs:Invoke",
         "Resource": "*",
         "Condition": {
            "StringNotEquals": {
               "aws:PrincipalType": "Anonymous"
            },
            "StringEquals": {
               "vpc-lattice-svcs:SourceVpc": "vpc-1a2b3c4d"
            }
         }
      }
   ]
}
```

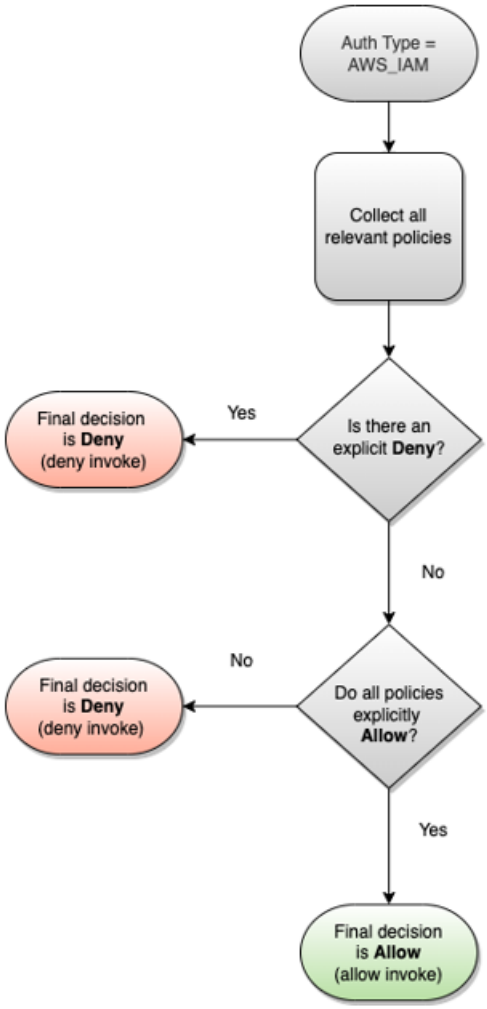
授權如何運作

當 VPC 萊迪思服務收到請求時， AWS 強制代碼會一起評估所有相關權限策略，以確定是否授權還是拒絕請求。它會評估授權期間適用於請求內容的所有 IAM 身分型政策和驗證政策。默認情況下，當 auth 類型為AWS_IAM時，所有請求都被隱式拒絕。來自所有相關策略的明確允許會覆寫預設值。

授權包括：

- 收集所有相關的 IAM 身分識別政策和身份驗證政策。
- 評估產生的原則集：
  - 確認請求者 (例如 IAM 使用者或角色) 具有從要求者所屬帳戶執行作業的權限。如果沒有明確的 allow 聲明，則 AWS 不授權請求。
  - 驗證服務網絡的身份驗證策略允許該請求。如果啟用了身份驗證策略，但沒有明確的 allow 語句，則 AWS 不授權請求。如果有明確的 allow 語句，或者 auth 類型是NONE，則代碼將繼續。
  - 驗證服務的身份驗證策略是否允許該請求。如果啟用了身份驗證策略，但沒有明確的 allow 語句，則 AWS 不授權請求。如果有明確的 allow 語句，或者 auth 類型是NONE，則強制代碼返回允許的最終決定。
  - 任何政策中的明確拒絕會覆寫任何允許。

該圖顯示了授權工作流程。提出要求時，相關原則會允許或拒絕要求存取特定服務。



使用安全群組控制 VPC 格子中的流量

AWS 安全性群組充當虛擬防火牆，可控制與其相關聯之資源之間的網路流量。使用 VPC 萊迪思，您可以建立安全群組，並將其指派給 VPC 關聯，將 VPC 連結至服務網路，以便為您的服務網路強制執行額外的網路層級安全性保護。

目錄

管理前綴列表

VPC 萊迪思提供受管理的前置碼清單，其中包括用於透過虛擬私人 VPC 萊迪思網路路由傳送流量的 IP 位址。您可以在安全群組規則中參考 VPC 萊迪思託管前綴清單。這可讓流量從用戶端流動、透過 VPC 萊迪思服務網路，以及 VPC 萊迪思服務目標。

例如，假設您已在美國西部 (奧勒岡) 區域 (us-west-2) 註冊為目標的 EC2 執行個體。您可以將規則新增至執行個體安全性群組，該群組允許從 VPC 萊迪思託管前綴清單進行傳入 HTTPS 存取，以便此區域中的 VPC LADS 流量可以連接到執行個體。如果您從安全群組中移除所有其他輸入規則，則可以防止 VPC Lights 流量以外的任何流量到達執行個體。

VPC 格子的受管理前綴列表的名稱如下：

- com.amazonaws.*region*.vpc-lattice
- com.amazonaws.*region*.ipv6.vpc-lattice

如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的 AWS受管字首清單。

Windows 用戶端

VPC 格子前置詞清單中的位址為連結本機位址。如果您從 Windows 用戶端連線到 VPC 格子，您必須更新 Windows 用戶端的組態，以便它將 VPC 格子使用的連結本機位址轉送到用戶端的主要 IP 位址。以下是更新 Windows 用戶端組態的範例命令，其中169.254.171.0是 VPC 格子使用的連結本機位址。

```
C:\> route add 169.254.171.0 mask 255.255.255.0 primary-ip-address
```

安全群組規則

搭配或不搭配安全群組使用 VPC Lacither 都不會影響您現有的 VPC 安全群組組態。不過，您可以隨時新增自己的安全性群組。

關鍵考量

- 用戶端的安全群組規則可控制傳送至 VPC 萊迪思的輸出流量。
- 目標的安全群組規則可控制從 VPC Latds 到目標的輸入流量，包括健康狀態檢查流量。
- 用於服務網路與 VPC 控制之間關聯的安全群組規則，這些用戶端可以存取 VPC 萊迪思服務網路。

服務網路和 VPC 關聯的建議輸入規則

若要讓流量從屬端 VPC 流向與服務網路相關聯的服務，您必須為服務的監聽器連接埠和監聽器協定建立輸入規則。

傳入

來源	通訊協定	連接埠範圍	註解
VPC CIDR	*listener*	*listener*	允許從用戶端到 VPC 格子的流量

從用戶端執行個體流向 VPC 萊迪思的流量的建議輸出規則

根據預設，安全群組允許所有對外流量。但是，如果您有自訂輸出規則，則必須允許對接聽程式連接埠和通訊協定的 VPC 萊迪思前綴的輸出流量，以便用戶端執行個體可以連接到與 VPC Latess 服務網路相關聯的所有服務。您可以透過參考 VPC 萊迪格前置詞清單的識別碼來允許此流量。

傳出

目的地	通訊協定	連接埠範圍	註解
VPC ##########	*listener*	*listener*	允許從用戶端到 VPC 格子的流量

從 VPC 萊迪思流向目標執行個體的流量的建議輸入規則

您無法使用用戶端安全群組做為目標安全群組的來源，因為流量會從 VPC Latds 流出。您可以參考 VPC 格子前置詞清單的 ID。

傳入

來源	通訊協定	連接埠範圍	註解
VPC ##########	*target*	*target*	允許從 VPC 格子到目標的流量
VPC ##########	*health check*	*health check*	允許從 VPC 格子到目標的健康狀態檢查流量

管理 VPC 關聯的安全群組

您可以使用 AWS CLI 來檢視、新增或更新 VPC 上的安全性群組以服務網路關聯。使用時 AWS CLI，請記住您的命令會在為您的設定檔所 AWS 區域 設定的中執行。如果您想在不同區域中執行命令，則可變更設定檔的預設區域，或搭配 `--region` 參數使用命令。

開始之前，請確認您已在與要新增至服務網路的 VPC 相同的 VPC 中建立安全性群組。如需詳細資訊，請參閱 Amazon VPC 使用者指南中的使用安全群組控制資源流量

使用主控台建立 VPC 關聯時新增安全群組

1. 前往 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在功能窗格的 VPC Landers 下，選擇 [服務網路]。
3. 選取服務網路的名稱，以開啟其詳細資訊頁面。
4. 在 [VPC 關聯] 索引標籤上，選擇 [建立 VPC 關聯]，然後選擇 [新增 V PC 關聯]。
5. 選取 VPC 和最多五個安全群組。
6. 選擇儲存變更。

使用主控台新增或更新現有 VPC 關聯的安全群組

1. 前往 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在功能窗格的 VPC Landers 下，選擇 [服務網路]。
3. 選取服務網路的名稱，以開啟其詳細資訊頁面。
4. 在 [VPC 關聯] 索引標籤上，選取關聯的核取方塊，然後選擇 [動作] > [編輯安全性群組]。
5. 視需要新增和移除安全性群組。
6. 選擇儲存變更。

使用建立 VPC 關聯時新增安全群組 AWS CLI

使用 create-service-network-vpc-關聯指令指定VPC 關聯的 VPC 識別碼，以及要新增的安全性群組識別碼。

```
aws vpc-lattice create-service-network-vpc-association \
    --service-network-identifier sn-0123456789abcdef0 \
    --vpc-identifier vpc-1a2b3c4d \
    --security-group-ids sg-7c2270198example
```

如果成功，此命令傳回的輸出會類似如下。

```
{
  "arn": "arn",
  "createdBy": "464296918874",
  "id": "snva-0123456789abcdef0",
  "status": "CREATE_IN_PROGRESS",
  "securityGroupIds": ["sg-7c2270198example"]
}
```

使用新增或更新現有 VPC 關聯的安全群組 AWS CLI

使用 update-service-network-vpc-soci ation 指令，指定服務網路的識別碼和安全性群組的識別碼。這些安全群組會覆寫任何先前關聯的安全群組。更新清單時，至少定義一個安全性群組。

```
aws vpc-lattice update-service-network-vpc-association
    --service-network-vpc-association-identifier sn-903004f88example \
    --security-group-ids sg-7c2270198example sg-903004f88example
```

> **Warning**
>
> 您無法移除所有安全性群組。您必須先刪除 VPC 關聯，然後在沒有任何安全群組的情況下重新建立 VPC 關聯。刪除 VPC 關聯時請務必小心。這樣可以防止流量到達該服務網路中的服務。

使用網路 ACL 控制前往 VPC 晶格的流量

網路存取控制清單 (ACL) 會允許或拒絕子網層級的特定傳入或傳出流量。預設的網路 ACL 會允許所有外傳和傳入流量。您可以為子網路建立自訂網路 ACL，以提供額外的安全層。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的網路 ACL。

目錄

用戶端子網路的網路 ACL

用戶端子網路的網路 ACL 必須允許用戶端和 VPC 萊迪格之間的流量。您可以從 VPC 萊迪思的託管前綴列表中獲取允許的 IP 地址範圍。

傳入

來源	通訊協定	連接埠範圍	註解
vpc_ ## _ ## _ ## #	TCP	1025-65535	允許從 VPC 格子到用戶端的流量

傳出

目的地	通訊協定	連接埠範圍	註解
vpc_ ## _ ## _ ## #	*listener*	*listener*	允許從用戶端到 VPC 格子的流量

目標子網路的網路 ACL

目標子網路的網路 ACL 必須同時允許目標連接埠和健全狀況檢查連接埠上的目標和 VPC L格之間的流量。您可以從 VPC 萊迪思的託管前綴列表中獲取允許的 IP 地址範圍。

傳入

來源	通訊協定	連接埠範圍	註解
vpc_ ## _ ## _ ## #	*target*	*target*	允許從 VPC 格子到目標的流量
vpc_ ## _ ## _ ## #	*health check*	*health check*	允許從 VPC 格子到目標的健康狀態檢查流量

傳出

目的地	通訊協定	連接埠範圍	註解
vpc_ ## _ ## _ # #	*target*	1024-65535	允許從目標到 VPC 格子的流量
vpc_ ## _ ## _ # #	*health check*	1024-65535	允許從目標到 VPC 格子的健康狀態檢查流量

簽章版本 4 驗證要求的範例

VPC 格子使用簽名版本 4（SIGv4）或簽名版本 4A（SigV4a）進行客戶端身份驗證。如需詳細資訊，請參閱 IAM 使用者指南中的簽署 AWS API 請求。

考量事項

- VPC 萊迪思會嘗試驗證使用 SIGv4 或 SigV4a 簽署的任何請求。要求會失敗，但未經驗證。
- VPC 萊迪思不支援有效負載簽署。您必須傳送值設定為的`x-amz-content-sha256`標頭`"UNSIGNED-PAYLOAD"`。

範例

- Python
- 帶有攔截器的 Java
- 沒有攔截器的 Java
- Node.js

Python

此範例會透過安全連線，將已簽署的要求傳送至網路中註冊的服務。如果您喜歡使用請求，botocore 軟件包簡化了身份驗證過程，但並非嚴格要求。如需詳細資訊，請參閱 Boto3 文件中的認證。

若要安裝`botocore`和`awscrt`套件，請使用下列命令。如需詳細資訊，請參閱 AWS CRT Python。

```
pip install botocore awscrt
```

在下列範例中，以您自己的值取代預留位置值。

SIGv4

```
from botocore import crt
import requests
from botocore.awsrequest import AWSRequest
from botocore.credentials import Credentials
import botocore.session

if __name__ == '__main__':
    session = botocore.session.Session()
    signer = crt.auth.CrtS3SigV4Auth(session.get_credentials(), 'vpc-lattice-svcs',
 'us-west-2')
    endpoint = 'https://user-02222f67d3a427111.1234abc.vpc-lattice-svcs.us-
west-2.on.aws/create'
    data = "some-data-here"
    headers = {'Content-Type': 'application/json'}
    request = AWSRequest(method='POST', url=endpoint, data=data, headers=headers)
    request.context["payload_signing_enabled"] = False # payload signing is not
 supported
    signer.add_auth(request)

    prepped = request.prepare()

    response = requests.post(prepped.url, headers=prepped.headers, data=data)
```

SIGv4A

```
from botocore import crt
import requests
from botocore.awsrequest import AWSRequest
from botocore.credentials import Credentials
import botocore.session

if __name__ == '__main__':
    session = botocore.session.Session()
    signer = crt.auth.CrtS3SigV4AsymAuth(session.get_credentials(), 'vpc-lattice-
svcs', 'us-west-2')
    endpoint = 'https://user-02222f67d3a427111.1234abc.vpc-lattice-svcs.us-
west-2.on.aws/create'
    data = "some-data-here"
    headers = {'Content-Type': 'application/json'}
```

```
    request = AWSRequest(method='POST', url=endpoint, data=data, headers=headers)
    request.context["payload_signing_enabled"] = False # payload signing is not
supported
    signer.add_auth(request)

    prepped = request.prepare()

    response = requests.post(prepped.url, headers=prepped.headers, data=data)
```

帶有攔截器的 Java

此範例使用 Amazon 請求簽署攔截器來處理請求簽署。

```
import com.amazonaws.http.AwsRequestSigningApacheInterceptor;
import software.amazon.awssdk.auth.credentials.DefaultCredentialsProvider;
import software.amazon.awssdk.auth.signer.Aws4UnsignedPayloadSigner;
import software.amazon.awssdk.regions.Region;

import java.nio.charset.StandardCharsets;

import org.apache.http.client.methods.HttpPost;
import org.apache.http.entity.ByteArrayEntity;
import org.apache.http.impl.client.CloseableHttpClient;
import org.apache.http.impl.client.HttpClients;

public class App {
    public static void main(String[] args) {
      var interceptor = new AwsRequestSigningApacheInterceptor(
          "vpc-lattice-svcs",
          Aws4UnsignedPayloadSigner.create(), // requires HTTPS
          DefaultCredentialsProvider.create(),
          Region.US_WEST_2.id()
          );
      CloseableHttpClient client = HttpClients.custom()
        .addInterceptorLast(interceptor)
        .build();

      var httpPost = new HttpPost("https://user-02222f67d3a427111.1234abc.vpc-lattice-
svcs.us-west-2.on.aws/create");
      httpPost.addHeader("content-type", "application/json");

      var body = """
```

```
      {
        "name": "Jane Doe",
        "job": "Engineer"
      }
      """;
      httpPost.setEntity(new ByteArrayEntity(body.getBytes(StandardCharsets.UTF_8)));

      try (var response = client.execute(httpPost)) {
        System.out.println(new
 String(response.getEntity().getContent().readAllBytes()));
      } catch (Exception e) {
        throw new RuntimeException(e);
      }
    }
}
```

沒有攔截器的 Java

此範例顯示如何使用自訂攔截器執行要求簽署。它使用默認憑據提供程序類 AWS SDK for Java 2.x，從中獲取正確的憑據。如果您想要使用特定的認證提供者，您可以從中選取AWS SDK for Java 2.x。只 AWS SDK for Java 允許透過 HTTPS 未簽署的承載。不過，您可以擴充簽署者，以透過 HTTP 支援未簽署的承載。

```
import java.io.ByteArrayInputStream;
import java.io.IOException;
import java.nio.charset.StandardCharsets;
import java.util.HashMap;
import java.util.List;
import java.util.Map;
import software.amazon.awssdk.auth.credentials.DefaultCredentialsProvider;
import software.amazon.awssdk.auth.signer.Aws4UnsignedPayloadSigner;
import software.amazon.awssdk.auth.signer.AwsSignerExecutionAttribute;
import software.amazon.awssdk.core.interceptor.ExecutionAttributes;
import software.amazon.awssdk.http.SdkHttpFullRequest;
import software.amazon.awssdk.http.SdkHttpMethod;
import software.amazon.awssdk.regions.Region;

import org.apache.http.client.methods.HttpPost;
import org.apache.http.entity.ByteArrayEntity;
import org.apache.http.impl.client.CloseableHttpClient;
import org.apache.http.impl.client.HttpClients;

public class App {
```

```
    public static void main(String[] args) {
        var signer = Aws4UnsignedPayloadSigner.create(); // requires HTTPS

        Map<String, String> headers = new HashMap<>();
        headers.put("content-type", "application/json");
        var body = """
        {
            "name": "Jane Doe",
            "job": "Engineer"
        }
        """;

        String endpoint = "https://user-02222f67d3a427111.1234abc.vpc-lattice-svcs.us-
west-2.on.aws/create";

        var sdkRequest = SdkHttpFullRequest.builder().method(SdkHttpMethod.POST);

        sdkRequest.host("user-02222f67d3a427111.1234abc.vpc-lattice-svcs.us-
west-2.on.aws");
        sdkRequest.protocol("HTTPS");
        sdkRequest.encodedPath("/create");
        sdkRequest.contentStreamProvider(() -> new
 ByteArrayInputStream(body.getBytes(StandardCharsets.UTF_8)));


        for (Map.Entry<String, String> header : headers.entrySet()) {
            sdkRequest.putHeader(header.getKey(), header.getValue());
        }

        ExecutionAttributes attributes = ExecutionAttributes.builder()
                .put(AwsSignerExecutionAttribute.AWS_CREDENTIALS,
 DefaultCredentialsProvider.create().resolveCredentials())
                .put(AwsSignerExecutionAttribute.SERVICE_SIGNING_NAME, "vpc-lattice-
svcs")
                .put(AwsSignerExecutionAttribute.SIGNING_REGION, Region.US_WEST_2)
                .build();

        SdkHttpFullRequest prepRequest = signer.sign(sdkRequest.build(), attributes);

        HttpPost httpPost = new HttpPost(endpoint);
        for (Map.Entry<String, List<String>> header : prepRequest.headers().entrySet())
 {
            if (header.getKey().equalsIgnoreCase("host")) { continue; }
```

```
            for(var value : header.getValue()) {
                httpPost.addHeader(header.getKey(), value);
            }
        }

        CloseableHttpClient client = HttpClients.custom().build();

        httpPost.setEntity(new ByteArrayEntity(body.getBytes(StandardCharsets.UTF_8)));

        try (var response = client.execute(httpPost)){
            System.out.println(new
 String(response.getEntity().getContent().readAllBytes()));
        } catch (IOException e) {
            throw new RuntimeException(e);
        }
    }
}
```

Node.js

這個範例會使用 aws-crt NodeJS 繫結來使用 HTTPS 傳送已簽署的要求。

若要安裝aws-crt套件，請使用下列命令。

```
npm -i aws-crt
```

如果AWS_REGION環境變數存在，則範例會使用由指定的 Region AWS_REGION。預設「區域」為us-east-1。

SIGv4

```
const https = require('https')
const crt = require('aws-crt')
const { HttpRequest } = require('aws-crt/dist/native/http')

function sigV4Sign(method, endpoint, service, algorithm) {
    const host = new URL(endpoint).host
    const request = new HttpRequest(method, endpoint)
    request.headers.add('host', host)
    // crt.io.enable_logging(crt.io.LogLevel.INFO)
    const config = {
        service: service,
        region: process.env.AWS_REGION ? process.env.AWS_REGION : 'us-east-1',
```

```
        algorithm: algorithm,
        signature_type: crt.auth.AwsSignatureType.HttpRequestViaHeaders,
        signed_body_header: crt.auth.AwsSignedBodyHeaderType.XAmzContentSha256,
        signed_body_value: crt.auth.AwsSignedBodyValue.UnsignedPayload,
        provider: crt.auth.AwsCredentialsProvider.newDefault()
    }

    return crt.auth.aws_sign_request(request, config)
}

if (process.argv.length === 2) {
  console.error(process.argv[1] + ' <url>')
  process.exit(1)
}

const algorithm = crt.auth.AwsSigningAlgorithm.SigV4;

sigV4Sign('GET', process.argv[2], 'vpc-lattice-svcs').then(
  httpResponse => {
    var headers = {}

    for (const sigv4header of httpResponse.headers) {
      headers[sigv4header[0]] = sigv4header[1]
    }

    const options = {
      hostname: new URL(process.argv[2]).host,
      path: '/',
      method: 'GET',
      headers: headers
    }

    req = https.request(options, res => {
      console.log('statusCode:', res.statusCode)
      console.log('headers:', res.headers)
      res.on('data', d => {
        process.stdout.write(d)
      })
    })
    req.on('error', err => {
      console.log('Error: ' + err)
    })
    req.end()
  }
```

```
)
```

SIGv4A

```
const https = require('https')
const crt = require('aws-crt')
const { HttpRequest } = require('aws-crt/dist/native/http')

function sigV4Sign(method, endpoint, service, algorithm) {
    const host = new URL(endpoint).host
    const request = new HttpRequest(method, endpoint)
    request.headers.add('host', host)
    // crt.io.enable_logging(crt.io.LogLevel.INFO)
    const config = {
        service: service,
        region: process.env.AWS_REGION ? process.env.AWS_REGION : 'us-east-1',
        algorithm: algorithm,
        signature_type: crt.auth.AwsSignatureType.HttpRequestViaHeaders,
        signed_body_header: crt.auth.AwsSignedBodyHeaderType.XAmzContentSha256,
        signed_body_value: crt.auth.AwsSignedBodyValue.UnsignedPayload,
        provider: crt.auth.AwsCredentialsProvider.newDefault()
    }

    return crt.auth.aws_sign_request(request, config)
}

if (process.argv.length === 2) {
  console.error(process.argv[1] + ' <url>')
  process.exit(1)
}

const algorithm = crt.auth.AwsSigningAlgorithm.SigV4Asymmetric;

sigV4Sign('GET', process.argv[2], 'vpc-lattice-svcs').then(
  httpResponse => {
    var headers = {}

    for (const sigv4header of httpResponse.headers) {
      headers[sigv4header[0]] = sigv4header[1]
    }

    const options = {
      hostname: new URL(process.argv[2]).host,
```

```
      path: '/',
      method: 'GET',
      headers: headers
    }

    req = https.request(options, res => {
      console.log('statusCode:', res.statusCode)
      console.log('headers:', res.headers)
      res.on('data', d => {
        process.stdout.write(d)
      })
    })
    req.on('error', err => {
      console.log('Error: ' + err)
    })
    req.end()
  }
)
```

Amazon VPC 晶格中的資料保護

AWS 共同責任模型適用於 Amazon VPC 萊迪思中的資料保護。如此模型所述， 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。此內容包括您所使用 AWS 服務 的安全組態和管理任務。如需有關資料隱私權的更多相關資訊，請參閱資料隱私權常見問答集。如需有關歐洲資料保護的相關資訊，請參閱 AWS 安全性部落格上的 AWS 共同的責任模型和 GDPR 部落格文章。

傳輸中加密

VPC 萊迪思是由控制平面和資料層組成的全受管服務。每架飛機在服務中都有不同的目的。控制平面提供用於建立、讀取/描述、更新、刪除和列出 (CRUDL) 資源的管理 API (例如，`CreateService`和. `UpdateService` 與 VPC 萊迪思的控制平面之間的通訊受到 TLS 的保護。資料平面是 VPC 萊迪思的 Invoke API，可提供服務之間的互連。TLS 也會加密與 VPC 萊迪思資料層的通訊。密碼套件和通訊協定版本使用由 VPC 萊迪斯提供的預設值，且無法設定。如需詳細資訊，請參閱 適用於 VPC 格子服務的 HTTPS 接聽程式。

靜態加密

預設情況下，靜態資料加密有助於降低保護敏感資料所涉及的營運開銷和複雜性。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。

目錄

使用 Amazon S3 受管金鑰 (SSE-S3) 的伺服器端加密

使用伺服器端加密搭配 Amazon S3 受管金鑰 (SSE-S3) 時，每個物件都會使用唯一金鑰來加密。它使用定期輪換的根金鑰自行加密金鑰，提供額外的防護。Amazon S3 伺服器端加密使用目前最強大的其中一種區塊加密法 (256 位元進階加密標準 (AES-256) GCM)，加密您的資料。對於在 AES-GCM 之前加密的物件，仍支援以 AES-CBC 解密這些物件。如需詳細資訊，請參閱將伺服器端加密與 Amazon S3 受管加密金鑰搭配使用 (SSE-S3)。

如果針對 VPC 萊迪斯存取日誌的 S3 儲存貯體使用 Amazon S3 受管加密金鑰 (SSE-S3) 啟用伺服器端加密，則會在每個存取日誌檔存放在 S3 儲存貯體之前 AWS 自動加密每個存取日誌檔。如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南中的傳送到 Amazon S3 的日誌。

使用儲存於 AWS KMS (SSE-KMS) 的 AWS KMS 金鑰進行伺服器端加密

使用金 AWS KMS 鑰 (SSE-KMS) 的伺服器端加密類似於 SSE-S3，但使用此服務還有一些額外的優點和費用。使用 AWS KMS 金鑰有個別的許可，可提供額外的保護，防止未經授權存取 Amazon S3 中的物件。SSE-KMS 也會為您提供稽核追蹤，顯示金 AWS KMS 鑰的使用時間以及使用者。如需詳細資訊，請參閱搭配使用伺服器端加密 AWS Key Management Service (SSE-KMS)。

目錄

加密和解密您的證書的私鑰

您的 ACM 憑證和私密金鑰會使用別名 aw s/acm 的 AWS 受管 KMS 金鑰加密。您可以在 AWS 受管理金鑰底下的 AWS KMS 主控台中檢視具有此別名的金鑰 ID。

VPC 萊迪思不會直接存取您的 ACM 資源。它會使用 AWS TLS 連線管理員來保護和存取憑證的私密金鑰。當您使用 ACM 憑證建立 VPC 萊迪思服務時，VPC 萊迪思會將您的憑證與 AWS TLS 連線管理員建立關聯。這是通過在您的 AWS 託管密鑰中 AWS KMS 創建一個帶有前綴 aws/ acm 的授予來完

成的。授權是允許 TLS 連線管理員在密碼編譯作業中使用 KMS 金鑰的原則工具。授權允許受權者主體 (TLS 連線管理員) 呼叫 KMS 金鑰上指定的授權作業，以解密憑證的私密金鑰。然後 TLS 連線管理員會使用憑證和解密 (純文字) 私密金鑰，與 VPC 萊迪思服務的用戶端建立安全連線 (SSL/TLS 工作階段)。當憑證與 VPC 萊迪思服務中斷關聯時，授權就會被淘汰。

如果您想要移除對 KMS 金鑰的存取權，建議您使用或使用`update-service`命令取代 AWS Management Console 或刪除服務中的憑證 AWS CLI。

VPC 格子的加密內容

加密上下文是一組可選的鍵值對，其中包含有關私鑰可能用於什麼的其他上下文信息。 AWS KMS 將加密內容繫結至加密的資料，並將其用作其他驗證資料，以支援已驗證的加密。

當您的 TLS 金鑰與 VPC 萊迪思和 TLS 連線管理員搭配使用時，您的 VPC 萊迪思服務的名稱會包含在用來加密您的靜態金鑰的加密內容中。您可以檢視 CloudTrail 記錄檔中的加密內容 (如下一節所示)，或查看 ACM 主控台中的 [關聯資源] 索引標籤，來驗證您的憑證和私密金鑰正在使用哪個 VPC Layther 服務。

若要解密資料，請求中會包含相同的加密內容。VPC 萊迪思在所有 AWS KMS 加密操作中使用相同的加密內容，其中金鑰是`aws:vpc-lattice:arn`，值為 VPC 萊迪斯服務的 Amazon 資源名稱 (ARN)。

下列範例會顯示作業輸出中的加密內容，例如`CreateGrant`：

```
"encryptionContextEquals": {
    "aws:acm:arn": "arn:aws:acm:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "aws:vpc-lattice:arn": "arn:aws:vpc-lattice:us-west-2:111122223333:service/
svc-0b23c1234567890ab"
}
```

監控 VPC 晶格的加密金鑰

當您將 AWS 受管金鑰與 VPC 萊迪思服務搭配使用時，您可以使用AWS CloudTrail來追蹤 VPC 萊迪思傳送到的請求。 AWS KMS

CreateGrant

當您將 ACM 憑證新增至 VPC 萊迪思服務時，系統會代表您傳送`CreateGrant`要求，讓 TLS 連線管理員能夠解密與您的 ACM 憑證相關聯的私密金鑰

您可以檢視CreateGrant作業在 >> 事件歷史記錄 CloudTrail **CreateGrant** >> 中的事件。

以下是CreateGrant作業事件歷史記錄中的範例 CloudTrail 事件記錄：


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "sessionContext": {
            "sessionIssuer": {
                "type": "IAMUser",
                "principalId": "EX_PRINCIPAL_ID",
                "arn": "arn:aws:iam::111122223333:user/Alice",
                "accountId": "111122223333",
                "userName": "Alice"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-02-06T23:30:50Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "acm.amazonaws.com"
    },
    "eventTime": "2023-02-07T00:07:18Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateGrant",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "acm.amazonaws.com",
    "userAgent": "acm.amazonaws.com",
    "requestParameters": {
        "granteePrincipal": "tlsconnectionmanager.amazonaws.com",
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
        "operations": [
            "Decrypt"
        ],
        "constraints": {
            "encryptionContextEquals": {
                "aws:acm:arn": "arn:aws:acm:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
```

```
                "aws:vpc-lattice:arn": "arn:aws:vpc-lattice:us-
west-2:111122223333:service/svc-0b23c1234567890ab"
            }
        },
        "retiringPrincipal": "acm.us-west-2.amazonaws.com"
    },
    "responseElements": {
        "grantId": "f020fe75197b93991dc8491d6f19dd3cebb24ee62277a05914386724f3d48758",
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "requestID": "ba178361-8ab6-4bdd-9aa2-0d1a44b2974a",
    "eventID": "8d449963-1120-4d0c-9479-f76de11ce609",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

在上述CreateGrant範例中，您會注意到受權者主體是 TLS 連線管理員，而加密內容具有 VPC 萊迪思服務 ARN。

ListGrants

您可以使用 KMS 金鑰識別碼和帳戶識別碼來呼叫 ListGrants API。這會取得指定 KMS 金鑰的所有授權清單。如需詳細資訊，請參閱ListGrants。

使用中的下列ListGrants命令 AWS CLI 來查看所有授權的詳細資訊：

```
aws kms list-grants –key-id your-kms-key-id
```

您的輸出看起來應該類似於以下範例：

```
{
```

```
    "Grants": [
        {
            "Operations": [
                "Decrypt"
            ],
            "KeyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
            "Name": "IssuedThroughACM",
            "RetiringPrincipal": "acm.us-west-2.amazonaws.com",
            "GranteePrincipal": "tlsconnectionmanager.amazonaws.com",
            "GrantId":
 "f020fe75197b93991dc8491d6f19dd3cebb24ee62277a05914386724f3d48758",
            "IssuingAccount": "arn:aws:iam::111122223333:root",
            "CreationDate": "2023-02-06T23:30:50Z",
            "Constraints": {
                "encryptionContextEquals": {
                  "aws:acm:arn": "arn:aws:acm:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
                  "aws:vpc-lattice:arn": "arn:aws:vpc-lattice:us-
west-2:111122223333:service/svc-0b23c1234567890ab"
                }
            }
        }
    ]
}
```

在上述ListGrants範例中，您會注意到受權者主體是 TLS 連線管理員，而加密內容具有 VPC 萊迪思服務 ARN。

解密

VPC 萊迪思使用 TLS 連線管理員呼叫Decrypt作業來解密您的私密金鑰，以便在您的 VPC 萊迪思服務中提供 TLS 連線。您可以在 **>>** 事件歷史記錄 CloudTrail **>>** 中將**Decrypt**作業視為事件**Decrypt**。

以下是Decrypt作業事件歷史記錄中的範例 CloudTrail 事件記錄：

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "tlsconnectionmanager.amazonaws.com"
    },
```

```
    "eventTime": "2023-02-07T00:07:23Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "tlsconnectionmanager.amazonaws.com",
    "userAgent": "tlsconnectionmanager.amazonaws.com",
    "requestParameters": {
        "encryptionContext": {
            "aws:acm:arn": "arn:aws:acm:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
            "aws:vpc-lattice:arn": "arn:aws:vpc-lattice:us-west-2:111122223333:service/
svc-0b23c1234567890ab"
        },
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT"
    },
    "responseElements": null,
    "requestID": "12345126-30d5-4b28-98b9-9153da559963",
    "eventID": "abcde202-ba1a-467c-b4ba-f729d45ae521",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "sharedEventID": "abcde202-ba1a-467c-b4ba-f729d45ae521",
    "eventCategory": "Management"
}
```


適用於 Amazon VPC 萊迪思的身分和存取管理

以下各節說明如何使用 AWS Identity and Access Management (IAM) 透過控制誰可以執行 VPC 萊迪思 API 動作來協助保護您的 VPC 萊迪思資源。

主題

- Amazon VPC 晶格如何與 IAM 搭配使用
- VPC 格子 API 權限

- Amazon VPC 格子的基於身份的政策
- 針對 VPC 格子使用服務連結角色
- AWS 適用於 VPC 萊迪思的受管政策

Amazon VPC 晶格如何與 IAM 搭配使用

在您使用 IAM 管理 VPC 萊迪思的存取權限之前，請先了解哪些 IAM 功能可用於 VPC 萊迪思。

您可以搭配 Amazon VPC 晶格使用的 IAM 功能

IAM 功能	VPC 格子支援
身分型政策	是
資源型政策	是
政策動作	是
政策資源	是
政策條件索引鍵	是
ACL	否
ABAC (政策中的標籤)	是
臨時憑證	是
服務角色	否
服務連結角色	是

有關 VPC Ratts 和其他 AWS 服務如何與大多數 IAM 功能搭配使用的高階檢視，請參閱 IAM 使用者指南中的可與 IAM 搭配使用的AWS 服務。

適用於 VPC 晶格的身分識別原則

支援身分型政策	是

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

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

VPC 格內以資源為基礎的政策

支援以資源基礎的政策	是

資源型政策是連接到資源的 JSON 政策文件。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。

VPC 萊迪思支援身份驗證政策，這是一種以資源為基礎的政策，可讓您控制對服務網路中服務的存取。如需詳細資訊，請參閱 使用身份驗證策略控制服務的訪問。

VPC 萊迪思也支援以資源為基礎的權限原則，以便與之整合。 AWS Resource Access Manager您可以使用這些以資源為基礎的策略，將使用權限授與其他 AWS 帳號或組織，以啟用資源共用。如需詳細資訊，請參閱 分享您的 VPC 萊迪思資源。

針對 VPC 格子的政策動作

支援政策動作	是

在 IAM 政策陳述式中，您可以從任何支援 IAM 的服務指定任何 API 動作。對於 VPC 格子，請使用以下前綴和 API 動作的名稱：`vpc-lattice:`例如：`vpc-lattice:CreateService`、`vpc-lattice:CreateTargetGroup` 和 `vpc-lattice:PutAuthPolicy`。

若要在單一陳述式中指定多個動作，請以逗號分隔它們，如下所示：

```
"Action": [ "vpc-lattice:action1", "vpc-lattice:action2" ]
```

您也可以使用萬用字元指定多個動作。例如，您可以指定名稱以該字開頭的所有動作`Get`，如下所示：

```
"Action": "vpc-lattice:Get*"
```

如需 VPC 萊迪思 API 動作的完整清單，請參閱服務授權參考資料中的 Amazon VPC 萊迪思定義的動作。

VPC 格子的政策資源

支援政策資源	是

在 IAM 政策陳述式中，Resource 元素指定陳述式所涵蓋的一個或多個物件。對於 VPC 萊迪思，每個 IAM 政策聲明都適用於您使用其 ARN 指定的資源。

特定的 Amazon 資源名稱 (ARN) 格式取決於資源。當您提供 ARN 時，請以您的資源特定資訊取代*##*文字。

- 訪問日誌訂閱：

```
"Resource": "arn:aws:vpc-lattice:region:account-id:accesslogsubscription/access-log-subscription-id"
```

- 聽眾：

```
"Resource": "arn:aws:vpc-lattice:region:account-id:service/service-id/
listener/listener-id"
```

- 規則：

```
"Resource": "arn:aws:vpc-lattice:region:account-id:service/service-id/
listener/listener-id/rule/rule-id"
```

- 服務：

```
"Resource": "arn:aws:vpc-lattice:region:account-id:service/service-id"
```

- 服務網絡：

```
"Resource": "arn:aws:vpc-lattice:region:account-id:servicenetwork/service-network-id"
```

- 服務網絡服務協會：

```
"Resource": "arn:aws:vpc-lattice:region:account-
id:servicenetworkserviceassociation/service-network-service-association-id"
```

- 服務網路 VPC 關聯：

```
"Resource": "arn:aws:vpc-lattice:region:account-
id:servicenetworkvpcassociation/service-network-vpc-association-id"
```

- 目標群體：

```
"Resource": "arn:aws:vpc-lattice:region:account-id:targetgroup/target-group-id"
```

VPC 格子的原則條件金鑰

支援服務特定政策條件金鑰	是

您可以在 IAM 政策中指定控制 VPC 萊迪思資源存取的條件。政策陳述式只有在符合下列條件時才有效。

VPC 萊迪思支援下列服務定義的條件金鑰，您可以在身分型原則中使用這些金鑰，以決定誰可以執行 VPC 萊迪思 API 動作。如需詳細資訊，請參閱服務授權參考中的 Amazon VPC 萊迪思服務的條件金鑰。

基於身份的策略的服務定義條件密鑰

條件索引鍵	描述	支援這些動作
vpc-lattice:AuthType	按請求中的 auth 類型過濾訪問（AWS_IAM或NONE	• CreateService • CreateServiceNetwork • UpdateService • UpdateServiceNetwork
vpc-lattice:Protocol	依要求中的通訊協定篩選存取 (HTTP或HTTPS)	• CreateListener

條件索引鍵	描述	支援這些動作
vpc-lattice:SecurityGroupIds	依要求中的安全性群組 ID 篩選存取	• CreateServiceNetworkVpcAssociation • UpdateServiceNetworkVpcAssociation
vpc-lattice:ServiceArn	篩選要求中服務 ARN 的存取	• CreateServiceNetworkServiceAssociation • DeleteServiceNetworkServiceAssociation • GetServiceNetworkServiceAssociation • ListServiceNetworkServiceAssociations
vpc-lattice:ServiceNetworkArn	篩選要求中服務網路 ARN 的存取	• CreateServiceNetworkServiceAssociation • CreateServiceNetworkVpcAssociation • DeleteServiceNetworkVpcAssociation • GetServiceNetworkServiceAssociation • GetServiceNetworkVpcAssociation • ListServiceNetworkServiceAssociations • ListServiceNetworkVpcAssociations • UpdateServiceNetworkVpcAssociation
vpc-lattice:TargetGroupArns	依要求中目標群組的 ARN 篩選存取	• CreateListener • CreateRule • UpdateListener • UpdateRule
vpc-lattice:VpcId	依要求中虛擬私有雲 (VPC) 的 ID 篩選存取	• CreateServiceNetworkVpcAssociation • CreateTargetGroup • DeleteServiceNetworkVpcAssociation • GetServiceNetworkVpcAssociation • ListServiceNetworkVpcAssociations • UpdateServiceNetworkVpcAssociation

AWS 支援全域條件金鑰和服務特定條件金鑰。如需 AWS 全域條件金鑰的相關資訊，請參閱《IAM 使用者指南》中的AWS 全域條件內容金鑰。

VPC 格子中的存取控制清單 (ACL)

支援 ACL	否

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

以屬性為基礎的存取控制 (ABAC) 搭配 VPC 格子

支援 ABAC (政策中的標籤)	是

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

ABAC 在成長快速的環境中相當有幫助，並能在政策管理變得繁瑣時提供協助。

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

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

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

搭配 VPC 格子使用臨時登入資料

支援臨時憑證	是

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

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

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

VPC 格子的服務角色

支援服務角色	否

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

> **Warning**
>
> 變更服務角色的權限可能會中斷 VPC 萊迪斯功能。僅在 VPC 萊迪思提供指導時，才編輯服務角色。

VPC 格子的服務連結角色

支援服務連結角色	是

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

如需建立或管理 VPC Landis 服務連結角色的相關資訊，請參閱。針對 VPC 格子使用服務連結角色

VPC 格子 API 權限

您必須授予 IAM 身分 (例如使用者或角色) 權限，才能呼叫他們所需的 VPC 萊迪思 API 動作，如中針對 VPC 格子的政策動作所述。此外，對於某些 VPC 萊迪思動作，您必須授予 IAM 身分權限，才能從其他 AWS API 呼叫特定動作。

API 的必要許可

從 API 呼叫下列動作時，您必須授與 IAM 使用者呼叫指定動作的權限。

CreateServiceNetworkVpcAssociation

- vpc-lattice:CreateServiceNetworkVpcAssociation
- ec2:DescribeVpcs
- ec2:DescribeSecurityGroups（僅在提供安全組時才需要）

UpdateServiceNetworkVpcAssociation

- vpc-lattice:UpdateServiceNetworkVpcAssociation
- ec2:DescribeSecurityGroups（僅在提供安全組時才需要）

CreateTargetGroup

- vpc-lattice:CreateTargetGroup
- ec2:DescribeVpcs

RegisterTargets

- vpc-lattice:RegisterTargets
- ec2:DescribeInstances（僅當INSTANCE是目標群組類型時才需要）
- ec2:DescribeVpcs(僅當INSTANCE或IP為目標群組類型時才需要)
- ec2:DescribeSubnets(僅當INSTANCE或IP為目標群組類型時才需要)
- lambda:GetFunction（僅當LAMBDA是目標群組類型時才需要）
- lambda:AddPermission(只有在目標群組尚未具備叫用指定 Lambda 函數的權限時才需要)

DeregisterTargets

- vpc-lattice:DeregisterTargets

CreateAccessLogSubscription

- vpc-lattice:CreateAccessLogSubscription
- logs:GetLogDelivery
- logs:CreateLogDelivery

DeleteAccessLogSubscription

- vpc-lattice:DeleteAccessLogSubscription
- logs:DeleteLogDelivery

`UpdateAccessLogSubscription`

- `vpc-lattice:UpdateAccessLogSubscription`
- `logs:UpdateLogDelivery`

Amazon VPC 格子的基於身份的政策

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

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

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

如需詳細資訊，請參閱服務授權參考中的 Amazon VPC Lights 的動作、資源和條件金鑰。

主題

- 政策最佳實務
- 完整存取權限的其他必要權限
- VPC 格子的身分識別原則範例

政策最佳實務

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

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

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

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

完整存取權限的其他必要權限

要使用 VPC 萊迪思集成的其他 AWS 服務以及整個 VPC 萊迪思功能套件，您必須具有特定的附加權限。這些權限不包含在VPCLatticeFullAccess受管理的策略中，因為副權限提升風險混淆。

您必須將下列原則附加至您的角色，並搭配VPCLatticeFullAccess受管理的原則使用。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "firehose:TagDeliveryStream",
                "lambda:AddPermission",
                "s3:PutBucketPolicy"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "logs:PutResourcePolicy"
            ],
            "Resource": "*",
            "Condition": {
```

```
                "ForAnyValue:StringEquals": {
                    "aws:CalledVia": [
                        "vpc-lattice.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:AttachRolePolicy",
                "iam:PutRolePolicy"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/vpc-
lattice.amazonaws.com/AWSServiceRoleForVpcLattice"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:AttachRolePolicy",
                "iam:PutRolePolicy"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/
delivery.logs.amazonaws.com/AWSServiceRoleForLogDelivery*"
        }
    ]
}
```

此原則提供下列其他權限：

- `iam:AttachRolePolicy`：可讓您將指定的受管政策附加到指定的 IAM 角色。
- `iam:PutRolePolicy`：可讓您新增或更新內嵌在指定 IAM 角色中的內嵌政策文件。
- `s3:PutBucketPolicy`：可讓您將儲存貯體政策套用至 Amazon S3 儲存貯體。
- `firehose:TagDeliveryStream`：可讓您新增或更新 Firehose 傳送串流的標籤。

VPC 格子的身分識別原則範例

主題

- 管理 VPC 與服務網路的關聯
- 建立服務網路的服務關聯

- 將標籤新增到資源
- 建立服務連結角色

管理 VPC 與服務網路的關聯

下列範例示範一項原則，該原則可讓具有此原則的使用者建立、更新和刪除 VPC 關聯與服務網路之間的權限，但僅限於條件中指定的虛擬私人 VPC 和服務網路。如需指定條件索引鍵的詳細資訊，請參閱 VPC 格子的原則條件金鑰。

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "vpc-lattice:CreateServiceNetworkVpcAssociation",
            "vpc-lattice:UpdateServiceNetworkVpcAssociation",
            "vpc-lattice:DeleteServiceNetworkVpcAssociation"
         ],
         "Resource": [
            "*"
         ],
         "Condition": {
            "StringEquals": {
               "vpc-lattice:ServiceNetworkArn": "arn:aws:vpc-lattice:us-
west-2:123456789012:servicenetwork/sn-903004f88example",
               "vpc-lattice:VpcId": "vpc-1a2b3c4d"
            }
         }
      }
   ]
}
```

建立服務網路的服務關聯

如果您不使用條件索引鍵來控制對 VPC Latds 資源的存取，則可以在Resource元素中指定資源的 ARN 來控制存取。

下列範例示範的原則會將服務關聯限制在具有此原則的使用者可以建立的服務網路，方法是指定可與 CreateServiceNetworkServiceAssociation API 動作搭配使用的服務網路和服務網路的 ARN。如需指定 ARN 值的詳細資訊，請參閱VPC 格子的政策資源。

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "vpc-lattice:CreateServiceNetworkServiceAssociation"
         ],
         "Resource": [
            "arn:aws:vpc-lattice:us-
west-2:123456789012:servicenetworkserviceassociation/*",
            "arn:aws:vpc-lattice:us-west-2:123456789012:service/svc-04d5cc9b88example",
            "arn:aws:vpc-lattice:us-west-2:123456789012:servicenetwork/
sn-903004f88example"
         ]
      }
   ]
}
```

將標籤新增到資源

下列範例示範一項政策，該原則授予具有此原則權限的使用者在 VPC Latds 資源上建立標籤的權限。

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "vpc-lattice:TagResource"
         ],
         "Resource": "arn:aws:vpc-lattice:us-west-2:123456789012:*/*"
      }
   ]
}
```

建立服務連結角色

VPC 萊迪思需要權限，才能在您的任何使用者第一次建 AWS 帳戶 立 VPC 萊迪思資源時建立服務連結角色。如果服務連結角色尚未存在，則 VPC Landers 會在您的帳戶中建立該角色。服務連結角色將權限授予 VPC 萊迪思，以便它可以代表您呼叫其他 AWS 服務 角色。

為能成功自動建立該角色，使用者必須已獲許可執行 `iam:CreateServiceLinkedRole` 動作。

```
"Action": "iam:CreateServiceLinkedRole"
```

下列範例示範一項政策，該原則授予具有此原則之權限的使用者，以便為 VPC Lagits 建立服務連結角色。

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": "iam:CreateServiceLinkedRole",
         "Resource": "arn:aws:iam::*:role/aws-service-role/vpc-lattice.amazonaws.com/
AWSServiceRoleForVpcLattice",
         "Condition": {
            "StringLike": {
               "iam:AWSServiceName":"vpc-lattice.amazonaws.com"
            }
         }
      }
   ]
}
```

針對 VPC 格子使用服務連結角色

Amazon VPC 萊迪斯使用服務連結角色來取得代表您呼叫其他人所需 AWS 服務 的許可。如需詳細資訊，請參閱《 IAM 使用者指南》中的使用服務連結角色。

VPC 格子的服務連結角色權限

VPC 萊迪格使用名為的服務連結角色。AWSServiceRoleForVpcLattice

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

- `vpc-lattice.amazonaws.com`

名為的角色權限原則AWSVpcLatticeServiceRolePolicy允許 VPC 萊迪思在命名AWS/VpcLattice空間中發佈 CloudWatch 指標。

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

```
        {
            "Effect": "Allow",
            "Action": "cloudwatch:PutMetricData",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": "AWS/VpcLattice"
                }
            }
        }
    ]
}
```

您必須設定許可，IAM 實體 (如使用者、群組或角色) 才可建立、編輯或刪除服務連結角色。如需詳細資訊，請參閱 IAM 使用者指南中的服務連結角色許可。

為 VPC 格子建立服務連結角色

您不需要手動建立一個服務連結角色。當您在 AWS Management Console、或 AWS API 中建立 VPC 萊迪思資源時 AWS CLI，VPC 萊迪思會為您建立服務連結角色。

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。當您創建 VPC 萊迪思資源時，VPC 萊迪思會再次為您創建服務鏈接的角色。

編輯 VPC 格子的服務連結角色

您可以編輯使AWSServiceRoleForVpcLattice用 IAM 的說明。如需詳細資訊，請參閱 IAM 使用者指南中的編輯服務連結角色。

刪除 VPC 格子的服務連結角色

如果您不再需要使用 Amazon VPC 格子，我們建議您刪除AWSServiceRoleForVpcLattice。

您只能在刪除所有 VPC 萊迪思資源之後刪除此服務連結角色。 AWS 帳戶

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

刪除服務連結角色後，VPC 萊迪思會在您的中建立 VPC 萊迪思資源時再次建立角色。 AWS 帳戶

VPC 萊迪思服務連結角色的支援區域

VPC 萊迪思支援在所有提供服務的區域中使用服務連結角色。

AWS 適用於 VPC 萊迪思的受管政策

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 AWS 服務 的 API 操作可用於現有服務時，最有可能更新 AWS 受管理策略。

如需詳細資訊，請參閱《IAM 使用者指南》中的 AWS 受管政策。

AWS 受管理原則：VPC LatticeFullAccess

此政策提供對 Amazon VPC 萊迪思的完整存取權限，以及對其他相依服務的有限存取權。它包括執行以下操作的權限：

- ACM — 擷取自訂網域名稱的 SSL/TLS 憑證 ARN。
- CloudWatch — 查看訪問日誌和監控數據.
- CloudWatch 防護記錄 — 設定存取記錄並傳送至防 CloudWatch 護記錄。
- Amazon EC2 — 擷取 EC2 執行個體和 VPC 的相關資訊，以建立目標群組和註冊目標。
- Elastic Load Balancing — 擷取 Application Load Balancer 的相關資訊，以將其註冊為目標。
- Firehose — 擷取用來儲存存取記錄之傳送串流的相關資訊。
- Lambda — 擷取 Lambda 函數的相關資訊，以將其註冊為目標。
- Amazon S3 — 擷取用於存放存取日誌的 S3 儲存貯體的相關資訊。

若要檢視此原則的權限，請參閱AWS 受管理原則參考LatticeFullAccess中的 VPC。

要使用 VPC 萊迪思集成的其他 AWS 服務以及整個 VPC 萊迪思功能套件，您必須具有特定的附加權限。這些權限不包含在`VPCLatticeFullAccess`受管理的策略中，因為副權限提升風險混淆。如需詳細資訊，請參閱 完整存取權限的其他必要權限。

AWS 受管理原則：VPC LatticeReadOnlyAccess

此政策提供 Amazon VPC 萊迪思的唯讀存取權限，以及對其他相依服務的有限存取。它包括執行以下操作的權限：

- ACM — 擷取自訂網域名稱的 SSL/TLS 憑證 ARN。
- CloudWatch — 查看訪問日誌和監控數據.
- CloudWatch 防護記錄 — 檢視存取記錄訂閱的記錄傳送資訊。
- Amazon EC2 — 擷取 EC2 執行個體和 VPC 的相關資訊，以建立目標群組和註冊目標。
- Elastic Load Balancing — 擷取應用程式負載平衡器的相關資訊。
- Firehose — 擷取有關傳送存取記錄傳送之傳送串流的資訊。
- Lambda — 檢視有關 Lambda 函數的資訊。
- Amazon S3 — 擷取 S3 儲存貯體的相關資訊以進行存取日誌交付。

若要檢視此原則的權限，請參閱AWS 受管理原則參考LatticeReadOnlyAccess中的 VPC。

AWS 受管理原則：VPC LatticeServicesInvokeAccess

此政策提供叫用 Amazon VPC 萊迪思服務的存取權。

若要檢視此原則的權限，請參閱AWS 受管理原則參考LatticeServicesInvokeAccess中的 VPC。

AWS 受管理的策略： AWSVpcLatticeServiceRolePolicy

此原則附加至名為的服務連結角色，AWSServiceRoleForVpcLattice以允許 VPC 萊迪思代表您執行動作。您無法將此政策連接至 IAM 實體。如需詳細資訊，請參閱 針對 VPC 格子使用服務連結角色。

若要檢視此原則的權限，請參閱AWS 受管理AWSVpcLatticeServiceRolePolicy的策略參考中的。

AWS 受管理原則的 VPC 萊迪思更新

檢視有關 VPC 萊迪思 AWS 受管政策更新的詳細資料，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 VPC Layds 使用者指南的 RSS 摘要。

變更	描述	日期
VPC LatticeFullAccess	VPC 萊迪思新增了一項新政策，以授予完整存取 Amazon VPC 萊迪斯和對其他相依服務的有限存取權限的許可。	2023 年 3 月 31 日
VPC LatticeReadOnlyAccess	VPC 萊迪思新增了一項新政策，以授予對 Amazon VPC 萊迪思的唯讀存取	2023 年 3 月 31 日

變更	描述	日期
	權限以及對其他相依服務的有限存取權限的許可。	
VPC LatticeServicesInvokeAccess	VPC 萊迪思新增一項新政策，以授與叫用 Amazon VPC 萊迪思服務的存取權。	2023 年 3 月 31 日
AWSVpcLatticeServiceRolePolicy	VPC 萊迪思將權限新增至其服務連結角色，以允許 VPC 萊迪思在命名空間中發佈 CloudWatch 指標。`AWS/VpcLattice` 此原`AWSVpcLatticeServiceRolePolicy` 則包含呼叫 CloudWatch PutMetricDataAPI 動作的權限。如需詳細資訊，請參閱 針對 VPC 格子使用服務連結角色。	2022 年 12 月 5 日
VPC 格子開始追蹤變更	VPC 萊迪思開始追蹤其 AWS 受管理政策的變更。	2022 年 12 月 5 日

Amazon VPC 萊迪格的合規驗證

第三方稽核員會評估 Amazon VPC 萊迪思的安全性和合規性，做為多個 AWS 合規計劃的一部分。

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 於資料的敏感性、公司的合規目標以及適用的法律和法規。AWS 提供下列資源以協助遵循法規：

- 安全性與合規性快速入門指南 — 這些部署指南討論架構考量，並提供部署以安全性和合規性 AWS 為重點的基準環境的步驟。

- 在 Amazon Web Services 上架構 HIPAA 安全性與合規性 — 本白皮書說明公司如何使用建立符合 HIPAA 資格的應 AWS 用程式。

> **Note**
>
> 並非所有人 AWS 服務 都符合 HIPAA 資格。如需詳細資訊，請參閱 HIPAA 資格服務參照。

- AWS 合規資源AWS — 此工作簿和指南集合可能適用於您的產業和所在地。
- AWS 客戶合規指南 — 透過合規的角度瞭解共同的責任模式。這份指南總結了在多個架構 (包括美國國家標準技術研究所 (NIST)、支付卡產業安全標準委員會 (PCI) 和國際標準化組織 (ISO)) 中，保 AWS 服務 護指引並對應至安全控制的最佳實務。
- 使用AWS Config 開發人員指南中的規則評估資源 — 此 AWS Config 服務會評估您的資源組態符合內部實務、產業準則和法規的程度。
- AWS Security Hub— 這 AWS 服務 提供了內部安全狀態的全面視圖 AWS。Security Hub 使用安全控制，可評估您的 AWS 資源並檢查您的法規遵循是否符合安全業界標準和最佳實務。如需支援的服務和控制清單，請參閱 Security Hub controls reference。
- 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。

使用介面端點存取 VPC 晶格 () PrivateLink

您可以透過建立介面 VPC 端點，在虛擬私人雲端和 Amazon VPC 萊迪格之間建立私有連線。介面端點採用這項技術 AWS PrivateLink，可讓您在沒有網際網路閘道、NAT 裝置、VPN 連線或 AWS Direct Connect 連線的情況下私密存取 VPC 萊迪思 API。VPC 中的執行個體不需要公有 IP 位址即可與 VPC 萊迪格 API 進行通訊。

每個介面端點由子網路中的一或多個網路介面來表示。

介面 VPC 端點的考量

在為 VPC 萊迪思設定介面 VPC 端點之前，請確保您使用 Amazon VPC 使用者指南中的介面 VPC 端點檢閱存取 AWS 服務。

VPC 萊迪思支援從您的 VPC 呼叫其所有 API 動作。

建立 VPC 晶格的介面 VPC 端點

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

使用以下服務名稱為 VPC 萊迪思建立 VPC 端點：

`com.amazonaws.region.vpc-lattice`

如果您為端點啟用私有 DNS，則可以使用該區域的預設 DNS 名稱向 VPC 萊迪思發出 API 請求，例如，`vpc-lattice.us-east-1.amazonaws.com`。

如需詳細資訊，請參閱 Amazon VPC 使用者指南中的使用介面 VPC 端點存取 AWS 服務。

Amazon VPC 格子的彈性

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，這些區域與低延遲、高輸送量和高冗餘網路相連。

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。

Amazon VPC 格子的基礎設施安全

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

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

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

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

監控亞馬遜 VPC 晶格

使用本節中的功能來監控您的 Amazon VPC 萊迪思服務網路、服務、目標群組和 VPC 連線。

目錄

CloudWatch VPC 格子的指標

Amazon VPC 萊迪思會將與您的目標群組和服務相關的資料傳送到 Amazon CloudWatch，並將其處理為可讀且近乎即時的指標。這些指標會保留 15 個月，因此您可以存取歷史資訊，並更好地瞭解 Web 應用程式或服務的執行情況。您也可以設定警報監看特定閾值，在達到閾值發出通知或採取動作。如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南。

Amazon VPC 萊迪斯在您的AWS帳戶中使用服務連結角色，將指標傳送到 Amazon。 CloudWatch如需詳細資訊，請參閱針對 VPC 格子使用服務連結角色。

目錄

查看亞馬遜 CloudWatch 指標

您可以使用 CloudWatch 主控台或檢視目標群組和服務的 Amazon CloudWatch 指標AWS CLI。

使用 CloudWatch 主控台檢視指標

1. 在以下位置打開亞馬遜 CloudWatch 控制台 https://console.aws.amazon.com/cloudwatch/。
2. 在導覽窗格中，選擇 Metrics (指標)。
3. 选择 `AWS/VpcLattice` 命名空间。
4. (選擇性) 若要檢視所有維度的量度，請在搜尋欄位中輸入其名稱。
5. (選用) 若要根據維度來篩選，請選取下列其中一項：

- 若只要顯示針對目標群組報告的測量結果，請選擇「目標群組」。若要檢視單一目標群組的測量結果，請在搜尋欄位中輸入其名稱。
- 若只要顯示針對您的服務回報的指標，請選擇「服務」。若要檢視單一服務的測量結果，請在搜尋欄位中輸入其名稱。

若要使用 AWS CLI

使用下列清單CloudWatch 公制指AWS CLI令列出可用的量度：

```
aws cloudwatch list-metrics --namespace AWS/VpcLattice
```

如需有關每個量度及其維度的資訊，請參閱目標群組量度和服務指標。

目標群組量度

VPC 萊迪思會在 AWS/VpcLattice Amazon CloudWatch 命名空間中自動存放與目標群組相關的指標。如需目標群組的詳細資訊，請參閱VPC 格子中的目標群體。

您可能想要監督HTTP code目標群組的RequestTime測量結果。您可以依可用區域 (AZ) 篩選這些測量結果，以判斷目標群組所在的 AZ。

指標	描述
TotalConnectionCount	連線總數。 報告準則 • 始終從資源接收流量開始報告（無論是零值還是非零值）。 報告頻率 • 每分鐘一次 統計 • 最有用的統計數據是Sum。 Dimensions (尺寸)

指標	描述
	• 名稱：TargetGroup ，值：目標群組的名稱。 • 名稱：AvailabilityZone ，值：目標群組所在的 AZ。
ActiveConnectionCount	作用中的連線。 報告準則 • 始終從資源接收流量開始報告（無論是零值還是非零值）。 報告頻率 • 每分鐘一次 統計 • 最有用的統計數據是Sum。 Dimensions (尺寸) • 名稱：TargetGroup ，值：目標群組的名稱。 • 名稱：AvailabilityZone ，值：目標群組所在的 AZ。

指標	描述
ConnectionErrorCount	連線失敗總數。 報告準則 • 始終從資源接收流量開始報告（無論是零值還是非零值）。 報告頻率 • 每分鐘一次 統計 • 最有用的統計數據是Sum。 Dimensions (尺寸) • 名稱：TargetGroup ，值：目標群組的名稱。 • 名稱：AvailabilityZone ，值：目標群組所在的 AZ。

指標	描述
HTTP1_ConnectionCount	HTTP/1.1 連線總數。 報告準則 • 始終從資源接收流量開始報告（無論是零值還是非零值）。 報告頻率 • 每分鐘一次 統計 • 最有用的統計數據是Sum。 Dimensions (尺寸) • 名稱：TargetGroup ，值：目標群組的名稱。 • 名稱：AvailabilityZone ，值：目標群組所在的 AZ。

指標	描述
HTTP2_ConnectionCount	HTTP/2 連線總數。 報告準則 • 始終從資源接收流量開始報告（無論是零值還是非零值）。 報告頻率 • 每分鐘一次 統計 • 最有用的統計數據是Sum。 Dimensions (尺寸) • 名稱：TargetGroup ，值：目標群組的名稱。 • 名稱：AvailabilityZone ，值：目標群組所在的 AZ。

指標	描述
ConnectionTimeoutCount	連線連線逾時總數。 報告準則 • 始終從資源接收流量開始報告（無論是零值還是非零值）。 報告頻率 • 每分鐘一次 統計 • 最有用的統計數據是Sum。 Dimensions (尺寸) • 名稱：TargetGroup ，值：目標群組的名稱。 • 名稱：AvailabilityZone ，值：目標群組所在的 AZ。

指標	描述
TotalReceivedConnectionBytes	接收的連線位元組總數。 報告準則 • 始終從資源接收流量開始報告（無論是零值還是非零值）。 報告頻率 • 每分鐘一次 統計 • 最有用的統計數據是Sum。 Dimensions (尺寸) • 名稱：TargetGroup ，值：目標群組的名稱。 • 名稱：AvailabilityZone ，值：目標群組所在的 AZ。

指標	描述
TotalSentConnectionBytes	總傳送連線位元組。 報告準則 • 始終從資源接收流量開始報告（無論是零值還是非零值）。 報告頻率 • 每分鐘一次 統計 • 最有用的統計數據是Sum。 Dimensions (尺寸) • 名稱：TargetGroup ，值：目標群組的名稱。 • 名稱：AvailabilityZone ，值：目標群組所在的 AZ。

指標	描述
TotalRequestCount	請求總數。 報告準則 • 始終從資源接收流量開始報告（無論是零值還是非零值）。 報告頻率 • 每分鐘一次 統計 • 最有用的統計數據是Sum。 Dimensions (尺寸) • 名稱：TargetGroup ，值：目標群組的名稱。 • 名稱：AvailabilityZone ，值：目標群組所在的 AZ。

指標	描述
ActiveRequestCount	作用中要求總數。 報告準則 • 始終從資源接收流量開始報告（無論是零值還是非零值）。 報告頻率 • 每分鐘一次 統計 • 最有用的統計數據是Sum。 Dimensions (尺寸) • 名稱：TargetGroup ，值：目標群組的名稱。 • 名稱：AvailabilityZone ，值：目標群組所在的 AZ。

指標	描述
RequestTime	請求時間（毫秒）。 報告準則 • 始終從資源接收流量開始報告（無論是零值還是非零值）。 報告頻率 • 每分鐘一次 統計 • 最有用的統計數據是Average和pNN.NN（百分位數）。 Dimensions (尺寸) • 名稱：TargetGroup ，值：目標群組的名稱。 • 名稱：AvailabilityZone ，值：目標群組所在的 AZ。

指標	描述
HTTPCode_2XX_Count, HTTPCode_3XX_Count, HTTPCode_4XX_Count, HTTPCode_5XX_Count	彙總 HTTP 回應代碼。 報告準則 • 始終從資源接收流量開始報告（無論是零值還是非零值）。 報告頻率 • 每分鐘一次 統計 • 最有用的統計數據是Sum。 Dimensions (尺寸) • 名稱：TargetGroup ，值：目標群組的名稱。 • 名稱：AvailabilityZone ，值：目標群組所在的 AZ。

指標	描述
TLSConnectionErrorCount	TLS 連線錯誤總數不包括失敗的憑證驗證。 報告準則 • 始終從資源接收流量開始報告（無論是零值還是非零值）。 報告頻率 • 每分鐘一次 統計 • 最有用的統計數據是Sum。 Dimensions (尺寸) • 名稱：TargetGroup ，值：目標群組的名稱。 • 名稱：AvailabilityZone ，值：目標群組所在的 AZ。

指標	描述
TotalTLSConnection HandshakeCount	完全成功的 TLS 連線交握。 報告準則 • 始終從資源接收流量開始報告（無論是零值還是非零值）。 報告頻率 • 每分鐘一次 統計 • 最有用的統計數據是Sum。 Dimensions (尺寸) • 名稱：TargetGroup ，值：目標群組的名稱。 • 名稱：AvailabilityZone ，值：目標群組所在的 AZ。

服務指標

VPC 萊迪思會在 AWS/VpcLattice Amazon CloudWatch 命名空間中自動存放與服務相關的指標。如需服務的詳細資訊，請參閱VPC 格子的服務。

您可能想要監視HTTP code和服務的RequestTime指標。您可以依可用區域 (AZ) 篩選這些指標，以判斷服務所在的 AZ。

指標	描述
RequestTimeoutCount	等待回應逾時的要求總數。 報告準則 • 始終從資源接收流量開始報告（無論是零值還是非零值）。

指標	描述
	報告頻率 • 每分鐘一次 統計 • 最有用的統計數據是Sum。 Dimensions (尺寸) • 名稱：Service，值：服務的識別碼。 • 名稱：AvailabilityZone ，值：目標群組所在的 AZ。
TotalRequestCount	請求總數。 報告準則 • 始終從資源接收流量開始報告（無論是零值還是非零值）。 報告頻率 • 每分鐘一次 統計 • 最有用的統計數據是Sum。 Dimensions (尺寸) • 名稱：Service，值：服務的識別碼。 • 名稱：AvailabilityZone ，值：目標群組所在的 AZ。

指標	描述
RequestTime	請求時間（毫秒）。 報告準則 • 始終從資源接收流量開始報告（無論是零值還是非零值）。 報告頻率 • 每分鐘一次 統計 • 最有用的統計數據是Average和pNN.NN（百分位數）。 Dimensions (尺寸) • 名稱：Service，值：服務的識別碼。 • 名稱：AvailabilityZone ，值：目標群組所在的 AZ。

指標	描述
HTTPCode_2XX_Count ，HTTPCode_3XX_Count ，HTTPCode_4XX_Count ，HTTPCode_5XX_Count	彙總 HTTP 回應代碼。 報告準則 • 始終從資源接收流量開始報告（無論是零值還是非零值）。 報告頻率 • 每分鐘一次 統計 • 最有用的統計數據是Sum。 Dimensions (尺寸) • 名稱：Service，值：服務的識別碼。 • 名稱：AvailabilityZone ，值：目標群組所在的 AZ。

VPC 格子的存取記錄

存取記錄會擷取有關 VPC 萊迪思服務的詳細資訊。您可以使用這些存取記錄來分析流量模式並稽核網路中的所有服務。

存取記錄是選擇性的，預設為停用。啟用存取記錄後，您可以隨時停用它們。

定價

發佈存取記錄時會收取費用。代表您 AWS 原生發佈的記錄稱為付費記錄。如需有關付費日誌定價的詳細資訊，請參閱 Amazon CloudWatch 定價、選擇日誌，然後在付費日誌下檢視定價。

目錄

- 訪問日誌內容
- 疑難排解存取記

啟用存取日誌所需的 IAM 許可

若要啟用存取記錄並將記錄傳送至其目的地，您必須在政策中將下列動作連接至您正在使用的 IAM 使用者、群組或角色。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Sid": "ManageVPCLatticeAccessLogSetup",
            "Action": [
                "logs:CreateLogDelivery",
                "logs:GetLogDelivery",
                "logs:UpdateLogDelivery",
                "logs:DeleteLogDelivery",
                "logs:ListLogDeliveries",
                "vpc-lattice:CreateAccessLogSubscription",
                "vpc-lattice:GetAccessLogSubscription",
                "vpc-lattice:UpdateAccessLogSubscription",
                "vpc-lattice:DeleteAccessLogSubscription",
                "vpc-lattice:ListAccessLogSubscriptions"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

如需詳細資訊，請參閱《AWS Identity and Access Management 使用者指南》中的新增和移除 IAM 身分許可。

更新附加至您正在使用之 IAM 使用者、群組或角色的政策後，請移至啟用存取日誌。

存取記錄目的地

您可以將存取記錄傳送至下列目的地。

Amazon CloudWatch 日誌

- VPC 萊迪思通常會在 2 分鐘內將記 CloudWatch 錄傳送到記錄檔。不過，請記住，實際的記錄傳送時間是最佳的基礎，而且可能會有額外的延遲。
- 如果 CloudWatch 記錄群組沒有特定權限，則會自動建立資源原則並新增至記錄群組。如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南中的傳送至 CloudWatch 日誌的日誌。
- 您可以在主控台的 [記錄群組 CloudWatch] 底下找到傳送至的存取記 CloudWatch 錄。如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南中的檢視傳送至 CloudWatch 日誌的日誌資料。

Amazon S3

- VPC 萊迪思通常會在 6 分鐘內將日誌交付到 Amazon S3。不過，請記住，實際的記錄傳送時間是最佳的基礎，而且可能會有額外的延遲。
- 如果儲存貯體沒有特定許可，系統會自動建立儲存貯體政策並新增至您的 Amazon S3 儲存貯體。如需詳細資訊，請參閱 Amazon CloudWatch使用者指南中的傳送到 Amazon S3 的日誌。
- 傳送至 Amazon S3 的存取日誌會使用下列命名慣例：

```
[bucket]/[prefix]/AWSLogs/[accountId]/VpcLattice/AccessLogs/[region]/[YYYY/
MM/DD]/[resource-id]/[accountId]_VpcLatticeAccessLogs_[region]_[resource-
id]_YYYYMMDDTHHmmZ_[hash].json.gz
```

Amazon Data Firehose

- VPC 萊迪思通常會在 2 分鐘內將日誌交付給 Firehose。不過，請記住，實際的記錄傳送時間是最佳的基礎，而且可能會有額外的延遲。
- 系統會自動建立服務連結角色，授與 VPC 萊迪思傳送存取記錄的權限。 Amazon Data Firehose為了成功自動建立該角色，使用者必須有 `iam:CreateServiceLinkedRole` 動作的許可。如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南 Amazon Data Firehose中的傳送日誌。
- 如需檢視傳送至的日誌的詳細資訊 Amazon Data Firehose，請參閱Amazon Data Firehose 開發人員指南中的監控 Amazon Kinesis Data Streams。

啟用存取日誌

完成下列程序來設定存取日誌，以擷取存取日誌並將其傳送至您選擇的目的地。

目錄

- 使用主控台啟用存取記錄
- 使用啟用存取記錄 AWS CLI

使用主控台啟用存取記錄

您可以在建立期間啟用服務網路或服務的存取記錄。您也可以在建立服務網路或服務之後啟用存取記錄，如下列程序所述。

使用主控台建立基本服務

1. 前往 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 選取服務網路或服務。
3. 選擇 [動作]、[編輯記錄設定]
4. 開啟存取記錄切換開關。
5. 新增存取記錄的傳送目的地，如下所示：
   - 選取CloudWatch 記錄群組，然後選擇記錄群組。若要建立記錄群組，請在中選擇 [建立記錄群組] CloudWatch。
   - 選取 S3 儲存貯體並輸入 S3 儲存貯體路徑，包括任何前置詞。若要搜尋 S3 儲存貯體，請選擇瀏覽 S3。
   - 選取 Kinesis Data Firehose 傳送串流，然後選擇交付串流。若要建立交付串流，請選擇在 Kinesis 中建立交付串流。
6. 選擇儲存變更。

使用啟用存取記錄 AWS CLI

使用 CLI 命令可啟create-access-log-subscription用服務網路或服務的存取記錄。

訪問日誌內容

下表說明存取日誌項目的欄位。

欄位	描述	格式
hostHeader	請求的權威標頭。	string

欄位	描述	格式
sslCipher	用來建立用戶端 TLS 連線之密碼集的 OpenSSL 名稱。	string
serviceNetworkArn	服務網絡 ARN。	*arn: aws: vpc-##:##:## #:####/ID*
resolvedUser	啟用驗證並完成驗證時，使用者的 ARN。	空 | ARN |「匿名」|「未知」
authDeniedReason	啟用驗證時拒絕存取的原因。	空 |「服務」|「網絡」|「身份」
requestMethod	請求的方法頭。	string
targetGroupArn	目標主機所屬的目標主機群組。	string
tlsVersion	TLS 版本。	*TLSv x*
userAgent	使用者代理程式標頭。	string
ServerNameIndication	[僅限 HTTPS] 針對伺服器名稱指示 (SNI) 在 ssl 連線通訊端上設定的值。	string
destinationVpcId	目的地 VPC 識別碼。	*vpc*
sourceIpPort	來源的 IP 位址和:連接埠。	*IP*: *###*
targetIpPort	目標的 IP 位址和連接埠。	*IP*: *###*
serviceArn	該服務 ARN。	*arn: AW: vpc-##:##:## #:##/###*
sourceVpcId	來源 VPC 識別碼。	*vpc*
requestPath	請求的路徑。	LatticePath? : *##*
startTime	請求開始時間。	*#-##-# T #####SS Z*

欄位	描述	格式
protocol	通訊協定。目前無論是 HTTP /1.1 或 HTTP/2。	string
responseCode	HTTP 回應代碼。只會記錄最終標頭的回應碼。如需詳細資訊，請參閱 疑難排解存取記。	integer
bytesReceived	接收到的主體和標頭字節。	integer
bytesSent	正文和頭字節發送。	integer
duration	從開始時間到最後一個位元組輸出之要求的總持續時間 (以毫秒為單位)。	integer
requestToTargetDuration	從開始時間到傳送至目標的最後一個位元組的要求總持續時間 (以毫秒為單位)。	integer
responseFromTargetDuration	從目標主機讀取的第一個位元組到傳送至用戶端的最後一個位元組的要求總持續時間 (以毫秒為單位)。	integer
grpcResponseCode	gRPC 響應代碼。如需詳細資訊，請參閱狀態碼及其在 gRPC 中的使用。只有在服務支援 gRPC 時，才會記錄此欄位。	integer
callerPrincipal	已驗證的主體。	string
callerX509SubjectCN	主旨名稱 (CN)。	string
callerX509IssuerOU	發行者 (OU)。	string
callerX509SANNameCN	發行人替代（名稱/CN）。	string

欄位	描述	格式
callerX509SANDNS	主體替代名稱 (DNS)。	string
callerX509SANURI	主旨替代名稱 (URI)。	string
sourceVpcArn	產生請求所在的 VPC 的 ARN。	*arn: aw:ec2: ##:##:vpc / ID*

範例

以下為日誌項目的範例。

```
{
    "hostHeader": "example.com",
    "sslCipher": "-",
    "serviceNetworkArn": "arn:aws:vpc-lattice:us-west-2:123456789012:servicenetwork/
svn-1a2b3c4d",
    "resolvedUser": "Unknown",
    "authDeniedReason": "null",
    "requestMethod": "GET",
    "targetGroupArn": "arn:aws:vpc-lattice:us-west-2:123456789012:targetgroup/
tg-1a2b3c4d",
    "tlsVersion": "-",
    "userAgent": "-",
    "serverNameIndication": "-",
    "destinationVpcId": "vpc-0abcdef1234567890",
    "sourceIpPort": "178.0.181.150:80",
    "targetIpPort": "131.31.44.176:80",
    "serviceArn": "arn:aws:vpc-lattice:us-west-2:123456789012:service/svc-1a2b3c4d",
    "sourceVpcId": "vpc-0abcdef1234567890",
    "requestPath": "/billing",
    "startTime": "2023-07-28T20:48:45Z",
    "protocol": "HTTP/1.1",
    "responseCode": 200,
    "bytesReceived": 42,
    "bytesSent": 42,
    "duration": 375,
    "requestToTargetDuration": 1,
    "responseFromTargetDuration": 1,
    "grpcResponseCode": 1
```

```
}
```

疑難排解存取記

本節包含您可能在存取記錄中看到的 HTTP 錯誤碼的說明。

錯誤代碼	可能原因
HTTP 400：錯誤的請求	• 用戶端傳送格式錯誤的要求，不符合 HTTP 規格。 • 整個請求標頭的請求標頭超過 60K 或超過 100 個標頭。 • 用戶端在傳送完整請求內文之前關閉了連線。
HTTP 403：禁止	已針對服務設定驗證，但未驗證或授權傳入要求。
不存在的服務	您嘗試連線到不存在或未註冊到正確服務網路的服務。
HTTP 500：內部伺服器錯誤	VPC 萊迪斯遇到錯誤，例如無法連接到目標。
HTTP 502：無效的閘道	VPC 格子遇到錯誤。

CloudTrail VPC 格子的日誌

AWS CloudTrail是提供使用者、角色或AWS服務所採取之動作記錄的AWS服務。 CloudTrail 將 VPC 格子的 API 呼叫擷取為事件。 CloudTrail 在您創建它AWS 帳戶時啟用它。當 VPC Ratters 中發生活動時，該活動會與事件歷史記錄中的其他AWS服務 CloudTrail 事件一起記錄為事件。擷取的呼叫包括來自 VPC 萊迪思主控台的呼叫，以及對 VPC 萊迪思 API 作業的程式碼呼叫。如需有關 CloudTrail 的詳細資訊，請參閱《使用者指南》AWS CloudTrail。

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

若要監視其他動作，請使用存取記錄。如需詳細資訊，請參閱存取日誌。

瞭解 VPC 格子記錄檔項目

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，包括有關請求的操作，動作的日期和時

間，請求參數等信息。 CloudTrail 日誌文件不是公共 API 調用的有序堆棧跟踪，因此它們不會以任何特定順序顯示。

如需記錄中關於索引鍵值配對的資訊，請參閱《AWS CloudTrail使用指南》中的CloudTrail 記錄內容。

以下是呼叫 CreateServiceAPI 動作的範例記錄項目。

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "abcdef01234567890",
    "arn": "arn:abcdef01234567890",
    "accountId": "abcdef01234567890",
    "accessKeyId": "abcdef01234567890",
    "sessionContext": {
        "sessionIssuer": {
            "type": "Role",
            "principalId": "abcdef01234567890",
            "arn": "arn:abcdef01234567890",
            "accountId": "abcdef01234567890",
            "userName": "abcdef01234567890"
        },
        "webIdFederationData": {},
        "attributes": {
            "creationDate": "2022-08-16T03:34:54Z",
            "mfaAuthenticated": "false"
        }
    }
  },
  "eventTime": "2022-08-16T03:36:12Z",
  "eventSource": "vpc-lattice.amazonaws.com",
  "eventName": "CreateService",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "abcdef01234567890",
  "userAgent": "abcdef01234567890",
  "requestParameters": {
    "name": "rates-service"
  },
  "responseElements": {
    "name": "rates-service",
    "id": "abcdef01234567890",
    "arn": "arn:abcdef01234567890",
    "status": "CREATE_IN_PROGRESS"
```

```
  },
  "requestID": "abcdef01234567890",
  "eventID": "abcdef01234567890",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "abcdef01234567890",
  "eventCategory": "Management"
}
```

以下是呼叫 DeleteServiceAPI 動作的範例記錄項目。

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "abcdef01234567890",
    "arn": "arn:ABCXYZ123456",
    "accountId": "abcdef01234567890",
    "accessKeyId": "abcdef01234567890",
    "sessionContext": {
        "sessionIssuer": {
            "type": "Role",
            "principalId": "abcdef01234567890",
            "arn": "arn:aws:iam::AIDACKCEVSQ6C2EXAMPLE:role/Admin",
            "accountId": "abcdef01234567890",
            "userName": "Admin"
        },
        "webIdFederationData": {},
        "attributes": {
            "creationDate": "2022-10-27T17:42:36Z",
            "mfaAuthenticated": "false"
        }
    }
  },
  "eventTime": "2022-10-27T17:56:41Z",
  "eventSource": "vpc-lattice.amazonaws.com",
  "eventName": "DeleteService",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "72.21.198.64",
  "userAgent": "abcdef01234567890",
  "requestParameters": {
    "serviceIdentifier": "abcdef01234567890"
```

```
  },
  "responseElements": {
    "name": "test",
    "id": "abcdef01234567890",
    "arn": "arn:abcdef01234567890",
    "status": "DELETE_IN_PROGRESS"
  },
  "requestID": "abcdef01234567890",
  "eventID": "abcdef01234567890",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "abcdef01234567890",
  "eventCategory": "Management"
}
```

Amazon VPC 格子的配額

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。您可以請求提高某些配額，而其他配額無法提高。

若要檢視 VPC 格子的配額，請開啟 Service Quotas 主控台。在導航窗格中，選擇AWS 服務並選擇 VPC 格子。

若要要求提高配額，請連絡 Sup AWS port 部門，或參閱 Service Quotas 使用者指南中的要求提高配額。

您 AWS 帳戶 有以下與 VPC 格子相關的配額。

名稱	預設	可調整	描述
驗證原則大小	每個支持的地區：10 千字節	否	驗證策略中 JSON 文件的最大大小。
每個服務的監聽	每個支持地區：2	是	您可以為服務建立的監聽器數目上限。如需額外的容量和上限增加，請聯絡 Sup AWS port 部門。
每個監聽器的規	每個受支援的區域：5	是	您可以為服務接聽程式定義的規則數目上限。如需額外的容量和上限增加，請聯絡 Sup AWS port 部門。
每個關聯的安全群組	每個受支援的區域：5	否	您可以新增至 VPC 與服務網路之間關聯的安全群組數目上限。
每個服務網路的服務關聯	每個受支援的區域：500	是	可與單一服務網路建立關聯的服務數目上限。如需額外的容量和上限增加，

名稱	預設	可調整	描述
			請聯絡 Sup AWS port 部門。
每個地區的服務網路	每個受支援的區域：10	是	每個區域的服務網路數目上限。如需額外的容量和上限增加，請聯絡 Sup AWS port 部門。
每個地區的服務	每個受支援的區域：500	是	每個區域的服務數目上限。如需額外的容量和上限增加，請聯絡 Sup AWS port 部門。
每個區域的目標群組	每個受支援的區域：500	是	每個區域的目標群組數目上限。如需額外的容量和上限增加，請聯絡 Sup AWS port 部門。
每個服務的目標群組	每個受支援的區域：5	是	可與服務關聯的目標群組數目上限。如需額外的容量和上限增加，請聯絡 Sup AWS port 部門。
每個目標群組的目標	每個受支援的區域：1,000	是	可與單一目標群組相關聯的目標數目上限。如需額外的容量和上限增加，請聯絡 Sup AWS port 部門。
每個服務網路的 VPC 關聯	每個受支援的區域：500	是	可與單一服務網路建立關聯的 VPC 數目上限。如需額外的容量和上限增加，請聯絡 Sup AWS port 部門。

以下限制也適用。

限制	值
每個可用區域每個服務的頻寬	10 Gbps
每個連接的最大傳輸單元 (MTU)	八百個字節
每個可用區域每個服務的每秒要求數	10,000

VPC 格子使用者指南的文件歷史記錄

下表說明 VPC 格子的文件版本。

變更	描述	日期
Lambda 事件結構版本	VPC 格子現在支援新版本的 Lambda 事件結構。	2023 年 9 月 7 日
Support 共用 VPC	參與者可以在共用的 VPC 中建立 VPC 萊迪思目標群組。	2023 年 7 月 5 日
一般可用性版本	VPC 萊迪格使用者指南發行的一般可用性 (GA)	2023 年 3 月 31 日
VPC 萊迪思現在會報告其AWS受管理政策的變更	對受管理政策的變更會在「安全性」一章中的「VPC 萊迪思的AWS受管理策略」中報告。	2023 年 3 月 29 日
Support 應用程式負載平衡器目標類型	VPC 萊迪思現在支援建立 Application Load Balancer 類型的目標群組。	2023 年 3 月 29 日
Support 所有執行個體類型	VPC 萊迪思現在支援所有執行個體類型。	2023 年 3 月 27 日
IPv6 支援	VPC 晶格現在同時支援 IPv4 和 IPv6 的 IP 目標群組。	2023 年 3 月 27 日
用於健康檢查的 HTTP2 通訊協定版	目標群組通訊協定版本為 HTTP2 時，現在支援 Health 檢查。	2023 年 3 月 27 日
修正接聽程式規則的回應動作	VPC 萊迪思服務的接聽程式現在除了轉寄動作外，還支援固定回應動作。	2023 年 3 月 27 日
Support 自訂網域名稱	您現在可以為您的 VPC 萊迪思服務設定自訂網域名稱	2023 年 2 月 14 日

BYOC Support (攜帶您自己的憑證)	VPC 萊迪思支援在 ACM 中使用您自己的 SSL/TLS 憑證來進行自訂網域名稱。	2023 年 2 月 14 日
VPC Ladits 現在會報告不受支援執行個體類型的更新清單	另外三個執行個體已新增至不支援的執行個體清單。	2023 年 1 月 26 日
VPC 萊迪思現在會報告其AWS受管理政策的變更	自 2022 年 12 月 5 日起，「安全性」一章中的「VPC 萊迪思的AWS受管理策略」主題中報告了對受管理策略的變更。列出的第一個變更是新增 CloudWatch 監視所需的權限。	2022 年 12 月 5 日
初始版本	VPC 格子使用者指南的初始版本	2022 年 12 月 5 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。