aws

使用者指南

AWS Direct Connect

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Direct Connect: 使用者指南

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商標和商業外觀不得用於任何非 Amazon 的產品或服務，也不能以任何可能造成客戶混淆、任何貶低或使 Amazon 名譽受損的方式使用 Amazon 的商標和商業外觀。所有其他非 Amazon 擁有的商標均為其各自擁有者的財產，這些擁有者可能附屬於 Amazon，或與 Amazon 有合作關係，亦或受到 Amazon 贊助。

Table of Contents

什麼是 AWS Direct Connect？ 1
Direct Connect 元件 1
網路需求 2
支援的 Direct Connect 虛擬介面類型 3
Direct Connect 定價 4
存取遠端 AWS 區域 4
存取遠端區域中的公有服務 4
存取遠端區域中VPCs 5
網路對 Amazon VPC 連線選項 5
路由政策和 BGP 社群 5
公用虛擬介面路由政策 5
公有虛擬介面 BGP 社群 7
私有虛擬介面和傳輸虛擬介面路由政策 8
私有虛擬介面路由範例 10
AWS Direct Connect 彈性工具組 12
先決條件 13
最大彈性 15
高彈性 16
開發和測試 16
傳統 17
先決條件 17
容錯移轉測試 18
設定最大彈性 18
步驟 1：註冊 AWS 18
步驟 2：設定彈性模型 20
步驟 3：建立您的虛擬介面 21
步驟 4：驗證您的虛擬介面彈性組態 27
步驟 5：驗證您的虛擬介面連線能力 27
設定高彈性 28
步驟 1：註冊 AWS 28
步驟 2：設定彈性模型 30
步驟 3：建立您的虛擬介面 31
步驟 4：驗證您的虛擬介面彈性組態 38
步驟 5：驗證您的虛擬介面連線能力 38

設定開發和測試彈性 38
步驟 1：註冊 AWS 39
步驟 2：設定彈性模型 40
步驟 3：建立虛擬介面 41
步驟 4：驗證您的虛擬介面彈性組態 47
步驟 5：驗證您的虛擬介面 47
設定 Classic 連線 48
步驟 1：註冊 AWS 48
步驟 2：請求 AWS Direct Connect 專用連線 50
(專用連線) 步驟 3：下載 LOA-CFA 51
步驟 4：建立虛擬介面 52
步驟 5：下載路由器組態 58
步驟 6：驗證您的虛擬介面 59
(建議) 步驟 7：設定備援連線 60
Direct Connect 容錯移轉測試 61
測試歷史記錄 62
驗證許可 62
啟動虛擬介面容錯移轉測試 62
檢視虛擬介面容錯移轉測試歷史記錄 63
停止虛擬介面容錯移轉測試 64
Direct Connect 維護 65
規劃的維護 65
..... 65
緊急維護 66
第三方維護 66
維護事件準備 66
彈性驗證 67
維護事件延遲 67
MAC 安全性 (MACsec) 68
MACsec 概念 68
MACsec 金鑰輪換 69
支援的連線 70
專用連線 70
LAG 71
服務連結角色 71
MACsec 預先共用 CKN/CAK 金鑰考量 71

在專用連線上開始使用 MACsec 72
建立連線 72
（選用）建立 LAG 72
將 CKN/CAK 與連線或 LAG 建立關聯 72
設定您的內部部署路由器 72
移除 CKN/CAK 與連線或 LAG 之間的關聯 73
專用和託管連線 74
專用連線 74
授權書和連線設施指派 (LOA-CFA) 75
使用連線精靈建立連線 76
建立傳統連線 78
下載 LOA-CFA 79
將 MACsec CKN/CAK 與連線建立關聯 80
移除 MACsec 私密金鑰和連線之間的關聯 81
託管連線 81
接受託管連線 82
刪除一個連線 83
更新連線 84
檢視連線詳細資訊 85
交叉連線 86
連線選項 86
美國東部 (俄亥俄) 88
美國東部 (維吉尼亞北部) 88
美國西部 (加利佛尼亞北部) 89
美國西部 (奧勒岡) 90
非洲 (開普敦) 91
亞太區域 (雅加達) 91
亞太區域 (孟買) 91
亞太區域 (首爾) 92
亞太區域 (新加坡) 92
亞太區域 (悉尼) 93
亞太區域 (東京) 93
加拿大 (中部) 94
中國 (北京) 94
中國 (寧夏) 94
歐洲 (法蘭克福) 95

歐洲 (愛爾蘭) 96
歐洲 (米蘭) 96
歐洲 (倫敦) 96
Europe (Paris) 97
歐洲 (斯德哥爾摩) 97
歐洲 (蘇黎世) 97
以色列 (特拉維夫) 97
Middle East (Bahrain) 98
中東 (阿拉伯聯合大公國) 98
南美洲 (聖保羅) 98
AWS GovCloud （美國東部） 99
AWS GovCloud （美國西部） 99
虛擬介面和託管虛擬介面 100
公有虛擬介面字首公告規則 100
SiteLink 101
虛擬介面的先決條件 102
私有虛擬介面或傳輸虛擬介面的 MTUs 107
虛擬介面 108
將虛擬介面傳輸到 Direct Connect 閘道的先決條件 108
建立公有虛擬介面 109
建立私有虛擬介面。 110
建立傳輸虛擬介面以連往 Direct Connect 閘道 113
下載路由組態檔案 115
託管虛擬介面 116
建立私有託管虛擬介面 120
建立公有託管虛擬介面 122
建立託管傳輸虛擬介面 123
檢視虛擬介面詳細資訊 125
加入 BGP 對等 126
刪除 BGP 對等 128
設定私有虛擬介面的 MTU 128
新增或移除虛擬介面標籤 129
刪除虛擬介面 130
接受託管虛擬介面 130
遷移虛擬介面 131
連結彙總群組 (LAGs) 133

MACsec 考量 134
建立 LAG 135
檢視 LAG 詳細資訊 137
更新 LAG 138
將連線與 LAG 產生關聯。 139
取消連線與 LAG 的關聯。 140
將 MACsec CKN/CAK 與 LAG 產生關聯 140
移除 MACsec 私密金鑰和 LAG 之間的關聯 141
刪除 LAG 142
閘道 143
Direct Connect 閘道 143
案例 145
建立 Direct Connect 閘道 148
從虛擬私有閘道遷移至 Direct Connect 閘道 149
刪除 Direct Connect 閘道 149
虛擬私有閘道關聯 150
建立虛擬私有閘道 151
關聯或取消關聯虛擬私有閘道 153
建立 Direct Connect 閘道的私有虛擬介面 154
跨帳戶建立虛擬私有閘道的關聯 156
傳輸閘道關聯 156
跨帳戶建立傳輸閘道關聯 157
將傳輸閘道與 Direct Connect 建立關聯或取消關聯。 157
建立傳輸虛擬介面以連往 Direct Connect 閘道 159
建立傳輸閘道關聯提案 162
接受或拒絕傳輸閘道關聯提案 162
更新傳輸閘道關聯的允許字首 164
刪除傳輸閘道關聯提案 164
雲端 WAN 核心網路關聯 165
先決條件 167
考量事項 167
Direct Connect 閘道與 Cloud WAN 核心網路的關聯 168
驗證 Direct Connect 閘道關聯 168
允許字首互動 168
虛擬私有閘道關聯 169
傳輸閘道關聯 169

範例：允許傳輸閘道組態中的字首 170
標籤資源 172
標籤限制 173
透過 CLI 或 API 使用標籤 173
範例 174
安全 175
資料保護 175
網際網路流量隱私權 176
加密 177
身分和存取權管理 177
目標對象 178
使用身分驗證 178
使用政策管理存取權 181
Direct Connect 搭配 IAM 的運作方式 183
Direct Connect 的身分型政策範例 188
服務連結角色 198
AWS 受管政策 200
故障診斷 202
日誌記錄和監控 203
法規遵循驗證 204
Direct Connect 中的彈性 204
容錯移轉 205
基礎架構安全 205
邊界閘道協定 206
使用 AWS CLI 207
步驟 1：建立連線 207
步驟 2：下載 LOA-CFA 208
步驟 3：建立虛擬介面並取得路由器組態 209
記錄 API 呼叫 214
AWS Direct Connect CloudTrail 中的資訊 214
了解 AWS Direct Connect 日誌檔案項目 215
監控 Direct Connect 資源 220
監控工具 220
自動化監控工具 220
手動監控工具 221
使用 Amazon CloudWatch 監控 221

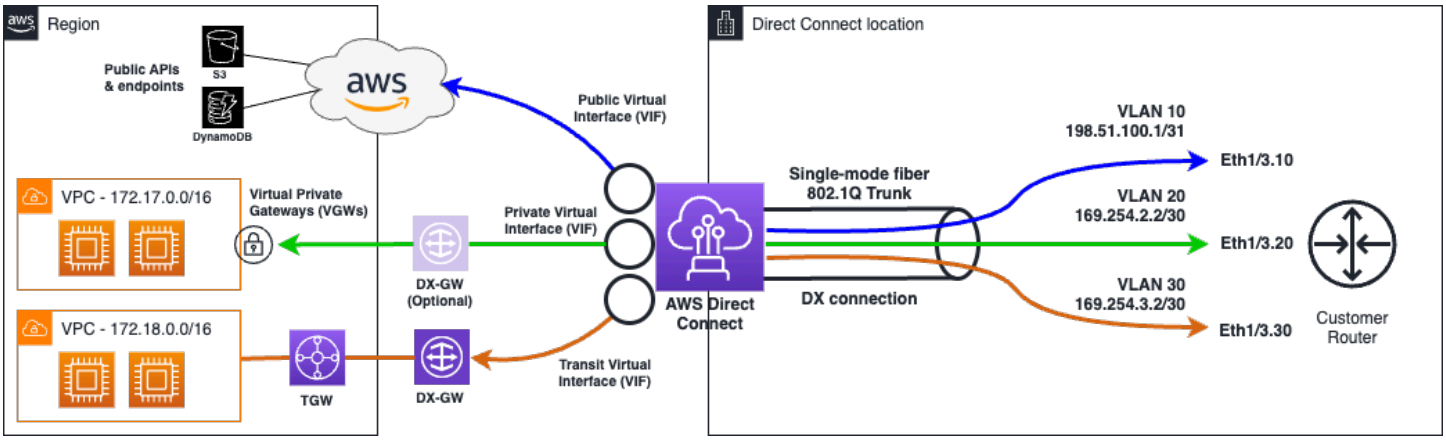
AWS Direct Connect 指標和維度 222
檢視 Direct Connect CloudWatch 指標 226
建立警示以監控連線 228
Direct Connect 配額 229
BGP 配額 231
負載平衡考量 232
疑難排解 233
第 1 層 (實體) 問題 233
第 2 層 (資料連結) 問題 235
第 3/4 層 (網路/傳輸) 問題 236
路由問題 239
文件歷史紀錄 241
..... ccxlvi

什麼是 AWS Direct Connect？

AWS Direct Connect 會透過標準乙太網路光纖纜線將您的內部網路連結至 AWS Direct Connect 位置。纜線的一端連接到您的路由器，而另一端連接到 AWS Direct Connect 路由器。透過此連線，您可以直接建立與公有 AWS 服務（例如 Amazon S3) 或 Amazon VPC 的虛擬介面，繞過網路路徑中的網際網路服務供應商。 AWS Direct Connect 位置可讓您存取與其建立關聯的 AWS 區域中的 。您可以使用公有區域中的單一連線 AWS GovCloud (US) ，或存取所有其他公有區域中的公有 AWS 服務。

- 如需您可以連線的 Direct Connect 位置清單，請參閱 AWS Direct Connect Locations。
- 如需 Direct Connect 相關問題的解答，請參閱 Direct Connect 常見問答集。

下圖顯示如何與您的網路 AWS Direct Connect 連接的高層級概觀。



目錄

- AWS Direct Connect 元件
- 網路需求
- 支援的 Direct Connect 虛擬介面類型
- Direct Connect 定價
- 存取遠端 AWS Direct Connect 區域
- AWS Direct Connect 路由政策和 BGP 社群

AWS Direct Connect 元件

以下是您用於 Direct Connect 的關鍵元件：

連線

在 AWS Direct Connect 位置建立連線，以建立從現場部署到 AWS 區域的網路連線。如需詳細資訊，請參閱AWS Direct Connect 專用和託管連線。

虛擬介面

建立虛擬介面以啟用 AWS 服務的存取。公有虛擬介面可供存取公眾的服務，如 Amazon S3。私有虛擬介面可供存取您的 VPC。支援的界面類型如下所述the section called “支援的 Direct Connect 虛擬介面類型”。如需支援介面的詳細資訊，請參閱 AWS Direct Connect 虛擬介面和託管虛擬介面和 虛擬介面的先決條件。

網路需求

若要 AWS Direct Connect 在 AWS Direct Connect 位置使用 ，您的網路必須符合下列其中一個條件：

- 您的網路與現有 AWS Direct Connect 位置共置。如需可用 AWS Direct Connect 位置的詳細資訊，請參閱 AWS Direct Connect 產品詳細資訊。
- 您正在與合作夥伴網路 AWS Direct Connect (APN) 成員的 AWS 合作夥伴合作。如需相關資訊，請參閱支援 AWS Direct Connect 的 APN 合作夥伴。
- 您憑藉某家獨立的服務供應商連接到 AWS Direct Connect。

此外，您的網路還必須符合以下條件：

- 您的網路必須使用單模光纖搭配適用於 1 GB 乙太網路的 1000BASE-LX (1310 nm) 收發器、適用於 10 GB 的 10GBASE-LR (1310 nm) 收發器、適用於 100 GB 乙太網路的 100GBASE-LR4，或適用於 400 Gbps 乙太網路的 400GBASE-LR4。
- 連接埠速度大於 1 Gbps 速度的連線必須停用連接埠的自動交涉功能。不過，根據為您的連線提供服務的 AWS Direct Connect 端點，可能需要啟用或停用 1 Gbps 連線的自動交涉。如果您的虛擬介面仍未開通，請參閱 診斷排解第 2 層 (資料鏈路) 問題。視連線終止的 Direct Connect 端點而定，可能需要相應地啟用或停用自動交涉。
- 802.1Q VLAN 封裝必須取得整個連線的支援，包含中繼裝置。
- 您的裝置必須支援邊界閘道協定 (BGP) 及 BGP MD5 驗證。
- (選用) 您可以在網路上設定雙向轉寄偵測 (BFD)。系統會為每個 AWS Direct Connect 虛擬界面自動啟用非同步 BFD。它會自動啟用 Direct Connect 虛擬介面，但要在您於路由器上設定之後才會生效。如需詳細資訊，請參閱啟用 Direct Connect 連線的 BFD。

AWS Direct Connect 同時支援 IPv4 和 IPv6 通訊協定。公有 AWS 服務提供的 IPv6 地址可透過 AWS Direct Connect 公有虛擬介面存取。

AWS Direct Connect 支援在連結層的乙太網路訊框大小 1522 或 9023 位元組 (14 位元組乙太網路標頭 + 4 位元組 VLAN 標籤 + IP 資料包的位元組 + 4 位元組 FCS)。您可以設定您的私有虛擬介面的 MTU。如需詳細資訊，請參閱私有虛擬介面或傳輸虛擬介面的 MTUs 。

支援的 Direct Connect 虛擬介面類型

AWS Direct Connect 支援以下三種虛擬介面 (VIF) 類型：

- 私有虛擬介面

  此類型的界面用於使用私有 IP 地址存取 Amazon Virtual Private Cloud (VPC)。透過私有虛擬界面，您可以

  - 直接連接到每個私有虛擬介面的單一 VPC，以使用相同區域中IPs 存取這些資源。
  - 將私有虛擬介面連接至 Direct Connect 閘道，以存取任何帳戶和 AWS 區域的多個虛擬私有閘道（AWS 中國區域除外）。
- 公有虛擬界面

  這種類型的虛擬界面用於使用 AWS 公有 IP 地址存取所有公有服務。透過公有虛擬界面，您可以連線到全球所有 AWS 公有 IP 地址和服務。
- 傳輸虛擬介面

  此類型的界面用於存取與 Direct Connect 閘道相關聯的一或多個 Amazon VPC Transit Gateway。使用傳輸虛擬介面，您可以跨多個帳戶和 AWS 區域（AWS 中國區域除外） 連接多個 Amazon VPC Transit Gateway。

> **Note**
>
> Direct Connect 閘道與虛擬介面之間不同類型的關聯數量有限制。如需特定限制的詳細資訊，請參閱 Direct Connect 配額頁面。

如需虛擬介面的詳細資訊，請參閱 虛擬介面和託管虛擬介面。

Direct Connect 定價

AWS Direct Connect 有兩個計費元素：連接埠小時和傳出資料傳輸。連接埠小時定價由容量和連線類型 (專用連線或託管連線) 確定。

私有介面和傳輸虛擬介面的資料傳輸費用會分配給負責資料傳輸 AWS 的帳戶。使用多帳戶 AWS Direct Connect 閘道無需額外費用。

對於可公開定址 AWS 的資源 （例如，透過網際網路閘道的 Amazon S3 儲存貯體、Classic EC2 執行個體或 EC2 流量），如果傳出流量目的地為相同 AWS 付款人帳戶擁有的公有字首，並透過 AWS Direct Connect 公 AWS 有虛擬介面主動公告給 ，則會以 AWS Direct Connect 資料傳輸率向資源擁有者計量資料傳輸輸出 (DTO) 用量。

如需詳細資訊，請參閱 AWS Direct Connect 定價。

存取遠端 AWS Direct Connect 區域

AWS Direct Connect 位於公有區域的位置，或 AWS GovCloud (US) 可以存取任何其他公有區域 （中國 （北京和寧夏） 除外） 的公有服務。此外，公有區域中的 AWS Direct Connect 連線 AWS GovCloud (US) 或 可設定為在任何其他公有區域中 （不包括中國 （北京和寧夏） 存取您帳戶中的 VPC。也就是說，您可以使用單一 AWS Direct Connect 連線建構多重區域服務。無論您存取的是公有 AWS 服務或另一個區域中的 VPC，所有聯網流量都會保留在 AWS 全域網路骨幹上。

從遠端區域傳出的任何資料一概依遠端區域資料傳輸費率計費。如需資料傳輸定價的詳細資訊，請參閱 AWS Direct Connect 詳細資訊頁面的定價一節。

如需 AWS Direct Connect 連線的路由政策以及所支援 BGP 社群的詳細資訊，請參閱 路由政策和 BGP 社群。

存取遠端區域中的公有服務

若要存取位於遠端區域的公有資源，您必須設定公有虛擬介面並建立邊界閘道協定 (BGP) 工作階段。如需詳細資訊，請參閱虛擬介面和託管虛擬介面。

在您建立公有虛擬介面並為其建立 BGP 工作階段之後，您的路由器會學習其他公有 AWS 區域的路由。如需目前公告的字首詳細資訊 AWS，請參閱 中的 AWS IP 地址範圍Amazon Web Services 一般參考。

存取遠端區域中VPCs

您可以在任何公有區域內建立 Direct Connect 閘道。使用它透過私有虛擬界面將 AWS Direct Connect 連線連接到您帳戶中位於不同 區域的 VPCs 或傳輸閘道。如需詳細資訊，請參閱AWS Direct Connect 閘道。

或者，您可以為您的 AWS Direct Connect 連線建立公有虛擬介面，然後在遠端區域中建立與 VPC 的 VPN 連線。如需有關設定 VPN 連線至 VPC 的詳細資訊，請參閱 Amazon VPC 使用者指南中的使用 Amazon 虛擬私有雲端案例。

網路對 Amazon VPC 連線選項

以下組態可用於將遠端網路與 Amazon VPC 環境連線。這些選項有助於將 AWS 資源與您現有的現場服務整合：

- Amazon Virtual Private Cloud 連線選項

AWS Direct Connect 路由政策和 BGP 社群

AWS Direct Connect 會套用公有 AWS Direct Connect 連線的傳入（來自您的內部部署資料中心）和傳出（來自您的 AWS 區域）路由政策。您也可以將邊界閘道協定 (BGP) 社群標籤用於 Amazon 公告的路由，並對您向 Amazon 公告的路由套用 BGP 社群標籤。

公用虛擬介面路由政策

如果您使用 AWS Direct Connect 存取公有 AWS 服務，則必須指定要透過 BGP 公告的公有 IPv4 字首或 IPv6 字首。

實施的傳入路由政策如下：

- 您必須擁有公有字首，且這些字首務必照實登錄於相應的區域網際網路登錄檔。
- 流量必須通往 Amazon 公有字首。各連線之間互傳的路由不受支援。
- AWS Direct Connect 會執行傳入封包篩選，以驗證來自您公告字首的流量來源。

實施的傳出路由政策如下：

- AS_PATH 和最長字首比對用於判斷路由路徑。 AWS AWS Direct Connect 如果同時向網際網路和公有虛擬介面公告相同的字首， 建議使用 來公告更具體的路由。

- AWS Direct Connect 會在可用時公告所有本機和遠端 AWS 區域字首，並在可用時包含來自其他 AWS 非區域存在點 (PoP) 的網路字首；例如 CloudFront 和 Route 53。

  > **Note**
  >
  > - AWS IP 地址範圍 JSON 檔案 ip-ranges.json 中列出的字首 AWS 僅適用於 AWS 中國區域。
  > - AWS 商業區域的 AWS IP 地址範圍 JSON 檔案 ip-ranges.json 中列出的字首只會在 AWS 商業區域中公告。
  >
  > 如需有關 ip-ranges.json 檔案的詳細資訊，請參閱 AWS 一般參考 中的 AWS IP 地址範圍。

- AWS Direct Connect 公告路徑長度下限為 3 的字首。
- AWS Direct Connect 會向知名的 NO_EXPORT BGP 社群公告所有公有字首。
- 如果您使用兩個不同的公有虛擬介面從兩個不同的 區域公告相同的字首，且兩個 都具有相同的 BGP 屬性和最長字首長度，則 AWS 會優先考慮主要區域的傳出流量。
- 如果您有多個 AWS Direct Connect 連線，您可以透過公告具有相同路徑屬性的字首來調整傳入流量的負載共用。
- 公告的字首 AWS Direct Connect 不得超出連線的網路邊界。例如，這類字首不得納入到任何的公有網際網路路由表。
- AWS Direct Connect 會保留 Amazon 網路內客戶公告的字首。我們不會重新公告從公有 VIF 得到的客戶字首至下列其中任何一項：
  - 其他 AWS Direct Connect 客戶
  - 與 AWS 全球網路對等的網路
  - Amazon 的傳輸供應商
- 使用公有界面時，您可以使用公有或私有 ASN。不過，有重要的考量事項：
  - 公有 ASNs：您必須擁有 ASN 並有權宣告。 AWS 會驗證您對 ASN 的擁有權。
  - 私有 ASNs：您可以使用私有 ASNs(64512-65534、4200000000-4294967294)。不過，當您向其他 AWS 客戶或網際網路公告字首時， AWS Direct Connect 會將私有 ASN 取代為 AWS ASN (7224)。
  - ASN 前置：
    - 使用公有 ASN 時，前綴將如預期運作，而您前綴的 ASN 將可見於其他網路。
    - 使用私有 ASN 時，當 將私有 ASN AWS 取代為 7224 時，您所做的任何前綴都會被剔除。這表示在公有虛擬界面上使用私有 ASN AWS 時，前置 ASN 對於影響 外部的路由決策無效。

- 透過公 AWS 有虛擬介面使用 建立 BGP 對等工作階段時，請針對自治系統編號 (ASN) 使用 7224 在 AWS 側面建立 BGP 工作階段。路由器或客戶閘道裝置上的 ASN 應與該 ASN 不同。

公有虛擬介面 BGP 社群

AWS Direct Connect 支援範圍 BGP 社群標籤，以協助控制公有虛擬介面上流量的範圍 （ 區域或全域 ） 和路由偏好設定。 會將從公有 VIF 接收的所有路由 AWS 視為已加上 NO_EXPORT BGP 社群標籤，這表示只有 AWS 網路會使用該路由資訊。

範圍 BGP 社群

對於您向 Amazon 公告的公有字首，您可以套用 BGP 社群標籤，表明您的字首在 Amazon 網路內將傳播多遠，包括：僅限本地 AWS 區域、某一洲的所有區域，或是所有公有區域。

AWS 區域 社群

對於傳入路由政策，您的字首可以使用下列 BGP 社群：

- `7224:9100`—本機 AWS 區域
- `7224:9200`- AWS 區域 適用於某洲的所有 ：
  - 整個北美洲
  - 亞太區域
  - 歐洲、中東和非洲
- `7224:9300`—全球 （ 所有公有 AWS 區域 ）

> **Note**
>
> 如果您不套用任何社群標籤，字首預設會公告至所有公有 AWS 區域 （ 全域 ）。
> 標示為相同社群且有相同 AS_PATH 屬性的前綴是多路徑的候選項。

AWS Direct Connect保留 `7224:1` – `7224:65535` 社群。

對於傳出路由政策， 會將下列 BGP 社群 AWS Direct Connect 套用至其公告的路由：

- `7224:8100`- 源自與存在 AWS Direct Connect 點相關聯的相同 AWS 區域的路由。
- `7224:8200`- 源自與存在 AWS Direct Connect 點相關聯的同一洲的路由。

- 無標籤 - 來自其他洲的路由。

> **Note**
>
> 若要接收所有 AWS 公有字首，請勿套用任何篩選條件。

會移除 AWS Direct Connect 公有連線不支援的社群。

`NO_EXPORT` BGP 社群

對於傳出路由政策，公有虛擬介面支援 `NO_EXPORT` BGP 社群標籤。

AWS Direct Connect 也會在公告的 Amazon 路由上提供 BGP 社群標籤。如果您使用 AWS Direct Connect 存取公有 AWS 服務，您可以根據這些社群標籤建立篩選條件。

對於公有虛擬介面，所有向客戶 AWS Direct Connect 公告的路由都會加上 NO_EXPORT 社群標籤。

私有虛擬介面和傳輸虛擬介面路由政策

如果您使用 AWS Direct Connect 存取私有 AWS 資源，則必須指定要透過 BGP 公告的 IPv4 或 IPv6 字首。這些字首可以是公有或私有。

根據公告的字首，適用下列傳出路由規則：

- AWS 會先評估最長的字首長度。如果所需的路由路徑適用於主動/被動連線， AWS 則建議使用多個 Direct Connect 虛擬介面公告更特定的路由。如需詳細資訊，請參閱使用最長字首比對透過混合網路影響流量。
- 本機偏好設定是當所需的路由路徑適用於作用中/被動連線，且公告的字首長度相同時，建議使用的 BGP 屬性。每個區域都會設定此值，以偏好 AWS 區域 使用`7224:7200`中本機偏好設定社群值具有相同關聯的AWS Direct Connect 位置。如果本機區域未與 Direct Connect 位置建立關聯，則會將其設定為較低的值。這僅適用於未指派本機偏好設定社群標籤的情況。
- 當字首長度和本機偏好設定相同時，AS_PATH 長度可用來判斷路由路徑。
- 當字首長度、本機偏好設定和 AS_PATH 相同時，多出口辨別器 (MED) 可用來判斷路由路徑。AWS 不建議在評估中使用較低優先順序的 MED 值。
- AWS 當字首具有相同的 AS_PATH 長度和 BGP 屬性時， 會使用跨多個傳輸或私有虛擬介面的相等成本多路徑 (ECMP) 路由。字首 AS_PATH 中的 ASNs 不需要相符。

私有虛擬介面與傳輸虛擬介面 BGP 社群

當 透過 Direct Connect 私有或傳輸虛擬介面將流量 AWS 區域 路由到內部部署位置 AWS 區域 時，與 Direct Connect 位置相關聯的 會影響在 AWS 區域 預設相關聯的相同 中使用 ECMP. AWS 區域 prefer Direct Connect 位置的能力。請參閱AWS Direct Connect 位置以識別 AWS 區域 與任何 Direct Connect 位置相關聯的 。

未套用本機偏好設定社群標籤時，在下列情況下，Direct Connect 會透過私有或傳輸虛擬介面支援 ECMP，在兩個或多個路徑上具有相同、AS_PATH 長度和 MED 值的字首：

- 無論在相同或不同的主機代管設施中 AWS 區域， AWS 區域 傳送流量都有來自相同關聯位置的兩個或多個虛擬介面路徑。
- AWS 區域 傳送流量有兩個或多個虛擬介面路徑，來自不在相同區域中的位置。

如需詳細資訊，請參閱如何 AWS 從私有或傳輸虛擬介面設定與 的主動/主動或主動/被動 Direct Connect 連線？

> **Note**
>
> 這不會影響 AWS 區域 從內部部署位置到 的 ECMP。

為了控制路由偏好設定，Direct Connect 支援私有虛擬介面和傳輸虛擬介面的本機偏好設定 BGP 社群標籤。

本地偏好 BGP 社群

您可以利用本地偏好 BGP 社群標籤，實現網路傳入流量的負載平衡和路由偏好。凡是您透過 BGP 工作階段公告的每個字首，均可套用社群標籤以表明傳回流量的關聯路徑優先順序。

支援的本地偏好 BGP 社群標籤如下：

- `7224:7100` - 低偏好度
- `7224:7200` - 中偏好度
- `7224:7300` - 高偏好度

本地偏好 BGP 社群標籤為互斥。若要在屬於相同或不同 AWS 區域的多個 AWS Direct Connect 連線（主動/主動）之間負載平衡流量，請在連線的字首之間套用相同的社群標籤，例如 `7224:7200`（中

等偏好）。如果其中一個連線失敗，則無論其主要區域關聯為何，都會在剩餘的作用中連線中使用 ECMP 來平衡流量。若要在多個 AWS Direct Connect 連線 (主動/被動) 間相互支援容錯移轉，請對主要或作用中虛擬介面的字首套用較高偏好度的社群標籤，並對備份或被動虛擬介面的字首套用較低偏好度。例如，將主要或主動虛擬介面的 BGP 社群標籤設定為被動虛擬介面的 `7224:7300` (高偏好設定) 和 `7224:7100` (低偏好設定)。

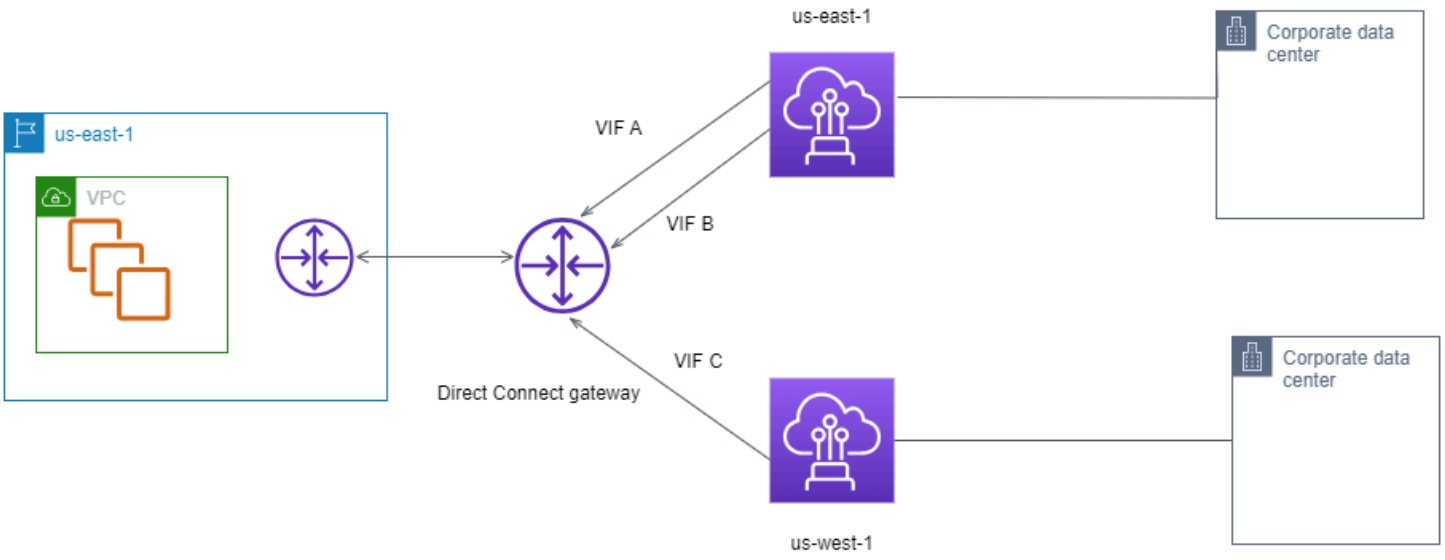
評估順序時是本地偏好 BGP 社群標籤優先於任何的 AS_PATH 屬性，且評估順序是從最低到最高的偏好度 (最好是使用最高偏好度)。

AWS Direct Connect 私有虛擬介面路由範例

請考慮 AWS Direct Connect 位置 1 主要區域與 VPC 主要區域相同的組態。不同區域中有一個備援 AWS Direct Connect 位置 從 AWS Direct Connect 位置 1 (us-east-1) 到 Direct Connect 閘道有兩個私有 VIFs (VIF A 和 VIF B)。從 AWS Direct Connect 位置 (us-west-1) 到 Direct Connect 閘道有一個私有 VIF (VIF C)。若要在 VIF A 之前透過 VIF B AWS 路由流量，請將 VIF B 的 AS_PATH 屬性設定為短於 VIF A AS_PATH 屬性。

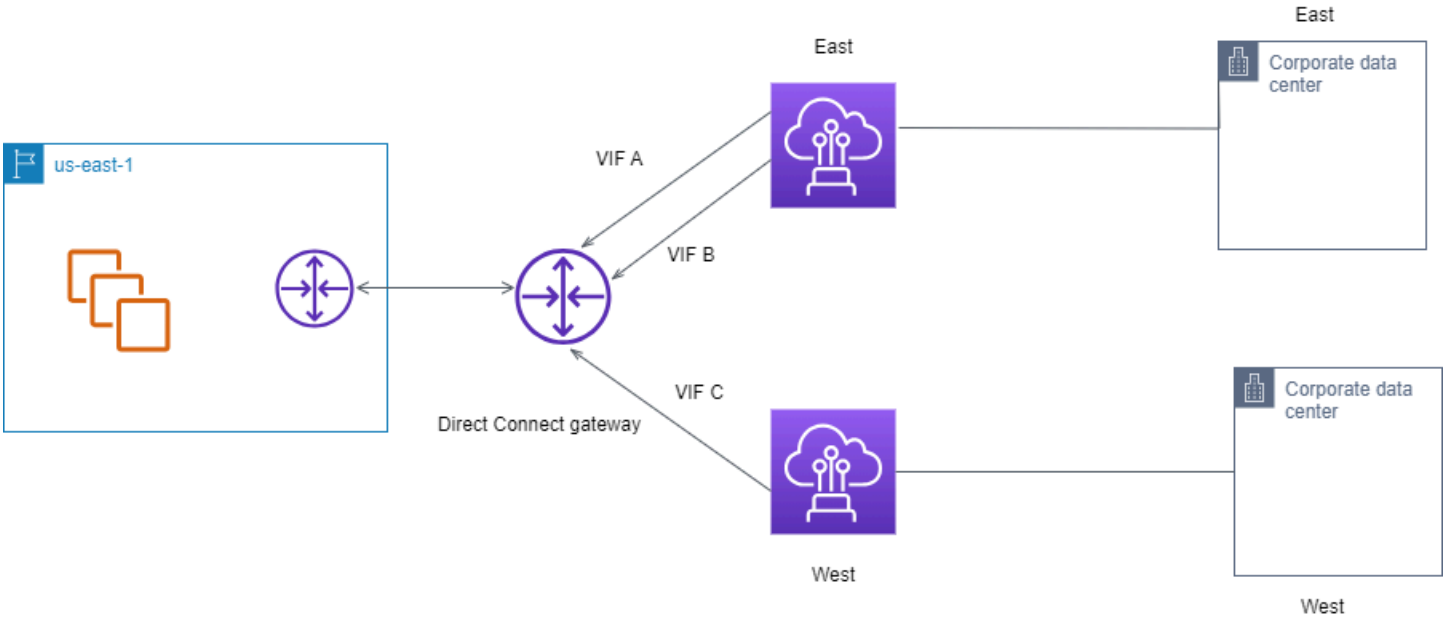
VIF 具有下列組態：

- VIF A (在 us-east-1) 公告 172.16.0.0/16，且具有 65001, 65001, 65001 的 AS_PATH 屬性
- VIF B (在 us-east-1) 公告 172.16.0.0/16，且具有 65001, 65001 的 AS_PATH 屬性
- VIF C (在 us-west-1) 公告 172.16.0.0/16，且具有 65001 的 AS_PATH 屬性



如果您變更 VIF C 的 CIDR 範圍組態，屬於 VIF C CIDR 範圍的路由會使用 VIF C，因為其字首長度最長。

- VIF C (在 us-west-1) 公告 172.16.0.0/24，且具有 65001 的 AS_PATH 屬性



AWS Direct Connect 彈性工具組

AWS 讓客戶能夠在 Amazon Virtual Private Cloud (Amazon VPC) 與其內部部署基礎設施之間實現高彈性的網路連線。 AWS Direct Connect 彈性工具組提供具有多個彈性模型的連線精靈。這些模型可協助您進行判斷，並接著訂購可讓您達成 SLA 目標的專用連線數目。您可以選擇彈性模型，然後 AWS Direct Connect 彈性工具組會引導您完成專用連線排序程序。彈性模型的設計旨在確保您在多個位置擁有適當數量的專用連線。

AWS Direct Connect 彈性工具組具有下列優點：

- 指引您如何判斷，然後訂購適當的備援 AWS Direct Connect 專用連線。
- 確保備援專用連線具有相同的速度。
- 自動設定專用連線名稱。
- 當您擁有現有 AWS 帳戶並選取已知的 AWS Direct Connect 合作夥伴時， 會自動核准您的專用連線。授權書 (LOA) 可供立即下載。
- 當您是新 AWS 客戶或選取未知 (其他) 合作夥伴時，會自動建立專用連線核准的支援票證。
- 為您的專用連線提供訂單摘要，其中包括您可以實現的 SLA，以及所訂購專用連線的連接埠小時成本。
- 建立連結彙總群組 (LAGs)，並在您選擇 1 Gbps、10 Gbps、100 Gbps 或 400 Gbps 以外的速度時，將適當數量的專用連線新增至 LAGs。
- 提供 LAG 摘要，其中包括您可以實現的專用連線 SLA，以及做為 LAG一部分之每個所訂購專用連線的連接埠小時總成本。
- 防止您在相同 AWS Direct Connect 裝置上終止專用連線。
- 提供讓您測試組態彈性的方法。您可以使 AWS 用關閉 BGP 對等互連工作階段，驗證流量路由確實連接至其中一個備援虛擬介面。如需詳細資訊，請參閱the section called “Direct Connect 容錯移轉測試”。
- 提供連線和虛擬介面的 Amazon CloudWatch 指標。如需詳細資訊，請參閱監控 Direct Connect 資源。

彈性工具組中提供下列 AWS Direct Connect 彈性模型：

- Maximum Resiliency (最大彈性)：此模型提供一種方式，讓您可以訂購專用連線，以實現 99.99% 的 SLA。它需要您符合所有要求，以實現 AWS Direct Connect 服務水準協議中指定的 SLA。

- High Resiliency (高彈性)：此模型提供一種方式，讓您可以訂購專用連線，以實現 99.9% 的 SLA。它需要您符合所有要求，以實現 AWS Direct Connect 服務水準協議中指定的 SLA。
- Development and Test (開發和測試)：此模型提供一種方式，讓您可以在某個位置使用終止於個別裝置的個別連線，為非關鍵工作負載實現開發及測試彈性。
- Classic (傳統)。此模型旨在針對擁有現有連線並想要新增其他連線的使用者。此模型不提供 SLA。

最佳實務是使用 AWS Direct Connect 彈性工具組中的連線精靈來訂購專用連線，以實現您的 SLA 目標。

選取彈性模型之後， AWS Direct Connect 彈性工具組會逐步引導您完成下列程序：

- 選取專用連線數量
- 選擇連線容量和專用連線位置
- 訂購專用連線
- 驗證專用連線是否準備好可供使用
- 下載每個專用連線的授權書 (LOA-CFA)
- 驗證您的組態符合您的彈性需求

先決條件

AWS Direct Connect 透過單模光纖支援下列連接埠速度：適用於 1 GB 乙太網路的 1000BASE-LX (1310 nm) 收發器、適用於 10 GB 的 10GBASE-LR (1310 nm) 收發器、適用於 100 GB 乙太網路的 100GBASE-LR4，或適用於 400 Gbps 乙太網路的 400GBASE-LR4。

您可以透過下列其中一種方式設定 AWS Direct Connect 連線：

模型	頻寬	方法
專用連線	1 Gbps、10 Gbps、100 Gbps 和 400 Gbps	與 AWS Direct Connect 合作夥伴或網路提供者合作，將路由器從資料中心、辦公室或主機代管環境連接到 AWS Direct Connect 位置。網路提供者不必是 AWS Direct Connect 合作夥伴，即可將您連線至專用

模型	頻寬	方法
		連線。 AWS Direct Connect 專用連線支援透過單模光纖的這些連接埠速度：1 Gbps：1000BASE-LX (1310 nm)、10 Gbps：10GBASE-LR (1310 nm)、100Gbps：100GBASE-LR4 或 400GBASE-LR4，適用於 400 Gbps 乙太網路。
託管連線	50 Mbps、100 Mbps、200 Mbps、300 Mbps、400 Mbps、500 Mbps、1 Gbps、2 Gbps、5 Gbps、10 Gbps 和 25 Gbps。	與合作夥伴AWS Direct Connect 計劃中的合作夥伴合作，將路由器從資料中心、辦公室或主機代管環境連接到 AWS Direct Connect 位置。 只有某些合作夥伴會提供更高容量連線。

對於頻寬 AWS Direct Connect 為 1 Gbps 或更高的 連線，請確定您的網路符合下列要求：

- 您的網路必須使用單模光纖搭配適用於 1 GB 乙太網路的 1000BASE-LX (1310 nm) 收發器、適用於 10 GB 的 10GBASE-LR (1310 nm) 收發器、適用於 100 GB 乙太網路的 100GBASE-LR4，或適用於 400 Gbps 乙太網路的 400GBASE-LR4。
- 連接埠速度大於 1 Gbps 速度的連線必須停用連接埠的自動交涉功能。不過，根據為您的連線提供服務的 AWS Direct Connect 端點，可能需要啟用或停用 1 Gbps 連線的自動交涉。如果您的虛擬介面仍未開通，請參閱 診斷排解第 2 層 (資料鏈路) 問題。視連線終止的 Direct Connect 端點而定，可能需要相應地啟用或停用自動交涉。
- 802.1Q VLAN 封裝必須取得整個連線的支援，包含中繼裝置。
- 您的裝置必須支援邊界閘道協定 (BGP) 及 BGP MD5 驗證。
- (選用) 您可以在網路上設定雙向轉寄偵測 (BFD)。系統會為每個 AWS Direct Connect 虛擬界面自動啟用非同步 BFD。它會自動啟用 Direct Connect 虛擬介面，但要在您於路由器上設定之後才會生效。如需詳細資訊，請參閱啟用 Direct Connect 連線的 BFD。

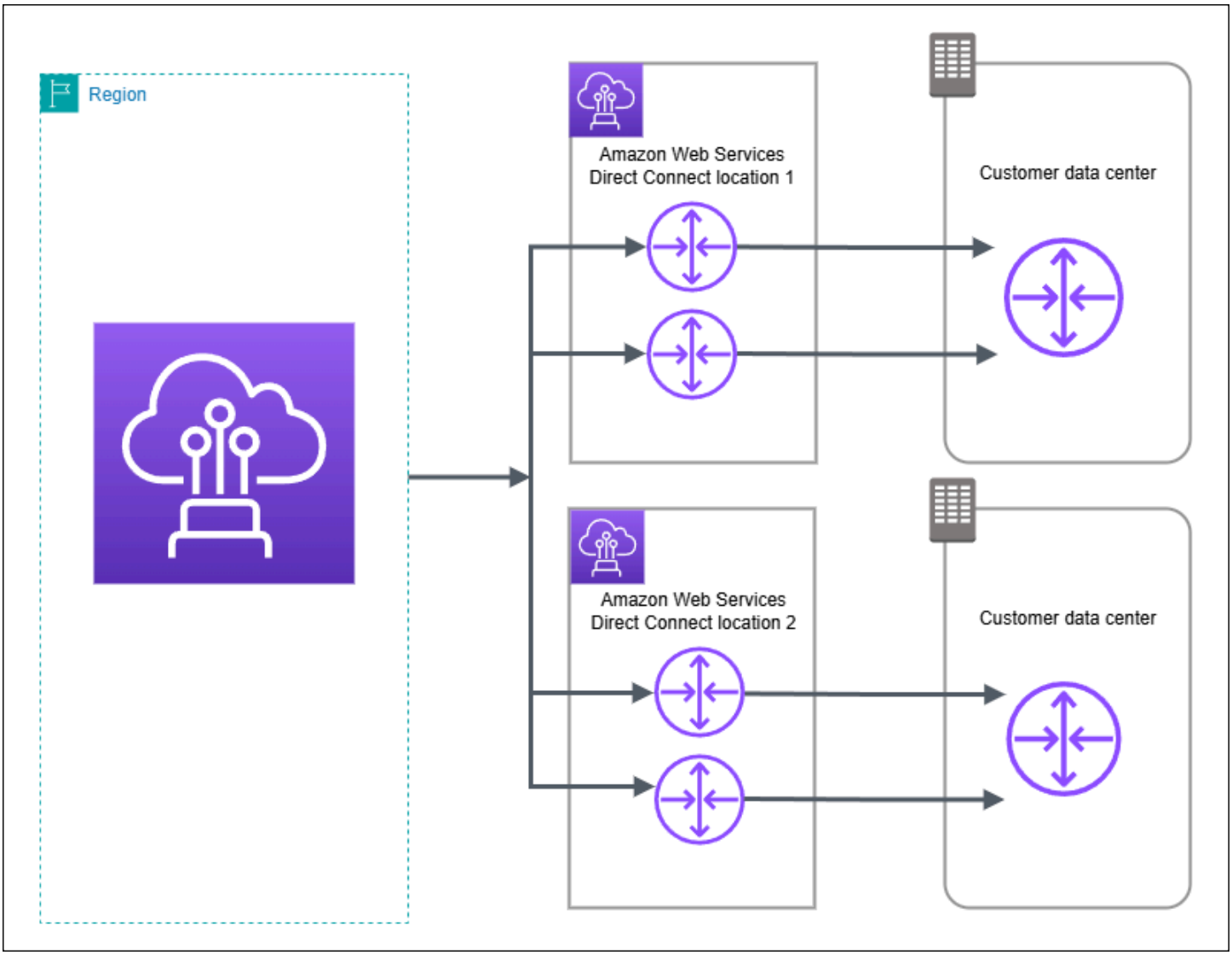
開始設定之前，請確定您具有下列資訊：

- 您要使用的彈性模型。
- 所有連線的速度、位置和合作夥伴。

  您只需要一個連線的速度。

最大彈性

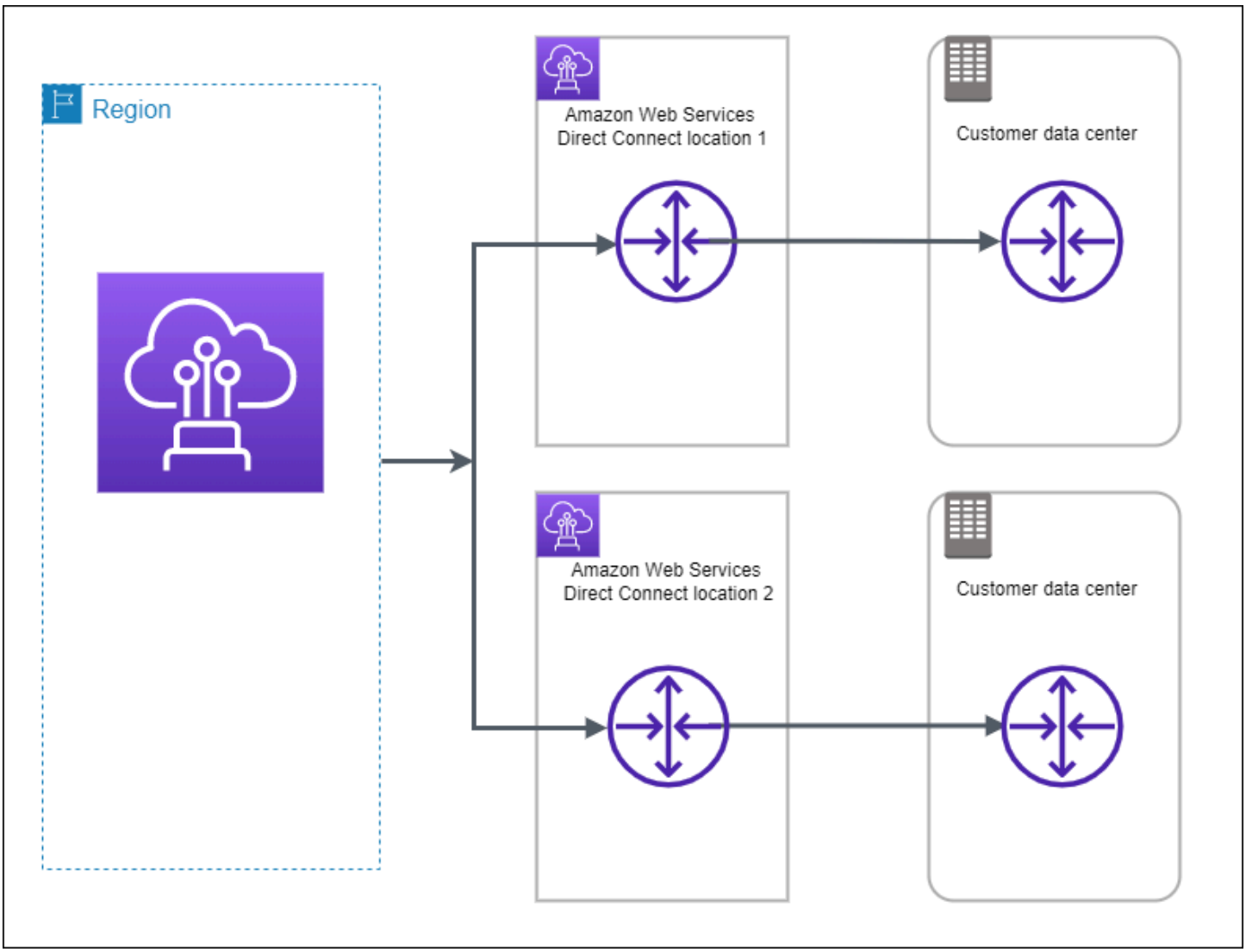
您可以在多個位置使用終止於個別裝置的個別連線，為關鍵工作負載實現最大彈性。此模型可針對裝置、連線能力及完整位置故障提供彈性。下圖顯示從每個客戶資料中心前往相同 AWS Direct Connect 位置的兩個連線。您可以選擇將客戶資料中心的每個連線移至不同位置。



如需使用 AWS Direct Connect 彈性工具組設定最大彈性模型的程序，請參閱 設定最大彈性。

高彈性

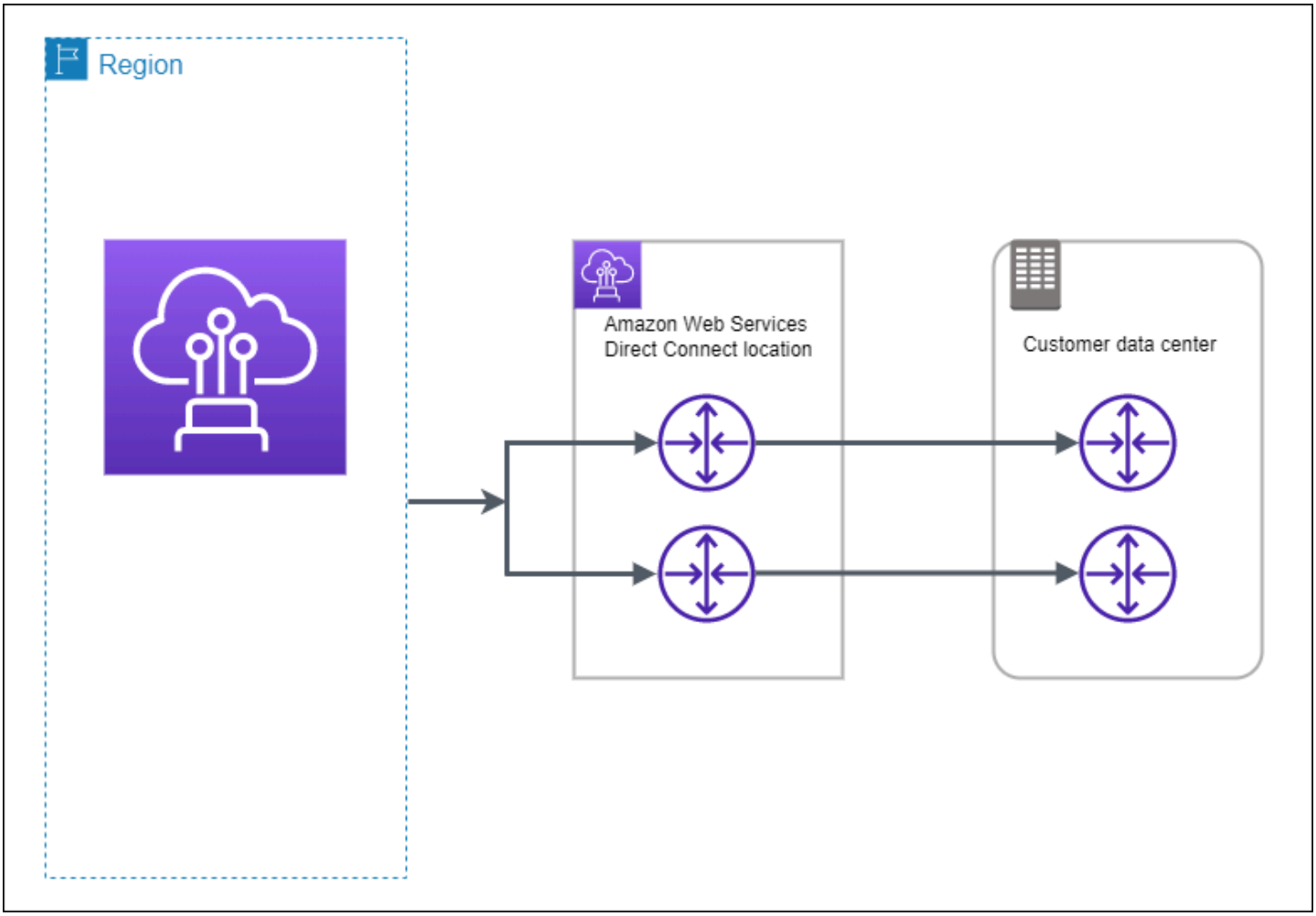
您可以使用連至多個位置的兩個單一連線 (如下圖所示)，即可為關鍵工作負載取得高彈性。此模型可針對因光纖切割或裝置故障所造成的連線故障提供彈性。它也有助於防止完整的位置故障。



如需使用 AWS Direct Connect 彈性工具組設定高彈性模型的程序，請參閱 設定高彈性。

開發和測試

您可以在多個位置使用終止於個別裝置的個別連線 (如下圖所示)，為非關鍵工作負載實現開發及測試彈性。此模型可針對裝置故障提供彈性，但無法針對位置故障提供彈性。



如需使用 AWS Direct Connect 彈性工具組設定最大彈性模型的程序，請參閱 設定開發和測試彈性。

傳統

當您擁有現有的連線時，請選取 Classic (傳統)。

以下程序示範著手設定 AWS Direct Connect 連線的常見案例。

先決條件

對於 AWS Direct Connect 連接埠速度為 1 Gbps 或更高的 連線，請確定您的網路符合下列要求：

- 您的網路必須使用單模光纖搭配適用於 1 GB 乙太網路的 1000BASE-LX (1310 nm) 收發器、適用於 10 GB 的 10GBASE-LR (1310 nm) 收發器、適用於 100 GB 乙太網路的 100GBASE-LR4，或適用於 400 Gbps 乙太網路的 400GBASE-LR4。

- 連接埠速度大於 1 Gbps 速度的連線必須停用連接埠的自動交涉功能。不過，根據為您的連線提供服務的 AWS Direct Connect 端點，可能需要啟用或停用 1 Gbps 連線的自動交涉。如果您的虛擬介面仍未開通，請參閱 診斷排解第 2 層 (資料鏈路) 問題。視連線終止的 Direct Connect 端點而定，可能需要相應地啟用或停用自動交涉。
- 802.1Q VLAN 封裝必須取得整個連線的支援，包含中繼裝置。
- 您的裝置必須支援邊界閘道協定 (BGP) 及 BGP MD5 驗證。
- (選用) 您可以在網路上設定雙向轉寄偵測 (BFD)。系統會為每個 AWS Direct Connect 虛擬界面自動啟用非同步 BFD。它會自動啟用 Direct Connect 虛擬介面，但要在您於路由器上設定之後才會生效。如需詳細資訊，請參閱啟用 Direct Connect 連線的 BFD。

如需使用 AWS Direct Connect 彈性工具組設定 Classic 連線的程序，請參閱 設定 Classic 連線。

AWS Direct Connect FailoverTest

使用 AWS Direct Connect 彈性工具組來驗證流量路由，以及這些路由是否符合您的彈性需求。

如需使用 AWS Direct Connect 彈性工具組執行容錯移轉測試的程序，請參閱 Direct Connect 容錯移轉測試。

使用 AWS Direct Connect 彈性工具組來設定 AWS Direct Connect 最大彈性

在此範例中， AWS Direct Connect 彈性工具組用於設定最大彈性模型

任務

- 步驟 1：註冊 AWS
- 步驟 2：設定彈性模型
- 步驟 3：建立您的虛擬介面
- 步驟 4：驗證您的虛擬介面彈性組態
- 步驟 5：驗證您的虛擬介面連線能力

步驟 1：註冊 AWS

若要使用 AWS Direct Connect，如果您還沒有帳戶，則需要 AWS 帳戶。

註冊 AWS 帳戶

如果您沒有 AWS 帳戶，請完成下列步驟來建立一個。

註冊 AWS 帳戶

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

   部分註冊程序需接收來電，並在電話鍵盤輸入驗證碼。

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

AWS 會在註冊程序完成後傳送確認電子郵件給您。您可以隨時登錄 https://aws.amazon.com/ 並選擇我的帳戶，以檢視您目前的帳戶活動並管理帳戶。

建立具有管理存取權的使用者

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

保護您的 AWS 帳戶根使用者

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

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

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

建立具有管理存取權的使用者

1. 啟用 IAM Identity Center。

   如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的啟用 AWS IAM Identity Center。
2. 在 IAM Identity Center 中，將管理存取權授予使用者。

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

以具有管理存取權的使用者身分登入

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

  如需使用 IAM Identity Center 使用者登入的說明，請參閱AWS 登入 《 使用者指南》中的登入 AWS 存取入口網站。

指派存取權給其他使用者

1. 在 IAM Identity Center 中，建立一個許可集來遵循套用最低權限的最佳實務。

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

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

步驟 2：設定彈性模型

設定最大彈性模型

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2. 在導覽窗格中，選擇連線，然後選擇建立連線。
3. 在 Connection ordering type (連線訂購類型) 下，選擇 Connection wizard (連線精靈)。
4. 在 Resiliency level (彈性層級) 下，選擇 Maximum Resiliency (最大彈性)，然後選擇 Next (下一步)。
5. 在 Configure connections (設定連線) 窗格的 Connection settings (連線設定) 下，執行下列動作：

   a. 對於 Bandwidth (頻寬)，選擇專用連線頻寬。

      此頻寬適用於所有建立的連線。

   b. 針對第一個位置服務提供者，選取專用連線的適當 AWS Direct Connect 位置。

c. 如適用，將第一個子位置選為最靠近您本身或網路供應商的樓層。此選項僅適用於該位置所在建築物的多個樓層設有匯接機房 (MMR) 的情況。

d. 如果您對第一個位置服務供應商選取其他，則對其他供應商的名稱，請輸入您使用的合作夥伴名稱。

e. 對於第二個位置服務提供者，選取適當的 AWS Direct Connect 位置。

f. 如適用，將第二個子位置選為最靠近您本身或網路供應商的樓層。此選項僅適用於該位置所在建築物的多個樓層設有匯接機房 (MMR) 的情況。

g. 如果您對第二個位置服務供應商選取其他，則對其他供應商的名稱，請輸入您使用的合作夥伴名稱。

h. (選用) 新增或移除標籤。

[新增標籤] 選擇 Add tag (新增標籤)，並執行下列動作：

- 對於 Key (金鑰)，輸入金鑰名稱。
- 在值中，進入索引鍵值。

[移除標籤] 在標籤旁邊，選擇 移除標籤。

6. 選擇下一步。

7. 檢閱您的連線，然後選擇 Continue (繼續)。

如果您的 LOA 已就緒，您可以選擇 Download LOA (下載 LOA)，然後按一下 Continue(繼續)。

最多可能需要 72 小時 AWS 才能檢閱您的請求，並為您的連線佈建連接埠。在此期間，您可能會收到一封電子郵件，要求您就自身使用案例或指定的據點補齊更多資訊。電子郵件會傳送至您在註冊時使用的電子郵件地址 AWS。您必須在 7 日內回覆，否則將刪除連線。

步驟 3：建立您的虛擬介面

您可以建立私有虛擬介面以連接到您的 VPC。或者，您可以建立公有虛擬介面，以連線至不在 VPC 中的公有 AWS 服務。建立通往 VPC 的私有虛擬介面時，您所連接的每個 VPC 都需要一個私有虛擬介面。例如，連接到三個 VPC 共需要三個私有虛擬介面。

開始之前，請務必備妥下列資訊：

資源	必要資訊
Connection (連線)	您要為其建立虛擬介面的 AWS Direct Connect 連線或連結彙總群組 (LAG)。
虛擬介面名稱	虛擬介面的名稱。
虛擬介面擁有者	如果您要為另一個帳戶建立虛擬介面，則需要另一個帳戶 AWS 的帳戶 ID。
(僅限私有虛擬介面) 連線	若要連線到相同區域中的 VPC AWS ，您需要 VPC 的虛擬私有閘道。BGP 工作階段的 Amazon 端 ASN 是繼承自虛擬私有閘道。當您建立虛擬私有閘道時，您可指定自己的私有 ASN。否則，Amazon 會提供預設的 ASN。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的建立虛擬私有閘道。若要透過 Direct Connect 閘道連線至 VPC，您需要該 Direct Connect 閘道。如需詳細資訊，請參閱 Direct Connect 閘道。
VLAN	您的連線尚未使用的唯一虛擬區域網路 (VLAN) 標籤。此值必須介於 1 到 4094 之間，且必須符合乙太網路 802.1Q 標準。任何周遊 AWS Direct Connect 連線的流量都需使用此標籤。 如果您有託管連線，您的 AWS Direct Connect 合作夥伴會提供此值。建立虛擬介面後，就無法修改該值。

對等 IP 地址	虛擬介面可以支援 IPv4、IPv6 或其中一個 (雙堆疊) 的 BGP 對等工作階段。請勿使用彈性 IPs(EIPs) 或從 Amazon 集區使用您自己的 IP 地址 (BYOIP) 來建立公有虛擬介面。您無法在相同的虛擬介面上為相同 IP 地址系列建立多個 BGP 工作階段。IP 地址範圍會指派給 BGP 對等工作階段之虛擬介面的每一端。
	
	• IPv4：
	  • (僅限公有虛擬介面) 您必須指定您擁有的唯一公有 IPv4 地址。值可為下列其中之一：
	  • 客戶擁有的 IPv4 CIDR
	
	這些可以是任何公有 IPs (客戶擁有或提供 AWS)，但您的對等 IP 和 AWS 路由器對等 IP 都必須使用相同的子網路遮罩。例如，如果您配置/31範圍，例如 203.0.113.0/31 ，則可以將 203.0.113.0 用於對等 IP 和 203.0.113.1 用於 AWS 對等 IP。或者，如果您配

資源	必要資訊
	置/24範圍，例如 198.51.100.0/24 ，您可以將 198.51.100.10 用於對等 IP 和198.51.100.20 對 AWS 等 IP。 • AWS Direct Connect 合作夥伴或 ISP 擁有的 IP 範圍，以及 LOA-CFA 授權 • AWS提供的 /31 CIDR。請聯絡 AWS Support 以請求公有 IPv4 CIDR (並在請求中提供使用案例) **Note** 我們無法保證我們能夠滿足 AWS提供公有 IPv4 地址的所有請求。 • (僅限私有虛擬介面) Amazon 可以為您產生私有 IPv4 地址。如果您指定自己的 CIDRs。 AWS 例如，請勿從您的本機網路指定其他 IP 地址。與公有虛擬介面類似，相同的子網路遮罩必須同時用於對等 IP 和 AWS 路由器對等 IP。例如，如果您配置/30範圍，例如 192.168.0.0/30 ，則可以將 192.168.0.1 用於對等 IP 和 192.168.0.2 用於 AWS 對等 IP。 • IPv6：Amazon 會自動為您配置一個 /125 IPv6 CIDR。您無法指定自己的對等 IPv6 地址。
地址系列	BGP 對等工作階段是否會透過 IPv4 或 IPv6 進行。
BGP 資訊	• BGP 工作階段在您這端的公有或私有邊界閘道協定 (BGP) 自治系統編號 (ASN)。您必須擁有公有 ASN 才能使用。如果您使用的是私有 ASN，即可設定自訂 ASN 值。對於 16 位元的 ASN，此值的範圍必須為 64512 到 65534。對於 32 位元的 ASN，此值的範圍必須為 1 到 2147483647。如果您使用私有 ASN 做為公有虛擬介面，則自治系統 (AS) 前置無法運作。 • AWS 根據預設， 會啟用 MD5。您無法修改此選項。 • 一個 MD5 BGP 驗證金鑰。您可以提供自己的資訊，或是由 Amazon 為您生成。

資源	必要資訊

(僅限公有虛擬介面) 您要公告的字首	要透過 BGP 公告的公有 IPv4 路由或 IPv6 路由。您必須使用 BGP 公告至少一個字首，最多可公告 1,000 個字首。
	• IPv4：當下列任一情況成立 AWS Direct Connect 時，IPv4 CIDR 可以與使用 宣布的另一個公有 IPv4 CIDR 重疊：
	  • CIDRs 來自不同的 AWS 區域。請確定您在公有字首上套用 BGP 社群標籤。
	  • 主動/被動組態中具備公有 ASN 時，您可以使用 AS_PATH。
	  如需更多資訊，請參閱路由政策和 BGP 社群。
	• 透過 Direct Connect 公有虛擬界面，您可以為 IPv4 指定從 /1 到 /32 的任何字首長度，並為 IPv6 指定從 /1 到 /IPv64 的任何字首長度。
	• 您可以將其他字首新增至現有的公有 VIF，並透過聯絡 AWS 支援部門來公告。在您的支援案例中，提供您要新增至公有 VIF 並公告的其他 CIDR 字首清單。

（僅限私有和傳輸虛擬介面） 巨型訊框	封包經過的最大傳輸單位 (MTU) AWS Direct Connect。預設值為 1500。設定虛擬介面的 MTU 為 9001 (巨型訊框)，可能導致基礎實體連線的更新，如果未更新到支援巨型訊框。更新連線會干擾所有連線相關聯的虛擬介面的網路連線能力達 30 秒。巨型訊框僅適用於從 傳播的路由 AWS Direct Connect。如果您將靜態路由新增至指向虛擬私有閘道的路由表格，則透過靜態路由傳送的流量會使用 1500 MTU。若要檢查連線或虛擬介面是否支援巨型訊框，請在 AWS Direct Connect 主控台中選取它，然後在虛擬介面一般組態頁面上尋找支援的巨型訊框。

如果您的公有字首或 ASN 屬於某家 ISP 或網路電信業者，我們會要求您提供額外的資訊。其形式可能是採用公司信箋的正式行文或寄自公司網域名稱的電子郵件，以茲確認該網路字首/ASN 可供您使用。

當您建立公有虛擬介面時， 最多可能需要 72 小時 AWS 才能檢閱和核准您的請求。

佈建公有虛擬介面連往非 VPC 服務

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2. 在導覽窗格中，選擇 Virtual Interfaces (虛擬介面)。

3. 選擇建立虛擬介面。
4. 在虛擬介面類型之下，針對類型選擇公有。
5. 在公有虛擬介面設定 之下，執行下列動作：

   a. 針對虛擬介面名稱，輸入虛擬介面的名稱。

   b. 針對連線，選擇要用於此介面的 Direct Connect 連線。

   c. 針對 VLAN，為您的虛擬區域網路 (VLAN) 輸入 ID 號碼。

   d. 針對 BGP ASN，輸入您閘道的邊界閘道協定 (BGP) 自發系統編號 (ASN)。

      有效值為 1-2147483647。
6. 在 Additional settings (其他設定) 之下，執行下列動作：

   a. 若要設定 IPv4 BGP 或 IPv6 對等，請執行下列動作：

      [IPv4] 若要設定 IPv4 BGP 對等，請選擇 IPv4，然後執行以下動作：

      - 若要自行指定這些 IP 地址，對於 Your router peer ip (您的路由器對等 IP)，輸入 Amazon 應傳送流量至該處的目的地 IPv4 CIDR 地址。
      - 對於 Amazon router peer IP (Amazon 路由器對等 IP)，輸入用以傳送流量至 AWS的 IPv4 CIDR 地址。

      [IPv6] 若要設定 IPv6 BGP 對等，請選擇 IPv6。對等 IPv6 地址是自動從 Amazon 的 IPv6 地址集區所指派。您無法指定自訂 IPv6 地址。

   b. 若要提供自己的 BGP 金鑰，請輸入您的 BGP MD5 金鑰。

      如果您未輸入值，我們會產生 BGP 金鑰。

   c. 若要對 Amazon 公告字首，對於欲公告的字首，輸入應透過虛擬介面將流量路由傳送至該處的目的地 IPv4 CIDR 地址 (以逗號分隔)。

   d. (選用) 新增或移除標籤。

      [新增標籤] 選擇 Add tag (新增標籤)，並執行下列動作：

      - 對於 Key (金鑰)，輸入金鑰名稱。
      - 在值中，進入索引鍵值。

      [移除標籤] 在標籤旁邊，選擇 移除標籤。
7. 選擇建立虛擬介面。

佈建私有虛擬介面連往 VPC

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2. 在導覽窗格中，選擇 Virtual Interfaces (虛擬介面)。
3. 選擇建立虛擬介面。
4. 在虛擬介面類型之下，對於類型，請選擇私有。
5. 在公有虛擬介面設定之下，執行下列動作：

   a. 針對虛擬介面名稱，輸入虛擬介面的名稱。

   b. 針對連線，選擇要用於此介面的 Direct Connect 連線。

   c. 對於閘道類型，選擇「虛擬私有閘道」或「Direct Connect 閘道」。

   d. 對於虛擬介面擁有者，選擇另一個 AWS 帳戶，然後輸入 AWS 帳戶。

   e. 對於虛擬私有閘道，請選擇您用於此介面的虛擬私有閘道。

   f. 針對 VLAN，為您的虛擬區域網路 (VLAN) 輸入 ID 號碼。

   g. 針對 BGP ASN，為新的虛擬介面輸入您內部部署對等路由器的邊界閘道協定自治系統編號。

   有效值為 1 至 2147483647。
6. 在 Additional settings (其他設定) 之下，執行下列動作：

   a. 若要設定 IPv4 BGP 或 IPv6 對等，請執行下列動作：

   [IPv4] 若要設定 IPv4 BGP 對等，請選擇 IPv4，然後執行以下動作：

   - 若要自行指定這些 IP 地址，對於 Your router peer ip (您的路由器對等 IP)，輸入 Amazon 應傳送流量至該處的目的地 IPv4 CIDR 地址。
   - 對於 Amazon 路由器對等 IP，輸入用以傳送流量至 AWS的 IPv4 CIDR 地址。

   > **Important**
   >
   > 設定 AWS Direct Connect 虛擬介面時，您可以使用 RFC 1918 指定自己的 IP 地址、使用其他定址機制，或選擇從 RFC 3927 169.25IPv4.0.0/16 IPv4 Link-Local 範圍配置的 AWS 指派 IPv4/29 CIDR 地址point-to-point連線。這些point-to-point連線應僅用於客戶閘道路由器和 Direct Connect 端點之間的 eBGP 互連。針對 VPC 流量或通道用途，例如 AWS Site-to-Site私有 IP VPN 或 Transit Gateway Connect， AWS 建議使用客戶閘道路由器上的迴路或 LAN 界面做為來源或目的地地址，而非point-to-point連線。

- 如需有關 RFC 1918 的詳細資訊，請參閱私有網路的地址配置。
- 如需有關 RFC 3927 的詳細資訊，請參閱 IPv4 Link-Local 地址的動態組態。

[IPv6] 若要設定 IPv6 BGP 對等，請選擇 IPv6。對等 IPv6 地址是自動從 Amazon 的 IPv6 地址集區所指派。您無法指定自訂 IPv6 地址。

b. 若要將最大傳輸單位 (MTU) 從 1500 (預設) 變更至 9001 (巨型框架)，請選取巨型 MTU (MTU 大小 9001)。

c. (選用) 在啟用 SiteLink 之下，選擇啟用以啟用 Direct Connect 連接點之間的直接連線。

d. (選用) 新增或移除標籤。

[新增標籤] 選擇 Add tag (新增標籤)，並執行下列動作：

- 對於 Key (金鑰)，輸入金鑰名稱。
- 在值中，進入索引鍵值。

[移除標籤] 在標籤旁邊，選擇 移除標籤。

7. 選擇建立虛擬介面。

步驟 4：驗證您的虛擬介面彈性組態

在您建立 AWS 雲端或 Amazon VPC 的虛擬介面之後，請執行虛擬介面容錯移轉測試，以確認您的組態符合您的彈性需求。如需詳細資訊，請參閱the section called “Direct Connect 容錯移轉測試”。

步驟 5：驗證您的虛擬介面連線能力

建立 AWS 雲端或 Amazon VPC 的虛擬介面之後，您可以使用下列程序來驗證您的 AWS Direct Connect 連線。

驗證與 AWS 雲端的虛擬介面連線

- 執行`traceroute`並確認 AWS Direct Connect 識別符位於網路追蹤中。

驗證虛擬介面至 Amazon VPC 的連線

1. 使用可透過 ping 存取的 AMI 如 Amazon Linux AMI，在連接至虛擬私有閘道的 VPC 中啟動 EC2 執行個體。當您使用 Amazon EC2 主控台的執行個體啟動精靈時，可在快速入門索引標籤取得 Amazon Linux AMI。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的啟動執行個體。

Amazon EC2 確認與執行個體關聯的安全群組，包含一個規則允許流量傳入 ICMP (適用於 ping 請求)。

2. 待執行個體執行之後，取得其私有 IPv4 地址 (例如 10.0.0.4)。Amazon EC2 主控台顯示的執行個體詳細資訊將包含該地址。
3. Ping 到該私有 IPv4 地址並獲得回應。

使用 AWS Direct Connect 彈性工具組來設定 AWS Direct Connect 高彈性

在此範例中， AWS Direct Connect 彈性工具組用於設定高彈性模型

任務

- 步驟 1：註冊 AWS
- 步驟 2：設定彈性模型
- 步驟 3：建立您的虛擬介面
- 步驟 4：驗證您的虛擬介面彈性組態
- 步驟 5：驗證您的虛擬介面連線能力

步驟 1：註冊 AWS

若要使用 AWS Direct Connect，如果您還沒有帳戶，則需要 AWS 帳戶。

註冊 。 AWS 帳戶

如果您沒有 AWS 帳戶，請完成下列步驟來建立一個。

註冊 AWS 帳戶

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

   部分註冊程序需接收來電，並在電話鍵盤輸入驗證碼。

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

AWS 會在註冊程序完成後傳送確認電子郵件給您。您可以隨時登錄 https://aws.amazon.com/ 並選擇我的帳戶，以檢視您目前的帳戶活動並管理帳戶。

建立具有管理存取權的使用者

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

保護您的 AWS 帳戶根使用者

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

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

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

建立具有管理存取權的使用者

1. 啟用 IAM Identity Center。

   如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的啟用 AWS IAM Identity Center。
2. 在 IAM Identity Center 中，將管理存取權授予使用者。

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

以具有管理存取權的使用者身分登入

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

  如需使用 IAM Identity Center 使用者登入的說明，請參閱AWS 登入 《 使用者指南》中的登入 AWS 存取入口網站。

指派存取權給其他使用者

1. 在 IAM Identity Center 中，建立一個許可集來遵循套用最低權限的最佳實務。

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

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

步驟 2：設定彈性模型

設定高彈性模型

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2. 在導覽窗格中，選擇連線，然後選擇建立連線。
3. 在 Connection ordering type (連線訂購類型) 下，選擇 Connection wizard (連線精靈)。
4. 在 Resiliency level (彈性層級) 下，選擇 High Resiliency (高彈性)，然後選擇 Next (下一步)。
5. 在 Configure connections (設定連線) 窗格的 Connection settings (連線設定) 下，執行下列動作：

   a. 對於 bandwidth (頻寬)，選擇連線頻寬。

      此頻寬適用於所有建立的連線。

   b. 針對第一個位置服務提供者，選取適當的 AWS Direct Connect 位置。

   c. 如適用，將第一個子位置選為最靠近您本身或網路供應商的樓層。此選項僅適用於該位置所在建築物的多個樓層設有匯接機房 (MMR) 的情況。

   d. 如果您對第一個位置服務供應商選取其他，則對其他供應商的名稱，請輸入您使用的合作夥伴名稱。

   e. 針對第二個位置服務提供者，選取適當的 AWS Direct Connect 位置。

   f. 如適用，將第二個子位置選為最靠近您本身或網路供應商的樓層。此選項僅適用於該位置所在建築物的多個樓層設有匯接機房 (MMR) 的情況。

   g. 如果您對第二個位置服務供應商選取其他，則對其他供應商的名稱，請輸入您使用的合作夥伴名稱。

   h. (選用) 新增或移除標籤。

      [新增標籤] 選擇 Add tag (新增標籤)，並執行下列動作：

- 對於 Key (金鑰)，輸入金鑰名稱。
- 在值中，進入索引鍵值。

[移除標籤] 在標籤旁邊，選擇 移除標籤。

6. 選擇下一步。
7. 檢閱您的連線，然後選擇 Continue (繼續)。

   如果您的 LOA 已就緒，您可以選擇 Download LOA (下載 LOA)，然後按一下 Continue(繼續)。

   最多可能需要 72 小時 AWS 才能檢閱您的請求，並為您的連線佈建連接埠。在此期間，您可能會收到一封電子郵件，要求您就自身使用案例或指定的據點補齊更多資訊。電子郵件會傳送至您在註冊時使用的電子郵件地址 AWS。您必須在 7 日內回覆，否則將刪除連線。

步驟 3：建立您的虛擬介面

您可以建立私有虛擬介面以連接到您的 VPC。或者，您可以建立公有虛擬介面，以連線至不在 VPC 中的公有 AWS 服務。建立通往 VPC 的私有虛擬介面時，您所連接的每個 VPC 都需要一個私有虛擬介面。例如，連接到三個 VPC 共需要三個私有虛擬介面。

開始之前，請務必備妥下列資訊：

資源	必要資訊
Connection (連線)	您要為其建立虛擬介面的 AWS Direct Connect 連線或連結彙總群組 (LAG)。
虛擬介面名稱	虛擬介面的名稱。
虛擬介面擁有者	如果您要為另一個帳戶建立虛擬介面，則需要另一個帳戶 AWS 的帳戶 ID。
(僅限私有虛擬介面) 連線	若要連線到相同區域中的 VPC AWS ，您需要 VPC 的虛擬私有閘道。BGP 工作階段的 Amazon 端 ASN 是繼承自虛擬私有閘道。當您建立虛擬私有閘道時，您可指定自己的私有 ASN。否則，Amazon 會提供預設的 ASN。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的建立虛擬私有閘道。若要透過 Direct Connect 閘道連線至 VPC，您需要該 Direct Connect 閘道。如需詳細資訊，請參閱 Direct Connect 閘道。

資源	必要資訊
VLAN	您的連線尚未使用的唯一虛擬區域網路 (VLAN) 標籤。此值必須介於 1 到 4094 之間，且必須符合乙太網路 802.1Q 標準。任何周遊 AWS Direct Connect 連線的流量都需使用此標籤。 如果您有託管連線，您的 AWS Direct Connect 合作夥伴會提供此值。建立虛擬介面後，就無法修改該值。

資源	必要資訊

對等 IP 地址	虛擬介面可以支援 IPv4、IPv6 或其中一個 (雙堆疊) 的 BGP 對等工作階段。請勿使用彈性 IPs(EIPs) 或從 Amazon 集區使用您自己的 IP 地址 (BYOIP) 來建立公有虛擬介面。您無法在相同的虛擬介面上為相同 IP 地址系列建立多個 BGP 工作階段。IP 地址範圍會指派給 BGP 對等工作階段之虛擬介面的每一端。
	
	• IPv4：
	  • (僅限公有虛擬介面) 您必須指定您擁有的唯一公有 IPv4 地址。值可為下列其中之一：
	  • 客戶擁有的 IPv4 CIDR
	
	這些可以是任何公有 IPs（客戶擁有或提供 AWS)，但相同的子網路遮罩必須同時用於對等 IP 和 AWS 路由器對等 IP。例如，如果您配置/31範圍，例如 `203.0.113.0/31` ，則可以將 `203.0.113.0` 用於對等 IP 和 `203.0.113.1` 用於 AWS 對等 IP。或者，如果您配置/24範圍，例如 `198.51.100.0/24` ，則可以將 `198.51.100.10` 用於對等 IP 和`198.51.100.20` 對 AWS 等 IP。
	  • AWS Direct Connect 合作夥伴或 ISP 擁有的 IP 範圍，以及 LOA-CFA 授權
	  • AWS提供的 /31 CIDR。請聯絡 AWS Support 以請求公有 IPv4 CIDR (並在請求中提供使用案例)
	
	Note
	我們無法保證我們能夠滿足 AWS提供公有 IPv4 地址的所有請求。
	
	  • (僅限私有虛擬介面) Amazon 可以為您產生私有 IPv4 地址。如果您指定自己的 CIDRs。 AWS 例如，請勿從您的本機網路指定其他 IP 地址。與公有虛擬介面類似，您的對等 IP 和 AWS 路由器對等 IP 必須使用相同的子網路遮罩。例如，如果您配置/30範圍，例如 `192.168.0.0/30` ，則可以將 `192.168.0.1` 用於對等 IP 和 `192.168.0.2` 用於 AWS 對等 IP。
	• IPv6：Amazon 會自動為您配置一個 /125 IPv6 CIDR。您無法指定自己的對等 IPv6 地址。

資源	必要資訊
地址系列	BGP 對等工作階段是否會透過 IPv4 或 IPv6 進行。
BGP 資訊	• BGP 工作階段在您這端的公有或私有邊界閘道協定 (BGP) 自治系統編號 (ASN)。您必須擁有公有 ASN 才能使用。如果您使用的是私有 ASN，即可設定自訂 ASN 值。對於 16 位元的 ASN，此值的範圍必須為 64512 到 65534。對於 32 位元的 ASN，此值的範圍必須為 1 到 2147483647。如果您使用私有 ASN 做為公有虛擬介面，則自治系統 (AS) 前置無法運作。 • AWS 預設會啟用 MD5。您無法修改此選項。 • 一個 MD5 BGP 驗證金鑰。您可以提供自己的資訊，或是由 Amazon 為您生成。

(僅限公有虛擬介面) 您要公告的字首	要透過 BGP 公告的公有 IPv4 路由或 IPv6 路由。您必須使用 BGP 公告至少一個字首，最多可公告 1,000 個字首。
	• IPv4：當下列任一情況成立 AWS Direct Connect 時，IPv4 CIDR 可以與使用 宣布的另一個公有 IPv4 CIDR 重疊：
	  • CIDRs 來自不同的 AWS 區域。請確定您在公有字首上套用 BGP 社群標籤。
	  • 主動/被動組態中具備公有 ASN 時，您可以使用 AS_PATH。
	  如需更多資訊，請參閱路由政策和 BGP 社群。
	• 透過 Direct Connect 公有虛擬介面，您可以為 IPv4 指定從 /1 到 /32 的任何字首長度，並為 IPv6 指定從 /1 到 /IPv64 的任何字首長度。
	• 您可以將其他字首新增至現有的公有 VIF，並透過聯絡 AWS 支援部門來公告。在您的支援案例中，提供您要新增至公有 VIF 並公告的其他 CIDR 字首清單。

資源	必要資訊
（僅限私有和傳輸虛擬介面）巨型訊框	封包經過的最大傳輸單位 (MTU) AWS Direct Connect。預設值為 1500。設定虛擬介面的 MTU 為 9001 (巨型訊框)，可能導致基礎實體連線的更新，如果未更新到支援巨型訊框。更新連線會干擾所有連線相關聯的虛擬介面的網路連線能力達 30 秒。巨型訊框僅適用於從 傳播的路由 AWS Direct Connect。如果您將靜態路由新增至指向虛擬私有閘道的路由表格，則透過靜態路由傳送的流量會使用 1500 MTU。若要檢查連線或虛擬介面是否支援巨型訊框，請在 AWS Direct Connect 主控台中選取它，然後在虛擬介面一般組態頁面上尋找支援的巨型訊框。

如果您的公有字首或 ASNs屬於 ISP 或網路電信業者， 會向您 AWS 請求其他資訊。其形式可能是採用公司信箋的正式行文或寄自公司網域名稱的電子郵件，以茲確認該網路字首/ASN 可供您使用。

當您建立公有虛擬介面時， 最多可能需要 72 小時 AWS 才能檢閱和核准您的請求。

佈建公有虛擬介面連往非 VPC 服務

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2. 在導覽窗格中，選擇 Virtual Interfaces (虛擬介面)。
3. 選擇建立虛擬介面。
4. 在虛擬介面類型之下，針對類型選擇公有。
5. 在公有虛擬介面設定 之下，執行下列動作：

   a. 針對虛擬介面名稱，輸入虛擬介面的名稱。

   b. 針對連線，選擇要用於此介面的 Direct Connect 連線。

   c. 針對 VLAN，為您的虛擬區域網路 (VLAN) 輸入 ID 號碼。

   d. 針對 BGP ASN，輸入您閘道的邊界閘道協定 (BGP) 自發系統編號 (ASN)。

      有效值為 1-2147483647。
6. 在 Additional settings (其他設定) 之下，執行下列動作：

   a. 若要設定 IPv4 BGP 或 IPv6 對等，請執行下列動作：

      [IPv4] 若要設定 IPv4 BGP 對等，請選擇 IPv4，然後執行以下動作：

- 若要自行指定這些 IP 地址，對於 Your router peer ip (您的路由器對等 IP)，輸入 Amazon 應傳送流量至該處的目的地 IPv4 CIDR 地址。
- 對於 Amazon router peer IP (Amazon 路由器對等 IP)，輸入用以傳送流量至 AWS的 IPv4 CIDR 地址。

[IPv6] 若要設定 IPv6 BGP 對等，請選擇 IPv6。對等 IPv6 地址是自動從 Amazon 的 IPv6 地址集區所指派。您無法指定自訂 IPv6 地址。

b. 若要提供自己的 BGP 金鑰，請輸入您的 BGP MD5 金鑰。

如果您未輸入值，我們會產生 BGP 金鑰。

c. 若要對 Amazon 公告字首，對於欲公告的字首，輸入應透過虛擬介面將流量路由傳送至該處的目的地 IPv4 CIDR 地址 (以逗號分隔)。

d. (選用) 新增或移除標籤。

[新增標籤] 選擇 Add tag (新增標籤)，並執行下列動作：

- 對於 Key (金鑰)，輸入金鑰名稱。
- 在值中，進入索引鍵值。

[移除標籤] 在標籤旁邊，選擇 移除標籤。

7. 選擇建立虛擬介面。

佈建私有虛擬介面連往 VPC

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2. 在導覽窗格中，選擇 Virtual Interfaces (虛擬介面)。
3. 選擇建立虛擬介面。
4. 在虛擬介面類型之下，對於類型，請選擇私有。
5. 在公有虛擬介面設定之下，執行下列動作：

a. 針對虛擬介面名稱，輸入虛擬介面的名稱。

b. 針對連線，選擇要用於此介面的 Direct Connect 連線。

c. 對於閘道類型，選擇「虛擬私有閘道」或「Direct Connect 閘道」。

d. 對於虛擬介面擁有者，選擇另一個 AWS 帳戶，然後輸入 AWS 帳戶。

e. 對於虛擬私有閘道，請選擇您用於此介面的虛擬私有閘道。

f. 針對 VLAN，為您的虛擬區域網路 (VLAN) 輸入 ID 號碼。

g. 針對 BGP ASN，為新的虛擬介面輸入您內部部署對等路由器的邊界閘道協定自治系統編號。

有效值為 1 至 2147483647。

6. 在 Additional settings (其他設定) 之下，執行下列動作：

a. 若要設定 IPv4 BGP 或 IPv6 對等，請執行下列動作：

[IPv4] 若要設定 IPv4 BGP 對等，請選擇 IPv4，然後執行以下動作：

- 若要自行指定這些 IP 地址，對於 Your router peer ip (您的路由器對等 IP)，輸入 Amazon 應傳送流量至該處的目的地 IPv4 CIDR 地址。
- 對於 Amazon 路由器對等 IP，輸入用以傳送流量至 AWS的 IPv4 CIDR 地址。

> **Important**
>
> 設定 AWS Direct Connect 虛擬介面時，您可以使用 RFC 1918 指定自己的 IP 地址、使用其他定址機制，或選擇從 RFC 3927 169.25IPv4.0.0/16 IPv4 Link-Local 範圍配置的 AWS 指派 IPv4/29 CIDR 地址point-to-point連線。這些point-to-point連線應僅用於客戶閘道路由器和 Direct Connect 端點之間的 eBGP 互連。針對 VPC 流量或通道用途，例如 AWS Site-to-Site私有 IP VPN 或 Transit Gateway Connect， AWS 建議使用客戶閘道路由器上的迴路或 LAN 介面做為來源或目的地地址，而非point-to-point連線。
>
> - 如需有關 RFC 1918 的詳細資訊，請參閱私有網路的地址配置。
> - 如需有關 RFC 3927 的詳細資訊，請參閱 IPv4 Link-Local 地址的動態組態。

[IPv6] 若要設定 IPv6 BGP 對等，請選擇 IPv6。對等 IPv6 地址是自動從 Amazon 的 IPv6 地址集區所指派。您無法指定自訂 IPv6 地址。

b. 若要將最大傳輸單位 (MTU) 從 1500 (預設) 變更至 9001 (巨型框架)，請選取巨型 MTU (MTU 大小 9001)。

c. (選用) 在啟用 SiteLink 之下，選擇啟用以啟用 Direct Connect 連接點之間的直接連線。

d. (選用) 新增或移除標籤。

[新增標籤] 選擇 Add tag (新增標籤)，並執行下列動作：

- 對於 Key (金鑰)，輸入金鑰名稱。
- 在值中，進入索引鍵值。

[移除標籤] 在標籤旁邊，選擇 移除標籤。

7. 選擇建立虛擬介面。

步驟 4：驗證您的虛擬介面彈性組態

在您建立 AWS 雲端或 Amazon VPC 的虛擬介面之後，請執行虛擬介面容錯移轉測試，以確認您的組態符合您的彈性需求。如需詳細資訊，請參閱the section called “Direct Connect 容錯移轉測試”。

步驟 5：驗證您的虛擬介面連線能力

建立 AWS 雲端或 Amazon VPC 的虛擬介面之後，您可以使用下列程序驗證您的 AWS Direct Connect 連線。

驗證與 AWS 雲端的虛擬介面連線

- 執行`traceroute`並確認 AWS Direct Connect 識別符位於網路追蹤中。

驗證虛擬介面至 Amazon VPC 的連線

1. 使用可透過 ping 存取的 AMI 如 Amazon Linux AMI，在連接至虛擬私有閘道的 VPC 中啟動 EC2 執行個體。當您使用 Amazon EC2 主控台的執行個體啟動精靈時，可在快速入門索引標籤取得 Amazon Linux AMI。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的啟動執行個體。Amazon EC2 確認與執行個體關聯的安全群組，包含一個規則允許流量傳入 ICMP (適用於 ping 請求)。
2. 待執行個體執行之後，取得其私有 IPv4 地址 (例如 10.0.0.4)。Amazon EC2 主控台顯示的執行個體詳細資訊將包含該地址。
3. Ping 到該私有 IPv4 地址並獲得回應。

使用 AWS Direct Connect 彈性工具組來設定 AWS Direct Connect 開發和測試彈性

在此範例中， AWS Direct Connect 彈性工具組用於設定開發和測試彈性模型

任務

- 步驟 1：註冊 AWS

- 步驟 2：設定彈性模型
- 步驟 3：建立虛擬介面
- 步驟 4：驗證您的虛擬介面彈性組態
- 步驟 5：驗證您的虛擬介面

步驟 1：註冊 AWS

若要使用 AWS Direct Connect，如果您還沒有帳戶，則需要 AWS 帳戶。

註冊 AWS 帳戶

如果您沒有 AWS 帳戶，請完成下列步驟來建立一個。

註冊 AWS 帳戶

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

   部分註冊程序需接收來電，並在電話鍵盤輸入驗證碼。

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

AWS 會在註冊程序完成後傳送確認電子郵件給您。您可以隨時登錄 https://aws.amazon.com/ 並選擇我的帳戶，以檢視您目前的帳戶活動並管理帳戶。

建立具有管理存取權的使用者

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

保護您的 AWS 帳戶根使用者

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

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

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

建立具有管理存取權的使用者

1. 啟用 IAM Identity Center。

   如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的啟用 AWS IAM Identity Center。

2. 在 IAM Identity Center 中，將管理存取權授予使用者。

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

以具有管理存取權的使用者身分登入

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

  如需使用 IAM Identity Center 使用者登入的說明，請參閱AWS 登入 《 使用者指南》中的登入 AWS 存取入口網站。

指派存取權給其他使用者

1. 在 IAM Identity Center 中，建立一個許可集來遵循套用最低權限的最佳實務。

   如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的建立許可集。

2. 將使用者指派至群組，然後對該群組指派單一登入存取權。

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

步驟 2：設定彈性模型

設定彈性模型

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2. 在導覽窗格中，選擇連線，然後選擇建立連線。

3. 在 Connection ordering type (連線訂購類型) 下，選擇 Connection wizard (連線精靈)。
4. 在 Resiliency level (彈性層級) 下，選擇 Development and test (開發和測試)，然後選擇 Next (下一步)。
5. 在 Configure connections (設定連線) 窗格的 Connection settings (連線設定) 下，執行下列動作：

   a. 對於 bandwidth (頻寬)，選擇連線頻寬。

      此頻寬適用於所有建立的連線。

   b. 針對第一個位置服務提供者，選取適當的 AWS Direct Connect 位置。

   c. 如適用，將第一個子位置選為最靠近您本身或網路供應商的樓層。此選項僅適用於該位置所在建築物的多個樓層設有匯接機房 (MMR) 的情況。

   d. 如果您對第一個位置服務供應商選取其他，則對其他供應商的名稱，請輸入您使用的合作夥伴名稱。

   e. (選用) 新增或移除標籤。

      [新增標籤] 選擇 Add tag (新增標籤)，並執行下列動作：

      - 對於 Key (金鑰)，輸入金鑰名稱。
      - 在值中，進入索引鍵值。

      [移除標籤] 在標籤旁邊，選擇 移除標籤。
6. 選擇下一步。
7. 檢閱您的連線，然後選擇 Continue (繼續)。

   如果您的 LOA 已就緒，您可以選擇 Download LOA (下載 LOA)，然後按一下 Continue(繼續)。

   最多可能需要 72 小時 AWS 才能檢閱您的請求，並為您的連線佈建連接埠。在此期間，您可能會收到一封電子郵件，要求您就自身使用案例或指定的據點補齊更多資訊。電子郵件會傳送至您在註冊時使用的電子郵件地址 AWS。您必須在 7 日內回覆，否則將刪除連線。

步驟 3：建立虛擬介面

若要開始使用您的 AWS Direct Connect 連線，您必須建立虛擬界面。您可以建立私有虛擬介面以連接到您的 VPC。或者，您可以建立公有虛擬介面，以連線至不在 VPC 中的公有 AWS 服務。建立通往 VPC 的私有虛擬介面時，您所連接的每個 VPC 都需要一個私有虛擬介面。例如，連接到三個 VPC 共需要三個私有虛擬介面。

開始之前，請務必備妥下列資訊：

資源	必要資訊
Connection (連線)	您要為其建立虛擬介面的 AWS Direct Connect 連線或連結彙總群組 (LAG)。
虛擬介面名稱	虛擬介面的名稱。
虛擬介面擁有者	如果您要為另一個帳戶建立虛擬介面，則需要另一個帳戶 AWS 的帳戶 ID。
(僅限私有虛擬介面) 連線	若要連線到相同區域中的 VPC AWS ，您需要 VPC 的虛擬私有閘道。BGP 工作階段的 Amazon 端 ASN 是繼承自虛擬私有閘道。當您建立虛擬私有閘道時，您可指定自己的私有 ASN。否則，Amazon 會提供預設的 ASN。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的建立虛擬私有閘道。若要透過 Direct Connect 閘道連線至 VPC，您需要該 Direct Connect 閘道。如需詳細資訊，請參閱 Direct Connect 閘道。
VLAN	您的連線尚未使用的唯一虛擬區域網路 (VLAN) 標籤。此值必須介於 1 到 4094 之間，且必須符合乙太網路 802.1Q 標準。任何周遊 AWS Direct Connect 連線的流量都需使用此標籤。 如果您有託管連線，您的 AWS Direct Connect 合作夥伴會提供此值。建立虛擬介面後，就無法修改該值。

對等 IP 地址	虛擬介面可以支援 IPv4、IPv6 或其中一個 (雙堆疊) 的 BGP 對等工作階段。請勿使用彈性 IPs(EIPs) 或從 Amazon 集區使用您自己的 IP 地址 (BYOIP) 來建立公有虛擬介面。您無法在相同的虛擬介面上為相同 IP 地址系列建立多個 BGP 工作階段。IP 地址範圍會指派給 BGP 對等工作階段之虛擬介面的每一端。
	
	• IPv4：
	  • (僅限公有虛擬介面) 您必須指定您擁有的唯一公有 IPv4 地址。值可為下列其中之一：
	  • 客戶擁有的 IPv4 CIDR
	
	這些可以是任何公有 IPs (客戶擁有或提供 AWS)，但您的對等 IP 和 AWS 路由器對等 IP 都必須使用相同的子網路遮罩。例如，如果您配置/31範圍，例如 `203.0.113.0/31` ，則可以將 `203.0.113.0` 用於對等 IP 和 `203.0.113.1` 用於 AWS 對等 IP。或者，如果您配

資源	必要資訊
	置/24範圍，例如 198.51.100.0/24 ，您可以將 198.51.100.10 用於對等 IP 和198.51.100.20 對 AWS 等 IP。 • AWS Direct Connect 合作夥伴或 ISP 擁有的 IP 範圍，以及 LOA-CFA 授權 • AWS提供的 /31 CIDR。請聯絡 AWS Support 以請求公有 IPv4 CIDR (並在請求中提供使用案例) **Note** 我們無法保證我們能夠滿足 AWS提供公有 IPv4 地址的所有請求。 • (僅限私有虛擬介面) Amazon 可以為您產生私有 IPv4 地址。如果您指定自己的 CIDRs。 AWS 例如，請勿從您的本機網路指定其他 IP 地址。與公有虛擬介面類似，相同的子網路遮罩必須同時用於對等 IP 和 AWS 路由器對等 IP。例如，如果您配置/30範圍，例如 192.168.0.0/30 ，則可以將 192.168.0.1 用於對等 IP 和 192.168.0.2 用於 AWS 對等 IP。 • IPv6：Amazon 會自動為您配置一個 /125 IPv6 CIDR。您無法指定自己的對等 IPv6 地址。
地址系列	BGP 對等工作階段是否會透過 IPv4 或 IPv6 進行。
BGP 資訊	• BGP 工作階段在您這端的公有或私有邊界閘道協定 (BGP) 自治系統編號 (ASN)。您必須擁有公有 ASN 才能使用。如果您使用的是私有 ASN，即可設定自訂 ASN 值。對於 16 位元的 ASN，此值的範圍必須為 64512 到 65534。對於 32 位元的 ASN，此值的範圍必須為 1 到 2147483647。如果您使用私有 ASN 做為公有虛擬介面，則自治系統 (AS) 前置無法運作。 • AWS 根據預設， 會啟用 MD5。您無法修改此選項。 • 一個 MD5 BGP 驗證金鑰。您可以提供自己的資訊，或是由 Amazon 為您生成。

資源	必要資訊

(僅限公有虛擬介面) 您要公告的字首	要透過 BGP 公告的公有 IPv4 路由或 IPv6 路由。您必須使用 BGP 公告至少一個字首，最多可公告 1,000 個字首。
	• IPv4：當下列任一情況成立 AWS Direct Connect 時，IPv4 CIDR 可以與使用 宣布的另一個公有 IPv4 CIDR 重疊：
	  • CIDRs 來自不同的 AWS 區域。請確定您在公有字首上套用 BGP 社群標籤。
	  • 主動/被動組態中具備公有 ASN 時，您可以使用 AS_PATH。
	  如需更多資訊，請參閱路由政策和 BGP 社群。
	• 透過 Direct Connect 公有虛擬界面，您可以為 IPv4 指定從 /1 到 /32 的任何字首長度，並為 IPv6 指定從 /1 到 /IPv64 的任何字首長度。
	• 您可以將其他字首新增至現有的公有 VIF，並透過聯絡 AWS 支援部門來公告。在您的支援案例中，提供您要新增至公有 VIF 並公告的其他 CIDR 字首清單。

（僅限私有和傳輸虛擬介面） 巨型訊框	封包經過的最大傳輸單位 (MTU) AWS Direct Connect。預設值為 1500。設定虛擬介面的 MTU 為 9001 (巨型訊框)，可能導致基礎實體連線的更新，如果未更新到支援巨型訊框。更新連線會干擾所有連線相關聯的虛擬介面的網路連線能力達 30 秒。巨型訊框僅適用於從 傳播的路由 AWS Direct Connect。如果您將靜態路由新增至指向虛擬私有閘道的路由表格，則透過靜態路由傳送的流量會使用 1500 MTU。若要檢查連線或虛擬介面是否支援巨型訊框，請在 AWS Direct Connect 主控台中選取它，然後在虛擬介面一般組態頁面上尋找能夠使用的巨型訊框。

如果您的公有字首或 ASN 屬於某家 ISP 或網路電信業者，我們會要求您提供額外的資訊。其形式可能是採用公司信箋的正式行文或寄自公司網域名稱的電子郵件，以茲確認該網路字首/ASN 可供您使用。

建立公有虛擬介面之後， AWS 從審查到核准您的申請可能需要 72 小時的時間。

佈建公有虛擬介面連往非 VPC 服務

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2. 在導覽窗格中，選擇 Virtual Interfaces (虛擬介面)。

3. 選擇建立虛擬介面。
4. 在虛擬介面類型之下，針對類型選擇公有。
5. 在公有虛擬介面設定 之下，執行下列動作：

   a. 針對虛擬介面名稱，輸入虛擬介面的名稱。

   b. 針對連線，選擇要用於此介面的 Direct Connect 連線。

   c. 針對 VLAN，為您的虛擬區域網路 (VLAN) 輸入 ID 號碼。

   d. 針對 BGP ASN，輸入您閘道的邊界閘道協定 (BGP) 自發系統編號 (ASN)。

      有效值為 1-2147483647。
6. 在 Additional settings (其他設定) 之下，執行下列動作：

   a. 若要設定 IPv4 BGP 或 IPv6 對等，請執行下列動作：

      [IPv4] 若要設定 IPv4 BGP 對等，請選擇 IPv4，然後執行以下動作：

      - 若要自行指定這些 IP 地址，對於 Your router peer ip (您的路由器對等 IP)，輸入 Amazon 應傳送流量至該處的目的地 IPv4 CIDR 地址。
      - 對於 Amazon router peer IP (Amazon 路由器對等 IP)，輸入用以傳送流量至 AWS的 IPv4 CIDR 地址。

      [IPv6] 若要設定 IPv6 BGP 對等，請選擇 IPv6。對等 IPv6 地址是自動從 Amazon 的 IPv6 地址集區所指派。您無法指定自訂 IPv6 地址。

   b. 若要提供自己的 BGP 金鑰，請輸入您的 BGP MD5 金鑰。

      如果您未輸入值，我們會產生 BGP 金鑰。

   c. 若要對 Amazon 公告字首，對於欲公告的字首，輸入應透過虛擬介面將流量路由傳送至該處的目的地 IPv4 CIDR 地址 (以逗號分隔)。

   d. (選用) 新增或移除標籤。

      [新增標籤] 選擇 Add tag (新增標籤)，並執行下列動作：

      - 對於 Key (金鑰)，輸入金鑰名稱。
      - 在值中，進入索引鍵值。

      [移除標籤] 在標籤旁邊，選擇 移除標籤。
7. 選擇建立虛擬介面。

佈建私有虛擬介面連往 VPC

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2. 在導覽窗格中，選擇 Virtual Interfaces (虛擬介面)。
3. 選擇建立虛擬介面。
4. 在虛擬介面類型之下，對於類型，請選擇私有。
5. 在公有虛擬介面設定之下，執行下列動作：

   a. 針對虛擬介面名稱，輸入虛擬介面的名稱。

   b. 針對連線，選擇要用於此介面的 Direct Connect 連線。

   c. 對於閘道類型，選擇「虛擬私有閘道」或「Direct Connect 閘道」。

   d. 對於虛擬介面擁有者，選擇另一個 AWS 帳戶，然後輸入 AWS 帳戶。

   e. 對於虛擬私有閘道，請選擇您用於此介面的虛擬私有閘道。

   f. 針對 VLAN，為您的虛擬區域網路 (VLAN) 輸入 ID 號碼。

   g. 針對 BGP ASN，為新的虛擬介面輸入您內部部署對等路由器的邊界閘道協定自治系統編號。

   有效值為 1 至 2147483647。
6. 在 Additional settings (其他設定) 之下，執行下列動作：

   a. 若要設定 IPv4 BGP 或 IPv6 對等，請執行下列動作：

   [IPv4] 若要設定 IPv4 BGP 對等，請選擇 IPv4，然後執行以下動作：

   - 若要自行指定這些 IP 地址，對於 Your router peer ip (您的路由器對等 IP)，輸入 Amazon 應傳送流量至該處的目的地 IPv4 CIDR 地址。
   - 對於 Amazon 路由器對等 IP，輸入用以傳送流量至 AWS的 IPv4 CIDR 地址。

   > **Important**
   >
   > 設定 AWS Direct Connect 虛擬介面時，您可以使用 RFC 1918 指定自己的 IP 地址、使用其他定址機制，或選擇從 RFC 3927 169.25IPv4.0.0/16 IPv4 Link-Local 範圍配置的 AWS 指派 IPv4/29 CIDR 地址point-to-point連線。這些point-to-point連線應僅用於客戶閘道路由器和 Direct Connect 端點之間的 eBGP 互連。針對 VPC 流量或通道用途，例如 AWS Site-to-Site私有 IP VPN 或 Transit Gateway Connect， AWS 建議使用客戶閘道路由器上的迴路或 LAN 界面做為來源或目的地地址，而非point-to-point連線。

- 如需有關 RFC 1918 的詳細資訊，請參閱私有網路的地址配置。
- 如需有關 RFC 3927 的詳細資訊，請參閱 IPv4 Link-Local 地址的動態組態。

[IPv6] 若要設定 IPv6 BGP 對等，請選擇 IPv6。對等 IPv6 地址是自動從 Amazon 的 IPv6 地址集區所指派。您無法指定自訂 IPv6 地址。

b. 若要將最大傳輸單位 (MTU) 從 1500 (預設) 變更至 9001 (巨型框架)，請選取巨型 MTU (MTU 大小 9001)。

c. (選用) 在啟用 SiteLink 之下，選擇啟用以啟用 Direct Connect 連接點之間的直接連線。

d. (選用) 新增或移除標籤。

[新增標籤] 選擇 Add tag (新增標籤)，並執行下列動作：

- 對於 Key (金鑰)，輸入金鑰名稱。
- 在值中，進入索引鍵值。

[移除標籤] 在標籤旁邊，選擇 移除標籤。

7. 選擇建立虛擬介面。

步驟 4：驗證您的虛擬介面彈性組態

在您建立 AWS 雲端或 Amazon VPC 的虛擬介面之後，請執行虛擬介面容錯移轉測試，以確認您的組態符合您的彈性需求。如需詳細資訊，請參閱the section called “Direct Connect 容錯移轉測試”。

步驟 5：驗證您的虛擬介面

建立 AWS 雲端或 Amazon VPC 的虛擬介面之後，您可以使用下列程序來驗證您的 AWS Direct Connect 連線。

驗證與 AWS 雲端的虛擬介面連線

- 執行`traceroute`並確認 AWS Direct Connect 識別符位於網路追蹤中。

驗證虛擬介面至 Amazon VPC 的連線

1. 使用可透過 ping 存取的 AMI 如 Amazon Linux AMI，在連接至虛擬私有閘道的 VPC 中啟動 EC2 執行個體。當您使用 Amazon EC2 主控台的執行個體啟動精靈時，可在快速入門索引標籤取得 Amazon Linux AMI。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的啟動執行個體。

Amazon EC2 確認與執行個體關聯的安全群組，包含一個規則允許流量傳入 ICMP (適用於 ping 請求)。

2. 待執行個體執行之後，取得其私有 IPv4 地址 (例如 10.0.0.4)。Amazon EC2 主控台顯示的執行個體詳細資訊將包含該地址。
3. Ping 到該私有 IPv4 地址並獲得回應。

設定 AWS Direct Connect Classic 連線

當您有現有的 Direct Connect 連線時，請設定 Classic 連線。

步驟 1：註冊 AWS

若要使用 AWS Direct Connect，如果您還沒有帳戶，則需要 帳戶。

註冊 。 AWS 帳戶

如果您沒有 AWS 帳戶，請完成下列步驟來建立一個。

註冊 AWS 帳戶

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

   部分註冊程序需接收來電，並在電話鍵盤輸入驗證碼。

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

AWS 會在註冊程序完成後傳送確認電子郵件給您。您可以隨時登錄 https://aws.amazon.com/ 並選擇我的帳戶，以檢視您目前的帳戶活動並管理帳戶。

建立具有管理存取權的使用者

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

保護您的 AWS 帳戶根使用者

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

   如需使用根使用者登入的說明，請參閱 AWS 登入 使用者指南中的以根使用者身分登入。

2. 若要在您的根使用者帳戶上啟用多重要素驗證 (MFA)。

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

建立具有管理存取權的使用者

1. 啟用 IAM Identity Center。

   如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的啟用 AWS IAM Identity Center。

2. 在 IAM Identity Center 中，將管理存取權授予使用者。

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

以具有管理存取權的使用者身分登入

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

  如需使用 IAM Identity Center 使用者登入的說明，請參閱AWS 登入 《 使用者指南》中的登入 AWS 存取入口網站。

指派存取權給其他使用者

1. 在 IAM Identity Center 中，建立一個許可集來遵循套用最低權限的最佳實務。

   如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的建立許可集。

2. 將使用者指派至群組，然後對該群組指派單一登入存取權。

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

步驟 2：請求 AWS Direct Connect 專用連線

對於專用連線，您可以使用 AWS Direct Connect 主控台提交連線請求。對於託管連線，請與 AWS Direct Connect 合作夥伴合作請求託管連線。請務必備妥下列資訊：

- 您需要的連接埠速度。在您建立連線要求之後，就無法變更連接埠速度。
- 要終止連線 AWS Direct Connect 的位置。

> **Note**
>
> 您無法使用 AWS Direct Connect 主控台請求託管連線。反之，請聯絡 AWS Direct Connect 合作夥伴，他們可以為您建立您接著接受的託管連線。略過以下程序並前往 接受託管連線。

建立新的 AWS Direct Connect 連線

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2. 在導覽窗格中，選擇連線，然後選擇建立連線。
3. 選擇 Classic (傳統)。
4. 在 Create Connection (建立連線) 窗格的 Connection settings (連線設定) 之下，執行下列動作：
   a. 對於 Name (連線)，輸入連線的名稱。
   b. 對於 Location (據點)，選取合適的 AWS Direct Connect 據點。
   c. 如適用，將 Sub Location (子據點) 選為最靠近您本身或網路供應商的樓層。此選項僅適用於該據點所在建築物的多個樓層設有匯接機房 (MMR) 的情況。
   d. 對於 Port Speed (連接埠速度)，選擇連線頻寬。
   e. 對於內部部署，當您使用此連線連線到您的資料中心時，請選取透過 AWS Direct Connect 合作夥伴連線。
   f. 針對服務提供者，選取 AWS Direct Connect 合作夥伴。如果您使用不在清單中的合作夥伴，請選取 Other (其他)。
   g. 如果您對服務供應商選取其他，則對其他供應商的名稱，請輸入您使用的合作夥伴名稱。
   h. (選用) 新增或移除標籤。

      [新增標籤] 選擇 Add tag (新增標籤)，並執行下列動作：

- 對於 Key (金鑰)，輸入金鑰名稱。
- 在值中，進入索引鍵值。

[移除標籤] 在標籤旁邊，選擇 移除標籤。

5. 選擇建立連線。

最多可能需要 72 小時 AWS 才能檢閱您的請求，並為您的連線佈建連接埠。在此期間，您可能會收到一封電子郵件，要求您就自身使用案例或指定的據點補齊更多資訊。電子郵件會傳送至您在註冊時使用的電子郵件地址 AWS。您必須在 7 日內回覆，否則將刪除連線。

如需詳細資訊，請參閱AWS Direct Connect 專用和託管連線。

接受託管連線

您必須先接受 AWS Direct Connect 主控台中的託管連線，才能建立虛擬介面。此步驟僅適用於託管連線。

接受託管虛擬介面

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2. 在導覽窗格中，選擇 Connections (連線)。
3. 選取託管連線，然後選擇「接受」。

   選擇 Accept (接受)。

(專用連線) 步驟 3：下載 LOA-CFA

在您申請連線之後，我們會提供《授權書和連線設施指派》(LOA-CFA) 讓您下載，也可能寄發電子郵件要求您補齊更多資訊。LOA-CFA 是連線的授權 AWS，主機代管提供者或您的網路提供者需要此授權才能建立跨網路連線 （ 交叉連線 ）。

下載 LOA-CFA

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2. 在導覽窗格中，選擇 Connections (連線)。
3. 選取連線，然後選擇 View Details (檢視詳細資訊)。

4. 選擇 Download LOA-CFA (下載 LOA-CFA)。

   PDF 檔案格式的 LOA-CFA 即會下載到您的電腦。

   > **Note**
   >
   > 如果該連結為未啟用狀態，即表示尚未提供 LOA-CFA 讓您下載。請檢查您是否收到要求補齊更多資訊的電子郵件。若仍然無法使用，或是您在 72 小時之後還未收到電子郵件，請聯絡 AWS Support。

5. 下載 LOA-CFA 之後，執行以下其中一項操作：

   - 如果您與 AWS Direct Connect 合作夥伴或網路提供者合作，請將 LOA-CFA 傳送給他們，讓他們可以在 AWS Direct Connect 位置為您訂購交叉連線。若對方無法為您訂購交叉連接，您可以直接聯繫主機代管服務供應商。
   - 如果您在 AWS Direct Connect 據點有設備，請聯絡主機代管供應商請求跨網路連線。您必須是主機代管供應商的客戶。您也必須向他們提供 LOA-CFA，該 LOA-CFA 授權 AWS 路由器的連線，以及連線至您的網路所需的資訊。

AWS Direct Connect 列為多個站台的位置 （ 例如，Equinix DC1-DC6 和 DC10-DC11) 會設定為校園。若您的設備或網路供應商的設備位於任一個這類站點，您便能夠申請交叉連接至您指派的連接埠，即使該連接埠位不同園區建築物。

> **Important**
>
> 校園視為單一 AWS Direct Connect 位置。為了實現高可用性，請設定連線到不同的 AWS Direct Connect 位置。

如果您本身或網路供應商在建立實體連線時遭遇問題，請參閱 診斷排解第 1 層 (實體) 問題。

步驟 4：建立虛擬介面

若要開始使用您的 AWS Direct Connect 連線，您必須建立虛擬界面。您可以建立私有虛擬介面以連接到您的 VPC。或者，您可以建立公有虛擬介面，以連線至不在 VPC 中的公有 AWS 服務。建立連往 VPC 的私有虛擬介面時，連接的每個 VPC 都需要一個私有虛擬介面。例如，連接到三個 VPC 共需要三個私有虛擬介面。

開始之前，請務必備妥下列資訊：

資源	必要資訊
Connection (連線)	您要為其建立虛擬介面的 AWS Direct Connect 連線或連結彙總群組 (LAG)。
虛擬介面名稱	虛擬介面的名稱。
虛擬介面擁有者	如果您要為另一個帳戶建立虛擬介面，則需要另一個帳戶 AWS 的帳戶 ID。
(僅限私有虛擬介面) 連線	若要連線到相同區域中的 VPC AWS ，您需要 VPC 的虛擬私有閘道。BGP 工作階段的 Amazon 端 ASN 是繼承自虛擬私有閘道。當您建立虛擬私有閘道時，您可指定自己的私有 ASN。否則，Amazon 會提供預設的 ASN。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的建立虛擬私有閘道。若要透過 Direct Connect 閘道連線至 VPC，您需要該 Direct Connect 閘道。如需詳細資訊，請參閱 Direct Connect 閘道。
VLAN	您的連線尚未使用的唯一虛擬區域網路 (VLAN) 標籤。此值必須介於 1 到 4094 之間，且必須符合乙太網路 802.1Q 標準。任何周遊 AWS Direct Connect 連線的流量都需使用此標籤。 如果您有託管連線，您的 AWS Direct Connect 合作夥伴會提供此值。建立虛擬介面後，就無法修改該值。

對等 IP 地址	虛擬介面可以支援 IPv4、IPv6 或其中一個 (雙堆疊) 的 BGP 對等工作階段。請勿使用彈性 IPs(EIPs) 或從 Amazon 集區使用您自己的 IP 地址 (BYOIP) 來建立公有虛擬介面。您無法在相同的虛擬介面上為相同 IP 地址系列建立多個 BGP 工作階段。IP 地址範圍會指派給 BGP 對等工作階段之虛擬介面的每一端。
	
	• IPv4：
	  • (僅限公有虛擬介面) 您必須指定您擁有的唯一公有 IPv4 地址。值可為下列其中之一：
	  • 客戶擁有的 IPv4 CIDR
	
	這些可以是任何公有 IPs (客戶擁有或提供 AWS)，但相同的子網路遮罩必須同時用於對等 IP 和 AWS 路由器對等 IP。例如，如果您配置/31範圍，例如 `203.0.113.0/31` ，則可以將 `203.0.113.0` 用於對等 IP 和 `203.0.113.1` 用於 AWS 對等 IP。或者，如果您配置/24範圍，

資源	必要資訊
	例如 198.51.100.0/24 ，則可以將 198.51.100.10 用於對等 IP 和198.51.100.20 對 AWS 等 IP。 • AWS Direct Connect 合作夥伴或 ISP 擁有的 IP 範圍，以及 LOA-CFA 授權 • AWS提供的 /31 CIDR。請聯絡 AWS Support 以請求公有 IPv4 CIDR (並在請求中提供使用案例) **Note** 我們無法保證我們能夠滿足 AWS提供公有 IPv4 地址的所有請求。 • (僅限私有虛擬介面) Amazon 可以為您產生私有 IPv4 地址。如果您指定自己的 CIDRs。 AWS 例如，請勿從您的本機網路指定其他 IP 地址。與公有虛擬介面類似，您的對等 IP 和 AWS 路由器對等 IP 必須使用相同的子網路遮罩。例如，如果您配置/30範圍，例如 192.168.0.0/30 ，則可以將 192.168.0.1 用於對等 IP 和 192.168.0.2 用於 AWS 對等 IP。 • IPv6：Amazon 會自動為您配置一個 /125 IPv6 CIDR。您無法指定自己的對等 IPv6 地址。
地址系列	BGP 對等工作階段是否會透過 IPv4 或 IPv6 進行。
BGP 資訊	• BGP 工作階段在您這端的公有或私有邊界閘道協定 (BGP) 自治系統編號 (ASN)。您必須擁有公有 ASN 才能使用。如果您使用的是私有 ASN，即可設定自訂 ASN 值。對於 16 位元的 ASN，此值的範圍必須為 64512 到 65534。對於 32 位元的 ASN，此值的範圍必須為 1 到 2147483647。如果您使用私有 ASN 做為公有虛擬介面，則自治系統 (AS) 前置無法運作。 • AWS 預設會啟用 MD5。您無法修改此選項。 • 一個 MD5 BGP 驗證金鑰。您可以提供自己的資訊，或是由 Amazon 為您生成。

資源	必要資訊

(僅限公有虛擬介面) 您要公告的字首	要透過 BGP 公告的公有 IPv4 路由或 IPv6 路由。您必須使用 BGP 公告至少一個字首，最多可公告 1,000 個字首。
	• IPv4：當下列任一情況成立 AWS Direct Connect 時，IPv4 CIDR 可以與使用 宣布的另一個公有 IPv4 CIDR 重疊：
	  • CIDRs 來自不同的 AWS 區域。請確定您在公有字首上套用 BGP 社群標籤。
	  • 主動/被動組態中具備公有 ASN 時，您可以使用 AS_PATH。
	  如需更多資訊，請參閱路由政策和 BGP 社群。
	• 透過 Direct Connect 公有虛擬介面，您可以為 IPv4 指定從 /1 到 /32 的任何字首長度，並為 IPv6 指定從 /1 到 /IPv64 的任何字首長度。
	• 您可以將其他字首新增至現有的公有 VIF，並透過聯絡 AWS 支援部門來公告。在您的支援案例中，提供您要新增至公有 VIF 並公告的其他 CIDR 字首清單。

（僅限私有和傳輸虛擬介面） 巨型訊框	封包經過的最大傳輸單位 (MTU) AWS Direct Connect。預設值為 1500。設定虛擬介面的 MTU 為 9001 (巨型訊框)，可能導致基礎實體連線的更新，如果未更新到支援巨型訊框。更新連線會干擾所有連線相關聯的虛擬介面的網路連線能力達 30 秒。巨型訊框僅適用於從 傳播的路由 AWS Direct Connect。如果您將靜態路由新增至指向虛擬私有閘道的路由表格，則透過靜態路由傳送的流量會使用 1500 MTU。若要檢查連線或虛擬介面是否支援巨型訊框，請在 AWS Direct Connect 主控台中選取它，然後在虛擬介面一般組態頁面上尋找能夠使用的巨型訊框。

如果您的公有字首或 ASN 屬於某家 ISP 或網路電信業者，則我們會要求您提供額外的資訊。其形式可能是採用公司信箋的正式行文或寄自公司網域名稱的電子郵件，以茲確認該網路字首/ASN 可供您使用。

對於私有虛擬介面和公有虛擬介面，網路連線的最大傳輸單位 (MTU) 是可透過連線傳遞之最大允許封包的大小 (以位元組為單位)。虛擬私有介面的 MTU 可以是 1500 或 9001 (巨型訊框)。傳輸虛擬介面的 MTU 可以是 1500 或 8500 (巨型訊框)。當您可以在建立介面或在建立後更新時，指定 MTU。設定虛擬介面的 MTU 為 8500 (巨型訊框) 9001 (巨型訊框)，可能導致基礎實體連線的更新，如果未更新到支援巨型訊框。更新連線會干擾所有連線相關聯的虛擬介面的網路連線能力達 30 秒。若要檢查連線或虛

擬介面是否支援巨型訊框，請在 AWS Direct Connect 主控台中選取它，然後在摘要索引標籤上尋找巨型訊框功能。

當您建立公有虛擬介面時， 最多可能需要 72 小時 AWS 才能檢閱和核准您的請求。

佈建公有虛擬介面連往非 VPC 服務

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2. 在導覽窗格中，選擇 Virtual Interfaces (虛擬介面)。
3. 選擇建立虛擬介面。
4. 在虛擬介面類型之下，針對類型選擇公有。
5. 在公有虛擬介面設定 之下，執行下列動作：

   a. 針對虛擬介面名稱，輸入虛擬介面的名稱。

   b. 針對連線，選擇要用於此介面的 Direct Connect 連線。

   c. 針對 VLAN，為您的虛擬區域網路 (VLAN) 輸入 ID 號碼。

   d. 針對 BGP ASN，為新的虛擬介面輸入您內部部署對等路由器的邊界閘道協定自治系統編號。

      有效值為 1-2147483647。
6. 在 Additional settings (其他設定) 之下，執行下列動作：

   a. 若要設定 IPv4 BGP 或 IPv6 對等，請執行下列動作：

      [IPv4] 若要設定 IPv4 BGP 對等，請選擇 IPv4，然後執行以下動作：

      - 若要自行指定這些 IP 地址，對於 Your router peer ip (您的路由器對等 IP)，輸入 Amazon 應傳送流量至該處的目的地 IPv4 CIDR 地址。
      - 對於 Amazon router peer IP (Amazon 路由器對等 IP)，輸入用以傳送流量至 AWS的 IPv4 CIDR 地址。

      [IPv6] 若要設定 IPv6 BGP 對等，請選擇 IPv6。對等 IPv6 地址是自動從 Amazon 的 IPv6 地址集區所指派。您無法指定自訂 IPv6 地址。

   b. 若要提供自己的 BGP 金鑰，請輸入您的 BGP MD5 金鑰。

      如果您未輸入值，我們會產生 BGP 金鑰。

   c. 若要對 Amazon 公告字首，對於欲公告的字首，輸入應透過虛擬介面將流量路由傳送至該處的目的地 IPv4 CIDR 地址 (以逗號分隔)。

d. (選用) 新增或移除標籤。

[新增標籤] 選擇 Add tag (新增標籤)，並執行下列動作：

- 對於 Key (金鑰)，輸入金鑰名稱。
- 在值中，進入索引鍵值。

[移除標籤] 在標籤旁邊，選擇 移除標籤。

7. 選擇建立虛擬介面。

佈建私有虛擬介面連往 VPC

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2. 在導覽窗格中，選擇 Virtual Interfaces (虛擬介面)。
3. 選擇建立虛擬介面。
4. 在虛擬介面類型之下，對於類型，請選擇私有。
5. 在公有虛擬介面設定之下，執行下列動作：

a. 針對虛擬介面名稱，輸入虛擬介面的名稱。

b. 針對連線，選擇要用於此介面的 Direct Connect 連線。

c. 對於閘道類型，選擇「虛擬私有閘道」或「Direct Connect 閘道」。

d. 針對虛擬介面擁有者，選擇另一個 AWS 帳戶，然後輸入 AWS 帳戶。

e. 對於虛擬私有閘道，請選擇您用於此介面的虛擬私有閘道。

f. 針對 VLAN，為您的虛擬區域網路 (VLAN) 輸入 ID 號碼。

g. 針對 BGP ASN，為新的虛擬介面輸入您內部部署對等路由器的邊界閘道協定自治系統編號。

有效值為 1 至 2147483647。

6. 在 Additional settings (其他設定) 之下，執行下列動作：

a. 若要設定 IPv4 BGP 或 IPv6 對等，請執行下列動作：

[IPv4] 若要設定 IPv4 BGP 對等，請選擇 IPv4，然後執行以下動作：

- 若要自行指定這些 IP 地址，對於 Your router peer ip (您的路由器對等 IP)，輸入 Amazon 應傳送流量至該處的目的地 IPv4 CIDR 地址。
- 對於 Amazon 路由器對等 IP，輸入用以傳送流量至 AWS的 IPv4 CIDR 地址。

> **Important**
>
> 設定 AWS Direct Connect 虛擬介面時，您可以使用 RFC 1918 指定自己的 IP 地址、使用其他定址機制，或選擇從 RFC 3927 169.25IPv4.0.0/16 IPv4 Link-Local 範圍配置的 AWS 指派 IPv4/29 CIDR 地址point-to-point連線。這些point-to-point連線應僅用於客戶閘道路由器和 Direct Connect 端點之間的 eBGP 互連。針對 VPC 流量或通道用途，例如 AWS Site-to-Site私有 IP VPN 或 Transit Gateway Connect， AWS 建議使用客戶閘道路由器上的迴路或 LAN 介面做為來源或目的地地址，而非point-to-point連線。
>
> - 如需有關 RFC 1918 的詳細資訊，請參閱私有網路的地址配置。
> - 如需有關 RFC 3927 的詳細資訊，請參閱 IPv4 Link-Local 地址的動態組態。

[IPv6] 若要設定 IPv6 BGP 對等，請選擇 IPv6。對等 IPv6 地址是自動從 Amazon 的 IPv6 地址集區所指派。您無法指定自訂 IPv6 地址。

b. 若要將最大傳輸單位 (MTU) 從 1500 (預設) 變更至 9001 (巨型框架)，請選取巨型 MTU (MTU 大小 9001)。

c. (選用) 在啟用 SiteLink 之下，選擇啟用以啟用 Direct Connect 連接點之間的直接連線。

d. (選用) 新增或移除標籤。

[新增標籤] 選擇 Add tag (新增標籤)，並執行下列動作：

- 對於 Key (金鑰)，輸入金鑰名稱。
- 在值中，進入索引鍵值。

[移除標籤] 在標籤旁邊，選擇 移除標籤。

7. 選擇建立虛擬介面。
8. 您必須使用 BGP 裝置公告您用於公有 VIF 連線的網路。

步驟 5：下載路由器組態

建立 AWS Direct Connect 連線的虛擬介面之後，您可以下載路由器組態檔案。該檔案包含將您的路由器設定成搭配私有或公有虛擬介面使用所需的命令。

若要下載路由器組態

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2. 在導覽窗格中，選擇 Virtual Interfaces (虛擬介面)。
3. 選取連線，然後選擇 View Details (檢視詳細資訊)。
4. 選擇 Download router configuration (下載路由器組態)。
5. 對於 Download Router Configuration (下載路由器組態)，請執行以下動作：
   a. 針對 Vendor (廠商)，選取路由器的製造商。
   b. 針對 Platform (平台)，選取路由器的型號。
   c. 針對 Software (軟體)，選取路由器的軟體版本。
6. 選擇 Download (下載)，接著使用路由器的適當組態來確保您可以連接至 AWS Direct Connect。

如需手動設定路由器的詳細資訊，請參閱下載路由組態檔案。

您的路由器設定妥之後，虛擬介面的狀態會變成 UP。如果虛擬介面保持關閉，且您無法 ping AWS Direct Connect 裝置的對等 IP 地址，請參閱 診斷排解第 2 層 (資料鏈路) 問題。若您能夠 ping 到對等 IP 地址，請參閱診斷排解第 3/4 層 (網路/傳輸) 問題。若 BGP 對等工作階段已建立但流量無法路由，請參閱疑難排解路由問題。

步驟 6：驗證您的虛擬介面

建立 AWS 雲端或 Amazon VPC 的虛擬介面之後，您可以使用下列程序驗證您的 AWS Direct Connect 連線。

驗證與 AWS 雲端的虛擬介面連線

- 執行`traceroute`並確認 AWS Direct Connect 識別符位於網路追蹤中。

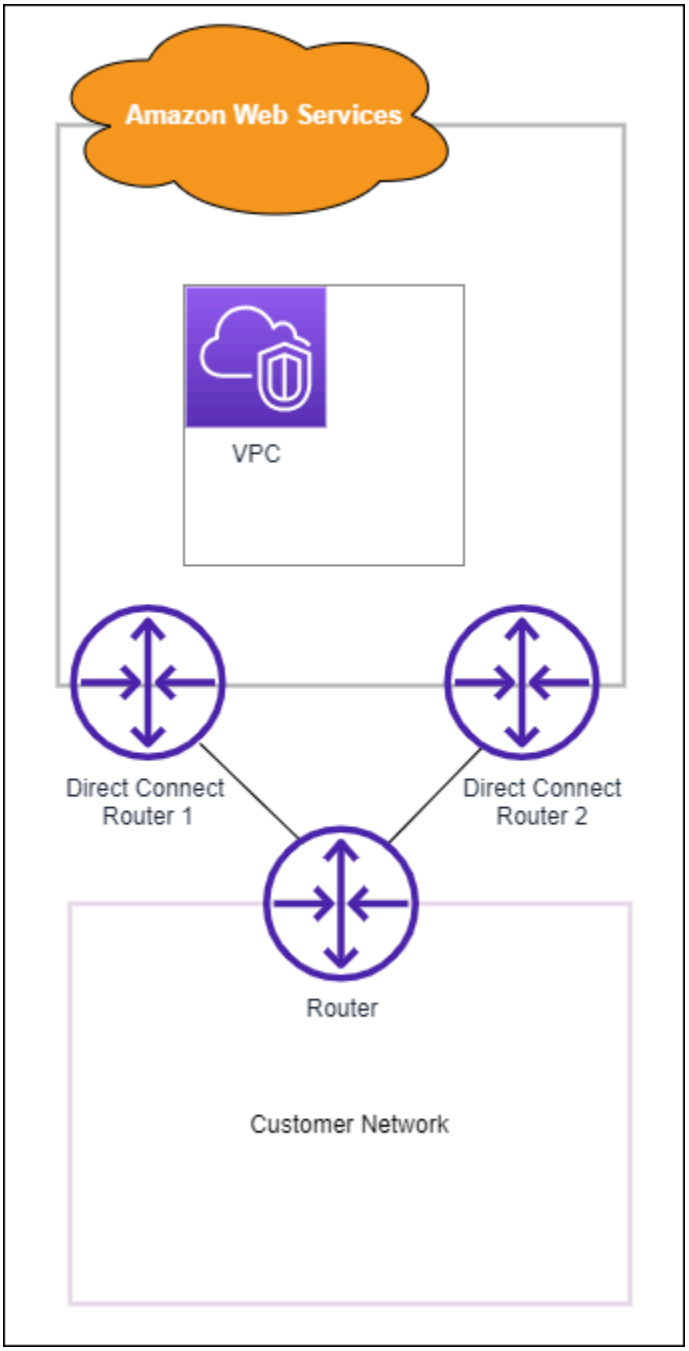
驗證與 Amazon VPC 的虛擬 int+erface 連線

1. 使用可透過 ping 存取的 AMI 如 Amazon Linux AMI，在連接至虛擬私有閘道的 VPC 中啟動 EC2 執行個體。當您使用 Amazon EC2 主控台的執行個體啟動精靈時，可在快速入門索引標籤取得 Amazon Linux AMI。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的啟動執行個體。Amazon EC2 確認與執行個體關聯的安全群組，包含一個規則允許流量傳入 ICMP (適用於 ping 請求)。

2. 待執行個體執行之後，取得其私有 IPv4 地址 (例如 10.0.0.4)。Amazon EC2 主控台顯示的執行個體詳細資訊將包含該地址。
3. Ping 到該私有 IPv4 地址並獲得回應。

(建議) 步驟 7：設定備援連線

若要提供容錯移轉，建議您請求並設定兩個專用連線 AWS，如下圖所示。這些連線的終端處可能是您網路上的一部或兩部路由器。



佈建兩個專屬連線的情況下，有不同的組態可供選擇：

- 主動/主動 (BGP 多重路徑)。這是預設組態，其中兩個連線都處於作用中狀態。 AWS Direct Connect 支援對相同位置內的多個虛擬介面進行多路徑，並根據流程在介面之間負載共用流量。若其中一個連線無法使用，所有流量都將轉往另一連線。
- 主動/被動 (容錯移轉)。由其中一個連線處理流量，另一連線處於待命狀態。若主動連線無法使用，所有流量都將轉往被動連線。您需要就其中一條鏈路在路由前面加上 AS 路徑，使其成為被動鏈路。

您的連線採用哪種組態並不會影響備援，但將影響兩個連線間決定資料路由方式的政策。建議您將兩個連線都設定成主動連線。

如果您是使用 VPN 連接提供備援，請確定您已實施運作狀態檢查和容錯移轉機制。如果使用下列任一組態，則需檢查您的路由表路由，以路由至新的網路介面。

- 您可以將自己的執行個體用於路由，例如執行個體是防火牆。
- 您可以使用自己用於終止 VPN 連線的執行個體。

為了實現高可用性，強烈建議您設定不同 AWS Direct Connect 位置的連線。

如需 AWS Direct Connect 彈性的詳細資訊，請參閱AWS Direct Connect 彈性建議。

AWS Direct Connect 容錯移轉測試

AWS Direct Connect 彈性工具組彈性模型旨在確保您在多個位置擁有適當數量的虛擬介面連線。完成精靈後，請使用 AWS Direct Connect 彈性工具組容錯移轉測試來關閉 BGP 對等互連工作階段，以確認流量路由至其中一個備援虛擬介面，並滿足您的彈性需求。

使用此測試，可確保當虛擬介面中斷服務時，流量會透過備援虛擬介面路由傳送。您可以透過選取虛擬界面、BGP 對等工作階段，以及執行 test 的時間長度來開始測試。 會將選取的虛擬界面 BGP 對等工作階段 AWS 置於關閉狀態。當介面處於此狀態時，流量應該會經過備援虛擬介面。如果您的組態未包含適當的備援連線，則 BGP 對等互連工作階段會失敗，且流量不會獲得路由傳送。當測試完成或您手動停止測試時， 會 AWS 還原 BGP 工作階段。測試完成後，您可以使用 AWS Direct Connect 彈性工具組來調整您的組態。

> **Note**
>
> 請勿在 Direct Connect 維護期間使用此功能，因為 BGP 工作階段可能會在維護期間或之後提早還原。

測試歷史記錄

AWS 會在 365 天後刪除測試歷史記錄。測試歷程記錄包含所有 BGP 對等節點上所執行測試的狀態。歷程記錄包括測試哪些 BGP 對等互連工作階段、開始和結束時間，以及測試狀態 (可以是下列任一值) :

- 進行中 - 測試目前正在執行中。
- 已完成 - 測試已在您指定的時間內進行。
- 已取消 - 測試已在指定時間前取消。
- 失敗 - 測試未在您指定的時間內執行。當路由器發生問題時，可能會發生這種情況。

如需詳細資訊，請參閱the section called “檢視虛擬介面容錯移轉測試歷史記錄”。

驗證許可

擁有虛擬介面的帳戶，即擁有執行容錯移轉測試許可的唯一帳戶。帳戶擁有者透過 收到指示 AWS CloudTrail ，指出測試在虛擬介面上執行。

主題

- 啟動 AWS Direct Connect 彈性工具組虛擬介面容錯移轉測試
- 檢視 AWS Direct Connect 彈性工具組虛擬介面容錯移轉測試歷史記錄
- 停止 AWS Direct Connect 彈性工具組虛擬界面容錯移轉測試

啟動 AWS Direct Connect 彈性工具組虛擬介面容錯移轉測試

您可以使用 AWS Direct Connect 主控台或 啟動虛擬介面容錯移轉測試 AWS CLI。

從 AWS Direct Connect 主控台啟動虛擬介面容錯移轉測試

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。

2. 選擇 Virtual interfaces (虛擬界面)。
3. 選取虛擬介面，然後選擇動作、帶入 BGP。

   您可以在公有、私有或傳輸虛擬介面上執行測試。
4. 在 Start failure test (啟動失敗測試) 對話方塊中，執行下列動作：

   a. 使用要帶入測試的「對等互連」時，請選擇要測試的對等互連工作階段，例如 IPv4。

   b. 使用 Test maximum time (測試時間上限) 時，輸入測試將持續的分鐘數。

      最大值為 4,320 分鐘 (72 小時)。

      預設值為 180 分鐘 (3 小時)。

   c. 使用 To confirm test (確認測試) 時，輸入 Confirm (確認)。

   d. 選擇確認。

   BGP 對等互連工作階段會處於「向下」狀態。您可以傳送流量來驗證沒有中斷。如有需要，您可以立即停止測試。

使用 啟動虛擬介面容錯移轉測試 AWS CLI

使用 StartBgpFailoverTest。

檢視 AWS Direct Connect 彈性工具組虛擬介面容錯移轉測試歷史記錄

您可以使用 AWS Direct Connect 主控台或 檢視虛擬介面容錯移轉測試歷史記錄 AWS CLI。

從 AWS Direct Connect 主控台檢視虛擬介面容錯移轉測試歷程記錄時

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2. 選擇 Virtual interfaces (虛擬界面)。
3. 選取虛擬介面，然後選擇檢視詳細資訊。
4. 選擇 Test history (測試歷程記錄)。

   主控台會顯示您先前對虛擬介面執行的虛擬介面測試。
5. 若要檢視特定測試的詳細資訊，請選取該測試 ID。

使用 檢視虛擬介面容錯移轉測試歷史記錄 AWS CLI

使用 ListVirtualInterfaceTestHistory。

停止 AWS Direct Connect 彈性工具組虛擬界面容錯移轉測試

您可以使用 AWS Direct Connect 主控台或 停止虛擬介面容錯移轉測試 AWS CLI。

從 AWS Direct Connect 主控台停止虛擬介面容錯移轉測試

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2. 選擇 Virtual interfaces (虛擬界面)。
3. 選取虛擬介面，然後選擇動作、取消測試。
4. 選擇確認。

AWS 會還原 BGP 對等互連工作階段。測試歷程記錄會顯示測試為「已取消」。

使用 停止虛擬介面容錯移轉測試 AWS CLI

使用 StopBgpFailoverTest。

AWS Direct Connect 維護

AWS Direct Connect 致力於確保服務的安全性、可用性和可擴展性。為了維護這些標準，硬體網路裝置需要定期維護。Direct Connect 維護分為兩種類型：規劃和緊急。

這些維護事件包括解決安全漏洞、硬體問題、執行裝置遷移以符合標準、修正瑕疵，以及提供新功能。透過遵循中所述的實務維護事件準備，您可以更好地準備 Direct Connect 環境，以避免在維護事件期間中斷。如果您有非彈性的網路設定或單一連線，則內部部署網路 AWS 和資源之間的連線會中斷。

Direct Connect 會將有關計劃和緊急維護事件的電子郵件通知傳送到與擁有 Direct Connect 連線或虛擬介面資源 AWS 的帳戶相關聯的電子郵件地址。如果您將 Direct Connect 託管連線與其中一個 Direct Connect 交付合作夥伴搭配使用，系統會向您和合作夥伴帳戶傳送有關維護事件的電子郵件通知。您也可以新增其他電子郵件地址或分發清單來接收通知。如需詳細資訊，請參閱更新 AWS 帳戶的替代聯絡人。

維護事件

- Direct Connect 計劃維護
- Direct Connect 緊急維護
- 第三方維護
- 維護事件準備
- 維護事件延遲或取消的請求

Direct Connect 計劃維護

計劃的維護事件涉及網路升級，例如硬體裝置端點上的作業系統修補和組態更新，這些端點是改善可用性和提供新功能所需的。

這些維護事件會提前 14 天排程，通常在裝置端點所在 Direct Connect 位置的低流量時段內四小時發生。維護活動通常在完整的四小時時段到期之前完成，一旦工作完成，您將會收到通知。在極少數情況下，如果無法預期的情況需要延長維護時段，我們會傳送單獨的通知，其中包含修訂後的完成預估。

使用以下排程，初始通知和提醒通知會傳送至擁有資源 AWS 的帳戶：

- 規劃維護事件前 14 個日曆天，
- 規劃維護事件前 7 個日曆天，以及
- 規劃維護事件前 1 天。

> **Note**
>
> 日曆日包括非工作日和當地假日。

此外，

- 與 整合，在您的監控或票證系統中接收通知 AWS Health。若要整合 AWS Health，請參閱AWS Health 《 使用者指南》中的 AWS Health 使用 Amazon EventBridge 監控 中的事件。
- 在 上檢視計劃的維護排程AWS Health Dashboard。

在極少數情況下，計劃的維護事件無法如期發生。如果發生這種情況，我們會傳送取消通知，並遵循上述相同的程序，在未來重新排程事件。

Direct Connect 緊急維護

緊急維護事件會以關鍵為基礎啟動，以防止即將發生的服務影響事件或解決已導致連線中斷的損害。在這種情況下，必須立即採取動作，將受影響的端點還原至運作狀態良好。

雖然我們努力盡可能提供預先通知，但某些情況可能需要立即開始維護。緊急維護排定或進行中時，您會收到通知，並在完成時再次收到通知。

這些事件通常發生在裝置端點所在的 Direct Connect 位置的兩小時時段。維護活動通常會在此時段內完成。如果無法預期的情況需要延長維護時段，例如硬體替換，我們將傳送單獨的通知，其中包含修訂後的完成估計。

第三方維護

除了 AWS 啟動的維護事件之外，提供從現場部署到 Direct Connect 位置網路連線的 Direct Connect 交付合作夥伴或網路服務供應商可能會執行維護活動。Direct Connect Delivery 合作夥伴會收到來自的維護事件通知， AWS 以便他們可以規劃自己的維護排程以避免重疊。 AWS 無法查看合作夥伴的維護活動，因此您需要與他們確認其排程程序、通知方法和最佳實務。

維護事件準備

為了確保生產工作負載在維護事件期間持續運作，Direct Connect 建議您使用 AWS Direct Connect 彈性工具組來設定網路連線以實現最大的彈性。如需最大彈性的範例模型，請參閱 最大彈性。

使用最大彈性，連線會分散到至少兩個 Direct Connect 位置，並在每個 Direct Connect 位置中的兩個唯一裝置端點上終止。這提供多層備援，可降低單一端點故障的風險，並有助於在維護事件期間維持連線。Direct Connect 永遠不會排程規劃的維護事件，該事件會同時關閉備援連線。如需使用 AWS Direct Connect 彈性工具組設定最大彈性的步驟，請參閱 設定最大彈性。

在計劃的維護事件期間，Direct Connect 會耗盡往返進行維護之連線端點的流量，並強制流量使用您的備援連線。如果未設定最大彈性，這允許更無縫的網路流量重新路由，而不需要手動介入。或者，您可以選擇使用本機偏好設定邊界閘道協定 (BGP) 社群，在維護時段期間控制備援連線之間的流量重新路由。如需 BGP 社群的詳細資訊，請參閱 路由政策和 BGP 社群。

使用最大彈性模型設定 Direct Connect 環境，有助於確保您的業務在維護事件和基礎設施故障期間不會受到影響。當正確實作和測試時，您通常不需要對這些維護事件採取任何動作。

彈性驗證

如果您已將 Direct Connect 環境設定為具有彈性，請定期驗證當連線out-of-service時，您的流量是否透過其他備援連線路由。定期主動測試有助於在實際維護事件或故障案例影響生產工作負載之前識別和解決任何潛在問題。這將確保在維護事件期間對網路的可靠性更具可信度。使用 Direct Connect 容錯移轉測試來驗證備援連線的彈性。如需使用 AWS Direct Connect 容錯移轉測試的步驟，請參閱 Direct Connect 容錯移轉測試。

您也可以利用 Amazon CloudWatch Network Monitor 來主動監控 Direct Connect 連線。如需詳細資訊，請參閱使用 Amazon CloudWatch Network Synthetic Monitor 監控混合連線。

維護事件延遲或取消的請求

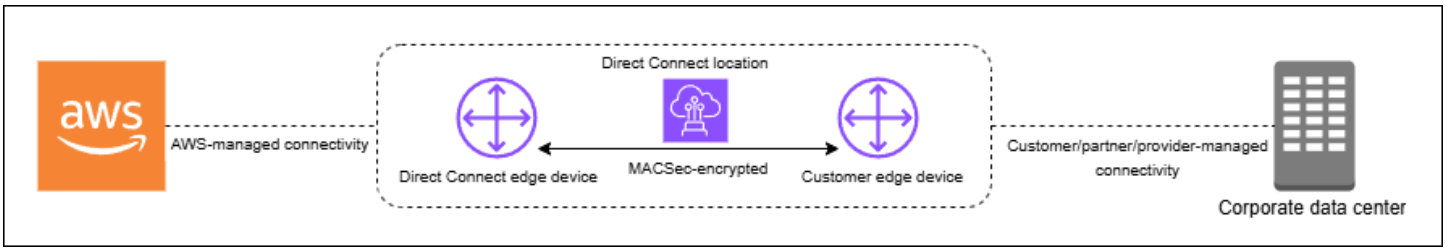
Direct Connect 裝置會跨多個客戶共用。因此，我們不支援維護重新排程或取消的特定請求。為某個客戶重新排程或取消請求可能會對使用該端點的其他客戶產生負面影響。這也可能會造成及時緩解可用性或安全問題的風險。

中的 MAC 安全性 AWS Direct Connect

MAC Security (MACsec) 是 IEEE 標準，提供資料機密性、資料完整性和資料來源真實性。MACsec 透過交叉連線提供第 2 層point-to-point加密 AWS，可在兩個第 3 層路由器之間運作。雖然 MACsec 會保護路由器與第 2 層 Direct Connect 位置之間的連線，但當實體層在 AWS Direct Connect 位置與 AWS 區域之間透過網路流動時， 會透過加密實體層上的所有資料 AWS 來提供額外的安全性。這會建立分層安全方法，在初始進入網路期間 AWS 以及在跨 AWS 網路傳輸期間保護您的流量。

在下圖中， AWS Direct Connect 交叉連接必須連接到客戶邊緣裝置上具備 MACsec 功能的介面。透過 Direct Connect 的 MACsec 為 Direct Connect 邊緣裝置與客戶邊緣裝置之間的point-to-point流量提供第 2 層加密。在交叉連線兩端的介面之間交換和驗證安全金鑰之後，就會發生此加密。

> **Note**
>
> MACsec 在乙太網路連結上提供point-to-point安全性；因此，它不會跨多個循序乙太網路或其他網路區段提供end-to-end加密。



MACsec 概念

以下是 MACsec 的重要概念：

- MAC Security (MACsec) — 是 IEEE 802.1 Layer 2 標準，提供資料機密性、資料完整性和資料來源真實性。如需有關通訊協定的詳細資訊，請參閱 802.1AE: MAC Security (MACsec)。
- 安全關聯金鑰 (SAK) — 工作階段金鑰，可在客戶內部部署路由器與 Direct Connect 位置的連接埠之間建立 MACsec 連線。SAK 不是預先共用的，而是透過密碼編譯金鑰產生程序自動衍生自 CKN/CAK 對。在您提供和佈建 CKN/CAK 對之後，此衍生會在連線的兩端發生。基於安全考量，每當建立 MACsec 工作階段時，SAK 都會定期重新產生。
- 連線關聯金鑰名稱 (CKN) 和連線關聯金鑰 (CAK) — 此對中的值用於產生 MACsec 金鑰。您可以產生配對值，將它們與 AWS Direct Connect 連線建立關聯，然後在 AWS Direct Connect 連線結束時

將其佈建在邊緣裝置上。Direct Connect 僅支援靜態 CAK 模式，但不支援動態 CAK 模式。由於僅支援靜態 CAK 模式，建議您遵循自己的金鑰管理政策來產生、分佈和輪換金鑰。

- 金鑰格式 — 金鑰格式應使用十六進位字元，長度剛好為 64 個字元。Direct Connect 僅支援專用連線的進階加密標準 (AES) 256 位元金鑰，對應至 64 個字元的十六進位字串。
- 加密模式 — Direct Connect 支援兩種 MACsec 加密模式：
  - must_encrypt — 在此模式中，連線需要所有流量的 MACsec 加密。如果 MACsec 交涉失敗或無法建立加密，連線將不會傳輸任何流量。此模式提供最高的安全性保證，但如果有任何 MACsec 相關問題，可能會影響可用性。
  - should_encrypt — 在此模式中，連線會嘗試建立 MACsec 加密，但如果 MACsec 交涉失敗，則會回復為未加密的通訊。此模式提供更大的彈性和更高的可用性，但在某些情況下，可能會允許未加密的流量。

  加密模式可以在連線組態期間設定，之後可以修改。根據預設，啟用 MACsec 的新連線會設定為「should_encrypt」模式，以防止在初始設定期間發生潛在的連線問題。

MACsec 金鑰輪換

- CNN/CAK 輪換（手動）

  Direct Connect MACsec 支援容量高達三個 CKN/CAK 對的 MACsec 金鑰鏈。這可讓您手動輪換這些長期金鑰，而不會中斷連線。當您使用 `associate-mac-sec-key`命令關聯新的 CKN/CAK 配對時，您必須在裝置上設定相同的配對。Direct Connect 裝置會嘗試使用最近新增的金鑰。如果該金鑰與您裝置的金鑰不相符，則會回復到先前的工作金鑰，以確保輪換期間的連線穩定性。

  如需使用 的資訊`associate-mac-sec-key`，請參閱 associate-mac-sec-key。
- 安全關聯金鑰 (SAK) 輪換（自動）

  SAK 衍生自作用中 CKN/CAK 對，會根據下列項目進行自動輪換：
  - 時間間隔
  - 加密流量的磁碟區
  - MACsec 工作階段建立

  此輪換由通訊協定自動處理，以透明方式進行，不會中斷連線，而且不需要手動介入。SAK 永遠不會持續儲存，並透過遵循 IEEE 802.1X 標準的安全金鑰衍生程序進行重新產生。

支援的連線

MACsec 可在專用 Direct Connect 連線和連結彙總群組上使用：

支援的 MACsec 連線

- 專用連線
- LAG

> **Note**
>
> 託管連線和 Direct Connect Gateway 關聯不支援 MACsec 加密。

如需如何排序支援 MACsec 的連線之詳細資訊，請參閱 AWS Direct Connect。

專用連線

以下可協助您熟悉 AWS Direct Connect 專用連線上的 MACsec。使用 MACsec 無需額外費用。您可以在 中找到在專用連線上設定 MACsec 的步驟在專用連線上開始使用 MACsec 。

專用連線的 MACsec 先決條件

請注意專用連線上 MACsec 的下列需求：

- 在所選存在點的 10 Gbps、100 Gbps 和 400 Gbps 專用 Direct Connect 連線上支援 MACsec。對於這些連線，支援下列 MACsec 密碼套件：
  - 對於 10Gbps 連線，GCM-AES-256 和 GCM-AES-XPN-256。
  - 對於 100 Gbps 和 400 Gbps 連線，GCM-AES-XPN-256。
- 僅支援 256 位元 MACsec 金鑰。
- 100Gbps 和 400 Gbps 連線需要擴充封包編號 (XPN)。對於 10Gbps 連線，Direct Connect 同時支援 GCM-AES-256 和 GCM-AES-XPN-256。100 Gbps 和 400 Gbps 專用連線等高速連線可以快速耗盡 MACsec 的原始 32 位元封包編號空間，這需要您每隔幾分鐘輪換加密金鑰以建立新的連線關聯。為了避免這種情況，IEEE Std 802.1AEbw-2013 修訂引入了延伸封包編號，將編號空間增加到 64 位元，減輕了金鑰輪換的及時性要求。
- 安全頻道識別符 (SCI) 是必要項目，且必須開啟。此設定無法調整。

- IEEE 802.1Q (Dot1q/VLAN) 標籤位移/dot1q-in-clear 不支援將 VLAN 標籤移出加密的承載。

此外，在專用連線上設定 MACsec 之前，您應該完成下列任務。

- 為 MACsec 金鑰建立 CKN/CAK 對。

  您可以使用開放的標準工具建立配對。配對必須符合 the section called “設定您的內部部署路由器” 中指定的要求。
- 確認您連線端的裝置支援 MACsec。
- 必須開啟安全頻道識別符 (SCI)。
- 僅支援 256 位元 MACsec 金鑰，可提供最新的進階資料保護。

LAG

下列需求可協助您熟悉適用於 Direct Connect 連結彙總群組 (LAGs MACsec：

- LAGs 必須由具備 MACsec 功能的專用連線組成，支援 MACsec 加密
- LAG 中的所有連線都必須具有相同的頻寬，並支援 MACsec
- MACsec 組態會統一套用到 LAG 中的所有連線
- LAG 建立和 MACsec 啟用可以同時完成

服務連結角色

AWS Direct Connect use AWS Identity and Access Management (IAM) 服務連結角色。服務連結角色是直接連結至 的唯一 IAM 角色類型 AWS Direct Connect。服務連結角色由 預先定義， AWS Direct Connect 並包含該服務代表您呼叫其他 AWS 服務所需的所有許可。服務連結角色可讓您更 AWS Direct Connect 輕鬆地設定，因為您不必手動新增必要的許可。 AWS Direct Connect 會定義其服務連結角色的許可，除非另有定義，否則只能 AWS Direct Connect 擔任其角色。定義的許可包括信任政策和許可政策，且該許可政策無法附加至其他 IAM 實體。如需詳細資訊，請參閱the section called “服務連結角色”。

MACsec 預先共用 CKN/CAK 金鑰考量

AWS Direct Connect 會將 AWS 受管 CMKs 用於您與連線或 LAGs 建立關聯的預先共用金鑰。Secrets Manager 將您預先共用的 CKN 和 CAK 對儲存為密碼，Secrets Manager 的根金鑰會對該密碼加密。如需詳細資訊，請參閱《AWS Key Management Service 開發人員指南》中的 AWS 受管 CMK。

儲存的金鑰依設計為唯讀，但您可以使用 AWS Secrets Manager 主控台或 API 來排程 7 到 30 天的刪除。排程刪除作業時無法讀取 CKN，這可能會影響您的網路連線。發生這種情況時，我們將採用以下規則：

- 如果連線處於擱置狀態，我們會取消 CKN 與連線的關聯。
- 如果連線處於可用狀態，我們會透過電子郵件通知連線擁有者。如果您在 30 天內未採取任何行動，我們會取消 CKN 與您連線的關聯。

當我們取消最後一個 CKN 與您連線的關聯，並且將連線加密模式設為「必須加密」時，我們會將模式設置為「should_encrypt」以防止突然遺失封包。

在專用 AWS Direct Connect 連線上使用 MACsec 的入門

下列任務可讓您開始設定要在 Direct Connect 專用連線上使用的 MACsec

步驟 1：建立連線

若要開始使用 MACsec，您必須在建立專用連線時開啟此功能。

(選用) 步驟 2：建立鏈路彙整群組 (LAG)

如果您使用多個連線進行備援，您可以建立支援 MACsec 的 LAG。如需詳細資訊，請參閱 MACsec 考量和建立 LAG。

步驟 3：將 CKN/CAK 與連線或 LAG 產生關聯

建立支援 MACsec 的連線或 LAG 之後，您需要將 CKN/CAK 與連線產生關聯。如需詳細資訊，請參閱下列其中一個項目：

- 將 MACsec CKN/CAK 與連線建立關聯
- 將 MACsec CKN/CAK 與 LAG 產生關聯

步驟 4：設定內部部署路由器

使用 MACsec 私密金鑰來更新您的內部部署路由器。內部部署路由器和 AWS Direct Connect 位置上的 MACsec 私密金鑰必須相符。如需詳細資訊，請參閱下載路由組態檔案。

步驟 5：(選用) 移除 CKN/CAK 與連線或 LAG 之間的關聯

您可以選擇性地移除 CKN/CAK 與連線或 LAG 之間的關聯。如果您需要移除關聯，請參閱下列其中一項：

- 移除 MACsec 私密金鑰和連線之間的關聯
- 移除 MACsec 私密金鑰和 LAG 之間的關聯

AWS Direct Connect 專用和託管連線

AWS Direct Connect 可讓您在網路與其中一個 AWS Direct Connect 位置之間建立專用網路連線。

有兩種類型的連線：

- 專用連線：與單一客戶相關聯的實體乙太網路連線。客戶可以透過 AWS Direct Connect 主控台、CLI 或 API 請求專用連線。如需詳細資訊，請參閱專用連線。
- 託管連線： AWS Direct Connect 合作夥伴代表客戶佈建的實體乙太網路連線。客戶可在 AWS Direct Connect 合作夥伴計畫中聯絡合作夥伴 (佈建連線的合作夥伴) 來要求託管連線。如需詳細資訊，請參閱託管連線。

主題

- 專用 AWS Direct Connect 連線
- 託管 AWS Direct Connect 連線
- 刪除 AWS Direct Connect 連線
- 更新 AWS Direct Connect 連線
- 檢視 AWS Direct Connect 連線詳細資訊

專用 AWS Direct Connect 連線

建立 AWS Direct Connect 專用連線時需要以下資訊：

AWS Direct Connect 位置

與 合作夥伴計劃中的 AWS Direct Connect 合作夥伴合作，協助您在 AWS Direct Connect 位置與資料中心、辦公室或主機代管環境之間建立網路電路。他們也能夠在和該據點相同設施內提供主機代管空間。如需詳細資訊，請參閱 APN 合作夥伴支援 AWS Direct Connect。

連接埠速度

可能的值為 1 Gbps、10 Gbps、100 Gbps 和 400 Gbps。

在您建立連線要求之後，就無法變更連接埠速度。若要變更連接埠速度，您必須建立並設定新的連線。

您可以使用連線精靈建立連線，或建立傳統連線。如果您使用連線精靈，則可以使用備援建議來設定連線。如果您是第一次設定連線，建議使用精靈。如果您願意，您可以使用 Classic one-at-a-time建立連

線。如果您已經有要新增連線的現有設定，建議使用傳統方式。您可以建立獨立的連線，或者建立連線與您帳戶中的 LAG 產生關聯。如果您將連線與 LAG 產生關聯，便會使用如同 LAG 所指定的連接埠速度和據點建立該連線。

在您請求連線後，我們會提供授權書和連線設施指派 (LOA-CFA)，供您下載或傳送電子郵件給您以取得詳細資訊。若您收到要求補齊更多資訊的郵件，即必須在 7 日內回覆，否則將刪除該連線。LOA-CFA 是連線的授權 AWS，您的網路提供者需要此授權才能為您訂購交叉連線。如果您在該 AWS Direct Connect 位置沒有設備，則無法自行訂購交叉連線。

下列作業適用於專用連線：

- 使用連線精靈建立連線
- 建立傳統連線
- the section called “檢視連線詳細資訊”
- the section called “更新連線”
- 將 MACsec CKN/CAK 與連線建立關聯
- the section called “移除 MACsec 私密金鑰和連線之間的關聯”
- the section called “刪除一個連線”

您可以新增鏈路彙整群組 (LAG) 的專用連線，讓您將多個連線視為單一連線。如需相關資訊，請參閱將連線與 LAG 產生關聯。。

建立連線之後，您要建立虛擬介面以連接至公有和私有 AWS 資源。如需詳細資訊，請參閱虛擬介面和託管虛擬介面。

如果您在某個 AWS Direct Connect 位置沒有設備，請先聯絡 AWS Direct Connect 合作夥伴計劃中的 AWS Direct Connect 合作夥伴。如需詳細資訊，請參閱 APN 合作夥伴支援 AWS Direct Connect。

如果您要建立使用 MAC Security (MACsec) 的連線，請在建立連線之前檢閱先決條件。如需詳細資訊，請參閱the section called “專用連線的 MACsec 先決條件”。

授權書和連線設施指派 (LOA-CFA)

我們處理您的連線請求後，您便可以下載 LOA-CFA。如果該連結為未啟用狀態，即表示尚未提供 LOA-CFA 讓您下載。請檢查您是否收到要求補齊資訊的電子郵件。

下載的 LoA 經過數位簽章和浮水印，以驗證 發行之 LoA 的真實性 AWS。LoA 中的數位簽章和浮水印。PDF 文件可防止 Direct Connect 站點的設施供應商對修改過的或潛在的欺詐性 LoA 採取行動。開啟 PDF 並檢閱簽章面板，即可驗證數位簽章。有效的文件將顯示「簽章有效」和「自簽章套用後文件

尚未修改」。浮水印會重複在 LoA 內文中指派的修補程式面板和絞線，做為視覺效果，但非安全真偽指標。

在連接埠處於作用中或 LOA 發出 90 天後 (以先發生者為準) 會自動開始計費。您可以在啟用前刪除連接埠，或在 LOA 發出後 90 天內刪除連接埠，以避免產生費用。

如果您的連線在 90 天後仍未啟用，且 LOA-CFA 尚未發出，我們將向您發送一封電子郵件，提醒您該連接埠將在 10 天內刪除。如果您在額外的 10 天內無法啟用連接埠，連接埠將會自動刪除，而您必須重新啟動連接埠建立程序。

如需下載 LoA-CFA 的步驟，請參閱 下載 LOA-CFA。

> **Note**
>
> 如需定價的詳細資訊，請參閱AWS Direct Connect 定價。LOA-CFA 重新核發之後若您不再需要該連線，則必須自行刪除連線。如需詳細資訊，請參閱刪除 AWS Direct Connect 連線。

主題

- 使用連線精靈建立 AWS Direct Connect 專用連線
- 建立 AWS Direct Connect Classic 連線
- 下載 AWS Direct Connect LOA-CFA
- 將 MACsec CKN/CAK 與 AWS Direct Connect 連線建立關聯
- 移除 MACsec 私密金鑰與 AWS Direct Connect 連線之間的關聯

使用連線精靈建立 AWS Direct Connect 專用連線

本節會說明使用連線精靈建立連線。如果您想要建立傳統連線，請參閱 the section called “步驟 2：請求 AWS Direct Connect 專用連線” 中的步驟。

建立連線精靈連線

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2. 在導覽窗格中，選擇連線，然後選擇建立連線。
3. 在建立連線頁面的連線順序類型之下，選擇「連線精靈」。
4. 為您的網路連線選擇「彈性等級」。彈性等級可為下列其中之一：

- 最大彈性
- 高彈性
- 開發和測試

如需有關這些彈性等級的說明和更多詳細資訊，請參閱 AWS Direct Connect 彈性工具組。

5. 選擇下一步。
6. 在設定連線頁面上，提供下列詳細資料。

   a. 從頻寬下拉式清單中，選擇連線所需的頻寬。這可以是 1Gbps 到 400 Gbps 的任何位置。

   b. 針對位置，選擇適當的 AWS Direct Connect 位置，然後選擇第一個位置服務供應商，選取在此位置提供連線連線的服務供應商。

   c. 對於第二個位置， AWS Direct Connect 在第二個位置選擇適當的 ，然後選擇第二個位置服務提供者，選擇在此第二個位置提供連線連線的服務提供者。

   d. (選用) 設定連線的 MAC Security (MACsec)。在其他設定之下，選取「要求具 MACsec 能力的連接埠」。

      MACsec 僅能用於專用連線。

   e. (選用) 選擇「新增標籤」以新增金鑰/值配對，進一步協助識別此連線。

      - 在索引鍵中，輸入索引鍵名稱。
      - 在值中，進入索引鍵值。

      若要移除現有的標籤，請選擇該標籤，然後選擇「移除標籤」。標籤不能為空白。

7. 選擇下一步。
8. 在檢閱並建立頁面上，確認連線。此頁面也會顯示連接埠使用量的估計成本和額外的資料傳輸費用。
9. 選擇建立。
10. 下載您的授權書和連線設施指派 (LOA-CFA)，如需詳細資訊，請參閱 the section called “授權書和連線設施指派 (LOA-CFA)”。

請使用下列其中一個命令。

- create-connection (AWS CLI)
- CreateConnection (AWS Direct Connect API)

建立 AWS Direct Connect Classic 連線

對於專用連線，您可以使用 AWS Direct Connect 主控台提交連線請求。對於託管連線，請與 AWS Direct Connect 合作夥伴合作請求託管連線。請務必備妥下列資訊：

- 您需要的連接埠速度。若為專用連線，建立連線請求後，就無法變更連接埠速度。對於託管連線，您的 AWS Direct Connect 合作夥伴可以變更速度。
- 要終止連線 AWS Direct Connect 的位置。

> **Note**
>
> 您無法使用 AWS Direct Connect 主控台請求託管連線。反之，請聯絡 AWS Direct Connect 合作夥伴，他們可以為您建立您接著接受的託管連線。略過以下程序並前往 接受託管連線。

建立新的 AWS Direct Connect 連線

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2. 在 AWS Direct Connect 畫面的 Get Started (開始使用) 區段之下，選擇 Create a connection (建立連線)。
3. 選擇 Classic (傳統)。
4. 對於 Name (連線)，輸入連線的名稱。
5. 對於 Location (據點)，選取合適的 AWS Direct Connect 據點。
6. 如適用，將 Sub Location (子據點) 選為最靠近您本身或網路供應商的樓層。此選項僅適用於該據點所在建築物的多個樓層設有匯接機房 (MMR) 的情況。
7. 對於 Port Speed (連接埠速度)，選擇連線頻寬。
8. 對於內部部署，當您使用此連線來連接到資料中心時，請選取透過 AWS Direct Connect 合作夥伴進行連線。
9. 針對服務提供者，選取 AWS Direct Connect 合作夥伴。如果您使用不在清單中的合作夥伴，請選取 Other (其他)。
10. 如果您對服務供應商選取其他，則對其他供應商的名稱，請輸入您使用的合作夥伴名稱。
11. (選用) 選擇「新增標籤」以新增金鑰/值配對，進一步協助識別此連線。
    - 在索引鍵中，輸入索引鍵名稱。

- 在值中，進入索引鍵值。

若要移除現有的標籤，請選擇該標籤，然後選擇「移除標籤」。標籤不能為空白。

12. 選擇建立連線。

最多可能需要 72 小時 AWS 才能檢閱您的請求，並為您的連線佈建連接埠。在此期間，您可能會收到一封電子郵件，要求您就自身使用案例或指定的據點補齊更多資訊。電子郵件會傳送至您在註冊時使用的電子郵件地址 AWS。您必須在 7 日內回覆，否則將刪除連線。

如需詳細資訊，請參閱專用和託管連線。

下載 AWS Direct Connect LOA-CFA

您可以使用 AWS Direct Connect 主控台或透過命令列下載 LOA-CFA。下載 LOA-CFA 並將其提供給網路或主機代管供應商後，該供應商可以為您訂購交叉連線。

下載 LOA-CFA

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2. 在導覽窗格中，選擇 Connections (連線)。
3. 選取連線，然後選擇檢視詳細資訊。
4. 選擇 Download LOA-CFA (下載 LOA-CFA)。

> **Note**
>
> 如果該連結為未啟用狀態，即表示尚未提供 LOA-CFA 讓您下載。系統會建立支援案例，並請求提供其他資訊。一旦您回應了請求且該請求受到辦理，LOA-CFA 就可以下載。如果仍無法取得，請聯絡 AWS 支援。

5. 將 LOA-CFA 傳送給您的網路供應商或主機代管服務供應商，以便對方能為您訂購交叉連接。各家主機代管服務供應商的聯繫流程可能有所不同。如需詳細資訊，請參閱在 AWS Direct Connect 據點請求交叉連線。

使用命令列或 API 下載 LOA-CFA

- describe-loa (AWS CLI)

- DescribeLoa (AWS Direct Connect API)

將 MACsec CKN/CAK 與 AWS Direct Connect 連線建立關聯

建立支援 MACsec 的連線後，您可以將 CKN/CAK 與連線建立關聯。您可以使用 AWS Direct Connect 主控台或透過命令列或 API 建立關聯。

> **Note**
>
> 將 MACsec 私密金鑰與連線建立關聯之後，即無法修改。如果您需要修改金鑰，請取消金鑰與連線的關聯，然後將新金鑰與連線產生關聯。如需移除關聯的資訊，請參閱 移除 MACsec 私密金鑰和連線之間的關聯。

將 MACsec 金鑰與連線產生關聯

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2. 在左窗格中，選擇 Connections (連線)。
3. 選取連線，然後選擇檢視詳細資訊。
4. 選擇關聯金鑰。
5. 輸入 MACsec 金鑰。

   [使用 CAK/CKN 對] 選擇「金鑰對」，然後執行下列動作：

   - 對於連線關聯金鑰 (CAK)，輸入 CAK。
   - 對於連線關聯金鑰名稱 (CKN)，請輸入 CKN。

   [使用密碼] 選擇「現有的 Secret Manager 密碼，然後對於密碼選取 MACsec 私密金鑰。
6. 選擇關聯金鑰。

使用命令列或 API 將 MACsec 金鑰與連線建立關聯

- associate-mac-sec-key (AWS CLI)
- AssociateMacSecKey (AWS Direct Connect API)

移除 MACsec 私密金鑰與 AWS Direct Connect 連線之間的關聯

您可以使用 AWS Direct Connect 主控台或透過命令列或 API 移除連線與 MACsec 金鑰之間的關聯。

移除連線與 MACsec 金鑰之間的關聯

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2.
3. 在左窗格中，選擇 Connections (連線)。
4. 選取連線，然後選擇檢視詳細資訊。
5. 選取要移除的 MACsec 密碼，然後選擇「取消關聯金鑰]。
6. 在確認對話方塊中，輸入取消關聯，然後選擇取消關聯。

使用命令列或 API 移除連線與 MACsec 金鑰之間的關聯

- disassociate-mac-sec-key (AWS CLI)
- DisassociateMacSecKey (AWS Direct Connect API)

託管 AWS Direct Connect 連線

若要建立 AWS Direct Connect 託管連線，您需要以下資訊：

AWS Direct Connect 位置

在 AWS Direct Connect 合作夥伴計劃中與 AWS Direct Connect 合作夥伴合作，協助您在 AWS Direct Connect 位置與資料中心、辦公室或主機代管環境之間建立網路電路。他們也能夠在和該據點相同設施內提供主機代管空間。如需詳細資訊，請參閱 AWS Direct Connect 交付合作夥伴。

> **Note**
>
> 您無法透過 AWS Direct Connect 主控台請求託管連線。不過， AWS Direct Connect 合作夥伴可以為您建立和設定託管連線。一旦連線設定妥當，連線就會顯示在主控台的連線窗格中。
> 您必須先接受託管連線，才可以使用它。如需詳細資訊，請參閱接受託管連線。

連接埠速度

對於託管連線，可能的值為 50 Mbps、100 Mbps、200 Mbps、300 Mbps、400 Mbps、500 Mbps、1 Gbps、2 Gbps、5 Gbps、10 Gbps 和 25 Gbps。請注意，只有符合特定需求的 AWS Direct Connect 合作夥伴才能建立 1 Gbps、2 Gbps、5 Gbps、10 Gbps 或 25 Gbps 託管連線。25 Gbps 連線僅適用於可提供 100 Gbps 連接埠速度的 Direct Connect 位置。

注意下列事項：

- 連線連接埠速度只能由 AWS Direct Connect 合作夥伴變更。請洽詢您的 AWS Direct Connect 合作夥伴，了解他們是否支援現有連線的升級或降級。如果您的 合作夥伴支援連線的升級/降級，您不需要再刪除並重新建立連線，即可升級或降級現有託管連線的頻寬。
- AWS 會在託管連線上使用流量監管，這表示當流量速率達到設定的最大速率時，會捨棄多餘的流量。這可能會導致突發流量的輸送量低於非突發流量。
- 只有在最初於 AWS Direct Connect 託管父連線上啟用巨型訊框的情況下，巨型訊框才能在連線上啟用。如果未在父連線上啟用巨型訊框，則無法在任何連線上啟用它。

請求託管連線並接受後，可以使用以下主控台操作：

- 刪除一個連線
- 更新連線
- 檢視連線詳細資訊

接受連線之後，您要建立虛擬介面以連接至公有和私有 AWS 資源。如需詳細資訊，請參閱虛擬介面和託管虛擬介面。

接受 AWS Direct Connect 託管連線

如果您有興趣購買託管連線，您必須聯絡 AWS Direct Connect 合作夥伴計劃中的 AWS Direct Connect 合作夥伴。接洽的合作夥伴將為您佈建連線。連線設定妥之後，即會顯示在 主控台的 Connections AWS Direct Connect (連線) 窗格中。

開始使用託管連線之前，您必須先接受該連線。您可以使用 AWS Direct Connect 主控台或使用命令列或 API 接受託管連線。

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。

2. 在導覽窗格中，選擇 Connections (連線)。
3. 選取託管連線，然後選擇檢視詳細資訊。
4. 選取確認核取方塊，然後選擇接受。

使用命令列或 API 接受託管連線

- confirm-connection (AWS CLI)
- ConfirmConnection (AWS Direct Connect API)

刪除 AWS Direct Connect 連線

連線只要沒有虛擬介面與之連接，您就可以將其刪除。刪除您的連線會停止此連線的所有連接埠小時費用，但您可能仍會產生跨連線或網路線路費用（請參閱下文）。 AWS Direct Connect資料傳輸費用與虛擬介面相關聯。如需如何刪除虛擬介面的詳細資訊，請參閱刪除虛擬介面。

刪除連線之前，請下載包含跨帳戶資訊的連線的 LOA，以便您擁有中斷連線之電路的相關資訊。如需下載連線 LOA 的步驟，請參閱 授權書和連線設施指派 (LOA-CFA)。

當您刪除連線時， AWS 會指示主機代管供應商從適用的 AWS 修補程式面板移除光纖交叉連線纜線，以中斷網路裝置與 Direct Connect 路由器的連線。不過，您的主機代管或電路供應商可能仍會向您收取交叉連線或網路電路費用，因為交叉連線纜線可能仍會連接至您的網路裝置。這些交叉連線的費用與 Direct Connect 無關，必須使用來自 LOA 的資訊與主機代管或電路供應商取消。

如果連線是鏈路彙整群組 (LAG) 的一部分，您無法刪除該連線，因為這麼做會導致 LAG 低於其設定的營運連線數目下限。

您可以使用 AWS Direct Connect 主控台或使用命令列或 API 來刪除連線。

刪除連線

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2. 在導覽窗格中，選擇 Connections (連線)。
3. 選取連線，然後選擇 Delete (刪除)。
4. 在 Delete (刪除) 確認對話方塊中，選擇 Delete (刪除)。

使用命令列或 API 刪除連線

- delete-connection (AWS CLI)
- DeleteConnection (AWS Direct Connect API)

更新 AWS Direct Connect 連線

您可以使用 AWS Direct Connect 主控台或使用命令列或 API 更新下列連線屬性。

- 連線的名稱。
- 連線的 MACsec 加密模式。

> **Note**
>
> MACsec 僅能用於專用連線。

有效值為：

- `should_encrypt`
- `must_encrypt`

  當您將加密模式設定為此值時，連線會在加密關閉時一併關閉。
- `no_encrypt`

更新連線

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2. 在導覽窗格中，選擇 Connections (連線)。
3. 選取連線，然後選擇編輯。
4. 修改連線：

   [變更名稱] 針對 Name (名稱)，輸入新的連線名稱。

   [新增標籤] 選擇新增標籤，並執行下列動作：

   - 對於 Key (金鑰)，輸入金鑰名稱。

- 在值中，進入索引鍵值。

[移除標籤] 在標籤旁邊，選擇 移除標籤。

5. 選擇 Edit connection (編輯連線)。

使用命令列或 API 更新連線

- update-connection (AWS CLI)
- UpdateConnection (AWS Direct Connect API)

檢視 AWS Direct Connect 連線詳細資訊

您可以使用 AWS Direct Connect 主控台或使用命令列或 API 來檢視連線的目前狀態。您還能查看其連線 ID (例如 `dxcon-12nikabc`) 並確認是否與您收到或下載的 LOA-CFA 所登記的連線 ID 相符。

如需監控連線的資訊，請參閱 監控 Direct Connect 資源。

檢視連線的相關詳細資訊

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2. 在左窗格中，選擇 Connections (連線)。
3. 選取連線，然後選擇檢視詳細資訊。

使用命令列或 API 描述連線

- describe-connections (AWS CLI)
- DescribeConnections (AWS Direct Connect API)

在 AWS Direct Connect 據點請求交叉連線

下載《授權書和連線設施指派》(LOA-CFA) 之後，您必須完成跨網路連線，也就是交叉連接。如果您已有設備位於 AWS Direct Connect 位置，請聯絡適當的供應商以完成交叉連線。如需每個供應商的特定說明，請參閱下表。合作夥伴和聯絡資訊會依區域組織。對於特定的交叉連線定價，您需要直接聯絡 Direct Connect 合作夥伴。建立交叉連線後，您可以使用 AWS Direct Connect 主控台建立虛擬介面。

有些地點是設定為園區。如需詳細資訊，包含每個位置提供的可用速度，請參閱 AWS Direct Connect 位置。

如果您還沒有位於 AWS Direct Connect 位置的設備，則可以與 AWS 合作夥伴網路 (APN) 中的其中一個合作夥伴合作。他們會協助您連接到 AWS Direct Connect 據點。如需詳細資訊，請參閱 APN 合作夥伴支援 AWS Direct Connect。您必須向所選的供應商提供 LOA-CFA 以利申請交叉連接。

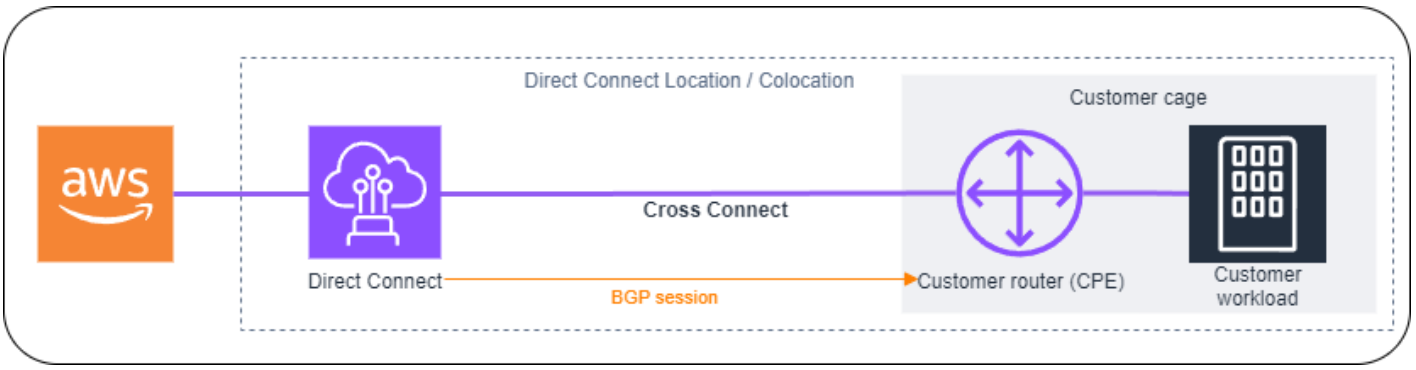
AWS Direct Connect 連線可以提供存取其他 區域中的資源。如需詳細資訊，請參閱存取遠端 AWS Direct Connect 區域。

> **Note**
>
> 若交叉連接未於 90 天內完成，LOA-CFA 授予的權限即告過期。要更新已過期的 LOA-CFA，您可以從 AWS Direct Connect 主控台再次下載。如需詳細資訊，請參閱授權書和連線設施指派 (LOA-CFA)。

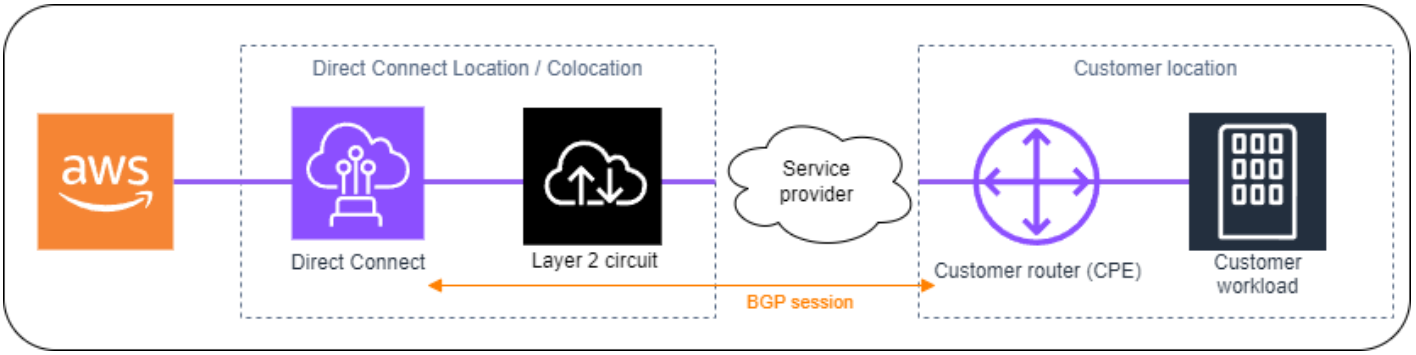
連線選項

連線至 Direct Connect 位置的可用選項可能會因合作夥伴和 AWS 區域而有所不同。您可以與 AWS 合作夥伴網路 (APN) 中的其中一個合作夥伴合作，他們可以提供下列一或多個連線選項：

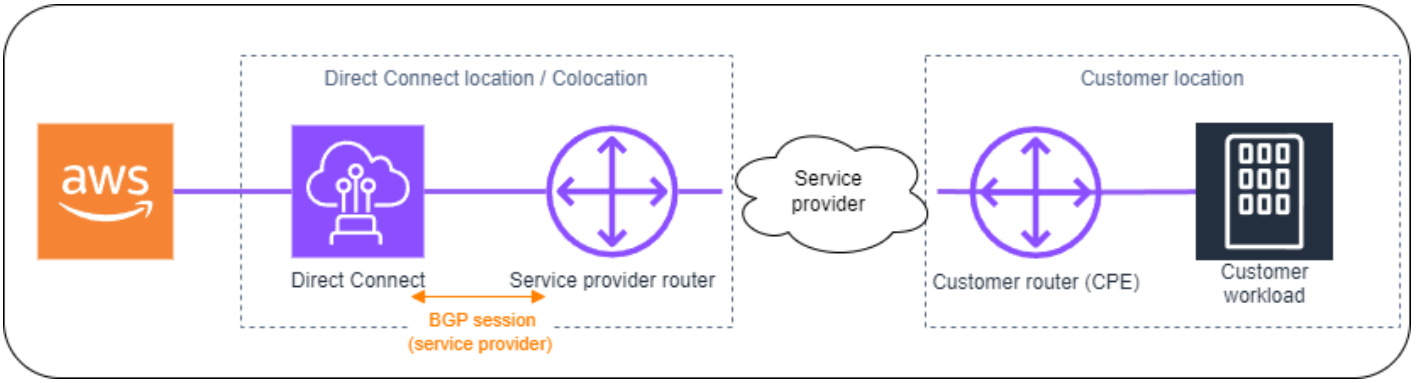
- 如果您將資源部署在與 Direct Connect 位置相同的資料中心/主機代管設施中，該設施可以在 AWS Direct Connect 設備和資源之間提供交叉連線。您必須先提供 LOA-CFA 給設施。如需詳細資訊，請參閱授權書和連線設施指派 (LOA-CFA)。以下顯示此 Direct Connect 連線選項的範例：



- 與 Direct Connect 合作夥伴合作，透過「電路」將第 2 層 （資料連結層） 的 Direct Connect 連線從 Direct Connect 位置擴展到客戶位置。安裝在客戶位置的路由器會直接與 AWS 設備形成 BGP 工作階段。例如，可使用的技術包括 Metro Ethernet、Dark Fibre 或 Wavelength。以下顯示此 Direct Connect 連線選項的範例。



- 與 Direct Connect 合作夥伴合作，將第 3 層 （網路層） 的 Direct Connect 連線從 Direct Connect 位置擴展至您的位置。在此連線選項中，Direct Connect 合作夥伴會在 Direct Connect 位置內提供路由器，以與 AWS 設備形成邊界閘道協定 (BGP) 工作階段。Direct Connect 合作夥伴接著會與您建立另一個 BGP；例如，這可能是透過多協定標籤切換 (MPLS)。以下顯示此 Direct Connect 連線選項的範例。



美國東部 (俄亥俄)

位置	連線申請方式
Cologix COL2，哥倫布	透過 sales@cologix.com 聯絡 Cologix。
Cologix MIN3，明尼亞波利斯	透過 sales@cologix.com 聯絡 Cologix。
CyrusOne West III，休士頓	使用客戶聯絡表單提交請求。
Equinix CH2，芝加哥	透過 awsdealreg@equinix.com 聯絡 Equinix。
QTS，芝加哥	透過 AConnect@qtsdatacenters.com 聯絡 QTS。
Netrality Data Centers, 1102 Grand，堪薩斯市	透過 support@netrality.com 聯絡 Netrality Data Centers。

美國東部 (維吉尼亞北部)

位置	連線申請方式
165 Halsey Street，紐澤克	透過電子郵件聯絡 operations@165halsey.com。
CoreSite 32k，紐約	使用 CoreSite 客戶入口網站下單。填妥表單之後，請檢查訂單的正確性，然後利用網站送交核准。
CoreSite VA1-VA2， Reston	到 CoreSite 客戶入口網站下單。填妥表單之後，請檢查訂單的正確性，然後利用網站送交核准。
Digital Realty ATL1 &ATL2，亞特蘭大	透過 amazon.orders@digitalrealty.com 聯絡 Digital Realty。
Digital Realty IAD38、Ashburn	透過 amazon.orders@digitalrealty.com 聯絡 Digital Realty。
Equinix DC1-DC6 和 DC10-D12，Ashburn	透過 awsdealreg@equinix.com 聯絡 Equinix。

位置	連線申請方式
Equinix DAA1-DC3 和 DC6，達拉斯	透過 awsdealreg@equinix.com 聯絡 Equinix。
Equinix MI1，邁阿密	透過 awsdealreg@equinix.com 聯絡 Equinix。
Equinix NY5， Seacaucus	透過 awsdealreg@equinix.com 聯絡 Equinix。
KIO Networks QRO1、Queretaro、MX	聯絡 KIO Networks"。
Markley, One Summer Street, Boston	對於目前客戶，請使用客戶入口網站建立請求。對於新的查詢，請聯絡 sales@markleygroup.com。
Netrality 資料中心、二樓 MMR、費城	透過 support@netrality.com 聯絡 Netrality Data Centers。
QTS ATL1，亞特蘭大	透過 AConnect@qtsdatacenters.com 聯絡 QTS。

美國西部 (加利佛尼亞北部)

位置	連線申請方式
CoreSite、LA1、洛杉磯	使用 CoreSite 客戶入口網站下單。填妥表單之後，請檢查訂單的正確性，然後利用網站送交核准。
CoreSite SV2，米爾皮塔斯	使用 CoreSite 客戶入口網站下單。填妥表單之後，請檢查訂單的正確性，然後利用網站送交核准。
CoreSite SV4，聖塔克拉拉	使用 CoreSite 客戶入口網站下單。填妥表單之後，請檢查訂單的正確性，然後利用 MyCoreSite 網站送交核准。
EdgeConneX、Phoenix	使用 EdgeOS 客戶入口網站下單。提交表單之後，EdgeConneX 將提供服務訂購單讓您送交核准。如有任何問題請寄至 cloudaccess@edgeconnex.com。
Equinix LA3，艾爾塞貢多	透過 awsdealreg@equinix.com 聯絡 Equinix。

位置	連線申請方式
Equinix SV1 和 SV5，聖荷西	透過 awsdealreg@equinix.com 聯絡 Equinix。
PhoenixNAP，鳳凰城	透過 provisioning@phoenixnap.com 聯絡 phoenixNAP Provisioning。

美國西部 (奧勒岡)

位置	連線申請方式
CoreSite DE1，丹佛	使用 CoreSite 客戶入口網站下單。填妥表單之後，請檢查訂單的正確性，然後利用網站送交核准。
Digital Realty SEA10，Westin Building，西雅圖	透過 amazon.orders@digitalrealty.com 聯絡 Digital Realty。
EdgeConneX，波特蘭	使用 EdgeOS 客戶入口網站下單。提交表單之後，EdgeConneX 將提供服務訂購單讓您送交核准。如有任何問題請寄至 cloudaccess@edgeconnex.com。
Equinix SE2，西雅圖	透過 support@equinix.com 聯絡 Equinix。
Pittock Block，波特蘭	透過電子郵件 crossconnect@pittock.com 或電話 +1 503 226 6777 傳送請求。
Switch SUPERNAP 8，拉斯維加斯	透過 orders@supernap.com 聯絡 Switch SUPERNAP。
TierPoint，西雅圖	透過 sales@tierpoint.com 聯絡 TierPoint。

非洲 (開普敦)

位置	連線申請方式
開普敦網際網路交換中心 / Teraco 資料中心	透過 support@teraco.co.za 聯絡 Teraco 的 Teraco 現有客戶，或透過 connect@teraco.co.za 聯絡新客戶。
Teraco JB1，約翰尼斯堡，南非	透過 support@teraco.co.za 聯絡 Teraco 的 Teraco 現有客戶，或透過 connect@teraco.co.za 聯絡新客戶。

亞太區域 (雅加達)

位置	連線申請方式
DCI JK3，雅加達	透過 jessie.w@dci-indonesia.com.com 聯絡 DCI Indonesia。
NTT 2 Data Center，雅加達	透過 tps.cms.presales@global.ntt 聯絡 NTT。

亞太區域 (孟買)

位置	連線申請方式
Equinix，孟買	透過 awsdealreg@equinix.com 聯絡 Equinix。
NetMagic DC2，邦加羅爾	以免費電話 18001033130 或以 marketing@netmagicsolutions.com 聯絡 NetMagic 銷售和行銷。
Sify Rabale，孟買	透過 aws.directconnect@sifycorp.com 聯絡 Sify。
STT Delhi DC2，德里	透過 enquiry.AWSDX@sttelemediagdc.in 聯絡 STT。
STT GDC Pvt. Ltd. VSB，清奈	透過 enquiry.AWSDX@sttelemediagdc.in 聯絡 STT。
STT Hyderabad DC1，海德拉巴	透過 enquiry.AWSDX@sttelemediagdc.in 聯絡 STT。

亞太區域 (首爾)

位置	連線申請方式
Digital Realty ICN1，首爾	透過 amazon.orders@digitalrealty.com 聯絡 Digital Realty。
KINX Gasan Data Center，首爾	透過 sales@kinx.net 聯絡 KINX。
LG U+ Pyeong-Chon Mega Center，首爾	提交 LOA 文件到 kidcadmin@lguplus.co.kr 和 center8@kidc.net。

亞太區域 (新加坡)

位置	連線申請方式
Equinix HK1, Tsuen Wan N.T.，香港特別行政區	透過 awsdealreg@equinix.com 聯絡 Equinix。
Equinix SG2，新加坡	透過 awsdealreg@equinix.com 聯絡 Equinix。
Global Switch，新加坡	透過 salessingapore@globalswitch.com 聯絡全球交換器。
GPX，孟買	透過 awsdealreg@equinix.com 聯絡 GPX (Equinix)。
iAdvantage Mega-i，香港	透過 cs@iadvantage.net 聯絡 iAdvantage，或使用 iAdvantage 佈線訂購電子表單下單申請。
Menara AIMS，吉隆坡	現有的 AIMS 客戶可至客戶服務入口網站填寫工程施工申請表，申請交叉連接訂單。如果提交申請表時遇到任何問題，請聯絡 service.delivery@aims.com.my。
TCC Data Center，曼谷	透過 gateway.ne@tcc-technology.com 聯絡 TCC Technology Co., Ltd。

亞太區域 (悉尼)

位置	連線申請方式
CDC Hume 2，Canberra	登入 CDC 客戶入口網站的客戶入口網站。
Datacom DH6，奧克蘭	請聯絡 Datacom Orbit –Auckland 的 Datacom。
Equinix ME2，墨爾本	透過 awsdealreg@equinix.com 聯絡 Equinix。
Equinix SY3，雪梨	透過 awsdealreg@equinix.com 聯絡 Equinix。
Global Switch，雪梨	透過 salessydney@globalswitch.com 聯絡全球交換器。
NEXTDC C1，坎培拉	透過 nxtops@nextdc.com 聯絡 NEXTDC。
NEXTDC M1，墨爾本	透過 nxtops@nextdc.com 聯絡 NEXTDC。
NEXTDC P1，伯斯	透過 nxtops@nextdc.com 聯絡 NEXTDC。
NEXTDC S2，雪梨	透過 nxtops@nextdc.com 聯絡 NEXTDC。

亞太區域 (東京)

位置	連線申請方式
AT Tokyo Chuo 資料中心，東京	聯絡 AT TOKYO (at-sales@attokyo.co.jp)。
Chief Telecom LY，台北	透過 vicky_chan@chief.com.tw 聯絡 Chief Telecom。
中華電信，台北	透過 taipei_idc@cht.com.tw 聯絡台北的中華電信 IDC 網路維運中心。
Equinix OS1，大阪	透過 awsdealreg@equinix.com 聯絡 Equinix。
Equinix TY2，東京	透過 awsdealreg@equinix.com 聯絡 Equinix。
NEC Inzai，印西市	透過 connection_support@ices.jp.nec.com 聯絡 NEC Inzai。

加拿大 (中部)

位置	連線申請方式
Telehouse，250 Front St W，多倫多	請聯絡 product@ca.telehouse.com。
Cologix MTL3，蒙特婁	透過 sales@cologix.com 聯絡 Cologix。
Cologix VAN2，溫哥華	透過 sales@cologix.com 聯絡 Cologix。
eStruxture，蒙特婁	透過 directconnect@estruxture.com 聯絡 eStruxture。

中國 (北京)

位置	連線申請方式
CIDS Jiachuang IDC，北京	聯絡 dx-order@sinnet.com.cn。
Sinnet Jiuxianqiao IDC，北京	聯絡 dx-order@sinnet.com.cn。
GDS No. 3 Data Center, Shanghai	聯絡 dx@nwcdcloud.cn。
GDS No. 3 Data Center, Shenzhen	聯絡 dx@nwcdcloud.cn。

中國 (寧夏)

位置	連線申請方式
Industrial Park IDC，寧夏	聯絡 dx@nwcdcloud.cn。
Shapotou IDC，寧夏	聯絡 dx@nwcdcloud.cn。

歐洲 (法蘭克福)

位置	連線申請方式
CE Colo，布拉格，捷克共和國	透過 info@cecolo.com 聯絡 CE Colo。
DigiPlex Ulven，奧斯陸，挪威	透過 helpme@digiplex.com 聯絡 DigiPlex。
Equinix AM3，阿姆斯特丹，荷蘭	透過 awsdealreg@equinix.com 聯絡 Equinix。
Equinix FR5，法蘭克福	透過 awsdealreg@equinix.com 聯絡 Equinix。
Equinix HE6，赫爾辛基	透過 awsdealreg@equinix.com 聯絡 Equinix。
Equinix MU1，慕尼黑	透過 awsdealreg@equinix.com 聯絡 Equinix。
Equinix WA1，華沙	透過 awsdealreg@equinix.com 聯絡 Equinix。
Interxion AMS7，阿姆斯特丹	透過 customer.services@interxion.com 聯絡 Interxion。
Interxion CPH2，哥本哈根	透過 customer.services@interxion.com 聯絡 Interxion。
Interxion FRA6，法蘭克福	透過 customer.services@interxion.com 聯絡 Interxion。
Interxion MAD2，馬德里	透過 customer.services@interxion.com 聯絡 Interxion。
Interxion VIE2，維也納	透過 customer.services@interxion.com 聯絡 Interxion。
Interxion ZUR1，蘇黎世	透過 customer.services@interxion.com 聯絡 Interxion。
IPB，柏林	透過 kontakt@ipb.de 聯絡 IPB。
Equinix ITConic MD2，馬德里	透過 awsdealreg@equinix.com 聯絡 Equinix。

歐洲 (愛爾蘭)

位置	連線申請方式
Digital Realty (UK)，碼頭新區	透過 amazon.orders@digitalrealty.com 聯絡 Digital Realty (英國)。
Eircom Clonshaugh	透過 datacentre@eirevo.ie 聯絡 Eircom。
Equinix DX1，都柏林	透過 awsdealreg@equinix.com 聯絡 Equinix。
Equinix LD5，倫敦 (斯勞區)	透過 awsdealreg@equinix.com 聯絡 Equinix。
Interxion DUB2，都伯林	透過 customer.services@interxion.com 聯絡 Interxion。
Interxion MRS1，馬賽	透過 customer.services@interxion.com 聯絡 Interxion。

歐洲 (米蘭)

位置	連線申請方式
CDLAN Srl in Via Caldera 21，義大利米蘭	透過 sales@cdlan.it 聯絡 CDLAN。
Equinix, ML2，米蘭，義大利	透過 awsdealreg@equinix.com 聯絡 Equinix。

歐洲 (倫敦)

位置	連線申請方式
Digital Realty (UK)，碼頭新區	透過 amazon.orders@digitalrealty.com 聯絡 Digital Realty (英國)。
Equinix LD5，倫敦 (斯勞區)	透過 awsdealreg@equinix.com 聯絡 Equinix。
Equinix MA3，曼徹斯特	透過 awsdealreg@equinix.com 聯絡 Equinix。

位置	連線申請方式
Telehouse West，倫敦	透過 sales.support@uk.telehouse.net 聯絡 Telehouse UK。

Europe (Paris)

位置	連線申請方式
Equinix PA3，巴黎	透過 awsdealreg@equinix.com 聯絡 Equinix。
Interxion PAR7，巴黎	透過 customer.services@interxion.com 聯絡 Interxion。
Telehouse Voltaire，巴黎	使用聯絡我們頁面聯絡 Telehouse Paris Voltaire。

歐洲 (斯德哥爾摩)

位置	連線申請方式
Interxion STO1，斯德哥爾摩	透過 customer.services@interxion.com 聯絡 Interxion。

歐洲 (蘇黎世)

位置	連線申請方式
Equinix ZRH51，上恩斯特林根，瑞士	透過 awsdealreg@equinix.com 聯絡 Equinix。

以色列 (特拉維夫)

位置	連線申請方式
MedOne、海法文	MedOne 聯絡方式： support@Medone.co.il

位置	連線申請方式
EdgeConnex，Herzliya	透過 info@edgeconnecx.com 聯絡 EdgeConnect

Middle East (Bahrain)

位置	連線申請方式
AWS 巴林 DC53，麥納馬	若要完成連線，您可以在要建立連線的位置，使用我們配合的任一網路供應商合作夥伴。然後，您將 AWS 透過AWS 支援中心提供來自網路提供者的授權書 (LOA) 給 。 完成此位置 AWS 的交叉連線。
AWS 巴林 DC52，麥納馬	若要完成連線，您可以在要建立連線的位置，使用我們配合的任一網路供應商合作夥伴。然後，您將 AWS 透過AWS 支援中心提供來自網路提供者的授權書 (LOA) 給 。 完成此位置 AWS 的交叉連線。

中東 (阿拉伯聯合大公國)

位置	連線申請方式
Equinix DX1，杜拜，阿聯酋	透過 awsdealreg@equinix.com 聯絡 Equinix。
Etisalat SmartHub Data Centre，富查伊哈，阿聯酋	透過 IntlSales-C&WS@etisalat.ae 聯絡 Etisalat SmartHub Data Centre。

南美洲 (聖保羅)

位置	連線申請方式
Cirion BNARAGMS，布宜諾斯艾利斯	透過 cloud.connect@ciriontechnologies.com 聯絡 Cirion。

位置	連線申請方式
Equinix RJ2，里約熱內盧	透過 awsdealreg@equinix.com 聯絡 Equinix。
Equinix SP4，聖保羅	透過 awsdealreg@equinix.com 聯絡 Equinix。
Tivit	透過 aws@tivit.com.br 聯絡 Tivit。

AWS GovCloud（美國東部）

您無法在此區域中排序連線。

AWS GovCloud（美國西部）

位置	連線申請方式
Equinix SV5，聖荷西	透過 awsdealreg@equinix.com 聯絡 Equinix。

AWS Direct Connect 虛擬介面和託管虛擬介面

您必須建立下列其中一個虛擬介面 VIFs)，才能開始使用您的 AWS Direct Connect 連線。

- 私有虛擬介面：私有虛擬介面應使用私有 IP 地址來存取 Amazon VPC。
- 公有虛擬介面：公有虛擬介面可以使用 AWS 公有 IP 地址存取所有公有服務。
- 傳輸虛擬介面：傳輸虛擬介面應該用於將一或多個關聯至 Direct Connect 閘道的 Amazon VPC Transit Gateways。您可以使用傳輸虛擬介面搭配任何速度的任何 AWS Direct Connect 專用或託管連線。如需 Direct Connect 閘道組態的相關資訊，請參閱Direct Connect 閘道。

若要使用 IPv6 地址連線至其他 AWS 服務，請檢查服務文件以確認支援 IPv6 定址。

公有虛擬介面字首公告規則

我們會向您公告適當的 Amazon 字首，以便您可以存取 VPCs和其他 AWS 服務中工作負載的公有 IP 地址。您可以透過此連線存取所有字 AWS 首；例如，Amazon EC2 執行個體、Amazon S3、 AWS 服務 API 端點和 Amazon.com 所使用的公有 IP 地址。您無權存取非 Amazon 字首。如需 使用的目前字首清單 AWS，請參閱《Amazon VPC 使用者指南》中的 AWS IP 地址範圍。在此頁面上，您可以下載目前發佈 AWS IP 範圍`.json`的檔案。請注意，對於已發佈的 IP 地址範圍：

- 與 AWS IP 地址範圍清單中列出的項目相比，透過 BGP 透過公有虛擬界面宣布的字首可能會彙總或取消彙總。
- 您 AWS 透過自己的 IP 地址 (BYOIP) 帶到 的任何 IP 地址範圍都不會包含在 `.json` 檔案中，但仍會透過公有虛擬界面 AWS 公告這些 BYOIP 地址。
- AWS 不會將透過 Direct Connect 公有虛擬介面接收的客戶字首重新公告到 外部的網路 AWS。所有客戶都可看見在公有虛擬界面上公告的字首 AWS。

> **Note**
>
> 建議您使用防火牆篩選條件 (根據封包的來源/目的地的地址) 來控制某些字首的流量進出。

如需有關公有虛擬介面和路由政策的詳細資訊，請參閱 the section called “公用虛擬介面路由政策”。

SiteLink

如果您要建立私有或傳輸虛擬介面，您可以使用 SiteLink。

SiteLink 是虛擬私有介面的選用 Direct Connect 功能，可使用 AWS 網路中最短的可用路徑，在相同 AWS 分割區中的任何兩個 Direct Connect 存在點 (PoPs) 之間進行連線。這可讓您透過 AWS 全球網路連線內部部署網路，而不需要透過區域路由流量。如需 SiteLink 的詳細資訊，請參閱 Introducing AWS Direct Connect SiteLink。

> **Note**
>
> - SiteLink 不適用於 AWS GovCloud (US) 和中國區域。
> - 如果內部部署路由器在多個虛擬介面 AWS 上向 公告相同的路由，則 SiteLink 無法運作。

使用 SiteLink 需要另外付費。如需詳細資訊，請參閱 AWS Direct Connect 定價。

SiteLink 不支援所有虛擬介面類型。下表顯示介面類型以及是否可支援。

虛擬介面類型	支援/不支援
傳輸虛擬介面	支援
私有虛擬介面附加至 Direct Connect 閘道 (具有虛擬閘道)	支援
附加至 Direct Connect 閘道的私有虛擬介面不會與虛擬閘道或傳輸閘道建立關聯	支援
連接至虛擬閘道的私有虛擬介面	不支援
公有虛擬介面	不支援

透過啟用 SiteLink 的虛擬界面，從 AWS 區域（虛擬或傳輸閘道）到內部部署位置的流量路由行為，與 AWS 路徑前面的預設 Direct Connect 虛擬介面行為略有不同。啟用 SiteLink 時，無論相關聯的

區域為何，來自 的虛擬介面 AWS 區域 偏好具有較低 AS 路徑長度的 BGP 路徑。例如，會針對每個 Direct Connect 位置公告相關聯的區域。如果停用 SiteLink，則根據預設，來自虛擬或傳輸閘道的流量會偏好與 AWS 區域相關聯的 Direct Connect 位置，即使來自與不同區域相關聯之 Direct Connect 位置的路由器公告具有較短 AS 路徑長度的路徑也一樣。虛擬或傳輸閘道仍然偏好從關聯 AWS 區域的本機 Direct Connect 位置的路徑。

SiteLink 支援的巨型框架 MTU 大小上限為 8500 或 9001，這會因虛擬介面類型而有所不同。如需詳細資訊，請參閱私有虛擬介面或傳輸虛擬介面的 MTUs 。

虛擬介面的先決條件

在建立虛擬介面之前，請先執行下列操作：

- 建立連線。如需詳細資訊，請參閱使用連線精靈建立連線。
- 當您有想要視為單一連線的多個連線時，建立鏈路彙總群組 (LAG)。如需相關資訊，請參閱將連線與 LAG 產生關聯。 。

建立虛擬介面時需要以下資訊：

資源	必要資訊
Connection (連線)	您要為其建立虛擬介面的 AWS Direct Connect 連線或連結彙總群組 (LAG)。
虛擬介面名稱	虛擬介面的名稱。
虛擬介面擁有者	如果您要為另一個帳戶建立虛擬介面，則需要另一個帳戶 AWS 的帳戶 ID。
(僅限私有虛擬介面) 連線	若要連線到相同區域中的 VPC AWS ，您需要 VPC 的虛擬私有閘道。BGP 工作階段的 Amazon 端 ASN 是繼承自虛擬私有閘道。當您建立虛擬私有閘道時，您可指定自己的私有 ASN。否則，Amazon 會提供預設的 ASN。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的建立虛擬私有閘道。若要透過 Direct Connect 閘道連線至 VPC，您需要該 Direct Connect 閘道。如需詳細資訊，請參閱 Direct Connect 閘道。 **Note** •

資源	必要資訊
	您無法將相同的 ASN 用於客戶閘道和虛擬介面上的虛擬閘道/Direct Connect 閘道。 • 您可以針對多個虛擬介面使用相同的客戶閘道 ASN。 • 多個虛擬介面可以具有相同的虛擬閘道/Direct Connect 閘道 ASN 和客戶閘道 ASN，只要它們是不同 Direct Connect 連線的一部分。例如： 虛擬閘道 (ASN 64，496) <---虛擬介面 1 (Direct Connect 連線 1)---> 客戶閘道 (ASN 64，511) 虛擬閘道 (ASN 64，496) <---虛擬介面 2 (Direct Connect 連線 2)---> 客戶閘道 (ASN 64，511)
VLAN	您的連線尚未使用的唯一虛擬區域網路 (VLAN) 標籤。此值必須介於 1 到 4094 之間，且必須符合乙太網路 802.1Q 標準。任何周遊 AWS Direct Connect 連線的流量都需使用此標籤。 如果您有託管連線，您的 AWS Direct Connect 合作夥伴會提供此值。建立虛擬介面後，就無法修改該值。

資源	必要資訊
對等 IP 地址	虛擬介面可以支援 IPv4、IPv6 或其中一個 (雙堆疊) 的 BGP 對等工作階段。請勿使用彈性 IPs(EIPs) 或從 Amazon 集區使用您自己的 IP 地址 (BYOIP) 來建立公有虛擬介面。您無法在相同的虛擬介面上為相同 IP 地址系列建立多個 BGP 工作階段。IP 地址範圍會指派給 BGP 對等工作階段之虛擬介面的每一端。 • IPv4： • (僅限公有虛擬介面) 您必須指定您擁有的唯一公有 IPv4 地址。 Note • 私有和傳輸虛擬介面的對等 IPs 可以來自任何有效的 IP 範圍。這也可以包含客戶擁有的公有 IP 地址，只要這些地址僅用於建立 BGP 對等互連工作階段，而不是透過虛擬介面公告或用於 NAT。 • 我們無法保證能夠滿足所提供公有 AWS IPv4 地址的所有請求。 值可為下列其中之一： • 客戶擁有的 IPv4 CIDR 這些可以是任何公有 IPs（客戶擁有或提供 AWS)，但您的對等 IP 和 AWS 路由器對等 IP 都必須使用相同的子網路遮罩。例如，如果您配置/31範圍，例如 `203.0.113.0/31` ，則可以將 `203.0.113.0` 用於對等 IP 和 `203.0.113.1` 用於 AWS 對等 IP。或者，如果您配置/24範圍，例如 `198.51.100.0/24` ，您可以將 `198.51.100.10` 用於對等 IP 和`198.51.100.20` 對 AWS 等 IP。 • AWS Direct Connect 合作夥伴或 ISP 擁有的 IP 範圍，以及 LOA-CFA 授權。

資源	必要資訊
	• AWS 提供的 /31 CIDR。請聯絡 AWS Support 以請求公有 IPv4 CIDR (並在請求中提供使用案例) • (僅限私有虛擬介面) Amazon 可以為您產生私有 IPv4 地址。如果您指定自己的 IP 地址，請確認僅為您的路由器介面和 AWS Direct Connect 介面指定私有 CIDR。例如，請勿從您的本機網路指定其他 IP 地址。與公有虛擬介面類似，相同的子網路遮罩必須同時用於對等 IP 和 AWS 路由器對等 IP。例如，如果您配置/30範圍，例如 192.168.0.0/30 ，則可以將 192.168.0.1 用於對等 IP 和 192.168.0.2 用於 AWS 對等 IP。 • IPv6：Amazon 會自動為您配置一個 /125 IPv6 CIDR。您無法指定自己的對等 IPv6 地址。
地址系列	BGP 對等工作階段是否會透過 IPv4 或 IPv6 進行。
BGP 資訊	• BGP 工作階段在您這端的公有或私有邊界閘道協定 (BGP) 自治系統編號 (ASN)。您必須擁有公有 ASN 才能使用。如果您使用的是私有 ASN，即可設定自訂 ASN 值。對於 16 位元的 ASN，此值的範圍必須為 64512 到 65534。對於 32 位元的 ASN，此值的範圍必須為 1 到 2147483647。如果您使用私有 ASN 做為公有虛擬介面，則自治系統 (AS) 前置無法運作。 • AWS 根據預設， 會啟用 MD5。您無法修改此選項。 • 一個 MD5 BGP 驗證金鑰。您可以提供自己的資訊，或是由 Amazon 為您生成。

資源	必要資訊
(僅限公有虛擬介面) 您要公告的字首	要透過 BGP 公告的公有 IPv4 路由或 IPv6 路由。您必須使用 BGP 公告至少一個字首，最多可公告 1,000 個字首。 • IPv4：當下列任一情況成立 AWS Direct Connect 時，IPv4 CIDR 可以與使用 宣布的另一個公有 IPv4 CIDR 重疊： • CIDRs 來自不同的 AWS 區域。請確定您在公有字首上套用 BGP 社群標籤。 • 主動/被動組態中具備公有 ASN 時，您可以使用 AS_PATH。 如需更多資訊，請參閱路由政策和 BGP 社群。 • 透過 Direct Connect 公有虛擬界面，您可以為 IPv4 指定從 /1 到 /32 的任何字首長度，並為 IPv6 指定從 /1 到 /IPv64 的任何字首長度。 • 您可以將其他字首新增至現有的公有 VIF，並透過聯絡 AWS 支援部門來公告。在您的支援案例中，提供您要新增至公有 VIF 並公告的其他 CIDR 字首清單。
（僅限私有和傳輸虛擬介面） 巨型訊框	封包經過的最大傳輸單位 (MTU) AWS Direct Connect。預設值為 1500。設定虛擬介面的 MTU 為 8500 (巨型訊框)，可能導致基礎實體連線的更新，如果未更新到支援巨型訊框。更新連線會干擾所有連線相關聯的虛擬介面的網路連線能力達 30 秒。Direct Connect 支援高達 8500 MTU 的巨型訊框。傳輸閘道路由表中設定的靜態路由和傳播路由會支援巨型訊框，包含從具有 VPC 靜態路由表項目的 EC2 執行個體到傳輸閘道連接。若要檢查連線或虛擬介面是否支援巨型訊框，請在 AWS Direct Connect 主控台中選取它，然後在虛擬介面一般組態頁面上尋找支援的巨型訊框。

建立虛擬介面時，您可以指定擁有該虛擬介面的帳戶。當您選擇不是您 AWS 帳戶的帳戶時，適用下列規則：

- 對於私有 VIF 與傳輸 VIF，該帳戶適用於虛擬介面和虛擬私有閘道/Direct Connect 閘道目標。
- 對於公有 VIF，該帳戶用於虛擬介面計費。資料傳輸輸出 (DTO) 用量會以 AWS Direct Connect 資料傳輸率向資源擁有者計量。

> **Note**
>
> 所有 Direct Connect 虛擬介面類型都支援 31 位元字首。如需詳細資訊，請參閱 RFC 3021：在 IPv4 點對點連結上使用 31 位元字首。

私有虛擬介面或傳輸虛擬介面的 MTUs

AWS Direct Connect 在連結層支援 1522 或 9023 位元組的乙太網路框架大小 (14 位元組乙太網路標頭 + 4 位元組 VLAN 標籤 + IP 資料包的位元組 + 4 位元組 FCS)。

網路連線的最大傳輸單位 (MTU) 係允許通過該連線的最大封包大小 (以位元組為單位)。虛擬私有介面的 MTU 可以是 1500 或 9001 (巨型訊框)。傳輸虛擬介面的 MTU 可以是 1500 或 8500 (巨型訊框)。當您可以在建立介面或在建立後更新時，指定 MTU。設定虛擬介面的 MTU 為 8500 (巨型訊框) 9001 (巨型訊框)，可能導致基礎實體連線的更新，如果未更新到支援巨型訊框。更新連線會干擾所有連線相關聯的虛擬介面的網路連線能力達 30 秒。若要檢查連線或虛擬介面是否支援巨型訊框，請在 AWS Direct Connect 主控台中選取它，然後在摘要索引標籤上尋找巨型訊框功能。

在您為私有虛擬介面或傳輸虛擬介面啟用巨型訊框後，您可以將它與連線或具巨型訊框能力的 LAG 建立關聯。巨型訊框在附加至虛擬私有閘道或 Direct Connect 閘道的私有虛擬介面上受到支援，或在附加至 Direct Connect 閘道的傳輸虛擬介面上受到支援。如果您有兩個公告相同路由，但使用不同 MTU 值的私有虛擬介面，或若您有公告相同路由的站對站 VPN，請使用 1500 MTU。

> **Important**
>
> 巨型訊框僅適用於透過 傳播的路由， AWS Direct Connect 以及透過傳輸閘道傳播的靜態路由。傳輸閘道上的巨型框架僅支援 8500 位元組。
> 如果 EC2 執行個體不支援巨型訊框，它會從 Direct Connect 下拉巨型訊框架。所有 EC2 執行個體類型支援巨型框架，C1、CC1、T1 和 M1 除外。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的 EC2 執行個體的網路最大傳輸單位 (MTU)。 Amazon EC2
> 對於託管連線，唯有在最初已於 Direct Connect 託管的上階連線上啟用巨型訊框的情況下，巨型訊框才能啟用。如果未在父連線上啟用巨型訊框，則無法在任何連線上啟用它。
> 私有 VIFs MTUs 正在標準化為 8500。9001 將繼續被接受，直到移除為止。

如需設定私有虛擬介面 MTU 的步驟，請參閱設定私有虛擬介面的 MTU。

AWS Direct Connect 虛擬介面

您可以建立傳輸虛擬介面以連接至傳輸閘道，或建立公有虛擬介面以連接至公有資源 (非 VPC 服務)，或者建立私有虛擬介面以連接至 VPC。

若要為 內的帳戶建立虛擬介面 AWS Organizations，或與 AWS Organizations 不同的帳戶，請建立託管虛擬介面。

請參閱以下內容以建立虛擬介面：

- 建立公有虛擬介面
- 建立私有虛擬介面。
- 建立傳輸虛擬介面以連往 Direct Connect 閘道

先決條件

開始之前，請務必先詳閱虛擬介面的先決條件所述資訊。

將虛擬介面傳輸到 Direct Connect 閘道的先決條件

若要將 AWS Direct Connect 連線連接到傳輸閘道，您必須為連線建立傳輸介面。指定要連接的 Direct Connect 閘道。

網路連線的最大傳輸單位 (MTU) 係允許通過該連線的最大封包大小 (以位元組為單位)。虛擬私有介面的 MTU 可以是 1500 或 9001 (巨型訊框)。傳輸虛擬介面的 MTU 可以是 1500 或 8500 (巨型訊框)。當您可以在建立介面或在建立後更新時，指定 MTU。設定虛擬介面的 MTU 為 8500 (巨型訊框) 9001 (巨型訊框)，可能導致基礎實體連線的更新，如果未更新到支援巨型訊框。更新連線會干擾所有連線相關聯的虛擬介面的網路連線能力達 30 秒。若要檢查連線或虛擬介面是否支援巨型訊框，請在 AWS Direct Connect 主控台中選取該巨型訊框，然後在摘要索引標籤上找出具備巨型訊框能力。

> **Important**
>
> 如果您將傳輸閘道與一或多個 Direct Connect 閘道產生關聯，則傳輸閘道和 Direct Connect 閘道所使用的自治系統編號 (ASN) 必須不同。例如，如果您同時針對傳輸閘道和 Direct Connect 閘道使用預設 ASN 64512，則關聯要求會失敗。

建立 AWS Direct Connect 公有虛擬介面

建立公有虛擬介面之後，從審查到核准您的申請可能需要 72 小時的時間。

佈建公有虛擬介面

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2. 在導覽窗格中，選擇 Virtual Interfaces (虛擬介面)。
3. 選擇建立虛擬介面。
4. 在虛擬介面類型之下，針對類型選擇公有。
5. 在公有虛擬介面設定 之下，執行下列動作：

   a. 針對虛擬介面名稱，輸入虛擬介面的名稱。

   b. 針對連線，選擇要用於此介面的 Direct Connect 連線。

   c. 針對 VLAN，為您的虛擬區域網路 (VLAN) 輸入 ID 號碼。

   d. 針對 BGP ASN，輸入新虛擬介面內部部署對等路由器的邊界閘道通訊協定自治系統編號 (ASN)。

   有效值為 1-2147483647。

   > **Note**
   >
   > 透過公 AWS 有虛擬介面使用 建立 BGP 對等互連工作階段時，請使用 7224 做為 ASN，在 AWS 側邊建立 BGP 工作階段。路由器或客戶閘道裝置上的 ASN 應與該 ASN 不同。

6. 在 Additional settings (其他設定) 之下，執行下列動作：

   a. 若要設定 IPv4 BGP 或 IPv6 對等，請執行下列動作：

   [IPv4] 若要設定 IPv4 BGP 對等，請選擇 IPv4，然後執行以下動作：

   - 若要自行指定這些 IP 地址，對於 Your router peer ip (您的路由器對等 IP)，輸入 Amazon 應傳送流量至該處的目的地 IPv4 CIDR 地址。
   - 對於 Amazon router peer IP (Amazon 路由器對等 IP)，輸入用以傳送流量至 AWS的 IPv4 CIDR 地址。

[IPv6] 若要設定 IPv6 BGP 對等，請選擇 IPv6。對等 IPv6 地址是自動從 Amazon 的 IPv6 地址集區所指派。您無法指定自訂 IPv6 地址。

b. 若要提供自己的 BGP 金鑰，請輸入您的 BGP MD5 金鑰。

如果您未輸入值，我們會產生 BGP 金鑰。如果您提供了自己的金鑰，或者我們為您產生了金鑰，則該值會顯示在虛擬介面的虛擬介面詳細資料頁面之 BGP 驗證金鑰欄中。

c. 若要對 Amazon 公告字首，對於欲公告的字首，輸入應透過虛擬介面將流量路由傳送至該處的目的地 IPv4 CIDR 地址 (以逗號分隔)。

> **Important**
>
> 您可以將其他字首新增至現有的公有 VIF，並透過聯絡 AWS 支援部門來公告。在您的支援案例中，提供您要新增至公有 VIF 並公告的其他 CIDR 字首清單。

d. (選用) 新增或移除標籤。

[新增標籤] 選擇 Add tag (新增標籤)，並執行下列動作：

- 對於 Key (金鑰)，輸入金鑰名稱。
- 在值中，進入索引鍵值。

[移除標籤] 在標籤旁邊，選擇 移除標籤。

7. 選擇建立虛擬介面。
8. 為您的裝置下載路由器組態。如需詳細資訊，請參閱下載路由組態檔案。

使用命令列或 API 建立公有虛擬介面

- create-public-virtual-interface (AWS CLI)
- CreatePublicVirtualInterface (AWS Direct Connect API)

建立 AWS Direct Connect 私有虛擬介面

您可以將私有虛擬介面佈建至與 AWS Direct Connect 連線位於相同區域中的虛擬私有閘道。如需將私有虛擬介面佈建至 AWS Direct Connect 閘道的詳細資訊，請參閱 AWS Direct Connect 閘道。

如果您是使用 VPC 精靈建立 VPC，系統將自動為您啟用路由傳播。透過路由傳播，路由會自動填入到您 VPC 中的路由表。您可以選擇停用路由傳播。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的在路由表中啟用路由傳播。

網路連線的最大傳輸單位 (MTU) 係允許通過該連線的最大封包大小 (以位元組為單位)。虛擬私有介面的 MTU 可以是 1500 或 9001 (巨型訊框)。傳輸虛擬介面的 MTU 可以是 1500 或 8500 (巨型訊框)。當您可以在建立介面或在建立後更新時，指定 MTU。設定虛擬介面的 MTU 為 8500 (巨型訊框) 9001 (巨型訊框)，可能導致基礎實體連線的更新，如果未更新到支援巨型訊框。更新連線會干擾所有連線相關聯的虛擬介面的網路連線能力達 30 秒。若要檢查連線或虛擬介面是否支援巨型訊框，請在 AWS Direct Connect 主控台中選取該巨型訊框，然後在摘要索引標籤上找出具備巨型訊框能力。

> **Note**
>
> 私有虛擬介面的 MTU 正在標準化為 8500；不過，系統將繼續支援 9100，直到移除為止。

佈建私有虛擬介面連往 VPC

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2. 在導覽窗格中，選擇 Virtual Interfaces (虛擬介面)。
3. 選擇建立虛擬介面。
4. 在虛擬介面類型之下，選擇「私有」。
5. 在公有虛擬介面設定之下，執行下列動作：

   a. 針對虛擬介面名稱，輸入虛擬介面的名稱。

   b. 針對連線，選擇要用於此介面的 Direct Connect 連線。

   c. 對於虛擬介面擁有者， AWS 如果虛擬介面適用於您的帳戶，請選擇我的 AWS 帳戶。

   d. 對於 Direct Connect gateway (Direct Connect 閘道)，選擇 Direct Connect 閘道。

   e. 針對 VLAN，為您的虛擬區域網路 (VLAN) 輸入 ID 號碼。

   f. 針對 BGP ASN，為新的虛擬介面輸入您內部部署對等路由器的邊界閘道協定自治系統編號。

      有效值為 1 至 2147483647。
6. 在 Additional settings (其他設定) 之下，執行下列動作：

   a. 若要設定 IPv4 BGP 或 IPv6 對等，請執行下列動作：

[IPv4] 若要設定 IPv4 BGP 對等，請選擇 IPv4，然後執行以下動作：

- 若要自行指定這些 IP 地址，對於 Your router peer ip (您的路由器對等 IP)，輸入 Amazon 應傳送流量至該處的目的地 IPv4 CIDR 地址。
- 對於 Amazon 路由器對等 IP，輸入用以傳送流量至 AWS的 IPv4 CIDR 地址。

> **Important**
>
> 設定 AWS Direct Connect 虛擬介面時，您可以使用 RFC 1918 指定自己的 IP 地址、使用其他定址機制，或選擇從 RFC 3927 169.25IPv4.0.0/16 IPv4 Link-Local 範圍配置的 AWS 指派 IPv4/29 CIDR 地址point-to-point連線。這些point-to-point連線應僅用於客戶閘道路由器和 Direct Connect 端點之間的 eBGP 互連。針對 VPC 流量或通道用途，例如 AWS Site-to-Site私有 IP VPN 或 Transit Gateway Connect， AWS 建議使用客戶閘道路由器上的迴路或 LAN 界面做為來源或目的地地址，而非point-to-point連線。
>
> - 如需有關 RFC 1918 的詳細資訊，請參閱私有網路的地址配置。
> - 如需有關 RFC 3927 的詳細資訊，請參閱 IPv4 Link-Local 地址的動態組態。

[IPv6] 若要設定 IPv6 BGP 對等，請選擇 IPv6。對等 IPv6 地址是自動從 Amazon 的 IPv6 地址集區所指派。您無法指定自訂 IPv6 地址。

b. 若要將最大傳輸單位 (MTU) 從 1500 (預設) 變更至 8500 (巨型框架)，請選取 Jumbo MTU (MTU size 8500) (巨型 MTU (MTU 大小 8500))。

> **Note**
>
> 私有虛擬介面的 MTU 正在標準化為 8500；不過，系統將繼續支援 9100，直到移除為止。

c. (選用) 在啟用 SiteLink 之下，選擇啟用以啟用 Direct Connect 連接點之間的直接連線。

d. (選用) 新增或移除標籤。

[新增標籤] 選擇 Add tag (新增標籤)，並執行下列動作：

- 對於 Key (金鑰)，輸入金鑰名稱。
- 在值中，進入索引鍵值。

[移除標籤] 在標籤旁邊，選擇 移除標籤。

7. 選擇建立虛擬介面。
8. 為您的裝置下載路由器組態。如需詳細資訊，請參閱下載路由組態檔案。

使用命令列或 API 建立私有虛擬介面

- create-private-virtual-interface (AWS CLI)
- CreatePrivateVirtualInterface (AWS Direct Connect API)

建立傳輸虛擬介面到 AWS Direct Connect 閘道

將傳輸虛擬介面連線至 Direct Connect 閘道之前，請先熟悉文字。

將傳輸虛擬介面佈建於 Direct Connect 閘道

1. 開啟 AWS Direct Connect主控台，網址為 http：//https://console.aws.amazon.com/directconnect/v2/home。
2. 在導覽窗格中，選擇 Virtual Interfaces (虛擬介面)。
3. 選擇建立虛擬介面。
4. 在虛擬介面類型之下，針對類型選擇傳輸。
5. 在傳輸虛擬介面設定之下，執行下列動作：

   a. 針對虛擬介面名稱，輸入虛擬介面的名稱。
   b. 針對連線，選擇要用於此介面的 Direct Connect 連線。
   c. 對於虛擬介面擁有者， AWS 如果虛擬介面適用於您的帳戶，請選擇我的 AWS 帳戶。
   d. 對於 Direct Connect gateway (Direct Connect 閘道)，選擇 Direct Connect 閘道。
   e. 針對 VLAN，為您的虛擬區域網路 (VLAN) 輸入 ID 號碼。
   f. 針對 BGP ASN，為新的虛擬介面輸入您內部部署對等路由器的邊界閘道協定自治系統編號。

      有效值為 1 至 2147483647。
6. 在 Additional settings (其他設定) 之下，執行下列動作：

   a. 若要設定 IPv4 BGP 或 IPv6 對等，請執行下列動作：

      [IPv4] 若要設定 IPv4 BGP 對等，請選擇 IPv4，然後執行以下動作：
      - 若要自行指定這些 IP 地址，對於 Your router peer ip (您的路由器對等 IP)，輸入 Amazon 應傳送流量至該處的目的地 IPv4 CIDR 地址。

- 對於 Amazon 路由器對等 IP，輸入用以傳送流量至 AWS的 IPv4 CIDR 地址。

> **Important**
>
> 設定 AWS Direct Connect 虛擬介面時，您可以使用 RFC 1918 指定自己的 IP 地址、使用其他定址機制，或選擇從 RFC 3927 169.254.0.0/16 IPv4 連結本機範圍配置的 AWS 指派 IPv4 /29 CIDR 地址point-to-point連線。這些point-to-point連線應僅用於客戶閘道路由器和 Direct Connect 端點之間的 eBGP 互連。針對 VPC 流量或通道用途，例如 AWS Site-to-Site私有 IP VPN 或 Transit Gateway Connect， AWS 建議使用客戶閘道路由器上的迴路或 LAN 界面作為來源或目的地地址，而非point-to-point連線。
>
> - 如需有關 RFC 1918 的詳細資訊，請參閱私有網路的地址配置。
> - 如需有關 RFC 3927 的詳細資訊，請參閱 IPv4 Link-Local 地址的動態組態。

[IPv6] 若要設定 IPv6 BGP 對等，請選擇 IPv6。對等 IPv6 地址是自動從 Amazon 的 IPv6 地址集區所指派。您無法指定自訂 IPv6 地址。

b. 若要將最大傳輸單位 (MTU) 從 1500 (預設) 變更至 8500 (巨型框架)，請選取 Jumbo MTU (MTU size 8500) (巨型 MTU (MTU 大小 8500))。

c. (選用) 在啟用 SiteLink 之下，選擇啟用以啟用 Direct Connect 連接點之間的直接連線。

d. (選用) 新增或移除標籤。

[新增標籤] 選擇 Add tag (新增標籤)，並執行下列動作：

- 對於 Key (金鑰)，輸入金鑰名稱。
- 在值中，進入索引鍵值。

[移除標籤] 在標籤旁邊，選擇 移除標籤。

7. 選擇建立虛擬介面。

建立虛擬介面之後，您可為您的裝置下載路由器組態。如需詳細資訊，請參閱下載路由組態檔案。

使用命令列或 API 建立傳輸虛擬介面

- create-transit-virtual-interface (AWS CLI)
- CreateTransitVirtualInterface (AWS Direct Connect API)

使用命令列或 API 檢視連接至 Direct Connect 閘道的虛擬介面

- describe-direct-connect-gateway-attachments (AWS CLI)
- DescribeDirectConnectGatewayAttachments (AWS Direct Connect API)

下載 AWS Direct Connect 路由器組態檔案

建立虛擬介面且介面狀態為啟動之後，您可以下載路由器的路由器組態檔案。

如果您將以下任何路由器用於已啟用 MACsec 的虛擬介面，我們會自動為您的路由器建立組態檔案：

- 執行 NX-OS 9.3 或更新版本軟體的 Cisco Nexus 9K+ Series switches
- 執行 JunOS 9.5 或更新版本軟體的 Juniper Networks M/MX Series Routers

下載路由器組態檔案

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2. 在導覽窗格中，選擇 Virtual Interfaces (虛擬介面)。
3. 選取虛擬介面，然後選擇檢視詳細資訊。
4. 選擇 Download router configuration (下載路由器組態)。
5. 對於 Download Router Configuration (下載路由器組態)，請執行以下動作：
   a. 針對 Vendor (廠商)，選取路由器的製造商。
   b. 針對 Platform (平台)，選取路由器的型號。
   c. 針對 Software (軟體)，選取路由器的軟體版本。
6. 選擇 Download (下載)，接著使用路由器的適當組態來確保您可以連接至 AWS Direct Connect。
7. 如果您需要為 MACsec 手動設定路由器，請使用下表作為指導方針。

參數	描述
CKN 長度	這是 64 個十六進位字元 (0–9，A–E) 字串。使用完整長度來最大化跨平台相容性。
CAK 長度	這是 64 個十六進位字元 (0–9，A–E) 字串。使用完整長度來最大化跨平台相容性。

參數	描述
密碼編譯演算法	AES_256_CMAC
SAK 密碼套件	• 對於 100 Gbps 連線：GCM_AES_XPN_256 • 對於 10 Gbps 連線：GCM_AES_XPN_256 or GCM_AES _256
金鑰密碼套件	16
機密性位移	0
ICV 指示器	否
SAK 重設金鑰時間	PN 變換 >

託管 AWS Direct Connect 虛擬介面

若要使用與其他帳戶的 AWS Direct Connect 連線，您可以為該帳戶建立託管虛擬介面。另一帳戶的擁有者必須接受此託管虛擬介面後才能開始加以使用。託管虛擬介面的作用與標準虛擬介面相同，可以連接到公有資源或 VPC。

您可以使用傳輸虛擬介面搭配任何速度的 Direct Connect 專用或託管連線。託管連線僅支援一個虛擬介面。

建立虛擬介面時需要以下資訊：

資源	必要資訊
Connection (連線)	您要為其建立虛擬介面的 AWS Direct Connect 連線或連結彙總群組 (LAG)。
虛擬介面名稱	虛擬介面的名稱。
虛擬介面擁有者	如果您要為另一個帳戶建立虛擬介面，則需要另一個帳戶 AWS 的帳戶 ID。
(僅限私有虛擬介面) 連線	若要連線到相同區域中的 VPC AWS ，您需要 VPC 的虛擬私有閘道。BGP 工作階段的 Amazon 端 ASN 是繼承自虛擬私有閘道。當您建立虛擬私有閘道時，您可指定自己的私有 ASN。否則，Amazon 會提供預設的 ASN。如需詳細

資源	必要資訊
	資訊，請參閱《Amazon VPC 使用者指南》中的建立虛擬私有閘道。若要透過 Direct Connect 閘道連線至 VPC，您需要該 Direct Connect 閘道。如需詳細資訊，請參閱 Direct Connect 閘道。
VLAN	您的連線尚未使用的唯一虛擬區域網路 (VLAN) 標籤。此值必須介於 1 到 4094 之間，且必須符合乙太網路 802.1Q 標準。任何周遊 AWS Direct Connect 連線的流量都需使用此標籤。 如果您有託管連線，您的 AWS Direct Connect 合作夥伴會提供此值。建立虛擬介面後，就無法修改該值。

資源	必要資訊

對等 IP 地址	虛擬介面可以支援 IPv4、IPv6 或其中一個 (雙堆疊) 的 BGP 對等工作階段。請勿使用彈性 IPs(EIPs) 或從 Amazon 集區使用您自己的 IP 地址 (BYOIP) 來建立公有虛擬介面。您無法在相同的虛擬介面上為相同 IP 地址系列建立多個 BGP 工作階段。IP 地址範圍會指派給 BGP 對等工作階段之虛擬介面的每一端。
	
	• IPv4：
	  • (僅限公有虛擬介面) 您必須指定您擁有的唯一公有 IPv4 地址。值可為下列其中之一：
	  • 客戶擁有的 IPv4 CIDR
	
	這些可以是任何公有 IPs（客戶擁有或提供 AWS)，但相同的子網路遮罩必須同時用於對等 IP 和 AWS 路由器對等 IP。例如，如果您配置/31範圍，例如 `203.0.113.0/31` ，則可以將 `203.0.113.0` 用於對等 IP 和 `203.0.113.1` 用於 AWS 對等 IP。或者，如果您配置/24範圍，例如 `198.51.100.0/24` ，則可以將 `198.51.100.10` 用於對等 IP 和`198.51.100.20` 對 AWS 等 IP。
	  • AWS Direct Connect 合作夥伴或 ISP 擁有的 IP 範圍，以及 LOA-CFA 授權
	  • AWS提供的 /31 CIDR。請聯絡 AWS Support 以請求公有 IPv4 CIDR (並在請求中提供使用案例)
	
	Note
	我們無法保證我們能夠滿足 AWS提供公有 IPv4 地址的所有請求。
	
	  • (僅限私有虛擬介面) Amazon 可以為您產生私有 IPv4 地址。如果您指定自己的 CIDRs。 AWS 例如，請勿從您的本機網路指定其他 IP 地址。與公有虛擬介面類似，您的對等 IP 和 AWS 路由器對等 IP 必須使用相同的子網路遮罩。例如，如果您配置/30範圍，例如 `192.168.0.0/30` ，則可以將 `192.168.0.1` 用於對等 IP 和 `192.168.0.2` 用於 AWS 對等 IP。
	• IPv6：Amazon 會自動為您配置一個 /125 IPv6 CIDR。您無法指定自己的對等 IPv6 地址。

資源	必要資訊
地址系列	BGP 對等工作階段是否會透過 IPv4 或 IPv6 進行。
BGP 資訊	• BGP 工作階段在您這端的公有或私有邊界閘道協定 (BGP) 自治系統編號 (ASN)。您必須擁有公有 ASN 才能使用。如果您使用的是私有 ASN，即可設定自訂 ASN 值。對於 16 位元的 ASN，此值的範圍必須為 64512 到 65534。對於 32 位元的 ASN，此值的範圍必須為 1 到 2147483647。如果您使用私有 ASN 做為公有虛擬介面，則自治系統 (AS) 前置無法運作。 • AWS 預設會啟用 MD5。您無法修改此選項。 • 一個 MD5 BGP 驗證金鑰。您可以提供自己的資訊，或是由 Amazon 為您生成。

(僅限公有虛擬介面) 您要公告的字首	要透過 BGP 公告的公有 IPv4 路由或 IPv6 路由。您必須使用 BGP 公告至少一個字首，最多可公告 1,000 個字首。
	• IPv4：當下列任一情況成立 AWS Direct Connect 時，IPv4 CIDR 可以與使用 宣布的另一個公有 IPv4 CIDR 重疊：
	  • CIDRs 來自不同的 AWS 區域。請確定您在公有字首上套用 BGP 社群標籤。
	  • 主動/被動組態中具備公有 ASN 時，您可以使用 AS_PATH。
	  如需更多資訊，請參閱路由政策和 BGP 社群。
	• 透過 Direct Connect 公有虛擬介面，您可以為 IPv4 指定從 /1 到 /32 的任何字首長度，並為 IPv6 指定從 /1 到 /IPv64 的任何字首長度。
	• 您可以將其他字首新增至現有的公有 VIF，並透過聯絡 AWS 支援部門來公告。在您的支援案例中，提供您要新增至公有 VIF 並公告的其他 CIDR 字首清單。

資源	必要資訊
（僅限私有和傳輸虛擬介面）巨型訊框	封包經過的最大傳輸單位 (MTU) AWS Direct Connect。預設值為 1500。設定虛擬介面的 MTU 為 9001 (巨型訊框)，可能導致基礎實體連線的更新，如果未更新到支援巨型訊框。更新連線會干擾所有連線相關聯的虛擬介面的網路連線能力達 30 秒。巨型訊框僅適用於從 傳播的路由 AWS Direct Connect。如果您將靜態路由新增至指向虛擬私有閘道的路由表格，則透過靜態路由傳送的流量會使用 1500 MTU。若要檢查連線或虛擬介面是否支援巨型訊框，請在 AWS Direct Connect 主控台中選取它，然後在虛擬介面一般組態頁面上尋找支援的巨型訊框。

在 中建立託管私有虛擬介面 AWS Direct Connect

開始之前，請務必先詳閱虛擬介面的先決條件所述資訊。

建立私有託管虛擬介面

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2. 在導覽窗格中，選擇 Virtual Interfaces (虛擬介面)。
3. 選擇建立虛擬介面。
4. 在虛擬介面類型之下，對於類型，請選擇私有。
5. 在公有虛擬介面設定之下，執行下列動作：

   a. 針對虛擬介面名稱，輸入虛擬介面的名稱。

   b. 針對連線，選擇要用於此介面的 Direct Connect 連線。

   c. 對於虛擬介面擁有者，請選擇「其他 AWS 帳戶」，然後針對虛擬介面擁有者輸入要擁有此虛擬介面的帳戶 ID。

   d. 針對 VLAN，為您的虛擬區域網路 (VLAN) 輸入 ID 號碼。

   e. 針對 BGP ASN，為新的虛擬介面輸入您內部部署對等路由器的邊界閘道協定自治系統編號。

   有效值為 1-2147483647。
6. 在 Additional settings (其他設定) 之下，執行下列動作：

   a. 若要設定 IPv4 BGP 或 IPv6 對等，請執行下列動作：

[IPv4] 若要設定 IPv4 BGP 對等，請選擇 IPv4，然後執行以下動作：

- 若要自行指定這些 IP 地址，對於 Your router peer ip (您的路由器對等 IP)，輸入 Amazon 應傳送流量至該處的目的地 IPv4 CIDR 地址。
- 對於 Amazon 路由器對等 IP，輸入用以傳送流量至 AWS的 IPv4 CIDR 地址。

> **Important**
>
> 設定 AWS Direct Connect 虛擬介面時，您可以使用 RFC 1918 指定自己的 IP 地址、使用其他定址機制，或選擇從 RFC 3927 169.25IPv4.0.0/16 IPv4 Link-Local 範圍配置的 AWS 指派 IPv4/29 CIDR 地址point-to-point連線。這些point-to-point連線應僅用於客戶閘道路由器和 Direct Connect 端點之間的 eBGP 互連。針對 VPC 流量或通道用途，例如 AWS Site-to-Site私有 IP VPN 或 Transit Gateway Connect， AWS 建議使用客戶閘道路由器上的迴路或 LAN 界面做為來源或目的地地址，而非point-to-point連線。
>
> - 如需有關 RFC 1918 的詳細資訊，請參閱私有網路的地址配置。
> - 如需有關 RFC 3927 的詳細資訊，請參閱 IPv4 Link-Local 地址的動態組態。

[IPv6] 若要設定 IPv6 BGP 對等，請選擇 IPv6。對等 IPv6 地址是自動從 Amazon 的 IPv6 地址集區所指派。您無法指定自訂 IPv6 地址。

b. 若要將最大傳輸單位 (MTU) 從 1500 (預設) 變更至 8500 (巨型框架)，請選取 Jumbo MTU (MTU size 8500) (巨型 MTU (MTU 大小 8500))。

> **Note**
>
> 私有虛擬介面的 MTU 正在標準化為 8500；不過，系統將繼續支援 9100，直到移除為止。

c. (選用) 新增或移除標籤。

[新增標籤] 選擇 Add tag (新增標籤)，並執行下列動作：

- 對於 Key (金鑰)，輸入金鑰名稱。
- 在值中，進入索引鍵值。

[移除標籤] 在標籤旁邊，選擇 移除標籤。

7. 在另一個 AWS 帳戶的擁有者接受託管虛擬界面之後，您可以下載組態檔案。如需詳細資訊，請參閱下載路由組態檔案。

使用命令列或 API 建立私有託管虛擬介面

- allocate-private-virtual-interface (AWS CLI)
- AllocatePrivateVirtualInterface (AWS Direct Connect API)

在 中建立託管公有虛擬介面 AWS Direct Connect

開始之前，請務必先詳閱虛擬介面的先決條件所述資訊。

建立公有託管虛擬介面

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2. 在導覽窗格中，選擇 Virtual Interfaces (虛擬介面)。
3. 選擇建立虛擬介面。
4. 在虛擬介面類型之下，針對類型選擇公有。
5. 在公有虛擬介面設定之下，執行下列動作：

   a. 針對虛擬介面名稱，輸入虛擬介面的名稱。

   b. 針對連線，選擇要用於此介面的 Direct Connect 連線。

   c. 對於虛擬介面擁有者，請選擇另一個 AWS 帳戶，然後對於虛擬介面擁有者，輸入帳戶 ID 以擁有此虛擬介面。

   d. 針對 VLAN，為您的虛擬區域網路 (VLAN) 輸入 ID 號碼。

   e. 針對 BGP ASN，為新的虛擬介面輸入您內部部署對等路由器的邊界閘道協定自治系統編號。

   有效值為 1-2147483647。
6. 若要設定 IPv4 BGP 或 IPv6 對等，請執行下列動作：

   [IPv4] 若要設定 IPv4 BGP 對等，請選擇 IPv4，然後執行以下動作：

   - 若要自行指定這些 IP 地址，對於 Your router peer ip (您的路由器對等 IP)，輸入 Amazon 應傳送流量至該處的目的地 IPv4 CIDR 地址。
   - 對於 Amazon 路由器對等 IP，輸入用以傳送流量至 AWS的 IPv4 CIDR 地址。

[IPv6] 若要設定 IPv6 BGP 對等，請選擇 IPv6。對等 IPv6 地址是自動從 Amazon 的 IPv6 地址集區所指派。您無法指定自訂 IPv6 地址。

7. 若要對 Amazon 公告字首，對於欲公告的字首，輸入應透過虛擬介面將流量路由傳送至該處的目的地 IPv4 CIDR 地址 (以逗號分隔)。
8. 若要提供自己的金鑰來驗證 BGP 工作階段，請在 Additional Settings (其他設定) 之下，針對 BGP authentication key (BGP 驗證金鑰) 輸入金鑰。

   如果您未輸入值，則我們會產生 BGP 金鑰。
9. (選用) 新增或移除標籤。

   [新增標籤] 選擇 Add tag (新增標籤)，並執行下列動作：

   - 對於 Key (金鑰)，輸入金鑰名稱。
   - 在值中，進入索引鍵值。

   [移除標籤] 在標籤旁邊，選擇 移除標籤。
10. 選擇建立虛擬介面。
11. 在另一個 AWS 帳戶的擁有者接受託管虛擬介面之後，您可以下載組態檔案。如需詳細資訊，請參閱下載路由組態檔案。

使用命令列或 API 建立公有託管虛擬介面

- allocate-public-virtual-interface (AWS CLI)
- AllocatePublicVirtualInterface (AWS Direct Connect API)

建立 AWS Direct Connect 託管傳輸虛擬介面

建立託管的傳輸虛擬介面

> **Important**
>
> 如果您將傳輸閘道與一或多個 Direct Connect 閘道產生關聯，則傳輸閘道和 Direct Connect 閘道所使用的自治系統編號 (ASN) 必須不同。例如，如果您同時針對傳輸閘道和 Direct Connect 閘道使用預設 ASN 64512，則關聯要求會失敗。

1. 開啟 AWS Direct Connect主控台，網址為 https://console.aws.amazon.com/directconnect/v2/home：//。
2. 在導覽窗格中，選擇 Virtual Interfaces (虛擬介面)。
3. 選擇建立虛擬介面。
4. 在虛擬介面類型之下，針對類型選擇傳輸。
5. 在傳輸虛擬介面設定之下，執行下列動作：

   a. 針對虛擬介面名稱，輸入虛擬介面的名稱。

   b. 針對連線，選擇要用於此介面的 Direct Connect 連線。

   c. 對於虛擬介面擁有者，請選擇另一個 AWS 帳戶，然後對於虛擬介面擁有者，輸入帳戶 ID 以擁有此虛擬介面。

   d. 針對 VLAN，為您的虛擬區域網路 (VLAN) 輸入 ID 號碼。

   e. 針對 BGP ASN，為新的虛擬介面輸入您內部部署對等路由器的邊界閘道協定自治系統編號。

   有效值為 1-2147483647。
6. 在 Additional settings (其他設定) 之下，執行下列動作：

   a. 若要設定 IPv4 BGP 或 IPv6 對等，請執行下列動作：

   [IPv4] 若要設定 IPv4 BGP 對等，請選擇 IPv4，然後執行以下動作：

   - 若要自行指定這些 IP 地址，對於 Your router peer ip (您的路由器對等 IP)，輸入 Amazon 應傳送流量至該處的目的地 IPv4 CIDR 地址。
   - 對於 Amazon 路由器對等 IP，輸入用以傳送流量至 AWS的 IPv4 CIDR 地址。

   > **Important**
   >
   > 設定 AWS Direct Connect 虛擬介面時，您可以使用 RFC 1918 指定自己的 IP 地址、使用其他定址機制，或選擇從 RFC 3927 169.254.0.0/16 IPv4 連結本機範圍配置的 AWS 指派 IPv4 /29 CIDR 地址point-to-point連線。這些point-to-point連線應僅用於客戶閘道路由器和 Direct Connect 端點之間的 eBGP 互連。針對 VPC 流量或通道用途，例如 AWS Site-to-Site私有 IP VPN 或 Transit Gateway Connect， AWS 建議使用客戶閘道路由器上的迴路或 LAN 界面做為來源或目的地地址，而非point-to-point連線。
   >
   > - 如需有關 RFC 1918 的詳細資訊，請參閱私有網路的地址配置。
   > - 如需有關 RFC 3927 的詳細資訊，請參閱 IPv4 Link-Local 地址的動態組態。

[IPv6] 若要設定 IPv6 BGP 對等，請選擇 IPv6。對等 IPv6 地址是自動從 Amazon 的 IPv6 地址集區所指派。您無法指定自訂 IPv6 地址。

b. 若要將最大傳輸單位 (MTU) 從 1500 (預設) 變更至 8500 (巨型框架)，請選取 Jumbo MTU (MTU size 8500) (巨型 MTU (MTU 大小 8500))。

c. [選用] 新增標籤。請執行下列操作：

[新增標籤] 選擇新增標籤，並執行下列動作：

- 對於 Key (金鑰)，輸入金鑰名稱。
- 在值中，進入索引鍵值。

[移除標籤] 在標籤旁邊，選擇 移除標籤。

7. 選擇建立虛擬介面。
8. 在另一個 AWS 帳戶的擁有者接受託管虛擬界面之後，您可以下載裝置的路由器組態檔案。如需詳細資訊，請參閱下載路由組態檔案。

使用命令列或 API 建立傳輸託管虛擬介面

- allocate-transit-virtual-interface (AWS CLI)
- AllocateTransitVirtualInterface (AWS Direct Connect API)

檢視 AWS Direct Connect 虛擬介面詳細資訊

您可以使用 AWS Direct Connect 主控台或使用命令列或 API 檢視虛擬介面的目前狀態。詳細資訊包含：

- 連線狀態
- 名稱
- 位置
- VLAN
- BGP 詳細資訊
- 對等 IP 地址

檢視虛擬介面的相關詳細資訊

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2. 在左窗格中，選擇虛擬介面。
3. 選取虛擬介面，然後選擇檢視詳細資訊。

使用命令列或 API 描述虛擬介面

- describe-virtual-interfaces (AWS CLI)
- DescribeVirtualInterfaces (AWS Direct Connect API)

將 BGP 對等新增至 AWS Direct Connect 虛擬介面

使用 AWS Direct Connect 主控台或使用命令列或 API，將 IPv4 或 IPv6 BGP 對等工作階段新增至虛擬介面。

虛擬介面可支援單一 IPv4 BGP 對等工作階段以及單一 IPv6 BGP 對等工作階段。您無法為 IPv6 BGP 對等工作階段自行指定對等 IPv6 地址。Amazon 會自動為您配置一個 /125 IPv6 CIDR。

多重協定 BGP 不受支援。IPv4 和 IPv6 在虛擬介面的雙堆疊模式下運作。

AWS 預設會啟用 MD5。您無法修改此選項。

請使用下列程序來新增 BGP 對等。

新增 BGP 對等

1. 開啟 AWS Direct Connect主控台，網址為 https://console.aws.amazon.com/directconnect/v2/home：//。
2. 在導覽窗格中，選擇 Virtual Interfaces (虛擬介面)。
3. 選取虛擬介面，然後選擇檢視詳細資訊。
4. 選擇 Add peering (新增對等)。
5. (私有虛擬介面) 如要新增 IPv4 BGP 對等，請執行以下操作：
   - 選擇 IPv4。

- 若要自行指定這些 IP 地址，對於 Your router peer ip (您的路由器對等 IP)，輸入 Amazon 應傳送流量至該處的目的地 IPv4 CIDR 地址。對於 Amazon 路由器對等 IP，輸入用以傳送流量至 AWS的 IPv4 CIDR 地址。

6. (公有虛擬介面) 如要新增 IPv4 BGP 對等，請執行以下操作：

   - 對於 Your router peer ip (您的路由器對等 IP)，輸入應傳送流量至該處的目的地 IPv4 CIDR 地址。
   - 對於 Amazon router peer IP (Amazon 路由器對等 IP)，輸入用以傳送流量至 AWS的 IPv4 CIDR 地址。

   > **Important**
   >
   > 設定 AWS Direct Connect 虛擬介面時，您可以使用 RFC 1918 指定自己的 IP 地址、使用其他定址機制，或選擇從 RFC 3927 169.254.0.0/16 IPv4 連結本機範圍配置的 AWS 指派 IPv4 /29 CIDR 地址point-to-point連線。這些point-to-point連線應僅用於客戶閘道路由器和 Direct Connect 端點之間的 eBGP 互連。針對 VPC 流量或通道用途，例如 AWS Site-to-Site私有 IP VPN 或 Transit Gateway Connect， AWS 建議使用客戶閘道路由器上的迴路或 LAN 界面做為來源或目的地地址，而非point-to-point連線。
   >
   > - 如需有關 RFC 1918 的詳細資訊，請參閱私有網路的地址配置。
   > - 如需有關 RFC 3927 的詳細資訊，請參閱 IPv4 Link-Local 地址的動態組態。

7. (私有或公有虛擬介面) 若要新增 IPv6 BGP 對等，請選擇 IPv6。對等 IPv6 地址是自動從 Amazon 的 IPv6 地址集區所指派；您無法指定自訂 IPv6 地址。
8. 針對 BGP ASN，為新的虛擬介面輸入您內部部署對等路由器的邊界閘道協定自治系統編號。

   若為公有虛擬介面，ASN 必須屬於私有或已列入虛擬介面的允許名單。

   有效值為 1-2147483647。

   請注意，如果您不輸入值，我們就會自動指派一個值。
9. 若要提供自己的 BGP 金鑰，對於 BGP Authentication Key (BGP 驗證金鑰)，輸入您的 BGP MD5 金鑰。
10. 選擇 Add peering (新增對等)。

使用命令列或 API 建立 BGP 對等

- create-bgp-peer (AWS CLI)

- CreateBGPPeer (AWS Direct Connect API)

刪除 AWS Direct Connect 虛擬介面 BGP 對等

如果您的虛擬介面同時有 IPv4 和 IPv6 BGP 對等工作階段，您可以刪除其中一個 BGP 對等工作階段 (但不能兩者都刪除)。您可以使用 AWS Direct Connect 主控台或使用命令列或 API 來刪除虛擬介面 BGP 對等。

刪除 BGP 對等

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2. 在導覽窗格中，選擇 Virtual Interfaces (虛擬介面)。
3. 選取虛擬介面，然後選擇檢視詳細資訊。
4. 在 Peerings (對等互連) 之下，選取您要刪除的對等互連，然後選擇 Delete (刪除)。
5. 在從虛擬介面移除對等互連對話方塊中，選擇刪除。

使用命令列或 API 刪除 BGP 對等

- delete-bgp-peer (AWS CLI)
- DeleteBGPPeer (AWS Direct Connect API)

設定 AWS Direct Connect 私有虛擬介面的 MTU

如果您的虛擬介面同時有 IPv4 和 IPv6 BGP 對等工作階段，您可以刪除其中一個 BGP 對等工作階段 (但不能兩者都刪除)。如需 MTUs和私有虛擬介面的詳細資訊，請參閱私有虛擬介面或傳輸虛擬介面 MTUs。

您可以使用 AWS Direct Connect 主控台或使用命令列或 API 來設定私有虛擬介面的 MTU。

建立私有虛擬介面的 MTU

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2. 在導覽窗格中，選擇 Virtual Interfaces (虛擬介面)。
3. 選取虛擬界面，然後選擇 Edit (編輯)。

4. 在巨型 MTU (MTU 大小 8500) 下，選取已啟用。
5. 在 Acknowledge (認可) 之下，選取 I understand the selected connection(s) will go down for a brief period (我了解選取的連線將短暫關閉一段期間)。虛擬介面的狀態是 `pending` 直到更新完成為止。

使用命令列或 API 設定建立私有虛擬介面的 MTU

- update-virtual-interface-attributes (AWS CLI)
- UpdateVirtualInterfaceAttributes (AWS Direct Connect API)

新增或移除 AWS Direct Connect 虛擬介面標籤

標籤可供識別虛擬介面。如果您是虛擬介面的帳戶擁有者，您可以使用 AWS Direct Connect 主控台或使用命令列或 API 來新增或移除標籤。

新增或移除虛擬介面標籤

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2. 在導覽窗格中，選擇 Virtual Interfaces (虛擬介面)。
3. 選取虛擬界面，然後選擇 Edit (編輯)。
4. 新增或移除標籤。

   [新增標籤] 選擇新增標籤，並執行下列動作：

   - 對於 Key (金鑰)，輸入金鑰名稱。
   - 在值中，進入索引鍵值。

   [移除標籤] 在標籤旁邊，選擇 移除標籤。
5. 選擇編輯虛擬介面。

若要使用命令列新增標籤和移除標籤

- tag-resource (AWS CLI)
- untag-resource (AWS CLI)

刪除 AWS Direct Connect 虛擬介面

刪除一或多個虛擬介面。刪除連線之前，您必須先刪除其虛擬介面。刪除虛擬介面會停止與虛擬介面相關聯的 AWS Direct Connect 資料傳輸費用。

您可以使用 AWS Direct Connect 主控台或命令列或 API 刪除虛擬介面。

刪除虛擬介面

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2. 在左窗格中，選擇虛擬介面。
3. 選取虛擬介面，然後選擇刪除。
4. 在 Delete (刪除) 確認對話方塊中，選擇 Delete (刪除)。

使用命令列或 API 刪除虛擬介面

- delete-virtual-interface (AWS CLI)
- DeleteVirtualInterface (AWS Direct Connect API)

接受託管 AWS Direct Connect 虛擬介面

開始使用託管虛擬介面之前，您必須先接受該虛擬介面。若為私有虛擬介面，您還必須已有虛擬私有閘道或是 Direct Connect 閘道。若為傳輸虛擬介面，您還必須已有傳輸閘道或是 Direct Connect 閘道。

您可以使用 AWS Direct Connect 主控台或命令列或 API 接受託管虛擬介面。

接受託管虛擬介面

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2. 在導覽窗格中，選擇 Virtual Interfaces (虛擬介面)。
3. 選取虛擬介面，然後選擇檢視詳細資訊。
4. 選擇 Accept (接受)。
5. 這適用於私有虛擬介面和傳輸虛擬介面。

(傳輸虛擬介面) 在接受虛擬介面對話方塊中，選取 Direct Connect 閘道，然後選擇接受虛擬介面。

(私有虛擬介面) 在接受虛擬介面對話方塊中，選取虛擬私有閘道或 Direct Connect 閘道，然後選擇接受虛擬介面。

6. 當您接受了此託管虛擬介面之後， AWS Direct Connect 連線的擁有者便可下載路由器組態檔案。下載路由器組態選項不適用於接受託管虛擬介面的帳戶。

使用命令列或 API 接受私有託管虛擬介面

- confirm-private-virtual-interface (AWS CLI)
- ConfirmPrivateVirtualInterface (AWS Direct Connect API)

使用命令列或 API 接受公有託管虛擬介面

- confirm-public-virtual-interface (AWS CLI)
- ConfirmPublicVirtualInterface (AWS Direct Connect API)

使用命令列或 API 接受公有託管虛擬介面

- confirm-transit-virtual-interface (AWS CLI)
- ConfirmTransitVirtualInterface (AWS Direct Connect API)

遷移 AWS Direct Connect 虛擬介面

當您想要執行下列任一虛擬介面遷移操作時，請使用此程序：

- 將與連線相關聯的現有虛擬介面遷移至另一個 LAG。
- 將與現有 LAG 相關聯的現有虛擬介面遷移至新 LAG。
- 將與連線相關聯的現有虛擬介面遷移至另一個連線。

Note

- 您可以將虛擬介面遷移到相同區域內的新連線，但無法將其從一個區域遷移到另一個區域。當您將現有虛擬介面遷移到新連線或與新連線產生關聯時，與那些虛擬介面相關聯的組態參數是相同的。若要避開此狀況，您可以在連線上預先安裝設定，然後更新 BGP 組態。
- 您無法將 VIF 從一個託管連線遷移到另一個託管連線。VLAN ID 是唯一的；因此，以這種方式遷移 VIF 表示 VLAN 不會相符。您需要刪除連線或 VIF，然後使用連線和 VIF 均相同的 VLAN 重新建立連線。

Important

虛擬介面將短時間關閉。我們建議您在維護期間執行此程序。

遷移虛擬介面

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2. 在導覽窗格中，選擇 Virtual Interfaces (虛擬介面)。
3. 選取虛擬介面，然後選擇編輯。
4. 對於 Connection (連線)，請選取 LAG 或連線。
5. 選擇編輯虛擬介面。

使用命令列或 API 遷移虛擬介面

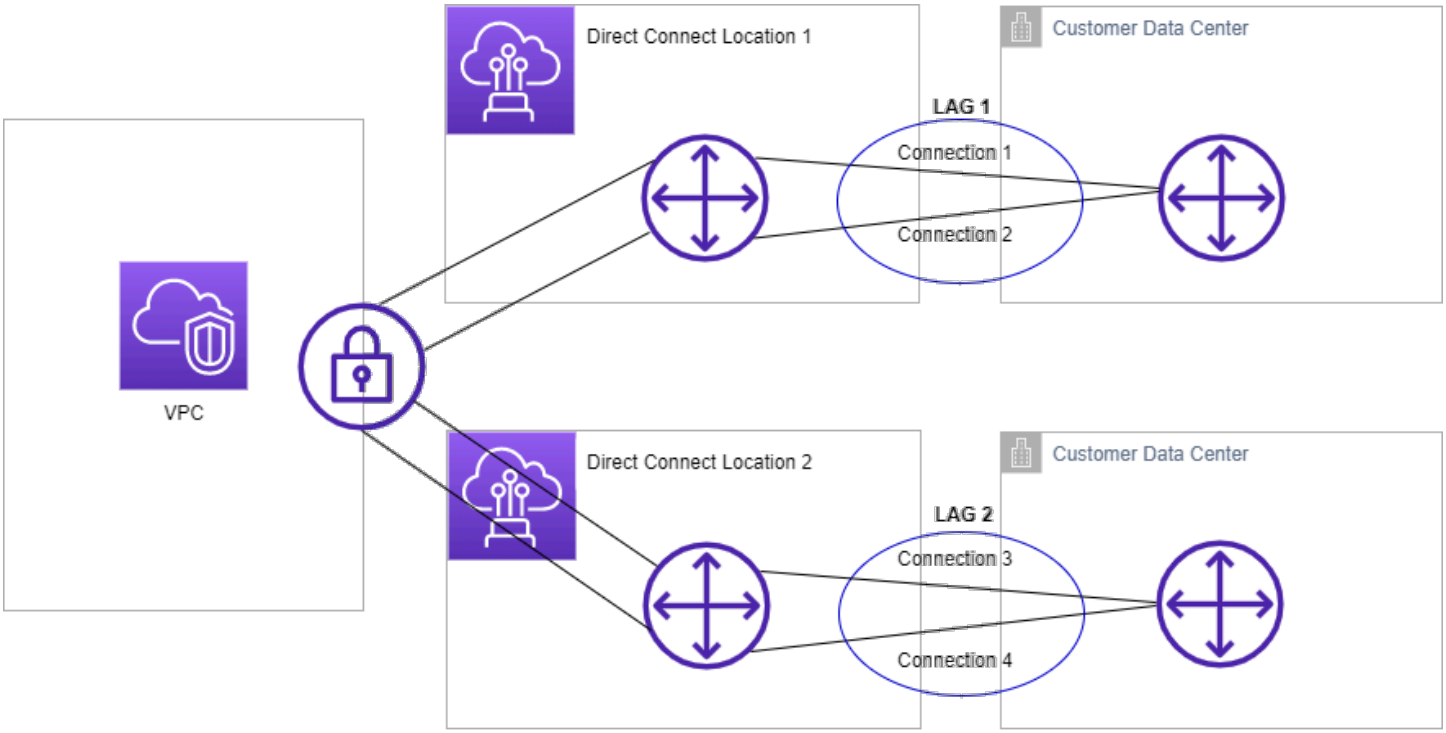
- associate-virtual-interface (AWS CLI)
- AssociateVirtualInterface (AWS Direct Connect API)

AWS Direct Connect 連結彙總群組 (LAGs)

您可以使用多個連線來增加可用頻寬。連結彙總群組 (LAG) 是邏輯界面，使用連結彙總控制通訊協定 (LACP) 在單一 AWS Direct Connect 端點彙總多個連線，可讓您將它們視為單一受管連線。LAG 可簡化組態，因為 LAG 組態適用於群組中的所有連線。

> **Note**
>
> 不支援多機箱 LAG (MLAG) AWS。

在下圖中，您有四個連線，而且每個位置都有兩個連線。您可以為在相同 AWS 裝置和相同位置終止的連線建立 LAG，然後使用兩個 LAGs，而不是四個連線進行組態和管理。



您可以從現有的連線建立 LAG，或者佈建新的連線。建立 LAG 之後，您可將現有的連線 (無論其為獨立的連線或屬於另一個 LAG) 與該 LAG 產生關聯。

適用的規定如下：

- 所有連線都必須是專用連線，連接埠速度必須為 1 Gbps、10 Gbps、100 Gbps 或 400 Gbps。
- LAG 中的所有連線必須使用相同的頻寬。

- 您最多可以擁有兩個 100 Gbps 或 400 Gbps 的連線，或四個連接埠速度小於 100 Gbps 的連線。LAG 中的每個連線都將計入區域的整體連線限制。
- LAG 中的所有連線都必須在相同的 AWS Direct Connect 端點終止。
- 所有虛擬介面類型 (包含公有、私有和傳輸) 均支援 LAG。

當您建立 LAG 時，您可以從 AWS Direct Connect 主控台個別下載新實體連線的授權與連線設施指派 (LOA-CFA)。如需詳細資訊，請參閱授權書和連線設施指派 (LOA-CFA)。

所有 LAG 皆具備一個屬性，決定了 LAG 本身要能夠運作，該 LAG 中必須保持運作的最少連線數目。預設情況下，新的 LAG 都是將此屬性設為 0。您可以更新 LAG 將其指定成另一數值，這樣做意味著一旦運作中連線數目低於此閾值時，整個 LAG 便無法運作。此屬性可用於防止過度使用剩餘的連線。

LAG 中的所有連線皆以主動/主動模式運作。

> **Note**
>
> 當您建立 LAG 或將更多連線與 LAG 建立關聯時，我們可能無法保證特定 AWS Direct Connect 端點上有足夠的可用連接埠。

主題

- 的 MACsec 考量 AWS Direct Connect
- 在 AWS Direct Connect 端點建立 LAG
- 在 AWS Direct Connect 端點檢視 LAG 詳細資訊
- 在 AWS Direct Connect 端點更新 LAG
- 將連線與 AWS Direct Connect 端點的 LAG 建立關聯
- 在 AWS Direct Connect 端點取消與 LAG 的連線關聯
- 將 MACsec CKN/CAK 與 AWS Direct Connect 端點 LAG 建立關聯
- 移除 MACsec 私密金鑰與 AWS Direct Connect 端點 LAG 之間的關聯
- 刪除 AWS Direct Connect 端點 LAG

的 MACsec 考量 AWS Direct Connect

設定 LAG 上的 MACsec 時，請考慮下列事項：

- 當您從現有連線建立 LAG 時，我們會取消所有 MACsec 金鑰與連線的關聯。然後我們會將連線新增至 LAG，並將 LAG MACsec 金鑰與連線產生關聯。
- 當您將現有連線與 LAG 產生關聯時，目前與 LAG 相關聯的 MACsec 金鑰會與連線產生關聯。因此，我們會取消 MACsec 金鑰與連線的關聯，將連線新增至 LAG，然後將 LAG MACsec 金鑰與連線產生關聯。

在 AWS Direct Connect 端點建立 LAG

您可以透過佈建新的連線或彙整現有的連線，建立 LAG。

如果使用新的連線會導致您超出區域的整體連線限制，您就不能以這種方式建立 LAG。

若要從現有連線建立 LAG，連線必須位於相同的 AWS 裝置（在相同的 AWS Direct Connect 端點終止）。它們還必須使用相同的頻寬。如果移除連線會導致原始 LAG 低於其設定的運作中連線數目下限，您即無法從現有的 LAG 遷移連線。

> **Important**
>
> 對於現有的連線，在建立 LAG 期間，對 的連線 AWS 會中斷。

使用新的連線建立 LAG

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2. 在導覽窗格中，選擇 LAGs。
3. 選擇 Create LAG (建立 LAG)。
4. 在 Lag creation type (延遲建立類型) 之下，選擇 Request new connections (申請新連線)，並提供下列資訊：
   - LAG Name (LAG 名稱)：LAG 的名稱。
   - Location (據點)：選取 LAG 所在據點。
   - Port speed (連接埠速度)：連線的連接埠速度。
   - Number of new connections (新連線數)：要建立的新連線數。當連接埠速度為 1G 或 10G 時，您最多可以有四個連線；當連接埠速度為 100 Gbps 或 400 Gbps 時，您最多可以有兩個連線。
   - (選用) 設定連線的 MAC Security (MACsec)。在其他設定之下，選取「要求具 MACsec 能力的連接埠」。

MACsec 僅能用於專用連線。

- (選用) 新增或移除標籤。

  [新增標籤] 選擇 Add tag (新增標籤)，並執行下列動作：

  - 對於 Key (金鑰)，輸入金鑰名稱。
  - 在值中，進入索引鍵值。

  [移除標籤] 在標籤旁邊，選擇 移除標籤。

5. 選擇 Create LAG (建立 LAG)。

從現有的連線建立 LAG

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2. 在導覽窗格中，選擇 LAGs。
3. 選擇 Create LAG (建立 LAG)。
4. 在 Lag creation type (延遲建立類型) 之下，選擇 Use existing connections (使用現有連線)，並提供下列資訊：

   - LAG Name (LAG 名稱)：LAG 的名稱。
   - 既有連線：要用於 LAG 的 Direct Connect 連線。
   - (選用) 新連線數：要建立的新連線數。連接埠速度為 1G 或 10G 時，您最多可以有四個連線，連接埠速度為 100 Gbps 或 400 Gbps 時，則最多可以有兩個連線。
   - Minimum links (最少鏈路數)：LAG 本身要能夠運作，必須保持運作的最少連線數目。若您未指定此數值，系統將指派預設值 0。
5. (選用) 新增或移除標籤。

   [新增標籤] 選擇 Add tag (新增標籤)，並執行下列動作：

   - 對於 Key (金鑰)，輸入金鑰名稱。
   - 在值中，進入索引鍵值。

   [移除標籤] 在標籤旁邊，選擇 移除標籤。
6. 選擇 Create LAG (建立 LAG)。

使用命令列或 API 建立 LAG

- create-lag (AWS CLI)
- CreateLag (AWS Direct Connect API)

使用命令列或 API 描述 LAG

- describe-lags (AWS CLI)
- DescribeLags (AWS Direct Connect API)

使用命令列或 API 下載 LOA-CFA

- describe-loa (AWS CLI)
- DescribeLoa (AWS Direct Connect API)

建立 LAG 之後，您可以將其與連線產生關聯或取消兩者間的關聯。如需詳細資訊，請參閱將連線與 LAG 建立關聯，以及取消與 LAG 的連線關聯。

在 AWS Direct Connect 端點檢視 LAG 詳細資訊

建立 LAG 之後，您可以使用 AWS Direct Connect 主控台或使用命令列或 API 檢視其詳細資訊。

檢視您的 LAG 相關資訊

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2. 在導覽窗格中，選擇 LAGs。
3. 選取 LAG，然後選擇 View details (檢視詳細資訊)。
4. 您可以檢視 LAG 的相關資訊，包括其 ID，以及連線終止所在的 AWS Direct Connect 端點。

使用命令列或 API 檢視有關 LAG 的資訊

- describe-lags (AWS CLI)
- DescribeLags (AWS Direct Connect API)

在 AWS Direct Connect 端點更新 LAG

您可以使用 AWS Direct Connect 主控台或使用命令列或 API 更新下列連結彙總群組 (LAG) 屬性：

- LAG 的名稱。
- LAG 本身要能夠運作，必須至少維持最少連線數量的值。
- LAG 的 MACsec 加密模式。

  MACsec 僅能用於專用連線。

  AWS 會將此值指派給屬於 LAG 一部分的每個連線。

  有效值為：

  - `should_encrypt`
  - `must_encrypt`

    當您將加密模式設定為此值時，連線會在加密關閉時一併關閉。
  - `no_encrypt`
- 此標籤。

> **Note**
>
> 如果您調整運作中連線數目下限的閾值，請確保新值不會導致 LAG 因低於該閾值而無法運作。

更新 LAG

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2. 在導覽窗格中，選擇 LAGs。
3. 選取 LAG，然後選擇編輯。
4. 修改 LAG

   [變更名稱] 針對 LAG Name (LAG 名稱)，輸入新的 LAG 名稱。

   [調整連線數目下限] 針對最少連結數，輸入運作中連線數目下限。

[新增標籤] 選擇新增標籤，並執行下列動作：

- 對於 Key (金鑰)，輸入金鑰名稱。
- 在值中，進入索引鍵值。

[移除標籤] 在標籤旁邊，選擇 移除標籤。

5. 選擇 Edit LAG (編輯 LAG)。

使用命令列或 API 更新 LAG

- update-lag (AWS CLI)
- UpdateLag (AWS Direct Connect API)

將連線與 AWS Direct Connect 端點的 LAG 建立關聯

您可以使用 AWS Direct Connect 主控台或使用命令列或 API 將現有連線與 LAG 建立關聯。連線可以是獨立的連線，或者屬於另一個 LAG。連線必須位於相同的 AWS 裝置上，且必須使用與 LAG 相同的頻寬。若連線已與另一個 LAG 相關聯，而移除該連線將導致原始 LAG 低於其運作中連線數目下限閾值，您即無法重新關聯該連線。

連線與 LAG 產生關聯時，其虛擬介面會自動重新關聯到該 LAG。

> **Important**
>
> 透過連線的 連線 AWS 會在關聯期間中斷。

將連線與 LAG 產生關聯

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2. 在導覽窗格中，選擇 LAGs。
3. 選取 LAG，然後選擇檢視詳細資訊。
4. 在 Connections (連線) 之下，選擇 Associate connection (與連線產生關聯)。
5. 針對 Connection (連線)，選擇要用於 LAG 的 Direct Connect 連線。
6. 選擇 Associate Connection (與連線產生關聯)。

使用命令列或 API 關聯連線

- associate-connection-with-lag (AWS CLI)
- AssociateConnectionWithLag (AWS Direct Connect API)

在 AWS Direct Connect 端點取消與 LAG 的連線關聯

使用 AWS Direct Connect 主控台或使用命令列或 API 將連線與 LAG 取消關聯，將連線轉換為獨立連線。如果取消連線的關聯會導致 LAG 低於其運作中連線數目下限閾值，您即無法執行此操作。

取消連線與 LAG 的關聯並不會自動取消關聯任何虛擬介面。

> **Important**
>
> 您的 連線 AWS 會在取消關聯期間中斷。

取消連線與 LAG 的關聯

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2. 從左側窗格選擇 LAG。
3. 選取 LAG，然後選擇檢視詳細資訊。
4. 在 Connections (連線) 之下，從可用的連線清單中選取連線，然後選擇 Disassociate (取消關聯)。
5. 在確認對話方塊中，選擇 Disassociate (取消關聯)。

使用命令列或 API 取消連線的關聯

- disassociate-connection-from-lag (AWS CLI)
- DisassociateConnectionFromLag (AWS Direct Connect API)

將 MACsec CKN/CAK 與 AWS Direct Connect 端點 LAG 建立關聯

建立支援 MACsec 的 LAG 之後，您可以使用 AWS Direct Connect 主控台或使用命令列或 API 將 CKN/CAK 與連線建立關聯。

> **Note**
>
> 將 MACsec 私密金鑰與 LAG 建立關聯之後，即無法修改。如果您需要修改金鑰，請取消金鑰與連線的關聯，然後將新金鑰與連線產生關聯。如需移除關聯的資訊，請參閱 the section called “移除 MACsec 私密金鑰和 LAG 之間的關聯”。

將 MACsec 金鑰與 LAG 產生關聯

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2. 在導覽窗格中，選擇 LAGs。
3. 選取 LAG，然後選擇 View details (檢視詳細資訊)。
4. 選擇關聯金鑰。
5. 輸入 MACsec 金鑰。

   [使用 CAK/CKN 對] 選擇「金鑰對」，然後執行下列動作：

   - 對於連線關聯金鑰 (CAK)，輸入 CAK。
   - 對於連線關聯金鑰名稱 (CKN)，請輸入 CKN。

   [使用密碼] 選擇「現有的 Secret Manager 密碼，然後對於密碼選取 MACsec 私密金鑰。
6. 選擇關聯金鑰。

使用命令列或 API 將 MACsec 金鑰與 LAG 建立關聯

- associate-mac-sec-key (AWS CLI)
- AssociateMacSecKey (AWS Direct Connect API)

移除 MACsec 私密金鑰與 AWS Direct Connect 端點 LAG 之間的關聯

您可以使用 AWS Direct Connect 主控台或使用命令列或 API 來移除 LAG 與 MACsec 金鑰之間的關聯。

移除 LAG 和 MACsec 金鑰之間的關聯

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2. 在導覽窗格中，選擇 LAGs。
3. 選取 LAG，然後選擇 View details (檢視詳細資訊)。
4. 選取要移除的 MACsec 密碼，然後選擇「取消關聯金鑰]。
5. 在確認對話方塊中，輸入取消關聯，然後選擇取消關聯。

使用命令列或 API 移除 LAG 與 MACsec 金鑰之間的關聯

- disassociate-mac-sec-key (AWS CLI)
- DisassociateMacSecKey (AWS Direct Connect API)

刪除 AWS Direct Connect 端點 LAG

如果您不再需要 LAG，可將其刪除。若 LAG 有相關聯的虛擬介面，您就無法將其刪除。您必須先刪除虛擬介面，或將其與不同的 LAG 或連線建立關聯。刪除 LAG 並不會刪除該 LAG 中的連線；您必須自行刪除這些連線。如需詳細資訊，請參閱刪除一個連線。

您可以使用 AWS Direct Connect 主控台或使用命令列或 API 刪除 LAG。

刪除 LAG

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2. 在導覽窗格中，選擇 LAGs。
3. 選取 LAG，然後選擇刪除。
4. 在確認對話方塊中，選擇 Delete (刪除)。

使用命令列或 API 刪除 LAG

- delete-lag (AWS CLI)
- DeleteLag (AWS Direct Connect API)

AWS Direct Connect 閘道

您可以使用 Amazon VPC 主控台或 來使用 AWS Direct Connect 閘道 AWS CLI。

- Direct Connect 閘道

  使用 Direct Connect 閘道，您可以將 Direct Connect 閘道與傳輸閘道與多個 VPCs、虛擬私有閘道建立關聯，或者如果您使用 AWS Cloud WAN，則與 Cloud WAN 核心網路建立關聯。
- 虛擬私有閘道關聯

  使用虛擬私有閘道，您可以透過私有虛擬介面將 Direct Connect 閘道與位於相同或不同區域的任何帳戶中VPCs 建立關聯。
- 傳輸閘道關聯

  使用 Direct Connect 閘道，透過傳輸虛擬介面將 Direct Connect 連線連接到連接到傳輸閘道VPCs VPNs。
- 雲端 WAN 核心網路關聯

  使用 Direct Connect 閘道將 Direct Connect 閘道與 AWS Network Manager 核心網路建立關聯。
- 允許字首互動

  使用允許的字首與傳輸閘道和虛擬私有閘道互動。

主題

- AWS Direct Connect 閘道
- AWS Direct Connect 虛擬私有閘道關聯
- AWS Direct Connect 閘道和傳輸閘道關聯
- AWS Direct Connect 閘道和 AWS Cloud WAN 核心網路關聯
- AWS Direct Connect 閘道允許的字首互動

AWS Direct Connect 閘道

使用 AWS Direct Connect 閘道來連接 VPCs。您可以將 AWS Direct Connect 閘道與下列任何項目建立關聯：

- 您在相同區域擁有多個 VPC 時的傳輸閘道

- 虛擬私有閘道
- AWS Cloud WAN 核心網路

您也可以使用虛擬私有閘道來擴充本機區域。此組態可讓與本機區域相關聯的 VPC 連線到 Direct Connect 閘道。Direct Connect 閘道可連線至區域中的 Direct Connect 位置。內部部署資料中心有 Direct Connect 連至 Direct Connect 的位置。如需詳細資訊，請參閱 Amazon VPC 使用者指南中的使用 Direct Connect 閘道存取本機區域。

Direct Connect 閘道是一項全球可用的資源。您可以使用 Direct Connect 閘道連線到全域的任何區域。這包括 AWS GovCloud (US)，但不包括 AWS 中國區域。Direct Connect 閘道是 Direct Connect 的虛擬元件，旨在充當一組分佈的 BGP 路由反射器。因為它在資料流量路徑之外運作，因此可避免建立單一故障點或引入特定相依性 AWS 區域。高可用性本質上內建於其設計中，無需多個 Direct Connect 閘道。

使用 Direct Connect 搭配目前繞過父可用區域的 VPC 的客戶將無法遷移其 Direct Connect 連線或虛擬介面。

以下描述的案例是您可以使用 Direct Connect 閘道的案例。

Direct Connect 閘道不允許位於相同 Direct Connect 閘道上的閘道關聯彼此傳送流量 (例如，虛擬私有閘道到另一個虛擬私有閘道)。2021 年 11 月實施的此規則出現例外情況，當超級網路跨兩個或多個 VPC 公告時，這些 VPC 的附接虛擬私有閘道 (VGW) 與相同的 Direct Connect 閘道相關聯，且在相同的虛擬介面上。在此情況下，VPC 可透過 Direct Connect 端點互相通訊。例如，如果您公告超級網路 (例如，10.0.0.0/8 或 0.0.0.0/0) 與附接至 Direct Connect 閘道的 VPC 重疊 (例如，10.0.0.0/24 和 10.0.1.0/24)，而且在相同的虛擬介面上，VPC 就可以從您的內部部署網路互相通訊。

如果您想要封鎖 Direct Connect 閘道內的 VPC-to-VPC 通訊，請執行下列動作：

1. 在 VPC 中的執行個體和其他資源上設定安全群組，以封鎖 VPC 之間的流量，同時將其用作 VPC 中預設安全群組的一部分。
2. 避免從內部部署網路公告與 VPC 重疊的超級網路。您可以改為從內部部署網路公告不與 VPC 重疊的更具體路由。
3. 為您要連線到內部部署網路的每個 VPC 佈建單一 Direct Connect 閘道，而不是針對多個 VPC 使用相同的 Direct Connect 閘道。例如，不要為開發和生產 VPC 使用單一 Direct Connect 閘道，而是為各個 VPC 使用單獨的 Direct Connect 閘道。

Direct Connect 閘道不會防止流量從一個閘道關聯傳回閘道關聯本身 (例如，當您有內部部署超級網路路由，且其中包含來自閘道關聯的字首)。如果您的組態具有多個 VPC 連線至與相同 Direct Connect

閘道相關聯的傳輸閘道，則 VPC 可以進行通訊。為了防止 VPCs通訊，請將路由表與已設定黑洞選項的 VPC 附件建立關聯。

主題

- 案例
- 建立 AWS Direct Connect 閘道
- 從虛擬私有閘道遷移至 AWS Direct Connect 閘道
- 刪除 AWS Direct Connect 閘道

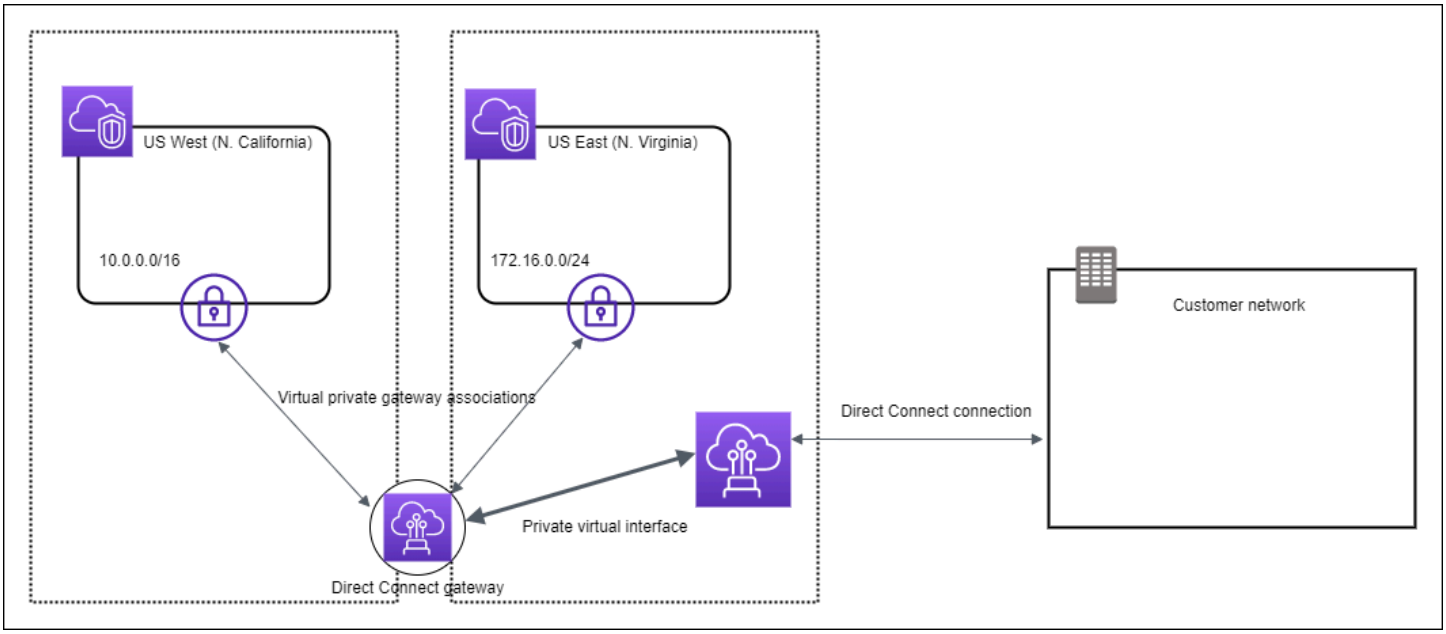
案例

以下僅說明使用 Direct Connect 閘道的幾個案例。

案例：虛擬私有閘道關聯

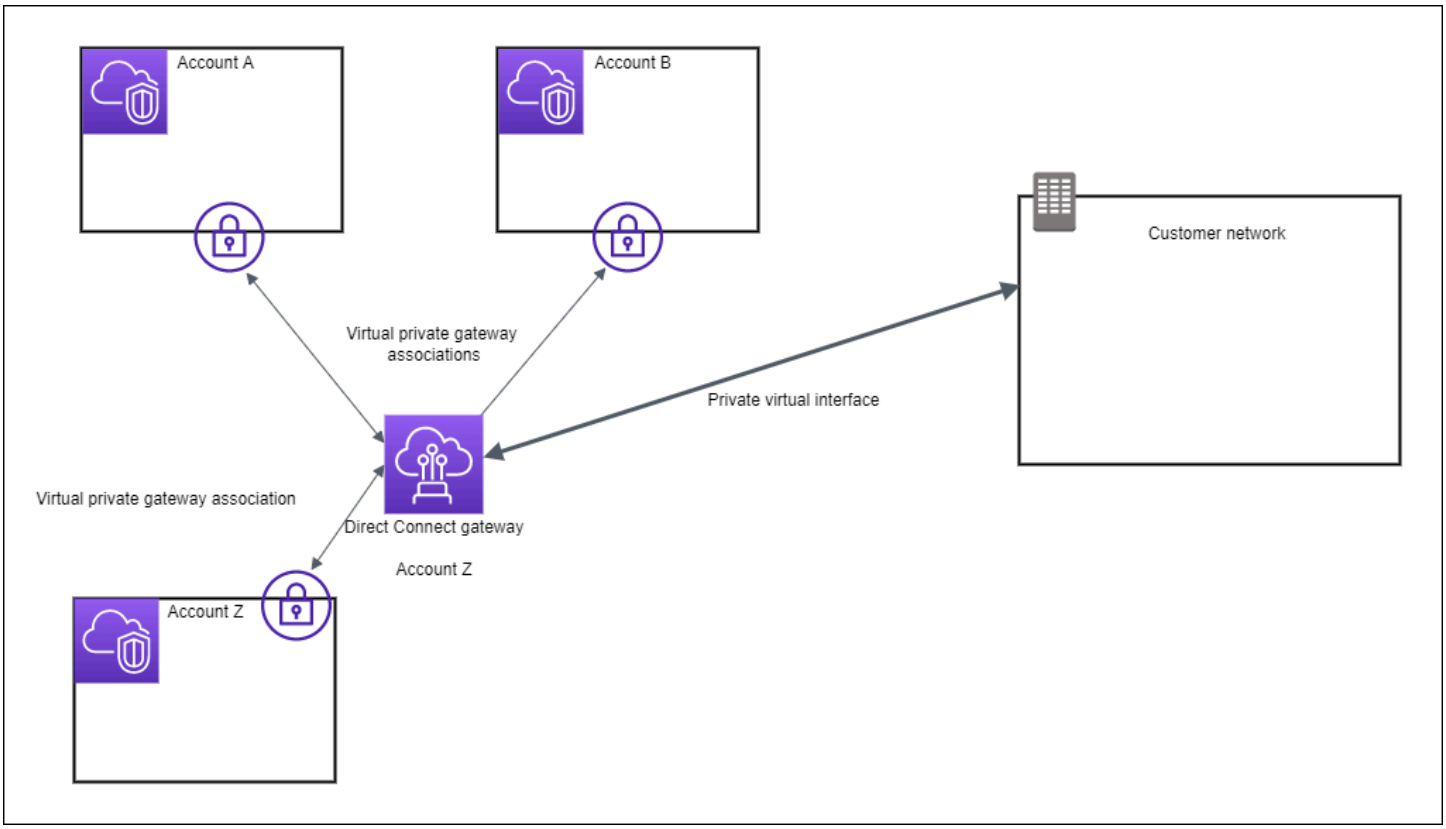
在下圖中，Direct Connect 閘道可讓您使用美國東部 (維吉尼亞北部) 區域的 AWS Direct Connect 連線，在美國東部 (維吉尼亞北部) 和美國西部 (加利佛尼亞北部) 區域中存取帳戶中的 VPC。

每個 VPC 都有一個虛擬私有閘道，該閘道使用虛擬私有閘道關聯連線至 Direct Connect 閘道。Direct Connect 閘道使用私有虛擬介面來連線至 AWS Direct Connect 位置。從該位置到客戶資料中心有一個 AWS Direct Connect 連線。



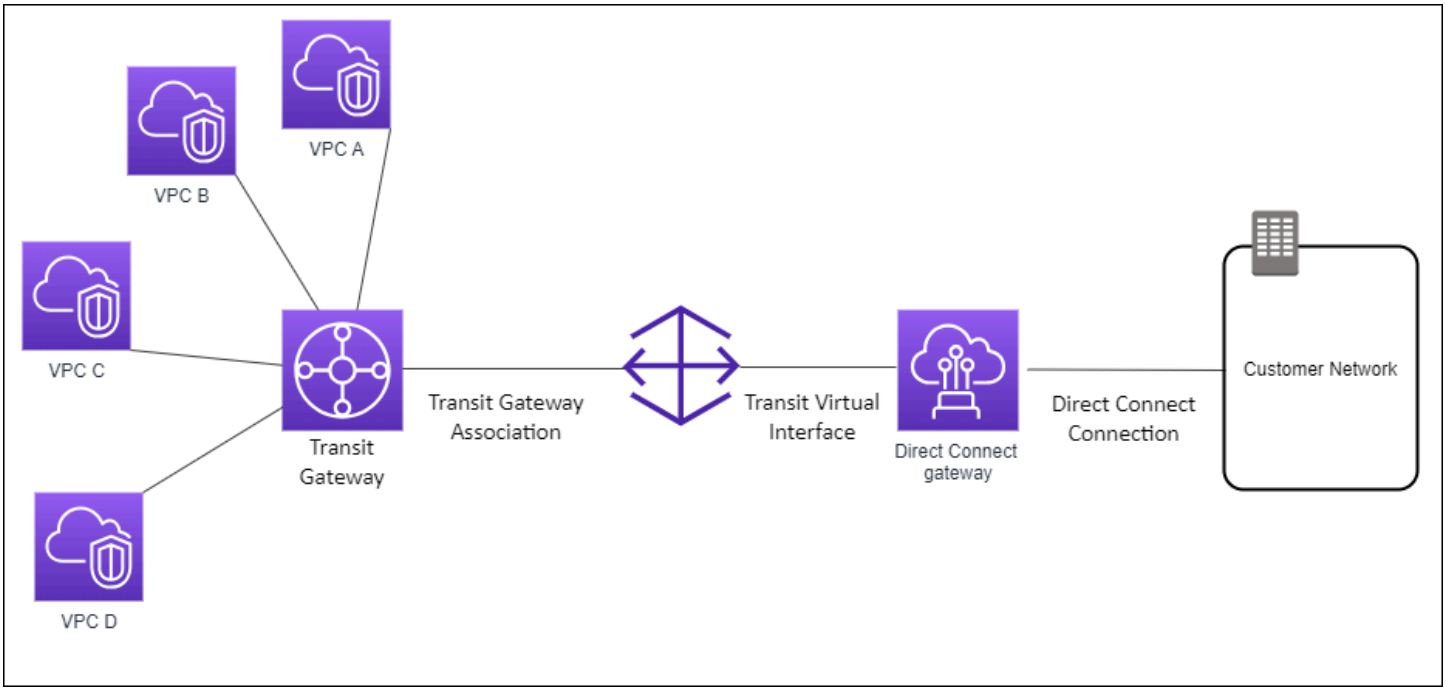
案例：跨帳戶的虛擬私有閘道關聯

考慮這個案例的 Direct Connect 閘道擁有者 (帳戶 Z) 擁有 Direct Connect 閘道。帳戶 A 和帳戶 B 都想使用 Direct Connect 閘道。帳戶 A 和帳戶 B 各自將關聯提案傳送至帳戶 Z。帳戶 Z 會接受關聯提案，並可選擇性更新允許來自帳戶 A 的虛擬私有閘道或帳戶 B 的虛擬私有閘道的字首。在帳戶 Z 接受提案之後，帳戶 A 和帳戶 B 可以將來自其虛擬私有閘道的流量路由傳送到 Direct Connect 閘道。帳戶 Z 還擁有客戶的路由，因為帳戶 Z 擁有閘道。



案例：傳輸閘道關聯

下圖說明 Direct Connect 閘道如何讓您建立單一連線到您的 Direct Connect 連線，以供您所有 VPC 使用。



此解決方案包含下列元件：

- 具有 VPC 連接的傳輸閘道。
- Direct Connect 閘道。
- Direct Connect 閘道和傳輸閘道之間的關聯。
- 連接至 Direct Connect 閘道的傳輸虛擬介面。

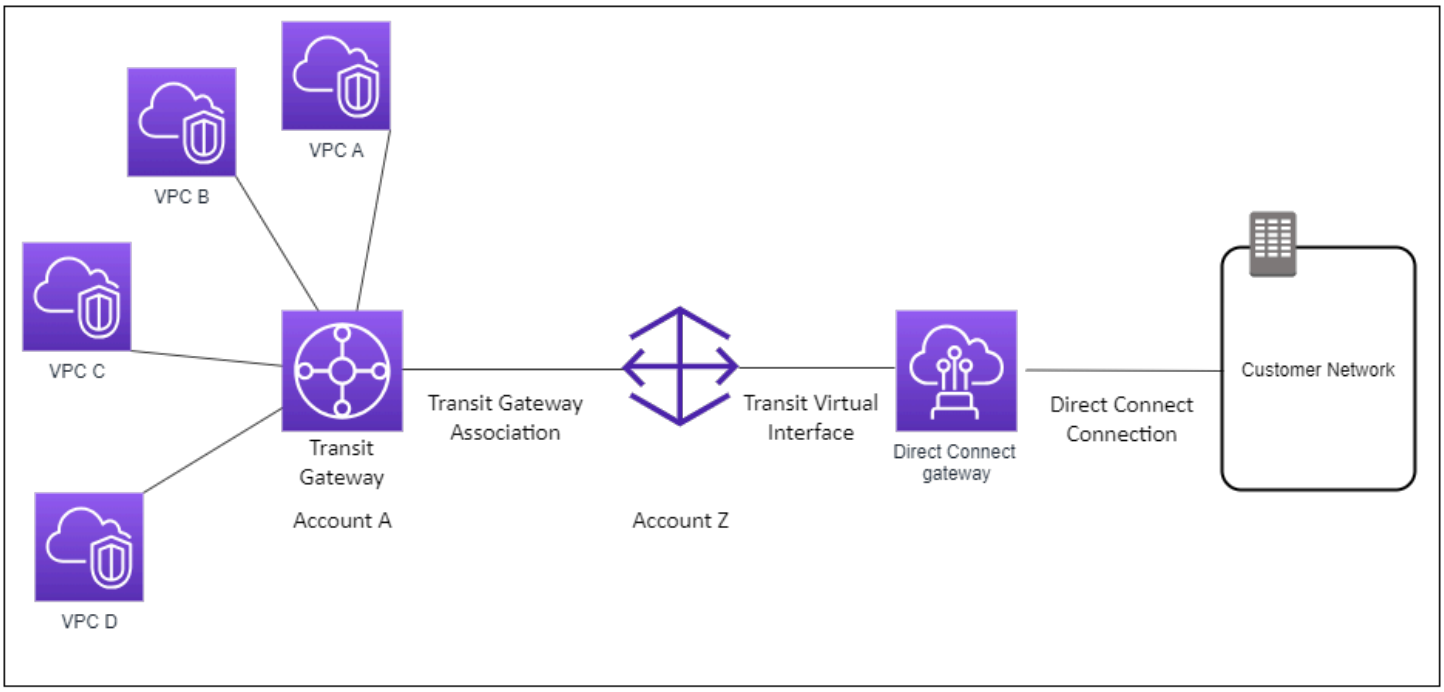
此組態具有以下好處。您可以：

- 管理相同區域中多個 VPC 或 VPN 的單一連線。
- 將字首從現場部署公告到現場部署 AWS ，以及從現場部署公告 AWS 到現場部署。

如需設定傳輸閘道的相關資訊，請參閱《Amazon VPC 傳輸閘道指南》中的使用傳輸閘道。

案例：跨帳戶傳輸閘道關聯

考慮這個案例的 Direct Connect 閘道擁有者 (帳戶 Z) 擁有 Direct Connect 閘道。帳戶 A 擁有傳輸閘道且想要使用 Direct Connect 閘道。帳戶 Z 接受關聯提案且可選擇更新允許來自帳戶 A 的傳輸閘道字首。帳戶 Z 接受提案後，連接到傳輸閘道的 VPC 可以從傳輸閘道路由流量到 Direct Connect 閘道。帳戶 Z 還擁有客戶的路由，因為帳戶 Z 擁有閘道。



建立 AWS Direct Connect 閘道

您可以使用主控台或使用命令列或 API， AWS Direct Connect 在任何支援的區域中建立 Direct Connect 閘道。

建立 Direct Connect 閘道

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2. 在導覽窗格中，選擇 Direct Connect Gateways (Direct Connect 閘道)。
3. 選擇 Create Direct Connect Gateway (建立 Direct Connect 閘道)。
4. 指定以下資訊，然後選擇 Create Direct Connect gateway (建立 Direct Connect 閘道)。

   - Name (名稱)：輸入一個名稱以協助您識別此 Direct Connect 閘道。
   - Amazon side ASN (Amazon 端 ASN)：指定 BGP 工作階段的 Amazon 端 ASN。此 ASN 必須在 64,512 到 65,534 的範圍或 4,200,000,000 到 4,294,967,294 的範圍。

   > **Note**
   >
   > 如果您想要建立 Direct Connect 閘道以搭配 AWS Cloud WAN 核心網路使用。ASN 不得與核心網路的 ASN 位於相同的範圍內。

使用命令列或 API 建立 Direct Connect 閘道

- create-direct-connect-gateway (AWS CLI)
- CreateDirectConnectGateway (AWS Direct Connect API)

從虛擬私有閘道遷移至 AWS Direct Connect 閘道

您可以將連接到虛擬介面的虛擬私有閘道遷移至 Direct Connect 閘道。

如果您將 Direct Connect 與目前略過父可用區域的 VPCs 搭配使用，您將無法遷移 Direct Connect 連線或虛擬介面。

下列步驟說明將虛擬私有閘道遷移至 Direct Connect 閘道所需的步驟。

遷移至 Direct Connect 閘道

1. 建立一個 Direct Connect 閘道。

   如果 Direct Connect 閘道尚不存在，您將需要建立它。如需建立 Direct Connect 閘道的步驟，請參閱 建立 Direct Connect 閘道。
2. 建立 Direct Connect 閘道的虛擬介面。

   遷移需要虛擬介面。如果界面不存在，您將需要建立它。如需建立虛擬介面的步驟，請參閱虛擬介面。
3. 將虛擬私有閘道與 Direct Connect 閘道建立關聯。

   Direct Connect 閘道和虛擬私有閘道都需要建立關聯。如需建立關聯的步驟，請參閱 關聯或取消關聯虛擬私有閘道。
4. 刪除與虛擬私有閘道關聯的虛擬介面。如需詳細資訊，請參閱刪除虛擬介面。

刪除 AWS Direct Connect 閘道

如果您不再需要某個 Direct Connect 閘道，可以將其刪除。您必須先取消關聯所有相關聯的虛擬私有閘道並刪除已連接的私有虛擬介面。取消關聯任何相關聯的虛擬私有閘道並刪除任何連接的虛擬私有介面後，您可以使用 AWS Direct Connect 主控台或使用命令列或 API 刪除 Direct Connect 閘道。

- 如需取消關聯惡意私有閘道的步驟，請參閱 關聯或取消關聯虛擬私有閘道。
- 如需刪除虛擬介面的步驟，請參閱刪除虛擬介面。

刪除 Direct Connect 閘道

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2. 在導覽窗格中，選擇 Direct Connect Gateways (Direct Connect 閘道)。
3. 選取閘道，然後選擇 Delete (刪除)。

使用命令列或 API 刪除 Direct Connect 閘道

- delete-direct-connect-gateway (AWS CLI)
- DeleteDirectConnectGateway (AWS Direct Connect API)

AWS Direct Connect 虛擬私有閘道關聯

您可以使用 AWS Direct Connect 閘道，透過私有虛擬介面將連線連接到 AWS Direct Connect 位於相同或不同區域中的任何帳戶中的一或多個 VPCs。您為 Direct Connect 閘道與 VPC 的虛擬私有閘道建立關聯。然後，您可以為 Direct Connect 閘道的 AWS Direct Connect 連線建立私有虛擬介面。您可以將多個私有虛擬介面連接到您的 Direct Connect 閘道。

下列規則適用於虛擬私有閘道關聯：

- 在您將虛擬閘道與 Direct Connect 閘道建立關聯之前，請勿啟用路由傳播。如果您在與閘道建立關聯之前啟用路由傳播，則路由可能傳播不正確。
- 建立與使用 Direct Connect 閘道均設有限制。如需詳細資訊，請參閱Direct Connect 配額。
- 當 Direct Connect 閘道已與傳輸閘道關聯時，您就無法將 Direct Connect 閘道附加到虛擬私有閘道。
- 透過 Direct Connect 閘道所連接的 VPC 不得有重疊的 CIDR 區塊。如果您為 Direct Connect 閘道的某個相關聯 VPC 新增 IPv4 CIDR 區塊，請確定該 CIDR 區塊並未與任何其他相關聯 VPC 的現有 CIDR 區塊重疊。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的將 IPv4 CIDR 區塊新增至 VPC。
- 您無法建立公有虛擬介面連往 Direct Connect 閘道。
- Direct Connect 閘道僅支援連接的私有虛擬介面與關聯虛擬私有閘道之間的通訊，並且可以啟用通往其他私有閘道的虛擬私有閘道。以下流量不受支援：
  - 與單一 Direct Connect 閘道相關聯的各 VPC 之間的直接通訊。這包括透過內部部署網路，以單一 Direct Connect 閘道在不同 VPC 之間來回傳送的流量。

  - 連接至單一 Direct Connect 閘道的各虛擬介面之間的直接通訊。
  - 連接至單一 Direct Connect 閘道的虛擬介面與同一個 Direct Connect 閘道之相關聯虛擬私有閘道上的 VPN 連接之間的直接通訊。
- 您無法將同一虛擬私有閘道與多個 Direct Connect 閘道產生關聯，且無法將同一私有虛擬介面連接至多個 Direct Connect 閘道。
- 透過 Direct Connect 閘道相關聯的虛擬私有閘道必須連接至 VPC。
- 虛擬私有閘道關聯提案會在其建立後 7 天過期。
- 已接受的虛擬私有閘道提案或已遭刪除的虛擬私有閘道提案，則會持續保留 3 天。
- 虛擬私有閘道可以與 Direct Connect 閘道建立關聯，也可以連接至虛擬介面。
- 從 VPC 分離虛擬私有閘道也會取消虛擬私有閘道與 Direct Connect 閘道的關聯。
- 如果您打算將虛擬私有閘道用於 Direct Connect 閘道及動態 VPN 連線，請將虛擬私有閘道上的 ASN 設定為需用於 VPN 連接的值。否則，請將虛擬私有閘道上的 ASN 設定為任何許可值。Direct Connect 閘道透過指派給它的 ASN 公告所有連線的 VPC。

若要僅將 AWS Direct Connect 連線連接到相同區域中的 VPC，您可以建立 Direct Connect 閘道。或者，您可以建立一個私有虛擬介面，並將它連接到 VPC 的虛擬私有閘道。如需詳細資訊，請參閱建立私有虛擬介面。及 VPN CloudHub。

若要在其他帳戶中使用與 VPC 的 AWS Direct Connect 連線，您可以為該帳戶建立託管私有虛擬介面。另一帳戶的擁有者接受該託管虛擬介面時，可選擇將之連接至其帳戶中的虛擬私有閘道或 Direct Connect 閘道。如需詳細資訊，請參閱虛擬介面和託管虛擬介面。

主題

- 建立 AWS Direct Connect 虛擬私有閘道
- 關聯或取消關聯 AWS Direct Connect 虛擬私有閘道
- 建立 AWS Direct Connect 閘道的私有虛擬介面
- 跨帳戶建立 AWS Direct Connect 虛擬私有閘道的關聯

建立 AWS Direct Connect 虛擬私有閘道

虛擬私有閘道必須連接至您要連接的 VPC。您可以使用主控台或使用命令列或 API AWS Direct Connect 來建立虛擬私有閘道，並將其連接至 VPC。

> **Note**
>
> 如果您打算將虛擬私有閘道用於 Direct Connect 閘道及動態 VPN 連線，請將虛擬私有閘道上的 ASN 設定為需用於 VPN 連接的值。否則，請將虛擬私有閘道上的 ASN 設定為任何許可值。Direct Connect 閘道透過指派給它的 ASN 公告所有連線的 VPC。

在您建立虛擬私有閘道之後，您必須予以連接至您的 VPC。

建立虛擬私有閘道並予以連接至您的 VPC

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2. 在導覽窗格中，選擇虛擬私有閘道，然後選擇建立虛擬私有閘道。
3. (選用) 輸入您虛擬私有閘道的名稱。執行此作業會使用 Name 做為鍵，以及您指定的值來建立標籤。
4. 針對 ASN，保留預設選項以使用預設的 Amazon ASN。否則，請選擇 Custom ASN (自訂 ASN) 並輸入值。對於 16 位元的 ASN，此值的範圍必須為 64512 到 65534。對於 32 位元的 ASN，此值的範圍必須為 4200000000 到 4294967294。
5. 選擇 Create Virtual Private Gateway (建立虛擬私有閘道)。
6. 選取您建立的虛擬私有閘道，然後選擇 Actions (動作)、Attach to VPC (連接到 VPC)。
7. 從清單選取您的 VPC，然後選擇 Yes, Attach (是，連接)。

使用命令列或 API 建立虛擬私有閘道

- CreateVpnGateway (Amazon EC2 查詢 API)
- create-vpn-gateway (AWS CLI)
- New-EC2VpnGateway (AWS Tools for Windows PowerShell)

使用命令列或 API 將虛擬私有閘道連接到 VPC

- AttachVpnGateway (Amazon EC2 查詢 API)
- attach-vpn-gateway (AWS CLI)
- Add-EC2VpnGateway (AWS Tools for Windows PowerShell)

關聯或取消關聯 AWS Direct Connect 虛擬私有閘道

您可以使用 AWS Direct Connect 主控台或使用命令列或 API 來關聯或取消虛擬私有閘道和 Direct Connect 閘道的關聯。虛擬私有閘道的帳戶擁有者會執行這些操作。

關聯虛擬私有閘道

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2. 在導覽窗格中，選擇 Direct Connect 閘道，然後選擇 Direct Connect 閘道。
3. 請選擇檢視詳細資料。
4. 選擇閘道關聯，然後選擇建立閘道關聯。
5. 對於 Gateways (閘道)，選擇要建立關聯的虛擬私有閘道，然後選擇 Associate gateway (建立閘道關聯)。

您可藉由選擇 Gateway associations (閘道關聯)，檢視與 Direct Connect 閘道相關聯的所有虛擬私有閘道。

取消虛擬私有閘道的關聯

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2. 在導覽窗格中，選擇 Direct Connect Gateways (Direct Connect 閘道)，然後選取 Direct Connect 閘道。
3. 請選擇檢視詳細資料。
4. 選擇 Gateway associations (閘道關聯)，然後選擇虛擬私有閘道。
5. 選擇取消關聯。

使用命令列或 API 關聯虛擬私有閘道

- create-direct-connect-gateway-association (AWS CLI)
- CreateDirectConnectGatewayAssociation (AWS Direct Connect API)

使用命令列或 API 檢視與 Direct Connect 閘道相關聯的虛擬私有閘道

- describe-direct-connect-gateway-associations (AWS CLI)

- DescribeDirectConnectGatewayAssociations (AWS Direct Connect API)

使用命令列或 API 取消虛擬私有閘道的關聯

- delete-direct-connect-gateway-association (AWS CLI)
- DeleteDirectConnectGatewayAssociation (AWS Direct Connect API)

建立 AWS Direct Connect 閘道的私有虛擬介面

若要將 AWS Direct Connect 連線連線至遠端 VPC，您必須為連線建立私有虛擬介面。指定要連接的 Direct Connect 閘道。您可以使用 AWS Direct Connect 主控台或使用命令列或 API 來建立私有虛擬介面。

> **Note**
>
> 如果您接受了某個私有託管虛擬介面，則可將其與您帳戶中的 Direct Connect 閘道產生關聯。如需詳細資訊，請參閱接受託管虛擬介面。

將私有虛擬介面佈建於 Direct Connect 閘道

1. 開啟 AWS Direct Connect主控台，網址為 https://console.aws.amazon.com/directconnect/v2/home：//。
2. 在導覽窗格中，選擇 Virtual Interfaces (虛擬介面)。
3. 選擇建立虛擬介面。
4. 在虛擬介面類型之下，選擇「私有」。
5. 在公有虛擬介面設定之下，執行下列動作：

   a. 針對虛擬介面名稱，輸入虛擬介面的名稱。
   b. 針對連線，選擇要用於此介面的 Direct Connect 連線。
   c. 對於虛擬介面擁有者， AWS 如果虛擬介面適用於您的帳戶，請選擇我的 AWS 帳戶。
   d. 對於 Direct Connect gateway (Direct Connect 閘道)，選擇 Direct Connect 閘道。
   e. 針對 VLAN，為您的虛擬區域網路 (VLAN) 輸入 ID 號碼。
   f. 針對 BGP ASN，為新的虛擬介面輸入您內部部署對等路由器的邊界閘道協定自治系統編號。

      有效值為 1 至 2147483647。

6. 在 Additional settings (其他設定) 之下，執行下列動作：

   a. 若要設定 IPv4 BGP 或 IPv6 對等，請執行下列動作：

      [IPv4] 若要設定 IPv4 BGP 對等，請選擇 IPv4，然後執行以下動作：

      - 若要自行指定這些 IP 地址，對於 Your router peer ip (您的路由器對等 IP)，輸入 Amazon 應傳送流量至該處的目的地 IPv4 CIDR 地址。
      - 對於 Amazon 路由器對等 IP，輸入用以傳送流量至 AWS的 IPv4 CIDR 地址。

      > **Important**
      >
      > 設定 AWS Direct Connect 虛擬介面時，您可以使用 RFC 1918 指定自己的 IP 地址、使用其他定址機制，或選擇從 RFC 3927 169.254.0.0/16 IPv4 連結本機範圍配置的 AWS 指派 IPv4/29 CIDR 地址，以進行point-to-point連線。這些point-to-point連線應僅用於客戶閘道路由器和 Direct Connect 端點之間的 eBGP 互連。針對 VPC 流量或通道用途，例如 AWS Site-to-Site私有 IP VPN 或 Transit Gateway Connect，AWS 建議使用客戶閘道路由器上的迴路或 LAN 界面作為來源或目的地地址，而非point-to-point連線。
      >
      > - 如需有關 RFC 1918 的詳細資訊，請參閱私有網路的地址配置。
      > - 如需有關 RFC 3927 的詳細資訊，請參閱 IPv4 Link-Local 地址的動態組態。

      [IPv6] 若要設定 IPv6 BGP 對等，請選擇 IPv6。對等 IPv6 地址是自動從 Amazon 的 IPv6 地址集區所指派。您無法指定自訂 IPv6 地址。

   b. 若要將最大傳輸單位 (MTU) 從 1500 (預設) 變更至 9001 (巨型框架)，請選取巨型 MTU (MTU 大小 9001)。

   c. (選用) 在啟用 SiteLink 之下，選擇啟用以啟用 Direct Connect 連接點之間的直接連線。

   d. (選用) 新增或移除標籤。

      [新增標籤] 選擇 Add tag (新增標籤)，並執行下列動作：

      - 對於 Key (金鑰)，輸入金鑰名稱。
      - 在值中，進入索引鍵值。

      [移除標籤] 在標籤旁邊，選擇 移除標籤。

7. 選擇建立虛擬介面。

建立虛擬介面之後，您可為您的裝置下載路由器組態。如需詳細資訊，請參閱下載路由組態檔案。

使用命令列或 API 建立私有虛擬介面

- create-private-virtual-interface (AWS CLI)
- CreatePrivateVirtualInterface (AWS Direct Connect API)

使用命令列或 API 檢視連接至 Direct Connect 閘道的虛擬介面

- describe-direct-connect-gateway-attachments (AWS CLI)
- DescribeDirectConnectGatewayAttachments (AWS Direct Connect API)

跨帳戶建立 AWS Direct Connect 虛擬私有閘道的關聯

您可以將 Direct Connect 閘道與任何 AWS 帳戶擁有的虛擬私有閘道建立關聯。Direct Connect 閘道可以是現有閘道，或者您也可以建立新閘道。虛擬私有閘道的擁有者會建立關聯提案，而 Direct Connect 閘道的擁有者則必須接受此關聯提案。

關聯提案可以包含允許來自虛擬私有閘道的字首。Direct Connect 閘道的擁有者可以選擇性覆寫關聯提案中任何要求的字首。

允許字首

當您將虛擬私有閘道與 Direct Connect 閘道建立關聯時，您會指定要向 Direct Connect 閘道公告的 Amazon VPC 字首清單。字首清單可做為篩選條件，允許向 Direct Connect 閘道宣告相同的 CIDR 或較小的 CIDR。您必須將 Allowed prefixes (允許字首) 設定為與 VPC CIDR 相同或更廣的範圍，因為我們在虛擬私有閘道上佈建整個 VPC CIDR。

考慮 VPC CIDR 是 10.0.0.0/16 的案例。您可以將 Allowed prefixes (允許字首) 設定為 10.0.0.0/16 (VPC CIDR 值) 或 10.0.0.0/15 (比 VPC CIDR 更廣的值)。

透過 Direct Connect 公告的網路字首內的任何虛擬界面只會傳播到跨 區域的傳輸閘道，而不是在同一區域內。如需允許字首如何與虛擬私有閘道和傳輸閘道互動的詳細資訊，請參閱 允許字首互動。

AWS Direct Connect 閘道和傳輸閘道關聯

您可以使用 AWS Direct Connect 閘道，透過傳輸虛擬介面將 Direct Connect 連線連接到連接到傳輸閘道VPCs VPNs。您將 Direct Connect 閘道與傳輸閘道建立關聯。然後，為 Direct Connect 閘道的 AWS Direct Connect 連線建立傳輸虛擬介面。

下列規則適用於傳輸閘道關聯：

- 當 Direct Connect 閘道已與虛擬私有閘道相關聯或已附加至私有虛擬介面時，您就無法將 Direct Connect 閘道附加至傳輸閘道。
- 建立與使用 Direct Connect 閘道均設有限制。如需詳細資訊，請參閱Direct Connect 配額。
- Direct Connect 閘道支援連接傳輸虛擬介面與相關聯傳輸閘道之間的通訊。
- 如果您連接到位於不同區域的多個傳輸閘道，請為每個傳輸閘道使用唯一的 ASN。
- 使用/30範圍的任何point-to-point連線地址，例如192.168.0.0/30，不會傳播到傳輸閘道。

跨帳戶建立傳輸閘道關聯

您可以將現有的 Direct Connect 閘道或新的 Direct Connect 閘道與任何 AWS 帳戶擁有的傳輸閘道建立關聯。傳輸閘道的擁有者會建立關聯提案，而 Direct Connect 閘道的擁有者則必須接受此關聯提案。

關聯提案可以包含允許來自傳輸閘道的字首。Direct Connect 閘道的擁有者可以選擇性覆寫關聯提案中任何要求的字首。

允許字首

對於傳輸閘道關聯，您可在 Direct Connect 閘道上佈建允許字首的清單。即使連接到傳輸閘道VPCs 沒有指派 CIDRs，此清單也會用來將流量從內部部署路由 AWS 到傳輸閘道。Direct Connect 閘道允許字首清單中的字首，都來自 Direct Connect 閘道，並公告到現場部署網路。如需允許字首如何與傳輸閘道和虛擬私有閘道互動的詳細資訊，請參閱 允許字首互動。

主題

- 建立或取消 AWS Direct Connect 與傳輸閘道的關聯
- 建立傳輸虛擬介面到 AWS Direct Connect 閘道
- 建立傳輸閘道和 AWS Direct Connect 關聯提案
- 接受或拒絕傳輸閘道和 AWS Direct Connect 關聯提案
- 更新傳輸閘道和 AWS Direct Connect 關聯的允許字首
- 刪除傳輸閘道和 AWS Direct Connect 關聯提案

建立或取消 AWS Direct Connect 與傳輸閘道的關聯

使用 AWS Direct Connect 主控台或使用命令列或 API 來關聯或取消傳輸閘道的關聯。

建立傳輸閘道的關聯

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2. 在導覽窗格中，選擇 Direct Connect Gateways (Direct Connect 閘道)，然後選取 Direct Connect 閘道。
3. 請選擇檢視詳細資料。
4. 選擇 Gateway associations (閘道關聯)，然後選擇 Associate gateway (建立閘道關聯)。
5. 對於閘道，選擇要產生關聯的傳輸閘道。
6. 在允許的字首中，輸入 Direct Connect 閘道向內部部署資料中心公告的字首 (以逗號分隔或換行)。如需允許字首的詳細資訊，請參閱 允許字首互動。
7. 選擇「關聯閘道」

您可藉由選擇 Gateway associations (閘道關聯)，檢視與 Direct Connect 閘道相關聯的所有閘道。

取消傳輸閘道的關聯

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2. 在導覽窗格中，選擇 Direct Connect gateways (Direct Connect 閘道)，然後選取 Direct Connect 閘道。
3. 請選擇檢視詳細資料。
4. 選擇 Gateway associations (閘道關聯)，然後選擇傳輸閘道。
5. 選擇取消關聯。

更新傳輸閘道允許的字首

您可以新增或移除傳輸閘道的字首。

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2. 在導覽窗格中，選擇 Direct Connect 閘道，然後選擇您要新增或移除允許字首的 Direct Connect 閘道。
3. 選擇「閘道關聯」標籤。
4. 選擇您要修改允許字首的閘道，然後選擇編輯。

5. 在允許的字首中，輸入 Direct Connect 閘道向內部部署資料中心公告的字首。對於多個字首，請用逗號分隔每個字首或在新的一行輸入每個字首。您新增的字首應與所有虛擬私有閘道的 Amazon VPC CIDR 相符。如需允許字首的詳細資訊，請參閱 允許字首互動。
6. 選擇 Edit association (編輯關聯)。

   在「閘道關聯」區段中，「狀態」會顯示為更新中。完成後，「狀態」會變更為「已關聯」。這可能需要幾分鐘或更長的時間才能完成。

使用命令列或 API 關聯傳輸閘道

- create-direct-connect-gateway-association (AWS CLI)
- CreateDirectConnectGatewayAssociation (AWS Direct Connect API)

使用命令列或 API 檢視與 Direct Connect 閘道關聯的傳輸閘道

- describe-direct-connect-gateway-associations (AWS CLI)
- DescribeDirectConnectGatewayAssociations (AWS Direct Connect API)

使用命令列或 API 中斷關聯傳輸閘道

- delete-direct-connect-gateway-association (AWS CLI)
- DeleteDirectConnectGatewayAssociation (AWS Direct Connect API)

使用命令列或 API 為傳輸閘道更新允許的字首

- update-direct-connect-gateway-association (AWS CLI)
- UpdateDirectConnectGatewayAssociation (AWS Direct Connect API)

建立傳輸虛擬介面到 AWS Direct Connect 閘道

若要將 AWS Direct Connect 連線連線至傳輸閘道，您必須為連線建立傳輸介面。指定要連接的 Direct Connect 閘道。您可以使用 AWS Direct Connect 主控台或使用命令列或 API。

> **Important**
>
> 如果您將傳輸閘道與一或多個 Direct Connect 閘道產生關聯，則傳輸閘道和 Direct Connect 閘道所使用的自治系統編號 (ASN) 必須不同。例如，如果您同時針對傳輸閘道和 Direct Connect 閘道使用預設 ASN 64512，則關聯要求會失敗。

將傳輸虛擬介面佈建於 Direct Connect 閘道

1. 在 httpsAWS Direct Connect：//https://console.aws.amazon.com/directconnect/v2/home。
2. 在導覽窗格中，選擇 Virtual Interfaces (虛擬介面)。
3. 選擇建立虛擬介面。
4. 在虛擬介面類型之下，針對類型選擇傳輸。
5. 在傳輸虛擬介面設定之下，執行下列動作：

   a. 針對虛擬介面名稱，輸入虛擬介面的名稱。

   b. 針對連線，選擇要用於此介面的 Direct Connect 連線。

   c. 對於虛擬介面擁有者， AWS 如果虛擬介面適用於您的帳戶，請選擇我的 AWS 帳戶。

   d. 對於 Direct Connect gateway (Direct Connect 閘道)，選擇 Direct Connect 閘道。

   e. 針對 VLAN，為您的虛擬區域網路 (VLAN) 輸入 ID 號碼。

   f. 針對 BGP ASN，為新的虛擬介面輸入您內部部署對等路由器的邊界閘道協定自治系統編號。

   有效值為 1 至 2147483647。
6. 在 Additional settings (其他設定) 之下，執行下列動作：

   a. 若要設定 IPv4 BGP 或 IPv6 對等，請執行下列動作：

   [IPv4] 若要設定 IPv4 BGP 對等，請選擇 IPv4，然後執行以下動作：

   - 若要自行指定這些 IP 地址，對於 Your router peer ip (您的路由器對等 IP)，輸入 Amazon 應傳送流量至該處的目的地 IPv4 CIDR 地址。
   - 對於 Amazon 路由器對等 IP，輸入用以傳送流量至 AWS的 IPv4 CIDR 地址。

   > **Important**
   >
   > 設定 AWS Direct Connect 虛擬介面時，您可以使用 RFC 1918 指定自己的 IP 地址、使用其他定址機制，或選擇從 RFC 3927 169.254.0.0/16 IPv4 連結本機範圍配

置的 AWS 指派 IPv4 /29 CIDR 地址point-to-point連線。這些point-to-point連線應僅用於客戶閘道路由器和 Direct Connect 端點之間的 eBGP 互連。針對 VPC 流量或通道用途，例如 AWS Site-to-Site私有 IP VPN 或 Transit Gateway Connect， AWS 建議使用客戶閘道路由器上的迴路或 LAN 界面作為來源或目的地地址，而非point-to-point連線。

- 如需有關 RFC 1918 的詳細資訊，請參閱私有網路的地址配置。
- 如需有關 RFC 3927 的詳細資訊，請參閱 IPv4 Link-Local 地址的動態組態。

[IPv6] 若要設定 IPv6 BGP 對等，請選擇 IPv6。對等 IPv6 地址是自動從 Amazon 的 IPv6 地址集區所指派。您無法指定自訂 IPv6 地址。

b. 若要將最大傳輸單位 (MTU) 從 1500 (預設) 變更至 8500 (巨型框架)，請選取 Jumbo MTU (MTU size 8500) (巨型 MTU (MTU 大小 8500))。

c. (選用) 在啟用 SiteLink 之下，選擇啟用以啟用 Direct Connect 連接點之間的直接連線。

d. (選用) 新增或移除標籤。

[新增標籤] 選擇 Add tag (新增標籤)，並執行下列動作：

- 對於 Key (金鑰)，輸入金鑰名稱。
- 在值中，進入索引鍵值。

[移除標籤] 在標籤旁邊，選擇 移除標籤。

7. 選擇建立虛擬介面。

建立虛擬介面之後，您可為您的裝置下載路由器組態。如需詳細資訊，請參閱下載路由組態檔案。

使用命令列或 API 建立傳輸虛擬介面

- create-transit-virtual-interface (AWS CLI)
- CreateTransitVirtualInterface (AWS Direct Connect API)

使用命令列或 API 檢視連接至 Direct Connect 閘道的虛擬介面

- describe-direct-connect-gateway-attachments (AWS CLI)
- DescribeDirectConnectGatewayAttachments (AWS Direct Connect API)

建立傳輸閘道和 AWS Direct Connect 關聯提案

如果您擁有傳輸閘道，則必須建立關聯提案。傳輸閘道必須連接到您 AWS 帳戶中的 VPC 或 VPN。Direct Connect 閘道的擁有者必須共用 Direct Connect 閘道 ID 及其 AWS 帳戶的 ID。在您建立提案之後，Direct Connect 閘道的擁有者必須接受該提案，您才能夠透過 AWS Direct Connect存取現場部署網路。您可以使用 AWS Direct Connect 主控台或使用命令列或 API 建立關聯提案。

建立關聯提案

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2. 在導覽窗格中，選擇傳輸閘道，接著選取傳輸閘道。
3. 請選擇檢視詳細資料。
4. 選擇 Direct Connect gateway associations (Direct Connect 閘道關聯) 然後選擇 Associate Direct Connect gateway (建立 Direct Connect 閘道關聯)。
5. 在 Association account type (關聯帳戶類型) 之下，針對 Account owner (帳戶擁有者) 選擇 Another account (另一個帳戶)。
6. 對於 Direct Connect 閘道擁有者，輸入擁有 Direct Connect 閘道的帳戶 ID。
7. 在 Association settings (關聯設定) 下，執行下列動作：
   a. 對於 Direct Connect gateway ID (Direct Connect 閘道 ID)，輸入 Direct Connect 閘道的 ID。
   b. 對於虛擬介面擁有者，輸入擁有關聯的虛擬介面之帳戶的 ID。
   c. (選用) 若要指定允許來自傳輸閘道的字首清單，請將字首新增至允許字首 (使用逗號分隔)，或在分開的行上輸入。
8. 選擇 Associate Direct Connect gateway (建立 Direct Connect 閘道關聯)。

使用命令列或 API 建立關聯提案

- create-direct-connect-gateway-association-proposal (AWS CLI)
- CreateDirectConnectGatewayAssociationProposal (AWS Direct Connect API)

接受或拒絕傳輸閘道和 AWS Direct Connect 關聯提案

如果您擁有 Direct Connect 閘道，則必須接受關聯提案，以便建立關聯。您也可以選擇拒絕關聯提案。您可以使用 AWS Direct Connect 主控台或使用命令列或 API 來接受或拒絕關聯提案。

接受關聯提案

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2. 在導覽窗格中，選擇 Direct Connect gateways (Direct Connect 閘道)。
3. 選取具有待定提案的 Direct Connect 閘道，然後選擇 View details (查看詳細資訊)。
4. 在 Pending proposals (待定提案) 標籤上，選取提案並選擇 Accept proposal (接受提案)。
5. ((選用) 若要指定允許來自傳輸閘道的字首清單，請將字首新增至允許字首 (使用逗號分隔)，或在分開的行上輸入。
6. 選擇 Accept proposal (接受提案)。

拒絕關聯提案

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2. 在導覽窗格中，選擇 Direct Connect gateways (Direct Connect 閘道)。
3. 選取具有待定提案的 Direct Connect 閘道，然後選擇 View details (查看詳細資訊)。
4. 在 Pending proposals (待定提案) 標籤上，選取傳輸閘道並選擇 Reject proposal (拒絕提案)。
5. 在 Reject proposal (拒絕提案) 對話方塊中，輸入 Delete 並選擇 Reject proposal (拒絕提案)。

使用命令列或 API 檢視關聯提案

- describe-direct-connect-gateway-association-proposals (AWS CLI)
- DescribeDirectConnectGatewayAssociationProposals (AWS Direct Connect API)

使用命令列或 API 接受關聯提案

- accept-direct-connect-gateway-association-proposal (AWS CLI)
- AcceptDirectConnectGatewayAssociationProposal (AWS Direct Connect API)

使用命令列或 API 拒絕關聯提案

- delete-direct-connect-gateway-association-proposal (AWS CLI)
- DeleteDirectConnectGatewayAssociationProposal (AWS Direct Connect API)

更新傳輸閘道和 AWS Direct Connect 關聯的允許字首

您可以使用 AWS Direct Connect 主控台或使用命令列或 API，更新透過 Direct Connect 閘道從傳輸閘道允許的字首。若要使用 AWS Direct Connect 主控台更新傳輸閘道和 Direct Connect 關聯的允許字首，

- 如果您是傳輸閘道的擁有者。您需要為該 Direct Connect 閘道建立新的關聯提案，指定要允許的字首。如需建立新關聯提案的步驟，請參閱建立傳輸閘道關聯提案。
- 如果您是 Direct Connect 閘道的擁有者，您可以在接受關聯提案時更新允許的字首，或更新現有關聯允許的字首。如需在接受關聯時更新允許字首的步驟，請參閱 接受或拒絕傳輸閘道關聯提案。

使用命令列或 API 更新現有關聯的允許字首

- update-direct-connect-gateway-association (AWS CLI)
- UpdateDirectConnectGatewayAssociation (AWS Direct Connect API)

刪除傳輸閘道和 AWS Direct Connect 關聯提案

傳輸閘道的擁有者可以刪除仍待接受的 Direct Connect 閘道關聯提案。接受關聯提案之後，您便無法將其刪除，但是您可以取消傳輸閘道與 Direct Connect 閘道的關聯。如需詳細資訊，請參閱建立傳輸閘道關聯提案。

您可以使用 AWS Direct Connect 主控台或使用命令列或 API 來刪除傳輸閘道和 Direct Connect 關聯提案。

刪除關聯提案

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2. 在導覽窗格中，選擇傳輸閘道，接著選取傳輸閘道。
3. 請選擇檢視詳細資料。
4. 選擇 Pending gateway associations (待定閘道關聯)，選取關聯並選擇 Delete association (刪除關聯)。
5. 在 Delete association proposal (刪除關聯提案) 對話方塊中，輸入Delete (刪除) 並選擇 Delete (刪除)。

使用命令列或 API 刪除待定關聯提案

- delete-direct-connect-gateway-association-proposal (AWS CLI)
- DeleteDirectConnectGatewayAssociationProposal (AWS Direct Connect API)

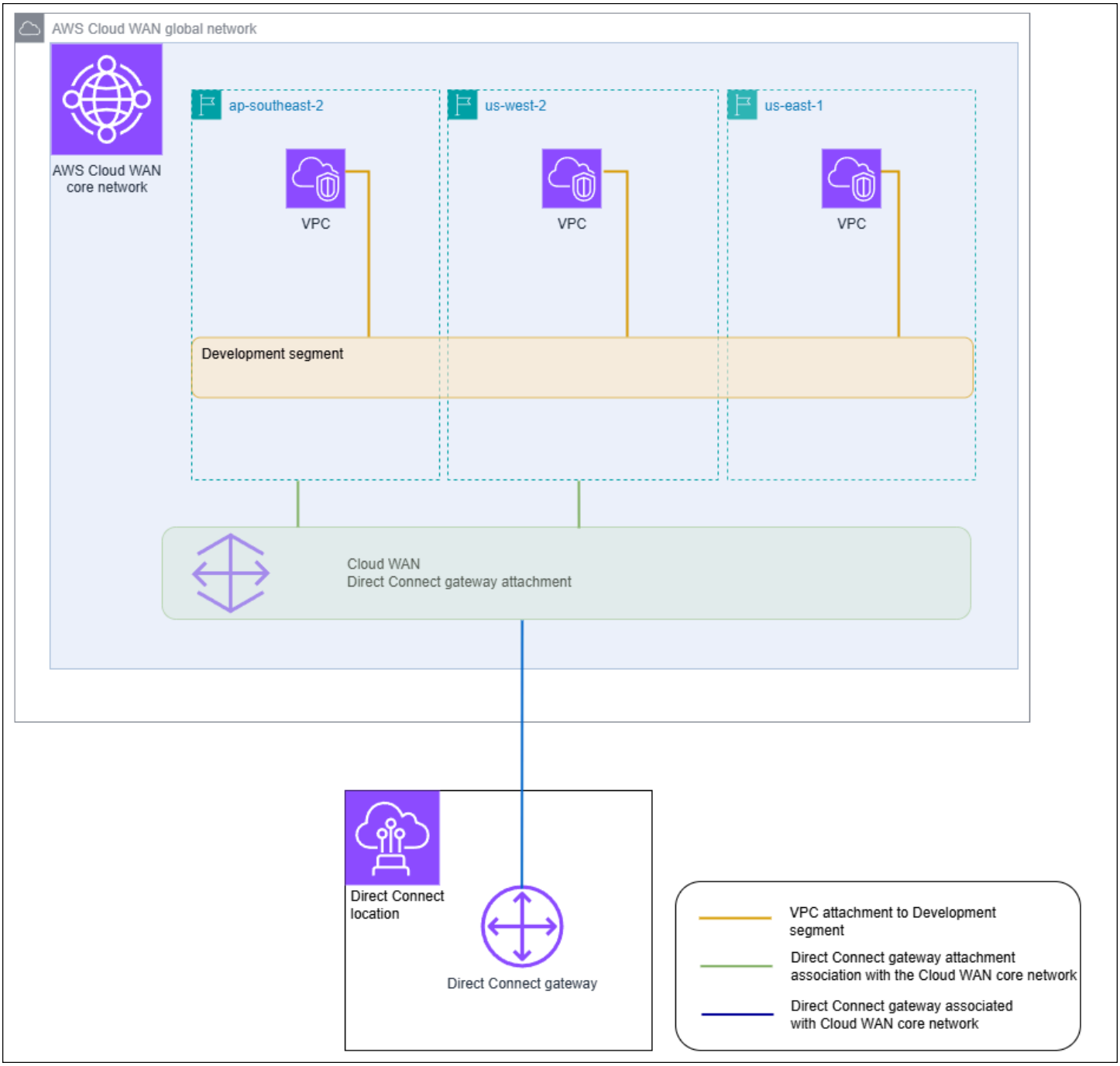
AWS Direct Connect 閘道和 AWS Cloud WAN 核心網路關聯

使用 AWS Cloud WAN 中的 Direct Connect 連接類型，將 AWS Direct Connect 閘道與 Cloud WAN 核心網路建立關聯。此直接關聯會使用最短的可用路徑，在核心網路的所選節點與 Direct Connect 連線之間路由流量

Direct Connect 閘道連接類型支援 BGP （邊界閘道通訊協定），可在核心網路和內部部署位置之間自動傳播路由資訊。Direct Connect 附件也支援標準 Cloud WAN 功能，例如中央政策型管理、標籤型附件自動化，以及進階安全組態的分割。

> **Note**
>
> 核心網路與 Direct Connect 閘道之間的關聯會從 Network Manager 中的 Cloud WAN Console 建立、刪除和管理。搭配 Cloud WAN 使用 Direct Connect 閘道時，Direct Connect 主控台和 APIs 和 CLI 會反映關聯，但無法用來修改關聯。不過，您可以使用 Direct Connect API 或命令列來驗證是否建立關聯。

下列範例顯示 Cloud WAN 全域網路，在 Cloud WAN 核心網路中具有三個區域。每個區域都有自己的 VPC 連接到這三個區域共用的核心網路開發區段。使用 Cloud WAN 時，會使用 Direct Connect 閘道在 Cloud WAN 內建立 Direct Connect 閘道連接，而該閘道是使用 Direct Connect 建立。附件與三個區域中的兩個相關聯：ap-southeast-2 和 us-west-2，並允許存取開發客群。即使 us-east-1 共用相同的開發客群，Direct Connect 閘道連接也不會與該區域共用，因此無法使用。



主題

- 先決條件
- 考量事項
- Direct Connect 閘道與 Cloud WAN 核心網路的關聯
- 驗證與 AWS Cloud WAN 核心網路的 AWS Direct Connect 閘道關聯

先決條件

與 Cloud WAN 核心網路的 Direct Connect 閘道關聯需要下列項目：

- 現有的 Direct Connect 閘道。如需建立 Direct Connect 閘道的步驟，請參閱建立 Direct Connect 閘道。
- AWS Cloud WAN 核心網路。如需有關 Cloud WAN 的資訊，請參閱 AWS Cloud WAN 使用者指南。

考量事項

下列限制適用於與 Cloud WAN 核心網路的 Direct Connect 閘道關聯：

- Direct Connect 閘道可以與單一 Cloud WAN 核心網路和該核心網路的單一區段建立關聯。建立關聯後，該閘道就無法與 AWS 區域中的其他資源建立關聯。如果您取消閘道與核心網路的關聯，則可以將該閘道用於其他關聯類型。
- Cloud WAN Direct Connect 閘道連接使用傳輸虛擬介面類型進行連線。
- Cloud WAN 連接不支援允許的字首清單。核心網路區段中的所有字首都會公告到與該區段相關聯的 Direct Connect 閘道。
- 可以從內部部署公告到 AWS 透過傳輸虛擬界面公告的最大字首配額與從 Cloud WAN 核心網路公告到內部部署字首的配額不同。與雲端 WAN 關聯搭配使用的其他 Direct Connect 資源配額也適用。請參閱 Direct Connect 配額。
- AS-PATH BGP 屬性會保留在核心網路、Direct Connect 閘道和虛擬介面。
- Direct Connect 閘道的 ASN 必須在針對 Cloud WAN 核心網路設定的 ASN 範圍之外。例如，如果您的核心網路的 ASN 範圍為 64512 - 65534，則 Direct Connect 閘道的 ASN 必須使用該範圍之外的 ASN。
- Cloud WAN 可能不支援使用 Direct Connect 連接類型進行傳輸的特定連接類型。如需連接到 Cloud WAN 核心網路的 Direct Connect 閘道附件的詳細資訊，請參閱AWS 《Cloud WAN 使用者指南》中的 AWS Cloud WAN 中的 Direct Connect 閘道附件。
- 搭配 Cloud WAN Direct Connect 閘道連接類型使用時，CloudWatch Network Monitor 支援延遲和封包遺失指標。不支援網路運作狀態指示器功能。如需詳細資訊，請參閱Amazon CloudWatch 《 使用者指南》中的使用 Amazon CloudWatch 網路監視器。

Direct Connect 閘道與 Cloud WAN 核心網路的關聯

使用 AWS Cloud WAN 主控台或 AWS Cloud WAN APIs 或命令列來執行將 Direct Connect 閘道與 Cloud WAN 核心網路建立關聯。

若要將現有的 Direct Connect 閘道與 Cloud WAN 核心網路建立關聯，請在 Cloud WAN 主控台中建立新的 Direct Connect 附件。建立 Direct Connect 附件之後，就會建立關聯。根據預設，在建立關聯時，您可以選擇預設值，以包含所選核心網路區段中的所有核心網路邊緣位置。或者，您可以指定個別節點。

如需連接到 Cloud WAN 核心網路的 Direct Connect 閘道附件的詳細資訊，請參閱AWS 《Cloud WAN 使用者指南》中的 AWS Cloud WAN 中的 Direct Connect 閘道附件。

驗證與 AWS Cloud WAN 核心網路的 AWS Direct Connect 閘道關聯

您可以使用 Direct Connect 主控台或 Direct Connect API 或命令列，驗證 Direct Connect 閘道與 Cloud WAN 核心網路的關聯。

使用主控台驗證與 Cloud WAN 核心網路的 Direct Connect 閘道關聯

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2. 在導覽窗格中選擇 Direct Connect 閘道。
3. 選擇您要檢視其關聯的 Direct Connect 閘道附件。
4. 選擇「閘道關聯」標籤。

   - ID 欄會顯示與 Direct Connect 閘道相關聯的核心網路 ID。
   - 狀態資料欄會顯示相關聯的 。
   - 關聯類型欄會顯示 Cloud WAN Core Network。

使用命令列或 API 驗證與 Cloud WAN 核心網路的 Direct Connect 閘道關聯

- DescribeDirectConnectGatewayAssociations (AWS Direct Connect API)
- describe-direct-connect-gateway-association (AWS CLI)

AWS Direct Connect 閘道允許的字首互動

瞭解允許的字首如何與傳輸閘道和虛擬私有閘道互動。如需詳細資訊，請參閱路由政策和 BGP 社群。

虛擬私有閘道關聯

字首清單 (IPv4 和 IPv6) 可做為篩選條件，允許向 Direct Connect 閘道公告相同的 CIDR 或較小範圍的 CIDR。您必須將字首設定為與 VPC CIDR 區塊相同或更寬的範圍。

> **Note**
>
> 允許的清單僅可作為篩選條件使用，並且只有相關聯的 VPC CIDR 會公告至客戶閘道。

考量以下情境：您的 VPC 使用 CIDR 10.0.0.0/16 並連接到虛擬私有閘道。

- 允許字首清單設定為 22.0.0.0/24 時，您不會收到任何路由，因為 22.0.0.0/24 與 10.0.0.0/16 不相同或更廣泛。
- 允許字首清單設定為 10.0.0.0/24 時，您不會收到任何路由，因為 10.0.0.0/24 與 10.0.0.0/16 不相同。
- 允許字首清單設定為 10.0.0.0/15 時，您會收到 10.0.0.0/16，因為 IP 地址比 10.0.0.0/16 更廣泛。

當您移除或新增允許的字首時，不使用該字首的流量不會受到影響。在更新期間，狀態會從 `associated` 變更為 `updating`。修改現有字首只會延遲使用該字首的流量。

傳輸閘道關聯

對於傳輸閘道關聯，您可在 Direct Connect 閘道上佈建允許字首的清單。即使附加到傳輸閘道的 VPC 沒有指派的 CIDR，清單仍可路由內部部署流量至傳輸閘道，或從 Direct Connect 閘道路由內部部署流量至傳輸閘道。根據閘道類型，允許的字首運作方式會有所不同：

- 對於傳輸閘道關聯，只有輸入的允許字首會公告到內部部署。這些會顯示為來自 Direct Connect 閘道 ASN。
- 對於虛擬私有閘道，輸入的允許字首會做為篩選條件，以允許使用相同或較小的 CIDR。

考量以下情景：您的 VPC 使用 CIDR 10.0.0.0/16 並連接到傳輸閘道。

- 允許字首清單設定為 22.0.0.0/24 時，您會在傳輸虛擬介面中透過 BGP 收到 22.0.0.0/24。您無法收到 10.0.0.0/16，因為我們直接佈建允許字首清單中的字首。
- 允許字首清單設定為 10.0.0.0/24 時，您會在傳輸虛擬介面中透過 BGP 收到 10.0.0.0/24。您無法收到 10.0.0.0/16，因為我們直接佈建允許字首清單中的字首。

- 允許字首清單設定為 10.0.0.0/8 時，您會在傳輸虛擬介面中透過 BGP 收到 10.0.0.0/8。

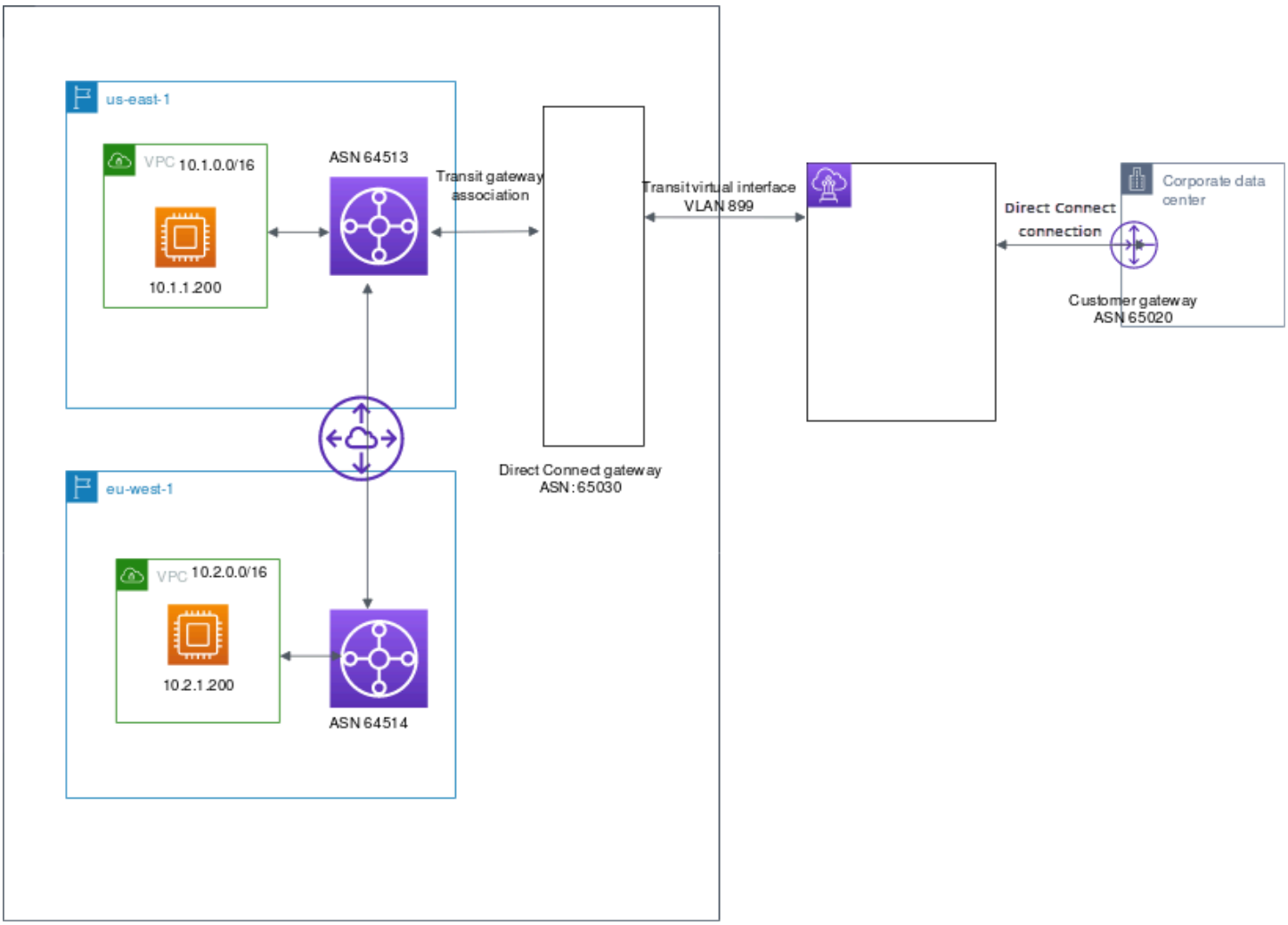
當多個傳輸閘道與 Direct Connect 閘道相關聯時，不允許使用允許的字首重疊。例如，如果您的傳輸閘道具有包含 10.1.0.0/16 的允許字首清單，而第二個傳輸閘道具有包含 10.2.0.0/16 和 0.0.0.0/0 的允許字首清單，則無法將第二個傳輸閘道的關聯設定為 0.0.0.0/0。由於 0.0.0.0/0 包含所有 IPv4 網路，因此，如果多個傳輸閘道與一個 Direct Connect 閘道相關聯，您就無法設定 0.0.0.0/0。傳回錯誤，指出允許的路由與 Direct Connect 閘道上的一或多個現有允許的路由重疊。

當您移除或新增允許的字首時，不使用該字首的流量不會受到影響。在更新期間，狀態會從 `associated` 變更為 `updating`。修改現有字首只會延遲使用該字首的流量。

範例：允許傳輸閘道組態中的字首

請考慮您在兩個不同 AWS 區域中有執行個體需要存取公司資料中心的組態。您可以為此組態使用下列資源：

- 每個區域中的傳輸閘道。
- 傳輸閘道對等連線。
- Direct Connect 閘道。
- 其中一個傳輸閘道 (us-east-1 中的閘道) 與 Direct Connect 閘道之間的傳輸閘道關聯。
- 來自內部部署位置和 AWS Direct Connect 位置的傳輸虛擬介面。



設定下列的資源選項。

- Direct Connect 閘道：將 ASN 設定為 65030。如需詳細資訊，請參閱建立 Direct Connect 閘道。
- 傳輸虛擬介面：將 VLAN 設定為 899，將 ASN 設定為 65020。如需詳細資訊，請參閱建立傳輸虛擬介面以連往 Direct Connect 閘道。
- 與傳輸閘道的 Direct Connect 閘道關聯：將允許的字首設定為 10.0.0.0/8。

  此 CIDR 區塊涵蓋兩個 VPC CIDR 區塊。如需詳細資訊，請參閱將傳輸閘道與 Direct Connect 建立關聯或取消關聯。。
- VPC 路由：若要將來自 10.2.0.0 VPC 的流量進行路由，請在 VPC 路由表 (具有目的地 0.0.0.0/0，傳輸閘道 ID 做為目標) 中建立路由。如需有關路由至傳輸閘道的詳細資訊，請參閱《Amazon VPC 使用者指南》中的傳輸閘道的路由。

標記 AWS Direct Connect 資源

標籤是資源擁有者指派給其 AWS Direct Connect 資源的標籤。每個標籤皆包含由您定義的一個金鑰與一個選用值。標籤可讓資源擁有者以不同的方式分類您的 AWS Direct Connect 資源，例如依用途或環境。當您有許多相同類型的資源時，這將會很有用，因為您可以依據先前指派的標籤，快速識別特定的資源。

例如，您在一個區域中有兩個 AWS Direct Connect 連線，分別位於不同的位置。連線 dxcon-11aa22bb 是服務生產流量的連線，與虛擬介面 dxvif-33cc44dd 相關聯。連線 dxcon-abcabcab 是備援 (備用) 連線，與虛擬介面 dxvif-12312312 相關聯。您可以選擇為這些連線和虛擬介面加上標籤，幫助您進行區分，如下所示：

資源 ID	標籤鍵	標籤值
dxcon-11aa22bb	用途	生產
	位置	阿姆斯特丹
dxvif-33cc44dd	用途	生產
dxcon-abcabcab	用途	備份
	位置	法蘭克福
dxvif-12312312	用途	備份

我們建議您為每種資源類型建立符合您需求的標籤金鑰。使用一致的標籤金鑰組可讓您更輕鬆管理您的資源。標籤對 沒有任何語意意義， AWS Direct Connect 並嚴格解譯為字元字串。此外，標籤不會自動指派給您的資源。您可以編輯標籤金鑰和值，並且可以隨時從資源移除標籤。您可以將標籤的值設為空白字串，但您無法將標籤的值設為 Null。若您將與現有標籤具有相同鍵的標籤新增到該資源，則新值會覆寫舊值。如果您刪除資源，也會刪除任何該資源的標籤。

您可以使用 AWS Direct Connect 主控台、 AWS Direct Connect API、 AWS Tools for Windows PowerShell、 或 AWS SDK AWS CLI來標記下列 AWS Direct Connect 資源。當您使用這些工具來管理標籤時，您必須指定資源的 Amazon Resource Name (ARN)。如需 ARN 的詳細資訊，請參閱《Amazon Web Services 一般參考》中的 Amazon Resource Name (ARN)。

資源	支援標籤	支援建立時加上標籤	支援標籤控制存取和資源分配	支援成本分配
連線	是	是	是	是
虛擬介面	是	是	是	否
鏈路彙整群組 (LAG)	是	是	是	是
互連	是	是	是	是
Direct Connect 閘道	是	是	是	否

標籤限制

標籤適用的規定和限制如下：

- 每個資源的標籤數上限：50
- 索引鍵長度上限：128 個 Unicode 字元
- 數值長度上限：265 個 Unicode 字元
- 標籤金鑰與值皆區分大小寫。
- 字aws:首會保留供 AWS 使用。如果標籤具有字首為 aws: 的標籤金鑰時，您無法編輯或刪除標籤的金鑰或值。具有字首為 aws: 的標籤金鑰的標籤，不會算在每個資源的標籤數限制內。
- 允許使用的字元包括可用 UTF-8 表示的英文字母、空格和數字，還有以下特殊字元：+ - = . _ : / @
- 只有資源擁有者可以新增或移除標籤。例如，如果存在託管連線，則合作夥伴無法新增、移除或檢視這些標籤。
- 成本分配標籤只支援連線、互連和 LAG。如需如何搭配成本管理使用標籤的詳細資訊，請參閱《AWS 帳單與成本管理 使用者指南》中的使用成本分配標籤。

透過 CLI 或 API 使用標籤

使用下列項目新增、更新、列出和刪除您資源的標籤。

任務	API	CLI
新增或覆寫一或多個標籤。	TagResource	tag-resource
刪除一或多個標籤。	UntagResource	untag-resource
說明一或多個標籤。	DescribeTags	describe-tags

範例

使用 tag-resource 命令，來標記連線 dxcon-11aa22bb。

```
aws directconnect tag-resource --resource-arn arn:aws:directconnect:us-
east-1:123456789012:dxcon/dxcon-11aa22bb --tags "key=Purpose,value=Production"
```

使用 describe-tags 命令來描述連線 dxcon-11aa22bb 標籤。

```
aws directconnect describe-tags --resource-arn arn:aws:directconnect:us-
east-1:123456789012:dxcon/dxcon-11aa22bb
```

使用 untag-resource 命令來移除連線 dxcon-11aa22bb 的標籤。

```
aws directconnect untag-resource --resource-arn arn:aws:directconnect:us-
east-1:123456789012:dxcon/dxcon-11aa22bb --tag-keys Purpose
```

中的安全性 AWS Direct Connect

的雲端安全性 AWS 是最高優先順序。身為 AWS 客戶，您可以從資料中心和網路架構中受益，該架構旨在滿足最安全敏感組織的需求。

安全性是 AWS 和 之間的共同責任。共同責任模型 將此描述為雲端的安全和雲端內的安全：

- 雲端的安全性 – AWS 負責保護在 AWS Cloud 中執行 AWS 服務的基礎設施。 AWS 也為您提供可安全使用的服務。在 AWS 合規計畫中，第三方稽核員會定期測試並驗證我們的安全功效。若要了解適用於 的合規計劃 AWS Direct Connect，請參閱AWS 合規計劃範圍內的服務。
- 雲端安全 – 您的責任取決於您使用 AWS 的服務。您也必須對其他因素負責，包括資料的機密性、您公司的要求和適用法律和法規。

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

主題

- 中的資料保護 AWS Direct Connect
- 適用於 Direct Connect 的 Identity and Access Management
- 在 中記錄和監控 AWS Direct Connect
- 的合規驗證 AWS Direct Connect
- 中的彈性 AWS Direct Connect
- 中的基礎設施安全性 AWS Direct Connect

中的資料保護 AWS Direct Connect

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

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

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用 設定 API 和使用者活動記錄 AWS CloudTrail。如需使用 CloudTrail 追蹤擷取 AWS 活動的資訊，請參閱AWS CloudTrail 《 使用者指南》中的使用 CloudTrail 追蹤。
- 使用 AWS 加密解決方案，以及其中的所有預設安全控制 AWS 服務。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果您在 AWS 透過命令列界面或 API 存取 時需要 FIPS 140-3 驗證的密碼編譯模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的更多相關資訊，請參閱聯邦資訊處理標準 (FIPS) 140-3。

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

如需關於資料保護的詳細資訊，請參閱 AWS 安全部落格上的 AWS 共同責任模型和歐盟《一般資料保護規範》(GDPR) 部落格文章。

主題

- AWS Direct Connect中的網際網路流量隱私權
- 傳輸中加密 AWS Direct Connect

AWS Direct Connect中的網際網路流量隱私權

服務和內部部署用戶端與應用程式之間的流量。

您的私有網路與 之間有兩個連線選項 AWS：

- 與 AWS Site-to-Site VPN的關聯。如需詳細資訊，請參閱基礎架構安全。
- 與 VPC 的關聯。如需詳細資訊，請參閱 虛擬私有閘道關聯 和 傳輸閘道關聯。

相同區域中 AWS 資源之間的流量

您有兩種連線選項：

- 與 AWS Site-to-Site VPN的關聯。如需詳細資訊，請參閱基礎架構安全。
- 與 VPC 的關聯。如需詳細資訊，請參閱 虛擬私有閘道關聯 和 傳輸閘道關聯。

傳輸中加密 AWS Direct Connect

AWS Direct Connect 根據預設， 不會加密傳輸中的流量。若要加密周遊的傳輸中資料 AWS Direct Connect，您必須使用該服務的傳輸加密選項。若要了解 EC2 執行個體流量加密，請參閱《Amazon EC2 使用者指南》中的傳輸中加密。

使用 AWS Direct Connect 和 AWS Site-to-Site VPN時，您可以將一或多個 AWS Direct Connect 專用網路連線與 Amazon VPC VPN 結合。這種組合可提供 IPsec 加密的私有連線，同時降低網路成本、增加頻寬輸送量，並提供比一般網際網路 VPN 連線更一致的網路體驗。如需詳細資訊，請參閱 Amazon VPC-to-Amazon VPC 連線選項。

MAC Security (MACsec) 是 IEEE 標準，提供資料機密性、資料完整性和資料來源真實性。您可以使用支援 MACsec 的 AWS Direct Connect 連線，將資料從公司資料中心加密到 AWS Direct Connect 位置。如需詳細資訊，請參閱MAC 安全性 (MACsec)。

適用於 Direct Connect 的 Identity and Access Management

AWS Identity and Access Management (IAM) 是一種 AWS 服務 ，可協助管理員安全地控制對 AWS 資源的存取。IAM 管理員會控制誰可經身分驗證 (已登入) 和授權 (具有許可) 來使用 Direct Connect 資源。IAM 是 AWS 服務 您可以免費使用的 。

主題

- 目標對象
- 使用身分驗證
- 使用政策管理存取權
- Direct Connect 搭配 IAM 的運作方式
- Direct Connect 的身分型政策範例
- 的服務連結角色 AWS Direct Connect
- AWS 的 受管政策 AWS Direct Connect
- 疑難排解 Direct Connect 身分和存取

目標對象

使用方式 AWS Identity and Access Management (IAM) 會有所不同，具體取決於您在 Direct Connect 中執行的工作。

服務使用者 – 如果您使用 Direct Connect 服務來執行任務，您的管理員會為您提供所需的憑證和許可。隨著您為了執行作業而使用的 Direct Connect 功能數量變多，您可能會需要額外的許可。了解存取許可的管理方式可協助您向管理員請求正確的許可。若您無法存取 Direct Connect 中的某項功能，請參閱 疑難排解 Direct Connect 身分和存取。

服務管理員 – 如果您負責公司內的 Direct Connect 資源，您可能具備 Direct Connect 的完整存取權。您的任務是判斷服務使用者應存取的 Direct Connect 功能及資源。接著，您必須將請求提交給您的 IAM 管理員，來變更您服務使用者的許可。檢閱此頁面上的資訊，了解 IAM 的基本概念。若要進一步瞭解貴公司可搭配 Direct Connect 使用 IAM 的方式，請參閱 Direct Connect 搭配 IAM 的運作方式。

IAM 管理員 – 如果您是 IAM 管理員，建議您掌握如何撰寫政策以管理 Direct Connect 存取權的詳細資訊。若要檢視您可以在 IAM 中使用的範例 Direct Connect 身分型政策，請參閱 Direct Connect 的身分型政策範例。

使用身分驗證

身分驗證是您 AWS 使用身分憑證登入 的方式。您必須以 AWS 帳戶根使用者身分、IAM 使用者身分或擔任 IAM 角色來驗證 （ 登入 AWS)。

您可以使用透過身分來源提供的憑證，以聯合身分 AWS 身分身分身分登入 。 AWS IAM Identity Center (IAM Identity Center) 使用者、您公司的單一登入身分驗證，以及您的 Google 或 Facebook 登入資料，都是聯合身分的範例。您以聯合身分登入時，您的管理員先前已設定使用 IAM 角色的聯合身分。當您使用聯合 AWS 身分存取 時，您會間接擔任角色。

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

如果您以 AWS 程式設計方式存取 ， AWS 會提供軟體開發套件 (SDK) 和命令列界面 (CLI)，以使用您的登入資料以密碼編譯方式簽署您的請求。如果您不使用 AWS 工具，則必須自行簽署請求。如需使用建議的方法自行簽署請求的詳細資訊，請參閱《IAM 使用者指南》中的適用於 API 請求的AWS Signature 第 4 版。

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

AWS 帳戶 根使用者

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

聯合身分

最佳實務是， 要求人類使用者，包括需要管理員存取權的使用者，使用臨時登入資料 AWS 服務 與身分提供者聯合來存取 。

聯合身分是來自您企業使用者目錄、Web 身分提供者、 AWS Directory Service、身分中心目錄或任何使用透過身分來源提供的憑證 AWS 服務 存取的使用者。當聯合身分存取時 AWS 帳戶，它們會擔任角色，而角色會提供臨時憑證。

對於集中式存取權管理，我們建議您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中建立使用者和群組，或者您可以連接並同步到您自己的身分來源中的一組使用者 AWS 帳戶 和群組，以便在所有 和應用程式中使用。如需 IAM Identity Center 的詳細資訊，請參閱 AWS IAM Identity Center 使用者指南中的什麼是 IAM Identity Center？。

IAM 使用者和群組

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

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

使用者與角色不同。使用者只會與單一人員或應用程式建立關聯，但角色的目的是在由任何需要它的人員取得。使用者擁有永久的長期憑證，但角色僅提供臨時憑證。如需更多資訊，請參閱《IAM 使用者指南》中的 IAM 使用者的使用案例。

IAM 角色

IAM 角色是 中具有特定許可 AWS 帳戶 的身分。它類似 IAM 使用者，但不與特定的人員相關聯。若要暫時在 中擔任 IAM 角色 AWS Management Console，您可以從使用者切換至 IAM 角色 （主控台）。

您可以透過呼叫 AWS CLI 或 AWS API 操作或使用自訂 URL 來擔任角色。如需使用角色的方法詳細資訊，請參閱《IAM 使用者指南》中的擔任角色的方法。

使用臨時憑證的 IAM 角色在下列情況中非常有用：

- 聯合身分使用者存取 — 如需向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並獲授予由角色定義的許可。如需有關聯合角色的相關資訊，請參閱《IAM 使用者指南》中的為第三方身分提供者 (聯合) 建立角色。如果您使用 IAM Identity Center，則需要設定許可集。為控制身分驗證後可以存取的內容，IAM Identity Center 將許可集與 IAM 中的角色相關聯。如需有關許可集的資訊，請參閱 AWS IAM Identity Center 使用者指南中的許可集。
- 暫時 IAM 使用者許可 – IAM 使用者或角色可以擔任 IAM 角色來暫時針對特定任務採用不同的許可。
- 跨帳戶存取權：您可以使用 IAM 角色，允許不同帳戶中的某人 (信任的主體) 存取您帳戶的資源。角色是授予跨帳戶存取權的主要方式。不過，對於某些 AWS 服務，您可以直接將政策連接到資源（而不是使用角色做為代理）。如需了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱《IAM 使用者指南》中的 IAM 中的跨帳戶資源存取。
- 跨服務存取 – 有些 AWS 服務 使用其他 中的功能 AWS 服務。例如，當您在服務中進行呼叫時，該服務通常會在 Amazon EC2 中執行應用程式或將物件儲存在 Amazon Simple Storage Service (Amazon S3) 中。服務可能會使用呼叫主體的許可、使用服務角色或使用服務連結角色來執行此作業。
  - 轉送存取工作階段 (FAS) – 當您使用 IAM 使用者或角色在 中執行動作時 AWS，您會被視為主體。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 使用呼叫 的委託人許可 AWS 服務，並結合 AWS 服務 請求向下游服務提出請求。只有當服務收到需要與其他 AWS 服務 或 資源互動才能完成的請求時，才會提出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的政策詳細資訊，請參閱《轉發存取工作階段》。
  - 服務角色 – 服務角色是服務擔任的 IAM 角色，可代表您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需詳細資訊，請參閱《IAM 使用者指南》中的建立角色以委派許可權給 AWS 服務。
  - 服務連結角色 – 服務連結角色是一種連結至 的服務角色。 AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會出現在您的 中 AWS 帳戶 ，並由服務擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。
- 在 Amazon EC2 上執行的應用程式 – 您可以使用 IAM 角色來管理在 EC2 執行個體上執行之應用程式的臨時登入資料，以及提出 AWS CLI 或 AWS API 請求。這是在 EC2 執行個體內儲存存取金鑰的較好方式。若要將 AWS 角色指派給 EC2 執行個體，並將其提供給其所有應用程式，您可以建立連接至執行個體的執行個體描述檔。執行個體設定檔包含該角色，並且可讓 EC2 執行個體上執行的

程式取得臨時憑證。如需詳細資訊，請參閱《IAM 使用者指南》中的使用 IAM 角色來授予許可權給 Amazon EC2 執行個體上執行的應用程式。

使用政策管理存取權

您可以透過建立政策並將其連接到身分或資源 AWS 來控制 AWS 中的存取。政策是 中的物件， AWS 當與身分或資源建立關聯時， 會定義其許可。當委託人（使用者、根使用者或角色工作階段）發出請求時， 會 AWS 評估這些政策。政策中的許可決定是否允許或拒絕請求。大多數政策會以 JSON 文件 AWS 的形式存放在 中。如需 JSON 政策文件結構和內容的詳細資訊，請參閱 IAM 使用者指南中的 JSON 政策概觀。

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

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

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

身分型政策

身分型政策是可以附加到身分 (例如 IAM 使用者、使用者群組或角色) 的 JSON 許可政策文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的透過客戶管理政策定義自訂 IAM 許可。

身分型政策可進一步分類成內嵌政策或受管政策。內嵌政策會直接內嵌到單一使用者、群組或角色。受管政策是獨立的政策，您可以連接到 中的多個使用者、群組和角色 AWS 帳戶。受管政策包括 AWS 受管政策和客戶受管政策。如需了解如何在受管政策及內嵌政策之間選擇，請參閱《IAM 使用者指南》中的在受管政策和內嵌政策間選擇。

資源型政策

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

資源型政策是位於該服務中的內嵌政策。您無法在資源型政策中使用來自 IAM 的 AWS 受管政策。

存取控制清單 (ACL)

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

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

其他政策類型

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

- 許可界限 – 許可範圍是一種進階功能，可供您設定身分型政策能授予 IAM 實體 (IAM 使用者或角色) 的最大許可。您可以為實體設定許可界限。所產生的許可會是實體的身分型政策和其許可界限的交集。會在 `Principal` 欄位中指定使用者或角色的資源型政策則不會受到許可界限限制。所有這類政策中的明確拒絕都會覆寫該允許。如需許可界限的詳細資訊，請參閱 IAM 使用者指南中的 IAM 實體許可界限。
- 服務控制政策 SCPs) – SCPs是 JSON 政策，可指定 in. 中組織或組織單位 (OU) 的最大許可 AWS Organizations。 AWS Organizations 是一種用於分組和集中管理您企業擁有 AWS 帳戶 的多個的服務。若您啟用組織中的所有功能，您可以將服務控制政策 (SCP) 套用到任何或所有帳戶。SCP 會限制成員帳戶中實體的許可，包括每個實體 AWS 帳戶根使用者。如需 Organizations 和 SCP 的詳細資訊，請參閱《AWS Organizations 使用者指南》中的服務控制政策。
- 資源控制政策 (RCP) - RCP 是 JSON 政策，可用來設定您帳戶中資源的可用許可上限，採取這種方式就不需要更新附加至您所擁有的每個資源的 IAM 政策。RCP 會限制成員帳戶中資源的許可，並可能影響身分的有效許可，包括 AWS 帳戶根使用者，無論它們是否屬於您的組織。如需 Organizations 和 RCPs的詳細資訊，包括 AWS 服務 支援 RCPs的 清單，請參閱AWS Organizations 《 使用者指南》中的資源控制政策 RCPs)。
- 工作階段政策 – 工作階段政策是一種進階政策，您可以在透過撰寫程式的方式建立角色或聯合使用者的暫時工作階段時，做為參數傳遞。所產生工作階段的許可會是使用者或角色的身分型政策和工作階段政策的交集。許可也可以來自資源型政策。所有這類政策中的明確拒絕都會覆寫該允許。如需詳細資訊，請參閱 IAM 使用者指南中的工作階段政策。

多種政策類型

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

Direct Connect 搭配 IAM 的運作方式

在您使用 IAM 管理 Direct Connect 的存取權限之前，請瞭解搭配 Direct Connect 使用的 IAM 功能有哪些。

您可以搭配 Direct Connect 使用的 IAM 功能

IAM 功能	Direct Connect 支援
身分型政策	是
資源型政策	否
政策動作	是
政策資源	是
政策條件索引鍵 (服務特定)	是
ACL	否
ABAC(政策中的標籤)	部分
臨時憑證	是
主體許可	是
服務角色	是
服務連結角色	否

若要取得 Direct Connect 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AWS 與 IAM 搭配使用的 服務。

Direct Connect 的身分型政策

支援身分型政策：是

身分型政策是可以附加到身分 (例如 IAM 使用者、使用者群組或角色) 的 JSON 許可政策文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的透過客戶管理政策定義自訂 IAM 許可。

使用 IAM 身分型政策，您可以指定允許或拒絕的動作和資源，以及在何種條件下允許或拒絕動作。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。

Direct Connect 的身分型政策範例

若要檢視 Direct Connect 身分型政策的範例，請參閱 Direct Connect 的身分型政策範例。

Direct Connect 內的資源型政策

支援資源型政策：否

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

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

Direct Connect 的政策動作

支援政策動作：是

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

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

政策會使用動作來授予執行相關聯動作的許可。

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

Direct Connect 中的政策動作會在動作之前使用以下字首：

```
Direct Connect
```

若要在單一陳述式中指定多個動作，請用逗號分隔。

```
"Action": [
      "directconnect:action1",
      "directconnectaction2"
         ]
```

Direct Connect 的政策資源

支援政策資源：是

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

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

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

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

若要查看 Direct Connect 資源類型及其 ARN 的清單，請參閱《AWS Direct Connect API 參考》中的 Direct Connect 定義的資源。若要瞭解您可以使用哪些動作指定每個資源的 ARN，請參閱 Direct Connect 定義的動作。

若要檢視 Direct Connect 身分型政策的範例，請參閱 Direct Connect 的身分型政策範例。

若要檢視 Direct Connect 資源型政策的範例，請參閱 Direct Connect 身分型政策範例使用標籤型條件。

Direct Connect 的政策條件索引鍵

支援服務特定政策條件金鑰：是

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

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

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

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

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

若要查看 Direct Connect 條件金鑰清單，請參閱 AWS Direct Connect API 參考中的 Direct Connect 的條件金鑰。若要了解您可以使用條件金鑰的動作和資源，請參閱服務授權參考中的 Direct Connect 的動作、資源和條件金鑰。

若要檢視 Direct Connect 身分型政策的範例，請參閱 Direct Connect 的身分型政策範例。

Direct Connect 中的 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。

ABAC 搭配 Direct Connect

支援 ABAC (政策中的標籤)：部分

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。您可以將標籤連接至 IAM 實體 （使用者或角色） 和許多 AWS 資源。為實體和資源加上標籤是 ABAC 的第一步。您接著要設計 ABAC 政策，允許在主體的標籤與其嘗試存取的資源標籤相符時操作。

ABAC 在成長快速的環境中相當有幫助，並能在政策管理變得繁瑣時提供協助。

如需根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件索引鍵，在政策的條件元素中，提供標籤資訊。

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

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

將暫時憑證搭配 Direct Connect 使用

支援臨時憑證：是

當您使用臨時憑證登入時，有些 AWS 服務 無法使用。如需詳細資訊，包括 AWS 服務 使用哪些臨時登入資料，請參閱《AWS 服務 IAM 使用者指南》中的使用 IAM 的 。

如果您 AWS Management Console 使用使用者名稱和密碼以外的任何方法登入 ，則會使用臨時登入資料。例如，當您 AWS 使用公司的單一登入 (SSO) 連結存取 時，該程序會自動建立臨時登入資料。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》中的從使用者切換至 IAM 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。

Direct Connect 的跨服務委託人許可

支援轉寄存取工作階段 (FAS)：是

當您使用 IAM 使用者或角色在 中執行動作時 AWS，您會被視為委託人。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 使用呼叫 的委託人許可 AWS 服務，並結合 AWS 服務 請求向下游服務提出請求。只有當服務收到需要與其他 AWS 服務 或 資源互動才能完成的請求時，才會提出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的政策詳細資訊，請參閱轉發存取工作階段。

Direct Connect 的服務角色

支援服務角色：是

服務角色是服務擔任的 IAM 角色，可代您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需詳細資訊，請參閱《IAM 使用者指南》中的建立角色以委派許可權給 AWS 服務。

> **Warning**
>
> 變更服務角色的許可可能會讓 Direct Connect 功能故障。只有在 Direct Connect 提供指引時，才能編輯服務角色。

Direct Connect 的服務連結角色

支援服務連結角色：否

服務連結角色是連結至 的服務角色類型 AWS 服務。服務可以擔任代表您執行動作的角色。服務連結角色會出現在您的 中 AWS 帳戶 ，並由服務擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

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

Direct Connect 的身分型政策範例

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

如需了解如何使用這些範例 JSON 政策文件建立 IAM 身分型政策，請參閱《IAM 使用者指南》中的建立 IAM 政策 (主控台)。

如需 Direct Connect 所定義之動作和資源類型的詳細資訊，包括每種資源類型的 ARN 格式，請參閱《服務授權參考》中的適用於 Direct Connect 的動作、資源和條件索引鍵。

主題

- 政策最佳實務
- Direct Connect 的動作、資源和條件
- 使用 Direct Connect 主控台
- 允許使用者檢視他們自己的許可
- 唯讀存取 AWS Direct Connect
- AWS Direct Connect的完整存取權
- Direct Connect 身分型政策範例使用標籤型條件

政策最佳實務

身分型政策會判斷您帳戶中的某個人員是否可以建立、存取或刪除 Direct Connect 資源。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管政策並邁向最低權限許可 – 若要開始將許可授予您的使用者和工作負載，請使用 AWS 受管政策來授予許多常見使用案例的許可。它們可在您的 中使用 AWS 帳戶。我們建議您定義特定於使用案例 AWS 的客戶受管政策，進一步減少許可。如需更多資訊，請參閱 IAM 使用者指南中的 AWS 受管政策或任務職能的AWS 受管政策。

- 套用最低權限許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的許可。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的更多相關資訊，請參閱 IAM 使用者指南中的 IAM 中的政策和許可。
- 使用 IAM 政策中的條件進一步限制存取權 – 您可以將條件新增至政策，以限制動作和資源的存取。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。如果透過特定 使用服務動作，您也可以使用條件來授予存取服務動作的權限 AWS 服務，例如 AWS CloudFormation。如需詳細資訊，請參閱 IAM 使用者指南中的 IAM JSON 政策元素：條件。
- 使用 IAM Access Analyzer 驗證 IAM 政策，確保許可安全且可正常運作 – IAM Access Analyzer 驗證新政策和現有政策，確保這些政策遵從 IAM 政策語言 (JSON) 和 IAM 最佳實務。IAM Access Analyzer 提供 100 多項政策檢查及切實可行的建議，可協助您撰寫安全且實用的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的使用 IAM Access Analyzer 驗證政策。
- 需要多重要素驗證 (MFA)：如果您的案例需要 IAM 使用者或 中的根使用者 AWS 帳戶，請開啟 MFA 以增加安全性。如需在呼叫 API 操作時請求 MFA，請將 MFA 條件新增至您的政策。如需詳細資訊，請參閱《IAM 使用者指南》https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_configure-api-require.html中的透過 MFA 的安全 API 存取。

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

Direct Connect 的動作、資源和條件

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。Direct Connect 支援特定動作、資源和條件索引鍵。若要了解您在 JSON 政策中使用的所有元素，請參閱 IAM 使用者指南中的 JSON 政策元素參考。

動作

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

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

政策會使用動作來授予執行相關聯動作的許可。

Direct Connect 中的政策動作會在動作之前使用以下字首：`directconnect:`例如，若要授予某人使用 Amazon EC2 `DescribeVpnGateways` API 作業來執行 Amazon EC2 執行個體的許可，請在其政策中加入 `ec2:DescribeVpnGateways` 動作。政策陳述式必須包含 `Action` 或 `NotAction` 元素。Direct Connect 會定義自己的一組動作，描述您可以使用此服務執行的任務。

下列範例政策授予 的讀取存取權 AWS Direct Connect。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "directconnect:Describe*",
                "ec2:DescribeVpnGateways"
            ],
            "Resource": "*"
        }
    ]
}
```

下列範例政策授予 的完整存取權 AWS Direct Connect。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "directconnect:*",
                "ec2:DescribeVpnGateways"
            ],
            "Resource": "*"
        }
    ]
}
```

若要查看 Direct Connect 動作清單，請參閱 IAM 使用者指南中的 Direct Connect 定義的動作。

資源

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

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

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

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

Direct Connect 使用下列 ARN：

Direct Connect 資源 ARN

資源類型	ARN
dxcon	`arn:${Partition}:directconnect:${Region}:${Account}:dxcon/${ConnectionId}`
dxlag	`arn:${Partition}:directconnect:${Region}:${Account}:dxlag/${LagId}`
dx-vif	`arn:${Partition}:directconnect:${Region}:${Account}:dxvif/${VirtualInterfaceId}`
dx-gateway	`arn:${Partition}:directconnect::${Account}:dx-gateway/${DirectConnectGatewayId}`

如需 ARNs 格式的詳細資訊，請參閱 Amazon Resource Name (ARNs) AWS 和服務命名空間。

例如，若要在陳述式中指定 dxcon-11aa22bb 介面，請使用以下 ARN：

```
"Resource": "arn:aws:directconnect:us-east-1:123456789012:dxcon/dxcon-11aa22bb
```

若要指定屬於特定帳戶的所有虛擬介面，請使用萬用字元 (*)：

```
"Resource": "arn:aws:directconnect:*:*:dxvif/*"
```

有些 Direct Connect 動作 (例如用來建立資源的動作) 無法在特定資源上執行。在這些情況下，您必須使用萬用字元 (*)。

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

若要查看 Direct Connect 資源類型及其 ARN 的清單，請參閱《IAM 使用者指南》中的 AWS Direct Connect定義的資源類型。若要瞭解您可以使用哪些動作指定每個資源的 ARN，請參閱 Direct Connect 定義的動作。

如果在 DescribeConnections、DescribeVirtualInterfaces、DescribeDirectConnectGateways、DescribeInterconnects 或 DescribeLags 的 IAM 政策陳述式`Resource`欄位中`*`指定資源 ARN 或 以外的資源 ARN 模式，則除非在 API 呼叫中也傳遞相符的資源 ID，否則`Effect`不會發生指定的資源。不過，如果您在 IAM 政策陳述式中以資源而非特定資源 ID `*`提供 ，則指定的 `Effect`將會運作。

在下列範例中，如果在請求中未`connectionId`傳遞 的情況下呼叫`DescribeConnections`動作，則不會`Effect`成功指定。

```
"Statement": [
    {
        "Effect": "Allow",
        "Action": [
            "directconnect:DescribeConnections"
        ],
        "Resource": [
            "arn:aws:directconnect:*:123456789012:dxcon/*"
        ]
    },
{
        "Effect": "Deny",
        "Action": [
            "directconnect:DescribeConnections"
        ],
        "Resource": [
            "arn:aws:directconnect:*:123456789012:dxcon/example1"
        ]
    }
]
```

不過，在下列範例中，無論請求中是否`connectionId`指定 ， 會在 * IAM 政策陳述式 `Resource` 欄位提供的 `"Effect": "Allow"`DescribeConnections動作成功。

```
"Statement": [
    {
```

```
        "Effect": "Allow",
        "Action": [
            "directconnect:DescribeConnections
        ],
        "Resource": [
            "*"
        ]
    }
]
```

條件索引鍵

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

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

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

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

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

Direct Connect 會定義自己的一組條件索引鍵，也支援一些全域條件索引鍵的使用。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。

您可以將條件金鑰與標籤資源搭配使用。如需詳細資訊，請參閱範例：將存取限制在特定區域。

若要查看 Direct Connect 條件索引鍵清單，請參閱 IAM 使用者指南中的 Direct Connect 的條件索引鍵。若要瞭解您可以針對何種動作及資源使用條件索引鍵，請參閱 Direct Connect 定義的動作。

使用 Direct Connect 主控台

若要存取 Direct Connect 主控台，您必須擁有最基本的一組許可。這些許可必須允許您列出和檢視 AWS 帳戶中 Direct Connect 資源的詳細資訊。如果您建立比最基本必要許可更嚴格的身分型政策，則對於具有該政策的實體 (s 或角色) 而言，主控台就無法如預期運作。

為了確保這些實體仍然可以使用 Direct Connect 主控台，請將下列 AWS 受管政策連接至實體。如需更多資訊，請參閱 IAM 使用者指南中的新增許可到使用者：

```
directconnect
```

對於僅對 AWS CLI 或 AWS API 進行呼叫的使用者，您不需要允許最低主控台許可。反之，只需允許存取符合您嘗試執行之 API 操作的動作就可以了。

允許使用者檢視他們自己的許可

此範例會示範如何建立政策，允許 IAM 使用者檢視附加到他們使用者身分的內嵌及受管政策。此政策包含在主控台上完成此動作的許可，或使用 AWS CLI 或 AWS API 以程式設計方式完成此動作的許可。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
```

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

唯讀存取 AWS Direct Connect

下列範例政策授予 的讀取存取權 AWS Direct Connect。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "directconnect:Describe*",
                "ec2:DescribeVpnGateways"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS Direct Connect的完整存取權

下列範例政策授予 的完整存取權 AWS Direct Connect。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "directconnect:*",
                "ec2:DescribeVpnGateways"
            ],
            "Resource": "*"
        }
    ]
}
```

Direct Connect 身分型政策範例使用標籤型條件

透過使用標籤金鑰條件，您就可以控制對於資源和請求的存取。您也可以在 IAM 政策中使用條件，控制可在資源或請求中使用特定的標籤金鑰。

如需有關如何使用具有 IAM 政策之標籤的資訊，請參閱《IAM 使用者指南》中的使用標籤控制存取權。

根據標籤與 Direct Connect 虛擬介面產生關聯

以下範例將示範如何建立政策，以便僅在標籤包含環境金鑰、preprod 或 production 等值的條件下，才能與虛擬介面建立關聯。

```
 {
"Version": "2012-10-17",
"Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "directconnect:AssociateVirtualInterface"
    ],
    "Resource": "arn:aws:directconnect:*:*:dxvif/*",
    "Condition": {
      "StringEquals": {
        "aws:ResourceTag/environment": [
          "preprod",
          "production"
        ]
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": "directconnect:DescribeVirtualInterfaces",
    "Resource": "*"
  }
]
}
```

根據標籤控制對請求的存取

您可以使用 IAM 政策中的條件，控制哪些標籤鍵/值對可以在標記 AWS 資源的請求中傳遞。下列範例示範如何建立政策，允許使用 AWS Direct Connect TagResource 動作，僅在標籤包含環境金

鑰和預製或生產值時，才將標籤連接至虛擬介面。最佳實務是，搭配 aws:TagKeys 條件金鑰使用 ForAllValues 修飾詞，以表示僅允許在請求中使用金鑰環境。

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": "directconnect:TagResource",
        "Resource": "arn:aws:directconnect:*:*:dxvif/*",
        "Condition": {
            "StringEquals": {
                "aws:RequestTag/environment": [
                    "preprod",
                    "production"
                ]
            },
            "ForAllValues:StringEquals": {"aws:TagKeys": "environment"}
        }
    }
}
```

控制標籤鍵

您可以在 IAM 政策中使用條件，以控制是否可對資源或在請求中使用特定標籤索引鍵。

以下範例將示範如何建立政策，以便僅在搭配標籤金鑰環境的條件下，才能為資源加上標籤。

```
 {
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "directconnect:TagResource",
    "Resource": "*",
    "Condition": {
      "ForAllValues:StringEquals": {
        "aws:TagKeys": [
          "environment"
        ]
      }
    }
  }
}
```

的服務連結角色 AWS Direct Connect

AWS Direct Connect use AWS Identity and Access Management (IAM) 服務連結角色。服務連結角色是直接連結至 的唯一 IAM 角色類型 AWS Direct Connect。服務連結角色由 預先定義， AWS Direct Connect 並包含該服務代表您呼叫其他 AWS 服務所需的所有許可。

服務連結角色可讓設定 AWS Direct Connect 更容易，因為您不必手動新增必要的許可。 AWS Direct Connect 會定義其服務連結角色的許可，除非另有定義，否則只能 AWS Direct Connect 擔任其角色。定義的許可包括信任政策和許可政策，且該許可政策無法附加至其他 IAM 實體。

您必須先刪除服務連結角色的相關資源，才能將其刪除。這可保護您的 AWS Direct Connect 資源，因為您不會不小心移除存取資源的許可。

如需關於支援服務連結角色的其他服務的資訊，請參閱可搭配 IAM 運作的AWS 服務，並尋找 Service-Linked Role (服務連結角色) 欄顯示為 Yes (是) 的服務。選擇具有連結的是，以檢視該服務的服務連結角色文件。

的服務連結角色許可 AWS Direct Connect

AWS Direct Connect 使用名為 的服務連結角色AWSServiceRoleForDirectConnect。這可讓 AWS Secrets Manager 代表您 AWS Direct Connect 擷取存放在 中的 MACSec 秘密。

AWSServiceRoleForDirectConnect 服務連結角色信任下列服務以擔任角色：

- directconnect.amazonaws.com

AWSServiceRoleForDirectConnect 服務連結角色使用受管政策 AWSDirectConnectServiceRolePolicy。

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。為成功建立 AWSServiceRoleForDirectConnect 服務連結角色，您搭配 AWS Direct Connect 使用的 IAM 身分必須擁有必要的許可。若要授予必要許可，請將下列政策連接至 IAM 身分。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "iam:CreateServiceLinkedRole",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "directconnect.amazonaws.com"
```

```
                }
            },
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": "iam:GetRole",
            "Effect": "Allow",
            "Resource": "*"
       }
    ]
}
```

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 建立服務連結角色 AWS Direct Connect

您不需要手動建立服務連結角色。 會為您 AWS Direct Connect 建立服務連結角色。當您執行`associate-mac-sec-key`命令時， 會 AWS 建立服務連結角色， AWS Direct Connect 允許 AWS Secrets Manager 擷取代表您存放在 中的 MACsec 秘密，這些秘密存放在 AWS Management Console、 AWS CLI或 AWS API 中。

> **Important**
>
> 此服務連結角色可以顯示在您的帳戶，如果您於其他服務中完成一項動作時，可以使用支援此角色的功能。若要進一步了解，請參閱我的 IAM 帳戶中出現的新角色。

如果您刪除此服務連結角色，然後需要再次建立該角色，您可以使用相同的程序在帳戶中重新建立角色。 會再次為您 AWS Direct Connect 建立服務連結角色。

您也可以使用 IAM 主控台透過 AWS Direct Connect 使用案例以建立一個服務連結角色。在 AWS CLI 或 AWS API 中，使用服務名稱建立`directconnect.amazonaws.com`服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的「建立服務連結角色」。如果您刪除此服務連結角色，您可以使用此相同的程序以再次建立該角色。

編輯 的服務連結角色 AWS Direct Connect

AWS Direct Connect 不允許您編輯`AWSServiceRoleForDirectConnect`服務連結角色。因為可能有各種實體會參考服務連結角色，所以您無法在建立角色之後變更其名稱。然而，您可使用 IAM 來編輯角色描述。如需詳細資訊，請參閱「IAM 使用者指南」的編輯服務連結角色。

刪除 的服務連結角色 AWS Direct Connect

您不需要手動刪除 `AWSServiceRoleForDirectConnect` 角色。刪除服務連結角色時，您必須刪除存放在 AWS Secrets Manager Web 服務中的所有相關資源。 AWS Management Console、 AWS CLI或 AWS API 會 AWS Direct Connect 為您清理資源並刪除服務連結角色。

您也可以使用 IAM 主控台刪除該服務連結角色。若要執行此操作，您必須先手動清除服務連結角色的資源，然後才能刪除它。

> **Note**
>
> 如果您嘗試刪除資源時 AWS Direct Connect ，服務正在使用該角色，則刪除可能會失敗。若此情況發生，請等待數分鐘，然後再次嘗試操作。

刪除 使用 AWS Direct Connect 的資源 **`AWSServiceRoleForDirectConnect`**

1. 移除所有 MACsec 金鑰和連線之間的關聯。如需詳細資訊，請參閱 the section called “移除 MACsec 私密金鑰和連線之間的關聯”
2. 移除所有 MACsec 金鑰和 LAG 之間的關聯。如需詳細資訊，請參閱 the section called “移除 MACsec 私密金鑰和 LAG 之間的關聯”

使用 IAM 手動刪除服務連結角色

使用 IAM 主控台 AWS CLI、 或 AWS API 來刪除`AWSServiceRoleForDirectConnect`服務連結角色。如需詳細資訊，請參閱「IAM 使用者指南」中的刪除服務連結角色。

AWS Direct Connect 服務連結角色支援的區域

AWS Direct Connect 支援 AWS 區域 在提供 MAC 安全功能的所有 中使用服務連結角色。如需詳細資訊，請參閱 AWS Direct Connect 據點。

AWS 的 受管政策 AWS Direct Connect

AWS 受管政策是由 AWS AWS 受管政策建立和管理的獨立政策旨在為許多常見使用案例提供許可，以便您可以開始將許可指派給使用者、群組和角色。

請記住， AWS 受管政策可能不會授予特定使用案例的最低權限許可，因為這些許可可供所有 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 AWS 受管政策中定義的許可。如果 AWS 更新受管政策中 AWS 定義的許可，則更新會影響政策連接的所有主體身分（使用者、群組和角色）。當新的 AWS 服務 啟動或新的 API 操作可用於現有服務時， AWS 最有可能更新受 AWS 管政策。

如需詳細資訊，請參閱《IAM 使用者指南》中的 AWS 受管政策。

AWS 受管政策：AWSDirectConnectFullAccess

您可將 `AWSDirectConnectFullAccess` 政策連接到 IAM 身分。此政策會授予許可，以允許完整存取 AWS Direct Connect。

若要檢視此政策的許可，請參閱 AWS Management Console中的 AWSDirectConnectFullAccess。

AWS 受管政策：AWSDirectConnectReadOnlyAccess

您可將 `AWSDirectConnectReadOnlyAccess` 政策連接到 IAM 身分。此政策會授予許可，以允許唯讀存取 AWS Direct Connect。

若要檢視此政策的許可，請參閱 AWS Management Console中的 AWSDirectConnectReadOnlyAccess。

AWS 受管政策：AWSDirectConnectServiceRolePolicy

此政策會連接至名為 AWSServiceRoleForDirectConnect 的服務連結角色，以允許 代表您 AWS Direct Connect 擷取 MAC 安全秘密。如需詳細資訊，請參閱the section called “服務連結角色”。

若要檢視此政策的許可，請參閱 AWS Management Console中的 AWSDirectConnectServiceRolePolicy。

AWS Direct Connect 受 AWS 管政策的更新

檢視自此服務開始追蹤這些變更 AWS Direct Connect 以來， AWS 受管政策更新的詳細資訊。如需此頁面變更的自動提醒，請訂閱 AWS Direct Connect 文件歷史記錄頁面上的 RSS 摘要。

變更	描述	日期
AWSDirectConnectServiceRolePolicy - 全新政策	為了支援 MAC Security，已新增 AWSServiceRoleForDirectConnect 服務連結角色。	2021 年 3 月 31 日

變更	描述	日期
AWS Direct Connect 開始追蹤變更	AWS Direct Connect 開始追蹤其 AWS 受管政策的變更。	2021 年 3 月 31 日

疑難排解 Direct Connect 身分和存取

請使用以下資訊來協助您診斷和修復使用 Direct Connect 和 IAM 時發生的常見問題。

主題

- 我未獲授權在 Direct Connect 中執行動作
- 我未獲得執行 iam:PassRole 的授權
- 我想要允許 以外的人員 AWS 帳戶 存取我的 Direct Connect 資源

我未獲授權在 Direct Connect 中執行動作

如果您收到錯誤，告知您未獲授權執行動作，您的政策必須更新，允許您執行動作。

下列範例錯誤會在mateojackson IAM 使用者嘗試使用主控台檢視一個虛構 *my-example-widget* 資源的詳細資訊，但卻無虛構 directconnect:*GetWidget* 許可時發生。

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

在此情況下，必須更新 mateojackson 使用者的政策，允許使用 directconnect:*GetWidget* 動作存取 *my-example-widget* 資源。

如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的簽署憑證。

我未獲得執行 iam:PassRole 的授權

如果您收到錯誤，告知您未獲授權執行 iam:PassRole 動作，您的政策必須更新，允許您將角色傳遞給 Direct Connect。

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

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

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

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

如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的簽署憑證。

我想要允許 以外的人員 AWS 帳戶 存取我的 Direct Connect 資源

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

如需進一步了解，請參閱以下內容：

- 若要瞭解 Direct Connect 是否支援這些功能，請參閱 Direct Connect 搭配 IAM 的運作方式。
- 若要了解如何 AWS 帳戶 在您擁有的 資源間提供存取權，請參閱《IAM 使用者指南》中的在您擁有 AWS 帳戶 的另一個資源中提供存取權給 IAM 使用者。
- 若要了解如何將資源的存取權提供給第三方 AWS 帳戶，請參閱《IAM 使用者指南》中的提供存取權給第三方 AWS 帳戶 擁有。
- 如需了解如何透過聯合身分提供存取權，請參閱 IAM 使用者指南中的將存取權提供給在外部進行身分驗證的使用者 (聯合身分)。
- 如需了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱《IAM 使用者指南》中的 IAM 中的跨帳戶資源存取。

在 中記錄和監控 AWS Direct Connect

您可以使用下列自動化監控工具來監看 AWS Direct Connect ，並在發生錯誤時進行回報：

- Amazon CloudWatch 警示 – 在您指定的一段時間內監看單一指標。根據在數個期間與指定閾值相關的指標值，執行一個或多個動作。動作是傳送至 Amazon SNS 主題的通知。CloudWatch 警示不會只因處於特定狀態就叫用動作，狀態必須已變更並已維持一段指定的時間。如需詳細資訊，請參閱使用 Amazon CloudWatch 監控 。
- AWS CloudTrail 日誌監控 – 透過將日誌檔案傳送至 CloudWatch Logs，在帳戶之間共用日誌檔案並即時監控 CloudTrail 日誌檔案。 CloudWatch 您也能夠以 Java 應用程式語言撰寫日誌記錄處理應用程式的方式、驗證日誌檔在由 CloudTrail 交付後並沒有發生改變。如需詳細資訊，請參閱 使用

記錄 AWS Direct Connect API 呼叫 AWS CloudTrail 和《AWS CloudTrail 使用者指南》中的使用 CloudTrail 記錄檔案。

如需詳細資訊，請參閱監控 Direct Connect 資源。

的合規驗證 AWS Direct Connect

若要了解 是否 AWS 服務 在特定合規計劃的範圍內，請參閱AWS 服務 合規計劃範圍內然後選擇您感興趣的合規計劃。如需一般資訊，請參閱 AWS Compliance Programs。

您可以使用 下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱在 中下載報告 AWS Artifact。

使用 時的合規責任 AWS 服務 取決於資料的敏感度、您公司的合規目標，以及適用的法律和法規。AWS 提供下列資源以協助合規：

- 安全合規與治理 - 這些解決方案實作指南內容討論了架構考量，並提供部署安全與合規功能的步驟。
- HIPAA 合格服務參考 – 列出 HIPAA 合格服務。並非所有 AWS 服務 都符合 HIPAA 資格。
- AWS 合規資源 – 此工作手冊和指南的集合可能適用於您的產業和位置。
- AWS 客戶合規指南 – 透過合規的角度了解共同責任模型。本指南摘要說明保護 的最佳實務， AWS 服務 並將指南映射到跨多個架構的安全控制 （ 包括國家標準和技術研究所 (NIST)、支付卡產業安全標準委員會 (PCI) 和國際標準化組織 (ISO))。
- AWS Config 開發人員指南中的使用規則評估資源 – AWS Config 服務會評估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 可讓您全面檢視其中的安全狀態 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 控制參考」。
- Amazon GuardDuty – 這可透過監控您的環境是否有可疑和惡意活動，來 AWS 服務 偵測對您 AWS 帳戶、工作負載、容器和資料的潛在威脅。GuardDuty 可滿足特定合規架構所規定的入侵偵測需求，以協助您因應 PCI DSS 等各種不同的合規需求。
- AWS Audit Manager – 這 AWS 服務 可協助您持續稽核 AWS 用量，以簡化您管理風險的方式，以及符合法規和產業標準的方式。

中的彈性 AWS Direct Connect

AWS 全域基礎設施是以 AWS 區域和可用區域為基礎建置。 AWS 區域提供多個實體隔離和隔離的可用區域，這些區域與低延遲、高輸送量和高度冗餘聯網連接。透過可用區域，您所設計與操作的應用程

式和資料庫，就能夠在可用區域之間自動容錯移轉，而不會發生中斷。可用區域的可用性、容錯能力和擴充能力，均較單一或多個資料中心的傳統基礎設施還高。

如需 AWS 區域和可用區域的詳細資訊，請參閱AWS 全球基礎設施。

除了 AWS 全球基礎設施之外， AWS Direct Connect 還提供多種功能，以協助支援您的資料彈性和備份需求。

如需如何搭配 VPN 使用的資訊 AWS Direct Connect，請參閱 AWS Direct Connect Plus VPN。

容錯移轉

AWS Direct Connect 彈性工具組提供具有多個彈性模型的連線精靈，可協助您訂購專用連線，以實現 SLA 目標。您可以選擇彈性模型，然後 AWS Direct Connect 彈性工具組會引導您完成專用連線排序程序。彈性模型的設計旨在確保您在多個位置擁有適當數量的專用連線。

- 最大彈性：您可以使用在多個位置終止個別裝置的個別連線，就能獲得執行關鍵工作負載的最大彈性。此模型可針對裝置、連線能力及完整位置故障提供彈性。
- 高彈性：您可以使用連至多個位置的兩個單一連線，即可為關鍵工作負載取得高彈性。此模型可針對因光纖切割或裝置故障所造成的連線故障提供彈性。它也有助於防止完整的位置故障。
- 開發和測試：您可以使用在多個位置終止個別裝置的個別連線，就能獲得執行非關鍵工作負載的開發及測試彈性。此模型可針對裝置故障提供彈性，但無法針對位置故障提供彈性。

如需詳細資訊，請參閱AWS Direct Connect 彈性工具組。

中的基礎設施安全性 AWS Direct Connect

作為受管服務， AWS Direct Connect 受到 AWS 全球網路安全程序的保護。您可以使用 AWS 發佈的 API 呼叫， AWS Direct Connect 透過網路存取 。用戶端必須支援 Transport Layer Security (TLS) 1.2 或更新版本。我們建議使用 TLS 1.3。用戶端也必須支援具備完美轉送私密 (PFS) 的密碼套件，例如臨時 Diffie-Hellman (DHE) 或橢圓曲線臨時 Diffie-Hellman (ECDHE)。現代系統 (如 Java 7 和更新版本) 大多會支援這些模式。

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

您可以從任何網路位置呼叫這些 API 操作，但 AWS Direct Connect 支援以資源為基礎的存取政策，其中可能包含根據來源 IP 地址的限制。您也可以使用 AWS Direct Connect 政策來控制來自特定

Amazon Virtual Private Cloud (Amazon VPC) 端點或特定 VPCs存取。實際上，這只會隔離網路中特定 VPC 對指定 AWS Direct Connect 資源 AWS 的網路存取。如需範例，請參閱 the section called “Direct Connect 的身分型政策範例”。

邊界閘道協定 (BGP) 安全

網際網路大致上倚賴 BGP 取得網路系統之間的路由資訊。BGP 路由有時可能會受到惡意攻擊或 BGP 攔截。若要了解如何 AWS 更安全地保護您的網路免受 BGP 劫持，請參閱如何 AWS 協助保護網際網路路由。

使用 AWS Direct Connect CLI

您可以使用 AWS CLI 來建立和使用 AWS Direct Connect 資源。

下列範例使用 AWS CLI 命令來建立 AWS Direct Connect 連線。您也可以下載《授權書和連線設施指派》(LOA-CFA) 或佈建私有或公有虛擬介面。

開始之前，請確定您已安裝並設定妥 AWS CLI。如需詳細資訊，請參閱「AWS Command Line Interface 使用者指南」。

目錄

- 步驟 1：建立連線
- 步驟 2：下載 LOA-CFA
- 步驟 3：建立虛擬介面並取得路由器組態

步驟 1：建立連線

第一個步驟是提交連線申請。請確定您知道所需的連接埠速度和 AWS Direct Connect 位置。如需詳細資訊，請參閱專用和託管連線。

建立連線申請

1. 描述目前區域 AWS Direct Connect 的位置。在傳回的輸出中，記下您要建立連線的據點其據點代碼。

```
aws directconnect describe-locations
```

```
{
    "locations": [
        {
            "locationName": "City 1, United States",
            "locationCode": "Example Location 1"
        },
        {
            "locationName": "City 2, United States",
            "locationCode": "Example location"
        }
    ]
```

```
}
```

2. 建立連線並指定其名稱、連接埠速度和據點代碼。在傳回的輸出中，記下連線 ID。下一個步驟將需要此 ID 以取得 LOA-CFA。

```
aws directconnect create-connection --location Example location --bandwidth 1Gbps
 --connection-name "Connection to AWS"
```

```
{
    "ownerAccount": "123456789012",
    "connectionId": "dxcon-EXAMPLE",
    "connectionState": "requested",
    "bandwidth": "1Gbps",
    "location": "Example location",
    "connectionName": "Connection to AWS",
    "region": "sa-east-1"
}
```

步驟 2：下載 LOA-CFA

申請連線之後，您可以使用 `describe-loa` 命令取得 LOA-CFA。輸出內容為 base64 編碼。您必須擷取相關的 LOA 內容、將其解碼並建立 PDF 檔案。

使用 Linux 或 macOS 取得 LOA-CFA

本範例中，命令的最末部分使用 base64 公用程式將內容解碼並傳送輸出至 PDF 檔案。

```
aws directconnect describe-loa --connection-id dxcon-fg31dyv6 --output text --query
 loaContent|base64 --decode > myLoaCfa.pdf
```

使用 Windows 取得 LOA-CFA

本範例中，輸出將擷取至名為 myLoaCfa.base64 的檔案。第二個命令使用 `certutil` 公用程式將該檔案解碼並傳送輸出至 PDF 檔案。

```
aws directconneawsct describe-loa --connection-id dxcon-fg31dyv6 --output text --query
 loaContent > myLoaCfa.base64
```

```
certutil -decode myLoaCfa.base64 myLoaCfa.pdf
```

下載 LOA-CFA 之後，將其傳送給您的網路供應商或主機代管服務供應商。

步驟 3：建立虛擬介面並取得路由器組態

訂購 AWS Direct Connect 連線之後，您必須建立虛擬介面才能開始使用它。您可以建立私有虛擬介面以連接到您的 VPC。或者，您可以建立公有虛擬介面，以連線至不在 VPC 中的 AWS 服務。您可以建立支援 IPv4 或 IPv6 流量的虛擬介面。

開始之前，請務必先詳閱the section called “虛擬介面的先決條件”所列各項先決條件。

當您使用 建立虛擬介面時 AWS CLI，輸出會包含一般路由器組態資訊。若要建立裝置專屬的路由器組態，請使用 AWS Direct Connect 主控台。如需詳細資訊，請參閱下載路由組態檔案。

建立私有虛擬介面

1. 取得連接至您 VPC 的虛擬私有閘道的 ID (vgw-xxxxxxxx)。下一個步驟將需要此 ID 以建立虛擬介面。

```
aws ec2 describe-vpn-gateways
```

```
{
    "VpnGateways": [
        {
            "State": "available",
            "Tags": [
                {
                    "Value": "DX_VGW",
                    "Key": "Name"
                }
            ],
            "Type": "ipsec.1",
            "VpnGatewayId": "vgw-ebaa27db",
            "VpcAttachments": [
                {
                    "State": "attached",
                    "VpcId": "vpc-24f33d4d"
                }
            ]
        }
    ]
}
```

2. 建立私有虛擬介面。您必須指定其名稱、VLAN ID 以及 BGP 自發系統編號 (ASN)。

   對於 IPv4 流量，您需要 BGP 對等工作階段每一端的私有 IPv4 地址。您可以自行指定 IPv4 地址，或者由 Amazon 為您產生地址。以下範例將會為您產生 IPv4 地址。

```
aws directconnect create-private-virtual-interface --
connection-id dxcon-fg31dyv6 --new-private-virtual-interface
 virtualInterfaceName=PrivateVirtualInterface,vlan=101,asn=65000,virtualGatewayId=vgw-
ebaa27db,addressFamily=ipv4
```

```
{
    "virtualInterfaceState": "pending",
    "asn": 65000,
    "vlan": 101,
    "customerAddress": "192.168.1.2/30",
    "ownerAccount": "123456789012",
    "connectionId": "dxcon-fg31dyv6",
    "addressFamily": "ipv4",
    "virtualGatewayId": "vgw-ebaa27db",
    "virtualInterfaceId": "dxvif-ffhhk74f",
    "authKey": "asdf34example",
    "routeFilterPrefixes": [],
    "location": "Example location",
    "bgpPeers": [
        {
            "bgpStatus": "down",
            "customerAddress": "192.168.1.2/30",
            "addressFamily": "ipv4",
            "authKey": "asdf34example",
            "bgpPeerState": "pending",
            "amazonAddress": "192.168.1.1/30",
            "asn": 65000
        }
    "customerRouterConfig": "<?xml version=\"1.0\" encoding=
\"UTF-8\"?>\n<logical_connection id=\"dxvif-ffhhk74f\">\n  <vlan>101</
vlan>\n  <customer_address>192.168.1.2/30</customer_address>\n
 <amazon_address>192.168.1.1/30</amazon_address>\n  <bgp_asn>65000</bgp_asn>
\n  <bgp_auth_key>asdf34example</bgp_auth_key>\n  <amazon_bgp_asn>7224</
amazon_bgp_asn>\n  <connection_type>private</connection_type>\n</
logical_connection>\n",
    "amazonAddress": "192.168.1.1/30",
    "virtualInterfaceType": "private",
```

```
    "virtualInterfaceName": "PrivateVirtualInterface"
}
```

若要建立支援 IPv6 流量的私有虛擬介面，請使用以上相同的命令並對 addressFamily 參數指定 ipv6。您無法自行指定 BGP 對等工作階段的 IPv6 地址；Amazon 會為您配置 IPv6 地址。

3. 如欲查看 XML 格式的路由器組態資訊，請描述您所建立的虛擬介面。使用 --query 參數可擷取 customerRouterConfig 資訊，使用 --output 參數可將文字整理成標籤分隔文字行。

```
aws directconnect describe-virtual-interfaces --virtual-interface-id dxvif-ffhhk74f
 --query virtualInterfaces[*].customerRouterConfig --output text
```

```
<?xml version="1.0" encoding="UTF-8"?>
<logical_connection id="dxvif-ffhhk74f">
  <vlan>101</vlan>
  <customer_address>192.168.1.2/30</customer_address>
  <amazon_address>192.168.1.1/30</amazon_address>
  <bgp_asn>65000</bgp_asn>
  <bgp_auth_key>asdf34example</bgp_auth_key>
  <amazon_bgp_asn>7224</amazon_bgp_asn>
  <connection_type>private</connection_type>
</logical_connection>
```

建立公有虛擬介面

1. 若要建立公有虛擬介面，您必須指定其名稱、VLAN ID 以及 BGP 自治系統編號 (ASN)。

   對於 IPv4 流量，您還必須指定 BGP 對等工作階段每一端的公有 IPv4 地址，以及您將透過 BGP 公告的公有 IPv4 路由。以下範例建立用於 IPv4 流量的公有虛擬介面。

```
aws directconnect create-public-virtual-interface --
connection-id dxcon-fg31dyv6 --new-public-virtual-interface
 virtualInterfaceName=PublicVirtualInterface,vlan=2000,asn=65000,amazonAddress=203.0.113.1/
{cidr=203.0.113.4/30}]
```

```
{
    "virtualInterfaceState": "verifying",
    "asn": 65000,
    "vlan": 2000,
    "customerAddress": "203.0.113.2/30",
```

```
    "ownerAccount": "123456789012",
    "connectionId": "dxcon-fg31dyv6",
    "addressFamily": "ipv4",
    "virtualGatewayId": "",
    "virtualInterfaceId": "dxvif-fgh0hcrk",
    "authKey": "asdf34example",
    "routeFilterPrefixes": [
        {
            "cidr": "203.0.113.0/30"
        },
        {
            "cidr": "203.0.113.4/30"
        }
    ],
    "location": "Example location",
    "bgpPeers": [
        {
            "bgpStatus": "down",
            "customerAddress": "203.0.113.2/30",
            "addressFamily": "ipv4",
            "authKey": "asdf34example",
            "bgpPeerState": "verifying",
            "amazonAddress": "203.0.113.1/30",
            "asn": 65000
        }
    ],
    "customerRouterConfig": "<?xml version=\"1.0\" encoding=\"UTF-8\"?
>\n<logical_connection id=\"dxvif-fgh0hcrk\">\n  <vlan>2000</
vlan>\n  <customer_address>203.0.113.2/30</customer_address>\n
 <amazon_address>203.0.113.1/30</amazon_address>\n  <bgp_asn>65000</bgp_asn>
\n  <bgp_auth_key>asdf34example</bgp_auth_key>\n  <amazon_bgp_asn>7224</
amazon_bgp_asn>\n  <connection_type>public</connection_type>\n</logical_connection>
\n",
    "amazonAddress": "203.0.113.1/30",
    "virtualInterfaceType": "public",
    "virtualInterfaceName": "PublicVirtualInterface"
}
```

若要建立支援 IPv6 流量的公有虛擬介面，您可以指定將透過 BGP 公告的 IPv6 路由。您無法指定對等工作階段的 IPv6 地址；Amazon 會為您配置 IPv6 地址。以下範例建立用於 IPv6 流量的公有虛擬介面。

```
aws directconnect create-public-virtual-interface --
connection-id dxcon-fg31dyv6 --new-public-virtual-interface
 virtualInterfaceName=PublicVirtualInterface,vlan=2000,asn=65000,addressFamily=ipv6,routeFi
{cidr=2001:db8:64ce:ba01::/64}]
```

2. 如欲查看 XML 格式的路由器組態資訊，請描述您所建立的虛擬介面。使用 `--query` 參數可擷取 `customerRouterConfig` 資訊，使用 `--output` 參數可將文字整理成標籤分隔文字行。

```
aws directconnect describe-virtual-interfaces --virtual-interface-id dxvif-fgh0hcrk
 --query virtualInterfaces[*].customerRouterConfig --output text
```

```
<?xml version="1.0" encoding="UTF-8"?>
<logical_connection id="dxvif-fgh0hcrk">
  <vlan>2000</vlan>
  <customer_address>203.0.113.2/30</customer_address>
  <amazon_address>203.0.113.1/30</amazon_address>
  <bgp_asn>65000</bgp_asn>
  <bgp_auth_key>asdf34example</bgp_auth_key>
  <amazon_bgp_asn>7224</amazon_bgp_asn>
  <connection_type>public</connection_type>
</logical_connection>
```

使用 記錄 AWS Direct Connect API 呼叫 AWS CloudTrail

AWS Direct Connect 已與 整合 AWS CloudTrail，此服務提供使用者、角色或服務在 AWS 中採取動作的記錄 AWS Direct Connect。CloudTrail 會將 AWS Direct Connect 的所有 API 呼叫擷取為事件。擷取的呼叫包括從 AWS Direct Connect 主控台呼叫，以及對 AWS Direct Connect API 操作的程式碼呼叫。如果您建立線索，您可以啟用 CloudTrail 事件持續交付至 Amazon S3 儲存貯體，包括 的事件 AWS Direct Connect。即使您未設定追蹤，依然可以透過 CloudTrail 主控台中的事件歷史記錄檢視最新事件。使用 CloudTrail 所收集的資訊，您可以判斷提出的請求 AWS Direct Connect、提出請求的 IP 地址、提出請求的人員、提出請求的時間，以及其他詳細資訊。

如需詳細資訊，請參閱《AWS CloudTrail 使用者指南》https://docs.aws.amazon.com/awscloudtrail/latest/userguide/。

AWS Direct Connect CloudTrail 中的資訊

當您建立 AWS 帳戶時，會在您的帳戶上啟用 CloudTrail。當活動在 中發生時 AWS Direct Connect，該活動會記錄於 CloudTrail 事件，以及事件歷史記錄中的其他服務 AWS 事件。您可以檢視、搜尋和下載 AWS 帳戶的最新事件。如需詳細資訊，請參閱使用 CloudTrail 事件歷史記錄檢視事件。

若要持續記錄您 AWS 帳戶中的事件，包括 的事件 AWS Direct Connect，請建立追蹤。線索能讓 CloudTrail 將日誌檔案交付至 Amazon S3 儲存貯體。根據預設，當您在主控台中建立追蹤時，追蹤會套用至所有 AWS 區域。追蹤會記錄 AWS 分割區中所有 區域的事件，並將日誌檔案交付至您指定的 Amazon S3 儲存貯體。此外，您可以設定其他 AWS 服務，以進一步分析 CloudTrail 日誌中收集的事件資料並對其採取行動。如需詳細資訊，請參閱下列內容：

- 建立追蹤的概觀
- CloudTrail 支援的服務和整合
- 設定 CloudTrail 的 Amazon SNS 通知
- 從多個區域接收 CloudTrail 日誌檔案，以及從多個帳戶接收 CloudTrail 日誌檔案

CloudTrail 會記錄所有 AWS Direct Connect 動作，並記錄在 AWS Direct Connect API 參考中。例如，對 `CreateConnection` 以及 `CreatePrivateVirtualInterface` 動作發出的呼叫會在 CloudTrail 日誌檔案中產生項目。

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

- 是否使用根登入資料或 AWS Identity and Access Management (IAM 使用者) 登入資料提出請求。

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

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

了解 AWS Direct Connect 日誌檔案項目

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

以下是 的範例 CloudTrail 日誌記錄 AWS Direct Connect。

Example 範例：CreateConnection


```
{
    "Records": [
    {
        "eventVersion": "1.0",
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::123456789012:user/Alice",
            "accountId": "123456789012",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice",
            "sessionContext": {
                "attributes": {
                    "mfaAuthenticated": "false",
                    "creationDate": "2014-04-04T12:23:05Z"
                }
            }
        },
        "eventTime": "2014-04-04T17:28:16Z",
        "eventSource": "directconnect.amazonaws.com",
        "eventName": "CreateConnection",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "127.0.0.1",
        "userAgent": "Coral/Jakarta",
        "requestParameters": {
```

```
            "location": "EqSE2",
            "connectionName": "MyExampleConnection",
            "bandwidth": "1Gbps"
        },
        "responseElements": {
            "location": "EqSE2",
            "region": "us-west-2",
            "connectionState": "requested",
            "bandwidth": "1Gbps",
            "ownerAccount": "123456789012",
            "connectionId": "dxcon-fhajolyy",
            "connectionName": "MyExampleConnection"
        }
    },
    ...
  ]
}
```

Example 範例：CreatePrivateVirtualInterface

```
{
    "Records": [
    {
        "eventVersion": "1.0",
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::123456789012:user/Alice",
            "accountId": "123456789012",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice",
            "sessionContext": {
                "attributes": {
                    "mfaAuthenticated": "false",
                    "creationDate": "2014-04-04T12:23:05Z"
                }
            }
        },
        "eventTime": "2014-04-04T17:39:55Z",
        "eventSource": "directconnect.amazonaws.com",
        "eventName": "CreatePrivateVirtualInterface",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "127.0.0.1",
```

```
        "userAgent": "Coral/Jakarta",
        "requestParameters": {
            "connectionId": "dxcon-fhajolyy",
            "newPrivateVirtualInterface": {
                "virtualInterfaceName": "MyVirtualInterface",
                "customerAddress": "[PROTECTED]",
                "authKey": "[PROTECTED]",
                "asn": -1,
                "virtualGatewayId": "vgw-bb09d4a5",
                "amazonAddress": "[PROTECTED]",
                "vlan": 123
            }
        },
        "responseElements": {
            "virtualInterfaceId": "dxvif-fgq61m6w",
            "authKey": "[PROTECTED]",
            "virtualGatewayId": "vgw-bb09d4a5",
            "customerRouterConfig": "[PROTECTED]",
            "virtualInterfaceType": "private",
            "asn": -1,
            "routeFilterPrefixes": [],
            "virtualInterfaceName": "MyVirtualInterface",
            "virtualInterfaceState": "pending",
            "customerAddress": "[PROTECTED]",
            "vlan": 123,
            "ownerAccount": "123456789012",
            "amazonAddress": "[PROTECTED]",
            "connectionId": "dxcon-fhajolyy",
            "location": "EqSE2"
        }
    },
    ...
  ]
}
```

Example 範例：DescribeConnections

```
{
    "Records": [
    {
        "eventVersion": "1.0",
        "userIdentity": {
            "type": "IAMUser",
```

```
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::123456789012:user/Alice",
            "accountId": "123456789012",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice",
            "sessionContext": {
                "attributes": {
                    "mfaAuthenticated": "false",
                    "creationDate": "2014-04-04T12:23:05Z"
                }
            }
        },
        "eventTime": "2014-04-04T17:27:28Z",
        "eventSource": "directconnect.amazonaws.com",
        "eventName": "DescribeConnections",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "127.0.0.1",
        "userAgent": "Coral/Jakarta",
        "requestParameters": null,
        "responseElements": null
    },
    ...
  ]
}
```

Example 範例：DescribeVirtualInterfaces

```
{
    "Records": [
    {
        "eventVersion": "1.0",
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::123456789012:user/Alice",
            "accountId": "123456789012",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice",
            "sessionContext": {
                "attributes": {
                    "mfaAuthenticated": "false",
                    "creationDate": "2014-04-04T12:23:05Z"
                }
```

```
            }
        },
        "eventTime": "2014-04-04T17:37:53Z",
        "eventSource": "directconnect.amazonaws.com",
        "eventName": "DescribeVirtualInterfaces",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "127.0.0.1",
        "userAgent": "Coral/Jakarta",
        "requestParameters": {
            "connectionId": "dxcon-fhajolyy"
        },
        "responseElements": null
    },
    ...
  ]
}
```

監控 AWS Direct Connect 資源

監控是維護 Direct Connect 資源可靠性、可用性和效能的重要部分。您應該從 AWS 解決方案的所有部分收集監控資料，以便在發生多點故障時更輕鬆地偵錯。開始監控 Direct Connect 之前，您應該建立監控計畫，其中包含下列問題的答案：

- 監控目標是什麼？
- 應該監控哪些資源？
- 應多久一次監控這些資源？
- 可使用哪些監控工具？
- 誰會執行監控任務？
- 發生問題時應該通知誰？

下一個步驟是建立環境中正常 Direct Connect 效能的基準，方法是測量各種時間和不同負載條件下的效能。當您監控 Direct Connect 時，請存放歷史監控資料。如此做，您才能與目前的效能資料做比較、辨識正常效能模式和效能異常狀況、規劃問題處理方式。

若要建立基準，您應該監控實體 Direct Connect 連線的使用情況、狀態和運作狀態。

目錄

- 監控工具
- 使用 Amazon CloudWatch 監控

監控工具

AWS 提供各種工具，您可以用來監控 AWS Direct Connect 連線。您可以設定其中一些工具來進行監控，但有些工具需要手動介入。建議您盡可能自動化監控任務。

自動化監控工具

您可以使用下列自動化監控工具來監看 Direct Connect，並在發生錯誤時回報：

- Amazon CloudWatch 警示 – 在您指定的一段時間內監看單一指標。根據在數個期間與指定閾值相關的指標值，執行一個或多個動作。動作是傳送至 Amazon SNS 主題的通知。CloudWatch 警示不會

只因處於特定狀態就叫用動作，狀態必須已變更並已維持一段指定的時間。如需可用指標和維度的相關資訊，請參閱 使用 Amazon CloudWatch 監控 。

- AWS CloudTrail 日誌監控 – 透過將日誌檔案傳送至 CloudWatch Logs，在帳戶之間共用日誌檔案並即時監控 CloudTrail 日誌檔案。 CloudWatch 您也能夠以 Java 應用程式語言撰寫日誌記錄處理應用程式的方式、驗證日誌檔在由 CloudTrail 交付後並沒有發生改變。如需詳細資訊，請參閱 記錄 API 呼叫 和《AWS CloudTrail 使用者指南》中的使用 CloudTrail 記錄檔案。

手動監控工具

監控 AWS Direct Connect 連線的另一個重要部分包括手動監控 CloudWatch 警示未涵蓋的項目。Direct Connect 和 CloudWatch 主控台儀表板提供at-a-glance。 AWS

- AWS Direct Connect 主控台會顯示：
  - 連線狀態 (請參閱 State (狀態) 欄)
  - 虛擬介面狀態 (請參閱狀態直欄)
- CloudWatch 首頁會顯示：
  - 目前警示與狀態
  - 警示與資源的圖表
  - 服務運作狀態

  此外，您可以使用 CloudWatch 執行下列動作：
  - 建立自訂儀表板來監控您關心的服務。
  - 用於疑難排解問題以及探索驅勢的圖形指標資料。
  - 搜尋並瀏覽所有 AWS 資源指標。
  - 建立與編輯要通知發生問題的警示。

使用 Amazon CloudWatch 監控

您可以使用 CloudWatch 監控實體 AWS Direct Connect 連線和虛擬介面。CloudWatch 會從 Direct Connect 收集原始資料，並將其處理為可讀取的指標。根據預設，CloudWatch 會以 5 分鐘的間隔提供 Direct Connect 指標資料。每個間隔中的指標資料是該間隔期間至少收集兩個樣本的彙總。

如需有關 CloudWatch 的詳細資訊，請參閱《Amazon CloudWatch 使用者指南》。您也可以監控您的服務 CloudWatch，以瞭解哪些服務正在使用資源。如需詳細資訊，請參閱AWS 發佈 CloudWatch 指標的 服務。

目錄

- AWS Direct Connect 指標和維度
- View AWS Direct Connect CloudWatch 指標
- 建立 Amazon CloudWatch 警示以監控 AWS Direct Connect 連線

AWS Direct Connect 指標和維度

指標可用於 AWS Direct Connect 實體連線和虛擬界面。

AWS Direct Connect 連線指標

下列指標可從 Direct Connect 專用連線取得。

指標	描述
ConnectionState	連線的狀態 1 表示啟動，0 表示關閉。 此指標適用於專用和託管連線。 **Note** 除了連線擁有者帳戶之外，託管虛擬介面擁有者帳戶也可以使用此指標。 單位：此指標不會傳回任何單位。
ConnectionBpsEgress	從連線 AWS 端傳出資料的位元速率。 回報的數字是指定時段的彙總數字 (平均值) (預設為 5 分鐘，最少 1 分鐘)。您可以變更預設彙總。 新連線或裝置重新開機時，此指標可能無法使用。當使用連線來傳送或接收流量時，指標便會開始。 單位：位元/秒
ConnectionBpsIngress	傳入資料的位元速率至連線的 AWS 端。

指標	描述
	新連線或裝置重新開機時，此指標可能無法使用。當使用連線來傳送或接收流量時，指標便會開始。 單位：位元/秒
ConnectionPpsEgress	` 從連線 AWS 端傳出資料的封包速率。 回報的數字是指定時段的彙總數字 (平均值) (預設為 5 分鐘，最少 1 分鐘)。您可以變更預設彙總。 新連線或裝置重新開機時，此指標可能無法使用。當使用連線來傳送或接收流量時，指標便會開始。 單位：封包/秒
ConnectionPpsIngress	傳入資料的封包速率至連線的 AWS 端。 回報的數字是指定時段的彙總數字 (平均值) (預設為 5 分鐘，最少 1 分鐘)。您可以變更預設彙總。 新連線或裝置重新開機時，此指標可能無法使用。當使用連線來傳送或接收流量時，指標便會開始。 單位：封包/秒
ConnectionCRCErrorCount	此計數已不再使用。請改用 ConnectionErrorCount 。

指標	描述
ConnectionErrorCount	AWS 裝置上所有類型之 MAC 層級錯誤的錯誤總計。總計包括循環冗餘檢查 (CRC) 錯誤。 此指標是從最後一個報告資料點之後發生的錯誤計數。當介面發生錯誤時，指標會回報非零的值。若要取得 CloudWatch 中所選間隔的所有錯誤總數，例如 5 分鐘，請套用「總和」統計資料。 當介面上的錯誤停止時，指標值會設為 0。 **Note** 此指標會取代 ConnectionCRCError Count （已不再使用)。 單位：計數
ConnectionLightLevelTx	指出從連線 AWS 端傳出（傳出）流量的光纖連線運作狀態。 此指標有兩個維度。如需詳細資訊，請參閱Direct Connect 可用維度。 單位：dBm
ConnectionLightLevelRx	指出傳入（傳入）流量至連線 AWS 端的光纖連線運作狀態。 此指標有兩個維度。如需詳細資訊，請參閱Direct Connect 可用維度。 單位：dBm

指標	描述
ConnectionEncryptionState	表示連線加密狀態。1 表示連線加密為 up，0 表示連線加密為 down。將此指標套用至 LAG 時，1 表示 LAG 中的所有連線都具有加密 up。0 表示至少有一個 LAG 連線加密為 down。

AWS Direct Connect 虛擬介面指標

下列指標可從 AWS Direct Connect 虛擬介面取得。

指標	描述
VirtualInterfaceBpsEgress	從虛擬界面的 AWS 端傳出資料的位元速率。 回報的數字是指定時段的彙總數字 (平均值) (預設為 5 分鐘)。 單位：位元/秒
VirtualInterfaceBpsIngress	傳入資料至虛擬界面 AWS 端的位元速率。 回報的數字是指定時段的彙總數字 (平均值) (預設為 5 分鐘)。 單位：位元/秒
VirtualInterfacePpsEgress	從虛擬介面的 AWS 端傳出資料的封包速率。 回報的數字是指定時段的彙總數字 (平均值) (預設為 5 分鐘)。 單位：封包/秒
VirtualInterfacePpsIngress	傳入資料至虛擬介面 AWS 端的封包速率。 回報的數字是指定時段的彙總數字 (平均值) (預設為 5 分鐘)。

指標	描述
	單位：封包/秒

AWS Direct Connect 可用維度

您可以使用下列維度來篩選 AWS Direct Connect 資料。

維度	描述
`ConnectionId`	此維度適用於 Direct Connect 連線和虛擬界面的指標。此維度可藉由此連線來篩選資料。
`OpticalLaneNumber`	此維度會篩選`ConnectionLightLevelTx` 資料和`ConnectionLightLevelRx` 資料，並依 Direct Connect 連線的光學通道號碼篩選資料。
`VirtualInterfaceId`	此維度可用於 Direct Connect 虛擬界面的指標，並依虛擬界面篩選資料。

主題

- View AWS Direct Connect CloudWatch 指標
- 建立 Amazon CloudWatch 警示以監控 AWS Direct Connect 連線

View AWS Direct Connect CloudWatch 指標

AWS Direct Connect 會傳送有關 Direct Connect 連線的下列指標。然後，Amazon CloudWatch 會將這些資料點彙總為 1 分鐘或 5 分鐘的間隔。根據預設，Direct Connect 指標資料會以 5 分鐘的間隔寫入 CloudWatch。

> **Note**
>
> 透過 CloudWatch 監控 Direct Connect 時，您可以每隔 1 分鐘請求指標。不過，實際更新頻率是由 CloudWatch 控制。由於 CloudWatch 控制間隔，因此 Direct Connect 無法保證間隔少於五分鐘。

您可以使用下列程序來檢視 Direct Connect 連線的指標。

使用 CloudWatch 主控台檢視指標

指標會先依服務命名空間分組，再依各命名空間內不同的維度組合分類。如需有關使用 Amazon CloudWatch 檢視 Direct Connect 指標 (包含新增數學函數或預先建置的查詢) 的詳細資訊，請參閱 Amazon CloudWatch 使用者指南中的使用 Amazon CloudWatch 指標。

1. 透過 https://console.aws.amazon.com/cloudwatch/ 開啟 CloudWatch 主控台。
2. 在導覽窗格中，選擇 Metrics (指標)，然後選擇 All metrics (所有指標)。
3. 在「指標」區段中，選擇「DX」。
4. 選擇「ConnectionId」或「指標名稱」，然後選擇下列任一項目來進一步定義指標：
   - 新增至搜尋 - 將此指標新增至您的搜尋結果。
   - 僅搜尋此項目 - 僅搜尋此指標。
   - 從圖表中移除 - 從圖表中移除此指標。
   - 僅繪製此指標 - 僅繪製此指標。
   - 繪製所有搜尋結果 - 繪製所有指標。
   - 使用 SQL 查詢繪製圖表 - 開啟 Metric Insights 查詢建置器，可讓您透過建立 SQL 查詢來選擇要繪製圖表的內容。如需使用 Metric Insights 的詳細資訊，請參閱 Amazon CloudWatch 使用者指南中的使用 CloudWatch Metric Insights 查詢指標。

使用 AWS Direct Connect 主控台檢視指標

1. 在 https：//https://console.aws.amazon.com/directconnect/v2/home 開啟 AWS Direct Connect主控台。
2. 在導覽窗格中，選擇 Connections (連線)。
3. 選取連線。
4. 選擇監控索引標籤以顯示連線的指標。

使用 檢視指標 AWS CLI

在命令提示中，使用下列命令。

```
aws cloudwatch list-metrics --namespace "AWS/DX"
```

建立 Amazon CloudWatch 警示以監控 AWS Direct Connect 連線

您可以建立 CloudWatch 警報，在警示變更狀態時傳送 Amazon SNS 訊息。警示會在您指定的期間監看單一指標。警報會根據在數個期間與指定閾值相關的指標值，傳送通知給 Amazon SNS 主題。

例如，您可以建立用於監控 AWS Direct Connect 連接狀態的警示。當連線狀態處於連續五個連續 1 分鐘期間為關閉時，便會傳送通知。如需建立警示的詳細資訊，請參閱 Amazon CloudWatch 使用者指南中的使用 Amazon CloudWatch 警示。

建立 CloudWatch 警示。

1. 透過 https://console.aws.amazon.com/cloudwatch/ 開啟 CloudWatch 主控台。
2. 在導覽窗格中，選擇 Alarms (警示)，然後選擇 All alarms (所有警示)。
3. 選擇建立警示 。
4. 選擇選取指標，然後選擇 DX。
5. 選擇「連線指標」指標。
6. 選取 AWS Direct Connect 連線，然後選擇選取指標指標。
7. 在指定指標和條件頁面上，設定警示的參數。如需取得更多指定指標與條件，請參閱《Amazon CloudWatch 使用者指南》中的使用 Amazon CloudWatch 警示。
8. 選擇 Next (下一步)。
9. 在設定動作頁面上設定警示動作。如需設定警示動作的詳細資訊，請參閱 Amazon CloudWatch 使用者指南中的警示動作。
10. 選擇 Next (下一步)。
11. 在新增名稱和描述頁面上，輸入名稱和選用的警示描述來描述此警示，然後選擇下一步。
12. 在預覽和建立頁面上確認提出的警示。
13. 如果需要，請選擇「編輯」來變更任何資訊，然後選擇「建立警示」。

    警示頁面會顯示新的資料列，其中包含新警示的相關資訊。「動作」狀態會顯示「已啟用動作」，表示警示處於作用中。

AWS Direct Connect 配額

下表列出與 相關的配額 AWS Direct Connect。

元件	配額	說明
每個 AWS Direct Connect 專用連線的私有或公有虛擬介面	50	此限制無法提高。
每個 AWS Direct Connect 專用連線的傳輸虛擬介面。 傳輸虛擬介面可用來連線至 Transit Gateway 或 AWS Cloud WAN 核心網路。如需詳細資訊，請參閱閘道。	4	請聯絡您的解決方案架構師 (SA) 或技術客戶經理 (TAM) 以取得進一步協助。
每個 AWS Direct Connect 專用連線的私有或公有虛擬介面，以及每個 AWS Direct Connect 專用連線的傳輸虛擬介面	51	啟動 Amazon VPC Transit Gateways AWS Direct Connect 支援時，會將一 (1) 個傳輸虛擬介面的配額新增至每個專用連線 50 個私有或公有虛擬介面的配額。允許的傳輸虛擬介面數目現在為四 (4) 個，並計入每個專用連線 51 個虛擬介面的上限。此限制無法提高。
每個 AWS Direct Connect 託管連線的私有、公有或傳輸虛擬介面	1	此限制無法提高。
每個帳戶每個區域每個 Direct Connect 位置的作用中 AWS Direct Connect 連線數	10	請聯絡您的解決方案架構師 (SA) 或技術客戶經理 (TAM) 以取得進一步協助。
每個鏈路彙整群組 (LAG) 的虛擬介面數量	54	啟動對 Amazon VPC Transit Gateways 的 AWS Direct Connect 支援時，會將一 (1) 個傳輸虛擬介面的配額新增至每個 LAG 50 個私有或公有虛擬介面的配額。允許的傳輸虛擬介面數目現在為四 (4) 個，並計入每個 LAG 的 51 個虛擬介面之上限。此限制無法提高。

元件	配額	說明
私有虛擬介面上每個邊界閘道協定 (BGP) 工作階段的路由，或從內部部署傳輸虛擬介面到 AWS。 如果您在整個 BGP 工作階段為 IPv4 和 IPv6 公告超過 100 個路由，此 BGP 工作階段將進入閒置狀態且 BGP 工作階段關閉。	IPv4 和 IPv6 各 100	請聯絡您的解決方案架構師 (SA) 或技術客戶經理 (TAM) 以取得進一步協助。
公有虛擬介面上每一邊界閘道協定 (BGP) 工作階段的路由數目	1,000	此限制無法提高。
每一鏈路彙整群組 (LAG) 的專用連線	4 當連接埠速度小於 100G 時 2 當連接埠速度為 100G 時	
每一區域的鏈路彙整群組 (LAG)	10	請聯絡您的解決方案架構師 (SA) 或技術客戶經理 (TAM) 以取得進一步協助。
AWS Direct Connect 每個帳戶的閘道數	200	請聯絡您的解決方案架構師 (SA) 或技術客戶經理 (TAM) 以取得進一步協助。
每個閘道的虛擬私有 AWS Direct Connect 閘道	20	此限制無法提高。
每個閘道的傳輸 AWS Direct Connect 閘道數	6	此限制無法提高。

元件	配額	說明
從 AWS Cloud WAN 核心網路 Direct Connect 閘道連接至內部部署的公告路由字首數目上限。 Note 連接到該 Direct Connect 閘道的所有傳輸虛擬介面都會收到核心網路公告的所有路由字首。	5,000	請聯絡您的解決方案架構師 (SA) 或技術客戶經理 (TAM) 以取得進一步協助。
每個 AWS Direct Connect 閘道的虛擬介面 （私有或傳輸）	30	此限制無法提高。
傳輸虛擬介面上每個 AWS Transit Gateway 從 AWS 到內部部署的字首數量	IPv4 和 IPv6 合計 200	請聯絡您的解決方案架構師 (SA) 或技術客戶經理 (TAM) 以取得進一步協助。
每個虛擬私有閘道的虛擬介面數目	沒有限制。	
與傳輸閘道關聯的 Direct Connect 閘道數量	20	此限制無法提高。
SiteLink 字首限制	100	請聯絡您的解決方案架構師 (SA) 或技術客戶經理 (TAM) 以取得進一步協助。

AWS Direct Connect 透過單模光纖支援這些連接埠速度：1 Gbps：1000BASE-LX (1310 nm)、10 Gbps：10GBASE-LR (1310 nm)、100Gbps：100GBASE-LR4 和 400 Gbps：400GBASE-LR4。

BGP 配額

以下是 BGP 配額。BGP 計時器會交涉至路由器之間的最低值。BFD 間隔由最慢的裝置定義。

- 預設保留計時器：90 秒
- 最短保留計時器：3 秒

不支援保留值為 0。

- 預設保持連線計時器：30 秒
- 最短保持連線計時器：1 秒
- 正常重新啟動計時器：120 秒

建議您不要同時設定正常重新啟動和 BFD。

- BFD 存活偵測最短間隔：300 毫秒
- BFD 最小乘數：3

負載平衡考量

如果您想要搭配多個公有 VIF 使用負載平衡 , 所有 VIF 必須位於相同區域。

故障診斷 AWS Direct Connect

下列疑難排解資訊有助於您就 AWS Direct Connect 連線的問題進行診斷與修正。

內容

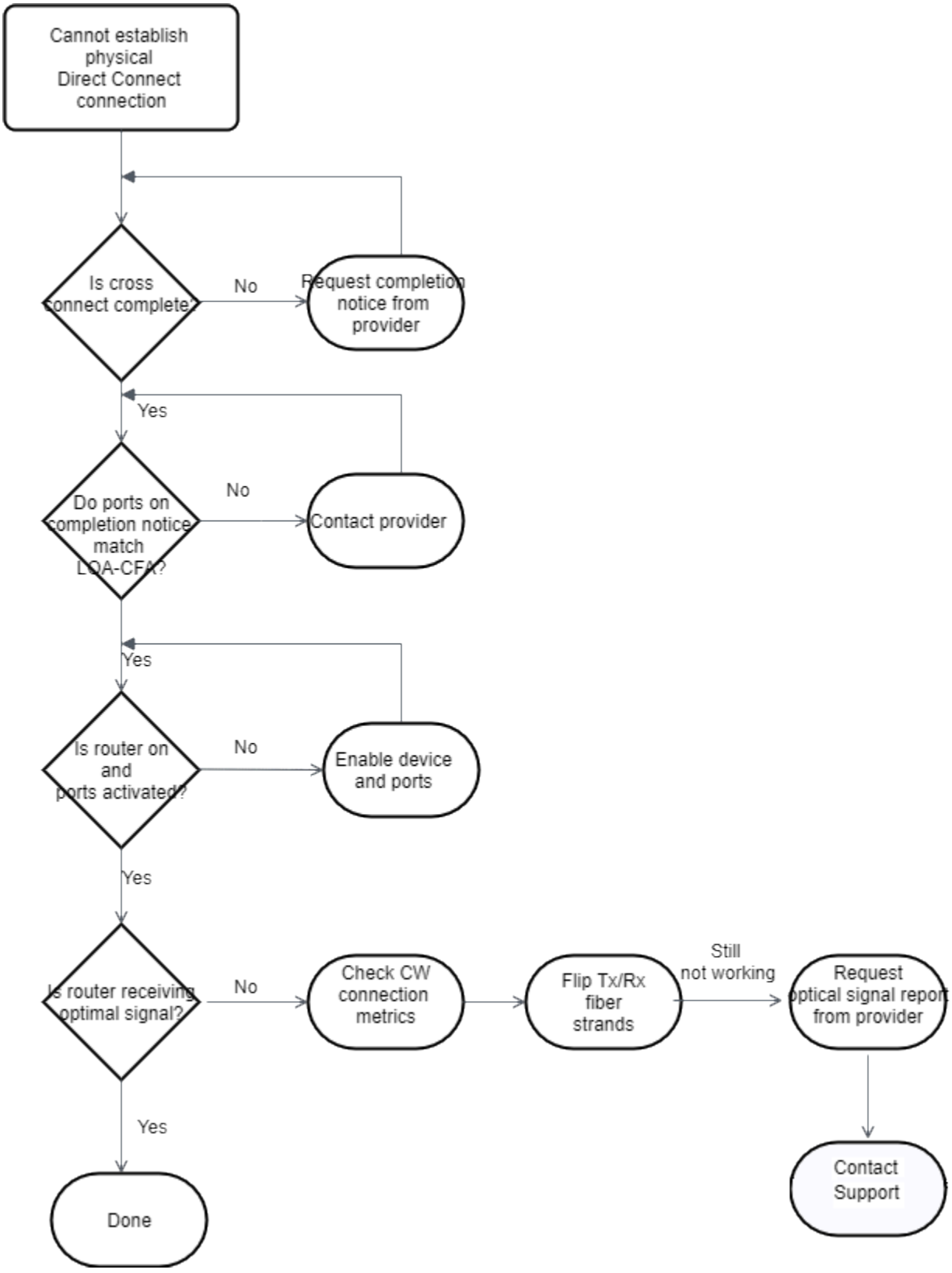
- 診斷排解第 1 層 (實體) 問題
- 診斷排解第 2 層 (資料鏈路) 問題
- 診斷排解第 3/4 層 (網路/傳輸) 問題
- 疑難排解路由問題

診斷排解第 1 層 (實體) 問題

如果您或您的網路提供者無法建立與 AWS Direct Connect 裝置的實體連線，請使用下列步驟對問題進行疑難排解。

1. 向主機代管服務供應商確認是否已完成交叉連接。請主機代管服務供應商或網路供應商向您提供交叉連接完成通知，收到後將連接埠與 LOA-CFA 所列的連接埠進行比對。
2. 確認您的路由器或供應商的路由器是否開機，連接埠是否已啟用。
3. 確保路由器使用正確的光學收發器。如果您有連接埠速度大於 1 Gbps 的連線，則必須停用連接埠的自動交涉。不過，根據為您的連線提供服務的 AWS Direct Connect 端點，可能需要啟用或停用 1 Gbps 連線的自動交涉。如果您的連線需要停用自動交涉功能，則必須手動設定連接埠速度和全雙工模式。如果您的虛擬介面仍未開通，請參閱 診斷排解第 2 層 (資料鏈路) 問題。視連線終止的 Direct Connect 端點而定，可能需要相應地啟用或停用自動交涉。
4. 確認路由器是否正透過交叉連接，接收夠強的光訊號。
5. 嘗試翻轉 (又稱為滾動) Tx/Rx 光纖索股。
6. 檢查 的 Amazon CloudWatch 指標 AWS Direct Connect。您可以驗證 AWS Direct Connect 裝置的 Tx/Rx 光學讀數 (1 Gbps 和 10 Gbps)、實體錯誤計數和操作狀態。如需詳細資訊，請參閱透過 Amazon CloudWatch 進行監控。
7. 聯繫主機代管服務供應商以申請一份跨交叉連接的 Tx/Rx 光訊號書面報告。
8. 若上述步驟未能解決實體連線問題，請聯絡 AWS 支援 並向其提供由主機代管服務供應商給予的交叉連接完成通知以及光訊號報告。

以下流程圖包含診斷實體連線問題的步驟。

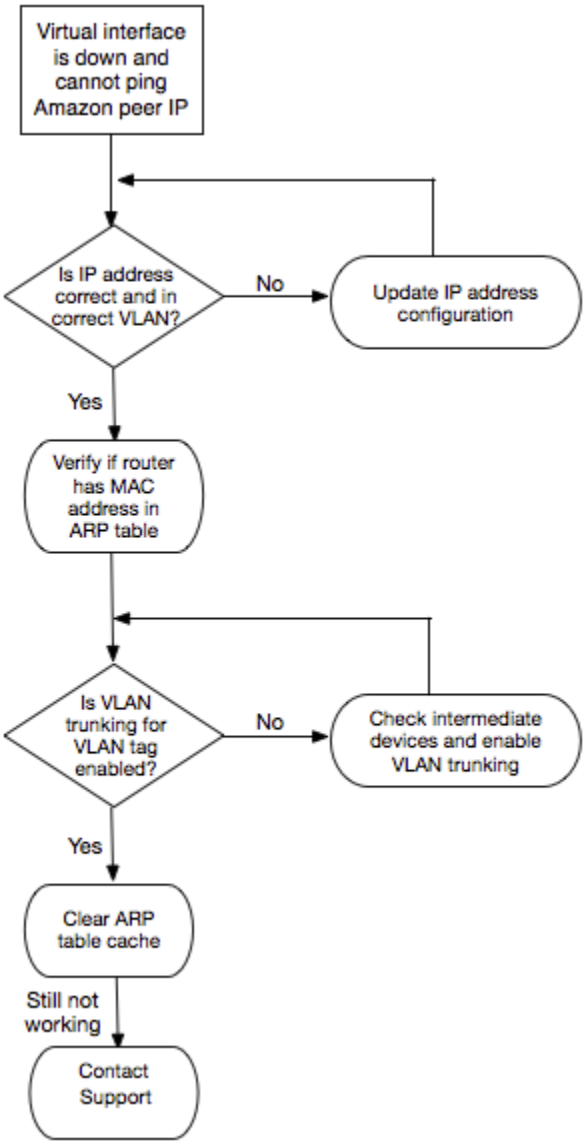

Cannot establish physical Direct Connect connection
Is cross connect complete?
No
Request completion notice from provider
Yes
Do ports on completion notice match LOA-CFA?
No
Contact provider
Yes
Is router on and ports activated?
No
Enable device and ports
Yes
Is router receiving optimal signal?
No
Check CW connection metrics
Flip Tx/Rx fiber strands
Still not working
Request optical signal report from provider
Contact Support
Yes
Done

診斷排解第 2 層 (資料鏈路) 問題

如果您的 AWS Direct Connect 實體連線已啟動，但您的虛擬介面已停機，請使用下列步驟對問題進行故障診斷。

1. 若您無法 ping 到 Amazon 對等 IP 地址，請確認您的對等 IP 地址已正確設定且位於正確的 VLAN。確定該 IP 地址是設定在 VLAN 子介面而非實體介面 (例如，GigabitEthernet0/0.123 而不是 GigabitEthernet0/0)。
2. 驗證路由器是否有來自您地址解析通訊協定 (ARP) 資料表中 AWS 端點的 MAC 地址項目。
3. 確定各端點間的任何中介裝置皆已針對您的 802.1Q VLAN 標籤啟用 VLAN 中繼。在 AWS 收到標記的流量之前，無法在 AWS 端建立 ARP。
4. 清除您本身或是供應商的 ARP 表快取。
5. 如果上述步驟未建立 ARP，或者您仍然無法 ping Amazon 對等 IP，請聯絡 AWS Support。

以下流程圖包含診斷資料鏈路問題的步驟。



若查驗上述步驟後仍無法建立 BGP 工作階段，請參閱診斷排解第 3/4 層 (網路/傳輸) 問題。若 BGP 工作階段已建立但路由發生問題，請參閱疑難排解路由問題。

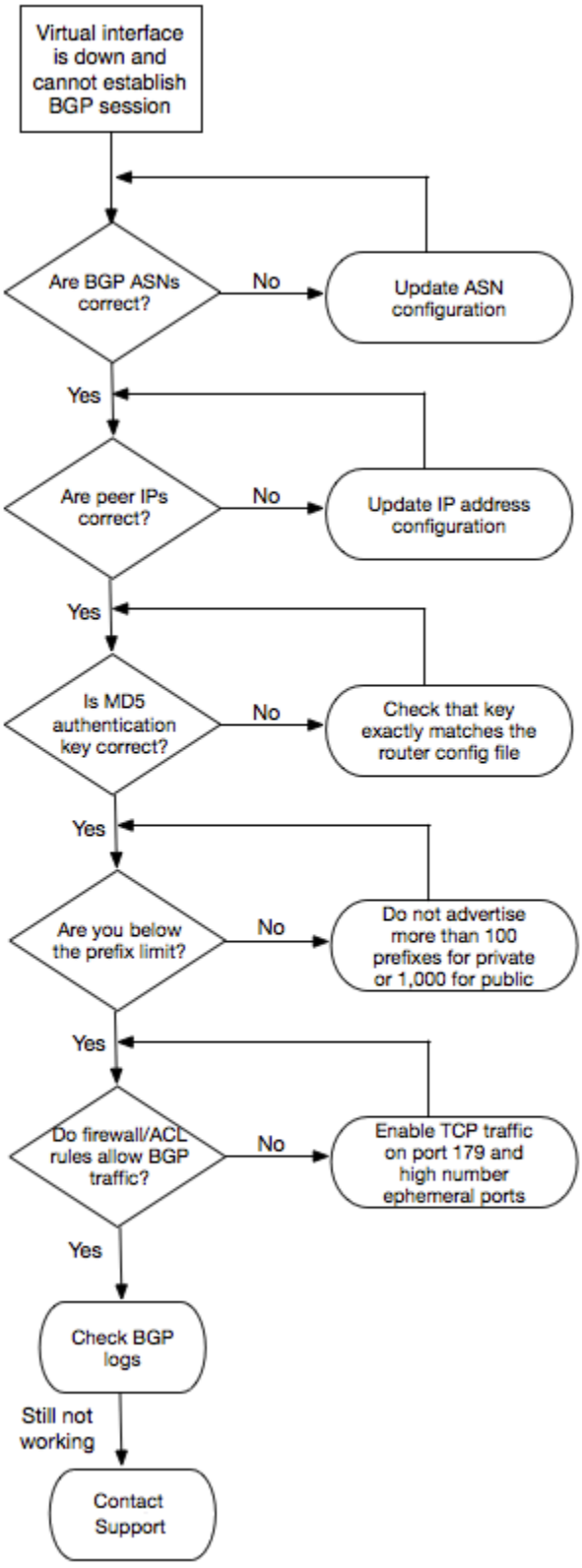
診斷排解第 3/4 層 (網路/傳輸) 問題

假設您的 AWS Direct Connect 實體連線正常，而且您可以 ping Amazon 對等 IP 地址。如果您的虛擬介面已啟動，且無法建立 BGP 對等互連工作階段，請使用下列步驟對問題進行疑難排解：

1. 確定您的 BGP 本地自發系統編號 (ASN) 和 Amazon 的 ASN 皆已正確設定。
2. 確定 BGP 對等工作階段兩端的對等 IP 皆已正確設定。

3. 確定您的 MD5 身分驗證金鑰已設定妥，與下載的路由器組態檔案中的金鑰完全相符。確認無任何多餘的空格或字元。
4. 確認您本身或是供應商就私有虛擬介面所公告的字首未超過 100 個，就公有虛擬介面所公告的字首未超過 1,000 個。此為硬性限制，不得超出。
5. 確定無任何防火牆或 ACL 規則封鎖了 TCP 連接埠 179 或任何高埠號的暫時性 TCP 連接埠。BGP 在各個對等之間建立 TCP 連線需要這些連接埠。
6. 檢查您的 BGP 日誌是否有任何錯誤或警告訊息。
7. 如果上述步驟未建立 BGP 互連工作階段，請聯絡 AWS Support。

以下流程圖包含診斷 BGP 對等工作階段問題的步驟。



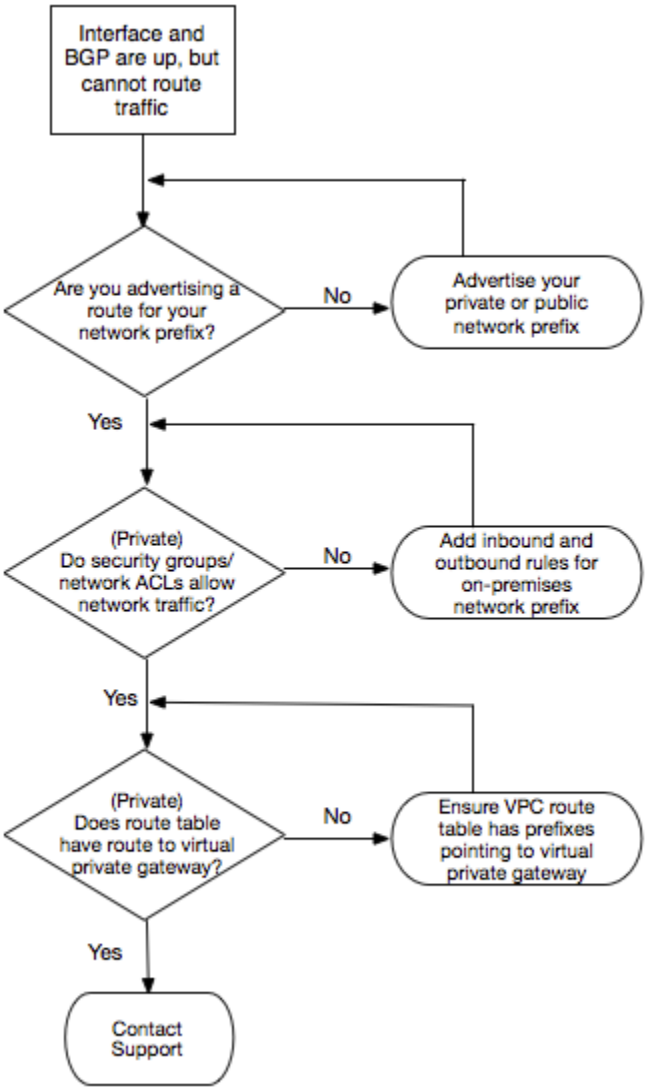
若 BGP 對等工作階段已建立但路由發生問題，請參閱[疑難排解路由問題](#)。

疑難排解路由問題

假設一種情況，您的虛擬介面連線正常，而且您已建立 BGP 對等工作階段。如果您無法透過虛擬介面路由流量，請使用下列步驟來排除問題：

1. 確定您是透過 BGP 工作階段為您的現場部署網路字首公告路由。若為私有虛擬介面，其對象可以是私有或公有網路字首。若為公有虛擬介面，則必須是公共可路由的網路字首。
2. 對於私有虛擬介面，確定您的 VPC 安全群組和網路 ACL 允許由您的現場部署網路字首傳入及傳出流量。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的安全群組和網路 ACL。
3. 對於私有虛擬介面，確定您的 VPC 路由表已填上字首指向該私有虛擬介面所連接的虛擬私有閘道。例如，若您希望預設情況下將所有流量路由至您的現場部署網路，即可在 VPC 路由表中加入預設路由 (0.0.0.0/0 或 ::/0) 以此虛擬私有閘道為目標。
   - 或者啟用路由傳播，使路由表根據您的動態 BGP 路由公告自動更新路由。每個路由表最多可有 100 個傳播路由。此限制無法提高。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的啟用和停用路由傳播。
4. 如果上述步驟無法解決您的轉接問題，請聯絡 AWS Support。

以下流程圖包含診斷路由問題的步驟。


Interface and BGP are up, but cannot route traffic
Are you advertising a route for your network prefix?
No
Advertise your private or public network prefix
Yes
(Private) Do security groups/ network ACLs allow network traffic?
No
Add inbound and outbound rules for on-premises network prefix
Yes
(Private) Does route table have route to virtual private gateway?
No
Ensure VPC route table has prefixes pointing to virtual private gateway
Yes
Contact Support

文件歷史紀錄

下表說明 的版本 AWS Direct Connect。

功能	描述	日期
在 Direct Connect 閘道與 AWS Network Manager 核心網路之間建立關聯	您現在可以直接在 Direct Connect 和 AWS Cloud WAN 核心網路之間建立 Direct Connect 閘道關聯。如需詳細資訊，請參閱 雲端 WAN 核心網路關聯。	2024-11-25
支援 400G	更新主題以包含對 400G 連線的支援。	2024-07-18
新增 SiteLink 字首限制	SiteLink 的字首限制已新增至 Direct Connect 配額。	2023-06-15
SiteLink 的支援	您可以建立虛擬私有介面，以在同一 AWS 區域中啟用兩個 Direct Connect 存在點 (PoPs之間的連線。如需詳細資訊，請參閱 託管 AWS Direct Connect 虛擬介面。	2021-12-01
支援 MAC Security	您可以使用支援 MACsec 的 AWS Direct Connect 連線，將資料從公司資料中心加密到 AWS Direct Connect 位置。如需詳細資訊，請參閱MAC 安全性 (MACsec)。	2021-03-31
支援 100G	已更新主題，納入了對 100G 專用連線的支援。	2021-02-12
在義大利的新據點	已更新主題，納入了在義大利增設的新據點。如需詳細資訊，請參閱the section called “歐洲 (米蘭)”。	2021-01-22
在以色列的新據點	更新主題，包含在以色列增加新的據點。如需詳細資訊，請參閱the section called “以色列 (特拉維夫)”。	2020-07-07
彈性工具組容錯移轉測試支援	使用「彈性工具組容錯移轉測試」功能來測試連線能力的彈性。如需詳細資訊，請參閱the section called “Direct Connect 容錯移轉測試”。	2020-06-03

功能	描述	日期
CloudWatch VIF 指標支援	您可以使用 CloudWatch 監控實體 AWS Direct Connect 連線和虛擬介面。如需詳細資訊，請參閱the section called “使用 Amazon CloudWatch 監控 ”。	2020-05-11
AWS Direct Connect 彈性工具組	AWS Direct Connect 彈性工具組提供具有多個彈性模型的連線精靈，可協助您訂購專用連線，以實現 SLA 目標。如需詳細資訊，請參閱AWS Direct Connect 彈性工具組。	2019-10-07
AWS Transit Gateway 跨帳戶支援的額外區域支援	如需相關資訊，請參閱 the section called “傳輸閘道關聯”。	2019-09-30
AWS Direct Connect 的支援 AWS Transit Gateway	您可以使用AWS Direct Connect 閘道，透過傳輸虛擬介面將 AWS Direct Connect 連線連接到連接到傳輸閘道VPCs 或 VPNs。您將 Direct Connect 閘道與傳輸閘道建立關聯。然後，為您的 Direct Connect 閘道連線建立傳輸虛擬介面 AWS Direct Connect 。如需相關資訊，請參閱 the section called “傳輸閘道關聯”。	2019-03-27
巨型訊框支援	您可以傳送巨型訊框 (9001 MTU) AWS Direct Connect。如需詳細資訊，請參閱私有虛擬介面或傳輸虛擬介面的 MTUs 。	2018-10-11
本地偏好 BGP 社群	您可以利用本地偏好 BGP 社群標籤，實現網路傳入流量的負載平衡和路由偏好。如需詳細資訊，請參閱本地偏好 BGP 社群。	2018-02-06
AWS Direct Connect 閘道	您可以使用 Direct Connect 閘道將 AWS Direct Connect 連線連線至遠端區域中VPCs。如需詳細資訊，請參閱AWS Direct Connect 閘道。	2017-11-01
Amazon CloudWatch 指標	您可以檢視 AWS Direct Connect 連線的 CloudWatch 指標。如需詳細資訊，請參閱使用 Amazon CloudWatch 監控 。	2017-06-29
鏈路彙整群組	您可以建立鏈路彙整群組 (LAG) 來彙整多個 AWS Direct Connect 連線。如需詳細資訊，請參閱AWS Direct Connect 連結彙總群組 (LAGs)。	2017-02-13

功能	描述	日期
IPv6 支援	您的虛擬介面現已支援 IPv6 BGP 對等工作階段。如需詳細資訊，請參閱將 BGP 對等新增至 AWS Direct Connect 虛擬介面。	2016-12-01
標籤支援	您現在可以標記 AWS Direct Connect 資源。如需詳細資訊，請參閱標記 AWS Direct Connect 資源。	2016-11-04
自助式 LOA-CFA	您現在可以使用 AWS Direct Connect 主控台或 API 下載授權與連線設施指派 (LOA-CFA)。	2016-06-22
矽谷增設新據點	已更新主題，納入了在美國西部 (加利佛尼亞北部) 區域的矽谷增設的新據點。	2016-06-03
阿姆斯特丹增設新據點	已更新主題，納入了在歐洲 (法蘭克福) 區域的阿姆斯特丹增設的新據點。	2016-05-19
奧勒岡州波特蘭及新加坡增設新據點	已更新主題，納入了在美國西部 (奧勒岡) 區域的奧勒岡州波特蘭及亞太區域 (新加坡) 區域的新加坡增設的新據點。	2016-04-27
巴西聖保羅增設新據點	已更新主題，納入了在南美洲 (聖保羅) 區域的聖保羅增設的新據點。	2015-12-09
達拉斯、倫敦、矽谷及孟買增設新據點	更新主題，以包含新增達拉斯（美國東部（維吉尼亞北部）區域）、倫敦（歐洲（愛爾蘭）區域）、矽谷 (AWS GovCloud（美國西部）區域）和孟買（亞太區域（新加坡）區域）的新據點。	2015-11-27
中國 (北京) 區域的新據點	已更新主題，納入了在中國 (北京) 區域的北京增設的新據點。	2015-04-14
美國西部 (奧勒岡) 區域的拉斯維加斯增設新據點	更新主題，以包含在美國西部（奧勒岡）區域新增 AWS Direct Connect 的拉斯維加斯據點。	2014-11-10
新增歐洲 (法蘭克福) 區域	更新主題，以包含新增服務歐盟（法蘭克福）區域的新 AWS Direct Connect 據點。	2014-10-23

功能	描述	日期
亞太區域 (雪梨) 區域增設新據點	更新主題，以包含新增服務亞太區域 （ 雪梨 ） 區域的新 AWS Direct Connect 據點。	2014-07-14
的支援 AWS CloudTrail	新增了主題，說明如何使用 CloudTrail 來記錄 AWS Direct Connect中的活動。如需詳細資訊，請參閱使用 記錄 AWS Direct Connect API 呼叫 AWS CloudTrail。	2014-04-04
支援存取遠端 AWS 區域	增加了一個新主題，說明如何存取位於遠端區域的公有資源。如需詳細資訊，請參閱存取遠端 AWS Direct Connect 區域。	2013-12-19
支援託管連線	已更新主題，納入了對託管連線的支援。	2013-10-22
歐洲 (愛爾蘭) 區域增設新據點	更新主題，以包含新增服務於歐洲 （ 愛爾蘭 ） 區域的新 AWS Direct Connect 據點。	2013-06-24
美國西部 (奧勒岡) 區域的西雅圖增設新據點	更新主題，以包含新增在西雅圖為美國西部 （ 奧勒岡 ） 區域提供服務的新 AWS Direct Connect 據點。	2013-05-08
支援搭配使用 IAM AWS Direct Connect	新增使用 AWS Identity and Access Management 搭配 的主題 AWS Direct Connect。如需詳細資訊，請參閱the section called “身分和存取權管理”。	2012-12-21
新增亞太區域 (雪梨) 區域	更新主題，以包含新增服務亞太區域 （ 雪梨 ） 區域的新 AWS Direct Connect 據點。	2012-12-14

功能	描述	日期
新的 AWS Direct Connect 主控台，以及美國東部（維吉尼亞北部）和南美洲（聖保羅）區域	將 AWS Direct Connect 入門指南取代為 AWS Direct Connect 使用者指南。新增主題以涵蓋新的 AWS Direct Connect 主控台、新增帳單主題、新增路由器組態資訊，以及更新主題以包含新增兩個新 AWS Direct Connect 據點，服務美國東部（維吉尼亞北部）和南美洲（聖保羅）區域。	2012-08-13
支援歐洲 (愛爾蘭)、亞太區域 (新加坡) 及亞太區域 (東京) 區域	新增了新的故障診斷章節，並更新了主題，納入了為美國西部（加利佛尼亞北部）、歐洲（愛爾蘭）、亞太區域（新加坡）和亞太區域（東京）區域提供服務的四個新 AWS Direct Connect 據點。	2012-01-10
支援美國西部 (加利佛尼亞北部) 區域	已更新主題，納入了新增的美國西部 (加利佛尼亞北部) 區域。	2011-09-08
公開發行	AWS Direct Connect首度發行。	2011-08-03

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。