開發人員指南

AWS 區塊鏈範本

AWS 區塊鏈範本: 開發人員指南

Table of Contents

AWS 區塊鏈範本已於 2019 年 4 月 30 日終止。不會進一步更新此服務或此支援文件。為了獲得最佳的受管區塊鏈體驗 AWS，我們建議您使用 Amazon Managed Blockchain (AMB)。若要進一步了解 Amazon Managed Blockchain 入門，請參閱 Hyperledger Fabric 上的研討會，或有關部署 Ethereum 節點的部落格。如果您對 AMB 有任何疑問或需要進一步支援，請聯絡 支援 或您的 AWS 客戶團隊。

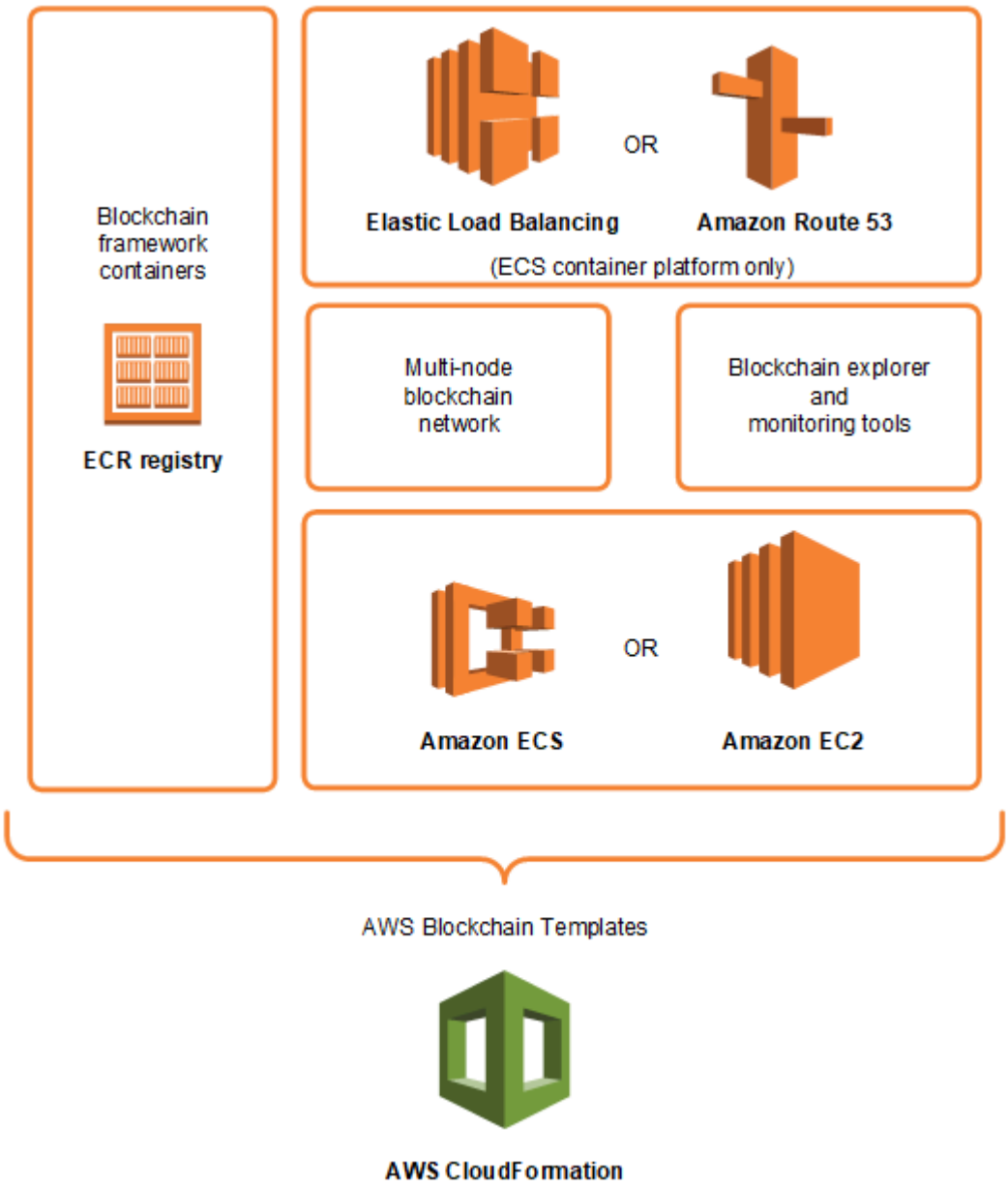
本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。

什麼是 AWS Blockchain 範本？

AWS Blockchain Templates 可協助您 AWS 使用不同的區塊鏈架構，在 上快速建立和部署區塊鏈網路。區塊鏈是分散式資料庫技術，使用密碼編譯來加強不斷擴充的交易集和智慧型合約對於竄改和修改的防護。

區塊鏈網路是一種對等網路，可改進商業程序交易的效率和不變性，像是國際支付、供應鏈管理、土地登記、群眾募資、治理、金融交易等等。這可讓彼此不認識的人和組織信任並獨立驗證交易記錄。

您可以使用 AWS Blockchain 範本來設定和啟動 CloudFormation 堆疊，以建立區塊鏈網路。您使用 AWS 的資源和服務取決於您選擇的 AWS Blockchain 範本和您指定的選項。如需可用範本及其功能的詳細資訊，請參閱AWS 區塊鏈範本和功能。使用 AWS 區塊鏈範本 AWS 建立的 區塊鏈網路的基本元件如下圖所示。



如何開始

最好的起點取決於您對區塊鏈的專業知識水準 AWS，特別是與 AWS 區塊鏈範本相關的服務。

我精通 AWS 和 區塊鏈

請從AWS 區塊鏈範本和功能中，您想要使用的架構相關主題開始。使用連結啟動 AWS 區塊鏈範本並設定區塊鏈網路，或下載範本自行簽出。

我精通 AWS 和 區塊鏈的新手

請從AWS 區塊鏈範本入門教學課程開始。此教學課程會逐步解說如何使用預設設定，建立入門 Ethereum 區塊鏈網路。完成後，請參閱AWS 區塊鏈範本和功能以獲得區塊鏈架構的概觀，並可利用其中的連結進一步了解組態選項和功能。

我是初學者 AWS ，精通區塊鏈

請從設定 AWS 區塊鏈範本開始。這可協助您設定 的基本概念 AWS，例如 帳戶和使用者設定檔。接著，請進行AWS 區塊鏈範本入門教學課程。此教學課程會逐步解說如何建立入門 Ethereum 區塊鏈網路。即使您最終不使用 Ethereum，您仍可獲得設定相關服務的實作經驗。這個體驗對於所有區塊鏈架構都很有幫助。最後，請參閱AWS 區塊鏈範本和功能一節中適用於您架構的主題。

我初次使用 AWS 和 區塊鏈

請從設定 AWS 區塊鏈範本開始。這可協助您設定 的基本概念 AWS，例如 帳戶和使用者設定檔。接著，請進行AWS 區塊鏈範本入門教學課程。此教學課程會逐步解說如何建立入門 Ethereum 區塊鏈網路。花點時間探索連結，以進一步了解 AWS 服務和 Ethereum。

相關服務

根據您選取的選項，AWS Blockchain Templates 可以使用下列 AWS 服務來部署區塊鏈：

- Amazon EC2 - 為您的區塊鏈網路提供運算容量。如需詳細資訊，請參閱《Amazon EC2 使用者指南》。
- Amazon ECS—如果您選擇使用，請在區塊鏈網路的叢集中協調 EC2 執行個體之間的容器部署。如需詳細資訊，請參閱《Amazon Elastic Container Service 開發人員指南》。
- Amazon VPC - 為您建立的 Ethereum 資源提供網路存取。您可以自訂存取能力和安全性的設定。如需詳細資訊，請參閱《Amazon VPC 開發人員指南》。
- Application Load Balancing - 做為單一聯絡點，可在使用 Amazon ECS 做為容器平台時存取可用的使用者介面和內部服務探索。如需詳細資訊，請參閱《Application Load Balancer 使用者指南》中的什麼是 Application Load Balancer？。

設定 AWS 區塊鏈範本

開始使用 AWS 區塊鏈範本之前，請先完成下列任務：

- 註冊 AWS 帳號：
- 建立 IAM 使用者
- 建立金鑰對

這些是所有區塊鏈組態的基本先決條件。此外，您選擇的區塊鏈網路可能會有先決條件，這取決於您所需的環境和組態選項。如需詳細資訊，請參閱AWS 區塊鏈範本和功能中與您區塊鏈範本相關的部分。

如需使用 Amazon ECS 叢集設定私有 Ethereum 網路先決條件的step-by-step說明，請參閱 AWS 區塊鏈範本入門。

註冊 AWS 帳號：

當您註冊 時 AWS， AWS 您的帳戶會自動註冊所有 服務。您只需支付實際使用服務的費用。

如果您已經有 AWS 帳戶，請跳到下一個任務。若您尚未擁有 AWS 帳戶，請使用下列程序建立帳戶。

建立 AWS 帳戶

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

   部分註冊程序需接收來電或簡訊，並在電話鍵盤輸入驗證碼。

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

請記下您的 AWS 帳戶號碼。在下一個任務中建立 IAM 使用者時需要它。

建立 IAM 使用者

中的服務 AWS 需要您在存取憑證時提供憑證，以便服務可以判斷您是否具有存取其資源的許可。主控台需要您的密碼。您可以為 AWS 您的帳戶建立存取金鑰，以存取命令列界面或 API。不過，我們不

建議您 AWS 使用 AWS 帳戶的登入資料來存取 ；建議您改用 AWS Identity and Access Management (IAM)。建立 IAM 使用者，然後將使用者新增至具有管理許可的 IAM 群組，或再授予此使用者管理許可。然後，您可以使用 AWS 特殊 URL 和 IAM 使用者的登入資料來存取 。

如果您已註冊 ， AWS 但尚未為自己建立 IAM 使用者，您可以使用 IAM 主控台建立一個使用者。如果您已有 IAM 使用者，可以略過此步驟。

若要建立管理員使用者，請選擇下列其中一個選項。

選擇一種管理管理員的方式	到	根據	您也可以
在 IAM Identity Center (建議)	使用短期憑證存取 AWS。 這與安全性最佳實務一致。有關最佳實務的資訊，請參閱 IAM 使用者指南中的 IAM 安全最佳實務。	請遵循 AWS IAM Identity Center 使用者指南的入門中的說明。	透過在 AWS Command Line Interface 使用者指南中設定 AWS CLI 以使用 來設定 AWS IAM Identity Center程式設計存取。
在 IAM 中 (不建議使用)	使用長期憑證存取 AWS。	請遵循《IAM 使用者指南》中建立 IAM 使用者以進行緊急存取 的指示。	請依照《IAM 使用者指南》中的管理 IAM 使用者的存取金鑰設定以程式設計方式存取。

若要以這個新的 IAM 使用者身分登入，請登出 AWS 管理主控台，然後使用下列 URL，其中 your_aws_account_id 是不含連字號 AWS 的帳號 （ 例如，如果 AWS 您的帳戶號碼是 1234-5678-9012，則 AWS 您的帳戶 ID 是 123456789012) :

```
https://your_aws_account_id.signin.aws.amazon.com/console/
```

輸入您剛才建立的 IAM 使用者名稱和密碼。登入時導覽列會顯示「your_user_name @ your_aws_account_id」。

如果您不希望登入頁面的 URL 包含 AWS 您的帳戶 ID，您可以建立帳戶別名。從 IAM 儀表板中，選擇建立帳戶別名，然後輸入別名，例如您的公司名稱。若要在建立帳戶別名後登入，請使用下列 URL：

```
https://your_account_alias.signin.aws.amazon.com/console/
```

若要驗證帳戶的 IAM 使用者的登入連結，請開啟 IAM 主控台，然後在儀表板的 IAM users sign-in link (IAM 使用者登入連結) 下方檢查。

如需詳細資訊，請參閱 AWS Identity and Access Management 使用者指南。

建立金鑰對

AWS 使用公有金鑰密碼編譯來保護區塊鏈網路中執行個體的登入資訊。當您使用每個 AWS 區塊鏈範本時，您可以指定金鑰對的名稱。然後，您可以使用金鑰對直接存取執行個體，例如，使用 SSH 登入。

如果您在正確的區域中已有金鑰對，則可略過此步驟。如果您尚未建立金鑰對，可以使用 Amazon EC2 主控台來建立。在您用來啟動 Ethereum 網路的相同區域中建立金鑰對。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的區域與可用區域。

建立一組金鑰對

1. 前往 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 從導覽列中，為金鑰對選取區域。無論您的位置為何，您都可以選取任何您可用的區域：不過，金鑰對具區域專用性。例如，如果您計劃在美國東部（俄亥俄）區域啟動執行個體，則必須為相同區域中的執行個體建立金鑰對。
3. 在導覽窗格中，選擇 Key Pairs (金鑰對)、Create Key Pair (建立金鑰對)。
4. 對於 Key pair name (金鑰對名稱)，輸入新金鑰對的名稱。選擇易於記住的名稱，例如您的 IAM 使用者名稱，後面接著 `-key-pair`，以及區域名稱。例如，me-key-pair-useast2。選擇建立。
5. 您的瀏覽器會自動下載私有金鑰檔案。基礎檔案名稱為您所指定的金鑰對名稱，副檔名為 `.pem`。將私有金鑰檔案存放在安全的地方。

> **Important**
>
> 這是您儲存私有金鑰檔案的唯一機會。當您啟動 Ethereum 網路時，需要提供金鑰對的名稱。

如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的 Amazon EC2 金鑰對。如需使用金鑰對連線至 EC2 執行個體的詳細資訊，請參閱《Amazon EC2 使用者指南》中的連線至您的 Linux 執行個體。

AWS 區塊鏈範本入門

本教學課程示範如何使用適用於 Ethereum 的 AWS 區塊鏈範本， AWS 透過 建立私有區塊鏈網路 CloudFormation。您建立的網路有兩個 Ethereum 用戶端和一個在 Amazon ECS 叢集中的 Amazon EC2 執行個體上執行的礦工。Amazon ECS 會在從 Amazon ECR 提取的 Docker 容器中執行這些服務。在開始本教學課程之前，了解區塊鏈網路和涉及 AWS 的服務會很有幫助，但並非必要。

此教學課程假設您已設定設定 AWS 區塊鏈範本中涵蓋的一般先決條件。此外，在使用範本之前，您必須設定一些 AWS 資源，例如 Amazon VPC 網路和 IAM 角色的特定許可。

教學課程會示範如何設定這些先決條件。我們已進行好設定選項，但並非規定性。只要您滿足先決條件，就可以根據應用程式和環境的需求進行其他組態選擇。如需每個範本的功能和一般先決條件的詳細資訊，以及下載範本或直接在 CloudFormation啟動範本，請參閱 AWS 區塊鏈範本和功能。

在本教學課程中，範例使用美國西部 （ 奧勒岡 ） 區域 (us-west-2)，但您可以使用支援 AWS 區塊鏈範本的任何區域：

- 美國西部 (奧勒岡) 區域 (us-west-2)
- 美國東部 (維吉尼亞北部) 區域 (us-east-1)
- 美國東部 (俄亥俄) 區域 (us-east-2)

> **Note**
>
> 在上面未列出的區域中執行範本會在美國東部 （ 維吉尼亞北部 ） 區域 (us-east-1) 啟動資源。

您使用此教學課程設定的適用於 Ethereum 的 AWS Blockchain 範本會建立下列資源：

- 您指定的隨需 EC2 執行個體類型和數量。此教學課程使用預設的 t2.medium 執行個體類型。
- 內部 Application Load Balancer。

在本教學課程中，會提供清除您所建立資源的步驟。

主題

- 設定先決條件
- 建立 Ethereum 網路

- 使用堡壘主機連線到 EthStats 和 EthExplorer
- 清除 資源

設定先決條件

您在本教學課程中指定的 Ethereum 組態 AWS Blockchain 範本需要您執行下列動作：

- 建立 VPC 和子網路
- 建立安全群組
- 為 Amazon ECS 和 EC2 執行個體設定檔建立 IAM 角色
- 建立堡壘主機

建立 VPC 和子網路

適用於 Ethereum 的 AWS 區塊鏈範本會將資源啟動至您使用 Amazon Virtual Private Cloud (Amazon VPC) 定義的虛擬網路。您在本教學中指定的組態會建立 Application Load Balancer，需要兩個在不同可用區域的公有子網路。此外，需要適用於容器執行個體的私有子網路，而且子網路必須與 Application Load Balancer 位於相同的可用區域。首先，使用 VPC 精靈在相同的可用區域中建立一個公有子網路和一個私有子網路。然後在不同的可用區域中，在此 VPC 內建立第二個公有子網路。

如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的什麼是 Amazon VPC？。

使用 Amazon VPC 主控台 (https://console.aws.amazon.com/vpc/：//) 建立彈性 IP 地址、VPC 和子網路，如下所述。

建立彈性 IP 地址

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 選擇 Elastic IPs (彈性 IP)、Allocate new address (配置新地址)、Allocate (配置)。
3. 記下您建立的彈性 IP 地址，並選擇 Close (關閉)。
4. 在彈性 IP 地址的清單中，尋找稍早建立之彈性 IP 地址的 Allocation ID (配置 ID)。當您建立 VPC 時需用到此項。

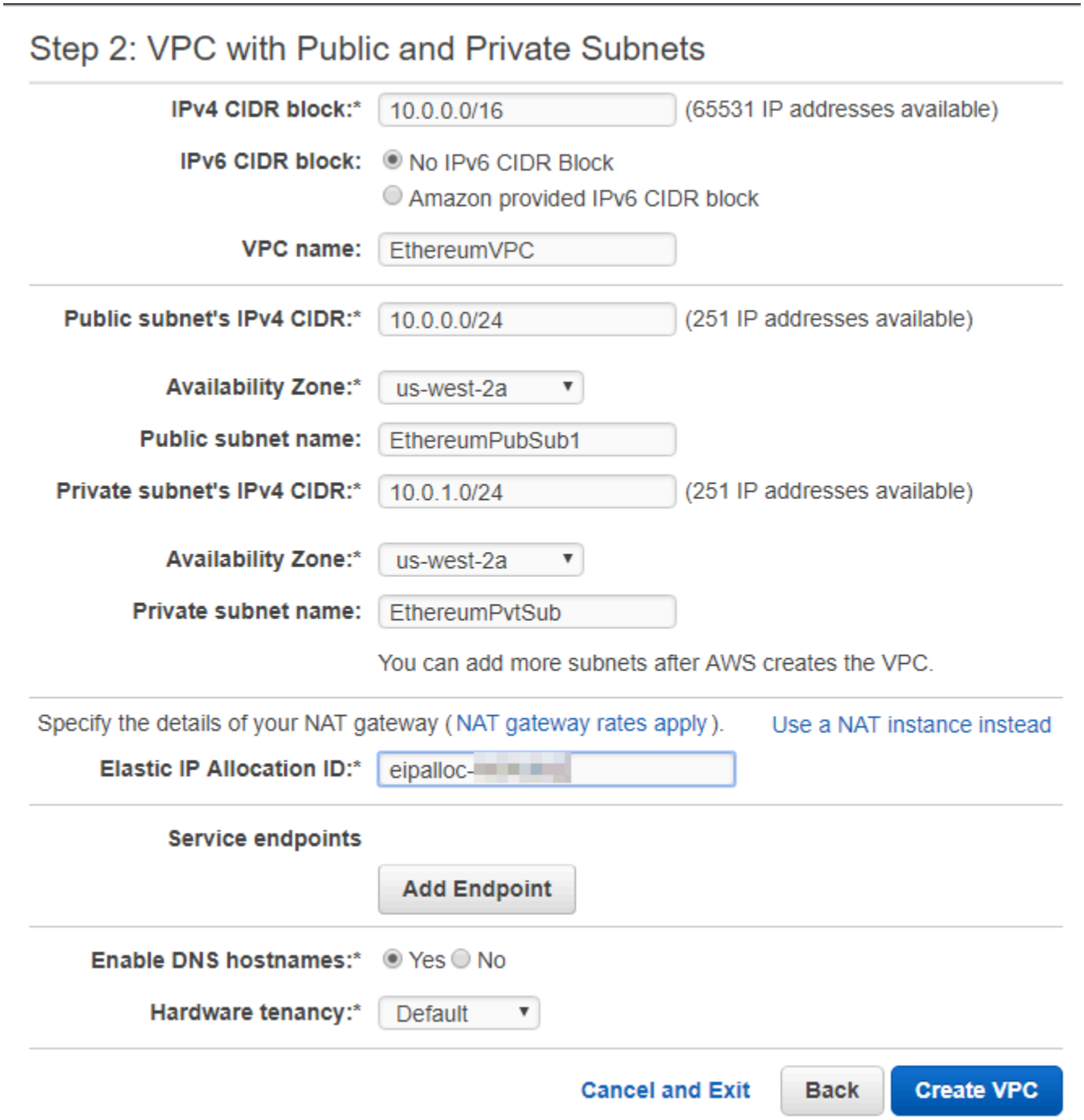
若要建立 VPC

1. 從導覽列中，為 VPC 選取區域。VPC 是專屬於特定區域，因此請選擇您建立金鑰對以及啟動 Ethereum 堆疊的同一個區域。如需詳細資訊，請參閱建立金鑰對。
2. 在 VPC 儀表板上，選擇 Start VPC Wizard (啟動 VPC 精靈)。
3. 在 Step 1: Select a VPC Configuration (步驟 1：選取 VPC 組態) 頁面，依序選擇 VPC with Public and Private Subnets (含公有和私有子網路的 VPC)、Select (選取)。
4. 在 Step 2: VPC with Public and Private Subnets (步驟 2：含公有和私有子網路的 VPC) 頁面，保留 IPv4 CIDR block (IPv4 CIDR 區塊) 和 IPv6 CIDR block (IPv6 CIDR 區塊) 的預設值。對於 VPC name (VPC 名稱)，輸入易記的名稱。
5. 對於 Public subnet's IPv4 CIDR (公有子網路的 IPv4 CIDR)，保留預設值。對於 Availability Zone (可用區域)，選擇區域。對於 Public subnet name (公有子網路名稱)，輸入易記的名稱。

   當您使用範本時，會將這個子網路指定為 Application Load Balancer 的兩個子網中的第一個。

   請記下此子網路的可用區域，因為您為私有子網路選取相同的可用區域，並為另一個公有子網路選取不同的可用區域。
6. 對於 Private subnet's IPv4 CIDR (私有子網路的 IPv4 CIDR)，保留預設值。對於 Availability Zone (可用區域)，選取與上一個步驟相同的可用區域。對於 Private subnet name (私有子網路名稱)，輸入易記的名稱。
7. 對於 Elastic IP Allocation ID (彈性 IP 配置 ID)，選取稍早建立的彈性 IP 地址。
8. 保留其他設定的預設值。
9. 選擇建立 VPC。

   以下範例顯示一個 VPC EthereumNetworkVPC 搭配公有子網路 EthereumPubSub1 和私有子網路 EthereumPvtSub1。公有子網路使用可用區域 us-west-2a。

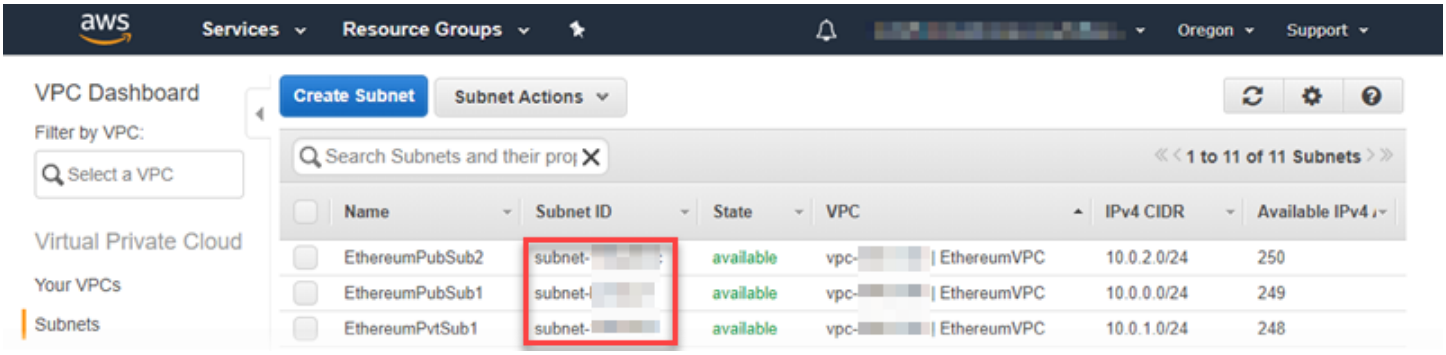


若要在不同的可用區域建立第二個公有子網路

1. 選擇 Subnets (子網路)，然後從清單中選取稍早建立的公有子網路。選取 Route Table (路由表) 標籤，並記下 Route table (路由表) ID。為下列第二個公有子網路指定相同的路由表。
2. 選擇 Create Subnet (建立子網路)。

3. 對於 Name tag (名稱標籤)，輸入子網路的名稱。您稍後在該網路中建立堡壘主機時，會使用此名稱。
4. 對於 VPC，選取稍早建立的 VPC。
5. 對於 Availability Zone (可用區域)，選取與第一個公有子網路所選區域不同的區域。
6. 對於 IPv4 CIDR block (IPv4 CIDR 區塊)，輸入 10.0.2.0/24。
7. 選擇 Yes, Create (是，建立)。子網路隨即新增至子網路清單中。
8. 從清單選取子網路，然後選擇 Subnet Actions (子網路動作)、Modify auto-assign IP settings (修改自動指派 IP 設定)。選取 Auto-assign IPs (自動指派 IP)、Save (儲存)、Close (關閉)。這樣可讓您在子網路中建立堡壘主機時，使其取得公有 IP 地址。
9. 在 Route Table (路由表) 標籤中，選擇 Edit (編輯)。對於 Change to (變更為)，選取您稍早記下的路由表 ID，並選擇 Save (儲存)。

您現在應該會看到您先前建立之 VPC 的三個子網路。請記下這些子網路名稱和 ID，以便可以使用範本來指定它們。



建立安全群組

安全群組可以做為防火牆，控制對資源的傳入和傳出流量。當您使用 範本在 Amazon ECS 叢集上建立 Ethererum 網路時，您可以指定兩個安全群組：

- 適用於 EC2 執行個體的安全群組，用以控制叢集中往返 EC2 執行個體的流量
- Application Load Balancer 的安全群組，可控制 Application Load Balancer、EC2 執行個體和堡壘主機之間的流量。您也可以將此安全群組與堡壘主機建立關聯。

每個安全群組具備允許 Application Load Balancer 和 EC2 執行個體之間通訊的規則，以及其他最低規則。這需要安全群組參考其他安全群組。因此，您需先建立安全群組，然後根據適當的規則更新它們。

若要建立兩個安全群組

1. 前往 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在導覽窗格中，選擇 Security Groups (安全群組)、Create Security Group (建立安全群組)。
3. 在 Security group name (安全群組名稱) 中，為安全群組輸入易於識別並可彼此區別的名稱，例如 EthereumEC2-SG 或 EthereumALB-SG。您稍後會用到這些名稱。對於 Description (描述)，輸入簡短摘要。
4. 對於 VPC，選取稍早建立的 VPC。
5. 選擇建立。
6. 重複上述步驟來建立其他的安全群組。

為 EC2 執行個體新增安全群組的傳入規則

1. 選取您稍早為 EC2 執行個體建立的安全群組
2. 在 Inbound (傳入) 標籤上，選擇 Edit (編輯)。
3. 針對類型，選擇所有流量。對於 Source (來源)，將 Custom (自訂) 保持選取狀態，然後從清單中選擇您目前正在編輯的安全群組，例如 EthereumEC2-SG。這可讓安全群組中的 EC2 執行個體彼此通訊。
4. 選擇 Add Rule (新增規則)。
5. 針對類型，選擇所有流量。對於 Source (來源)，將 Custom (自訂) 保持選取狀態，然後從清單中選擇 Application Load Balancer 的安全群組，例如 EthereumALB-SG。這可讓安全群組中的 EC2 執行個體與 Application Load Balancer 通訊。
6. 選擇儲存。

為 Application Load Balancer 的安全群組新增傳入規則和編輯傳出規則

1. 選取您稍早為 Application Load Balancer 建立的安全群組
2. 在 Inbound (傳入) 標籤上，選擇 Edit (編輯)，然後新增以下傳入規則：

    a. 針對類型，選擇所有流量。對於 Source (來源)，將 Custom (自訂) 保持選取狀態，然後從清單中選擇您目前正在編輯的安全群組，例如 EthereumALB-SG。這可讓 Application Load Balancer 與本身和堡壘主機通訊。

    b. 選擇 Add Rule (新增規則)。

c. 針對類型，選擇所有流量。對於 Source (來源)，將 Custom (自訂) 保持選取狀態，然後從清單中選擇 EC2 執行個體的安全群組，例如 EthereumEC2-SG。這可讓安全群組中的 EC2 執行個體與 Application Load Balancer 和堡壘主機通訊。

d. 選擇 Add Rule (新增規則)。

e. 針對 Type (類型)，選擇 SSH。對於 Source (來源)，選取 My IP (我的 IP)，這會偵測到您電腦的 IP CIDR，並進入其中。

> **Important**
>
> 此規則允許堡壘主機接受來自您電腦的 SSH 流量，讓您的電腦能夠使用堡壘主機檢視 Web 界面，並連線到 Ethereum 網路上的 EC2 執行個體。若要允許其他人連線到 Ethereum 網路，請將他們新增為此規則的來源。僅允許傳入流量流向受信任的來源。

f. 選擇儲存。

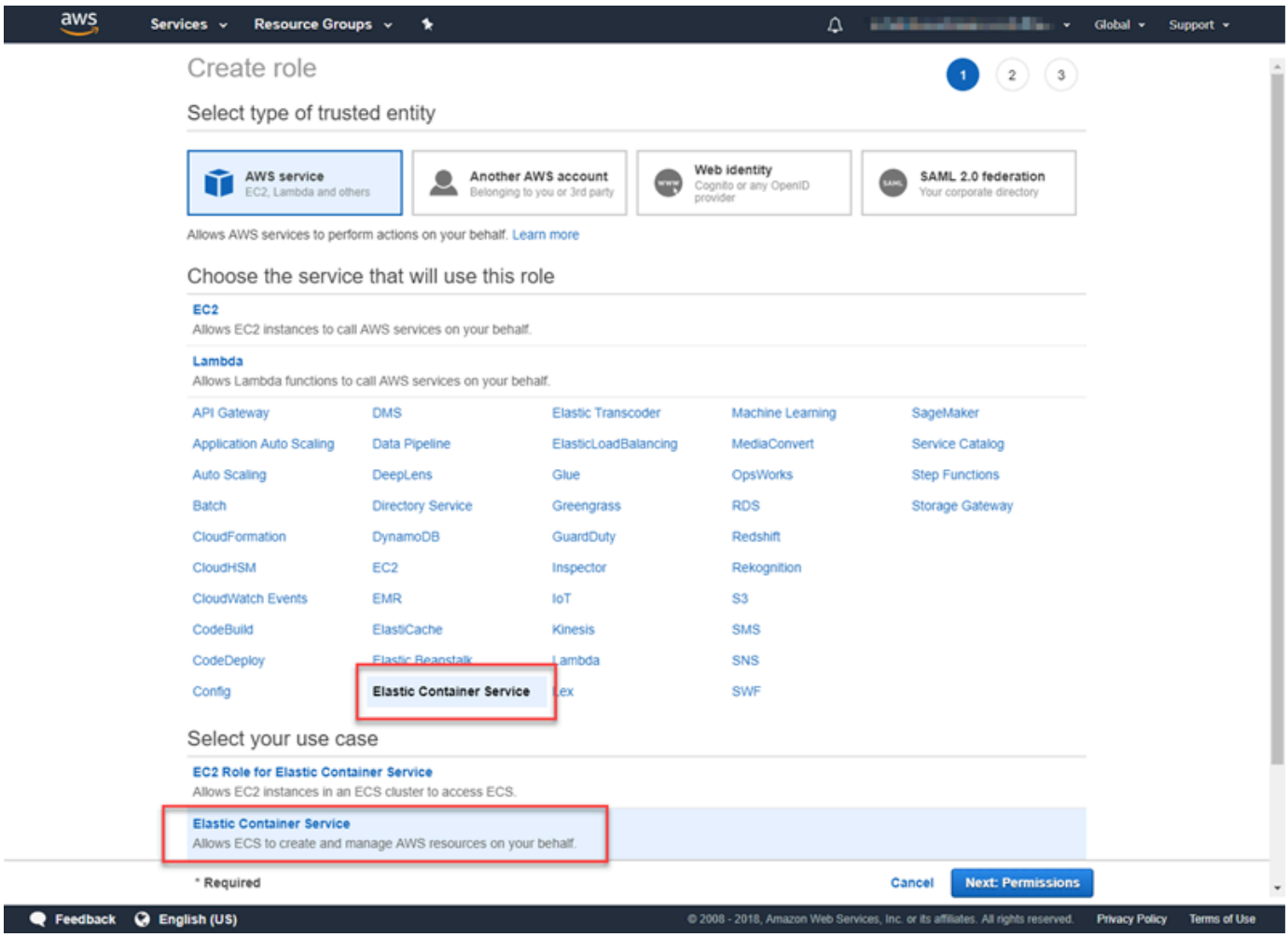
3. 在 Outbound (傳出) 標籤上，選擇 Edit (編輯)，然後刪除允許傳出流量至所有 IP 地址的自動建立規則。
4. 選擇 Add Rule (新增規則)。
5. 針對類型，選擇所有流量。對於 Destination (目的地)，將 Custom (自訂) 保持選取狀態，然後從清單中選擇 EC2 執行個體的安全群組。這會允許來自 Application Load Balancer 和堡壘主機前往 Ethereum 網路中 EC2 執行個體的傳出連線。
6. 選擇 Add Rule (新增規則)。
7. 針對類型，選擇所有流量。對於 Destination (目的地)，將 Custom (自訂) 保持選取狀態，然後從清單中選擇您目前正在編輯的安全群組，例如 EthereumALB-SG。這可讓 Application Load Balancer 與本身和堡壘主機通訊。
8. 選擇儲存。

為 Amazon ECS 和 EC2 執行個體設定檔建立 IAM 角色

使用此範本時，您可以指定 Amazon ECS 的 IAM 角色和 EC2 執行個體描述檔。連接到這些角色的許可政策，能讓叢集中的 AWS 資源和執行個體與其他 AWS 資源互動。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 角色。您可以使用 IAM 主控台 (https://console.aws.amazon.com/iam/：//) 為 Amazon ECS 和 EC2 執行個體設定檔設定 IAM 角色。

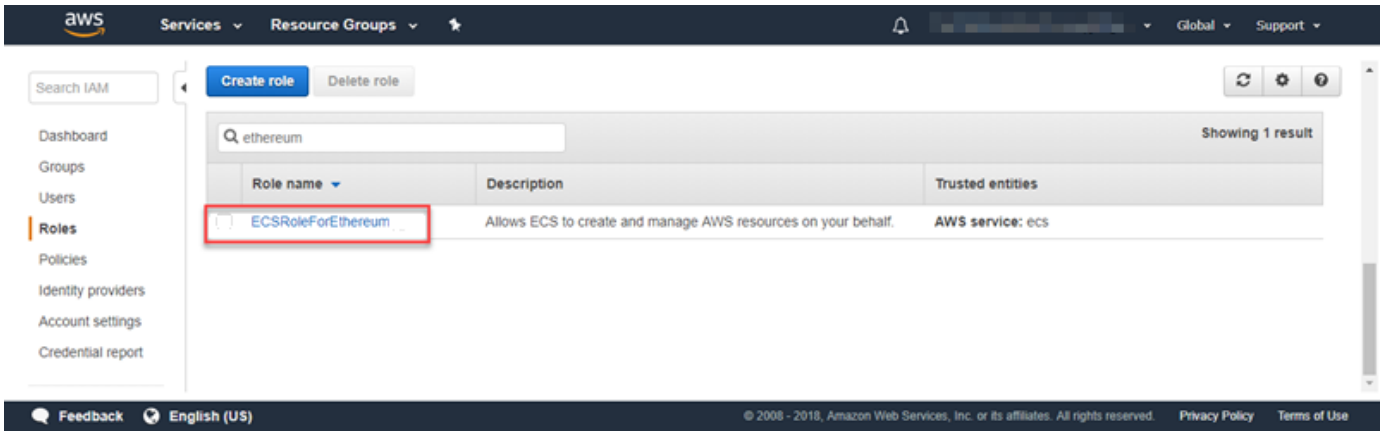
建立 Amazon ECS 的 IAM 角色

1. 前往網址 https://console.aws.amazon.com/iam/ 開啟 IAM 主控台。
2. 在導覽窗格中，選擇角色 、建立角色。
3. 在 Select type of trusted entity (選擇信任的實體類型) 下，選擇 AWS service (AWS 服務)。
4. 針對 Choose the service that will use this role (選擇將使用此角色的服務)，請選擇 Elastic Container Service。
5. 在 Select your use case (選擇您的使用案例) 下方選擇 Elastic Container Service、Next:Permissions (下一步：許可)。

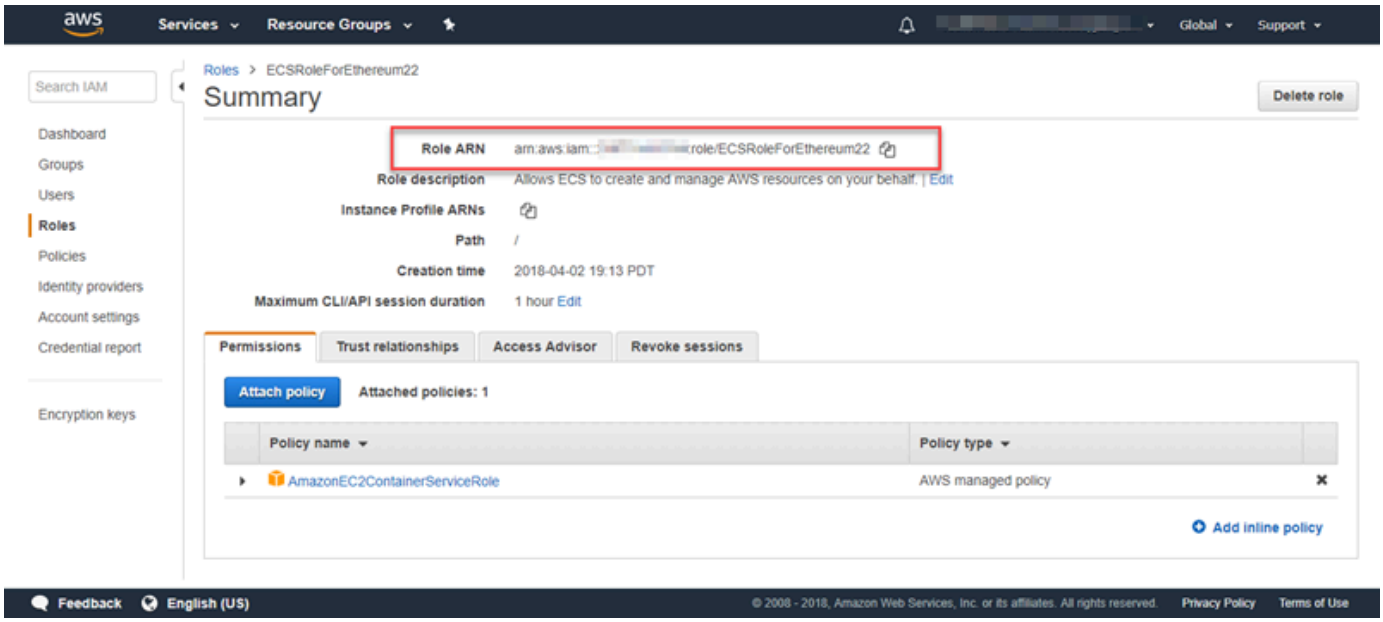


6. 維持選取 Permissions policy (許可政策) 中的預設政策 (AmazonEC2ContainerServiceRole)，然後選擇 Next:Review (下一步：檢閱)。
7. 在 Role name (角色名稱) 中輸入可協助您識別此角色的值，例如 ECSRoleForEthereum。在 Role Description (角色描述) 中輸入簡短摘要。請記下稍後的角色名稱。
8. 選擇建立角色。

9. 從清單中選擇您剛剛建立的角色。如果您的帳戶有許多角色，您可以搜尋角色名稱。



10. 複製 Role ARN (角色 ARN) 值並加以儲存，讓您稍後可以再次複製。建立 Ethereum 網路時會需要此 ARN。



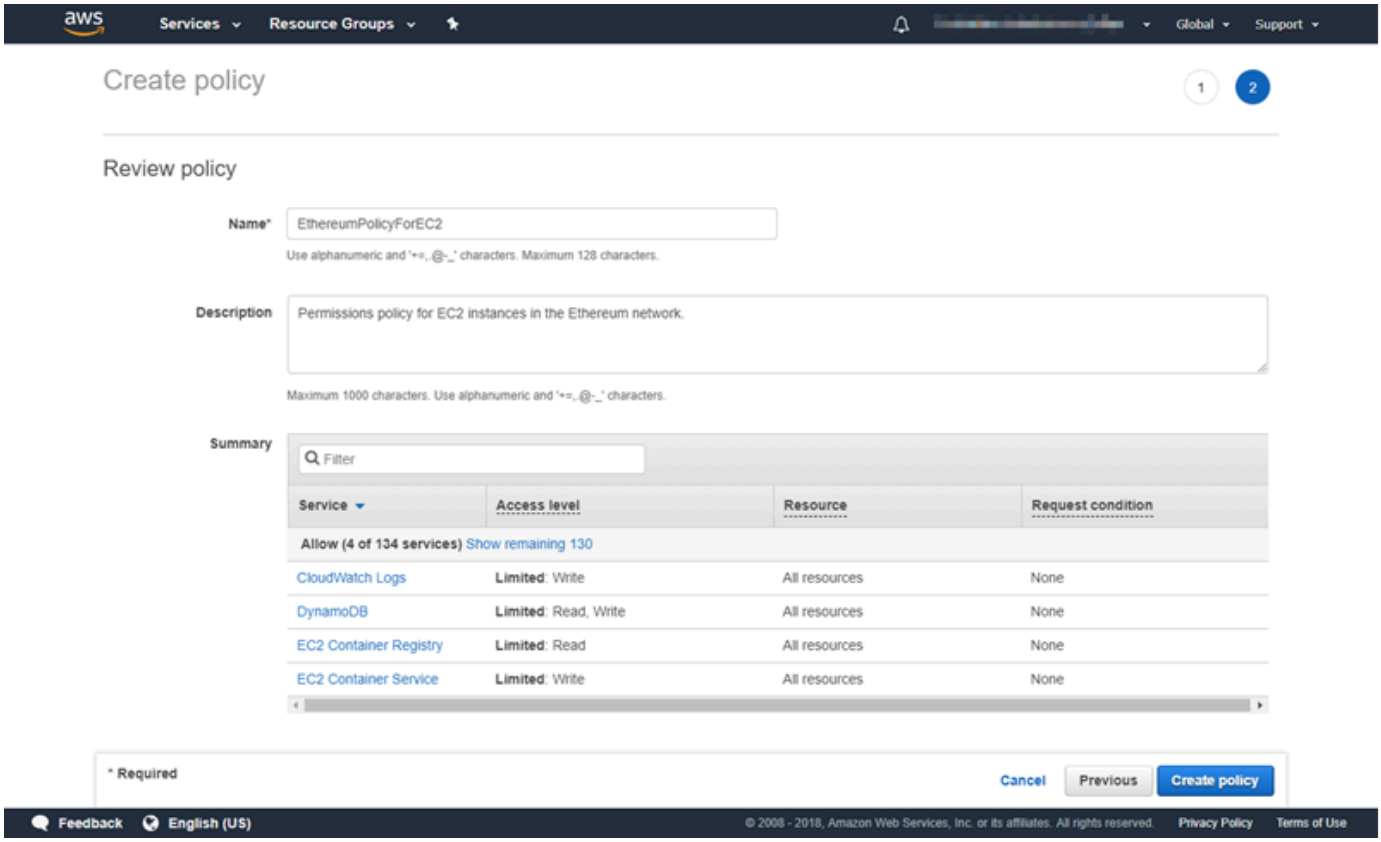
您在範本中指定的 EC2 執行個體描述檔由 Ethereum 網路中的 EC2 執行個體擔任，以與其他 AWS 服務互動。您為角色建立許可政策、建立該角色 (這會自動建立相同名稱的執行個體描述檔)，然後將許可政策連接至角色。

若要建立 EC2 執行個體描述檔

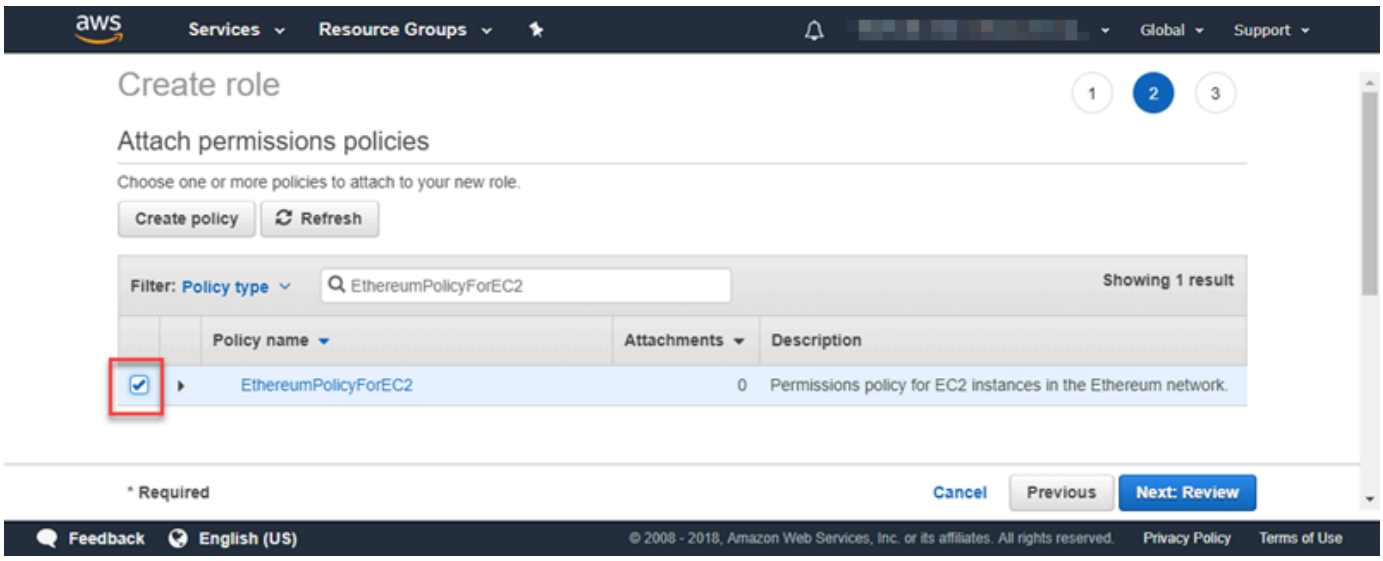
1. 在導覽窗格中，選擇政策、建立政策。
2. 選擇 JSON，並將預設政策陳述式取代為下列 JSON 政策：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:CreateCluster",
                "ecs:DeregisterContainerInstance",
                "ecs:DiscoverPollEndpoint",
                "ecs:Poll",
                "ecs:RegisterContainerInstance",
                "ecs:StartTelemetrySession",
                "ecs:Submit*",
                "ecr:GetAuthorizationToken",
                "ecr:BatchCheckLayerAvailability",
                "ecr:GetDownloadUrlForLayer",
                "ecr:BatchGetImage",
                "logs:CreateLogStream",
                "logs:PutLogEvents",
                "dynamodb:BatchGetItem",
                "dynamodb:BatchWriteItem",
                "dynamodb:PutItem",
                "dynamodb:DeleteItem",
                "dynamodb:GetItem",
                "dynamodb:Scan",
                "dynamodb:Query",
                "dynamodb:UpdateItem"
            ],
            "Resource": "*"
        }
    ]
}
```

3. 選擇檢閱政策。
4. 對於 Name (名稱)，輸入可協助您識別此許可政策的值，例如 EthereumPolicyForEC2。對於 Description (描述)，輸入簡短摘要。選擇建立政策。

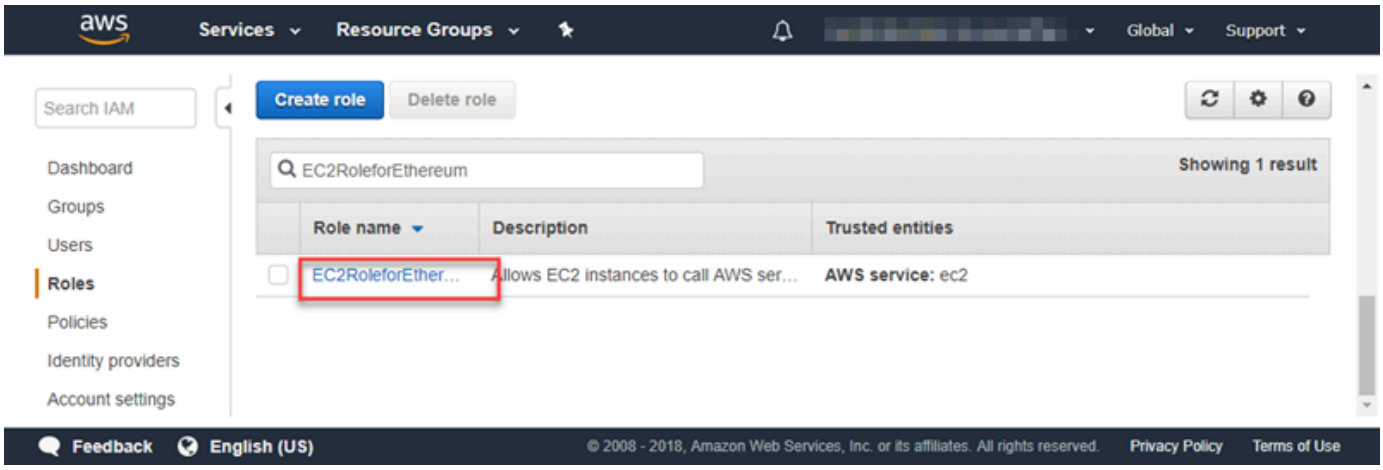


5. 選擇 Roles (角色)、Create role (建立角色)。
6. 選擇 EC2、Next: Permissions (下一步：許可)。
7. 在 Search (搜尋) 欄位中，輸入您稍早建立的許可政策名稱，例如 EthereumPolicyForEC2。
8. 選取您稍早建立之政策的核取記號，然後選擇 Next: Review (下一步：檢閱)。

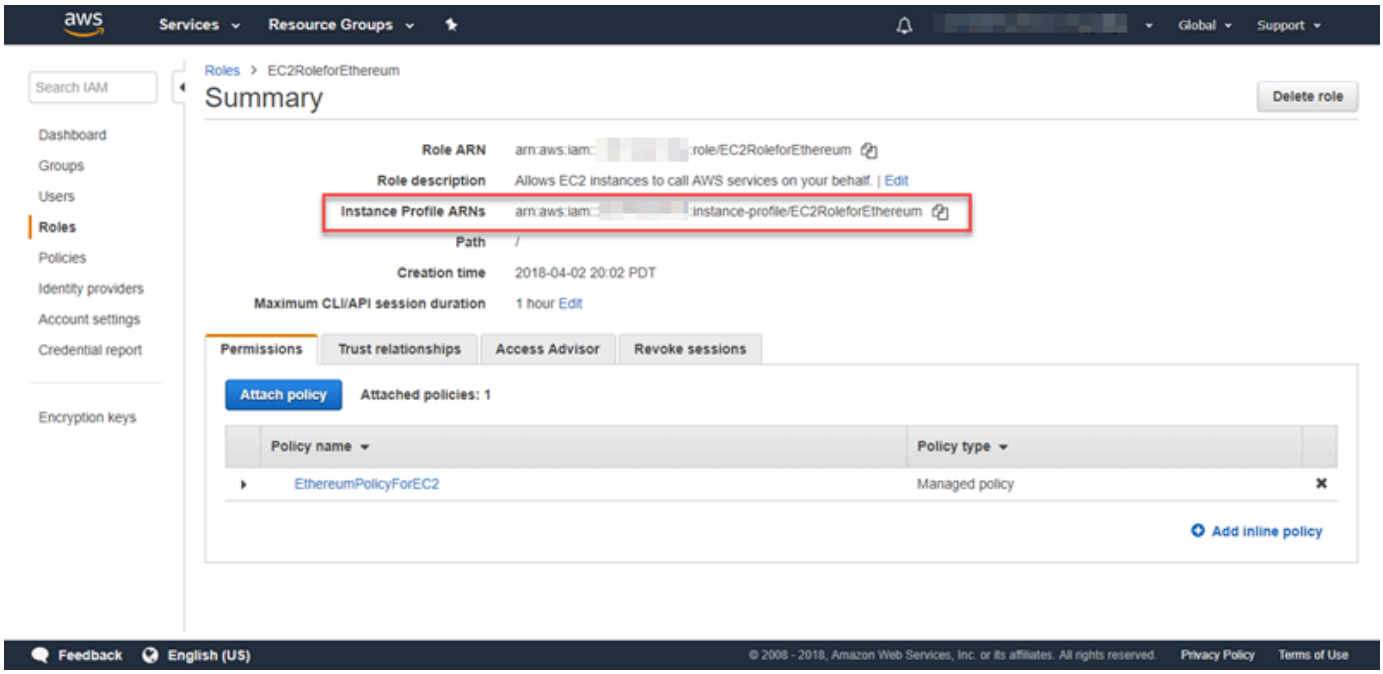


9. 對於 Role name (角色名稱)，輸入可協助您識別此角色的值，例如 EC2RoleForEthereum。對於 Role description (角色描述)，輸入簡短摘要。選擇 Create role (建立角色)。

10. 從清單中選擇您剛剛建立的角色。如果您的帳戶有很多角色，則可在 Search (搜尋) 欄位中輸入角色名稱。



11. 複製 Instance Profile ARN (執行個體描述檔 ARN) 值並加以儲存，讓您稍後可以再次複製。建立 Ethereum 網路時會需要此 ARN。



建立堡壘主機

在此教學中，您會建立堡壘主機。這是 EC2 執行個體，您可用來連線至 Ethereum 網路中的 Web 介面和執行個體。其唯一目的是轉送來自 VPC 外部之受信任用戶端的 SSH 流量，以便其可以存取 Ethereum 網路資源。

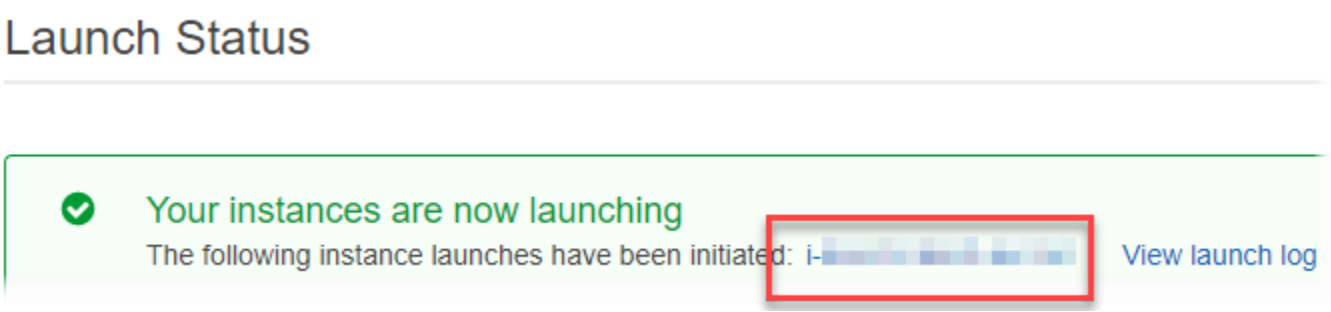
您設定堡壘主機是因為範本建立的 Application Load Balancer 是內部的，表示它僅路由內部 IP 地址。堡壘主機：

- 具有 Application Load Balancer 可辨識的內部 IP 地址，因為您在稍早建立的第二個公有子網路中啟動該地址。
- 具有子網路指派的公有 IP 地址，VPC 外部受信任的來源可存取該位址。
- 與您先前建立之 Application Load Balancer 的安全群組相關聯，該群組具有允許來自受信任用戶端之 SSH 流量 (連接埠 22) 的傳入規則。

為了能夠存取 Ethereum 網路，必須設定受信任的用戶端，才能透過堡壘主機進行連線。如需詳細資訊，請參閱使用堡壘主機連線到 EthStats 和 EthExplorer。堡壘主機是一種方法。您可以使用任何方法，從受信任的用戶端存取 VPC 內的私有資源。

建立堡壘主機

1. 遵循《Amazon EC2 使用者指南》中的前五個步驟來啟動執行個體。
2. 選擇邊值執行個體詳細資訊。對於 Network (網路)，選擇您稍早建立的 VPC，對於 Subnet (子網路)，選取您稍早建立的第二個公有子網路。將所有其他設定保持為預設值。
3. 出現提示時確認變更，然後選擇 Review and Launch (檢閱和啟動)。
4. 選擇 Edit Security Groups (編輯安全群組)。在 Assign a security group (指派安全群組) 中，選擇 Select an existing security group (選取現有的安全群組)。
5. 從安全群組的清單中，選取您稍早建立之 Application Load Balancer 的安全群組，然後選擇 Review and Launch (檢閱和啟動)。
6. 選擇啟動。
7. 請記下執行個體 ID。您稍後會在使用堡壘主機連線到 EthStats 和 EthExplorer時，需要該 ID。



建立 Ethereum 網路

您在本主題中使用 範本指定的 Ethereum 網路會啟動 CloudFormation 堆疊，為 Ethereum 網路建立 EC2 執行個體的 Amazon ECS 叢集。範本需倚賴您稍早在設定先決條件 中建立的資源。

當您使用 範本啟動 CloudFormation 堆疊時，它會為某些任務建立巢狀堆疊。上述工作完成後，您可以透過堡壘主機連線到網路的 Application Load Balancer 提供的資源，確認您的 Ethereum 網路可以執行並可供存取。

使用適用於 Ethereum 的 AWS 區塊鏈範本建立 Ethereum 網路

1. 請參閱 AWS 區塊鏈範本入門，並使用您 AWS 區域的快速連結，在 CloudFormation 主控台中開啟適用於 Ethereum 的最新 AWS 區塊鏈範本。
2. 根據下列指導方針輸入值：

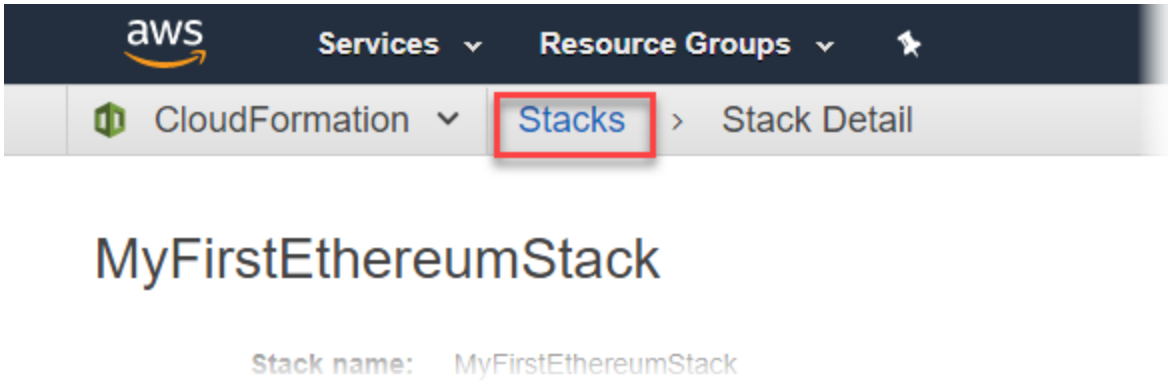
   - 對於 Stack name (堆疊名稱)，輸入您可輕鬆識別的名稱。這個名稱將用於堆疊建立的資源名稱中。
   - 在 Ethereum Network Parameters (Ethereum 網路參數) 和 Private Ethereum Network Parameters (私有 Ethereum 網路參數) 下，保留預設設定。

     > **Warning**
     >
     > 預設帳戶和相關聯的助憶鍵片語僅供測試之用。不要使用預設的一組帳戶傳送發送真實的 Ether，因為可存取助憶鍵片語的任何人都能存取或 Ether 或從帳戶竊取 Ether。相反地，為了生產目的才指定自訂帳戶。與預設帳戶相關聯的助憶鍵片語是 `outdoor father modify clever trophy abandon vital feel portion grit evolve twist`。

   - 在平台組態下，保留預設設定，這會建立 EC2 執行個體的 Amazon ECS 叢集。另一個方法 docker-local，則會使用單一 EC2 執行個體建立 Ethereum 網路。
   - 在 EC2 configuration (EC2 組態) 下，根據下列指導方針選取選項：
     - 對於 EC2 Key Pair (EC2 金鑰對)，選取金鑰對。如需建立金鑰對的相關資訊，請參閱建立金鑰對。
     - 對於 EC2 Security Group (EC2 安全群組)，選取您稍早在建立安全群組 中建立的安全群組。
     - 對於 EC2 Instance Profile ARN (EC2 執行個體描述檔 ARN)，輸入您稍早在為 Amazon ECS 和 EC2 執行個體設定檔建立 IAM 角色 中建立的執行個體描述檔 ARN。
   - 在 VPC network configuration (VPC 網路組態) 下，根據下列指導方針選取選項：

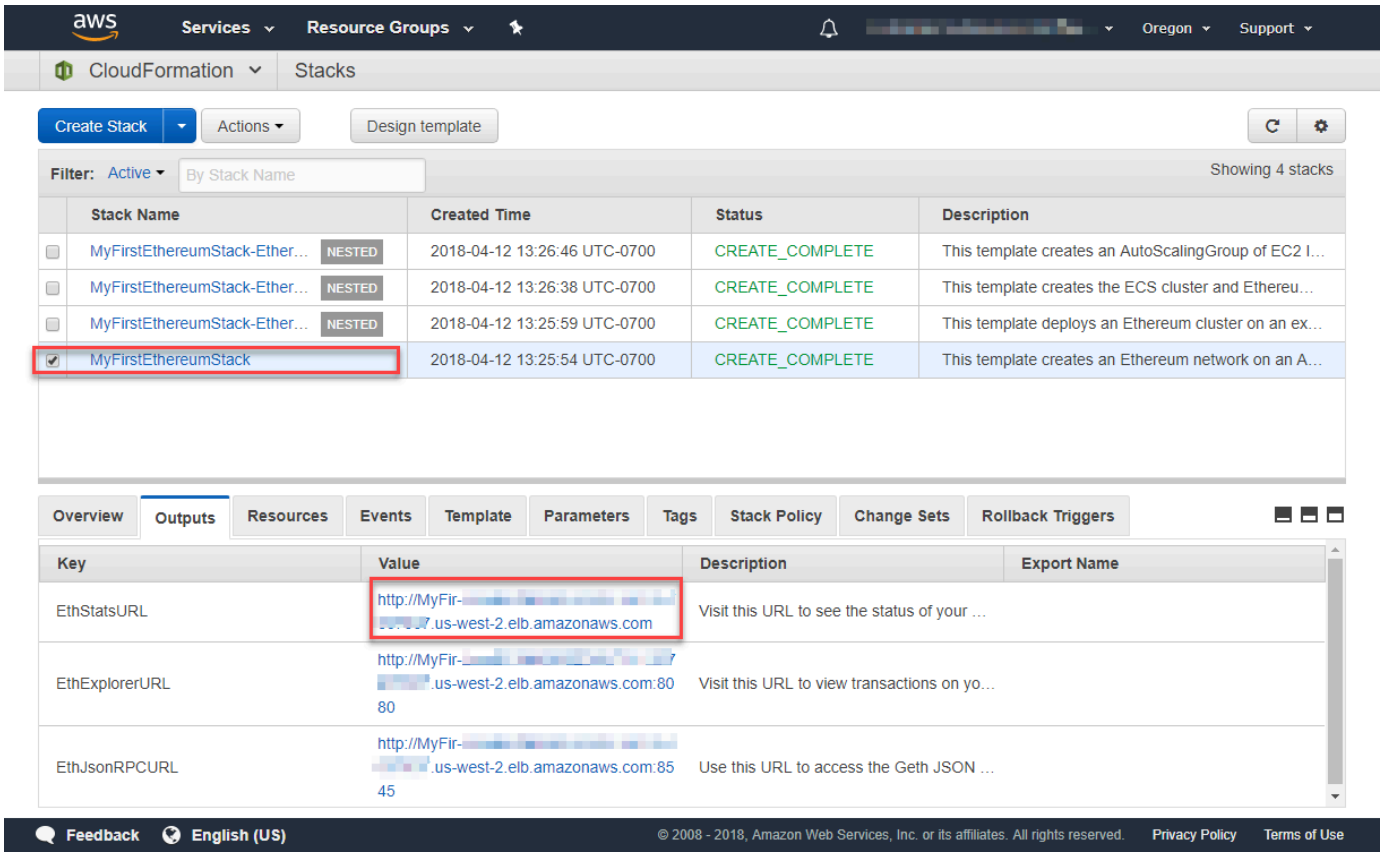
    - 對於 VPC ID，選取您稍早在建立 VPC 和子網路 中建立的 VPC。
    - 對於 Ethereum Network Subnet IDs (Ethereum 網路子網路 ID)，選取您稍早在To create the VPC 程序中建立的單一私有子網路。
  - 在 ECS cluster configuration (ECS 叢集組態) 下，保留預設值。這會建立一個包含三個 EC2 執行個體的 ECS 叢集。
  - 在 Application Load Balancer configuration (ECS only) (Application Load Balancer 組態 (僅限 ECS))，根據下列指導方針選取選項：
    - 對於 Application Load Balancer Subnet IDs (Application Load Balancer 子網路 ID)，從您稍早記下的list of subnets 中，選取兩個公有子網路。
    - 對於 Application Load Balancer Security Group (Application Load Balancer 安全群組)，選取您稍早在建立安全群組 中建立的 Application Load Balancer 安全群組。
    - 針對 IAM 角色，輸入您先前在 中建立之 ECS 角色的 ARN為 Amazon ECS 和 EC2 執行個體設定檔建立 IAM 角色。
  - 在 EthStats 下，根據下列指導方針選取選項：
    - 對於 Deploy EthStats (部署 EthStats)，保留預設設定，也就是 true。
    - 對於 EthStats Connection Secret (EthStats 連線密碼)，輸入至少六個字元的任意值。
  - 在 EthExplorer 下，為 Deploy EthExplorer (部署 EthExplorer) 保留預設設定，也就是 true。
  - 在 Other parameters (其他參數) 下，為 Nested Template S3 URL Prefix (巢狀範本 S3 URL 前綴) 保留預設值，並記下該值。這是您可以找到巢狀範本的地方。
3. 保留所有其他設定的預設值、選取確認核取方塊，然後選擇 Create (建立)。

   CloudFormation 啟動的根堆疊的堆疊詳細資訊頁面隨即出現。
4. 若要監控根堆疊和巢狀堆疊的進度，請選擇 Stacks (堆疊)。



5. 當所有堆疊顯示 CREATE_COMPLETE for Status 時，您可以連線至 Ethereum 使用者介面，以確認網路正在執行並可存取。使用 ECS 容器平台時，透過 Application Load Balancer 連線到 EthStats、EthExplorer 和 EthJsonRPC 的 URL 會顯示在根堆疊的 Outputs (輸出) 標籤中。

> **Important**
>
> 在透過用戶端電腦上的堡壘主機設定代理連線之前，您無法直接連線至這些 URL 或 SSH。如需詳細資訊，請參閱使用堡壘主機連線到 EthStats 和 EthExplorer。



使用堡壘主機連線到 EthStats 和 EthExplorer

若要在本教學中連線到 Ethereum 資源，您可以透過堡壘主機設定 SSH 連接埠轉送 (SSH 通道)。下列指示示範如何執行這項操作，以便您可以使用瀏覽器連線到 ETStats 和 ETExplorer URL。在下列說明中，先在本機連接埠上設定 SOCKS 代理。然後，使用瀏覽器延伸 FoxyProxy，為您的 Ethereum 網路 URL 使用此轉送連接埠。

如果您使用 Mac OS 或 Linux，請使用 SSH 用戶端來設定與堡壘主機的 SOCKS 代理連線。如果您是 Windows 使用者，請使用 PuTTY。連線之前，請確認您正在使用的用戶端電腦在您之前為 Application Load Balancer 設定的安全群組中，指定為傳入 SSH 流量的允許來源。

使用 SSH 透過 SSH 連接埠轉送連線到堡壘主機

- 請遵循《Amazon EC2 使用者指南》中的使用 SSH 連線至 Linux 執行個體的程序。針對連線至 Linux 執行個體程序的步驟 4，將 `-D 9001`新增至 SSH 命令，指定您在 Ethereum 組態的 AWS 區塊鏈範本中指定的相同金鑰對，並指定堡壘主機的 DNS 名稱。

  ```
  ssh -i /path/my-template-key-pair.pem ec2-user@bastion-host-dns -D 9001
  ```

使用 PuTTY 透過 SSH 連接埠轉送連線到堡壘主機 (Windows)

1. 遵循《Amazon EC2 使用者指南》中的使用 PuTTY 從 Windows 連線至 Linux 執行個體中的程序，直到啟動 PuTTY 工作階段程序的步驟 7，使用您在適用於 Ethereum 的 AWS 區塊鏈範本組態中指定的相同金鑰對。
2. 在 PuTTY 中的 Category (類別) 下，選擇 Connection (連線)、SSH、Tunnels (通道)。
3. 對於 Port forwarding (連接埠轉送)，選擇 Local ports accept connections from other hosts (本機連接埠接受來自其他主機的連線)。
4. 在 Add new forwarded port (新增轉送的連接埠) 下：

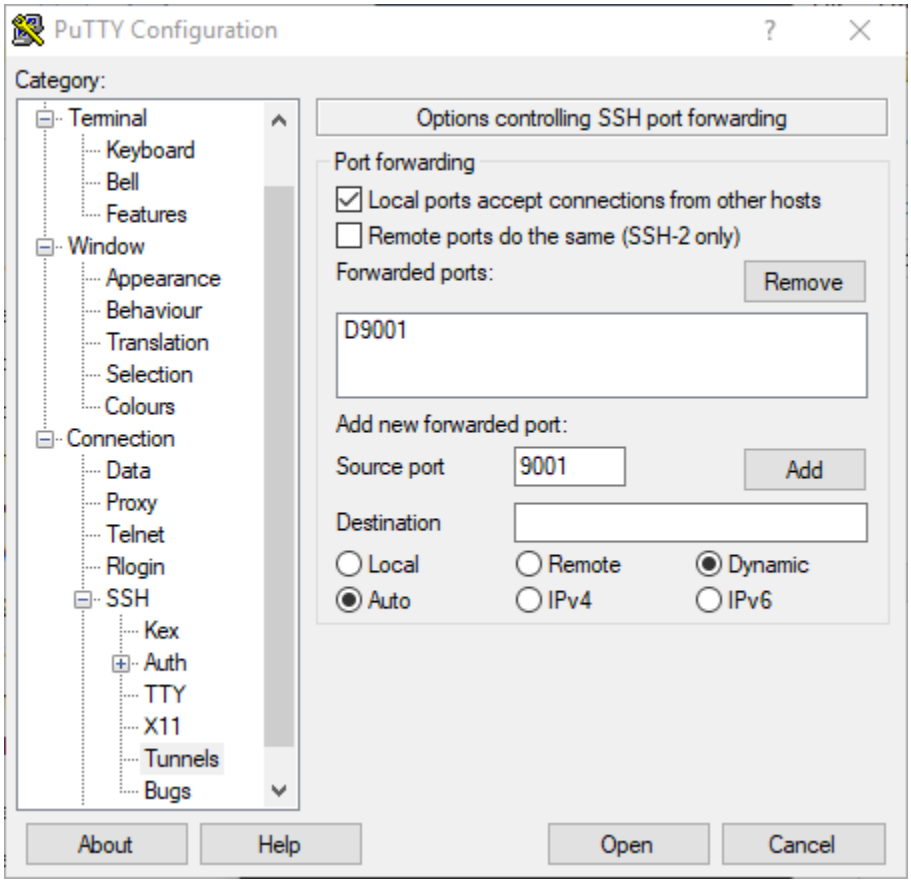
   a. 對於 Source port (來源連接埠)，輸入 9001。這是我們選擇的任一未使用的連接埠，如有需要，您可以選擇其他連接埠。

   b. 將 Destination (目的地) 保留空白。

   c. 選取 Dynamic (動態)。

   d. 選擇新增。

   對於 Forwarded ports (轉送的連接埠)，D9001 應該顯示如下。



5. 選擇 Open (開啟)，然後根據您的金鑰組態向堡壘主機進行身分驗證。保持連線開啟。

PuTTY 連線開啟後，您現在可以設定系統或瀏覽器延伸，以將轉送的連接埠用於 Ethereum 網路 URL。下列說明的基礎是根據您先前建立為轉送連接埠的 EthStats 和 EthExplorer 的 URL 模式和連接埠 9001，使用 FoxyProxy Standard 來轉送連線，但您可以使用任何偏好的方法。

將 FoxyProxy 設為使用 Ethereum 網路 URL 的 SSH 通道

此程序是以 Chrome 為基礎編寫的。如果您使用其他瀏覽器，請將設定和順序轉換為該瀏覽器的 FoxProxy 版本。

1. 下載並安裝 FoxyProxy Standard 瀏覽器延伸，然後根據瀏覽器的指示，開啟 Options (選項)。
2. 選擇 Add New Proxy (新增代理)。
3. 在 General (一般) 標籤上，確定代理是 Enabled (已啟用)，並輸入 Proxy Name (代理名稱) 和 Proxy Notes (代理備註)，以幫助您識別此代理組態。
4. 在 Proxy Details (代理詳細資訊) 標籤中，選擇 Manual Proxy Configuration (手動代理組態)。對於 Host or IP Address (主機或 IP 地址) (或某些版本中的 Server or IP Address (伺服器或 IP 地址)，輸入 localhost。對於 Port (連接埠)，輸入 9001。選取 SOCKS Proxy? (SOCKS 代理？)。

5. 在 URL Pattern (URL 模式) 標籤上，選擇 Add New Pattern (新增模式)。
6. 對於 Pattern name (模式名稱)，輸入容易識別的名稱，對於 URL Pattern (URL 模式)，輸入與您使用範本建立之所有 Ethereum 資源 URL 相符的模式，例如 http://internal-MyUser-LoadB-*。如需有關檢視 URL 的資訊，請參閱 Ethereum URLs。
7. 保留其他設定的預設選項，並選擇 Save (儲存)。

現在，您可以使用以範本建立之根堆疊的 Outputs (輸出) 標籤，連線至 CloudFormation 主控台上可用的 Ethereum URL。

清除 資源

CloudFormation 可讓您輕鬆清除堆疊建立的資源。刪除堆疊時，會一併刪除堆疊建立的所有資源。

若要刪除範本建立的資源

- 開啟 CloudFormation 主控台，選取您先前建立的根堆疊，選擇動作、刪除。

  您稍早建立之根堆疊及相關巢狀堆疊的 Status (狀態) 會更新為 DELETE_IN_PROGRESS。

您可以選擇刪除您為 Ethereum 網路建立的先決條件。

刪除 VPC

- 開啟 Amazon VPC 主控台，選取您先前建立的 VPC，然後選擇動作、刪除 VPC。這也會刪除 VPC 關聯的子網路、安全群組和 NAT 閘道。

刪除 IAM 角色與 EC2 執行個體描述檔

- 開啟 IAM 主控台，然後選擇角色。選取您之前建立的 ECS 角色和 EC2 角色，然後選擇 Delete (刪除)。

終止堡壘主機的 EC2 執行個體

- 開啟 Amazon EC2 儀表板，選擇執行中的執行個體，選擇您為堡壘主機建立的 EC2 執行個體，選擇動作、執行個體狀態、終止。

AWS 區塊鏈範本和功能

本節提供的連結，可讓您立即開始建立區塊鏈網路，並提供在 AWS上設定網路的組態選項和先決條件。

可使用以下範本：

- Ethereum 的 AWS 區塊鏈範本
- Hyperledger Fabric 的 AWS 區塊鏈範本

AWS 區塊鏈範本可在下列區域使用：

- 美國西部 (奧勒岡) 區域 (us-west-2)
- 美國東部 (維吉尼亞北部) 區域 (us-east-1)
- 美國東部 (俄亥俄) 區域 (us-east-2)

> **Note**
>
> 在上面未列出的區域中執行範本會在美國東部 （ 維吉尼亞北部 ） 區域 (us-east-1) 啟動資源。

使用 Ethereum 的 AWS 區塊鏈範本

Ethereum 是區塊鏈架構，可使用 Solidity (這是一種 Ethereum 專屬語言) 來執行智慧型合約。Homestead 是 Ethereum 的最新版本。如需詳細資訊，請參閱 Ethereum Homestead 文件和實體文件。

啟動連結

如需使用 Ethereum 範本在特定區域中啟動的連結，請參閱 AWS 區塊鏈範本入門。 CloudFormation

Ethereum 選項

使用範本設定 Ethereum 網路時，您所做的選擇將決定後續要求：

- 選擇容器平台

- 選擇私有或公有 Ethereum 網路
- 變更預設帳戶和助憶鍵片語

選擇容器平台

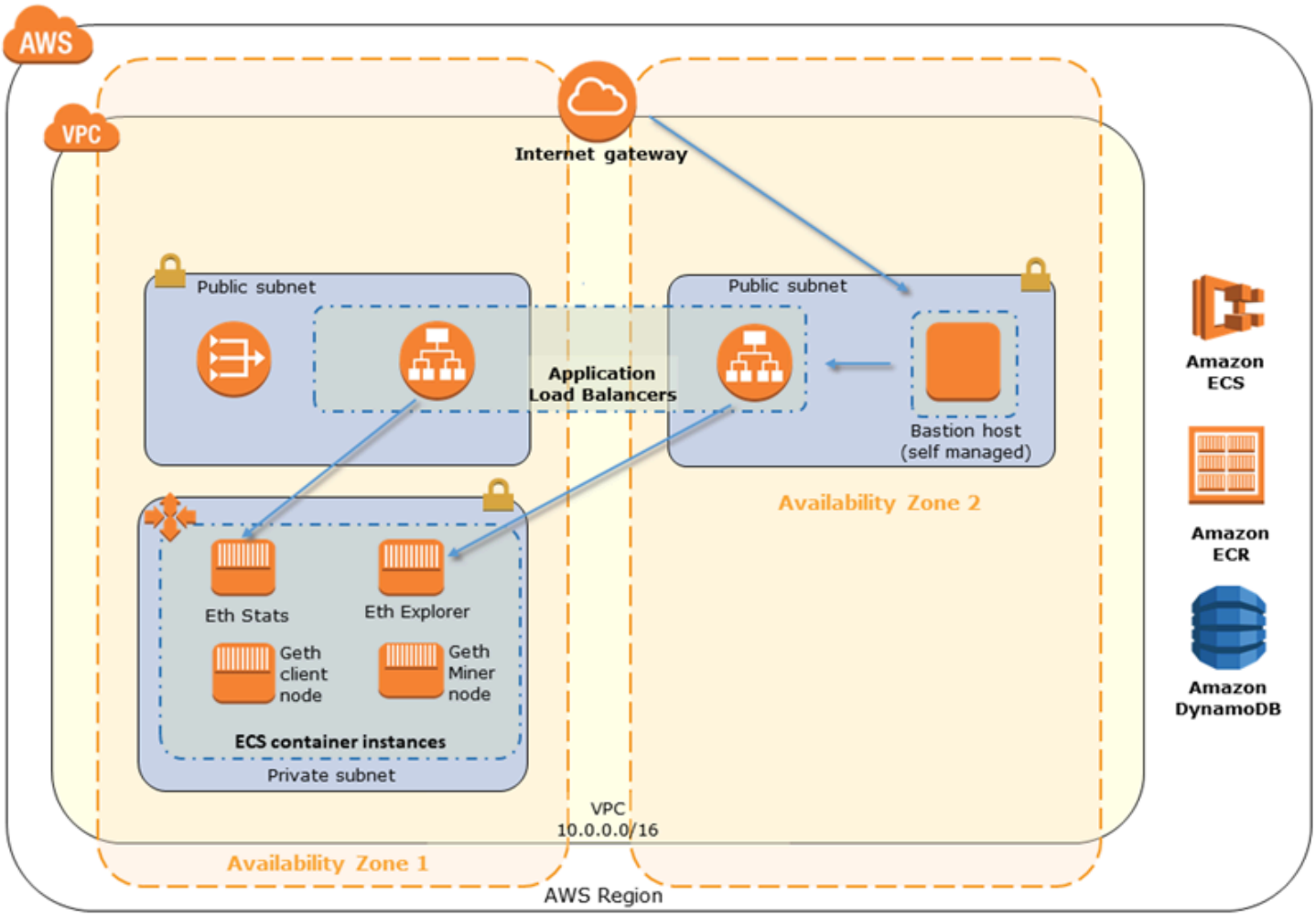
AWS Blockchain 範本使用存放在 Amazon ECR 中的 Docker 容器來部署區塊鏈軟體。適用於 Ethereum 的 AWS 區塊鏈範本為容器平台 提供兩種選擇：

- ecs—指定 Ethereum 在 Amazon EC2 執行個體的 Amazon ECS 叢集上執行。
- docker-local - 指定 Ethereum 在單一 EC2 執行個體上執行。

使用 Amazon ECS 容器平台

使用 Amazon ECS，您可以在由多個 EC2 執行個體組成的 ECS 叢集上建立 Ethereum 網路，其中包含 Application Load Balancer 和相關資源。如需使用 Amazon ECS 組態的詳細資訊，請參閱 AWS 區塊鏈範本入門教學課程。

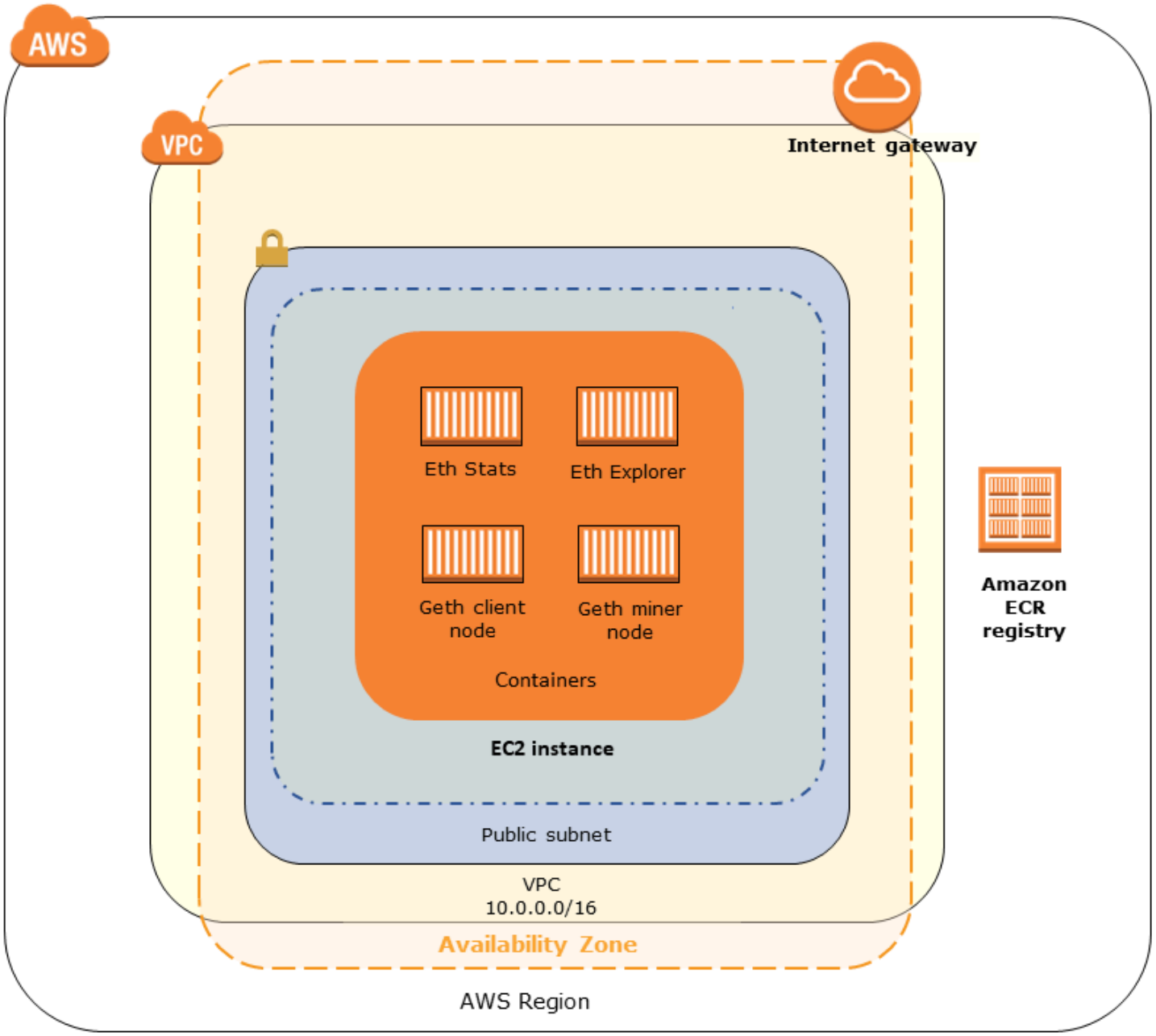
下圖說明使用範本搭配 ECS 容器平台選項建立的 Ethereum 網路：



使用 Docker-Local 平台

或者，您可以在單一 Amazon EC2 執行個體中啟動 Ethereum 容器。所有容器都在單一 EC2 執行個體上執行。這是一個簡化設定。

下圖說明使用範本搭配 docker-local 容器平台選項建立的 Ethereum 網路：



選擇私有或公有 Ethereum 網路

選擇 1-4 以外的 Ethereum Network ID (Ethereum 網路 ID) 值，可建立在您定義的網路內執行的私有 Ethereum 節點，並使用您指定的私有網路參數。

當您從 1–4 選擇 Ethereum Network ID 時，您建立的 Ethereum 節點會加入公有 Ethereum 網路。您可以忽略私有網路設定及其預設值。如果您選擇將 Ethereum 節點加入公有 Ethereum 網路，請確保您網路中的適當服務可以透過網際網路存取。

變更預設帳戶和助憶鍵片語

助憶鍵片語是一組隨機的字詞，您可用於為任何網路上的相關帳戶產生 Ethereum 錢包 (也就是私有/公有金鑰對)。助憶鍵片語可用於存取相關帳戶的 Ether。我們建立與 Ethereum 範本使用的預設帳戶相關聯的預設助憶鍵。

> **Warning**
>
> 預設帳戶和相關聯的助憶鍵片語僅供測試之用。不要使用預設的一組帳戶傳送發送真實的 Ether，因為可存取助憶鍵片語的任何人都能存取或 Ether 或從帳戶竊取 Ether。相反地，為了生產目的才指定自訂帳戶。與預設帳戶相關聯的助憶鍵片語是 `outdoor father modify clever trophy abandon vital feel portion grit evolve twist`。

先決條件

當您使用適用於 Ethereum 的 AWS 區塊鏈範本設定 Ethereum 網路時，必須符合下列最低要求。範本需要下列每個類別列出的 AWS 元件：

主題

存取 Ethereum 資源的先決條件

先決條件	對於 ECS 平台	對於 Docker-Local
可用來存取 Amazon EC2 EC2 金鑰對。金鑰必須與 ECS 叢集及其他資源位於相同的區域。	✓	✓
網際網路對應元件 (例如堡壘主機或網際網路對應的負載平衡器) 具有內部地址，允許該地址	✓	✓ (使用私有子網路)

先決條件	對於 ECS 平台	對於 Docker-Local
中的流量進入 Application Load Balancer。ECS 平台需要此元件，因為基於安全原因，範本會建立內部負載平衡器。當 EC2 執行個體位於私有子網路時，docker-local 平台需要此元件 (建議做法)。如需設定堡壘主機的相關資訊，請參閱 建立堡壘主機。		

IAM 先決條件

先決條件	對於 ECS 平台	對於 Docker-Local
有權使用所有相關服務的 IAM 主體 （使用者或群組）。	✓	✓
Amazon EC2 執行個體描述檔，具有 EC2 執行個體與其他服務互動的適當許可。如需詳細資訊，請參閱To create an EC2 instance profile。	✓	✓
具有 Amazon ECS 與其他 服務互動許可的 IAM 角色。如需詳細資訊，請參閱建立 ECS 角色和許可。	✓	

安全群組必要條件

先決條件	對於 ECS 平台	對於 Docker-Local
適用於 EC2 執行個體的安全群組，具備以下要求：	✓	✓

先決條件	對於 ECS 平台	對於 Docker-Local
• 傳出規則，允許流量前往 0.0.0.0/0 (預設)。	✓	✓
• 傳入規則，允許來自本身 (相同安全群組) 的所有流量。	✓	✓
• 輸入規則，允許來自 Application Load Balancer 安全群組的所有流量。	✓	
• 傳入規則，允許來自受信任的外部來源 (例如用戶端電腦的 IP CIDR) 的HTTP (連接埠 80)、EthStats (在連接埠 8080 提供)、JSON RPC over HTTP (連接埠 8545)，以及 SSH (連接埠 22)。		✓

先決條件	對於 ECS 平台	對於 Docker-Local
Application Load Balancer 的安全群組，具備以下要求： • 傳入規則，允許來自本身 (相同安全群組) 的所有流量。 • 傳入規則，允許所有來自 EC2 執行個體安全群組的流量。 • 傳出規則，僅允許所有流量流向 EC2 執行個體的安全群組。如需詳細資訊，請參閱建立安全群組。 • 如果將此相同的安全群組與堡壘主機建立關聯，則為允許來自受信任來源之 SSH (連接埠 22) 流量的傳入規則。 • 如果堡壘主機或其他網際網路相應元件位於不同的安全群組中，則為允許來自該元件之流量的傳入規則。	✓	

VPC 先決條件

先決條件	對於 ECS 平台	對於 Docker-Local
彈性 IP 地址，用於存取 Ethereum 服務。	✓	✓
執行 EC2 執行個體的子網路。強烈建議使用私有子網路。	✓	✓
兩個可公開存取的子網路。每個子網路必須位於彼此不同的	✓	

先決條件	對於 ECS 平台	對於 Docker-Local
可用區域中，其中一個子網路與 EC2 執行個體的子網路位於相同的可用區域中。		

EC2 執行個體描述檔和 ECS 角色的 IAM 許可範例

您可以指定 EC2 執行個體描述檔 ARN 做為使用範本時的其中一個參數。如果您使用 ECS 容器平台，您也要指定 ECS 角色 ARN。連接到這些角色的許可政策，能讓叢集中的 AWS 資源和執行個體與其他 AWS 資源互動。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 角色。使用下列政策陳述式和程序做為起點，來建立許可。

EC2 執行個體描述檔的範例許可政策

下列許可政策示範當您選擇 ECS 容器平台時，EC2 執行個體描述檔可以執行的動作。相同的政策陳述式可以用在 docker-local 容器平台中，其中移除 `ecs` 內容金鑰以限制存取。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:CreateCluster",
                "ecs:DeregisterContainerInstance",
                "ecs:DiscoverPollEndpoint",
                "ecs:Poll",
                "ecs:RegisterContainerInstance",
                "ecs:StartTelemetrySession",
                "ecs:Submit*",
                "ecr:GetAuthorizationToken",
                "ecr:BatchCheckLayerAvailability",
                "ecr:GetDownloadUrlForLayer",
                "ecr:BatchGetImage",
                "logs:CreateLogStream",
                "logs:PutLogEvents",
                "dynamodb:BatchGetItem",
                "dynamodb:BatchWriteItem",
                "dynamodb:PutItem",
```

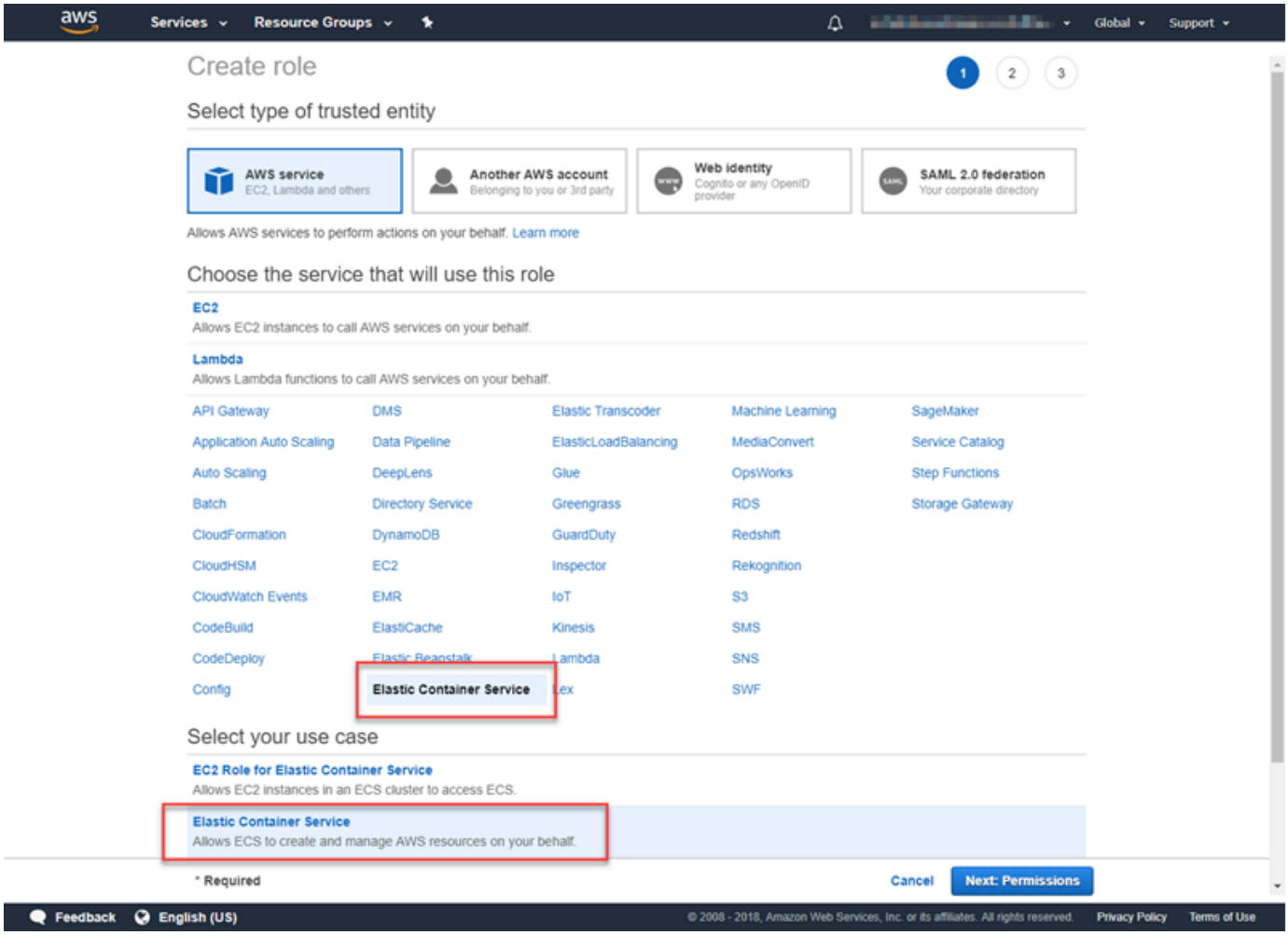
```
                "dynamodb:DeleteItem",
                "dynamodb:GetItem",
                "dynamodb:Scan",
                "dynamodb:Query",
                "dynamodb:UpdateItem"
            ],
            "Resource": "*"
        }
    ]
}
```

建立 ECS 角色和許可

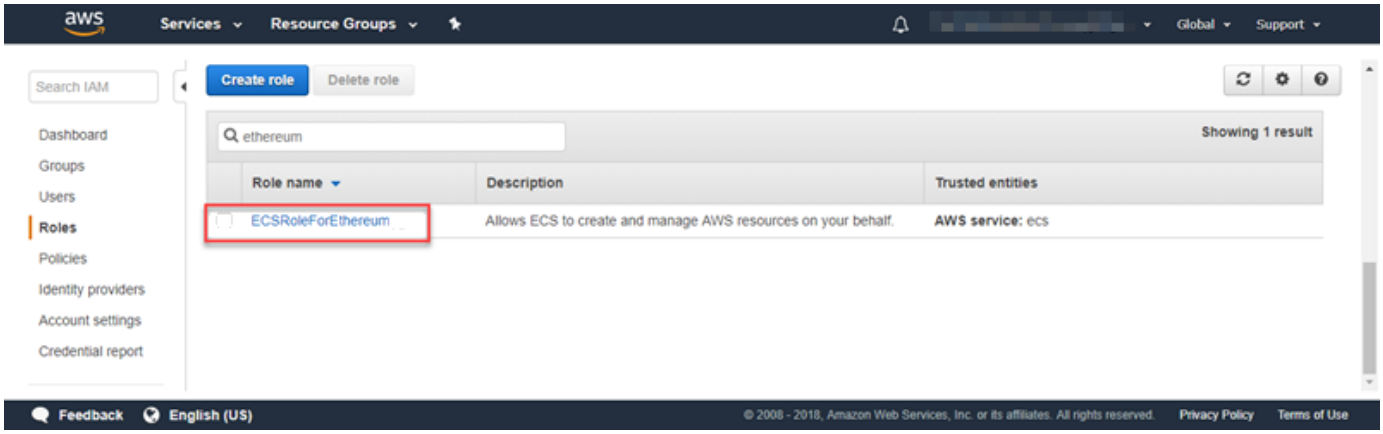
對於連接到 ECS 角色的許可，我們建議您從 AmazonEC2ContainerServiceRole 許可政策開始。請使用下列步驟來建立角色，並連接將此許可政策。使用 IAM 主控台檢視此政策中up-to-date許可。

建立 Amazon ECS 的 IAM 角色

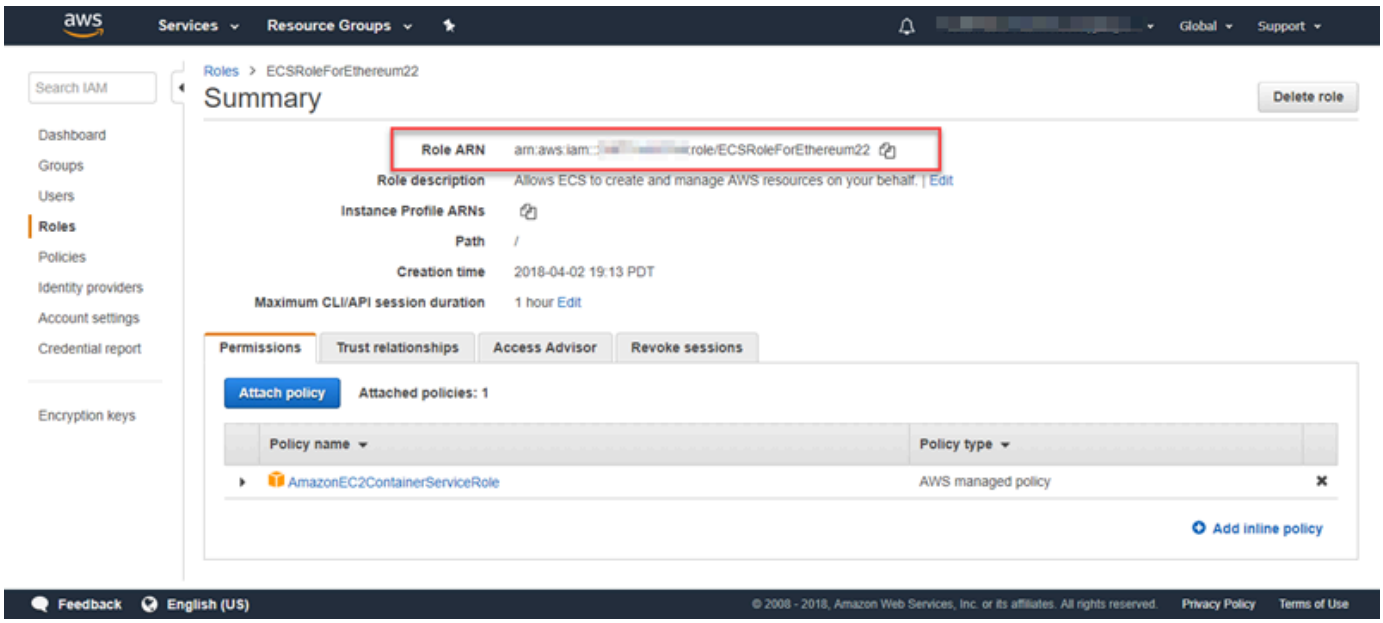
1. 前往網址 https://console.aws.amazon.com/iam/ 開啟 IAM 主控台。
2. 在導覽窗格中，選擇角色 、建立角色。
3. 在 Select type of trusted entity (選擇信任的實體類型) 下，選擇 AWS service (AWS 服務)。
4. 針對 Choose the service that will use this role (選擇將使用此角色的服務)，請選擇 Elastic Container Service。
5. 在 Select your use case (選擇您的使用案例) 下方選擇 Elastic Container Service、Next:Permissions (下一步：許可)。



6. 維持選取 Permissions policy (許可政策) 中的預設政策 (AmazonEC2ContainerServiceRole)，然後選擇 Next:Review (下一步：檢閱)。
7. 在 Role name (角色名稱) 中輸入可協助您識別此角色的值，例如 ECSRoleForEthereum。在 Role Description (角色描述) 中輸入簡短摘要。請記下稍後的角色名稱。
8. 選擇建立角色。
9. 從清單中選擇您剛剛建立的角色。如果您的帳戶有許多角色，您可以搜尋角色名稱。



10. 複製 Role ARN (角色 ARN) 值並加以儲存，讓您稍後可以再次複製。建立 Ethereum 網路時會需要此 ARN。



連線至 Ethereum 資源

在您使用 範本建立的根堆疊顯示 CREATE_COMPLETE 之後，您可以使用 CloudFormation 主控台連線到 Ethereum 資源。您的連線方式取決於您選擇的容器平台，ECS 或 docker-local：

- ECS - 根堆疊的輸出索引標籤提供在 Application Load Balancer 上執行之服務的連結。基於安全理由，無法直接存取這些 URL。若要連線，您可以設定和使用堡壘主機來代理連線。如需詳細資訊，請參閱下面的使用堡壘主機的代理連線。
- docker-local - 您可以使用託管 Ethereum 服務的 EC2 執行個體 IP 地址進行連線，如下所示。使用 EC2 主控台找到範本建立之執行個體的 *ec2-IP-address*。

- EthStats - 使用 http：//*ec2-IP-address*
- EthExplorer - 使用 http：//*ec2-IP-address*：8080
- EthJsonRpc - 使用 http：//*ec2-IP-address*：8545

如果您為 Ethereum Network Subnet ID (Ethereum 網路子網路 ID) (範本中的 List of VPC Subnets to use (要使用的 VPC 子網路清單)) 指定公有子網路，您可以直接連線。您的用戶端對於 SSH (連接埠 22) 以及所列出的連接埠，必須是傳入流量的信任來源。這取決於您使用 Ethereum 的 AWS Blockchain 範本指定的 EC2 安全群組。

如果已指定私有子網路，您可以設定並使用堡壘主機以代理連線至這些地址。如需詳細資訊，請參閱下面的使用堡壘主機的代理連線。

使用堡壘主機的代理連線

在某些組態中，Ethereum 服務可能無法公開使用。在這些情況下，您可以透過堡壘主機連線到 Ethereum 資源。如需堡壘主機的詳細資訊，請參閱 Linux 堡壘主機快速入門指南中的 Linux 堡壘主機架構。

堡壘主機是 EC2 執行個體。請確定符合下列要求：

- 堡壘主機的 EC2 執行個體位於已啟用自動指派公有 IP 且具有網際網路閘道的公有子網路內。
- 堡壘主機具有允許 SSH 連線的金鑰對。
- 堡壘主機與安全群組相關聯，該安全群組允許來自連線用戶端的傳入 SSH 流量。
- 指派給 Ethereum 主機的安全群組（例如，如果 ECS 是容器平台，則為 Application Load Balancer，如果 docker-local 是容器平台，則為主機 EC2 執行個體）允許來自 VPC 內來源的所有連接埠上的傳入流量。

設定堡壘主機後，請確定連線的用戶端使用堡壘主機做為代理。下列範例示範使用 Mac OS 設定代理連線。以堡壘主機 EC2 執行個體的 IP 地址取代 *BastionIP*，並以您複製至堡壘主機的金鑰對檔案取代 *MySshKey.pem*。

在命令列上，輸入下列內容：

```
ssh -i mySshKey.pem  ec2-user@BastionIP -D 9001
```

這會為本機電腦上的連接埠 9001 設定連接埠轉送至堡壘主機。

接著，將您的瀏覽器或系統設定為使用 的 SOCKS 代理`localhost:9001`。例如，使用 Mac OS，選取 System Preferences (系統偏好設定)、Network (網路)、Advanced (進階)，選取 SOCKS proxy (SOCKS 代理)，然後輸入 localhost:9001。

在 Chrome 上使用 FoxyProxy Standard，請選取 More Tools (更多工具)、Extensions (擴充功能)。在 FoxyProxy Standard 下方選取 Details (詳細資訊)、Extension options (擴充功能選項)、Add New Proxy (新增代理)。選取 Manual Proxy Configuration (手動代理組態)。在 Host or IP Address (主機或 IP 地址) 中輸入 localhost，在 Port (連接埠) 中輸入 9001。選取 SOCKS Proxy? (SOCKS 代理？)、Save (儲存)。

您現在應該能夠連線到範本輸出中列出的 Ethereum 主機地址。

使用適用於 Hyperledger Fabric 的 AWS 區塊鏈範本

Hyperledger Fabric 是一種區塊鏈架構，可執行名為 chaincode 的智慧合約，以 Go 撰寫。您可以使用 Hyperledger Fabric 建立私有網路，限制可連線至網路並參與網路的對等。如需 Hyperledger Fabric 的詳細資訊，請參閱 Hyperledger Fabric 文件。如需鏈結碼的詳細資訊，請參閱 Hyperledger Fabric 文件中的開發人員的鏈結碼主題。

適用於 Hyperledger Fabric 的 AWS Blockchain 範本僅支援 docker-local 容器平台，這表示 Hyperledger Fabric 容器部署在單一 EC2 執行個體上。

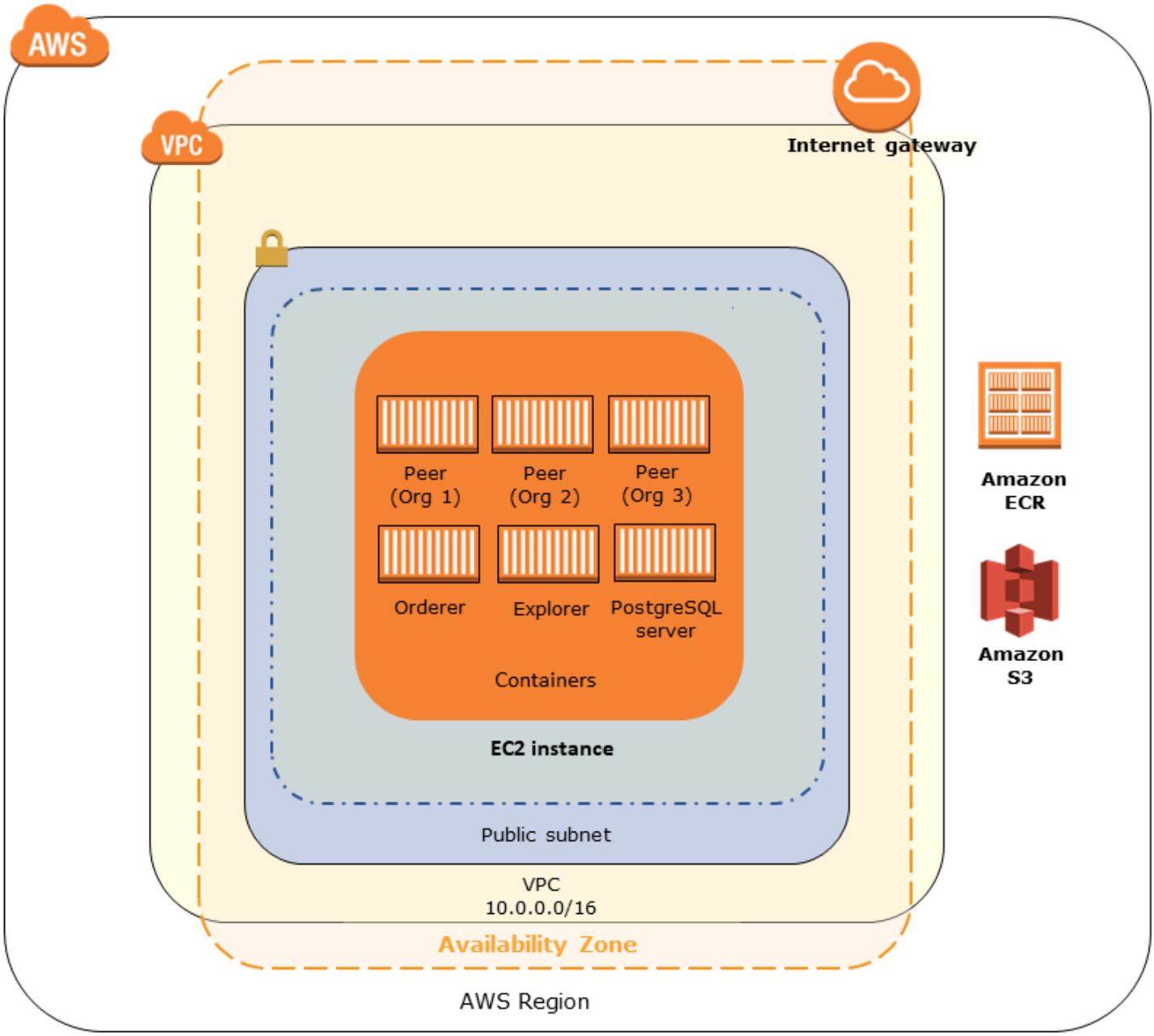
啟動連結

如需使用 Hyperledger Fabric 範本在特定區域中啟動的連結，請參閱 AWS 區塊鏈範本入門。CloudFormation

Hyperledger Fabric 元件的 AWS 區塊鏈範本

適用於 Hyperledger Fabric 的 AWS Blockchain 範本會使用 Docker 建立 EC2 執行個體，並使用該執行個體上的容器啟動 Hyperledger Fabric 網路。網路包含一個訂單服務和三個組織，每個都有一個對等服務。範本還會啟動 Hyperledger Explorer 容器，可讓您以瀏覽區塊鏈資料。並啟動 PostgreSQL 伺服器容器來支援 Hyperledger Explorer。

下圖說明使用 範本建立的 Hyperledger Fabric 網路：



先決條件

使用範本啟動 Hyperledger Fabric 網路之前，請確定滿足下列要求：

- 您使用的 IAM 原則 （使用者或群組） 必須具有使用所有相關服務的許可。
- 您必須能夠存取金鑰對，以便用於存取 EC2 執行個體 (例如，使用 SSH)。金鑰必須與執行個體位於相同的區域。

- 您必須連接具有許可政策的 EC2 執行個體描述檔，以允許存取 Amazon S3 和 Amazon Elastic Container Registry (Amazon ECR) 以提取容器。如需許可政策範例，請參閱 EC2 執行個體描述檔的範例 IAM 許可。
- 您必須擁有具有公有子網路的 Amazon VPC 網路，或是具有 NAT 閘道和彈性 IP 地址的私有子網路 CloudFormation，才能存取 Amazon S3 和 Amazon ECR。
- 您的 EC2 安全群組規則必須擁有傳入規則，以允許來自需使用 SSH 連接到執行個體之 IP 地址的 SSH 流量 (連接埠 22)，以及需要連接到 Hyperledger Explorer (連接埠 8080) 的用戶端。

EC2 執行個體描述檔的範例 IAM 許可

當您使用適用於 Hyperledger Fabric 的 AWS Blockchain 範本時，您可以將 EC2 執行個體描述檔 ARN 指定為其中一個參數。使用以下政策陳述式做為起點，來建立連接到 EC2 角色和執行個體描述檔的許可政策。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecr:GetAuthorizationToken",
                "ecr:BatchCheckLayerAvailability",
                "ecr:GetDownloadUrlForLayer",
                "ecr:GetRepositoryPolicy",
                "ecr:DescribeRepositories",
                "ecr:ListImages",
                "ecr:DescribeImages",
                "ecr:BatchGetImage",
                "s3:Get*",
                "s3:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

連線至 Hyperledger Fabric 資源

在您使用範本建立的根堆疊顯示 CREATE_COMPLETE 之後，您就可以連線到 EC2 執行個體上的 Hyperledger Fabric 資源。如果指定了公有子網路，則可以像連接到任何其他 EC2 執行個體一樣地連接到 EC2 執行個體。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的使用 SSH 連線至 Linux 執行個體。

如果您指定了私有子網路，則可以設定並使用堡壘主機來代理與 Hyperledger Fabric 資源的連線。如需詳細資訊，請參閱下面的使用堡壘主機的代理連線。

> **Note**
>
> 您可能會注意到範本會將公有 IP 地址配置給託管 Hyperledger Fabric 服務的 EC2 執行個體；不過，此 IP 地址無法公開存取，因為您指定的私有子網路中的路由政策不允許此 IP 地址與公有來源之間的流量。

使用堡壘主機的代理連線

在某些組態中，Hyperledger Fabric 服務可能無法公開使用。在這些情況下，您可以透過堡壘主機連線到 Hyperledger Fabric 資源。如需堡壘主機的詳細資訊，請參閱《Linux 堡壘主機快速入門指南》中的 Linux 堡壘主機架構。

堡壘主機是 EC2 執行個體。請確定符合下列要求：

- 堡壘主機的 EC2 執行個體位於已啟用自動指派公有 IP 且具有網際網路閘道的公有子網路內。
- 堡壘主機具有允許 SSH 連線的金鑰對。
- 堡壘主機與安全群組相關聯，該安全群組允許來自連線用戶端的傳入 SSH 流量。
- 指派給 Hyperledger Fabric 主機的安全群組（例如，如果 ECS 是容器平台，則為 Application Load Balancer，如果 docker-local 是容器平台，則為主機 EC2 執行個體）允許來自 VPC 內來源的所有連接埠上的傳入流量。

設定堡壘主機後，請確定連線的用戶端使用堡壘主機做為代理。下列範例示範使用 Mac OS 設定代理連線。以堡壘主機 EC2 執行個體的 IP 地址取代 *BastionIP*，並以您複製至堡壘主機的金鑰對檔案取代 *MySshKey.pem*。

在命令列上，輸入下列內容：

```
ssh -i mySshKey.pem  ec2-user@BastionIP -D 9001
```

這會為本機電腦上的連接埠 9001 設定連接埠轉送至堡壘主機。

接著，將您的瀏覽器或系統設定為使用 的 SOCKS 代理`localhost:9001`。例如，使用 Mac OS，選取 System Preferences (系統偏好設定)、Network (網路)、Advanced (進階)，選取 SOCKS proxy (SOCKS 代理)，然後輸入 localhost:9001。

在 Chrome 上使用 FoxyProxy Standard，請選取 More Tools (更多工具)、Extensions (擴充功能)。在 FoxyProxy Standard 下方選取 Details (詳細資訊)、Extension options (擴充功能選項)、Add New Proxy (新增代理)。選取 Manual Proxy Configuration (手動代理組態)。在 Host or IP Address (主機或 IP 地址) 中輸入 localhost，在 Port (連接埠) 中輸入 9001。選取 SOCKS Proxy? (SOCKS 代理？)、Save (儲存)。

您現在應該能夠連線到範本輸出中列出的 Hyperledger Fabric 主機地址。

文件歷史記錄

下表說明此指南的文件變更。

最新文件更新：2019 年 5 月 1 日

變更	描述	Date
終止 AWS Blockchain 範本。	AWS 區塊鏈範本已於 2019 年 4 月 30 日終止。不會對此服務或此支援文件進行進一步更新。為了獲得最佳的受管區塊鏈體驗 AWS，我們建議您使用 Amazon Managed Blockchain (AMB)。	2019 年 5 月 1 日
堡壘主機更新。	已修改新增堡壘主機的入門教學和 Ethereum 先決條件需求，其允許在使用 ECS 平台時，存取透過內部負載平衡器提供的 Web 資源，而在使用 docker-local 時，可存取 EC2 執行個體。	2018 年 5 月 3 日
建立指南。	支援 AWS Blockchain 範本初始版本的新開發人員指南。	2018 年 4 月 19 日

AWS 詞彙表

如需最新的 AWS 術語，請參閱 AWS 詞彙表 參考中的AWS 詞彙表。