



使用者指南

# Amazon Lightsail



# Amazon Lightsail: 使用者指南

Copyright © 2024 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 Lightsail ? .....	1
功能 .....	1
Lightsail 是為誰提供的 ? .....	2
訪問 Lightsail .....	3
開始使用 .....	4
相關服務 .....	4
估算、計費和成本最佳化 .....	4
設定 .....	6
註冊一個 AWS 帳戶 .....	6
建立具有管理存取權的使用者 .....	6
開始使用 .....	8
步驟 1：完成先決條件 .....	8
步驟 2：建立執行個體 .....	8
步驟 3：連接到您的執行個體 .....	9
步驟 4：將儲存體新增至執行個體 .....	11
步驟 5：建立快照 .....	11
步驟 6：清除 .....	11
後續步驟 .....	12
執行個體 .....	13
建立 執行個體 .....	13
Linux 執行個體 .....	13
Windows 執行個體 .....	17
Blueprints (藍圖) .....	25
作業系統 .....	25
資料庫應用 .....	28
CMS應用 .....	28
應用程式堆疊和伺服 .....	30
電子商務應用程式 .....	32
專案管理應用程式 .....	33
執行個體防火牆 .....	33
Lightsail 防火牆 .....	33
建立防火牆規則 .....	34
指定通訊協定 .....	35
指定連接埠 .....	36

指定應用程式層級通訊協定類型 .....	37
指定來源 IP 地址 .....	38
預設 Lightsail 牆規則 .....	38
新增防火牆規則 .....	40
刪除防火牆規則 .....	42
執行個體防火牆規則 .....	43
突發容量和效能 .....	45
CPU性能 .....	46
突發容量累積 .....	48
識別執行個體突發 .....	49
監視器爆發容量 .....	50
檢視突發容量 .....	52
高 CPU 的疑難排解 .....	55
執行個體管理 .....	55
啟動、停止或重新啟動您的 執行個體 .....	55
強制停止實例 .....	58
增強型網路 .....	60
擴充視窗伺服器檔案系統 .....	61
Linux shell 指令碼 .....	64
PowerShell 腳本 .....	66
Windows 安全最佳實務 .....	68
刪除實例 .....	73
從 Lightsail 主控台首頁刪除執行個體 .....	73
從 Lightsail 主控台執行個體管理頁面刪除執行個體 .....	74
使用刪除執行個體 AWS CLI .....	74
後續步驟 .....	76
SSH並連線至執行個體 .....	76
選擇金鑰對選項 .....	77
連線至您的執行個體 .....	78
管理執行個體上儲存的金鑰 .....	79
設定SSH金鑰 .....	79
管理 SSH 金鑰 .....	82
管理執行個體 SSH 金鑰 .....	95
連接至 Linux 執行個體 .....	100
連接至 Windows 執行個體 .....	120
AWS CloudShell .....	134

執行個體中繼資料服務 .....	139
使用執行個體中繼資料服務 .....	139
其他 IMDS 文件 .....	139
設定 IMDS .....	140
磁碟 .....	146
區塊儲存磁碟 .....	146
磁碟配額 .....	146
將磁碟連結至 Linux 執行個體 .....	147
步驟 1：建立新的磁碟並將其連接至您的執行個體 .....	147
步驟 2：連接執行個體以格式化和掛載磁碟 .....	148
步驟 3：在每次重新啟動執行個體時掛載磁碟 .....	153
將磁碟連結至 Windows 執行個體 .....	154
步驟 1：建立新的區塊儲存磁碟，並將它連接至您的執行個體 .....	154
步驟 2：連線至執行個體並讓區塊儲存磁碟上線 .....	156
步驟 3：初始化區塊儲存磁碟 .....	158
步驟 4：以檔案系統格式化磁碟 .....	160
卸離和刪除磁碟 .....	162
必要條件 .....	162
分離和刪除磁碟 .....	162
快照 .....	164
手動快照 .....	164
自動快照 .....	164
系統磁碟快照 .....	165
透過快照建立新的資源 .....	165
複製快照 .....	166
將快照匯出到 Amazon EC2 .....	166
刪除快照 .....	166
自動快照 .....	166
自動快照限制 .....	167
自動快照保留 .....	167
使用 Lightsail 主控台啟用或停用自動執行個體快照 .....	167
啟用或停用執行個體或區塊儲存磁碟的自動快照，使用 AWS CLI .....	169
變更快照時間 .....	172
刪除自動快照 .....	176
保留自動快照 .....	180
快照 .....	185

視窗快照和系統 .....	186
步驟 1：在執行 Sysprep 前建立備份快照 .....	187
步驟 2：連線到您的執行個體，並使用 Sysprep 將其關閉 .....	188
步驟 3：在執行 Sysprep 後建立快照 .....	191
後續步驟 .....	191
建立區塊儲存磁碟快照 .....	192
從快照建立磁碟 .....	193
步驟 1：尋找您的磁碟快照，然後選擇建立新的磁碟 .....	193
步驟 2：從磁碟快照建立新磁碟 .....	194
建立根磁碟區快照。 .....	196
步驟 1：完成先決條件 .....	196
步驟 2：建立執行個體根磁碟區的快照 .....	196
步驟 3：從快照建立區塊儲存磁碟並將其連接至執行個體 .....	198
步驟 4：從執行個體存取區塊儲存磁碟 .....	200
透過快照建立執行個體 .....	205
透過快照建立更大的資源 .....	207
必要條件 .....	208
建立您的資源 .....	208
使用從快照建立更大的資源 AWS CLI .....	209
必要條件 .....	209
步驟 1：取得您的快照名稱 .....	210
步驟 2：選擇搭售套件 .....	210
第 3 步：編寫 AWS CLI 命令並創建新實例 .....	213
後續步驟 .....	214
刪除快照 .....	214
跨區域複製快照 .....	216
必要條件 .....	216
複製快照 .....	216
後續步驟 .....	218
將快照匯出至 EC2 .....	218
從匯出的 Lightsail 快照建立 Amazon EC2 資源 .....	220
選擇 Amazon 執行個體 EC2 類型 .....	221
Connect 到 Amazon EC2 實例 .....	221
保護 Amazon 執行個體 EC2 .....	222
如何匯出快照 .....	222
監控出口 .....	226

透過匯出的快照建立 EC2 執行個體 .....	227
透過匯出的快照建立 EBS 磁碟區 .....	235
Connect 至 EC2 執行個體 .....	237
安全執行個體 .....	244
連接至 Windows EC2 執行個體 .....	253
保護 Windows EC2 執行個體 .....	259
AWS CloudFormation 堆疊 .....	261
域和 DNS .....	263
域註冊的運作方式 .....	263
您可以在其中註冊的 Lightsail .....	264
域註冊的定價 .....	264
網域的其他相關資訊 .....	264
DNS 在 Lightsail .....	265
DNS 術語 .....	265
DNS Lightsail DNS 區域支援的記錄類型 .....	267
建立 DNS 區域 .....	269
編輯 DNS 區域 .....	275
刪除 DNS 區域 .....	275
網際網路流量路由 .....	276
將網域指向執行個體 .....	278
將域引導至負載平衡器 .....	280
傳輸 DNS 管理 .....	283
使用 Route 53 .....	284
註冊網域 .....	288
使用註冊新網域 .....	289
域詳細資訊 .....	292
格式化域名稱 .....	293
格式化域名稱註冊的域名稱 .....	293
格式化 DNS 區域和記錄的域名稱 .....	293
在 DNS 區域和記錄的名稱中使用星號 (*) .....	293
後續步驟 .....	295
管理 R53 中的域 .....	295
檢視域註冊的狀態 .....	295
鎖定域以防止未經授權轉移到另一個註冊商 .....	296
還原已過期或已刪除的域 .....	296
轉移域註冊 .....	296

刪除域名稱註冊 .....	296
註冊信息 .....	296
術語 .....	297
自動網域續約 .....	297
註冊者、管理和技術聯絡人 .....	298
與註冊者相同 .....	298
聯絡人類型 .....	298
名字、姓氏 .....	298
組織 .....	298
電子郵件 .....	299
電話 .....	299
地址 1 .....	299
地址 2 .....	299
國家 .....	299
州 .....	299
城市 .....	299
郵遞區號 .....	300
隱私權保護 .....	300
註冊續約 .....	300
自動續約 .....	301
在網域註冊期間為網域設定自動續約 .....	302
為已註冊的網域設定自動續約 .....	302
隱私權保護 .....	303
完成先決條件 .....	303
管理網域的隱私權保護 .....	303
域聯絡資訊 .....	304
網域擁有者是誰？ .....	304
更新域的聯絡資訊 .....	304
資料庫 .....	306
比較資料庫 .....	306
比較 Lightsail 中的受管資料庫 .....	306
將資料匯入最佳化 .....	308
高可用性資料庫 .....	308
建立 資料庫 .....	308
後續步驟 .....	312
連接至 MySQL .....	312

步驟 1：取得 MySQL 資料庫的連線詳細資訊 .....	312
步驟 2：設定 MySQL 資料庫的公有可用性 .....	313
步驟 3：設定您的資料庫用戶端來連接到 MySQL 資料庫 .....	314
後續步驟 .....	316
使用 SSL 連接到 MySQL .....	316
支援的連線 .....	317
必要條件 .....	317
使用 SSL 連接到 MySQL 資料庫 .....	317
連接至 PostgreSQL .....	319
步驟 1：取得您的 PostgreSQL 資料庫連線詳細資訊 .....	320
步驟 2：設定您 PostgreSQL 資料庫的公有可用性 .....	321
步驟 3：設定您的資料庫用戶端來連接到 PostgreSQL 資料庫 .....	321
後續步驟 .....	324
使用 Connect 到波斯特格雷 SQL SSL .....	324
必要條件 .....	324
使用 Connect 到您的 Postgres 數據庫 SSL .....	324
刪除資料庫 .....	325
資料匯入模式 .....	326
匯入 SQL 資料 .....	327
匯入資料 PostgreSQL .....	329
資料庫日誌 .....	331
MySQL 查詢日誌 .....	333
停用 point-in-time-backups .....	336
先決條件 .....	336
停用資料庫 point-in-time 備份 .....	336
資料庫快照 .....	338
後續步驟 .....	339
還原資料庫 .....	339
透過快照建立資料庫 .....	342
下載 SSL 憑證 .....	344
所有 AWS 區域的憑證套件 .....	345
特定 AWS 區域的憑證套件 .....	345
更新 CA 憑證 .....	345
維護和備份時段 .....	348
必要條件 .....	349
為您的資料庫變更維護時段 .....	349

後續步驟 .....	352
管理資料庫密碼 .....	352
後續步驟 .....	354
公開模式 .....	354
後續步驟 .....	355
更新參數 .....	355
必要條件 .....	355
取得可用資料庫參數的清單 .....	356
更新資料庫參數 .....	357
升級主要版本 .....	359
必要條件 .....	359
更新資料庫主要版本 .....	359
後續步驟 .....	362
從 MySQL 移 .....	362
步驟 1：了解變更 .....	363
步驟 2：完成事前準備 .....	363
步驟 3：連接到 MySQL 5.6 資料庫並匯出資料 .....	363
步驟 4：連接到 MySQL 5.7 資料庫並匯入資料 .....	367
步驟 5：測試應用程式並完成遷移 .....	370
負載平衡器 .....	371
負載平衡器功能 .....	371
何時使用負載平衡器 .....	372
建議的負載平衡 應用程式 .....	372
開始使用負載平衡器 .....	372
建立負載平衡器 .....	372
必要條件 .....	372
建立負載平衡器 .....	373
將執行個體附接至負載平衡器 .....	374
後續步驟 .....	374
更新 負載平衡器設定 .....	375
運作狀態檢查 .....	375
加密流量 (HTTPS) .....	376
工作階段持續性 .....	376
執行個體負載平衡 .....	376
一般準則：使用資料庫的應用程式 .....	376
WordPress .....	376

Node.js .....	377
Magento .....	377
GitLab .....	377
Drupal .....	378
LAMP堆疊 .....	378
MEAN堆疊 .....	379
Redmine .....	379
Nginx .....	379
Joomla! .....	379
設定 TLS 安全政策 .....	380
安全政策概觀 .....	380
支援的安全政策和通訊協定 .....	380
完成先決條件 .....	382
使用主控台設定安全性原則 .....	382
使用設定安全性原則 AWS CLI .....	382
HTTP 至 HTTPS 重新導向 .....	383
完成先決條件 .....	384
使用 Lightsail 主控台在負載平衡器上設定 HTTPS 重新導向 .....	384
為負載平衡器設定 HTTP 至 HTTPS 重新導向，並使用 AWS CLI .....	385
工作階段持續性 .....	386
啟用工作階段持續性 .....	386
調整 Cookie 持續時間 .....	386
運作狀態檢查 .....	387
自訂您的運作狀態檢查路徑 .....	388
運作狀態檢查指標 .....	389
運作狀態檢查 .....	391
分離執行個體 .....	392
刪除負載平衡器 .....	392
分發 .....	393
使用案例 .....	395
設定分發 .....	396
節點和 IP 地址範圍 .....	397
建立分發 .....	397
必要條件 .....	398
原始伺服器資源 .....	398
原始伺服器通訊協定政策 .....	399

快取行為和快取預設 .....	400
最適合 WordPress 緩存預設 .....	401
預設行為 .....	401
目錄和檔案覆寫 .....	402
進階快取設定 .....	403
分發計劃 .....	406
建立分發 .....	406
後續步驟 .....	408
刪除 分發 .....	409
刪除分發 .....	409
快取行為 .....	409
快取預設 .....	410
最適合 WordPress 緩存預設 .....	411
預設行為 .....	411
目錄和檔案覆寫 .....	412
進階快取設定 .....	413
變更分發的快取行為 .....	415
重設快取 .....	416
變更原始伺服器 .....	416
原始伺服器通訊協定政策 .....	417
變更分發原始伺服器 .....	417
搭配使用儲存貯體與分發 .....	419
步驟 1：完成先決條件 .....	419
步驟 2：修改儲存貯體許可 .....	420
步驟 3：建立具有儲存貯體作為原始伺服器的分發 .....	423
步驟 4：啟用分發的自訂子網域 .....	425
第 5 步：在您 WordPress 的網站上安裝 WP 卸載媒體精簡版插件 .....	425
步驟 6：測試您的 WordPress 網站與 Lightsail 儲存貯體和發行版本之間的連線 .....	431
管理儲存貯體和物件 .....	434
變更計畫 .....	436
變更您的分發計劃 .....	436
分發自訂域 .....	436
必要條件 .....	437
啟用分發的自訂網域 .....	437
將域指向分發 .....	438
變更自訂域 .....	440

停用分發自訂網域 .....	440
將分發域新增至容器服務 .....	441
請求和回應行為 .....	443
分發如何處理和轉送請求至原始伺服器 .....	443
分發如何處理來自原始伺服器的回應 .....	457
POST 分發 .....	460
測試您的分發 .....	460
聯網 .....	462
負載平衡器 .....	462
靜態 IPs .....	462
IP 地址 .....	462
執行個體的私人和公用IPv4位址 .....	462
執行個體的靜態IPv4位址 .....	464
IPv6適用於執行個體、容器服務、CDN分發和負載平衡器 .....	465
靜態 IP 地址 .....	467
雙堆疊網路 .....	472
僅限 IPV6 的網路功能 .....	475
區域與可用區域 .....	479
SSH按鍵和 Lightsail 區域 .....	480
使用 Lightsail 區域的秘訣 .....	480
Lightsail 可用區域 .....	481
可用區域和您的 Lightsail 程式 .....	481
VPC窺視 .....	481
SSL/TLS證書 .....	482
為什麼要使用 HTTPS ? .....	483
程序概觀 .....	483
在您的分發或容器服務中使用SSL/TLS憑證 .....	484
搭配負載平衡器使用SSL/TLS憑證 .....	484
容器憑證 .....	485
分發憑證 .....	489
負載平衡器憑證 .....	500
設定反向 DNS .....	508
必要條件 .....	508
將請求提交到 AWS Support 來設定反向 DNS .....	509
儲存貯體 .....	511
物件儲存概念 .....	511

管理儲存貯體和物件 .....	513
建立儲存貯體 .....	513
建立 儲存貯體 .....	514
管理儲存貯體和物件 .....	514
刪除儲存貯體 .....	516
強制刪除儲存貯體 .....	516
使用主控台刪除值區 .....	517
使用刪除值區 AWS CLI .....	517
管理儲存貯體和物件 .....	519
存取金鑰 .....	521
建立儲存貯體的存取金鑰 .....	521
封鎖公有存取權 .....	522
為您的帳戶設定封鎖公有存取 .....	523
管理儲存貯體和物件 .....	525
儲存貯體存取日誌 .....	527
啟用日誌傳送需要什麼？ .....	527
日誌物件金鑰格式 .....	528
交付日誌的方式？ .....	528
存取日誌傳送最佳作法 .....	529
儲存貯體記錄狀態變更會在一段時間後生效 .....	529
存取日誌格式 .....	529
管理存取記錄 .....	542
使用存取日誌 .....	546
儲存貯體物件 .....	550
使用主控台篩選物件 .....	551
使用檢視物件 AWS CLI .....	553
管理儲存貯體和物件 .....	555
複製和移動物件 .....	557
刪除物件 .....	561
下載物件 .....	568
篩選物件 .....	572
管理物件版本控制 .....	576
還原物件版本 .....	581
標記物件 .....	585
儲存貯體資源存取 .....	589
設定儲存貯體的資源存取 .....	589

變更儲存貯體計畫 .....	590
使用 Lightsail 主控台變更值區的儲存空間計畫 .....	590
使用變更儲存貯體的儲存空間計畫 AWS CLI .....	590
設定存取許可 .....	592
設定儲存貯體存取許可 .....	593
跨帳戶存取權 .....	594
設定儲存貯體的跨帳戶存取 .....	594
個別物件存取許可 .....	595
設定個別物件存取許可 .....	595
分段上傳 .....	596
分段上傳程序 .....	597
並行分段上傳操作 .....	599
分段上傳保留 .....	600
Amazon Simple Storage Service 分段上傳限制 .....	600
分割要上傳的檔案 .....	600
使用 AWS CLI 啟動分段上傳 .....	600
使用上傳零件 AWS CLI .....	601
列出多部分上傳的部分使用 AWS CLI .....	602
建立分段上傳 .json 檔案 .....	604
使用完成多部分上傳 AWS CLI .....	606
列出值區的多部分上傳內容，使用 AWS CLI .....	607
使用停止多部分上傳 AWS CLI .....	608
命名規則 .....	609
儲存貯體名稱的範例 .....	610
物件索引鍵名稱 .....	610
鍵值名稱 .....	610
物件索引鍵命名準則 .....	611
XML 相關物件索引鍵約束 .....	613
物件儲存安全最佳實務 .....	614
預防性安全最佳實務 .....	615
監控和稽核最佳實務 .....	619
儲存貯體許可 .....	620
儲存貯體存取許可 .....	621
個別物件存取許可 .....	621
跨帳戶存取權 .....	622
存取金鑰 .....	622

資源存取 .....	622
Amazon S3 封鎖公開存取 .....	622
將文件上傳到存儲桶 .....	623
物件索引鍵名稱和版本控制 .....	623
使用 Lightsail 主控台將檔案上傳至值區 .....	624
使用 AWS CLI將檔案上傳至儲存貯體 .....	624
設定IPv6僅AWSCLI用於要求 .....	625
管理值區和物件 .....	626
容器服務 .....	629
容器 .....	629
Lightsail 集裝箱服務元素 .....	630
Lightsail 貨櫃服務 .....	630
容器服務容量 (規模和動力) .....	631
定價 .....	632
部署 .....	632
部署版本 .....	633
容器映像來源 .....	633
貨櫃服務 ARN .....	633
公有端點和預設網域 .....	634
自訂網域和 SSL/TLS 憑證 .....	635
容器日誌 .....	635
指標 .....	635
使用 Lightsail 貨櫃服務 .....	635
建立容器 .....	637
容器服務容量 (規模和動力) .....	637
定價 .....	637
容器服務狀態 .....	638
建立容器服務 .....	639
容器映像 .....	641
步驟 1：完成先決條件 .....	641
步驟 2：建立 Dockerfile 並建置容器映像 .....	642
步驟 3：執行新的容器映像 .....	643
(選用) 步驟 4：清理在本機電腦上執行的容器 .....	644
建立容器映像後的後續步驟 .....	645
管理容器映像 .....	645
安裝容器服務插件 .....	649

ECR 私有儲存庫存取 .....	656
管理容器和部署 .....	672
必要條件 .....	673
部署參數 .....	673
容器之間的通訊 .....	677
容器日誌 .....	677
部署版本 .....	678
部署狀態 .....	678
部署失敗 .....	678
檢視目前的容器服務部署 .....	678
建立或修改容器服務部署 .....	679
變更容器容量 .....	681
管理部署版本 .....	682
檢視容器日誌 .....	683
容器服務自訂域 .....	686
容器服務自訂網域限制 .....	686
必要條件 .....	686
檢視容器服務的自訂網域 .....	687
啟用容器服務的自訂網域 .....	687
停用容器服務的自訂網域 .....	688
將 Lightsail 網域指向容器 .....	689
將 Route 53 域指向容器 .....	691
刪除容器 .....	696
刪除容器服務 .....	696
安全 .....	698
基礎架構安全 .....	698
恢復能力 .....	698
身分與存取管理 .....	699
物件 .....	699
使用身分來驗證 .....	699
使用政策管理存取權 .....	703
AWS 受管政策 .....	706
Lightsail 和角色 .....	708
管理 IAM 使用者存取權 .....	727
更新管理 .....	733
執行個體藍圖軟體支援 .....	733

法規遵循驗證 .....	734
監控效能 .....	736
有效監控您的資源 .....	736
指標概念和術語 .....	736
指標 .....	737
指標保留 .....	737
統計資料 .....	737
單位 .....	737
期間 .....	738
警示 .....	738
Lightsail 中的可用度量 .....	738
執行個體指標 .....	738
資料庫指標 .....	739
分發指標 .....	739
負載平衡器指標 .....	740
容器服務指標 .....	741
儲存貯體指標 .....	741
資源運作狀態指標 .....	742
執行個體指標 .....	742
資料庫指標 .....	743
分發指標 .....	743
負載平衡器指標 .....	743
容器服務指標 .....	744
儲存貯體指標 .....	745
指標通知 .....	745
檢視 執行個體指標 .....	746
指標警示 .....	749
建立執行個體警示 .....	759
刪除或停用警示 .....	764
儲存貯體指標 .....	765
儲存貯體指標 .....	765
在 Lightsail 主控台中檢視儲存貯體指標 .....	765
管理儲存貯體和物件 .....	766
建立 警示 .....	768
容器指標 .....	771
容器服務指標 .....	772

在 Lightsail 主控台中檢視容器服務指標 .....	772
資料庫指標 .....	773
資料庫指標 .....	773
在 Lightsail 主控台中檢視資料庫度量 .....	773
檢視資料庫指標後的後續步驟 .....	774
建立資料庫警示 .....	774
分發指標 .....	779
分發指標 .....	779
在 Lightsail 主控台中檢視分佈指標 .....	780
檢視分發指標後的後續步驟 .....	780
建立分發警示 .....	781
負載平衡器指標 .....	785
負載平衡器指標 .....	786
檢視負載平衡器指標 .....	787
後續步驟 .....	787
負載平衡器警示 .....	788
新增通知聯絡人 .....	792
區域性通知聯絡人限制 .....	793
簡訊支援 .....	793
電子郵件聯絡人驗證 .....	794
使用 Lightsail 主控台新增通知連絡人 .....	795
使用 AWS CLI 新增通知聯絡人 .....	800
新增通知聯絡人之後的後續步驟 .....	802
刪除通知聯絡人 .....	802
使用 Lightsail 主控台刪除通知連絡人 .....	802
使用 AWS CLI 刪除通知聯絡人 .....	803
刪除通知聯絡人後的後續步驟 .....	804
標籤 .....	805
使用標籤來整理帳單和控制存取 .....	805
支援標記的 Lightsail 資源 .....	805
標籤限制 .....	807
新增標籤 .....	807
後續步驟 .....	809
刪除標籤 .....	809
基於標籤的許可和授權 .....	811
使用標籤來控制存取 .....	811

步驟 1：建立 IAM 政策 .....	811
步驟 2：將政策連接至使用者或群組 .....	813
使用標籤整理成本 .....	813
步驟 1：新增索引鍵值標籤至 資源 .....	813
步驟 2：啟用使用者定義的成本分配標籤 .....	814
步驟 3：設定成本分配報告並檢視 .....	814
使用標籤來整理資源 .....	814
檢視資源的標籤 .....	815
使用標籤篩選資源 .....	816
故障診斷 .....	818
WordPress 設置 .....	818
常見錯誤 .....	819
安裝失敗 .....	822
403 錯誤 (未經授權) .....	826
區塊儲存磁碟 .....	827
一般磁碟錯誤 .....	827
基於瀏覽器SSH或RDP客戶端 .....	828
錯誤訊息：無法連線 .....	828
錯誤訊息：目前無法連線 .....	830
Ghost 服務無法使用 .....	831
啟動 Ghost 服務 .....	831
IAM問題 .....	833
我沒有執行任何動作的 Lightsail .....	834
我沒有授權執行 iam : PassRole .....	834
我想要檢視我的存取金鑰 .....	835
我是系統管理員，想要允許其他人存取 Lightsail .....	835
我想允許我 AWS 帳戶以外的人員存取我的 Lightsail 資源 .....	836
IPv6 可達性 .....	836
為雙堆疊執行個體啟用 IPv6 .....	836
設定執行個體的防火牆 .....	838
測試執行個體的可達性 .....	839
執行個體容量不足錯誤 .....	841
啟動新的執行個體時容量不足 .....	841
啟動停止的執行個體時容量不足 .....	842
相關資訊 .....	842
負載平衡器 .....	842

一般負載平衡器錯誤 .....	843
通知 .....	843
SSL/TLS證書 .....	845
教學課程 .....	846
快速入門指南 .....	847
AlmaLinux .....	847
cPanel & WHM .....	856
Drupal .....	869
Ghost .....	878
GitLab 特首 .....	890
Joomla! .....	900
LAMP .....	911
Magento .....	913
Nginx .....	929
Node.js .....	931
Plesk .....	933
PrestaShop .....	937
Redmine .....	952
WordPress .....	962
WordPress 多站點 .....	968
Bitnami .....	976
Bitnami 使用者名稱和密碼 .....	976
移除 Bitnami 橫幅 .....	984
WordPress .....	987
配置 WordPress .....	987
連接至 Amazon S3 .....	995
連接至 Aurora 資料庫 .....	1003
連接至 MySQL .....	1010
Connect 至儲存桶 .....	1014
配置一個 CDN .....	1029
啟用電子郵件 .....	1033
啟用 HTTPS .....	1043
遷移到 Lightsail .....	1052
WordPress 多站點 .....	1060
WordPress 多站點：將博客添加為域 .....	1060
WordPress 多網站：將部落格新增為子網域 .....	1067

WordPress 多站點：定義域 .....	1070
Let's Encrypt .....	1072
LAMP Let's Encrypt 憑證 .....	1073
Nginx Let's Encrypt 憑證 .....	1086
WordPress 讓我們加密證書 .....	1101
IPv6網路 .....	1116
IPv6為 cPanel 和 WHM .....	1116
IPv6對於 Debian 8 .....	1122
IPv6對於 GitLab .....	1125
IPv6對於尼金克斯 .....	1128
IPv6對於普萊斯克 .....	1131
IPv6適用於 Ubuntu .....	1134
AWS CLI 對於 Lightsail .....	1137
設定存取金鑰 .....	1138
啟動和設定 LAMP .....	1139
步驟 1：註冊 AWS .....	1140
步驟 2：建立 LAMP 執行個體 .....	1140
步驟 3：透過 SSH 連接至您的執行個體，並為您的 LAMP 執行個體取得應用程式密碼 .....	1144
步驟 4：在您的 LAMP 執行個體上安裝應用程式 .....	1145
步驟 5：建立 靜態 IP 地址並將它連接到您的 LAMP 執行個體 .....	1145
步驟 6：建立 DNS 區域並將域對應到 LAMP 執行個體 .....	1147
後續步驟 .....	1147
將 LAMP 執行個體連接至 Aurora 資料庫 .....	1148
啟動和設定 Windows Server 2016 .....	1153
步驟 1：註冊 AWS .....	1153
步驟 2：建立視窗伺服器 2016 年執行 Lightsail .....	1153
步驟 3：透過 RDP 連接至您的 Windows Server 2016 執行個體 .....	1157
步驟 4：建立 靜態 IP 地址並將它連接到您的 Windows Server 2016 執行個體 .....	1158
步驟 5：建立 DNS 區域並將域對應至您的 Windows Server 2016 執行個體 .....	1160
後續步驟 .....	1161
CloudTrail 記錄 .....	1161
Lightsail 資訊 CloudTrail .....	1162
瞭解 Lightsail 記錄檔項目 .....	1162
建立 HAR 檔案 .....	1163
第 1 步：在瀏覽器中建立 HAR 檔案 .....	1163
第 2 步：編輯 HAR 檔案以移除敏感資訊 .....	1165

第 3 步：提交 HAR 檔案以供檢視 .....	1165
安裝 Prometheus .....	1165
步驟 1：完成先決條件 .....	1166
步驟 2：將使用者和本機系統目錄新增至 Lightsail 執行個體 .....	1166
步驟 3：下載 Prometheus 二進位套件 .....	1167
步驟 4：設定 Prometheus .....	1170
步驟 5：啟動 Prometheus .....	1172
步驟 6：啟動 Node Exporter .....	1174
步驟 7：使用 Node Exporter 資料收集器設定 Prometheus .....	1176
使用 scp 傳輸檔案 .....	1178
必要條件 .....	1179
步驟 1：將私鑰 ( .pem ) 文件保存到本地計算機 .....	1179
步驟 2：變更私密金鑰的權限 .....	1180
步驟 3：將私密金鑰轉移到執行個體 .....	1181
步驟 4：安全地在 Lightsail Linux 和 Unix 執行個體之間傳輸檔案 .....	1182
與其他AWS服務合作 .....	1183
虛擬機器 (虛擬私有伺服器) .....	1183
無伺服器運算 .....	1184
資料庫 .....	1185
負載平衡器 .....	1185
大數據 .....	1186
儲存 .....	1187
監控和警示 .....	1187
應用程式部署 .....	1188
應用程式容器 .....	1188
安全性和使用者登入功能 .....	1188
來源控制和應用程式生命週期管理 .....	1189
佇列和簡訊 .....	1189
工作流程 .....	1190
串流應用程式 .....	1190
AWS CloudFormation 資源 .....	1191
Lightsail 和 AWS CloudFormation 模板 .....	1191
進一步了解 AWS CloudFormation .....	1191
關於 Lightsail 的其他資訊 .....	1192
部落格 .....	1192
教學課程 .....	1194

影片 .....	1196
帳單 .....	1199
檢視您的詳細帳單 .....	1199
帳單用量類型 .....	1200
帳單中的區域代碼 .....	1201
FAQs .....	1203
關於 Lightsail .....	1203
什麼是 Amazon Lightsail ? .....	1203
我可以使用 Lightsail 做什麼 ? .....	1204
Lightsail 是否提供 ? API .....	1204
我要如何註冊成為 Lightsail ? .....	1204
Lightsail AWS 區域 有哪些可用 ? .....	1204
什麼是可用區域 ? .....	1205
什麼是 Lightsail 服務配額 ? .....	1205
如何獲得更多協助 ? .....	1205
帳單和帳戶管理 .....	1205
Lightsail 計劃的費用是多少 ? .....	1205
何時需要支付計劃的費用 ? .....	1206
我可以免費試用 Lightsail 執行個體嗎 ? .....	1206
免費試用版何時開始 ? .....	1206
Lightsail 受管資料庫的成本為何 ? .....	1206
我可以免費試用 Lightsail 受管理的資料庫嗎 ? .....	1206
區塊儲存的 Lightsail 本是多少 ? .....	1207
Lightsail 負載平衡器的成本是多少 ? .....	1207
憑證管理費用是多少 ? .....	1207
什麼是 Lightsail 靜態IPv4地址的成本 ? .....	1207
資料傳輸的費用是多少 ? .....	1207
資料傳輸額度如何用於執行個體 ? .....	1207
資料傳輸額度如何與負載平衡器搭配使用 ? .....	1209
萬一超出資料傳輸計劃額度呢 ? .....	1209
我需要支付哪種資料傳輸類型的費用 ? .....	1209
我的執行個體資料傳輸額度有何不同 AWS 區域 ? .....	1210
Lightsail 網域的費用是多少 ? .....	1210
Lightsail DNS 管理的成本是多少 ? .....	1210
Lightsail 快照的費用是多少 ? .....	1211
如何管理我的 AWS 帳戶 ? .....	1211

什麼是 Lightsail 法律使用條款？ .....	1211
我該如何支付我的帳單？ .....	1211
區塊儲存 (磁碟) .....	1211
我可以使用 Lightsail 區塊儲存裝置做什麼？ .....	1211
連接的磁碟與 Lightsail 方案中包含的儲存空間有何不同？ .....	1212
連接磁碟可以有多大？ .....	1212
每個 Lightsail 執行個體可以連接多少個磁碟？ .....	1212
是否可將磁碟連接到多個執行個體？ .....	1212
磁碟是否一定要連接到執行個體？ .....	1212
是否可增加連接磁碟的大小？ .....	1212
Lightsail 區塊儲存是否提供加密功能？ .....	1212
我可以期待 Lightsail 區塊儲存裝置有哪些可用性？ .....	1213
如何備份連接磁碟？ .....	1213
憑證 .....	1213
如何使用 Lightsail 建的憑證？ .....	1213
如何驗證我的憑證？ .....	1213
如果無法驗證我的網域，會發生什麼情況？ .....	1213
可以在憑證增加多少個網域和子網域？ .....	1213
如何變更與憑證關聯的網域？ .....	1214
如何續約憑證？ .....	1214
刪除負載平衡器時，我的憑證會發生什麼狀況？ .....	1214
我可以下載我提供的憑證嗎？ .....	1214
聯繫人和監控通知 .....	1214
什麼是通知？ .....	1214
我可以新增多少個聯絡人？ .....	1214
容器服務 .....	1215
我可以使用 Lightsail 貨櫃服務做什麼？ .....	1215
Lightsail 容器服務是否可以執行碼頭集裝箱？ .....	1215
如何將我的公用容器映像檔與 Lightsail 容器服務搭配使用？ .....	1215
我是否可以從私有容器登錄檔中提取容器映像？ .....	1215
我是否可以根據需求變更服務的能力和規模？ .....	1215
我可以自訂 Lightsail 容器服務所建立之HTTPS端點的名稱嗎？ .....	1215
我可以將自訂網域用於 Lightsail 容器服務的HTTPS端點嗎？ .....	1215
Lightsail 集裝箱服務的費用是多少？ .....	1216
即使我的容器服務執行時間只有幾天，我是否仍需要支付整個月的費用？ .....	1216
我是否需要為進出容器服務的資料傳輸量付費？ .....	1216

停用和刪除容器服務有什麼區別？ .....	1217
如果我的容器服務處於停用狀態，系統是否會向我收取費用？ .....	1217
我可以將容器服務做為 Lightsail 內容傳遞網路 (CDN) 發佈的來源嗎？ .....	1217
我可以將容器服務做為 Lightsail 負載平衡器的目標嗎？ .....	1217
我可以將容器服務的公用端點設定為將HTTP要求重新導向至HTTPS嗎？ .....	1217
容器服務是否支援監控和提醒？ .....	1217
Lightsail 集裝箱服務是否支援IPv6？ .....	1218
內容交付網路分發 .....	1218
我可以將 Lightsail CDN 發行版做為什麼？ .....	1218
我可以將哪些類型的資源做為分發的原始伺服器？ .....	1218
我是否需要將靜態IPv4位址附加至 Lightsail 執行個體，才能將其用作 Lightsail 發行版本的來源？ .....	1218
如何在我的 WordPress 網站上設定 Lightsail 發行版本？ .....	1218
我是否可以連接多個原始伺服器？ .....	1218
Lightsail 發行版是否支援憑證建立？ .....	1218
是否需要憑證？ .....	1219
可建立的憑證數量是否有限？ .....	1219
如何配置我的分發以將HTTP請求重定向到HTTPS？ .....	1219
如何將我的頂點網域設定為指向我的 Lightsail 發行版本？ .....	1219
Lightsail 的執行個體資料傳輸配額和散發資料傳輸配額有何差異？ .....	1219
我是否可以變更與分發相關聯的計劃？ .....	1219
如何知道我的分發是否有效？ .....	1219
我可以刪除 Lightsail 發行版本上的快取內容嗎？ .....	1219
什麼時候應該使用 Lightsail 發行版與 Amazon 發行 CloudFront 版？ .....	1220
我可以將 Lightsail 內容交付網路 (CDN) 分發移到 Amazon CloudFront 嗎？ .....	1220
如何使用 LightsailCDN？ .....	1220
Lightsail CDN 發行版是否支援IPv6？ .....	1221
是否需要IPv6啟用來源才能與 Lightsail CDN 發行版一起使用？ .....	1221
資料庫 .....	1221
什麼是 Lightsail 資料庫？ .....	1221
我可以將 Lightsail 受管資料庫做為什麼？ .....	1221
Lightsail 為我管理什麼？ .....	1222
Lightsail 支援哪些類型的資料庫以及這些資料庫的哪些版本？ .....	1222
Lightsail 提供哪些受管理的資料庫計劃？ .....	1222
什麼是高可用性計劃？ .....	1222
如何擴展或縮小 Lightsail 受管資料庫？ .....	1222

如何備份受管理 Lightsail 料庫？ .....	1222
如果我刪除 Lightsail 受管理的資料庫，我的資料會發生什麼情況？ .....	1223
是否可以將執行個體連線到在不同 AWS 區域 或不同可用區域中執行的 Lightsail 受管資料庫？ .....	1223
如何將資料載入 Lightsail 受管理的資料庫？ .....	1223
如何存取 Lightsail 受管資料庫上的資料？ .....	1223
Lightsail 受管資料庫如何與我的 Lightsail 執行個體搭配使用？ .....	1223
如何將 Lightsail 受管資料庫連線到 AWS 帳戶中 EC2 執行的執行個體？ .....	1224
Lightsail 受管資料庫的公開和私有模式有何不同？ .....	1224
我可以管理 Lightsail 受管資料庫所使用的連接埠嗎？ .....	1224
是否 Lightsail 受管資料庫服務 IPv6？ .....	1224
網域 .....	1224
我可以使用 Lightsail 網域做什麼？ .....	1224
我可以使用哪些頂層網域 (TLDs)？ .....	1224
我可以讓 Lightsail 成為我現有網域的 DNS 服務嗎？ .....	1225
如何開始在 Lightsail 中註冊網域？ .....	1225
什麼時候應該在 Lightsail 和 Route 53 中註冊網域？ .....	1225
我可以將我的網域轉移到我 Lightsail 嗎？ .....	1225
我可以將哪些 Lightsail 資源和網域搭配使用？ .....	1225
將資源導出到 Amazon EC2 .....	1225
什麼是出口到 Amazon EC2？ .....	1225
我為什麼要出口到 Amazon EC2？ .....	1225
出口到 Amazon 如何 EC2 工作？ .....	1226
如何計費？ .....	1226
是否可匯出受管資料庫或磁碟快照？ .....	1226
我可以匯出哪些資源？ .....	1226
執行個體 .....	1227
什麼是執 Lightsail 體？ .....	1227
什麼是 Lightsail 計劃？ .....	1227
我可以在執行個體上執行什麼軟體？ .....	1227
我可以搭配哪些作業系統使 Lightsail？ .....	1227
我是否需要攜帶自己的授權才能使用 Lightsail 執行個體？ .....	1227
如何建立執 Lightsail 體？ .....	1227
執行個 Lightsail 如何執行？ .....	1228
如何知道我的執行個體高載？ .....	1228
如何連線至 Lightsail 執行個體？ .....	1228

如何備份執行個體？ .....	1228
是否可以升級我的計劃？ .....	1228
如何將 Lightsail 執行個體連線到我 AWS 帳戶中的其他資源？ .....	1229
停用執行個體和刪除執行個體有什麼區別？ .....	1229
<b>負載平衡器</b> .....	1229
我可以使用 Lightsail 負載平衡器做什麼？ .....	1229
是否可以在不同 AWS 區域 或不同可用區域中的執行個體使用負載平衡器？ .....	1230
我的 Lightsail 負載平衡器如何處理流量尖峰？ .....	1230
Lightsail 負載平衡器如何將流量路由到我的目標執行個體？ .....	1230
Lightsail 如何知道我的目標執行個體是否健康？ .....	1230
負載平衡器可連接多少個執行個體？ .....	1230
是否可將一個執行個體指派給多個負載平衡器？ .....	1230
刪除負載平衡器時，目標執行個體會發生什麼狀況？ .....	1230
什麼是工作階段持久性？ .....	1231
Lightsail 負載平衡器支援哪些類型的連線？ .....	1231
是否支 Lightsail 負載平衡器？IPv6 .....	1231
是否需要IPv6啟用負載平衡器後面的執行個體，才能使用已IPv6啟用的負載平衡器？ .....	1231
<b>快照</b> .....	1231
什麼是快照？ .....	1231
什麼是自動快照？ .....	1232
手動和自動快照有何不同？ .....	1232
哪些資源支援快照？ .....	1232
快照可以存放多長時間？ .....	1232
如何啟用自動快照？ .....	1232
何時建立自動快照？ .....	1233
可以存放多少個快照？ .....	1233
快照如何計費？ .....	1233
如果停用自動快照，是否會遺失快照？ .....	1233
如果不想取代自動快照，該怎麼辦？ .....	1233
是否可以刪除自動快照？ .....	1233
如何使用快照？ .....	1233
<b>指標與警示</b> .....	1234
什麼是指標？ .....	1234
什麼是警示？ .....	1234
我可以新增多少個警示？ .....	1234
<b>聯網</b> .....	1234

我要如何使用 IP Lightsail ? .....	1234
Lightsail 是否IPv6僅支援執行個體 ? .....	1234
什麼是靜態 IP ? .....	1235
我IPs可以將多少個靜態連接到一個實例 ? .....	1235
什麼是DNS記錄 ? .....	1235
是否可以管理執行個體的防火牆設定 ? .....	1235
物件儲存 (值區) .....	1235
我能用 Lightsail 物件儲存做什麼 ? .....	1235
Lightsail 物件儲存的費用是多少 ? .....	1236
Lightsail 物件儲存是否有超額費用 ? .....	1236
資料傳輸額度如何與物件儲存搭配使用 ? .....	1236
我是否可以變更與 Lightsail 儲存貯體相關的計劃 ? .....	1236
我是否可以將物件從 Lightsail 物件儲存複製到 Amazon S3 ? .....	1236
如何開始使用 Lightsail 物件儲存 ? .....	1236
如何將物件上傳到儲存貯體 ? .....	1237
我是否可以封鎖對儲存貯體的公有存取 ? .....	1237
如何提供對儲存貯體的程式設計存取 ? .....	1237
如何與其他 AWS 帳戶共用儲存貯體 ? .....	1237
什麼是版本控制 ? .....	1237
如何將我的 Lightsail 儲存貯體與我的發 Lightsail CDN 版本相關聯 ? .....	1237
Lightsail 物件儲存服務有什麼限制 ? .....	1238
Lightsail 物件儲存是否支援監控和提醒 ? .....	1238
Lightsail 中的標籤 .....	1238
什麼是標籤 ? .....	1238
如何在 Lightsail 中使用標籤 ? .....	1238
可以標記哪些資源 ? .....	1238
如何標記我的 Lightsail 照 ? .....	1239
鍵值標籤和僅索引鍵標籤有何不同 ? .....	1239
取得說明 .....	1240
即時線上說明面板 .....	1240
關於使用者指南 .....	1240
使用搜尋 .....	1241
使用 Lightsail CLI 和 API .....	1241
AWS 論壇和其他社群資源 .....	1241
.....	mccxliv

# 什麼是 Amazon Lightsail ？

對於需要建立網站或 Web 應用程式的任何人，亞馬 Amazon Lightsail 是開始使用 Amazon Web Services ( AWS ) 的最簡單方法。其中包含快速啟動專案所需的一切，例如執行個體 ( 虛擬專用伺服器 )、容器服務、受管資料庫、內容傳遞網路 (CDN) 發佈、負載平衡器、SSD 基於區塊儲存、靜態 IP 位址、註冊網域的 DNS 管理，以及資源快照 ( 備份 )，每月價格低廉。

Lightsail 還提供亞馬遜研究用的光帆。有了 Lightsail 研究用，學者和研究人員可以在 AWS 雲端這些虛擬計算機帶有預先安裝的研究應用程序，例如 RStudio 和 Scilab。如需詳細資訊，請參閱 [Amazon Lightsail 研究用戶指南](#)。

## 主題

- [Lightsail 的功能](#)
- [Lightsail 是為誰提供的？](#)
- [訪問 Lightsail](#)
- [開始使用 Lightsail](#)
- [相關服務](#)
- [估算、計費和成本最佳化](#)

## Lightsail 的功能

Lightsail 提供下列高階功能：

### 執行個體

Lightsail 提供虛擬專用伺服器 ( 執行個體 )，這些伺服器可輕鬆設定，並具備的功能和可靠性 AWS。您可以在幾分鐘內啟動網站、Web 應用程式或專案，並從直覺式 Lightsail 主控台或 API 管理執行個體。

當您建立執行個體時，您會有 click-to-launch 一個簡單的作業系統 (OS)、預先設定的應用程式或開發堆疊 — 例如 Windows WordPress、Plesk LAMP、Nginx 等等。每個 Lightsail 執行個體都隨附內建防火牆，可讓您根據來源 IP、連接埠和通訊協定允許或限制執行個體的流量。[進一步了解](#)

### 容器

在雲端中執行並安全存取容器化應用程式。容器是標準的軟體單位，可將程式碼及其依存項目封裝在一起，讓應用程式在各個運算環境間快速可靠地執行。[進一步了解](#)

## 負載平衡器

跨執行個體路由網路流量，讓您的網站和應用程式能夠適應流量的變化、防止中斷，並提供順暢的訪客體驗。[進一步了解](#)

## 受管資料庫

Lightsail 提供完整設定的 My SQL 或 Postgre SQL 資料庫計劃，其中包括記憶體、處理、儲存和傳輸容量。透過 Lightsail 受管理的資料庫，您可以輕鬆擴充資料庫，獨立於虛擬伺服器、改善應用程式可用性，或在雲端中執行獨立資料庫。[進一步了解](#)

## 區塊與物件儲存

Lightsail 同時提供區塊和物件儲存空間。您可以透過適用於 Linux 或 Windows 虛擬伺服器的高可用性 SSD 支援儲存裝置，快速輕鬆地擴充儲存。[進一步了解](#)

有了 Lightsail 物件儲存貯體，您可以隨時隨地在網際網路上的任何地方儲存和擷取物件。您也可以上雲端託管靜態內容。[進一步了解](#)

## CDN 分佈

Lightsail 啟用內容交付網路 (CDN) 分發，這些分發是建立在與 Amazon CloudFront 相同的基礎設施上。您可以通過在世界各地設置代理伺服器輕鬆地將內容分發給全球受眾，以便您的用戶可以更接近地理位置訪問您的網站，從而減少延遲。[進一步了解](#)

## 存取 AWS 服務

Lightsail 使用一組重點功能，例如執行個體、受管資料庫和負載平衡器，讓您更輕鬆地開始使用。但這並不意味著您只能使用這些選項-您可以通過 Amazon 對等互連將 Lightsail 項目與 90 多種其他服務中的一些服務集 AWS 成在一起。[VPC 進一步了解](#)

有關 Lightsail 的更多詳細信息，請參閱 [Amazon Light sail](#)。

## Lightsail 是為誰提供的？

Lightsail 適合所有人。您可以為 Lightsail 執行個體選擇映像檔，以便快速啟動專案，因此您不必花費太多時間安裝軟體或架構。

如果您是個別開發人員或業餘愛好者，Lightsail 可協助您部署和管理基本雲端資源。此外，您可能想要了解或體驗虛擬機器、域或聯網等雲端服務。Lightsail 提供了一種快速開始使用的方法。

Lightsail 具有基本操作系統的圖像，開發堆棧一樣 LAMP, LEMP (Nginx 的)，和 SQL 服務器快遞，和應用程序，如，Drupal 的 WordPress, 和 Magento 的。如需有關每個映像檔上安裝之軟體的詳細資訊，請參閱 [選擇 Lightsail 實體映像檔](#)。

隨著專案的成長，您可以新增區塊儲存磁碟，並將它們附加到 Lightsail 執行個體。您可以擷取上述執行個體和磁碟的快照，進而透過這些快照輕鬆地建立新的執行個體。您也可以對等，以 VPC 便 Lightsail 執行個體可以使用 Lightsail 以外的其他 AWS 資源。

您也可以建立 Lightsail 負載平衡器並連接目標執行個體，以建立高可用性應用程式。您也可以設定負載平衡器來處理加密的 (HTTPS) 流量、工作階段持續性、健康狀況檢查等。

## 訪問 Lightsail

您可以使用下列介面建立及管理 Lightsail 資源：

### Amazon Lightsail 制台

一個簡單的網頁介面，可用來建立和管理 Lightsail 執行個體和資源。如果您已註冊 AWS 帳戶，則可以登入 AWS Management Console 並從主控台首頁選取 Lightsail，以存取 Lightsail 主控台。

### AWS Command Line Interface

可讓您使用命令列殼層中的命令與 AWS 服務互動。Windows、Mac 和 Linux 系統皆提供支援。如需有關 AWS CLI 的詳細資訊，請參閱 [《AWS Command Line Interface 使用者指南》](#)。您可以在 [亞馬遜光帆參考中找到 Lightsail API 命令](#)。

### AWS Tools for PowerShell

— PowerShell 組以公開的功能為基礎建置的模組 AWS SDK for .NET。「工具」可 PowerShell 讓您從命令列對資 AWS 源執行作業的 PowerShell 指令碼。若要開始使用，請參閱 [《使用者指南 AWS Tools for Windows PowerShell》](#)。您可以在指令程式參考資料中找到 Lightsail 的 [AWS Tools for PowerShell 指令程式](#)。

### 查詢 API

Lightsail 提供了一個查詢 API。這些請求是 HTTP 或使用 HTTP 動詞 GET 或名為 POST 的 Query 參數的 HTTPS 請求 Action。如需有關 Lightsail API 動作的詳細資訊，請參閱 Amazon Lightsail 參考資料中的 [動作](#)。API

### AWS SDKs

如果您偏好使用特定語言來建置應用程式，APIs 而不是透過 HTTP 或提交要求 HTTPS，請為軟體開發人員 AWS 提供程式庫、範例程式碼、教學課程和其他資源。這些程式庫提供的基本功能可自動

化任務，例如密碼編譯簽署要求、重試要求，以及處理錯誤回應，讓您更容易入門。如需詳細資訊，請參閱[建置在其上的工具 AWS](#)。

## 開始使用 Lightsail

設定使用 Lightsail 之後，您可[開始使用虛擬私人伺服器 Lightsail](#)以逐步啟動、連線和清理執行個體。

## 相關服務

您可以直接使用 Lightsail 佈建 Lightsail 資源，例如執行個體和磁碟。此外，您還可以使用其他 AWS 服務佈建資源，例如：

- [Amazon EC2](#)

提供可調整大小的運算容量 (實際上是 Amazon 資料中心中的伺服器)，可用來建置和託管軟體系統。要比較 Lightsail 和 AmazonEC2，請參閱 [Amazon Lightsail 或 Amazon EC2](#)。

- [Amazon EC2 Auto Scaling](#)

協助確保您擁有正確數量的 Amazon EC2 執行個體可用來處理應用程式的負載。

- [Elastic Load Balancing](#)

自動將傳入應用程式流量分配至多個執行個體。

- [Amazon Relational Database Service \( AmazonRDS \)](#)

在雲端環境中設定、操作和擴展受管關聯式資料庫。

- [Amazon 彈性容器服務 \( AmazonECS \)](#)

在 Amazon EC2 執行個體叢集上部署、管理和擴展容器化應用程式。

## 估算、計費和成本最佳化

若要為您的 AWS 使用案例建立估算值，請使用 [AWS Pricing Calculator](#)。

若要查看您的帳單，請前往 [AWS Billing and Cost Management 主控台](#) 中的帳單與成本管理儀表板。您的帳單內含用量報告的連結，可提供帳單的詳細資訊。若要深入瞭解 AWS 帳戶帳單，請參閱 [AWS Billing and Cost Management 使用者指南](#)。

如果您對帳 AWS 單、帳戶和事件有任何疑問，請聯絡 [Sup AWS port](#) 部門。

您可以使用最佳化 AWS 環境的成本、安全性和效能 [AWS Trusted Advisor](#)。

# 設定 AWS 帳戶 和管理使 Lightsail

如果您是新 AWS 客戶，請在開始使用 Amazon Lightsail 之前完成此頁面上列出的設定先決條件。對於這些安裝程序，您可以使用 AWS Identity and Access Management (IAM) 服務。如需有關的完整資訊 IAM，請參閱 [《IAM使用者指南》](#)。

## 註冊一個 AWS 帳戶

如果您沒有 AWS 帳戶，請完成以下步驟來建立一個。

若要註冊成為 AWS 帳戶

1. 打開<https://portal.aws.amazon.com/billing/註冊>。
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，會建立AWS 帳戶根使用者一個。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 註冊過程完成後，會向您發送確認電子郵件。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，請保護 AWS 帳戶 AWS 帳戶根使用者、啟用和建立系統管理使用者 AWS IAM Identity Center，這樣您就不會將 root 使用者用於日常工作。

保護您的 AWS 帳戶根使用者

1. 選擇 Root 使用者並輸入您的 AWS 帳戶 電子郵件地址，以帳戶擁有者身分登入。[AWS Management Console](#)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. 為您的 root 使用者開啟多因素驗證 (MFA)。

如需指示，請參閱《[使用指南](#)》中的「IAM為 AWS 帳戶 root 使用者啟用虛擬MFA裝置 (主控台)」。

## 建立具有管理存取權的使用者

1. 啟用IAM身分識別中心。

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身分識別中心中，將管理存取權授與使用者。

[若要取得有關使用 IAM Identity Center 目錄 做為身分識別來源的自學課程，請參閱《使用指南》IAM Identity Center 目錄中的「以預設值設定使用AWS IAM Identity Center 者存取」。](#)

## 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 使用者登入URL，請使用建立IAM身分識別中心使用者時傳送至您電子郵件地址的登入資訊。

如需使用IAM身分識別中心使用者[登入的說明](#)，請參閱使用指南中的[登入 AWS 存取入口網站](#)。AWS 登入

## 指派存取權給其他使用者

1. 在 IAM Identity Center 中，建立遵循套用最低權限權限的最佳作法的權限集。

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](#)。

# 開始使用虛擬私人伺服器 Lightsail

在 Lightsail 中，執行個體是虛擬私人伺服器 (也稱為虛擬機器)。您可以在中建立和管理 Lightsail 實體。AWS 雲端建立執行個體時，選擇具有作業系統 (OS) 的映像。您也可以選擇擁有應用程式或開發堆疊 (包括基礎作業系統) 的執行個體映像。

您在本教學課程中建立的執行個體將從建立之時起產生使用費用，直到您刪除執行個體為止。刪除是本教學課程的最後一個步驟。如需有關定價的詳細資訊，請參閱 [Lightsail 定價](#)。

## 主題

- [步驟 1：完成先決條件](#)
- [步驟 2：建立執行個體](#)
- [步驟 3：連接到您的執行個體](#)
- [步驟 4：將儲存體新增至執行個體](#)
- [步驟 5：建立快照](#)
- [步驟 6：清除](#)
- [後續步驟](#)

## 步驟 1：完成先決條件

如果您是新 AWS 客戶，請先完成設定先決條件，然後再開始使用 Amazon Lightsail。如需詳細資訊，請參閱 [設定 AWS 帳戶和管理使用 Lightsail](#)。

## 步驟 2：建立執行個體

您可以使用 [Lightsail 主控台](#) 建立執行個體，如下列程序所述。本教學課程旨在協助快速啟動您的第一個執行個體。我們也建議探索可用的應用程式和硬體計畫。如需詳細資訊，請參閱 [檢閱 Lightsail 執行個體藍圖供應項目](#)。

1. 登入主 [Lightsail 台](#)。
2. 在首頁上選擇 Create instance (建立執行個體)。
3. 選取執行個體的位置 (AWS 區域 和可用區域)。選擇最接近您實體位置的位置 AWS 區域，以減少延遲。

選擇 [變更 AWS 區域 和可用區域]，在其他位置建立執行個體。

4. 可選擇應用程式 (應用程式與作業系統) 或作業系統 (僅作業系統)。

若要深入了解 Lightsail 實體影像，請參閱[檢閱 Lightsail 執行個體藍圖供應項目](#)。

5. 選擇您的執行個體方案。

選擇您的執行個體使用雙堆疊 (IPv4和IPv6)，還是IPv6僅使用網路。有些 Lightsail 藍圖目前不支援IPv6只有網路功能。若要查看哪些藍圖IPv6僅支援網路，請參閱[檢閱 Lightsail 執行個體藍圖供應項目](#)。

您可以免費試用 5 美元的 USD Lightsail 計劃一個月 (最多 750 小時)。我們將在您的帳戶扣除一個月免費試用的費用。請前往我們的[定價頁面](#)進一步了解。

6. 輸入您執行個體的名稱。

資源名稱：

- 每個 Lightsail 帳戶 AWS 區域 中的每個項目都必須是唯一的。
- 必須包含 2 至 255 個字元。
- 開頭和結尾必須是英數字元或數字。
- 可以包含英數字元、數字、句點、破折號和底線。

7. 選擇 建立執行個體。

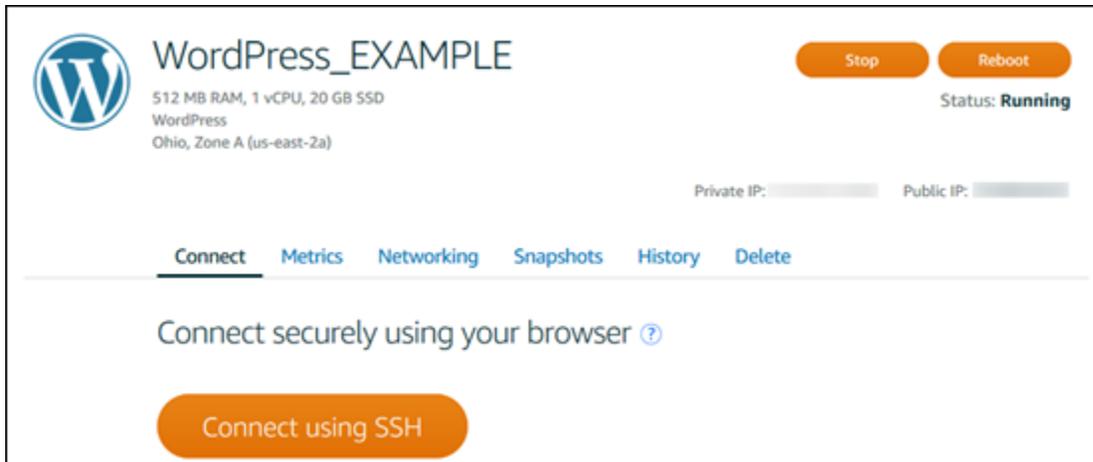
只需幾分鐘，您的 Lightsail 執行個體就緒，您就可以連線到該執行個體。

## 步驟 3：連接到您的執行個體

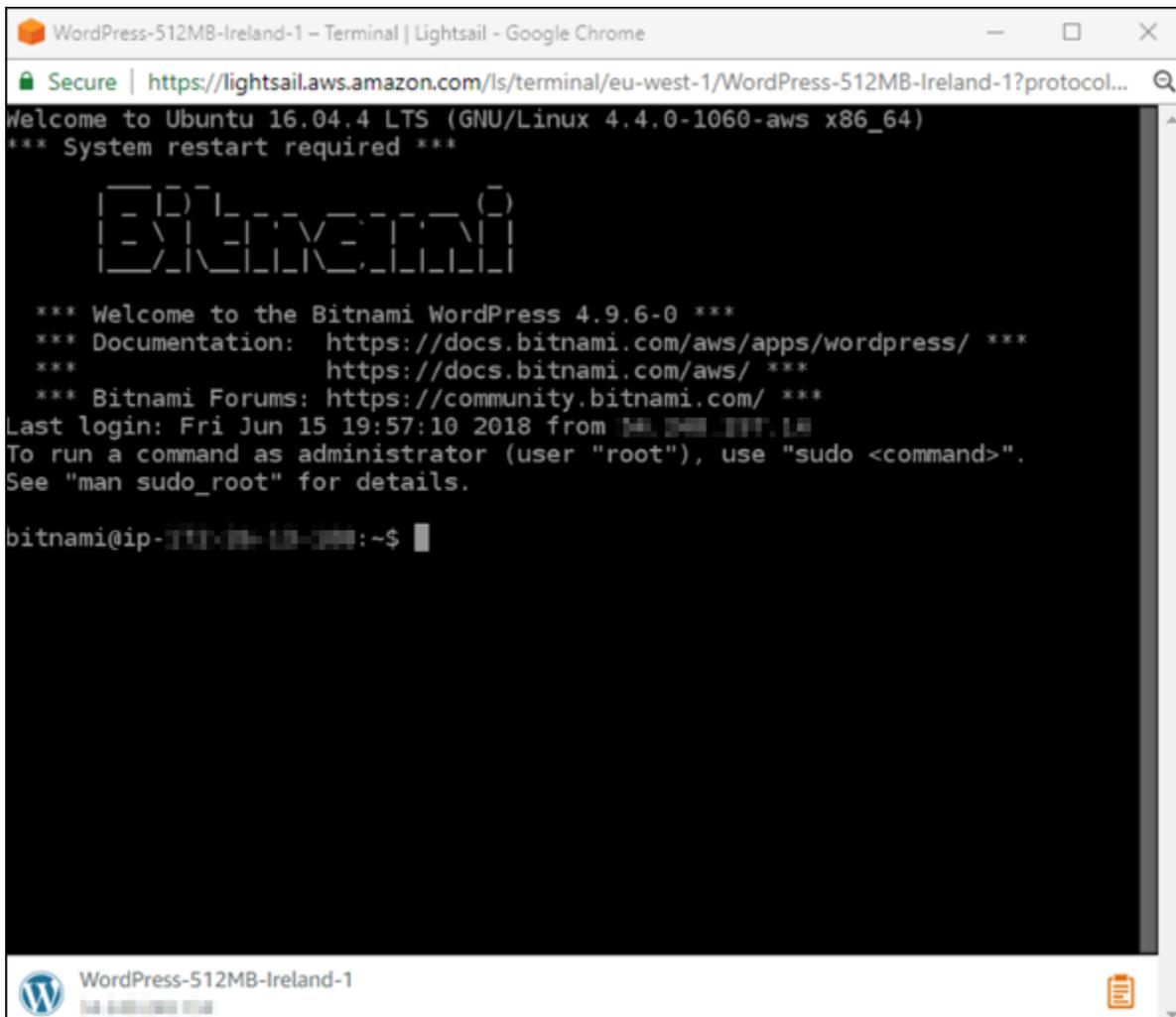
1. 在 Lightsail 首頁中，選擇執行個體名稱右側的選單，然後選擇「Connect」。



或者，您可以開啟執行個體管理頁面，然後選擇 Connect (連線) 索引標籤。



2. 您現在可以在終端機中輸入命令，並管理 Lightsail 實體，而無需設定用SSH戶端。



若要瞭解如何連線以新增額外的儲存空間至虛擬電腦，請繼續學習本教學課程的下一個步驟。

## 步驟 4：將儲存體新增至執行個體

Lightsail 提供可連接至執行個體的區塊層級儲存磁碟區 (磁碟)。即使您的執行個體隨附有系統磁碟，也可以在需求變化時附接額外的儲存磁碟。也可以將磁碟從某個執行個體分離，然後附接至另一個執行個體。

建立額外的磁碟之後，您必須連線至 Lightsail 執行個體，才能格式化和掛接磁碟。

如需有關建立、附接和管理磁碟的相關資訊，請參閱 [建立區塊儲存磁碟並將其連接至 Linux 執行個體](#)。

若要了解如何備份虛擬電腦，請繼續本教學課程的下一個步驟。

## 步驟 5：建立快照

快照是資料的 point-in-time 副本。可建立執行個體的快照，並將它們用作建立新執行個體或資料備份的基準。快照包含還原執行個體所需的所有資料 (從建立快照的那一刻開始)。

如需有關建立和管理快照的詳細資訊，請參閱 [使用快照備份 Linux/UniLightsail 執行個體](#)。

若要了解如何清除虛擬電腦資源，請繼續本教學課程的下一個步驟。

## 步驟 6：清除

如果不再使用為此教學課程建立的執行個體，可將其刪除。如果不再需要執行個體，這可停止執行個體產生費用。

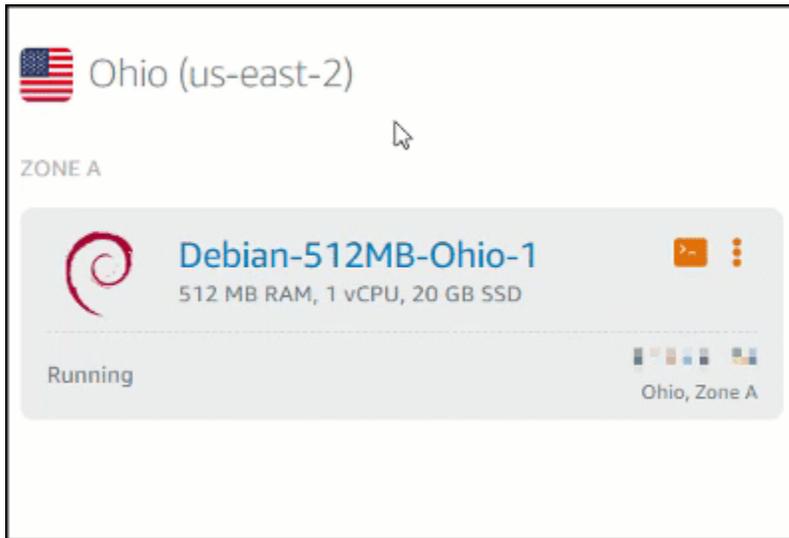
刪除執行個體並不會刪除其關聯的快照或附接的磁碟。如果您為本教學課程建立了快照和磁碟，也應該將其刪除。

若要儲存執行個體以待後用，但希望避免產生費用，可停止執行個體，而非將其刪除。然後，可以稍後再次將其啟動。如需有關定價的詳細資訊，請參閱 [Lightsail 定價](#)。

### Important

刪除 Lightsail 資源是一項永久性的動作。刪除的資料無法復原。如果稍後可能需要資料，請在刪除之前建立虛擬電腦的快照。如需詳細資訊，請參閱 [使用快照備份 Linux/UniLightsail 執行個體](#)。

1. 登入主 [Lightsail](#) 台。
2. 在導覽窗格中，選擇 Instances (執行個體)。
3. 針對您要刪除的執行個體，選擇操作功能表圖示 (:)，然後選擇 Delete (刪除)。



4. 選擇 Yes, Delete (是，刪除) 以確認刪除。

## 後續步驟

您可以使用下列主題開始使用 Amazon Lightsail Linux 和視窗型執行個體。

- [在 Lightsail 上使用應用程式建立 Linux/Unix 執行個體](#)
- [建立視窗伺服器執 Lightsail 個體](#)

## 虛擬私人伺服器執 Lightsail 個體

您的 Lightsail 執行個體是虛擬私人伺服器 (也稱為虛擬機器)。在您建立執行個體時，您將選擇具有作業系統 (OS) 的映像。您也可以選擇擁有應用程式或開發堆疊 (包括基礎作業系統) 的執行個體映像。

如需作業系統、應用程式和開發架構的完整清單，請參閱[選擇 Lightsail 執行個體映像檔](#)。

如需執行個體的詳細資訊，請參閱下列主題：

### 主題

- [建 Lightsail 體](#)
- [檢閱 Lightsail 執行個體藍圖供應項目](#)
- [使用 Lightsail 中的防火牆控制執行個體流](#)
- [偵測 Lightsail 執行個體爆發，以獲得最佳效能](#)
- [Connect 並管理您的執行個體](#)
- [刪 Lightsail 體](#)
- [管理SSH金鑰配對並連線至您的 Lightsail 執行個體](#)
- [在 Lightsail 中存取執行個體中繼資料服務 \(IMDS\) 和使用者資料](#)

## 建 Lightsail 體

本節涵蓋下列與在 Amazon Lightsail 中建立執行個體相關的主題：

### 主題

- [在 Lightsail 上使用應用程式建立 Linux/Unix 執行個體](#)
- [建立視窗伺服器執 Lightsail 個體](#)

## 在 Lightsail 上使用應用程式建立 Linux/Unix 執行個體

建立以 Linux/UNIX 為基礎的 Amazon Lightsail 執行個體 (虛擬私有伺服器)，執行類似應用程式或類似 WordPress 的開發堆疊。LAMP執行個體開始執行之後，您可以透過連線至該執行個體，SSH而不必離開 Lightsail。方法如下。

若要建立以視窗為基礎的執行個體，請參閱[在 Amazon Lightsail 中開始使用視窗型執行個體](#)。

## 建立以 Linux 為基礎的執行個體

1. 在首頁上選擇 Create instance (建立執行個體)。
2. 選取執行個體的位置 ( AWS 區域 和可用區域)。

選擇 [變更 AWS 區域 和可用區域]，在其他位置建立執行個體。

3. 或者，您可以變更可用區域。

選擇變更您的可用區域。

4. 選擇 Linux 平台。
5. 選擇應用程式 (Apps + OS (應用程式與作業系統)) 或作業系統 (OS Only (僅作業系統))。

若要進一步了解 Lightsail 執行個體映像檔，請參閱[選擇 Amazon Lightsail 執行個體映像檔](#)。

6. 選擇您的執行個體方案。

選擇您的執行個體使用雙堆疊 (IPv4和IPv6)，還是IPv6僅使用網路。有些 Lightsail 藍圖目前不支援IPv6只有網路功能。若要查看哪些藍圖IPv6僅支援網路，請參閱[檢閱 Lightsail 執行個體藍圖供應項目](#)。

您可以免費試用 5 美元的 USD Lightsail 計劃一個月 (最多 750 小時)。我們將在您的帳戶扣除一個月免費試用的費用。請前往我們的[定價頁面](#)進一步了解。

### Note

作為 AWS 免費方案的一部分，您可以在特定執行個體套裝軟體上免費開始使用 Amazon Lightsail。如需詳細資訊，請參閱 [Amazon Lightsail 定價頁面](#) 上的 AWS 免費方案。

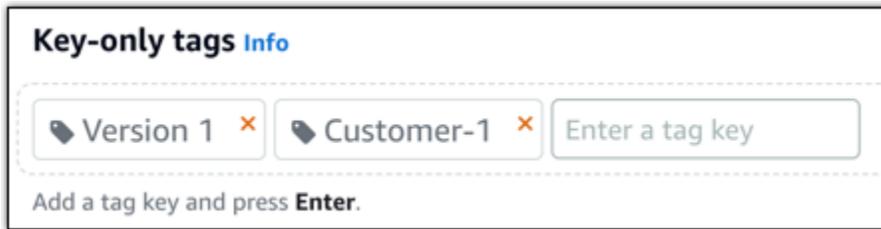
7. 輸入您執行個體的名稱。

資源名稱：

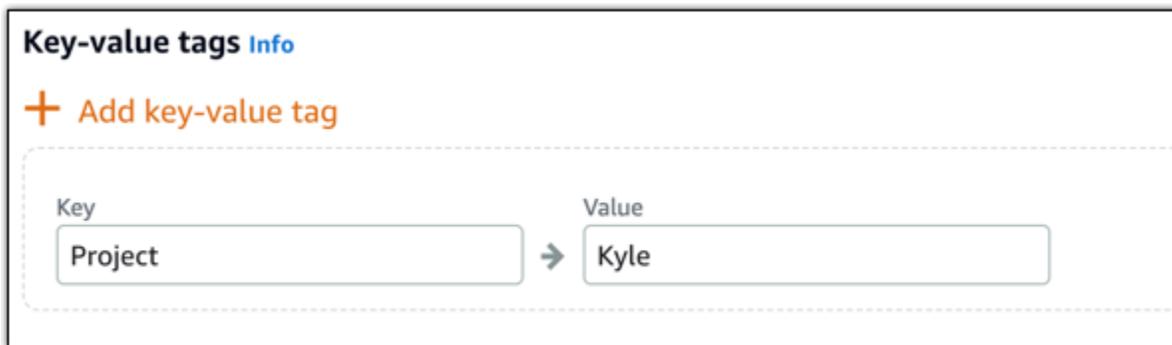
- 每個 Lightsail 帳戶 AWS 區域 中的每個項目都必須是唯一的。
- 必須包含 2 至 255 個字元。
- 開頭和結尾必須是英數字元或數字。
- 可以包含英數字元、數字、句點、破折號和底線。

8. 選擇下列其中一個選項以新增標籤至您的執行個體：

- 新增僅索引鍵標籤。在標籤索引鍵文字方塊中輸入新的標籤，接著按 Enter (輸入)。選擇X移除任何您不想保留的標籤。



- Create a key-value tag (建立索引鍵值標籤)，接著將索引鍵輸入 Key (索引鍵) 文字方塊，將值輸入 Value (值) 文字方塊。索引鍵值標籤一次只能新增一個。選擇新增索引鍵值標籤以新增其他索引鍵值標籤，或選擇X移除任何您不想保留的標籤。



#### Note

如需有關僅索引鍵和索引鍵值標籤的詳細資訊，請參閱[標籤](#)。

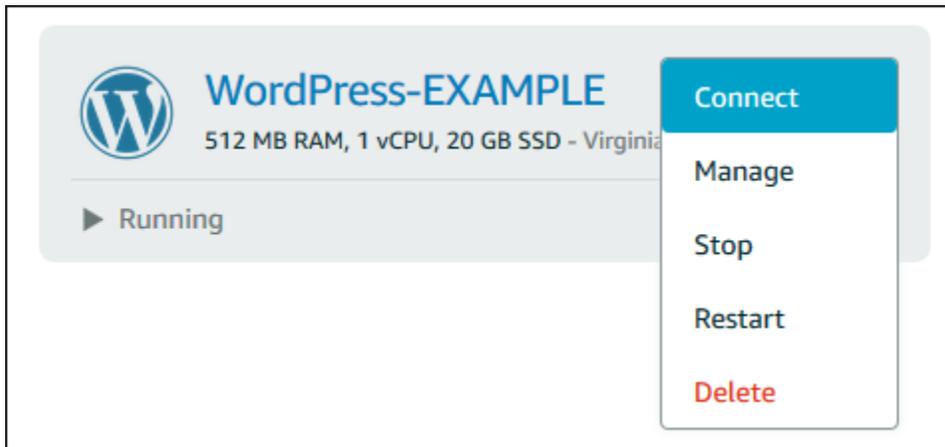
## 9. 選擇 建立執行個體。

如需進階建立選項，請參閱在[啟動 Amazon Lightsail 執行個體時使用啟動指令碼設定執行個體](#)，或為以 [Linux SSH 為基礎的 Lightsail 執行個體進行設定](#)。

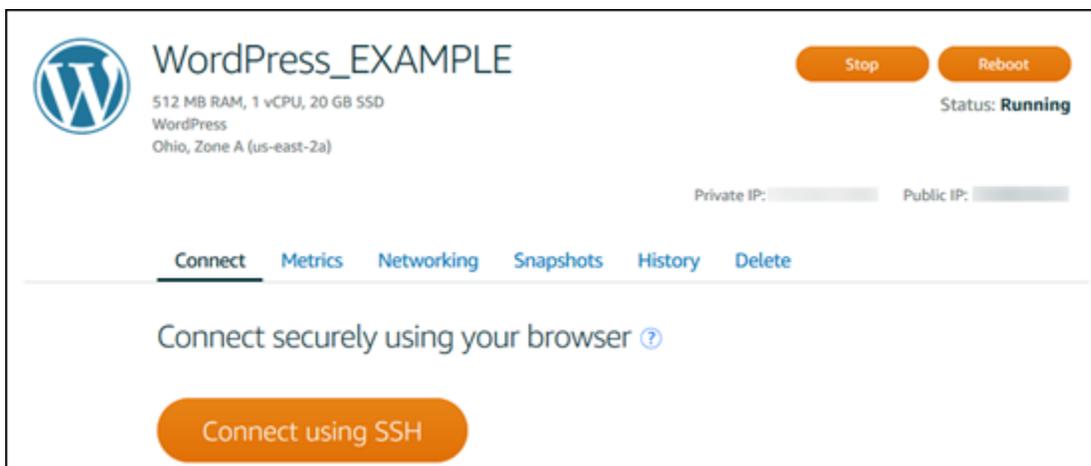
幾分鐘之內，您的 Lightsail 執行個體就已準備就緒，您可以透過連線至該執行個體SSH，而無需離開 Lightsail !

## 連接至您的執行個體

1. 在 Lightsail 首頁上，選擇執行個體名稱右側的選單，然後選擇「Connect」。



或者，您可以開啟執行個體管理頁面，然後選擇 Connect (連線) 索引標籤。



### Note

若要使用SSH戶端 (例如 Pu) 連線至執行個體TTY，您可以遵循下列程序：[設定 Pu 以連線TTY至 Lightsail 執行個體](#)。

- 現在，您可以在終端機中輸入命令並管理 Lightsail 實體，而無需設定用SSH戶端。



本主題提供有關選擇軟體、建立並連接至以 Windows Server 為基礎之執行個體的資訊。

進一步了解[視窗伺服器 AWS](#)

## 選擇以 Windows Server 為基礎的執行個體

有三個選項可在 Lightsail 中建立以 Windows 伺服器為基礎的執行個體。

### Windows Server 2022

運行 Windows 服務器的 Lightsail 是一個快速可靠的環境，用於使用 Microsoft 網絡平台部署應用程序。有了 Lightsail，您就可以在高效能、可靠且具成本效益的運 AWS 雲端 算平台上執行任何相容的 Windows 解決方案。常見的 Windows 使用案例包括企業基於 Windows 的應用程序託管，網站和 Web 服務託管，數據處理，分佈式測試，ASP.NET 應用程式主機，以及任何其他需要 Windows 軟體的應用程式

進一步了解[Windows Server 2022 映像](#)

### Windows Server 2019

除非您出於某種原因需要運行視窗服務器 2016 或視窗服務器 2019，否則我們建議您使用最新版本的視窗服務器 2022。

運行 Windows 服務器的 Lightsail 是一個快速可靠的環境，用於使用 Microsoft 網絡平台部署應用程序。Lightsail 可讓您在 AWS 「高效能、可靠、具成本效益的雲端運算平台上執行任何相容的 Windows 解決方案。常見的 Windows 使用案例包括企業基於 Windows 的應用程序託管，網站和 Web 服務託管，數據處理，分佈式測試，。ASP.NET 應用程式主機，以及任何其他需要 Windows 軟體的應用程式

進一步了解[Windows Server 2019 映像](#)

### Windows Server 2016

除非您出於某種原因需要運行視窗服務器 2016 或視窗服務器 2019，否則我們建議您使用最新版本的視窗服務器 2022。

運行 Windows 服務器的 Lightsail 是一個快速可靠的環境，用於使用 Microsoft 網絡平台部署應用程序。Lightsail 可讓您在 AWS 「高效能、可靠、具成本效益的雲端運算平台上執行任何相容的 Windows 解決方案。常見的 Windows 使用案例包括企業基於 Windows 的應用程序託管，網站和 Web 服務託管，數據處理，分佈式測試，。ASP.NET 應用程式主機，以及任何其他需要 Windows 軟體的應用程式

## [進一步了解 Windows Server 2016 映像](#)

### SQL 伺服器快速

SQL 伺服器 Express 是一個關係數據庫管理系統，可以免費下載，分發和使用。它包含專門用於內嵌和較小規模應用程式的資料庫。這個 Lightsail 映像運行在視窗伺服器 2022 的基本操作系統上。

## [深入瞭解 2022 年 SQL 伺服器快速映像](#)

### SQL 伺服器快速

SQL 伺服器 Express 是一個關係數據庫管理系統，可以免費下載，分發和使用。它包含專門用於內嵌和較小規模應用程式的資料庫。這個 Lightsail 映像運行在視窗伺服器 2022 的基本操作系統上。

## [進一步了解 SQL 伺服器快速 2019 映像](#)

### SQL 伺服器快速

SQL 伺服器 Express 是一個關係數據庫管理系統，可以免費下載，分發和使用。它包含專門用於內嵌和較小規模應用程式的資料庫。這個 Lightsail 映像運行在視窗伺服器 2016 的基本操作系統上。

## [深入瞭解 SQL 伺服器快速映像檔](#)

## 建立以 Windows Server 為基礎的執行個體

您可以使用 Lightsail 主控台或使用 AWS Command Line Interface (AWS CLI) 來建立以 Windows 伺服器為基礎的執行個體。

### 使用主控台建立執行個體

1. 登入 Lightsail，然後移至首頁。
2. 選擇 建立執行個體。
3. 選取您要建立以 Windows 伺服器為基礎之 Lightsail 實體的 AWS 區域 位置。

例如：Ohio (us-east-2)。

4. 選擇 Microsoft Windows 平台。
5. 若要選擇 Windows Server 2022、Windows Server 2019、Windows Server 2016 藍圖，請選擇僅作業系統。

若要選擇 SQL 伺服器快速藍圖，請選擇應用程式 + 作業系統。

6. 選擇您的執行個體方案。

選擇執行個體使用雙堆疊 (IPv4和IPv6)，還是IPv6僅使用網路。有些 Lightsail 藍圖目前不支援 IPv6 只有網路功能。若要查看哪些藍圖 IPv6 僅支援網路，請參閱[檢閱 Lightsail 執行個體藍圖供應項目](#)。

計劃還包括低廉且可預測的成本和機器配置 ( RAMSSD , , vCPU ) 以及數據傳輸。

**Note**

有些執行個體方案不適用於某些藍圖。例如，您無法搭配 SQL 伺服器快速藍圖使用這兩個最小的計劃。您至少必須使用 2 GB RAM 和 50 GB 的計劃 SSD，或者選擇較大的計劃之一。

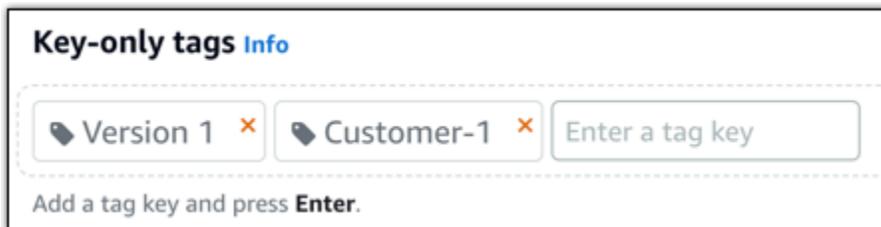
7. 輸入您執行個體的名稱。

資源名稱：

- 每個 Lightsail 帳戶 AWS 區域 中的每個項目都必須是唯一的。
- 必須包含 2 至 255 個字元。
- 開頭和結尾必須是英數字元或數字。
- 可以包含英數字元、數字、句點、破折號和底線。

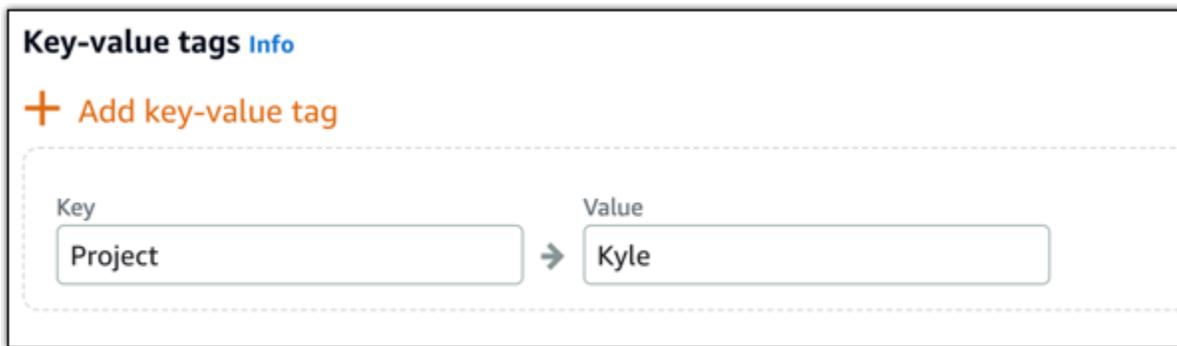
8. 選擇下列其中一個選項以新增標籤至您的執行個體：

- Add key-only tags (新增僅索引鍵標籤) 或 Edit key-only tags (編輯僅索引鍵標籤) (若標籤已新增)。在標籤索引鍵文字方塊中輸入新的標籤，接著按 Enter (輸入)。輸入標籤以新增之後，請選擇 Save (儲存)，如果不要新增則選擇 Cancel (取消)。



- Create a key-value tag (建立索引鍵值標籤)，接著將索引鍵輸入 Key (索引鍵) 文字方塊，將值輸入 Value (值) 文字方塊。完成輸入標籤後，請選擇 Save (儲存)，如果不要新增則選擇 Cancel (取消)。

鍵值標籤在儲存前一次只能新增一個。若要新增超過一個索引鍵值標籤，請重複之前的步驟。

**Note**

如需有關僅索引鍵和索引鍵值標籤的詳細資訊，請參閱[標籤](#)。

**9. 選擇 建立執行個體。**

若要使用建立執行個體 AWS CLI

1. 如果您尚未安裝和設定 AWS CLI，請先執行這項動作。

如需詳細資訊，請參閱[設定 AWS Command Line Interface 以與 Amazon Lightsail 搭配使用](#)。

2. 開啟命令提示或終端機視窗。
3. 如果您尚未這樣做，請設定 AWS CLI 使用 `aws configure` 並選取您 AWS 區域 要建立 Lightsail 資源的位置。
4. 輸入下列 AWS CLI 命令，以建立在俄亥俄州地區執行的 USD 每月 44 美元 Windows 伺服器 2022 執行個體：

```
aws lightsail create-instances --instance-names InstanceName --availability-zone us-east-2a --blueprint-id windows_server_2022 --bundle-id medium_win_3_0
```

在命令中，替換 *InstanceName* 使用新實例的名稱。

如果成功，您將會在 AWS CLI 看到以下輸出。

```
{
  "operations": [
    {
      "status": "Started",
```

```
    "resourceType": "Instance",
    "isTerminal": false,
    "statusChangedAt": 1508086226.4,
    "location": {
      "availabilityZone": "us-east-2a",
      "regionName": "us-east-2"
    },
    "operationType": "CreateInstance",
    "resourceName": "my-windows-instance",
    "id": "344acdc8-f9c4-4eda-8232-12345EXAMPLE",
    "createdAt": 1508086225.467
  }
]
}
```

### Note

若要取得可用藍圖清單，請使用 [get-blueprints](#) 命令。若要取得可用搭售套件清單，請使用 [get-bundles](#) 命令。進一步瞭解如何使用 [get-instance-access-details](#) 指令取得執行個體的密碼。

## 連接至您的執行個體

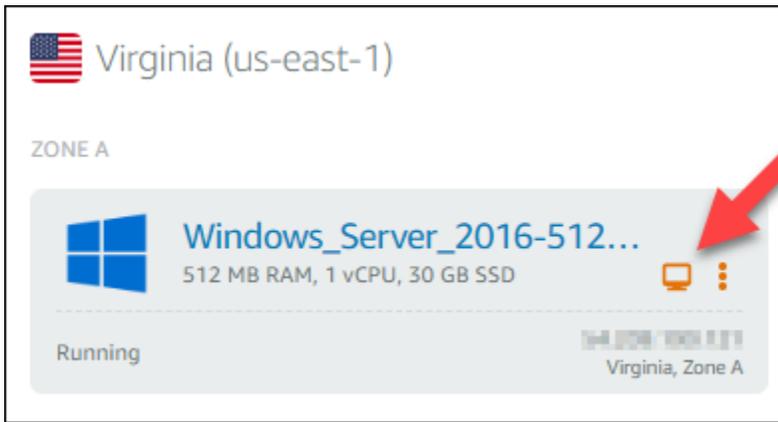
建立 Windows 伺服器型 Lightsail 執行個體之後，您可以使用瀏覽器型用 RDP 戶端或您選擇的遠端桌面用戶端來連線至該執行個體。

### Note

在您建立執行個體之後，您最多可能需要等待 15 分鐘，才能夠連接至執行個體。

若要使用 Lightsail 瀏覽器 RDP 型用戶端進行連線

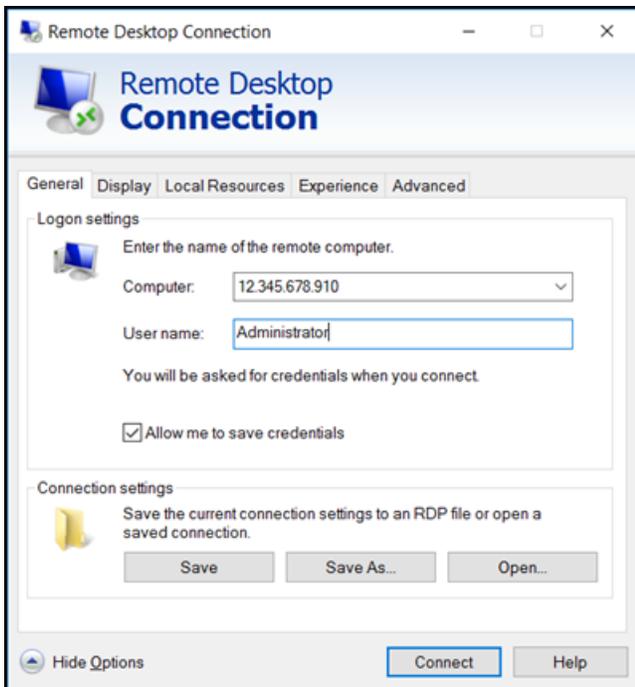
1. 在首頁上，選擇執行個體旁邊的 [Connect 方式] RDP 圖示。



2. 或者，您可以從捷徑選單或執行個體管理頁面連接至您的執行個體。

### 使用您自己的用RDP戶端連線

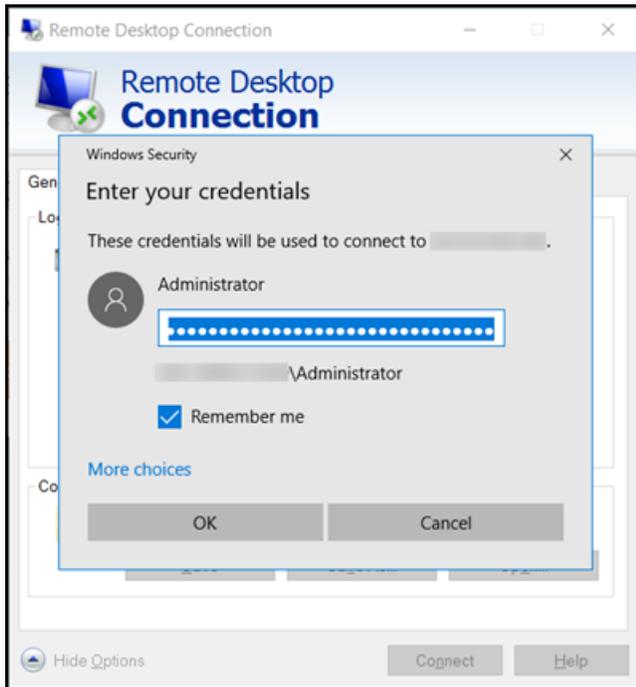
1. 若要取得您的 IP 位址，請移 Lightsail 首頁。
2. 將 IP 地址複製到剪貼簿。
3. 在 Windows 中開啟RDP用戶端，例如「遠端桌面連線」。
4. 將 IP 地址貼至 Computer (電腦) 欄位。
5. 選擇 Show Options (顯示選項)，然後輸入 Administrator 做為您的 User name (使用者名稱)。



6. 選擇連線。
7. 若要取得密碼，請前往 Lightsail 中的執行個體管理頁面。

您可以在 Lightsail 首頁上選擇執行個體名稱 (或從捷徑功能表選擇「管理」)，進入執行個體管理頁面。

- 選擇 Show default password (顯示預設的密碼)。
- 將預設的密碼複製到剪貼簿。
- 將您的密碼貼至 Remote Desktop Connection (遠端桌面連線)，然後選擇 Remember me (記住我)，以避免未來再次出現此對話方塊。



- 選擇 OK (確定)。
- 選擇 Don't ask me again for connections to this computer (連線至此電腦時不要再詢問我)，然後選擇 Yes (是)。

按照 step-by-step 說明創建運行 Linux 和 Unix 發行版的實例，如 Amazon Linux，Ubuntu，Debian 或視窗伺服器操作系統，如視窗伺服器 2022，2019 和 2016 年。

對於 Linux 和 Unix 執行個體，您可以從各種應用程式藍圖中進行選擇 WordPressLAMP，例如 LEMP、、或僅選取作業系統。對於 Windows 伺服器執行個體，您可以選擇 Windows 伺服器藍圖或 SQL 伺服器快速藍圖。

本指南涵蓋選取 AWS 區域 和可用區域、選擇具有所需運算和儲存資源的執行個體計劃 (套裝軟體)、設定網路選項 (例如 IPv4 和 IPv6)、命名執行個體，以及新增標記。建立執行個體之後，您可以使用 Lightsail 瀏覽器 SSH 或用戶端連線至執行個體，或使用您自己 SSH 或用 RDP 用戶端提供的連線詳細

資料。遵循本指南，您可以在 Lightsail 中快速啟動和存取 Linux 和 Unix 或 Windows 伺服器執行個體，並根據您的特定需求量身打造。

## 檢閱 Lightsail 執行個體藍圖供應項目

Lightsail 提供數個選項供您建立虛擬專用伺服器。此主題可協助您決定哪種作業系統 (OS)、應用程式或開發堆疊適合您的專案。我們按功能區域 (例如 CMS 和電子商務) 組織了應用程序。

### 作業系統

Lightsail 有幾個基於 Linux /Unix 或基於 Windows 的操作系統可供選擇。

#### 視窗伺服器

運行 Windows 服務器的 Lightsail 是一個快速可靠的環境，用於使用 Microsoft 網絡平台部署應用程序。有了 Lightsail，您就可以在高效能、可靠且具成本效益的運 AWS 雲端算平台上執行任何相容的 Windows 解決方案。常見的 Windows 使用案例包括企業基於 Windows 的應用程序託管，網站和 Web 服務託管，數據處理，分佈式測試，ASP。NET 應用程式主機，以及任何其他需要 Windows 軟體的應用程式 如需有關終止支援的資訊，請參閱 [Microsoft 網站](#)。

此藍圖與 IPv6 僅限 Lightsail 執行個體計劃相容。

進一步了解 [視窗伺服器 2022](#)。

#### 視窗伺服器

運行 Windows 服務器的 Lightsail 是一個快速可靠的環境，用於使用 Microsoft 網絡平台部署應用程序。Lightsail 可讓您在高效能、可靠、具成本效益的 AWS 雲端運算平台上執行任何相容的 Windows 解決方案。常見的 Windows 使用案例包括企業基於 Windows 的應用程序託管，網站和 Web 服務託管，數據處理，分佈式測試，ASP。NET 應用程式主機，以及任何其他需要 Windows 軟體的應用程式 如需有關終止支援的資訊，請參閱 [Microsoft 網站](#)。

此藍圖與 IPv6 僅限 Lightsail 執行個體計劃相容。

進一步瞭解 [視窗伺服器 2019](#)。

#### 視窗伺服器

運行 Windows 服務器的 Lightsail 是一個快速可靠的環境，用於使用 Microsoft 網絡平台部署應用程序。Lightsail 可讓您在高效能、可靠、具成本效益的 AWS 雲端運算平台上執行任何相容的 Windows 解決方案。常見的 Windows 使用案例包括企業基於 Windows 的應用程序託管，網站和

Web 服務託管，數據處理，分佈式測試，ASP。NET 應用程式主機，以及任何其他需要 Windows 軟體的應用程式 如需有關終止支援的資訊，請參閱 [Microsoft 網站](#)。

此藍圖與 IPv6 僅限 Lightsail 執行個體計劃相容。

進一步瞭解 [視窗伺服器 2016](#)。

## Amazon Linux 2023

Amazon Linux 2023 (AL2023) 是下一代 Amazon Linux，非常適合用於以上的一般用途工作負載。AWS AL2023 將在普遍推出後獲得五年的支持。AL2023 會鎖定到特定版本的 Amazon Linux 套件儲存庫，讓您控制吸收更新的方式和時機。AL2023 也提供取得頻繁更新的功能，並提供協助您符合法規遵循需求的功能。

從 AL2023 啟動的 Lightsail 執行個體預設會強制執行個體中繼資料服務版本 2 (IMDSv2)。如需詳細資訊，請參閱 [執行個體中繼資料服務第 2 版的運作方式](#)。

此藍圖與 IPv6 僅限 Lightsail 執行個體計劃相容。

了解有關 [Amazon 2023 的更多信息](#)。

## Amazon

Amazon Linux 2 是新一代的 Amazon Linux，這是來自 AWS 的 Linux 伺服器作業系統。其為開發和執行雲端和企業應用程式提供了一個安全、穩定和高效能的執行環境。使用 Amazon Linux 2，您可以獲得一個應用程式環境，該環境提供長期支援並可讓您利用 Linux 中的最新創新技術。Amazon Linux 2 是免費提供的服務。如需終止支援的資訊，請參閱 [Amazon Linux 2 FAQs](#)。

此藍圖與 IPv6 僅限 Lightsail 執行個體計劃相容。

了解有關 [Amazon 2 的更多信息](#)。

## AlmaLinux 作業系統 9

AlmaLinux OS 9 是一個開源，社區擁有和管理，永遠免費的企業 Linux 發行版，專注於長期穩定性，提供強大的生產級平台。AlmaLinux 與 RHEL® 及串流前 CentOS 相容。如需結束支援資訊，請參閱 [AlmaLinux OS 基金會網站](#)。

此藍圖與 IPv6 僅限 Lightsail 執行個體計劃相容。

進一步瞭解 [AlmaLinux 作業系統 9](#)。

## CentOS 串流 9

CentOS Stream 9 是 CentOS Stream 發行版的下一個主要發行版。CentOS 串流 9 是一個持續交付的發行版本，可追蹤 RHEL (RHEL) 發展的前面，定位為 Fedora Linux 和 RHEL 它的設計與功

能相容，RHEL並提供穩定、可預測、可管理且可重現的 Linux 環境。如需有關終止支援的資訊，請參閱 [CentOS 網站](#)。

此藍圖與IPv6僅限 Lightsail 執行個體計劃相容。

請瀏覽 [CentOS 串流](#)網站了解更多資訊。

## Debian 十一和十二

Debian 是免費的作業系統，由成千上萬來自世界各地的志願者開發，他們在網際網路上共同合作。Debian 專案的主要優勢在於其志願者協作的基礎、其對於 Debian 社群契約和免費軟體的奉獻精神，以及其致力於提供最佳作業系統的承諾。這個新版本是朝此方向發展的另一個重要步驟。如需有關終止支援的資訊，請參閱 [Debian 網站](#)。

此藍圖與IPv6僅限 Lightsail 執行個體計劃相容。

請訪問 [Debian](#) 網站了解更多信息。

## 免費 BSD 13 次

Free BSD 是一種用於為伺服器、桌上型電腦和嵌入式系統供電的作業系統。源自BSD加州大學伯克利分校UNIX開發的版本，Free BSD 已經由一個大型社區不斷開發 30 多年。Free BSD 的網絡，安全性，存儲和監控功能，包括 pf 防火牆，Capsicum 和雲ABI能力框架，ZFS文件系統和DTrace 動態跟踪框架，使 Free 成為許多最繁忙BSD的網站和最普遍的嵌入式網絡和存儲系統的首選平台。如需結束支援資訊，請參閱[免費BSD](#)網站。

此藍圖與IPv6僅限 Lightsail 執行個體計劃相容。

在[免費BSD](#)網站了解更多信息。

## 開啟中 SUSE 15 個

開放SUSE發行版是一個穩定，易於使用和完整的多用途 Linux 發行版。其目標對象是使用桌上型電腦或伺服器的使用者和開發人員。它非常適合初學者、有經驗的使用者和超級極客，簡單說，它非常適合每個人！如需結束支援資訊，請參閱[開放](#)的SUSE網站。

此藍圖與IPv6僅限 Lightsail 執行個體計劃相容。

在[開放](#)的SUSE網站上了解更多信息。

## Ubuntu 20 和 22

Ubuntu Server 用於虛擬伺服器，是以 Debian 為基礎的 Linux 作業系統。Ubuntu 的默認安裝包含了廣泛的軟件，其中包括 LibreOffice, 火狐, 雷鳥, 和傳輸. 您可以使用APT基於軟件包管理工具 ( )

來安裝許多其他軟件包，例如 Evolution，洋涇浜和 Synaptic。GIMP apt-get 如需有關終止支援的資訊，請參閱 [Ubuntu 網站](#)。

此藍圖與IPv6僅限 Lightsail 執行個體計劃相容。

前往 [Ubuntu](#) 網站瞭解更多資訊。

## 資料庫應用

下列資料庫應用程式可在 Lightsail 中使用：

### SQL 伺服器快遞

SQL 伺服器 Express 是一個關係數據庫管理系統，可以免費下載，分發和使用。它包含專門用於內嵌和較小規模應用程式的資料庫。這個 Lightsail 映像運行在視窗伺服器 2022 的基本操作系統上。

此藍圖與IPv6僅限 Lightsail 執行個體計劃相容。

進一步瞭解 [SQL 伺服器 2022 年快遞](#)。

### SQL 伺服器快遞

SQL 伺服器 Express 是一個關係數據庫管理系統，可以免費下載，分發和使用。它包含專門用於內嵌和較小規模應用程式的資料庫。這個 Lightsail 映像運行在視窗伺服器 2022 的基本操作系統上。

此藍圖與IPv6僅限 Lightsail 執行個體計劃相容。

進一步了解 [SQL 伺服器 2019 快遞](#)。

### SQL 快遞伺服器

SQL 伺服器 Express 是一個關係數據庫管理系統，可以免費下載，分發和使用。它包含專門用於內嵌和較小規模應用程式的資料庫。這個 Lightsail 映像運行在視窗伺服器 2016 的基本操作系統上。

此藍圖與IPv6僅限 Lightsail 執行個體計劃相容。

深入瞭解 [SQL 伺服器 2016 年快遞](#)。

## CMS 應用

下列內容管理系統 (CMS) 應用程式可在 Lightsail 中使用：

## WordPress 通過比特納米認證

Bitnami WordPress 是一個預先配置的 ready-to-use 映像，用於在 Lightsail 上運 WordPress 行。WordPress 是一個流行的網絡發布平台，用於構建博客和網站。您可以使用多種主題、延伸模組、外掛程式和工具進行自訂。

WordPress 設有一個完整的主題系統，它使您能夠改變你的網站的外觀和感覺，點擊幾下。您也可以使用現有的免費或商業 WordPress 佈景主題。WordPress 完全符合萬維網聯盟 ( W3C ) 的標準。

### [WordPress 在 Lightsail 上啟動和設定](#)

了解更多關於[WordPress](#)在 Bitnami 網站。

## WordPress 多站點通過比特納米認證

WordPress 多站點使管理員能夠從同一個 WordPress 實例託管和管理多個網站。這些網站可以有唯一的網域名稱，並可由擁有者自訂，同時可共享資產，例如伺服器管理所提供的主题和外掛程式。您可以將更新一次推送至所有網站，以確保它們始終保持安全無虞。

WordPress 多站點是偉大的組織，如大學，公司，和機構，需要使許多人能夠託管自己的網站，同時給予整體控制中央管理員。

### [在 Lightsail 上設置 WordPress 多站點](#)

在 Bitnami 網站上了解有關[WordPress 多站點](#)的更多信息。

## cPanel WebHost 經理人 (AWHM)

cPanel & WHM 是一套專為 Linux OS 構建的工具，它使您能夠通過使用簡單的圖形用戶界面自動執行 Web 託管任務。其目標是讓您更容易管理伺服器，並讓您的客戶更容易管理網站。

### [在 Lightsail 上使用 cPanel 和 WHM 託管網站、電子郵件和服務](#)

在cPanel網站上了解有關 [cPanel & WHM](#) 的更多信息。

## PrestaShop 由比特納米包裝

PrestaShop 是世界上最多產的電子商務解決方案之一。這是免費的開放原始碼軟體，擁有包含超過 100 萬活躍成員的社群。它旨在讓您的在線商店啟動並快速運行，具有預配置的主題，這樣就可以開始幾乎立即與現場配置器一起銷售，輕鬆自定義您的網站的外觀。PrestaShop 具有多店支持 URLs，可定制的多個支付網關選項（包括 PayPal 和條紋），以及與 AmazonBay，Facebook 等的市場集成。

### [在 Lightsail 上建立 PrestaShop 網站](#)

了解有關PrestaShop網站[PrestaShop](#)的更多信息。

## Bitnami 封裝的 Ghost

Ghost 是一個從個人部落格到主流新聞網站都適用的出版平台。建置在 Node.js 上，它的現代技術堆疊可使開發人員多樣且彈性地尋求與其他應用程式和工具整合，同時又可讓內容創作者輕鬆使用。

### [在 Lightsail 上部署幽靈網站](#)

了解更多關於[比特納米鬼魂在 Bit nami](#) 網站。

## Bitnami 封裝的 Joomla!

名字的 Joomla! 是一個預先設定好的 ready-to-use 映像檔，用來執行 Joomla! 在 Lightsail 上。Joomla! 是一個您可以用來構建各種網站或門戶網站。這包括個人、公司、小型企業、非營利及其他組織網站。

Joomla! 還包含註冊系統，可讓使用者設定個人選項。身份驗證是用戶管理的重要組成部分，而 Joomla! 支持多種協議LDAP，包括 OpenID 等。Joomla! 支援許多不同的語言，並提供使用方式的指導和管理面板。此外，Banner Manager (橫幅管理員) 可讓您輕鬆地設定和管理您網站的橫幅。您可以追蹤指標，包括設定曝光次數URLs、特殊值等。

### [開始使用! 關於 Lightsail](#)

進一步了解! 在比特納米網站。

## Bitnami 封裝的 Drupal

Drupal 的位置是一個預配置, ready-to-use 圖像上運行 Drupal 的 Lightsail. Drupal 是一種內容管理平台，可協助使用者輕鬆發佈、管理和組織內容。它用於社群 Web 入口網站、討論網站、公司網站等。您可以透過插入模組以輕鬆擴展 Drupal。Drupal 是專為高性能而構建的，可擴展到許多服務器，並且易於與REST，JSONSOAP，和其他格式集成。

您可以使用適用於 Drupal 的數千種免費附加模組和設計。Drupal 也支援多種語言。

### [在 Lightsail 上設置和自定義您的 Drupal 網站](#)

了解有關 [Drupal](#) 的更多信息在比特南美網站。

## 應用程式堆疊和伺服

Lightsail 有五個應用程式堆疊和伺服器，適用於各種開發專案。每個映像皆使用 Linux/Unix (Ubuntu) 做為基礎作業系統。

## LAMP堆棧 ( PHP8 ) 由比特納米打包

Bitnami LAMP 堆疊可簡化應用程式的開發與部署作業PHP。它包括 Apache、My SQL、PHP和的 ready-to-run 版本 phpMyAdmin，以及執行這些元件所需的其他軟體。Bitnami LAMP 堆疊已完全整合和設定，因此只要在 Lightsail 中建立執行個體，就可以立即開始開發應用程式。Bitnami LAMP 堆棧會定期更新，以確保您始終可以訪問每個捆綁組件的最新穩定版本。

此藍圖與IPv6僅限 Lightsail 執行個體計劃相容。

### [在 Lightsail 上設置燈具堆疊](#)

在 Bitnami 網站上了解有關 [Bitnami LAMP 堆棧](#) 的更多信息。

## Bitnami 封裝的 Django

Django 是高階 Python Web 框架，可激發快速開發和簡潔實用的設計。Python 是一種動態物件導向程式設計語言，可用於多種軟體開發。比特納米 Django 堆棧極大地簡化了 Django 的部署及其運行時依賴關係，並包括 Python，Django 的，我的和阿帕奇的 ready-to-run 版本。SQL

在比特納米網站上了解有關[比特納米 Django 堆棧](#)的更多信息。

## Bitnami 封裝的 Node.js

名稱 Node.js 是一個預先配置的 ready-to-use 映像，用於在 Lightsail 上運行 Node.js。Node.js 是一個基於 Chrome JavaScript 運行時構建的平台，可輕鬆創建快速，可擴展的網絡應用程序。它使用事件驅動型、非封鎖式 I/O 模型，因此它很輕便且高效。Node.js 非常適合用於資料密集型的即時應用程式。

### [在 Lightsail 上開始使用 Node.js](#)

在網站上了解有關 [Node.js 堆棧](#) 的更多信息。

## MEAN堆棧打包由比特納米

Bitnami MEAN 堆棧為 MongoDB 和 Node.js 提供了一個完整的開發環境，您可以在一鍵部署。它包括最新的穩定版本的 MongoDB，快遞，角，Node.js，Git 的PHP，和 RockMongo。

此藍圖與IPv6僅限 Lightsail 執行個體計劃相容。

在 Bitnami 網站上了解有關[MEAN堆棧](#)的更多信息。

## GitLab CE 由比特奈米包裝

比特納米 GitLab 社區版 ( CE ) 是一個預先配置的 ready-to-use 映像，用於在 Lightsail 上運 GitLab 行。GitLab 是自託管的 Git 管理軟件，它是快速，安全的，基於 Rails 的 Ruby。GitLab CI ( 也包括在內 ) 是一個開源持續集成 ( CI ) 服務器，與 Git 和 GitLab。

您可以 GitLab 在自己的伺服器上保護程式碼安全、管理儲存庫、使用者和存取權限。它可獨立自主運作，因此您可以輕鬆地將它複製或移動至不同的伺服器。

### [在 Lightsail 上設定和設定 GitLab CE 執行個體](#)

在 Bitnami 網站上了解有關 [GitLab 堆棧](#) 的更多信息。

### Ngix ( LEMP 堆棧 ) 由比特納米打包

Bitnami NGINX 堆棧提供了一個完整的 PHPSQL，我的和 NGINX 開發環境，您可以一鍵啟動。它還捆綁 phpMyAdmin，，SQLite ImageMagick，快速 CGI，內存緩存，GD，，CURLPEARPECL，和其他組件。

NGINX 是非同步伺服器，其主要優點是可擴充性。該 NGINX 堆棧也被稱為 LEMP ( Linux NGINX SQL，我的和 PHP )。

### [在 Lightsail 上部署和管理 Ngix 網路伺服器](#)

在網站上了解有關 [Ngix 堆棧](#) 的更多信息。

### Plesk Hosting Stack on Ubuntu (Ubuntu 上的 Plesk 託管堆疊)

使用由 Plesk 提供支援的主機堆疊，在 Lightsail 上建置、保護和執行網站和應 AWS 應用程式。這包括所有基於 Web 的服務器管理和安全工具，以及圖形用戶界面中的 WordPress 自動化。它可簡化 Web 專業人員的工作，並提供您客戶所需的可擴展性、安全性和效能。

### [設定並配置 Plesk。](#)

在 Plesk 網站上了解有關 [Plesk 堆棧](#) 的更多信息。

## 電子商務應用程式

Lightsail 目前擁有一個電子商務應用程式圖像：Magento。Magento 映像使用 Linux/Unix (Ubuntu) 做為基礎作業系統。

### Bitnami 封裝的 Magento

Magento 的是一個預先配置, ready-to-use 圖像上運行 Magento 的 Lightsail. 您可以使用 Magento 建立吸引人、反應快速且安全的網站。Magento 是一種功能豐富且有彈性的電子商務解決方案，包含交易選項、多商店功能、忠誠度計畫、產品分類、購物者篩選、提升規則等。

您可以使用 Magento 建立高度自訂的電子商務網站以反映您的品牌。Magento 整合您的商業營運，因此您可以依照業務需求來管理您的電子商務網站。

## [在 Lightsail 上設置和配置](#)

了解更多關於 [Magento 的堆棧](#) 在比特南美網站。

## 專案管理應用程式

Lightsail 目前有一個項目管理應用程式映像，紅礦。此映像使用 Linux/Unix (Ubuntu) 做為基礎作業系統。

由比特納米包裝的紅礦

Bitnami 紅礦是一個預先配置的 ready-to-use 圖像，用於在 Lightsail 上運行紅礦。Redmine 是一種有彈性的專案管理 Web 應用程式。它包括對多個項目的支持，基於角色的訪問控制，甘特圖和日曆，新聞，文檔和文件的管理，每個項目的維基和論壇，SCM集成等。

此藍圖與IPv6僅限 Lightsail 執行個體計劃相容。

### [在 Lightsail 上設定和保護紅礦執行個體](#)

在 Bitnami 網站上了解有關[紅礦堆棧](#)的更多信息。

## 使用 Lightsail 中的防火牆控制執行個體流

Amazon Lightsail 主控台內的防火牆充當虛擬防火牆，可控制允許透過其公有 IP 位址連接到執行個體的流量。您在 Lightsail 中建立的每個執行個體都有兩個防火牆；一個用於IPv4地址，另一個用於IPv6位址。每個防火牆都包含一組篩選進入執行個體之流量的規則。兩個防火牆彼此獨立；您必須為和分別設定防火牆規則IPv4則IPv6。您可隨時新增和刪除允許或限制流量的規則，以編輯執行個體的防火牆。

## Lightsail 防火牆

每個 Lightsail 執行個體都有兩個防火牆；一個用於IPv4地址，另一個用於IPv6地址。進出 Lightsail 執行個體的所有網際網路流量都會通過其防火牆。執行個體防火牆會控制可流入執行個體的網際網路流量。不過，防火牆不會控制從中流出的流量 – 防火牆允許所有傳出流量。您可隨時新增和刪除允許或限制傳入流量的規則，以編輯執行個體的防火牆。請注意，兩個防火牆彼此獨立；您必須為IPv4和分別設定防火牆規則IPv6。

防火牆規則一律為許可制。您無法建立拒絕存取的規則。您可將規則新增至執行個體防火牆，以允許流量觸達執行個體。將規則新增至執行個體的防火牆時，必須指定要使用的通訊協定、要開啟的連接埠，

以IPv4及允許連線至執行個體的和IPv6位址，如下列範例 (用於IPv4) 所示。您也可以指定應用程式層通訊協定類型，這是根據您打算在執行個體上使用的服務，為您指定通訊協定和連接埠範圍的預設。

### IPv4 Firewall [?](#)

Create rules to open ports to the internet, or to a specific IPv4 address or range.

[Learn more about firewall rules](#)

**+ Add rule**

Application	Protocol	Port or range / Code	Restricted to		
SSH	TCP	22	Any IPv4 address Lightsail browser SSH/RDP <a href="#">?</a>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
HTTP	TCP	80	Any IPv4 address	<input checked="" type="checkbox"/>	<input type="checkbox"/>
HTTPS	TCP	443	Any IPv4 address	<input checked="" type="checkbox"/>	<input type="checkbox"/>

#### **⚠ Important**

防火牆規則僅會影響流經執行個體之公有 IP 地址的流量。它不會影響流入執行個體私有 IP 位址的流量，而執行個體可能來自您帳戶中的 Lightsail 資源 AWS 區域，或是對等虛擬私有雲端 (VPC) 中的資源。AWS 區域

本指南的後續幾個章節將說明防火牆規則及其可設定的參數。

## 建立防火牆規則

建立防火牆規則以讓用戶端能夠與執行個體建立連線，或與執行個體上執行的應用程式建立連線。例如，若要讓所有 Web 瀏覽器連線至執行個體上的 WordPress 應用程式，您可以設定防火牆規則，以便從任何 IP 位址透過連接埠 80 啟用傳輸控制通訊協定 (TCP)。如果執行個體的防火牆上已設定此規則，您可以刪除該規則，以封鎖 Web 瀏覽器連線至執行個體上的 WordPress 應用程式。

#### **⚠ Important**

您可以使用 Lightsail 主控台一次最多新增 30 個來源 IP 位址。若要一次最多新增 60 個 AWS SDK IP 位址，請使用 Lightsail API、AWS Command Line Interface (AWS CLI) 或。此配額會針對IPv4規則和IPv6規則分別強制執行。例如，防火牆可以有 60 個IPv4流量輸入規則和 60 個輸入規則的IPv6流量。我們建議您將個別 IP 位址合併為CIDR範圍。如需詳細資訊，請參閱本指南的[指定來源 IP 地址](#)一節。

您也可以透過設定僅從需要建立連線之電腦 IP 位址透 TCP 過連接埠 22 啟用的防火牆規則，讓用 SSH 戶端連線至您的執行個體，以便在伺服器上執行管理工作。在這種情況下，您不希望允許任何 IP 位址建立與執行個體的 SSH 連線，因為這樣做可能會導致執行個體的安全風險。

### Note

本節所述的防火牆規則範例可能會依預設存在於執行個體的防火牆中。如需詳細資訊，請參閱本指南後續章節所述的[預設防火牆規則](#)。

若特定連接埠有超過一個規則，我們會套用最寬鬆的規則。例如，如果您新增允許從 IP 位址 192.0.2.1 存取 TCP 連接埠 22 (SSH) 的規則。然後，您新增另一個允許所有人存取 TCP 連接埠 22 的規則。因此，每個人都可以訪問 TCP 端口 22。

## 指定通訊協定

通訊協定是指在兩部電腦之間傳輸資料時所採用的格式。Lightsail 可讓您在防火牆規則中指定下列通訊協定：

- 傳輸控制通訊協定 (TCP) 主要用於建立和維護用戶端與執行個體上執行的應用程式之間的連線，直到資料交換完成為止。這是廣泛使用的通訊協定，而且是您通常可能會在防火牆規則中指定的通訊協定。TCP 保證不會遺失任何傳輸的資料，而且傳送的所有資料都會傳送給預期的收件者。它的理想用途是需要高可靠性的網路應用程式，以及用於傳輸時間相對較不緊急的情況，例如 Web 瀏覽、金融交易和文字簡訊服務。如果資料的部分遺失，這些使用案例將會失去重要的價值。
- 使用者資料包通訊協定 (UDP) 主要用於在用戶端與執行個體上執行的應用程式之間建立低延遲和容錯的連線。它的理想用途是將感知延遲視為至關重要的網路應用程式，例如遊戲、語音和視訊通訊。這些使用案例可能會遭受一些資料遺失，而不會對感知品質造成負面影響。
- 網際網路控制訊息通訊協定 (ICMP) 主要用於診斷網路通訊問題，例如判斷資料是否及時到達其預期目的地。它的理想用途是 Ping 公用程式，可用來測試本機電腦與執行個體之間的連線速度。它會回報資料觸達執行個體並返回本機電腦所需的時間。

### Note

當您使用 Lightsail 主控台將 ICMP 規則新增至執行個體的 IPv6 防火牆時，規則會自動設定為使用 ICMPv6。有關更多信息，請參閱維基百科 IPv6 上的[互聯網控制消息協議](#)。

- 全部可用來允許所有通訊協定流量流入執行個體。當您不確定要指定哪個通訊協定時，請指定此通訊協定。這包含所有網際網路通訊協定；不只是以上指定的通訊協定。如需詳細資訊，請參閱 Internet Assigned Numbers Authority 網站上的[通訊協定號碼](#)。

## 指定連接埠

類似於電腦上的實體連接埠，可讓電腦與鍵盤和滑鼠等周邊裝置進行通訊，網路連接埠可做為執行個體的網際網路通訊端點。當電腦想要與執行個體連線時，它會公開連接埠以建立通訊。

您可在防火牆規則中指定的連接埠可能介於 0 至 65535。當您建立防火牆規則以讓用戶端能夠與執行個體建立連線時，您需要指定將使用的通訊協定 (請參閱本指南前述章節)，以及可透過哪些連接埠號碼建立連線。您也可以指定允許使用通訊協定和連接埠建立連線的 IP 地址；請參閱本指南下一節所述。

以下是與服務搭配使用的其中一些常用連接埠：

- 透過檔案傳輸通訊協定 (FTP) 的資料傳輸會使用連接埠 20。
- 命令控制FTP使用端口 21。
- 安全殼層 (SSH) 使用連接埠 22。
- Telnet 遠端登入服務以及未加密文字簡訊使用連接埠 23。
- 簡易郵件傳送通訊協定 (SMTP) 電子郵件路由使用通訊埠 25。

### Important

若要在執行個體SMTP上啟用，您也必須為執行個體設DNS定反向功能。否則，您的電子郵件可能會受到TCP通訊埠 25 的限制。如需詳細資訊，請參閱在 [Amazon Lightsail 執行個體上DNS為電子郵件伺服器設定反向設定](#)。

- 網域名稱系統 (DNS) 服務使用連接埠 53。
- Web 瀏覽器用來連接到網站的超文本傳輸協議 ( HTTP ) 使用端口 80。
- 郵局協議 ( POP3 ) 用於電子郵件客戶端從伺服器檢索電子郵件使用端口 110。
- 網路新聞傳輸通訊協定 (NNTP) 使用連接埠 119。
- 網路時間通訊協定 (NTP) 使用連接埠 123。
- 用來管理數位郵件的網際網路訊息存取通訊協定 (IMAP) 會使用連接埠 143。
- 簡易網路管理通訊協定 (SNMP) 使用連接埠 161。
- HTTP網絡瀏覽器使SSL用的安全 ( HTTPS ) 通HTTP過TLS/使用建立與網站的加密連接使用端口 443。

如需詳細資訊，請參閱 Internet Assigned Numbers Authority 網站上的[服務名稱和傳輸通訊協議連接埠號碼登錄檔](#)。

## 指定應用程式層級通訊協定類型

您可在建立防火牆規則時指定應用程式層通訊協定類型，這些是根據您要在執行個體上啟用的服務，為您指定規則的通訊協定和連接埠範圍的預設集。如此一來，您就不必搜尋一般通訊協定和連接埠，即可用於SSH、RDP、HTTP、和其他服務。您可以直接選擇應用程式層通訊協定類型，以及為您指定的通訊協定和連接埠。如果您偏好指定自己的通訊協定和連接埠，您可以選擇 Custom rule (自訂規則) 應用程式層通訊協定類型，這會讓您控制這些參數。

### Note

您只能使用 Lightsail 主控台來指定應用程式層通訊協定類型。您無法使用 Lightsail API、AWS Command Line Interface (AWS CLI) 或 SDKs 指定應用程式層通訊協定類型。

Lightsail 主控台提供下列應用程式層通訊協定類型：

- Custom (自訂) – 選擇此選項以指定您自己的通訊協定和連接埠。
- All protocols (所有通訊協定) – 選擇此選項以指定所有通訊協定，以及指定您自己的連接埠。
- 全部 TCP — 選擇此選項可使用TCP通訊協定，但您不確定要開啟哪個連接埠。如此可TCP在所有連接埠上啟用 (0-65535)。
- 全部 UDP — 選擇此選項可使用UDP通訊協定，但您不確定要開啟哪個連接埠。如此可UDP在所有連接埠上啟用 (0-65535)。
- 全部 ICMP — 選擇此選項可指定所有ICMP類型和代碼。
- 自訂 ICMP — 選擇此選項可使用ICMP通訊協定並定義ICMP類型和代碼。有關ICMP類型和代碼的更多信息，請參閱維基百科上的[控制消息](#)。
- DNS — 當您想要在執行個體DNS上啟用時，請選擇此選項。這會啟用TCP並透UDP過連接埠 53。
- HTTP — 當您想要啟用 Web 瀏覽器連線至執行個體上託管的網站時，請選擇此選項。這會啟用TCP通訊埠 80 以上。
- HTTPS — 當您想要啟用 Web 瀏覽器以建立與執行個體上託管之網站的加密連線時，請選擇此選項。這可透TCP過連接埠 443 啟用。
- 我SQL的/Aurora — 選擇此選項可讓用戶端連線至執行個體上託管的 My SQL 或 Aurora 資料庫。這可以透TCP過連接埠 3306 啟用。

- Oracle-RDS — 選擇此選項可讓從屬端連線至執行處理上託管的 Oracle 或RDS資料庫。這可透TCP過連接埠 1521 啟用。
- Ping (ICMP) — 選擇此選項可讓您的執行個體使用 Ping 公用程式回應要求。在IPv4防火牆上，這會啟用ICMP類型 8 ( 迴聲 ) 和代碼 -1 ( 所有代碼 )。在IPv6防火牆上，這會啟用ICMP類型 129 ( 回應回覆 ) 和代碼 0。
- RDP— 選擇此選項可讓用RDP戶端連線至您的執行個體。這會透TCP過連接埠 3389 啟用。
- SSH— 選擇此選項可讓用SSH戶端連線至您的執行個體。這可透TCP過連接埠 22 啟用。

## 指定來源 IP 地址

根據預設，防火牆規則可讓所有 IP 地址透過指定的通訊協定和連接埠連線至執行個體。這是理想的流量，如網絡瀏覽器HTTP和HTTPS。但是，這會對諸如SSH和之類的流量構成安全風險RDP，因為您不希望允許所有 IP 地址都能夠使用這些應用程序連接到您的執行個體。因此，您可以選擇將防火牆規則限制為 IP 位IPv6址IPv4或某個位址或範圍。

- 針對IPv4防火牆-您可以指定單一IPv4位址 (例如 203.0.113.1) 或位址範圍。IPv4在 Lightsail 主控台中，您可以使用破折號 (例如，192.0.0-192.0.2.255) 或區塊標記法 (例如，192.0.2.0/24) 來指定範圍。CIDR有關CIDR塊表示法的更多信息，請參閱維基百科上的[無類別域間路由](#)。
- 對於IPv6防火牆-您可以指定單一IPv6位址 (例如，2001:0 資料庫 8:85 和 3:0000:8)，或是位址範圍。IPv6在 Lightsail 主控台中，只IPv6能使用CIDR區塊標記法 (例如 2001: db8:: /32) 來指定範圍。有關IPv6CIDR塊符號的更多信息，請參閱維基百科上的[IPv6CIDR塊](#)。

## 預設 Lightsail 牆規則

當您建立新的執行個體時，其執行個體IPv4和IPv6防火牆會預先設定下列一組預設規則，以便進行基本存取您的執行個體。根據您建立的執行個體類型，預設規則會有所不同。這些規則會以應用程式、通訊協定、連接埠和來源 IP 地址的形式列出 (例如應用程式 - 通訊協定 - 連接埠 - 來源 IP 地址)。

AlmaLinux, Amazon Linux 2, Amazon Linux 2023, CentOS, Debian, 自由, 開放 BSDSUSE, 和 Ubuntu (基本操作系統)

SSH-TCP-22-所有 IP 位址

HTTP-TCP-80-所有 IP 位址

WordPress, 鬼, 是啊!、 PrestaShop、 和 Drupal (CMS應用程式)

SSH-TCP-22-所有 IP 位址

HTTP-TCP-80-所有 IP 位址

HTTPS-TCP-443-所有 IP 位址

cPanel & WHM ( CMS 應用程式 )

SSH-TCP-22-所有 IP 位址

DNS(UDP)-UDP-53-所有 IP 位址

DNS(TCP)-TCP-53-所有 IP 位址

HTTP-TCP-80-所有 IP 位址

HTTPS-TCP-443-所有 IP 位址

自訂-TCP-2078-所有 IP 位址

自訂-TCP-2083-所有 IP 位址

自訂-TCP-2087-所有 IP 位址

自訂-TCP-2089-所有 IP 位址

LAMP、傑戈、Node.js MEAN GitLab、和尼金克斯 (開發堆疊)

SSH-TCP-22-所有 IP 位址

HTTP-TCP-80-所有 IP 位址

HTTPS-TCP-443-所有 IP 位址

Magento 的eCommerce 應用程式

SSH-TCP-22-所有 IP 位址

HTTP-TCP-80-所有 IP 位址

HTTPS-TCP-443-所有 IP 位址

Redmine (專案管理應用程式)

SSH-TCP-22-所有 IP 位址

HTTP-TCP-80-所有 IP 位址

HTTPS-TCP-443-所有 IP 位址

## Plesk (託管堆疊)

SSH-TCP-22-所有 IP 位址

HTTP-TCP-80-所有 IP 位址

HTTPS-TCP-443-所有 IP 位址

自訂-TCP-53-所有 IP 位址

自訂-UDP-53-所有 IP 位址

自訂-TCP-8443-所有 IP 位址

自訂-TCP-8447-所有 IP 位址

視窗伺服器 2022、視窗伺服器 2019 及視窗伺服器 2016

SSH-TCP-22-所有 IP 位址

HTTP-TCP-80-所有 IP 位址

RDP-TCP-3389-所有 IP 地址

SQL2022 年伺服器速遞、2019 年SQL伺服器快遞和SQL伺服器快遞 2016

SSH-TCP-22-所有 IP 位址

HTTP-TCP-80-所有 IP 位址

RDP-TCP-3389-所有 IP 地址

## 新增防火牆規則至 Lightsail 執行個體

您可以將規則新增至 Amazon Lightsail 執行個體的IPv4和IPv6防火牆，以控制允許連線到該執行個體的流量。新增防火牆規則時，您可以指定應用程式層通訊協定類型、通訊協定、連接埠，IPv4以及允許連線至執行個體的來源IPv6位址。如需有關防火牆的詳細資訊，請參閱[防火牆和連接埠](#)。

### 新增和編輯執行個體防火牆規則

完成下列步驟，即可在 Lightsail 主控台中新增或編輯防火牆規則。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁上，選擇「實體」索引標籤。

3. 選擇您要新增或編輯防火牆規則的執行個體名稱。
4. 選擇執行個體管理頁面上的 Networking (聯網) 標籤。

[網路功能] 索引標籤會顯示執行個體的公有和私有 IP 位址，以及執行個體已設定的IPv4或IPv6防火牆。

 Note

只有在您已IPv6啟用執行個體的情況下，才會顯示IPv6防火牆。如需詳細資訊，請參閱[啟用或停用IPv6](#)。

5. 根據規則的來源 IP 是否為IPv4或位IPv6址，完成下列其中一個步驟：
  - 若要新增IPv4防火牆規則，請向下捲動至頁面的「IPv4防火牆」區段，然後選擇「新增規則」。
  - 若要新增IPv6防火牆規則，請向下捲動至頁面的「IPv6防火牆」區段，然後選擇「新增規則」。

您也可以選擇現有任一防火牆規則旁的 Edit (編輯) 鉛筆圖示以進行編輯。

6. 在 Application (應用程式) 下拉式功能表中選擇應用程式層協定類型。

當您選擇應用程式層協定類型時，系統會為您指定一組協定和連接埠預設值。範例值為「自訂」、「全部」TCP、「全部 UDP」ICMP SSH、「自訂」和RDP。

根據選擇的應用程式層通訊協定類型，您可以設定下列選用設定：

- (選用) 如果您選擇 Custom (自訂) 選項，然後您可以在 Protocol (協定) 下拉式功能表中選取值。可用的通訊協定值為TCP和UDP。

您也可以在 Port (連接埠) 欄位中輸入單一連接埠號碼或某個連接埠號碼範圍 (例如 7000-8000)。

- (選擇性) 如果您選擇「自訂」ICMP 選項，則可以在「ICMP類型」欄位中指定類型，並在「ICMP代碼」欄位中指定代碼。有關ICMP類型和代碼的更多信息，請參閱維基百科上的[控制消息](#)。

 Note

當您使用 Lightsail 主控台將ICMP規則新增至執行個體的IPv6防火牆時，規則會自動設定為使用ICMPv6。有關更多信息，請參閱維基百科IPv6上的[互聯網控制消息協議](#)。

- (選用) 選取 Restrict to IP address (限制 IP 地址)，以將特定協定和連接埠的存取權限制為某個特定 IP 地址或 IP 地址範圍。若不選取此選項，則可為指定的協定和通訊部允許所有 IP 地址。

您可以輸入單一位IPv4址 (例如，203.0.113.1) 或地IPv4址範圍。您可以使用破折號 (例如，192.0.2.0-192.0.2.255) 或CIDR區塊標記法 (例如，192.0.2.0/24) 來指定範圍。有關CIDR塊標記法的更多信息，請參閱維基百科上的[無類別域間路由](#)。

- (選擇性) 如果您選擇SSH或RDP應用程式層通訊協定類型，然後選擇 [限制為 IP 位址]，您可以選擇 [允許 Lightsail 瀏覽器SSH/RDP]，允許使用 Lightsail 主控台中提供的瀏覽器型SSH和用RDP戶端連線至您的執行個體。若不選取此選項，則可封鎖透過這些瀏覽器型用戶端進行存取。

## 7. 選擇 Create (建立) 以將規則新增至防火牆。

防火牆規則會在幾分鐘後新增。

## 刪除防火牆規則

除了新增和編輯防火牆規則之外，您可能還想要刪除 Amazon Lightsail 執行個體的現有規則。如果您不再需要允許某些輸入流量進入執行個體，則可能需要移除防火牆規則。刪除IPv4和IPv6防火牆規則的過程非常簡單，可以直接透過 Lightsail 主控台完成。完成下列步驟，以在 Lightsail 主控台中刪除執行個體防火牆規則。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁上，選擇「實體」索引標籤。
3. 選擇您要刪除防火牆規則的執行個體名稱。
4. 選擇執行個體管理頁面上的 Networking (聯網) 標籤。
5. 根據規則的來源 IP 是否為IPv4或位IPv6址，完成下列其中一個步驟：
  - 若要刪除IPv4防火牆規則，請向下捲動至頁面的「IPv4防火牆」區段，然後選擇現有規則旁邊的「刪除」(垃圾桶圖示) 將其刪除。
  - 若要刪除IPv6防火牆規則，請向下捲動至頁面的「IPv6防火牆」區段，然後選擇現有規則旁邊的「刪除」(垃圾桶圖示) 將其刪除。

### Important

防火牆規則僅會影響流經執行個體之公有 IP 地址的流量。它不會影響流入執行個體私有 IP 位址的流量，而執行個體可能來自您帳戶中的 Lightsail 資源 AWS 區域，或是對等虛擬

私有雲端 (VPC) 中的資源。AWS 區域例如，如果您從執行個體防火牆刪除SSH規則 (連接TCP埠 22)，則相同 Lightsail 帳戶中的其他執行個體可以SSH透過指定執行個體的私有 IP 位址，繼續使用連線至該規則。AWS 區域

防火牆規則會在幾分鐘後刪除。

## Lightsail 執行個體的防火牆規則參考

您可以將規則新增至反映執行個體角色的 Amazon Lightsail 執行個體防火牆。例如，設定為 Web 伺服器的執行個體需要允許輸入 HTTP 和 HTTPS 存取的防火牆規則。資料庫執行個體需要允許存取資料庫類型的規則，例如 MySQL 透過連接埠 3306 的存取。如需防火牆的詳細資訊，請參閱 [Lightsail 中的執行個體防火牆](#)。

本指南提供可為特定存取類型新增至執行個體防火牆的防火牆規則類型範例。除非另有說明，否則規則會以應用程式、協定、連接埠和來源 IP 地址的形式列出 (例如應用程式 - 協定 - 連接埠 - 來源 IP 地址)。

### 內容

- [Web 伺服器規則](#)
- [從電腦連線至執行個體的規則](#)
- [資料庫伺服器規則](#)
- [DNS 伺服器規則](#)
- [SMTP 電子郵件](#)

## Web 伺服器規則

以下傳入規則會允許 HTTP 和 HTTPS 存取。

### Note

某些 Lightsail 執行個體預設會設定下列防火牆規則。如需詳細資訊，請參閱[防火牆和連接埠](#)。

## HTTP

HTTP - TCP - 80 - 所有 IP 地址

## HTTPS

HTTPS - TCP - 443 - 所有 IP 地址

### 從電腦連線至執行個體的規則

若要連線至執行個體，請新增允許 SSH 存取 (適用於 Linux 執行個體) 或 RDP 存取 (適用於 Windows 執行個體) 的規則。

#### Note

根據預設，所有 Lightsail 執行個體都會設定下列任一防火牆規則。如需詳細資訊，請參閱[防火牆和連接埠](#)。

## SSH

SSH - TCP - 22 - 電腦的公有 IP 地址，或是本機網路中的 IP 地址範圍 (CIDR 區塊標記法)。

## RDP

RDP - TCP - 3389 - 電腦的公有 IP 地址，或是本機網路中的 IP 地址範圍 (CIDR 區塊標記法)。

### 資料庫伺服器規則

以下傳入規則是您可以為資料庫存取新增之規則的範例，取決於您在執行個體上執行的資料庫類型為何。

#### SQL Server

自訂 - TCP - 1433 - 電腦的公有 IP 地址，或是本機網路中的 IP 地址範圍 (CIDR 區塊標記法)。

#### MySQL/Aurora

MySQL/Aurora - TCP - 3306 - 電腦的公有 IP 地址，或是本機網路中的 IP 地址範圍 (CIDR 區塊標記法)。

#### PostgreSQL

PostgreSQL - TCP - 5432 - 電腦的公有 IP 地址，或是本機網路中的 IP 地址範圍 (CIDR 區塊標記法)。

## Oracle-RDS

Oracle-RDS - TCP - 1521 - 電腦的公有 IP 地址，或是本機網路中的 IP 地址範圍 (CIDR 區塊標記法)。

## Amazon Redshift

自訂 - TCP - 5439 - 電腦的公有 IP 地址，或是本機網路中的 IP 地址範圍 (CIDR 區塊標記法)。

## DNS 伺服器規則

若您已將執行個體設為 DNS 伺服器，您必須確保 TCP 和 UDP 流量能透過連接埠 53 觸達 DNS 伺服器。

### DNS (TCP)

DNS (TCP) - TCP - 53 - 電腦的 IP 地址，或是本機網路中的 IP 地址範圍 (CIDR 區塊標記法)。

### DNS (UDP)

DNS (UDP) - UDP - 53 - 電腦的 IP 地址，或是本機網路中的 IP 地址範圍 (CIDR 區塊標記法)。

## SMTP 電子郵件

若要在執行個體上啟用 SMTP，您必須設定下列防火牆規則。

### Important

設定下列規則後，您也必須設定執行個體的反向 DNS。否則，電子郵件可能會限制為須透過 TCP 連接埠 25 傳送。如需詳細資訊，請參閱[設定電子郵件伺服器的反向 DNS](#)。

## SMTP

自訂 - TCP - 25 - 與您執行個體通訊之主機的 IP 地址

## 偵測 Lightsail 執行個體爆發，以獲得最佳效能

Amazon Lightsail 執行個體可提供基準的 CPU 效能，但也可以視需要暫時提供超過基準的額外 CPU 效能。這稱為高載。基準效能和高載能力是由下列執行個體指標所控制：

- CPU使用率 — 已配置運算單元在執行個體上使用的百分比。此指標可識別在執行個體上執行應用程式所使用的處理能力。
- CPU成組分解容量百分比 — 執行個體可用的CPU效能百分比。
- CPU突發容量分鐘 — 執行個體以 100% CPU 使用率爆發的可用時間量。

透過下列主題，您將了解如何監視這些指標，以最大限度地提高執行個體的可用性。

## 主題

- [瞭解 Lightsail 執行個體的基準CPU效能和超載容量累積](#)
- [檢視 Light CPU sail 執行個體的高載容量應計](#)
- [識別 Lightsail 實體爆發的時間](#)
- [監控您的執行個體的 CPU 高載容量](#)
- [檢視 Lightsail 執行個體的CPU使用率和高載容量](#)
- [疑難排解 Lightsail 執行個體的高 CPU 使用率](#)

## 瞭解 Lightsail 執行個體的基準CPU效能和超載容量累積

Lightsail 執行個體每小時持續獲得 (以毫秒級解析度) 設定的CPU突發容量速率，當執行個體CPU使用率大於 0% 時也會消耗這個速率。是否累積或消耗突發容量的會計過程也會以毫秒級的分辨率進行，因此您不必擔心超支CPU突發容量; 短時間的突發CPU使用了一小部分的突發容量。

如果執行個體使用的CPU資源少於基準效能所需的資源 (例如閒置時)，則會以CPU成組分解容量百分比和分鐘的形式累積未耗用的CPU成組分組容量。如果您的執行個體需要超越基準效能等級，就會花費累積的CPU成組分解容量。您的執行個體累積的CPU成組分解容量越多，在需要更高效能時，就會超越基準線的時間就越長。

## 基準CPU效能

下表概述 Lightsail 中雙堆疊執行個體計劃的效能基準。雖然IPv6僅計劃的價格不同，但性能基準是相同的。

實例計劃	vCPUs	記憶體	儲存	效能基準
Linux 或 Unix 5 美元和視窗 9.50	2	512 MB	20 GB	5%
Linux 或 Unix 7 美元和視窗 14 美元	2	1 GB	四十英寸	10%

實例計劃	vCPUs	記憶體	儲存	效能基準
Linux 或 Unix 12 美元和視窗 22 美元	2	2 GB	六十 GB	20%
Linux 或 Unix 24 美元和視窗 44 美元	2	4 GB	80 英寸	20%
Linux 或 Unix 44 美元和視窗 74 美元	2	8 GB	英格蘭	30%
Linux 或 Unix 84 美元和視窗 124 美元	4	16 GB	三百二十	40%
Linux 或 Unix 164 美元和視窗 244 美元	8	32 GB	英國	40%
* Linux 或 Unix 384 美元和視窗 574 元	16	64 GB	英国	40%

\* Linux 或 Unix 384 和視窗 574 執行個體計劃不會累積CPU成組分解容量。他們會根據需要自動爆裂。

這些效能基準是每 v CPU。Lightsail 主控台內的CPU使用率量度圖表會針對具有一個以上 v 的執行個體CPU使用率和基準平均值。CPU例如，以 Linux 或 UNIX 為基礎的USD每月 44 美元執行個體具有兩個執行個體，vCPUs 而平均CPU使用率基準為 30%。因此，假如：

- 一 v 以 50% CPU 運作，另一個則為 0%，圖表上顯示 25% 的平均CPU使用率。這使得執行個體的CPU使用率低於 30% 的基準線，並處於可持續發展區域。
- 一 v 以 30% CPU 運作，另一個為 20%，圖表上會顯示 25% 的平均CPU使用率。這使得執行個體的CPU使用率低於 30% 的基準線，並處於可持續發展區域。
- 其中一個 v 以 35% CPU 運作，另一個為 25%，圖表上會顯示 30% 的平均CPU使用率。這會使執行個體的CPU使用率達到 30% 的基準。
- 一 v 以 100% CPU 運作，另一個則為 90%，圖表上會顯示 95% 的平均CPU使用率。這會使執行個體的CPU使用率高於 30% 的基準線，而且位於高載區域中。

如需有關永續和可高載區域的詳細資訊，請參閱本指南稍後的[識別您的執行個體高載的時間](#)。

## 前一代CPU效能

下表列出在 2023 年 6 月 29 日之前建立之 Lightsail 執行個體的效能基準。這些效能基準是每 v CPU。

實例計劃	vCPUs	記憶體	儲存	效能基準
Linux 或 Unix 5 美元和視窗 9.50	1	512 MB	20 GB	5%
Linux 或 Unix 7 美元和視窗 14 美元	1	1 GB	四十英寸	10%
Linux 或 Unix 12 美元和視窗 22 美元	1	2 GB	六十 GB	20%
Linux 或 Unix 24 美元和視窗 44 美元	2	4 GB	80 英寸	20%
Linux 或 Unix 44 美元和視窗 74 美元	2	8 GB	英格蘭	30%
Linux 或 Unix 84 美元和視窗 124 美元	4	16 GB	三百二十	22.5%
Linux 或 Unix 164 美元和視窗 244 美元	8	32 GB	英國	17%

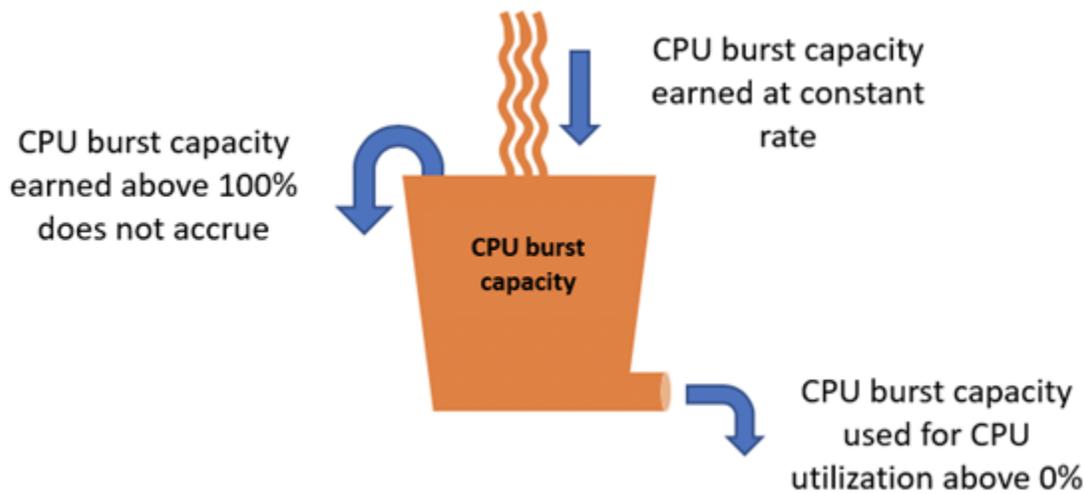
## 檢視 Light CPU sail 執行個體的高載容量應計

Amazon Lightsail 執行個體計劃 (Linux 或 Unix 384 美元和視窗 574 美元計劃除外) 每小時累積 4.17% 的突發容量。CPU 可累積的最大 CPU 成組容量等於 24 小時期間內可獲得的 CPU 突發容量百分比量。當 CPU 突發容量百分比達到 100% 時，您的執行個體會停止累積 CPU 成組分解容量。

### Important

#### 累計的 CPU 爆裂容量

- Linux 或 Unix 384 和視窗 574 美元執行個體計劃 — 這些計劃不會累積 CPU 成組分解容量。他們會根據需要自動爆裂。
- 2023 年 6 月 29 日之前建立的執行個體 — 如果執行個體停止，則不會持續 CPU 成組分解容量。如果您停止執行個體，則會失去所有累積的成組分解容量。
- 在 2023 年 6 月 29 日當天或之後建立的執行個體 — CPU 爆發容量在執行個體停止和啟動之間持續七天。
- 執行中執行個體上的累積 CPU 成組分解容量不會過期。

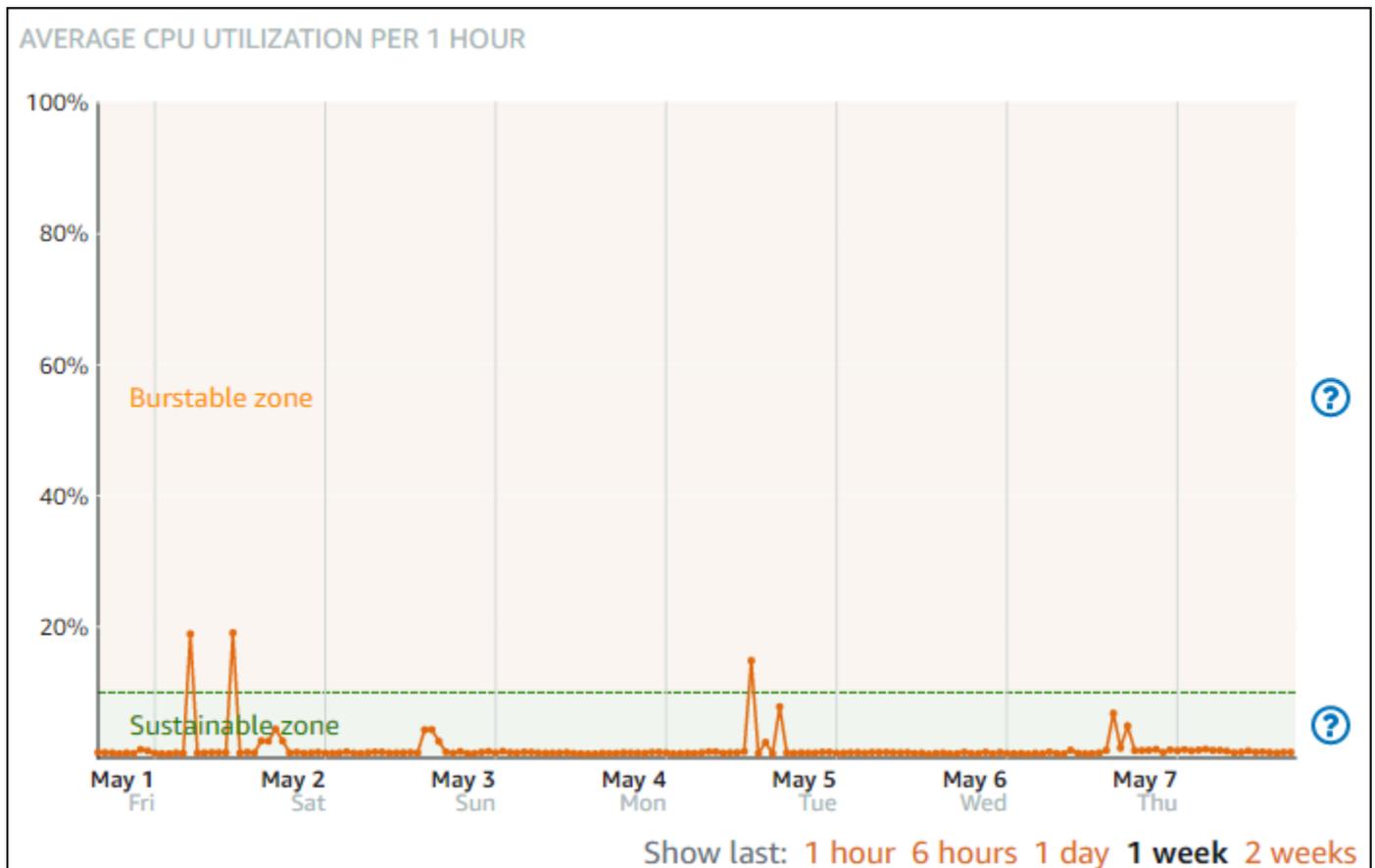


Lightsail 執行個體在啟動時會收到額外的CPU爆發容量，這稱為啟動CPU爆發容量。啟動CPU成組分解容量可讓執行個體在啟動後立即成組分解，再累積額外成組分解容量。啟動CPU爆發容量不計入爆發容量限制。如果您的執行個體尚未使用啟動CPU突發容量，而且在累積更多突發容量的同時仍處於閒置狀態，則其成CPU組分解容量 (百分比) 量度圖表將會顯示為 100% 以上。

此外，某些 Lightsail 實體會以啟動模式啟動，這會暫時移除部分高載執行個體通常存在的效能限制。啟動模式可讓您在啟動時執行耗用大量資源的指令碼，而不會影響執行個體的整體效能。

## 識別 Lightsail 實體爆發的時間

在執行個體的 CPU 使用率指標圖表上，您會看到永續區域和可高載區域。在下列 CPU 使用率指標圖表範例中，效能基準為 10%，因為執行個體使用 Linux 或 UNIX 為基礎的每月 7 美元/月執行個體計劃。



您的 Lightsail 執行個體可以在永續區域中無限期地運作，而不會影響您的系統運作。在重度負載下，例如編譯程式碼、安裝新軟體、執行批次任務或提供尖峰負載請求時，您的執行個體可能會開始在可高載區域中運作。在可高載區域中運作時，您的執行個體會耗用大量的 CPU 週期。因此，其只能於有限的時段內在此區域中運作。

執行個體可在可高載區域中運作的期間取決於其深入可高載區域的程度。相較於在可高載區域較高端運作的執行個體，在可高載區域較低端運作的執行個體可維持高載的期間比較長。不過，在可高載區域中任意處持續一段時間的執行個體最終會耗盡所有 CPU 容量，直到它再次在永續區域中運作為止。因此，同時監控剩餘的 CPU 高載容量非常重要，本指南的下一節將說明。

## 監控您的執行個體的 CPU 高載容量

Lightsail 主控台內的 CPU 概觀頁面會顯示執行個體的 CPU 使用率，與其可用的 CPU 高載容量相比。在以下的 CPU 概觀範例中，CPU 高載容量百分比已增加，因為執行個體在可永續區域的基準以下持續運作。



剩餘的 CPU 高載容量圖表檢視可在 CPU 高載容量百分比和分鐘之間切換。在高載區域中運作時，您的執行個體會耗用更多 CPU 高載容量。CPU 高載容量分鐘指標是您的執行個體以 100% CPU 使用率高載的可用時間量，在可高載區域中運作時，耗用的速率與執行個體目前 CPU 使用率百分比相同。例如，以 Linux 或 UNIX 為基礎的每月 7 美元執行個體的 CPU 使用率基準為 10%，每小時會累積 6 分鐘的 CPU 突發容量分鐘。因此，如果執行個體運作使用率為：

- 可高載區域中 100% CPU 使用率 60 分鐘，然後在該期間以 100% 的速率消耗 CPU 高載容量分鐘。執行個體耗用 60 分鐘的 CPU 高載容量，並累積 6 分鐘，因此共耗用 54 分鐘。
- 可高載區域中 50% CPU 使用率 60 分鐘，然後在該期間以 50% 的速率消耗 CPU 高載容量分鐘。執行個體耗用 30 分鐘的 CPU 高載容量，並累積 6 分鐘，因此共耗用 24 分鐘。

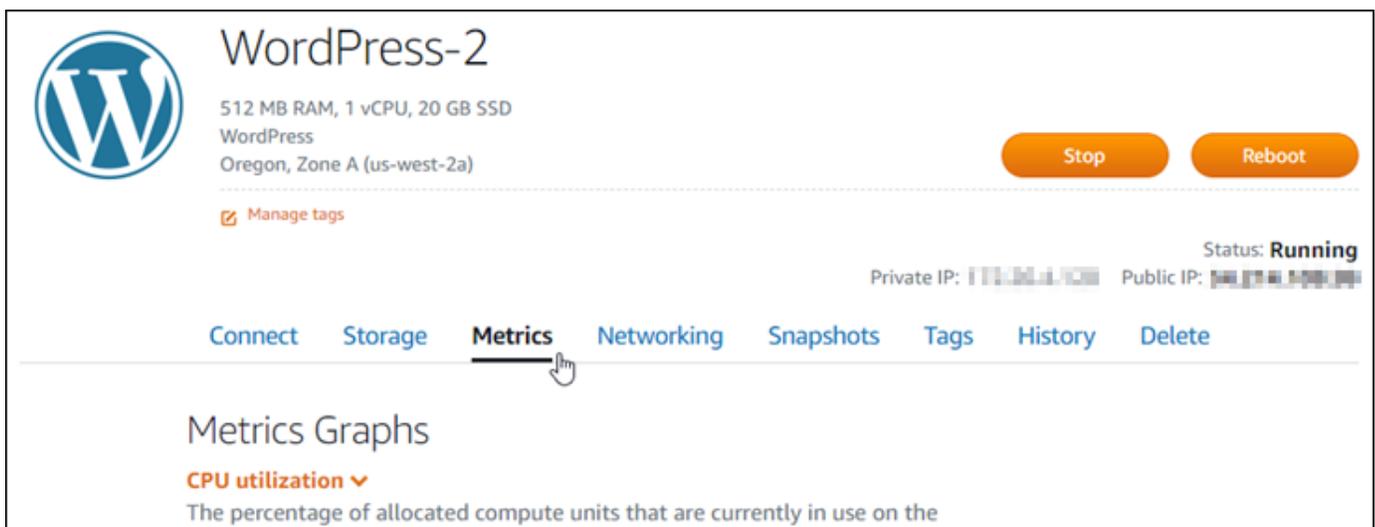
- 執行個體基準的 10% CPU 使用率 60 分鐘，然後在該期間以 10% 的速率消耗 CPU 高載容量分鐘。執行個體耗用 6 分鐘的 CPU 高載容量，並累積 6 分鐘。執行個體以基準運作時，CPU 高載容量分鐘不會增加或減少。
- 永續區域中 5% CPU 使用率 60 分鐘，然後在該期間以 5% 的速率消耗 CPU 高載容量分鐘。執行個體耗用 3 分鐘的 CPU 高載容量，並累積 6 分鐘，因此共累積 3 分鐘。

或者，如果執行個體已累積 60 分鐘的 CPU 高載容量，則它能夠以 100% 的 CPU 使用率運作 60 分鐘、50% 的 CPU 使用率運作 120 分鐘，或 25% 的 CPU 使用率運作 150 分鐘。

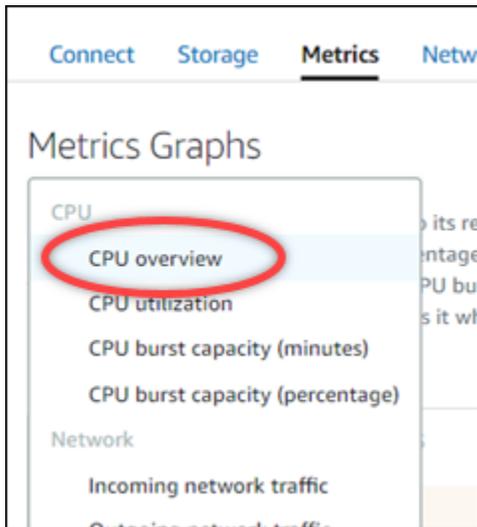
## 檢視 Lightsail 執行個體的 CPU 使用率和高載容量

請完成下列步驟以存取 CPU 概觀頁面，並檢視執行個體的 CPU 使用率和剩餘的成 CPU 組分解容量。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁上，選擇您要檢視其 CPU 使用率和爆發容量的執行個體名稱。
3. 選擇執行個體管理頁面上的 Metrics (指標) 標籤。



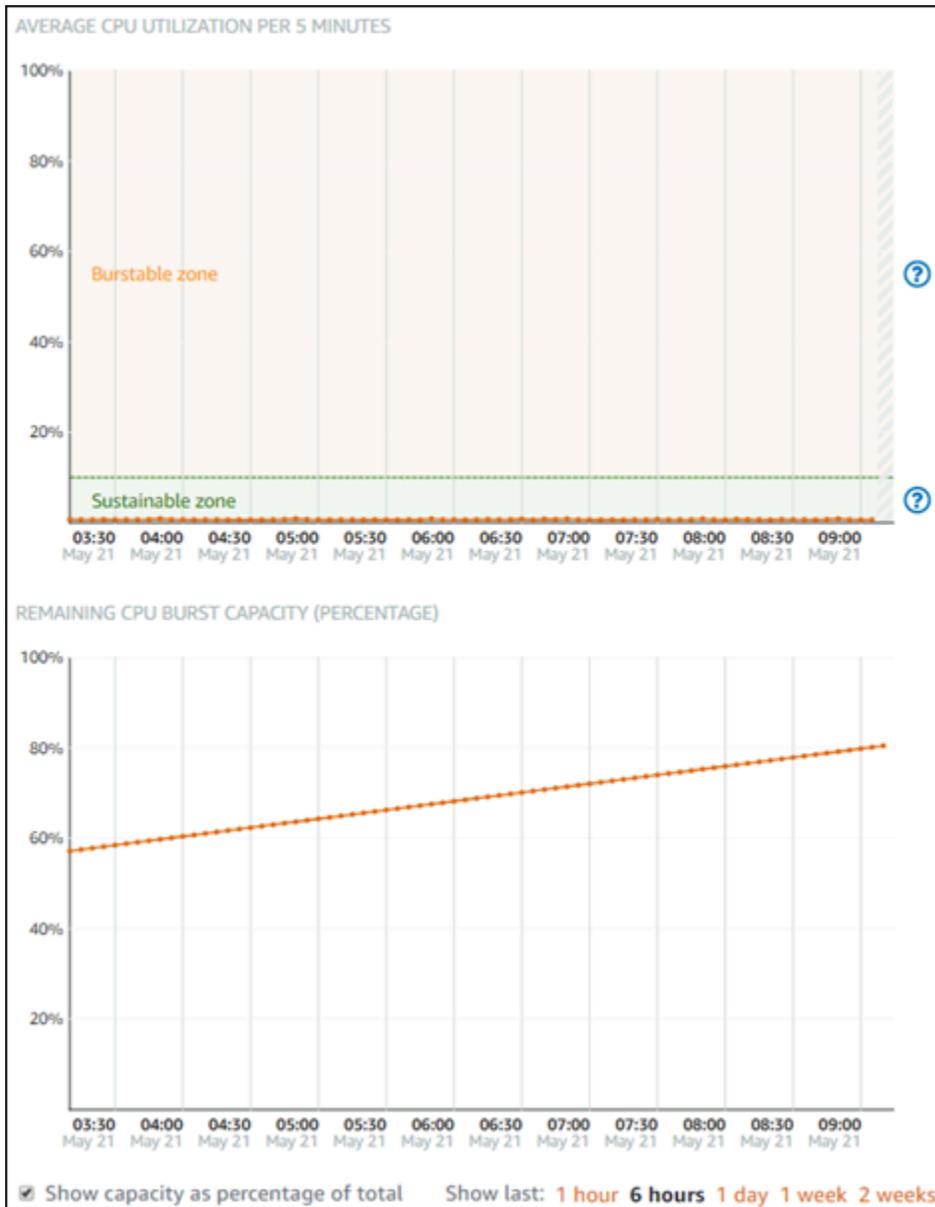
4. 在「量度」圖表標題下的下拉式功能表中選擇 CPU 概觀。



此頁面會顯示每 5 分鐘的平均CPU使用率和剩餘CPU成組分解容量圖表。

#### Note

建立執行個體後，剩餘CPU成組分解容量圖表可能會在短時間內顯示啟動模式區域。某些 Lightsail 實體會以啟動模式啟動，這會暫時移除部分高載執行個體通常存在的效能限制。啟動模式可讓您在啟動時執行耗用大量資源的指令碼，而不會影響執行個體的整體效能。



5. 您可以在指標圖表上執行下列動作：

- 針對高載容量圖表，選擇 Show capacity as percentage of total (以總計的百分比顯示容量)，將檢視從可用的高載容量分鐘變更為可用的高載容量百分比。
- 變更圖表的檢視，以顯示 1 小時、6 小時、1 天、1 週和 2 週的資料。
- 將游標暫停在資料點上，以檢視有關該資料點的詳細資訊。
- 新增警示，以在 CPU 使用率和突發容量超過您指定的閾值時收到通知。無法在 CPU 概述頁面中新增警報。您必須將它們新增至個別 CPU 使用率、CPU 成組分鐘容量百分比和 CPU 成組分鐘量度圖表頁面中。如需詳細資訊，請參閱 [警示](#) 和 [建立執行個體指標警示](#)。

## 疑難排解 Lightsail 執行個體的高 CPU 使用率

如果您的執行個體經常在高載區域運作或長時間運作，執行個體將會使用其所有的高載容量。這可能表示您的執行個體佈建不足。也可能是服務執行頻率太高，或者您的執行個體正執行不必要的軟體。

使用 Linux/Unix 執行個體上的 `top` 和 Windows Server 執行個體上的工作管理員等工具，調查導致您的執行個體高載的原因。這些工具會顯示正在耗用執行個體資源的服務。判斷哪些服務耗用最多的資源，並識別是否可以停用這些服務，而不會影響執行個體的工作負載。透過停用服務或解除安裝軟體，您應該能夠降低執行個體爆發的情況，並避免必須擴大執行個體的大小。

如果您的執行個體確實佈建不足，而且您無法降低其 CPU 使用率，則可以藉由增加更多處理能力來減輕高載容量消耗。您可以建立執行個體的快照，然後使用較大的 Lightsail 執行個體計劃，從快照建立新執行個體來達到這個目的。例如，在您的新執行個體上使用以 Linux 或 UNIX 為基礎的每月 24 美元計劃，而不是在上一個執行個體上使用的每月以 Linux 或 UNIX 為基礎的 \$12 美元計劃。當新執行個體啟動並執行時，請視需要變更工作負載的 DNS，以便將舊執行個體換成新執行個體。流量開始路由至新執行個體後，請刪除佈建不足的舊執行個體。如需詳細資訊，請參閱[快照](#)。

## Connect 並管理您的執行個體

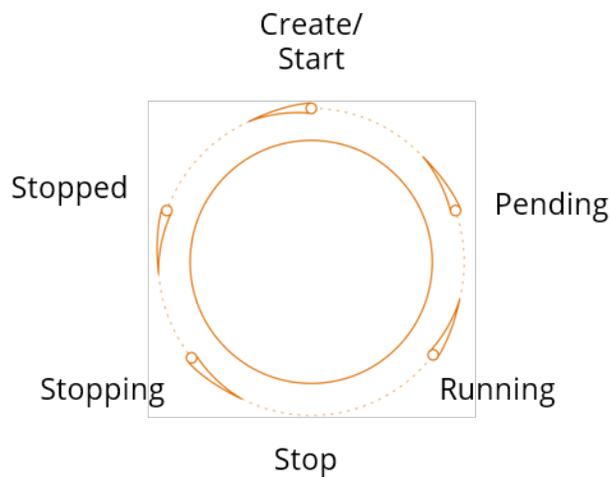
本指南涵蓋下列與管理和連接 Amazon Lightsail 執行個體相關的主題：

### 主題

- [啟動、停止或重新啟動您的 Lightsail 執行個體](#)
- [強制停止卡住 Lightsail 實例](#)
- [為 Amazon EC2 執行個體啟用增強型聯網](#)
- [在 Lightsail 中擴充 Windows 伺服器執行個體的檔案系統](#)
- [在 Lightsail 中使用啟動指令碼設定 Linux/Unix 執行個體](#)
- [使用 PowerShell 和批次指令碼設定視窗 Lightsail 執行個體](#)
- [保護 Windows 伺服器執行 Lightsail](#)

## 啟動、停止或重新啟動您的 Lightsail 執行個體

Amazon Lightsail 建立您的執行個體時，您的機器會在開始執行之前進入擱置中狀態。在您的執行個體執行之後，您可以將其重新啟動或停止，然後再重新啟動。該週期看起來像這樣：



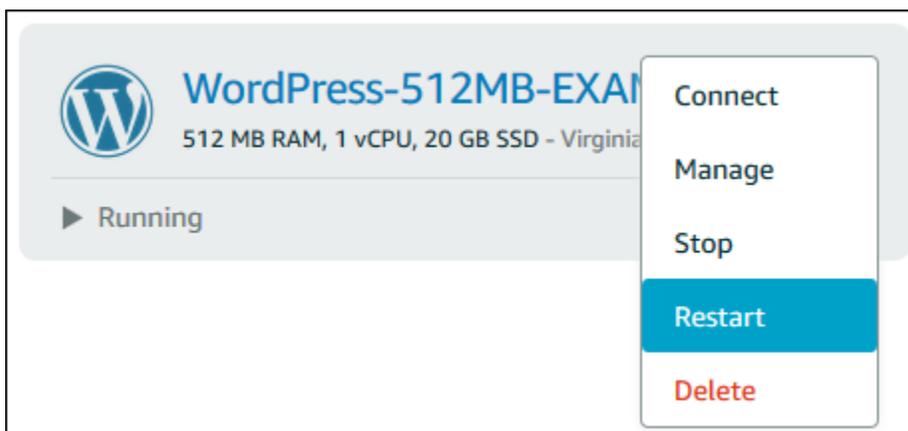
您可以在管理執行個體或在首頁上檢視執行個體時查看執行個體狀態。

#### **⚠ Important**

當您停止並啟動執行個體時，指派給執行個體的預設公用IPv4位址將會變更。您可以選擇性地建立靜態IPv4位址，並將其附加至執行個體。靜態IPv4位址會取代執行個體的預設公用IPv4位址，當您停止並啟動執行個體時，它會保持不變。如需詳細資訊，請參閱[建立靜態 IP 並將其附加至執行個體](#)。

## 在執行個體執行時將其重新啟動

- 在首頁選擇您要重新啟動的執行個體，或是從管理執行個體選單選擇 Restart (重新啟動)。



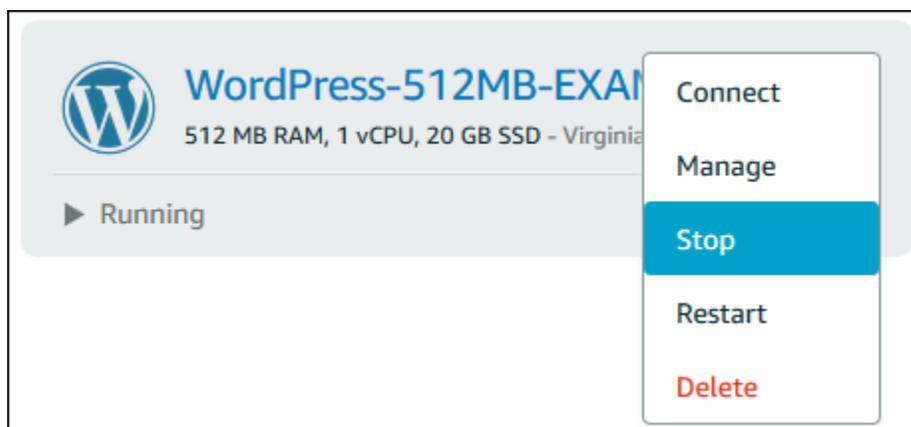
如果您是從執行個體管理頁面檢視您的執行個體，請選擇 Restart (重新啟動)，然後在提示出現時選擇 Confirm (確認)。

**Note**

若要 Restart (重新啟動) 您的執行個體，則它必須在 Running (執行中) 的狀態。

## 停止執行中的執行個體

- 在首頁選擇您要停止的執行個體，或是從管理執行個體選單選擇 Stop (停止)。



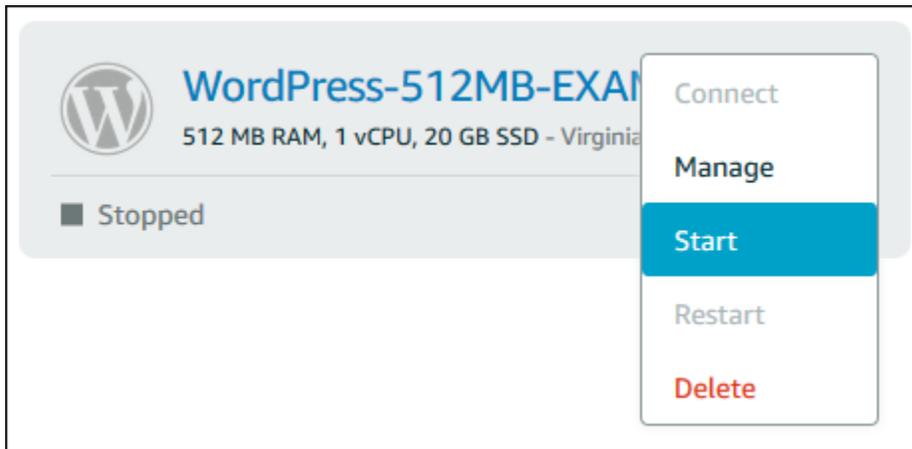
如果您是從執行個體管理頁面檢視您的執行個體，請選擇 Stop (停止)，然後在提示出現時選擇 Confirm (確認)。

**Note**

若要 Stop (停止) 您的執行個體，則它必須在 Running (執行中) 的狀態。

## 在執行個體停止之後將其啟動

- 在首頁選擇您要啟動的執行個體，或是從管理執行個體選單選擇 Start (啟動)。



如果您正在從執行個體管理頁面檢視執行個體，請選擇 Start (啟動)。

#### Note

若要 Start (啟動) 您的執行個體，則它必須在 Stopped (已停止) 的狀態。

## 強制停止卡住 Lightsail 實例

執行個體很少會卡在 Stopping 狀態。如果發生這種情況，託管 Amazon Lightsail 執行個體的基礎硬體可能會發生問題。在本指南中，您將學習如何強制停止卡在 stopping 狀態的執行個體。如需有關執行個體狀態的詳細資訊，請參閱[啟動、停止或重新啟動 Lightsail 執行個體](#)。

### 如何強制停止執行個體

您可以使用 Lightsail 主控台強制停止執行個體，但只有在執行個體處於stopping狀態時才能停止執行個體。或者，當執行個體處於 shutting-down 和 terminated 以外的任何狀態時，使用 AWS Command Line Interface (AWS CLI) 強制停止該執行個體。強制停止可能需要幾分鐘完成。如果執行個體在 10 分鐘後仍未停止，請再次強制停止。

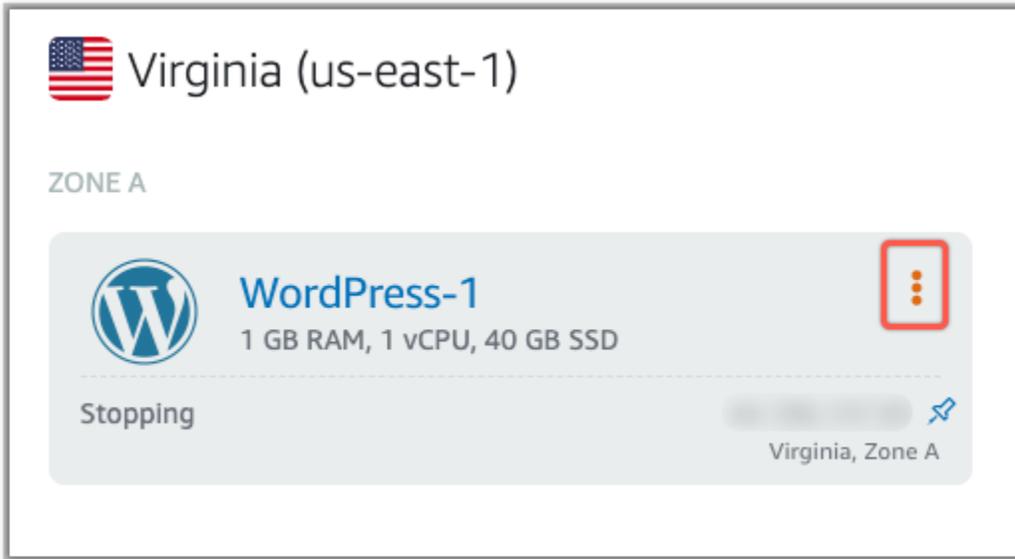
強制停止執行個體時，其沒有機會排清檔案系統快取或檔案系統中繼資料。強制停止執行個體之後，您應該執行檔案系統檢查和修復程序。

下列程序說明強制停止 Lightsail 實體的不同方式。

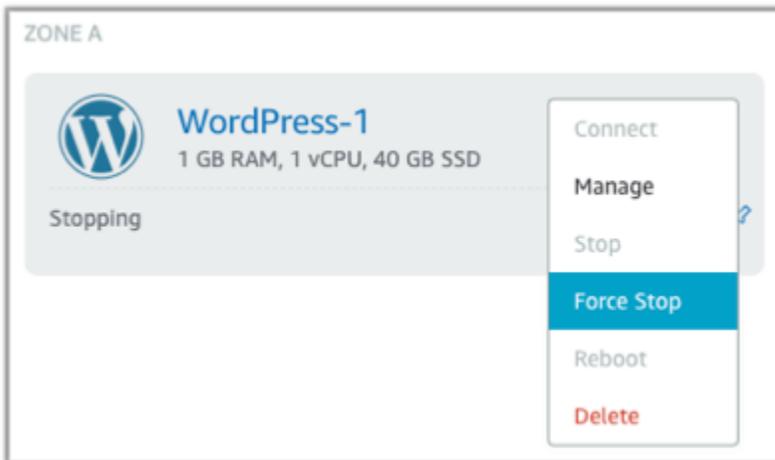
#### 強制停止 Lightsail 主控台內的執行個體

1. 登入主 [Lightsail 台](#)。
2. 選擇執行個體標籤。

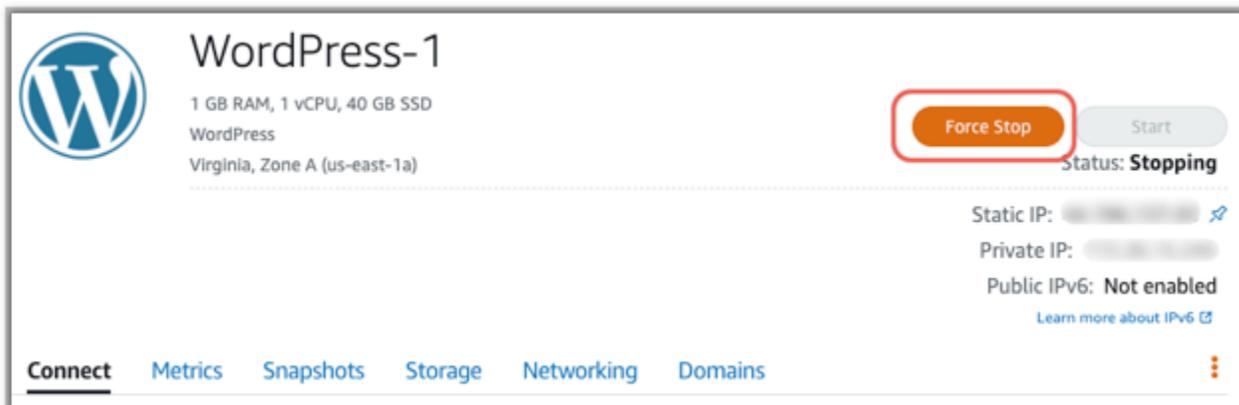
- 找出卡在 Stopping 狀態的執行個體。然後，選擇執行個體名稱旁邊顯示的動作功能表圖示 (⋮)。



- 在出現的下拉式清單中選擇強制停止。



或者，您也可以選擇執行個體名稱來存取執行個體管理頁面。然後，選擇強制停止按鈕。



## 強制停止執行個體 AWS CLI

1. 開始之前，需要安裝 AWS CLI。若要進一步了解，請參閱[安裝 AWS Command Line Interface](#)。請務必在安裝之後[設定 AWS CLI](#)。
2. 如下所示使用 `stop-instance` 命令和 `--force` 參數：

```
aws lightsail stop-instance --instance-name Wordpress-1 --force
```

## 為 Amazon EC2 執行個體啟用增強型聯網

某些 Lightsail 執行個體與目前一代 EC2 執行個體類型 (T3、M5、C5 或 R5) 不相容，因為這些執行個體並未啟用增強型聯網功能。如果來源 Lightsail 執行個體不相容，則從匯出的快照建立 EC2 執行個體時，您將需要選擇上一代執行個體類型 (T2、M4、C4 或 R4)。使用 Lightsail 主控台內的「建立 Amazon EC2 執行個體」頁面建立 EC2 執行個體時，會顯示這些執行個體類型選項。

### Note

如需有關增強型聯網的詳細資訊，請參閱 Amazon EC2 文件中的 [Linux 上的增強型聯網](#) 或 [Windows 上的增強型聯網](#)。

若要在來源 Lightsail 執行個體不相容時使用最新一代 EC2 執行個體類型，您需要使用上一代執行個體類型 (T2、M4、C4 或 R4) 建立新的 EC2 執行個體，更新執行個體上的聯網驅動程式，然後將執行個體升級為所需的目前世代執行個體類型。

### 必要條件

您必須從匯出的 Lightsail 快照建立 Amazon EC2 執行個體。如果您的 Lightsail 執行個體不相容，您將在建立 Amazon EC2 執行個體時選擇上一代執行個體類型 (T2、M4、C4 或 R4)。若要進一步了解，請參閱 [Lightsail 中的從匯出的快照建立 Amazon EC2 執行個體](#)。

新的 EC2 執行個體啟動和執行後，請繼續前往本指南的 [使用彈性網路轉接器啟用增強型聯網](#) 一節，以了解如何啟用增強型聯網。

### 使用彈性網路轉接器啟用增強型聯網

新的執行個體啟動和執行後，請參閱 Amazon EC2 文件中的以下指南，以使用彈性網路介面卡 (ENA) 增強聯網能力：

- [在 Linux 執行個體上使用 ENA 啟用增強型聯網](#)

- [在 Windows 執行個體上使用 ENA 啟用增強型聯網](#)

## 升級您的執行個體類型

啟用增強型聯網後，您可以依照以下其中一項指南的指示升級執行個體類型：

- 針對 Windows Server 執行個體 — [遷移至最新一代執行個體類型](#)
- 針對 Linux 或 Unix 執行個體 — [變更執行個體類型](#)

## 在 Lightsail 中擴充 Windows 伺服器執行個體的檔案系統

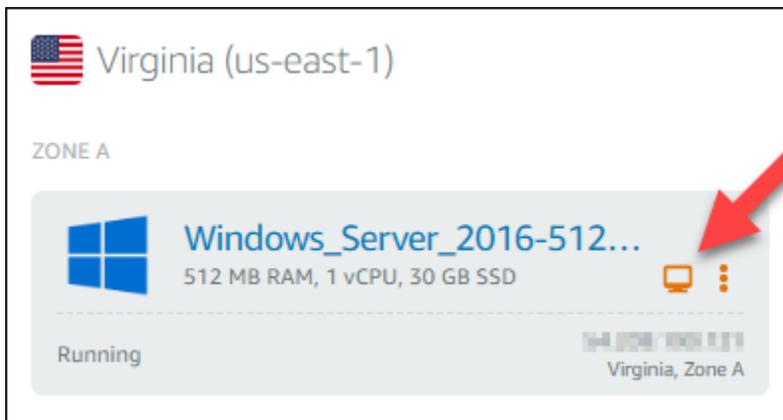
在您使用快照建立較大型方案的新 Windows Server 執行個體之後，您可能會看到可用儲存空間量低於方案指定的量。這通常是因為較大方案提供的額外儲存空間尚未配置；因此，作用中的磁碟區尚未使用到這部分的空間。此主題的步驟說明如何擴展 Windows Server 執行個體的檔案系統，以使用最大的可用儲存空間。

### Note

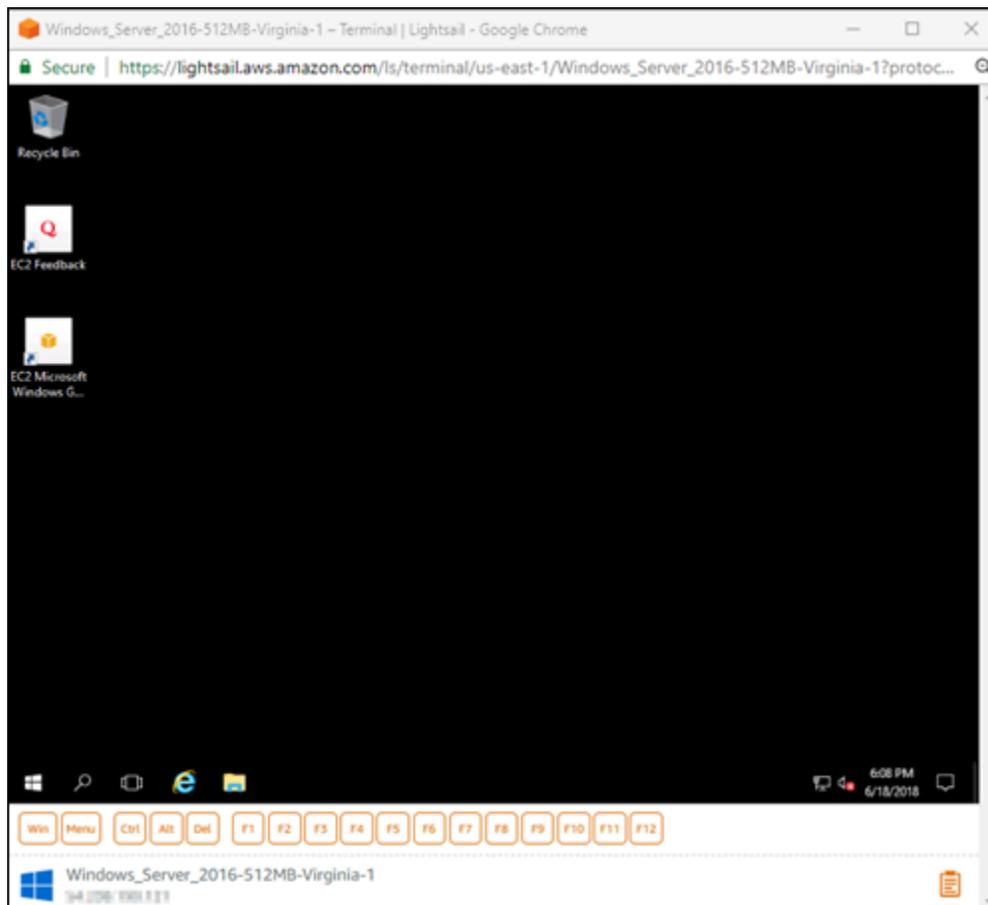
此案例只會發生在使用 (在執行系統準備 (Sysprep) 公用程式前建立的) 快照建立 Windows Server 執行個體時。如需詳細資訊，請參閱[建立 Windows Server 執行個體的快照](#)。

### 擴展 Windows Server 執行個體的檔案系統

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁上，選擇您要連線之執行個體的 RDP 用戶端圖示。

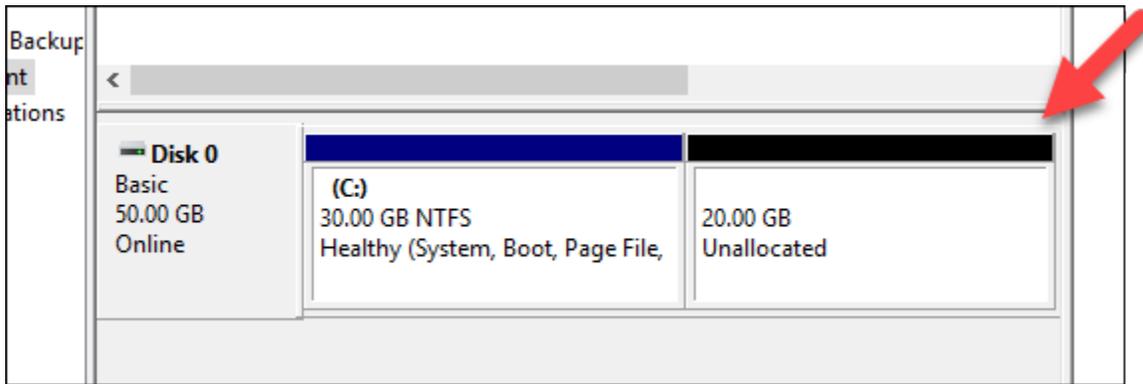


以瀏覽器為基礎的 RDP 用戶端視窗隨即開啟，如下列範例所示：

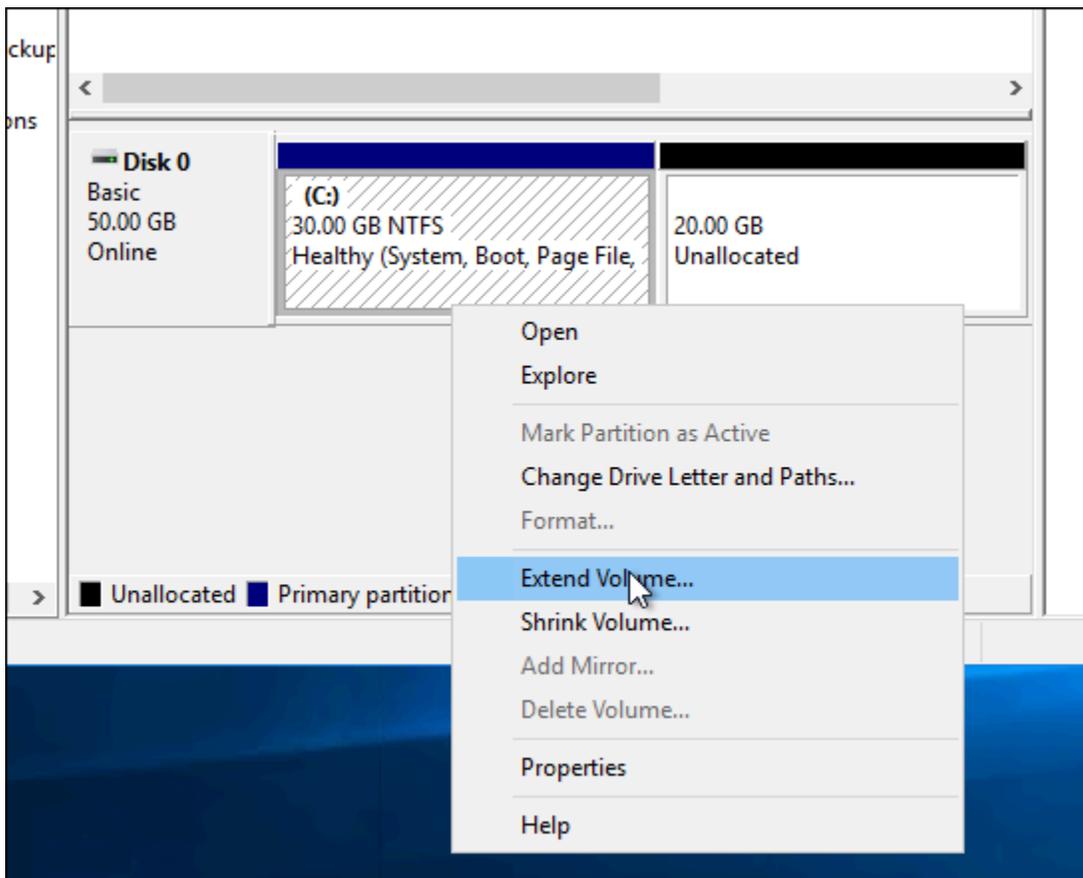


3. 選擇工作列上的 Windows 圖示，然後選擇以下其中一個選項：
  - 在視窗伺服器 2022、視窗伺服器 2019 和視窗伺服器 2016 執行個體上，選擇開始，然後選擇視窗系統管理工具。
4. 選擇 Computer Management (電腦管理)。
5. 在 Computer Management (電腦管理) 主控台的左側窗格中，選擇 Disk Management (磁碟管理)。
6. 在 Actions (動作) 選單上，選擇 Rescan Disks (重新掃描磁碟)。

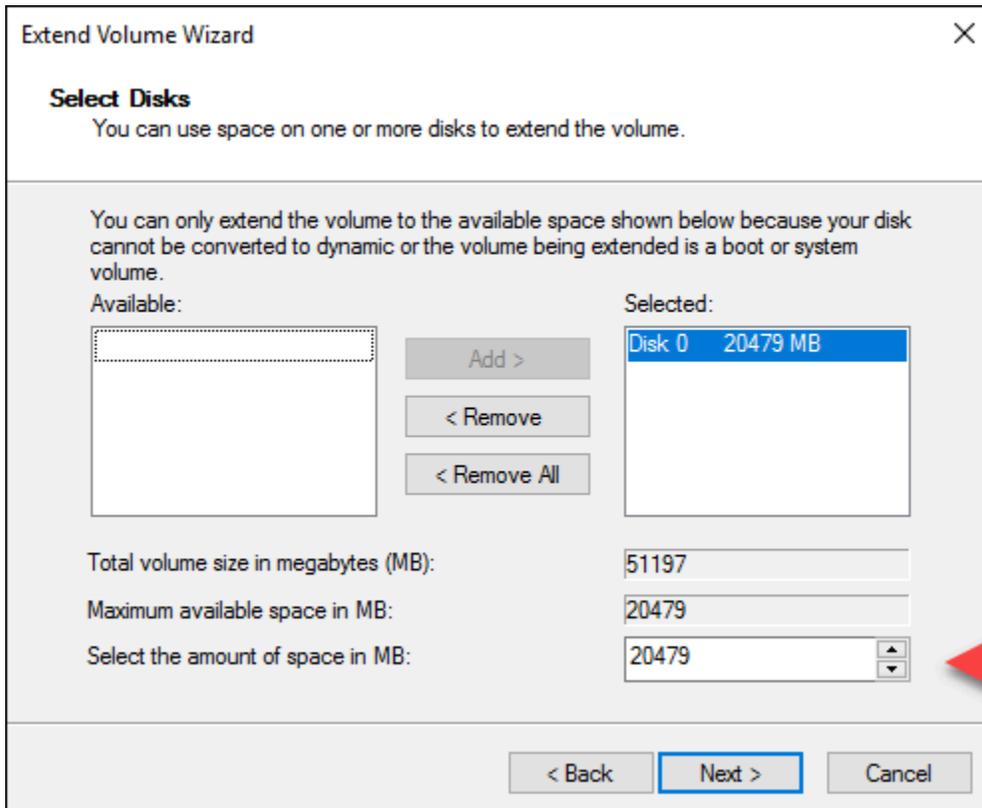
您可以查看磁碟的未配置空間。擴展磁碟的作用中磁碟區以使用未配置的空間。



7. 在與未配置空間相同磁碟的作用中磁碟區上按一下滑鼠右鍵，然後選擇 Extend Volume (擴展磁碟區)。

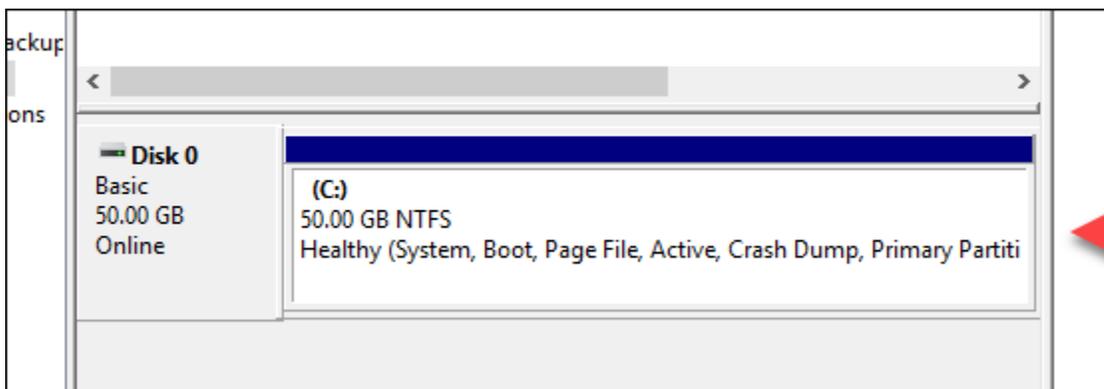


8. 當擴展磁碟區精靈開啟時，選擇 Next (下一步)。
9. 在 Select the amount of space in MB (選擇空間容量，以 MB 計) 欄位中輸入要擴展磁碟區的 MB 數。此值通常設定為最大的未配置空間。您輸入的值是您要新增的空間量，而非最終磁碟區大小。



## 10. 完成擴展磁碟區精靈。

作用中磁碟區將會擴展以使用您指定的未配置空間。下列範例顯示已選取的所有未配置空間。



## 在 Lightsail 中使用啟動指令碼設定 Linux/Unix 執行個體

建立 Linux 或 UNIX 執行個體時，您可以新增啟動指令碼來新增或更新軟體，或以其他方式設定執行個體。若要使用其他資料設定 Windows 型執行個體，請參閱[使用 Windows 設定新的 Lightsail 執行個體](#)。PowerShell

**Note**

根據您選擇的機器映像、命令來取得適合您執行個體的軟體。Amazon Linux 使用yum, 而 Debian 和 Ubuntu 都使用apt-get. WordPress 和其他應用程序映像使用 , apt-get因為它們將 Debian 作為其操作系統運行。免費BSD和開啟SUSE需要額外的使用者設定才能使用自訂工具, 例如freebsd-update或 zypper (openSUSE)。

## 範例：設定 Ubuntu 伺服器以安裝 Node.js

以下範例將更新套件清單, 然後透過 apt-get 命令安裝 Node.js。

1. 在 Create an instance (建立執行個體) 頁面, 在 OS Only (僅作業系統) 索引標籤上選擇 Ubuntu。
2. 向下捲動並選擇 Add launch script (新增啟動指令碼)。
3. 輸入下列內容：

```
# update package list
apt-get update -y
# install some of my favorite tools
apt-get install nodejs -y
```

**Note**

用來設定伺服器而傳送的命令會做為根執行, 因此命令前無須納入 sudo。

4. 選擇 建立執行個體。

## 範例：設定 WordPress 伺服器以下載並安裝外掛程式

下列範例會更新套件清單, 然後下載並安裝的 [BuddyPress 外掛程式](#) WordPress。

1. 在 [建立執行個體] 頁面上, 選擇WordPress。
2. 選擇 Add launch script (新增啟動指令碼)。
3. 輸入下列內容：

```
# update package list
apt-get update
# download wordpress plugin
```

```
wget "https://downloads.wordpress.org/plugin/buddypress.14.0.0.zip"  
apt-get install unzip  
# unzip into wordpress plugin directory  
unzip buddypress.14.0.0.zip -d /bitnami/wordpress/wp-content/plugins
```

#### 4. 選擇 建立執行個體。

## 使用 PowerShell 和批次指令碼設定視窗 Lightsail 執行個體

當您建立 Windows 型執行個體時，可以使用 Windows PowerShell 指令碼或任何其他批次指令碼加以設定。這是在您的執行個體啟動後執行的一次性指令碼。此主題顯示指令碼的語法，並提供範例以協助您快速上手。我們也說明如何執行測試指令碼以查看它是否成功執行。

### 建立啟動並執行 PowerShell 指令碼的執行個體

下列程序會在新執行個體啟動後，在其上安裝名為 chocolatey 的工具。

1. 在 Lightsail 首頁上，選擇「建立實體」。
2. 選擇您要在其中 AWS 區域 建立執行個體的可用區域。
3. 在 Select a platform (選擇平台) 下，選擇 Microsoft Windows。
4. 選擇僅限作業系統，然後選擇視窗伺服器 2022、視窗伺服器 2019、視窗伺服器 2016 年。
5. 選擇 Add launch script (新增啟動指令碼)。
6. 輸入下列內容：

```
<powershell>  
iex ((New-Object System.Net.WebClient).DownloadString('https://chocolatey.org/  
install.ps1'))  
</powershell>
```

#### Note

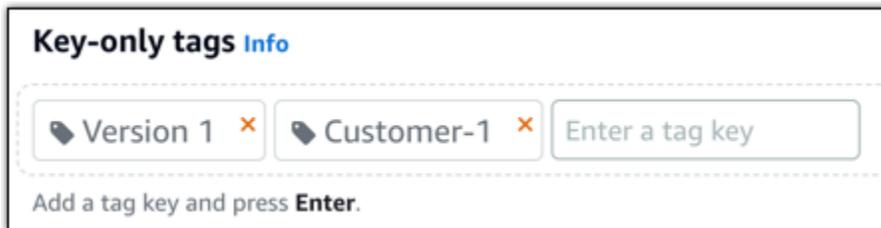
您必須始終將 PowerShell 腳本包裝在 `<powershell></powershell>` 標籤中。您可以使用標籤或不使用任何 `<script></script>` 標籤來輸入非 PowerShell 命令或批次指令碼。

7. 輸入您執行個體的名稱。

資源名稱：

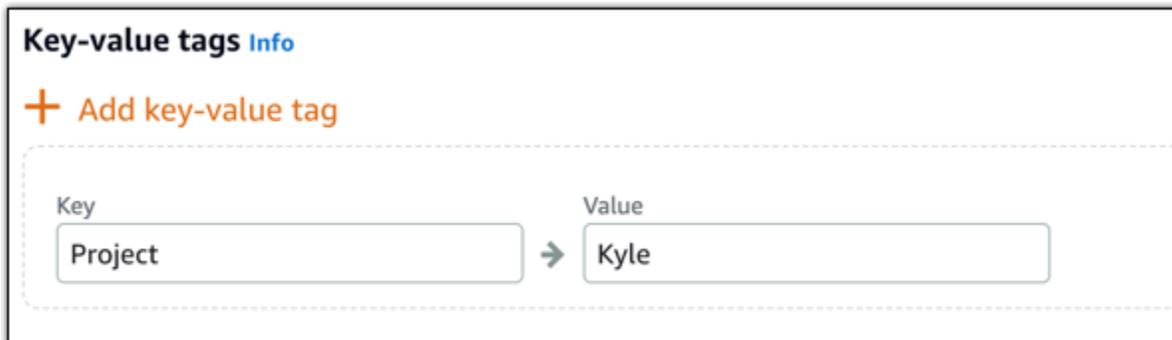
- 每個 Lightsail 帳戶 AWS 區域 中的每個項目都必須是唯一的。
  - 必須包含 2 至 255 個字元。
  - 開頭和結尾必須是英數字元或數字。
  - 可以包含英數字元、數字、句點、破折號和底線。
8. 選擇下列其中一個選項以新增標籤至您的執行個體：

- Add key-only tags (新增僅索引鍵標籤) 或 Edit key-only tags (編輯僅索引鍵標籤) (若標籤已新增)。在標籤索引鍵文字方塊中輸入新的標籤，接著按 Enter (輸入)。輸入標籤以新增之後，請選擇 Save (儲存)，如果不要新增則選擇 Cancel (取消)。



- Create a key-value tag (建立索引鍵值標籤)，接著將索引鍵輸入 Key (索引鍵) 文字方塊，將值輸入 Value (值) 文字方塊。完成輸入標籤後，請選擇 Save (儲存)，如果不要新增則選擇 Cancel (取消)。

鍵值標籤在儲存前一次只能新增一個。若要新增超過一個索引鍵值標籤，請重複之前的步驟。



#### Note

如需有關僅索引鍵和索引鍵值標籤的詳細資訊，請參閱[標籤](#)。

9. 選擇 建立執行個體。

## 驗證您的指令碼是否成功執行

您可以登入您的執行個體，以驗證指令碼是否成功執行。Windows 執行個體最多可能需要 15 分鐘的時間才能準備好接受 RDP 連線。準備就緒後，使用基於瀏覽器的 RDP 客戶端登錄或配置自己的 RDP 客戶端。如需詳細資訊，請參閱[連線至以 Windows 為基礎的執行個體](#)。

1. 一旦您可以連線到 Lightsail 執行個體，請開啟命令提示字元 (或開啟 Windows 檔案總管)。
2. 輸入下列命令以變更至 Log 目錄：

```
cd C:\ProgramData\Amazon\EC2-Windows\Launch\Log
```

3. 在文字編輯器中開啟 UserdataExecution.log，或輸入以下命令：`type UserdataExecution.log`。

您應該會在日誌檔案中看到以下內容。

```
2017/10/11 20:32:12Z: <powershell> tag was provided.. running powershell content
2017/10/11 20:32:13Z: Message: The output from user scripts: iex ((New-Object
System.Net.WebClient).DownloadString('https://chocolatey.org/install.ps1'))
2017/10/11 20:32:13Z: Userdata execution done
```

## 保護 Windows 伺服器執行 Lightsail

在本文中，我們提供了提示和技巧，以協助您在使用執行 Windows 伺服器的 Lightsail 執行個體時避免安全性風險。

### 關 Lightsail 碼

當您建立以 Windows 伺服器為基礎的執行個體時，Lightsail 會隨機產生一個難以猜測的長密碼。您可以唯一使用此密碼與您的新執行個體。您可以使用預設密碼，透過遠端桌面 (RDP) 快速連線至執行個體。您一律會在 Lightsail 執行個體上以管理員身分登入。

### 管理您的密碼

您可以在以 Windows Server 為基礎的執行個體上變更密碼。如果您想要使用遠端桌面用戶端存取 Lightsail 執行個體，這可能會很有用。Lightsail 永遠不會儲存您產生的密碼。

**Note**

您可以在 Lightsail 中使用 LightSail 產生的密碼或您自己的自訂密碼搭配瀏覽器型 RDP 用戶端。如果您使用自訂密碼，系統將會在您每次登入時提示您輸入您的密碼。如果您想要快速存取執行個體，可以更輕鬆地將 Lightsail 產生的預設密碼與瀏覽器型 RDP 用戶端搭配使用。

使用 Windows Server 密碼管理工具安全地變更您的密碼。按 `Ctrl + Alt + Del`，然後選擇 `Change a password` (變更密碼)。請務必保留您的密碼記錄，因為 Lightsail 不會儲存您的密碼。如果需要擷取密碼，請參閱下列內容：[變更以 Windows 為基礎的執行個體的管理員密碼](#)。

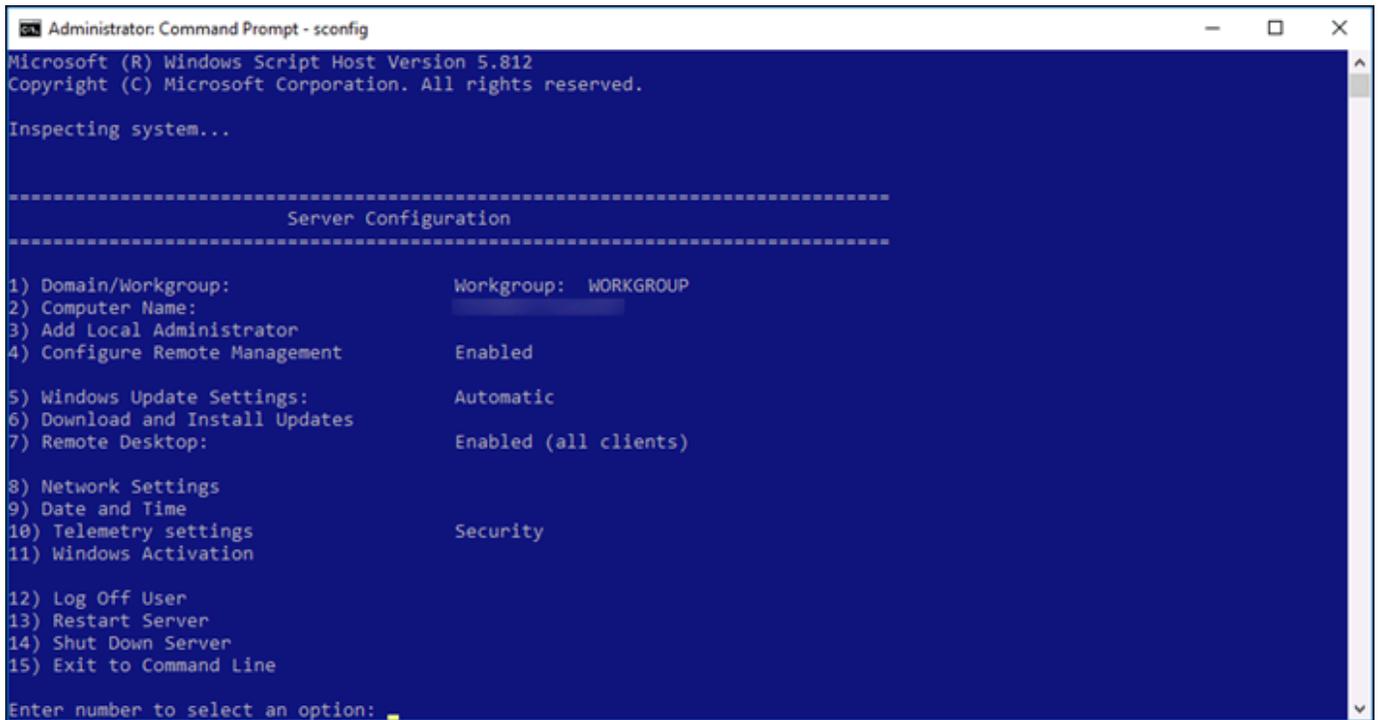
如果您要變更此唯一的預設密碼，請務必使用強式密碼。您應該避免使用姓名、字典字詞或重複的字元序列來設定密碼。

## 安全性修補程式

建議您使用最新的安全性修補程式，讓您的 Windows 伺服器型 Lightsail 執行個體更新。請確定您的伺服器已設定為下載並安裝更新。下列程序會告訴您如何直接在執行 Windows 伺服器的 Lightsail 執行個體上執行這項操作。

1. 在您以 Windows Server 為基礎的執行個體上開啟命令提示字元。
2. 輸入 `sconfig`，然後按 `Enter`。

預設的 Windows 更新設定 (第 5 項) 為 `Automatic`。

A screenshot of a Windows Command Prompt window titled "Administrator: Command Prompt - sconfig". The window displays the output of the "Server Configuration" tool. The text is as follows:

```
Microsoft (R) Windows Script Host Version 5.812
Copyright (C) Microsoft Corporation. All rights reserved.

Inspecting system...

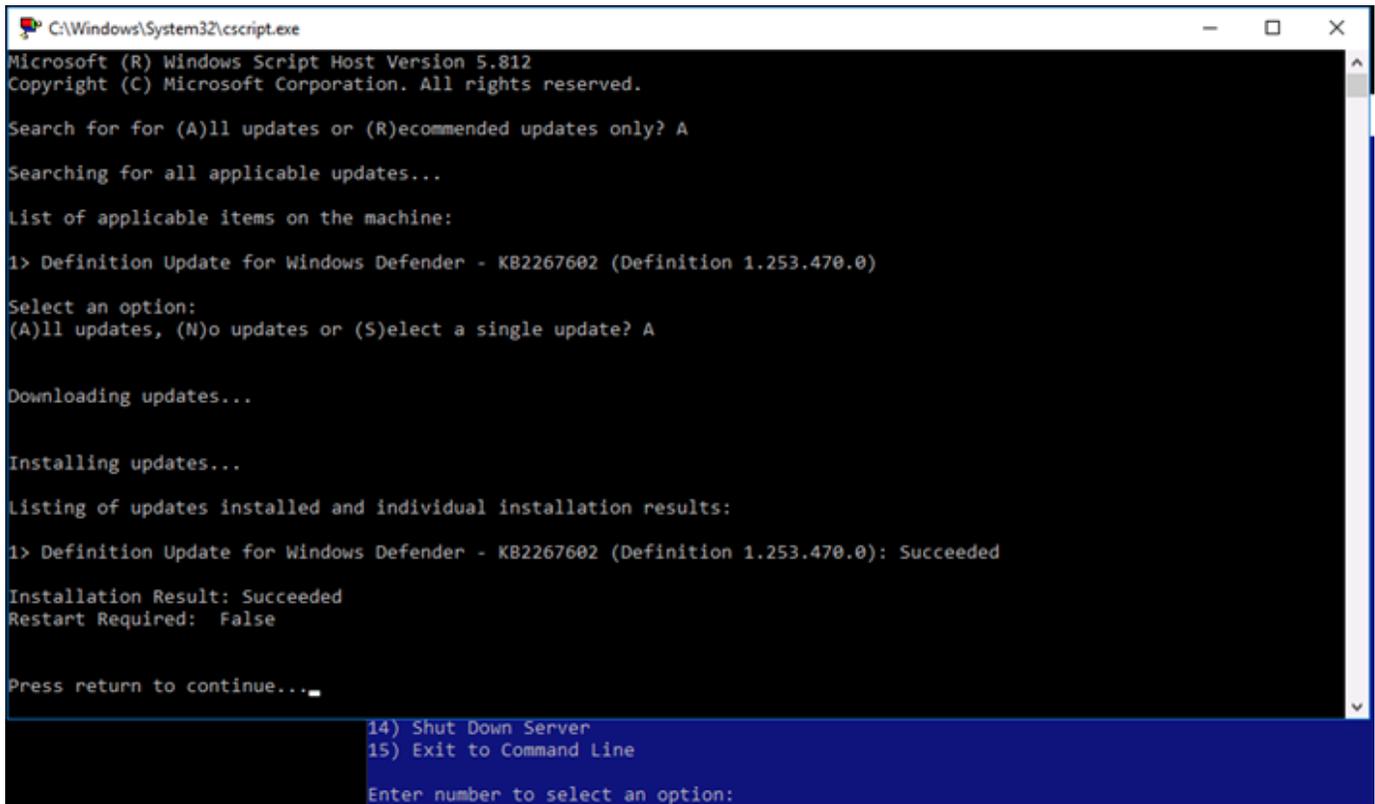
-----
                        Server Configuration
-----

1) Domain/Workgroup:                Workgroup: WORKGROUP
2) Computer Name:
3) Add Local Administrator
4) Configure Remote Management      Enabled
5) Windows Update Settings:        Automatic
6) Download and Install Updates
7) Remote Desktop:                  Enabled (all clients)
8) Network Settings
9) Date and Time
10) Telemetry settings              Security
11) Windows Activation
12) Log Off User
13) Restart Server
14) Shut Down Server
15) Exit to Command Line

Enter number to select an option: _
```

3. 若要下載並安裝新的更新，請輸入 6，然後按下 Enter。
4. 在新的命令視窗中輸入 A 來搜尋 (A)ll updates (全部更新)，然後按下 Enter。
5. 再次輸入 A 以安裝 (A)ll updates (全部更新)，然後按下 Enter。

完成後，您會看到包含安裝結果和更多指示的訊息 (如果適用)。



```
C:\Windows\System32\cmd.exe
Microsoft (R) Windows Script Host Version 5.812
Copyright (C) Microsoft Corporation. All rights reserved.

Search for for (A)ll updates or (R)ecommended updates only? A
Searching for all applicable updates...

List of applicable items on the machine:
1> Definition Update for Windows Defender - KB2267602 (Definition 1.253.470.0)

Select an option:
(A)ll updates, (N)o updates or (S)elect a single update? A

Downloading updates...

Installing updates...

Listing of updates installed and individual installation results:
1> Definition Update for Windows Defender - KB2267602 (Definition 1.253.470.0): Succeeded

Installation Result: Succeeded
Restart Required: False

Press return to continue...

14) Shut Down Server
15) Exit to Command Line
Enter number to select an option:
```

## 在 Windows Server 中啟用帳戶鎖定政策

您可以設定 Windows Server 在嘗試登入失敗達到特定次數時，暫時或無限期停用帳戶。例如，您可以鎖定使用三個錯誤密碼嘗試登入執行個體的使用者。

如需詳細資訊，請參閱 Windows Server 文件中的[帳戶鎖定政策](#)。

## 連接埠和防火牆設定

在預設情況下，我們會在以 Windows Server 為基礎的執行個體上開放以下連接埠。

## Firewall ?

You can control which ports on this instance accept connections.

Application	Protocol	Port range
SSH	TCP	22
HTTP	TCP	80
RDP	TCP	3389

[+ Add another](#) [Edit rules](#) 

您啟用的連接埠將向全世界公開，而且無法依據來源 IP 施加限制。若要限制存取您的執行個體，您可以關閉這些連接埠，而且只在您需要存取執行個體時才啟用這些連接埠。方法如下：

1. 在 Lightsail 中尋找您要管理的實體，然後選擇 [管理]。
2. 選擇 Networking (聯網)。
3. 在您執行個體的 Networking (聯網) 頁面上，選擇 Edit rules (編輯規則)。
4. 選擇規則旁邊的橘色「X」，以刪除 RDP/TCP/3389 規則。

## Firewall ?

You can control which ports on this instance accept connections.

Application	Protocol	Port range	
HTTP	TCP	80	
RDP	TCP	3389	

[+ Add another](#) [Cancel](#)  [Save](#) 

5. 選擇 Save (儲存)。

遵循 step-by-step 指示瞭解如何控制執行個體的狀態、強制停止卡住的執行個體、更新增強型聯網的執行個體、擴充 Windows Server 執行個體的檔案系統、使用指令碼在啟動時設定執行個體，以及保護 Windows Server 執行個體的安全。

本指南涵蓋 Linux 或 Unix 及 Windows Server 執行個體，提供安裝軟體、更新組態、管理密碼、啟用安全性修補程式及設定防火牆設定等工作的秘訣與最佳作法。遵循本指南，您可以有效地管理和保護 Lightsail 執行個體，確保針對特定使用案例提供最佳效能、安全性和自訂功能。

## 刪 Lightsail 體

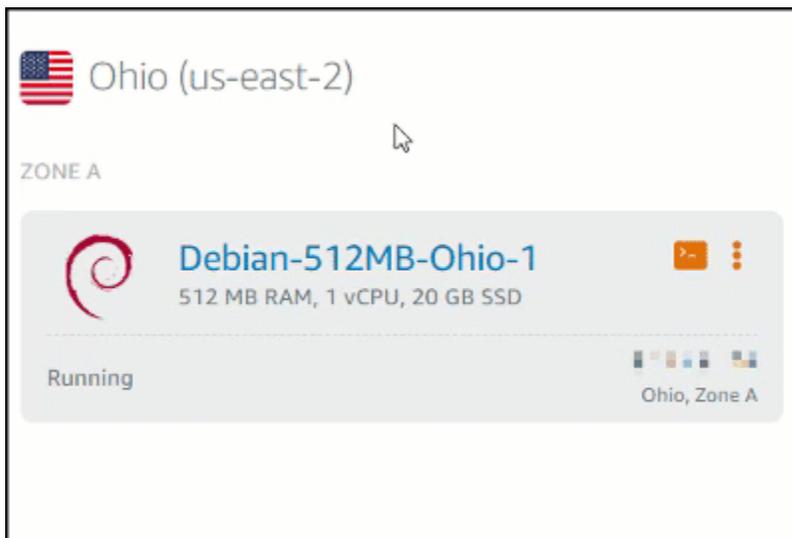
如果您不再需要執行個體，可以使用 Amazon Lightsail 主控台或 AWS Command Line Interface (AWS CLI) 將其刪除。一旦刪除執行個體後，您即無須再支付其費用。不過，附加至已刪除執行個體的資源 (例如靜態IPs和快照) 會繼續產生費用，直到您刪除它們為止。

### Note

已刪除的執行個體無法復原。如果您之後可能會需要執行個體中的資料，請先建立執行個體快照，再進行刪除。如需詳細資訊，請參閱[建立 Linux 或 Unix 執行個體的快照](#)或[建立 Windows Server 執行個體的快照](#)。

## 從 Lightsail 主控台首頁刪除執行個體

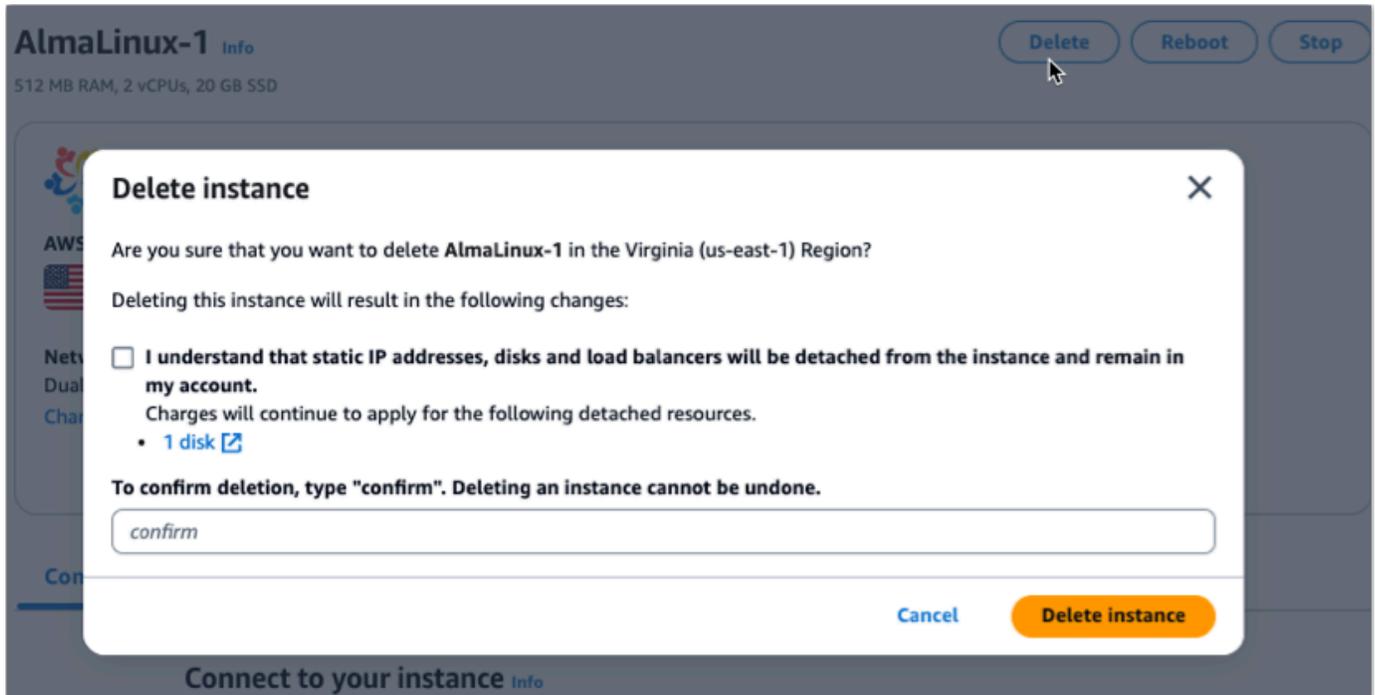
1. 登入主 [Lightsail 台](#)。
2. 針對您要刪除的執行個體，選擇操作功能表圖示 (:)，然後選擇 Delete (刪除)。



3. 選擇 Yes, Delete (是，刪除) 以確認刪除。

## 從 Lightsail 主控台執行個體管理頁面刪除執行個體

1. 在首頁的 Lightsail 主控台中，選擇您要刪除的實體。
2. 選擇「刪除」按鈕，然後選擇「刪除實例」。



3. 選取核取方塊，然後在輸入欄位中輸入「確認」，以確認您要刪除執行個體。
4. 選擇刪除執行個體以確認刪除。

## 使用刪除執行個體 AWS CLI

1. 如果您尚未完成以下必要條件。
  - a. 安裝 AWS CLI. 如需詳細資訊，請參閱[安裝 AWS CLI](#)。
  - b. 設定 AWS CLI. 如需詳細資訊，請參閱[設定 AWS CLI](#)。
  - c. (選擇性) 使用 AWS CloudShell. 如需詳細資訊，請參閱[???](#)。
2. 開啟 [終端機]、[命令提示字元] 或 CloudShell 視窗，然後輸入下列命令以取得您要刪除的執行個體名稱：

```
aws lightsail get-instances
```

您應該會看到類似下列的結果：

```
C:\>aws lightsail get-instance --instance-name Ubuntu-512MB-Ohio-1
{
  "instance": {
    "username": "ubuntu",
    "isStaticIp": false,
    "networking": {
      "monthlyTransfer": {
        "gbPerMonthAllocated": 1024
      },
      "ports": [
        {
          "protocol": "tcp",
          "accessType": "public",
          "commonName": "",
          "accessFrom": "Anywhere (0.0.0.0/0)",
          "fromPort": 80,
          "accessDirection": "inbound",
          "toPort": 80
        },
        {
          "protocol": "tcp",
          "accessType": "public",
          "commonName": "",
          "accessFrom": "Anywhere (0.0.0.0/0)",
          "fromPort": 22,
          "accessDirection": "inbound",
          "toPort": 22
        }
      ]
    },
    "name": "Ubuntu-512MB-Ohio-1",
    "resourceType": "Instance",
    "supportCode": "LIGHTSAILING-1-854-4094-184066",
    "blueprintName": "Ubuntu",
    "hardware": {
      "cpuCount": 1,
```

3. 選取和複製您要刪除之執行個體的名稱，以便於下一步驟使用。

**Note**

如果您要刪除的執行個體沒有出現，請確認您的執行 AWS CLI 個體已設定為執行個體所 AWS 區域 在的位置。如需詳細資訊，請參閱[設定 AWS CLI](#)。

4. 輸入下列命令以刪除執行個體。

```
aws lightsail delete-instance --instance-name InstanceName
```

在命令中，替換 *InstanceName* 使用實例的名稱。

如果刪除成功，您應該會看到類似以下的確認：

```
C:\>aws lightsail delete-instance --instance-name Ubuntu-512MB-Ohio-1
{
  "operations": [
    {
      "status": "Succeeded",
      "resourceType": "Instance",
      "isTerminal": true,
      "statusChangedAt": 1527202978.962,
      "location": {
        "availabilityZone": "us-east-2a",
        "regionName": "us-east-2"
      },
      "operationType": "DeleteInstance",
      "resourceName": "Ubuntu-512MB-Ohio-1",
      "id": "aws-lightsail-7927-4-699-0278-031202116618",
      "createdAt": 1527202978.962
    }
  ]
}
```

#### Note

如果刪除失敗，您應該會看到錯誤訊息。確認您的複製並貼上的執行個體名稱無誤，然後再試一次。

## 後續步驟

刪除執行個體後，與執行個體相關聯的靜態 IP、快照、區塊儲存磁碟和負載平衡器會保留在 Lightsail 中，並產生額外費用。如需有關如何刪除這些資源的詳細資訊，請參閱以下文章：

- [刪除靜態 IP](#)
- [刪除快照](#)
- [分離和刪除區塊儲存磁碟](#)
- [刪除負載平衡器](#)

## 管理SSH金鑰配對並連線至您的 Lightsail 執行個體

key pair 是一組安全登入資料，可在連線至 Amazon Lightsail 執行個體時用來證明您的身分。金鑰對包含公有金鑰和私有金鑰。Lightsail 會將公開金鑰儲存在您的執行個體上，而您也會儲存私密金鑰。

金鑰對檔案包含下列文字：

```

Example public key file text:
-----BEGIN PUBLIC KEY-----
AAAAB3NEXAMPLEAAAAAQABAAQDQsF85afw9ctz6maFF1c+1ZmTAFW0N5a+9nVvWkLLeO
R00Zn7XuTc6T0MS/ouPg45h2w07L+5hN01+jgINTknanFk1dE0KANPLEce4OnD0q915TT55
4106o/71kfEh110YFQnKt10v04EKANPLEce0hah5n;01E5E;7Kj;ai+00070dypFUI0Wv
zqBp1tU1d8L1yX7UFFEVL11v0T02h30yTL01e9p9tKk/VWqF0q4ggQqZYfXc3neKk
STFT0d;21Ytp06dXVv+ec2z2pE2EKANPLEK0R664F9pcvYh;D0;7UfuhBqXp/M0;3m
81THC/ha/LNEKANPLELq7L;2BakE05EcoybaNwhR0wF7H50h+;iJ7v1hPzKcEw43;FzNQ
81LmL1q0M1/83j0c9+M/0e4p9qC1T3TmupK0/;2eN240he9DTJEXANPLEQ/kmKtdzXm0
L2mk0e6qgAV0t29/acL0Kc
-----

Example private key file text:
-----BEGIN OPENSSH PRIVATE KEY-----
b3B1bnNaZc1ZkKt4jEAAAAmF1c1Ih1JdHIAAAAGNyeXk0AAAAAQAAB3NEXAMPLEce4OnD0q915TT55
y5nuhNLe7e+q4EAKANPLEAAAGNAAAB3NzAc1yc2EAAAADQABAAQDQsF85afw9ctz6maFF1c
51z6maFF1c+1ZmTAFW0N5a+9nVvWkLLeO00Zm7XuTc6T0MS/ouPg45h2w07L+5hN01
0MTF0eabMk1dE0KANPLEce4OnD0q915TT554106o/71kfEh110YFQnKt10v04EKANPLELq
7L;2BakE05EcoybaNwhR0wF7H50h+;iJ7v1hPzKcEw43;FzNQ81LmL1q0M1/83j0c9+M/0e4p9qC1T3TmupK0/;2eN240he9DTJEXANPLEQ/kmKtdzXm0L2mk0e6qgAV0t29/acL0Kc
-----

```

在 Linux 和 Unix 執行個體上，私密金鑰可讓您建立與執行個體的安全SSH連線。在 Windows 執行個體上，私密金鑰會解密您用來建立執行個體之安全RDP連線的預設管理員密碼。

任何具有您私有金鑰存取權的人都可以連線到您的執行個體，因此請務必將私有金鑰存放在安全的位置。

### 內容

- [選擇金鑰對選項](#)
- [連線到您的執行個體](#)
- [管理執行個體上儲存的金鑰](#)

## 選擇金鑰對選項

您可以在建立 Lightsail 實體時，選擇下列其中一個 key pair 選項。Windows 執行個體一律會使用預設金鑰；因此，您無法在建立 Windows 執行個體時建立金鑰對或上傳金鑰。

- 預設 key pair — Lightsail 會在您建立執行個體的每個 AWS 區域 位置自動建立預設 key pair。當您將預設金鑰組與執行個體搭配使用時，Lightsail 會將公開金鑰儲存在您的執行個體上。您可以隨時從 Lightsail 主控台的「帳戶」頁面下載預設 key pair 的私密金鑰。每個金鑰組最多可以有一個預設 key pair AWS 區域。
- 建立 key pair (Linux 和 Unix 執行個體) — 您可以使用 Lightsail 主控台建立新的自訂 key pair，以便與執行個體搭配使用。建立自訂 key pair 時，您會為其指定唯一名稱，而 Lightsail 會將公開金鑰儲存在您的執行個體上。只有在首次建立自訂金鑰對時，才能下載自訂金鑰對的私有金鑰。

- 上傳金鑰 (Linux 和 Unix 執行個體) — 若要使用您自己的現有 key pair，您可以將公開金鑰上傳至 Lightsail。當您上傳要搭配執行個體使用的公開金鑰時，您會為其指定唯一名稱，而 Lightsail 會將其儲存在您的執行個體中。您要保留並存放金鑰對的私有金鑰。

如果您在多個執行個體上設定單一公有金鑰，則可以使用金鑰對的相同私有金鑰連接到那些執行個體。如需有關管理金鑰配對的詳細資訊，請參閱[在 Amazon Lightsail 中管理金鑰配對](#)。

## 連線至您的執行個體

您可以使用下列其中一個選項連線至 Lightsail 執行個體。

### Lightsail 瀏覽器SSH和客戶 RDP

在 Lightsail 主控台中，您可以使用以瀏覽器為基礎的用戶端立即連線到 Linux 和 Unix 執行個體，並使用以瀏覽器為基礎的SSH用戶端連線至 Windows 執行個體。RDP當您使用瀏覽器型用戶SSH端連線至執行個體時，您不需要在電腦上安裝用戶端、設定金鑰配對或指定管理員密碼。這是連接到執行個體的最快方式。如需詳細資訊，請參閱[在 Amazon Lightsail 中連接到 Linux 或 Unix 執行個體](#)和[在 Amazon Lightsail 中連接到 Windows 執行個體](#)。

瀏覽器型用戶端使用的金鑰對與您建立執行個體時設定的金鑰對不同，例如預設金鑰或您建立或上傳的金鑰。因此，即使您刪除或遺失最初設定的金鑰其中之一，您也可以使用瀏覽器型用戶端繼續連接到您的執行個體。

### 第三方SSH和RDP客戶

您可以使用協力廠商用SSH用戶端連線至 Linux 和 Unix 執行個體，並使用協力廠商用RDP用戶端連線至 Windows 執行個體。使用SSH用戶端時，您必須將其設定為使用您在執行個體上設定之 key pair 的私密金鑰。使用RDP用戶端時，您必須指定 Windows 執行個體的管理員密碼。

如果您在本機使用 Windows 電腦，您可以使用下列用戶端連線至您的 Lightsail 執行個體。

- 普 TTY — 使用 Pu 連線TTY至 Linux 或 Unix 執行個體，使用SSH。如需詳細資訊，請參閱將 [Pu 設定為連線TTY至執行個體](#)。
- 遠端桌面連線 — 使用遠端桌面連線用戶端連線至使用的 Windows 執行個體RDP。如需詳細資訊，請參閱[使用 Windows 電腦上的遠端桌面連線用戶端連線至 Windows 執行個體](#)。

如果您在本機使用 Mac 電腦，請使用下列用戶端連線至 Lightsail 執行個體。

- 終SSH端機中的原生用戶端 — 使用終SSH端機中的原生用戶端連線至 Linux 和 Unix 執行個體。如需詳細資訊，請參閱[SSH在終端機中使用 Connect 到 Linux 或 Unix 執行個體](#)。

- Microsoft 遠端桌面 — 使用適用於 macOS 的 Microsoft 遠端桌面用戶端，以連接到 Windows 執行個體 RDP。如需詳細資訊，請參閱[使用 Mac 上的 Microsoft 遠端桌面用戶端連接至 Windows 執行個體](#)。

## 管理執行個體上儲存的金鑰

執行個體開始運作後，您就可以將新的金鑰新增至執行個體，或取代您最初指派給執行個體的金鑰。例如：您組織中的使用者如需使用不同的金鑰來存取執行個體，您可以將該金鑰新增至執行個體。另一個範例可能是有人離開您的組織，而他們擁有私密金鑰的副本 (. PEM) 檔案。您可以透過以全新金鑰取代此金鑰，或徹底移除此金鑰的方式，來防止連接到您的執行個體。如需詳細資訊，請參閱[在 Amazon Lightsail 中管理存放在執行個體上的金鑰](#)。

### 主題

- [設定適用於 Lightsail 的 SSH 按鍵](#)
- [使用 Lightsail 安全殼層金鑰控制安全執行個體](#)
- [管理安全殼層金鑰](#)
- [Connect 到 Linux 或 Unix 執行 Lightsail](#)
- [使用 Connect 至 Lightsail 執行個體 RDP](#)
- [使用管理 Lightsail 資源 AWS CloudShell](#)

## 設定適用於 Lightsail 的 SSH 按鍵

Secure Shell (SSH) 是一種安全連線至虛擬私有伺服器 (或 Lightsail 執行個體) 的通訊協定。SSH 通過創建將遠程服務器與授權用戶匹配的公鑰和私鑰來工作。使用該 key pair，您可以使用瀏覽器式 SSH 終端機連線至 Lightsail 執行個體。

如需相關資訊 SSH，請參閱[瞭解 SSH](#)。

當您建立 Lightsail 實體時，預設選項是讓 Lightsail 為您管理 SSH 金鑰。Lightsail 提供以瀏覽器為基礎的 SSH 用戶端，以安全地連線至 Linux 型執行個體。它是功能完整的終端機，您可以輸入命令及變更執行個體。

以 Windows 為基礎的 SSH 執行個體使用遠端桌面 (RDP) 通訊協定而非。如需 Lightsail 中以視窗為基礎的執行個體的詳細資訊，請參閱 Lightsail 中[以視窗為基礎的執行個體入門](#)。

### ⚠ Important

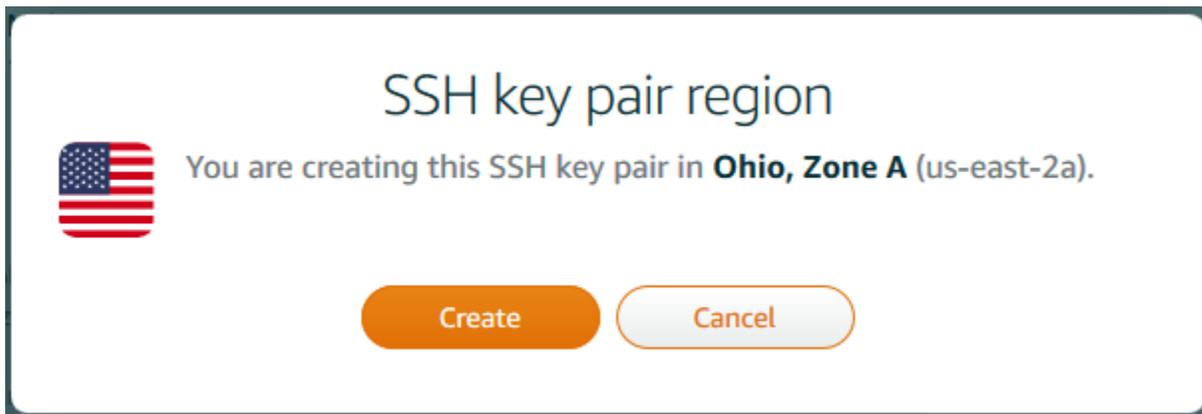
SSH密鑰管理是區域性的。當您在新的執行個體中建立執行個體時 AWS 區域，您可以選擇使用該區域的預設 key pair。您也可以在此區域中使用自訂的金鑰。請記住，如果您上傳自己的金鑰，則必須針對擁有 Lightsail 執行個體的每個區域執行此動作。

如果您使用預設金鑰，仍可下載私有金鑰以確保安全。此動作可在您建立執行個體當時或之後進行。如果您選擇在建立執行個體之後下載金鑰，您可以在 [帳戶] 頁面的SSH金鑰下執行這項操作。

## 建立新的金鑰

如果您不選擇使用預設金鑰，您可以在建立 Lightsail 實體時建立新的 key pair。

1. 如果您尚未完成，請選擇 Create instance (建立執行個體)。
2. 在 [建立執行個體] 頁面上，選擇 [變更 SSH key pair]。
3. 選擇 Create new (建立新項目)。
4. Lightsail 會顯示我們要建立新金鑰的區域。



選擇 Create (建立)。

5. 輸入金鑰對的名稱。

資源名稱：

- 每個 Lightsail 帳戶 AWS 區域 中的每個項目都必須是唯一的。
- 必須包含 2 至 255 個字元。
- 開頭和結尾必須是英數字元或數字。
- 可以包含英數字元、數字、句點、破折號和底線。

## 6. 選擇 Generate key pair (產生金鑰對)。

### Important

將您的金鑰存放在可以輕鬆找到的位置。此外，最好能夠確定已設定許可，讓其他人無法讀取。

## 7. 繼續建立您的執行個體。

## 上傳現有的金鑰

您也可以選擇在建立 Lightsail 實體時上傳現有的金鑰。

1. 如果您尚未完成，請選擇 Create instance (建立執行個體)。
2. 在 [建立執行個體] 頁面上，選擇 [變更 SSH key pair]。
3. 選擇 Upload new (上傳新項目)。
4. Lightsail 會顯示您要上傳新金鑰的區域。

選擇 Upload (上傳)。

5. 選擇 Browse (瀏覽) 以找到本機電腦上的金鑰。

請務必上傳公有金鑰 (而非私有金鑰)。例如：`github_rsa.pub`。

6. 選擇 Upload key (上傳金鑰)。
7. 繼續建立您的執行個體。

## 管理您的金鑰

您可以在 [帳戶] 頁面的 [SSH金鑰] 索引標籤上管理您的金鑰。您將會看到各個區域正在使用的各個金鑰對。

The screenshot shows the 'SSH keys' tab in the Amazon Lightsail console. At the top, there are three tabs: 'Profile', 'SSH keys' (which is selected), and 'Advanced'. Below the tabs, the heading is 'SSH key pairs' with a help icon. The text below reads: 'Choose your preferred key pair in each Region. You can also create a new key pair or upload an existing key. SSH key pairs can only be used in the Region where they are created or uploaded. You may store up to 100 keys per Region.' Below this text are two buttons: 'Create New +' and 'Upload New' with an upload icon. The main content is organized by region, each with an American flag icon and the region name. For each region, there is a list of key pairs. Each key pair has a radio button to select it, a name, and a 'Download' button with a download icon or a red 'X' icon. The regions and their key pairs are: Virginia (us-east-1) with 'Default' (selected), 'custom.keypair', and 'Test\_Keypair1'; Oregon (us-west-2) with 'Default' and 'github\_rsa'; and Ohio (us-east-2) with 'Default'.

在此頁面上，您可以變更建立新 Lightsail 實體時預設使用的金鑰。您也可以建立新的金鑰、上傳現有的金鑰，或下載私有金鑰。您可能需要使用像 Pu 這樣的 SSH 客戶端 TTY 進行連接，這將需要您擁有密鑰的私有一半。您可以在 Account (帳戶) 頁面下載金鑰。進一步瞭解如何設定 Pu TTY 以連線至 [Lightsail 執行個體](#)。

## 使用 Lightsail 安全殼層金鑰控制安全執行個體

您可以使用金鑰配對建立與 Amazon Lightsail 執行個體的安全連線。當您第一次建立 Amazon Lightsail 執行個體時，您可以選擇使用 Lightsail 為您建立的金鑰對 (Lightsail 預設 key pair) 或您建立的自訂 key pair。如需詳細資訊，請參閱 [金鑰配對和連線到 Amazon Lightsail 中的執行個體](#)。

在 Linux 和 Unix 執行個體上，私有金鑰允許您建立與執行個體的安全 SSH 連線。在 Windows 執行個體上，私有金鑰會解密您用於建立與執行個體的安全 RDP 連線的預設管理員密碼。

在本指南中，我們將說明如何管理可用於 Lightsail 執行個體的金鑰。您可以檢視金鑰、刪除現有金鑰以及建立或上傳新金鑰。

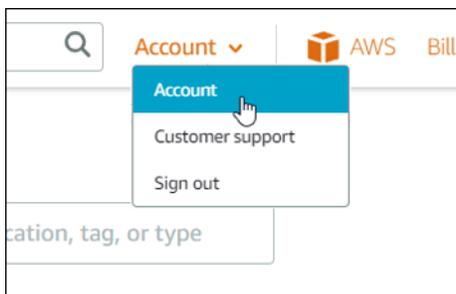
## 內容

- [檢視您的預設和自訂金鑰](#)
- [從 Lightsail 主控台下載預設金鑰的私密金鑰](#)
- [在主控台中刪除自訂金鑰](#)
- [刪除預設金鑰並在 Lightsail 主控台中建立新金鑰](#)
- [使用主控台建立自訂金鑰](#)
- [使用 SSH 凱基創建一個自定義密鑰並上 Lightsail](#)

## 檢視您的預設和自訂金鑰

完成下列程序，即可從 Lightsail 主控台檢視您的預設和自訂按鍵。

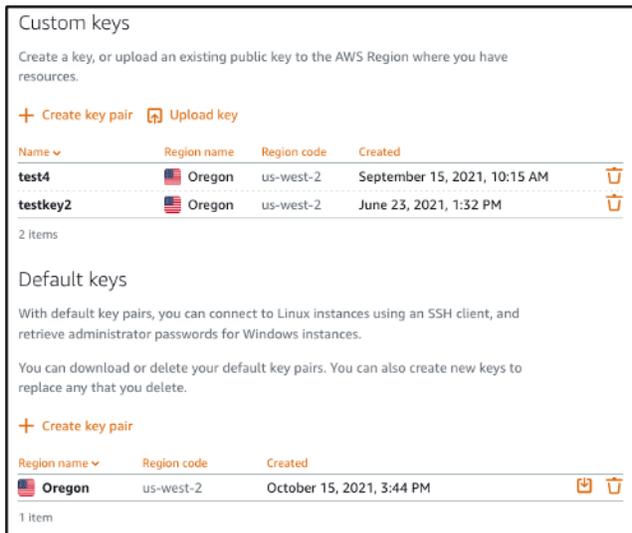
1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁上，請在頂部導覽選單中選擇 Account (帳戶)。
3. 在下拉式選單中選擇 Account (帳戶)。



4. 選擇 SSH Keys (SSH 金鑰) 索引標籤。

SSH 金鑰頁面會列出：

- 自訂金鑰 — 這些是您使用 Lightsail 主控台或第三方工具 (例如 ssh-keygen) 建立的金鑰。您可以在每個鍵中有許多自定義密鑰 AWS 區域。
- 預設按鍵 — 這些是 Lightsail 為您建立的按鍵。您最多僅能在每個 AWS 區域中擁有一個預設金鑰。



自訂和預設金鑰為區域性的。例如，美國西部 (奧勒岡) AWS 區域 中的金鑰只能在該區域中建立的執行個體上進行設定。如需有關金鑰的詳細資訊，請參閱 [Amazon Lightsail 中的金鑰配對和連線到執行個體](#)。

在 SSH 金鑰頁面上，您可以建立 key pair、上傳金鑰、刪除金鑰，以及下載 Lightsail 預設金鑰配對的私密金鑰。

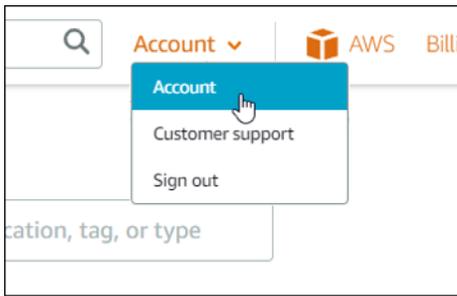
#### Note

您無法下載自訂金鑰組的私 key pair，因為 Lightsail 不會為您儲存該金鑰。如果您遺失了自訂金鑰對的私有金鑰，則應建立新的私有金鑰，並在您的執行個體上對其進行設定。然後，刪除已遺失的金鑰。如需詳細資訊，請參閱本指南 [稍後的使用 Lightsail 主控台建立自訂金鑰或使用 ssh-keygen 建立自訂金鑰](#)，然後上傳至 Lightsail。

## 從 Lightsail 主控台下載預設金鑰的私密金鑰

完成下列程序，即可從 Lightsail 主控台下載預設 key pair 的私密金鑰。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁上，選擇頂端導覽窗格中的 [帳戶]。
3. 在下拉式選單中選擇 Account (帳戶)。



4. 選擇 SSH Keys (SSH 金鑰) 索引標籤。
5. 在頁面的 Default keys (預設金鑰) 區段，選擇您要下載之金鑰的下載圖示。



### Important

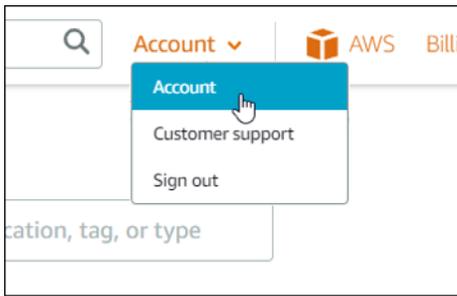
請將私有金鑰存放在安全位置。請勿公開共享金鑰，因為該金鑰可用來連接到您的執行個體。

您可以設定 SSH 用戶端，以使用私有金鑰來連接您的執行個體。如需詳細資訊，請參閱[連線至執行個體](#)。

## 在主控台中刪除自訂金鑰

請完成下列程序，以刪除 Lightsail 主控台自訂金鑰。如此可避免在您在 Lightsail 中建立的新執行個體上設定自訂金鑰。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁上，選擇頂端導覽窗格中的 [帳戶]。
3. 在下拉式選單中選擇 Account (帳戶)。



4. 選擇 SSH Keys (SSH 金鑰) 索引標籤。
5. 在頁面的自訂金鑰部分，選擇您要刪除之金鑰的刪除圖示。

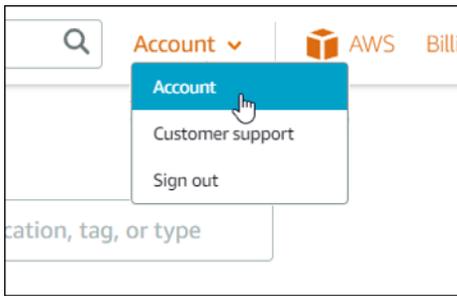


此動作不會從先前建立且目前正在執行的執行個體中移除自訂金鑰對的公有金鑰。若要移除先前存放在執行中執行個體上設定的公開金鑰，請參閱在 [Amazon Lightsail 中管理存放在執行個體上的金鑰](#)。

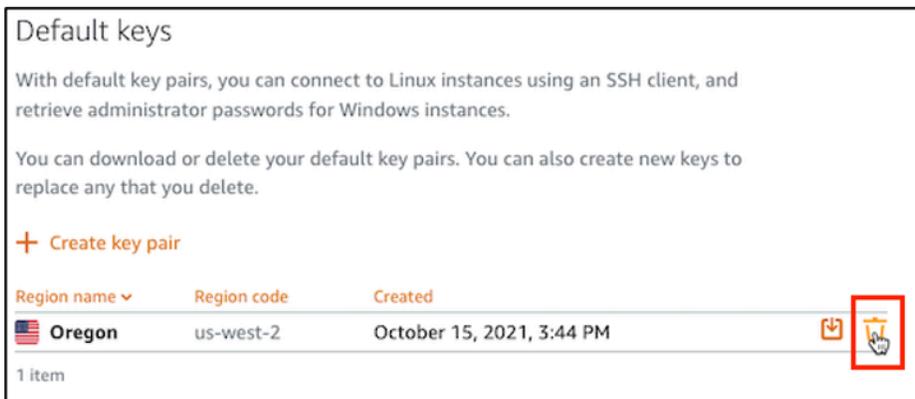
## 刪除預設金鑰並在 Lightsail 主控台中建立新金鑰

請完成下列程序，以刪除 Lightsail 主控台內的預設金鑰。這樣可防止在您在 Lightsail 中建立的新執行個體上設定該預設金鑰。然後，您就可以建立新的預設金鑰來取代您刪除的金鑰。您可以在 Lightsail 中建立的新執行個體上設定新的預設金鑰。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁上，選擇頂部導覽窗格上的 [帳戶]。
3. 在下拉式選單中選擇 Account (帳戶)。



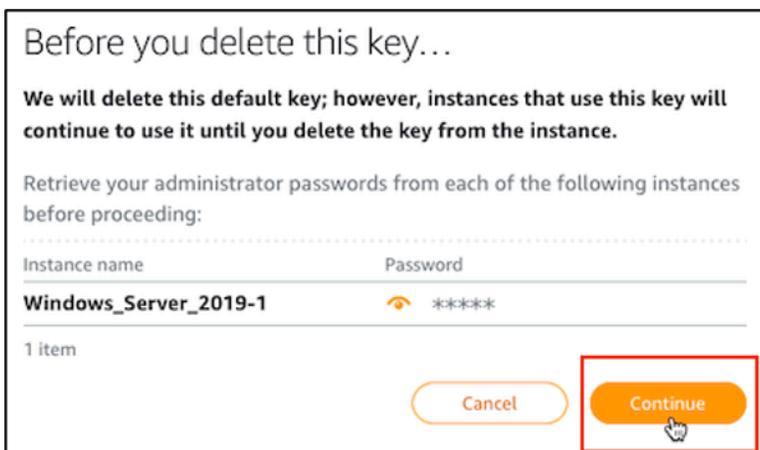
4. 選擇 SSH Keys (SSH 金鑰) 索引標籤。
5. 在頁面的預設金鑰部分，選擇您要刪除之預設金鑰的刪除圖示。



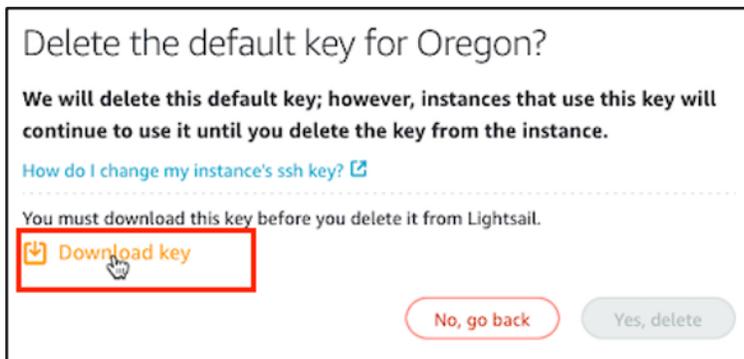
### Important

刪除預設金鑰不會從先前建立且目前正在執行的執行個體中移除自訂金鑰對的公有金鑰。如需詳細資訊，請參閱[在 Amazon Lightsail 中管理存放在執行個體上的金鑰](#)。

6. 預設金鑰可用來產生 Windows 執行個體的管理員密碼。刪除預設金鑰之前，請先從使用要刪除的預設金鑰之任何 Windows 執行個體中擷取並儲存管理員密碼。
7. 選擇 Continue (繼續) 以刪除預設金鑰。



8. 您必須先下載預設金鑰，才能加以刪除。下載預設金鑰後，您可以選擇 Yes, delete (是，刪除) 來永久刪除預設金鑰。



9. 已刪除預設金鑰。選擇 Okay (確定)。



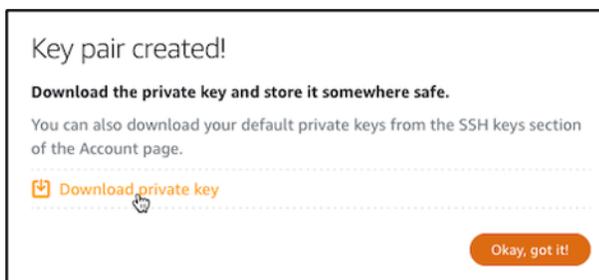
下列步驟為選用步驟，只有當您要取代您所刪除的預設金鑰對時，才需要完成這些步驟。

10. 在頁面的 Default keys (預設金鑰) 區段，選擇 Create key pair (建立金鑰對)。
11. 在出現的「選取區域」提示中，選擇您要 AWS 區域在其中建立新預設金鑰的。您將能夠在相同的 AWS 區域中建立的新執行個體上設定新的預設金鑰。

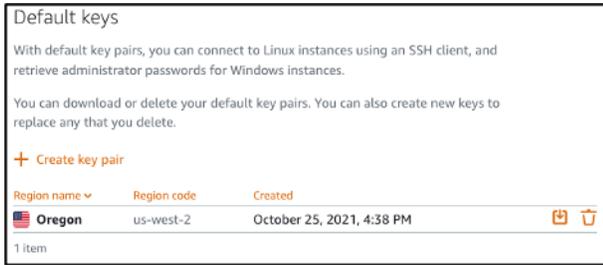
#### Note

使用這些步驟，您只能在已建立 Lightsail 資源 AWS 區域的位置建立預設金鑰配對。若要在新區域中建立預設 key pair，您必須在該區域中建立 Lightsail 資源。建立資源也會建立預設金鑰對。

12. 下載私有金鑰並將其存放在安全的位置。
13. 選擇 Ok, got it! (好的，我知道了!) 以繼續進行。



## 14. 在 Lightsail 主控台安全殼層金鑰頁面上確認新的預設金鑰。

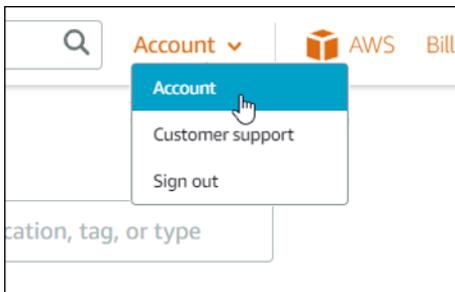


您可以在 Lightsail 中建立的新執行個體上設定新的預設金鑰。若要在先前建立且目前正在執行的執行個體上設定新的預設金鑰，請參閱[管理存放在 Amazon Lightsail 中執行個體上的金鑰](#)。

## 使用主控台建立自訂金鑰

請完成下列程序，以使用 Lightsail 主控台建立自訂 key pair。您將能夠在 Lightsail 中建立的新執行個體上設定新的自訂金鑰。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁上，選擇頂部導覽窗格上的 [帳戶]。
3. 在下拉式選單中選擇 Account (帳戶)。



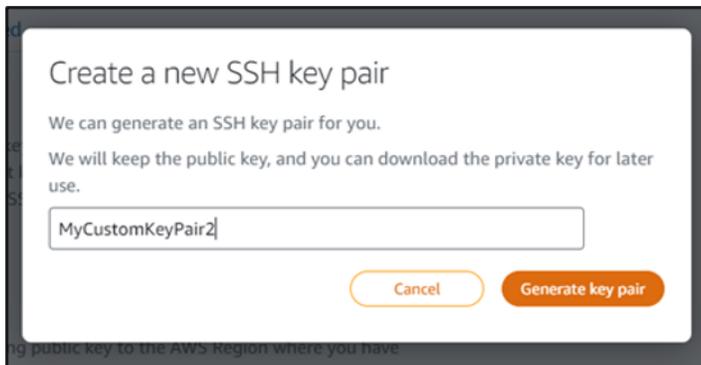
4. 選擇 SSH Keys (SSH 金鑰) 索引標籤。
5. 選擇此頁面的 Custom keys (自訂金鑰) 區段下的 Create key pair (建立金鑰對)。



6. 在畫面上顯示的選取區域提示中，選擇您要建立新自訂金鑰的 AWS 區域。您將能夠在相同的 AWS 區域中建立的新執行個體上設定新的自訂金鑰。



7. 在畫面上顯示的建立新的 SSH 金鑰對提示中，為您的自訂金鑰指定名稱，然後選擇 Generate key pair (建立金鑰對)。

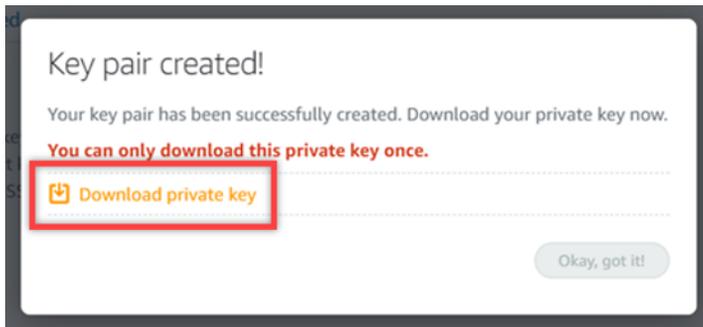


8. 在畫面上顯示的已建立金鑰對！提示中，選擇 Download private key (下載私有金鑰) 以將私有金鑰儲存到本機電腦。

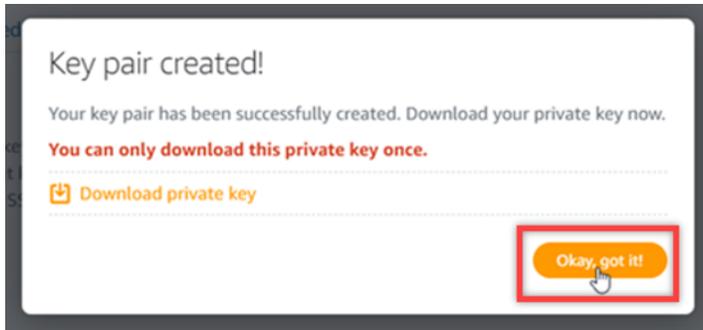
### **⚠ Important**

請將私有金鑰存放在安全位置。請勿公開共享金鑰，因為該金鑰可用來連接到您的執行個體。

這是您可以下載自訂金鑰對的私有金鑰的唯一機會。Lightsail 不會儲存自訂金鑰配對的私密金鑰。關閉此提示後，您將無法再次下載。



- 選擇 Ok, got it! (好的，我知道了!) 以關閉提示。



- 您的新自訂金鑰會在頁面的自訂金鑰部分下列出。



您可以在 Lightsail 中建立的新執行個體上設定新的自訂金鑰。若要在先前建立且目前正在執行的執行個體上設定新的自訂金鑰，請參閱[管理存放在 Amazon Lightsail 中執行個體上的金鑰](#)。

## 使用 SSH 凱基創建一個自定義密鑰並上 Lightsail

完成下列程序以使用第三方工具 (如 ssh-keygen) 在本機電腦上建立自訂金鑰對。建立金鑰之後，您可以將金鑰上傳到 Lightsail 主控台。您將能夠在 Lightsail 中建立的新執行個體上設定新的自訂金鑰。

- 開啟您本機電腦的命令提示或終端機。
- 輸入以下命令來建立金鑰對。

```
ssh-keygen -t rsa
```

3. 在電腦上指定金鑰對儲存的目錄位置。

例如，您可以指定下列目錄其中之一：

- a. 在 Windows 上：`C:\Users\<UserName>\.ssh\<KeyPairName>`
- b. 在 macOS、Linux 或 Unix 上：`/home/<UserName>/.ssh/<KeyPairName>`

以您目前登入的使用者名稱來取代 *<UserName>*，然後以新金鑰對名稱來取代 *<KeyPairName>*。

在下列範例中，我們會在 Windows 電腦上指定 `C:\Keys` 目錄，並將新的金鑰命名為 `MyNewLightsailCustomKey`。

```
C:\Users\<User Name>>ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (C:\Users\<User Name>\.ssh\id_rsa): C:\Keys\MyNewLighstailCustomKey
```

4. 輸入金鑰的密碼短語，然後按下 Enter。您不會在輸入密碼短語時看見內容。

稍後在 SSH 用戶端上設定金鑰對的私有金鑰，以便連接到設定了金鑰對之私有金鑰的執行個體時，您會需要此密碼短語。

```
Enter passphrase (empty for no passphrase):
```

5. 請再次輸入密碼短語以確認，然後按下 Enter。您不會在輸入密碼短語時看見內容。

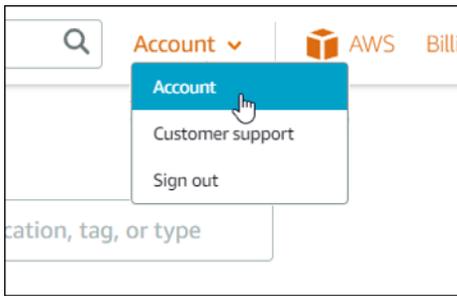
```
Enter same passphrase again:
```

6. 畫面上會出現提示，確認您的私有金鑰和公有金鑰已儲存至指定的目錄。

```
Your identification has been saved in C:\Keys\MyNewLighstailCustomKey.
Your public key has been saved in C:\Keys\MyNewLighstailCustomKey.pub.
```

接下來，您會將 key pair 的公開金鑰上傳至 Lightsail 主控台。

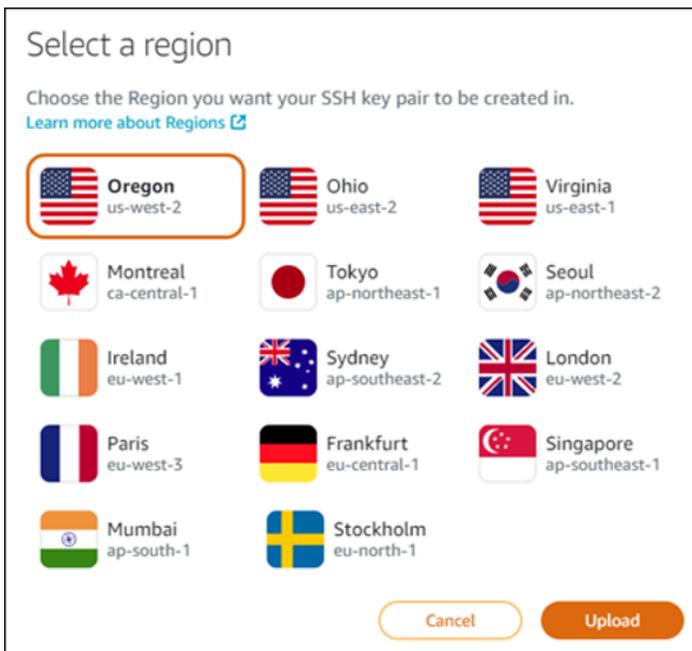
7. 登入主 [Lightsail 台](#)。
8. 在 Lightsail 首頁上，選擇頂端導覽窗格中的 [帳戶]。
9. 在下拉式選單中選擇 Account (帳戶)。



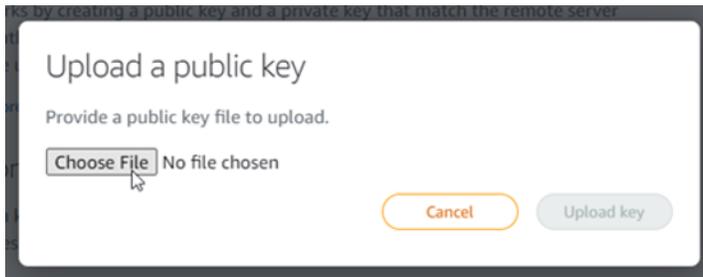
10. 選擇 SSH Keys (SSH 金鑰) 索引標籤。
11. 選擇此頁面的 Custom keys (自訂金鑰) 區段下的 Upload key (上傳金鑰)。



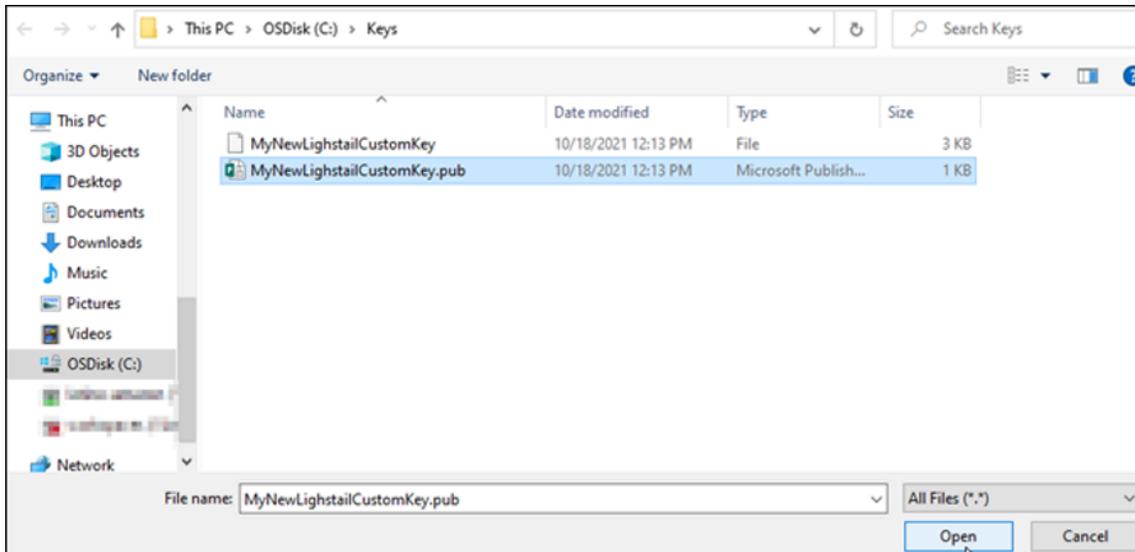
12. 在出現的「選取地區」提示 AWS 區域中，選擇您要上傳新自訂金鑰的位置。您將能夠在相同的 AWS 區域中建立的新執行個體上設定新的自訂金鑰。



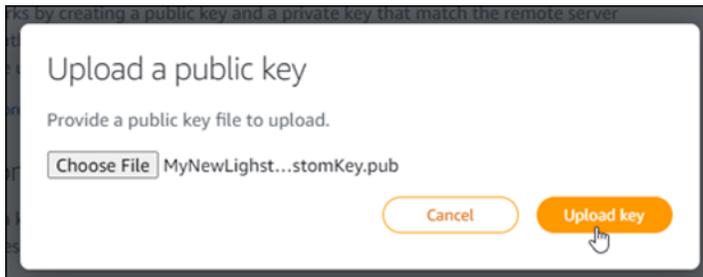
13. 選擇上傳。
14. 在畫面上顯示的上傳公有金鑰提示中，按一下 Choose File (選擇檔案)。



15. 找出稍早在此程序中建立之金鑰對的公有金鑰 (在您的本機電腦上) , 然後選擇 Open (開啟)。金鑰對的公有金鑰是具有 .PUB 副檔名的檔案。



16. 選擇 Upload key (上傳金鑰)。



17. 您的新自訂金鑰會在頁面的自訂金鑰部分中列出。



您可以在 AWS 區域 (此為您上傳金鑰的區域) 中建立的新執行個體上設定新的自訂金鑰。若要在先前建立且目前正在執行的執行個體上設定新的自訂金鑰，請參閱[管理存放在 Amazon Lightsail 中執行個體上的金鑰](#)。

## 管理安全殼層金鑰

您可以使用金鑰配對建立與 Amazon Lightsail 執行個體的安全連線。當您第一次建立金鑰時，Lightsail 會在 Linux 或 Unix 執行個體上設定 key pair 的公開金鑰。建立執行個體的 SSH 連線時，您可以使用金鑰對的私有金鑰來驗證執行個體。如需金鑰的詳細資訊，請參閱[金鑰對與連接到執行個體](#)。

執行個體開始運作後，您就可以變更有來連接至執行個體的金鑰對，方法是在執行個體上新增公有金鑰，或是取代執行個體上的公有金鑰 (刪除現有公有金鑰並在執行個體上新增一個)。這樣做的原因如下：

- 如果您組織中的使用者需要使用不同的金鑰對來存取執行個體，您可以將該公有金鑰新增到執行個體。
- 如果您需要確保從執行個體 (使用了已洩露金鑰) 的快照建立的新執行個體安全無虞。
- 如果某些人擁有私有金鑰的複本，而您希望阻止他們連線到您的執行個體 (例如，如果他們已離開您的組織)，則您可刪除該共有金鑰並用新的金鑰來取代它。

若要新增或取代執行個體上的金鑰，您必須能夠連線至您的執行個體。如果您遺失現有的私有金鑰，您可以使用 Lightsail 瀏覽器型 SSH 用戶端來連接到執行個體。如需詳細資訊，請參閱[連接至 Linux 或 Unix 執行個體](#)。

### 內容

- 步驟 1：[了解程序](#)
- 步驟 2：[建立金鑰對](#)
- 步驟 3：[新增公有金鑰至執行個體](#)
- 步驟 4：[使用新的金鑰對連線至執行個體](#)
- 步驟 5：[從執行個體中刪除現有的公有金鑰](#)

### 步驟 1：了解程序

以下是在執行個體上新增和移除金鑰的一般步驟。如果您想從執行個體中移除金鑰而不新增金鑰，請參閱本指南稍後提及的步驟 5：[從執行個體中刪除現有公有金鑰](#)。

1. 建立金鑰對 – 若要新增金鑰至執行個體，您必須先建立新的金鑰對。您可以使用 Lightsail 主控台或使用協力廠商工具 (例如 ssh-keygen) 在本機電腦上建立自訂或預設 key pair。兩種方法都會產生新的金鑰對，包含公有金鑰和私有金鑰。如需詳細資訊，請參閱本指南稍後提及的步驟 2：[建立金鑰對](#)。
2. 新增公有金鑰至執行個體 – 建立金鑰對後，您可以使用 SSH 連接到您的執行個體，並將金鑰對的公有金鑰新增至您的執行個體。如需詳細資訊，請參閱本指南稍後提及的步驟 3：[新增公有金鑰至執行個體](#)。
3. 測試是否能使用新的金鑰對連接到執行個體 – 在執行個體上儲存金鑰對的公有金鑰後，您應該測試是否可以使用金鑰對的私有金鑰，以 SSH 連接到執行個體。如需詳細資訊，請參閱本指南稍後提及的步驟 4：[使用新的金鑰對連接至執行個體](#)。
4. 從執行個體移除舊公有金鑰 – 使用新金鑰順利連接執行個體後，您就可以從執行個體移除舊金鑰。完成此步驟可防止使用者透過舊金鑰對連接到執行個體。如需詳細資訊，請參閱本指南稍後提及的步驟 5：[從執行個體刪除現有的公有金鑰](#)。

## 步驟 2：建立金鑰對

完成下列程序以使用 ssh-keygen 在本機電腦上建立金鑰對。

1. 開啟您本機電腦的命令提示或終端機。
2. 輸入以下命令來建立金鑰對。

```
ssh-keygen -t rsa
```

3. 在電腦上指定金鑰對儲存的目錄位置。

例如：

- 在 Windows 上：`C:\Users\<UserName>\.ssh\<KeyPairName>`
- 在 macOS、Linux 或 Unix 上：`/home/<UserName>/.ssh/<KeyPairName>`

以您目前登入的使用者名稱來取代 `<UserName>`，然後以新金鑰對名稱來取代 `<KeyPairName>`。

在下列範例中，我們會在 Windows 電腦上指定 `C:\Keys` 目錄，並將新的金鑰命名為 `MyNewLightsailCustomKey`。

```
C:\Users\<user>>ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (C:\Users\<user>\.ssh/id_rsa): C:\Keys\MyNewLighstailCustomKey
```

- 輸入金鑰的密碼短語，然後按下 Enter。您不會在輸入密碼短語時看見內容。

稍後在 SSH 用戶端上設定私有金鑰以連接到執行個體 (已設定了公有金鑰) 時，您會需要此密碼短語。

```
Enter passphrase (empty for no passphrase):
```

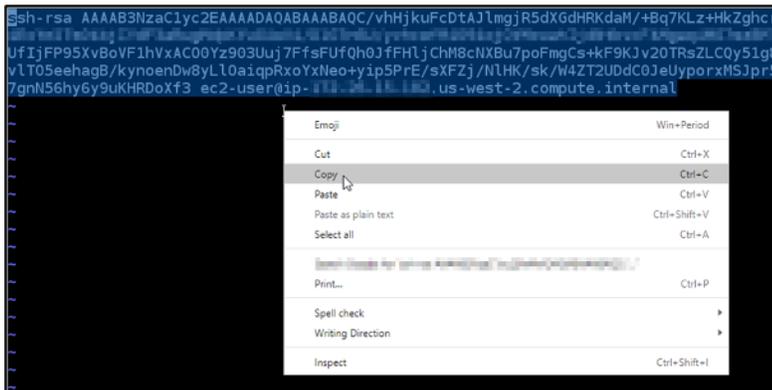
- 請再次輸入密碼短語以確認，然後按下 Enter。您不會在輸入密碼短語時看見內容。

```
Enter same passphrase again:
```

- 畫面上會出現提示，確認您的私有金鑰和公有金鑰已儲存至指定的目錄。

```
Your identification has been saved in C:\Keys\MyNewLighstailCustomKey.
Your public key has been saved in C:\Keys\MyNewLighstailCustomKey.pub.
```

- 開啟公有金鑰 (.PUB) 檔案，然後複製檔案中的文字。



請繼續閱讀本指南的下一節，將新的公開金鑰新增至 Lightsail 執行個體。

### 步驟 3：新增公有金鑰至執行個體

完成以下程序來新增公有金鑰至執行個體。公開金鑰內容儲存於 Linux 和 Unix 執行個體上的 `~/.ssh/authorized_keys` 檔案。

- 登入主 [Lightsail 台](#)。
- 選擇 Lightsail 首頁上的 Instances (執行個體) 索引標籤。
- 選擇您要連接之執行個體的瀏覽器型 SSH 用戶端圖示。



4. 連接後，輸入下列命令以使用您選擇的文字編輯器來編輯 `authorized_keys` 檔案。下列步驟使用 Vim 做為示範。

```
sudo vim ~/.ssh/authorized_keys
```

您應該會看到類似於以下範例的結果，這將顯示執行個體上目前設定的公有金鑰。在我們的案例中，建立執行個體所 AWS 區域 在的 Lightsail 預設金鑰是執行個體上唯一設定的公開金鑰。

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQBAQC+QizYnwmJ
R6b23qBWH00Siy5uUFh5Yyn4TX5I5070cIA+l5AGxjZpWiyR
dFL5RwR1Dws7pret5LC6l+PSalD4eJ7g2z0RUKIf6G6G1Neh
vyXdzVeg0G0iflMbez0V LightsailDefaultKeyPair
~
~
~
```

5. 按下 `I` 鍵以進入 Vim 編輯器的插入模式。
6. 在檔案上的最後一個公有金鑰之後輸入換行符號。
7. 貼上您先前在本指南中複製的公有金鑰文字 (建立新金鑰對之後)。您應該會看到類似以下範例的結果：

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQBAQC+QizYnwmJZ63wmRgTWSlkI7gF0qQ14sqIf5Z2
R6b23qBWH00Siy5uUFh5Yyn4TX5I5070cIA+l5AGxjZpWiyRBo5YFBgSP0QT0wR9A+s55DYU6rSY
dFL5RwR1Dws7pret5LC6l+PSalD4eJ7g2z0RUKIf6G6G1NehLmupFYqaPPiEV8DAtwSjqoHgEaj9
vyXdzVeg0G0iflMbez0V LightsailDefaultKeyPair
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQBAQC/vhHjkuFcDtAJlmgjR5dXGdHRKdaM/+Bq7KLz
UfIjFP95XvBoVF1hVxAC00Yz903Uuj7FfsFufQh0JfFHljChM8cNXBu7poFmgCs+kF9KJv20TRsZ
v1T05eehagB/kynoenDw8yLl0a1qpRxoYxNeo+yip5PrE/sXFZj/NLHK/sk/W4ZT2UDdC0JeUyp0
7gnN56hy6y9uKHRDoXf3 ec2-user@ip- us-west-2.compute.internal
~
~
```

8. 按下 `ESC` 鍵。接下來，鍵入 `:wq!` 並按下 `Enter` 以儲存編輯內容並結束 Vim 編輯器。

全新公有金鑰現已新增至您的執行個體。請繼續前往本指南的下一節，以瞭解使用新的金鑰對連接至執行個體的相關資訊。

## 步驟 4：使用新的金鑰對連線至執行個體

若要測試新的金鑰對，請中斷與執行個體的連線，然後使用您在本指南稍早建立的私有金鑰重新連接至該執行個體。如需詳細資訊，請參閱[金鑰配對和連線到 Amazon Lightsail 中的執行個體](#)。使用新金鑰順利連接到執行個體後，您就可以從執行個體中移除舊金鑰。繼續下一個步驟，瞭解如何從執行個體中刪除公有金鑰。

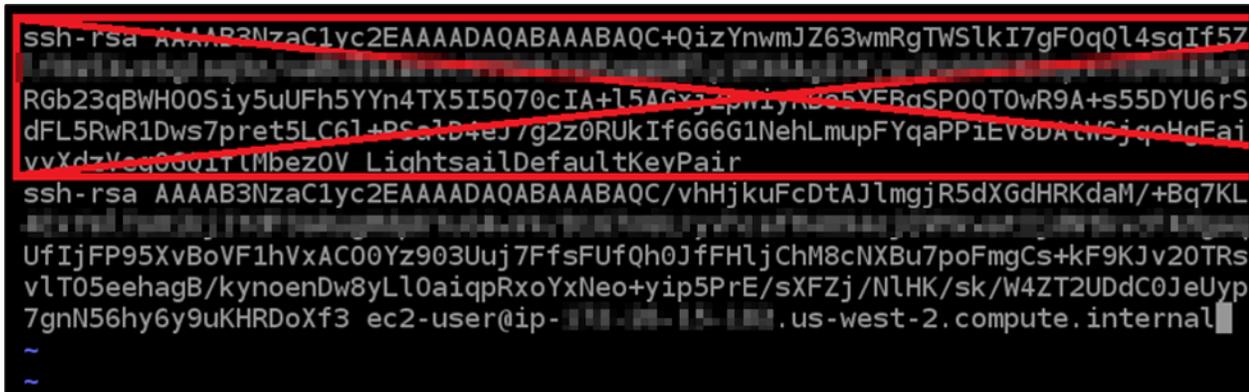
## 步驟 5：從執行個體中刪除現有的公有金鑰

完成下列程序以便從執行個體移除公有金鑰。如此可防止使用者透過舊金鑰對連接到執行個體。使用新金鑰對順利連接到執行個體後，請執行此動作。

1. 使用 SSH 連接至您的執行個體。
2. 輸入下列命令以使用您選擇的文字編輯器來編輯 `authorized_keys` 檔案。下列步驟使用 Vim 做為示範。

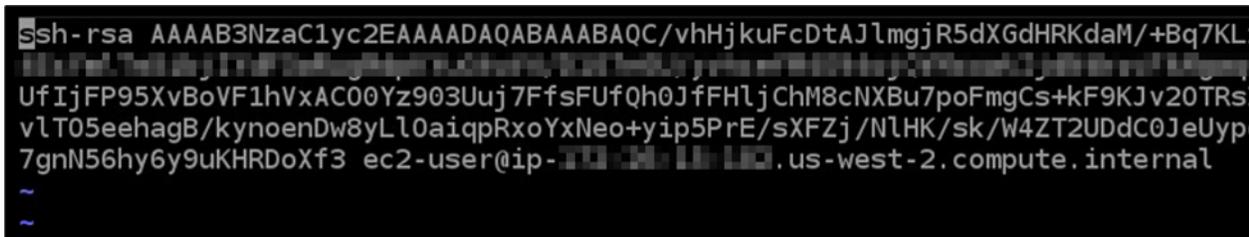
```
sudo vim ~/.ssh/authorized_keys
```

3. 按下字母 `I` 鍵以進入 Vim 編輯器的插入模式。
4. 刪除您要從執行個體移除且內含公有金鑰的文字行。



```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQAC+QizYnwmJZ63wmRgTWSlkI7gF0qQl4sqIf5Z
R5b23qBWH00Siy5uUFh5Yyn4TX5I5Q70cIA+l5AGxj2pw1yR05YERqSP0QT0wR9A+s55DYU6rS
dFL5RwR1Dws7pret5LC6l+PSa1B4eJ7g2z0RUkIf6G6G1NehLmupFYqaPP1EV8DAtnSjqHqFaj
vvXdzYc900ITLMbez0V LightsailDefaultKeyPair
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQAC/vhHjkuFcDtAJlmgjR5dXGdHRKdaM/+Bq7KL
UfIjFP95XvBoVF1hVxAC00Yz903Uuj7FfsFUfQh0JfFHljChM8cNXBu7poFmgCs+kF9KJv20TRs
vLT05eehagB/kynoenDw8yLl0aiqpRxoYxNeo+yip5PrE/sXFZj/NlHK/sk/W4ZT2UDdC0JeUyp
7gnN56hy6y9uKHRDoXf3 ec2-user@ip-10-10-10-10.us-west-2.compute.internal
~
~
```

結果應如下列範例所示，顯示的唯一金鑰即為新的公有金鑰。



```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQAC/vhHjkuFcDtAJlmgjR5dXGdHRKdaM/+Bq7KL
UfIjFP95XvBoVF1hVxAC00Yz903Uuj7FfsFUfQh0JfFHljChM8cNXBu7poFmgCs+kF9KJv20TRs
vLT05eehagB/kynoenDw8yLl0aiqpRxoYxNeo+yip5PrE/sXFZj/NlHK/sk/W4ZT2UDdC0JeUyp
7gnN56hy6y9uKHRDoXf3 ec2-user@ip-10-10-10-10.us-west-2.compute.internal
~
~
```

5. 按下 `ESC` 鍵。接下來，鍵入 `:wq!` 並按下 `Enter` 以儲存編輯內容並結束 Vim 編輯器。

需刪除的公有金鑰現已從執行個體移除。您的執行個體會拒絕使用該金鑰對之私有金鑰的連線。

## Connect 到 Linux 或 Unix 執行 Lightsail

Amazon Lightsail 為您提供以瀏覽器為基礎的SSH用戶端，這是連接到 Linux 或 Unix 執行個體的最快方式。您也可以使用自己的用SSH戶端連線至執行個體。如需詳細資訊，請參閱[下載並設定 Pu TTY](#)。

使用 Connect 至執行個體，SSH以便在伺服器上執行管理工作，例如安裝軟體套件或設定 Web 應用程式。以瀏覽器為基礎的用SSH戶端不需要安裝軟體，而且在您建立執行個體之後幾乎可以立即使用。

若要連線至 Lightsail 中的 Windows 伺服器執行個體，請參閱 [Connect 至您的視窗執行個體](#)。

連線至您的 Linux 或 Unix 執行個體

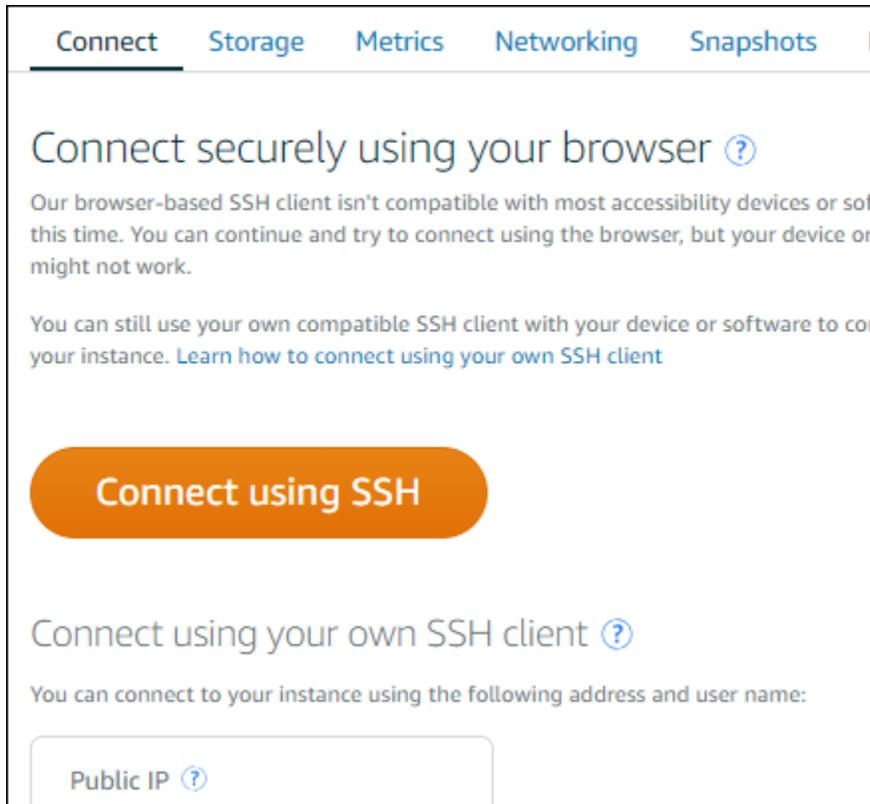
1. 登入主 [Lightsail 台](#)。
2. 使用下列任一方法，存取您要連線之執行個體的瀏覽器用SSH戶端：
  - 選擇快速連線圖示，如以下範例中所示。



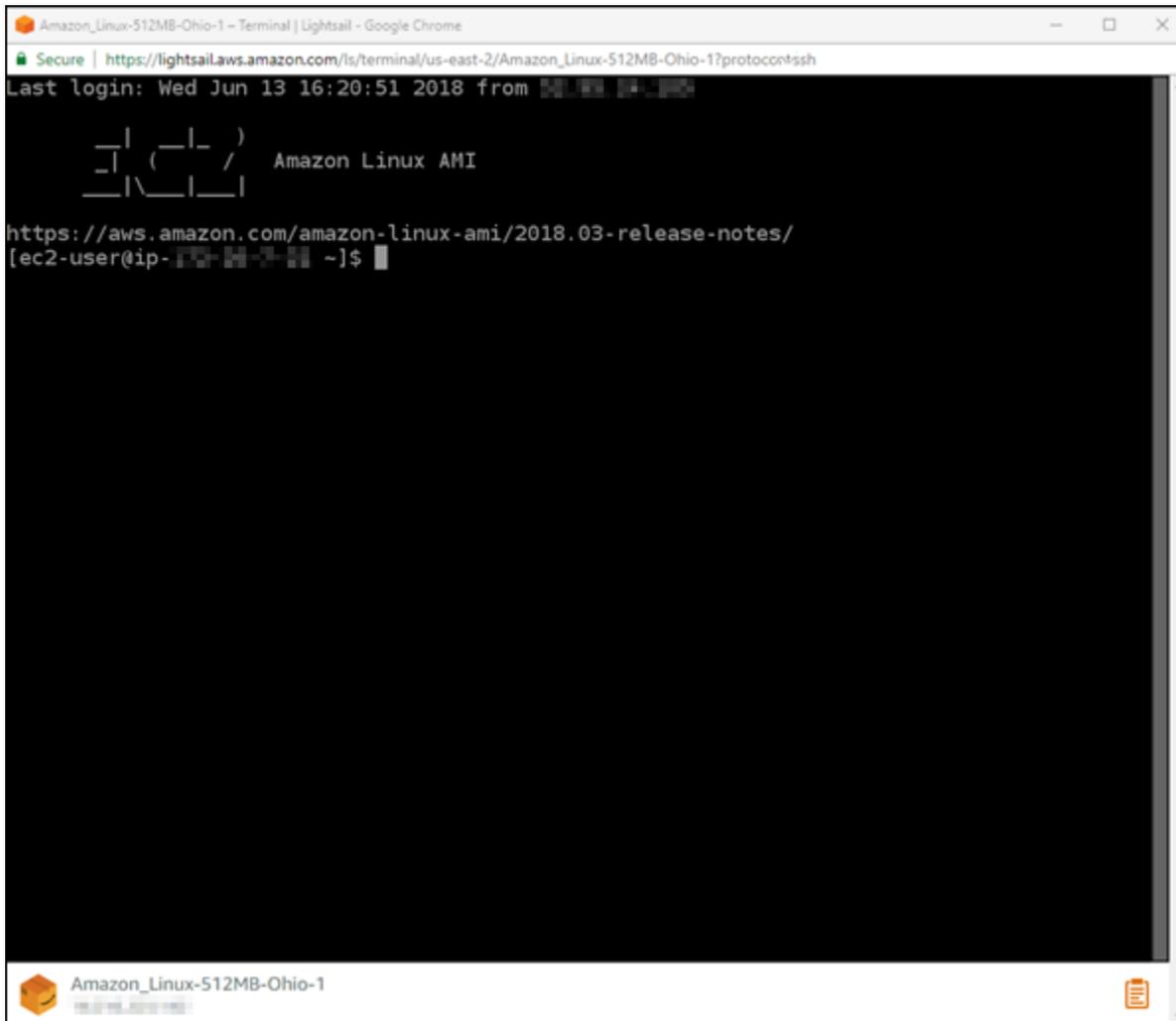
- 選擇動作功能表圖示 (:), 接著選擇 Connect (連接)。



- 選擇執行個體的名稱，然後在 [Connect] 索引標籤上選擇 [Connect 方式] SSH。



您可以在以瀏覽器為基礎的SSH用戶端開啟時開始與執行個體互動，並顯示終端機畫面，如下列範例所示：



### Note

[Connect] 索引標籤也提供使用您自己的用SSH戶端進行連線所需的資訊。如需詳細資訊，請參閱[下載和設定 PuTTY](#)

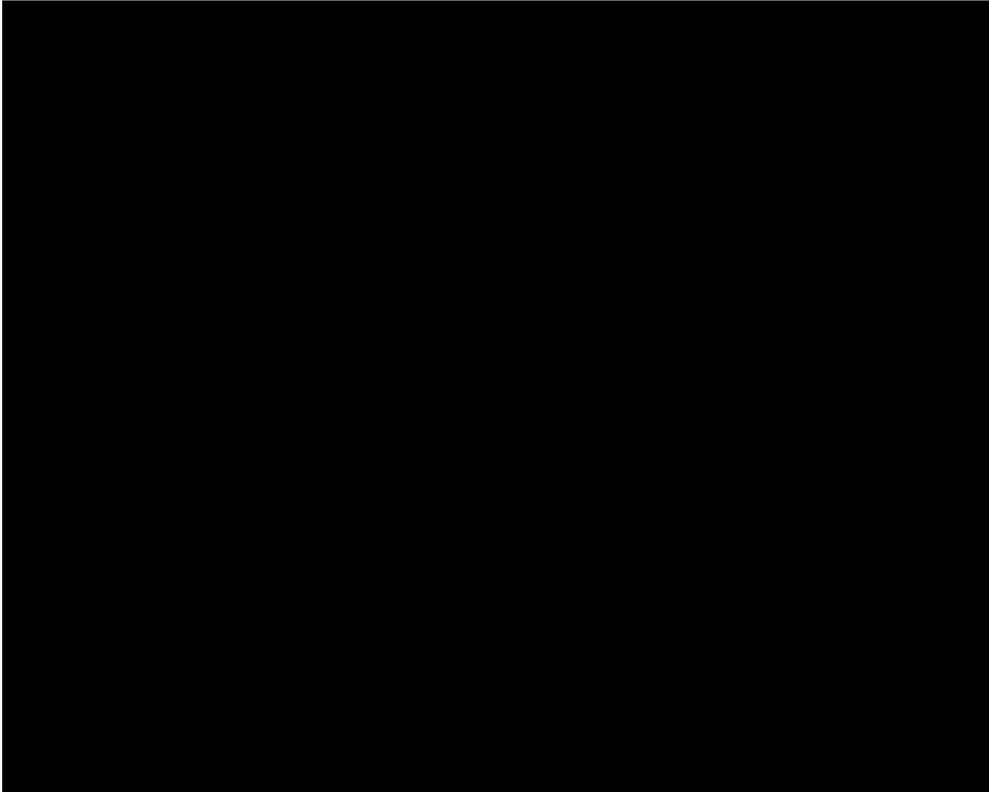
## 使用以瀏覽器為基礎SSH的用戶端與 Linux 或 Unix 執行個體互動

直接在終端機螢幕中鍵入 Linux 或 Unix 命令，將文字貼到終端機螢幕，或從瀏覽器用戶端的終SSH端螢幕複製文字。以下各節將說明如何在中將文字複製到剪貼簿或從剪貼簿貼上文字SSH。

將文字貼到以瀏覽器為基礎SSH的用戶端

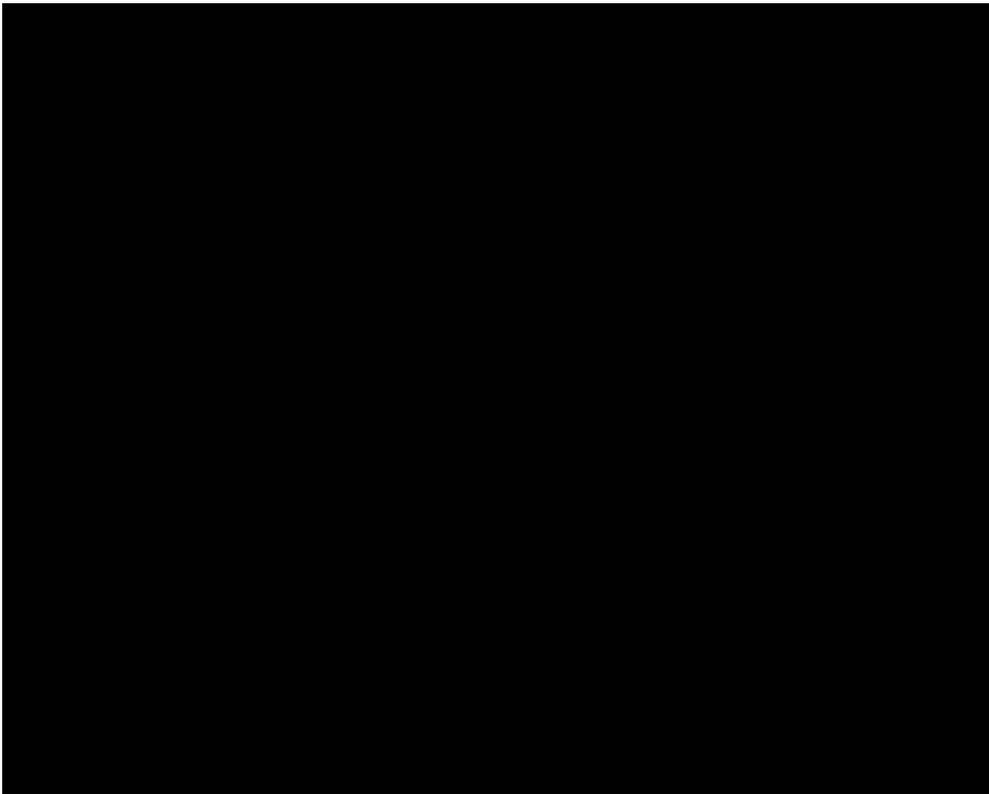
1. 在您的本機桌面反白文字，接著按 Ctrl+C (Ctrl+C) 或 Cmd+C (Cmd+C) 將其複製到您的本機剪貼簿。

2. 在以瀏覽器為基礎的SSH用戶端的右下角，選擇剪貼簿圖示。瀏覽器式SSH用戶端剪貼簿文字方塊隨即出現。
3. 按一下文字方塊，然後按 `Ctrl+V` 或 `Cmd+V`，將內容從本機剪貼簿貼上到以瀏覽器SSH為基礎的用戶端剪貼簿。
4. 以滑鼠右鍵按一下SSH終端機畫面上的任何區域，將文字從瀏覽器SSH用戶端剪貼簿貼上到終端機畫面。



#### 從以瀏覽器為基礎SSH的用戶端複製文字

1. 在終端機畫面上反白文字。
2. 在以瀏覽器為基礎的SSH用戶端的右下角，選擇剪貼簿圖示。瀏覽器式SSH用戶端剪貼簿文字方塊隨即出現。
3. 反白您要複製的文字，接著按 `Ctrl+C` (`Ctrl+C`) 或 `Cmd+C` (`Cmd+C`) 將文字複製到本機剪貼簿。您現在可以將複製的文字貼到本機桌面上任何地方。



## 使用指令 Connect 至執行個體 SSH

如果您的本機電腦使用 Linux 或 Unix 作業系統 (包括 macOS)，則您可以透過終端機視窗使用 SSH 戶端連線到 Amazon Lightsail 中的 Linux 或 Unix 執行個體。

本指南中描述的連接至執行個體的方法是許多方法中的一種。如需其他方法的詳細資訊，請參閱[SSH 金鑰配對](#)。

若要在 Lightsail 中連線到 Linux 或 Unix 執行個體，最簡單的方法是使用 Lightsail 主控台中提供的瀏覽器型用 SSH 戶端。如需詳細資訊，請參閱[連接至 Linux 或 Unix 執行個體](#)。

### 目錄

- [步驟 1：確認執行個體正在執行並取得公有 IP 地址](#)
- [步驟 2：確認執行個體正在使用的 SSH key pair](#)
- [步驟 3：變更私密金鑰的權限，並使用以下方式連線至執行個體 SSH](#)

## 步驟 1：確認執行個體正在執行並取得公有 IP 地址

在下列程序中，您會登入 Lightsail 主控台以確認執行個體處於執行中狀態，並取得執行個體的公用 IP 位址。您的執行個體必須處於執行中狀態才能建立 SSH 連線，而且稍後在本指南中，您將需要執行個體的公有 IP 位址才能連線至該執行個體。

1. 登入主 [Lightsail](#) 台。
2. 在 Lightsail 首頁的「實體」索引標籤中，找出您要連線的執行個體。
3. 確認執行個體處於執行中狀態，並記下執行個體的公有 IP 地址。

執行個體的狀態及其公有 IP 地址會列在執行個體名稱旁，如下列範例所示。

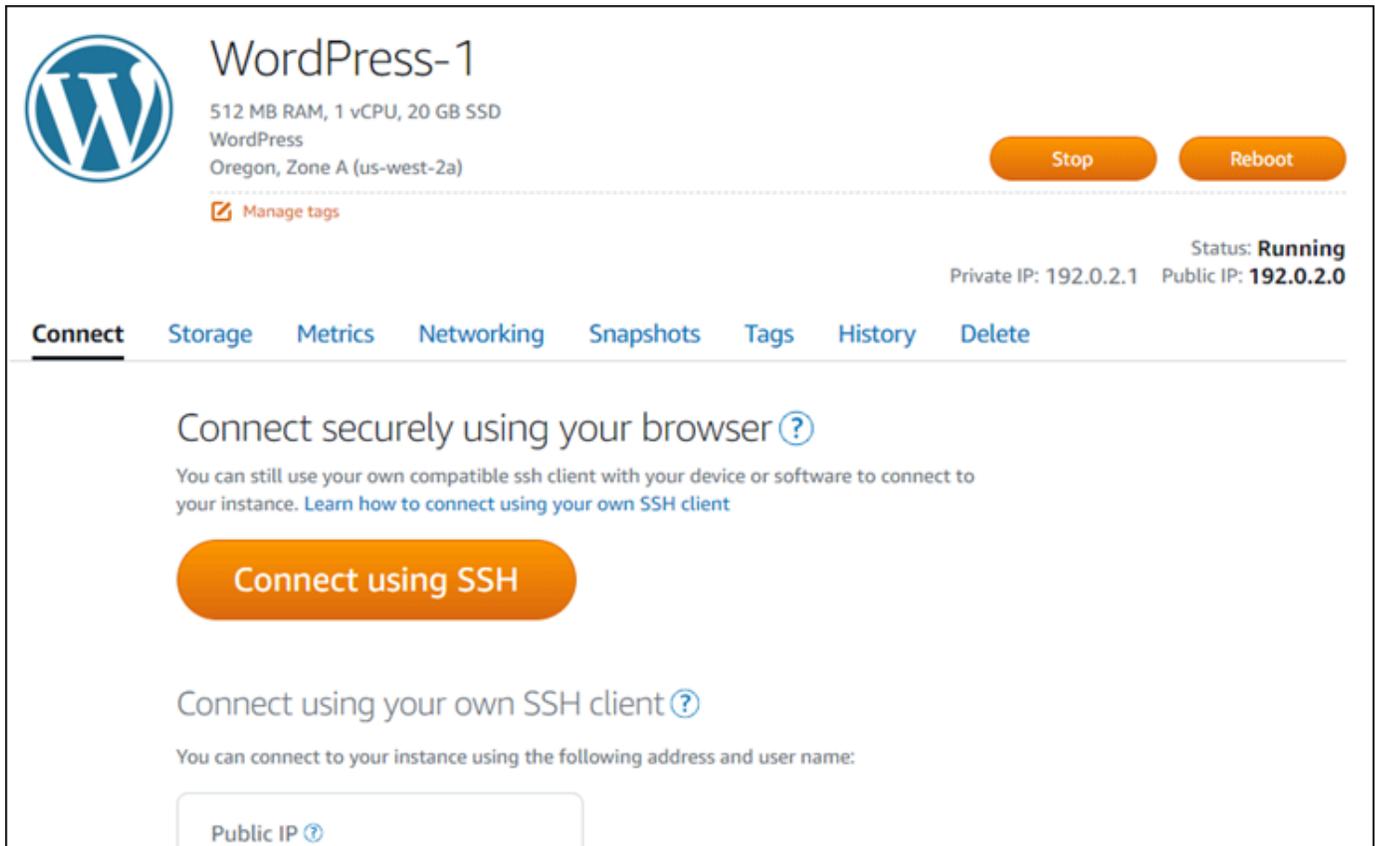


## 步驟 2：確認執行個體正在使用的 SSH key pair

在下列程序中，您可以確認執行個體正在使用的 SSH key pair。您需要金鑰組的私密金 key pair，才能向執行個體驗證並建立 SSH 連線。

1. 在 Lightsail 首頁的「實體」索引標籤中，選擇您要連線的執行個體名稱。

隨即會出現 Instance management (執行個體管理) 頁面，並包含各種管理執行個體的索引標籤選項。



WordPress-1

512 MB RAM, 1 vCPU, 20 GB SSD  
WordPress  
Oregon, Zone A (us-west-2a)

Manage tags

Status: **Running**  
Private IP: 192.0.2.1 Public IP: **192.0.2.0**

Connect Storage Metrics Networking Snapshots Tags History Delete

Connect securely using your browser ?

You can still use your own compatible ssh client with your device or software to connect to your instance. [Learn how to connect using your own SSH client](#)

Connect using SSH

Connect using your own SSH client ?

You can connect to your instance using the following address and user name:

Public IP ?

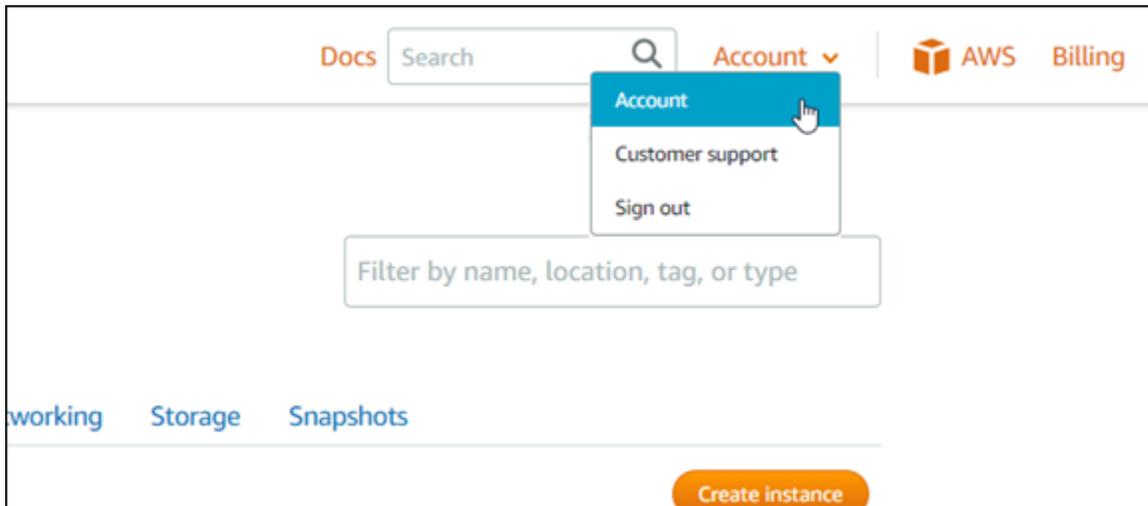
2. 在 Connect (連接) 索引標籤中，向下捲動以查看執行個體正在使用的金鑰對。有兩種可能：
  1. 下列範例顯示針對您在其中建立執行個體之AWS區域使用預設金鑰組的執行個體。如果您的執行個體使用預設金鑰對，則可以繼續執行此程序的步驟 3，以下載金鑰對的私有金鑰。Lightsail 只會儲存每個AWS區域之預設 key pair 的私密金鑰。

You configured this instance to use **default (us-west-2)** key pair.  
You can download your default private key from the [Account page](#).

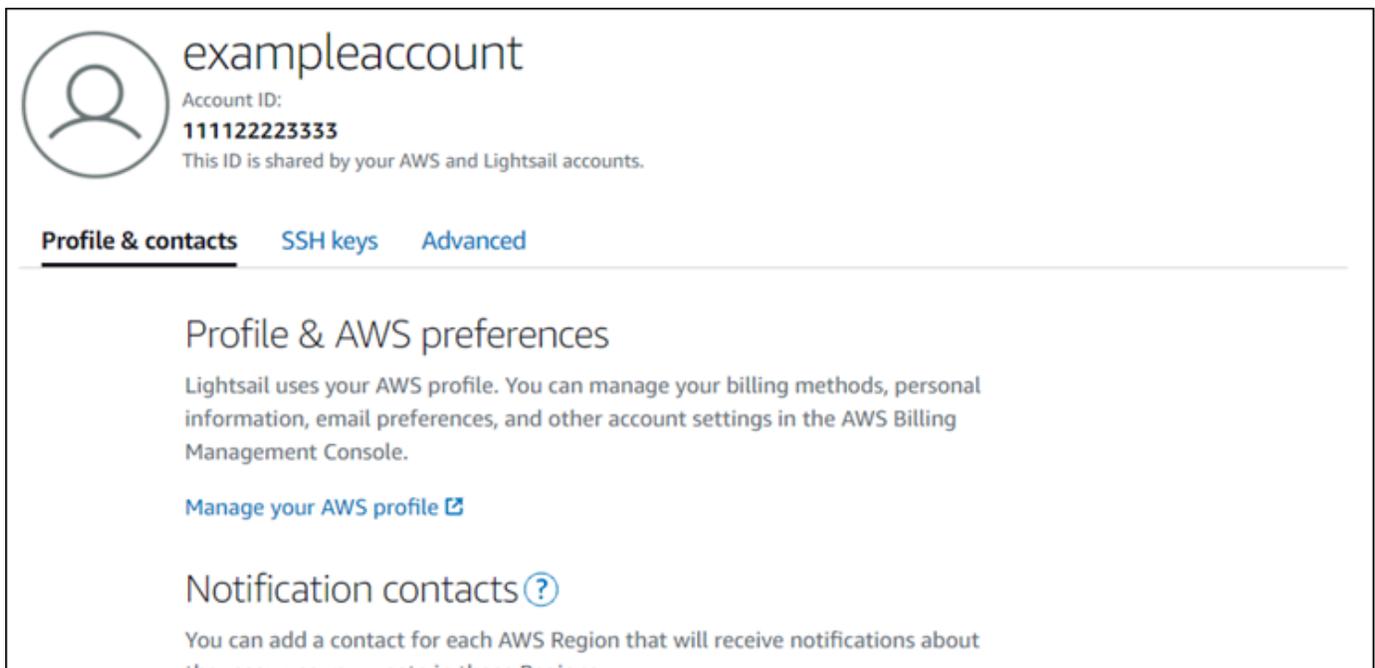
2. 下列範例顯示使用您上傳或建立之自訂金鑰對的執行個體。如果您的執行個體使用自訂金鑰對，則需要找到您存放金鑰的自訂金鑰對的私有金鑰。如果您遺失了自訂金鑰組的私 key pair，您將無法使用自己的用戶端建立與執行個體的SSH連線。不過，您可以繼續使用 Lightsail 主控台中提供的瀏覽器型用SSH戶端。找到自訂金鑰 key pair 的**私密金鑰**後，[請繼續進行下一步驟 3：變更私密金鑰的權限，並使用本指南SSH章節連線至執行個體](#)。

You configured this instance to use **MyKeyPair (us-west-2)** key pair.

3. 在頂部導覽選單上選擇 Account (帳戶)，然後選擇 Account (帳戶)。



出現的 Account management (帳戶管理) 頁面，包含各種管理帳戶設定的索引標籤選項。



4. 選擇SSH金鑰索引標籤。
5. 向下捲動，然後在您要連線的執行個體AWS區域的預設金鑰旁邊選擇下載圖示。

### Default keys

With default key pairs, you can connect to Linux instances using an SSH client, and retrieve administrator passwords for Windows instances.

You can download or delete your default key pairs. You can create one default key per AWS Region where you previously created resources.

[+ Create key pair](#)

Region name	Region code	Created		
Frankfurt	eu-central-1	April 27, 2018, 3:14 PM		
Ireland	eu-west-1	April 27, 2018, 3:14 PM		
Mumbai	ap-south-1	April 20, 2018, 2:54 PM		
Ohio	us-east-2	February 2, 2022, 4:17 PM		
Oregon	us-west-2	April 19, 2018, 9:11 AM		
Seoul	ap-northeast-2	August 23, 2018, 9:11 AM		
Singapore	ap-southeast-1	June 20, 2018, 3:45 PM		
Stockholm	eu-north-1	May 13, 2021, 10:03 AM		
Sydney	ap-southeast-2	April 30, 2019, 3:51 PM		

系統會將私有金鑰下載到您的本機電腦。您可能想要將下載的金鑰移至儲存所有SSH金鑰的目錄，例如使用者主目錄中的「金鑰」資料夾。您需要參考本指南下一節中儲存私有金鑰的目錄。如果私有金鑰嘗試儲存為 .pem 以外的格式，則應在儲存之前手動將格式更改為 .pem。

#### Note

Lightsail 不提供用於操作 .pem 檔案或其他憑證格式的公用程式。如果您需要轉換私鑰文件的格式，則可以隨時使用免費的開源工具，例SSL如 [Open](#)。

繼續進行下一步驟 3：變更私密金鑰的權限，並使用本指南章節的 [SSH 節](#) 連線至執行個體，以使用剛才下載的私密金鑰，並建立與執行個體的SSH連線。

步驟 3：變更私密金鑰的權限，並使用以下方式連線至執行個體 SSH

在下列程序中，您需變更私有金鑰檔案的許可，以確保只有您可讀取和寫入該檔案。然後，您可以在本機電腦中開啟終端機視窗，然後執行SSH命令以在 Lightsail 中建立與執行個體的連線。

1. 在您的本機電腦上開啟終端機視窗。

- 輸入下列命令，讓金鑰對的私有金鑰只能由您讀取和寫入。這是某些作業系統所需的安全性最佳實務。

```
sudo chmod 400 /path/to/private-key.pem
```

在命令中，將 `/path/to/private-key.pem` 取代為儲存執行個體正使用的金鑰對之私有金鑰的目錄路徑。

範例：

```
sudo chmod 400 /Users/user/Keys/LightsailDefaultKey-us-west-2.pem
```

- 輸入下列命令，使SSH用以連線至 Lightsail 中的執行個體：

```
ssh -i /path/to/private-key.pem username@public-ip-address
```

在命令中：

- `/path/to/private-key.pem` 使用目錄路徑到您保存實例正在使用的 key pair 的私鑰的位置。
- `username` 使用您的實例的用戶名。您可以根據執行個體使用的藍圖指定下列其中一個使用者名稱：
  - AlmaLinux 作業系統 9、Amazon Linux 2、Amazon Linux 2023、CentOS 串流 9、免費BSD 和開放SUSE的執行個體：`ec2-user`
  - Debian 執行個體：`admin`
  - Ubuntu 執行個體：`ubuntu`
  - Bitnami 執行個體：`bitnami`
  - Plesk 執行個體：`ubuntu`
  - cPanel WHM實例 (E)：`centos`
- Replace (取代) `public-ip-address` 使用您在本指南稍早前面的 Lightsail 主控台所記錄的執行個體公有 IP 位址。

絕對路徑的範例：

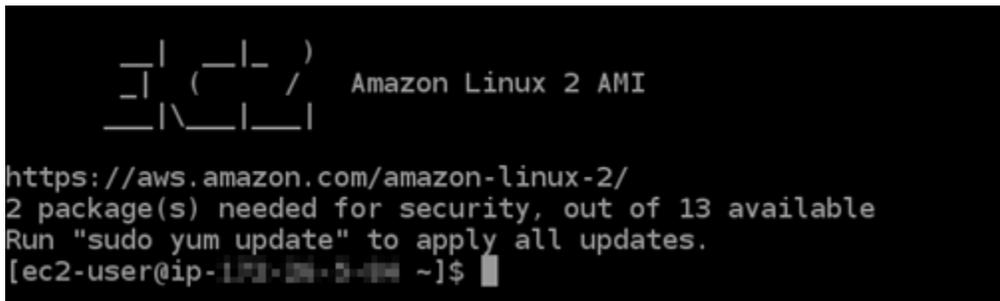
```
ssh -i /Users/user/Keys/LightsailDefaultKey-us-west-2.pem ec2-user@192.0.1.0
```

相對路徑的範例：

請注意為 .pem 檔案加上字首的 ./。省略 ./ 並單單寫入 LightsailDefaultKey-us-west-2.pem 將無法運作。

```
ssh -i ./LightsailDefaultKey-us-west-2.pem ec2-user@192.0.1.0
```

如果您看到執行個體的歡迎訊息，就代表已成功連接至執行個體。下列範例顯示 Amazon Linux 2 執行個體的歡迎訊息；其他執行個體藍圖具有類似的歡迎訊息。連線之後，您就可以在 Lightsail 中的執行個體上執行指令。若要中斷連接，請輸入 exit 並按 Enter (確認)。



```

  _ | ( _ | )
  _ | ( _ | )
  _ | \ _ | /
  _ |  _ |  _ |

Amazon Linux 2 AMI

https://aws.amazon.com/amazon-linux-2/
2 package(s) needed for security, out of 13 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-192-0-1-0 ~]$
```

## 使用 Connect 連接到 Linux/Unix Lightsail 執行個體 TTY

除了 Lightsail 中以瀏覽器為基礎的 SSH 終端機之外，您也可以使用 SSH 戶端 (例如 Pu) 連線到 Linux 型執行個體。TTY 若要瞭解如何設定 PuTTY，請參閱 [下載並設定 Pu TTY 以使用 Lightsail SSH 進行連線](#)。

### Note

若要使用 Connect 到以 Windows 為基礎的執行個體 RDP，請參閱 [連線到您的視窗型 Lightsail 執行個體](#)。

您可以使用 Lightsail 提供的預設私密金鑰、Lightsail 的新私密金鑰，或是與其他服務搭配使用的其他私密金鑰。

1. 啟動 PuTTY (例如，從「開始」功能表中選擇「所有程式」、「Pu」TTY、「Pu」TTY)。
2. 選擇 Load (載入)，接著尋找儲存的工作階段。

如果您沒有儲存的工作階段，請參閱 [步驟 4：TTY 使用私密金鑰和執行個體資訊完成 Pu 的設定](#)。

3. 根據您的執行個體作業系統，使用以下其中一個預設的使用者名稱登入：

- AlmaLinux, Amazon Linux 2, Amazon Linux 2023, CentOS 流 9, 免費BSD和開放SUSE的執行個體：ec2-user
- Debian 執行個體：admin
- Ubuntu 執行個體：ubuntu
- Bitnami 執行個體：bitnami
- Plesk 執行個體：ubuntu
- cPanel WHM實例 (E)：centos

如需執行[個體作業系統的詳細資訊](#)，請參閱在 Lightsail 中選擇映像檔。

若要進一步了解SSH，請參閱[SSH並連接到您的 Amazon Lightsail 執行個體](#)。

## 使用 PuTTY 連接至 Lightsail 的執行個體 TTY

您可以使用像 PuTTY 這樣的用SSH戶端連線TTY到您的 Amazon Lightsail 執行個體。PuTTY 需要您的私SSH鑰的副本。您可能已經擁有金鑰，或者您可能想要使用 Lightsail 建立的 key pair。無論何者，我們都能滿足您。如需有關的詳細資訊SSH，請參閱[SSH金鑰配對](#)。本主題將逐步引導您下載 key pair 並設定 PuTTY 連線TTY至執行個體的步驟。

本指南中描述的連接至執行個體的方法是許多方法中的一種。如需其他方法的詳細資訊，請參閱[SSH金鑰配對](#)。

若要在 Lightsail 中連線到 Linux 或 Unix 執行個體，最簡單的方法是使用 Lightsail 主控台中提供的瀏覽器型用SSH戶端。如需詳細資訊，請參閱[在 Amazon Lightsail 中連線到 Linux 或 Unix 執行個體](#)。

### 必要條件

- 您需要在 Lightsail 中執行中的執行個體。如需詳細資訊，請參閱[在 Amazon Lightsail 中建立執行個體](#)。
- 我們建議您建立靜態 IP 位址並將其附加至執行個體，如此一來，TTY如果您的公用 IP 位址稍後變更，就不必重新設定 PuTTY。如需詳細資訊，請參閱[建立靜態 IP 並將其附接至執行個體](#)。

### 步驟 1：下載並安裝 PuTTY

PuTTY是一個免費實現SSH的視窗。在 PuTTY [網站](#) 上了解有關 PuTTY 的更多信息，包括與不允許加密的國家/地區有關的限制。如果您已經擁有 PuTTY，則可以跳到步驟 2。

1. 從以下鏈接下載 PuTTY 安裝程序或可執行文件：[下載 PuTTY](#)。

如果您需要決定要選擇哪個下載的協助，請參閱 [PuTTY 文件](#)。我們建議使用最新版本。

2. 在配置 Pu 之前，請轉到步驟 2 以獲取您的私鑰 TTY。

## 步驟 2：準備好您的私有金鑰

您有幾個選項可取得您的私有金鑰。您可能想要使用 Lightsail 產生的預設私密金鑰，您可能希望 Lightsail 為您建立新的私密金鑰，或者您可能已經擁有來自其他服務的私密金鑰。這些選項的步驟皆列於下列程序：

1. 登入主 [Lightsail 台](#)。
2. 在最上方的導覽列中選擇 Account (帳戶)，然後從下拉式清單中選擇 Account (帳戶)。
3. 選擇 [SSH金鑰] 索引標籤。
4. 根據您偏好使用的私有金鑰，選擇以下其中一個選項：
  - 若要使用 Lightsail 產生的預設私密金鑰，請在頁面的「預設金鑰」區段中，選擇執行個體所在位 AWS 區域 置之預設私密金鑰旁邊的下載圖示。

### Default keys

With default key pairs, you can connect to Linux instances using an SSH client, and retrieve administrator passwords for Windows instances.

You can download or delete your default key pairs. You can create one default key per AWS Region where you previously created resources.

[+ Create key pair](#)

Region name	Region code	Created		
Frankfurt	eu-central-1	April 27, 2018, 3:14 PM		
Ireland	eu-west-1	April 27, 2018, 3:14 PM		
Mumbai	ap-south-1	April 20, 2018, 2:54 PM		
Ohio	us-east-2	February 2, 2022, 4:17 PM		
Oregon	us-west-2	April 19, 2018, 9:11 AM		
Seoul	ap-northeast-2	August 23, 2018, 9:11 AM		
Singapore	ap-southeast-1	June 20, 2018, 3:45 PM		
Stockholm	eu-north-1	May 13, 2021, 10:03 AM		
Sydney	ap-southeast-2	April 30, 2019, 3:51 PM		

- 若要在 Lightsail 中建立新的 key pair，請在頁面的 [自訂金鑰] 區段中選擇 [建立 key pair]。選擇執行個體所 AWS 區域 在的位置，然後選擇 [建立]。輸入名稱，然後選擇 Generate key pair (產生金鑰對)。您將會看到私有金鑰的下載選項。

#### Important

您只能下載私有金鑰一次。將金鑰儲存在安全的位置。

- 若要使用自己的金鑰對，請選擇 Upload New (上傳新項目)。選擇執行個體所 AWS 區域 在的位置，然後選擇 [上傳]。選擇 Upload file (上傳檔案)，然後在您的本機磁碟機中找到檔案。當您準備好將公開金鑰檔案上傳至 Lightsail 時，請選擇 [上傳金鑰]。
5. 如果您下載了私密金鑰，或是在 Lightsail 中建立了新的私密金鑰，請務必將 .pem 金鑰檔案儲存在您可以輕鬆找到的位置。

我們也建議您設定該檔案的許可，讓其他人無法讀取檔案。

### 步驟 3：uTTYgen 使用您的 Lightsail 鑰設定 P

現在，你有你的 .pem 密鑰文件的副本，你可以設置 PuTTY 使用 PuTTY 密鑰生成器 (PuTTYgen)。

1. 啟動 PuTTYgen (例如，從「開始」功能表中選擇「所有程式」、「Pu」TTY、「P」uTTYgen)。
2. 選擇載入。

依預設，PuTTYgen 會顯示副檔名為 .ppk 檔案。若要尋找 .pem 檔案，請選擇顯示所有檔案類型的選項。

3. 選擇 lightsailDefaultKey.pem，然後按下 Open (開啟)。

PuTTYgen 確認您已成功匯入金鑰，然後您可以選擇 [確定]。

4. 選擇 Save private key (儲存私有金鑰)，然後確認您不想要使用密碼短語來進行儲存。

如果您選擇建立密碼作為額外的安全性措施，請記得每次使用 PuTTY 連線至執行個體時，都必須輸入密碼。

5. 指定儲存私密金鑰的名稱和位置，然後選擇 Save (儲存)。
6. 關閉 PuTTYgen。

## 步驟 4：TTY使用私密金鑰和執行個體資訊完成 Pu 的設定

您快完成了！請稍等，我們將進行最後一個變更。

1. 打開普TTY。
2. 從 Lightsail，從執行個體管理頁面取得公用 [IP 位址](#) (希望您使用的是靜態 IP 位址)。

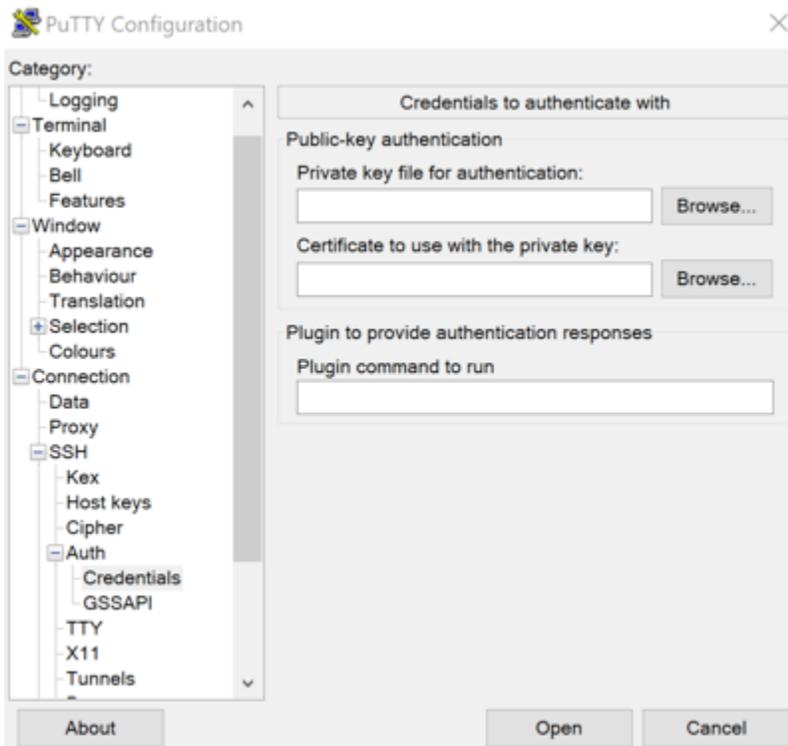
您可以從 Lightsail 首頁取得公用 IP 位址，或選擇執行個體以檢視相關詳細資訊。

3. 將公有 IP 地址輸入 (或貼上) 至 Host Name (or IP address) (主機名稱 (或 IP 地址)) 欄位。

### Note

Lightsail 實體SSH上的連接埠 22 已開啟，因此請接受預設連接埠。

4. 在 [連線] 下，展開SSH並 [驗證]，然後選擇 [認證]。



5. 選擇 Browse (瀏覽) 以導覽至您在上個步驟中建立的 .ppk 檔案，然後選擇 Open (開啟)。
6. 再次選擇開啟，然後選擇是，即表示在日後信任此連線。
7. 根據您的執行個體作業系統，使用以下其中一個預設的使用者名稱登入：

- AlmaLinux, Amazon Linux 2, Amazon Linux 2023, CentOS 流 9, 免費BSD和開放SUSE的執行個體：ec2-user

- Debian 執行個體 : admin
- Ubuntu 執行個體 : ubuntu
- Bitnami 執行個體 : bitnami
- Plesk 執行個體 : ubuntu
- cPanel WHM實例 (E) : centos

如需有關執行個體作業系統的詳細資訊，請參閱[選擇映像](#)。

8. 請務必儲存您的連線以供日後使用。

## 後續步驟

如果您需要再次 Connect，請參閱使用 Pu [連線到以 Linux 為基礎的 UNIX 執行個體](#)。TTY

## 使用以下方式將檔案安全地傳輸至執行個體 SFTP

您可以使用 (檔案傳輸通訊協定) 連線至執行個體，在本機電腦與 Amazon Lightsail 中的 Linux 或 Unix 執行個體之間傳輸SSH檔案。若要這麼做，您必須取得執行個體的私密金鑰，然後使用它來設定用FTP戶端。本教學課程說明如何將 FileZilla FTP用戶端設定為連線至執行個體。這些步驟也可能適用於其他用FTP戶端。

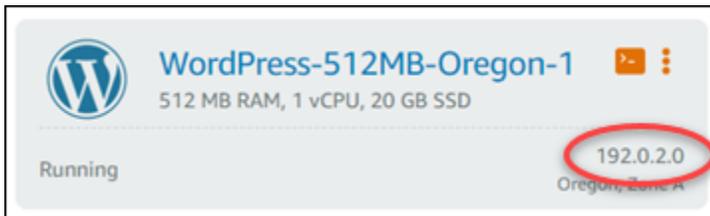
## 目錄

- [必要條件](#)
- [取得執行個體的SSH金鑰](#)
- [設定 FileZilla 並連線至您的執行個體](#)

## 必要條件

請先完成事前準備 (若尚未完成)：

- 下載並安裝 FileZilla 在本地計算機上。如需詳細資訊，請參閱下列下載選項：
  - [下載視窗 FileZilla 用戶端](#)
  - [下載適 FileZilla 用於 Mac OS X 的客戶端](#)
  - [下載 FileZilla 用戶端](#)
- 取得執行個體的公有 IP 地址。登入 [Lightsail 主控台](#)，然後複製顯示在執行個體旁邊的公用 IP 位址，如下列範例所示：



## 取得執行個體的SSH金鑰

完成下列步驟即可取得執行個體AWS區域的預設私密金鑰，這是使用連線至執行個體所需的 FileZilla。

### Note

如果您使用自己的金鑰組，或是使用 Lightsail 主控台建立 key pair，請找出您自己的私密金鑰，並使用該金鑰連線至執行個體。當您上傳自己的金鑰或使用 Lightsail 主控台建立 key pair 時，Lightsail 不會儲存您的私密金鑰。如果SFTP沒有私密金鑰，就無法連線至執行個體。

1. 登入主 [Lightsail](#) 台。
2. 在最上方的導覽列中選擇 Account (帳戶)，然後從下拉式清單中選擇 Account (帳戶)。
3. 選擇 [SSH金鑰] 索引標籤。
4. 向下捲動至頁面的 Default keys (預設金鑰) 區段。
5. 選擇您執行個體所在的區域之預設金鑰旁的 Download (下載)。

**Default keys**

With default key pairs, you can connect to Linux instances using an SSH client, and retrieve administrator passwords for Windows instances.

You can download or delete your default key pairs. You can create one default key per AWS Region where you previously created resources.

[+ Create key pair](#)

Region name	Region code	Created		
Frankfurt	eu-central-1	April 27, 2018, 3:14 PM		
Ireland	eu-west-1	April 27, 2018, 3:14 PM		
Mumbai	ap-south-1	April 20, 2018, 2:54 PM		
Ohio	us-east-2	February 2, 2022, 4:17 PM		
Oregon	us-west-2	April 19, 2018, 9:11 AM		
Seoul	ap-northeast-2	August 23, 2018, 9:11 AM		
Singapore	ap-southeast-1	June 20, 2018, 3:45 PM		
Stockholm	eu-north-1	May 13, 2021, 10:03 AM		
Sydney	ap-southeast-2	April 30, 2019, 3:51 PM		

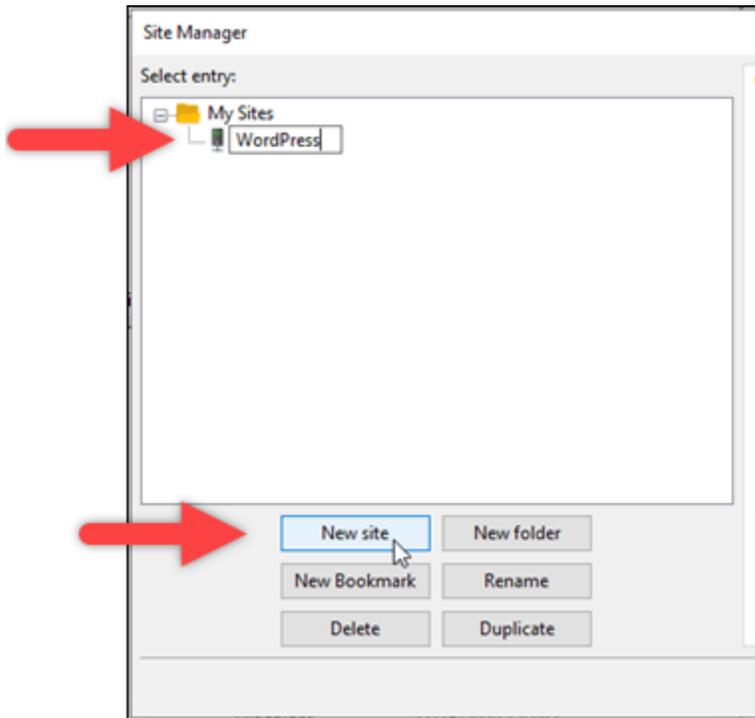


6. 將您的私有金鑰存放在本機磁碟上的安全位置。

設定 FileZilla 並連線至您的執行個體

完成下列步驟以設定連線 FileZilla 至執行個體。

1. 打開 FileZilla。
2. 選擇 File (檔案)、Site Manager (網站管理員)。
3. 選擇 New Site (新增網站)，然後為網站命名。

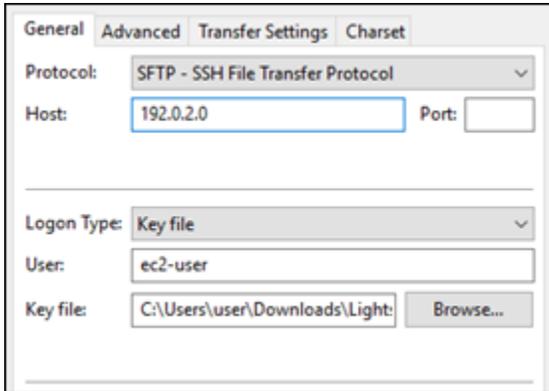


4. 在協議下拉列表中，選擇 SFTP-SSH 文件傳輸協議。
5. 在 Host (主機) 文字方塊中，輸入或貼上您執行個體的公有 IP 地址。
6. 在 Logon Type (登入類型) 下拉式選單中選擇 Key File (金鑰檔案)。
7. 在 User (使用者) 文字方塊中，根據您的執行個體作業系統，輸入以下其中一個預設的使用者名稱：
  - AlmaLinux, Amazon Linux 2, Amazon Linux 2023, CentOS 流 9, 免費BSD和開放SUSE的執行個體：`ec2-user`
  - Debian 執行個體：`admin`
  - Ubuntu 執行個體：`ubuntu`
  - Bitnami 執行個體：`bitnami`
  - Plesk 執行個體：`ubuntu`
  - cPanel WHM實例 (E)：`centos`

**⚠ Important**

如果您使用的使用者名稱不同於此處列出的預設使用者名稱，則可能需要授予使用者對執行個體的寫入許可。

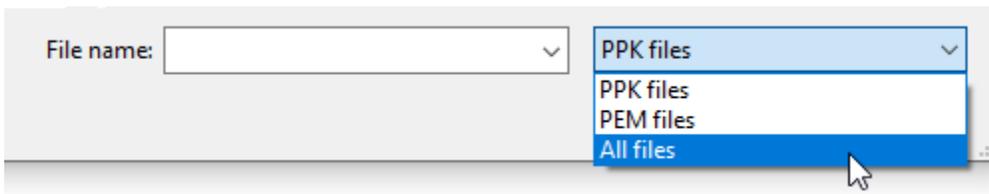
8. 在 Key File (金鑰檔案) 文字方塊旁選擇 Browse (瀏覽)。



9. 在此程序中，找出您先前從 Lightsail 主控台下載的私密金鑰檔案，然後選擇 [開啟]。

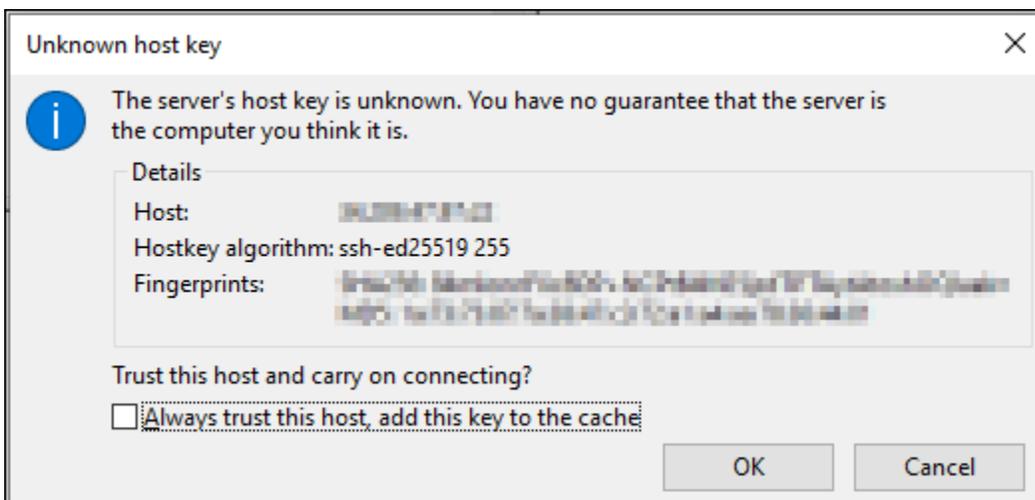
**Note**

如果您使用的是 Windows，搜尋 PEM 檔案時請將預設檔案類型變更為 All files (所有檔案)。



10. 選擇連線。

11. 您可能會看到類似以下範例的提示，指示主機金鑰不明。選擇 OK (確定) 以確認提示並連接至執行個體。



如果您看到類似以下範例的狀態訊息，您就成功連上了：

```
Status:    Connecting to 192.0.2.0. .
Status:    Connected to 192.0.2.0
Status:    Retrieving directory listing...
Status:    Listing directory /home/ec2-user
Status:    Directory listing of "/home/ec2-user" successful
```

如需有關使用的詳細資訊 FileZilla，包括如何在本機電腦和執行個體之間傳輸檔案，請參閱 [FileZilla Wiki 頁面](#)。

## 使用 Connect 至 Lightsail 執行個體 RDP

您可以使用 Lightsail 主控台中提供的瀏覽器型用RDP戶端，連線到 Amazon Lightsail 中的 Windows 伺服器執行個體。以瀏覽器為基礎的用RDP戶端不需要安裝軟體，而且您可以在建立 Windows Server 執行個體之後立即連線到 Windows Server 執行個體，它就會變成可用。連接到執行個體以在伺服器上執行管理任務，例如安裝軟體或設定 Web 應用程式。

您也可以使用自己的用RDP戶端連線至執行個體，例如 Windows 隨附的遠端桌面連線。如需 [有關設定自己RDP用戶端的詳細資訊](#)，請參閱 [使用遠端桌面連線用戶端連線到 Windows 執行個體](#)。若要連線到 Lightsail 中的 Linux 或 Unix 執行個體，請參閱 [Connect 到您的 Linux 或 Unix 執行個體](#)。

## Windows Server 執行個體的預設管理員密碼

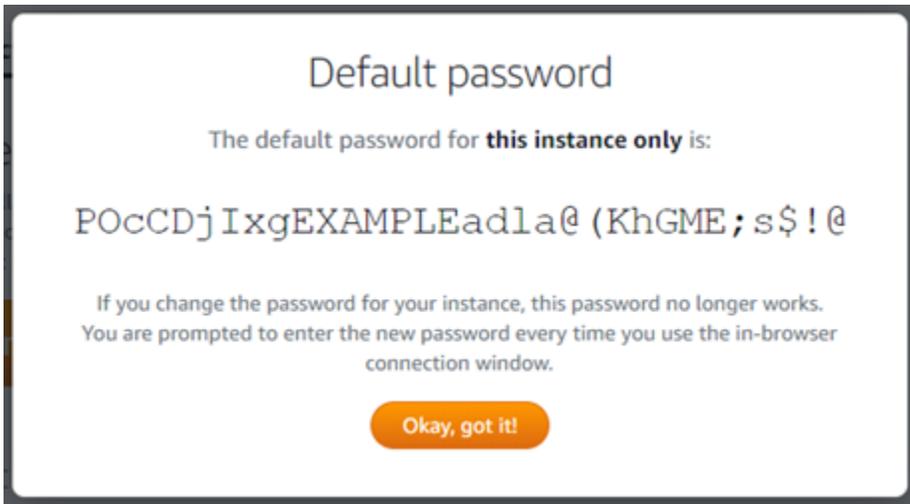
會在建立 Windows Server 執行個體時，將隨機產生的預設系統管理員密碼指派給它們。Lightsail 主控台中以瀏覽器為基礎的用RDP戶端會使用預設的管理員密碼登入您的執行個體。如果您變更執行個體上的系統管理員密碼，每次嘗試使用瀏覽器型用RDP戶端連線至執行個體時，系統都會提示您手動輸入新密碼。Lightsail 不會儲存您的新管理員密碼，也無法從您的執行個體擷取密碼。

### Important

如果遺失管理員密碼，將無法登入執行個體，也無法重設密碼。將新的系統管理員密碼儲存在安全的位置，以便日後遺失時可擷取密碼，例如 AWS Secrets Manager。如需詳細資訊，請參閱 [AWS Secrets Manager 使用手冊](#)。

您可以將系統管理員密碼變更回原始的預設管理員密碼，以避免每次使用瀏覽器型用RDP戶端存取執行個體時，系統都會收到提示。您可以在 [Lightsail 首頁](#) 中選擇「執行個體」索引標籤，找到原始的

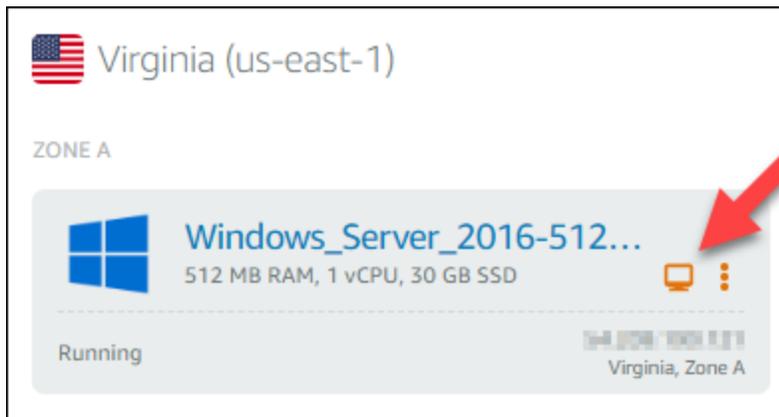
預設管理員密碼。選擇 Windows Server 執行個體的名稱，選擇 Connect (連線) 索引標籤，然後選擇 Show default password (顯示預設密碼)，檢視原始的預設管理員密碼，如下列範例所示。



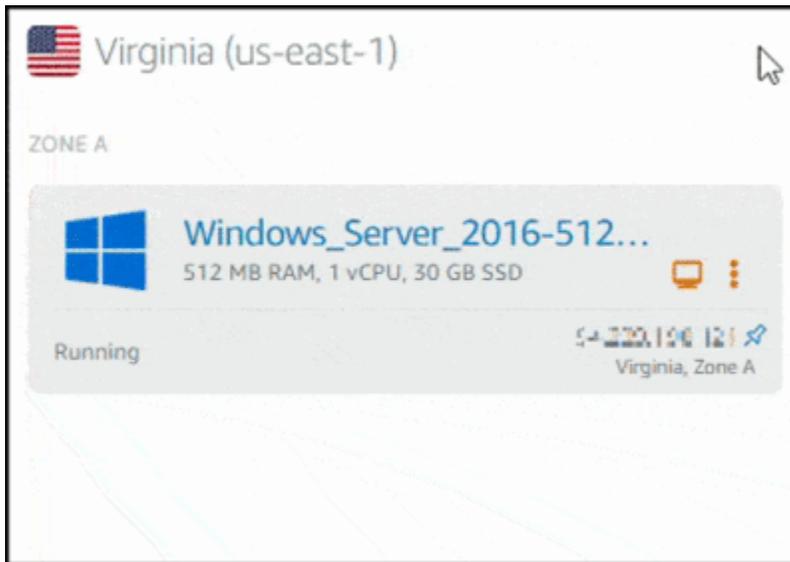
## 使用瀏覽器型用戶端 Connect 到 Windows 伺服器RDP執行個體

請使用下列程序，透過 Lightsail 主控台中的瀏覽器型用RDP戶端連線至 Windows 伺服器執行個體。

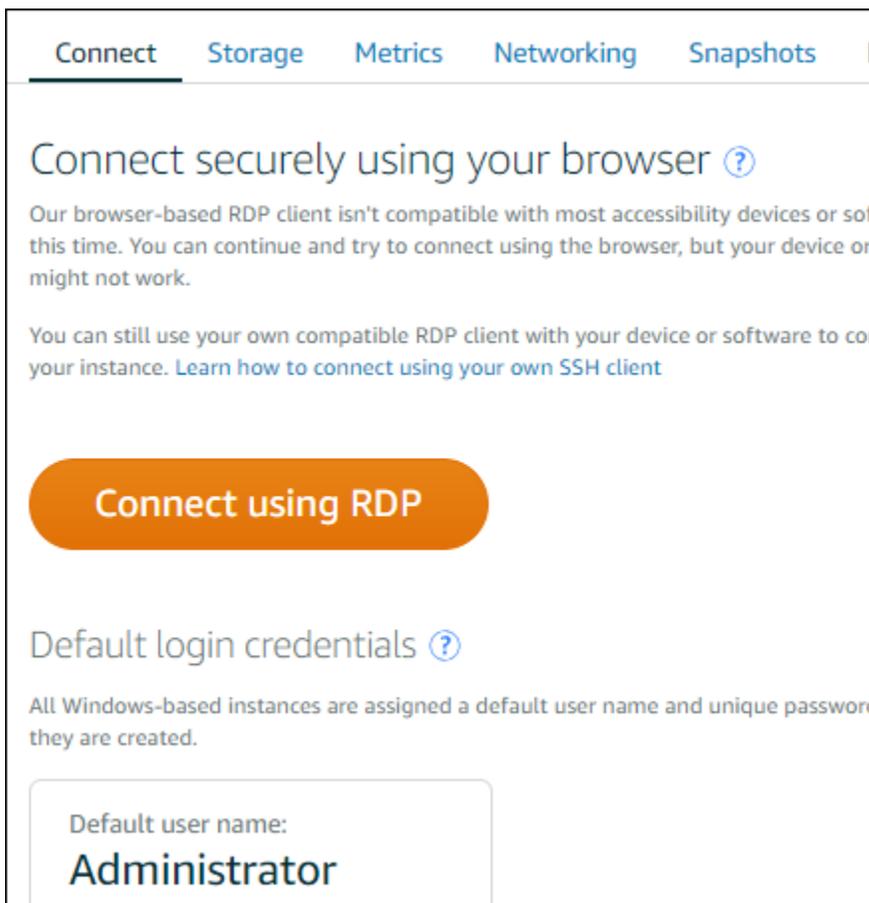
1. 登入主 [Lightsail](#) 台。
2. 使用下列其中一個步驟，存取您要連線之執行個體的瀏覽器用RDP戶端：
  - 選擇以瀏覽器為基礎的RDP用戶端圖示，如下列範例所示。



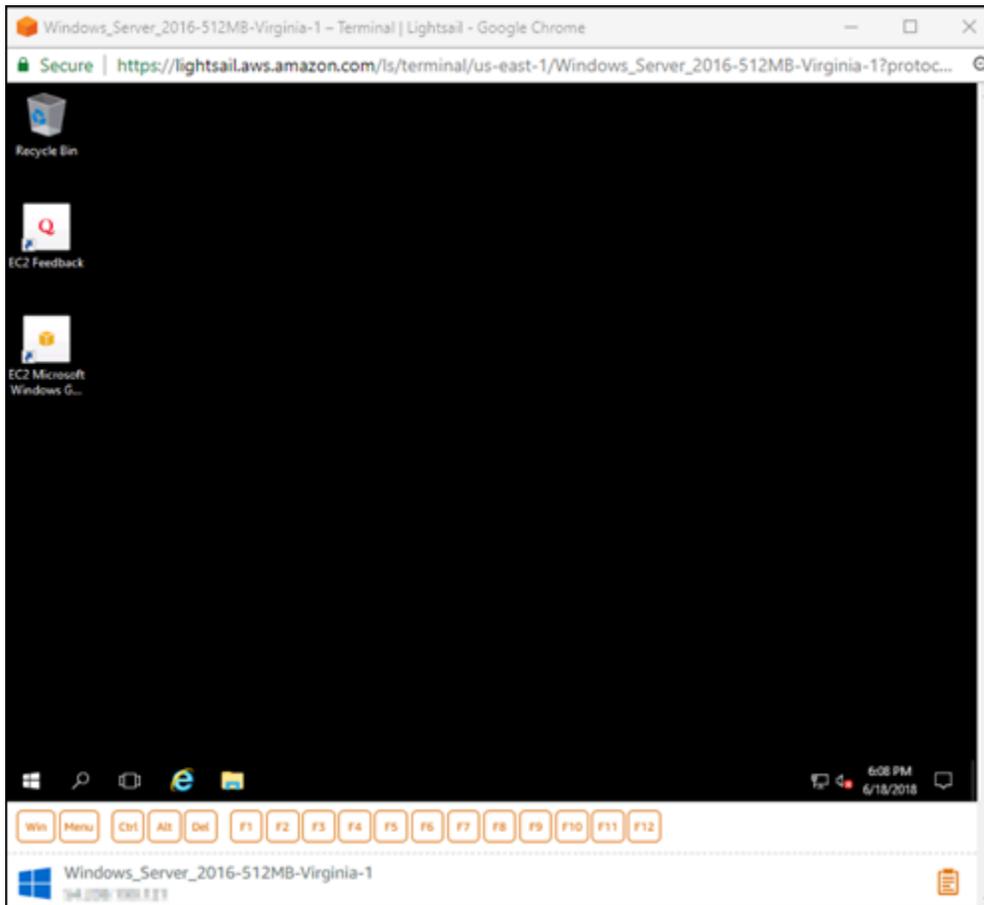
- 選擇動作選單圖示 (:)，然後選擇連接，如下列範例所示。



- 選擇執行個體的名稱，然後在 [Connect] 索引標籤上選擇 [Connect 方式] RDP。



當以瀏覽器為基礎的RDP用戶端開啟時，您可以開始與執行個體互動，並顯示 Windows 桌面，如下列範例所示。



### Note

[Connect] 索引標籤也會提供使用您自己的用RDP戶端連線所需的資訊，例如 Windows 執行個體的預設使用者名稱和密碼。如需有關設定自己用RDP戶端的詳細資訊，請參閱[使用遠端桌面連線用戶端在 Amazon Lightsail 中連線到 Windows 執行個體](#)。

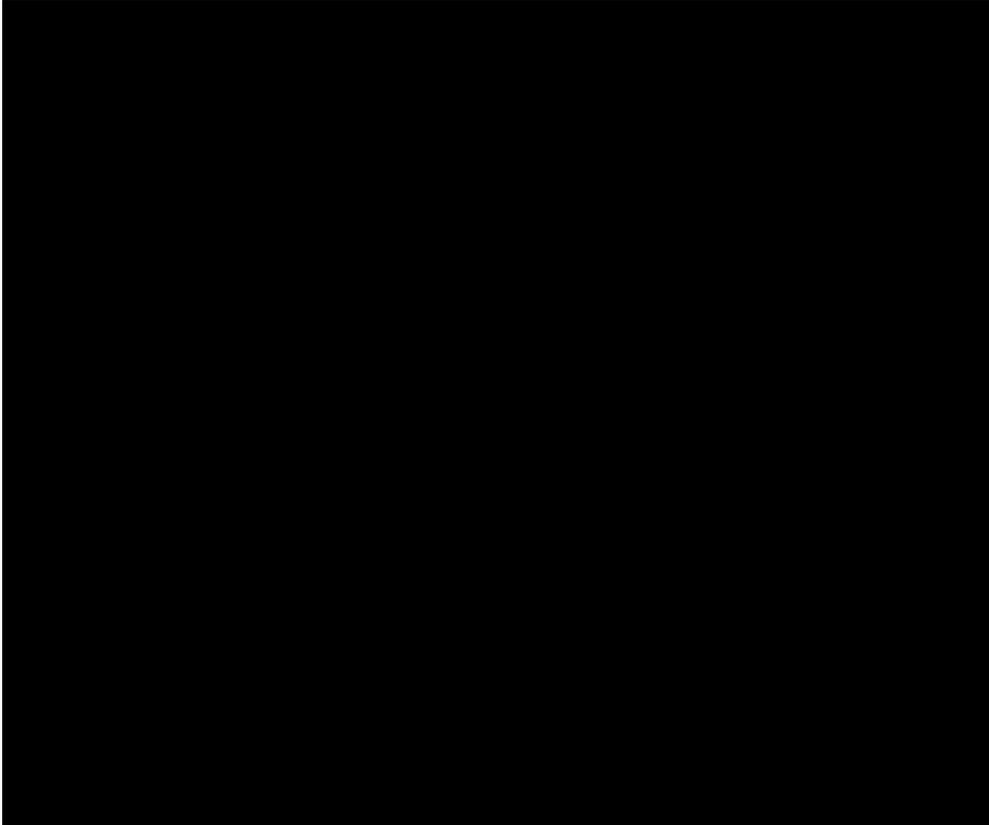
## 使用以瀏覽器為基礎RDP的用戶端與 Windows 執行個體互動

使用以瀏覽器為基礎的用RDP戶端，就像使用自己的本機 Windows 桌面一樣。RDP包括功能鍵和 Windows 專用的其他按鍵，可協助您與執行個體互動。以下各節將說明如何在中將文字複製到剪貼簿或從剪貼簿貼上文字RDP。

將文字貼到以瀏覽器為基礎RDP的用戶端

1. 在您的本機桌面反白文字，接著按 Ctrl+C (Ctrl+C) 或 Cmd+C (Cmd+C) 將其複製到您的本機剪貼簿。

2. 在瀏覽器RDP用戶端的右下角，選擇剪貼簿圖示。瀏覽器式RDP用戶端剪貼簿文字方塊隨即出現。
3. 按一下文字方塊，然後按 Ctrl+V 或 Cmd+V，將內容從本機剪貼簿貼上到以瀏覽器RDP為基礎的用戶端剪貼簿。
4. 在遠端桌面平台畫面的任何區域上按一下滑鼠右鍵，將文字從瀏覽器RDP用戶端剪貼簿貼上到遠端桌面平台畫面。



#### 從以瀏覽器為基礎RDP的用戶端複製文字

1. 在遠端桌面畫面上反白文字。
2. 在瀏覽器RDP用戶端的右下角，選擇剪貼簿圖示。瀏覽器式RDP用戶端剪貼簿文字方塊隨即出現。
3. 反白您要複製的文字，接著按 Ctrl+C (Ctrl+C) 或 Cmd+C (Cmd+C) 將文字複製到本機剪貼簿。您現在可以將複製的文字貼到本機桌面上任何地方。



## 變更執行個體的管理員密碼

當您建立以 Windows 伺服器為基礎的 Lightsail 執行個體時，我們會使用建立執行個體的 AWS 區域預設密碼。這使得使用基於瀏覽器的遠程桌面 ( RDP ) 客戶端以及遠程桌面連接之類的客戶端更容易進行連接。

### Important

我們強烈建議您讓 Lightsail 為您的執行個體產生密碼。由於我們不會儲存您的自訂密碼，因此如果您變更管理員密碼，您可能會失去 Lightsail 執行個體的存取權。

## 使用 Windows Server 變更管理員密碼

您可以使用 Windows Server 的 Change Password (變更密碼) 工具來變更管理員密碼。Del 在以 Windows 伺服器為基礎的 Lightsail 實體上輸入 Ctrl Alt + ，然後選擇 [變更密碼]。

## 使用以取得您的金 Lightsail 對的密文 AWS CLI

如果您在 Windows 伺服器型 Lightsail 執行個體上變更密碼，您可以使用 AWS Command Line Interface (AWS CLI) 取得可協助您解密密碼的資訊。

### 取得您的密文

1. 如果您尚未安裝和設定 AWS CLI，請先執行這項動作。

如需詳細資訊，請參閱[設定 AWS Command Line Interface 以與 Amazon Lightsail 搭配使用](#)。

2. 開啟命令提示字元或終端機。
3. 鍵入下列命令。

```
aws lightsail get-instance-access-details --instance-name my-instance
```

位置 *my-instance* 是您要取得相關資訊的執行個體名稱。

您將會看到類似下列的輸出。

```
{
  "accessDetails": {
    "username": "Administrator",
    "protocol": "rdp",
    "ipAddress": "12.345.678.910",
    "passwordData": {
      "ciphertext": "cipher",
      "keyPairName": "my-ohio-key"
    },
    "password": "",
    "instanceName": "2016-ohio-windows"
  }
}
```

4. 您可以搭配使用加密文字與任何可用的應用程式，進而解密密碼。

#### Note

Lightsail 不提供用於操作 .pem 檔案的公用程式。如果您需要轉換私鑰文件的格式，可以隨時使用免費和開源放源代碼的工具，例如 Linux 版「打開」和「Windows 版 base64」。

## 從具有遠端桌面的視窗 Connect 至 Lightsail 視窗執行個體

您可以使用 Windows 作業系統隨附的遠端桌面連線 (RDC) 用戶端連線到 Amazon Lightsail 中的 Windows 執行個體。RDC 會要求您使用 Windows 執行個體的管理員使用者名稱和密碼，這可以是建立執行個體時指派給執行個體的預設密碼，或是您自己的密碼 (如果您已變更預設密碼)。

本主題將逐步引導您從 Lightsail 主控台取得預設管理員密碼，並將 RDC 設定為連線至 Windows 執行個體的步驟。您也可以使用瀏覽器從 Lightsail 主控台連線至執行個體。如需詳細資訊，請參閱[使用 Web 型 RDP 用戶端連接至 Windows 執行個體](#)。

### 取得您 Windows 執行個體的預設管理員密碼

完成以下步驟以取得您 Windows 執行個體的預設管理員密碼，這是使用 RDC 連接到執行個體所需的密碼。

#### Note

如果您變更了預設管理員密碼，則 Lightsail 主控台中顯示的密碼將無法運作。您需要記住您的密碼。若沒有管理員密碼，您無法使用 RDC 連接到執行個體。

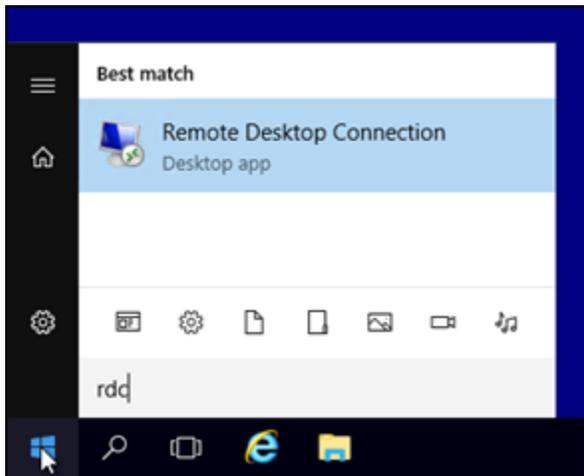
1. 登入主 [Lightsail](#) 台。
2. 選擇欲連接的 Windows 執行個體。
3. 在執行個體管理頁面的 Connect (連線) 索引標籤中，選擇 Show default password (顯示預設密碼)。
4. 反白所顯示的預設密碼，然後按下 Ctrl+C 或 Cmd+C 複製它。密碼現在位於剪貼簿中。

前往本指南下一節設定 RDC，並將密碼貼入用戶端中。

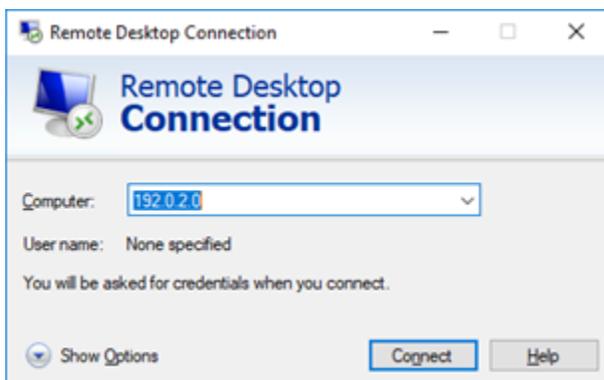
### 設定 RDC 並連接到您的 Windows 執行個體

完成以下步驟來設定 RDC 並連接到您的 Windows 執行個體。

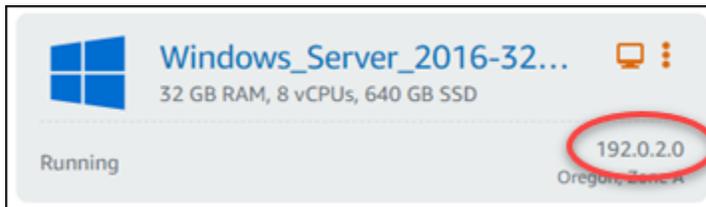
1. 開啟 Windows 功能表，然後搜尋 Remote Desktop Connection 或 RDC。
2. 在搜尋結果中選擇 Remote Desktop Connection (遠端桌面連線)。



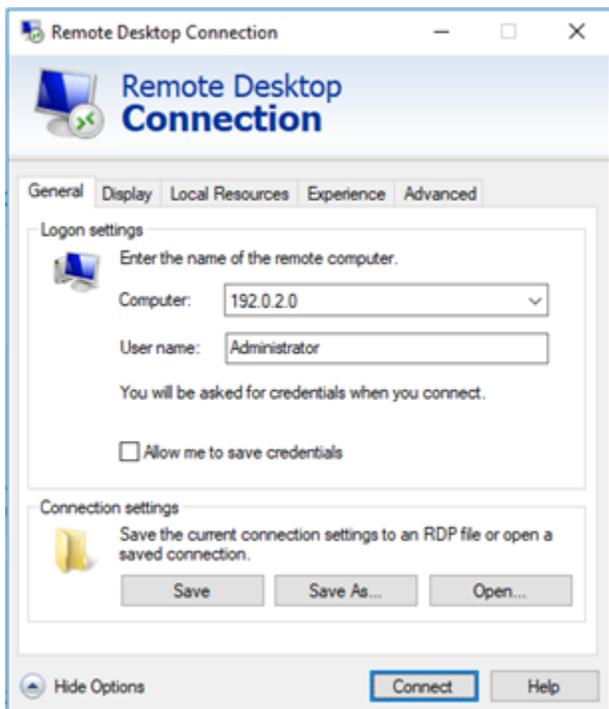
3. 在 Computer (電腦) 文字方塊中，輸入您 Windows 執行個體的公有 IP 地址。



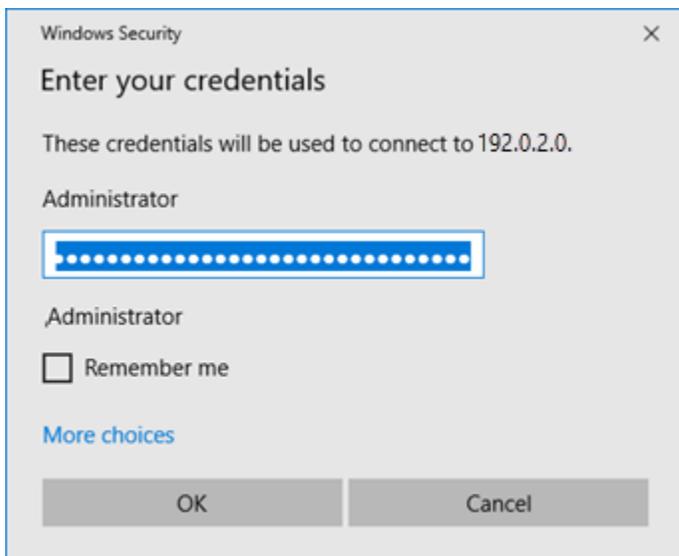
公用 IP 會顯示在 Lightsail 主控台中的執行個體旁邊，如下列範例所示：



4. 選擇 Show Options (顯示選項) 以檢視其他連線選項。
5. 在「使用者名稱」文字方塊中輸入 Administrator，這是 Lightsail 中所有 Windows 實體的預設使用者名稱。



6. 選擇連線。
7. 在出現的提示中，輸入或貼上您先前在此程序中從 Lightsail 主控台複製的預設管理員密碼，然後選擇 [確定]。



8. 在出現的提示中，選擇 Yes (是)，儘管憑證發生錯誤，還是連接到 Windows 執行個體。



在您連接到執行個體之後，應該會看到類似以下範例的畫面：



## 透過遠端桌面從 macOS Connect 線至 Lightsail 視窗執行個體

您可以使用 Microsoft 遠端桌面用戶端從 macOS 電腦連接到 Windows 執行個體。Microsoft 遠端桌面會要求您使用 Lightsail Windows 執行個體的系統管理員使用者名稱和密碼。這可以是建立執行個體時指派給執行個體的預設密碼，或是您自己的密碼 (如果您已變更預設密碼)。

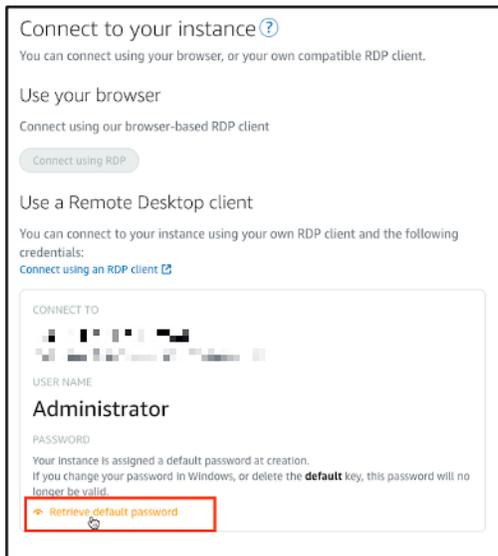
本主題將引導您完成從 Lightsail 主控台取得預設管理員密碼的步驟，以及將 Microsoft 遠端桌面設定為連線到 Windows 執行個體。您也可以使用瀏覽器從 Lightsail 主控台連線至執行個體。如需更多資訊，請參閱[使用 Microsoft 遠端桌面用戶端連接至 Windows 執行個體](#)。

## 取得 Windows 執行個體所需的連線資訊

您需要 Windows 執行個體的公有 IP 地址、使用者名稱和管理員密碼，才能使用 Microsoft 遠端桌面用戶端連接到該執行個體。

完成下列程序以取得所需資訊。

1. 登入主 [Lightsail](#) 台。
2. 選擇 Lightsail 首頁上的 Instances (執行個體) 索引標籤。
3. 記下您想要連接到之執行個體的公有 IP 地址。
4. 選擇您要連接之執行個體的名稱。
5. 選擇 Connect (連線) 索引標籤。
6. 選擇 Show default password (顯示預設密碼) 以取得執行個體的 Windows 管理員密碼。



畫面上的提示會顯示 Windows 執行個體的預設管理員密碼。

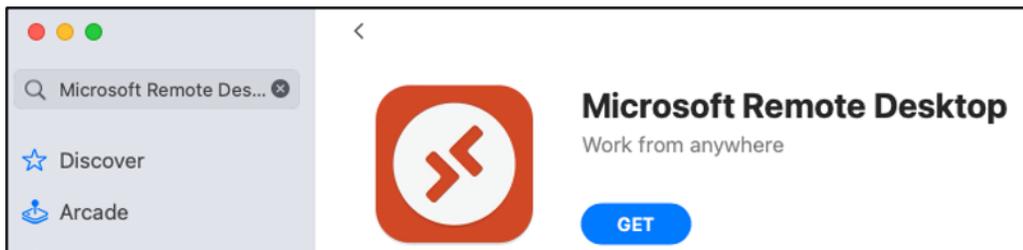


7. 複製管理員密碼。您會透過此資訊來使用 Microsoft 遠端桌面用戶端 (稍後於本指南提及) 登入執行個體。

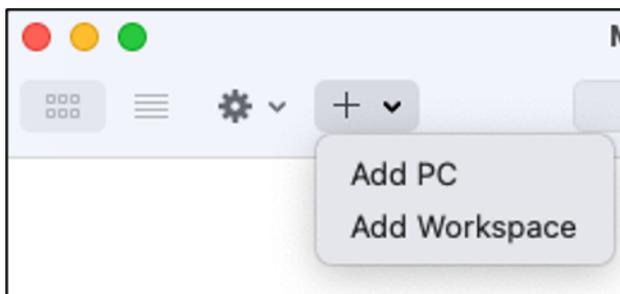
### 設定 Microsoft 遠端桌面並連接到執行個體

完成下列程序以便於 Mac 上安裝 Microsoft 遠端桌面用戶端，然後將其設定為連接到您的執行個體。

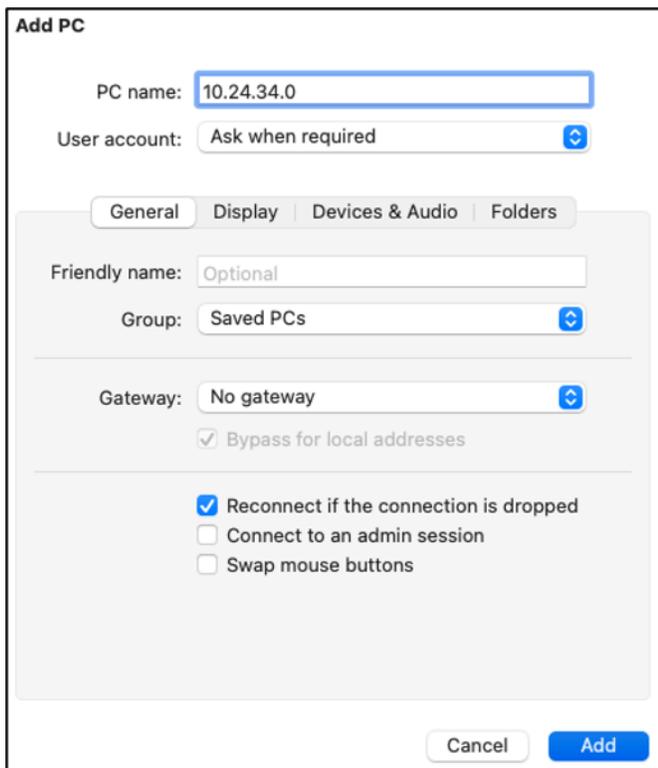
1. 在 Mac 上開啟 App Store，然後搜尋 Microsoft Remote Desktop (Microsoft 遠端桌面)。
2. 在搜尋結果中找出 Microsoft Remote Desktop (Microsoft 遠端桌面) App，然後選擇 GET (取得) 來安裝應用程式。



3. 安裝完成後，開啟 Microsoft Remote Desktop (Microsoft 遠端桌面)。
4. 在最上方，選擇加號 (+) 圖示，然後選擇新增 PC。



5. 在 PC name (PC 名稱) 文字方塊中，貼上執行個體的公有 IP 地址。
6. 選擇新增。



**Add PC**

PC name: 10.24.34.0

User account: Ask when required

General | Display | Devices & Audio | Folders

Friendly name: Optional

Group: Saved PCs

Gateway: No gateway

Bypass for local addresses

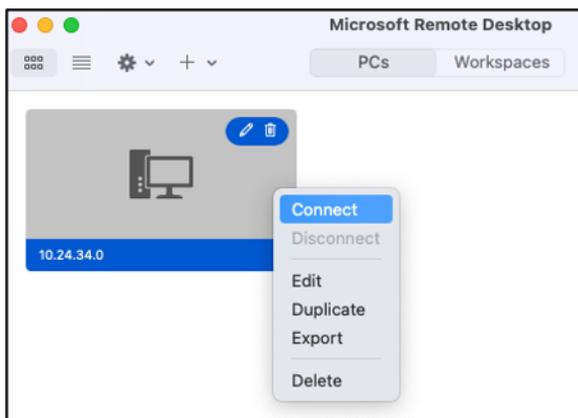
Reconnect if the connection is dropped

Connect to an admin session

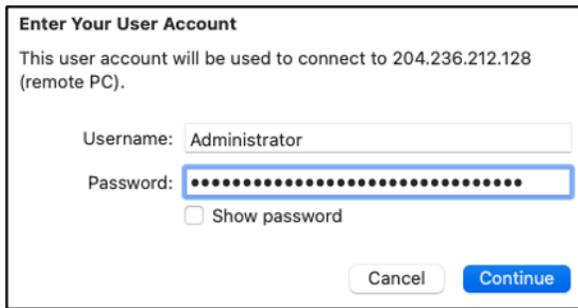
Swap mouse buttons

Cancel Add

7. 用滑鼠右鍵按一下執行個體的圖示，然後選擇 Connect (連接)。



8. 在 Username (使用者名稱) 文字方塊中輸入 Administrator (管理員)，並且將您稍早於本指南中取得的預設管理員密碼輸入 Password (密碼) 文字方塊。
9. 選擇 Continue (繼續) 以連接到您的執行個體。



您現在已連線至您的視窗執行個體。



## 使用管理 Lightsail 資源 AWS CloudShell

AWS CloudShell 這是一個以瀏覽器為基礎的預先驗證殼層，您可以直接從 Amazon Lightsail 主控台啟動。用 CloudShell 於從命令列介面管理您的 Lightsail 資源。您可以使用偏好的外殼執行 AWS Command Line Interface (AWS CLI) 命令 PowerShell，例如 Bash 或 Z 殼層。無需下載或安裝命令列工具即可執行此操作。當您啟動時 CloudShell，就會建立以 Amazon Linux 2 為基礎的[運算環境](#)。在此環境中，可以存取廣泛的預先安裝開發工具，例如 AWS CLI。如需預先安裝工具的完整清單，請參閱 CloudShell 使用者指南中的[預先安裝軟體](#)。

### 持久性儲存

有了 AWS CloudShell，您可以在每個儲存空間中使用高達 1 GB 的持續性儲存空 AWS 區域間，而無需額外費用。持續性儲存空間位於主目錄 (\$HOME) 中，而且對您來說是私有的。與在每個 Shell 工作階段結束後刪除的暫時環境資源不同，主目錄中的資料會在工作階段之間持續存在。

如果您停止 AWS CloudShell 在中使用 AWS 區域，資料會在上次工作階段結束後保留在該區域的永久性儲存空間中 120 天。120 天後，除非您採取行動，否則您的資料會自動從該區域的永久儲存中刪

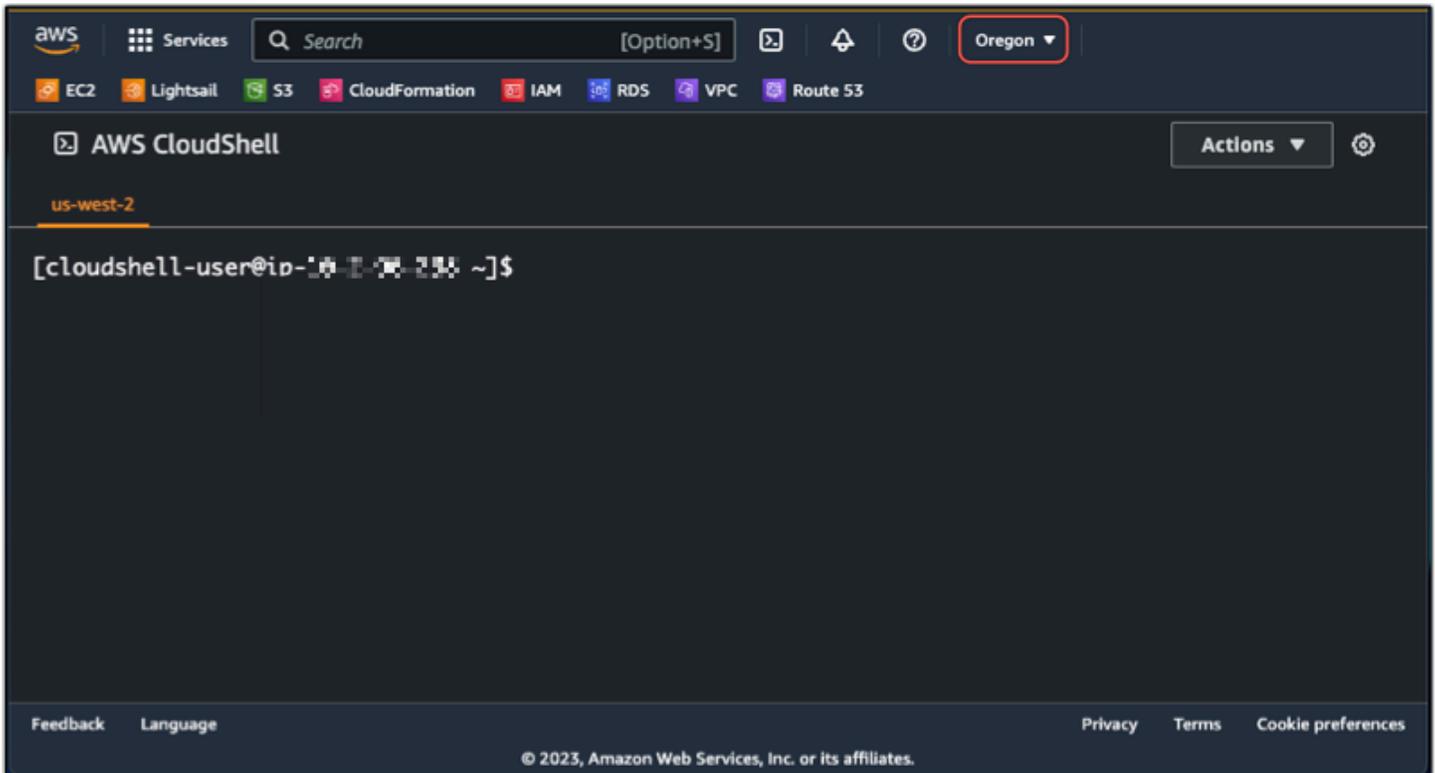
除。您可以通過 AWS CloudShell 再次啟動來防止刪除 AWS 區域。如需有關在永久儲存裝置中保留資料的詳細資訊，請參閱 CloudShell 使用者指南中的 [持續性儲存裝置](#)。

## AWS 區域

在 Lightsail 中，會在中開啟一個 CloudShell 工作階段 AWS 區域，為您的實體位置提供最低延遲。這表示 AWS 區域 可以在工作階段之間變更。請注意您的 CloudShell 工作階段位於哪個 AWS 區域-->，以便您可以使用 1 GB 的永久性儲存空間。若要變更工作階段的 AWS 區域，請選擇在新瀏覽器標籤中開啟圖示。這提供了在新瀏覽器視窗中存取 CloudShell 工作階段的選項。



在新瀏覽器標籤的導覽列中，選擇目前顯示的 AWS 區域 名稱。然後選擇您 AWS 區域 要切換到的目標。



若要取得有關的更多資訊 CloudShell，請參閱[CloudShell 使用者指南](#)。

## 啟動和使用 AWS CloudShell

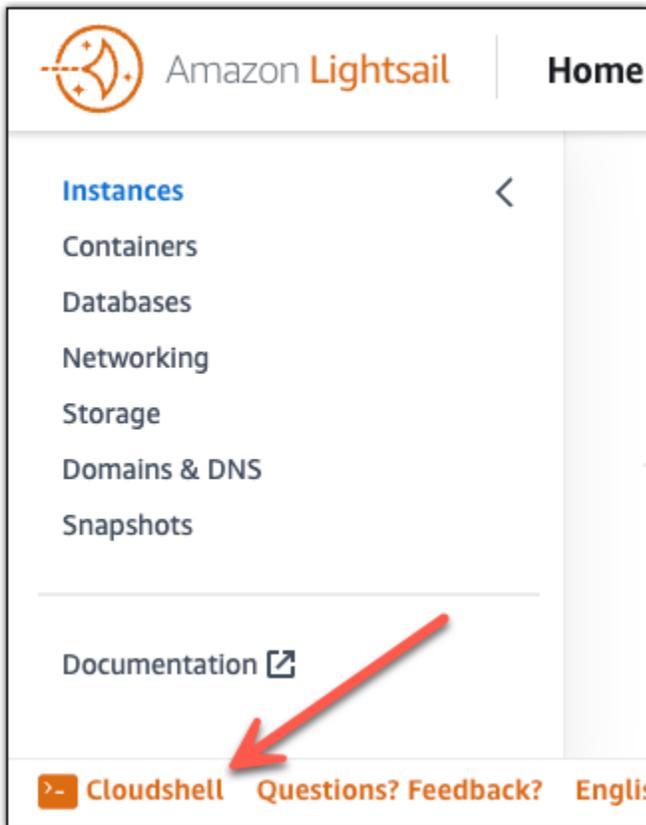
瞭解如何在 Lightsail 中啟動和使用 AWS CloudShell 工作階段。如果您沒有執行權限 CloudShell，則必須將`arn:aws:iam::aws:policy/AWSCloudShellFullAccess`原則新增至您正在使用的 AWS Identity and Access Management (IAM) 身分識別。如果您已附加`arn:aws:iam::aws:policy/AdministratorAccess`原則，您應該可以存取 CloudShell。如需詳細資訊，請參閱[???](#)。

### 啟動 AWS CloudShell

您可以 CloudShell 從亞馬遜控制台啟動。工作階段開始後，可以切換至偏好的 Shell，例如 Bash、PowerShell 或 Z shell。

請完成下列步驟，以在 Lightsail 中啟動新的 AWS CloudShell 工作階段：

1. 請使用 <https://lightsail.aws.amazon.com/>登 Lightsail 主控台。
2. 在主控台左下方的 [主控台] 工具列 CloudShell 上選擇。出現命令提示時，表示 Shell 已準備好開始互動。



3. (選用) 若要選擇要使用的預先安裝的 Shell，請在命令列提示中輸入下列其中一個程式名稱：

Bash : **bash**

如果切換至 Bash，則命令提示中的符號會更新為 \$。Bash 是中的預設外殼 AWS CloudShell。

PowerShell: **pwsh**

如果切換至 PowerShell，則指令提示下的符號會更新為 PS>。

Z Shell : **zsh**

如果切換至 Z Shell，則命令提示中的符號會更新為 %。

Example 示例 Lightsail API 命令 AWS CloudShell

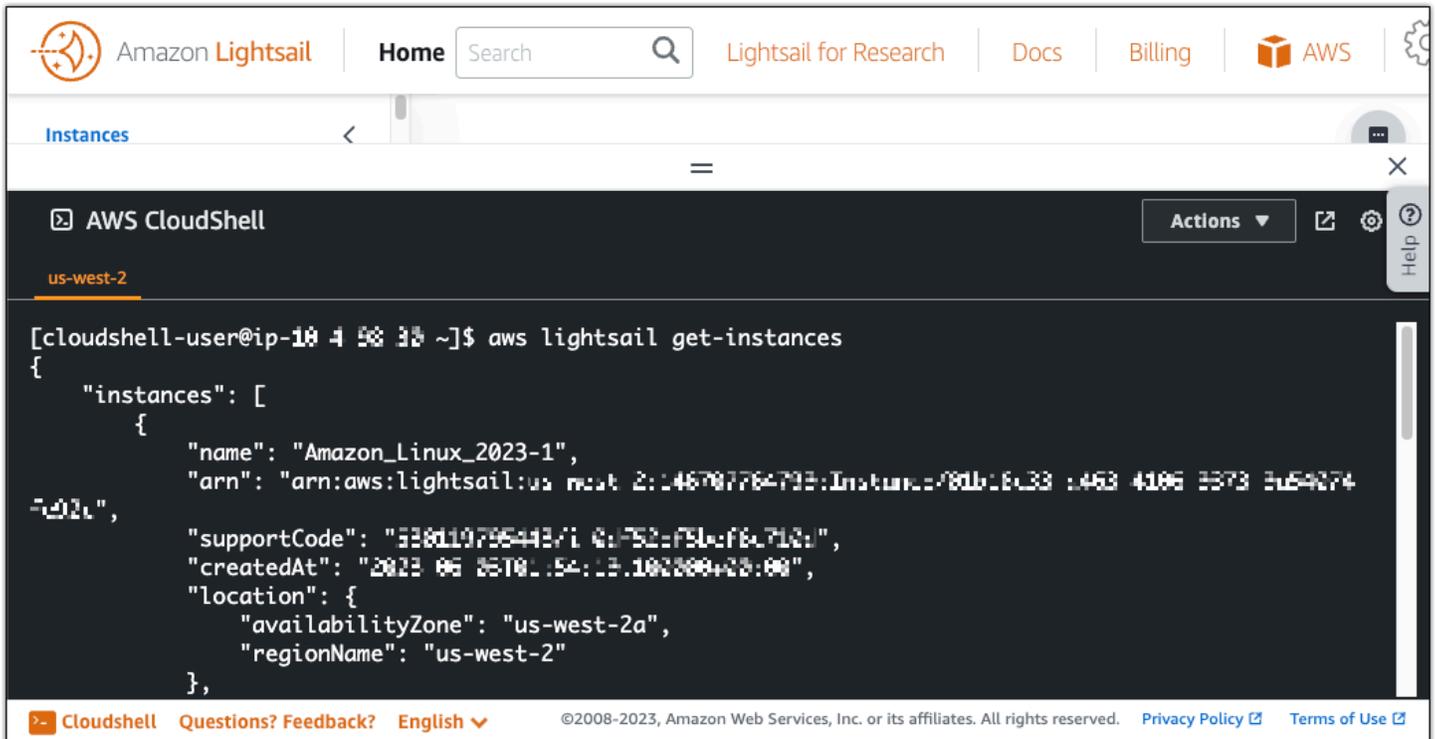
工 CloudShell 作階段中有多個預先安裝的命令列工具供您使用。在此範例中，您可以使用 Lightsail GetInstances API 作業來檢視 Lightsail 帳戶中的執行個體。若要進一步了解 GetInstances API 操作，請參閱亞馬遜 Lightsail API 參考資料 [GetInstances](#) 中的。

1. 請使用 <https://lightsail.aws.amazon.com/> 登 Lightsail 主控台。

2. 在主控制台左下方的 [主控台] 工具列 CloudShell 上選擇。
3. 出現提示後輸入以下命 AWS CloudShell 令：

```
aws lightsail get-instances
```

您現在應該會看到 Lightsail 帳戶中執行個體的完整清單。



The screenshot shows the AWS CloudShell interface. At the top, there's a navigation bar with the Amazon Lightsail logo, 'Home', a search box, and links for 'Lightsail for Research', 'Docs', 'Billing', and 'AWS'. Below this, the 'Instances' page is visible. The main area is a terminal window titled 'AWS CloudShell' with a sub-tab for 'us-west-2'. The terminal shows the command `aws lightsail get-instances` being executed, resulting in a JSON response. The response includes details for an instance named 'Amazon\_Linux\_2023-1', such as its ARN, support code, creation time, and location (us-west-2a).

```
[cloudshell-user@ip-10-4-58-35 ~]$ aws lightsail get-instances
{
  "instances": [
    {
      "name": "Amazon_Linux_2023-1",
      "arn": "arn:aws:lightsail:us-west-2:146707764735:Instance/8db16c33-1463-4106-b373-3a54274
7c02a",
      "supportCode": "338d11979544371-0-752-f51e-f6c712:",
      "createdAt": "2023-06-25T01:54:13.102889+00:00",
      "location": {
        "availabilityZone": "us-west-2a",
        "regionName": "us-west-2"
      }
    }
  ],
}
```

## 其他資訊

如需有關的詳細資訊，請參閱下列文件 AWS CloudShell：

- [Amazon Lightsail API 參考](#)
- [中的常見問題解答 AWS CloudShell](#)
- [支援的瀏覽器 AWS CloudShell](#)
- [疑難排解 AWS CloudShell](#)
- [AWS 服務 在中使用 AWS CloudShell](#)

## 在 Lightsail 中存取執行個體中繼資料服務 (IMDS) 和使用者資料

執行個體中繼資料 是關於您執行個體的資料，您可以用來設定或管理執行中的執行個體。執行個體中繼資料會分為幾個類別，例如主機名稱、事件及安全群組。您也可以使用執行個體中繼資料，存取您在啟動執行個體時指定的 使用者資料。例如，您可以指定設定您執行個體的參數，或是包含簡單的指令碼。執行個體同時也會包含動態資料，例如執行個體啟動時產生的執行個體身分文件。

### Important

雖然您只能在執行個體內部存取執行個體中繼資料和使用者資料，資料並未受到驗證或密碼編譯法保護。可直接存取執行個體的任何人，以及可能在該執行個體上執行的任何軟體，都能檢視其中繼資料。因此，您不應該將敏感性資料 (例如密碼或長期加密金鑰) 儲存為使用者資料。

## 使用執行個體中繼資料服務

您可以使用下列其中一種方法，從 Lightsail 中執行中的執行個體存取執行個體中繼資料：

- 執行個體中繼資料服務第 1 版 (IMDSv1) – 請求/回應方法
- 執行個體中繼資料服務第 2 版 (IMDSv2) – 工作階段導向方法

### Important

並非所有執行個體藍 Lightsail 支援 ImDSv2。使用 MetadataNoToken 執行個體指標追蹤對於正在使用 IMDSv1 的執行個體中繼資料服務所發出的呼叫次數。如需詳細資訊，請參閱[檢視執行個體指標](#)。

如需有關使用 IMDS 的詳細資訊，請參閱[設定執行個體中繼資料服務 \(IMDS\)](#)。

## 其他 IMDS 文件

可在《適用於 Linux 執行個體的 Amazon Elastic Compute Cloud 使用者指南》與《適用於 Windows 執行個體的 Amazon Elastic Compute Cloud 使用者指南》中找到以下 IMDS 文件：

### Note

在 Amazon EC2 中，執行個體藍圖稱為 Amazon Machine Image (AMI)。

- 對於 Linux 執行個體：
  - [設定執行個體中繼資料選項](#)
  - [擷取執行個體中繼資料](#)
  - [使用執行個體使用者資料](#)
  - [擷取動態資料](#)
  - [執行個體中繼資料分類](#)
  - [範例：AMI 啟動索引值](#)
  - [執行個體身分文件](#)
- 對於 Windows 執行個體：
  - [設定執行個體中繼資料選項](#)
  - [擷取執行個體中繼資料](#)
  - [使用執行個體使用者資料](#)
  - [擷取動態資料](#)
  - [執行個體中繼資料分類](#)
  - [範例：AMI 啟動索引值](#)
  - [執行個體身分文件](#)

## 在 Lightsail 上存取和設定執行個體中繼資料服務 (IMDS)

您可以使用下列任一種方法，從執行中的執行個體存取執行個體中繼資料：

- 執行個體中繼資料服務第 1 版 (IMDSv1) – 請求/回應方法
- 執行個體中繼資料服務第 2 版 (IMDSv2) – 工作階段導向方法

### Important

並非所有執行個體藍 Lightsail 支援 ImDSv2。使用 MetadataNoToken 執行個體指標追蹤對於正在使用 IMDSv1 的執行個體中繼資料服務所發出的呼叫次數。如需詳細資訊，請參閱 [檢視執行個體指標](#)。

依預設，您可以使用 IMDSv1 或 IMDSv2，或兩者。執行個體中繼資料服務會依據任何指定請求中是否存在 IMDSv2 特有的 PUT 或 GET 標頭來區分 IMDSv1 和 IMDSv2 請求。如需詳細資訊，請參閱 [透過](#)

## [EC2 執行個體中繼資料服務的增強功能，提高開放式防火牆、反向代理伺服器及 SSRF \(伺服器端請求偽造\) 弱點的防禦能力。](#)

您可以在每個執行個體上設定執行個體中繼資料服務，此類本機程式碼或使用者必須使用 IMDSv2。當您指定必須使用該 IMDSv2 時，IMDSv1 則無法繼續運作。如需詳細資訊，請參閱《Amazon Elastic Compute Cloud 使用者指南》中的[設定執行個體中繼資料選項](#)。

若要擷取執行個體中繼資料，請參閱《適用於 Linux 執行個體的 Amazon Elastic Compute Cloud 使用者指南》中的[擷取執行個體中繼資料](#)。

### Note

本節中的範例使用執行個體中繼資料服務的 IPv4 地址：169.254.169.254。如果您要從 IPv6 地址上的執行個體擷取執行個體中繼資料，請先確保您已啟用並改用 IPv6 地址：fd00:ec2::254。執行個體中繼資料服務的 IPv6 地址與 IMDSv2 命令相容。

## 執行個體中繼資料服務第 2 版的運作方式

IMDSv2 會使用工作階段導向請求。使用工作階段導向請求，您就能建立定義工作階段持續期間的工作階段字符，此期間最短 1 秒，最長可達 6 小時。在指定持續期間，您可以將相同的工作階段字符用於後續請求。在指定持續期間到期之後，您必須建立新的工作階段字符，才能使用未來請求。

### Important

從 Amazon 2023 啟動的 Lightsail 執行個體預設會設定 ImDSv2。

下列範例使用 Linux 和 PowerShell 殼層指令碼和 ImDSv2 來擷取頂層執行個體中繼資料項目。這些範例會執行下列操作：

- 使用 PUT 請求，建立持續六小時 (21,600 秒) 的工作階段字符
- 將工作階段字符標頭存放到名為 TOKEN (在 Linux 上) 或 token (在 Windows 上) 的變數中
- 使用字符請求最上層中繼資料項目

首先執行下列命令：

- 在 Linux 上：
  - 首先，使用下列命令產生字符。

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600" `
```

- 然後，使用字符透過下列命令產生最上層中繼資料項目。

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/
```

- 在 Windows 上：

- 首先，使用下列命令產生字符。

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

- 然後，使用字符透過下列命令產生最上層中繼資料項目。

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method GET -Uri http://169.254.169.254/latest/meta-data/
```

建立字符後，您可以重複使用直至其到期為止。在下列範例中，每個命令會取得用於啟動執行個體的藍圖 (Amazon Machine Image (AMI) ID)。上一個範例中的字符會被重複使用。其會存放在 \$TOKEN (在 Linux 上) 或 \$token (在 Windows 上) 中。

- 在 Linux 上：

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/ami-id
```

- 在 Windows 上：

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method GET -uri http://169.254.169.254/latest/meta-data/ami-id
```

當您使用 IMDSv2 請求執行個體中繼資料時，請求必須包含下列項目：

- 一個 **PUT** 請求 – 使用 PUT 請求啟動針對執行個體中繼資料服務的工作階段。PUT 請求會傳回一個字符，其必須包含在執行個體中繼資料服務的後續 GET 請求中。使用 IMDSv2 時，需要該字符才能存取中繼資料。

- 字符 – 在針對執行個體中繼資料服務的所有 GET 請求中包含該字符。字符使用方式設定為 required 時，不包含有效字符或字符已到期的請求會收到 401 - Unauthorized HTTP 錯誤碼。如需變更 Token 使用需求的相關資訊，請參閱《AWS CLI 命令參考》[update-instance-metadata-options](#)中的 `<`。
- 字符是執行個體特定金鑰。字符在其他執行個體上無效，而且如果您嘗試在產生字符的執行個體外部使用該字符，則會遭到拒絕。
- PUT 請求必須包含指定字符存留時間 (TTL) 的標頭，時間會以秒數表示。可將 TTL 指定為最多六小時 (21,600 秒)。字符會代表邏輯工作階段。TTL 會指定字符有效的時間長度，也就是工作階段的持續期間。
- 在字符到期後，若要繼續存取執行個體中繼資料，您必須使用另一個 PUT 請求建立新的工作階段。
- 您可以選擇重複使用字符或使用每個請求來建立新字符。對於少量請求，您每次需要存取執行個體中繼資料服務時，就能更輕鬆地產生和立即使用字符。但為了提升效率，您可以為字符指定更長的存留期間，並重複使用該字符，而不用在每次需請求執行個體中繼資料時寫入 PUT 請求。並行字符數量沒有實際限額，每個都代表它自己的工作階段。但 IMDS2 仍會受到正常執行個體中繼資料服務連線和調節限額的限制。如需詳細資訊，請參閱《適用於 Linux 執行個體的 Amazon Elastic Compute Cloud 使用者指南》中的[查詢限流](#)。

HTTP GET 及 HEAD 方法可在 IMDSv2 執行個體中繼資料請求中使用。如果 PUT 請求中包含 X-Forwarded-For 標頭，則會遭到拒絕。

依預設，PUT 請求在 IP 通訊協定等級的 1 回應跳轉限額 (存留時間)。如果需要更大的跳轉限額，您可以使用 `update-instance-metadata-options` 命令調整跳轉限額。例如，您可以需要較大的跳轉限額，才能與執行個體上執行之容器服務回溯相容。若要取得更多資訊，請參閱《指AWS CLI 令參考》[update-instance-metadata-options](#)中的。

## 轉換為使用 執行個體中繼資料服務第 2 版

可選擇使用 Instance Metadata Service Version 2 (IMDSv2)。Instance Metadata Service Version 1 (IMDSv1) 將持續無限期受到支援。如果您選擇使用 IMDSv2 進行移轉，我們建議您使用下列工具和轉換路徑。

### 協助轉換至 IMDSv2 的工具

如果您的軟體使用 IMDSv1，請使用下列工作，以協助將您的軟體重新設定為使用 IMDSv2。

- AWS 軟體：最新版本的 AWS 開發套件和 AWS CLI 支援的 ImDSv2。若要使用 IMDSv2，請確定您的執行個體具有最新版本的 AWS SDK 和 AWS CLI。若要取得有關更新的資訊 AWS CLI，請參

閱《使用指南》AWS CLI中的〈[安裝、更新和解除安裝AWS Command Line Interface](#)〉。所有 Amazon Linux 2 軟體套件都支援 IMDSv2。

- 執行個體指標：IMDSv2 使用字符支援的工作階段，而 IMDSv1 不使用。MetadataNoToken 執行個體指標會追蹤針對正在使用 IMDSv1 的執行個體中繼資料服務所發出的呼叫次數。透過追蹤此指標至零，您可以決定是否要升級所有軟體以使用 IMDSv2 及升級時間。如需詳細資訊，請參閱在 [Amazon Lightsail 中檢視執行個體指標](#)。
- Lightsail API 作業和命 AWS CLI 令的更新：對於現有的執行個體，您可以使用 [update-instance-metadata-options](#) AWS CLI 命令 (或 [UpdateInstanceMetadataOptions](#) API 作業) 來要求使用 ImDSv2。下列是範例命令。確保用實例的名稱替換 *InstanceName* 為實例的名稱，並使 *RegionName* 用 AWS 區域 您的實例所在的名稱。

```
aws lightsail update-instance-metadata-options --region RegionName --instance-name InstanceName --http-tokens required
```

### 建議路徑需要 IMDSv2 存取

使用上述工具時，我們建議您遵循此路徑來轉換到 IMDSv2：

#### 步驟 1：開始時

將在執行個體上使用角色認證的 AWS SDK AWS CLI、和軟體更新為 IMDSv2 相容版本。若要取得有關更新的資訊 AWS CLI，請參閱《[使用指南](#)》AWS CLI中的〈[升級到最新版本AWS Command Line Interface](#)〉。

然後，使用 IMDSv2 要求變更直接存取執行個體中繼資料的軟體 (換句話說，不使用 AWS SDK)。

#### 步驟 2：轉換期間

使用執行個體指標 MetadataNoToken 追蹤您的轉換進度。此指標會顯示對您執行個體上正在使用 IMDSv1 的執行個體中繼資料服務的呼叫次數。如需詳細資訊，請參閱[檢視執行個體指標](#)。

#### 步驟 3：所有執行個體上一切都準備就緒時

當執行個體指標 MetadataNoToken 記錄的 IMDSv1 用量為零時，即表示所有執行個體上一切都已準備就緒。在此階段，您可以要求透過指 [update-instance-metadata-options](#) 令使用 IMDSv2。您可以對執行中的執行個體進行這些變更，您也不需要重新啟動執行個體。

更新現有執行個體的執行個體中繼資料選項只能透過 Lightsail API 或 AWS CLI目前無法在 Lightsail 主控台中使用此功能。如需詳細資訊，請參閱[update-instance-metadata-options](#)。

## 其他 IMDS 文件

可在《適用於 Linux 執行個體的 Amazon Elastic Compute Cloud 使用者指南》與《適用於 Windows 執行個體的 Amazon Elastic Compute Cloud 使用者指南》中找到以下 IMDS 文件：

### Note

在 Amazon EC2 中，執行個體藍圖稱為 Amazon Machine Image (AMI)。

- 對於 Linux 執行個體：
  - [設定執行個體中繼資料選項](#)
  - [擷取執行個體中繼資料](#)
  - [使用執行個體使用者資料](#)
  - [擷取動態資料](#)
  - [執行個體中繼資料分類](#)
  - [範例：AMI 啟動索引值](#)
  - [執行個體身分文件](#)
- 對於 Windows 執行個體：
  - [設定執行個體中繼資料選項](#)
  - [擷取執行個體中繼資料](#)
  - [使用執行個體使用者資料](#)
  - [擷取動態資料](#)
  - [執行個體中繼資料分類](#)
  - [範例：AMI 啟動索引值](#)
  - [執行個體身分文件](#)

# 使用 Lightsail 區塊儲存磁碟擴充儲存空間和效能

系統磁碟為您提供執行工作負載所需的一致性和低延遲效能。使用 Lightsail 磁碟，您可以在幾分鐘內擴展或縮減使用量，並且只為佈建的內容支付低廉的價格。

您最多可以在以 Linux/Unix 為基礎或以 Windows Server 為基礎的執行個體上選擇 80 GB 系統磁碟。請參閱在 [Lightsail 中開始使用 Linux 型執行個體](#) 或 [開始使用 Windows 伺服器型執行個體](#)。

您也可以建立額外的區塊儲存磁碟，將更多儲存新增到您的虛擬私有伺服器上。請參閱 [建立區塊儲存磁碟並將其附接至 Linux 執行個體](#) 或 [建立區塊儲存磁碟並將其附接至 Windows Server 執行個體](#)。

## 區塊儲存磁碟

區塊儲存是一種儲存架構，能以「區塊」來管理資料。每個儲存區塊 (在 Lightsail 中稱為「磁碟」) 的作用類似於您可以連接至伺服器的個別硬碟。一般而言，您可以將額外的區塊儲存用於需要從核心服務區分特定資料的應用程式和軟體，以及保護應用程式資料不受執行個體和開機儲存磁碟故障或其他問題的影響。

Lightsail 提供用於區塊儲存的固態硬碟 (SSD)。此類區塊儲存可在合理價格和良好效能之間取得平衡。它旨在支援在 Lightsail 上執行的絕大多數工作負載。Lightsail 額外的區塊儲存磁碟可提供一致的效能，以及經常存取儲存資料的應用程式或軟體所需的低延遲。

### Note

對於需要持續 IOPS 效能或每個磁碟高輸送量的應用程式的客戶，或者對於執行 MongoDB、Cassandra 等大型資料庫的客戶，我們建議您使用 Amazon EC2 搭配 GP2 或佈建 IOPSSSD 儲存，而不是 Lightsail。

您可以在 Amazon EC2 用戶指南中了解有關 Amazon EBS [卷](#) 的更多信息。

## 磁碟配額

- 每個區域 20,000 GB。
- 每個磁碟上限為 16 TB，每個磁碟下限為 8 GB。
- 每個執行個體最多可有 15 個連接的磁碟和 1 個啟動磁碟區磁碟。

## 建立區塊儲存磁碟並將其連接至 Linux 執行個體

您可以為 Amazon Lightsail 執行個體建立和連接其他區塊儲存磁碟。建立額外的磁碟之後，您需要連線至以 Linux 為基礎的 Lightsail 執行個體，然後格式化並掛接磁碟。

本主題說明如何使用 Lightsail 建立新磁碟並將其附加。它還說明如何使用連接到以 Linux/UNIX 為基礎的執行個體SSH，以便您可以格式化和掛接連接的磁碟。

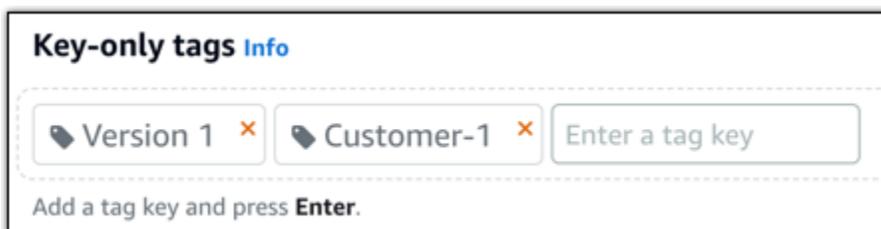
如果您擁有 Windows Server 型執行個體，請參閱以下主題：[建立區塊儲存磁碟並將其附接至 Windows Server 執行個體](#)。

### 步驟 1：建立新的磁碟並將其連接至您的執行個體

1. 在 Lightsail 首頁上，選擇「儲存空間」。
2. 選擇 Create disk (建立磁碟)。
3. 選擇 Lightsail 執行個體所在的 AWS 區域 和可用區域。
4. 選擇大小。
5. 輸入磁碟的名稱。

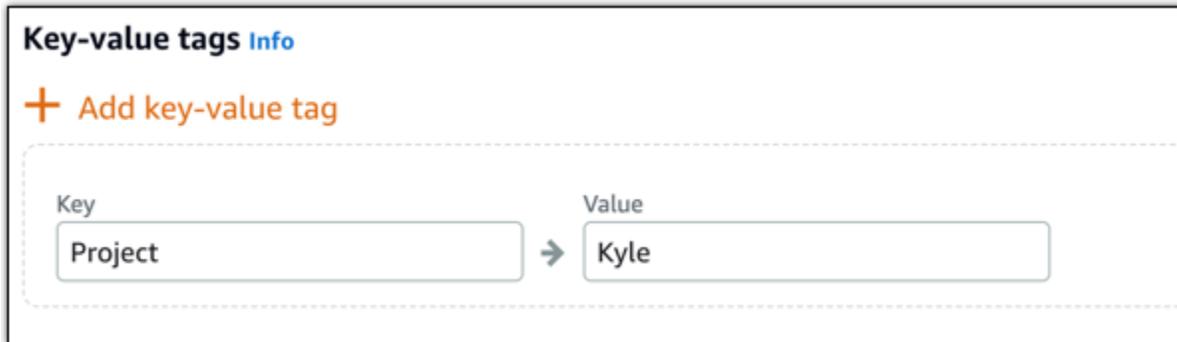
資源名稱：

- 每個 Lightsail 帳戶 AWS 區域 中的每個項目都必須是唯一的。
  - 必須包含 2 至 255 個字元。
  - 開頭和結尾必須是英數字元或數字。
  - 可以包含英數字元、數字、句點、破折號和底線。
6. 選擇下列其中一個選項以新增標籤至您的磁碟：
    - Add key-only tags (新增僅索引鍵標籤) 或 Edit key-only tags (編輯僅索引鍵標籤) (若標籤已新增)。在標籤索引鍵文字方塊中輸入新的標籤，接著按 Enter (輸入)。輸入標籤以新增之後，請選擇 Save (儲存)，如果不要新增則選擇 Cancel (取消)。



- Create a key-value tag (建立索引鍵值標籤)，接著將索引鍵輸入 Key (索引鍵) 文字方塊，將值輸入 Value (值) 文字方塊。完成輸入標籤後，請選擇 Save (儲存)，如果不要新增則選擇 Cancel (取消)。

鍵值標籤在儲存前一次只能新增一個。若要新增超過一個索引鍵值標籤，請重複之前的步驟。



Key-value tags Info

+ Add key-value tag

Key: Project → Value: Kyle

#### Note

如需有關僅索引鍵和索引鍵值標籤的詳細資訊，請參閱[標籤](#)。

7. 選擇 Create disk (建立磁碟)。

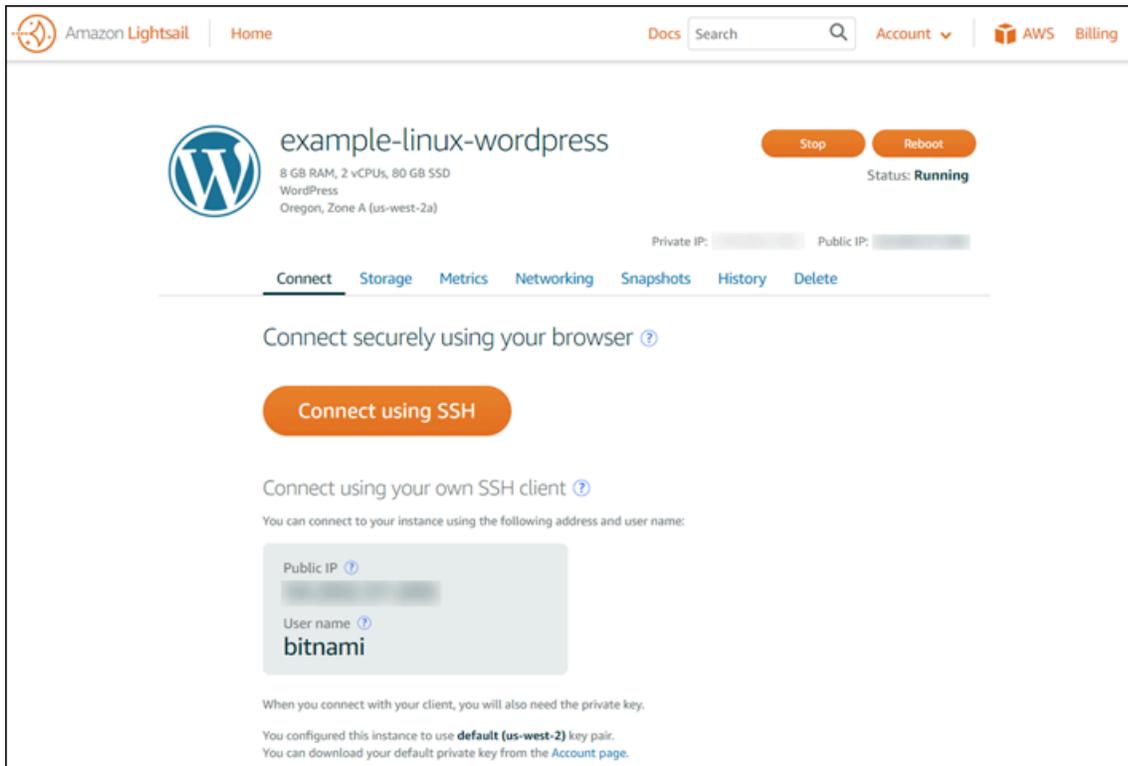
幾秒鐘後，磁碟就會建立，而您會看到新的磁碟管理頁面。

8. 從清單選擇執行個體，接著選擇 Attach (連接) 將新的磁碟連接至執行個體。

## 步驟 2：連接執行個體以格式化和掛載磁碟

1. 建立並連接磁碟後，請返回 Lightsail 中的執行個體管理頁面。

Connect (連接) 索引標籤會依預設顯示。



2. 選擇 [Connect 方式] SSH 以連線至您的執行個體。
3. 在終端機視窗中輸入以下命令：

```
lsblk
```

的輸出 `lsblk` 會省略磁碟路徑的 `/dev/` 前置詞。

### Note

我們在 2023 年 6 月 29 日更新了 Lightsail 執行個體的基礎硬體。在下列範例中，上一代執行個體的裝置名稱會顯示為 `/dev/xvda`。在此日期之後建立的執行個體的裝置名稱會顯示為 `/dev/nvme0n1`。

### Current generation instances

在下列範例輸出中，根磁碟區 (`nvme0n1`) 有兩個分割區 (`nvme0n1p1` 和 `nvme0n1p128`)，而額外的磁碟區 (`nvme1n1`) 沒有分割區。

```
[ec2-user ~]$ sudo lsblk
NAME          MAJ:MIN RM  SIZE RO  TYPE MOUNTPOINT
```

```
nvme1n1      259:0    0  30G  0 disk /data
nvme0n1      259:1    0  16G  0 disk
##nvme0n1p1  259:2    0   8G  0 part /
##nvme0n1p128 259:3    0   1M  0 part
```

## Previous generation instances

在下列範例輸出中，根磁碟區 (xvda) 有一個分割區 (xvda1)，而額外的磁碟區 (xvdf) 沒有分割區。

```
[ec2-user ~]$ sudo lsblk
NAME      MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda      202:0    0  16G  0 disk
##xvda1   202:1    0   8G  0 part /
xvdf      202:80   0  24G  0 disk
```

- 判斷是否在磁碟上建立檔案系統。新磁碟是原始的區塊型儲存設備，您必須先在這些磁碟區上建立檔案系統，才能掛載和使用它們。從快照還原的磁碟可能已經有檔案系統了。如果您在現有檔案系統上建立新的檔案系統，此操作會覆寫您的資料。

使用以下內容來確定您的磁盤是否具有文件系統。如果您的磁碟沒有檔案系統，請繼續執行步驟 2.5。如果您的磁碟有檔案系統，請跳至步驟 2.6。

## Current generation instances

```
sudo file -s /dev/nvme1n1
```

您應該會看到以下在全新磁碟上的輸出。

```
/dev/nvme1n1: data
```

如果您看到類似以下的輸出，這表示您的磁碟已經有檔案系統了。

```
/dev/nvme1n1: SGI XFS filesystem data (blksz 4096, inosz 512, v2 dirs)
```

## Previous generation instances

```
sudo file -s /dev/xvdf
```

您應該會看到以下在全新磁碟上的輸出。

```
/dev/xvdf: data
```

如果您看到類似以下的輸出，這表示您的磁碟已經有檔案系統了。

```
/dev/xvda1: Linux rev 1.0 ext4 filesystem data, UUID=1701d228-e1bd-4094-a14c-12345EXAMPLE (needs journal recovery) (extents) (large files) (huge files)
```

5. 使用以下命令在磁盤上創建一個新的文件系統。以下列項目取代裝置名稱 (例如 `/dev/nvme1n1`) *device\_name*。根據應用程式的需求或作業系統的限制，您可以選擇不同的檔案系統類型，例如 `ext3` 或 `ext4`。

### Important

此步驟假設您要掛載空的磁碟。如果您要掛載的磁碟已有資料 (例如，從快照還原的磁碟)，掛載磁碟之前請不要使用 `mkfs`。請改為跳至步驟 2.6 並建立掛載點。否則，您會格式化磁碟並刪除現有的資料。

## Current generation instances

```
sudo mkfs -t xfs device_name
```

您應該會看到類似以下的輸出。

```
meta-data=/dev/nvme1n1      isize=512    agcount=16, agsize=1048576 blks
      =                       sectsz=512   attr=2, projid32bit=1
      =                       crc=1        finobt=1, sparse=1, rmapbt=0
      =                       reflink=1    bigtime=1 inobtcount=1
data      =                       bsize=4096  blocks=16777216, imaxpct=25
      =                       sunit=1     swidth=1 blks
naming    =version 2          bsize=4096  ascii-ci=0, ftype=1
log       =internal log     bsize=4096  blocks=16384, version=2
      =                       sectsz=512  sunit=1 blks, lazy-count=1
realtime  =none              extsz=4096  blocks=0, rtextents=0
```

## Previous generation instances

```
sudo mkfs -t ext4 device_name
```

你應該看到下面的輸出，如下所示。

```
mke2fs 1.42.9 (4-Feb-2014)
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=0 blocks
4194304 inodes, 16777216 blocks
838860 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=4294967296
512 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
4096000, 7962624, 11239424

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
```

6. 使用以下命令建立磁碟的掛載點目錄。掛載點是磁碟在檔案系統樹狀目錄中的位置，也是您在掛載磁碟後讀取和寫入檔案的位置。取代位置 *mount\_point*，針對未使用的空間，例如/data。

```
sudo mkdir mount_point
```

7. 您可以輸入以下指令來驗證磁碟上是否有檔案系統。

## Current generation instances

```
sudo file -s /dev/nvme1n1
```

您會看到類似以下的輸出而非 /dev/nvme1n1: data。

```
/dev/nvme1n1: SGI XFS filesystem data (blksz 4096, inosz 512, v2 dirs)
```

## Previous generation instances

```
sudo file -s /dev/xvdf
```

您會看到類似以下的輸出而非 `/dev/xvdf: data`。

```
/dev/xvdf: Linux rev 1.0 ext4 filesystem data, UUID=0ee83fdf-e370-442e-ae38-12345EXAMPLE (extents) (large files) (huge files)
```

8. 最後，通過輸入以下命令來掛載磁盤。

```
sudo mount device_name mount_point
```

檢閱新磁碟掛載的檔案許可，以確保您的使用者和應用程式可寫入此磁碟。如需檔案許可的詳細資訊，請參閱 [Amazon 使用EC2者指南中的讓 Amazon EBS 磁碟區可供使用](#)。

## 步驟 3：在每次重新啟動執行個體時掛載磁碟

您可能希望在每次重新啟動 Lightsail 執行個體時掛載此磁碟。如果您不這麼做，此步驟為選用。

1. 若要在每次系統重新啟動時掛載此磁碟，請在 `/etc/fstab` 檔案中新增裝置的項目。

建立 `/etc/fstab` 檔案的備份，如果在編輯檔案時不小心損毀或刪除此檔案，即可使用檔案的備份。

```
sudo cp /etc/fstab /etc/fstab.orig
```

2. 使用任何文字編輯器 (例如 vim) 開啟 `/etc/fstab` 檔案。

您必須 `sudo` 先輸入才能開啟檔案，才能儲存變更。

3. 使用以下格式在磁碟的檔案結尾新增新的一行。

```
device_name mount_point file_system_type fs_mntops fs_freq fs_passno
```

例如，您的新行看起來可能類似以下內容。

### Current generation instances

```
/dev/nvme1n1 /data xfs defaults,nofail 0 2
```

### Previous generation instances

```
/dev/xvdf /data ext4 defaults,nofail 0 2
```

4. 儲存檔案並結束您的文字編輯器。

## 建立 Lightsail 區塊儲存磁碟並將其連接至 Windows 伺服器執行個體

如果您需要額外的儲存空間，您可以在 Amazon Lightsail 中建立區塊儲存磁碟並將其連接到 Windows 伺服器執行個體。如需有關區塊儲存磁碟的詳細資訊，請參閱[區塊儲存磁碟](#)。

本指南說明如何使用 Lightsail 主控台建立新的區塊儲存磁碟，並將其附加至 Windows 伺服器執行個體。它還描述了如何使用連接到 Windows Server 實例，以 RDP 使您可以使磁盤上線並對其進行初始化。

### Note

如果您擁有 Linux 或 Unix 執行個體，請參閱[建立磁碟並將其附接至 Linux 或 Unix 執行個體](#)。

## 步驟 1：建立新的區塊儲存磁碟，並將其連接至您的執行個體

建立新的區塊儲存磁碟，並使用 Amazon Lightsail 主控台將其附加到您的執行個體。

建立新的區塊儲存磁碟，並將其連接至您的執行個體

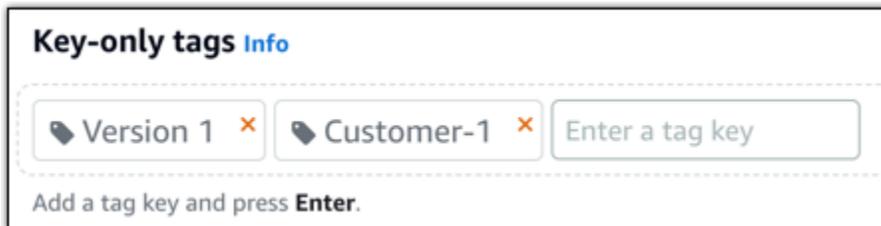
1. 登入主 [Lightsail](#) 台。
2. 選擇 Storage (儲存) 索引標籤，然後選擇 Create disk (建立磁碟)。
3. 選擇 Lightsail 執行個體所在的 AWS 區域 和可用區域。
4. 選擇磁碟大小。
5. 輸入儲存磁碟的名稱。

資源名稱：

- 每個 Lightsail 帳戶 AWS 區域 中的每個項目都必須是唯一的。
- 必須包含 2 至 255 個字元。
- 開頭和結尾必須是英數字元或數字。
- 可以包含英數字元、數字、句點、破折號和底線。

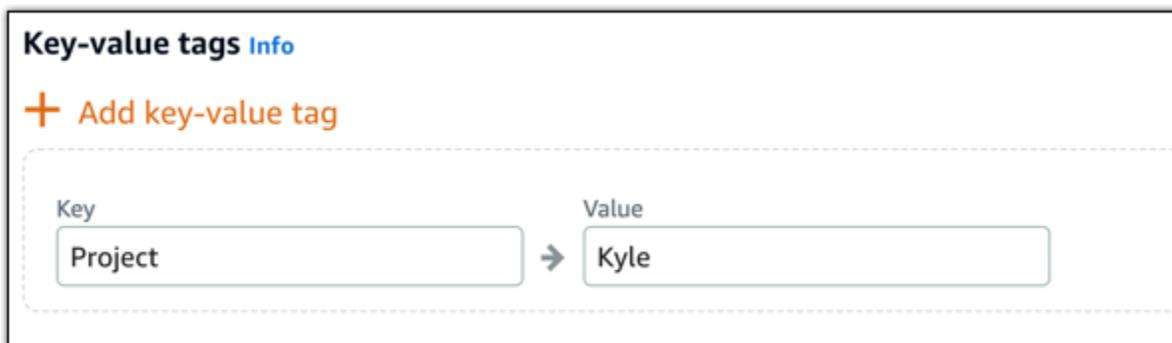
6. 選擇下列其中一個選項以新增標籤至您的磁碟：

- Add key-only tags (新增僅索引鍵標籤) 或 Edit key-only tags (編輯僅索引鍵標籤) (若標籤已新增)。在標籤索引鍵文字方塊中輸入新的標籤，接著按 Enter (輸入)。輸入標籤以新增之後，請選擇 Save (儲存)，如果不要新增則選擇 Cancel (取消)。



- Create a key-value tag (建立索引鍵值標籤)，接著將索引鍵輸入 Key (索引鍵) 文字方塊，將值輸入 Value (值) 文字方塊。完成輸入標籤後，請選擇 Save (儲存)，如果不要新增則選擇 Cancel (取消)。

鍵值標籤在儲存前一次只能新增一個。若要新增超過一個索引鍵值標籤，請重複之前的步驟。



**Note**

如需有關僅索引鍵和索引鍵值標籤的詳細資訊，請參閱[標籤](#)。

7. 選擇 Create disk (建立磁碟)。

幾秒鐘之後，磁碟將會建立完成，您將可磁碟管理頁面檢視有關此磁碟的資訊。

- 從清單選擇執行個體，接著選擇 Attach (連接) 將新的磁碟連接至執行個體。



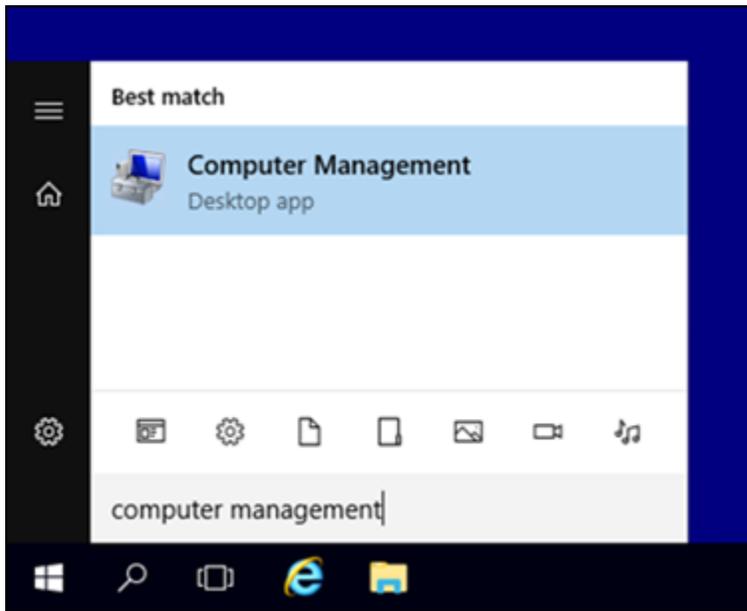
繼續前往本指南的[步驟 2：連線至執行個體並讓區塊儲存磁碟上線](#)一節，讓區塊儲存磁碟上線。

## 步驟 2：連線至執行個體並讓區塊儲存磁碟上線

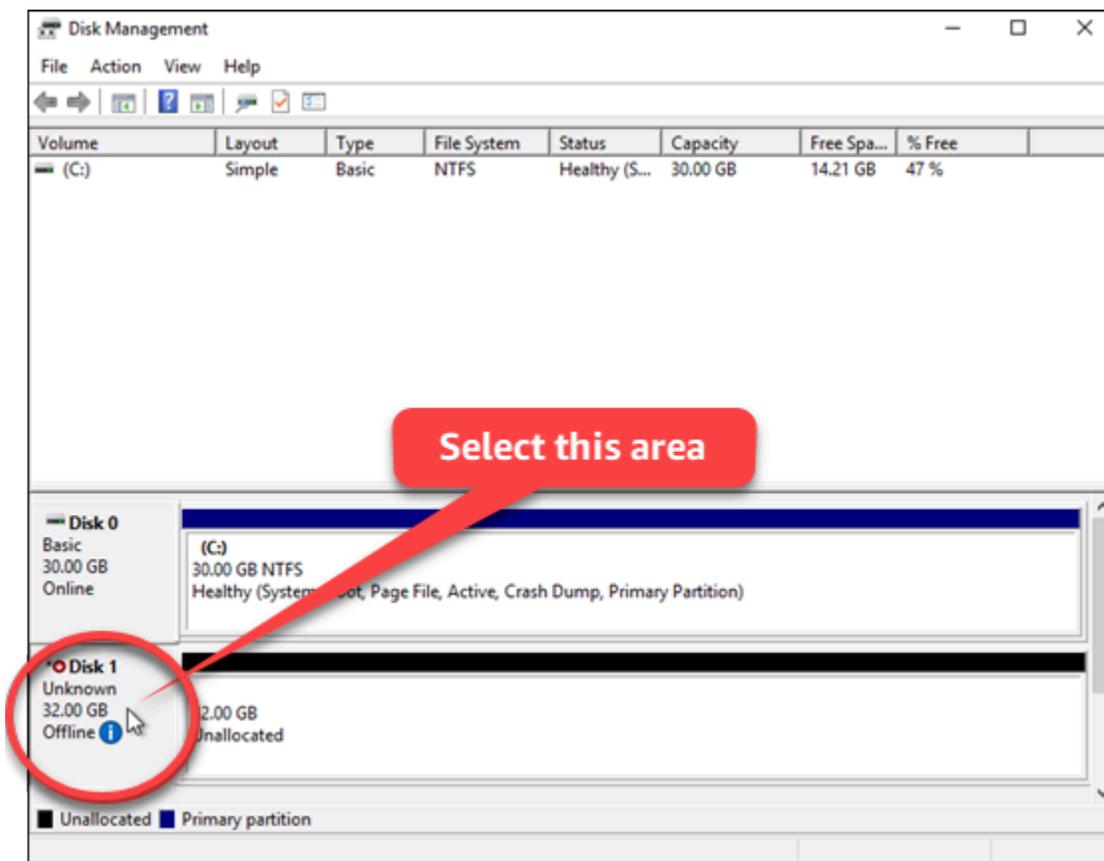
您可以連線至 Windows Server 執行個體，並使用磁碟管理公用程式來讓最近連接的區塊儲存磁碟上線。

### 連線至執行個體並讓區塊儲存磁碟上線

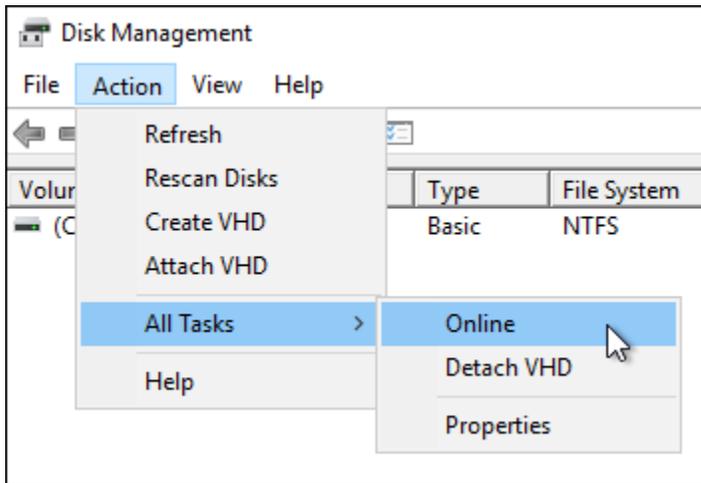
- 瀏覽至 [Lightsail 主控台首頁](#)。
- 選擇您先前在此指南中用於連接其他儲存磁碟的執行個體名稱。
- 在「Connect」標籤下，選擇「Connect 方式」RDP。
- 在 Windows 開始選單上搜尋 Computer Management (電腦管理)，然後在搜尋結果中選擇 Computer Management (電腦管理)。



5. 在 Computer Management (電腦管理) 的左側窗格中，選擇 Disk Management (磁碟管理)。
6. 在磁碟管理公用程式的底部窗格中，選取標示為 Unknown/Offline (不明/離線) 的磁碟。這是您先前在本指南中連接至執行個體的區塊儲存磁碟。



7. 選取磁碟之後，在 Action (動作) 選單中選擇 All Tasks (所有工作)，然後選擇 Online (線上)。



您應該會看到區塊儲存磁碟的狀態更新為 Not Initialized (尚未初始化)。區塊儲存磁碟尚未上線。繼續前往本指南的[步驟 3：初始化區塊儲存磁碟](#)一節，以初始化區塊儲存磁碟。

## 步驟 3：初始化區塊儲存磁碟

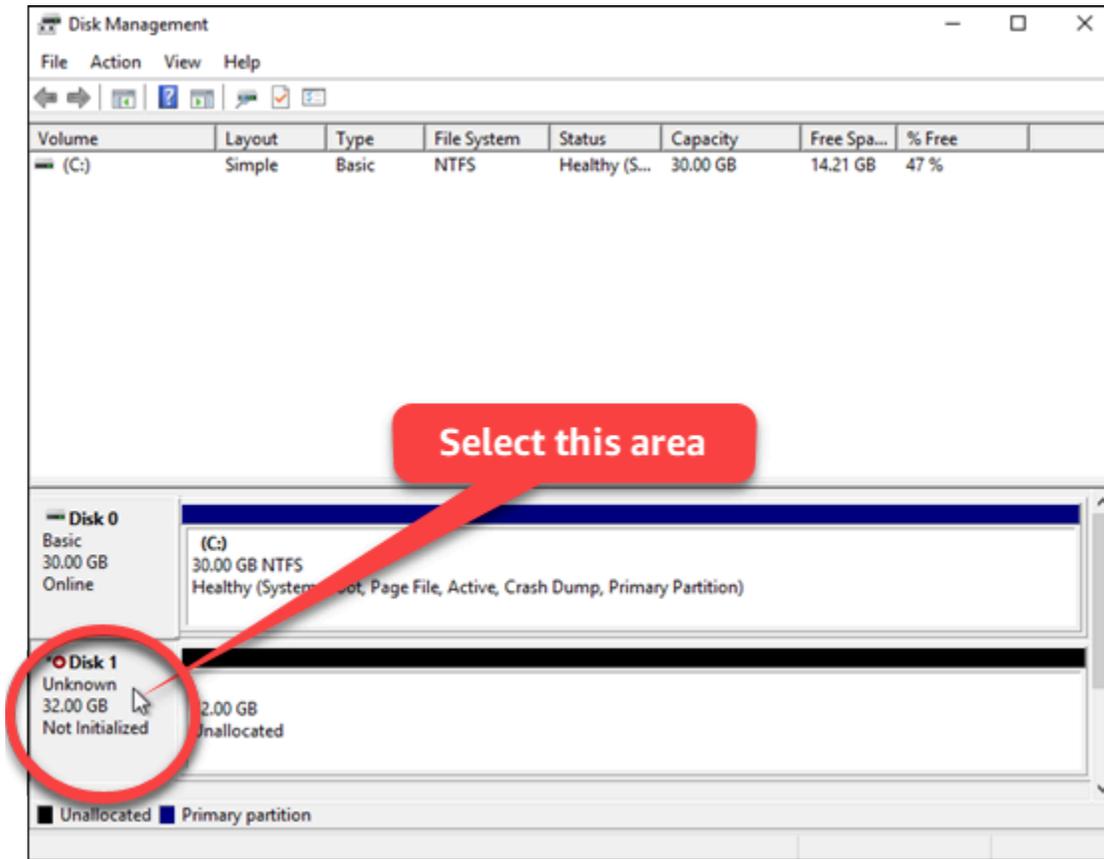
您可以初始化區塊儲存磁碟，藉此將該磁碟格式化。

### **⚠ Important**

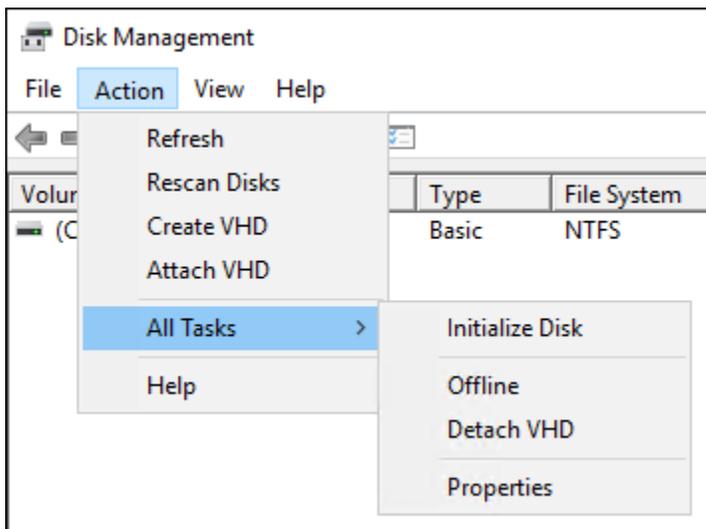
如果掛載的磁碟 (例如從快照建立的磁碟) 已有資料，則請勿重新格式化該磁碟和刪除現有資料。

### 初始化區塊儲存磁碟

1. 在磁碟管理公用程式的底部窗格中，選取標示為 Unknown/Not initialized (不明/尚未初始化) 的磁碟。



2. 選取磁碟之後，在 Action (動作) 選單中選擇 All Tasks (所有工作)，然後選擇 Initialize Disk (初始化磁碟)。



3. 選擇新磁碟的分割區樣式，然後選擇 OK (確定)。

**Note**

如需有關分割區樣式的詳細資訊，請參閱[關於分割區樣式-GPT 和 Microsoft 的 MBR 文章](#)。

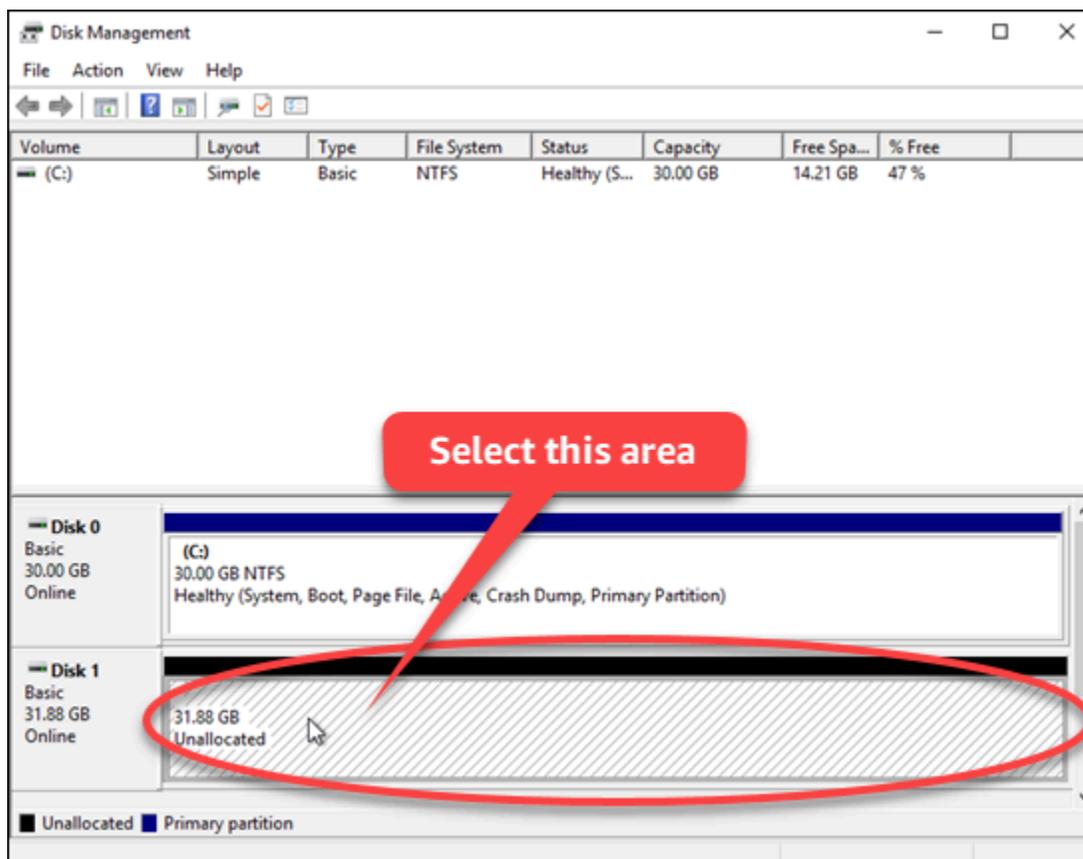
您應該會看到區塊儲存磁碟的狀態更新為 Online (線上)。繼續前往本指南的[步驟 4：以檔案系統格式化磁碟](#)一節，以檔案系統格式化您的區塊儲存磁碟。

## 步驟 4：以檔案系統格式化磁碟

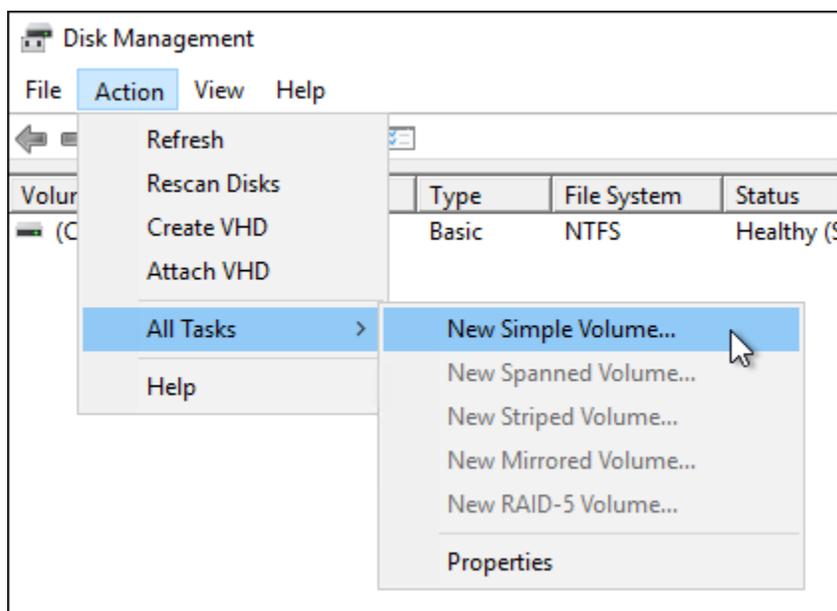
使用 Windows Server 中的 New Simple Volume (新增簡易磁碟區) 精靈，指派磁碟代號，然後以檔案系統格式化磁碟。

### 以檔案系統格式化磁碟

1. 在磁碟管理公用程式的底部窗格中，選取標示為 Unallocated (未配置) 之區塊儲存磁碟上的分割區。



2. 選取分割區之後，在 Action (動作) 選單中選擇 All Tasks (所有工作)，然後選擇 New Simple Volume (新增簡易磁碟區)。

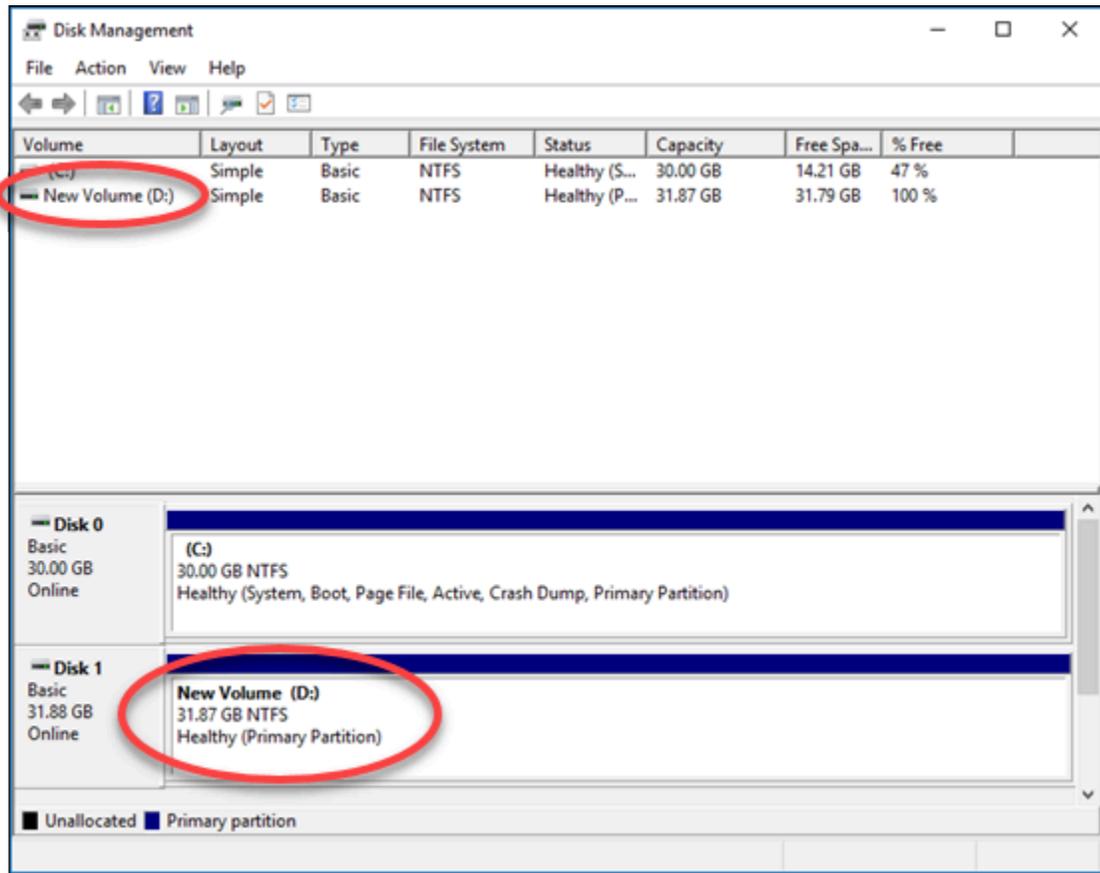


3. 依照新增簡單磁碟區精靈中的指示，選擇NTFSFAT32、或 ReFS 檔案系統類型並格式化磁碟。

#### Note

如需有關這些檔案系統的詳細資訊，請參閱 Microsoft 的 [NTFS概觀](#)、[復原檔案系統 \(ReFS\) 概觀](#) 和 [FAT32檔案系統文件的說明](#)。

完成後，您可以在磁碟管理公用程式中查看磁碟機代號和後續訊息。



## 卸離和刪除 Lightsail 儲存磁碟

如果您不再需要區塊儲存磁碟，可以將其從停止的 Amazon Lightsail 執行個體中分離，然後將其刪除。此主題說明如何備份您的資料，並安全地刪除磁碟。

### 必要條件

- 停止執行中的執行個體。您必須執行此動作，然後才能分離和刪除您的磁碟。[了解如何停止執行個體](#)
- (選用)，我們建議您為磁碟建立一個快照。如此一來，當您改變決定時，還有一個備份可用。如需詳細資訊，請參閱[建立資料庫快照](#)。

### 分離和刪除磁碟

停止 Lightsail 執行個體之後，您就可以安全地卸離並刪除磁碟。

1. 在首頁上選擇 Storage (儲存)。

2. 選擇您已連接的磁碟名稱以進行管理。



3. 在磁碟管理頁面，選擇 Detach (分離)。

在幾秒鐘之後，磁碟將會分離並準備好刪除或重新連接。

4. 選擇 Delete (刪除) 索引標籤。
5. 選擇 Delete disk (刪除磁碟)，然後選擇 Yes, delete (是，刪除) 確認刪除。

**⚠ Important**

這是永久性操作，而且無法還原。刪除磁碟之後，您將失去磁碟上的所有資料。

# Amazon Lightsail 中的快照

您可以在 Amazon Lightsail 中建立執行個體、資料庫和區塊儲存磁碟的 point-in-time 快照，並將其用作基準以建立新資源或進行資料備份。快照包含還原資源所需的所有資料 (從建立快照的那一刻開始)。當您從快照建立資源以還原資源時，新的資源將開始做為用於建立快照之原始資源的確切複本。對於 Lightsail 帳戶上的[快照，無論是手動快照、自動快照、複製的快照還是系統磁碟快照，都需支付快照儲存費用](#)。如果您遇到資料損毀或磁碟故障，您可以從已擷取的快照建立磁碟，然後取代舊磁碟。您也可以使用快照來佈建新磁碟，並在新執行個體啟動期間連接它們。

## 內容

- [手動快照](#)
- [自動快照](#)
- [系統磁碟快照](#)
- [透過快照建立新的資源](#)
- [複製快照](#)
- [將快照匯出到 Amazon EC2](#)
- [刪除快照](#)

## 手動快照

隨時建立執行個體、受管資料庫和區塊儲存磁碟的手動快照。手動快照會無限期存放，直到您刪除為止。

如需有關建立手動快照的詳細資訊，請參閱下列指南：

- [建立 Linux 或 Unix 執行個體快照](#)
- [建立 Windows Server 執行個體快照](#)
- [建立資料庫快照](#)
- [建立區塊儲存磁碟快照](#)

## 自動快照

如果您要在 Lightsail 執行個體或區塊儲存磁碟上託管重要資訊，則應經常建立手動快照來備份這些資訊。不過，找出時間來經常執行管理任務並不容易。如果是這種情況，請使用自動快照讓 Lightsail 代

表您建立執行個體或區塊儲存磁碟的每日備份，而無需手動互動。在由最新快照取代最舊快照之前，會儲存最新的七個每日自動快照。

如需有關自動快照的詳細資訊，請參閱下列指南：

- [啟用或停用自動執行個體快照](#)
- [變更執行個體或磁碟的自動快照時間](#)
- [刪除自動快照](#)

#### Important

刪除來源資源時，與該資源相關聯的所有自動快照也會一併刪除。此行為與手動快照不同，即使您刪除來源資源，這些快照仍會保留在您的 Lightsail 帳戶中。若要在刪除來源資源時保留自動快照，請參閱[保留自動快照](#)。

## 系統磁碟快照

如果您的執行個體沒有回應，而您需要存取系統磁碟上的檔案，您可以建立執行個體根磁碟區的快照作為備份。接著，您可以從該快照建立新的區塊儲存磁碟，並連接至另一個執行個體，以便存取系統中的檔案。如需詳細資訊，請參閱[建立執行個體根磁碟區的快照](#)。

## 透過快照建立新的資源

使用快照建立新的 Lightsail 資源，使用與原始資源相同或更大的計劃。當您以快照為基礎建立資源時，新的資源將開始做為用於建立快照之原始資源的複本。使用較小的 Lightsail 方案，無法使用快照建立新資源。

如需詳細資訊，請參閱下列指南：

- [透過快照建立執行個體](#)
- [透過快照建立資料庫](#)
- [透過快照建立區塊儲存磁碟](#)
- [透過快照建立較大的執行個體、區塊儲存磁碟或資料庫](#)

## 複製快照

執行個體和區塊儲存磁碟快照可以從一個 Amazon Web Services (AWS) 區域複製到同一 Lightsail 帳戶中的另一個區域。不得在區域間複製資料庫快照。如需詳細資訊，請參閱[將快照從一個快照複製 AWS 區域 到另一個](#)。

## 將快照匯出到 Amazon EC2

Lightsail 是開始使用 AWS 的最簡單方法。但是，Lightsail 存在一些限制，這些限制不存在於 Amazon EC2 或其他 AWS 服務中。將 Lightsail 執行個體和區塊儲存磁碟快照匯出 EC2 到 Amazon，以利用更廣泛的可用執行個體類型，並使用中 AWS 的全方位服務。如需詳細資訊，請參閱[將快照匯出到 Amazon EC2](#)。

### Note

cPanel & WHM (CentOS 7) 執行個體的快照不能匯出到 Amazon EC2。

## 刪除快照

當您不再需要 Lightsail 快照時，請刪除這些快照，以避免產生每月[快照儲存](#)費用。如需詳細資訊，請參閱[刪除快照](#)。

## 設定 Lightsail 執行個體和磁碟的自動快照

啟用執行個體或區塊儲存磁碟的自動快照功能時，Amazon Lightsail 會在預設的自動快照時間或您指定的時間內建立資源的每日快照。就像手動快照一樣，您可以使用自動快照作為建立新資源或資料備份的基準。

建立自動快照後，您需要針對 Lightsail 帳戶中[儲存的自動快照支付快照儲存費用](#)。

### 內容

- [自動快照限制](#)
- [自動快照保留](#)
- [使用 Lightsail 主控台啟用或停用自動執行個體快照](#)

- [使用 AWS CLI 啟用或停用執行個體或區塊儲存磁碟的自動快照](#)

## 自動快照限制

下列限制適用於自動快照：

- 您無法使用 Lightsail 主控台為區塊儲存磁碟啟用或停用自動快照。若要啟用或停用區塊儲存磁碟的自動快照，您必須使用 Lightsail API、AWS Command Line Interface (AWS CLI) 或開發套件。如需詳細資訊，請參閱[使用 AWS CLI 啟用或停用自動快照](#)。
- Windows 執行個體或受管資料庫目前不支援自動快照。反之，您必須建立 Windows 執行個體或受管資料庫的手動快照才能備份。如需詳細資訊，請參閱[建立 Windows Server 執行個體的快照](#)以及[建立資料庫快照](#)。受管理的資料庫也會預設啟用 point-in-time 備份功能，您可以使用這項功能將資料還原至新的資料庫。如需詳細資訊，請參閱[從 point-in-time 備份建立資料庫](#)。
- 自動快照不會保留來源資源的標籤。若要在從自動快照建立的新資源保留來源資源的標籤，您必須在從自動快照建立新資源時手動加入標籤。如需詳細資訊，請參閱[將標籤新增至資源](#)。

## 自動快照保留

在由最新快照取代最舊快照之前，會儲存最新的七個每日自動快照。此外，刪除來源資源時，與該資源相關聯的所有自動快照也會一併刪除。此行為與手動快照不同，即使您刪除來源資源，這些快照仍會保留在您的 Lightsail 帳戶中。若要避免自動快照遭到取代，或避免在刪除來源資源時遭到刪除，您可以[將自動快照複製為手動快照](#)。

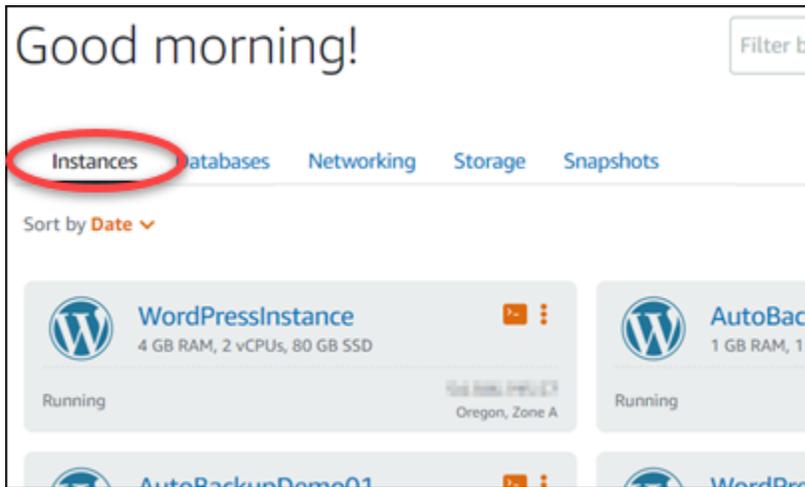
當您停用資源的自動快照功能時，資源的現有自動快照會與來源資源一起保留，直到您執行下列其中一項操作：

- 重新啟用自動快照，現有的自動快照會由較新的快照取代。
- [手動刪除現有的自動快照](#)。
- 刪除來源資源，以刪除相關聯的自動快照。

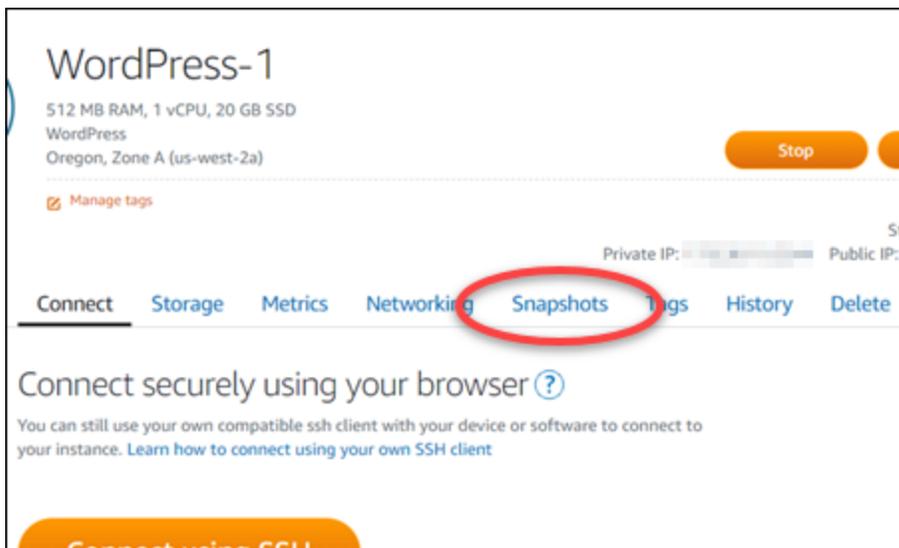
## 使用 Lightsail 主控台啟用或停用自動執行個體快照

完成下列步驟，即可使用 Lightsail 主控台啟用或停用執行個體的自動快照。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁上，選擇「實體」索引標籤。



3. 選擇您要啟用或停用自動快照的執行個體名稱。
4. 在執行個體管理頁面，選擇 Snapshots (快照) 索引標籤。



5. 在 Automatic snapshots (自動快照) 區段中，選擇切換開關以啟用。同樣地，若已啟用時，選擇切換開關以停用。
6. 出現提示時，選擇 Yes, enable (是，啟用) 以啟用自動快照，或 Yes, disable (是，停用) 以停用此功能。

自動快照會在幾分鐘後啟用或停用。

- 如果您已啟用自動快照功能，您可能也想要變更自動快照時間。如需詳細資訊，請參閱[變更執行個體或區塊儲存磁碟的自動快照時間](#)。
- 如果您已停用自動快照功能，則會保留資源的現有自動快照，直到您重新啟用此功能，而由新快照取代，或直到您刪除自動快照。您需要為 Lightsail 帳戶中[儲存的自動快照支付快照儲存費用](#)。如需有關刪除自動快照的詳細資訊，請參閱[刪除自動執行個體快照](#)。

## 啟用或停用執行個體或區塊儲存磁碟的自動快照，使用 AWS CLI

完成下列步驟，以使用 AWS CLI 啟用或停用執行個體或區塊儲存磁碟的自動快照。

1. 開啟終端機或命令提示視窗。

如果您尚未[安裝](#)，請[安裝 AWS CLI](#)並將其設定為與 Lightsail 搭配使用。

2. 根據您要啟用還是停用自動快照而定，輸入在此步驟中描述的其中一個命令：

### Note

在這些命令中，`autoSnapshotAddOnRequest={snapshotTimeOfDay=HH:00}` 參數為選用。如果您在啟用自動快照時未指定每日自動快照時間，Lightsail 會為您的資源指派預設快照時間。如需詳細資訊，請參閱[變更執行個體或區塊儲存磁碟的自動快照時間](#)。

- 輸入以下命令，為現有資源啟用自動快照：

```
aws lightsail enable-add-on --region Region --resource-name ResourceName --add-on-request  
addOnType=AutoSnapshot,autoSnapshotAddOnRequest={snapshotTimeOfDay=HH:00}
```

在命令中：

- 資源所 AWS 區域 在的 `##`。
- `ResourceName` 與資源的名稱。
- 使用以小時增量為單位，且以國際標準時間 (UTC) 計算的每日自動快照取代 `HH#00`。

範例：

```
aws lightsail enable-add-on --region us-west-2 --resource-name WordPress-1 --add-on-request  
addOnType=AutoSnapshot,autoSnapshotAddOnRequest={snapshotTimeOfDay=18:00}
```

- 在建立新執行個體時輸入以下命令以啟用自動快照：

```
aws lightsail create-instances --region Region --availability-zone AvailabilityZone --blueprint-id BlueprintID --
```

```
bundle-id BundleID --instance-name InstanceName --add-ons  
addOnType=AutoSnapshot,autoSnapshotAddOnRequest={snapshotTimeOfDay=HH:00}
```

在命令中：

- 應 AWS 區域 在其中建立執行個體的 **##**。
- *AvailabilityZone* 使用應在其中建立執行個體的可用區域。
- 使用執行個體要使用的藍圖 ID 取代 *BlueprintID*。
- 使用執行個體要使用的套件 ID 取代 *BundleID*。
- *InstanceName* 具有用於實例的名稱。
- 使用以小時增量為單位，且以國際標準時間 (UTC) 計算的每日自動快照取代 *HH#00*。

範例：

```
aws lightsail create-instances --region us-west-2 --availability-  
zone us-west-2a --blueprint-id wordpress_5_1_1_2 --bundle-  
id medium_2_0 --instance-name WordPressInstance --add-ons  
addOnType=AutoSnapshot,autoSnapshotAddOnRequest={snapshotTimeOfDay=20:00}
```

- 在建立新磁碟時輸入以下命令以啟用自動快照：

```
aws lightsail create-disk --region Region --availability-  
zone AvailabilityZone --size-in-gb Size --disk-name DiskName --add-ons  
addOnType=AutoSnapshot,autoSnapshotAddOnRequest={snapshotTimeOfDay=HH:00}
```

在命令中：

- 應 AWS 區域 在其中建立磁碟的 **##**。
- *AvailabilityZone* 使用應在其中建立磁碟的可用區域。
- 使用選擇的磁碟大小 (以 GB 為單位) 取代 **##**。
- *DiskName* 具有要用於磁碟的名稱。
- 使用以小時增量為單位，且以國際標準時間 (UTC) 計算的每日自動快照取代 *HH#00*。

範例：

```
aws lightsail create-disk --region us-west-2 --availability-  
zone us-west-2a --size-in-gb 32 --disk-name Disk01 --add-ons  
addOnType=AutoSnapshot,autoSnapshotAddOnRequest={snapshotTimeOfDay=18:59}
```

- 輸入以下命令，為資源停用自動快照：

```
aws lightsail disable-add-on --region Region --resource-name ResourceName --add-on-type AutoSnapshot
```

在命令中：

- 資源所 AWS 區域 在的##。
- *ResourceName*與資源的名稱。

範例：

```
aws lightsail disable-add-on --region us-west-1 --resource-name MyFirstWordPressWebsite01 --add-on-type AutoSnapshot
```

您應該會看到類似以下範例的結果：

```
{
  "operations": [
    {
      "id": "2610213c-d68f-488e-9124-245913a2a22a",
      "resourceName": "WordPressInstance",
      "resourceType": "Instance",
      "createdAt": 1566431564.323,
      "location": {
        "availabilityZone": "us-west-2a",
        "regionName": "us-west-2"
      },
      "isTerminal": false,
      "operationType": "CreateInstance",
      "status": "Started",
      "statusChangedAt": 1566431564.323
    },
    {
      "id": "fd04446d-8106-4c7e-8d69-f42be811453a",
      "resourceName": "WordPressInstance",
      "resourceType": "Instance",
      "createdAt": 1566431566.368,
      "location": {
        "availabilityZone": "us-west-2",
        "regionName": "us-west-2"
      },
      "isTerminal": false,
      "operationDetails": "EnableAddOn - AutoBackup",
      "operationType": "EnableAddOn",
      "status": "Started"
    }
  ]
}
```

自動快照會在幾分鐘後啟用或停用。

- 如果您已啟用自動快照，您可能也想要變更自動快照時間。如需詳細資訊，請參閱[變更執行個體或區塊儲存磁碟的自動快照時間](#)。

- 如果您已停用自動快照，則會保留現有的自動快照，直到您重新啟用此功能，而由新快照取代，或直到您刪除自動快照。您需要為 Lightsail 帳戶中[儲存的自動快照支付快照儲存費用](#)。如需有關刪除自動快照的詳細資訊，請參閱[刪除自動執行個體快照](#)。

#### Note

如需這些命令中 EnableAddOn 和 DisableAddOn API 作業的詳細資訊，請參閱 Lightsail API 文件[DisableAddOn](#)中的[EnableAddOn](#)和。

## 調整 Lightsail 執行個體和磁碟的自動快照排程

當您為執行個體或區塊儲存磁碟[啟用自動快照功能](#)時，Lightsail 會在[預設的自動快照時間或您指定的時間內建立資源的每日快照](#)。遵循本指南中的步驟，變更資源的自動快照時間。

### 內容

- [自動快照時間限制](#)
- [的預設自動快照時間 AWS 區域](#)
- [使用 Lightsail 主控台變更自動快照時間](#)
- [使用變更自動快照時間和區塊儲存磁碟 AWS CLI](#)

### 自動快照時間限制

下列限制適用於自動快照時間：

- 無法使用 Lightsail 主控台變更區塊儲存磁碟的自動快照時間。若要變更區塊儲存磁碟的自動快照時間，您必須使用 Lightsail API、AWS Command Line Interface (AWS CLI) 或開發套件。如需詳細資訊，請參閱[使用 AWS CLI 變更自動快照時間](#)。
- 指定自動快照時間時，只能以小時為單位遞增。且距目前時間必須超過 30 分鐘。Lightsail 會在您指定的時間到最多 45 分鐘後建立自動快照。

#### Important

建立自動快照時，您無法建立手動快照。

- 當您變更資源的自動快照時間時，通常會立即生效，除非有下列情況：

- 若當天已建立自動快照，且您將快照時間變更為一天中較晚的時間，則新的快照時間將在隔天生效。這可確保當天不會建立兩個快照。
- 如果當天尚未建立自動快照，且您將快照時間變更為一天中較早的時間，則新的快照時間將在隔天生效。此外，快照會在當天於之前設定的時間自動建立。這可確保當天會建立快照。
- 如果當天尚未建立自動快照，且您將快照時間變更為距目前時間 30 分鐘內的時間，則新的快照時間將在隔天生效。此外，快照會在當天於之前設定的時間自動建立。這可確保當天會建立快照，因為目前時間和您指定的新快照時間之間需要間隔 30 分鐘。
- 如果自動快照排定距目前時間 30 分鐘內建立，且您變更快照時間，則新的快照時間將在隔天生效。此外，快照會在當天於之前設定的時間自動建立。這可確保當天會建立快照，因為目前時間和您指定的新快照時間之間需要間隔 30 分鐘。

當上述任一條件成立時，Lightsail 主控台會顯示訊息，通知您新的快照時間最多可能需要 24 小時才會生效。

## AWS 區域的預設自動快照時間

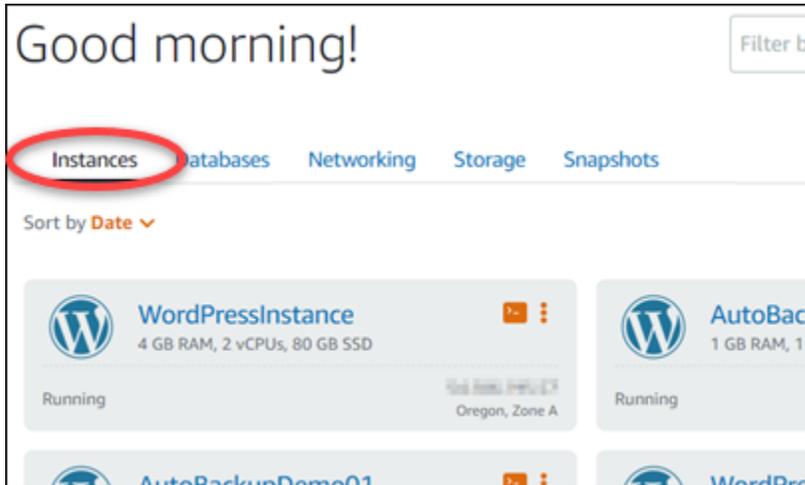
如果您在啟用自動快照時未指定自動快照時間，Lightsail 會指定下列其中一個預設自動快照時間。時間取決於執行 AWS 區域 個體或區塊儲存磁碟的所在位置：

- 美國東部 (俄亥俄) (us-east-2) : 03:00 UTC
- 美國東部 (維吉尼亞北部) (us-east-1) : 06:00 UTC
- 美國西部 (奧勒岡) (us-west-2) : 06:00 UTC
- 亞太區域 (孟買) (ap-south-1) : 17:00 UTC
- 亞太區域 (首爾) (ap-northeast-2) : 13:00 UTC
- 亞太區域 (新加坡) (ap-southeast-1) : 14:00 UTC
- 亞太區域 (雪梨) (ap-southeast-2) : 12:00 UTC
- 亞太區域 (東京) (ap-northeast-1) : 13:00 UTC
- 加拿大 (中部) (ca-central-1) : 06:00 UTC
- 歐洲 (法蘭克福) (eu-central-1) : 20:00 UTC
- 歐洲 (愛爾蘭) (eu-west-1) : 22:00 UTC
- 歐洲 (倫敦) (eu-west-2) : 06:00 UTC
- 歐洲 (巴黎) (eu-west-3) : 07:00 UTC
- 歐洲 (斯德哥爾摩) (eu-north-1) : 08:00 UTC

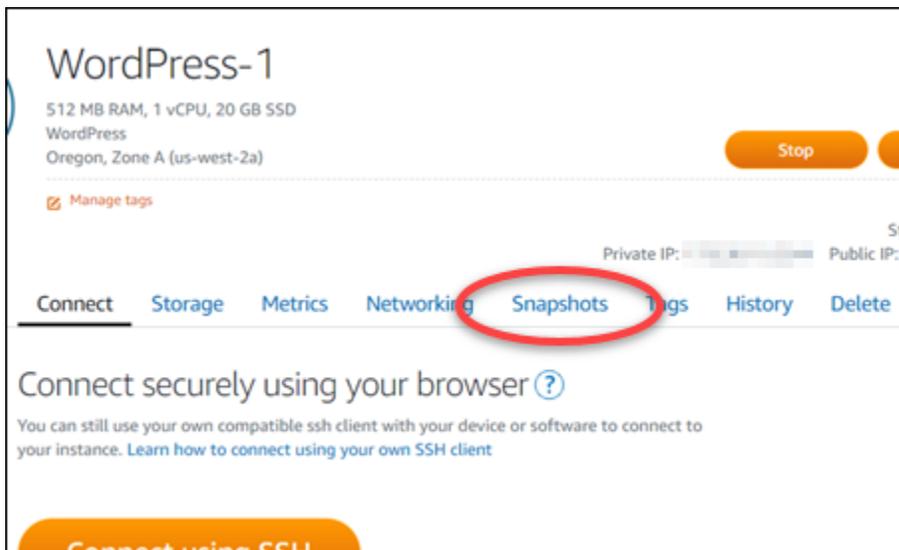
## 使用 Lightsail 主控台變更自動快照時間

完成下列步驟，即可使用 Lightsail 主控台變更執行個體的自動快照時間。

1. 登入主 [Lightsail](#) 台。
2. 在 Lightsail 首頁上，選擇「實體」索引標籤。



3. 選擇您要變更自動快照時間的執行個體名稱。
4. 在執行個體管理頁面，選擇 Snapshots (快照) 索引標籤。



5. 在 Automatic snapshots (自動快照) 區段中，選擇 Change snapshot time (變更快照時間)。
6. 選擇您希望 Lightsail 建立自動快照的時間。您選擇的時間必須採用國際標準時間 (UTC)。
7. 選擇 Change (變更) 以儲存新的快照時間。

自動快照時間會在幾分鐘後更新。新的自動快照時間生效日期可能有所限制。如需詳細資訊，請參閱[自動快照時間限制](#)。

## 使用變更執行個體和區塊儲存磁碟的自動快照時間 AWS CLI

完成下列步驟，以使用 AWS CLI 變更執行個體或區塊儲存磁碟的自動快照時間。

1. 開啟終端機或命令提示視窗。

如果您尚未[安裝](#)，請[安裝 AWS CLI](#)並將其設定為與 Lightsail 搭配使用。

2. 輸入下列命令，變更資源的自動快照時間：

```
aws lightsail enable-add-on --region Region --resource-name ResourceName --add-on-request addOnType=AutoSnapshot,autoSnapshotAddOnRequest={snapshotTimeOfDay=HH:00}
```

在命令中：

- 資源所 AWS 區域 在的 *##*。
- *ResourceName* 與資源的名稱。
- 使用以小時增量為單位，且以國際標準時間 (UTC) 計算的每日自動快照取代 *HH#00*。

範例：

```
aws lightsail enable-add-on --region us-west-1 --resource-name MyFirstWordPressWebsite01 --add-on-request addOnType=AutoSnapshot,autoSnapshotAddOnRequest={snapshotTimeOfDay=12:00}
```

您應該會看到類似以下範例的結果：

```
{
  "operation": {
    "id": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
    "resourceName": "WordPress-1",
    "resourceType": "Instance",
    "createdAt": 1566501867.165,
    "location": {
      "availabilityZone": "us-west-2",
      "regionName": "us-west-2"
    },
    "isTerminal": false,
    "operationDetails": "EnableAddOn - AutoBackup",
    "operationType": "EnableAddOn",
    "status": "Started"
  }
}
```

自動快照時間會在幾分鐘後更新。新的自動快照時間生效日期可能有所限制。如需詳細資訊，請參閱[自動快照時間限制](#)。

#### Note

如需有關此命令中 EnableAddOn API 作業的詳細資訊，請參閱 Lightsail API 文件[EnableAddOn](#)中的。

## 刪除未使用的 Lightsail 實體和磁碟快照

您可以隨時在 Amazon Lightsail 中刪除執行個體或區塊儲存磁碟的自動快照；無論該功能是否已啟用，還是在啟用後停用該功能。您需要為 Lightsail 帳戶中[儲存的自動快照支付快照儲存費用](#)。如果您不再需要自動快照，請遵循本指南中的步驟刪除。例如，如果您已[將自動快照複製到手動快照](#)，且不再需要原始快照，或者，如果您已對資源[停用自動快照功能](#)，且不需要保留的現有自動快照。

### 內容

- [刪除自動快照限制](#)
- [使用 Lightsail 主控台刪除執行個體的自動快照](#)
- [使用刪除執行個體或區塊儲存磁碟的自動快照 AWS CLI](#)

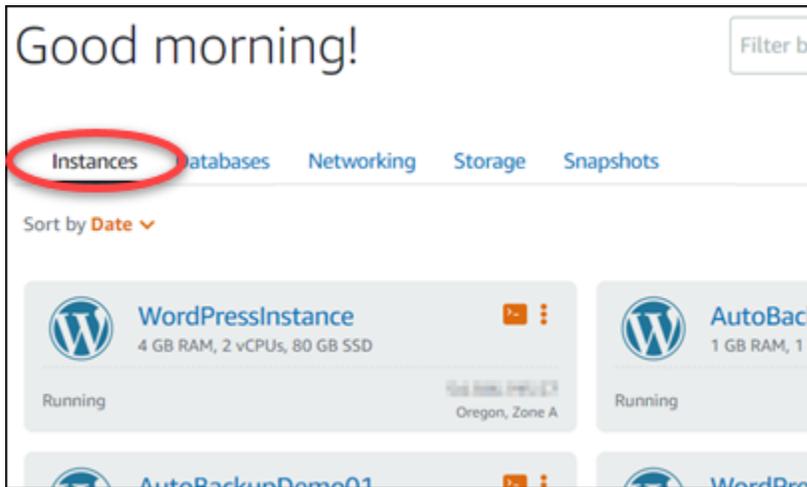
### 刪除自動快照限制

您無法使用 Lightsail 主控台刪除區塊儲存磁碟的自動快照。若要刪除區塊儲存磁碟的自動快照，您必須使用 Lightsail API、AWS Command Line Interface (AWS CLI) 或開發套件。如需詳細資訊，請參閱[使用 AWS CLI 刪除執行個體或區塊儲存磁碟的自動快照](#)。

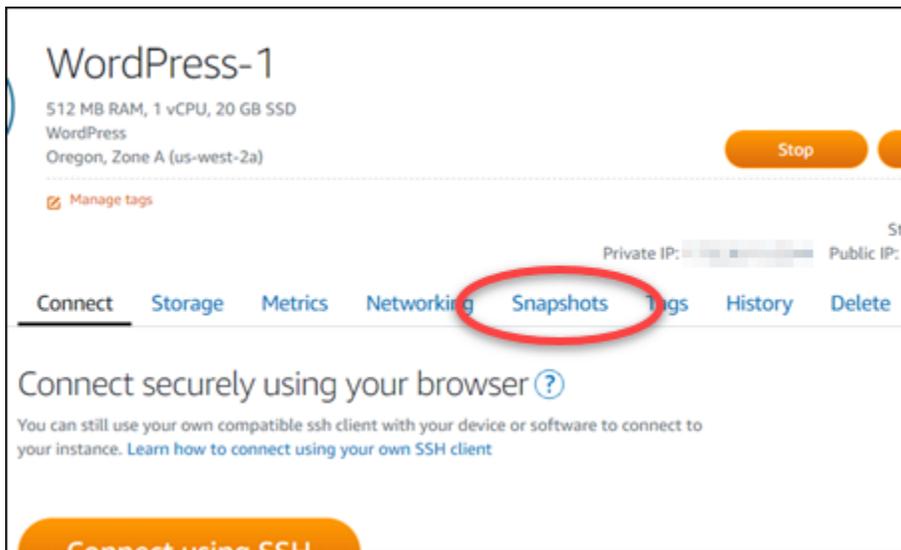
### 使用 Lightsail 主控台刪除執行個體的自動快照

若要使用 Lightsail 主控台刪除執行個體的自動快照，請完成下列步驟。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁上，選擇「實體」索引標籤。



3. 選擇您要刪除自動快照的執行個體名稱。
4. 在執行個體管理頁面，選擇 Snapshots (快照) 索引標籤。



5. 在 Automatic snapshots (自動快照) 區段中，選擇您想要刪除之自動快照旁的省略符號圖示，然後選擇 Delete snapshot (刪除快照)。
6. 出現提示時，選擇 Yes (是)，確認您要刪除快照。

自動快照會在幾分鐘後刪除。

## 使用刪除執行個體或區塊儲存磁碟的自動快照 AWS CLI

完成下列步驟，以使用 AWS CLI 刪除執行個體或區塊儲存磁碟的自動快照。

1. 開啟終端機或命令提示視窗。

如果您尚未[安裝](#)，請[安裝 AWS CLI](#)並將其設定為與 Lightsail 搭配使用。

2. 輸入下列命令，以取得特定資源可用的自動快照日期。在後續命令中，您將需要自動快照的日期來指定做為 `date` 參數。

```
aws lightsail --region Region get-auto-snapshots --resource-name ResourceName
```

在命令中：

- 資源所 AWS 區域 在的 `##`。
- `ResourceName` 與資源的名稱。

範例：

```
aws lightsail --region us-west-2 get-auto-snapshots --resource-name MyFirstWordPressWebsite01
```

您應該會看到類似以下的結果，其中列出可用的自動快照：

```
{
  "resourceName": "Magento-2",
  "resourceType": "Instance",
  "autoBackups": [
    {
      "date": "2019-08-22",
      "createdAt": 1566455335.0,
      "status": "Success",
      "fromAttachedDisks": [
        {
          "path": "/dev/xvdf",
          "sizeInGb": 8
        }
      ]
    },
    {
      "date": "2019-08-21",
      "createdAt": 1566368935.0,
      "status": "Success",
      "fromAttachedDisks": []
    },
    {
      "date": "2019-08-20",
      "createdAt": 1566282535.0,
      "status": "Success",
      "fromAttachedDisks": []
    },
    {
      "date": "2019-08-19",
      "createdAt": 1566196135.0,
      "status": "Success",
      "fromAttachedDisks": []
    }
  ]
}
```

### 3. 輸入下列命令來刪除自動快照：

```
aws lightsail --region Region delete-auto-snapshot --resource-name ResourceName --
date YYYY-MM-DD
```

在命令中：

- 資源所 AWS 區域 在的 *##*。
- *ResourceName* 與資源的名稱。
- 使用您使用上述命令取得的可用自動快照日期取代 *YYYY-MM-DD*。

範例：

```
aws lightsail --region us-west-2 delete-auto-snapshot --resource-  
name MyFirstWordPressWebsite01 --date 2019-09-16
```

您應該會看到類似以下範例的結果：

```
{  
  "operation": {  
    "id": "8f253c00-c34f-4073-9b0e-e5507ce264d9",  
    "resourceName": "Magento-2",  
    "resourceType": "Instance",  
    "createdAt": 1566507472.323,  
    "location": {  
      "availabilityZone": "us-west-2",  
      "regionName": "us-west-2"  
    },  
    "isTerminal": true,  
    "operationDetails": "DeleteAutoBackup-2019-08-16",  
    "operationType": "DeleteAutoBackup",  
    "status": "Succeeded"  
  }  
}
```

自動快照會在幾分鐘後刪除。

#### Note

如需這些命令中 `GetAutoSnapshots` 和 `DeleteAutoSnapshot` API 作業的詳細資訊，請參閱 Lightsail API 文件 [DeleteAutoSnapshot](#) 中的 [GetAutoSnapshots](#) 和。

## 防止在 Lightsail 中取代自動快照

當您在 Amazon Lightsail [中為執行個體或區塊儲存磁碟啟用自動快照功能](#) 時，只會儲存資源的最新 7 個每日自動快照。然後，系統就會以最新的取代最舊的。此外，刪除來源資源時，與該資源相關聯的所有自動快照也會一併刪除。

如果您想要避免特定的自動快照遭到取代，或避免特定的自動快照在您刪除來源資源時遭到刪除，您可將其複製為手動快照。手動快照會保留到您手動刪除它們為止。

遵循本指南中的步驟，將自動快照複製為手動快照保留下來。您需要為 Lightsail 帳戶中 [儲存的自動快照支付快照儲存費用](#)。

**Note**

如果您停用資源的自動快照功能，則會保留資源的現有自動快照，直到您重新啟用此功能，而由較新的快照取代，或直到您[刪除自動快照](#)。

## 內容

- [保留自動快照限制](#)
- [使用 Lightsail 主控台保留執行個體的自動快照](#)
- [保留執行個體和區塊儲存磁碟的自動快照，AWS CLI](#)

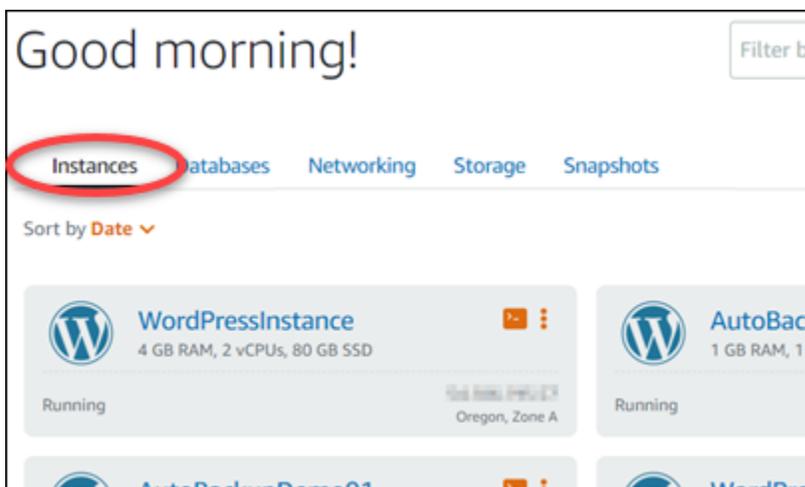
## 保留自動快照限制

無法使用 Lightsail 主控台將區塊儲存磁碟的自動快照複製到手動快照。若要複製區塊儲存磁碟的自動快照，您必須使用 Lightsail API、AWS Command Line Interface (AWS CLI) 或開發套件。如需詳細資訊，請參閱[使用 AWS CLI 保留執行個體和區塊儲存磁碟的自動快照](#)。

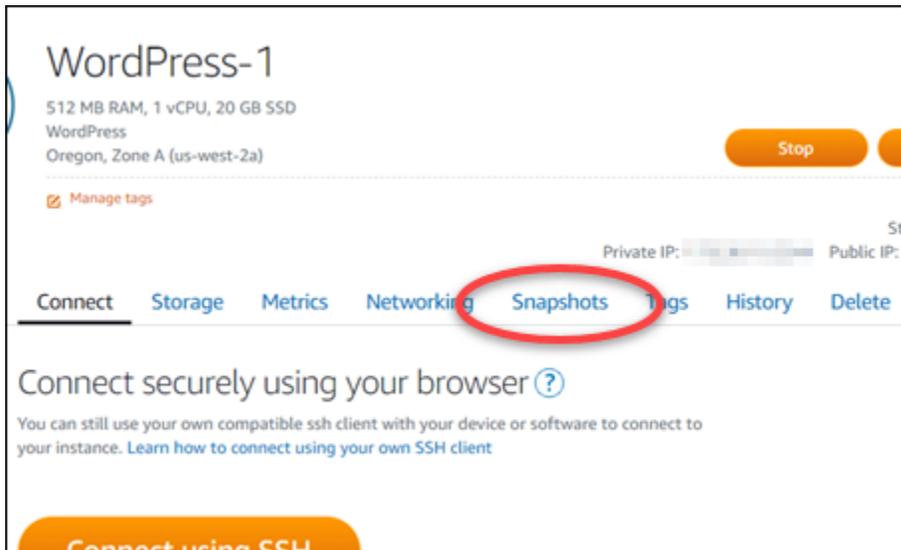
## 使用 Lightsail 主控台保留執行個體的自動快照

完成下列步驟，即可使用 Lightsail 主控台保留執行個體的自動快照。

1. 登入主 [Lightsail](#) 台。
2. 在 Lightsail 首頁上，選擇「實體」索引標籤。



3. 選擇您要保留自動快照的執行個體名稱。
4. 在執行個體管理頁面，選擇 Snapshots (快照) 索引標籤。



5. 在 Automatic snapshots (自動快照) 區段中，選擇您想要保留之自動快照旁的省略符號圖示，然後選擇 Keep snapshot (保留快照)。
6. 出現提示時，選擇 Yes, save (是，儲存)，以確認您要保留自動快照。

自動快照會在幾分鐘後複製為手動快照。手動快照會保留到您刪除為止。

#### Important

如果您不再需要自動快照，建議刪除。否則，您需支付 Lightsail 帳戶中[儲存的自動快照和重複手動快照的快照儲存費用](#)。如需詳細資訊，請參閱[刪除自動執行個體快照](#)。

## 保留執行個體和區塊儲存磁碟的自動快照，AWS CLI

完成下列步驟，以使用 AWS CLI 保留執行個體或區塊儲存磁碟的自動快照。

1. 開啟終端機或命令提示視窗。

如果您尚未[安裝](#)，請[安裝 AWS CLI](#)並將其設定為與 Lightsail 搭配使用。

2. 輸入下列命令，以取得特定資源可用的自動快照日期。在後續命令中，您需要自動快照的日期來指定做為 restore date 參數。

```
aws lightsail get-auto-snapshots --region Region --resource-name ResourceName
```

在命令中：

- 資源所 AWS 區域 在的##。
- *ResourceName*與資源的名稱。

範例：

```
aws lightsail get-auto-snapshots --region us-west-2 --resource-  
name MyFirstWordPressWebsite01
```

您應該會看到類似以下的結果，其中列出可用的自動快照：

```
{  
  "resourceName": "Magento-2",  
  "resourceType": "Instance",  
  "autoBackups": [  
    {  
      "date": "2019-08-22",  
      "createdAt": 1566455335.0,  
      "status": "Success",  
      "fromAttachedDisks": [  
        {  
          "path": "/dev/xvdf",  
          "sizeInGb": 8  
        }  
      ]  
    },  
    {  
      "date": "2019-08-21",  
      "createdAt": 1566368935.0,  
      "status": "Success",  
      "fromAttachedDisks": []  
    },  
    {  
      "date": "2019-08-20",  
      "createdAt": 1566282535.0,  
      "status": "Success",  
      "fromAttachedDisks": []  
    },  
    {  
      "date": "2019-08-19",  
      "createdAt": 1566196135.0,  
      "status": "Success",  
      "fromAttachedDisks": []  
    }  
  ]  
}
```

3. 輸入下列命令，以保留特定資源的自動快照：

```
aws lightsail copy-snapshot --region TargetRegion --source-resource-name ResourceName --restore-date YYYY-MM-DD --source-region SourceRegion --target-snapshot-name SnapshotName
```

在命令中：

- *TargetRegion* 使用您要將快照複製到其 AWS 區域 中的。
- *ResourceName* 與資源的名稱。
- 使用您使用上述命令取得的可用自動快照日期取代 *YYYY-MM-DD*。
- *SourceRegion* 與自 AWS 區域 動快照目前所在的。
- *SnapshotName* 與要創建的新快照的名稱。

範例：

```
aws lightsail copy-snapshot --region us-west-2 --source-resource-name MyFirstWordPressWebsite01 --restore-date 2019-09-16 --source-region us-west-2 --target-snapshot-name Snapshot-Copied-From-Auto-Snapshot
```

您應該會看到類似以下範例的結果：

```
{
  "operations": [
    {
      "id": "6f2607ca-c3d3-4e92-9795-8d7c8d72b038",
      "resourceName": "Snapshot-Copied-From-Auto-Backup",
      "resourceType": "InstanceSnapshot",
      "createdAt": 1566504306.107,
      "location": {
        "availabilityZone": "all",
        "regionName": "us-west-2"
      },
      "isTerminal": false,
      "operationDetails": "us-west-2:Magento-2",
      "operationType": "CopySnapshot",
      "status": "Started",
      "statusChangedAt": 1566504306.107
    }
  ]
}
```

自動快照會在幾分鐘後複製為手動快照。手動快照會保留到您刪除為止。

**⚠ Important**

如果您不再需要自動快照，建議刪除。否則，您需支付 Lightsail 帳戶中[儲存的自動快照和複製手動快照的快照儲存費用](#)。如需詳細資訊，請參閱[刪除自動執行個體快照](#)。

**ℹ Note**

如需這些命令中 `GetAutoSnapshots` 和 `CopySnapshot` API 作業的詳細資訊，請參閱 Lightsail API 文件 [CopySnapshot](#) 中的 [GetAutoSnapshots](#) 和。

## 使用快照備份 Linux/UniLightsail 執行個體

您可以為基於 Linux/Unix 的 Amazon Lightsail 執行個體建立快照。執行個體快照是系統磁碟的副本，符合原始機器設定 (記憶體CPU、磁碟大小和資料傳輸速率)。如果您已將區塊儲存磁碟連結至執行個體，Lightsail 會將這些額外的磁碟複製為快照的一部分。如需詳細資訊，請參閱[快照](#)。

**ℹ Note**

建立以 Windows 伺服器為基礎之 Lightsail 實體快照的步驟有所不同。如需詳細資訊，請參閱[建立 Windows Server 執行個體的快照](#)。

您必須已在 Lightsail 中擁有實體，才能建立該實體的快照。在您擁有執行個體之後，請依照以下步驟建立快照：

1. 在 Lightsail 首頁上，選擇您要為其建立快照的執行個體名稱。
2. 選擇 Snapshots (快照) 索引標籤。
3. 在頁面的手動快照部分中，選擇 Create snapshot (建立快照)，然後輸入快照的名稱。

資源名稱：

- 每個 Lightsail 帳戶 AWS 區域 中的每個項目都必須是唯一的。
- 必須包含 2 至 255 個字元。
- 開頭和結尾必須是英數字元或數字。

- 可以包含英數字元、數字、句點、破折號和底線。

#### 4. 選擇 Create (建立)。

您可以使用 Snapshotting。。。 (快照。。。) 查看您剛建立的快照。

快照完成後，您即可[從該快照建立另一個執行個體](#)。例如，您可能會想選擇大小比先前更大的搭售套件。

#### Important

當您從快照建立新的執行個體時，Lightsail 可讓您建立大小相同或更大的執行個體套裝軟體。我們目前不支援從快照建立較小的執行個體大小。當您從快照建立執行個體時，較小的選項將變成灰色。

若要從快照建立較大的執行個體大小，您可以使用 Lightsail 主控台、create-instances-from-snapshotCLI指令或作業。CreateInstancesFromSnapshotAPI如需詳細資訊，請參閱[透過快照建立執行個體](#)。如需有關 Lightsail 套件組合的詳細資訊，請參閱 [Lightsail 定價](#)。

## 建立您的視窗伺服器執行個體的快照

快照是執行個體之系統磁碟和原始組態的複本。快照包括記憶體CPU、磁碟大小和資料傳輸速率等資訊。如需詳細資訊，請參閱[快照](#)。

若要在 Lightsail 中建立 Windows 伺服器執行個體的快照，請先建立備份快照。接著，使用稱作 System Preparation (Sysprep) (系統準備) 的特殊公用程式建立第二份快照。Sysprep 會將 Windows Server 安裝一般化，以便將執行個體備份為快照。然後，當您從該快照集建立執行個 out-of-box 體時，就會有如同您第一次執行該 Windows 執行個體一樣的體驗。

若要建立 Linux 或 Unix 執行個體快照，請參閱[建立 Linux 或 Unix 執行個體快照](#)。

### 內容

- [步驟 1：在執行 Sysprep 前建立備份快照](#)
- [步驟 2：連線到您的執行個體，並使用 Sysprep 將其關閉](#)
- [步驟 3：在執行 Sysprep 後建立快照](#)

## 步驟 1：在執行 Sysprep 前建立備份快照

在您執行 Sysprep 以建立快照時，系統專屬資訊將從您的執行個體中移除。這可能會對該執行個體上執行的應用程式產生各種意外後果。因此，您應該先建立備份快照後再執行 Sysprep，以確保在發生錯誤時可使用替代快照。

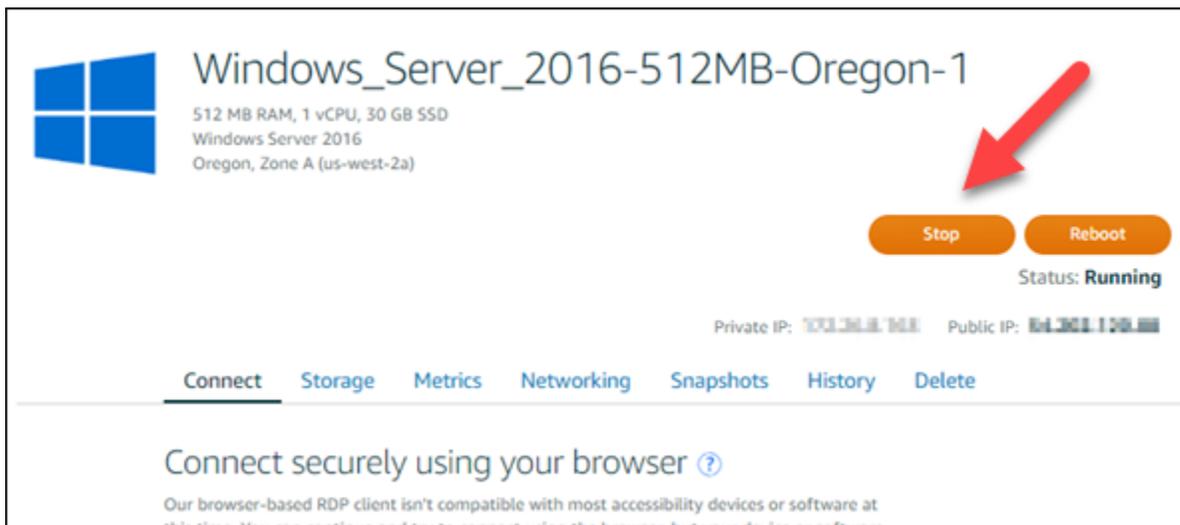
當您在執行 Sysprep 前建立快照時，使用備份快照建立的執行個體會擁有與原始執行個體相同的管理員密碼。您無法使用 Lightsail 主控台中以瀏覽器為基礎的用 RDP 戶端連線到這些執行個體。不過，您可以使用自己的用 RDP 戶端和原始執行個體相同的系統管理員密碼來連線。如需更多資訊，請查看[使用 Windows 電腦上的遠端桌面連線用戶端連線至 Amazon Lightsail 中的 Windows 執行個體](#)。

### ⚠ Important

儲存原始 Windows 執行個體的管理員密碼，然後將其存放在安全的地方。如果稍後發生問題，您會需要該管理員密碼，並且在執行 Sysprep 之前，需先從建立的快照建立執行個體。

### 在執行 Sysprep 前建立備份快照

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁上，選擇您要建立快照之 Windows 伺服器執行個體的名稱。
3. 在執行個體管理頁面上方選擇 Stop (停止) 以停止您的執行個體。



### 📘 Note

停用執行個體將造成其中所有網站與服務均無法使用，除非您再次啟動該執行個體。

4. 選擇 Snapshots (快照) 索引標籤。
5. 在頁面的手動快照部分中，選擇 Create snapshot (建立快照)，然後輸入快照的名稱。

資源名稱：

- 每個 Lightsail 帳戶 AWS 區域 中的每個項目都必須是唯一的。
  - 必須包含 2 至 255 個字元。
  - 開頭和結尾必須是英數字元或數字。
  - 可以包含英數字元、數字、句點、破折號和底線。
6. 選擇 Create (建立)。
  7. 出現提示時，再次選擇 Create snapshot (建立快照) 以確認。  
  
該快照可能需要幾分鐘來完成。
  8. 快照建立之後，在執行個體管理頁面上方選擇 Start (啟動) 以再次啟動您的執行個體。

## 步驟 2：連線到您的執行個體，並使用 Sysprep 將其關閉

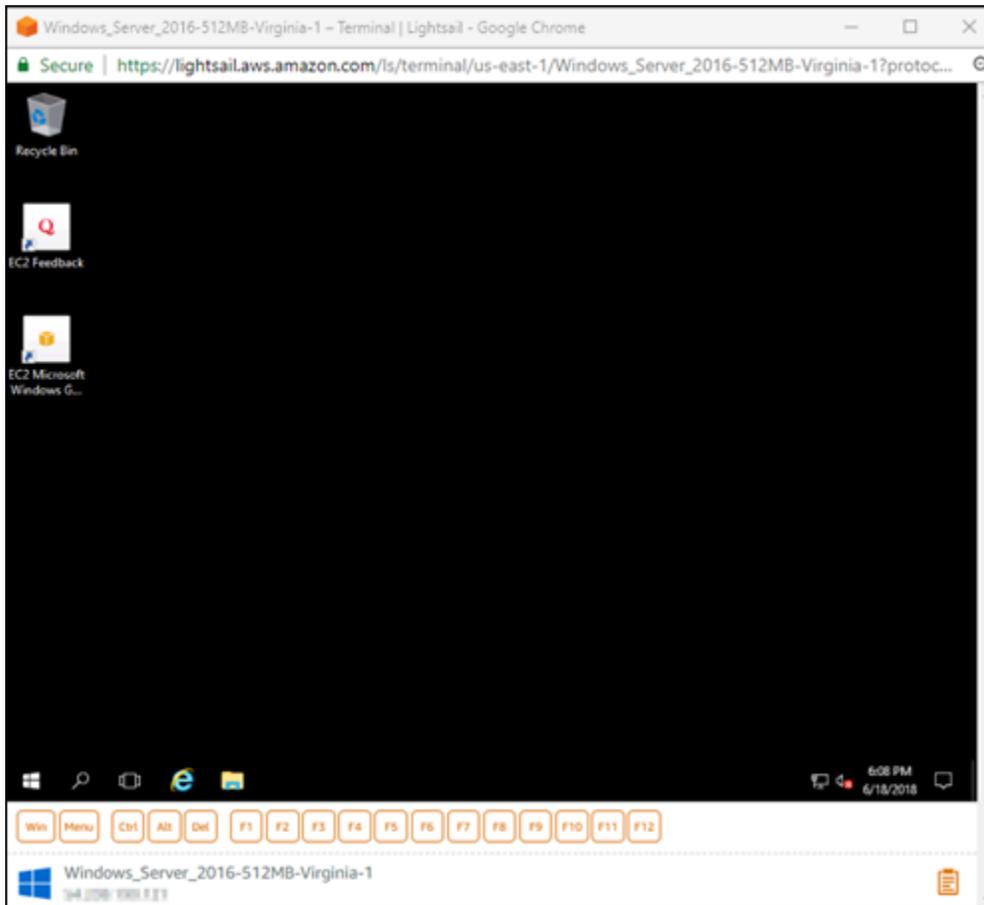
現在您已備份快照，便可開始在您的 Windows Server 執行個體上執行 Sysprep。這會導致該執行個體關閉，您便可以拍攝快照。如需有關 Sysprep 的詳細資訊，請參閱 Microsoft 文件中的 [Sysprep 概觀](#)。

在此步驟中，連接到您的執行個體並透過預先安裝的應用程式執行 Sysprep。該應用程式 EC2LaunchSettings 在 Windows 服務器 2019 和視窗服務器 2016 實例上調用，並在 Windows 服務器 2012 實例上調用 EC2 ConfigService 設置。

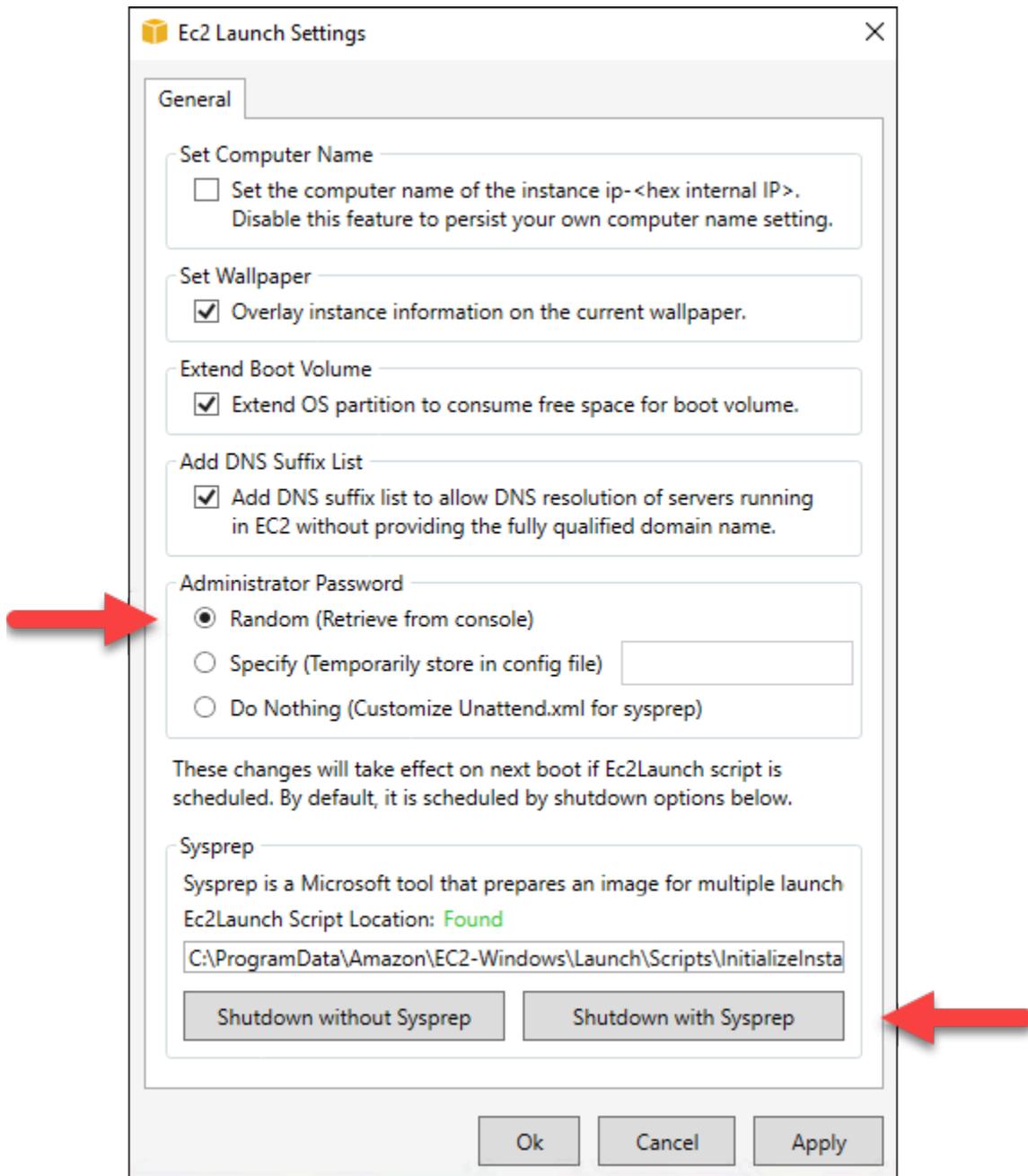
連線到您的執行個體並執行 Sysprep

1. 在執行個體管理頁面上，選擇 [Connect] 索引標籤，然後選擇 [Connect 方式] RDP。

以瀏覽器為基礎的 RDP 視窗隨即開啟，如下列範例所示：



2. 在工作列上選擇 Windows 圖示，或選擇 Win 以開啟 Start (開始) 選單。
3. 選擇這些選項的其中之一：
  - 在視窗伺服器 2022、視窗伺服器 2019 和視窗伺服器 2016 執行個體上，選擇 [開始]，然後選擇 [EC2] LaunchSettings。
4. 在 Administrator Password (管理員密碼) 區段，選擇 Random (Retrieve from console) (隨機 (從主控台擷取))，然後選擇 Shutdown with Sysprep (使用 Sysprep 關機)。



5. 請選擇 Yes (是) 以確認您要執行 Sysprep 並將執行個體關機。

您的執行個體開始執行 Sysprep，RDP連線會關閉，而 Lightsail 執行個體會在幾分鐘後停止執行。

## 步驟 3：在執行 Sysprep 後建立快照

執行個體處於停止狀態後，請在 Lightsail 主控台中建立快照。當您在執行 Sysprep 前建立 Windows Server 執行個體快照時，所有您根據快照建立的執行個體會擁有唯一的管理員密碼。您可以使用 Lightsail 主控台中以瀏覽器為基礎的用 RDP 戶端來連線到這些執行個體。

若要在主控台中建立快照

1. 切換回 Lightsail 主控台。
2. 在 Windows Server 執行個體的執行個體管理頁面中，選擇 Snapshots (快照) 索引標籤
3. 在頁面的手動快照部分中，選擇 Create snapshot (建立快照)，然後輸入快照的名稱。

資源名稱：

- 每個 Lightsail 帳戶 AWS 區域 中的每個項目都必須是唯一的。
  - 必須包含 2 至 255 個字元。
  - 開頭和結尾必須是英數字元或數字。
  - 可以包含英數字元、數字、句點、破折號和底線。
4. 選擇 Create (建立)。
  5. 出現提示時，選擇 Create snapshot (建立快照) 以確認該執行個體已準備好進行快照。

該快照可能需要幾分鐘來完成。

6. 快照建立之後，在執行個體管理頁面上方選擇 Start (啟動) 以再次啟動您的執行個體。

此時，您應該擁有 Windows Server 執行個體的兩個快照，如下所示：



使用 Sysprep 快照來建立新執行個體。只有在執行 Sysprep 後，原始執行個體未如預期作用時，始可使用備份快照。

## 後續步驟

現在您已經擁有 Sysprep 和備份快照了，以下是您應該完成的一些後續步驟：

- 連線到您的原始執行個體，並確認您的應用程式在 Sysprep 執行之後如預期作用。如需詳細資訊，請參閱[使用 Amazon Lightsail Connect 到您的視窗伺服器執行個體](#)。
- 使用 Sysprep 快照建立新執行個體，連線至此執行個體，並確認您的應用程式在新的執行個體上作用正常。如需詳細資訊，請參閱[透過快照建立執行個體](#)。
- 在您確認執行 Sysprep 後原始執行個體功能正常，即可刪除您的備份快照。如需詳細資訊，請參閱[刪除快照](#)。
- 如果在執行 Sysprep 後，執行個體未如預期運作，請按照[透過快照建立執行個體](#)中的步驟進行操作，以便透過備份快照建立新執行個體。

## 建立 Lightsail 區塊儲存磁碟快照以進行備份或基準

您可以在 Amazon Lightsail 中建立磁碟快照，做為額外區塊儲存磁碟的備份。

您可以使用磁碟快照做為新磁碟或資料備份的基準。如果您定期建立磁碟快照，則快照為遞增。只有在您上次執行裝置快照之後發生變更的區塊會儲存至新的快照。雖然快照是遞增儲存，但快照刪除程序的设计方式，可讓您只需要儲存最新快照，就能復原整個磁碟。

如需詳細資訊，請參閱[快照](#)。

1. 在 Lightsail 首頁上，選擇儲存空間索引標籤。
2. 選擇您要建立快照的區塊儲存磁碟名稱。
3. 選擇 Snapshots (快照) 索引標籤。
4. 在頁面的手動快照部分中，選擇 Create snapshot (建立快照)，然後輸入快照的名稱。

資源名稱：

- 每個 Lightsail 帳戶 AWS 區域 中的每個項目都必須是唯一的。
  - 必須包含 2 至 255 個字元。
  - 開頭和結尾必須是英數字元或數字。
  - 可以包含英數字元、數字、句點、破折號和底線。
5. 選擇 Create (建立)。

您可以使用 Snapshotting。。。 (快照。。。) 查看您剛建立的快照。

快照完成後，您即可[從該快照建立另一個磁碟](#)。

## 在 Lightsail 中從快照建立區塊儲存磁碟

您可以從磁碟快照建立新的區塊儲存磁碟。如果要建立全新的磁碟，請另行參閱以下其中一個主題：[建立額外的區塊儲存磁碟 \(Linux/Unix\)](#) 或 [建立區塊儲存磁碟並將其附接至 Windows Server 執行個體](#)。

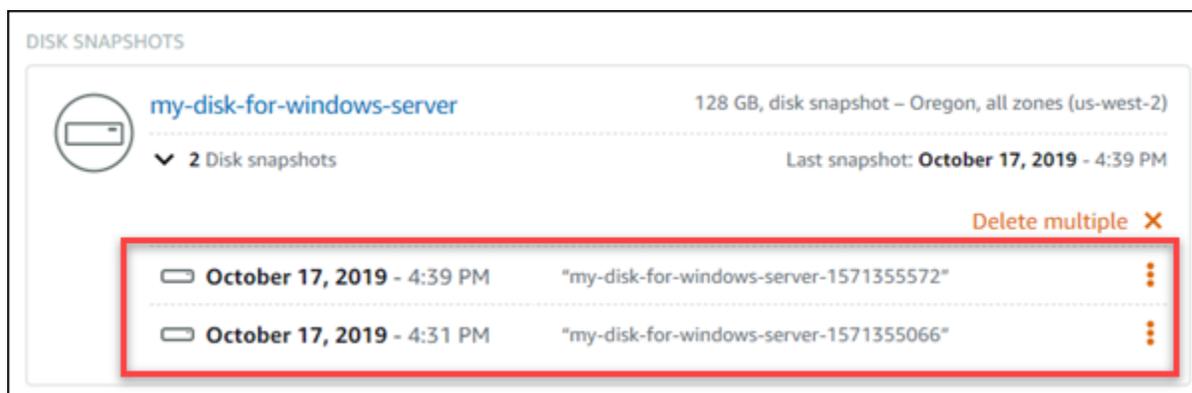
您可以使用區塊儲存磁碟的快照，做為新磁碟或資料備份的基準。如果您定期建立磁碟快照，則快照為遞增。只有在您上次執行磁碟快照之後發生變更的區塊會儲存至新的快照。雖然快照是遞增儲存，但快照刪除程序的設計方式，可讓您只需要儲存最新快照，就能復原整個磁碟。若要建立區塊儲存磁碟的快照，請參閱[建立區塊儲存磁碟快照](#)。

### 步驟 1：尋找您的磁碟快照，然後選擇建立新的磁碟

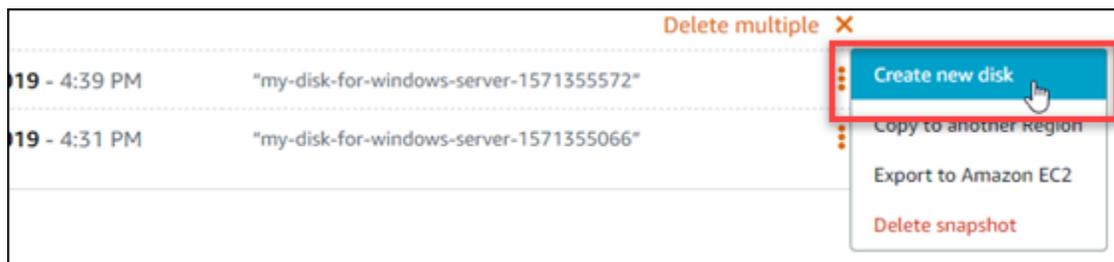
您可以在 Lightsail 的兩個位置之一，從磁碟快照建立新執行個體：Lightsail 首頁的 [快照] 索引標籤上，或在 [磁碟管理] 頁面的 [快照] 索引標籤上。

從 Lightsail 首頁

1. 在 Lightsail 首頁的左側導覽列上，選擇 [快照]。
2. 尋找磁碟的名稱，然後展開其下方的節點，即可查看該磁碟所有可用的快照。

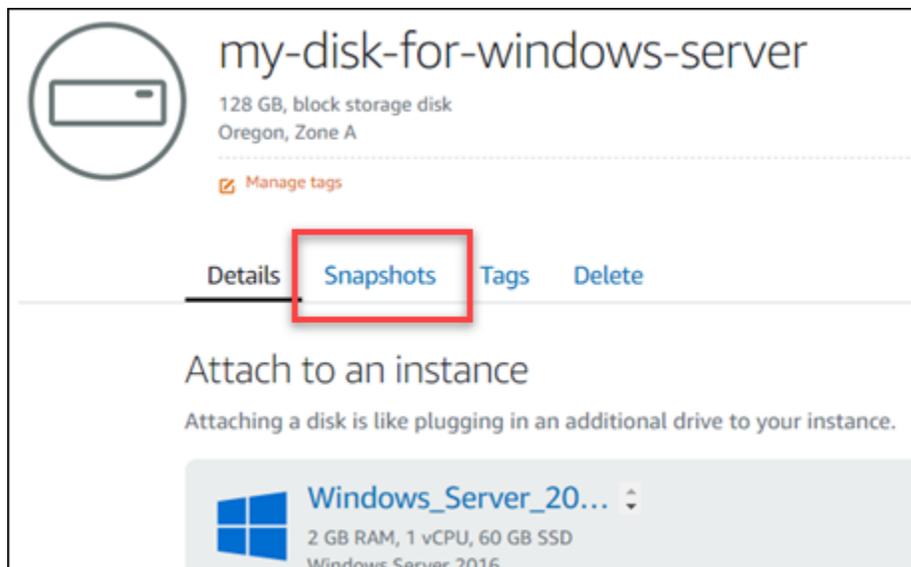


3. 在您要建立新磁碟的快照旁選擇動作選單圖示 (:)，然後選擇 Create new disk (建立新磁碟)。

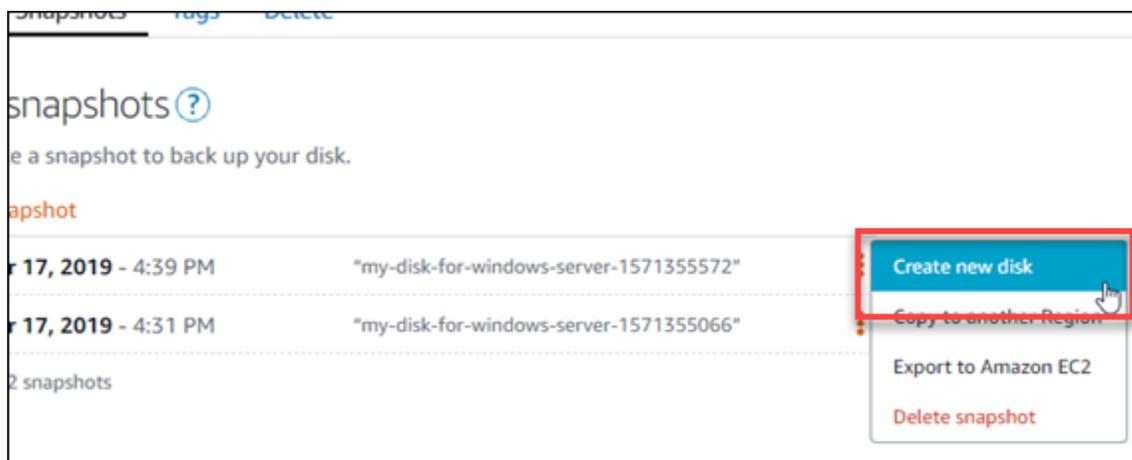


## 從磁碟管理 Lightsail

1. 在 Lightsail 首頁的左側導覽列上，選擇儲存空間索引標籤。
2. 選擇要檢視快照的磁碟名稱。
3. 選擇 Snapshots (快照) 索引標籤。



4. 在頁面的 Manual snapshots (手動快照) 部分中，在您要建立的新磁碟旁選擇動作選單圖示 (:)，然後選擇 Create new disk (建立新磁碟)。



## 步驟 2：從磁碟快照建立新磁碟

1. 選擇新磁碟的可用區域，或接受預設值 (us-east-2a)。  
您必須在與來源磁碟相同 AWS 區域 的位置建立新磁碟。
2. 為您的新磁碟選擇大小，它等於或大於來源快照的大小。

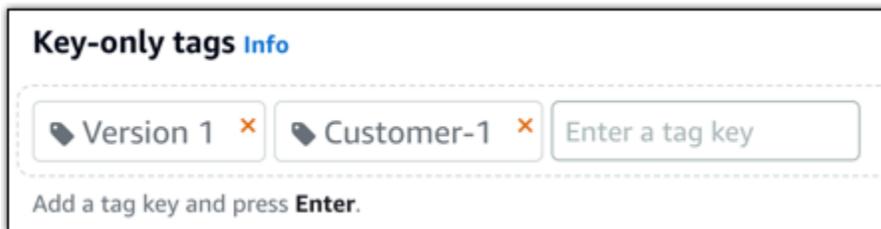
### 3. 輸入磁碟的名稱。

資源名稱：

- 每個 Lightsail 帳戶 AWS 區域 中的每個項目都必須是唯一的。
- 必須包含 2 至 255 個字元。
- 開頭和結尾必須是英數字元或數字。
- 可以包含英數字元、數字、句點、破折號和底線。

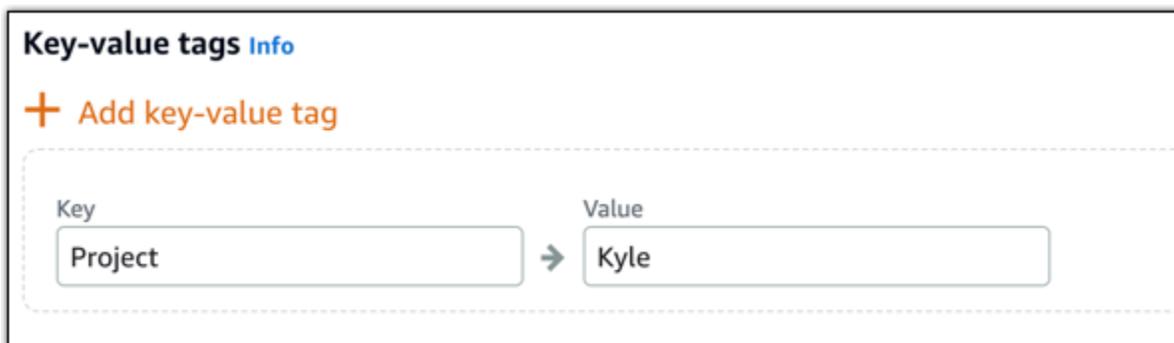
### 4. 選擇下列其中一個選項以新增標籤至您的磁碟：

- Add key-only tags (新增僅索引鍵標籤) 或 Edit key-only tags (編輯僅索引鍵標籤) (若標籤已新增)。在標籤索引鍵文字方塊中輸入新的標籤，接著按 Enter (輸入)。輸入標籤以新增之後，請選擇 Save (儲存)，如果不要新增則選擇 Cancel (取消)。



- Create a key-value tag (建立索引鍵值標籤)，接著將索引鍵輸入 Key (索引鍵) 文字方塊，將值輸入 Value (值) 文字方塊。完成輸入標籤後，請選擇 Save (儲存)，如果不要新增則選擇 Cancel (取消)。

鍵值標籤在儲存前一次只能新增一個。若要新增超過一個索引鍵值標籤，請重複之前的步驟。



#### **i** Note

如需有關僅索引鍵和索引鍵值標籤的詳細資訊，請參閱[標籤](#)。

## 5. 選擇 Create disk (建立磁碟)。

# 為 Lightsail 執行個體建立根磁碟區的快照

您可透過建立系統磁碟的快照，來在 Amazon Lightsail 中備份執行個體根磁碟區。接著從該快照建立新的區塊儲存磁碟，並將其連接至另一個執行個體，以便存取備份中的檔案。建議您在需要進行下列作業時執行此操作：

- 從失敗的執行個體根磁碟區復原資料。
- 建立執行個體根磁碟區的備份，如您為區塊儲存磁碟所做的那樣。

您可以使用 AWS Command Line Interface (AWS CLI) 或建立執行個體根磁碟區快照 AWS CloudShell。建立快照後，請使用 Lightsail 主控台從快照建立區塊儲存磁碟。然後，將該磁碟連接至執行中的執行個體，並從該執行個體進行存取。

### 內容

- [步驟 1：完成先決條件](#)
- [步驟 2：建立執行個體根磁碟區的快照](#)
- [步驟 3：從快照建立區塊儲存磁碟並將其連接至執行個體](#)
- [步驟 4：從執行個體存取區塊儲存磁碟](#)

## 步驟 1：完成先決條件

使用 AWS Command Line Interface (AWS CLI) 或 AWS CloudShell 建立執行個體根磁碟區快照。CloudShell 這是一個以瀏覽器為基礎的預先驗證殼層，您可以直接從 Lightsail 主控台啟動。如需詳細資訊，請參閱 [設定 AWS CLI 供 Lightsail 作業使用](#) 和 [使用管理 Lightsail 資源 AWS CloudShell](#)。

## 步驟 2：建立執行個體根磁碟區的快照

開啟 [終端機] CloudShell 或 [命令提示字元] 視窗，然後輸入下列指令以建立執行個體根磁碟區快照。

```
aws lightsail create-disk-snapshot --region AWSRegion --instance-name InstanceName --disk-snapshot-name DiskSnapshotName
```

在命令中：

- *AWSRegion* 使用執 AWS 區域 行個體的。
- *InstanceName* 使用您要備份其根磁碟區的執行個體名稱。
- *DiskSnapshotName* 具有要創建的新磁碟快照的名稱。

範例：

```
aws lightsail create-disk-snapshot --region us-west-2 --instance-  
name Amazon_Linux-32MB-Oregon-1 --disk-snapshot-name root-volume-linux
```

如果成功，您會看到類似如下的結果：

```
H:\>aws lightsail create-disk-snapshot --region us-west-2 --instance-name Amazon_Linux-32GB-Oregon-1  
--disk-snapshot-name root-volume-linux  
  
{  
  "operations": [  
    {  
      "status": "Started",  
      "resourceType": "DiskSnapshot",  
      "isTerminal": false,  
      "operationDetails": "Amazon_Linux-32GB-Oregon-1",  
      "statusChangedAt": 1548799955.599,  
      "location": {  
        "availabilityZone": "all",  
        "regionName": "us-west-2"  
      },  
      "operationType": "CreateDiskSnapshot",  
      "resourceName": "root-volume-linux",  
      "id": "99111111-1111-1111-1111-111111111111",  
      "createdAt": 1548799955.599  
    },  
    {  
      "status": "Started",  
      "resourceType": "Instance",  
      "isTerminal": false,  
      "operationDetails": "root-volume-linux",  
      "statusChangedAt": 1548799955.599,  
      "location": {  
        "availabilityZone": "us-west-2a",  
        "regionName": "us-west-2"  
      },  
      "operationType": "CreateDiskSnapshot",  
      "resourceName": "Amazon Linux-32GB-Oregon-1",  
      "id": "99111111-1111-1111-1111-111111111111",  
      "createdAt": 1548799955.599  
    }  
  ]  
}
```

請稍後幾分鐘，待快照建立完畢。建立完成後，您可以選擇 [快照] 索引標籤並捲動至 [磁碟快照] 區段，在 Lightsail 首頁中檢視它，如下列範例所示。

The screenshot displays the 'Snapshots' tab in the Amazon Lightsail console. It is sorted by Region and then by Date. The page is divided into two sections: 'INSTANCE SNAPSHOTS' and 'DISK SNAPSHOTS'. Under 'INSTANCE SNAPSHOTS', the 'Ohio (us-east-2)' region is shown with one snapshot: 'Magento-512MB-Ohio-1', which has 512 MB RAM, 1 vCPU, and 20 GB SSD. Under 'DISK SNAPSHOTS', the 'Oregon (us-west-2)' region is shown with two snapshots: 'Windows\_Server\_2016-32GB-Oregon-1' and 'Amazon\_Linux-32GB-Oregon-1'. The 'Amazon\_Linux-32GB-Oregon-1' snapshot has a red circle around the 'root-volume-linux' label.

### 步驟 3：從快照建立區塊儲存磁碟並將其連接至執行個體

如果您必須存取磁碟內容，則可從執行個體根磁碟區快照建立新的區塊儲存磁碟，並將該磁碟連接至另一個執行個體。建議您在需要從失敗的執行個體根磁碟區復原資料時，再執行此操作。

#### Note

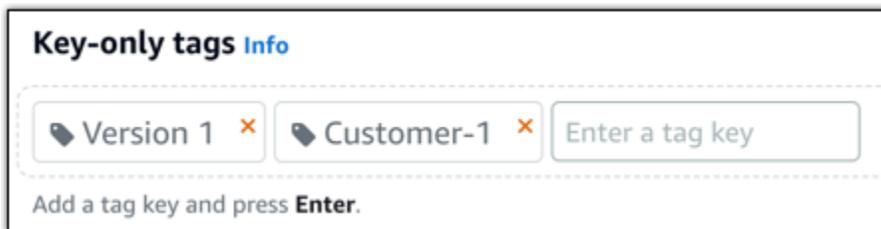
新的區塊儲存磁碟會建立在與來源快照 AWS 區域 相同的位置。若要在不同區域建立區塊儲存磁碟，請將快照複製到所需區域，然後從該快照複本建立新的磁碟。如需詳細資訊，請參閱[將快照從一個快照複製 AWS 區域 到另一個](#)。

1. 登入主 [Lightsail](#) 台。
2. 在 Lightsail 首頁上，選擇 [快照] 索引標籤。
3. 選擇欲使用根磁碟區磁碟快照旁顯示的動作功能表圖示 (:)，接著選擇 Create new disk (建立新磁碟)。
4. 選擇該磁碟的可用區域，或接受預設值。

5. 選擇該磁碟的大小，其應等於或大於來源磁碟的大小。
6. 輸入磁碟的名稱。

資源名稱：

- 每個 Lightsail 帳戶 AWS 區域 中的每個項目都必須是唯一的。
  - 必須包含 2 至 255 個字元。
  - 開頭和結尾必須是英數字元或數字。
  - 可以包含英數字元、數字、句點、破折號和底線。
7. 選擇下列其中一個選項以新增標籤至您的磁碟：
- Add key-only tags (新增僅索引鍵標籤) 或 Edit key-only tags (編輯僅索引鍵標籤) (若標籤已新增)。在標籤索引鍵文字方塊中輸入新的標籤，接著按 Enter (輸入)。輸入標籤以新增之後，請選擇 Save (儲存)，如果不要新增則選擇 Cancel (取消)。



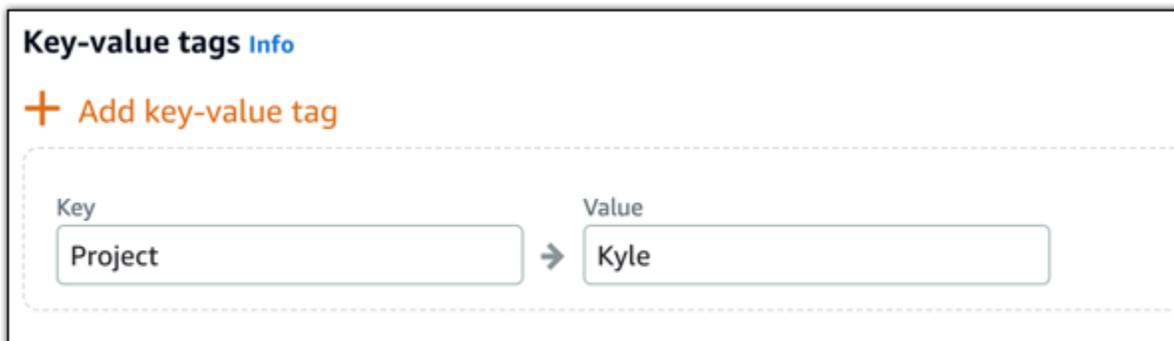
Key-only tags Info

Version 1 × Customer-1 × Enter a tag key

Add a tag key and press Enter.

- Create a key-value tag (建立索引鍵值標籤)，接著將索引鍵輸入 Key (索引鍵) 文字方塊，將值輸入 Value (值) 文字方塊。完成輸入標籤後，請選擇 Save (儲存)，如果不要新增則選擇 Cancel (取消)。

鍵值標籤在儲存前一次只能新增一個。若要新增超過一個索引鍵值標籤，請重複之前的步驟。



Key-value tags Info

+ Add key-value tag

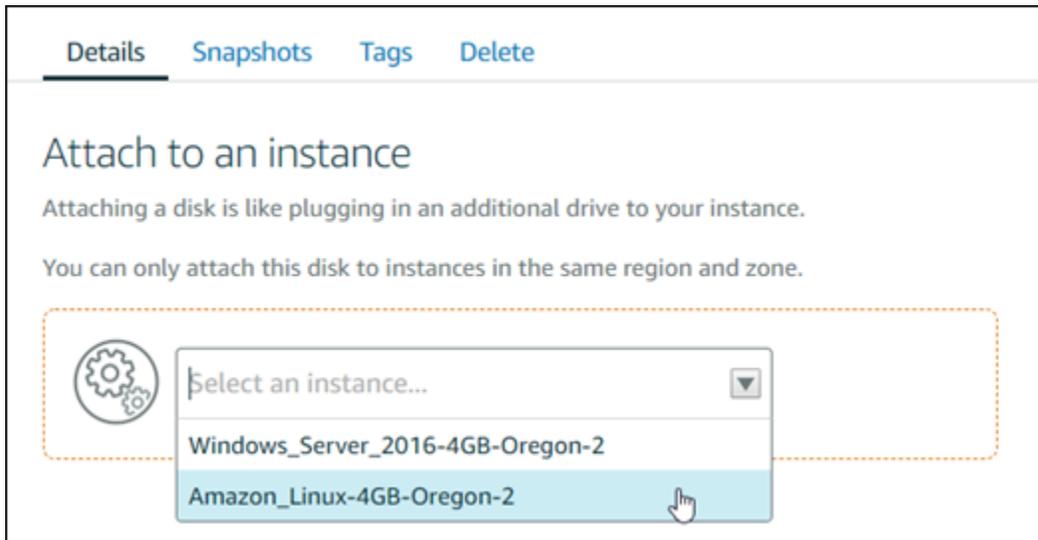
Key Value

Project → Kyle

**Note**

如需有關僅索引鍵和索引鍵值標籤的詳細資訊，請參閱[標籤](#)。

- 選擇 Create disk (建立磁碟)。
- 完成磁碟建立作業後，在 Select an instance (選取執行個體) 下拉式功能表中選擇要連接該磁碟的執行個體。如以下範例所示。



- 選擇 Attach (連接)，以便將磁碟連接至所選執行個體。

系統會隨即將磁碟連接至該執行個體。接著，請將磁碟掛載至 Linux 或讓其在 Windows 上線，使適用的作業系統可進行存取。如需詳細資訊，請參閱本指南下一節的從執行個體存取區塊儲存磁碟。

## 步驟 4：從執行個體存取區塊儲存磁碟

您需要將區塊儲存磁碟掛載至 Linux 或 Unix，或是讓其在 Windows 上線，才能在區塊儲存磁碟連接至執行個體後進行存取。

在 Linux 或 Unix 執行個體上掛載和存取區塊儲存磁碟

- 在 [Lightsail 首頁](#) 上，為您附加區塊儲存磁碟的 Linux 或 Unix 執行個體選擇以瀏覽器為基礎的 SSH 用戶端圖示。



2. 在以瀏覽器為基礎的SSH用戶端連線之後，輸入下列命令以檢視連接至執行個體的區塊儲存磁碟裝置：

```
lsblk
```

您應該會看到類似以下範例的結果。在本範例中，連接至執行個體的 `xvdf1` 區塊儲存磁碟沒有掛載點，因此其處於尚未掛載的狀態。此外，結果會省略裝置名稱中的 `/dev/`，所以實際的裝置名稱是 `/dev/xvdf1`。

```
[ec2-user@ip-172.31.0.11 ~]$ lsblk
NAME      MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda      202:0    0   80G  0  disk
└─xvda1   202:1    0   80G  0  part /
xvdf      202:80   0  640G  0  disk
└─xvdf1   202:81   0  640G  0  part
```

3. 輸入下列命令，即可為區塊儲存磁碟建立掛載點。

```
sudo mkdir MountPoint
```

在命令中，替換 `MountPoint` 使用將掛載和存取區塊儲存磁碟的目錄名稱。

範例：

```
sudo mkdir xvdf
```

4. 輸入下列命令，以便將區塊儲存磁碟掛載至您在上一步建立的掛載點。

```
sudo mount /dev/DeviceName MountPoint
```

在命令中：

- *DeviceName* 與區塊儲存磁碟裝置的名稱。
- *MountPoint* 使用您在上一個步驟中建立的掛接點目錄。

範例：

```
sudo mount /dev/xvdf1 xvdf
```

5. 若要檢視連接至執行個體的區塊儲存磁碟裝置，請輸入下列命令：

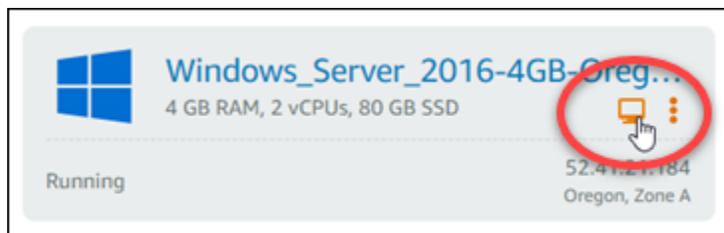
```
lsblk
```

您應該會看到類似以下範例的結果。在此範例中，*xvdf1* 裝置現已安裝並可存取 */home/ec2-user/xvdf* 目錄。您現在可以前往掛載點目錄，存取該區塊儲存磁碟及其內容。

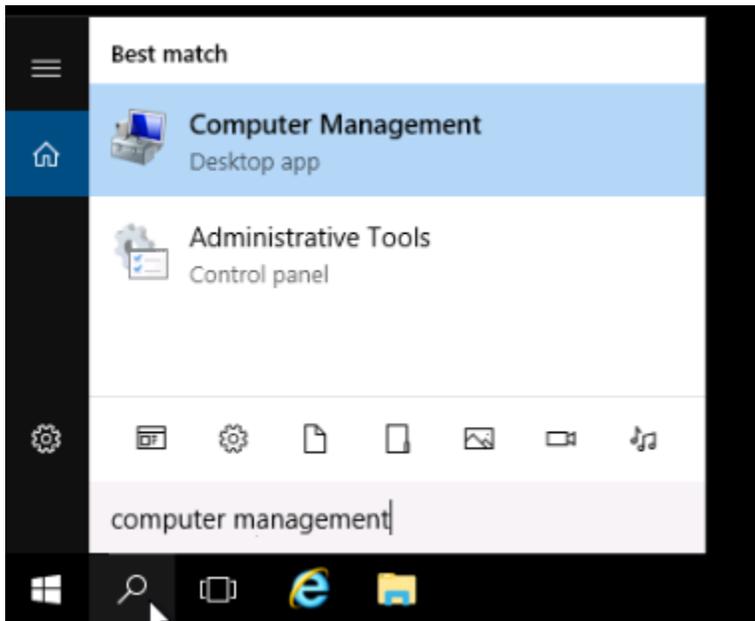
```
[ec2-user@ip-10-10-10-10 ~]$ lsblk
NAME        MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda        202:0    0   80G  0 disk
└─xvda1     202:1    0   80G  0 part /
xvdf        202:80   0  640G  0 disk
└─xvdf1     202:81   0  640G  0 part /home/ec2-user/xvdf
```

在 Windows 執行個體中將區塊儲存磁碟上線並進行存取

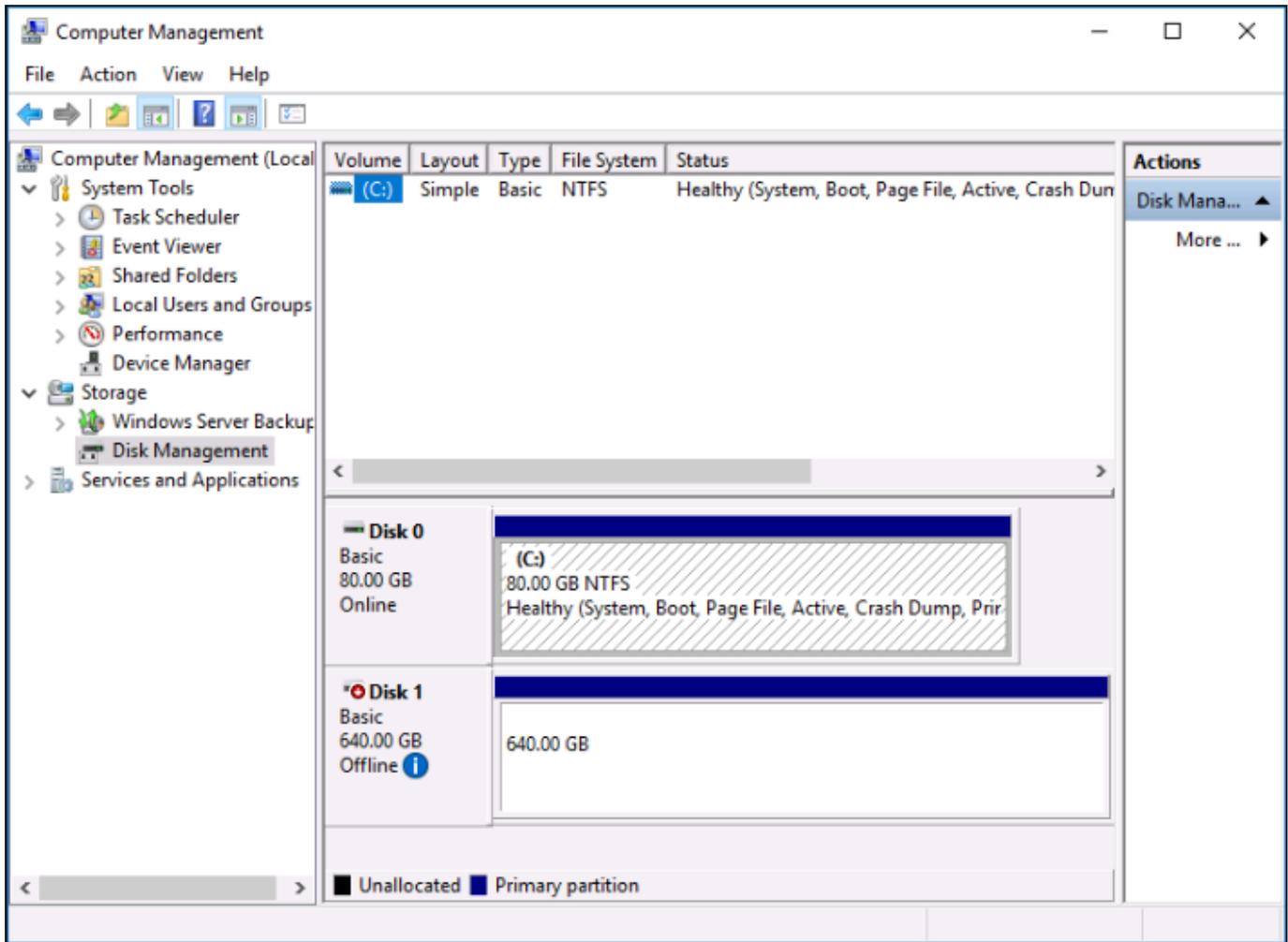
1. 在 [Lightsail 首頁](#) 上，為您附加區塊儲存磁碟的 Windows 執行個體選擇以瀏覽器為基礎的 RDP 用戶端圖示。



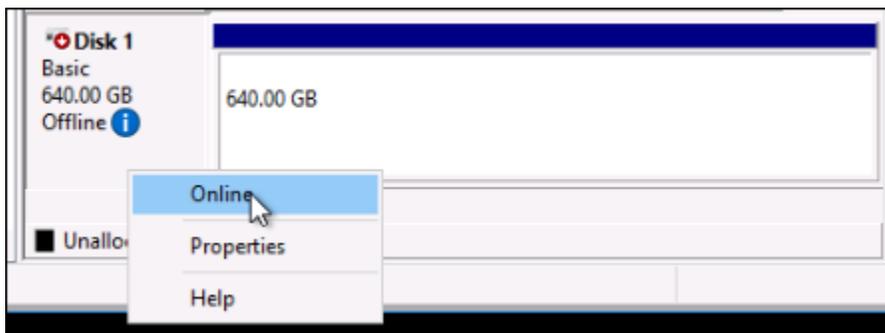
2. 連線瀏覽器 SSH 用戶端之後，在 Windows 工作列中搜尋「電腦管理」，然後從結果中選擇「電腦管理」。



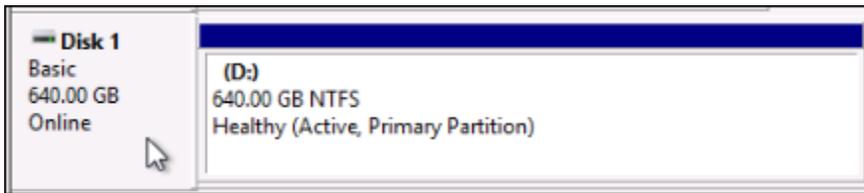
3. 在 Computer Management (電腦管理) 主控台的左側導覽功能表中，選擇 Disk Management (磁碟管理)，如以下範例所示。



4. 找到您最近連接至執行個體的磁碟。該磁碟應標示為 Offline (離線)。
5. 在 Offline (離線) 標籤上按一下滑鼠右鍵，然後選擇 Online (上線)。



磁碟的標籤現應為 Online (上線)，且會具備相關聯的磁碟機代號。現在，您可以開啟檔案總管並瀏覽至指定的磁碟機代號，藉此存取區塊儲存磁碟及其內容。

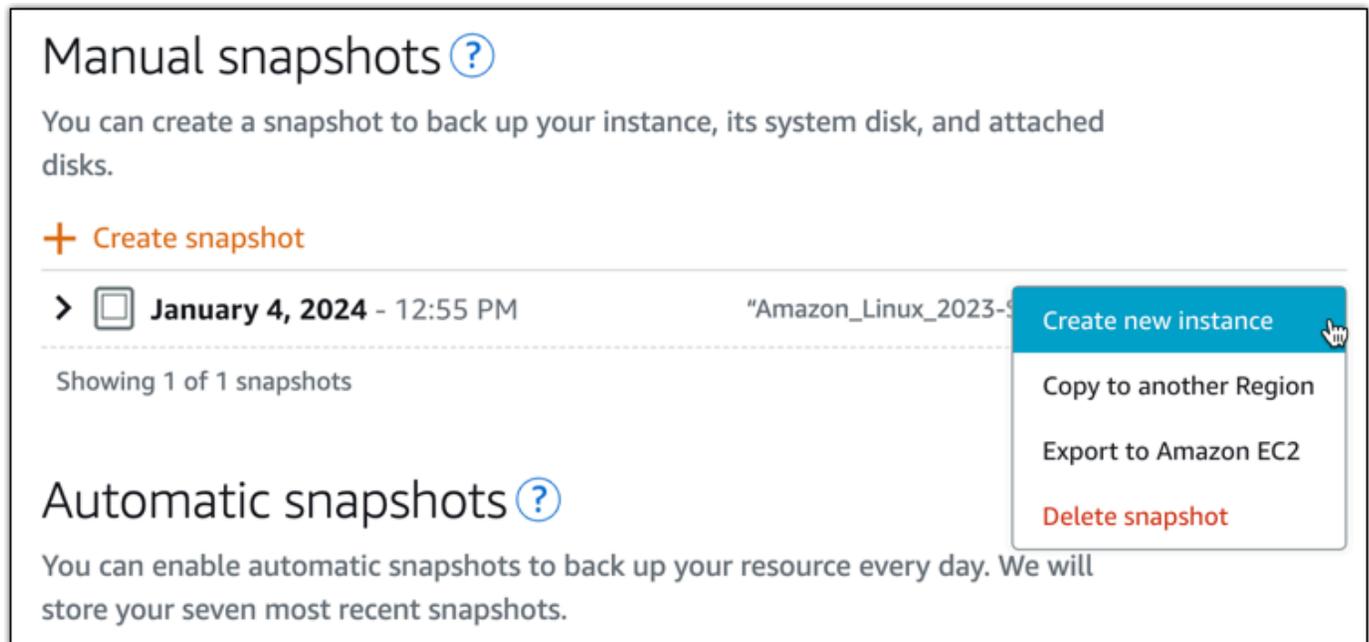


## 從快照建立 Lightsail 執行個體

在 Lightsail 中建立快照之後，您可以從該快照建立新的實體。您可以變更新執行個體的屬性，例如執行個體大小和網路類型 — 雙堆疊或IPv6僅。新執行個體包括系統磁碟和您新增的連接區塊儲存磁碟。

您必須擁有執行個體的快照，才能從該快照建立另一個執行個體。如需詳細資訊，請參閱 [使用快照備份 Linux/UniLightsail 執行個體](#) 或 [建立您的視窗伺服器執行個體的快照](#)。

1. 在 Lightsail 主控台上，選擇您要快照的執行個體，以建立新的執行個體。
2. 選擇 Snapshots (快照) 索引標籤。
3. 在 [手動快照] 區段中，選擇快照旁邊的動作功能表圖示 ( )，然後選擇 [建立新執行個體]。



4. [從快照建立執行個體] 頁面隨即開啟。選擇您要使用的選用設定。例如，您可以變更可用區域、[新增啟動指令碼](#)，或[變更連接至執行個體的方式](#)。
5. 為您的新執行個體選擇方案 (或套裝方案)。您可以選擇建立使用雙堆疊 (IPv4和IPv6) 執行個體計劃的執行個體，也可以選擇IPv6僅建立執行個體。您也可以選擇比原始執行個體大的套裝軟體大小。如需IPv6僅執行個體計劃的詳細資訊，請參閱 [為 Lightsail 執行個體設定僅限 IPv4 的網路](#)。

**Note**

您無法建立使用比原始執行個體更小套裝軟體大小的執行個體。

**Choose a new instance plan** [Info](#)

You can pick a machine the same size or larger than the source snapshot.

**Select an IP address type - new** [Info](#)

**Dual stack** Recommended  
Includes both a public IPv4 and IPv6 address. Suitable for most use cases due to wide compatibility with IPv4 addresses.

**IPv6 only**  
Includes a public IPv6 address. An advanced option for use cases where IPv6 access limitations are acceptable.

**Updated pricing for instances with public IPv4** [Learn more](#)

Starting June 1, 2024, all Lightsail instance bundles that include a public IPv4 address will incur a new price. You can now launch IPv6-only bundles if your instance doesn't require a public IPv4 address.

**6. 輸入您執行個體的名稱。**

資源名稱：

- 在您 AWS 區域 的每個 Lightsail 帳戶中都必須是唯一的。
- 必須包含 2 至 255 個字元。
- 必須以英數字元開頭和結尾。
- 可以包含英數字元、句號、破折號和底線。

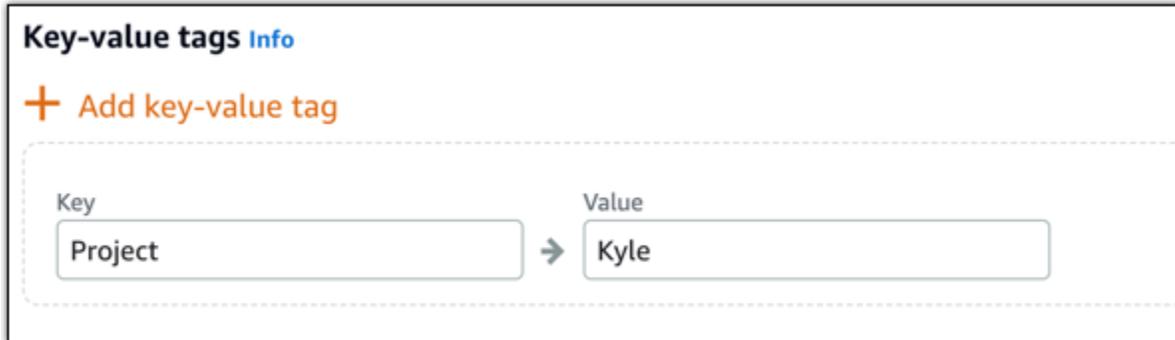
**7. 選擇下列其中一個選項以新增標籤至您的執行個體：**

- Add key-only tags (新增僅索引鍵標籤) 或 Edit key-only tags (編輯僅索引鍵標籤) (若標籤已新增)。在文字方塊中輸入新標籤，然後按 Enter。選擇儲存或取消。

**Key-only tags** [Info](#)  
    
Add a tag key and press **Enter**.

- 建立鍵值標籤，然後在機碼文字方塊中輸入機碼，並在「值」文字方塊中輸入一個值。選擇儲存或取消。

鍵值標籤在儲存前一次只能新增一個。若要新增超過一個索引鍵值標籤，請重複之前的步驟。



The screenshot displays the 'Key-value tags' configuration interface. At the top, there is a title 'Key-value tags Info' and a button labeled '+ Add key-value tag'. Below this is a dashed-line box containing two input fields. The first field is labeled 'Key' and contains the text 'Project'. The second field is labeled 'Value' and contains the text 'Kyle'. A right-pointing arrow is positioned between the two fields, indicating a mapping from the key to the value.

#### Note

如需有關僅索引鍵和索引鍵值標籤的詳細資訊，請參閱[標籤](#)。

## 8. 選擇 建立執行個體。

Lightsail 會開啟管理頁面，您可以在其中管理新執行個體。

#### Important

原始執行個體的自訂防火牆規則不會複製到您從快照建立的新執行個體。只有預設規則會複製到新執行個體。如需詳細資訊，請參閱[預設執行個體防火牆規則](#)。

## 將 Lightsail 執行個體、儲存體或資料庫從快照增加大小

您有可能會遇到這種情況。您的雲端專案不斷成長，立刻需要更多的運算能力！我們可以幫助您達成此目標。若要擴大 Lightsail 執行個體、區塊儲存磁碟或資料庫的大小，請建立資源的快照集，然後使用快照建立該資源的新較大版本。

#### Note

您無法使用比原始資源更小的計劃大小，從快照建立資源，例如您無法從 8 GB 執行個體前往 2 GB 執行個體。

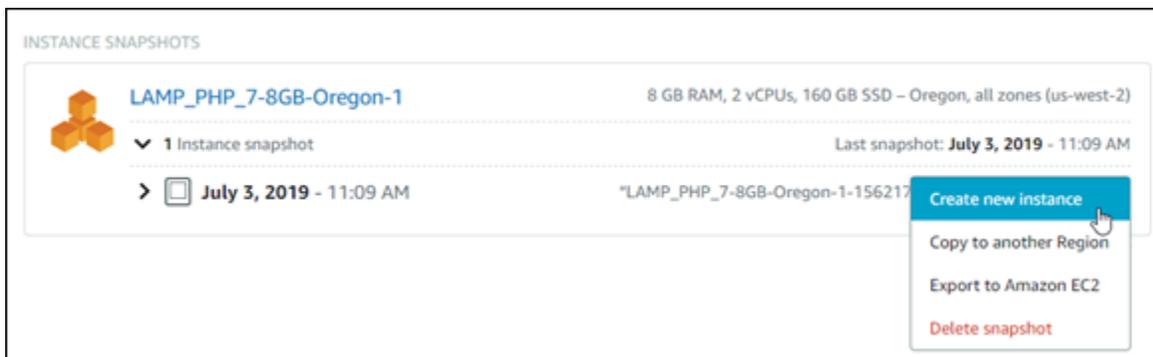
當您停止並啟動執行個體時，指派給執行個體的預設公用IPv4位址將會變更。您可以選擇性地建立靜態IPv4位址，並將其附加至執行個體。透過靜態 IP 地址，您可以將地址快速重新映射至帳戶中的其他執行個體，以遮罩執行個體或軟體的故障狀況。或者，您也可以將地址在網域的DNS記錄中指定靜態 IP 位址，讓網域指向您的執行個體。如需詳細資訊，請參閱 [IP 地址](#)。

## 必要條件

您需要 Lightsail 執行個體、區塊儲存磁碟或資料庫的快照。如需詳細資訊，請參閱 [快照](#)。

## 建立您的資源

1. 登入主 [Lightsail 台](#)。
2. 選擇 Snapshots (快照) 索引標籤。
3. 尋找您要使用其快照建立更大新資源的 Lightsail 資源，然後選擇向右箭號以展開快照清單。
4. 選擇您想要使用之快照旁邊的省略符號圖示，然後選擇 Create new (建立新項目)。



5. 在 Create (建立) 頁面上，您有幾個選用設定可供選擇。例如，您可以變更可用區域。對於執行個體，您可以 [新增啟動指令碼](#)，或 [變更為用於連線至指令碼的SSH金鑰](#)。

您可以接受所有預設值，並移至下一個步驟。

6. 為您的新資源選擇計劃 (或搭售套件)。此時，您可以選擇比原始資源更大的搭售套件大小 (如果要的話)。

### Note

您無法使用小於原始資源的計劃大小來建立資源。小於原始資源的搭售套件選項將無法使用。

7. 輸入您執行個體的名稱。

資源名稱：

- 每個 Lightsail 帳戶 AWS 區域 中的每個項目都必須是唯一的。
- 必須包含 2 至 255 個字元。
- 開頭和結尾必須是英數字元或數字。
- 可以包含英數字元、數字、句點、破折號和底線。

8. 選擇 Create (建立)。

Lightsail 會帶您前往新資源的管理頁面，然後您就可以開始對其進行管理。

## 使用 Lightsail 快照建立更大的執行個體、區塊儲存磁碟或資料庫 AWS CLI

您有可能會遇到這種情況。您的雲端專案不斷成長，立刻需要更多的運算能力！我們可以幫助您達成此目標。您可以在 Lightsail 主控台內執行所有操作，或者使用 AWS Command Line Interface (AWS CLI) 來執行這項操作。

我們將示範如何拍攝目前 Lightsail 執行個體的快照，並根據該快照建立具有所需運算能力的新執行個體。

### Note

目前，我們不支援從快照建立較小的執行個體 (或搭售套件)。您只能建立大小相同或更大的執行個體。

## 必要條件

1. 首先，如果您還沒有，則需要安裝 AWS CLI。若要進一步了解，請參閱[安裝 AWS Command Line Interface](#)。請確定您設定 [AWS CLI](#)。
2. 您也需要執行個體的快照以進行此項作業。若要進一步了解，請參閱[建立 Linux 或 Unix 執行個體的快照](#)。

## 步驟 1：取得您的快照名稱

這可能很明顯，但您需要快照名稱，然後執行此 AWS CLI 命令來建立更大的執行個體。好消息是它很容易取得。

1. 在中 AWS CLI，鍵入下列內容。

```
aws lightsail get-instance-snapshots
```

您應該會看到類似下列的輸出。

```
{
  "instanceSnapshots": [
    {
      "fromInstanceName": "WordPress-512MB-EXAMPLE",
      "name": "WordPress-512MB-EXAMPLE-system-1234567891011",
      "sizeInGb": 20,
      "resourceType": "InstanceSnapshot",
      "fromInstanceArn":
        "arn:aws:lightsail:us-east-1:123456789101:Instance/86f49ee4-26cc-4802-9b0d-12345EXAMPLE",
      "state": "available",
      "arn": "arn:aws:lightsail:us-east-1:123456789101:InstanceSnapshot/
c87acb5f-851e-4fbc-94f1-12345EXAMPLE",
      "fromBundleId": "nano_1_0",
      "fromBlueprintId": "wordpress_4_6_1",
      "createdAt": 1480898073.653,
      "location": {
        "availabilityZone": "all",
        "regionName": "us-east-2"
      }
    }
  ]
}
```

2. 將 name (名稱) 值複製到您之後可以取得的位置。這是您將會在 AWS CLI 命令中使用的 `--instance-snapshot-name` 值。

## 步驟 2：選擇搭售套件

搭售套件只是一個定價計劃和執行個體的組態。例如，以中型 Linux 為基礎的服務包 USD 每月花費 24 美元，而且有 4.0 GB 的儲存空間 RAM、80 GB 的 SSD 儲存空間等等。

如果您一開始使用較小的搭售套件，但現在需要更多的運算能力，您可能會想要升級到較大的搭售套件。如需詳細資訊，請參閱[透過快照建立較大的執行個體、區塊儲存磁碟或資料庫](#)。

### Important

您無法從快照重新調整為較小的搭售套件。如果您要建立較小的搭售套件，必須重新開始。

1. 鍵入以下 AWS CLI 命令。

```
aws lightsail get-bundles
```

輸出內容應如下所示。

```
{
  "bundles": [
    {
      "price": 5.0,
      "cpuCount": 2,
      "diskSizeInGb": 20,
      "bundleId": "nano_3_0",
      "instanceType": "nano",
      "isActive": true,
      "name": "Nano",
      "power": 298,
      "ramSizeInGb": 0.5,
      "transferPerMonthInGb": 1024,
      "supportedPlatforms": [
        "LINUX_UNIX"
      ],
    },
    {
      "price": 7.0,
      "cpuCount": 2,
      "diskSizeInGb": 40,
      "bundleId": "micro_3_0",
      "instanceType": "micro",
    }
  ]
}
```

```
    "isActive": true,
    "name": "Micro",
    "power": 500,
    "ramSizeInGb": 1.0,
    "transferPerMonthInGb": 2048,
    "supportedPlatforms": [
      "LINUX_UNIX"
    ],
  },
  {
    "price": 12.0,
    "cpuCount": 2,
    "diskSizeInGb": 60,
    "bundleId": "small_3_0",
    "instanceType": "small",
    "isActive": true,
    "name": "Small",
    "power": 1000,
    "ramSizeInGb": 2.0,
    "transferPerMonthInGb": 3072,
    "supportedPlatforms": [
      "LINUX_UNIX"
    ],
  },
  {
    "price": 24.0,
    "cpuCount": 2,
    "diskSizeInGb": 80,
    "bundleId": "medium_3_0",
    "instanceType": "medium",
    "isActive": true,
    "name": "Medium",
    "power": 2000,
    "ramSizeInGb": 4.0,
    "transferPerMonthInGb": 4096,
    "supportedPlatforms": [
      "LINUX_UNIX"
    ],
  },
  {
    "price": 44.0,
    "cpuCount": 2,
    "diskSizeInGb": 160,
    "bundleId": "large_3_0",
```

```
        "instanceType": "large",
        "isActive": true,
        "name": "Large",
        "power": 3000,
        "ramSizeInGb": 8.0,
        "transferPerMonthInGb": 5120,
        "supportedPlatforms": [
            "LINUX_UNIX"
        ],
    },
]
}
```

2. 找到您想要的套裝軟體的bundleId值。如需詳細資訊，請 [Lightsail 定價](#)。

### 第 3 步：編寫 AWS CLI 命令並創建新實例

現在您已有參數值，您已準備好編寫和執行您的命令以建立執行個體！

1. 輸入下列內容。

```
aws lightsail create-instances-from-snapshot --instance-names
MyNewInstanceFromSnapshot --availability-zone us-east-1a --instance-snapshot-name
WordPress-512MB-EXAMPLE-system-1234567891011 --bundle-id medium_1_0
```

輸出內容應如下所示。

```
{
  "operations": [
    {
      "status": "Started",
      "resourceType": "Instance",
      "isTerminal": false,
      "statusChangedAt": 1486863990.961,
      "location": {
        "availabilityZone": "us-east-2a",
        "regionName": "us-east-2"
      },
      "operationType": "CreateInstance",
      "resourceName": "MyNewInstanceFromSnapshot",
      "id": "30fec45e-e7d7-4e18-96c8-12345EXAMPLE",
      "createdAt": 1486863989.784
    }
  ]
}
```

```
    }  
  ]  
}
```

### Note

您也可以使用傳回區域和可用區域的清單 AWS CLI。只需輸入 `aws lightsail get-regions --include-availability-zones` 與您的 `get-regions` 請求，即可傳回可用區域清單。

2. 現在，在 Lightsail 主控台中開啟您的新執行個體並開始修改它。

## 後續步驟

從快照建立新執行個體之後，接下來您可以執行以下任務：

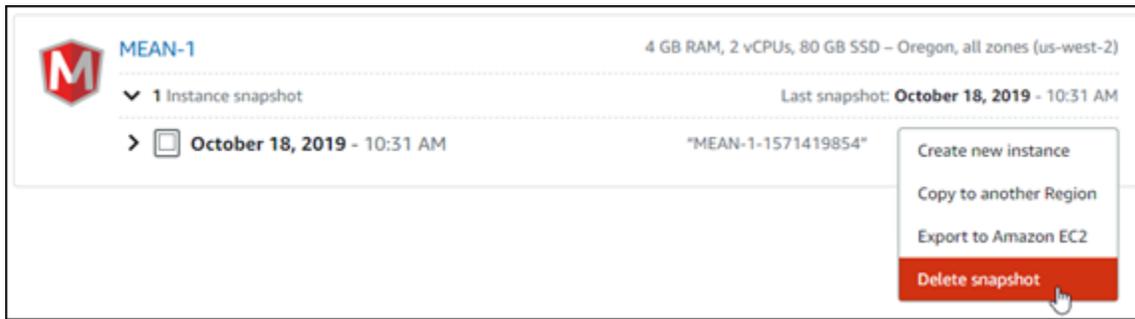
- 如果您已不再需要舊執行個體，可以將其刪除。您可以使用 Lightsail 控制台或[刪除CLI](#)實例命令來執行此操作。
- 如果您不再需要舊快照，可以將其刪除。您可以使用 Lightsail 主控台或[delete-instance-snapshot CLI指令](#)來執行此操作。
- 如果您有靜態 IP 地址連接至舊執行個體，您可能會想要保留此 IP 地址，並將它連接至新的執行個體。您可以使用主控台執行這項作業。請參閱[建立靜態 IP 地址並將它連接至執行個體](#)。

## 刪除未使用的 Lightsail 快照以避免每月費用

如果您不再需要 Amazon Lightsail 中的執行個體、資料庫和磁碟快照，請刪除這些快照，以避免產生每月費用。

### 刪除個別快照

1. 在 [Lightsail 主控台](#)上，選擇 [快照] 索引標籤。
2. 找出您要刪除其快照的 Lightsail 資源，然後選擇向右箭號以展開該資源的可用快照清單。
3. 選擇您要刪除之快照旁邊的動作選單圖示 (:)，然後選擇 Delete snapshot (刪除快照)。



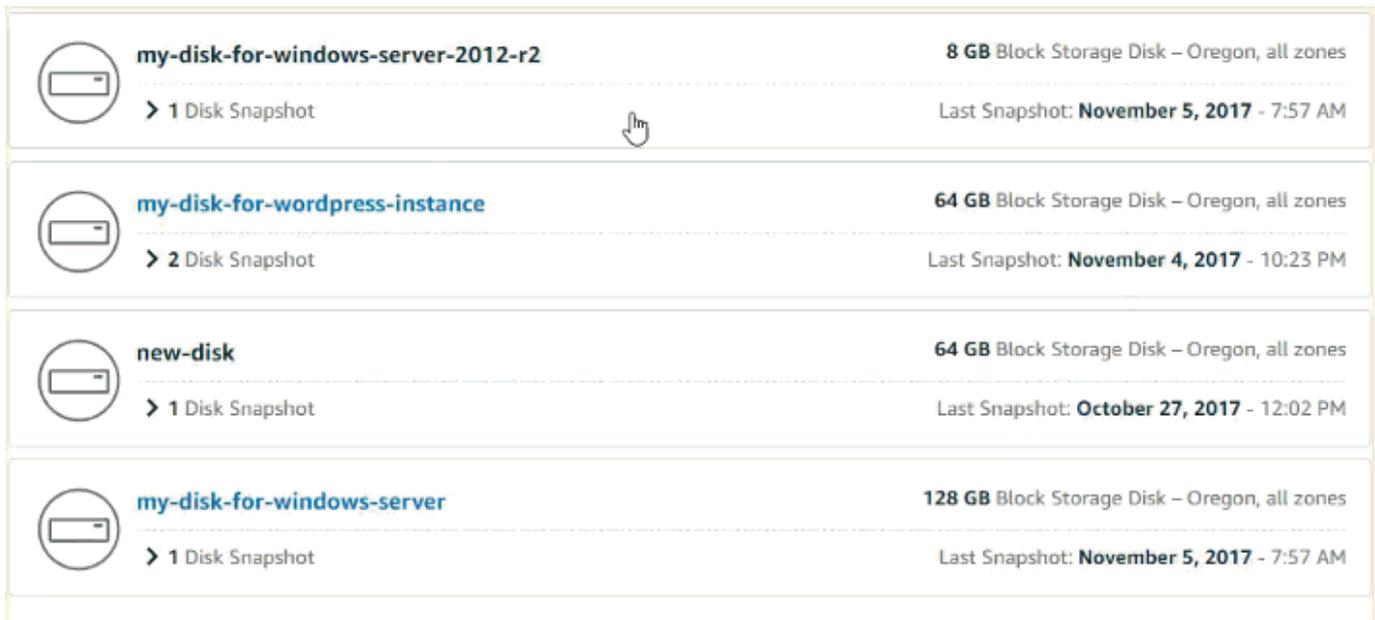
4. 選擇 Yes (是)，確認要刪除該快照。

#### **⚠ Important**

這是永久性操作，而且無法還原。刪除快照後，您將失去該快照上的所有資料。

### 刪除多個快照

1. 在 Lightsail 首頁中，選擇快照。
2. 找出您要刪除其快照的 Lightsail 資源，然後選擇向右箭號以展開快照清單。



3. 選擇 Delete multiple (刪除多個)。
4. 選擇要刪除的快照，然後選擇 Delete (刪除)。
5. 選擇 Yes (是)，確認要刪除這些快照。

### Important

這是永久性操作，而且無法還原。刪除這些快照後，您將失去快照上的所有資料。

## 在其中複製 Lightsail 快照 AWS 區域

在 Amazon Lightsail 中，您可以將執行個體快照和區塊儲存磁碟快照從一個快照複製 AWS 區域 到另一個或同一區域內。如果您在某個區域中建立並設定了資源，但後來決定不同的區域較為適當，請在區域之間複製快照。或是您想跨多個區域複製您的資源。本指南說明複製快照的 Lightsail 序。

### 必要條件

建立您要複製的 Lightsail 執行個體或區塊儲存磁碟的快照。如需詳細資訊，請參閱下列其中一項指南：

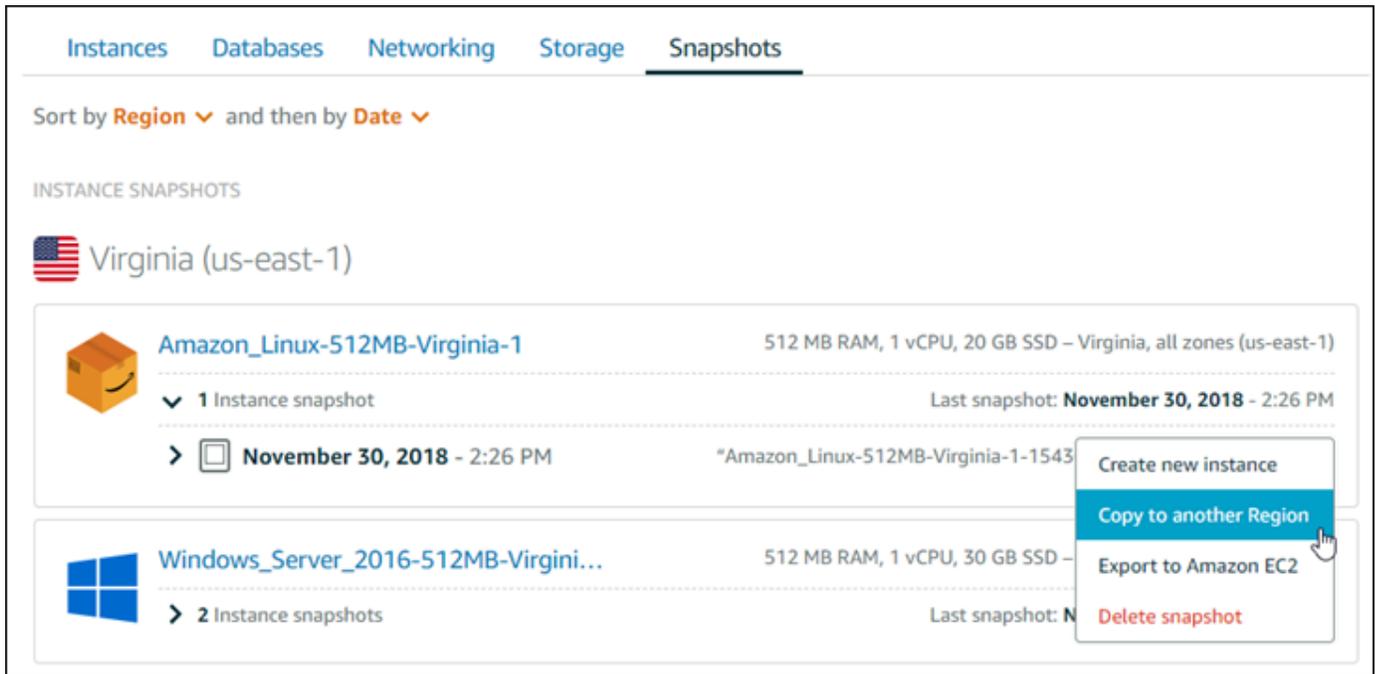
- [建立 Linux 或 Unix 執行個體快照](#)
- [建立 Windows Server 執行個體快照](#)
- [建立區塊儲存磁碟快照](#)

### 複製快照

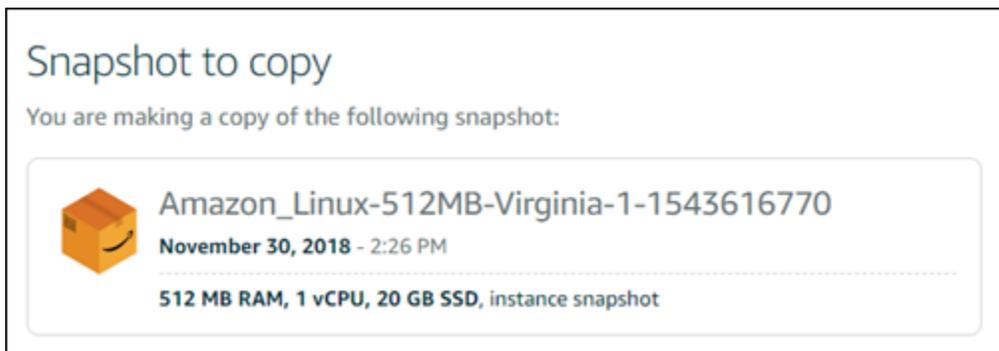
您可以將 Lightsail 執行個體快照和區塊儲存磁碟快照從一個快照複製 AWS 區域 到另一個或相同區域內。

#### 複製 Lightsail 照

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁中，選擇快照索引標籤。
3. 找出您想複製的執行個體或區塊儲存磁碟，接著展開節點以檢視該資源可用的快照。
4. 針對所選的快照選擇動作選單圖示 (:)，接著選擇 Copy to another Region (複製到另一個區域)。



5. 在 Copy a snapshot (複製快照) 頁面上 Snapshot to copy (要複製的快照) 部分，確認顯示的快照詳細資訊符合來源執行個體或區塊儲存磁碟的規格。

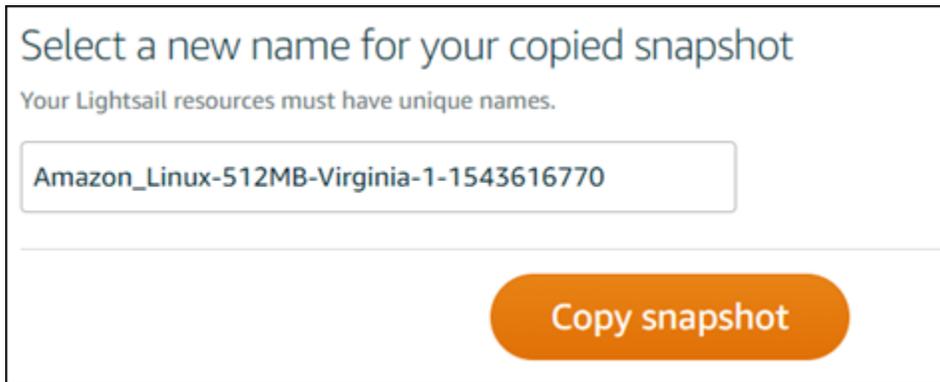


6. 在頁面的 Select a Region (選取區域) 部分，選擇快照複本的區域。
7. 輸入快照複本的名稱。

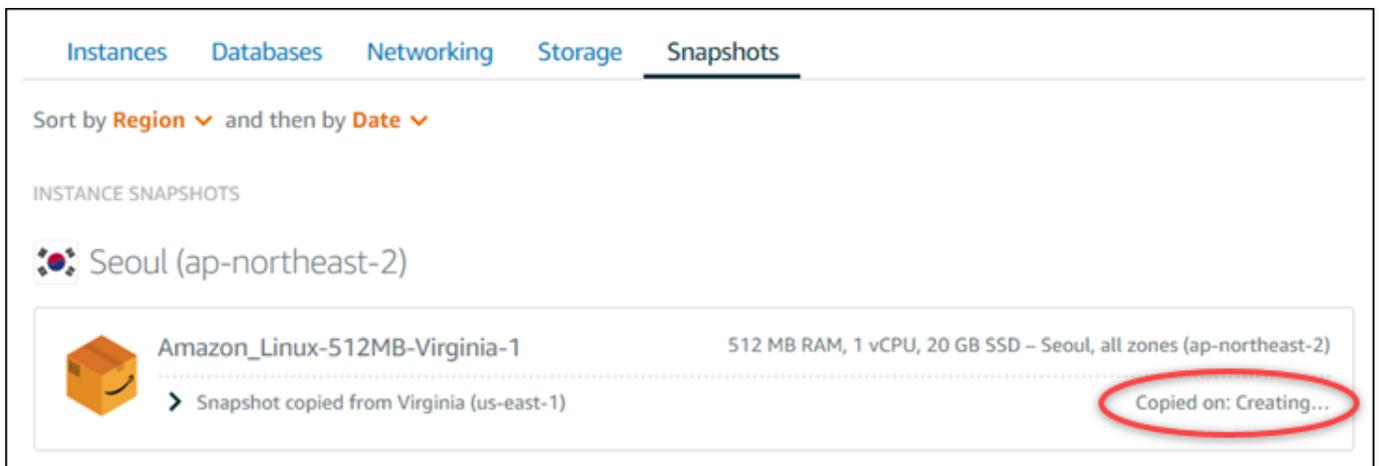
資源名稱：

- 每個 Lightsail 帳戶 AWS 區域 中的每個項目都必須是唯一的。
- 必須包含 2 至 255 個字元。
- 開頭和結尾必須是英數字元或數字。
- 可以包含英數字元、數字、句點、破折號和底線。

8. 選擇 Copy Snapshot (複製快照)。



您的快照複本應該很快就能使用。這取決於來源執行個體的大小和組態。您可以瀏覽至 Lightsail 首頁上的 [快照] 索引標籤來檢查快照副本的狀態，並尋找狀態為 [建立] 的快照，如下面的螢幕擷取畫面所示。狀態會在快照準備就緒時變更。



## 後續步驟

在 Lightsail 中將快照複製到其他區域後，您可以執行以下幾個其他步驟：

- 從可使用的已複製快照建立新的執行個體。如需詳細資訊，請參閱[透過快照建立執行個體](#)。
- 如果您不再需要來源快照，請予以刪除。否則，存放快照將會計費。

## 了解如何將快 Lightsail 匯出到 Amazon EC2

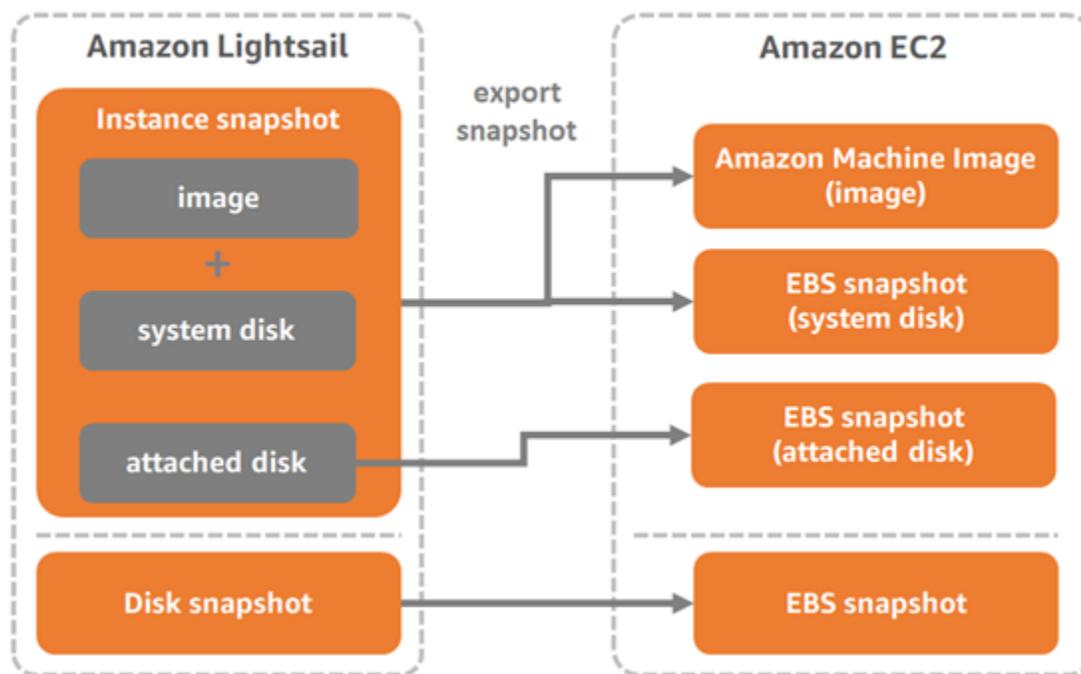
了解如何將 Lightsail 快照匯出到 Amazon EC2、從匯出的快照建立 EC2 資源、選擇相容 EC2 的執行個體類型、連接至 EC2 執行個體，以及保護從 Lightsail 快照建立的 EC2 執行個體的安全。Amazon Lightsail 執行個體和區塊儲存磁碟快照可以使用下列其中一種方法匯出至 Amazon 彈性運算雲端 (Amazon EC2)：

- Lightsail 主控台。如需詳細資訊，請參閱[將快照匯出到 Amazon EC2](#)。
- Lightsail API、AWS Command Line Interface (AWS CLI) 或 SDKs。如需詳細資訊，請參閱 Lightsail API 文件中的[ExportSnapshot 作業](#)，或文件中的[匯出快照命令](#)。AWS CLI

您可以匯出執行個體快照和區塊儲存磁碟快照。但是，cPanel & WHM (CentOS 7) 執行個體的快照不能匯出到 Amazon EC2。快照會 AWS 區域 從 Lightsail 匯出到相同的快照到 Amazon EC2。若要將快照匯出至不同的區域，請先將快照複製到 Lightsail 中的其他區域，然後執行匯出作業。如需詳細資訊，請參閱[將快照從一個快照複製 AWS 區域 到另一個](#)。

匯出 Lightsail 執行個體快照會導致 Amazon 機器映像 (AMI) 和 Amazon 彈性區塊存放區 (Amazon EBS) 快照在 Amazon EC2 中建立。這是因為 Lightsail 執行個體由映像檔和系統磁碟組成，但兩者都會在 Lightsail 主控台中群組為單一執行個體實體，以提高管理效率。如果來源 Lightsail 執行個體在建立快照時連接了一或多個區塊儲存磁碟，則會在 Amazon EC2 中為每個連接的磁碟建立其他 EBS 快照。匯出 Lightsail 區塊儲存磁碟快照會導致在 Amazon EC2 中建立單一 EBS 快照。Amazon 中所有匯出的資源都 EC2 有自己獨特的唯一識別碼，這些識別碼與其 Lightsail 對應的識別碼不同。

### Export Lightsail snapshots to Amazon EC2



#### Note

Lightsail 使用 AWS Identity and Access Management (IAM) 服務連結角色 (SLR) 將快照匯出至 Amazon。EC2 如需相關資訊 SLRs，請參閱[服務連結角色](#)。

匯出程序需要一些時間。這取決於來源執行個體或區塊儲存磁碟的大小和組態。使用 Lightsail 主控台 中的 [匯出] 區段來追蹤匯出狀態。如需詳細資訊，請參閱[追蹤快照匯出狀態](#)。

## 從匯出的 Lightsail 快照建立 Amazon EC2 資源

在匯出 Lightsail 快照並在 Amazon 中使用後 EC2 (以EBS快照形式AMI或兩者皆有)，您可以使用下列 其中一種方法從快照建立 Amazon EC2 資源：

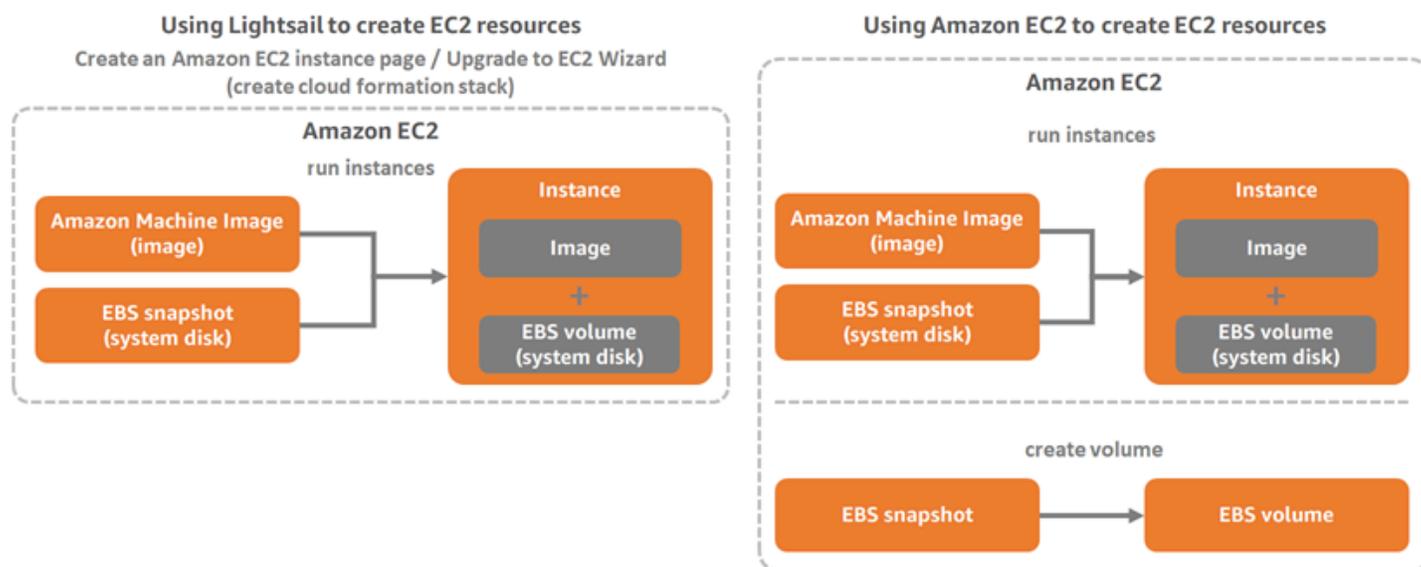
- Lightsail 主控台中的「建立 Amazon EC2 執行個體」頁面，也稱為「升級至 Amazon EC2 精靈」。如需詳細資訊，請參閱[從匯出的快照建立 Amazon EC2 執行個體](#)。
- Lightsail API AWS CLI、或SDKs。如需詳細資訊，請參閱 Lightsail API 文件中的[CreateCloudFormationStack 作業](#)，或文 AWS CLI 件中的[create-cloud-formation-stack 命令](#)。

### Note

Lightsail 可用於從匯出的EC2執行個體快照建立 Amazon 執行個體，但無法用於從匯出的 EBS區塊儲存磁碟快照建立磁碟區。為此，您必須使用 Amazon EC2 控制台API，或 AWS CLI。如需詳細資訊，請參閱[從匯出的磁碟快照建立 Amazon 磁碟EBS區](#)。

- Amazon EC2 控制台 EC2API，Amazon AWS CLI，或SDKs。[如需詳細資訊，請參閱 Amazon EC2 文件中的使用啟動執行個體精靈啟動執行個體或從快照還原 Amazon EBS 磁碟區](#)。

從匯出的EC2執行個體快照 (AMI和快EBS照) 建立 Amazon 執行個體會導致單一EC2執行個體啟 動。匯出 Lightsail 實體EBS快照所產生的快照AMI和快照會自動連結在一起，形成EC2實體。匯出的 Lightsail 區塊儲存磁碟快EBS照 (快照) 可用於在 Amazon EC2 中建立EBS磁碟區。



**Note**

Lightsail 使用 CloudFormation 堆疊在 EC2 中建立執行個體及其相關資源。如需詳細資訊，請參閱 [Lightsail 的 AWS CloudFormation 堆疊](#)。

從匯出的快照建立 Amazon EC2 資源的程序可能需要一段時間。這取決於來源執行個體的大小和組態。使用 Lightsail 主控台中的 [匯出] 區段來追蹤匯出狀態。如需詳細資訊，請參閱 [追蹤快照匯出狀態](#)。

## 選擇 Amazon 執行個體 EC2 類型

Amazon EC2 提供的執行個體選項比 Lightsail 提供的範圍更廣泛。在 Amazon 中 EC2，您可以選擇針對運算 (C5)、記憶體 (R5) 或兩者的平衡 (T3 和 M5) 進行優化的執行個體類型。Lightsail 在「建立 Amazon EC2 執行個體」頁面中提供了這些選項；但是，如果您使用 Amazon 從匯出的快照建立新執行個體，則可 EC2 以使用更多執行個體類型選項。如需 EC2 執行個體類型的詳細資訊，請參閱 Amazon EC2 文件中的 [執行個體類型](#)。

在從匯出的快照建立 EC2 執行個體之前，請務必瞭解 Lightsail 和 Amazon EC2 之間的執行個體價格差異。如需執行個體定價的詳細資訊，請參閱 [Lightsail 定價](#) 和 [Amazon EC2 定價](#) 頁面。

### Lightsail 和 Amazon EC2 執行個體類型相容

某些 Lightsail 執行個體與目前一代的 EC2 執行個體類型 (T3、M5、C5 或 R5) 不相容，因為這些執行個體並未啟用增強型聯網功能。如果來源 Lightsail 實體不相容，您必須在從匯出的快照建立執行個體 EC2 時，選擇上一代執行個體類型 (T2、M4、C4 或 R4)。使用 Lightsail 主控台中的「建立 Amazon EC2 執行個體」頁面建立 EC2 執行個體時，會顯示這些選項。

若要在來源 Lightsail EC2 執行個體不相容時使用最新一代的執行個體類型，您需要使用上一代 EC2 執行個體類型 (T2、M4、C4 或 R4) 建立新執行個體，更新網路驅動程式，然後將執行個體升級為所需的目前世代執行個體類型。如需詳細資訊，請參閱 [Amazon EC2 執行個體的增強型聯網](#)。

## Connect 到 Amazon EC2 實例

您可以連接到 Amazon EC2 執行個體，類似於連接 Lightsail 執行個體的方式。這意味著使 SSH 用 Linux 和 Unix 實例以及 RDP Windows 服務器實例。不過，EC2 視您使用的瀏覽器版本而定，在 Lightsail 主控台中可能無法使用您在 Lightsail Amazon 控台中使用的瀏覽器型 SSH/用戶 RDP 端，因此您可能需要設定自己的 SSH/用戶 RDP 端才能連線到執行個體 EC2。如需詳細資訊，請參閱下列指南：

- [Connect 到從快照建立的 Amazon EC2 Linux 或 Unix 執行個體](#)
- [Connect 到從快照建立的 Amazon EC2 視窗伺服器執行個體](#)

## 保護 Amazon 執行個EC2體

從匯出的 Lightsail 快照建立EC2執行個體後，您可能需要執行一些動作來改善新執行個體的安全性。動作會根據EC2執行個體的作業系統而有所不同。

### 保護 Amazon 中的 Linux 和 Unix 實例 EC2

如果您使用匯出的快照 EC2 (EC2主控台、用 AWS CLI 於或用於EC2) 在 Amazon EC2 中建立 Linux 或 SDKs Unix 執行個體EC2，則新EC2執行個體可能包含 Lightsail 服務的剩餘SSH金鑰。EC2 API我們建議您移除這些金鑰來為新執行個體增強安全性。

如需詳細資訊，請參閱[保護從 Lightsail 快照建立的 Amazon EC2 Linux 或 Unix 執行個體的安全](#)。

### 保護 Amazon 中的 Windows 伺服器執行 EC2

EC2從匯出的快照在 Amazon 中建立 Windows Server 執行個體後，您 AWS 帳戶中擁有 Lightsail 存取權的任何使用者EC2都可以先擷取指派給來源執行個體的預設管理員密碼，也是新EC2執行個體的密碼。為了提高安全性，建議您變更 Amazon EC2 執行個體的預設管理員密碼 (如果尚未變更)。

如需詳細資訊，請參閱[保護從 Lightsail 快照建立的 Amazon EC2 視窗伺服器執行個體的安全](#)。

## 將快 Lightsail 出到 Amazon EC2

您可以將 Amazon Lightsail 執行個體和區塊儲存磁碟快照匯出到 Amazon 彈性運算雲端 (AmazonEC2)。匯出 Lightsail 執行個體快照會導致 Amazon 機器映像 (AMI) 和 Amazon 彈性區塊存放區 (AmazonEBS) 快照在 Amazon EC2 中建立。這是因為 Lightsail 執行個體由映像檔和系統磁碟組成，但兩者都會在 Lightsail 主控台中群組為單一執行個體實體，以提高管理效率。如果來源 Lightsail 執行個體在建立快照時連接了一或多個區塊儲存磁碟，則會在 Amazon EC2 中為每個連接磁碟建立其他EBS快照。

匯出 Lightsail 區塊儲存磁碟快照會導致在 Amazon EC2 中建立單一EBS快照。Amazon 中所有匯出的資源都EC2有自己獨特的唯一識別碼，這些識別碼與其 Lightsail 對應的識別碼不同。

本指南說明如何匯出 Lightsail 快照、追蹤匯出狀態，以及如何在 Amazon 提供匯出快照後的後續步驟 EC2 (以EBS快照或兩者形式)。AMI

### ⚠ Important

建議您先熟悉 Lightsail 匯出程序，然後再完成本指南中的步驟。如需詳細資訊，請參閱[將快照匯出到 Amazon EC2](#)。

## 內容

- [匯出 Lightsail 快照所需的服務連結角色和所需的IAM權限](#)
- [先決條件](#)
- [將快照導 Lightsail 到 Amazon EC2](#)
- [追蹤匯出的狀態](#)

## 匯出 Lightsail 快照所需的服務連結角色和所需的IAM權限

Lightsail 使用 AWS Identity and Access Management (IAM) 服務連結角色 (SLR) 將快照匯出至 Amazon。EC2 如需相關資訊 SLRs，請參閱[服務連結角色](#)。

視將執行快照匯出的使用者 IAM 而定，可能需要在中設定下列其他權限：

- 如果 [Amazon 帳戶根使用者](#) 會執行匯出，則請繼續前往本指南的[先決條件](#)一節。帳戶根使用者已具備執行快照匯出所需的許可。
- 如果 IAM 使用者將執行匯出，則 AWS 帳戶管理員必須將下列策略新增至使用者。如需如何變更使用者權限的詳細資訊，請參閱 IAM 文件中的[變更 IAM 使用者權限](#)。

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

```
"Resource": "arn:aws:iam::*:role/aws-service-role/
lightsail.amazonaws.com/AWSServiceRoleForLightsail*"
  }
]
}
```

## 必要條件

建立您要匯出至 Amazon EC2 的 Lightsail 執行個體或區塊儲存磁碟的快照。如需詳細資訊，請參閱下列其中一項指南：

- [建立 Linux 或 Unix 執行個體快照](#)
- [建立 Windows Server 執行個體快照](#)
- [建立區塊儲存磁碟快照](#)

## 將快照導 Lightsail 到 Amazon EC2

將快照匯出到 Amazon 最有效的方法 EC2 是使用 Lightsail 主控台。您也可以使用 Lightsail API、AWS Command Line Interface (AWS CLI) 或 SDKs 匯出快照。如需詳細資訊，請參閱 Lightsail API 文件中的 [ExportSnapshot 作業](#)，或文件中的 [匯出快照命令](#)。AWS CLI

### Note

快照會 AWS 區域 從 Lightsail 匯出到相同的快照到 Amazon EC2。若要將快照匯出至不同的區域，請先將快照複製到 Lightsail 中的其他區域，然後執行匯出作業。如需詳細資訊，請參閱 [將快照從一個快照複製 AWS 區域 到另一個](#)。

## 將快 Lightsail 匯出到 Amazon EC2

1. 登入主 [Lightsail 台](#)。
2. 在左側導覽窗格中選擇 [快照]。
3. 找出您想匯出的執行個體或區塊儲存磁碟，接著展開節點以檢視該資源可用的快照。
4. 選擇所需快照的「動作」功能表，然後選擇「匯出到 Amazon」EC2。

The screenshot shows the Amazon Lightsail console interface. It displays two instance snapshots:

- CentOS-512MB-Virginia-1**: 512 MB RAM, 1 vCPU, 20 GB SSD – Virginia, all zones (us-east-1). It has 1 instance snapshot. The last snapshot was taken on November 26, 2018, at 4:04 PM. A context menu is open over this snapshot, showing options: 'Create new instance', 'Copy to another Region', 'Export to Amazon EC2' (highlighted), and 'Delete snapshot'.
- Amazon\_Linux-512MB-Virginia-1**: 512 MB RAM, 1 vCPU, 20 GB SSD. It has 3 instance snapshots. The last snapshot was taken on November 26, 2018, at 4:04 PM.

### Note

cPanel & WHM (CentOS 7) 執行個體的快照不能匯出到 Amazon EC2。

5. 檢閱在提示中顯示的重要詳細資訊。
6. 如果您同意出口到 AmazonEC2，請選擇是，繼續開始該過程。

匯出程序需要一些時間。這取決於來源執行個體或區塊儲存磁碟的大小和組態。使用 Lightsail 主控台內的 [匯出] 區段來追蹤匯出狀態。如需詳細資訊，請參閱[追蹤快照匯出狀態](#)。

## 追蹤匯出的狀態

在 Lightsail 主控台的「匯出」區段中追蹤匯出狀態。您可以從 Lightsail 主控台所有頁面上的左側導覽窗格存取此功能。如需詳細資訊，請參閱[追蹤快照匯出狀態](#)。

匯出中會顯示下列資訊：

- 快照名稱 — 來源快照的 Lightsail 稱。
- 「狀態」 — 導出的狀態。此值可以為 In progress、Successful 或 Failed。
- 匯出已開始 — 快照匯出開始的日期和時間。
- 來源詳細資料 — 來源 Lightsail 執行個體的規格，例如記憶體、處理和儲存。
- 來源執行環境名稱 — 快照的來源執行環境名稱。
- 快照類型 — Lightsail 快照的類型。類型可以是執行個體快照或磁碟快照。
- 已建立快照 — 建立來源 Lightsail 快照的日期和時間。

下列資訊會顯示在已完成匯出的「工作歷程記錄」區段中：

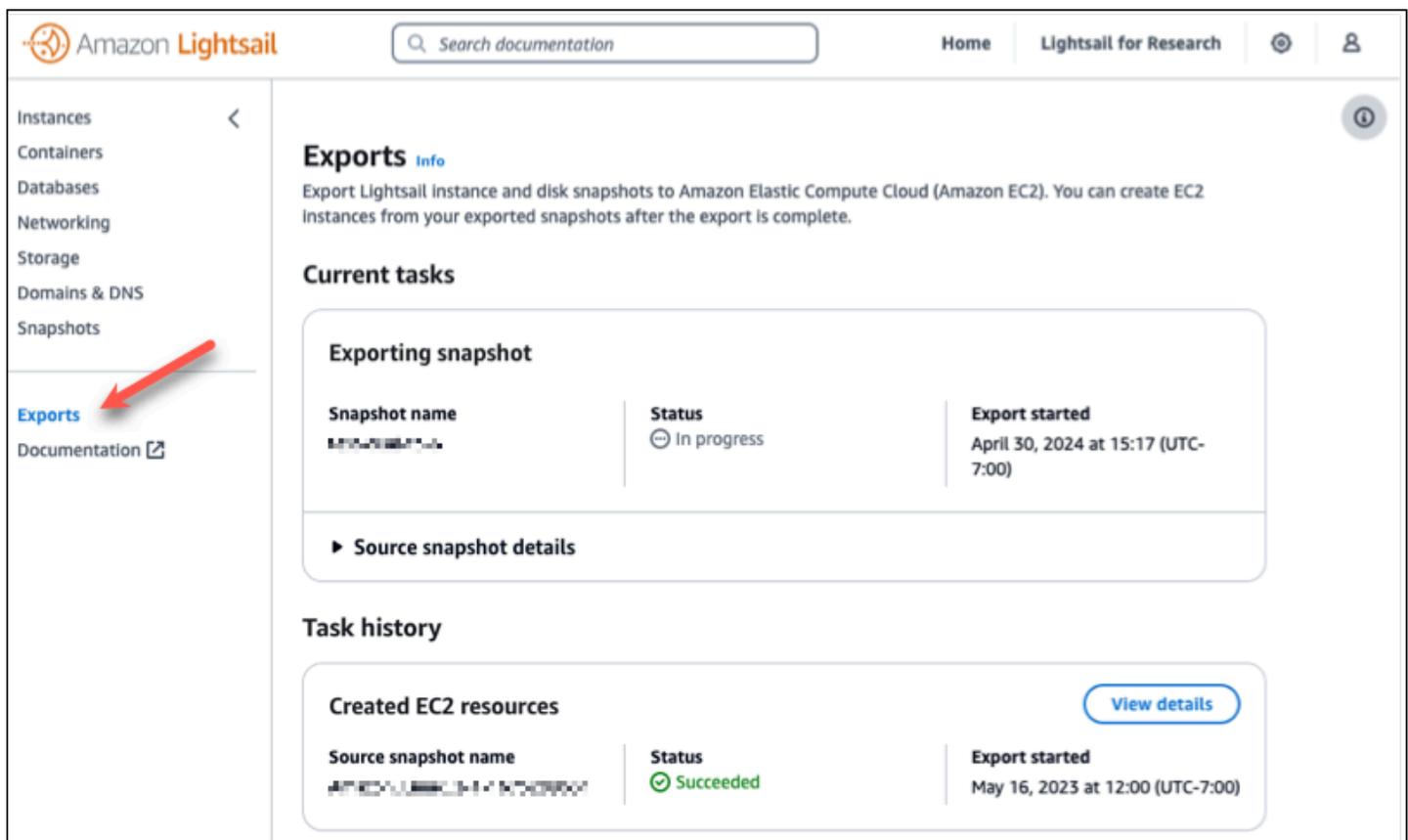
- 在中建立執行個體 EC2 — 選擇此選項可 EC2 使用 Lightsail 主控台在 Amazon 中建立新執行個體。如需詳細資訊，請參閱[從匯出的快照建立 Amazon EC2 執行個體](#)。
- 開啟 EC2 — 選擇此選項可使用 Amazon EC2 主控台從匯出的快照建立新 EC2 資源。如果您匯出了 Lightsail EBS 區塊儲存磁碟快照，則必須使 EC2 用 Amazon 從快照 (快 EBS 照) 建立磁碟區。[如需詳細資訊，請參閱 Amazon EC2 文件中的使用啟動執行個體精靈啟動執行個體或從快照還原 Amazon EBS 磁碟區](#)。

### Note

如果您不再需要，請刪除來源 Lightsail 快照。否則，存放快照將會計費。

## 追蹤快照匯出狀態

您可以在 Amazon Lightsail 主控台上的 [匯出] 區段追蹤將 Lightsail 快照匯出到 Amazon EC2 的狀態，或從匯出的執行個體快照建立新的 EC2 執行個體。匯出工作可能需要一段時間，視來源執行個體或區塊儲存磁碟的大小和組態而定。您可以從 Lightsail 主控台所有頁面的左側導覽窗格存取匯出。



The screenshot displays the Amazon Lightsail console interface. On the left, a navigation sidebar lists various services, with 'Exports' highlighted by a red arrow. The main content area is titled 'Exports' and includes a search bar, navigation links for 'Home' and 'Lightsail for Research', and a user profile icon. Below the title, there is a brief description of the export process. The 'Current tasks' section shows a task named 'Exporting snapshot' with a status of 'In progress' and an 'Export started' timestamp of 'April 30, 2024 at 15:17 (UTC-7:00)'. A 'Source snapshot details' link is provided below this task. The 'Task history' section shows a previous task 'Created EC2 resources' with a status of 'Succeeded' and an 'Export started' timestamp of 'May 16, 2023 at 12:00 (UTC-7:00)'. A 'View details' button is located next to this task.

如需將 Lightsail 快照匯出至 Amazon EC2，或從匯出的快照建立 EC2 執行個體的詳細資訊，請參閱下列指南：

- [將快照匯出至 Amazon EC2](#)
- [透過匯出的快照建立 Amazon EC2 執行個體](#)

## 從匯出的快照建立 Amazon EC2 執行個體

在匯出 Lightsail 執行個體快照並在 Amazon EC2 中使用後 (以 AMI 和 EBS 快照的形式)，您可以使用 Amazon Lightsail 主控台內的「建立 Amazon EC2 執行個體」頁面 (也稱為「升級至 Amazon EC2 精靈」)，從快照建立 Amazon EC2 執行個體。這會引導您執行 EC2 執行個體組態選項，例如選擇符合需求的 EC2 執行個體類型、設定安全群組連接埠、新增啟動指令碼等。Lightsail 主控台內的精靈可簡化建立新 EC2 執行個體及其相關資源的程序。

### Note

若要透過匯出的區塊儲存磁碟快照建立 Amazon Elastic Block Store (Amazon EBS) 磁碟區，請參閱[透過匯出的磁碟快照建立 Amazon EBS 磁碟區](#)。

您也可以使用 Lightsail API 或開發套件建立新的 EC2 執行個體。AWS CLI 如需詳細資訊，請參閱 Lightsail API 文件中的[CreateCloudFormationStack 作業](#)，或文 AWS CLI 文件中的[create-cloud-formation-stack 命令](#)。或者，如果您對 Amazon EC2 感到滿意，則可以使用 EC2 主控台、Amazon EC2 API 或開發套件。AWS CLI 如需詳細資訊，請參閱 Amazon EC2 文件中的[使用啟動執行個體精靈來啟動執行個體](#)或[從快照中還原 Amazon EBS 磁碟區](#)。

### Important

建議您先熟悉 Lightsail 匯出程序，然後再完成本指南中的步驟。如需詳細資訊，請參閱[將快照匯出至 Amazon EC2](#)。

## 內容

- [AWS CloudFormation Lightsail 的堆棧](#)
- [先決條件](#)
- [在 Lightsail 主控台中存取建立 Amazon EC2 執行個體頁面](#)

- [建立 Amazon EC2 執行個體](#)
- [追蹤新 Amazon EC2 執行個體的狀態](#)

## AWS CloudFormation Lightsail 的堆棧

Lightsail 會使用 AWS CloudFormation 堆疊來建立 EC2 執行個體及其相關資源。如需有關 Lightsail CloudFormation 堆疊的詳細資訊，請參閱 [Lightsail 的 AWS CloudFormation 堆疊](#)。

可能需要在 IAM 中設定以下額外許可，這取決於將使用建立 Amazon EC2 執行個體頁面來建立 EC2 執行個體的使用者身分：

- 如果 [Amazon 帳戶根使用者](#) 會建立 EC2 執行個體，則請繼續前往本指南的 [先決條件](#) 一節。根使用者已具備使用 Lightsail 建立 EC2 執行個體所需的權限。
- 如果 IAM 使用者將建立 EC2 執行個體，則 AWS 帳戶管理員必須向使用者新增下列許可。如需有關如何變更使用者許可的詳細資訊，請參閱 IAM 文件中的 [變更 IAM 使用者的許可](#)。
- 使用者需要下列許可才能使用 Lightsail 建立 Amazon EC2 執行個體：

### Note

這些權限允許建立 CloudFormation 堆疊。然而，如果建立失敗，轉返程序可能會需要更多許可。缺少許可或許會導致剩餘的資源無法在 Amazon EC2 中轉返。如果發生這種情況，您可以前往 AWS CloudFormation 主控台並手動刪除 EC2 資源。如需詳細資訊，請參閱 [適用於 Lightsail 的 AWS CloudFormation 堆疊](#)

- ec2 : DescribeAvailabilityZones
- ec2 : DescribeSubnets
- ec2 : DescribeRouteTables
- ec2 : DescribeInternetGateways
- ec2 : DescribeVpcs
- 雲形 : CreateStack
- 雲形 : ValidateTemplate
- IAM : CreateServiceLinkedRole
- IAM : PutRolePolicy
- 如果使用者會在 EC2 執行個體的安全群組中設定連接埠，則必須有以下許可：

- ec2 : DescribeSecurityGroups
- ec2 : CreateSecurityGroup
- ec2 : AuthorizeSecurityGroupIngress
- 如果使用者要在 Amazon EC2 中建立 Windows Server 執行個體，則必須擁有以下許可：
  - ec2 : DescribeKeyPairs
  - ec2 : ImportKeyPair
- 如果使用者是第一次建立 Amazon EC2 執行個體，或虛擬私有雲端 (VPC) 無法設定完全時，則必須擁有以下許可：
  - ec2 : AssociateRouteTable
  - ec2 : AttachInternetGateway
  - ec2 : CreateInternetGateway
  - ec2 : CreateRoute
  - ec2 : CreateRouteTable
  - ec2 : CreateSubnet
  - ec2 : CreateVpc
  - ec2 : ModifySubnetAttribute
  - ec2 : ModifyVpcAttribute

## 必要條件

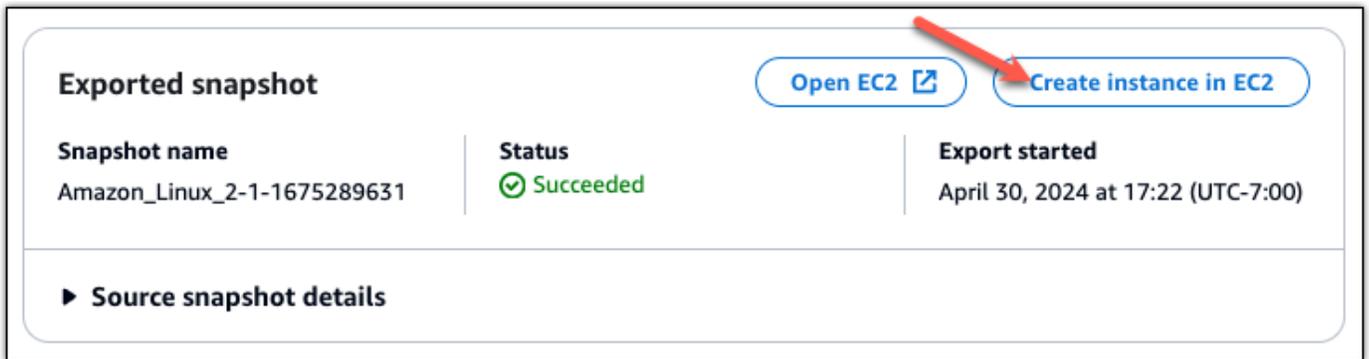
將 Lightsail 執行個體快照匯出至 Amazon EC2。如需詳細資訊，請參閱[將快照匯出至 Amazon EC2](#)。

## 在 Lightsail 主控台中存取建立 Amazon EC2 執行個體頁面

只有在執行個體快照成功匯出至 EC2 之後，才能從任務監視器存取 Lightsail 主控台中的「建立 Amazon EC2 執行個體」頁面。

在 Lightsail 主控台中存取建立 Amazon EC2 執行個體頁面

1. 登入主 [Lightsail](#) 台。
2. 從頂部導覽窗格選擇 Task monitor (任務監控) 圖示。
3. 找到任務歷史記錄區段中已完成的執行個體快照匯出，然後選擇建立新的 Amazon EC2 執行個體。



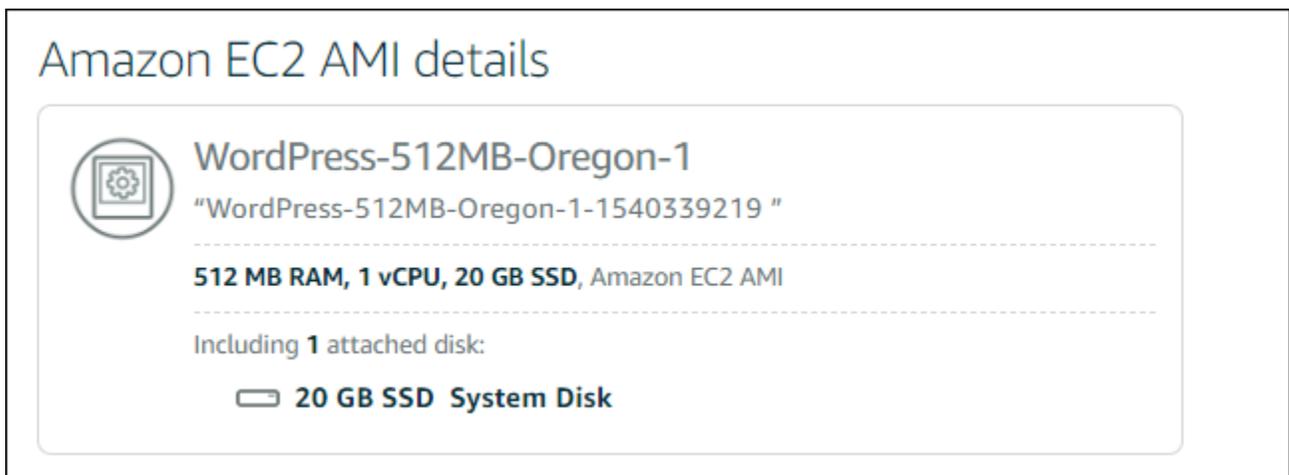
系統會顯示建立 Amazon EC2 執行個體頁面。繼續本指南的下列[建立 Amazon EC2 執行個體](#)一節，了解如何使用此頁面設定和建立 EC2 執行個體。

## 建立 Amazon EC2 執行個體

使用建立 Amazon EC2 執行個體頁面來建立 EC2 執行個體。若要從匯出的 Lightsail 快照建立多個 EC2 執行個體，請多次重複下列步驟，但請等到建立每個執行個體後再建立下一個執行個體。

### 建立 Amazon EC2 執行個體

1. 在頁面的 Amazon EC2 AMI 詳細資料區段中，確認顯示的 Amazon 機器映像 (AMI) 詳細資料符合來源 Lightsail 執行個體的規格。



2. 在頁面的 Resource location (資源位置) 部分，視需要變更執行個體的可用區域。Amazon EC2 資源的建立方式與來源快 Lightsail 同 AWS 區域。

**Note**

並非所有可用區域皆適用於所有使用者。選擇無法使用的可用區域會在建立 EC2 執行個體時導致錯誤。

## Resource location



You are creating this EC2 instance in **Oregon, Zone A (us-west-2a)**

[Change zone](#)



**Amazon EC2 uses a different zone letter mapping than Lightsail.**  
Your preferred zone for Oregon (us-west-2) may not be available.

3. 在頁面的 Compute resource (運算資源) 部分，選擇以下其中一個選項：

## Compute resource

[Find closest match](#)[Help me choose](#)[Select manually](#)

The closest match to your **512 MB RAM, 1 vCPU, 20 GB SSD** Lightsail instance is:



General Purpose EC2 Instance

**"WordPress-512MB-Oregon-1"**

2 vCPUs, 512 MB RAM, network up to 5 Gbps, IPv6 support, EBS optimized.

- 尋找最接近的相符項目，以自動選取與來源 Lightsail 執行個體規格最接近的 Amazon EC2 執行個體類型。
- 協助我選擇以回答關於新 Amazon EC2 執行個體規格的快速問卷。您可以選取運算最佳化、記憶體最佳化或兩者平衡的執行個體類型。
- 手動選取以透過建立 Amazon EC2 執行個體頁面來檢視可用的執行個體類型清單。

**Note**

某些 Lightsail 執行個體與目前一代 EC2 執行個體類型 (T3、M5、C5 或 R5) 不相容，因為這些執行個體並未啟用增強型聯網功能。如果來源 Lightsail 執行個體不相容，則從匯出的快照建立 EC2 執行個體時，您將需要選擇上一代執行個體類型 (T2、M4、C4 或 R4)。這些執行個體類型選項會顯示在 Lightsail 主控台的 [建立 Amazon EC2 執行個體] 頁面上。

若要在來源 Lightsail 執行個體不相容時使用最新一代 EC2 執行個體類型，您需要使用上一代執行個體類型 (T2、M4、C4 或 R4) 建立新的 EC2 執行個體，更新聯網驅動程式，然後將執行個體升級為所需的目前一代執行個體類型。如需詳細資訊，請參閱[更新 Amazon EC2 執行個體以增強聯網](#)。

## 4. 在頁面的 Optional (選用) 部分：

## OPTIONAL

The firewall port configuration for your Amazon EC2 instance are configured in the instance's security group.

 Specify port configuration

You can add a shell script that will run on your instance the first time it launches.

 Add launch script

- a. 選擇指定連接埠組態以選取 Amazon EC2 執行個體的防火牆設定，然後選擇以下其中一個選項：

Security groups 

How would you like to configure the security group for your Amazon EC2 instance?

- Use the default firewall settings from the Lightsail image.
- Use the source Lightsail instance firewall settings.

The following open ports will be imported into the security group for your EC2 instance:

APPLICATION	PROTOCOL	PORT RANGE
SSH	TCP	22
HTTP	TCP	80
HTTPS	TCP	443

- i. 使用 Lightsail 映像檔中的預設防火牆設定，從新 EC2 執行個體上的來源 Lightsail 藍圖設定預設連接埠。如需 Lightsail 藍圖預設連接埠的詳細資訊，請參閱[防火牆和連接埠](#)。
    - ii. 使用來源 Lightsail 執行個體防火牆設定，在新 EC2 執行個體上設定來源 Lightsail 執行個體的連接埠。只有在來源 Lightsail 實體仍在執行中時，才能使用此選項。
  - b. 在頁面的 Launch script (啟動指令碼) 部分，如果您想要新增指令碼以在 EC2 執行個體啟動時設定之，請選擇 Add launch script (新增啟動指令碼)。
5. 在頁面的 [連線安全性] 區段中，決定您連線至來源 Lightsail 執行個體的方式。這會確保您獲得正確 SSH 金鑰以連接至新的 EC2 執行個體。您可以使用以下其中一個方法連接到來源 Lightsail 執行個體：
- a. 使用來源執行個體區域的預設 Lightsail key pair — 下載並使用該金鑰的唯一預設 Lightsail 金鑰以連線 AWS 區域 至 EC2 執行個體。

 Note

預設的 Lightsail key pair 一律會用於 Lightsail 中的 Windows 伺服器執行個體。

- b. 使用您自己的金鑰對 — 找出私密金鑰並用於連接至 EC2 執行個體。

 Note

Lightsail 不會儲存您的個人私密金鑰。因此，不提供私密金鑰下載的選項。如果您無法找出您的私密金鑰，您就無法連接至 EC2 執行個體。

6. 在頁面的 [儲存資源] 區段中，確認所建立的 EBS 磁碟區與來源 Lightsail 執行個體的系統磁碟和任何連結的區塊儲存磁碟相符。

## Storage resources

We will create **2** EBS volumes for you and link them to your instance



Storage volume  
**/dev/xvdf**  
**8 GB** General Purpose (GP2) Encrypted EBS Volume



System volume  
**/dev/xvda**  
**20 GB** General Purpose (GP2) Encrypted EBS Volume

7. 檢閱有關在 Lightsail 之外建立資源的重要詳細資料。
8. 如果您同意在 Amazon EC2 中建立執行個體，請選擇在 EC2 中建立資源。

Lightsail 會確認您的執行個體正在建立中，並顯示 AWS CloudFormation 堆疊的相關資訊。Lightsail 會使用 CloudFormation 堆疊來建立 EC2 執行個體及其相關資源。如需詳細資訊，請參閱 [Lightsail 的 AWS CloudFormation 堆疊](#)。

繼續本指南的 [追蹤新 Amazon EC2 執行個體的狀態](#) 一節，以追蹤新 EC2 執行個體的状态。

### Important

請等到新的 EC2 執行個體建立完畢，再從相同的匯出快照建立另一個 EC2 執行個體。

## 追蹤新 Amazon EC2 執行個體的状态

使用 Lightsail 主控台中的 [匯出] 區段來追蹤 EC2 執行個體的状态。如需詳細資訊，請參閱 [追蹤快照匯出状态](#)。

針對正在建立的 EC2 執行個體，會顯示下列資訊：

- 來源名稱 — 來源快照的 Lightsail 稱。
- 已開始 — 建立請求開始的日期和時間。

以下資訊會在已建立的 EC2 執行個體之任務監控中顯示：

- Amazon EC2 資源成功建立時會顯示 Created (已建立)。
- 如果建立 EC2 執行個體時發生問題，則會顯示 Failed (失敗)。

## 從匯出的 Lightsail 磁碟快照建立 Amazon 彈性區塊存放磁碟區

在匯出 Lightsail 區塊儲存磁碟快照並在 Amazon EC2 中使用 (做為 EBS 快照) 之後，您可以使用 Amazon EC2 主控台從快照建立 EBS 磁碟區。

### Note

若要從匯出的執行個體快照建立 [EC2 執行個體](#)，請參閱 Lightsail 中的 [從匯出的快照建立 Amazon EC2 執行個體](#)。

您也可以使用 Amazon EC2 API 或開發套件建立新的 EBS 磁碟區。AWS CLI 如需詳細資訊，請參閱 Amazon EC2 文件中的 [使用啟動執行個體精靈來啟動執行個體](#) 或 [從快照中還原 Amazon EBS 磁碟區](#)。

### Important

建議您先熟悉 Lightsail 匯出程序，然後再完成本指南中的步驟。如需詳細資訊，請參閱 [將快照匯出至 Amazon EC2](#)。

## 必要條件

將 Lightsail 區塊儲存磁碟快照匯出至 Amazon EC2。如需詳細資訊，請參閱 [將快照匯出至 Amazon EC2](#)。

## 從匯出的 Lightsail 區塊儲存磁碟快照建立 EBS 磁碟區

使用 Amazon EC2 主控台，從匯出的 Lightsail 區塊儲存磁碟快照建立新的 EBS 磁碟區。

**Note**

Amazon EC2 文件中也有這些步驟。欲進一步了解，請參閱 Amazon EC2 文件中的 [從快照還原 Amazon EBS 磁碟區](#)。

若要從匯出的 Lightsail 區塊儲存磁碟快照建立 EBS 磁碟區

1. 登入 [Amazon EC2 主控台](#)。
2. 從導覽列選取您快照所在的區域。
3. 在導覽窗格中，選擇 Elastic Block Store (Elastic Block Store)，然後選擇 Snapshots (快照)。
4. 找出並選取匯出的 Lightsail 區塊儲存磁碟快照。

匯出的磁碟快照可透過從 Amazon Lightsail 匯出的 EBS 快照說明來識別，如下列螢幕擷取畫面所示：

Snapshot ID	Size	Description
snap-0c8daaae6d815c3f7	20 GiB	Copied for DestinationPool and-01c7882040111760r from SourcePool and-0a1...
snap-06bbbf02cdbe92137	30 GiB	Copied for DestinationPool and-01a0a01110101010 from SourcePool and-0a1...
snap-044c549df2bf34f5e	8 GiB	A disk snapshot exported from Amazon Lightsail MyDiskSnapshot
snap-01fe78a3c611911ed	20 GiB	Copied for DestinationPool and-01c7882040111760r from SourcePool and-0a1...
snap-0c635b87c5675cb8d	8 GiB	Copied for DestinationPool and-01c7882040111760r from SourcePool and-0a1...
snap-0964d597917e3487d	30 GiB	Copied for DestinationPool and-01c7882040111760r from SourcePool and-0a1...
snap-054c5c705820b90e1	8 GiB	Copied for DestinationPool and-01c7882040111760r from SourcePool and-0a1...
snap-0a80ad5fd849fcd1b	20 GiB	Copied for DestinationPool and-01c7882040111760r from SourcePool and-0a1...
snap-0042eb3868771694d	20 GiB	Copied for DestinationPool and-01c7882040111760r from SourcePool and-0a1...
snap-014a072c2a77360bb	8 GiB	Copied for DestinationPool and-01c7882040111760r from SourcePool and-0a1...
snap-0c0f05832bd08a09b	8 GiB	A disk snapshot exported from Amazon Lightsail MyDiskSnapshot
snap-0763258cc2b12f96a	20 GiB	Copied for DestinationPool and-01c7882040111760r from SourcePool and-0a1...

5. 選擇 Actions (動作)，然後選擇 Create Volume (建立磁碟區)。
6. 從 Volume Type (磁碟區類型) 下拉式功能表選擇磁碟區類型。如需詳細資訊，請參閱 Amazon EC2 文件中的 [Amazon EBS 磁碟區類型](#)。
7. 針對 Size (GiB) (大小 (GiB))，輸入磁碟區大小，或確認快照的預設大小是否足夠。
8. 若是佈建 IOPS SSD 磁碟區，請在 IOPS (IOPS) 輸入磁碟區應支援的最大每秒輸入/輸出操作次數 (IOPS)。

9. 針對 Availability Zone (可用區域)，選擇要建立磁碟區的可用區域。EBS 磁碟區只能連接到同一可用區域內的 EC2 執行個體。
10. (選用) 選擇 Create additional tags (建立其他標籤) 將標籤新增至磁碟區。針對每個標籤，提供標籤金鑰和標籤值。
11. 選擇 Create Volume (建立磁碟區)。建立磁碟區後，它會列於 Amazon EC2 主控台的 Elastic Block Store > 磁碟區部分中。

## Connect 到從快照建立的 Linux Amazon EC2 執行個體

從 Amazon Lightsail 快照在 Amazon 彈性運算雲端 (亞馬遜EC2) 中建立 Linux 或 Unix 執行個體之後，您可以透過SSH與來源 Lightsail 執行個體的連線方式類似連線到執行個體。若要驗證您的執行個體，請使用來源執行個體的預設 Lightsail key pair 組或您自己的 key pair。AWS 區域本指南說明如何在EC2使用 Pu 時連接到 Linux 或 Unix 實例TTY。

### Note

如需有關連線至 Windows 伺服器執行個體的詳細資訊，請參閱[連線至透過 Lightsail 快照建立的 Amazon EC2 Windows 伺服器執行個體](#)。

## 內容

- [取得執行個體的金鑰](#)
- [取得執行個體的公用DNS位址](#)
- [下載並安裝 Pu TTY](#)
- [使用 P 配置密鑰 uTTYgen](#)
- [將 Pu 設定TTY為連線至您的執行個體](#)
- [後續步驟](#)

## 取得執行個體的金鑰

取得連線至新 Amazon EC2 執行個體所需的正確金鑰。您需要的金鑰取決於您連接來源 Lightsail 實體的方式。您可以使用以下其中一個方法連接到來源 Lightsail 執行個體：

- 使用來源執行個體區域的預設 Lightsail key pair — 從 [Lightsail 帳戶](#) 頁面上的SSH金鑰索引標籤下載預設私密金鑰。如需有關預設 Lightsail 金鑰的詳細資訊，請參閱[金SSH鑰配對](#)。

**Note**

連線至EC2執行個體之後，建議您從執行個體移除預設的 Lightsail 金鑰，並以您自己的 key pair 取代。如需詳細資訊，請參閱[保護您在 Amazon 中透過 Lightsail 快照EC2建立的 Linux 或 Unix 執行個體安全](#)。

- 使用您自己的 key pair — 找到您的私密金鑰，並使用它連接到 Amazon EC2 執行個體。當您使用自己的金鑰組時，Lightsail 不會儲存您的私 key pair。如果您遺失了私密金鑰，就無法連線到 Amazon EC2 執行個體。

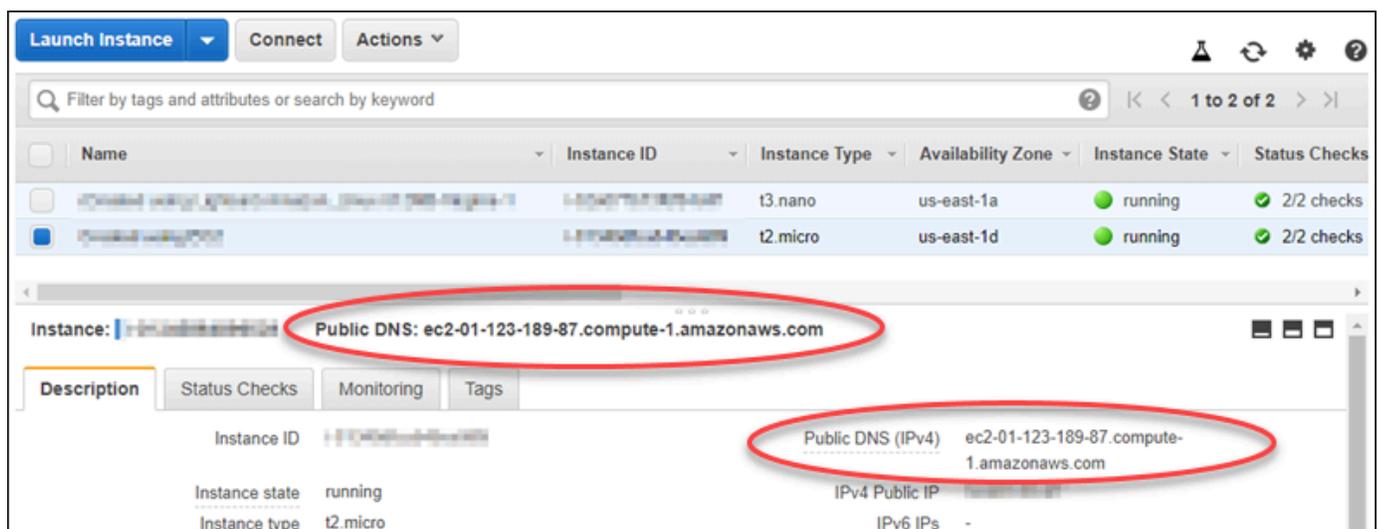
## 取得執行個體的公用DNS位址

取得 Amazon EC2 執行個體的公用DNS地址，以便在設定用SSH戶端 (例如 PuTTY) 以連接至執行個體時使用該地址。

### 取得執行個體的公用DNS位址

1. 登錄到 [Amazon 控EC2制台](#)。
2. 從左側導覽窗格中選擇 Instances (執行個體)。
3. 選擇您想要連接的執行中 Linux 或 Unix 執行個體。
4. 在下方窗格中，找出執行個體的公用位DNS址。

這是您將在設定用SSH戶端連線至執行個體時使用的位址。繼續閱讀本指南的「[下載並安裝 PuTTY](#)」一節，瞭解如何下載和安裝 PuTTY SSH 用戶端。



The screenshot shows the Amazon Management Console interface for an EC2 instance. At the top, there are buttons for 'Launch Instance', 'Connect', and 'Actions'. Below that is a search bar and a table of instances. The table has columns for Name, Instance ID, Instance Type, Availability Zone, Instance State, and Status Checks. Two instances are listed: one with type 't3.nano' and one with type 't2.micro'. The 't2.micro' instance is selected. Below the table, the details for the selected instance are shown. The 'Public DNS' field is circled in red and contains the address 'ec2-01-123-189-87.compute-1.amazonaws.com'. Below that, the 'Public DNS (IPv4)' field is also circled in red and contains the same address. Other fields like 'IPv4 Public IP' and 'IPv6 IPs' are also visible.

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks
...	...	t3.nano	us-east-1a	running	2/2 checks
...	...	t2.micro	us-east-1d	running	2/2 checks

Instance: ... Public DNS: ec2-01-123-189-87.compute-1.amazonaws.com

Field	Value
Public DNS (IPv4)	ec2-01-123-189-87.compute-1.amazonaws.com
IPv4 Public IP	...
IPv6 IPs	-

## 下載並安裝 PuTTY

PuTTY是一個免費的SSH客戶端視窗。有關 [PuTTY 的更多信息](#)，請參閱 [PuTTY：免費SSH和Telnet客戶端](#)。這個網站也說明在不允許加密之國家的限制。如果您已經擁有 PuTTY，可以跳至本指南的以下使用 P 設定金鑰一節。

[下載 PuTTY 安裝程序或可執行文件](#)。我們建議使用最新版本。不過，如需選擇哪個下載的相關資訊，請參閱 [PuTTY 文件](#)。

請繼續參閱本指南的 uTTYgen [〈使用 P 設定金鑰〉](#) 一節，以 P 設定金鑰 uTTYgen。

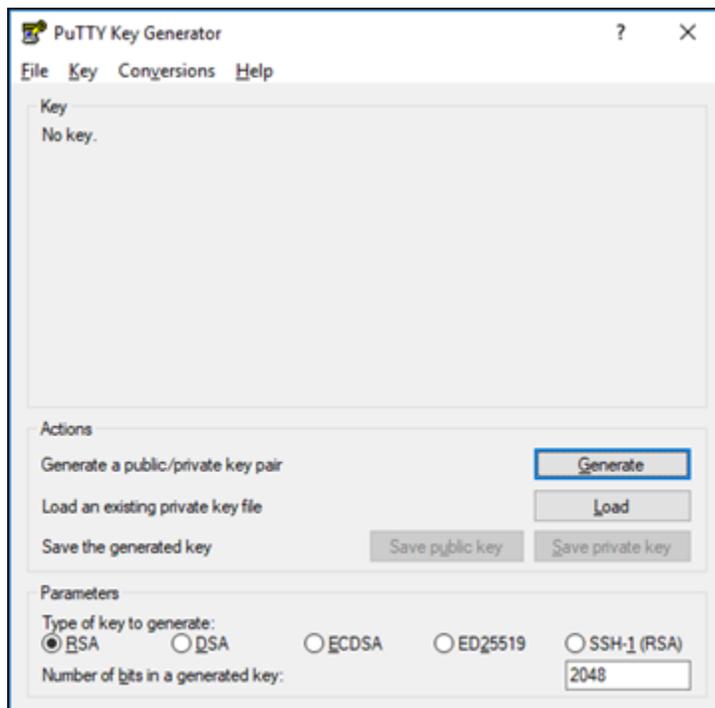
## 使用 P 配置密鑰 uTTYgen

PuTTYgen 生成對與 PuTTY 使用的公鑰和私鑰。需要執行此步驟才能使用金鑰檔案類型 (. PPK )，PuTTY 接受。

### 使用 P 設定金鑰 uTTYgen

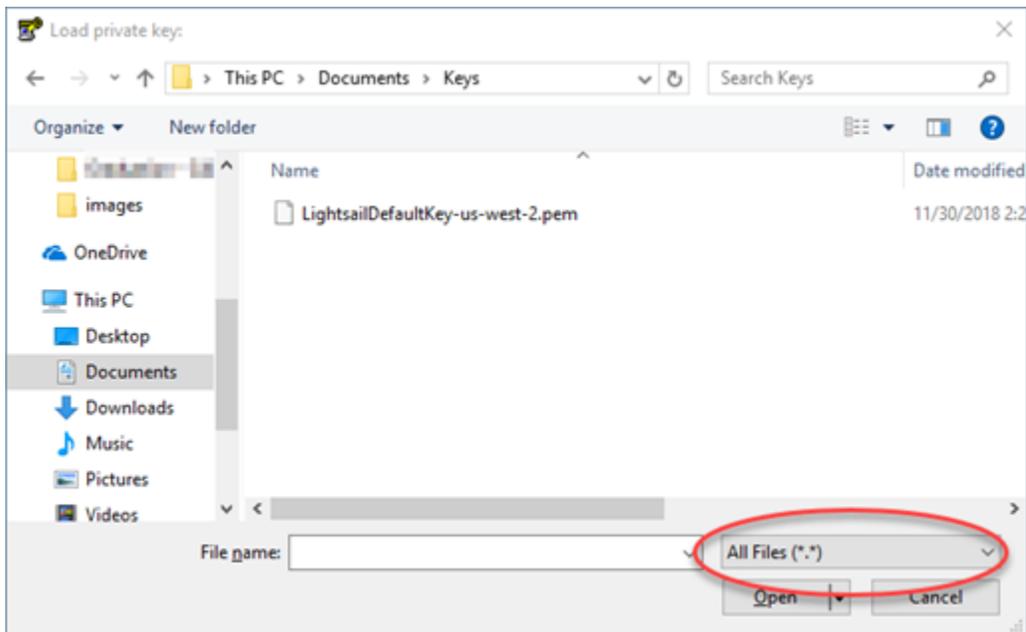
#### 1. 開始 PuTTYgen。

例如，選擇 Windows「開始」功能表，選擇「所有程式」，選擇「PuTTY」，然後選擇「P」uTTYgen。

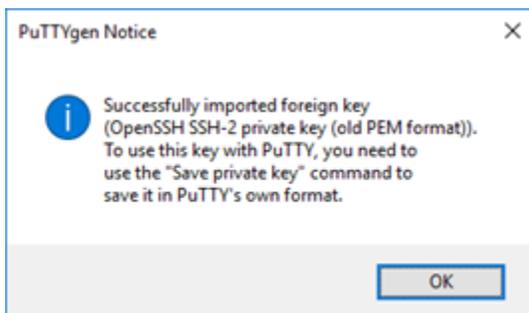


#### 2. 選擇載入。

依預設，PuTTYgen 顯示具有 .PPK 副檔名。若要尋找您的 .PEM 文件中，選擇顯示所有類型文件的選項。

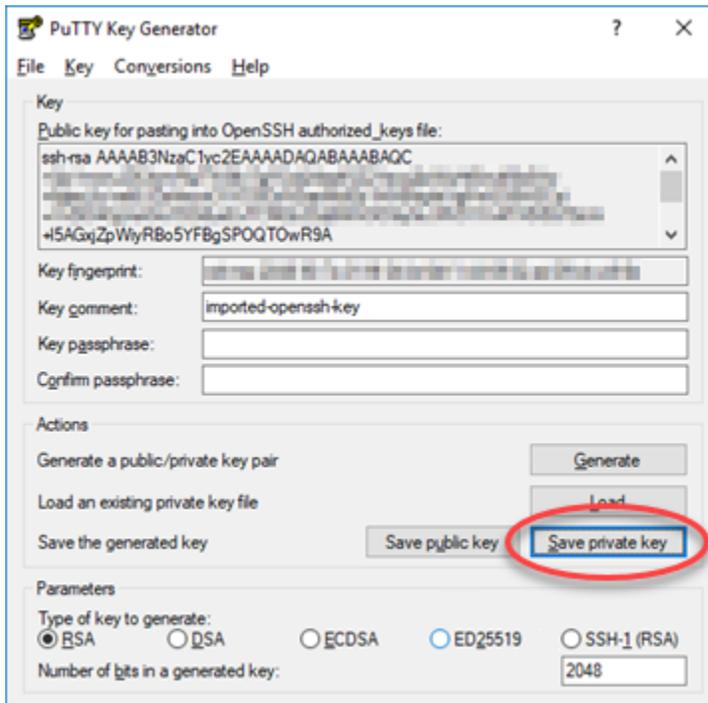


3. 選擇預設的 Lightsail 金鑰檔案 (.PEM) 您先前在本指南中下載的，然後選擇 [開啟]。
4. PuTTYgen 確認您已成功匯入金鑰之後，請選擇「確定」。



5. 選擇 Save private key (儲存私密金鑰)，然後確認您不想要使用密碼短語來進行儲存。

如果您建立密碼作為額外的安全性措施，則每次使用 Pu 連線至執行個體時，都必須輸入密碼。TTY



6. 指定儲存私密金鑰的名稱和位置，然後選擇 Save (儲存)。

PuTTYgen 將您的新密鑰文件另存為 .PPK 檔案類型。

7. 關閉 PuTTYgen。

繼續參閱本指南的 < [設定 PuTTY 以連線至執行個體](#) > 一節，以使用新的 .PPK 您生成用於配置 PuTTY 並連接到 Amazon 中的 Linux 或 Unix 實例的文件 EC2。

## 將 PuTTY 設定 TTY 為連線至您的執行個體

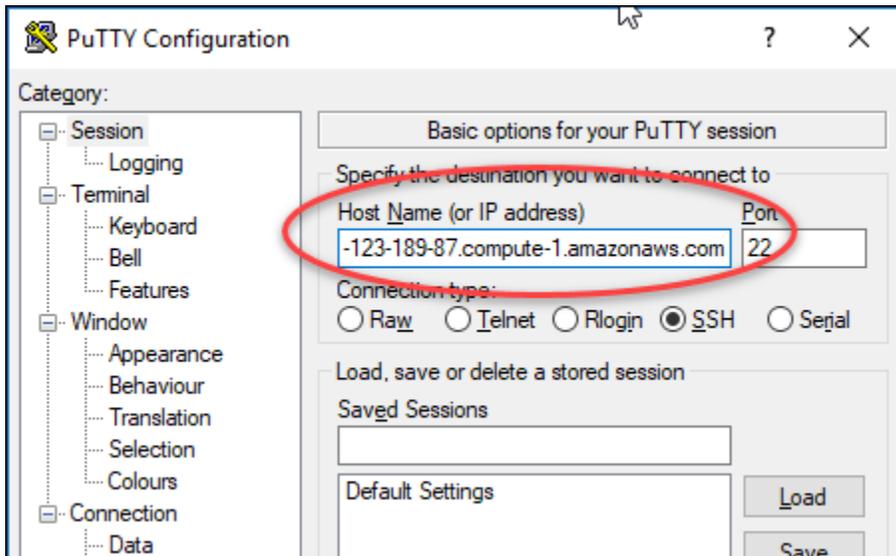
配置 PuTTY，現在您具有使用連接到 Linux 或 Unix 實例的所有要求 SSH。

若要將 PuTTY 設定 TTY 為連線到您的 Linux 或 Unix 執行個體

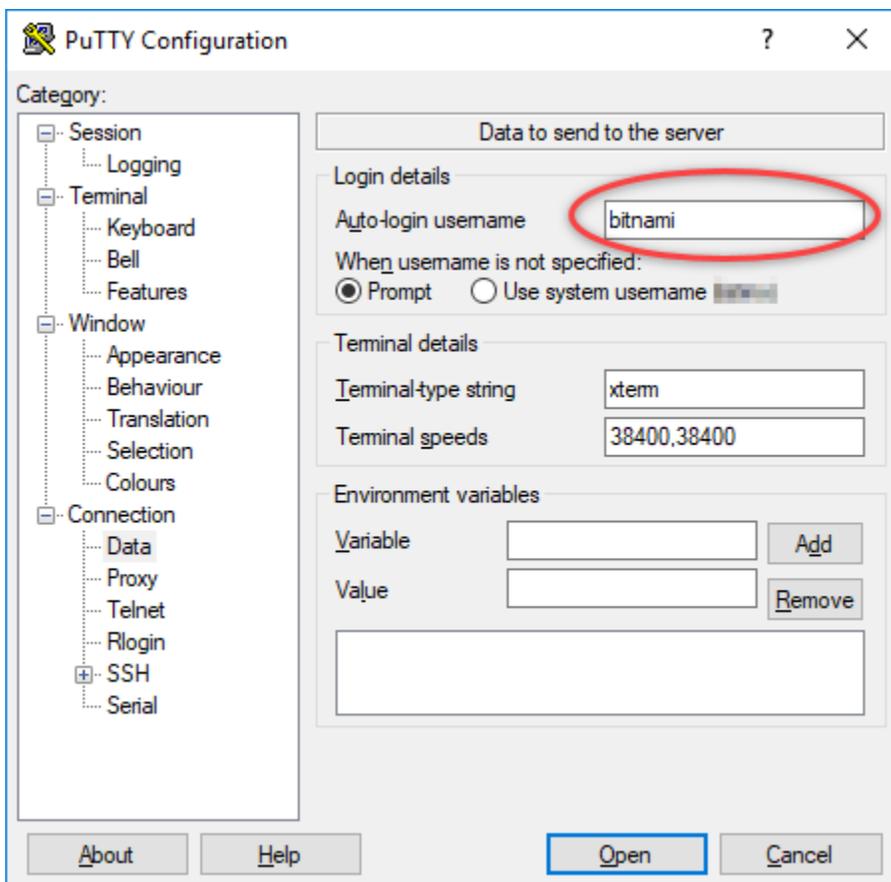
1. 打開 PuTTY。

例如，選擇 Windows [開始] 功能表，選擇 [所有程式]，選擇 [PuTTY]，然後選擇 [PuTTY]。

2. 在 [主機名稱] 文字方塊中，輸入您在本指南前面從 Amazon 主 EC2 控制台取得的執行個體公用 DNS 位址。

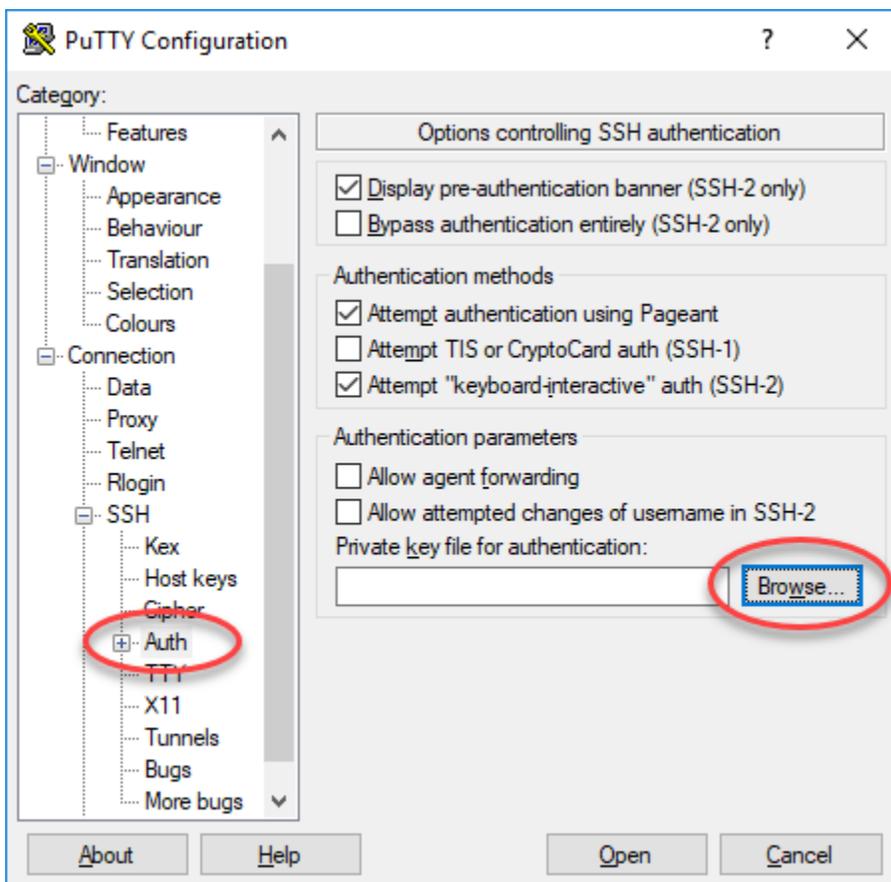


3. 在左側導覽窗格的 Connection (連線) 部分，選擇 Data (資料)。
4. 在 Auto-login username (自動登入使用者名稱) 文字方塊中，輸入在登入執行個體時使用的使用者名稱。



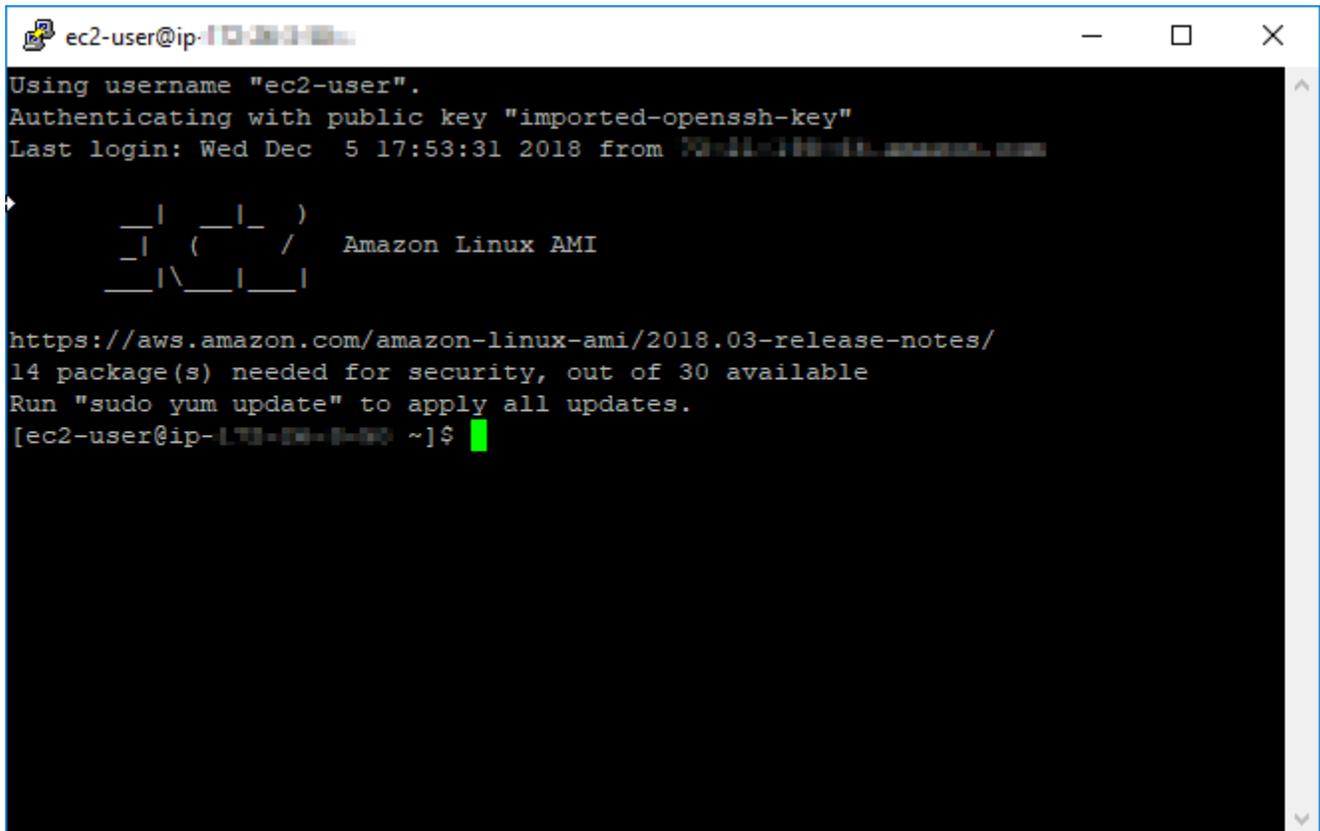
根據來源 Lightsail 執行個體的藍圖，輸入下列其中一個預設使用者名稱：

- AlmaLinux, Amazon Linux 2, Amazon Linux 2023, CentOS 流 9, 免費BSD和開放SUSE的執行個體 : `ec2-user`
  - Debian 執行個體 : `admin`
  - Ubuntu 執行個體 : `ubuntu`
  - Bitnami 執行個體 : `bitnami`
  - Plesk 執行個體 : `ubuntu`
  - cPanel WHM實例 (E) : `centos`
5. 在左側導覽窗格的 [連線] 區段下，展開 SSH，然後選擇 [驗證]。
  6. 選擇「瀏覽」以導覽至。PPK您在在本指南上一節中建立的檔案，然後選擇 [開啟]。



7. 選擇 Open (開啟) 連接到執行個體，然後選擇 Yes (是) 以在日後信任此連線。

如果您已成功連接到執行個體，您應該會看到類似以下的畫面：



```
ec2-user@ip-172-31-0-50:~$ ssh -i /home/ec2-user/.ssh/important-key.pem ec2-user@ip-172-31-0-50
Using username "ec2-user".
Authenticating with public key "imported-openssh-key"
Last login: Wed Dec  5 17:53:31 2018 from 73.11.174.100 [ip-172-31-0-50]
_ _ | _ _ | _ _ )
_ | ( _ | _ /   Amazon Linux AMI
_ | \ _ | _ | _ |

https://aws.amazon.com/amazon-linux-ami/2018.03-release-notes/
14 package(s) needed for security, out of 30 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-31-0-50 ~]$
```

## 後續步驟

如果您使用 Amazon 從導出的快照創建新的實例，則 Amazon EC2 中的新 Linux 或 Unix 實例 EC2 包含 Lightsail 服務的剩餘密鑰。建議您移除這些密鑰，以增強新 Amazon EC2 執行個體的安全性。如需詳細資訊，請參閱[保護您在 Amazon 中透過 Lightsail 快照 EC2 建立的 Linux 或 Unix 執行個體安全](#)。

## 從快照啟動的安全 Amazon EC2 執行個體

Amazon Lightsail 和亞馬遜彈性運算雲端 (Amazon EC2) 使用公開密鑰加密技術來加密和解密登入資訊。公有密鑰加密法使用公有密鑰將密碼等資料加密，再由收件人使用私有密鑰將資料解密。公有密鑰和私有密鑰稱為密鑰對。

當您將 Linux 或 Unix Lightsail 執行個體匯出至 EC2 時，新的 EC2 執行個體將包含來自 Lightsail 服務的剩餘密鑰。基於安全最佳實務，您應該從執行個體移除未使用的密鑰。

若要改善 EC2 中從 Lightsail 快照建立的 Linux 或 Unix 執行個體的安全性，建議您在建立執行個體之後執行下列動作：

- 如果您使用 Lightsail 預設金鑰連線至 Lightsail 中的來源實體，請移除並取代該按鍵。如果您使用自己的金鑰連線至執行個體，或在 Lightsail 主控台中為執行個體建立金鑰，則 Lightsail 預設金鑰不會出現在 Amazon EC2 執行個體中。
- 移除 Lightsail 系統金鑰，也稱為lightsail\_instance\_ca.pub金鑰。Linux 和 Unix 執行個體上的這個金鑰可讓 Lightsail 瀏覽器型安全殼層用戶端進行連線。使用 Lightsail 主控台中央的「建立 Amazon EC2 執行個體」頁面或 Lightsail API 建立 EC2 執行個體時，系統會自動移除lightsail\_instance\_ca.pub金鑰。

## 內容

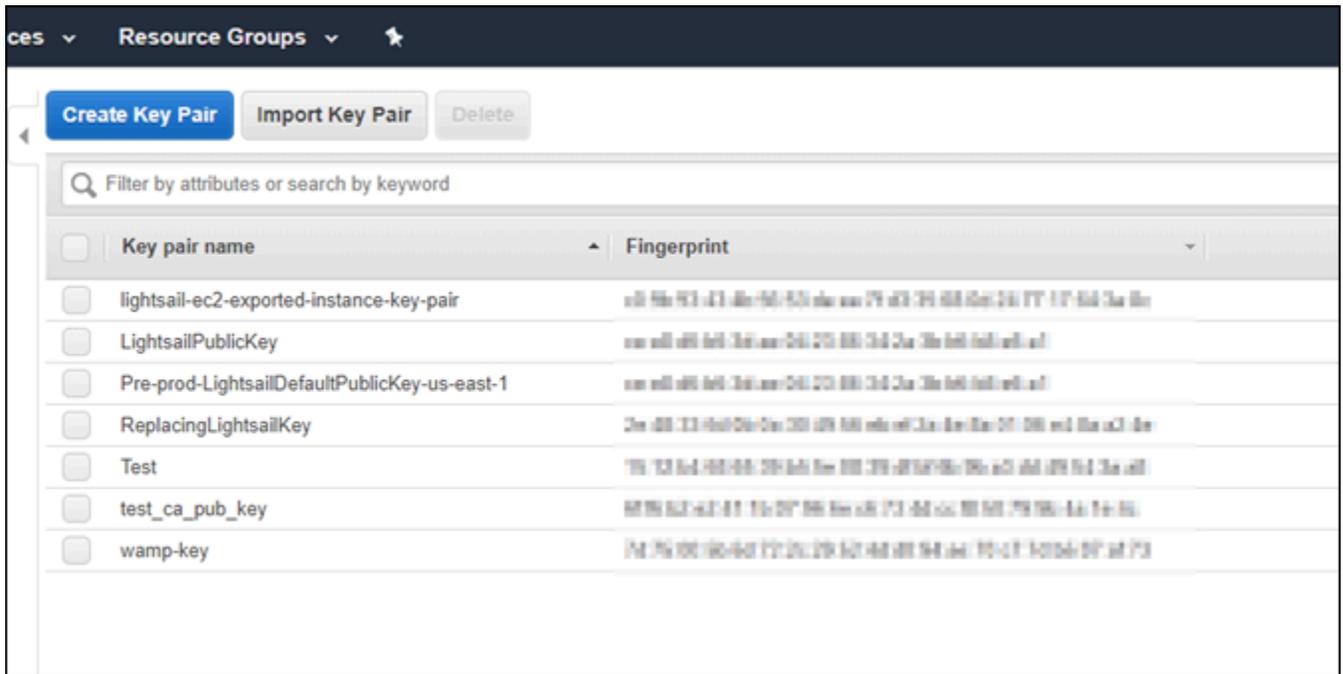
- [使用 Amazon EC2 建立私有金鑰](#)
- [使用 PuTTYgen 建立公開金鑰](#)
- [在 Amazon EC2 中連線至 Linux 或 Unix 執行個體](#)
- [新增公開金鑰至執行個體並測試連線](#)
- [移除 Lightsail 金鑰](#)
- [移除 Lightsail 系統鍵](#)

## 使用 Amazon EC2 建立私有金鑰

使用 Amazon EC2 主控台建立新的金鑰對，您可以用來取代 Lightsail 預設 key pair。

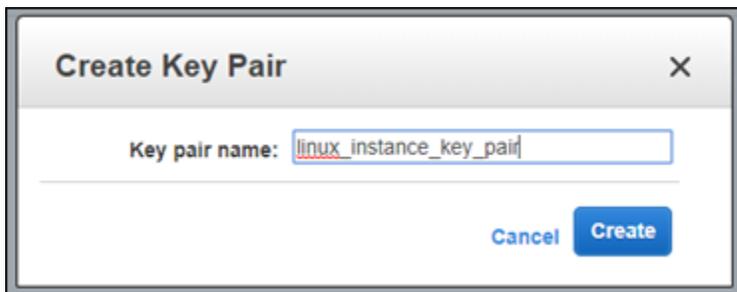
### 使用 Amazon EC2 建立私有金鑰

1. 登入 [Amazon EC2 主控台](#)。
2. 從左側導覽窗格選擇 Key Pairs (金鑰對)。
3. 選擇 Create key pair (建立金鑰對)。



- 將金鑰名稱輸入 Key pair name (金鑰對名稱) 文字方塊，接著選擇 Create (建立)。

新的私密金鑰會自動下載。記下私密金鑰儲存的位置。您會在本指南以下的使用 PuTTYgen 建立公開金鑰部分需要它來建立公開金鑰。



## 使用 PuTTYgen 建立公開金鑰

PuTTYgen 是一種工具，包含於 PuTTY。使用 PuTTYgen 產生公開金鑰文字，而您會在本指南稍後將其新增至執行個體。

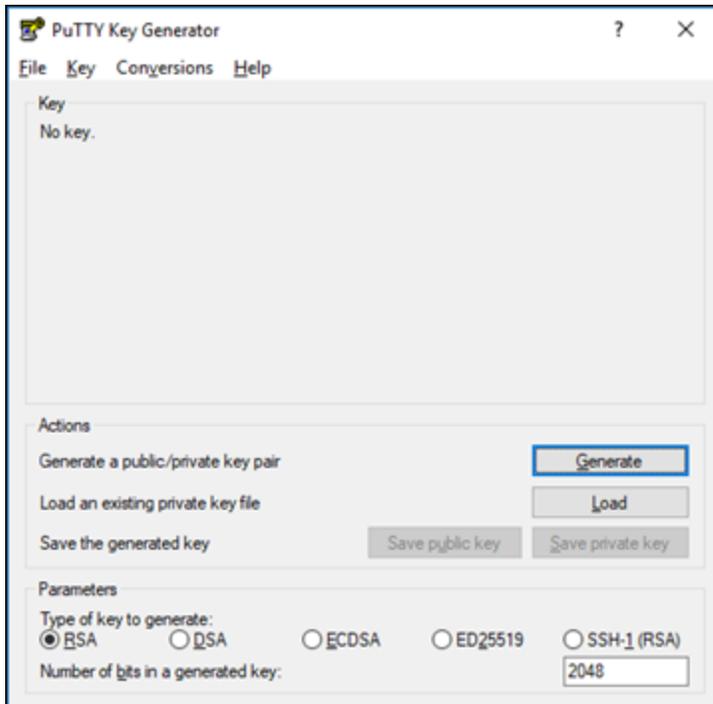
### Note

如需有關如何設定 PuTTY 以 Connect 到 Linux 或 Unix 執行個體的詳細資訊，請參閱[連接至透過 Lightsail 快照建立的 Amazon EC2 Linux 或 Unix 執行個體](#)。

## 若要使用 PuTTYgen 建立公開金鑰

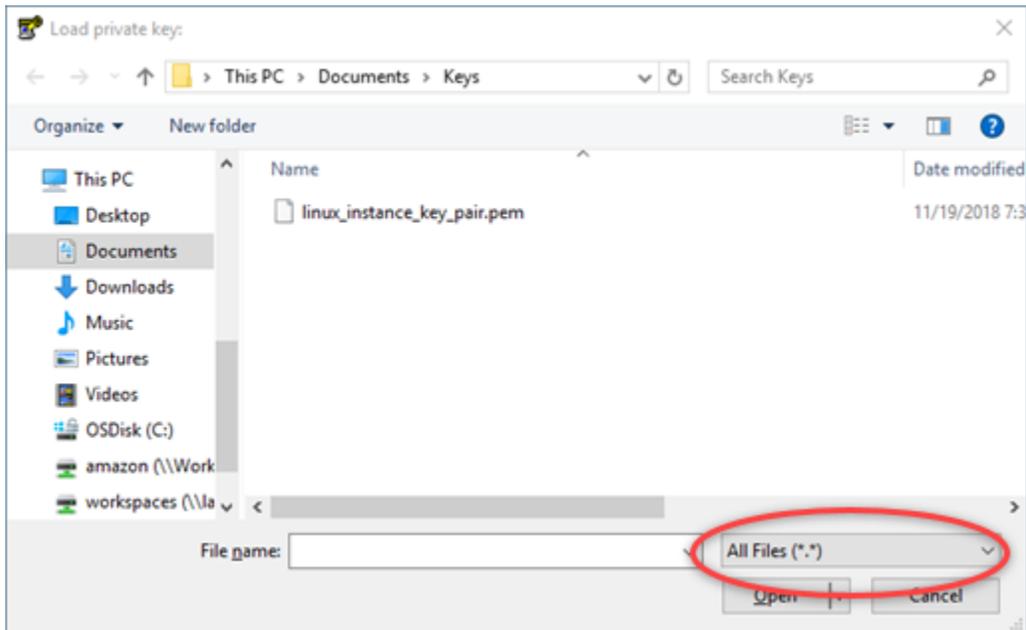
### 1. 啟動 PuTTYgen。

例如，依序選擇 Windows Start (Windows 開始) 功能表、All Programs (所有程式)、PuTTY (PuTTY) 和 PuTTYgen (PuTTYgen)。



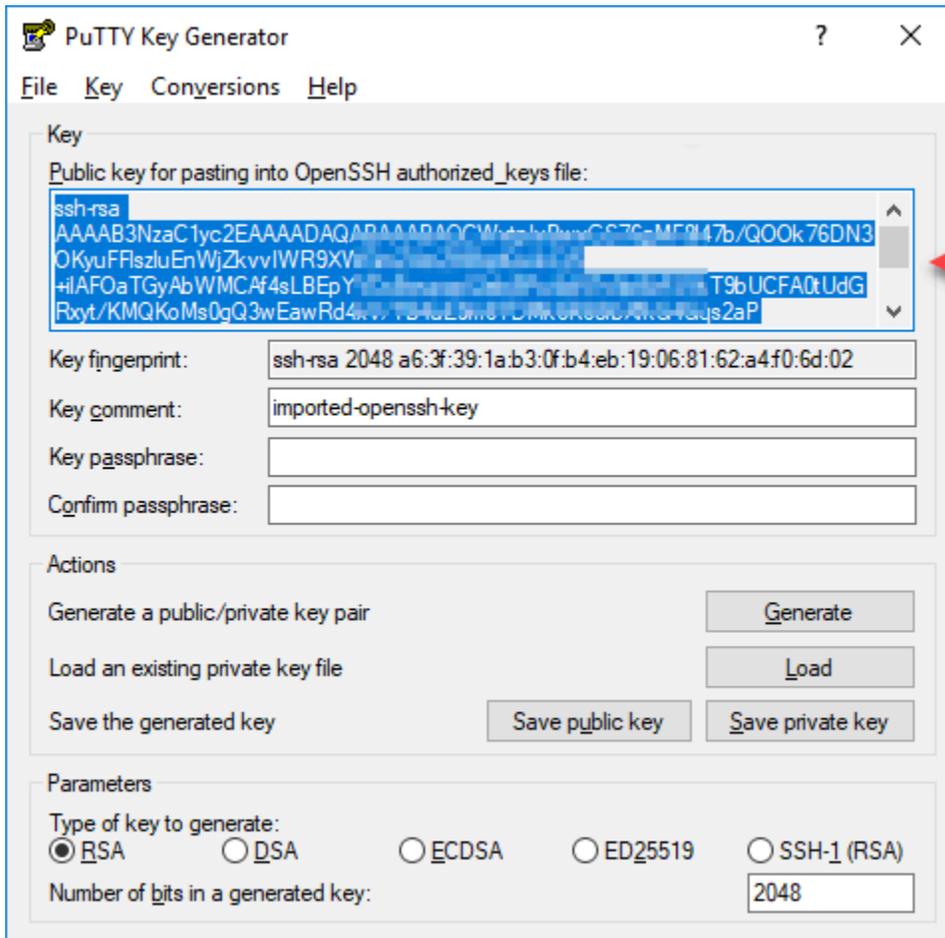
### 2. 選擇 Load (載入)。

根據預設，PuTTYgen 只會顯示副檔名為 .PPK 的檔案。若要尋找 .PEM 檔案，請選擇顯示所有檔案類型的選項。



3. 前往先前在本指南中建立的私密金鑰位置。選擇私密金鑰，接著選擇 Open (開啟)。
4. 在 PuTTYgen 確認您成功匯入金鑰後，請選擇 OK (確定)。
5. 反白 Public key (公開金鑰) 文字方塊的內容並複製到剪貼簿 (若您使用 Windows 請按 Ctrl+C (Ctrl+C)，若您使用 macOS 則按 Cmd+C (Cmd+C))。

如果您使用的是 Windows，請開啟文字編輯器 (例如「記事本」) TextEdit，然後按 Ctrl+V 將公開金鑰文字貼入其中，或者如果您使用的是 macOS，則按下「Cmd+V」。將公開金鑰文字存檔；您稍後在本指南中會需要。



- 繼續本指南的[在 Amazon EC2 中連接至 Linux 或 Unix 執行個體](#)一節，以連接至 EC2 執行個體並新增公有金鑰。

## 在 Amazon EC2 中連線至 Linux 或 Unix 執行個體

使用安全殼層 Connect 至 Amazon EC2 中的 Linux 或 Unix 執行個體，以移除 Lightsail 預設金鑰和系統金鑰。如需詳細資訊，請參閱[從亞馬遜快照建立的 Amazon EC2 中 Connect 到 Linux 或 Unix 執行個體](#)。

在 Amazon EC2 中連接至執行個體之後，繼續本指南的[新增公有金鑰至執行個體並測試連線](#)一節。

## 新增公開金鑰至執行個體並測試連線

公開金鑰內容儲存於 Linux 和 Unix 執行個體上的 `~/.ssh/authorized_keys` 檔案。編輯檔案以移除和取代您在 Amazon EC2 中的 Linux 或 Unix 執行個體中的 Lightsail 預設金鑰。

## 新增公開金鑰至執行個體和測試連線

1. 建立到執行個體的 SSH 連線後，輸入下列命令以使用 Vim 文字編輯器編輯 `authorized_keys` 檔案。

```
sudo vim ~/.ssh/authorized_keys
```

### Note

這些步驟使用 Vim 做為示範。然而，您可以針對這些步驟使用任何文字編輯器。

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQcQPFGPJSL0aAMzjPfuV2fpgkoHFohXJpybmXVisPuC
v6iGYfmb8flA89Eel4bKrl>
GyGFjY/wONNp3/8wNfeRei2
+tY/T3dxQvMI0Ti1Pv5mhUL
cbpEv3ISF9vdmsUs8kUlayf
LightsailDefaultKey
Pair
~
~
~
```

2. 按 **I** 鍵進入 Vim 編輯器的插入模式。
3. 在預設金鑰之後輸入額外的行。
4. 複製和貼上您先前在本指南中儲存的公開金鑰文字。

結果應如下列範例所示：

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQcQPFGPJSL0aAMzjPfuV2fpgkoHFohXJpybmXVisPuC
v6iGYfmb8flA89Eel4bKrl>
GyGFjY/wONNp3/8wNfeRei2
+tY/T3dxQvMI0Ti1Pv5mhUL
cbpEv3ISF9vdmsUs8kUlayfLkUFIic+TVLjKlK+PYkxVH+0qPZevu2gd9R2f LightsailDefaultKey
Pair
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQcWvtpIvBwvGS76gMF8l47b/Q00k76DN30KyUFFlszl
Pymgci5iWdhx1a8aDpgEvClwjsw+P9c7380Qny9PsUkifLYmJE000Sb9czuR imported-openssh-ke
y
~
~
```

Lightsail default key

New key

5. 按 **ESC** 鍵，然後輸入 `:wq!` 以儲存您的編輯並退出 Vim。
6. 輸入下列命令以重新啟動 Open SSH 伺服器：

```
sudo /etc/init.d/sshd restart
```

您應該會看到類似以下的結果：

```
[ec2-user@ip-172-26-11-173 ~]$ sudo /etc/init.d/sshd restart
Stopping sshd: [ OK ]
Starting sshd: [ OK ]
[ec2-user@ip-172-26-11-173 ~]$
```

新的公開金鑰現在已新增至您的執行個體。若要測試新的金鑰對，請與執行個體中斷連線。將 PuTTY 設定為使用新的私密金鑰，而非 Lightsail 預設金鑰。如果您能夠使用新 key pair 成功連線至執行個體，請繼續前往本指南的 [\[移除 Lightsail 預設金鑰\]](#) 區段，移除 Lightsail 預設金鑰。

## 移除 Lightsail 金鑰

將新的公開金鑰新增至執行個體，並使用新金鑰組成功連線至該金鑰後，請移除 Lightsail 預設 key pair。

若要移除 Lightsail 金鑰

1. 建立到執行個體的 SSH 連線後，輸入下列命令以使用 Vim 文字編輯器編輯 `authorized_keys` file。

```
sudo vim ~/.ssh/authorized_keys
```

2. 按 `I` 鍵進入 Vim 編輯器的插入模式。
3. 刪除以 `LightsailDefaultKeyPair` 結尾的行。這是預 Lightsail 金鑰。

```
sh- rsa AAAAB3NzaC1yc2EAAAADAQABAAQcQPFGPJSL0aAMzjPfUv2fpgkoHFohXJpybmXVisPuC
cbpEv3ISF9vdmsUs8kUlayFlKuFIIc+TVLjKlK+PYkxVH+0qPZevu2gd9R2f LightsailDefaultKey
Pair
ssh- rsa AAAAB3NzaC1yc2EAAAADAQABAAQcWvtpIvBwvGS76gMF8l47b/Q00k76DN30KyuFFlszl
Pymgci5iWdhx1a8aDpgEvClwjsw+P9c7380Qny9PsUkiflymJE000Sb9czuR imported-openssh-ke
y
~
~
```

4. 按 `ESC` 鍵，然後輸入 `:wq!` 以儲存您的編輯並退出 Vim。
5. 輸入下列命令以重新啟動 Open SSH 伺服器：

```
sudo /etc/init.d/sshd restart
```

您應該會看到類似以下的結果：

```
[ec2-user@ip-172-26-11-173 ~]$ sudo /etc/init.d/sshd restart
Stopping sshd: [ OK ]
Starting sshd: [ OK ]
[ec2-user@ip-172-26-11-173 ~]$
```

Lightsail 預設金鑰現在已從您的執行個體中移除。您的執行個體現在會拒絕使用 Lightsail 預設金鑰的連線。請繼續閱讀本指南的〈[移除 Lightsail 系統金鑰](#)〉一節，以移除 Lightsail 系統金鑰。

## 移除 Lightsail 系統鍵

在 Linux 和 Unix 執行個體上，Lightsail 系統金鑰也稱為 `lightsail_instance_ca.pub` 金鑰，可讓 Lightsail 以瀏覽器為基礎的安全殼層用戶端進行連線。執行下列步驟，在 Amazon EC2 中移除 Linux 或 Unix 執行個體的 `lightsail_instance_ca.pub` 金鑰，並編輯 `/etc/ssh/sshd_config` 檔案。`/etc/ssh/sshd_config` 檔案會定義到執行個體之 SSH 連線的參數。

若要移除 Lightsail 金鑰

1. 在連接至執行個體的 SSH 終端機視窗中，輸入下令命令以移除 `lightsail_instance_ca.pub` 金鑰：

```
sudo rm -r /etc/ssh/lightsail_instance_ca.pub
```

2. 輸入下列命令以使用 Vim 文字編輯器編輯 `sshd_config` 檔案。

```
sudo vim /etc/ssh/sshd_config
```

3. 按 `I` 鍵進入 Vim 編輯器的插入模式。
4. 從檔案刪除以下文字 (若存在)：

```
TrustedUserCAKeys /etc/ssh/lightsail_instance_ca.pub
```

5. 按 `ESC` 鍵，然後輸入 `:wq!` 以儲存您的編輯並退出 Vim。
6. 輸入下列命令以重新啟動 Open SSH 伺服器：

```
sudo /etc/init.d/sshd restart
```

您應該會看到類似以下的結果：

```
[ec2-user@ip-172-26-11-173 ~]$ sudo /etc/init.d/sshd restart
Stopping sshd: [ OK ]
Starting sshd: [ OK ]
[ec2-user@ip-172-26-11-173 ~]$
```

lightsail\_instance\_ca.pub 金鑰現在已從您的執行個體移除。相關聯的 sshd\_config 檔案已更新以排除該金鑰。

## Connect 到從快照建立的視窗伺服器 Amazon EC2 執行個體

在 Amazon Elastic Compute Cloud (Amazon EC2) 中建立新的 Windows Server 執行個體後，即可使用遠端桌面通訊協定 (RDP) 加以連線。這類似於您連接到來源 Amazon Lightsail 執行個體的方式。使用來源執行個體的預設 Lightsail key pair Connect 線至您的 AWS 區域 EC2 執行個體。本指南說明如何使用 Microsoft 遠端桌面連線連往您的 Windows Server 執行個體。

### Note

如需有關連線至 Linux 或 Unix 執行個體的詳細資訊，請參閱 [Connect 過 Lightsail 快照建立的 Amazon EC2 中的 Linux 或 Unix 執行個體連線](#)。

## 內容

- [取得執行個體的金鑰](#)
- [取得執行個體的公有 DNS 地址](#)
- [取得 Windows Server 執行個體的密碼](#)
- [設定遠端桌面連線連往您的 Windows Server 執行個體](#)
- [後續步驟](#)

## 取得執行個體的金鑰

您在 Amazon EC2 中的 Windows 伺服器執行個體使用來源執行個體區域的預設 Lightsail key pair 來擷取預設管理員密碼。

從 [Lightsail 帳戶頁面](#) 上的安全殼層金鑰索引標籤下載預設私密金鑰。如需有關預設 Lightsail 安全殼層金鑰的詳細資訊，請參閱 [安全殼層金鑰配對](#)。

**Note**

連接至 EC2 執行個體後，建議在 Amazon EC2 中變更 Windows Server 執行個體的管理員密碼。它會移除預設的 Lightsail key pair 和您在 Amazon EC2 中的 Windows 伺服器執行個體之間的關聯。如需詳細資訊，請參閱[保護從 Lightsail 快照建立的 Amazon EC2 視窗伺服器執行個體的安全](#)。

## 取得執行個體的公有 DNS 地址

取得 Amazon EC2 執行個體的公有 DNS 地址，並在設定 RDP 用戶端 (如 Microsoft 遠端桌面通訊協定) 時，使用該地址來連接到執行個體。

若要取得執行個體的公有 DNS 地址

1. 登入 [Amazon EC2 主控台](#)。
2. 從左側導覽窗格中選擇 Instances (執行個體)。
3. 選擇欲連接的執行中 Windows Server 執行個體。
4. 在窗格下方中，找到您執行個體的 Public DNS (公有 DNS) 地址。

這是您在設定 RDP 用戶端時用來連接到執行個體的地址。繼續本指南的[取得 Windows Server 執行個體密碼](#)章節，了解如何在 Amazon EC2 中取得 Windows Server 執行個體的預設管理員密碼。

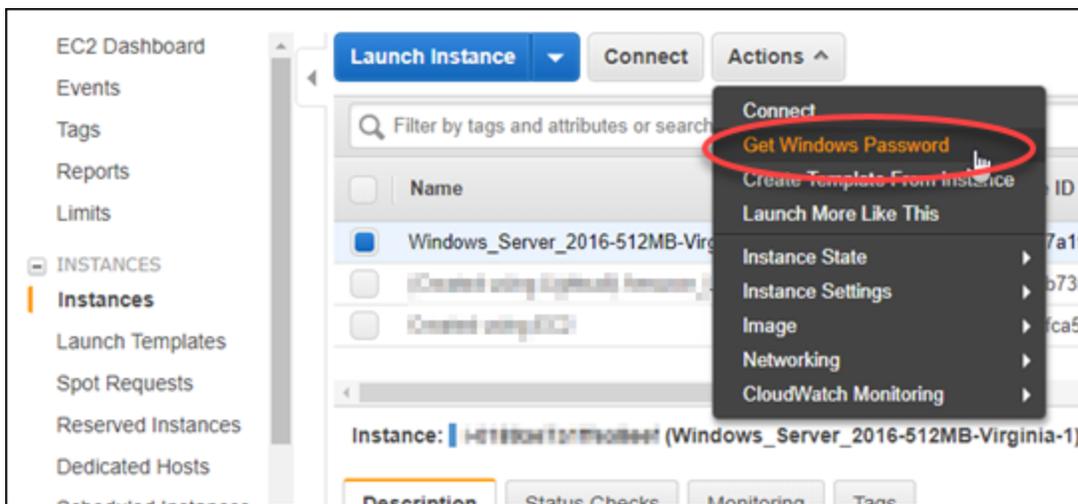
The screenshot shows the Amazon EC2 console interface. At the top, there are buttons for 'Launch Instance', 'Connect', and 'Actions'. Below that is a search bar and a table of instances. The table has columns for Name, Instance ID, Instance Type, Availability Zone, Instance State, and Status Checks. Two instances are listed: one with Instance ID 'i-0123456789abcdef0' (t3.nano) and another with Instance ID 'i-0123456789abcdef1' (t2.micro). The t2.micro instance is selected. Below the table, the details for the selected instance are shown. The 'Public DNS' field is circled in red and contains the address 'ec2-01-123-189-87.compute-1.amazonaws.com'. Below this, the 'Public DNS (IPv4)' field is also circled in red and contains the same address. Other fields include 'Instance ID', 'Instance state' (running), 'Instance type' (t2.micro), 'IPv4 Public IP', and 'IPv6 IPs'.

## 取得 Windows Server 執行個體的密碼

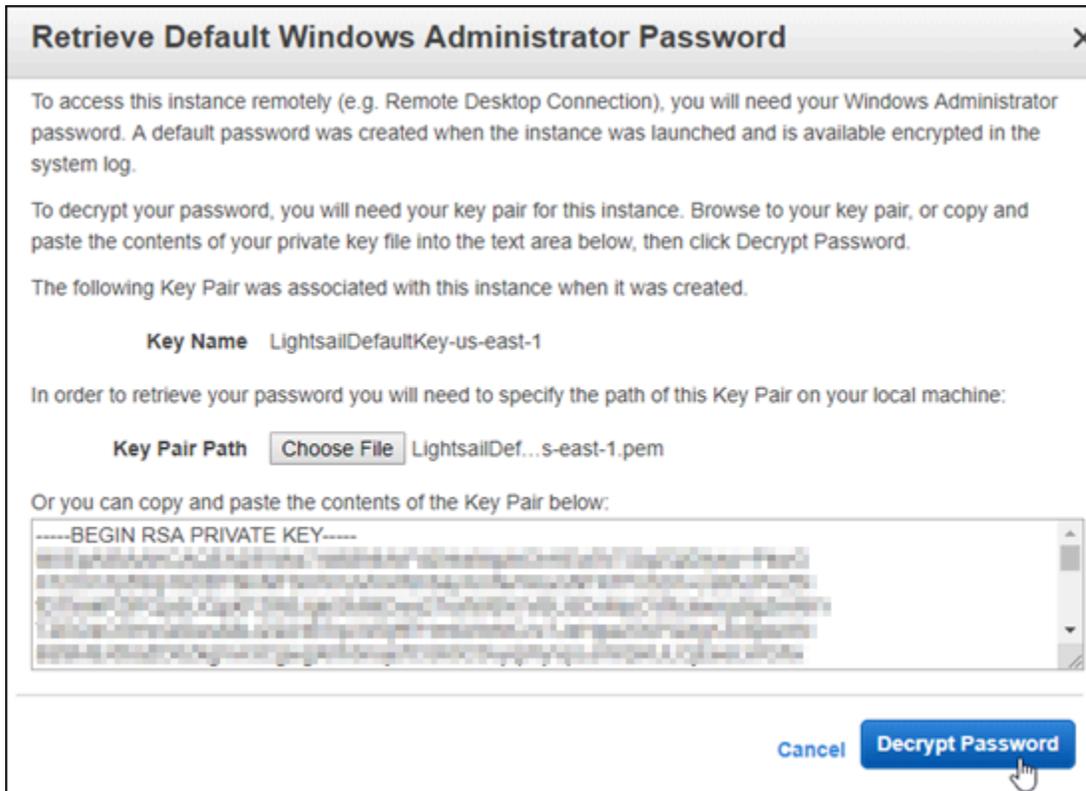
從 Amazon EC2 主控台取得 Windows Server 執行個體的密碼。透過 RDP 連接至 Windows Server 執行個體時，您必須使用此密碼來登入其中。

若要取得 Windows Server 執行個體的密碼

1. 登入 [Amazon EC2 主控台](#)。
2. 從左側導覽窗格中選擇 Instances (執行個體)。
3. 選擇欲連接的 Windows Server 執行個體。
4. 選擇 Actions (動作)，然後選擇 Get Windows Password (取得 Windows 密碼)。



5. 出現提示時，選擇「瀏覽」，然後開啟您從本指南稍早前面的 Lightsail 下載的預設私密金鑰檔案。
6. 選擇 Decrypt Password (解密密碼)。



螢幕上會顯示密碼，以及公有 DNS 和使用者名稱。將密碼複製到剪貼簿，本指南下一節[設定遠端桌面連線連往 Windows Server 執行個體](#)將使用此密碼。反白選取密碼，然後按下 Ctrl+C (Ctrl+C) (若您使用 Windows) 或 Cmd+C (Cmd+C) (若您使用 macOS)。



繼續本指南的[設定遠端桌面連線連以連接至 Windows Server 執行個體](#)一節，了解如何設定遠端桌面連線，以便在 Amazon EC2 中連接至 Windows Server 執行個體。

## 設定遠端桌面連線連往您的 Windows Server 執行個體

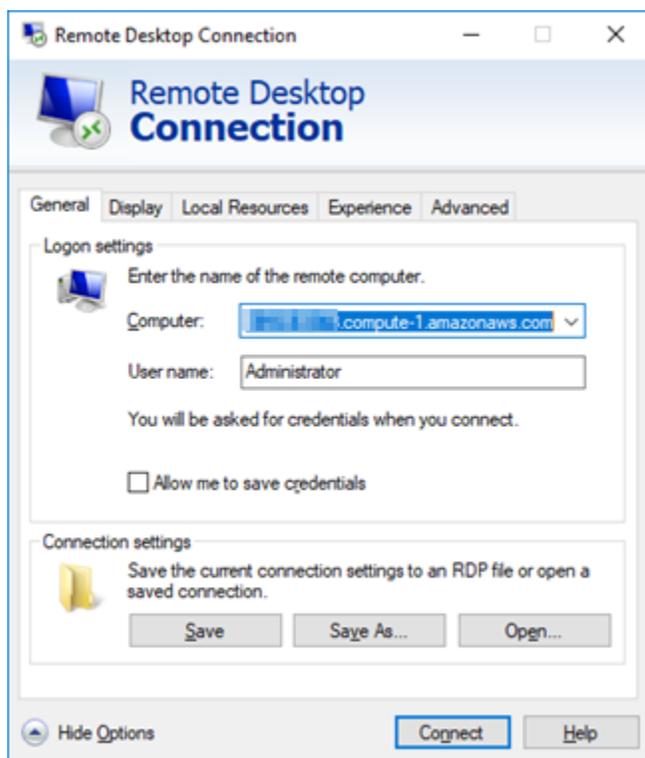
遠端桌面連線為 RDP 用戶端，多數 Windows 作業系統均已預先安裝。使用此功能連接到 Amazon EC2 中的 Windows Server 執行個體。

若要設定遠端桌面連線連往您的 Windows Server 執行個體

1. 開啟遠端桌面連線。

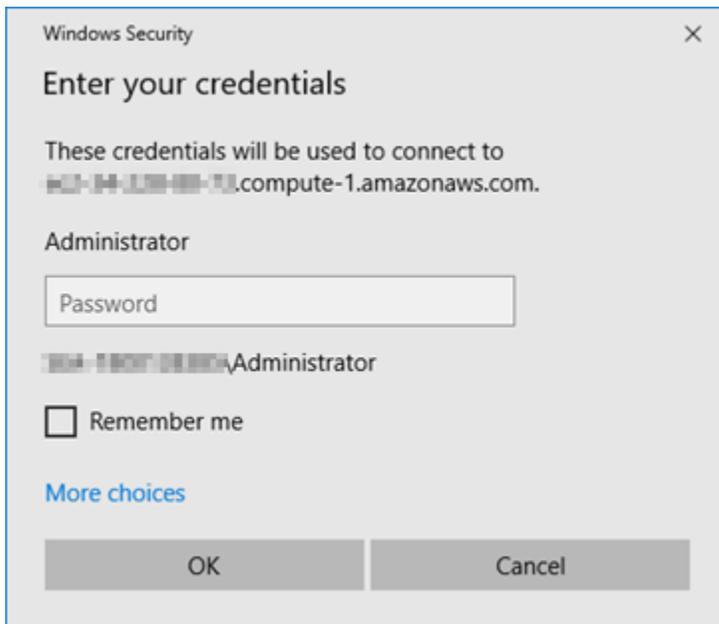
例如，選擇 Windows Start (開始) 功能表，然後搜尋 Remote Desktop Connection (遠端桌面連線)。

2. 在電腦文字方塊中，輸入您之前遵循本指南取得的 Amazon EC2 中的 Windows Server 執行個體的公有 DNS 地址。
3. 選擇 Show Options (顯示選項) 來檢視其他選項。
4. 將 Administrator 輸入 User name (使用者名稱) 文字方塊。

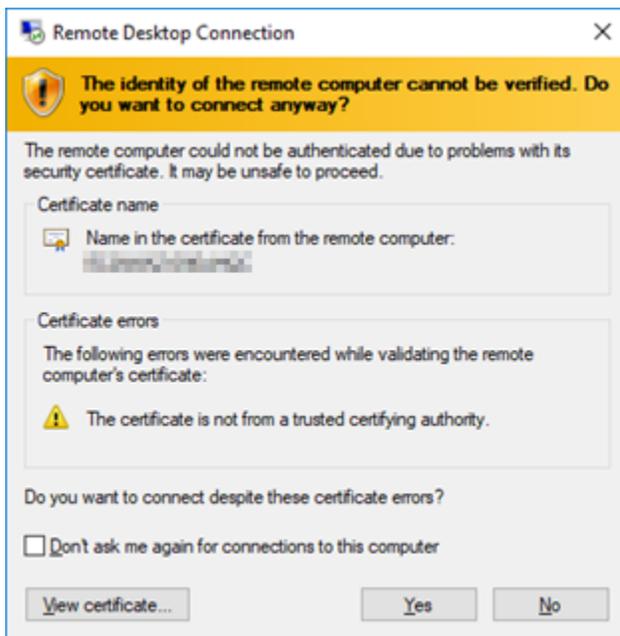


5. 選擇 Connect (連接) 以連接到您的 Windows Server 執行個體。

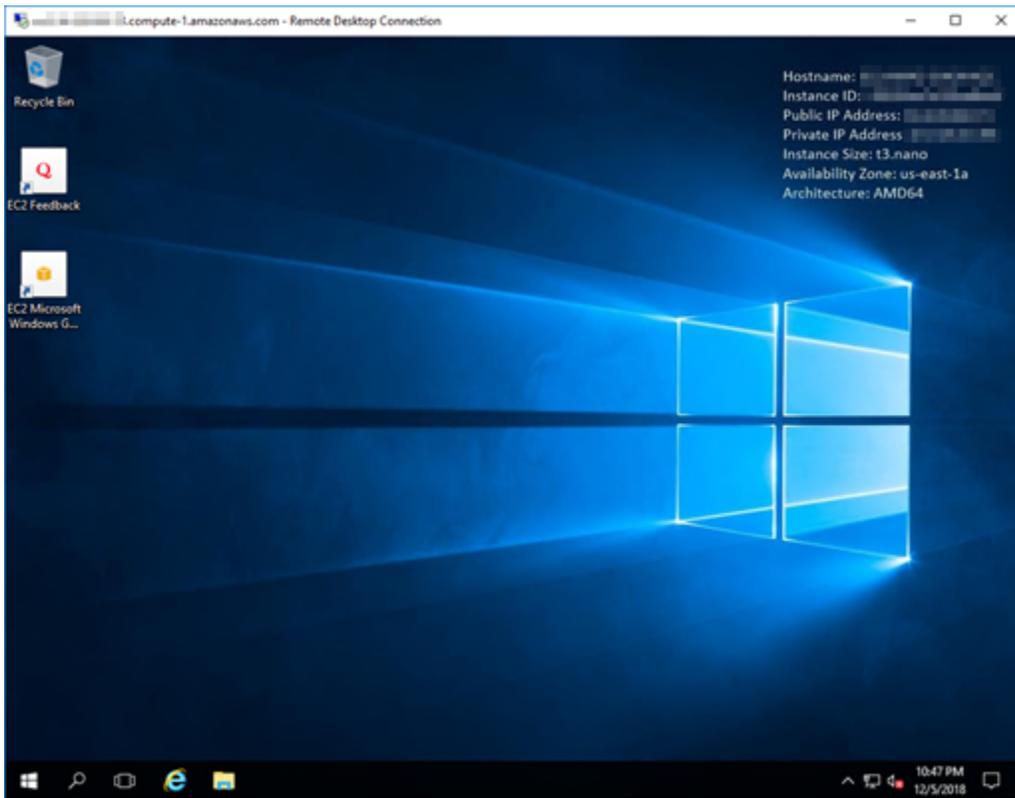
- 在 Windows 安全性提示中，於 Password (密碼) 文字方塊中輸入您 Windows Server 執行個體的密碼，然後選擇 OK (確定)。



- 在遠端桌面連線提示中，選擇 Yes (是) 來連線。



如果您已成功連接到執行個體，您應該會看到類似以下的畫面：



## 後續步驟

建議您變更 Amazon EC2 中 Windows Server 執行個體的管理員密碼。它會移除預設的 Lightsail key pair 和您在 Amazon EC2 中的 Windows 伺服器執行個體之間的關聯。如需詳細資訊，請參閱[保護從 Lightsail 快照建立的 Amazon EC2 中的 Windows 伺服器執行個體安全](#)。

## 從快照啟動的安全視窗伺服器 Amazon EC2 執行個體

若要改善從 Amazon Amazon Lightsail 快照建立的 Amazon Elastic Compute Cloud (Amazon EC2) 中 Windows 伺服器執行個體的安全性，建議您變更預設管理員密碼。這會移除您的 Lightsail 金鑰配對與 Amazon EC2 中新視窗伺服器執行個體之間的關聯。

### Note

如果您是透過 Lightsail 快照在 Amazon EC2 中建立 Linux 或 Unix 執行個體，則應執行幾個步驟來保護這些執行個體的安全。如需詳細資訊，請參閱[保護透過 Lightsail 快照建立的 Amazon EC2 Linux 或 Unix 執行個體的安全](#)。

## 內容

- [在 Amazon EC2 中連接至 Windows Server 執行個體](#)
- [在 Amazon EC2 中變更 Windows Server 執行個體的預設管理員密碼](#)

### 在 Amazon EC2 中連接至 Windows Server 執行個體

使用遠端桌面通訊協定 (RDP)，在 Amazon EC2 中變更 Windows Server 管理員密碼，連接至 Windows Service 執行個體。要了解如何 Connect 到您的執行個體，請參閱從 [Lightsail 快照建立的 Amazon EC2 中連接到 Windows 伺服器執行個體](#)。

連接至 Amazon EC2 中的執行個體後，請繼續本指南的 [在 Amazon EC2 中變更 Windows Server 執行個體的預設管理員密碼](#) 一節。

### 在 Amazon EC2 中變更 Windows Server 執行個體的預設管理員密碼

變更 Windows 伺服器執行個體上的預設密碼，以移除 Lightsail 金鑰配對與 Amazon EC2 中新 Windows 伺服器執行個體之間的關聯。

在 Amazon EC2 中變更 Windows Server 執行個體的預設管理員密碼

1. 建立到執行個體的 RDP 連線後，請開啟命令提示並輸入以下命令。

```
net user Administrator "Password"
```

在命令中，將 *Password* 取代為您的新密碼。

範例：

```
net user Administrator "%4=Bwk^GEAg8$u@5"
```

您應該會看到類似以下的結果：

```
C:\Users\Administrator>net user Administrator "%4=Bwk^GEAg8$u@5"  
The command completed successfully.
```

```
C:\Users\Administrator>_
```

2. 將新密碼存放於安全處。您無法使用 Amazon EC2 主控台擷取新密碼。主控台只會擷取預設密碼。如果您在變更密碼後嘗試使用預設密碼連接至執行個體，則會顯示錯誤訊息指出您的登入資料無法作用。

如果您的密碼遺失或過期，您可產生新的密碼。如需密碼重設程序，請參閱 Amazon EC2 文件中的 [重設遺失或過期的 Windows 管理員密碼](#)。

## 檢視 Lightsail 實體的 AWS CloudFormation 堆疊

Amazon Lightsail 使用匯出 AWS CloudFormation 的快照建立亞馬遜彈性運算雲端 (Amazon EC2) 執行個體。當您請求使用 Lightsail 主控台或 Lightsail API 建立 Amazon EC2 執行個體時，會建立一個 CloudFormation 堆疊。該堆疊會在您的 Amazon Web Services (AWS) 帳戶中執行一系列動作，以便為執行個體 (例如 Amazon Machine Image (AMI) 中的 Amazon EC2 執行個體)、EBS 快照中的 Elastic Block Store (EBS) 系統磁碟區以及執行個體的安全群組建立所有相關資源。若要進一步了解 AWS CloudFormation 堆疊，請參閱 [AWS CloudFormation 文件中的使用堆疊](#)。

您可以透過 Lightsail 主控台或主控台存取 AWS CloudFormation AWS CloudFormation 堆疊。本指南說明如何存取兩者。

### Note

用來建立 Amazon EC2 資源的 AWS CloudFormation 堆疊會永久連結至您的 Amazon EC2 資源。如果您刪除堆疊，則會將所有相關資源自動刪除。因此，您不應刪除 Lightsail 建立的任何 AWS CloudFormation 堆疊，而是使用 EC2 主控台刪除 Amazon EC2 資源。

## 透過主 AWS CloudFormation 控制台存 Lightsail 堆疊

當您選擇使用 Lightsail 主控台或 Lightsail API 在 Amazon EC2 中建立執行個體之後，便會建立一個 AWS CloudFormation 堆疊，並在 Lightsail 主控台的「匯出」區段中追蹤其狀態。若要進一步瞭解匯出，請參閱 [追蹤快照匯出狀態](#)。

若要在 Lightsail 主控台中檢視 AWS CloudFormation 堆疊

1. 登入主 [Lightsail 台](#)。
2. 在左側導覽窗格中選擇 [匯出]。
3. 若要存取先前建立之 Amazon EC2 執行個體的 CloudFormation 堆疊，請針對標示為已建立 EC2 資源的任務選擇 [檢視詳細資料]。

**Task history**

**Created EC2 resources**

Source snapshot name	Status	Export started
Amazon_Linux_2-1-1675289631	✔ Succeeded	April 30, 2024 at 18:11 (UTC-7:00)

[View details](#)

- 出現的確認頁面會列出工作的 CloudFormation 堆疊。選擇堆疊名稱以在 AWS CloudFormation 主控台中開啟堆疊詳細資料。

## 在 AWS CloudFormation 控制台中訪問堆棧

您也可以透過 [AWS CloudFormation 主控台](#) 存取堆疊詳細資訊。由 Lightsail 創建的堆棧開始「Lightsail 堆棧」，並具有「用於創建 Amazon EC2 資源的 CloudFormation 堆棧」的描述，如下面的螢幕截圖。

具有「建立 \_ 進度」狀態的堆疊正在從匯出的 Lightsail 快照建立 Amazon EC2 資源。狀態為 CREATE\_COMPLETED 的堆疊已完成建立 Amazon EC2 資源的程序。要查看堆疊建立的資源，選擇堆疊名稱旁的核取方塊，然後選擇 Resources (資源) 索引標籤。

Filter: Active ▾ By Stack Name Showing 4 stacks

Stack Name	Created Time	Status	Drift Status	Description
<input checked="" type="checkbox"/> Lightsail-Stack-a0e00482-77a3-4f32-a3...	2018-11-19 09:46:24 UTC-0800	CREATE_COMPLETE	NOT_CHECKED	CloudFormation stack used...
<input type="checkbox"/> Lightsail-Stack-104e982e-cba3-49d7-96...	2018-11-19 09:15:51 UTC-0800	CREATE_COMPLETE	NOT_CHECKED	CloudFormation stack used...
<input type="checkbox"/> Lightsail-Stack-ff4267e8-44c6-49e0-941...	2018-11-12 11:17:42 UTC-0800	CREATE_COMPLETE	NOT_CHECKED	CloudFormation stack used...
<input type="checkbox"/> Lightsail-Stack-0e805e88-f78a-4c4e-85...	2018-11-02 14:35:24 UTC-0700	CREATE_COMPLETE	NOT_CHECKED	CloudFormation stack used...

Overview Outputs **Resources** Events Template Parameters Tags Stack Policy Change Sets Rollback Triggers

To view detailed drift information for specific resources, visit the [Drift Details page](#).

Logical ID	Physical ID	Type	Drift Status	Status	Status Reason
Instance3fd67c5c...	i-09a6442334a538516	AWS::EC2::Instance	NOT_CHECKED	CREATE_COMPL...	
SecurityGroup9e8...	sg-0359d91e0b64c4556	AWS::EC2::SecurityGroup	NOT_CHECKED	CREATE_COMPL...	

# 為您的網站註冊和管理 Lightsail

您的網站需要名稱，例如 `example.com`。使用 Amazon Lightsail，您可以為您的網站註冊一個名稱，稱為域名。為了存取您的網站，使用者會在網頁瀏覽器中輸入您的網域名稱。

使用 Amazon Lightsail 主控台內的網域和 DNS 索引標籤來註冊和管理網域名稱。Lightsail 使用 Amazon Route 53，這是一種高可用性和可擴展的網域名稱系統 (DNS) 網路服務，為您註冊網域。註冊網域之後，您可以將網域指派給 Lightsail 資源或管理該網域的 DNS 記錄。如需 DNS 的一般資訊，請參閱 [DNS](#)。

有關 Amazon Lightsail 域名註冊的更多信息，請繼續閱讀。

## 內容

- [域註冊的運作方式](#)
- [您可以在其中註冊的 Lightsail](#)
- [域註冊的定價](#)

## 域註冊的運作方式

以下概觀說明如何在 Amazon Lightsail 中註冊網域名稱：

1. 確認您想要的網域名稱可在網際網路上使用。如果您想要的網域名稱不可用，您可以嘗試使用其他名稱，或只將頂層網域(如 `.com`) 變更為另一個頂層網域(如 `.org` 或 `.net`)。如需 Lightsail 支援的頂層網域 (TLD) 清單，請參閱[您可以在 Amazon Lightsail 中註冊的網域](#)。
2. 向 Lightsail 註冊網域名稱。當您註冊網域時，提供網域擁有人和其他聯絡人的姓名和聯絡資訊。

在註冊程序結束時，我們會將您提供的資訊傳送給網域註冊商。網域註冊商是網際網路名稱與數字位址分配機構 (ICANN) 認可的公司，旨在處理特定 TLD 的網域註冊。網域的註冊商是 Amazon Registrar，或我們的註冊商合作夥伴 Gandi。

Amazon Registrar 和 Gandi 預設會隱藏不同的資訊。Amazon Registrar, Inc. 會隱藏所有聯絡人資訊，Gandi 則會隱藏組織名稱以外的所有聯絡人資訊。

- 若要瞭解您網域的註冊商是誰，請參閱[您可以在 Amazon Lightsail 中註冊的網域](#)。
- 註冊商會將您的資訊傳送給網域的「註冊機構」。註冊機構是銷售一或多個頂層網域(如 `.com`) 的網域註冊的公司。

- 註冊機構將您的網域相關資訊存放在其自己的資料庫中，並將其中一些資訊存放在公共 WHOIS 資料庫中。

如需有關如何註冊域名稱的詳細資訊，請參閱[註冊新域](#)。

使用 Lightsail 註冊網域之後，Route 53 會將一組名稱伺服器指派給您的網域，讓自己成為網域的 DNS 服務。名稱伺服器是協助將網域名稱轉譯成 IP 地址的伺服器。

Lightsail 會自動執行下列動作，使其本身成為網域的 DNS 服務：

- 建立與您的網域名稱相同的 [Lightsail DNS 區域](#)。
- 將一組四個名稱伺服器指派給 Lightsail DNS 區域。
- 將網域的 Route 53 名稱伺服器取代為來自您 Lightsail DNS 區域的名稱伺服器。

如果您已經向另一個註冊商註冊網域名稱，可以選擇將網域 DNS 的管理作業轉移到 Lightsail。使用其他 Lightsail 功能不需要此操作。如需詳細資訊，請參閱[建立 DNS 區域以管理域的 DNS 記錄](#)。

## 您可以在其中註冊的 Lightsail

Lightsail 使用與 Route 53 相同的通用頂層網域 (TLD)。如需可用於在 Lightsail 中註冊網域的一般頂級域名清單，請參閱 Amazon Route 53 開發人員指南中[可向 Amazon Route 53 註冊的網域](#)。

如果 TLD 未包含在清單中，或者您想要註冊地理域，建議您使用 Route 53 主控台。您的地理網域在使用 Route 53 註冊之後，就可以在 Lightsail 主控台中使用該網域。如需詳細資訊，請參閱《Amazon Route 53 開發人員指南》中的[地理頂層域](#)。

## 域註冊的定價

Lightsail 使用 Route 53 進行網域註冊。因此，Route 53 的定價也適用於 Lightsail 註冊。

如需註冊域費用的資訊，請參閱《Amazon Route 53 開發人員指南》中的[可在 Amazon Route 53 中註冊的域](#)。

## 網域的其他相關資訊

下列文章可協助您管理 Lightsail 中的網域：

- [DNS](#)

- [格式化域名稱](#)
- [管理 Amazon Route 53 中的 Lightsail 域名](#)
- [建立 DNS 區域以管理域的 DNS 記錄](#)
- [域註冊續約](#)
- [編輯或刪除 DNS 區域](#)
- [將域指向負載平衡器](#)
- [將域指向分發](#)
- [將域指向執行個體](#)
- [將域流量路由至容器服務](#)

## 了解 DNS Lightsail

使用者可以瀏覽執行個體的公用網際網路通訊協定 (IP) 位址 (可能是 IPv4 或 IPv6 位址)，存取 Lightsail 執行個體上的 Web 應用程式。然而，IP 地址對人們而言比較複雜也很難記住。因此，您應該讓人們瀏覽至網域 easy-to-remember 域名稱，例如 `example.com`，以存取執行個體上的 Web 應用程式。這是透過網域名稱系統 (DNS) 來實現的，該系統可作為將註冊的網域名稱對應至 IP 位址的目錄。

若要將網域名稱的流量路由至 Lightsail 執行個體，請新增地址 (A) 記錄，將網域名稱指向執行個體的靜態 IPv4 位址，或指向執行個體 IPv6 位址的 AAAA 記錄。如果您使用 Lightsail 註冊網域名稱，則可以從註冊網域名稱時建立的 DNS 區域管理 DNS 記錄。如果您的網域是透過其他註冊商註冊，您可以在註冊商處管理 DNS 記錄，也可以將網域的管理權限轉移 DNS 至 Lightsail。

若要更輕鬆地將您的網域名稱對應至 Lightsail 執行個體，建議您建立區域，將網域 DNS 記錄的管理作業移轉至 Lightsail。如需詳細資訊，請參閱 [建立 DNS 區域以管理網域 DNS 記錄](#)。您最多可以在 Lightsail 中建立六個 DNS 區域。如果您需要六個以上 DNS 的 DNS 區域，我們建議您使用 Route 53 來管理所有網域。您可以使用 Route 53 將網域名稱指向您的 Lightsail 執行個體。如需使用 Route 53 進行管理 DNS 的詳細資訊，請參閱 [使用 Amazon Route 53 將網域指向執行個體](#)。

## DNS 術語

為了讓您可以管理您的域，有一些您應該熟悉的術語。

### Apex 網域/根網域

Apex 網域也稱為根網域，是不包含子網域部分的網域。Apex 網域的範例為 `example.com`。而子網域的範例為 `www.example.com` 和 `blog.example.com`。這些是子網域，因為它們分別包含 `www` 和 `blog` 子網域部分。

## 網域名稱系統 (DNS)

DNS路由網 easy-to-remember 域名稱，例如example.com，到 Web 伺服器的 IP 位址。

如需詳細資訊，請參閱 Wikipedia 上的[網域名稱系統](#)。

## DNS記錄

記DNS錄是一個映射參數。它告訴DNS服務器的 IP 地址或主機名與域或子域相關聯。

有關更多信息，請參閱維基百科上的[DNS記錄類型列表](#)。

## DNS區域

DNS區域是一個容器，其中包含您希望如何在網際網路上為特定網域 (例如) 及其子網域 (例如example.com) 路由流量的資訊。blog.example.com

有關更多信息，請參見維基百科上的[DNS區域](#)。

## 網域名稱註冊機構

網域名稱註冊機構 (也稱為網域名稱供應商) 是管理網域名稱指派作業的公司或組織。您可以使用 Lightsail、Amazon Route 53 或任何其他網域名稱註冊商購買網域或管理現有網域。

如需詳細資訊，請參閱 Wikipedia 上的[網域名稱註冊機構](#)。

## 名稱伺服器

名稱伺服器會將流量路由到您的網域。在 Lightsail 中，名稱伺服器是執行網路服務的執行個 AWS 體，可協助將網 easy-to-remember 域名稱轉譯為 IP 位址。Lightsail 提供數個 AWS 名稱伺服器選項 (例如ns-NN.awsdns-NN.com)，可將流量路由到您的網域。當您使用網域註冊商變更網域時，您可以從這些 AWS 名稱伺服器中進行選擇。

如需詳細資訊，請參閱 Wikipedia 上的[名稱伺服器](#)。

## 子網域

子網域是網域階層中的任何內容，和較大網域的一部分的根網域不同。例如，blog 是 blog.example.com 子網域的子網域部分。

如需詳細資訊，請參閱 Wikipedia 上的[子網域](#)。

## 生活時間 (TTL)

TTL規定本機解析名稱伺服器上DNS記錄的壽命；例如，較短的時間表示等待變更生效的時間越少。TTL無法在 Lightsail DNS 區域中設定。相反地，所有 Lightsail DNS 記錄的預設值為 60 秒。TTL

如需詳細資訊，請參閱 Wikipedia 上的[存留時間](#)。

## 通配符DNS記錄

萬用字元DNS記錄會比對不存在網域名稱的要求。萬用字元DNS記錄是使用星號 (\*) 做為網域名稱最左邊的部分，例如 \*.example.com 或 \*example.com

### Note

Lightsail DNS 區域支援名稱伺服器 (NS\*awsdns.com) 記錄中定義的名稱伺服器網域 () 萬用字元記錄。

## DNS Lightsail DNS 區域支援的記錄類型

### 地址 (A) 記錄

A 記錄可將網域 (例如 example.com) 或子網域 (例如 blog.example.com) 映射至 web 伺服器的 IP 地址。

例如，在 Lightsail DNS 區域中，您想要將 example.com (網域頂點) 的網路流量導向至執行個體。您會建立一個 A 記錄，輸入一個 @ 符號至 Subdomain (子網域) 的文字方塊中，然後將 web 伺服器的 IP 地址輸入到 Resolves to address (解析為地址) 的文字方塊中。

有關 A 記錄的更多信息，請參閱維基百科上的[DNS記錄類型列表](#)。

### AAAA記錄

AAAA記錄會將網域 (例如example.com) 或子網域 (例如blog.example.com) 對應至 Web 伺服器的IPv6位址。

例如，在 Lightsail DNS 區域中，您想要透過通IPv6訊協定將 example.com (網域頂點) 的網路流量導向至您的執行個體。您可以建立AAAA記錄，在 [子網域] 文字方塊中輸入@符號，然後在 [解析為位址] 文字方塊中輸入 Web 伺服器的 IP 位址。

有關AAAA記錄的更多信息，請參閱維基百科IPv6上的[域名系統](#)。

### Note

Lightsail 不支援靜態IPv6位址。如果您刪除 Lightsail 資源並建立新資源，或者停用並重新 IPv6 啟用相同資源，則可能需要更新AAAA記錄以反映資源的最新IPv6位址。

## 標準名稱 () CNAME 記錄

記CNAME錄會將別名或子網域 (例如blog.example.com) 對應至其他網域或子網域。

例如，在 Lightsail DNS 區域中，您想要將的網路流量導向www.example.com至example.com。您可以使用的「解析為www」地址建立別名CNAME記錄example.com。

有關更多信息，請參閱維基百科上的[CNAME記錄](#)。

## 郵件交換程式 (MX) 記錄

MX 記錄可將子網域 (例如 mail.example.com) 映射至電子郵件伺服器地址，如果定義了多部伺服器，還能包含優先順序值。

例如，在 Lightsail DNS 區域中，您想要將郵件導向mail.example.com至 10 inbound-smtp.us-west-2.amazonaws.com Amazon WorkMail 伺服器。您將以 example.com 的子網域建立 MX 記錄，優先順序為 10，以及 inbound-smtp.us-west-2.amazonaws.com 的「resolves to」(解析為) 地址。

如需詳細資訊，請參閱 Wikipedia 上的 [MX 記錄](#)。

## 名稱伺服器 (NS) 記錄

NS 記錄會委派一個子網域 (例如 test.example.com) 到名稱伺服器，例如 ns-NN.awsdns-NN.com。

如需詳細資訊，請參閱 Wikipedia 上的[名稱伺服器](#)。

## 服務定位器 (SRV) 記錄

SRV記錄會將子網域 (例如) 對應至具有優先順序service.example.com、權重和連接埠號碼值的服務位址。電話語音或即時消息是一對夫婦通常與SRV記錄相關聯的服務。

例如，在 Lightsail DNS 區域中，您想要將流量引導service.example.com至1 10 5269 xmpp-server.example.com。您可以建立具有的優先順序1、權重10、連接埠號碼以及「對應至」位址的SRV記錄xmpp-server.example.com。5269

有關更多信息，請參閱維基百科上的[SRV記錄](#)。

## 文字 (TXT) 記錄

記TXT錄會將子網域對應至純文字。您可以建立TXT記錄，以向服務供應商確認您的網域擁有權。

例如，在 Lightsail DNS 區域中，您想要在查詢 `_amazonchime.example.com` 主機名稱 `23223a30-7f1d-4sx7-84fb-31bdes7csdbb` 時回應。您可以建立子網域值的 TXT 記錄，`_amazonchime` 且值為的「回應」。 `23223a30-7f1d-4sx7-84fb-31bdes7csdbb`

有關更多信息，請參閱維基百科上的 [TXT 記錄](#)。

## 建立 DNS 區域以管理 Lightsail 執行個體的網域記錄

若要將網域名稱 (例如) 的流量路由至 Amazon Lightsail 執行個體，請將記錄新增至網域的網域名稱系統 (DNS)。 `example.com` 您可以使用註冊網域的註冊商來管理網域 DNS 記錄，也可以使用 Lightsail 來管理網域記錄。

我們建議您將網域 DNS 記錄的管理作業移轉至 Lightsail。這可讓您在同一個位置 (Lightsail) 中有效管理網域和運算資源。您可以透過建立 Lightsail 區域來管理您的網域 DNS 記錄。DNS 您最多可以建立六個 Lightsail DNS 區域。如果您需要六個以上的 DNS 區域，因為您管理的網域名稱超過六個，建議您使用 Amazon Route 53 管理所有網域。DNS 您可以使用 Route 53 將您網域的流量路由至您的 Lightsail 資源。如需使用 Route 53 進行管理 DNS 的詳細資訊，請參閱 [使用 Amazon Route 53 將網域指向執行個體](#)。

本指南說明如何為您的網域建立 Lightsail DNS 區域，以及如何將網域 DNS 記錄的管理轉移至 Lightsail。將網域 DNS 記錄的管理移轉至 Lightsail 之後，您將繼續在網域註冊商管理網域的續約和帳單。

### Important

您對域所做 DNS 的任何更改都可能需要幾個小時才能通過互聯網傳播。DNS 因此，您應該將網域的 DNS 記錄保留在網域目前的主機服務供應商，同時將管理資料移轉至 Lightsail。這可確保網域的流量在轉移過程中可持續不間斷地路由到您的資源。

## 步驟 1：完成先決條件

請先完成事前準備 (若尚未完成)：

1. 註冊一個網域名稱。接著確認您具有管理存取權，可編輯網域的名稱伺服器。

如果您需要註冊的網域名稱，可以使用 Lightsail 註冊網域。如需詳細資訊，請參閱 [域註冊](#)。

2. 確認 Lightsail DNS 區域支援您網域的必要DNS記錄類型。Lightsail DNS 區域目前支援位址 (A 和 AAAA)、標準名稱 (CNAME)、郵件交換器 (MX)、名稱伺服器 (NS)、服務定位器 (SRV) 和文字 (TXT) 記錄類型。對於 NS 記錄，您可以使用萬用字元DNS記錄項目。

如果 Lightsail DNS 區域不支援您網域所需的DNS記錄類型，您可能需要使用 Route 53 作為網域的DNS託管服務供應商，因為它支援更多記錄類型。如需詳細資訊，請參閱 [Amazon Route 53 開發人員指南中的支援DNS記錄類型和使 Amazon Route 53 成為現有網域的DNS服務](#)。

3. 建立您要將網域指向的 Lightsail 實體。如需詳細資訊，請參閱[建立執行個體](#)。
4. 建立靜態 IP 並將其附加至您的 Lightsail 執行個體。如需詳細資訊，請參閱[建立靜態 IP 並將其附接至執行個體](#)。

## 步驟 2：在主控台中建立DNS區域

請完成下列步驟，以在 Lightsail 中建立DNS區域。建立DNS區域時，您必須指定要套用DNS區域的網域名稱。

1. 登入主 [Lightsail 台](#)。
2. 在左側導覽窗格中，選擇 [網域與] DNS。然後選擇「建立DNS區域」。
3. 請選擇下列其中一個選項：
  - 使用向 Amazon Route 53 註冊的域，以指定向 Amazon Route 53 註冊的域
  - Use a domain from another registrar (使用其他註冊商的網域)，指定使用其他註冊商註冊的網域
4. 選取或輸入註冊的網域名稱，例如 example.com。

輸入網域名稱時，不需要包含 www。您可以將www使用地址 (A) 記錄新增為本指南稍後「[步驟 3：將記錄新增至DNS區域](#)」一節的一部分。

### Note

Lightsail DNS 區域是在維吉尼亞州 (us-east-1) AWS 區域建立的。如果您將該區域中的資源命名為與要建立的 Lightsail DNS 區域 () 相同，則會出現資源名稱衝突錯誤 (「某些名稱已在使用中」example.com)。

若要解決錯誤，請[建立資源的快照](#)。再[從快照建立新的資源](#)，並賦予該資源全新的唯一名稱。然後，刪除名稱與您要為其建立 Lightsail DNS 區域的網域相同的原始資源。

5. 選擇「建立DNS區域」。

系統會將您重新導向至「DNS區域指派」頁面，您可以在此處管理網域資源指派。使用指派將網域指向您的 Lightsail 資源，例如負載平衡器和執行個體。

### 步驟 3：將記錄新增至DNS區域

請完成以下步驟，將記錄新增至您的網域DNS區域。DNS記錄會指定網域的網際網路流量路由方式。舉例來說，您可以將頂層網域 (如 example.com) 的流量路由至一個執行個體，並將子網域 (如 blog.example.com) 的流量路由至不同的執行個體。

1. 在DNS區域指派頁面中，選擇記DNS錄標籤。

您的DNS區域會列在 [Lightsail 主控台](#) 的 DNS「網域和」索引標籤中。

#### Note

在DNS區域指派頁面上，您可以新增、移除或變更網域指向的 Lightsail 資源。您可以將網域指向 Lightsail 執行個體、分佈、容器服務、負載平衡器、靜態 IP 地址等。在DNS記錄頁面上，您可以新增、編輯或刪除網域的DNS記錄。

2. 選擇以下其中一項記錄類型：

#### 地址 (A) 記錄

A 記錄會將網域 (例如) 或子網域 (例如) 對應至 Web 伺服器或執行個體的IPv4位址，例如192.0.2.255.example.com blog.example.com

1. 在 Record name (記錄名稱) 文字方塊中，輸入該記錄的目標子網域，或輸入 @ 符號來定義網域頂點。
2. 在 Resolves to (解析為) 文字方塊中，輸入該記錄的目標 IP 地址，選取您的執行中執行個體或已設定的負載平衡器。選取執行中的執行個體時，系統即會自動新增該執行個體的公有 IP 地址。
3. 選取「是 AWS 資源別名」，將流量路由至 Lightsail 和 AWS 資源，例如散發或容器服務。您也可以將DNS區域中某個記錄的流量路由至另一筆記錄。

#### Note

建議您將靜態 IP 附加至 Lightsail 執行個體，然後選擇靜態 IP 作為記錄解析的值。如需詳細資訊，請參閱[建立靜態 IP](#)。

## AAAA記錄

AAAA記錄會將網域 (例如) 或子網域 (例如) 對應至 Web 伺服器或執行個體的IPv6位址，例如2001:0db8:85a3:0000:0000:8a2e:0370:7334. example.com blog.example.com

### Note

Lightsail 不支援靜態IPv6位址。如果您刪除 Lightsail 資源並建立新資源，或者停用並重新啟IPv6用相同資源，則可能需要更新AAAA記錄以反映資源的最新IPv6位址。

1. 在 Record name (記錄名稱) 文字方塊中，輸入該記錄的目標子網域，或輸入 @ 符號來定義網域頂點。
2. 在 [解析為] 文字方塊中，輸入記錄的目標IPv6位址、選取執行中的執行個體或已設定的負載平衡器。當您選取執行中的執行個體時，系統會自動新增該執行個體的公用IPv6位址。
3. 選取「是 AWS 資源別名」，將流量路由至 Lightsail 和 AWS 資源，例如散發或容器服務。您也可以將DNS區域中某個記錄的流量路由至另一筆記錄。

## 標準名稱 () CNAME 記錄

記CNAME錄會將別名或子網域 (例如www.example.com) 對應至其他網域，例如example.com，或其他子網域，例如。blog.example.com

1. 在 Record name (記錄名稱) 文字方塊中，輸入該記錄的子網域。
2. 在 Route traffic to (將流量路由至) 文字方塊中，輸入該記錄的目標網域或子網域。

## 郵件交換程式 (MX) 記錄

MX 記錄可將子網域 (如 mail.example.com) 對應至電子郵件伺服器地址，若同時定義多個伺服器，還能包含優先順序值。

1. 在 Record name (記錄名稱) 文字方塊中，輸入該記錄的子網域。
2. 在 Priority (優先順序) 文字方塊中，輸入該記錄的優先順序。這對於為多個伺服器新增記錄而言是很重要的。
3. 在 Route traffic to (將流量路由至) 文字方塊中，輸入該記錄的目標網域或子網域。

## 服務定位器 (SRV) 記錄

SRV記錄會將子網域 (例如) 對應至具有優先順序service.example.com、權重和連接埠號碼值的服務位址。電話語音或即時消息是一對夫婦通常與SRV記錄相關聯的服務。

2. 在 Priority (優先順序) 文字方塊中，輸入該記錄的優先順序。
3. 在「線寬」文字方塊中，為具有相同優先順序的SRV記錄輸入相對權重。
4. 在 Route traffic to (將流量路由至) 文字方塊中，輸入該記錄的目標網域或子網域。
5. 在 Port (連接埠) 文字方塊中，輸入可用於連線至服務的連接埠號碼。

### 文字 (TXT) 記錄

記TXT錄會將子網域對應至純文字。您可以建立TXT記錄，以向服務供應商確認您的網域擁有權。

1. 在 Record name (記錄名稱) 文字方塊中，輸入該記錄的子網域。
2. 在 Responds with (回應內容) 文字方塊中，輸入在子網域被查詢時所提供的文字回應。

#### Note

輸入文字不需使用引號括起來。

3. 當您完成新增記錄時，請選擇 Save (儲存) 圖示以儲存變更。

記錄即會加入至DNS區域。重複上述步驟，將多筆記錄新增至您的網域DNS區域。

#### Note

無法在 Lightsail DNS 區域中設定DNS記錄的存留時間 (TTL)。相反地，所有 Lightsail DNS 記錄的預設值為 60 秒。TTL如需詳細資訊，請參閱 Wikipedia 上的[存留時間](#)。

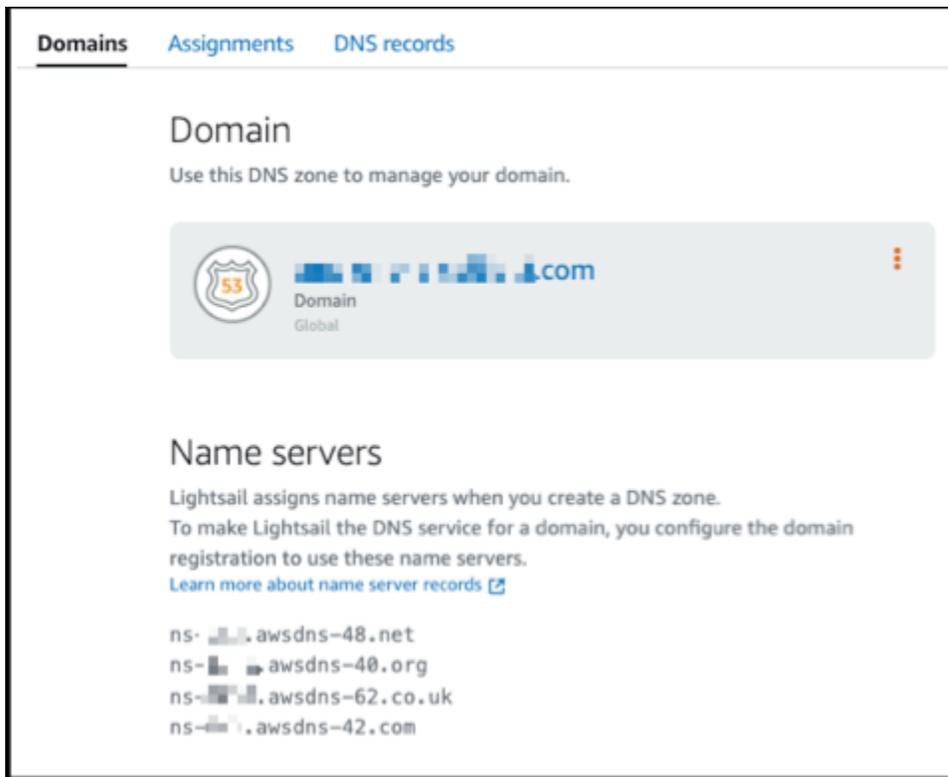
## 步驟 4：變更網域目前DNS主機供應商的名稱伺服器

請完成下列步驟，將您網域DNS記錄的管理作業移轉至 Lightsail。若要這麼做，請登入網域目前DNS主機供應商的網站，然後將網域的名稱伺服器變更為 Lightsail 名稱伺服器。

#### Important

如果網路流量目前正在路由至您的網域，請先確定 Lightsail DNS 區域中已有所有現有DNS記錄，然後再變更網域目前DNS主機供應商的名稱伺服器。這樣，在傳輸到 Lightsail DNS 區域之後，流量會持續不間斷地流動。

1. 記下網域DNS區域管理頁面上列出的 Lightsail 名稱伺服器。名稱伺服器位於 Lightsail DNS 區域的「網域」索引標籤上。



2. 登入您網域目前的DNS主機供應商網站。
3. 尋找可用於編輯您網域的名稱伺服器的頁面。

如需尋找此頁面的詳細資訊，請參閱您網域目前DNS主機供應商提供的說明文件。

4. 輸入 Lightsail 名稱伺服器，並移除列出的其他名稱伺服器。
5. 儲存您的變更。

允許一些時間讓名稱伺服器變更透過網際網路傳播DNS，這可能需要數小時。完成後，您網域的網際網路流量應該會開始透過 Lightsail DNS 區域進行路由。

## 後續步驟

- [編輯DNS區域](#)
- [建立負載平衡器並將其與執行個體附接](#)

## 編輯 Lightsail DNS 區域

編輯您網域DNS區域中的DNS記錄。如果您想要將網域DNS記錄的管理轉移到另一個DNS託管服務供應商，或傳回註冊網域的註冊商，也可以在 Amazon Lightsail 中刪除網域的DNS區域。如需詳細資訊，請參閱 [???](#)

### Note

在 Lightsail 主控台中使用編DNS輯器編輯記錄之前，您必須先將網域DNS記錄的管理移轉至 Lightsail。如需詳細資訊，請參閱[建立DNS區域以管理網域DNS記錄](#)。

## 編輯DNS記錄

您可以隨時使用 Lightsail 主控台編輯網域DNS區域的DNS記錄。

### 編輯區DNS域

1. 登入主 Lightsail 台。
2. 在 Lightsail 主控台首頁的左側導覽窗格中，選擇 [網域和 DNS]。
3. 選擇您要編輯的DNS區域名稱。
4. 在DNS區域DNS記錄頁面上，選擇您要刪除的記錄旁邊的「刪除」圖示。
5. 當您完成後，請選擇 Save (儲存) 圖示來儲存變更。

### Note

允許通過互聯網傳播DNS記錄更改的時間DNS，這可能需要幾個小時。

## 在 Lightsail 中刪除DNS區域

在某些情況下，您可能會想要完全移除在 Amazon Lightsail 中設定的DNS區域，以管理網域DNS記錄。也許您想要將DNS管理轉移給其他供應商，或者回到您的網域註冊商。刪除DNS區域是一個簡單的過程，但請務必事先規劃，以確保您的網域流量繼續正確路由。讓我們來看看在 Lightsail 中刪除DNS區域的步驟。

### Important

如果您打算繼續透過網域轉送流量，請在 Lightsail 中刪除網域DNS區域之前，先準備不同的DNS主機服務供應商。否則，當您刪除 Lightsail DNS 區域時，您網站的所有流量都會停止。

## 刪除DNS區域

1. 在 Lightsail 主控台首頁的左側導覽窗格中，選擇 [網域和 DNS]。
2. 選擇您要刪除的DNS區域名稱。
3. 選擇垂直省略符號選單 (:)。接著選擇 Delete (刪除) 選項。
4. 選擇刪除DNS區域以確認刪除。

該DNS區域會從 Lightsail 中刪除。

## 瞭解如何在 Lightsail 中將網際網路流量路由至您的網站

網際網路上的所有電腦，包括智慧型手機、筆記型電腦和網站伺服器，會使用唯一的字元字串彼此通訊。這些字串 (稱為 IP 地址) 採用下列其中一個格式：

- 網際網路通訊協定第 4 版 (IPv4) 格式，例如 192.0.2.44
- 網際網路通訊協定第 6 版 (IPv6) 格式，例如 2001:DB8::/32

當您開啟瀏覽器並移至網站時，不需要記住並輸入這麼長的字元字串。相反地，您可以輸入網域名稱 (例如 example.com)，仍然可移至預期的網站。這可透過網域名稱系統 (DNS) 來達成，該系統的作用為將註冊的網域名稱對應至 IP 地址。

### 內容

- [如何設定 Lightsail 以路由網域的網際網路流量概觀](#)
- [如何為您的網域路由流量](#)
- [後續步驟](#)

## 如何設定 Lightsail 以路由網域的網際網路流量概觀

本概述說明如何使用 Lightsail 註冊和設定將網際網路流量路由到您的網站或 Web 應用程式的網域。

1. 註冊您的網域名稱。如需概觀，請參閱[域註冊](#)。
2. 註冊網域名稱後，Lightsail 會自動建立與網域名稱相同的 DNS 區域。
3. Lightsail 主控台可讓您輕鬆地將網域指派給 Lightsail 資源，例如執行個體或負載平衡器。您也可以在此 DNS 區域中建立 DNS 記錄，將流量路由到您的資源。每個記錄包含有關您希望如何路由網域流量的資訊，例如：

### 名稱

記錄名稱對應於網域名稱 (example.com) 或子網域名稱 (www.example.com、retail.example.com)。DNS 區域中每個記錄的名稱必須以 DNS 區域名稱結尾。例如，如果 DNS 區域的名稱是 example.com，所有記錄名稱都必須以 example.com 結尾。

### 類型

記錄類型通常取決於您希望流量路由到的資源類型。例如，若要將流量路由到電子郵件伺服器，請將 Type (類型) 指定為 MX。若要將網域名稱的流量路由至 Lightsail 執行個體，請新增 A 記錄，將網域名稱指向執行個體的靜態 IPv4 位址，或是指向執行個體 IPv6 位址的 AAAA 記錄。

## 4. 目標

目標是您要將流量路由到的位置。您可以建立別名記錄，將流量路由至 Lightsail 執行個體、Lightsail 容器服務及其他 Lightsail 資源。如需更多詳細資訊，請參閱[DNS](#)。

## 如何為您的網域路由流量

設定 Lightsail 將網際網路流量路由至您的資源 (例如執行個體、負載平衡器、分發或容器服務) 之後，當有人要求 www.example.com 的內容時，會發生以下情況。

1. 使用者開啟 Web 瀏覽器並在網址列中輸入 www.example.com，然後按 Enter。
2. 對 www.example.com 的請求路由到 DNS 解析程式，該解析程式通常由使用者的網際網路服務供應商 (ISP) 管理。ISP 可以是有線網際網路供應商、DSL 寬頻供應商或公司網路。
3. ISP 的 DNS 解析程式將對 www.example.com 的請求轉送到 DNS 根名稱伺服器。
4. DNS 解析程式再次轉送對 www.example.com 的請求，這次轉送到 .com 網域的其中一個 TLD 名稱伺服器。 .com 網域的名稱伺服器，使用與 example.com 網域關聯的四個名稱伺服器的名稱來回應該請求。

DNS 解析程式快取 (存放) 四個名稱伺服器。下次有人瀏覽 example.com，解析程式會略過步驟 3 和 4，因為它已有 example.com 的名稱伺服器。名稱伺服器通常會快取兩天。

5. DNS 解析程式會選擇名稱伺服器，並將對 `www.example.com` 的請求轉送至該名稱伺服器。
6. 名稱伺服器在 `example.com` DNS 區域中尋找 `www.example.com` 記錄，並取得關聯值，例如 Web 伺服器的 IP 地址 (`192.0.2.44`)。接著，名稱伺服器會將該 IP 地址傳回 DNS 解析程式。
7. DNS 解析程式最終取得使用者所需的 IP 地址。解析程式將該值傳回給 Web 瀏覽器。
8. Web 瀏覽器將對 `www.example.com` 的請求，傳送至它從 DNS 解析程式取得的 IP 地址。這是您的內容所在的位置，例如，在 Lightsail 執行個體或設定為網站端點的容器服務上執行的 Web 伺服器。
9. `192.0.2.44` 的 Web 伺服器或其他資源，將 `www.example.com` 的網頁傳回到 Web 瀏覽器，而 Web 瀏覽器會顯示該頁面。

## 後續步驟

- [DNS](#)
- [將域指向執行個體](#)
- [將域指向負載平衡器](#)
- [將域指向分發](#)

## 將網域流量路由至 Lightsail 執行個體

您可以使用 Amazon Lightsail 中的 DNS 區域，將已註冊的網域名稱 (例如 `.com`) 指向在 Lightsail 執行個體 (也稱為虛擬私人伺服器 (VPS) 上執行的網站。您最多可以在您的帳戶中建立六個 DNS 區域。並非支援所有 DNS 記錄類型。如需有關 DNS 區域 Lightsail 細資訊，請參閱 [DNS](#)。

如果您希望建立六個以上的 DNS 區域，或使用 Lightsail 不支援的 DNS 記錄類型，建議您使用 Amazon Route 53 託管區域。使用 Route 53，您可以為多達 500 個域管理 DNS。這還支援更多種 DNS 記錄類型。如需詳細資訊，請參閱 Amazon Route 53 開發人員指南中的 [使用託管區域](#)。

本指南說明如何編輯在 Lightsail 中管理之網域的 DNS 記錄，以便它指向您的 Lightsail 執行個體。允許最多 48 小時，透過網際網路 DNS 傳播 DNS 區域變更。

### 先決條件

請先完成事前準備 (若尚未完成)：

- 使用註冊網域 Lightsail。如需詳細資訊，請參閱 [註冊新域](#)。
- 如果您已註冊網域，但並未使用 Lightsail 來管理其記錄，則必須將網域 DNS 記錄的管理轉移至 Lightsail。如需詳細資訊，請參閱 [建立 DNS 區域以管理域的 DNS 記錄](#)。

- 每當您停止並重新啟動執行個體時，連接至 Lightsail 執行個體的預設動態公用 IP 位址都會變更。建立靜態 IP 並將其連接到執行個體，以防止公有 IP 地址變更。在本指南中，您會在解析至靜態 IP 地址的網域 DNS 區域中，建立 DNS 記錄，這樣您就不必在每次停止和重新啟動執行個體時，更新網域的 DNS 記錄。如需詳細資訊，請參閱[建立靜態 IP 並將其附接至執行個體](#)。

選用 — 您可以讓您的 Lightsail 執行個體保持啟用 IPv6 功能。在您停止和啟動執行個體時，系統會持續保留 IPv6 地址。如需詳細資訊，請參閱[啟用和停用 IPv6](#)。

## 將網域指派 Lightsail 體

使用下列其中一種方法，將網域指派給 Lightsail 中的實體：

- [執行個體 Domains \(網域\) 索引標籤](#)
- [靜態 IP Domains \(網域\) 索引標籤](#)
- [DNS 區域 Assignments \(指派\) 索引標籤](#)

## 執行個體 Domains (網域) 索引標籤

請完成下列程序，將您的網域指派給 Lightsail 主控台的執行個體網域索引標籤中的 Lightsail 執行個體。

使用執行個體 Domains (網域) 索引標籤指派網域

1. 登入主 [Lightsail 台](#)。
2. 選擇您要將網域指派給的執行個體名稱。
3. 選擇 Domains (網域) 索引標籤中的 Assign domain (指派網域)。
4. 選取您要指派給 Lightsail 實體的網域。
5. 確認路由資訊正確無誤，然後選擇 Assign (指派)。

## 選用

若要從執行個體中編輯或移除網域指派，請選擇網域名稱旁的編輯圖示或垃圾桶圖示。

## 靜態 IP Domains (網域) 索引標籤

請完成下列程序，將您的網域指派給 Lightsail 主控台的靜態 IP 網域索引標籤中的 Lightsail 執行個體。

若要使用靜態 IP Domains (網域) 索引標籤指派網域

1. 登入主 [Lightsail 台](#)。
2. 選擇 Networking (網路) 索引標籤。
3. 選擇您要將網域指派至的靜態 IP。
4. 選擇 Domains (網域) 索引標籤中的 Assign domain (指派網域)。
5. 選取要指派給靜態 IP 的網域。
6. 確認路由資訊正確無誤，然後選擇 Assign (指派)。

## 選用

若要從靜態 IP 中編輯或移除網域指派，請選擇網域名稱旁的編輯圖示或垃圾桶圖示。

## DNS 區域 Assignments (指派) 索引標籤

完成下列程序，即可在 DNS 區域的 [指派] 索引標籤中將您的網域指派給 Lightsail 執行個體。

若要使用 Assignments (指派) 索引標籤指派網域

1. 登入主 [Lightsail 台](#)。
2. 選擇 Domains & DNS (網域和 DNS) 索引標籤。
3. 為要使用的網域名稱選擇 DNS 區域。
4. 選擇 Assignments (指派) 索引標籤中的 Add assignment (新增指派)。
5. 選取您要指派給 Lightsail 實體的網域名稱。如果尚未將靜態 IP 連接至執行個體，系統會提示您連接一個靜態 IP。
6. 確認路由資訊正確無誤，然後選擇 Assign (指派)。

## 選用

若要從資源中編輯或移除網域指派，請選擇網域名稱旁的編輯圖示或垃圾桶圖示。

## 將您的網域指向 Lightsail 負載平衡器

[確認您控制要加密 \(HTTPS\) 流量的網域之後，您需要將位址 \(A\) 記錄新增至網域的 DNS 主控供應商](#)，以將您的網域指向 Lightsail 負載平衡器。在本指南中，我們將向您展示如何將 A 記錄添加到 Lightsail DNS 區域和 Amazon Route 53 託管區域。

## 使用 DNS 區域 - 指派頁面新增 A 記錄

1. 在首頁 Lightsail，選擇網域和 DNS。

2. 選擇您要管理的 DNS 區域。
3. 選擇指派索引標籤。
4. 選擇 Add assignment (新增指派)。
5. 在選取網域名稱欄位中，選擇是否使用網域名稱或網域的子網域。
6. 在選取資源下拉式清單中，選取要指派網域的負載平衡器。
7. 選擇 Assign (指派)。

請等待變更透過網際網路 DNS 進行傳播。這可能需要幾分鐘到幾小時不等。

## 使用 DNS 區域 - DNS 記錄頁面新增 A 記錄

1. 在首頁 Lightsail，選擇網域和 DNS。
2. 選擇您要管理的 DNS 區域。
3. 選擇 DNS records (DNS 記錄) 索引標籤。
4. 根據您 DNS 區域的目前狀態，完成下列其中一個步驟：
  - 如果您尚未新增 A 記錄，請選擇 Add record (新增記錄)。
  - 如果您先前已新增 A 記錄，請選擇頁面上列出的現有 A 記錄旁的編輯圖示，然後跳到此程序的步驟 5。
5. 在 Record type (記錄類型) 下拉式選單中選擇 A record (A 記錄)。
6. 在 Record name (記錄名稱) 文字方塊中，輸入下列任一選項：
  - 輸入 @ 以將網域 (例如 example.com) 的 apex 的流量路由至負載平衡器。
  - 輸入 www 以將 www subdomain (例如 www.example.com) 的流量路由至負載平衡器。
7. 在「解析為」文字方塊中，選擇 Lightsail 負載平衡器的名稱。
8. 選擇 Save (儲存) 圖示。

請等待變更透過網際網路 DNS 進行傳播。這可能需要幾分鐘到幾小時不等。

## 在 Route 53 中新增 A 記錄

1. 登入 [Route 53 主控台](#)。
2. 在導覽窗格中，選擇 Hosted zones (託管區域)。
3. 選擇您希望用來將流量路由至負載平衡器的網域名稱的託管區域。

#### 4. 選擇建立記錄。

Quick create record (快速建立記錄) 頁面隨即出現。

Route 53 > Hosted zones > example.com > Create record

Quick create record [Info](#) [Switch to wizard](#) [Add another record](#)

▼ Record 1 [Delete](#)

Record name [Info](#) Record type [Info](#) Value [Info](#)  Alias

example.com

Valid characters: a-z, 0-9, ! \* # \$ % & ' ( ) + , - / : ; < = > ? @ [ \ ] ^ \_ ` { } . ~

Enter multiple values on separate lines.

TTL (seconds) [Info](#) Routing policy [Info](#)

Recommended values: 60 to 172800 (two days)

[Cancel](#) [Create records](#)

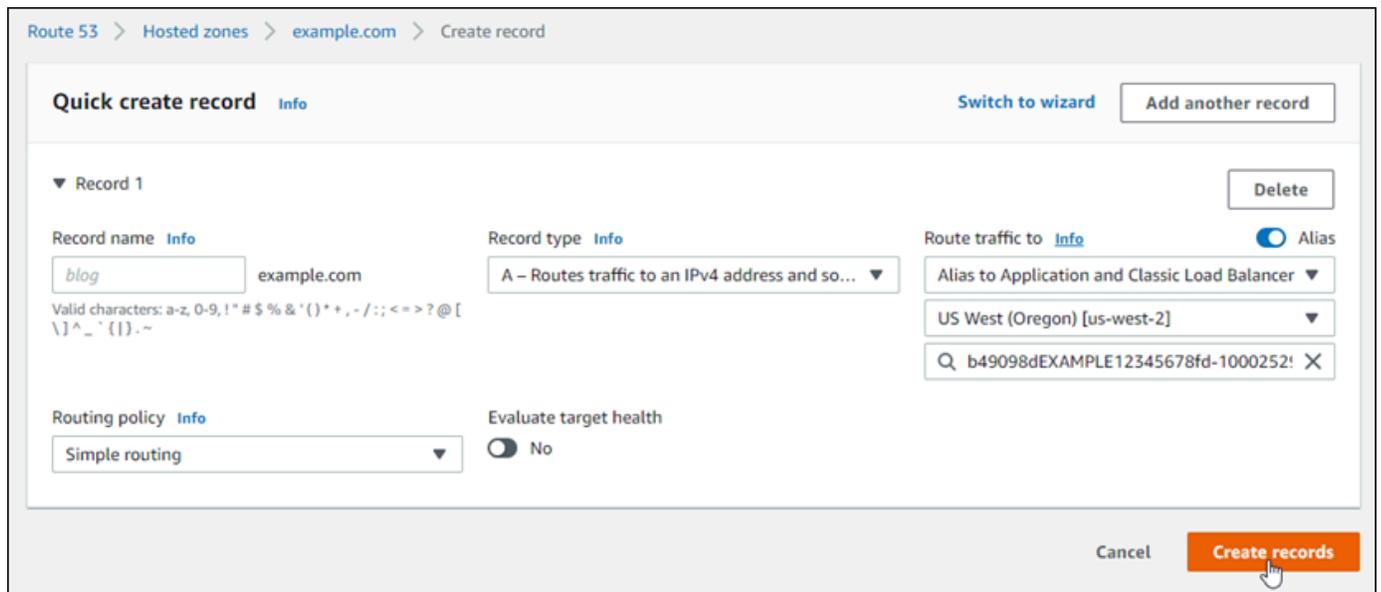
#### Note

如果您看到 Choose routing policy (選擇路由政策) 頁面，則選擇 Switch to quick create (切換至快速建立)，以切換至快速建立精靈，然後再繼續執行下列步驟。

- 針對 Record name (記錄名稱)，如果您計劃使用 www 子網域 (即 www.example.com)，請鍵入 www，或者如果您計劃使用網域 (即 example.com) 的 apex，請將其留為空白。
- 針對 Record type (記錄類型)，選擇 A - Routes traffic to an IPv4 address and some AWS resources (A – 將流量路由至 IPv4 地址和某些 AWS 資源)。
- 選擇 Alias (別名) 切換開關，以啟用別名記錄。
- 選擇下列 Route traffic to (將流量路由至) 的選項：
  - 針對 Choose endpoint (選擇端點)，請選擇 Alias to Application and Classic Load Balancer (應用程式和 Classic Load Balancer 的別名)。
  - 在「選擇區域」中，選擇您在其中建立 Lightsail 負載平衡器的 AWS 區域。
  - 在「選擇負載平衡器」中，輸入或貼上 Lightsail 負載平衡器的端點 URL (即 DNS 名稱)。
- 針對 (路由政策)，請選擇 Simple routing (簡便路由)，並停用 Evaluate target health (評估目標運作狀態) 切換開關。

Lightsail 已經在您的負載平衡器上執行健康狀態檢查。如需詳細資訊，請參閱[負載平衡器的運作狀態檢查](#)。

您的記錄看起來應該如下列範例所示。



The screenshot shows the 'Create record' interface in the Amazon Lightsail console. The breadcrumb navigation is 'Route 53 > Hosted zones > example.com > Create record'. The main heading is 'Quick create record' with an 'Info' link. There are two buttons: 'Switch to wizard' and 'Add another record'. Below this is a section for 'Record 1' with a 'Delete' button. The form fields include: 'Record name' (value: 'blog', domain: 'example.com'), 'Record type' (value: 'A - Routes traffic to an IPv4 address and so...'), 'Route traffic to' (value: 'Alias', sub-value: 'Alias to Application and Classic Load Balancer'), 'US West (Oregon) [us-west-2]', and a target ID 'b49098dEXAMPLE12345678fd-1000252!'. There are also 'Routing policy' (value: 'Simple routing') and 'Evaluate target health' (value: 'No') options. At the bottom right, there are 'Cancel' and 'Create records' buttons.

10. 選擇 Create records (建立記錄) 以新增記錄到您的託管區域。

#### Note

請等待變更透過網際網路 DNS 進行傳播。這可能需要幾分鐘到幾小時不等。

## 為您的網域轉移 DNS 管理

您可以使用 Amazon Lightsail DNS 區域來管理您使用 Lightsail 註冊之網域的 DNS 記錄。或者，如果您願意，也可以將網域的 DNS 記錄管理作業轉移到其他 DNS 託管供應商。在本指南中，我們將說明如何將您在 Lightsail 註冊之網域的 DNS 記錄管理轉移給其他 DNS 主機供應商。

#### Important

您對網域的 DNS 所做的任何變更，可能需要幾個小時才能透過網際網路的 DNS 傳播。因此，您應該在完成轉移管理作業前，將網域的 DNS 記錄保存在目前 DNS 託管供應商處。這可確保網域的流量在轉移過程中可持續不間斷地路由到您的資源。

## 內容

- [完成先決條件](#)
- [新增記錄至 DNS 區域](#)

## 完成先決條件

請先完成事前準備 (若尚未完成)：

1. 註冊一個網域名稱。您可以使用 Lightsail 註冊網域名稱。如需詳細資訊，請參閱[註冊新域](#)。
2. 使用由 DNS 服務提供的程序，取得網域的名稱伺服器。

## 新增記錄至 DNS 區域

請完成下列程序，將其他 DNS 主機提供者的名稱伺服器新增至您在 Lightsail 中註冊的網域。

1. 登入主 [Lightsail 台](#)。
2. 選擇 Domains & DNS (網域和 DNS) 索引標籤。
3. 選擇您要設定為使用其他 DNS 服務的網域的名稱。
4. 選擇 Edit Name Servers (編輯名稱伺服器)。
5. 將名稱伺服器的名稱，變更為您在完成先決條件時，從 DNS 服務獲得的名稱伺服器。
6. 選擇 Save (儲存)。

## 使用 Amazon Route 53 將網域指向您的 Lightsail 執行個體

Amazon Lightsail 中的 DNS 區域可讓您輕鬆地將已註冊的網域名稱 (例如example.com) 指向在 Lightsail 執行個體上執行的網站。您最多可以建立六個 Lightsail DNS 區域，但並非所有 DNS 記錄類型都受到支援。如需有關 DNS 區域 Lightsail 細資訊，請參閱 [DNS](#)。

如果 Lightsail DNS 區域對您來說太受限，我們建議您使用 Amazon Route 53 託管區域來管理您網域的 DNS 記錄。您可以使用 Route 53 來管理高達 500 個域的 DNS，而且其也支援更多種的 DNS 記錄類型。或者，您可能已經在使用 Route 53 管理域的 DNS 記錄，且希望繼續沿用。本指南說明如何編輯 Route 53 中管理之網域的 DNS 記錄，以指向您的 Lightsail 執行個體。

## 必要條件

請先完成事前準備 (若尚未完成)：

- 使用 Route 53 註冊域名稱。如需詳細資訊，請參閱 Route 53 文件中的[註冊新域](#)。
- 如果您已經註冊域但並未使用 Route 53 管理其記錄，則您必須為指向至 Route 53 的域傳輸 DNS 管理記錄。如需詳細資訊，請參閱 Route 53 文件中的[將 Amazon Route 53 設定為現有域的 DNS 服務](#)。
- 為 Route 53 中的域建立公有託管區域。如需詳細資訊，請參閱 Route 53 文件中的[建立公有託管區域](#)。
- 建立靜態 IP 並將其附加至您的 Lightsail 執行個體。在本指南中，將在域的 Route 53 託管區域中建立 DNS 記錄，它會解析為執行個體的靜態 IP 地址 (公有 IP 地址)。如需詳細資訊，請參閱[建立靜態 IP 並將其附接至執行個體](#)。

## 使用 Route 53 將網域指向 Lightsail 實體

完成下列步驟，在 Route 53 中設定兩個最常見的 DNS 記錄、位址和標準名稱，以將您的網域指向 Lightsail 執行個體。

### Note

《Route 53 開發人員指南》中也記錄了此程序。如需詳細資訊，請參閱 Route 53 文件中的[使用 Amazon Route 53 主控台建立記錄](#)。

1. 登入 [Route 53 主控台](#)。
2. 在導覽窗格中，選擇 Hosted zones (託管區域)。
3. 選擇您希望用來將流量路由至負載平衡器的網域名稱的託管區域。
4. 選擇建立記錄。

Quick create record (快速建立記錄) 頁面隨即出現。

Route 53 > Hosted zones > example.com > Create record

Quick create record [Info](#) [Switch to wizard](#) [Add another record](#)

▼ Record 1 [Delete](#)

Record name [Info](#) Record type [Info](#) Value [Info](#)  Alias

blog example.com A - Routes traffic to an IPv4 address and so... 192.0.2.235

Valid characters: a-z, 0-9, !\*# \$% & '()\*+,-./:;<=>?@[ \ ] ^ \_ ` { } . ~

TTL (seconds) [Info](#) Routing policy [Info](#)

300 Simple routing

1m 1h 1d

Recommended values: 60 to 172800 (two days)

Cancel [Create records](#)

**Note**

如果您看到 Choose routing policy (選擇路由政策) 頁面，則選擇 Switch to quick create (切換至快速建立)，以切換至快速建立精靈，然後再繼續執行下列步驟。

**5. 針對 Record type (記錄類型)，選擇以下其中一個選項：****A - 將流量路由至 IPv4 地址和某些 AWS 資源**

地址 (A) 記錄可將網域 (例如 example.com) 或子網域 (例如 blog.example.com) 映射至 web 伺服器的 IP 地址，例如 192.0.2.255。

1. 將 Record name (記錄名稱) 文字方塊保留空白，以將網域的頂點 (例如 example.com) 指向某個 IP 地址，或輸入子網域。
2. 在 Record type (記錄類型) 下拉式選單中，選擇 A - Routes traffic to an IPv4 address and some AWS resources (A - 將流量路由至 IPv4 地址和某些 AWS 資源)。
3. 在 [值] 文字方塊中輸入 Lightsail 執行個體的靜態 IP 位址 (公用 IP 位址)。
4. 將 TTL 保持為 300，路由政策保持為 Simple routing (簡易路由)。

Route 53 > Hosted zones > example.com > Create record

Quick create record [Info](#) [Switch to wizard](#) [Add another record](#)

▼ Record 1 [Delete](#)

Record name [Info](#)  example.com Record type [Info](#)  Value [Info](#)   Alias

Valid characters: a-z, 0-9, !\*#\$%&'()\*+,-./:;<=>?@[ \]^\_`{|}~  
Enter multiple values on separate lines.

TTL (seconds) [Info](#)  Routing policy [Info](#)

Recommended values: 60 to 172800 (two days)

[Cancel](#) [Create records](#)

## CNAME - 將流量路由至其他網域名稱和某些 AWS 資源

正式名稱 (CNAME) 記錄會映射別名或子網域 (例如 `www.example.com`) 至一個網域 (例如 `example.com`) 或子網域 (例如 `www2.example.com`)。CNAME 記錄會將一個網域重新引導到另一個。

1. 在 Record name (記錄名稱) 文字方塊中輸入子網域。
2. 在 Record type (記錄類型) 下拉式選單中，選擇 CNAME - Routes traffic to another domain name and to some AWS resources (CNAME - 將流量路由至其他網域名稱和某些 AWS 資源)。
3. 在 Value (值) 文字方塊中輸入網域 (即 `example.com`) 或子網域 (即 `another.example.com`)。
4. 將 TTL 保持為 300，路由政策保持為 Simple routing (簡易路由)。

Route 53 > Hosted zones > example.com > Create record

Quick create record [Info](#) [Switch to wizard](#) [Add another record](#)

▼ Record 1 [Delete](#)

Record name [Info](#)  example.com Record type [Info](#)  Value [Info](#)   Alias

Valid characters: a-z, 0-9, ! \* # \$ % & ' ( ) \* + , - / : ; < = > ? @ [ \ ] ^ \_ ` { } . ~  
Enter multiple values on separate lines.

TTL (seconds) [Info](#)  Routing policy [Info](#)

Recommended values: 60 to 172800 (two days)

[Cancel](#) [Create records](#)

6. 選擇 Create records (建立記錄) 以新增記錄到您的託管區域。

#### Note

請等待變更透過網際網路 DNS 進行傳播。這可能需要幾分鐘到幾小時不等。

若要編輯 Route 53 託管區域中的現有記錄集，請選擇要編輯的記錄、輸入您的變更，然後選擇儲存。

## 註冊網域

您可以使用 Amazon Lightsail 註冊新域。Lightsail 網域是透過 Amazon Route 53 註冊的，這是一種高度可用且可擴展的 DNS 網路服務。如果您擁有向其他供應商註冊的網域，則可以將這些網域的 DNS 管理轉移至 Lightsail。您也可以將這些網域指向您的 Lightsail 資源。

選擇下列其中一個程序，在 Lightsail 註冊新網域：

- 如需註冊新網域，請參閱[使用 Lightsail 註冊新網域](#)。
- 若為現有域，請參閱[建立 DNS 區域以管理域的 DNS 記錄](#)。
- 如需將網域移至其他註冊商，請參閱[在 Amazon Route 53 中管理 Lightsail 網域](#)。

開始前，請注意下列網域註冊注意事項：

## 網域註冊定價

如需註冊域的費用資訊，請參閱 [Amazon Route 53 定價指南](#)。

## 網域服務配額

您可以註冊的網域數量有上限。如需詳細資訊，請參閱《Amazon Route 53 開發人員指南》中的 [服務配額](#)。如果您想要提高上限，請聯絡 Route 53。

## 支援的網域

Lightsail 支援所有通用頂層網域 (TLD) 的註冊。如需受支援的 TLD 清單，請參閱《Amazon Route 53 開發人員指南》中的 [可在 Amazon Route 53 中註冊的域](#)。

必須使用 Route 53 來註冊地理頂層域。如需詳細資訊，請參閱《Amazon Route 53 開發人員指南》中的 [地理頂層域](#)。

註冊後無法變更網域名稱。

如果您不慎註冊了錯誤的網域名稱，將無法變更。反之，您必須註冊另一個網域名稱，並指定正確的名稱。意外註冊的網域名稱不予退款。

## DNS 區域的費用

當您向 Lightsail 註冊網域時，我們會自動為該網域建立 DNS 區域。Lightsail 不會對 DNS 區域收取任何費用。

## 使用註冊新網域

### 內容

- [完成先決條件](#)
- [註冊新的網域](#)
- [驗證網域聯絡人資訊](#)

## 完成先決條件

請先完成事前準備 (若尚未完成)：

1. 確認您網域的必要 DNS 記錄類型受 Lightsail 支援。Lightsail DNS 區域目前支援位址 (A)、標準名稱 (CNAME)、郵件交換器 (MX)、名稱伺服器 (NS)、服務定位器 (SRV) 和文字 (TXT) 記錄類型。處理 NS 記錄時，您可以使用萬用字元 DNS 記錄項目。

如果 Lightsail DNS 區域不支援您網域所需的 DNS 記錄類型，您可以使用 Route 53 作為網域的 DNS 代管服務供應商。Route 53 支援更多記錄類型。如需詳細資訊，請參閱《Amazon Route 53 開發人員指南》中的[支援的 DNS 記錄類型](#)和[將 Amazon Route 53 設定為現有域的 DNS 服務](#)。

## 註冊新的網域

若要註冊新的網域

1. 登入主 [Lightsail 台](#)。
2. 選擇 Domains & DNS (網域和 DNS) 索引標籤。
3. 選擇 Register Domain (註冊網域)，並指定您想註冊的網域。
  - a. 輸入要註冊的網域名稱，然後選擇 Check availability (檢查可用性)，了解該網域名稱是否可用。如果網域可用，請繼續前往 Automatic domain renewal (自動網域續約)。
  - b. 如果網域名稱不可用，您會看到建議您註冊的其他網域清單，而不是首選網域，或者首選網域之外的其他網域。針對您想註冊的網域，選擇 Select (選取)。
4. 選擇是否要在過期日期之前自動續約您的網域註冊。註冊網域名稱時，您預設擁有該網域名稱一年。如果您沒有續約網域名稱註冊，該註冊會過期，其他人就可註冊該網域名稱。若要確保保留您的網域名稱，您可以選擇每年自動續約網域名稱，或選取較長期限。
5. 在 Domain contact information (網域聯絡人資訊) 區段中，輸入網域註冊者、管理員和技術聯絡人的聯絡資訊。如需詳細資訊，請參閱[註冊或轉移網域時所指定的值](#)。

請注意下列注意事項：

### 名字和姓氏

針對 First Name (名字) 和 Last Name (姓氏)，建議您指定官方證件上的姓名。對於網域設定的某些變更，有些網域註冊機構要求您提供身分證明。您的 ID 的姓名必須與該網域的註冊聯絡人的姓名相符。

### 不同的聯絡人

在預設情況下，我們對所有三個聯絡人使用相同的資訊。如果您想為一或多個聯絡人輸入不同的資訊，請取消勾選 Same as registrant (與註冊者相同) 核取方塊，然後輸入新的聯絡人資訊。

6. 在 Privacy protection (隱私權保護) 區段中，選擇是否要在 WHOIS 查詢中隱藏您的聯絡人資訊。

如需詳細資訊，請參閱下列主題：

- [隱私權保護](#)

- [可向 Amazon Route 53 註冊的域](#)
7. 選擇 Register domain (註冊網域) 以繼續操作。DNS zones (DNS 區域) 和 Summary (摘要) 區段會顯示網域的 DNS 區域、定價和續約排程相關資訊。
  8. 必須先接受 [Amazon Route 53 域名稱註冊合約](#)，才能註冊域。

## 驗證網域聯絡人資訊

註冊網域後，您必須驗證註冊聯絡人的電子郵件地址有效。

我們會自動從下列其中一個電子郵件地址，傳送驗證電子郵件：

noreply@registrar.amazon.com

註冊商為 Amazon Registrar 的網域

noreply@domainnameverification.net

註冊商為我們註冊商合作夥伴 Gandi 的網域。若要判斷適合 TLD 的註冊商，請參閱《Amazon Route 53 開發人員指南》中的 [可向 Amazon Route 53 註冊的域](#)。

請使用下列程序，完成網域驗證流程。

### 若要完成網域驗證

1. 當您收到驗證電子郵件，選擇電子郵件中用於確認電子郵件地址是否有效的連結。如果您沒有立即收到電子郵件，請檢查您的垃圾電子郵件資料夾。
2. 返回 Lightsail 台。如果狀態未自動更新為 Verified (已驗證)，請選擇 Refresh status (重新整理狀態)。

#### Important

註冊聯絡人必須按照電子郵件中的指示來驗證已收到電子郵件，否則我們會按照 ICANN 的要求暫停該網域。當網域已暫停，無法在網際網路上存取該網域。

3. 網域註冊完成後，請選擇要使用 Lightsail 做為您的 DNS 服務，還是使用不同的 DNS 服務。

- Lightsail

在 Lightsail 註冊網域時建立的 DNS 區域中，建立記錄，告知 Lightsail 您希望如何路由網域和子網域的流量。

例如，當有人在瀏覽器中輸入您的網域名稱，並將該查詢轉寄給 Lightsail 時，您是否希望 Lightsail 以 Web 伺服器的 IP 位址或負載平衡器的名稱回應查詢？如需詳細資訊，請參閱[編輯或刪除 DNS 區域](#)。

- 使用其他 DNS 服務

將您的新網域設定為將 DNS 查詢路由傳送至 Lightsail 以外的 DNS 服務。如需詳細資訊，請參閱[在您要使用其他 DNS 服務時更新網域的名稱伺服器](#)。

## 檢視已向 Amazon 註冊商註冊之網域的註冊詳細資訊

您可以查看有關使用 Amazon Lightsail 和亞馬遜 Amazon Route 53 註冊的 .com，.net 和 .org 域的信息，亞馬遜註冊商是註冊商。此資訊包括網域最初註冊時間的詳細資訊，以及網域擁有者以及技術和管理聯絡人的聯絡資訊。

注意下列事項：

在啟用隱私權保護時傳送電子郵件給域聯絡人

如果已為網域啟用隱私權保護，註冊者、技術和管理聯絡人的聯絡資訊，會更換為 Amazon Registrar 隱私權服務的聯絡資訊。例如，如果 example.com 網域已向 Amazon 註冊商註冊，且隱私權保護處於作用中狀態，則在回應 WHOIS 查詢時，註冊人電子郵件的值會類似於。owner1234@example.com.whoisprivacyservice.org

若要在啟用隱私權保護時聯絡一或多位網域聯絡人，請傳送電子郵件到相應的電子郵件地址。我們會自動將您的電子郵件轉寄給適用的聯絡人。

檢舉濫用情況

若要舉報任何非法活動或違反合理[使用政策](#)的行為，包括不適當的內容、網路釣魚、惡意軟體或垃圾郵件，請傳送電子郵件至 trustandsafety@support.aws.com。

檢視已向 Amazon Registrar 註冊之網域的相關資訊

1. 在 Web 瀏覽器中，前往下列其中一個網站。兩個網站都會顯示相同資訊。但它們使用不同的通訊協定，並以不同的格式顯示資訊：
  - WHOIS: <https://registrar.amazon.com/whois>
  - RDAP: <https://registrar.amazon.com/rdap>
2. 請輸入您要檢視相關資訊的網域名稱，然後選擇 Search (搜尋)。如果您搜尋的網域並未使用 Amazon Lightsail 或 Route 53 註冊，您會看到一則訊息，指出該網域不在註冊商資料庫中。

# 格式化網域 Lightsail

若要協助使用者存取網站或應用程式，請選擇容易記住的網域名稱。網域名稱 (以及 DNS 區域名稱和記錄) 是由一系列以句點 (.) 分隔的標籤所組成。命名要求取決於您是註冊網域名稱，還是指定 DNS 區域或記錄的名稱。

根據以下準則，設定您網域名稱的格式。

## 內容

- [格式化域名稱註冊的域名稱](#)
- [格式化 DNS 區域和記錄的域名稱](#)
- [在 DNS 區域和記錄的名稱中使用星號 \(\\*\)](#)
- [後續步驟](#)

## 格式化域名稱註冊的域名稱

若為網域名稱註冊，您的網域名稱必須有 1 到 255 個字元。網域名稱的有效字元包括 (a-z)、(A-Z)、(0-9)、連字號 (-) 和句點 (.)。

不能在域名稱的開頭或結尾使用空格或連字號。Lightsail 支援任何有效的通用頂層網域 (TLD) 名稱。如需詳細資訊，請參閱《Amazon Route 53 開發人員指南》中的[一般頂層域](#)。

## 格式化 DNS 區域和記錄的域名稱

若為 DNS 區域和記錄，網域名稱必須有 1 到 255 個字元。網域名稱的有效字元包括 (a-z)、(A-Z)、(0-9)、連字號 (-) 和句點 (.)。您不能使用空格。

Lightsail 會將字母字元儲存為小寫字母 (a-z)，即使您將字母指定為大寫字母 (A-Z) 也一樣。

Lightsail 同時支援一般和地理頂級域名的 DNS 區域。如需地理 TLD 的更多範例，請參閱《Amazon Route 53 開發人員指南》中的[地理頂層域](#)。

## 在 DNS 區域和記錄的名稱中使用星號 (\*)

DNS 會根據星號出現在名稱中的位置，將星號 (\*) 字元視為萬用字元。萬用字元 DNS 記錄是回應您尚未定義之子網域 DNS 請求的記錄。在 Lightsail 中，您可以在下列情況下建立名稱中包含星號 (\*) 的 DNS 區域和記錄：

## DNS 區域

- 域名稱最左邊的標籤中不可包含星號 (\*)。例如，您不能使用 `subdomain*.example.com`。
- 如果您在其他位置包含星號 (\*)，DNS 會將它視為 ASCII 42 字元，而不是萬用字元。如需 ASCII 字元的詳細資訊，請參閱 Wikipedia 中的 [ASCII](#)。

## DNS 記錄

請注意下列在 DNS 記錄名稱中使用星號 (\*) 作為萬用字元的限制：

- 星號作為萬用字元，必須取代網域名稱最左邊的標籤，例如 `*.example.com` 或 `*.acme.example.com`。如果您在任何其他位置包含星號 (例如 `prod*.example.com`)，則 DNS 會將其視為 ASCII 42 字元，而不是萬用字元。
- 星號必須取代整個標籤。例如，您無法指定 `*prod.example.com` 或 `prod*.example.com`。
- 特定網域名稱具有高優先順序。例如，如果您建立 `*.example.com` 和 `acme.example.com` 的記錄，會使用 `acme.example.com` 記錄中的值，回應 `acme.example.com` 的 DNS 查詢。
- 星號適用於包含星號之子網域層級的 DNS 查詢，以及該子網域的所有子網域。舉例來說，如果您建立名為 `*.example.com` 的記錄，`*.example.com` 的 DNS 查詢會回應下列項目：

`zenith.example.com`

`acme.zenith.example.com`

`pinnacle.acme.zenith.example.com` (如果沒有該 DNS 區域任何類型的記錄)

如果您建立名為 `*.example.com` 的記錄，但沒有範例 `.com` 記錄，則 Lightsail 會針對範例網域 (不存在的網域) 回應 DNS 查詢。NXDOMAIN

您可以將 Lightsail 設定為針對相同層級以及網域名稱的所有子網域，傳回相同的 DNS 查詢回應。例如，您可以將 Lightsail 設定為回應 DNS 查詢，例如使用例子記錄來回應例子。執行下列步驟，將子網域的流量路由至 `example.com` 頂層網域：

1. 建立網域的記錄，例如 `example.com`。
2. 建立子網域的別名記錄，例如 `*.example.com`。指定您在上一步建立的記錄，作為別名記錄的目標。

## 後續步驟

如需詳細資訊，請參閱下列主題：

- [建立 DNS 區域以管理域的 DNS 記錄](#)
- [DNS](#)

## 使用進階 Route 53 功能管理網域

Amazon Lightsail 通過 Amazon Route 53 註冊域，這是一種高可用性和可擴展的 DNS 網絡服務。當您使用 Lightsail 註冊網域時，您可以在 Lightsail 和 Route 53 中管理網域。

例如註冊網域，以及將網域的流量路由至 Lightsail 資源等工作，都可以在 Lightsail 主控台中完成。如需詳細資訊，請參閱[網域註 Amazon Lightsail](#)。

轉移域和刪除註冊等進階任務，必須在 Amazon Route 53 主控台中完成。

本指南提供您可使用 Route 53 主控台完成的部分進階管理任務的資訊。有關 Route 53 的完整概述，請參閱《Amazon Route 53 開發人員指南》中的[什麼是 Amazon Route 53 ?](#)。

### 內容

- [檢視域註冊的狀態](#)
- [鎖定域以防止未經授權轉移到另一個註冊商](#)
- [還原已過期或已刪除的域](#)
- [轉移域](#)
- [刪除域名稱註冊](#)

## 檢視域註冊的狀態

網域名稱有狀態，也稱為「可延伸佈建通訊協定」(EPP) 狀態碼。ICANN 這個維護網域名稱中央資料庫的組織，開發了 EPP 狀態碼。EPP 狀態碼會告訴您各種作業的狀態。例如，註冊網域名稱、續約註冊網域名稱等等。所有註冊商都使用這組相同的狀態碼。若要檢視域的狀態碼，請參閱《Amazon Route 53 開發人員指南》中的[檢視域註冊的狀態](#)。

## 鎖定域以防止未經授權轉移到另一個註冊商

所有一般頂層網域 (TLD) 的網域註冊機構都允許您鎖定網域，以防止有人在未經您許可的情況下，將網域轉移到其他註冊商。如需詳細資訊，請參閱《Amazon Route 53 開發人員指南》中的[鎖定域以防止未經授權轉移到另一個註冊商](#)。

## 還原已過期或已刪除的域

如果您沒有在延遲續約期間結束之前續約網域，或者您不小心刪除該網域，一些頂層網域 (TLD) 註冊機構在提供網域給他人註冊，可讓您還原網域。請使用連結的程序，試著還原您的網域註冊。如需詳細資訊，請參閱《Amazon Route 53 開發人員指南》中的[還原已過期或已刪除的域](#)。

## 轉移域註冊

您可以將在另一個註冊機構註冊的域轉移到 Route 53、從一個 AWS 帳戶轉移到另一個帳戶，或從 Route 53 轉移到其他註冊機構。如需詳細資訊，請參閱《Amazon Route 53 開發人員指南》中的[轉移域](#)。

## 刪除域名稱註冊

對於大多數頂層網域 (TLD)，可在不再需要網域時刪除註冊。如果註冊機構允許刪除註冊，請執行此主題中的程序。如需詳細資訊，請參閱《Amazon Route 53 開發人員指南》中的[刪除網域名稱註冊](#)。

## 在 Lightsail 中註冊或轉移網域時提供網域資訊

當您使用 Amazon Lightsail 註冊網域時，您需要提供網域資訊，例如註冊期限 (期限) 和網域聯絡資訊。您也可以設定自動網域續約和隱私權保護。

您也可以變更目前已向 Lightsail 註冊之網域的資訊。注意下列事項：

- 如果您變更網域的聯絡資訊，我們會向註冊聯絡人傳送有關此變更的電子郵件通知。這封電子郵件來自 [noreply@amazon.com](mailto:noreply@amazon.com)。對於大多數變更，註冊聯絡人不需要回應。
- 如果聯絡資訊變更還構成所有權變更，我們會向註冊聯絡人另外傳送一封電子郵件。ICANN 是維護網域名稱中央資料庫的組織，會要求註冊聯絡人確認收到這封電子郵件。如需詳細資訊，請參閱本節後面的[名字、姓氏和組織](#)。

如需變更現有域聯絡人資訊的詳細資訊，請參閱[更新域的聯絡人資訊](#)。

## 您提供的網域資訊

- [期間](#)
- [自動網域續約](#)
- [註冊者、管理和技術聯絡人](#)
- [與註冊者相同](#)
- [聯絡人類型](#)
- [名字、姓氏](#)
- [組織](#)
- [電子郵件](#)
- [電話](#)
- [地址 1](#)
- [地址 2](#)
- [國家/地區](#)
- [州](#)
- [城市](#)
- [郵遞區號](#)
- [隱私權保護](#)

## 術語

網域的註冊期間。期限通常為一年，但您可以在註冊網域時，將期限增加至最多十年。

## 自動網域續約

當您向 Lightsail 註冊網域時，我們會將網域設定為自動續約。自動續約期間通常為一年。選擇是否讓 Lightsail 在網域到期前自動續約網域。註冊費將從您的 AWS 帳戶中收取。如需詳細資訊，請參閱[域註冊續約](#)。

### Important

如果您停用自動網域續約，過期日期過後將不續約網域註冊。因此，您可能會失去對網域名稱的控制權。

## 註冊者、管理和技術聯絡人

在預設情況下，我們對所有三個聯絡人使用相同的資訊。如果您想要為一或多個聯絡人輸入不同資訊，請針對每個聯絡人，取消勾選 Same as registrant (與註冊者相同) 旁的核取方塊。

### 與註冊者相同

指定是否要對網域註冊者、管理聯絡人和技術聯絡人使用相同的聯絡資訊。

### 聯絡人類型

此聯絡人的類別。注意下列事項：

- 如果您選擇 Company (公司) 或 Association (關聯) 選項，必須輸入組織名稱。
- 對於某些頂層網域 (TLD)，隱私權保護可用性取決於您為 Contact type (聯絡人類型) 選擇的值。如需 TLD 的隱私權保護設定，請參閱 [可向 Amazon Route 53 註冊的域](#)

•

### 名字、姓氏

聯絡人的姓氏和名字。針對 First Name (名字) 和 Last Name (姓氏)，建議您使用官方證件上的姓名。對於網域設定的某些變更，您必須提供身分證明。在這些情況下，您證件上的姓名必須與該網域註冊聯絡人的姓名相符。

如果您變更註冊聯絡人的電子郵件地址，我們會同時向新舊電子郵件地址傳送此電子郵件。

### 組織

與聯絡人相關聯的組織 (如果有)。對於申請人和管理聯絡人，此組織通常為註冊網域的組織。對於技術聯絡人，這可能是管理網域的組織。

當聯絡人類型是 Person (個人) 以外的任何值，且您變更註冊聯絡人的 Organization (組織) 欄位時，您會變更網域擁有者。ICANN 要求我們向註冊聯絡人傳送電子郵件以獲得核准。電子郵件來自下列其中一個電子郵件地址：

- noreply@registrar.amazon.com – 用於 Amazon Registrar 註冊的 TLD
- noreply@domainnameverification.net – 用於我們的註冊商合作夥伴 Gandi 註冊的 TLD

若要判斷適合 TLD 的註冊商，請參閱[可向 Amazon Route 53 註冊的域](#)。

如果您變更註冊聯絡人的電子郵件地址，我們會同時向新舊電子郵件地址傳送此電子郵件。

## 電子郵件

聯絡人的電子郵件地址。注意下列事項：

如果您變更註冊聯絡人的電子郵件地址，我們會同時向新舊電子郵件地址傳送通知電子郵件。這封電子郵件來自 noreply@amazon.com。

## 電話

聯絡人的電話號碼：

- 如果您輸入美國或加拿大境內位置的電話號碼，請輸入 1，後面接著 10 位數的區碼和電話號碼。
- 如果要輸入任何其他位置的電話號碼，請輸入國碼 (地區碼)，後面接著電話號碼的其餘部分。如需國際電話國碼 (地區碼) 的清單，請參閱 Wikipedia 上的[國際電話區號列表](#)。

## 地址 1

聯絡人的街道地址或郵政信箱。

## 地址 2

聯絡人的其他地址資訊，例如公寓、套房、住宅、大樓、樓層或收件處。

## 國家

聯絡人的國家/地區。

## 州

聯絡人的州或省 (如果有)。

## 城市

聯絡人的城市。

## 郵遞區號

聯絡人的郵遞區號。

## 隱私權保護

選擇是否要向 WHOIS 查詢隱藏您的聯絡資訊。如果您為網域聯絡人資訊啟用隱私權保護，WHOIS ("who is") 查詢會傳回網域註冊商的聯絡資訊，而非您的個人資訊。網域註冊商是管理網域名稱註冊的公司。

### Note

相同隱私權設定適用於管理聯絡人、註冊者和技術聯絡人。

如果您為網域聯絡人資訊停用隱私權保護，您會在指定的電子郵件地址收到更多垃圾電子郵件。

任何人都可以傳送針對某個網域的 WHOIS 查詢，並取得該網域的所有聯絡資訊。WHOIS 命令在許多作業系統中都可用，在許多網站上也會以 Web 應用程式的形式提供。

### Important

雖然有合法使用者希望取得與您的網域聯絡人資訊，但最常見的使用者是垃圾郵件傳送者，他們的目標是向網域聯絡人傳送不需要的電子郵件和偽造優惠。一般而言，我們建議您為 Contact information (聯絡人資訊) 啟用 Privacy protection (隱私權保護)。

如需隱私權保護的詳細資訊，請參閱下列主題：

- [管理域的隱私權保護](#)
- [可向 Amazon Route 53 註冊的域](#)

## 續約或停用網域 Lightsail

當您向 Amazon Lightsail 註冊網域時，我們會將網域設定為依預設自動續約。預設自動續約期間為一年，但某些頂層網域 (TLD) 的註冊機構提供更長的續約期間。所有一般 TLD 都允許將網域註冊延長為更長的期間，通常可長達十年 (以一年為單位增加)。

**Note**

如果您打算關閉您的 AWS 帳戶，否則，即使您已關閉帳戶，您的網域註冊也會續約。

**內容**

- [自動續約](#)
- [在網域註冊期間為網域設定自動續約](#)
- [為已註冊的網域設定自動續約](#)

## 自動續約

以下時間表說明自動續約為作用中狀態時會發生的情況：

### 過期前 45 天

我們會傳送電子郵件給註冊聯絡人，告知您自動續約為作用中狀態。此電子郵件也包含如何停用自動續約的指示。將註冊聯絡人的電子郵件地址保持最新，以免錯過此電子郵件。

### 過期前 35 或 30 天

對於 .com.ar、.com.br 和 .jp 網域以外的所有網域，我們會在過期日期前 35 天，續約網域註冊。如此一來，我們就有時間在網域名稱過期前，解決續約的任何問題。

.com.ar、.com.br 和 .jp 網域的註冊機構，要求在網域過期前 30 天內續約網域。我們的註冊商合作夥伴 Gandi，會在過期前 30 天傳送續約電子郵件。如果自動續約為作用中狀態，系統會在我們續約網域的同一天，傳送此電子郵件。

如果自動續約為非作用中狀態，以下時間表說明網域名稱過期日期接近時會發生的情況：

### 過期前 45 天

我們會傳送電子郵件，通知註冊聯絡人自動續約目前為非作用中狀態。此電子郵件也包含如何啟用自動續約的指示。將註冊聯絡人的電子郵件地址保持最新，以免錯過此電子郵件。

### 過期前 35 天和 7 天

如果網域自動續約為停用狀態，網域註冊管理機構 ICANN 會要求註冊商傳送一封電子郵件給註冊聯絡人。電子郵件來自下列其中一個電子郵件地址：

noreply@registrar.amazon.com – 適用於註冊商為 Amazon Registrar 的域

noreply@domainnameverification.net – 適用於註冊商是我們的註冊商合作夥伴 Gandi 的域

如果您在過期前 30 天內啟用自動續約，我們會在 24 小時內續約網域註冊。

如需有關續約期的詳細資訊，請參閱《Amazon Route 53 開發人員指南》的 [可在 Amazon Route 53 註冊的域](#) 中的 TLD 的「續約及還原域的截止日期」一節。

## 在過期日期之後

對於大多數網域，註冊商都會在網域過期之後短時間內予以保留，這樣您便可以在過期日期之後續約已過期的網域，但如果您要保留網域，我們強烈建議將自動續約功能保持啟用狀態。如需有關在過期日期後嘗試續約域的資訊，請參閱《Amazon Route 53 開發人員指南》中的 [還原已過期或已刪除的域](#)。

如果您的網域過期，但允許延遲續約，您可以按標準續約價格續約網域。若要判斷域是否仍在延遲續約期間內，請執行《Amazon Route 53 開發人員指南》中 [延長域的註冊期](#) 中的程序。如果仍列出網域，表示它仍在延遲續約期間內。

## 在網域註冊期間為網域設定自動續約

當您向 Lightsail 註冊新網域名稱時，我們會將網域設定為自動續約。您可以選擇在網域註冊程序期間，停用自動網域續約。

1. 登入主 [Lightsail 台](#)。
2. 選擇 Domains & DNS (網域和 DNS) 索引標籤。
3. 選擇 Register domain (註冊網域) 按鈕。
4. 指定您要向 Lightsail 註冊的網域名稱，然後選擇 Check availability (檢查可用性)。
5. 如果網域名稱可用，您會看到網域註冊頁面。在 Automatic domain renewal (自動網域續約) 區段中，開啟或關閉切換開關，以啟用或停用自動網域續約。

## 為已註冊的網域設定自動續約

如果您想要變更 Lightsail 在到期日前不久自動續約網域的註冊，或是要檢視目前的自動續約設定時，請執行下列程序。

1. 登入主 [Lightsail 台](#)。

2. 選擇 Domains & DNS (網域和 DNS) 索引標籤。
3. 選擇要檢視或更新的網域。
4. 選擇 Contact info (聯絡人資訊) 索引標籤
5. 在 Automatic domain renewal (自動網域續約) 區段中，開啟或關閉切換開關，以啟用或停用網域註冊期間的自動續約。

## 管理網域聯絡人的隱私保護

當您在 Amazon Lightsail 上註冊網域時，我們預設會為所有網域聯絡人啟用隱私保護。這通常會在 WHOIS (即「誰是」) 查詢中隱藏大聯絡資訊，並減少收到的垃圾郵件數量。您的聯絡人資訊會更換為註冊商的聯絡資訊或 "REDACTED FOR PRIVACY" (受隱私權保護) 字樣。使用隱私權保護免費。

如果您選擇停用隱私權保護，任何人都可以傳送該網域的 WHOIS 查詢，且對於大多數頂層網域 (TLD)，他們可能取得您在註冊網域時提供的所有聯絡人資訊。此資訊包括姓名、地址、電話號碼和電子郵件地址。WHOIS 命令廣泛可用。它包含在許多作業系統中，也在許多網站上以 Web 應用程式的形式提供。

若要管理您使用 Lightsail 註冊之網域的隱私權保護，請執行下列程序。

### 內容

- [完成先決條件](#)
- [管理網域的隱私權保護](#)

## 完成先決條件

透過註冊 Lightsail。如需詳細資訊，請參閱[註冊新域](#)。

## 管理網域的隱私權保護

1. 登入主 [Lightsail 台](#)。
2. 選擇 Domains & DNS (網域和 DNS) 索引標籤。
3. 選擇要為其變更隱私權保護的網域名稱。
4. 選擇 Contact info (聯絡人資訊)。
5. 您可以開啟或關閉 Privacy protection (隱私權保護) 切換開關，管理聯絡人資訊的隱私權保護。

## 更新網域聯絡人 Lightsail

當您向 Amazon Lightsail 註冊網域時，您可以指定網域的聯絡資訊。下列是三種聯絡人資訊：

- 註冊者：網域的擁有者
- 管理員：負責管理您網域的人員
- 技術人員：負責對您網域進行技術變更的人員

您網域的聯絡人資訊會用來驗證您的網域擁有權，並讓您隨時掌握與您網域名稱相關的任何資訊。

### 主題

- [網域擁有者是誰？](#)
- [更新域的聯絡資訊](#)

## 網域擁有者是誰？

當聯絡人類型是 Person (個人)，而您變更註冊聯絡人的 First Name (名字) 或 Last Name (姓氏) 欄位時，您會變更網域的擁有者。

當聯絡人類型是 Person (個人) 以外的任何值，而您變更 Organization (組織) 時，您會變更網域的擁有者。

當您變更目前已向 Lightsail 註冊之網域的連絡人資訊時，會發生下列動作：

- 如果您變更網域的聯絡資訊，我們會向註冊聯絡人傳送有關此變更的電子郵件通知。這封電子郵件來自 [noreply@amazon.com](mailto:noreply@amazon.com)。對於大多數變更，註冊聯絡人不需要回應。
- 如果聯絡資訊變更還構成所有權變更，我們會向註冊聯絡人另外傳送一封電子郵件。ICANN 是維護網域名稱中央資料庫的組織，會要求註冊聯絡人確認收到這封電子郵件。

## 更新域的聯絡資訊

若要更新網域的聯絡資訊，請執行以下程序。

1. 登入主 [Lightsail 台](#)。
2. 選擇 Domains & DNS (網域和 DNS) 索引標籤。
3. 選擇要更新的網域名稱。

4. 選擇 Contact info (聯絡人資訊) 索引標籤。接著選擇 Edit contact (編輯聯絡人)。
5. 更新適用的值。如需詳細資訊，請參閱《Amazon Route 53 開發人員指南》中的[註冊或轉移域時所指定的值](#)。
6. 選擇 Save (儲存)。

## 在 Lightsail 中建立和管理關聯式資料庫

只要幾個步驟 MySQL 您 PostgreSQL 可以在 Amazon Lightsail 中建立受管資料庫。Lightsail 可管理常見的維護和安全性工作，讓資料庫管理更有效率。您可以使用主控台執行下列作業：

- 將資料庫備份至快照。
- 從快照建立更大的新資料庫。
- 透過瀏覽器型日誌和指標針對常見問題進行疑難排解。
- 使用 point-in-time 備份和還原作業來復原資料。

您可以在 Lightsail 執行個體上建置應用程式，並將其連接至 Lightsail 受管理的資料庫。您也可以建立獨立資料庫，並為您的公司連接分析或查詢工具。選擇標準或高可用性資料庫計畫，其中包括預先設定資料庫、以 SSD 為基礎的儲存，以及固定月費的資料傳輸配置。您也可以使用 AWS Command Line Interface (AWS CLI)、API 或 SDK 來管理 Lightsail 資料庫。

## 為您的專案選擇合適的 Lightsail 資料庫

Amazon Lightsail 供最新的主要版本的 MySQL 和 PostgreSQL 資料庫。本指南可協助您決定適合專案的資料庫。

Lightsail 還提供具有 SQL 伺服器的 2022 年視窗伺服器執行個體。如需詳細資訊，請參閱[選擇 Amazon Lightsail 執行個體映像檔](#)。

## 比較 Lightsail 中的受管資料庫

### MySQL

在 Lightsail 中提供了 MySQL 5.7 和 8.0。MySQL 是世界上最多人採用的開放原始碼關聯式資料庫。它可做為許多熱門網站、應用程式和商業產品的主要關聯式資料存放區。MySQL 是一種可靠、穩定且安全的以 SQL 為基礎的資料庫管理系統，具有超過 20 年的社群支援的開發和支援。MySQL 資料庫適用於各式各樣的使用案例，包括關鍵任務應用程式和動態網站。它還做為軟體、硬體和設備的內嵌資料庫。

**⚠ Important**

自 2024 年 6 月 30 日起，Lightsail 將不再支援 MySQL 5.7，而且您將無法使用此藍圖建立新的資料庫。若要瞭解如何升級資料庫執行個體的主要版本，請參閱[升級 Lightsail 資料庫的主要版本](#)。

如需更多詳細資訊，請參閱下列 MySQL 文件：

- [MySQL 5.7 文件](#)
- [MySQL 8.0 文件](#)

## PostgreSQL

Lightsail 中提供第 11、12、13、14、15 和 16 版。PostgreSQL 是功能強大的開放原始碼物件關聯式資料庫系統，在經過 30 多年的積極開發後，該系統在可靠性、功能穩健度和效能方面皆擁有相當傑出的評價。

[官方文件](#)提供了極為豐富的資訊，可讓您了解如何安裝和使用 PostgreSQL。[PostgreSQL 社群](#)也有介紹許多可提供協助的地點，您能藉此熟悉這項技術並探索其運作方式，同時也能尋找各種就業機會。

**⚠ Important**

自 2024 年 6 月 30 日起，Lightsail 將不再支援 PostgreSQL 11，而且您將無法使用此藍圖建立新的資料庫。若要瞭解如何升級資料庫執行個體的主要版本，請參閱[升級 Lightsail 資料庫的主要版本](#)。

如需詳細資訊，請參閱下列 PostgreSQL 文件：

- [PostgreSQL 11 文件](#)
- [PostgreSQL 12 文件](#)
- [PostgreSQL 集](#)
- [PostgreSQL 集](#)
- [PostgreSQL 集](#)
- [PostgreSQL 集](#)

## 將資料匯入最佳化

Lightsail 提供多種資料庫計劃，每個計劃都有特定的記憶體、vCPU、儲存空間和資料傳輸額度規格。由於每個資料庫計劃都有這些規格，因此請務必針對要匯入新 Lightsail 資料庫的資料量，選擇適當大小的資料庫計劃。如果您選擇低於大小要求的計劃，資料匯入的速度可能會變慢。若要選取符合您資料匯入需求的適當資料庫計劃，則可運用下列準則：

- 微型資料庫計劃 (每月 15 USD) — 如果傳輸的資料超過 10 GB，資料匯入的速度可能會變慢。
- 小型資料庫計劃 (每月 30 USD) — 如果傳輸的資料超過 20 GB，資料匯入的速度可能會變慢。
- 中型資料庫計劃 (每月 60 USD) — 如果傳輸的資料超過 85 GB，資料匯入的速度可能會變慢。
- 大型資料庫計劃 (每月 115 USD) — 如果傳輸的資料超過 156 GB，資料匯入的速度可能會變慢。

### Note

如需有關將資料匯入資料庫的詳細資訊，請參閱[將資料匯入 MySQL 資料庫](#)或[將資料匯入 PostgreSQL 資料庫](#)。

## 高可用性資 Lightsail

Lightsail 高可用性受管資料庫可在一個可用區域中的主要資料庫提供容錯移轉支援，在另一個可用區域提供次要待命資料庫。我們建議將高可用性的資料庫用於使用量高且需要資料冗餘的生產工作負載。針對開發和測試目的，您可以使用非高可用性的標準資料庫。

若要建立高可用性資料庫，請在建立受管理的資料庫時，選取 Lightsail 提供的其中一個高可用性資料庫計劃。如需詳細資訊，請參閱[建立資料庫](#)。您也可以將標準資料庫變更為高可用性資料庫。建立標準資料庫的快照、從快照建立新的資料庫，然後選擇一個高可用性計劃。如需詳細資訊，請參閱[透過快照建立資料庫](#)。

## 建立具有高可用性的 Lightsail 資料庫

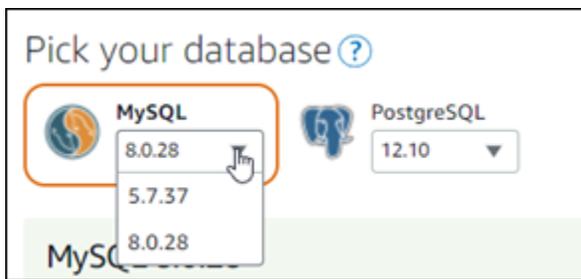
只要幾分鐘就能在 Amazon Lightsail 中建立受管資料庫。您可以選擇 MySQL 或 PostgreSQL 的最新主要版本，然後使用標準或高可用性計劃來設定資料庫。

### Note

如需 Lightsail 中受管理資料庫的詳細資訊，請參閱[選擇資料庫](#)。

## 若要建立資料庫

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁上，選擇「資料庫」索引標籤。
3. 選擇建立資料庫。
4. 選擇資料庫的 AWS 區域 和可用區域。
  1. 選擇「變更 AWS 區域 與可用區域」，然後選擇「區域」。
  2. 選擇 Change your Availability Zone (變更您的可用區域)，接著選擇可用區域。
5. 選擇資料庫類型。在其中一個可用的資料庫引擎選項下，選擇下拉式功能表，然後選擇 Lightsail 支援的最新主要資料庫版本之一。



6. 如有必要，請選擇下列其中一個選項：
  - 指定登入資料 — 指定您自己的資料庫使用者名稱和密碼。否則，Lightsail 會指定使用者名稱，並為您建立強式密碼。
  - 若要指定自己的使用者名稱，請選擇 Specify login credentials (指定登入資料)，並將使用者名稱輸入文字方塊。根據您選取的資料庫引擎，套用下列限制：

### MySQL

- MySQL 必要條件。
- 必須為 1 到 16 個字母或數字。
- 第一個字元必須是字母。
- 不能是所選資料庫引擎的保留字。如需有關 MySQL 中保留字的詳細資訊，請參閱 [MySQL 5.6](#)、[MySQL 5.7](#) 或 [MySQL 8.0](#) 的「關鍵字與保留字」文章。

### PostgreSQL

- PostgreSQL 必要條件。
- 必須為 1 到 63 個字母或數字。
- 第一個字元必須是字母。

- 不能是所選資料庫引擎的保留字。如需 PostgreSQL 中保留字的詳細資訊，請參閱 [PostgreSQL 9.6](#)、[PostgreSQL 10](#)、[PostgreSQL 11](#) 或 [PostgreSQL 12](#) 的「SQL 關鍵字」文章。
- 若要指定自己的密碼，請清除 Create a strong password for me (為我建立高強度密碼) 核取方塊，並將密碼輸入文字方塊。密碼可包含任何能印出的 ASCII 字元，但 "/"、"'" 或 "@" 除外。對於 MySQL 資料庫，密碼可以包含 8 到 41 個字元。對於 PostgreSQL 資料庫，密碼可以包含 8 到 128 個字元。
- 指定主資料庫名稱 — 指定您自己的主要資料庫名稱，否則 Lightsail 會為您指定名稱。若要指定您的主要資料庫名稱，請選擇 Specify the master database name (指定主要資料庫名稱)，並將名稱輸入文字方塊。根據您選取的資料庫引擎，套用下列限制：

### MySQL

- 必須包含 1 到 64 個字母或數字。
- 必須以字母開頭。後續字元可以是字母、底線或數字 (0-9)。
- 不能是所選資料庫引擎的保留字。如需有關 MySQL 中保留字的詳細資訊，請參閱 [MySQL 5.6](#)、[MySQL 5.7](#) 或 [MySQL 8.0](#) 的「關鍵字與保留字」文章。

### PostgreSQL

- 必須包含 1 到 63 個字母、數字或底線。
- 必須以字母開頭。後續字元可以是字母、底線或數字 (0-9)。
- 不能是所選資料庫引擎的保留字。如需 PostgreSQL 中保留字的詳細資訊，請參閱 [PostgreSQL 9.6](#)、[PostgreSQL 10](#)、[PostgreSQL 11](#) 或 [PostgreSQL 12](#) 的「SQL 關鍵字」文章。

## 7. 選擇高可用性或標準資料庫計劃。

以高可用性計畫建立的資料庫會有一個主要資料庫，並在另一個可用區域有一個次要備用資料庫 (用於容錯移轉支援)。如需詳細資訊，請參閱 [高可用性資料庫](#)。不同定價的資料庫套件組合選項均有提供，每個組合都有不同層級的記憶體、處理、儲存空間，以及傳輸費率。

## 8. 為您的資料庫輸入名稱。

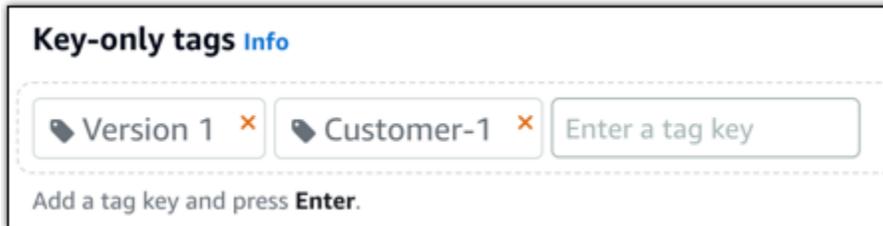
資源名稱：

- 每個 Lightsail 帳戶 AWS 區域 中的每個項目都必須是唯一的。
- 必須包含 2 至 255 個字元。
- 開頭和結尾必須是英數字元或數字。

- 可以包含英數字元、數字、句點、破折號和底線。

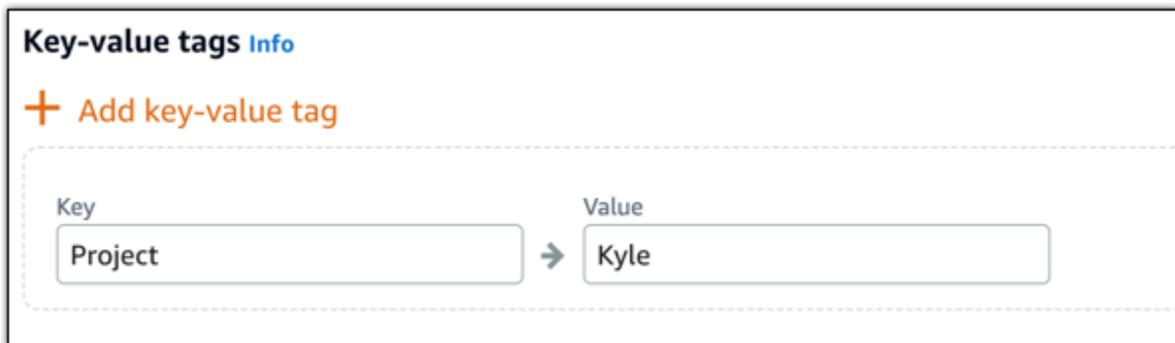
9. 選擇下列其中一個選項以新增標籤至您的資料庫：

- Add key-only tags (新增僅索引鍵標籤) 或 Edit key-only tags (編輯僅索引鍵標籤) (若標籤已新增)。在標籤索引鍵文字方塊中輸入新的標籤，接著按 Enter (輸入)。輸入標籤以新增之後，請選擇 Save (儲存)，如果不要新增則選擇 Cancel (取消)。



- Create a key-value tag (建立索引鍵值標籤)，接著將索引鍵輸入 Key (索引鍵) 文字方塊，將值輸入 Value (值) 文字方塊。完成輸入標籤後，請選擇 Save (儲存)，如果不要新增則選擇 Cancel (取消)。

鍵值標籤在儲存前一次只能新增一個。若要新增超過一個索引鍵值標籤，請重複之前的步驟。



**Note**

如需有關僅索引鍵和索引鍵值標籤的詳細資訊，請參閱[標籤](#)。

10. 選擇建立資料庫。

幾分鐘內，您的 Lightsail 資料庫就可以準備就緒。您可以開始設定其用於資料匯入，或使用資料庫用戶端連接。

## 後續步驟

以下是一些指南，可協助您在 Lightsail 中管理新資料庫啟動並執行之後：

- [設定資料庫的資料匯入模式](#)
- [在 Amazon Lightsail 中為您的資料庫設定公用模式](#)
- [管理資料庫密碼](#)
- [連線至 MySQL 資料庫](#)
- [連線至 PostgreSQL 資料庫](#)
- [將資料匯入 MySQL 資料庫](#)
- [將資料匯入 PostgreSQL 資料庫](#)
- [建立資料庫快照](#)

## 從用戶端應用程式 Connect 到您的 Lightsail MySQL 資料庫

在 Amazon Lightsail 中建立 MySQL 受管資料庫之後，您可以使用任何標準 MySQL 用戶端應用程式或公用程式來連線到該資料庫。您必須從 Lightsail 主控台的資料庫管理頁面取得資料庫端點、連接埠、使用者名稱和密碼。在用戶端或 Web 應用程式設定資料庫連線時，必須指定這些值。

本指南會說明如何取得所需的連線資訊，以及如何設定 MySQL Workbench 來連線至受管資料庫。

### Note

如需有關連線至 PostgreSQL 資料庫的詳細資訊，請參閱[連線至 PostgreSQL 資料庫](#)。

## 步驟 1：取得 MySQL 資料庫的連線詳細資訊

從 Lightsail 主控台取得資料庫端點和連接埠資訊。您稍後設定用戶端來連接至資料庫時，將使用這些資訊。

取得資料庫連線詳細資訊

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁上，選擇「資料庫」索引標籤。
3. 選擇欲連接的資料庫名稱。

- 在 Connect (連線) 索引標籤 Endpoint and port (端點和連接埠) 區段下，請記下端點及連接埠資訊。

為避免輸入錯誤，建議您將端點複製到剪貼簿。方法是反白選取端點，然後按下 Ctrl+C (Ctrl+C) (若您使用 Windows) 或 Cmd+C (Cmd+C) (若您使用 macOS)，將端點複製到剪貼簿。然後，在適當位置按下 Ctrl+V (Ctrl+V) 或 Cmd+V (Cmd+V) 來貼上。



- 在 Connect (連接) 索引標籤的 User name and passwords (使用者名稱和密碼) 區段下，記下使用者名稱，然後選擇 Password (密碼) 區段下的 Show (顯示) 來檢視目前的資料庫密碼。

由於受管密碼十分複雜，因此建議您採取複製貼上以避免輸入錯誤。反白選取受管的密碼，然後按下 Ctrl+C (Ctrl+C) (若您使用 Windows) 或 Cmd+C (Cmd+C) (若您使用 macOS)，將密碼複製到剪貼簿。然後，在適當位置按下 Ctrl+V (Ctrl+V) 或 Cmd+V (Cmd+V) 來貼上。

## 步驟 2：設定 MySQL 資料庫的公有可用性

您必須為資料庫啟用公用模式，才能從外部連線到資料庫，或從與資料庫不同 AWS 區域的 Lightsail 執行個體連線。公有模式啟用時，任何擁有您資料庫使用者名稱和密碼的使用者，都能連線至該資料庫。若要設定資料庫的公有可用性，請依照[設定資料庫的公有模式](#)指南中的步驟進行操作。

### Note

如果您打算從與資料庫位於相同區域的其中一個 Lightsail 執行個體連線至資料庫，請跳至步驟 3。

## 步驟 3：設定您的資料庫用戶端來連接到 MySQL 資料庫

您需要將資料庫用戶端設定為使用先前取得的端點和連接埠，才能連線至 MySQL 資料庫。下列步驟會說明如何設定 MySQL Workbench，但這些步驟可能與其他用戶端類似。

### Note

如需有關使用 MySQL Workbench 的詳細資訊，請參閱 [MySQL Workbench 手冊](#)。

### 設定 MySQL Workbench 以連線至資料庫

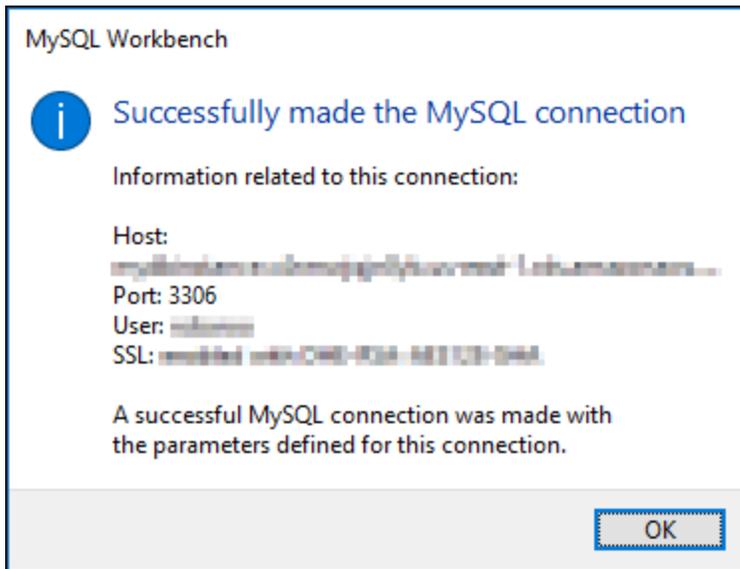
1. 開啟 MySQL Workbench (MySQL Workbench)。
2. 選擇 Database (資料庫) 功能表，然後選擇 Manage connections (管理連線)。
3. 將下列資訊輸入至相對應的表單內：

The screenshot shows the MySQL Workbench connection configuration window. At the top, there is a 'Connection Name' text box. Below it, the 'Connection' tab is active, showing a 'Connection Method' dropdown menu set to 'Standard (TCP/IP)'. Underneath, there are three sub-tabs: 'Parameters', 'SSL', and 'Advanced', with 'Parameters' selected. The 'Parameters' section contains several fields: 'Hostname' with the value '127.0.0.1', 'Port' with the value '3306', 'Username' with the value 'root', 'Password' with buttons for 'Store in Vault ...' and 'Clear', and 'Default Schema' which is empty. To the right of these fields are descriptive labels for each field.

- Connection Name (連線名稱) — 建議您使用與資料庫類似的名稱做為連線名稱。將有助您未來能夠加以辨識。
- Connection Method (連線方法) — 選擇 Standard (TCP/IP) (標準 (TCP/IP))。
- Port (連接埠) - 輸入您稍早取得的資料庫連接埠。MySQL 的預設連接埠為 3306。
- Hostname (主機名稱) — 輸入您稍早取得的資料庫端點。如果您是從 Lightsail 主控台複製資料庫端點，而該端點仍在剪貼簿中，請按 Ctrl+V (如果您使用的是 Windows)，或按下 Cmd+V (如果您使用的是 macOS) 來貼上它。

- Username (使用者名稱) — 輸入您之前取得的資料庫使用者名稱。
  - Password (密碼) — 選擇 Store in vault (存放在保存庫)。在出現的視窗中，輸入您之前取得的資料庫密碼。如果您是從 Lightsail 主控台複製密碼，但密碼仍在剪貼簿中，請按 Ctrl+V (如果您使用的是 Windows)；如果您使用的是 macOS，請按下 Cmd+V 鍵來貼上密碼。選擇 OK (確定) 來儲存您的密碼。
  - Default Schema (預設結構描述) — 此文字方塊保持空白。
4. 選擇 Test connection (測試連線) 來判斷用戶端是否能夠與您的資料庫建立連線。

如果連線成功，將出現如下範例的提示。閱讀資訊後，請選擇 OK (確定) 來將其關閉。

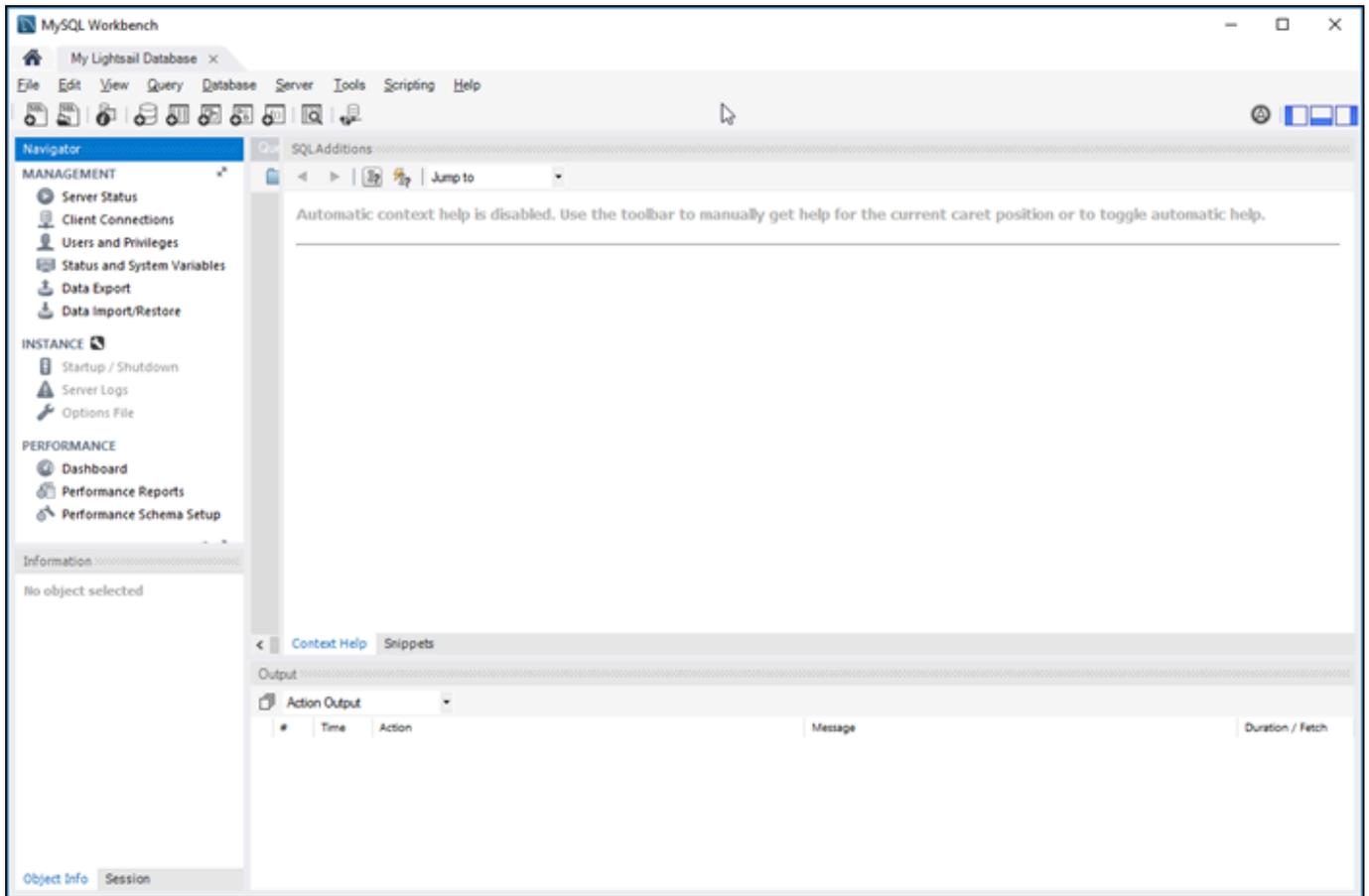


5. 選擇 New (新增) 來儲存新的連線詳細資訊，然後選擇 Close (關閉) 來關閉連線管理視窗。

新資料庫連線會顯示於 MySQL Workbench 應用程式首頁的 MySQL Connections 部分。

6. 欲連接至您的資料庫，請選擇新的資料庫連線。

如果連線成功，將出現如下範例的視窗。



## 後續步驟

以下是協助您在 Lightsail 中將資料匯入資料庫的指南：

- [將資料匯入 MySQL 資料庫](#)

## 使用 SSL/TLS 安全地連接到 Lightsail MySQL 資料庫

Amazon Lightsail 會建立 SSL 憑證，並在佈建時將其安裝在您的 MySQL 受管資料庫上。憑證是由憑證授權機構 (CA) 簽署，而且其包含資料庫執行個體端點做為 SSL 憑證的一般名稱 (CN)，以防止詐騙攻擊。

Lightsail 建立的 SSL 憑證是受信任的根實體，在大多數情況下應該可以運作，但如果您的應用程式不接受憑證鏈結，則可能會失敗。若您的應用程式不接受憑證鏈結，您可能需要使用中繼憑證來連線至您的 AWS 區域。

如需受管資料庫之 CA 憑證、支援的 AWS 區域，以及如何為應用程式下載中繼憑證的詳細資訊，請參閱[為受管資料庫下載 SSL 憑證](#)。

## 支援的連線

下列 MySQL 版本的安全連線使用 yaSSL：

- MySQL 5.7.19 版和更舊的 5.7 版
- MySQL 5.6.37 版和更舊的 5.6 版
- MySQL 5.5.57 版和更舊的 5.5 版

下列 MySQL 版本的安全連線使用 OpenSSL：

- MySQL 8.0 版
- MySQL 5.7.21 版和更新的 5.7 版
- MySQL 5.6.39 版和更新的 5.6 版
- MySQL 5.5.59 版和更新的 5.5 版

MySQL 受管資料庫支援 Transport Layer Security (TLS) 1.0、1.1 和 1.2 版。下列清單顯示 MySQL 版本的 TLS 支援：

- MySQL 8.0 - TLS1.0，TLS 1.1 以及 TLS 1.2
- MySQL 5.7 - TLS1.0 和 TLS 1.1。只有 MySQL 5.7.21 及更新版本才支援 TLS 1.2。
- MySQL 5.6 - TLS1.0
- MySQL 5.5 - TLS1.0

## 必要條件

- 將 MySQL 伺服器安裝在您要用於連接到資料庫的電腦上。如需詳細資訊，請參閱 MySQL 網站的[MySQL 社群伺服器檔案下載](#)。
- 為您的資料庫下載適用的憑證。如需詳細資訊，請參閱[為受管資料庫下載 SSL 憑證](#)。

## 使用 SSL 連接到 MySQL 資料庫

完成以下步驟，以使用 SSL 連接到 MySQL 資料庫。

1. 開啟終端機或命令提示視窗。
2. 根據您的 MySQL 資料庫版本，輸入下列其中一個命令：
  - 輸入以下命令，以連接到 MySQL 5.7 或更新版本的資料庫。

```
mysql -h DatabaseEndpoint --ssl-ca=/path/to/certificate/rds-combined-ca-bundle.pem --ssl-mode=VERIFY_IDENTITY -u UserName -p
```

在命令中：

- *DatabaseEndpoint* 與您的數據庫的端點。
- */path/to /##/ rds-combined-ca-bundle .pem* 與您下載並保存數據庫證書的本地路徑。
- *UserName* 使用您的數據庫的用戶名。

範例：

```
mysql -h ls-1c51a7c70a4fb55e542829a4e4e0d735ba42.czowadgeezqi.us-west-2.rds.amazonaws.com --ssl-ca=/home/ec2-user/rds-combined-ca-bundle.pem --ssl-mode=VERIFY_IDENTITY -u dbmasteruser -p
```

- 輸入以下命令，以連接到 MySQL 6.7 或更早版本的資料庫。

```
mysql -h DatabaseEndpoint --ssl-ca=/path/to/certificate/rds-combined-ca-bundle.pem --ssl-verify-server-cert -u UserName -p
```

在命令中：

- *DatabaseEndpoint* 與您的數據庫的端點。
- */path/to /##/ rds-combined-ca-bundle .pem* 與您下載並保存數據庫證書的本地路徑。
- *UserName* 使用您的數據庫的用戶名。

範例：

```
mysql -h ls-1c51a7c70a4fb55e542829a4e4e0d735ba42.czowadgeezqi.us-west-2.rds.amazonaws.com --ssl-ca=/home/ec2-user/rds-combined-ca-bundle.pem --ssl-verify-server-cert -u dbmasteruser -p
```

3 出現提示時，針對您在上一個命令中指定的資料庫使用者，鍵入密碼，並按下 Enter。

您應該會看到類似以下範例的結果：

```
[ec2-user@ip-172-26-5-44 ~]$ mysql -h ls-1c51a7beedc70a4fb55e542829a4e4e0d735ba42.czowadgeezi.us-west-2.rds.amazonaws.com --ssl-ca=/home/ec2-user/rds-ca-2015-root.pem --ssl-verify-server-cert -u dbmasteruser -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 2727
Server version: 8.0.16 Source distribution

Copyright (c) 2000, 2018, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> █
```

4. 鍵入 **status**，並按下 Enter，以檢視您的連線狀態。

如果在 SSL 旁邊看見“Cipher in use is”的值，則表示已加密連線。

```
mysql> status
-----
mysql Ver 14.14 Distrib 5.5.62, for Linux (x86_64) using readline 5.1

Connection id:          2727
Current database:
Current user:           dbmasteruser@ip-172-26-5-44
SSL:                    Cipher in use is DHE-RSA-AES256-SHA
Current pager:         stdout
Using outfile:         ''
Using delimiter:       ;
Server version:        8.0.16 Source distribution
Protocol version:      10
Connection:            ls-1c51a7beedc70a4fb55e542829a4e4e0d735ba42.czowadgeezi.us-west-2.rds.amazonaws.com via TCP/IP
Server characterset:   utf8mb4
Db characterset:       utf8mb4
Client characterset:   utf8
Conn. characterset:    utf8
TCP port:              3306
Uptime:                9 days 16 hours 24 min 33 sec

Threads: 3 Questions: 557480 Slow queries: 0 Opens: 242 Flush tables: 3 Open tables: 146 Queries per second avg: 0.666
-----
```

## Connect 至您 Lightsail PostgreSQL 執行個體

在 Amazon Lightsail 中建立 PostgreSQL 受管資料庫之後，您可以使用任何標準 PostgreSQL 用戶端應用程式或公用程式來連線到該資料庫。您必須從 Lightsail 主控台的資料庫管理頁面取得資料庫端點、連接埠、使用者名稱和密碼。在用戶端或 Web 應用程式設定資料庫連線時，必須指定這些值。

本指南說明如何取得所需的連線資訊，以及如何設定 pgAdmin 來連接到您的受管資料庫。

**Note**

如需有關連接至 MySQL 資料庫的詳細資訊，請參閱[連接至 MySQL 資料庫](#)。

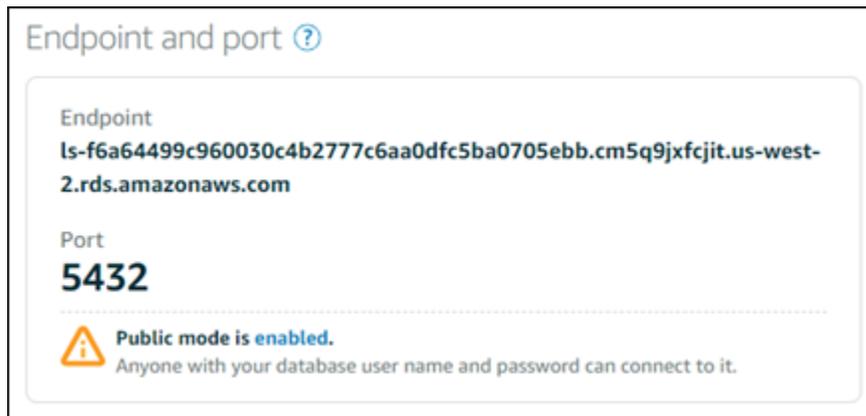
## 步驟 1：取得您的 PostgreSQL 資料庫連線詳細資訊

從 Lightsail 主控台取得資料庫端點和連接埠資訊。您稍後設定用戶端來連接至資料庫時，將使用這些資訊。

### 取得資料庫連線詳細資訊

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁上，選擇「資料庫」索引標籤。
3. 選擇欲連接的資料庫名稱。
4. 在 Connect (連線) 索引標籤 Endpoint and port (端點和連接埠) 區段下，請記下端點及連接埠資訊。

為避免輸入錯誤，建議您將端點複製到剪貼簿。方法是反白選取端點，然後按下 Ctrl+C (Ctrl+C) (若您使用 Windows) 或 Cmd+C (Cmd+C) (若您使用 macOS)，將端點複製到剪貼簿。然後，在適當位置按下 Ctrl+V (Ctrl+V) 或 Cmd+V (Cmd+V) 來貼上。



5. 在 Connect (連接) 索引標籤的 User name and passwords (使用者名稱和密碼) 區段下，記下使用者名稱，然後選擇 Password (密碼) 區段下的 Show (顯示) 來檢視目前的資料庫密碼。

由於受管密碼十分複雜，因此建議您採取複製貼上以避免輸入錯誤。反白選取受管的密碼，然後按下 Ctrl+C (Ctrl+C) (若您使用 Windows) 或 Cmd+C (Cmd+C) (若您使用 macOS)，將密碼複製到剪貼簿。然後，在適當位置按下 Ctrl+V (Ctrl+V) 或 Cmd+V (Cmd+V) 來貼上。

## 步驟 2：設定您 PostgreSQL 資料庫的公有可用性

您必須為資料庫啟用公用模式，才能從外部連線到該資料庫，或從與資料庫不同區域的 Lightsail 執行個體連線。公有模式啟用時，任何擁有您資料庫使用者名稱和密碼的使用者，都能連線至該資料庫。若要設定資料庫的公有可用性，請依照[設定資料庫的公有模式](#)指南中的步驟進行操作。

### Note

如果您打算從與資料庫位於相同區域的其中一個 Lightsail 執行個體連線至資料庫，請跳至步驟 3。

## 步驟 3：設定您的資料庫用戶端來連接到 PostgreSQL 資料庫

欲連接至您的 PostgreSQL 資料庫，請將資料庫用戶端設定為使用您之前取得的端點及連接埠。以下步驟說明如何設定 pgAdmin，但這些步驟可能與其他用戶端類似。

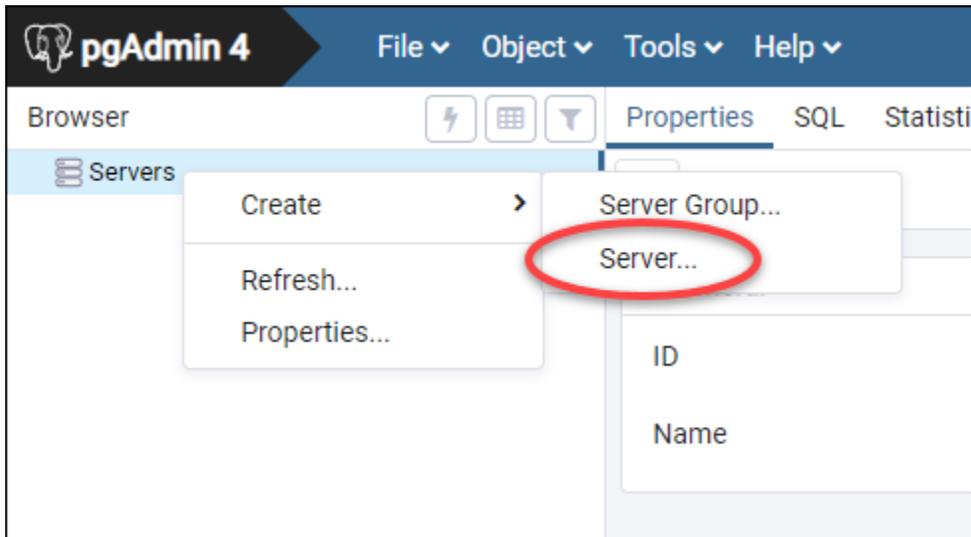
### Note

如需有關使用 pgAdmin 的詳細資訊，請參閱 [pgAdmin 文件](#)。

設定 pgAdmin 以連接到您的資料庫

1. 開啟 pgAdmin。
2. 在左側導覽功能表的 Servers (伺服器) 按一下滑鼠右鍵。
3. 選擇 Create (建立)，然後選擇 Server (伺服器)。

4.



5. 在 Create - Server (建立 - 伺服器) 表單中，為伺服器輸入名稱。建議您使用與資料庫類似的名稱做為連線名稱。將有助您未來能夠加以辨識。
6. 選擇 Connection (連線) 索引標籤，然後在顯示的表格中輸入以下資訊：

A screenshot of the 'Create - Server' dialog box in pgAdmin 4. The 'Connection' tab is selected. The form contains the following fields:

- Host name/address: A text input field with a red warning icon and a red border.
- Port: A text input field containing '5432'.
- Maintenance database: A text input field containing 'postgres'.
- Username: A text input field containing 'postgres'.
- Password: A text input field.
- Save password?: A checkbox that is unchecked.
- Role: A text input field.
- Service: A text input field.

At the bottom, there is a red error message: 'Either Host name, Address or Service must be specified.' Below the error message are buttons for 'Cancel', 'Reset', and 'Save'.

- Host name/address (主機名稱/地址) - 輸入您稍早取得的資料庫終端節點。如果您是從 Lightsail 主控台複製資料庫端點，而該端點仍在剪貼簿中，請按 Ctrl+V (如果您使用的是 Windows)，或按下 Cmd+V (如果您使用的是 macOS) 來貼上它。

- Port (連接埠) - 輸入您稍早取得的資料庫連接埠。PostgreSQL 的預設連接埠為 5432。
- Maintenance database (維護資料庫) - 指定用戶端將連接的初始資料庫名稱。這是您在 Lightsail 中建立 PostgreSQL 資料庫時所指定的主要資料庫名稱。

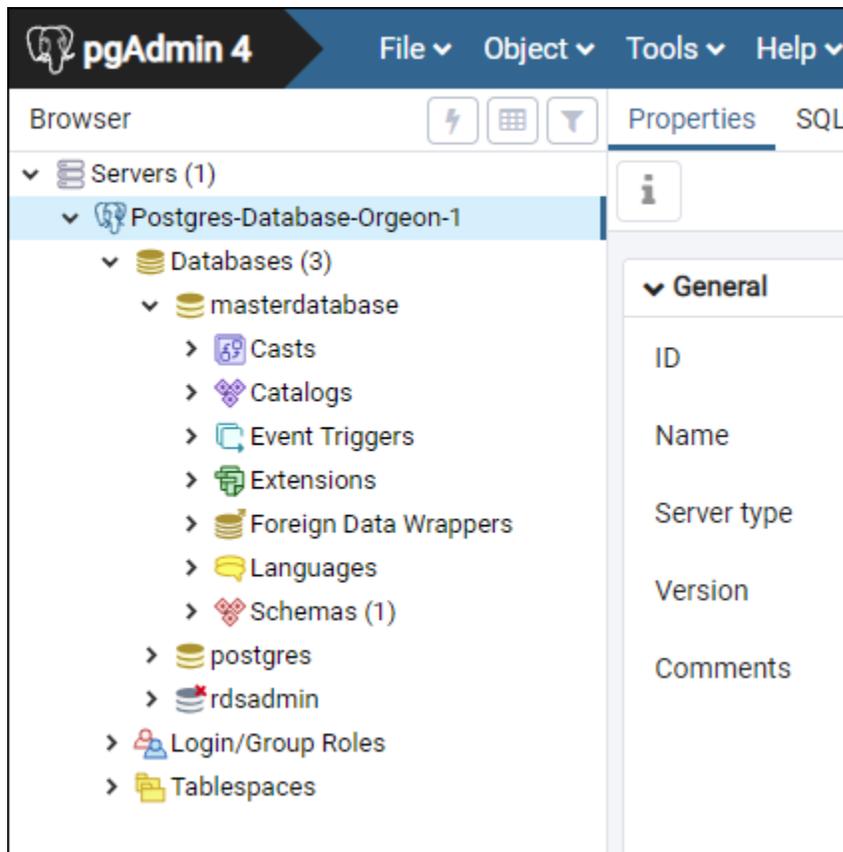
如果您不記得主要資料庫的名稱，請輸入 postgres。每個 PostgreSQL 受管資料庫都有一個可供您連接的 postgres 資料庫，在連接之後，您將可以存取在 PostgreSQL 受管資料庫上的所有其他資料庫。

- Username (使用者名稱) — 輸入您之前取得的資料庫使用者名稱。
  - Password (密碼) - 輸入您稍早取得的資料庫密碼。如果您是從 Lightsail 主控台複製密碼，但密碼仍在剪貼簿中，請按 Ctrl+V (如果您使用的是 Windows)；如果您使用的是 macOS，請按下 Cmd+V 鍵來貼上密碼。選擇 Save password (儲存密碼) 以儲存您的密碼。
  - Role (角色) 和 Service (服務) - 將這些欄位保留空白。
7. 選擇 Save (儲存) 以儲存新的伺服器詳細資訊。

新資料庫連線會出現在 pgAdmin 應用程式左側導覽功能表上的 Servers (伺服器) 部分。

8. 若要連接到您的資料庫，請在您的新資料庫連線上按兩下。

如果連線成功，您將看到該資料庫的可用資源清單。



## 後續步驟

以下是協助您在 Lightsail 中將資料匯入資料庫的指南：

- [將資料匯入 PostgreSQL 資料庫](#)

## 使用以下方式安全地連接到 Lightsail 資料庫 SQL SSL

Amazon Lightsail 會建立一個 SSL 憑證，並在佈建時將其安裝在您的 Postgre SQL (Postgres) 受管資料庫上。憑證由憑證授權單位 (CA) 簽署，而且包含資料庫端點做為一般名稱 (CN)，讓 SSL 憑證防範詐騙攻擊。

Lightsail 建立的 SSL 憑證是受信任的根實體，在大多數情況下應該可以運作，但如果您的應用程式不接受憑證鏈結，則可能會失敗。若您的應用程式不接受憑證鏈結，您可能需要使用中繼憑證來連線至您的 AWS 區域。

如需有關受管理資料庫的 CA 憑證、支援 AWS 區域的憑證，以及如何為應用程式下載中繼憑證的詳細資訊，請參閱[下載受管理資料庫的憑SSL證](#)。

## 必要條件

- 在您將用來連接到數據庫的計算機上安裝 Postgre SQL 服務器。有關更多信息，請參閱 [Postg SQL res 網站上的下載](#)
- 為您的資料庫下載適用的憑證。如需詳細資訊，請參閱[下載受管理資料庫的SSL憑證](#)。

## 使用 Connect 到您的 Postgres 數據庫 SSL

請完成下列步驟，以使用連線到 Postgres 資料庫。SSL

1. 開啟終端機或命令提示視窗。
2. 輸入下列指令以連線至 Postgre SQL 資料庫。

```
psql -h DatabaseEndpoint -p 5432 "dbname=DatabaseName user=UserName sslrootcert=  
path/to/certificate/rds-combined-ca-bundle.pem sslmode=verify-full"
```

在命令中：

- *DatabaseEndpoint* 與數據庫的端點。

- *DatabaseName* 使用要連接到的數據庫的名稱。
- *UserName* 使用您的數據庫的用戶名。
- */path/to/certificate/rds-combined-ca-bundle.pem* 使用您下載並保存數據庫證書的本地路徑。

範例：

```
psql -h ls-8e81e07f8b821917b11e1c6a0e26cb73c203.czowadgeezqi.us-west-2.rds.amazonaws.com -p 5432 "dbname=dbmaster user=dbmasteruser sslrootcert=/home/ec2-user/rds-combined-ca-bundle.pem sslmode=verify-full"
```

3. 出現提示時，針對您在上一個命令中指定的資料庫使用者，鍵入密碼，並按下 Enter。

您應該會看到類似以下範例的結果。如果您看到「連線」值，您的SSL連線會加密。

```
[ec2-user@ip-172-31-26-115 ~]$ psql -h ls-8e81e04e807f8b821917b11e1c6a0e26cb73c203.czowadgeezqi.us-west-2.rds.amazonaws.com -p 5432 "dbname=dbmaster user=dbmasteruser sslrootcert=/home/ec2-user/rds-combined-ca-bundle.pem sslmode=verify-full"
Password:
psql (10.4, server 11.5)
SSL connection (protocol: TLSv1.2, cipher: ECDHE-RSA-AES256-GCM-SHA384, bits: 256, compression: off)
type "help" for help.

dbmaster=> █
```

## 刪除 Lightsail 資料庫並建立最終快照

如果您不再需要，請在 Amazon Lightsail 中刪除受管資料庫。一旦刪除資料庫，便會停止收取費用。

### Note

您無法復原已刪除的資料庫。您可以依照本指南涵蓋的步驟建立資料庫的最終快照，或者您可以從刪除程序分別建立快照。如需詳細資訊，請參閱[建立資料庫快照](#)。

### 若要刪除資料庫

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁上，選擇「資料庫」索引標籤。
3. 選擇要刪除的資料庫名稱。
4. 選擇 Delete (刪除) 索引標籤。

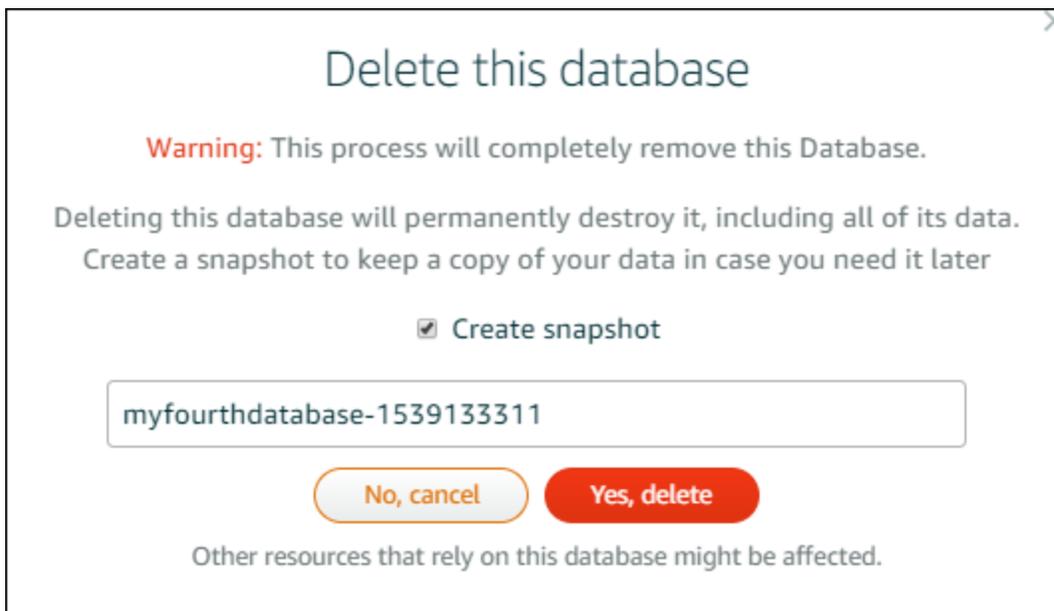
5. 於在刪除前建立快照旁新增核取記號，以在刪除資料庫之前建立最終快照。然後輸入快照的名稱。

資源名稱：

- 每個 Lightsail 帳戶 AWS 區域 中的每個項目都必須是唯一的。
- 必須包含 2 至 255 個字元。
- 開頭和結尾必須是英數字元或數字。
- 可以包含英數字元、數字、句點、破折號和底線。

6. 選擇 Delete database (刪除資料庫)。

7. 選擇 Yes, Delete (是，刪除) 以確認刪除。



如果您選擇在刪除之前建立快照，您可以在 Lightsail 首頁的 [快照] 索引標籤上檢視快照。

## 將大型資料集匯入您的 Lightsail 資料庫，不會延遲

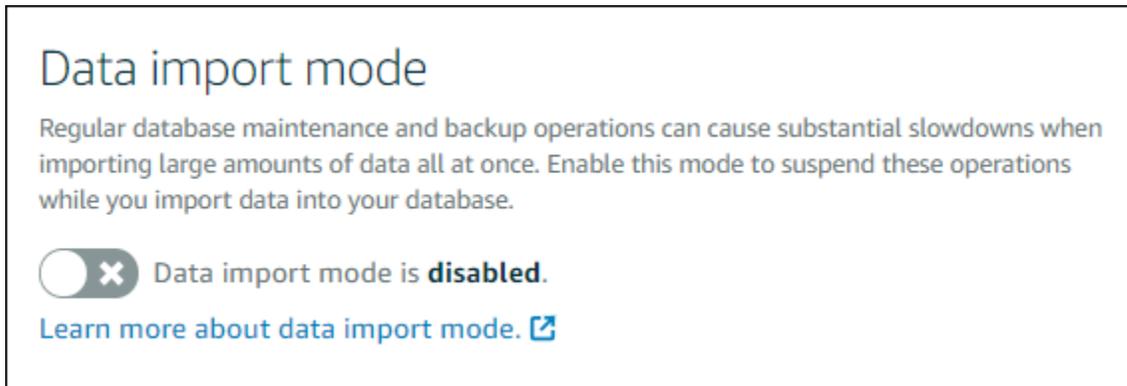
一次匯入大量資料時，一般的資料庫備份操作可能會大幅延遲或降低效能。為 Amazon Lightsail 受管資料庫啟用資料匯入模式，以便在匯入大量資料時暫停這些操作。

### **⚠ Important**

資料匯入模式啟用時，所有緊急恢復備份也會刪除。如果您希望在資料匯入模式啟用前擁有備份，請建立資料庫快照。如需詳細資訊，請參閱[建立資料庫快照](#)。

## 設定資料庫的資料匯入模式

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁上，選擇「資料庫」索引標籤。
3. 選擇須設定資料匯入模式的資料庫名稱。
4. 在 Connect (連線) 索引標籤 Data import mode (資料匯入模式) 部分底下，請將資料匯入模式切換為開啟。匯入完成後，請執行相同操作將其關閉。



現已啟用資料匯入模式，因此資料庫備份操作會暫停。建議您短暫啟用資料匯入模式即可，只有在您必須將大量資料匯入資料庫時才使用。匯入完成後，請立即停用資料匯入模式來恢復備份操作。

### Note

您的匯入速度可能會因您匯入的資料量而減緩。如需詳細資訊，請參閱 [最佳化資料匯入](#)。

## 將 SQL 資料匯入 Lightsail 資料庫

您可以使用 MySQL 工作台將 SQL 文件 (.SQL) 導入到 Amazon Lightsail 中的 MySQL 受管數據庫中。

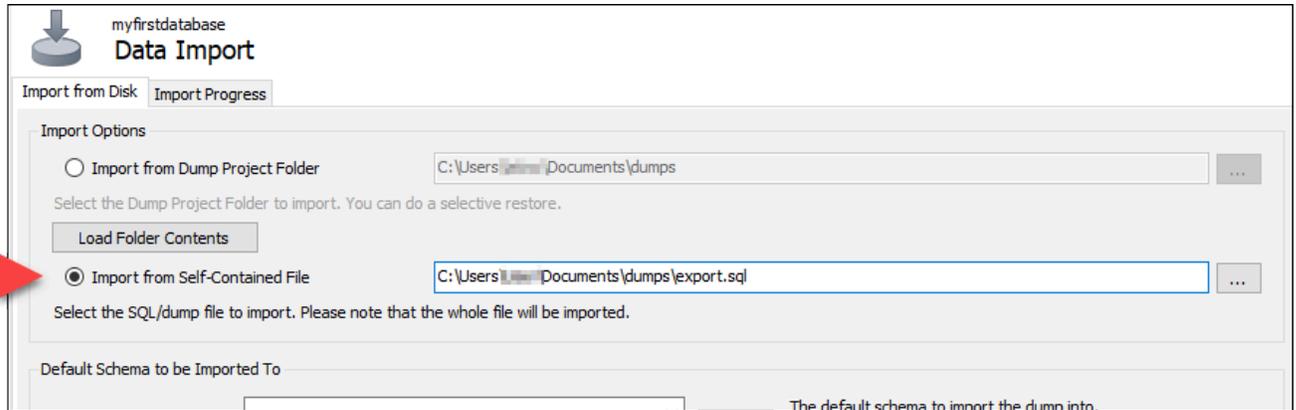
### Note

若要了解如何將 MySQL Workbench 連接至資料庫，請參閱 [連接至 MySQL 資料庫](#)。

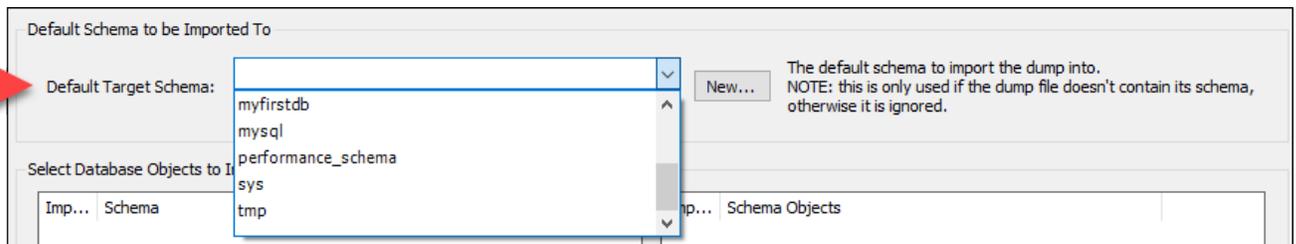
## 將資料匯入資料庫

1. 開啟 MySQL Workbench (MySQL Workbench)。

- 在 MySQL 連線清單中，選擇 MySQL 受管資料庫。
- 從左側導覽功能表選擇 Data Import/Restore (資料匯入/還原)。
- 在 Data Import (資料匯入) 窗格中，在 Import Options (匯入選項) 區段下選擇 Import from Self-Contained File (從可獨自運作的檔案匯入)。

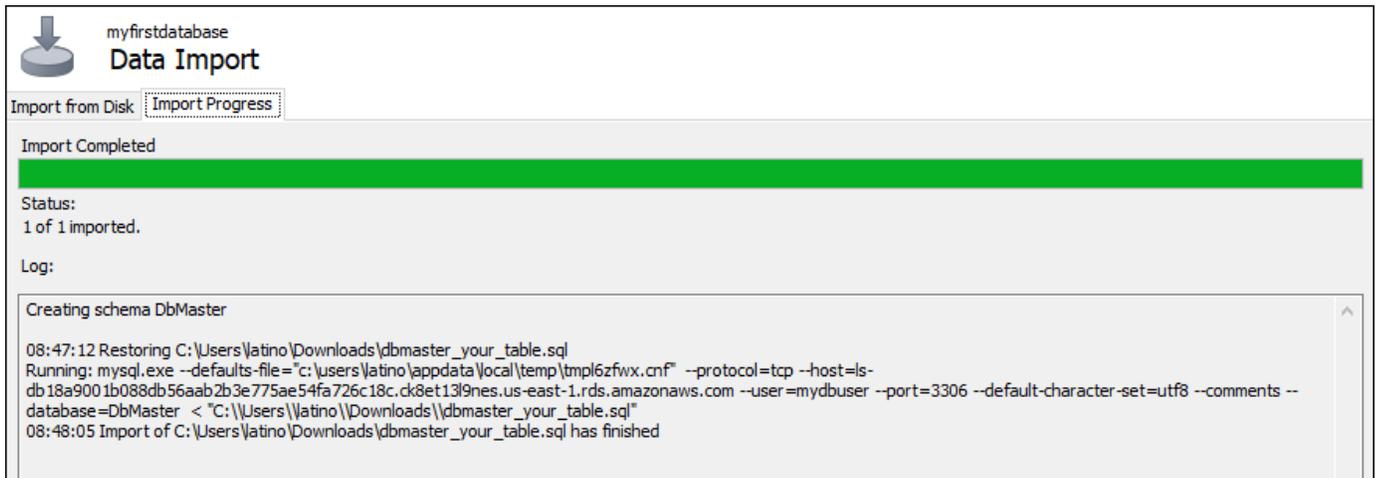


- 選擇省略按鈕以瀏覽您想要匯入的。SQL 檔案本機磁碟機。
- 選擇要匯入的。SQL 檔案，然後選擇 Open (開啟)。
- 選擇 Default Target Schema (預設目標結構描述) 下拉式功能表，然後選取要匯入檔案的現有資料庫。您也可以選擇 New (新建) 來建立新的資料庫。



- 選擇 Start Import (開始匯入)，即可開始匯入。

根據。SQL 檔案的大小，匯入作業可能需要幾分鐘或更久的時間。匯入完成後，您應該會看到類似如下的訊息：



## 將資 PostgreSQL 庫備份匯入至受管 Lightsail 資料庫

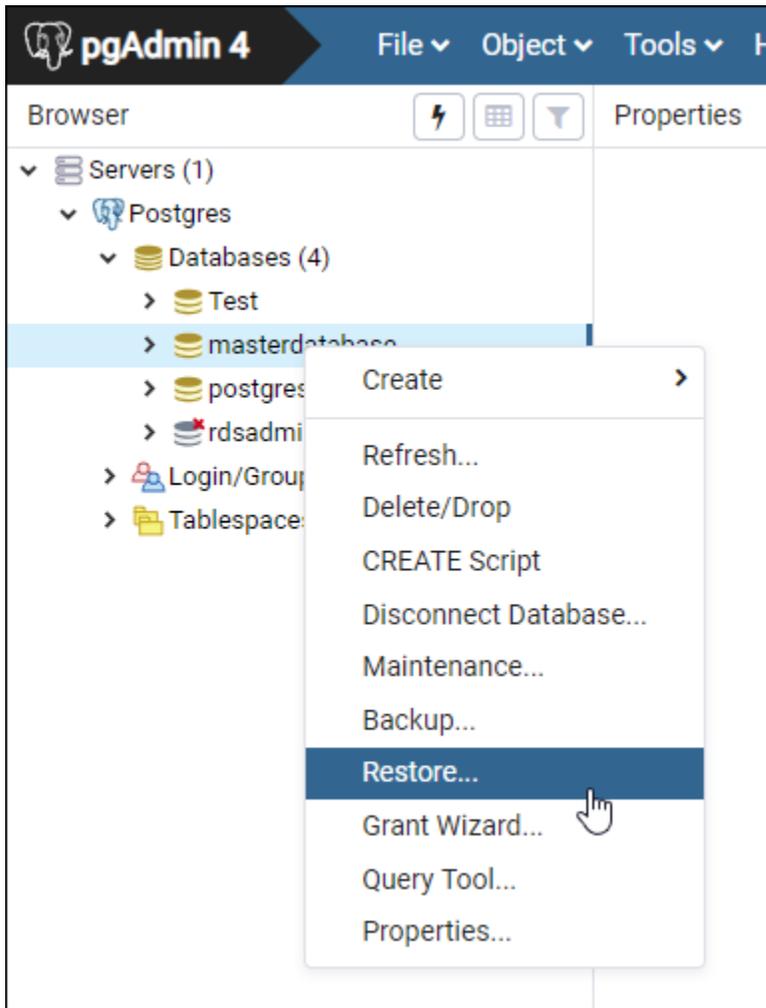
您可以使用 pgAdmin 將資料庫備份檔案匯入您的 PostgreSQL 受管資料庫。

### Note

若要了解如何將 pgAdmin 連接至資料庫，請參閱[連接至 PostgreSQL 資料庫](#)。如需建立 PostgreSQL 資料庫備份以匯入其他資料庫的詳細資訊，請參閱 pgAdmin 文件中的[Backup Dialog](#)。

### 將備份檔案匯入資料庫

1. 開啟 pgAdmin。
2. 在伺服器連線清單中，按兩下您在 Amazon Lightsail 中的 PostgreSQL 受管資料庫以連線到該資料庫。
3. 展開 Databases (資料庫) 節點。
4. 在要匯入資料庫備份檔案資料的資料庫上按一下滑鼠右鍵，然後選擇 Restore (還原)。

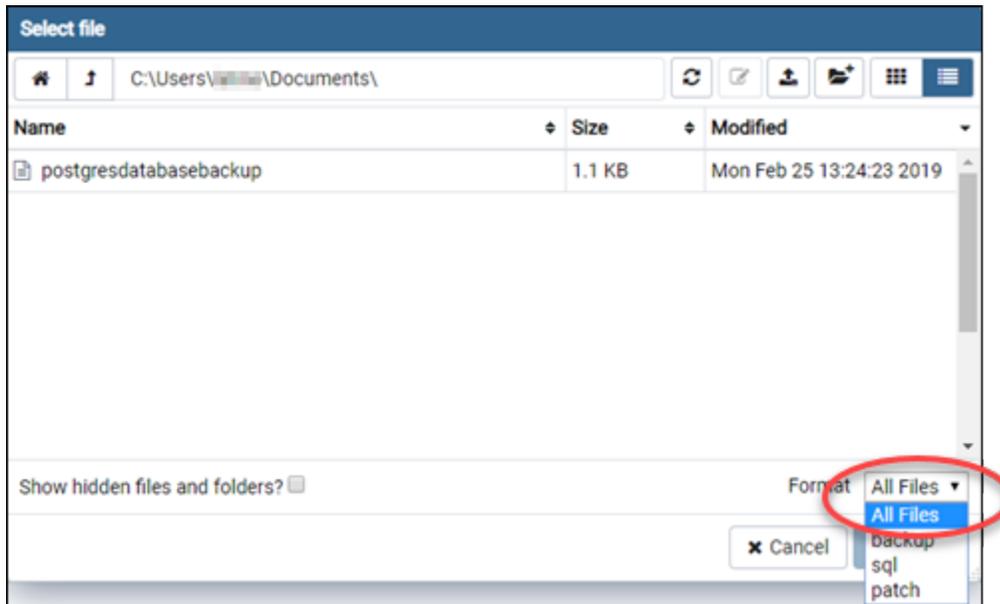


5. 在 Restore (還原) 表單中，填寫下列欄位：

- Format (格式) — 選擇備份檔案的格式。
- Filename (檔案名稱) — 選擇省略符號圖示，接著尋找並選擇本機磁碟機上的資料庫備份檔案。反白該檔案後，請選擇 Select (選取) 以返回 Restore (還原) 提示畫面。

**Note**

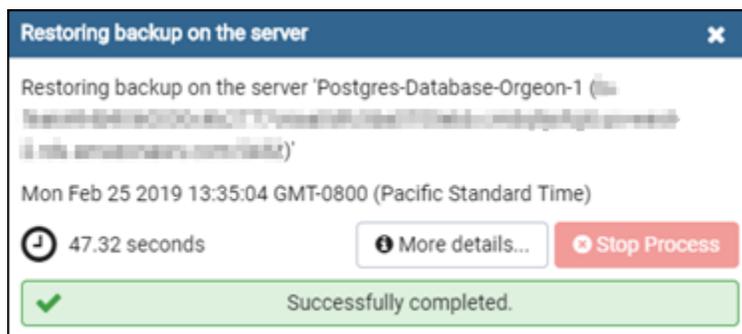
選擇 Format (格式) 下拉式功能表，然後選取 All files (所有檔案) 來檢視本機磁碟機上的所有檔案格式。系統可能會以不同於預設選用格式 (sql) 的檔案類型來儲存備份檔案。



- Number of jobs (任務數量) 和 Role name (角色名稱) — 請將這些欄位保留空白。

## 6. 選擇 Restore (還原) 開始匯入。

根據資料庫備份檔案的大小，匯入作業可能需要幾分鐘或更久的時間。匯入完成後，您應該會看到類似如下的訊息：



## 檢視您的 Lightsail 資料庫記錄和歷程記錄

在 Amazon Lightsail 主控台中檢視您的資料庫日誌和變更歷史記錄。資料庫日誌提供有用的資訊，可協助您診斷資料庫的問題。同樣的，資料庫歷程記錄可顯示資料庫所做的變更，讓您掌握問題與最近變更之間的關聯。

### 檢視您的資料庫日誌

1. 登入主 [Lightsail](#) 台。

2. 在 Lightsail 首頁上，選擇「資料庫」索引標籤。
3. 選擇要檢視日誌的資料庫名稱。
4. 選擇 Logs and history (日誌和歷程記錄) 索引標籤。

此頁面會顯示資料庫日誌和資料庫的變更歷程記錄。

5. 選擇資料庫日誌。下列資料庫日誌皆可供使用：

### MySQL 資料庫日誌

- 錯誤日誌 – mysqld 啟動和關閉時間的記錄。它還包含伺服器啟動、關閉及運作時的診斷訊息，例如錯誤、警告和備註。如需詳細資訊，請參閱 [MySQL 5.6](#)、[MySQL 5.7](#) 或 [MySQL 8.0](#) 文件中的錯誤日誌文章。
- 一般日誌 — mysqld 的一般作業記錄。用戶端連線或中斷連線時，伺服器會將資訊寫入此日誌，並記錄從用戶端接收的各個 SQL 陳述式。如需詳細資訊，請參閱 [MySQL 5.6](#)、[MySQL 5.7](#) 或 [MySQL 8.0](#) 文件中的一般查詢日誌文章。
- 慢查詢日誌 — 執行時間超過 long\_query\_time 秒數，且至少有 min\_examined\_row\_limit 列需要檢查之 SQL 陳述式的記錄。如需詳細資訊，請參閱 [MySQL 5.6](#)、[MySQL 5.7](#) 或 [MySQL 8.0](#) 文件中的慢查詢日誌文章。

#### Note

MySQL 資料庫預設會停用一般日誌和慢查詢日誌。藉由更新一些資料庫參數，您就可以啟用這些日誌，並開始收集資料。如需詳細資訊，請參閱在 [Amazon Lightsail 中啟用 MySQL 資料庫一般與慢查詢日誌](#)。

### PostgreSQL 資料庫日誌

- Postgres 日誌 – 資料庫啟動和關閉時間的記錄。該日誌可能也會包含診斷資訊，例如資料庫啟動、關閉和執行期間所出現的錯誤、警告、通知和偵錯訊息。如需詳細資訊，請參閱 [PostgreSQL 9.6](#)、[PostgreSQL 10](#)、[PostgreSQL 11](#) 或 [PostgreSQL 12](#) 文件中說明錯誤回報和記錄的文章。

### 主題

- [使用一般和緩慢的查詢記錄來監控 MySQL 查詢效 Lightsail](#)

## 使用一般和緩慢的查詢記錄來監控 MySQL 查詢效 Lightsail

針對 Amazon Lightsail 中的 MySQL 資料庫，預設會停用 [一般和慢速查詢記錄](#)。藉由更新一些資料庫參數，您就可以啟用這些日誌，並開始收集資料。使用 Lightsail API、AWS Command Line Interface (AWS CLI) 或開發套件來更新資料庫參數。在本指南中，我們將說明如何使用更新資料庫參數，AWS CLI 以及啟用一般和緩慢的查詢記錄檔。我們也會提供額外選項來控制一般與慢查詢日誌以及資料保留的處理方式。

### 先決條件

如果您尚未安裝和設定 AWS CLI，請先執行這項動作。如需詳細資訊，請參閱 [設定 AWS Command Line Interface 以與 Amazon Lightsail 搭配使用](#)。

### 在 Lightsail 主控台中啟用一般和緩慢的查詢記錄

若要在 Lightsail 主控台中啟用一般和緩慢的查詢記錄檔，您必須使用值更新 `general_log` 和 `slow_query_log` 資料庫參數 `log_output` 為 1，且參數 `FILE` 值為。

若要在 Lightsail 主控台中啟用一般和緩慢的查詢記錄

1. 開啟終端機或命令提示視窗。
2. 輸入下列命令將 `general_log` 參數更新為值 1，此為 `true` 或啟用。

```
aws lightsail update-relational-database-parameters --  
region Region --relational-database-name DatabaseName --parameters  
"parameterName=general_log,parameterValue=1,applyMethod=pending-reboot"
```

在命令中：

- *DatabaseName* 使用您的數據庫的名稱。
- *##* 與您 AWS 區域 的數據庫。

3. 輸入下列命令將 `slow_query_log` 參數更新為值 1，此為 `true` 或啟用。

```
aws lightsail update-relational-database-parameters --  
region Region --relational-database-name DatabaseName --parameters  
"parameterName=slow_query_log,parameterValue=1,applyMethod=pending-reboot"
```

在命令中：

- *DatabaseName* 使用您的數據庫的名稱。

- **##**與您 AWS 區域 的數據庫。
4. 輸入下列命令，將log\_output參數更新為的值FILE，這樣會將記錄資料寫入系統檔案，並使其能夠顯示在 Lightsail 主控台中。

```
aws lightsail update-relational-database-parameters --  
region Region --relational-database-name DatabaseName --parameters  
"parameterName=log_output,parameterValue=FILE,applyMethod=pending-reboot"
```

在命令中：

- *DatabaseName*使用您的數據庫的名稱。
  - **##**與您 AWS 區域 的數據庫。
5. 輸入下列命令重新啟動資料庫並使變更生效。

```
aws lightsail reboot-relational-database --region Region --relational-database-  
name DatabaseName
```

在命令中：

- *DatabaseName*使用您的數據庫的名稱。
- **##**與您 AWS 區域 的數據庫。

此時，資料庫會重新啟動並無法使用。等待幾分鐘，然後登入 [Lightsail 主控台](#)，以檢視資料庫的一般和緩慢查詢記錄。如需詳細資訊，請參閱[在 Amazon Lightsail 中檢視資料庫日誌和歷史記錄](#)。

#### Note

如需更新資料庫參數的詳細資訊，請參閱[在 Amazon Lightsail 中更新資料庫參數](#)。

## 控制其他資料庫日誌選項

若要控制 MySQL 一般與慢查詢日誌的其他選項，請更新以下參數：

- log\_output — 將此參數設為 TABLE。這會將一般查詢寫入 mysql.general\_log 表格，並將慢查詢寫入 mysql.slow\_log 表格。您也可以將 log\_output 參數設定為 NONE 以停用日誌記錄。

**Note**

設定 `log_output` 參數以 TABLE 停用 Lightsail 主控台中顯示的一般和緩慢查詢記錄檔資料。反之，您必須參閱資料庫的 `mysql.general_log` 和 `mysql.slow_log` 表格以檢視日誌資料。

- `long_query_time` - 若要避免快速執行查詢記錄於慢查詢日誌中，請為需記錄之最短查詢執行時間指定一個值，以秒為單位。預設為 10 秒，而下限為 0。若 `log_output` 參數設為 FILE，您可以指定以微秒解析度為單位的浮點值。若 `log_output` 參數設為 TABLE，您必須以秒解析度指定整數值。只有執行時間超過 `long_query_time` 參數值的查詢會記錄。例如，將 `long_query_time` 設為 0.1 可避免記錄任何在 100 毫秒內執行之查詢。
- `log_queries_not_using_indexes` — 若要將所有不使用索引的查詢記錄於慢查詢日誌中，請設為 1。預設為 0。將會記錄不使用索引的查詢，即使其執行時間低於 `long_query_time` 參數的值。

## 日誌資料保留

記錄啟用時，表格日誌會定期輪換或日誌檔案會定期刪除。此方法為預防措施，可降低大型日誌檔封鎖資料庫使用或影響效能的可能性。當 `log_output` 參數設為 FILE 或 TABLE，記錄會以下列方式處理：

- 當 FILE 日誌記錄啟用時，每個小時將檢視日誌檔，而早於 24 小時前的日誌檔將會刪除。在某些情況下，刪除後剩餘的總日誌檔案大小可能會超過資料庫配得之空間的 2% 閾值。在這些情況中，最大的日誌檔將被刪除，直到日誌檔大小不再超過閾值。
- TABLE 記錄啟用時，日誌表格在某些情況下會每 24 小時輪換。

在表格日誌使用的空間超過配得之儲存空間的 20% 時，或者所有日誌的總容量高於 10 GB 時就會發生輪換。

若資料庫使用的空間總量高於資料庫配置儲存空間的 90%，日誌輪換的閾值會降低。

在表格日誌使用的空間超過配得之儲存空間的 10% 時，或者所有日誌的總容量高於 5 GB 時，日誌表格就會輪換。

您可訂閱 `low_free_storage` 事件，日誌表格輪換以釋放空間時就會通知您。

- 輪換日誌資料表時，目前日誌資料表會複製到備份日誌資料表，並移除目前日誌資料表中的項目。如果備份日誌資料表已存在，則其會在目前日誌資料表複製到備份之前

刪除。您可以查詢備份日誌表格。mysql.general\_log 資料表的備份日誌資料表名為 mysql.general\_log\_backup。mysql.slow\_log 資料表的備份日誌資料表名為 mysql.slow\_log\_backup。

- 您可以呼叫 mysql.general\_log 以輪換 mysql.rds\_rotate\_general\_logprocedure 資料表。您可以呼叫 mysql.slow\_log 以輪換 mysql.rds\_rotate\_slow\_logprocedure 資料表。
- 表格日誌會在資料庫版本升級時輪換。

## 停用 point-in-time 資料 Lightsail 的備份

請使用下列程序來停用 Lightsail 受管理資料庫的 point-in-time 備份。

### Important

使用 point-in-time 備份，如果數據庫失敗，您可以輕鬆恢復數據。建議您為 Lightsail 管理的資料庫保持啟用時間點備份。

## 先決條件

使用 AWS Command Line Interface (AWS CLI) 或啟用或停 AWS CloudShell 用 Lightsail 資料庫的 point-in-time 備份。CloudShell 是以瀏覽器為基礎的預先驗證殼層，您可以直接從 Lightsail 主控台啟動。如需詳細資訊，請參閱 [設定 AWS CLI 供 Lightsail 作業使用](#) 和 [使用管理 Lightsail 資源 AWS CloudShell](#)。

## 停用資料庫 point-in-time 備份

若要在 Lightsail 中停用受管理資料庫的 point-in-time 備份，您必須使用的 update-relational-database Lightsail 命令更新資料庫。AWS CLI 如需詳細資訊，請參閱 AWS CLI 命令參考 [update-relational-database](#) 中的。

- 在終端機、命令提示字元或 CloudShell 視窗中輸入下列命令：

```
aws lightsail update-relational-database --region Region --relational-database-name DatabaseName --disable-backup-retention --apply-immediately
```

指令中的 `--disable-backup-retention` 值會關閉指定資料庫的 point-in-time 備份。在命令中：

- `DatabaseName` 使用您的數據庫的名稱。
- `##` 與您 AWS 區域的數據庫。

您應該會看到狀態為的作業回應 Succeeded。更新資料庫的狀態會在短時間內變更為 [修改]。當資料庫的狀態變回 [可用] 時，將會停用 point-in-time 還原選項，如下列範例所示。

```
AWS CloudShell
us-west-2

"operations": [
  {
    "id": "a1e099c0-3e5e-4d11-bd7c-49108aa412c5",
    "resourceName": "Database-1",
    "resourceType": "RelationalDatabase",
    "createdAt": "2023-09-28T16:29:15.186000+00:00",
    "location": {
      "availabilityZone": "us-west-2a",
      "regionName": "us-west-2"
    },
    "isTerminal": true,
    "operationDetails": "",
    "operationType": "UpdateRelationalDatabase",
    "status": "Succeeded",
    "statusChangedAt": "2023-09-28T16:29:15.491000+00:00"
  }
]
```

#### Note

若要啟用 point-in-time 備份，請執行前面列出的相同命令，但改為使用 `--enable-backup-retention` 參數。

## 使用快照備份您的 Lightsail 資料庫

您可以在 Amazon Lightsail 中建立受管資料庫的快照。快照是您資料庫的複本，若出現意外，您可用其來還原資料庫。您亦可使用快照來建立採用不同計畫的新資料庫，例如高可用性或標準計畫。

建立標準資料庫的快照時，將無法使用該資料庫幾秒鐘到幾分鐘，時間長度視其大小而定。快照操作不會影響高可用性資料庫，因為快照係使用待命資料庫來建立。

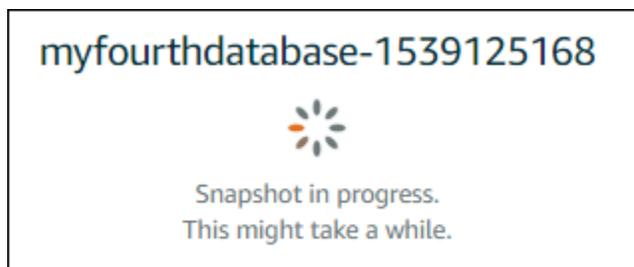
### 建立您資料庫的快照

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁上，選擇「資料庫」索引標籤。
3. 選擇您要建立快照的資料庫名稱。
4. 選擇 Snapshots & restore (快照和還原) 索引標籤。
5. 在頁面的手動快照部分中，選擇 Create snapshot (建立快照)，然後輸入快照的名稱。

資源名稱：

- 每個 Lightsail 帳戶 AWS 區域 中的每個項目都必須是唯一的。
  - 必須包含 2 至 255 個字元。
  - 開頭和結尾必須是英數字元或數字。
  - 可以包含英數字元、數字、句點、破折號和底線。
6. 選擇建立。

快照建立程序將開始，畫面會顯示 Snapshot in progress (快照處理中) 狀態。



快照建立程序完成後，新的快照會列於 Recent snapshots (最新的快照) 部分底下。您也可以直接在 Lightsail 首頁的 [快照] 索引標籤下檢視您帳戶的所有快照。



## 後續步驟

快照就緒後，即可從快照建立新的資料庫，此為原始資料庫的複本。如需詳細資訊，請參閱[透過快照建立資料庫](#)。

### 主題

- [從 point-in-time 備份還原資料庫](#)
- [在 Lightsail 中從快照集建立受管理的資料庫](#)

## 從 point-in-time 備份還原資料庫

您可以使用 Amazon Lightsail 中的 point-in-time 備份來建立新的受管資料庫。資料庫的 Point-in-time 備份以 5 分鐘為單位提供，以及前七天的增量。這能夠讓您將故障的資料庫還原至上週的特定日期和時間。

您也可以從快照建立新的資料庫。如需詳細資訊，請參閱[在 Amazon Lightsail 中從快照建立資料庫](#)。

若要從 point-in-time 備份建立資料庫

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁上，選擇「資料庫」索引標籤。
3. 選擇您要變更計畫的資料庫名稱。
4. 選擇 Snapshots and restore (快照和還原) 索引標籤。
5. 在 Emergency restore (緊急還原) 部分，選取您要用於新資料庫的備份日期和時間。

## Emergency restore

Lightsail retains a week of minute-to-minute backups of your database. Select a point in time from the last week to create a new database from that backup.

 If you recently enabled data import mode, you can only restore from a point in time after you disabled it.

Today ▼ , 17 ▼ : 50 ▼ — Pacific Daylight Time (GMT-7) ▼

[Restore to new database](#)

6. 選擇 Restore to new database (還原至新的資料庫)。
7. 在 Create a new database (建立新的資料庫) 頁面，選擇 Change zone (變更區域) 以選取不同的可用區域。您的新資料庫會在與您先前所選快照相同的 AWS 區域中建立。
8. 選擇您的新資料庫計畫。

選擇高可用性或標準資料庫計畫。以高可用性計畫建立的資料庫會有一個主要資料庫，並在另一個可用區域有一個次要備用資料庫 (用於容錯移轉支援)。如需詳細資訊，請參閱[高可用性資料庫](#)。

### Note

您無法選擇小於原始資料庫之計畫的資料庫計畫。

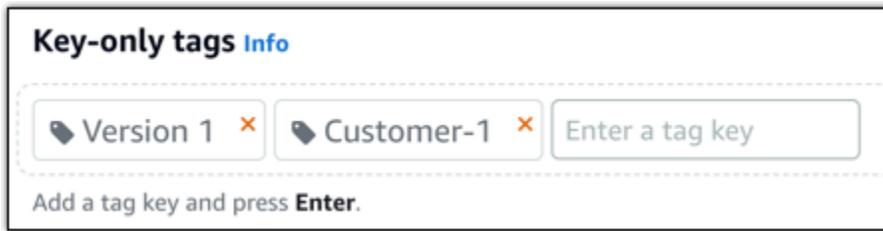
9. 為您的資料庫輸入名稱。

資源名稱：

- 每個 Lightsail 帳戶 AWS 區域 中的每個項目都必須是唯一的。
- 必須包含 2 至 255 個字元。
- 開頭和結尾必須是英數字元或數字。
- 可以包含英數字元、數字、句點、破折號和底線。

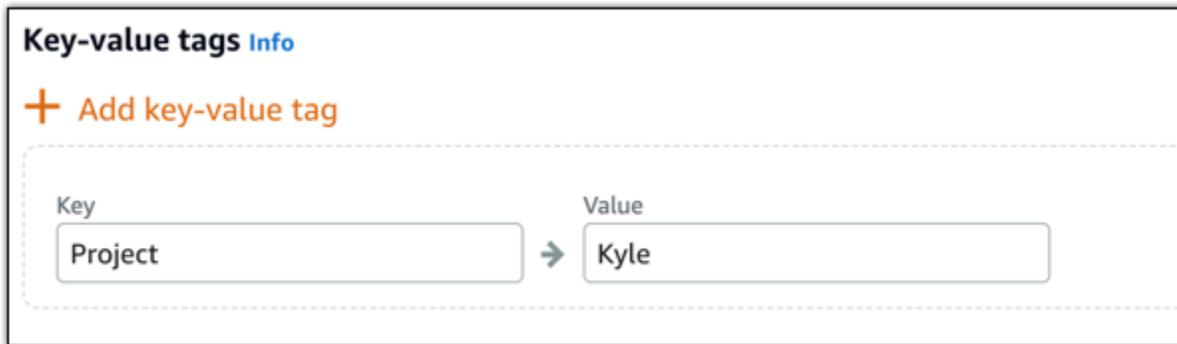
10. 選擇下列其中一個選項以新增標籤至您的資料庫：

- Add key-only tags (新增僅索引鍵標籤) 或 Edit key-only tags (編輯僅索引鍵標籤) (若標籤已新增)。在標籤索引鍵文字方塊中輸入新的標籤，接著按 Enter (輸入)。輸入標籤以新增之後，請選擇 Save (儲存)，如果不要新增則選擇 Cancel (取消)。



- Create a key-value tag (建立索引鍵值標籤)，接著將索引鍵輸入 Key (索引鍵) 文字方塊，將值輸入 Value (值) 文字方塊。完成輸入標籤後，請選擇 Save (儲存)，如果不要新增則選擇 Cancel (取消)。

鍵值標籤在儲存前一次只能新增一個。若要新增超過一個索引鍵值標籤，請重複之前的步驟。



#### Note

如需有關僅索引鍵和索引鍵值標籤的詳細資訊，請參閱[標籤](#)。

## 11. 選擇建立資料庫。

在幾分鐘內，您的新 Lightsail 資料庫即可使用新的資料庫計劃或服務包。

## 後續步驟

在新資料庫啟動和執行後完成以下動作：

- 如果您不再需要原始資料庫，請將其刪除。如需詳細資訊，請參閱[刪除資料庫](#)。
- 從 point-in-time 備份建立的資料庫會設定為使用 Lightsail 建立的強式密碼。如需詳細資訊，請參閱[管理資料庫密碼](#)。

## 在 Lightsail 中從快照集建立受管理的資料庫

如果原始資料庫出現問題，您可以從 Amazon Lightsail 中的快照建立新的受管資料庫。您亦可變更資料庫計畫，例如高可用性或標準計畫。您也可以從原始資料庫的 point-in-time 備份建立新資料庫。如需詳細資訊，請參閱在 [Amazon Lightsail 中從 point-in-time 備份建立資料庫](#)。

建立複本資料庫時，您可選擇不同或較原始資料庫更大的計畫。然而，您無法選擇小於原始資料庫的計畫。

### Note

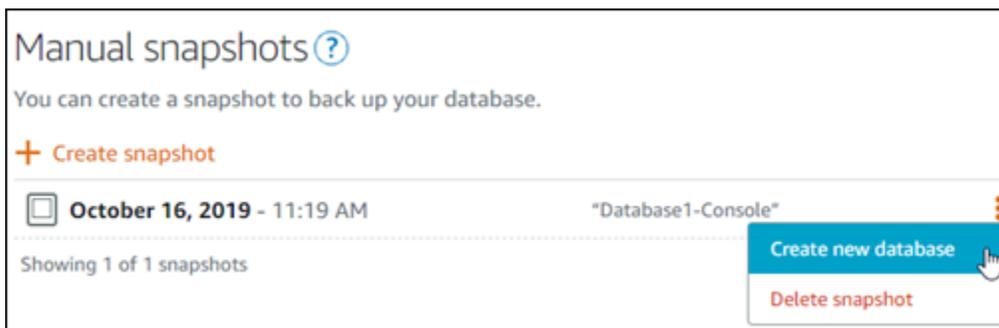
以高可用性計畫建立的資料庫會有一個主要資料庫，並在另一個可用區域有一個次要備用資料庫 (用於容錯移轉支援)。如需詳細資訊，請參閱 [高可用性資料庫](#)。

### 若要從快照建立資料庫

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁上，選擇「資料庫」索引標籤。
3. 選擇您要從快照建立新資料庫來進行複製的資料庫名稱。
4. 選擇 Snapshots & restore (快照和還原) 索引標籤。
5. 在頁面的 Manual snapshots (手動快照) 部分中，在您要建立的新資料庫旁選擇動作選單圖示 (:)，然後選擇 Create new database (建立新資料庫)。

### Note

您必須使用資料庫的快照來執行此操作。若尚未建立快照，請參閱 [建立資料庫快照](#)。



6. 選擇 Create new database (建立新的資料庫)。

- 在 **Create a new database (建立新的資料庫)** 頁面，選擇 **Change zone (變更區域)** 以選取不同的可用區域。您的新資料庫會建立於您先前所選快照的相同 AWS 區域。
- 選擇您的新資料庫計畫。

選取高可用性或標準資料庫計畫。以高可用性計畫建立的資料庫會有一個主要資料庫，並在另一個可用區域有一個次要備用資料庫 (用於容錯移轉支援)。如需詳細資訊，請參閱 [高可用性資料庫](#)。

**Note**

您選擇的資料庫計畫不得小於用來建立快照之原始資料庫所採取的計畫。

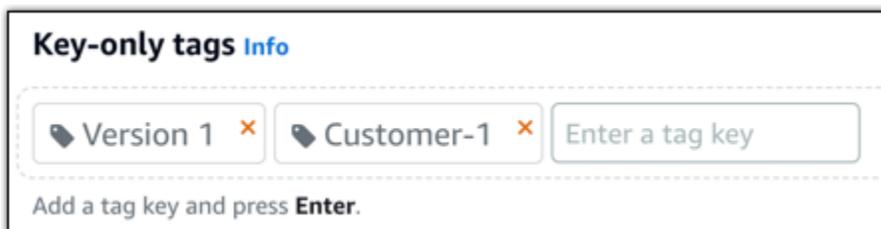
- 為您的資料庫輸入名稱。

資源名稱：

- 每個 Lightsail 帳戶 AWS 區域 中的每個項目都必須是唯一的。
- 必須包含 2 至 255 個字元。
- 開頭和結尾必須是英數字元或數字。
- 可以包含英數字元、數字、句點、破折號和底線。

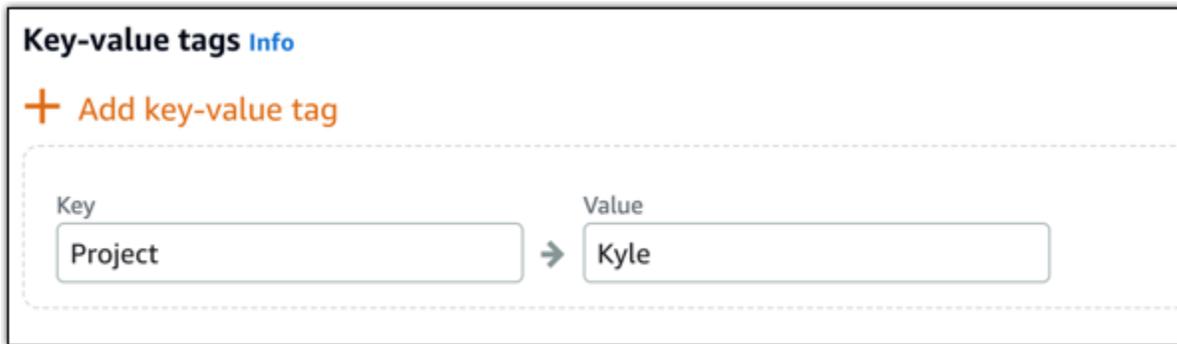
- 選擇下列其中一個選項以新增標籤至您的資料庫：

- Add key-only tags (新增僅索引鍵標籤)** 或 **Edit key-only tags (編輯僅索引鍵標籤)** (若標籤已新增)。在標籤索引鍵文字方塊中輸入新的標籤，接著按 **Enter (輸入)**。輸入標籤以新增之後，請選擇 **Save (儲存)**，如果不要新增則選擇 **Cancel (取消)**。



- Create a key-value tag (建立索引鍵值標籤)**，接著將索引鍵輸入 **Key (索引鍵)** 文字方塊，將值輸入 **Value (值)** 文字方塊。完成輸入標籤後，請選擇 **Save (儲存)**，如果不要新增則選擇 **Cancel (取消)**。

鍵值標籤在儲存前一次只能新增一個。若要新增超過一個索引鍵值標籤，請重複之前的步驟。



**Key-value tags** Info

+ Add key-value tag

Key: Project → Value: Kyle

**Note**

如需有關僅索引鍵和索引鍵值標籤的詳細資訊，請參閱[標籤](#)。

## 11. 選擇建立資料庫。

在幾分鐘內，您的新 Lightsail 資料庫即可使用新的資料庫計劃或服務包。

## 後續步驟

在新資料庫啟動和執行後完成以下動作：

- 若您建立新資料庫是為了替換現有資料庫，而且您的應用程式與現有資料庫相依，請務必將應用程式的依存項目更新為新的資料庫。
- 如果您不再需要原始資料庫，請將其刪除。如需詳細資訊，請參閱[刪除資料庫](#)。
- 從快照建立的資料庫會設定為使用 Lightsail 建立的強式密碼。如需詳細資訊，請參閱[管理資料庫密碼](#)。

## 下載 SSL/TLS 憑證，以確保應用程式與 Lightsail 資料庫的安全連線

您可以使用應用程式的安全通訊端層 (SSL) 或傳輸層安全性 (TLS)，在執行 MySQL 或 PostgreSQL 的 Amazon Lightsail 中加密與受管資料庫的連線。每個資料庫引擎都有自己實作 SSL/TLS 的程序。如需詳細資訊，請參閱[使用 SSL 連接到 MySQL 資料庫](#)或[使用 SSL 連接到 PostgreSQL 資料庫](#)。

**Note**

可供下載的憑證會標示為適用於 Amazon Relational Database Service 服務 (Amazon RDS) , 但也適用於 Lightsail 中的受管資料庫。

## 所有 AWS 區域的憑證套件

若要取得同時包含所有中繼憑證和根憑證的憑證組合，或 AWS 區域者如果您的應用程式位於 [Microsoft Windows](#) 且需要 PKCS7 檔案，請參閱 [Amazon 關聯式資料庫服務使用者指南中的所有 AWS 區域憑證服務包](#)。

此根憑證是可信任的根實體，在大多數情況下都適用。但是，如果您的應用程式不接受憑證鏈，則此憑證就不適用。如果您的應用程式不接受憑證鏈，請參閱本文件的下一節。

## 特定 AWS 區域的憑證套件

若要取得同時包含特定中繼憑證和根憑證的憑證服務包 AWS 區域，請參閱 [Amazon Relational Database Service 使用者指南中的特定 AWS 區域憑證組合](#)。

## 更新您的資料庫的 CA 憑證版本

Amazon Lightsail 已發佈新的憑證授權單位 (CA) 憑證，以使用 SSL/TLS 連接到受管資料庫。本指南說明如何升級至新的 CA 憑證。您只能使用 [update-relational-database](#) API 動作來升級憑證。新憑證稱為 `rds-ca-rsa2048-g1`、`rds-ca-rsa4096-g1`、和 `rds-ca-ecc384-g1`。舊憑證稱為 `rds-ca-2019`。我們提供 CA 憑證作為安 AWS 全性最佳做法。如需受管理資料庫的 CA 憑證及支援的相關資訊 AWS 區域，請參閱 [下載受管理資料庫的憑SSL證](#)。

舊的 CA 憑證 (`rds-ca-2019`) 將於 2024 年 8 月 22 日到期。因此，我們強烈建議您盡快完成本指南中的步驟，以將受管資料庫修改為使用新憑證。如果您的應用程式未使用 SSL/連線至 Lightsail 受管理的資料庫 TLS，則不需要採取任何動作。如果這些步驟未完成，您的應用程式將無法在 2024 年 8 月 22 日 TLS 之後使用 SSL/連線到受管理的資料庫。

根據預設，在 2024 年 1 月 26 日之後建立的新受管理資料庫將使用 `rds-ca-rsa2048-g1` 憑證。如果您想要暫時修改新的受管理資料庫以使用舊憑證 (`rds-ca-2019`)，您可以使用 AWS Command Line Interface (AWS CLI)。在 2024 年 1 月 26 日之前建立的任何受管理的資料庫都會使用憑 `rds-ca-2019` 證，直到您將它們更新為 `rds-ca-rsa2048-g1`、`rds-ca-rsa4096-g1`、和 `rds-ca-ecc384-g1` 憑證為止。

**Note**

在實際執行環境中使用這些步驟之前，請先在開發或預備環境中測試本指南中的步驟。

## 必要條件

- 在完成此程序中的步驟之前，請先更新資料庫用戶端應用程式以使用新的 SSL/TLS 憑證。

更新新 SSL/TLS 憑證應用程式的方法取決於您的特定應用程式。與您的應用程式開發人員合作，為您的應用程式更新 SSL/TLS 憑證。若要進一步了解如何更新新 SSL/TLS 憑證的應用程式，請參閱 Amazon 關聯式資料 [SQL 庫服務使用者指南中的更新 SSL 應用程式以 Connect 到我的資料 SQL 庫執行個體](#)，或 [使用新的 SSL/TLS 憑證更新應用程式以 Connect 到 Postgre 資料庫執行個體](#)。TLS

- 在本指南中，您將使用 AWS CloudShell 來執行升級。CloudShell 是一個以瀏覽器為基礎的預先驗證殼層，您可以直接從 Lightsail 主控台啟動。使用時 CloudShell，您可以使用您偏好的外圍程序來運行 AWS Command Line Interface (AWS CLI) 命令 PowerShell，例如 Bash 或 Z 外殼。無需下載或安裝命令列工具即可執行此操作。如需有關如何設定和使用的詳細資訊 CloudShell，請參閱 [Lightsail AWS CloudShell](#) 中的。

## 識別受管理資料庫的作用中 CA 憑證

請完成下列步驟，以識別 Lightsail 資料庫執行個體的作用中 CA 憑證。

- 開啟「終端機」或「命令提示字元」視窗。[AWS CloudShell](#)
- 輸入下列命令，以識別受管理資料庫的作用中 CA 憑證。

```
aws lightsail get-relational-database --relational-database-name DatabaseName --  
region DatabaseRegion | grep "caCertificateIdentifier"
```

在命令中，替換 *DatabaseName* 使用您要修改的數據庫的名稱，並且 *DatabaseRegion* 與數 AWS 區域 據庫實例所在的。

### 範例

```
aws lightsail get-relational-database --relational-database-name Database-1 --  
region us-east-1 | grep "caCertificateIdentifier"
```

該命令將返回數據庫的活動 CA 證書的 ID。

## 範例

```
"caCertificateIdentifier": "rds-ca-rsa2048-g1"
```

## 修改受管資料庫以使用新 CA 憑證

請完成下列步驟，在 Lightsail 中修改受管理的資料庫，以使用其中一個新的 CA 憑證 (rds-ca-rsa2048-g1、rds-ca-rsa4096-g1、和 rds-ca-ecc384-g1)。

### Important

更新資料庫上的 CA 憑證之前，請先更新任何使用 CA 憑證的用戶端應用程式。

1. 開啟「終端機」或「命令提示字元」視窗。[AWS CloudShell](#)
2. 輸入下列命令，在受管理的資料庫上使用新憑證。

```
aws lightsail update-relational-database --relational-database-name DatabaseName --  
region DatabaseRegion --ca-certificate-identifier rds-ca-rsa2048-g1
```

在命令中，替換 *DatabaseName* 使用您要修改的數據庫的名稱，並且 *DatabaseRegion* 與數 AWS 區域 據庫實例所在的。

## 範例

```
aws lightsail update-relational-database --relational-database-name Database-1 --  
region us-east-1 --ca-certificate-identifier rds-ca-rsa2048-g1
```

您受管理的資料庫所使用的 CA 憑證會在資料庫的下一個維護時段期間進行更新，或者如果您將 `--apply-immediately` 參數新增至命令結尾，則會立即更新。

## 修改受管資料庫以使用舊 CA 憑證

請完成下列步驟，在 Lightsail 中修改受管理的資料庫，以使用舊的 CA 憑證 (rds-ca-2019)。只有在您遇到其中一個新憑證 (rds-ca-rsa2048-g1、和 rds-ca-ecc384-g1) 的嚴重問題 rds-ca-rsa4096-g1，且需要暫時還原舊憑證時，才執行此動作。

**⚠ Important**

更新資料庫上的 CA 憑證之前，請先更新任何使用 CA 憑證的用戶端應用程式。

1. 開啟「終端機」或「命令提示字元」視窗。[AWS CloudShell](#)
2. 輸入下列命令，以在您的受管資料庫上使用 rds-ca-2019。

```
aws lightsail update-relational-database --relational-database-name DatabaseName --  
region DatabaseRegion --ca-certificate-identifier rds-ca-2019
```

在命令中，替換 *DatabaseName* 使用您要修改的資料庫的名稱，並且 *DatabaseRegion* 與數 AWS 區域 據庫實例所在的。

**範例**

```
aws lightsail update-relational-database --relational-database-name Database-1 --  
region us-east-1 --ca-certificate-identifier rds-ca-2019
```

您受管理的資料庫所使用的 CA 憑證會在資料庫的下一個維護時段期間進行更新，或者如果您將 `--apply-immediately` 參數新增至命令結尾，則會立即更新。

## 排程 Lightsail 資料庫的維護和備份

當 Amazon Lightsail 支援新版本的資料庫時，您現有的受管資料庫即可升級至該資料庫。升級有兩種：次要版本升級和主要版本升級。目前，Lightsail 僅支援次要版本升級。

會在資料庫的偏好維護時段期間自動執行次要版本升級以及其他資料庫維護任務。首選的維護時段是 30 分鐘的時段，每個 AWS 區域時段從 8 小時的時間段中隨機選擇。它會在一週內的哪天隨機發生。會在偏好的備份時段期間執行資料庫備份。首選的備份時段是 30 分鐘的時間從每 AWS 區域個 8 小時的時間段中隨機選擇。它也會在一週內的哪天隨機發生。

**i Note**

如需每個區域中偏好的維護時段時間範圍的詳細資訊，請參閱 Amazon Relational Database Service (Amazon RDS) 文件中的[維護資料庫執行個體](#)指南。如需每個區域之偏好備份時段時間範圍的更多資訊，請參閱 Amazon RDS 文件中的[使用備份](#)指南。

本指南說明如何變更偏好的維護和備份時段，讓這些時段在您的資料庫負載最低時發生。

## 必要條件

您必須使用 AWS Command Line Interface (AWS CLI) 來變更資料庫偏好的維護和備份時段。

完成下列先決條件：

- 安裝 AWS CLI — 如需詳細資訊，請參閱[安裝 AWS CLI](#)。
- 配置 AWS CLI — 如需詳細資訊，請參閱[配置 AWS CLI](#)。

## 為您的資料庫變更維護時段

您的資料庫在維護或備份操作期間可能無法使用。因此，您可能想要將偏好的維護或備份時段變更到您的資料庫負載最低的時間。

若要為您的資料庫變更維護時段

1. 開啟終端機或命令提示視窗。
2. 輸入下列命令來取得您要變更維護時段的資料庫名稱：

```
aws lightsail get-relational-databases
```

您應該會看到類似以下範例的結果：

```
{
  "relationalDatabases": [
    {
      "name": "myfirstttestdatabase",
      "arn": "arn:aws:lightsail:us-east-1:13869536:relationaldatabase:mysql_5_7-13869536-084884343714-8e39329c39ee-1538755937.532",
      "supportCode": "084884343714/ls-8e39329c39ee-1538755937.532",
      "createdAt": 1538755937.532,
      "location": {
        "availabilityZone": "us-east-1a",
        "regionName": "us-east-1"
      },
      "resourceType": "RelationalDatabase",
      "relationalDatabaseBlueprintId": "mysql_5_7",
      "relationalDatabaseBundleId": "medium_1_0",
      "masterDatabaseName": "myseconddb",
      "hardware": {
        "cpuCount": 2,
        "diskSizeInGb": 120,
        "ramSizeInGb": 4.0
      },
      "state": "available",
      "backupRetentionEnabled": false,
      "pendingModifiedValues": {},
      "engine": "mysql",
      "engineVersion": "5.7.23",
      "masterUsername": "myfirstuser",
      "parameterApplyStatus": "in-sync",
      "preferredBackupWindow": "08:49-09:19",
      "preferredMaintenanceWindow": "mon:10:16-mon:10:46",
      "publiclyAccessible": true,
      "masterEndpoint": {
        "port": 3306,
        "address": "i-8a19039e29aac346e5fa1a25a54e7699c14f44:db:mysql-57-13869536-us-east-1.rds.amazonaws.com"
      },
      "pendingMaintenanceActions": []
    }
  ]
}
```

### Note

如果未列出您要修改的資料庫，請確認已針對資料庫所 AWS 區域 在位置設定您 AWS CLI 的資料庫。如需詳細資訊，請參閱[設定 AWS CLI](#)。

- 反白顯示您想要修改的資料庫名稱，然後按 Ctrl+C (Ctrl+C) (如果您使用的是 Windows)，或者按 Cmd+C (Cmd+C) (如果您使用的是 macOS)，來將該名稱複製到您的剪貼簿，讓您可以在下一個步驟使用。

```
{
  "relationalDatabases": [
    {
      "name": "myfirstttestdatabase",
      "arn": "arn:aws:lightsail:us-east-1:13869536:relationaldatabase:mysql_5_7-13869536-084884343714-8e39329c39ee-1538755937.532",
      "supportCode": "084884343714/ls-8e39329c39ee-1538755937.532",
      "createdAt": 1538755937.532,
      "location": {
        "availabilityZone": "us-east-1a",
        "regionName": "us-east-1"
      },
      "resourceType": "RelationalDatabase",
      "relationalDatabaseBlueprintId": "mysql_5_7",
      "relationalDatabaseBundleId": "medium_1_0",
      "masterDatabaseName": "myseconddb",
      "hardware": {
        "cpuCount": 2,
        "diskSizeInGb": 120,
        "ramSizeInGb": 4.0
      },
      "state": "available",
      "backupRetentionEnabled": false,
      "pendingModifiedValues": {},
      "engine": "mysql",
      "engineVersion": "5.7.23",
      "masterUsername": "myfirstuser",
      "parameterApplyStatus": "in-sync",
      "preferredBackupWindow": "08:49-09:19",
      "preferredMaintenanceWindow": "mon:10:16-mon:10:46",
      "publiclyAccessible": true,
      "masterEndpoint": {
        "port": 3306,
        "address": "i-8a19039e29aac346e5fa1a25a54e7699c14f44:db:mysql-57-13869536-us-east-1.rds.amazonaws.com"
      },
      "pendingMaintenanceActions": []
    }
  ]
}
```

- 根據於您所變更的慣用時段，輸入以下其中一個命令。

- 輸入以下命令來變更資料庫維護時段。

```
aws lightsail update-relational-database --relational-database-name DatabaseName
--preferred-maintenance-window MaintenanceWindow
```

在命令中：

- *DatabaseName* 與數據庫的名稱。
- *MaintenanceWindow* 與新的維護窗口的時間框架。

以 `ddd : hh24 : mi-ddd : hh24 : mi` 格式定義偏好的維護時段時間。此時段也必須使用國際標準時間 (UTC) 格式和定義最短時段為 30 分鐘。偏好的維護時段不能與偏好的備份時段重疊。

範例：

```
aws lightsail update-relational-database --relational-database-
name myproductiondb --preferred-maintenance-window Tue:16:00-Tue:16:30
```

- 輸入以下命令來變更資料庫備份時段。

```
aws lightsail update-relational-database --relational-database-name DatabaseName
--preferred-backup-window BackupWindow
```

在命令中：

- *DatabaseName* 與數據庫的名稱。
- *BackupWindow* 與新的備份窗口時間範圍。

以 `hh24 : mi-hh24 : mi` 格式定義偏好的備份時段範圍。此時段也必須使用國際標準時間 (UTC) 格式和定義最短時段為 30 分鐘。偏好的備份時段不能與偏好的維護時段重疊。

範例：

```
aws lightsail update-relational-database --relational-database-
name myproductiondb --preferred-backup-window 14:00-14:30
```

您應該會看到類似以下範例的結果：

```
{
  "operations": [
    {
      "id": "xxxxxxxx-xxxx-4xxx-xxxx-xxxxxxxxxxxx",
      "resourceName": "myfirsttestdatabase",
      "resourceType": "RelationalDatabase",
      "createdAt": 1539124310.116,
      "location": {
        "availabilityZone": "us-east-1a",
        "regionName": "us-east-1"
      },
      "isTerminal": true,
      "operationType": "UpdateRelationalDatabase",
      "status": "Succeeded",
      "statusChangedAt": 1539124310.283
    }
  ]
}
```

## 後續步驟

以下是可協助您管理資料庫的一些指南：

- [設定資料庫的資料匯入模式](#)
- [為資料庫設定公有模式](#)
- [管理資料庫密碼](#)
- [連線至 MySQL 資料庫](#)
- [連線至 PostgreSQL 資料庫](#)
- [將資料匯入 MySQL 資料庫](#)
- [將資料匯入 PostgreSQL 資料庫](#)
- [建立資料庫快照](#)

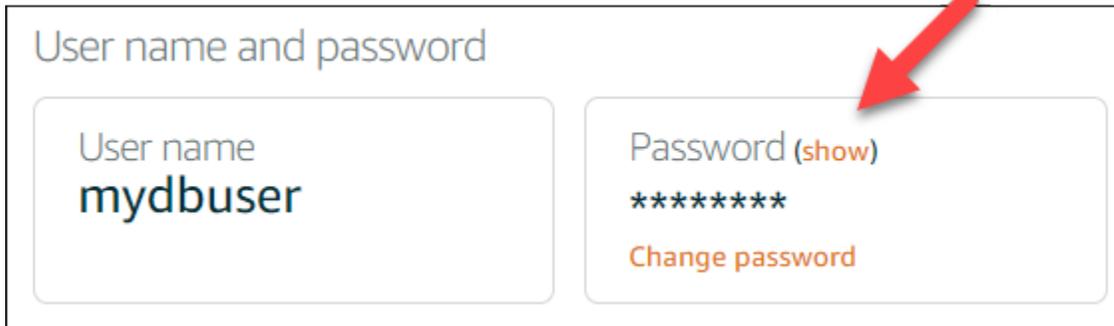
## 變更您的資料庫密碼

當您在 Amazon Lightsail 中建立新資料庫時，您可以讓 Lightsail 為您建立強式密碼，也可以指定您自己的密碼。您可以隨時在 Lightsail 主控台中檢視或變更目前的資料庫密碼。

### 管理資料庫密碼

1. 登入主 [Lightsail](#) 台。

2. 在 Lightsail 首頁上，選擇「資料庫」索引標籤。
3. 選擇您想要管理密碼的資料庫名稱。
4. 在 Connect (連線) 的索引標籤 User name and passwords (使用者名稱和密碼) 區段下，以選擇 Show (顯示) 來檢視目前的資料庫密碼。



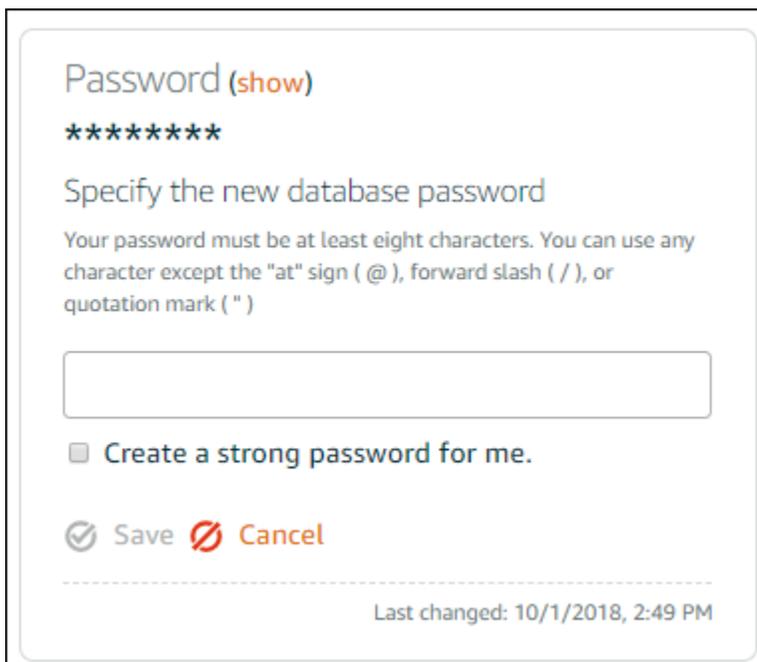
User name and password

User name  
mydbuser

Password (show)  
\*\*\*\*\*  
Change password

5. 若要變更資料庫密碼，請選擇 Change password (變更密碼)。

您可以選擇讓 Lightsail 為您建立強式密碼，也可以在文字方塊中輸入您自己的密碼。密碼可包含任何能印出的 ASCII 字元，但 "/"、"'" 或 "@" 除外。對於 MySQL 資料庫，密碼必須包含 8 到 41 個字元。對於 PostgreSQL，密碼必須包含 8 到 128 個字元。



Password (show)  
\*\*\*\*\*

Specify the new database password

Your password must be at least eight characters. You can use any character except the "at" sign ( @ ), forward slash ( / ), or quotation mark ( " )

Create a strong password for me.

Save  Cancel

-----  
Last changed: 10/1/2018, 2:49 PM

6. 完成後，請選擇 Save (儲存)。

資料庫密碼變更會立即生效。如果您輸入自己的密碼，密碼會立即儲存。如果 Lightsail 為您建立密碼，則會在幾秒鐘內產生密碼。選擇 Show (顯示) 以檢視新密碼。

## 後續步驟

以下是一些可協助您在 Lightsail 中管理資料庫的指南：

- [連線至 MySQL 資料庫](#)
- [連線至 PostgreSQL 資料庫](#)
- [建立資料庫快照](#)

## 為您的資料庫設定公開存取權

您在 Amazon Lightsail 中的受管資料庫只能由位於相同 Lightsail 帳戶中的 Lightsail 資源 (執行個體、負載平衡器等) 存取。一個常見的案例是建立 Lightsail 執行個體，其中包含公開 Web 應用程式，以及不可公開存取的 Lightsail 資料庫，然後將兩者連接起來。

啟用公有模式功能，讓您的資料庫可公開存取。任何人都可以透過這種方式，將資料庫端點、連接埠、使用者名稱和密碼，連接到您的資料庫。如需詳細資訊，請參閱[連線至 MySQL 資料庫](#)或[連線至 PostgreSQL 資料庫](#)。

為資料庫設定公開模式

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁上，選擇「資料庫」索引標籤。
3. 選擇您要設定公開模式的資料庫名稱。
4. 選擇 Networking (網路) 索引標籤。
5. 在 Public mode (公有模式) 區段，使用切換來將此功能開啟。同樣地，使用切換來將此功能關閉。

### Public mode

When public mode is enabled, anyone with your database user name and password can connect to it. When this mode is disabled, only your Lightsail resources in the same Region as your database can connect to it



Public mode is **disabled**.

Only your Lightsail resources in the same Region as your database can connect to it.

公有可存取性設定會立即開始套用，但可能需要幾分鐘的時間才能完成。在這段期間，資料庫的狀態會變更為 Modifying (修改中)。資料庫的狀態會在公有可存取性設定套用之後變更為 Available (可用)。

## 後續步驟

以下是可協助您管理資料庫的一些指南：

- [設定資料庫的資料匯入模式](#)
- [管理資料庫密碼](#)
- [連線至 MySQL 資料庫](#)
- [連線至 PostgreSQL 資料庫](#)
- [將資料匯入 MySQL 資料庫](#)
- [將資料匯入 PostgreSQL 資料庫](#)
- [建立資料庫快照](#)

## 利用參數更新將 Lightsail 資料庫效能最佳

資料庫參數 (也稱為資料庫系統變數) 可在 Amazon Lightsail 中定義受管資料庫的基本屬性。例如，您可以定義一個資料庫參數來限制資料庫連線數量，或定義另一個參數來限制資料庫緩衝集區大小。本指南說明如何取得受管理資料庫的參數清單，以及如何使用 AWS Command Line Interface (AWS CLI) 進行更新。

### Note

如需 MySQL 系統變數的詳細資訊，請參閱 [MySQL 5.6](#)、[MySQL 5.7](#) 或 [MySQL 8.0](#) 文件。如需 PostgreSQL 系統變數的詳細資訊，請參閱 [PostgreSQL 9.6](#)、[PostgreSQL 10](#)、[PostgreSQL 11](#) 或 [PostgreSQL 12](#) 的文件。

## 必要條件

- 如果您尚未安裝和設定 AWS CLI，請先執行這項動作。如需詳細資訊，請參閱 [設 AWS CLI 定使用 Lightsail](#)。

## 取得可用資料庫參數的清單

資料庫參數依據資料庫引擎而有不同；因此，您應取得可用於您的受管資料庫的參數清單。這可讓您決定您要修改哪些參數，以及參數生效的方式。

若要取得可用資料庫參數的清單

1. 開啟終端機或命令提示視窗。
2. 輸入下列命令，取得您資料庫的參數清單。

```
aws lightsail get-relational-database-parameters --relational-database-name DatabaseName
```

在命令中，*DatabaseName*用數據庫的名稱替換。

您應該會看到類似以下範例的結果：

```
{
  "parameters": [
    {
      "allowedValues": "0,1",
      "applyMethod": "pending-reboot",
      "applyType": "static",
      "dataType": "boolean",
      "description": "Controls whether user-defined functions that have only an xxx symbol for the main function can be loaded",
      "isModifiable": false,
      "parameterName": "allow-suspicious-udfs"
    },
    {
      "allowedValues": "0,1",
      "applyMethod": "pending-reboot",
      "applyType": "static",
      "dataType": "boolean",
      "description": "Controls whether the server autogenerates SSL key and certificate files in the data directory, if they do not already exist.",
      "isModifiable": false,
      "parameterName": "auto_generate_certs"
    },
    {
      "allowedValues": "1-65535",
      "applyMethod": "pending-reboot",
      "applyType": "dynamic",
      "dataType": "integer",
      "description": "Intended for use with master-to-master replication, and can be used to control the operation of AUTO_INCREMENT columns",
      "isModifiable": true,
      "parameterName": "auto_increment_increment"
    },
    {
      "allowedValues": "1-65535",
      "applyMethod": "pending-reboot"
    }
  ]
}
```

### Note

如果參數結果分成多個頁面，將會列出下一個頁面的符記 ID。請記下下一個頁面符記 ID，然後如下一個步驟所示，用它來檢視下一頁的參數結果。

3. 如果您的結果分成多個頁面，請使用下列命令來檢視額外的一組參數。否則，跳至下一步。

```
aws lightsail get-relational-database-parameters --relational-database-name DatabaseName --page-token NextPageTokenID
```

在命令中：

- *DatabaseName* 使用您的數據庫的名稱。
- *NextPageToken##### ID # ID#*

結果將顯示各資料庫參數的下列資訊：

- 允許的值 - 指定參數值的有效範圍。
  - 套用方法 - 指定何時可套用參數變更。允許的選項為 `immediate` 或 `pending-reboot`。請參閱以下套用類型，以了解如何定義套用方法的詳細資訊。
  - 套用類型 - 指定引擎特定的提交類型。如果列出的是 `dynamic`，表示該參數可透過 `immediate` 套用方法加以套用，資料庫將會立即開始使用新的參數值。如果列出的是 `static`，表示該參數只能透過 `pending-reboot` 套用方法加以套用，資料庫只有在重新啟動之後才會開始使用新的參數值。
  - 資料類型 - 指定參數的有效資料類型。
  - 在說明 - 提供參數的說明。
  - 可修改 - 此布林值用於指示是否可修改參數。如果列出的是 `true`，表示可修改參數。
  - 參數名稱 - 指定參數的名稱。使用此值搭配 `update relational database` 操作和 `parameter name` 參數。
4. 尋找您要變更的參數，然後記下參數名稱、允許值，以及套用方法。我們建議將參數名稱複製到您的剪貼簿，以避免輸入錯誤的參數名稱。若要這麼做，如果您使用的是 Windows，請反白選取參數名稱並按 `Ctrl+C` (`Ctrl+C`)，或者如果您使用的是 macOS，請反白選取參數名稱並按 `Cmd+C` (`Cmd+C`)，將參數名稱複製到您的剪貼簿。然後，在適當位置按下 `Ctrl+V` (`Ctrl+V`) 或 `Cmd+V` (`Cmd+V`) 來貼上。

在您識別想要修改的參數的名稱之後，請繼續本指南的下一個部分，將參數變更為您想要的值。

## 更新資料庫參數

取得要變更的參數名稱後，請執行下列步驟，在 Lightsail 中修改受管理資料庫的參數：

## 若要更新資料庫參數

- 將下列命令輸入至終端機或命令提示字元視窗，以更新您的受管資料庫的參數。

```
aws lightsail update-relational-database-parameters
--relational-database-name DatabaseName --parameters
"parameterName=ParameterName,parameterValue=NewParameterValue,applyMethod=ApplyMethod"
```

在命令中：

- DatabaseName* 使用您的數據庫的名稱。
- ParameterName* 使用您要修改的參數名稱。
- NewParameterValue* 具有參數的新值。
- ApplyMethod* 使用參數的應用方法。

如果參數的套用類型是 `dynamic`，表示該參數可透過 `immediate` 套用方法加以套用，資料庫將會立即開始使用新的參數值。但是，如果參數套用類型是 `static`，表示該參數只能透過 `pending-reboot` 套用方法加以套用，資料庫只有在重新啟動之後才會開始使用新的參數值。

您應該會看到類似以下範例的結果：

```
{
  "operations": [
    {
      "id": "2c650987-11e8-463f-94d5-0c15aacaf12b",
      "resourceName": "myfirsttestdatabase",
      "resourceType": "RelationalDatabase",
      "createdAt": 1539204831.214,
      "location": {
        "availabilityZone": "us-east-1a",
        "regionName": "us-east-1"
      },
      "isTerminal": true,
      "operationType": "UpdateRelationalDatabaseParameters",
      "status": "Succeeded",
      "statusChangedAt": 1539204831.214
    }
  ]
}
```

資料庫參數會依據所使用的套用方式進行更新。

## 升級資料庫的主要版本

當 Amazon Lightsail 支援新版本的資料庫引擎時，您可以將資料庫升級到新版本。Lightsail 提供兩個資料庫藍圖，分別是 MySQL 和 PostgreSQL。本指南說明如何升級 MySQL 或 PostgreSQL 資料庫執行個體的主要版本。您只能使用 [update-relational-database](#) API 動作升級資料庫主要版本。

我們將用 AWS CloudShell 來執行升級。CloudShell 是以瀏覽器為基礎的預先驗證殼層，您可以直接從 Lightsail 主控台啟動。使用時 CloudShell，您可以使用您偏好的外圍程序 AWS Command Line Interface（例如 Bash 或 Z 外殼）運行（AWS CLI）命令。PowerShell 無需下載或安裝命令列工具即可執行此操作。如需有關如何設定和使用的詳細資訊 CloudShell，請參閱 [Lightsail AWS CloudShell 中的](#)。

### 了解變化

主要版本升級可能會導致許多與先前版本不相容的問題。這些不相容性可能會在升級期間造成問題。您可能需要準備資料庫，才能成功升級。如需有關升級資料庫主要版本的資訊，請參閱 MySQL 和 PostgreSQL 網站上的下列主題。

- [準備安裝以進行升級](#)
- [MySQL 升級檢查工具](#)
- [升 PostgreSQL 集](#)

## 必要條件

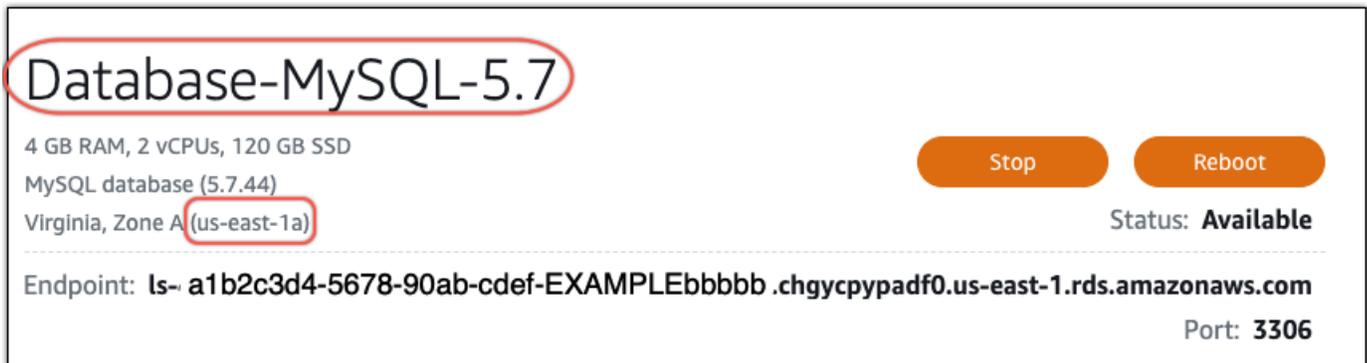
1. 確認您的應用程式支援資料庫的兩個主要版本。
2. 建議您在進行任何變更之前，先建立資料庫執行個體的快照集。如需詳細資訊，請參閱 [建立 Lightsail 資料庫的快照集](#)。
3. (選擇性) 從您剛建立的快照集建立新的資料庫執行處理。由於資料庫更新需要停機時間，因此您可以在升級目前作用中的資料庫之前，先在新資料庫上測試升級。如需有關製作資料庫複本的詳細資訊，請參閱 [建立 Lightsail 資料庫的快照集](#)。

## 更新資料庫主要版本

Lightsail 支援 MySQL 和 PostgreSQL 資料庫執行個體的主要版本升級。在下列程序中，會使用 MySQL 資料庫做為範例。但是，PostgreSQL 資料庫的程序和命令是相同的。

完成下列程序，即可升級 Lightsail 資料庫的資料庫主要版本。

1. 登入主 [Lightsail](#) 台。
2. 在左側的導覽窗格中，選擇資料庫。
3. 請注意您要升級之資料庫執行處理的名稱和 AWS 區域 資料庫執行處理。



Database-MySQL-5.7

4 GB RAM, 2 vCPUs, 120 GB SSD

MySQL database (5.7.44)

Virginia, Zone A (us-east-1a)

Status: Available

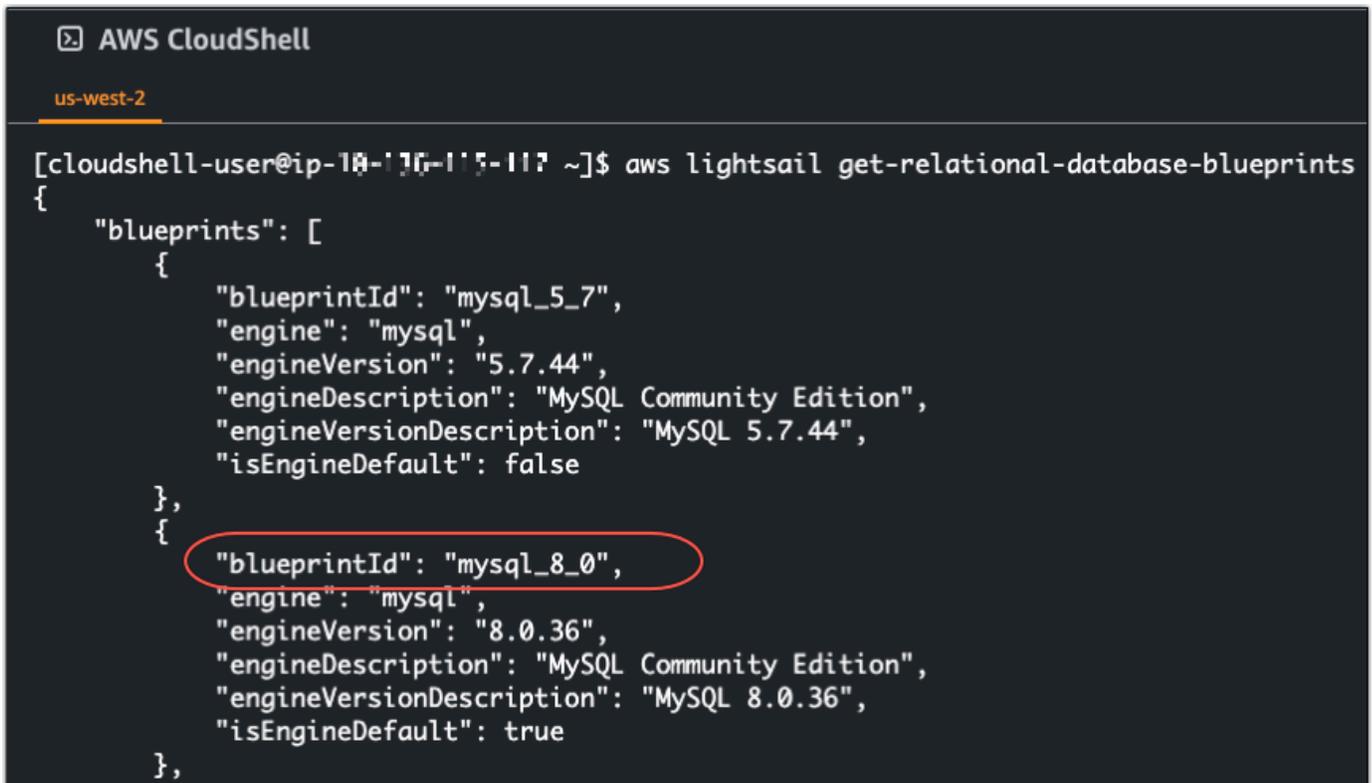
Endpoint: ls-a1b2c3d4-5678-90ab-cdef-EXAMPLEbbbb.chgycpypadf0.us-east-1.rds.amazonaws.com

Port: 3306

4. 在 Lightsail 主控台的左下角，選擇 CloudShell。CloudShell 終端機將在同一瀏覽器選項卡中打開。出現命令提示時，表示 Shell 已準備好開始互動。
5. 在 CloudShell 提示下輸入下列命令，以取得可用的資料庫藍圖 ID 清單。

```
aws lightsail get-relational-database-blueprints
```

6. 您要升級的主要版本的藍圖 ID 附註。例如 `mysql_8_0`。



```
AWS CloudShell
us-west-2

[cloudshell-user@ip-10-17-15-117 ~]$ aws lightsail get-relational-database-blueprints
{
  "blueprints": [
    {
      "blueprintId": "mysql_5_7",
      "engine": "mysql",
      "engineVersion": "5.7.44",
      "engineDescription": "MySQL Community Edition",
      "engineVersionDescription": "MySQL 5.7.44",
      "isEngineDefault": false
    },
    {
      "blueprintId": "mysql_8_0",
      "engine": "mysql",
      "engineVersion": "8.0.36",
      "engineDescription": "MySQL Community Edition",
      "engineVersionDescription": "MySQL 8.0.36",
      "isEngineDefault": true
    }
  ]
}
```

- 輸入以下命令以升級數據庫的主要版本。升級會在資料庫的下一個維護時段進行。在命令中，*DatabaseName*用資料庫的名稱 *Blueprint ID* 替換為您要升級到的主要版本的藍圖 ID，以及資料庫所在*DatabaseRegion*的藍圖 ID。AWS 區域

```
aws lightsail update-relational-database \  
  --relational-database-name DatabaseName \  
  --relational-database-blueprint-id blueprintId \  
  --region DatabaseRegion
```

(選擇性) 若要立即套用升級，請在指令中包含 `--apply-immediately` 參數。您會看到類似下列範例的回應，而且套用升級時，您的資料庫將無法使用。如需詳細資訊，請參閱 [update-relational-database](#) 中 Lightsail 參考資料。

```
% aws lightsail update-relational-database \  
--relational-database-name "Database-Mysql-5.7" \  
--relational-database-blueprint-id "mysql_8_0" \  
--apply-immediately \  
[--region us-east-1  
{  
  "operations": [  
    {  
      "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLEbbbb",  
      "resourceName": "Database-Mysql-5.7",  
      "resourceType": "RelationalDatabase",  
      "createdAt": 2024-01-01T00:00:00.000000+00:00",  
      "location": {  
        "availabilityZone": "us-east-1a",  
        "regionName": "us-east-1"  
      },  
      "isTerminal": true,  
      "operationDetails": "",  
      "operationType": "UpdateRelationalDatabase",  
      "status": "Succeeded",  
      "statusChangedAt": 2024-01-01T00:00:00.000000+00:00",  
    }  
  ]  
}
```

- 輸入下列命令，以確認主要版本升級是否已排程於下一個資料庫維護時段進行。在命令中，*DatabaseName*用數據庫的名稱和*DatabaseRegion*數據庫所在 AWS 區域 的名稱替換。

```
aws lightsail get-relational-database \  
  --relational-database-name DatabaseName \  
  --region DatabaseRegion
```

在get-relational-database回應中，資料庫會在下一個維護時段`state`通知您擱置的主要版本升級。您可以在響應部分中找到下一個維護時`preferredMaintenanceWindow`段的日期和時間。

### 數據庫實例狀態

```
"state": "upgrading",  
  "backupRetentionEnabled": true,  
  "pendingModifiedValues": {  
    "engineVersion": "8.0.36"
```

### Maintenance window (維護時段)

```
"preferredMaintenanceWindow": "wed: 09:22-wed: 09:52"
```

## 後續步驟

如果您已建立測試資料庫，則可以在確認應用程式可以與升級的資料庫搭配使用之後將其刪除。保留您先前數據庫創建的快照，以防需要返回該快照。您也應該建立已升級之資料庫的快照集，以便取得新的point-in-time 複本。

## 將資料從 MySQL 5.6 資料庫遷移至較新的 Lightsail

在本教學課程中，我們向您展示如何在 Amazon Lightsail 中，將資料從 MySQL 5.6 資料庫遷移至新的 MySQL 5.7 資料庫。若要執行遷移，您可以連接到 MySQL 5.6 資料庫並匯出現有資料。然後，您可以連接到 MySQL 5.7 資料庫並匯入資料。新的資料庫擁有所需資料之後，您便可以重新設定應用程式以連接到新的資料庫。

### 內容

- [步驟 1：了解變更](#)
- [步驟 2：完成事前準備](#)
- [步驟 3：連接到 MySQL 5.6 資料庫並匯出資料](#)
- [步驟 4：連接到 MySQL 5.7 資料庫並匯入資料](#)

## • [步驟 5：測試應用程式並完成遷移](#)

### 步驟 1：了解變更

從 MySQL 5.6 資料庫移至 MySQL 5.7 資料庫，是一項主要版本升級。主要版本升級可能包含與現有應用程式回溯不相容的資料庫變更。我們建議您在將任何升級套用至生產執行個體之前，先進行完整測試。如需詳細資訊，請參閱 MySQL 文件中的 [MySQL 5.7 中的變更](#)。

我們建議您先將資料從現有 MySQL 5.6 資料庫遷移至新的 MySQL 5.7 資料庫。然後在生產前執行個體上使用新的 MySQL 5.7 資料庫來測試應用程式。如果應用程式如預期般運作，請將變更套用至生產執行個體中的應用程式。為了更進一步，您可以將資料從現有的 MySQL 5.7 資料庫遷移到新的 MySQL 8.0 資料庫，以便在生產前再次測試應用程式，並在生產環境中將變更套用至應用程式。

### 步驟 2：完成事前準備

您必須完成下列事前準備，才能繼續前往本教學課程的後續章節：

- 在本機電腦上安裝 MySQL Workbench，您將使用它來連接到資料庫以匯出和匯入資料。如需詳細資訊，請參閱 MySQL 網站上的 [MySQL Workbench 下載](#)。
- 在 Lightsail 中建立 MySQL 5.7 資料庫。如需詳細資訊，請參閱 [在 Amazon Lightsail 中建立資料庫](#)。
- 為資料庫啟用公有模式。這允許您使用 MySQL Workbench 連接到這些資料庫。當您完成資料的匯出和匯入時，您可以停用資料庫的公有模式。如需詳細資訊，請參閱 [為資料庫設定公有模式](#)。
- 設定 MySQL Workbench 以連接到資料庫。如需詳細資訊，請參閱 [連接到 MySQL 資料庫](#)。

### 步驟 3：連接到 MySQL 5.6 資料庫並匯出資料

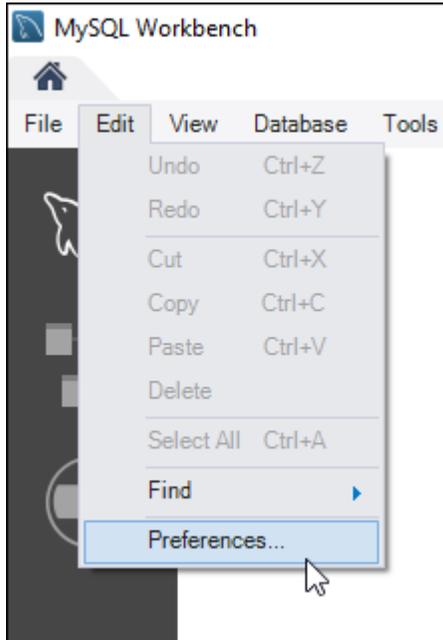
在本教學課程的本節中，您將連接到 MySQL 5.6 資料庫，並使用 MySQL Workbench 從其中匯出資料。如需有關使用 MySQL Workbench 匯出資料的詳細資訊，請參閱《MySQL Workbench 手冊》中的 [SQL 資料匯出與匯入精靈](#)。

1. 使用 MySQL Workbench 連接到 MySQL 5.6 資料庫。

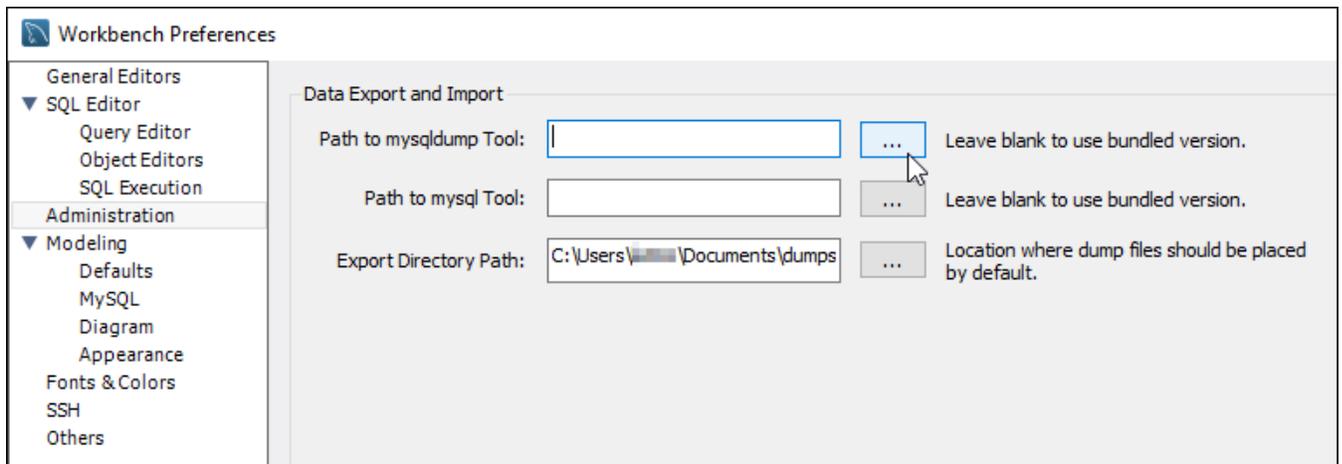
MySQL Workbench 使用 mysqldump 來匯出資料。MySQL Workbench 使用的 mysqldump 的版本必須與您將從中匯出資料的 MySQL 資料庫版本相同 (或比該資料庫的版本更高)。例如，如果您從 MySQL 5.6.51 資料庫匯出資料，則您必須使用 mysqldump 版本 5.6.51 或更高版本。您可能需要在本機電腦上下載並安裝適當版本的 MySQL 伺服器，以確保您使用的是正確的 mysqldump 版本。若要下載特定版本的 MySQL 伺服器，請參閱 MySQL 網站上的 [MySQL 社群下載](#)。適用於 Windows MSI 的 MySQL 安裝程式提供任何版本的 MySQL 伺服器的下載選項。

請完成以下步驟，以選擇在 MySQL Workbench 中使用的正確 mysqldump 版本：

1. 在 MySQL Workbench 中，選擇 Edit (編輯)，然後選擇 Preferences (偏好設定)。

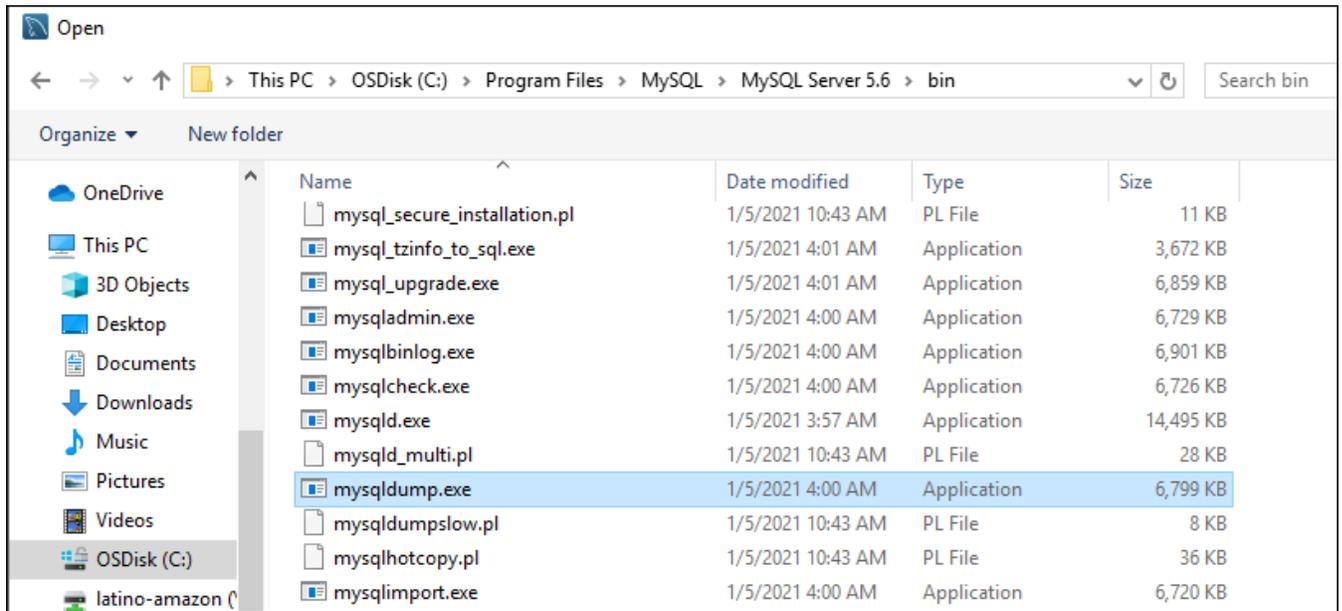


2. 在導覽窗格中選擇 Administration (管理)。
3. 在出現的 Workbench Preferences (Workbench 偏好設定) 視窗中，選擇 Path to mysqldump Tool (mysqldump 工具的路徑) 文字方塊旁的省略符號按鈕。

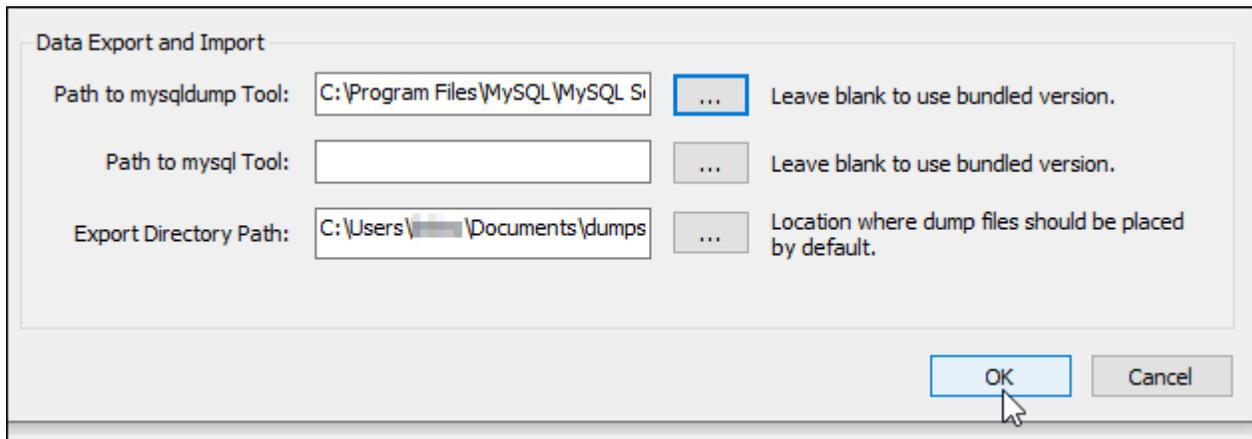


4. 瀏覽至適當的 mysqldump 可執行檔的位置，然後按兩下該檔案。

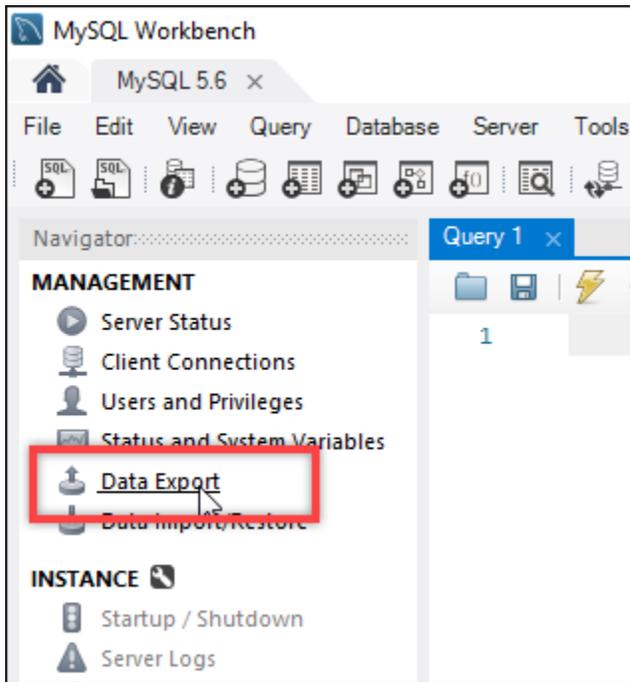
在 Windows 中，mysqldump.exe 檔案通常位於 C:\Program Files\MySQL\MySQL Server 5.6\bin 目錄。在 Linux 中，在終端機中輸入 which mysqldump，以查看 mysqldump 檔案的所在位置。



5. 在 Workbench Preferences (Workbench 偏好設定) 視窗中選擇 OK (確定)。



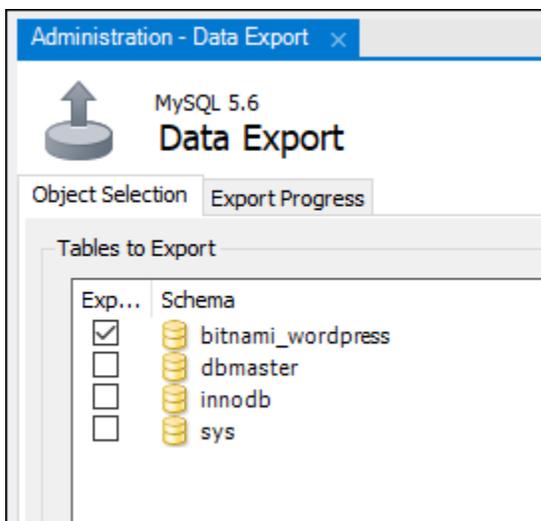
2. 在 Navigator (導覽器) 窗格中選擇 Data Export (資料匯出)



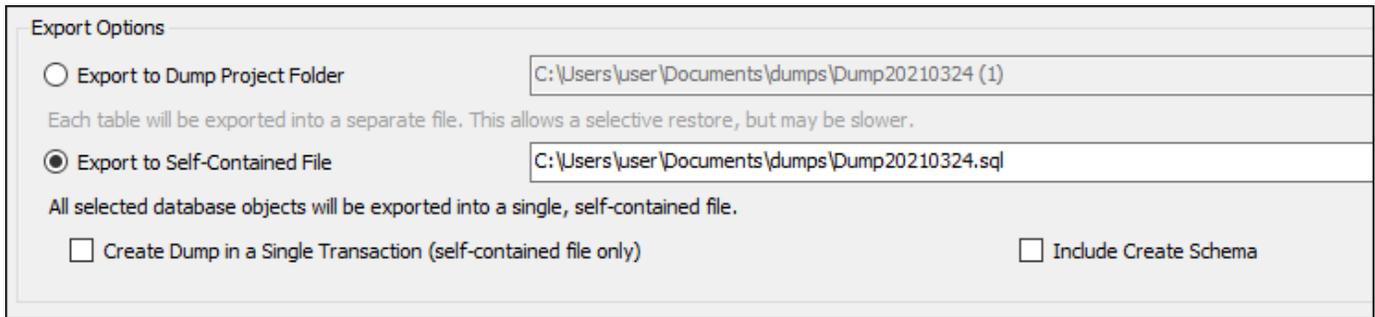
3. 在出現的資料匯出索引標籤中，在您要匯出的資料表旁新增核取記號。

**Note**

在此範例中，我們選擇了包bitnami\_wordpress含「由 Bitnami 認證」WordPress 執行個體上 WordPress 網站資料的表格。

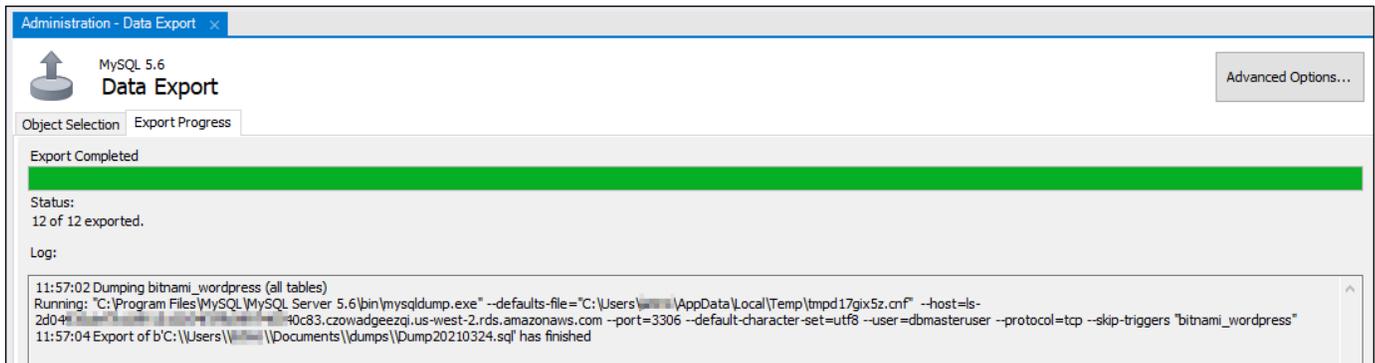


4. 在 Export Options (匯出選項) 區段中，選擇 Export to Self-Contained File (匯出為可獨自運作的檔案)，然後記下要儲存匯出檔案的目錄。



The screenshot shows the 'Export Options' dialog box in MySQL Workbench. It has two radio buttons: 'Export to Dump Project Folder' (unselected) and 'Export to Self-Contained File' (selected). The 'Export to Self-Contained File' option has a text field containing the path 'C:\Users\user\Documents\dumps\Dump20210324.sql'. Below the radio buttons, there is a note: 'Each table will be exported into a separate file. This allows a selective restore, but may be slower.' Underneath, it says 'All selected database objects will be exported into a single, self-contained file.' At the bottom, there are two checkboxes: 'Create Dump in a Single Transaction (self-contained file only)' (unselected) and 'Include Create Schema' (unselected).

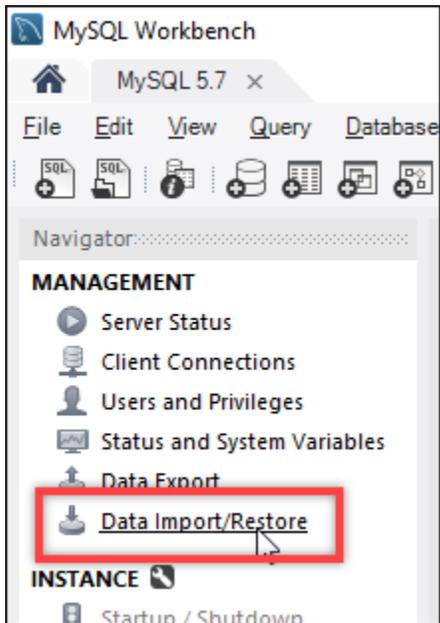
5. 選擇 Start Export (開始匯出)。
6. 等待匯出完成，然後繼續前往本教學課程的下一節。



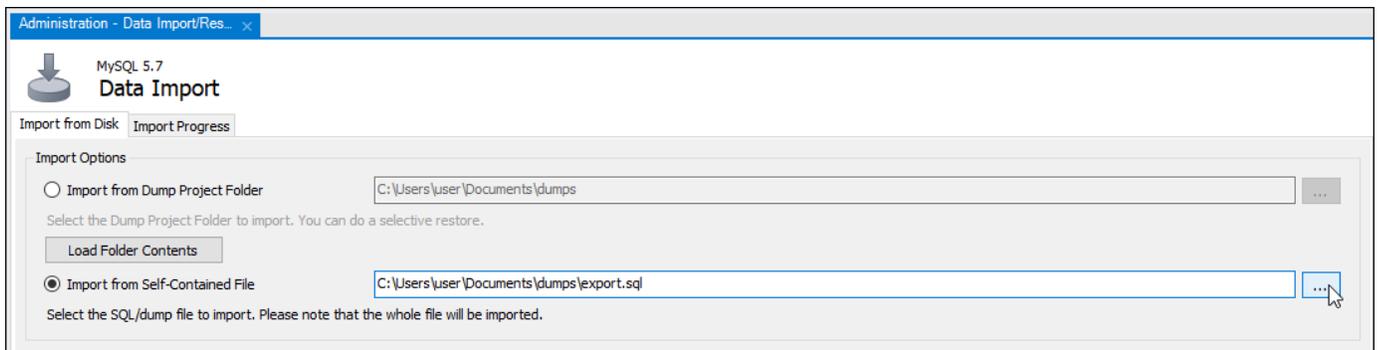
## 步驟 4：連接到 MySQL 5.7 資料庫並匯入資料

在本教學課程的這一節中，您需連接到 MySQL 5.7 資料庫，並使用 MySQL Workbench 將資料匯入該資料庫。

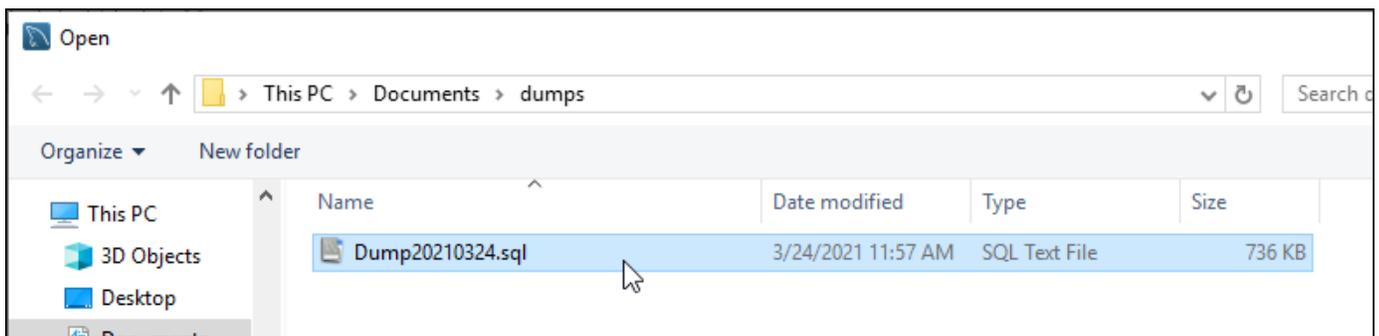
1. 在本機電腦上使用 MySQL Workbench 連接到 MySQL 5.7 資料庫。
2. 在 Navigator (導覽器) 窗格中選擇 Data Import/Restore (資料匯入/還原)。



3. 在出現的 Data Import (資料匯入) 索引標籤中，選擇 Import from Self-Contained File (從可獨自運作的檔案匯入)，然後選擇文字方塊旁邊的省略符號按鈕。



4. 瀏覽至匯出檔案的儲存位置，然後按兩下該檔案。



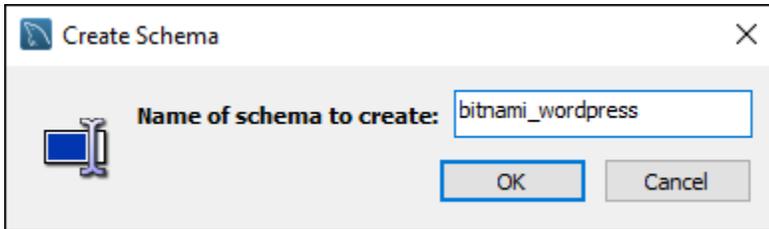
5. 在 Default Schema to be imported To (匯入目標的預設結構描述) 區段中選擇 New (新增)。



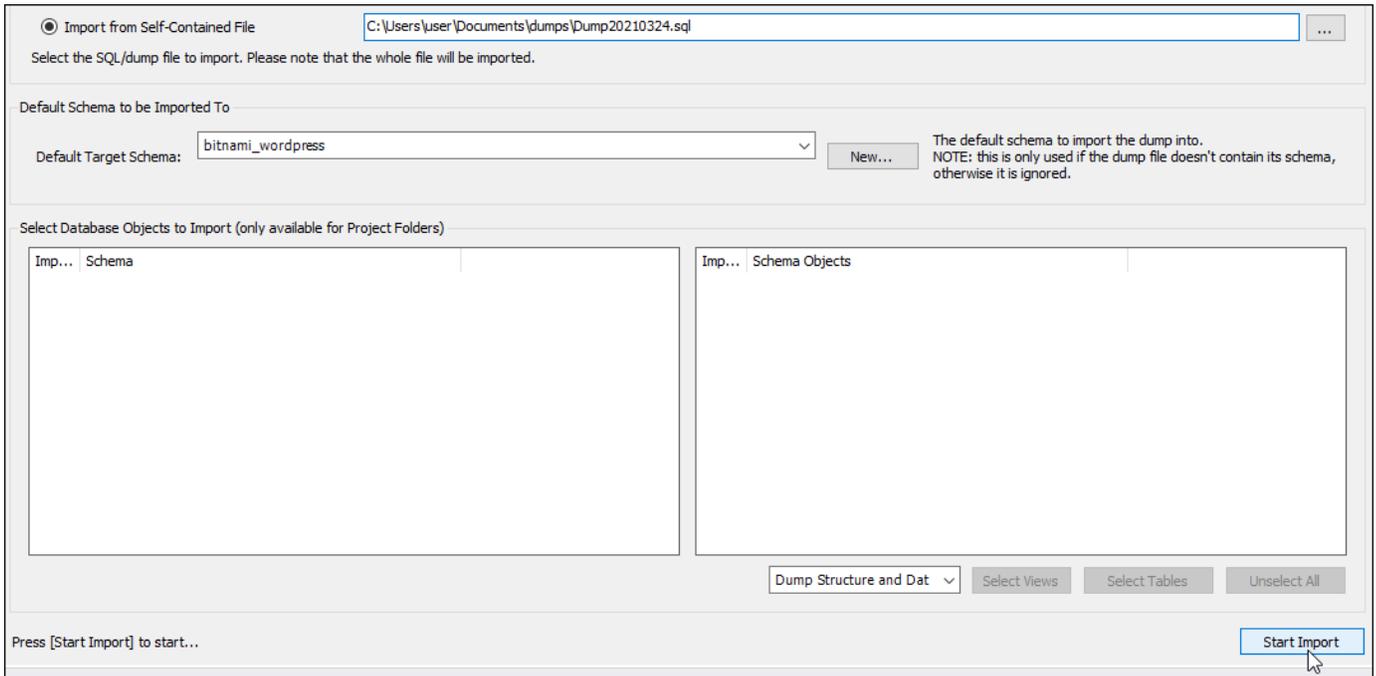
- 在出現的 Create Schema (建立結構描述) 視窗中輸入結構描述的名稱。

**Note**

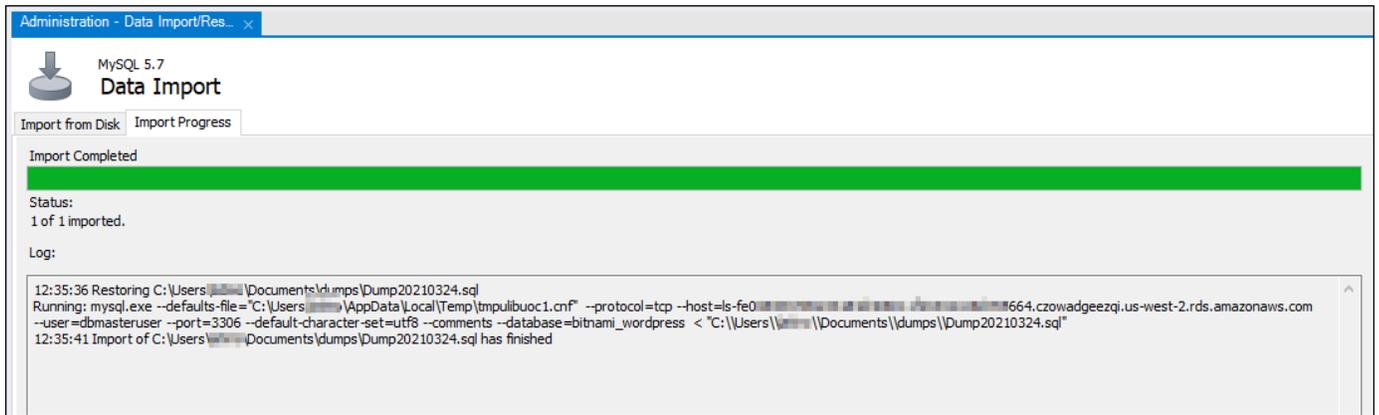
在此範例中，我們輸入的是 `bitnami_wordpress`，因為這是我們匯出的資料庫資料表的名稱。



- 選擇 Start import (開始匯入)。



- 請等待匯入完成，然後繼續前往本教學課程的下一節。



## 步驟 5：測試應用程式並完成遷移

此時，您的資料位於新的 MySQL 5.7 資料庫中。在預生產環境中設定應用程式，並測試應用程式與新 MySQL 5.7 資料庫之間的連線。如果應用程式的行為符合預期，則繼續對生產環境中的應用程式進行變更。

當您完成遷移時，您應該停用資料庫的公有模式。當您確定您不再需要 MySQL 5.6 資料庫時，就可以將其刪除。但是，您應該在刪除 MySQL 5.6 資料庫之前建立其快照。當您這樣做時，您還應該建立新 MySQL 5.7 資料庫的快照。如需詳細資訊，請參閱[建立資料庫快照](#)。

# 使用 Lightsail 負載平衡器分配網路流量

Lightsail 負載平衡器會在多個可用區域中的多個 Lightsail 執行個體之間分散傳入的網路流量。進行負載平衡可提高執行個體上應用程式的可用性與容錯能力。您可以在需求變更時從 Lightsail 負載平衡器新增和移除執行個體，而不會中斷應用程式的整體要求流程。

透過 Lightsail 負載平衡，我們會建立 DNS 主機名稱，並將傳送至此主機名稱的任何要求路由到目標 Lightsail 執行個體集區。您可以根據需要將任意數量的目標執行個體新增至負載平衡器，只要您保留在 Lightsail 帳戶的執行個體總數內即可。

## 負載平衡器功能

Lightsail 負載平衡器提供以下功能：

- **HTTPS 加密** — 依預設，Lightsail 負載平衡器會透過連接埠 80 處理未加密 (HTTP) 流量要求。透過將經過驗證的 Lightsail SSL/TLS 證書附加到負載平衡器來啟用加 HTTPS 密。這可讓您的負載平衡器透過連接埠 443 處理加密 (HTTPS) 流量要求。如需詳細資訊，請參閱 [SSL/TLS 憑證](#)。

在負載平衡器上啟用 HTTPS 加密之後，即可使用下列功能：

- **HTTP 至重 HTTPS 新導向** — 啟動 HTTP 至重 HTTPS 新導向，以自動將 HTTP 要求重新導向至加 HTTPS 密的連線。如需詳細資訊，請參閱 [HTTP 為負載平衡器設定為 HTTPS 重新導向](#)。
- **TLS 安全性原則** — 在負載平衡器上設定 TLS 安全性原則。如需詳細資訊，請參閱在 [Amazon Lightsail 負載平衡器上設定 TLS 安全政策](#)。
- **運作狀態檢查** – 預設情況下，系統會在所附接執行個體上執行的 Web 應用程式根目錄，對執行個體執行運作狀態檢查。您可藉由運作狀態檢查來監控執行個體的運作狀態，使負載平衡器只能傳送請求至運作狀態良好的執行個體。如需詳細資訊，請參閱 [Lightsail 負載平衡器的 Health 檢查](#)。
- **工作階段持續性** – 如果將工作階段資訊儲存於網站訪客的本機瀏覽器，請設定工作階段持續性。例如，您可能在負載平衡的 Lightsail 執行個體上執行含有購物車的 Magento 電子商務應用程式。在設定工作階段持續性的情況下，如果網站訪客將商品新增至購物車，接著就結束工作階段，之後使用者返回購物車時，仍可在購物車中找到這些商品。如需詳細資訊，請參閱 [為負載平衡器啟用工作階段持續性](#)。

## 何時使用負載平衡器

當您的網站偶爾出現流量高峰時，您應該使用負載平衡器；或者當許多訪客同時使用它時，主機內容可能會在執行個體上產生大量負載。例如，如果您擁有一個大量影像的網站，您可以使用其他頁面請求來負載平衡影像請求。如此一來，您的頁面載入速度會更快，使用者也會有更愉悅的體驗。

您可以使用負載平衡器來建立高度可用的網站。高可用性是指您的網站或應用程式在特定時間內能夠存活多久。如果您曾經歷過網站故障，則負載平衡器可能會協助您擁有更長的運作時間。您可以使用 Lightsail 負載平衡器新增分散在多個可用區域的目標執行個體，以提高應用程式的可用性。

容錯能力是一種相關的概念。如果您的網站在其中一個執行個體或您的資料庫故障後仍持續運作，就視為容忍。負載平衡器可協助您建立具備容錯能力的應用程式或網站。

## 建議的負載平衡 應用程式

並非所有 Lightsail 應用程式都需要負載平衡器。如果您決定建立負載平衡的應用程式，您必須先設定您的應用程式。例如，若要準備用於負載平衡的 LAMP 堆疊應用程式，您應該先建立一個集中式的專用資料庫，供所有目標執行個體讀取和寫入。您也可以考慮建立集中式媒體儲存體，例如 Lightsail 物件儲存貯體。如需詳細資訊，請參閱[設定執行個體以進行負載平衡](#)。

## 開始使用負載平衡器

您可以[使用 Lightsail 主控台、AWS Command Line Interface \(AWS CLI\) 或 Lightsail 建立負載平衡器](#)。API 您也必須[設定執行個體以用於負載平衡](#)。

建立負載平衡器並連接設定的執行個體之後，您可以 HTTPS 使用下列主題來啟用。如需詳細資訊，請參閱[為負載平衡器建立 SSL/TLS 憑證](#)。

## 使用 Lightsail 負載平衡器分配網路流量

建立一個負載平衡器以新增冗餘到您的應用程式或處理更多的 Web 流量。建立負載平衡器之後，您可以附加要平衡的 Lightsail 執行個體。若要進一步了解，請參閱[負載平衡器](#)

### 必要條件

在開始之前，請確定您已準備好 Lightsail 執行個體以進行負載平衡。如需詳細資訊，請參閱[設定執行個體以進行負載平衡](#)。

## 建立負載平衡器

1. 登入主 [Lightsail 台](#)。
2. 選擇 Networking (網路) 索引標籤。
3. 選擇 Create load balancer (建立負載平衡器)。
4. 確認將建立負載平衡器的 AWS 區域 位置，或選擇 [變更區域] 以選取其他區域。

### Note

依預設，將建立負載平衡器，並開啟連接埠 80 以接受 HTTP 要求。建立負載平衡器之後，您可以建立 SSL/TLS 憑證並進行設定 HTTPS。如需詳細資訊，請參閱 [為負載平衡器建立 SSL/TLS 憑證](#)

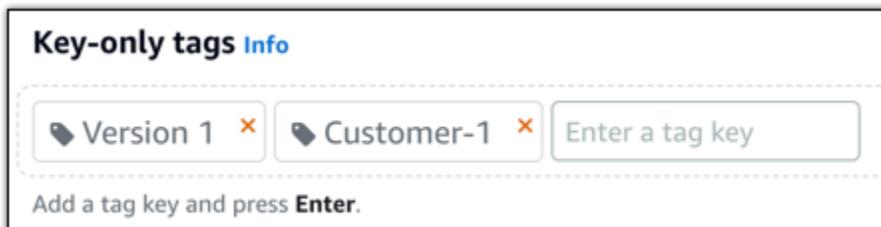
5. 輸入負載平衡器的名稱。

資源名稱：

- 每個 Lightsail 帳戶 AWS 區域 中的每個項目都必須是唯一的。
- 必須包含 2 至 255 個字元。
- 開頭和結尾必須是英數字元或數字。
- 可以包含英數字元、數字、句點、破折號和底線。

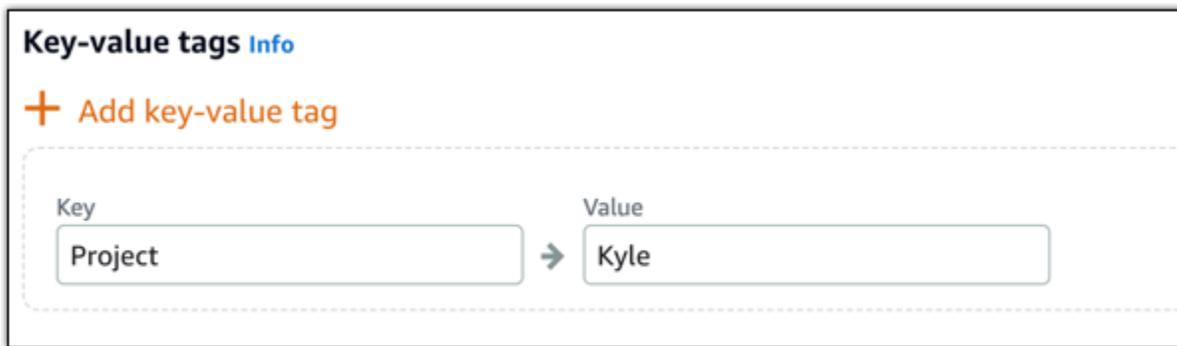
6. 選擇下列其中一個選項以新增標籤至您的負載平衡器：

- Add key-only tags (新增僅索引鍵標籤) 或 Edit key-only tags (編輯僅索引鍵標籤) (若標籤已新增)。在標籤索引鍵文字方塊中輸入新的標籤，接著按 Enter (輸入)。輸入標籤以新增之後，請選擇 Save (儲存)，如果不要新增則選擇 Cancel (取消)。



- Create a key-value tag (建立索引鍵值標籤)，接著將索引鍵輸入 Key (索引鍵) 文字方塊，將值輸入 Value (值) 文字方塊。完成輸入標籤後，請選擇 Save (儲存)，如果不要新增則選擇 Cancel (取消)。

鍵值標籤在儲存前一次只能新增一個。若要新增超過一個索引鍵值標籤，請重複之前的步驟。

**Note**

如需有關僅索引鍵和索引鍵值標籤的詳細資訊，請參閱[標籤](#)。

7. 選擇 Create load balancer (建立負載平衡器)。

## 將執行個體附接至負載平衡器

建立負載平衡器之後，Lightsail 會帶您前往負載平衡器管理頁面。如果您需要再次尋找該頁面，請選擇 Lightsail 首頁上的 [網路] 索引標籤，然後選擇 Lightsail 負載平衡器的名稱進行管理。

**Note**

您的 Lightsail 執行個體必須在執行中，才能成功將其連接至負載平衡器。

1. 在負載平衡器管理頁面上選擇 Target instances (目標執行個體)。
2. 在 Target instances (目標執行個體) 下拉式選單中選擇執行個體。
3. 選擇 Attach (連接)。連接作業可能需要幾分鐘的時間。

選擇 Attach another (連接另一個) 以將另一個執行個體連接到負載平衡器，然後重複前面的步驟。

## 後續步驟

在建立負載平衡器並連接執行個體後，請完成以下後續步驟以設定您的負載平衡器：

- [SSL為負載平衡器建立/憑TLS證](#)
- [自訂負載平衡器的運作狀態檢查](#)

如果負載平衡器遇到問題，請參閱[對負載平衡器進行故障診斷](#)

## 自訂 Lightsail 負載平衡器健康狀態檢查和HTTPS設定

當您建立 Lightsail 負載平衡器時，請選擇 AWS 區域 和名稱。本主題會指導如何更新負載平衡器，以便啟用更多選項。

若尚未如此操作，則需建立負載平衡器。[建立負載平衡器](#)

### 運作狀態檢查

您要做的第一件事情就是[設定執行個體以進行負載平衡](#)。完成後，請將該執行個體連接至負載平衡器。一旦連接執行個體，系統即會開始運作狀態檢查程序，而負載平衡器管理頁面上會顯示 Passed (通過) 或 Failed (失敗) 訊息。

Target Instances   Inbound Traffic   Delete

### Target Instances

Traffic will be evenly distributed to the following instances:

[Attach another](#)

	<b>example-1</b> 8 GB RAM, 2 vCPUs, 80 GB SSD WordPress Health Check: <b>Passed</b>	Detach 
	<b>example-2</b> 8 GB RAM, 2 vCPUs, 80 GB SSD WordPress Health Check: <b>Passed</b>	Detach 

 Your instances will receive traffic from this load balancer on port 80  
[Learn more about load balancing](#)

您也可以自訂運作狀態檢查的路徑。例如，如果您的首頁載入速度緩慢或上面有很多影像，您可以設定 Lightsail 檢查載入速度較快的其他頁面。[自訂負載平衡器運作狀態檢查路徑](#)

## 加密流量 (HTTPS)

您可以設置HTTPS為網站用戶創建更安全的體驗。設定負載平衡器後，建立和驗證SSL/TLS憑證是一個三個步驟的程序。

### [進一步了解 HTTPS](#)

## 工作階段持續性

當您要在使用者的本機瀏覽器中存放工作階段資訊時，工作階段持續性功能相當實用。例如，您可能會在 Lightsail 上執行 Magento 電子商務應用程式和購物車系統。如果您開啟工作階段持續性，使用者便能新增商品至購物車，接著結束工作階段。當使用者返回應用程式時，仍可在購物車中找到這些商品。

您也可以為持續性工作階段調整 Cookie 持續時間。如果您想要特別長或短的持續時間，此功能是很有用的。如需詳細資訊，請參閱[為負載平衡器啟用工作階段持續性](#)。

## 設定 Lightsail 執行個體進行負載平衡

將執行個體連接到 Amazon Lightsail 負載平衡器之前，您需要評估應用程式的組態。例如，資料層與應用程式其他部分隔開時，負載平衡器運作的效果通常會更好。本主題說明每個 Lightsail 實體的相關資訊，並針對負載平衡 (或水平擴展)，以及如何進行最佳設定應用程式提供建議。

### 一般準則：使用資料庫的應用程式

對於使用資料庫的 Lightsail 應用程式，建議您將資料庫執行個體與應用程式的其餘部分分開來，以便您只有一個資料庫執行個體。主要原因是這樣可避免將資料寫入超過一個資料庫。如果您不建立單一的資料庫執行個體，資料就會寫入使用者碰巧叫用的執行個體之資料庫。

## WordPress

水平擴展？是的，對於 WordPress 博客或網站。

使用 Lightsail 負載平衡器之前的組態建議

- 將資料庫分開，以便在負載平衡器後面 WordPress 執行的每個執行個體都從相同位置儲存和擷取資訊。如果需要資料庫的更高效能，您可以獨立在 Web 伺服器外複寫或變更處理能力或記憶體。
- 將您的檔案和靜態內容卸載至 Lightsail 值區。為此，您必須在 WordPress 網站上安裝 WP 卸載媒體精簡版插件，並將其配置為連接到 Lightsail 存儲桶。如需詳細資訊，請參閱[教學課程：將 WordPress 執行個體連線到儲存貯體](#)。

## Node.js

水平擴展？ 是，但有一些考量。

使用 Lightsail 負載平衡器之前的組態建議

- 在 Lightsail，Node.js 堆棧打包由 Bitnami 包含 Node.js，阿帕奇，雷迪斯（一個內存數據庫）和 Python。根據您部署的應用程式，您可以跨幾個伺服器執行負載平衡。然而，您需要設定負載平衡器以在所有 Web 伺服器之間平衡流量並將 Redis 移至另一個伺服器。
- 分割 Redis 伺服器至另一個伺服器以和所有執行個體通訊。視需要新增資料庫伺服器。
- Redis 的其中一個主要使用案例是在本機快取資料，如此您就不必持續叫用中央資料庫。建議您啟用工作階段持續性以運用 Redis 的效能提升。如需詳細資訊，請參閱[為負載平衡器啟用工作階段持續性](#)。
- 您也可以有共用的 Redis 節點，這樣您也能夠共用節點或在使用工作階段持續性的每個機器上使用本機快取。
- 如果您想要使用 Apache 部署負載平衡器，請考量將 mod\_proxy\_balancer 包含於 Apache 伺服器中。

如需詳細資訊，請參閱[擴展 Node.js 應用程式](#)。

## Magento

水平擴展？ 是。

使用 Lightsail 負載平衡器之前的組態建議

- 您可以使用 Magento 的 AWS 參考部署，使用其他組件，如 Amazon RDS 數據庫：[地形 Magento 的 Adobe 商務](#)上。AWS
- 請務必啟用工作階段持續性。Magento 使用購物車，這可協助確保在超過一個工作階段造訪多次的客戶可於新工作階段返回時在其購物車中保留項目。如需詳細資訊，請參閱[為負載平衡器啟用工作階段持續性](#)。

## GitLab

水平擴展？ 是，但有考量。

使用 Lightsail 負載平衡器之前的組態建議

您必須有以下項目：

- 執行中且可使用的 Redis 節點
- 共用網路儲存伺服器 (NFS)
- 該應用程序的集中式數據庫 ( 我的SQL或 PostgreSQL )。請參閱以上關於資料庫的一般準則。

如需詳細資訊，請參閱GitLab網站上的[高可用性](#)。

#### Note

上述的共用網路儲存區伺服器 (NFS) 目前無法與 GitLab 藍圖一起使用。

## Drupal

水平擴展？是。Drupal 有一份正式文件說明如何水平擴展您的應用程式：[伺服器擴展](#)。

使用 Lightsail 負載平衡器之前的組態建議

您必須設定 Drupal 模組以在不同的執行個體間同步檔案。Drupal 網站有數個模組，但可能更適用於建立原型而非生產使用。

使用模組將檔案存放於 Amazon S3。這可讓您集中您的檔案，不必在每個目標執行個體上保留個別的複本。如此一來，假設您編輯檔案，集中存放區就可提供更新，而您的使用者無論叫用哪個執行個體都會看見相同的檔案。

- [Amazon S3 檔案系統](#)
- [內容同步](#)

如需詳細資訊，請參閱[水平和在雲端中擴展 Drupal](#)。

## LAMP堆疊

水平擴展？是。

使用 Lightsail 負載平衡器之前的組態建議

- 您應該在單獨的執行個體上建立資料庫。負載平衡器後方的所有執行個體都應指向此單獨的資料庫執行個體，以從相同的地方存放和擷取資訊。

- 視您要部署的應用程式而定，請考慮如何共用檔案系統 (NFS Lightsail 區塊儲存磁碟或 Amazon S3 儲存)。

## MEAN堆疊

水平擴展？ 是。

使用 Lightsail 負載平衡器之前的組態建議

將 MongoDB 移至另一部電腦，並設定機制，以便在 Lightsail 執行個體之間共用根文件。

## Redmine

水平擴展？ 是。

使用 Lightsail 負載平衡器之前的組態建議

- 取得 [Redmine\\_S3 plugin](#)，在 Amazon S3 而非本機檔案系統中儲存附件。
- 將資料庫分隔到不同的執行個體。

## Nginx

水平擴展？ 是。

您可以將一或多個 Lightsail 執行個體執行 Nginx 並連接至 Lightsail 負載平衡器。如需詳細資訊，請參閱 [調整 Web 應用程式的規模 NGINX，第 1 部分：負載平衡](#)。

## Joomla!

水平擴展？ 是，但有考量。

使用 Lightsail 負載平衡器之前的組態建議

雖然 Joomla 網站上沒有正式文件，但在其社群論壇上有一些討論。有些使用者成功水平擴展了 Joomla 執行個體，而其叢集具有以下組態：

- 設定為啟用工作階段持續性的 Lightsail 負載平衡器。如需詳細資訊，請參閱 [為負載平衡器啟用工作階段持續性](#)。

- 執行 Joomla 的數個執行個體，並使用 Joomla! 同步。您可以使用 Rsync 之類的工具來執行此操作，擁有負責在所有 Lightsail 實例之間同步內容的 NFS 服務器，或使用共享文件。AWS
- 設定了複寫叢集的數個資料庫伺服器。
- 在每個 Lightsail 實體中設定的相同快取系統。有一些有用的擴展，例如 [JotCache](#)。

## 為您的負載平衡器設定 TLS 安全性原則

在 Amazon Lightsail 負載平衡器上啟用 HTTPS 之後，您可以為加密的連線設定 TLS 安全政策。本指南提供您可在 Lightsail 負載平衡器上設定的安全性原則的相關資訊，以及更新負載平衡器安全性原則的程序。如需負載平衡器的詳細資訊，請參閱[負載平衡器](#)。

### 安全政策概觀

Lightsail 負載平衡使用安全通訊端層 (SSL) 交涉組態 (稱為安全性原則) 來交涉用戶端與負載平衡器之間的 SSL 連線。安全政策為通訊協定與加密的組合。通訊協定會在用戶端與伺服器之間建立安全連線，並確保在用戶端與負載平衡器之間傳遞的所有資料為私有。隨碼是一項加密演算法，使用加密金鑰來建立編碼的訊息。通訊協定使用多個加密來加密透過網際網路的資料。在連線交涉程序期間，用戶端與負載平衡器會出示它們分別支援的加密和通訊協定的清單 (以偏好的順序)。在預設情況下，將針對安全連線選取伺服器清單上符合任何用戶端加密的第一個加密。Lightsail 負載平衡器不支援用戶端或目標連線的 SSL 重新交涉。

當您在 Lightsail 負載平衡器上啟用 HTTPS 時，依預設會設定 TLS-2016-08 安全性原則。您可以根據需求設定其他安全政策，如本指南下文所述。您可以選擇僅適用於前端連線的安全政策。TLS-2016-08 安全政策始終用於後端連接。Lightsail 負載平衡器不支援自訂安全性原則。

### 支援的安全政策和通訊協定

Lightsail 負載平衡器可以使用下列安全性原則和通訊協定進行設定：

Security policies	TLS-2016-08 (default)	TLS-FS-1-2-Res-2019-08
<b>TLS Protocols</b>		
Protocol-TLSv1	✓	
Protocol-TLSv1.1	✓	
Protocol-TLSv1.2	✓	✓
<b>TLS Ciphers</b>		
ECDHE-ECDSA-AES128-GCM-SHA256	✓	✓
ECDHE-RSA-AES128-GCM-SHA256	✓	✓
ECDHE-ECDSA-AES128-SHA256	✓	✓
ECDHE-RSA-AES128-SHA256	✓	✓
ECDHE-ECDSA-AES128-SHA	✓	
ECDHE-RSA-AES128-SHA	✓	
ECDHE-ECDSA-AES256-GCM-SHA384	✓	✓
ECDHE-RSA-AES256-GCM-SHA384	✓	✓
ECDHE-ECDSA-AES256-SHA384	✓	✓
ECDHE-RSA-AES256-SHA384	✓	✓
ECDHE-RSA-AES256-SHA	✓	
ECDHE-ECDSA-AES256-SHA	✓	
AES128-GCM-SHA256	✓	
AES128-SHA256	✓	
AES128-SHA	✓	

## 完成先決條件

請先完成事前準備 (若尚未完成)：

- 建立 負載平衡器，並將其與執行個體連接。如需詳細資訊，請參閱[建立負載平衡器並將執行個體與其附接](#)。
- 建立 SSL/TLS 憑證，並將其連接到您的負載平衡器，以啟用 HTTPS。如需詳細資訊，請參閱[為 Lightsail 負載平衡器建立 SSL/TLS 憑證](#)。如需憑證的詳細資訊，請參閱 [SSL/TLS 憑證](#)。

## 使用主控台設定安全性原則

請完成下列程序，以使用 Lightsail 主控台設定安全性原則。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁，選擇 Networking (聯網) 索引標籤。
3. 選擇您要設定 TLS 安全政策的負載平衡器名稱。
4. 選擇 Inbound traffic (傳入流量) 索引標籤。
5. 在頁面的 TLS security protocols (TLS 安全通訊協定) 區段底下，選擇 Change protocols (變更通訊協定)。
6. 從 Supported protocols (支援的通訊協定) 下拉式選單中選擇下列任一選項：
  - TLS 1.2 版 – 此選項最安全，但舊版瀏覽器可能無法連線。
  - TLS 1.0、1.1 和 1.2 版 – 此選項與瀏覽器的相容程度最高。
7. 選擇 Save (儲存)，將您選取的通訊協定套用至負載平衡器。

您所做的變更需要一些時間才會生效。

## 使用設定安全性原則 AWS CLI

完成下列程序，使用 AWS Command Line Interface (AWS CLI) 設定安全政策。您可以使用 `update-load-balancer-attribute` 命令來執行此動作。若要取得更多資訊，請參閱《指AWS CLI 令參考》[update-load-balancer-attribute](#)中的。

**Note**

您必須先為 Lightsail 安裝 AWS CLI 並對其進行設定，然後才能繼續執行此程序。如需詳細資訊，請參閱[設定 AWS CLI 定使用 Lightsail](#)。

1. 開啟命令提示或終端機視窗。
2. 輸入下列命令，變更負載平衡器的 TLS 安全政策。

```
aws lightsail update-load-balancer-attribute --load-balancer-name LoadBalancerName --attribute-name TlsPolicyName --attribute-value AttributeValue
```

將命令中的以下範例文字更改為自訂文字：

- *LoadBalancerName* 具有您要變更其 TLS 安全性原則之負載平衡器的名稱。
- *AttributeValue* 使用 TLS-2016-08 或 TLS-FS-1-2-Res-2019-08 安全策略。

**Note**

命令中的 TlsPolicyName 屬性代表您希望編輯 TLS 安全政策，在負載平衡器上完成設定。

範例：

```
aws lightsail update-load-balancer-attribute --load-balancer-name MyLoadBalancer --attribute-name TlsPolicyName --attribute-value TLS-2016-08
```

您所做的變更需要一些時間才會生效。

## 將負載平衡器的 Lightsail 重新導向至 HTTPS

在 Amazon Lightsail 負載平衡器上設定 HTTPS 之後，您可以設定 HTTP 至 HTTPS 重新導向，以便使用 HTTP 連線瀏覽至您網站或 Web 應用程式的使用者會自動重新導向至加密的 HTTPS 連線。如需負載平衡器的詳細資訊，請參閱[負載平衡器](#)。

## 完成先決條件

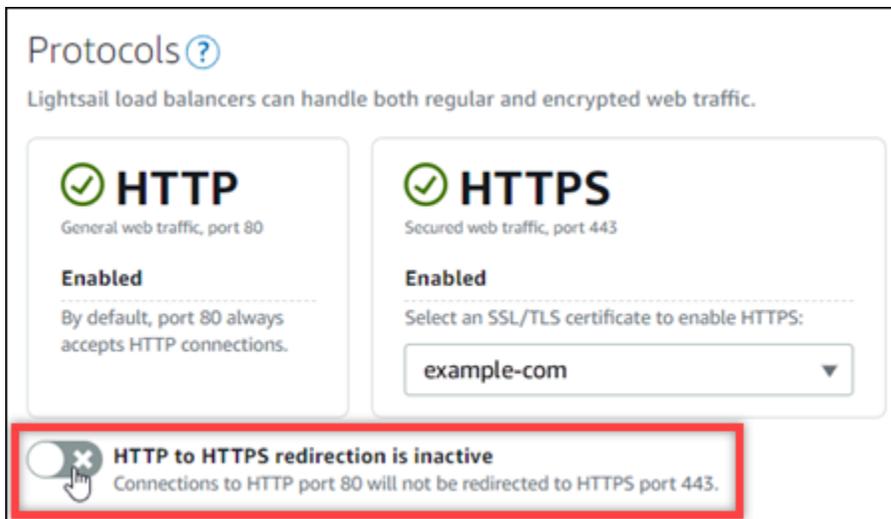
請先完成事前準備 (若尚未完成)：

- 建立 負載平衡器，並將其與執行個體連接。如需詳細資訊，請參閱[建立負載平衡器並將執行個體與其附接](#)。
- 建立 SSL/TLS 憑證，並將其連接到您的負載平衡器，以啟用 HTTPS。如需詳細資訊，請參閱[為 Lightsail 負載平衡器建立 SSL/TLS 憑證](#)。如需憑證的詳細資訊，請參閱 [SSL/TLS 憑證](#)。

## 使用 Lightsail 主控台在負載平衡器上設定 HTTPS 重新導向

完成下列程序，以使用 Lightsail 主控台在負載平衡器上設定 HTTPS 重新導向。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁，選擇 Networking (聯網) 索引標籤。
3. 選擇您要設定 HTTPS 重新引導機制的負載平衡器名稱。
4. 選擇 Inbound traffic (傳入流量) 索引標籤。
5. 您可以在頁面的 Protocols (通訊協定) 區段執行下列任一動作：



- 將引導選項切換為啟用，即可開啟 HTTP 至 HTTPS 的重新引導機制。
- 將引導選項切換為停用，即可關閉 HTTP 至 HTTPS 的重新引導機制。

您所做的變更需要一些時間才會生效。

## 為負載平衡器設定 HTTP 至 HTTPS 重新導向，並使用 AWS CLI

完成下列程序，以使用 AWS Command Line Interface (AWS CLI) 在負載平衡器上設定 HTTPS 重新導向。您可以使用 `update-load-balancer-attribute` 命令來執行此動作。若要取得更多資訊，請參閱《指AWS CLI 令參考》[update-load-balancer-attribute](#) 中的。

### Note

您必須先為 Lightsail 安裝 AWS CLI 並對其進行設定，然後才能繼續執行此程序。如需詳細資訊，請參閱[設定 AWS CLI 定使用 Lightsail](#)。

1. 開啟命令提示或終端機視窗。
2. 輸入下列命令，設定負載平衡器的 HTTPS 重新引導機制。

```
aws lightsail update-load-balancer-attribute --load-balancer-name LoadBalancerName
--attribute-name HttpsRedirectionEnabled --attribute-value AttributeValue
```

將命令中的以下範例文字取代為自訂文字：

- *LoadBalancerName* 使用您要啟動或停用 HTTP 至 HTTPS 重新導向之負載平衡器的名稱。
- *AttributeValue* 與 `true` 激活重定向，或停 `false` 用重定向。

### Note

命令中的 `HttpsRedirectionEnabled` 屬性代表您希望針對指定的負載平衡器編輯內容，指定是要啟用或停用 HTTPS 重新引導機制。

範例：

- 如要啟用負載平衡器的 HTTP 至 HTTPS 重新引導機制，請執行以下操作：

```
aws lightsail update-load-balancer-attribute --load-balancer-name MyLoadBalancer
--attribute-name HttpsRedirectionEnabled --attribute-value true
```

- 如要停用負載平衡器的 HTTP 至 HTTPS 重新引導機制，請執行以下操作：

```
aws lightsail update-load-balancer-attribute --load-balancer-name MyLoadBalancer
--attribute-name HttpsRedirectionEnabled --attribute-value false
```

您所做的變更需要一些時間才會生效。

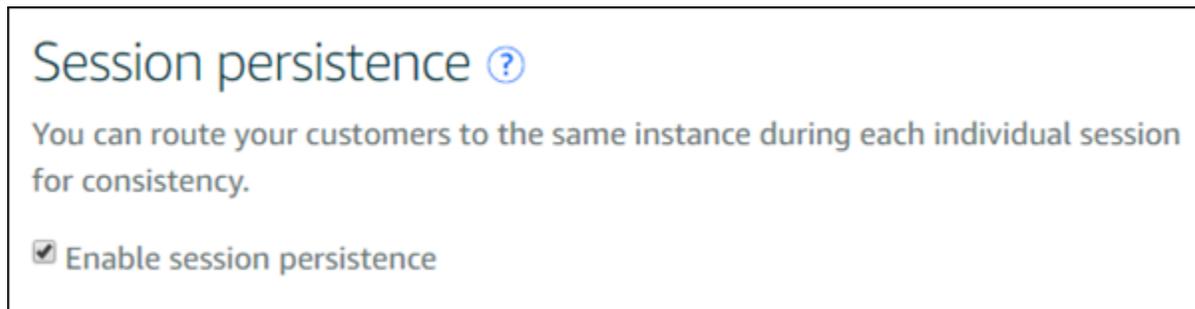
## 為 Lightsail 負載平衡器啟用工作階段持續性

您可以為您的使用者啟用工作階段持續性。如果您將工作階段資訊儲存於使用者瀏覽器本機，這會是很有用的。例如，您可能在 Amazon Lightsail 上運行帶有購物車的 Magento 電子商務應用程序。如果您開啟工作階段持續性，您的使用者可新增項目到購物車、離開網站，然後在返回時仍可在購物車中找到這些項目。

您也可以使用 AWS Command Line Interface (AWS CLI) 或 Lightsail API 調整 Cookie 持續時間。

### 啟用工作階段持續性

1. 在 Lightsail 首頁上，選擇 [網路功能]。
2. 選擇您的負載平衡器來進行管理。
3. 選擇 Inbound traffic (傳入流量) 索引標籤。
4. 選擇 Enable session persistence (啟用工作階段持續性)。



### 調整 Cookie 持續時間

您也可以為持續性工作階段調整 Cookie 持續時間。如果您想要特別長或短的持續時間，此功能是很有用的。例如，許多電子商務網站的持續時間非常長。這可讓客戶離開網站再返回時，不會遺失購物車中的項目。

如果您尚未這樣做，請設定 AWS CLI 並進行設定。

## 配置與 AWS Command Line Interface Amazon Lightsail 一起工作

1. 開啟命令提示或終端機視窗。
2. 鍵入以下 AWS CLI 命令，將 Cookie 持續時間增加到三天 ( 259,200 秒 )。

```
aws lightsail update-load-balancer-attribute --load-balancer-name LoadBalancerName
--attribute-name SessionStickiness_LB_CookieDurationSeconds --attribute-value
259200
```

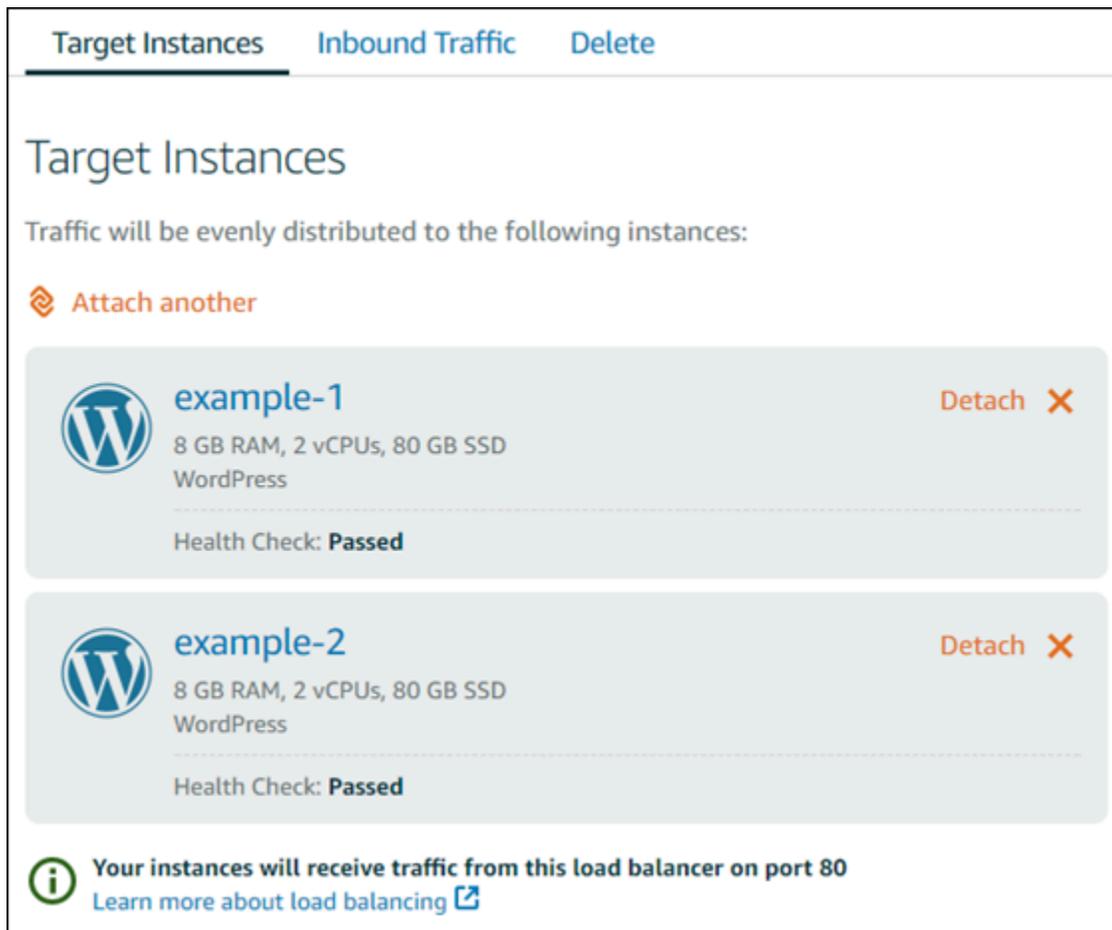
在命令中，替換 *LoadBalancerName* 使用負載平衡器的名稱。

如果成功完成設定，您應可看到以下回應。

```
{
  "operations": [
    {
      "status": "Succeeded",
      "resourceType": "LoadBalancer",
      "isTerminal": true,
      "operationDetails": "SessionStickiness_LB_CookieDurationSeconds",
      "statusChangedAt": 1511758936.174,
      "location": {
        "availabilityZone": "all",
        "regionName": "us-west-2"
      },
      "operationType": "UpdateLoadBalancerAttribute",
      "resourceName": "example-load-balancer",
      "id": "681c2bd9-9a51-402b-8ad2-12345EXAMPLE",
      "createdAt": 1511758936.174
    }
  ]
}
```

## 設定 Lightsail 負載平衡器的健康狀態檢查設定

Health 狀態檢查會在您將 Lightsail 執行個體連接至負載平衡器後立即啟動，之後每 30 秒進行一次。您可以在負載平衡器管理頁面上查看運作狀態檢查。



Target Instances   Inbound Traffic   Delete

## Target Instances

Traffic will be evenly distributed to the following instances:

 **Attach another**

 **example-1** Detach 

8 GB RAM, 2 vCPUs, 80 GB SSD  
WordPress

---

Health Check: **Passed**

 **example-2** Detach 

8 GB RAM, 2 vCPUs, 80 GB SSD  
WordPress

---

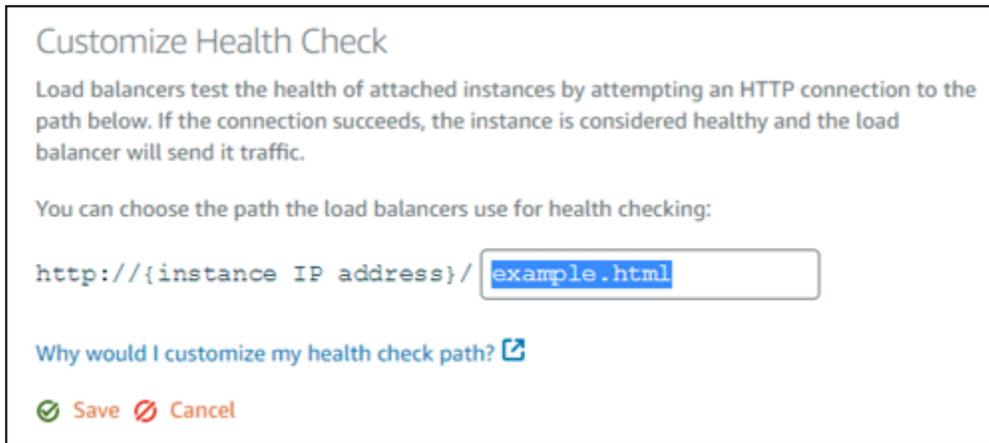
Health Check: **Passed**

 **Your instances will receive traffic from this load balancer on port 80**  
[Learn more about load balancing](#) 

## 自訂您的運作狀態檢查路徑

您可能會想要自訂您的運作狀態檢查路徑。例如，如果您的首頁載入速度緩慢或上面有很多影像，您可以設定 Lightsail 檢查載入速度較快的其他頁面。

1. 在 Lightsail 首頁上，選擇 [網路功能]。
2. 選擇您的負載平衡器來進行管理。
3. 在 Target instances (目標執行個體) 索引標籤，選擇 Customize health checking (自訂運作狀態檢查)。
4. 輸入有效的運作狀態檢查路徑，然後選擇 Save (儲存)。



## 運作狀態檢查指標

以下指標可協助您診斷運作狀態檢查問題。使用 AWS Command Line Interface 或 Lightsail API 傳回特定健全狀況檢查量度的相關資訊。

- **ClientTLSNegotiationErrorCount**-未與負載平衡器建立工作階段的用戶端所起始的 TLS 連線數目。可能的原因包含晶片或協定不相符。

Statistics : 最實用的統計資訊是 Sum。

- **HealthyHostCount** - 視為健康的目標執行個體數目。

Statistics : 最實用的統計資訊是 Average、Minimum 和 Maximum。

- **UnhealthyHostCount** - 視為不健康的目標執行個體數目。

Statistics : 最實用的統計資訊是 Average、Minimum 和 Maximum。

- **HTTPCode\_LB\_4XX\_Count**-源自負載平衡器的 HTTP 4XX 用戶端錯誤代碼數目。要求的格式不正確或不完整時，會產生用戶端錯誤。目標執行個體尚未收到這些要求。此計數不包含目標執行個體產生的任何回應碼。

Statistics : 最實用的統計資訊是 Sum。請注意，Minimum、Maximum 與 Average 都會傳回 1。

- **HTTPCode\_LB\_5XX\_Count**-源自負載平衡器的 HTTP 5XX 伺服器錯誤代碼數目。此計數不包含目標執行個體產生的任何回應碼。

Statistics : 最實用的統計資訊是 Sum。請注意，Minimum、Maximum 與 Average 都會傳回 1。請注意，Minimum、Maximum 與 Average 都會傳回 1。

- **HTTPCode\_Instance\_2XX\_Count**-目標執行個體產生的HTTP回應碼數目。這未包含負載平衡器所產生的任何回應碼。

Statistics : 最實用的統計資訊是 Sum。請注意 , Minimum、Maximum 與 Average 都會傳回 1。

- **HTTPCode\_Instance\_3XX\_Count**-目標執行個體產生的HTTP回應碼數目。這未包含負載平衡器所產生的任何回應碼。

Statistics : 最實用的統計資訊是 Sum。請注意 , Minimum、Maximum 與 Average 都會傳回 1。

- **HTTPCode\_Instance\_4XX\_Count**-目標執行個體產生的HTTP回應碼數目。這未包含負載平衡器所產生的任何回應碼。

Statistics : 最實用的統計資訊是 Sum。請注意 , Minimum、Maximum 與 Average 都會傳回 1。

- **HTTPCode\_Instance\_5XX\_Count**-目標執行個體產生的HTTP回應碼數目。這未包含負載平衡器所產生的任何回應碼。

Statistics : 最實用的統計資訊是 Sum。請注意 , Minimum、Maximum 與 Average 都會傳回 1。

- **InstanceResponseTime** - 要求離開負載平衡器之後到收到目標執行個體回應之前所經歷的時間(秒)。

Statistics : 最實用的統計資訊是 Average。

- **RejectedConnectionCount**-因負載平衡器已達其連線數目上限而拒絕的連線數目。

Statistics : 最實用的統計資訊是 Sum。

- **RequestCount**-已處理的要求數目IPv4。此計數只包含具有負載平衡器目標執行個體所產生之回應的要求。

Statistics : 最實用的統計資訊是 Sum。請注意 , Minimum、Maximum 與 Average 都會傳回 1。

## 主題

- [設定負載平衡器健康狀態檢查](#)

## 設定負載平衡器健康狀態檢查

根據預設，Lightsail 會在 Web 應用程式的根 ("/") 對執行個體執行健康狀態檢查。運作狀態檢查用於監控已註冊執行個體的運作狀態，因此負載平衡器只能傳送請求至運作狀態良好的執行個體。在您將執行個體連接到負載平衡器時，運作狀態檢查就會立刻開始進行。

將傳回下列狀態之一。

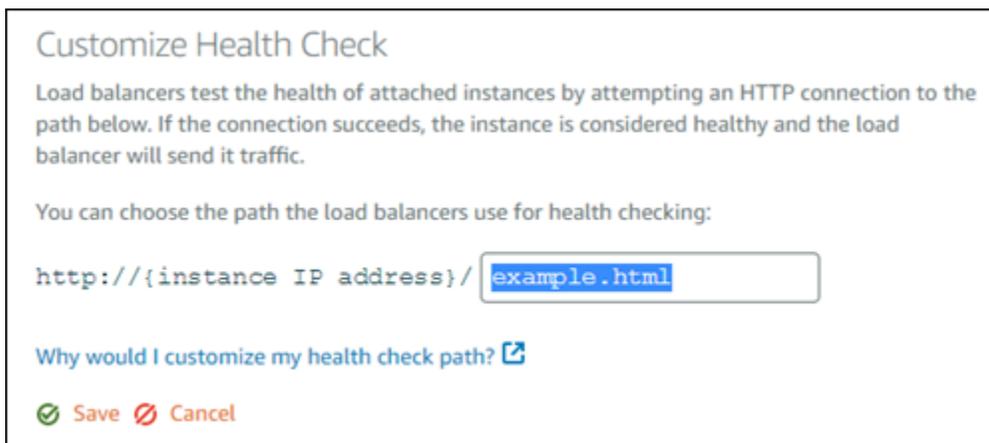
- Passed (通過)
- 失敗

如果您的健康狀態檢查失敗，您可以嘗試使用 AWS Command Line Interface 或 Lightsail API 來找出什麼問題。詳細資訊請參閱疑難排解指南。

### 自訂您的運作狀態檢查路徑

您可能會想要自訂您的運作狀態檢查路徑。例如，如果您的首頁載入速度緩慢或上面有很多影像，您可以設定 Lightsail 檢查載入速度較快的其他頁面。

1. 在 Lightsail 首頁上，選擇 [網路功能]。
2. 選擇您的負載平衡器來進行管理。
3. 在 Target instances (目標執行個體) 索引標籤，選擇 Customize health checking (自訂運作狀態檢查)。
4. 輸入有效的運作狀態檢查路徑，然後選擇 Save (儲存)。



Customize Health Check

Load balancers test the health of attached instances by attempting an HTTP connection to the path below. If the connection succeeds, the instance is considered healthy and the load balancer will send it traffic.

You can choose the path the load balancers use for health checking:

`http://{instance IP address}/`

[Why would I customize my health check path?](#)

Save  Cancel

## 將執行個體從 Lightsail 負載平衡器中分離

如果您不想再將執行個體連接到 Amazon Lightsail 負載平衡器，可以將其分離。當您將 Lightsail 執行個體從負載平衡器中分離時，我們會等到不再需要指定的執行個體，然後再分離。

1. 在 Lightsail 首頁上，選擇 [網路功能]。
2. 選擇您要管理的負載平衡器。
3. 在 Target instances (目標執行個體) 標籤上，選擇您要分離之負載平衡器旁的 Detach (分離)。

## 刪除負載平衡器

如果不再需要 Lightsail 負載平衡器，您可以刪除該負載平衡器。刪除負載平衡器也會分離任何連接至該負載平衡器的 Lightsail 執行個體，但不會刪除 Lightsail 執行個體。如果您使用SSL/TLS憑證啟用加密 (HTTPS) 流量，刪除負載平衡器也會永久刪除與負載平衡器相關聯的任何SSL/TLS憑證。

### Important

刪除 Lightsail 負載平衡器及其相關聯的憑證是最終結果，且無法復原。

1. 在 Lightsail 首頁上，選擇 [網路功能]。
2. 選擇您要刪除的負載平衡器。
3. 選擇 刪除。
4. 選擇 Delete load balancer (刪除負載平衡器)。
5. 選擇 Yes, delete (是，刪除)。

## 利用 Lightsail 內容交付散佈在全球提供網頁內容

Lightsail 散佈使用遍佈全球的伺服器網路 (也稱為邊緣位置)，以便更快地將內容交付給使用者。若要使用散發，您必須先在 Lightsail 執行個體或容器服務或連接至 Lightsail 負載平衡器的多個執行個體上建立並託管網站或 Web 應用程式，或將靜態內容儲存在 Lightsail 值區上。然後，您可以建立並設定 Lightsail 發行版，以從執行個體、容器服務、負載平衡器或儲存貯體提取、快取和提供內容。執行個體、容器服務、負載平衡器或儲存貯體亦稱為分發的原始伺服器，是內容的最終來源。

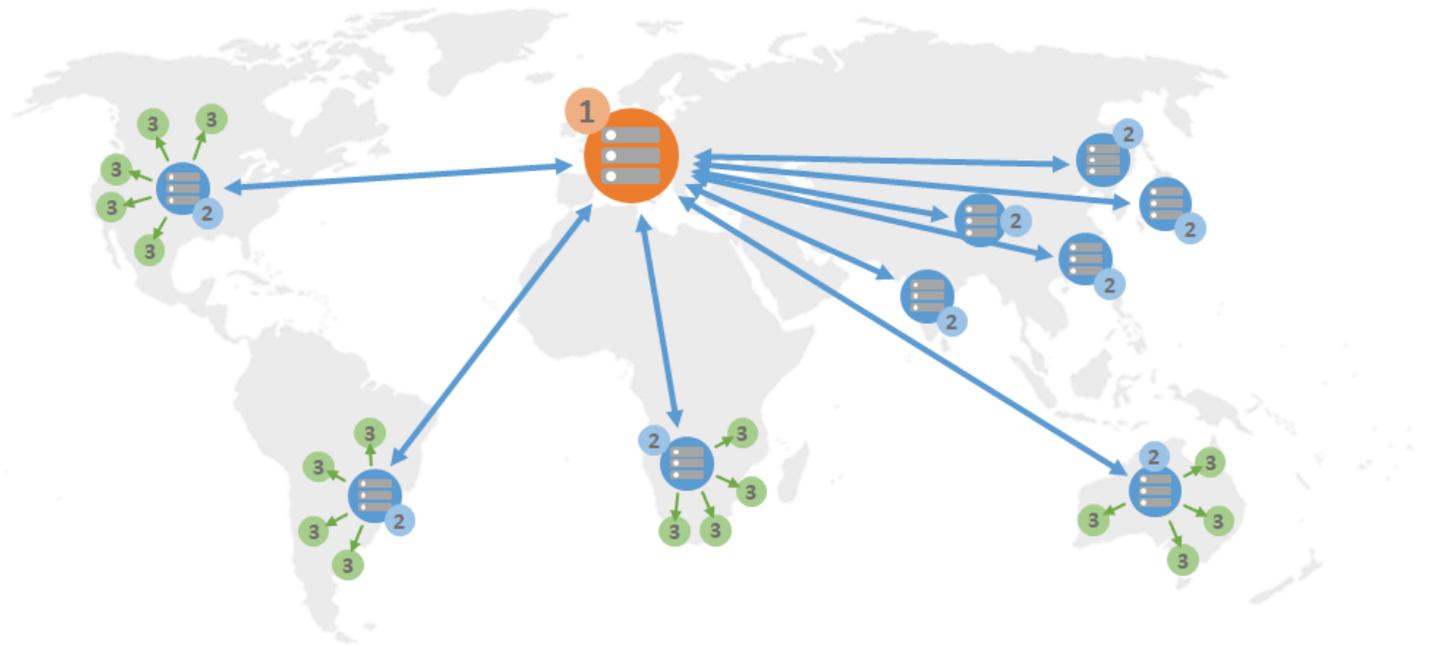
當使用者造訪您透過分發提供的網站來請求內容時，請求會根據延遲路由到最近的位置。然後分發會執行下列其中一個動作：

- 若已經在節點中快取內容，分發會立即將其提供給使用者。
- 若尚未在節點中快取內容，分發會從指定原始伺服器擷取、快取內容並提供給使用者。

在您為分發指定的快取壽命 (存留時間) 期間，內容會在節點中快取，以便立即滿足相同位置的其他請求。當快取的內容達到快取壽命期限時，系統會從節點中將其清除。下次有內容請求路由至節點時，分發會擷取、快取並提供內容。

如下圖所示：

- 1 代表發行版的來源，例如裝載您網站的 Lightsail 執行個體或容器服務、連接執行個體的負載平衡器，或是託管靜態內容的值區。
- 2 代表分發，或是從原始伺服器提取、快取和提供內容的節點。
- 3 代表從節點獲得內容的使用者。

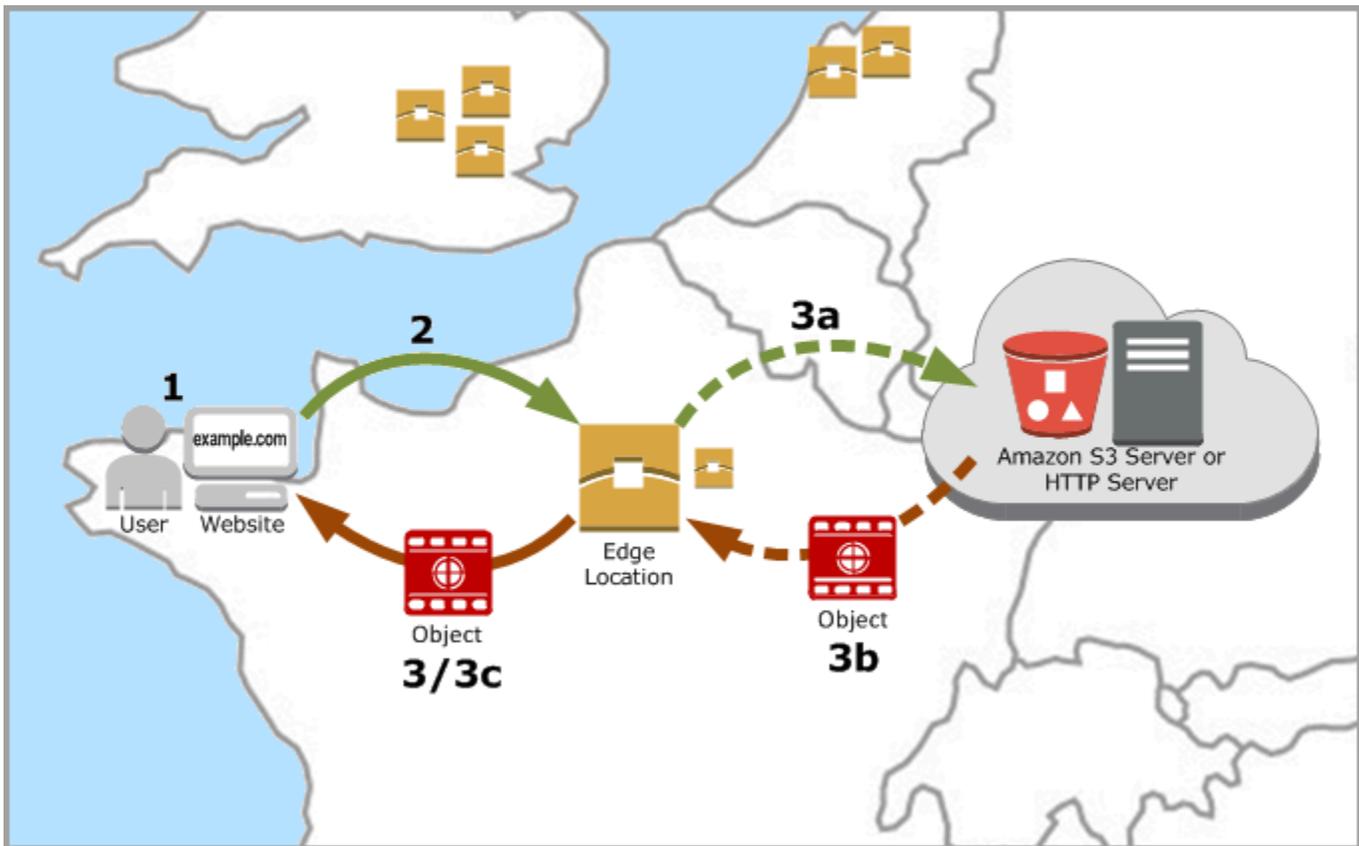
**Note**

本圖表僅供說明之用，並不顯示實際節點。如需有關節點的詳細資訊，請參閱本指南後述的[節點和 IP 地址範圍](#)。

舉例來說，如果您的網站託管於法國，法國其他地區的使用者想要查看您的內容時，頁面會在幾毫秒內載入。

如果訪客的所在位置不在附近，事情就會變得有點困難。

如果澳洲的使用者想要查看您的內容，瀏覽器就必須從位於法國的伺服器擷取內容，再將內容提供給幾千英哩以外的使用者。如果不同國家/地區的使用者同時提出查看相同內容的請求，伺服器會因為收到眾多請求而需要更長的時間才能載入及提供內容。這會影響系統為最終使用者載入內容的速度。



CDN 能在節點快取您的網站內容，藉此解決這種情況。比起以往僅從單一中央資源提供內容，這種內容提供方式更快速，也更有效率。檢視者在您的網站上或透過您的應用程式發出請求時，DNS 會將請求路由到最能及時滿足使用者請求的位置。使用者從附近位置存取內容，而不是所有使用者存取遠處同一個中央資源。

## 使用案例

### 提供快速且安全的網站

Lightsail 發佈可加快向全球觀眾傳送內容 (例如網站頁面、影像 JavaScript、樣式表等) 的速度。藉由使用分發，您可以利用 AWS 骨幹網路和邊緣伺服器，在檢視者造訪您的網站時提供快速且安全可靠的體驗。

### 提升網站安全

分發可讓您利用 TLS 終止，透過將密碼編譯處理卸載至分發，減少原始伺服器的負載，達到強化網站及提升效能的目的。您可以將您註冊的網域名稱與 Lightsail SSL/TLS 憑證一起使用，為您的散佈啟用超文字傳輸通訊協定安全 (HTTPS)。使用者會對分發建立加密 HTTPS 連線，而分發則會使用 HTTP 從原始伺服器提取內容。

## 應用程式最佳化

針對各種應用程式 (包括 WordPress 靜態網站) 輕鬆最佳化您的散佈版本。使用分發來快取和提供內容亦可減少原始伺服器上的負載，因為大多數請求是由分發提供，而非執行個體、容器服務、負載平衡器或儲存貯體。

## 設定分發

這些是使用 Lightsail 執行個體和發行版為您的網站或 Web 應用程式提供服務時所需遵循的一般步驟。

1. 視您要將執行個體、容器服務或儲存貯體用於分發而定，完成下列步驟之一。

- 建立 Lightsail 實體來代管您的內容。執行個體會作為分發的原始伺服器。原始伺服器會儲存內容的原始最終版本。如需詳細資訊，請參閱[建立執行個體](#)。

將 Lightsail 靜態 IP 附加至您的執行個體。如果您停止並啟動執行個體，則執行個體的預設公有 IP 地址會變更，使分發與原始伺服器執行個體之間的連線中斷。停止並啟動執行個體時，靜態 IP 不會變更。如需詳細資訊，請參閱[建立靜態 IP 並將其附接至執行個體](#)。

將內容和檔案上傳至執行個體。您的檔案 (也稱為物件) 通常包含網頁、影像和媒體檔案，但也可以是能透過 HTTP 提供的任何內容。

- 建立 Lightsail 容器服務來託管您的網站或網路應用程式。容器服務會作為分發的原始伺服器。原始伺服器會儲存內容的原始最終版本。如需詳細資訊，請參閱[建立 Amazon Lightsail 容器服務](#)。
- 建立 Lightsail 值區來儲存您的靜態內容。儲存貯體會作為分發的原始伺服器。原始伺服器會儲存內容的原始最終版本。如需詳細資訊，請參閱[建立儲存貯體](#)。

使用 Lightsail 主控台、AWS Command Line Interface (AWS CLI) 和 AWS API，將檔案上傳到值區。如需有關上傳檔案的詳細資訊，請參閱[將檔案上傳至儲存貯體](#)。

2. (選擇性) 如果您的網站託管在執行個體上需要容錯，請建立 Lightsail 負載平衡器。然後，將執行個體的多件複本連接至負載平衡器。您可以將負載平衡器 (含一或多個連接其上的執行個體) 設定為分發的原始伺服器，而不將執行個體設定為原始伺服器。如需詳細資訊，請參閱[建立負載平衡器並將執行個體與其附接](#)。

3. 建立 Lightsail 散發，並將您的執行個體、容器服務、負載平衡器或值區設定為來源。同時，您可以指定詳細資訊，例如內容的快取壽命，以及網站或 Web 應用程式中要快取的元素。如需詳細資訊，請參閱[建立分發](#)。

4. (選擇性) 如果發行版的來源是 WordPress 執行個體，您必須在執行個體中編輯 WordPress 設定檔案，讓您的 WordPress 網站能夠與您的發行版一起使用。如需詳細資訊，請參閱[設定您的 WordPress 執行個體以搭配您的發佈](#)使用。

5. (選擇性) 建立 Lightsail DNS 區域，以便在主控台中管理網域的 DNS。這可讓您輕鬆將網域對應至 Lightsail 資源。如需詳細資訊，請參閱[建立 DNS 區域以管理域的 DNS 記錄](#)。或者，您亦可繼續在目前的位置託管網域的 DNS。
6. 為您的網域建立 Lightsail SSL/TLS 憑證，以便在您的發佈中使用該憑證。Lightsail 發行版本需要使用 HTTPS，因此您必須要求您的網域的 SSL/TLS 憑證，才能在您的散佈中使用該憑證。如需詳細資訊，請參閱[為分發建立 SSL/TLS 憑證](#)。
7. 為分發啟用自訂域，以便搭配使用所註冊的域名稱和分發。若要啟用自訂網域，您必須指定為網域建立的 Lightsail SSL/TLS 憑證。此操作會將網域新增至分發，並啟用 HTTPS。如需詳細資訊，請參閱[啟用分發的自訂域](#)。
8. 將別名記錄新增至網域的 DNS，以開始將網域流量路由至分發。新增別名記錄之後，造訪您網域的使用者會透過分發路由。如需詳細資訊，請參閱[將域指向分發](#)。
9. 測試分發是否正在快取內容。如需詳細資訊，請參閱[測試您的分發](#)。

## 節點和 IP 地址範圍

Lightsail 發行版使用與 Amazon CloudFront 相同的邊緣伺服器和 IP 地址範圍。如需 CloudFront 邊緣伺服器位置的清單，請參閱[Amazon CloudFront 產品詳細資訊頁面](#)。如需 CloudFront IP 範圍的清單，請參閱[CloudFront 全域 IP 清單](#)。

## 建立內 Lightsail 遞網路發佈

在本指南中，我們將向您展示如何使用 Lightsail 主控台建立 Amazon Lightsail 分發，並說明您可以設定的分發設定。如需有關分發的詳細資訊，請參閱[內容交付網路分發](#)。

### 內容

- [先決條件](#)
- [原始伺服器資源](#)
- [原始伺服器通訊協定政策](#)
- [快取行為和快取預設](#)
- [最適合 WordPress 緩存預設](#)
- [預設行為](#)
- [目錄和檔案覆寫](#)
- [進階快取設定](#)

- [分發計劃](#)
- [建立分發](#)
- [後續步驟](#)

## 必要條件

在您開始建立分發之前，請先完成以下事前準備：

1. 視您要將執行個體、容器服務或儲存貯體用於分發而定，完成下列步驟之一。
  - 建立 Lightsail 實體來代管您的內容。執行個體會作為分發的原始伺服器。原始伺服器會儲存內容的原始最終版本。如需詳細資訊，請參閱[建立執行個體](#)。

將 Lightsail 靜態 IP 附加至您的執行個體。如果您停止並啟動執行個體，則執行個體的預設公有 IP 地址會變更，使分發與原始伺服器執行個體之間的連線中斷。停止並啟動執行個體時，靜態 IP 不會變更。如需詳細資訊，請參閱[建立靜態 IP 並將其附接至執行個體](#)。

將內容和檔案上傳至執行個體。您的檔案 (也稱為物件) 通常包含網頁、影像和媒體檔案，但也可以是能透過 HTTP 提供的任何內容。

- 建立 Lightsail 容器服務來託管您的網站或網路應用程式。容器服務會作為分發的原始伺服器。原始伺服器會儲存內容的原始最終版本。如需詳細資訊，請參閱[建立 Amazon Lightsail 容器服務](#)。
- 建立 Lightsail 值區來儲存您的靜態內容。儲存貯體會作為分發的原始伺服器。原始伺服器會儲存內容的原始最終版本。如需詳細資訊，請參閱[建立儲存貯體](#)。

使用 Lightsail 主控台、AWS Command Line Interface (AWS CLI) 和 AWS API，將檔案上傳到值區。如需有關上傳檔案的詳細資訊，請參閱[將檔案上傳至儲存貯體](#)。

2. (選擇性) 如果您的網站需要容錯，請建立 Lightsail 負載平衡器。然後，將執行個體的多件複本連接至負載平衡器。您可以將負載平衡器 (含一或多個連接其上的執行個體) 設定為分發的原始伺服器，而不將執行個體設定為原始伺服器。如需詳細資訊，請參閱[建立負載平衡器並將執行個體與其附接](#)。

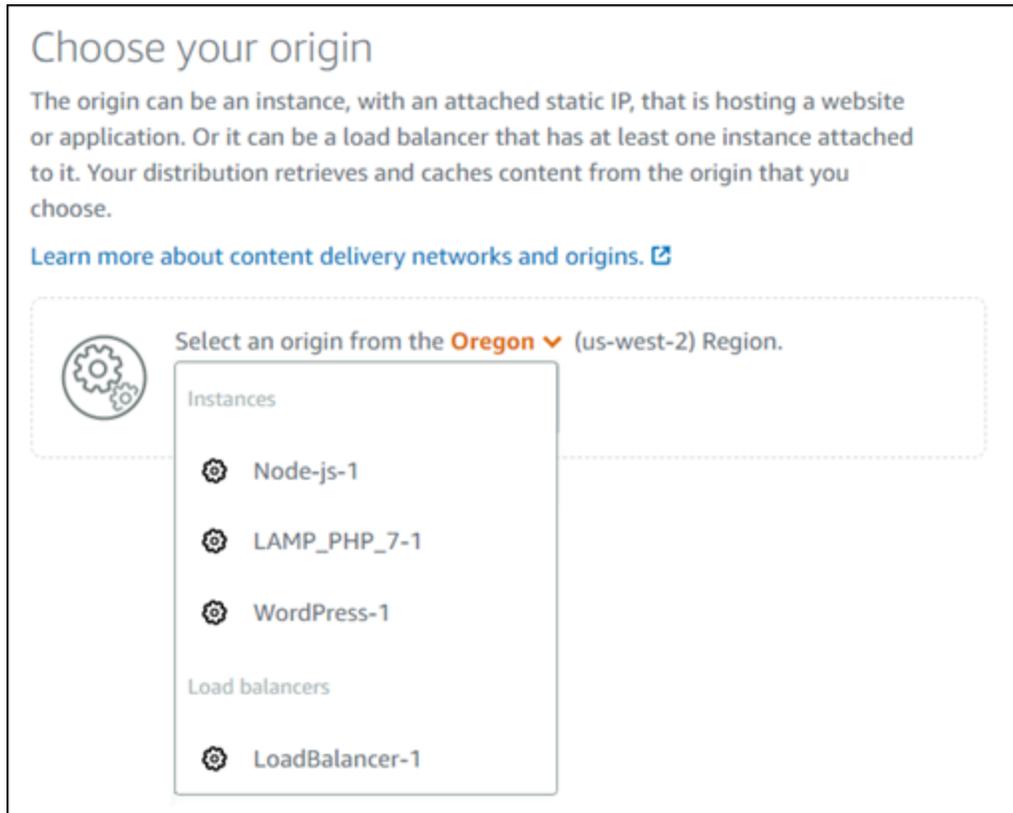
## 原始伺服器資源

原始伺服器是分發內容的最終來源。建立分發時，您可以選擇裝載網站或 Web 應用程式內容的 Lightsail 執行個體、容器服務、儲存貯體或負載平衡器 (連接一個或多個執行個體)。

**Note**

目前，僅限 IPv4 的執行個體無法設定為 Lightsail 內容傳遞網路 (CDN) 分發的來源。

每個分發僅能選擇一個原始伺服器。在建立分發後，您可以隨時變更原始伺服器。如需詳細資訊，請參閱[變更分發的原始伺服器](#)。



## 原始伺服器通訊協定政策

您的分發在從原始伺服器提取內容時所使用的通訊協定政策，即為原始伺服器通訊協定政策。在您選擇分發的原始伺服器後，您應判斷分發在從原始伺服器提取內容時，是否應使用超文字傳輸通訊協定 (HTTP) 或超文字傳輸通訊協定安全 (HTTPS)。如果您的原始伺服器未設定使用 HTTPS，則必須使用 HTTP。

您可以為分發選擇以下其中一個原始伺服器通訊協定政策：

- 僅限 HTTP - 您的分發僅使用 HTTP 來存取原始伺服器。這是預設設定。
- 僅限 HTTPS - 您的分發僅使用 HTTPS 來存取原始伺服器。

編輯原始伺服器通訊協定政策的步驟包含在本指南後續的[建立分發](#)章節中。

### Note

當您選取 Lightsail 儲存貯體做為發佈的來源時，原始通訊協定原則僅預設為 HTTPS。在儲存貯體為分發原始伺服器時，您便無法變更原始伺服器通訊協定政策。

## 快取行為和快取預設

快取預設會針對您在原始伺服器上託管的內容類型，自動設定分發的設定。例如，選擇 Best for static content (靜態內容最佳選擇) 預設，會使用最適合靜態網站的設定來自動設定您的分發。如果您的網站託管在 WordPress 執行個體上，請選擇「最適合 WordPress 預設」，讓您的發佈自動設定為與您的 WordPress 網站搭配使用。

### Note

當您選取 Lightsail 值區做為發行版本的來源時，無法使用快取預設集選項。我們會自動套用最適合存放在儲存貯體中靜態內容的分發設定。

您可以針對分發選擇下列其中一個快取預設：

- Best for static content (靜態內容最佳選擇) - 此預設會設定您的分發為快取所有內容。如果您在原始伺服器上託管靜態內容 (例如靜態 HTML 頁面)，或託管不會針對造訪您網站的每位使用者變更的內容，則此預設非常適合。當您選擇此預設時，系統會快取分發中的所有內容。
- Best for dynamic content (動態內容的最佳選擇) - 此預設會將您的分發設定為不快取，除了您在 Create a distribution (建立分發) 頁面的 Directory and file overrides (目錄和檔案覆寫) 區段中指定為 Cache (快取) 的內容以外。如需詳細資訊，請參閱本指南中的[目錄和檔案覆寫](#)。如果您在原始伺服器上託管動態內容，或託管可能會針對造訪您網站或 Web 應用程式的每位使用者變更的內容，則此預設非常適合。
- 最適合 WordPress-此預設集可將您的發行版配置為緩存除了實例wp-includes/和wp-content/目錄中的文件以外的 WordPress 任何內容。如果您的來源是使用 Bitnami WordPress 認證和自動藍圖 (不包括多網站藍圖) 的執行個體，則此預設集是理想的選擇。如需有關此預設集的詳細資訊，請參閱[最適合 WordPress 快取預設集](#)。

**Note**

無法選取 Custom settings (自訂設定) 預設。如果您選擇某個預設，然後手動修改分發設定，則系統會自動為您選取該預設。

快取預設集只能在 Lightsail 主控台中指定。您無法使用 Lightsail API 和開發套件來指定它。AWS CLI

## 最適合 WordPress 緩存預設

當您選取使用「由 Bitnami WordPress 認證」和「自動化」藍圖做為發佈來源的執行個體時，Lightsail 會詢問您是否要將最佳 WordPress 快取預設集套用至您的發佈。如果您應用當前，則會自動配置您的分發以最適合您的 WordPress 網站。您不需要套用其他分發設定。最適合 WordPress 預設緩存除了網站 `wp-includes/` 和 `wp-content/` 目錄中的文件之外沒有任何內 WordPress 容。它也會將分發設定為每天清除其快取 (快取壽命為 1 天)，允許所有 HTTP 方法、僅轉送 Host 標頭，不轉送 Cookie 並轉送所有查詢字串。

**Important**

您必須在執行個體中編輯 WordPress 設定檔，才能讓您的 WordPress 網站與您的發行版一起運作。如需詳細資訊，請參閱 [設定您的 WordPress 執行個體以搭配您的發佈](#) 使用。

## 預設行為

預設行為會指定分發處理內容快取的方式。系統會根據您選取的 [快取預設](#) 自動為您指定分發的預設行為。如果您選取不同的預設行為，則快取預設會自動變更為 Custom settings (自訂設定)。

**Note**

當您選取 Lightsail 值區做為發佈的原點時，無法使用預設行為選項。我們會自動套用最適合存放在儲存貯體中靜態內容的分發設定。

您可以為分發選擇以下其中一個預設行為：

- 快取所有內容 - 這種行為會將分發設定為快取整個網站並將其作為靜態內容。如果您的原始伺服器託管的內容不會因檢視器而變更，或者您的網站不使用 Cookie、標頭或查詢字串來個人化內容，則此選項非常適合。
- 不快取 - 這種行為會將您的分發設定為只快取您指定的原始伺服器檔案和資料夾路徑。如果您的網站或 Web 應用程式使用 Cookie、標頭和查詢字串為個別使用者個人化內容，則此選項非常適合。如果您選取此選項，您必須指定要快取的[目錄和檔案路徑覆寫](#)。

## 目錄和檔案覆寫

目錄和檔案覆寫可用來覆寫您選取的預設行為，或在該行為中新增例外狀況。例如，如果您選擇快取所有內容，請使用覆寫來指定分發不該快取的目錄、檔案或檔案類型。或者，如果您選擇不快取，請使用覆寫來指定分發應該快取的目錄、檔案或檔案類型。

在該頁面的 Directory and file overrides (目錄和檔案覆寫) 區段中，您可以指定目錄或檔案的路徑，以進行快取或不快取。使用星號符號指定萬用字元目錄 (path/to/assets/\*) 和檔案類型 (\*.html、\*.jpg、\*.js)。目錄和檔案路徑區分大小寫。

### Note

當您選取 Lightsail 值區做為發行版本的原點時，無法使用目錄和檔案覆寫選項。存放在所選儲存貯體中的所有內容都會受到快取。

以下僅為如何指定目錄和檔案覆寫的範例：

- 指定下列項目，快取在 Lightsail 實體上執行之 Apache 網頁伺服器之文件根目錄中的所有檔案。

```
var/www/html/
```

- 指定下列檔案，以僅快取 Apache Web 伺服器文件根目錄中的索引頁面。

```
var/www/html/index.html
```

- 指定下列項目，以僅快取 Apache Web 伺服器文件根目錄中的 .html 檔案。

```
var/www/html/*.html
```

- 指定下列項目，以僅快取 Apache Web 伺服器文件根目錄映像子目錄中的 .jpg、.png 和 .gif 檔案。

```
var/www/html/images/*.jpg
```

```
var/www/html/images/*.png
```

```
var/www/html/images/*.gif
```

指定下列項目，以僅快取 Apache Web 伺服器文件根目錄映像子目錄中的所有檔案。

```
var/www/html/images/
```

## 進階快取設定

進階設定可用來指定分發中的內容快取壽命、允許的 HTTP 方法、HTTP 標頭轉送、Cookie 轉送和查詢字串轉送。您指定的進階設定僅適用於分發所快取的目錄和檔案，包括您指定為 Cache (快取) 的目錄和檔案覆寫。

### Note

當您選取 Lightsail 儲存貯體作為發行版本的來源時，無法在 [建立發佈] 頁面上使用進階快取設定。我們會自動套用最適合存放在儲存貯體中靜態內容的分發設定。不過，您可以在分發建立之後修改分發管理頁面中的進階快取設定。

您可以進行下列進階設定：

### Cache lifespan (TTL) (快取壽命 (TTL))

在分發轉送另一個請求到原始伺服器，以判斷您的內容是否已更新之前，請控制您的內容在分發快取中停留的時間量。預設值為一天。縮短持續時間後，您可以更好地提供動態內容。增加持續時間會讓您的使用者取得更好的效能，因為檔案更有可能是直接從節點提供。增加持續時間也能減少原始伺服器的負載，因為分發提取內容的頻率減少。

### Note

您指定的快取壽命值僅在原始伺服器不新增 HTTP 標頭至您的內容時才適用，例如不新增 Cache-Control max-age、Cache-Control s-maxage 或 Expires。

## Allowed HTTP methods (允許的 HTTP 方法)

控制分發處理及轉送至原始伺服器的 HTTP 方法。HTTP 方法表示想要在原始伺服器上執行的動作。例如，GET 方法會從您的原始伺服器擷取資料，而 PUT 方法會請求將封閉的實體存放在您的原始伺服器上。

您可以為分發選擇下列其中一個 HTTP 方法選項：

- Allow GET, HEAD, OPTIONS, PUT, PATCH, POST, and DELETE methods (允許 GET、HEAD、OPTIONS、PUT、PATCH、POST 和 DELETE 方法)
- Allow the GET, HEAD, and OPTIONS methods (允許 GET、HEAD 和 OPTIONS 方法)
- Allow the GET and HEAD methods (允許 GET 和 HEAD 方法)

您的分發一律會快取針對 GET 與 HEAD 請求的回應。如果您選擇允許這些請求，您的分發也會快取針對 OPTIONS 請求的回應。您的分發不會快取針對任何其他 HTTP 方法的回應。如需詳細資訊，請參閱 [HTTP 方法](#)。

### Important

如果您將分發設定為允許支援的所有 HTTP 方法，則您必須將原始伺服器執行個體設定為處理所有方法。例如，如果因為想要使用 POST，而將您的分發設定為允許這些方法，則您必須將原始伺服器設定為以適當方式處理 DELETE 請求，讓檢視器無法刪除您不希望其刪除的資源。如需詳細資訊，請搜尋您的網站或 Web 應用程式的文件。

## HTTP header forwarding (HTTP 標頭轉送)

控制分發是否根據指定標頭的值來快取內容，如果是的話，是根據哪些標頭的值。HTTP 標頭攜帶有關用戶端瀏覽器、請求的頁面、原始伺服器等的資訊。例如，Accept-Language 標頭會傳送用戶端的語言 (例如針對英文是 en-US)，以便原始伺服器能以用戶端語言的內容 (如果可用) 來回應。

您可以為分發選擇下列其中一個 HTTP 標頭選項：

- Forward no headers (不轉送標頭)
- Forward only the headers I specify (只轉送我指定的標頭)

如果您選取 Forward no headers (不轉送標頭)，您的分發不會根據標頭值快取內容。無論您選取的選項為何，您的分發皆會轉送特定標頭至原始伺服器，並根據您轉送的標頭來採取特定動作。如需有關分發處理標頭轉送的詳細資訊，請參閱 [HTTP 請求標頭和分發行為](#)。

### Cookie forwarding (Cookie 轉送)

控制您的分發是否將 Cookie 轉送到原始伺服器，若要轉送，是哪些 Cookie 要轉送。Cookie 包含傳送至原始伺服器的一小段資料，例如有關訪客在您原始伺服器網頁上的動作的資訊，以及訪客提供的任何資訊，例如他們的姓名和興趣。

您可以為您的分發選擇下列其中一個 Cookie 轉送選項：

- Don't forward cookies (請勿轉送 Cookie)
- Forward all cookies (轉送所有 Cookie)
- Forward cookies I specify (轉送我指定的 Cookie)

如果您選擇 Forward all cookies (轉送所有 Cookie)，無論您的應用程式使用多少 Cookie，您的分發都會轉送所有 Cookie。如果您選擇 Forward cookies I specify (轉送我指定的 Cookie)，然後在顯示的文字方塊中輸入您要分發轉送之 Cookie 的名稱。當您指定 Cookie 名稱時，您可以指定以下萬用字元：

- \* 符合 Cookie 名稱中的 0 個或多個字元
- ? 完全符合 Cookie 名稱中的一個字元

例如，假設檢視器針對某個物件的請求包含名稱為 `userid_member-number` 的 Cookie。其中每個使用者都有 member-number (`userid_123`、`userid_124`、`userid_125` 等) 的唯一值。您希望分發為每個成員快取單獨版本的內容。您可以透過將所有 Cookie 轉送到原始伺服器以達成此目標，但檢視器請求包含一些您不希望分發快取的 Cookie。您可以指定以下值作為 Cookie 名稱，這會導致分發將所有以 `userid_` 開頭的 Cookie 轉送至您的原始伺服器：`userid_*`

### Query string forwarding (查詢字串轉送)

控制您的分發是否將查詢字串轉送至原始伺服器，若要轉送，是哪些查詢字串要轉送。查詢字串是指派值給指定參數的 URL 的一部分。例如，`https://example.com/over/there?name=ferret` URL 包含 `name=ferret` 查詢字串。當伺服器收到該等頁面的請求時，它可能會執行一個程式，並將不變的 `name=ferret` 查詢字串傳遞至該程式。問號用作分隔符號，而非查詢字串的一部分。

您可以選擇讓分發不轉送查詢字串，或只轉送您指定的查詢字串。如果您的原始伺服器傳回相同版本的內容，而不考慮查詢字串參數的值，請選擇不轉送查詢字串。這會讓分發更有可能提供來自快取的請

求，從而提高效率並降低原始伺服器的負載。如果您的原始伺服器根據一或多個查詢字串參數傳回不同版本的內容，請選擇只轉送您指定的查詢字串。

## 分發計劃

分發計劃會指定每月的資料傳輸配額和分發成本。如果您的分發傳輸的資料數量超過計劃的每月資料傳輸配額，則會向您收取超額費用。如需詳細資訊，請參閱 [Lightsail 定價頁面](#)。

若要避免產生超額費用，請將目前的分發計劃變更為不同的計劃，以便在分發超過每月配額之前，提供更多的每月資料傳輸量。在每個 AWS 帳單週期內，您只能變更一次配送方案。如需有關在建立分發計畫後再變更的詳細資訊，請參閱 [變更分發計畫](#)。

## 建立分發

完成下列程序以建立分發。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁，選擇 Networking (聯網) 索引標籤。
3. 選擇 Create Distribution (建立分佈)。
4. 在頁面的選擇原始伺服器區段中，選擇已在其中建立原始伺服器資源的 AWS 區域。

分發為全域資源。他們可以引用任何來源 AWS 區域，並在全球範圍內分發其內容。

5. 選擇您的原始伺服器。來源可以是 Lightsail 執行個體、容器服務、儲存貯體或負載平衡器 (連接一或多個執行個體)。如需詳細資訊，請參閱 [原始伺服器資源](#)。

### Important

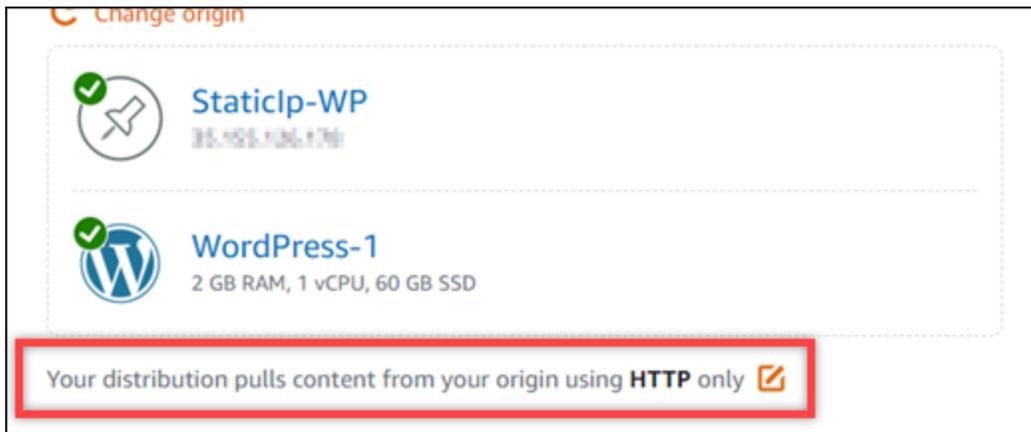
如果您選擇 Lightsail 容器服務做為分發的來源，Lightsail 會自動將分發的預設網域名稱新增為容器服務上的自訂網域。這樣就可以在分發和容器服務之間路由流量。但是，在某些情況下，您可能需要手動將分發的預設網域名稱新增至容器服務。如需詳細資訊，請參閱 [將分發的預設域新增至容器服務](#)。

6. (選用) 若要變更來源通訊協定政策，請選擇顯示於分發使用的目前原始伺服器通訊協定政策旁的鉛筆圖示。如需詳細資訊，請參閱 [原始伺服器通訊協定政策](#)。

此選項列於該頁面的 Choose your origin (選擇原始伺服器) 區段中，位於您為分發選取的原始伺服器資源下方。

**Note**

當您選取 Lightsail 儲存貯體做為發佈的來源時，原始通訊協定原則僅預設為 HTTPS。在儲存貯體為分發原始伺服器時，您便無法變更原始伺服器通訊協定政策。



7. 為分發選擇快取行為 (亦稱為快取預設)。如需詳細資訊，請參閱[快取行為和快取預設](#)。

**Note**

當您選取 Lightsail 值區做為發行版本的來源時，無法使用快取預設集選項。我們會自動套用最適合存放在儲存貯體中靜態內容的分發設定。

8. (選用) 選擇 Show all settings (顯示全部設定)，以檢視分發的其他快取行為設定。

**Note**

當您選取 Lightsail 值區做為發行版本的來源時，無法使用快取行為設定。我們會自動套用最適合存放在儲存貯體中靜態內容的分發設定。

9. (選用) 為分發選擇預設行為。如需詳細資訊，請參閱[預設行為](#)。

**Note**

當您選取 Lightsail 值區做為發佈的原點時，無法使用預設行為選項。我們會自動套用最適合存放在儲存貯體中靜態內容的分發設定。

10. (選用) 選擇 Add path (新增路徑)，以將目錄和檔案覆寫新增至分發的快取行為中。如需詳細資訊，請參閱[目錄和檔案覆寫](#)。

**Note**

當您選取 Lightsail 值區做為發行版本的原點時，無法使用目錄和檔案覆寫選項。我們會自動套用最適合存放在儲存貯體中靜態內容的分發設定。

11. (選用) 選擇顯示在您要為分發編輯的進階設定旁的鉛筆圖示。如需詳細資訊，請參閱[進階快取設定](#)。

**Note**

當您選取 Lightsail 儲存貯體作為發行版本的來源時，無法在 [建立發佈] 頁面上使用進階快取設定。我們會自動套用最適合存放在儲存貯體中靜態內容的分發設定。不過，您可以在分發建立之後修改分發管理頁面中的進階快取設定。

12. 選擇您的分發計劃。如需詳細資訊，請參閱[分發計劃](#)。
13. 輸入分發名稱。

資源名稱：

- 每個 Lightsail 帳戶 AWS 區域 中的每個項目都必須是唯一的。
- 必須包含 2 至 255 個字元。
- 開頭和結尾必須是英數字元或數字。
- 可以包含英數字元、數字、句點、破折號和底線。

14. 檢閱分發成本。
15. 選擇 Create Distribution (建立分佈)。

系統會在數分鐘後建立分發。

## 後續步驟

建議您在分發啟動並執行之後，完成下列後續步驟。

1. 如果您發行版的來源是 WordPress 執行個體，您必須在執行個體中編輯 WordPress 設定檔，讓您的 WordPress 網站與您的發行版一起使用。如需詳細資訊，請參閱[設定您的 WordPress 執行個體以搭配您的發佈](#)使用。
2. (選擇性) 建立 Lightsail DNS 區域，以便在主控台中管理網域的 DNS。這可讓您輕鬆將網域對應至 Lightsail 資源。如需詳細資訊，請參閱[建立 DNS 區域以管理域的 DNS 記錄](#)。或者，您亦可繼續在目前的位置託管網域的 DNS。
3. 為您的網域建立 Lightsail SSL/TLS 憑證，以便在您的發佈中使用該憑證。Lightsail 發行版本需要使用 HTTPS，因此您必須要求您的網域的 SSL/TLS 憑證，才能在您的散佈中使用該憑證。如需詳細資訊，請參閱[為分發建立 SSL/TLS 憑證](#)。
4. 啟用分發的自訂網域，以便將網域與分發搭配使用。若要啟用自訂網域，您必須指定為網域建立的 Lightsail SSL/TLS 憑證。此操作會將網域新增至分發，並啟用 HTTPS。如需詳細資訊，請參閱[啟用分發的自訂域](#)。
5. 將別名記錄新增至網域的 DNS，以開始將網域流量路由至分發。新增別名記錄之後，造訪您網域的使用者會透過分發路由。如需詳細資訊，請參閱[將域指向分發](#)。
6. 測試分發是否正在快取內容。如需詳細資訊，請參閱[測試您的分發](#)。

## 刪除 Lightsail 發行版

如果您不再使用 Amazon Lightsail 分發，您可以隨時刪除它。

### 刪除分發

完成下列程序以刪除分發。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁，選擇 Networking (聯網) 索引標籤。
3. 選擇要刪除之分發的名稱。
4. 選擇分發管理頁面上的 Delete (刪除) 索引標籤。
5. 選擇 Delete distribution (刪除分發) 以刪除分發。
6. 選擇 Yes, Delete (是，刪除) 以確認刪除。

## 設定您的發 Lightsail 版本的快取

快取行為可讓您設定 Amazon Lightsail 分發從來源快取或未快取的內容。例如，您可以指定快取原始伺服器中的個別目錄、檔案或檔案類型。您也可以指定轉送給原始伺服器的 HTML 方法和標頭。在本

指南中，我們會為您介紹如何變更分發的快取行為。如需有關分發的詳細資訊，請參閱[內容交付網路分發](#)。

## 內容

- [快取預設](#)
- [最適合 WordPress 緩存預設](#)
- [預設行為](#)
- [目錄和檔案覆寫](#)
- [進階快取設定](#)
- [變更分發的快取行為](#)

## 快取預設

快取預設會針對您在原始伺服器上託管的內容類型，自動設定分發的設定。例如，選擇 Best for static content (靜態內容最佳選擇) 預設，會使用最適合靜態網站的設定來自動設定您的分發。如果您的網站託管在 WordPress 執行個體上，請選擇「最適合 WordPress 預設」，讓您的發佈自動設定為與您的 WordPress 網站搭配使用。

您可以針對分發選擇下列其中一個快取預設：

- Best for static content (靜態內容最佳選擇) - 此預設會設定您的分發為快取所有內容。如果您在原始伺服器上託管靜態內容 (例如靜態 HTML 頁面)，或託管不會針對造訪您網站的每位使用者變更的內容，則此預設非常適合。當您選擇此預設時，系統會快取分發中的所有內容。
- Best for dynamic content (動態內容的最佳選擇) - 此預設會將您的分發設定為不快取，除了您在 Create a distribution (建立分發) 頁面的 Directory and file overrides (目錄和檔案覆寫) 區段中指定為 Cache (快取) 的內容以外。如需詳細資訊，請參閱本指南中的[目錄和檔案覆寫](#)。如果您在原始伺服器上託管動態內容，或託管可能會針對造訪您網站或 Web 應用程式的每位使用者變更的內容，則此預設非常適合。
- 最適合 WordPress-此預設集可將您的發行版配置為緩存除了實例wp-includes/和wp-content/目錄中的文件以外的 WordPress 任何內容。如果您的來源是使用 Bitnami WordPress 認證和自動藍圖 (不包括多網站藍圖) 的執行個體，則此預設集是理想的選擇。如需有關此預設集的詳細資訊，請參閱[最適合 WordPress 快取預設集](#)。

**Note**

無法選取 Custom settings (自訂設定) 預設。如果您選擇某個預設，然後手動修改分發設定，則系統會自動為您選取該預設。

快取預設集只能在 Lightsail 主控台中指定。您無法使用 Lightsail API 和開發套件來指定它。AWS CLI

## 最適合 WordPress 緩存預設

當您選取使用「由 Bitnami WordPress 認證」和「自動化」藍圖做為發佈來源的執行個體時，Lightsail 會詢問您是否要將最佳 WordPress 快取預設集套用至您的發佈。如果您應用當前，則會自動配置您的分發以最適合您的 WordPress 網站。您不需要套用其他分發設定。最適合 WordPress 預設緩存除了網站 `wp-includes/` 和 `wp-content/` 目錄中的文件之外沒有任何內 WordPress 容。它也會將分發設定為每天清除其快取 (快取壽命為 1 天)，允許所有 HTTP 方法、僅轉送 Host 標頭，不轉送 Cookie 並轉送所有查詢字串。

**Important**

您必須在執行個體中編輯 WordPress 設定檔，才能讓您的 WordPress 網站與您的發行版一起運作。如需詳細資訊，請參閱 [設定您的 WordPress 執行個體以搭配您的發佈](#) 使用。

## 預設行為

預設行為會指定分發處理內容快取的方式。系統會根據您選取的 [快取預設](#) 自動為您指定分發的預設行為。如果您選取不同的預設行為，則快取預設會自動變更為 Custom settings (自訂設定)。

您可以為分發選擇以下其中一個預設行為：

- 快取所有內容 - 這種行為會將分發設定為快取整個網站並將其作為靜態內容。如果您的原始伺服器託管的內容不會因檢視器而變更，或者您的網站不使用 Cookie、標頭或查詢字串來個人化內容，則此選項非常適合。
- 不快取 - 這種行為會將您的分發設定為只快取您指定的原始伺服器檔案和資料夾路徑。如果您的網站或 Web 應用程式使用 Cookie、標頭和查詢字串為個別使用者個人化內容，則此選項非常適合。如果您選取此選項，您必須指定要快取的 [目錄和檔案路徑覆寫](#)。

## 目錄和檔案覆寫

目錄和檔案覆寫可用來覆寫您選取的預設行為，或在該行為中新增例外狀況。例如，如果您選擇快取所有內容，請使用覆寫來指定分發不該快取的目錄、檔案或檔案類型。或者，如果您選擇不快取，請使用覆寫來指定分發應該快取的目錄、檔案或檔案類型。

在該頁面的 Directory and file overrides (目錄和檔案覆寫) 區段中，您可以指定目錄或檔案的路徑，以進行快取或不快取。使用星號符號指定萬用字元目錄 (path/to/assets/\*) 和檔案類型 (\*.html、\*.jpg、\*.js)。目錄和檔案路徑區分大小寫。

以下是有關如何指定目錄和檔案覆寫的範例：

- 指定下列項目，快取在 Lightsail 實體上執行之 Apache 網頁伺服器之文件根目錄中的所有檔案。

```
var/www/html/
```

- 指定下列項目，以僅快取 Apache Web 伺服器文件根目錄中的索引頁面。

```
var/www/html/index.html
```

- 指定下列項目，以僅快取 Apache Web 伺服器文件根目錄中的 .html 檔案。

```
var/www/html/*.html
```

- 指定下列項目，以僅快取 Apache Web 伺服器文件根目錄映像子目錄中的 .jpg、.png 和 .gif 檔案。

```
var/www/html/images/*.jpg
```

```
var/www/html/images/*.png
```

```
var/www/html/images/*.gif
```

指定下列項目，以僅快取 Apache Web 伺服器文件根目錄映像子目錄中的所有檔案。

```
var/www/html/images/
```

## 進階快取設定

進階設定可用來指定分發中的內容快取壽命、允許的 HTTP 方法、HTTP 標頭轉送、Cookie 轉送和查詢字串轉送。您指定的進階設定僅適用於分發所快取的目錄和檔案，包括您指定為 Cache (快取) 的目錄和檔案覆寫。

您可以進行下列進階設定：

### Cache lifespan (TTL) (快取壽命 (TTL))

在分發轉送另一個請求到原始伺服器，以判斷您的內容是否已更新之前，請控制您的內容在分發快取中停留的時間量。預設值為一天。縮短持續時間後，您可以更好地提供動態內容。增加持續時間會讓您的使用者取得更好的效能，因為檔案更有可能是直接從節點提供。增加持續時間也能減少原始伺服器的負載，因為分發提取內容的頻率減少。

#### Note

您指定的快取壽命值僅在原始伺服器不新增 HTTP 標頭至您的內容時才適用，例如不新增 `Cache-Control max-age`、`Cache-Control s-maxage` 或 `Expires`。

### Allowed HTTP methods (允許的 HTTP 方法)

控制分發處理及轉送至原始伺服器的 HTTP 方法。HTTP 方法表示想要在原始伺服器上執行的動作。例如，GET 方法會從您的原始伺服器擷取資料，而 PUT 方法會請求將封閉的實體存放在您的原始伺服器上。

您可以為分發選擇下列其中一個 HTTP 方法選項：

- Allow GET, HEAD, OPTIONS, PUT, PATCH, POST, and DELETE methods (允許 GET、HEAD、OPTIONS、PUT、PATCH、POST 和 DELETE 方法)
- Allow the GET, HEAD, and OPTIONS methods (允許 GET、HEAD 和 OPTIONS 方法)
- Allow the GET and HEAD methods (允許 GET 和 HEAD 方法)

您的分發一律會快取針對 GET 與 HEAD 請求的回應。如果您選擇允許這些請求，您的分發也會快取針對 OPTIONS 請求的回應。您的分發不會快取針對任何其他 HTTP 方法的回應。

### ⚠ Important

如果您將分發設定為允許支援的所有 HTTP 方法，則您必須將原始伺服器執行個體設定為處理所有方法。例如，如果因為想要使用 POST，而將您的分發設定為允許這些方法，則您必須將原始伺服器設定為以適當方式處理 DELETE 請求，讓檢視器無法刪除您不希望其刪除的資源。如需詳細資訊，請搜尋您的網站或 Web 應用程式的文件。

## HTTP header forwarding (HTTP 標頭轉送)

控制分發是否根據指定標頭的值來快取內容，如果是的話，是根據哪些標頭的值。HTTP 標頭攜帶有關用戶端瀏覽器、請求的頁面、原始伺服器等的資訊。例如，Accept-Language 標頭會傳送用戶端的語言 (例如針對英文是 en-US)，以便原始伺服器能以用戶端語言的內容 (如果可用) 來回應。

您可以為分發選擇下列其中一個 HTTP 標頭選項：

- Forward no headers (不轉送標頭)
- Forward only the headers I specify (只轉送我指定的標頭)

如果您選取 Forward no headers (不轉送標頭)，您的分發不會根據標頭值快取內容。無論您選取的選項為何，您的分發皆會轉送特定標頭至原始伺服器，並根據您轉送的標頭來採取特定動作。

## Cookie forwarding (Cookie 轉送)

控制您的分發是否將 Cookie 轉送到原始伺服器，若要轉送，是哪些 Cookie 要轉送。Cookie 包含傳送至原始伺服器的一小段資料，例如有關訪客在您原始伺服器網頁上的動作的資訊，以及訪客提供的任何資訊，例如他們的姓名和興趣。

您可以為您的分發選擇下列其中一個 Cookie 轉送選項：

- Don't forward cookies (請勿轉送 Cookie)
- Forward all cookies (轉送所有 Cookie)
- Forward cookies I specify (轉送我指定的 Cookie)

如果您選擇 Forward all cookies (轉送所有 Cookie)，無論您的應用程式使用多少 Cookie，您的分發都會轉送所有 Cookie。如果您選擇 Forward cookies I specify (轉送我指定的 Cookie)，然後在顯示的文字方塊中輸入您要分發轉送之 Cookie 的名稱。當您指定 Cookie 名稱時，可以指定以下萬用字元符號：

- \* 符合 Cookie 名稱中的 0 個或多個字元
- ? 完全符合 Cookie 名稱中的一個字元

例如，假設檢視器針對某個物件的請求包含名為 `userid_member-number` 的 Cookie。其中每個使用者都有 `member-number` (`userid_123`、`userid_124`、`userid_125` 等) 的唯一值。您希望分發為每個成員快取單獨版本的內容。您可以透過將所有 Cookie 轉送到原始伺服器以達成此目標，但檢視器請求包含一些您不希望分發快取的 Cookie。您可以指定以下值作為 Cookie 名稱，這會導致分發將所有以 `userid_` 開頭的 Cookie 轉送至您的原始伺服器：`userid_*`

### Query string forwarding (查詢字串轉送)

控制您的分發是否將查詢字串轉送至原始伺服器，若要轉送，是哪些查詢字串要轉送。查詢字串是指派值給指定參數的 URL 的一部分。例如，`https://example.com/over/there?name=ferret` URL 包含 `name=ferret` 查詢字串。當伺服器收到該等頁面的請求時，它可能會執行一個程式，並將不變的 `name=ferret` 查詢字串傳遞至該程式。問號用作分隔符號，而非查詢字串的一部分。

您可以選擇讓分發不轉送查詢字串，或只轉送您指定的查詢字串。如果您的原始伺服器傳回相同版本的內容，而不考慮查詢字串參數的值，請選擇不轉送查詢字串。這會讓分發更有可能提供來自快取的請求，從而提高效率並降低原始伺服器的負載。如果您的原始伺服器根據一或多個查詢字串參數傳回不同版本的內容，請選擇只轉送您指定的查詢字串。

## 變更分發的快取行為

請完成下列程序來變更分發的預設快取行為。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁，選擇 Networking (聯網) 索引標籤。
3. 選擇您要變更預設快取行為之分發的名稱。
4. 選擇分發管理頁面上的 Cache (快取) 索引標籤。
5. 在該頁面的 Configure caching (設定快取) 區段中，選擇分發的快取預設。如需詳細資訊，請參閱 [快取預設](#)。
6. 選擇 Change default cache behavior (變更預設快取行為)，以變更分發的預設行為。然後，為分發選擇預設行為。如需詳細資訊，請參閱 [預設行為](#)。
7. 選擇 Add path (新增路徑)，以將目錄和檔案覆寫新增至分發的快取行為中。如需詳細資訊，請參閱 [目錄和檔案覆寫](#)。
8. 選擇顯示在您要為分發編輯的進階設定旁的鉛筆圖示。如需詳細資訊，請參閱 [進階快取設定](#)。

當您將變更儲存至分發組態時，您的分發會開始將變更傳播到所有節點。分發會根據之前的組態繼續從該位置提供內容，直到在節點中更新組態為止。在節點中更新組態後，分發便會立即根據新組態從該位置提供內容。

您的變更不會立即傳播到每個節點。傳輸完成時，發佈的狀態會從變更為「已啟InProgress用」。儘管您的分發傳播變更，但我們仍無法根據先前的組態或新組態來判斷指定節點是否提供內容。

## 主題

- [重設您的發 Lightsail 版本的快取](#)

## 重設您的發 Lightsail 版本的快取

快取壽命 (存留時間) 設定可控制內容在 Amazon Lightsail 分發快取中停留的時間長度。若您需要在快取壽命間隔之前清除快取，您也可以手動重設分發上的快取。清除快取後，下次當使用者請求內容時，您的分發會從原始伺服器提取最新版本的內容，並快取該內容。在本指南中，我們會為您介紹如何手動重設分發上的快取。如需有關分發的詳細資訊，請參閱[內容交付網路分發](#)。

### 重設分發的快取

請完成以下程序來重設分發的快取。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁，選擇 Networking (聯網) 索引標籤。
3. 選擇您要重設快取之分發的名稱。
4. 選擇分發管理頁面上的 Cache (快取) 索引標籤。
5. 捲動至頁面的 Reset cache (重設快取) 區段，然後選擇 Reset cache (重設快取)。
6. 出現確認提示時，選擇 Yes, reset (是，重設) 以確認您要重設分散式快取。或者選擇 No, cancel (否，取消) 以不重設分散式快取。

## 變更 Lightsail 發行版的內容來源

在本指南中，我們將向您展示如何在建立 Amazon Lightsail 分發之後變更其來源。原始伺服器是分發內容的最終來源。建立分發時，您可以選擇裝載網站或 Web 應用程式內容的 Lightsail 執行個體、Lightsail 儲存貯體或 Lightsail 負載平衡器 (連接一個或多個執行個體)。如需詳細資訊，請參閱[內容交付網路分發](#)。

在建立分發後，您可以隨時變更原始伺服器。當您變更原始伺服器時，您的分發會立即開始將變更複製至節點。您的分發將繼續轉送請求至特定節點的先前原始伺服器，直到分發更新為該節點的新原始伺服器為止。

變更原始伺服器不需要分發使用新原始伺服器中的內容來重新填入節點快取。只要您的網站或 Web 應用程式中的使用者請求尚未變更，您的分發便會繼續為已存在於節點快取中的內容提供服務，直到內容的快取壽命到期。

## 原始伺服器通訊協定政策

您的分發在從原始伺服器提取內容時所使用的通訊協定政策，即為原始伺服器通訊協定政策。在您選擇分發的原始伺服器後，您應判斷分發在從原始伺服器提取內容時，是否應使用超文字傳輸通訊協定 (HTTP) 或超文字傳輸通訊協定安全 (HTTPS)。如果您的原始伺服器未設定使用 HTTPS，則必須使用 HTTP。

您可以為分發選擇以下其中一個原始伺服器通訊協定政策：

- 僅限 HTTP - 您的分發僅使用 HTTP 來存取原始伺服器。這是預設設定。
- 僅限 HTTPS - 您的分發僅使用 HTTPS 來存取原始伺服器。

編輯原始伺服器通訊協定政策的步驟包含在本指南下列[變更分發的原始伺服器](#)章節中。

## 變更分發原始伺服器

請完成下列程序來變更分發原始伺服器。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁，選擇 Networking (聯網) 索引標籤。
3. 選擇您要變更原始伺服器之分發的名稱。
4. 在分發管理頁面上選擇 Details (詳細資訊) 索引標籤，然後捲動至該頁面的 Choose your origin (選擇原始伺服器) 區段。

該頁面的 Select your origin (選取原始伺服器) 區段會顯示分發目前的原始伺服器。

5. 選擇 Change origin (變更原始伺服器)。
6. 選擇建立原始伺服器資源的 AWS 區域。

分發為全域資源。其可在任何 AWS 區域中參考原始伺服器，並在全域分配內容。

7. 選擇您的原始伺服器。原始伺服器可以是執行個體、儲存貯體或負載平衡器 (具有一個或多個連接至其上的執行個體)。
8. 選擇 Save (儲存), 用新原始伺服器更新您的分發。

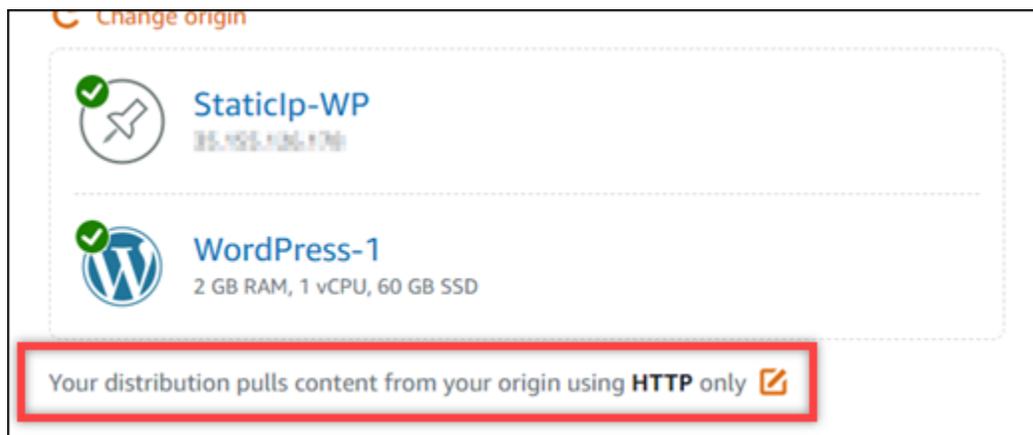
在您選擇分發的原始伺服器後, 您應判斷分發在從原始伺服器提取內容時, 是否應使用超文字傳輸通訊協定 (HTTP) 或超文字傳輸通訊協定安全 (HTTPS)。

9. (選用) 若要變更來源通訊協定政策, 請選擇顯示於分發使用的目前原始伺服器通訊協定政策旁的鉛筆圖示。如需詳細資訊, 請參閱[原始伺服器通訊協定政策](#)。

此選項列於該頁面的 Choose your origin (選擇原始伺服器) 區段中, 位於您為分發選取的原始伺服器資源下方。

#### Note

當您選取 Lightsail 儲存貯體做為發佈的來源時, 原始通訊協定原則僅預設為 HTTPS。在儲存貯體為分發原始伺服器時, 您便無法變更原始伺服器通訊協定政策。



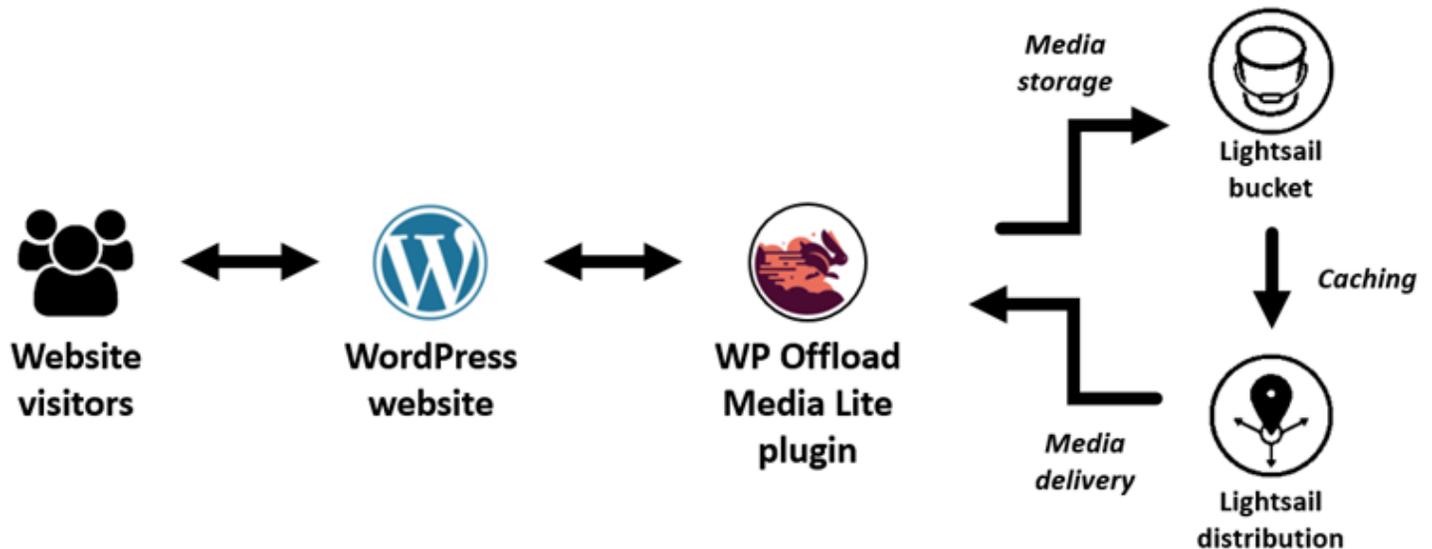
10. 選擇 HTTP only (僅限 HTTP) 或 HTTPS only (僅限 HTTPS), 然後選擇 Save (儲存), 以儲存原始伺服器通訊協定政策。

當您將變更儲存至分發組態時, 您的分發會開始將變更傳播到所有節點。分發會根據之前的組態繼續從該位置提供內容, 直到在節點中更新組態為止。在節點中更新組態後, 分發便會立即根據新組態從該位置提供內容。

您的變更不會立即傳播到每個節點。傳輸完成時, 發佈的狀態會從變更為「已啟InProgress用」。儘管您的分發傳播變更, 但我們仍無法根據先前的組態或新組態來判斷指定節點是否提供內容。

## 使用 Lightsail 儲存貯體和 CDN 分發，有效率地提供媒體檔案

本教學說明將 Amazon Lightsail 儲存貯體設定為 Lightsail 內容交付網路 (CDN) 分發的來源所需的步驟。它還描述了如何將您的 WordPress 網站配置為在儲存桶上傳和存儲媒體（例如圖像和電影文件），以及如何從您的分發中傳遞媒體。如何執行此操作的範例之一是使用 [WP Offload Media Lite 外掛程式](#)。下圖說明了此設定。



將網站媒體儲存在 Lightsail 儲存貯體中，不必儲存和提供這些檔案，就能減輕執行個體的負載。從 Lightsail 發行版本快取和提供媒體，可加快這些檔案傳遞給網站訪客的速度，並改善整體網站效能。如需有關分發的詳細資訊，請參閱 [內容交付網路分發](#)。如需有關儲存貯體的詳細資訊，請參閱 [物件儲存](#)。

### 內容

- [步驟 1：完成先決條件](#)
- [步驟 2：修改儲存貯體許可](#)
- [步驟 3：建立具有儲存貯體作為原始伺服器的分發](#)
- [步驟 4：啟用分發的自訂子網域](#)
- [第 5 步：在您 WordPress 的網站上安裝 WP 卸載媒體精簡版插件](#)
- [步驟 6：測試您的 WordPress 網站與 Lightsail 儲存貯體和發行版本之間的連線](#)

### 步驟 1：完成先決條件

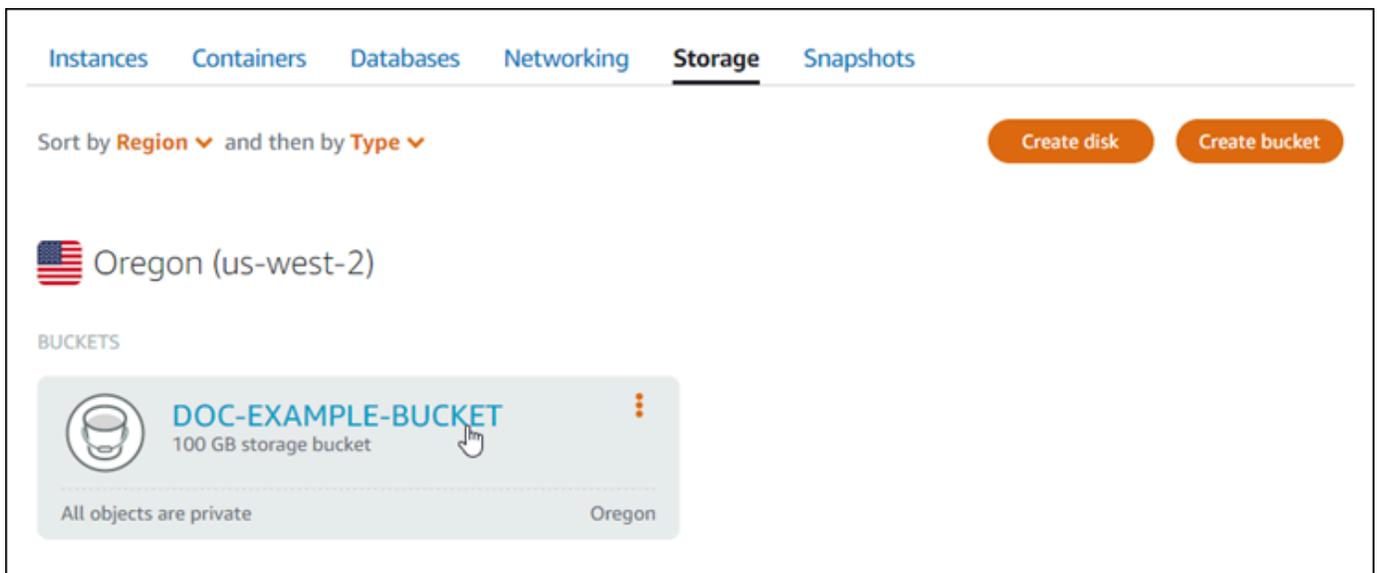
請先完成事前準備 (若尚未完成)：

- 在 Lightsail 中建立並設定 WordPress 執行個體，並取得登入管理儀表板的密碼。如需詳細資訊，請參閱[教學課程：在 Amazon Lightsail 中啟動和設定 WordPress 執行個體](#)。
- 在 Lightsail 物件儲存服務中建立值區。如需詳細資訊，請參閱[在 Lightsail 中建立值區](#)。

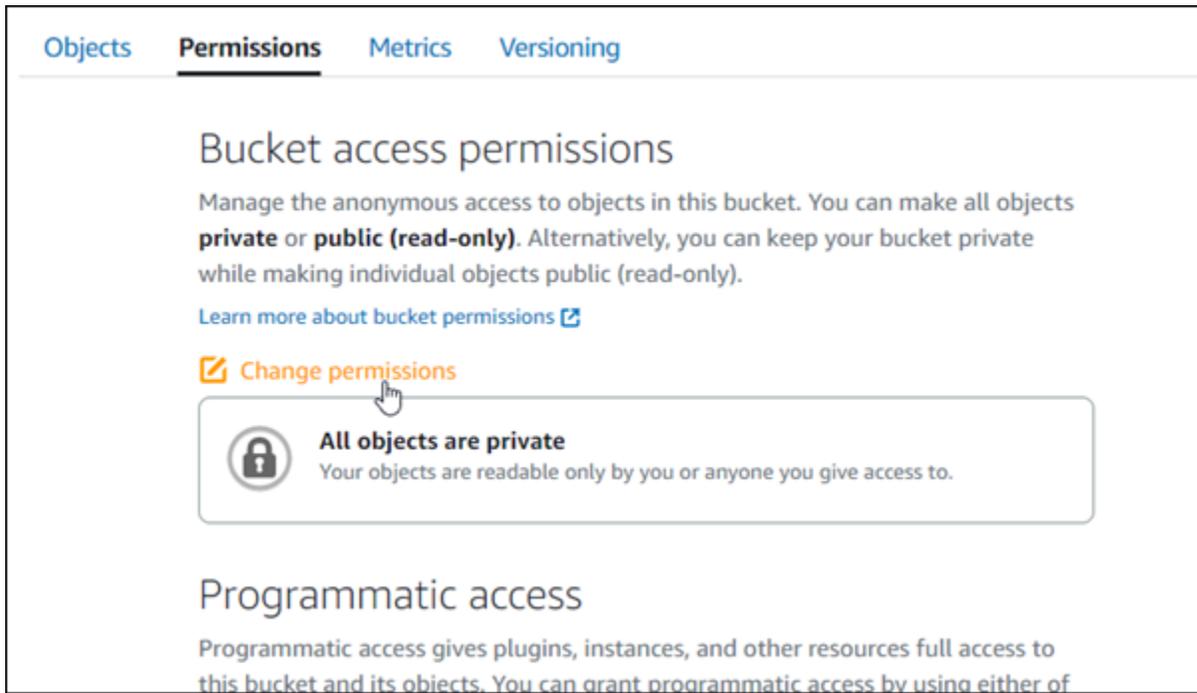
## 步驟 2：修改儲存貯體許可

完成以下程序，讓您的 WordPress 執行個體和 WP 卸載媒體精簡版外掛程式存取您的值區。儲存貯體的許可必須設為 Individual objects can be made public (read only) (可將個別物件設為公有 (唯讀))。您也必須將 WordPress 執行個體附加至儲存貯體。如需有關儲存貯體許可的詳細資訊，請參閱[儲存貯體許可](#)。

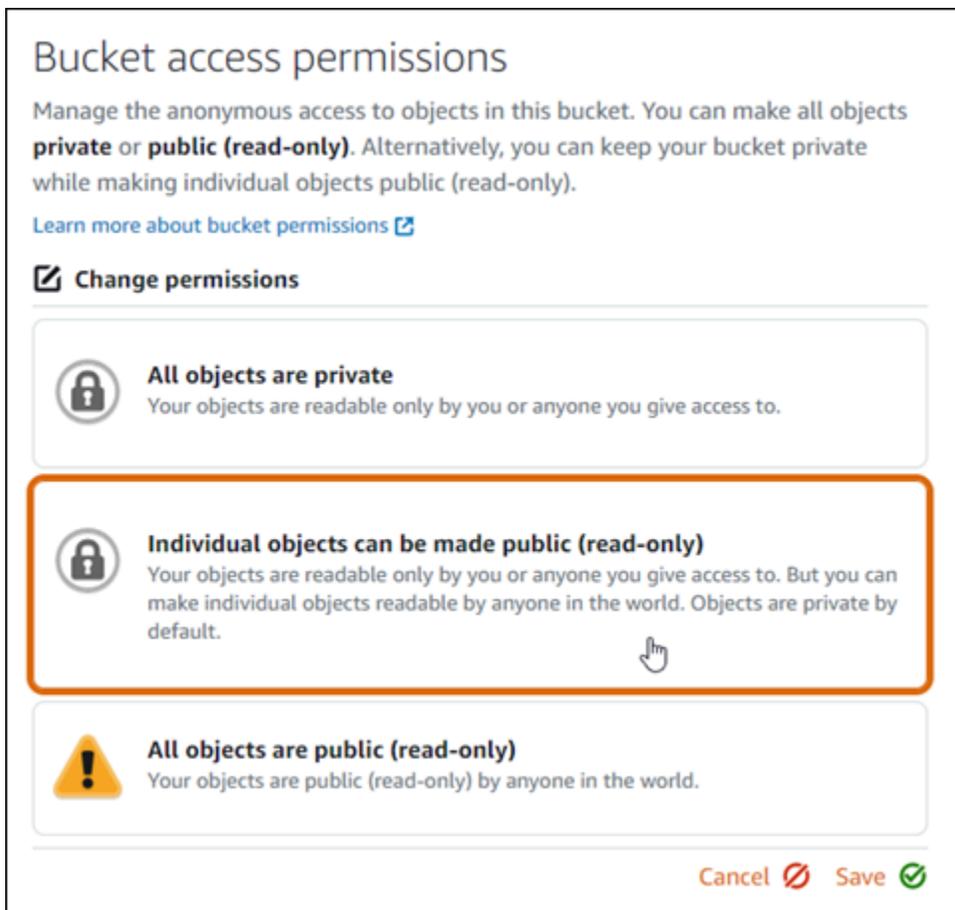
1. 登入主 [Lightsail](#) 台。
2. 在 Lightsail 首頁上，選擇儲存空間索引標籤。
3. 選擇您要在 WordPress 網站上使用的值區名稱。



4. 選擇 Bucket management (儲存貯體管理) 頁面上的 Permissions (許可) 索引標籤。
5. 在頁面的 Bucket access permissions (儲存貯體存取許可) 區段下選擇 Change permissions (變更許可)。

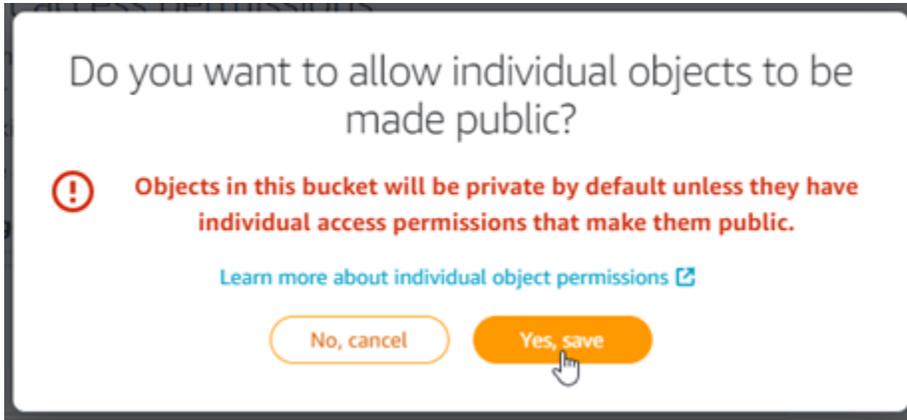


6. 選擇 Individual objects can be made public and read only (可將個別物件設為公有和唯讀)。



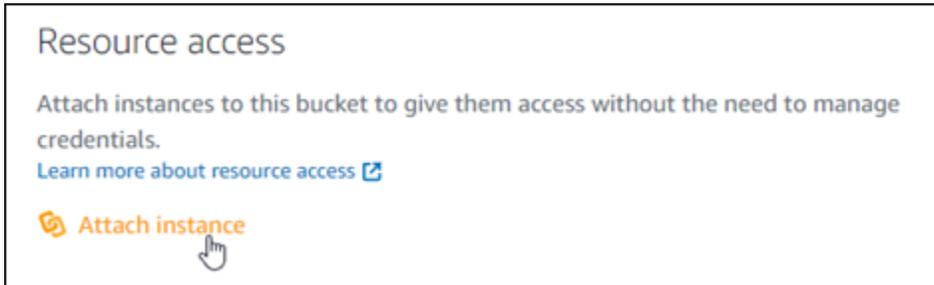
7. 選擇 Save (儲存)。

- 在出現的確認提示中，選擇 Yes, save (是，儲存)。

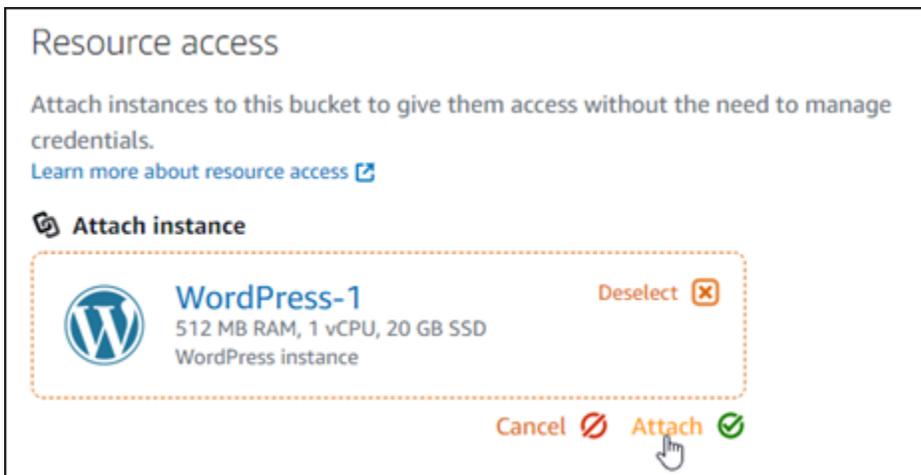


幾分鐘後，儲存貯體將會設定為允許個別物件存取。這樣可確保使用卸載 Media Lite 外掛程式從您的 WordPress 網站上傳到值區的物件對您的客戶而言是可讀的。

- 捲動至頁面的 Resource access (資源存取) 區段，然後選擇 Attach instance (連接執行個體)。



- 在出現的下拉式清單中選擇 WordPress 執行個體的名稱，然後選擇 [連接]。

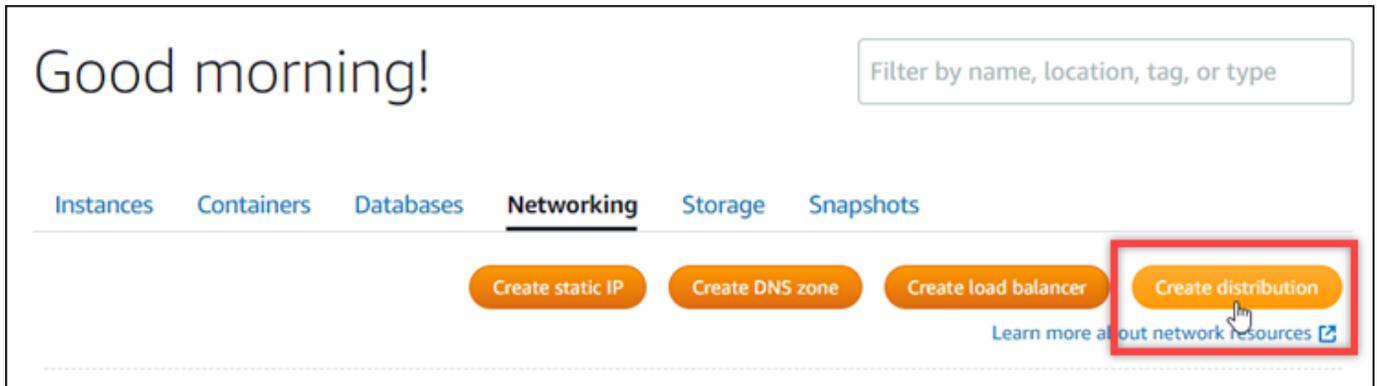


片刻之後，您的 WordPress 執行個體就會連接到儲存貯體。這可讓您的 WordPress 執行個體存取權以管理值區及其物件。

## 步驟 3：建立具有儲存貯體作為原始伺服器的分發

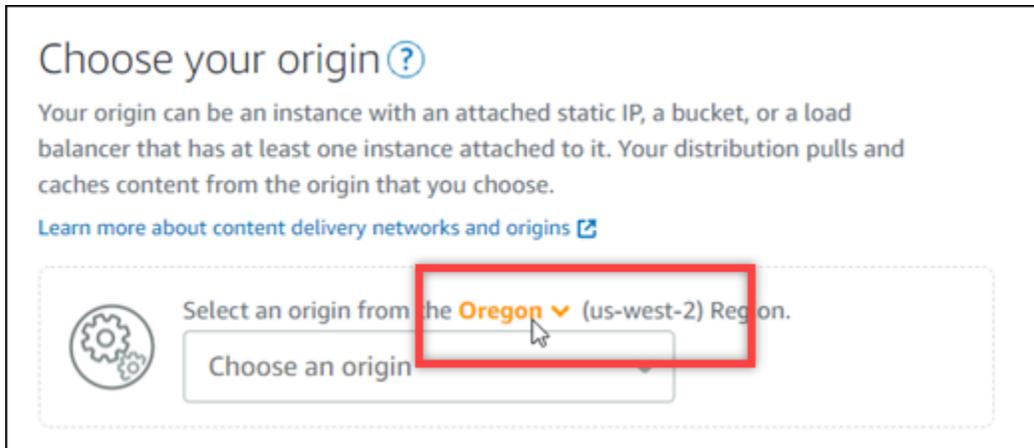
請完成下列程序來建立 Lightsail 發行版本，並選擇您的 Lightsail 值區做為原點。

1. 選擇 Lightsail 主控台頂端導覽功能表上的 [首頁]。
2. 在 Lightsail 首頁，選擇 Networking (聯網) 索引標籤。
3. 選擇 Create Distribution (建立分佈)。

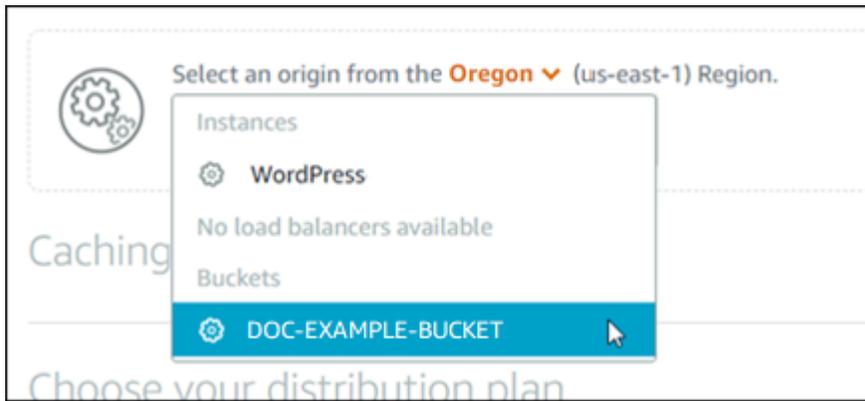


4. 在頁面的選擇原始伺服器區段中，選擇建立儲存貯體所在的 AWS 區域。

分發為全域資源。他們可以引用任何值區中的值區 AWS 區域，並在全球範圍內分發其內容。



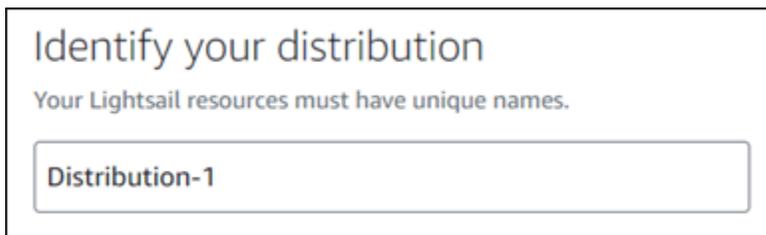
5. 選擇您的儲存貯體作為原始伺服器。



### Note

儲存貯體的許可必須設為 Individual objects can be made public (read only) (可將個別物件設為公有 (唯讀))。只會快取公有的個別物件並藉由分發提供服務。當您選擇儲存貯體作為分發的原始伺服器時，指定原始伺服器通訊協定政策、快取行為、預設行為以及目錄和檔案覆寫的選項將無法使用且無法編輯。原始伺服器通訊協定政策預設為 HTTP only (僅限 HTTP)，並且快取行為預設為 Cache everything (快取所有內容)。建立分發後，您可以變更分發的進階快取設定。

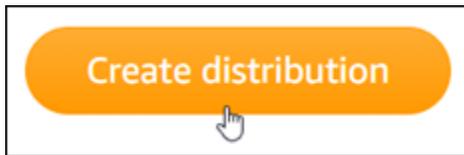
6. 選擇您的分發計劃。
7. 輸入分發名稱。



分發名稱：

- 每個 Lightsail 帳戶 AWS 區域 中的每個項目都必須是唯一的。
- 必須包含 2–255 個字元。
- 開頭和結尾必須是英數字元或數字。
- 可以包含英數字元、數字、句點、破折號和底線。

8. 選擇 Create Distribution (建立分佈)。



系統會在數分鐘後建立分發。當新分發達到 Enabled (已啟用) 狀態時，即已準備好提供並快取儲存貯體中的物件。

## 步驟 4：啟用分發的自訂子網域

建立分發時，會設定類似於 `123abc.cloudfront.net` 的預設網域。設定 WP Offload Media Lite 外掛程式時，可以指定預設網域作為媒體檔案的來源。但我們強烈建議為分發啟用自訂網域。您為分發啟用的自訂網域應該是您在網站上使用的網域的子 WordPress 網域。例如，如果您 `mycustomdomain.com` 與 WordPress 網站搭配使用，則可以選擇將自訂網域 `media.mycustomdomain.com` 與您的分發搭配使用。在您的網站和分佈之間使用相同的域和子域名組合有助於提高 WordPress 網站的搜索引擎優化分數。

請完成下列步驟，為您的分發設定自訂網域：

1. 為您的網域建立 Lightsail SSL/TLS 憑證，以便在您的發佈中使用該憑證。Lightsail 發行版本需要使用 HTTPS，因此您必須要求您的網域的 SSL/TLS 憑證，才能在您的散佈中使用該憑證。如需詳細資訊，請參閱 [為分發建立 SSL/TLS 憑證](#)。
2. 啟用分發的自訂網域，以便將網域與分發搭配使用。若要啟用自訂網域，您必須指定為網域建立的 Lightsail SSL/TLS 憑證。此操作會將網域新增至分發，並啟用 HTTPS。如需詳細資訊，請參閱 [啟用分發的自訂域](#)。
3. 將別名記錄新增至網域 DNS。新增別名記錄之後，造訪您網域的使用者會透過分發路由。如需詳細資訊，請參閱 [將域指向分發](#)。

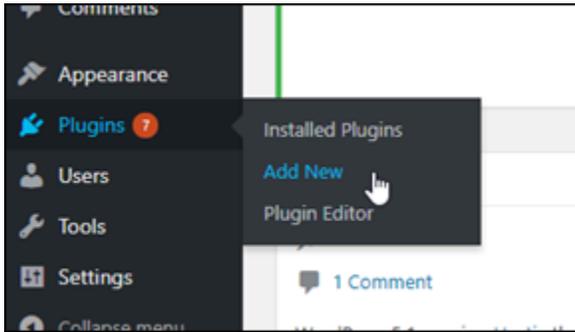
## 第 5 步：在您 WordPress 的網站上安裝 WP 卸載媒體精簡版插件

完成以下步驟，在您的 WordPress 網站上安裝 WP 卸載媒體精簡版外掛程式。此插件會自動複製圖像，視頻，文檔以及通過 WordPress 「媒體上傳器」添加到 Lightsail 存儲桶的任何其他媒體。您也可以將其設定為透過 Lightsail 發行版本提供儲存貯體中的媒體。有關更多信息，請參閱 [WP 卸載媒體精簡版](#) 在 WordPress 網站上。

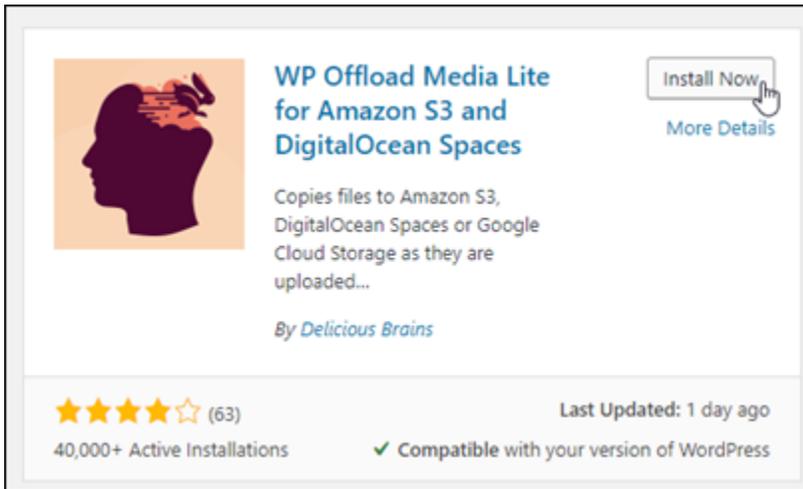
1. 以系統管理員身分登入您 WordPress 網站的儀表板。

如需詳細資訊，請參閱在 [Amazon Lightsail](#) 中取得 Bitnami 執行個體的應用程式使用者名稱和密碼。

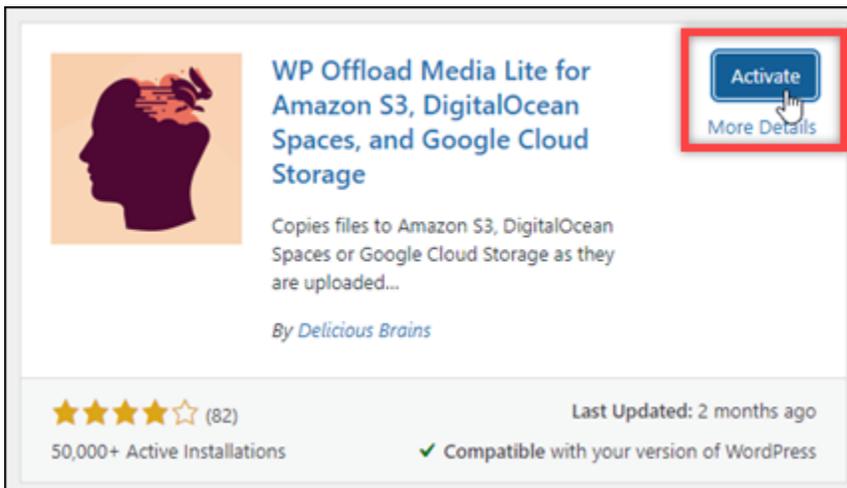
- 將滑鼠游標暫停在左側導覽選單中的 Plugins (外掛程式) 上，然後選擇 Add New (新增)。



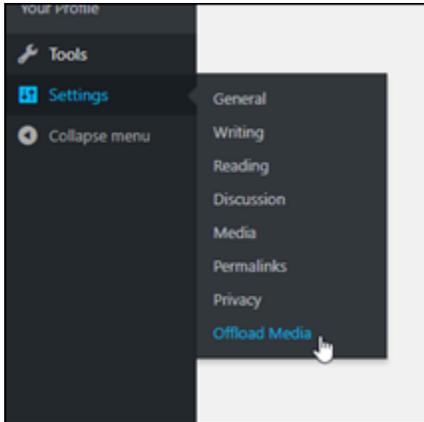
- 搜尋 WP Offload Media Lite。
- 在搜尋結果中，選擇 WP Offload Media Lite 外掛程式旁的 Install Now (立即安裝)。



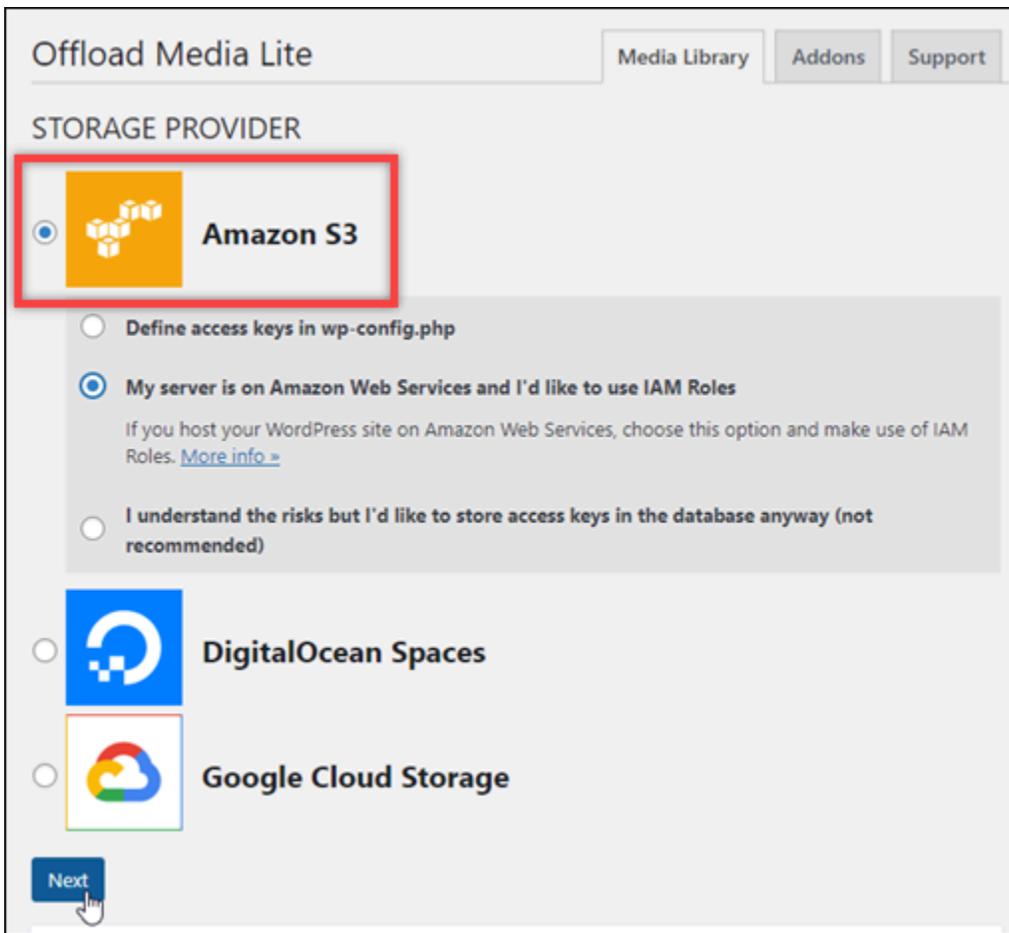
- 在外掛程式完成安裝後，選擇 Activate (啟用)。



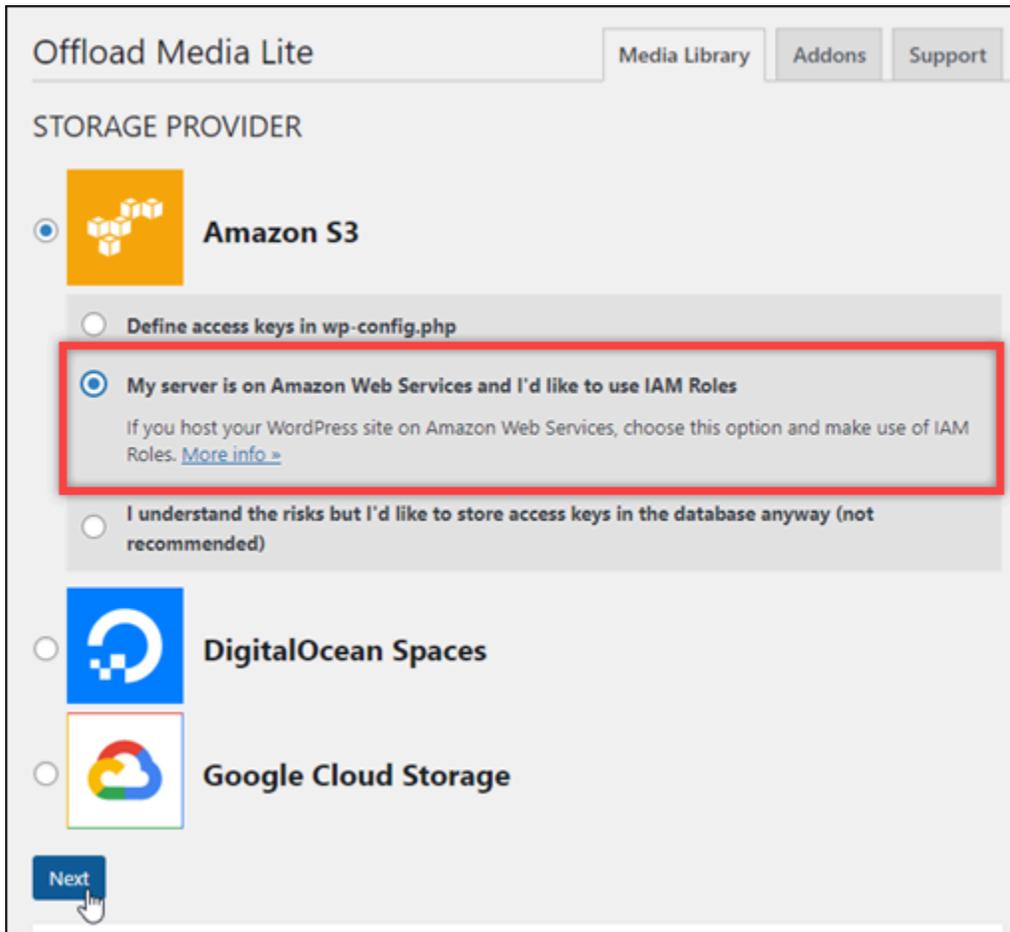
- 在左側導覽功能表中，選擇 Settings (設定)，然後選擇 Offload Media (卸載媒體)。



- 在 Offload Media Lite 頁面中，選擇 Amazon S3 作為儲存供應商。



- 選擇 My server is on Amazon Web Services and I'd like to use IAM Roles (我的伺服器在 Amazon Web Services 上，我想使用 IAM 角色)。



Offload Media Lite Media Library Addons Support

STORAGE PROVIDER

 **Amazon S3**

Define access keys in wp-config.php

**My server is on Amazon Web Services and I'd like to use IAM Roles**  
If you host your WordPress site on Amazon Web Services, choose this option and make use of IAM Roles. [More info >](#)

I understand the risks but I'd like to store access keys in the database anyway (not recommended)

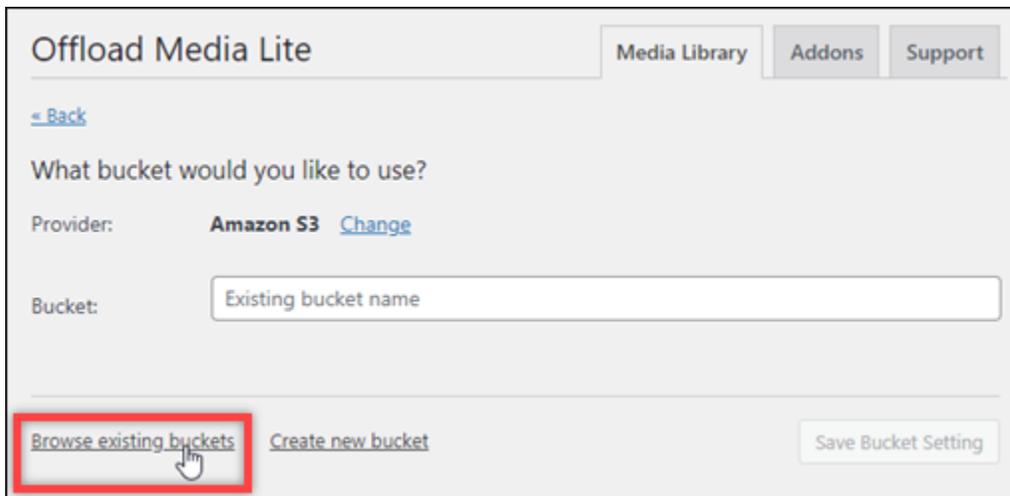
 **DigitalOcean Spaces**

 **Google Cloud Storage**

[Next](#)

9. 選擇 Next (下一步)。

10. 在出現的 What bucket would you like to use (您要使用的儲存貯體) 頁面中，選擇 Browse existing buckets (瀏覽現有儲存貯體)。



Offload Media Lite Media Library Addons Support

[← Back](#)

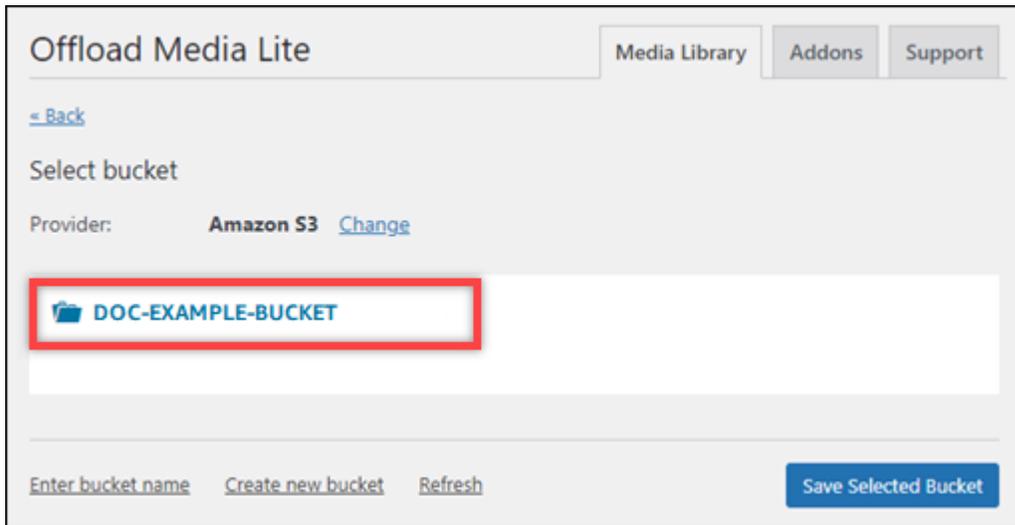
What bucket would you like to use?

Provider: **Amazon S3** [Change](#)

Bucket:

[Browse existing buckets](#) [Create new bucket](#) [Save Bucket Setting](#)

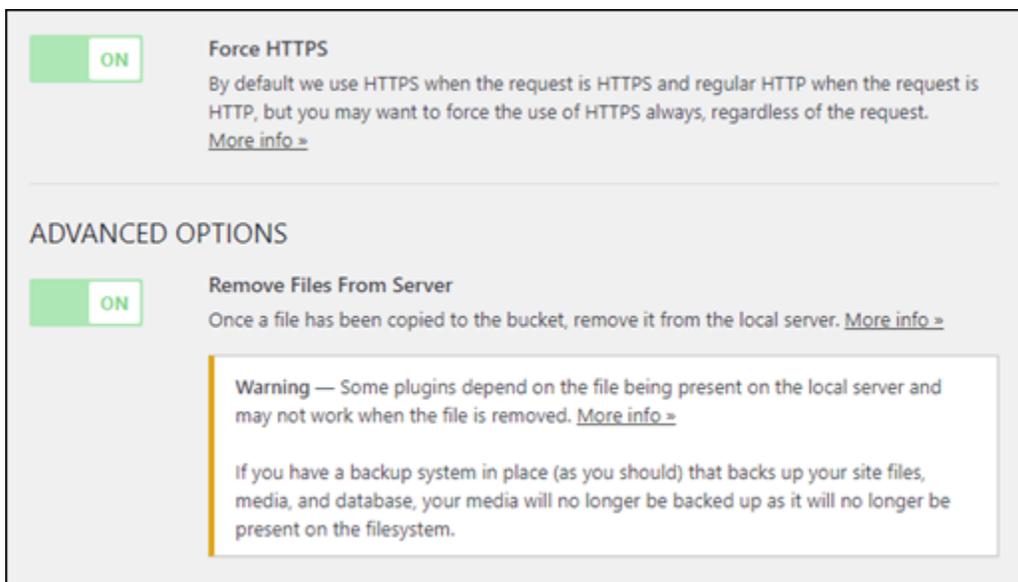
11. 選擇您建立要搭配執行個體使用的值區名 WordPress 稱。



12. 在出現的 Offload Media Lite Settings (Offload Media Lite 設定) 頁面中，開啟 Force HTTPS (強制執行 HTTPS) 和 Remove Files From Server (從伺服器移除檔案)。

- 必須開啟 [強制 HTTPS] 設定，因為 Lightsail 值區預設會使用 HTTPS 來提供媒體檔案。如果您未開啟此功能，從您的 WordPress 網站上傳至 Lightsail 儲存貯體的媒體檔案將無法正確提供給您的網站訪客。

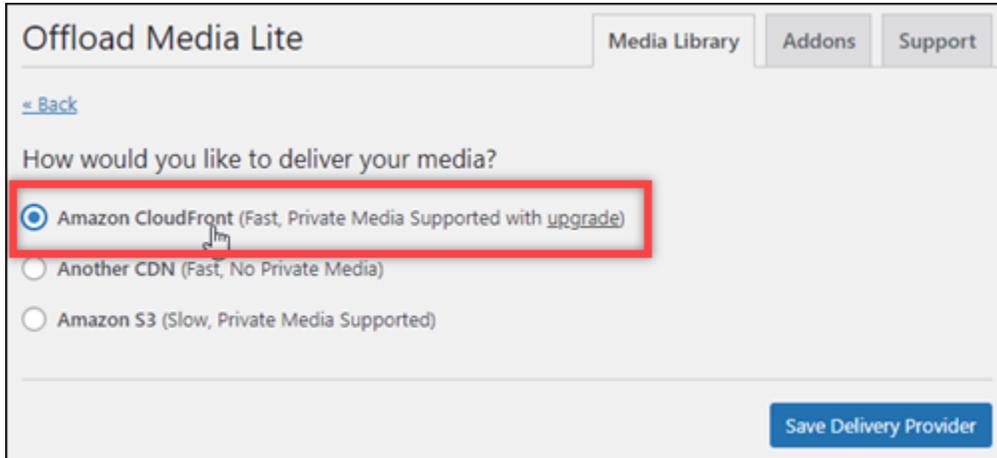
「從伺服器移除檔案」設定可確保上傳至 Lightsail 儲存貯體的媒體也不會儲存在執行個體的磁碟上。如果未開啟此功能，上傳至 Lightsail 儲存貯體的媒體檔案也會儲存在 WordPress 執行個體的本機儲存空間中。



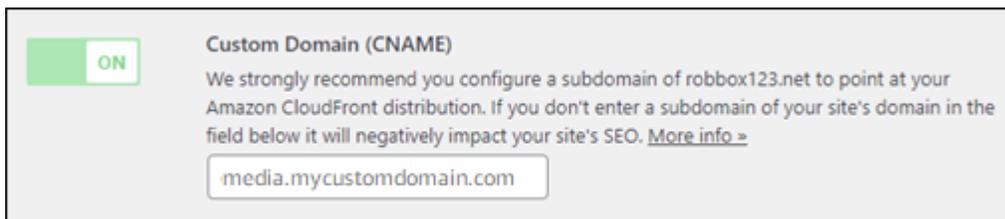
13. 在頁面的 Delivery (交付) 區段下，選擇 Amazon S3 標籤旁的 Change (變更)。



14. 在您希望如何傳送媒體？出現的頁面，選擇 Amazon CloudFront。



15. 選擇 Save Delivery Provider (儲存交付提供者)。
16. 在出現的 Offload Media Lite Settings (Offload Media Lite 設定) 頁面中，開啟 Custom Domain (CNAME) (自訂網域 (CNAME))。然後，在文字方塊中輸入 Lightsail 發行版的網域。這可能是分發的預設網域 (例如 123abc.cloudfront.net)，如果您啟用分發的自訂網域，也可能是自訂網域 (例如 media.mycustomdomain.com)。



17. 選擇 Save Changes (儲存變更)。

#### **Note**

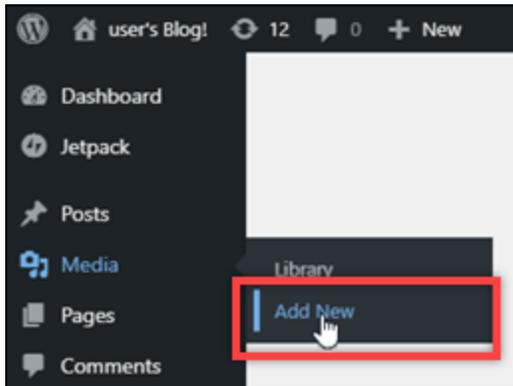
若要稍後返回 Offload Media Lite Settings (Offload Media Lite 設定) 頁面，請滑鼠游標暫停在左側導覽選單中的 Settings (設定) 上，然後選擇 Offload Media。

您的 WordPress 網站現在已設定為使用媒體精簡版外掛程式。下次您透過上傳媒體檔案時 WordPress，該檔案會自動上傳至您的 Lightsail 儲存貯體，並由散佈提供。若要測試組態，請繼續前往本教學課程下一節。

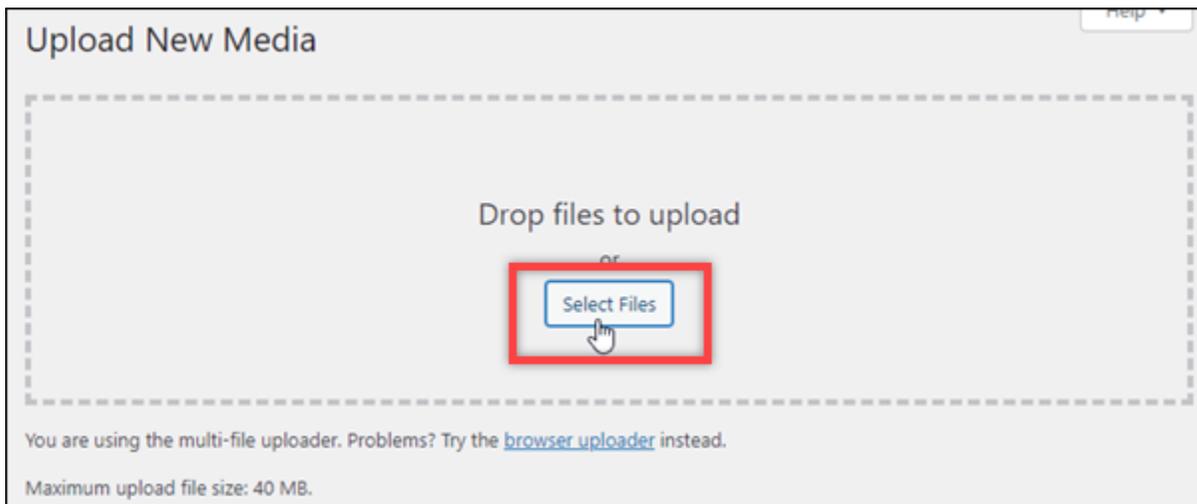
## 步驟 6：測試您的 WordPress 網站與 Lightsail 儲存貯體和發行版本之間的連線

請完成下列程序，將媒體檔案上傳至您的 WordPress 執行個體，並確認該檔案已上傳至 Lightsail 儲存貯體，並從您的發行版本提供。

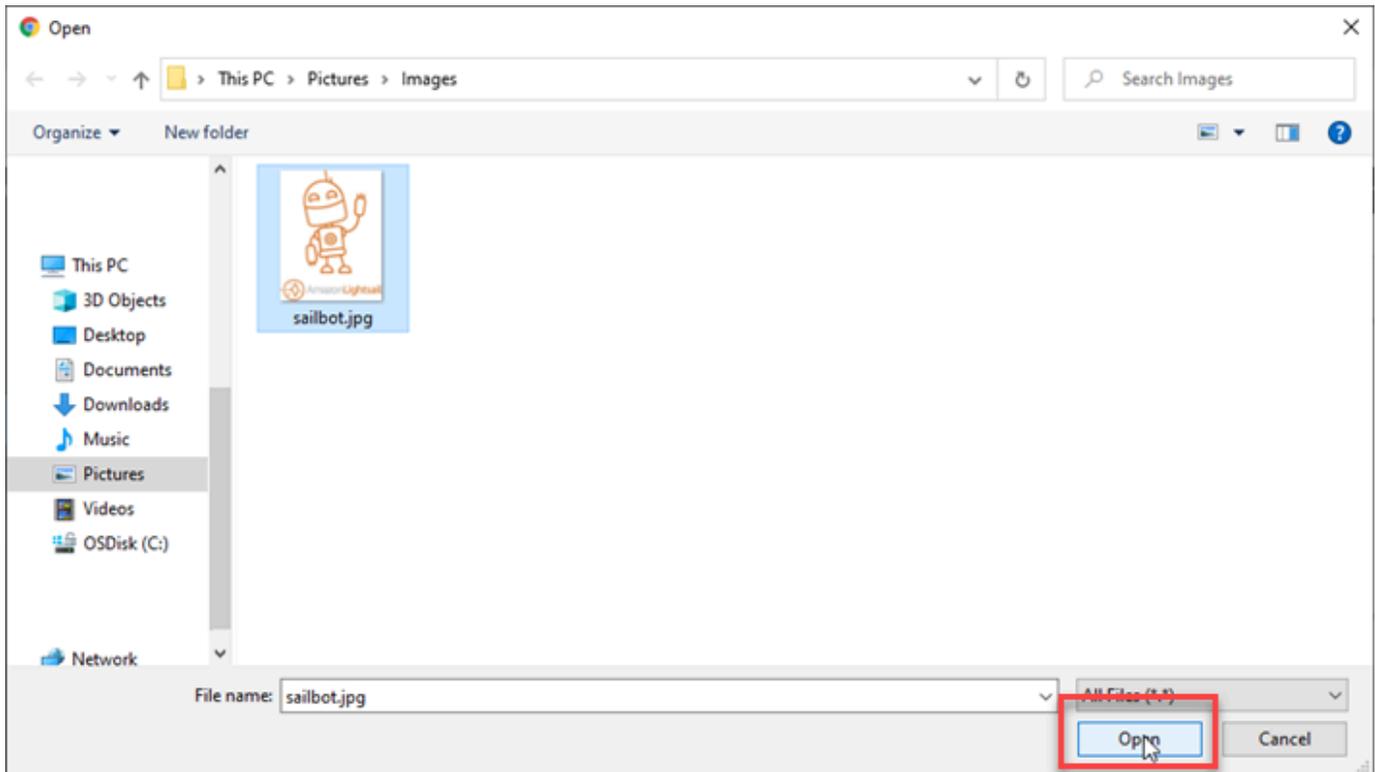
1. 暫停 WordPress 儀表板左側導覽功能表中的「媒體」，然後選擇「新增」。



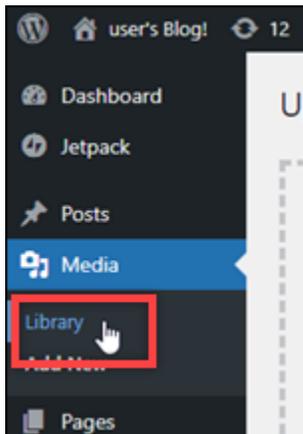
2. 在出現的 Upload New Media (上傳新媒體) 頁面上，選擇 Select Files (選取檔案)。



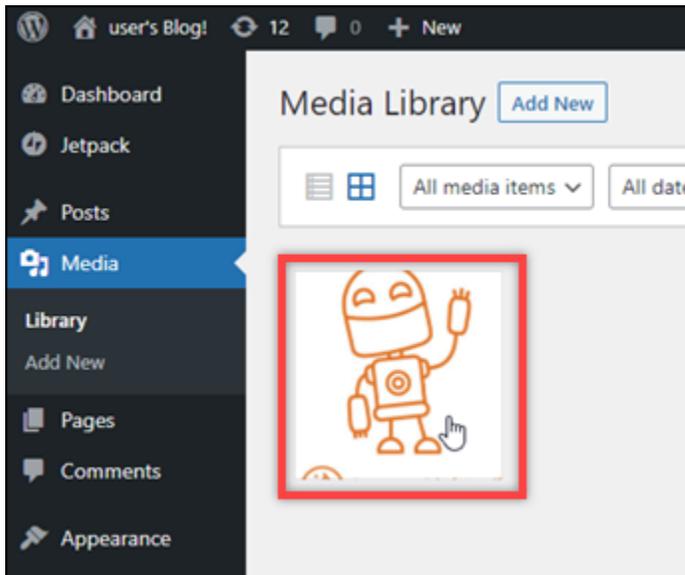
3. 選擇要從本機電腦上傳的媒體檔案，然後選擇 Open (開啟)。



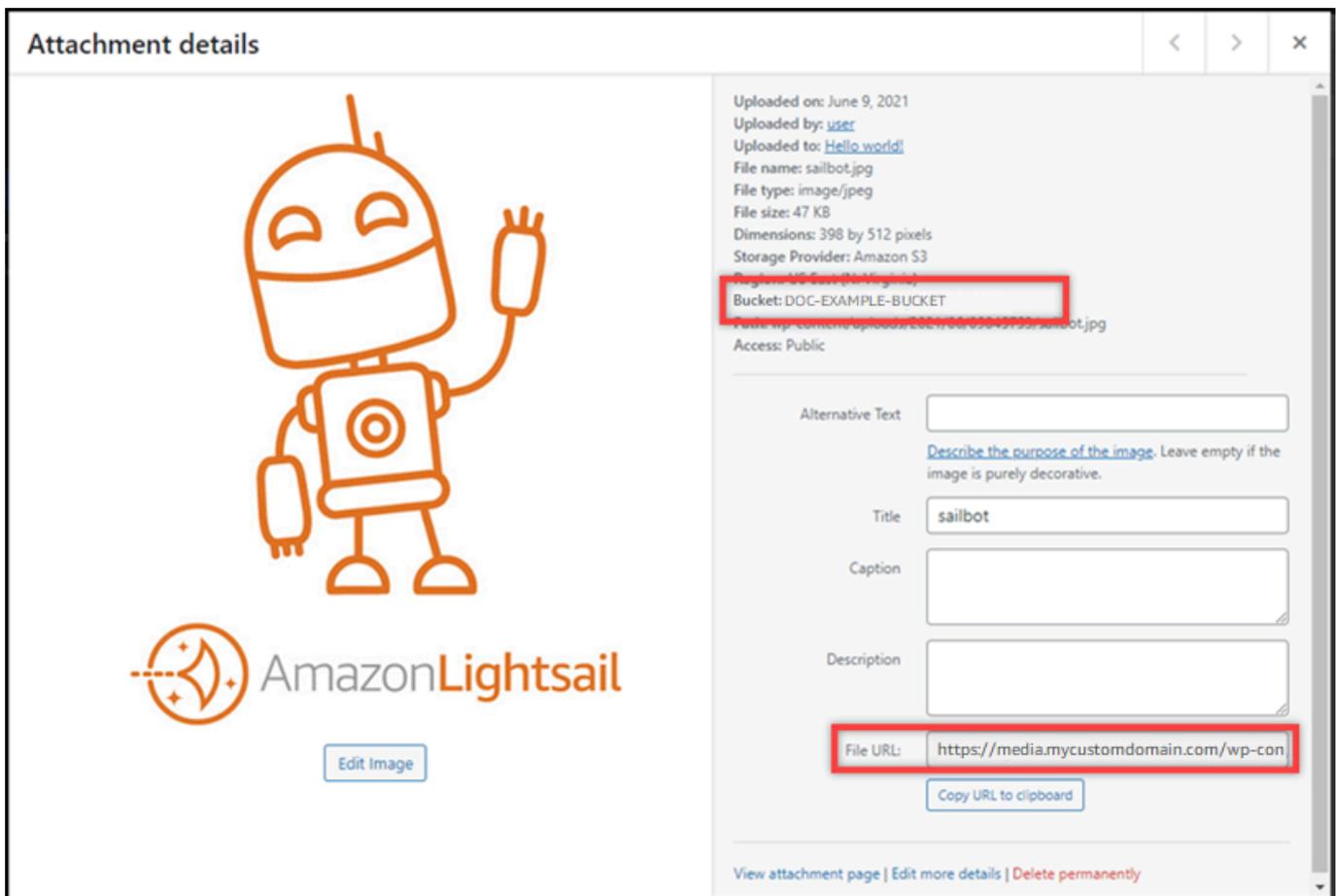
4. 檔案上傳完畢時，選擇左側導覽選單中 Media (媒體) 下方的 Library (程式庫)。



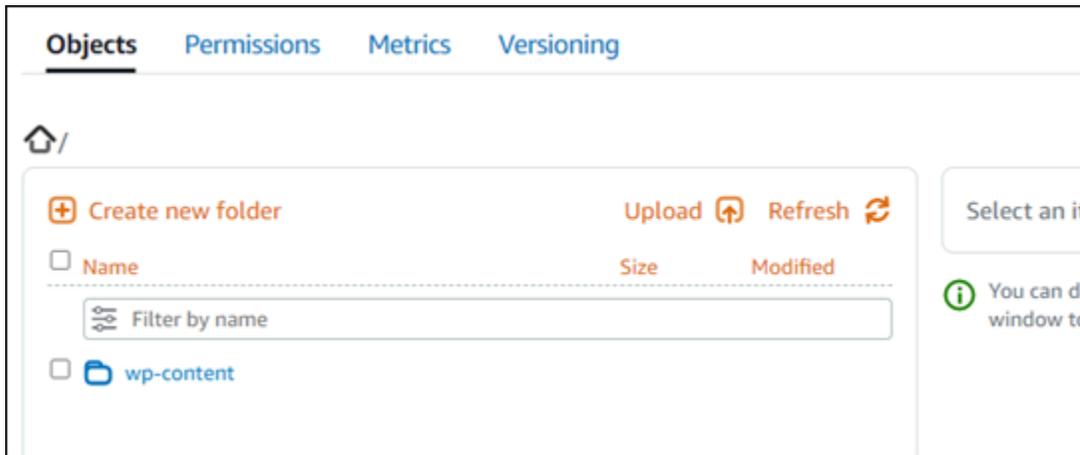
5. 選擇最近上傳的檔案。



- 在檔案的詳細資訊面板中，Bucket (儲存貯體) 欄位會出現儲存貯體名稱。分發的 URL 會出現在 File URL (檔案 URL) 欄位中。



- 如果您移至 Lightsail 值區管理頁面的 [物件] 索引標籤，您應該會看到可濕性粉劑內容資料夾。此資料夾由 Offload Media Lite 外掛程式建立，用於存放上傳的媒體檔案。



## 管理儲存貯體和物件

以下是管理 Lightsail 物件儲存貯體的一般步驟：

1. 了解 Amazon Lightsail 物件儲存服務中的物件和值區。如需詳細資訊，請參閱 [Amazon Lightsail 中的物件儲存](#)。
2. 了解您可以在 Amazon Lightsail 中為您的儲存貯體提供哪些名稱。如需詳細資訊，請參閱 [Amazon Lightsail 中的儲存貯體命名規則](#)。
3. 透過建立值區開始使用 Lightsail 物件儲存服務。如需詳細資訊，請參閱 [在 Amazon Lightsail 中建立值區](#)。
4. 了解儲存貯體的安全最佳實務，以及可以為儲存貯體設定的存取許可。可以將儲存貯體中的所有物件設為公有或私有，也可以選擇將個別物件設為公有。也可以透過建立存取金鑰、將執行個體附接至儲存貯體以及授予對其他 AWS 帳戶的存取權，來授予對儲存貯體的存取權。如需詳細資訊，請參閱 [Amazon Lightsail 物件儲存的安全最佳實務和了解 Amazon Lightsail 中的儲存貯體許可](#)。

了解儲存貯體存取許可後，請參閱下列指南來授予對儲存貯體的存取權：

- [封鎖儲存貯體的公開存取](#)
  - [在 Amazon Lightsail 中設定儲存貯體存取權限](#)
  - [在 Amazon Lightsail 中為儲存貯體中的個別物件設定存取權限](#)
  - [在 Amazon Lightsail 中為存儲桶創建訪問密鑰](#)
  - [在 Amazon Lightsail 中設定儲存貯體的資源存取](#)
  - [在 Amazon Lightsail 中設定儲存貯體的跨帳戶存取](#)
5. 了解如何為儲存貯體啟用存取日誌記錄，以及如何使用存取日誌來稽核儲存貯體的安全性。如需詳細資訊，請參閱下列指南。

- [Amazon Lightsail 物件儲存服務中儲存貯體的存取記錄](#)
  - [存取 Amazon Lightsail 物件儲存服務中儲存貯體的日誌格式](#)
  - [在 Amazon Lightsail 物件儲存服務中啟用儲存貯體的存取記錄](#)
  - [在 Amazon Lightsail 中使用儲存貯體的存取日誌來識別請求](#)
6. 建立 IAM 政策，讓使用者能夠在 Lightsail 中管理值區。如需詳細資訊，請參閱[在 Amazon Lightsail 中管理儲存貯體的 IAM 政策](#)。
  7. 了解儲存貯體中物件的標記和識別方式。如需詳細資訊，請參閱[了解 Amazon Lightsail 中的物件金鑰名稱](#)。
  8. 了解如何在儲存貯體中上傳檔案及管理物件。如需詳細資訊，請參閱下列指南。
    - [將文件上傳到 Amazon Lightsail](#)
    - [使用多部分上傳將檔案上傳到 Amazon Lightsail 中的儲存貯體](#)
    - [檢視儲存貯體中 Amazon Lightsail](#)
    - [在 Amazon Lightsail 中複製或移動值區中的物件](#)
    - [從儲存貯體中下載物件](#)
    - [在 Amazon Lightsail 中過濾存儲桶中的對象](#)
    - [標記存儲桶中 Amazon Lightsail](#)
    - [刪除存儲桶中 Amazon Lightsail](#)
  9. 啟用物件版本控制功能來保留、擷取和恢復儲存貯體中所儲存每個物件的各個版本。如需詳細資訊，請參閱在 [Amazon Lightsail 中啟用和暫停儲存貯體中的物件版本控制](#)。
  10. 啟用物件版本控制之後，可以還原儲存貯體中物件的先前版本。如需詳細資訊，請參閱在 [Amazon Lightsail 中還原儲存貯體中的舊版物件](#)。
  11. 監控儲存貯體的使用率。如需詳細資訊，請參閱[在 Amazon Lightsail 中檢視儲存貯體的指標](#)。
  12. 設定儲存貯體指標的警示，以便在儲存貯體的使用率超過閾值時收到通知。如需詳細資訊，請參閱[在 Amazon Lightsail 中建立儲存貯體指標警示](#)。
  13. 如果儲存空間和網路傳輸不足，請變更儲存貯體的儲存計畫。如需詳細資訊，請參閱[在 Amazon Lightsail 中變更儲存貯體的計畫](#)。
  14. 了解如何將儲存貯體連線至其他資源。如需詳細資訊，請參閱下列教學課程。
    - [教學課程：將 WordPress 執行個體連接至 Amazon Lightsail 儲存貯體](#)
    - [教學課程：將 Amazon Lightsail 儲存貯體與 Lightsail 內容交付網路分發搭配使用](#)
  15. 如果不再使用儲存貯體，請刪除它。如需詳細資訊，請參閱[在 Amazon Lightsail 中刪除值區](#)。

## 調整 Lightsail 發佈的資料傳輸配額

建立 Amazon Lightsail 分發時，您可以選擇指定每月資料傳輸配額和分發成本的分配計劃。如果您的分發傳輸的資料數量超過計劃的每月資料傳輸配額，則會向您收取超額費用。如需超額定價的詳細資訊，請參閱 [Lightsail 定價](#) 頁面。

若要避免產生超額費用，請將目前的分發計劃變更為不同的計劃，以便在分發超過每月配額之前，提供更多的每月資料傳輸量。在每個 AWS 帳單週期內，您只能變更一次配送方案。在本指南中，我們會為您介紹如何變更您的分發計劃。

如需有關分發的詳細資訊，請參閱 [內容交付網路分發](#)。

### 變更您的分發計劃

請完成下列程序來變更分發計劃。

1. 登入主 [Lightsail](#) 台。
2. 在 Lightsail 首頁，選擇 Networking (聯網) 索引標籤。
3. 選擇您要檢視目前每月資料傳輸的分發名稱。
4. 選擇分發管理頁面上的 Details (詳細資訊) 索引標籤。
5. 在該頁面的 Data transfer (資料傳輸) 區段中，選擇 Change distribution plan (變更分發計劃)。
6. 出現確認提示時，選擇 Yes, change (是，變更)，確認您要變更分發計劃。
7. 出現下一個提示時，選擇分發的新計劃，然後選擇 Select plan (選取計劃)。
8. 出現下一個提示時，選擇 Yes, apply (是，套用)，確認您要將新計劃套用至您的分發。或者選擇 No, go back (不，返回)，不將新計劃套用至您的分發。

## 為您的 Lightsail 發行版本提供具有自訂網域的內容

為您的 Amazon Lightsail 分發啟用自訂網域，以便在您的分發中使用已註冊的網域名稱。在您啟用自訂網域前，在首次建立分發時，其僅接受與分發相關聯的預設網域 (例如 123456abcdef.cloudfront.net) 流量。當您啟用自訂網域時，您必須選擇您針對要用於發佈的網域所建立的 Lightsail SSL/TLS 憑證。啟用自訂網域之後，分發會接受與所選憑證相關聯之所有網域的流量。

### Important

每個分發一次只能使用一個憑證。如果您停用分發上的自訂網域，您的分發將無法再為您註冊的網域處理 HTTPS 流量，直到您再次啟用自訂網域為止。

與 SSL/TLS 憑證相關聯的網域名稱不能被所有 Amazon 網路服務 (AWS) 帳戶 (包括 Amazon 服務上的分發) 的其他分發使用。CloudFront 您能夠為網域建立憑證，但無法將其與分發搭配使用。

如需有關分發的詳細資訊，請參閱[內容交付網路分發](#)。

## 必要條件

在開始之前，您必須先建立 Lightsail 發行版本。如需詳細資訊，請參閱[建立分發](#)。

您也應為分發建立並驗證 SSL/TLS 憑證。如需詳細資訊，請參閱[建立分發的 SSL/TLS 憑證](#)以及[驗證分發的 SSL/TLS 憑證](#)。

## 啟用分發的自訂網域

請完成以下程序，以啟用分發的自訂網域。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁，選擇 Networking (聯網) 索引標籤。
3. 選擇要啟用自訂網域之分發的名稱。
4. 選擇分發管理頁面上的 Custom domains (自訂網域) 索引標籤。
5. 選擇 Attach certificate (連接憑證)。

若您沒有憑證，則必須先為您的網域建立並驗證 SSL/TLS 憑證，再將其連接至分發。如需詳細資訊，請參閱[為分發建立 SSL/TLS 憑證](#)。

6. 在顯示的下拉式選單中，為您要搭配分發使用的網域，選取有效憑證。
7. 確認憑證資訊正確無誤，然後選擇 Attach (連接)。
8. 分發的 Status (狀態) 會變更為 Updating (正在更新)。狀態變更為 Enabled (已啟用) 後，憑證的網域就會出現在 Custom domains (自訂網域) 區段中。
9. 選擇 Add domain assignment (新增網域指派)，將網域指向您的分發。
10. 確認憑證和 DNS 資訊正確無誤，然後選擇 Add assignment (新增指派)。稍待片刻後，分發就會開始接受您所選網域的流量。

## 主題

- [將自訂網域指向發 Lightsail 版](#)
- [為您的發 Lightsail 版本更新 SSL/TLS 憑證網域](#)
- [停用發佈的 Lightsail 訂網域](#)
- [將發佈的預設網域新增至 Lightsail 容器服務](#)

## 將自訂網域指向發 Lightsail 版

在為分發啟用自訂網域之後，您必須將註冊的網域名稱指向 Amazon Lightsail 分發。您可以將別名記錄新增至在您與分發搭配使用的憑證上，所指定之每個網域的 DNS 區域來執行這項操作。您新增的所有記錄都應該指向分發的預設網域 (例如 123456abcdef.cloudfront.net)。

在本指南中，我們提供了使用 Lightsail DNS 區域將網域指向您的分發的程序。使用不同的 DNS 託管服務提供商 (例如 Domain.com 或 GoDaddy) 將域指向您的分發的過程可能類似。如需有關 DNS 區域 Lightsail 細資訊，請參閱 [DNS](#)。

如需有關分發的詳細資訊，請參閱[建立分發](#)。

## 內容

- [步驟 1：完成先決條件](#)
- [步驟 2：取得分發的預設網域](#)
- [步驟 3：新增記錄至網域的 DNS 區域](#)

### 步驟 1：完成先決條件

在開始之前，您應該為 Lightsail 發行版啟用自訂網域。如需詳細資訊，請參閱[啟用分發的自訂域](#)。

### 步驟 2：取得分發的預設網域

請完成下列程序，以取得分發的預設網域名稱，此名稱是在您將別名記錄新增至網域的 DNS 時所指定。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁，選擇 Networking (聯網) 索引標籤。
3. 選擇希望取得預設網域名稱之分發的名稱。

- 在分發管理頁面的標頭區段中，記下分發的預設網域名稱。分發的預設網域名稱與 `123456abcdef.cloudfront.net` 類似。

您必須在網域的 DNS 中新增此值作為別名記錄的一部分。建議您複製此值並貼至稍後可參考的文字檔案中。繼續至本教學課程的下一章節 [步驟 3：新增記錄至網域的 DNS 區域](#)。

### 步驟 3：新增記錄至網域的 DNS 區域

請完成以下程序，將記錄新增至網域的 DNS 區域。

- 選擇 Lightsail 首頁上的 Domains & DNS (網域和 DNS) 索引標籤。
- 在該頁面的 DNS zones (DNS 區域) 區段下，選擇您要在其中新增將網域流量導向至分發之記錄的網域名稱。
- 選擇 DNS records (DNS 記錄) 索引標籤。接著選擇 Add record (新增記錄)。
- 根據您希望指向分發的網域類型，完成下列其中一個步驟：

- 選擇地址 (A) 記錄來將頂點網域 (例如 `example.com`) 指向分發。

如果網域頂點的 A 記錄已經存在於 DNS 區域中，則您需要編輯該現有記錄，而不是新增其他 A 記錄。

- 選擇正式名稱 (CNAME) 來將子網域 (例如 `website.example.com`) 指向分發。
- 如果您要新增 A 記錄，則在 Resolves to (解析為) 文字方塊中，選擇分發的名稱。如果您要新增 CNAME 記錄，則在 Maps to (對應至) 文字方塊中，輸入分發的預設網域名稱。

#### Note

當您將 A 記錄新增至 DNS 區域，並選擇分發的名稱時，您實際上新增的是與地址記錄不同的別名記錄。Lightsail 可讓您輕鬆新增別名記錄，而無需執行其他 DNS 主機服務供應商通常需要的其他步驟。

- 選擇儲存圖示，將記錄儲存到 DNS 區域。

重複以上步驟，為與分發搭配使用的憑證上的網域新增其他 DNS 記錄。允許透過網際網路 DNS 傳播的變更時間。幾分鐘後，您應該就會看到網域是否指向分發。您也應該測試分發。如需詳細資訊，請參閱下面的 [測試分發](#)。

## 為您的發 Lightsail 版本更新 SSL/TLS 憑證網域

您可以將 Amazon Lightsail 分發所使用的自訂網域變更為另一個網域或一組網域。若要執行這項操作，您必須先為您要搭配分發使用的網域建立新的 SSL/TLS 憑證。如需詳細資訊，請參閱[為分發建立 SSL/TLS 憑證](#)。驗證新憑證之後，您需將舊憑證交換為新憑證，從而變更分發的自訂網域。

如需有關分發的詳細資訊，請參閱[建立分發](#)。

### 變更分發的自訂域

請完成下列程序，以變更分發的自訂網域。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁，選擇 Networking (聯網) 索引標籤。
3. 選擇您要變更自訂網域之分發的名稱。
4. 選擇分發管理頁面上的 Custom domains (自訂網域) 索引標籤。
5. 中斷連接目前連接到分發的 SSL/TLS 憑證。

分發的狀態會變更為 In progress (進行中)。

6. 分發的狀態變回 Enabled (已啟用) 後，選擇 Attach certificate (連接憑證)。
7. 在顯示的下拉式選單中，為您要搭配分發使用的網域，選取有效憑證。
8. 確認憑證資訊正確無誤，然後選擇 Attach (連接)。
9. 將網域指派新增至網域的 DNS，以將網域指向您的分發。

分發的 Status (狀態) 會變更為 Updating (正在更新)。狀態變更為 Ready (就緒) 後，憑證的網域就會出現在 Custom domains (自訂網域) 區段中。選擇 Add domain assignment (新增網域指派)，將網域指向您的分發。

10. 選擇 Add assignment (新增指派)。稍待片刻後，分發就會開始接受您所選網域的流量。
11. 選擇 Save (儲存)。

### 停用發佈的 Lightsail 訂網域

停用 Amazon Lightsail 分發的自訂網域，以停止在您的分發中使用已註冊的網域名稱。在您停用自訂網域後，分發僅會接受您第一次建立分發時與其相關聯的預設網域 (例如 123456abcdef.cloudfront.net) 之流量，而對於先前關聯自訂網域的流量將出現 403 錯誤。

如需有關分發的詳細資訊，請參閱[內容交付網路分發](#)。

## 停用分發的自訂網域

請完成下列程序，以停用分發的自訂網域。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁，選擇 Networking (聯網) 索引標籤。
3. 選擇要停用自訂網域之分發的名稱。
4. 選擇分發管理頁面上的 Custom domains (自訂網域) 索引標籤。

Custom domains (自訂網域) 頁面會顯示目前連接至分發的 SSL/TLS 憑證 (若有)。

5. 請選擇下列其中一個選項：
  1. 選擇 Configure distribution domains (設定分發網域)，以取消選取先前選取的網域，或選取與分發相關聯的更多網域。
  2. 選擇中斷連結，將憑證與分發中斷連結，並移除所有相關聯的域。
6. 系統會提交您停用自訂網域的請求，且分發狀態會變更為 In progress (進行中)。一段時間後，分發的狀態會變更為 Enabled (已啟用)。

在您停用自訂網域後，分發僅會接受您第一次建立分發時與其相關聯的預設網域 (例如 123456abcdef.cloudfront.net) 之流量，而對於先前關聯自訂網域的流量將出現 403 錯誤。您應更新網域的 DNS 記錄，以便將這些網域的流量引導至其他資源。

## 將發佈的預設網域新增至 Lightsail 容器服務

您可以選擇 Amazon Lightsail 容器服務做為內容交付網路 (CDN) 分發的來源。然後，分發會快取並服務容器服務上託管的網站或 Web 應用程式。如果您將 Lightsail 分發與 Lightsail 容器服務搭配使用，Lightsail 會自動將分發的預設網域名稱新增為容器服務上的自訂網域。這樣就可以在分發和容器服務之間路由流量。但是，您必須執行本指南中概述的步驟，在以下情況中手動將分發的預設網域名新增至容器服務：

- 如果出現問題，並且分發的預設網域名不會自動新增至容器服務。
- 如果您在容器服務中使用 Lightsail 配送以外的散佈。

您只能使用 ()，將散發的預設網域名稱手動新增至容器 AWS Command Line Interface 服務 AWS CLI。如需有關容器服務的詳細資訊，請參閱[容器服務](#)。如需有關分發的詳細資訊，請參閱[物件儲存](#)。

## 將分發的預設網域新增至 容器服務

完成下列程序，以使用 AWS Command Line Interface (AWS CLI) 將散發的預設網域新增至 Lightsail 中的容器服務。您可以使用 `update-container-service` 命令來執行此動作。若要取得更多資訊，請參閱《指AWS CLI 令參考》[update-container-service](#)中的。

### Note

您必須先為 Lightsail 安裝 AWS CLI 並對其進行設定，然後才能繼續執行此程序。如需詳細資訊，請參閱[設定 AWS CLI 定使用 Lightsail](#)。

1. 開啟命令提示或終端機視窗。
2. 輸入以下其中一條命令，將分發的預設網域新增至容器服務。

### Note

如果您將自訂網域新增至容器服務，則需要同時指定分發的自訂網域和預設網域。

容器服務上沒有設定自訂網域：

```
aws lightsail update-container-service --service-name ContainerServiceName --public-domain-names '{"_": ["DistributionDefaultDomain"]}'
```

在容器服務上設定了一個或多個自訂網域：

```
aws lightsail update-container-service --service-name ContainerServiceName --public-domain-names '{"CertificateName": ["ExistingCustomDomain"], "_": ["DistributionDefaultDomain"]}'
```

將命令中的以下範例文字取代為自訂文字：

- *ContainerServiceName*-指定為發行版本來源之 Lightsail 容器服務的名稱。
- *DistributionDefaultDomain*-使用容器服務作為來源之發行版的預設網域。例如 `example123.cloudfront.net`。
- *CertificateName* 「-目前附加至容器服務之自訂網域的 Lightsail 憑證名稱 (如果有的話)。如果沒有連接至容器服務的自訂網域，則使用標示為容器服務上沒有設定自訂網域的命令。

- *DistributionDefaultDomain*-目前附加至容器服務的自訂網域。

範例：

- 容器服務上沒有設定自訂網域：

```
aws lightsail update-container-service --service-name ContainerServiceName --public-domain-names '{"_": ["example123.cloudfront.net"]}'
```

- 在容器服務上設定了一個或多個自訂網域：

```
aws lightsail update-container-service --service-name ContainerServiceName --public-domain-names '{"example-com": ["example.com"], "_": ["example123.cloudfront.net"]}'
```

## 管理 Lightsail 發佈的請求和回應行為

在本指南中，我們說明 Amazon Lightsail 分發在處理和轉寄請求至您的來源，以及處理來自來源的回應時的行為方式。如需有關分發的詳細資訊，請參閱[內容交付網路分發](#)。

主題

- [分發如何處理和轉送請求至原始伺服器](#)
- [分發如何處理來自原始伺服器的回應](#)

## 分發如何處理和轉送請求至原始伺服器

本節包含相關資訊，說明分發如何處理檢視器的請求，以及如何將這些請求轉送至原始伺服器。

內容

- [身分驗證](#)
- [快取持續時間](#)
- [用戶端 IP 地址](#)
- [用戶端 SSL 身分驗證](#)
- [壓縮](#)
- [條件式請求](#)

- [Cookie](#)
- [跨原始伺服器資源分享 \(CORS\)](#)
- [加密](#)
- [包括內文的 GET 請求](#)
- [HTTP 方法](#)
- [HTTP 請求標頭和分發行為](#)
- [HTTP 版本](#)
- [最大請求長度和最大 URL 長度](#)
- [OCSP 裝訂](#)
- [持久性連線](#)
- [通訊協定](#)
- [查詢字串](#)
- [原始伺服器連線逾時和嘗試次數](#)
- [原始伺服器回應逾時](#)
- [相同物件之同步請求 \(流量高峰\)](#)
- [使用者代理程式標頭](#)

## 身分驗證

針對 DELETE、GET、HEAD、PATCH、POST 和 PUT 請求，如果您設定分發，以將 Authorization 標頭轉送至原始伺服器，則您可以設定原始伺服器以請求用戶端身分驗證。

針對 OPTIONS 請求，您可以將原始伺服器設定為只在您使用下列分發設定時，才會請求用戶端身分驗證：

- 將分發設定為將 Authorization 標頭轉送至原始伺服器。
- 將分發設定為不針對 OPTIONS 請求的回應進行快取。

您可以將分發設定為使用 HTTP 或 HTTPS 將請求轉送至原始伺服器。

## 快取持續時間

若要控制在分發將另一個請求轉送至原始伺服器之前，您的物件留存於分發快取中的時間長度，您可以：

- 設定原始伺服器在每個物件中新增 Cache-Control 或 Expires 標頭欄位。
- 使用 1 天的快取壽命 (TTL) 預設值。

如需詳細資訊，請參閱[分發進階設定](#)。

## 用戶端 IP 地址

如果檢視器將請求傳送至您的分發，且未包含 X-Forwarded-For 請求標頭，則分發會從 TCP 連線取得檢視器的 IP 地址，新增包含該 IP 地址的 X-Forwarded-For 標頭，然後將該請求轉送至原始伺服器。例如，如果您的分發從 TCP 連線取得 IP 地址 192.0.2.2，其會將以下標頭轉送至原始伺服器：

```
X-Forwarded-For: 192.0.2.2
```

如果檢視器將請求傳送到您的分發，且包含 X-Forwarded-For 請求標頭，則分發會從 TCP 連線取得檢視器的 IP 地址，將該 IP 地址附加到 X-Forwarded-For 標頭的結尾，然後將該請求轉送至原始伺服器。例如，如果檢視器的請求包含 X-Forwarded-For: 192.0.2.4,192.0.2.3，且您的分發從 TCP 連線取得 IP 地址 192.0.2.2，則分發會將以下標頭轉送至原始伺服器：

```
X-Forwarded-For: 192.0.2.4,192.0.2.3,192.0.2.2
```

某些應用程式，例如負載平衡器、Web 應用程式防火牆、反向代理伺服器、入侵防護系統和 API Gateway，會針對轉送請求的分發邊緣伺服器，將該伺服器的 IP 地址附加到 X-Forwarded-For 標頭的結尾。例如，如果您的分發在轉送給 ELB 的請求中加入 X-Forwarded-For: 192.0.2.2，且分發邊緣伺服器的 IP 地址為 192.0.2.199，則執行個體所收到的請求會包含以下標頭：

```
X-Forwarded-For: 192.0.2.2,192.0.2.199
```

### Note

X-Forwarded-For 標頭包含 IPv4 地址 (如 192.0.2.44) 和 IPv6 地址 (如 2001:0db8:85a3:0000:0000:8a2e:0370:7334)。

## 用戶端 SSL 身分驗證

Lightsail 發行版本不支援使用用戶端 SSL 憑證的用戶端驗證。如果原始伺服器請求用戶端憑證，您的分發會放棄請求。

## 壓縮

Lightsail 會向前發佈具有 Accept-Encoding 欄位值 "identity" 和 "gzip" 的請求。

## 條件式請求

如果您的分發收到請求，要求取得邊緣快取中已過期的物件，分發會將該請求轉送至原始伺服器，以取得物件的最新版本，或是從原始伺服器取得分發邊緣快取已具有最新版本的確認訊息。一般而言，當原始伺服器最後將物件傳送到您的分發時，會在回應中加入 ETag 值和/或 LastModified 值。在分發轉送至原始伺服器的新請求中，分發會新增以下其中一個或兩個項目：

- 含有已過期版本物件 If-Match 值的 If-None-Match 或 ETag 標頭。
- 含有已過期版本物件 If-Modified-Since 值的 LastModified 標頭。

原始伺服器使用此資訊來判斷物件是否已更新，且因此是否需傳回整個物件至分發，或只傳回 HTTP 304 狀態碼 (而非修改)。

## Cookie

您可以將分發設定為轉送 Cookie 至原始伺服器。如需詳細資訊，請參閱[分發進階設定](#)。

## 跨來源資源共享 (CORS)

如果您想讓分發遵循跨原始伺服器資源共享設定，請設定您的原始伺服器，以將 Origin 標頭轉送至原始伺服器。

## 加密

您可以要求檢視器使用 HTTPS 連接至分發，並要求分發使用 HTTP 或 HTTPS 將請求轉送至原始伺服器。

您的分發會使用 SSLv3、TLSv1.0、TLSv1.1 和 TLSv1.2 通訊協定，將 HTTPS 請求轉送至原始伺服器。其他 SSL 和 TLS 的版本不支援。

## 包括內文的 GET 請求

如果檢視器的 GET 請求包含內文，您的分發會將 HTTP 狀態碼 403 (禁止) 傳回給檢視器。

## HTTP 方法

如果將您的分發設定為允許所有其支援的 HTTP 方法，您的分發會接受檢視器的下列請求，然後將這些請求轉送至原始伺服器：

- DELETE
- GET
- HEAD
- OPTIONS
- PATCH
- POST
- PUT

您的分發一律會針對 GET 與 HEAD 請求的回應進行快取。您也可以設定分發以快取 OPTIONS 請求的回應。分發不會快取使用其他方法的請求的回應。

如需有關設定原始伺服器是否處理這些方法的詳細資訊，請參閱適用於原始伺服器的文件。

#### Important

如果您將分發設定為接受其支援的所有 HTTP 方法，並將這些方法轉送至原始伺服器，請設定您的原始伺服器來處理所有方法。例如，如果因為要使用 POST，而將分發設定為接受和轉送這些方法，則您必須設定原始伺服器，以適當地處理 DELETE 請求，讓檢視器無法刪除您不希望其刪除的資源。如需詳細資訊，請參閱您的 HTTP 伺服器文件。

## HTTP 請求標頭和分發行為

下列清單包含可以轉送至原始伺服器的 HTTP 請求標頭 (已指明例外狀況)。對於每個標頭，該清單包含下列項目的相關資訊：

- Supported (是否支援) - 您是否可以將分發設定為根據該標頭的標頭值快取物件。

您可以將分發設定為根據 Date 與 User-Agent 標頭中的值來快取物件，但我們不建議這麼做。這些標頭有許多可能的值，且根據其值來快取會導致分發轉送更多請求至原始伺服器。

- Behavior if you not configured (未設定時的行為) - 未將分發設定為將標頭轉送至原始伺服器時的分發行為，此行為會讓分發根據標頭值來快取物件。

- Header (標頭) - 其他定義的標頭

Supported (是否支援) - 是

Behavior if not configured (未設定時的行為) - 您的分發會將標頭轉送至原始伺服器。

- Header (標頭) - Accept

Supported (是否支援) - 是

Behavior if not configured (未設定時的行為) - 您的分發會移除標頭。

- Header (標頭) - Accept-Charset

Supported (是否支援) - 是

Behavior if not configured (未設定時的行為) - 您的分發會移除標頭。

- Header (標頭) - Accept-Encoding

Supported (是否支援) - 是

Behavior if not configured (未設定時的行為) - 若該值包含 gzip，您的分發會將 Accept-Encoding: gzip 轉送至原始伺服器。如果該值未包含 gzip，您的分發會在將請求轉送至原始伺服器之前，移除 Accept-Encoding 標頭欄位。

- Header (標頭) - Accept-Language

Supported (是否支援) - 是

Behavior if not configured (未設定時的行為) - 您的分發會移除標頭。

- Header (標頭) - Authorization

Supported (是否支援) - 是

Behavior if not configured (未設定時的行為) :

- GET 與 HEAD 請求 – 您的分發會在將請求轉送至原始伺服器之前，移除 Authorization 標頭欄位。
- OPTIONS 請求 – 若設定分發以快取 OPTIONS 請求的回應，則分發會在將請求轉送至原始伺服器之前移除 Authorization 標頭欄位。

如果您不將分發設定為快取 OPTIONS 請求的回應，則分發會將 Authorization 標頭欄位轉送至原始伺服器。

- DELETE、PATCH、POST 與 PUT 請求 – 您的分發不會在將請求轉送至原始伺服器之前移除標頭欄位。
- Header (標頭) - Cache-Control

Supported (是否支援) - 否

Behavior if not configured (未設定時的行為) - 您的分發會將標頭轉送至原始伺服器。

- Header (標頭) - CloudFront-Forwarded-Proto

Supported (是否支援) - 是

Behavior if not configured (未設定時的行為) - 您的分發在將請求轉送至原始伺服器之前，不會新增標頭。

- Header (標頭) - CloudFront-Is-Desktop-Viewer

Supported (是否支援) - 是

Behavior if not configured (未設定時的行為) - 您的分發在將請求轉送至原始伺服器之前，不會新增標頭。

- Header (標頭) - CloudFront-Is-Mobile-Viewer

Supported (是否支援) - 是

Behavior if not configured (未設定時的行為) - 您的分發在將請求轉送至原始伺服器之前，不會新增標頭。

- Header (標頭) - CloudFront-Is-Tablet-Viewer

Supported (是否支援) - 是

Behavior if not configured (未設定時的行為) - 您的分發在將請求轉送至原始伺服器之前，不會新增標頭。

- Header (標頭) - CloudFront-Viewer-Country

Supported (是否支援) - 是

Behavior if not configured (未設定時的行為) - 您的分發在將請求轉送至原始伺服器之前，不會新增標頭。

- Header (標頭) - Connection

Supported (是否支援) - 否

Behavior if not configured (未設定時的行為) - 您的分發會將請求轉送至原始伺服器之前，使用 Connection: Keep-Alive 取代此標頭。

- Header (標頭) - Content-Length

Supported (是否支援) - 否

Behavior if not configured (未設定時的行為) - 您的分發會將標頭轉送至原始伺服器。

- Header (標頭) - Content-MD5

Supported (是否支援) - 是

Behavior if not configured (未設定時的行為) - 您的分發會將標頭轉送至原始伺服器。

- Header (標頭) - Content-Type

Supported (是否支援) - 是

Behavior if not configured (未設定時的行為) - 您的分發會將標頭轉送至原始伺服器。

- Header (標頭) - Cookie

Supported (是否支援) - 否

Behavior if not configured (未設定時的行為) - 如果您將分發設定為轉送 Cookie，則其會將 Cookie 標頭欄位轉送至原始伺服器。如果未如此設定，您的分發會移除 Cookie 標頭欄位。

- Header (標頭) - Date

Supported (是否支援) - 是，但不建議

Behavior if not configured (未設定時的行為) - 您的分發會將標頭轉送至原始伺服器。

- Header (標頭) - Expect

Supported (是否支援) - 是

Behavior if not configured (未設定時的行為) - 您的分發會移除標頭。

- Header (標頭) - From

Supported (是否支援) - 是

Behavior if not configured (未設定時的行為) - 您的分發會將標頭轉送至原始伺服器。

- Header (標頭) - Host

Supported (是否支援) - 是

分發如何處理和轉送請求至原始伺服器

Behavior if not configured (未設定時的行為) - 您的分發會將該值設定為與請求物件相關聯之原始伺服器的網域名稱。

- Header (標頭) - If-Match

Supported (是否支援) - 是

Behavior if not configured (未設定時的行為) - 您的分發會將標頭轉送至原始伺服器。

- Header (標頭) - If-Modified-Since

Supported (是否支援) - 是

Behavior if not configured (未設定時的行為) - 您的分發會將標頭轉送至原始伺服器。

- Header (標頭) - If-None-Match

Supported (是否支援) - 是

Behavior if not configured (未設定時的行為) - 您的分發會將標頭轉送至原始伺服器。

- Header (標頭) - If-Range

Supported (是否支援) - 是

Behavior if not configured (未設定時的行為) - 您的分發會將標頭轉送至原始伺服器。

- Header (標頭) - If-Unmodified-Since

Supported (是否支援) - 是

Behavior if not configured (未設定時的行為) - 您的分發會將標頭轉送至原始伺服器。

- Header (標頭) - Max-Forwards

Supported (是否支援) - 否

Behavior if not configured (未設定時的行為) - 您的分發會將標頭轉送至原始伺服器。

- Header (標頭) - Origin

Supported (是否支援) - 是

Behavior if not configured (未設定時的行為) - 您的分發會將標頭轉送至原始伺服器。

- Header (標頭) - Pragma

Supported (是否支援) - 否

Behavior if not configured (未設定時的行為) - 您的分發會將標頭轉送至原始伺服器。

- Header (標頭) - Proxy-Authenticate

Supported (是否支援) - 否

Behavior if not configured (未設定時的行為) - 您的分發會移除標頭。

- Header (標頭) - Proxy-Authorization

Supported (是否支援) - 否

Behavior if not configured (未設定時的行為) - 您的分發會移除標頭。

- Header (標頭) - Proxy-Connection

Supported (是否支援) - 否

Behavior if not configured (未設定時的行為) - 您的分發會移除標頭。

- Header (標頭) - Range

Supported (是否支援) - 是，此為預設

Behavior if not configured (未設定時的行為) - 您的分發會將標頭轉送至原始伺服器。

- Header (標頭) - Referer

Supported (是否支援) - 是

Behavior if not configured (未設定時的行為) - 您的分發會移除標頭。

- Header (標頭) - Request-Range

Supported (是否支援) - 否

Behavior if not configured (未設定時的行為) - 您的分發會將標頭轉送至原始伺服器。

- Header (標頭) - TE

Supported (是否支援) - 否

Behavior if not configured (未設定時的行為) - 您的分發會移除標頭。

- Header (標頭) - Trailer

Supported (是否支援) - 否

Behavior if not configured (未設定時的行為) - 您的分發會移除標頭。

- Header (標頭) - Transfer-Encoding

Supported (是否支援) - 否

Behavior if not configured (未設定時的行為) - 您的分發會將標頭轉送至原始伺服器。

- Header (標頭) - Upgrade

支援-否 (除了 WebSocket 連線)

行為 ( 如果未配置 ) - 除非您已經建立了 WebSocket 連接，否則您的發行版會刪除標題。

- Header (標頭) - User-Agent

Supported (是否支援) - 是，但不建議

Behavior if not configured (未設定時的行為) - 您的分發會以 Amazon CloudFront 取代此標頭欄位的值。

- Header (標頭) - Via

Supported (是否支援) - 是

Behavior if not configured (未設定時的行為) - 您的分發會將標頭轉送至原始伺服器。

- Header (標頭) - Warning

Supported (是否支援) - 是

Behavior if not configured (未設定時的行為) - 您的分發會將標頭轉送至原始伺服器。

- Header (標頭) - X-Amz-Cf-Id

Supported (是否支援) - 否

Behavior if not configured (未設定時的行為) - 您的分發會在將請求轉送至原始伺服器之前，新增標頭至檢視器請求。此標頭值包含可唯一識別請求的加密字串。

- Header (標頭) - X-Edge-\*

Supported (是否支援) - 否

Behavior if not configured (未設定時的行為) - 您的分發會移除所有 X-Edge-\* 標頭。

- Header (標頭) - X-Forwarded-For

Supported (是否支援) - 是

Behavior if not configured (未設定時的行為) - 您的分發會將標頭轉送至原始伺服器。

- Header (標頭) - X-Forwarded-Proto

Supported (是否支援) - 否

Behavior if not configured (未設定時的行為) - 您的分發會移除標頭。

- Header (標頭) - X-Real-IP

Supported (是否支援) - 否

Behavior if not configured (未設定時的行為) - 您的分發會移除標頭。

## HTTP 版本

您的分發會使用 HTTP/1.1 將請求轉送至原始伺服器。

## 最大請求長度和最大 URL 長度

最大請求長度，包括路徑、查詢字串 (如果有) 和標頭是 20,480 位元組。

您的分發會從請求建構 URL。此 URL 的最大長度為 8192 位元組。

如果請求或 URL 超過這些最大值，您的分發會向檢視器傳回 HTTP 狀態碼 413、Request Entity Too Large (請求實體太大)，然後終止與檢視器的 TCP 連線。

## OCSP 裝訂

在檢視器為物件提交 HTTPS 請求時，您的分發或檢視器必須以憑證授權機構 (CA) 確認網域的 SSL 憑證尚未撤銷。OCSP 裝訂會透過允許您的分發從 CA 驗證憑證和快取回應，加速憑證驗證，讓用戶端不需直接以 CA 驗證憑證。

OCSP 裝訂的效能提升，在您的分發收到相同網域中物件的許多 HTTPS 請求時，更加明顯。分發節點中的每個伺服器均須提交單獨的驗證請求。當您的分發收到同一個網域的大量 HTTPS 請求時，節點中的每個伺服器很快就會收到來自 CA 的回應，伺服器可將此回應「釘」到 SSL 交握中的封包；當檢視

器確認憑證為有效時，您的分發即可提供請求的物件。如果您的分發無法取得節點中的許多流量，新的請求更有可能被引導至尚未使用 CA 驗證憑證的伺服器。在此情況下，檢視器會單獨執行驗證步驟，且分發伺服器會提供物件。該分發伺服器也會提交驗證請求至 CA，因此下次收到包含相同網域名稱的請求時，伺服器會取得來自 CA 的驗證回應。

## 持久性連線

當您的分發從原始伺服器獲得回應時，其會嘗試維持幾秒鐘連線，以確保在該段期間內另一個請求送達。維護持久性連線可節省重新建立 TCP 連線所需的時間，並為後續請求執行另一個 TLS 交握。

## 通訊協定

您的分發會根據 Lightsail 主控台中「原始通訊協定原則」欄位的值，將 HTTP 或 HTTPS 要求轉寄至原始伺服器。在主 Lightsail 中，選項只有 HTTP，而只有 HTTPS。

如果您指定 HTTP Only (僅限 HTTP) 或 HTTPS Only (僅限 HTTPS)，則無論檢視器請求中的通訊協定為何，您的分發都會使用指定的通訊協定，將請求轉送至原始伺服器。

### Important

如果您的分發使用 HTTPS 通訊協定來將請求轉送至原始伺服器，而且原始伺服器傳回無效的憑證或自簽憑證，您的分發會捨棄 TCP 連線。

## 查詢字串

您可以設定分發是否將查詢字串參數轉送至原始伺服器。

## 原始伺服器連線逾時和嘗試次數

依據預設，您的分發會等待 30 秒 (嘗試 3 次，每次 10 秒)，然後再將錯誤回應傳回給檢視器。

## 原始伺服器回應逾時

「原始伺服器回應逾時」，也稱為「原始伺服器讀取逾時」或「原始伺服器請求逾時」，適用於以下兩個數值：

- 在將請求轉送至原始伺服器之後，您的分發等待回應的時間 (以秒為單位)。
- 您的分發在收到來自原始伺服器的回應封包後，並在接收下一個封包前所等待的時間 (以秒為單位)。

分發的行為取決於檢視器請求的 HTTP 方法：

- GET 與 HEAD 請求 – 如果原始伺服器在回應逾時期間未回應或是停止回應，您的分發會捨棄連線。如果指定的原始伺服器連線嘗試次數超過 1，您的分發會再次嘗試取得完整的回應。您的分發可嘗試最多 3 次，由原始伺服器連線嘗試次數設定的值決定。如果原始伺服器在最後一次嘗試時未回應，則您的分發不會再嘗試，直到其收到針對同一原始伺服器上的內容的另一個請求。
- DELETE、OPTIONS、PATCH、PUT 與 POST 請求 – 如果原始伺服器未在 30 秒內回應，您的分發會捨棄連線，而且不會再嘗試聯絡原始伺服器。用戶端可以視需要重新提交請求。

## 相同物件之同步請求 (流量高峰)

如果分發節點收到物件請求，而且該物件目前不在快取中或物件已過期，您的分發會立即將該請求傳送到原始伺服器。如果流量突增 (在原始伺服器回應第一個請求之前，如果有對同一個物件的其他請求送達邊緣節點)，則在將對該物件的其他請求轉送到原始伺服器之前，分發會短暫地暫停。一般而言，第一個請求的回應將在後續請求的回應之前抵達分發節點。此暫時暫停有助於減少您的原始伺服器上不必要的負載。如果其他請求不一樣 (例如，因為您將分發設定為根據請求標頭或 Cookie 來進行快取)，則您的分發會將所有獨特的請求轉送至原始伺服器。

## 使用者代理程式標頭

如果您希望分發根據使用者用來檢視內容的裝置，快取不同的物件版本，我們建議您將分發設定為將以下一個或多個標頭轉送至原始伺服器：

- CloudFront-Is-Desktop-Viewer
- CloudFront-Is-Mobile-Viewer
- CloudFront-Is-SmartTV-Viewer
- CloudFront-Is-Tablet-Viewer

根據 User-Agent 標頭的值，您的分發會將這些標頭的值設定為 true 或 false，然後將請求轉送至原始伺服器。如果裝置屬於多個類別，一個以上的值可能是 true。例如，針對部分平板電腦裝置，您的分發可能會將 CloudFront-Is-Mobile-Viewer 與 CloudFront-Is-Tablet-Viewer 同時設定為 true。

您可以將分發設定為根據 User-Agent 標頭中的值來快取物件，但我們不建議這麼做。User-Agent 標頭有許多可能的值，且根據這些值來快取會導致分發轉送更多請求至原始伺服器。

如果不將分發設定為根據 User-Agent 標頭中的值來快取物件，您的分發會在將請求轉送至原始伺服器之前，新增具有下列值的 User-Agent 標頭：

## User-Agent = Amazon CloudFront

無論檢視器所傳來的請求是否包含 User-Agent 標頭，您的分發都會新增此標頭。如果檢視器所傳來的請求包含 User-Agent 標頭，您的分發會將其移除。

## 分發如何處理來自原始伺服器的回應

本章節包含相關資訊，說明分發如何處理來自原始伺服器的回應。

### 內容

- [100-Continue 回應](#)
- [快取](#)
- [已取消請求](#)
- [內容議價](#)
- [Cookie](#)
- [已捨棄 TCP 連線](#)
- [您的分發移除或取代的 HTTP 回應標頭](#)
- [檔案大小上限](#)
- [原始伺服器無法使用](#)
- [重新引導](#)
- [傳輸編碼](#)

### 100-Continue 回應

您的原始伺服器無法傳送一個以上的 100-Continue 回應給分發。在第一個 100-Continue 回應之後，您的分發會預期獲得 HTTP 200 OK 回應。如果您的原始伺服器在第一個 100-Continue 回應之後傳送另一個回應，您的分發將傳回錯誤。

### 快取

- 請確保您的原始伺服器為 Date 和 Last-Modified 標頭欄位設定有效且準確的值。
- 如果從瀏覽者請求包含 If-Match 或 If-None-Match 請求標頭欄位，設定 ETag 回應標頭欄位。如果您未指定 ETag 值，則您的分發會忽略後續的 If-Match 或 If-None-Match 標頭。
- 您的分發通常會遵循原始伺服器回應中的 Cache-Control: no-cache 標頭。如需了解例外情況，請參閱[同時請求相同物件 \(流量尖峰\)](#)。

## 已取消請求

如果物件不在邊緣快取中，且在您的分發從原始伺服器取得物件之後，但在傳送請求的物件前，檢視器就已終止工作階段 (例如，關閉瀏覽器)，則您的分發不會在節點中快取該物件。

## 內容議價

如果您的原始伺服器在回應中傳回 `Vary: *`，而且對應快取行為的 Minimum TTL (最短 TTL) 值為 0，則您的分發會快取物件，但仍會將針對該物件的每個後續請求轉送至原始伺服器，以確認快取包含物件的最新版本。您的分發不包含任何條件式標頭，例如 `If-None-Match` 或 `If-Modified-Since`。因此，您的原始伺服器會將物件傳回給分發，以回應每個請求。

如果您的來源 `Vary: *` 在回應中傳回，並且對應快取行為的「最小 TTL」值是任何其他值，則會依照[您的散佈移除或取代的 HTTP 回應標頭](#) `Vary` 頭中所述 CloudFront 處理標頭的標頭。

## Cookie

如果您為快取行為啟用 Cookie，而且如果原始伺服器隨物件傳回 Cookie，則您的分發會快取物件和 Cookie。請注意，這會降低對象的緩存能力。

## 已捨棄 TCP 連線

如果在您的原始伺服器將物件傳回分發時，您的分發與原始伺服器之間的 TCP 連線中斷，則分發會根據原始伺服器是否在回應中加入了 `Content-Length` 標頭來執行動作：

- `Content-Length` 標頭 – 您的分發會在從原始伺服器取得物件時，將物件傳回給檢視器。不過，如果 `Content-Length` 標頭的值不符合物件的大小，您的分發就不會快取物件。
- `Transfer-Encoding: Chunked` – 您的分發會在從原始伺服器取得物件時，將物件傳回給檢視器。不過，如果區塊回應不完整，您的分發不會快取物件。
- 無 `Content-Length` 標頭 – 您的分發會將物件傳回給檢視器並快取物件，但物件可能會不完整。如果沒有 `Content-Length` 標頭，您的分發就無法判斷 TCP 連線中斷是意外或刻意造成。

我們建議您設定 HTTP 伺服器以新增 `Content-Length` 標頭，來防止您的分發僅快取部分物件。

## 您的分發移除或取代的 HTTP 回應標頭

在將原始伺服器傳來的回應轉送給檢視器之前，您的分發會移除或更新以下標頭欄位：

- `Set-Cookie` – 如果您設定分發以轉送 Cookie，它會將 `Set-Cookie` 標頭欄位轉送給用戶端。

- Trailer
- Transfer-Encoding – 如果您的原始伺服器傳回此標頭欄位，則您的分發會在將回應傳回給檢視器之前，將值設定為 chunked。
- Upgrade
- Vary – 請注意以下各項：
  - 如果您將分發設定為將任何裝置特定的標頭轉送至原始伺服器 (CloudFront-Is-Desktop-Viewer、CloudFront-Is-Mobile-Viewer、CloudFront-Is-SmartTV-Viewer、CloudFront-Is-Tablet-Viewer)，且設定原始伺服器以將 Vary:User-Agent 傳回給分發，則分發會將 Vary:User-Agent 傳回給檢視器。
  - 如果您將原始伺服器設定為在 Vary 標頭中加入 Accept-Encoding 或 Cookie，則您的分發會在對檢視器的回應中加入這些值。
  - 如果您將發行版配置為將允許標題列表轉發到您的來源，並且如果將來源配置為將標題名稱返回到標Vary題中的發行版（例如，Vary:Accept-Charset,Accept-Language），則您的發行版將帶有這些值的標Vary頭返回給查看器。
  - 如需有關分發如何處理 Vary 標頭中的 \* 值的詳細資訊，請參閱[內容議價](#)。
  - 如果您將原始伺服器設定為在 Vary 標頭中加入其他任何值，您的分發會在把回應傳回給檢視器之前，移除這些值。
- Via – 您的分發會在對檢視器的回應中將該值設定為以下值：

Via: *http-## ##-##*.cloudfront.net (CloudFront)

例如，如果用戶端透過 HTTP/1.1 發出請求，則值將類似以下內容：

Via: 1.1 1026589cc7887e7a0dc7827b4example.cloudfront.net (CloudFront)

## 檔案大小上限

您的分發將傳回給檢視器之回應內文的大小上限為 20 GB。此包含未指定 Content-Length 標頭值的區塊傳輸回應。

## 原始伺服器無法使用

如果您的原始伺服器無法使用，且您的分發已收到請求，要求取得邊緣快取中已經過期的物件（例如，因為 Cache-Control max-age 指令中所指定的期間已過），則分發會提供該物件已過期的版本，或是提供自訂的錯誤頁面。

在某些情況下，很少請求的物件會被移出並在節點快取中不可再用。您的分發無法提供已移出的物件。

## 重新引導

如果您在原始伺服器中變更物件的位置，您可以設定 Web 伺服器以將請求重新引導至新位置。在您設定重新引導後，檢視器第一次提交對物件的請求時，您的分發會將請求傳送至原始伺服器，且原始伺服器以重新引導回應 (例如 302 Moved Temporarily)。您的分發會快取重新引導，並將其傳回給檢視器。分發不會遵循重新引導。

您可以設定您的 Web 伺服器重新引導請求以下其中一個位置：

- 在原始伺服器中物件的新 URL。當檢視器遵循重新引導至新 URL 時，檢視器會略過您的分發，並直接前往原始伺服器。因此，我們建議您不要重新引導請求到原始伺服器中物件的新 URL。
- 物件的新分發 URL。如果檢視器提交請求，其中包含新的分發 URL，則您的分發會從原始伺服器上的新位置取得物件，在節點上快取該物件，然後將物件傳回給檢視器。物件的後續請求會被節點提供。這可避免與從原始伺服器瀏覽者請求的物件有關的延遲和負載。然而，每個新的物件請求會就針對分發的兩個請求產生費用。

## 傳輸編碼

Lightsail 發行版僅支援 Transfer-Encoding 標頭的 chunked 值。如果您的原始伺服器傳回 Transfer-Encoding: chunked，則您的分發會在節點接收到物件時，將物件傳回給用戶端，並以區塊的格式快取物件，來因應後續的請求。

如果檢視器提出 Range GET 請求，而原始伺服器傳回 Transfer-Encoding: chunked，則您的分發會將整個物件 (而非請求的範圍) 傳回給檢視器。

如果您無法預定回應內容的長度，我們建議您使用區塊編碼。如需詳細資訊，請參閱[捨棄 TCP 連線](#)。

## 驗證您的 Lightsail 發行版本的內容快取

在本指南中，您將了解如何測試 Amazon Lightsail 分發是否正在從您的來源快取和提供內容。將註冊的網域名稱新增至分發後應執行此測試。如需有關分發的詳細資訊，請參閱[內容交付網路分發](#)。

## 測試您的分發

請完成下列程序來測試您的分發。我們在此程序中使用 Chrome Web 瀏覽器；其他瀏覽器可能會採用類似的步驟。

1. 開啟 Chrome Web 瀏覽器。

2. 開啟瀏覽器視窗 — upper-right-hand 角的 Chrome 選單，然後選取 [更多工具] > [開發人員工具]。  
您也可以使用捷徑選項 + ⌘ + J (在 macOS 上)，或是 Shift + CTRL + J (在 Windows/Linux 上)。
3. 在開發人員工具窗格中，選擇 Network (網路) 索引標籤。
4. 瀏覽至分發的網域 (例如 <https://www.example.com>)。

Chrome 開發人員工具的 Network (網路) 索引標籤應該會填入網站上的物件清單。

5. 選擇靜態物件，例如影像檔 (.jpg、.png、.gif)。
6. 在出現的「標題」面板中，您應該看到 via 和 x-cache 標題都提到了 CloudFront。這可確認您的分發正在從原始伺服器快取並提供內容。

The screenshot shows the Chrome DevTools Network tab. The left pane displays a list of requests, with 'sailbot.jpg' selected and circled in red. The right pane shows the 'General' tab of the selected request. The 'Response Headers' section contains the following headers:

```
accept-ranges: bytes
age: 8
cache-control: s-maxage=10
content-length: 48224
content-type: image/jpeg
date: Thu, 25 Jun 2020 12:11:46 GMT
etag: "bc60-5a8e774882d25"
last-modified: Thu, 25 Jun 2020 12:08:49 GMT
server: Apache
status: 200
via: 1.1 9b311162717b41c968f6f00426d88aaa.cloudfront.net (CloudFront)
x-amz-cf-id: guY1UdZ6jAKfg8CNIw_EuYGD7ELe8zhPfaktKrF4GQaNRokpCoMBA=
x-cache: Hit from cloudfront
x-frame-options: deny
```

The 'via' and 'x-cache' headers are circled in red, indicating that the content was served from a CloudFront cache.

# Amazon Lightsail 中的聯網資源

Lightsail 網路資源可改善使用者和外部服務與 Lightsail 執行個體的連線方式。

## 負載平衡器

您可以建立負載平衡器，藉此新增備援機制或處理更多流量。如需詳細資訊，請參閱[負載平衡器](#)。

## 靜態 IPs

您可以建立靜態 IP 地址，如此每次重新啟動執行個體時，都能繼續使用相同的 IP 地址。如需詳細資訊，請參閱[靜態 IP 地址](#)。

## 檢視和管理資源的 Lightsail 址

您可以使用這些執行個體的 IP 位址與 Lightsail 執行個體及其他 Lightsail 資源進行通訊。例如，使用執行個體的公有 IP 位址，您可以檢查執行個體的網路狀態 (使用PING)、建立與執行個體的SSH連線，以及從自訂網域名稱將流量路由至執行個體。您還可以使用 Lightsail 資源的 IP 位址執行更多作業。

Lightsail 執行個體、容器服務和負載平衡器同時支援IPv4和IPv6定址通訊協定。這些資源預設會使用定IPv4址通訊協定；您無法停用此行為。您可以選擇IPv6為執行個體、容器服務和負載平衡器啟用。

在本指南中，我們涵蓋了您在 Lightsail 中需要瞭解的 IP 位址的相關資訊。

### 內容

- [執行個體的私人和公用IPv4位址](#)
- [執行個體的靜態 IP 地址](#)
- [IPv6適用於執行個體、容器服務、CDN分發和負載平衡器](#)

## 執行個體的私人和公用IPv4位址

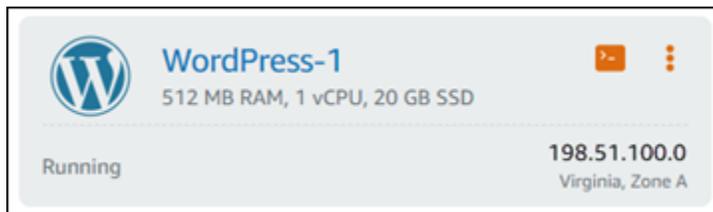
當您建立 Lightsail 實體時，系統會為其指派公用和私人IPv4位址。公用 IP 位址可供網際網路存取，而私人 IP 位址僅供 Lightsail 帳戶中的資源存取。AWS 區域

**Note**

您執行個體的私有 IP 位址可供相同AWS區域中的其他AWS資源存取，但如果您啟用VPC對等互連，則可在 Lightsail 帳戶之外存取。如需詳細資訊，請參閱[設定 Amazon VPC 對等互連以使用 Lightsail 以外的AWS資源](#)。

您執行個體的 IP 位址會顯示在 Lightsail 主控台的下列區域中：

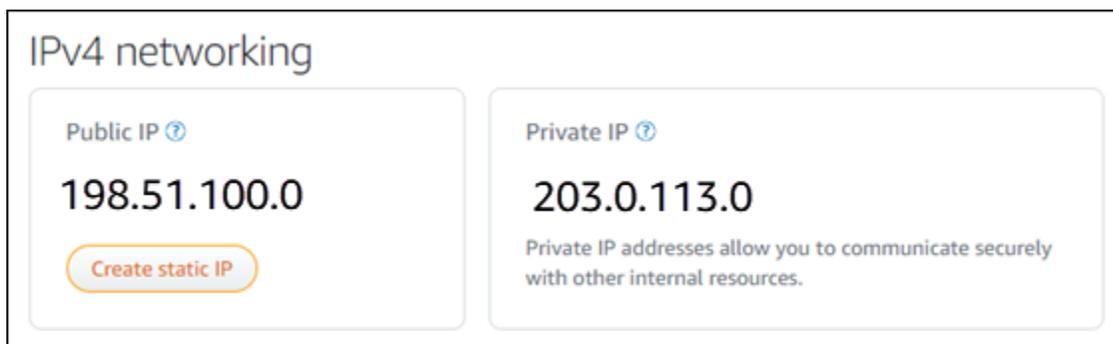
- 下列範例顯示 Lightsail 首頁上執行個體的公用 IP 位址。



- 下列範例顯示執行個體管理頁面標頭區域中的執行個體公有和私有 IP 地址。



- 下列範例顯示執行個體管理頁面的 Networking (聯網) 索引標籤上的執行個體公有和私有 IP 地址。



使用執行個體的IPv4位址時，請記住下列事項：

- 執行個體的公有 IP 地址可能會變動。將靜態 IP 連接到執行個體，為您的執行個體提供一個永不變動的 IP 地址。如需詳細資訊，請參閱本指南的[執行個體的靜態 IP 地址](#)一節。

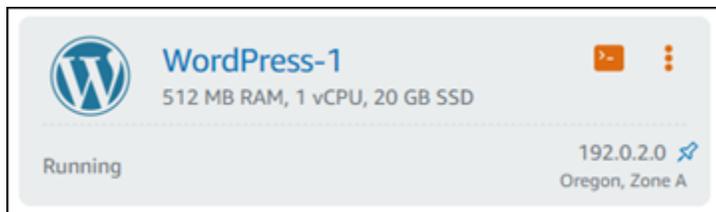
- 依預設，Lightsail 會使用IPv4位址。不過，您可以選擇性地啟IPv6用某些在 2021 年 1 月 12 日之前建立的 Lightsail 資源。在 2021 年 1 月 12 日當天或之後建立的資源預設已IPv6啟用。如需詳細資訊，請參閱本指南的[IPv6針對執行個體、容器服務、CDN分發和負載平衡器](#)一節。
- 將規則新增到執行個體防火牆，以控制可連接到該執行個體的流量。如需詳細資訊，請參閱[執行個體防火牆](#)。

## 執行個體的靜態IPv4位址

當您停止並啟動執行個體時，指派給執行個體的預設公用IPv4位址將會變更。您可以選擇性地建立靜態IPv4位址，並將其附加至執行個體。靜態IPv4位址會取代執行個體的預設公用IPv4位址，當您停止並啟動執行個體時，它會保持不變。您可以將一個靜態 IP 連接至一個執行個體。如需詳細資訊，請參閱[建立靜態 IP 並將其附接至執行個體](#)。

建立靜態 IP 並將其附加至執行個體後，該 IP 會顯示在 Lightsail 主控台的下列區域中：

- 下列範例顯示 Lightsail 首頁上執行個體的靜態 IP 位址。圖釘圖示表示公有 IP 地址是靜態 IP 地址。



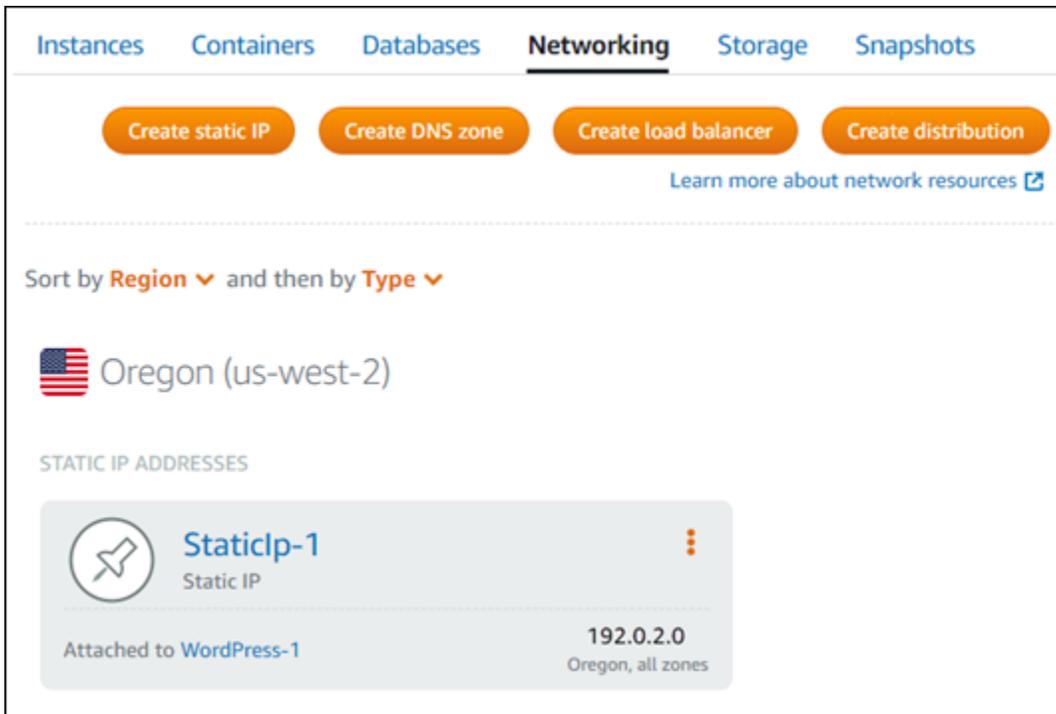
- 下列範例顯示執行個體管理頁面標頭區域中的執行個體靜態 IP 地址。圖釘圖示表示公有 IP 地址是靜態 IP 地址。



- 下列範例會顯示執行個體管理頁面的 Networking (聯網) 索引標籤上的執行個體靜態 IP 地址。預設的公有 IP 地址不再列出，而且已由靜態 IP 地址取代。圖釘圖示表示公有 IP 地址是靜態 IP 地址。



- 您可以移至 Lightsail 首頁的 [網路功能] 索引標籤，檢視您所建立的所有靜態IPs，如下列範例所示。



## IPv6適用於執行個體、容器服務、CDN分發和負載平衡器

IPv6依預設，針對在 2021 年 1 月 12 日或之後建立的 Lightsail 執行個體、容器服務、CDN分發和負載平衡器啟用。您可以選擇IPv6為那些在 2021 年 1 月 12 日之前建立的資源啟用。當您IPv6針對特定資源啟用時，Lightsail 會自動為該資源指派IPv6位址；您無法自行選擇或指定IPv6位址。如需詳細資訊，請參閱[啟用或停用IPv6](#)。

您也可以建立IPv6唯一的執行個體。IPv6只有執行個體IPv6只能透過公開通訊，而且沒有公開IPv4位址。如需詳細資訊，請參閱 [為 Lightsail 執行個體設定僅限 IPv4 的網路](#)

您的執行個體IPv6位址會顯示在 Lightsail 主控台的下列區域中：

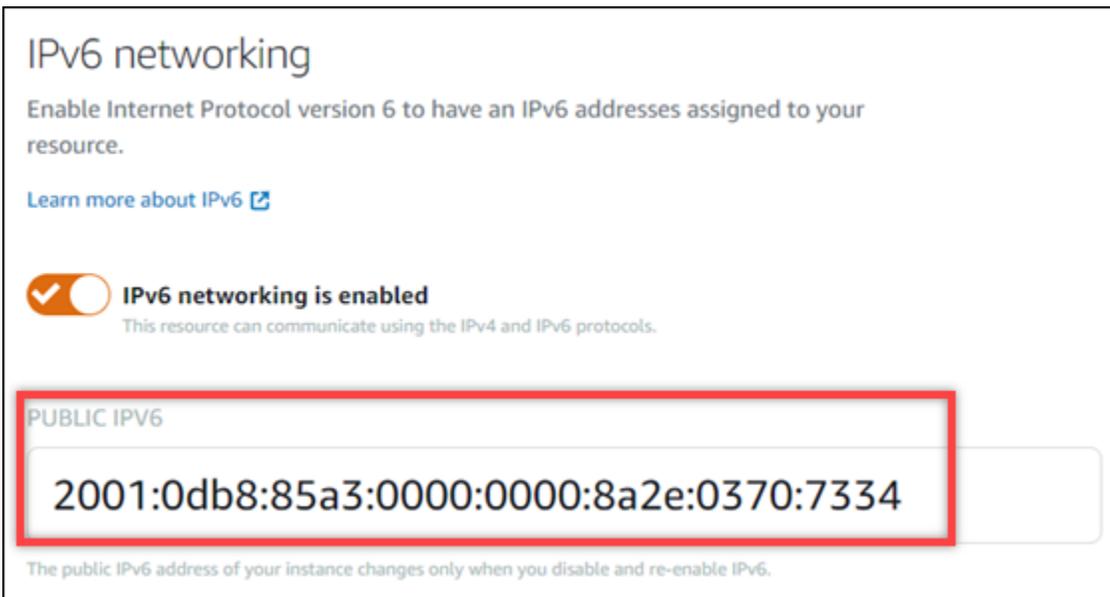
- 下列範例顯示 Lightsail 首頁上執行個體的IPv6位址。



- 下列範例會顯示資源管理頁面標頭區域中資源的IPv6位址。



- 下列範例顯示資源管理頁面之 [網路功能] 索引標籤上的資源IPv6位址。



啟用IPv6和使用資源時，請記住以下事項：

- 當您啟用資源時，或IPv4僅在啟用IPv6資源時，您的資源可以透過IPv4和IPv6（在雙堆疊模式下）進行通訊。

- 當您IPv6為資源啟用時，Lightsail 會自動為該資源指派IPv6位址；您無法自行選擇或指定IPv6位址。當您啟用IPv6資源時，它會開始接受透過通IPv6訊協定的網路流量。
- 當您停止並啟動執行個體時，執行個體的IPv6位址仍然存在。只有在您刪除執行個體或停用IPv6執行個體時，系統才會發佈此功能。執行上述任一動作之後，您都無法取回該IPv6位址。
- 指派給執行個體的所有IPv6位址都是公開的，可透過網際網路存取。沒有指派給執行個體的私人IPv6地址。
- IPv4和執行個體的IPv6位址彼此獨立；您必須為IPv4和分別設定執行個體防火牆規則IPv6。如需詳細資訊，請參閱[執行個體防火牆](#)。
- 並非所有 Lightsail 中可用的執行個體藍圖都會在啟用IPv6時IPv6自動設定。使用下列藍圖的執行個體在啟IPv6用後需要額外的設定步驟：
  - cPanel— 如需詳細資訊，請參閱[IPv6針對cPanel執行個體設定](#)。
  - Debian 8 — 有關更多信息，請參見[IPv6為 Debian 8 個實例配置](#)。
  - GitLab— 如需詳細資訊，請參閱[IPv6針對 GitLab執行個體設定](#)。
  - Nginx — 如需詳細資訊，請參閱針對 [Nginx 執行個體IPv6進行設定](#)。
  - Plesk — 如需詳細資訊，請參閱為 [Plesk 執行個體IPv6設定](#)。
  - Ubuntu 16 — 如需詳細資訊，請參閱[針對IPv6對 Ubuntu 16 執行個體進行設定](#)。

#### Note

PrestaShop 目前不支援IPv6地址。您可以IPv6為執行個體啟用，但 PrestaShop 軟體不會透過IPv6網路回應要求。

## Lightsail 中的靜態 IP 位址

靜態 IP 即為固定的公有 IP 地址，您可以將其指派及重新指派給執行個體或其他資源。如果您尚未設定靜態 IP 位址，則每次停止或重新啟動執行個體時，Lightsail 都會指派新的公用 IP 位址。

#### Important

如果您在沒有先建立靜態 IP 地址並將其連接至執行個體的情況下停止或重新啟動執行個體，則重新啟動執行個體時將導致 IP 地址遺失。您應該建立靜態 IP 地址並將其連接至執行個體，以確保您的執行個體永遠擁有相同的公有 IP 地址。如需詳細資訊，請參閱[建立靜態 IP 地址](#)。

## 目錄

- [建立靜態 IP 並將其附加至您的 Lightsail 執行個體](#)
- [刪除靜態 IP Lightsail](#)

## 建立靜態 IP 並將其附加至您的 Lightsail 執行個體

每當您停止並重新啟動執行個體時，連接到 Amazon Lightsail 執行個體的預設動態公有 IP 地址都會變更。建立靜態 IP 地址並將其連接到執行個體，以防止公有 IP 地址變更。稍後，當您將已註冊的網域名稱指向執行個體時，每次停止並重新啟動執行個體時，就不必更新網域的 DNS 記錄。您可以將一個靜態 IP 連接至一個執行個體。如需詳細資訊，請參閱[靜態 IP 地址](#)。

### 必要條件

您至少需要一個在 Lightsail 中執行的雙堆疊執行個體。若要建立執行個體，請參閱[建立執行個體](#)。

### 建立並指派靜態 IP 地址至執行個體

請依照下列步驟建立新的靜態 IP 位址，並將其附加至 Lightsail 中的執行個體。

1. 登入 Lightsail 主控台，網址為 <https://lightsail.aws.amazon.com/>。
2. 在 Lightsail 首頁上，選擇 [網路功能]。
3. 選擇 Create static IP (建立靜態 IP)。
4. 選取您 AWS 區域 要建立靜態 IP 的位置。

#### Note

靜態 IP 地址只能連接到相同區域中的執行個體。

5. 選擇您要附加靜態 IP 的 Lightsail 資源。
6. 輸入靜態 IP 的名稱。

#### 資源名稱：

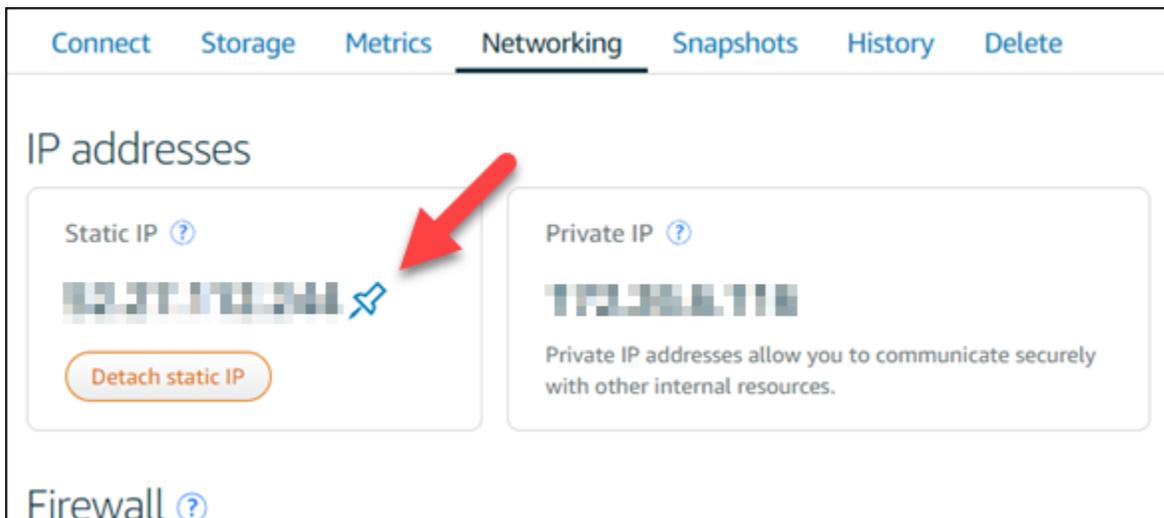
- 每個 Lightsail 帳戶 AWS 區域 中的每個項目都必須是唯一的。
- 必須包含 2 至 255 個字元。
- 開頭和結尾必須是英數字元或數字。
- 可以包含英數字元、數字、句點、破折號和底線。

7. 選擇 Create (建立)。

現在，當您移至首頁，您將看到您可管理的靜態 IP 地址。



同時，在執行個體管理頁面的 Networking (聯網) 索引標籤上，您將在公有 IP 地址旁看到藍色圖釘。這表示該 IP 地址現在為靜態。



如需詳細資訊，請參閱[公有 IP 地址和私有 IP 地址](#)。

## 刪除靜態 IP Lightsail

您最多可以在您的 Amazon Lightsail 帳戶 AWS 區域中為 IP 每個建立五個靜態。如果您刪除連接了靜態 IP 地址的執行個體，相應靜態 IP 地址仍會保留在您的帳戶中。如果您不再需要靜態 IP 位址，您可以使用 Lightsail 主控台或 AWS Command Line Interface (AWS CLI) 將其刪除。在本指南中，我們將向您展示如何從 Lightsail 帳戶刪除靜態 IP 位址。如需有關靜態的詳細資訊 IP 位址，請參閱[IP 位址](#)。

### **⚠ Important**

刪除靜態 IP 會完全移除您的 Lightsail 帳戶中的靜態 IP。使用該靜態 IP 地址的資源 (例如執行個體) 會受到影響。刪除靜態 IP 地址後，您就無法取回它。

## 使用主控台刪除靜態 IP

若要使用 Lightsail 主控台刪除靜態 IP，請完成下列程序。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁上，選擇 [網路功能]。
3. 在 [網路] 頁面上，選擇您要刪除的靜態 IP 位址旁邊的垂直省略符號 (⋮) 圖示，然後選擇 [刪除]。



## 使用刪除靜態 IP AWS CLI

完成下列程序，以使用 AWS CLI 刪除靜態 IP 地址。從您的 Lightsail 帳戶中刪除靜態 IP 的命令是 [release-static-ip](#)。當您建立靜態 IP 時，您實際上是在配置。因此，您實際上並非刪除靜態 IP，而是釋出。

### 先決條件

首先，如果您還沒有，則需要安裝 AWS CLI。若要進一步了解，請參閱 [安裝 AWS Command Line Interface](#)。請確定您設定 [AWS CLI](#)。

您將需要靜態 IP 的名稱以便將其釋出。您可以使用 `get-static-ips` AWS CLI 命令來取得。

1. 輸入以下命令：

```
aws lightsail get-static-ips
```

您應該會看到類似下列的輸出。

```
{
  "staticIps": [
    {
      "name": "Example-StaticIP",
      "resourceType": "StaticIp",
```

```
    "attachedTo": "MyInstance",
    "arn": "arn:aws:lightsail:us-east-2:123456789101:StaticIp/5282f35e-
c720-4e5a-1234-12345EXAMPLE",
    "isAttached": true,
    "ipAddress": "192.0.2.0",
    "createdAt": 1489750629.026,
    "location": {
      "availabilityZone": "all",
      "regionName": "us-east-2"
    }
  },
  {
    "name": "my-other-static-ip",
    "resourceType": "StaticIp",
    "arn": "arn:aws:lightsail:us-east-2:123456789101:StaticIp/
f5885e14-8984-49e5-1234-12345EXAMPLE",
    "isAttached": false,
    "ipAddress": "192.0.2.2",
    "createdAt": 1483653597.815,
    "location": {
      "availabilityZone": "all",
      "regionName": "us-east-2"
    }
  }
]
}
```

2. 選取您要釋出的靜態 IP 的 `name` (名稱) 值，然後將它記下來，以便在後續步驟中使用。

例如，您可以將該值複製至剪貼簿。

3. 輸入下列命令。

```
aws lightsail release-static-ip --static-ip-name StaticIpName
```

在命令中，替換 *StaticIpName* 使用您的靜態 IP 的名稱。

如果執行成功，您應該會看到類似下列的輸出。

```
{
  "operations": [
    {
      "status": "Succeeded",
```

```
    "resourceType": "StaticIp",
    "isTerminal": true,
    "statusChangedAt": 1489860944.19,
    "location": {
      "availabilityZone": "all",
      "regionName": "us-east-2"
    },
    "operationType": "ReleaseStaticIp",
    "resourceName": "Example-StaticIP",
    "id": "92a2f0d2-eef2-4e6f-1234-12345EXAMPLE",
    "createdAt": 1489860944.19
  }
]
```

## 啟用或停用 Lightsail 資源的雙堆疊網路

在 2021 年 1 月 12 日或之後建立的 Lightsail 雙堆疊執行個體、容器服務和負載平衡器，預設會啟用 IPv6。您可以選擇為在 2021 年 1 月 12 日之前建立的資源啟用 IPv6。在本指南中，我們將示範如何啟用或停用雙堆疊執行個體的 IPv6 網路。如需有關 IPv6 的詳細資訊，請參閱 [IP 地址](#)。

### 雙堆疊考量

IPv6 於 2021 年 1 月 12 日在 Lightsail 中推出；因此，您可能需要根據下列準則手動啟用或停用某些資源的 IPv6：

- 在 1 月 12 日之前建立的執行個體和負載平衡器會停用 IPv6，直到您啟用它為止。不過，在 1 月 12 日之後建立的執行個體和負載平衡器會在建立時啟用 IPv6。
- 在 1 月 12 日之前或之後建立的容器服務皆已啟用 IPv6。
- 您可以隨時為執行個體手動啟用或停用 IPv6，並可以隨時啟用負載平衡器。無法為容器服務停用 IPv6。

在您啟用和使用 IPv6 時，請謹記下列事項：

- 在您為資源啟用 IPv6 時，您的資源僅能透過 IPv4 或透過 IPv4 和 IPv6 (在雙堆疊模式下) 進行通訊。
- 在您為執行個體啟用 IPv6 時，Lightsail 會自動將 IPv6 地址指派給該執行個體；您無法自行選擇或指定 IPv6 地址。當您為容器服務或負載平衡器啟用 IPv6 時，該資源將開始接受透過 IPv6 的網際網路流量。

- 在您停止和啟動執行個體時，系統會持續保留執行個體的 IPv6 地址。只有在刪除執行個體或停用執行個體的 IPv6 時才會釋放該地址。在執行以上任一動作後，您便無法取回 IPv6 地址。
- 所有指派給執行個體的 IPv6 地址皆為公有，且可以透過網際網路存取。沒有指派給執行個體的私有 IPv6 地址。
- 執行個體的 IPv4 和 IPv6 地址彼此互相獨立；您必須分別為 IPv4 和 IPv6 設定執行個體防火牆規則。如需詳細資訊，請參閱[執行個體防火牆](#)。
- 並非所有 Lightsail 中可用的執行個體藍圖都會在啟用 IPv6 時自動設定 IPv6。為執行個體啟用 IPv6 後，使用以下藍圖的執行個體會需要其他設定步驟：
  - cPanel - 如需詳細資訊，請參閱[設定 cPanel 執行個體的 IPv6](#)。
  - Debian 8 - 如需詳細資訊，請參閱[設定 Debian 8 執行個體的 IPv6](#)。
  - GitLab— 如需詳細資訊，請參閱[針對 GitLab 執行個體設定 IPv6](#)。
  - Nginx - 如需詳細資訊，請參閱[設定 Nginx 執行個體的 IPv6](#)。
  - Plesk - 如需詳細資訊，請參閱[設定 Plesk 執行個體的 IPv6](#)。
  - Ubuntu 16 - 如需詳細資訊，請參閱[設定 Ubuntu 16 執行個體的 IPv6](#)。

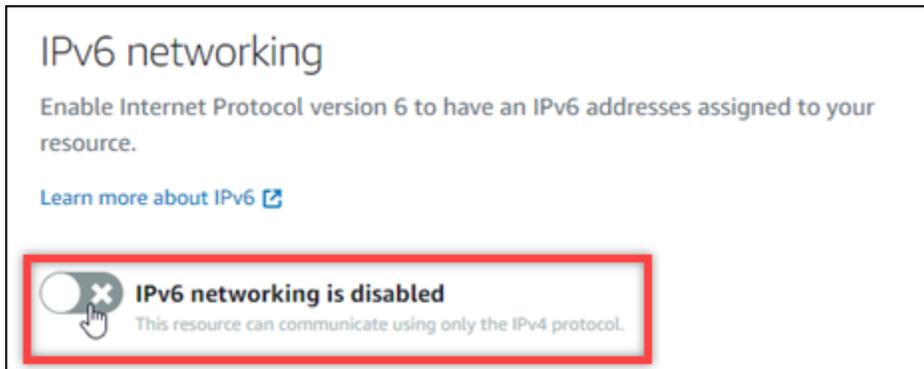
## 主題

- [啟用 Lightsail 資源的 IPv6 網路](#)
- [停用 Lightsail 資源的 IPv6 網路](#)

## 啟用 Lightsail 資源的 IPv6 網路

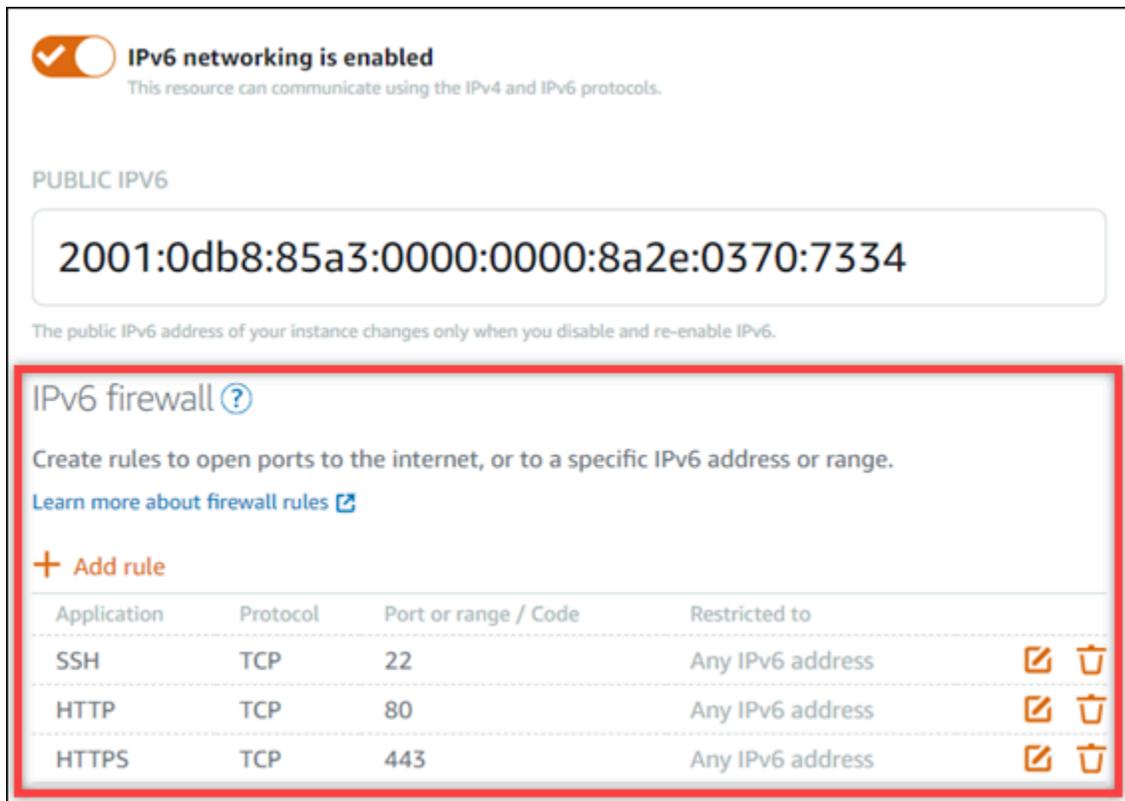
完成下列程序，以針對 IPv6 對執行個體、CDN 分配和負載平衡器啟用。

1. 登入主 [Lightsail 台](#)。
2. 根據您要啟用的資源，完成下列其中一個步驟 IPv6：
  - 若要 IPv6 為實體啟用，請選擇 Lightsail 首頁上的「實體」索引標籤，然後選擇要啟用 IPv6 的實體名稱。
  - 若要啟用 IPv6 用 CDN 分發或負載平衡器，請選擇 Lightsail 首頁上的 [網路] 索引標籤，然後選擇要啟用 IPv6 的 CDN 分發或負載平衡器的名稱。
3. 選擇資源管理頁面上的 Networking (聯網) 索引標籤。
4. 在頁面的「IPv6 網路功能」段落中，選擇要為資源啟用 IPv6 的切換開關。



IPv6為資源啟用後，請注意下列項目：

- 如果您啟IPv6用CDN分發或負載平衡器，則該資源會開始接受IPv6流量。如果您IPv6針對執行個體啟用，則會為執行個體指派IPv6位址，而IPv6防火牆就會變成可用，如下列範例所示。



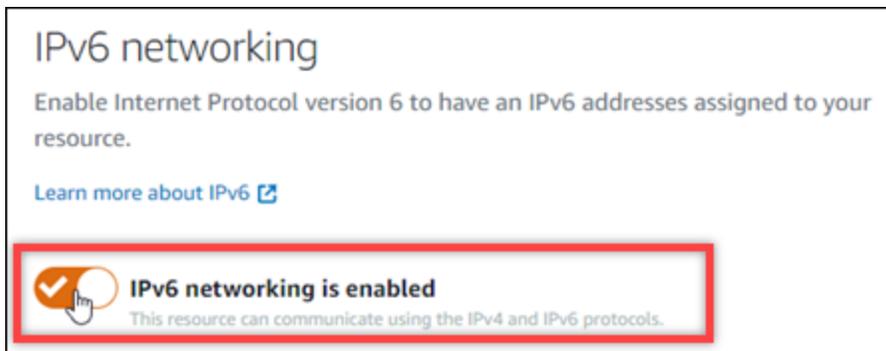
- 啟用後，使用下列藍圖的執行個體需要額外的步驟，IPv6才能確保執行個體知道其新IPv6位址：
  - cPanel— 如需詳細資訊，請參閱[IPv6針對cPanel執行個體設定](#)。
  - Debian 8 — 有關更多信息，請參見[IPv6為 Debian 8 個實例配置](#)。
  - GitLab— 如需詳細資訊，請參閱[IPv6針對 GitLab執行個體設定](#)。
  - Nginx — 如需詳細資訊，請參閱針對 [Nginx 執行個體IPv6進行設定](#)。

- Plesk — 如需詳細資訊，請參閱針對 [Plesk 執行個體IPv6進行設定](#)。
- Ubuntu 16 — 如需詳細資訊，請參閱[針IPv6對 Ubuntu 16 執行個體](#)進行設定。
- 如果您有已註冊的網域名稱，將流量導向您的執行個體、容器服務、CDN散發或負載平衡器，請務必在網域中建立IPv6位址記錄 (AAAA)，以將IPv6流量路由至您的資源。DNS

## 停用 Lightsail 資源的IPv6網路

請完成下列程序以停IPv6用執行個體、CDN分發和負載平衡器。

1. 登入主 [Lightsail 台](#)。
2. 根據您要停用的資源，完成下列其中一個步驟IPv6：
  - 若要停IPv6用某個實體，請選擇 Lightsail 首頁上的「實體」索引標籤，然後選擇要停用IPv6的實體名稱。
  - 若要停IPv6用CDN分發或負載平衡器，請選擇 Lightsail 首頁上的 [網路] 索引標籤，然後選擇要停用IPv6的CDN分發或負載平衡器的名稱。
3. 選擇資源管理頁面上的 Networking (聯網) 索引標籤。
4. 在頁面的 [IPv6網路功能] 段落中，選擇要停用資源IPv6的切換開關。



## 為 Lightsail 執行個體設定僅限 IPv4 的網路

Lightsail 執行個體支援兩種類型的網路：雙堆疊網路 (IPv4 和 IPv6) 和僅限 IPv4 的網路功能。透過雙堆疊網路，您的執行個體會被指派一個公用 IPv4 和一個公用 IPv6 位址；您可以視需要啟用或停用 IPv6。

使用僅限 IPv6 的網路，您的執行個體會被指派公用 IPv6 位址，而且不支援公用 IPv4 流量。並非所 Lightsail 藍圖都與 IPv6 相容。若要瞭解哪些藍圖僅支援 IPv6，請參閱 [相容藍圖](#)

**⚠ Warning**

Amazon Lightsail 有終端節點目前不支援 IPv6。如需詳細資訊，請參閱 Amazon VPC 使用者指南中的 [支援 IPv6 的服務](#)。

如果您不需要公用 IPv4 位址，請使用僅限 IPv6 的網路。但首先，請確定您的區域網路、電腦、裝置和使用者可以使用 IPv6 進行通訊。如需詳細資訊，請參閱中的 IPv6 可達性。[確認 Lightsail 執行個體的 IPv6 連線能力](#)若要變更現有執行個體的網路類型，請參閱[在 Lightsail 中將執行個體網路類型切換為 IPv6 或雙堆疊](#)。

**主題**

- [在 Lightsail 中將執行個體網路類型切換為 IPv6 或雙堆疊](#)
- [相容藍圖](#)

**在 Lightsail 中將執行個體網路類型切換為 IPv6 或雙堆疊**

執行個體的網路類型會決定執行個體透過網際網路通訊所使用的通訊協定。建立執行個體時，您可以選擇雙堆疊或 IPv6 僅網路。您也可以將現有執行個體的網路類型從雙堆疊變更為 IPv6-only，反之亦然。使用引導式、step-by-step 工作流程或完成個別步驟來變更網路類型。

透過引導式工作流程，您的執行個體會設定新的網路類型時繼續執行。使用此選項可讓您的執行個體在變更時仍可透過網際網路存取。但首先，請確保您的本地網路，計算機，設備和最終用戶可以使用 IPv6。如需詳細資訊，請參閱[確認 Lightsail 執行個體的 IPv6 連線能力](#)。

透過各個步驟，您將為執行個體建立快照，然後從快照建立新的執行個體。您可以在建立新執行個體時選擇不同的網路類型。使用此選項可在變更其他執行個體的組態之前驗證 IPv6 相容性。在開始之前，我們建議您先檢閱[IPv6 僅考慮因素](#)。

**IPv6 僅考慮因素**

請檢閱下列注意事項：

- 您的執行個體方案會在網路類型有所變更時變更。如需詳細資訊，請參閱 AWS 運算部落格 [上的 Amazon Lightsail 宣布 IPv6 執行個體套裝軟體和定價更新](#)。
- 目前 IPv6 前不支援 Amazon Lightsail 公有終端節點。如需詳細資訊，請參閱 Amazon VPC 使用者指南 IPv6 中的 [支援服務](#)。

- 您的執行個體將透過公開通訊IPv6。它不支持傳入或傳出的公共IPv4流量。它將收到一個私人IPv4地址，以便與您的 Lightsail 帳戶中的其他資源進行通訊。如需詳細資訊，請參閱[檢視和管理資源的 Lightsail 址](#)。
- IPv6只有執行個體無法設定為 Lightsail 內容傳遞網路 (CDN) 散發的來源。
- 您IPv6只能將執行個體新增至 Lightsail 負載平衡器。
- 當您變更網路類型時，執行個體資料傳輸計劃的限額將會繼續保留。它不會重置。
- 確認您的本機裝置、網路和網際網路服務供應商 (ISP) 是否IPv6相容。如需詳細資訊，請參閱[確認 Lightsail 執行個體的 IPv6 連線能力](#)。

## 選項：引導式工作流

### 使用精靈設定執行個體網路類型

1. 在執行個體管理頁面的資訊面板上，選擇 [變更網路類型]。
2. 針對 [選取網路類型]，選取 [雙堆疊] 或 [IPv6僅]。檢閱所選選項下方反白顯示的資訊，然後選擇「下一步」。
3. 對於 Review 資源，請檢閱將對目前與執行個體相關聯的資源所做的變更。資源可以是靜態 IP 位址，也可以是 Lightsail 負載平衡器。如果您的執行個體沒有附加資源，則不會進行任何變更。在您完成下一個步驟的工作流程之前，資源變更才會發生。選擇 Next (下一步) 繼續。
4. 在 [確認變更] 中，檢閱新執行個體網路類型、定價和資源變更，然後選擇 [確認變更]。我們開始設定您的 Lightsail 資源。
5. (選擇性) 在工作流程完成後更新執行個體組態。例如，將靜態 IP 附加到您的執行個體，或更新的 DNS IPv4 A AAAA 記錄和記錄IPv6。如需後續步驟，請參閱[the section called “後續步驟”](#)閱本指南的章節。

## 選項：個別步驟

### 完成個別步驟以設定執行個體網路類型

1. 在執行個體管理頁面的 [快照] 索引標籤上，選擇 [建立快照]。如需詳細資訊，請參閱下列其中一個主題：
  - [使用快照備份 Linux/UniLightsail 執行個體](#)
  - [建立您的視窗伺服器執行個體的快照](#)
2. 為快照命名，然後選擇「建立」。

3. 在快照動作功能表 () 中，選擇 [建立新的執行個體]。如需詳細資訊，請參閱[從快照建立 Lightsail 執行個體](#)。
4. 在 [選取網路類型] 區段中，選擇 [雙堆疊] 或 [IPv6僅]。
5. 檢閱其餘選項並選擇 [建立執行個體]。您的新執行個體已建立完成。
6. (選擇性) 在工作流程完成後更新執行個體組態。例如，將靜態 IP 附加到您的執行個體，或更新的 DNS IPv4 A AAAA 記錄和記錄IPv6。如需後續步驟，請參閱[the section called “後續步驟”](#)閱本指南的章節。

## 後續步驟

在變更執行個體的聯網類型之後，您還可以執行一些其他工作：

- ( IPv6只 ) 確保您的應用程序和用戶能夠通信IPv6。如需詳細資訊，請參閱[確認 Lightsail 執行個體的 IPv6 連線能力](#)。
- (雙堆疊) 將靜態 IP 位址附加至您的執行個體。如需詳細資訊，請參閱[將靜態 IP 連接至執行個體](#)。
- (雙堆疊) 將您的執行個體設定為 Lightsail 發行版本的來源。如需詳細資訊，請參閱 [Lightsail 中的 CDN發行版](#)。
- (兩者) 新增或更新執行個體的防火牆設定。如需詳細資訊，請參閱 [Lightsail 中的執行個體防火牆](#)。
- (兩者) 新增或更新 DNS A 記錄IPv4，以及的AAAA記錄IPv6。如需詳細資訊，請參閱[將網域指向執行個體](#)。
- (兩者) 將您的執行個體新增至 Lightsail 負載平衡器。如需詳細資訊，請參閱 [Lightsail 中的負載平衡器](#)。

## 相容藍圖

下列 Lightsail 藍圖與僅限 IPv6 的執行個體計劃相容

- [Windows Server 2022](#)
- [Windows Server 2019](#)
- [Windows Server 2016](#)
- [Amazon Linux 2023](#)
- [Amazon Linux 2](#)
- [AlmaLinux OS 9](#)

- [CentOS Stream 9](#)
- [Debian 11, and 12](#)
- [FreeBSD 13](#)
- [Ubuntu 20, and 22](#)
- [SQL Server 2022 Express](#)
- [SQL Server 2019 Express](#)
- [SQL Server 2016 Express](#)
- [LAMP stack \(PHP 8\) packaged by Bitnami](#)
- [MEAN stack packaged by Bitnami](#)
- [Redmine packaged by Bitnami](#)

如需有關 Lightsail 藍圖的詳細資訊，請參閱 [the section called “Blueprints \(藍圖\)”](#)

## Lightsail 的區域和可用區域

在 Amazon Lightsail 中建立資源時，請在最接近使用者的資源中建立資源。AWS 區域 舉例來說，如果您的部落格流量主要是來自瑞士，則可選擇 Frankfurt (法蘭克福) 或 Paris (巴黎)。

### Note

DNS區域是全球資源。只能在美國東部 (維吉尼亞北部) (us-east-1) 區域中建立它們，但它們可以參考任何 AWS 區域中的任何執行個體。

Lightsail 可用於以下 AWS 區域產品：

- 美國東部 (俄亥俄) (us-east-2)
- 美國東部 (維吉尼亞北部) (us-east-1)
- 美國西部 (奧勒岡) (us-west-2)
- 亞太區域 (孟買) (ap-south-1)
- 亞太區域 (首爾) (ap-northeast-2)
- 亞太區域 (新加坡) (ap-southeast-1)
- 亞太區域 (雪梨) (ap-southeast-2)

- 亞太區域 (東京) (ap-northeast-1)
- 加拿大 (中部) (ca-central-1)
- 歐洲 (法蘭克福) (eu-central-1)
- 歐洲 (愛爾蘭) (eu-west-1)
- 歐洲 (倫敦) (eu-west-2)
- 歐洲 (巴黎) (eu-west-3)
- 歐洲 (斯德哥爾摩) (eu-north-1)



## SSH按鍵和 Lightsail 區域

在 Lightsail 中，只要您在中建立執行個體 AWS 區域，我們就會在該區域中建立預設SSH金鑰。此預設金鑰可用於僅連接至該特定區域的執行個體。若要在具備執行個體的所有區域中使用相同金鑰，則請建立您自己的金鑰對並將其上傳至每個區域。或者，您也能在這些區域中上傳現有的金鑰對。

如需詳細資訊，請參閱[SSH金鑰配對](#)。

## 使用 Lightsail 區域的秘訣

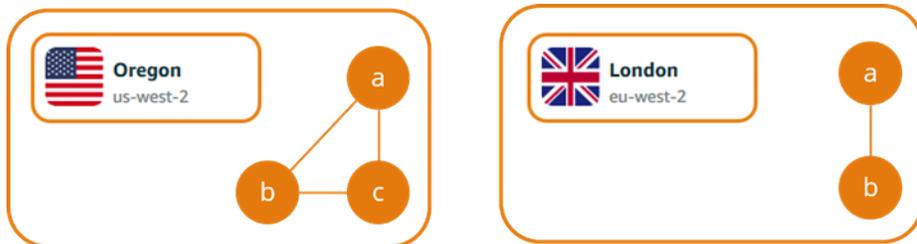
每個都 AWS 區域 被設計為完全隔離從其他 AWS 區域。如此可達到最高的容錯能力與穩定性。

系統會透過公有網際網路在各區域間進行通訊。因此，您應該使用適當的加密方法來保護資料。請注意，跨區域傳輸資料會產生費用。如需詳細資訊，請參閱 [Amazon EC2 定價-資料傳輸](#)。

當您使用 AWS Command Line Interface (AWS CLI) 或作API業使用 Lightsail 執行個體時，必須指定其地區端點。使用指 AWS CLI 令中的 `--region` 選項，並指定 `us-east-1` 以傳回有關DNS區域和網路資源的資訊。如需有關使用選 AWS CLI `--region` 項的詳細資訊，請參閱AWS CLI 參考中的 [一般選項](#)。

## Lightsail 可用區域

可用區域即為資料中心的集合，其可在不同的獨立實體基礎設施上運作。同時，可用區域也具備高度可靠的設計。可用區域之間不會共用常見的故障點，如發電機和冷卻設備等。可用區域各自獨立，即使發生火災、風災或水災等極端氣候災難，也只會影響發生此災難的單一可用區域。



每個區域都 AWS 區域 有多個隔離的可用區域，這些可用區域在區域名稱 (us-east-2a) 後面以字母表示。您一次只能在一個可用區域中建立 Lightsail 執行個體。建立執行個體的期間，您可能看不到所有可用區域。如果完全沒有看見可用區域清單，請確保您在先前的步驟中已選取一個區域。

### 可用區域和您的 Lightsail 程式

只要在不同的可用區域中啟動執行個體，就能避免應用程式在單一位置發生故障情形。

若要建立多個可用區域都能使用的執行個體，請先[建立執行個體的快照](#)。接著，在您[從建立的快照建立新執行個體](#)時，選擇另一個可用區域。

如需詳細資訊，請參閱 Amazon EC2 使用者指南中的 AWS 區域 和可用 [區域](#)。

## 使用對等互連將 Lightsail 資源 Connect 至 AWS 服VPC務

透過 Lightsail，您可以透過虛擬私有雲端 (VPC) 對等連線連線至 AWS 資源，例如 Amazon 資RDS料庫。A VPC 是專用於您 AWS 帳戶的虛擬網路。您在 Lightsail 中創建的所有內容都在一個內部VPC，您可以將 Lightsail 連接VPC到 Amazon。VPC

某些 AWS 資源 (例如 Amazon S3 CloudFront、Amazon 和亞馬遜 DynamoDB) 不需要啟用VPC對等互連。

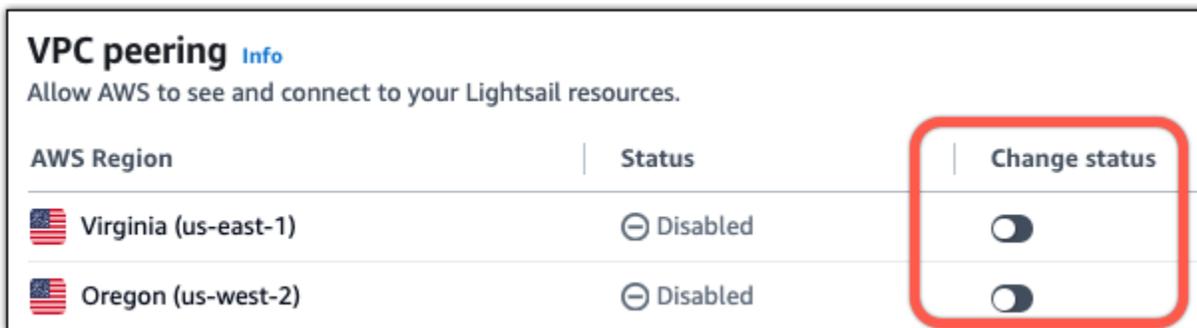
#### Note

要在 Lightsail 中啟用VPC對等互連，您需要有一個默認的 Amazon。VPC如果你沒有一個默認的 AmazonVPC，你可以創建一個。若要進一步了解，請參閱 [Amazon VPC 使用者指南 VPC中的建立預設值](#)。

由於 AWS 區域是彼此隔離的，因此在 VPC 您建立它的區域中也會隔離出來。您必須在擁有 Lightsail 資源的每個區域啟用 VPC 對等互連功能。

擁有默認 Amazon 後 VPC，請按照以下說明將您的 Lightsail VPC 與 Amazon VPC 對等。

1. 在 [Lightsail 主控台](#) 中，在頂端導覽功能表上選擇您的使用者名稱。
2. 從下拉式清單中選擇 Account (帳戶)。
3. 選擇 Advanced (進階) 索引標籤。
4. 切換您要啟用 VPC 對等互連的 AWS 區域 位置旁的狀態。



如果對等連線失敗，請嘗試再次啟用 VPC 對等互連。如果它不起作用，請聯繫 [AWS Support](#)。

如果對等連線要求成功，則會在您的 AWS 帳戶中建立對等連線。轉到 [Amazon VPC 儀表板](#)，然後在導航窗格中選擇對等連接以查看所建立的對等連接。

有關 Amazon 的更多信息 VPC，請參閱 Amazon VPC 用戶指南中的 [VPC 和子網](#)。

## SSL/Light TLS sail 中的證書

Amazon Lightsail 使用 SSL/TLS 憑證來驗證可與 Lightsail 負載平衡器、內容交付網路 ( ) 分發和容器服務搭配使用的自訂 (已註冊 CDN) 網域。將經過驗證的憑證附加至其中一個 Lightsail 資源後，透過網域路由至該資源的流量會使用超文字傳輸通訊協定 Secure ( ) HTTPS 加密。

您可以在 Amazon Lightsail 中建立傳輸層安全性 (TLS) 憑證，為要與 Lightsail 負載平衡器內容交付網路分發和容器服務搭配使用的自訂 (已註冊) 網域啟用加密的 Web 流量。TLS 是安全通訊端層 (SSL) 的更新、更安全的版本。在整個 Lightsail 文件和主控台中，您會看到我們將其稱為 SSL/TLS。

### ⚠ Important

您可以附加至負載平衡器、CDN分發和容器服務的 Lightsail 憑證是由 AWS Certificate Manager (ACM) 服務所核發。自 2022 年 10 月 11 日起，透過 Lightsail 為您的負載平衡器、CDN分發器和容器服務取得的任何公開憑證，都將從管理的多個中繼憑證授權單位 (ICAs) 或下屬CAs之一發行。ACM如需詳細資訊，請參閱 [Amazon 在AWS安全部落格中介紹動態中繼憑證授權單位](#)。

## 為什麼要使用 HTTPS ?

首先，最重要的部分就是安全考量。HTTPS提供額外的安全層，因為它會用TLS來移動資料。HTTPSWeb 伺服器 and 用戶端瀏覽器之間的加密是機密的，因為它們是唯一可以解密流量的兩個實體。HTTPS連接也更安全，因為客戶端與伺服器交換的數據不能被另一方修改。

除了上面提到的安全優勢外，還有其他原因可以使用HTTPSHTTP。舉例來說，2014 年時，Google 開始提高安全網站在搜尋結果中的排名。換句話說，與僅使用的網站相比，使用的HTTPS排名更接近搜索結果頂部的網站HTTP (所有其他事情都是相同的)。

### [進一步瞭解HTTPS解排名訊號](#)

## 程序概觀

使用 Lightsail 憑證的程序很簡單。包括下列步驟：

1. 建立可使用 Lightsail 憑證的 Lightsail 資源，例如負載平衡器、CDN散發或容器服務。
2. 使用 Lightsail 為您的網域建立憑證。
3. 在您DNS的網域中新增標準名稱 (CNAME) 記錄來驗證憑證
4. 將經過驗證的憑證附加至您的 Lightsail 資源。
5. 修改您DNS的網域，將流量路由至您的 Lightsail 資源。



憑證附加至資源後，會使用加密透過網域路由至該資源的流量HTTPS。

## 在您的分發或容器服務中使用SSL/TLS憑證

HTTPS在 Lightsail 配送和容器服務上是必需的。當您建立這些資源時，HTTPS預設會針對資源的預設網域啟用 (例如，<https://123456abcdef.cloudfront.net/>針對散佈或<https://container-service-1.123456abcdef.us-west-2.cs.amazonlightsail.com/>容器服務)。如果您想要將註冊的網域名稱 (例如example.com) 用於分發或容器服務，您必須建立 LightsailSSL/TLS憑證、使用您的網域名稱驗證，並在資源上啟用自訂網域。啟用分發或容器服務上的自訂網域也會將網域經驗證的憑證連接至資源。

您可以通過以下鏈接開始啟用自定義域和HTTPS分發。

- [為您的發行版建立SSL/TLS憑證](#)
- [驗證SSL/您的發行版TLS憑證](#)
- [檢視SSL/TLS您的發佈的證書](#)
- [啟用分發的自訂域](#)
- [將域指向分發](#)

如需有關分發的詳細資訊，請參閱[內容交付網路分發](#)。

您可以按照以下鏈接開始啟用自定義域和HTTPS容器服務。

- [建立容器服務SSL/TLS憑證](#)
- [驗證容器服務SSL/TLS憑證](#)
- [啟用和管理自訂域](#)

如需有關容器服務的詳細資訊，請參閱[容器服務](#)。

## 搭配負載平衡器使用SSL/TLS憑證

當您建立 Lightsail 負載平衡器時，預設會開啟連接埠 80 以處理一般HTTP流量。若要透過連接埠 443 啟用HTTPS流量，您必須建立SSL/TLS憑證、使用您的網域名稱進行驗證，然後將其附加至負載平衡器。

每個負載平衡器最多可以建立兩個SSL/TLS憑證。每個負載平衡器一次只能使用一個憑證。如果您從負載平衡器刪除有效的使用中憑證，則在您附加另一個有效憑證之前，負載平衡器將無法處理指定網域的HTTPS流量。

您可以按照以下連結開始 HTTPS 在負載平衡器上啟用。

- [建立負載平衡器並將其與執行個體附接](#)
- [建立 SSL/TLS 憑證](#)
- [驗證網域所有權](#)
- [附加已驗證的憑證以啟用 HTTPS](#)

如需負載平衡器的詳細資訊，請參閱 [負載平衡器](#)。

## 為安全的容器服務網域建立 SSL/TLS 憑證

您可以為 Lightsail 容器服務建立 Amazon Lightsail TLS/SSL 憑證。建立憑證時，請指定憑證的主要和替代網域名稱。當您為容器服務啟用自訂網域並選擇憑證時，可以從憑證中選擇最多四個網域，這些網域將新增為容器服務的自訂網域。在您更新網域的 DNS 記錄，將流量引導至容器服務之後，服務就會接受流量並使用 HTTPS 提供內容。您可以建立的憑證數量有配額。如需詳細資訊，請參閱 [Lightsail 服務配額](#)。

如需有關 SSL/TLS 憑證的詳細資訊，請參閱 [容器服務憑證](#)。

### 必要條件

開始之前，您需要建立 Lightsail 容器服務。如需詳細資訊，請參閱 [建立容器服務](#) 和 [容器服務](#)。

### 建立容器服務的 SSL/TLS 憑證

請完成下列程序，為容器服務建立 SSL/TLS 憑證。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁，選擇 Containers (容器) 索引標籤。
3. 選擇要建立憑證之容器服務的名稱。
4. 在容器服務管理頁面上，選擇 Custom domains (自訂網域) 索引標籤。
5. 向下捲動至頁面的 Attached certificates (連接的憑證) 區段。

您的所有憑證都會列在頁面的「附加憑證」區段下，包括為其他 Lightsail 資源建立的憑證，以及使用中且未使用的憑證。

6. 選擇 Create certificate (建立憑證)。

7. 在 Certificate name (憑證名稱) 文字方塊中輸入唯一名稱，以識別您的憑證。然後選擇 Continue (繼續)。
8. 將您要搭配憑證使用的主要網域名稱 (例如 example.com)，輸入 Specify up to 10 domains or subdomains (指定最多 10 個網域或子網域) 欄位中。
9. (選用) 將其他網域名稱 (例如 www.example.com)，輸入 Specify up to 10 domains or subdomains (指定最多 10 個網域或子網域) 欄位中。

您可新增最多 9 個替代網域至憑證。在您啟用自訂網域並選取服務的憑證之後，容器服務可使用最多 4 個憑證的網域。

10. 選擇 Create certificate (建立憑證)。

系統會提交您的憑證請求，新憑證的狀態會變更為 Attempting to validate your certificate (正在嘗試驗證您的憑證)。在此期間，Lightsail 會嘗試將憑證的驗證記錄新增至主要網域的 DNS。一段時間後，狀態會變更為 Valid (有效)。

如果自動驗證失敗，您必須使用您的網域驗證憑證，才能搭配容器服務使用。如需詳細資訊，請參閱 [驗證容器服務 SSL/TLS 憑證](#)。

## 主題

- [驗證 Lightsail 容器服務的 SSL/TLS 憑證](#)
- [檢視適用於 Lightsail 容器服務的 SSL/TLS 憑證](#)

## 驗證 Lightsail 容器服務的 SSL/TLS 憑證

Amazon Lightsail SSL/TLS 憑證在建立之後，您必須先經過驗證，然後才能將其與 Lightsail 容器服務搭配使用。提交憑證請求後，新憑證的狀態會變更為 Attempting to validate your certificate (正在嘗試驗證您的憑證)。在此期間，Lightsail 會嘗試將憑證的驗證記錄新增至您為憑證指定之網域名稱的 DNS。一段時間後，狀態會變更為 Valid (有效) 或 Validation timed out (驗證逾時)。

如果自動驗證失敗，您必須確認控制了要建立憑證時，為該憑證指定的所有網域名稱。若要執行此操作，您可以將正式名稱 (CNAME) 記錄新增至憑證上指定的每個網域的 DNS 區域。您必須新增的記錄列於憑證的 Validation details (驗證詳細資訊) 區段。

在本指南中，我們提供了使用 Lightsail DNS 區域手動驗證憑證的程序。使用不同的 DNS 主機供應商 (例如 Domain.com 或 GoDaddy) 驗證憑證的程序可能類似。如需有關 DNS 區域 Lightsail 細資訊，請參閱 [DNS](#)。

如需有關 SSL/TLS 憑證的詳細資訊，請參閱 [SSL/TLS 憑證](#)。

## 先決條件

開始之前，您需要為容器服務建立 SSL/TLS 憑證。如需詳細資訊，請參閱 [為容器服務建立 SSL/TLS 憑證](#)。

## 取得 CNAME 記錄值以驗證憑證

請完成下列程序，以取得必須新增至網域以驗證憑證的 CNAME 記錄。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁，選擇 Containers (容器) 索引標籤。
3. 選擇要建立憑證之容器服務的名稱。
4. 在容器服務管理頁面上，選擇 Custom domains (自訂網域) 索引標籤。
5. 向下捲動至頁面的 Attached certificates (連接的憑證) 區段。

您的所有憑證都會列在頁面的「附加憑證」區段下，包括為其他 Lightsail 資源建立的憑證，以及等待驗證的憑證。

6. 尋找您要驗證的憑證，展開 Validation details (驗證詳細資訊)，並記下您必須為列出的每個網域新增之 CNAME 記錄的 Name (名稱) 和 Value (值)。

您必須完全依照列出的方式新增這些記錄。建議您複製這些值並貼至稍後可參考的文字檔案中。如需詳細資訊，請參閱本指南的下列 [將 CNAME 記錄新增至網域的 DNS 區域](#) 章節。

## 新增 CNAME 記錄至網域的 DNS 區域

請完成以下程序，將 CNAME 記錄新增至網域的 DNS 區域。

1. 選擇 Lightsail 首頁上的 Domains & DNS (網域和 DNS) 索引標籤。
2. 在頁面的 DNS zones (DNS 區域) 區段下，選擇您要新增 CNAME 記錄以驗證憑證的網域名稱。
3. 選擇 DNS records (DNS 記錄) 索引標籤。
4. 在 DNS 記錄管理頁面上，選擇 Add record (新增記錄)。
5. 在 Record type (記錄類型) 下拉式選單中，選擇 CNAME。
6. 在 Record name (記錄名稱) 文字方塊中，輸入您從憑證取得之 CNAME 記錄的 Name (名稱) 值。

Lightsail 主控台會預先填入您網域的頂點部分。例如，如果您要新增 `www.example.com` 子網域，則只需在文字方塊中輸入 `www`，當您儲存記錄時，Lightsail 會新增 `.example.com` 部分。

7. 在 Route traffic to (將流量路由至) 文字方塊中，輸入您從憑證取得之 CNAME 記錄的 Value (值) 部分。
8. 確認您輸入的值與您要驗證的憑證上列出的值完全相同。
9. 選擇儲存圖示，將記錄儲存到 DNS 區域。

重複這些步驟，為憑證上需要驗證的網域新增其他 CNAME 記錄。允許透過網際網路 DNS 傳播的變更時間。幾分鐘後，憑證的狀態應該變更為 Valid (有效)。如需詳細資訊，請參閱本指南下列[檢視憑證的狀態](#)章節。

## 檢視憑證的狀態

請完成下列程序，以檢視 SSL/TLS 憑證的狀態。

1. 在 Lightsail 首頁，選擇 Containers (容器) 索引標籤。
2. 選擇要檢視憑證狀態之容器服務的名稱。
3. 在容器服務管理頁面上，選擇 Custom domains (自訂網域) 索引標籤。
4. 向下捲動至頁面的 Attached certificates (連接的憑證) 區段。

所有憑證都會列在頁面 Attached certificates (連接的憑證) 區段下，包括狀態為 Pending validation (待驗證) 和 Valid (有效) 的憑證。

### Note

如果您在驗證憑證時保持 Custom domains (自訂網域) 頁面開啟，您可能必須重新整理才能查看憑證的更新狀態。

Valid (有效) 狀態確認您已使用新增至網域的 CNAME 記錄成功驗證憑證。選擇 Details (詳細資訊)，檢視憑證的重要日期、加密詳細資訊、身分識別和驗證記錄。您的憑證自驗證之日起 13 個月內有效，此後 Lightsail 會嘗試自動重新驗證這些憑證。請勿刪除您新增至網域的 CNAME 記錄，因為在列出的 Valid until (有效期) 日期重新驗證憑證時需要這些記錄。

驗證 SSL/TLS 憑證之後，您應該啟用容器服務的自訂網域，以便在服務上使用憑證的網域名稱。如需詳細資訊，請參閱[啟用和管理容器服務的自訂域](#)。

## 檢視適用於 Lightsail 容器服務的 SSL/TLS 憑證

您可以檢視您為 Lightsail 容器服務建立的 Amazon Lightsail SSL/TLS 憑證。您可以在 Lightsail 主控台中存取任何容器服務的管理頁面來完成此操作。

如需有關 SSL/TLS 憑證的詳細資訊，請參閱 [SSL/TLS 憑證](#)。

### 必要條件

開始之前，您需要建立 Lightsail 容器服務。如需詳細資訊，請參閱 [建立 Amazon Lightsail 容器服務](#) 和 [容器服務](#)。

您還應該為容器服務建立 SSL/TLS 憑證。如需詳細資訊，請參閱 [建立容器服務 SSL/TLS 憑證](#)。

### 檢視容器服務的 SSL/TLS 憑證

請完成下列程序，以檢視容器服務的 SSL/TLS 憑證。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁，選擇 Containers (容器) 索引標籤。
3. 選擇容器服務的名稱。

無論您選擇的容器服務為何，您都可以檢視所有憑證。

4. 在容器服務管理頁面上，選擇 Custom domains (自訂網域) 索引標籤。
5. 向下捲動至頁面的 Attached certificates (連接的憑證) 區段。

您的所有憑證都會列在頁面的 Attached certificates (連接的憑證) 區段。選擇 Details (詳細資訊)，檢視憑證的重要日期、加密詳細資訊、身分識別和網域。選擇 Validation details (驗證詳細資訊)，檢視憑證的驗證記錄。您的憑證自建立之日起 13 個月內有效，此後 Lightsail 會嘗試自動重新驗證這些憑證。請勿刪除您新增至網域的 CNAME 記錄，因為在列出的 Valid until (有效期) 日期重新驗證憑證時需要這些記錄。

在您擁有有效的 SSL/TLS 憑證與容器服務搭配使用之後，您應該啟用自訂網域，以便您可以在服務上使用憑證的網域名稱。如需詳細資訊，請參閱 [啟用和管理自訂域](#)。

## 使用 SSL/TLS 憑證安全 Lightsail CDN 散佈

您可以為您 Lightsail 分發建立亞馬遜 TLS/SSL 憑證。建立憑證時，請指定憑證的主要和替代網域名稱。當您啟用分發的自訂網域，並選擇憑證時，這些網域會新增為分發的自訂網域。在您更新網域的

DNS 記錄來指向分發後，分發就會接受流量並使用 HTTPS 提供內容。您可以建立的憑證數量有配額。如需詳細資訊，請參閱 [Lightsail 服務配額](#)。

如需有關 SSL/TLS 憑證的詳細資訊，請參閱 [SSL/TLS 憑證](#)。

#### Important

您在為分發建立 SSL/TLS 憑證時指定的網域名稱不能被所有 Amazon 網路服務 (AWS) 帳戶 (包括 Amazon 服務上的分發) 的另一個分發使用。CloudFront 您能夠為網域建立憑證，但無法將憑證與分發搭配使用。

## 先決條件

在開始之前，您必須先建立 Lightsail 發行版本。如需詳細資訊，請參閱 [建立分發](#) 和 [內容交付網路分發](#)。

## 建立分發的 SSL/TLS 憑證

請完成下列程序，為分發建立 SSL/TLS 憑證。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁，選擇 Networking (聯網) 索引標籤。
3. 選擇要建立憑證之分發的名稱。
4. 選擇分發管理頁面上的 Custom domains (自訂網域) 索引標籤。
5. 向下捲動至頁面的 Attached certificates (連接的憑證) 區段。

您的所有分發憑證都會列在該頁面的 Attached certificates (連接的憑證) 區段下，包括為其他分發建立的憑證，以及使用中和未使用的憑證。

6. 選擇 Create certificate (建立憑證)。
7. 在 Certificate name (憑證名稱) 文字方塊中輸入唯一名稱，以識別您的憑證。然後選擇 Continue (繼續)。
8. 將您要搭配憑證使用的主要網域名稱 (例如 example.com)，輸入 Specify up to 10 domains or subdomains (指定最多 10 個網域或子網域) 欄位中。
9. (選用) 將替代網域名稱 (例如 www.example.com)，輸入剩餘 Specify up to 10 domains or subdomains (指定最多 10 個網域或子網域) 欄位中。

您可新增最多 9 個替代網域至憑證。啟用自訂網域並選取分發的憑證之後，就能夠將憑證的所有網域與分發搭配使用。

## 10. 選擇建立。

系統會提交您的憑證請求，新憑證的狀態會變更為 Attempting to validate your certificate (正在嘗試驗證您的憑證)。在此期間，Lightsail 會嘗試將憑證的驗證記錄新增至主要網域的 DNS。一段時間後，狀態會變更為 Valid (有效)。

如果自動驗證失敗，您必須使用您的網域驗證憑證，才能搭配分發使用。如需詳細資訊，請參閱[驗證分發的 SSL/TLS 憑證](#)。

## 主題

- [檢視適用於光賽發行版的 SSL/TLS 憑證](#)
- [驗證光賽發行版的 SSL/TLS 憑證](#)
- [使用最低 TLS 通訊協定版本保護您的 Lightsail 發行版](#)
- [從發 Lightsail 版本中刪除未使用的 SSL/TLS 憑證](#)

## 檢視適用於光賽發行版的 SSL/TLS 憑證

您可以檢視您為您的分發建立的 Amazon Lightsail SSL/TLS 憑證。您可以在 Lightsail 主控台中存取任何發行版的管理頁面來執行此操作。

如需有關 SSL/TLS 憑證的詳細資訊，請參閱[SSL/TLS 憑證](#)。

## 必要條件

在開始之前，您必須先建立 Lightsail 發行版本。如需詳細資訊，請參閱[建立分發](#)和[內容交付網路分發](#)。

您還應該為分發建立 SSL/TLS 憑證。如需詳細資訊，請參閱[為分發建立 SSL/TLS 憑證](#)。

## 檢視分發的 SSL/TLS 憑證

請完成下列程序，以檢視分發的 SSL/TLS 憑證。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁，選擇 Networking (聯網) 索引標籤。

### 3. 選擇分發的名稱。

無論您選擇的分發為何，您都可以檢視所有憑證。

### 4. 選擇分發管理頁面上的 Custom domains (自訂網域) 索引標籤。

### 5. 向下捲動至頁面的 Attached certificates (連接的憑證) 區段。

所有的分發憑證都會列在頁面的 Attached certificates (連接的憑證) 區段下。展開 Validation details (驗證詳細資訊)，檢視憑證的重要日期、加密詳細資訊、身分識別和驗證記錄。您的憑證自建立之日起 13 個月內有效，此後 Lightsail 會嘗試自動重新驗證這些憑證。請勿刪除您新增至網域的 CNAME 記錄，因為在列出的 Valid until (有效期) 日期重新驗證憑證時需要這些記錄。

在您擁有有效的 SSL/TLS 憑證與分發搭配使用之後，您應該啟用自訂網域，以便您可以在分發上使用憑證的網域名稱。如需詳細資訊，請參閱[啟用分發的自訂域](#)。

## 驗證光賽發行版的 SSL/TLS 憑證

Amazon Lightsail SSL/TLS 憑證在建立之後，您必須先經過驗證，然後才能將其與您的 Lightsail 分發搭配使用。提交憑證請求後，新憑證的狀態會變更為 Attempting to validate your certificate (正在嘗試驗證您的憑證)。在此期間，Lightsail 會嘗試將憑證的驗證記錄新增至您為憑證指定之網域名稱的 DNS。一段時間後，狀態會變更為 Valid (有效) 或 Validation timed out (驗證逾時)。

如果自動驗證失敗，您必須確認控制了要建立憑證時，為該憑證指定的所有網域名稱。若要執行此操作，您可以將正式名稱 (CNAME) 記錄新增至憑證上指定的每個網域的 DNS 區域。您必須新增的記錄列於憑證的 Validation details (驗證詳細資訊) 區段。

在本指南中，我們提供了使用 Lightsail DNS 區域手動驗證憑證的程序。使用不同的 DNS 主機供應商 (例如 Domain.com 或 GoDaddy) 驗證憑證的程序可能類似。如需有關 DNS 區域 Lightsail 細資訊，請參閱 [DNS](#)。

如需有關 SSL/TLS 憑證的詳細資訊，請參閱 [SSL/TLS 憑證](#)。

### 內容

- [必要條件](#)
- [取得 CNAME 記錄值以驗證憑證](#)
- [新增 CNAME 記錄至網域的 DNS 區域](#)
- [檢視分發憑證的狀態](#)

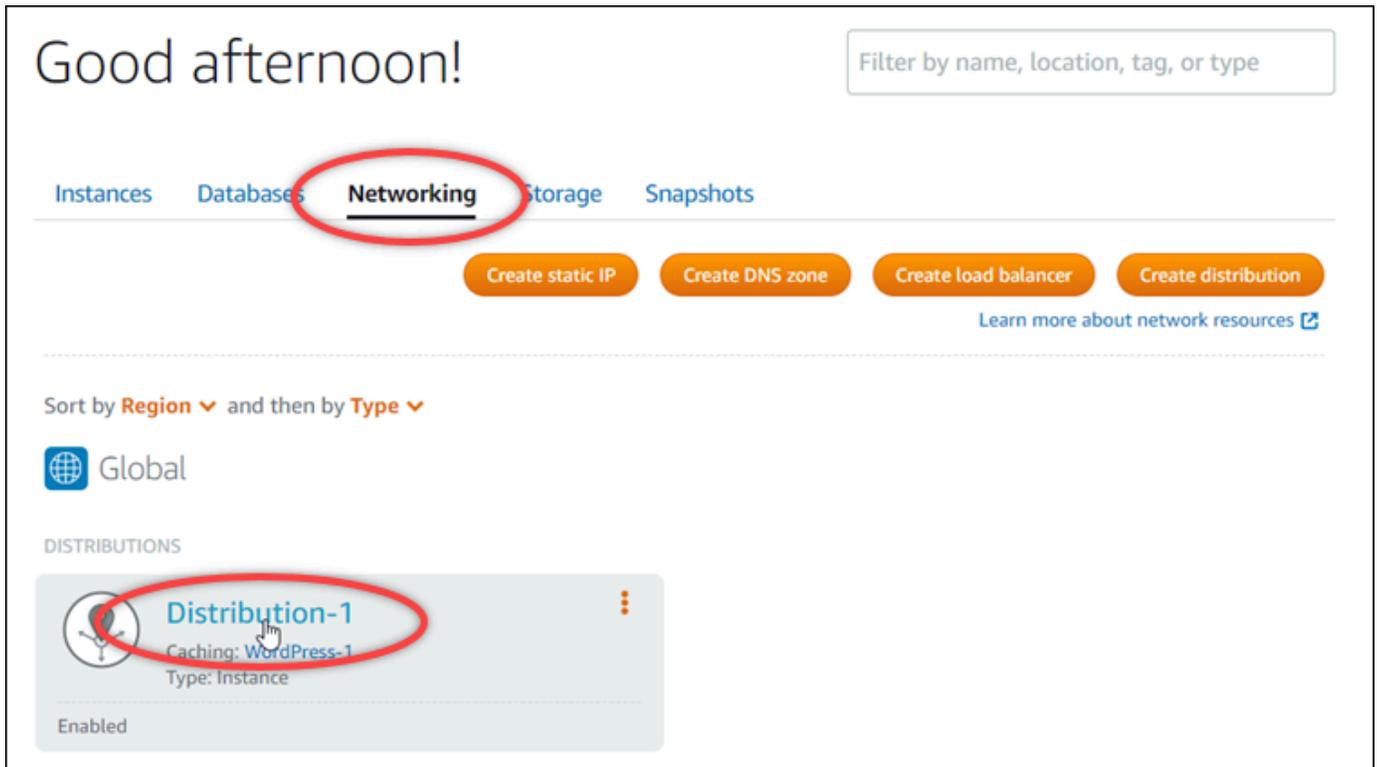
## 先決條件

開始之前，您需要為分發建立 SSL/TLS 憑證。如需詳細資訊，請參閱[為分發建立 SSL/TLS 憑證](#)。

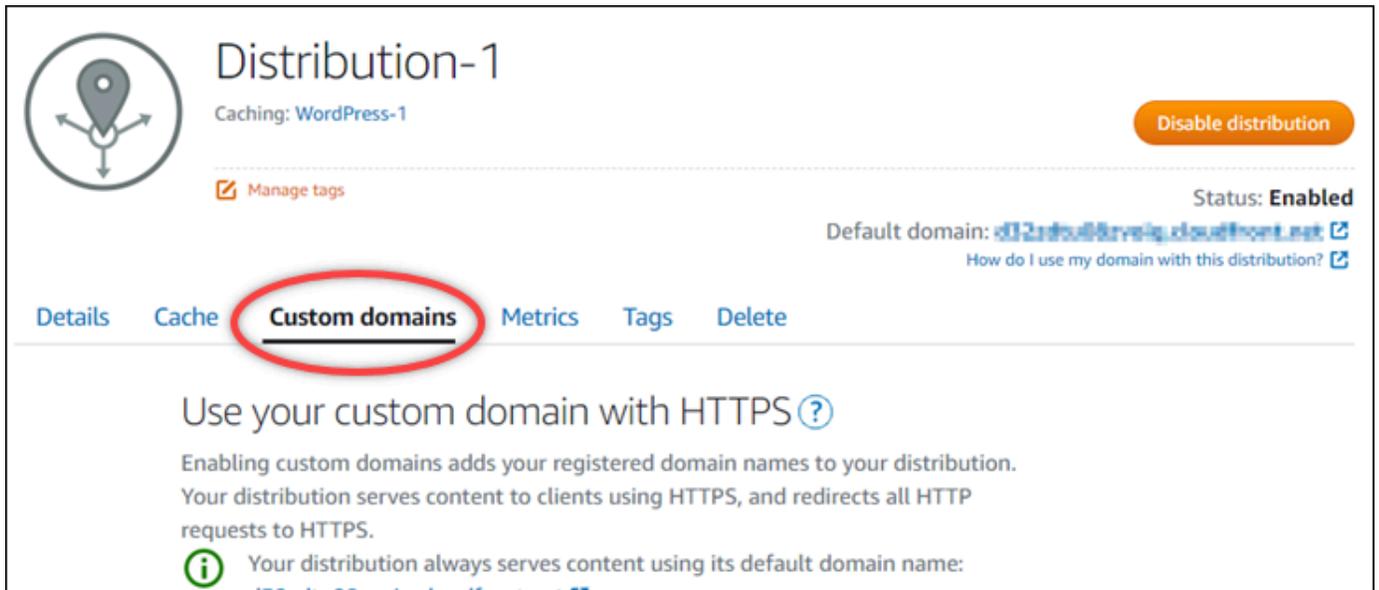
### 取得 CNAME 記錄值以驗證憑證

請完成下列程序，以取得必須新增至網域以驗證憑證的 CNAME 記錄。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁，選擇 Networking (聯網) 索引標籤。
3. 選擇要取得憑證的 CNAME 記錄值的分發名稱。



4. 選擇分發管理頁面上的 Custom domains (自訂網域) 索引標籤。



5. 向下捲動至頁面的 Attached certificates (連接的憑證) 區段。

您所有的散發憑證都會列在頁面的「附加憑證」區段下，包括為其他 Lightsail 資源建立的憑證，以及等待驗證的憑證。

6. 尋找您要驗證的憑證，展開 Validation details (驗證詳細資訊)，並記下您必須為列出的每個網域新增之 CNAME 記錄的 Name (名稱) 和 Value (值)。

您必須完全依照列出的方式新增這些記錄。建議您複製這些值並貼至稍後可參考的文字檔案中。如需詳細資訊，請參閱本指南的下列[將 CNAME 記錄新增至網域的 DNS 區域](#)章節。

### 新增 CNAME 記錄至網域的 DNS 區域

請完成以下程序，將 CNAME 記錄新增至網域的 DNS 區域。

1. 選擇 Lightsail 首頁上的 Domains & DNS (網域和 DNS) 索引標籤。
2. 在頁面的 DNS zones (DNS 區域) 區段下，選擇您要新增 CNAME 記錄以驗證憑證的網域名稱。
3. 選擇 DNS records (DNS 記錄) 索引標籤。
4. 在 DNS 記錄管理頁面上，選擇 Add record (新增記錄)。
5. 在 Record type (記錄類型) 下拉式選單中，選擇 CNAME。
6. 在 Record name (記錄名稱) 文字方塊中，輸入您從憑證取得之 CNAME 記錄的 Name (名稱) 值。

Lightsail 主控台會預先填入您網域的頂點部分。例如，如果您要新增 `www.example.com` 子網域，則只需在文字方塊中輸入 `www`，當您儲存記錄時，Lightsail 會新增 `.example.com` 部分。

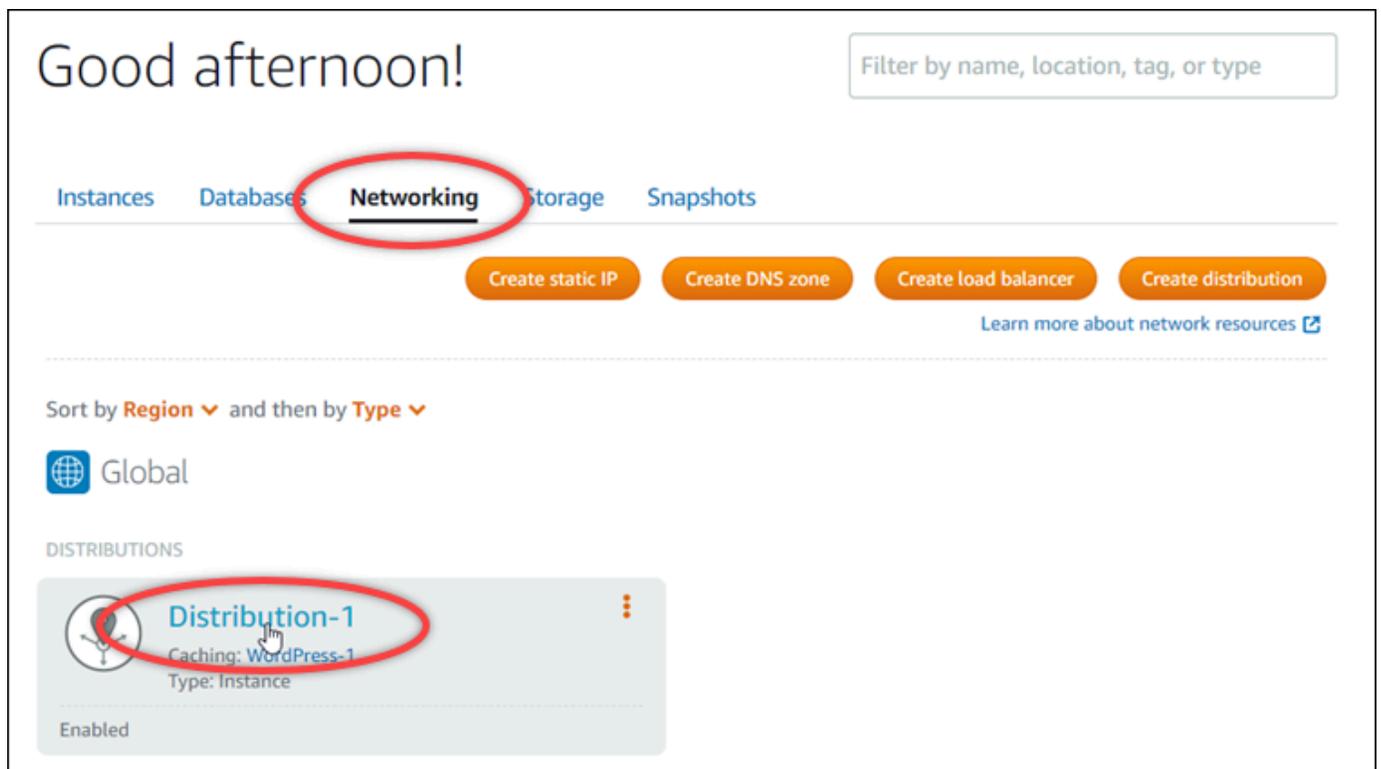
7. 在 Route traffic to (將流量路由至) 文字方塊中，輸入您從憑證取得之 CNAME 記錄的 Value (值) 部分。
8. 確認您輸入的值與您要驗證的憑證上列出的值完全相同。
9. 選擇儲存圖示，將記錄儲存到 DNS 區域。

重複這些步驟，為憑證上需要驗證的網域新增其他 CNAME 記錄。允許透過網際網路 DNS 傳播的變更時間。幾分鐘後，分發憑證的狀態應該變更為 Valid (有效)。如需詳細資訊，請參閱本指南的[檢視分發憑證的狀態](#)一節。

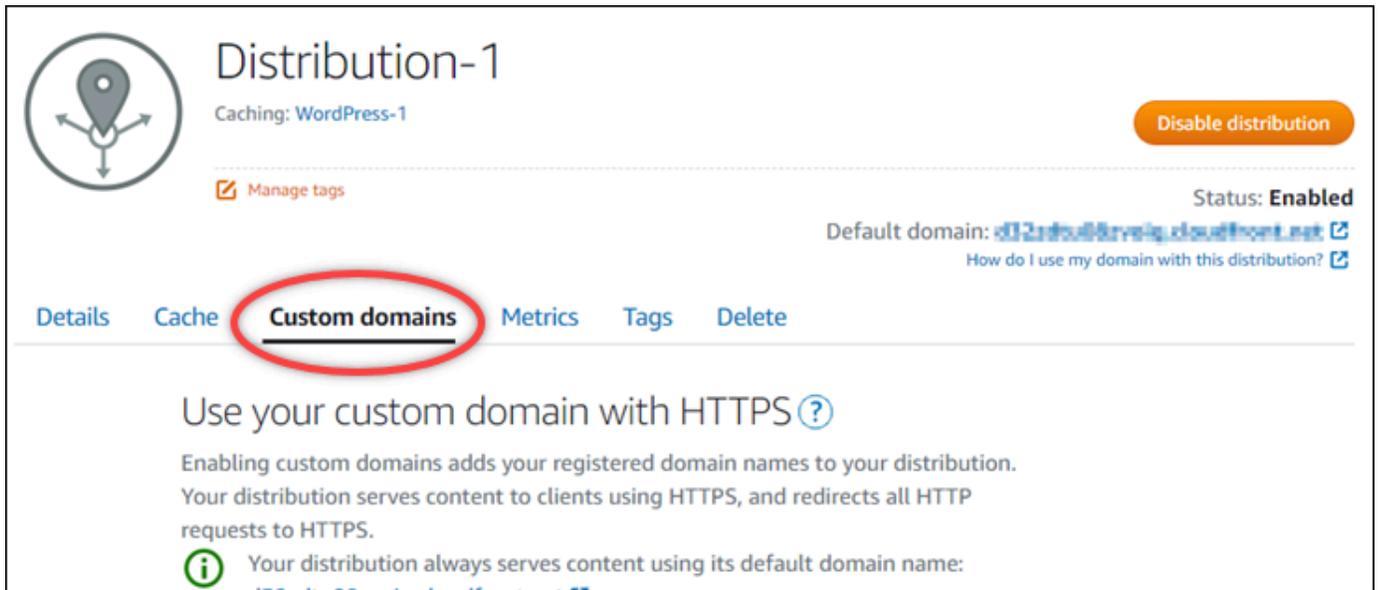
## 檢視分發憑證的狀態

請完成下列程序，以檢視分發的 SSL/TLS 憑證的狀態。

1. 在 Lightsail 首頁，選擇 Networking (聯網) 索引標籤。
2. 選擇要檢視憑證狀態的分發名稱。

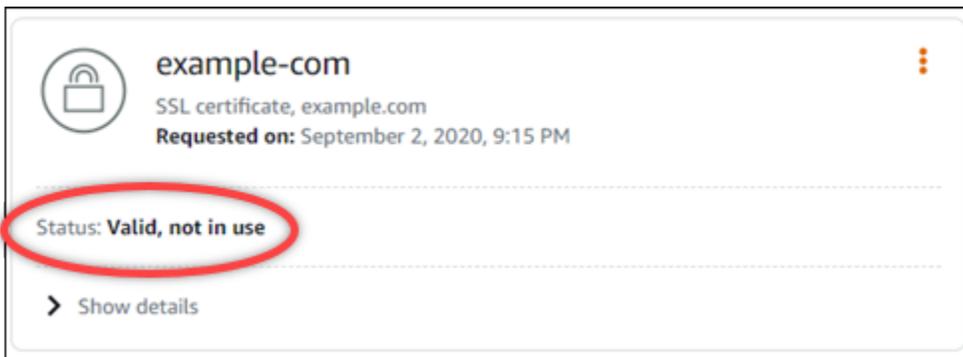


3. 選擇分發管理頁面上的 Custom domains (自訂網域) 索引標籤。



4. 向下捲動至頁面的 Attached certificates (連接的憑證) 區段。

所有的分發憑證都會列在頁面的 Attached certificates (連接的憑證) 區段下，包括狀態為 Pending validation (待驗證) 和 Valid (有效) 的憑證。



Valid (有效) 狀態確認您已使用新增至網域的 CNAME 記錄成功驗證憑證。選擇 Details (詳細資訊)，檢視憑證的重要日期、加密詳細資訊、身分識別和驗證記錄。您的憑證自驗證之日起 13 個月內有效，此後 Lightsail 會嘗試自動重新驗這些證憑證。請勿刪除您新增至網域的 CNAME 記錄，因為在列出的 Valid until (有效期) 日期重新驗證憑證時需要這些記錄。

驗證 SSL/TLS 憑證之後，您應該啟用分發的自訂網域，以便在分發上使用憑證的網域名稱。如需詳細資訊，請參閱[啟用分發的自訂域](#)。

## 使用最低 TLS 通訊協定版本保護您的 Lightsail 發行版

Amazon Lightsail 使用 SSL/TLS 憑證來驗證您可以與您的分發搭配使用的自訂 (已註冊) 網域。本指南提供您可為 SSL/TLS 憑證設定的檢視器最低 TLS 通訊協定版本 (通訊協定版本) 的相關資訊。如需有關 SSL/TLS 憑證的詳細資訊，請參閱 [Lightsail 中的 SSL/TLS 憑證](#)。檢視器是一種應用程式，可以向與 Lightsail 發佈相關聯的邊緣位置發出 HTTP 要求。如需有關發佈的詳細資訊，請參閱 [Lightsail 中的內容傳遞網路發佈](#)。

當您啟用發佈的自訂網域時，依預設會設定 TLSv1.2\_2021 通訊協定版本。您可以設定不同的通訊協定版本，如本指南稍後所述。Lightsail 發行版本不支援自訂 TLS 通訊協定版本。

### 支援的通訊協定

您可以使用下列 TLS 通訊協定來設定 Lightsail 發行版：

- (建議使用)
- TLSv1.2\_2019
- TLSv1.2\_2018
- TLSv1.1\_2016

### 必要條件

請先完成事前準備 (若尚未完成)：

- [建立內 Lightsail 遞網路發佈](#)
- [建立分發的 SSL/TLS 憑證](#)
- [驗證分發的 SSL/TLS 憑證](#)
- [啟用分發的自訂域](#)
- [將您的網域指向發行版](#)

### 識別您發佈的最低 TLS 通訊協定版本

請完成下列步驟，以識別 Lightsail 發行版本的最低 TLS 通訊協定版本

#### Note

在本指南中，您將使用 AWS CloudShell 來執行升級。CloudShell 是以瀏覽器為基礎的預先驗證殼層，您可以直接從 Lightsail 主控台啟動。使用時 CloudShell，您可以使用偏好的外殼程

序來執行 AWS CLI 命令 PowerShell，例如 Bash 或 Z 殼層。無需下載或安裝命令列工具即可執行此操作。如需有關如何設定和使用的詳細資訊 CloudShell，請參閱 [如需詳細資訊，請參閱 Lightsail AWS CloudShell 中的](#)。

1. 開啟「終端機」或「命令提示字元」視窗。[AWS CloudShell](#)
2. 輸入下列命令，以識別 Lightsail 發行版本的最低 TLS 通訊協定版本。

```
aws lightsail get-distributions --distribution-name DistributionName --region us-east-1 | grep "viewerMinimumTlsProtocolVersion"
```

在命令中，*DistributionName* 以您要修改的發行版名稱取代。

#### 範例

```
aws lightsail get-distributions --distribution-name Distribution-1 --region us-east-1 | grep "viewerMinimumTlsProtocolVersion"
```

該命令將返回您的發行版本的最低 TLS 協議版本的 ID。

#### 範例

```
"viewerMinimumTlsProtocolVersion": "TLSv1.2_2021"
```

## 使用 AWS CLI

完成下列程序，以使用 AWS Command Line Interface (AWS CLI) 設定 TLS 通訊協定版本。您可以使用 `update-distribution` 命令來執行此動作。如需詳細資訊，請參閱《AWS CLI 命令參考》中的 [更新分發屬性](#)。

1. 開啟「終端機」或「命令提示字元」視窗。[AWS CloudShell](#)
2. 輸入下列命令以變更發佈的最低 TLS 通訊協定版本。

```
aws lightsail update-distribution --distribution-name DistributionName --viewer-minimum-tls-protocol-version ProtocolVersion
```

將命令中的以下範例文字取代為自訂文字：

- *DistributionName* 使用您要更新的發行版的名稱。
- *ProtocolVersion* 使用有效的 TLS 協議版本。例如 TLSv1.2\_2021 或 TLSv1.2\_2019。

範例：

```
aws lightsail update-distribution --distribution-name MyDistribution --viewer-  
minimum-tls-protocol-version TLSv1.2_2021
```

您所做的變更需要一些時間才會生效。

## 從發 Lightsail 版本中刪除未使用的 SSL/TLS 憑證

您可以刪除您不再在發行版上使用的 Amazon Lightsail SSL/TLS 憑證。例如，您的憑證可能已過期，而您已連接通過驗證的更新憑證。如需憑證的詳細資訊，請參閱 [SSL/TLS 憑證](#)。如需有關分發的詳細資訊，請參閱 [內容交付網路分發](#)。

刪除 SSL/TLS 憑證是最終的步驟，而且無法還原。您在 365 天的期間內，可建立的憑證數量是有配額的。 [如需詳細資訊，請參閱 AWS 一般參考](#)

### 刪除分發的 SSL/TLS 憑證

請完成下列程序以刪除分發的 SSL/TLS 憑證。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁，選擇 Networking (聯網) 索引標籤。
3. 選擇您要從中刪除 SSL/TLS 憑證之分發的名稱。因為所有憑證都會列於每個分發中，如果憑證目前未在使用中，您便可以選擇任何分發。
4. 選擇分發管理頁面上的 Custom domains (自訂網域) 索引標籤。
5. 在該頁面的憑證區段中，為您要刪除的憑證選擇省略符號圖示 (:)，然後選擇刪除。

如果您要刪除的憑證正在使用中，則 Delete (刪除) 選項無法使用。若要刪除使用中的憑證，您需要先變更使用憑證之分發的自訂網域，或停用使用憑證之分發上的自訂網域。如需詳細資訊，請參閱 [變更分發的自訂域](#) 和 [啟用分發的自訂域](#)。

6. 選擇 Yes, Delete (是，刪除) 以確認刪除。

## 為您的 Lightsail 負載平衡器啟用HTTPS用SSL/TLS憑證

建立 Lightsail 負載平衡器之後，您可以附加要啟用HTTPS的傳輸層安全性 (TLS) 憑證。SSL/TLS憑證可讓您的負載平衡器處理加密的 Web 流量，讓您可以為使用者提供更安全的體驗。要了解更多信息，請參閱 [SSL/TLS證書](#)。

### 必要條件

在開始使用之前，您將需要滿足以下條件。

- 一個 Lightsail 平衡器。若要進一步了解，請參閱[建立負載平衡器](#)。

### 建立憑證請求

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁上，選擇 [網路功能]。
3. 選擇您要設定SSL/TLS憑證的負載平衡器名稱。
4. 選擇 Custom domains (自訂網域) 索引標籤。
5. 選擇 Create certificate (建立憑證)。
6. 輸入憑證的名稱或接受預設。

資源名稱：

- 每個 Lightsail 帳戶 AWS 區域 中的每個項目都必須是唯一的。
  - 必須包含 2 至 255 個字元。
  - 開頭和結尾必須是英數字元或數字。
  - 可以包含英數字元、數字、句點、破折號和底線。
7. 輸入您的主要網域 (www.example.com)，以及最多 9 個替代網域或子網域。

如需詳細資訊，請參閱[將替代網域和子網域新增至SSL/TLS憑證](#)

8. 選擇 Create certificate (建立憑證)。

Lightsail 驗證程序。您有 72 小時可以驗證您擁有您的網域。

在您建立憑證之後，您會看到憑證與網域名稱以及所有替代網域和子網域。您需要為每個域和子域創建一個DNS記錄。

## 下一步驟

- [驗證您擁有您的網域](#)

### 主題

- [將替代網域和子網域 Lightsail 至您的網域](#)
- [在 Lightsail 中使用CNAME記錄驗TLS證SSL/憑證網域](#)
- [將經過驗證的SSL/TLS憑證附加至您的 Lightsail 負載平衡器](#)
- [從負載平衡器移除SSL/TLS憑證](#)

## 將替代網域和子網域 Lightsail 至您的網域

當您為 Lightsail 負載平衡器建立 SSL/TLS 憑證時，您可以在其中新增替代網域和子網域。這些替代名稱有助於確保所有到達您負載平衡器的流量都經過加密。

指定主要網域時，可使用完全合格的網域名稱 (如 `www.example.com`) 或 apex 網域名稱 (如 `example.com`)。

網域和子網域的總數不得超過 10，因此您至多可將 9 個替代網域和子網域新增到您的憑證。建議您新增如下列清單的項目。

- `example.com`
- `example.net`
- `blog.example.com`
- `myexamples.com`

### 建立具有替代網域和子網域的憑證

1. 請先[建立負載平衡器](#) (若您還沒有的話)。
2. 在 Lightsail 首頁，選擇 Networking (聯網) 索引標籤。
3. 選擇您的負載平衡器。
4. 選擇 Custom domains (自訂網域) 索引標籤。
5. 選擇 Create certificate (建立憑證)。
6. 輸入憑證的名稱，或接受預設名稱。

資源名稱：

- 每個 Lightsail 帳戶 AWS 區域 中的每個項目都必須是唯一的。
  - 必須包含 2 至 255 個字元。
  - 開頭和結尾必須是英數字元或數字。
  - 可以包含英數字元、數字、句點、破折號和底線。
7. 輸入您的主要網域 (www.example.com) ，以及最多 9 個替代網域或子網域。
  8. 選擇 Create certificate (建立憑證)。

建立後，您有 72 小時可以驗證您擁有您的網域。

後續步驟

- [使用 DNS 驗證網域所有權](#)

驗證後，您可以選取已驗證的憑證，將其與 Lightsail 負載平衡器建立關聯。

- [啟用工作階段持續性](#)

## 在 Lightsail 中使用 CNAME 記錄驗 TLS 證 SSL/憑證網域

在 Lightsail 中建立 SSL/TLS 憑證之後，您需要確認您控制新增至憑證的所有網域和子網域。

內容

- [步驟 1：為您的網域建立 Lightsail DNS 區域](#)
- [步驟 2：將記錄新增至您網域的 DNS 區域](#)
- [下一步驟](#)

### 步驟 1：為您的網域建立 Lightsail DNS 區域

如果您尚未這麼做，請為您的網域建立 Lightsail DNS 區域。如需詳細資訊，請參閱[建立 DNS 區域以管理網域 DNS 記錄](#)

### 步驟 2：將記錄新增至您網域的 DNS 區域

您建立的憑證會提供一組正式名稱 (CNAME) 記錄。您可以將這些記錄新增至網域的 DNS 區域，以確認您擁有或控制該網域。

**⚠ Important**

建立憑證時，Lightsail 會嘗試自動驗證您是否控制了指定的網域或子網域。選取 [建立憑證] 後，CNAME 記錄就會新增至您網域的 DNS 區域。如果自動驗證成功，憑證的狀態會從 Attempting to validate your certificate (正在嘗試驗證您的憑證)，變更為 Valid, in use (有效，使用中)。

如果自動驗證失敗，請繼續執行下列步驟。

在以下步驟中，我們將向您展示如何取得 CNAME 記錄，並將其新增至 Lightsail 主控台內的網域 DNS 區域。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁上，請在頂部導覽選單中選擇 Account (帳戶)。
3. 在下拉式選單中選擇 Account (帳戶)。
4. 選擇 Certificates (憑證) 索引標籤。
5. 尋找您要驗證的憑證，並記下您必須為每個網域新增的 CNAME 記錄的名稱和值

請將這些記錄複製到剪貼簿。如果您使用的是 Windows，按下 Ctrl+C (Ctrl+C)；如果您使用的是 Mac，則需按下 Cmd+C (Cmd+C)。



**example.com**  
SSL certificate, example.com  
**Requested on:** January 15, 2019, 2:57 PM

---

Status:  **Validation in progress...**

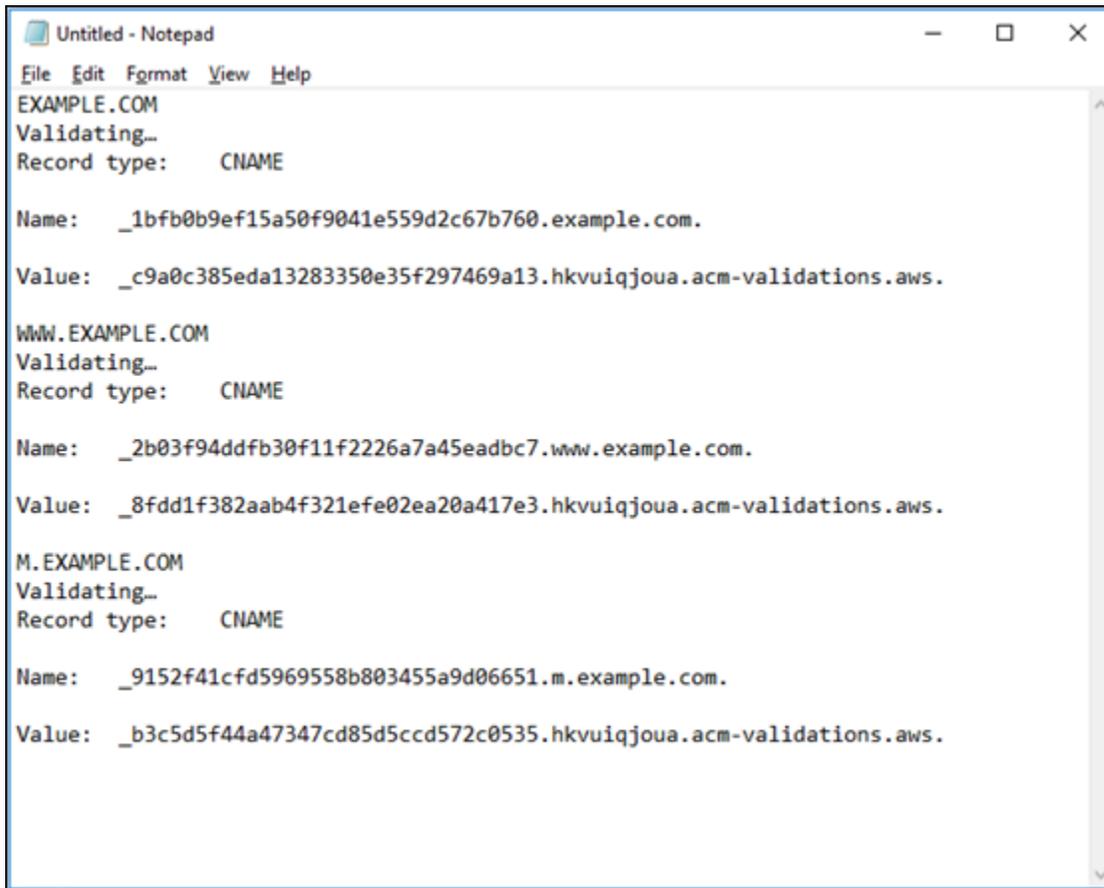
You must prove you control the domains and subdomains specified in this certificate before it can be used for HTTPS encryption.

**Please create a DNS record for each domain with the following values:**

<b>EXAMPLE.COM</b>	Validating...
<b>Record type:</b> CNAME	
<b>Name:</b> 1bfb0b9ef15a50f9041e559d2c67b760.example.com.	
<b>Value:</b> c9a0c385eda13283350e35f297469a13.hkvuiqjoua.acm-validations.aws.	
<hr/>	
<b>WWW.EXAMPLE.COM</b>	Validating...
<b>Record type:</b> CNAME	
<b>Name:</b> 2b03f94ddf30f11f2226a7a45eadbc7.www.example.com.	
<b>Value:</b> 8fdd1f382aab4f321efe02ea20a417e3.hkvuiqjoua.acm-validations.aws.	
<hr/>	
<b>M.EXAMPLE.COM</b>	Validating...
<b>Record type:</b> CNAME	
<b>Name:</b> 9152f41cfd5969558b803455a9d06651.m.example.com.	
<b>Value:</b> b3c5d5f44a47347cd85d5ccd572c0535.hkvuiqjoua.acm-validations.aws.	

- 如果您使用 Windows 或使用 Mac，請開啟文字編輯器，例 TextEdit 如「記事本」。在文字檔案中，請按下 Ctrl+V (Ctrl+V) (適用於 Windows 作業系統)，或是按下 Cmd+V (Cmd+V) (適用於 Mac 作業系統)，以將該值貼至文字檔案中。

將此文字檔保持開啟狀態；本指南稍後將記錄新增至您的網域DNS區域時，您將需要這些CNAME值。



```
Untitled - Notepad
File Edit Format View Help
EXAMPLE.COM
Validating...
Record type: CNAME

Name: _1bfb0b9ef15a50f9041e559d2c67b760.example.com.
Value: _c9a0c385eda13283350e35f297469a13.hkvuijqoua.acm-validations.aws.

WWW.EXAMPLE.COM
Validating...
Record type: CNAME

Name: _2b03f94ddfb30f11f2226a7a45eadbc7.www.example.com.
Value: _8fdd1f382aab4f321efe02ea20a417e3.hkvuijqoua.acm-validations.aws.

M.EXAMPLE.COM
Validating...
Record type: CNAME

Name: _9152f41cfd5969558b803455a9d06651.m.example.com.
Value: _b3c5d5f44a47347cd85d5ccd572c0535.hkvuijqoua.acm-validations.aws.
```

7. 選擇 Lightsail 主控台頂端導覽列上的 [首頁]。
8. 在首頁DNS上選 Lightsail 域和。
9. 選擇將使用憑證之網域的DNS區域。
10. 選擇「記錄」標籤中的「新增DNS記錄」。
11. 選擇CNAME記錄類型。
12. 切換至包含憑證CNAME記錄的文字檔案。

複製CNAME記錄的名稱。例如：\_1bfb0b9ef15a50f9041e559d2c67b760。

13. 切換至DNS記錄頁面，然後將「名稱」貼到「記錄名稱」欄位中。

#### Important

新增包含網域名稱的CNAME記錄 (例如.example.com) 會導致網域名稱重複 (例如.example.com.example.com)。若要避免重複，請編輯項目，以便只新增CNAME您需要的部分。此處指的是 \_1bfb0b9ef15a50f9041e559d2c67b760。

14. 複製CNAME記錄的值。例  
如：`_c9a0c385eda13283350e35f297469a13.hkvuiqjoua.acm-validations.aws.`。
15. 切換至DNS記錄頁面，並將「值」貼到「將流量路由到」欄位中。
16. 選擇 Save (儲存)，即可新增記錄。
17. 若您有替代子網域，則需選擇 Add record (新增記錄) 以新增另一個記錄。

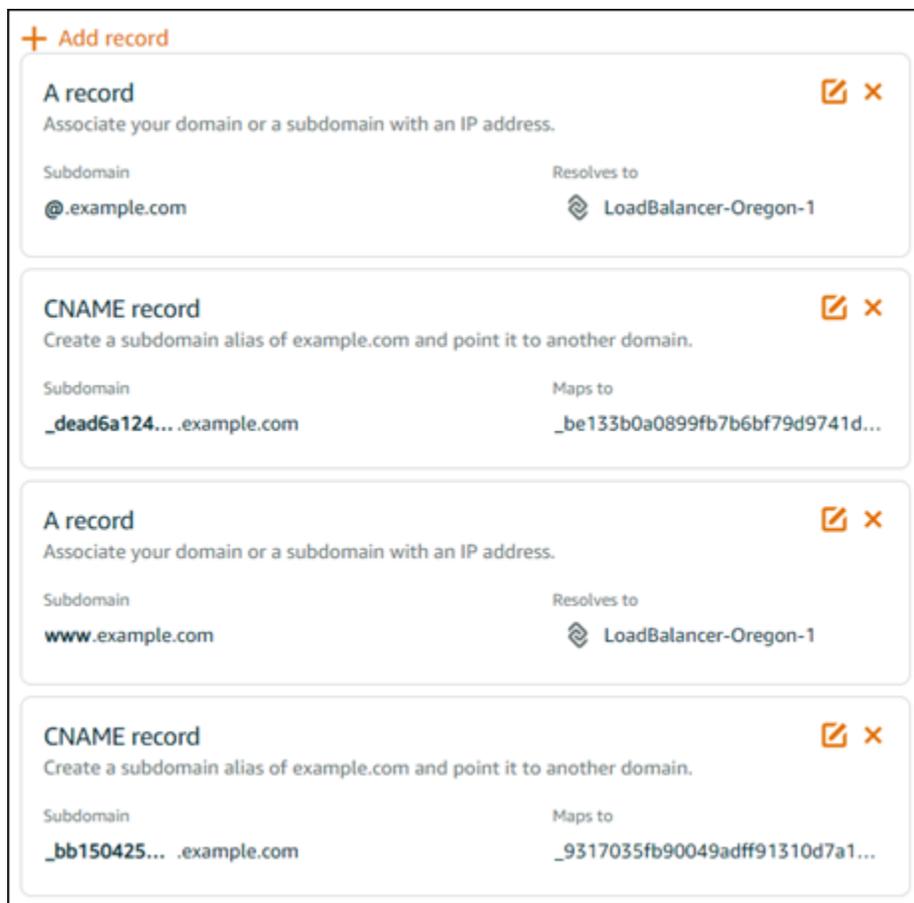
#### Note

若要進一步了解替代網域或子網域，請參閱[在 Amazon Lightsail 中將替代網域和子網域新增至您的SSL/TLS憑證。](#)

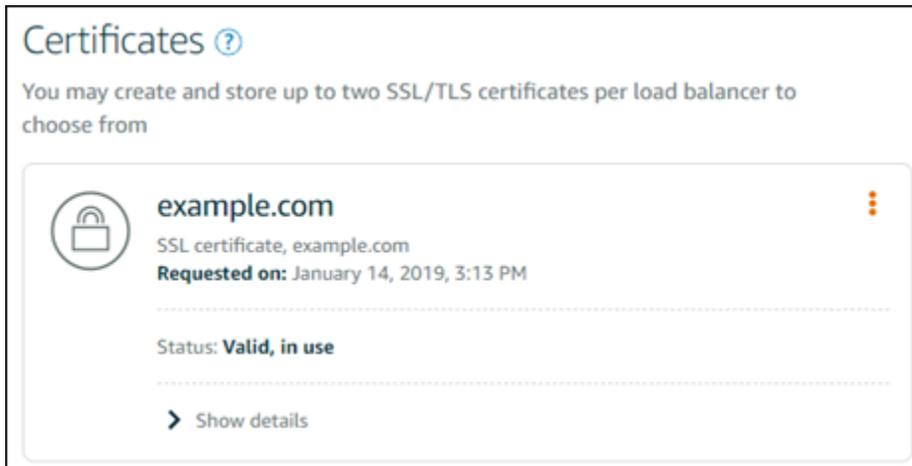
18. 重複步驟 11-17，以新增替代子網域的CNAME記錄。

您也可以在DNS區域管理頁面上[新增別名 \(A\) 記錄以指向負載平衡器](#)或其他 Lightsail 資源。

完成後，您的DNS區域應該看起來像下面的屏幕截圖。



請稍待一段時間，網域通過驗證後，您會在憑證上看到以下訊息。

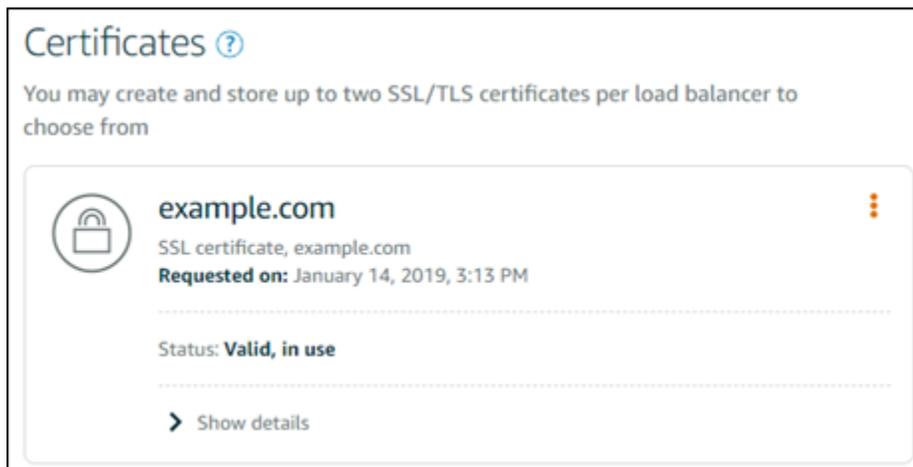


## 下一步驟

一旦您的網域通過驗證，您就可以將經過驗證的SSL/TLS憑證附加到負載平衡器。

## 將經過驗證的SSL/TLS憑證附加至您的 Lightsail 負載平衡器

驗證您可控制網域後，憑證的狀態會變更為 Valid (有效)。



您的下一個步驟是將憑證附加至 Lightsail 負載平衡器。

1. 在 Lightsail 首頁中，選擇 [網路功能]。
2. 選擇您的 負載平衡器。
3. 選擇 Custom domains (自訂網域) 索引標籤。
4. 在 Certificates (憑證) 區段中，選擇 Attach certificate (連接憑證)。
5. 從下拉式清單中選取憑證。
6. 選擇附加，以附加憑證。

## 從負載平衡器移除SSL/TLS憑證

您可以刪除不再使用的SSL/TLS憑證。例如，您的憑證可能已過期，而您已連接通過驗證的更新憑證。如果您要在刪除憑證之前複製憑證，可在與下方步驟 5 的相同捷徑選單中選擇 Duplicate (複製)。

### Important

如果您要刪除的憑證有效且正在使用中，您的負載平衡器將無法再處理加密 (HTTPS) 流量。您的 Lightsail 負載平衡器仍將支援未加密的 (HTTP) 流量。

刪除SSL/TLS證書是最終的，無法撤消。您在 365 天的期間內，可建立的憑證數量是有配額的。如需詳細資訊，請參閱 [Certificate Manager 使用指南](#) 中的 [配額](#)。

1. 在 Lightsail 首頁上，選擇 [網路功能]。
2. 選擇連接SSL/TLS憑證的負載平衡器。
3. 選擇負載平衡器管理頁面上的 Inbound traffic (傳入流量) 索引標籤。
4. 在該頁面的憑證區段中，為您要刪除的憑證選擇省略符號圖示 (:)，然後選擇刪除。

如果您要刪除的憑證正在使用中，則 Delete (刪除) 選項無法使用。若要刪除使用中的憑證，您必須先變更正在使用憑證之負載平衡器的憑證，或在使用憑證的負載平衡器HTTPS上停用。

## 設定反向 DNS 以防止 Lightsail 執行個體發生垃圾郵件

電子郵件伺服器會使用反向網域名稱系統 (DNS) 查詢，來追蹤訊息來源並確認該郵件不是垃圾或惡意郵件。反向 DNS 查詢會傳回 IP 地址的網域名稱。這與正向 DNS 查詢的情況相反，因為這會傳回網域的 IP 地址。

例如，如果 IP 地址為 192.168.1.2 的反向 DNS 查詢會傳回子網域 mail.example.com，子網域為 mail.example.com 的正向 DNS 查詢會傳回 IP 地址 192.168.1.2，然後會正向確認 IP 地址為 192.168.1.2 的反向 DNS。要進一步了解，請參閱在 Wikipedia 上的 [正向確認反向 DNS](#)。

您可以完成必要條件，然後向 AWS Support 部門提交請求以移除輸出訊息配額，以便為 Amazon Lightsail 執行個體設定反向 DNS。詳細步驟請參閱下列各節。

### 必要條件

要設定反向 DNS，請依顯示的順序填寫以下必要條件：

1. 建立要當作電子郵件伺服器使用的 Lightsail 實體。如需詳細資訊，請參閱[建立執行個體](#)。
2. 建立要用於反向 DNS 記錄的靜態 IP，並將它連接到執行中的執行個體。如需詳細資訊，請參閱[建立靜態 IP 並將其附接至執行個體](#)。

#### Important

您不能對反向 DNS 使用預設的公有 IP，也就是您在第一次建立執行個體時指派至其中的 IP。這是因為在您停止和啟動執行個體時，執行個體的預設公有 IP 將會改變。

3. 在網域的 DNS 區域中，將指向子網域 (例如 mail.example.com) 的別名記錄新增至執行中執行個體的靜態 IP 地址。這是在執行靜態 IP 地址的反向 DNS 查詢時傳回的子網域。如需詳細資訊，請參閱[建立 DNS 區域以管理域的 DNS 記錄](#)。

#### Note

我們建議您將網域 DNS 記錄的管理作業移轉至 Lightsail。這可讓您在 Lightsail 主控台的單一位置管理所有資源 (包括網域)。如需詳細資訊，請參閱[建立 DNS 區域以管理域的 DNS 記錄](#)。

4. 允許透過網際網路 DNS 傳播的變更時間。然後，您可以繼續將請求提交到 AWS Support 來設定反向 DNS。

## 將請求提交到 AWS Support 來設定反向 DNS

基於安全理由，Lightsail 預設會透過連接埠 25 限制輸出郵件。不過，您可以請求 AWS Support 將此配額從您的帳戶中移除並為您的靜態 IP 設定反向 DNS。

將請求提交給 AWS Support

1. 以 AWS 帳戶根使用者身分登入 [Lightsail 主控台](#)。

#### Important

必須使用 AWS 帳戶根使用者來提交請求。如需有關 AWS 帳戶根使用者的詳細資訊，請參閱 [AWS 帳戶根使用者](#)。

2. 導覽到[請求以移除電子郵件傳送限制](#)表單，然後輸入下列必要資訊：

**Note**

該表單會參考 Amazon Elastic Compute (EC2) 資源 (例如彈性 IP (EIP) 和 EC2 執行個體)。不過，您也可以將表單用於 Lightsail 資源，例如靜態 IP 和 Lightsail 執行個體。

- 電子郵件地址 - 輸入您收到與請求相關之對應的電子郵件地址。系統已在這個文字方塊中預先填入您的帳戶電子郵件地址。
  - 使用案例描述 - 輸入電子郵件配額移除的請求原因。
  - 彈性 IP 地址 - 輸入您先前在此指南中必要條件之步驟 2 中，連接到執行個體的靜態 IP 地址。您可以輸入最多兩個靜態 IP 地址。
  - EIP 的反向 DNS 記錄 - 輸入您先前在此指南中必要條件之步驟 3 中定義的子網域。這是在執行反向 DNS 查詢時傳回的網域。
3. 完成時選擇 Submit (提交)。

在 AWS Support 完成您的請求後，您可透過反向 DNS 查詢正向確認您的靜態 IP 地址。

如果您稍後想要從 Lightsail 帳戶刪除靜態 IP 位址，則必須向 AWS Support 部門提交請求，以移除反向 DNS 組態。移除反向 DNS 設定之後，您可以使用 Lightsail 主控台從 Lightsail 帳戶中刪除靜態 IP 位址。如需詳細資訊，請參閱[刪除靜態 IP](#)。

# 使用 Lightsail 物件儲存貯體來儲存及管理資料

使用 Amazon Lightsail 物件儲存服務，隨時隨地在網際網路上的任何地方存放和擷取物件。它旨在降低開發人員進行網路規模運算的難度，並使用 Amazon Simple Storage Service (Amazon S3) 進行建置。Lightsail 物件儲存可讓您存取 Amazon 用來執行其全球網站網路的相同高度可擴展、可靠、快速、廉價的資料儲存基礎設施。該服務的目的是要盡可能增加擴展的好處，並將這些好處傳遞給您。

## 物件儲存概念

下列概念和術語適用於 Lightsail 物件儲存。

### 儲存貯體

值區是儲存在 Lightsail 物件儲存服務中之物件的容器。每個物件都包含在具有自己的值區中 URL。例如，如果名 `media/sailbot.jpg` 為的物件儲存在美國東部 (維吉尼亞北部) 區域 (`us-east-1`) 的 `DOC-EXAMPLE-BUCKET` 值區中，則可以使用類似的來定址 URL 該物件。`https://DOC-EXAMPLE-BUCKET.us-east-1.amazonaws.com/media/sailbot.jpg`

您可以在可使用 Lightsail 的 AWS 區域 地方建立值區。如需有關哪些 AWS 區域 Lightsail 可在中使用的詳細資訊，請參閱 AWS 一般參考中的 [區域和端點](#)。

### 儲存貯體儲存計劃

儲存空間計劃 (在中稱為服務包) 會指定值區的每月成本、儲存空間和資料傳輸配額。AWS API 您必須在第一次建立儲存貯體時選擇儲存計劃。您可以稍後在儲存貯體啟動並執行後進行變更。

在每月 AWS 帳單週期內，您只能變更值區的計劃一次。如果儲存貯體的計劃一直超過儲存空間或資料傳輸配額，或儲存貯體的儲存空間或資料傳輸配額一直用量偏低，則請變更計劃。由於儲存貯體可能會遇到無法預測的使用量波動，我們強烈建議您將儲存貯體計劃的變更作為長期策略，而不是作為每月降低成本的短期措施。選擇一個儲存計畫，讓您的儲存貯體往後能擁有充足的儲存空間和資料傳輸配額。

### 物件

物件是存放在儲存貯體中的基本實體。您上傳到儲存貯體的檔案在存放時稱為物件。物件是由資料與中繼資料構成。資料部分對 Lightsail 物件儲存服務而言是不透明的。中繼資料是一組成對的名稱與數值，會說明該物件。這些包括一些默認元數據 (例如上次修改日期) 和標準 HTTP 元數據 (例如 `Content-Type`)。

在儲存貯體中，每個物件都是由索引鍵名稱與版本 ID 來唯一識別。

## 物件索引鍵名稱

索引鍵名稱是儲存貯體中物件的唯一識別符。儲存貯體中的每個物件只能有一個索引鍵。儲存貯體、索引鍵和版本 ID 的組合唯一識別每個物件。因此，您可以將 Lightsail 對象存儲視為「存儲桶 + 鍵 + 版本」和對象本身之間的基本數據映射。Lightsail 物件儲存中的每個物件都可透過 Web 服務端點、值區名稱、金鑰以及選擇性的版本組合來唯一定址。例如，在中 URL `https://DOC-EXAMPLE-BUCKET.us-east-1.amazonaws.com/media/sailbot.jpg`，DOC-EXAMPLE-BUCKET 是值區的名稱，media/sailbot.jpg 是物件索引鍵名稱。

## 物件版本控制

版本控制是可讓您在相同儲存貯體中保留多個物件版本的功能。啟用版本控制功能來保留、擷取和恢復儲存貯體中所存放每個物件的各個版本。透過版本控制，您可以更輕鬆地復原失誤的使用者動作和故障的應用程式。

在建立儲存貯體時，根據預設會停用版本控制功能。啟用版本控制之後，存放在儲存貯體中的每個物件版本都會保留，直到您手動刪除所存放的版本為止。例如，如果您儲存 media/sailbot.jpg 物件，而稍後使用相同的物件索引鍵名稱儲存較大的檔案，則原始較小的物件將保留為舊版本。新的較大物件會成為目前版本。如果您決定不需要物件的先前版本，您可以將其刪除。刪除物件的目前版本時，會一併刪除物件的所有先前已存放版本。

存放的物件版本會以與已存放目前物件版本相同的方式耗用儲存貯體的儲存空間。啟用版本控制之後，您可以暫停此功能以停止存放物件版本。當您上傳新物件版本時，這也會消耗較少的儲存貯體儲存空間。暫停版本控制時，會保留已存放的物件版本，但不會保留您在暫停版本控制時上傳的新物件版本。

## 儲存貯體和物件存取

根據預設，所有物件儲存資源 (儲存貯體和物件) 皆為私有。這表示只有值區擁有者 (建立該值區的 Lightsail 帳戶) 可以存取值區及其物件。儲存貯體擁有者可選擇性地將存取許可授予他人。若要執行此操作，您可將所有物件或單個物件設定為公有，使世界上的任何人都可以讀取物件。您也可以將 Lightsail 執行個體附加至值區，或為值區建立存取金鑰，授予完整的程式設計存取權。最後，您可以授予其他 AWS 帳戶以程式設計方式對儲存貯體的唯一讀存取權。

## AWS 區域

您可以在所有可使用 Lightsail 的物件儲存貯體中建立 Lightsail 物件儲存貯體。AWS 區域 您可以選擇區域以最佳化延遲、降低成本或因應法規需求。儲存在的物件 AWS 區域 不會離開區域，除非您明確地將它們轉移到另一個區域。例如，儲存在美國西部 (奧勒岡) 區域的物件不會離開該區域。

## 管理儲存貯體和物件

Lightsail 物件儲存是特意使用最小的功能集來建置，專注於簡單性和穩固性。以下是一些管理儲存貯體和物件的元素：

- **Create buckets (建立儲存貯體)** – 建立存放資料的儲存貯體。值區是 Lightsail 物件儲存服務中的基本容器。如需詳細資訊，請參閱[建立儲存貯體](#)。
- **儲存資料** — 使用 Lightsail 主控台、AWS Command Line Interface (AWS CLI) 和 AWS APIs 將檔案上傳到值區。如需有關上傳檔案的詳細資訊，請參閱[將檔案上傳至儲存貯體](#)。
- **Download data (下載資料)** — 根據需要隨時下載已存放的物件。如需詳細資訊，請參閱[從儲存貯體中下載物件](#)。
- **Grant access (授予存取權限)** - 針對想要上傳或下載儲存貯體中資料的其他使用者 (例如軟體或個人)，授予或拒絕存取權。身分驗證機制可協助保護資料不受未經授權的存取。如需詳細資訊，請參閱[儲存貯體許可](#)。
- **Manage versioning (管理版本控制)** – 啟用版本控制功能來保留儲存貯體中所存放每個物件的各個版本。如需詳細資訊，請參閱[在儲存貯體中啟用和暫停物件版本控制](#)。
- **Monitor usage (監控用量)** - 監控儲存貯體中存放的物件數量，以及使用的儲存空間量。如需詳細資訊，請參閱[檢視儲存貯體指標](#)。
- **Change the storage plan (變更儲存計劃)** - 如果儲存貯體的使用率過高，請將其擴大；如果儲存貯體的使用率過低，則將其縮減。如需詳細資訊，請參閱[變更儲存貯體的計畫](#)。
- **Connect 儲存貯體** — 將 Lightsail 儲存貯體 Connect 到您的 WordPress 網站，以儲存網站影像和附件。您也可以將儲存貯體指定為 Lightsail 內容傳遞網路 (CDN) 發佈的來源。這可加速將儲存貯體中的物件交付給世界各地的使用者。如需詳細資訊，請參閱[教學課程：將值區 Connect 至 WordPress 執行個體](#)和[教學課程：使用含有內容傳遞網路散發的值區](#)。
- **Delete your bucket (刪除儲存貯體)** - 刪除不再使用的儲存貯體。如需詳細資訊，請參閱[刪除儲存貯體](#)。

## 建立用於物件儲存的 Lightsail 值區

當您準備好開始將檔案上傳到雲端時，請在 Amazon Lightsail 物件儲存服務中建立儲存貯體。您上傳至 Lightsail 物件儲存服務每個檔案都會儲存在 Lightsail 值區中。如需有關儲存貯體的詳細資訊，請參閱[物件儲存](#)。

## 建立 儲存貯體

請完成下列程序來建立 Lightsail 值區。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁上，選擇儲存空間索引標籤。
3. 選擇建立儲存貯體。
4. 選擇變更 AWS 區域 以選擇要在其中建立儲存貯體的區域。

我們建議您使用與計劃搭配儲存貯體使用的資源相同 AWS 區域 的方式建立值區。建立儲存貯體後，便無法變更其區域。

5. 選擇儲存貯體的儲存計劃。

儲存計劃會指定儲存貯體的每月成本、儲存空間配額和資料傳輸配額。

在每月 AWS 帳單週期內，您只能變更值區的計劃一次。如果儲存貯體的計劃一直超過儲存空間或資料傳輸配額，或儲存貯體的儲存空間或資料傳輸配額一直用量偏低，則請變更計劃。如需詳細資訊，請參閱[變更儲存貯體的計畫](#)。

6. 輸入儲存貯體的名稱。

如需值區名稱的詳細資訊，請參閱 [Amazon Lightsail 中的儲存貯體命名規則](#)。

7. 選擇 Create bucket (建立儲存貯體)。

系統會將您重新引導至新儲存貯體的管理頁面。前往本指南「後續步驟」一節瀏覽其他文件，以使用和管理儲存貯體。

## 管理儲存貯體和物件

以下是管理 Lightsail 物件儲存貯體的一般步驟：

1. 了解 Amazon Lightsail 物件儲存服務中的物件和值區。如需詳細資訊，請參閱 [Amazon Lightsail 中的物件儲存](#)。
2. 了解您可以在 Amazon Lightsail 中為您的儲存貯體提供哪些名稱。如需詳細資訊，請參閱 [Amazon Lightsail 中的儲存貯體命名規則](#)。
3. 透過建立值區開始使用 Lightsail 物件儲存服務。如需詳細資訊，請參閱 [在 Amazon Lightsail 中建立值區](#)。

4. 了解儲存貯體的安全最佳實務，以及可以為儲存貯體設定的存取許可。可以將儲存貯體中的所有物件設為公有或私有，也可以選擇將個別物件設為公有。也可以透過建立存取金鑰、將執行個體附接至儲存貯體以及授予對其他 AWS 帳戶的存取權，來授予對儲存貯體的存取權。如需詳細資訊，請參閱 [Amazon Lightsail 物件儲存的安全最佳實務](#)和[了解 Amazon Lightsail 中的儲存貯體許可](#)。

了解儲存貯體存取許可後，請參閱下列指南來授予對儲存貯體的存取權：

- [封鎖儲存貯體的公開存取](#)
  - [在 Amazon Lightsail 集團中設定儲存貯體存取權限](#)
  - [在 Amazon Lightsail 中為儲存貯體中的個別物件設定存取權限](#)
  - [在 Amazon Lightsail 中為存儲桶創建訪問密鑰](#)
  - [在 Amazon Lightsail 中設定儲存貯體的資源存取](#)
  - [在 Amazon Lightsail 中設定儲存貯體的跨帳戶存取](#)
5. 了解如何為儲存貯體啟用存取日誌記錄，以及如何使用存取日誌來稽核儲存貯體的安全性。如需詳細資訊，請參閱下列指南。
    - [Amazon Lightsail 物件儲存服務中儲存貯體的存取記錄](#)
    - [存取 Amazon Lightsail 物件儲存服務中儲存貯體的日誌格式](#)
    - [在 Amazon Lightsail 物件儲存服務中啟用儲存貯體的存取記錄](#)
    - [在 Amazon Lightsail 中使用儲存貯體的存取日誌來識別請求](#)
  6. 建立 IAM 政策，讓使用者能夠在 Lightsail 中管理值區。如需詳細資訊，請參閱[在 Amazon Lightsail 中管理儲存貯體的 IAM 政策](#)。
  7. 了解儲存貯體中物件的標記和識別方式。如需詳細資訊，請參閱[了解 Amazon Lightsail 中的物件金鑰名稱](#)。
  8. 了解如何在儲存貯體中上傳檔案及管理物件。如需詳細資訊，請參閱下列指南。
    - [將文件上傳到 Amazon Lightsail](#)
    - [使用多部分上傳將檔案上傳到 Amazon Lightsail 中的儲存貯體](#)
    - [檢視儲存貯體中 Amazon Lightsail](#)
    - [在 Amazon Lightsail 中複製或移動值區中的物件](#)
    - [從儲存貯體下 Amazon Lightsail](#)
    - [在 Amazon Lightsail 中過濾存儲桶中的對象](#)
    - [標記存儲桶中 Amazon Lightsail](#)
    - [刪除存儲桶中 Amazon Lightsail](#)

9. 啟用物件版本控制功能來保留、擷取和恢復儲存貯體中所儲存每個物件的各個版本。如需詳細資訊，請參閱在 [Amazon Lightsail 中啟用和暫停儲存貯體中的物件版本控制](#)。
10. 啟用物件版本控制之後，可以還原儲存貯體中物件的先前版本。如需詳細資訊，請參閱在 [Amazon Lightsail 中還原儲存貯體中的舊版物件](#)。
11. 監控儲存貯體的使用率。如需詳細資訊，請參閱在 [Amazon Lightsail 中檢視儲存貯體的指標](#)。
12. 設定儲存貯體指標的警示，以便在儲存貯體的使用率超過閾值時收到通知。如需詳細資訊，請參閱在 [Amazon Lightsail 中建立儲存貯體指標警示](#)。
13. 如果儲存空間和網路傳輸不足，請變更儲存貯體的儲存計畫。如需詳細資訊，請參閱在 [Amazon Lightsail 中變更儲存貯體的計畫](#)。
14. 了解如何將儲存貯體連線至其他資源。如需詳細資訊，請參閱下列教學課程。
  - [教學課程：將 WordPress 執行個體連接至 Amazon Lightsail 儲存貯體](#)
  - [教學課程：將 Amazon Lightsail 儲存貯體與 Lightsail 內容交付網路分發搭配使用](#)
15. 如果不再使用儲存貯體，請刪除它。如需詳細資訊，請參閱 [刪除儲存貯體](#)。

## 刪除 Lightsail 儲存貯體

如果您不再使用您的儲存貯體，請在 Amazon Lightsail 物件儲存服務中刪除該儲存貯體。刪除儲存貯體時，儲存貯體中的所有物件 (包括物件的存放版本和存取金鑰) 都會永久刪除。

如需有關儲存貯體的詳細資訊，請參閱 [物件儲存](#)。

### 強制刪除儲存貯體

除非您確認刪除，否則無法刪除符合以下條件之一的儲存貯體：

- 儲存貯體是分發的原始伺服器。
- 儲存貯體具有連接至其上的執行個體。
- 儲存貯體具有物件。
- 儲存貯體具有存取金鑰。

您必須確認刪除，以確保您不會中斷依賴儲存貯體的現有工作流程。例如，將媒體儲存在值區上的 WordPress 網站，或是在值區中快取和提供物件的散佈。

若要確認刪除符合前述條件之一的儲存貯體，您必須強制刪除該儲存貯體。刪除值區之前，Lightsail 服務會提示您其上存在哪些條件。如果您使用 Lightsail 主控台刪除值區，系統會顯示強制刪除值區的選

項。如果您使用 AWS CLI，則必須在提出 `delete-bucket` 請求時指定 `--force-delete` 標誌。使用 [Lightsail 主控台刪除值 AWS CLI 區以及使用](#) 本指南各節 [刪除值區的說明中都涵蓋了](#) 這兩個程序。

## 使用主控台刪除值區

請完成下列程序，以使用 Lightsail 主控台刪除值區。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁上，選擇儲存空間索引標籤。
3. 選擇您要刪除之儲存貯體的名稱。
4. 在索引標籤選單中選擇省略符號 (:) 圖示，然後選擇 Delete (刪除)。
5. 選擇 Delete Bucket (刪除儲存貯體)。
6. 在顯示的提示中，確認您的儲存貯體是否符合以下任一條件：
  - 包含物件
  - 具有存取金鑰
  - 已附加至執行個體
  - 是分發的原始伺服器

如果儲存貯體符合任一條件，則您必須選擇強制刪除。

7. 請選擇下列其中一個選項：
  - 選擇 Force delete (強制刪除) 以刪除儲存貯體，即使其符合此程序中步驟 6 列出的任何條件亦同。
  - 如果儲存貯體不符合此程序中步驟 6 列出的任何條件，則選擇 Yes, delete (是，刪除) 以刪除儲存貯體。
  - 選擇 No, cancel (否，取消) 以取消刪除。

## 使用刪除值區 AWS CLI

若要使用 AWS Command Line Interface (AWS CLI) 刪除值區，請完成下列程序。您可以使用 `delete-bucket` 命令來執行此動作。如需詳細資訊，請參閱《AWS CLI 命令參考》中的 [delete-bucket](#)。

**Note**

您必須先為 Lightsail AWS CLI 和 Amazon S3 安裝並進行設定，然後才能繼續執行此程序。如需詳細資訊，請參閱[設定 AWS CLI 定使用 Lightsail](#)。

1. 開啟命令提示或終端機視窗。
2. 在命令提示或終端機視窗中，輸入以下其中一個命令：
  - 針對不符合列於本指南[強制刪除儲存貯體](#)章節之條件的儲存貯體，請輸入以下命令以將其刪除。

```
aws lightsail delete-bucket --bucket-name BucketName
```

- 針對符合列於本指南[強制刪除儲存貯體](#)章節之條件的儲存貯體，請輸入以下命令以將其強制刪除。

```
aws lightsail delete-bucket --bucket-name BucketName --force-delete
```

在命令中，替換 *BucketName* 使用您要刪除的存儲桶的名稱。

範例：

```
aws lightsail delete-bucket --bucket-name amzn-s3-demo-bucket
```

您應該會看到類似以下範例的結果：

```
C:\>aws lightsail delete-bucket --bucket-name DOC-EXAMPLE-BUCKET
{
  "operations": [
    {
      "id": "6example-4d30-4442-ae9a-examplef4f52",
      "resourceName": "DOC-EXAMPLE-BUCKET",
      "resourceType": "Bucket",
      "createdAt": "2021-06-30T13:42:43.873000-07:00",
      "location": {
        "availabilityZone": "all",
        "regionName": "us-west-2"
      },
      "isTerminal": true,
      "operationDetails": "62example362/DOC-EXAMPLE-BUCKET/small_1_0",
      "operationType": "DeleteBucket",
      "status": "Succeeded",
      "statusChangedAt": "2021-06-30T13:42:43.873000-07:00",
      "errorCode": "",
      "errorDetails": ""
    }
  ]
}
```

## 管理儲存貯體和物件

以下是管理 Lightsail 物件儲存貯體的一般步驟：

1. 了解 Amazon Lightsail 物件儲存服務中的物件和值區。如需詳細資訊，請參閱 [Amazon Lightsail 中的物件儲存](#)。
2. 了解您可以在 Amazon Lightsail 中為您的儲存貯體提供哪些名稱。如需詳細資訊，請參閱 [Amazon Lightsail 中的儲存貯體命名規則](#)。
3. 透過建立值區開始使用 Lightsail 物件儲存服務。如需詳細資訊，請參閱 [在 Amazon Lightsail 中建立值區](#)。
4. 了解儲存貯體的安全最佳實務，以及可以為儲存貯體設定的存取許可。可以將儲存貯體中的所有物件設為公有或私有，也可以選擇將個別物件設為公有。您也可以建立存取金鑰、將執行個體附加至儲存貯體，以及授予其他AWS帳戶的存取權，以授予儲存貯體的存取權。如需詳細資訊，請參閱 [Amazon Lightsail 物件儲存的安全最佳實務和了解 Amazon Lightsail 中的儲存貯體許可](#)。

了解儲存貯體存取許可後，請參閱下列指南來授予對儲存貯體的存取權：

- [封鎖儲存貯體的公開存取](#)
- [在 Amazon Lightsail 集團中設定儲存貯體存取權限](#)

- [在 Amazon Lightsail 中為儲存貯體中的個別物件設定存取權限](#)
  - [在 Amazon Lightsail 中為存儲桶創建訪問密鑰](#)
  - [在 Amazon Lightsail 中設定儲存貯體的資源存取](#)
  - [在 Amazon Lightsail 中設定儲存貯體的跨帳戶存取](#)
5. 了解如何為儲存貯體啟用存取日誌記錄，以及如何使用存取日誌來稽核儲存貯體的安全性。如需詳細資訊，請參閱下列指南。
- [Amazon Lightsail 物件儲存服務中儲存貯體的存取記錄](#)
  - [存取 Amazon Lightsail 物件儲存服務中儲存貯體的日誌格式](#)
  - [在 Amazon Lightsail 物件儲存服務中啟用儲存貯體的存取記錄](#)
  - [在 Amazon Lightsail 中使用儲存貯體的存取日誌來識別請求](#)
6. 建立IAM政策以授與使用者在 Lightsail 中管理值區的能力。如需詳細資訊，請參閱[在 Amazon Lightsail 中管理儲存貯體的IAM政策](#)。
7. 了解儲存貯體中物件的標記和識別方式。如需詳細資訊，請參閱[了解 Amazon Lightsail 中的物件金鑰名稱](#)。
8. 了解如何在儲存貯體中上傳檔案及管理物件。如需詳細資訊，請參閱下列指南。
- [將文件上傳到 Amazon Lightsail](#)
  - [使用多部分上傳將檔案上傳到 Amazon Lightsail 中的儲存貯體](#)
  - [檢視儲存貯體中 Amazon Lightsail](#)
  - [在 Amazon Lightsail 中複製或移動值區中的物件](#)
  - [從儲存貯體下 Amazon Lightsail](#)
  - [在 Amazon Lightsail 中過濾存儲桶中的對象](#)
  - [標記存儲桶中 Amazon Lightsail](#)
  - [刪除存儲桶中 Amazon Lightsail](#)
9. 啟用物件版本控制功能來保留、擷取和恢復儲存貯體中所儲存每個物件的各個版本。如需詳細資訊，請參閱在 [Amazon Lightsail 中啟用和暫停儲存貯體中的物件版本控制](#)。
10. 啟用物件版本控制之後，可以還原儲存貯體中物件的先前版本。如需詳細資訊，請參閱在 [Amazon Lightsail 中還原儲存貯體中的舊版物件](#)。
11. 監控儲存貯體的使用率。如需詳細資訊，請參閱[在 Amazon Lightsail 中檢視儲存貯體的指標](#)。
12. 設定儲存貯體指標的警示，以便在儲存貯體的使用率超過閾值時收到通知。如需詳細資訊，請參閱[在 Amazon Lightsail 中建立儲存貯體指標警示](#)。

13. 如果儲存空間和網路傳輸不足，請變更儲存貯體的儲存計畫。如需詳細資訊，請參閱 [在 Amazon Lightsail 中變更儲存貯體的計畫](#)。
14. 了解如何將儲存貯體連線至其他資源。如需詳細資訊，請參閱下列教學課程。
  - [教學課程：將 WordPress 執行個體連接至 Amazon Lightsail 儲存貯體](#)
  - [教學課程：將 Amazon Lightsail 儲存貯體與 Lightsail 內容交付網路分發搭配使用](#)
15. 如果不再使用儲存貯體，請刪除它。如需詳細資訊，請參閱 [刪除儲存貯體](#)。

## 建立 Lightsail 物件儲存貯體存取金鑰

請使用存取金鑰建立一組憑證，以授予對儲存貯體及其物件的完整程式設計存取權。您可以在軟體或外掛程式上設定存取金鑰，使其可以使用 AWS API 和 AWS SDK 對值區具有完整讀取和寫入存取權。亦可在 AWS CLI 上設定存取金鑰。

存取金鑰是存取金鑰 ID 和私密存取金鑰為一組所組成。私密存取金鑰只有在建立時可見。如果私密存取金鑰已被複製、遺失或洩露，則應該刪除存取金鑰並建立新的存取金鑰。每個儲存貯體可擁有最多兩個存取金鑰。即使可擁有兩個存取金鑰，但在需要輪換金鑰時，儲存貯體配一個存取金鑰便已堪用。若要輪換存取金鑰，請建立新的存取金鑰，在軟體上設定並進行測試，然後刪除舊金鑰。刪除後，存取金鑰即永久消失且無法復原。您只能改用新的存取金鑰。

如需有關許可選項的詳細資訊，請參閱 [儲存貯體許可](#)。如需安全最佳實務的詳細資訊，請參閱 [物件儲存的安全最佳實務](#)。如需有關儲存貯體的詳細資訊，請參閱 [物件儲存](#)。

### 建立儲存貯體的存取金鑰

請完成下列程序來建立儲存貯體的存取金鑰。

1. 登入主 [Lightsail](#) 台。
2. 在 Lightsail 首頁上，選擇儲存空間索引標籤。
3. 選擇您要設定存取許可之儲存貯體的名稱。
4. 選擇許可索引標籤標籤。

該頁面的 Access keys (存取金鑰) 區段會顯示儲存貯體的現有存取金鑰 (如果有)。

5. 選擇 Create access key (建立存取金鑰)，為儲存貯體建立新的存取金鑰。

**Note**

您亦可對要刪除的金鑰選擇垃圾桶圖示，以刪除現有的存取金鑰。

6. 在出現的提示中，選擇 Yes, create (是，建立)，確認您要建立新的存取金鑰。否則，請選擇 No, cancel (否，取消)。
7. 出現成功提示時，記下存取金鑰 ID。
8. 選擇 Show secret access key (顯示私密存取金鑰) 以檢視私密存取金鑰，並記下金鑰。私密存取金鑰將不再顯示。

**Important**

請將存取金鑰 ID 和私密存取金鑰存放在安全之處。如果金鑰洩露，則應該將其刪除並建立新的金鑰。

9. 選擇 Continue (繼續) 以完成操作。

新的存取金鑰會在頁面的 Access keys (存取金鑰) 區段列出。如果存取金鑰洩露或遺失，請將其刪除，並且建立新的存取金鑰。

**Note**

每個存取金鑰旁邊顯示的上次使用時間欄位註明了上次使用金鑰的時間。未使用的金鑰會顯示連接號。展開存取金鑰節點以檢視服務 AWS 區域 以及上次使用金鑰的位置。

## 限制公開存取 Lightsail 值區和物件

Amazon Simple Storage Service (Amazon S3) 是一種物件儲存服務，客戶可以使用此服務來儲存與保護資料。Amazon Lightsail 物件儲存服務建立在 Amazon S3 技術之上。Amazon S3 提供帳戶層級封鎖公有存取，讓您能用來限制對 AWS 帳戶中的所有 S3 儲存貯體的公有存取。無論現有的個別儲存貯體和物件許可為何，帳戶層級區塊公開存取都可以將所有 S3 儲存貯體設為 AWS 帳戶 私有儲存貯體。

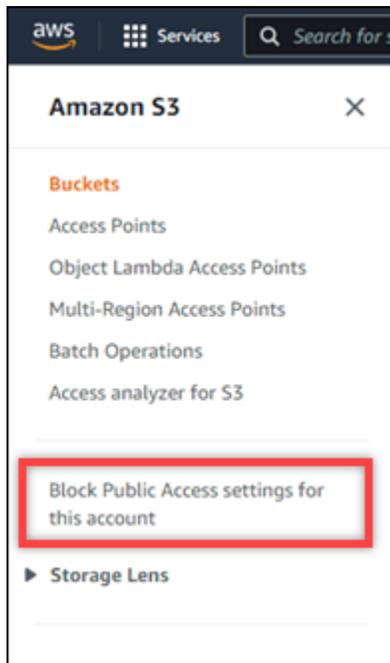
允許或拒絕公開存取時，Lightsail 物件儲存貯體會考慮下列事項：

- 儲存 Lightsail 體存取權限。如需詳細資訊，請參閱[儲存貯體許可](#)。
- Amazon S3 帳戶層級區塊公開存取組態，這會覆寫 Lightsail 儲存貯體存取權限。

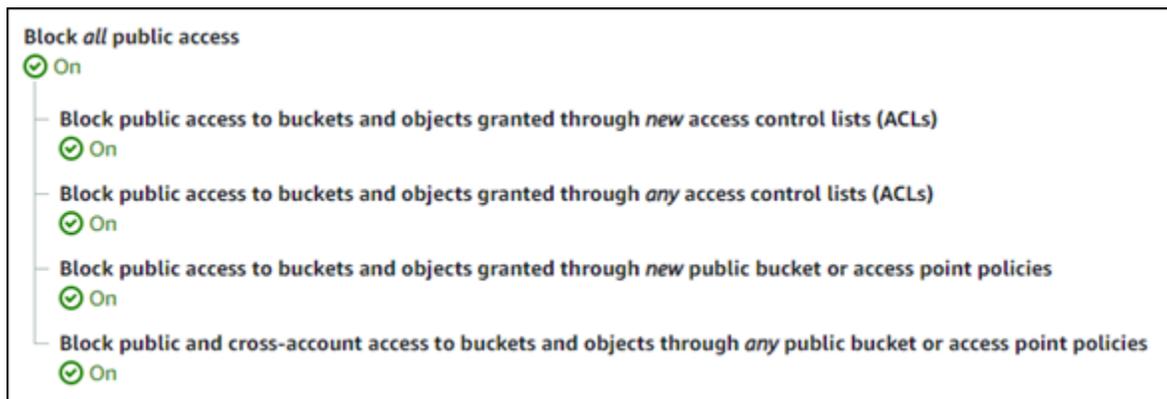
如果您開啟帳戶層級封鎖 Amazon S3 中的所有公開存取，您的公用 Lightsail 儲存貯體和物件會變成私有且不再可公開存取。

## 為您的帳戶設定封鎖公有存取

您可以使用 Amazon S3 主控台、AWS Command Line Interface (AWS CLI)、開 AWS 發套件和 REST API 來設定區塊公開存取設定。可以在 Amazon S3 主控台的導覽窗格中存取帳戶層級封鎖公有存取功能，如以下範例所示。



Amazon S3 主控台提供的設定可封鎖所有公有存取、封鎖透過新的或任何存取控制清單授予的公有存取，以及封鎖透過新的或任何公有儲存貯體或存取點政策授予的對儲存貯體和物件的公有存取。



可以在 Amazon S3 主控台中將每項設定設為開啟或關閉。在 API 中，對應的設定為 TRUE (開啟) 或 FALSE (關閉)。下列各節說明每個設定對 S3 儲存貯體和 Lightsail 值區的影響。

**Note**

以下章節會提到存取控制清單 (ACL)。ACL 定義擁有或能夠存取儲存貯體或個別物件的使用者。如需詳細資訊，請參閱《Amazon S3 使用者指南》中的[存取控制清單概觀](#)。

- 封鎖所有公開存取 — 開啟此設定即可封鎖對 S3 儲存貯體、Lightsail 儲存貯體及其對應物件的所有公開存取。此設定包含以下所有設定。當您開啟此設定時，只有您 (儲存貯體擁有者) 和授權的使用者能夠存取您的儲存貯體及其物件。只能在 Amazon S3 主控台中開啟此設定。它在 Amazon S3 API 或 AWS 開發套件中不可用。AWS CLI
- 封鎖透過新的存取控制清單 (ACL) 授予的對儲存貯體和物件的公有存取 – 開啟此設定以阻止在儲存貯體和物件上放置公有 ACL。此設定不會影響現有的 ACL。因此，已經具有公有 ACL 的物件仍將保持為公有。由於儲存貯體存取許可設定為 All objects are public and read-only (所有物件皆為公有且唯讀)，故此設定也不會對公有物件造成影響。此設定在 Amazon S3 API 中標示為 BlockPublicAcls。

**Note**

WordPress 將媒體置於 Lightsail 值區的外掛程式 (例如卸載媒體燈外掛程式) 可能會在此設定開啟時停止運作。這是因為大多數 WordPress 外掛程式會在物件上設定公開讀取 ACL。WordPress 切換物件 ACL 的外掛程式也可能會停止運作。

- 封鎖透過任何存取控制清單 (ACL) 授予的對儲存貯體和物件的公有存取 – 開啟此設定以忽略公有 ACL 並封鎖對儲存貯體和物件的公有存取。此設定允許將公有 ACL 放置在儲存貯體和物件上，但在授予存取時會忽略。對於 Lightsail 值區，將值區的存取權限設定為「所有」物件都是公用且唯讀的，或者將個別物件的權限設定為「公用」(唯讀) 等同於將公用 ACL 置於其中一個物件上。此設定在 Amazon S3 API 中標示為 IgnorePublicAcls。
- 封鎖透過新公用值區或存取點原則授與之值區和物件的公用存取權限 — 開啟此設定即可封鎖 Lightsail 值區中設定「所有物件都是公用和唯讀值區存取」權限。此設定不會影響已設定為 All objects are public and read-only (所有物件皆為公有且唯讀) 存取許可的儲存貯體。此設定在 Amazon S3 API 中標示為 BlockPublicPolicy。
- 透過任何公用值區或存取點政策封鎖值區和物件的公開和跨帳戶存取 — 開啟此設定即可將所有 Lightsail 值區設為私有。這會使所有 Lightsail 值區設定為私有，即使它們設定為「所有物件都是公用的」和「唯讀值區」存取權限。此設定在 Amazon S3 API 中標示為 RestrictPublicBuckets。

### Important

此設定也會封鎖在 Lightsail 儲存貯體上設定的跨帳戶存取，該儲存貯體也設定了 Lightsail 中的「所有物件都是公用」和「唯讀值區存取」權限。若要繼續允許跨帳戶存取，請確保在 Lightsail 中使用「所有物件都是私有儲存貯體存取」權限設定 Lightsail 儲存貯體，然後透過 Amazon S3 中的任何公用儲存貯體或存取點政策開啟封鎖公用和跨帳戶存取值區和物件。

如需有關封鎖公有存取及如何進行設定的詳細資訊，請參閱《Amazon S3 使用者指南》中的下列資源：

- [封鎖對 Amazon S3 儲存體的公開存取權](#)
- [為您的帳戶設定封鎖公有存取](#)

使用 Lightsail 主控台 AWS CLI、AWS 開發套件和 REST API 來設定 Lightsail 值區的存取權限。如需詳細資訊，請參閱[儲存貯體許可](#)。

### Note

Lightsail 使用服務連結角色從 Amazon S3 取得目前的帳戶層級區塊公開存取組態，並將其套用至 Lightsail 物件儲存資源。在 Amazon S3 中設定區塊公開存取之後，請等待至少一小時，使其在 Lightsail 中生效。如需詳細資訊，請參閱[服務連結角色](#)。

## 管理儲存貯體和物件

以下是管理 Lightsail 物件儲存貯體的一般步驟：

1. 了解 Amazon Lightsail 物件儲存服務中的物件和值區。如需詳細資訊，請參閱 [Amazon Lightsail 中的物件儲存](#)。
2. 了解您可以在 Amazon Lightsail 中為您的儲存貯體提供哪些名稱。如需詳細資訊，請參閱 [Amazon Lightsail 中的儲存貯體命名規則](#)。
3. 透過建立值區開始使用 Lightsail 物件儲存服務。如需詳細資訊，請參閱 [在 Amazon Lightsail 中建立值區](#)。

4. 了解儲存貯體的安全最佳實務，以及可以為儲存貯體設定的存取許可。可以將儲存貯體中的所有物件設為公有或私有，也可以選擇將個別物件設為公有。也可以透過建立存取金鑰、將執行個體附接至儲存貯體以及授予對其他 AWS 帳戶的存取權，來授予對儲存貯體的存取權。如需詳細資訊，請參閱 [Amazon Lightsail 物件儲存的安全最佳實務](#)和[了解 Amazon Lightsail 中的儲存貯體許可](#)。

了解儲存貯體存取許可後，請參閱下列指南來授予對儲存貯體的存取權：

- [封鎖儲存貯體的公開存取](#)
  - [在 Amazon Lightsail 集團中設定儲存貯體存取權限](#)
  - [在 Amazon Lightsail 中為儲存貯體中的個別物件設定存取權限](#)
  - [在 Amazon Lightsail 中為存儲桶創建訪問密鑰](#)
  - [在 Amazon Lightsail 中設定儲存貯體的資源存取](#)
  - [在 Amazon Lightsail 中設定儲存貯體的跨帳戶存取](#)
5. 了解如何為儲存貯體啟用存取日誌記錄，以及如何使用存取日誌來稽核儲存貯體的安全性。如需詳細資訊，請參閱下列指南。
    - [Amazon Lightsail 物件儲存服務中儲存貯體的存取記錄](#)
    - [存取 Amazon Lightsail 物件儲存服務中儲存貯體的日誌格式](#)
    - [在 Amazon Lightsail 物件儲存服務中啟用儲存貯體的存取記錄](#)
    - [在 Amazon Lightsail 中使用儲存貯體的存取日誌來識別請求](#)
  6. 建立 IAM 政策，讓使用者能夠在 Lightsail 中管理值區。如需詳細資訊，請參閱[在 Amazon Lightsail 中管理儲存貯體的 IAM 政策](#)。
  7. 了解儲存貯體中物件的標記和識別方式。如需詳細資訊，請參閱[了解 Amazon Lightsail 中的物件金鑰名稱](#)。
  8. 了解如何在儲存貯體中上傳檔案及管理物件。如需詳細資訊，請參閱下列指南。
    - [將文件上傳到 Amazon Lightsail](#)
    - [使用多部分上傳將檔案上傳到 Amazon Lightsail 中的儲存貯體](#)
    - [檢視儲存貯體中 Amazon Lightsail](#)
    - [在 Amazon Lightsail 中複製或移動值區中的物件](#)
    - [從儲存貯體下 Amazon Lightsail](#)
    - [在 Amazon Lightsail 中過濾存儲桶中的對象](#)
    - [標記存儲桶中 Amazon Lightsail](#)
    - [刪除存儲桶中 Amazon Lightsail](#)

9. 啟用物件版本控制功能來保留、擷取和恢復儲存貯體中所儲存每個物件的各個版本。如需詳細資訊，請參閱在 [Amazon Lightsail 中啟用和暫停儲存貯體中的物件版本控制](#)。
10. 啟用物件版本控制之後，可以還原儲存貯體中物件的先前版本。如需詳細資訊，請參閱在 [Amazon Lightsail 中還原儲存貯體中的舊版物件](#)。
11. 監控儲存貯體的使用率。如需詳細資訊，請參閱在 [Amazon Lightsail 中檢視儲存貯體的指標](#)。
12. 設定儲存貯體指標的警示，以便在儲存貯體的使用率超過閾值時收到通知。如需詳細資訊，請參閱在 [Amazon Lightsail 中建立儲存貯體指標警示](#)。
13. 如果儲存空間和網路傳輸不足，請變更儲存貯體的儲存計畫。如需詳細資訊，請參閱在 [Amazon Lightsail 中變更儲存貯體的計畫](#)。
14. 了解如何將儲存貯體連線至其他資源。如需詳細資訊，請參閱下列教學課程。
  - [教學課程：將 WordPress 執行個體連接至 Amazon Lightsail 儲存貯體](#)
  - [教學課程：將 Amazon Lightsail 儲存貯體與 Lightsail 內容交付網路分發搭配使用](#)
15. 如果不再使用儲存貯體，請刪除它。如需詳細資訊，請參閱 [刪除儲存貯體](#)。

## 使用存取記錄追蹤物件儲存貯體要求

存取記錄可針對 Amazon Lightsail 物件儲存服務中對儲存貯體發出的請求提供詳細記錄。這資訊可能包含要求類型、要求中指定的資源，以及要求的處理時間和日期。存取日誌對許多應用程式來說，都是個很有用的資料。舉例來說，存取記錄資訊在安全與存取稽核中相當實用。您也可藉由該資訊了解自己的客戶群。

### 內容

- [啟用日誌傳送需要什麼？](#)
- [日誌物件金鑰格式](#)
- [交付日誌的方式？](#)
- [存取日誌傳送最佳作法](#)
- [儲存貯體記錄狀態變更會在一段時間後生效](#)

## 啟用日誌傳送需要什麼？

啟用日誌傳送之前，請考慮下列事項。如需詳細資訊，請參閱 [啟用儲存貯體存取記錄](#)。

1. 識別日誌的目標儲存貯體。此值區是您希望 Lightsail 將存取記錄檔儲存為物件的位置。來源儲存貯體和目標儲存貯體必須位於同一 AWS 區域，並且由相同帳戶擁有。

您可將日誌交付給所有您擁有的儲存貯體，在同一的區域當做來源儲存貯體，包括來源儲存貯體本身。但為了更簡易進行記錄管理，建議您將存取記錄儲存在不同的儲存貯體中。

當來源儲存貯體和目標儲存貯體位於同一個儲存貯體，會為儲存貯體建立額外的日誌。這方式可能不甚理想，因為它可能會導致您的儲存體耗用稍微增加。此外，額外的日誌可能會增加您的搜尋困難。若您選擇將存取日誌儲存於來源儲存貯體中，建議您為日誌物件金鑰指定字首，以常見的字串和日誌物件為字首，以便輕鬆地識別。當多個儲存貯體登入相同的目標儲存貯體時，[金鑰前綴](#)也可用來區分來源儲存貯體。

- (選用) 識別日誌物件金鑰的字首。此字首方便您尋找日誌物件。例如，如果您指定前置詞值logs/，Lightsail 建立的每個記錄物件都會以其索引鍵中的logs/前置詞開頭。需要使用結尾斜線 / 來表示字首的結尾。以下是包含 logs/ 字首的日誌物件金鑰範例：

```
logs/2021-11-31-21-32-16-E568B2907131C0C0
```

## 日誌物件金鑰格式

Lightsail 會針對其在目標值區中上傳的記錄物件使用下列物件金鑰格式：

```
TargetPrefix/YYYY-mm-DD-HH-MM-SS-UniqueString
```

在金鑰中，YYYY、mm、DD、HH、MM 與 SS 分別是交付日誌檔的年、月、日、時、分與秒的數字。這些日期和時間都使用國際標準時間 (UTC)。

在特定時間交付的日誌檔，會包含該時間之前的任何時間點所寫入之記錄。但無法得知某特定時間間隔的所有日誌記錄是否皆已交付。

金鑰的 UniqueString 元件的存在原因，就是為了要避免覆寫檔案。它沒有任何意義，所以日誌處理軟體應會忽略它。

## 交付日誌的方式？

Lightsail 會定期收集存取日誌記錄、合併記錄檔中的記錄，然後將記錄檔做為記錄物件上傳至目標值區。若您對多個傳遞到同一個目標儲存貯體的來源儲存貯體啟用了記錄，則此目標儲存貯體就會有所有這些來源儲存貯體的存取日誌。但每個日誌物件都會回報特定來源儲存貯體的存取日誌記錄。

## 存取日誌傳送最佳作法

存取日誌記錄會依最佳作法交付。大多數儲存貯體的要求，為日誌記錄結果適合組態，交付日誌記錄。大多數的日誌記錄會於記錄後的數小時內交付，但也可以常交付。

並不保證存取記錄的完成程度與時間先後順序。特定要求的日誌記錄，可能會在實際處理要求之後很久才交付，或者有可能完全不會交付。存取日誌的目的在於讓您能了解儲存貯體流量的真實狀態。雖然日誌記錄極少會缺失，但存取記錄並不代表所有請求的完整記錄。

## 儲存貯體記錄狀態變更會在一段時間後生效

記錄儲存貯體狀態的變更，要一段時間後才會實際影響到日誌檔交付。例如，若已啟用儲存貯體記錄，則在接下來的一小時內提出之要求，可能有些會記錄下來，有些則不會。若您將目標儲存貯體記錄，從儲存貯體 A 變更為儲存貯體 B，則接下來的一小時內，有些日誌可能會繼續交付到儲存貯體 A，而有些則可能會交付到新的目標儲存貯體 B。在任何情況之下，新的設定最後都會生效，您無須採取任何動作。

### 主題

- [使用 Lightsail 值區記錄分析物件儲存空間存取](#)
- [啟用儲存貯體存取記錄](#)
- [使用 Lightsail 中的 Amazon Athena 分析值區存取日誌](#)

## 使用 Lightsail 值區記錄分析物件儲存空間存取

存取記錄可針對 Amazon Lightsail 物件儲存服務中對儲存貯體發出的請求提供詳細記錄。您可以使用存取日誌進行安全和存取稽核，或了解您的客戶群。本節說明存取日誌檔案的格式和其他詳細資訊。如需有關日誌基本概念的詳細資訊，請參閱[儲存貯體存取日誌](#)。

存取日誌檔是由一連串換行分隔日誌記錄所組成。每筆日誌記錄都代表一項要求，且由多個空格分隔欄位所組成。

以下為五筆日誌記錄所組成的日誌範例。

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
amzn-s3-demo-bucket [06/Feb/2019:00:00:38 +0000] 192.0.2.3
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be 3E57427F3EXAMPLE
REST.GET.VERSIONING - "GET /amzn-s3-demo-bucket?versioning HTTP/1.1" 200 - 113 - 7 -
```

```
"-" "S3Console/0.4" - s9lzHYrFp76ZVxRcpX9+5cjAnEH2R0uNkd2BHfIa6UkFVdtjf5mKR3/eTPFvsiP/
XV/VLi31234= SigV2 ECDHE-RSA-AES128-GCM-SHA256 AuthHeader amzn-s3-demo-bucket.s3.us-
west-1.amazonaws.com TLSV1.1
```

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
amzn-s3-demo-bucket [06/Feb/2019:00:00:38 +0000] 192.0.2.3
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be 891CE47D2EXAMPLE
REST.GET.LOGGING_STATUS - "GET /amzn-s3-demo-bucket?logging HTTP/1.1" 200 -
242 - 11 - "-" "S3Console/0.4" - 9vKBE6vMhrNiWHZmb2L0mX0cqPGzQ0I5XLnCtZNPxev+Hf
+7tpT6sxDwDty4LHBU0ZJG96N1234= SigV2 ECDHE-RSA-AES128-GCM-SHA256 AuthHeader amzn-s3-
demo-bucket.s3.us-west-1.amazonaws.com TLSV1.1
```

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
amzn-s3-demo-bucket [06/Feb/2019:00:00:38 +0000] 192.0.2.3
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be A1206F460EXAMPLE
REST.GET.BUCKETPOLICY - "GET /amzn-s3-demo-bucket?policy HTTP/1.1" 404
NoSuchBucketPolicy 297 - 38 - "-" "S3Console/0.4" - BNaBsXZQQDbssi6xMBdBU2sLt
+Yf5kZDmeBUP35sFoKa3sLLeMC78iwEIWxs99CRUrbS4n11234= SigV2 ECDHE-RSA-AES128-GCM-SHA256
AuthHeader amzn-s3-demo-bucket.s3.us-west-1.amazonaws.com TLSV1.1
```

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
amzn-s3-demo-bucket [06/Feb/2019:00:01:00 +0000] 192.0.2.3
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be 7B4A0FABBEXAMPLE
REST.GET.VERSIONING - "GET /amzn-s3-demo-bucket?versioning HTTP/1.1" 200 -
113 - 33 - "-" "S3Console/0.4" - Ke1bUcazaN1jWuU1PJaxF64cQVpUEhoZKEG/hmy/gijN/
I1DeWqDfFvnpbybfEseEME/u7ME1234= SigV2 ECDHE-RSA-AES128-GCM-SHA256 AuthHeader amzn-s3-
demo-bucket.s3.us-west-1.amazonaws.com TLSV1.1
```

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
amzn-s3-demo-bucket [06/Feb/2019:00:01:57 +0000] 192.0.2.3
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
DD6CC733AEXAMPLE REST.PUT.OBJECT s3-dg.pdf "PUT /amzn-s3-demo-bucket/
s3-dg.pdf HTTP/1.1" 200 - - 4406583 41754 28 "-" "S3Console/0.4" -
10S62Zv81kBW7BB6SX4XJ48o6kpc16LPwEoizZQqxJd5qDSCTLX0TgS37kYUBKQW3+bPdrg1234= SigV4
ECDHE-RSA-AES128-SHA AuthHeader amzn-s3-demo-bucket.s3.us-west-1.amazonaws.com TLSV1.1
```

### Note

任何日誌檔欄位都可以設成 - (破折號)，指出資料為未知或不可用，或欄位不適用於此要求。

## 內容

- [日誌記錄欄位](#)
- [複製操作的其他日誌](#)
- [自訂存取日誌資訊](#)
- [可擴展存取日誌格式的程式設計考量](#)

## 日誌記錄欄位

下列清單說明日誌記錄欄位。

### 存取點 ARN (Amazon 資源名稱)

請求存取點的 Amazon 資源名稱 (ARN)。如果存取點 ARN 格式錯誤或未使用，則欄位將包含「-」。如需存取點的詳細資訊，請參閱[使用存取點](#)。如需有關的詳細資訊 ARNs，請參閱 AWS 一般參考中有關[Amazon 資源名稱 \(ARN\)](#) 的主題。

### 項目範例

```
arn:aws:s3:us-east-1:123456789012:accesspoint/example-AP
```

### 儲存貯體擁有者

來源儲存貯體擁有者的正式使用者 ID。標準用戶 ID 是另一種形式的 AWS 帳戶 ID。如需有關規範使用者 ID 的詳細資訊，請參閱 AWS 一般參[AWS 考資料中的帳戶識別碼](#)。如需如何尋找帳戶的標準使用者 ID 的詳細資訊，請參閱[尋找帳戶的標準使用者 ID](#)。AWS

### 項目範例

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
```

### 儲存貯體

要求處理對象的儲存貯體名稱。如果系統收到格式錯誤的要求且無法判斷儲存貯體，則儲存貯體要求就不會出現在任何存取日誌中。

### 項目範例

```
amzn-s3-demo-bucket
```

## Time (時間)

收到請求的時間；這些日期和時間均為協調世界時 (UTC)。格式，使用 *strftime()* 術語，如下所示：  
`[%d/%b/%Y:%H:%M:%S %z]`

### 項目範例

```
[06/Feb/2019:00:00:38 +0000]
```

## 遠端 IP

申請者清楚的網際網路位址。中間代理伺服器與防火牆可能會模糊提出要求電腦的真實位址。

### 項目範例

```
192.0.2.3
```

## 要求者

要求者的正式使用者 ID，或未經驗證要求者的 -。如果請求者是 IAM 使用者，此欄位會傳回請求者的 IAM 使用者名稱以及使用 IAM 者所屬的 AWS root 帳戶。此識別符與用於存取控制目的的識別符相同。

### 項目範例

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
```

## 請求 ID

Lightsail 所產生的字串，可唯一識別每個要求。

### 項目範例

```
3E57427F33A59F07
```

## 操作

這裡列出的操作會宣告為

SOAP.*operation*、REST.*HTTP\_method.resource\_type*、WEBSITE.*HTTP\_method.resource\_type*  
或 BATCH.DELETE.OBJECT。

## 項目範例

```
REST.PUT.OBJECT
```

## 索引鍵

請求的「key」部分，URL編碼，或「-」，如果操作不採取關鍵參數。

## 項目範例

```
/photos/2019/08/puppy.jpg
```

## 請求-URI

請求-請HTTP求消息的—URI部分。

## 項目範例

```
"GET /amzn-s3-demo-bucket/photos/2019/08/puppy.jpg?x-foo=bar HTTP/1.1"
```

## HTTP狀態

響應的數字HTTP狀態碼。

## 項目範例

```
200
```

## 錯誤代碼

Amazon S3 [錯誤代碼](#)；或者，如果沒有發生錯誤，則為「-」。

## 項目範例

```
NoSuchBucket
```

## 已傳送的位元組

傳送的回應位元組數 (不包括HTTP通訊協定額外負荷)，若為零，則為「-」。

## 項目範例

```
2662992
```

## 物件大小

所提及之物件的總大小。

## 項目範例

```
3462992
```

## 總時間

從儲存貯體角度計算的要求所經過的毫秒數。此值是從收到您要求的時間開始，計算到回應傳送出最後一組位元組的時間。因為網路延遲，從用戶端角度計算的時間可能較長。

## 項目範例

```
70
```

## 周轉時間

Lightsail 處理您的要求所花費的毫秒數。此值是從收到您要求的最後位元組的時間開始，計算到回應傳送出第一組位元組的時間。

## 項目範例

```
10
```

## Referer

HTTP裁判者標頭的值 (如果存在)。HTTP用戶代理 (例如，瀏覽器) 通常在提出請求時將此標頭設置為鏈接或嵌入頁面URL的。

## 項目範例

```
"http://www.amazon.com/webservices"
```

## 使用者代理程式

HTTP使用者代理程式標頭的值。

### 項目範例

```
"curl/7.15.1"
```

## 版本 Id

要求的版本 ID；或者，如果操作不採用 `versionId` 參數則為 `-`。

### 項目範例

```
3HL4kqtJvjVBH40NrjfkD
```

## 主機 Id

`x-amz-id-2` 或 Lightsail 延伸要求識別碼。

### 項目範例

```
s91zHYrFp76ZVxRcpX9+5cjAnEH2R0uNkd2BHfIa6UkFVdtjf5mKR3/eTPFvsiP/XV/VLi31234=
```

## 簽章版本

簽章版本 (SigV2 或 SigV4)，用來驗證請求或未驗證請求的 `-`。

### 項目範例

```
SigV2
```

## 密碼套件

為HTTPS請求或用於協商的安全套接字層 (SSL) 密碼。 - HTTP

### 項目範例

```
ECDHE-RSA-AES128-GCM-SHA256
```

## 身分驗證類型

用於驗證標頭的請求驗證類型，AuthHeader用QueryString於查詢字串 (預先簽署URL) 或未驗證要求的要-求驗證類型。

### 項目範例

```
AuthHeader
```

## 主機標頭

用來連線至 Lightsail 的端點。

### 項目範例

```
s3.us-west-2.amazonaws.com
```

## TLS版本

用戶端協商的傳輸層安全性 (TLS) 版本。此值為下列其中一項：TLSv1、TLSv1.1、TLSv1.2; 或者-如果TLS未使用。

### 項目範例

```
TLSv1.2
```

## 複製操作的其他記錄

複製操作包括 GET 與 PUT。因此，執行複製操作時，我們會記錄兩筆記錄。上節說明與操作的 PUT 部分有關的欄位。下列清單說明記錄中與複製操作的 GET 部分有關的欄位。

### 儲存貯體擁有者

存放要複製物件之儲存貯體的正式使用者 ID。標準用戶 ID 是另一種形式的AWS帳戶 ID。如需有關規範使用者 ID 的詳細資訊，請參閱AWS一般參[AWS考資料中的帳戶識別碼](#)。如需如何尋找帳戶的標準使用者 ID 的詳細資訊，請參閱[尋找帳戶的標準使用者 ID](#)。AWS

### 項目範例

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
```

## 儲存貯體

存放要複製物件的儲存貯體名稱。

### 項目範例

```
amzn-s3-demo-bucket
```

## Time (時間)

收到請求的時間；這些日期和時間均為協調世界時間 (UTC)。使用 `strftime()` 術語的格式如下：`[%d/%B/%Y:%H:%M:%S %z]`

### 項目範例

```
[06/Feb/2019:00:00:38 +0000]
```

## 遠端 IP

申請者清楚的網際網路位址。中間代理伺服器與防火牆可能會模糊提出要求電腦的真實位址。

### 項目範例

```
192.0.2.3
```

## 要求者

要求者的正式使用者 ID，或未經驗證要求者的 `-`。如果要求者是 IAM 使用者，此欄位會傳回要求者的 IAM 使用者名稱以及使用 IAM 者所屬的 AWS root 帳戶。此識別符與用於存取控制目的的識別符相同。

### 項目範例

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
```

## 請求 ID

Lightsail 所產生的字串，可唯一識別每個要求。

### 項目範例

```
3E57427F33A59F07
```

## 操作

這裡列出的操作會宣告為

SOAP.*operation*、REST.*HTTP\_method.resource\_type*、WEBSITE.*HTTP\_method.resource\_type*  
或 BATCH.DELETE.OBJECT。

## 項目範例

```
REST.COPY.OBJECT_GET
```

## 索引鍵

要複製的物件的「金鑰」；或者，如果操作不採用金鑰參數則為「-」。

## 項目範例

```
/photos/2019/08/puppy.jpg
```

## 請求-URI

請求-請HTTP求消息的—URI部分。

## 項目範例

```
"GET /amzn-s3-demo-bucket/photos/2019/08/puppy.jpg?x-foo=bar"
```

## HTTP狀態

複製作業GET部分的數字HTTP狀態碼。

## 項目範例

```
200
```

## 錯誤代碼

複製操作之 GET 部分的 Amazon S3 錯誤代碼；或者，如未發生任何錯誤則為「-」。

## 項目範例

```
NoSuchBucket
```

## 已傳送的位元組

傳送的回應位元組數 (不包括HTTP通訊協定額外負荷)，若為零，則為「-」。

## 項目範例

```
2662992
```

## 物件大小

所提及之物件的總大小。

## 項目範例

```
3462992
```

## 總時間

從儲存貯體角度計算的要求所經過的毫秒數。此值是從收到您要求的時間開始，計算到回應傳送出最後一組位元組的時間。因為網路延遲，從用戶端角度計算的時間可能較長。

## 項目範例

```
70
```

## 周轉時間

Lightsail 處理您的要求所花費的毫秒數。此值是從收到您要求的最後位元組的時間開始，計算到回應傳送出第一組位元組的時間。

## 項目範例

```
10
```

## Referer

HTTP 裁判者標頭的值 (如果存在)。HTTP 用戶代理 (例如, 瀏覽器) 通常在提出請求時將此標頭設置為鏈接或嵌入頁面 URL 的。

#### 項目範例

```
"http://www.amazon.com/webservices"
```

#### 使用者代理程式

HTTP 使用者代理程式標頭的值。

#### 項目範例

```
"curl/7.15.1"
```

#### 版本 Id

複製的物件的版本 ID, 如果 `x-amz-copy-source` 標頭並未將 `versionId` 參數指定為複製來源的一部分, 則為「-」。

#### 項目範例

```
3HL4kqtJvjVBH40N1rjfkd
```

#### 主機 Id

`x-amz-id-2` 或 Lightsail 延伸要求識別碼。

#### 項目範例

```
s91zHYrFp76ZVxRcpX9+5cjAnEH2R0uNkd2BHfIa6UkFVdtjf5mKR3/eTPFvsiP/XV/VLi31234=
```

#### 簽章版本

簽章版本 (SigV2 或 SigV4), 用來驗證請求或未驗證請求的 -。

#### 項目範例

```
SigV2
```

#### 密碼套件

為HTTPS請求或用於協商的安全套接字層 ( SSL ) 密碼。 - HTTP

### 項目範例

```
ECDHE-RSA-AES128-GCM-SHA256
```

### 身分驗證類型

用於驗證標頭的要求驗證類型，AuthHeader用QueryString於查詢字串 (預先簽署URL) 或未驗證要求的要-求驗證類型。

### 項目範例

```
AuthHeader
```

### 主機標頭

用來連線至 Lightsail 的端點。

### 項目範例

```
s3.us-west-2.amazonaws.com
```

### TLS版本

用戶端協商的傳輸層安全性 (TLS) 版本。此值為下列其中一項：TLSv1、TLSv1.1、TLSv1.2; 或者-如果TLS未使用。

### 項目範例

```
TLSv1.2
```

## 客戶存取日誌資訊

您可以包含要存放在請求存取日誌記錄中的自訂資訊。若要這麼做，請將自訂查詢字串參數新增至要URL求的。Lightsail 會忽略以「x-」開頭的查詢字串參數，但會將這些參數納入要求的存取記錄記錄中，做為記錄檔記錄Request-URI欄位的一部分。

例如，GET 請求的 "s3.amazonaws.com/amzn-s3-demo-bucket/photos/2019/08/puppy.jpg?x-user=johndoe" 運作方式與 "s3.amazonaws.com/amzn-s3-demo-bucket/

photos/2019/08/puppy.jpg" 請求相同，不同之處在於該 "x-user=johndoe" 字串包含在關聯日誌記錄的 Request-URI 欄位中。此功能僅在REST介面中提供。

## 可擴展存取日誌格式的程式設計考量

有時候，我們可能要在每行結尾新增欄位，擴展存取日誌記錄的格式。因此，您應編寫任何解析存取日誌的程式碼，來處理其可能不理解的結尾欄位。

## 啟用儲存貯體存取記錄

存取記錄可針對 Amazon Lightsail 物件儲存服務中對儲存貯體發出的請求提供詳細記錄。存取日誌對許多應用程式來說，都是個很有用的資料。舉例來說，存取記錄資訊在安全與存取稽核中相當實用。您也可藉由該資訊了解自己的客戶群。

根據預設，Lightsail 不會收集值區的存取記錄。啟用記錄功能時，Lightsail 會將來源儲存貯體的存取記錄傳送至您選擇的目標儲存貯體。來源值區和目標值區都必須位於相同 AWS 區域 且由相同帳戶擁有。

存取日誌記錄包含對儲存貯體提出要求，內有詳細資訊。這資訊可能包含要求類型、要求中指定的資源，以及要求的處理時間和日期。在本指南中，我們將說明如何使用 Lightsail API、AWS Command Line Interface (AWS CLI) 或來啟用或AWSSDKs停用值區的存取記錄。

如需有關日誌基本概念的詳細資訊，請參閱[儲存貯體存取日誌](#)。

### 內容

- [存取記錄的成本](#)
- [使用 AWS CLI啟用存取記錄](#)
- [使用 AWS CLI停用存取記錄](#)

## 存取記錄的成本

啟用儲存貯體的存取記錄沒有額外的費用。不過，系統傳遞至儲存貯體的日誌檔會耗用儲存空間。您隨時都可刪除日誌檔。當日誌儲存貯體的資料傳輸在其設定的每月限額內時，我們不會估算日誌檔傳遞的資料傳輸費。

您的目標儲存貯體不應啟用存取記錄。您可將日誌交付給所有您擁有的儲存貯體，在同一的區域當做來源儲存貯體，包括來源儲存貯體本身。不過，為了更簡易進行記錄管理，建議您將存取記錄儲存在不同的儲存貯體中。

## 使用啟用存取記錄 AWS CLI

若要啟用值區的存取記錄功能，建議您在每個擁有值區的記錄值區中建立專用 AWS 區域 的記錄值區。然後將存取日誌傳遞至該專屬的記錄儲存貯體。

完成下列程序，即可使用 AWS CLI 啟用存取記錄。

### Note

您必須先為 Lightsail 安裝 AWS CLI 並對其進行設定，然後才能繼續執行此程序。如需詳細資訊，請參閱[設定 AWS CLI 定使用 Lightsail](#)。

1. 開啟您本機電腦的命令提示或終端機視窗。
2. 輸入下列命令以啟用存取記錄。

```
aws lightsail update-bucket --bucket-name SourceBucketName --access-log-config
"{\"enabled\": true, \"destination\": \"TargetBucketName\", \"prefix\":
\"ObjectKeyNamePrefix/\"}"
```

將命令中的以下範例文字取代為自訂文字：

- *SourceBucketName* -將為其建立存取記錄的來源值區名稱。
- *TargetBucketName* — 將儲存存取記錄的目標儲存貯體的名稱。
- *ObjectKeyNamePrefix/* -存取記錄的選用物件金鑰名稱前置詞。請注意，字首必須以正斜線 (/) 為結尾。

### 範例

```
aws lightsail update-bucket --bucket-name amzn-s3-demo-bucket1 --access-log-config
"{\"enabled\": true, \"destination\": \"amzn-s3-demo-bucket2\", \"prefix\":
\"logs/amzn-s3-demo-bucket1/\"}"
```

在此範例中，*amzn-s3-demo-bucket1* 是將為其建立存取記錄的來源值區，*amzn-s3-demo-bucket2* 是要儲存存取記錄的目的地值區，以及 *logs/amzn-s3-demo-bucket1/* 是存取記錄的物件索引鍵名稱前置詞。

您在執行下列命令後，應該會看到類似以下範例的結果。隨即更新來源儲存貯體，且存取日誌應該開始產生並儲存在目的地儲存貯體上。

```
c:\Models>aws lightsail update-bucket --bucket-name MyExampleBucket
--access-log-config "{\"enabled\": true, \"destination\": \"MyExampleLogDestinationBucket\", \"prefix\": \"logs/MyExampleBucket/\"}"

{
  "bucket": {
    "resourceType": "Bucket",
    "accessRules": {
      "getObject": "private",
      "allowPublicOverrides": false
    },
    "arn": "arn:aws:s3:::MyExampleBucket",
    "bundleId": "large_1_0",
    "createdAt": "2021-06-29T08:12:39.163000-07:00",
    "url": "https://MyExampleBucket.s3.amazonaws.com",
    "location": {
      "availabilityZone": "all",
      "regionName": "us-west-2"
    },
    "name": "MyExampleBucket",
    "supportCode": "MyExampleBucket",
    "tags": [],
    "objectVersioning": "Suspended",
    "ableToUpdateBundle": true,
    "readonlyAccessAccounts": [
      "MyExampleAccount"
    ],
    "state": {
      "code": "OK"
    }
  },
  "accessLogConfig": {
    "enabled": true,
    "destination": "MyExampleLogDestinationBucket"
    "prefix": "logs/MyExampleBucket/"
  },
  "operations": [
    {
      "id": "7ee31ae9-2946-4889-9083-4b0459538162",
      "resourceName": "MyExampleBucket",
      "resourceType": "Bucket",
      "createdAt": "2021-10-22T12:42:11.792000-07:00",
      "location": {
        "availabilityZone": "all",
        "regionName": "us-west-2"
      },
      "isTerminal": true,
      "operationDetails": "MyExampleBucket",
      "operationType": "UpdateBucket",
      "status": "Succeeded",
      "statusChangedAt": "2021-10-22T12:42:11.792000-07:00",
      "errorCode": "",
      "errorDetails": ""
    }
  ]
}
```

## 使用停用存取記錄 AWS CLI

完成下列程序，即可使用 AWS CLI 停用存取記錄。

### Note

您必須先為 Lightsail 安裝 AWS CLI 並對其進行設定，然後才能繼續執行此程序。如需詳細資訊，請參閱 [設 AWS CLI 定使用 Lightsail](#)。

1. 開啟您本機電腦的命令提示或終端機視窗。
2. 輸入下列命令以停用存取記錄。

```
aws lightsail update-bucket --bucket-name SourceBucketName --access-log-config  
"{\"enabled\": false}"
```

在命令中，替換 *SourceBucketName* 使用要停用存取記錄之來源值區的名稱。

#### 範例

```
aws lightsail update-bucket --bucket-name amzn-s3-demo-bucket --access-log-config  
"{\"enabled\": false}"
```

您在執行下列命令後，應該會看到類似以下範例的結果。

```
➤ aws lightsail update-bucket --bucket-name MyExampleBucket --access-log-config "{\"enabled\": false}"
{
  "bucket": {
    "resourceType": "Bucket",
    "accessRules": {
      "getObject": "private",
      "allowPublicOverrides": false
    },
    "arn": "arn:aws:lightsail:us-west-2:123456789012:bucket:MyExampleBucket",
    "bundleId": "large_1_0",
    "createdAt": "2021-06-29T08:12:39.163000-07:00",
    "url": "https://lightsail-us-west-2-123456789012.s3.amazonaws.com",
    "location": {
      "availabilityZone": "all",
      "regionName": "us-west-2"
    },
    "name": "MyExampleBucket",
    "supportCode": "lightsail-us-west-2-123456789012",
    "tags": [],
    "objectVersioning": "Suspended",
    "ableToUpdateBundle": true,
    "readonlyAccessAccounts": [
      "lightsail-us-west-2-123456789012"
    ],
    "state": {
      "code": "OK"
    },
    "accessLogConfig": {
      "enabled": false
    }
  },
  "operations": [
    {
      "id": "lightsail-us-west-2-123456789012",
      "resourceName": "MyExampleBucket",
      "resourceType": "Bucket",
      "createdAt": "2021-10-22T13:24:36.881000-07:00",
      "location": {
        "availabilityZone": "all",
        "regionName": "us-west-2"
      },
      "isTerminal": true,
      "operationDetails": "lightsail-us-west-2-123456789012",
      "operationType": "UpdateBucket",
      "status": "Succeeded",
      "statusChangedAt": "2021-10-22T13:24:36.881000-07:00",
      "errorCode": "",
      "errorDetails": ""
    }
  ]
}
```

## 使用 Lightsail 中的 Amazon Athena 分析值區存取日誌

在本指南中，我們會為您介紹如何使用存取日誌來識別儲存貯體請求。如需詳細資訊，請參閱[儲存貯體存取日誌](#)。

### 內容

- [使用 Amazon Athena 查詢請求的存取日誌](#)
- [使用 Amazon S3 存取日誌來識別物件存取請求](#)

## 使用 Amazon Athena 查詢請求的存取日誌

您可以使用 Amazon Athena 在存取日誌中查詢和識別對儲存貯體的請求。

Lightsail 會將存取記錄做為物件儲存在 Lightsail 值區中。使用可以分析日誌的工具通常比較容易。Athena 支援分析物件，還可用來查詢存取日誌。

### 範例

以下範例示範如何在 Amazon Athena 中查詢儲存貯體伺服器存取日誌。

#### Note

若要在 Athena 查詢中指定儲存貯體位置，您需要格式化目標儲存貯體名稱和目標前置詞，以 S3 形式傳送日誌URI，如下所示：`s3://amzn-s3-demo-bucket1-logs/prefix/`

1. 在 <https://console.aws.amazon.com/athena/> 中開啟 Athena 主控台。
2. 在查詢編輯器中，執行類似如下的命令。

```
create database bucket_access_logs_db
```

#### Note

最佳做法是在與 S3 儲存貯體相同 AWS 區域的位置建立資料庫。

3. 在查詢編輯器中，執行類似如下的命令，在您於步驟 2 建立的資料庫中建立資料表結構描述。STRING 及 BIGINT 資料類型值為存取日誌屬性。您可以在 Athena 中查詢這些屬性。在 LOCATION 的部分，輸入稍早記下的儲存貯體和字首路徑。

```
CREATE EXTERNAL TABLE `s3_access_logs_db.amzn-s3-demo-bucket_logs`(  
  `bucketowner` STRING,  
  `bucket_name` STRING,  
  `requestdatetime` STRING,  
  `remoteip` STRING,  
  `requester` STRING,  
  `requestid` STRING,  
  `operation` STRING,  
  `key` STRING,  
  `request_uri` STRING,
```

```

`httpstatus` STRING,
`errorcode` STRING,
`bytessent` BIGINT,
`objectsize` BIGINT,
`totaltime` STRING,
`turnaroundtime` STRING,
`referrer` STRING,
`useragent` STRING,
`versionid` STRING,
`hostid` STRING,
`sigv` STRING,
`ciphersuite` STRING,
`authtype` STRING,
`endpoint` STRING,
`tlsversion` STRING)
ROW FORMAT SERDE
  'org.apache.hadoop.hive.serde2.RegexSerDe'
WITH SERDEPROPERTIES (
  'input.regex'='([^\ ]*) ([^\ ]*) \\\[(.??)\\] ([^\ ]*) ([^\ ]*) ([^\ ]*) ([^\ ]*)
([^\ ]*) (\\"[^\\"]*"\\|-) (-|[0-9]*) ([^\ ]*) ([^\ ]*) ([^\ ]*) ([^\ ]*) ([^\ ]*) ([^\ ]*)
(\\"[^\\"]*"\\|-) ([^\ ]*)(?: ([^\ ]*) ([^\ ]*) ([^\ ]*) ([^\ ]*) ([^\ ]*) ([^\ ]*))?.*$')
STORED AS INPUTFORMAT
  'org.apache.hadoop.mapred.TextInputFormat'
OUTPUTFORMAT
  'org.apache.hadoop.hive.q1.io.HiveIgnoreKeyTextOutputFormat'
LOCATION
  's3://amzn-s3-demo-bucket1-logs/prefix/'

```

4. 在導覽窗格的 Database (資料庫) 下，選擇您的資料庫。
5. 在 Tables (表格) 底下，選擇資料表名稱旁的 Preview table (預覽資料表)。

在 Results (結果) 窗格中，應出現伺服器存取日誌的資料，例如 bucketowner、bucket、requestdatetime 等。這表示您成功建立 Athena 資料表。您現可查詢儲存貯體伺服器存取日誌。

**範例 — 顯示刪除物件的使用者及時間 (時間戳記、IP 位址和IAM使用者)**

```

SELECT RequestDateTime, RemoteIP, Requester, Key
FROM s3_access_logs_db.amzn-s3-demo-bucket_logs
WHERE key = 'images/picture.jpg' AND operation like '%DELETE%';

```

**範例 — 顯示IAM使用者執行的所有作業**

```
SELECT *
FROM s3_access_logs_db.amzn-s3-demo-bucket_logs
WHERE requester='arn:aws:iam::123456789123:user/user_name';
```

### 範例 — 顯示特定期間內針對某物件執行的所有操作

```
SELECT *
FROM s3_access_logs_db.amzn-s3-demo-bucket_logs
WHERE Key='prefix/images/picture.jpg'
      AND parse_datetime(RequestDateTime, 'dd/MMM/yyyy:HH:mm:ss Z')
      BETWEEN parse_datetime('2017-02-18:07:00:00', 'yyyy-MM-dd:HH:mm:ss')
      AND parse_datetime('2017-02-18:08:00:00', 'yyyy-MM-dd:HH:mm:ss');
```

### 範例 — 顯示特定期間內特定 IP 地址傳輸的資料量

```
SELECT SUM(bytesent) AS uploadTotal,
       SUM(objectsize) AS downloadTotal,
       SUM(bytesent + objectsize) AS Total
FROM s3_access_logs_db.amzn-s3-demo-bucket_logs
WHERE RemoteIP='1.2.3.4'
      AND parse_datetime(RequestDateTime, 'dd/MMM/yyyy:HH:mm:ss Z')
      BETWEEN parse_datetime('2017-06-01', 'yyyy-MM-dd')
      AND parse_datetime('2017-07-01', 'yyyy-MM-dd');
```

## 使用 Amazon S3 存取日誌來識別物件存取請求

您可以使用存取日誌上的查詢來識別物件存取要求，執行諸如GET、和之類的作業PUTDELETE，並探索有關這些要求的進一步資訊。

以下 Amazon Athena 查詢範例示範如何從伺服器存取日誌取得儲存貯體的所有 PUT 物件請求。

### 範例 — 顯示在特定期間內傳送PUT物件要求的所有請求者

```
SELECT Bucket, Requester, RemoteIP, Key, HTTPStatus, ErrorCode, RequestDateTime
FROM s3_access_logs_db
WHERE Operation='REST.PUT.OBJECT' AND
      parse_datetime(RequestDateTime, 'dd/MMM/yyyy:HH:mm:ss Z')
      BETWEEN parse_datetime('2019-07-01:00:42:42', 'yyyy-MM-dd:HH:mm:ss')
      AND
      parse_datetime('2019-07-02:00:42:42', 'yyyy-MM-dd:HH:mm:ss')
```

以下 Amazon Athena 查詢範例顯示如何從伺服器存取日誌取得 Amazon S3 的所有 GET 物件請求。

範例 — 顯示在特定期間內傳送 GET 物件要求的所有請求者

```
SELECT Bucket, Requester, RemoteIP, Key, HTTPStatus, ErrorCode, RequestDateTime
FROM s3_access_logs_db
WHERE Operation='REST.GET.OBJECT' AND
parse_datetime(RequestDateTime, 'dd/MMM/yyyy:HH:mm:ss Z')
BETWEEN parse_datetime('2019-07-01:00:42:42', 'yyyy-MM-dd:HH:mm:ss')
AND
parse_datetime('2019-07-02:00:42:42', 'yyyy-MM-dd:HH:mm:ss')
```

以下 Amazon Athena 查詢範例示範如何從伺服器存取日誌取得 S3 儲存貯體的所有匿名請求。

範例 — 顯示在特定期間向儲存貯體提出請求的所有匿名請求者

```
SELECT Bucket, Requester, RemoteIP, Key, HTTPStatus, ErrorCode, RequestDateTime
FROM s3_access_logs_db.amzn-s3-demo-bucket_logs
WHERE Requester IS NULL AND
parse_datetime(RequestDateTime, 'dd/MMM/yyyy:HH:mm:ss Z')
BETWEEN parse_datetime('2019-07-01:00:42:42', 'yyyy-MM-dd:HH:mm:ss')
AND
parse_datetime('2019-07-02:00:42:42', 'yyyy-MM-dd:HH:mm:ss')
```

#### Note

- 您可以修改日期範圍以符合您的需求。
- 對安全監控時而言，這些查詢範例也可能相當實用。您可以檢閱來自意外或未授權 IP 地址/請求者的 PutObject 或 GetObject 呼叫的結果，以及識別對您儲存貯體的任何匿名請求。
- 此查詢只會擷取啟用日誌之後的資訊。

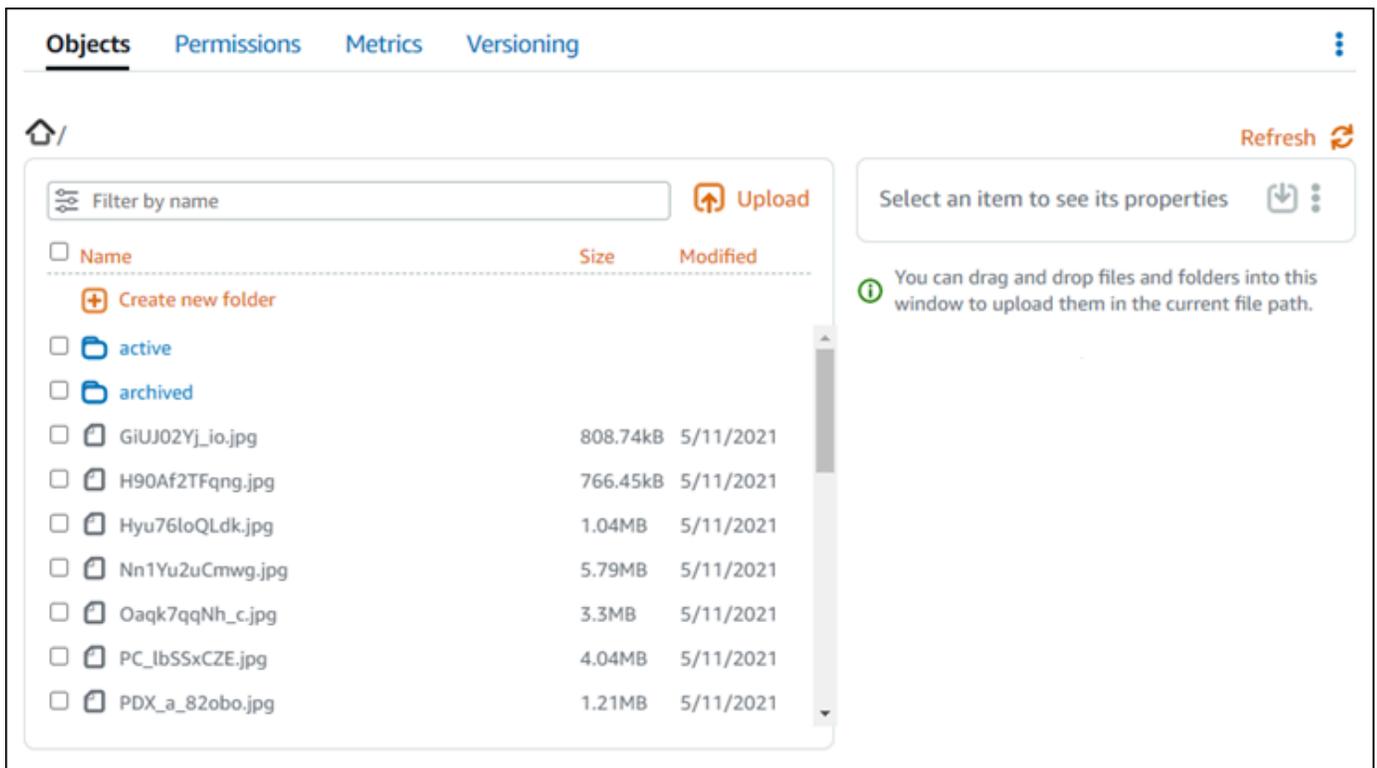
## 在 Lightsail 值區中管理檔案和資料夾

您可以使用 Lightsail 主控台，在 Amazon Lightsail 物件儲存服務中檢視儲存在儲存貯體中的所有物件。您也可以使用 AWS Command Line Interface (AWS CLI) 和列 AWS SDKs 出值區中的物件索引鍵。如需有關儲存貯體的詳細資訊，請參閱 [物件儲存](#)。

## 使用主控台篩選物件

若要使用 Lightsail 主控台檢視儲存在值區中的物件，請完成下列程序。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁上，選擇儲存空間索引標籤。
3. 選擇您要檢視物件之儲存貯體的名稱。
4. Objects (物件) 索引標籤中的 Objects browser (物件瀏覽器) 窗格會顯示存放在儲存貯體中的物件和資料夾。



5. 瀏覽至要檢視屬性的物件位置。
6. 在您要檢視屬性的物件旁新增核取記號。
7. 頁面右側的 Object properties (物件屬性) 窗格會顯示關於物件的資訊。

The screenshot displays the Amazon Lightsail console's 'Objects' tab. At the top, there are navigation tabs for 'Objects', 'Permissions', 'Metrics', and 'Versioning'. Below these is a search bar labeled 'Filter by name' and an 'Upload' button. A list of objects is shown with columns for 'Name', 'Size', and 'Modified'. The object 'sailbot.jpg' is selected. To the right of the list, a detailed view for 'sailbot.jpg' is shown, including its size (42.232 kB / 43,246 byte), last modified date (May 11, 2021), permissions (private), metadata (contentType: image/jpeg), and tags. Red callout boxes numbered 1 through 7 highlight specific UI elements: 1. Upload button, 2. Object actions menu (download, refresh, etc.), 3. Object size and last modified information, 4. Permissions section, 5. Metadata section, 6. Object tags section, and 7. Versions section.

顯示的資訊包括：

1. 檢視和下載物件的連結。
2. 用於複製或刪除物件的動作選單 (:)。如需有關複製和刪除物件的詳細資訊，請參閱在 [Amazon Lightsail 中複製或移動值區中的物件](#)和[刪除值區物件](#)。
3. 物件大小以及上次修改的時間戳記。
4. 個別物件的存取許可，可能是私有或公有 (唯讀)。如需有關物件許可的詳細資訊，請參閱[儲存貯體許可](#)。
5. 物件的中繼資料。內容類型 (ContentType) 鍵是目前 Lightsail 物件儲存服務唯一支援的中繼資料。
6. 物件索引鍵值標籤。如需詳細資訊，請參閱[標記儲存貯體物件](#)。
7. 用於管理物件已儲存版本的選項。如需詳細資訊，請參閱在[儲存貯體中啟用和暫停物件版本控制](#)。

#### Note

當您選取多個物件時，Object properties (物件屬性) 窗格只會顯示所選物件的總大小。

## 使用檢視物件 AWS CLI

完成下列程序，以使用 AWS Command Line Interface (AWS CLI) 在儲存貯體中列出物件金鑰。您可以使用 `list-objects-v2` 命令來執行此動作。若要取得更多資訊，請參閱《AWS CLI 指令參考》中的 [list-objects-v2](#)。

### Note

您必須先為 Lightsail AWS CLI 和 Amazon S3 安裝並進行設定，然後才能繼續執行此程序。如需詳細資訊，請參閱 [設定 AWS Command Line Interface 以與 Amazon Lightsail 搭配使用](#)。

1. 開啟命令提示或終端機視窗。
2. 輸入以下其中一個命令。
  - 輸入下列命令以列出儲存貯體中的所有物件索引鍵。

```
aws s3api list-objects-v2 --bucket BucketName --query "Contents[].{Key: Key, Size: Size}"
```

在命令中，替換 *BucketName* 與您要列出所有對象的存儲桶的名稱。

- 輸入下列命令，以列出以特定物件索引鍵名稱字首開頭的物件。

```
aws s3api list-objects-v2 --bucket BucketName --prefix ObjectKeyNamePrefix --query "Contents[].{Key: Key, Size: Size}"
```

將命令中的以下範例文字取代為自訂文字：

- *BucketName* -您要列出所有物件的值區名稱。
- *ObjectKeyNamePrefix* -物件索引鍵名稱前置詞，可限制回應以指定前置詞開頭的金鑰。

### Note

這些命令會使用 `--query` 參數來篩選 `list-objects-v2` 請求的回應，而該請求針對每個物件的索引鍵值和大小。

範例：

列出儲存貯體中的所有物件索引鍵：

```
aws s3api list-objects-v2 --bucket amzn-s3-demo-bucket --query "Contents[].{Key: Key, Size: Size}"
```

對於前述命令，您應該會看到類似以下範例的結果。

```
C:\>aws s3api list-objects-v2 --bucket DOC-EXAMPLE-BUCKET --query "Contents[].{Key: Key, Size: Size}"
[
  {
    "Key": "GiUJ02Yj_io.jpg",
    "Size": 828150
  },
  {
    "Key": "H90Af2TFqng.jpg",
    "Size": 784846
  },
  {
    "Key": "Hyu761oQLdk.jpg",
    "Size": 1086363
  },
  {
    "Key": "Nn1Yu2uCmwg.jpg",
    "Size": 6075006
  },
  {
    "Key": "Oaqk7qqNh_c.jpg",
    "Size": 3458557
  },
  {
    "Key": "PC_lbSSxCZE.jpg",
    "Size": 4239636
  },
  {
    "Key": "PDX_a_820hg.jpg"
```

列出以 `archived/` 物件索引鍵名稱字首開頭的物件索引鍵：

```
aws s3api list-objects-v2 --bucket amzn-s3-demo-bucket --prefix archived/ --query "Contents[].{Key: Key, Size: Size}"
```

對於前述命令，您應該會看到類似以下範例的結果。

```
C:\>aws s3api list-objects-v2 --bucket DOC-EXAMPLE-BUCKET --prefix archived/ --query "Contents[].[Key: Key, Size: Size]"
[
  {
    "Key": "archived/",
    "Size": 0
  },
  {
    "Key": "archived/1_CMoFsPfso.jpg",
    "Size": 2561865
  },
  {
    "Key": "archived/3y1zF4hIPCg.jpg",
    "Size": 6404907
  },
  {
    "Key": "archived/5IH5WhosQE.jpg",
    "Size": 2377975
  },
  {
    "Key": "archived/sailbot.jpg",
    "Size": 43246
  }
]
```

## 管理儲存貯體和物件

以下是管理 Lightsail 物件儲存貯體的一般步驟：

1. 了解 Amazon Lightsail 物件儲存服務中的物件和值區。如需詳細資訊，請參閱 [Amazon Lightsail 中的物件儲存](#)。
2. 了解您可以在 Amazon Lightsail 中為您的儲存貯體提供哪些名稱。如需詳細資訊，請參閱 [Amazon Lightsail 中的儲存貯體命名規則](#)。
3. 透過建立值區開始使用 Lightsail 物件儲存服務。如需詳細資訊，請參閱 [在 Amazon Lightsail 中建立值區](#)。
4. 了解儲存貯體的安全最佳實務，以及可以為儲存貯體設定的存取許可。可以將儲存貯體中的所有物件設為公有或私有，也可以選擇將個別物件設為公有。您也可以建立存取金鑰、將執行個體附加至儲存貯體，以及授予其他AWS帳戶的存取權，以授予儲存貯體的存取權。如需詳細資訊，請參閱 [Amazon Lightsail 物件儲存的安全最佳實務和了解 Amazon Lightsail 中的儲存貯體許可](#)。

了解儲存貯體存取許可後，請參閱下列指南來授予對儲存貯體的存取權：

- [封鎖儲存貯體的公 Amazon Lightsail](#)
- [在 Amazon Lightsail 中設定儲存貯體存取權限](#)
- [在 Amazon Lightsail 中為儲存貯體中的個別物件設定存取權限](#)
- [在 Amazon Lightsail 中為存儲桶創建訪問密鑰](#)
- [在 Amazon Lightsail 中設定儲存貯體的資源存取](#)
- [在 Amazon Lightsail 中設定儲存貯體的跨帳戶存取](#)

5. 了解如何為儲存貯體啟用存取日誌記錄，以及如何使用存取日誌來稽核儲存貯體的安全性。如需詳細資訊，請參閱下列指南。
  - [Amazon Lightsail 物件儲存服務中儲存貯體的存取記錄](#)
  - [存取 Amazon Lightsail 物件儲存服務中儲存貯體的日誌格式](#)
  - [在 Amazon Lightsail 物件儲存服務中啟用儲存貯體的存取記錄功能](#)
  - [在 Amazon Lightsail 中使用儲存貯體的存取日誌來識別請求](#)
6. 建立IAM政策，讓使用者能夠在 Lightsail 中管理值區。如需詳細資訊，請參閱[在 Amazon Lightsail 中管理儲存貯體的IAM政策](#)。
7. 了解儲存貯體中物件的標記和識別方式。如需詳細資訊，請參閱[了解 Amazon Lightsail 中的物件金鑰名稱](#)。
8. 了解如何在儲存貯體中上傳檔案及管理物件。如需詳細資訊，請參閱下列指南。
  - [將文件上傳到 Amazon Lightsail](#)
  - [使用多部分上傳將檔案上傳到 Amazon Lightsail 中的儲存貯體](#)
  - [檢視儲存貯體中 Amazon Lightsail](#)
  - [在 Amazon Lightsail 中複製或移動值區中的物件](#)
  - [從儲存貯體下 Amazon Lightsail](#)
  - [在 Amazon Lightsail 中過濾存儲桶中的對象](#)
  - [標記存儲桶中 Amazon Lightsail](#)
  - [刪除存儲桶中 Amazon Lightsail](#)
9. 啟用物件版本控制功能來保留、擷取和恢復儲存貯體中所儲存每個物件的各個版本。如需詳細資訊，請參閱在[Amazon Lightsail 中啟用和暫停儲存貯體中的物件版本控制](#)。
10. 啟用物件版本控制之後，可以還原儲存貯體中物件的先前版本。如需詳細資訊，請參閱在[Amazon Lightsail 中還原儲存貯體中的舊版物件](#)。
11. 監控儲存貯體的使用率。如需詳細資訊，請參閱[在 Amazon Lightsail 中檢視儲存貯體的指標](#)。
12. 設定儲存貯體指標的警示，以便在儲存貯體的使用率超過閾值時收到通知。如需詳細資訊，請參閱[在 Amazon Lightsail 中建立儲存貯體指標警示](#)。
13. 如果儲存空間和網路傳輸不足，請變更儲存貯體的儲存計畫。如需詳細資訊，請參閱[在 Amazon Lightsail 中變更儲存貯體的計畫](#)。
14. 了解如何將儲存貯體連線至其他資源。如需詳細資訊，請參閱下列教學課程。
  - [教學課程：將 WordPress 執行個體連接至 Amazon Lightsail 儲存貯體](#)
  - [教學課程：將 Amazon Lightsail 儲存貯體與 Lightsail 內容交付網路分發搭配使用](#)
15. 如果不再使用儲存貯體，請刪除它。如需詳細資訊，請參閱[刪除儲存貯體](#)。

## 主題

- [在 Lightsail 值區之間複製和移動物件](#)
- [透過刪除物件來清除 Lightsail 儲存貯體](#)
- [從儲存貯體下載物件](#)
- [依名稱前置詞篩選 Lightsail 值區中的物件](#)
- [在 Lightsail 中啟用和暫停物件版本控制](#)
- [在 Lightsail 值區中復原先前的物件版本](#)
- [在 Lightsail 值區中標記物件](#)

## 在 Lightsail 值區之間複製和移動物件

您可以在 Amazon Lightsail 物件儲存服務中複製已存放在儲存貯體中的物件。在本指南中，我們將示範如何使用 Lightsail 主控台並使用 AWS Command Line Interface (AWS CLI) 複製物件。拷貝值區中的物件以建立物件的複製副本、重新命名物件，或在 Lightsail 位置之間移動物件 (例如，將物件從一個物件移 AWS 區域 到另一個可使用 Lightsail 的位置)。您只能使用 AWS APIs、AWS SDKs 和 AWS Command Line Interface (AWS CLI) 跨位置複製物件。

如需有關儲存貯體的詳細資訊，請參閱[物件儲存](#)。

### 複製物件的限制

您可以使用 Lightsail 主控台，建立大小上限為 2 GB 的物件副本。您可以使用 AWS Command Line Interface (AWS CLI)、AWS APIs 和，使用單一複製物件動作，建立大小上限為 5 GB 的物件副本 AWS SDKs。若要複製大小超過 5 GB 的物件，您必須使用、和 AWS SDKs 的多部分上傳動作。AWS CLI AWS APIs 如需詳細資訊，請參閱[使用分段上傳將檔案上傳至儲存貯體](#)。

### 使用主控台複製物件

請完成下列程序，以使用 Lightsail 主控台複製儲存在值區中的物件。若要移動儲存貯體中的物件，則應該將其複製到新位置，然後刪除原始物件。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁上，選擇儲存空間索引標籤。
3. 選擇您要複製物件之儲存貯體的名稱。
4. 在 Objects (物件) 索引標籤中，使用 Objects browser (物件瀏覽器) 窗格瀏覽至您要複製的物件所在位置。

5. 在要複製的物件旁新增核取記號。
6. 在 Object information (物件資訊) 窗格中，選擇動作 (:) 選單，然後選擇 Copy to (複製至)。
7. 在顯示的 Select destination (選取目的地) 窗格中，瀏覽至儲存貯體中您要複製所選物件的位置。您亦可將資料夾名稱輸入 Destination path (目的地路徑) 文字方塊來建立新路徑。
8. 選擇 Copy (複製)，以將物件複製到選取或指定的目的地。否則，請選擇 No, cancel (否，取消)。

成功複製物件時會顯示 Copy complete (複製完成) 訊息。如果您要移動物件，則應刪除原始物件。如需詳細資訊，請參閱[刪除儲存貯體物件](#)。

## 使用複製物件 AWS CLI

若要使用 AWS Command Line Interface (AWS CLI) 複製值區中的物件，請完成下列程序。您可以使用 `copy-object` 命令來執行此動作。如需詳細資訊，請參閱《AWS CLI 命令參考》中的 [copy-object](#)。

### Note

您必須先為 Lightsail AWS CLI 和 Amazon S3 安裝並進行設定，然後才能繼續執行此程序。如需詳細資訊，請參閱[設 AWS CLI 定使用 Lightsail](#)。

1. 開啟命令提示或終端機視窗。
2. 輸入下列命令以複製儲存貯體中的物件。

```
aws s3api copy-object --copy-source SourceBucketNameAndObjectKey --  
key DestinationObjectKey --bucket DestinationBucketName --acl bucket-owner-full-  
control
```

將命令中的以下範例文字取代為自訂文字：

- *SourceBucketNameAndObjectKey* -來源物件目前存在的值區名稱，以及要複製之物件的完整物件金鑰。例如，若要從儲存貯體 `amzn-s3-demo-bucket` 複製物件 `images/sailbot.jpg`，請指定 `amzn-s3-demo-bucket/images/sailbot.jpg`。
- *DestinationObjectKey* -新物件副本的完整物件金鑰。
- *DestinationBucket* -目的地值區的名稱。

## 範例：

- 將儲存貯體中的物件複製到同一個儲存貯體：

```
aws s3api copy-object --copy-source amzn-s3-demo-bucket1/images/sailbot.jpg
--key media/sailbot.jpg --bucket amzn-s3-demo-bucket --acl bucket-owner-full-
control
```

- 從一個儲存貯體複製物件至另一個儲存貯體：

```
aws s3api copy-object --copy-source amzn-s3-demo-bucket1/images/sailbot.jpg --
key images/sailbot.jpg --bucket amzn-s3-demo-bucket2 --acl bucket-owner-full-
control
```

您應該會看到類似以下範例的結果：

```
C:\>aws s3api copy-object --copy-source DOC-EXAMPLE-BUCKET/images/sailbot.jpg --key images/archived/sailbot.jpg --bucket DOC-EXAMPLE-BUCKET
{
  "ServerSideEncryption": "AES256",
  "CopyObjectResult": {
    "ETag": "\"694d34example91d92d64f342aa234c3\"",
    "LastModified": "2021-05-10T05:35:42+00:00"
  }
}
```

## 管理儲存貯體和物件

以下是管理 Lightsail 物件儲存貯體的一般步驟：

1. 了解 Amazon Lightsail 物件儲存服務中的物件和值區。如需詳細資訊，請參閱 [Amazon Lightsail 中的物件儲存](#)。
2. 了解您可以在 Amazon Lightsail 中為您的儲存貯體提供哪些名稱。如需詳細資訊，請參閱 [Amazon Lightsail 中的儲存貯體命名規則](#)。
3. 透過建立值區開始使用 Lightsail 物件儲存服務。如需詳細資訊，請參閱 [在 Amazon Lightsail 中建立值區](#)。
4. 了解儲存貯體的安全最佳實務，以及可以為儲存貯體設定的存取許可。可以將儲存貯體中的所有物件設為公有或私有，也可以選擇將個別物件設為公有。您也可以建立存取金鑰、將執行個體附加至儲存貯體，以及授予其他AWS帳戶的存取權，以授予儲存貯體的存取權。如需詳細資訊，請參閱 [Amazon Lightsail 物件儲存的安全最佳實務和了解 Amazon Lightsail 中的儲存貯體許可](#)。

- 了解儲存貯體存取許可後，請參閱下列指南來授予對儲存貯體的存取權：
- [封鎖儲存貯體的公開存取](#)
  - [在 Amazon Lightsail 中設定儲存貯體存取權限](#)
  - [在 Amazon Lightsail 中為儲存貯體中的個別物件設定存取權限](#)
  - [在 Amazon Lightsail 中為存儲桶創建訪問密鑰](#)
  - [在 Amazon Lightsail 中設定儲存貯體的資源存取](#)
  - [在 Amazon Lightsail 中設定儲存貯體的跨帳戶存取](#)
5. 了解如何為儲存貯體啟用存取日誌記錄，以及如何使用存取日誌來稽核儲存貯體的安全性。如需詳細資訊，請參閱下列指南。
- [Amazon Lightsail 物件儲存服務中儲存貯體的存取記錄](#)
  - [存取 Amazon Lightsail 物件儲存服務中儲存貯體的日誌格式](#)
  - [在 Amazon Lightsail 物件儲存服務中啟用儲存貯體的存取記錄](#)
  - [在 Amazon Lightsail 中使用儲存貯體的存取日誌來識別請求](#)
6. 建立IAM原則，讓使用者能夠在 Lightsail 中管理值區。如需詳細資訊，請參閱[在 Amazon Lightsail 中管理儲存貯體的IAM政策](#)。
7. 了解儲存貯體中物件的標記和識別方式。如需詳細資訊，請參閱[了解 Amazon Lightsail 中的物件金鑰名稱](#)。
8. 了解如何在儲存貯體中上傳檔案及管理物件。如需詳細資訊，請參閱下列指南。
- [將文件上傳到 Amazon Lightsail](#)
  - [使用多部分上傳將檔案上傳到 Amazon Lightsail 中的儲存貯體](#)
  - [檢視儲存貯體中 Amazon Lightsail](#)
  - [在 Amazon Lightsail 中複製或移動值區中的物件](#)
  - [從儲存貯體下 Amazon Lightsail](#)
  - [在 Amazon Lightsail 中過濾存儲桶中的對象](#)
  - [標記存儲桶中 Amazon Lightsail](#)
  - [刪除存儲桶中 Amazon Lightsail](#)
9. 啟用物件版本控制功能來保留、擷取和恢復儲存貯體中所儲存每個物件的各個版本。如需詳細資訊，請參閱在 [Amazon Lightsail 中啟用和暫停儲存貯體中的物件版本控制](#)。
10. 啟用物件版本控制之後，可以還原儲存貯體中物件的先前版本。如需詳細資訊，請參閱在 [Amazon Lightsail 中還原儲存貯體中的舊版物件](#)。
11. 監控儲存貯體的使用率。如需詳細資訊，請參閱[在 Amazon Lightsail 中檢視儲存貯體的指標](#)。

12. 設定儲存貯體指標的警示，以便在儲存貯體的使用率超過閾值時收到通知。如需詳細資訊，請參閱 [在 Amazon Lightsail 中建立儲存貯體指標警示](#)。
13. 如果儲存空間和網路傳輸不足，請變更儲存貯體的儲存計畫。如需詳細資訊，請參閱 [在 Amazon Lightsail 中變更儲存貯體的計畫](#)。
14. 了解如何將儲存貯體連線至其他資源。如需詳細資訊，請參閱下列教學課程。
  - [教學課程：將 WordPress 執行個體連接至 Amazon Lightsail 儲存貯體](#)
  - [教學課程：將 Amazon Lightsail 儲存貯體與 Lightsail 內容交付網路分發搭配使用](#)
15. 如果不再使用儲存貯體，請刪除它。如需詳細資訊，請參閱 [刪除儲存貯體](#)。

## 透過刪除物件來清除 Lightsail 儲存貯體

您可以在 Amazon Lightsail 物件儲存服務中刪除值區中的物件。若要釋放儲存空間，請刪除不再需要的物件。例如，如果您要收集日誌檔案，最好在不再需要時將其刪除。

如需有關儲存貯體的詳細資訊，請參閱 [物件儲存](#)。

### 內容

- [刪除啟用版本控制之儲存貯體中的物件](#)
- [使用主控台刪除物件](#)
- [使用 Lightsail 主控台刪除物件版本](#)
- [刪除單一物件或物件版本 AWS CLI](#)
- [刪除多個物件或物件版本 AWS CLI](#)

## 刪除啟用版本控制之儲存貯體中的物件

如果已在儲存貯體上啟用版本控制，則其中可存在同一個物件的多個版本。您可以使用 Lightsail 主控台、AWS CLI 或 AWS SDKs 刪除任何版本的物件。AWS APIs 不過，您應考慮以下選項。

### 使用 Lightsail 主控台刪除物件和物件版本

當您在 Lightsail 主控台的「物件」索引標籤的「物件」瀏覽器窗格中刪除物件的目前版本時，這也會刪除該物件的所有先前版本。若要刪除物件的特定版本，您必須從 Manage versions (管理版本) 窗格中執行此動作。如果您使用 Manage versions (管理版本) 窗格來刪除物件的目前版本，則會將最新的前一版本還原為目前版本。如需詳細資訊，請參閱 [本指南稍後的使用 Lightsail 主控台刪除物件版本](#)。

使用 Lightsail 刪除物件和物件版本 API AWS CLI，或 AWS SDKs

若要刪除單一物件及其所有已存放版本，請僅在刪除請求中指定該物件的金鑰。若要刪除物件的特定版本，請指定物件金鑰和版本 ID。如需詳細資訊，請參閱本指南後續的[使用 AWS CLI 來刪除單一物件或物件版本](#)。

## 使用主控台刪除物件

請完成下列程序，使用 Lightsail 主控台刪除物件，包括其儲存的先前版本。您一次只能使用 Lightsail 主控台刪除一個物件。使用 AWS CLI 可一次刪除多個物件。如需詳細資訊，請參閱本指南後續的[使用 AWS CLI 來刪除多個物件或物件版本](#)。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁上，選擇儲存空間索引標籤。
3. 選擇您要刪除物件之儲存貯體的名稱。
4. 在 Objects (物件) 索引標籤中，使用 Objects browser (物件瀏覽器) 窗格瀏覽至您要刪除的物件所在位置。
5. 在要刪除的物件旁新增核取記號。
6. 在 Object information (物件資訊) 窗格中，選擇動作 (:) 選單，然後選擇 Delete (刪除)。
7. 在顯示的確認窗格中，選擇 Yes, delete (是，刪除) 以確認您要永久刪除該物件。

如果您刪除所在資料夾中的唯一物件，此舉也會刪除該資料夾。發生這種情況是因為該資料夾為物件金鑰名稱的一部分，當儲存貯體中沒有其他物件共用相同物件字首時，刪除該物件也會刪除前述資料夾。如需詳細資訊，請參閱[物件儲存儲存貯體的金鑰名稱](#)。

## 使用 Lightsail 主控台刪除物件版本

請完成下列程序，以刪除存放的物件版本。這僅適用於已啟用版本控制的儲存貯體。如需詳細資訊，請參閱[在儲存貯體中啟用和暫停物件版本控制](#)。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁上，選擇儲存空間索引標籤。
3. 選擇您要刪除物件之儲存貯體的名稱。
4. 使用 Objects browser (物件瀏覽器) 窗格瀏覽至您要刪除的物件所在位置。
5. 在您要刪除其儲存的舊版本的物件旁，新增核取記號。
6. 選擇 Object information (物件資訊) 窗格的 Versions (版本) 區段中的 Manage (管理)，然後選擇 Manage (管理)。
7. 在顯示的管理儲存的物件版本窗格中，在要刪除的物件版本旁新增核取記號。

您也可以選擇刪除物件的目前版本。

8. 選擇 Delete selected (刪除所選項)，以刪除選取的版本。

如果您刪除：

- 物件的目前版本 - 該物件的最新版本會還原為目前版本。
- 物件的唯一版本 - 系統會從儲存貯體中刪除該物件。如果您刪除的版本是目前資料夾中唯一的物件，則該資料夾也會遭到刪除。發生這種情況是因為該資料夾為物件金鑰名稱的一部分，當儲存貯體中沒有其他物件共用相同物件金鑰字首時，刪除該物件也會刪除前述資料夾。如需詳細資訊，請參閱[在儲存貯體中啟用和暫停物件版本控制](#)。

## 刪除單一物件或物件版本 AWS CLI

若要使用 AWS Command Line Interface (AWS CLI) 刪除值區中的單一物件或物件版本，請完成下列程序。您可以使用 `delete-object` 命令來執行此動作。如需詳細資訊，請參閱《AWS CLI 命令參考》中的 [delete-object](#)。

### Note

您必須先為 Lightsail AWS CLI 和 Amazon S3 安裝並進行設定，然後才能繼續執行此程序。如需詳細資訊，請參閱[設定 AWS Command Line Interface 以與 Amazon Lightsail 搭配使用](#)。

1. 開啟命令提示或終端機視窗。
2. 輸入下列命令以刪除儲存貯體中的物件或物件版本。

若要刪除物件：

```
aws s3api delete-object --bucket BucketName --key ObjectKey
```

若要刪除物件版本：

### Note

刪除物件版本僅適用於已啟用版本控制的儲存貯體。如需詳細資訊，請參閱[在儲存貯體中啟用和暫停物件版本控制](#)。

```
aws s3api delete-object --bucket BucketName --key ObjectKey --version-id VersionID
```

將命令中的以下範例文字取代為自訂文字：

- *BucketName* -您要從中刪除物件的值區名稱。
- *ObjectKey* -要刪除之物件的完整物件金鑰。
- *VersionID* -您要刪除的物件版本 ID。

範例：

刪除物件：

```
aws s3api delete-object --bucket amzn-s3-demo-bucket --key images/sailbot.jpg
```

刪除物件版本：

```
aws s3api delete-object --bucket amzn-s3-demo-bucket --key images/sailbot.jpg --  
version-id YF0YMB1Uvexample00712vJi9hRz4ujX
```

您應該會看到類似以下範例的結果：

```
C:\Users\latino>aws s3api delete-object --bucket DOC-EXAMPLE-BUCKET --key images/sailbot.jpg --version-id YF0YMB1Uvexample00712vJi9hRz4ujX  
{  
  "VersionId": "YF0YMBexampleY7P00712vJi9hRz4ujX"  
}
```

## 使用 AWS CLI 來刪除多個物件或物件版本

請完成下列程序，使用 AWS Command Line Interface (AWS CLI) 在儲存貯體中刪除多個物件。您可以使用 `delete-objects` 命令來執行此動作。若要取得更多資訊，請參閱 [《AWS CLI 指令參考》中的刪除物件](#)。

### Note

您必須先為 Lightsail AWS CLI 和 Amazon S3 安裝並進行設定，然後才能繼續執行此程序。如需詳細資訊，請參閱 [設定 AWS Command Line Interface 以與 Amazon Lightsail 搭配使用](#)。

1. 開啟命令提示或終端機視窗。
2. 輸入下列命令，以刪除儲存貯體中的多個物件或多個物件版本。

```
aws s3api delete-objects --bucket BucketName --delete file:///LocalDirectory
```

將命令中的以下範例文字取代為自訂文字：

- *BucketName* -您要從中刪除多個物件或多個物件版本的值區名稱。
- *LocalDirectory* -指定要刪除的物件或版本之 .json 文件的電腦上的目錄路徑。該 .json 文件可格式化如下。

若要刪除物件，請在 .json 檔案中輸入下列文字並取代 *ObjectKey* 使用要刪除的對象的對象鍵。

```
{
  "Objects": [
    {
      "Key": "ObjectKey1"
    },
    {
      "Key": "ObjectKey2"
    }
  ],
  "Quiet": false
}
```

若要刪除物件版本，請在 .json 檔案中輸入下列文字。Replace (取代) *ObjectKey* 以及 *VersionID* 使用物件索引鍵以及您要刪除IDs的物件版本。

#### Note

刪除物件版本僅適用於已啟用版本控制的儲存貯體。如需詳細資訊，請參閱[在儲存貯體中啟用和暫停物件版本控制](#)。

```
{
  "Objects": [
    {
      "Key": "ObjectKey1",
```

```

    "VersionId": "VersionID1"
  },
  {
    "Key": "ObjectKey2",
    "VersionId": "VersionID2"
  }
],
"Quiet": false
}

```

範例：

- 在 Linux 或 Unix 電腦上：

```
aws s3api delete-objects --bucket amzn-s3-demo-bucket --delete file://home/user/
Documents/delete-objects.json
```

- 在 Windows 電腦上：

```
aws s3api delete-objects --bucket amzn-s3-demo-bucket --delete file://C:\Users
\user\Documents\delete-objects.json
```

您應該會看到類似以下範例的結果：

```

C:\>aws s3api delete-objects --bucket DOC-EXAMPLE-BUCKET --delete file://C:\Users\user\Documents\delete-objects.json
{
  "Deleted": [
    {
      "Key": "images/sailbot.jpg",
      "VersionId": "26sqexamplezRiT6TsGhMMz0FxQAEw."
    },
    {
      "Key": "images/sailbot.jpg",
      "VersionId": "QwDrexampleDJxJtZC1CrExbpN1EC504"
    }
  ]
}

```

## 管理儲存貯體和物件

以下是管理 Lightsail 物件儲存貯體的一般步驟：

1. 了解 Amazon Lightsail 物件儲存服務中的物件和值區。如需詳細資訊，請參閱 [Amazon Lightsail 中的物件儲存](#)。

2. 了解您可以在 Amazon Lightsail 中為您的儲存貯體提供哪些名稱。如需詳細資訊，請參閱 [Amazon Lightsail 中的儲存貯體命名規則](#)。
3. 透過建立值區開始使用 Lightsail 物件儲存服務。如需詳細資訊，請參閱 [在 Amazon Lightsail 中建立值區](#)。
4. 了解儲存貯體的安全最佳實務，以及可以為儲存貯體設定的存取許可。可以將儲存貯體中的所有物件設為公有或私有，也可以選擇將個別物件設為公有。您也可以建立存取金鑰、將執行個體附加至儲存貯體，以及授予其他AWS帳戶的存取權，以授予儲存貯體的存取權。如需詳細資訊，請參閱 [Amazon Lightsail 物件儲存的安全最佳實務](#)和了解 [Amazon Lightsail 中的儲存貯體許可](#)。

了解儲存貯體存取許可後，請參閱下列指南來授予對儲存貯體的存取權：

- [封鎖儲存貯體的公開存取](#)
  - [在 Amazon Lightsail 集團中設定儲存貯體存取權限](#)
  - [在 Amazon Lightsail 中為儲存貯體中的個別物件設定存取權限](#)
  - [在 Amazon Lightsail 中為存儲桶創建訪問密鑰](#)
  - [在 Amazon Lightsail 中設定儲存貯體的資源存取](#)
  - [在 Amazon Lightsail 中設定儲存貯體的跨帳戶存取](#)
5. 了解如何為儲存貯體啟用存取日誌記錄，以及如何使用存取日誌來稽核儲存貯體的安全性。如需詳細資訊，請參閱下列指南。
    - [Amazon Lightsail 物件儲存服務中儲存貯體的存取記錄](#)
    - [存取 Amazon Lightsail 物件儲存服務中儲存貯體的日誌格式](#)
    - [在 Amazon Lightsail 物件儲存服務中啟用儲存貯體的存取記錄](#)
    - [在 Amazon Lightsail 中使用儲存貯體的存取日誌來識別請求](#)
  6. 建立IAM政策以授與使用者在 Lightsail 中管理值區的能力。如需詳細資訊，請參閱 [在 Amazon Lightsail 中管理儲存貯體的IAM政策](#)。
  7. 了解儲存貯體中物件的標記和識別方式。如需詳細資訊，請參閱 [了解 Amazon Lightsail 中的物件金鑰名稱](#)。
  8. 了解如何在儲存貯體中上傳檔案及管理物件。如需詳細資訊，請參閱下列指南。
    - [將文件上傳到 Amazon Lightsail](#)
    - [使用多部分上傳將檔案上傳到 Amazon Lightsail 中的儲存貯體](#)
    - [檢視儲存貯體中 Amazon Lightsail](#)
    - [在 Amazon Lightsail 中複製或移動值區中的物件](#)

- [在 Amazon Lightsail 中過濾儲存桶中的對象](#)
  - [標記儲存桶中 Amazon Lightsail](#)
  - [刪除儲存桶中 Amazon Lightsail](#)
9. 啟用物件版本控制功能來保留、擷取和恢復儲存貯體中所儲存每個物件的各個版本。如需詳細資訊，請參閱在 [Amazon Lightsail 中啟用和暫停儲存貯體中的物件版本控制](#)。
  10. 啟用物件版本控制之後，可以還原儲存貯體中物件的先前版本。如需詳細資訊，請參閱在 [Amazon Lightsail 中還原儲存貯體中的舊版物件](#)。
  11. 監控儲存貯體的使用率。如需詳細資訊，請參閱在 [Amazon Lightsail 中檢視儲存貯體的指標](#)。
  12. 設定儲存貯體指標的警示，以便在儲存貯體的使用率超過閾值時收到通知。如需詳細資訊，請參閱在 [Amazon Lightsail 中建立儲存貯體指標警示](#)。
  13. 如果儲存空間和網路傳輸不足，請變更儲存貯體的儲存計畫。如需詳細資訊，請參閱在 [Amazon Lightsail 中變更儲存貯體的計畫](#)。
  14. 了解如何將儲存貯體連線至其他資源。如需詳細資訊，請參閱下列教學課程。
    - [教學課程：將 WordPress 執行個體連接至 Amazon Lightsail 儲存貯體](#)
    - [教學課程：將 Amazon Lightsail 儲存貯體與 Lightsail 內容交付網路分發搭配使用](#)
  15. 如果不再使用儲存貯體，請刪除它。如需詳細資訊，請參閱 [刪除儲存貯體](#)。

## 從儲存貯體下載物件

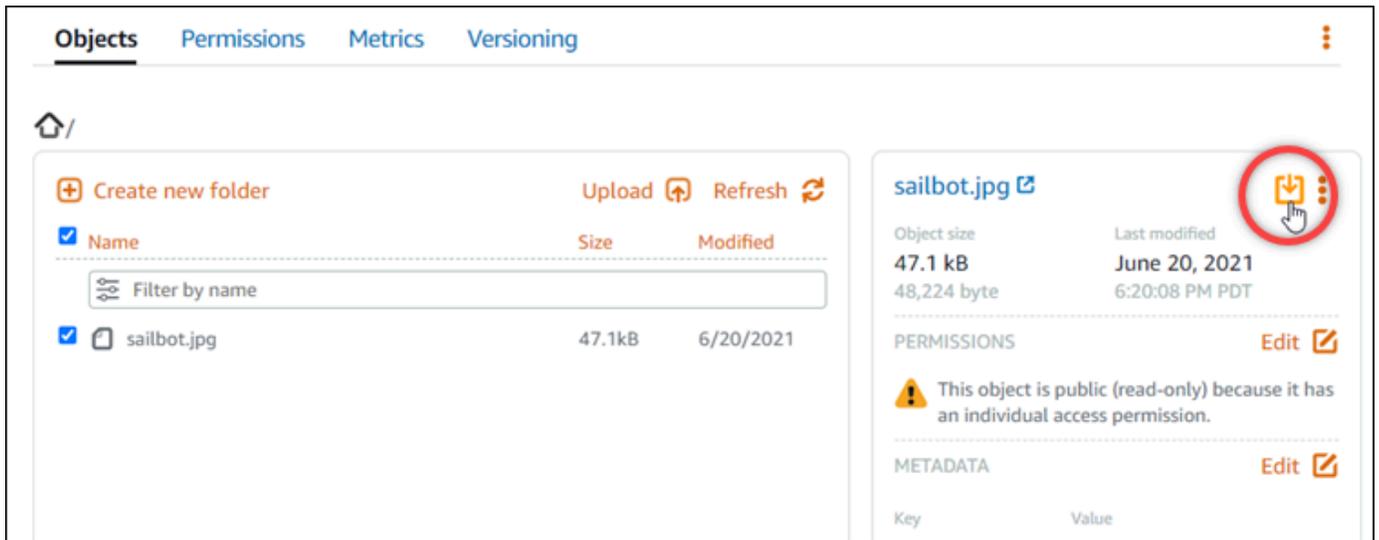
您可以從 Amazon Lightsail 物件儲存服務中可存取的值區或公用 (唯讀) 的值區下載物件。您可以使用 Lightsail 主控台一次下載單一物件。若要在一個請求中下載多個物件，請使用 AWS Command Line Interface (AWS CLI) AWS SDKs、或 REST API。在本指南中，我們將向您展示如何使用 Lightsail 主控台和 AWS CLI。如有有關儲存貯體的詳細資訊，請參閱 [物件儲存](#)。

### 使用主控台下載物件

請完成下列程序，以使用 Lightsail 主控台從值區下載物件。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁上，選擇儲存空間索引標籤。
3. 選擇您要從中下載檔案之儲存貯體的名稱。
4. 在 Objects (物件) 索引標籤中，使用 Objects browser (物件瀏覽器) 窗格瀏覽至您要下載的物件所在位置。

5. 在要下載的物件旁新增核取記號。
6. 在 Object information (物件資訊) 窗格中，選擇下載圖示。



視瀏覽器的組態而定，您選擇的檔案會顯示在頁面上，或下載至您的電腦中。如果該檔案顯示在頁面上，您可以用滑鼠右鍵按一下該檔案，然後選擇 Save as (另存為) 以將其儲存到您的電腦中。

## 使用下載物件 AWS CLI

完成下列程序，以使用 AWS Command Line Interface (AWS CLI) 從儲存貯體中下載物件。您可以使用 `get-object` 命令來執行此動作。如需詳細資訊，請參閱《AWS CLI 命令參考》中的 [get-object](#)。

### Note

您必須先為 Lightsail AWS CLI 和 Amazon S3 安裝並進行設定，然後才能繼續執行此程序。如需詳細資訊，請參閱 [設定 AWS Command Line Interface 以與 Amazon Lightsail 搭配使用](#)。

1. 開啟命令提示或終端機視窗。
2. 輸入下列命令以從儲存貯體下載物件。

```
aws s3api get-object --bucket BucketName --key ObjectKey LocalFilePath
```

將命令中的以下範例文字取代為自訂文字：

- *BucketName* -您要從中下載物件的值區名稱。

- *ObjectKey* -您要下載的物件的完整物件金鑰。
- *LocalFilePath* -計算機上要保存下載文件的完整文件路徑。

範例：

```
aws s3api get-object --bucket amzn-s3-demo-bucket --key images/sailbot.jpg C:\Users\user\Pictures\sailbot.jpg
```

您應該會看到類似以下範例的結果：

```
C:\>aws s3api get-object --bucket DOC-EXAMPLE-BUCKET --key images/sailbot.jpg C:\Users\user\Pictures\sailbot.jpg
{
  "AcceptRanges": "bytes",
  "LastModified": "2021-05-10T05:09:31+00:00",
  "ContentLength": 48224,
  "ETag": "\"694d34example91d92d64f342aa234c3\"",
  "ContentType": "binary/octet-stream",
  "ServerSideEncryption": "AES256",
  "Metadata": {}
}
```

## 管理儲存貯體和物件

以下是管理 Lightsail 物件儲存貯體的一般步驟：

1. 了解 Amazon Lightsail 物件儲存服務中的物件和值區。如需詳細資訊，請參閱 [Amazon Lightsail 中的物件儲存](#)。
2. 了解您可以在 Amazon Lightsail 中為您的儲存貯體提供哪些名稱。如需詳細資訊，請參閱 [Amazon Lightsail 中的儲存貯體命名規則](#)。
3. 透過建立值區開始使用 Lightsail 物件儲存服務。如需詳細資訊，請參閱 [在 Amazon Lightsail 中建立值區](#)。
4. 了解儲存貯體的安全最佳實務，以及可以為儲存貯體設定的存取許可。可以將儲存貯體中的所有物件設為公有或私有，也可以選擇將個別物件設為公有。您也可以建立存取金鑰、將執行個體附加至儲存貯體，以及授予其他AWS帳戶的存取權，以授予儲存貯體的存取權。如需詳細資訊，請參閱 [Amazon Lightsail 物件儲存的安全最佳實務和了解 Amazon Lightsail 中的儲存貯體許可](#)。

了解儲存貯體存取許可後，請參閱下列指南來授予對儲存貯體的存取權：

- [封鎖儲存貯體的公開存取](#)
- [在 Amazon Lightsail 集團中設定儲存貯體存取權限](#)
- [在 Amazon Lightsail 中為儲存貯體中的個別物件設定存取權限](#)

- [在 Amazon Lightsail 中為存儲桶創建訪問密鑰](#)
  - [在 Amazon Lightsail 中設定儲存貯體的資源存取](#)
  - [在 Amazon Lightsail 中設定儲存貯體的跨帳戶存取](#)
5. 了解如何為儲存貯體啟用存取日誌記錄，以及如何使用存取日誌來稽核儲存貯體的安全性。如需詳細資訊，請參閱下列指南。
- [Amazon Lightsail 物件儲存服務中儲存貯體的存取記錄](#)
  - [存取 Amazon Lightsail 物件儲存服務中儲存貯體的日誌格式](#)
  - [在 Amazon Lightsail 物件儲存服務中啟用儲存貯體的存取記錄](#)
  - [在 Amazon Lightsail 中使用儲存貯體的存取日誌來識別請求](#)
6. 建立IAM政策以授與使用者在 Lightsail 中管理值區的能力。如需詳細資訊，請參閱[在 Amazon Lightsail 中管理儲存貯體的IAM政策](#)。
7. 了解儲存貯體中物件的標記和識別方式。如需詳細資訊，請參閱[了解 Amazon Lightsail 中的物件金鑰名稱](#)。
8. 了解如何在儲存貯體中上傳檔案及管理物件。如需詳細資訊，請參閱下列指南。
- [將文件上傳到 Amazon Lightsail](#)
  - [使用多部分上傳將檔案上傳到 Amazon Lightsail 中的儲存貯體](#)
  - [檢視儲存貯體中 Amazon Lightsail](#)
  - [在 Amazon Lightsail 中複製或移動值區中的物件](#)
  - [從儲存貯體下 Amazon Lightsail](#)
  - [在 Amazon Lightsail 中過濾存儲桶中的對象](#)
  - [標記存儲桶中 Amazon Lightsail](#)
  - [刪除存儲桶中 Amazon Lightsail](#)
9. 啟用物件版本控制功能來保留、擷取和恢復儲存貯體中所儲存每個物件的各個版本。如需詳細資訊，請參閱在 [Amazon Lightsail 中啟用和暫停儲存貯體中的物件版本控制](#)。
10. 啟用物件版本控制之後，可以還原儲存貯體中物件的先前版本。如需詳細資訊，請參閱在 [Amazon Lightsail 中還原儲存貯體中的舊版物件](#)。
11. 監控儲存貯體的使用率。如需詳細資訊，請參閱[在 Amazon Lightsail 中檢視儲存貯體的指標](#)。
12. 設定儲存貯體指標的警示，以便在儲存貯體的使用率超過閾值時收到通知。如需詳細資訊，請參閱[在 Amazon Lightsail 中建立儲存貯體指標警示](#)。
13. 如果儲存空間和網路傳輸不足，請變更儲存貯體的儲存計畫。如需詳細資訊，請參閱[在 Amazon Lightsail 中變更儲存貯體的計畫](#)。

14. 了解如何將儲存貯體連線至其他資源。如需詳細資訊，請參閱下列教學課程。

- [教學課程：將 WordPress 執行個體連接至 Amazon Lightsail 儲存貯體](#)
- [教學課程：將 Amazon Lightsail 儲存貯體與 Lightsail 內容交付網路分發搭配使用](#)

15. 如果不再使用儲存貯體，請刪除它。如需詳細資訊，請參閱[刪除儲存貯體](#)。

## 依名稱前置詞篩選 Lightsail 值區中的物件

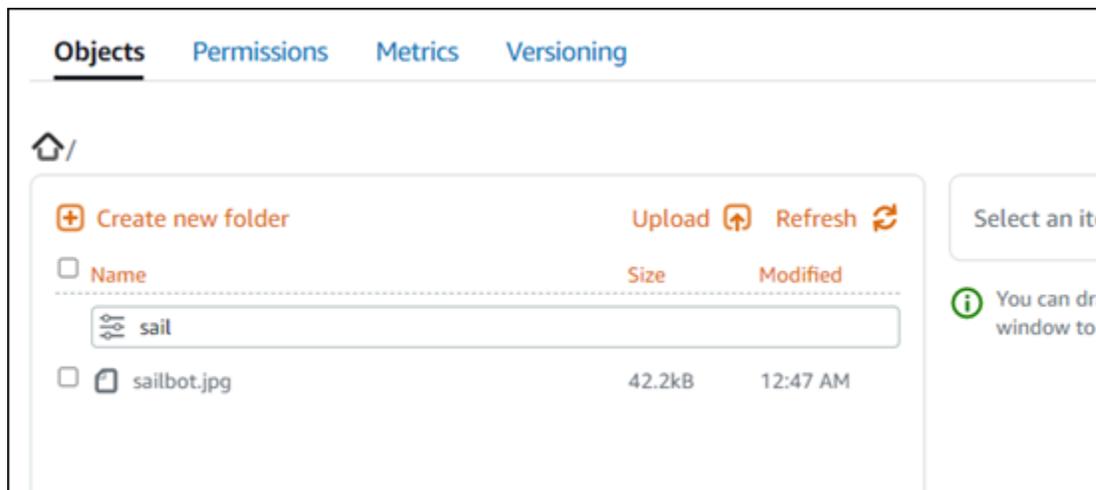
您可以使用篩選功能在 Amazon Lightsail 物件儲存服務中尋找值區中的物件。在本指南中，我們將向您展示如何使用 Lightsail 主控台和 AWS Command Line Interface (AWS CLI) 來篩選物件。如需有關儲存貯體的詳細資訊，請參閱[物件儲存](#)。

### 使用主控台篩選物件

請完成下列程序，以使用 Lightsail 主控台篩選值區中的物件。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁上，選擇儲存空間索引標籤。
3. 選擇您要尋找物件之目標儲存貯體的名稱。
4. 在 Objects (物件) 索引標籤中，在 Filter by name (依名稱篩選) 文字方塊中輸入物件字首。

您目前正在檢視的資料夾中的物件清單會經過篩選，以符合您輸入的文字。下列範例顯示，如果您輸入 `sail`，頁面上的物件清單會經過篩選，以僅顯示以 `sail` 開頭的物件。



若要篩選不同資料夾中的物件清單，請導覽至該資料夾。然後，在該處的 Filter by name (依名稱篩選) 文字方塊中輸入物件字首。

## 使用篩選物件 AWS CLI

完成下列程序，使用 AWS Command Line Interface (AWS CLI) 主控台在儲存貯體中篩選物件。您可以使用 `list-objects-v2` 命令來執行此動作。若要取得更多資訊，請參閱《AWS CLI 指令參考》中的 [list-objects-v2](#)。

### Note

您必須先為 Lightsail AWS CLI 和 Amazon S3 安裝並進行設定，然後才能繼續執行此程序。如需詳細資訊，請參閱[設定 AWS Command Line Interface 以與 Amazon Lightsail 搭配使用](#)。

1. 開啟命令提示或終端機視窗。
2. 輸入下列命令，以列出以特定物件索引鍵名稱字首開頭的物件。

```
aws s3api list-objects-v2 --bucket BucketName --prefix ObjectKeyNamePrefix --query "Contents[].{Key: Key, Size: Size}"
```

將命令中的以下範例文字取代為自訂文字：

- *BucketName* -您要列出所有物件的值區名稱。
- *ObjectKeyNamePrefix* -物件索引鍵名稱前置詞，可限制回應以指定前置字元開頭的金鑰。

### Note

這個命令會使用 `--query` 參數來篩選 `list-objects-v2` 請求的回應，而該請求針對每個物件的索引鍵值和大小。

範例：

```
aws s3api list-objects-v2 --bucket amzn-s3-demo-bucket --prefix archived/ --query "Contents[].{Key: Key, Size: Size}"
```

您應該會看到類似以下範例的結果。

```
C:\>aws s3api list-objects-v2 --bucket DOC-EXAMPLE-BUCKET --prefix archived/ --query "Contents[].[Key: Key, Size: Size]"
[
  {
    "Key": "archived/",
    "Size": 0
  },
  {
    "Key": "archived/1_CMoFsPfso.jpg",
    "Size": 2561865
  },
  {
    "Key": "archived/3y1zF4hIPCg.jpg",
    "Size": 6404907
  },
  {
    "Key": "archived/5IH5WhosQE.jpg",
    "Size": 2377975
  },
  {
    "Key": "archived/sailbot.jpg",
    "Size": 43246
  }
]
```

## 管理儲存貯體和物件

以下是管理 Lightsail 物件儲存貯體的一般步驟：

1. 了解 Amazon Lightsail 物件儲存服務中的物件和值區。如需詳細資訊，請參閱 [Amazon Lightsail 中的物件儲存](#)。
2. 了解您可以在 Amazon Lightsail 中為您的儲存貯體提供哪些名稱。如需詳細資訊，請參閱 [Amazon Lightsail 中的儲存貯體命名規則](#)。
3. 透過建立值區開始使用 Lightsail 物件儲存服務。如需詳細資訊，請參閱 [在 Amazon Lightsail 中建立值區](#)。
4. 了解儲存貯體的安全最佳實務，以及可以為儲存貯體設定的存取許可。可以將儲存貯體中的所有物件設為公有或私有，也可以選擇將個別物件設為公有。您也可以建立存取金鑰、將執行個體附加至儲存貯體，以及授予其他AWS帳戶的存取權，以授予儲存貯體的存取權。如需詳細資訊，請參閱 [Amazon Lightsail 物件儲存的安全最佳實務](#)和了解 [Amazon Lightsail 中的儲存貯體許可](#)。

了解儲存貯體存取許可後，請參閱下列指南來授予對儲存貯體的存取權：

- [封鎖儲存貯體的公開存取](#)
- [在 Amazon Lightsail 集團中設定儲存貯體存取權限](#)
- [在 Amazon Lightsail 中為儲存貯體中的個別物件設定存取權限](#)
- [在 Amazon Lightsail 中為存儲桶創建訪問密鑰](#)
- [在 Amazon Lightsail 中設定儲存貯體的資源存取](#)
- [在 Amazon Lightsail 中設定儲存貯體的跨帳戶存取](#)

5. 了解如何為儲存貯體啟用存取日誌記錄，以及如何使用存取日誌來稽核儲存貯體的安全性。如需詳細資訊，請參閱下列指南。
  - [Amazon Lightsail 物件儲存服務中儲存貯體的存取記錄](#)
  - [存取 Amazon Lightsail 物件儲存服務中儲存貯體的日誌格式](#)
  - [在 Amazon Lightsail 物件儲存服務中啟用儲存貯體的存取記錄](#)
  - [在 Amazon Lightsail 中使用儲存貯體的存取日誌來識別請求](#)
6. 建立IAM政策以授與使用者在 Lightsail 中管理值區的能力。如需詳細資訊，請參閱[在 Amazon Lightsail 中管理儲存貯體的IAM政策](#)。
7. 了解儲存貯體中物件的標記和識別方式。如需詳細資訊，請參閱[了解 Amazon Lightsail 中的物件金鑰名稱](#)。
8. 了解如何在儲存貯體中上傳檔案及管理物件。如需詳細資訊，請參閱下列指南。
  - [將文件上傳到 Amazon Lightsail](#)
  - [使用多部分上傳將檔案上傳到 Amazon Lightsail 中的儲存貯體](#)
  - [檢視儲存貯體中 Amazon Lightsail](#)
  - [在 Amazon Lightsail 中複製或移動值區中的物件](#)
  - [從儲存貯體下 Amazon Lightsail](#)
  - [在 Amazon Lightsail 中過濾存儲桶中的對象](#)
  - [標記存儲桶中 Amazon Lightsail](#)
  - [刪除存儲桶中 Amazon Lightsail](#)
9. 啟用物件版本控制功能來保留、擷取和恢復儲存貯體中所儲存每個物件的各個版本。如需詳細資訊，請參閱在 [Amazon Lightsail 中啟用和暫停儲存貯體中的物件版本控制](#)。
10. 啟用物件版本控制之後，可以還原儲存貯體中物件的先前版本。如需詳細資訊，請參閱在 [Amazon Lightsail 中還原儲存貯體中的舊版物件](#)。
11. 監控儲存貯體的使用率。如需詳細資訊，請參閱[在 Amazon Lightsail 中檢視儲存貯體的指標](#)。
12. 設定儲存貯體指標的警示，以便在儲存貯體的使用率超過閾值時收到通知。如需詳細資訊，請參閱[在 Amazon Lightsail 中建立儲存貯體指標警示](#)。
13. 如果儲存空間和網路傳輸不足，請變更儲存貯體的儲存計畫。如需詳細資訊，請參閱[在 Amazon Lightsail 中變更儲存貯體的計畫](#)。
14. 了解如何將儲存貯體連線至其他資源。如需詳細資訊，請參閱下列教學課程。
  - [教學課程：將 WordPress 執行個體連接至 Amazon Lightsail 儲存貯體](#)
  - [教學課程：將 Amazon Lightsail 儲存貯體與 Lightsail 內容交付網路分發搭配使用](#)
15. 如果不再使用儲存貯體，請刪除它。如需詳細資訊，請參閱[刪除儲存貯體](#)。

## 在 Lightsail 中啟用和暫停物件版本控制

Amazon Lightsail 物件儲存服務中的版本控制是將物件的多個變體保存在同一個儲存貯體中的一種方法。您可以使用版本控制功能，保留、擷取和恢復在儲存貯體中所存放之每個物件的各個版本。透過版本控制，您可以更輕鬆地復原失誤的使用者動作和故障的應用程式。當您為值區啟用版本控制時，如果 Lightsail 物件儲存服務同時收到相同物件的多個寫入要求，就會儲存所有這些物件。Lightsail 物件儲存服務中的值區預設會停用版本控制，因此您必須明確啟用它。如需有關儲存貯體的詳細資訊，請參閱[物件儲存](#)。

### Important

當您在設定有 Individual objects can be made public (read-only) (可將個別物件設為公有 (唯讀)) 存取許可的儲存貯體上啟用或暫停版本控制時，該許可會重設為 All objects are private (所有物件皆為私有)。如果您想繼續選擇將個別物件設為公有，則必須手動將儲存貯體的存取許可更改回 Individual objects can be made public (read-only) (可將個別物件設為公有 (唯讀))。如需詳細資訊，請參閱[設定儲存貯體存取許可](#)。

### 版本已停用、已啟用和已暫停的儲存貯體

值區版本控制可以是 Lightsail 主控台其中的三種狀態之一：

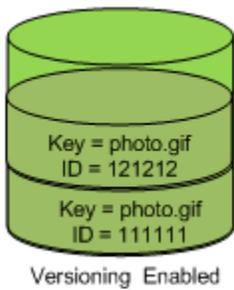
- 已停用 (NeverEnabled在API和中SDKs)
- 已啟用 (Enabled在API和中SDKs)
- 暫停 (Suspended在API和SDKs)

在儲存貯體中啟用版本控制之後，它就無法回到已停用狀態。但您可以暫停版本控制。您可以在儲存貯體層級啟用和暫停版本控制。

版本控制狀態會套用至該儲存貯體中的所有 (不是一些) 物件。當您在儲存貯體中啟用版本控制時，所有新物件都會進行版本控制，並提供唯一的版本 ID。啟用版本控制時，存在於儲存貯體中的物件一律會繼續受到版本控制。在未來請求修改這些物件時，系統會提供唯一的版本 ID。

### 版本 IDs

如果您啟用值區版本控制，Lightsail 物件儲存服務會自動為要儲存的物件產生唯一的版本 ID。例如，在一個值區中，您可以擁有兩個具有相同金鑰但版本不同的物件IDs，例如 photo.gif (版本 111111) 和 photo.gif (版本 121212)。



IDs無法編輯版本。它們是 Unicode，UTF-8 編碼，URL就緒，不透明的字符串，長度不超過 1,024 個字節。下列為版本 ID 的範例：

```
3sL4kqtJ1cpXroDTDmJ+rmSpXd3dIbrHY+MTRCxf3vjVBH40Nr8X8gdRQBpUMLUo
```

## 使用 Lightsail 主控台啟用或暫停物件版本控制

若要使用 Lightsail 主控台啟用或暫停物件版本化，請完成下列程序。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁上，選擇儲存空間索引標籤。
3. 選擇要為其啟用或暫停版本控制之儲存貯體的名稱。
4. 選擇 Versioning (版本控制) 索引標籤。
5. 根據儲存貯體的目前版本控制狀態，完成下列其中一個動作：
  - 如果版本控制目前已暫停或尚未啟用，請選擇該頁面 Object versioning (物件版本控制) 區段下的切換開關，以啟用版本控制。
  - 如果目前已啟用版本控制，請選擇該頁面的 Object versioning (物件版本控制) 區段下的切換開關，以暫停版本控制。

## 啟用或暫停物件版本化 AWS CLI

請完成下列程序，以使用 AWS Command Line Interface (AWS CLI) 來啟用或暫停物件版本控制。您可以使用 `update-bucket` 命令來執行此動作。如需詳細資訊，請參閱《AWS CLI 命令參考》中的 [update-bucket](#)。

**Note**

您必須先為 Lightsail AWS CLI 和 Amazon S3 安裝並進行設定，然後才能繼續執行此程序。如需詳細資訊，請參閱[設定 AWS CLI 定使用 Lightsail](#)。

1. 開啟命令提示或終端機視窗。
2. 輸入下列命令，以啟用或暫停物件版本控制。

```
aws lightsail update-bucket --bucket-name BucketName --versioning VersioningState
```

將命令中的以下範例文字取代為自訂文字：

- *BucketName* -您要啟用物件版本管理的值區名稱。
- *VersioningState* -下列其中一項：
  - Enabled – 啟用物件版本控制。
  - Suspended – 暫停物件版本控制 (如果先前已啟用)。

範例：

```
aws lightsail update-bucket --bucket-name amzn-s3-demo-bucket --versioning Enabled
```

您應該會看到類似以下範例的結果：

```
C:\>aws lightsail update-bucket --bucket-name DOC-EXAMPLE-BUCKET --versioning Enabled
{
  "bucket": {
    "resourceType": "Bucket",
    "accessRules": {
      "getObject": "private",
      "allowPublicOverrides": false
    },
    "arn": "arn:aws:lightsail:us-west-2:1example7491:Bucket/f067383e-ee41-4485-b934-example2e2fd",
    "bundleId": "small_1_0",
    "createdAt": "2021-06-29T08:12:39.163000-07:00",
    "url": "https://DOC-EXAMPLE-BUCKET.s3.us-west-2.amazonaws.com",
    "location": {
      "availabilityZone": "all",
      "regionName": "us-west-2"
    },
    "name": "DOC-EXAMPLE-BUCKET",
    "supportCode": "621291663362/DOC-EXAMPLE-BUCKET/small_1_0",
    "tags": [],
    "objectVersioning": "Enabled",
    "ableToUpdateBundle": true
  },
  "operations": [
    {
      "id": "0d53d290-f4b2-43f0-89d2-example43448",
      "resourceName": "DOC-EXAMPLE-BUCKET",
      "resourceType": "Bucket",
      "createdAt": "2021-06-29T08:29:56.241000-07:00",
      "location": {
        "availabilityZone": "all",
        "regionName": "us-west-2"
      },
      "isTerminal": true,
      "operationDetails": "6example3362/DOC-EXAMPLE-BUCKET/small_1_0",
      "operationType": "UpdateBucket",
      "status": "Succeeded",
      "statusChangedAt": "2021-06-29T08:29:56.241000-07:00",
      "errorCode": "",
      "errorDetails": ""
    }
  ]
}
```

## 管理儲存貯體和物件

以下是管理 Lightsail 物件儲存貯體的一般步驟：

1. 了解 Amazon Lightsail 物件儲存服務中的物件和值區。如需詳細資訊，請參閱 [Amazon Lightsail 中的物件儲存](#)。
2. 了解您可以在 Amazon Lightsail 中為您的儲存貯體提供哪些名稱。如需詳細資訊，請參閱 [Amazon Lightsail 中的儲存貯體命名規則](#)。
3. 透過建立值區開始使用 Lightsail 物件儲存服務。如需詳細資訊，請參閱 [在 Amazon Lightsail 中建立值區](#)。

4. 了解儲存貯體的安全最佳實務，以及可以為儲存貯體設定的存取許可。可以將儲存貯體中的所有物件設為公有或私有，也可以選擇將個別物件設為公有。您也可以建立存取金鑰、將執行個體附加至儲存貯體，以及授予其他AWS帳戶的存取權，以授予儲存貯體的存取權。如需詳細資訊，請參閱 [Amazon Lightsail 物件儲存的安全最佳實務](#) 和 [了解 Amazon Lightsail 中的儲存貯體許可](#)。

了解儲存貯體存取許可後，請參閱下列指南來授予對儲存貯體的存取權：

- [封鎖儲存貯體的公開存取](#)
  - [在 Amazon Lightsail 中設定儲存貯體存取權限](#)
  - [在 Amazon Lightsail 中為儲存貯體中的個別物件設定存取權限](#)
  - [在 Amazon Lightsail 中為存儲桶創建訪問密鑰](#)
  - [在 Amazon Lightsail 中設定儲存貯體的資源存取](#)
  - [在 Amazon Lightsail 中設定儲存貯體的跨帳戶存取](#)
5. 了解如何為儲存貯體啟用存取日誌記錄，以及如何使用存取日誌來稽核儲存貯體的安全性。如需詳細資訊，請參閱下列指南。
    - [Amazon Lightsail 物件儲存服務中儲存貯體的存取記錄](#)
    - [存取 Amazon Lightsail 物件儲存服務中儲存貯體的日誌格式](#)
    - [在 Amazon Lightsail 物件儲存服務中啟用儲存貯體的存取記錄](#)
    - [在 Amazon Lightsail 中使用儲存貯體的存取日誌來識別請求](#)
  6. 建立IAM政策以授與使用者在 Lightsail 中管理值區的能力。如需詳細資訊，請參閱 [在 Amazon Lightsail 中管理儲存貯體的IAM政策](#)。
  7. 了解儲存貯體中物件的標記和識別方式。如需詳細資訊，請參閱 [了解 Amazon Lightsail 中的物件金鑰名稱](#)。
  8. 了解如何在儲存貯體中上傳檔案及管理物件。如需詳細資訊，請參閱下列指南。
    - [將文件上傳到 Amazon Lightsail](#)
    - [使用多部分上傳將檔案上傳到 Amazon Lightsail 中的儲存貯體](#)
    - [檢視儲存貯體中 Amazon Lightsail](#)
    - [在 Amazon Lightsail 中複製或移動值區中的物件](#)
    - [從儲存貯體中下載物件](#)
    - [在 Amazon Lightsail 中過濾存儲桶中的對象](#)
    - [標記存儲桶中 Amazon Lightsail](#)
    - [刪除存儲桶中 Amazon Lightsail](#)

9. 啟用物件版本控制功能來保留、擷取和恢復儲存貯體中所儲存每個物件的各個版本。如需詳細資訊，請參閱在 [Amazon Lightsail 中啟用和暫停儲存貯體中的物件版本控制](#)。
10. 啟用物件版本控制之後，可以還原儲存貯體中物件的先前版本。如需詳細資訊，請參閱在 [Amazon Lightsail 中還原儲存貯體中的舊版物件](#)。
11. 監控儲存貯體的使用率。如需詳細資訊，請參閱在 [Amazon Lightsail 中檢視儲存貯體的指標](#)。
12. 設定儲存貯體指標的警示，以便在儲存貯體的使用率超過閾值時收到通知。如需詳細資訊，請參閱在 [Amazon Lightsail 中建立儲存貯體指標警示](#)。
13. 如果儲存空間和網路傳輸不足，請變更儲存貯體的儲存計畫。如需詳細資訊，請參閱在 [Amazon Lightsail 中變更儲存貯體的計畫](#)。
14. 了解如何將儲存貯體連線至其他資源。如需詳細資訊，請參閱下列教學課程。
  - [教學課程：將 WordPress 執行個體連接至 Amazon Lightsail 儲存貯體](#)
  - [教學課程：將 Amazon Lightsail 儲存貯體與 Lightsail 內容交付網路分發搭配使用](#)
15. 如果不再使用儲存貯體，請刪除它。如需詳細資訊，請參閱在 [Amazon Lightsail 中刪除值區](#)。

## 在 Lightsail 值區中復原先前的物件版本

如果 Amazon Lightsail 物件儲存服務中的儲存貯體已啟用版本功能，則您可以還原物件的先前版本。為非預期的使用者動作失誤或應用程式故障中復原的物件還原舊版本。

您可以使用 Lightsail 主控台還原物件的先前版本。您也可以使用 AWS Command Line Interface (AWS CLI) 並 AWS SDKs 還原物件的先前版本。若要執行此操作，請將物件的特定版本複製到相同的儲存貯體，並使用相同的物件索引鍵名稱。這麼做會以舊版本取代目前版本，使舊版本成為目前版本。如需有關版本控制的詳細資訊，請參閱 [啟用和暫停儲存貯體物件版本控制](#)。如需有關儲存貯體的詳細資訊，請參閱 [物件儲存](#)。

### 使用 Lightsail 主控台還原物件的先前版本

若要使用 Lightsail 主控台還原物件的先前版本，請完成下列程序。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁上，選擇儲存空間索引標籤。
3. 選擇您要還原物件舊版本之儲存貯體的名稱。
4. 使用 Objects (物件) 索引標籤中的 Objects browser (物件瀏覽器) 窗格瀏覽至物件所在的位置。
5. 在您要還原舊版本的物件旁邊新增核取記號。

6. 選擇 Object information (物件資訊) 窗格的 Versions (版本) 區段下的 Manage (管理)。
7. 選擇 Restore (還原)。
8. 在出現的已存放版本窗格的 Restore object (還原物件) 中，選擇您要還原的物件版本。
9. 選擇 Continue (繼續)。
10. 在出現的確認提示中，選擇 Yes, restore (是，還原) 以還原物件版本。否則，請選擇 No, cancel (否，取消)。

## 使用還原物件的先前版本 AWS CLI

完成下列程序，以使用 AWS Command Line Interface (AWS CLI) 還原物件的舊版本。您可以使用 `copy-object` 命令來執行此動作。您必須使用相同的物件索引鍵，將物件的舊版本複製到相同的儲存貯體。如需詳細資訊，請參閱《AWS CLI 命令參考》中的 [copy-object](#)。

### Note

您必須先為 Lightsail AWS CLI 和 Amazon S3 安裝並進行設定，然後才能繼續執行此程序。如需詳細資訊，請參閱[設定 AWS Command Line Interface 以與 Amazon Lightsail 搭配使用](#)。

1. 開啟命令提示或終端機視窗。
2. 輸入以下指令，以還原物件的舊版本。

```
aws s3api copy-object --copy-source "BucketName/ObjectKey?versionId=VersionId" --  
key ObjectKey --bucket BucketName
```

將命令中的以下範例文字取代為自訂文字：

- ***BucketName*** -您要還原物件先前版本的值區名稱。您必須為 `--copy-source` 和 `--bucket` 參數指定相同的儲存貯體名稱。
- ***ObjectKey*** -要還原的物件名稱。您必須為 `--copy-source` 和 `--key` 參數指定相同的物件索引鍵名稱。
- ***VersionId*** -您要還原至目前版本之前物件版本的 ID。使用 `list-object-versions` 指令取得值區中物件IDs的版本清單。

範例：

```
aws s3api copy-object --copy-source "amzn-s3-demo-bucket/sailbot.jpg?
versionId=GQWEexample87Md18Q_DKdVTiVMi_VyU" --key sailbot.jpg --bucket amzn-s3-demo-
bucket
```

您應該會看到類似以下範例的結果：

```
C:\>aws s3api copy-object --copy-source "DOC-EXAMPLE-BUCKET/sailbot.jpg?versionId=GQWEexample87Md18Q_DKdVTiVMi_VyU"
--key sailbot.jpg --bucket DOC-EXAMPLE-BUCKET
{
  "CopySourceVersionId": "GQWEexample87Md18Q_DKdVTiVMi_VyU",
  "VersionId": "hjl8anKzI1xcXYexampleDvvqMXSLoi",
  "ServerSideEncryption": "AES256",
  "CopyObjectResult": {
    "ETag": "\"dc5afd388fb3example20cda3fe41c54\"",
    "LastModified": "2021-05-16T06:45:35+00:00"
  }
}
```

## 管理儲存貯體和物件

以下是管理 Lightsail 物件儲存貯體的一般步驟：

1. 了解 Amazon Lightsail 物件儲存服務中的物件和值區。如需詳細資訊，請參閱 [Amazon Lightsail 中的物件儲存](#)。
2. 了解您可以在 Amazon Lightsail 中為您的儲存貯體提供哪些名稱。如需詳細資訊，請參閱 [Amazon Lightsail 中的儲存貯體命名規則](#)。
3. 透過建立值區開始使用 Lightsail 物件儲存服務。如需詳細資訊，請參閱 [在 Amazon Lightsail 中建立值區](#)。
4. 了解儲存貯體的安全最佳實務，以及可以為儲存貯體設定的存取許可。可以將儲存貯體中的所有物件設為公有或私有，也可以選擇將個別物件設為公有。您也可以建立存取金鑰、將執行個體附加至儲存貯體，以及授予其他AWS帳戶的存取權，以授予儲存貯體的存取權。如需詳細資訊，請參閱 [Amazon Lightsail 物件儲存的安全最佳實務和了解 Amazon Lightsail 中的儲存貯體許可](#)。

了解儲存貯體存取許可後，請參閱下列指南來授予對儲存貯體的存取權：

- [封鎖儲存貯體的公 Amazon Lightsail](#)
- [在 Amazon Lightsail 中設定儲存貯體存取權限](#)
- [在 Amazon Lightsail 中為儲存貯體中的個別物件設定存取權限](#)
- [在 Amazon Lightsail 中為存儲桶創建訪問密鑰](#)
- [在 Amazon Lightsail 中設定儲存貯體的資源存取](#)
- [在 Amazon Lightsail 中設定儲存貯體的跨帳戶存取](#)

5. 了解如何為儲存貯體啟用存取日誌記錄，以及如何使用存取日誌來稽核儲存貯體的安全性。如需詳細資訊，請參閱下列指南。
  - [Amazon Lightsail 物件儲存服務中儲存貯體的存取記錄](#)
  - [存取 Amazon Lightsail 物件儲存服務中儲存貯體的日誌格式](#)
  - [在 Amazon Lightsail 物件儲存服務中啟用儲存貯體的存取記錄功能](#)
  - [在 Amazon Lightsail 中使用儲存貯體的存取日誌來識別請求](#)
6. 建立IAM政策，讓使用者能夠在 Lightsail 中管理值區。如需詳細資訊，請參閱[在 Amazon Lightsail 中管理儲存貯體的IAM政策](#)。
7. 了解儲存貯體中物件的標記和識別方式。如需詳細資訊，請參閱[了解 Amazon Lightsail 中的物件金鑰名稱](#)。
8. 了解如何在儲存貯體中上傳檔案及管理物件。如需詳細資訊，請參閱下列指南。
  - [將文件上傳到 Amazon Lightsail](#)
  - [使用多部分上傳將檔案上傳到 Amazon Lightsail 中的儲存貯體](#)
  - [檢視儲存貯體中 Amazon Lightsail](#)
  - [在 Amazon Lightsail 中複製或移動值區中的物件](#)
  - [從儲存貯體下 Amazon Lightsail](#)
  - [在 Amazon Lightsail 中過濾存儲桶中的對象](#)
  - [標記存儲桶中 Amazon Lightsail](#)
  - [刪除存儲桶中 Amazon Lightsail](#)
9. 啟用物件版本控制功能來保留、擷取和恢復儲存貯體中所儲存每個物件的各個版本。如需詳細資訊，請參閱在 [Amazon Lightsail 中啟用和暫停儲存貯體中的物件版本控制](#)。
10. 啟用物件版本控制之後，可以還原儲存貯體中物件的先前版本。如需詳細資訊，請參閱在 [Amazon Lightsail 中還原儲存貯體中的舊版物件](#)。
11. 監控儲存貯體的使用率。如需詳細資訊，請參閱[在 Amazon Lightsail 中檢視儲存貯體的指標](#)。
12. 設定儲存貯體指標的警示，以便在儲存貯體的使用率超過閾值時收到通知。如需詳細資訊，請參閱[在 Amazon Lightsail 中建立儲存貯體指標警示](#)。
13. 如果儲存空間和網路傳輸不足，請變更儲存貯體的儲存計畫。如需詳細資訊，請參閱[在 Amazon Lightsail 中變更儲存貯體的計畫](#)。
14. 了解如何將儲存貯體連線至其他資源。如需詳細資訊，請參閱下列教學課程。
  - [教學課程：將 WordPress 執行個體連接至 Amazon Lightsail 儲存貯體](#)
  - [教學課程：將 Amazon Lightsail 儲存貯體與 Lightsail 內容交付網路分發搭配使用](#)
15. 如果不再使用儲存貯體，請刪除它。如需詳細資訊，請參閱[刪除儲存貯體](#)。

## 在 Lightsail 值區中標記物件

在儲存貯體中標記物件以依據用途、擁有者、環境或其他條件對物件進行分類。您可以在上傳物件時或在上傳物件之後，為這些物件新增標籤。如需有關儲存貯體的詳細資訊，請參閱[物件儲存](#)。

### 使用 Lightsail 主控台新增和刪除物件的標籤

請完成下列程序，以使用 Lightsail 主控台從值區中的物件新增或刪除標籤。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁上，選擇儲存空間索引標籤。
3. 選擇您要標記物件之儲存貯體的名稱。
4. 使用 Objects (物件) 索引標籤中的 Objects browser (物件瀏覽器) 窗格瀏覽至物件所在的位置。
5. 在您要新增或刪除標籤的物件旁新增核取記號。
6. 在物件資訊窗格中，在 Object tags (物件標籤) 區段下選擇下列其中一個選項：
  - Add (新增) 或 Edit (編輯) (若已新增標籤)。將索引鍵輸入 Key (索引鍵) 文字方塊，並將值輸入 Value (值) 文字方塊。然後選擇 Save (儲存) 以新增標籤。否則，請選擇 Cancel (取消)。
  - Edit (編輯)，然後在您要刪除的索引鍵值標籤旁選擇 X。刪除標籤後，選擇 Save (儲存)，或選擇 Cancel (取消) 以取消刪除標籤。

### 使用 AWS CLI 新增和刪除物件標籤

完成下列程序，以使用 AWS Command Line Interface (AWS CLI) 將標籤新增至物件或刪除物件中的標籤。您可以使用 `put-object-tagging` 和 `delete-object-tagging` 命令來執行此操作。若要取得更多資訊，請參閱《AWS CLI 指令參考》[delete-object-tagging](#) 中的 [put-object-tagging](#) 和。

#### Note

您必須先為 Lightsail AWS CLI 和 Amazon S3 安裝並進行設定，然後才能繼續執行此程序。如需詳細資訊，請參閱[設 AWS CLI 定使用 Lightsail](#)。

1. 開啟命令提示或終端機視窗。
2. 輸入下列其中一個命令：
  - 若要將標籤新增至物件：

```
aws s3api put-object-tagging --bucket BucketName --key ObjectKey --tagging
"{\"TagSet\": [{ \"Key\": \"KeyTag\", \"Value\": \"ValueTag\" } ]}"
```

將命令中的以下範例文字取代為自訂文字：

- *BucketName* -包含您要標記之物件的值區名稱。
- *ObjectKey* -您要標記的物件的完整物件金鑰。
- *KeyTag* -標籤的關鍵值。
- *ValueTag* -你的標籤的價值。
- 若要將標籤新增至物件：

```
aws s3api put-object-tagging --bucket BucketName --key ObjectKey --tagging
"{\"TagSet\": [{ \"Key\": \"KeyTag1\", \"Value\": \"ValueTag1\" }, { \"Key\":
\"KeyTag2\", \"Value\": \"ValueTag2\" } ]}"
```

將命令中的以下範例文字取代為自訂文字：

- *BucketName* -包含您要標記之物件的值區名稱。
- *ObjectKey* -您要標記的物件的完整物件金鑰。
- *KeyTag1* -第一個標籤的關鍵值。
- *ValueTag1* -您的第一個標籤的價值。
- *KeyTag2* -第二個標籤的關鍵值。
- *ValueTag2* -第二個標籤的價值。
- 若要刪除物件上的全部標籤：

```
aws s3api delete-object-tagging --bucket BucketName --key ObjectKey
```

將命令中的以下範例文字取代為自訂文字：

- *BucketName* -包含您要刪除其所有標籤之物件的值區名稱。
- *ObjectKey* -您要標記的物件的完整物件金鑰。

範例：

```
aws s3api delete-object --bucket amzn-s3-demo-bucket --key nptLmg6jqDo.jpg --
tagging "{ \"TagSet\": [{ \"Key\": \"Importance\", \"Value\": \"High\" } ]}"
```

您應該會看到類似以下範例的結果：

```
C:\>aws s3api put-object-tagging --bucket DOC-EXAMPLE-BUCKET --key nptLmg6jqDo.jpg
--tagging "{\"TagSet\": [{ \"Key\": \"Importance\", \"Value\": \"High\" } ]}"
{
  "VersionId": "9nL2d41NuZdhdk4HS3kZIwOxJeS1kCkm"
}
```

## 管理儲存貯體和物件

以下是管理 Lightsail 物件儲存貯體的一般步驟：

1. 了解 Amazon Lightsail 物件儲存服務中的物件和值區。如需詳細資訊，請參閱 [Amazon Lightsail 中的物件儲存](#)。
2. 了解您可以在 Amazon Lightsail 中為您的儲存貯體提供哪些名稱。如需詳細資訊，請參閱 [Amazon Lightsail 中的儲存貯體命名規則](#)。
3. 透過建立值區開始使用 Lightsail 物件儲存服務。如需詳細資訊，請參閱 [在 Amazon Lightsail 中建立值區](#)。
4. 了解儲存貯體的安全最佳實務，以及可以為儲存貯體設定的存取許可。可以將儲存貯體中的所有物件設為公有或私有，也可以選擇將個別物件設為公有。您也可以建立存取金鑰、將執行個體附加至儲存貯體，以及授予其他AWS帳戶的存取權，以授予儲存貯體的存取權。如需詳細資訊，請參閱 [Amazon Lightsail 物件儲存的安全最佳實務和了解 Amazon Lightsail 中的儲存貯體許可](#)。

了解儲存貯體存取許可後，請參閱下列指南來授予對儲存貯體的存取權：

- [封鎖儲存貯體的公開存取](#)
  - [在 Amazon Lightsail 中設定儲存貯體存取權限](#)
  - [在 Amazon Lightsail 中為儲存貯體中的個別物件設定存取權限](#)
  - [在 Amazon Lightsail 中為存儲桶創建訪問密鑰](#)
  - [在 Amazon Lightsail 中設定儲存貯體的資源存取](#)
  - [在 Amazon Lightsail 中設定儲存貯體的跨帳戶存取](#)
5. 了解如何為儲存貯體啟用存取日誌記錄，以及如何使用存取日誌來稽核儲存貯體的安全性。如需詳細資訊，請參閱下列指南。
    - [Amazon Lightsail 物件儲存服務中儲存貯體的存取記錄](#)
    - [存取 Amazon Lightsail 物件儲存服務中儲存貯體的日誌格式](#)
    - [在 Amazon Lightsail 物件儲存服務中啟用儲存貯體的存取記錄](#)

- [在 Amazon Lightsail 中使用儲存貯體的存取日誌來識別請求](#)
6. 建立IAM政策，讓使用者能夠在 Lightsail 中管理值區。如需詳細資訊，請參閱[在 Amazon Lightsail 中管理儲存貯體的IAM政策](#)。
  7. 了解儲存貯體中物件的標記和識別方式。如需詳細資訊，請參閱[了解 Amazon Lightsail 中的物件金鑰名稱](#)。
  8. 了解如何在儲存貯體中上傳檔案及管理物件。如需詳細資訊，請參閱下列指南。
    - [將文件上傳到 Amazon Lightsail](#)
    - [使用多部分上傳將檔案上傳到 Amazon Lightsail 中的儲存貯體](#)
    - [檢視儲存貯體中 Amazon Lightsail](#)
    - [在 Amazon Lightsail 中複製或移動值區中的物件](#)
    - [從儲存貯體下 Amazon Lightsail](#)
    - [在 Amazon Lightsail 中過濾存儲桶中的對象](#)
    - [標記存儲桶中 Amazon Lightsail](#)
    - [刪除存儲桶中 Amazon Lightsail](#)
  9. 啟用物件版本控制功能來保留、擷取和恢復儲存貯體中所儲存每個物件的各個版本。如需詳細資訊，請參閱在 [Amazon Lightsail 中啟用和暫停儲存貯體中的物件版本控制](#)。
  10. 啟用物件版本控制之後，可以還原儲存貯體中物件的先前版本。如需詳細資訊，請參閱在 [Amazon Lightsail 中還原儲存貯體中的舊版物件](#)。
  11. 監控儲存貯體的使用率。如需詳細資訊，請參閱[在 Amazon Lightsail 中檢視儲存貯體的指標](#)。
  12. 設定儲存貯體指標的警示，以便在儲存貯體的使用率超過閾值時收到通知。如需詳細資訊，請參閱[在 Amazon Lightsail 中建立儲存貯體指標警示](#)。
  13. 如果儲存空間和網路傳輸不足，請變更儲存貯體的儲存計畫。如需詳細資訊，請參閱[在 Amazon Lightsail 中變更儲存貯體的計畫](#)。
  14. 了解如何將儲存貯體連線至其他資源。如需詳細資訊，請參閱下列教學課程。
    - [教學課程：將 WordPress 執行個體連接至 Amazon Lightsail 儲存貯體](#)
    - [教學課程：將 Amazon Lightsail 儲存貯體與 Lightsail 內容交付網路分發搭配使用](#)
  15. 如果不再使用儲存貯體，請刪除它。如需詳細資訊，請參閱[刪除儲存貯體](#)。

## 控制執行個體對 Lightsail 值區的存取

將 Amazon Lightsail 執行個體連接至 Lightsail 儲存貯體，以便提供儲存貯體及其物件的完整程式設計存取權。當您將執行個體連接至儲存貯體時，您不必管理憑證 (如存取金鑰)。您附接的執行個體和儲存貯體必須位於相同的 AWS 區域中。您無法將執行個體連接至位於不同區域的儲存貯體。

如果您在執行個體上設定軟體或外掛程式，以直接將檔案上傳至儲存貯體，則資源存取會非常適合。例如，如果您想要將 WordPress 執行個體設定為將媒體檔案儲存在值區上。如需詳細資訊，請參閱[教學課程：將值區 Connect 至 WordPress 執行個體](#)。

如需有關許可選項的詳細資訊，請參閱[儲存貯體許可](#)。如需安全最佳實務的詳細資訊，請參閱[物件儲存的安全最佳實務](#)。如需有關儲存貯體的詳細資訊，請參閱[物件儲存](#)。

### 設定儲存貯體的資源存取

請完成下列程序來設定儲存貯體的資源存取。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁上，選擇儲存空間索引標籤。
3. 選擇您要設定資源存取之儲存貯體的名稱。
4. 選擇許可索引標籤標籤。

該頁面的 Resource access (資源存取) 區段會顯示目前連接至儲存貯體的執行個體 (如果有)。

5. 選擇 Attach instance (連接執行個體)，將執行個體連接至儲存貯體。
6. 在 Select an instance (選取執行個體) 下拉式選單中，選取您要連接至儲存貯體的執行個體。

#### Note

您只能連接正在執行中或停止狀態的執行個體。此外，您只能附加與值區位於相同 AWS 區域的執行個體。

7. 選擇 Attach (連接) 以連接執行個體。否則，請選擇 Cancel (取消)。

執行個體在連接後可以完全存取儲存貯體及其物件。您可以在執行個體上設定軟體或外掛程式，以程式設計方式上傳和存取在儲存貯體中的檔案。例如，如果您想要將 WordPress 執行個體設定為將媒體檔案儲存在值區上。如需詳細資訊，請參閱[教學課程：將值區 Connect 至 WordPress 執行個體](#)。

## 針對使用量波動調整 Lightsail 儲存貯體計劃

在 Amazon Lightsail 物件儲存服務中，儲存貯體的儲存計劃會指定其每月成本、儲存空間配額和資料傳輸配額。在每月計 AWS 費週期內，您只能更新儲存貯體的儲存空間方案一次。當您變更儲存貯體的儲存計劃時，儲存空間和網路傳輸配額會重設。不過，您使用先前的儲存計劃可能產生的超額儲存空間和資料傳輸費不涵蓋在內。

如果儲存貯體持續超過儲存空間或資料傳輸配額，或者儲存貯體的使用量始終在配額的較低範圍內，請更新儲存貯體的儲存計劃。由於儲存貯體可能會遇到無法預測的使用量波動，我們強烈建議您將儲存貯體儲存計劃的更新作為長期策略，而不是作為每月降低成本的短期措施。選擇一個儲存計劃，讓您的儲存貯體往後能擁有充足的儲存空間和資料傳輸配額。

如需有關儲存貯體的詳細資訊，請參閱[物件儲存](#)。

### 使用 Lightsail 主控台變更值區的儲存空間計劃

若要使用 Lightsail 主控台變更值區的儲存空間計劃，請完成下列程序。

1. 登入主 [Lightsail](#) 台。
2. 在 Lightsail 首頁上，選擇儲存空間索引標籤。
3. 選擇您要變更計劃之儲存貯體的名稱。
4. 選擇儲存貯體管理頁面中的 Metrics (指標) 索引標籤。
5. 選擇 Change storage plan (變更儲存計劃)。
6. 在顯示的確認提示中，請選擇 Yes, change (是，變更)，繼續變更儲存貯體儲存計劃。否則，請選擇 No, cancel (否，取消)。
7. 選擇您想要使用的計劃，然後選擇 Select plan (選擇計劃)。
8. 在顯示的確認提示中，請選擇 (是，套用)，將變更套用至您的儲存貯體，或選擇 No, go back (不，返回) 不套用變更。

### 使用變更儲存貯體的儲存空間計劃 AWS CLI

若要使用 AWS Command Line Interface (AWS CLI) 變更值區的計劃，請完成下列程序。您可以使用 `update-bucket-bundle` 命令來執行此動作。請注意，值區儲存體計劃在中稱為值區組合包API。若要取得更多資訊，請參閱《指AWS CLI 令參考》[update-bucket-bundle](#)中的。

**Note**

您必須先為 Lightsail AWS CLI 和 Amazon S3 安裝並進行設定，然後才能繼續執行此程序。如需詳細資訊，請參閱[設定 AWS CLI 定使用 Lightsail](#)。

1. 開啟命令提示或終端機視窗。
2. 輸入下列命令來變更儲存貯體的計劃。

```
aws lightsail update-bucket-bundle --bucket-name BucketName --bundle-id BundleID
```

在該命令中，將以下範例文字取代為自訂文字：

- *BucketName* -您要更新儲存空間計劃的值區名稱。
- *BundleID* -您要套用至值區的新值區組合包 ID。使用 `get-bucket-bundles` 指令查看可用值區套件及其清單 IDs。若要取得更多資訊，請參閱《指 AWS CLI 令參考》[get-bucket-bundles](#) 中的。

範例：

```
aws lightsail update-bucket-bundle --bucket-name amzn-s3-demo-bucket --bundle-id medium_1_0
```

您應該會看到類似以下範例的結果：

```
C:\>aws lightsail update-bucket-bundle --bucket-name DOC-EXAMPLE-BUCKET --bundle-id medium_1_0

{
  "operations": [
    {
      "id": "8example-8176-48bd-b1da-exampleb8404",
      "resourceName": "DOC-EXAMPLE-BUCKET",
      "resourceType": "Bucket",
      "createdAt": "2021-06-30T12:05:57.362000-07:00",
      "location": {
        "availabilityZone": "all",
        "regionName": "us-west-2"
      },
      "isTerminal": true,
      "operationDetails": "62example362/DOC-EXAMPLE-BUCKET/medium_1_0",
      "operationType": "UpdateBucketBundle",
      "status": "Succeeded",
      "statusChangedAt": "2021-06-30T12:05:57.362000-07:00",
      "errorCode": "",
      "errorDetails": ""
    }
  ]
}
```

## 管理 Lightsail 儲存貯體存取權限以增強安全性

使用儲存貯體存取許可來控制對儲存貯體中物件的公有 (未驗證) 唯讀存取。您可以將儲存貯體設為私有或公有 (唯讀)。您也可以將儲存貯體設為私有，同時還可以選擇將個別物件設為公有 (唯讀)。

### Important

當您將儲存貯體設為公有 (唯讀) 時，您可以透過儲存貯體的 URL (例如 <https://DOC-EXAMPLE-BUCKET.us-east-1.amazonaws.com/media/sailbot.jpg>)，讓網際網路上的任何人都可以讀取儲存貯體中的所有物件。如果您不希望網際網路上的任何人都能存取您的物件，請不要將儲存貯體設為公有 (唯讀)。

如需有關許可選項的詳細資訊，請參閱[儲存貯體許可](#)。如需安全最佳實務的詳細資訊，請參閱[物件儲存的 safety 最佳實務](#)。如需有關儲存貯體的詳細資訊，請參閱[物件儲存](#)。

### Important

Lightsail 物件儲存資源在允許或拒絕公開存取時，會將 Lightsail 儲存貯體存取權限和 Amazon S3 帳戶層級區塊公開存取組態納入考量。如需詳細資訊，請參閱[封鎖儲存貯體的公有存取](#)。

## 設定儲存貯體存取許可

請完成下列程序來設定儲存貯體的存取許可。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁上，選擇儲存空間索引標籤。
3. 選擇您要設定存取許可之儲存貯體的名稱。
4. 選擇許可索引標籤標籤。

該頁面的 Bucket access permissions (儲存貯體存取許可) 區段會顯示目前為儲存貯體設定的存取許可。

5. 選擇 Change permission (變更許可) 來變更儲存貯體的存取許可。
6. 請選擇下列其中一個選項：
  - All objects are private (所有物件皆為私有) – 儲存貯體中的所有物件僅限於您或您授予存取權的任何人讀取。
  - Individual objects can be made public (read-only) (可將個別物件設為公有 (唯讀)) – 除非您將個別物件指定為公有 (唯讀)，否則儲存貯體中的物件僅限於您或您授予存取權的任何人讀取。如需有關個別物件存取許可的詳細資訊，請參閱[在儲存貯體中設定個別物件的存取許可](#)。

建議您僅在有特定需要時，選取 Individual objects can be made public (read-only) (可將個別物件設為公有 (唯讀)) 選項，例如只將儲存貯體中的一些物件設為公有，而所有其他物件維持私有狀態。例如，某些 WordPress 外掛程式要求儲存貯體允許公開個別物件。如需詳細資訊，請參閱[教學課程：將值區 Connect 至 WordPress 執行個體](#)和[教學課程：使用含有內容傳遞網路散發的值區](#)。

- All objects are public (read-only) (所有物件皆為公有 (唯讀)) – 儲存貯體中的所有物件可供網際網路上的任何人讀取。

### Important

當您將儲存貯體設為公有 (唯讀) 時，您可以透過儲存貯體的 URL (例如 <https://DOC-EXAMPLE-BUCKET.us-east-1.amazonaws.com/media/sailbot.jpg>)，讓網際網路上的任何人都可以讀取儲存貯體中的所有物件。如果您不希望網際網路上的任何人都能存取您的物件，請不要將儲存貯體設為公有 (唯讀)。

7. 選擇 Save (儲存) 儲存變更。否則，請選擇 Cancel (取消)。

系統會根據您變更的儲存貯體存取許可實作下列變更：

- All objects are private (所有物件皆為私有) - 即使儲存貯體中所有物件先前設定為 Public (read-only) (公有 (唯讀)) 個別物件存取許可，它們也都會變為私有。
- Individual objects can be made public (read-only) (可將個別物件設為公有 (唯讀)) - 先前設定為 Public (read-only) (公有 (唯讀)) 個別物件存取許可的物件會變成公有。您現在可以設定物件的個別物件存取許可。
- All objects are public (read-only) (所有物件皆為公有 (唯讀)) - 即使儲存貯體中所有物件先前設定為 Private (私有) 個別物件存取許可，它們也都會變為公有 (唯讀)。

如需有關個別物件存取許可的詳細資訊，請參閱[在儲存貯體中設定個別物件的存取許可](#)。

## 授與跨 AWS 帳戶對 Lightsail 值區的唯讀存取權

使用跨帳戶存取，為其他 AWS 帳戶及其使用者授予儲存貯體中所有物件的唯讀存取權。如果您想與其他帳戶共享對象，則跨 AWS 帳戶訪問是理想的選擇。當您將跨帳戶存取權授予其他 AWS 帳戶時，該帳戶中的使用者可以透過儲存貯體和物件的 URL (例如 `https://DOC-EXAMPLE-BUCKET.us-east-1.amazonaws.com/media/sailbot.jpg`) 擁有儲存貯體中物件的唯讀存取權。您最多可以將儲存貯體存取權授予 10 個 AWS 帳戶。

如需有關許可選項的詳細資訊，請參閱[儲存貯體許可](#)。如需安全最佳實務的詳細資訊，請參閱[物件儲存的安全最佳實務](#)。如需有關儲存貯體的詳細資訊，請參閱[物件儲存](#)。

## 設定儲存貯體的跨帳戶存取

請完成下列程序來設定儲存貯體的跨帳戶存取。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁上，選擇儲存空間索引標籤。
3. 選擇您要設定跨帳戶存取之儲存貯體的名稱。
4. 選擇許可索引標籤標籤。

該頁面的跨帳戶存取權區段會顯示目前設定為可存取儲存貯體的 AWS 帳戶 ID (如果有)。

5. 選擇「新增跨帳戶存取權」，以授與其他 AWS 帳戶存取值區的存取權。
6. 在 [AWS 帳戶 ID] 文字方塊中輸入您要授與存取權的帳戶 ID。
7. 選擇 Save (儲存) 以授予存取權。否則，請選擇 Cancel (取消)。

您新增的 AWS 帳戶 ID 會列在頁面的「跨帳戶存取」區段中。若要移除 AWS 帳戶的跨帳戶存取權，請選擇要移除之 AWS 帳戶 ID 旁的刪除 (垃圾桶) 圖示。

## 在 Amazon Lightsail 中授予對個別值區物件的公開存取權

使用個別物件存取許可來控制儲存貯體中對個別物件的公有 (未驗證) 唯讀存取。您可以將儲存貯體中的個別物件設為私有或公有 (唯讀)。

### Important

個別物件存取許可只能在儲存貯體的存取許可設為 Individual objects can be made public (read-only) (個別物件可設為公有 (唯讀)) 時設定。如需有關儲存貯體許可選項的詳細資訊，請參閱[儲存貯體許可](#)。如需有關儲存貯體的詳細資訊，請參閱[物件儲存](#)。

建議您僅在有特定需要時設定個別物件存取許可，例如只將儲存貯體中一些物件設為公有，而所有其他物件維持私有狀態。例如，某些 WordPress 外掛程式要求儲存貯體允許公開個別物件。如需詳細資訊，請參閱[教學課程：將值區 Connect 至 WordPress 執行個體](#)和[教學課程：使用含有內容傳遞網路散發的值區](#)。

如需有關許可選項的詳細資訊，請參閱[儲存貯體許可](#)。如需安全最佳實務的詳細資訊，請參閱[物件儲存的安全最佳實務](#)。如需有關儲存貯體的詳細資訊，請參閱[物件儲存](#)。

## 設定個別物件存取許可

請完成下列程序來設定儲存貯體中個別物件的存取許可。如需授予使用者能夠在 Lightsail 中管理值區的 IAM 政策範例，請參閱[管理值區的 IAM 政策](#)。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁上，選擇儲存空間索引標籤。
3. 選擇您要設定個別物件存取許可之儲存貯體的名稱。
4. 選擇 Objects (物件) 索引標籤。
5. 在要設定存取許可的物件旁新增核取記號。

物件資訊窗格會顯示物件目前的存取許可。

6. 在物件資訊窗格的 Permissions (許可) 區段中，選擇 Edit (編輯) 以變更物件的存取許可。

**Note**

如果編輯選項無法使用，則儲存貯體存取許可不允許設定個別物件存取許可。若要設定個別物件存取許可，儲存貯體存取許可必須設為 Individual objects can be made public (read-only) (個別物件可設為公有 (唯讀))。如需詳細資訊，請參閱[設定儲存貯體存取許可](#)。

7. 在 Select a permission (選取許可) 下拉式選單中，選擇下列其中一個選項：
  - Private (私有) – 僅限於您或您授予存取權的任何人讀取物件。
  - Public (read-only) (公有 (唯讀)) – 全球所有人皆可讀取物件。
8. 選擇 Save (儲存) 儲存變更。否則，請選擇 Cancel (取消)。

儲存貯體的 Bucket access permission (儲存貯體存取許可) 設定會對個別物件存取許可產生下列影響：

- 若將儲存貯體存取許可變更為 All objects are private (所有物件皆為私有)，即使儲存貯體中所有物件設定為 Public (read-only) (公有 (唯讀)) 個別物件存取許可，它們也都會變為私有。但是，已設定的個別物件存取許可會保留。例如，如果將儲存貯體存取許可變更回 Individual objects can be made public (read-only) (個別物件可設為公有 (唯讀))，則具有公有 (唯讀) 個別存取許可的所有物件會再變為可公開讀取。
- 若將儲存貯體存取許可變更為 All objects are public (read-only) (所有物件皆為公有 (唯讀))，即使儲存貯體中所有物件設定為 Private (私有) 個別物件存取許可，它們也都會變為公有 (唯讀)。

如需有關儲存貯體存取許可的詳細資訊，請參閱[設定儲存貯體存取許可](#)。

## 使用多部分上傳功能將檔案上傳至 Lightsail 儲存貯體

分段上傳可將單個檔案分成幾組分段上傳至儲存貯體。每個組件都是檔案資料的接續部分。您可依任何順序分別上傳這些檔案組件。若任何組件的傳輸失敗，您可再次傳輸該組件，而不會影響其他組件。上傳檔案的所有部分之後，Amazon S3 會組合這些零件，並在 Amazon Lightsail 的儲存貯體中建立物件。一般而言，當物件大小達到 100 MB 時，應考慮使用分段上傳，而不是以單次操作上傳物件。如需有關儲存貯體的詳細資訊，請參閱[物件儲存](#)。

使用分段上傳具備下列優勢：

- 改善傳輸量 - 您可平行上傳各組件以改進傳輸量。

- 快速從任何網路問題復原 - 組件大小若較小，對於重新開始因為網路發生錯誤而上傳失敗的影響可降到最低。
- 隨時間上傳 - 您可以隨時間上傳檔案組件。啟動分段上傳之後，您有 24 小時完成分段上傳。
- 在您知道最終檔案大小前開始上傳 - 您可在建立檔案的同時上傳它。

建議您依照下列方式使用分段上傳：

- 若您透過穩定的高頻寬網路上傳大型檔案，使用分段上傳可同時上傳多個檔案組件以取得多執行緒效能，因而完全善用可用的頻寬使用量。
- 若是透過不穩定的網路進行上傳，使用分段上傳可避免上傳重新開始，因而此更快從網路故障中復原。使用分段上傳時，只有組件中斷才需要重試上傳。不需要重新開始或再次上傳整個檔案。

## 內容

- [分段上傳程序](#)
- [並行分段上傳操作](#)
- [分段上傳保留](#)
- [Amazon Simple Storage Service 分段上傳限制](#)
- [分割要上傳的檔案](#)
- [使用啟動多部分上傳 AWS CLI](#)
- [使用上載零件 AWS CLI](#)
- [列出多部分上傳的部分使用 AWS CLI](#)
- [建立分段上傳 .json 檔案](#)
- [使用完成多部分上傳 AWS CLI](#)
- [列出值區的多部分上傳內容，使用 AWS CLI](#)
- [使用 AWS CLI 停止分段上傳](#)

## 分段上傳程序

分段上傳是一個三個步驟的程序，使用 Amazon S3 動作將檔案上傳到 Lightsail 中的儲存貯體：

1. 您可以使用動作啟[CreateMultipartUpload](#)動分段上傳。
2. 您可以使用[UploadPart](#)動作上載檔案部分。

### 3. 您可以使用 [CompleteMultipartUpload](#) 動作完成分段上傳。

#### Note

您可以在啟動多部分上傳之後，使用 [AbortMultipartUpload](#) 動作來停止它。

當分段上傳請求完成時，Amazon Simple Storage Service 會從上傳的分段中建構物件。然後，您可以使用與存取儲存貯體中任何其他物件相同的方式來存取物件。

您可以列出所有進行中的分段上傳，或是取得特定分段上傳之已上傳組件的清單。本節會一一說明這些操作。

#### 啟動分段上傳

當您傳送請求以啟動分段上傳時，Amazon Simple Storage Service 會傳回具有上傳 ID 的回應。這是分段上傳的唯一識別符。每次上傳各組件、列出各組件、完成上傳或停止上傳時，都必須納入上傳 ID。若您希望提供任何中繼資料，說明正在上傳中的物件，您必須在分段上傳啟動請求中指定中繼資料。

#### 組件上傳

上傳某個分段組件時，除了上傳 ID 之外，還必須指定組件編號。您可選擇 1 到 10,000 之間的任何組件編號。組件編號可找出獨特的某個組件，以及其在上傳中物件內的位置。您選擇的組件編號無須為連續的號碼 (例如，其可為 1、5 和 14)。若使用和前一個上傳組件相同的組件編號上傳新的組件，將會覆寫前一個已上傳的組件。

每當您上傳零件時，Amazon 簡易儲存服務都會在其回應中傳回 ETag 標頭。對於每個零件上載，您必須記錄零件編號和 ETag 值。後續的要求中必須包含這些值，才能完成分段上傳。

#### Note

分段上傳的所有已上傳組件都存放在儲存貯體上。它們會消耗儲存貯體的儲存空間，直到您完成上傳、停止上傳或上傳逾時為止。如需詳細資訊，請參閱本指南稍後的 [分段上傳保留](#)。

#### 完成分段上傳

當您完成分段上傳時，Amazon Simple Storage Service 會根據分段編號以遞增順序串連各個分段，從而建立物件。分段上傳啟動請求中若已提供任何物件中繼資料，Amazon Simple Storage Service 便會將該中繼資料與物件建立關聯。成功完成請求之後，這些組件就不再存在。

您的完整分段上傳請求必須包含上傳 ID 以及零件編號和對應ETag值的清單。Amazon 簡易儲存服務回應包含可唯ETag一識別合併物件資料的回應。這不一定ETag是對象數據的MD5哈希值。

您也可以選擇性停止分段上傳。停止分段上傳之後，即無法再次使用該上傳 ID 上傳任何組件。之後，取消的分段上傳中的任何部分會釋出所有儲存空間。如有任何分段上傳正在進行，則會在您中止後成功或失敗。若要釋出所有組件所使用之全部的儲存體，您必須在所有上傳組件都已完成後，再停止分段上傳。

### 分段上傳清單

您可列出特定分段上傳的組件或所有進行之分段上傳。列出組件操作會傳回特定分段上傳之已上傳組件的資訊。Amazon Simple Storage Service 會為每項列出的分段請求，傳回指定分段上傳的各分段資訊，上限為 1,000 個分段。若分段組件上傳中有超過 1,000 個組件，您必須傳送一連串的列出組件要求，才可擷取所有組件。請注意，傳回的組件清單不包含仍在上傳程序中的組件。使用列出分段上傳操作，即可取得進行之分段上傳清單。

進行之分段上傳是您已啟動但尚未完成或已停止的上傳。每個要求最多可傳回 1,000 個分段上傳。若正在進行超過 1,000 個的分段上傳，您必須另行傳送請求以擷取剩餘的分段上傳。僅使用傳回的清單進行驗證。在傳送完成的分段上傳請求時，請勿使用此清單的結果。請改為維護您自己的清單，列出您在上傳零件時指定的零件編號，以及 Amazon 簡單儲存服務傳回的對應ETag值。

## 並行分段上傳操作

在分散式開發環境中，您的應用程式有可能同時對相同的物件啟動數項更新。您的應用程式可能使用相同的物件金鑰，啟動數項分段上傳。對於每一個上傳，應用程式會上傳各分段，並對 Amazon Simple Storage Service 傳送完整的上傳請求，以建立物件。當儲存貯體啟用版本控制之後，完成分段上傳一律會建立新的版本。對於未啟用版本控制的儲存貯體，可能優先考慮其他請求，例如在分段上傳啟動後與分段上傳完成前收到的請求。

### Note

可能優先考慮其他請求，例如在分段上傳啟動後與分段上傳完成前收到的請求。例如，在您透過金鑰啟動分段上傳後，以及分段上傳完成前，另一個操作可能會刪除該金鑰。若發生此情形，完成的分段上傳回應可能顯示物件建立成功，就算您沒有見到該物件也一樣。

## 分段上傳保留

分段上傳的所有已上傳組件都存放在儲存貯體上。它們會消耗儲存貯體的儲存空間，直到您完成上傳、停止上傳或上傳逾時為止。分段上傳逾時且會在建立後的 24 小時後刪除分段上傳。當您停止分段上傳或其逾時時，所有上傳的組件都會被刪除，並釋出儲存貯體上消耗的儲存空間。

## Amazon Simple Storage Service 分段上傳限制

下表提供分段上傳核心規格。

- 物件大小上限：5 TB
- 每次上傳的組件數目上限：10,000
- 組件編號：1 到 10,000 (含)
- 組件大小：5 MB (最小值) - 5 GB (最大值)。您的多段上傳的最後一部分沒有大小限制。
- 列出組件請求的傳回組件數目上限：1,000
- 列出分段上傳請求中傳回的分段上傳數目上限：1,000

## 分割要上傳的檔案

使用 Linux 或 Unix 作業系統中的 `split` 命令，以將檔案分割成多個組件，然後上傳至儲存貯體。您可以在 Windows 作業系統中使用類似的免費軟體應用程式來分割檔案。將檔案分割成多個組件後，請繼續前往本指南的[啟動分段上傳](#)一節。

## 使用 AWS CLI 啟動分段上傳

完成下列程序以使用 AWS Command Line Interface (AWS CLI) 啟動分段上傳。您可以使用 `create-multipart-upload` 命令來執行此動作。若要取得更多資訊，請參閱《指AWS CLI 令參考》[create-multipart-upload](#)中的。

### Note

您必須先為 Lightsail AWS CLI 和 Amazon S3 安裝並進行設定，然後才能繼續執行此程序。如需詳細資訊，請參閱[設定 AWS CLI 定使用 Lightsail](#)。

1. 開啟命令提示或終端機視窗。
2. 輸入下列命令，以建立儲存貯體的分段上傳。

```
aws s3api create-multipart-upload --bucket BucketName --key ObjectKey --acl bucket-owner-full-control
```

將命令中的以下範例文字取代為自訂文字：

- *BucketName*-您要為其建立多部分上傳的值區名稱。
- *ObjectKey*-用於您要上傳的檔案的物件金鑰。

範例：

```
aws s3api create-multipart-upload --bucket amzn-s3-demo-bucket --key sailbot.mp4 --acl bucket-owner-full-control
```

您應該會看到類似以下範例的結果。回應包括 UploadID，您必須在後續命令中指定該 ID，以上傳組件並完成此物件的分段上傳。

```
C:\>aws s3api create-multipart-upload --bucket DOC-EXAMPLE-BUCKET --key sailbot.mp4
{
  "AbortDate": "2021-05-20T00:00:00+00:00",
  "AbortRuleId": "ExpireMultiPart",
  "ServerSideEncryption": "AES256",
  "Bucket": "DOC-EXAMPLE-BUCKET",
  "Key": "sailbot.mp4",
  "UploadId": "R4QU.m0.exampleiHWiLOeNw7JtXX70otRhTLsXXCzF21CzdYlfj51fjtiMnpzVw2WPj.exampleBTmL_N_.42.D1HYOTsITFsX.t03XOUTTAHicxY5VR8jWRGdkVkuG"
}
```

獲得分段上傳的 UploadID 之後，請繼續本指南的[使用 AWS CLI 上傳分段](#)章節，並開始上傳各分段。

## 使用上載零件 AWS CLI

完成下列程序以使用 AWS Command Line Interface (AWS CLI) 上傳分段上傳的某分段。您可以使用 `upload-part` 命令來執行此動作。如需詳細資訊，請參閱《AWS CLI 命令參考》中的 [upload-part](#)。

### Note

您必須先為 Lightsail AWS CLI 和 Amazon S3 安裝並進行設定，然後才能繼續執行此程序。如需詳細資訊，請參閱[設 AWS CLI 定使用 Lightsail](#)。

1. 開啟命令提示或終端機視窗。

## 2. 輸入下列命令，以將組件上傳至儲存貯體。

```
aws s3api upload-part --bucket BucketName --key ObjectKey --part-number Number --
body FilePart --upload-id "UploadID" --acl bucket-owner-full-control
```

將命令中的以下範例文字取代為自訂文字：

- *BucketName*-您要為其建立多部分上傳的值區名稱。
- *ObjectKey*-用於您要上傳的檔案的物件金鑰。
- *Number* -您要上傳的零件的零件編號。組件編號可找出獨特的某個組件，以及其在上傳中物件內的位置。務必隨您上傳的每個組件逐步增加 `--part-number` 參數。若要這樣做，請在完成分段上傳時，按照 Amazon Simple Storage Service 組裝物件的順序對它們進行編號。
- *FilePart* -要從您的計算機上傳的零件文件。
- *UploadID* -您先前在本指南中建立的多部分上傳的上傳 ID。

範例：

```
aws s3api upload-part --bucket amzn-s3-demo-bucket --
key sailbot.mp4 --part-number 1 --body sailbot.mp4.001 --upload-id
"R4QU.m0.exampleiHWiLOeNw7JtXX70otRhTLsXXCzF21CZdYlfj51fjtiMnpzVw2WPj.exampleBTmL_N_.42.D1
--acl bucket-owner-full-control
```

您應該會看到類似以下範例的結果。為您上傳的每個組件重複 `upload-part` 命令。每個上傳組件請求的回應包含您所上傳組件的 ETag 值。為您上傳的每個組件記錄 ETag 值。您需要所有 ETag 值以完成分段上傳，本指南稍後會加以說明。

```
C:\>aws s3api upload-part --bucket DOC-EXAMPLE-BUCKET --key sailbot.mp4 --part-number 1 --body sailbot.mp4.001
--upload-id "R4QU.m0.exampleiHWiLOeNw7JtXX70otRhTLsXXCzF21CZdYlfj51fjtiMnpzVw2WPj.exampleBTmL_N_.42.D1HYOTsITFsX.t03XOUTTAHicxY5VR8jwRgdkvKUG"
{
  "ServerSideEncryption": "AES256",
  "ETag": "\"4example7530246113e837a860a38bbb\""
}
```

## 列出多部分上傳的部分使用 AWS CLI

完成下列程序以使用 AWS Command Line Interface (AWS CLI) 列出分段上傳的各部分。您可以使用 `list-parts` 命令來執行此動作。如需詳細資訊，請參閱《AWS CLI 命令參考》中的 [list-parts](#)。

完成此程序以取得在分段上傳中所有已上傳組件的 ETag 值。您需要這些值以完成本指南稍後的分段上傳。不過，如果您從組件上傳的回應記錄所有 ETag 值，則您可以跳過此程序並繼續前往本指南的[建立分段上傳 .json 檔案](#)一節。

### Note

您必須先為 Lightsail AWS CLI 和 Amazon S3 安裝並進行設定，然後才能繼續執行此程序。如需詳細資訊，請參閱[設定 AWS CLI 定使用 Lightsail](#)。

1. 開啟命令提示或終端機視窗。
2. 輸入以下命令以列出儲存貯體上分段上傳的組件。

```
aws s3api list-parts --bucket BucketName --key ObjectKey --upload-id "UploadID"
```

將命令中的以下範例文字取代為自訂文字：

- *BucketName*-您要列出多部分上傳部分的值區名稱。
- *ObjectKey*-多部分上傳的物件索引鍵。
- *UploadID*-您先前在本指南中建立的多部分上傳的上傳 ID。

範例：

```
aws s3api list-parts --bucket amzn-s3-demo-bucket --key sailbot.mp4 --upload-id  
"R4QU.m0.exampleiHWiL0eNw7JtXX70otRhTLsXXCzF21CZdYlfj5lfjtiMnpzVw2WPj.exampleBTmL_N_.42.DL"
```

您應該會看到類似以下範例的結果。回應會列出所有組件編號和在分段上傳中上傳的組件 ETag 值。將這些值複製到剪貼簿，然後繼續前往本指南的[建立分段上傳 .json](#) 一節。

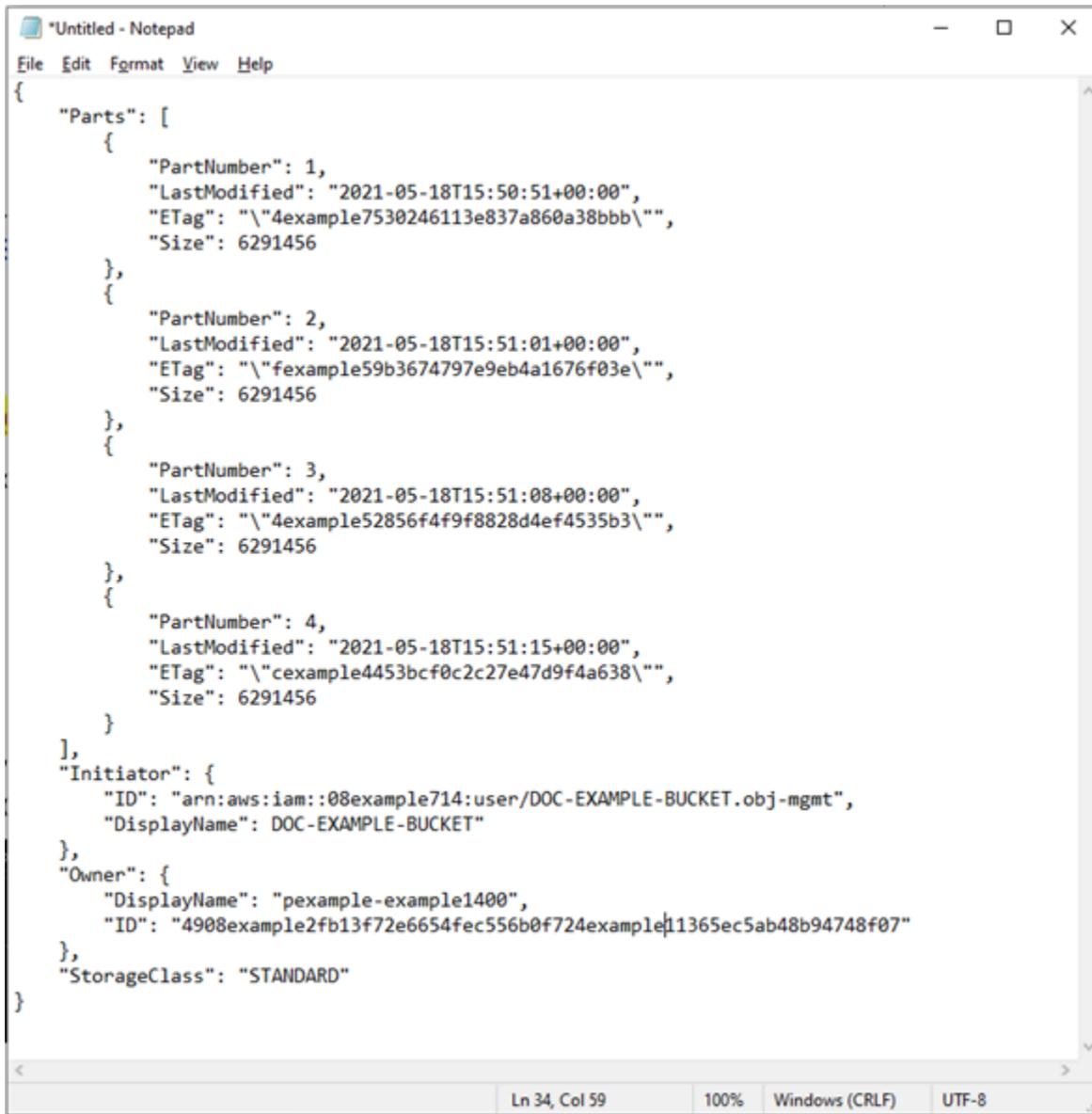
```
C:\>aws s3api list-parts --bucket DOC-EXAMPLE-BUCKET --key sailbot.mp4 --upload-id "R4QU.m0.exampleiHWiLOeNw7JtXX7OotR
hTLsXXCzF21CZdY1fj51fjtiMnpzVw2WPj.exampleBTmL_N_.42.D1HYOTsITFsX.t03XOUTTAHiCxY5VR8jWRGdkVkuG"
{
  "Parts": [
    {
      "PartNumber": 1,
      "LastModified": "2021-05-18T15:50:51+00:00",
      "ETag": "\"4example7530246113e837a860a38bbb\"",
      "Size": 6291456
    },
    {
      "PartNumber": 2,
      "LastModified": "2021-05-18T15:51:01+00:00",
      "ETag": "\"fexample59b3674797e9eb4a1676f03e\"",
      "Size": 6291456
    },
    {
      "PartNumber": 3,
      "LastModified": "2021-05-18T15:51:08+00:00",
      "ETag": "\"4example52856f4f9f8828d4ef4535b3\"",
      "Size": 6291456
    },
    {
      "PartNumber": 4,
      "LastModified": "2021-05-18T15:51:15+00:00",
      "ETag": "\"cexample4453bcf0c2c27e47d9f4a638\"",
      "Size": 6291456
    }
  ],
  "Initiator": {
    "ID": "arn:aws:iam:08example714:user/DOC-EXAMPLE-BUCKET.obj-mgmt",
    "DisplayName": "DOC-EXAMPLE-BUCKET"
  },
  "Owner": {
    "DisplayName": "pexample-example1400",
    "ID": "4908example2fb13f72e6654fec556b0f724example11365ec5ab48b94748f07"
  },
  "StorageClass": "STANDARD"
}
```

## 建立分段上傳 .json 檔案

完成下列程序以建立分段上傳 .json 檔案，該檔案定義您上傳的所有組件及其 ETag 值。本指南中稍後需要此動作才能完成分段上傳。

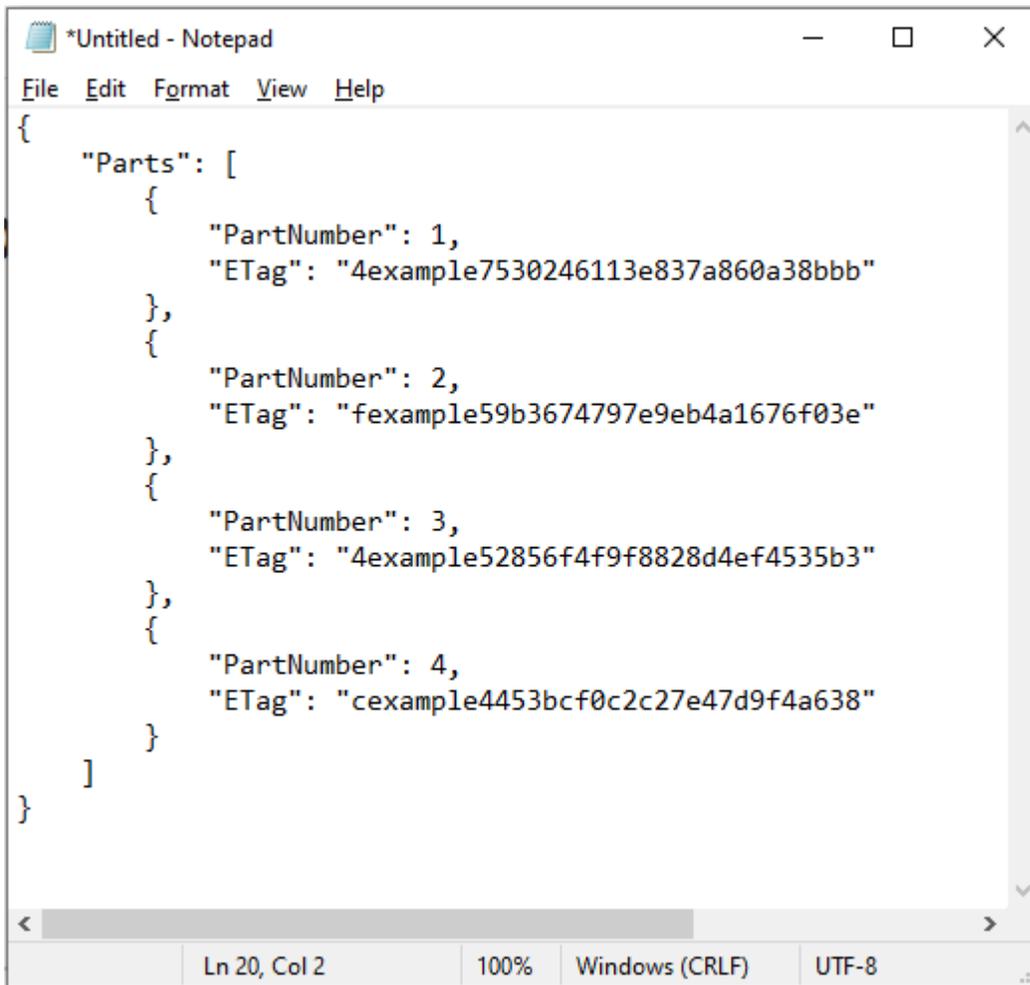
1. 開啟文字編輯器，並貼上來自您在本指南之前章節中請求的 `list-parts` 命令的回應。

結果應如下列範例所示。



```
{
  "Parts": [
    {
      "PartNumber": 1,
      "LastModified": "2021-05-18T15:50:51+00:00",
      "ETag": "\"4example7530246113e837a860a38bbb\"",
      "Size": 6291456
    },
    {
      "PartNumber": 2,
      "LastModified": "2021-05-18T15:51:01+00:00",
      "ETag": "\"fexample59b3674797e9eb4a1676f03e\"",
      "Size": 6291456
    },
    {
      "PartNumber": 3,
      "LastModified": "2021-05-18T15:51:08+00:00",
      "ETag": "\"4example52856f4f9f8828d4ef4535b3\"",
      "Size": 6291456
    },
    {
      "PartNumber": 4,
      "LastModified": "2021-05-18T15:51:15+00:00",
      "ETag": "\"cexample4453bcf0c2c27e47d9f4a638\"",
      "Size": 6291456
    }
  ],
  "Initiator": {
    "ID": "arn:aws:iam::08example714:user/DOC-EXAMPLE-BUCKET.obj-mgmt",
    "DisplayName": "DOC-EXAMPLE-BUCKET"
  },
  "Owner": {
    "DisplayName": "pexample-example1400",
    "ID": "4908example2fb13f72e6654fec556b0f724example11365ec5ab48b94748f07"
  },
  "StorageClass": "STANDARD"
}
```

2. 重新格式化文字檔案，如下列範例所示：



```
{
  "Parts": [
    {
      "PartNumber": 1,
      "ETag": "4example7530246113e837a860a38bbb"
    },
    {
      "PartNumber": 2,
      "ETag": "fexample59b3674797e9eb4a1676f03e"
    },
    {
      "PartNumber": 3,
      "ETag": "4example52856f4f9f8828d4ef4535b3"
    },
    {
      "PartNumber": 4,
      "ETag": "cexample4453bcf0c2c27e47d9f4a638"
    }
  ]
}
```

3. 將文字檔儲存至您的電腦 `mpstructure.json`，然後 [使用本指南的 AWS CLI 章節繼續執行「完成多部分上傳」](#)。

## 使用完成多部分上傳 AWS CLI

完成下列程序以使用 AWS Command Line Interface (AWS CLI) 完成分段上傳。您可以使用 `complete-multipart-upload` 命令來執行此動作。若要取得更多資訊，請參閱《指 AWS CLI 命令參考》[complete-multipart-upload](#) 中的。

### Note

您必須先為 Lightsail AWS CLI 和 Amazon S3 安裝並進行設定，然後才能繼續執行此程序。如需詳細資訊，請參閱 [設定 AWS CLI 定使用 Lightsail](#)。

1. 開啟命令提示或終端機視窗。

## 2. 輸入下列命令，以將組件上傳至儲存貯體。

```
aws s3api complete-multipart-upload --multipart-upload file://JSONFileName --
bucket BucketName --key ObjectKey --upload-id "UploadID" --acl bucket-owner-full-
control
```

將命令中的以下範例文字取代為自訂文字：

- *JSONFileName*-您先前在本指南中建立的 .json 檔案名稱 (例如 mpstructure.json)。
- *BucketName*-您要完成多部分上傳的值區名稱。
- *ObjectKey*-多部分上傳的物件索引鍵。
- *UploadID*-您先前在本指南中建立的多部分上傳的上傳 ID。

Example:

```
aws s3api complete-multipart-upload --multipart-upload file://mpstructure.json
--bucket amzn-s3-demo-bucket --key sailbot.mp4 --upload-id
"R4QU.m0.exampleiHWiL0eNw7JtXX70otRhTLsXXCzF21CZdYlfj5lfjtiMnpzVw2WPj.exampleBTmL_N_.42.D1HYOTsITfsX.t03XOUTTAHicxY5VR8jWRGdkVkuG"
--acl bucket-owner-full-control
```

您應該會看到類似於以下範例的回應。這可確認分段上傳已完成。物件現在已組裝並可在儲存貯體中使用。

```
C:\>aws s3api complete-multipart-upload --multipart-upload file://mpstructure.json --bucket DOC-EXAMPLE-BUCKET --key sailbot.mp4
--upload-id "R4QU.m0.exampleiHWiL0eNw7JtXX70otRhTLsXXCzF21CZdYlfj5lfjtiMnpzVw2WPj.exampleBTmL_N_.42.D1HYOTsITfsX.t03XOUTTAHicxY5VR8jWRGdkVkuG"
{
  "ServerSideEncryption": "AES256",
  "VersionId": "MexampleKmdfPQb.2YZHqOvE.T.vSDtY",
  "Location": "https://DOC-EXAMPLE-BUCKET.s3.us-west-2.amazonaws.com/sailbot.mp4",
  "Bucket": "DOC-EXAMPLE-BUCKET",
  "Key": "sailbot.mp4",
  "ETag": "\"1example5964e3115e5d3f3c9a731585-4\""
}
```

## 列出值區的多部分上傳內容，使用 AWS CLI

完成下列程序以使用 AWS Command Line Interface (AWS CLI) 列出所有分段上傳。您可以使用 `list-multipart-uploads` 命令來執行此動作。若要取得更多資訊，請參閱《指AWS CLI 令參考》[list-multipart-uploads](#)中的。

**Note**

您必須先為 Lightsail AWS CLI 和 Amazon S3 安裝並進行設定，然後才能繼續執行此程序。如需詳細資訊，請參閱[設定 AWS CLI 定使用 Lightsail](#)。

1. 開啟命令提示或終端機視窗。
2. 輸入下列命令，以將組件上傳至儲存貯體。

```
aws s3api list-multipart-uploads --bucket BucketName
```

在命令中，替換 *BucketName* 使用您要列出所有多部分上傳的儲存桶的名稱。

範例：

```
aws s3api list-multipart-uploads --bucket amzn-s3-demo-bucket
```

您應該會看到類似於以下範例的回應。

```
C:\>aws s3api list-multipart-uploads --bucket DOC-EXAMPLE-BUCKET
{
  "Uploads": [
    {
      "UploadId": "R4QU.m0.exampleiHwiL0eNw7JtXX70otRhTLsXXCzF21CZdYlfj51fjtiMnpzVw2WPj.exampleBTmL_N_.42.D1HYOTsITFsX.t03XOUTTAHicxY5VR8jwRGdkVkuG",
      "Key": "sailbot.mp4",
      "Initiated": "2021-05-18T15:49:11+00:00",
      "StorageClass": "STANDARD",
      "Owner": {
        "DisplayName": "pexample-example1400",
        "ID": "4908example2fb13f72e6654fec556b0f724example11365ec5ab48b94748f07"
      },
      "Initiator": {
        "ID": "arn:aws:iam::08example714:user/DOC-EXAMPLE-BUCKET.obj-mgmt",
        "DisplayName": "DOC-EXAMPLE-BUCKET"
      }
    }
  ]
}
```

## 使用停止多部分上傳 AWS CLI

請完成下列程序，以使用 AWS Command Line Interface (AWS CLI) 停止分段上傳。如果您已啟動分段上傳，但不想再繼續上傳，請執行此操作。您可以使用 `abort-multipart-upload` 命令來執行此動作。若要取得更多資訊，請參閱《指AWS CLI 令參考》[abort-multipart-upload](#)中的。

**Note**

您必須先為 Lightsail AWS CLI 和 Amazon S3 安裝並進行設定，然後才能繼續執行此程序。如需詳細資訊，請參閱[設定 AWS CLI 定使用 Lightsail](#)。

1. 開啟命令提示或終端機視窗。
2. 輸入下列命令，以將組件上傳至儲存貯體。

```
aws s3api abort-multipart-upload --bucket BucketName --key ObjectKey --upload-id  
"UploadID" --acl bucket-owner-full-control
```

將命令中的以下範例文字取代為自訂文字：

- *BucketName*-您要停止多部分上傳的值區名稱。
- *ObjectKey*-多部分上傳的物件索引鍵。
- *UploadID* -您要停止的多部分上傳的上傳 ID。

範例：

```
aws s3api abort-multipart-upload --bucket amzn-s3-demo-bucket --key sailbot.mp4 --  
upload-id  
"R4QU.m0.exampleiHWiL0eNw7JtXX70otRhTLsXXCzF21CZdYlfj5lfjtiMnpzVw2WPj.exampleBTmL_N_.42.DL  
--acl bucket-owner-full-control
```

此命令不會傳回回應。您可以執行 `list-multipart-uploads` 命令以確認分段上傳已停止。

## 遵循 Lightsail 物件儲存體的值區命名需求

在 Amazon Lightsail 物件儲存體服務中建立值區時，必須為其命名。值區的名稱是您的客戶在存取儲存在值區中的物件時將使用的名稱的一部分。URL 例如，如果您 `DOC-EXAMPLE-BUCKET` 在中命名值區 `us-east-1` AWS 區域，則值區 URL 的名稱為 `DOC-EXAMPLE-BUCKET.s3.us-east-1.amazonaws.com`。在您建立儲存貯體後，即無法變更其名稱。請記住，客戶可以看到您指定的儲存貯體名稱。如需 Lightsail 物件儲存服務的詳細資訊，請參閱[物件儲存體](#)。如需有關建立儲存貯體的詳細資訊，請參閱[建立儲存貯體](#)。

值區名稱必須 DNS 符合-規範。因此，下列規則適用於 Lightsail 中的命名值區：

- 儲存貯體名稱長度必須介於 3 到 56 個字元之間。
- 儲存貯體名稱只能由小寫字母、數字和連字號 (-) 組成。
- 儲存貯體名稱的開頭和結尾必須為字母或數字。
- 連字號 (-) 可以用於分隔單字，但不可連續指定。例如，允許 doc-example-bucket，但不允許 doc--example--bucket。
- 儲存貯體名稱在 aws (標準區域) 分區中必須唯一，包括 Amazon Simple Storage Service (Amazon S3) 中的儲存貯體。

## 儲存貯體名稱的範例

下列範例儲存貯體名稱有效，並遵循建議的命名指導方針：

- docexamplebucket1
- log-delivery-march-2020
- my-hosted-content

不允許下列範例儲存貯體名稱：

- doc.example.bucket
- doc--example--bucket
- doc-example-bucket-

## Lightsail 物件儲存值區的主要名稱

您上傳到儲存貯體的檔案會以物件形式存放在 Amazon Lightsail 物件儲存服務中。物件索引鍵 (或索引鍵名稱) 可唯一識別存放於儲存貯體中的物件。本指南說明組成透過 Lightsail 主控台檢視之值區之資料夾結構的金鑰名稱和金鑰名稱前置詞的概念。如需有關儲存貯體的詳細資訊，請參閱[物件儲存](#)。

## 鍵值名稱

Lightsail 物件儲存服務資料模型使用扁平結構，而不是階層式結構，就像您在檔案系統中看到的那樣。沒有分階層的資料夾和子資料夾。但您可以使用索引鍵名稱字首以及分隔符號來推斷邏輯階層。Lightsail 主控台會使用索引鍵名稱前置字元，以資料夾結構顯示物件。

假設您的儲存貯體具有四個物件，其物件索引鍵如下：

- Development/Projects.xls
- Finance/statement1.pdf
- Private/taxdocument.pdf
- to-dos.doc

Lightsail 主控台會使用金鑰名稱前置字元 (Development/Finance/、和Private/) 和分隔符號 (/) 來呈現資料夾結構。to-dos.doc 索引鍵名稱沒有字首，因此其物件會直接在儲存貯體的根層級顯示。如果您在 Lightsail 主控台中瀏覽至該Development/資料夾，就會看到該Projects.xls物件。在 Finance/ 資料夾中，您會看到 statement1.pdf 物件，而在 Private/ 資料夾中，則會看到 taxdocument.pdf 物件。

Lightsail 主控台可建立資料夾，方法是以金鑰名稱前置字元和分隔符號值做為金鑰名稱來建立零位元組物件。這些資料夾物件不會出現在主控台中。但是，這些物件的行為就如同任何其他物件。您可以使用 Amazon S3 API、AWS Command Line Interface (AWS CLI) 或來檢視和操作它們 AWS SDKs。

## 物件索引鍵命名準則

您可以在物件索引鍵名稱中使用任何 UTF -8 個字元。但是，在索引鍵名稱中使用特定字元可能對某些應用程式和通訊協定造成問題。下列準則可協助您最大程度地遵DNS循 Web 安全字元、XML 剖析器和其他項目。APIs

### 安全字元

下列字元集通常可安心用於索引鍵名稱中。

- 英數字元
  - 0-9
  - a-z
  - A-Z
- 特殊字元
  - 正斜線 (/)
  - 驚嘆號 (!)
  - 連字號 (-)
  - 底線 (\_)
  - 句號 (.)

- 星號 (\*)
- 單引號 (')
- 左括號 ((
- 右括號 ())

有效的物件索引鍵名稱範例如下：

- 4my-organization
- my.great\_photos-2014/jan/myvacation.jpg
- videos/2014/birthday/video1.wmv

#### Important

如果物件索引鍵名稱以單一句點 (.) 或兩個句點 (..) 結尾，您就無法使用 Lightsail 主控台下載物件。若要下載金鑰名稱以一或兩個期間結尾的物件，您必須使用 Amazon S3 API、AWS CLI、和 AWS SDKs。如需詳細資訊，請參閱[下載儲存貯體物件](#)。

## 可能需要特殊處理的字元

金鑰名稱中的下列字元可能需要額外的程式碼處理，而且可能需要URL編碼或參照為HEX。其中一部分是您的瀏覽器可能無法處理的不可列印字元，這些字元也需要特殊處理：

- & 符號 ("&")
- 貨幣符號 ("\$")
- ASCII字元範圍介於 00—1 樓的十六進位 (0 至 31 個十進位數) 和 7F (十進位 127 位數)
- @ 符號 ("@")
- 等號 ("=")
- 分號 (";")
- 冒號 (":")
- 加號 ("+")
- 空格 - 在某些情況下，可能會遺失大量連續空格 (特別是多個空格)
- 逗號 (",")
- 問號 ("?")

## 需要避免的字元

請避免在索引鍵名稱中使用下列字元，因為這些字元需要經過大量的特殊處理，才能在所有應用程式之間達到一致。

- 反斜線 ("\\")
- 左大括弧 ("{"
- 不可列印的ASCII字元 (128 至 255 個十進位字元)
- 插入號 ("^")
- 右大括弧 ("}")
- 百分比字元 ("%")
- 重音符號/反引號 ("`")
- 右方括號 ("]")
- 問號
- 「大於」符號 (">")
- 左方括號 ("["
- 波狀符號 ("~")
- 「小於」符號 ("<")
- 井字號 ("#")
- 垂直分隔號/縱線字元 ("|")

## XML相關物件索引鍵約束

正如 [end-of-line 處理標XML準所指定的](#) 那樣，所有XML文本都被標準化，以便單個回車符 ( 字ASCII碼 13 ) 和回車緊跟一個換行符 ( ASCII代碼 10 ) 被單行換行字符替換。為了確保XML要求中物件索引鍵的正確剖析，在XML標籤中插入歸位字元和其他特殊字元時，必須以對等的XML實體程式碼取代它們。以下是此類特殊字元及其對等實體程式碼的清單：

- ' 作為 &apos;
- " 作為 &quot;
- & 作為 &amp;
- < 作為 &lt;
- > 作為 &gt;

- \r 作為 `&#13;` 或 `&#x0D;`;
- \n 作為 `&#10;` 或 `&#x0A;`;

下列範例說明如何使用XML實體程式碼做為歸位字元的取代。此 DeleteObjects 請求刪除具有 /some/prefix/objectwith\r\n 索引鍵參數的物件：(其中 \r 是歸位字元)。

```
<Delete xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Object>
    <Key>/some/prefix/objectwith\r\n</Key>
  </Object>
</Delete>
```

## 安全 Lightsail 物件儲存貯體

Amazon Lightsail 物件儲存提供許多安全功能，可在您開發和實作自己的安全政策時考慮。以下最佳實務為一般準則，並不代表完整的安全解決方案。這些最佳實務可能不適用或無法滿足您的環境需求，因此請將其視為實用建議就好，而不要當作是指示。

### 內容

- [預防性安全最佳實務](#)
  - [實作最低權限存取](#)
  - [確認您的 Lightsail 值區無法公開存取](#)
  - [在 Amazon S3 中啟用封鎖公有存取](#)
  - [將執行個體連接至儲存貯體以授予完整的程式設計存取權](#)
  - [使用跨帳戶存取權授予其他 AWS 帳戶存取值區中物件的權限](#)
  - [資料加密](#)
  - [啟用版本控制](#)
- [監控和稽核最佳實務](#)
  - [啟用存取記錄並定期執行安全和存取稽核](#)
  - [識別、標記及稽核儲存貯體](#)
  - [使用監視工具實作 AWS 監控](#)
  - [使用 AWS CloudTrail](#)
  - [監控 AWS 安全建議](#)

## 預防性安全最佳實務

下列最佳做法可協助防止 Lightsail 值區發生安全性事件。

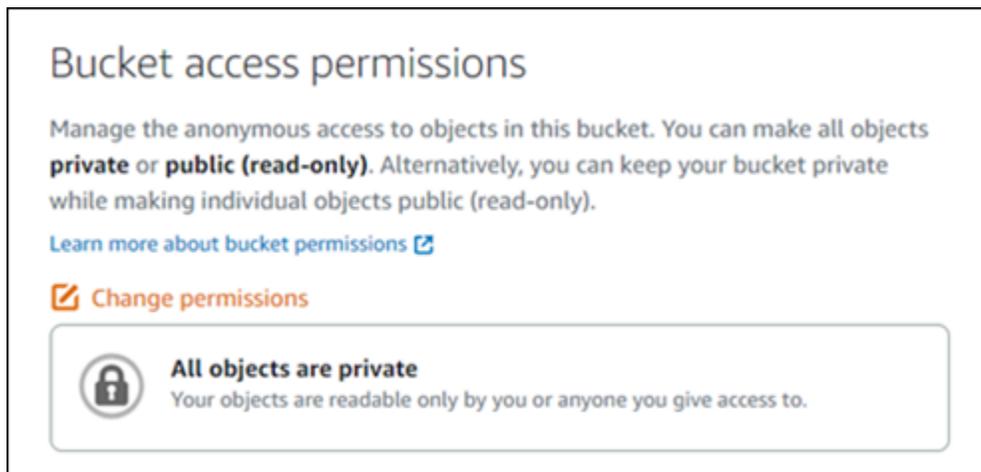
### 實作最低權限存取

授與權限時，您可以決定誰取得哪些 Lightsail 資源的權限。您還需針對這些資源啟用允許執行的動作，因此，您只應授予執行任務所需的許可。對降低錯誤或惡意意圖所引起的安全風險和影響而言，實作最低權限存取是相當重要的一環。

如需有關建立 IAM 政策以管理儲存貯體的詳細資訊，請參閱[用於管理儲存貯體的 IAM 政策](#)。如需 Lightsail 儲存貯體支援的 Amazon S3 動作的詳細資訊，請參閱 Amazon Lightsail API 參考資料中的[物件儲存動作](#)。

### 確認您的 Lightsail 值區無法公開存取

根據預設，儲存貯體與物件皆為私有。將儲存貯體存取許可設為 All objects are private (所有物件皆為私有)，使您的儲存貯體保持私有。對於大多數使用案例，您不需要將儲存貯體或個別物件設為公開。如需詳細資訊，請參閱[設定儲存貯體中個別物件的存取許可](#)。



但是，如果您是使用儲存貯體來託管網站或應用程式的媒體，在某些情況下，您可能需要將儲存貯體或個別物件設為公開。您可以設定下列其中一個選項，使儲存貯體或個別物件設為公開：

- 如果儲存貯體中只有某些物件需要對網際網路上的任何人員公開 (唯讀)，則將儲存貯體存取許可變更為 Individual objects can be made public and read-only (個別物件可設為公開和唯讀)，並且只將需要公開的物件變更為 Public (read-only) (公開 (唯讀))。此選項可讓儲存貯體保持私有，但可讓您選擇將個別物件設為公開。如果個別物件包含您不希望公開存取的敏感或機密資訊，則請勿將其設為公開。如果您將個別物件設為公開，您應該定期驗證每個個別物件的公開可存取性。

## Bucket access permissions

Manage the anonymous access to objects in this bucket. You can make all objects **private** or **public (read-only)**. Alternatively, you can keep your bucket private while making individual objects public (read-only).

[Learn more about bucket permissions](#)

 **Change permissions**



**Individual objects can be made public and read-only**  
Your objects are readable only by you or anyone you give access to. But you can make individual objects readable by anyone in the world. Objects are private by default.

 You can change individual object access permissions in the Objects tab.

- 如果儲存貯體中的所有物件都需要對網際網路上的任何人員公開 (唯讀)，則將儲存貯體存取許可變更為 All objects are public and read-only (所有物件皆為公開和唯讀)。如果儲存貯體中的任何物件包含敏感或機密資訊，請勿使用此選項。

## Bucket access permissions

Manage the anonymous access to objects in this bucket. You can make all objects **private** or **public (read-only)**. Alternatively, you can keep your bucket private while making individual objects public (read-only).

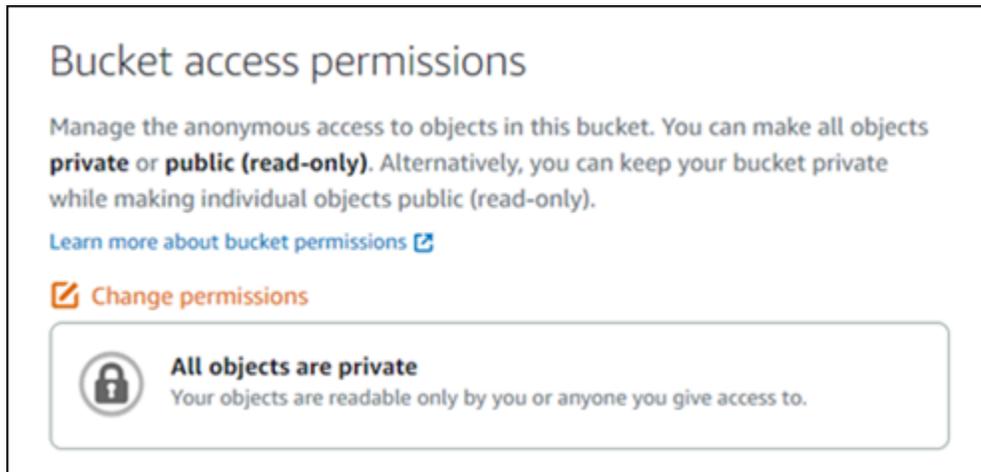
[Learn more about bucket permissions](#)

 **Change permissions**



**All objects are public and read-only**  
Your objects are public (read-only) to anyone in the world.

- 如果您先前將儲存貯體變更為公開，或將個別物件變更為公開，則可將儲存貯體存取許可變更為 All objects are private (所有物件皆為私有)，快速將儲存貯體及其所有物件變更為私有。



### Bucket access permissions

Manage the anonymous access to objects in this bucket. You can make all objects **private** or **public (read-only)**. Alternatively, you can keep your bucket private while making individual objects public (read-only).

[Learn more about bucket permissions](#)

[Change permissions](#)

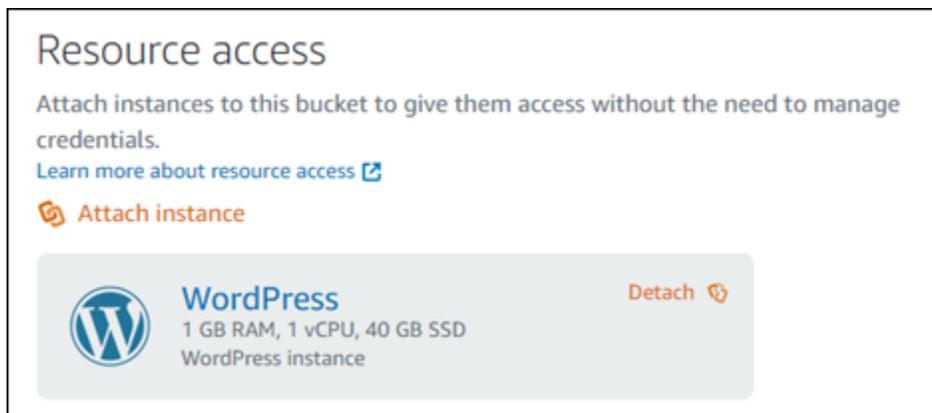
 **All objects are private**  
Your objects are readable only by you or anyone you give access to.

## 在 Amazon S3 中啟用封鎖公有存取

Lightsail 物件儲存資源在允許或拒絕公開存取時，會將 Lightsail 儲存貯體存取權限和 Amazon S3 帳戶層級區塊公開存取組態納入考量。透過 Amazon S3 帳戶層級區塊公開存取，帳戶管理員和儲存貯體擁有者可以集中限制公開存取其 Amazon S3 和 Lightsail 儲存貯體。無論資源的建立方式為何，以及可能已設定的個別儲存貯體和物件許可為何，封鎖公用存取都可以將所有 Amazon S3 和 Lightsail 儲存貯體設為私有。如需詳細資訊，請參閱[封鎖儲存貯體的公有存取](#)。

## 將執行個體連接至儲存貯體以授予完整的程式設計存取權

將執行個體附加至 Lightsail 物件儲存貯體是提供值區存取權的最安全方式。資源存取功能是您將執行個體連接至儲存貯體的方式，可授予執行個體對儲存貯體的完整程式設計存取權。使用此方法，您就不必將儲存貯體憑證直接儲存在執行個體或應用程式中，也不必定期輪換憑證。例如，某些 WordPress 外掛程式可以存取執行個體可存取的值區。如需詳細資訊，請參閱[設定值區的資源存取權限](#)和[教學課程：將值區 Connect 至 WordPress 執行個體](#)。



### Resource access

Attach instances to this bucket to give them access without the need to manage credentials.

[Learn more about resource access](#)

[Attach instance](#)

 **WordPress**  
1 GB RAM, 1 vCPU, 40 GB SSD  
WordPress instance

[Detach](#)

不過，如果應用程式不在 Lightsail 執行個體上，您可以建立和設定值區存取金鑰。儲存貯體存取金鑰是不會自動輪換的長期憑證。

### Access keys

Create access keys to generate credentials for this bucket that you can use in your code, plugins, and applications. You can have a maximum of 2 access keys at a time.

[Learn more about access keys](#)

[+ Create access key](#)

Access key ID	Secret access key	Created	Last used
> AKIAIOSFODNN7EXAMPLE	****	8/20/2021, 10:45 AM	— 

您可以建立並使用存取金鑰，授予應用程式或外掛程式對您儲存貯體中物件的完整程式設計存取權。如果您在儲存貯體中使用存取金鑰，則應定期輪換金鑰並清點現有金鑰。確認上次使用存取金鑰的日期，以及使用該金鑰的日期符合您對金鑰使用方式的期望。AWS 區域 上次使用存取金鑰的日期會顯示在 Lightsail 主控台中；值區管理頁面「權限」索引標籤的「存取金鑰」區段。刪除未使用的存取金鑰。

如果您不小心公開了私密存取金鑰，則應將它刪除並新建一個。每個儲存貯體可擁有最多兩個存取金鑰。您可以同時擁有兩個不同的存取金鑰，但在您的儲存貯體中有一個未使用的存取金鑰，對於您需要以最少的停機時間輪換金鑰也很有幫助。若要輪換存取金鑰，請建立新的存取金鑰，在軟體上設定並進行測試，然後刪除舊金鑰。刪除後，存取金鑰即永久消失且無法復原。您只能改用新的存取金鑰。如需詳細資訊，請參閱[建立儲存貯體存取金鑰](#)。

## 使用跨帳戶存取權授予其他 AWS 帳戶存取值區中物件的權限

您可以使用跨帳戶存取權，讓擁有 AWS 帳戶的特定個人存取值區中的物件，而不會將值區及其物件公開。如果您已設定跨帳戶存取權，請確定所列出的帳戶 ID 是您要授與儲存貯體中物件存取權的正確帳戶。如需詳細資訊，請參閱[設定儲存貯體的跨帳戶存取權](#)。

### Cross-account access

Add cross-account access to give another AWS account access to this bucket without managing credentials. You can give a maximum of 10 accounts access to this bucket.

[Learn more about cross-account access](#)

[+ Add cross-account access](#)

111122223333	 
--------------	---

## 資料加密

Lightsail 會使用 Amazon 受管金鑰執行伺服器端加密，並透過強制執行 HTTPS (TLS) 對傳輸中的資料進行加密。伺服器端加密會使用存放在另一套服務中的金鑰來加密資料，有助於降低您資料的風險。此外，加密傳輸中的資料有助於防止潛在攻擊者利用 person-in-the-middle 或類似攻擊竊取或操控網路流量。

## 啟用版本控制

版本控制是在相同儲存貯體中保留多個物件版本的方式。您可以使用版本控制來保留、擷取和還原 Lightsail 值區中儲存之每個物件的每個版本。透過版本控制，您就可以輕鬆地復原失誤的使用者動作和故障的應用程式。如需詳細資訊，請參閱[啟用和暫停儲存貯體物件版本控制](#)。

## 監控和稽核最佳實務

下列最佳做法有助於偵測 Lightsail 值區的潛在安全弱點和事件。

### 啟用存取記錄並定期執行安全和存取稽核

存取記錄會提供對儲存貯體所提出要求的詳細記錄。這資訊可能包括要求類型 (GET、PUT)、要求中指定的資源，以及要求的處理時間和日期。啟用儲存貯體的存取記錄，並定期執行安全和存取稽核，以識別存取您儲存貯體的實體。根據預設，Lightsail 不會收集值區的存取記錄。您必須手動啟用存取記錄。如需詳細資訊，請參閱[儲存貯體存取日誌](#)和[啟用儲存貯體存取日誌](#)。

### 識別、標記及稽核您的 Lightsail 儲存貯體

識別 IT 資產是控管和保障安全的重要環節。您必須掌握所有 Lightsail 值區，才能評估其安全狀態，並針對潛在的弱點區域採取行動。

您可使用標記來識別重視安全或重視稽核的資源，接著在需要搜尋上述資源時運用這些標籤。如需詳細資訊，請參閱[標籤](#)。

### 使用 AWS 監控工具來實作監控

監控是維護 Lightsail 儲存貯體和其他資源的可靠性、安全性、可用性和效能的重要組成部分。您可以在 Lightsail 中監視和建立值區大小 (BucketSizeBytes) 和 Number of objects (NumberOfObjects) 儲存貯體量度的通知警示。例如，您可能需要在儲存貯體的大小增加或減少到特定大小時，或者當儲存貯體中的物件數目上升或下降到特定數目時收到通知。如需詳細資訊，請參閱[建立儲存貯體指標警示](#)。

## 使用 AWS CloudTrail

AWS CloudTrail 提供 Lightsail 中使用者、角色或 AWS 服務所採取之動作的記錄。您可以使用收集的資訊 CloudTrail 來判斷向 Lightsail 提出的要求、提出要求的 IP 位址、提出要求的人員、提出要求的時間以及其他詳細資訊。例如，您可以識別影響資料存取的動作 CloudTrail 項目 `CreateBucketAccessKey`，特別是 `GetBucketAccessKeysDeleteBucketAccessKey`、`SetResourceAccessForBucket`、和 `UpdateBucket`。設定 AWS 帳戶時，預設 CloudTrail 為啟用狀態。您可以在 CloudTrail 主控台中檢視最近的事件。若要為 Lightsail 值區建立持續的活動和事件記錄，您可以在 CloudTrail 主控台中建立追蹤。如需詳細資訊，請參閱《AWS CloudTrail 使用者指南》中的[記錄資料事件](#)。

## 監控 AWS 安全建議

主動監控註冊到 AWS 帳戶的主要電子郵件地址。AWS 將使用此電子郵件地址與您聯繫，以了解可能影響您的新興安全問題。

AWS 具有廣泛影響的作業問題會張貼在 [AWS Service Health Dashboard](#) 上。系統也會透過 Personal Health Dashboard，將操作問題張貼至個別帳戶。如需詳細資訊，請參閱 [AWS 運作狀態文件](#)。

## 控制對 Lightsail 值區和物件的存取

根據預設，所有 Amazon Lightsail 物件儲存資源 (儲存貯體和物件) 都是私有的。這表示只有值區擁有者 (建立該值區的 Lightsail 帳戶) 可以存取值區及其物件。儲存貯體擁有者可選擇性地將存取權授予他人。您可以採用下列方式授予儲存貯體及其物件的存取權：

- 唯讀存取權 – 下列選項透過儲存貯體的 URL (例如 `https://DOC-EXAMPLE-BUCKET.us-east-1.amazonaws.com/media/sailbot.jpg`) 控制儲存貯體及其物件的唯讀存取權。
  - 儲存貯體存取許可 – 使用儲存貯體存取許可，為網際網路上的任何人授予儲存貯體中所有物件的存取權。如需詳細資訊，請參閱本指南稍後的[儲存貯體存取許可](#)。
  - 個別物件存取許可 – 使用個別物件存取許可，為網際網路上的任何人授予儲存貯體中個別物件的存取權。如需詳細資訊，請參閱本指南稍後的[個別物件存取許可](#)。
  - 跨帳戶存取 — 使用跨帳戶存取權，將值區中所有物件的存取權授與其他 AWS 帳戶。如需詳細資訊，請參閱本指南稍後的[跨帳戶存取](#)。
- 讀取和寫入存取 – 下列選項會控制儲存貯體及其物件的完整讀取和寫入存取權。搭配 AWS Command Line Interface (AWS CLI)、AWS API 和 AWS SDK 使用這些選項。
  - Access keys (存取金鑰) – 使用存取金鑰授予應用程式或外掛程式的存取權。如需詳細資訊，請參閱本指南稍後的[存取金鑰](#)。

- 資源存取權 — 使用資源存取權授與 Lightsail 執行個體的存取權。如需詳細資訊，請參閱本指南稍後的[資源存取](#)。
- Amazon 簡易儲存服務區塊公開存取 — 使用 Amazon Simple Storage Service (Amazon S3) 帳戶層級區塊公開存取功能，集中限制公眾對 Amazon S3 和 Lightsail 儲存貯體的存取。無論個別儲存貯體和物件許可為何，封鎖公用存取都可以將所有 Amazon S3 和 Lightsail 儲存貯體設為私有。如需詳細資訊，請參閱本指南稍後的[Amazon S3 封鎖公開存取](#)。

如需有關儲存貯體的詳細資訊，請參閱[物件儲存](#)。如需有關安全最佳實務的詳細資訊，請參閱[物件儲存的安全最佳實務](#)。

## 儲存貯體存取許可

使用儲存貯體存取許可來控制對儲存貯體中物件的公有 (未驗證) 唯讀存取。設定儲存貯體存取許可時，您可以選擇以下其中一個選項：

- All objects are private (所有物件皆為私有) – 儲存貯體中的所有物件僅限於您或您授予存取權的任何人讀取。此選項不允許將個別物件設為公有 (唯讀)。
- Individual objects can be made public (read-only) (可將個別物件設為公有 (唯讀)) – 除非您將個別物件指定為公有 (唯讀)，否則儲存貯體中的物件僅限於您或您授予存取權的任何人讀取。此選項允許將個別物件設為公有 (唯讀)。如需詳細資訊，請參閱本指南稍後的[個別物件存取許可](#)。
- All objects are public (read-only) (所有物件皆為公有 (唯讀)) – 儲存貯體中的所有物件可供網際網路上的任何人讀取。在您選擇此選項時，儲存貯體中的所有物件都可以透過儲存貯體的 URL (例如 `https://DOC-EXAMPLE-BUCKET.us-east-1.amazonaws.com/media/sailbot.jpg`) 供網際網路上的任何人讀取。

如需有關設定儲存貯體存取許可的詳細資訊，請參閱[設定儲存貯體存取許可](#)。

## 個別物件存取許可

使用個別物件存取許可來控制儲存貯體中對個別物件的公有 (未驗證) 唯讀存取。個別物件存取許可只能在儲存貯體的 [Bucket access permissions](#) (儲存貯體存取許可) 允許將個別物件設為公有 (唯讀) 時進行設定。為個別物件設定存取許可時，您可以選擇以下其中一個選項：

- Private (私有) – 僅限於您或您授予存取權的任何人讀取物件。
- Public (read-only) (公有 (唯讀)) – 網際網路上的任何人皆可讀取物件。網際網路上的任何人都能透過儲存貯體的 URL (例如 `https://DOC-EXAMPLE-BUCKET.us-east-1.amazonaws.com/media/sailbot.jpg`) 讀取個別物件。

如需有關設定個別物件存取許可的詳細資訊，請參閱[設定儲存貯體中個別物件的存取許可](#)。

## 跨帳戶存取權

使用跨帳戶存取權，將值區中所有物件的已驗證唯讀存取權授與其他 AWS 帳戶及其使用者。如果您想與其他帳戶共享對象，則跨 AWS 帳戶訪問是理想的選擇。當您將跨帳戶存取權授予其他 AWS 帳戶，該帳戶中的使用者可以透過儲存貯體的 URL 擁有儲存貯體物件的唯讀權限 (例如 `https://DOC-EXAMPLE-BUCKET.us-east-1.amazonaws.com/media/sailbot.jpg`)。您最多可以授予 10 個 AWS 帳戶的存取權。

如需有關設定跨帳戶存取的詳細資訊，請參閱[設定儲存貯體的跨帳戶存取權](#)。

## 存取金鑰

請使用存取金鑰建立一組憑證，以授予對儲存貯體及其物件的完整讀寫存取權。存取金鑰是存取金鑰 ID 和私密存取金鑰為一組所組成。每個儲存貯體可擁有最多兩個存取金鑰。您可以在應用程式上設定存取金鑰，以便它可以使用 AWS API 和 AWS SDK 存取值區及其物件。您也可以使用 AWS CLI 設定存取金鑰。

如需有關建立存取金鑰的詳細資訊，請參閱[為儲存貯體建立存取金鑰](#)。

## 資源存取

針對 Lightsail 執行個體，使用資源存取權授與值區及其物件的完整讀取和寫入存取權。透過資源存取，您不必管理如存取金鑰這類憑證。若要授予執行個體的存取權，請將執行個體附接至同一 AWS 區域中的儲存貯體。若要拒絕存取，請從儲存貯體分開執行個體。如果您在執行個體上設定應用程式，以程式設計方式上傳和存取儲存貯體上的檔案，則資源存取是理想的選擇。其中一個使用案 WordPress 例是將執行個體設定為將媒體檔案儲存在值區上。如需詳細資訊，請參閱[教學課程：將值區 Connect 至 WordPress 執行個體](#)和[教學課程：使用含有內容傳遞網路散發的值區](#)。

如需有關設定資源存取的詳細資訊，請參閱[設定儲存貯體的資源存取](#)。

## Amazon S3 封鎖公開存取

使用 Amazon S3 區塊公開存取功能，集中限制公開存取 Amazon S3 和 Lightsail 中的儲存貯體。無論個別儲存貯體和物件許可為何，封鎖公用存取都可以將所有 Amazon S3 和 Lightsail 儲存貯體設為私有。您可以使用 Amazon S3 主控台、AWS CLI、開發套件和 REST API，為帳戶中的所有儲存貯體 (包括 Lightsail 物件儲存服務中的儲存貯體) 設定區塊公開存取設定。如需詳細資訊，請參閱[封鎖儲存貯體的公有存取](#)。

## 將檔案上傳至 Lightsail 物件儲存貯體

當您將檔案上傳到 Amazon Lightsail 物件儲存服務中的儲存貯體時，該檔案會以物件形式存放。物件是由檔案資料與說明物件的中繼資料所組成。您可以在每個儲存貯體內擁有任意物件數量。

您可以將任何檔案類型 (影像、備份、資料、影片等) 上傳至儲存貯體。您可以使用 Lightsail 主控台上傳的檔案大小上限為 2 GB。若要上傳較大的檔案，請使用 Lightsail API、AWS Command Line Interface (AWS CLI) 或 AWS SDKs。

Lightsail 會根據您要上傳的檔案大小提供下列選項：

- 使用 Lightsail 主控台上傳大小不超過 2 GB 的物件 — 透過 Lightsail 主控台，您可以上傳大小最大 2 GB 的單一物件。如需詳細資訊，請參閱本指南稍後的[使用 Lightsail 主控台將檔案上傳至值區](#)。
- 使用 AWS SDKs、REST API 或 AWS CLI — 透過單一作業上傳大小最多 5 GB 的物件，您可以上傳大小不超過 5 GB 的單一物件。PUT 如需詳細資訊，請參閱本指南稍後的[使用 AWS CLI 將檔案上傳至儲存貯體](#)。
- 使用 AWS SDKs REST API、或 AWS CLI — 使用分段上傳物件 API，您可以上傳 5 MB 到 5 TB 的單一大型物件。分段上傳 API 是為了改善大型物件的上傳體驗而設計。您可以上傳零件中的物件。這些物件部分可個別、依任何順序以及同時上傳。如需詳細資訊，請參閱[使用分段上傳將檔案上傳至儲存貯體](#)。

如需有關儲存貯體的詳細資訊，請參閱[物件儲存](#)。

### 物件索引鍵名稱和版本控制

當您使用 Lightsail 主控台上傳檔案時，會使用檔案名稱做為物件索引鍵名稱。物件索引鍵 (或索引鍵名稱) 可唯一識別存放於儲存貯體中的物件。檔案上傳到的資料夾 (如果有) 會用作索引鍵名稱字首。例如，如果您將名為 `sailbot.jpg` 的檔案上傳至儲存貯體中名為 `images` 的檔案夾，則完整的物件索引鍵名稱和字首為 `images/sailbot.jpg`。不過，該物件在主控台中會顯示為 `images` 資料夾中的 `sailbot.jpg`。如需有關物件金鑰名稱的詳細資訊，請參閱[物件儲存貯體的金鑰名稱](#)。

當您使用 Lightsail 主控台上傳目錄時，目錄中的所有檔案和子資料夾都會上傳至值區。然後，Lightsail 會指定物件索引鍵名稱，該名稱是每個上傳的檔案名稱和資料夾名稱的組合。例如，如果您上傳的檔案夾名稱包含 `images` 含兩個檔案 `sample2.jpg`，`sample1.jpg` 並且 Lightsail 會上傳這些檔案，然後指定對應的按鍵名稱 `images/sample1.jpg` 和 `images/sample2.jpg`。物件會在主控台中顯示為 `images` 檔案夾中的 `sample1.jpg` 與 `sample2.jpg`。

如果您上傳的檔案具有已存在的索引鍵名稱，並且您的儲存貯體未啟用版本控制，則新上傳的物件會取代先前的物件。但是，如果值區已啟用版本控制，Lightsail 會建立物件的新版本，而不是取代現有物件。如需詳細資訊，請參閱[啟用和暫停儲存貯體物件版本控制](#)。

## 使用 Lightsail 主控台將檔案上傳至值區

請完成下列程序，以使用 Lightsail 主控台上傳檔案和目錄。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁上，選擇儲存空間索引標籤。
3. 選擇您要向其上傳檔案和資料夾之儲存貯體的名稱。
4. 在 Object (物件) 索引標籤中，執行下列其中一個動作：
  - 將檔案和資料夾拖放至 Object (物件) 頁面。
  - 選擇 Upload (上傳)，然後選擇 File (檔案) 來上傳個別檔案，或選擇 Directory (目錄) 來上傳資料夾及其所有內容。

### Note

您也可以選擇 Create new folder (建立新的資料夾) 來建立資料夾。然後，您可以瀏覽至新資料夾並將檔案上傳至該資料夾。

當上傳完成時會顯示 Upload successful (上傳成功) 訊息。

## 使用 AWS CLI將檔案上傳至儲存貯體

完成下列程序，以使用 AWS Command Line Interface (AWS CLI) 將檔案和資料夾上傳至儲存貯體。您可以使用 `put-object` 命令來執行此動作。如需詳細資訊，請參閱《AWS CLI 命令參考》中的 [put-object](#)。

### Note

您必須先為 Lightsail AWS CLI 和 Amazon S3 安裝並進行設定，然後才能繼續執行此程序。如需詳細資訊，請參閱[設 AWS CLI 定使用 Lightsail](#)。

1. 開啟命令提示或終端機視窗。

## 2. 輸入下列命令，以將檔案上傳至儲存貯體。

```
aws s3api put-object --bucket BucketName --key ObjectKey --body LocalDirectory --acl bucket-owner-full-control
```

將命令中的以下範例文字取代為自訂文字：

- *BucketName* 使用您要將檔案上傳到的值區的名稱。
- *ObjectKey* 使用存儲桶中對象的完整對象密鑰。
- *LocalDirectory* 使用要上傳的文件的計算機上的本地目錄文件夾路徑。

範例：

- 在 Linux 或 Unix 電腦上：

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key images/sailbot.jpg --body home/user/Pictures/sailbot.jpg --acl bucket-owner-full-control
```

- 在 Windows 電腦上：

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key images/sailbot.jpg --body "C:\Users\user\Pictures\sailbot.jpg" --acl bucket-owner-full-control
```

您應該會看到類似以下範例的結果：

```
C:\>aws s3api put-object --bucket DOC-EXAMPLE-BUCKET --key images/sailbot.jpg --body "C:\Users\user\Pictures\sailbot.jpg"
{
  "ETag": "\"694d34edexamp1ed92d64f342aa234c3\""
}
```

## 設定IPv6僅AWSCLI用於要求

Amazon S3 支持存儲桶訪問IPv6。您可以使用雙堆疊端點IPv6透過 Amazon S3 API 呼叫提出請求。本節提供如何對雙堆疊端點發出要求的範例。IPv6如需詳細資訊，請參閱 [Amazon S3 使用者指南中的使用 Amazon S3 雙堆疊端點](#)。如需有關設定的指示 AWS CLI，請參閱 [AWS Command Line Interface 定與 Amazon Lightsail 搭配使用](#)。

### ⚠ Important

必須啟用用戶端和存取值區的網路才能使用IPv6。如需詳細資訊，請參閱可[IPv6達性](#)。

有兩種方法可以從IPv6僅執行個體發出 S3 請求。您可以設定 AWS CLI 將所有 Amazon S3 請求導向至指定 AWS 區域的雙堆疊端點。或者，如果您只想將雙堆疊端點用於指定的 AWS CLI 命令 (並非所有命令)，您可以將 S3 雙堆疊端點新增至每個命令。

## 配置 AWS CLI

在設定檔中的設定檔true中use\_dualstack\_endpoint將組態值設AWS定為，以將 Amazon S3 和 s3api AWS CLI 命令發出的所有 Amazon S3 請求導向指定區域的雙堆疊端點。您可以在 AWS CLI 組態檔案中指定區域，或使用--region 選項的指令中指定區域。

輸入下列指令來配置 AWS CLI。

```
aws configure set default.s3.use_dualstack_endpoint true
```

```
aws configure set default.s3.addressing_style virtual
```

## 將雙堆疊端點新增至特定指令

您可以將--endpoint-url參數設定為或用http://s3.dualstack.*aws-region*.amazonaws.com於任何 s3 https://s3.dualstack.*aws-region*.amazonaws.com 或 s3api 命令，以每個命令使用雙堆疊端點。在下面的例子中，替換*bucketname* 以及 *aws-region* 用你的桶的名稱和你的 AWS 區域。

```
aws s3api list-objects --bucket bucketname --endpoint-url https://s3.dualstack.aws-region.amazonaws.com
```

## 管理值區和物件

以下是管理 Lightsail 物件儲存貯體的一般步驟：

1. 了解 Amazon Lightsail 物件儲存服務中的物件和值區。如需詳細資訊，請參閱 [Amazon Lightsail 中的物件儲存](#)。

2. 了解您可以在 Amazon Lightsail 中為您的儲存貯體提供哪些名稱。如需詳細資訊，請參閱 [Amazon Lightsail 中的儲存貯體命名規則](#)。
3. 透過建立值區開始使用 Lightsail 物件儲存服務。如需詳細資訊，請參閱 [在 Amazon Lightsail 中建立值區](#)。
4. 了解儲存貯體的安全最佳實務，以及可以為儲存貯體設定的存取許可。可以將儲存貯體中的所有物件設為公有或私有，也可以選擇將個別物件設為公有。您也可以建立存取金鑰、將執行個體附加至儲存貯體，以及授予其他AWS帳戶的存取權，以授予儲存貯體的存取權。如需詳細資訊，請參閱 [Amazon Lightsail 物件儲存的安全最佳實務](#)和了解 [Amazon Lightsail 中的儲存貯體許可](#)。

了解儲存貯體存取許可後，請參閱下列指南來授予對儲存貯體的存取權：

- [封鎖儲存貯體的公開存取](#)
  - [在 Amazon Lightsail 集團中設定儲存貯體存取權限](#)
  - [在 Amazon Lightsail 中為儲存貯體中的個別物件設定存取權限](#)
  - [在 Amazon Lightsail 中為存儲桶創建訪問密鑰](#)
  - [在 Amazon Lightsail 中設定儲存貯體的資源存取](#)
  - [在 Amazon Lightsail 中設定儲存貯體的跨帳戶存取](#)
5. 了解如何為儲存貯體啟用存取日誌記錄，以及如何使用存取日誌來稽核儲存貯體的安全性。如需詳細資訊，請參閱下列指南。
    - [Amazon Lightsail 物件儲存服務中儲存貯體的存取記錄](#)
    - [存取 Amazon Lightsail 物件儲存服務中儲存貯體的日誌格式](#)
    - [在 Amazon Lightsail 物件儲存服務中啟用儲存貯體的存取記錄](#)
    - [在 Amazon Lightsail 中使用儲存貯體的存取日誌來識別請求](#)
  6. 建立IAM政策以授與使用者在 Lightsail 中管理值區的能力。如需詳細資訊，請參閱 [在 Amazon Lightsail 中管理儲存貯體的IAM政策](#)。
  7. 了解儲存貯體中物件的標記和識別方式。如需詳細資訊，請參閱 [了解 Amazon Lightsail 中的物件金鑰名稱](#)。
  8. 了解如何在儲存貯體中上傳檔案及管理物件。如需詳細資訊，請參閱下列指南。
    - [將文件上傳到 Amazon Lightsail](#)
    - [使用多部分上傳將檔案上傳到 Amazon Lightsail 中的儲存貯體](#)
    - [檢視儲存貯體中 Amazon Lightsail](#)
    - [在 Amazon Lightsail 中複製或移動值區中的物件](#)

- [在 Amazon Lightsail 中過濾儲存桶中的對象](#)
  - [標記儲存桶中 Amazon Lightsail](#)
  - [刪除儲存桶中 Amazon Lightsail](#)
9. 啟用物件版本控制功能來保留、擷取和恢復儲存貯體中所儲存每個物件的各個版本。如需詳細資訊，請參閱在 [Amazon Lightsail 中啟用和暫停儲存貯體中的物件版本控制](#)。
  10. 啟用物件版本控制之後，可以還原儲存貯體中物件的先前版本。如需詳細資訊，請參閱在 [Amazon Lightsail 中還原儲存貯體中的舊版物件](#)。
  11. 監控儲存貯體的使用率。如需詳細資訊，請參閱在 [Amazon Lightsail 中檢視儲存貯體的指標](#)。
  12. 設定儲存貯體指標的警示，以便在儲存貯體的使用率超過閾值時收到通知。如需詳細資訊，請參閱在 [Amazon Lightsail 中建立儲存貯體指標警示](#)。
  13. 如果儲存空間和網路傳輸不足，請變更儲存貯體的儲存計畫。如需詳細資訊，請參閱在 [Amazon Lightsail 中變更儲存貯體的計畫](#)。
  14. 了解如何將儲存貯體連線至其他資源。如需詳細資訊，請參閱下列教學課程。
    - [教學課程：將 WordPress 執行個體連接至 Amazon Lightsail 儲存貯體](#)
    - [教學課程：將 Amazon Lightsail 儲存貯體與 Lightsail 內容交付網路分發搭配使用](#)
  15. 如果不再使用儲存貯體，請刪除它。如需詳細資訊，請參閱 [刪除儲存貯體](#)。

# 在 Amazon Lightsail 上部署和管理容器

Amazon Lightsail 容器服務是可高度擴展的運算和聯網資源，您可以在其上部署、執行和管理容器。容器是標準的軟體單位，可將程式碼及其依存項目封裝在一起，讓應用程式在各個運算環境間快速可靠地執行。

您可以將 Lightsail 容器服務視為可讓您在 AWS 基礎設施上執行容器的運算環境，方法是使用您在本機電腦上建立並推送至服務的映像，或使用線上儲存庫 (例如 Amazon ECR Public Gallery) 的映像檔，在基礎設施上執行容器。

也可以透過安裝諸如 Docker 等軟體，在本機電腦上執行容器。Amazon Elastic Container Service (Amazon ECS) 和 Amazon Elastic Compute Cloud (Amazon EC2) 是您可以在其中執行容器的 AWS 基礎設施內的其他資源。如需詳細資訊，請參閱 [《Amazon ECS 開發人員指南》](#)。

## 內容

- [容器](#)
- [Lightsail 集裝箱服務元素](#)
  - [Lightsail 貨櫃服務](#)
  - [容器服務容量 \(規模和動力\)](#)
  - [定價](#)
  - [部署](#)
  - [部署版本](#)
  - [容器映像來源](#)
  - [貨櫃服務 ARN](#)
  - [公有端點和預設網域](#)
  - [自訂網域和 SSL/TLS 憑證](#)
  - [容器日誌](#)
  - [指標](#)
- [使用 Lightsail 貨櫃服務](#)

## 容器

容器是標準的軟體單位，可將程式碼及其依存項目封裝在一起，讓應用程式在各個運算環境間快速可靠地執行。您可以在開發環境中執行容器，將其部署至預生產環境，然後再部署至生產環境。無論開發環

境是本機電腦，預生產環境是資料中心的實體伺服器，或生產環境是雲端中的虛擬私有伺服器，容器都會可靠地執行。

容器映像是一種輕量、獨立、可執行的軟體套件，包含執行應用程式所需的一切：程式碼、執行時間、系統工具、系統程式庫和設定。容器映像在執行時間會成為容器。藉由容器化應用程式及其依存項目，您不必再操心軟體部署至作業系統和基礎設施上之後是否會正確執行 – 您能用更多時間專注於程式碼。

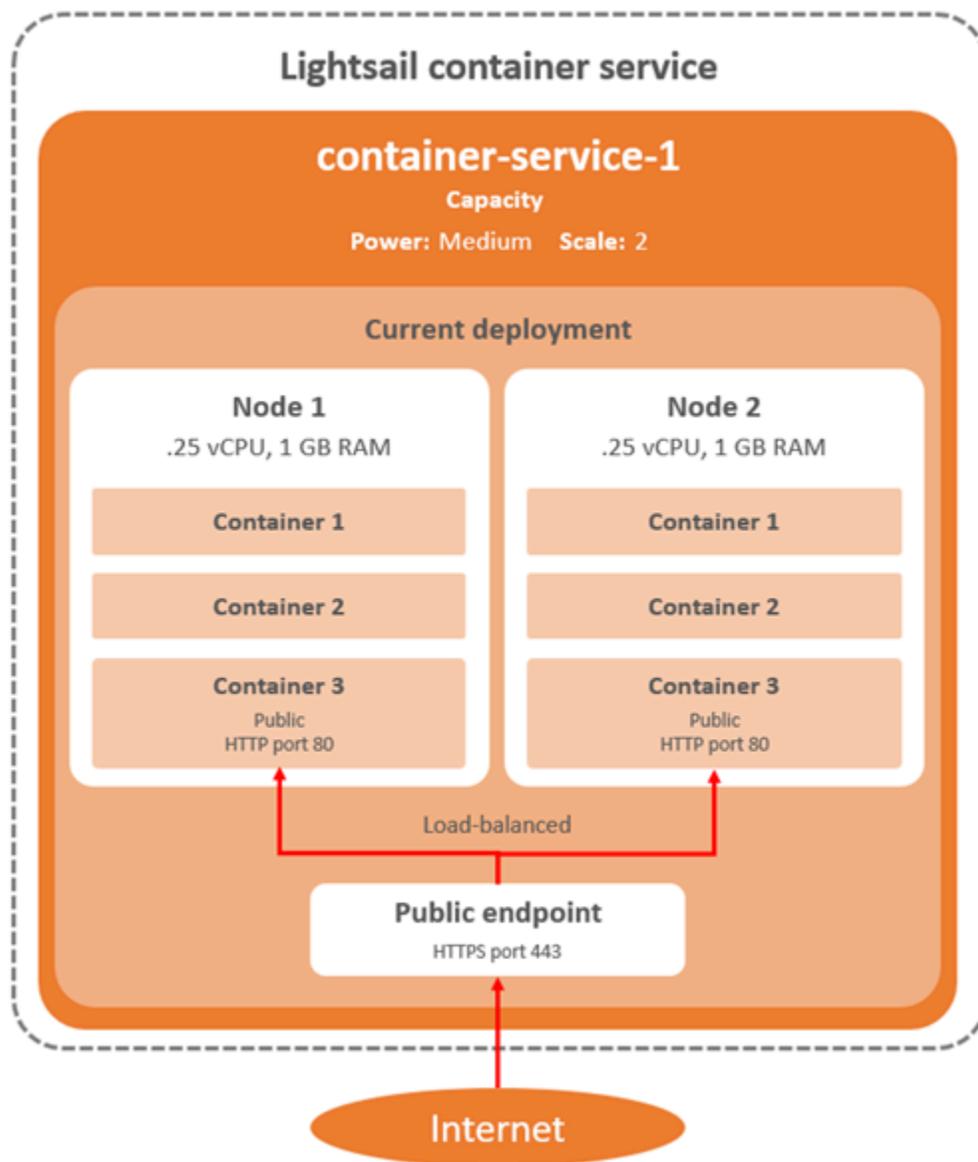
如需有關容器和容器映像的詳細資訊，請參閱 Docker 文件中的[何謂容器？](#)。

## Lightsail 集裝箱服務元素

以下是您在開始之前應瞭解的 Lightsail 容器服務的關鍵要素。

### Lightsail 貨櫃服務

容器服務是 Lightsail 運算資源，您可以在任何可使用 Lightsail AWS 區域的地方建立。您可以隨時建立和刪除容器服務。如需詳細資訊，請參閱[建立 Lightsail 容器服務](#)和[刪除 Lightsail 容器服務](#)。



## 容器服務容量 (規模和動力)

首次建立容器服務時，必須選擇下列容量參數：

- **Scale (規模)** – 您希望容器工作負載在其中執行的運算節點數量。系統會跨服務的運算節點複製容器工作負載。您可為容器服務指定最多 20 個運算節點。您可以根據要為服務提供動力的節點數來挑選規模，以獲得最佳的可用性和更高容量。流向容器的流量將在所有節點中進行負載平衡。
- **Power (動力)** – 容器服務中每個節點的記憶體和 vCPU。您可以選擇的動力包括超微型 (Na)、微型 (Mi)、小型 (Sm)、中型 (Md)、大型 (Lg) 和超大型 (XL)，每個都有遞增的記憶體和 vCPU。

如果將容器服務的規模指定為 1 以上，則系統會跨服務的多個運算節點複製容器工作負載。例如，如果服務規模為 3，且動力為超微型，則會有三個容器工作負載複本在三個運算資源上執行，每個資源都有 512 MB RAM 和 0.25 vCPU。傳入流量會在三個資源之間進行負載平衡。為容器服務指定越大的容量，就能處理越多的流量。

如果發現容器服務佈建不足，則可隨時動態增加容器服務的動力和規模，而不需要停機；如果發現容器服務過度佈建，則可予以減少。Lightsail 會隨著您目前的部署自動管理容量變更。如需詳細資訊，請參閱 [變更容器服務的容量](#)。

## 定價

容器服務每月計價方式是將動力價格乘以其運算節點數 (服務規模)。例如，服務具有中等動力 (價格為 40 USD)，且規模為 3 個運算節點，則每月費用為 120 USD。無論容器服務已啟用或停用，以及是否已有部署，都需要支付費用。您必須刪除容器服務才會停止收費。

每個容器服務不分所設定的容量，皆包含 500 GB 的每月資料傳輸配額。無論為服務選擇的動力和規模為何，資料傳輸配額都維持不變。超出配額的資料傳出至網際網路時，會產生超額費用 AWS 區域，每 GB 0.09 USD 起。從網際網路傳入的資料傳輸超過配額，不會產生超額費用。如需詳細資訊，請參閱 [Lightsail 定價頁面](#)。

## 部署

您可以在 Lightsail 容器服務中建立部署。部署是您希望在服務上啟動之容器工作負載的一組規格。

您可以為部署中的每個容器項目指定下列參數：

- 將啟動之容器的名稱
- 要用於容器的來源容器映像
- 啟動容器時要執行的命令
- 要套用至容器的環境變數
- 要在容器上開啟的網路連接埠
- 部署中要透過容器服務預設網域公開存取的容器

### Note

每個容器服務只能讓部署中的一個容器公開存取。

下列運作狀態檢查參數會套用至部署的公用端點 (在其啟動後)：

- 執行運作狀態檢查的目錄路徑。
- 進階運作狀態檢查設定，例如間隔秒數、逾時秒數、成功代碼、狀況良好的臨界值和狀況不良的臨界值。

容器服務一次可以有一個作用中的部署，而部署可有最多 10 個容器項目。您可以在建立容器服務的同時建立部署，也可在服務開始運作後建立部署。如需詳細資訊，請參閱[建立和管理容器服務部署](#)。

## 部署版本

您在容器服務中建立的每個部署都會儲存為部署版本。如果修改現有部署的參數，容器會重新部署至服務，而經修改的部署會產生新部署版本。每個容器服務的最新 50 個部署版本會儲存下來。您可使用 50 個部署版本之中任一個，在相同的容器服務中建立新部署。如需詳細資訊，請參閱[建立和管理容器服務部署](#)。

## 容器映像來源

建立部署時，您必須為部署中的每個容器項目指定來源容器映像。建立部署之後，容器服務會立即從您指定的來源提取映像，並用於建立容器。

指定的映像可取自以下來源：

- 公有登錄檔 (例如 Amazon ECR Public Gallery) 或一些其他公有容器映像登錄檔。如需有關 Amazon ECR Public 的詳細資訊，請參閱《Amazon ECR Public 使用者指南》中的[什麼是 Amazon Elastic Container Registry Public ?](#)。
- 已從本機電腦將映像推送到容器服務。如果在本機電腦上建立容器映像，則可將其推送到容器服務，以便在建立部署時使用。如需詳細資訊，請參閱[建立容器服務映像](#)以及[推送和管理容器映像](#)。

Lightsail 容器服務支援以 Linux 為基礎的容器映像檔。目前不支援以視窗為基礎的容器映像檔，但您可以在 Windows 上執行泊塢視窗、AWS Command Line Interface (AWS CLI) 和 Lightsail 控制項 (lightsailctl) 外掛程式，以建置並將您的 Linux 映像推送至 Lightsail 容器服務。

## 貨櫃服務 ARN

Amazon 資源名稱 (ARN) 可以唯一識別 AWS 資源。當您需要在所有項目 (例如 IAM 政策和 API 呼叫) 中明確指定資源時 AWS，我們需要 ARN。

若要取得容器服務的 ARN，請使用 `GetContainerServices` Lightsail API 動作，並使用參數指定容器服務的名稱。`serviceName` 您的容器服務 ARN 將列在該動作的結果中，如下列範例所示。如需詳細資訊，請參閱亞馬遜 API 參考 [GetContainerServices](#) 中的。

輸出結果會類似如下：

```
{
  "containerServices": [
    {
      "containerServiceName": "container-service-1",
      "arn": "arn:aws:lightsail: :111122223333:ContainerService/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
      "createdAt": "2024-01-01T00:00:00+00:00",
      "location": {
        "availabilityZone": "all",
        "regionName": "us-west-2"
      },
      .....
    }
  ]
}
```

## 公有端點和預設網域

建立部署時，您可以在部署中指定容器項目，作為容器服務的公有端點。公有端點容器上的應用程式可透過隨機產生的容器服務預設網域，在網際網路上公開存取。預設網域的格式為 `https://<ServiceName>.<RandomGUID>.<AWSRegion>.cs.amazonlightsail.com`，其中 `<ServiceName>` 是容器服務的名稱，`<RandomGUID>` 是 Lightsail 帳戶中隨機產生容器服務 AWS 區域的全域唯一識別碼，而 `<AWSRegion>` 是建立容器服務的位置。AWS 區域 Lightsail 容器服務的公用端點僅支援 HTTPS，而且不支援 TCP 或 UDP 流量。一項服務只能以一個容器為公有端點。因此，請務必選擇託管應用程式前端的容器作為公有端點，而其他容器則在內部存取。

您可以使用容器服務的預設網域，亦或使用自訂網域 (註冊的網域名稱)。如需有關搭配使用自訂域和容器服務的詳細資訊，請參閱 [啟用和管理容器服務的自訂域](#)。

### 私有網域

所有容器服務也都有格式化為的私有網域 `<ServiceName>.service.local`，其中 `<ServiceName>` 是容器服務的名稱。使用私有網域，以從與您的服務相同 AWS 區域的另一個 Lightsail 資源存取容器服務。如果您未在服務的部署中指定公有端點，則私有網域是存取容器服務的唯一方法。即使您未指定公有端點，系統仍會為容器服務產生預設網域，但在您嘗試瀏覽時會顯示 404 No Such Service 錯誤訊息。

若要使用容器服務的私有網域來存取特定容器，則必須指定容器的開放連接埠，以接受您的連線請求。您可以將要求的網域格式化為 `<ServiceName>.service.local:<PortNumber>`，其中 `<ServiceName>` 是容器服務的名稱，而 `<PortNumber>` 是您想要連接到的容器的開放連接埠來執行此操作。例如，如果在名為 `container-service-1` 的容器服務上建立部署，並指定連接埠 6379 開啟的 Redis 容器，則請求的網域格式應該為 `container-service-1.service.local:6379`。

## 自訂網域和 SSL/TLS 憑證

容器服務最多可使用 4 個自訂網域，而不使用預設網域。例如，您可以將自訂網域 (例如 `example.com`) 的流量引導至部署中標記為公有端點的容器。

若要搭配使用自訂網域與服務，則必須先針對要使用的網域請求 SSL/TLS 憑證。接著，您必須將一組 CNAME 記錄新增到網域的 DNS 來驗證 SSL/TLS 憑證。SSL/TLS 憑證驗證完畢後，您便可透過將有效的 SSL/TLS 憑證連接至服務，在容器服務上啟用自訂網域。如需詳細資訊，請參閱為 [您的 Lightsail 容器服務建立 SSL/TLS 憑證](#)、[驗證適用於您的 Lightsail 容器服務的 SSL/TLS 憑證](#)，以及為 [您的 Lightsail 容器服務啟用和管理自訂網域](#)。

## 容器日誌

容器服務中每個容器都會產生日誌，可讓您存取以診斷容器的操作。這些日誌會提供在容器中執行的 `stdout` 和 `stderr` 程序串流。如需詳細資訊，請參閱 [檢視容器服務日誌](#)。

## 指標

請監控容器服務指標，以診斷可能由過度使用導致的問題。您亦可監控指標，以協助判斷服務是否佈建不足或過度佈建。如需詳細資訊，請參閱 [檢視容器服務指標](#)。

## 使用 Lightsail 貨櫃服務

如果您打算將容器映像從本機電腦推送至服務，並在部署中使用這些映像，以下是管理 Lightsail 容器服務的一般步驟：

1. 在 Lightsail 帳戶中建立容器服務。如需詳細資訊，請參閱 [建立 Lightsail 容器服務](#)。
2. 在本機電腦上安裝所需軟體來建立自己的容器映像，並將其推送到 Lightsail 容器服務。如需詳細資訊，請參閱下列指南：
  - [安裝軟體以管理 Lightsail 容器服務的容器映像檔](#)
  - [為您的容器服務建立容 Lightsail 映像檔](#)

- [在您的 Lightsail 容器服務上推送和管理容器映像檔](#)
3. 在容器服務中建立部署，以設定和啟動容器。如需詳細資訊，請參閱[建立和管理 Lightsail 容器服務的部署](#)。
  4. 檢視容器服務的先前部署。您可以使用先前的部署版本來建立新部署。如需詳細資訊，請參閱[檢視和管理 Lightsail 容器服務的部署版本](#)。
  5. 檢視容器服務上的容器日誌。如需詳細資訊，請參閱[檢視 Lightsail 容器服務的容器記錄](#)。
  6. 針對要用於容器的網域建立 SSL/TLS 憑證。如需詳細資訊，請參閱[為您的容器服務建立 SSL/TLS 憑證](#)。
  7. 透過將記錄新增至網域的 DNS，驗證 SSL/TLS 憑證。如需詳細資訊，請參閱[驗證您的容器服務 Lightsail SSL/TLS 憑證](#)。
  8. 藉由將有效的 SSL/TLS 憑證連接至容器服務，啟用自訂網域。如需詳細資訊，請參閱[啟用和管理 Lightsail 容器服務的自訂網域](#)。
  9. 監控容器服務的使用率指標。如需詳細資訊，請參閱[檢視容器服務指標](#)。
  - 10.(選用) 將容器服務提高動力規格來垂直擴展其容量，並且提高規模規格來水平擴展容量。如需詳細資訊，請參閱[變更 Lightsail 容器服務的容量](#)。
  11. 若未使用容器服務，請將其刪除，避免每月產生費用。如需詳細資訊，請參閱[刪除 Lightsail 容器服務](#)。

如果您計劃在部署中使用來自公用登錄的容器映像，以下是管理 Lightsail 容器服務的一般步驟：

1. 在 Lightsail 帳戶中建立容器服務。如需詳細資訊，請參閱[建立 Lightsail 容器服務](#)。
2. 如果您打算使用公有登錄檔中的容器映像，請從 Amazon ECR Public Gallery 之類的公有登錄檔中尋找要使用的容器映像。如需有關 Amazon ECR Public 的詳細資訊，請參閱《Amazon ECR Public 使用者指南》中的[什麼是 Amazon Elastic Container Registry Public ?](#)。
3. 在容器服務中建立部署，以設定和啟動容器。如需詳細資訊，請參閱[建立和管理 Lightsail 容器服務的部署](#)。
4. 檢視容器服務的先前部署。您可以使用先前的部署版本來建立新部署。如需詳細資訊，請參閱[檢視和管理 Lightsail 容器服務的部署版本](#)。
5. 檢視容器服務上的容器日誌。如需詳細資訊，請參閱[檢視 Lightsail 容器服務的容器記錄](#)。
6. 針對要用於容器的網域建立 SSL/TLS 憑證。如需詳細資訊，請參閱[為您的容器服務建立 SSL/TLS 憑證](#)。
7. 透過將記錄新增至網域的 DNS，驗證 SSL/TLS 憑證。如需詳細資訊，請參閱[驗證您的容器服務 Lightsail SSL/TLS 憑證](#)。

8. 藉由將有效的 SSL/TLS 憑證連接至容器服務，啟用自訂網域。如需詳細資訊，請參閱[啟用和管理 Lightsail 容器服務的自訂網域](#)。
9. 監控容器服務的使用率指標。如需詳細資訊，請參閱[檢視容器服務指標](#)。
- 10.(選用) 將容器服務提高動力規格來垂直擴展其容量，並且提高規模規格來水平擴展容量。如需詳細資訊，請參閱[變更 Lightsail 容器服務的容量](#)。
11. 若未使用容器服務，請將其刪除，避免每月產生費用。如需詳細資訊，請參閱[刪除 Lightsail 容器服務](#)。

## 使用 Lightsail 建立高可用性的容器服務

在本指南中，我們將示範如何使用 Lightsail 主控台建立 Amazon Lightsail 容器服務，並說明您可以設定的容器服務設定。

在開始之前，我們建議您先熟悉 Lightsail 容器服務的元素。如需詳細資訊，請參閱[容器服務](#)。

### 容器服務容量 (規模和動力)

首次建立容器服務時，必須選擇容器服務的容量。容量由下列參數組合而成：

- **Scale (規模)** - 您希望容器工作負載在其中執行的運算節點數量。系統會跨服務的運算節點複製容器工作負載。您可為容器服務指定最多 20 個運算節點。您可以根據要為服務提供動力的節點數來挑選規模，以獲得最佳的可用性和更高容量。流向容器的流量將在所有節點中進行負載平衡。
- **Power (動力)** - 容器服務中每個節點的記憶體和 vCPU。您可以選擇的動力包括超微型 (Na)、微型 (Mi)、小型 (Sm)、中型 (Md)、大型 (Lg) 和超大型 (XL)，每個都有遞增的記憶體和 vCPU。

傳入流量會跨容器服務的規模 (運算節點數目) 進行負載平衡。例如，超微型動力且規模為 3 的服務，將會有 3 份執行中的容器工作負載複本。每個節點具有 512 MB RAM 和 0.25 vCPU。傳入流量會在 3 個節點之間進行負載平衡。為容器服務選擇越大的容量，就能處理越多的流量。

如果發現容器服務佈建不足，則可隨時動態增加容器服務的動力和規模，而不需要停機；如果發現容器服務過度佈建，則可予以減少。Lightsail 會隨著您目前的部署自動管理容量變更。如需詳細資訊，請參閱[變更 Lightsail 容器服務的容量](#)。

### 定價

容器服務每月計價方式是將動力基價乘以規模 (運算節點數)。例如，服務具有中等動力 (價格為 40 USD)，且規模為 3，則每月費用為 120 USD。

每個容器服務不分所設定的容量，皆包含 500 GB 的每月資料傳輸配額。無論為服務選擇的動力和規模為何，資料傳輸配額都維持不變。傳出到網際網路的資料傳輸超過配額會收取超額費用，價格因 AWS 區域而異，每 GB 為 0.09 USD 起。從網際網路傳入的資料傳輸超過配額，不會產生超額費用。如需詳細資訊，請參閱 [Lightsail 定價頁面](#)。

無論容器服務已啟用或停用，以及是否已有部署，都需要支付費用。您必須刪除容器服務才會停止收費。如需詳細資訊，請參閱 [刪除 Lightsail 容器服務](#)。

## 容器服務狀態

容器服務可處於下列狀態之一：

- Pending (待定) – 容器服務正在建立中。
- Ready (就緒)– 容器服務正在執行，但不具有作用中的容器部署。
- Deploying (部署中) – 部署正在啟動至容器服務。
- Running (執行中) – 容器服務正在執行，且具有作用中的容器部署。
- Updating (更新中)– 容器服務容量或其自訂網域正在更新中。
- Deleting (刪除中) – 容器服務正在刪除中。選擇刪除後，容器服務會變成此狀態，且僅在短時間內處於此狀態。
- Disabled (已停用) – 容器服務已停用，且其作用中的部署和容器 (如果有) 已關閉。

### 容器服務子狀態

如果容器服務處於部署中或更新中狀態，則容器服務狀態下方會另顯示下列子狀態之一：

- Creating system resources (建立系統資源) - 容器服務的系統資源正在建立中。
- Creating network infrastructure (建立網路基礎設施) - 容器服務的網路基礎設施正在建立中。
- Provisioning certificate (佈建憑證) - 容器服務的 SSL/TLS 憑證正在建立中。
- Provisioning service (佈建服務) - 容器服務正在佈建中。
- Creating deployment (建立部署) - 部署正在容器服務上建立。
- Evaluating health check (評估運作狀態檢查) - 部署的運作狀態正在評估中。
- Activating deployment (啟用部署) - 部署正在啟用中。

如果容器服務處於 Pending (待定) 狀態，則容器服務狀態下方會另顯示下列子狀態之一：

- Certificate limit exceeded (超過憑證限制) - 容器服務所需 SSL/TLS 憑證超過帳戶允許的憑證數目上限。
- Unknown error (不明錯誤) - 建立容器服務時發生錯誤。

## 建立容器服務

請完成下列程序，以建立 Lightsail 容器服務。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁，選擇 Containers (容器) 索引標籤。
3. 選擇 Create container service (建立容器服務)。
4. 在「建立容器服務」頁面中，選擇「變更」AWS 區域，然後 AWS 區域 為您的容器服務選擇一個。
5. 選擇容器服務的容量。如需詳細資訊，請參閱本指南的[容器服務容量 \(規模和動力\)](#) 一節。
6. 完成下列步驟來建立部署，此部署將在建立容器服務的同時啟動。否則，請跳至步驟 7 以建立無部署的容器服務。

若打算使用公有登錄檔中的容器映像，請建立有部署的容器服務。若打算使用本機電腦上的容器映像，請建立無部署的服務。您可以在服務開始運作後，將本機電腦中的容器映像推送到容器服務。接著便可使用於容器服務註冊的已推送容器映像來建立部署。

- a. 選擇 Create a deployment (建立部署)。
- b. 請選擇下列其中一個選項：
  - 選擇部署範例 — 選擇此選項，即可使用 Lightsail 團隊使用一組預先設定的部署參數策劃的容器映像來建立部署。此選項以最快最簡單的方式，讓熱門的容器在容器服務上運作。
  - Specify a custom deployment (指定自訂部署) – 選擇此選項，以指定您選擇的容器來建立部署。

部署表單檢視隨即開啟，您可在此輸入新的部署參數。

- c. 輸入部署的參數。如需有關可指定之部署參數的詳細資訊，請參閱[建立和管理 Lightsail 容器服務的部署指南中的部署參數](#)一節。
- d. 選擇 Add container entry (新增容器項目)，以將多個容器項目新增至部署。部署可有最多 10 個容器項目。
- e. 部署參數輸入完畢時，請選擇 Save and deploy (儲存和部署)，以在容器服務上建立部署。

## 7. 輸入容器服務的名稱。

容器服務名稱須符合下列原則：

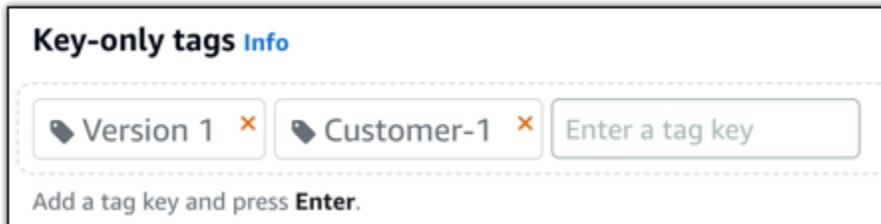
- 每個 Lightsail 帳戶 AWS 區域 中的每個項目都必須是唯一的。
- 必須包含 2 至 63 個字元。
- 只能包含英數字元和連字號。
- 連字號 (-) 可以分隔單字，但不能位於名稱的頭尾。

### Note

您指定的名稱是容器服務預設網域名稱的一部分，將在公開網路顯示。

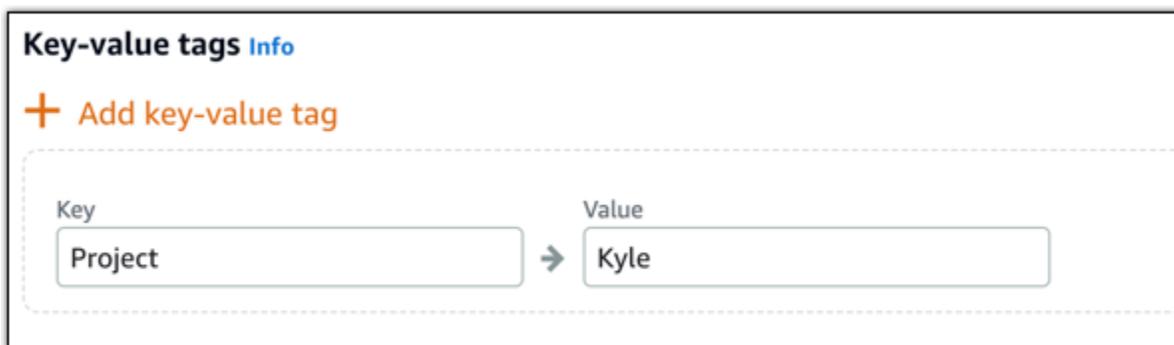
## 8. 選擇下列其中一個選項以新增標籤至容器服務：

- Add key-only tags (新增僅索引鍵標籤) 或 Edit key-only tags (編輯僅索引鍵標籤) (若標籤已新增)。在標籤索引鍵文字方塊中輸入新的標籤，接著按 Enter (輸入)。輸入標籤以新增之後，請選擇 Save (儲存)，如果不要新增則選擇 Cancel (取消)。



- Create a key-value tag (建立索引鍵值標籤)，接著將索引鍵輸入 Key (索引鍵) 文字方塊，將值輸入 Value (值) 文字方塊。完成輸入標籤後，請選擇 Save (儲存)，如果不要新增則選擇 Cancel (取消)。

鍵值標籤在儲存前一次只能新增一個。若要新增超過一個索引鍵值標籤，請重複之前的步驟。



**Note**

如需有關僅索引鍵和索引鍵值標籤的詳細資訊，請參閱[標籤](#)。

## 9. 選擇 Create container service (建立容器服務)。

系統會將您重新引導至新容器服務的管理頁面。正在建立中的新容器服務處於 Pending (待定) 狀態。幾分鐘後，若目前無部署，服務狀態會變更為 Ready (就緒)；若已建立部署，則會變更為 Running (執行中)。

## 為 Lightsail 容器服務建置和測試泊塢視窗映像檔

透過 Docker，可建置、執行、測試和部署以容器為基礎的分散式應用程式。Amazon Lightsail 容器服務在部署中使用 Docker 容器映像來啟動容器。

在本指南中，我們會為您介紹如何使用 Dockerfile 在本機電腦上建立容器映像。建立映像後，便可將其推送到 Lightsail 容器服務進行部署。

若要完成本指南中的程序，您應該對 Docker 及其運作方式有基本認識。如需有關 Docker 的詳細資訊，請參閱[什麼是 Docker?](#) 和 [Docker 概觀](#)。

### 內容

- [步驟 1：完成先決條件](#)
- [步驟 2：建立 Dockerfile 並建置容器映像](#)
- [步驟 3：執行新的容器映像](#)
- [\(選用\) 步驟 4：清理在本機電腦上執行的容器](#)
- [建立容器映像後的後續步驟](#)

## 步驟 1：完成先決條件

開始之前，您必須安裝所需軟體來建立容器，然後將其推送到 Lightsail 容器服務。例如，您必須安裝並使用 Docker 來建立和建置容器映像，以用於 Lightsail 容器服務。如需詳細資訊，請參閱[安裝軟體以管理 Amazon Lightsail 容器服務的容器映像](#)。

## 步驟 2：建立 Dockerfile 並建置容器映像

請完成下列程序來建立 Dockerfile，並利用其建置 mystaticwebsite Docker 容器映像。容器映像將用於 Ubuntu 上 Apache Web 伺服器所託管的簡單靜態網站。

1. 在您要存放 Dockerfile 的本機電腦上建立 mystaticwebsite 資料夾。
2. 在剛建立的資料夾中建立 Dockerfile。

Dockerfile 不使用副檔名，例如 .TXT。完整的檔案名稱為 Dockerfile。

3. 根據您設定容器映像的方式，複製下列其中一個程式碼區塊並貼至 Dockerfile：
  - 若要建立具有 Hello World 訊息的簡單靜態網站容器映像，請複製下列程式碼區塊並貼至 Dockerfile。此程式碼範本使用 Ubuntu 18.04 映像。RUN 指令會更新套件快取，以及安裝和設定 Apache，並將 Hello World 訊息寫至 Web 伺服器的文件根目錄。EXPOSE 指令會公開容器上的連接埠 80，而 CMD 指令會啟動 Web 伺服器。

```
FROM ubuntu:18.04

# Install dependencies
RUN apt-get update && \
    apt-get -y install apache2

# Write hello world message
RUN echo 'Hello World!' > /var/www/html/index.html

# Open port 80
EXPOSE 80

# Start Apache service
CMD ["/usr/sbin/apache2ctl", "-D", "FOREGROUND"]
```

- 若要將自己的一組 HTML 檔案用於靜態網站容器映像，請在存放 Dockerfile 的同一個資料夾中建立 html 資料夾。然後將 HTML 檔案放入該資料夾中。

HTML 檔案位於 html 資料夾中之後，請複製以下程式碼區塊並貼至 Dockerfile。此程式碼範本使用 Ubuntu 18.04 映像。RUN 指令會更新套件快取，以及安裝和設定 Apache。COPY 指令會將 html 資料夾內容複製到 Web 伺服器的文件根目錄。EXPOSE 指令會公開容器上的連接埠 80，而 CMD 指令會啟動 Web 伺服器。

```
FROM ubuntu:18.04
```

```
# Install dependencies
RUN apt-get update && \
    apt-get -y install apache2

# Copy html directory files
COPY html /var/www/html/

# Open port 80
EXPOSE 80

CMD ["/usr/sbin/apache2ctl", "-D", "FOREGROUND"]
```

4. 開啟命令提示或終端機視窗，並將目錄變更為存放 Dockerfile 的資料夾。
5. 輸入下列命令來使用資料夾中的 Dockerfile 建置容器映像。此命令會建置新的 Docker 容器映像，名為 mystaticwebsite。

```
docker build -t mystaticwebsite .
```

這時應該會出現確認映像建置成功的訊息。

6. 輸入下列命令來檢視本機電腦上的容器映像。

```
docker images --filter reference=mystaticwebsite
```

這時應該會出現類似以下範例的結果，顯示所建立的新容器映像。

```
C:\Users\user\Documents\Docker\Dockerfiles\mystaticwebsite>docker images --filter reference=mystaticwebsite
REPOSITORY          TAG         IMAGE ID      CREATED      SIZE
mystaticwebsite     latest     8f7ffd1013e0 8 minutes ago 199MB
```

新建置的容器映像已可進行在本機電腦上執行新容器的測試。前往本指南下一節[步驟 3：執行新的容器映像](#)。

## 步驟 3：執行新的容器映像

請完成以下步驟，以執行您建立的新容器映像。

1. 在命令提示或終端機視窗中，輸入下列命令來執行在本指南上一節[步驟 2：建立 Dockerfile 並建置容器映像](#)所建置的容器映像。-p 8080:80 選項會將容器上的公開連接埠 80 對應至本機電腦上的連接埠 8080。-d 選項指定容器應在分離模式下執行。

```
docker container run -d -p 8080:80 --name mystaticwebsite mystaticwebsite:latest
```

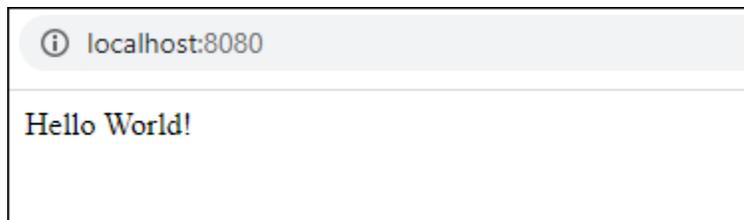
2. 輸入下列命令來檢視執行中的容器。

```
docker container ls -a
```

這時應該會出現類似以下範例的結果，顯示新的執行中容器。

```
C:\Users\... \Documents\Docker\Dockerfiles\mystaticwebsite>docker container ls -a
CONTAINER ID   IMAGE                COMMAND                  CREATED        STATUS        PORTS                NAMES
62382081e06b  mystaticwebsite:latest  "/bin/sh -c /root/ru..." 6 minutes ago  Up 6 minutes  0.0.0.0:8080->80/tcp  mystaticwebsite
```

3. 若要確認容器已處於運作狀態，請開啟新的瀏覽器視窗並瀏覽至 <http://localhost:8080>。這時應該會出現類似以下範例的訊息。此訊息確認容器已在本機電腦上運作。



新建置的容器映像已可推送到 Lightsail 帳戶，以便您將其部署至 Lightsail 容器服務。如需詳細資訊，請參閱[推送和管理 Amazon Lightsail 容器服務上的容器映像](#)。

## (選用) 步驟 4：清理在本機電腦上執行的容器

現在已建立可推送到 Lightsail 容器服務的容器映像，接著要按本指南所述程序清理本機電腦上執行的容器。

請完成下列步驟，以清理在本機電腦上執行的容器：

1. 執行下列命令來檢視正在本機電腦上執行的容器。

```
docker container ls -a
```

這時應該會出現類似下面的結果，其中列出了在本機電腦上執行之容器的名稱。

```
C:\Users\... \Documents\Docker\Dockerfiles\mystaticwebsite>docker container ls -a
CONTAINER ID   IMAGE                COMMAND                  CREATED        STATUS        PORTS                NAMES
62382081e06b  mystaticwebsite:latest  "/bin/sh -c /root/ru..." 6 minutes ago  Up 6 minutes  0.0.0.0:8080->80/tcp  mystaticwebsite
```

2. 執行下列命令來移除在本指南先前建立的執行中容器。這樣會強制停用容器，並將其永久刪除。

```
docker container rm <ContainerName> --force
```

在命令中，以您要停止的容器名稱取代 < ContainerName >，然後刪除。

範例：

```
docker container rm mystaticwebsite --force
```

本指南所建立的容器現在應已刪除。

## 建立容器映像後的後續步驟

建立容器映像後，請在準備好部署映像時將其推送到 Lightsail 容器服務。如需詳細資訊，請參閱[管理 Lightsail 容器服務映像](#)。

主題

- [推送、檢視和刪除 Lightsail 容器服務的容器映像檔](#)
- [安裝碼頭視窗 AWS CLI，以及容器的 Lightsail 控制外掛程式](#)
- [授予 Lightsail 容器服務存取 Amazon ECR 私有儲存庫](#)

## 推送、檢視和刪除 Lightsail 容器服務的容器映像檔

在 Amazon Lightsail 容器服務中建立部署時，您必須為每個容器項目指定來源容器映像。可以使用來自 Amazon ECR Public Gallery 等公有登錄檔的映像，也可以使用您在本機電腦上建立的映像。在本指南中，我們向您展示如何將容器映像從本機電腦推送到 Lightsail 容器服務。如需有關建立容器映像的詳細資訊，請參閱[建立容器服務映像](#)。

內容

- [先決條件](#)
- [將容器映像從本機電腦推送到容器服務](#)
- [檢視在容器服務上存放的容器映像](#)
- [刪除在容器服務上存放的容器映像](#)

## 必要條件

開始將容器映像推送到容器服務之前，請先滿足以下先決條件：

- 在 Lightsail 帳戶中建立容器服務。如需詳細資訊，請參閱[建立 Amazon Lightsail 容器服務](#)。
- 在本機電腦上安裝所需軟體來建立自己的容器映像，並將其推送到 Lightsail 容器服務。如需詳細資訊，請參閱[安裝軟體以管理 Amazon Lightsail 容器服務的容器映像](#)。
- 在本機電腦上建立您可以推送到 Lightsail 容器服務的容器映像。如需詳細資訊，請參閱[為 Amazon Lightsail 容器服務建立容器映像](#)。

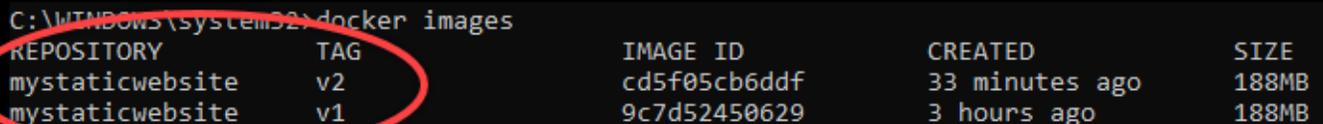
## 將容器映像從本機電腦推送到容器服務

請完成下列程序，以將容器映像推送到容器服務。

1. 開啟命令提示或終端機視窗。
2. 在命令提示或終端機視窗中，輸入下列命令以檢視本機電腦上目前的 Docker 映像。

```
docker images
```

3. 在結果中，找出您想要推送到容器服務之容器映像的名稱 (儲存庫名稱) 和標籤。請記下該資訊，因為您在下一個步驟會用到它。



```
C:\WINDOWS\system32>docker images
REPOSITORY          TAG                 IMAGE ID            CREATED             SIZE
mystaticwebsite     v2                 cd5f05cb6ddf       33 minutes ago    188MB
mystaticwebsite     v1                 9c7d52450629       3 hours ago       188MB
```

4. 輸入以下命令，將本機電腦上的容器映像推送到容器服務。

```
aws lightsail push-container-image --region <Region> --service-
name <ContainerServiceName> --label <ContainerImageLabel> --
image <LocalContainerImageName>:<ImageTag>
```

在命令中：

- 將 *<Region>* 替換為容器服務建立所在的 AWS 區域。
- *< ContainerServiceName >* 與您的容器服務的名稱。
- *< ContainerImageLabel >* 當您存儲在容器服務上時，帶有您想要為容器映像提供的標籤。指定描述性標籤，您可使用此標籤來追蹤已註冊容器映像的不同版本。

該標籤將成為容器服務產生的容器映像名稱的一部分。例如，如果容器服務名稱為 `container-service-1`，容器映像標籤為 `mystaticsite`，而這是您正在推送的容器映像的第一個版本，則容器服務產生的映像名稱將是 `:container-service-1.mystaticsite.1`。

- `< LocalContainerImageName >` 以您要推送至容器服務的容器映像檔名稱。您已在此程序的前一個步驟中取得容器映像名稱。
- `< ImageTag >` 帶有要推送到容器服務的容器映像的標籤。您已在此程序的前一個步驟中取得容器映像標籤。

範例：

```
aws lightsail push-container-image --region us-west-2 --service-name myservice --label mystaticwebsite --image mystaticwebsite:v2
```

您應該會看到類似以下範例的結果，其會確認容器映像已推送到容器服務。

```
C:\WINDOWS\system32>aws lightsail push-container-image --service-name myservice --label mystaticwebsite --image mystaticwebsite:v2

[185a355b95: Preparing
[180994b087: Preparing
[180c904ff3: Preparing
[18370aa736: Preparing
[18f192bbc8: Preparing
[18bc0bd923: Preparing
[7BDigest: sha256:3a585ca39bba342e390b39f2fea00bbc20f492c0cda7b923dd766abe31918f3b8/1.96kB
Image "mystaticwebsite:v2" registered.
Refer to this image as ":myservice.mystaticwebsite.2" in deployments.
```

請參閱本指南的下列[檢視在容器服務上存放的容器映像](#)章節，以在 Lightsail 主控台上的容器服務中檢視已推送的容器映像。

## 檢視在容器服務上存放的容器映像

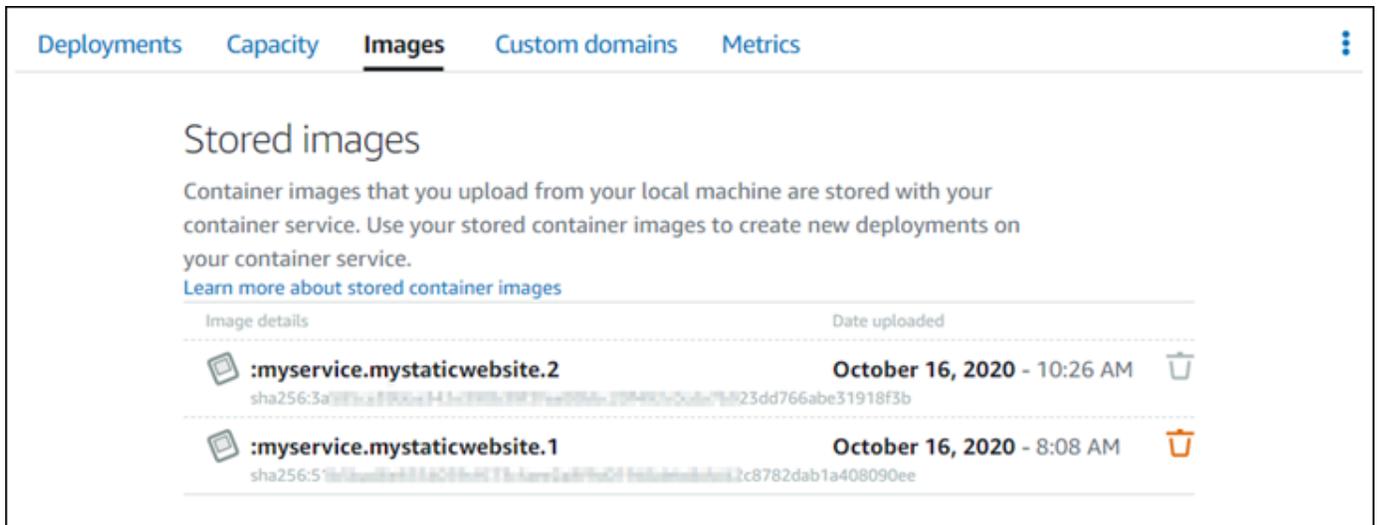
請完成下列程序，以檢視已推送並存放在容器服務上的容器映像。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁，選擇 Containers (容器) 索引標籤。
3. 選擇您要檢視其存放容器映像之容器服務的名稱。
4. 在容器服務管理頁面上，選擇 Images (映像) 索引標籤。

**Note**

如果您尚未將映像推送到容器服務，則不會顯示 Images (映像) 索引標籤。若要顯示容器服務的 Images (映像) 索引標籤，您必須先將容器映像推送到服務。

Images (映像) 頁面會列出已推送到容器服務且目前存放在服務上的容器映像。目前部署中正在使用的容器映像無法刪除，並以灰色的刪除圖示列出。



您可以使用在服務上存放的容器映像來建立部署。如需詳細資訊，請參閱「[建立和管理 Amazon Lightsail 容器服務的部署](#)」。

## 刪除在容器服務上存放的容器映像

請完成下列程序，以刪除已推送並正存放在容器服務上的容器映像。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁，選擇 Containers (容器) 索引標籤。
3. 選擇您要檢視目前部署之容器服務的名稱。
4. 在容器服務管理頁面上，選擇 Images (映像) 索引標籤。

**Note**

如果您尚未將映像推送到容器服務，則不會顯示 Images (映像) 索引標籤。若要顯示容器服務的 Images (映像) 索引標籤，您必須先將容器映像推送到服務。

5. 尋找您要刪除的容器映像，然後選擇刪除 (垃圾桶) 圖示。

**Note**

目前部署中正在使用的容器映像無法刪除，且其刪除圖示會呈現灰色。

6. 在出現的確認提示中，選擇 Yes, delete (是，刪除) 以確認要永久刪除存放的映像。

您存放的容器映像會立即從容器服務中刪除。

## 安裝碼頭視窗 AWS CLI，以及容器的 Lightsail 控制外掛程式

您可以使用 Amazon Lightsail 主控台建立您的 Lightsail 容器服務，並使用線上公有登錄檔 (例如 Amazon ECR 公用圖庫) 的容器映像建立部署。但若要建立自己的容器映像，並將其推送到容器服務，您必須在打算建立容器映像的同一台電腦上安裝下列其他軟體：

- 泊塢視窗 — 執行、測試和建立您自己的容器映像檔，然後可與 Lightsail 容器服務搭配使用。
- AWS Command Line Interface (AWS CLI) — 指定您建立之容器映像檔的參數，然後將其推送至 Lightsail 容器服務。2.1.1 版及更高版本將與 Lightsail 控制插件一起使用。
- Lightsail 控制項 (lightsailctl) 外掛程式 — 允許存 AWS CLI 取本機電腦上的容器映像檔。

本指南的下列章節說明如何下載和安裝這些軟體套件。如需有關容器服務的詳細資訊，請參閱[容器服務](#)。

### 內容

- [安裝 Docker](#)
- [安裝 AWS CLI](#)
- [安裝 Lightsail 控制外掛程式](#)
  - [在 Windows 中安裝 lightsailctl 外掛程式](#)
  - [在 macOS 中安裝 lightsailctl 外掛程式](#)

- [在 Linux 中安裝 lightsailctl 外掛程式](#)

## 安裝 Docker

Docker 是一種技術，可讓您建置、執行、測試和部署以 Linux 容器為基礎的分散式應用程式。如果您想要建立自己的容器映像檔，然後可與 Lightsail 容器服務搭配使用，則必須安裝並使用 Docker 軟體。如需詳細資訊，請參閱[為您的 Lightsail 容器服務建立容器映像](#)。

Docker 可在多個不同的作業系統上使用，包括大部分的現代 Linux 發行版本，例如 Ubuntu，甚至是 macOS 和 Windows。如需有關如何在特定作業系統上安裝 Docker 的詳細資訊，請參閱《[Docker 安裝指南](#)》。

### Note

請一律安裝最新版本的 Docker。舊版本的泊塢視窗無法保證可與本指南稍後描述的 AWS CLI 和 Lightsail 控制 (lightsailctl) 外掛程式一起使用。

## 安裝 AWS CLI

這 AWS CLI 是一個開放原始碼工具，可讓您使用命令列殼層中的命令與 AWS 服務 (例如 Lightsail) 互動。您必須安裝並使用，AWS CLI 將在本機電腦上建立的容器映像推送至 Lightsail 容器服務。

提 AWS CLI 供下列版本：

- 2.x 版 – AWS CLI 目前全面推出的版本。這是最新的主要版本，支援所有最新功能，包括將容器映像推送至 Lightsail 容器服務的功能。AWS CLI 2.1.1 版及更高版本將與 Lightsail 控制插件一起使用。
- 版本 1.x — 可用於向後相容性的先前版本。AWS CLI 此版本不支援將容器映像推送至 Lightsail 容器服務的功能。因此，您必須改為安裝 AWS CLI 版本 2。

AWS CLI 版本 2 適用於 Linux、macOS 和視窗作業系統。如需有關如何在這些作業系統 AWS CLI 上安裝的指示，請參閱《AWS CLI 使用者指南》中的〈[安裝 AWS CLI 版本 2](#)〉。

## 安裝 Lightsail 控制外掛程式

Lightsail 控制項 (lightsailctl) 外掛程式是一個輕量級的應用程式，可讓您存 AWS CLI 取您在本機電腦上建立的容器映像。它可讓您將容器映像推送至 Lightsail 容器服務，以便將其部署到服務中。

## 系統要求

- 支援 64 位元的 Windows、macOS 或 Linux 作業系統。
- AWS CLI 版本 2 必須安裝在您的本機電腦上，才能使用 `lightsailctl` 外掛程式。如需詳細資訊，請參閱本指南前述的[安裝 AWS CLI](#) 一節。

### 使用最新版本的 `lightsailctl` 外掛程式

`lightsailctl` 外掛程式偶爾會更新以增強功能。每次使用 `lightsailctl` 外掛程式時，系統都會執行檢查以確認您使用的是最新版本。如果發現有可用的新版本，系統會提示您更新至最新版本以運用最新功能。當有可用的更新版本時，您必須重複安裝程序以取得最新版本的 `lightsailctl` 外掛程式。

下面列出了所有 `lightsailctl` 外掛程式的版本及每個版本包含的功能及增強功能。

- v1.0.0 版 (2020 年 11 月 12 日發行) — 初始版本新增了第 2 AWS CLI 版的功能，可將容器映像推送至 Lightsail 容器服務。

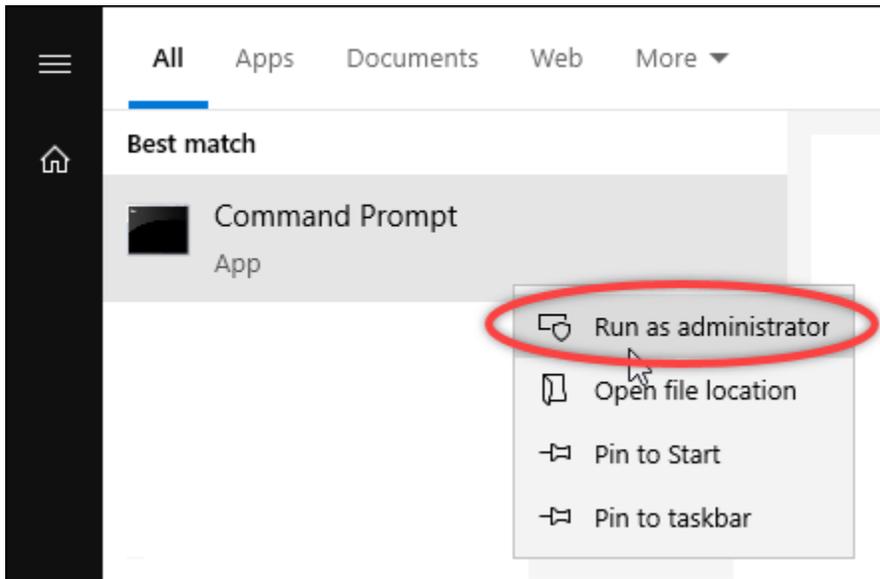
### 在 Windows 中安裝 `lightsailctl` 外掛程式

完成下列程序以在 Windows 中安裝 `lightsailctl` 外掛程式。

1. 從下列 URL 下載可執行檔，並將其儲存至 `C:\Temp\lightsailctl\` 目錄。

```
https://s3.us-west-2.amazonaws.com/lightsailctl/latest/windows-amd64/lightsailctl.exe
```

2. 選擇 Windows Start (開始) 按鈕，然後搜尋 `cmd`。
3. 在結果中，以右鍵按一下 `Command Prompt (命令提示) 應用程式`，然後選擇 `Run as administrator (以管理員身分執行)`。

**Note**

您可能會看到提示，其中會詢問您是否要允許命令提示對裝置進行變更。您必須選擇 Yes (是) 以繼續安裝。

4. 輸入下列命令以設定路徑環境變數，該變數會指向您在其中儲存了 lightsailctl 外掛程式的 C:\Temp\lightsailctl\ 目錄。

```
setx PATH "%PATH%;C:\Temp\lightsailctl" /M
```

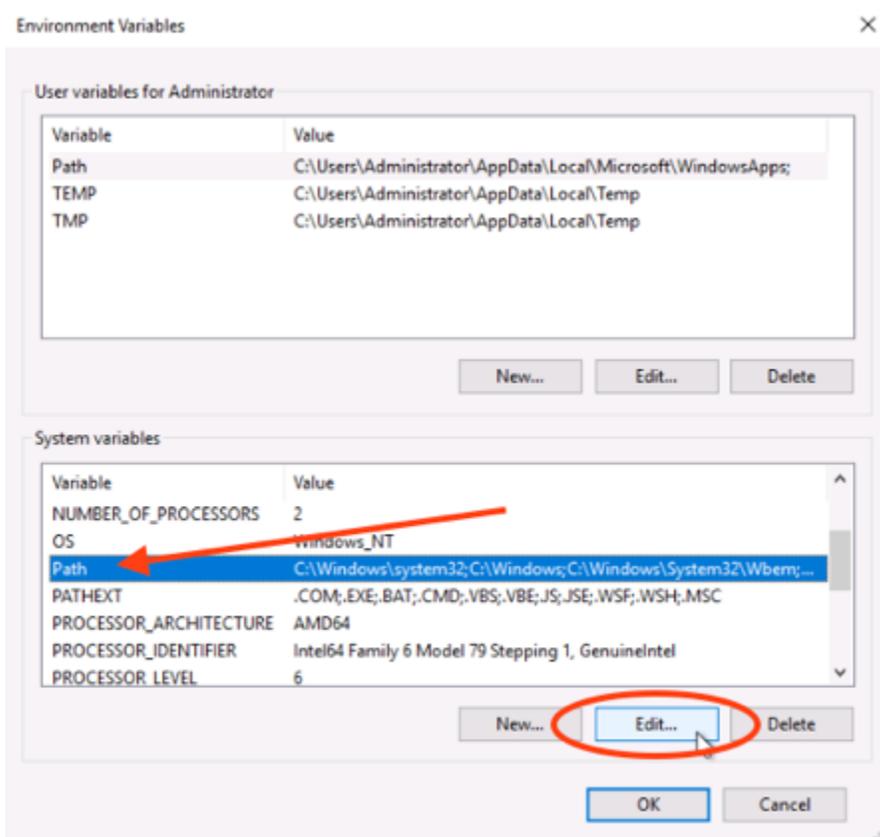
您應該會看到類似以下範例的結果。

```
C:\WINDOWS\system32>setx PATH "%PATH%;C:\Temp\lightsailctl\" /M
SUCCESS: Specified value was saved.
```

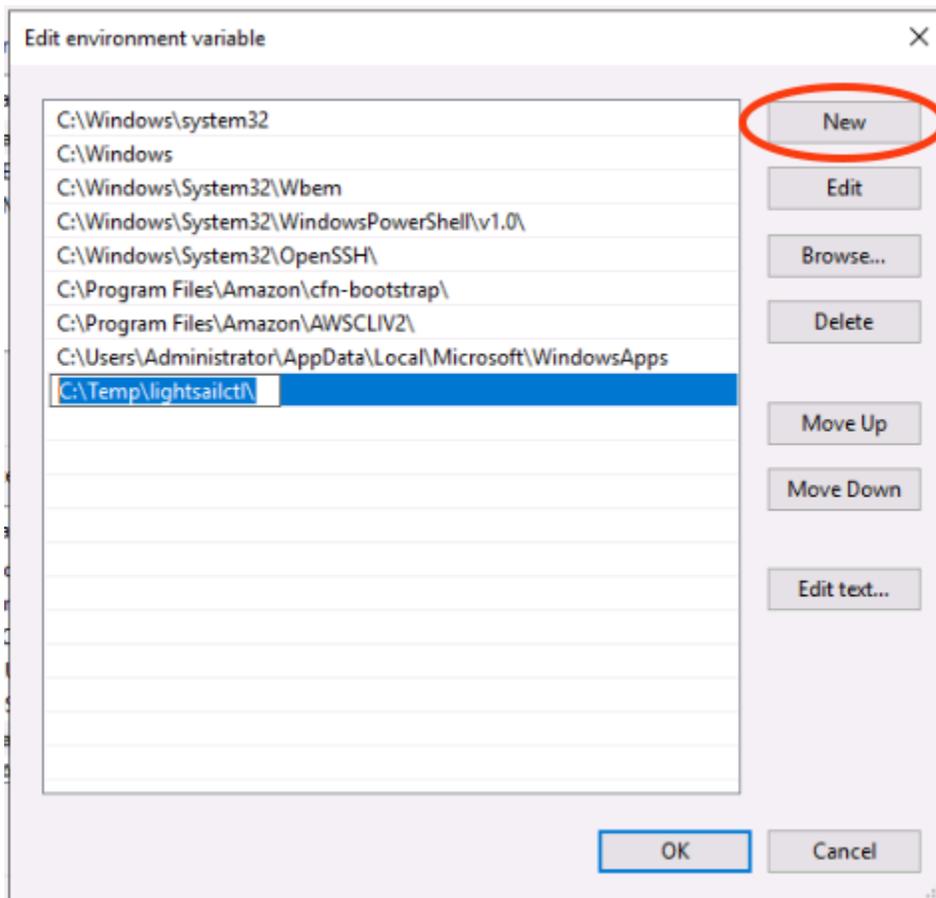
setx 命令將截斷超過 1024 個字元。如果您的 PATH 中已經設定多個變數，請使用下列程序來手動設定路徑環境變數。

1. 在 Start (開始) 選單上，開啟 Control Panel (控制面板)。
2. 選擇 System and Security (系統和安全性)，然後選擇 System (系統)。
3. 選擇進階系統設定。

- 在 System Properties (系統屬性) 對話方塊的 Advanced (進階) 索引標籤上，選擇 Environment Variables (環境變數)。
- 在 Environment Variables (環境變數) 對話方塊的 System Variables (系統變數) 方塊中，選取 Path (路徑)。
- 選擇位於 System Variables (系統變數) 方塊下的 Edit (編輯) 按鈕。



- 選擇 New (新增)，然後輸入下列路徑：C:\Temp\lightsailctl\



8. 在連續三個對話方塊中選擇 OK (確定)，然後關閉 System (系統) 對話方塊。

您現在可以使用 AWS Command Line Interface (AWS CLI) 將容器映像推送至 Lightsail 容器服務。如需詳細資訊，請參閱[推送和管理容器映像](#)。

在 macOS 中安裝 lightsailctl 外掛程式

請完成下列其中一個程序，以在 macOS 中下載並安裝 lightsailctl 外掛程式。

Homebrew 下載與安裝

1. 開啟終端機視窗。
2. 輸入下列命令，即可下載並安裝 lightsailctl 外掛程式。

```
brew install aws/tap/lightsailctl
```

**Note**

如需有關 Homebrew 的詳細資訊，請參閱 [Homebrew](#) 網站。

## 手動下載並安裝

1. 開啟終端機視窗。
2. 輸入以下命令即可下載 lightsailctl 外掛程式並將其複製到回收筒資料夾。

```
curl "https://s3.us-west-2.amazonaws.com/lightsailctl/latest/darwin-amd64/lightsailctl" -o "/usr/local/bin/lightsailctl"
```

3. 輸入下列命令即可使該外掛程式成為可執行檔。

```
chmod +x /usr/local/bin/lightsailctl
```

4. 輸入下列命令，即可清除外掛程式的擴充屬性。

```
xattr -c /usr/local/bin/lightsailctl
```

您現在可以使用將容器映像推送 AWS CLI 至 Lightsail 容器服務。如需詳細資訊，請參閱 [推送和管理容器映像](#)。

## 在 Linux 中安裝 lightsailctl 外掛程式

請完成下列程序，在 Linux 上安裝 Lightsail 容器服務外掛程式。

1. 開啟終端機視窗。
2. 輸入下列命令，即可下載 lightsailctl 外掛程式。

- 對於 AMD 64 位元架構版本的外掛程式：

```
curl "https://s3.us-west-2.amazonaws.com/lightsailctl/latest/linux-amd64/lightsailctl" -o "/usr/local/bin/lightsailctl"
```

- 對於 ARM 64 位元架構版本的外掛程式：

```
curl "https://s3.us-west-2.amazonaws.com/lightsailctl/latest/linux-arm64/lightsailctl" -o "/usr/local/bin/lightsailctl"
```

3. 輸入下列命令即可使該外掛程式成為可執行檔。

```
sudo chmod +x /usr/local/bin/lightsailctl
```

您現在可以使用將容器映像推送 AWS CLI 至 Lightsail 容器服務。如需詳細資訊，請參閱[推送和管理容器映像](#)。

## 授予 Lightsail 容器服務存取 Amazon ECR 私有儲存庫

Amazon Elastic Container Registry (Amazon ECR) 是一種 AWS 受管容器映像登錄服務，可使用 AWS Identity and Access Management (IAM) 支援具有以資源為基礎的許可的私有存放庫。您可以讓您的 Amazon Lightsail 容器服務存取您的 Amazon ECR 私有儲存庫。AWS 區域然後，可以將映像從私有儲存庫部署至容器服務。

您可以使用 Lightsail 主控台或 () 來管理 Lightsail 容器服務和 Amazon ECR 私有儲存庫的存取。AWS Command Line Interface AWS CLI 不過，我們建議您使用 Lightsail 主控台，因為這樣可以簡化程序。

如需有關容器服務的詳細資訊，請參閱[容器服務](#)。如需 Amazon ECR 的詳細資訊，請參閱《[Amazon ECR 使用者指南](#)》。

### 內容

- [必要許可](#)
- [使用 Lightsail 主控台來管理對私人存放庫的存取](#)
- [使用 AWS CLI 來管理私有存放庫的存取](#)
  - [啟用或停用 Amazon ECR 映像 puller IAM 角色](#)
  - [判定 Amazon ECR 私有儲存庫是否具有政策陳述式](#)
    - [將政策新增至沒有政策陳述式的私有儲存庫](#)
    - [將政策新增至具有政策陳述式的私有儲存庫](#)

## 所需的許可

將管理 Lightsail 容器服務存取 Amazon ECR 私有儲存庫的使用者必須在 IAM 中具有下列其中一項許可政策。如需詳細資訊，請參閱《AWS Identity and Access Management 使用者指南》中的[新增和移除 IAM 身分許可](#)。

授予對任何 Amazon ECR 私有儲存庫的存取權

下列許可政策會授予使用者許可，以設定對任何 Amazon ECR 私有儲存庫的存取權。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ManageEcrPrivateRepositoriesAccess",
      "Effect": "Allow",
      "Action": [
        "ecr:SetRepositoryPolicy",
        "ecr:DescribeRepositories",
        "ecr>DeleteRepositoryPolicy",
        "ecr:GetRepositoryPolicy"
      ],
      "Resource": "arn:aws:ecr:*:AwsAccountId:repository/*"
    }
  ]
}
```

在政策中，*AwsAccountId*以您的 AWS 帳戶 ID 號碼取代。

授予對特定 Amazon ECR 私有儲存庫的存取權

下列許可政策會給予使用者許可，在特定 AWS 區域區域中設定對特定 Amazon ECR 私有儲存庫的存取權。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ManageEcrPrivateRepositoriesAccess",
      "Effect": "Allow",
      "Action": [
        "ecr:SetRepositoryPolicy",
```

```

        "ecr:DescribeRepositories",
        "ecr>DeleteRepositoryPolicy",
        "ecr:GetRepositoryPolicy"
    ],
    "Resource": "arn:aws:ecr:AwsRegion:AwsAccountId:repository/RepositoryName"
}
]
}

```

將政策中的以下範例文字取代為自訂文字：

- *AwsRegion*— 私有存放庫的 AWS 區域 程式碼 (例如 , us-east-1)。您的 Lightsail 容器服務必須與您要存取 AWS 區域 的私有儲存庫位於相同的位置。
- *AwsAccountId*— 您的 AWS 帳戶 ID 號碼。
- *RepositoryName*— 您要管理其存取權的私人存放庫名稱。

下列是使用範例值填入的許可政策範例。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ManageEcrPrivateRepositoriesAccess",
      "Effect": "Allow",
      "Action": [
        "ecr:SetRepositoryPolicy",
        "ecr:DescribeRepositories",
        "ecr>DeleteRepositoryPolicy",
        "ecr:GetRepositoryPolicy"
      ],
      "Resource": "arn:aws:ecr:us-east-1:111122223333:repository/my-private-repo"
    }
  ]
}

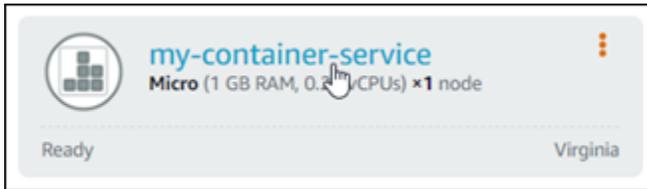
```

## 使用 Lightsail 主控台來管理對私人存放庫的存取

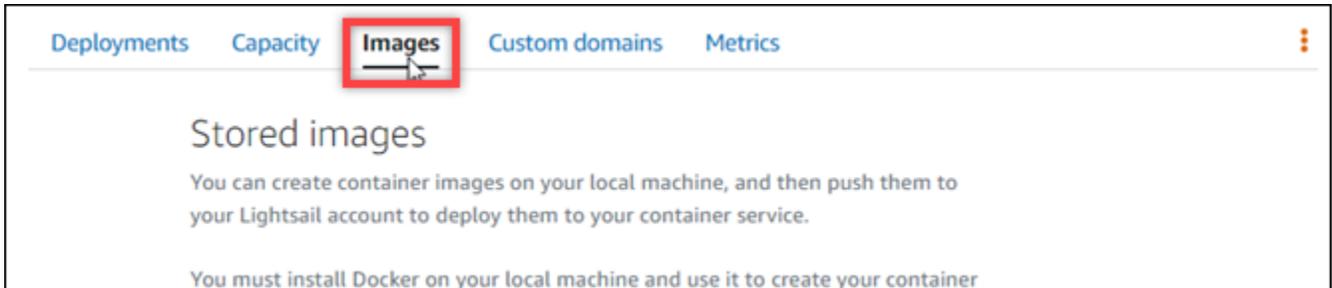
請完成下列程序，以使用 Lightsail 主控台來管理 Lightsail 容器服務對 Amazon ECR 私有儲存庫的存取。

1. 登入主 [Lightsail 台](#)。

2. 在 Lightsail 首頁，選擇 Containers (容器) 索引標籤。
3. 選擇想要為其設定對 Amazon ECR 私有儲存庫存取權的容器服務名稱。



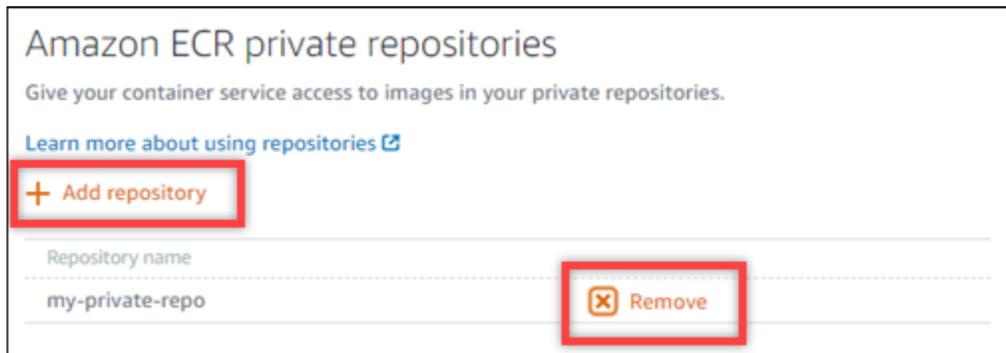
4. 選擇 Images (映像) 索引標籤。



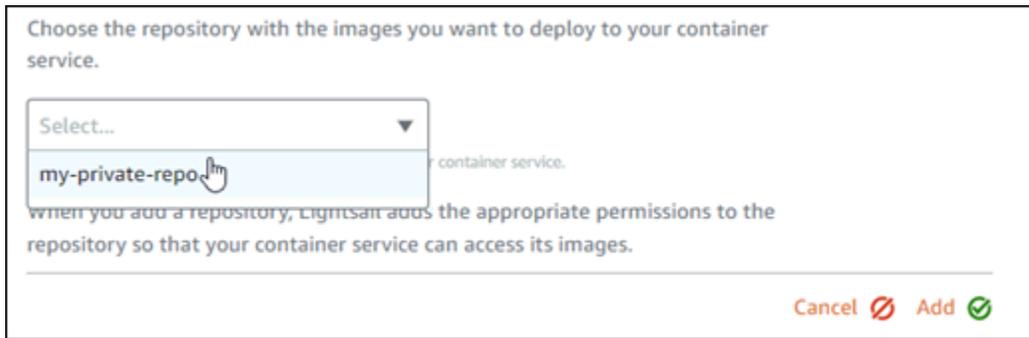
5. 選擇新增儲存庫以授予容器服務對於 Amazon ECR 私有儲存庫的存取權。

#### Note

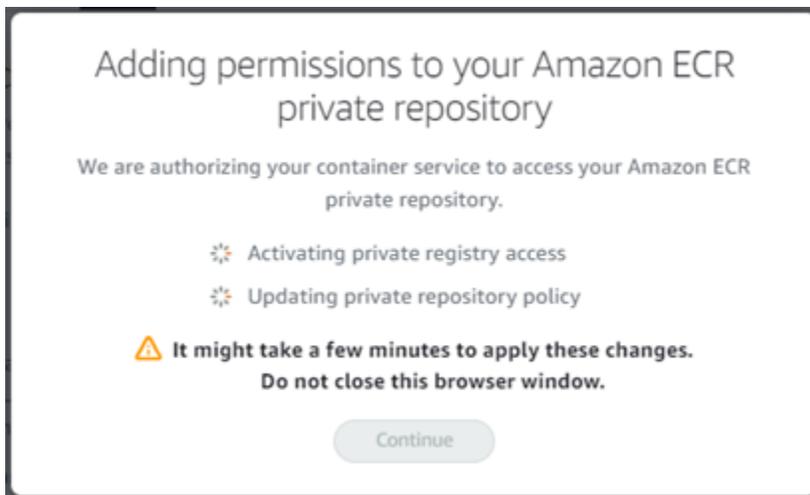
您可以選擇移除以移除容器服務對於先前新增的 Amazon ECR 私有儲存庫的存取權。



6. 在顯示的下拉式選單中，選擇要存取的私有儲存器，然後選擇 Add (新增)。



Lightsail 需要一些時間來為您的容器服務啟動 Amazon ECR 映像拉拔器 IAM 角色，其中包括主要的 Amazon 資源名稱 (ARN)。然後，Lightsail 會自動將 IAM 角色主體 ARN 新增至您所選取之 Amazon ECR 私有儲存庫的許可政策。這將授予容器服務對私有儲存庫及其映像的存取權。強制回應視窗出現並表明程序已完成且您可以選擇 Continue (繼續) 之前，請勿關閉瀏覽器視窗。



7. 啟用完成後，請選擇 Continue (繼續)。

新增選取的 Amazon ECR 私有儲存庫後，它會列於頁面的 Amazon ECR 私有儲存庫區段。此頁面包含如何將映像從私人存放庫部署至 Lightsail 容器服務的指示。若要使用私有儲存庫中的映像，請指定建立容器服務部署時頁面上顯示為 Image (映像) 值的 URI 格式。在指定的 URI 中，請將範例 `{image tag}` 取代為您要部署的映像標籤。如需詳細資訊，請參閱[建立和管理容器服務部署](#)。

### Next steps

To deploy an image from your private repository, configure a container service deployment with the following URI format in the image field:

```
111122223333.dkr.ecr.us-east-1.amazonaws.com/my-private-repo:{image tag}
```

You can manage your private repositories and images using the Amazon ECR console.

[Open the Amazon ECR console](#)

## 使用 AWS CLI 來管理私有存放庫的存取

使用 AWS Command Line Interface (AWS CLI) 管理 Lightsail 容器服務對 Amazon ECR 私有儲存庫的存取，需要執行下列步驟：

### Important

我們建議您使用 Lightsail 主控台來管理 Lightsail 容器服務對 Amazon ECR 私有儲存庫的存取，因為這樣可以簡化程序。如需詳細資訊，請參閱本指南前面的[使用 Lightsail 主控台來管理對私人存放庫的存取](#)。

1. 啟用或停用 Amazon ECR 映像拉拔器 IAM 角色 — 使用 Lightsail AWS CLI `update-container-service` 指令啟用或停用 Amazon ECR 映像拉拔器 IAM 角色。啟用 Amazon ECR 映像 puller IAM 角色之後，會為其建立一個主體 Amazon Resource Name (ARN)。如需詳細資訊，請參閱本指南的[啟用或停用 Amazon ECR 映像 puller IAM 角色](#)章節。
2. 判定 Amazon ECR 私有儲存庫是否具有政策陳述式 – 在啟用 Amazon ECR 映像 puller IAM 角色後，需要判定您想要容器服務存取的 Amazon ECR 私有儲存庫是否具有現有政策陳述式。如需詳細資訊，請參閱本指南後面所述的[判定 Amazon ECR 私有儲存庫是否具有政策陳述式](#)章節。

您可以使用以下方法之一將 IAM 角色主體 ARN 新增到儲存庫，具體方法取決於您的儲存庫是否具有現有政策陳述式：

- a. 將政策新增至沒有政策聲明的私有存放庫 — 使用 Amazon ECR AWS CLI `set-repository-policy` 命令將容器服務的 Amazon ECR 映像拉出器角色主體 ARN 新增至具有現有政策的私有存放庫。如需詳細資訊，請參閱本指南後述的[將政策新增至沒有政策陳述式的私有儲存庫](#)章節。
- b. 將政策新增至具有政策聲明的私有存放庫 — 使用 Amazon ECR AWS CLI `set-repository-policy` 命令將容器服務的 Amazon ECR 映像拉出器角色新增至沒有現有政策的私有存放庫。如需詳細資訊，請參閱本指南後述的[將政策新增至具有政策陳述式的私有儲存庫](#)章節。

## 啟用或停用 Amazon ECR 映像 puller IAM 角色

請完成下列程序，以啟用或停用 Lightsail 容器服務的 Amazon ECR 映像拉拔器 IAM 角色。您可以使用 Lightsail 的 AWS CLI `update-container-service` 命令來啟用或停用 Amazon ECR 映像拉拔器 IAM 角色。若要取得更多資訊，請參閱《指AWS CLI 令參考》[update-container-service](#) 中的。

### Note

您必須先安裝 AWS CLI 並針對 Lightsail 進行設定，然後才能繼續執行此程序。如需詳細資訊，請參閱[設定 AWS CLI 定使用 Lightsail](#)。

1. 開啟命令提示或終端機視窗。
2. 輸入以下命令，以更新容器服務並啟用或停用 Amazon ECR 映像 puller IAM 角色。

```
aws lightsail update-container-service --service-name ContainerServiceName --private-registry-access ecrImagePullerRole={isActive=RoleActivationState} --region AwsRegionCode
```

將命令中的以下範例文字取代為自訂文字：

- *ContainerServiceName*— 要為其啟用或停用 Amazon ECR 映像拉出器 IAM 角色的容器服務名稱。
- *RoleActivationState*— Amazon ECR 圖像拉拔器 IAM 角色的激活狀態。指定 `true` 即可啟用角色，指定 `false` 則可停用角色。
- *AwsRegionCode*— 容器服務的 AWS 區域 程式碼 (例如，`us-east-1`)。

範例：

- 啟用 Amazon ECR 映像 puller IAM 角色：

```
aws lightsail update-container-service --service-name my-container-service --private-registry-access ecrImagePullerRole={isActive=true} --region us-east-1
```

- 停用 Amazon ECR 映像 puller IAM 角色：

```
aws lightsail update-container-service --service-name my-container-service --private-registry-access ecrImagePullerRole={isActive=false} --region us-east-1
```

### 3. 如果您：

- 已啟用 Amazon ECR 映像 puller 角色 – 在獲得上一個回應後需要至少等待 30 秒。然後，繼續下一個步驟，取得容器服務的 Amazon ECR 映像 puller IAM 角色主體 ARN。
- 已停用 Amazon ECR 映像 puller 角色 – 如果之前已將 Amazon ECR 映像 puller IAM 角色主體 ARN 新增至 Amazon ECR 私有儲存庫的許可政策，則應從儲存庫中移除該許可政策。如需詳細資訊，請參閱《Amazon ECR 使用者指南》中的[刪除私有儲存庫政策陳述式](#)。

### 4. 輸入下列命令，以取得容器服務的 Amazon ECR 映像 puller IAM 角色主體 ARN。

```
aws lightsail get-container-services --service-name ContainerServiceName --  
region AwsRegionCode
```

將命令中的以下範例文字取代為自訂文字：

- *ContainerServiceName*— 要取得 Amazon ECR 映像拔出器 IAM 角色主體 ARN 的容器服務名稱。
- *AwsRegionCode*— 容器服務的 AWS 區域 程式碼 (例如，us-east-1)。

範例：

```
aws lightsail get-container-services --service-name my-container-service --  
region us-east-1
```

尋找回應中的 ECR 映像 puller IAM 角色主體 ARN。如果列出了某個角色，請複製該角色或將其寫下。本指南的下一節會用到該角色。接下來，需要判定您想要容器服務存取的 Amazon ECR 私有儲存庫上是否具有現有政策陳述式。繼續按本指南中的[判定 Amazon ECR 私有儲存庫是否具有政策陳述式](#)章節進行操作。

### 判定 Amazon ECR 私有儲存庫是否具有政策陳述式

使用以下程序來判定 Amazon ECR 私有儲存庫是否具有政策陳述式。您可以使用 Amazon ECR AWS CLI `get-repository-policy` 命令。若要取得更多資訊，請參閱《指 AWS CLI 令參考》[update-container-service](#) 中的。

**Note**

您必須先為 Amazon ECR 安裝 AWS CLI 並進行設定，然後才能繼續執行此程序。如需詳細資訊，請參閱《Amazon ECR 使用者指南》中的[設定 Amazon ECR](#)。

1. 開啟命令提示或終端機視窗。
2. 輸入下列命令，以取得特定私有儲存庫的政策陳述式。

```
aws ecr get-repository-policy --repository-name RepositoryName --
region AwsRegionCode
```

將命令中的以下範例文字取代為自訂文字：

- *RepositoryName*— 您要為其設定 Lightsail 容器服務存取權的私人存放庫名稱。
- *AwsRegionCode*— 私人存放庫的 AWS 區域 程式碼 (例如，us-east-1)。

範例：

```
aws ecr get-repository-policy --repository-name my-private-repo --region us-east-1
```

您應該會看到下列其中一個回應：

- `RepositoryPolicyNotFoundException`— 您的私人存放庫沒有政策聲明。如果您的儲存庫沒有政策陳述式，請遵循本指南後述的[將政策新增至沒有政策陳述式的私有儲存庫](#)章節中所述的步驟。

```
C:\>aws ecr get-repository-policy --repository-name my-private-repo

An error occurred (RepositoryPolicyNotFoundException) when calling the GetRepositoryPolicy operation: Repository policy does not exist for the repository with name 'my-private-repo' in the registry with id '12345678901'
```

- 找到儲存庫政策 - 您的私有儲存庫有一個政策陳述式，顯示在您的請求的回應中。如果您的儲存庫具有政策陳述式，請複製現有政策，然後遵循本指南後述的[將政策新增至具有政策陳述式的私有儲存庫](#)章節中所述的步驟。

```
C:\>aws ecr get-repository-policy --repository-name my-private-repo
{
  "registryId": "12345678901",
  "repositoryName": "my-private-repo",
  "policyText": "{\n  \"Version\": \"2012-10-17\", \n  \"Statement\": [ {\n    \"Sid\": \"AllowUserPushPull\", \n    \"Effect\": \"Allow\", \n    \"Principal\": {\n      \"AWS\": \"arn:aws:iam::12345678901:user/example-user\" \n    }, \n    \"Action\": [ \"ecr:BatchGetImage\", \"ecr:BatchCheckLayerAvailability\", \"ecr:CompleteLayerUpload\", \"ecr:GetDownloadUrlForLayer\", \"ecr:InitiateLayerUpload\", \"ecr:PutImage\", \"ecr:UploadLayerPart\" ] \n  } ] \n}"
```

## 將政策新增至沒有政策陳述式的私有儲存庫

完成下列程序，以將政策新增至沒有政策陳述式的 Amazon ECR 私有儲存庫。您新增的政策必須包含 Lightsail 容器服務的 Amazon ECR 映像拉出器 IAM 角色主體 ARN。這會授予您的容器服務存取權，從私有儲存庫部署映像。

### Important

當您使用 Lightsail 主控台設定存取權時，Lightsail 會自動將 Amazon ECR 映像拔模器角色新增至您的 Amazon ECR 私有儲存庫。在這種情況下，不必依本節中的步驟將 Amazon ECR 映像 puller 角色手動新增至私有儲存庫。如需詳細資訊，請參閱本指南前面的[使用 Lightsail 主控台來管理對私人存放庫的存取](#)。

可以使用 AWS CLI 將政策新增至私有儲存庫。可以透過建立包含政策的 JSON 檔案，然後使用 Amazon ECR 的 `set-repository-policy` 命令參考該檔案來執行此操作。若要取得更多資訊，請參閱《指 AWS CLI 令參考》[set-repository-policy](#) 中的。

### Note

您必須先為 Amazon ECR 安裝 AWS CLI 並進行設定，然後才能繼續執行此程序。如需詳細資訊，請參閱《Amazon ECR 使用者指南》中的[設定 Amazon ECR](#)。

1. 開啟文字編輯器，並將下列政策陳述式貼入新的文字檔案。

```
{
  "Version": "2008-10-17",
  "Statement": [
    {
      "Sid": "AllowLightsailPull-ecr-private-repo-demo",
      "Effect": "Allow",
      "Principal": {
        "AWS": "IamRolePrincipalArn"
      },
      "Action": [
        "ecr:BatchGetImage",
        "ecr:GetDownloadUrlForLayer"
      ]
    }
  ]
}
```

```
]
}
```

在文字中，請以本指南稍早取 *IamRolePrincipalArn* 得的容器服務的 Amazon ECR 影像拉出器 IAM 角色主體 ARN 取代。

2. 將檔案另存為 `ecr-policy.json` 並儲存在電腦上可存取的位置 (例如 Windows 上的 `C:\Temp\ecr-policy.json`，或 macOS 或 Linux 上的 `/tmp/ecr-policy.json`)。
3. 記下所建立的 `ecr-policy.json` 檔案的檔案路徑位置。此程序後續的命令中，會需要您指定路徑位置。
4. 開啟命令提示或終端機視窗。
5. 輸入下列命令，以設定您想要容器服務存取的私有儲存庫的政策陳述式。

```
aws ecr set-repository-policy --repository-name RepositoryName --policy-text
file://path/to/ecr-policy.json --region AwsRegionCode
```

將命令中的以下範例文字取代為自訂文字：

- *RepositoryName*— 您要新增原則之私人存放庫的名稱。
- *path/to/* – 您先前依本指南指示在電腦上建立的 `ecr-policy.json` 檔案路徑。
- *AwsRegionCode*— 私人存放庫的 AWS 區域 程式碼 (例如，`us-east-1`)。

範例：

- 在 Windows 上：

```
aws ecr set-repository-policy --repository-name my-private-repo --policy-text
file://C:\Temp\ecr-policy.json --region us-east-1
```

- 在 macOS 或 Linux 上：

```
aws ecr set-repository-policy --repository-name my-private-repo --policy-text
file:///tmp/ecr-policy.json --region us-east-1
```

您的容器服務現在可以存取私有儲存庫及其映像。若要使用儲存庫中的映像，請將以下 URI 指定為容器服務部署的 Image (映像) 值。在 URI 中，請將範例 `##` 取代為您要部署的映像標籤。如需詳細資訊，請參閱 [建立和管理容器服務部署](#)。

```
AwsAccountId.dkr.ecr.AwsRegionCode.amazonaws.com/RepositoryName:ImageTag
```

將 URI 中的以下範例文字取代為自訂文字：

- *AwsAccountId*— 您的 AWS 帳戶 ID 號碼。
- *AwsRegionCode*— 私人存放庫的 AWS 區域 程式碼 (例如, us-east-1)。
- *RepositoryName*— 要從中部署容器映像的私人存放庫名稱。
- *ImageTag*— 要部署在容器服務上的私有存放庫中的容器映像的標籤。

範例：

```
111122223333.dkr.ecr.us-east-1.amazonaws.com/my-private-repo:myappimage
```

將政策新增至具有政策陳述式的私有儲存庫

完成下列程序，將政策新增至具有政策陳述式的 Amazon ECR 私有儲存庫。您新增的政策必須包含現有政策和包含 Lightsail 容器服務之 Amazon ECR 映像拔出器 IAM 角色主體 ARN 的新政策。這會維護私有儲存庫上的現有許可，同時也會授予容器服務存取權，以從私有儲存庫部署映像。

#### Important

當您使用 Lightsail 主控台設定存取權時，Lightsail 會自動將 Amazon ECR 映像拔模器角色新增至您的 Amazon ECR 私有儲存庫。在這種情況下，不必依本節中的步驟將 Amazon ECR 映像 puller 角色手動新增至私有儲存庫。如需詳細資訊，請參閱本指南前面的[使用 Lightsail 主控台來管理對私人存放庫的存取](#)。

可以使用 AWS CLI 將政策新增至私有儲存庫。您可以透過建立包含現有政策和新政策的 JSON 檔案來執行此操作。然後，使用 Amazon ECR 的 `set-repository-policy` 命令來參考該檔案。若要取得更多資訊，請參閱《指 AWS CLI 令參考》[set-repository-policy](#) 中的。

#### Note

您必須先為 Amazon ECR 安裝 AWS CLI 並進行設定，然後才能繼續執行此程序。如需詳細資訊，請參閱《Amazon ECR 使用者指南》中的[設定 Amazon ECR](#)。

1. 開啟命令提示或終端機視窗。
2. 輸入下列命令，以取得特定私有儲存庫的政策陳述式。

```
aws ecr get-repository-policy --repository-name RepositoryName --
region AwsRegionCode
```

將命令中的以下範例文字取代為自訂文字：

- *RepositoryName*— 您要為其設定 Lightsail 容器服務存取權的私人存放庫名稱。
- *AwsRegionCode*— 私人存放庫的 AWS 區域 程式碼 (例如，us-east-1)。

範例：

```
aws ecr get-repository-policy --repository-name my-private-repo --region us-east-1
```

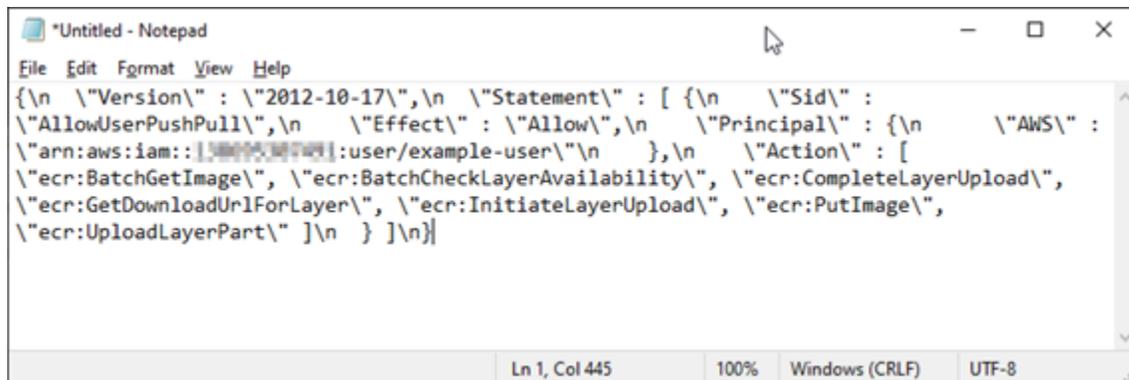
3. 請複製回應中的現有政策並繼續下一個步驟。

您應該僅複製出現在雙引號之間的 `policyText` 內容，也就是以下範例中反白顯示的內容。

```
C:\>aws ecr get-repository-policy --repository-name my-private-repo
{
  "registryId": "lightsail-ecr",
  "repositoryName": "my-private-repo",
  "policyText": "{\n  \"Version\" : \"2012-10-17\",\n  \"Statement\" : [ {\n    \"Sid\" : \"AllowUserPushPull\",\n    \"Effect\" : \"Allow\",\n    \"Principal\" : {\n      \"AWS\" : \"arn:aws:iam::123456789012:user/example-user\"\n    },\n    \"Action\" : [ \"ecr:BatchGetImage\", \"ecr:BatchCheckLayerAvailability\", \"ecr:CompleteLayerUpload\", \"ecr:GetDownloadUrlForLayer\", \"ecr:InitiateLayerUpload\", \"ecr:PutImage\", \"ecr:UploadLayerPart\" ]\n  } ]\n}"
```

4. 開啟文字編輯器，並貼上您在先前步驟中複製的私有儲存庫現有政策。

結果應如下列範例所示。



```
File Edit Format View Help
{\n  \"Version\" : \"2012-10-17\",\n  \"Statement\" : [ {\n    \"Sid\" :
\"AllowUserPushPull\",\n    \"Effect\" : \"Allow\",\n    \"Principal\" : {\n      \"AWS\" :
\"arn:aws:iam::123456789012:user/example-user\"\n    },\n    \"Action\" : [
\"ecr:BatchGetImage\", \"ecr:BatchCheckLayerAvailability\", \"ecr:CompleteLayerUpload\",
\"ecr:GetDownloadUrlForLayer\", \"ecr:InitiateLayerUpload\", \"ecr:PutImage\",
\"ecr:UploadLayerPart\" ]\n  } ]\n}
```

5. 在貼上的文字中，將 `\n` 取代為分行符號，然後刪除剩餘的 `\`。

結果應如下列範例所示。



```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowPushPull",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::123456789012:user/example-user"
        ]
      },
      "Action": [
        "ecr:BatchGetImage",
        "ecr:BatchCheckLayerAvailability",
        "ecr:CompleteLayerUpload",
        "ecr:GetDownloadUrlForLayer",
        "ecr:InitiateLayerUpload",
        "ecr:PutImage",
        "ecr:UploadLayerPart"
      ]
    }
  ]
}

```

6. 在文字檔案的結尾貼上下列政策陳述式。

```

/
{
  "Version": "2008-10-17",
  "Statement": [
    {
      "Sid": "AllowLightsailPull-ecr-private-repo-demo",
      "Effect": "Allow",
      "Principal": {
        "AWS": "IamRolePrincipalArn"
      },
      "Action": [
        "ecr:BatchGetImage",
        "ecr:GetDownloadUrlForLayer"
      ]
    }
  ]
}

```

- 在文字中，請以本指南稍早取 `IamRolePrincipalArn` 得的容器服務的 Amazon ECR 影像拉出器 IAM 角色主體 ARN 取代。

結果應如下列範例所示。



```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowPushPull",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::111111111111:user/example-user"
        ]
      },
      "Action": [
        "ecr:BatchGetImage",
        "ecr:BatchCheckLayerAvailability",
        "ecr:CompleteLayerUpload",
        "ecr:GetDownloadUrlForLayer",
        "ecr:InitiateLayerUpload",
        "ecr:PutImage",
        "ecr:UploadLayerPart"
      ]
    }
  ]
},
{
  "Version": "2008-10-17",
  "Statement": [
    {
      "Sid": "AllowLightsailPull-ecr-private-repo-demo",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::4211674488915:role/amazon/lightsail/us-east-a/containers/my-container-service/private-repo-access/3EXAMPLEm8gmrcs1vEXAMPLEkkemufe7ime26fo9i7e5ct93k7ng"
      },
      "Action": [
        "ecr:BatchGetImage",
        "ecr:GetDownloadUrlForLayer"
      ]
    }
  ]
}

```

- 將檔案另存為 `ecr-policy.json` 並儲存在電腦上可存取的位置 (例如 Windows 上的 `C:\Temp\ecr-policy.json`，或 macOS 或 Linux 上的 `/tmp/ecr-policy.json`)。
- 記下 `ecr-policy.json` 檔案的檔案路徑位置。此程序後續的命令中，會需要您指定路徑位置。
- 開啟命令提示或終端機視窗。
- 輸入下列命令，以設定您想要容器服務存取的私有儲存庫的政策陳述式。

```
aws ecr set-repository-policy --repository-name RepositoryName --policy-text
file://path/to/ecr-policy.json --region AwsRegionCode
```

將命令中的以下範例文字取代為自訂文字：

- *RepositoryName*— 您要新增原則之私人存放庫的名稱。
- *path/to/*— 您先前依本指南指示在電腦上建立的 `ecr-policy.json` 檔案路徑。
- *AwsRegionCode*— 私人存放庫的 AWS 區域 程式碼 (例如 , `us-east-1`)。

範例：

- 在 Windows 上：

```
aws ecr set-repository-policy --repository-name my-private-repo --policy-text
file:///C:\Temp\ecr-policy.json --region us-east-1
```

- 在 macOS 或 Linux 上：

```
aws ecr set-repository-policy --repository-name my-private-repo --policy-text
file:///tmp/ecr-policy.json --region us-east-1
```

您應該會看到類似於以下範例的回應。

```
C:\>aws ecr set-repository-policy --repository-name my-private-repo --policy-text file:///C:\Temp\ecr-policy.json --region
us-west-2
{
  "registryId": "123456789012",
  "repositoryName": "my-private-repo",
  "policyText": "{\n  \"Version\" : \"2012-10-17\",\n  \"Statement\" : [ {\n    \"Sid\" : \"AllowLightsailPull-my-cont
ainer-service\",\n    \"Effect\" : \"Allow\",\n    \"Principal\" : {\n      \"AWS\" : \"arn:aws:iam::123456789012:role/a
mazon/lightsail/us-west-2/containers/my-container-service/private-repo-access/iam-policy-for-ecr-access\"\n    },\n    \"Action\" : [ \"ecr:BatchGetImage\", \"ecr:GetDownloadUrlForLayer\" ]\n  }, {\n    \"Sid\" :
\"AllowUserPushPull\",\n    \"Effect\" : \"Allow\",\n    \"Principal\" : {\n      \"AWS\" : \"arn:aws:iam::123456789012:role/
user/example-user\"\n    },\n    \"Action\" : [ \"ecr:BatchCheckLayerAvailability\", \"ecr:BatchGetImage\", \"ecr:Comple
teLayerUpload\", \"ecr:GetDownloadUrlForLayer\", \"ecr:InitiateLayerUpload\", \"ecr:PutImage\", \"ecr:UploadLayerPart\"
 ]\n  } ]\n}"
```

如果再次執行 `get-repository-policy` 命令，您應該會在私有儲存庫上看到新的附加政策陳述式。您的容器服務現在可以存取私有儲存庫及其映像。若要使用儲存庫中的映像，請將以下 URI 指定為容器服務部署的 Image (映像) 值。在 URI 中，請將範例 `##` 取代為您要部署的映像標籤。如需詳細資訊，請參閱 [建立和管理容器服務部署](#)。

```
AwsAccountId.dkr.ecr.AwsRegionCode.amazonaws.com/RepositoryName:ImageTag
```

將 URI 中的以下範例文字取代為自訂文字：

- *AwsAccountId*— 您的 AWS 帳戶 ID 號碼。
- *AwsRegionCode*— 私人存放庫的 AWS 區域 程式碼 (例如 , us-east-1)。
- *RepositoryName*— 要從中部署容器映像的私人存放庫名稱。
- *ImageTag*— 要部署在容器服務上的私有存放庫中的容器映像的標籤。

範例：

```
111122223333.dkr.ecr.us-east-1.amazonaws.com/my-private-repo:myappimage
```

## 在 Lightsail 中建立和管理容器服務部署

當您準備好在 Amazon Lightsail 容器服務上啟動容器時，請建立部署。部署是您希望在服務上啟動之容器的一組規格。容器服務一次可以有一個執行中的部署，而部署最多可有 10 個容器項目。您可以在建立容器服務的同時建立部署，也可在服務開始運作後建立部署。

### Note

如果您建立新的部署，則容器服務的現有使用率指標將會消失，並且只顯示目前新部署的指標。

如需有關容器服務的詳細資訊，請參閱 [Amazon Lightsail 中的容器服務](#)。

### 內容

- [先決條件](#)
- [部署參數](#)
  - [容器項目參數](#)
  - [公有端點參數](#)
- [容器之間的通訊](#)

- [容器日誌](#)
- [部署版本](#)
- [部署狀態](#)
- [部署失敗](#)
- [檢視目前的容器服務部署](#)
- [建立或修改容器服務部署](#)

## 必要條件

開始在容器服務中建立部署之前，請完成以下事前準備：

- 在 Lightsail 帳戶中建立容器服務。如需詳細資訊，請參閱[建立 Amazon Lightsail 容器服務](#)。
- 找出您在容器服務上啟動容器時要使用的容器映像。
  - 在公有登錄檔 (例如 Amazon ECR Public Gallery) 上尋找容器映像。如需詳細資訊，請參閱《Amazon ECR Public 使用者指南》中的 [Amazon ECR Public Gallery](#)。
  - 在本機電腦上建立容器映像，然後將其推送到 Lightsail 容器服務。如需詳細資訊，請參閱下列指南：
    - [安裝軟體以管理您的 Amazon Lightsail 容器服務的容器映像檔](#)
    - [建立容器服務映像](#)
    - [推送和管理容器映像](#)

## 部署參數

本節說明您可以為部署的容器項目和公有端點指定的參數。

### 容器項目參數

您可以在部署中新增最多 10 個容器項目。您可以為每個容器項目指定下列參數：

**Container name**  
Container names must contain only alphanumeric characters and hyphens. A hyphen (-) can separate words but cannot be at the start or end of the name.

**Image**  
Enter the image reference from a public registry, such as DockerHub.

**Configuration**  
Optionally specify a command, the environment variables, and the ports to open on your container.

Launch command:

**Environment variables**

Key	Value (optional)
<input type="text"/>	<input type="text"/> <span style="color: red;">✕</span>

+ Add variable

**Open ports**  
Your application code for this container must listen to a port specified here.

Port	Protocol
<input type="text"/>	HTTP <span style="color: red;">✕</span>

+ Add port

- Container name (容器名稱) – 輸入容器的名稱。部署中所有容器的名稱不得重複，並且只能包含英數字元和連字號。連字號可以分隔單字，但不能位於名稱的頭尾。
- Source image (來源映像) – 指定容器的來源容器映像。您可以指定下列來源的容器映像：
  - 公有登錄檔 (例如 Amazon ECR Public Gallery) 或一些其他公有容器映像登錄檔。

如需有關 Amazon ECR Public 的詳細資訊，請參閱《Amazon ECR Public 使用者指南》中的[什麼是 Amazon Elastic Container Registry Public？](#)。

- 已從本機電腦將映像推送到容器服務。若要指定存放的映像，請選擇選擇存放的映像，然後選取要使用的映像。

如果在本機電腦上建立容器映像，則可將其推送到容器服務，以便在建立部署時使用。如需詳細資訊，請參閱為[Amazon Lightsail 容器服務建立容器映像](#)以及[推送和管理 Amazon Lightsail 容器服務上的容器映像](#)。

- Launch command (啟動命令) – 指定啟動命令以執行在建立容器時設定容器的 Shell 指令碼或 Bash 指令碼。啟動命令可以執行多項動作，例如新增軟體、更新軟體，或以某種其他方式設定容器。

- Environment variables (環境變數) – 指定環境變數。這些變數是索引鍵值參數，可提供由容器執行的應用程式或指令碼的動態組態。
- Open ports (開啟連接埠) – 指定要在容器上開啟的連接埠和通訊協定。您可以指定透過 HTTP、HTTPS、TCP 和 UDP 開啟任何連接埠。您必須為您打算用作容器服務公有端點的容器開啟 HTTP 或 HTTPS 連接埠。如需詳細資訊，請參閱本指南以下章節。

## 公有端點參數

您可以在部署中指定容器項目，作為容器服務的公有端點。公有端點容器上的應用程式可透過隨機產生的容器服務預設網域，在網際網路上公開存取。預設網域的格式為 `https://<ServiceName>.<RandomGUID>.<AWSRegion>.cs.amazonlightsail.com`，其中 `<ServiceName>` 是容器服務的名稱，`<RandomGUID>` 是您 Lightsail 帳戶在 AWS 區域中隨機產生的容器服務全域唯一識別碼，而 `<AWSRegion>` 是建立容器服務的 AWS 區域。Lightsail 容器服務的公用端點僅支援 HTTPS，而且不支援 TCP 或 UDP 流量。一項服務只能以一個容器為公有端點。因此，請務必選擇託管應用程式前端的容器作為公有端點，而其他容器則在內部存取。

### Note

您可以對容器服務使用自己的自訂網域名稱。如需詳細資訊，請參閱 [啟用和管理 Amazon Lightsail 容器服務的自訂網域](#)。

您可以為部署和容器服務的公有端點指定下列參數：

**PUBLIC ENDPOINT**  
Choose a container in your deployment that you want to make available to the internet as a public endpoint. Make sure to open an HTTP or HTTPS port on the selected container configuration, and then choose it as the port of your public endpoint.

**i** The container you choose as your public endpoint must respond to traffic on the specified port.

nginx

Port  
80

Health check path  
/

- Endpoint container (端點容器) – 選取部署中將作為容器服務公有端點之容器的名稱。下拉式選單只會列出在部署中開啟 HTTP 或 HTTPS 連接埠的容器。

- Port (連接埠) – 選取要用於公有端點的 HTTP 或 HTTPS 連接埠。下拉式選單只會列出在所選容器上開啟的 HTTP 和 HTTPS 連接埠。如果所選容器未設定為在初次啟動時支援 HTTPS 連線，請選取 HTTP 連接埠。

#### Note

即使您將 HTTP 連接埠選為公有端點連接埠，容器服務的預設網域也會預設使用 HTTPS。原因在於容器服務的負載平衡器雖預設為 HTTPS，但又是使用 HTTP 與容器建立連線。容器服務的負載平衡器是以 HTTP 連接至容器，但會使用 HTTPS 來提供內容給使用者。

- Health check path (運作狀態檢查路徑) – 在所選的公有端點容器上指定路徑，容器服務的負載平衡器會定期檢查路徑是否正常運作。
- Advanced health check settings (進階運作狀態檢查設定) - 您可以為選取的公用端點容器設定下列運作狀態檢查設定：
  - Health check timeout seconds (運作狀態檢查逾時的秒數) - 等待運作狀態檢查回應的時間，以秒為單位。如果在這段時間內沒有收到任何回應，運作狀態檢查就會失敗。可以指定 2–60 秒。
  - Health check interval seconds (運作狀態檢查間隔秒) - 容器運作狀態檢查之間的約略間隔，以秒為單位。可以指定 5–300 秒。
  - Health check success codes (運作狀態檢查成功代碼) - 檢查來自容器的成功回應時所使用的 HTTP 碼。您可以指定介於 200 到 499 之間的值。可以指定多個值 (例如，200、202) 或值範圍 (例如，200–299)。
  - Health check healthy threshold (運作狀態檢查狀況良好閾值) - 將容器移至正常狀態所需要的連續運作狀態檢查成功次數。
  - Health check unhealthy threshold (運作狀態檢查狀況不良閾值) - 將容器移至狀況不良狀態所需要的連續運作狀態檢查失敗次數。

## 私有網域

所有容器服務也都有格式化為的私有網域 `<ServiceName>.service.local`，其中 `<ServiceName>` 是容器服務的名稱。使用私有網域，以從與您的服務相同 AWS 區域的另一個 Lightsail 資源存取容器服務。如果您未在服務的部署中指定公有端點，則私有網域是存取容器服務的唯一方法。即使您未指定公有端點，系統仍會為容器服務產生預設網域，但在您嘗試瀏覽時會顯示 404 No Such Service 錯誤訊息。

若要使用容器服務的私有網域來存取特定容器，則必須指定容器的開放連接埠，以接受您的連線請求。您可以將要求的網域格式化為 `<ServiceName>.service.local:<PortNumber>`，

其中 `< ServiceName >` 是容器服務的名稱，而 `< PortNumber >` 是您想要連線到的容器的開放連接埠來執行此操作。例如，如果在名為 `container-service-1` 的容器服務上建立部署，並指定連接埠 6379 開啟的 Redis 容器，則請求的網域格式應該為 `container-service-1.service.local:6379`。

## 容器之間的通訊

使用環境變數，您可以開啟同一容器服務中的容器、不同容器服務中的容器之間或者容器與其他資源之間 (例如，容器和受管資料庫之間) 的通訊。

要在同一容器服務中開啟容器之間的通訊，請向引用 `localhost` 的容器部署新增一個環境變數，如下列範例所示。

Environment variables	
Key	Value (optional)
SERVICE_CON	service://localhost

要在不同容器服務中的容器之間開啟通訊，請將引用私有域的環境變量新增到容器部署中 (例如 `container-service-1.service.local`)，如下列範例所示。

Environment variables	
Key	Value (optional)
SERVICE_CON	service://container-service-1.service.local

要開啟容器和其他資源之間的通訊，請向容器部署中新增引用資源的公有端點 URL 的環境變數。例如，Lightsail 受管理資料庫的公用端點通常 `ls-123abc.czoexamplezqi.us-west-2.rds.amazonaws.com` 為。因此，您應按如下範例所示在環境變數中引用它。

Environment variables	
Key	Value (optional)
WORDPRESS_	ls-123abc.czoexamplezqi.us-west-2.rds.amazon

## 容器日誌

部署中每個容器都會產生日誌。容器日誌會提供在容器中執行的 `stdout` 和 `stderr` 程序串流。請定期存取容器日誌以診斷其操作。如需詳細資訊，請參閱[檢視 Amazon Lightsail 容器服務的容器日誌](#)。

## 部署版本

您在容器服務中建立的每個部署都會儲存為部署版本。如果修改現有部署的參數，容器會重新部署至服務，而經修改的部署會產生新部署版本。每個容器服務的最新 50 個部署版本會儲存下來。您可以使用 50 個部署版本之中任一個，在相同的容器服務中建立新部署。如需詳細資訊，請參閱[檢視和管理 Amazon Lightsail 容器服務的部署版本](#)。

## 部署狀態

部署在建立後可處於下列任一種狀態：

- Activating (啟動中) – 部署處於啟動中狀態，並且正在建立容器。
- Active (作用中) – 部署已建立成功，目前正在容器服務上執行。
- Inactive (非作用中) – 先前成功建立的部署不再在容器上執行。
- Failed (失敗) – 部署中指定的一或多個容器無法啟動，以致部署失敗。

## 部署失敗

如果部署中一或多個容器無法啟動，則部署就會失敗。如果部署失敗，而且容器服務上有先前的部署正在執行，則容器服務會將先前的部署保留為作用中的部署。如果不存在先前的部署，則容器服務會停在就緒狀態，無任何目前作用中的部署。

請檢視失敗部署的容器日誌，以診斷和排除問題。如需詳細資訊，請參閱[檢視 Amazon Lightsail 容器服務的容器日誌](#)。

## 檢視目前的容器服務部署

完成下列程序來檢視 Lightsail 容器服務上目前的部署。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁，選擇 Containers (容器) 索引標籤。
3. 選擇您要檢視目前部署之容器服務的名稱。
4. 在容器服務管理頁面上，選擇 Deployments (部署) 索引標籤。

Deployments (部署) 頁面會列出目前的部署和部署版本。如果您尚未在容器服務中建立部署，則該頁面的兩個區段皆為空白。

## 建立或修改容器服務部署

請完成下列程序，以在 Lightsail 容器服務上建立或修改部署。無論是建立新部署或修改現有部署，容器服務都會將每個部署儲存為新的部署版本。如需詳細資訊，請參閱[檢視和管理 Amazon Lightsail 容器服務的部署版本](#)。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁，選擇 Containers (容器) 索引標籤。
3. 選擇您要建立或修改容器服務部署之容器服務的名稱。
4. 在容器服務管理頁面上，選擇 Deployments (部署) 索引標籤。

Deployments (部署) 頁面會列出目前的部署和部署版本 (如果有)。

5. 請選擇下列其中一個選項：
  - 若容器服務具有現有的部署，則選擇 Modify your deployment (修改部署)。
  - 若容器服務尚未具有部署，則選擇 Create a deployment (建立部署)。

部署表單隨即開啟，您可以在上面編輯現有的部署參數，或輸入新的部署參數。

**Create your first deployment**

*Saving this deployment will create a new deployment version*

**CONTAINERS**

**Container name**  
Container names must contain only alphanumeric characters and hyphens. A hyphen (-) can separate words but cannot be at the start or end of the name.

container-name

**Image**  
Enter the image reference from a public registry, such as DockerHub.

imagename:latest or registry.hub.docker.com/library/imagename:latest

**Configuration**  
Optionally specify a command, the environment variables, and the ports to open on your container.

Launch command: launch.sh

+ Add environment variables  
+ Add open ports

+ Add container entry

*You can have up to 10 containers in a deployment*

**PUBLIC ENDPOINT**  
You must specify container names for the container entries in your deployment to be able to select a container as the public endpoint of your deployment.

*The container you choose as your public endpoint must respond to traffic on the specified port.*

Select container...

Cancel Save and deploy

6. 輸入部署的參數。如需有關可指定之部署參數的詳細資訊，請參閱本指南前面的[部署參數](#)一節。
7. 選擇 Add container entry (新增容器項目)，以將多個容器項目新增至部署。部署可有最多 10 個容器項目。
8. 選擇部署中的容器項目，作為容器服務的公有端點。這包括指定 HTTP 或 HTTPS 連接埠、所選容器項目上的運作狀態檢查路徑，以及進階運作狀態檢查設定。如需詳細資訊，請參閱本指南前述的[公有端點參數](#)。
9. 部署參數輸入完畢時，請選擇 Save and deploy (儲存和部署)，以在容器服務上建立部署。

部署正在建立時，容器服務狀態會變更為 Deploying (部署中)。幾分鐘之後，容器服務狀態會根據部署狀態變更為下列其中一種狀態：

- 如果部署成功，容器服務狀態會變更為 Running (執行中)，而部署狀態會變更為 Active (作用中)。如果您已在部署中設定公有端點，則可透過容器服務預設網域使用選為公有端點的容器。
- 如果部署失敗，而且容器服務上有先前的部署正在執行，則容器服務狀態會變更為 Running (執行中)，容器服務會將先前的部署保留為作用中的部署。如果不存在先前的部署，則容器服務狀態會變更為 Ready (就緒)，且無任何目前作用中的部署。請檢視失敗部署的容器日誌，以診斷和排除問題。如需詳細資訊，請參閱檢視 Amazon Lightsail 容器服務的容器日誌。

## 主題

- [為您的集裝箱服務擴充容量](#)
- [檢視及管理 Lightsail 容器服務部署版本](#)
- [分析 Lightsail 服務日誌](#)

## 為您的集裝箱服務擴充容量

Amazon Lightsail 容器服務的容量由其規模和功能組成。規模指定容器服務中的運算節點數目，而動力指定服務中每個節點的記憶體和 vCPU。您可以根據要為服務提供動力的節點數來挑選規模，以獲得最佳的可用性和更高容量。

遵循本指南中的程序，如果您發現容器服務佈建不足，則可隨時動態增加容器服務的動力和規模，而不需要停機；如果發現容器服務過度佈建，則可予以減少。Lightsail 會隨著您目前的部署自動管理容量變更。

### Note

如果您建立新的部署，則容器服務的現有使用率指標將會消失，並且只顯示目前新部署的指標。

如需有關容器服務的詳細資訊，請參閱[容器服務](#)。

## 變更 容器服務的容量

請完成下列程序以變更 Lightsail 貨櫃服務的容量。

1. 登入主 [Lightsail 控制台](#)。
2. 在 Lightsail 首頁，選擇 Containers (容器) 索引標籤。
3. 選擇您要變更容量之容器服務的名稱。
4. 在容器服務管理頁面上，選擇 Capacity (容量) 索引標籤。

容器服務的目前動力、規模和每月價格會顯示在 Capacity (容量) 頁面中。

5. 選擇 Change capacity (變更容量) 來變更動力和規模。
6. 在顯示的確認提示上，請選擇 Yes, continue (是，繼續)，確認變更容器服務的容量會重新部署目前的部署。
7. 選擇容器服務的新動力和規模。
8. 選擇 Yes, apply (是，套用) 以將新容量套用至您的容器服務。

容器服務的狀態會變更為 Updating (正在更新)。在一段時間之後，服務的狀態會變更為 Enabled (已啟用)，並開始在其新容量下運作。

## 檢視及管理 Lightsail 容器服務部署版本

在 Amazon Lightsail 容器服務中建立的每個部署都會儲存為部署版本。如果修改現有部署的參數，容器會重新部署至服務，而經修改的部署會產生新部署版本。每個容器服務的最新 50 個部署版本會儲存下來。您可使用 50 個部署版本之中任一個，在相同的容器服務中建立新部署。在本指南中，我們會為您介紹如何檢視和管理容器服務的部署版本。

如需有關容器服務的詳細資訊，請參閱[容器服務](#)。

### 部署版本狀態

每個部署版本建立後可為下列任一狀態：

- 部署中 (啟動中) – 正在啟動部署。
- Active (作用中) – 部署已建立成功，目前正在容器服務上執行。容器服務一次僅能有一個部署處於作用中狀態。
- Inactive (非作用中) – 先前成功建立的部署不再在容器上執行。
- Failed (失敗) – 部署中指定的一或多個容器無法啟動，以致部署失敗。

## 必要條件

開始之前，您需要建立 Lightsail 容器服務。如需詳細資訊，請參閱[建立容器服務](#)。

您亦應在容器服務中建立部署，以設定和啟動容器。如需詳細資訊，請參閱[建立和管理 Amazon Lightsail 容器服務的部署](#)。

## 檢視容器服務的部署版本

請完成下列程序來檢視 Lightsail 容器服務的部署版本。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁，選擇 Containers (容器) 索引標籤。
3. 選擇您要檢視部署版本之容器服務的名稱。
4. 在容器服務管理頁面上，選擇 Deployments (部署) 索引標籤。

Deployments (部署) 頁面會列出目前的部署和部署版本 (如果有)。

5. 容器服務部署版本列於該頁面的 Deployment versions (部署版本) 區段。

每個部署皆有建立日期、狀態和動作選單。

6. 透過部署版本的動作選單，選擇下列其中一個選項：
  - Create new deployment (建立新部署) – 選擇此項以從所選部署版本建立新部署。如需有關建立部署的詳細資訊，請參閱[建立或修改容器服務部署](#)。

### Note

若選擇從 Failed (失敗) 狀態的版本建立新部署，則必須在建立部署前更正失敗原因。否則，部署可能再次失敗。

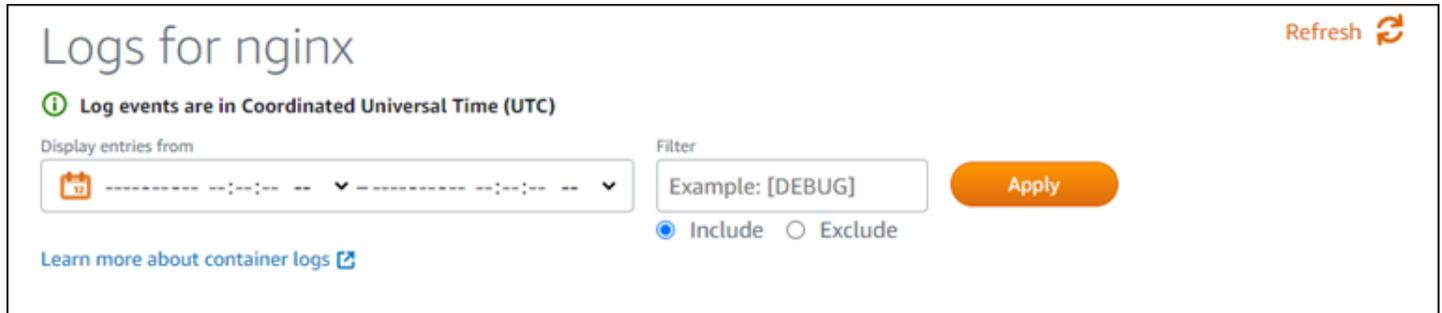
- View details (檢視詳細資訊) – 選擇此選項以檢視所選部署版本的容器項目和公有端點參數。您亦可檢視部署的容器日誌，以防您需要診斷失敗的部署。如需詳細資訊，請參閱[檢視容器服務日誌](#)。

## 分析 Lightsail 服務日誌

Amazon Lightsail 容器服務部署中的每個容器都會產生一個日誌。容器日誌會提供在容器中執行的 stdout 和 stderr 程序串流。請定期存取容器日誌以診斷其操作。系統會儲存最近三天的日誌項目，之後最舊的日誌項目即會被最新的項目取代。

## 篩選容器日誌

容器日誌每天可以有數百個項目。使用篩選選項可減少日誌視窗中顯示的項目數量，並讓您更容易找到要尋找的項目。您可以依開始和結束日期 (本地時間) 以及特定字詞來篩選容器日誌。依字詞篩選時，您可以選擇包含或排除指定字詞的日誌項目。



include (包含) 或 exclude (排除) 篩選條件會尋找區分大小寫的完全相符項目。例如，如果您指定僅包含訊息中具有 HTTP 的日誌事件，則您將看到訊息中包含 HTTP 的所有日誌事件，但沒有訊息中包含 http 的日誌事件。如果您指定要排除 Error，則您將看到訊息中不包含 Error 的所有日誌事件，而且也會看到訊息中包含 ERROR 的日誌事件。

### 必要條件

開始之前，您需要建立 Lightsail 容器服務。如需詳細資訊，請參閱[建立 Amazon Lightsail 容器服務](#)。

您亦應在容器服務中建立部署，以設定和啟動容器。如需詳細資訊，請參閱[建立和管理 Amazon Lightsail 容器服務的部署](#)。

### 檢視容器日誌

請完成下列程序，以檢視 Lightsail 容器服務的容器日誌。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁，選擇 Containers (容器) 索引標籤。
3. 選擇您要檢視容器日誌之容器服務的名稱。
4. 在容器服務管理頁面上，選擇 Deployments (部署) 索引標籤。

Deployments (部署) 頁面會列出目前的部署和部署版本 (如果有)。

5. 選擇下列其中一個選項來檢視容器日誌：

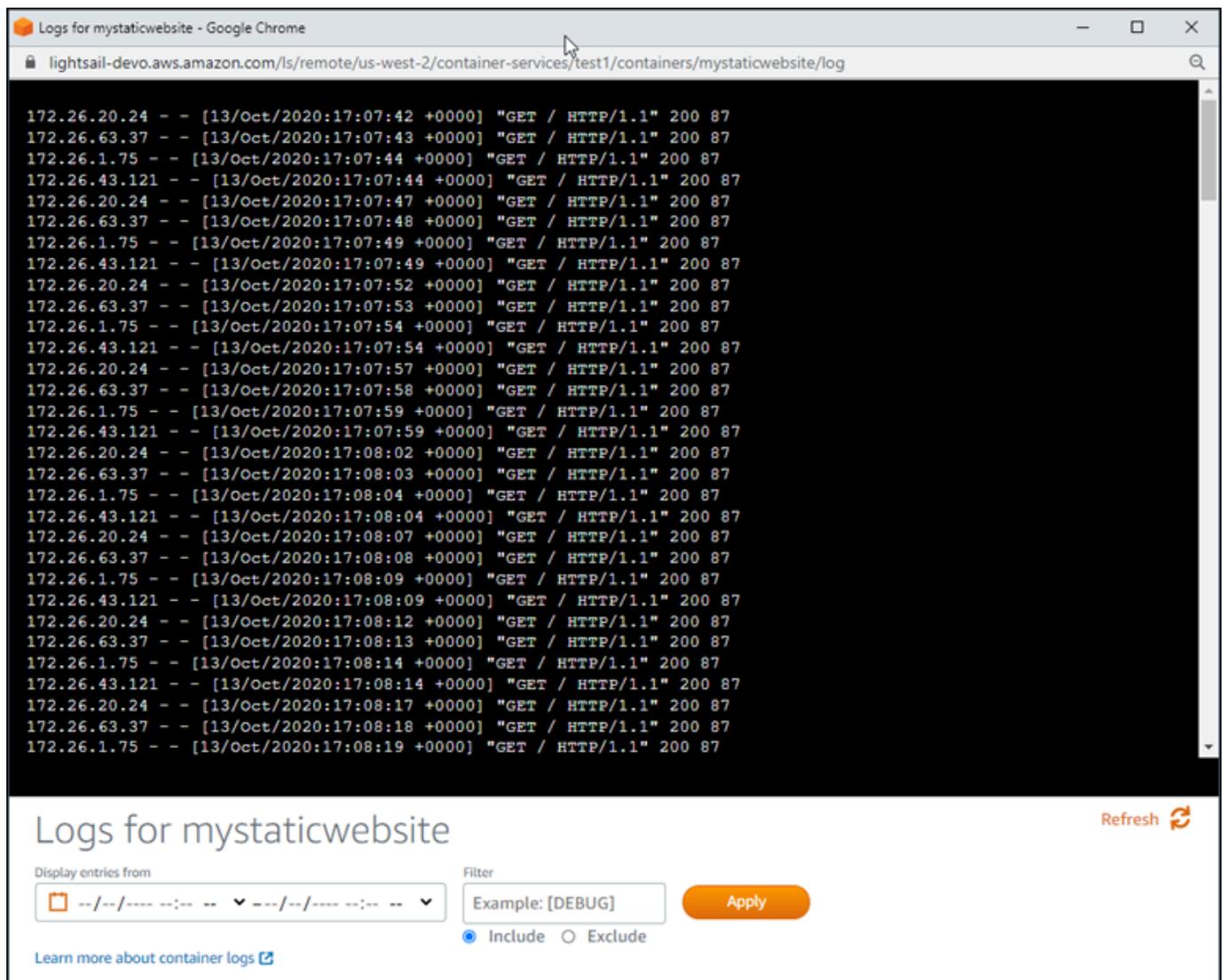
- 若要存取目前部署的容器日誌，請針對容器項目選擇頁面的 Current deployment (目前的部署) 區段下的 Open log (開啟日誌)。

- 若要存取先前部署的容器日誌，請在頁面的 Deployment versions (部署版本) 區段下針對先前部署選擇動作選單圖示 (:)，然後選擇 Show details (顯示詳細資訊)。在出現的 Version details (版本詳細資訊) 頁面中，為列出的容器項目選擇 Open log (開啟日誌)。

容器日誌會在新的瀏覽器視窗中開啟。您可以向下捲動以檢視更多的日誌項目，並重新整理頁面以載入最新的項目集合。篩選選項會顯示在頁面底部。

### Note

日誌項目會以遞增順序顯示，並以國際標準時間 (UTC) 為準。也就是說，最舊的日誌項目位於頂端，您必須向下捲動才能查看較新的日誌項目。



The screenshot shows a Google Chrome browser window titled "Logs for mystaticwebsite - Google Chrome". The address bar displays the URL: `lightsail-dev0.aws.amazon.com/ls/remote/us-west-2/container-services/test1/containers/mystaticwebsite/log`. The main content area is a dark-themed log viewer displaying a list of log entries. Each entry follows the format: `IP - - [timestamp] "method / HTTP/1.1" status code`. The logs show a series of "GET / HTTP/1.1" requests with a status code of 200, originating from various IP addresses like 172.26.20.24, 172.26.63.37, and 172.26.1.75. Below the log list, there is a control panel with the title "Logs for mystaticwebsite" and a "Refresh" button. The control panel includes a "Display entries from" dropdown menu, a "Filter" input field containing "Example: [DEBUG]", and an "Apply" button. There are also radio buttons for "Include" (selected) and "Exclude". A link "Learn more about container logs" is located at the bottom left of the control panel.

# 使用 Lightsail 中的自訂網域啟用安全的網頁存取

啟用 Amazon Lightsail 容器服務的自訂網域，以在您的服務中使用已註冊網域名稱。在您啟用自訂網域前，在首次建立容器服務時，其僅接受與服務相關聯的預設網域 (例如 `containerservicename.123456abcdef.us-west-2.cs.amazonlightsail.com`) 流量。在您啟用自訂網域時，請選擇您為要搭配容器服務使用之網域所建立的 Lightsail SSL/TLS 憑證，然後從該憑證中選擇要使用的網域。啟用自訂網域之後，容器服務會接受與所選憑證相關聯之所有網域的流量。

## Important

如果您選擇 Lightsail 容器服務做為分發的來源，Lightsail 會自動將分發的預設網域名稱新增為容器服務上的自訂網域。這樣就可以在分發和容器服務之間路由流量。但是，在某些情況下，您可能需要手動將分發的預設網域名新增至容器服務。如需詳細資訊，請參閱[將分發的預設域新增至容器服務](#)。

## 內容

- [容器服務自訂網域限制](#)
- [先決條件](#)
- [檢視容器服務的自訂網域](#)
- [啟用容器服務的自訂網域](#)
- [停用容器服務的自訂網域](#)

## 容器服務自訂網域限制

以下限制會套用至容器服務自訂網域：

- 您可以在每項 Lightsail 容器服務中使用最多 4 個自定網域，且不可在多項服務上使用相同的網域。
- 如果您使用 Lightsail DNS 區域來管理網域的 DNS，則您可以將網域的頂點 (例如 `example.com`) 和子網域 (例如 `www.example.com`) 流量路由到容器服務。

## 必要條件

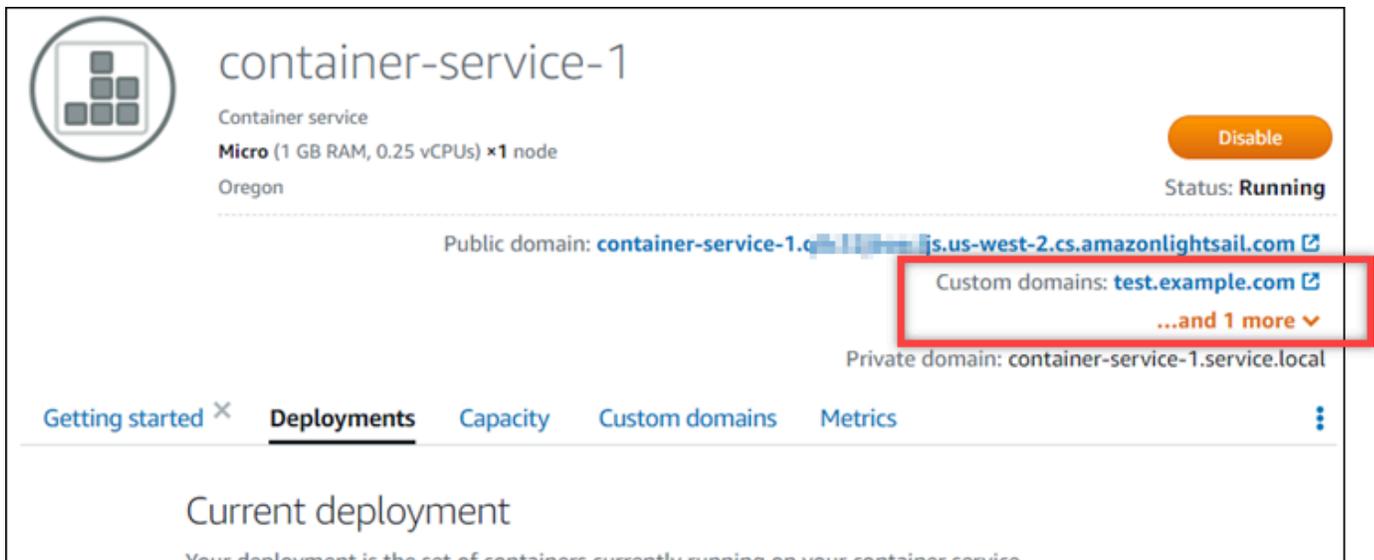
開始之前，您需要建立 Lightsail 容器服務。如需詳細資訊，請參閱[建立 Amazon Lightsail 容器服務](#)。

您也應為容器服務建立和驗證 SSL/TLS 憑證。如需詳細資訊，請參閱[建立容器服務 SSL/TLS 憑證](#)和[驗證容器服務 SSL/TLS 憑證](#)。

## 檢視容器服務的自訂網域

請完成以下程序，以檢視目前已為容器服務啟用的自訂網域。

1. 登入主 [Lightsail](#) 台。
2. 在 Lightsail 首頁，選擇 Containers (容器) 索引標籤。
3. 選擇您要檢視已啟用自訂網域之容器服務的名稱。
4. 在容器服務管理頁面的標頭中找到自訂網域值，如以下範例所示。這些是目前已為容器服務啟用的自訂網域。



5. 在容器服務管理頁面上，選擇 Custom domains (自訂網域) 索引標籤。

已連接憑證下使用的自訂網域，皆列於頁面的 Custom domain SSL/TLS certificates (自訂網域 SSL/TLS 憑證) 區段下。目前連接至您容器服務的憑證，會列於 Attached certificates (連接的憑證) 區段下。

## 啟用容器服務的自訂網域

完成以下程序，以藉由將憑證連接至服務來為 Lightsail 容器服務啟用自訂網域。

1. 登入主 [Lightsail](#) 台。
2. 在 Lightsail 首頁，選擇 Containers (容器) 索引標籤。

3. 選擇要為其啟用自訂網域之容器服務的名稱。
4. 在容器服務管理頁面上，選擇 Custom domains (自訂網域) 索引標籤。

Custom domains (自訂網域) 頁面會顯示目前連接至容器服務的 SSL/TLS 憑證 (若有)。

5. 選擇 Attach certificate (連接憑證)。

若您沒有憑證，則必須先為您的網域建立並驗證 SSL/TLS 憑證，再將其連接至容器服務。如需詳細資訊，請參閱[建立容器服務 SSL/TLS 憑證](#)。

6. 在顯示的下拉式選單中，為您要搭配容器服務使用的網域選取有效憑證。
7. 確認憑證資訊正確無誤，然後選擇 Attach (連接)。
8. 容器服務的 Status (狀態) 會變更為 Updating (正在更新)。狀態變更為 Ready (就緒) 後，憑證的網域就會出現在 Custom domains (自訂網域) 區段中。
9. 選擇 Add domain assignment (新增網域指派)，將網域指向您的容器服務
10. 確認憑證和 DNS 資訊正確無誤，然後選擇 Add assignment (新增指派)。稍待片刻後，容器服務就會開始接受您所選網域的流量。
11. 新增網域指派後，請開啟新的瀏覽器視窗，並瀏覽至已為容器服務啟用的自訂網域。若有任何在容器服務上執行的應用程式，應將其載入。

## 停用容器服務的自訂網域

完成以下程序，以藉由從服務中分開憑證或取消選取先前選取的網域，來停用 Lightsail 容器服務的自訂網域。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁，選擇 Containers (容器) 索引標籤。
3. 選擇要停用自訂網域之容器服務的名稱。
4. 在容器服務管理頁面上，選擇 Custom domains (自訂網域) 索引標籤。

Custom domains (自訂網域) 頁面會顯示目前連接至容器服務的 SSL/TLS 憑證 (若有)。

5. 請選擇下列其中一個選項：
  1. 選擇 Configure container service domains (設定容器服務網域)，以取消選取先前選取的網域，或選取與容器服務相關聯的更多網域。
  2. 選擇中斷連結，將憑證與容器服務中斷連結，並從服務中移除其所有相關聯的域。

**⚠ Important**

如果您尚未這麼做，請修改網域的 DNS 記錄，以便流量路由停止路由至容器服務，而改為路由至其他資源。

**主題**

- [將網域流量路由至 Lightsail 容器服務](#)
- [使用路線 53 將網域流量路由至 Lightsail 容器服務](#)

## 將網域流量路由至 Lightsail 容器服務

啟用服務的自訂網域後，您必須將註冊的網域名稱指向 Amazon Lightsail 容器服務。您可以將別名記錄新增至在您與容器服務搭配使用的憑證上，所指定之每個網域的 DNS 區域來執行這項操作。您新增的所有記錄都應該指向容器服務的預設網域 (例如 `https://<ServiceName>.<RandomGUID>.<AWSRegion>.cs.amazonlightsail.com`)。

在本指南中，我們會為您提供使用 Lightsail DNS 區域將網域指向容器服務的程序。如需有關 Lightsail DNS 區域的詳細資訊，請參閱 [Amazon Lightsail 中的 DNS](#)。

如需有關容器服務的詳細資訊，請參閱 [容器服務](#)。

**i Note**

如果您使用 Route 53 來託管域的 DNS，則應該將別名記錄新增至 Route 53 中域的託管區域。如需詳細資訊，請參閱 [路由 53 中網域的流量路由至 Amazon Lightsail 容器服務](#)。

## 先決條件

在開始之前，您應該為 Lightsail 容器服務啟用自訂網域。如需詳細資訊，請參閱 [啟用和管理 Amazon Lightsail 容器服務的自訂網域](#)。

## 取得容器服務的預設網域

請完成下列程序，以取得容器服務的預設網域名稱，此名稱是在您將別名記錄新增至網域的 DNS 時所指定。

1. 登入主 [Lightsail 控制台](#)。
2. 在 Lightsail 首頁，選擇 Containers (容器) 索引標籤。
3. 選擇要取得預設網域名稱之容器服務的名稱。
4. 在容器服務管理頁面的標頭區段中，記下您的預設網域名稱。容器服務預設網域名稱與 `<ServiceName>.<RandomGUID>.<AWSRegion>.cs.amazonlightsail.com` 類似。

您必須在網域的 DNS 中新增此值，作為正式名稱 (CNAME) 記錄的一部分。建議您複製此值並貼至稍後可參考的文字檔案中。如需詳細資訊，請參閱本指南的下列[將 CNAME 記錄新增至網域的 DNS 區域](#)章節。

## 將記錄新增至網域的 DNS 區域

請完成下列程序，以將地址 (A 代表 IPv4 或 AAAA 代表 IPv6) 記錄或正式 (CNAME) 記錄新增至網域的 DNS 區域。

1. 選擇 Lightsail 首頁上的 Domains & DNS (網域和 DNS) 索引標籤。
2. 在該頁面的 DNS zones (DNS 區域) 區段下，選擇您要在其中新增將網域流量導向至容器服務之記錄的網域名稱。
3. 選擇 DNS records (DNS 記錄) 索引標籤。
4. 根據您 DNS 區域的目前狀態，完成下列其中一個步驟：
  - 如果您尚未新增 A、AAAA 或 CNAME 記錄，請選擇 Add record (新增記錄)。
  - 如果您先前已新增 A、AAAA 或 CNAME 記錄，請選擇該頁面上列出的現有 A、AAAA 或 CNAME 記錄旁邊的編輯圖示，然後跳至此程序的步驟 5。
5. 在 Record type (記錄類型) 下拉式選單中，選擇 A record (A 記錄)、AAAA record (AAAA 記錄) 或 CNAME record (CNAME 記錄)。
  - 新增 A 記錄，以將您網域的頂點 (例如 example.com) 或某個子網域 (例如 www.example.com) 對應至 IPv4 網路下的容器服務。
  - 新增 AAAA 記錄，以將您網域的頂點 (例如 example.com) 或某個子網域 (例如 www.example.com) 對應至 IPv6 網路下的容器服務。
  - 新增 CNAME 記錄，以將子網域 (例如 www.example.com) 對應至容器服務的公有網域 (預設 DNS)。
6. 在 Record name (記錄名稱) 文字方塊中，輸入下列任一選項：

- 對於 A 記錄或 AAAA 記錄，請輸入 @ 來將網域 (例如 example.com) 頂點的流量路由至容器服務，或者輸入子網域 (例如 www) 來將子網域的流量 (例如 www.example.com) 路由至容器服務。
  - 對於 CNAME 記錄，請輸入子網域 (例如 www) 來將子網域的流量 (例如 www.example.com) 路由至容器服務。
7. 根據您正在新增的記錄，完成下列其中一個步驟：
- 對於 A 記錄或 AAAA 記錄，請在 Resolves to (解析為) 文字方塊中選擇容器服務的名稱。
  - 對於 CNAME 記錄，請將容器服務的預設網域名稱輸入 Maps to (對應至) 文字方塊中。
8. 選擇儲存圖示，將記錄儲存到 DNS 區域。

重複這些步驟，為您要與容器服務搭配使用的憑證上的網域新增其他 DNS 記錄。允許透過網際網路 DNS 傳播的變更時間。幾分鐘後，您應該會看到網域是否指向容器服務。

## 使用路線 53 將網域流量路由至 Lightsail 容器服務

您可以將已註冊網域 (例如 example.com) 的流量路由至 Amazon Lightsail 容器服務上執行的應用程式。您可以透過將別名記錄新增至網域的託管區域 (指向 Lightsail 容器服務的預設網域) 來執行此操作。

在本教學課程中，我們將示範如何將 Lightsail 容器服務的別名記錄新增至 Route 53 中的託管區域。您只能使用 AWS Command Line Interface (AWS CLI) 來執行此操作。不能使用 Route 53 主控台來完成。

### Note

如果您使用 Lightsail 來託管網域的 DNS，則應將別名記錄新增至 Lightsail 中網域的 DNS 區域。如需詳細資訊，請參閱將 [Amazon Lightsail 中網域的流量路由至 Lightsail 容器服務](#)。

## 內容

- [步驟 1：完成先決條件](#)
- [步驟 2：取得 Lightsail 容器服務的託管區域 ID](#)
- [步驟 3：建立記錄集 JSON 檔案](#)
- [步驟 4：將記錄新增至 Route 53 中域的託管區域](#)

## 步驟 1：完成先決條件

請先完成事前準備 (若尚未完成)：

- 在 Route 53 中註冊域名稱，或將 Route 53 設為您已註冊 (現有) 域名稱的 DNS 服務。如需詳細資訊，請參閱《Amazon Route 53 開發人員指南》中的[使用 Amazon Route 53 註冊域名稱或將 Amazon Route 53 設為現有域的 DNS 服務](#)。
- 將您的應用程式部署到您的 Lightsail 容器服務。如需詳細資訊，請參閱[建立和管理容器服務部署](#)。
- 在您的 Lightsail 容器服務上啟用您註冊的網域名稱。如需詳細資訊，請參閱[啟用和管理自訂域](#)。
- AWS CLI 使用您的帳戶配置。如需詳細資訊，請參閱[設 AWS CLI 定使用 Lightsail](#)。

## 步驟 2：取得 Lightsail 容器服務的託管區域 ID

在 Route 53 中將別名記錄新增至託管區域時，您必須為 Lightsail 容器服務指定託管區域 ID。例如，如果您的 Lightsail 容器服務位於美國西部 (奧勒岡州) (us-west-2) AWS 區域，則在將 Lightsail 容器服務的別名記錄新增至路由 53 中的託管區域 Z0959753D43BBB908BAV 時，您必須指定託管區域 ID。

以下是您可以在其中建立 Lightsail 容器服務的每個 AWS 區域的託管區域 ID。

歐洲 (倫敦) (eu-west-2) : Z0624918ZXDYQZLOXA66

美國東部 (維吉尼亞北部) (us-east-1) : Z06246771KYU0IRHI74W4

亞太區域 (新加坡) (ap-southeast-1) : Z0625921354DRJH4EY9V0

歐洲 (愛爾蘭) (eu-west-1) : Z0624732FELAMMKW3Y21

亞太區域 (東京) (ap-northeast-1) : Z0626125UUAU4JWQ9JSKN

亞太區域 (首爾) (ap-northeast-2) : Z06260262XZM84B2WPLHH

亞太區域 (孟買) (ap-south-1) : Z10460781IQMISS0I0VVY

亞太區域 (雪梨) (ap-southeast-2) : Z09597943PQQZATPFE96E

加拿大 (中部) (ca-central-1) : Z10450993RIRIJJUUMA5W

歐洲 (法蘭克福) (eu-central-1) : Z06137433FV04OY4EC6L0

歐洲 (斯德哥爾摩) (eu-north-1) : Z016970523TDG2TZMUXKK

歐洲 (巴黎) (eu-west-3) : Z09594631DSW2QUR7CFGO

美國東部 (俄亥俄) (us-east-2) : Z10362273VJ548563IY84

美國西部 (奧勒岡) (us-west-2): Z0959753D43BBB908BAV

### 步驟 3：建立記錄集 JSON 檔案

當您使用在 Route 53 中將 DNS 記錄新增至網域的託管區域時 AWS CLI，您必須為記錄指定一組組態參數。最簡單的方法是建立包含所有參數的 JSON (.json) 檔案，然後在 AWS CLI 要求中參考 JSON 檔案。

請完成下列程序，以建立具有別名記錄之記錄集參數的 JSON 檔案：

1. 開啟文字編輯器，例如 Windows 上的記事本或 Linux 上的 Nano。
2. 複製下列文字並貼至文字編輯器：

```
{
  "Comment": "Comment",
  "Changes": [
    {
      "Action": "CREATE",
      "ResourceRecordSet": {
        "Name": "Domain.",
        "Type": "A",
        "AliasTarget": {
          "HostedZoneId": "LightsailContainerServiceHostedZoneID",
          "DNSName": "LightsailContainerServiceAddress.",
          "EvaluateTargetHealth": true
        }
      }
    }
  ]
}
```

在您的檔案中，將以下範例文字取代為自訂文字：

- *Comment*，並附上關於記錄集的個人備註或註解。
- *#### Lightsail ##### (###example.com#www.example.com)#*若要將網域的根目錄與 Lightsail 容器服務搭配使用，您必須在網域的子網域空間中指定@符號 (例如)。@.example.com

- `LightsailContainerServiceHostedZone##### Lightsail ##### AWS ##### ## ID #####`如需詳細資訊，請參閱本指南前面的[步驟 2：取得 Lightsail 容器服務的託管區域 ID](#)。
- `LightsailContainerServiceAddress`使用您的 Lightsail 容器服務的公有網域名稱。您可以登入 Lightsail 主控台、瀏覽至您的容器服務，然後複製容器服務管理頁面標頭區段中列出的公用網域 (例如 `container-service-1.q8cexampleljs.us-west-2.cs.amazonlightsail.com`)，以取得此功能。

範例：

```
{
  "Comment": "Alias record for Lightsail container service",
  "Changes": [
    {
      "Action": "CREATE",
      "ResourceRecordSet": {
        "Name": "@.example.com.",
        "Type": "A",
        "AliasTarget": {
          "HostedZoneId": "Z0959753D43BBB908BAV",
          "DNSName": "container-service-1.q8cexampleljs.us-
west-2.cs.amazonlightsail.com.",
          "EvaluateTargetHealth": true
        }
      }
    }
  ]
}
```

3. 在您的本機目錄中將檔案儲存為 `change-resource-record-sets.json`。

#### 步驟 4：將記錄新增至 Route 53 中域的託管區域

完成下列程序，使用 AWS CLI 將記錄新增至 Route 53 中域的託管區域。您可以使用 `change-resource-record-sets` 命令來執行此動作。若要取得更多資訊，請參閱《指 AWS CLI 令參考》[change-resource-record-sets](#) 中的。

**Note**

您必須先為 Lightsail AWS CLI 和 Route 53 安裝並進行設定，然後才能繼續執行此程序。如需詳細資訊，請參閱[設 AWS CLI 定使用 Lightsail](#)。

1. 開啟命令提示或終端機視窗。
2. 輸入以下命令，將記錄新增至 Route 53 中網域的託管區域。

```
aws route53 change-resource-record-sets --hosted-zone-id HostedZoneID --change-batch PathToJsonFile
```

將命令中的以下範例文字取代為自訂文字：

- *HostedZone#### Route 53 ##### ID # ID* 使用 [list-hosted-zones](#) 命令取得 Route 53 帳戶中託管區域的 ID 清單。
- *PathToJsonFile* 使用包含記錄參數的 .json 文件的計算機上的本地目錄文件夾路徑。如需詳細資訊，請參閱本指南前述的 [步驟 3：建立記錄集 JSON 檔案](#) 一節。

範例：

在 Linux 或 Unix 電腦上：

```
aws route53 change-resource-record-sets --hosted-zone-id Z123456789ABCDEFGHJ --change-batch home/user/awscli/route53/change-resource-record-sets.json
```

在 Windows 電腦上：

```
aws route53 change-resource-record-sets --hosted-zone-id Z123456789ABCDEFGHJ --change-batch file://C:\awscli\route53\change-resource-record-sets.json
```

您應該會看到類似以下範例的結果：

```
H:\>aws route53 change-resource-record-sets --hosted-zone-id Z123456789ABCDEFGHIJ
--change-batch file://C:\awscli\route53\change-resource-record-sets.json

{
  "ChangeInfo": {
    "Id": "/change/C05953EXAMPLEZ4V4LOAC",
    "Status": "PENDING",
    "SubmittedAt": "2021-08-11T20:58:30.960000+00:00",
    "Comment": "Alias record for Lightsail container service"
  }
}
```

透過網際網路 DNS 傳播變更需要一些時間，最多可能需要幾個小時。完成後，您在 Route 53 中註冊網域的網際網路流量應該會開始路由傳送至您的 Lightsail 容器服務。

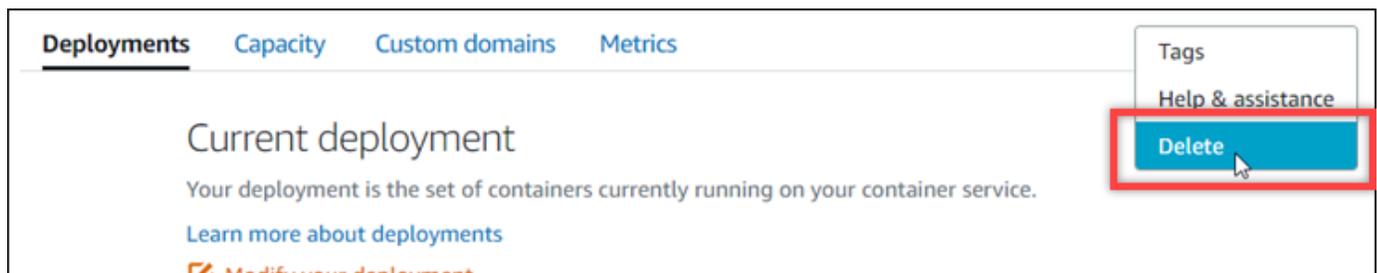
## 刪除集 Lightsail 服務

若您不再使用，您可以隨時刪除 Amazon Lightsail 容器服務。刪除容器服務時，與該服務相關聯的所有部署和已註冊容器映像都會永久銷毀。不過，您已建立的 SSL/TLS 憑證和網域會保留在 Lightsail 帳戶中，以便您可以將其與其他資源搭配使用。如需有關容器服務的詳細資訊，請參閱 [Amazon Lightsail 中的容器服務](#)。

### 刪除容器服務

請完成下列程序以刪除容器服務。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁，選擇 Containers (容器) 索引標籤。
3. 選擇您要刪除之容器服務的名稱。
4. 在索引標籤選單中選擇省略符號圖示，然後選擇 Delete (刪除)。



5. 選擇 Delete container service (刪除容器服務) 以刪除您的服務。
6. 在顯示的提示中，選擇 Yes, delete (是，刪除) 以確認該刪除為永久性操作。

容器服務會在幾分鐘後遭刪除。

# Amazon Lightsail 中的安全

雲安全 AWS 是最高的優先級。身為 AWS 客戶，您可以從資料中心和網路架構中獲益，該架構專為滿足對安全性最敏感的組織的需求而打造。

安全是 AWS 與您之間共同承擔的責任。[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 雲端中執行 AWS 服務的基礎架構。AWS 還為您提供可以安全使用的服務。若要了解合規計畫與適用的服務，請參閱[合規計畫範圍內的 AWS 服務](#)。
- 雲端中的安全性 — 您的責任取決於您使用的 AWS 服務。您也必須對其他因素負責，包括資料的機密性、您的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 Amazon Lightsail 時套用共同的責任模型。下列主題說明如何設定 Amazon Lightsail 以符合您的安全性和合規目標。您也會學到如何使用其他可協助您監控和保護 Amazon Lightsail 資源的 AWS 服務。

## Amazon Lightsail 基礎設施安全

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

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

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

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

## Amazon Lightsail 的韌性

AWS 全球基礎架構是圍繞 AWS 區域 s 和可用區域建立的。AWS 區域 s 提供多個實體分離和隔離的可用區域，這些區域透過低延遲、高輸送量和高度備援的網路連線。透過可用區域，您可以設計與操作

的應用程式和資料庫，在可用區域之間自動容錯移轉而不會發生中斷。可用區域的可用性、容錯能力和擴展能力，均較單一或多個資料中心的傳統基礎設施還高。

如需 AWS 區域 和可用區域的詳細資訊，請參閱[AWS 全域基礎結構](#)。

除了 AWS 全球基礎設施之外，Amazon Lightsail 還提供多種功能來協助支援您的資料彈性和備份需求。

- 跨區域複製執行個體和磁碟快照。如需詳細資訊，請參閱[快照](#)。
- 使執行個體和磁碟快照自動化。如需詳細資訊，請參閱[快照](#)。
- 使用負載平衡器，將傳入流量分配到單一可用區域或多個可用區域中的多個執行個體。如需詳細資訊，請參閱[負載平衡器](#)。

## Amazon Lightsail 的身分識別和存取管理

### 物件

根據您在亞 Amazon Lightsail 中執行的工作，使用方式 AWS Identity and Access Management (IAM) 會有所不同。

**服務使用者** — 如果您使用 Amazon Lightsail 服務執行工作，則管理員會為您提供所需的登入資料和許可。當您使用更多 Amazon Lightsail 功能完成工作時，您可能需要額外的許可。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。如果您無法在 Amazon Lightsail 中存取某項功能，請參閱[Identity and Access Management 疑難排解 \(IAM\)](#)。

**服務管理員** — 如果您負責公司的 Amazon Lightsail 資源，那麼您可能擁有對 Amazon Lightsail 的完整存取權。您的工作就是決定員工應該存取哪些 Amazon Lightsail 功能和資源。然後，您必須向IAM管理員提交請求，才能變更服務使用者的權限。檢閱此頁面上的資訊，以瞭解的基本概念IAM。若要進一步了解貴公司如何IAM搭配 Amazon Lightsail 使用，請參閱[Amazon Lightsail 如何搭配使用](#)。IAM

**IAM管理員** — 如果您是管理IAM員，您可能想要了解如何撰寫政策以管理 Amazon Lightsail 存取權的詳細資訊。若要檢視您可以在中使用的 Amazon Lightsail 身分型政策範例IAM，請參閱[Amazon Lightsail 身分識別政策範例](#)。

### 使用身分來驗證

驗證是您 AWS 使用身分認證登入的方式。如需有關使用登入的詳細資訊 AWS Management Console，請參閱使用IAM者指南中的[IAM主控台和登入頁面](#)。

您必須以 AWS 帳戶 root 使用者、使用者或假定IAM角色的IAM身分驗證 (登入 AWS)。您也可以使用貴公司的單一登入身分驗證，甚至使用 Google 或 Facebook 進行登入。在這些情況下，您的系統管理員先前使用IAM角色設定身分同盟。當您 AWS 使用其他公司的認證進行存取時，您會間接擔任角色。

若要直接登入 [AWS Management Console](#)，請使用您的密碼與 root 使用者電子郵件或您的使用IAM者名稱。您可以使用 root 使用者或IAM使用者存取金鑰以 AWS 程式設計方式存取。AWS 提供SDK和命令行工具，以使用您的憑據對請求進行密碼編譯簽名。如果您不使用 AWS 工具，則必須自行簽署要求。使用簽名版本 4 來執行此操作，這是一種用於驗證輸入API請求的協議。如需有關驗證請求的詳細資訊，請參閱《AWS 一般參考》中的 [Signature 第 4 版簽署程序](#)。

無論您使用何種身分驗證方法，您可能還需要提供額外的安全性資訊。例如，AWS 建議您使用多重要素驗證 (MFA) 來增加帳戶的安全性。若要深入瞭解，請參閱[使用IAM者指南中 AWS的使用多重要素驗證 \(MFA\)](#)。

## AWS 帳戶 根使用者

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

## IAM 使用者和群組

[IAM使用者](#)是您內部的身分，具 AWS 帳戶 有單一人員或應用程式的特定權限。在可能的情況下，我們建議您仰賴臨時登入資料，而不要建立具有長期認證 (例如密碼和存取金鑰) 的IAM使用者。不過，如果您的特定使用案例需要使用IAM者的長期認證，建議您輪換存取金鑰。如需詳細資訊，請參閱《[使用指南](#)》中的「[IAM定期輪換存取金鑰](#)」以瞭解需要長期認證的使用案例。

[IAM群組](#)是指定IAM使用者集合的身分識別。您無法以群組身分簽署。您可以使用群組來一次為多名使用者指定許可。群組可讓管理大量使用者許可的程序變得更為容易。例如，您可以擁有一個名為的群組，IAMAdmins並授與該群組管理IAM資源的權限。

使用者與角色不同。使用者只會與單一人員或應用程式建立關聯，但角色的目的是在由任何需要它的人員取得。使用者擁有永久的長期憑證，但角色僅提供暫時憑證。要了解更多信息，請參閱《[IAM用戶指南](#)》中的[創建用戶 \( 而不是角色 \) 的IAM時間](#)。

## IAM 角色

[IAM角色](#)是您 AWS 帳戶 中具有特定權限的身份。它類似於用IAM戶，但不與特定人員相關聯。您可以 AWS Management Console 透過[切換角色來暫時擔任中的角色](#)。IAM您可以透過呼叫 AWS CLI 或

AWS API作業或使用自訂來擔任角色URL。如需有關使用角色方法的詳細資訊，請參閱 [《使用指南》中的IAM〈使用IAM角色〉](#)。

IAM具有臨時認證的角色在下列情況下很有用：

- **聯合身分使用者存取** — 如需向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並獲授予由角色定義的許可。如需聯合角色的相關資訊，請參閱 [《使用指南》中的〈建立第三方身分識別提供IAM者的角色〉](#)。如果您使用IAM身分識別中心，則需要設定權限集。為了控制身分驗證後可以存取的內IAM容，IAM Identity Center 會將權限集與中的角色相關聯。如需有關許可集的資訊，請參閱 AWS IAM Identity Center 使用者指南中的 [許可集](#)。
- **暫時IAM使用者權限** — IAM 使用者或角色可以假定某個IAM角色，暫時取得特定工作的不同權限。
- **跨帳戶存取** — 您可以使用IAM角色允許不同帳戶中的某個人 (受信任的主體) 存取您帳戶中的資源。角色是授予跨帳戶存取權的主要方式。但是，對於某些策略 AWS 服務，您可以將策略直接附加到資源 (而不是使用角色作為代理)。若要瞭解跨帳戶存取角色與以資源為基礎的政策之間的差異，請參閱 [《IAM使用指南》IAM中的〈跨帳號資源存取〉](#)。
- **跨服務訪問** — 有些 AWS 服務 使用其他 AWS 服務功能。例如，當您在服務中撥打電話時，該服務通常會在 Amazon 中執行應用程式EC2或將物件存放在 Amazon S3 中。服務可能會使用呼叫主體的許可、使用服務角色或使用服務連結角色來執行此作業。
- **轉寄存取工作階段 (FAS)** — 當您使用IAM者或角色執行中的動作時 AWS，您會被視為主參與者。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS會使用主參與者呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。FAS只有當服務收到需要與其他 AWS 服務 資源互動才能完成的請求時，才會發出請求。在此情況下，您必須具有執行這兩個動作的許可。有關提出FAS請求時的策略詳細信息，請參閱 [轉發訪問會話](#)。
- **服務角色** — 服務角色是指服務代表您執行動作所代表的IAM角色。IAM管理員可以從中建立、修改和刪除服務角色IAM。如需詳細資訊，請參閱 [《IAM使用指南》AWS 服務中的建立角色以將權限委派給](#)
- **服務連結角色** — 服務連結角色是連結至 AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中，AWS 帳戶 且屬於服務所有。IAM管理員可以檢視 (但無法編輯服務連結角色) 的權限。
- **在 Amazon 上執行的應用程式 EC2** — 您可以使用IAM角色來管理在執行個體上EC2執行的應用程式以及發出 AWS CLI 或 AWS API請求的臨時登入資料。這比在EC2執行個體中儲存存取金鑰更可取。若要將 AWS 角色指派給EC2執行個體並讓其所有應用程式都能使用，請建立附加至執行個體的執行個體設定檔。執行個體設定檔包含角色，可讓執行個體上EC2執行的程式取得臨時登入資料。如需詳細資訊，請參閱 [使用者指南中的使用IAM角色將許可授與在 Amazon EC2 執行個體上執行的應IAM用程式](#)。

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

IAM具有臨時認證的角色在下列情況下很有用：

- 暫時IAM使用者權限 — IAM 使用者可以假定某個IAM角色暫時取得特定工作的不同權限。
- 聯合身分使用者存取 — 如需向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並獲授予由角色定義的許可。如需聯合角色的相關資訊，請參閱 [《使用指南》](#) 中的 [〈建立第三方身分識別提供IAM者的角色〉](#)。如果您使用IAM身分識別中心，則需要設定權限集。為了控制身分驗證後可以存取的內IAM容，IAMIdentity Center 會將權限集與中的角色相關聯。如需有關許可集的資訊，請參閱 AWS IAM Identity Center 使用者指南中的 [許可集](#)。
- 跨帳戶存取 — 您可以使用IAM角色允許不同帳戶中的某個人 (受信任的主體) 存取您帳戶中的資源。角色是授予跨帳戶存取權的主要方式。但是，對於某些策略 AWS 服務，您可以將策略直接附加到資源 ( 而不是使用角色作為代理 )。若要瞭解跨帳戶存取角色與以資源為基礎的政策之間的差異，請參閱 [《IAM使用指南》](#) 中的 [IAM角色與以資源為基礎的政策有何不同](#)。
- 跨服務訪問 — 有些 AWS 服務 使用其他 AWS 服務功能。例如，當您在服務中撥打電話時，該服務通常會在 Amazon 中執行應用程式EC2或將物件存放在 Amazon S3 中。服務可能會使用呼叫主體的許可、使用服務角色或使用服務連結角色來執行此作業。
  - 轉寄存取工作階段 (FAS) — 當您使用使用IAM者或角色執行中的動作時 AWS，您會被視為主參與者。政策能將許可授予主體。當您使用某些服務時，您可能會執行一個動作，然後在不同的服務中觸發另一個動作。在此情況下，您必須具有執行這兩個動作的許可。若要查看動作是否需要政策中的其他相依動作，請參閱 [服務授權參考中適用於 Amazon Lightsail 的動作、資源和條件金鑰](#)。
  - 服務角色 — 服務角色是指服務代表您執行動作所代表的IAM角色。IAM管理員可以從中建立、修改和刪除服務角色IAM。如需詳細資訊，請參閱 [《IAM使用指南》](#) AWS 服務中的 [建立角色以將權限委派給](#)
  - 服務連結角色 — 服務連結角色是連結至 AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中，AWS 帳戶 且屬於服務所有。IAM管理員可以檢視 (但無法編輯服務連結角色) 的權限。
- 在 Amazon 上執行的應用程式 EC2 — 您可以使用IAM角色來管理在執行個體上EC2執行的應用程式以及發出 AWS CLI 或 AWS API請求的臨時登入資料。這比在EC2執行個體中儲存存取金鑰更可取。若要將 AWS 角色指派給EC2執行個體並讓其所有應用程式都能使用，請建立附加至執行個體的執行個體設定檔。執行個體設定檔包含角色，可讓執行個體上EC2執行的程式取得臨時登入資料。如需詳細資訊，請參閱 [使用者指南中的使用IAM角色將許可授與在 Amazon EC2 執行個體上執行的應IAM用程式](#)。

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

## 使用政策管理存取權

您可以透過 AWS 過建立原則並將其附加至 AWS 身分識別或資源來控制中的存取。原則是一個物件 AWS，當與身分識別或資源相關聯時，會定義其權限。AWS 當主參與者 (使用者、root 使用者或角色工作階段) 提出要求時，評估這些原則。政策中的許可決定是否允許或拒絕請求。大多數原則會 AWS 以JSON文件的形式儲存在中。如需有關JSON原則文件結構和內容的詳細資訊，請參閱 [《IAM使用指南》](#) 中的策略 [概觀](#)。JSON

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

預設情況下，使用者和角色沒有許可。若要授與使用者對所需資源執行動作的權限，IAM管理員可以建立IAM策略。然後，系統管理員可以將IAM原則新增至角色，使用者可以擔任這些角色。

IAM原則會定義動作的權限，不論您用來執行作業的方法為何。例如，假設您有一個允許 `iam:GetRole` 動作的政策。具有該原則的使用者可以從 AWS Management Console AWS CLI、或取得角色資訊 AWS API。

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

每個IAM實體 (使用者或角色) 都不會有任何權限。換句話說，根據預設，使用者無法執行任何作業，甚至也無法變更他們自己的密碼。若要授予使用者執行動作的許可，管理員必須將許可政策連接到使用者。或者，管理員可以將使用者新增到具備預定許可的群組。管理員將許可給予群組時，該群組中的所有使用者都會獲得那些許可。

IAM原則會定義動作的權限，不論您用來執行作業的方法為何。例如，假設您有一個允許 `iam:GetRole` 動作的政策。具有該原則的使用者可以從 AWS Management Console AWS CLI、或取得角色資訊 AWS API。

## 身分型政策

以身分識別為基礎的原則是您可以附加至身分識別 (例如使用者、使用IAM者群組或角色) 的JSON權限原則文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。若要瞭解如何建立以身分識別為基礎的策略，請參閱 [《IAM使用指南》](#) 中的 [〈建立IAM策略〉](#)。

身分型政策可進一步分類成內嵌政策或受管政策。內嵌政策會直接內嵌到單一使用者、群組或角色。受管理的策略是獨立策略，您可以將其附加到您的 AWS 帳戶。受管政策包括 AWS 受管政策和客戶管理

的策略。若要了解如何在受管策略或內嵌策略之間進行選擇，請參閱《IAM使用手冊》中的「[在受管策略和內嵌策略之間進行選擇](#)」。

以身分識別為基礎的原則是您可以附加至身分識別 (例如使用者、使用IAM者群組或角色) 的JSON權限原則文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。若要瞭解如何建立以身分識別為基礎的策略，請參閱《IAM使用指南》中的〈[建立IAM策略](#)〉。

## 資源型政策

以資源為基礎的JSON策略是您附加至資源的政策文件。以資源為基礎的政策範例包括IAM角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中[指定主體](#)。主參與者可以包括帳戶、使用者、角色、同盟使用者或。AWS 服務

資源型政策是位於該服務中的內嵌政策。您無法在以資源為基礎的策略IAM中使用 AWS 受管政策。

以資源為基礎的JSON策略是您附加至資源的政策文件。以資源為基礎的政策範例包括IAM角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中[指定主體](#)。主參與者可以包括帳戶、使用者、角色、同盟使用者或。AWS 服務

## 存取控制清單 (ACLs)

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

Amazon S3 和 Amazon VPC 是支持服務的示例ACLs。AWS WAF若要進一步了解ACLs，請參閱 Amazon 簡單儲存服務開發人員指南中的存取控制清單 ([ACL](#)) 概觀。

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

## 其他政策類型

AWS 支援其他較不常見的原則類型。這些政策類型可設定較常見政策類型授予您的最大許可。

- 權限界限 — 權限界限是一項進階功能，您可以在其中設定以身分識別為基礎的原則可授與給IAM實體 (IAM使用者或角色) 的最大權限。您可以為實體設定許可界限。所產生的許可會是實體的身分型政

策和其許可界限的交集。會在 Principal 欄位中指定使用者或角色的資源型政策則不會受到許可界限限制。所有這類政策中的明確拒絕都會覆寫該允許。如需有關權限界限的詳細資訊，請參閱《IAM 使用指南》中的[IAM 實體的權限界限](#)。

- 服務控制策略 (SCPs) — SCPs 是指定中組織或組織單位 (OU) 最大權限的 JSON 策略 AWS Organizations。AWS Organizations 是一種用於分組和集中管理您企業擁有的多個 AWS 帳戶的服務。如果您啟用組織中的所有功能，則可以將服務控制策略 (SCPs) 套用至您的任何或所有帳戶。SCP 限制成員帳戶中實體的權限，包括每個帳戶的 AWS 帳戶根使用者。如需有關 Organizations 的詳細資訊 SCPs，請參閱 AWS Organizations 使用指南中的[服務控制原則](#)。
- 工作階段政策 – 工作階段政策是一種進階政策，您可以在透過編寫程式的方式建立角色或聯合使用者的暫時工作階段時，作為參數傳遞。所產生工作階段的許可會是使用者或角色的身分型政策和工作階段政策的交集。許可也可以來自資源型政策。所有這類政策中的明確拒絕都會覆寫該允許。如需詳細資訊，請參閱《IAM 使用指南》中的[工作階段原則](#)。
- 權限界限 — 權限界限是一項進階功能，您可以在其中設定以身分識別為基礎的原則可授與給 IAM 實體 (IAM 使用者或角色) 的最大權限。您可以為實體設定許可界限。所產生的許可會是實體的身分型政策和其許可界限的交集。會在 Principal 欄位中指定使用者或角色的資源型政策則不會受到許可界限限制。所有這類政策中的明確拒絕都會覆寫該允許。如需有關權限界限的詳細資訊，請參閱《IAM 使用指南》中的[IAM 實體的權限界限](#)。
- 服務控制策略 (SCPs) — SCPs 是指定中組織或組織單位 (OU) 最大權限的 JSON 策略 AWS Organizations。AWS Organizations 是一種用於分組和集中管理您企業擁有的多個 AWS 帳戶的服務。如果您啟用組織中的所有功能，則可以將服務控制策略 (SCPs) 套用至您的任何或所有帳戶。SCP 限制成員帳戶中實體的權限，包括每個 AWS 帳戶 root 使用者。若要取得有關 Organizations 的更多資訊 SCPs，請參閱 [《AWS Organizations 使用指南》中的〈SCPs 運作方式〉](#)
- 工作階段政策 – 工作階段政策是一種進階政策，您可以在透過編寫程式的方式建立角色或聯合使用者的暫時工作階段時，作為參數傳遞。所產生工作階段的許可會是使用者或角色的身分型政策和工作階段政策的交集。許可也可以來自資源型政策。所有這類政策中的明確拒絕都會覆寫該允許。如需詳細資訊，請參閱《IAM 使用指南》中的[工作階段原則](#)。

## 多種政策類型

將多種政策類型套用到請求時，其結果形成的許可會更為複雜、更加難以理解。若要瞭解如何在涉及多個原則類型時 AWS 決定是否允許要求，請參閱 IAM 使用指南中的[原則評估邏輯](#)。

### 主題

- [AWS Amazon Lightsail 管理政策](#)

- [亞 Amazon Lightsail 如何與 IAM](#)
- [授與 Lightsail 用者的存取權限](#)

## AWS Amazon Lightsail 管理政策

若要新增使用者、群組和角色的權限，使用 AWS 受管理的原則比自己撰寫原則更容易。建立 [IAM 客戶受管政策](#) 需要時間和專業知識，而受管政策可為您的團隊提供其所需的許可。若要快速開始使用，您可以使用我們的 AWS 受管政策。這些政策涵蓋常見的使用案例，並可在您的 AWS 帳戶中使用。如需 AWS 受管政策的詳細資訊，請參閱 IAM 使用者指南中的 [AWS 受管政策](#)。

AWS 服務會維護和更新 AWS 受管理的策略。您無法變更 AWS 受管理原則中的權限。服務有時會將其他權限新增至受 AWS 管理的策略，以支援新功能。此類型的更新會影響已連接政策的所有身分識別 (使用者、群組和角色)。當新功能啟動或新作業可用時，服務最有可能更新 AWS 受管理的策略。服務不會從 AWS 受管理的政策移除權限，因此政策更新不會破壞您現有的權限。

此外，還 AWS 支援跨多個服務之工作職能的受管理原則。例如，ReadOnlyAccess AWS 受管理的策略提供對所有 AWS 服務和資源的唯讀存取。當服務啟動新功能時，會為新作業和資源新 AWS 增唯讀權限。如需任務職能政策的清單和說明，請參閱 IAM 使用者指南中 [有關任務職能的 AWS 受管政策](#)。

### AWS 受管理策略：LightsailExportAccess

您無法附加 LightsailExportAccess 到 IAM 實體。此原則附加至服務連結角色，可讓 Lightsail 代表您執行動作。如需詳細資訊，請參閱 [服務連結角色](#)。

此政策授予允許 Lightsail 將執行個體和磁碟快照匯出到 Amazon 彈性運算雲端的許可，並從 Amazon 簡單儲存服務 (Amazon S3) 取得目前帳戶層級區塊公開存取組態。

#### 許可詳細資訊

此政策包含以下許可。

- ec2 – 允許列出和複製執行個體映像和磁碟快照的存取權。
- iam – 允許刪除服務連結角色並擷取服務連結角色刪除狀態的存取權。
- s3 – 允許存取擷取 AWS 帳戶的 PublicAccessBlock 組態。

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

```
"Statement": [  
  {  
    "Effect": "Allow",  
    "Action": [  
      "iam:DeleteServiceLinkedRole",  
      "iam:GetServiceLinkedRoleDeletionStatus"  
    ],  
    "Resource": "arn:aws:iam::*:role/aws-service-role/lightsail.amazonaws.com/  
AWSServiceRoleForLightsail*"  
  },  
  {  
    "Effect": "Allow",  
    "Action": [  
      "ec2:CopySnapshot",  
      "ec2:DescribeSnapshots",  
      "ec2:CopyImage",  
      "ec2:DescribeImages"  
    ],  
    "Resource": "*"   
  },  
  {  
    "Effect": "Allow",  
    "Action": [  
      "s3:GetAccountPublicAccessBlock"  
    ],  
    "Resource": "*"   
  }  
]
```

## AWS 受管理政策的更新

- 編輯 LightsailExportAccess 受管政策

新增 s3:GetAccountPublicAccessBlock 動作至 LightsailExportAccess 受管政策。它可讓 Lightsail 從 Amazon S3 取得目前帳戶層級的區塊公開存取組態。

2022 年 1 月 14 日

- Lightsail 開始追蹤變更

Lightsail 開始追蹤其 AWS 受管理原則的變更。

2022 年 1 月 14 日

## 亞 Amazon Lightsail 如何與 IAM

在您使用IAM來管理 Lightsail 的存取權限之前，您應該瞭解哪些IAM功能可與 Lightsail 搭配使用。若要取得 Lightsail 和其他 AWS 服務如何使用的高階檢視IAM，請參閱IAM使用者指南IAM中的可搭配使用的[AWS 服務](#)。

### 基於 Lightsail 身份的政策

使用以IAM身分識別為基礎的策略，您可以指定允許或拒絕的動作和資源，以及允許或拒絕動作的條件。Lightsail 支援特定的動作、資源和條件鍵。若要瞭解您在JSON策略中使用的所有元素，請參閱《使用IAM者指南》中的《[IAMJSON策略元素參考](#)》。

### 動作

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

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

政策會使用動作來授予執行相關聯動作的許可。

Lightsail 中的原則動作會在動作之前使用下列前置詞：lightsail:。例如，若要授與某人使用 Lightsail 作業執行 Lightsail 執行個體的權限，您可以將該lightsail:CreateInstances動CreateInstancesAPI作納入他們的原則中。政策陳述式必須包含 Action 或 NotAction 元素。Lightsail 會定義自己的一組動作，用來描述您可以使用此服務執行的工作。

若要在單一陳述式中指定多個動作，請用逗號分隔，如下所示：

```
"Action": [
    "lightsail:action1",
    "lightsail:action2"
```

您也可以使用萬用字元 (\*) 來指定多個動作。例如，若要指定開頭是 Create 文字的所有動作，請包含以下動作：

```
"Action": "lightsail:Create*"
```

若要查看 Lightsail 動作清單，請參閱IAM使用者指南中的[Amazon Lightsail 定義的動作](#)。

## 資源

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

ResourceJSON 原則元素會指定要套用動作的一或多個物件。陳述式必須包含 Resource 或 NotResource 元素。最佳做法是使用其 [Amazon 資源名稱 \(ARN\)](#) 指定資源。您可以針對支援特定資源類型的動作 (稱為資源層級許可) 來這麼做。

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

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

### Important

Lightsail 不支援某些動作的資源層級權限。API 如需詳細資訊，請參閱 [支援基於標籤的資源層級許可和授權](#)。

Lightsail 實體資源具有下列項目：ARN

```
arn:${Partition}:lightsail:${Region}:${Account}:Instance/${InstanceId}
```

如需的格式的詳細資訊 ARNs，請參閱 [Amazon 資源名稱 \(ARNs\)](#) 和 [AWS 服務命名空間](#)。

例如，若要在陳述式中指定 ea123456-e6b9-4f1d-b518-3ad1234567e6 執行個體，請使用下列指令 ARN：

```
"Resource": "arn:aws:lightsail:us-east-1:123456789012:Instance/ea123456-e6b9-4f1d-b518-3ad1234567e6" 
```

若要指定屬於特定帳戶的所有執行個體，請使用萬用字元 (\*)：

```
"Resource": "arn:aws:lightsail:us-east-1:123456789012:Instance/*" 
```

某些 Lightsail 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": "*" 
```

許多 Lightsail API 動作都涉及多種資源。例如，AttachDisk將 Lightsail 區塊儲存磁碟附加至執行個體，因此使用IAM者必須擁有使用該磁碟和執行個體的權限。若要在單一陳述式中指定多個資源，請以 ARNs 逗號分隔。

```
"Resource": [  
  "resource1",  
  "resource2"
```

若要查看 Lightsail 資源類型及其清單 ARNs，請參閱 IAM 使用者指南中的 [Amazon Lightsail 定義的資源](#)。若要了解可以針對每個資源指定哪些動作，請參閱 [Amazon Lightsail 定義 ARN 的動作](#)。

## 條件金鑰

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

Condition 元素 (或 Condition 區塊) 可讓您指定使陳述式生效的條件。Condition 元素是選用項目。您可以建立使用 [條件運算子](#) 的條件運算式 (例如等於或小於)，來比對政策中的條件和請求中的值。

若您在陳述式中指定多個 Condition 元素，或是在單一 Condition 元素中指定多個索引鍵，AWS 會使用邏輯 AND 操作評估他們。如果您為單一條件索引鍵指定多個值，請使用邏輯 OR 運算來 AWS 評估條件。必須符合所有條件，才會授與陳述式的許可。

您也可以指定條件時使用預留位置變數。例如，只有在 IAM 使用者名稱標記資源時，您才可以授與 IAM 使用者存取資源的權限。如需詳細資訊，請參閱 IAM 使用指南中的 [IAM 政策元素：變數和標籤](#)。

AWS 支援全域條件金鑰和服務特定條件金鑰。若要查看所有 AWS 全域條件索引鍵，請參閱《使用指南》中的 [AWS 全域條件內 IAM 容索引鍵](#)。

Lightsail 不提供任何服務特定的條件金鑰，但它確實支援使用某些全域條件金鑰。若要查看所有 AWS 全域條件索引鍵，請參閱使用指南中的 [AWS 全域條件內 IAM 容索引鍵](#)。

若要查看 Lightsail 條件金鑰清單，請參閱 IAM 使用者指南中的 [適用於 Amazon Lightsail 的條件金鑰](#)。若要了解可以使用條件金鑰的動作和資源，請參閱 [Amazon Lightsail 定義的動作](#)。

## 範例

若要檢視以身分識別為基礎的政策範例，請參閱 [Amazon Lightsail 以身分識別為基礎的政策範例](#)。

## Lightsail 資源型政策

Lightsail 不支援以資源為基礎的政策。

## 存取控制清單 (ACLs)

Lightsail 不支援存取控制清單 (ACLs)。

## 基於 Lightsail 標籤的授權

您可以將標籤附加至 Lightsail 資源，或將請求中的標籤傳遞給 Lightsail。如需根據標籤控制存取，請使用 `lightsail: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。

### Important

對於某些 API 動作，Lightsail 不支援以標籤為基礎的授權。如需詳細資訊，請參閱[支援基於標籤的資源層級許可和授權](#)。

如需有關標記 Lightsail 資源的詳細資訊，請參閱[標記](#)。

若要檢視以身分識別為基礎的原則範例，以根據該資源上的標籤限制對資源的存取，請參閱[允許根據標籤建立和刪除 Lightsail 資源](#)。

## Lightsail 角 IAM 色

[IAM 角色](#)是您 AWS 帳戶中具有特定權限的實體。

### 搭配使用臨時登入資料

您可以使用臨時認證登入同盟、擔任 IAM 角色或擔任跨帳戶角色。您可以透過呼叫[AssumeRole](#)或之類的 AWS STS API 作業來取得臨時安全登入資料[GetFederationToken](#)。

Lightsail 支援使用臨時登入資料。

### 服務連結角色

[服務連結角色](#)可讓 AWS 服務存取其他服務中的資源，以代表您完成動作。服務連結角色會顯示在您的 IAM 帳戶中，且屬於服務所有。IAM 管理員可以檢視但無法編輯服務連結角色的權限。

Lightsail 支援服務連結角色。如需有關建立或管理 Lightsail 服務連結角色的詳細資訊，請參閱[服務連結角色](#)。

### 服務角色

Lightsail 不支援服務角色。

## 主題

- [使用 Lightsail 中的IAM身分識別原則授予最低權限權限](#)
- [使IAM用原則授予特定 Lightsail 資源的存取權](#)
- [將服務連結角色用於 Amazon Lightsail](#)
- [使用 IAM 政策管理 Lightsail 值區](#)

## 使用 Lightsail 中的IAM身分識別原則授予最低權限權限

根據預設，IAM使用者和角色沒有建立或修改 Lightsail 資源的權限。他們也無法使用 AWS Management Console AWS CLI、或執行工作 AWS API。IAM管理員必須建立IAM政策，授與使用者和角色權限，才能對他們所需的指定資源執行特定API作業。然後，系統管理員必須將這些原則附加到需要這些權限的IAM使用者或群組。

若要瞭解如何使用這些範例原則文件建立以IAM身分識別為基礎的JSON策略，請參閱使用IAM者指南中的[JSON標籤上建立](#)策略。

### 政策最佳實務

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

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

- 需要多因素驗證 (MFA) — 如果您的案例需要使IAM用者或 root 使用者 AWS 帳戶，請開啟以取得額外MFA的安全性。若要在呼叫API作業MFA時需要，請在原則中新增MFA條件。如需詳細資訊，請參閱《IAM使用指南》中的 [< 設定MFA受保護的API存取 >](#)。

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

## 使用 Lightsail 台

若要存取 Amazon Lightsail 主控台，您必須擁有所有 Lightsail 動作和資源的完整存取權限。這些權限必須允許您列出並檢視 AWS 帳戶中 Lightsail 資源的詳細資料。如果您建立的以身分識別為基礎的原則，其限制性高於最低必要權限 (亦即非完整存取權)，則控制台將無法如預期用於具有該原則的實體 (IAM使用者或角色) 運作。

若要確保這些實體可以使用 Lightsail 主控台，請將下列原則附加至實體。如需詳細資訊，請參閱《[使用指南](#)》中的〈[將權限新增至IAM使用者](#)〉：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "lightsail:*"
      ],
      "Resource": "*"
    }
  ]
}
```

您不需要為只對 AWS CLI 或撥打電話的使用者允許最低主控台權限 AWS API。相反地，只允許存取與您嘗試執行之API作業相符的動作。

## 允許使用者檢視自己的許可

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

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

```

    "Effect": "Allow",
    "Action": [
      "iam:GetUserPolicy",
      "iam:ListGroupsWithUser",
      "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": "*"
  }
]
}

```

## 允許根據標籤建立和刪除 Lightsail 資源

您可以使用身分型原則中的條件，根據標籤來控制 Lightsail 資源的存取。此範例顯示如何建立政策，以限制使用者建立新的 Lightsail 資源，除非使用建立要求定義的索引鍵標記 `allow` 和值 `true`。此政策也會限制使用者刪除資源，除非他們具有 `allow/true` 索引鍵值標籤。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "lightsail:Create*",
        "lightsail:TagResource",
        "lightsail:UntagResource"
      ]
    }
  ]
}

```

```

    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:RequestTag/allow": "true"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "lightsail:Delete*",
      "lightsail:TagResource",
      "lightsail:UntagResource"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:ResourceTag/allow": "true"
      }
    }
  }
]
}

```

下列範例會限制使用者變更索引鍵值標籤並非 allow/false 之資源的標籤。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "lightsail:TagResource"
      ],
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:ResourceTag/allow": "false"
        }
      }
    }
  ]
}

```

```
}
```

您可以將這些策略附加到您帳IAM戶中的使用者。如需詳細資訊，請參閱《IAM使用指南》中的 [《IAMJSON策略元素：條件》](#)。

## 使IAM用原則授予特定 Lightsail 資源的存取權

資源層級許可一詞是指能夠讓您指定使用者可對其執行動作的資源。Amazon Lightsail 支援資源層級許可。這意味著對於某些 Lightsail 動作，您可以根據必須滿足的條件或允許使用者使用或編輯的特定資源來控制何時允許使用者使用這些動作。例如，您可以授與使用者管理具有特定 Amazon 資源名稱 (ARN) 的執行個體或資料庫的權限。

### Important

Lightsail 不支援某些動作的資源層級權限。API如需詳細資訊，請參閱[支援基於標籤的資源層級許可和授權](#)。

如需 Lightsail 動作建立或修改的資源，以及可在IAM政策陳述式中使用的ARNs和 Lightsail 條件金鑰的詳細資訊，請參閱使用者指南中的適用於[Amazon Lightsail 的動作、資源和條件金鑰](#)。IAM

### 允許管理特定執行個體

以下政策會授與存取權，以重新開機/啟動/停止執行個體、管理執行個體連接埠，以及建立特定執行個體的執行個體快照。它也提供 Lightsail 帳戶中其他執行個體相關資訊和資源的唯讀存取權。在原則中，取代 *InstanceARN* 使用您的實例的 Amazon 資源名稱 (ARN)。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "lightsail:GetActiveNames",
        "lightsail:GetAlarms",
        "lightsail:GetAutoSnapshots",
        "lightsail:GetBlueprints",
        "lightsail:GetBundles",
        "lightsail:GetCertificates",
        "lightsail:GetCloudFormationStackRecords",
        "lightsail:GetContactMethods",
```

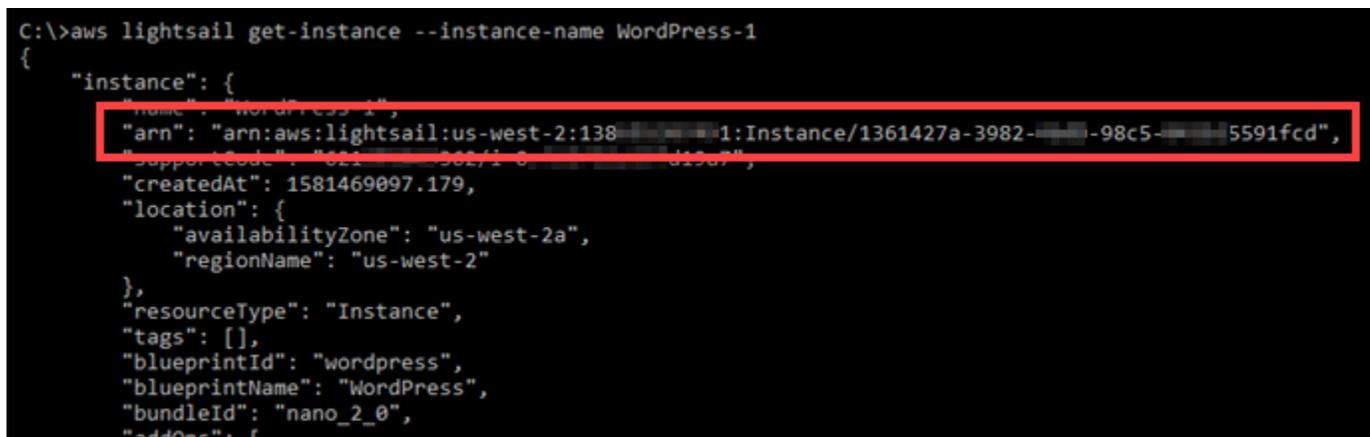
```
"lightsail:GetDisk",
"lightsail:GetDisks",
"lightsail:GetDiskSnapshot",
"lightsail:GetDiskSnapshots",
"lightsail:GetDistributionBundles",
"lightsail:GetDistributionLatestCacheReset",
"lightsail:GetDistributionMetricData",
"lightsail:GetDistributions",
"lightsail:GetDomain",
"lightsail:GetDomains",
"lightsail:GetExportSnapshotRecords",
"lightsail:GetInstance",
"lightsail:GetInstanceAccessDetails",
"lightsail:GetInstanceMetricData",
"lightsail:GetInstancePortStates",
"lightsail:GetInstances",
"lightsail:GetInstanceSnapshot",
"lightsail:GetInstanceSnapshots",
"lightsail:GetInstanceState",
"lightsail:GetKeyPair",
"lightsail:GetKeyPairs",
"lightsail:GetLoadBalancer",
"lightsail:GetLoadBalancerMetricData",
"lightsail:GetLoadBalancers",
"lightsail:GetLoadBalancerTlsCertificates",
"lightsail:GetOperation",
"lightsail:GetOperations",
"lightsail:GetOperationsForResource",
"lightsail:GetRegions",
"lightsail:GetRelationalDatabase",
"lightsail:GetRelationalDatabaseBlueprints",
"lightsail:GetRelationalDatabaseBundles",
"lightsail:GetRelationalDatabaseEvents",
"lightsail:GetRelationalDatabaseLogEvents",
"lightsail:GetRelationalDatabaseLogStreams",
"lightsail:GetRelationalDatabaseMetricData",
"lightsail:GetRelationalDatabaseParameters",
"lightsail:GetRelationalDatabases",
"lightsail:GetRelationalDatabaseSnapshot",
"lightsail:GetRelationalDatabaseSnapshots",
"lightsail:GetStaticIp",
"lightsail:GetStaticIps",
"lightsail:IsVpcPeered"
],
```

```

    "Resource": "*"
  },
  {
    "Sid": "VisualEditor2",
    "Effect": "Allow",
    "Action": [
      "lightsail:CloseInstancePublicPorts",
      "lightsail:CreateInstanceSnapshot",
      "lightsail:OpenInstancePublicPorts",
      "lightsail:PutInstancePublicPorts",
      "lightsail:RebootInstance",
      "lightsail:StartInstance",
      "lightsail:StopInstance"
    ],
    "Resource": "InstanceARN"
  }
]
}

```

若要取得執行個體的 ARN，請使用 `GetInstance` Lightsail API 動作，並使用 `instanceName` 參數指定執行個體的名稱。您的執行個體 ARN 將會列在該動作的結果中，如下列範例所示。如需詳細資訊，請參閱亞馬遜 Lightsail API 參考資料 [GetInstance](#) 中的。



```

C:\>aws lightsail get-instance --instance-name WordPress-1
{
  "instance": {
    "name": "WordPress-1",
    "arn": "arn:aws:lightsail:us-west-2:138-:1:Instance/1361427a-3982-98c5-5591fcd",
    "supportCode": "021-362/1-0-138-1387",
    "createdAt": 1581469097.179,
    "location": {
      "availabilityZone": "us-west-2a",
      "regionName": "us-west-2"
    },
    "resourceType": "Instance",
    "tags": [],
    "blueprintId": "wordpress",
    "blueprintName": "WordPress",
    "bundleId": "nano_2_0",
    "addOns": [

```

### 允許管理特定資料庫

下列政策會授與存取權，以重新開機/啟動/停止和更新特定資料庫。它也提供 Lightsail 帳戶中其他資料庫相關資訊和資源的唯讀存取權。在原則中，取代 *DatabaseARN* 使用數據庫的 Amazon 資源名稱 (ARN)。

```

{
  "Version": "2012-10-17",

```

```
"Statement": [  
  {  
    "Sid": "VisualEditor0",  
    "Effect": "Allow",  
    "Action": [  
      "lightsail:GetActiveNames",  
      "lightsail:GetAlarms",  
      "lightsail:GetAutoSnapshots",  
      "lightsail:GetBlueprints",  
      "lightsail:GetBundles",  
      "lightsail:GetCertificates",  
      "lightsail:GetCloudFormationStackRecords",  
      "lightsail:GetContactMethods",  
      "lightsail:GetDisk",  
      "lightsail:GetDisks",  
      "lightsail:GetDiskSnapshot",  
      "lightsail:GetDiskSnapshots",  
      "lightsail:GetDistributionBundles",  
      "lightsail:GetDistributionLatestCacheReset",  
      "lightsail:GetDistributionMetricData",  
      "lightsail:GetDistributions",  
      "lightsail:GetDomain",  
      "lightsail:GetDomains",  
      "lightsail:GetExportSnapshotRecords",  
      "lightsail:GetInstance",  
      "lightsail:GetInstanceAccessDetails",  
      "lightsail:GetInstanceMetricData",  
      "lightsail:GetInstancePortStates",  
      "lightsail:GetInstances",  
      "lightsail:GetInstanceSnapshot",  
      "lightsail:GetInstanceSnapshots",  
      "lightsail:GetInstanceState",  
      "lightsail:GetKeyPair",  
      "lightsail:GetKeyPairs",  
      "lightsail:GetLoadBalancer",  
      "lightsail:GetLoadBalancerMetricData",  
      "lightsail:GetLoadBalancers",  
      "lightsail:GetLoadBalancerTlsCertificates",  
      "lightsail:GetOperation",  
      "lightsail:GetOperations",  
      "lightsail:GetOperationsForResource",  
      "lightsail:GetRegions",  
      "lightsail:GetRelationalDatabase",  
      "lightsail:GetRelationalDatabaseBlueprints",
```

```

        "lightsail:GetRelationalDatabaseBundles",
        "lightsail:GetRelationalDatabaseEvents",
        "lightsail:GetRelationalDatabaseLogEvents",
        "lightsail:GetRelationalDatabaseLogStreams",
        "lightsail:GetRelationalDatabaseMetricData",
        "lightsail:GetRelationalDatabaseParameters",
        "lightsail:GetRelationalDatabases",
        "lightsail:GetRelationalDatabaseSnapshot",
        "lightsail:GetRelationalDatabaseSnapshots",
        "lightsail:GetStaticIp",
        "lightsail:GetStaticIps",
        "lightsail:IsVpcPeered"
    ],
    "Resource": "*"
},
{
    "Sid": "VisualEditor2",
    "Effect": "Allow",
    "Action": [
        "lightsail:RebootRelationalDatabase",
        "lightsail:StartRelationalDatabase",
        "lightsail:StopRelationalDatabase",
        "lightsail:UpdateRelationalDatabase"
    ],
    "Resource": "DatabaseARN"
}
]
}

```

若要取ARN得資料庫的，請使用 `GetRelationalDatabase` Lightsail API 動作，並使用 `relationalDatabaseName` 參數指定資料庫的名稱。您的數據庫ARN將在該操作的結果中列出，如下面的例子。如需詳細資訊，請參閱亞馬遜 Lightsail API 參考資料 [GetRelationalDatabase](#) 中的。

```

C:\>aws lightsail get-relational-database --relational-database-name Database-1
{
  "relationalDatabase": {
    "name": "Database-1",
    "arn": "arn:aws:lightsail:us-west-2:138111111111:RelationalDatabase/3fdf1bef-892c-4333-9ccf-110f67",
    "supportCode": "601111111111-111111111111-111111111111-111111111111",
    "createdAt": 1576533508.975,
    "location": {
      "availabilityZone": "us-west-2a",
      "regionName": "us-west-2"
    },
    "resourceType": "RelationalDatabase",
    "tags": [],
    "relationalDatabaseBlueprintId": "mysql_8_0",
    "relationalDatabaseBundleId": "micro_1_0",
    "masterDatabaseName": "dbmaster",
    "hardware": {

```

## 將服務連結角色用於 Amazon Lightsail

Amazon Lightsail 使用 AWS Identity and Access Management (IAM) [服務連結](#)角色。服務連結角色是一種獨特的 IAM 角色類型，可直接連結至 Amazon Lightsail。服務連結角色由 Amazon Lightsail 預先定義，並包含 Lightsail 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輕鬆地設定 Amazon Lightsail，因為您不必手動新增必要的許可。Amazon Lightsail 會定義其服務連結角色的許可，除非另有定義，否則只有 Amazon Lightsail 可以擔任其角色。定義的許可包含信任政策和許可政策，這些政策不能附接至任何其他 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。這樣可以保護您的 Amazon Lightsail 資源，因為您無法意外移除存取資源的權限。

如需支援服務連結角色其他服務的資訊，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 Yes (是) 的服務。選擇具有連結的 Yes (是)，以檢視該服務的服務連結角色文件。

### Amazon Lightsail 的服務連結角色許可

Amazon Lightsail 使用名為 AWSServiceRoleForLightsail— 角色的服務連結角色，將 Lightsail 執行個體和區塊儲存磁碟快照匯出到 Amazon 彈性運算雲端 (Amazon EC2)，並從 Amazon Simple Storage Service (Amazon S3) 取得目前帳戶層級區塊公開存取組態。

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

- `lightsail.amazonaws.com`

角色許可政策允許 Amazon Lightsail 在指定的資源上完成下列動作：

- 動作：`ec2:CopySnapshot`在所有 AWS 資源上。
- 動作：`ec2:DescribeSnapshots`在所有 AWS 資源上。
- 動作：`ec2:CopyImage`在所有 AWS 資源上。
- 動作：`ec2:DescribeImages`在所有 AWS 資源上。
- 動作：`cloudformation:DescribeStacks`在所有 AWS AWS CloudFormation 堆疊上。
- 動作：`s3:GetAccountPublicAccessBlock`在所有 AWS 資源上。

### 服務連結角色許可

您必須設定許可，IAM 實體 (如使用者、群組或角色) 才可建立或編輯服務連結角色的說明。

## 允許 IAM 實體建立特定服務連結角色

將下列政策新增至需要建立服務連結角色的 IAM 實體。

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

## 若要允許 IAM 實體建立任何服務連結角色

將下列陳述式新增至需要建立服務連結角色的 IAM 實體的許可政策，或包含所需政策的任何服務角色。此政策會見政策連接至角色。

```
{
  "Effect": "Allow",
  "Action": "iam:CreateServiceLinkedRole",
  "Resource": "arn:aws:iam::*:role/aws-service-role/*"
}
```

## 若要允許 IAM 實體編輯任何服務連結角色的說明

將下列陳述式新增至需要編輯服務連結角色說明或任何服務角色的 IAM 實體的許可政策。

```
{
  "Effect": "Allow",
  "Action": "iam:UpdateRoleDescription",
  "Resource": "arn:aws:iam::*:role/aws-service-role/*"
}
```

若要允許 IAM 實體刪除特定服務連結角色

將下列陳述式新增至需要刪除服務連結角色的 IAM 實體的許可政策。

```
{
  "Effect": "Allow",
  "Action": [
    "iam:DeleteServiceLinkedRole",
    "iam:GetServiceLinkedRoleDeletionStatus"
  ],
  "Resource": "arn:aws:iam::*:role/aws-service-role/lightsail.amazonaws.com/AWSServiceRoleForLightsail*"
}
```

允許 IAM 實體刪除任何服務角色

將下列陳述式新增至需要刪除服務連結角色或任何服務角色的 IAM 實體的許可政策。

```
{
  "Effect": "Allow",
  "Action": [
    "iam:DeleteServiceLinkedRole",
    "iam:GetServiceLinkedRoleDeletionStatus"
  ],
  "Resource": "arn:aws:iam::*:role/aws-service-role/*"
}
```

或者，您可以使用 AWS 受管理的策略來提供對服務的完整存取權。

## 為 Amazon Lightsail 建立服務連結角色

您不需要手動建立一個服務連結角色。當您將 Lightsail 執行個體或區塊儲存磁碟快照匯出至 Amazon EC2，或在、或 AWS API 中建立或更新 Lightsail 儲存貯體時 AWS CLI，Amazon Lightsail 會為您建立服務連結角色。AWS Management Console

若您刪除此服務連結角色，之後需要再次建立，您可以在帳戶中使用相同程序重新建立角色。當您將 Lightsail 執行個體或區塊儲存磁碟快照匯出至 Amazon EC2，或建立或更新 Lightsail 儲存貯體時，Amazon Lightsail 會再次為您建立服務連結角色。

### Important

您必須設定 IAM 許可，才能允許 Amazon Lightsail 建立服務連結角色。若要這樣做，請完成服務連結角色許可區段中的步驟。

## 編輯服務連結角色

Amazon Lightsail 不允許您編輯 AWSServiceRoleForLightsail 服務連結角色。因為有各種實體可能會參考服務連結角色，所以您無法在建立角色之後變更角色名稱。然而，您可使用 IAM 來編輯角色描述。如需更多資訊，請參閱 IAM 使用者指南中的[編輯服務連結角色](#)。

## 刪除 Amazon Lightsail 的服務連結角色

若您不再使用需要服務連結角色的功能或服務，我們建議您刪除該角色。如此一來，您就沒有未主動監控或維護的未使用實體。不過，您必須確認沒有任何 Amazon Lightsail 執行個體或磁碟快照處於擱置中的複製狀態，才能刪除 AWSServiceRoleForLightsail 服務連結角色。如需詳細資訊，請參閱[將快照匯出至 Amazon EC2](#)。

## 使用 IAM 手動刪除服務連結角色

使用 IAM 主控台或 AWS API 刪除 AWSServiceRoleForLightsail 服務連結角色。AWS CLI 如需詳細資訊，請參閱《IAM 使用者指南》中的[刪除服務連結角色](#)。

## 支援亞 Amazon Lightsail 服務連結角色的區域

Amazon Lightsail 支援在提供服務的所有區域中使用服務連結角色。如需有關 Lightsail 可在其中使用的區域的詳細資訊，請參閱 [Amazon Lightsail 區域](#)。

## 使用 IAM 政策管理 Lightsail 值區

下列政策授予使用者在 Amazon Lightsail 物件儲存服務中管理特定儲存貯體的存取權。此原則會透過 Lightsail 主控台 AWS Command Line Interface (AWS CLI)、AWS API 和 AWS 開發套件授予值區的存取權。在原則中，以要管理的值區名稱取代 `< BucketName >`。如需有關 IAM 政策的詳細資訊，請參閱《AWS Identity and Access Management 使用者指南》中的[建立 IAM 政策](#)。如需有關建立 IAM 使用者和使用者群組的詳細資訊，請參閱《AWS Identity and Access Management 使用者指南》中的[建立第一個 IAM 委派使用者和使用者群組](#)。

### Important

不具備此原則的使用者在 Lightsail 主控台中檢視值區管理頁面的 [物件] 索引標籤時，會遇到錯誤。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "LightsailAccess",
      "Effect": "Allow",
      "Action": "lightsail:*",
      "Resource": "*"
    },
    {
      "Sid": "S3BucketAccess",
      "Effect": "Allow",
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::<BucketName>/*",
        "arn:aws:s3:::<BucketName>"
      ]
    }
  ]
}
```

## 管理儲存貯體和物件

以下是管理 Lightsail 物件儲存貯體的一般步驟：

1. 了解 Amazon Lightsail 物件儲存服務中的物件和值區。如需詳細資訊，請參閱 [Amazon Lightsail 中的物件儲存](#)。
2. 了解您可以在 Amazon Lightsail 中為您的儲存貯體提供哪些名稱。如需詳細資訊，請參閱 [Amazon Lightsail 中的儲存貯體命名規則](#)。
3. 透過建立值區開始使用 Lightsail 物件儲存服務。如需詳細資訊，請參閱 [在 Amazon Lightsail 中建立值區](#)。
4. 了解儲存貯體的安全最佳實務，以及可以為儲存貯體設定的存取許可。可以將儲存貯體中的所有物件設為公有或私有，也可以選擇將個別物件設為公有。也可以透過建立存取金鑰、將執行個體附接至儲存貯體以及授予對其他 AWS 帳戶的存取權，來授予對儲存貯體的存取權。如需詳細資訊，請參閱 [Amazon Lightsail 物件儲存的安全最佳實務](#)和 [了解 Amazon Lightsail 中的儲存貯體許可](#)。

了解儲存貯體存取許可後，請參閱下列指南來授予對儲存貯體的存取權：

- [封鎖儲存貯體的公 Amazon Lightsail](#)
  - [在 Amazon Lightsail 中設定儲存貯體存取權限](#)
  - [在 Amazon Lightsail 中為儲存貯體中的個別物件設定存取權限](#)
  - [在 Amazon Lightsail 中為存儲桶創建訪問密鑰](#)
  - [在 Amazon Lightsail 中設定儲存貯體的資源存取](#)
  - [在 Amazon Lightsail 中設定儲存貯體的跨帳戶存取](#)
5. 了解如何為儲存貯體啟用存取日誌記錄，以及如何使用存取日誌來稽核儲存貯體的安全性。如需詳細資訊，請參閱下列指南。
    - [Amazon Lightsail 物件儲存服務中儲存貯體的存取記錄](#)
    - [存取 Amazon Lightsail 物件儲存服務中儲存貯體的日誌格式](#)
    - [在 Amazon Lightsail 物件儲存服務中啟用儲存貯體的存取記錄功能](#)
    - [在 Amazon Lightsail 中使用儲存貯體的存取日誌來識別請求](#)
  6. 建立 IAM 政策，讓使用者能夠在 Lightsail 中管理值區。如需詳細資訊，請參閱 [在 Amazon Lightsail 中管理儲存貯體的 IAM 政策](#)。
  7. 了解儲存貯體中物件的標記和識別方式。如需詳細資訊，請參閱 [了解 Amazon Lightsail 中的物件金鑰名稱](#)。
  8. 了解如何在儲存貯體中上傳檔案及管理物件。如需詳細資訊，請參閱下列指南。
    - [將文件上傳到 Amazon Lightsail](#)
    - [使用多部分上傳將檔案上傳到 Amazon Lightsail 中的儲存貯體](#)
    - [檢視儲存貯體中 Amazon Lightsail](#)
    - [在 Amazon Lightsail 中複製或移動值區中的物件](#)

- [從儲存貯體下 Amazon Lightsail](#)
  - [在 Amazon Lightsail 中過濾儲存桶中的對象](#)
  - [標記儲存桶中 Amazon Lightsail](#)
  - [刪除儲存桶中 Amazon Lightsail](#)
9. 啟用物件版本控制功能來保留、擷取和恢復儲存貯體中所儲存每個物件的各個版本。如需詳細資訊，請參閱在 [Amazon Lightsail 中啟用和暫停儲存貯體中的物件版本控制](#)。
  10. 啟用物件版本控制之後，可以還原儲存貯體中物件的先前版本。如需詳細資訊，請參閱在 [Amazon Lightsail 中還原儲存貯體中的舊版物件](#)。
  11. 監控儲存貯體的使用率。如需詳細資訊，請參閱在 [Amazon Lightsail 中檢視儲存貯體的指標](#)。
  12. 設定儲存貯體指標的警示，以便在儲存貯體的使用率超過閾值時收到通知。如需詳細資訊，請參閱在 [Amazon Lightsail 中建立儲存貯體指標警示](#)。
  13. 如果儲存空間和網路傳輸不足，請變更儲存貯體的儲存計畫。如需詳細資訊，請參閱在 [Amazon Lightsail 中變更儲存貯體的計畫](#)。
  14. 了解如何將儲存貯體連線至其他資源。如需詳細資訊，請參閱下列教學課程。
    - [教學課程：將 WordPress 執行個體連接至 Amazon Lightsail 儲存貯體](#)
    - [教學課程：將 Amazon Lightsail 儲存貯體與 Lightsail 內容交付網路分發搭配使用](#)
  15. 如果不再使用儲存貯體，請刪除它。如需詳細資訊，請參閱 [刪除儲存貯體](#)。

## 授與 Lightsail 用者的存取權限

身為 [AWS 帳戶根使用者](#) 或具有管理員存取權的 AWS Identity and Access Management (IAM) 使用者，您可以在 AWS 帳戶中建立一或多個 IAM 使用者，而這些使用者可以設定不同層級的存取權限 AWS。

對於 Amazon Lightsail，您可能想要建立一個只能存取 Lightsail 服務的 IAM 使用者。當有人加入您的團隊時，需要存取權才能檢視、建立、編輯或刪除 Lightsail 資源，但不需要存取其他提供的服務時，就可以執行 AWS 此操作。若要進行此設定，您必須先建立可授與 Lightsail 存取權的 IAM 政策，然後建立 IAM 群組，然後將該政策附加到群組。然後，您可以建立 IAM 使用者，並讓他們成為群組的成員，讓他們能夠存取 Lightsail。

當有人離開您的團隊時，您可以從 Lightsail 存取群組中移除該使用者，以撤銷他們對 Lightsail 的存取權，例如，他們離開您的團隊，但仍在您的公司工作。如果使用者離開公司且不再需要存取權，則可從 IAM 中刪除他們。

### ⚠ Warning

此案例需要具有程式設計存取權限和長期登入資料的 IAM 使用者，這會帶來安全風險。為了減輕此風險，我們建議您僅向這些使用者提供執行工作所需的權限，並在不再需要這些使用者時移除這些使用者。如有必要，可更新存取金鑰。如需詳細資訊，請參閱 IAM 使用者指南中的[更新存取金鑰](#)。

## 內容

- [建立存取權管理與存取權管理政策](#)
- [為 Lightsail 存取建立 IAM 群組，並附加存取政策](#)
- [建立 IAM 使用者，並將該使用者新增至 Lightsail 存取群組](#)

## 建立存取權管理與存取權管理政策

請依照下列步驟建立適用於 Lightsail 存取的 IAM 政策。如需詳細資訊，請參閱 IAM 文件中的[建立 IAM 政策](#)。

1. 登入 [IAM 主控台](#)。
2. 在左側導覽窗格中，選擇 Policies (政策)。
3. 選擇建立政策。
4. 在 Create Policy (建立政策) 頁面上，選擇 JSON 索引標籤。



```
1 - {  
2   "Version": "2012-10-17",  
3   "Statement": []  
4 }
```

5. 反白文字方塊的內容，然後複製該內容並貼到以下政策組態文字。

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

```

```

        "lightsail:*"
      ],
      "Resource": "*"
    }
  ]
}

```

結果應如下範例所示：

```

1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": [
7         "lightsail:*"
8       ],
9       "Resource": "*"
10    }
11  ]
12 }

```

這會授予對所有 Lightsail 動作和資源的存取權。需要存取其他服務的動作 (例如啟用 VPC 對等互連、將 Lightsail 快照匯出至 Amazon EC2 或使用 Lightsail 建立 Amazon EC2 資源) 需要此政策中未包含的其他許可。AWS 如需詳細資訊，請參閱下列指南：

- [設定 Amazon VPC 對等互連以使用 Amazon Lightsail 以外的 AWS 資源](#)
- [將亞馬遜快照匯出至 Amazon EC2](#)
- [從匯出的快照建立 Amazon EC2 執行個體](#)

如需您可授與的動作特定和資源特定許可的範例，請參閱 [Amazon Lightsail 資源層級許可政策範例](#)。

6. 選擇檢閱政策。
7. 在 Review Policy (檢閱政策) 頁面中，為政策命名。請設定一個描述名稱，例如 LightsailFullAccessPolicy。
8. 新增說明，然後檢閱政策設定。如需變更，請選擇 Previous (上一步) 來修改政策。

**Review policy**

**Name\***   
Use alphanumeric and '+,=, @, \_' characters. Maximum 128 characters.

**Description**   
Maximum 1000 characters. Use alphanumeric and '+,=, @, \_' characters.

**Summary**

Service	Access level	Resource	Request condition
Allow (1 of 176 services) <a href="#">Show remaining 175</a>			
Lightsail	Full access	All resources	None

9. 確定政策設定正確後，選擇 Create Policy (建立政策)。

政策現已建立完成且可新增至現有的 IAM 群組，或者您可以使用本指南下一節中的步驟來建立新的 IAM 群組。

## 為 Lightsail 存取建立 IAM 群組，並附加存取政策

請依照下列步驟為 Lightsail 存取建立 IAM 群組，然後附加本指南前一節中建立的 Lightsail 存取政策。如需詳細資訊，請參閱 IAM 文件中的[建立 IAM 群組](#)和[將政策附接至 IAM 群組](#)。

1. 在 [IAM 主控台](#) 的左側導覽窗格中，選擇群組。
2. 選擇 Create New Group (建立新群組)。
3. 在 Set Group Name (設定群組名稱) 頁面中，為群組命名。請設定一個描述名稱，例如 LightsailFullAccessGroup。
4. 在「附加原則」頁面中，搜尋您先前在本指南中建立的 Lightsail 原則，LightsailFullAccessPolicy 例如。
5. 在該政策旁新增核取記號，然後選擇 Next step (下一步)。
6. 檢閱群組設定。如需變更，請選擇 Previous (上一步) 來修改群組政策。
7. 確定群組設定正確後，選擇 Create Group (建立群組)。

現在已建立群組，新增至群組的使用者將可存取 Lightsail 動作和資源。您可以將現有的 IAM 使用者新增至該群組，或使用本指南下一節中的步驟來建立新的 IAM 使用者。

## 建立 IAM 使用者，並將該使用者新增至 Lightsail 存取群組

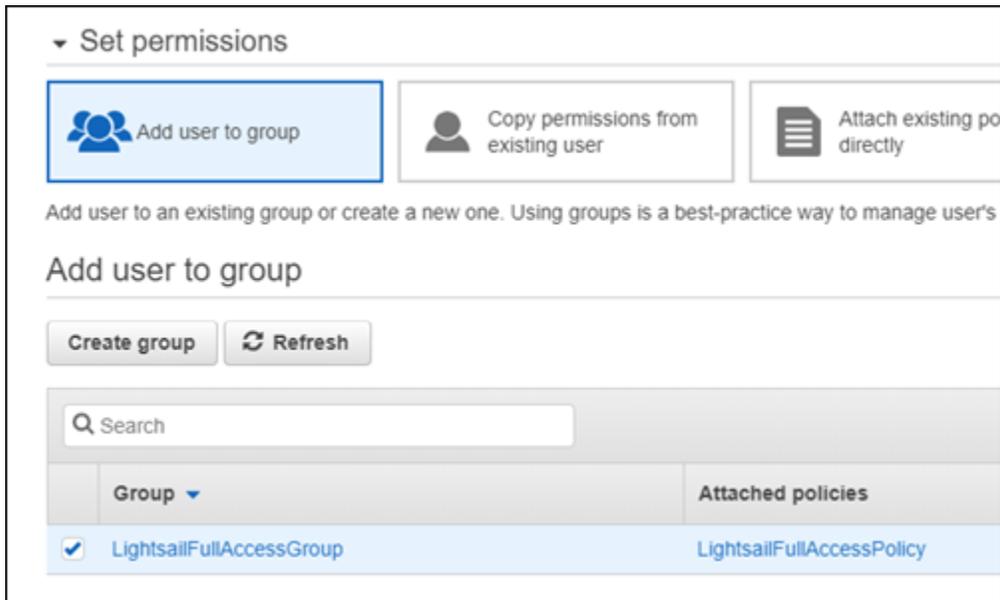
請依照下列步驟建立 IAM 使用者，並將該使用者新增至 Lightsail 存取群組。如需詳細資訊，請參閱 IAM 文件中的[在您的 AWS 帳戶中建立 IAM 使用者](#)以及[在 IAM 群組中新增和移除使用者](#)。

1. 在 [IAM 主控台](#) 的左側導覽窗格中，選擇使用者。
2. 選擇 Add user (新增使用者)。
3. 在該頁面的 Set user details (設定使用者詳細資訊) 區段中，為使用者命名。
4. 在頁面的「選 AWS 存取類型」段落下，選擇下列選項：
  - a. 選擇「程式設計存取」可為 AWS API、CLI、SDK 和其他開發工具 (可用於 Lightsail 動作和資源) 啟用存取金鑰 ID 和秘密存取金鑰。如需詳細資訊，請參閱[設 AWS CLI 定使用 Lightsail](#)。
  - b. 選擇 AWS 管理主控台存取以啟用密碼，讓使用者登入 AWS 管理主控台，從而登入 Lightsail 主控台。當您選取此選項時，即會顯示下列密碼選項：
    - i. 選擇自動產生密碼，讓 IAM 產生密碼，或選擇「自訂密碼」來輸入您自己的密碼。
    - ii. 選擇 Require password reset (需要密碼重設)，則使用者下次登入時就必須建立新的密碼 (重設密碼)。

### Note

如果您僅選擇「程式設計存取」選項，則使用者將無法登入 AWS 主控台和 Lightsail 主控台。

5. 選擇下一步：許可。
6. 在頁面的 [設定權限] 區段下，選擇 [新增使用者至群組]，然後選取您先前在本指南中建立的 Lightsail 存取群組，LightsailFullAccessGroup 例如。



7. 選擇 Next: Tags (下一步：標籤)。
8. (選用) 藉由連接標籤做為索引鍵/值組，將中繼資料新增至使用者。如需在 IAM 中使用標籤的詳細資訊，請參閱標記 IAM 實體。
9. 選擇下一步：檢閱。
10. 檢閱使用者設定。如需變更，請選擇 Previous (上一步) 來修改使用者群組或政策。
11. 確定使用者設定正確後，選擇 Create user (建立使用者)。

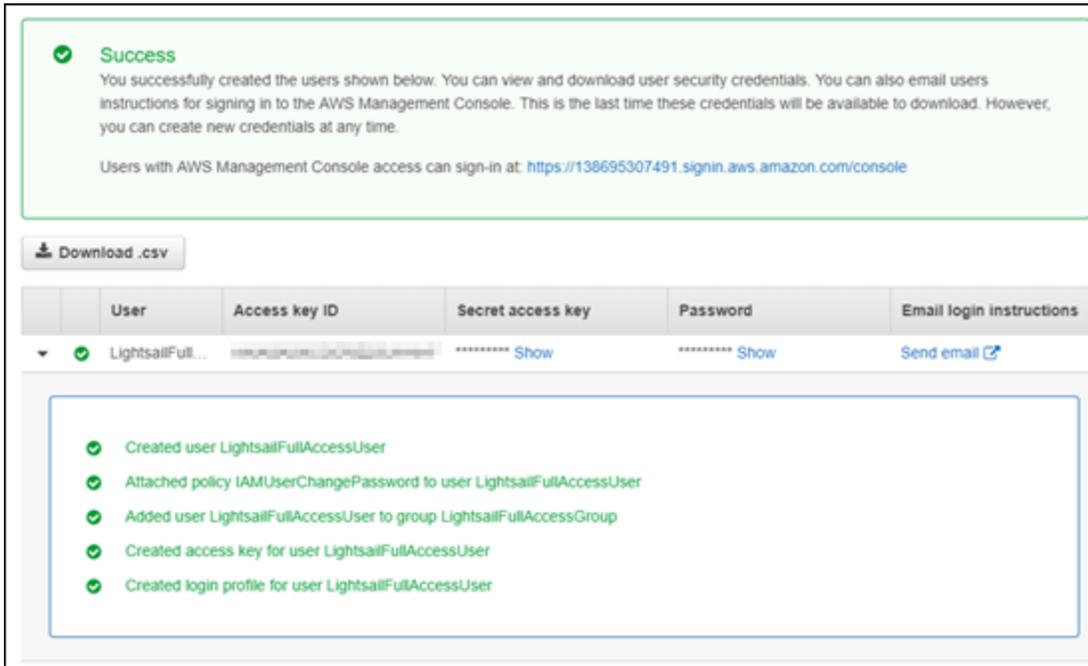
使用者已建立，而且使用者將可以存取 Lightsail。若要撤銷使用者的 Lightsail 存取權，請從 Lightsail 存取群組中移除該使用者。如需詳細資訊，請參閱 IAM 文件中的[在 IAM 群組中新增和移除使用者](#)。

12. 若要取得使用者的登入資料，則可選擇下列選項：
  - a. 選擇 [下載 .csv] 以下載包含您帳戶的使用者名稱、密碼、存取金鑰 ID、秘密存取金鑰和 AWS 主控台登入連結的檔案。
  - b. 選擇 [秘密存取金鑰] 下的 [顯示]，以檢視可用來以程式設計方式存取 Lightsail 的存取金鑰 (使用 AWS API、CLI、SDK 和其他開發工具)。

**⚠ Important**

這是您檢視或下載秘密存取金鑰的唯一機會，您必須先將此資訊提供給使用者，才能使用 AWS API。請將使用者的新存取金鑰 ID 和秘密存取金鑰存放在安全處。在此步驟之後，您將無法再存取該私密金鑰。

- c. 選擇密碼下的顯示，以檢視使用者的密碼 (如果密碼是由 IAM 所產生)。您應提供密碼給使用者，讓他們進行第一次登入。
- d. 選擇 [傳送電子郵件] 以傳送電子郵件給使用者，讓他們知道他們現在可以存取 Lightsail。



## 透過更新管理確保 Lightsail 執行個體和容器的安全

Amazon Web Services (AWS)、Amazon Lightsail 和第三方應用程式供應商會定期更新和修補 Lightsail 上可用的執行個體映像 (也稱為藍圖)。AWS 且 Lightsail 不會在您建立執行個體之後更新或修補執行個體上的作業系統或應用程式。Lightsail 也不會更新或修補您在 Lightsail 容器服務上設定的作業系統和軟體。因此，我們建議您定期更新、修補和保護 Amazon Lightsail 執行個體和容器服務上的作業系統和應用程式。如需詳細資訊，請參閱 [AWS 共同責任模型](#)。

### 執行個體藍圖軟體支援

下列 Amazon Lightsail 平台和藍圖清單連結到每個廠商的支援頁面。您可以在這裡檢視資訊，例如操作指南，以及讓作業系統和應用程式保持在最新狀態。您也可以使用任何自動更新服務或建議的程序，以安裝應用程式廠商提供的更新。

#### Windows

- [視窗伺服器 2022, 視窗伺服器 2019, 視窗伺服器](#)
- [Microsoft SQL Server](#)

## Linux 和 Unix - 僅限作業系統

- [Amazon Linux 2023](#)
- [Amazon Linux 2](#)
- [Ubuntu](#)
- [Debian](#)
- [FreeBSD](#)
- [openSUSE](#)
- [CentOS](#)

## Linux 和 Unix - 作業系統加上應用程式

- [Plesk Hosting Stack on Ubuntu \(Ubuntu 上的 Plesk 託管堆疊\)](#)
- [適用於 Linux 的 cPanel & WHM](#)
- [WordPress](#)
- [WordPress 多站點](#)
- [LAMP \(PHP 8\)](#)
- [Node.js](#)
- [Joomla!](#)
- [Magento](#)
- [MEAN](#)
- [Drupal](#)
- [GitLab 特首](#)
- [Redmine](#)
- [Nginx](#)
- [Ghost](#)
- [Django](#)
- [PrestaShop](#)

## 驗證 Amazon Lightsail 資源的合規性

AWS 提供下列資源以協助遵循法規：

- [安全性與合規性快速入門指南](#) — 這些部署指南討論架構考量，並提供在上部署以安全性和法規遵循為重點的基準環境的步驟。AWS
- [AWS 法規遵循資源](#) — 此工作簿和指南集合可能適用於您的產業和所在地。
- [使用AWS Config 開發人員指南中的規則評估資源](#) — 此 AWS Config 服務會評估您的資源組態符合內部實務、產業準則和法規的程度。
- [AWS Security Hub](#) — 此 AWS 服務提供安全狀態的全面檢視，協助您檢查您 AWS 是否符合安全性產業標準和最佳做法。

# 監控您 Lightsail 源指標

透過檢查並收集 Amazon Lightsail 中的執行個體、資料庫、分發、負載平衡器、容器服務和儲存貯體的效能，以監控其指標資料。建立一段時間的基準，那麼您就可以設定警示，以便更輕鬆地偵測資源效能的異常情況和問題。

Amazon Lightsail 會報告執行個體、資料庫、內容交付網路 (CDN) 分發、負載平衡器、容器服務和儲存貯體的指標資料。您可以在 Lightsail 主控台中檢視和監視這些資料。監控是維護資源可靠性、可用性與效能的重要環節。定期監控並從您的資源收集指標資料，即可更輕鬆地進行多點失敗的偵錯。

## 內容

- [有效監控您的資源](#)
- [指標概念和術語](#)
- [Lightsail 中的可用度量](#)

## 有效監控您的資源

您應該在環境中建立正常資源效能的基準。在不同的時間及負載條件下測量效能。當您監控資源時，您應該寫下並記錄一段時間內資源效能的歷程記錄。將資源的目前效能與您所收集的歷史資料進行比較。這可協助您識別正常效能模式和效能異常情況，並策劃解決這些情況的方法。

例如，您可以監控執行個體的 CPU 使用率、網路使用率和狀態檢查。若效能不符合您所建立的基準，您可能需要重新設定或將執行個體最佳化，以降低 CPU 使用率或降低網路流量。如果您的執行個體持續運作超過 CPU 使用率閾值，您可能想要為您的執行個體切換到更大的計劃 (使用每月 \$7 美元/月計劃，而不是每月 5 美元計劃)。您可以為執行個體建立新的快照，然後使用較大型的方案從快照建立新執行個體，以切換至較大型的方案。

建立基準之後，您可以在 Lightsail 主控台中設定警示，以便在資源超過指定閾值時通知您。如需詳細資訊，請參閱[通知](#)和[警示](#)。

## 指標概念和術語

下列術語和概念可協助您更好地瞭解 Lightsail 中度量的使用情況。

## 指標

指標代表按時間順序排列的資料集點。您可以將指標視為您所監控的變數，且資料點代表該變數隨著時間的值。指標是由名稱唯一定義。例如，Lightsail 提供的某些執行個體度量包括 CPU 使用率 (CPUUtilization)、傳入網路流量 (NetworkIn) 和外送網路流量 (NetworkOut)。如需 Lightsail 中所有可用資源量度的詳細資訊，請參閱 Lightsail [中可用的量度](#)。

## 指標保留

含少於 60 秒期間 (1 分鐘解析度) 的資料點可供使用 15 天。含少於 300 秒期間 (5 分鐘解析度) 的資料點可供使用 63 天。含少於 3600 秒期間 (1 小時解析度) 的資料點可供使用 455 天 (15 個月)。

原先以較短期間提供的資料點會一起彙總，以供長期儲存。例如，具有 1 分鐘精細程度的資料點 (1 分鐘解析度) 仍可供使用 15 天。在 15 天候，此資料仍可供使用，但會進行彙總並以僅 5 分鐘的解析度可供擷取。在 63 天候，此資料會進一步進行彙總並以僅 1 小時的解析度可供使用。如果您需要超過這些期間的指標可用性，您可以使用 Lightsail API、AWS Command Line Interface (AWS CLI) 和 SDK 來擷取離線或不同儲存空間的資料點。

如需詳細資訊 [GetInstanceMetricData](#) [GetBucketMetricData](#)，請參閱

〈〉 [GetLoadBalancerMetricData](#) [GetDistributionMetricData](#)、[GetRelationalDatabaseMetricData](#) 〈Lightsail〉和 〈

## 統計資料

指標統計資料是在一段時間內彙總資料的方法。統計資料範例包括 Average、Sum 和 Maximum。例如，使用 Average 統計資料可用來平均執行個體 CPU 使用率指標資料、Sum 統計資料可用來新增資料庫連線、Maximum 統計資料可用來擷取最大負載平衡器回應時間等等。

如需可用測量結果統計資料的清單，請參閱 [Lightsail API 參考](#) [GetRelationalDatabaseMetricData](#) 中的 [GetBucketMetricData](#) 統計資料 [GetLoadBalancerMetricData](#)、[統計資料](#) [GetDistributionMetricData](#)、[統計資料](#)、[統計資料](#) 以及 [統計資料](#)。 [GetInstanceMetricData](#)

## 單位

每個統計單位有量測單位。範例單位包括 Bytes、Seconds、Count 和 Percent。[如需完整的單位清單](#)，請參閱 [Lightsail API 參考資料](#) [GetRelationalDatabaseMetricData](#) 中的 [單位](#) [GetDistributionMetricData](#)、[單位](#)、[單位](#) 和 [單位](#)。 [GetInstanceMetricData](#) [GetLoadBalancerMetricData](#)

## 期間

期間是與特定資料點相關聯的時間長度 - 所傳回資料點的精細程度。每個資料點都代表在指定的期間內收集的指標資料彙總。期間會以秒定義，期間的有效值為 60 秒 (1 分鐘) 和 300 秒 (5 分鐘) 的倍數。

使用 Lightsail API 擷取資料點時，您可以指定期間、開始時間和結束時間。這些參數會判斷與資料點相關的整體時間長度。Lightsail 會以 1 分鐘或 5 分鐘的增量來報告量度資料；因此，您必須以 60 秒和 300 秒的倍數來指定期間。您為開始時間和結束時間指定的值會決定 Lightsail 傳回多少個期間。如果您偏好在十分鐘區塊內彙總的統計資料，指定期間為 600。對於在整個小時彙總的統計資料，將期間指定為 3600。

週期對於 Lightsail 警報也很重要。Lightsail 每 5 分鐘評估一次警示的資料點，而警示的每個資料點則代表 5 分鐘的彙總資料期間。當您建立警示來監控特定量度時，您會要求 Lightsail 將該量度與您指定的臨界值進行比較。您可以廣泛控制 Lightsail 進行比較的方式。您可以指定比較進行的期間，但也可以指定在總結時使用的評估期間數量。如需詳細資訊，請參閱 [警示](#)。

## 警示

警示會在指定的期間內監視單一指標，並在指標超過您指定的閾值時通知您。通知可以是 Lightsail 主控台中顯示的橫幅、傳送至您指定的電子郵件地址的電子郵件，以及傳送至您指定之行動電話號碼的 SMS 文字訊息。如需詳細資訊，請參閱 [警示](#)。

## Lightsail 中的可用度量

### 執行個體指標

以下是可用的執行個體指標。如需詳細資訊，請參閱在 [Amazon Lightsail 中檢視執行個體指標](#)。

- **CPU 使用率 (CPUUtilization)** – 執行個體上目前正在使用的已配置運算單位百分比。此指標可識別在執行個體上執行應用程式的處理能力。如果執行個體未配置完整的處理器核心，作業系統中的工具所顯示的百分比可能會低於 Lightsail。

在 Lightsail 主控台中檢視執行個體的 CPU 使用率指標圖表時，您會看到永續且高載的區域。如需這些區域代表意義的詳細資訊，請參閱 [CPU 使用率永續和可高載區域](#)。

- **高載容量分鐘 (BurstCapacityTime) 與百分比 (BurstCapacityPercentage)** – 高載容量分鐘代表執行個體以 100% CPU 使用率高載的可用時間量。高載容量百分比是執行個體可用的 CPU 效能百分比。您的執行個體會持續耗用並累積高載容量。只有當您的執行個體以 100% CPU 使用率運作時，才會以全速耗用高載容量分鐘。如需執行個體爆發容量的詳細資訊，請參閱在 [Amazon Lightsail 中檢視執行個體爆發容量](#)。

- **傳入網路流量 (NetworkIn)** – 執行個體在所有網路介面上收到的位元組數目。此指標可識別執行個體的傳入網路流量數量。所報告的數目是在期間內收到的位元組總數。因為此指標的報告間隔為 5 分鐘，所以將報告的數字除以 300 可找出每秒的位元組數。
- **傳出網路流量 (NetworkOut)** – 執行個體在所有網路介面上送出的位元組數目。此指標可識別來自執行個體的傳出網路流量數量。所報告的數目是在期間內送出的位元組總數。因為此指標的報告間隔為 5 分鐘，所以將報告的數字除以 300 可找出每秒的位元組數。
- **狀態檢查失敗 (StatusCheckFailed)** – 報告執行個體是否通過執行個體狀態檢查與系統狀態檢查。此指標可以是 0 (通過) 或 1 (失敗)。此指標是以 1 分鐘的頻率提供。
- **執行個體狀態檢查失敗 (StatusCheckFailed\_Instance)** – 報告執行個體是否通過執行個體狀態檢查。此指標可以是 0 (通過) 或 1 (失敗)。此指標是以 1 分鐘的頻率提供。
- **系統狀態檢查失敗 (StatusCheckFailed\_System)** – 報告執行個體是否通過系統狀態檢查。此指標可以是 0 (通過) 或 1 (失敗)。此指標是以 1 分鐘的頻率提供。
- **無字符中繼資料請求 (MetadataNoToken)** – 已在無字符的情況下成功存取執行個體中繼資料服務的次數。此指標可判斷是否有任何使用執行個體中繼資料服務第 1 版的程序，在未使用字符的情況下存取執行個體中繼資料。如果所有請求都使用字符後端工作階段 (例如執行個體中繼資料服務第 2 版)，則值為 0。如需詳細資訊，請參閱 [Amazon Lightsail 中的執行個體中繼資料和使用者](#) 資料。

## 資料庫指標

以下是可用的資料庫指標。如需詳細資訊，請參閱 [在 Amazon Lightsail 中檢視資料庫指標](#)。

- **CPU 使用率 (CPUUtilization)** – 資料庫目前使用的 CPU 使用率百分比。
- **資料庫連線 (DatabaseConnections)** – 使用中的資料庫連線數量。
- **磁碟佇列深度 (DiskQueueDepth)** – 正在等待存取磁碟的未完成 IO (讀/寫請求) 數量。
- **可用儲存空間 (FreeStorageSpace)** – 可用儲存空間的數量。
- **網路接收輸送量 (NetworkReceiveThroughput)** – 資料庫的傳入 (接收) 網路流量，包括客戶資料庫流量及用於監控與複寫的 AWS 流量。
- **網路傳輸輸送量 (NetworkTransmitThroughput)** – 資料庫的傳出 (傳輸) 網路流量，包括客戶資料庫流量及用於監控與複寫的 AWS 流量。

## 分發指標

以下為可供使用的分發指標。如需詳細資訊，請參閱 [在 Amazon Lightsail 中檢視分佈指標](#)。

- 請求 (**Requests**) – 對於所有 HTTP 方法以及 HTTP 和 HTTPS 請求，您的分發收到的檢視器請求總數。
- 上傳的位元組 (**BytesUploaded**) – 使用 POST 和 PUT 請求，透過您的分發上傳至原始伺服器的位元組數量。
- 下載的位元組 (**BytesDownloaded**) – 檢視器為 GET、HEAD 及 OPTIONS 請求下載的位元組數量。
- 總錯誤率 (**TotalErrorRate**) – 當回應的 HTTP 狀態碼為 4xx 或 5xx 時，全部檢視器請求的百分比。
- HTTP 4xx 錯誤率 (**4xxErrorRate**) – 當回應的 HTTP 狀態碼為 4xx 時，全部檢視器請求的百分比。在這些情況下，用戶端或用戶端檢視器可能發生錯誤。例如，404 (未找到) 狀態碼表示未找到用戶端請求的物件。
- HTTP 5xx 錯誤率 (**5xxErrorRate**) – 當回應的 HTTP 狀態碼為 5xx 時，全部檢視器請求的百分比。在這些情況下，原始伺服器不滿足要求。例如，503 (服務無法使用) 狀態碼表示原始伺服器目前無法使用。

## 負載平衡器指標

以下是可用的負載平衡器指標。如需詳細資訊，請參閱在 [Amazon Lightsail 中檢視負載平衡器指標](#)。

- 狀態正常的主機計數 (**HealthyHostCount**) – 視為狀態正常的目標執行個體數目。
- 狀態不正常的主機計數 (**UnhealthyHostCount**) – 視為狀態不正常目標執行個體數目。
- 負載平衡器 HTTP 4XX (**HTTPCode\_LB\_4XX\_Count**) – 源自於負載平衡器的 HTTP 4XX 用戶端錯誤碼數目。要求的格式不正確或不完整時，會產生用戶端錯誤。目標執行個體並未收到這些請求。此計數不包含目標執行個體產生的回應碼。
- 負載平衡器 HTTP 5XX (**HTTPCode\_LB\_5XX\_Count**) – 源自於負載平衡器的 HTTP 5XX 伺服器錯誤碼數目。其中不包含目標執行個體產生的任何回應碼。如果沒有狀態正常的執行個體附加至負載平衡器，或如果請求率超過執行個體 (溢出) 或負載平衡器的容量，則會回報此指標。
- 執行個體 HTTP 2XX (**HTTPCode\_Instance\_2XX\_Count**) – 目標執行個體所產生的 HTTP 2XX 回應碼數目。這未包含負載平衡器所產生的任何回應碼。
- 執行個體 HTTP 3XX (**HTTPCode\_Instance\_3XX\_Count**) – 目標執行個體所產生的 HTTP 3XX 回應碼數目。這未包含負載平衡器所產生的任何回應碼。
- 執行個體 HTTP 4XX (**HTTPCode\_Instance\_4XX\_Count**) – 目標執行個體所產生的 HTTP 4XX 回應碼數目。這未包含負載平衡器所產生的任何回應碼。

- 執行個體 HTTP 5XX (**HTTPCode\_Instance\_5XX\_Count**) – 目標執行個體所產生的 HTTP 5XX 回應碼數目。這未包含負載平衡器所產生的任何回應碼。
- 執行個體回應時間 (**InstanceResponseTime**) – 請求離開負載平衡器之後到收到目標執行個體回應之前所經歷的時間 (秒)。
- 用戶端 TLS 交涉錯誤計數 (**ClientTLSNegotiationErrorCount**) – 由於負載平衡器產生的 TLS 錯誤未與負載平衡器建立工作階段之用戶端所啟動的 TLS 連線數目。可能的原因包含晶片或協定不相符。
- 請求計數 (**RequestCount**) – 透過 IPv4 處理的請求數目。此計數只包含具有負載平衡器目標執行個體所產生之回應的要求。
- 拒絕的連線計數 (**RejectedConnectionCount**) – 因負載平衡器已達其連線數目上限而拒絕的連線數目。

## 容器服務指標

以下容器服務指標可供使用。如需詳細資訊，請參閱[檢視容器服務指標](#)。

- CPU 使用率 (**CPUUtilization**) – 目前在容器服務上跨全部節點使用之運算單位的平均百分比。此指標可識別在容器服務上執行容器所需的處理能力。
- 記憶體使用率 (**MemoryUtilization**) – 目前在容器服務上跨全部節點使用之記憶體的平均百分比。此指標會識別在容器服務上執行容器所需的記憶體。

## 儲存貯體指標

以下儲存貯體指標可供使用。如需詳細資訊，請參閱在 [Amazon Lightsail 中檢視儲存貯體指標](#)。

- 儲存貯體大小 (**BucketSizeBytes**) – 儲存貯體中儲存的資料量。此值是加總儲存貯體中所有物件的大小 (包含最新和非最新物件) 而計算得出，包括所有分段上傳到儲存貯體的所有不完整部分的大小。
- 物件數量 (**NumberOfObjects**) – 儲存貯體中儲存的物件總數。此值是計算儲存貯體中所有物件的數量 (包含最新和非最新物件) 以及所有分段上傳到儲存貯體的所有不完整部分的總數而計算得出。

### Note

當您的儲存貯體為空時，不會報告儲存貯體指標資料。

## 使用健康指標監控 Lightsail 資源

您可以檢視不同時段內的下列 Amazon Lightsail 資源指標。如需 Lightsail 中資源度量的詳細資訊，請參閱[資源量度](#)。

### 執行個體指標

以下是可用的執行個體指標。如需詳細資訊，請參閱[在 Amazon Lightsail 中檢視執行個體指標](#)。

- **CPUUse (CPUUtilization)** — 目前在執行個體上使用的已配置運算單元百分比。此指標可識別在執行個體上執行應用程式的處理能力。如果執行個體未配置完整的處理器核心，作業系統中的工具所顯示的百分比可能會低於 Lightsail。

在 Lightsail 主控台中檢視執行個體的 CPU 使用率指標圖表時，您會看到可持續且高載的區域。有關這些區域意味著什麼的更多信息，請參閱[CPU 利用率可持續和高載區域](#)。

- **突發容量分鐘 (BurstCapacityTime)** 和百分比 (**BurstCapacityPercentage**) — 突發容量分鐘代表執行個體以 100% CPU 使用率爆發的可用時間量。成組分解容量百分比是執行個體可用的 CPU 效能百分比。您的執行個體會持續耗用並累積高載容量。只有在執行個體以 100% CPU 使用率運作時，才會以完整速率消耗突發容量分鐘。如需有關執行個體高載容量的詳細資訊，請參閱[檢視執行個體高載容量](#)。
- **傳入網路流量 (NetworkIn)** – 執行個體在所有網路介面上收到的位元組數目。此指標可識別執行個體的傳入網路流量數量。所報告的數目是在期間內收到的位元組總數。因為此指標的報告間隔為 5 分鐘，所以將報告的數字除以 300 可找出每秒的位元組數。
- **傳出網路流量 (NetworkOut)** – 執行個體在所有網路介面上送出的位元組數目。此指標可識別來自執行個體的傳出網路流量數量。所報告的數目是在期間內送出的位元組總數。因為此指標的報告間隔為 5 分鐘，所以將報告的數字除以 300 可找出每秒的位元組數。
- **狀態檢查失敗 (StatusCheckFailed)** – 報告執行個體是否通過執行個體狀態檢查與系統狀態檢查。此指標可以是 0 (通過) 或 1 (失敗)。此指標是以 1 分鐘的頻率提供。
- **執行個體狀態檢查失敗 (StatusCheckFailed\_Instance)** – 報告執行個體是否通過執行個體狀態檢查。此指標可以是 0 (通過) 或 1 (失敗)。此指標是以 1 分鐘的頻率提供。
- **系統狀態檢查失敗 (StatusCheckFailed\_System)** – 報告執行個體是否通過系統狀態檢查。此指標可以是 0 (通過) 或 1 (失敗)。此指標是以 1 分鐘的頻率提供。
- **系統狀態檢查失敗 (StatusCheckFailed\_System)** – 報告執行個體是否通過系統狀態檢查。此指標可以是 0 (通過) 或 1 (失敗)。此指標是以 1 分鐘的頻率提供。
- **無字符中繼資料請求 (MetadataNoToken)** – 已在無字符的情況下成功存取執行個體中繼資料服務的次數。此指標可判斷是否有任何使用執行個體中繼資料服務第 1 版的程序，在未使用字符的情況

下存取執行個體中繼資料。如果所有請求都使用字符後端工作階段 (例如執行個體中繼資料服務第 2 版)，則值為 0。如需詳細資訊，請參閱[執行個體中繼資料和使用者資料](#)。

## 資料庫指標

以下是可用的資料庫指標。如需詳細資訊，請參閱[檢視資料庫指標](#)。

- CPUuse (**CPUUtilization**) — 資料庫中目前正在使用的使用CPU率百分比。
- 資料庫連線 (**DatabaseConnections**) – 使用中的資料庫連線數量。
- 磁碟佇列深度 (**DiskQueueDepth**) — 等待存取磁碟的未處理 IOs (讀取/寫入要求) 數目。
- 可用儲存空間 (**FreeStorageSpace**) – 可用儲存空間的數量。
- 網路接收輸送量 (**NetworkReceiveThroughput**) – 資料庫的傳入 (接收) 網路流量，包括客戶資料庫流量及用於監控與複寫的 AWS 流量。
- 網路傳輸輸送量 (**NetworkTransmitThroughput**) – 資料庫的傳出 (傳輸) 網路流量，包括客戶資料庫流量及用於監控與複寫的 AWS 流量。

## 分發指標

以下為可供使用的分發指標。如需詳細資訊，請參閱在 [Amazon Lightsail 中檢視分佈指標](#)。

- 請求 — 您的分發、所有HTTP方法以及和請求收到的查看者HTTPHTTPS請求總數。
- 已上傳的位元組數 — 您的發行版、使用POST和PUT要求上傳至來源的位元組數。
- 已下載位元組 — 檢視器為GET、HEAD和OPTIONS請求下載的位元組數。
- 總錯誤率 — 回應HTTP狀態碼為 4xx 或 5xx 之所有檢視者要求的百分比。
- HTTP4xx 錯誤率 — 回應HTTP狀態碼為 4xx 之所有檢視者要求的百分比。在這些情況下，用戶端或用戶端檢視器可能發生錯誤。例如，404 (未找到) 狀態碼表示未找到用戶端請求的物件。
- HTTP5xx 錯誤率 — 回應HTTP狀態碼為 5xx 之所有檢視者要求的百分比。在這些情況下，原始伺服器不滿足要求。例如，503 (服務無法使用) 狀態碼表示原始伺服器目前無法使用。

## 負載平衡器指標

以下是可用的負載平衡器指標。如需詳細資訊，請參閱[檢視負載平衡器指標](#)。

- 狀態正常的主機計數 (**HealthyHostCount**) – 視為狀態正常的目標執行個體數目。

- 狀態不正常的主機計數 (**UnhealthyHostCount**) – 視為狀態不正常的目標執行個體數目。
- 負載平衡器 HTTP 4XX (**HTTPCode\_LB\_4XX\_Count**) — 源自負載平衡器的 HTTP 4XX 用戶端錯誤代碼數目。要求的格式不正確或不完整時，會產生用戶端錯誤。目標執行個體並未收到這些請求。此計數不包含目標執行個體產生的回應碼。
- 負載平衡器 HTTP 5XX (**HTTPCode\_LB\_5XX\_Count**) — 源自負載平衡器的 HTTP 5XX 伺服器錯誤代碼數目。其中不包含目標執行個體產生的任何回應碼。如果沒有狀態正常的執行個體附加至負載平衡器，或如果請求率超過執行個體 (溢出) 或負載平衡器的容量，則會回報此指標。
- 執行處理 HTTP 2XX (**HTTPCode\_Instance\_2XX\_Count**) — 目標執行處理產生的 HTTP 2XX 回應代碼數目。這未包含負載平衡器所產生的任何回應碼。
- 執行處理 HTTP 3XX (**HTTPCode\_Instance\_3XX\_Count**) — 目標執行處理產生的 HTTP 3XX 回應代碼數目。這未包含負載平衡器所產生的任何回應碼。
- 執行處理 HTTP 4XX (**HTTPCode\_Instance\_4XX\_Count**) — 目標執行處理產生的 HTTP 4XX 回應代碼數目。這未包含負載平衡器所產生的任何回應碼。
- 執行處理 HTTP 5XX (**HTTPCode\_Instance\_5XX\_Count**) — 目標執行處理產生的 HTTP 5XX 回應代碼數目。這未包含負載平衡器所產生的任何回應碼。
- 執行個體回應時間 (**InstanceResponseTime**) – 請求離開負載平衡器之後到收到目標執行個體回應之前所經歷的時間 (秒)。
- 請求計數 (**RequestCount**) — 已處理的請求數目 IPv4。此計數只包含具有負載平衡器目標執行個體所產生之回應的要求。
- 用戶端 TLS 交涉錯誤計數 (**ClientTLSNegotiationErrorCount**) — 由於負載平衡器產生錯 TLS 誤而未與負載平衡器建立工作階段的用戶端所起始的 TLS 連線數目。可能的原因包含晶片或協定不相符。
- 拒絕的連線計數 (**RejectedConnectionCount**) – 因負載平衡器已達其連線數目上限而拒絕的連線數目。

## 容器服務指標

以下容器服務指標可供使用。如需詳細資訊，請參閱[檢視容器服務指標](#)。

- CPU 使用率 — 目前在容器服務的所有節點中使用的運算單元平均百分比。此指標可識別在容器服務上執行容器所需的處理能力。
- 記憶體使用率 — 目前在容器服務上跨全部節點使用的記憶體的平均百分比。此指標會識別在容器服務上執行容器所需的記憶體。

## 儲存貯體指標

以下儲存貯體指標可供使用。如需詳細資訊，請參閱[檢視儲存貯體指標](#)。

- **儲存貯體大小** — 儲存貯體中存放的資料量。此值是加總儲存貯體中所有物件的大小 (包含最新和非最新物件) 而計算得出，包括所有分段上傳到儲存貯體的所有不完整部分的大小。
- **物件數量** — 儲存貯體中存放的物件總數。此值是計算儲存貯體中所有物件的數量 (包含最新和非最新物件) 以及所有分段上傳到儲存貯體的所有不完整部分的總數而計算得出。

### Note

當您的儲存貯體為空時，不會報告儲存貯體指標資料。

### 主題

- [設定 Lightsail 資源的度量通知](#)
- [使用指標監控 Lightsail 執行個體效能](#)
- [Lightsail 中的公制警報](#)
- [建立 Lightsail 執行個體度量警示](#)
- [刪除或停 Lightsail 標警示](#)

## 設定 Lightsail 資源的度量通知

您可以設定 Lightsail，以在其中一個執行個體、資料庫、負載平衡器或內容傳遞網路 (CDN) 分發的指標超過指定閾值時通知您。通知的形式可以是 Lightsail 主控台中顯示的橫幅、傳送至您指定之地址的電子郵件，或傳送至您指定之行動電話號碼的簡訊。

若要取得通知，您必須設定警示來監控其中一個資源的指標。例如，您可以設定警示，使其在指定的時間長度內執行個體的傳出網路流量大於 500 KB 時通知您。如需詳細資訊，請參閱[指標警示](#)。

觸發警示時，Lightsail 主控台中會顯示通知橫幅。若要透過電子郵件和 SMS 簡訊收到通知，您必須將您的電子郵件地址和行動電話號碼新增為通知聯絡人，AWS 區域 在每個您想要監控資源的位置。如需詳細資訊，請參閱[新增通知聯絡人](#)。

**Note**

並非所有 AWS 區域可建立 Lightsail 資源的 SMS 文字訊息都受到支援，而且文字訊息無法傳送至世界某些國家和地區。如需詳細資訊，請參閱[新增通知聯絡人](#)。

如果在您預期收到通知時沒有收到通知，您應該檢查一些事項，確認您的通知聯絡人設定正確。若要進一步了解，請參閱[針對通知進行故障診斷](#)。

若要停止接收通知，您可以從 Lightsail 移除電子郵件和行動電話。如需詳細資訊，請參閱[刪除或停用指標警示](#)。您也可以停用或刪除警示，以停止接收特定警示的通知。如需詳細資訊，請參閱[刪除或停用指標警示](#)。

## 使用指標監控 Lightsail 執行個體效能

在 Amazon Lightsail 中啟動執行個體後，您可以在執行個體管理頁面的「指標」索引標籤上檢視其指標圖表。監控指標是維護資源可靠性、可用性與效能的重要環節。定期監控並從您的資源收集指標資料，即可更輕鬆地進行多點失敗的偵錯。如需有關指標的詳細資訊，請參閱[Amazon Lightsail 中的指標](#)。

監控資源時，您應該在環境中建立正常資源效能的基準。然後您可在 Lightsail 主控台中設定警示，以在資源執行超出指定閾值時通知您。如需詳細資訊，請參閱[通知](#)和[警示](#)。

### 內容

- [可用的執行個體度量](#)
- [CPU 使用率永續和可高載區域](#)
- [在 Lightsail 主控台中檢視執行個體指標](#)
- [檢視執行個體指標後的後續步驟](#)

### 可用的執行個體指標

以下是可用的執行個體指標：

- **CPU 使用率 (CPUUtilization)** – 執行個體上目前正在使用的已配置運算單位百分比。此指標可識別在執行個體上執行應用程式的處理能力。如果執行個體未配置完整的處理器核心，作業系統中的工具所顯示的百分比可能會低於 Lightsail。

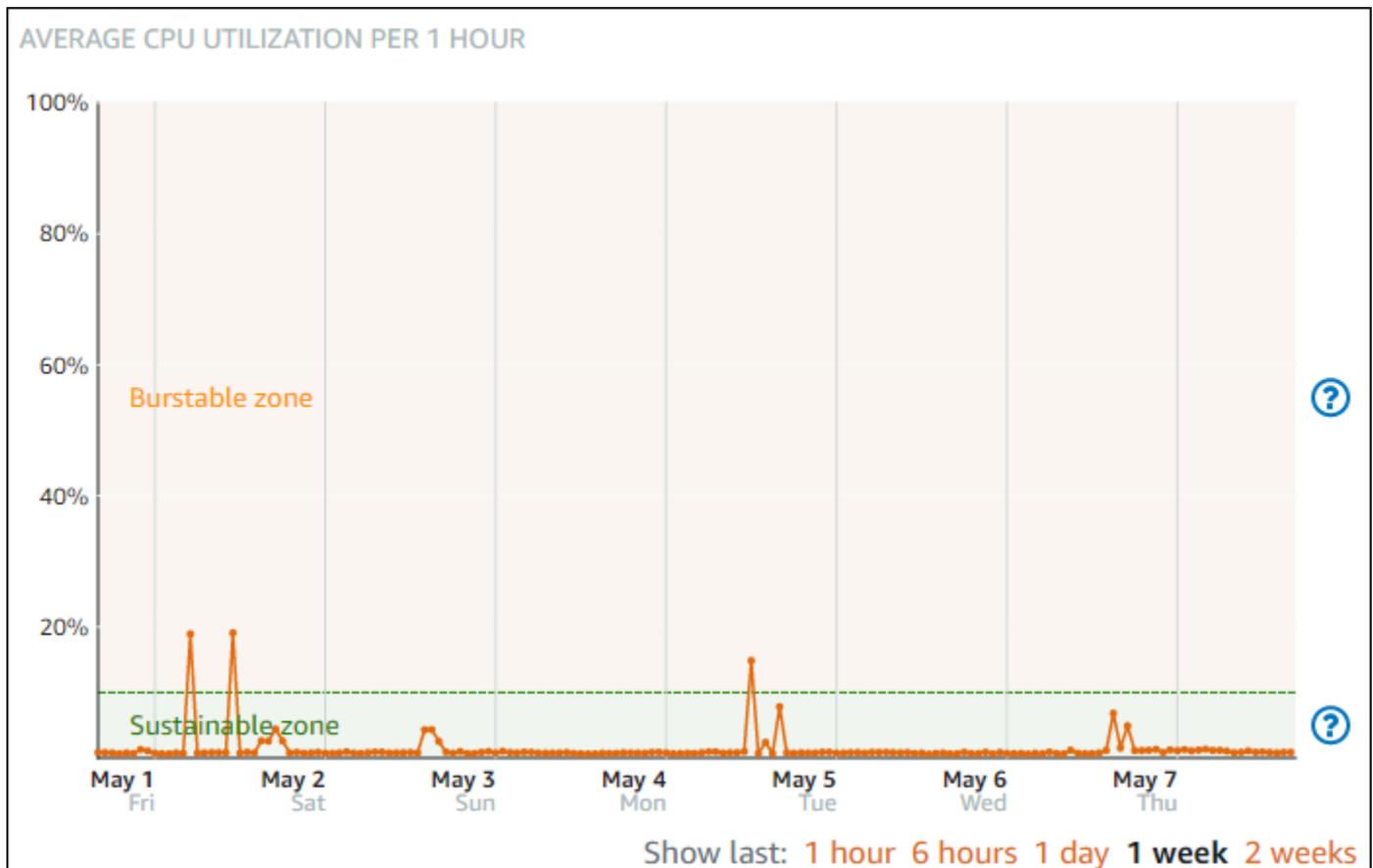
在 Lightsail 主控台中檢視執行個體的 CPU 使用率指標圖表時，您會看到永續且高載的區域。如需這些區域代表意義的詳細資訊，請參閱 [CPU 使用率永續和可高載區域](#)。

- **高載容量分鐘 (BurstCapacityTime)** 與百分比 (**BurstCapacityPercentage**) – 高載容量分鐘代表執行個體以 100% CPU 使用率高載的可用時間量。高載容量百分比是執行個體可用的 CPU 效能百分比。您的執行個體會持續耗用並累積高載容量。只有當您的執行個體以 100% CPU 使用率運作時，才會以全速耗用高載容量分鐘。如需有關執行個體高載容量的詳細資訊，請參閱 [檢視執行個體高載容量](#)。
- **傳入網路流量 (NetworkIn)** – 執行個體在所有網路介面上收到的位元組數目。此指標可識別執行個體的傳入網路流量數量。所報告的數目是在期間內收到的位元組總數。因為此指標的報告間隔為 5 分鐘，所以將報告的數字除以 300 可找出每秒的位元組數。
- **傳出網路流量 (NetworkOut)** – 執行個體在所有網路介面上送出的位元組數目。此指標可識別來自執行個體的傳出網路流量數量。所報告的數目是在期間內送出的位元組總數。因為此指標的報告間隔為 5 分鐘，所以將報告的數字除以 300 可找出每秒的位元組數。
- **狀態檢查失敗 (StatusCheckFailed)** – 報告執行個體是否通過執行個體狀態檢查與系統狀態檢查。此指標可以是 0 (通過) 或 1 (失敗)。此指標是以 1 分鐘的頻率提供。
- **執行個體狀態檢查失敗 (StatusCheckFailed\_Instance)** – 報告執行個體是否通過執行個體狀態檢查。此指標可以是 0 (通過) 或 1 (失敗)。此指標是以 1 分鐘的頻率提供。
- **系統狀態檢查失敗 (StatusCheckFailed\_System)** – 報告執行個體是否通過系統狀態檢查。此指標可以是 0 (通過) 或 1 (失敗)。此指標是以 1 分鐘的頻率提供。
- **無字符中繼資料請求 (MetadataNoToken)** – 已在無字符的情況下成功存取執行個體中繼資料服務的次數。此指標可判斷是否有任何使用執行個體中繼資料服務第 1 版的程序，在未使用字符的情況下存取執行個體中繼資料。如果所有請求都使用字符後端工作階段 (例如執行個體中繼資料服務第 2 版)，則值為 0。如需詳細資訊，請參閱 [執行個體中繼資料和使用者資料](#)。

## CPU 使用率永續和可高載區域

Lightsail 使用高載執行個體，這些執行個體可提供基準的 CPU 效能，但也可視需要暫時提供高於基準線的額外 CPU 效能。這稱為高載。有了可高載執行個體，您不必過度佈建執行個體來處理偶爾的效能尖峰，因而您不必為從未使用的容量付費。

在執行個體的 CPU 使用率指標圖表上，您會看到永續區域和可高載區域。您的 Lightsail 執行個體可以在永續區域中無限期地運作，而不會影響您的系統運作。



在重度負載下，例如編譯程式碼、安裝新軟體、執行批次任務或提供尖峰負載請求時，您的執行個體可能會開始在可高載區域中運作。在可高載區域中運作時，您的執行個體會耗用大量的 CPU 週期。因此，其只能於有限的時段內在此區域中運作。

執行個體可在可高載區域中運作的期間取決於其深入可高載區域的程度。相較於在可高載區域較高端運作的執行個體，在可高載區域較低端運作的執行個體可維持高載的期間比較長。不過，在可高載區域中任意處持續一段時間的執行個體最終會耗盡所有 CPU 容量，直到它再次在永續區域中運作為止。

監控執行個體的 CPU 使用率指標，以查看其效能如何在永續區域和可高載區域之間分配。如果您的系統只會偶爾移至可高載區域，您應可繼續使用您正在執行的執行個體。不過，如果您發現執行個體在高載區域花費了相當長的時間，您可能想要為您的執行個體切換到更大的計劃 (使用每月 \$12 美元/月計劃，而不是 \$5 USD /月計劃)。您可以為執行個體建立新的快照，然後從快照建立新執行個體，以切換至較大型的計劃。

## 在 Lightsail 主控台中檢視執行個體指標

完成下列步驟，即可在 Lightsail 主控台中檢視執行個體度量。

1. 登入主 [Lightsail 台](#)。

2. 在 Lightsail 首頁上，選擇「實體」索引標籤。
3. 選擇要檢視指標的執行個體名稱。
4. 選擇執行個體管理頁面上的 Metrics (指標) 標籤。
5. 在 Metrics graphs (指標圖表) 標題下的下拉式選單中，選擇您要檢視的指標。

圖表會顯示所選指標的資料點視覺化呈現。

#### Note

在 Lightsail 主控台中檢視執行個體的 CPU 使用率指標圖表時，您會看到永續且高載的區域。如需有關這些區域的詳細資訊，請參閱 [CPU 使用率永續和可高載區域](#)。

6. 您可以在指標圖表上執行下列動作：
  - 變更圖表的檢視，以顯示 1 小時、6 小時、1 天、1 週和 2 週的資料。
  - 將游標暫停在資料點上，以檢視有關該資料點的詳細資訊。
  - 新增所選指標的警示，以在指標超過您指定的閾值時收到通知。如需詳細資訊，請參閱 [警示](#) 和 [建立執行個體指標警示](#)。

## 後續步驟

您可以為執行個體指標執行一些其他工作：

- 新增所選指標的警示，以在指標超過您指定的閾值時收到通知。如需詳細資訊，請參閱 [指標警示](#) 和 [建立執行個體指標警示](#)。
- 觸發警示時，Lightsail 主控台中會顯示通知橫幅。若要透過電子郵件和 SMS 簡訊收到通知，您必須將您的電子郵件地址和行動電話號碼新增為通知聯絡人，AWS 區域 在每個您想要監控資源的位置。如需詳細資訊，請參閱 [新增通知聯絡人](#)。
- 若要停止接收通知，您可以從 Lightsail 移除電子郵件和行動電話。如需詳細資訊，請參閱 [刪除或停用指標警示](#)。您也可以停用或刪除警示，以停止接收特定警示的通知。如需詳細資訊，請參閱 [刪除或停用指標警示](#)。

## Lightsail 中的公制警報

您可以在 Amazon Lightsail 中建立警示，以監控執行個體、資料庫、負載平衡器和內容交付網路 (CDN) 分發的單一指標。您可將警示設定為根據您所指定閾值的相對指標值來通知您。通知可以是

Lightsail 主控台中顯示的橫幅、傳送至您的電子郵件地址的電子郵件，以及傳送至您的行動電話號碼的簡訊。在本指南中，我們會說明您可設定的警示條件和設定。

## 內容

- [設定警示](#)
- [警示狀態](#)
- [警示範例](#)
- [設定警示處理遺失資料的方式](#)
- [資料遺失時評估警示狀態的方式](#)
- [圖表範例中的遺失資料](#)
- [有關警示的詳細資訊](#)

## 設定警示

若要在 Lightsail 主控台中新增警示，請瀏覽至執行個體、資料庫、負載平衡器或 CDN 發佈的「指標」索引標籤。然後選擇要監控的指標，並選擇 Add alarm (新增警示)。您可以為每個指標新增兩個警示。如需指標的詳細資訊，請參閱[資源指標](#)。

若要設定警示，您必須先識別閾值，這就是警示將變更狀態的指標值 (例如，從 OK 狀態變更為 ALARM 狀態，反之亦然)。如需詳細資訊，請參閱[警示狀態](#)。然後選取要用來比較指標與閾值的比較運算子。可用的運算子為 greater than or equal to (大於或等於)、greater than (大於)、less than (小於) 及 less than or equal to (小於或等於)。

然後，您可以指定必須超過閾值的次數，以及將要評估指標的時段，以便進行變更警示的狀態。Lightsail 每 5 分鐘評估一次警示的資料點，而每個資料點代表 5 分鐘的彙總資料期間。例如，如果您指定要在超過閾值 2 次時觸發警示，則評估期間必須在過去 10 分鐘或更長 (最長 24 小時)。如果您指定要在超過閾值 10 次時觸發警示，則評估期間必須在過去 50 分鐘或更長 (最長 24 小時)。

設定警示的條件後，您可以設定您想要收到通知的方式。當鬧鐘從狀態變更為 OK 狀態時，通知橫幅一律會顯示在 Lightsail 主控台中 ALARM。您也可以選擇透過電子郵件和簡訊簡訊收到通知，但您必須設定其通知聯絡人。如需詳細資訊，請參閱[指標通知](#)。如果您選擇透過電子郵件和/或簡訊收到通知，您也可以選擇在警示狀態從 ALARM 狀態狀態變更為 OK 時收到通知，該狀態會被視為「警示解除」通知。

在鬧鐘的進階設定中，您可以選擇 Lightsail 如何處理遺失的量度資料。如需詳細資訊，請參閱[設定警示處理遺失資料的方式](#)。

## 警示狀態

警示一律處於下列其中一種狀態：

- ALARM – 指標在定義的閾值外。

例如，如果您選擇 greater than (大於) 比較運算子，則當指標大於指定的閾值時，警示就會處於 ALARM 狀態。如果您選擇 less than (小於) 比較運算子，則當指標小於指定的閾值時，警示就會處於 ALARM 狀態。

- OK – 指標位於定義閾值內。

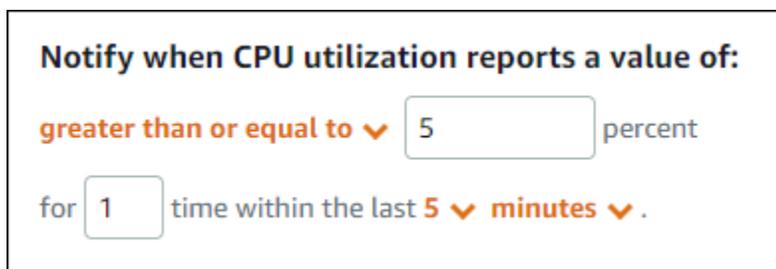
例如，如果您選擇 greater than (大於) 比較運算子，則當指標小於指定的閾值時，警示就會處於 OK 狀態。如果您選擇 less than (小於) 比較運算子，則當指標大於指定的閾值時，警示就會處於 OK 狀態。

- INSUFFICIENT\_DATA – 警示剛啟動，無法使用指標，或沒有足夠的指標資料可供警示判斷警示狀態。

系統只會針對狀態變更觸發警示。警示不會僅只因為其處於特定狀態而觸發 – 狀態必須已變更。觸發警示時，Lightsail 主控台中會顯示橫幅。您也可將警示設定為透過電子郵件和簡訊通知您。

## 警示範例

考慮到先前描述的警示條件，您可將警示設定為當執行個體的 CPU 使用率在單一 5 分鐘的期間內有一次大於或等於 5% 時進入 ALARM 狀態。下列範例顯示此鬧鐘在 Lightsail 主控台內的設定。



Notify when CPU utilization reports a value of:

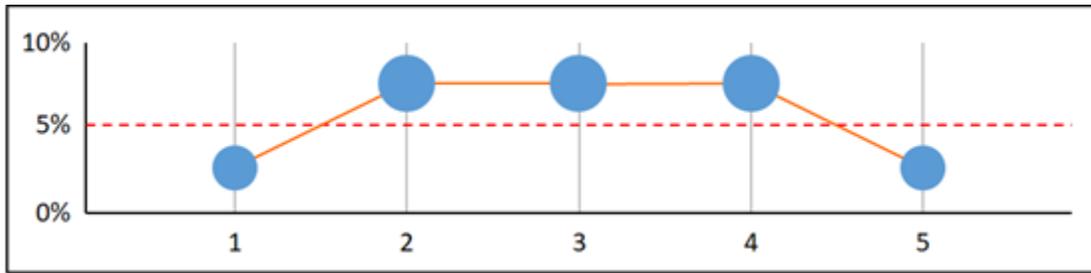
greater than or equal to  percent

for  time within the last  minutes.

在此範例中，如果執行個體的 CPU 使用率指標報告只有一個資料點的使用率為 5% 或以上，則警示會從 OK 狀態變更為 ALARM 狀態。系統報告使用率為 5% 或以上的每個後續資料點，其警示會保持 ALARM 狀態。當執行個體的 CPU 使用率指標報告只有一個資料點的使用率為 4.9% 或以下，則警示會從 ALARM 狀態變更為 OK 狀態。

下圖進一步說明此警示。紅色虛線代表 5% CPU 使用率閾值，而藍點代表指標資料點。第一個資料點的警示處於 OK 狀態。第二個資料點會將警示變更為 ALARM 狀態，因為此資料點大於閾值。第三和第

四個資料點會保持 ALARM 狀態，因為這些資料點持續大於閾值。第五個資料點會將警示變更為 OK 狀態，因為此資料點小於閾值。



## 設定 警示處理遺失資料的方式

在某些情況下，不會報告具有警示之指標的某些資料點。例如，當失去連線或伺服器當機時，可能會發生這種情況。

Lightsail 可讓您指定在設定警示時如何處理遺失的資料點。這可協助您設定警示，在適合受監控的資料類型時移至 ALARM 狀態。您可以在資料遺失並不表示有問題時避免誤報。

與每個警示總會是三種狀態中的其中一種相似，每個報告的特定資料點都會是三種類別中的其中一種類別：

- 未違反 – 資料點在閾值內。

例如，如果您選擇 `greater than` (大於) 比較運算子，則資料點在小於指定的閾值時就會處於 `Not breaching` 狀態。如果您選擇 `less than` (小於) 比較運算子，則資料點在大於指定的閾值時就會處於 `Not breaching` 狀態。

- 違反 – 資料點超出閾值。

例如，如果您選擇 `greater than` (大於) 比較運算子，則資料點在大於指定的閾值時就會處於 `Breaching` 狀態。如果您選擇 `less than` (小於) 比較運算子，則資料點在小於指定的閾值時就會處於 `Breaching` 狀態。

- 遺失 – 遺失資料點的行為是由 `treat missing data` 參數指定。

對於每個警報，您可以指定 Lightsail 將遺失的資料點視為下列任一項目：

- 未違反 – 將遺失的資料點視為「良好」且在閾值內。
- 違反 – 將遺失的資料點視為「不良」且超出閾值。
- 忽略 – 維持目前的警示狀態。
- 遺失 – 在評估是否變更狀態時，警示不會考慮遺失的資料點。這是警示的預設行為。

最佳選擇取決於指標類型。對於執行個體的 CPU 使用率之類的指標，您可以將遺失資料點視為違反。這是因為遺失資料點可能表示發生問題。但是，對於只有在發生錯誤時才會產生資料點的指標 (例如負載平衡器的 HTTP 500 伺服器錯誤計數)，您可以將遺失的資料視為未違反。

為警示選擇最佳選項，可避免不必要且誤導的警示條件變更。也可以更準確地指出系統的運作狀態。

## 資料遺失時評估警示狀態的方式

無論您為如何處理遺失的資料設定什麼值，當警示評估是否要變更狀態時，Lightsail 都會嘗試擷取比「評估期間」指定的資料點數量更多。其嘗試擷取的確切資料點數取決於警示期間的長度。其嘗試擷取的資料點時間範圍便是評估範圍。

Lightsail 擷取這些資料點之後，會發生下列情況：

- 如果評估範圍內沒有資料點遺失，Lightsail 會根據最近收集的資料點來評估警示。
- 如果評估範圍中的某些資料點遺失，但收集的現有資料點數量等於或大於警示的評估期間，Lightsail 會根據最近成功收集的現有資料點評估警示狀態。在這種情況下，不需要您針對遺失資料處理方式所設定的值，而後會予以忽略。
- 如果評估範圍中的某些資料點遺失，且收集的現有資料點數量小於警示的評估期間數，Lightsail 會使用您為如何處理遺失資料所指定的結果填入遺失的資料點，然後評估警示。不過，在評估範圍內的所有真實資料點 (無論何時報告) 都包含在評估內。Lightsail 只會盡可能少地使用遺失的資料點。

在這些情況下，評估的資料點數目等於 Evaluation periods (評估期間) 的值。如果少於違反 Data points to alarm (要警示的資料點) 值，則違反的警示狀態設定為 OK。否則狀態設定為 ALARM。

### Note

此行為的特定情況是，在指標停止流動後，Lightsail 警示可能會在一段時間內重複重新評估最後一組資料點。此重新評估可能會導致警示變更狀態和重新執行動作 (如果在指標串流停止前便已立即變更狀態的話)。為了減少這種行為，請使用較短的期間。

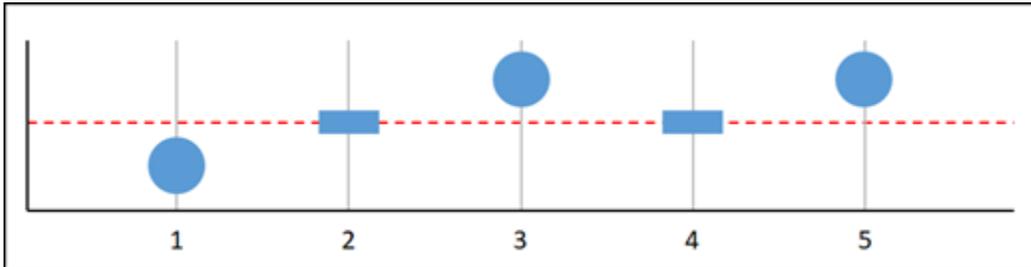
## 圖表範例中的遺失資料

這一節中的下列圖表協助說明警示評估行為的範例。在圖表 A、B、C、D 和 E 中，必須違反才會警示的資料點數目和評估時段都是 3。紅色虛線代表閾值，藍點代表有效的資料點，而虛線則代表遺失的資料。閾值線以上是違反的資料點，閾值以下則是未違反的資料點。如果最近三個資料點中的某些遺失，Lightsail 會嘗試擷取其他有效資料點。

### Note

如果在您建立警示後不久遺失資料點，而且在您建立鬧鐘之前已向 Lightsail 報告量度，Lightsail 會在評估警示時，從建立警示之前擷取最新的資料點。

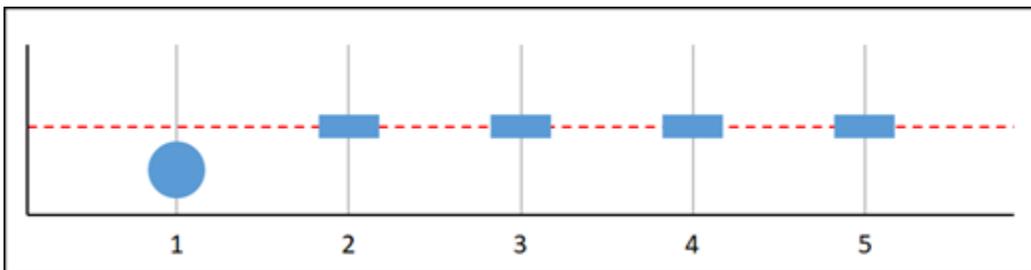
圖表 A



在前面的圖表指標中，資料點 1 在閾值內、資料點 2 遺失、資料點 3 違反、資料點 4 遺失，而資料點 5 違反。假設評估範圍中有三個有效資料點，則此指標沒有遺失資料點。如果您將警示設定為將遺失的資料點視為：

- 未違反 – 警示處於 OK 狀態。
- 違反 – 警示處於 OK 狀態。
- 忽略 – 警示處於 OK 狀態。
- 遺失 – 警示處於 OK 狀態。

圖表 B



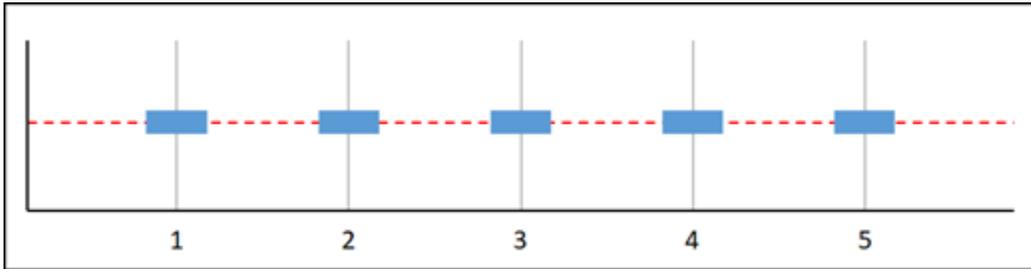
在前面的圖表指標中，資料點 1 在閾值內，而資料點 2 到 5 遺失。假設評估範圍中只有一個資料點，則此指標有兩個遺失資料點。如果您將警示設定為將遺失的資料點視為：

- 未違反 – 警示處於 OK 狀態。
- 違反 – 警示處於 OK 狀態。
- 忽略 – 警示處於 OK 狀態。

- 遺失 – 警示處於 OK 狀態。

在此案例中，即使遺失資料被視為違反，警示仍會維持 OK 狀態。這是因為有一個現有資料點並未違反，而且這個資料點會與兩個被視為違反的遺失資料點一起進行評估。下次評估此警示時，如果資料仍然遺失，則會進入 ALARM 狀態。這是因為未違反的資料點不再是最近擷取的五個資料點之一。

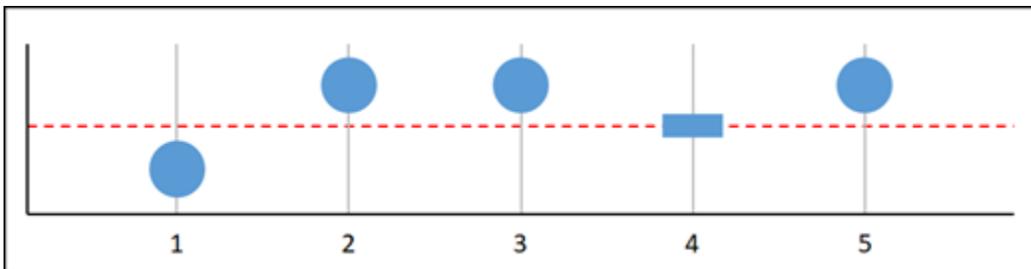
圖表 C



在前面的圖表指標中所有的資料點都遺失了。假設評估範圍中的所有資料點都遺失，則此指標有三個遺失資料點。如果您將警示設定為將遺失的資料點視為：

- 未違反 – 警示處於 OK 狀態。
- 違反 – 警示處於 ALARM 狀態。
- 忽略 – 警示會維持目前狀態。
- 遺失 – 警示處於 INSUFFICIENT\_DATA 狀態。

圖表 D



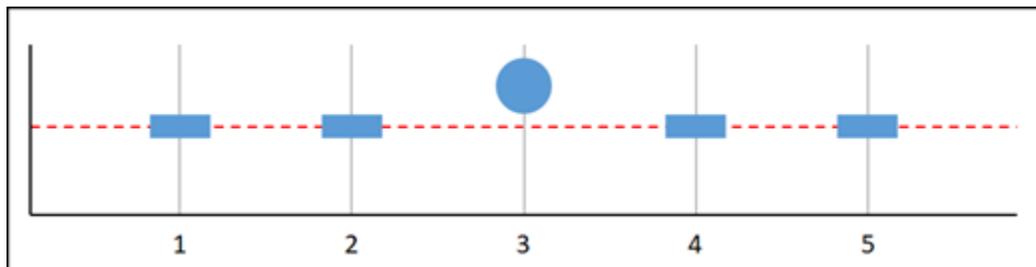
在前面的圖表指標中，資料點 1 在閾值內、資料點 2 違反、資料點 3 違反、資料點 4 遺失，而資料點 5 違反。假設評估範圍中有四個有效資料點，則此指標沒有遺失資料點。如果您將警示設定為將遺失的資料點視為：

- 未違反 – 警示處於 ALARM 狀態。
- 違反 – 警示處於 ALARM 狀態。
- 忽略 – 警示處於 ALARM 狀態。

- 遺失 – 警示處於 ALARM 狀態。

在此案例中，警示會在所有情況下進入 ALARM 狀態。這是因為有足夠的實際資料點不需要遺失資料處理方式的設定，而後會予以忽略。

圖表 E

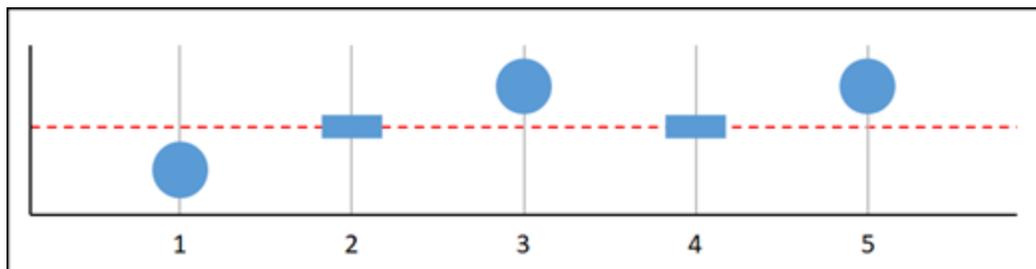


在前面的圖表指標中，資料點 1 和 2 遺失、資料點 3 違反，而資料點 4 和 5 遺失。假設評估範圍中只有一個資料點，則此指標有兩個遺失資料點。如果您將警示設定為將遺失的資料點視為：

- 未違反 – 警示處於 OK 狀態。
- 違反 – 警示處於 ALARM 狀態。
- 忽略 – 警示會維持目前狀態。
- 遺失 – 警示處於 ALARM 狀態。

在圖表 F、G、H、I 和 J 中，Datapoints to alarm (要警示的資料點) 為 2，而 Evaluation periods (評估期間) 為 3。這是指 3 個警示中有 2 個，N 個警示中有 M 個。5 是警示的評估範圍。

圖表 F

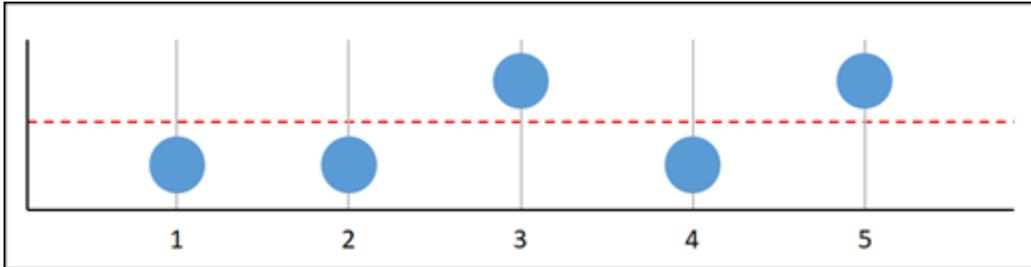


在前面的圖表指標中，資料點 1 在閾值內、資料點 2 遺失、資料點 3 違反、資料點 4 遺失，而資料點 5 違反。假設評估範圍中有三個資料點，則此指標沒有遺失資料點。如果您將警示設定為將遺失的資料點視為：

- 未違反 – 警示處於 ALARM 狀態。

- 違反 – 警示處於 ALARM 狀態。
- 忽略 – 警示處於 ALARM 狀態。
- 遺失 – 警示處於 ALARM 狀態。

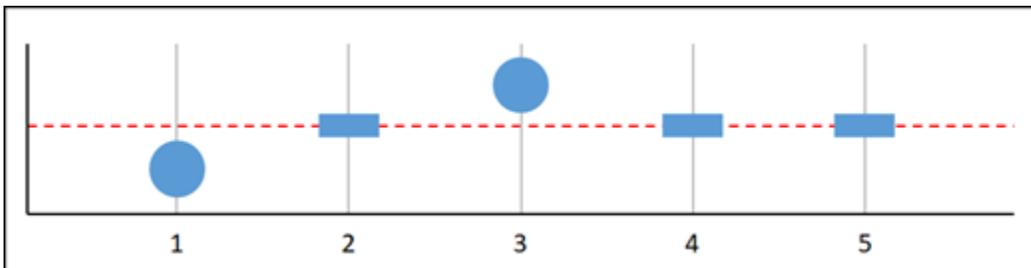
圖表 G



在前面的圖表指標中，資料點 1 和 2 在閾值內、資料點 3 違反、資料點 4 在閾值內，而資料點 5 違反。假設評估範圍中有五個資料點，則此指標沒有遺失資料點。如果您將警示設定為將遺失的資料點視為：

- 未違反 – 警示處於 ALARM 狀態。
- 違反 – 警示處於 ALARM 狀態。
- 忽略 – 警示處於 ALARM 狀態。
- 遺失 – 警示處於 ALARM 狀態。

圖表 H

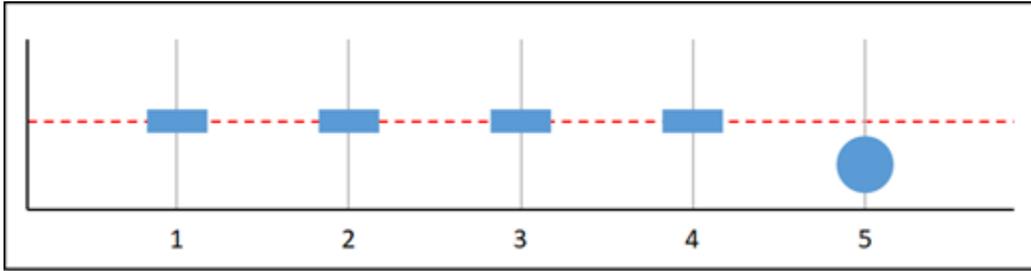


在前面的圖表指標中，資料點 1 在閾值內、資料點 2 遺失、資料點 3 違反，而資料點 4 和 5 遺失。假設評估範圍中有兩個資料點，則此指標有一個遺失資料點。如果您將警示設定為將遺失的資料點視為：

- 未違反 – 警示處於 OK 狀態。
- 違反 – 警示處於 ALARM 狀態。
- 忽略 – 警示處於 OK 狀態。

- 遺失 – 警示處於 OK 狀態。

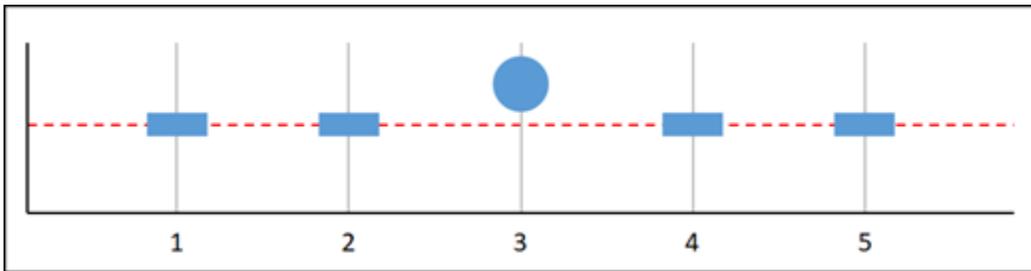
圖表 I



在前面的圖表指標中，資料點 1 到 4 遺失，而資料點 5 在閾值內。假設評估範圍中有一個資料點，則此指標有兩個遺失資料點。如果您將警示設定為將遺失的資料點視為：

- 未違反 – 警示處於 OK 狀態。
- 違反 – 警示處於 ALARM 狀態。
- 忽略 – 警示處於 OK 狀態。
- 遺失 – 警示處於 OK 狀態。

圖表 J



在前面的圖表指標中，資料點 1 和 2 遺失、資料點 3 違反，而資料點 4 和 5 遺失。假設評估範圍中有一個資料點，則此指標有兩個遺失資料點。如果您將警示設定為將遺失的資料點視為：

- 未違反 – 警示處於 OK 狀態。
- 違反 – 警示處於 ALARM 狀態。
- 忽略 – 警示會維持目前狀態。
- 遺失 – 警示處於 ALARM 狀態。

## 有關警示的詳細資訊

以下是一些可協助您在 Lightsail 中管理鬧鐘的文章：

- [建立執行個體指標警示](#)
- [建立資料庫指標警示](#)
- [建立負載平衡器指標警示](#)
- [建立分發指標警示](#)
- [刪除或停用指標警示](#)

## 建立 Lightsail 執行個體度量警示

您可以建立監控單一執行個體指標的 Amazon Lightsail 警示。您可將警示設定為根據您所指定閾值的相對指標值來通知您。通知可以是 Lightsail 主控台中顯示的橫幅、傳送至您的電子郵件地址的電子郵件，以及傳送至您的行動電話號碼的簡訊。如需有關警示的詳細資訊，請參閱[警示](#)。

### 內容

- [執行個體警示限制](#)
- [設定執行個體警示的最佳實務](#)
- [預設警示設定](#)
- [使用 Lightsail 主控台建立執行個體指標警示](#)
- [使用 Lightsail 主控台測試執行個體指標警示](#)
- [建立執行個體警示後的後續步驟](#)

## 執行個體警示限制

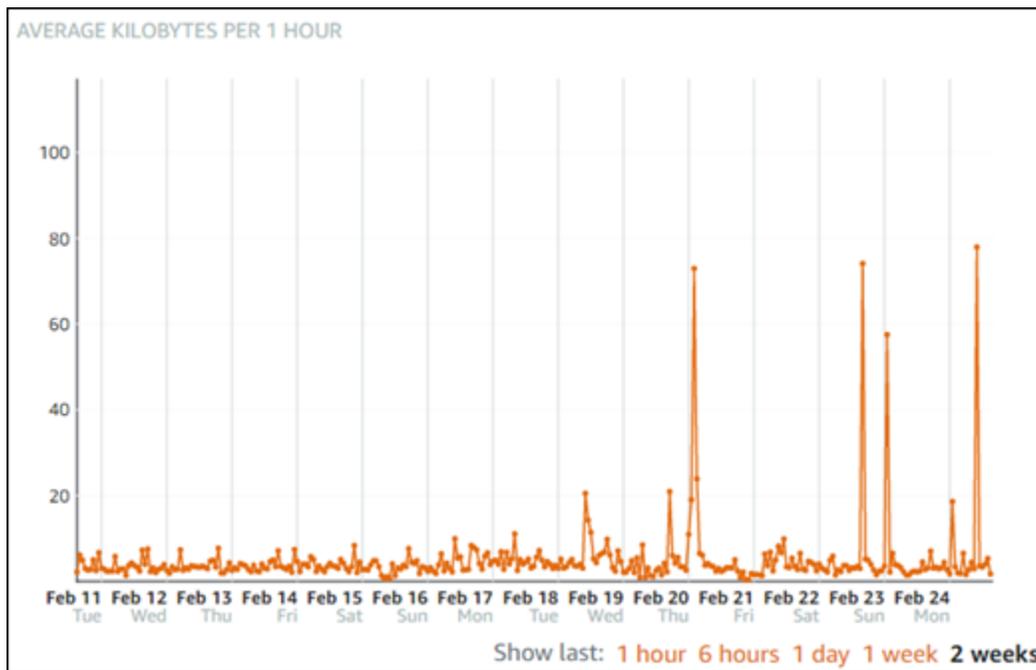
下列限制適用於警示：

- 您可以為每個指標設定兩個警示。
- 警示的評估間隔為 5 分鐘，而警示的每個資料點都代表為期 5 分鐘的彙總指標資料。
- 如果您將警示設定為透過電子郵件和/或簡訊通知您，則您只能將警示設定為在警示狀態更改為 OK 時通知您。
- 只有將警示設定為透過電子郵件和/或簡訊通知您，才能測試 OK 警示通知。

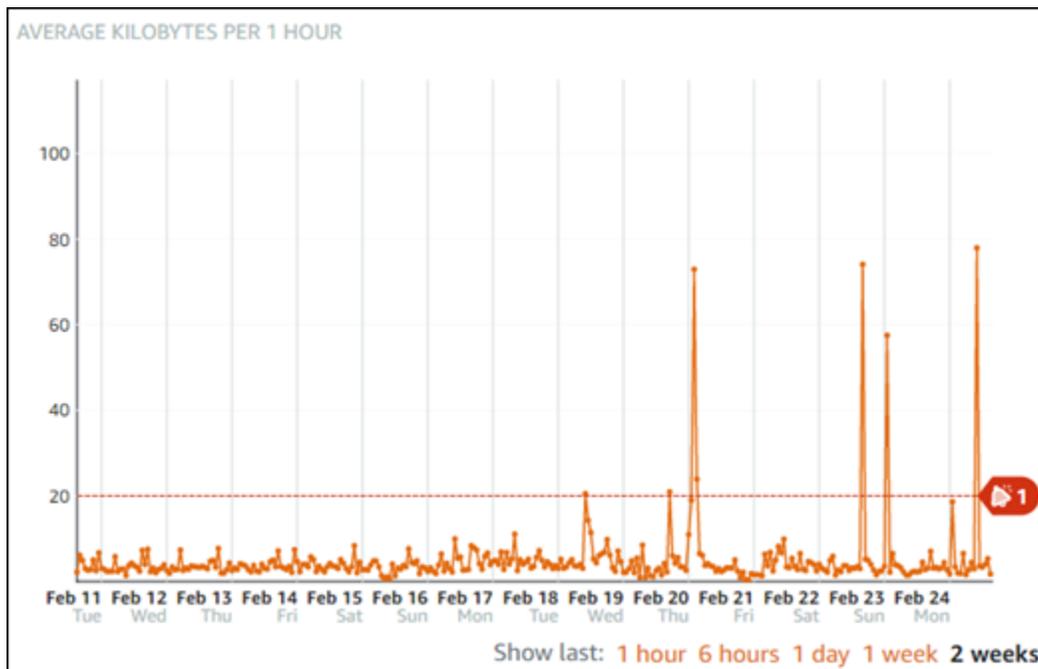
- 如果您將警示設定為透過電子郵件和/或簡訊通知您，並且如果您為遺失的資料點選擇 Do not evaluate the missing data (不評估遺失資料) 選項，則您只能將警示設定為在警示狀態更改為 INSUFFICIENT\_DATA 時通知您。
- 您只能在警示處於 OK (正常) 狀態時測試通知。

## 設定執行個體警示的最佳實務

設定執行個體的指標警示之前，您應該先檢視指標的歷史資料。識別過去兩週期間內的低層級、中層級和高層級。在下列傳出網路流量 (NetworkOut) 指標圖表範例中，低層級為每小時 0-10 KB、中層級介於每小時 10-20 KB 之間，而高層級介於每小時 20-80 KB 之間。



如果您將警示閾值設定為 greater than or equal to (大於或等於) 低層範圍中的某處 (例如，每小時 5 KB)，則會收到更頻繁且可能不必要的警示通知。如果您將警示閾值設定為 greater than or equal to (大於或等於) 高層範圍中的某處 (例如每小時 20 KB)，則會收到較不頻繁的警示通知，但調查可能更為重要。當您設定警示並加以啟用時，圖表上會出現代表閾值的警示線，如下列範例所示。標示為 1 的警示線代表警示 1 的閾值，標示為 2 的警示線代表警示 2 的閾值。



## 預設警示設定

當您在 Lightsail 主控台中新增開鐘時，會預先填入預設開鐘設定。這是您所選指標的建議警示組態。不過，您應該確認預設警示組態適合您的資源。例如，執行個體傳出網路流量 (NetworkOut) 指標的預設警示閾值為在過去 10 分鐘內 less than or equal to (小於或等於) 0 個位元組 2 次。不過，如果您有興趣收到高流量事件的通知，那麼可將警示閾值修改為在過去 10 分鐘內大於或等於 50 KB 兩次，或使用這些設定新增第二個警示，以便在沒有流量及有高流量時收到通知。應調整您指定的閾值，以符合本指南的[設定執行個體警示的最佳實務](#)一節中所述的指標高層級和低層級。

## 使用 Lightsail 主控台建立執行個體指標警示

完成下列步驟，以使用 Lightsail 主控台建立執行個體指標警示。

1. 登入主 [Lightsail](#) 台。
2. 在 Lightsail 首頁上，選擇「實體」索引標籤。
3. 選擇您要建立警示的執行個體名稱。
4. 選擇執行個體管理頁面上的 Metrics (指標) 標籤。
5. 在 Metrics Graphs (指標圖表) 標題下的下拉式功能表中，選擇您要建立其警示的指標。如需詳細資訊，請參閱[資源指標](#)。
6. 選擇該頁面 Alarms (警示) 區段中的 Add alarm (新增警示)。
7. 在下拉式功能表中選擇比較運算子值。範例值為大於或等於、大於、小於或小於或等於。

8. 輸入警示的閾值。
9. 輸入要警示的資料點。
10. 選擇評估期間。期間可以 5 分鐘的增量指定 (從 5 分鐘到 24 小時)。
11. 選擇下列其中一種通知方法：
  - 電子郵件 — 當警示狀態變更為 ALARM 時，您會透過電子郵件收到通知。
  - 簡訊 — 當警示狀態變更為 ALARM 時，您會透過簡訊收到通知。您可以在其中建立 Lightsail 資源的所有 AWS 區域都不支援 SMS 簡訊，而且 SMS 文字訊息無法傳送到所有國家/地區。如需詳細資訊，請參閱[簡訊支援](#)。

 Note

如果您選擇透過電子郵件或簡訊收到通知，但尚未在資源的 AWS 區域中設定通知聯絡人，則您需要新增電子郵件地址或行動電話號碼。如需詳細資訊，請參閱[指標通知](#)。

12. (選擇性) 選擇 Send me a notification when the alarm state change to OK (當警示狀態變更為正常時傳送通知給我)，以便在警示狀態變更為 OK (正常) 時收到通知。只有在您選擇透過電子郵件或簡訊收到通知時，才能使用此選項。
13. (選擇性) 選擇 Advanced settings (進階設定)，然後選擇下列其中一個選項：
  - 選擇警示應如何處理遺失的資料。以下是可用的選項：
    - 假設其不在閾值內 (違反閾值) — 遺失資料點會被視為「不良」並違反閾值。
    - 假設其在閾值內 (未違反閾值) — 遺失資料點會被視為「良好」且在閾值內。
    - 使用最後一個良好資料點的值 (忽略並維持目前的警示狀態) – 維持目前的警示狀態。
    - 不要評估 (將遺失的資料視為遺失) — 警示在評估是否要變更狀態時不會考慮遺失的資料點。
  - 選擇 Send a notification if there is insufficient data (如果資料不足則傳送通知)，以在警示狀態變更為 INSUFFICIENT\_DATA 時收到通知。只有在您選擇透過電子郵件或簡訊收到通知時，才能使用此選項。
14. 選擇 Create (建立) 以新增警示。

若要稍後編輯警示，請選擇您要編輯的警示旁邊的省略符號圖示 (:)，然後選擇編輯警示。

## 使用 Lightsail 主控台測試執行個體指標警示

請完成下列步驟，以使用 Lightsail 主控台測試警示。您可以測試警示，確認所設定的通知選項是否能運作，例如：確保在觸發警示時收到電子郵件或簡訊。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁上，選擇「實體」索引標籤。
3. 選擇您要測試警示的執行個體名稱。
4. 選擇執行個體管理頁面上的 Metrics (指標) 標籤。
5. 在 Metrics Graphs (指標圖表) 標題下的下拉式功能表中，選擇您要測試其警示的指標。
6. 向下捲動至頁面的警示區段，然後選擇您要測試的警示旁邊的省略符號圖示 (:)
7. 請選擇下列其中一個選項：
  - 測試警示通知 – 選擇此選項可在警示狀態變更為 ALARM 時測試通知。
  - 測試正常通知 – 選擇此選項可在警示狀態變更為 OK 時測試通知。

### Note

如果無法使用上述任何一個選項，則表示您可能尚未設定警示的通知選項，或警示可能目前處於 ALARM 狀態。如需詳細資訊，請參閱[執行個體警示限制](#)。

根據您選擇的測試選項，警示會暫時變更為 ALARM 或 OK 狀態，並根據您為警示設定的通知方法來傳送電子郵件和/或簡訊。只有當您選擇測試通知時，Lightsail 主控台才會顯示 ALARM 通知橫幅。如果您選擇測試 OK 通知，則不會顯示通知橫幅。警示通常會在幾秒鐘後回到其實際狀態。

## 後續步驟

您可以為執行個體警示執行一些其他工作：

- 若要停止接收通知，您可以從 Lightsail 移除電子郵件和行動電話。如需詳細資訊，請參閱[刪除通知聯絡人](#)。您也可以停用或刪除警示，以停止接收特定警示的通知。如需詳細資訊，請參閱[刪除或停用指標警示](#)。

## 刪除或停用 Lightsail 標警示

您可以刪除 Amazon Lightsail 警示，以停止警示監控的指標超過閾值時的通知。您也可以停用警示來停止接收通知。如需詳細資訊，請參閱 [警示](#)。

### 內容

- [使用 Lightsail 主控台刪除量度警示](#)
- [使用 Lightsail 主控台停用和啟用度量警示](#)

### 使用 Lightsail 主控台刪除量度警示

若要使用 Lightsail 主控台刪除度量警示，請完成下列步驟。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁上，選擇 Instances (執行個體)、Databases (資料庫) 或 Networking (網路) 標籤。
3. 選擇您要刪除其警示的資源 (執行個體、資料庫或負載平衡器) 名稱。
4. 選擇資源管理頁面上的 Metrics (指標) 標籤。
5. 在 Metrics graphs (指標圖表) 標題下的下拉式清單中，選擇您要刪除其警示的指標。
6. 向下捲動至頁面的警示區段，然後選擇要刪除的警示旁邊的省略符號圖示 (:)
7. 選擇刪除。
8. 出現提示時，選擇 Delete (刪除)，確認您要刪除警示。

### 使用 Lightsail 主控台停用和啟用度量警示

若要使用 Lightsail 主控台停用度量警示，請完成下列步驟。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁上，選擇 Instances (執行個體)、Databases (資料庫) 或 Networking (網路) 標籤。
3. 選擇您要停用其警示的資源 (執行個體、資料庫或負載平衡器) 名稱。
4. 選擇資源管理頁面上的 Metrics (指標) 標籤。
5. 在 Metrics graphs (指標圖表) 標題下的下拉式清單中，選擇您要停用其警示的指標。

6. 向下捲動至頁面的 Alarms (警示) 區段，找出您要停用的警示，然後選擇切換開關予以停用。同樣地，若已啟用，則選擇切換開關予以啟用。

## 監控儲存貯 Lightsail 效能和使用情況

在 Amazon Lightsail 物件儲存服務中建立值區之後，您可以在值區管理頁面的「指標」索引標籤上檢視其指標圖表。監控指標是維護儲存貯體可用性與效能的重要環節。定期監控並從儲存貯體收集指標資料，即可在需要時擴大或縮減儲存貯體的儲存空間和網路傳輸配額。如需指標的詳細資訊，請參閱[資源指標](#)。

監控資源時，您應該在環境中建立正常資源效能的基準。然後您可在 Lightsail 主控台中設定警示，以在資源執行超出指定閾值時通知您。如需詳細資訊，請參閱[通知](#)和[警示](#)。

### 儲存貯體指標

下列是可用的儲存貯體指標：

- 儲存貯體大小 — 儲存貯體中存放的資料量。此值是加總儲存貯體中所有物件的大小 (包含最新和非最新物件) 而計算得出，包括所有分段上傳到儲存貯體的所有不完整部分的大小。
- 物件數量 — 儲存貯體中存放的物件總數。此值是計算儲存貯體中所有物件的數量 (包含最新和非最新物件) 以及所有分段上傳到儲存貯體的所有不完整部分的總數而計算得出。

#### Note

當您的儲存貯體為空時，不會報告儲存貯體指標資料。

### 在 Lightsail 主控台中檢視儲存貯體指標

請完成下列程序，以在 Lightsail 主控台中檢視儲存貯體指標。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁上，選擇儲存空間索引標籤。
3. 選擇要檢視指標的儲存貯體名稱。
4. 選擇儲存貯體管理頁面上的 Metrics (指標) 索引標籤。
5. 在 Metrics graphs (指標圖表) 標題下的下拉式選單中，選擇您要檢視的指標。

圖表會顯示所選指標的資料點視覺化呈現。

### *Screenshot TBD*

您可以在指標圖表上執行下列動作：

- 變更圖表的檢視，以顯示 1 小時、6 小時、1 天、1 週和 2 週的資料。
- 將游標暫停在資料點上，以檢視有關該資料點的詳細資訊。
- 新增所選指標的警示，以在指標超過您指定的閾值時收到通知。如需詳細資訊，請參閱[警示](#)和[建立儲存貯體指標警示](#)。

## 管理儲存貯體和物件

以下是管理 Lightsail 物件儲存貯體的一般步驟：

1. 了解 Amazon Lightsail 物件儲存服務中的物件和值區。如需詳細資訊，請參閱 [Amazon Lightsail 中的物件儲存](#)。
2. 了解您可以在 Amazon Lightsail 中為您的儲存貯體提供哪些名稱。如需詳細資訊，請參閱 [Amazon Lightsail 中的儲存貯體命名規則](#)。
3. 透過建立值區開始使用 Lightsail 物件儲存服務。如需詳細資訊，請參閱 [在 Amazon Lightsail 中建立值區](#)。
4. 了解儲存貯體的安全最佳實務，以及可以為儲存貯體設定的存取許可。可以將儲存貯體中的所有物件設為公有或私有，也可以選擇將個別物件設為公有。也可以透過建立存取金鑰、將執行個體附接至儲存貯體以及授予對其他 AWS 帳戶的存取權，來授予對儲存貯體的存取權。如需詳細資訊，請參閱 [Amazon Lightsail 物件儲存的安全最佳實務](#)和[了解 Amazon Lightsail 中的儲存貯體許可](#)。

了解儲存貯體存取許可後，請參閱下列指南來授予對儲存貯體的存取權：

- [封鎖儲存貯體的公 Amazon Lightsail](#)
  - [在 Amazon Lightsail 中設定儲存貯體存取權限](#)
  - [在 Amazon Lightsail 中為儲存貯體中的個別物件設定存取權限](#)
  - [在 Amazon Lightsail 中為存儲桶創建訪問密鑰](#)
  - [在 Amazon Lightsail 中設定儲存貯體的資源存取](#)
  - [在 Amazon Lightsail 中設定儲存貯體的跨帳戶存取](#)
5. 了解如何為儲存貯體啟用存取日誌記錄，以及如何使用存取日誌來稽核儲存貯體的安全性。如需詳細資訊，請參閱下列指南。

- [Amazon Lightsail 物件儲存服務中儲存貯體的存取記錄](#)
  - [存取 Amazon Lightsail 物件儲存服務中儲存貯體的日誌格式](#)
  - [在 Amazon Lightsail 物件儲存服務中啟用儲存貯體的存取記錄功能](#)
  - [在 Amazon Lightsail 中使用儲存貯體的存取日誌來識別請求](#)
6. 建立 IAM 政策，讓使用者能夠在 Lightsail 中管理值區。如需詳細資訊，請參閱[在 Amazon Lightsail 中管理儲存貯體的 IAM 政策](#)。
  7. 了解儲存貯體中物件的標記和識別方式。如需詳細資訊，請參閱[了解 Amazon Lightsail 中的物件金鑰名稱](#)。
  8. 了解如何在儲存貯體中上傳檔案及管理物件。如需詳細資訊，請參閱下列指南。
    - [將文件上傳到 Amazon Lightsail](#)
    - [使用多部分上傳將檔案上傳到 Amazon Lightsail 中的儲存貯體](#)
    - [檢視儲存貯體中 Amazon Lightsail](#)
    - [在 Amazon Lightsail 中複製或移動值區中的物件](#)
    - [從儲存貯體下 Amazon Lightsail](#)
    - [在 Amazon Lightsail 中過濾存儲桶中的對象](#)
    - [標記存儲桶中 Amazon Lightsail](#)
    - [刪除存儲桶中 Amazon Lightsail](#)
  9. 啟用物件版本控制功能來保留、擷取和恢復儲存貯體中所儲存每個物件的各個版本。如需詳細資訊，請參閱在 [Amazon Lightsail 中啟用和暫停儲存貯體中的物件版本控制](#)。
  10. 啟用物件版本控制之後，可以還原儲存貯體中物件的先前版本。如需詳細資訊，請參閱在 [Amazon Lightsail 中還原儲存貯體中的舊版物件](#)。
  11. 監控儲存貯體的使用率。如需詳細資訊，請參閱[在 Amazon Lightsail 中檢視儲存貯體的指標](#)。
  12. 設定儲存貯體指標的警示，以便在儲存貯體的使用率超過閾值時收到通知。如需詳細資訊，請參閱[在 Amazon Lightsail 中建立儲存貯體指標警示](#)。
  13. 如果儲存空間和網路傳輸不足，請變更儲存貯體的儲存計畫。如需詳細資訊，請參閱[在 Amazon Lightsail 中變更儲存貯體的計畫](#)。
  14. 了解如何將儲存貯體連線至其他資源。如需詳細資訊，請參閱下列教學課程。
    - [教學課程：將 WordPress 執行個體連接至 Amazon Lightsail 儲存貯體](#)
    - [教學課程：將 Amazon Lightsail 儲存貯體與 Lightsail 內容交付網路分發搭配使用](#)
  15. 如果不再使用儲存貯體，請刪除它。如需詳細資訊，請參閱[刪除儲存貯體](#)。

## 主題

- [使用公制警報監控 Lightsail 桶儲存空間](#)

## 使用公制警報監控 Lightsail 桶儲存空間

您可以建立 Amazon Lightsail 警示來監控單一儲存貯體指標。您可將警示設定為根據您所指定閾值的相對指標值來通知您。通知可以是 Lightsail 主控台中顯示的橫幅、傳送至您的電子郵件地址的電子郵件，以及傳送至您的行動電話號碼的簡訊。如需有關警示的詳細資訊，請參閱[警示](#)。

## 內容

- [儲存貯體警示限制](#)
- [設定儲存貯體警示的最佳實務](#)
- [預設警示設定](#)
- [使用 Lightsail 主控台建立值區度量警示](#)
- [使用 Lightsail 主控台測試值區公制警示](#)
- [建立儲存貯體警示後的後續步驟](#)

## 儲存貯體警示限制

下列限制適用於警示：

- 您可以為每個指標設定兩個警示。
- 警示的評估間隔為 5 分鐘，而警示的每個資料點都代表為期 5 分鐘的彙總指標資料。
- 如果您將警示設定為透過電子郵件和/或簡訊通知您，則您只能將警示設定為在警示狀態更改為 OK 時通知您。
- 只有將警示設定為透過電子郵件和/或簡訊通知您，才能測試 OK 警示通知。
- 如果您將警示設定為透過電子郵件和/或簡訊通知您，並且如果您為遺失的資料點選擇 Do not evaluate the missing data (不評估遺失資料) 選項，則您只能將警示設定為在警示狀態更改為 INSUFFICIENT\_DATA 時通知您。
- 您只能在警示處於 OK (正常) 狀態時測試通知。

## 設定儲存貯體警示的最佳實務

設定儲存貯體的指標警示之前，您應該先決定要收到的通知內容。例如，考慮到儲存貯體大小，您可能希望在儲存貯體幾乎已滿時收到通知。如果您的儲存貯體目前計劃包含 5 GB 的儲存空間，則您可能需要為儲存貯體大小指標達到 4.5 GB 時設定警示。然後，您就會收到通知，讓您還有足夠的時間來擴大儲存貯體計劃的規模。

### 預設警示設定

當您在 Lightsail 主控台中新增開鐘時，會預先填入預設開鐘設定。這是您所選指標的建議警示組態。不過，您應該確認預設警示組態適合您的資源。例如，儲存貯體大小位元組指標的預設警示閾值為大於或等於 75 GB。但是，如果儲存貯體設定為只有 5 GB 的儲存空間，該請求閾值可能會太高。您可以將警示閾值修改為等於或大於 4.5 GB。

### 使用 Lightsail 主控台建立值區度量警示

若要使用 Lightsail 主控台建立值區度量警示，請完成下列步驟。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁上，選擇儲存空間索引標籤。
3. 選擇您要建立警示之儲存貯體的名稱。
4. 選擇儲存貯體管理頁面上的 Metrics (指標) 索引標籤。
5. 在 Metrics Graphs (指標圖表) 標題下的下拉式功能表中，選擇您要建立其警示的指標。如需詳細資訊，請參閱[資源指標](#)。
6. 選擇該頁面 Alarms (警示) 區段中的 Add alarm (新增警示)。
7. 在下拉式功能表中選擇比較運算子值。範例值為大於或等於、大於、小於或小於或等於。
8. 輸入警示的閾值。
9. 輸入要警示的資料點。
10. 選擇評估期間。期間可以 5 分鐘的增量指定 (從 5 分鐘到 24 小時)。
11. 選擇下列其中一種通知方法：
  - 電子郵件 — 當警示狀態變更為 ALARM 時，您會透過電子郵件收到通知。
  - 簡訊 — 當警示狀態變更為 ALARM 時，您會透過簡訊收到通知。所有 AWS 區域都不支援簡訊，而且無法將簡訊傳送到所有國家/區域。如需詳細資訊，請參閱[簡訊支援](#)。

**Note**

如果您選擇透過電子郵件或簡訊收到通知，但尚未在資源的 AWS 區域中設定通知聯絡人，則您需要新增電子郵件地址或行動電話號碼。如需詳細資訊，請參閱[通知](#)。

12. (選擇性) 選擇 Send me a notification when the alarm state change to OK (當警示狀態變更為正常時傳送通知給我)，以便在警示狀態變更為 OK (正常) 時收到通知。只有在您選擇透過電子郵件或簡訊收到通知時，才能使用此選項。
13. (選擇性) 選擇 Advanced settings (進階設定)，然後選擇下列其中一個選項：
  - 選擇警示應如何處理遺失的資料。可用的選項如下：
    - 假設其不在閾值內 (違反閾值) — 遺失資料點會被視為「不良」並違反閾值。
    - 假設其在閾值內 (未違反閾值) — 遺失資料點會被視為「良好」且在閾值內。
    - 使用最後一個良好資料點的值 (忽略並維持目前的警示狀態) – 維持目前的警示狀態。
    - 不要評估 (將遺失的資料視為遺失) — 警示在評估是否要變更狀態時不會考慮遺失的資料點。
  - 選擇 Send a notification if there is insufficient data (如果資料不足則傳送通知)，以在警示狀態變更為 INSUFFICIENT\_DATA 時收到通知。只有在您選擇透過電子郵件或簡訊收到通知時，才能使用此選項。
14. 選擇 Create (建立) 以新增警示。

若要稍後編輯警示，請選擇您要編輯的警示旁邊的省略符號圖示 (:)，然後選擇編輯警示。

## 使用 Lightsail 主控台測試值區公制警示

請完成下列步驟，以使用 Lightsail 主控台測試警示。您可以測試警示，確認所設定的通知選項是否能運作，例如：確保在觸發警示時收到電子郵件或簡訊。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁上，選擇儲存空間索引標籤。
3. 選擇您要測試警示之儲存貯體的名稱。
4. 選擇儲存貯體管理頁面上的 Metrics (指標) 索引標籤。
5. 在 Metrics Graphs (指標圖表) 標題下的下拉式功能表中，選擇您要測試其警示的指標。
6. 向下捲動至頁面的警示區段，然後選擇您要測試的警示旁邊的省略符號圖示 (:)

## 7. 請選擇下列其中一個選項：

- 測試警示通知 – 選擇此選項可在警示狀態變更為 ALARM 時測試通知。
- 測試正常通知 – 選擇此選項可在警示狀態變更為 OK 時測試通知。

### Note

如果無法使用上述任何一個選項，則表示您可能尚未設定警示的通知選項，或警示可能目前處於 ALARM 狀態。如需詳細資訊，請參閱[儲存貯體警示限制](#)。

根據您選擇的測試選項，警示會暫時變更為 ALARM 或 OK 狀態，並根據您為警示設定的通知方法來傳送電子郵件和/或簡訊。只有當您選擇測試通知時，Lightsail 主控台才會顯示 ALARM 通知橫幅。如果您選擇測試 OK 通知，則不會顯示通知橫幅。警示通常會在幾秒鐘後回到其實際狀態。

## 建立儲存貯體警示後的後續步驟

您可以為儲存貯體警示執行一些其他任務：

- 若要停止接收通知，您可以從 Lightsail 移除電子郵件和行動電話。如需詳細資訊，請參閱[刪除通知聯絡人](#)。您也可以停用或刪除警示，以停止接收特定警示的通知。如需詳細資訊，請參閱[刪除或停用指標警示](#)。

## 監控 Lightsail 容器服務資源使用率

建立 Amazon Lightsail 容器服務之後，您可以在服務管理頁面的 Metrics (指標) 索引標籤上檢視其指標圖表。監控指標是維護資源可靠性、可用性與效能的重要環節。定期監控並從您的資源收集指標資料，即可更輕鬆地進行多點失敗的偵錯。如需有關指標的詳細資訊，請參閱[Amazon Lightsail 中的指標](#)。

監控資源時，您應該在環境中建立正常資源效能的基準。

### Note

容器服務指標目前不支援警示和通知。

## 容器服務指標

以下是可用的容器服務指標：

- CPU 使用率 — 目前在容器服務上跨全部節點使用的運算單位的平均百分比。此指標可識別在容器服務上執行容器所需的處理能力。
- 記憶體使用率 — 目前在容器服務上跨全部節點使用的記憶體的平均百分比。此指標會識別在容器服務上執行容器所需的記憶體。

### Note

如果您建立新的部署，則容器服務的現有使用率指標將會消失，並且只顯示目前新部署的指標。

## 在 Lightsail 主控台中檢視容器服務指標

請完成下列程序，以在 Lightsail 主控台中檢視容器服務指標。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁，選擇 Containers (容器) 索引標籤。
3. 選擇要檢視指標的容器名稱。
4. 選擇容器服務管理頁面上的 Metrics (指標) 索引標籤。
5. 在 Metrics graphs (指標圖表) 標題下的下拉式選單中，選擇您要檢視的指標。

圖表會顯示所選指標的資料點視覺化呈現。

6. 您可以在指標圖表上執行下列動作：
  - 變更圖表的檢視，以顯示 1 小時、6 小時、1 天、1 週和 2 週的資料。
  - 將游標暫停在資料點上，以檢視有關該資料點的詳細資訊。

### Note

容器服務指標目前不支援警示和通知。

## 監控資料庫 Lightsail 能測量結果

在 Amazon Lightsail 中啟動資料庫之後，您可以在資料庫管理頁面的「指標」索引標籤上檢視其指標圖形。監控指標是維護資源可靠性、可用性與效能的重要環節。定期監控並從您的資源收集指標資料，即可更輕鬆地進行多點失敗的偵錯。如需指標的詳細資訊，請參閱[指標](#)。

監控資源時，您應該在環境中建立正常資源效能的基準。建立基準之後，您可以在 Lightsail 主控台中設定警示，以在資源執行超出指定閾值時通知您。如需詳細資訊，請參閱[通知](#)和[警示](#)。

### 內容

- [資料庫指標](#)
- [檢視資料庫指標](#)
- [檢視資料庫指標後的後續步驟](#)

## 資料庫指標

下列是可用的資料庫指標：

- CPU 使用率 (**CPUUtilization**) – 資料庫目前使用的 CPU 使用率百分比。
- 資料庫連線 (**DatabaseConnections**) – 使用中的資料庫連線數量。
- 磁碟佇列深度 (**DiskQueueDepth**) – 正在等待存取磁碟的未完成 IO (讀/寫請求) 數量。
- 可用儲存空間 (**FreeStorageSpace**) – 可用儲存空間的數量。
- 網路接收輸送量 (**NetworkReceiveThroughput**) – 資料庫的傳入 (接收) 網路流量，包括客戶資料庫流量及用於監控與複寫的 AWS 流量。
- 網路傳輸輸送量 (**NetworkTransmitThroughput**) – 資料庫的傳出 (傳輸) 網路流量，包括客戶資料庫流量及用於監控與複寫的 AWS 流量。

## 在 Lightsail 主控台中檢視資料庫度量

完成下列步驟，即可在 Lightsail 主控台中檢視資料庫度量。

1. 登入主 [Lightsail](#) 台。
2. 在 Lightsail 首頁上，選擇「資料庫」索引標籤。
3. 選擇要檢視指標的資料庫名稱。
4. 選擇資料庫管理頁面上的 Metrics (指標) 標籤。

5. 在 Metrics graphs (指標圖表) 標題下的下拉式選單中，選擇您要檢視的指標。

圖表會顯示所選指標的資料點視覺化呈現。

6. 您可以在指標圖表上執行下列動作：

- 變更圖表的檢視，以顯示 1 小時、6 小時、1 天、1 週和 2 週的資料。
- 將游標暫停在資料點上，以檢視有關該資料點的詳細資訊。
- 新增所選指標的警示，以在指標超過您指定的閾值時收到通知。如需詳細資訊，請參閱[警示](#)和[建立資料庫指標警示](#)。

## 檢視資料庫指標後的後續步驟

您可以為資料庫指標執行一些其他工作：

- 新增所選指標的警示，以在指標超過您指定的閾值時收到通知。如需詳細資訊，請參閱[警示](#)和[建立資料庫指標警示](#)。
- 觸發警示時，Lightsail 主控台中會顯示通知橫幅。若要透過電子郵件和 SMS 簡訊收到通知，您必須將您的電子郵件地址和行動電話號碼新增為通知聯絡人，並 AWS 區域 在每個您想要監控資源的位置中。如需詳細資訊，請參閱[新增通知聯絡人](#)。
- 若要停止接收通知，您可以從 Lightsail 移除電子郵件和行動電話。如需詳細資訊，請參閱[刪除或停用指標警示](#)。您也可以停用或刪除警示，以停止接收特定警示的通知。如需詳細資訊，請參閱[刪除或停用指標警示](#)。

### 主題

- [使用度量警示來監控 Lightsail 資料庫健康](#)

## 使用度量警示來監控 Lightsail 資料庫健康

您可以建立監視單一資料庫指標的 Amazon Lightsail 警示。您可將警示設定為根據您所指定閾值的相對指標值來通知您。通知可以是 Lightsail 主控台中顯示的橫幅、傳送至您的電子郵件地址的電子郵件，以及傳送至您的行動電話號碼的簡訊。如需有關警示的詳細資訊，請參閱[警示](#)。

### 內容

- [資料庫警示限制](#)
- [設定資料庫警示的最佳實務](#)

- [預設警示設定](#)
- [使用 Lightsail 主控台建立資料庫度量警示](#)
- [使用 Lightsail 主控台測試資料庫度量警示](#)
- [建立資料庫警示後的後續步驟](#)

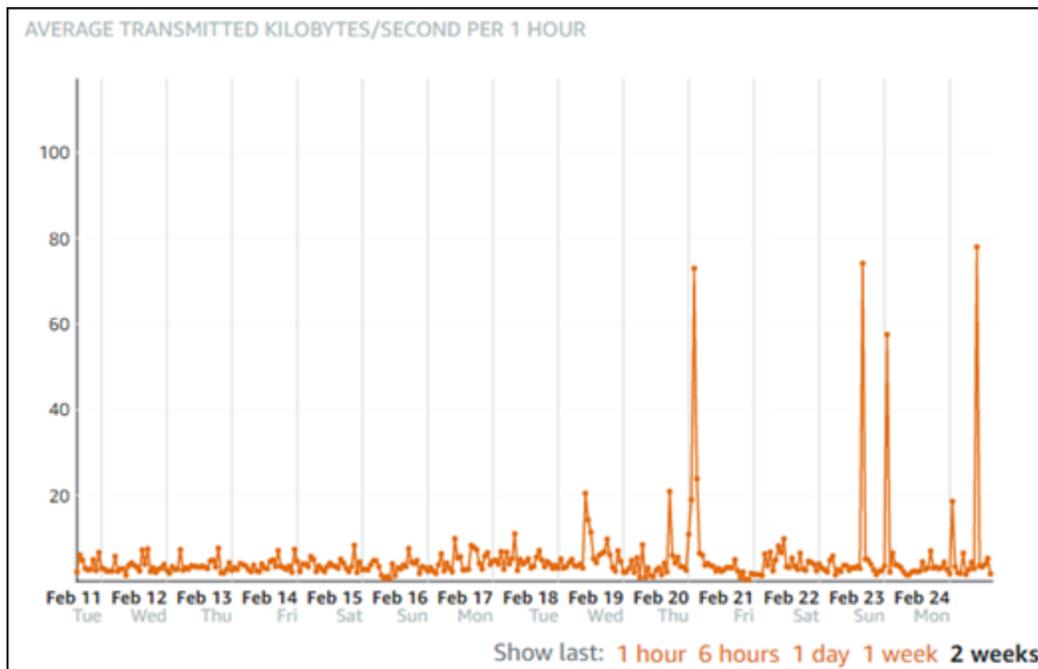
## 資料庫警示限制

下列限制適用於警示：

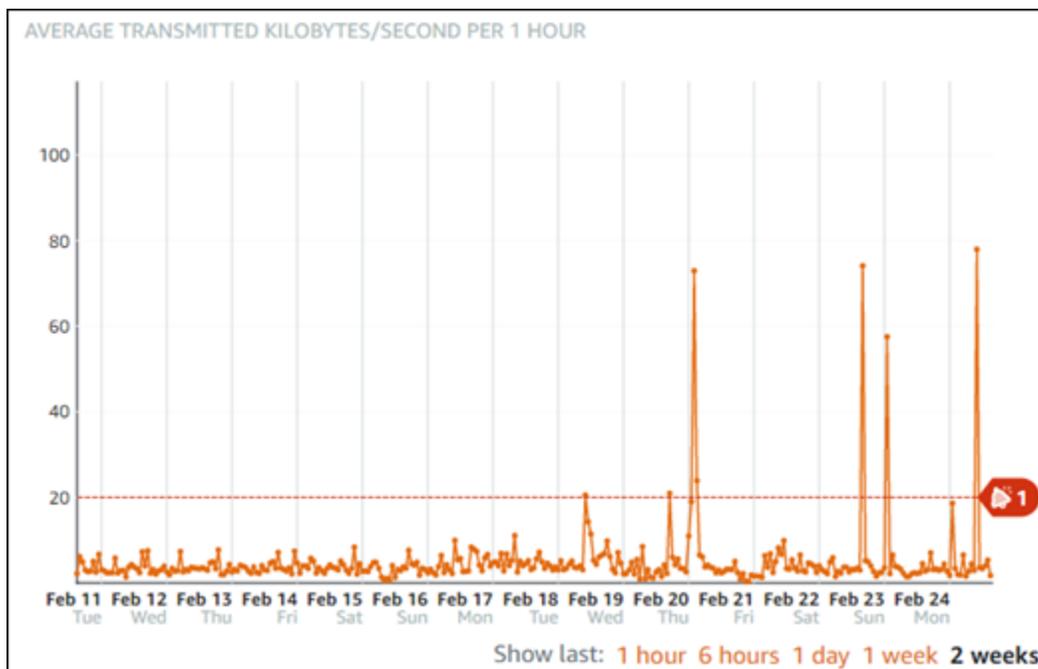
- 您可以為每個指標設定兩個警示。
- 警示的評估間隔為 5 分鐘，而警示的每個資料點都代表為期 5 分鐘的彙總指標資料。
- 如果您將警示設定為透過電子郵件和/或簡訊通知您，則您只能將警示設定為在警示狀態更改為 OK 時通知您。
- 只有將警示設定為透過電子郵件和/或簡訊通知您，才能測試 OK 警示通知。
- 如果您將警示設定為透過電子郵件和/或簡訊通知您，並且如果您為遺失的資料點選擇 Do not evaluate the missing data (不評估遺失資料) 選項，則您只能將警示設定為在警示狀態更改為 INSUFFICIENT\_DATA 時通知您。
- 您只能在警示處於 OK (正常) 狀態時測試通知。

## 設定資料庫警示的最佳實務

設定資料庫的指標警示之前，您應該先檢視指標的歷史資料。識別過去兩週期間內的低層級、中層級和高層級。在下列網路傳輸輸送量 (NetworkTransmitThroughput) 指標圖表範例中，低層級為每小時 0-10 KB/秒、中層級介於每小時 10-20 KB/秒之間，而高層級介於每小時 20-80 KB/秒之間。



如果您將警示閾值設定為 greater than or equal to (大於或等於) 低層範圍中的某處 (例如，每小時 5 KB/秒)，則會收到更頻繁且可能不必要的警示通知。如果您將警示閾值設定為 greater than or equal to (大於或等於) 高層範圍中的某處 (例如每小時 20 KB)，則會收到較不頻繁的警示通知，但調查可能更為重要。當您設定警示並加以啟用時，圖表上會出現代表閾值的警示線，如下列範例所示。標示為 1 的警示線代表警示 1 的閾值，標示為 2 的警示線代表警示 2 的閾值。



## 預設警示設定

當您在 Lightsail 主控台中新增鬧鐘時，會預先填入預設鬧鐘設定。這是您所選指標的建議警示組態。不過，您應該確認預設警示組態適合您的資源。例如，可用儲存空間 (FreeStorageSpace) 指標的預設警示閾值為在過去 5 分鐘內 less than (小於) 5 個位元組一次。不過，對您的資料庫而言，可用儲存空間閾值可能太低。您可以在將警示閾值修改為在過去 5 分鐘內 less than (小於) 4 GB 一次。

## 使用 Lightsail 主控台建立資料庫度量警示

若要使用 Lightsail 主控台建立資料庫度量警示，請完成下列步驟。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁上，選擇「資料庫」索引標籤。
3. 選擇您要建立警示的資料庫名稱。
4. 選擇資料庫管理頁面上的 Metrics (指標) 標籤。
5. 在 Metrics Graphs (指標圖表) 標題下的下拉式功能表中，選擇您要建立其警示的指標。如需詳細資訊，請參閱[資源指標](#)。
6. 選擇該頁面 Alarms (警示) 區段中的 Add alarm (新增警示)。
7. 在下拉式功能表中選擇比較運算子值。範例值為大於或等於、大於、小於或小於或等於。
8. 輸入警示的閾值。
9. 輸入要警示的資料點。
10. 選擇評估期間。期間可以 5 分鐘的增量指定 (從 5 分鐘到 24 小時)。
11. 選擇下列其中一種通知方法：
  - 電子郵件 — 當警示狀態變更為 ALARM 時，您會透過電子郵件收到通知。
  - 簡訊 — 當警示狀態變更為 ALARM 時，您會透過簡訊收到通知。您可以在其中建立 Lightsail 資源的所有 AWS 區域都不支援 SMS 簡訊，而且 SMS 文字訊息無法傳送到所有國家/地區。如需詳細資訊，請參閱[簡訊支援](#)。

### Note

如果您選擇透過電子郵件或簡訊收到通知，但尚未在資源的 AWS 區域中設定通知聯絡人，則您需要新增電子郵件地址或行動電話號碼。如需詳細資訊，請參閱[通知](#)。

12. (選擇性) 選擇 Send me a notification when the alarm state change to OK (當警示狀態變更為正常時傳送通知給我)，以便在警示狀態變更為 OK (正常) 時收到通知。只有在您選擇透過電子郵件或簡訊收到通知時，才能使用此選項。
13. (選擇性) 選擇 Advanced settings (進階設定)，然後選擇下列其中一個選項：
  - 選擇警示應如何處理遺失的資料。可用的選項如下：
    - 假設其不在閾值內 (違反閾值) — 遺失資料點會被視為「不良」並違反閾值。
    - 假設其在閾值內 (未違反閾值) — 遺失資料點會被視為「良好」且在閾值內。
    - 使用最後一個良好資料點的值 (忽略並維持目前的警示狀態) – 維持目前的警示狀態。
    - 不要評估 (將遺失的資料視為遺失) — 警示在評估是否要變更狀態時不會考慮遺失的資料點。
  - 選擇 Send a notification if there is insufficient data (如果資料不足則傳送通知)，以在警示狀態變更為 INSUFFICIENT\_DATA 時收到通知。只有在您選擇透過電子郵件或簡訊收到通知時，才能使用此選項。
14. 選擇 Create (建立) 以新增警示。

若要稍後編輯警示，請選擇您要編輯的警示旁邊的省略符號圖示 (:)，然後選擇編輯警示。

## 使用 Lightsail 主控台測試資料庫度量警示

請完成下列步驟，以使用 Lightsail 主控台測試警示。您可以測試警示，確認所設定的通知選項是否能運作，例如：確保在觸發警示時收到電子郵件或簡訊。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁上，選擇「資料庫」索引標籤。
3. 選擇您要測試警示的資料庫名稱。
4. 選擇資料庫管理頁面上的 Metrics (指標) 標籤。
5. 在 Metrics Graphs (指標圖表) 標題下的下拉式功能表中，選擇您要測試其警示的指標。
6. 向下捲動至頁面的警示區段，然後選擇您要測試的警示旁邊的省略符號圖示 (:)
7. 請選擇下列其中一個選項：
  - 測試警示通知 – 選擇此選項可在警示狀態變更為 ALARM 時測試通知。
  - 測試正常通知 – 選擇此選項可在警示狀態變更為 OK 時測試通知。

**Note**

如果無法使用上述任何一個選項，則表示您可能尚未設定警示的通知選項，或警示可能目前處於 ALARM 狀態。如需詳細資訊，請參閱[資料庫警示限制](#)。

根據您選擇的測試選項，警示會暫時變更為 ALARM 或 OK 狀態，並根據您為警示設定的通知方法來傳送電子郵件和/或簡訊。只有當您選擇測試通知時，Lightsail 主控台才會顯示 ALARM 通知橫幅。如果您選擇測試 OK 通知，則不會顯示通知橫幅。警示通常會在幾秒鐘後回到其實際狀態。

## 建立資料庫警示後的後續步驟

您可以為資料庫警示執行一些其他工作：

- 若要停止接收通知，您可以從 Lightsail 移除電子郵件和行動電話。如需詳細資訊，請參閱[刪除通知聯絡人](#)。您也可以停用或刪除警示，以停止接收特定警示的通知。如需詳細資訊，請參閱[刪除或停用指標警示](#)。

## 監控 Lightsail 分佈效能指標

在 Amazon Lightsail 中建立分發後，您可以在分發管理頁面的「指標」索引標籤上檢視其指標圖形。監控指標是維護資源可靠性、可用性與效能的重要環節。定期監控並從您的資源收集指標資料，即可更輕鬆地進行多點失敗的偵錯。如需指標的詳細資訊，請參閱[指標](#)。

監控資源時，您應該在環境中建立正常資源效能的基準。然後您可在 Lightsail 主控台中設定警示，以在資源執行超出指定閾值時通知您。如需詳細資訊，請參閱[通知](#)和[警示](#)。

內容

- [分發指標](#)
- [在 Lightsail 主控台中檢視分佈指標](#)
- [檢視分發指標後的後續步驟](#)

## 分發指標

以下是可用的分發指標：

- 請求 – 對於所有 HTTP 方法以及 HTTP 和 HTTPS 請求，您的分發收到的檢視器請求總數。
- 上傳的位元組 – 使用 POST 和 PUT 請求，透過您的分發上傳至原始伺服器的位元組數量。
- 下載的位元組 – 檢視器為 GET、HEAD 及 OPTIONS 請求下載的位元組數量。
- 總錯誤率 – 當回應的 HTTP 狀態碼為 4xx 或 5xx 時，全部檢視器請求的百分比。
- HTTP 4xx 錯誤率 – 當回應的 HTTP 狀態碼為 4xx 時，全部檢視器請求的百分比。在這些情況下，用戶端或用戶端檢視器可能發生錯誤。例如，404 (未找到) 狀態碼表示未找到用戶端請求的物件。
- HTTP 5xx 錯誤率 – 當回應的 HTTP 狀態碼為 5xx 時，全部檢視器請求的百分比。在這些情況下，原始伺服器不滿足要求。例如，503 (服務無法使用) 狀態碼表示原始伺服器目前無法使用。

## 在 Lightsail 主控台中檢視分佈指標

請完成下列程序，以在 Lightsail 主控台中檢視分佈量度。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁，選擇 Networking (聯網) 索引標籤。
3. 選擇要檢視指標的分發名稱。
4. 選擇分發管理頁面上的 Metrics (指標) 索引標籤。
5. 在 Metrics graphs (指標圖表) 標題下的下拉式選單中，選擇您要檢視的指標。

圖表會顯示所選指標的資料點視覺化呈現。

6. 您可以在指標圖表上執行下列動作：
  - 變更圖表的檢視，以顯示 1 小時、6 小時、1 天、1 週和 2 週的資料。
  - 將游標暫停在資料點上，以檢視有關該資料點的詳細資訊。
  - 新增所選指標的警示，以在指標超過您指定的閾值時收到通知。如需詳細資訊，請參閱 [警示](#) 和 [建立執行個體指標警示](#)。

## 檢視分發指標後的後續步驟

您可以為分發指標執行一些其他任務：

- 新增所選指標的警示，以在指標超過您指定的閾值時收到通知。如需詳細資訊，請參閱 [警示](#) 和 [建立分發指標警示](#)。

- 觸發警示時，Lightsail 主控台中會顯示通知橫幅。若要透過電子郵件和 SMS 簡訊收到通知，您必須將您的電子郵件地址和行動電話號碼新增為通知聯絡人，並 AWS 區域 在每個您想要監控資源的位置中。如需詳細資訊，請參閱[新增通知聯絡人](#)。
- 若要停止接收通知，您可以從 Lightsail 移除電子郵件和行動電話。如需詳細資訊，請參閱[刪除或停用指標警示](#)。您也可以停用或刪除警示，以停止接收特定警示的通知。如需詳細資訊，請參閱[刪除或停用指標警示](#)。

## 主題

- [使用公制警示監控 Lightsail 分配健康狀態](#)

## 使用公制警示監控 Lightsail 分配健康狀態

您可以建立監視單一分發指標的 Amazon Lightsail 警示。您可將警示設定為根據您所指定閾值的相對指標值來通知您。通知可以是 Lightsail 主控台中顯示的橫幅、傳送至您的電子郵件地址的電子郵件，以及傳送至您的行動電話號碼的簡訊。如需有關警示的詳細資訊，請參閱[警示](#)。

## 內容

- [分發警示限制](#)
- [設定分發警示的最佳實務](#)
- [預設警示設定](#)
- [使用 Lightsail 主控台建立分配量度警示](#)
- [測試分發指標警示](#)
- [建立分發警示後的後續步驟](#)

## 分發警示限制

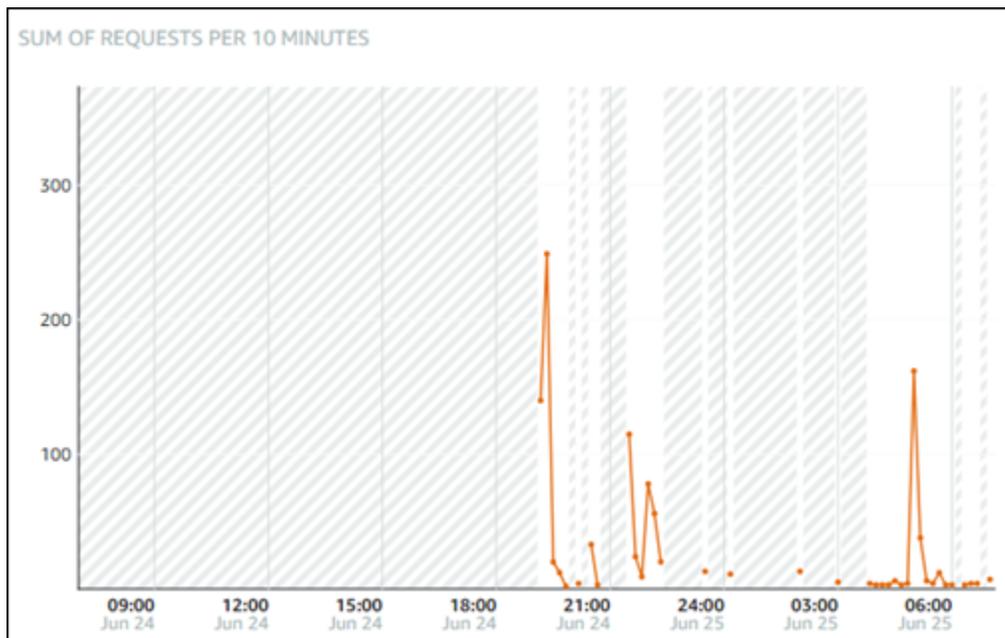
下列限制適用於警示：

- 您可以為每個指標設定兩個警示。
- 警示的評估間隔為 5 分鐘，而警示的每個資料點都代表為期 5 分鐘的彙總指標資料。
- 如果您將警示設定為透過電子郵件和/或簡訊通知您，則您只能將警示設定為在警示狀態更改為 OK 時通知您。
- 只有將警示設定為透過電子郵件和/或簡訊通知您，才能測試 OK 警示通知。

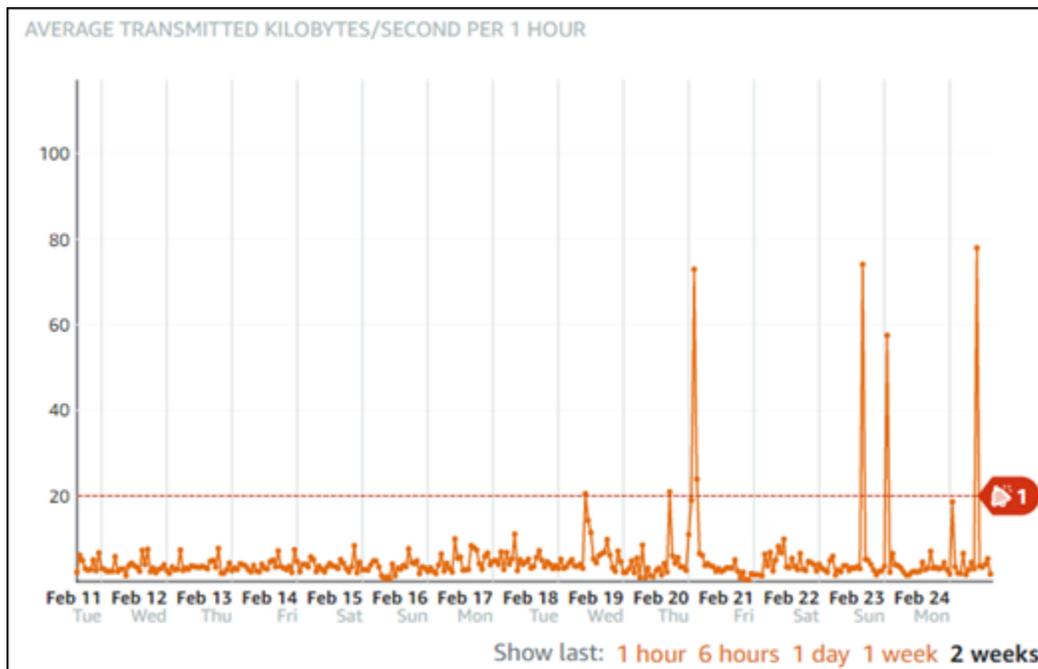
- 如果您將警示設定為透過電子郵件和/或簡訊通知您，並且如果您為遺失的資料點選擇 Do not evaluate the missing data (不評估遺失資料) 選項，則您只能將警示設定為在警示狀態更改為 INSUFFICIENT\_DATA 時通知您。
- 您只能在警示處於 OK (正常) 狀態時測試通知。

## 設定分發警示的最佳實務

設定分發的指標警示之前，您應該先檢視指標的歷史資料。識別過去兩週期間內的低層級、中層級和高層級。在以下請求指標圖表範例中，低層介於 0-10 個請求之間，中層介於 10-50 個請求之間，而高層介於 50-250 個請求之間。



如果您將警示閾值設定為 greater than or equal to (大於或等於) 低層範圍中的某處 (例如 5 個請求)，則會收到更頻繁且可能不必要的警示通知。如果您將警示閾值設定為 greater than or equal to (大於或等於) 高層範圍中的某處 (例如 150 個請求)，則會收到較不頻繁的警示通知，但調查可能更為重要。當您設定警示並加以啟用時，圖表上會出現代表閾值的警示線，如下列範例所示。標示為 1 的警示線代表警示 1 的閾值，標示為 2 的警示線代表警示 2 的閾值。



## 預設警示設定

當您在 Lightsail 主控台中新增開鐘時，會預先填入預設開鐘設定。這是您所選指標的建議警示組態。不過，您應該確認預設警示組態適合您的資源。例如，請求指標的預設警示閾值在過去 15 分鐘內 3 次大於 45 個請求。不過，對您的分發來說，該請求閾值可能太低。您可能需要將警示閾值修改為在過去 15 分鐘內 greater than (大於) 150 個請求 3 次。

## 使用 Lightsail 主控台建立分配量度警示

若要使用 Lightsail 主控台建立分配量度警示，請完成下列步驟。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁，選擇 Networking (聯網) 索引標籤。
3. 選擇您要建立警示之分發的名稱。
4. 選擇分發管理頁面上的 Metrics (指標) 索引標籤。
5. 在 Metrics Graphs (指標圖表) 標題下的下拉式功能表中，選擇您要建立其警示的指標。如需詳細資訊，請參閱[資源指標](#)。
6. 選擇該頁面 Alarms (警示) 區段中的 Add alarm (新增警示)。
7. 在下拉式功能表中選擇比較運算子值。範例值為大於或等於、大於、小於或小於或等於。
8. 輸入警示的閾值。
9. 輸入要警示的資料點。

10. 選擇評估期間。期間可以 5 分鐘的增量指定 (從 5 分鐘到 24 小時)。
11. 選擇下列其中一種通知方法：
  - 電子郵件 — 當警示狀態變更為 ALARM 時，您會透過電子郵件收到通知。
  - 簡訊 — 當警示狀態變更為 ALARM 時，您會透過簡訊收到通知。您可以在其中建立 Lightsail 資源的所有 AWS 區域都不支援 SMS 簡訊，而且 SMS 文字訊息無法傳送到所有國家/地區。如需詳細資訊，請參閱[簡訊支援](#)。

#### Note

如果您選擇透過電子郵件或簡訊收到通知，但尚未在資源的 AWS 區域中設定通知聯絡人，則您需要新增電子郵件地址或行動電話號碼。如需詳細資訊，請參閱[通知](#)。

12. (選擇性) 選擇 Send me a notification when the alarm state change to OK (當警示狀態變更為正常時傳送通知給我)，以便在警示狀態變更為 OK (正常) 時收到通知。只有在您選擇透過電子郵件或簡訊收到通知時，才能使用此選項。
13. (選擇性) 選擇 Advanced settings (進階設定)，然後選擇下列其中一個選項：
  - 選擇警示應如何處理遺失的資料。可用的選項如下：
    - 假設其不在閾值內 (違反閾值) — 遺失資料點會被視為「不良」並違反閾值。
    - 假設其在閾值內 (未違反閾值) — 遺失資料點會被視為「良好」且在閾值內。
    - 使用最後一個良好資料點的值 (忽略並維持目前的警示狀態) — 維持目前的警示狀態。
    - 不要評估 (將遺失的資料視為遺失) — 警示在評估是否要變更狀態時不會考慮遺失的資料點。
  - 選擇 Send a notification if there is insufficient data (如果資料不足則傳送通知)，以在警示狀態變更為 INSUFFICIENT\_DATA 時收到通知。只有在您選擇透過電子郵件或簡訊收到通知時，才能使用此選項。
14. 選擇 Create (建立) 以新增警示。

若要稍後編輯警示，請選擇您要編輯的警示旁邊的省略符號圖示 (:)，然後選擇編輯警示。

## 測試分發指標警示

請完成下列步驟，以使用 Lightsail 主控台測試警示。您可以測試警示，確認所設定的通知選項是否能運作，例如：確保在觸發警示時收到電子郵件或簡訊。

1. 登入主 [Lightsail 台](#)。

2. 在 Lightsail 首頁，選擇 Networking (聯網) 索引標籤。
3. 選擇您要測試警示之分發的名稱。
4. 選擇分發管理頁面上的 Metrics (指標) 索引標籤。
5. 在 Metrics Graphs (指標圖表) 標題下的下拉式功能表中，選擇您要測試其警示的指標。
6. 向下捲動至頁面的警示區段，然後選擇您要測試的警示旁邊的省略符號圖示 (:)
7. 請選擇下列其中一個選項：
  - 測試警示通知 – 選擇此選項可在警示狀態變更為 ALARM 時測試通知。
  - 測試正常通知 – 選擇此選項可在警示狀態變更為 OK 時測試通知。

#### Note

如果無法使用上述任何一個選項，則表示您可能尚未設定警示的通知選項，或警示可能目前處於 ALARM 狀態。如需詳細資訊，請參閱[分發警示限制](#)。

根據您選擇的測試選項，警示會暫時變更為 ALARM 或 OK 狀態，並根據您為警示設定的通知方法來傳送電子郵件和/或簡訊。只有當您選擇測試通知時，Lightsail 主控台才會顯示 ALARM 通知橫幅。如果您選擇測試 OK 通知，則不會顯示通知橫幅。警示通常會在幾秒鐘後回到其實際狀態。

## 建立分發警示後的後續步驟

您可以為分發警示執行一些其他任務：

- 若要停止接收通知，您可以從 Lightsail 移除電子郵件和行動電話。如需詳細資訊，請參閱[刪除通知聯絡人](#)。您也可以停用或刪除警示，以停止接收特定警示的通知。如需詳細資訊，請參閱[刪除或停用指標警示](#)。

## 監控 Lightsail 負載平衡器健康狀態指

在 Amazon Lightsail 中建立負載平衡器並將執行個體連接至其後，您可以在負載平衡器管理頁面的指標索引標籤上檢視其指標圖形。監控指標是維護資源可靠性、可用性與效能的重要環節。定期監控並從您的資源收集指標資料，即可更輕鬆地進行多點失敗的偵錯。如需指標的詳細資訊，請參閱[指標](#)。

監控資源時，您應該在環境中建立正常資源效能的基準。建立基準之後，您可以在 Lightsail 主控台中設定警示，以在資源執行超出指定閾值時通知您。如需詳細資訊，請參閱[通知](#)和[警示](#)。

## 內容

- [負載平衡器指標](#)
- [檢視負載平衡器指標](#)
- [後續步驟](#)

## 負載平衡器指標

下列是可用的負載平衡器指標：

- 狀態正常的主機計數 (**HealthyHostCount**) – 視為狀態正常的目標執行個體數目。
- 狀態不正常的主機計數 (**UnhealthyHostCount**) – 視為狀態不正常目標執行個體數目。
- 負載平衡器 HTTP 4XX (**HTTPCode\_LB\_4XX\_Count**) – 源自於負載平衡器的 HTTP 4XX 用戶端錯誤碼數目。要求的格式不正確或不完整時，會產生用戶端錯誤。目標執行個體並未收到這些請求。此計數不包含目標執行個體產生的回應碼。
- 負載平衡器 HTTP 5XX (**HTTPCode\_LB\_5XX\_Count**) – 源自於負載平衡器的 HTTP 5XX 伺服器錯誤碼數目。其中不包含目標執行個體產生的任何回應碼。如果沒有狀態正常的執行個體附加至負載平衡器，或如果請求率超過執行個體 (溢出) 或負載平衡器的容量，則會回報此指標。
- 執行個體 HTTP 2XX (**HTTPCode\_Instance\_2XX\_Count**) – 目標執行個體所產生的 HTTP 2XX 回應碼數目。這未包含負載平衡器所產生的任何回應碼。
- 執行個體 HTTP 3XX (**HTTPCode\_Instance\_3XX\_Count**) – 目標執行個體所產生的 HTTP 3XX 回應碼數目。這未包含負載平衡器所產生的任何回應碼。
- 執行個體 HTTP 4XX (**HTTPCode\_Instance\_4XX\_Count**) – 目標執行個體所產生的 HTTP 4XX 回應碼數目。這未包含負載平衡器所產生的任何回應碼。
- 執行個體 HTTP 5XX (**HTTPCode\_Instance\_5XX\_Count**) – 目標執行個體所產生的 HTTP 5XX 回應碼數目。這未包含負載平衡器所產生的任何回應碼。
- 執行個體回應時間 (**InstanceResponseTime**) – 請求離開負載平衡器之後到收到目標執行個體回應之前所經歷的時間 (秒)。
- 用戶端 TLS 交涉錯誤計數 (**ClientTLSNegotiationErrorCount**) – 由於負載平衡器產生的 TLS 錯誤未與負載平衡器建立工作階段之用戶端所啟動的 TLS 連線數目。可能的原因包含晶片或協定不相符。
- 請求計數 (**RequestCount**) – 透過 IPv4 處理的請求數目。此計數只包含具有負載平衡器目標執行個體所產生之回應的要求。

- 拒絕的連線計數 (**RejectedConnectionCount**) – 因負載平衡器已達其連線數目上限而拒絕的連線數目。

## 檢視負載平衡器指標

完成下列步驟，即可在 Lightsail 主控台中檢視負載平衡器指標。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁，選擇 Networking (聯網) 索引標籤。
3. 選擇您要檢視指標的負載平衡器名稱。
4. 選擇負載平衡器管理頁面上的 Metrics (指標) 標籤。
5. 在 Metrics graphs (指標圖表) 標題下的下拉式選單中，選擇您要檢視的指標。

圖表會顯示所選指標的資料點視覺化呈現。

6. 您可以在指標圖表上執行下列動作：

- 變更圖表的檢視，以顯示 1 小時、6 小時、1 天、1 週和 2 週的資料。
- 將游標暫停在資料點上，以檢視有關該資料點的詳細資訊。
- 新增所選指標的警示，以在指標超過您指定的閾值時收到通知。如需詳細資訊，請參閱[警示](#)和[建立負載平衡器指標警示](#)。

## 後續步驟

您可以為負載平衡器指標執行一些其他工作：

- 新增所選指標的警示，以在指標超過您指定的閾值時收到通知。如需詳細資訊，請參閱[警示](#)和[建立負載平衡器指標警示](#)。
- 觸發警示時，Lightsail 主控台中會顯示通知橫幅。若要透過電子郵件和 SMS 簡訊收到通知，您必須將您的電子郵件地址和行動電話號碼新增為通知聯絡人，AWS 區域 在每個您想要監控資源的位置。如需詳細資訊，請參閱[新增通知聯絡人](#)。
- 若要停止接收通知，您可以從 Lightsail 移除電子郵件和行動電話。如需詳細資訊，請參閱[刪除或停用指標警示](#)。您也可以停用或刪除警示，以停止接收特定警示的通知。如需詳細資訊，請參閱[刪除或停用指標警示](#)。

## 主題

- [使用警示監控 Lightsail 負載平衡器指標](#)

## 使用警示監控 Lightsail 負載平衡器指標

您可以建立監控單一負載平衡器指標的 Amazon Lightsail 警示。您可將警示設定為根據您所指定閾值的相對指標值來通知您。通知可以是 Lightsail 主控台中顯示的橫幅、傳送至您的電子郵件地址的電子郵件，以及傳送至您的行動電話號碼的簡訊。如需有關警示的詳細資訊，請參閱[警示](#)。

### 內容

- [負載平衡器警示限制](#)
- [設定負載平衡器警示的最佳實務](#)
- [預設警示設定](#)
- [使用 Lightsail 主控台建立負載平衡器指標警示](#)
- [使用 Lightsail 主控台測試負載平衡器度量警示](#)
- [後續步驟](#)

### 負載平衡器警示限制

下列限制適用於警示：

- 您可以為每個指標設定兩個警示。
- 警示的評估間隔為 5 分鐘，而警示的每個資料點都代表為期 5 分鐘的彙總指標資料。
- 如果您將警示設定為透過電子郵件和/或簡訊通知您，則您只能將警示設定為在警示狀態更改為 OK 時通知您。
- 只有將警示設定為透過電子郵件和/或簡訊通知您，才能測試 OK 警示通知。
- 如果您將警示設定為透過電子郵件和/或簡訊通知您，並且如果您為遺失的資料點選擇 Do not evaluate the missing data (不評估遺失資料) 選項，則您只能將警示設定為在警示狀態更改為 INSUFFICIENT\_DATA 時通知您。
- 您只能在警示處於 OK (正常) 狀態時測試通知。

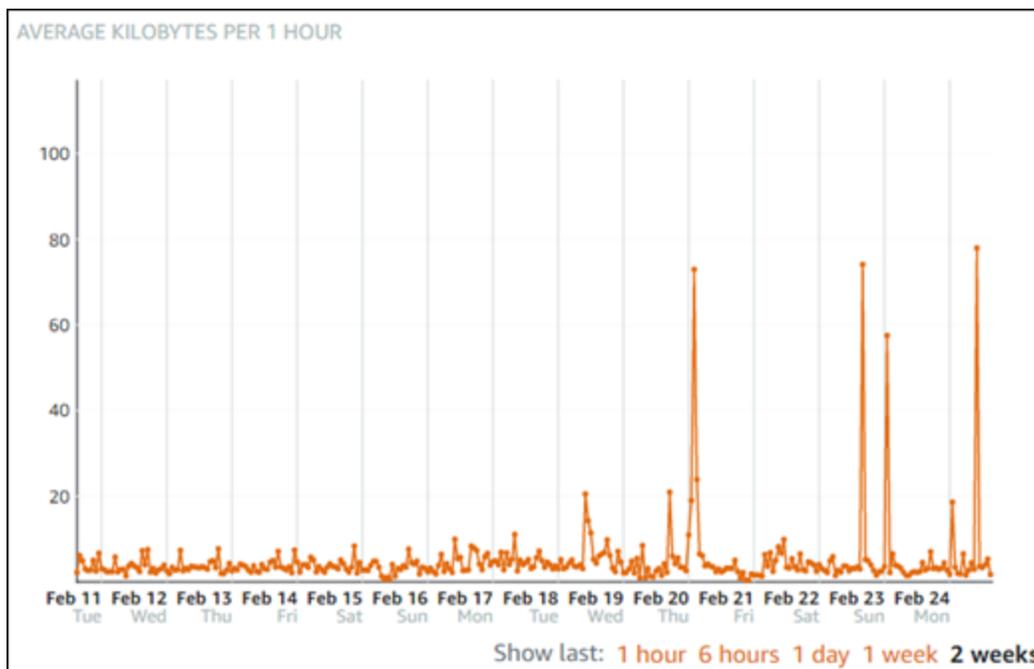
### 設定負載平衡器警示的最佳實務

下列限制適用於警示：

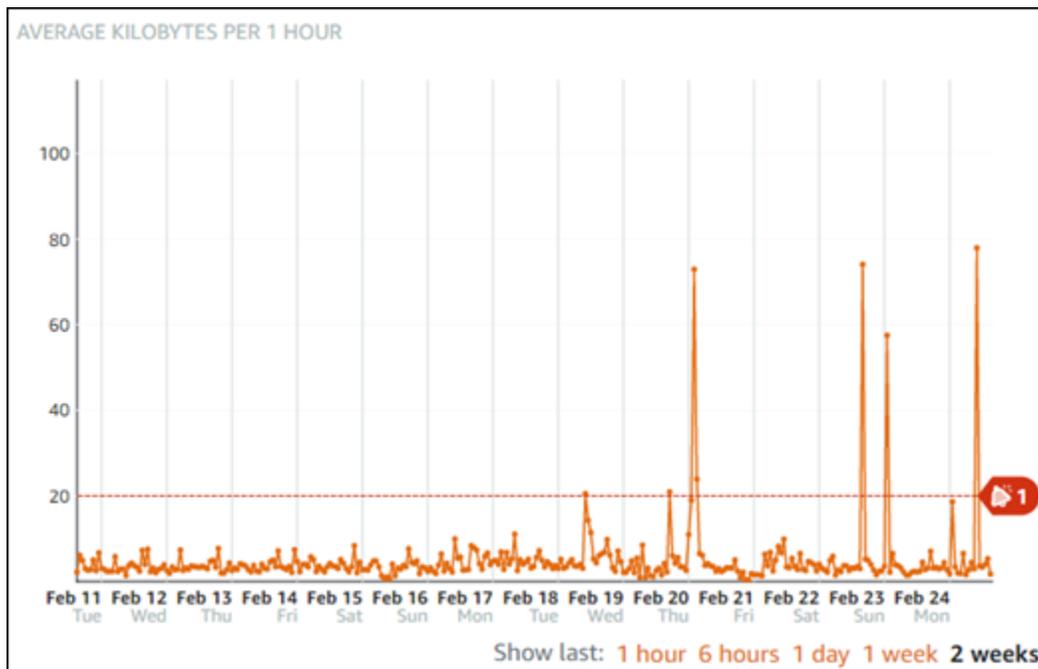
- 您可以為每個指標設定兩個警示。
- 警示的評估間隔為 5 分鐘，而警示的每個資料點都代表為期 5 分鐘的彙總指標資料。
- 如果您將警示設定為透過電子郵件和/或簡訊通知您，則您只能將警示設定為在警示狀態更改為 OK 時通知您。
- 只有將警示設定為透過電子郵件和/或簡訊通知您，才能測試 OK 警示通知。
- 如果您將警示設定為透過電子郵件和/或簡訊通知您，並且如果您為遺失的資料點選擇 Do not evaluate the missing data (不評估遺失資料) 選項，則您只能將警示設定為在警示狀態更改為 INSUFFICIENT\_DATA 時通知您。
- 您只能在警示處於 OK (正常) 狀態時測試通知。

## 預設警示設定

設定指標警示之前，您應該先檢視指標的歷史資料。識別過去兩週期間內的低層級、中層級和高層級。在下列執行個體傳出網路流量 (NetworkOut) 指標圖表範例中，低層級為每小時 0-10 KB、中層級介於每小時 10-20 KB 之間，而高層級介於每小時 20-80 KB 之間。



如果您將警示閾值設定為 greater than or equal to (大於或等於) 低層範圍中的某處 (例如，每小時 5 KB)，則會收到更頻繁且可能不必要的警示通知。如果您將警示閾值設定為 greater than or equal to (大於或等於) 高層範圍中的某處 (例如每小時 20 KB)，則會收到較不頻繁的警示通知，但調查可能更為重要。當您設定警示並加以啟用時，圖表上會出現代表閾值的警示線，如下列範例所示。標示為 1 的警示線代表警示 1 的閾值，標示為 2 的警示線代表警示 2 的閾值。



## 使用 Lightsail 主控台建立負載平衡器指標警示

完成下列步驟，以使用 Lightsail 主控台建立負載平衡器指標警示。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁，選擇 Networking (聯網) 索引標籤。
3. 選擇您要建立指標的負載平衡器名稱。
4. 選擇負載平衡器管理頁面上的 Metrics (指標) 標籤。
5. 在 Metrics Graphs (指標圖表) 標題下的下拉式功能表中，選擇您要建立其警示的指標。如需詳細資訊，請參閱[資源指標](#)。
6. 選擇該頁面 Alarms (警示) 區段中的 Add alarm (新增警示)。
7. 在下拉式功能表中選擇比較運算子值。範例值為大於或等於、大於、小於或小於或等於。
8. 輸入警示的閾值。
9. 輸入要警示的資料點。
10. 選擇評估期間。期間可以 5 分鐘的增量指定 (從 5 分鐘到 24 小時)。
11. 選擇下列其中一種通知方法：
  - 電子郵件 — 當警示狀態變更為 ALARM 時，您會透過電子郵件收到通知。

- 簡訊 — 當警示狀態變更為 ALARM 時，您會透過簡訊收到通知。您可以在其中建立 Lightsail 資源的所有 AWS 區域都不支援 SMS 簡訊，而且 SMS 文字訊息無法傳送到所有國家/地區。如需詳細資訊，請參閱[簡訊支援](#)。

#### Note

如果您選擇透過電子郵件或簡訊收到通知，但尚未在資源的 AWS 區域中設定通知聯絡人，則您需要新增電子郵件地址或行動電話號碼。如需詳細資訊，請參閱[通知](#)。

12. (選擇性) 選擇 Send me a notification when the alarm state change to OK (當警示狀態變更為正常時傳送通知給我)，以便在警示狀態變更為 OK (正常) 時收到通知。只有在您選擇透過電子郵件或簡訊收到通知時，才能使用此選項。
13. (選擇性) 選擇 Advanced settings (進階設定)，然後選擇下列其中一個選項：
  - 選擇警示應如何處理遺失的資料。可用的選項如下：
    - 假設其不在閾值內 (違反閾值) — 遺失資料點會被視為「不良」並違反閾值。
    - 假設其在閾值內 (未違反閾值) — 遺失資料點會被視為「良好」且在閾值內。
    - 使用最後一個良好資料點的值 (忽略並維持目前的警示狀態) – 維持目前的警示狀態。
    - 不要評估 (將遺失的資料視為遺失) — 警示在評估是否要變更狀態時不會考慮遺失的資料點。
  - 選擇 Send a notification if there is insufficient data (如果資料不足則傳送通知)，以在警示狀態變更為 INSUFFICIENT\_DATA 時收到通知。只有在您選擇透過電子郵件或簡訊收到通知時，才能使用此選項。
14. 選擇 Create (建立) 以新增警示。

若要稍後編輯警示，請選擇您要編輯的警示旁邊的省略符號圖示 (:)，然後選擇編輯警示。

## 使用 Lightsail 主控台測試負載平衡器度量警示

請完成下列步驟，以使用 Lightsail 主控台測試警示。您可以測試警示，確認所設定的通知選項是否能運作，例如：確保在觸發警示時收到電子郵件或簡訊。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁，選擇 Networking (聯網) 索引標籤。
3. 選擇您要測試警示的負載平衡器名稱。
4. 選擇負載平衡器管理頁面上的 Metrics (指標) 標籤。

5. 在 Metrics Graphs (指標圖表) 標題下的下拉式功能表中，選擇您要測試其警示的指標。
6. 向下捲動至頁面的警示區段，然後選擇您要測試的警示旁邊的省略符號圖示 (:)
7. 請選擇下列其中一個選項：
  - 測試警示通知 – 選擇此選項可在警示狀態變更為 ALARM 時測試通知。
  - 測試正常通知 – 選擇此選項可在警示狀態變更為 OK 時測試通知。

#### Note

如果無法使用上述任何一個選項，則表示您可能尚未設定警示的通知選項，或警示可能目前處於 ALARM 狀態。如需詳細資訊，請參閱[負載平衡器警示限制](#)。

根據您選擇的測試選項，警示會暫時變更為 ALARM 或 OK 狀態，並根據您為警示設定的通知方法來傳送電子郵件和/或簡訊。只有當您選擇測試通知時，Lightsail 主控台才會顯示 ALARM 通知橫幅。如果您選擇測試 OK 通知，則不會顯示通知橫幅。警示通常會在幾秒鐘後回到其實際狀態。

## 建立負載平衡器警示後的後續步驟

您可以為負載平衡器警示執行一些其他工作：

- 若要停止接收通知，您可以從 Lightsail 移除電子郵件和行動電話。如需詳細資訊，請參閱[刪除通知聯絡人](#)。您也可以停用或刪除警示，以停止接收特定警示的通知。如需詳細資訊，請參閱[刪除或停用指標警示](#)。

## 設定 Lightsail 監控的通知連絡人

您可以設定 Amazon Lightsail，以在其中一個執行個體、資料庫、負載平衡器或內容交付網路 (CDN) 分發的指標超過指定閾值時通知您。通知的形式可以是 Lightsail 主控台中顯示的橫幅、傳送至您指定之地址的電子郵件，或傳送至您指定之行動電話號碼的簡訊。若要透過電子郵件和 SMS 簡訊收到通知，您必須將您的電子郵件地址和行動電話號碼新增為通知聯絡人，並 AWS 區域 在每個您想要監控資源的位置中。如需有關通知的詳細資訊，請參閱[通知](#)。

### Important

簡訊文字訊息功能已暫時停用，目前不支援您可以建立 Lightsail 資源的任何 AWS 區域 功能。如需詳細資訊，請參閱[簡訊支援](#)。

## 內容

- [區域性通知聯絡人限制](#)
- [簡訊支援](#)
- [電子郵件聯絡人驗證](#)
- [使用 Lightsail 主控台新增通知連絡人](#)
- [新增通知聯絡人 AWS CLI](#)
- [新增通知聯絡人之後的後續步驟](#)

## 區域性通知聯絡人限制

您每個地址只能新增一個電子郵件地址和一個行動電話號碼 AWS 區域。如果您在已新增電子郵件地址或行動電話號碼的區域中新增電子郵件地址或行動電話號碼，系統會詢問您是否要以新的通知聯絡人取代現有聯絡人。

如果您在中需要多個電子郵件收件者 AWS 區域，則可以設定轉寄給多個收件者的通訊群組清單，並將通訊群組清單的電子郵件地址新增為通知連絡人。

## 簡訊支援

### Important

簡訊文字訊息功能已暫時停用，目前不支援您可以建立 Lightsail 資源的任何 AWS 區域 功能。或者，您可以設定電子郵件訊息，或依賴 Lightsail 主控台中顯示的通知橫幅。在我們停用此功能之前，已針對設定 SMS 文字簡訊的客戶發佈以下 SMS 文字簡訊支援資訊。

您可以建立 Lightsail 資源的所有 AWS 區域項目並不支援簡訊文字訊息。此外，簡訊無法傳送至世界上某些國家和區域。對於不支援 SMS 訊息的項目，您只能設定電子郵件通知連絡 AWS 區域人。

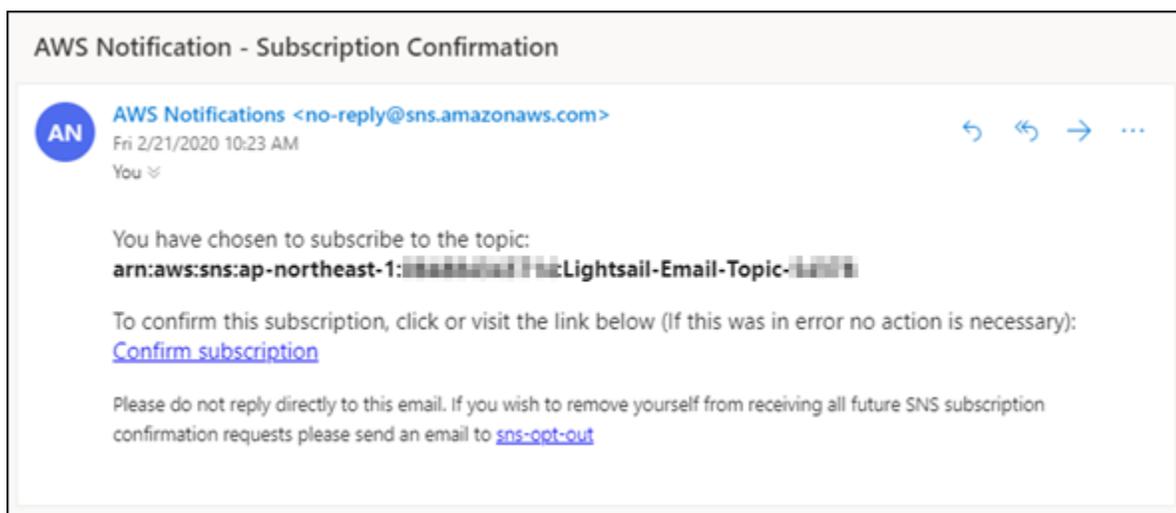
短信在以下幾 AWS 區域個支持。以下是 Amazon 簡單通知服務 (Amazon SNS) 支援 SMS 文字簡訊的區域，Lightsail 會使用此服務傳送通知給您：

- 美國東部 (維吉尼亞北部) (us-east-1)
- 美國西部 (奧勒岡) (us-west-2)
- 亞太區域 (新加坡) (ap-southeast-1)
- 亞太區域 (雪梨) (ap-southeast-2)
- 亞太區域 (東京) (ap-northeast-1)
- 歐洲 (愛爾蘭) (eu-west-1)

如需可傳送 SMS 文字訊息的全球國家和地區清單，以及支援 SMS 文字簡訊的最新 AWS 區域資訊，請參閱 Amazon SNS 開發人員指南中的[支援區域和國家/地區](#)。

## 電子郵件聯絡人驗證

當您在 Lightsail 中將電子郵件地址新增為通知聯絡人時，系統會向該地址傳送驗證要求。驗證要求電子郵件包含一個連結，收件者必須按一下該連結，以確認他們想要接收 Lightsail 通知。在通過驗證之後，通知才會傳送至電子郵件地址。驗證來自 AWS 通知 <no-reply@sns.amazonaws.com>，其主旨為 AWS 通知 - 訂閱確認。簡訊不需要驗證。



如果驗證請求不在收件匣資料夾中，請檢查信箱的垃圾郵件資料夾。如果驗證要求遺失或遭到刪除，請在 Lightsail 主控台和「帳戶」頁面中顯示的通知橫幅中選擇「重新傳送驗證」。

**example@example.com is waiting for verification.**

Notifications will not be sent to example@example.com about resources in the Seoul (ap-northeast-2) Region until the email address is verified

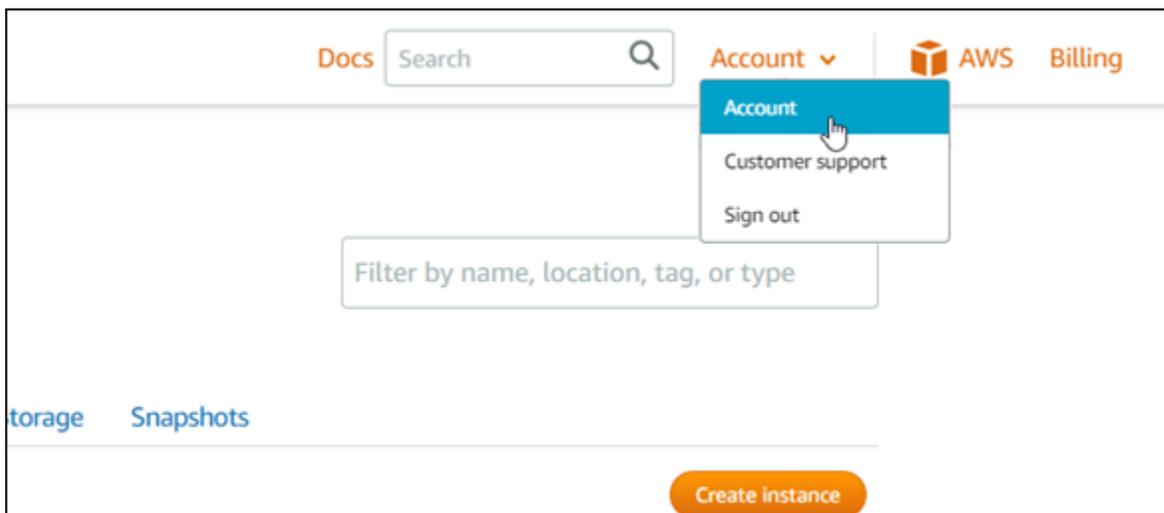
[Learn more about this notification.](#)

[Resend verification](#)

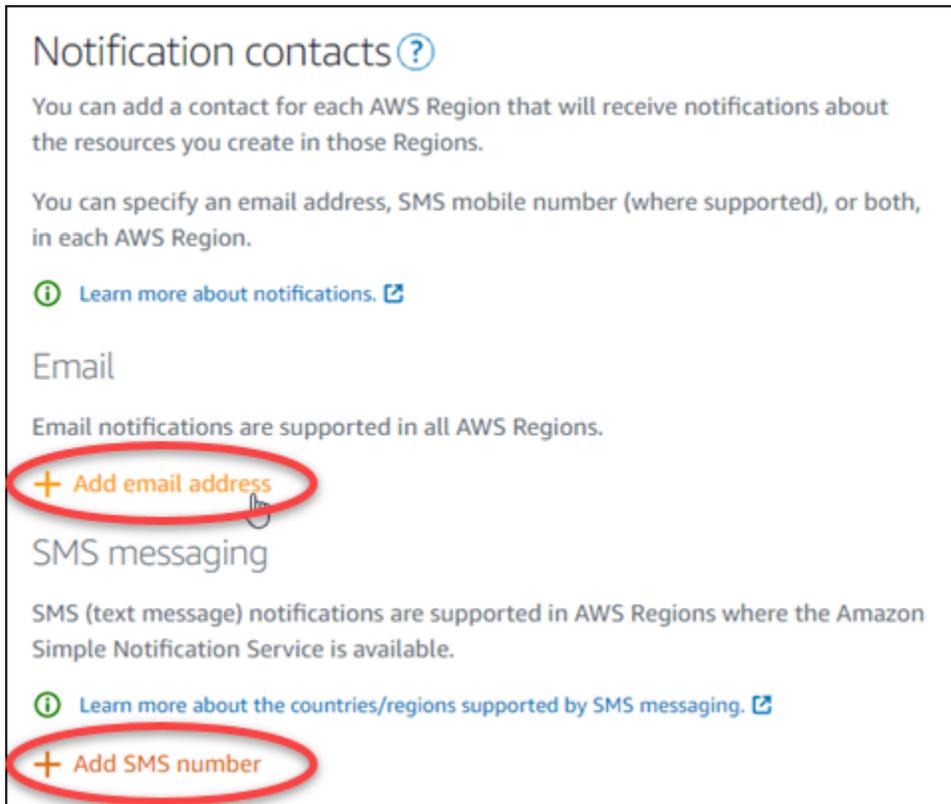
## 使用 Lightsail 主控台新增通知連絡人

若要使用 Lightsail 主控台新增通知連絡人，請完成下列步驟。

1. 登入主 [Lightsail](#) 台。
2. 在 Lightsail 首頁上，請在頂部導覽選單中選擇 Account (帳戶)。
3. 在下拉式功能表中選擇 Account (帳戶)。



4. 請在 Profile & contacts (設定檔與聯絡人) 索引標籤的 Notification contacts (通知聯絡人) 區段中，選擇 Add email address (新增電子郵件地址) 或 Add SMS number (新增簡訊電話號碼)。



## Notification contacts [?](#)

You can add a contact for each AWS Region that will receive notifications about the resources you create in those Regions.

You can specify an email address, SMS mobile number (where supported), or both, in each AWS Region.

[Learn more about notifications.](#)

### Email

Email notifications are supported in all AWS Regions.

[+ Add email address](#)

### SMS messaging

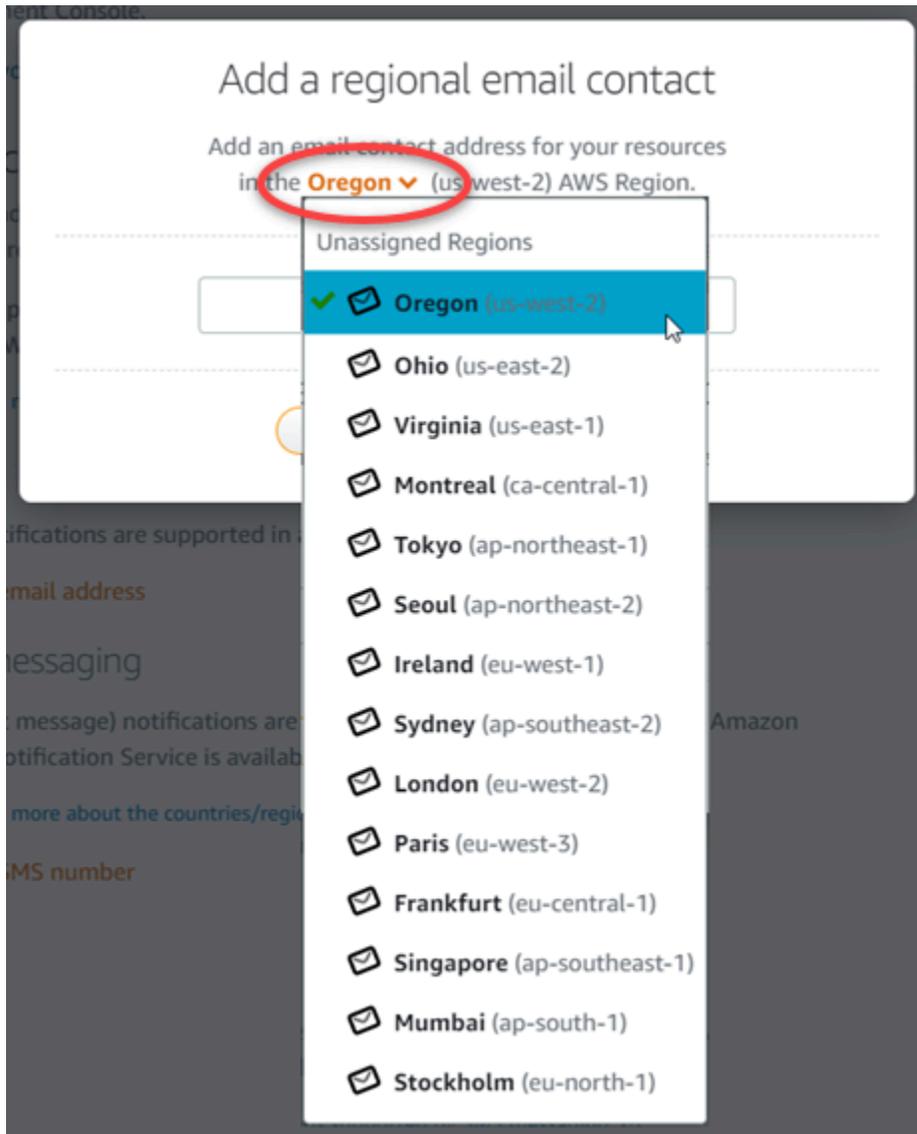
SMS (text message) notifications are supported in AWS Regions where the Amazon Simple Notification Service is available.

[Learn more about the countries/regions supported by SMS messaging.](#)

[+ Add SMS number](#)

5. 完成下列其中一個步驟：

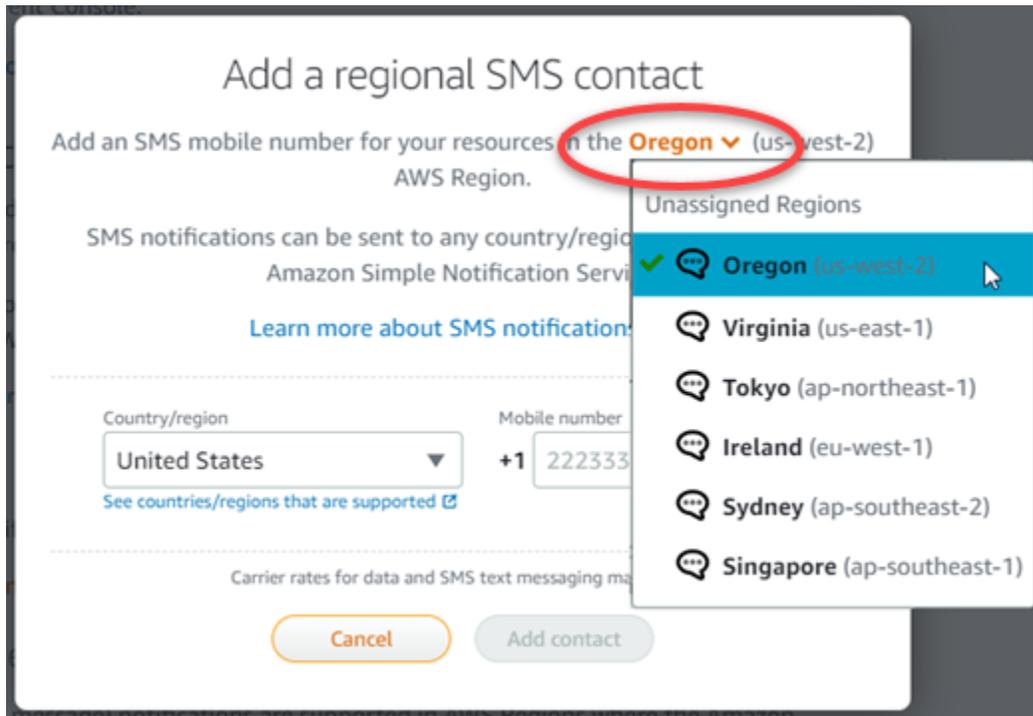
- 如果您要新增電子郵件地址，請選擇 AWS 區域 要新增通知連絡人的位置。在文字方塊中輸入您的電子郵件地址。



- 如果您要新增 SMS 號碼，請選擇 AWS 區域 要新增通知連絡人的位置。選擇您的行動電話號碼所屬的國家，然後輸入在文字方塊中。系統已為您輸入國碼。

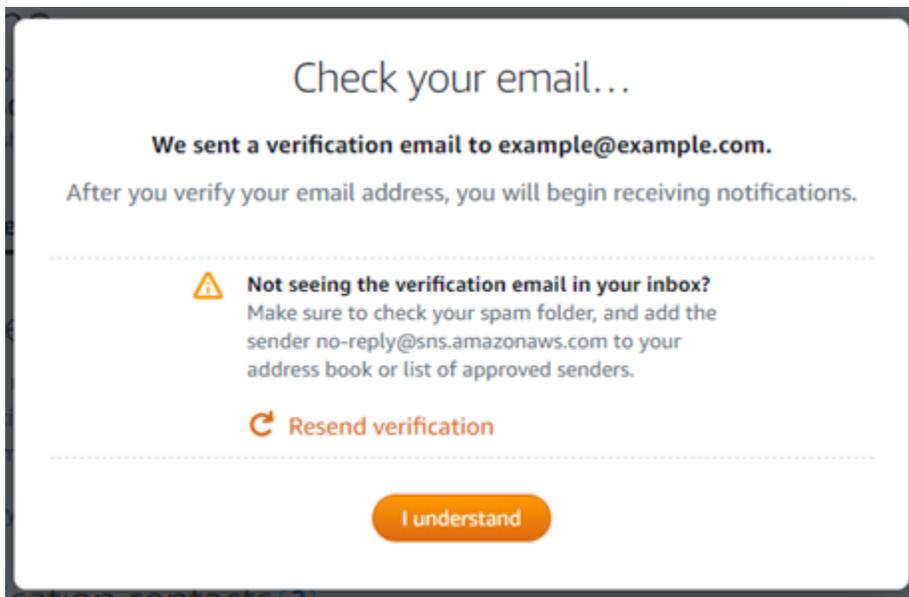
**⚠ Important**

簡訊文字訊息功能已暫時停用，目前不支援您可以建立 Lightsail 資源的任何 AWS 區域功能。如需詳細資訊，請參閱[簡訊支援](#)。



6. 選擇 Add Contact (新增聯絡人)。

將電子郵件地址新增為通知聯絡人時，驗證請求即會傳送至該地址。驗證要求電子郵件包含一個連結，收件者必須按一下該連結，以確認他們想要接收 Lightsail 通知。簡訊不需要驗證。



7. 選擇 I understand (我了解)。

您的電子郵件地址或行動電話號碼會新增至 Notification contacts (通知聯絡人) 區段。在完成下列步驟中的驗證程序之後，才會驗證電子郵件地址。在驗證過通知之後，通知才會傳送至電子郵件地址。如果驗證請求遺失或遭到刪除，請選擇其中一個區域性電子郵件地址旁邊的 Resent (重新傳送)，以傳送另一個驗證請求。

#### Note

簡訊不需要驗證。因此，在您新增簡訊通知聯絡人後，不需要完成此程序的步驟 8 到 10。

### Email

Email notifications are supported in all AWS Regions.

[+ Add email address](#)

Email	Region	Verified	
example@example.com	 Oregon (us-west-2)	No <a href="#">Resend</a>	

### SMS messaging

SMS (text message) notifications are supported in AWS Regions where the Amazon Simple Notification Service is available.

[Learn more about the countries/regions supported by SMS messaging.](#)

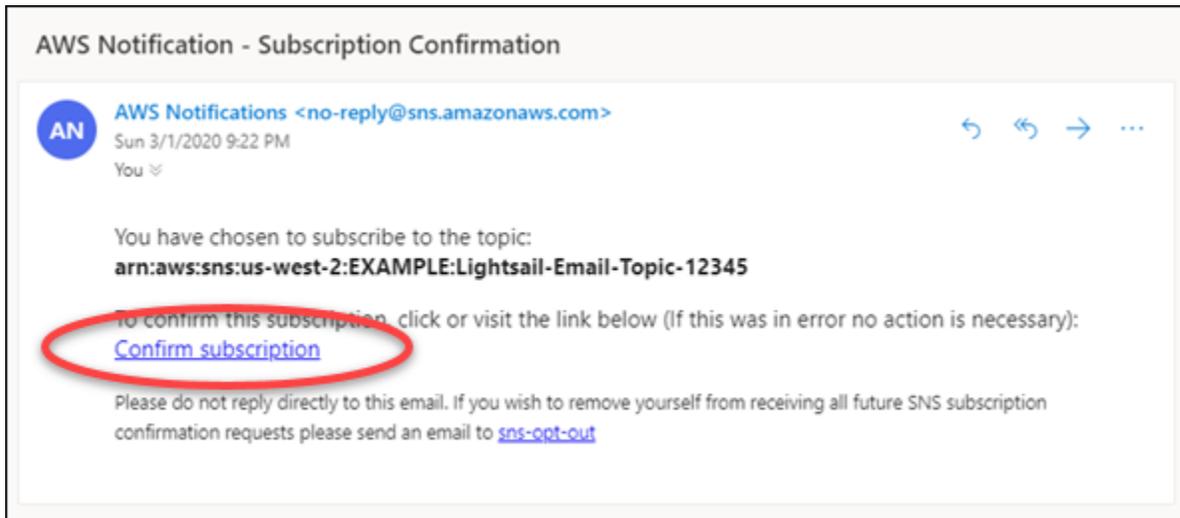
[+ Add SMS number](#)

Number	Region	
+1 222 333 4444	 Oregon (us-west-2)	

- 開啟您在 Lightsail 中新增為通知連絡人的電子郵件地址的收件匣。
- 開啟 no-reply@sns.amazonaws.com 寄來的 AWS 通知 - 訂閱確認電子郵件。

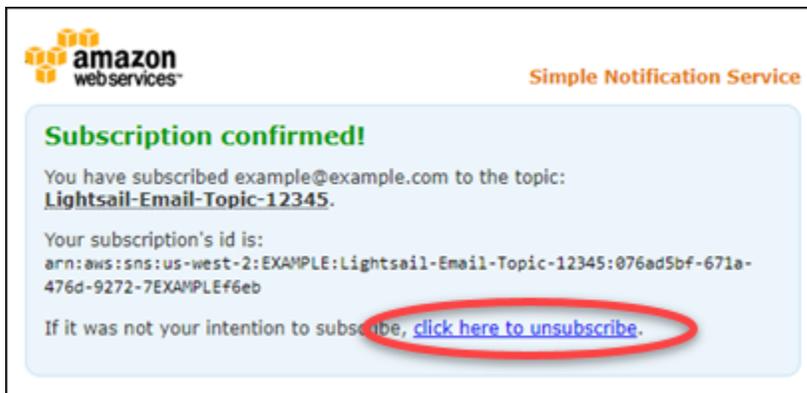
#### Note

如果驗證請求不在收件匣資料夾中，請檢查信箱的垃圾郵件資料夾。



10. 在電子郵件中選擇「確認訂閱」，以確認您要接收 Lightsail 通知。

瀏覽器視窗會開啟至下列頁面，確認您的訂閱。若要取消訂閱，請選擇頁面上的 [click here to unsubscribe](#) (按一下這裡以取消訂閱)。或者，如果您已關閉頁面，請完成 [刪除通知聯絡人](#) 的步驟。



## 使用 AWS CLI 新增通知聯絡人

若要使用 AWS Command Line Interface (AWS CLI) 新增 Lightsail 的通知聯絡人，請完成下列步驟。

1. 開啟終端機或命令提示視窗。

如果您尚未安裝，請安裝 [AWS CLI](#) 並將其設定為與 Lightsail 搭配使用。

2. 輸入下列命令以新增通知聯絡人：

```
aws lightsail create-contact-method --region Region --notificationProtocol Protocol
--contact-endpoint Destination
```

在命令中：

- 應 AWS 區域 在其中新增通知連絡人的##。
- 使用聯絡人的通知通訊協定 (應該是電子郵件或簡訊) 取代 *Protocol*。
- 使用您的電子郵件地址或行動電話號碼取代 *Destination*。

#### Note

指定行動電話號碼時，請使用 E. 164 格式。E. 164 是電話號碼結構的標準，用於國際電信通訊。遵循此格式的電話號碼最多可以有 15 位數，前面加上加號 (+) 字元和國碼。例如，[E. 164](#) 格式的美國電話號碼會指定為 +1XXX5550100。如需詳細資訊，請參閱 Wikipedia 中的 E. 164。

範例：

```
aws lightsail create-contact-method --region us-west-2 --notificationProtocol Email
--contact-endpoint example@example.com
```

```
aws lightsail create-contact-method --region us-east-1 --notificationProtocol SMS
--contact-endpoint +14445556666
```

當您按下 Enter 鍵時，您會看到一個操作回應，內含您的請求詳細資訊。

驗證請求會傳送至您指定為通知聯絡人的電子郵件地址。這會確認收件者想要訂閱 Lightsail 通知。在完成下列步驟中的驗證程序之後，才會驗證電子郵件地址。在電子郵件地址經過驗證之後，通知才會傳送至該電子郵件地址。如果原始通知錯置，請選擇其中一個區域性電子郵件地址旁邊的 Resent (重新傳送)，以傳送另一個驗證請求。

#### Note

簡訊不需要驗證。因此，當您新增簡訊通知聯絡人時，不需要完成此程序的步驟 8 到 10。

### 3. 開啟您新增為通知聯絡人之電子郵件地址的收件匣。

4. 開啟 [no-reply@sns.amazonaws.com](mailto:no-reply@sns.amazonaws.com) 寄來的 AWS 通知 - 訂閱確認電子郵件。
5. 在電子郵件中選擇「確認訂閱」，以確認您要接收來自 Lightsail 的電子郵件通知。

瀏覽器視窗會開啟至下列頁面，確認您的訂閱。若要取消訂閱，請選擇頁面上的 [click here to unsubscribe](#) (按一下這裡以取消訂閱)。或者，如果您已關閉頁面，請完成 [刪除通知聯絡人](#) 的步驟。

## 新增通知聯絡人之後的後續步驟

您可以為通知聯絡人執行一些其他工作：

- 在您新增通知聯絡人的 AWS 區域 位置新增鬧鐘。您可以選擇在警示啟動時透過電子郵件和簡訊收到通知。如需詳細資訊，請參閱 [警示](#)。
- 如果在您預期收到通知時沒有收到通知，您應該檢查一些事項，確認您的通知聯絡人設定正確。若要進一步了解，請參閱[針對通知進行故障診斷](#)。
- 若要停止接收通知，您可以從 Lightsail 移除電子郵件和行動電話。如需詳細資訊，請參閱[刪除或停用指標警示](#)。您也可以停用或刪除警示，以停止接收特定警示的通知。如需詳細資訊，請參閱[刪除或停用指標警示](#)。

## 刪除通知聯絡人

從 Amazon Lightsail 刪除您的電子郵件和行動電話號碼通知聯絡人，以停止接收 Lightsail 資源的電子郵件和簡訊文字訊息通知。如需有關通知的詳細資訊，請參閱[通知](#)。

您也可以停用或刪除警示，以停止接收特定警示的通知。如需詳細資訊，請參閱[刪除或停用指標警示](#)。

內容

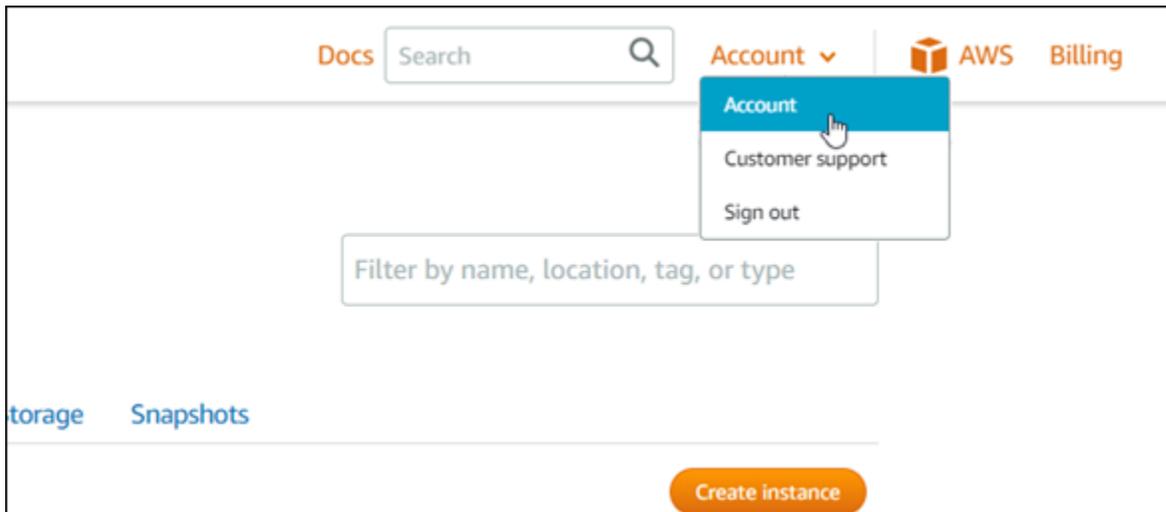
- [使用 Lightsail 主控台刪除通知聯絡人](#)
- [使用刪除通知聯絡人 AWS CLI](#)
- [刪除通知聯絡人後的後續步驟](#)

## 使用 Lightsail 主控台刪除通知聯絡人

若要使用 Lightsail 主控台刪除通知聯絡人，請完成下列步驟。

1. 登入主 [Lightsail 台](#)。

2. 在 Lightsail 首頁上，請在頂部導覽選單中選擇 Account (帳戶)。
3. 在下拉式功能表中選擇 Account (帳戶)。



4. 在 Profile & contacts (個人檔案與聯絡人) 索引標籤上的 Notification contacts (通知聯絡人) 區段中，選擇您要刪除的電子郵件地址或行動電話號碼旁的刪除圖示。
5. 選擇 Yes (是)，確認您要刪除通知聯絡人。

## 使用 AWS CLI 刪除通知聯絡人

若要使用 AWS Command Line Interface (AWS CLI) 刪除 Lightsail 的通知聯絡人，請完成下列步驟。

1. 開啟終端機或命令提示視窗。

如果您尚未[安裝](#)，請[安裝 AWS CLI](#)並將其設定為與 Lightsail 搭配使用。

2. 輸入下列命令以刪除通知聯絡人：

```
aws lightsail delete-contact-method --region Region --notificationProtocol Protocol
```

在命令中：

- 應刪除通知聯絡人的 **##**。AWS 區域
- 使用您要刪除之聯絡人的通知通訊協定 (例如電子郵件或簡訊) 取代 *Protocol*。

範例：

```
aws lightsail delete-contact-method --region us-west-2 --notificationProtocol SMS
```

當您按下 Enter 鍵時，您會看到一個操作回應，內含您的請求詳細資訊。

## 刪除通知聯絡人後的後續步驟

刪除通知聯絡人之後，您可以執行幾項其他工作：

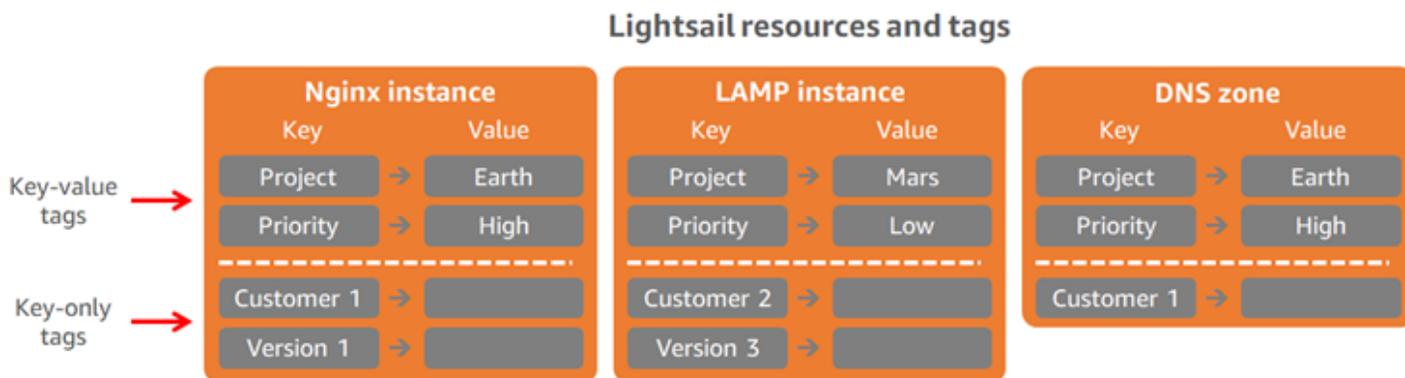
- 刪除通知聯絡人會停止電子郵件和 SMS 文字訊息通知，但不會停止在 Lightsail 主控台中顯示通知橫幅。若要停止通知橫幅，以及停止電子郵件和簡訊通知，請停用或刪除造成這些通知的警示。如需詳細資訊，請參閱[刪除或停用指標警示](#)。
- 在 Lightsail 中新增您的電子郵件地址和手機號碼作為通知聯絡人，以便重新開始接收電子郵件和 SMS 簡訊通知。如需詳細資訊，請參閱[新增通知聯絡人](#)。

## 使用標籤組織和篩選 Lightsail 資源

使用 Amazon Lightsail，您可以將標籤作為標籤指派給資源。每個標記都是由索引鍵和選用值組成的標籤，可讓管理、搜尋和篩選資源更有效率。

使用 Amazon Lightsail，您可以將標籤作為標籤指派給資源。每個標記都是由索引鍵和選用值組成的標籤，能夠有效率管理、搜尋和篩選資源。雖然沒有固有類型的標籤，但它們可讓您依據用途、擁有者、環境或其他條件來分類 Lightsail 資源。這在您擁有許多相同類型的資源時很有用。您可以根據您指派給資源的標籤快速識別特定資源。例如，針對資源定義一組能夠協助您追蹤每個資源之專案或優先順序的標籤。

沒有值的金鑰在 Lightsail 中稱為僅限金鑰的標籤。具有值的索引鍵稱為索引鍵值標籤。下圖說明標籤建立的運作方式。在此範例中，每個資源都有一組索引鍵值標籤和僅索引鍵標籤。索引鍵值標籤可識別專案和優先順序，而僅索引鍵標籤可識別客戶和應用程式版本。



## 使用標籤來整理帳單和控制存取

您也可以使用標籤來整理帳單、控制 Lightsail 中資源和請求的存取權，以及控制對標籤金鑰的存取。如需詳細資訊，請參閱以下其中一項指南：

- [使用標籤來整理資源成本](#)
- [使用標籤來控制資源存取](#)

## 支援標記的 Lightsail 資源

您可以在建立大多數 Lightsail 資源時或建立資源之後標記這些資源。如果在資源建立期間無法套用標籤，Lightsail 會回復資源建立程序。這可協助確保資源建立時具有標籤，否則資源就不會建立，而且無論何時都不會有應標記的資源未標記。

您可以在 Lightsail 主控台中標記下列 Lightsail 資源：

- 執行個體
- 容器服務
- 內容交付網路 (CDN) 分發
- 儲存貯體
- 資料庫
- 磁碟
- DNS 區域
- 負載平衡器

 Important

使用 Lightsail 主控台建立的快照會自動從來源資源繼承標籤。從該快照建立的 Lightsail 資源將具有與建立快照集時存在於來源資源上的相同標籤。

您可以使用 [Lightsail API](#)、[AWS Command Line Interface \(AWS CLI\)](#) 或開發套件來標記下列資源：

- 資料庫快照
- 資料庫
- 磁碟快照
- 磁碟
- 網域 (DNS 區域)
- 執行個體快照
- 執行個體
- 金鑰對
- 負載平衡器 TLS 憑證 (使用 Lightsail 建立的 TLS 憑證)
- 負載平衡器

### ⚠ Important

使用 Lightsail API 或 SDK 建立的快照不會自動從來源資源繼承標籤。AWS CLI 反之，您必須使用 `tags` 參數手動指定來源資源的標籤。

## 標籤限制

以下基本限制適用於標籤：

- 每個資源的標籤數上限 – 50。
- 每個資源的每個標籤索引鍵都必須是唯一的。每個標籤索引鍵只能有一個值。
- 索引鍵長度上限 - 128 個 UTF-8 Unicode 字元。
- 值長度上限 - 256 個 UTF-8 Unicode 字元。
- 如果您的標記結構描述是跨多項服務和資源使用，請記得其他服務可能會有字元使用限制。通常允許的字元為：字母、數字和空格，以及下列字元：+ - = 。 \_ : / @
- 標籤金鑰與值皆區分大小寫。
- 金鑰或值請勿使用 `aws:` 字首。該字首已保留供 AWS 使用。

## 使用標籤對 Lightsail 資源進行分類

在 Amazon Lightsail 中使用標籤，依目的、擁有者、環境或其他條件對資源進行分類。您可以在資源建立時或建立後將標籤新增至其中。依照以下步驟在資源建立後將標籤新增到其中。

### 📘 Note

如需有關標籤、可為哪些資源加上標籤以及限制的詳細資訊，請參閱[標籤](#)。

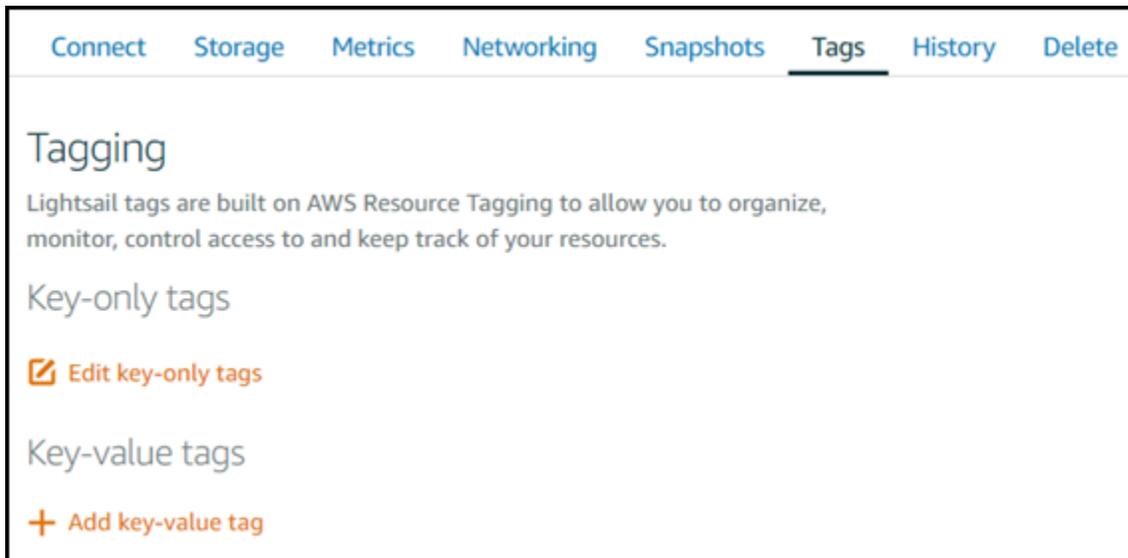
將標籤新增至資源

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁上，選擇您要標記之資源類型的索引標籤。例如，若要將標籤新增到 DNS 區域，請選擇 `Networking tab` (聯網索引標籤)。或者，選擇 `Instances` (執行個體) 索引標籤以將標籤新增到執行個體。

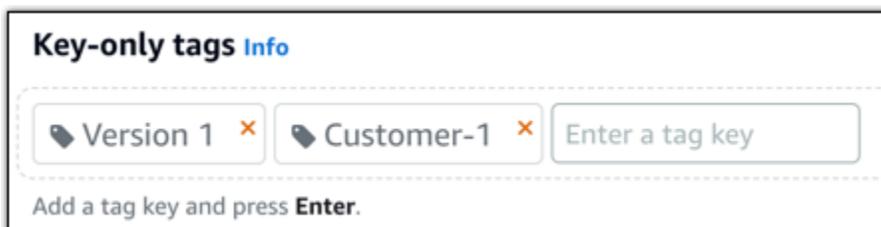
**Note**

您可以使用 Lightsail 主控台來標記執行個體、容器服務、CDN 散發、儲存貯體、資料庫、磁碟、DNS 區域和負載平衡器。不過，您可以使用 [Lightsail API 作業](#) 或 [AWS Command Line Interface \(AWS CLI\)](#) 或開發套件來標記更多 Lightsail 資源。如需支援標記的 Lightsail 資源完整清單，請參閱 [標記](#)。

3. 選擇您要加上標籤的資源。
4. 在您所選的資源管理頁面中，選擇 Tags (標籤) 索引標籤。

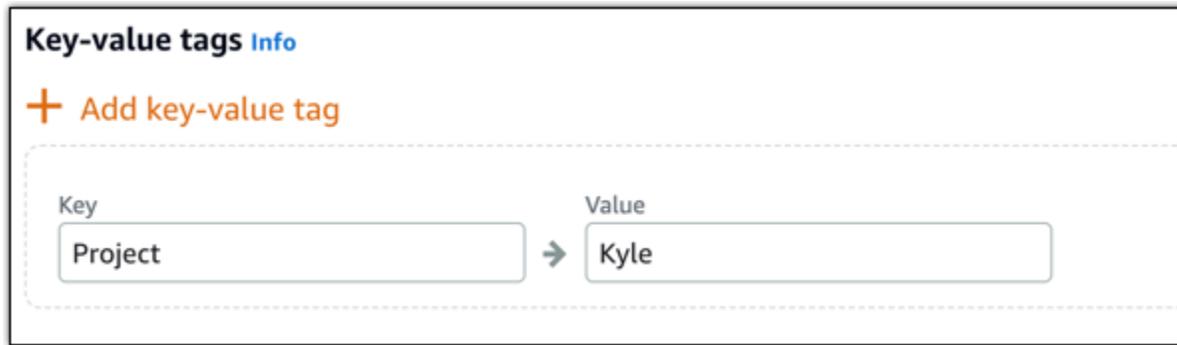


5. 根據您希望新增標籤的類型，選擇以下其中一個選項：
  - Add key-only tags (新增僅索引鍵標籤) 或 Edit key-only tags (編輯僅索引鍵標籤) (若標籤已新增)。在標籤索引鍵文字方塊中輸入新的標籤，接著按 Enter (輸入)。輸入標籤以新增之後，請選擇 Save (儲存)，如果不要新增則選擇 Cancel (取消)。



- Create a key-value tag (建立索引鍵值標籤)，接著將索引鍵輸入 Key (索引鍵) 文字方塊，將值輸入 Value (值) 文字方塊。完成輸入標籤後，請選擇 Save (儲存)，如果不要新增則選擇 Cancel (取消)。

鍵值標籤在儲存前一次只能新增一個。若要新增超過一個索引鍵值標籤，請重複之前的步驟。



## 後續步驟

如需您在將標籤新增到資源後可以執行之任務的詳細資訊，請參閱以下指南：

- [使用標籤來整理資源](#)
- [使用標籤來整理資源的成本](#)
- [使用標籤來控制對資源的存取](#)
- [刪除標籤](#)

## 從 Lightsail 資源移除標籤

您可以從 Amazon Lightsail 資源中刪除標籤。刪除一個資源的標籤不會刪除所有其他資源的相同標籤。若要完全刪除所有資源中的某個標籤，您必須從每個資源移除該標籤。本指南提供從資源刪除標籤的步驟。

### Note

如需有關標籤、可為哪些資源加上標籤以及標籤限制的詳細資訊，請參閱[標籤](#)。

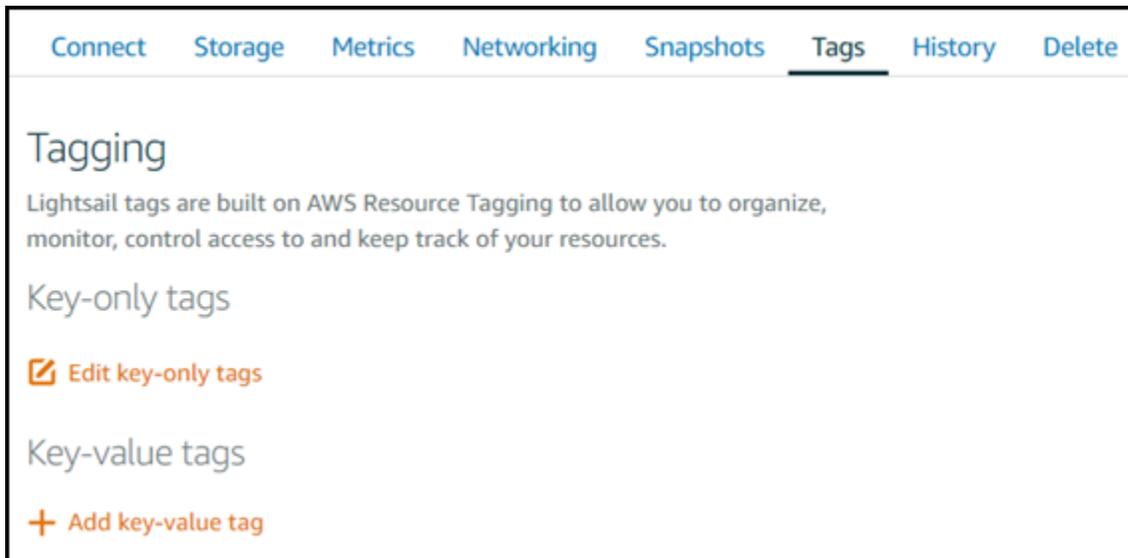
### 從資源刪除標籤

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁上，選擇您要從中刪除標籤之資源類型的索引標籤。例如，若要從 DNS 區域刪除標籤，請選擇 Networking (聯網) 索引標籤。或者選擇 Instances (執行個體) 索引標籤，以從執行個體刪除標籤。

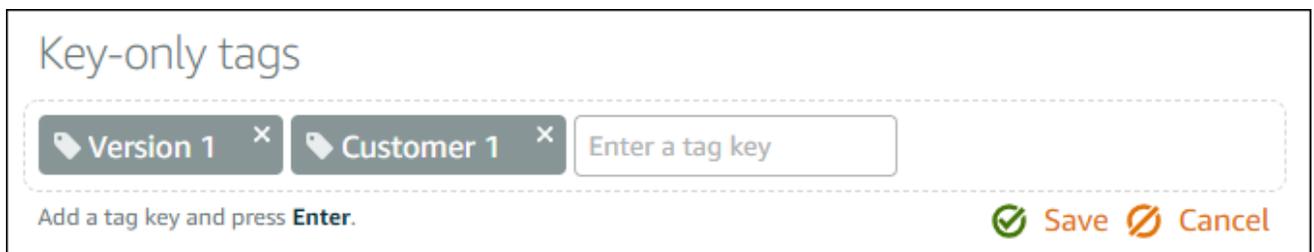
**Note**

您可以使用 Lightsail 主控台來標記執行個體、容器服務、CDN 散發、儲存貯體、資料庫、磁碟、DNS 區域和負載平衡器。不過，您可以使用 [Lightsail API 作業](#) 或 [AWS 命令列介面](#) (AWS CLI) 或開發套件來標記更多 Lightsail 資源。如需支援標記的 Lightsail 資源完整清單，請參閱 [標記](#)。

3. 選擇您想要刪除標籤的資源。
4. 在您所選的資源管理頁面，選擇 Tags (標籤) 索引標籤。



5. 根據您想要從資源刪除的標籤類型，執行以下其中一個項目：
  - a. 選擇 Edit key-only tags (編輯僅索引鍵標籤)，接著針對您想要從資源刪除的標籤選擇刪除圖示 (X)。完成刪除標籤以從資源移除之後，請選擇 Save (儲存)，若不移除則選擇 Cancel (取消)。



- b. 若要移除索引鍵值標籤，請選擇鍵值標籤的刪除圖示 (X)。出現提示時，選擇 Yes, delete (是，刪除) 以移除索引鍵值標籤，若不移除則選擇 No, cancel (否，取消)。



## 透過資源層級權限和以標籤為基礎的授權來控制 Lightsail 資源的存取

Lightsail 支援資源層級權限，並根據其某些動作的標籤進行授權。API 如需詳細資訊，請參閱服務授權參考中[適用於 Amazon Lightsail 的動作、資源和條件金鑰](#)。

### 使用標籤控制 Lightsail 資源存取

您可以在 Amazon Lightsail 中使用標籤來控制資源的存取、控制對請求的存取，以及控制對標籤金鑰的存取。在本指南中，您將學習如何建立 AWS Identity and Access Management (IAM) 政策，以指定建立或刪除 Lightsail 資源所需的索引鍵值標籤，並將該政策附加至需要提出這些要求的使用者或群組。

#### Note

若要深入了解 Lightsail 中的標籤、可以標記哪些資源以及限制，請參閱[標籤](#)。

### 步驟 1：建立 IAM 政策

首先，在 IAM 主控台建立下列 IAM 政策。如需有關建立 IAM 政策的詳細資訊，請參閱 IAM 文件中的[建立 IAM 政策](#)。

下列原則會限制使用者建立新的 Lightsail 資源，除非使用建立要求定義的 true 索引鍵標記 allow 和值。此政策也會限制使用者刪除資源，除非他們具有 allow/true 索引鍵值標籤。

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

```

"Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "lightsail:Create*",
      "lightsail:TagResource",
      "lightsail:UntagResource"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:RequestTag/allow": "true"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "lightsail>Delete*",
      "lightsail:TagResource",
      "lightsail:UntagResource"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:ResourceTag/allow": "true"
      }
    }
  }
]
}

```

下列政策會限制使用者變更索引鍵值標籤並非 allow/false 之資源的標籤。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "lightsail:TagResource"
      ]
    }
  ]
}

```

```
    ],
    "Resource": "*",
    "Condition": {
      "StringNotEquals": {
        "aws:ResourceTag/allow": "false"
      }
    }
  }
]
```

## 步驟 2：將政策連接至使用者或群組

建立 IAM 政策後，請將其連接至需要使用索引鍵/值組來建立 Lightsail 資源的使用者或群組。如需有關將 IAM 政策連接至使用者或群組的詳細資訊，請參閱 IAM 文件中的[新增和移除 IAM 政策](#)。

## 使用標籤整理 Lightsail 資源成本

您可以在 Amazon Lightsail 中使用標籤來整理 AWS 帳單，以反映您自己的成本結構。若要這麼做，請將索引鍵值標籤新增至您的 Lightsail 資源。然後在 AWS Billing and Cost Management 控制台中激活這些標籤。最後，註冊以使用成本分配報告中包含的標籤鍵值來取得 AWS 帳戶帳單。本指南提供了此設定的步驟。

### Note

如需 Lightsail 中的標籤、可標記哪些資源以及標記限制的詳細資訊，請參閱[標籤](#)。

### Important

目前無法在成本分配報表中追蹤 Lightsail 資料庫快照集，即使在成本配置標記新增至快照集之後也是如此。

## 步驟 1：新增索引鍵值標籤至資源

將索引鍵值標籤新增至您要在計費主控台中整理的 Lightsail 資源。如需索引鍵值標籤的詳細資訊，請參閱[新增標籤至資源](#)。

建議您設計一組標籤索引鍵以代表您整理成本的方式。成本分配報告會將標籤索引鍵顯示為額外欄，其中列出每一行的適用值。因此，如果您使用一組一致的標籤索引鍵，追蹤成本就會更有效率。例如，您可以使用特定的成本中心標記數個 Lightsail 資源。您可以使用「Cost center」(成本中心) 索引鍵和數值配對執行此項作業。接著整理帳單資訊，以檢視該成本中心跨數個資源的帳單。以下範例為可用於整理成本分配的索引鍵值標籤：

Key-value tags for cost centers		Key-value tags for projects		Key-value tags for country	
Key	Value	Key	Value	Key	Value
Cost center	→ 5465	Project	→ Earth	Country	→ United States
Cost center	→ 5472	Project	→ Mars	Country	→ England
Cost center	→ 5481	Project	→ Jupiter	Country	→ Paris
Cost center	→ 5486	Project	→ Saturn	Country	→ Japan

## 步驟 2：啟用使用者定義的成本分配標籤

將必要的標籤新增至 Lightsail 資源後，請在 [Billing and Cost Management] 主控台中啟用這些標籤以進行成本分配。例如，如果您建立了「Cost center」(成本中心) 索引鍵標籤，則在「帳單和成本管理」主控台啟用該索引鍵標籤以產生該標籤的成本分配報告。如需詳細資訊，請參閱 AWS Billing and Cost Management 文件中的[啟動使用者定義的成本配置標籤](#)。

## 步驟 3：設定成本分配報告並檢視

每月費用分配報告會依產品類別和連結帳戶 AWS 使用者，列出您帳戶的使用情況。報告包含與詳細帳單報告相同的明細項目和標籤索引鍵的額外欄。若要設定每月成本分配報告，請參閱 AWS Billing and Cost Management 文件中的[設定每月成本分配報告](#)。

設定成本分配報告時，會定義儲存報告的 Amazon Simple Storage Service (Amazon S3) 儲存貯體。開啟您定義的 Amazon S3 儲存貯體並在其可用後開啟成本分配報告。有關成本分配報告內容的詳細資訊，請參閱 AWS Billing and Cost Management 文件中[的檢視成本分配報告](#)。

## 標記 Lightsail 資源以進行組織和篩選

在您標記 Amazon Lightsail 資源之後，您可以依新增的標籤篩選資源。您可以在 Lightsail 主控台中選擇或搜尋標籤來執行此操作。本指南說明如何依標籤檢視和篩選 Lightsail 資源。

### Note

如需標籤、可為哪些資源加上標籤，以及標籤限制的詳細資訊，請參閱[標籤](#)。

## 檢視資源的標籤

執行個體、容器服務、CDN 分發、儲存貯體、資料庫、磁碟、DNS 區域和負載平衡器可以使用 Lightsail 主控台加上標籤，因此包含「標籤」索引標籤。該索引標籤可透過資源的管理頁面存取，如下執行個體資源範例所示。在 Tags (標籤) 索引標籤上，您可以新增、編輯或刪除標籤。如需詳細資訊，請參閱[為資源加上標籤](#)以及[刪除標籤](#)。

Connect Storage Metrics Networking Snapshots **Tags** History Delete

### Tagging

Lightsail tags are built on AWS Resource Tagging to allow you to organize, monitor, control access to and keep track of your resources.

#### Key-only tags

Version 1 Customer 1

Edit key-only tags

#### Key-value tags

Add key-value tag

Project → Earth

Priority → High

### Note

您可以使用 Lightsail 主控台來標記執行個體、容器服務、CDN 散發、儲存貯體、資料庫、磁碟、DNS 區域和負載平衡器。不過，您可以使用 [Lightsail API 作業](#) 或 [AWS Command Line Interface \(AWS CLI\)](#) 或開發套件來標記更多 Lightsail 資源。如需支援標記的 Lightsail 資源完整清單，請參閱[標記](#)。

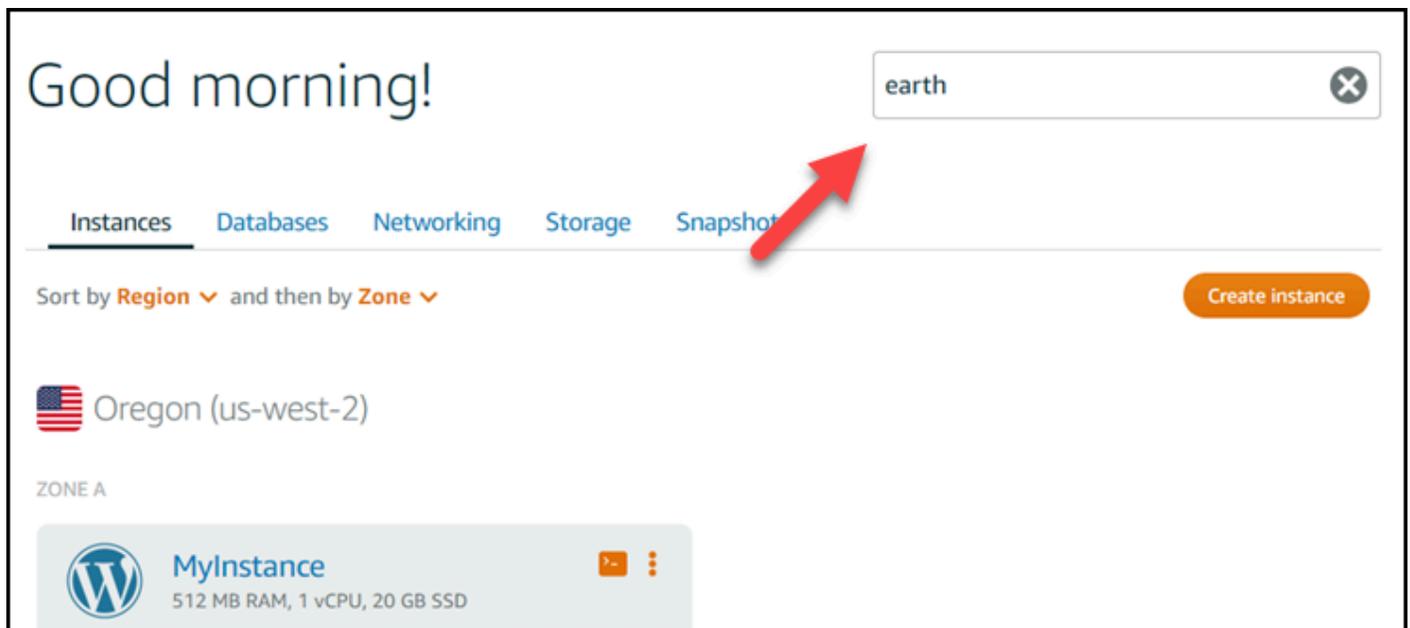
## 使用標籤篩選資源

Lightsail 主控台提供下列選項，可使用標籤篩選資源。所有這些選項都會重新整理 Lightsail 首頁，以僅顯示您搜尋或選取的標籤。

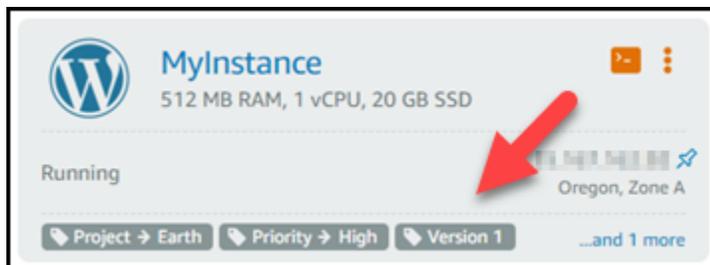
### Note

這些篩選選項具持久性。如果您依標記篩選，然後在 Lightsail 首頁的各個區段之間導覽，則仍會套用該篩選器。

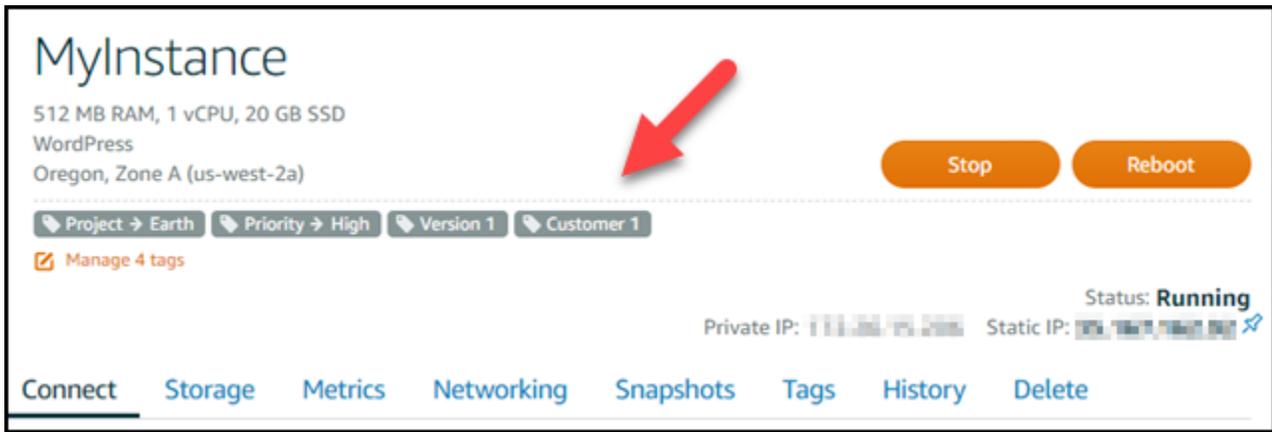
- 在 Lightsail 首頁上，在「搜尋」文字方塊中輸入僅限金鑰標籤或您要篩選依據的值，然後按 Enter。



- 選擇 Lightsail 首頁上顯示在資源下方的標籤。



- 選擇顯示於資源標頭的標籤。



The screenshot displays the Amazon Lightsail console for an instance named "MyInstance". The instance details include 512 MB RAM, 1 vCPU, and 20 GB SSD, running WordPress in the Oregon, Zone A (us-west-2a) region. A red arrow points to the "Project" tag in the list of tags. The instance status is "Running", and it has a private IP and a static IP. A navigation menu at the bottom includes options for Connect, Storage, Metrics, Networking, Snapshots, Tags, History, and Delete.

MyInstance

512 MB RAM, 1 vCPU, 20 GB SSD  
WordPress  
Oregon, Zone A (us-west-2a)

Project → Earth Priority → High Version 1 Customer 1

Manage 4 tags

Status: **Running**

Private IP: [REDACTED] Static IP: [REDACTED]

Connect Storage Metrics Networking Snapshots Tags History Delete

## 疑難排解常 Lightsail 資源問題

本節涵蓋下列 Amazon Lightsail 資源的疑難排解主題。遵循指 step-by-step 示和指導，診斷並解決您在使用 Lightsail 執行個體、資料庫、網路、負載平衡器和其他資源時可能遇到的常見問題。

疑難排解主題涵蓋各式各樣的案例，包括 WordPress 組態失敗、IAM 權限問題、磁碟錯誤、連線問題、服務無法使用、IPv6 連線能力、執行個體容量限制、負載平衡器錯誤、通知傳遞失敗以及 SSL/TLS 憑證問題。遵循本指南，您可以有效地疑難排解並解決與 Lightsail 資源相關的各種問題，確保應用程式和工作負載的順暢運作和最佳效能。

### 主題

- [排解 Lightsail WordPress 執行個體上的設定問題](#)
- [解決控制台中的 403 個 \( 未經授權 \) 錯誤](#)
- [解決 Lightsail 磁碟附件和使用問題](#)
- [解決 Lightsail 瀏覽器型 SSH 和用戶端的連線錯誤 RDP](#)
- [解決 Lightsail 上的幽靈實例 503 服務不可用錯誤](#)
- [疑難排解 Lightsail 中的 Identity and Access Management \(IAM\)](#)
- [確認 Lightsail 執行個體的 IPv6 連線能力](#)
- [解決 Lightsail 中執行個體容量不足的錯誤](#)
- [疑難排解負載平衡器問題](#)
- [疑難排解 Lightsail 中的通知傳遞](#)
- [疑難排解 SSL/TLS 憑證](#)

## 排解 Lightsail WordPress 執行個體上的設定問題

在 Amazon Lightsail 的 WordPress 設定工作流程期間，可能會出現兩種類型的錯誤訊息：

### 常見錯誤

在工作流程的最後一個步驟中選擇 [建立憑證] 之後，會立即發生這些類型的錯誤。這些錯誤會出現在 Lightsail 主控台頂端的橫幅中。這些問題通常是因為在較舊的執行個體上 WordPress 執行設定工作流程，或提交錯誤的資訊所造成。例如，選取不會指向執行個體公用 IP 位址的 DNS 記錄。

## 安裝失敗

這些類型的錯誤會在您完成工作流程的最後一個步驟後的幾分鐘內發生。這些失敗訊息會顯示在執行個體 [Connect] 索引標籤的 [設定您的 WordPress 網站] 區段中。當無法在您的執行個體上設定 Let's Encrypt HTTPS 憑證時，就會發生這些錯誤。

使用下列主題中的資訊，協助您診斷並修正在 WordPress 設定引導式工作流程中可能遇到的任何錯誤。

### 主題

- [解決 WordPress 安裝 Lightsail](#)
- [疑難排解 WordPress 安裝失敗](#)

如需 Amazon Lightsail 中 WordPress 設定引導式工作流程的詳細資訊，請參閱[設定您的 WordPress 執行個體](#)。

## 解決 WordPress 安裝 Lightsail

如果工作流程期間提交的資訊發生問題，Lightsail 主控台頂端會顯示錯誤訊息。

訊息的第一行通知您安裝程式遇到錯誤：

無法完成執行個體的設定 *InstanceName* 在 *InstanceRegion* 區域。

第二行包含安裝程式遇到的錯誤：

發生錯誤，我們無法連線或保持連線至您的執行個體

**We encountered an error while configuring the Let's Encrypt SSL/TLS certificate on your instance test-2 in the us-east-1 Region. Try again later. An error occurred and we were unable to connect or stay connected to your instance. If this instance has just started up, try again in a minute or two.**

若要開始疑難排解，請將訊息中出現的錯誤與下列其中一個錯誤相符。

### 錯誤

- [DNS找不到記錄。確認網域的DNS記錄指向執行個體的公用 IP 位址，並預留時間傳播DNS變更。](#)
- [DNS記錄不匹配。確認網域的DNS記錄指向執行個體的公用 IP 位址，並預留時間傳播DNS變更。](#)
- [無法連線至您的執行個體。等待幾分鐘，讓SSH連接準備就緒。然後，重新開始設定。](#)
- [不支援的 WordPress 版本。安裝程式僅支援 WordPress 版本 6 及以上版本。](#)
- [安裝程式僅支援在 2023 年 1 月 1 日或之後建立的 WordPress 執行個體。](#)

- [執行個體防火牆連接埠 22、80 和 443 必須允許在設定工作流程期間從任何 IP 位址進行TCP連線。您可以從執行個體網路索引標籤變更這些設定。](#)

DNS找不到記錄。確認網域的DNS記錄指向執行個體的公用 IP 位址，並預留時間傳播DNS變更。

#### 原因

此錯誤的原因是設定錯誤的DNS記錄，或是沒有足夠時間在整個網際網路上傳播的DNS記錄所造成。DNS

#### 修復

確認 A 或AAAADNS記錄存在於DNS區域中，並指向執行個體的公用 IP 位址。如需詳細資訊，請參閱[DNS中的](#)。

當您新增或更新指向來自頂點網域 (example.com) 及其www子網域 (www.example.com) 流量的DNS記錄時，這些記錄將需要在整個網際網路中傳播。DNS [您可以通過使用工具，如 nslookup，或 DNS查找來自驗證您的DNS更改已生效。MxToolbox](#)

#### Note

允許任何DNS記錄更改通過互聯網傳播的時間DNS，這可能需要幾個小時。

DNS記錄不匹配。確認網域的DNS記錄指向執行個體的公用 IP 位址，並預留時間傳播DNS變更。

#### 原因

A 或AAAADNS記錄不會指向執行個體的公用 IP 位址。

#### 修復

確認 A 或AAAADNS記錄存在於DNS區域中，並指向執行個體的公用 IP 位址。如需詳細資訊，請參閱[DNS中的](#)。

#### Note

允許任何DNS記錄更改通過互聯網傳播的時間DNS，這可能需要幾個小時。

無法連線至您的執行個體。等待幾分鐘，讓SSH連接準備就緒。然後，重新開始設定。

#### 原因

執行個體剛剛建立或重新啟動，且SSH連線尚未準備就緒。

#### 修復

等待幾分鐘，讓SSH連接準備就緒。然後，重試引導式工作流程。如需詳細資訊，請參閱 [Lightsail SSH 中的疑難排解](#)。

不支援的 WordPress 版本。安裝程式僅支援 WordPress 版本 6 及以上版本。

#### 原因

執行個體上安裝的 WordPress 版本比第 6 版舊。WordPress 舊 WordPress 版本包含不相容的軟體和相依性，可防止產生HTTPS憑證。

#### 修復

從 Lightsail 主控台建立新的 WordPress 執行個體。然後，將 WordPress 網站從舊執行個體遷移到新的執行個體。如需詳細資訊，請參閱 [移轉現有 WordPress 部落格](#)。

如果您要建立新的執行個體來取代現有的執行個體，請務必將應用程式相依性更新至新執行個體。

安裝程式僅支援在 2023 年 1 月 1 日或之後建立的 WordPress 執行個體。

#### 原因

與安裝程式搭配使用的執行個體可能包含過期的軟體。較舊的軟體將防止產生HTTPS憑證。

#### 修復

從 Lightsail 主控台建立新的 WordPress 執行個體。然後，將 WordPress 網站從舊執行個體遷移到新的執行個體。如需詳細資訊，請參閱 [移轉現有 WordPress 部落格](#)。

如果您要建立新的執行個體來取代現有的執行個體，請務必將應用程式相依性更新至新執行個體。

執行個體防火牆連接埠 22、80 和 443 必須允許在設定工作流程期間從任何 IP 位址進行 TCP 連線。您可以從執行個體網路索引標籤變更這些設定。

## 原因

執行個體防火牆連接埠 22、80 和 443 必須在安裝程式執行時允許來自任何 IP 位址的 TCP 連線。關閉其中一個或多個連接埠時，就會產生此錯誤。如需詳細資訊，請參閱[執行個體防火牆](#)。

## 修復

新增或編輯執行個體 IPv4 和 IPv6 防火牆規則，以允許 TCP 連接埠 22、80 和 443 進行連線。如需詳細資訊，請參閱[新增和編輯執行個體防火牆規則](#)。

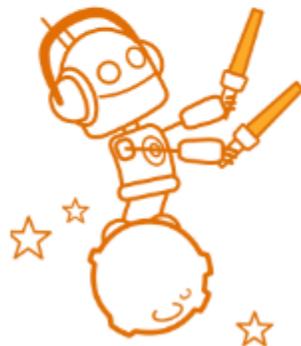
## 疑難排解 WordPress 安裝失敗

下列資訊可協助您疑難排解可能出現在執行個體 [Connect] 索引標籤 [設定您的 WordPress 網站] 區段中的失敗訊息。在您完成工作流程的最後一個步驟之後，可能會在幾分鐘內發生安裝失敗。這是因為無法在您的執行個體上設定 [讓我們加密 HTTPS 憑證] 時造成的。

無法完成設定 — 檢閱下列狀態訊息，然後重新啟動安裝程式以更新您的組態。如需詳細資訊，請下載錯誤記錄檔。

**✘ Failed to complete setup**  
Review the following status messages, and restart setup to update your configuration.  
[Download the error log](#) for more details.

[Restart setup](#)



- ✔ Domain
- ✔ DNS zone
- ✔ Static IP
- ✔ Map domains & subdomains
- ✘ **SSL/TLS certificate**  
Certificate failed to validate.

從失敗訊息中，選擇 [下載錯誤記錄檔] 連結以下載並檢視安裝程式產生的錯誤記錄檔。若要開始疑難排解，請將記錄檔中的錯誤訊息與下列其中一個錯誤相符。

## 錯誤

- [證書錯誤。 AuthorizationError: 有些挑戰失敗](#)
- [無法驗證某些網域](#)
- [存儲庫 <http://cdn-aws.deb.debian.org/debian> 破壞者反向端口不再具有發布文件](#)
- [存儲庫 <http://ppa.launchpad.net/certbot/certbot/ubuntu> 月球釋放沒有發布文件](#)
- [過去 168 小時內已經為這組確切的域發行了太多證書 \( 5 \)](#)
- [授權失敗太多](#)

## 證書錯誤。 AuthorizationError: 有些挑戰失敗

### 原因

此錯誤的原因是 DNS 記錄設定錯誤，或是沒有足夠時間在整個網際網路上傳播的 DNS 記錄所造成。

### 修復

確認 DNS 區域中存在 A 或 AAAA DNS 記錄，並且這些記錄指向執行個體的公用 IP 位址。如需詳細資訊，請參閱 [Lightsail](#)。

當您新增或更新指向來自頂點網域 (example.com) 及其www子網域 (www.example.com) 流量的 DNS 記錄時，這些記錄必須在整個網際網路中傳播。您可以驗證您的 DNS 更改已經通過使用工具生效，或 [DNS 查找](#) 從 MxToolbox

#### Note

預留時間讓任何 DNS 記錄變更透過網際網路的 DNS 傳播，這可能需要數小時。

## 無法驗證某些網域

### 原因

如果另一個進程正在使用端口 80，而在實例上配置 HTTPS 證書時，則可能會出現此錯誤。

### 修復

重新啟動 WordPress 執行個體。然後，再次執行引導式工作流程。如果重新啟動無法解決問題，請使用下列程序終止在連接埠 80 上執行的執行個體上的任何執行中處理序。

## 程序

1. 使用 Lightsail [瀏覽器型安全殼層用戶端](#) 或使用 Connect 線至執行個體。 [AWS CloudShell](#)
2. 停止執行個體上執行的 Bitnami 程序：

```
$ sudo /opt/bitnami/ctlscript.sh stop
```

確認 Bitnami 處理程序已停止：

```
$ sudo /opt/bitnami/ctlscript.sh status
```

3. 檢查是否有其他進程正在使用端口 80：

```
$ fuser -n tcp 80
```

4. 終止其他應用程序不需要的任何進程：

```
$ fuser -k -n tcp 80
```

5. 重新啟動 WordPress 設定。

存儲庫 <http://cdn-aws.deb.debian.org/debian> 破壞者反向端口不再具有發布文件

## 原因

您的執行個體上有一個不被取代的 Debian 儲存庫無法更新。

## 修復

使用以下步驟來編輯 Debian 軟件庫文件中列出的存儲庫 URL。

## 程序

1. 使用 Lightsail [瀏覽器型安全殼層用戶端](#) 或使用 Connect 線至執行個體。 [AWS CloudShell](#)
2. 導覽至 `/etc/apt/sources.list.d/` 目錄。

```
$ cd /etc/apt/sources.list.d/
```

3. 使用您選擇的文字編輯器來開啟 `buster-backports.list` 檔案。如果在此目錄中找不到檔案，您也可以入庫納管 `/etc/apt/sources.list`。在示例命令中使用預先安裝的 Vim 文本編輯器。有關更多信息，請參閱 [Vim 文檔](#)。

```
$ vim buster-backports.list
```

4. 找到包含下列文字的任何一行：`http://deb.debian.org/debian buster-backports main`。

使用 `archive.debian.org` 取代 `deb.debian.org`。例如，`http://deb.debian.org/debian buster-backports main contrib non-free` 會變成 `http://archive.debian.org/debian buster-backports main contrib non-free`。

5. 儲存並關閉檔案。
6. 重新啟動 WordPress 設定。

存儲庫 `http://ppa.launchpad.net/certbot/certbot/ubuntu` 月球釋放沒有發布文件

#### 原因

您的執行個體上有一個已取代的 Certbot 個人 Package 封存 (PPA) 儲存庫無法更新。

#### 修復

請使用下列程序，從執行個體手動移除已取代的 PPA 存放庫。

#### 程序

1. 使用 Lightsail [瀏覽器型安全殼層用戶端](#) 或使用 Connect 線至執行個體。 [AWS CloudShell](#)
2. 導覽至 `/etc/apt/sources.list.d/` 目錄。

```
$ cd /etc/apt/sources.list.d/
```

3. 使用您選擇的文字編輯器來開啟 `certbot-ubuntu-certbot-version.list` 檔案。在示例命令中使用預先安裝的 Vim 文本編輯器。有關更多信息，請參閱 [Vim 文檔](#)。

在命令中，**version** 替換為存儲庫不兼容的 Ubuntu 版本；這將與錯誤消息中顯示的版本相同。例如 **lunar** 或 **mantic**。

```
$ vim certbot-ubuntu-certbot-version.list
```

4. 刪除包含以下文本的任何行：`http://ppa.launchpad.net/certbot/certbot/ubuntu`。
5. 儲存並關閉檔案。
6. 重新啟動 WordPress 設定。

## 過去 168 小時內已經為這組確切的域發行了太多證書 ( 5 )

### 原因

在上週內，您的一個或多個網域或子網域已用於建立 5 個憑證。如需詳細資訊，請參閱讓我們加密網站上的[速率限制](#)。

### 修復

請等待一週 (168 小時)，然後重新啟動此網域的引導式工作流程。

## 授權失敗太多

### 原因

要求中的一或多個網域或子網域已超過每小時五次驗證的限制。如需詳細資訊，請參閱讓我們加密網站上的[速率限制](#)。

### 修復

等待一小時，然後再次執行 WordPress 安裝程式。在重新啟動安裝程式之前，請確認其他驗證錯誤已修正。

## 解決控制台中的 403 個 ( 未經授權 ) 錯誤

如果您在嘗試訪問 [Lightsail 控制台](#) 時出現 403 錯誤，請不要驚慌。嘗試以下步驟來排除問題：

- 如果您的 AWS 帳戶或 AWS Identity and Access Management (IAM) 使用者是最近建立的，請等待幾分鐘，然後重新整理瀏覽器。
- 如果距離您上次登入已有一段時間，請重新整理您的瀏覽器。如果系統提示您再次登入，請務必使用具有 Lightsail 存取權的使用 IAM 者。

- 如果您的IAM使用者無法存取 Lightsail，請聯絡[AWS 帳戶根使用者](#)或具有管理員存取權限的IAM使用者，以要求 Lightsail 存取權。若要進一步了解，請參閱[管理使用IAM者對 Amazon Lightsail 的存取權限](#)。
- 如果在嘗試上述步驟後仍持續出現 403 錯誤，請聯絡 [AWS Support](#)。在 2011 年之前建立的 AWS 帳戶的罕見情況下，支援人員必須手動將您的帳戶訂閱至 Lightsail。

## 解決 Lightsail 磁碟附件和使用問題

您可能會在 Lightsail 中遇到區塊儲存磁碟的錯誤。此主題可識別常見問題和這些錯誤的解決方法。

### 一般磁碟錯誤

在下方選擇最符合您狀況的問題，並依照連結來修正問題。如果您遇到的問題不在清單中，請使用此頁面底部的 Questions? 評論? 本頁底部的連結可提交意見反應或聯絡 Sup [AWSport](#) 部門。

我無法刪除磁碟，因為它的仍連接到執行個體。

嘗試將該磁碟從您的執行個體分離，然後嘗試刪除磁碟。如需詳細資訊，請參閱[分離並刪除區塊儲存磁碟](#)。

實際錯誤訊息：您無法執行此作業，因為磁碟仍附加至 Lightsail 執行個體：***YOUR\_INSTANCE***

我的磁碟狀態為錯誤。

錯誤狀態表示與 Lightsail 磁碟相關的基礎硬體發生故障。您可以從最近的快照還原磁碟，否則與該磁碟關聯的資料將無法復原。如需詳細資訊，請參閱[透過快照建立區塊儲存磁碟](#)。

如果磁碟狀態為錯誤，則不會向您收費。

我無法分離磁碟，因為 Lightsail 實例仍在運行。

若要將根磁碟區分離，請先停用執行個體。如需詳細資訊，請參閱[停止執行個體](#)。

實際錯誤訊息：You can't detach this disk right now. 此磁碟的狀態為：***DISK\_STATE***

我無法將自訂磁碟大小指定超過 16 TB (16,384 GB)。

嘗試建立較小的磁碟。其他磁碟最多可達 16 TB。如果您的磁碟已經少於 16 TB 卻仍然無法建立，您可能會在清單中遇到下一個錯誤 (太多大型磁碟)。這是因為您的AWS帳戶中的額外磁碟儲存空間不能超過 20 TB。如需詳細資訊，請參閱[區塊儲存磁碟](#)。

實際錯誤訊息：The size of a block storage disk must be between 8 and 16384 GB. (區塊儲存磁碟大小必須介於 8 和 16384 GB 之間。)

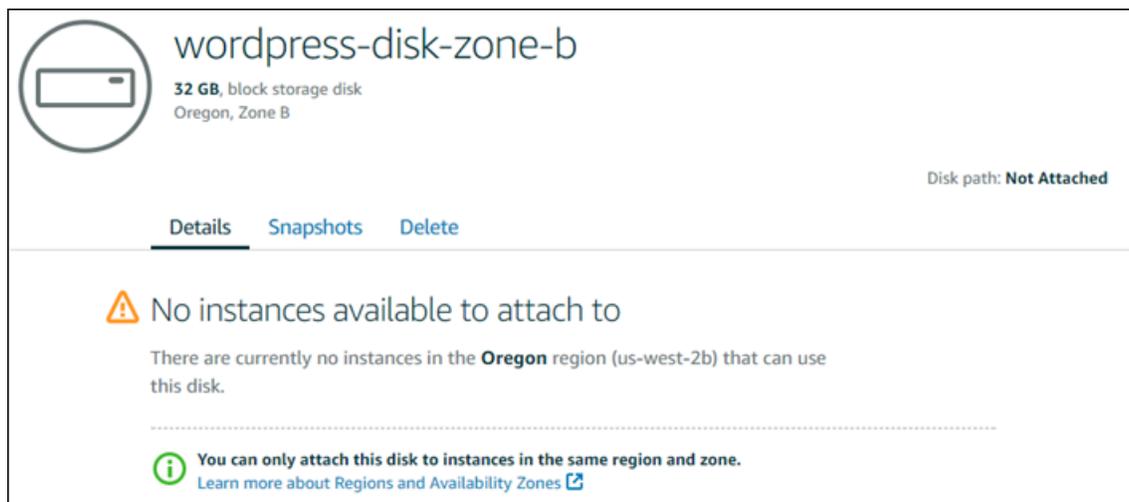
我無法在 Lightsail 中創建任何更多的磁盤。

您可能已達到可建立的磁碟數量配額。或者，您可能在AWS帳戶中建立了太多大磁碟 (磁碟儲存空間總大小不能超過 20 TB)。如需詳細資訊，請參閱[區塊儲存磁碟](#)。

實際錯誤訊息：You've reached the maximum size limit of all disks in this account. (您已達到此帳戶中所有磁碟的最大限制。) 或 You've reached the limit of disks in this account. (您已達到此帳戶的磁碟限制)。

我無法將我的磁碟附加到我的 Lightsail 執行個體

如果遇到下列錯誤，就必須在與計劃連接磁碟的執行個體相同的區AWS域和可用區域中重新建立磁碟。



實際錯誤訊息：目前中沒有執行個體 **AWS Region** 可以使用這個磁盤。

## 解決 Lightsail 瀏覽器型SSH和用戶端的連線錯誤 RDP

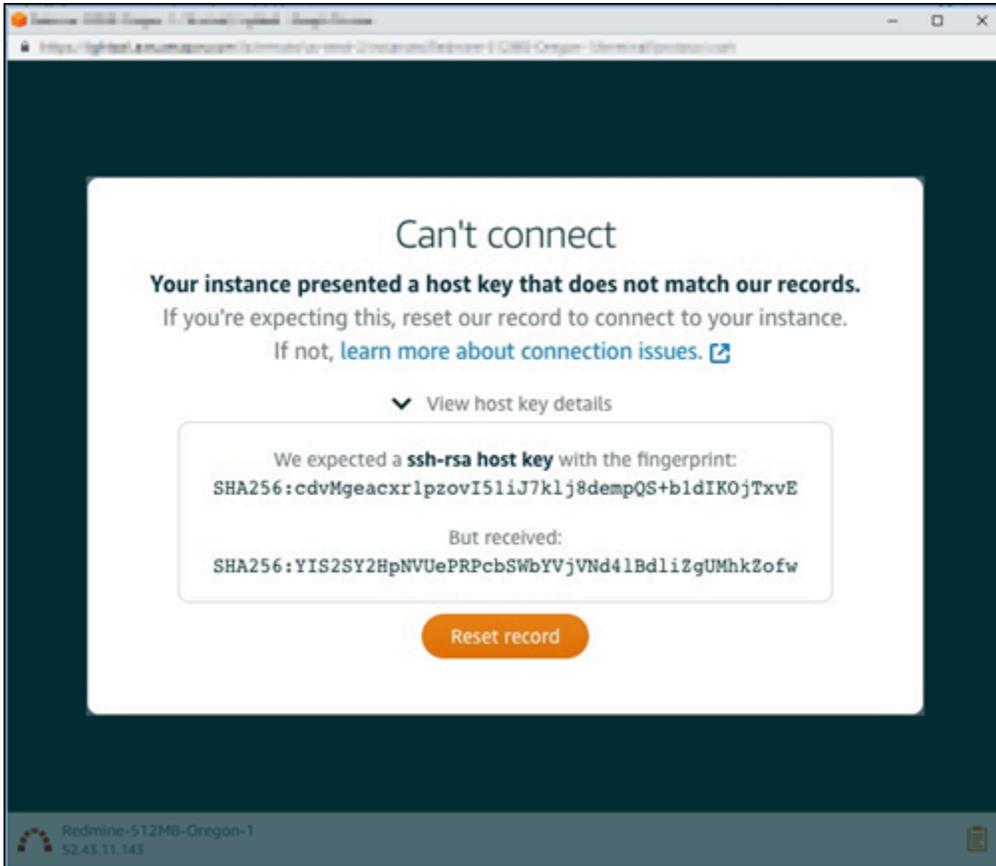
嘗試使用以瀏覽器為基礎的執行個體SSH或 Amazon Lightsail 主控台中可用的用RDP戶端連線到執行個體時，可能會收到錯誤訊息。下列各節旨在討論這個錯誤的可能原因。

### 錯誤訊息：無法連線

SSH和以RDP瀏覽器為基礎的用戶端會在嘗試連線至執行個體時使用主機金鑰或憑證驗證來驗證執行個體。如果執行個體顯示的主機金鑰或憑證與 Lightsail 記錄不符，則會顯示兩則錯誤訊息中的其中一則。本節會列出並說明這兩則錯誤訊息。

## Can't connect, reset record (無法連線，請重設記錄)

當主機金鑰或憑證不符時，會顯示下列錯誤訊息，且 Lightsail 判斷不相符可能是由於最近的作業系統升級，或是您或其他使用者故意更新主機金鑰或憑證所造成。在此情況下，Lightsail 已判斷主機金鑰或憑證不符合不是因為瀏覽器與執行個體之間網路上的錯誤動作者所造成。



如果您預期會出現這個不符錯誤，則可選擇 Reset record (重設記錄)。此動作會刪除 Lightsail 針對執行個體記錄的主機金鑰或憑證，並允許以瀏覽器為基礎SSH或RDP工作階段連線至執行個體。

您也可以使用下列 AWS Command Line Interface (AWS CLI) 命令，刪除 Lightsail 已記錄的主機金鑰或憑證。用於 *InstanceName* 下方，輸入您要刪除已知主機金鑰或憑證的執行個體名稱。用於 *Region* 下，輸入執行個體的「AWS區域」。

```
aws lightsail delete-known-host-keys --region Region --instance-name InstanceName
```

範例：

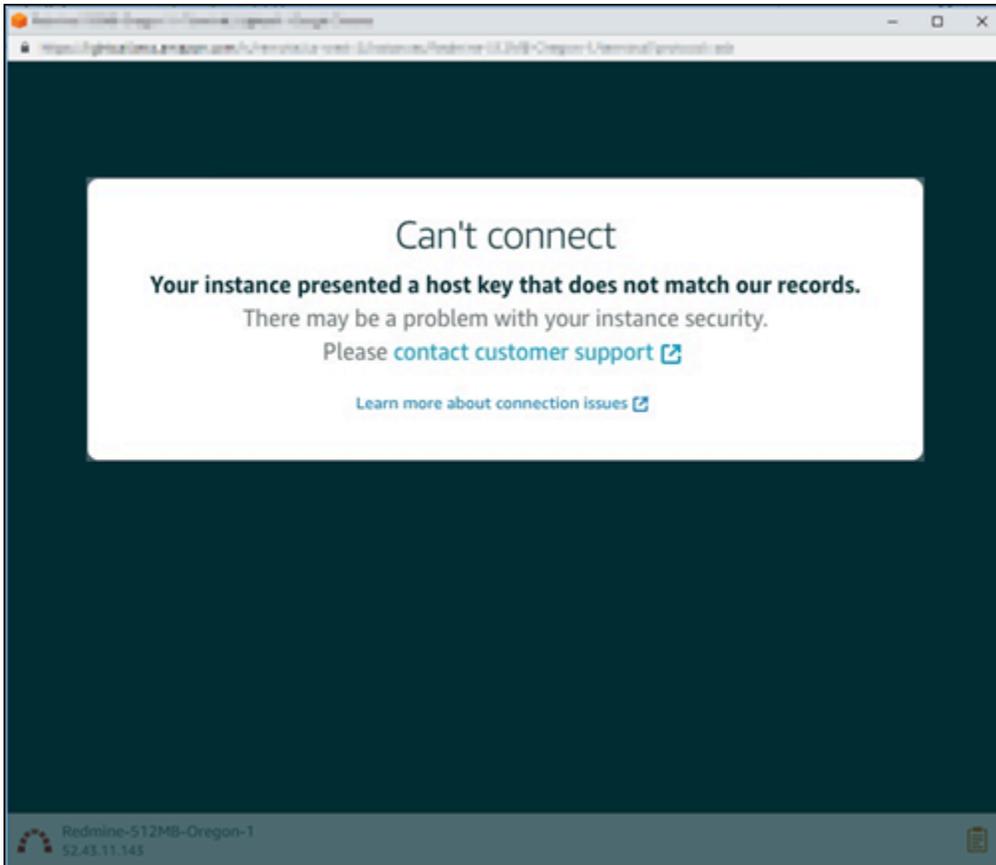
```
aws lightsail delete-known-host-keys --region us-west-2 --instance-name WordPress-512MB-Oregon-1
```

**Note**

如需有關的詳細資訊 AWS CLI，請參閱[設 AWS CLI 定使用 Lightsail](#)。

Can't connect, contact customer support (無法連線，請聯絡客戶支援)

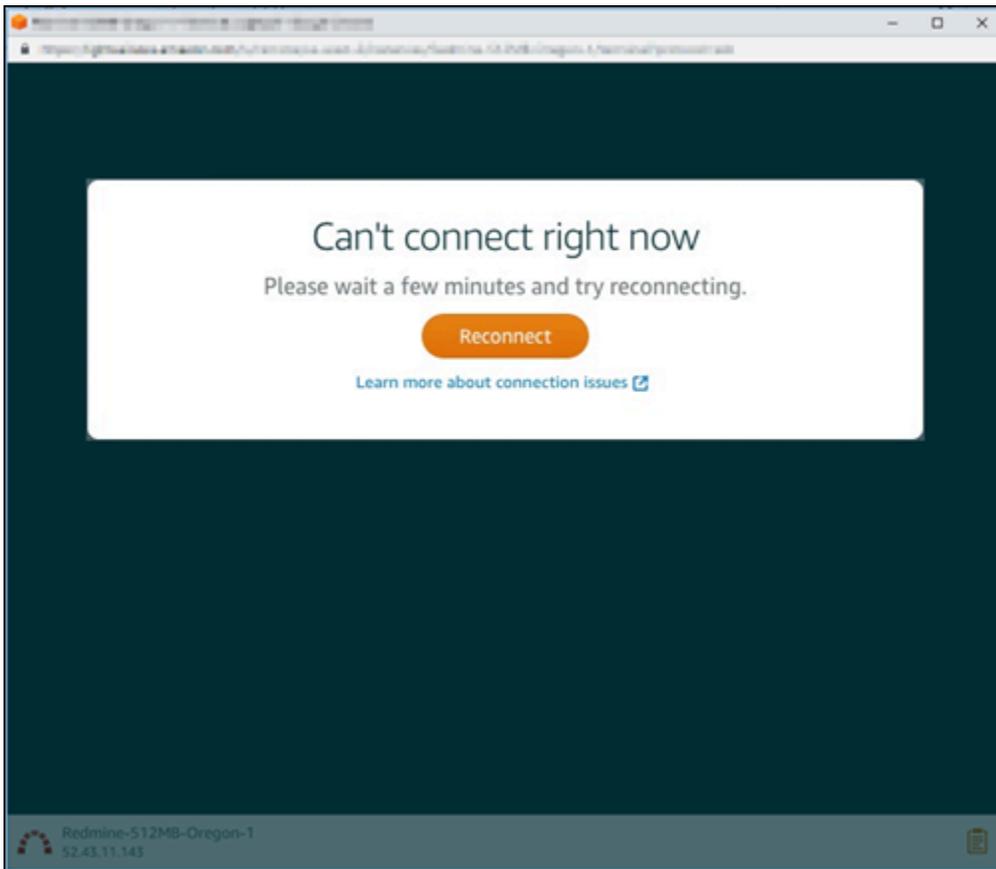
當主機金鑰或憑證不符時，會顯示下列錯誤訊息，且 Lightsail 判斷存在需要進一 man-in-the-middle 步調查的可疑活動 (例如攻擊)。



此錯誤訊息表示您無法使用瀏覽器SSH或用RDP戶端連線至執行個體。您可[聯絡支援](#)尋求協助。

## 錯誤訊息：目前無法連線

若您試著連線到完成建立、重新開機或重新啟動卻尚未啟動的執行個體，就會出現下列錯誤訊息。請稍候幾分鐘，然後選擇 Reconnect (重新連線)，再試一次。



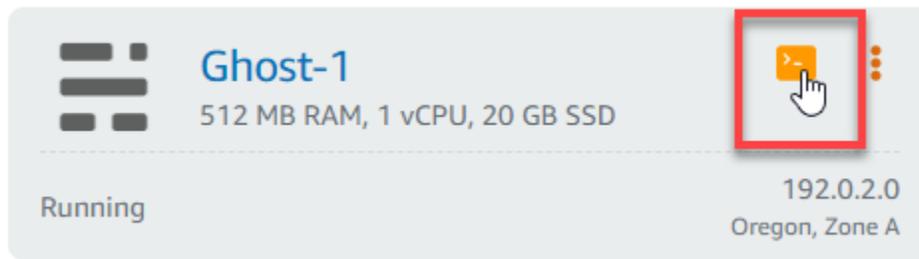
如果仍然無法連線，[請連絡 Sup AWS port](#) 部門。

## 解決 Lightsail 上的幽靈實例 503 服務不可用錯誤

在 Amazon Lightsail 中建立新的 Ghost 執行個體並嘗試存取您的網站後，您可能會看到錯誤訊息，指出服務無法使用 (503)。在某些情況下，執行個體建立時，不會自動啟動執行個體上的 Ghost 服務。當您為執行個體選取 USD 每月 \$5 美元的套裝軟體時，就會發生這種情況。請使用下列程序啟動 Ghost 服務，並解決「服務無法使用」錯誤。

### 啟動 Ghost 服務

1. 登入主 [Lightsail](#) 台。
2. 在 Lightsail 首頁上，選擇「實體」索引標籤。
3. 為 Ghost 執行個體選擇以瀏覽器為基礎的 SSH 用戶端圖示。



4. SSH用戶端連線之後，輸入下列命令以重新啟動執行個體上的所有服務：

```
sudo /opt/bitnami/ctlscript.sh restart
```

您應該會看到類似以下範例的結果：

```
bitnami@ip-172-26-11-214:~$ sudo /opt/bitnami/ctlscript.sh restart
Syntax OK
/opt/bitnami/apache2/scripts/ctl.sh : httpd stopped
/opt/bitnami/apps/ghost/scripts/ctl.sh : ghost not running
/opt/bitnami/mysql/scripts/ctl.sh : mysql stopped
/opt/bitnami/mysql/scripts/ctl.sh : mysql started at port 3306
[OK] Ensuring user is not logged in as ghost user [skipped]
[OK] Checking if logged in user is directory owner [skipped]
✓ Checking current folder permissions
✓ Validating config
✓ Checking memory availability
✓ Checking binary dependencies
✓ Starting Ghost: 127-0-0-1

-----

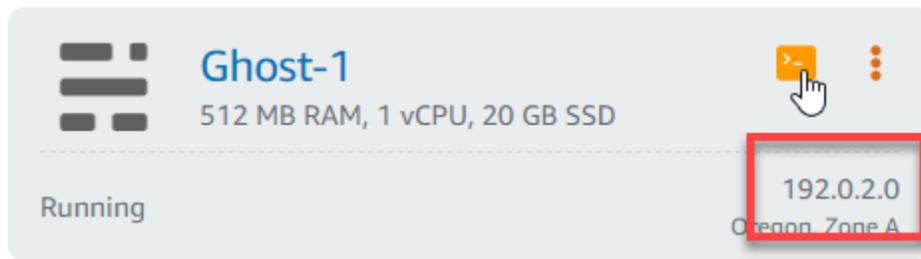
Your admin interface is located at:

  http://18.237.117.48:80/ghost/

/opt/bitnami/apps/ghost/scripts/ctl.sh : ghost started
Syntax OK
/opt/bitnami/apache2/scripts/ctl.sh : httpd started at port 80
```

5. 瀏覽至執行個體的公有 IP 地址，以確認您的 Ghost 網站已啟動並執行。

您執行個體的公有 IP 位址會列在 Lightsail 主控台的 [執行個體] 索引標籤中的執行個體名稱旁邊。



當您瀏覽至新 Ghost 執行個體的公有 IP 時，應該會看到預設 Ghost 網站範本：



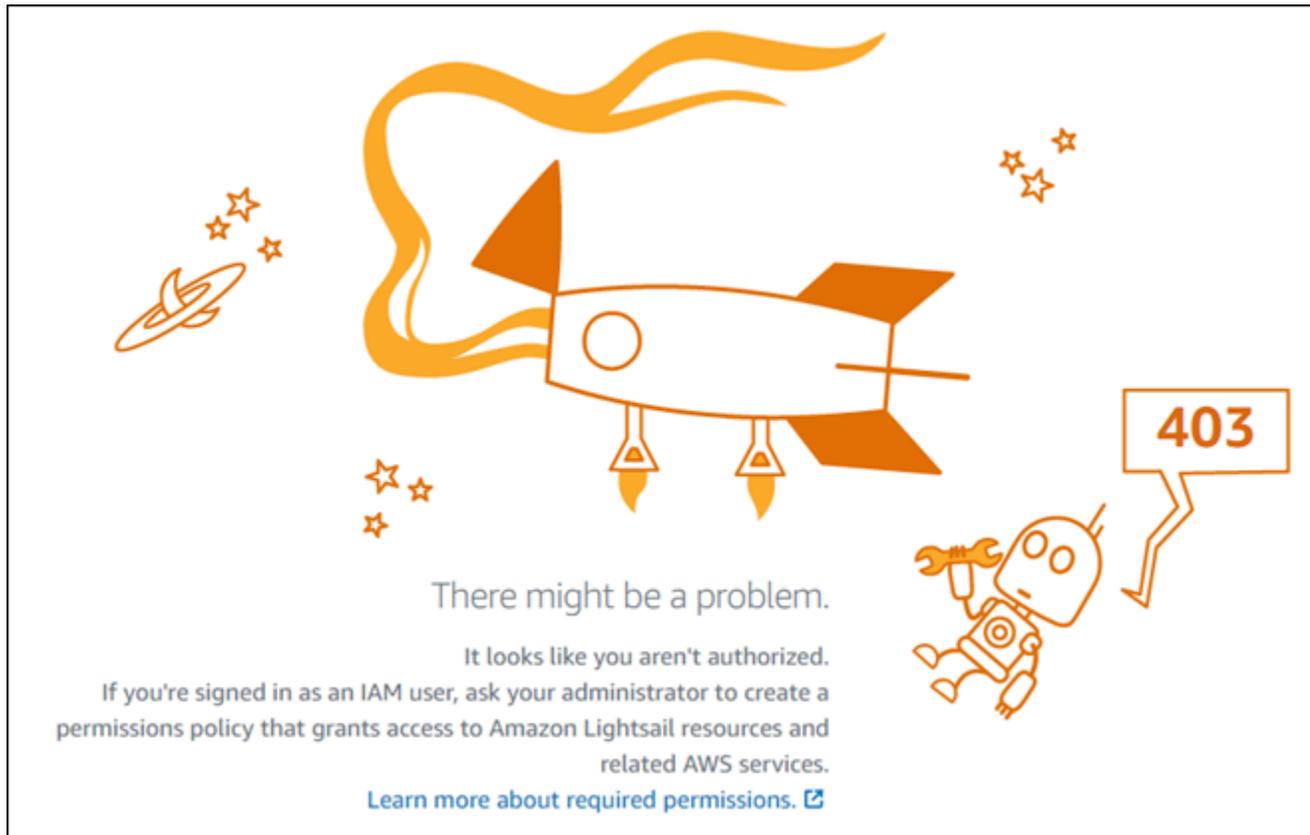
## 疑難排解 Lightsail 中的 Identity and Access Management (IAM)

使用下列資訊可協助您診斷並修正使用 Lightsail 和時可能會遇到的常見問題。IAM

## 我沒有執行任何動作的 Lightsail

如果 AWS Management Console 告訴您沒有執行動作的授權，則您必須聯絡管理員以尋求協助。您的管理員是提供您使用者名稱和密碼的人員。

當mateojacksonIAM使用者嘗試存取 Lightsail 主控台但沒有 `lightsail:*` (完整存取) 權限時，就會發生下列範例錯誤。



在此情況下，Mateo 會要求系統管理員更新原則，以允許他使用 `lightsail:*` (完整存取) 權限存取 Lightsail 主控台。

## 我沒有授權執行 iam : PassRole

如果您收到未獲授權執行 `iam:PassRole` 動作的錯誤訊息，則必須更新您的政策以允許您將角色傳遞給 Amazon Lightsail。

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

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

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

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

如果您需要協助，請聯絡您的 AWS 系統管理員。您的管理員提供您的登入憑證。

## 我想要檢視我的存取金鑰

建立使IAM用者存取金鑰後，您可以隨時檢視您的存取金鑰 ID。但是，您無法再次檢視您的私密存取金鑰。若您遺失了密碼金鑰，您必須建立新的存取金鑰對。

存取金鑰包含兩個部分：存取金鑰 ID (例如 AKIAIOSFODNN7EXAMPLE) 和私密存取金鑰 (例如 wJa1rXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY)。如同使用者名稱和密碼，您必須一起使用存取金鑰 ID 和私密存取金鑰來驗證您的請求。就如對您的使用者名稱和密碼一樣，安全地管理您的存取金鑰。

### Important

請勿將您的存取金鑰提供給第三方，甚至是協助[尋找您的標準使用者 ID](#)。通過這樣做，您可能會讓某人永久訪問您的 AWS 帳戶。

建立存取金鑰對時，您會收到提示，要求您將存取金鑰 ID 和私密存取金鑰儲存在安全位置。私密存取金鑰只會在您建立它的時候顯示一次。如果您遺失秘密存取金鑰，您必須將新的存取金鑰新增至您的 IAM 使用者。您最多可以擁有兩個存取金鑰。若您已有兩個存取金鑰，您必須先刪除其中一個金鑰對，才能建立新的金鑰對。若要檢視指示，請參閱《IAM 使用指南》中的 [〈管理存取金鑰〉](#)。

## 我是系統管理員，想要允許其他人存取 Lightsail

若要允許其他人存取 Amazon Lightsail，您必須將權限授予需要存取權的人員或應用程式。如果您使用 AWS IAM Identity Center 來管理人員和應用程式，您可以將權限集指派給使用者或群組，以定義其存取層級。權限集會自動建立原則，並將 IAM 原則指派給與人員或應用程式相關聯的 IAM 角色。如需詳細資訊，請參閱《AWS IAM Identity Center 使用指南》中的 [〈權限集〉](#)。

如果您未使用 IAM Identity Center，則必須為需要存取的人員或應用程式建立 IAM 實體 (使用者或角色)。然後，您必須將政策附加到實體，以便在 Amazon Lightsail 中授予他們正確許可。授與權限後，將認證提供給使用者或應用程式開發人員。他們將使用這些憑據來訪問 AWS。若要進一步了解如何建立 IAM 使 IAM 用者、群組、原則和權限，請參閱使用指南 IAM [中的 IAM 身分識別與原則與權限](#)。

## 我想允許我 AWS 帳戶以外的人員存取我的 Lightsail 資源

您可以建立一個角色，讓其他帳戶中的使用者或您組織外部的人員存取您的資源。您可以指定要允許哪些信任物件取得該角色。對於支援以資源為基礎的政策或存取控制清單 (ACLs) 的服務，您可以使用這些政策授與人員存取您的資源。

如需進一步了解，請參閱以下內容：

- 若要了解 Amazon Lightsail 是否支援這些功能，請參閱[亞 Amazon Lightsail 如何與 IAM](#)。
- 若要瞭解如何提供您所擁有資源 AWS 帳戶 的存取權，請參閱《[IAM使用者指南](#)》中 [AWS 帳戶 的〈提供存取權給其他IAM使用者〉](#)。
- 若要瞭解如何將資源存取權提供給第三方 AWS 帳戶，請參閱《[IAM使用指南](#)》中 [的提供第三方 AWS 帳戶 擁有的存取權](#)。
- 若要瞭解如何透過身分聯盟提供存取權，請參閱[使用指南中的提供對外部驗證使用IAM者的存取權 \(身分聯合\)](#)。
- 若要瞭解針對跨帳號存取使用角色與以資源為基礎的政策之間的差異，請參閱《[使用IAM者指南](#)》[IAM中的〈跨帳號資源存取〉](#)。

## 確認 Lightsail 執行個體的 IPv6 連線能力

您可以使用偵測工具驗證從本機電腦到 Amazon Lightsail 執行個體的 IPv6 連線。Ping 是一種網路診斷公用程式，用來疑難排解兩個或多個網路裝置之間的連線問題。如果 ping 成功，您應該可以透過 IPv6 連線到您的執行個體。如果網路設定或裝置未設定為允許 IPv6，ping 命令會失敗。如需更多資訊，請參閱[IPv6僅考慮因素](#)

### 目錄

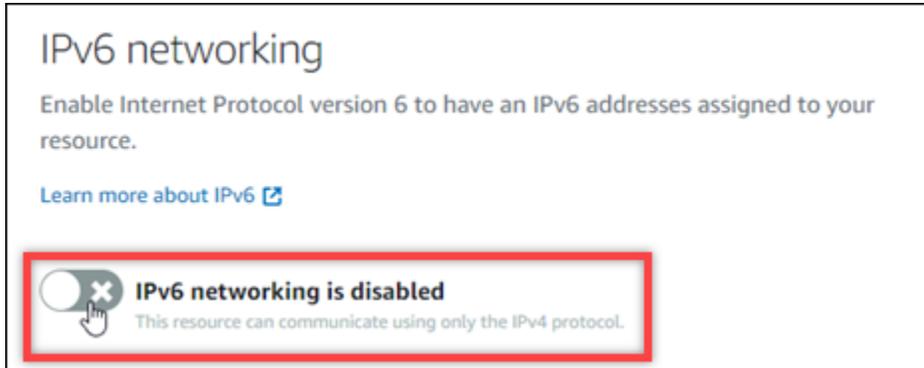
- [為雙堆疊執行個體啟用 IPv6](#)
- [設定執行個體的防火牆](#)
- [測試執行個體的可達性](#)

## 為雙堆疊執行個體啟用 IPv6

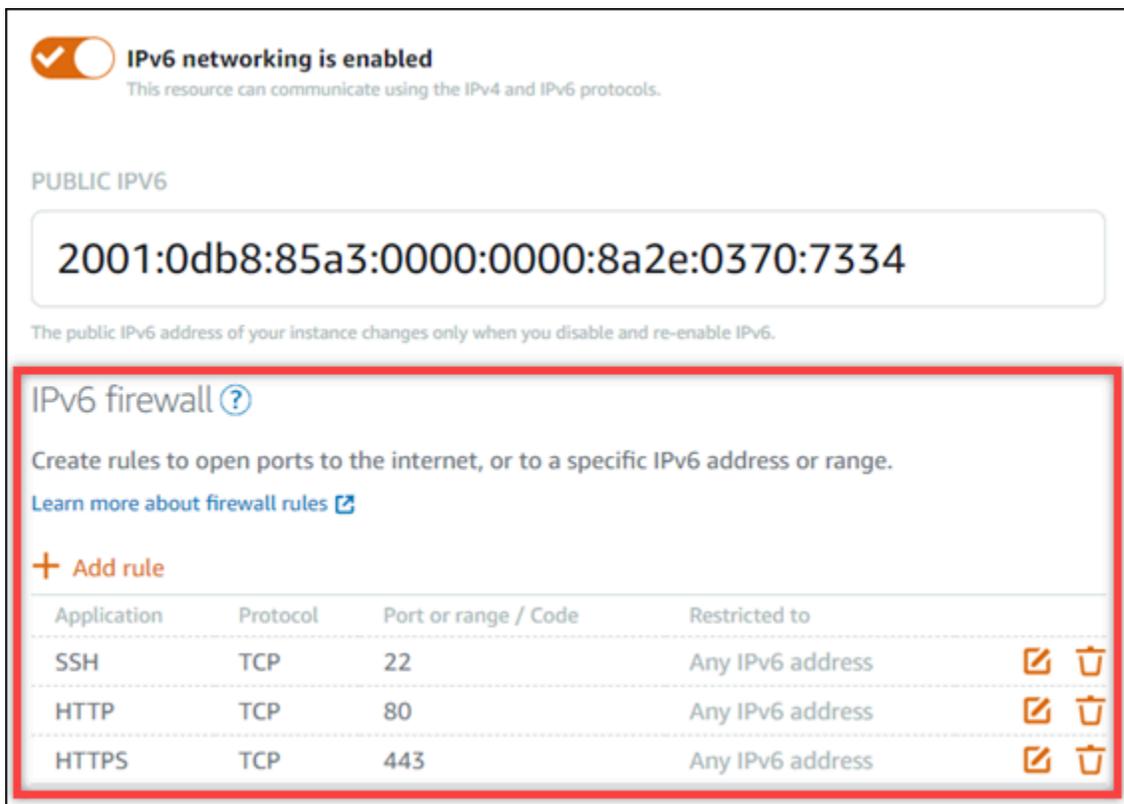
在開始測試之前，請為雙堆疊執行個體啟用 IPv6。對於僅限 IPv6 的執行個體，IPv6 永遠處於開啟狀態。

如果您的雙堆疊執行個體未啟用 IPv6，請完成下列程序來啟用 IPv6。

1. 登入主 [Lightsail 台](#)。
2. 選擇您要啟用 IPv6 的執行個體名稱。確定您的執行個體正在執行。
3. 從執行個體管理頁面選擇 [網路] 索引標籤。
4. 在頁面的 [IPv6 網路功能] 區段中啟用 IPv6。



啟用 IPv6 之後，會將公用 IPv6 位址指派給您的執行個體，而 IPv6 防火牆就會變成可用。



5. 記下頁面頂端執行個體的公用 IPv4 和公用 IPv6 位址。您將在以下各節中使用它們。

## 設定執行個體的防火牆

Lightsail 主控台中的防火牆充當虛擬防火牆。這意味著它控制允許哪些流量通過其公共 IP 地址連接到您的實例。您在 Lightsail 中建立的每個雙堆疊執行個體都有個別的 IPv4 位址防火牆，而另一個用於 IPv6 位址的防火牆。每個防火牆都包含一組篩選進入執行個體之流量的規則。兩個防火牆彼此獨立-您必須分別為 IPv4 和 IPv6 配置防火牆規則。使用僅限 IPv6 執行個體方案的執行個體沒有可設定的 IPv4 防火牆。

完成下列程序，以針對網際網路控制訊息通訊協定 (ICMP) 流量設定執行個體的防火牆。ping 公用程式會使用 ICMP 通訊協定與您的執行個體進行通訊。如需詳細資訊，請參閱 [使用 Lightsail 中的防火牆控制執行個體流](#)。

### Important

Windows 和 Linux 包含一個可以阻止 ping 命令的操作系統 (OS) 級防火牆。在繼續之前，請確認執行個體的作業系統防火牆可以接受 IPv4 和 IPv6 上的 ICMP 流量。如需詳細資訊，請參閱下列文件：

- [使用 Connect 至 Lightsail 執行個體 RDP](#)
- [Connect 到 Linux 或 Unix 執行 Lightsail](#)

1. 登入主 [Lightsail 台](#)。
2. 選擇您要設定防火牆的執行個體名稱。
3. 從執行個體管理頁面選擇 [網路功能] 索引標籤，然後針對您要使用的防火牆類型完成適當區段中的其餘步驟。對於 IPv4，請完成「IPv4 防火牆」一節中的步驟。對於 IPv6，請完成 IPv6 防火牆一節中的步驟。
  - a. 從應用程式下拉式功能表中，選擇 Ping (ICMP)。
  - b. 選取 [限制為 IP 位址] 方塊以允許從您的本機來源 IP 位址或範圍進行連線，然後輸入您的來源 IP 位址。(選擇性) 您可以不勾選此方塊，以允許來自任何 IP 位址的連線。建議您僅在測試環境中使用此選項。
  - c. 選擇 [建立]，將新規則套用至您的執行個體。

## 測試執行個體的可達性

請完成下列程序，測試從本機電腦或網路到 Lightsail 執行個體的 IPv4 或 IPv6 連線能力。您需要在 [Step 5](#) 記錄的執行個體公用 IPv4 和 IPv6 位址。

從 Linux、Unix 或 macOS 裝置

1. 在本機裝置上開啟終端機視窗。
2. 輸入下列其中一個命令來偵測您的 Lightsail 實體。將命令中的範例 *IP ##* 取代為執行個體的公用 IPv4 或 IPv6 位址。

若要透過 IPv4 進行測試

```
ping 192.0.2.0
```

若要透過 IPv6 進行測試

```
ping6 2001:db8::
```

3. 指令傳回一些回覆後，請 `ctrl+z` 在裝置的鍵盤上輸入以停止指令。

`ping` 命令會從執行個體的 IPv4 位址傳回成功的回覆 (如果成功)。結果應如下列範例所示。

```
$ ping 54.197.128.58
PING 54.197.128.58 56(84) bytes of data:
64 bytes from 54.197.128.58: icmp_seq=1 ttl=63 time=0.323 ms
64 bytes from 54.197.128.58: icmp_seq=2 ttl=63 time=0.284 ms
64 bytes from 54.197.128.58: icmp_seq=3 ttl=63 time=0.324 ms
64 bytes from 54.197.128.58: icmp_seq=4 ttl=63 time=0.617 ms
^Z
[1]+  Stopped                  ping 54.197.128.58
$
```

如果成功，`ping6` 命令會從執行個體的 IPv6 位址傳回成功的回覆。結果應如下列範例所示。

```
$ ping6 2001:1f18:17a0:68f4:b75e:3ee3:4bf1:67b7
PING 2001:1f18:17a0:68f4:b75e:3ee3:4bf1:67b7 56 data bytes
64 bytes from 2001:1f18:17a0:68f4:b75e:3ee3:4bf1:67b7: icmp_seq=1 ttl=255 time=0.698 ms
64 bytes from 2001:1f18:17a0:68f4:b75e:3ee3:4bf1:67b7: icmp_seq=2 ttl=255 time=0.228 ms
64 bytes from 2001:1f18:17a0:68f4:b75e:3ee3:4bf1:67b7: icmp_seq=3 ttl=255 time=0.322 ms
^Z
[1]+  Stopped                  ping6 2001:1f18:17a0:68f4:b75e:3ee3:4bf1:67b7
```

如果無法達到您的實例，這兩個命令都會返回請求超時。

### 從視窗裝置

1. 開啟命令提示。
2. 輸入下列其中一個命令來偵測您的 Lightsail 實體。將命令中的範例 *IP ##* 取代為執行個體的公用 IPv4 或 IPv6 位址。

若要透過 IPv4 進行測試

```
ping 192.0.2.0
```

若要透過 IPv6 進行測試

```
ping 2001:db8::
```

3. 指令傳回一些回覆後，請 `ctrl+z` 在裝置的鍵盤上輸入以停止指令。

`ping` 命令會從執行個體的 IPv4 位址傳回成功的回覆 (如果成功)。結果應如下列範例所示。

```
C:\Users\Administrator>ping 192.0.2.0

Pinging 192.0.2.0 with 32 bytes of data:
Reply from 192.0.2.0: bytes=32 time=10ms TTL=53
Reply from 192.0.2.0: bytes=32 time=10ms TTL=53
Reply from 192.0.2.0: bytes=32 time=11ms TTL=53
Reply from 192.0.2.0: bytes=32 time=10ms TTL=53

Ping statistics for 192.0.2.0:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 10ms, Maximum = 11ms, Average = 10ms
```

如果執行個體的 IPv6 位址成功，`ping` 命令會傳回成功的回覆。結果應如下列範例所示。

```
C:\Users\Administrator>ping 3a69:821:c21:1b:bc99:3066:1b:701:c2009:822

Pinging 3a69:821:c21:1b:bc99:3066:1b:701:c2009:822 with 32 bytes of data:
Reply from 3a69:821:c21:1b:bc99:3066:1b:701:c2009:822: time=74ms
Reply from 3a69:821:c21:1b:bc99:3066:1b:701:c2009:822: time=74ms
Reply from 3a69:821:c21:1b:bc99:3066:1b:701:c2009:822: time=74ms
Reply from 3a69:821:c21:1b:bc99:3066:1b:701:c2009:822: time=74ms

Ping statistics for 3a69:821:c21:1b:bc99:3066:1b:701:c2009:822:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 74ms, Maximum = 74ms, Average = 74ms
```

如果無法達到您的實體，這兩個命令都會返回請求超時。

## 解決 Lightsail 中執行個體容量不足的錯誤

當您嘗試啟動執行個體或重新啟動已停止的執行個體時，可能會發生容量不足的錯誤。這表示目前 AWS 沒有可用的執行個體容量來滿足您的要求。以下是執行個體容量不足錯誤的範例：

**InsufficientInstanceCapacity**：沒有足夠的容量來滿足您的執行個體要求。減少請求中的執行個體數量，或等候其他容量可供使用。您也可以選取較小的 Lightsail 方案 (您可以在稍後的階段調整大小) 來嘗試啟動實體。」

在本指南中，您將了解發生執行個體容量不足錯誤時可採取的動作。

### 內容

- [啟動新的執行個體時容量不足](#)
- [啟動停止的執行個體時容量不足](#)
- [相關資訊](#)

## 啟動新的執行個體時容量不足

如果在啟動新的執行個體時發生執行個體容量不足的錯誤，請採用下列選項。您可以依序完成每個選項，也可以選擇適合您的選項。

1. 等候幾分鐘，然後再次提交您的請求。執行個體容量會頻繁變化。如果您在等待幾分鐘後仍無法建立執行個體，請前往選項 2。

2. 建立執行個體時，請選取不同的可用區域 (AZ)。每個 AWS 區域 包含三個以上的 AZ，而且每個 AZ 維護的執行個體容量皆不同。透過選取不同的 AZ，您可以利用其目前的執行個體容量。如果您無法在其他 AWS 區域 或 AZ 中建立執行個體，請繼續進行選項 3。
3. 減少請求中的執行個體數量。如果您要同時建立多個執行個體，請減少執行個體數量，然後再次提交請求。如果減少執行個體數量無法解決問題，請前往選項 4。
4. 建立執行個體時，請選擇不同的執行個體計劃。如果您無法在不同的 AZ 或區域中建立執行個體，請選擇不同的執行個體計劃。您可以在後續階段調整執行個體大小。如需調整執行個體大小的詳細資訊，請參閱[從快照建立執行個體](#)。

## 啟動停止的執行個體時容量不足

如果您在啟動現有執行個體 (先前已停止) 時發生執行個體容量不足的錯誤，請採用下列選項。

1. 等候幾分鐘，然後再次提交您的請求。執行個體容量會頻繁變化。如果您在等待幾分鐘後仍無法建立執行個體，請前往選項 2。
2. 從快照建立新的執行個體。對於停止的執行個體取得快照。然後，使用快照在 AZ 中建立與原始執行個體不同的新執行個體。例如，如果您的執行個體目前位於 us-east-2a (區域 A)，請在建立新執行個體時選取 us-east-2c (區域 C)。如需詳細資訊，請參閱[透過快照建立執行個體](#)。
3. 從快照建立新的執行個體時，您也可以選擇不同的執行個體計劃。此動作為選用。

### Important

執行新的執行個體後，請確認您擁有新執行個體的存取權，並確認所有項目都正常運作。例如，如果您的執行個體正在執行應用程式，請確認該應用程式如預期運作。如果正常運作，您即可刪除先前的執行個體。

## 相關資訊

[常見問答集](#)

[Lightsail 中的韌性](#)

## 疑難排解負載平衡器問題

您可能會在使用 Lightsail 負載平衡器時遇到錯誤。此主題可識別常見問題和這些錯誤的解決方法。

## 一般負載平衡器錯誤

在下方選擇最符合您狀況的問題，並依照連結來修正問題。如果您遇到的問題不在清單中，請使用此頁面底部的 [Questions？ 評論？](#) 本頁底部的連結可提交意見反應或聯絡AWS客戶 Support。

我無法建立憑證。

您可以在帳戶中建立的憑證數量有配 AWS 額。如需詳細資訊，請參閱 [Cer AWS tificate Manager](#) 使用指南中的 [配額](#)。相同的配額適用於負載平衡器的 Lightsail 憑證。

實際錯誤訊息：Sorry, you've requested too many certificates for your account. (很抱歉，您已為帳戶申請太多憑證。)

我無法連接任何更多的執行個體到我的負載平衡器。

只要您保持在每 AWS 個帳戶總共 20 個 Lightsail 執行個體的配額內，您就可以將任意數量的 Lightsail 執行個體連接到負載平衡器。

實際錯誤訊息：Sorry, you've reached the maximum number of instances you can attach to this load balancer. (很抱歉，您已達到此負載平衡器可連接的執行個體最大數量。)

我無法連接特定執行個體到我的負載平衡器。

首先，請檢查以確定您的 Lightsail 執行個體正在執行。如果已停止，可以從執行個體管理頁面啟動它。Lightsail 執行個體必須在執行中，才能成功連接到負載平衡器。

可能是您將相同的執行個體連接到太多的負載均衡器。

實際錯誤訊息：Sorry, you've reached the maximum number of times an instance can be registered with a load balancer. (很抱歉，您已達到為負載平衡器註冊執行個體的次數上限。)

Lightsail 找不到我嘗試連接到負載平衡器的執行個體

您可能會嘗試連結已不存在或與目標群組不VPC同的執行個體。

實際錯誤訊息：抱歉，您指定的執行個體不存在、與目標群組不VPC相同，或具有不支援的執行個體類型。

## 疑難排解 Lightsail 中的通知傳遞

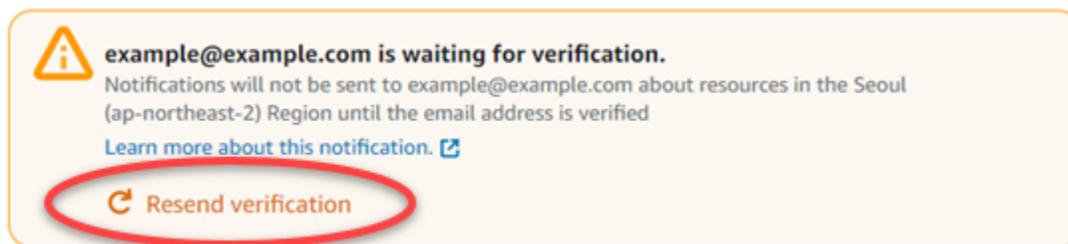
如果在您預期收到通知時沒有收到通知，您應該檢查一些事項，確認您的通知聯絡人設定正確。若要進一步了解通知，請參閱[通知](#)。

下列清單說明您可能遇到的常見通知聯絡人問題、其造成原因，以及其解決方式。如果您遇到的問題不在清單中，請使用此頁面底部的 [Questions?](#) 此頁面底部的 [評論?](#) 連結，用於提交意見回饋或聯絡 [AWS Support Support](#)。

我已將電子郵件地址新增為通知聯絡人，但我並未收到電子郵件通知

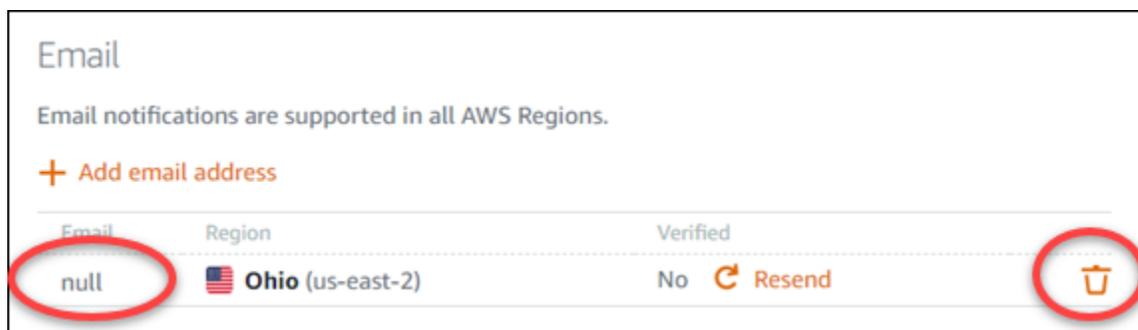
當您在 Lightsail 中將電子郵件地址新增為通知聯絡人時，系統會向該地址傳送驗證要求。驗證要求電子郵件包含一個連結，收件者必須按一下該連結，以確認他們想要接收 Lightsail 通知。在通過驗證之後，通知才會傳送至電子郵件地址。驗證來自 AWS 通知 <no-reply@sns.amazonaws.com>，其主旨為 AWS 通知 - 訂閱確認。簡訊不需要驗證。

如果驗證請求不在收件匣資料夾中，請檢查信箱的垃圾郵件資料夾。如果驗證要求遺失或遭到刪除，請在 Lightsail 主控台和「帳戶」頁面中顯示的通知橫幅中選擇「重新傳送驗證」。



我看到 null 列為我的電子郵件通知聯絡人。

電子郵件地址必須在新增後的 24 小時內進行驗證。如果您在 24 小時內驗證電子郵件失敗，系統會自動將該電子郵件的狀態指定為 `invalid` 並從 Lightsail 中移除。這就是您可能會看到一或多個電子郵件通知聯絡人為 `null` 值的原因。



若要修正這個問題，請移除 `null` 電子郵件通知聯絡人，並再次新增正確的電子郵件地址。請務必在將電子郵件地址新增至 Lightsail 後立即驗證該電子郵件地址。如需詳細資訊，請參閱 [通知](#)。

我沒有收到簡訊通知，或我最近已停止接收簡訊通知

您可能已選擇不接收簡訊通知。您可藉由以 ARRET (法文)、CANCEL、END、OPT-OUT、OPTOUT、QUIT、REMOVE、STOP、TD 或 UNSUBSCRIBE 回應簡訊通知來選擇退出。如果您

選擇不使用行動電話號碼，則必須等待 30 天，才能在 Lightsail 中再次將該行動電話號碼新增為通知聯絡人。

## 疑難排解SSL/TLS憑證

您可能會在使用 Lightsail 負載平衡器時遇到錯誤。此主題可識別常見問題和這些錯誤的解決方法。

在下方選擇最符合您狀況的問題，並依照連結來修正問題。如果您遇到的問題不在清單中，請使用此頁面底部的 Questions? 評論? 本頁底部的連結可提交意見反應或聯絡AWS客戶 Support。

我無法建立憑證。

您可以在帳戶中建立的憑證數量有配 AWS 額。如需詳細資訊，請參閱 [Cer AWS tificate Manager 使用指南](#)中的 [配額](#)。相同的配額也適用於負載平衡器的 Lightsail 憑證。

實際錯誤訊息：Sorry, you've requested too many certificates for your account. (很抱歉，您已為帳戶申請太多憑證。)

我的憑證請求失敗。

如果憑證請求失敗，您可以在負載平衡器管理頁面的 Inbound traffic (傳入流量) 索引標籤上執行 Retry (重試)。

如果仍然無法弄清楚出了什麼問題，請聯絡AWS客戶 Support。

我的網域顯示為無效。

如果您在驗證網域是否有控制權時遇到問題，請檢查您是否有權存取DNS管理。如果您確實執行了 [這些指示](#)，但仍無法驗證，請聯絡AWS客戶 Support。

# 透過教學課程探索 Lightsail 功能

本節涵蓋下列與 Amazon Lightsail 相關的主題：

## 主題

- [使用 Lightsail 藍圖快速部署應用程式](#)
- [在 Lightsail 上使用 Bitnami 應用程式和堆疊](#)
- [設定和管理執行 WordPress 個體](#)
- [在 Lightsail 上使用多站 WordPress 點管理多個網站](#)
- [使用「讓我們加密」為 Lightsail 資源啟用加密通訊](#)
- [為 Lightsail 執行個體設定 IPv6 網路](#)
- [設定 AWS CLI 供 Lightsail 作業使用](#)
- [在 Lightsail AMP 執行個體上部署 PHP 應用程式](#)
- [啟動並設定視窗伺服器 2016 年執行 Lightsail](#)
- [監控 Lightsail API 活動 AWS CloudTrail](#)
- [建立 HAR 檔案以進 Lightsail 難排解](#)
- [使用 Prometheus 監控系統資源和應用程式](#)
- [使用 scp 在 Lightsail 上的 Linux 執行個體之間傳輸檔案](#)
- [透過對等互連功能將 Lightsail 與其他 AWS 服務整合 VPC](#)
- [使用建立 Lightsail 資源 AWS CloudFormation](#)
- [探索應用程式部署的 Lightsail 資源](#)

請按照每個類別中提供的連結存取有關 Lightsail 各個層面的 step-by-step 指南、最佳做法以及其他資訊。

每個主題都涵蓋部署應用程式、設定網路、監視和記錄、與其他 AWS 服務整合等資訊。透過探索本節，您可以了解如何有效利用 Lightsail、運用其與其他 AWS 服務的整合，以及存取豐富的教學課程和資源，以增強您的雲端運算體驗。

## 使用 Lightsail 藍圖快速部署應用程式

使用下列快速入門指南開始使用 Lightsail 藍圖。在 Lightsail 中，藍圖是隨作業系統和應用程式預先封裝的虛擬映像。應用程式包括 WordPress, WordPress 多站點, cPanel & WHM PrestaShop, Drupal 的, 鬼, 的 Joomla! , Magento 的, 紅礦LAMP, 尼金克斯 (LEMP), 和 Node.js

### 主題

- [在 Lightsail 上啟動並設定 AlmaLinux 實體](#)
- [在 Lightsail 上使用 cPanel 和 WHM 託管網站、電子郵件和服務](#)
- [在 Lightsail 上設置和自定義您的 Drupal 網站](#)
- [在 Lightsail 上部署幽靈網站](#)
- [在 Lightsail 上設定和設定 GitLab CE 執行個體](#)
- [開始使用! 關於 Lightsail](#)
- [在 Lightsail 上設置燈具堆疊](#)
- [在 Lightsail 上設置和配置](#)
- [在 Lightsail 上部署和管理 Nginx 網路伺服器](#)
- [在 Lightsail 上開始使用 Node.js](#)
- [在 Lightsail 上部署一個託管堆疊](#)
- [在 Lightsail 上建立 PrestaShop 網站](#)
- [在 Lightsail 上設定和保護紅礦執行個體](#)
- [WordPress 在 Lightsail 上啟動和設定](#)
- [在 Lightsail 上設置 WordPress 多站點](#)

## 在 Lightsail 上啟動並設定 AlmaLinux 實體

本快速入門指南提供在 Amazon Lightsail 平台上建立和設定 AlmaLinux 執行個體的指 step-by-step 示。本主題涵蓋關鍵步驟，包括選擇您的執行個體位置和計劃、設定網路和安全性，以及從 CentOS 轉換為。AlmaLinux 透過執行下列步驟，您可以快速地在 Lightsail 上啟動並 AlmaLinux 執行您的執行個體。

### 主題

- [必要條件](#)
- [在 Light AlmaLinux sail 中建立實體](#)

- [\(選擇性\) 其他設定](#)
- [將數據從 CentOS 遷移到 Light AlmaLinux sail](#)

## 必要條件

- 如果您是新 AWS 客戶，請先完成設定先決條件，然後再開始使用 Amazon Lightsail。如需詳細資訊，請參閱 [設定 AWS 帳戶和管理使 Lightsail](#)。
- 閱讀 [AlmaLinuxWiki](#) 網站上的 AlmaLinux 文件。

## 在 Light AlmaLinux sail 中建立實體

請完成下列程序，以使用 [Lightsail 主控台](#) 建立 AlmaLinux 執行個體。

1. 登入主 [Lightsail 台](#)。
2. 在首頁上選擇 Create instance (建立執行個體)。
3. 選取執行個體的位置 (AWS 區域 和可用區域)。選擇最接近您實體位置的位置 AWS 區域，以減少延遲。

選擇 [變更您的可用區域]，在其他位置建立執行個體。

4. 選擇 Linux 平台。
5. 選擇「僅限作業系統 (OS)」，然後挑選 AlmaLinux 藍圖。

### Instance location [Info](#)

 You are creating this instance in **Virginia, Zone A** (us-east-1a)  
[Change AWS Region and Availability Zone](#)

### Pick your instance image [Info](#)

#### Select a platform

 **Linux/Unix**  
28 blueprints

 **Microsoft Windows**  
6 blueprints

#### Select a blueprint

Apps + OS

Operating System (OS) only

<input type="radio"/>  <b>Amazon Linux 2023</b> 2023.4.20240528.0	<input type="radio"/>  <b>Amazon Linux 2</b> 2.0.20240521.0	<input type="radio"/>  <b>Ubuntu</b> 22.04 LTS	<input type="radio"/>  <b>Ubuntu</b> 20.04 LTS
<input type="radio"/>  <b>Debian</b> 12.5	<input type="radio"/>  <b>Debian</b> 11.9	<input type="radio"/>  <b>Debian</b> 10.8	<input type="radio"/>  <b>FreeBSD</b> 13.2
<input type="radio"/>  <b>openSUSE</b> 15.5	<input checked="" type="radio"/>  <b>AlmaLinux</b> 9.3	<input type="radio"/>  <b>CentOS</b> CS9-20230110	<input type="radio"/>  <b>CentOS</b> 7 2009-01

6. 或者，您可以：

- 選取 [新增啟動指令碼]，新增將在執行個體首次啟動時在執行個體上執行的 shell 指令碼。如需詳細資訊，請參閱 [在 Lightsail 中使用啟動指令碼設定 Linux/Unix 執行個體](#)。
  - 選取 [變更安全殼層 key pair]，變更執行個體的安全殼層 key pair。如需詳細資訊，請參閱 [設定適用於 Lightsail 的 SSH 按鍵](#)。
  - 選取啟用自動快照，為您的執行個體和連結磁碟啟用自動快照。如需詳細資訊，請參閱 [設定 Lightsail 執行個體和磁碟的自動快照](#)。
7. 選擇您的執行個體方案。您可以選擇執行個體使用雙堆疊 (IPv4 和 IPv6)，還是僅使用 IPv6 網路功能。AlmaLinux 藍圖同時支援雙堆疊和僅限 IPv6 的服務包。若要進一步瞭解僅限 IPv6 網路，請參閱 [為 Lightsail 執行個體設定僅限 IPv4 的網路](#)

### Choose your instance plan [Info](#)

#### Select a network type [Info](#)

**Dual-stack** Recommended  
 For workloads that require full network compatibility. Includes a public IPv4 and a public IPv6 address.

**IPv6-only**  
 For workloads that do not require a public IPv4 address. Includes a public IPv6 address.

#### Select a size

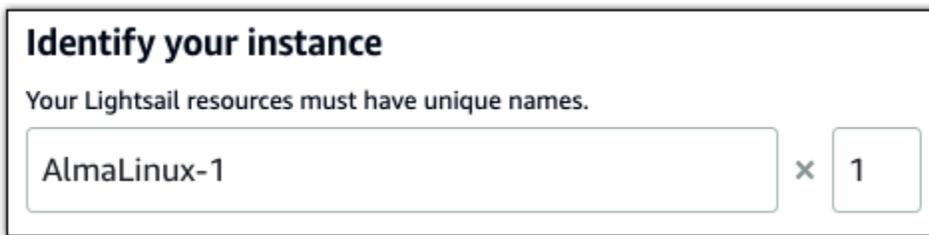
Sort by Price per month ▾

<input checked="" type="radio"/> <b>\$5</b> USD per month <hr/> 512 MB Memory 2 vCPUs Processing 20 GB SSD Storage 1 TB Transfer <span style="background-color: #007bff; color: white; padding: 2px 5px; font-weight: bold;">First 3 months free</span>	<input type="radio"/> <b>\$7</b> USD per month <hr/> 1 GB Memory 2 vCPUs Processing 40 GB SSD Storage 2 TB Transfer <span style="background-color: #007bff; color: white; padding: 2px 5px; font-weight: bold;">First 3 months free</span>	<input type="radio"/> <b>\$12</b> USD per month <hr/> 2 GB Memory 2 vCPUs Processing 60 GB SSD Storage 3 TB Transfer <span style="background-color: #007bff; color: white; padding: 2px 5px; font-weight: bold;">First 3 months free</span>	<input type="radio"/> <b>\$24</b> USD per month <hr/> 4 GB Memory 2 vCPUs Processing 80 GB SSD Storage 4 TB Transfer
<input type="radio"/> <b>\$44</b> USD per month <hr/> 8 GB Memory 2 vCPUs Processing 160 GB SSD Storage 5 TB Transfer	<input type="radio"/> <b>\$84</b> USD per month <hr/> 16 GB Memory 4 vCPUs Processing 320 GB SSD Storage 6 TB Transfer	<input type="radio"/> <b>\$164</b> USD per month <hr/> 32 GB Memory 8 vCPUs Processing 640 GB SSD Storage 7 TB Transfer	<input type="radio"/> <b>\$384</b> <span style="color: #007bff; font-weight: bold;">New</span> USD per month <hr/> 64 GB Memory 16 vCPUs Processing 1,280 GB SSD Storage 8 TB Transfer <span style="background-color: #28a745; color: white; padding: 2px 5px; font-weight: bold;">Largest plan</span>

## 8. 輸入您執行個體的名稱。

資源名稱：

- 每個 Lightsail 帳戶 AWS 區域 中的每個項目都必須是唯一的。
- 必須包含 2 至 255 個字元。
- 開頭和結尾必須是英數字元或數字。
- 可以包含英數字元、數字、句點、破折號和底線。



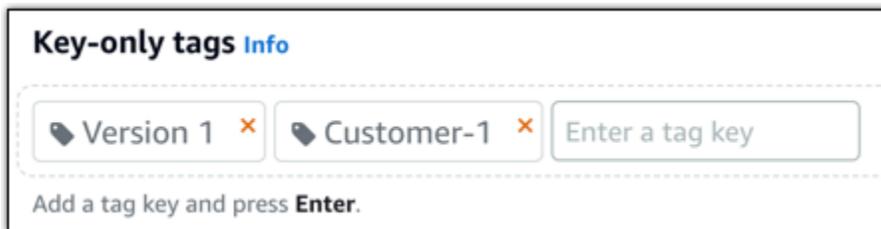
**Identify your instance**

Your Lightsail resources must have unique names.

AlmaLinux-1 x 1

9. 選擇下列其中一個選項以新增標籤至您的執行個體：

- 新增僅索引鍵標籤。在標籤索引鍵文字方塊中輸入新的標籤，接著按 Enter (輸入)。選擇 X 移除任何您不想保留的標籤。

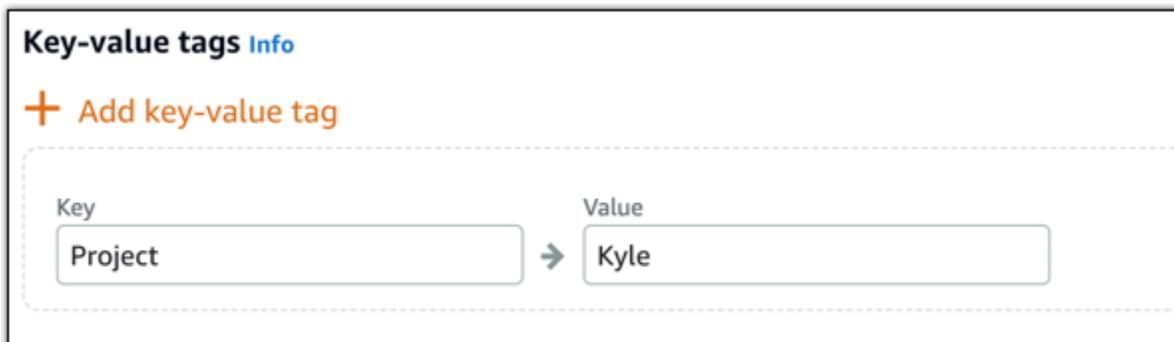


**Key-only tags** Info

Version 1 x Customer-1 x Enter a tag key

Add a tag key and press **Enter**.

- Create a key-value tag (建立索引鍵值標籤)，接著將索引鍵輸入 Key (索引鍵) 文字方塊，將值輸入 Value (值) 文字方塊。索引鍵值標籤一次只能新增一個。選擇新增索引鍵值標籤以新增其他索引鍵值標籤，或選擇 X 移除任何您不想保留的標籤。



**Key-value tags** Info

+ Add key-value tag

Key Value

Project → Kyle

如需有關僅鍵值和鍵值標籤的更多資訊，請參閱。[使用標籤組織和篩選 Lightsail 資源](#)

10. 選擇 建立執行個體。

只需幾分鐘，您的 Lightsail 執行個體就緒，您就可以連線到該執行個體。

### (選擇性) 其他設定

執行個體在 Lightsail 上啟動並 AlmaLinux 執行之後，您應採取以下幾個步驟來開始使用：

- 將靜態 IP 位址附加至您的執行個體 — 每當您停止並啟動執行個體時，連接到執行個體的預設動態公有 IP 位址都會變更。建立靜態 IP 地址並將其連接到執行個體，以防止公有 IP 地址變更。接著，使用網域名稱搭配執行個體時，您不必在每次停止和啟動執行個體時更新網域的 DNS 記錄。您可以將一個靜態 IP 連接至一個執行個體。

在執行個體管理頁面的 [網路功能] 索引標籤下，選擇 [建立靜態 IP]，然後依照頁面上的指示操作。如需詳細資訊，請參閱 [建立靜態 IP 並將其附加至您的 Lightsail 執行個體](#)。

- 在 Lightsail 註冊中註冊網域，並在 Lightsail 中管理網域名稱。Lightsail 使用 Amazon Route 53，這是一種高可用性和可擴展的網域名稱系統 (DNS) 網路服務，為您註冊網域。註冊網域之後，您可以將網域指派給 Lightsail 資源或管理該網域的 DNS 記錄。如需詳細資訊，請參閱 [為您的網站註冊和管理 Lightsail](#)。
- 將您的網域名稱對應至執行個體 — 若要將網域名稱對應至執行個體，請將記錄新增至網域的網域名稱系統 (DNS)。example.com DNS 記錄通常會在您註冊網域的註冊商處進行管理和託管。不過，我們建議您將網域 DNS 記錄的管理權限轉移至 Lightsail，以便您可以使用 Lightsail 主控台進行管理。

在 Lightsail 主控台首頁的 [網域與 DNS] 區段上，選擇 [建立 DNS 區域]，然後依照頁面上的指示進行。如需詳細資訊，請參閱 [建立 DNS 區域以管理 Lightsail 執行個體的網域記錄](#)。

- 建立執行個體的快照 — 快照是系統磁碟的副本以及執行個體的原始設定。快照包含的資訊有記憶體、CPU、磁碟大小和資料傳輸率。您可以使用快照做為新執行個體的基準，或做為資料備份。

在執行個體管理頁面的 Snapshot (快照) 索引標籤下方，輸入快照的名稱，接著選擇 Create snapshot (建立快照)。如需詳細資訊，請參閱 [使用快照備份 Linux/UniLightsail 執行個體](#)。

要了解如何從 CentOS 轉移到 AlmaLinux，請繼續下一個主題：[將數據從 CentOS 遷移到 Light AlmaLinux sail](#)。

## 將數據從 CentOS 遷移到 Light AlmaLinux sail

從 CentOS 遷移到 AlmaLinux 是一個直接的過程，您可以通過它將 Lightsail 中的數據從一個實例移動到另一個實例。本主題概述兩個可用於移轉資料的選項。

如需詳細資訊，請參 AlmaLinux 閱 [AlmaLinux Wiki](#) 網站上的文件。

### 內容

- [必要條件](#)
- [\(選擇性\) 使用安全副本 \(scp\) 在執行個體之間傳輸檔案](#)

- [\( 選擇性 \) 將區塊儲存磁碟從 CentOS 執行個體移至執行個體 AlmaLinux](#)

### 必要條件

- 如果您尚未建立，請建立 AlmaLinux Lightsail 實體。如需詳細資訊，請參閱 [在 Lightsail 上啟動並設定 AlmaLinux 實體](#)。
- 建立您計劃移至執行個 AlmaLinux 體的磁碟快照。如需詳細資訊，請參閱 [建立 Lightsail 區塊儲存磁碟快照以進行備份或基準](#)。

### (選擇性) 使用安全副本 (scp) 在執行個體之間傳輸檔案

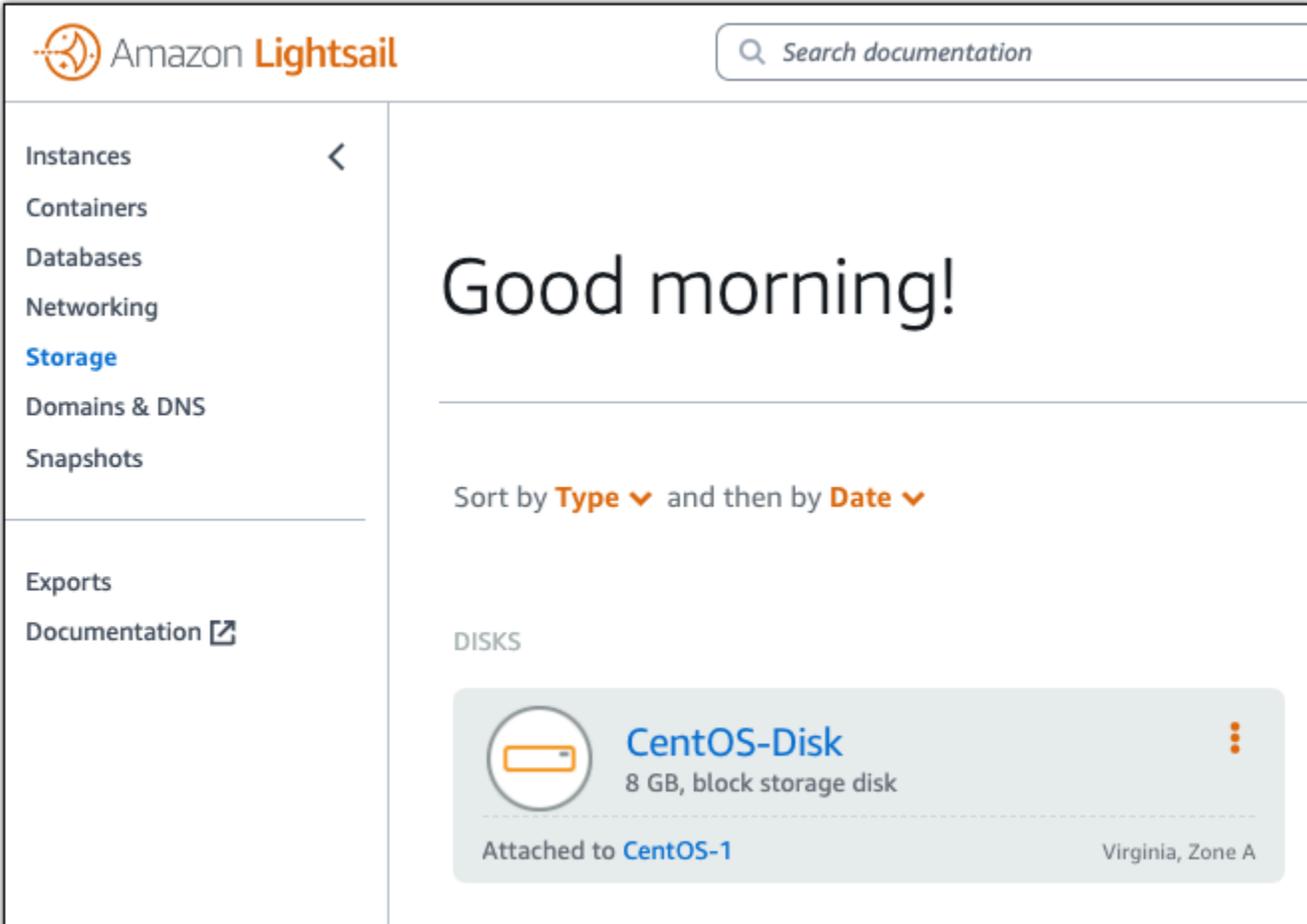
您可以使用 Linux 中的安全複製指令，安全地將檔案從 CentOS AlmaLinux 執行個體傳輸到新的執行個體。如需詳細資訊，請參閱 [使用 scp 在 Lightsail 上的 Linux 執行個體之間傳輸檔案](#)。

### ( 選擇性 ) 將區塊儲存磁碟從 CentOS 執行個體移至執行個體 AlmaLinux

請按照以下程序將第二個區塊儲存磁碟從 CentOS 執行個體套件組合移至該 AlmaLinux 套裝軟體。您無法卸離執行個體的開機磁碟區磁碟，也就是包含作業系統的磁碟。將磁碟連接至 AlmaLinux 執行個體後，您必須連線至該執行個體並掛接磁碟。如需詳細資訊，請參閱 [使用 Lightsail 區塊儲存磁碟擴充儲存空間和效能](#)。

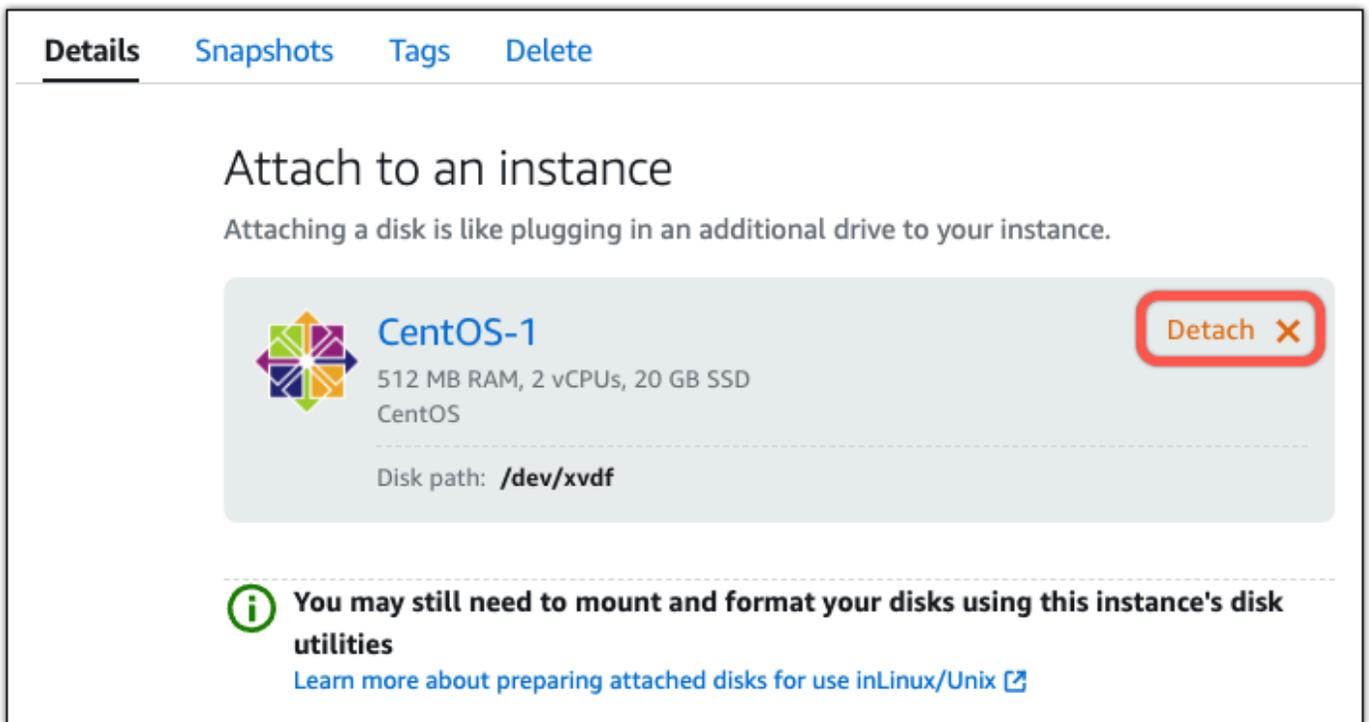
如果你的 CentOS 執行個體正在執行，你必須先停止它才能卸離磁碟。如需詳細資訊，請參閱[停止執行中的執行個體](#)。

1. 在 Lightsail 主控台的「儲存空間」區段中，選取您要從 CentOS 執行個體中分離的磁碟。



The screenshot shows the Amazon Lightsail console interface. On the left is a navigation sidebar with categories: Instances, Containers, Databases, Networking, Storage (highlighted in blue), Domains & DNS, and Snapshots. Below these are Exports and Documentation. The main content area features a search bar at the top right with the text 'Search documentation'. Below the search bar is a large 'Good morning!' greeting. Underneath, there are sorting instructions: 'Sort by Type ▼ and then by Date ▼'. A section titled 'DISKS' contains a single disk entry: 'CentOS-Disk', which is an 8 GB block storage disk. It is attached to an instance named 'CentOS-1' and is located in the Virginia, Zone A region. A three-dot menu icon is visible to the right of the disk name.

2. 在「詳細資料」頁籤上，選擇「卸離」



**Details** Snapshots Tags Delete

## Attach to an instance

Attaching a disk is like plugging in an additional drive to your instance.

 **CentOS-1** Detach ✕

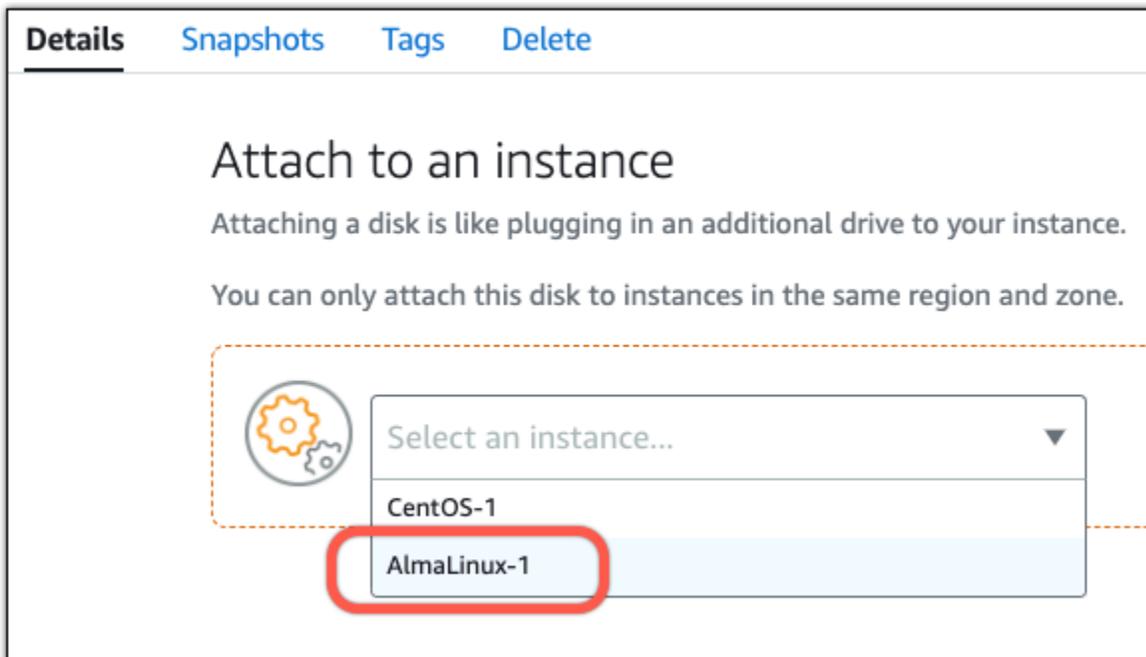
512 MB RAM, 2 vCPUs, 20 GB SSD  
CentOS

---

Disk path: `/dev/xvdf`

**i** You may still need to mount and format your disks using this instance's disk utilities  
[Learn more about preparing attached disks for use in Linux/Unix](#)

3. 在磁碟詳細資訊頁面中，選擇 [連接至執行個體] 下拉式功能表。然後選擇 AlmaLinux 執行個體的名稱。



**Details** Snapshots Tags Delete

## Attach to an instance

Attaching a disk is like plugging in an additional drive to your instance.

You can only attach this disk to instances in the same region and zone.

 Select an instance... ▼

- CentOS-1
- AlmaLinux-1**

4. 選擇 Attach (連接)。
5. (選擇性) 您可能需要連線至 AlmaLinux 執行個體並掛接磁碟，才能存取其資料。如需詳細資訊，請參閱 [Connect 到執行個體以格式化和掛接磁碟](#)。

**⚠ Warning**

上面的鏈接提供了有關如何安裝和格式化附加磁盤的說明。請勿格式化您連接到 AlmaLinux 執行個體的磁碟。格式化它將永久刪除存儲在磁盤上的所有信息。

## 在 Lightsail 上使用 cPanel 和 WHM 託管網站、電子郵件和服務

在您的 cPanel 和 WHM 實例在 Amazon Lightsail 上啟動並運行後，您應該採取以下幾個步驟來開始使用。

**⚠ Important**

您的 cPanel & WHM 執行個體包含 15 天的試用授權。15 天後，您必須從 cPanel 購買授權，以繼續使用 cPanel & WHM。若您打算購買授權，請在購買授權之前完成本指南的步驟 1-7。

### 內容

- [步驟 1：變更根使用者密碼](#)
- [步驟 2：將靜態 IP 地址連接至 cPanel & WHM 執行個體](#)
- [步驟 3：首次登入 Web 主機管理員](#)
- [步驟 4：變更 cPanel & WHM 執行個體的主機名稱和 IP 地址](#)
- [步驟 5：將網域名稱對應至 cPanel & WHM 執行個體](#)
- [步驟 6：編輯執行個體的防火牆](#)
- [步驟 7：從您的執行個體移除 SMTP 限制](#)
- [步驟 8：閱讀 cPanel & WHM 文件並取得支援](#)
- [步驟 9：購買 cPanel & WHM 的授權](#)
- [步驟 10：建立 cPanel & WHM 執行個體的快照](#)

### 步驟 1：變更根使用者密碼

完成以下程序以變更 cPanel 執行個體上的根使用者密碼。您將於稍後使用根使用者和密碼登入 Web 主機管理員 (WHM) 主控台。

1. 在執行個體管理頁面的 Connect (連接) 索引標籤下，選擇 Connect using SSH (使用 SSH 連接)。

2. 連接後，請輸入以下命令以變更根使用者密碼：

```
sudo passwd
```

3. 輸入高強度密碼並再次輸入以確認密碼。

#### Note

您的密碼不應包含字典單字，且字數應大於 7 個字元。若您未遵循這些準則，則會收到 BAD PASSWORD 警告。

請記住此密碼，因為您稍後將依照本指南使用此密碼登入 WHM 主控台。

## 步驟 2：將靜態 IP 地址連接至 cPanel & WHM 執行個體

連接到執行個體的預設動態公有 IP 地址會在每次停止和啟動執行個體時變更。建立靜態 IP 地址並將其連接到執行個體，以防止公有 IP 地址變更。接著，使用網域名稱搭配執行個體時，您不必在每次停止和啟動執行個體時更新網域的 DNS 記錄。或者，若執行個體失敗，您可以從備份還原執行個體，並將靜態 IP 重新指派給新的執行個體。您可以將一個靜態 IP 連接至一個執行個體。

#### Important

從 cPanel 購買授權時，您必須指定 cPanel & WHM 執行個體的公有 IP 地址。您購買的授權會與該 IP 地址相關聯。因此，若您計劃從 cPanel 購買授權，則必須將靜態 IP 連接至 cPanel & WHM 執行個體。當您從 cPanel 購買授權時，請指定靜態 IP，並且只要您打算將 cPanel 和 WHM 授權與 Lightsail 執行個體搭配使用，就可以保留靜態 IP。若您稍後需要將授權轉移至另一個 IP 地址，可以提交請求至 cPanel。如需詳細資訊，請參閱 WHM 文件中的[轉移授權](#)。

在執行個體管理頁面的 Networking (聯網) 索引標籤下，選擇 Create static IP (建立靜態 IP)，接著遵循頁面上的說明。

如需詳細資訊，請參閱[建立靜態 IP 並將其附接至執行個體](#)。

## 步驟 3：首次登入 Web 主機管理員

首次登入 WHM 主控台時，請完成以下程序。

1. 開啟 Web 瀏覽器，導覽至以下網址。將 `<StaticIP>` 取代為執行個體的靜態 IP 地址。請務必在地址的結尾處 (即您將與執行個體建立連接的連接埠) 新增 `:2087`。

```
https://<StaticIP>:2087
```

範例：

```
https://192.0.2.0:2087
```

### Important

當導覽至執行個體的 IP 地址和連接埠時，您必須在瀏覽器網址列中包含 `https://`。否則，你會收到錯誤通知，告知您無法造訪該網站。

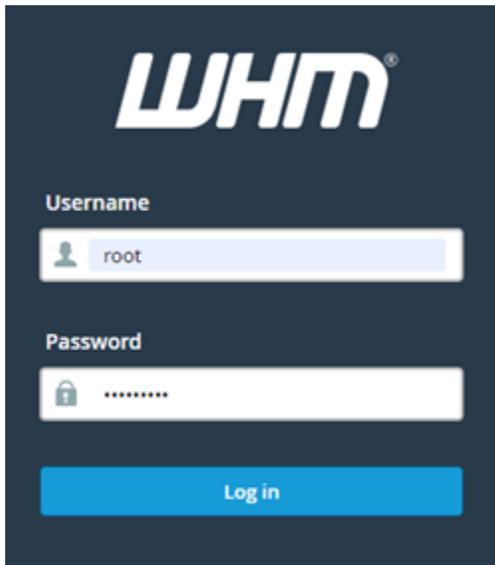
透過連接埠 2087 瀏覽至執行個體的靜態 IP 地址時，若無法建立連線，請檢查您的路由器、VPN 或網際網路服務供應商是否允許透過連接埠 2087 進行 HTTP/HTTPS 連線。若不允許，請嘗試使用不同的網路來連接。

您可能會看到瀏覽器的警告通知，告知您連線並非私有且不安全，或有安全性風險。發生這種情況是因為您的 cPanel 執行個體尚未套用 SSL/TLS 憑證。在瀏覽器視窗中，選擇 **Advanced** (進階)、**Details** (詳細資訊) 或 **More information** (更多資訊)，以檢視可用的選項。然後選擇繼續瀏覽該網站，即使該網站不是私有或安全的網站。

2. 在 Username (使用者名稱) 文字方塊中輸入 `root`。
3. 在 Password (密碼) 文字方塊中輸入根使用者密碼。

這是您稍早在本指南的 [步驟 1：變更根使用者密碼](#) 一節中指定的密碼。

4. 選擇 Log in (登入)。

The image shows a WHM login interface on a dark blue background. At the top is the 'WHM' logo in white. Below it, there are two input fields: 'Username' with a person icon and the text 'root', and 'Password' with a lock icon and seven dots. A blue 'Log in' button is positioned at the bottom of the form.

WHM<sup>®</sup>

Username

root

Password

.....

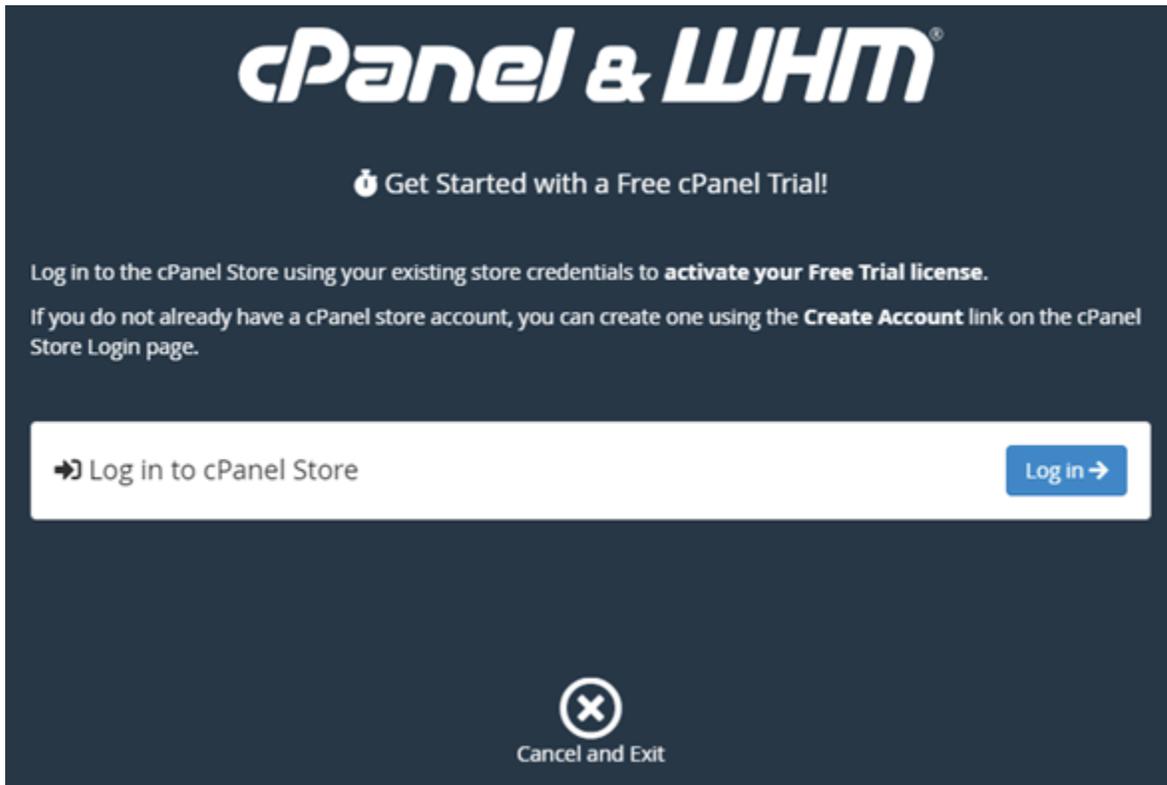
Log in

5. 閱讀 cPanel & WHM 條款，若您願意繼續，請選擇 Agree to all (同意全部)。



6. 在 Get started with a Free cPanel Trial (開始使用免費的 cPanel 試用版) 頁面，請選擇 Log in (登入) 以登入 cPanel 存放區。

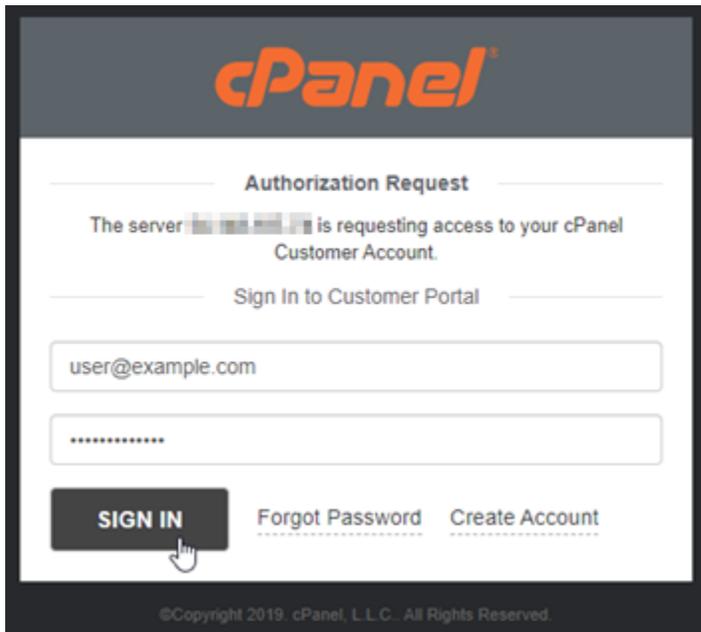
您必須登入 cPanel 存放區，才能將試用授權和您的帳戶建立關聯。若您沒有 cPanel 存放區帳戶，仍應該選擇 Log in (登入)，您將會看到建立 cPanel 存放區帳戶的選項。



7. 在顯示的 Authorization Request (授權請求) 頁面中，輸入電子郵件地址或使用者名稱，以及 cPanel 存放區帳戶密碼。

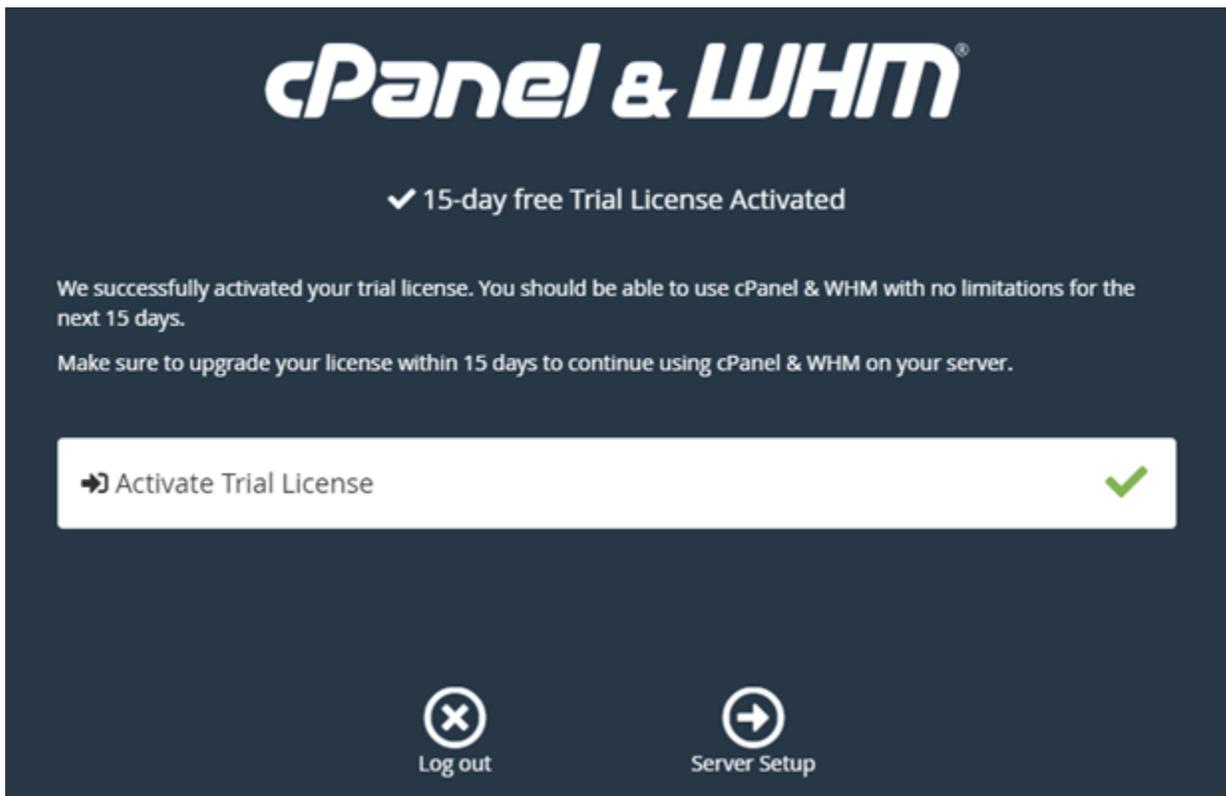
若您還沒有 cPanel 存放區帳戶，請選擇 Create Account (建立帳戶) 並依照提示來建立新的 cPanel 存放區帳戶。您會收到輸入電子郵件地址的請求以及一封電子郵件，幫助您設定 cPanel 存放區帳戶密碼。我們建議您使用新的瀏覽器索引標籤來設定 cPanel 存放區帳戶密碼。設定密碼後，您可以關閉該索引標籤並返回執行個體以授權您的帳戶，並繼續執行此程序的下一個步驟。

8. 選擇 Sign In (登入)。

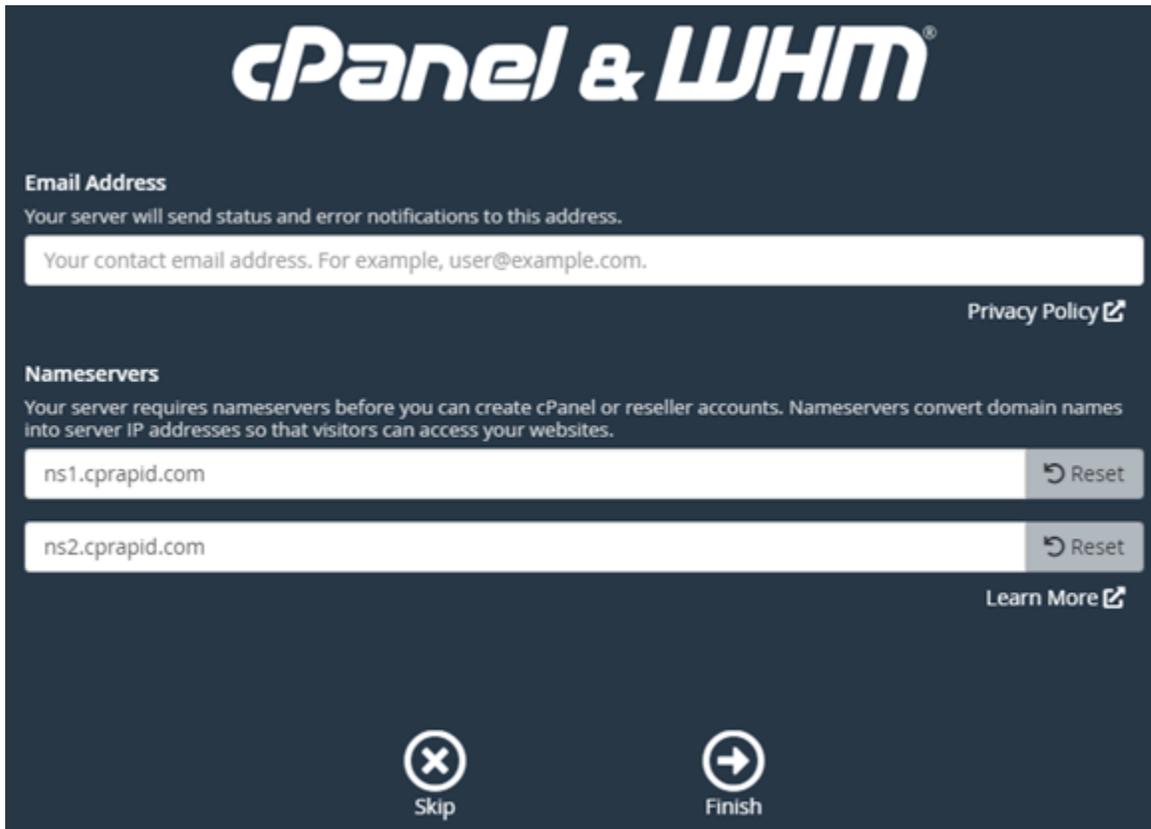


登入後，您的 cPanel & WHM 執行個體將獲得與 cPanel 存放區帳戶相關聯的 15 天試用授權。前往 cPanel 存放區中的 [Manage Licenses](#) (管理授權) 頁面，以查看已核發的授權，包括試用授權。

9. 請選擇 Server Setup (伺服器設定) 以繼續。



10. 在電子郵件地址和名稱伺服器頁面中，請選擇 Skip (略過)。這些可於稍後設定。

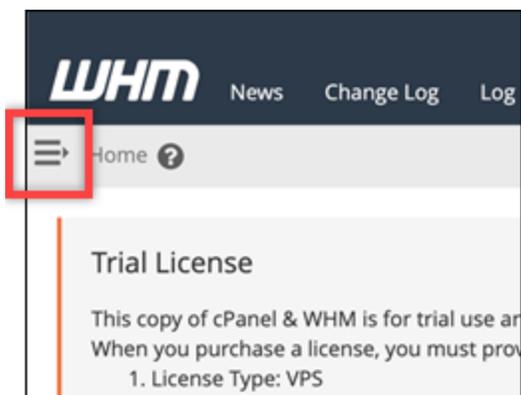


在 WHM 主控台中，您可以管理 cPanel 的設定和功能。

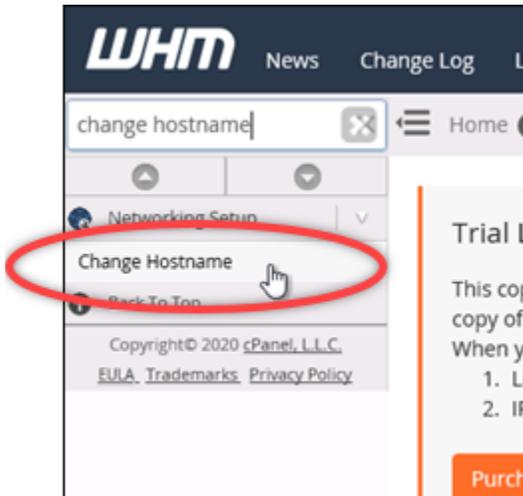
#### 步驟 4：變更 cPanel & WHM 執行個體的主機名稱和 IP 地址

完成以下步驟來變更執行個體的主機名稱，這樣您就不必使用其公有 IP 地址來存取 WHM 主控台。您也應該將執行個體的 IP 地址變更為先前在本指南的[步驟 2：將靜態 IP 地址連接至 cPanel & WHM 執行個體](#)一節中連接至執行個體的新靜態 IP 地址。

1. 請選擇 WHM 主控台左上區段的導覽選單圖示。



- 在 WHM 主控台的搜尋文字方塊中輸入 Change hostname，然後在搜尋結果中選擇 Change hostname (變更主機名稱) 選項。



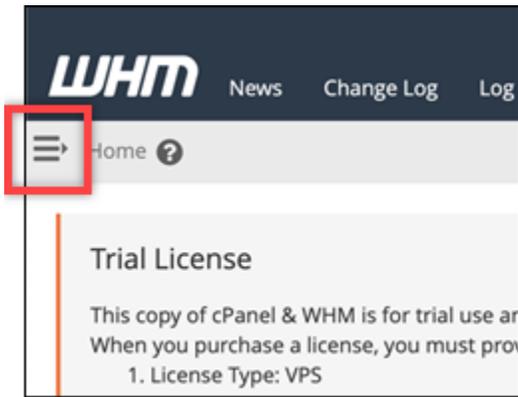
- 在 New hostname (新主機名稱) 文字方塊中，輸入您要用來存取 WHM 主控台的主機名稱。例如輸入 management.example.com 或 administration.example.com。

**Note**

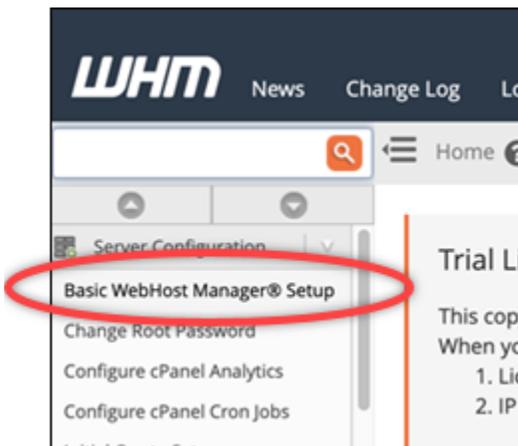
您只能指定子網域作為主機名稱，而且無法指定 whm 或 cpanel 作為子網域。

A screenshot of the 'Change Hostname' form in WHM. The form has a light blue header with the text 'Change Hostname'. Below the header, there's a section for 'Current Hostname' with a text input field containing 'ip-10-10-10-10.us-west-2.compute.internal'. Below that is a section for 'New Hostname:' with a text input field containing 'management.example.com'. At the bottom of the form is a blue 'Change' button.

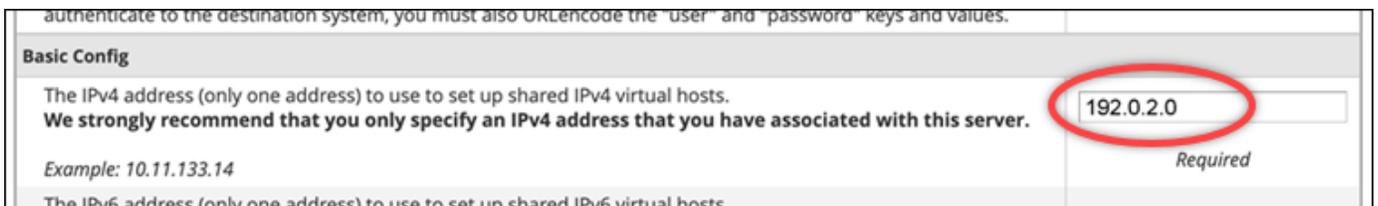
- 選擇 Change (變更)。
- 請選擇 WHM 主控台左上區段的導覽選單圖示。



6. 選擇基本 WebHost 管理員設定。



7. 在 All (全部) 索引標籤下，向下捲動頁面並尋找 Basic Config (基本組態) 區段。
8. 在 IPv4 地址文字方塊中，輸入執行個體的新靜態 IP 地址。如需 IPv6 的相關資訊，請參閱在 [cPanel 執行個體上設定 IPv6](#)。



9. 捲動到頁面底部，然後選擇 Save Changes (儲存變更)。

#### Note

若您收到 Invalid License file (無效授權檔案) 的錯誤訊息，請稍候並等待幾分鐘後再次嘗試變更 IP 地址。

現在執行個體的主機名稱和 IP 地址已變更，但您仍然必須將網域名稱對應至 cPanel & WHM 執行個體。若要執行此操作，您可以在已註冊網域名稱的網域名稱系統 (DNS) 中新增地址 (A) 記錄。A 記錄會將執行個體的主機名稱解析為執行個體的靜態 IP 地址。本指南的下一節將告訴您如何進行這些操作。

## 步驟 5：將網域名稱對應至 cPanel & WHM 執行個體

### Note

您可以將網域對應至 cPanel & WHM 執行個體，該執行個體可用來存取 WHM 主控台。您也可以將 WHM 中對應多個網域，以便您在 WHM 中管理網站。本節說明如何將您的網域對應至 cPanel & WHM 執行個體。如需有關在 WHM 主控台中對應多個網域 (您在建立新帳戶時便會執行這項操作) 的詳細資訊，請參閱 WHM 文件中的[建立新帳戶](#)。

為了將網域名稱 (例如 `management.example.com` 或 `administration.example.com`) 對應至執行個體，您需要將地址 (A) 記錄新增至網域的 DNS。該記錄會將 cPanel & WHM 執行個體的主機名稱對應至執行個體的靜態 IP 地址。您在 A 記錄中指定的子網域必須和您稍早在本指南的[步驟 4：變更 cPanel & WHM 執行個體的主機名稱和 IP 地址](#)一節中指定的主機名稱相符。新增 A 記錄後，您可以使用以下地址存取執行個體的 WHM 主控台，而非使用執行個體的靜態 IP 地址。將 `<InstanceHostName >` 取代為執行個體的主機名稱。

```
https://<InstanceHostName>/whm
```

範例：

```
https://management.example.com/whm
```

DNS 記錄通常會在您註冊網域的註冊商處進行管理和託管。不過，我們建議您將網域 DNS 記錄的管理權限轉移至 Lightsail，以便您可以使用 Lightsail 主控台進行管理。若要這麼做，請登入 Lightsail 主控台。在 Lightsail 主控台首頁上，選擇 [網域和 DNS] 索引標籤，然後選擇 [建立 DNS 區域]。依照頁面上的指示，將您的網域名稱新增至 Lightsail。如需詳細資訊，請參閱[在 Lightsail 中建立 DNS 區域以管理網域的 DNS 記錄](#)。

## 步驟 6：編輯執行個體的防火牆

以下防火牆連接埠在 cPanel & WHM 執行個體上預設為開啟：

- SSH - TCP - 22

- DNS (UDP) - UDP - 53
- DNS (TCP) - TCP - 53
- HTTP - TCP - 80
- HTTPS - TCP - 443
- 自訂 - TCP - 2078
- 自訂 - TCP - 2083
- 自訂 - TCP - 2087
- 自訂 - TCP - 2089

根據您計劃在執行個體上使用的服務和應用程式，您可能需要開啟其他連接埠。例如，針對電子郵件服務開啟連接埠 25、143、465、587、993、995、2096，並針對行事曆服務開啟連接埠 2080、2091。在執行個體管理頁面的 Networking (聯網) 索引標籤下，捲動至頁面的 Firewall (防火牆) 區段，然後選擇 Add rule (新增規則)。請選擇要開啟的應用程式、通訊協定以及連接埠或連接埠範圍。完成時，請選擇 Create (建立)。

如需有關要開啟哪些連接埠的詳細資訊，請參閱 cPanel 文件中的[如何為 cPanel 服務設定防火牆](#)。如需有關在 Lightsail 中編輯執行個體防火牆的詳細資訊，請參閱在[Amazon Lightsail 中新增和編輯執行個體防火牆規則](#)。

## 步驟 7：從您的執行個體移除 SMTP 限制

AWS 封鎖所有 Lightsail 執行個體上連接埠 25 上的輸出流量。若要在連接埠 25 中傳送輸出流量，可以請求移除此限制。如需詳細資訊，請參閱[如何從 Lightsail 執行個體移除連接埠 25 的限制？](#)。

### Important

如果您將 SMTP 設定為使用通訊埠 25、465 或 587，則必須在 Lightsail 主控台的執行個體防火牆中開啟這些連接埠。如需詳細資訊，請參閱在[Amazon Lightsail 中新增和編輯執行個體防火牆規則](#)。

## 步驟 8：閱讀 cPanel & WHM 文件並取得支援

閱讀 cPanel & WHM 文件以了解如何使用 cPanel & WHM 管理網站。如需詳細資訊，請參閱[cPanel & WHM 文件](#)。

若您有關於 cPanel & WHM 的問題或需要支援，您可以使用以下資源與 cPanel 聯絡：

- [cPanel 針對您的安裝進行疑難排解](#)
- [cPanel Discord 頻道](#)

## 步驟 9：購買 cPanel & WHM 的授權

您的 cPanel & WHM 執行個體包含 15 天的試用授權。15 天後，您必須從 cPanel 購買授權，以繼續使用 cPanel & WHM。如需詳細資訊，請參閱 cPanel 文件中的[如何購買 cPanel 授權](#)。

### Important

從 cPanel 購買授權時，您必須指定 cPanel & WHM 執行個體的公有 IP 地址。您購買的授權會與該 IP 地址相關聯。因此，您必須將靜態 IP 連接至 cPanel & WHM 執行個體，如同本指南的[步驟 2：將靜態 IP 地址連接至 cPanel & WHM 執行個體](#)一節中所說明的一樣。當您從 cPanel 購買授權時，請指定靜態 IP，並且只要您打算將 cPanel 和 WHM 授權與 Lightsail 執行個體搭配使用，就可以保留靜態 IP。若您稍後需要將授權轉移至另一個 IP 地址，可以提交請求至 cPanel。如需詳細資訊，請參閱 WHM 文件中的[轉移授權](#)。

## 步驟 10：建立 cPanel & WHM 執行個體的快照

快照是執行個體之系統磁碟和原始組態的複本。快照包含還原執行個體所需的所有資料 (從建立快照的那一刻開始)。您可以使用快照做為新執行個體的基準，或做為資料備份。您可以隨時建立手動快照，或啟用自動快照，讓 Lightsail 為您建立每日快照。

### Note

- 目前一代藍圖的 cPanel 和 WHM 的執行個體快照 AlmaLinux 可以匯出到 Amazon EC2。
- 上一代藍圖 cPanel & WHM for Linux 的執行個體快照此時無法匯出至 Amazon EC2。
- 如果您從快照建立新的執行個體，請在登入 WHM 之前給予執行個體額外的時間來完全啟動 (如[步驟 3](#) 所述)。

在執行個體管理頁面的 Snapshot (快照) 索引標籤下方，輸入快照的名稱，接著選擇 Create snapshot (建立快照)。或者捲動至頁面的 Automatic snapshots (自動快照) 區段，然後選擇切換開關以啟用自動快照。

如需詳細資訊，請參閱[建立 Linux 或 Unix 執行個體的快照和在 Amazon Lightsail 中啟用或停用執行個體或磁碟的自動快照](#)。

## 在 Lightsail 上設置和自定義您的 Drupal 網站

在 Amazon Lightsail 上啟動並運行 Drupal 實例後，您應該採取以下幾個步驟才能開始使用：

### 內容

- [步驟 1：閱讀 Bitnami 文件](#)
- [步驟 2：取得存取 Drupal 管理儀表板所需的預設應用程式密碼](#)
- [步驟 3：將靜態 IP 地址連接至您的執行個體](#)
- [步驟 4：登入 Drupal 網站的管理儀表板](#)
- [步驟 5：將已註冊網域的流量路由至 Drupal 網站](#)
- [步驟 6：為 Drupal 網站設定 HTTPS](#)
- [步驟 7：閱讀 Drupal 文件並繼續設定網站](#)
- [步驟 8：建立執行個體的快照](#)

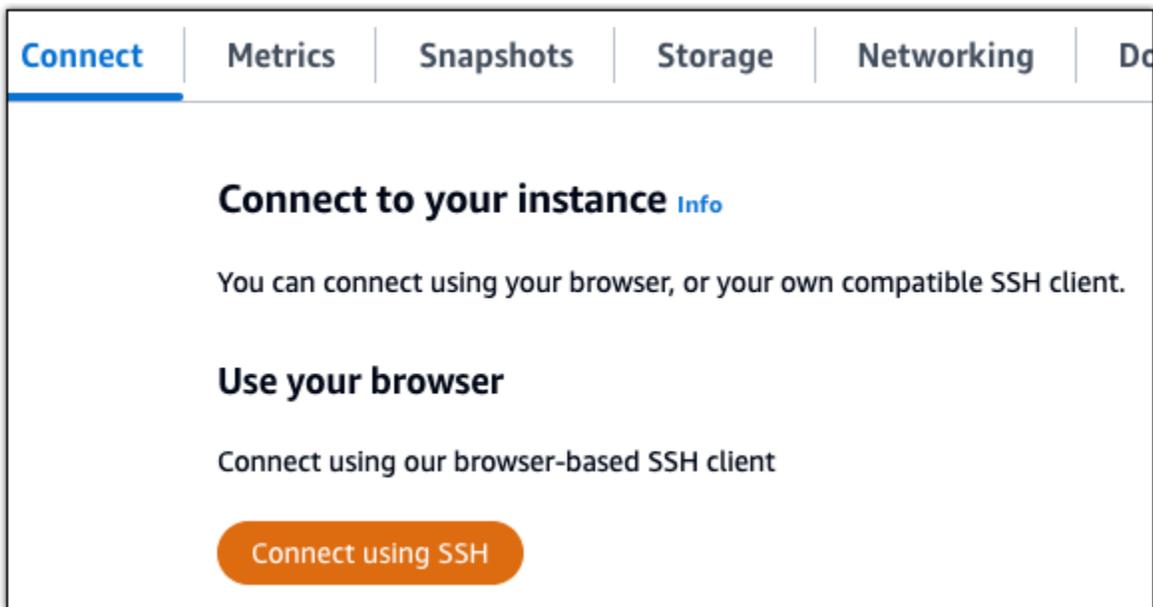
### 步驟 1：閱讀 Bitnami 文件

閱讀 Bitnami 文件以了解如何設定 Drupal 應用程式。如需詳細資訊，請參閱 [Drupal Packaged By Bitnami For AWS 雲端](#)。

### 步驟 2：取得存取 Drupal 管理儀表板所需的預設應用程式密碼

完成下列程序，以取得存取 Drupal 網站管理儀表板所需的預設應用程式密碼。如需詳細資訊，請參閱在 [Amazon Lightsail 中取得 Bitnami 執行個體的應用程式使用者名稱和密碼](#)。

1. 在執行個體管理頁面的 Connect (連接) 索引標籤下，選擇 Connect using SSH (使用 SSH 連接)。



2. 連線後，請輸入下列命令，以取得應用程式密碼：

```
cat $HOME/bitnami_application_password
```

您應該會看到類似於以下範例的回應，其中包含預設應用程式密碼：

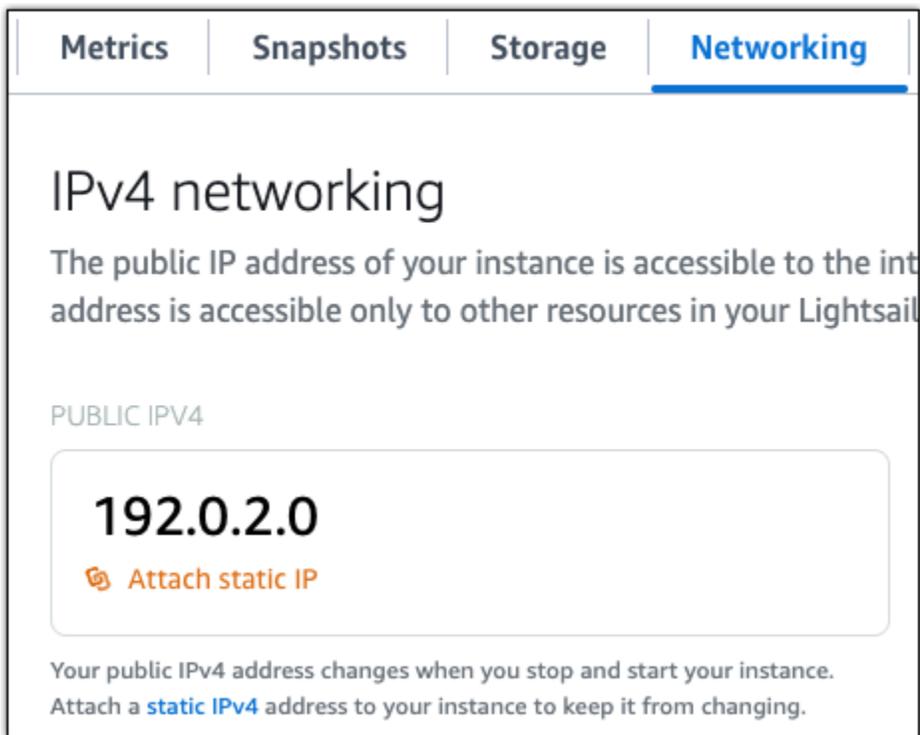
```
bitnami@ip-172-31-52-100:~$ cat bitnami_application_password
JeVN8xDWlCIp
bitnami@ip-172-31-52-100:~$
```



### 步驟 3：將靜態 IP 地址連接至您的執行個體

您第一次建立執行個體時，所指派的公有 IP 地址將會在每次停用和啟用執行個體時變更。您應該建立靜態 IP 地址並將其連接至執行個體，以確保其公有 IP 地址不會變更。當您將註冊的網域名稱 (例如 example.com) 與執行個體搭配使用時，便無須在每次停用或啟用執行個體時更新網域的 DNS 記錄。您可以將一個靜態 IP 連接至一個執行個體。

在執行個體管理頁面的 Networking#(聯網) 索引標籤下，選擇 Create a static IP (建立靜態 IP) 或 Attach static IP (連接靜態 IP)(若您先前已建立可以連接至執行個體的靜態 IP)，然後遵循頁面上的指示執行操作。如需詳細資訊，請參閱[建立靜態 IP 並將其附接至執行個體](#)。



#### 步驟 4：登入 Drupal 網站的管理儀表板

現在您有了預設使用者密碼，請導覽至 Drupal 網站首頁並登入管理儀表板。登入後，您可以開始自訂網站並進行管理級變更。如需詳細資訊，了解能在 Drupal 中執行哪些作業，請參閱本指南後述的[步驟 7：閱讀 Drupal 文件並繼續設定網站](#)章節。

1. 在執行個體管理頁面的 Connect (連接) 索引標籤下，記下執行個體的公有 IP 地址。公有 IP 地址也會顯示在執行個體管理頁面的標頭區段。



2. 瀏覽至執行個體的公有 IP 地址，例如前往 <http://203.0.113.0>。

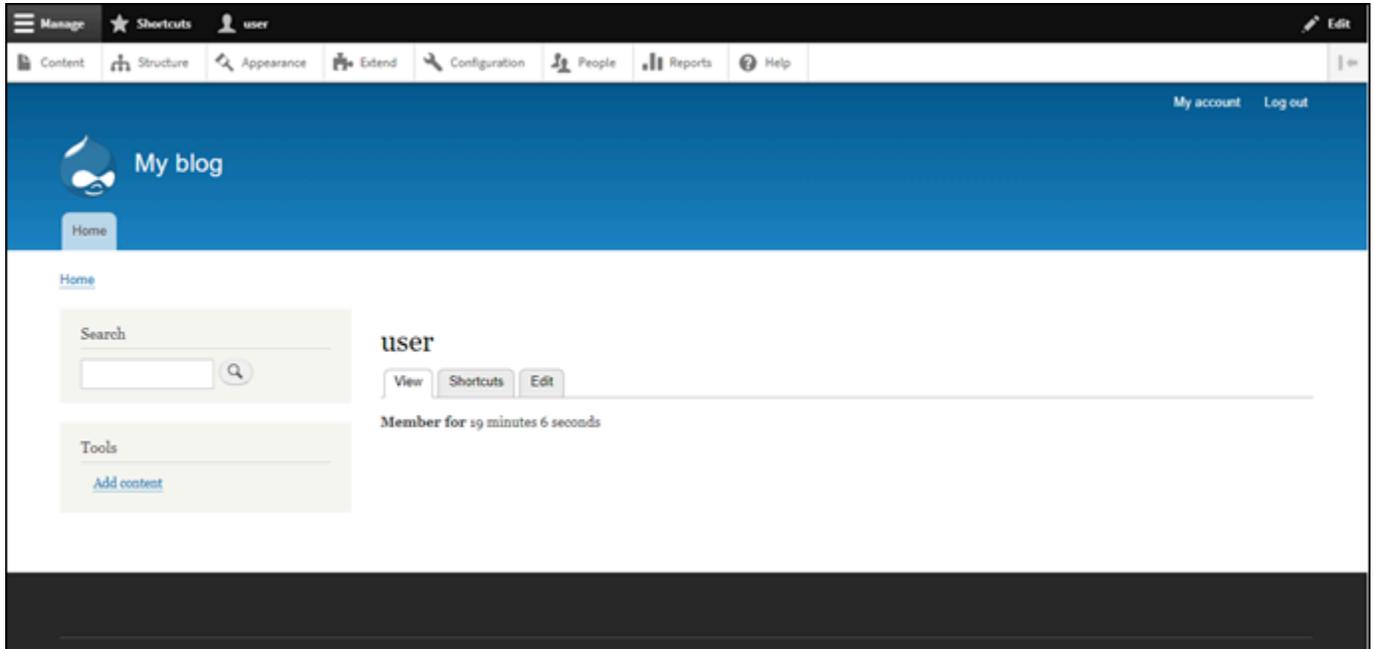
您會看到 Drupal 網站首頁。

3. 選擇 Drupal 網站首頁右下角的 Manage (管理)。

如果未顯示 Manage (管理) 橫幅，您可以透過瀏覽至 <http://<PublicIP>/user/login> 前往登入頁面。將 **<PublicIP>** 取代為您執行個體的公有 IP 地址。

4. 使用先前依本指南指示取得的預設使用者名稱 (user) 和預設密碼登入。

您會看到 Drupal 管理儀表板。



## 步驟 5：將已註冊網域的流量路由至 Drupal 網站

若要將已註冊網域 (例如 example.com) 的流量路由至 Drupal 網站，請新增記錄至網域的網域名稱系統 (DNS)。DNS 記錄通常會在您註冊網域的註冊商處進行管理和託管。不過，我們建議您將網域 DNS 記錄的管理權限轉移至 Lightsail，以便您可以使用 Lightsail 主控台進行管理。

在 Lightsail 主控台首頁的 [網域和 DNS] 索引標籤下，選擇 [建立 DNS 區域]，然後依照頁面上的指示進行。如需詳細資訊，請參閱[在 Lightsail 中建立 DNS 區域以管理網域的 DNS 記錄](#)。

若您瀏覽至您為執行個體設定的網域名稱，則會將您重新導向至 Drupal 網站首頁。接下來，您應該生成並設定 SSL/TLS 憑證，以啟用 Drupal 網站的 HTTPS 連接。如需詳細資訊，請繼續閱讀本指南的下一個章節[步驟 6：為 Drupal 網站設定 HTTPS](#)。

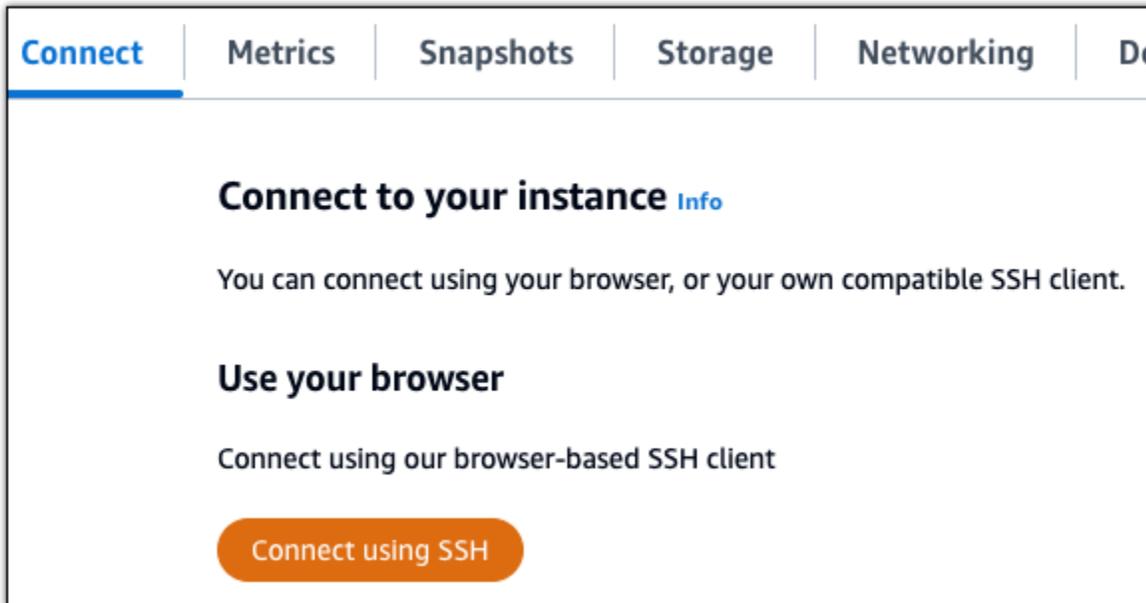
## 步驟 6：為 Drupal 網站設定 HTTPS

完成下列程序，以在 Drupal 網站上設定 HTTPS。這些步驟描述了如何使用 Bitnami HTTPS 組態工具 (bncert-tool)，這是一個命令行工具，用於請求 Let's Encrypt SSL/TLS 憑證。如需詳細資訊，請參閱 Bitnami 文件中的 [Learn About The Bitnami HTTPS Configuration Tool](#) (Bitnami HTTPS 組態工具簡介)。

**⚠ Important**

開始此程序之前，請確認您已將網域設定為將流量路由至 Drupal 執行個體。否則，SSL/TLS 憑證驗證過程會失敗。

1. 在執行個體管理頁面的 **Connect (連接)** 索引標籤下，選擇 **Connect using SSH (使用 SSH 連接)**。



2. 連接後，輸入下列命令，以確認執行個體已安裝 bncert 工具。

```
sudo /opt/bitnami/bncert-tool
```

您應該會看到下列其中一個回應：

- 如果您看見回應中未找到命令，則表示您的執行個體上未安裝 bncert 工具。繼續此程序的下一個步驟，在您的執行個體上安裝 bncert 工具。
  - 如果您在回應中看見 Welcome to the Bitnami HTTPS configuration tool (歡迎使用 Bitnami HTTPS 組態工具)，則您的執行個體上已安裝 bncert 工具。繼續執行此程序的步驟 8。
  - 如果您的執行個體已安裝 bncert 工具一段時間，則您可能會看到說明該工具已有可用更新版本的訊息。選擇下載該版本，然後輸入 `sudo /opt/bitnami/bncert-tool` 命令以再次執行 bncert 工具。繼續執行此程序的步驟 8。
3. 輸入以下命令，以下載 bncert 執行檔案至您的執行個體。

```
wget -O bncert-linux-x64.run https://downloads.bitnami.com/files/bncert/latest/bncert-linux-x64.run
```

- 輸入以下命令，以便為執行個體上的 bncert 工具執行檔案建立目錄。

```
sudo mkdir /opt/bitnami/bncert
```

- 輸入以下命令，以讓 bncert 執行可作為程式執行的檔案。

```
sudo chmod +x /opt/bitnami/bncert/bncert-linux-x64.run
```

- 輸入以下命令，以在您輸入 `sudo /opt/bitnami/bncert-tool` 命令時建立執行 bncert 工具的符號連結。

```
sudo ln -s /opt/bitnami/bncert/bncert-linux-x64.run /opt/bitnami/bncert-tool
```

您現已在執行個體上完成 bncert 工具安裝。

- 輸入下列命令，以執行 bncert 工具。

```
sudo /opt/bitnami/bncert-tool
```

- 輸入主要網域名稱和替代網域名稱，並以空格分隔，如以下範例所示。

如果您的網域未設為將流量路由至執行個體的公有 IP 地址，則 bncert 工具會要求您進行該設定，然後再繼續操作。您的網域必須將流量路由至執行個體的公有 IP 地址，而您需從該地址使用 bncert 工具來在執行個體上啟用 HTTPS。此舉措會確認您擁有該網域，並以此作為憑證的驗證。

```
Welcome to the Bitnami HTTPS Configuration tool.
-----
Domains

Please provide a valid space-separated list of domains for which you wish to
configure your web server.

Domain list []: example.com www.example.com
```

- bncert 工具會詢問您要如何設定網站的重新引導。可用的選項如下：

- Enable HTTP to HTTPS redirection (啟用 HTTP 至 HTTPS 重新引導) - 指定將瀏覽至網站 HTTP 版本 (即 `http://example.com`) 的使用者自動重新引導至 HTTPS 版本 (即 `https://`

example.com)。由於此選項會強制所有訪客使用加密的連線，建議啟用此選項。輸入 Y，並按 Enter 以啟用。

- Enable non-www to www redirection (啟用非 www 至 www 重新引導) - 指定將瀏覽至網域 (即 https://example.com) 頂點的使用者自動重新引導至您網域的 www 子網域 (即 https://www.example.com)。建議啟用此選項。不過，如果您已在搜索引擎工具 (如 Google 的網站管理員工具) 中將網域的頂點指定為您偏好的網站地址，或者如果您的頂點直接指向 IP，且 www 子網域透過 CNAME 記錄參考您的頂點，則您可能需要停用此選項並啟用替代選項 (啟用 www 至非 www 重新引導)。輸入 Y，並按 Enter 以啟用。
- Enable www to non-www redirection (啟用 www 至非 www 重新引導) - 指定將瀏覽至您網域 www 子網域 (即 https://www.example.com) 的使用者自動重新引導至網域的頂點 (即 https://example.com)。如果您已啟用非 www 重新引導至 www，我們建議您停用此選項。輸入 N，並按 Enter (確認) 以停用。

您的選取內容應看起來與下列範例類似。

```
Enable/disable redirections
Please select the redirections you wish to enable or disable on your Bitnami
installation.

Enable HTTP to HTTPS redirection [Y/n]: Y

Enable non-www to www redirection [Y/n]: Y

Enable www to non-www redirection [y/N]: N
```

10. 系統會列出即將進行的變更。輸入 Y，並按 Enter (確認) 以確認並繼續。

```

Changes to perform

The following changes will be performed to your Bitnami installation:

1. Stop web server
2. Configure web server to use a free Let's Encrypt certificate for the domains:
example.com www.example.com
3. Configure a cron job to automatically renew the certificate each month
4. Configure web server name to: example.com
5. Enable HTTP to HTTPS redirection (example: redirect http://example.com to
https://example.com)
6. Enable non-www to www redirection (example: redirect example.com to
www.example.com)
7. Start web server once all changes have been performed

Do you agree to these changes? [Y/n]: Y

```

11. 輸入您的電子郵件地址，以與您的 Let's Encrypt 憑證相關聯，然後按 Enter。

```

Create a free HTTPS certificate with Let's Encrypt

Please provide a valid e-mail address for which to associate your Let's Encrypt
certificate.

Domain list: example.com www.example.com

Server name: example.com

E-mail address []:

```

12. 檢閱 Let's Encrypt 訂閱者協議。輸入 Y，並按 Enter (確認) 以接受該協議並繼續。

```

The Let's Encrypt Subscriber Agreement can be found at:

https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf

Do you agree to the Let's Encrypt Subscriber Agreement? [Y/n]:

```

執行這些動作是為了在執行個體上啟用 HTTPS，包括請求憑證和設定您指定的重新引導。

```

Performing changes to your installation

The Bitnami HTTPS Configuration Tool will perform any necessary actions to your
Bitnami installation. This may take some time, please be patient.

|

```

系統已成功核發並驗證您的憑證，如果您看到類似以下範例的訊息，則表示已成功在執行個體上設定重新引導。

```
Success

The Bitnami HTTPS Configuration Tool succeeded in modifying your installation.

The configuration report is shown below.

Backup files:
* /opt/bitnami/apache2/conf/httpd.conf.back.202005290035
* /opt/bitnami/apache2/conf/bitnami/bitnami-apps-prefix.conf.back.202005290035
* /opt/bitnami/apache2/conf/bitnami/bitnami.conf.back.202005290035

Find more details in the log file:

/tmp/bncert-202005290035.log

If you find any issues, please check Bitnami Support forums at:

https://community.bitnami.com

Press [Enter] to continue:█
```

bncert 工具會在憑證過期前每 80 天執行自動續約一次。如果您要搭配執行個體使用其他網域和子網域，且要為這些網域啟用 HTTPS，請重複上述步驟。

您現已在 Drupal 執行個體上啟用 HTTPS。下次使用您設定的網域瀏覽至 Drupal 網站時，應該會看到您被重新導向至 HTTPS 連接。

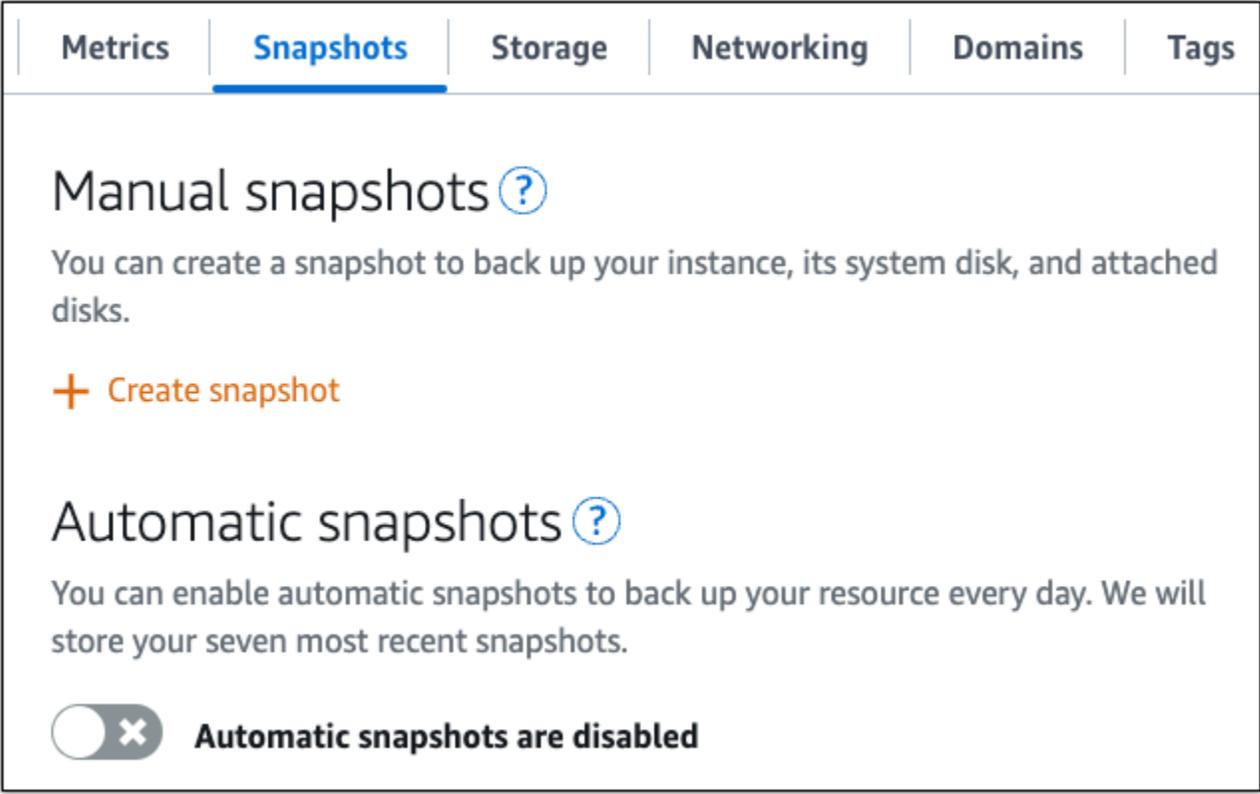
## 步驟 7：閱讀 Drupal 文件並繼續設定網站

閱讀 Drupal 文件以了解如何管理和自訂網站。如需詳細資訊，請參閱 [Drupal documentation](https://www.drupal.org/docs) (《Drupal 文件》)。

## 步驟 8：建立執行個體的快照

按照您想要的方式設定 Drupal 網站後，請定期建立執行個體的快照以作為備份。您可以手動建立快照，或啟用自動快照，讓 Lightsail 為您建立每日快照。若執行個體出現問題，您可以使用快照建立新的替代執行個體。如需詳細資訊，請參閱 [快照](#)。

在執行個體管理頁面的 Snapshot (快照) 索引標籤下，選擇 Create a snapshot (建立快照) 或選擇啟用自動快照。



Metrics | **Snapshots** | Storage | Networking | Domains | Tags

## Manual snapshots ?

You can create a snapshot to back up your instance, its system disk, and attached disks.

[+ Create snapshot](#)

## Automatic snapshots ?

You can enable automatic snapshots to back up your resource every day. We will store your seven most recent snapshots.

**Automatic snapshots are disabled**

如需詳細資訊，請參閱在 Amazon Lightsail 中建立 [Linux 或 Unix 執行個體的快照](#)或在 [Amazon Lightsail](#) 中 [啟用或停用執行個體或磁碟的自動快照](#)。

## 在 Lightsail 上部署幽靈網站

在 Amazon Lightsail 上啟動並執行 Ghost 執行個體後，您應採取以下幾個步驟來開始使用：

### 內容

- [步驟 1：閱讀 Bitnami 文件](#)
- [步驟 2：取得存取 Ghost 管理儀表板所需的預設應用程式密碼](#)
- [步驟 3：將靜態 IP 地址連接至您的執行個體](#)
- [步驟 4：登入 Ghost 網站的管理儀表板](#)
- [步驟 5：將已註冊網域的流量路由至 Ghost 網站](#)
- [步驟 6：為 Ghost 網站設定 HTTPS](#)
- [步驟 7：閱讀 Ghost 文件並繼續設定網站](#)
- [步驟 8：建立執行個體的快照](#)

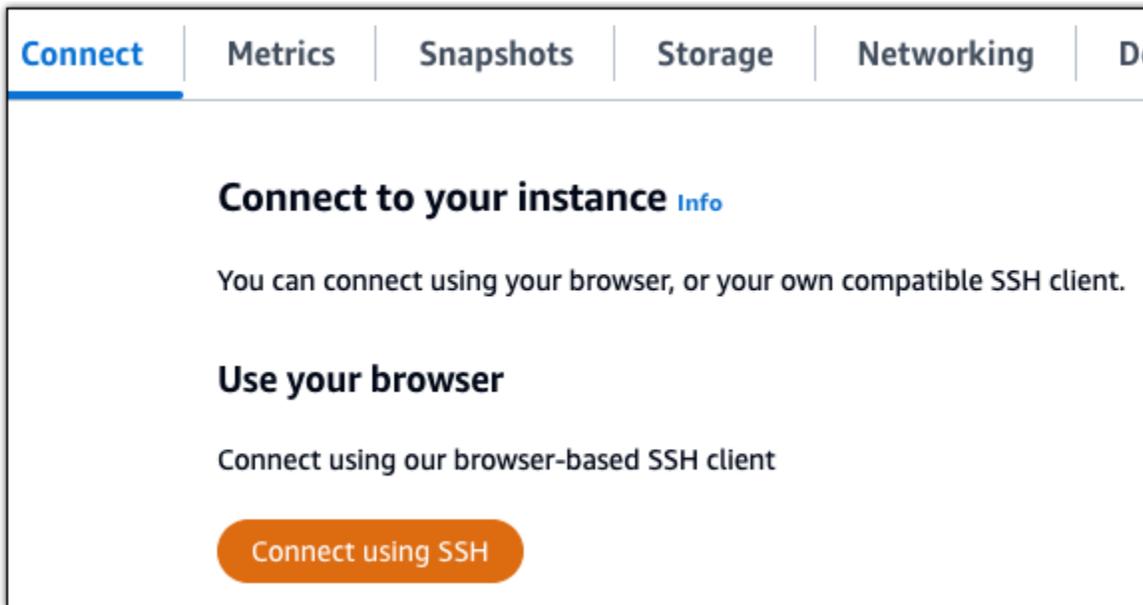
## 步驟 1：閱讀 Bitnami 文件

閱讀 Bitnami 文件以了解如何設定 Ghost 應用程式。如需詳細資訊，請參閱 [Ghost Packaged By Bitnami For AWS 雲端](#)。

## 步驟 2：取得存取 Ghost 管理儀表板所需的預設應用程式密碼

完成下列程序，以取得存取 Ghost 網站管理儀表板所需的預設應用程式密碼。如需詳細資訊，請參閱在 [Amazon Lightsail 中取得 Bitnami 執行個體的應用程式使用者名稱和密碼](#)。

1. 在執行個體管理頁面的 Connect (連接) 索引標籤下，選擇 Connect using SSH (使用 SSH 連接)。



2. 連線後，請輸入下列命令，以取得應用程式密碼：

```
$ cat $HOME/bitnami_application_password
```

您應該會看到類似下列內容的回應，其中包含預設的應用程式密碼：

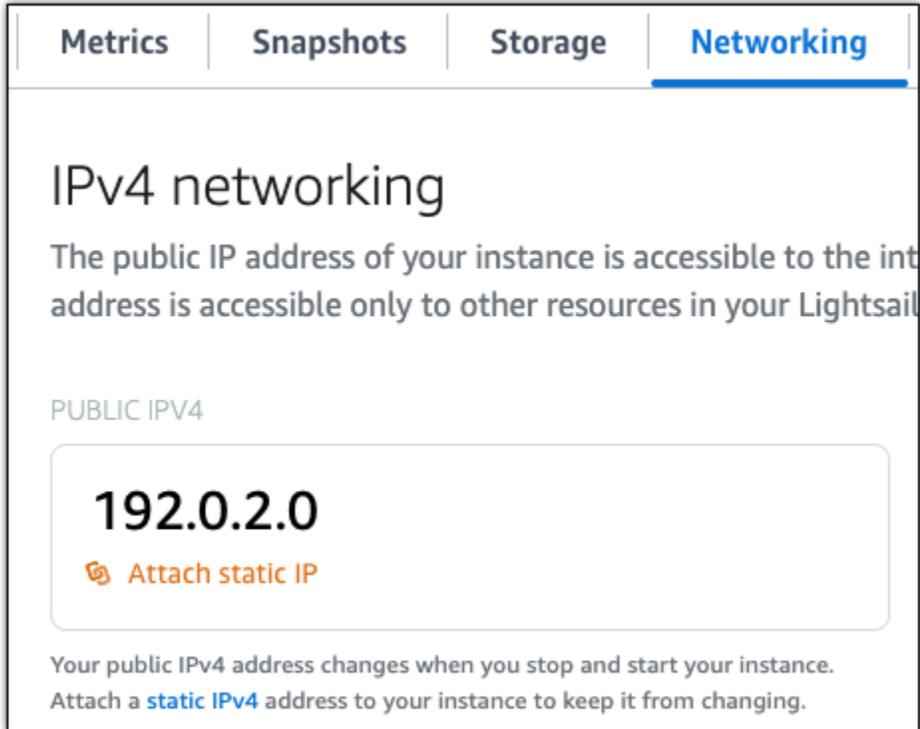
```
bitnami@ip-192-0-2-0:~$ cat $HOME/bitnami_application_password  
wB2Ex@mplEK6
```

## 步驟 3：將靜態 IP 地址連接至您的執行個體

您第一次建立執行個體時，所指派的公有 IP 地址將會在每次停用和啟用執行個體時變更。您應該建立靜態 IP 地址並將其連接至執行個體，以確保其公有 IP 地址不會變更。當您將註冊的網域名稱 (例如

example.com) 與執行個體搭配使用時，便無須在每次停用或啟用執行個體時更新網域的 DNS 記錄。您可以將一個靜態 IP 連接至一個執行個體。

在執行個體管理頁面的 Networking#(聯網) 索引標籤下，選擇 Create a static IP (建立靜態 IP) 或 Attach static IP (連接靜態 IP)(若您先前已建立可以連接至執行個體的靜態 IP)，然後遵循頁面上的指示執行操作。如需詳細資訊，請參閱[建立靜態 IP 並將其附接至執行個體](#)。



Metrics | Snapshots | Storage | **Networking**

## IPv4 networking

The public IP address of your instance is accessible to the internet. A private IP address is accessible only to other resources in your Lightsail account.

PUBLIC IPV4

**192.0.2.0**

 **Attach static IP**

Your public IPv4 address changes when you stop and start your instance. Attach a **static IPv4** address to your instance to keep it from changing.

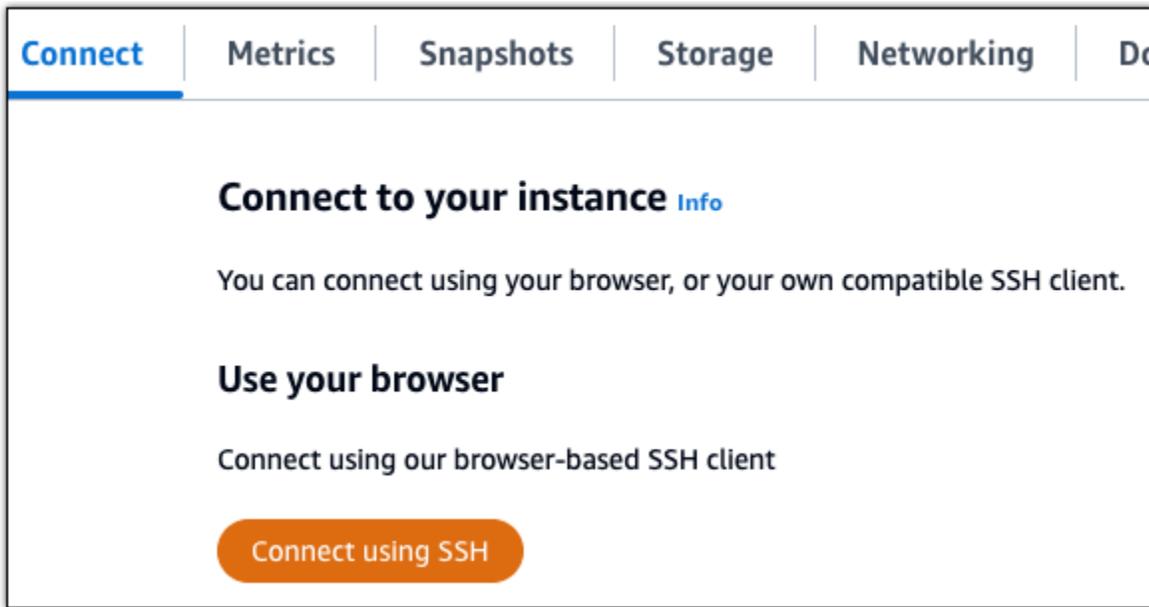
將新的靜態 IP 地址連接至執行個體後，必須完成以下步驟，以便應用程式知曉新的靜態 IP 地址。

1. 請記下執行個體的靜態 IP 地址。這會列在執行個體管理頁面的標頭區段中。



<b>Static IP address</b>  203.0.113.0	<b>Instance status</b>  <b>Running</b>
---	--

2. 在執行個體管理頁面的 Connect (連接) 索引標籤下，選擇 Connect using SSH (使用 SSH 連接)。



3. 連接後，請輸入以下命令。將 *<StaticIP>* 取代為執行個體新的靜態 IP 地址。

```
sudo /opt/bitnami/configure_app_domain --domain <StaticIP>
```

範例：

```
sudo /opt/bitnami/configure_app_domain --domain 203.0.113.0
```

您應該會看到類似以下內容的回應。您的執行個體上的應用程式現在應該已知曉新的靜態 IP 地址。

```
bitnami@ip-203.0.113.0:~$ sudo /opt/bitnami/configure_app_domain --domain
203.0.113.0
Configuring domain to 203.0.113.0
2024-06-06T21:43:42.393Z - info: Saving configuration info to disk
ghost 21:43:42.78 INFO ==> Configuring Ghost URL to http://203.0.113.0
Disabling automatic domain update for IP address changes
```

#### 步驟 4：登入 Ghost 網站的管理儀表板

現在您有了預設應用程式密碼，完成下列程序，以導覽至 Ghost 網站首頁並登入管理儀表板。登入後，您可以開始自訂網站並進行管理級變更。如需詳細資訊，了解 Ghost 可以執行哪些作業，請參閱 [步驟 6：閱讀 Ghost 文檔並繼續設定您的網站](#) 章節。

1. 在執行個體管理頁面的 Connect (連接) 索引標籤下，記下執行個體的公有 IP 地址。如果您之前已將靜態 IP 連接至執行個體，這將是靜態 IP 位址。公有 IP 地址也會顯示在執行個體管理頁面的標頭區段。



2. 瀏覽至執行個體的公有 IP 地址，例如前往 <http://203.0.113.0>。

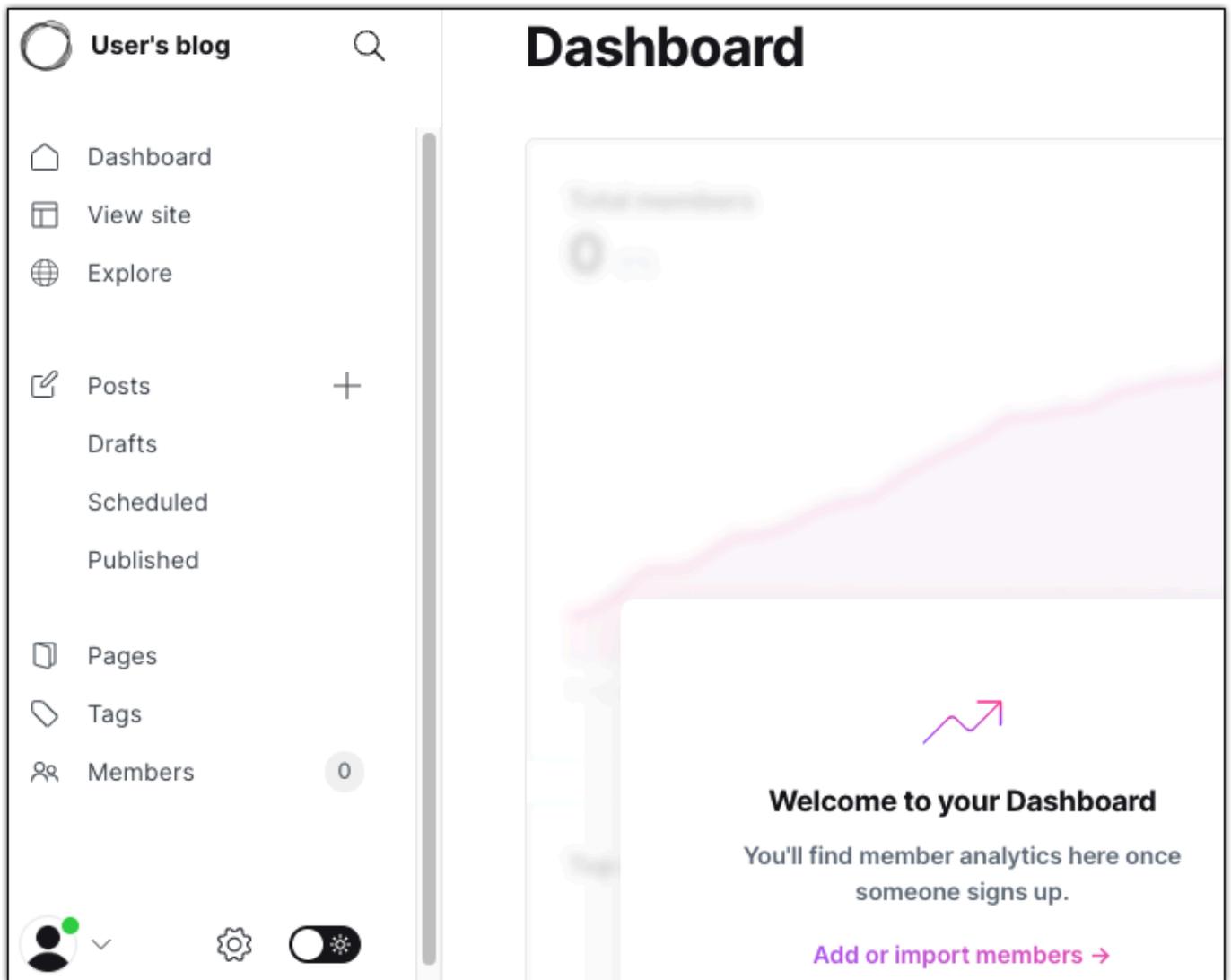
您會看到 Ghost 網站首頁。

3. 選擇 Ghost 網站首頁右下角的 Manage (管理)。

如果未顯示 Manage (管理) 橫幅，您可以透過瀏覽至 <http://<PublicIP>/ghost> 前往登入頁面。將 *<PublicIP>* 取代為您執行個體的公有 IP 地址。

4. 使用先前依本指南指示取得的預設使用者名稱 ([user@example.com](mailto:user@example.com)) 和預設密碼登入。

您會看到 Ghost 管理儀表板。



## 步驟 5：將已註冊網域的流量路由至 Ghost 網站

若要將已註冊網域 (例如 `example.com`) 的流量路由至 Ghost 網站，請新增記錄至網域的 DNS。DNS 記錄通常會在您註冊網域的註冊商處進行管理和託管。不過，我們建議您將網域 DNS 記錄的管理權限轉移至 Lightsail，以便您可以使用 Lightsail 主控台進行管理。

在 Lightsail 主控台首頁的 [網域與 DNS] 區段中，選擇 [建立 DNS 區域]，然後依照頁面上的指示進行。如需詳細資訊，請參閱 [在 Lightsail 中建立 DNS 區域以管理網域的 DNS 記錄](#)。

網域將流量路由至執行個體後，必須完成以下步驟，以便 Ghost 應用程式軟體知曉新網域。

1. 在執行個體管理頁面的 Connect (連接) 索引標籤下，選擇 Connect using SSH (使用 SSH 連接)。

2. 連接後，請輸入以下命令。將 `< DomainName >` 取代為將流量導向至 Ghost 執行個體的網域名稱。

```
$ sudo /opt/bitnami/configure_app_domain --domain <DomainName>
```

範例：

```
$ sudo /opt/bitnami/configure_app_domain --domain example.com
```

您應該會看到類似於以下範例的回應。Ghost 應用程式現在應該已知曉該網域。

```
bitnami@ip-203.0.113.0:~$ sudo /opt/bitnami/configure_app_domain --domain
example.com
Configuring domain to example.com
2024-06-06T21:50:00.393Z - info: Saving configuration info to disk
ghost 21:50:25.78 INFO ==> Configuring Ghost URL to http://example.com
Disabling automatic domain update for IP address changes
```

若您瀏覽至您為執行個體設定的網域名稱，則會將您重新導向至 Ghost 網站首頁。接下來，您應該生成並設定 SSL/TLS 憑證以啟用 Ghost 網站的 HTTPS 連接。如需詳細資訊，請繼續閱讀本指南的下一個章節 [步驟 6：為 Ghost 網站設定 HTTPS](#)。

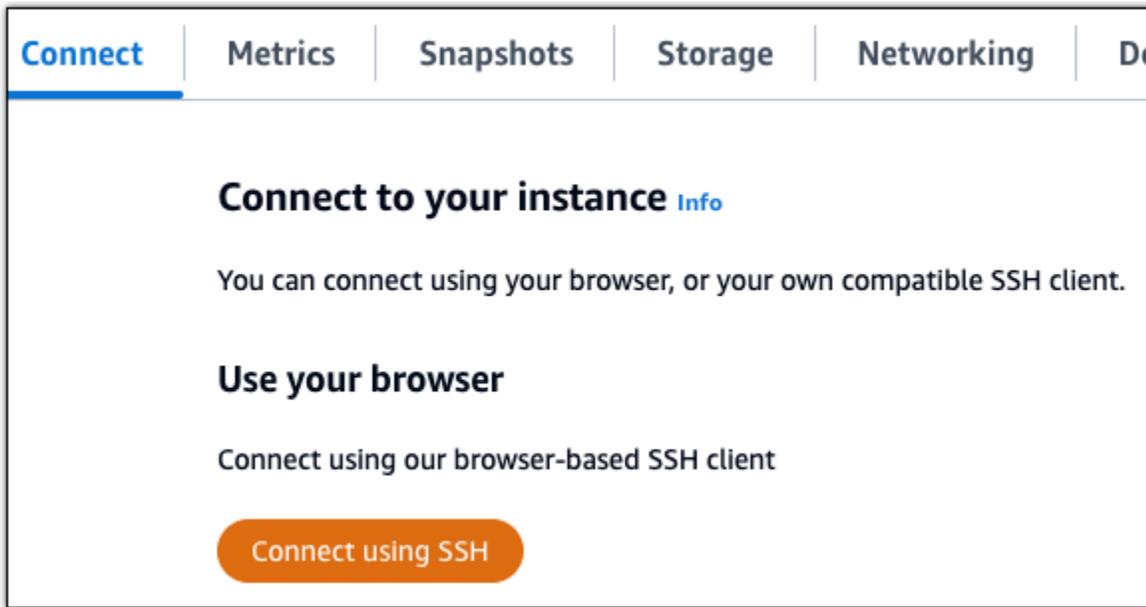
## 步驟 6：為 Ghost 網站設定 HTTPS

完成下列程序，以在 Ghost 網站上設定 HTTPS。這些步驟描述了如何使用 Bitnami HTTPS 組態工具 (bncert-tool)，這是一個命令行工具，用於請求 Let's Encrypt SSL/TLS 憑證。如需詳細資訊，請參閱 Bitnami 文件中的 [Learn About The Bitnami HTTPS Configuration Tool](#) (Bitnami HTTPS 組態工具簡介)。

### Important

開始此程序之前，請確認您已將網域設定為將流量路由至 Ghost 執行個體。否則，SSL/TLS 憑證驗證過程會失敗。

1. 在執行個體管理頁面的 Connect (連接) 索引標籤下，選擇 Connect using SSH (使用 SSH 連接)。



2. 連接後，輸入下列命令，以確認執行個體已安裝 bncert 工具。

```
sudo /opt/bitnami/bncert-tool
```

您應該會看到下列其中一個回應：

- 如果您看見回應中未找到命令，則表示您的執行個體上未安裝 bncert 工具。繼續此程序的下一個步驟，在您的執行個體上安裝 bncert 工具。
- 如果您在回應中看見 Welcome to the Bitnami HTTPS configuration tool (歡迎使用 Bitnami HTTPS 組態工具)，則您的執行個體上已安裝 bncert 工具。繼續執行此程序的步驟 8。
- 如果您的執行個體已安裝 bncert 工具一段時間，則您可能會看到說明該工具已有可用更新版本的訊息。選擇下載該版本，然後輸入 `sudo /opt/bitnami/bncert-tool` 命令以再次執行 bncert 工具。繼續執行此程序的步驟 8。

3. 輸入以下命令，以下載 bncert 執行檔案至您的執行個體。

```
wget -O bncert-linux-x64.run https://downloads.bitnami.com/files/bncert/latest/bncert-linux-x64.run
```

4. 輸入以下命令，以便為執行個體上的 bncert 工具執行檔案建立目錄。

```
sudo mkdir /opt/bitnami/bncert
```

5. 輸入以下命令，以讓 bncert 執行可作為程式執行的檔案。

```
sudo chmod +x /opt/bitnami/bncert/bncert-linux-x64.run
```

6. 輸入以下命令，以在您輸入 `sudo /opt/bitnami/bncert-tool` 命令時建立執行 `bncert` 工具的符號連結。

```
sudo ln -s /opt/bitnami/bncert/bncert-linux-x64.run /opt/bitnami/bncert-tool
```

您現已在執行個體上完成 `bncert` 工具安裝。

7. 輸入下列命令，以執行 `bncert` 工具。

```
sudo /opt/bitnami/bncert-tool
```

8. 輸入主要網域名稱和替代網域名稱，並以空格分隔，如以下範例所示。

如果您的網域未設為將流量路由至執行個體的公有 IP 地址，則 `bncert` 工具會要求您進行該設定，然後再繼續操作。您的網域必須將流量路由至執行個體的公有 IP 地址，而您需從該地址使用 `bncert` 工具來在執行個體上啟用 HTTPS。此舉措會確認您擁有該網域，並以此作為憑證的驗證。

```
-----
Welcome to the Bitnami HTTPS Configuration tool.
-----
Domains

Please provide a valid space-separated list of domains for which you wish to
configure your web server.

Domain list []: example.com www.example.com
```

9. `bncert` 工具會詢問您要如何設定網站的重新引導。可用的選項如下：
  - Enable HTTP to HTTPS redirection (啟用 HTTP 至 HTTPS 重新引導) - 指定將瀏覽至網站 HTTP 版本 (即 `http://example.com`) 的使用者自動重新引導至 HTTPS 版本 (即 `https://example.com`)。由於此選項會強制所有訪客使用加密的連線，建議啟用此選項。輸入 Y，並按 Enter 以啟用。
  - Enable non-www to www redirection (啟用非 www 至 www 重新引導) - 指定將瀏覽至網域 (即 `https://example.com`) 頂點的使用者自動重新引導至您網域的 `www` 子網域 (即 `https://www.example.com`)。建議啟用此選項。不過，如果您已在搜索引擎工具 (如 Google 的網站管理員工具) 中將網域的頂點指定為您偏好的網站地址，或者如果您的頂點直接指向 IP，且 `www` 子網域透過 CNAME 記錄參考您的頂點，則您可能需要停用此選項並啟用替代選項 (啟用 `www` 至非 `www` 重新引導)。輸入 Y，並按 Enter 以啟用。

- Enable www to non-www redirection (啟用 www 至非 www 重新引導) - 指定將瀏覽至您網域 www 子網域 (即 `https://www.example.com`) 的使用者自動重新引導至網域的頂點 (即 `https://example.com`)。如果您已啟用非 www 重新引導至 www，我們建議您停用此選項。輸入 N，並按 Enter (確認) 以停用。

您的選取內容應看起來與下列範例類似。

```
Enable/disable redirections
Please select the redirections you wish to enable or disable on your Bitnami
installation.

Enable HTTP to HTTPS redirection [Y/n]: Y

Enable non-www to www redirection [Y/n]: Y

Enable www to non-www redirection [y/N]: N
```

10. 系統會列出即將進行的變更。輸入 Y，並按 Enter (確認) 以確認並繼續。

```
Changes to perform

The following changes will be performed to your Bitnami installation:

1. Stop web server
2. Configure web server to use a free Let's Encrypt certificate for the domains:
example.com www.example.com
3. Configure a cron job to automatically renew the certificate each month
4. Configure web server name to: example.com
5. Enable HTTP to HTTPS redirection (example: redirect http://example.com to
https://example.com)
6. Enable non-www to www redirection (example: redirect example.com to
www.example.com)
7. Start web server once all changes have been performed

Do you agree to these changes? [Y/n]: Y
```

11. 輸入您的電子郵件地址，以與您的 Let's Encrypt 憑證相關聯，然後按 Enter。

```
Create a free HTTPS certificate with Let's Encrypt

Please provide a valid e-mail address for which to associate your Let's Encrypt
certificate.

Domain list: example.com www.example.com

Server name: example.com

E-mail address []: █
```

12. 檢閱 Let's Encrypt 訂閱者協議。輸入 Y，並按 Enter (確認) 以接受該協議並繼續。

```
The Let's Encrypt Subscriber Agreement can be found at:
https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf

Do you agree to the Let's Encrypt Subscriber Agreement? [Y/n]: █
```

執行這些動作是為了在執行個體上啟用 HTTPS，包括請求憑證和設定您指定的重新引導。

```
Performing changes to your installation

The Bitnami HTTPS Configuration Tool will perform any necessary actions to your
Bitnami installation. This may take some time, please be patient.
```

系統已成功核發並驗證您的憑證，如果您看到類似以下範例的訊息，則表示已成功在執行個體上設定重新引導。

```
Success

The Bitnami HTTPS Configuration Tool succeeded in modifying your installation.
The configuration report is shown below.

Backup files:
* /opt/bitnami/apache2/conf/httpd.conf.back.202005290035
* /opt/bitnami/apache2/conf/bitnami/bitnami-apps-prefix.conf.back.202005290035
* /opt/bitnami/apache2/conf/bitnami/bitnami.conf.back.202005290035

Find more details in the log file:
/tmp/bncert-202005290035.log

If you find any issues, please check Bitnami Support forums at:
https://community.bitnami.com

Press [Enter] to continue:█
```

bncert 工具會在憑證過期前每 80 天執行自動續約一次。如果您要搭配執行個體使用其他網域和子網域，且要為這些網域啟用 HTTPS，請重複上述步驟。

 Tip

輸入下列命令以重新啟動執行個體上的服務。

```
sudo /opt/bitnami/ctlscript.sh restart
```

您現已在 Ghost 執行個體上啟用 HTTPS。下次使用您設定的網域瀏覽至 Ghost 網站時，應該會看到您被重新導向至 HTTPS 連接。

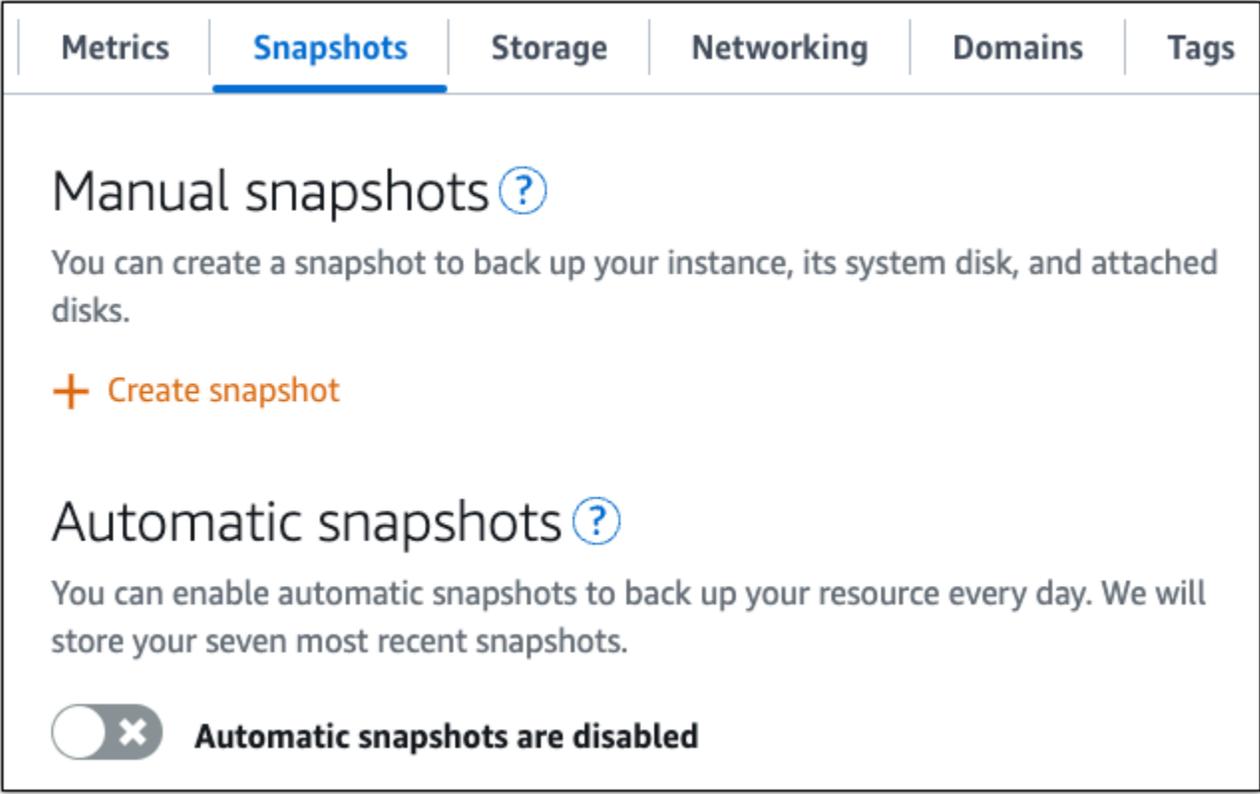
## 步驟 7：閱讀 Ghost 文件並繼續設定網站

閱讀 Ghost 文件以了解如何管理和自訂網站。如需詳細資訊，請參閱 [Ghost 文件](#)。

## 步驟 8：建立執行個體的快照

按照您想要的方式設定 Ghost 網站後，請定期建立執行個體的快照以作為備份。您可以手動建立快照，或啟用自動快照，讓 Lightsail 為您建立每日快照。若執行個體出現問題，您可以使用快照建立新的替代執行個體。如需詳細資訊，請參閱[快照](#)。

在執行個體管理頁面的 Snapshot (快照) 索引標籤下，選擇 Create a snapshot (建立快照) 或選擇啟用自動快照。



**Metrics** | **Snapshots** | Storage | Networking | Domains | Tags

## Manual snapshots ?

You can create a snapshot to back up your instance, its system disk, and attached disks.

[+ Create snapshot](#)

## Automatic snapshots ?

You can enable automatic snapshots to back up your resource every day. We will store your seven most recent snapshots.

**Automatic snapshots are disabled**

如需詳細資訊，請參閱在 Amazon Lightsail 中建立 [Linux 或 Unix 執行個體的快照](#)或在 [Amazon Lightsail](#) 中 [啟用或停用執行個體或磁碟的自動快照](#)。

## 在 Lightsail 上設定和設定 GitLab CE 執行個體

在您的 GitLab CE 執行個體在 Amazon Lightsail 上啟動並執行之後，您應該採取以下幾個步驟來開始使用：

### 內容

- [步驟 1：閱讀 Bitnami 文件](#)
- [步驟 2：獲取默認的應用程序密碼以訪問 GitLab CE 管理區](#)
- [步驟 3：將靜態 IP 地址連接至您的執行個體](#)
- [步驟 4：登入 Gitlab CE 網站的管理區](#)
- [步驟 5：將您註冊域名的流量路由到您的 GitLab CE 網站](#)
- [步驟 6：配置您HTTPS的 GitLab CE 網站](#)
- [步驟 7：閱讀 GitLab CE 文檔並繼續配置您的網站](#)
- [步驟 8：建立執行個體的快照](#)

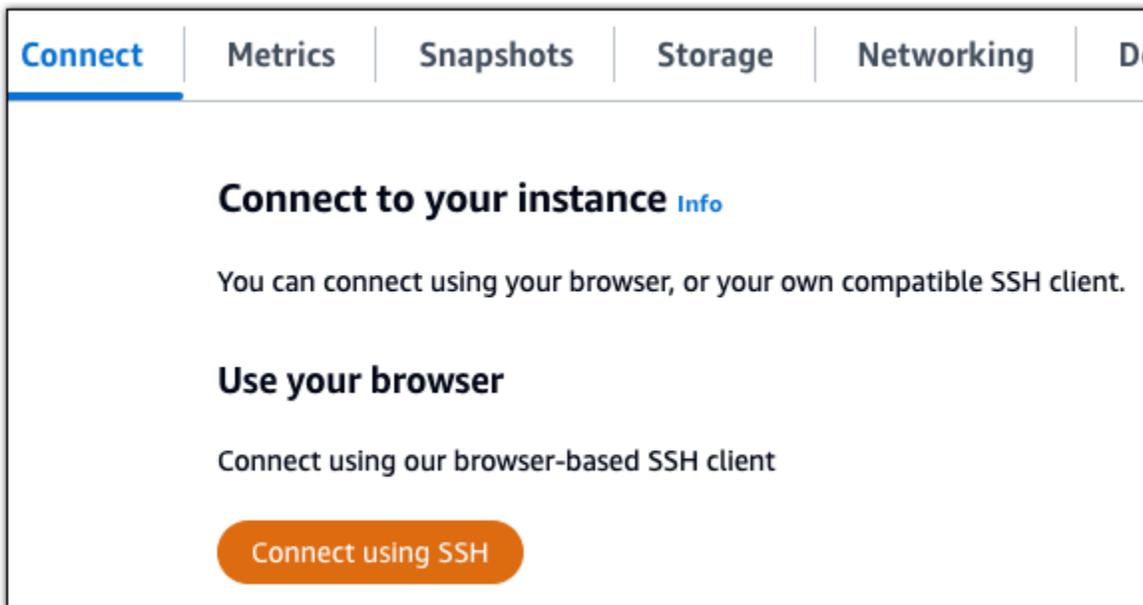
## 步驟 1：閱讀 Bitnami 文件

閱讀 Bitnami 文檔以了解如何配置您的 GitLab CE 應用程式。如需詳細資訊，請參閱[由 Bitnami 封裝的 GitLab CE](#)。AWS 雲端

## 步驟 2：獲取默認的應用程式密碼以訪問 GitLab CE 管理區

完成以下步驟以獲取訪問 GitLab CE 網站管理區域所需的默認應用程式密碼。如需詳細資訊，請參閱在[Amazon Lightsail 中取得 Bitnami 執行個體的應用程式使用者名稱和密碼](#)。

1. 在執行個體管理頁面的 [Connect] 索引標籤下，選擇 [Connect 方式] SSH。



2. 連線後，請輸入下列命令，以取得應用程式密碼：

```
cat $HOME/bitnami_application_password
```

您應該會看到類似於以下範例的回應，其中包含預設應用程式密碼：

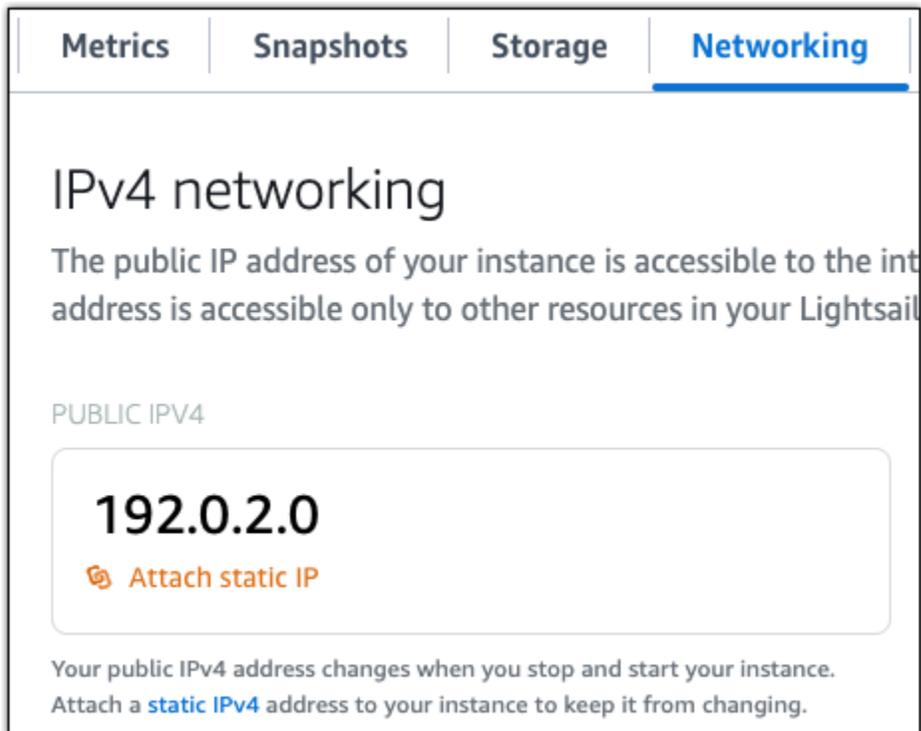
```
bitnami@ip-172-31-10-100:~$ cat bitnami_application_password
JeVN8xDWlCIp
bitnami@ip-172-31-10-100:~$
```

## 步驟 3：將靜態 IP 地址連接至您的執行個體

您第一次建立執行個體時，所指派的公有 IP 地址將會在每次停用和啟用執行個體時變更。您應該建立靜態 IP 地址並將其連接至執行個體，以確保其公有 IP 地址不會變更。稍後，當您在執行個體上使用已

註冊的網域名稱時，不必在每次停止並啟動執行個體時更新網域的DNS記錄。example.com您可以將一個靜態 IP 連接至一個執行個體。

在執行個體管理頁面的Networking#(聯網) 索引標籤下，選擇 Create a static IP (建立靜態 IP) 或 Attach static IP (連接靜態 IP)(若您先前已建立可以連接至執行個體的靜態 IP)，然後遵循頁面上的指示執行操作。如需詳細資訊，請參閱[建立靜態 IP 並將其附接至執行個體](#)。



Metrics | Snapshots | Storage | **Networking**

## IPv4 networking

The public IP address of your instance is accessible to the internet. The private IP address is accessible only to other resources in your Lightsail instance.

PUBLIC IPV4

**192.0.2.0**

 **Attach static IP**

Your public IPv4 address changes when you stop and start your instance. Attach a **static IPv4** address to your instance to keep it from changing.

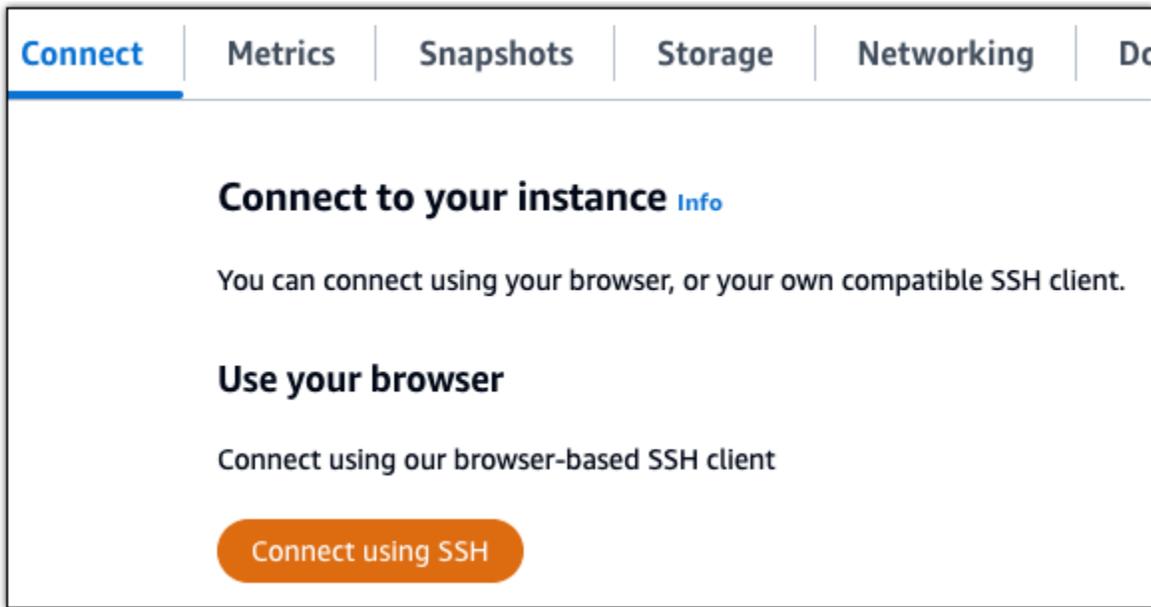
將新的靜態 IP 地址連接至執行個體後，必須完成以下步驟，以便應用程式知曉新的靜態 IP 地址。

1. 請記下執行個體的靜態 IP 地址。這會列在執行個體管理頁面的標頭區段中。



<b>Static IP address</b>  203.0.113.0	<b>Instance status</b>  <b>Running</b>
---	--

2. 在執行個體管理頁面的 [Connect] 索引標籤下，選擇 [Connect 方式] SSH。



3. 連接後，請輸入以下命令。Replace (取代) `<StaticIP>` 使用執行個體的新靜態 IP 位址。

```
sudo /opt/bitnami/configure_app_domain --domain <StaticIP>
```

範例：

```
sudo /opt/bitnami/configure_app_domain --domain 203.0.113.0
```

您應該會看到類似於以下範例的回應。您的執行個體上的應用程式現在應該已知曉新的靜態 IP 地址。

```
bitnami@ip-172-20-3-11:~$ sudo /opt/bitnami/configure_app_domain --domain 203.0.113.0
Configuring domain to 203.0.113.0
2022-06-09T16:47:06.737Z - info: Saving configuration info to disk
gitlab 16:47:06.86 INFO ==> Updating external URL in GitLab configuration
gitlab 16:47:06.88 INFO ==> Reconfiguring GitLab
gitlab 16:47:45.29 INFO ==> Starting GitLab services
Disabling automatic domain update for IP address changes
```

#### 步驟 4：登入 Gitlab CE 網站的管理區

現在您擁有了默認的用戶密碼，請導航到 GitLab CE 網站的主頁，然後登錄到管理區域。登入後，您可以開始自訂網站並進行管理級變更。有關您可以在 GitLab CE 中執行的操作的更多信息，請參閱本指南後面的[步驟 7：閱讀 GitLab CE 文檔並繼續配置您的網站](#)部分。

1. 在執行個體管理頁面的 Connect (連接) 索引標籤下，記下執行個體的公有 IP 地址。公有 IP 地址也會顯示在執行個體管理頁面的標頭區段。

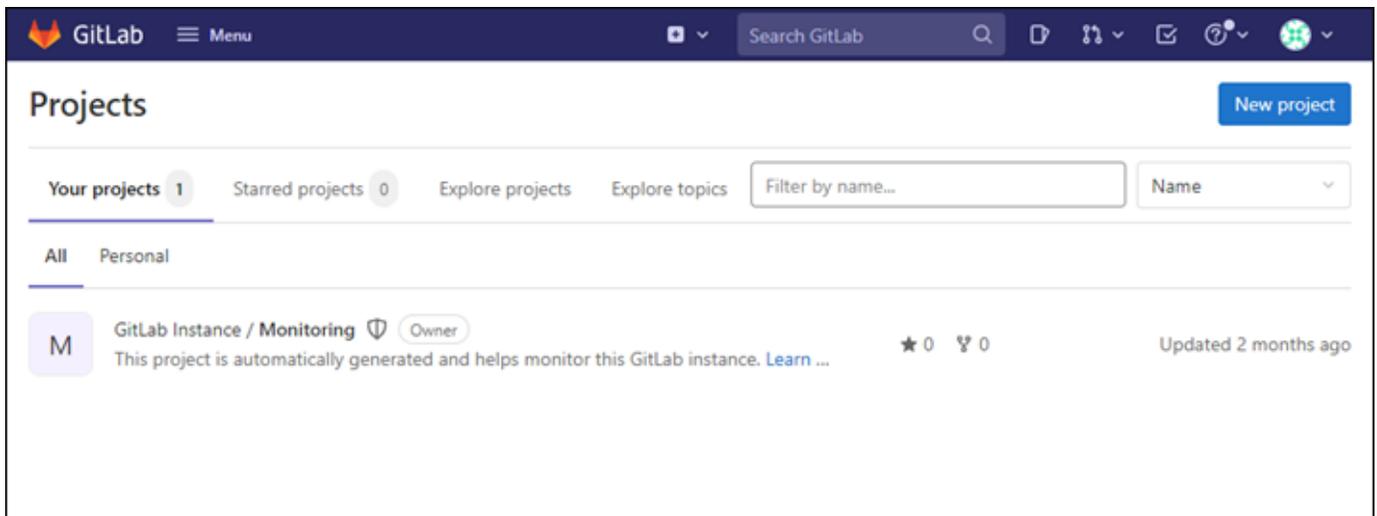


2. 瀏覽至執行個體的公有 IP 地址，例如前往 <http://203.0.113.0>。

您會看到 Gitlab CE 網站首頁。您可能會看到瀏覽器的警告通知，告知您連線並非私有且不安全，或有安全性風險。發生這種情況是因為您的 GitLab CE 實例尚未應用SSL/TLS證書。在瀏覽器視窗中，選擇 Advanced (進階)、Details (詳細資訊) 或 More information (更多資訊)，以檢視可用的選項。然後選擇繼續瀏覽該網站，即使該網站不是私有或安全的網站。

3. 使用先前依本指南指示取得的預設使用者名稱 (root) 和預設密碼登入。

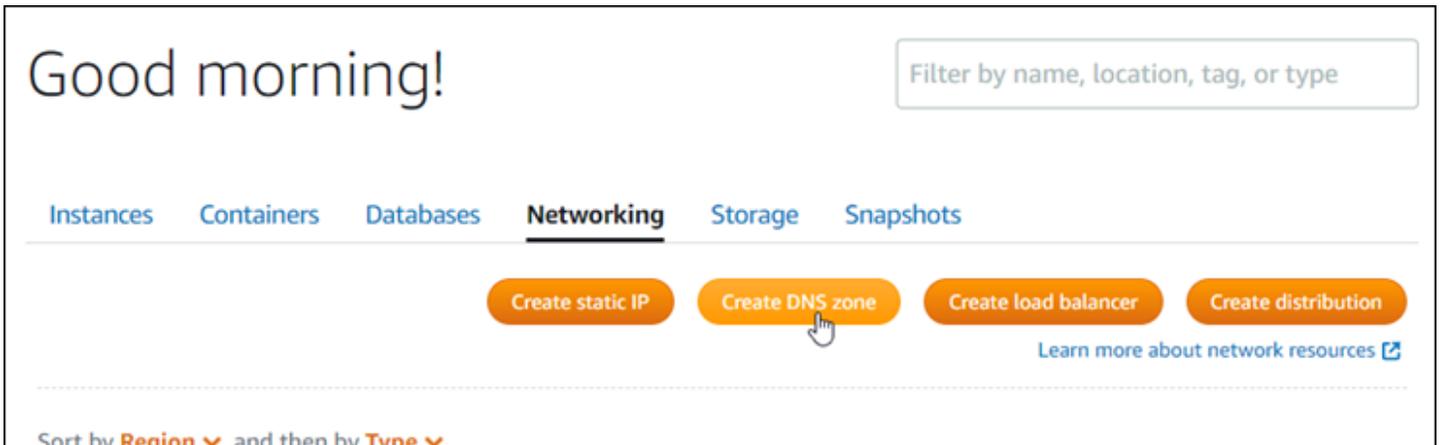
您會看到 Gitlab CE 管理儀表板。



## 步驟 5：將您註冊域名的流量路由到您的 GitLab CE 網站

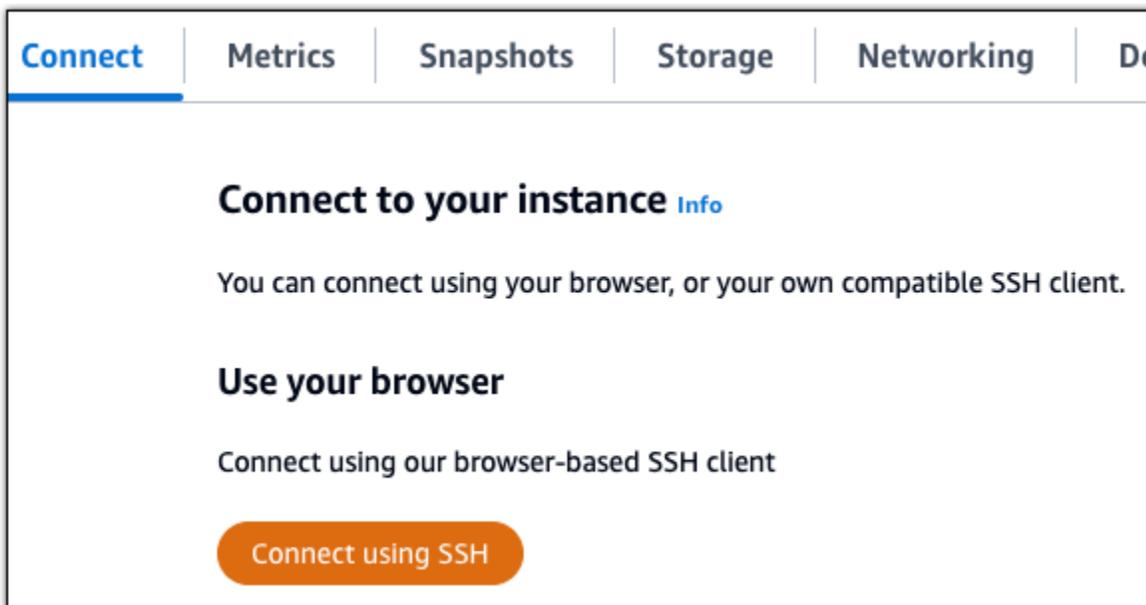
若要將已註冊網域名稱的流量路由至您的 GitLab CE 網站，請將記錄新增至您網域的網域名稱系統 (DNS)。example.com DNS 記錄通常在您註冊網域的註冊商處進行管理和託管。不過，我們建議您將網域 DNS 記錄的管理權限轉移至 Lightsail，以便您可以使用 Lightsail 主控台進行管理。

在 Lightsail 主控台首頁的 [網路功能] 索引標籤下，選擇 [建立 DNS 區域]，然後依照頁面上的指示進行。如需詳細資訊，請參閱 [建立 DNS 區域以管理網域 DNS 記錄](#)。



在您的網域名稱將流量路由到執行個體之後，您必須完成下列程序，讓 GitLab CE 知道網域名稱。

1. 在執行個體管理頁面的 [Connect] 索引標籤下，選擇 [Connect 方式] SSH。



2. 連接後，請輸入以下命令。Replace (取代) *<DomainName>* 使用將流量路由到您的執行個體的網域名稱。

```
sudo /opt/bitnami/configure_app_domain --domain <DomainName>
```

範例：

```
sudo /opt/bitnami/configure_app_domain --domain example.com
```

您應該會看到類似於以下範例的回應。您的 GitLab CE 執行個體現在應該知道網域名稱。

```
bitnami@ip-10.0.0.11:~$ sudo /opt/bitnami/configure_app_domain --domain example.com
Configuring domain to example.com
2022-06-09T18:44:00.235Z - info: Saving configuration info to disk
gitlab 18:44:00.36 INFO ==> Updating external URL in GitLab configuration
gitlab 18:44:00.37 INFO ==> Reconfiguring GitLab
gitlab 18:44:38.79 INFO ==> Starting GitLab services
Disabling automatic domain update for IP address changes
```

如果該命令失敗，您可能正在使用較舊版本的 GitLab CE 實例。改為嘗試執行下列命令。Replace (取代) *<DomainName>* 使用將流量路由到您的執行個體的網域名稱。

```
cd /opt/bitnami/apps/gitlab
sudo ./bnconfig --machine_hostname <DomainName>
```

在執行這些命令後，輸入以下命令，以防止 bnconfig 工具在伺服器每次重新啟動時自動執行。

```
sudo mv bnconfig bnconfig.disabled
```

接下來，您應該生成並配置SSL/TLS證書以啟用您的 GitLab CE 網站的HTTPS連接。如需詳細資訊，請繼續閱讀本指南的下一個[步驟 6：HTTPS為您的 GitLab CE 網站設定](#)一節。

## 步驟 6：配置您HTTPS的 GitLab CE 網站

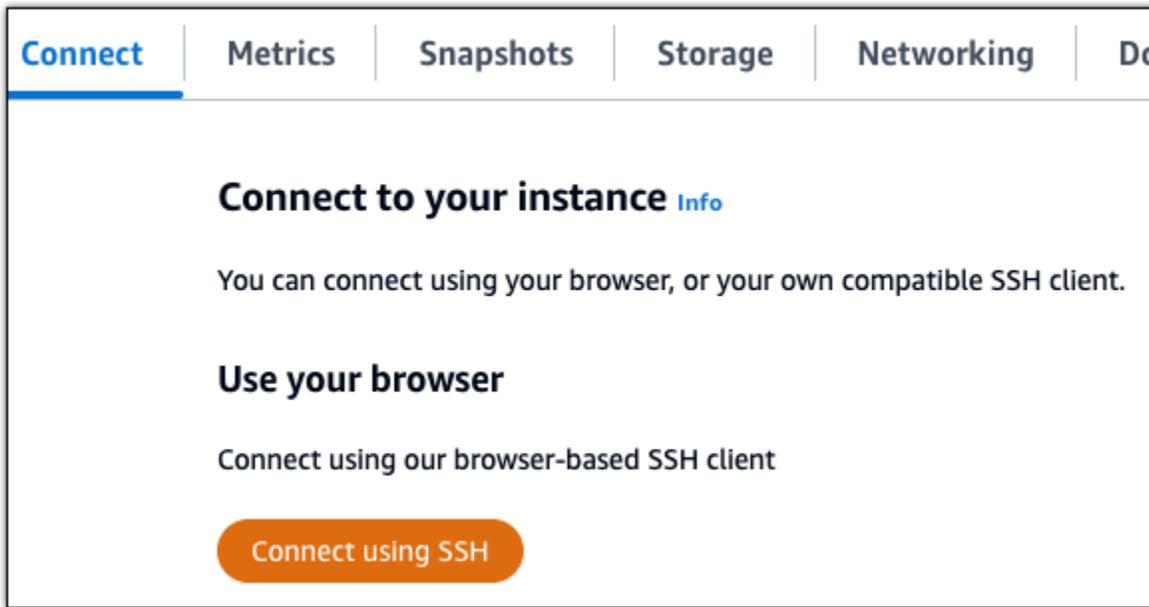
完成以下程序以HTTPS在您的 GitLab CE 網站上進行配置。這些步驟向您展示瞭如何使用[樂高客戶端](#)，這是請求 Let's EncryptSSL/TLS證書的命令行工具。

### Important

在開始此程序之前，請確定您已設定網域以將流量路由到 GitLab CE 執行個體。否則，SSL/TLS證書驗證過程將失敗。若要為您註冊的網域名稱路由流量，請將記錄新增至您DNS的網域。DNS記錄通常在您註冊網域的註冊商處進行管理和託管。不過，我們建議您將網域DNS記錄的管理權限轉移至 Lightsail，以便您可以使用 Lightsail 主控台進行管理。

在 Lightsail 主控台首頁的「網域與 DNS」索引標籤下，選擇「建立DNS區域」，然後依照頁面上的指示操作。如需詳細資訊，請參閱[在 Lightsail 中建立DNS區域以管理您的網域DNS記錄](#)。

1. 在執行個體管理頁面的 [Connect] 索引標籤下，選擇 [Connect 方式] SSH。



2. 連接之後，請輸入下列命令，以將目錄更改為臨時 (/tmp) 目錄。

```
cd /tmp
```

3. 輸入下列命令，以下載最新版本的 Lego 用戶端。此命令會下載磁帶歸檔 (tar) 檔案。

```
curl -Ls https://api.github.com/repos/xenolf/lego/releases/latest | grep  
browser_download_url | grep linux_amd64 | cut -d '"' -f 4 | wget -i -
```

4. 輸入下列命令，以從 tar 檔案中提取檔案。Replace (取代) *X.Y.Z* 與您下載的樂高客戶端的版本。

```
tar xf lego_vX.Y.Z_linux_amd64.tar.gz
```

範例：

```
tar xf lego_v4.7.0_linux_amd64.tar.gz
```

5. 輸入下列命令，以建立 /opt/bitnami/letsencrypt 目錄，您將把 Lego 用戶端檔案移動到其中。

```
sudo mkdir -p /opt/bitnami/letsencrypt
```

6. 輸入以下命令，以將 Lego 用戶端檔案移動到建立的目錄中。

```
sudo mv lego /opt/bitnami/letsencrypt/lego
```

- 依序輸入以下命令，以停止在執行個體上運行的應用程式服務。

```
sudo service bitnami stop
sudo service gitlab-runsrvdir stop
```

- 輸入以下命令以使用樂高客戶端請求讓我們加密SSL/TLS證書。

```
sudo /opt/bitnami/letsencrypt/lego --tls --email="EmailAddress" --
domains="RootDomain" --domains="WwwSubDomain" --path="/opt/bitnami/letsencrypt" run
```

將命令中的以下範例值取代為自訂值：

- EmailAddress* – 註冊通知所用的電子郵件地址。
- RootDomain*— 將流量路由到您的 GitLab CE 網站的主要根網域 (例如，example.com)。
- WwwSubDomain*— 將流量路由到您的 GitLab CE 網站的主要根網域的www子網域 (例如，www.example.com)。

您可以為憑證指定多個網域，方法是在命令中指定其他 `--domains` 參數。當您指定多個域時，樂高創建一個主題替代名稱 (SAN) 證書，該證書導致只有一個證書對您指定的所有域有效。清單中的第一個網域會新增為憑證的「CommonName」，其餘網域會新增為「DNSNames」至憑證中的SAN擴充功能。

範例：

```
sudo /opt/bitnami/letsencrypt/lego --tls --email="user@example.com" --
domains="example.com" --domains="www.example.com" --path="/opt/bitnami/letsencrypt"
run
```

- 提示接受服務條款時，請按 Y 和 Enter。

您應該會看到類似於以下範例的回應。

```
2022/06/09 19:23:27 [INFO] [ example.com ] Server responded with a certificate.
```

如果成功，將儲存一組憑證至 `/opt/bitnami/letsencrypt/certificates` 目錄中。此集包括伺服器憑證檔案 (例如 `example.com.crt`) 和伺服器憑證金鑰檔案 (例如 `example.com.key`)。

- 依序輸入以下命令，以重新命名執行個體上的現有憑證。稍後，您要用新的 Let's Encrypt 憑證替換現有憑證。

```
sudo mv /etc/gitlab/ssl/server.crt /etc/gitlab/ssl/server.crt.old
sudo mv /etc/gitlab/ssl/server.key /etc/gitlab/ssl/server.key.old
sudo mv /etc/gitlab/ssl/server.csr /etc/gitlab/ssl/server.csr.old
```

- 逐一輸入以下命令，為您的新 Let's Encrypt 憑證建立符號連結，目/etc/gitlab/ssl錄是 GitLab CE 執行個體上的預設憑證目錄。

```
sudo ln -sf /opt/bitnami/letsencrypt/certificates/Domain.key /etc/gitlab/ssl/
server.key
sudo ln -sf /opt/bitnami/letsencrypt/certificates/Domain.crt /etc/gitlab/ssl/
server.crt
```

在命令中，替換 *Domain* 使用您在要求 Let's Encrypt 憑證時指定的主要根網域。

範例：

```
sudo ln -sf /opt/bitnami/letsencrypt/certificates/example.com.key /etc/gitlab/ssl/
server.key
sudo ln -sf /opt/bitnami/letsencrypt/certificates/example.com.crt /etc/gitlab/ssl/
server.crt
```

- 依序輸入以下命令，以變更新 Let's Encrypt 憑證位於的目錄的權限。

```
sudo chown root:root /etc/gitlab/ssl/server*
sudo chmod 600 /etc/gitlab/ssl/server*
```

- 輸入以下命令以重新啟動 GitLab CE 實例上的應用程序服務。

```
sudo service bitnami start
```

下次使用您配置的域瀏覽到 GitLab CE 網站時，您應該會看到它重定向到HTTPS連接。請注意，GitLab CE 執行個體最多可能需要一個小時才能辨識新憑證。如果您的 GitLab CE 網站拒絕連接，請停止並啟動實例，然後再試一次。

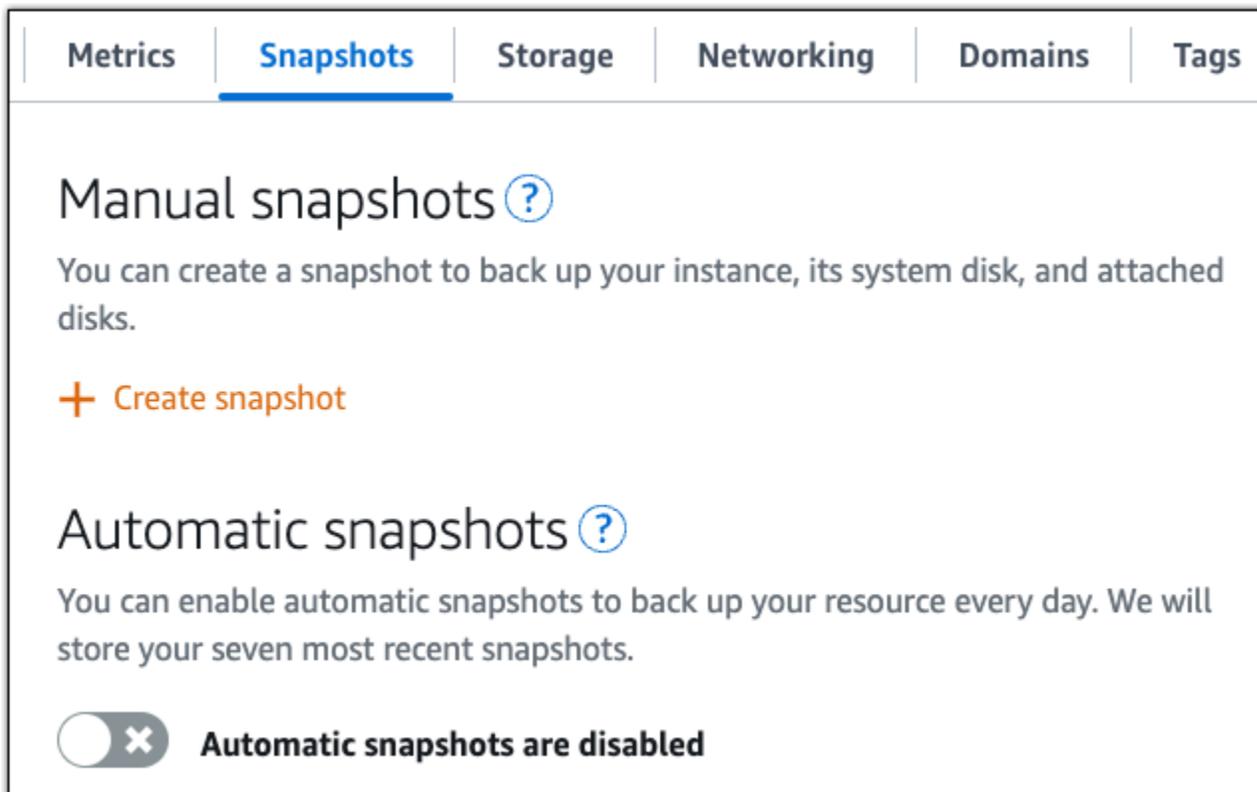
## 步驟 7：閱讀 GitLab CE 文檔並繼續配置您的網站

閱讀 GitLab CE 文檔以了解如何管理和自定義您的網站。如需詳細資訊，請參閱[GitLab 文件](#)。

## 步驟 8：建立執行個體的快照

按照您想要的方式配置 GitLab CE 網站後，請為實例創建定期快照以備份它。您可以手動建立快照，或啟用自動快照，讓 Lightsail 為您建立每日快照。若執行個體出現問題，您可以使用快照建立新的替代執行個體。如需詳細資訊，請參閱[快照](#)。

在執行個體管理頁面的 Snapshot (快照) 索引標籤下，選擇 Create a snapshot (建立快照) 或選擇啟用自動快照。



如需詳細資訊，請參閱在 Amazon Lightsail 中建立 [Linux 或 Unix 執行個體的快照](#)或在 [Amazon Lightsail](#) 中[啟用或停用執行個體或磁碟的自動快照](#)。

## 開始使用! 關於 Lightsail

這裡有幾個你應該採取的步驟來開始使用 Joomla! 實例已啟動並在 Amazon Lightsail 上運行：

內容

- [步驟 1：閱讀 Bitnami 文件](#)
- [步驟 2：取得存取 Joomla! 控制面板所需的預設應用程式密碼](#)
- [步驟 3：將靜態 IP 地址連接至您的執行個體](#)

- [步驟 4：登入 Joomla! 網站的控制面板](#)
- [步驟 5：將已註冊網域的流量路由至 Joomla! 網站](#)
- [步驟 6：為 Joomla! 網站設定 HTTPS](#)
- [步驟 7：閱讀 Joomla! 文件並繼續設定網站](#)
- [步驟 8：建立執行個體的快照](#)

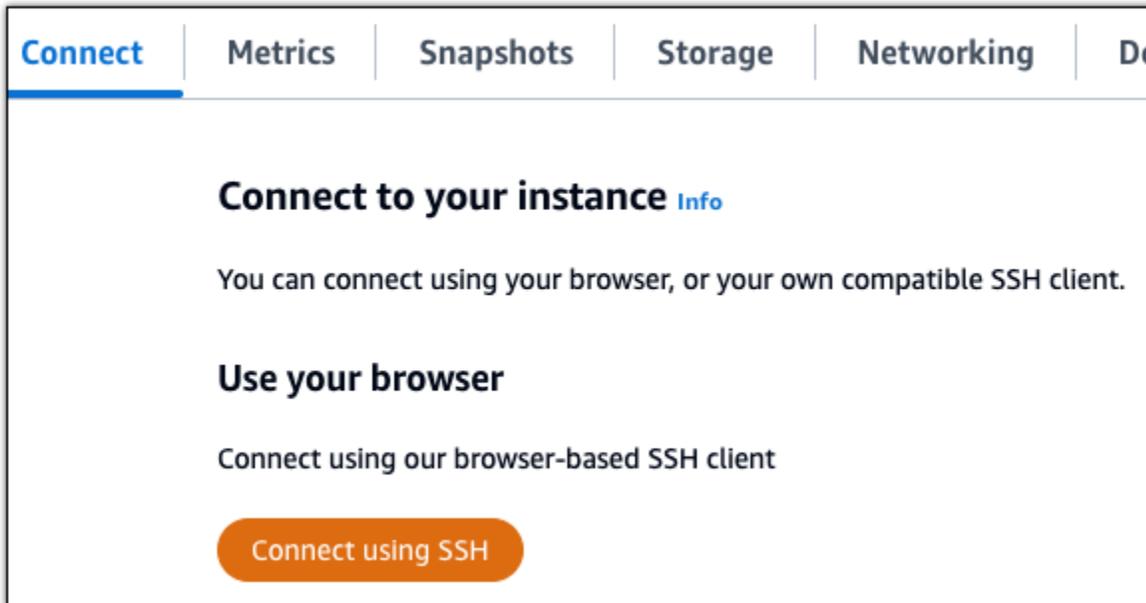
## 步驟 1：閱讀 Bitnami 文件

閱讀 Bitnami 文件以了解如何設定 Joomla! 應用程式。如需詳細資訊，請參閱 [Joomla! 由比特納米打包為 .AWS 雲端](#)

## 步驟 2：取得存取 Joomla! 控制面板所需的預設應用程式密碼

完成下列程序，以取得 Joomla! 網站控制面板所需的預設應用程式密碼。如需詳細資訊，請參閱在 [Amazon Lightsail 中取得 Bitnami 執行個體的應用程式使用者名稱和密碼](#)。

1. 在執行個體管理頁面的 Connect (連接) 索引標籤下，選擇 Connect using SSH (使用 SSH 連接)。



2. 連線後，請輸入下列命令，以取得應用程式密碼：

```
cat $HOME/bitnami_application_password
```

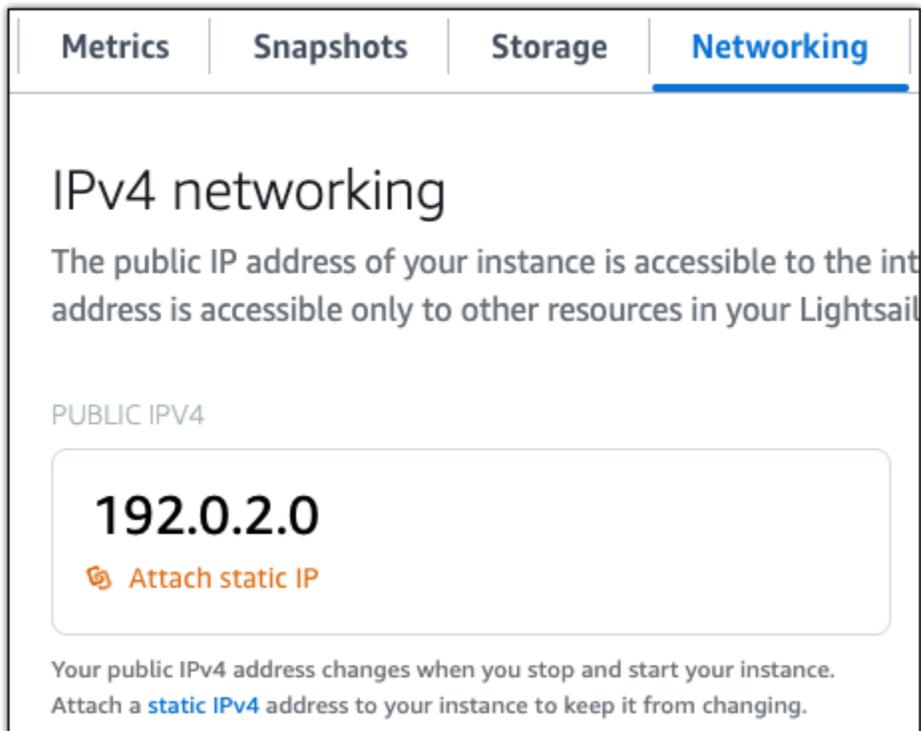
您應該會看到類似於以下範例的回應，其中包含預設應用程式密碼：

```
bitnami@ip-192-0-20-100:~$ cat bitnami_application_password
JeVN8xDWlCIp
bitnami@ip-192-0-20-100:~$
```

### 步驟 3：將靜態 IP 地址連接至您的執行個體

您第一次建立執行個體時，所指派的公有 IP 地址將會在每次停用和啟用執行個體時變更。您應該建立靜態 IP 地址並將其連接至執行個體，以確保其公有 IP 地址不會變更。當您將註冊的網域名稱 (例如 example.com) 與執行個體搭配使用時，便無須在每次停用或啟用執行個體時更新網域的 DNS 記錄。您可以將一個靜態 IP 連接至一個執行個體。

在執行個體管理頁面的 Networking#(聯網) 索引標籤下，選擇 Create a static IP (建立靜態 IP) 或 Attach static IP (連接靜態 IP)(若您先前已建立可以連接至執行個體的靜態 IP)，然後遵循頁面上的指示執行操作。如需詳細資訊，請參閱[建立靜態 IP 並將其附接至執行個體](#)。



The screenshot shows the 'Networking' tab in the AWS Lightsail console. Under 'IPv4 networking', it states: 'The public IP address of your instance is accessible to the internet. A private IP address is accessible only to other resources in your Lightsail instance.' Below this, the 'PUBLIC IPV4' section shows the IP address '192.0.2.0' and an 'Attach static IP' button. A note at the bottom reads: 'Your public IPv4 address changes when you stop and start your instance. Attach a static IPv4 address to your instance to keep it from changing.'

### 步驟 4：登入 Joomla! 網站的控制面板

現在您已擁有預設應用程式密碼，完成下列程序，以導覽至 Joomla! 網站首頁並登入控制面板。登入後，您可以開始自訂網站並進行管理級變更。如需詳細資訊，了解能在 Joomla! 中執行哪些作業，請參閱本指南後述的[步驟 7：閱讀 Joomla! 文件並繼續設定網站](#)章節。

1. 在執行個體管理頁面的 Connect (連接) 索引標籤下，記下執行個體的公有 IP 地址。公有 IP 地址也會顯示在執行個體管理頁面的標頭區段。



2. 瀏覽至執行個體的公有 IP 地址，例如前往 <http://203.0.113.0>。

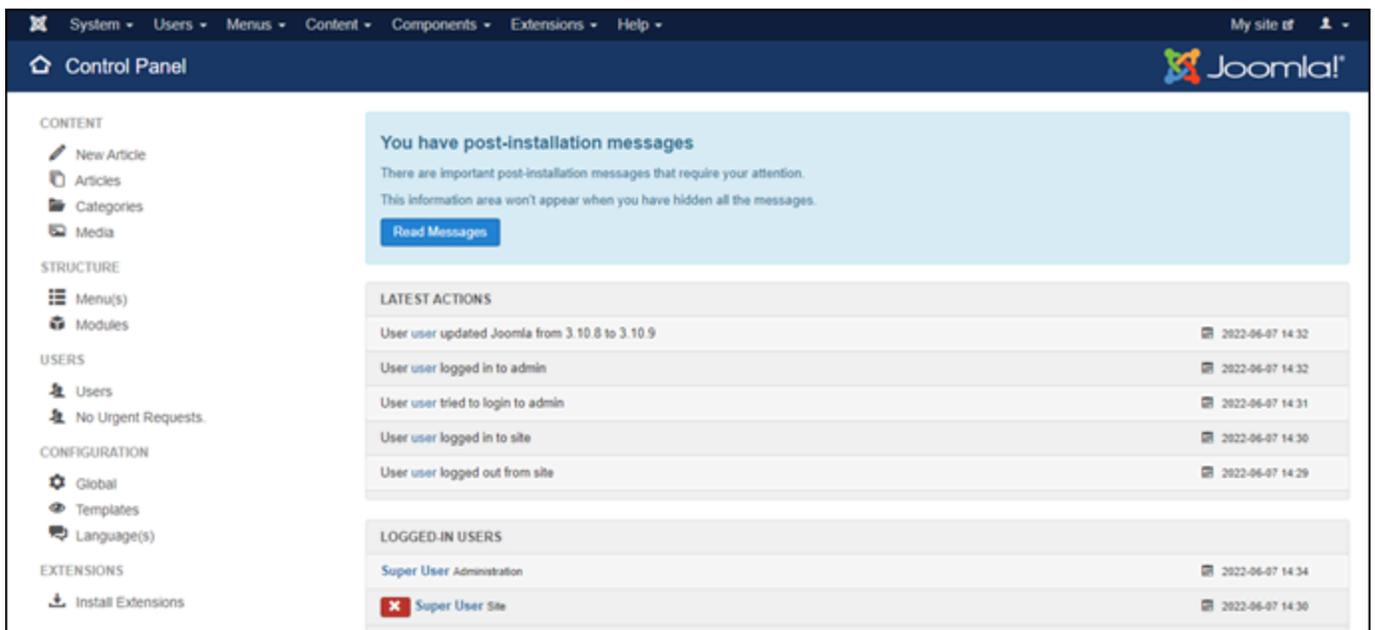
您會看到 Joomla! 網站首頁。

3. 選擇 Joomla! 網站首頁右下角的 Manage (管理)。

如果未顯示 Manage (管理) 橫幅，您可以透過瀏覽至 <http://<PublicIP>/administrator/> 前往登入頁面。將 *<PublicIP>* 取代為您執行個體的公有 IP 地址。

4. 使用先前依本指南指示取得的預設使用者名稱 (user) 和預設密碼登入。

您會看到 Joomla! 管理控制面板。



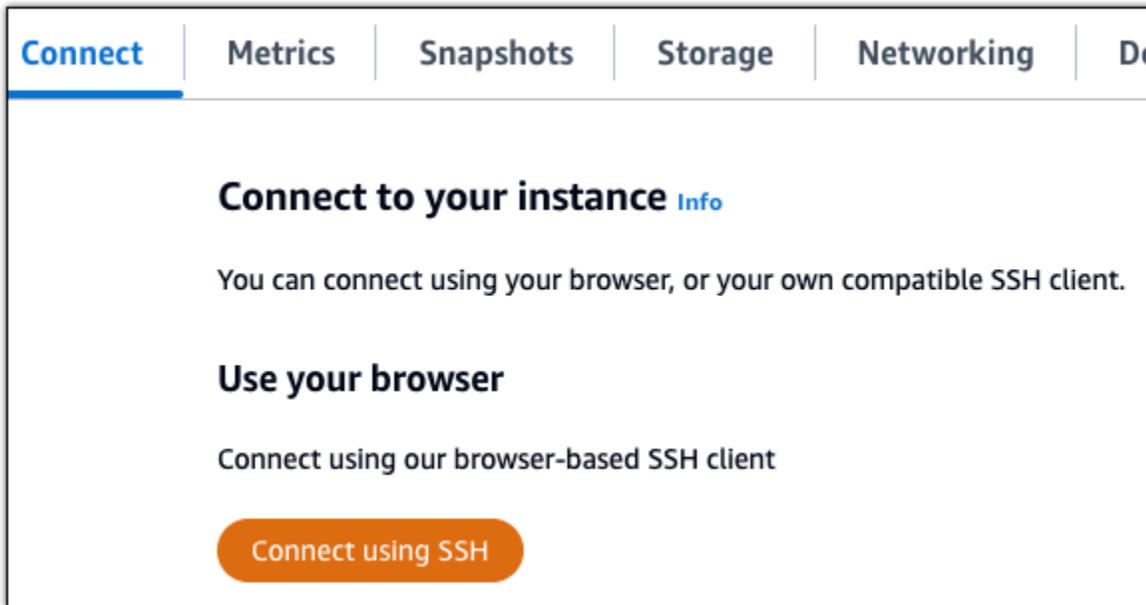
## 步驟 5：將已註冊網域的流量路由至 Joomla! 網站

若要將已註冊網域 (例如 [example.com](http://example.com)) 的流量路由至 Joomla! 網站，請新增記錄至網域的網域名稱系統 (DNS)。DNS 記錄通常會在您註冊網域的註冊商處進行管理和託管。不過，我們建議您將網域 DNS 記錄的管理權限轉移至 Lightsail，以便您可以使用 Lightsail 主控台進行管理。

在 Lightsail 主控台首頁的 [網域和 DNS] 索引標籤下，選擇 [建立 DNS 區域]，然後依照頁面上的指示進行。如需詳細資訊，請參閱[在 Lightsail 中建立 DNS 區域以管理網域的 DNS 記錄](#)。

網域將流量路由至執行個體後，您必須完成以下步驟，以便 Joomla! 軟體知曉該網域名稱。

1. 在執行個體管理頁面的 Connect (連接) 索引標籤下，選擇 Connect using SSH (使用 SSH 連接)。



2. Bitnami 正在修改其許多藍圖的檔案結構。本程序中的檔案路徑可能會因您的 Bitnami 藍圖是使用原生 Linux 系統套件 (方法 A)，還是為獨立安裝 (方法 B) 而異。若要識別您的 Bitnami 安裝類型以及要遵循的方法，請在連線後執行下列命令：

```
test ! -f "/opt/bitnami/common/bin/openssl" && echo "Approach A: Using system packages." || echo "Approach B: Self-contained installation."
```

3. 如果上一個命令的結果表明您應該使用方法 A，請完成以下步驟。如果上一個命令的結果表明您應該使用方法 B，則繼續執行步驟 4。

1. 輸入以下命令，以使用 Vim 開啟 Apache 虛擬主機組態檔案，並為您的網域建立虛擬主機。

```
sudo vim /opt/bitnami/apache2/conf/vhosts/joomla-vhost.conf
```

2. 在 Vim 中按 I 以進入插入模式。
3. 將網域名稱新增到檔案中，如下列範例所示。在此範例中，我們使用 example.com 和 www.example.com 網域。

```
<VirtualHost 127.0.0.1:80_default_:80>
  ServerName www.example.com
  ServerAlias example.com
  DocumentRoot /opt/bitnami/joomla
  <Directory "/opt/bitnami/joomla">
    Options -Indexes +FollowSymLinks -MultiViews
    AllowOverride None
    Require all granted
  </Directory>
  Include "/opt/bitnami/apache/conf/vhosts/htaccess/joomla-htaccess.conf"
</VirtualHost>
```

- 按 ESC 鍵，接著輸入 :wq! 以儲存您的編輯 (寫入)，然後退出 Vim。
- 輸入下列命令，以重新啟動 Apache 伺服器。

```
sudo /opt/bitnami/ctlscript.sh restart apache
```

- 如果上一個命令的結果表明您應該使用方法 B，請完成以下步驟。

- 輸入以下命令，以使用 Vim 開啟 Apache 虛擬主機組態檔案，並為您的網域建立虛擬主機。

```
sudo vim /opt/bitnami/apps/joomla/conf/httpd-vhosts.conf
```

- 在 Vim 中按 I 以進入插入模式。
- 將網域名稱新增到檔案中，如下列範例所示。在此範例中，我們使用 example.com 和 www.example.com 網域。

```
<VirtualHost *:80>
  ServerName example.com
  ServerAlias www.example.com
  ...
```

- 按 ESC 鍵，接著輸入 :wq! 以儲存您的編輯 (寫入)，然後退出 Vim。
- 輸入下列命令，以確認 bitnami-apps-vhosts.conf 檔案包含 Joomla! 的 httpd-vhosts.conf 文件。

```
sudo vim /opt/bitnami/apache2/conf/bitnami/bitnami-apps-vhosts.conf
```

在檔案尋找以下行內容。如果缺少這行內容，請進行新增。

```
Include "/opt/bitnami/apps/joomla/conf/httpd-vhosts.conf"
```

- 輸入下列命令，以重新啟動 Apache 伺服器。

```
sudo /opt/bitnami/ctlscript.sh restart apache
```

若您瀏覽至您為執行個體設定的網域名稱，則會將您重新導向至 Joomla! 網站首頁。接下來，您需要生成並設定 SSL/TLS 憑證以啟用 Joomla! 網站的 HTTPS 連接。如需詳細資訊，請繼續閱讀本指南的下一個章節 [步驟 6：為 Joomla! 網站設定 HTTPS](#)。

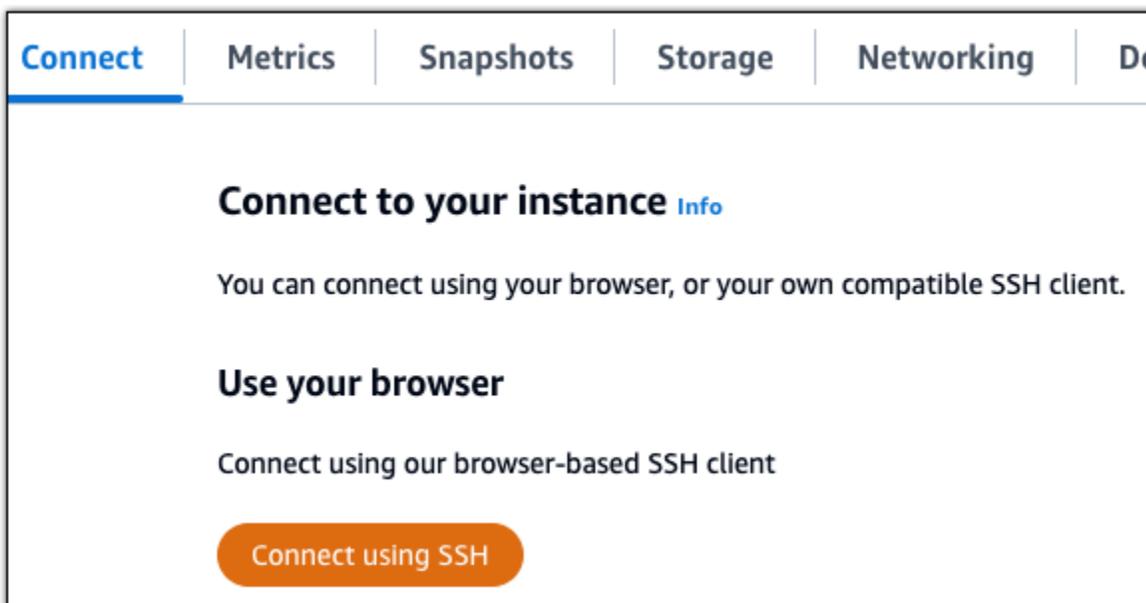
## 步驟 6：為 Joomla! 網站設定 HTTPS

完成下列程序，以在 Joomla! 網站上設定 HTTPS。這些步驟描述了如何使用 Bitnami HTTPS 組態工具 (bncert-tool)，這是一個命令行工具，用於請求 Let's Encrypt SSL/TLS 憑證。如需詳細資訊，請參閱 Bitnami 文件中的 [Learn About The Bitnami HTTPS Configuration Tool](#) (Bitnami HTTPS 組態工具簡介)。

### Important

開始此程序之前，請確認您已將網域設定為將流量路由至 Joomla! 執行個體。否則，SSL/TLS 憑證驗證過程會失敗。

- 在執行個體管理頁面的 Connect (連接) 索引標籤下，選擇 Connect using SSH (使用 SSH 連接)。



- 連接後，輸入下列命令，以確認執行個體已安裝 bncert 工具。

```
sudo /opt/bitnami/bncert-tool
```

您應該會看到下列其中一個回應：

- 如果您看見回應中未找到命令，則表示您的執行個體上未安裝 bncert 工具。繼續此程序的下一個步驟，在您的執行個體上安裝 bncert 工具。
- 如果您在回應中看見 Welcome to the Bitnami HTTPS configuration tool (歡迎使用 Bitnami HTTPS 組態工具)，則您的執行個體上已安裝 bncert 工具。繼續執行此程序的步驟 8。
- 如果您的執行個體已安裝 bncert 工具一段時間，則您可能看到說明該工具已有可用更新版本的訊息。選擇下載該版本，然後輸入 `sudo /opt/bitnami/bncert-tool` 命令以再次執行 bncert 工具。繼續執行此程序的步驟 8。

3. 輸入以下命令，以下載 bncert 執行檔案至您的執行個體。

```
wget -O bncert-linux-x64.run https://downloads.bitnami.com/files/bncert/latest/bncert-linux-x64.run
```

4. 輸入以下命令，以便為執行個體上的 bncert 工具執行檔案建立目錄。

```
sudo mkdir /opt/bitnami/bncert
```

5. 輸入以下命令，以讓 bncert 執行可作為程式執行的檔案。

```
sudo chmod +x /opt/bitnami/bncert/bncert-linux-x64.run
```

6. 輸入以下命令，以在您輸入 `sudo /opt/bitnami/bncert-tool` 命令時建立執行 bncert 工具的符號連結。

```
sudo ln -s /opt/bitnami/bncert/bncert-linux-x64.run /opt/bitnami/bncert-tool
```

您現已在執行個體上完成 bncert 工具安裝。

7. 輸入下列命令，以執行 bncert 工具。

```
sudo /opt/bitnami/bncert-tool
```

8. 輸入主要網域名稱和替代網域名稱，並以空格分隔，如以下範例所示。

如果您的網域未設為將流量路由至執行個體的公有 IP 地址，則 bncert 工具會要求您進行該設定，然後再繼續操作。您的網域必須將流量路由至執行個體的公有 IP 地址，而您需從該地址使

用 `bnccert` 工具來在執行個體上啟用 HTTPS。此舉措會確認您擁有該網域，並以此作為憑證的驗證。

```
-----
Welcome to the Bitnami HTTPS Configuration tool.
-----
Domains

Please provide a valid space-separated list of domains for which you wish to
configure your web server.

Domain list []: example.com www.example.com
```

9. `bnccert` 工具會詢問您要如何設定網站的重新引導。可用的選項如下：

- Enable HTTP to HTTPS redirection (啟用 HTTP 至 HTTPS 重新引導) - 指定將瀏覽至網站 HTTP 版本 (即 `http://example.com`) 的使用者自動重新引導至 HTTPS 版本 (即 `https://example.com`)。由於此選項會強制所有訪客使用加密的連線，建議啟用此選項。輸入 Y，並按 Enter 以啟用。
- Enable non-www to www redirection (啟用非 www 至 www 重新引導) - 指定將瀏覽至網域 (即 `https://example.com`) 頂點的使用者自動重新引導至您網域的 www 子網域 (即 `https://www.example.com`)。建議啟用此選項。不過，如果您已在搜索引擎工具 (如 Google 的網站管理員工具) 中將網域的頂點指定為您偏好的網站地址，或者如果您的頂點直接指向 IP，且 www 子網域透過 CNAME 記錄參考您的頂點，則您可能需要停用此選項並啟用替代選項 (啟用 www 至非 www 重新引導)。輸入 Y，並按 Enter 以啟用。
- Enable www to non-www redirection (啟用 www 至非 www 重新引導) - 指定將瀏覽至您網域 www 子網域 (即 `https://www.example.com`) 的使用者自動重新引導至網域的頂點 (即 `https://example.com`)。如果您已啟用非 www 重新引導至 www，我們建議您停用此選項。輸入 N，並按 Enter (確認) 以停用。

您的選取內容應看起來與下列範例類似。

```
Enable/disable redirections

Please select the redirections you wish to enable or disable on your Bitnami
installation.

Enable HTTP to HTTPS redirection [Y/n]: Y

Enable non-www to www redirection [Y/n]: Y

Enable www to non-www redirection [y/N]: N
```

10. 系統會列出即將進行的變更。輸入 Y，並按 Enter (確認) 以確認並繼續。

```
Changes to perform

The following changes will be performed to your Bitnami installation:

1. Stop web server
2. Configure web server to use a free Let's Encrypt certificate for the domains:
example.com www.example.com
3. Configure a cron job to automatically renew the certificate each month
4. Configure web server name to: example.com
5. Enable HTTP to HTTPS redirection (example: redirect http://example.com to
https://example.com)
6. Enable non-www to www redirection (example: redirect example.com to
www.example.com)
7. Start web server once all changes have been performed

Do you agree to these changes? [Y/n]: Y
```

11. 輸入您的電子郵件地址，以與您的 Let's Encrypt 憑證相關聯，然後按 Enter。

```
Create a free HTTPS certificate with Let's Encrypt

Please provide a valid e-mail address for which to associate your Let's Encrypt
certificate.

Domain list: example.com www.example.com

Server name: example.com

E-mail address []: 
```

12. 檢閱 Let's Encrypt 訂閱者協議。輸入 Y，並按 Enter (確認) 以接受該協議並繼續。

```
The Let's Encrypt Subscriber Agreement can be found at:  
https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf  
Do you agree to the Let's Encrypt Subscriber Agreement? [Y/n]: █
```

執行這些動作是為了在執行個體上啟用 HTTPS，包括請求憑證和設定您指定的重新引導。

```
Performing changes to your installation  
  
The Bitnami HTTPS Configuration Tool will perform any necessary actions to your  
Bitnami installation. This may take some time, please be patient.  
  
█
```

系統已成功核發並驗證您的憑證，如果您看到類似以下範例的訊息，則表示已成功在執行個體上設定重新引導。

```
Success  
  
The Bitnami HTTPS Configuration Tool succeeded in modifying your installation.  
  
The configuration report is shown below.  
  
Backup files:  
* /opt/bitnami/apache2/conf/httpd.conf.back.202005290035  
* /opt/bitnami/apache2/conf/bitnami/bitnami-apps-prefix.conf.back.202005290035  
* /opt/bitnami/apache2/conf/bitnami/bitnami.conf.back.202005290035  
  
Find more details in the log file:  
  
/tmp/bncert-202005290035.log  
  
If you find any issues, please check Bitnami Support forums at:  
  
https://community.bitnami.com  
  
Press [Enter] to continue:█
```

bncert 工具會在憑證過期前每 80 天執行自動續約一次。如果您要搭配執行個體使用其他網域和子網域，且要為這些網域啟用 HTTPS，請重複上述步驟。

您現已在 Joomla! 執行個體上啟用 HTTPS。下次使用您設定的網域瀏覽至 Joomla! 網站時，應該會看到您被重新導向至 HTTPS 連接。

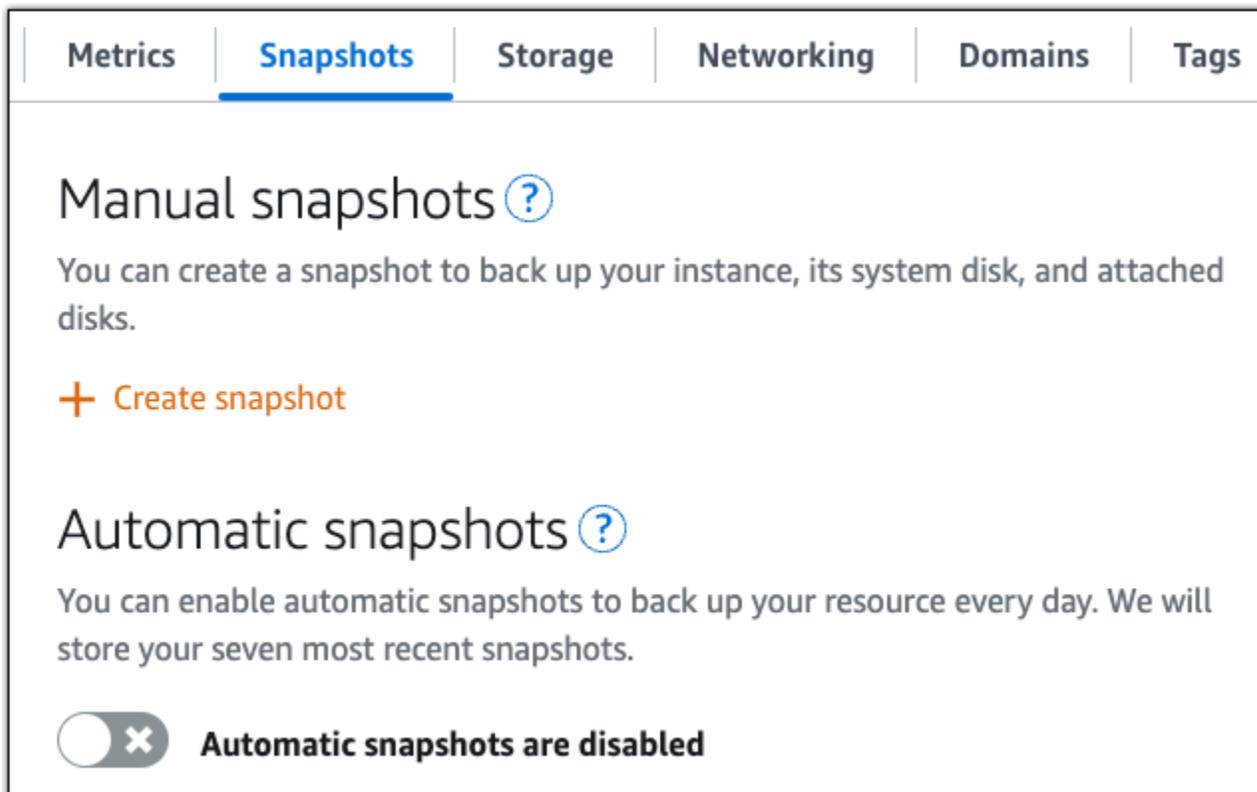
## 步驟 7：閱讀 Joomla! 文件並繼續設定網站

閱讀 Joomla! 文件以了解如何管理和自訂網站。如需詳細資訊，請參閱 [Joomla! 文件](#)。

## 步驟 8：建立執行個體的快照

按照您想要的方式設定 Joomla! 網站後，請定期建立執行個體的快照以作為備份。您可以手動建立快照，或啟用自動快照，讓 Lightsail 為您建立每日快照。若執行個體出現問題，您可以使用快照建立新的替代執行個體。如需詳細資訊，請參閱[快照](#)。

在執行個體管理頁面的 Snapshot (快照) 索引標籤下，選擇 Create a snapshot (建立快照) 或選擇啟用自動快照。



如需詳細資訊，請參閱在 Amazon Lightsail 中建立 [Linux 或 Unix 執行個體的快照](#)或在 [Amazon Lightsail](#) 中[啟用或停用執行個體或磁碟的自動快照](#)。

## 在 Lightsail 上設置燈具堆疊

在您的 LAMP 執行個體在 Amazon Lightsail 上啟動並執行之後，您應採取以下幾個步驟來開始使用：

### 步驟 1：取得 LAMP 執行個體的預設應用程式密碼

您需要預設應用程式密碼以存取執行個體上的預先安裝應用程式或服務。

1. 在執行個體管理頁面的 Connect (連接) 索引標籤下，選擇 Connect using SSH (使用 SSH 連接)。

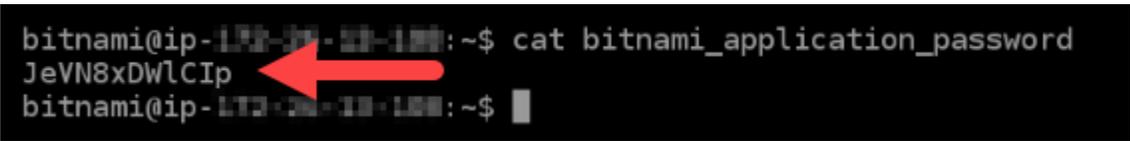
2. 連線後，請輸入下列命令以取得應用程式密碼：

```
cat bitnami_application_password
```

**Note**

若您是在使用者主目錄外的目錄中，則請輸入 `cat $HOME/bitnami_application_password`。

您應該會看到類似如下的回應，其中包含預設應用程式密碼：



```
bitnami@ip-192-0-2-3:~$ cat bitnami_application_password
JeVN8xDWlCIp
bitnami@ip-192-0-2-3:~$
```

如需詳細資訊，請參閱[在 Amazon Lightsail 中取得 Bitnami 執行個體的應用程式使用者名稱和密碼](#)。

## 步驟 2：將靜態 IP 地址連接至 LAMP 執行個體

連接到執行個體的預設動態公有 IP 地址會在每次停止和啟動執行個體時變更。建立靜態 IP 地址並將其連接到執行個體，以防止公有 IP 地址變更。接著，使用網域名稱搭配執行個體時，您不必在每次停止和啟動執行個體時更新網域的 DNS 記錄。您可以將一個靜態 IP 連接至一個執行個體。

在執行個體管理頁面的 Networking (聯網) 索引標籤下，選擇 Create static IP (建立靜態 IP)，接著遵循頁面上的說明。

如需詳細資訊，請參閱[建立靜態 IP 並將其附接至執行個體](#)。

## 步驟 3：瀏覽 LAMP 執行個體歡迎頁面

瀏覽至執行個體的公有 IP 位址，以存取安裝在其上的應用程式 phpMyAdmin、存取或存取 Bitnami 文件。

1. 在執行個體管理頁面的 Connect (連接) 索引標籤下，記下公有 IP。
2. 瀏覽至公有 IP 地址，例如前往 `http://192.0.2.3`。

如需詳細資訊，請參閱[在 Amazon Lightsail 中取得 Bitnami 執行個體的應用程式使用者名稱和密碼](#)。

## 步驟 4：將網域名稱對應至 LAMP 執行個體

若要將網域名稱 (例如 `example.com`) 對應至執行個體，請新增記錄至網域的網域名稱系統 (DNS)。DNS 記錄通常會在您註冊網域的註冊商處進行管理和託管。不過，我們建議您將網域 DNS 記錄的管理權限轉移至 Lightsail，以便您可以使用 Lightsail 主控台進行管理。

在 Lightsail 主控台首頁的 [網域和 DNS] 索引標籤下，選擇 [建立 DNS 區域]，然後依照頁面上的指示進行。

如需詳細資訊，請參閱[在 Lightsail 中建立 DNS 區域以管理網域的 DNS 記錄](#)。

## 步驟 5：閱讀 Bitnami 文件

閱讀 Bitnami 文件以了解如何部署應用程式、藉由 SSL 憑證啟用 HTTPS 支援、藉由 SFTP 上傳檔案到伺服器。

如需詳細資訊，請參閱[Bitnami LAMP for AWS 雲端](#)。

## 步驟 6：建立 LAMP 執行個體的快照

快照是執行個體之系統磁碟和原始組態的複本。快照包含的資訊有記憶體、CPU、磁碟大小和資料傳輸率。您可以使用快照做為新執行個體的基準，或做為資料備份。

在執行個體管理頁面的 Snapshot (快照) 索引標籤下方，輸入快照的名稱，接著選擇 Create snapshot (建立快照)。

如需詳細資訊，請參閱[建立 Linux 或 Unix 執行個體的快照](#)。

## 在 Lightsail 上設置和配置

在您的 Magento 執行個體在 Amazon Lightsail 上啟動並執行之後，您應該完成以下幾個步驟才能開始使用。

### 內容

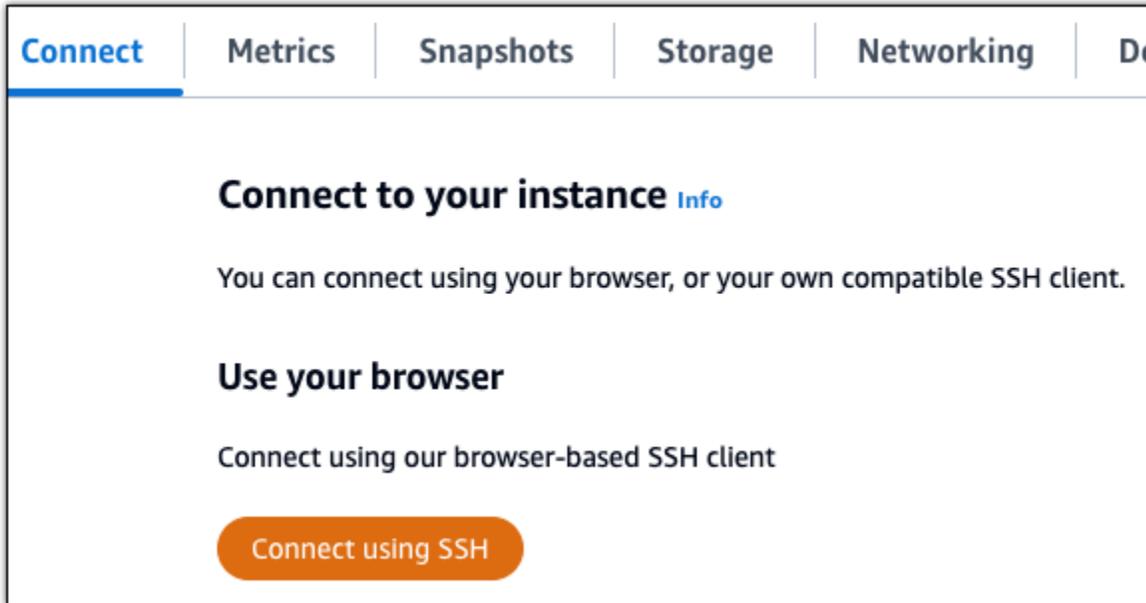
- [步驟 1：取得 Magento 網站的預設應用程式密碼](#)
- [步驟 2：將靜態 IP 地址連接至 Magento 執行個體](#)
- [步驟 3：登入 Magento 網站的管理儀表板](#)
- [步驟 4：將已註冊網域的流量路由至 Magento 網站](#)
- [步驟 5：為 Magento 網站設定 HTTPS](#)
- [步驟 6：為電子郵件通知設定 SMTP](#)

- [步驟 7：閱讀 Bitnami 和 Magento 文件](#)
- [步驟 8：建立 Magento 執行個體的快照](#)

## 步驟 1：取得 Magento 網站的預設應用程式密碼

請完成以下步驟，以取得 Magento 網站的預設應用程式密碼。如需詳細資訊，請參閱在 [Amazon Lightsail](#) 中取得 Bitnami 執行個體的應用程式使用者名稱和密碼。

1. 在執行個體管理頁面的 Connect (連接) 索引標籤下，選擇 Connect using SSH (使用 SSH 連接)。



2. 連線後，請輸入下列命令以取得預設應用程式密碼：

```
cat $HOME/bitnami_application_password
```

您應該會看到類似於以下範例的回應，其中包含預設應用程式密碼。請將此密碼存放在安全處。在本教學課程的下一節中，您會需要使用該密碼來登入 Magento 網站的管理儀表板。

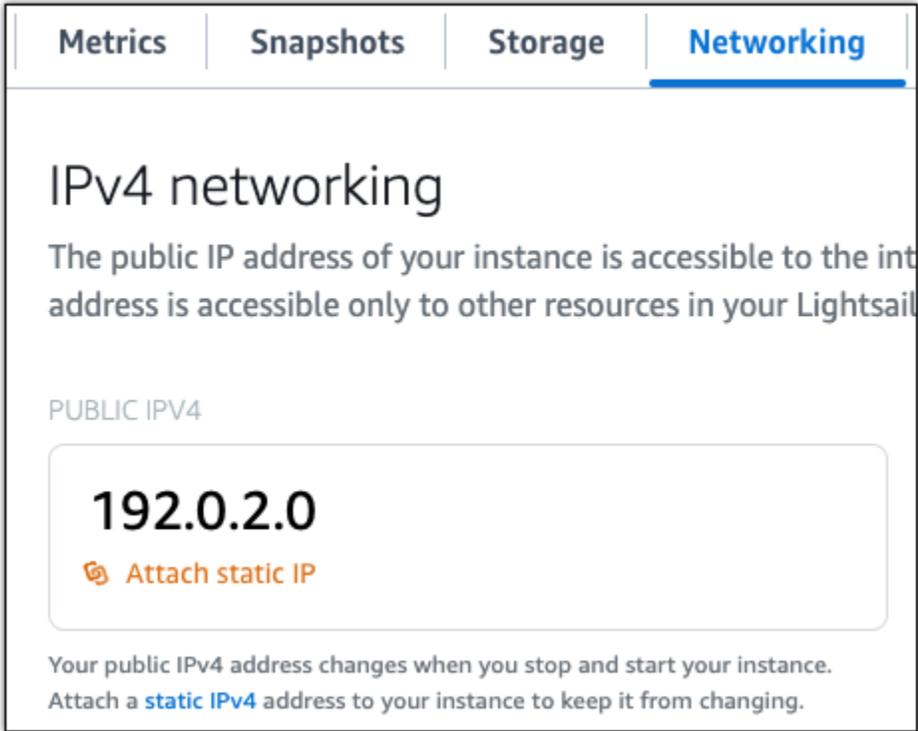
```
bitnami@ip-172-31-18-100:~$ cat bitnami_application_password
JeVN8xDWlCIp
bitnami@ip-172-31-18-100:~$
```

## 步驟 2：將靜態 IP 地址連接至 Magento 執行個體

您第一次建立執行個體時，所指派的公有 IP 地址將會在每次停用和啟用執行個體時變更。您應該建立靜態 IP 地址並將其連接至執行個體，以確保其公有 IP 地址不會變更。當您將註冊的網域名稱 (例如

example.com) 與執行個體搭配使用時，便無須在每次停用或啟用執行個體時更新網域的 DNS 記錄。您可以將一個靜態 IP 連接至一個執行個體。

在執行個體管理頁面的 Networking#(聯網) 索引標籤下，選擇 Create a static IP (建立靜態 IP) 或 Attach static IP (連接靜態 IP)(若您先前已建立可以連接至執行個體的靜態 IP)，然後遵循頁面上的指示執行操作。如需詳細資訊，請參閱[建立靜態 IP 並將其附接至執行個體](#)。



The screenshot shows the 'Networking' tab selected in the Amazon Lightsail console. The main heading is 'IPv4 networking'. Below it, there is a brief explanation: 'The public IP address of your instance is accessible to the internet. A private IP address is accessible only to other resources in your Lightsail instance.' Underneath, it says 'PUBLIC IPV4' and displays the IP address '192.0.2.0' in a large font. Below the IP address is an orange button with a plug icon and the text 'Attach static IP'. At the bottom, there is a note: 'Your public IPv4 address changes when you stop and start your instance. Attach a static IPv4 address to your instance to keep it from changing.'

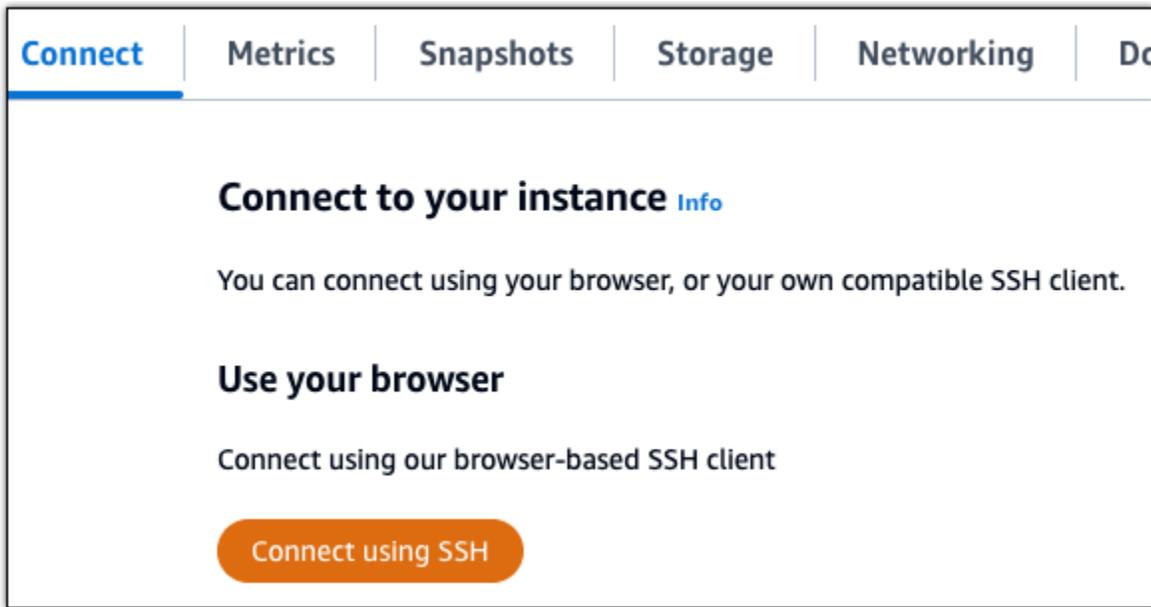
將新的靜態 IP 地址連接至執行個體後，您必須完成以下步驟，以便 Magento 軟體知曉新的靜態 IP 地址。

1. 請記下執行個體的靜態 IP 地址。這會列在執行個體管理頁面的標頭區段中。



The screenshot shows a header section with two columns. The left column is titled 'Static IP address' and shows a blue plug icon followed by the IP address '203.0.113.0'. The right column is titled 'Instance status' and shows a green checkmark icon followed by the word 'Running'.

2. 在執行個體管理頁面的 Connect (連接) 索引標籤下，選擇 Connect using SSH (使用 SSH 連接)。



3. 連接後，請輸入以下命令。請務必以執行個體的新靜態 IP 地址取代 *<StaticIP>*。

```
sudo /opt/bitnami/configure_app_domain --domain <StaticIP>
```

範例：

```
sudo /opt/bitnami/configure_app_domain --domain 203.0.113.0
```

您應該會看到類似於以下範例的回應。Magento 軟體現在應該已知曉新的靜態 IP 地址。

```
bitnami@ip-173-33-0-107:~$ sudo /opt/bitnami/configure_app_domain --domain 203.0.113.0
Configuring domain to 203.0.113.0
2021-03-12T15:49:22.000Z - info: Saving configuration info to disk
prestashop 15:49:22.41 INFO ==> Trying to connect to the database server
prestashop 15:49:22.44 INFO ==> Updating hostname in database
prestashop 15:49:22.46 INFO ==> Purging cache
Disabling automatic domain update for IP address changes
```

#### Note

Magento 目前不支援 IPv6 地址。您可以為執行個體啟用 IPv6，但 Magento 軟體不會回應透過 IPv6 網路提出的請求。

## 步驟 3：登入 Magento 網站的管理儀表板

請完成以下步驟，以存取 Magento 網站和登入其管理儀表板。若要登入，請使用預設使用者名稱 (user) 和您先前依本指南指示取得的預設應用程式密碼。

1. 在 Lightsail 主控台中，記下執行個體管理頁面標頭區域中列出的公用或靜態 IP 位址。



2. 瀏覽至以下地址，以存取 Magento 網站管理儀表板的登入頁面。請務必將 `<InstanceIpAddress>` 取代為執行個體的公用或靜態 IP 位址。

```
http://<InstanceIpAddress>/admin
```

範例：

```
http://203.0.113.0/admin
```

### Note

如果無法存取 Magento 管理儀表板的登入頁面，您可能需要重新啟動執行個體。

3. 輸入預設的使用者名稱 (user)，以及您先前依本指南指示取得的預設應用程式密碼，然後選擇 Sign in (登入)。



您會看到 Magento 管理儀表板。

One or more of the Cache Types are invalidated: Configuration. Please go to [Cache Management](#) and refresh cache. System Messages: 1

## Dashboard

Scope: All Store Views ? [Reload Data](#)

All other open sessions for this account were terminated.

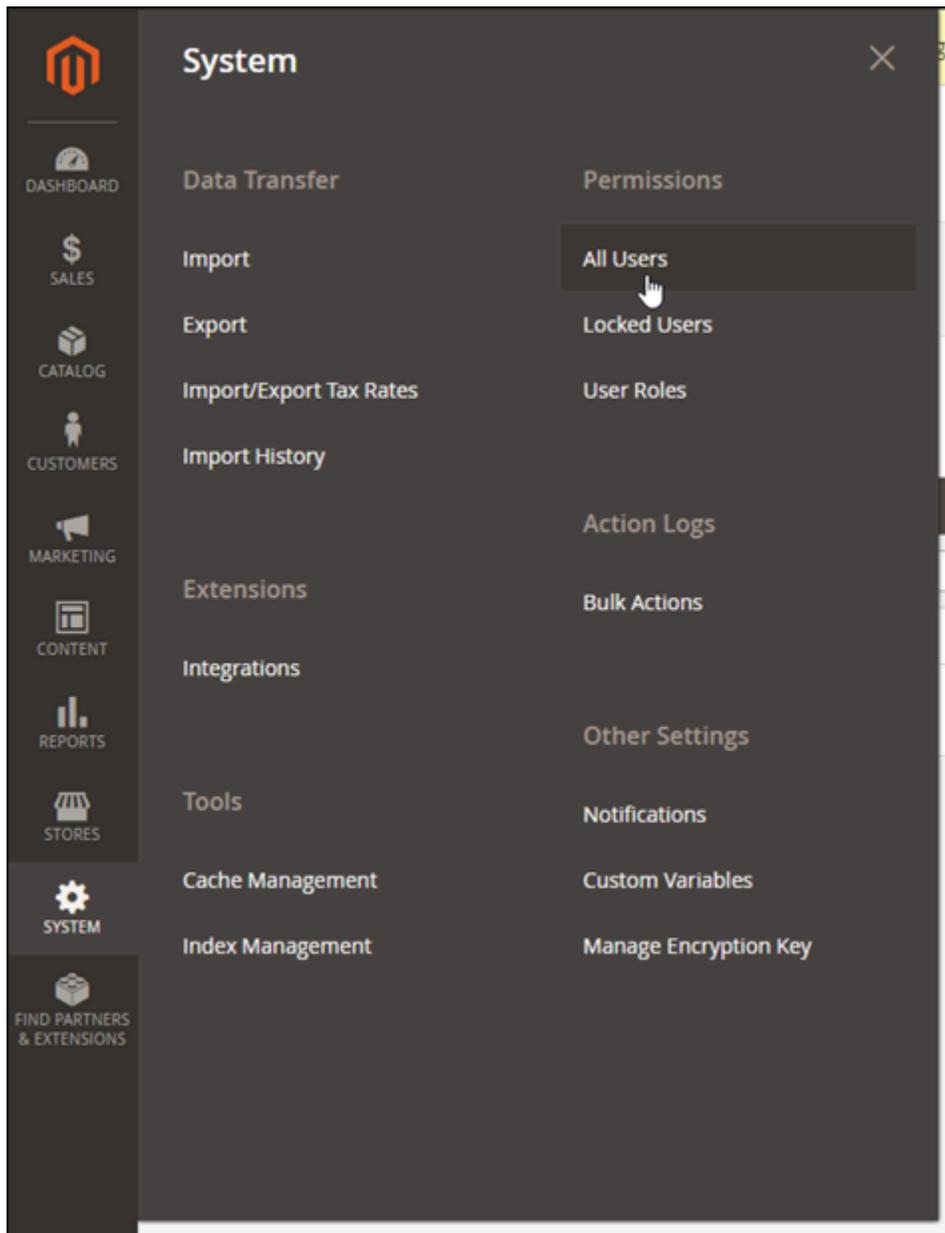
### Advanced Reporting

Gain new insights and take command of your business' performance, using our dynamic product, order, and customer reports tailored to your customer data. [Go to Advanced Reporting](#)

<b>Lifetime Sales</b>	Chart is disabled. To enable the chart, click <a href="#">here</a> .			
<b>\$0.00</b>	Revenue	Tax	Shipping	Quantity
	<b>\$0.00</b>	<b>\$0.00</b>	<b>\$0.00</b>	<b>0</b>

<b>Average Order</b>				
<b>\$0.00</b>				

若要變更您用來登入 Magento 網站管理儀表板的預設使用者名稱或密碼，請選擇導覽窗格中的 System (系統)，然後選擇 All Users (所有使用者)。如需詳細資訊，請參閱 Magento 文件中的 [Adding users](#) (新增使用者)。



如需有關管理儀表板的詳細資訊，請參閱 [Magento 2.4 User Guide](#) (《Magento 2.4 版使用者指南》)。

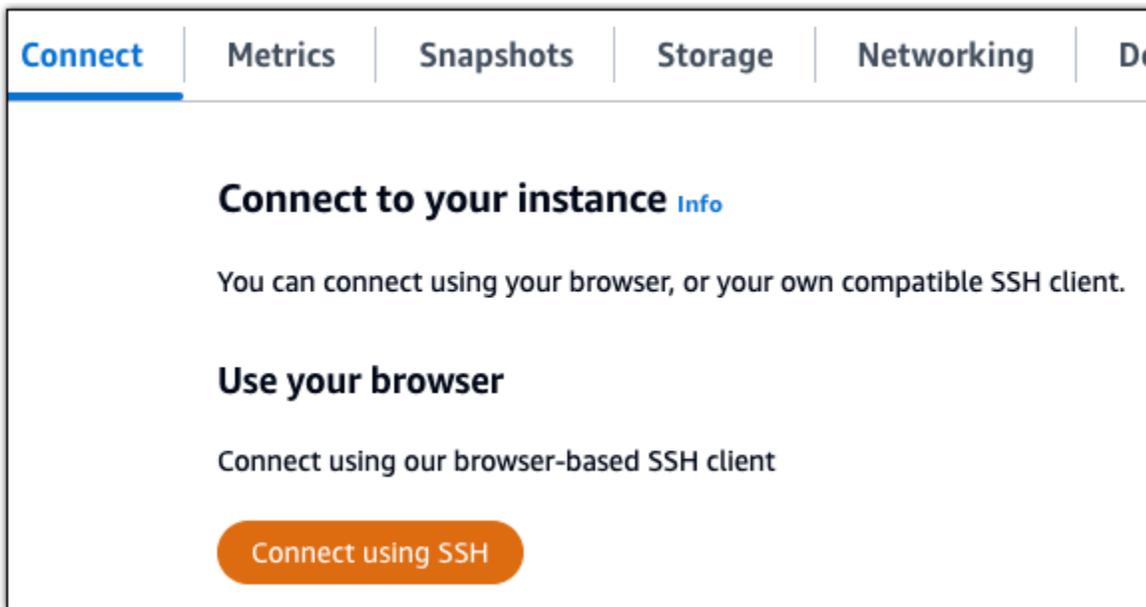
#### 步驟 4：將已註冊網域的流量路由至 Magento 網站

若要將已註冊網域名稱 (例如：example.com) 的流量路由至 Magento 網站，請新增紀錄至您網域的網域名稱系統 (DNS)。DNS 記錄通常會在您註冊網域的註冊商處進行管理和託管。不過，我們建議您將網域 DNS 記錄的管理權限轉移至 Lightsail，以便您可以使用 Lightsail 主控台進行管理。

在 Lightsail 主控台首頁的 [網域和 DNS] 索引標籤下，選擇 [建立 DNS 區域]，然後依照頁面上的指示進行。如需詳細資訊，請參閱[在 Lightsail 中建立 DNS 區域以管理網域的 DNS 記錄](#)。

網域將流量路由至執行個體後，您必須完成以下步驟，以便 Magento 軟體知曉該網域名稱。

1. 在執行個體管理頁面的 Connect (連接) 索引標籤下，選擇 Connect using SSH (使用 SSH 連接)。



2. 連接後，請輸入以下命令。請務必將 `< DomainName >` 取代為將流量轉送至執行個體的網域名稱。

```
sudo /opt/bitnami/configure_app_domain --domain <DomainName>
```

範例：

```
sudo /opt/bitnami/configure_app_domain --domain www.example.com
```

您應該會看到類似於以下範例的回應。Magento 軟體現在應該已知曉該網域名稱。

```
bitnami@ip-172-31-0-157:~$ sudo /opt/bitnami/configure_app_domain --domain www.example.com
Configuring domain to www.example.com
2021-03-12T15:49:22.000Z - info: Saving configuration info to disk
prestashop 15:49:22.41 INFO ==> Trying to connect to the database server
prestashop 15:49:22.44 INFO ==> Updating hostname in database
prestashop 15:49:22.46 INFO ==> Purging cache
Disabling automatic domain update for IP address changes
```

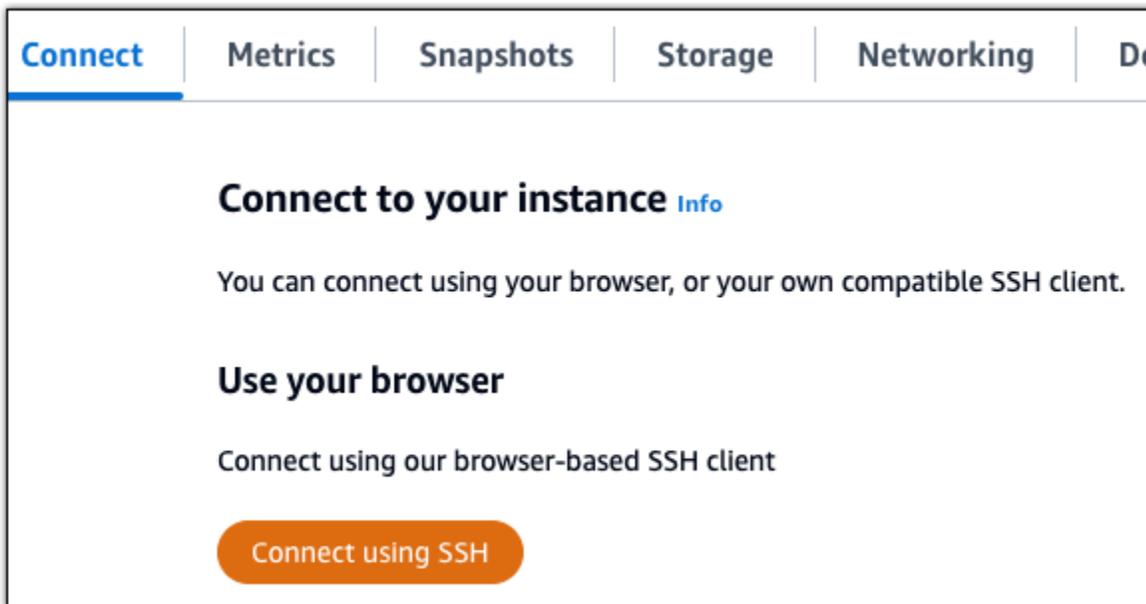
## 步驟 5：為 Magento 網站設定 HTTPS

完成以下步驟，以在 Magento 網站上設定 HTTPS。我們會在這些步驟中展示如何使用 Bitnami HTTPS 組態工具 (bncert)，這是用來請求 SSL/TLS 憑證、設定重新引導 (例如 HTTP 至 HTTPS) 以及更新憑證的命令列工具。

### ⚠ Important

bncert 工具只會向目前正將流量路由至 Magento 執行個體公有 IP 地址的網域核發憑證。在開始執行這些步驟之前，請先確定您已將 DNS 紀錄新增至要與 Magento 網站搭配使用的所有網域其 DNS 中。

1. 在執行個體管理頁面的 Connect (連接) 索引標籤下，選擇 Connect using SSH (使用 SSH 連接)。



2. 連接後，請輸入以下命令來啟動 bncert 工具。

```
sudo /opt/bitnami/bncert-tool
```

您應該會看到類似於以下範例的回應：

```
bitnami@ip-172-31-3-149:~$ sudo /opt/bitnami/bncert-tool
Warning: Custom redirections are not supported in the Bitnami Magento Stack.
This tool will not be able to enable/disable redirections.
Press [Enter] to continue:
```

3. 輸入主要網域名稱和替代網域名稱，並以空格分隔，如以下範例所示。

```
-----  
Welcome to the Bitnami HTTPS Configuration tool.  
-----  
Domains  
Please provide a valid space-separated list of domains for which you wish to  
configure your web server.  
Domain list []: example.com www.example.com
```

4. 系統會列出即將進行的變更。輸入 Y，並按 Enter (確認) 以確認並繼續。

```
-----  
Changes to perform  
The following changes will be performed to your Bitnami installation:  
1. Stop web server  
2. Configure web server to use a free Let's Encrypt certificate for the domains:  
   example.com www.example.com  
3. Configure a cron job to automatically renew the certificate each month  
4. Configure web server name to: example.com  
5. Start web server once all changes have been performed  
Do you agree to these changes? [Y/n]: Y
```

5. 輸入您的電子郵件地址，以與您的 Let's Encrypt 憑證相關聯，然後按 Enter。

```
Create a free HTTPS certificate with Let's Encrypt  
Please provide a valid e-mail address for which to associate your Let's Encrypt  
certificate.  
Domain list: example.com www.example.com  
Server name: example.com  
E-mail address []: 
```

6. 檢閱 Let's Encrypt 訂閱者協議。輸入 Y，並按 Enter (確認) 以接受該協議並繼續。

```
The Let's Encrypt Subscriber Agreement can be found at:  
https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf  
Do you agree to the Let's Encrypt Subscriber Agreement? [Y/n]: 
```

執行這些動作是為了在執行個體上啟用 HTTPS，包括請求憑證和設定您指定的重新引導。

```
Performing changes to your installation

The Bitnami HTTPS Configuration Tool will perform any necessary actions to your
Bitnami installation. This may take some time, please be patient.

|█
```

系統已成功核發並驗證您的憑證，如果您看到類似以下範例的訊息，則表示已成功在執行個體上設定重新引導。

```
Success

The Bitnami HTTPS Configuration Tool succeeded in modifying your installation.

The configuration report is shown below.

Backup files:
* /opt/bitnami/apache/conf/httpd.conf.back.202104052147
* /opt/bitnami/apache/conf/bitnami/bitnami.conf.back.202104052147
* /opt/bitnami/apache/conf/bitnami/bitnami-ssl.conf.back.202104052147
* /opt/bitnami/apache/conf/vhosts/magento-https-vhost.conf.back.202104052147
* /opt/bitnami/apache/conf/vhosts/magento-vhost.conf.back.202104052147

Find more details in the log file:

/tmp/bncert-202104052147.log

If you find any issues, please check Bitnami Support forums at:

https://community.bitnami.com

Press [Enter] to continue:

bitnami@ip-172-31-3-143:~$ █
```

bncert 工具會在憑證過期前每 80 天執行自動續約一次。繼續執行下一組步驟，以順利在 Magento 網站上完成 HTTPS 的啟用。

7. 瀏覽至以下地址，以存取 Magento 網站管理儀表板的登入頁面。請務必將 *< DomainName >* 取代為將流量轉送至執行個體的已註冊網域名稱。

```
http://<DomainName>/admin
```

範例：

```
http://www.example.com/admin
```

- 輸入預設的使用者名稱 (user)，以及您先前依本指南指示取得的預設應用程式密碼，然後選擇 Sign in (登入)。



The screenshot shows the Magento login interface. At the top left is the Magento logo. Below it, the text "Welcome, please sign in" is displayed in orange. There are two input fields: "Username \*" with the value "user" and "Password \*" with a masked password represented by asterisks. Below the password field is a blue link that says "Forgot your password?". At the bottom of the form is a blue "Sign in" button with a white mouse cursor pointing to it.

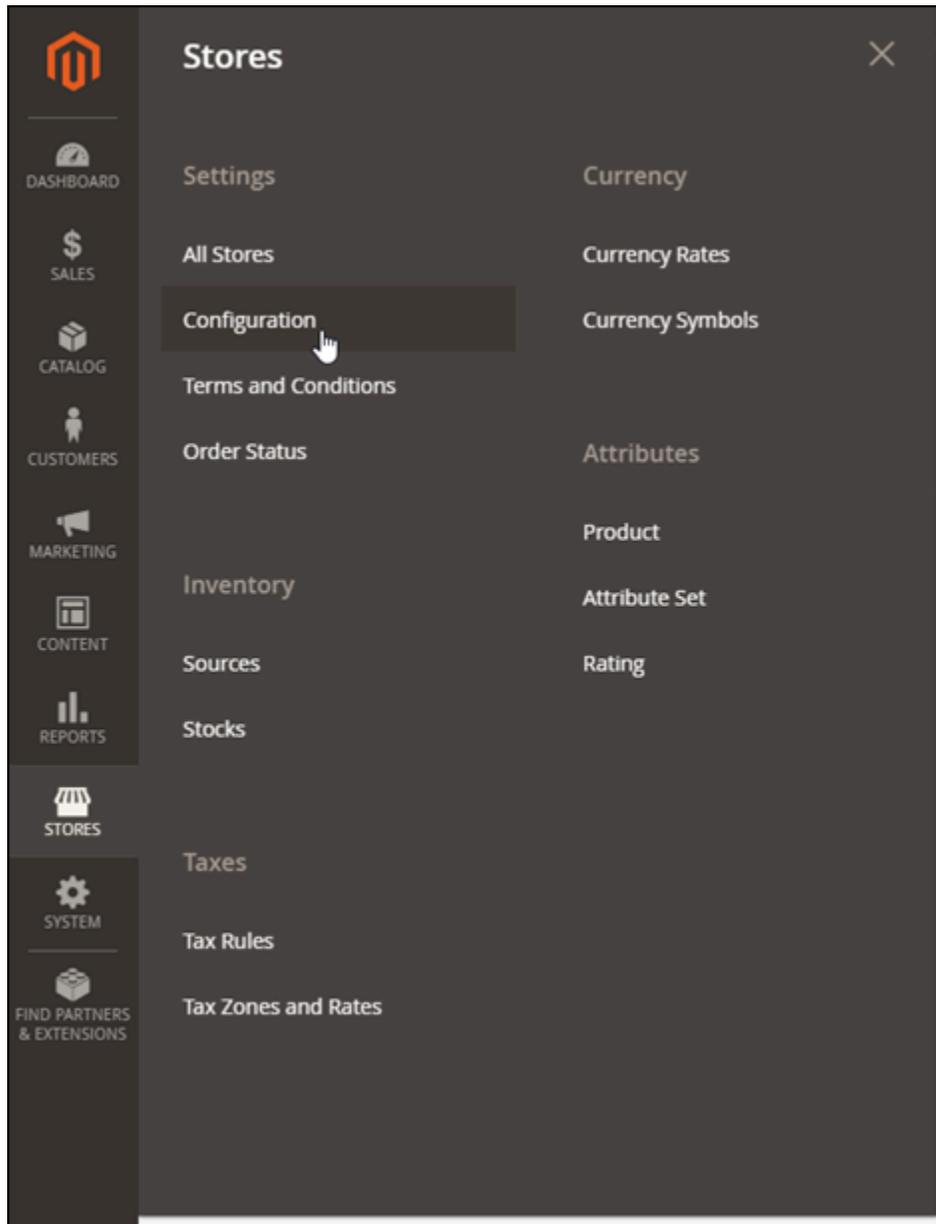
您會看到 Magento 管理儀表板。

The screenshot shows the Amazon Lightsail dashboard interface. At the top, a yellow system message banner states: "One or more of the Cache Types are invalidated: Configuration. Please go to [Cache Management](#) and refresh cache types." To the right of this message is a "System Messages: 1" dropdown. Below the banner is the "Dashboard" title, a search icon, a notification bell with a red "1", and a user profile icon labeled "user". A "Scope: All Store Views" dropdown with a help icon and a "Reload Data" button are also present. Another yellow banner below reads: "All other open sessions for this account were terminated." The "Advanced Reporting" section includes a description: "Gain new insights and take command of your business' performance, using our dynamic product, order, and customer reports tailored to your customer data." and a "Go to Advanced Reporting" button. The "Lifetime Sales" section shows a total of "\$0.00" and a note: "Chart is disabled. To enable the chart, click [here](#)." Below this is a table with the following data:

	Revenue	Tax	Shipping	Quantity
<b>Lifetime Sales</b>	\$0.00	\$0.00	\$0.00	0
<b>Average Order</b>	\$0.00	\$0.00	\$0.00	0

The left sidebar contains navigation icons for Dashboard, Sales, Catalog, Customers, Marketing, Content, Reports, Stores, and System.

9. 在導覽窗格中，選擇 Stores (儲存)，然後選擇 Configuration (組態)。



10. 選擇 Web，然後展開 Base URLs (基本 URL) 節點。
11. 在 Base URLs (基本 URL) 文字方框中，輸入您網站的完整 URL，例如 `https://www.example.com/`。

**Base URLs**

Any of the fields allow fully qualified URLs that end with '/' (slash) e.g. `http://example.com/magento/`

**Base URL**  
[store view]   
Specify URL or `{{base_url}}` placeholder.

**Base Link URL**  
[store view]   Use system value  
May start with `{{unsecure_base_url}}` placeholder.

**Base URL for Static View Files**  
[store view]   
May be empty or start with `{{unsecure_base_url}}` placeholder.

**Base URL for User Media Files**  
[store view]   
May be empty or start with `{{unsecure_base_url}}` placeholder.

12. 展開 Base URLs (Secure) (基本 URL (安全)) 節點。

13. 在 Secure Base URL (安全的基本 URL) 文字方框中，輸入您網站的完整 URL，例如 `https://www.example.com/`。

**Base URLs (Secure)**

Any of the fields allow fully qualified URLs that end with '/' (slash) e.g. `https://example.com/magento/`

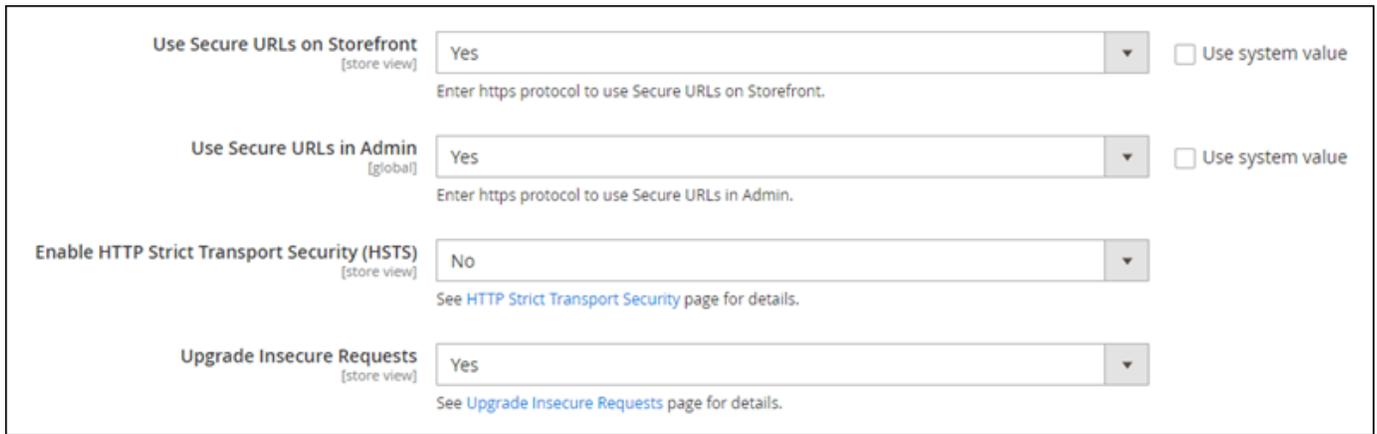
**Secure Base URL**  
[store view]   
Specify URL or `{{base_url}}`, or `{{unsecure_base_url}}` placeholder.

**Secure Base Link URL**  
[store view]   Use system value  
May start with `{{secure_base_url}}` or `{{unsecure_base_url}}` placeholder.

**Secure Base URL for Static View Files**  
[store view]   
May be empty or start with `{{secure_base_url}}`, or `{{unsecure_base_url}}` placeholder.

**Secure Base URL for User Media Files**  
[store view]   
May be empty or start with `{{secure_base_url}}`, or `{{unsecure_base_url}}` placeholder.

14. 在 Use Secure URLs on Storefront (在 Storefront 中使用安全的 URL)、Use Secure URLs in Admin (以管理員身分使用安全的 URL) 和 Upgrade Insecure Requests (升級不安全的請求) 等選項中選擇 Yes (是)。



The screenshot shows a configuration interface with four rows of settings:

- Use Secure URLs on Storefront** [store view]: A dropdown menu is set to "Yes". Below it is a text input field containing "https" and a note: "Enter https protocol to use Secure URLs on Storefront." To the right is an unchecked checkbox labeled "Use system value".
- Use Secure URLs in Admin** [global]: A dropdown menu is set to "Yes". Below it is a text input field containing "https" and a note: "Enter https protocol to use Secure URLs in Admin." To the right is an unchecked checkbox labeled "Use system value".
- Enable HTTP Strict Transport Security (HSTS)** [store view]: A dropdown menu is set to "No". Below it is a note: "See [HTTP Strict Transport Security](#) page for details."
- Upgrade Insecure Requests** [store view]: A dropdown menu is set to "Yes". Below it is a note: "See [Upgrade Insecure Requests](#) page for details."

15. 在頁面頂端選擇 Save Config (儲存設定)。

現在已為 Magento 網站設定 HTTPS。當客戶瀏覽至 Magento 網站的 HTTP 版本時 (例如：<http://www.example.com>)，系統會自動將他們重新導向至 HTTPS 版本 (例如：<https://www.example.com>)。

## 步驟 6：為電子郵件通知設定 SMTP

設置 Magento 網站的 SMTP 設定，以便為其啟用電子郵件通知。如需詳細資訊，請參閱 Bitnami 文件中的 [Install the Magento Magepal SMTP extension](#) (安裝 Magento Magepal SMTP 擴充功能)。

### Important

如果您將 SMTP 設定為使用通訊埠 25、465 或 587，則必須在 Lightsail 主控台的執行個體防火牆中開啟這些連接埠。如需詳細資訊，請參閱 [在 Amazon Lightsail 中新增和編輯執行個體防火牆規則](#)。

若您將 Gmail 帳戶設定為在 Magento 網站上傳送電子郵件，則您必須使用應用程式密碼，而非使用用來登入 Gmail 的標準密碼。如需詳細資訊，請參閱 [以應用程式密碼登入](#)。

## 步驟 7：閱讀 Bitnami 和 Magento 文件

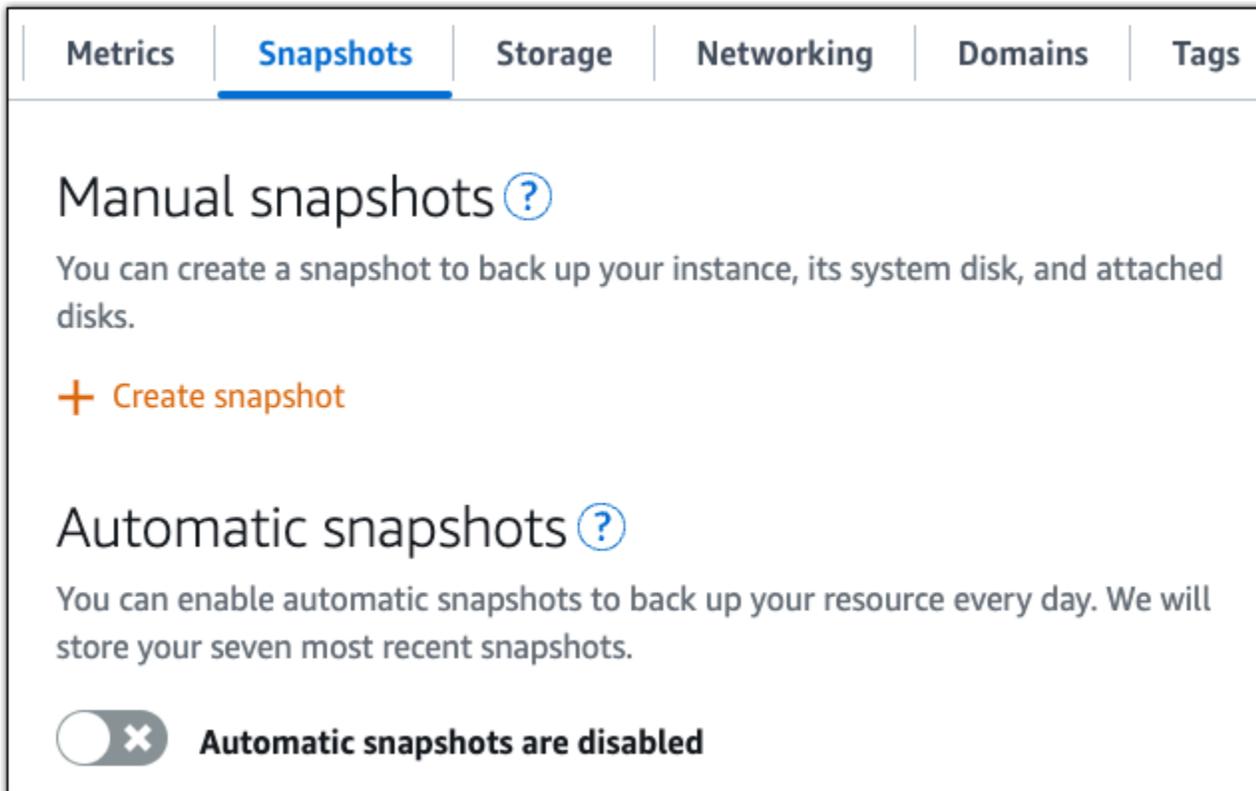
閱讀 Bitnami 文件以了解如何在 Magento 執行個體和網站上執行管理任務，例如：安裝外掛程式和自訂主題。如需詳細資訊，請參閱 Bitnami 文件中的 [Bitnami Magento Stack for AWS Cloud](#) (適用於 AWS 雲端的 Bitnami Magento Stack)。

您也應該閱讀 Magento 文件，以了解如何管理 Magento 網站。如需詳細資訊，請參閱 [Magento 2.4 User Guide](#) (《Magento 2.4 版使用者指南》)。

## 步驟 8：建立 Magento 執行個體的快照

按照您希望的方式設定 Magento 網站後，請定期建立執行個體的快照以作為備份。您可以手動建立快照，或啟用自動快照，讓 Lightsail 為您建立每日快照。若執行個體出現問題，您可以使用快照建立新的替代執行個體。如需詳細資訊，請參閱[快照](#)。

在執行個體管理頁面的 Snapshot (快照) 索引標籤下，選擇 Create a snapshot (建立快照) 或選擇啟用自動快照。



如需詳細資訊，請參閱在 Amazon Lightsail 中建立 [Linux 或 Unix 執行個體的快照](#)或在 [Amazon Lightsail](#) 中[啟用或停用執行個體或磁碟的自動快照](#)。

## 在 Lightsail 上部署和管理 Nginx 網路伺服器

在您的 Nginx 執行個體在 Amazon Lightsail 上啟動並執行之後，您應該採取以下幾個步驟來開始使用：

### 步驟 1：取得 Nginx 執行個體的預設應用程式密碼

您需要預設應用程式密碼以存取執行個體上的預先安裝應用程式或服務。

1. 在執行個體管理頁面的 [Connect] 索引標籤下，選擇 [Connect 方式] SSH。

2. 連線後，請輸入下列命令以取得預設應用程式密碼：

```
cat bitnami_application_password
```

**Note**

若您是在使用者主目錄外的目錄中，則請輸入 `cat $HOME/bitnami_application_password`。

您應該會看到類似如下的回應，其中包含預設應用程式密碼：

```
bitnami@ip-192-0-2-3:~$ cat bitnami_application_password
JeVN8xDWlCIp
bitnami@ip-192-0-2-3:~$
```

如需詳細資訊，請參閱[在 Amazon Lightsail 中取得 Bitnami 執行個體的應用程式使用者名稱和密碼](#)。

## 步驟 2：將靜態 IP 地址連接至 Nginx 執行個體

連接到執行個體的預設動態公有 IP 地址會在每次停止和啟動執行個體時變更。建立靜態 IP 地址並將其連接到執行個體，以防止公有 IP 地址變更。稍後，當您將網域名稱用於執行個體時，每次停止並啟動執行個體時，就不必更新網域的 DNS 記錄。您可以將一個靜態 IP 連接至一個執行個體。

在執行個體管理頁面的 [網域與 DNS] 索引標籤下，選擇 [建立靜態 IP]，然後依照頁面上的指示操作。

如需詳細資訊，請參閱[建立靜態 IP 並將其附加至 Lightsail 中的執行個體](#)。

## 步驟 3：瀏覽 Nginx 執行個體歡迎頁面

瀏覽至執行個體的公用 IP 位址，以存取安裝在其上的應用程式 phpMyAdmin、存取或存取 Bitnami 文件。

1. 在執行個體管理頁面的 Connect (連接) 索引標籤下，記下公有 IP。
2. 瀏覽至公有 IP 地址，例如前往 `http://192.0.2.3`。

如需詳細資訊，請參閱[在 Amazon Lightsail 中取得 Bitnami 執行個體的應用程式使用者名稱和密碼](#)。

## 步驟 4：將網域名稱對應至 Nginx 執行個體

若要將網域名稱 (例如) 對應至執行個體，請將記錄新增至網域的網域名稱系統 (DNS)。example.com DNS 記錄通常在您註冊網域的註冊商處進行管理和託管。不過，我們建議您將網域 DNS 記錄的管理轉移至 Lightsail，以便您可以使用 Lightsail 主控台進行管理。

在 Lightsail 主控台首頁的 [網路功能] 索引標籤下，選擇 [建立 DNS 區域]，然後依照頁面上的指示進行。

如需詳細資訊，請參閱 [建立 DNS 區域以管理網域 DNS 記錄](#)。

## 步驟 5：閱讀 Bitnami 文件

閱讀 Bitnami 文檔以了解如何部署 Nginx 應用程式，啟用 SSL 證書 HTTPS 支持，使用將文件上傳到服務器 SFTP 等。

如需詳細資訊，請參閱 [Bitnami Nginx for AWS 雲端](#)。

## 步驟 6：建立 Nginx 執行個體的快照

快照是執行個體之系統磁碟和原始組態的複本。快照包括記憶體 CPU、磁碟大小和資料傳輸速率等資訊。您可以使用快照做為新執行個體的基準，或做為資料備份。

在執行個體管理頁面的 Snapshot (快照) 索引標籤下方，輸入快照的名稱，接著選擇 Create snapshot (建立快照)。

如需詳細資訊，請參閱 [建立 Linux 或 Unix 執行個體的快照](#)。

## 在 Lightsail 上開始使用 Node.js

在您的 Node.js 執行個體在 Amazon Lightsail 上啟動並執行之後，您應該採取以下幾個步驟來開始使用：

### 步驟 1：取得 Node.js 執行個體的預設應用程式密碼

您需要預設應用程式密碼以存取執行個體上的預先安裝應用程式或服務。

1. 在執行個體管理頁面的 Connect (連接) 索引標籤下，選擇 Connect using SSH (使用 SSH 連接)。
2. 連線後，請輸入下列命令以取得預設應用程式密碼：

```
cat bitnami_application_password
```

### Note

若您是在使用者主目錄外的目錄中，則請輸入 `cat $HOME/bitnami_application_password`。

您應該會看到類似如下的回應，其中包含預設應用程式密碼：

```
bitnami@ip-192-0-2-3:~$ cat bitnami_application_password
JeVN8xDWlCIp
bitnami@ip-192-0-2-3:~$
```

如需詳細資訊，請參閱[在 Amazon Lightsail 中取得 Bitnami 執行個體的應用程式使用者名稱和密碼](#)。

## 步驟 2：將靜態 IP 地址連接至 Node.js 執行個體

連接到執行個體的預設動態公有 IP 地址會在每次停止和啟動執行個體時變更。建立靜態 IP 地址並將其連接到執行個體，以防止公有 IP 地址變更。接著，使用網域名稱搭配執行個體時，您不必在每次停止和啟動執行個體時更新網域的 DNS 記錄。您可以將一個靜態 IP 連接至一個執行個體。

在執行個體管理頁面的 Domains & DNS (網域和 DNS) 索引標籤下，選擇 Create static IP (建立靜態 IP)，接著遵循頁面上的說明。

如需詳細資訊，請參閱[建立靜態 IP 並將其附加至 Lightsail 中的執行個體](#)。

## 步驟 3：瀏覽 Node.js 執行個體歡迎頁面

瀏覽至執行個體的公有 IP 位址，以存取安裝在其上的應用程式 phpMyAdmin、存取或存取 Bitnami 文件。

1. 在執行個體管理頁面的 Connect (連接) 索引標籤下，記下公有 IP。
2. 瀏覽至公有 IP 地址，例如前往 `http://192.0.2.3`。

如需詳細資訊，請參閱[在 Amazon Lightsail 中取得 Bitnami 執行個體的應用程式使用者名稱和密碼](#)。

## 步驟 4：將網域名稱對應至 Node.js 執行個體

若要將網域名稱 (例如 `example.com`) 對應至執行個體，請新增記錄至網域的網域名稱系統 (DNS)。DNS 記錄通常會在您註冊網域的註冊商處進行管理和託管。不過，我們建議您將網域 DNS 記錄的管理權限轉移至 Lightsail，以便您可以使用 Lightsail 主控台進行管理。

在 Lightsail 主控台首頁的 [網路功能] 索引標籤下，選擇 [建立 DNS 區域]，然後依照頁面上的指示進行。

如需詳細資訊，請參閱[建立 DNS 區域以管理域的 DNS 記錄](#)。

## 步驟 5：閱讀 Bitnami 文件

閱讀 Bitnami 文件以了解如何部署 Node.js 應用程式、藉由 SSL 憑證啟用 HTTPS 支援、藉由 SFTP 上傳檔案到伺服器。

如需詳細資訊，請參閱[Bitnami Node.js for AWS 雲端](#)。

## 步驟 6：建立 Node.js 執行個體的快照

快照是執行個體之系統磁碟和原始組態的複本。快照包含的資訊有記憶體、CPU、磁碟大小和資料傳輸率。您可以使用快照做為新執行個體的基準，或做為資料備份。

在執行個體管理頁面的 Snapshot (快照) 索引標籤下方，輸入快照的名稱，接著選擇 Create snapshot (建立快照)。

如需詳細資訊，請參閱[建立 Linux 或 Unix 執行個體的快照](#)。

## 在 Lightsail 上部署一個託管堆疊

了解如何在 Amazon Lightsail 中建立 Plesk 執行個體，以及如何透過建立使用者名稱和密碼來首次登入 Plesk 使用者介面。您也將學習如何在 Plesk 執行個體啟動並執行後如何連線和設定它。

### Important

您的 Plesk 執行個體包含 30 天試用授權。30 天后，您必須從 Plesk 購買許可證才能繼續使用 Plesk 應用程式。

Plesk 託管堆疊 Lightsail 以下功能。

- WordPress 工具包，在圖形用戶界面中具有自動化功能

- 讓我們加密對SSL證書的支持，並在單個實例上配置加密 ( HTTPS ) 流量
- FTP存取您的執行個體與執行個體之間傳輸檔案
- Docker 代理規則
- 基於 Web 的服務器管理和安全工具，包括 Plesk 防火牆，日誌和 ModSecurity

## 步驟 1：建立 Plesk 執行個體

請完成下列步驟，在 Lightsail 上建立 Plesk 實體。

1. 登入 Lightsail 主控台，網址為 <https://lightsail.aws.amazon.com/>。
2. 在「執行處理」首頁上，選擇建立執行個體。
3. 選擇您要建立執行個體的位置。

選擇 [變更 AWS 區域 和可用區域] 以變更執行個體位置。

4. 在 Apps+OS 下，選擇 Plesk Hosting Stack on Ubuntu (Ubuntu 上的 Plesk 託管堆疊)。
5. 選擇您的執行個體方案。USD每月 5 美元的 Lightsail 計劃不支持 Plesk 託管堆棧。
6. 輸入您執行個體的名稱。

資源名稱：

- 每個 Lightsail 帳戶 AWS 區域 中的每個項目都必須是唯一的。
  - 必須包含 2 至 255 個字元。
  - 開頭和結尾必須是英數字元或數字。
  - 可以包含英數字元、數字、句點、破折號和底線。
7. (選用) 將標籤新增至您的執行個體。如需詳細資訊，請參閱[標籤](#)。
  8. 選擇 建立執行個體。

執行個體需要幾分鐘的時間才會佈建，並且在建立後即可使用。

如果您在啟動 Plesk 執行個體後遇到問題，請前往 Plesk 支援頁面查看執行個體上是否需要安裝更新。如需詳細資訊，請參閱《[Plesk 文件與說明入口網站](#)》中的 [Plesk 說明中心](#)和 Plesk 更新。

## 步驟 2：首次登入 Plesk 使用者介面

使用下列程序取得一次性登入URL。您需要一次性登入，才URL能以管理員身分存取 Plesk 使用者介面。

1. 在執行個體管理頁面的 [Connect] 索引標籤下，選擇 [Connect 方式] SSH。
2. 連線後，輸入以下指令以取得一次性登入URL。

```
sudo plesk login | grep -v internal:8
```

您應該會看到類似下列範例的回應，其中包含一次性登入URL。

```
https://heuristic-bassi.192-0-2-0.plesk.page/login?secret=ce-  
e3b0c44298fc1c149afbf4c8996fb92427
```

#### Tip

如果您最近將靜態 IP 連接到 Plesk 執行個體，則可能會取得使用舊公用 IP 位址URL的一次性登入。重新啟動執行個體，然後再次執行上述命令，以取得使URL用新靜態公用 IP 位址的一次性登入。

3. 將一次性登錄複製並粘貼URL到網絡瀏覽器中。

#### Note

您可能會看到瀏覽器警告，指出您的連線並非私有、不安全，或有安全性風險。發生這種情況是因為您的 Plesk 執行個體尚未套用SSL/TLS憑證。在瀏覽器視窗中，選擇 Advanced (進階)、Details (詳細資訊) 或 More information (更多資訊)，以檢視可用的選項。然後選擇繼續瀏覽該網站，即使該網站不是私有或安全的網站。

4. 按照頁面上的指示建立 Plesk 的登入資料。當您首次登入時，您應該會看到可將網域新增至 Plesk 的選項。

若要稍後再次登入，請瀏覽至`https://PublicIPAddress:8443`。Replace (取代) *PublicIPAddress* 使用執行個體的公用 IP 位址或靜態 IP 位址。例如：`https://192.0.2.0/:8443`。然後輸入您先前建立的使用者名稱和密碼，以登入 Plesk 使用者介面。

## 步驟 3：閱讀 Plesk 文件

閱讀 Plesk 文件以了解如何管理網站、自訂 Plesk 使用者介面等。

如需詳細資訊，請參閱 Plesk 文件與說明入口網站中的[在 Plesk 中開始管理網站](#)。

## 步驟 4：將靜態 IP 地址連接至 Plesk 執行個體

連接到執行個體的預設動態公有 IP 地址會在每次停止和啟動執行個體時變更。建立靜態 IP 地址並將其連接到執行個體，以防止公有 IP 地址變更。稍後，當您將網域名稱用於執行個體時，每次停止並啟動執行個體時，就不必更新網域的 DNS 記錄。您可以將一個靜態 IP 連接至一個執行個體。

在執行個體管理頁面的 [網路功能] 索引標籤下，選擇 [連接靜態 IP]，然後依照頁面上的指示操作。

如需詳細資訊，請參閱[建立靜態 IP 並將其附接至執行個體](#)。

## 步驟 5：將網域名稱對應至 Plesk 執行個體

將網域對應至您的 Plesk 執行個體，您可以使用該執行個體存取 Plesk 使用者介面。您也可以將 Plesk 使用者介面內對應多個網域，以使用來管理網站。本節說明如何將您的網域映射到您的 Plesk 執行個體。如需有關在 Plesk 使用者介面中對應多個網域的詳細資訊，請參閱 Plesk 文件與說明入口網站中的[在 Plesk 中新增網域](#)。

若要將網域名稱 (例如) 對應至執行個體，請將記錄新增至網域的網域名稱系統 (DNS)。example.com DNS 記錄通常在您註冊網域的註冊商處進行管理和託管。不過，我們建議您將網域 DNS 記錄的管理權限轉移至 Lightsail，以便您可以使用 Lightsail 主控台進行管理。

在 Lightsail 主控台首頁上的「網域與」上 DNS，選擇「建立 DNS 區域」，然後依照頁面上的指示操作。

如需詳細資訊，請參閱[在 Lightsail 中建立 DNS 區域以管理您的網域 DNS 記錄](#)。

## 步驟 6：購買普萊斯克許可證

您的 Plesk 執行個體包含 30 天試用授權。30 天后，您必須從 Plesk 購買許可證才能繼續使用它。如需詳細資訊，請參閱 Plesk 網站上的[定價](#)。

從 Plesk 購買許可證後，您必須安裝許可證。若要安裝您的 Plesk 授權，請參閱[如何在 Plesk 支援網站上安裝 Plesk 授權](#)。

## 步驟 7：建立 Plesk 執行個體的快照

快照是執行個體之系統磁碟和原始組態的複本。快照包括記憶體 CPU、磁碟大小和資料傳輸速率等資訊。您可以使用快照做為新執行個體的基準，或做為資料備份。

在執行個體管理頁面的 [快照] 索引標籤下，選擇 [建立快照]。然後，按照頁面上的說明進行操作。如需詳細資訊，請參閱[建立 Linux 或 Unix 執行個體的快照](#)。

## 在 Lightsail 上建立 PrestaShop 網站

執行個體在 Amazon Lightsail 上啟動並 PrestaShop 執行後，您應完成以下幾個步驟才能開始使用。

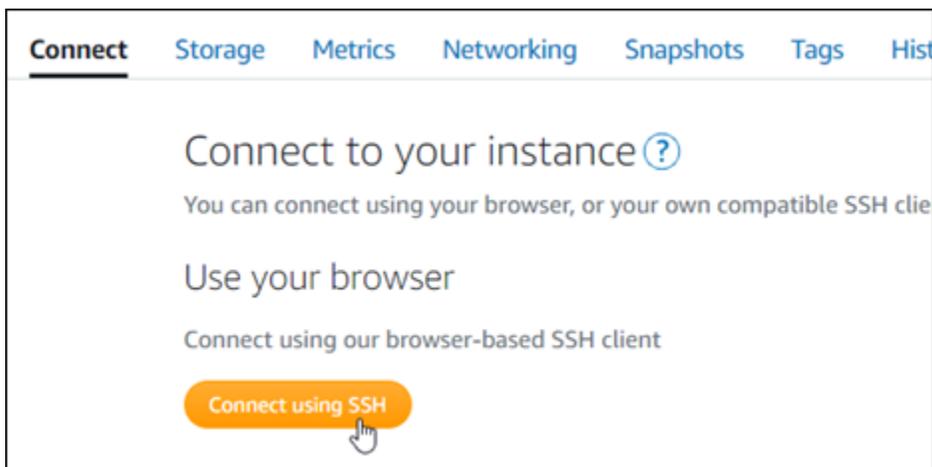
### 內容

- [步驟 1：獲取您 PrestaShop 網站的默認應用程式密碼](#)
- [步驟 2：將靜態 IP 位址附加至您的 PrestaShop 執行個體](#)
- [步驟 3：登錄到您 PrestaShop 網站的管理儀表板](#)
- [步驟 4：將您註冊的域名的流量路由到您的 PrestaShop 網站](#)
- [步驟 5：為您的 PrestaShop 網站設定 HTTPS](#)
- [步驟 6：為電子郵件通知設定 SMTP](#)
- [第 7 步：閱讀比特名稱和文檔 PrestaShop](#)
- [步驟 8：建立執行個 PrestaShop 體的快照](#)

### 步驟 1：獲取您 PrestaShop 網站的默認應用程式密碼

完成下列步驟，即可取得 PrestaShop 網站的預設應用程式密碼。

1. 在執行個體管理頁面的 Connect (連接) 索引標籤下，選擇 Connect using SSH (使用 SSH 連接)。

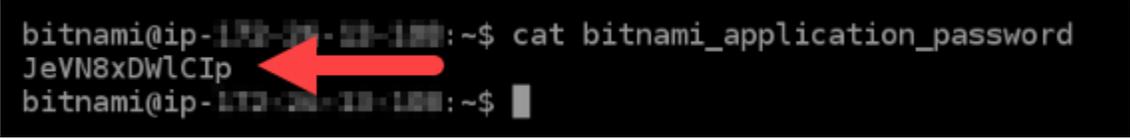


2. 連線後，請輸入下列命令以取得預設應用程式密碼：

```
cat $HOME/bitnami_application_password
```

您應該會看到類似於以下範例的回應，其中包含預設應用程式密碼。請將此密碼存放在安全處。您將在本教程的下一部分中使用它來登錄到您 PrestaShop 網站的管理儀表板。

```
bitnami@ip-192-0-2-0:~$ cat bitnami_application_password
JeVN8xDWlCIp
bitnami@ip-192-0-2-0:~$
```

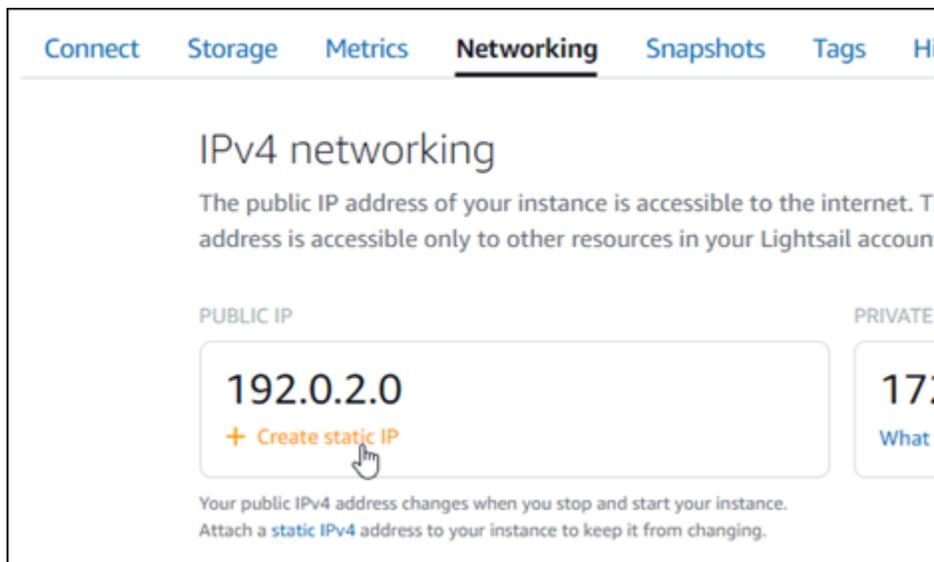


如需詳細資訊，請參閱[在 Amazon Lightsail 中取得 Bitnami 執行個體的應用程式使用者名稱和密碼](#)。

## 步驟 2：將靜態 IP 位址附加至您的 PrestaShop 執行個體

您第一次建立執行個體時，所指派的公有 IP 地址將會在每次停用和啟用執行個體時變更。您應該建立靜態 IP 地址並將其連接至執行個體，以確保其公有 IP 地址不會變更。當您將註冊的網域名稱 (例如 example.com) 與執行個體搭配使用時，便無須在每次停用或啟用執行個體時更新網域的 DNS 記錄。您可以將一個靜態 IP 連接至一個執行個體。

在執行個體管理頁面的 Networking#(聯網) 索引標籤下，選擇 Create a static IP (建立靜態 IP) 或 Attach static IP (連接靜態 IP) (若您先前已建立可以連接至執行個體的靜態 IP)，然後遵循頁面上的指示執行操作。



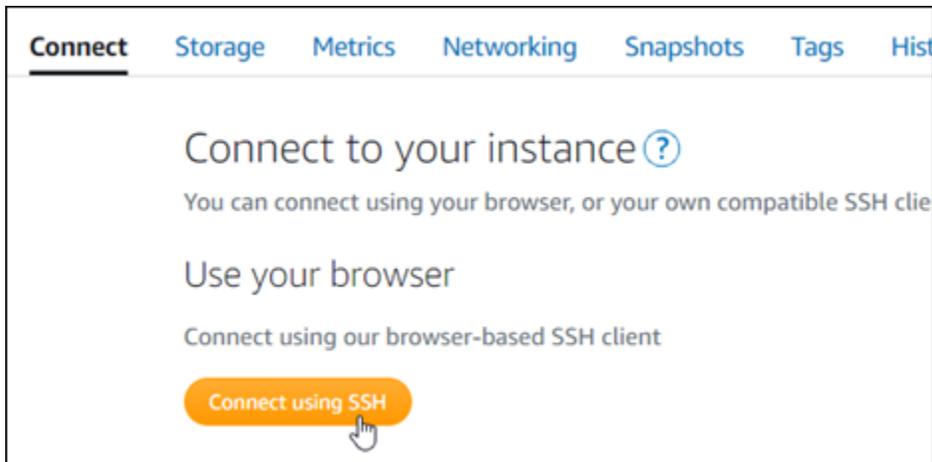
如需詳細資訊，請參閱[建立靜態 IP 並將其附接至執行個體](#)。

將新的靜態 IP 位址連接至執行個體後，您必須完成下列步驟，讓 PrestaShop 軟體知道新的靜態 IP 位址。

1. 請記下執行個體的靜態 IP 地址。這會列在執行個體管理頁面的標頭區段中。



2. 在執行個體管理頁面的 Connect (連接) 索引標籤下，選擇 Connect using SSH (使用 SSH 連接)。



3. 連接後，請輸入以下命令。請務必以執行個體的新靜態 IP 地址取代 *<StaticIP>*。

```
sudo /opt/bitnami/configure_app_domain --domain <StaticIP>
```

範例：

```
sudo /opt/bitnami/configure_app_domain --domain 203.0.113.0
```

您應該會看到類似於以下範例的回應。該 PrestaShop 軟件現在應該知道新的靜態 IP 地址。

```
bitnami@ip-198-51-100-100:~$ sudo /opt/bitnami/configure_app_domain --domain 203.0.113.0
Configuring domain to 203.0.113.0
2021-03-12T15:49:22.000Z - info: Saving configuration info to disk
prestashop 15:49:22.41 INFO ==> Trying to connect to the database server
prestashop 15:49:22.44 INFO ==> Updating hostname in database
prestashop 15:49:22.46 INFO ==> Purging cache
Disabling automatic domain update for IP address changes
```

**Note**

PrestaShop 目前不支援 IPv6 位址。您可以為執行個體啟用 IPv6，但 PrestaShop 軟體不會回應 IPv6 網路上的要求。

### 步驟 3：登錄到您 PrestaShop 網站的管理儀表板

完成以下步驟以存取您的 PrestaShop 網站並登入其管理儀表板。若要登入，請使用預設使用者名稱 (user@example.com) 和您先前依本指南指示取得的預設應用程式密碼。

1. 在 Lightsail 主控台中，記下執行個體管理頁面標頭區域中列出的公用或靜態 IP 位址。



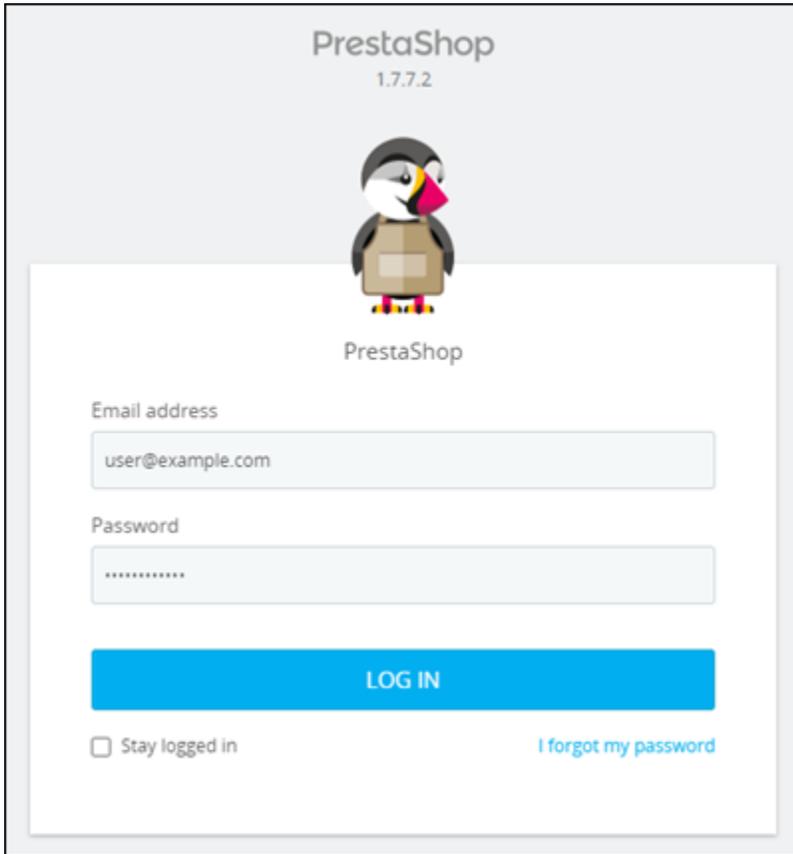
2. 瀏覽至下列位址，以存取您 PrestaShop 網站管理儀表板的登入頁面。請務必將 *<InstanceIpAddress>* 取代為執行個體的公用或靜態 IP 位址。

```
http://<InstanceIpAddress>/administration
```

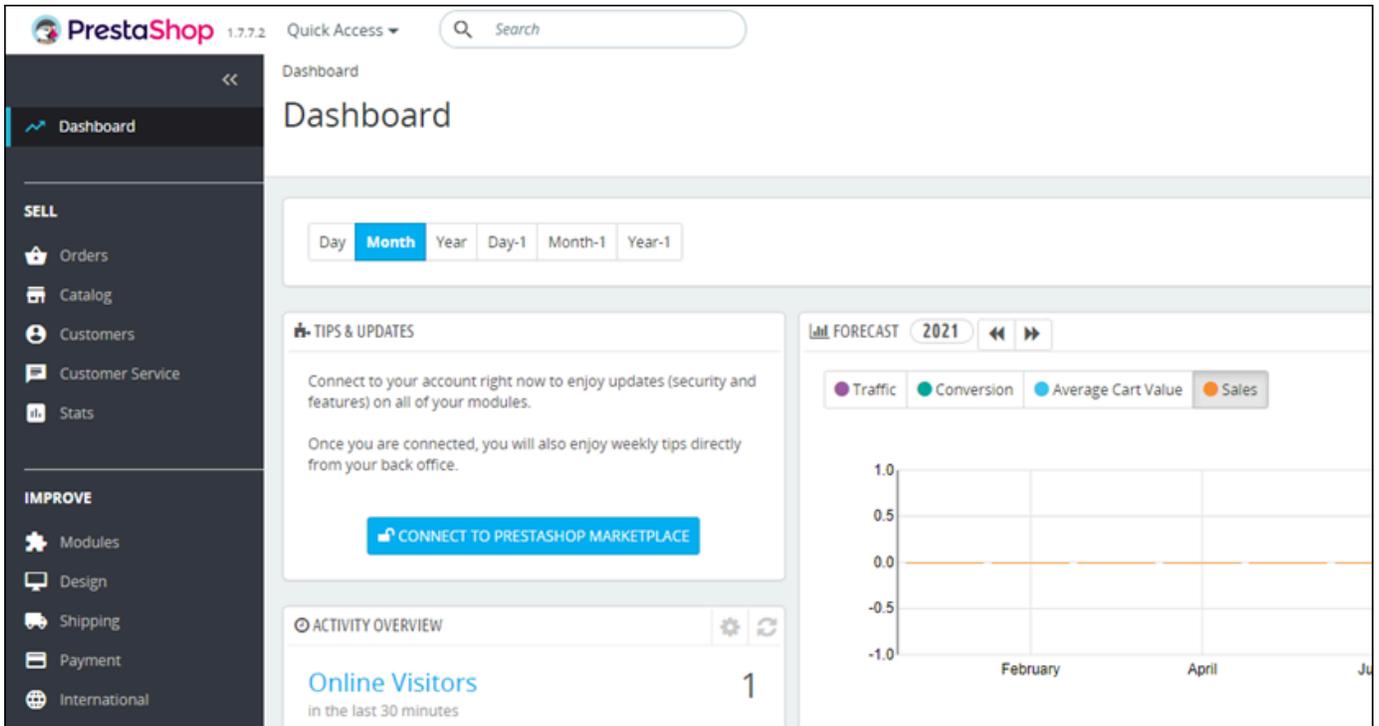
範例：

```
http://203.0.113.0/administration
```

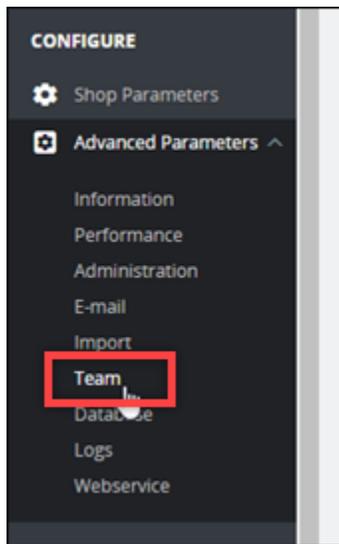
3. 請輸入預設的使用者名稱 (user@example.com)，以及您稍早在本指南中取得的預設應用程式密碼，然後選擇 Log in (登入)。



PrestaShop 管理儀表板隨即出現。



若要變更改用於登入 PrestaShop 網站管理儀表板的預設使用者名稱或密碼，請在導覽窗格中選擇 [進階參數]，然後選擇 [小組]。如需詳細資訊，請參閱 PrestaShop 文件 PrestaShop 中的 [使用者指南](#)。



如需有關管理儀表板的詳細資訊，請參閱 [如需詳細資訊](#)，請參閱 PrestaShop 文件 PrestaShop 中的 [使用者指南](#)。

#### 步驟 4：將您註冊的域名的流量路由到您的 PrestaShop 網站

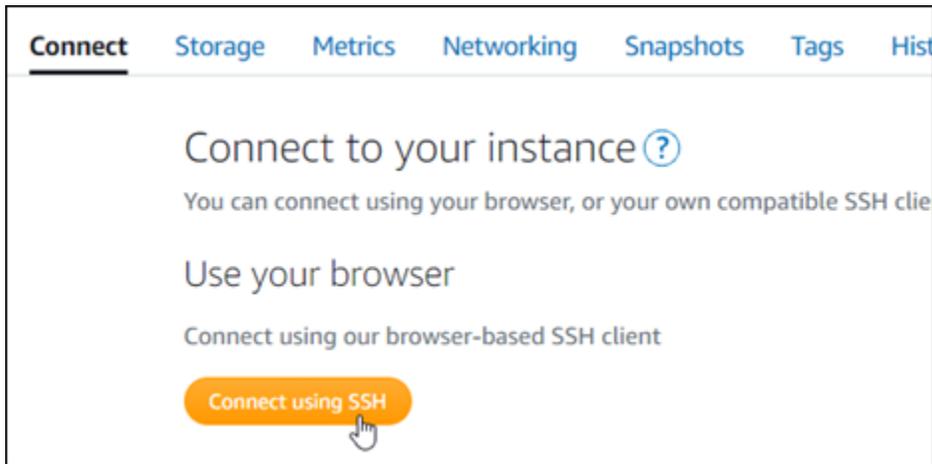
若要將已註冊網域名稱 (例如 example.com) 的流量路由到您的 PrestaShop 網站，請將記錄新增至網域的網域名稱系統 (DNS)。DNS 記錄通常會在您註冊網域的註冊商處進行管理和託管。不過，我們建議您將網域 DNS 記錄的管理權限轉移至 Lightsail，以便您可以使用 Lightsail 主控台進行管理。

在 Lightsail 主控台首頁的 [網域和 DNS] 索引標籤下，選擇 [建立 DNS 區域]，然後依照頁面上的指示進行。

如需詳細資訊，請參閱 [在 Lightsail 中建立 DNS 區域以管理網域的 DNS 記錄](#)。

在您的網域名稱將流量路由到執行個體之後，您必須完成下列步驟，讓 PrestaShop 軟體知道網域名稱。

1. 在執行個體管理頁面的 Connect (連接) 索引標籤下，選擇 Connect using SSH (使用 SSH 連接)。



2. 連接後，請輸入以下命令。請務必將 *< DomainName >* 取代為將流量轉送至執行個體的網域名稱。

```
sudo /opt/bitnami/configure_app_domain --domain <DomainName>
```

範例：

```
sudo /opt/bitnami/configure_app_domain --domain www.example.com
```

您應該會看到類似於以下範例的回應。該 PrestaShop 軟件現在應該知道域名。

```
bitnami@ip-173-20-0-197:~$ sudo /opt/bitnami/configure_app_domain --domain www.example.com
Configuring domain to www.example.com
2021-03-12T15:49:22.000Z - info: Saving configuration info to disk
prestashop 15:49:22.41 INFO ==> Trying to connect to the database server
prestashop 15:49:22.44 INFO ==> Updating hostname in database
prestashop 15:49:22.46 INFO ==> Purging cache
Disabling automatic domain update for IP address changes
```

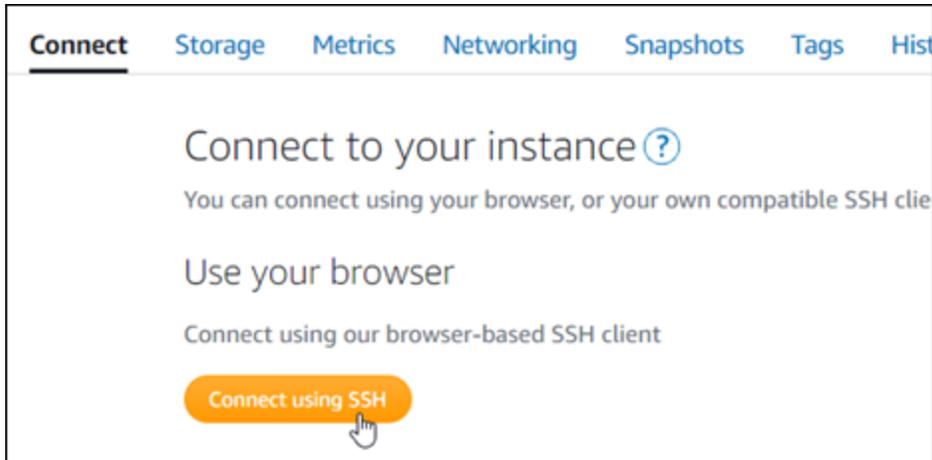
## 步驟 5：為您的 PrestaShop 網站設定 HTTPS

完成以下步驟，即可在您的 PrestaShop 網站上設定 HTTPS。我們會在這些步驟中展示如何使用 Bitnami HTTPS 組態工具 (bncert)，這是用來請求 SSL/TLS 憑證、設定重新引導 (例如 HTTP 至 HTTPS) 以及更新憑證的命令列工具。

**⚠ Important**

bncert 工具只會針對目前將流量路由到您執行個體的公用 IP 位址的 PrestaShop 網域核發憑證。在開始執行這些步驟之前，請確定您已將 DNS 記錄新增至您要與網站搭配使用的所有 PrestaShop 網域的 DNS。

1. 在執行個體管理頁面的 Connect (連接) 索引標籤下，選擇 Connect using SSH (使用 SSH 連接)。



2. 連接後，請輸入以下命令來啟動 bncert 工具。

```
sudo /opt/bitnami/bncert-tool
```

您應該會看到類似於以下範例的回應：

```
bitnami@ip-172-31-7-10:~$ sudo /opt/bitnami/bncert-tool
-----
Welcome to the Bitnami HTTPS Configuration tool.
-----
Domains

Please provide a valid space-separated list of domains for which you wish to
configure your web server.

Domain list []: █
```

3. 輸入主要網域名稱和替代網域名稱，並以空格分隔，如以下範例所示。

```
-----  
Welcome to the Bitnami HTTPS Configuration tool.  
-----  
Domains  
Please provide a valid space-separated list of domains for which you wish to  
configure your web server.  
Domain list []: example.com www.example.com
```

4. bncert 工具會詢問您希望如何設定網站的重新引導。可用的選項如下：
- Enable HTTP to HTTPS redirection (啟用 HTTP 至 HTTPS 重新引導) - 指定將瀏覽至網站 HTTP 版本 (即 `http://example.com`) 的使用者自動重新引導至 HTTPS 版本 (即 `https://example.com`)。由於此選項會強制所有訪客使用加密的連線，建議啟用此選項。輸入 Y，並按 Enter 以啟用。
  - Enable non-www to www redirection (啟用非 www 至 www 重新引導) - 指定將瀏覽至網域 (即 `https://example.com`) 頂點的使用者自動重新引導至您網域的 www 子網域 (即 `https://www.example.com`)。建議啟用此選項。不過，如果您已在搜索引擎工具 (如 Google 的網站管理員工具) 中將網域的頂點指定為您偏好的網站地址，或者如果您的頂點直接指向 IP，且 www 子網域透過 CNAME 記錄參考您的頂點，則您可能需要停用此選項並啟用替代選項 (啟用 www 至非 www 重新引導)。輸入 Y，並按 Enter 以啟用。
  - Enable www to non-www redirection (啟用 www 至非 www 重新引導) - 指定將瀏覽至您網域 www 子網域 (即 `https://www.example.com`) 的使用者自動重新引導至網域的頂點 (即 `https://example.com`)。如果您已啟用非 www 重新引導至 www，我們建議您停用此選項。輸入 N，並按 Enter (確認) 以停用。

您的選取內容應看起來與下列範例類似。

```
Enable/disable redirections

Please select the redirections you wish to enable or disable on your Bitnami
installation.

Enable HTTP to HTTPS redirection [Y/n]: Y

Enable non-www to www redirection [Y/n]: Y

Enable www to non-www redirection [y/N]: N
```

5. 系統會列出即將進行的變更。輸入 Y，並按 Enter (確認) 以確認並繼續。

```
Changes to perform

The following changes will be performed to your Bitnami installation:

1. Stop web server
2. Configure web server to use a free Let's Encrypt certificate for the domains:
example.com www.example.com
3. Configure a cron job to automatically renew the certificate each month
4. Configure web server name to: example.com
5. Enable HTTP to HTTPS redirection (example: redirect http://example.com to
https://example.com)
6. Enable non-www to www redirection (example: redirect example.com to
www.example.com)
7. Start web server once all changes have been performed

Do you agree to these changes? [Y/n]: Y
```

6. 輸入您的電子郵件地址，以與您的 Let's Encrypt 憑證相關聯，然後按 Enter。

```
Create a free HTTPS certificate with Let's Encrypt

Please provide a valid e-mail address for which to associate your Let's Encrypt
certificate.

Domain list: example.com www.example.com

Server name: example.com

E-mail address []: 
```

7. 檢閱 Let's Encrypt 訂閱者協議。輸入 Y，並按 Enter (確認) 以接受該協議並繼續。

```
The Let's Encrypt Subscriber Agreement can be found at:  
https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf  
Do you agree to the Let's Encrypt Subscriber Agreement? [Y/n]: █
```

執行這些動作是為了在執行個體上啟用 HTTPS，包括請求憑證和設定您指定的重新引導。

```
Performing changes to your installation  
  
The Bitnami HTTPS Configuration Tool will perform any necessary actions to your  
Bitnami installation. This may take some time, please be patient.  
  
█
```

系統已成功核發並驗證您的憑證，如果您看到類似以下範例的訊息，則表示已成功在執行個體上設定重新引導。

```
Success  
  
The Bitnami HTTPS Configuration Tool succeeded in modifying your installation.  
  
The configuration report is shown below.  
  
Backup files:  
* /opt/bitnami/apache2/conf/httpd.conf.back.202005290035  
* /opt/bitnami/apache2/conf/bitnami/bitnami-apps-prefix.conf.back.202005290035  
* /opt/bitnami/apache2/conf/bitnami/bitnami.conf.back.202005290035  
  
Find more details in the log file:  
  
/tmp/bncert-202005290035.log  
  
If you find any issues, please check Bitnami Support forums at:  
  
https://community.bitnami.com  
  
Press [Enter] to continue:█
```

bncert 工具會在憑證過期前每 80 天執行自動續約一次。繼續執行下一組步驟，以完成在您的 PrestaShop 網站上啟用 HTTPS。

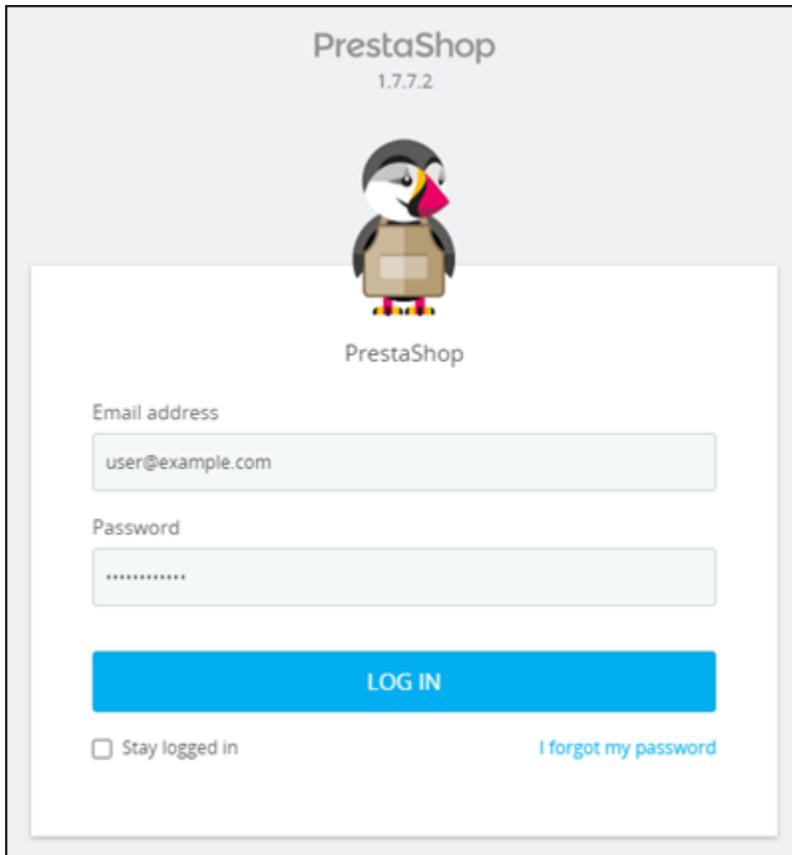
8. 瀏覽至下列位址，以存取您 PrestaShop 網站管理儀表板的登入頁面。請務必將 *< DomainName >* 取代為將流量轉送至執行個體的已註冊網域名稱。

```
http://<DomainName>/administration
```

範例：

`http://www.example.com/administration`

9. 請輸入預設的使用者名稱 (user@example.com)，以及您稍早在本指南中取得的預設應用程式密碼，然後選擇 Log in (登入)。



PrestaShop  
1.7.7.2

PrestaShop

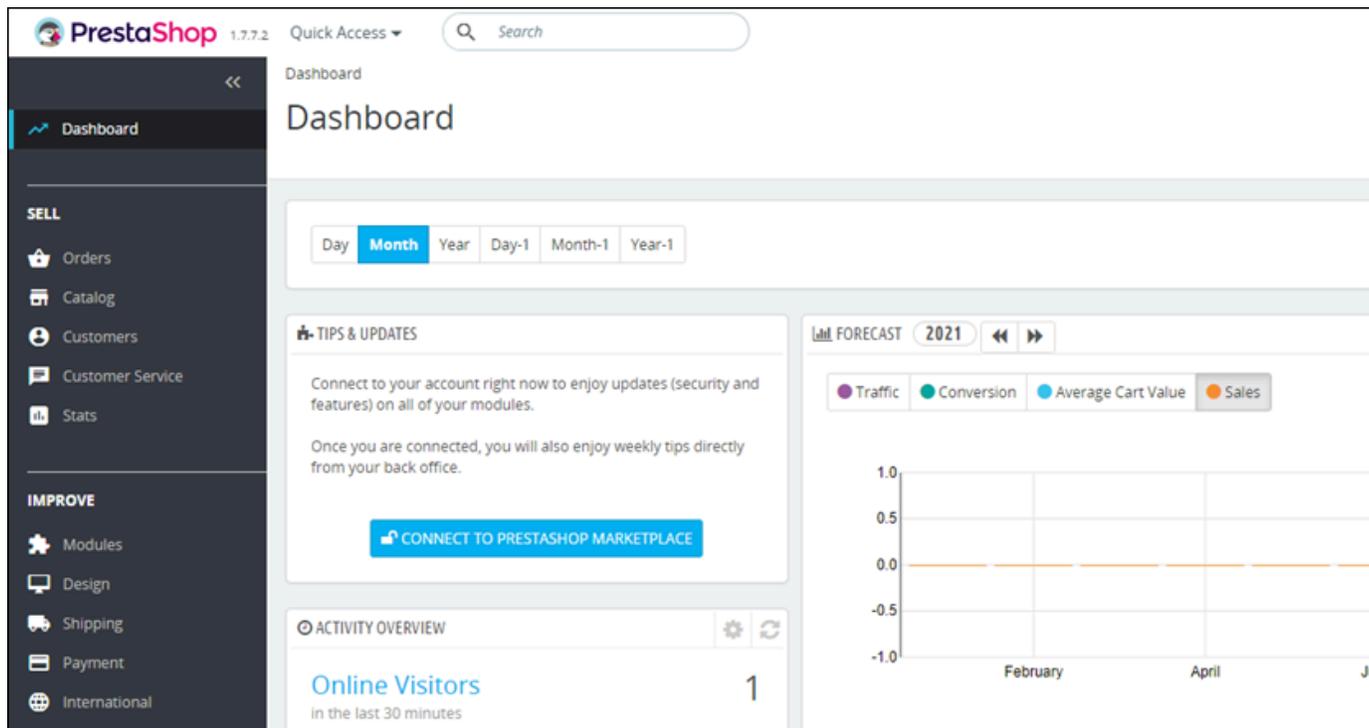
Email address  
user@example.com

Password  
\*\*\*\*\*

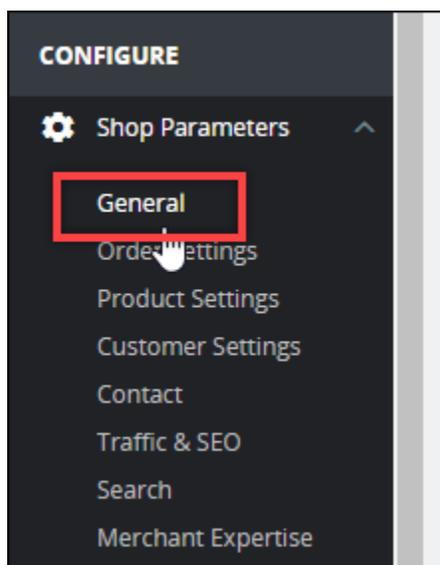
LOG IN

Stay logged in [I forgot my password](#)

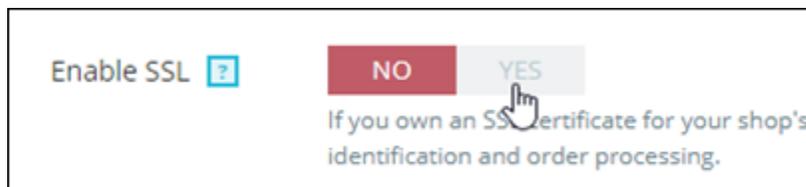
PrestaShop 管理儀表板隨即出現。



10. 選擇導覽窗格中的 Shop Parameters (工廠參數) ，然後選擇 General (一般)。

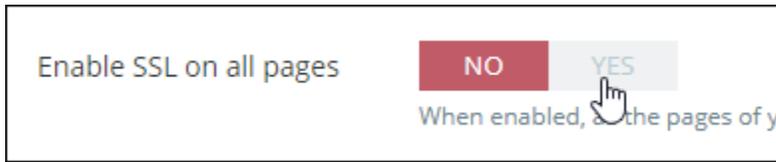


11. 選擇 Enable SSL (啟用 SSL) 旁邊的 Yes (是)。



12. 捲動至頁面底部，然後選擇 Save (儲存)。

- 當 General (一般) 頁面重新載入時，請選擇 Enable SSL on all pages (在全部頁面上啟用 SSL) 旁的 Yes (是)。

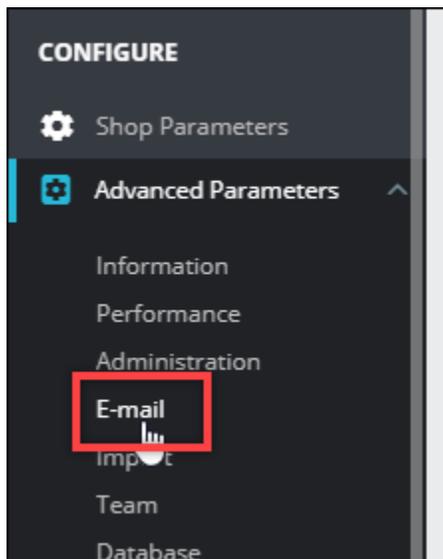


- 捲動至頁面底部，然後選擇 Save (儲存)。

HTTPS 現在已為您的 PrestaShop 網站配置。當客戶瀏覽到您 PrestaShop 網站的 HTTP 版本 (例如 `http://www.example.com`) 時，他們將自動重定向到 HTTPS 版本 (例如，`https://www.example.com`)。

## 步驟 6：為電子郵件通知設定 SMTP

設定網站的 SMTP 設定，以啟用 PrestaShop 網站的電子郵件通知。若要這麼做，請登入您 PrestaShop 網站的管理儀表板。在導覽窗格中選擇 Advanced Parameters (進階參數)，然後選擇 E-mail (電子郵件)。您也應該據此調整電子郵件聯絡人。若要這麼做，請選擇導覽窗格中的 Shop Parameters (商店參數)，然後選擇 Contact (聯絡人)。



如需詳細資訊，如需詳細資訊，請參閱文件 PrestaShop 中的 [使用者指南](#) 和 Bitnami PrestaShop 文件中的 [為輸出電子郵件設定 SMTP](#)。

### Important

如果您將 SMTP 設定為使用通訊埠 25、465 或 587，則必須在 Lightsail 主控台的執行個體防火牆中開啟這些連接埠。如需詳細資訊，請參閱[在 Amazon Lightsail 中新增和編輯執行個體防火牆規則](#)。

如果您將 Gmail 帳戶設定為在 PrestaShop 網站上傳送電子郵件，則必須使用應用程式密碼，而不是使用用來登入 Gmail 的標準密碼。如需詳細資訊，請參閱[以應用程式密碼登入](#)。

## 第 7 步：閱讀比特名稱和文檔 PrestaShop

請閱讀 Bitnami 文件，瞭解如何在執行 PrestaShop 個體和網站上執行管理工作，例如安裝外掛程式和自訂佈景主題。如需詳細資訊，請參閱[Bitnami 文件中的適用於 AWS 雲端的 Bit nami PrestaShop 堆疊](#)。

您還應該閱讀 PrestaShop 文檔以了解如何管理您的 PrestaShop 網站。如需詳細資訊，請參閱 PrestaShop 文件 PrestaShop 中的[使用者指南](#)。

## 步驟 8：建立執行個 PrestaShop 體的快照

依照您想要的方式設定 PrestaShop 網站後，請建立執行個體的定期快照以備份它。您可以手動建立快照，或啟用自動快照，讓 Lightsail 為您建立每日快照。若執行個體出現問題，您可以使用快照建立新的替代執行個體。如需詳細資訊，請參閱[快照](#)。

在執行個體管理頁面的 Snapshot (快照) 索引標籤下，選擇 Create a snapshot (建立快照) 或選擇啟用自動快照。

The screenshot displays the 'Snapshots' tab in the Amazon Lightsail console. At the top, there are navigation tabs: Connect, Storage, Metrics, Networking, **Snapshots**, Tags, History, and Delete. Below the tabs, the 'Manual snapshots' section is visible, featuring a title with a help icon, a brief description, a '+ Create snapshot' button, and a list of four snapshots with their creation times and IDs. Below this is the 'Automatic snapshots' section, which shows that automatic snapshots are enabled, the daily snapshot time is 10:00 PM PST, and a 'Change snapshot time' button. Underneath, a 'DAILY SNAPSHOTS' section lists snapshots for Thursday, Wednesday, and Tuesday with their respective dates.

如需詳細資訊，請參閱在 Amazon Lightsail 中建立 [Linux 或 Unix 執行個體的快照](#)或在 [Amazon Lightsail](#) 中[啟用或停用執行個體或磁碟的自動快照](#)。

## 在 Lightsail 上設定和保護紅礦執行個體

在 Redmine 執行個體在 Amazon Lightsail 上啟動並執行之後，您應該採取以下幾個步驟才能開始使用：

### 內容

- [步驟 1：閱讀 Bitnami 文件](#)
- [步驟 2：取得存取 Redmine 管理儀表板所需的預設應用程式密碼](#)

- [步驟 3：將靜態 IP 地址連接至您的執行個體](#)
- [步驟 4：登入 Redmine 網站的管理儀表板](#)
- [步驟 5：將已註冊網域的流量路由至 Redmine 網站](#)
- [步驟 6：為 Redmine 網站設定 HTTPS](#)
- [步驟 7：閱讀 Redmine 文件並繼續設定網站](#)
- [步驟 8：建立執行個體的快照](#)

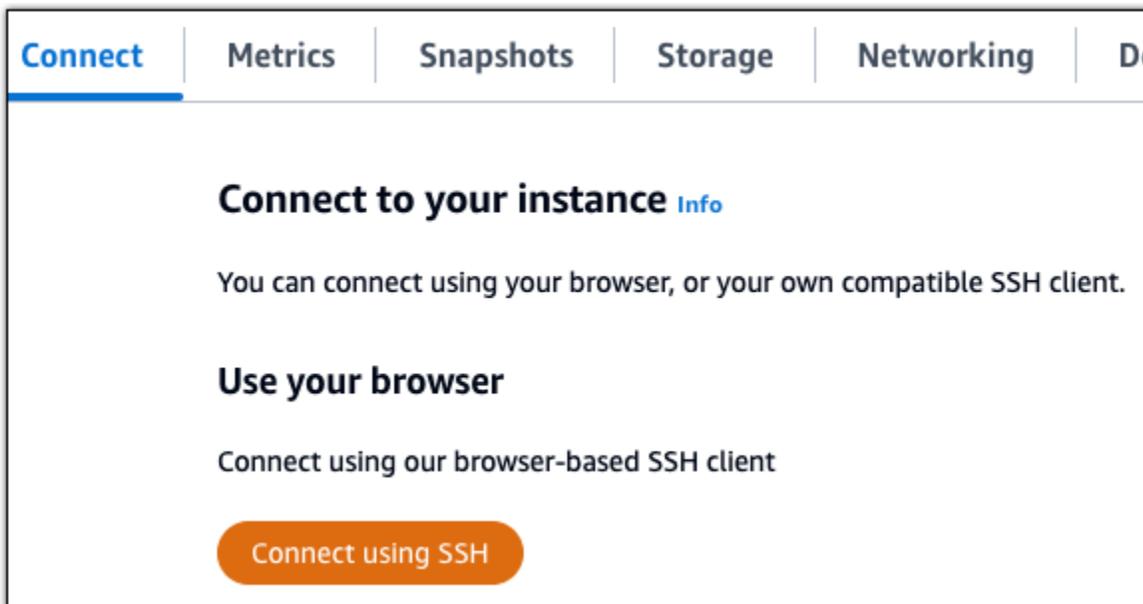
## 步驟 1：閱讀 Bitnami 文件

閱讀 Bitnami 文件以了解如何設定 Redmine 應用程式。如需詳細資訊，請參閱 [Redmine Packaged By Bitnami For AWS 雲端](#)。

## 步驟 2：取得存取 Redmine 管理儀表板所需的預設應用程式密碼

完成下列程序，以取得存取 Redmine 網站管理儀表板所需的預設應用程式密碼。如需詳細資訊，請參閱在 [Amazon Lightsail 中取得 Bitnami 執行個體的應用程式使用者名稱和密碼](#)。

1. 在執行個體管理頁面的 Connect (連接) 索引標籤下，選擇 Connect using SSH (使用 SSH 連接)。



2. 連線後，請輸入下列命令，以取得應用程式密碼：

```
cat $HOME/bitnami_application_password
```

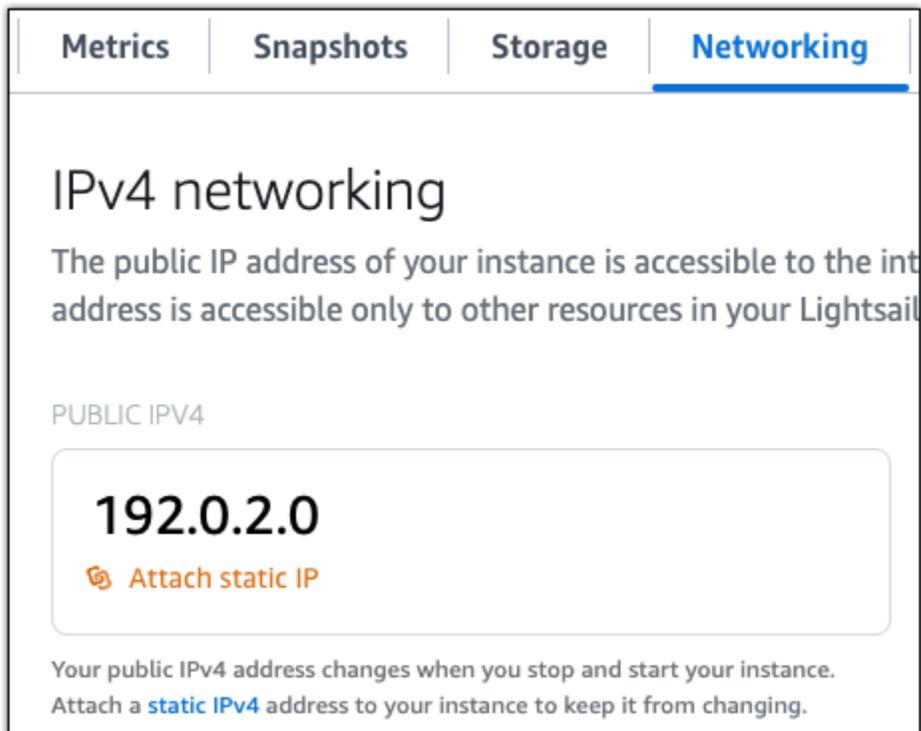
您應該會看到類似於以下範例的回應，其中包含預設應用程式密碼：

```
bitnami@ip-192-0-20-10:~$ cat bitnami_application_password
JeVN8xDWlCIp
bitnami@ip-192-0-20-10:~$
```

### 步驟 3：將靜態 IP 地址連接至您的執行個體

您第一次建立執行個體時，所指派的公有 IP 地址將會在每次停用和啟用執行個體時變更。您應該建立靜態 IP 地址並將其連接至執行個體，以確保其公有 IP 地址不會變更。當您將註冊的網域名稱 (例如 example.com) 與執行個體搭配使用時，便無須在每次停用或啟用執行個體時更新網域的 DNS 記錄。您可以將一個靜態 IP 連接至一個執行個體。

在執行個體管理頁面的 Networking#(聯網) 索引標籤下，選擇 Create a static IP (建立靜態 IP) 或 Attach static IP (連接靜態 IP)(若您先前已建立可以連接至執行個體的靜態 IP)，然後遵循頁面上的指示執行操作。如需詳細資訊，請參閱[建立靜態 IP 並將其附接至執行個體](#)。



The screenshot shows the 'Networking' tab in the AWS Lightsail console. Under 'IPv4 networking', the public IPv4 address is listed as '192.0.2.0'. Below the address is a button labeled 'Attach static IP'. A note at the bottom of the section reads: 'Your public IPv4 address changes when you stop and start your instance. Attach a static IPv4 address to your instance to keep it from changing.'

### 步驟 4：登入 Redmine 網站的管理儀表板

現在您已擁有預設應用程式的密碼，完成下列程序，以導覽至 Redmine 網站首頁並登入管理儀表板。登入後，您可以開始自訂網站並進行管理級變更。如需詳細資訊，了解能在 Redmine 中執行哪些作業，請參閱本指南後述的[步驟 7：閱讀 Redmine 文件並繼續設定網站](#)章節。

1. 在執行個體管理頁面的 Connect (連接) 索引標籤下，記下執行個體的公有 IP 地址。公有 IP 地址也會顯示在執行個體管理頁面的標頭區段。



2. 瀏覽至執行個體的公有 IP 地址，例如前往 <http://203.0.113.0>。

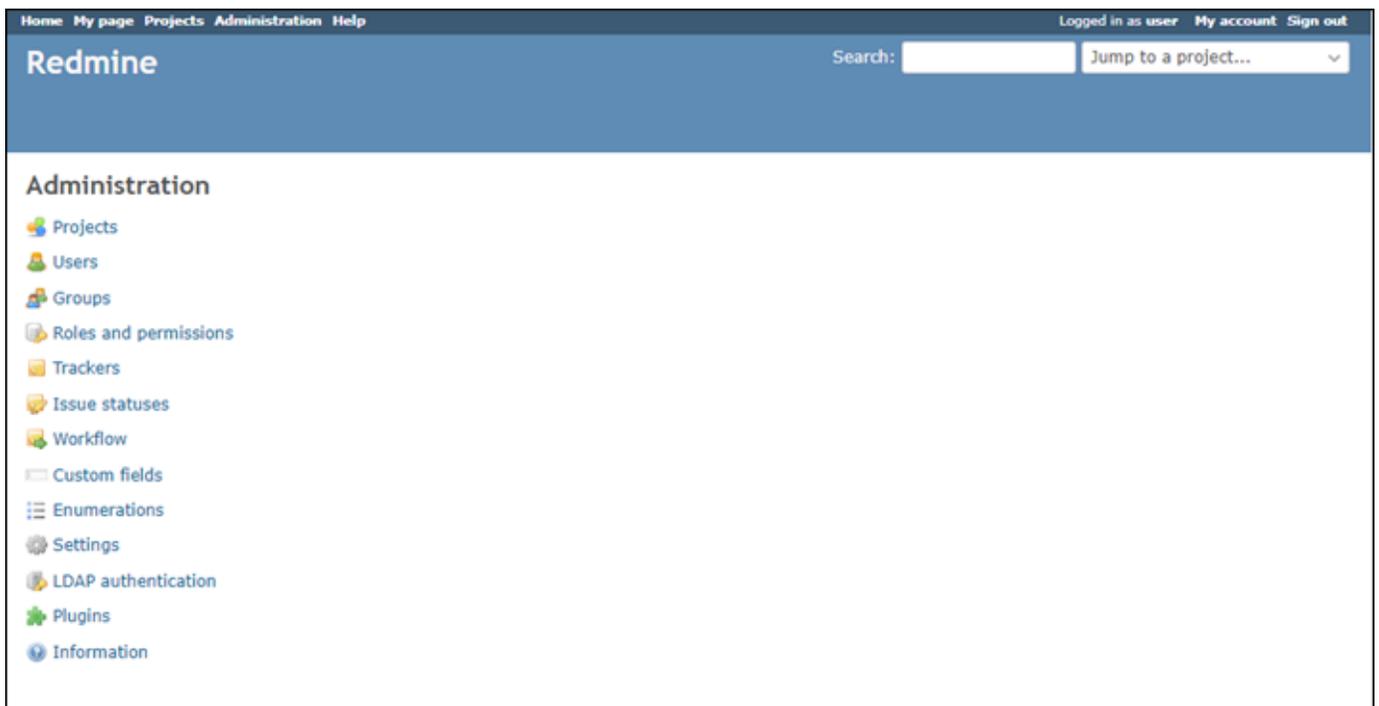
您會看到 Redmine 網站首頁。

3. 選擇 Redmine 網站首頁右下角的 Manage (管理)。

如果未顯示 Manage (管理) 橫幅，您可以透過瀏覽至 <http://<PublicIP>/admin> 前往登入頁面。將 *<PublicIP>* 取代為您執行個體的公有 IP 地址。

4. 使用先前依本指南指示取得的預設使用者名稱 (user) 和預設密碼登入。

您會看到 Redmine 管理儀表板。



## 步驟 5：將已註冊網域的流量路由至 Redmine 網站

若要將已註冊網域 (例如 `example.com`) 的流量路由至 Redmine 網站，請新增紀錄至網域的 DNS。DNS 記錄通常會在您註冊網域的註冊商處進行管理和託管。不過，我們建議您將網域 DNS 記錄的管理權限轉移至 Lightsail，以便您可以使用 Lightsail 主控台進行管理。

在 Lightsail 主控台首頁的 [網域和 DNS] 索引標籤下，選擇 [建立 DNS 區域]，然後依照頁面上的指示進行。如需詳細資訊，請參閱 [在 Lightsail 中建立 DNS 區域以管理網域的 DNS 記錄](#)。

若您瀏覽至您為執行個體設定的網域名稱，則會將您重新導向至 Redmine 網站首頁。接下來，您必須產生並設定 SSL/TLS 憑證，以啟用 Redmine 網站的 HTTPS 連線。如需詳細資訊，請繼續閱讀本指南的下一個章節 [步驟 6：為 Redmine 網站設定 HTTPS](#)。

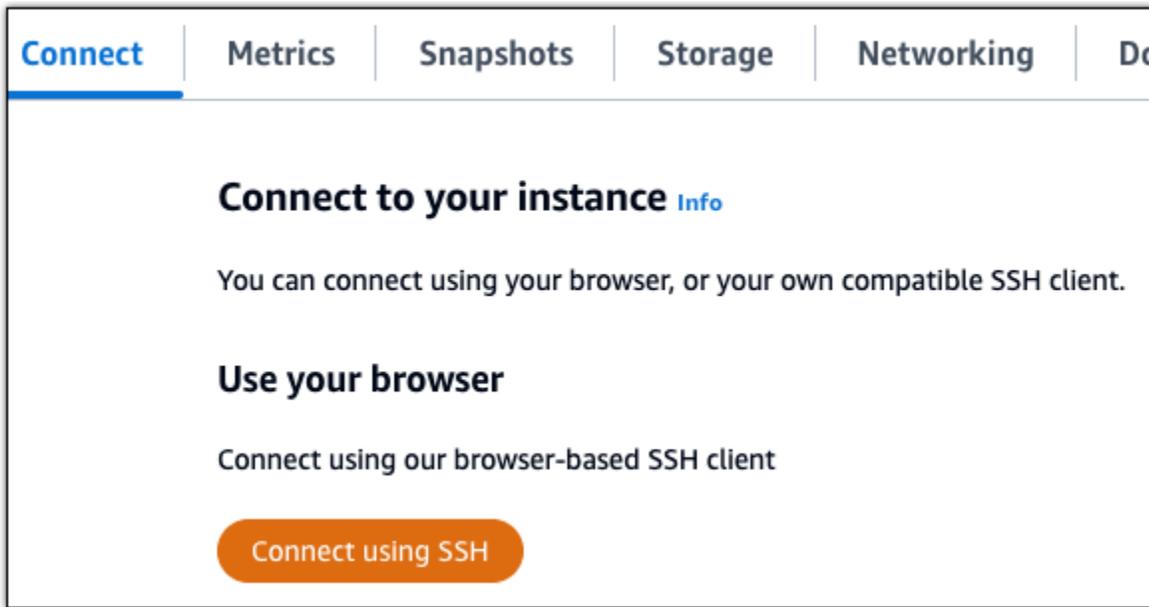
## 步驟 6：為 Redmine 網站設定 HTTPS

完成下列程序，以在 Redmine 網站上設定 HTTPS。這些步驟描述了如何使用 Bitnami HTTPS 組態工具 (`bncert-tool`)，這是一個命令行工具，用於請求 Let's Encrypt SSL/TLS 憑證。如需詳細資訊，請參閱 Bitnami 文件中的 [Learn About The Bitnami HTTPS Configuration Tool](#) (Bitnami HTTPS 組態工具簡介)。

### Important

開始此程序之前，請確認您已將網域設定為將流量路由至 Redmine 執行個體。否則，SSL/TLS 憑證驗證過程會失敗。

1. 在執行個體管理頁面的 Connect (連接) 索引標籤下，選擇 Connect using SSH (使用 SSH 連接)。



2. 連接後，輸入下列命令，以確認執行個體已安裝 bncert 工具。

```
sudo /opt/bitnami/bncert-tool
```

您應該會看到下列其中一個回應：

- 如果您看見回應中未找到命令，則表示您的執行個體上未安裝 bncert 工具。繼續此程序的下一個步驟，在您的執行個體上安裝 bncert 工具。
- 如果您在回應中看見 Welcome to the Bitnami HTTPS configuration tool (歡迎使用 Bitnami HTTPS 組態工具)，則您的執行個體上已安裝 bncert 工具。繼續執行此程序的步驟 8。
- 如果您的執行個體已安裝 bncert 工具一段時間，則您可能會看到說明該工具已有可用更新版本的訊息。選擇下載該版本，然後輸入 `sudo /opt/bitnami/bncert-tool` 命令以再次執行 bncert 工具。繼續執行此程序的步驟 8。

3. 輸入以下命令，以下載 bncert 執行檔案至您的執行個體。

```
wget -O bncert-linux-x64.run https://downloads.bitnami.com/files/bncert/latest/bncert-linux-x64.run
```

4. 輸入以下命令，以便為執行個體上的 bncert 工具執行檔案建立目錄。

```
sudo mkdir /opt/bitnami/bncert
```

5. 輸入以下命令，以讓 bncert 執行可作為程式執行的檔案。

```
sudo chmod +x /opt/bitnami/bncert/bncert-linux-x64.run
```

6. 輸入以下命令，以在您輸入 `sudo /opt/bitnami/bncert-tool` 命令時建立執行 `bncert` 工具的符號連結。

```
sudo ln -s /opt/bitnami/bncert/bncert-linux-x64.run /opt/bitnami/bncert-tool
```

您現已在執行個體上完成 `bncert` 工具安裝。

7. 輸入下列命令，以執行 `bncert` 工具。

```
sudo /opt/bitnami/bncert-tool
```

8. 輸入主要網域名稱和替代網域名稱，並以空格分隔，如以下範例所示。

如果您的網域未設為將流量路由至執行個體的公有 IP 地址，則 `bncert` 工具會要求您進行該設定，然後再繼續操作。您的網域必須將流量路由至執行個體的公有 IP 地址，而您需從該地址使用 `bncert` 工具來在執行個體上啟用 HTTPS。此舉措會確認您擁有該網域，並以此作為憑證的驗證。

```
-----  
Welcome to the Bitnami HTTPS Configuration tool.  
-----  
Domains  
  
Please provide a valid space-separated list of domains for which you wish to  
configure your web server.  
  
Domain list []: example.com www.example.com
```

9. `bncert` 工具會詢問您要如何設定網站的重新引導。可用的選項如下：
  - Enable HTTP to HTTPS redirection (啟用 HTTP 至 HTTPS 重新引導) - 指定將瀏覽至網站 HTTP 版本 (即 `http://example.com`) 的使用者自動重新引導至 HTTPS 版本 (即 `https://example.com`)。由於此選項會強制所有訪客使用加密的連線，建議啟用此選項。輸入 Y，並按 Enter 以啟用。
  - Enable non-www to www redirection (啟用非 www 至 www 重新引導) - 指定將瀏覽至網域 (即 `https://example.com`) 頂點的使用者自動重新引導至您網域的 `www` 子網域 (即 `https://www.example.com`)。建議啟用此選項。不過，如果您已在搜索引擎工具 (如 Google 的網站管理員工具) 中將網域的頂點指定為您偏好的網站地址，或者如果您的頂點直接指向 IP，且 `www` 子網域透過 CNAME 記錄參考您的頂點，則您可能需要停用此選項並啟用替代選項 (啟用 `www` 至非 `www` 重新引導)。輸入 Y，並按 Enter 以啟用。

- Enable www to non-www redirection (啟用 www 至非 www 重新引導) - 指定將瀏覽至您網域 www 子網域 (即 `https://www.example.com`) 的使用者自動重新引導至網域的頂點 (即 `https://example.com`)。如果您已啟用非 www 重新引導至 www，我們建議您停用此選項。輸入 N，並按 Enter (確認) 以停用。

您的選取內容應看起來與下列範例類似。

```
Enable/disable redirections
Please select the redirections you wish to enable or disable on your Bitnami
installation.

Enable HTTP to HTTPS redirection [Y/n]: Y

Enable non-www to www redirection [Y/n]: Y

Enable www to non-www redirection [y/N]: N
```

10. 系統會列出即將進行的變更。輸入 Y，並按 Enter (確認) 以確認並繼續。

```
Changes to perform

The following changes will be performed to your Bitnami installation:

1. Stop web server
2. Configure web server to use a free Let's Encrypt certificate for the domains:
example.com www.example.com
3. Configure a cron job to automatically renew the certificate each month
4. Configure web server name to: example.com
5. Enable HTTP to HTTPS redirection (example: redirect http://example.com to
https://example.com)
6. Enable non-www to www redirection (example: redirect example.com to
www.example.com)
7. Start web server once all changes have been performed

Do you agree to these changes? [Y/n]: Y
```

11. 輸入您的電子郵件地址，以與您的 Let's Encrypt 憑證相關聯，然後按 Enter。

```
Create a free HTTPS certificate with Let's Encrypt

Please provide a valid e-mail address for which to associate your Let's Encrypt
certificate.

Domain list: example.com www.example.com

Server name: example.com

E-mail address []: █
```

12. 檢閱 Let's Encrypt 訂閱者協議。輸入 Y，並按 Enter (確認) 以接受該協議並繼續。

```
The Let's Encrypt Subscriber Agreement can be found at:
https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf

Do you agree to the Let's Encrypt Subscriber Agreement? [Y/n]: █
```

執行這些動作是為了在執行個體上啟用 HTTPS，包括請求憑證和設定您指定的重新引導。

```
Performing changes to your installation

The Bitnami HTTPS Configuration Tool will perform any necessary actions to your
Bitnami installation. This may take some time, please be patient.

█
```

系統已成功核發並驗證您的憑證，如果您看到類似以下範例的訊息，則表示已成功在執行個體上設定重新引導。

```
Success

The Bitnami HTTPS Configuration Tool succeeded in modifying your installation.

The configuration report is shown below.

Backup files:
* /opt/bitnami/apache2/conf/httpd.conf.back.202005290035
* /opt/bitnami/apache2/conf/bitnami/bitnami-apps-prefix.conf.back.202005290035
* /opt/bitnami/apache2/conf/bitnami/bitnami.conf.back.202005290035

Find more details in the log file:

/tmp/bncert-202005290035.log

If you find any issues, please check Bitnami Support forums at:

https://community.bitnami.com

Press [Enter] to continue:█
```

bncert 工具會在憑證過期前每 80 天執行自動續約一次。如果您要搭配執行個體使用其他網域和子網域，且要為這些網域啟用 HTTPS，請重複上述步驟。

您現已在 Redmine 執行個體上啟用 HTTPS。下次使用您設定的網域瀏覽至 Redmine 網站時，應該會看到您被重新導向至 HTTPS 連線。

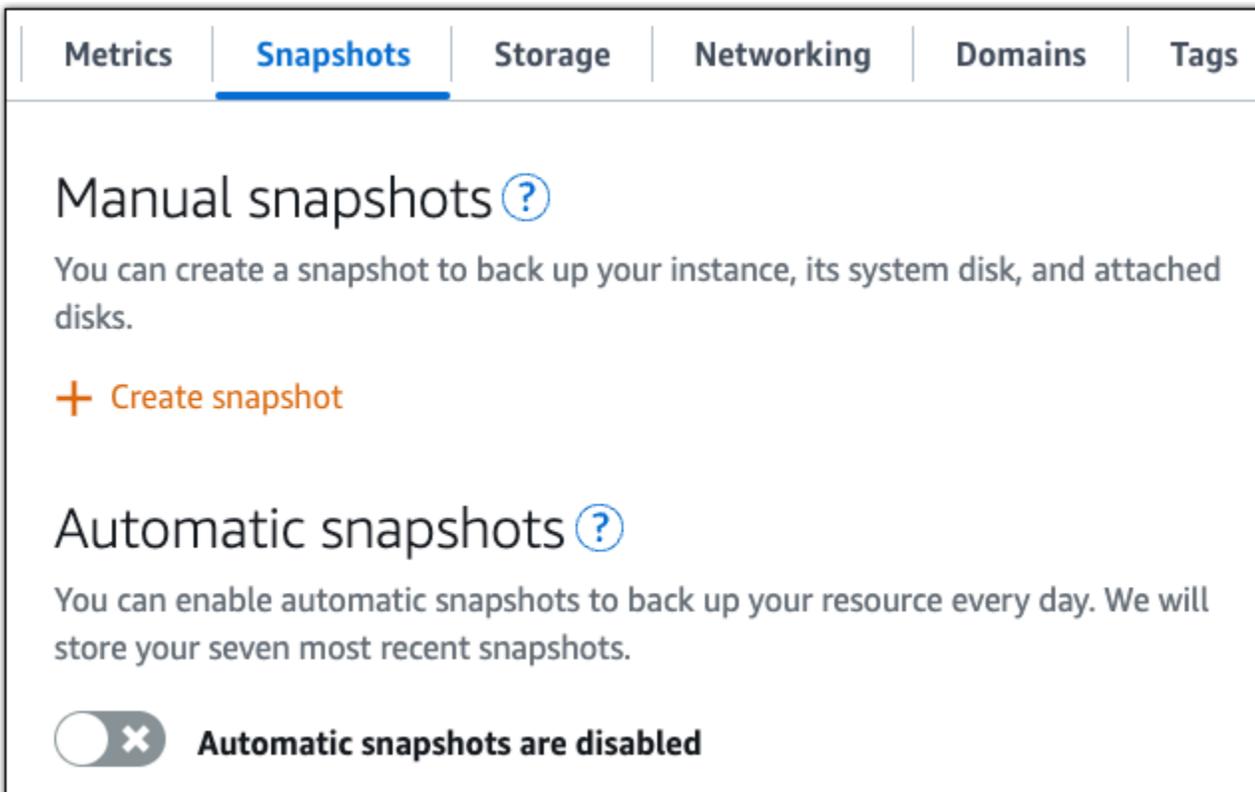
## 步驟 7：閱讀 Redmine 文件並繼續設定網站

閱讀 Redmine 文件以了解如何管理和自訂網站。如需詳細資訊，請參閱 [Redmine guide](#) (Redmine 指南)。

## 步驟 8：建立執行個體的快照

按照您希望的方式設定 Redmine 網站後，請定期建立執行個體的快照以作為備份。您可以手動建立快照，或啟用自動快照，讓 Lightsail 為您建立每日快照。若執行個體出現問題，您可以使用快照建立新的替代執行個體。如需詳細資訊，請參閱[快照](#)。

在執行個體管理頁面的 Snapshot (快照) 索引標籤下，選擇 Create a snapshot (建立快照) 或選擇啟用自動快照。



Metrics | **Snapshots** | Storage | Networking | Domains | Tags

### Manual snapshots ?

You can create a snapshot to back up your instance, its system disk, and attached disks.

**+ Create snapshot**

### Automatic snapshots ?

You can enable automatic snapshots to back up your resource every day. We will store your seven most recent snapshots.

**Automatic snapshots are disabled**

如需詳細資訊，請參閱在 Amazon Lightsail 中建立 [Linux 或 Unix 執行個體的快照](#)或在 [Amazon Lightsail](#) 中[啟用或停用執行個體或磁碟的自動快照](#)。

## WordPress 在 Lightsail 上啟動和設定

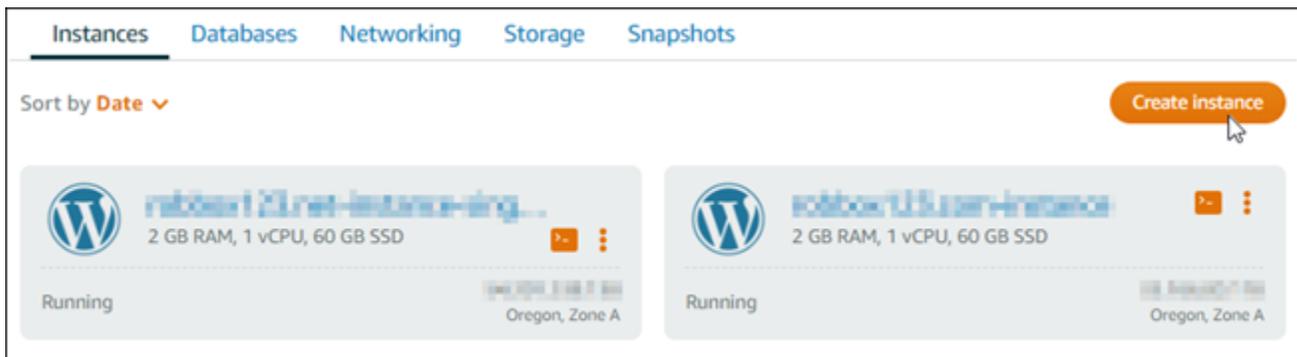
透過這份快速入門指南，您將了解如何在 Amazon Lightsail 上啟動和設定 WordPress 執行個體。

### 步驟 1：建立 WordPress 執行個體

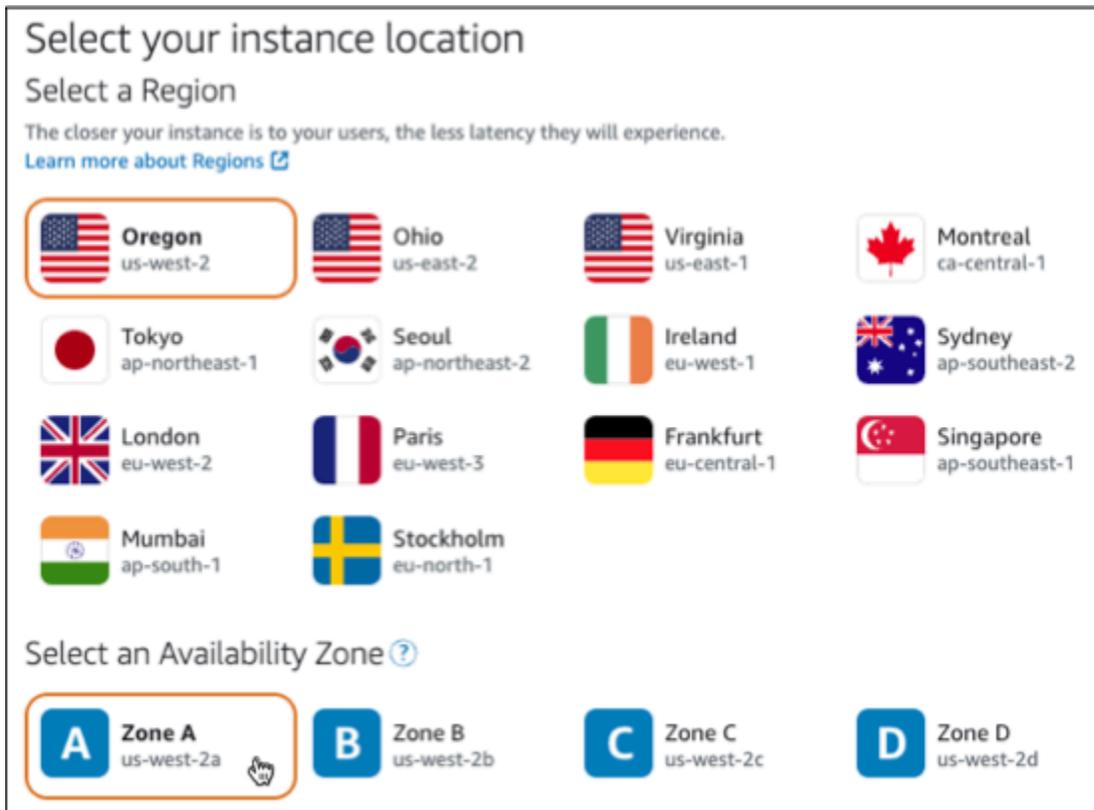
完成下列步驟，讓您的 WordPress 執行個體啟動並執行。

若要建立以下項 Lightsail 的實體 WordPress

1. 登入主 [Lightsail](#) 台。
2. 在 Lightsail 首頁的「實體」區段中，選擇「建立實體」。



3. 為您的執行個體選擇 AWS 區域 和可用區域。



4. 選擇執行個體的映像檔，如下所示：
  - a. 針對 [選取平台]，選擇 [Linux/Unix]。
  - b. 對於選取藍圖，請選擇WordPress。
5. 選擇執行個體方案。

計劃包括以低廉且可預測的成本的機器配置 ( RAM , SSD , vCPU ) 以及數據傳輸額度。

6. 輸入您執行個體的名稱。資源名稱：
  - 每個 Lightsail 帳戶 AWS 區域 中的每個項目都必須是唯一的。
  - 必須包含 2 至 255 個字元。
  - 開頭和結尾必須是英數字元或數字。
  - 可以包含英數字元、數字、句點、破折號和底線。
7. 選擇 建立執行個體。
8. 若要檢視測試部落格文章，請前往執行個體管理頁面，複製頁面右上角顯示的公用 IPv4 位址。將位址貼到連線至網際網路之網頁瀏覽器的位址欄位中。瀏覽器會顯示測試部落格文章。

## 步驟 2：設定您的 WordPress 執行個體

您可以使用可設定下列 WordPress 項目的引導式 step-by-step 工作流程來設定執行個體：

- 已註冊的網域名稱 — 您的 WordPress 網站需要一個容易記住的網域名稱。使用者將指定此網域名稱來存取您的 WordPress 網站。如需詳細資訊，請參閱 [域和 DNS](#)。
- DNS 管理 — 您必須決定如何管理網域的 DNS 記錄。DNS 記錄會告訴 DNS 伺服器與網域或子網域相關聯的 IP 位址或主機名稱。DNS 區域包含您網域的 DNS 記錄。如需詳細資訊，請參閱 [the section called “DNS 在 Lightsail”](#)。
- 靜態 IP 位址 — 如果您停止並啟動執行個體，WordPress 執行個體的預設公用 IP 位址就會變更。當您將靜態 IP 位址附加到執行個體時，即使您停止並啟動執行個體，它仍會保持不變。如需詳細資訊，請參閱 [the section called “IP 地址”](#)。
- SSL/TLS 憑證 — 建立驗證憑證並將其安裝在執行個體上之後，您可以為網站啟用 HTTPS，以便透過註冊 WordPress 網域路由傳送至執行個體的流量會使用 HTTPS 加密。如需詳細資訊，請參閱 [the section called “啟用 HTTPS”](#)。

### Tip

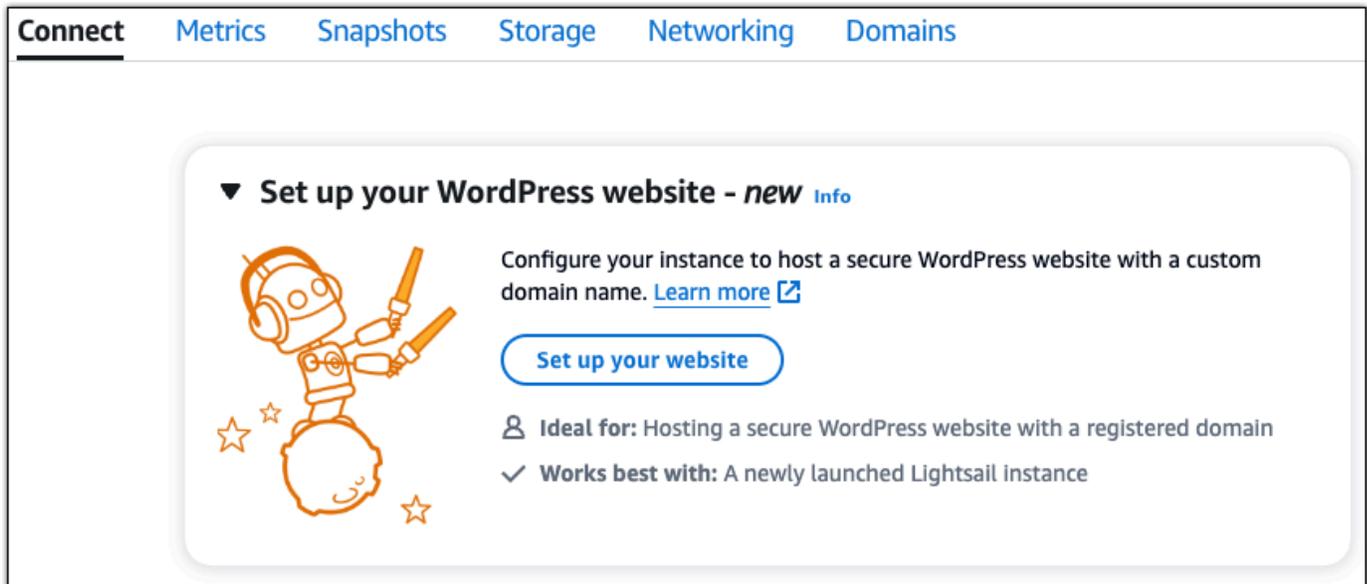
開始之前，請先檢閱下列秘訣。如需疑難排解的資訊，請參閱 [疑 WordPress 難排解](#)

- 安裝程式支援在 2023 年 1 月 1 日之後建立的 WordPress 版本 6 及更新版本的 Lightsail 執行個體。
- 在安裝期間執行的 Certbot 相依性檔案、HTTPS 重新寫入指令碼和憑證更新指令碼會儲存在執行個體的 `/opt/bitnami/lightsail/scripts/` 目錄中。
- 您的執行個體必須處於執行中狀態。如果執行個體剛啟動，請等待幾分鐘的時間讓 SSH 連線準備就緒。
- 執行個體防火牆上的連接埠 22、80 和 443 必須允許在安裝程式執行時從任何 IP 位址進行 TCP 連線。如需詳細資訊，請參閱 [執行個體防火牆](#)。
- 當您新增或更新指向來自頂點網域 (example.com) 及其 www 子網域 (www.example.com) 流量的 DNS 記錄時，這些記錄必須在整個網際網路中傳播。您可以驗證您的 DNS 更改已經通過使用工具生效，或 [DNS 查找](#) 從 MxToolbox
- 在 2023 年 1 月 1 日之前創建的 WordPress 實例可能包含一個不推薦使用的 Certbot 個人 Package 存檔 (PPA) 存儲庫，這將導致網站設置失敗。如果此儲存庫在安裝期間存在，它將從現有路徑中移除，並備份到執行個體上的下列位置：`~/opt/bitnami/lightsail/repo.backup` 有關已過時 PPA 的更多信息，請參閱規範網站上的 [Certbot PPA](#)。

- 讓我們加密證書將每 60 到 90 天自動續訂一次。
- 進行安裝程序時，請勿停止或變更執行個體。設定執行個體最多可能需要 15 分鐘的時間。您可以在執行個體連線索引標籤中檢視每個步驟的進度。

## 使用網站設定精靈設定執行個體

1. 在執行個體管理頁面的 [Connect] 索引標籤上，選擇 [設定您的網站]。



2. 針對「指定網域名稱」，請使用現有的 Lightsail 受管理網域、向 Lightsail 註冊新網域，或使用您透過其他網域註冊機構註冊的網域。選擇 [使用此網域] 以前往下一個步驟。
3. 對於設定 DNS，請執行下列其中一個動作：
  - 選擇受管理的網域以使用 Lightsail DNS 區域。選擇 [使用此 DNS 區域] 以前往下一個步驟。
  - 選擇第三方網域以使用管理您網域 DNS 記錄的主機服務。請注意，如果您稍後決定使用，我們會在您的 Lightsail 帳戶中建立相符的 DNS 區域。選擇「使用第三方 DNS」以進行下一步。
4. 在 [建立靜態 IP 位址] 中，輸入靜態 IP 位址的名稱，然後選擇 [建立靜態 IP]。
5. 針對 [管理網域指派]，選擇 [新增指派]，選擇網域類型，然後選擇 [新增]。選擇「繼續」以前往下一個步驟。
6. 在「建立 SSL/TLS 憑證」中，選擇您的網域和子網域、輸入電子郵件地址、選取「我授權 Lightsail 在我的執行個體上設定讓我們加密憑證」，然後選擇「建立憑證」。我們開始設定 Lightsail 資源。

進行安裝程序時，請勿停止或變更執行個體。設定執行個體最多可能需要 15 分鐘的時間。您可以在執行個體連線索引標籤中檢視每個步驟的進度。

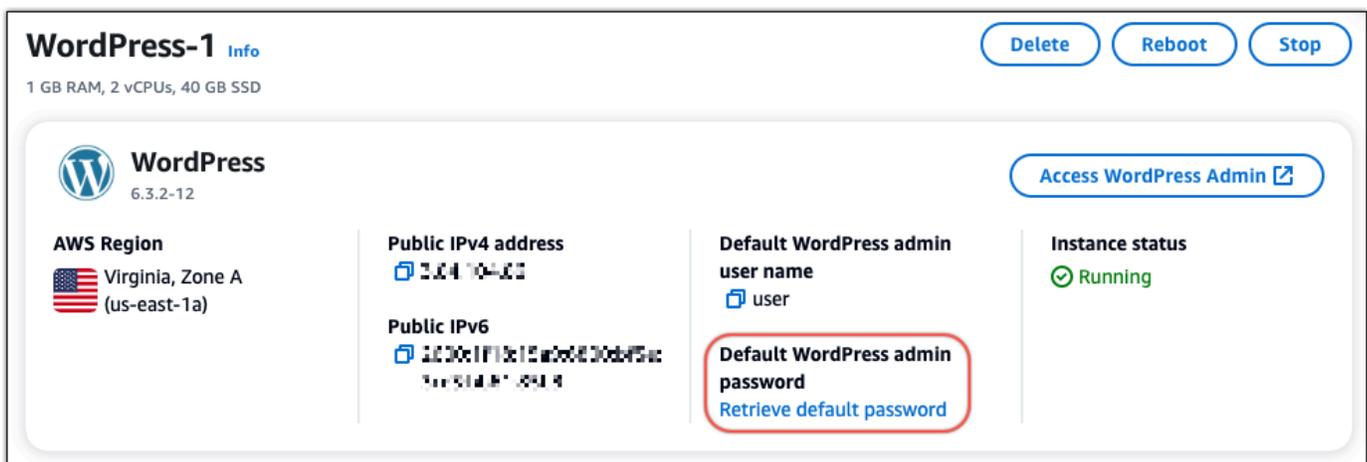
7. 網站設定完成後，請確認您在網域指派步驟中指定的 URL 是否開啟您的網 WordPress 站。

### 步驟 3：獲取您 WordPress 網站的默認應用程式密碼

您需要預設的應用程式密碼才能登入 WordPress 網站的管理儀表板。

取得 WordPress 管理員的預設密碼

1. 開啟執行個體的執行 WordPress 個體管理頁面。
2. 在 WordPress 面板上，選擇「擷取預設密碼」。這會展開頁面底部的存取預設密碼。



3. 選擇 [啟動] CloudShell。這將在頁面底部打開一個面板。
4. 選擇「複製」，然後將內容貼到 CloudShell 視窗中。您可以將光標放在 CloudShell 提示符處並按 Ctrl+V，也可以右鍵單擊以打開菜單，然後選擇粘貼。
5. 記下 CloudShell 視窗中顯示的密碼。您需要此功能才能登入 WordPress 網站的管理儀表板。

```
[cloudshell-user@ip-10-114-41-117 ~]$ AWS_REGION=us-east-1 ~/lightsail_connect WordPress-1 cat bitnami_application_password
JKzh8wB5FAR!
```

### 步驟 4：登入您的 WordPress 網站

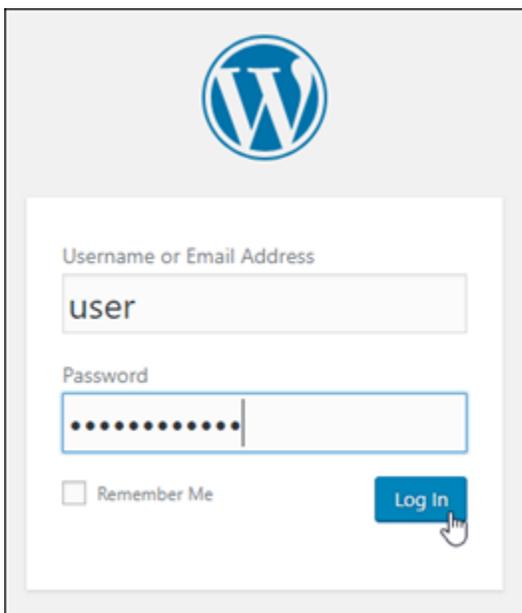
現在您擁有預設的使用者密碼，請瀏覽至 WordPress 網站的首頁，然後登入管理儀表板。登入之後，您可以變更預設密碼。

## 若要登入管理儀表板

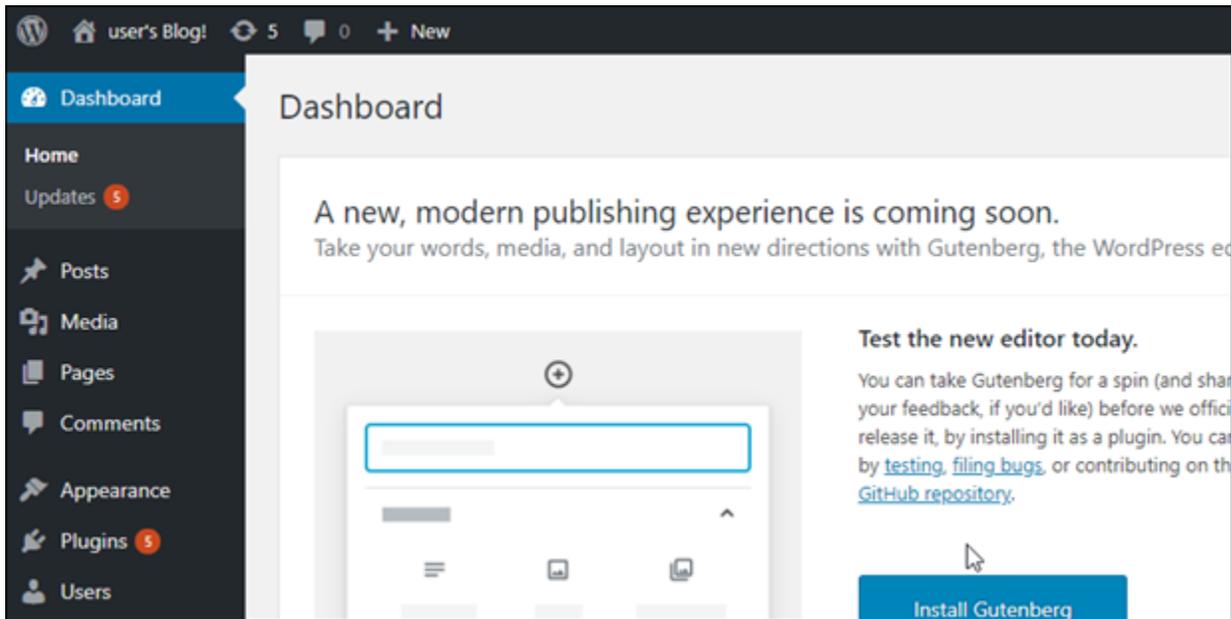
1. 開啟執行個體的執行 WordPress 個體管理頁面。
2. 在WordPress面板上，選擇 [存取 WordPress 管理員]。
3. 在 [存取您的 WordPress 管理儀表板] 面板的 [使用公用 IP 位址] 下方，選擇具有此格式的連結：

HTTP : *//## IPV4* 地址。 /WP-管理員

4. 針對使用者名稱或電子郵件地址，輸入 **user**
5. 在「密碼」中，輸入在上一個步驟中取得的密碼。
6. 選擇 Log in (登入)。



您現在已登入 WordPress 網站的管理儀表板，您可以在其中執行管理動作。有關管理 WordPress 網站的更多信息，請參閱文檔中的 [WordPress WordPress Codex](#)。



## 步驟 5：閱讀 Bitnami 文件

閱讀 Bitnami 文檔以了解如何在您的 WordPress 網站上執行管理任務，例如安裝插件，自定義主題以及升級您的版本。WordPress

如需詳細資訊，請參 [WordPress](#) 閱的. AWS 雲端

## 在 Lightsail 上設置 WordPress 多站點

在 Amazon Lightsail 上啟動並執行 WordPress 多網站執行個體後，您應採取以下幾個步驟才能開始使用：

### 內容

- [步驟 1：閱讀 Bitnami 文件](#)
- [步驟 2：獲取默認應用程序密碼以訪問 WordPress 管理儀表板](#)
- [步驟 3：將靜態 IP 地址連接至您的執行個體](#)
- [步驟 4：登入 WordPress 多網站網站的管理儀表板](#)
- [步驟 5：將您註冊的域名的流量路由到您的 WordPress 多站點網站](#)
- [第 6 步：將博客作為域或子域添加到您的 WordPress 多站點網站](#)
- [步驟 7：閱讀 WordPress 多站點文檔並繼續配置您的網站](#)
- [步驟 8：建立執行個體的快照](#)

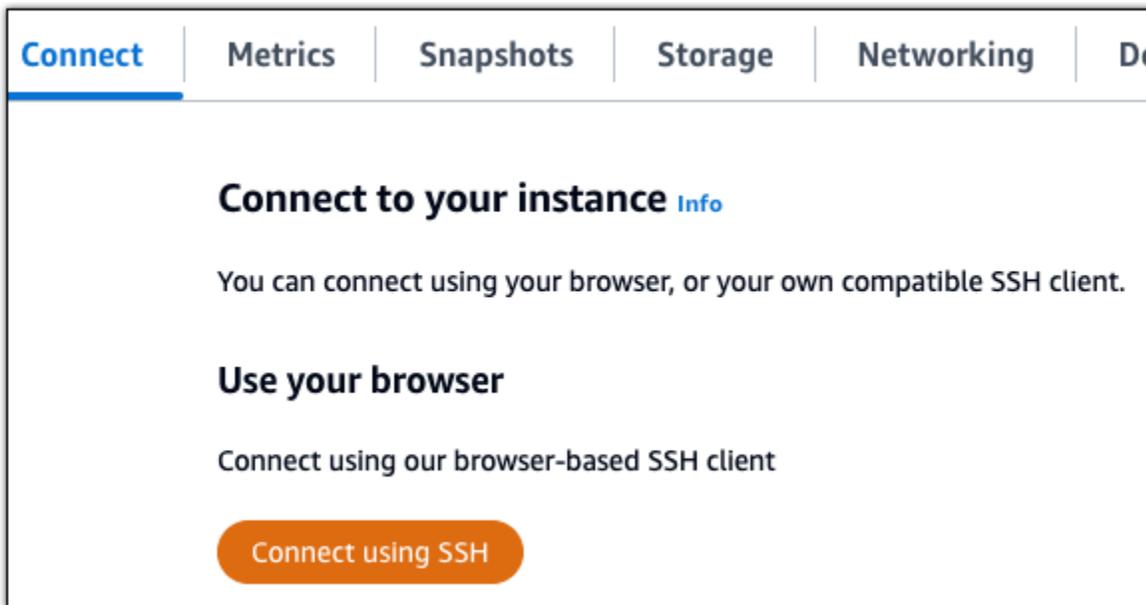
## 步驟 1：閱讀 Bitnami 文件

請閱讀 Bitnami 文件以了解如何設定 WordPress 多網站執行個體。如需詳細資訊，請參閱 [由 Bitnami 封裝的 WordPress 多網站](#)。AWS 雲端

## 步驟 2：獲取默認應用程式密碼以訪問 WordPress 管理儀表板

完成下列程序以取得存取 WordPress 多網站網站管理儀表板所需的預設應用程式密碼。如需詳細資訊，請參閱 [在 Amazon Lightsail 中取得 Bitnami 執行個體的應用程式使用者名稱和密碼](#)。

1. 在執行個體管理頁面的 Connect (連接) 索引標籤下，選擇 Connect using SSH (使用 SSH 連接)。



2. 連線後，請輸入下列命令以取得預設應用程式密碼：

```
cat $HOME/bitnami_application_password
```

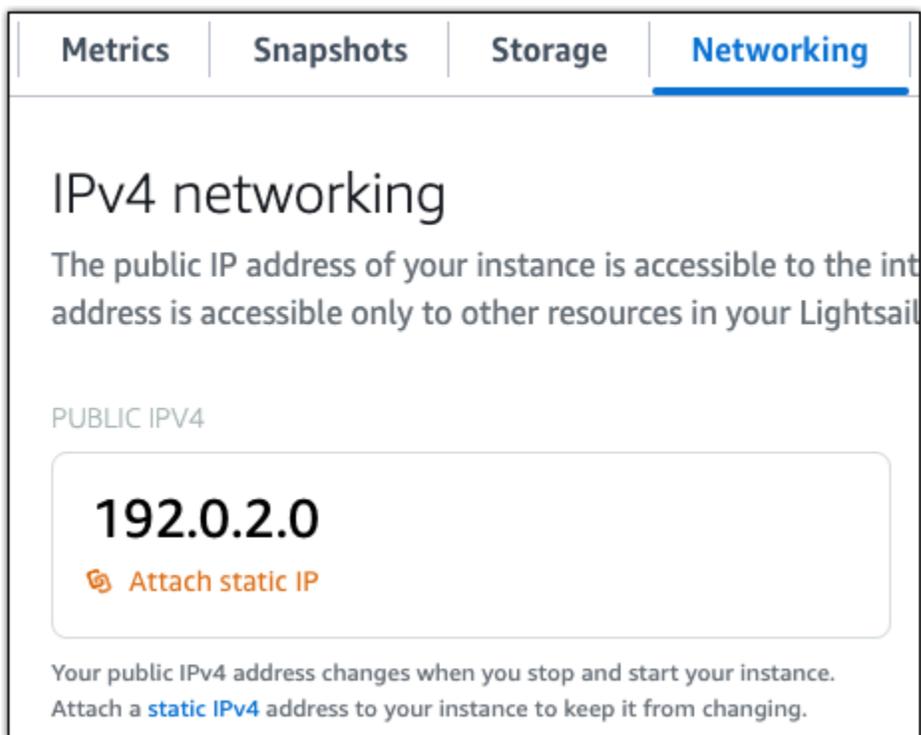
您應該會看到類似於以下範例的回應，其中包含預設應用程式密碼。使用此密碼登入 WordPress 多網站網站的管理儀表板。

```
bitnami@ip-172-31-23-100:~$ cat bitnami_application_password
JeVN8xDWlCIp
bitnami@ip-172-31-23-100:~$
```

### 步驟 3：將靜態 IP 地址連接至您的執行個體

您第一次建立執行個體時，所指派的公有 IP 地址將會在每次停用和啟用執行個體時變更。您應該建立靜態 IP 地址並將其連接至執行個體，以確保其公有 IP 地址不會變更。如果將註冊的網域 (例如 example.com) 與執行個體搭配使用，便無須在每次停用或啟用執行個體時更新您網域的網域名稱系統 (DNS)。您可以將一個靜態 IP 連接至一個執行個體。

在執行個體管理頁面的 Networking#(聯網) 索引標籤下，選擇 Create a static IP (建立靜態 IP) 或 Attach static IP (連接靜態 IP)(若您先前已建立可以連接至執行個體的靜態 IP)，然後遵循頁面上的指示執行操作。如需詳細資訊，請參閱[建立靜態 IP 並將其附接至執行個體](#)。

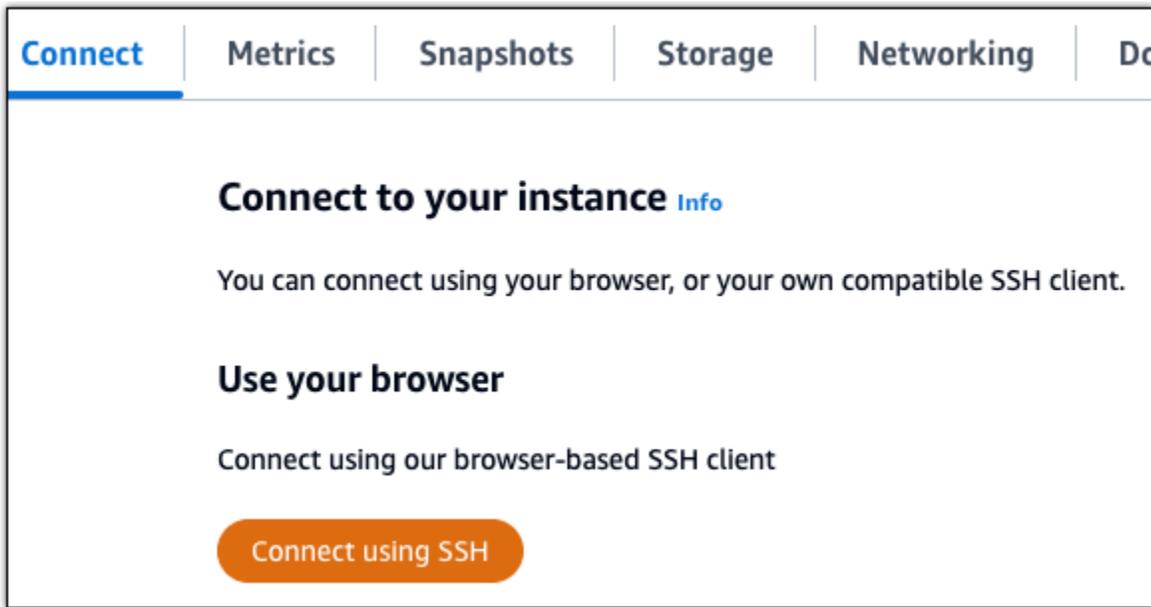


將新的靜態 IP 位址附加至執行個體之後，您必須完成下列程序，以 WordPress 瞭解新的靜態 IP 位址。

1. 請記下執行個體的新靜態 IP 地址。這會列在執行個體管理頁面的標頭區段中。



2. 在執行個體管理頁面的 Connect (連接) 索引標籤下，選擇 Connect using SSH (使用 SSH 連接)。



3. 連接後，請輸入以下命令。將 *<StaticIP>* 取代為執行個體新的靜態 IP 地址。

```
sudo /opt/bitnami/configure_app_domain --domain <StaticIP>
```

範例：

```
sudo /opt/bitnami/configure_app_domain --domain 203.0.113.0
```

您應該會看到類似於以下範例的回應。執行個體上的 WordPress 網站現在應該知道新的靜態 IP 位址。

```
bitnami@ip-173-20-0-107:~$ sudo /opt/bitnami/configure_app_domain --domain 203.0.113.0
Configuring domain to 203.0.113.0
2021-03-12T15:49:22.000Z - info: Saving configuration info to disk
prestashop 15:49:22.41 INFO ==> Trying to connect to the database server
prestashop 15:49:22.44 INFO ==> Updating hostname in database
prestashop 15:49:22.46 INFO ==> Purging cache
Disabling automatic domain update for IP address changes
```

如果該命令失敗，您可能正在使用較舊版本的 WordPress 多網站執行個體。改為嘗試執行下列命令。將 *<StaticIP>* 取代為執行個體新的靜態 IP 地址。

```
cd /opt/bitnami/apps/wordpress
sudo ./bnconfig --machine_hostname <StaticIP>
```

在執行這些命令後，輸入以下命令，以防止 bnconfig 工具在伺服器每次重新啟動時自動執行。

```
sudo mv bnconfig bnconfig.disabled
```

## 步驟 4：登入 WordPress 多網站網站的管理儀表板

現在您擁有預設的應用程式密碼，請完成下列程序以導覽至 WordPress 多網站網站的首頁，然後登入管理儀表板。登入後，您可以開始自訂網站並進行管理級變更。如需有關您可以在中執行的動作的詳細資訊 WordPress，請參閱本指南稍後的[步驟 7：閱讀 WordPress 多網站文件並繼續設定您的網站一節](#)。

1. 在執行個體管理頁面的 Connect (連接) 索引標籤下，記下執行個體的公有 IP 地址。公有 IP 地址也會顯示在執行個體管理頁面的標頭區段。



2. 瀏覽至執行個體的公有 IP 地址，例如前往 <http://203.0.113.0>。

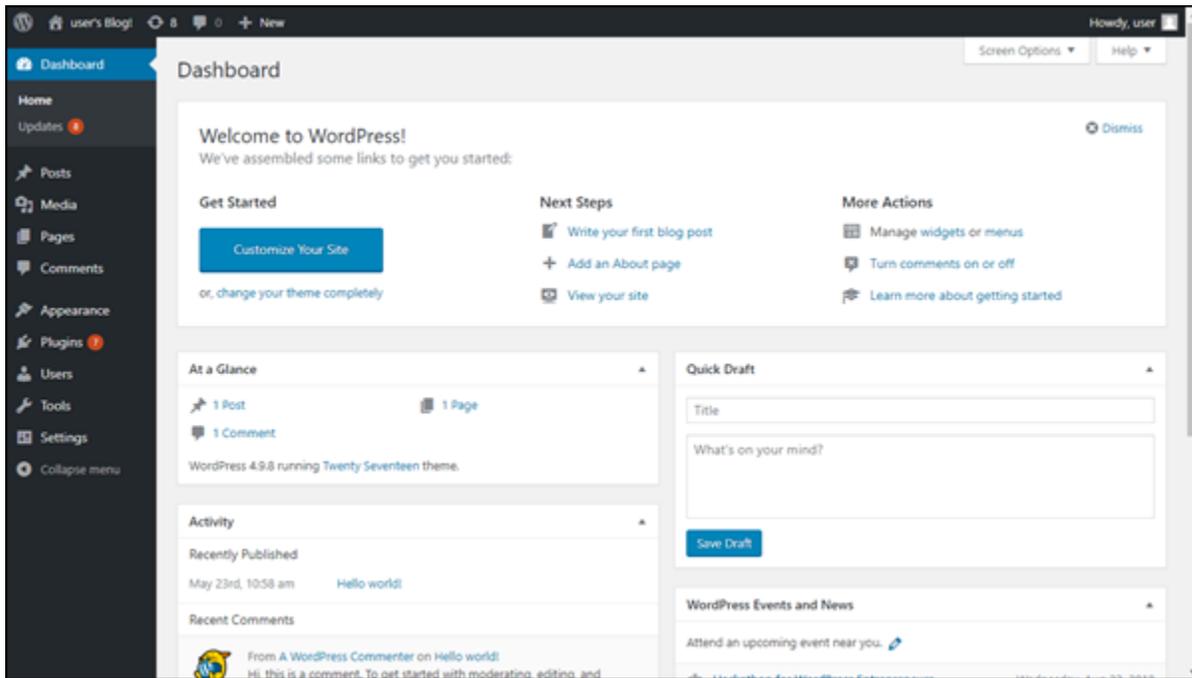
您 WordPress 網站的首頁應該會出現。

3. 選擇 WordPress 網站首頁右下角的「管理」。

如果未顯示 Manage (管理) 橫幅，您可以透過瀏覽至 <http://<PublicIP>/wp-login.php> 前往登入頁面。將 *<PublicIP>* 取代為您執行個體的公有 IP 地址。

4. 使用先前依本指南指示取得的預設使用者名稱 (user) 和預設密碼登入。

WordPress 管理儀表板隨即出現。



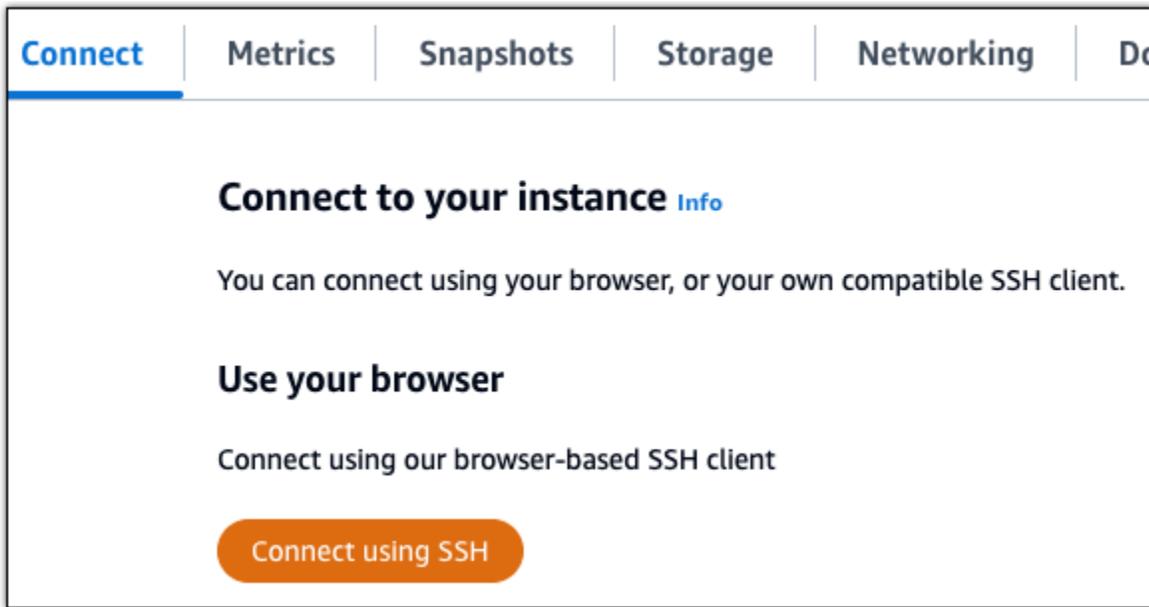
## 步驟 5：將您註冊的域名的流量路由到您的 WordPress 多站點網站

若要將已註冊網域名稱 (例如 `example.com`) 的流量路由到您的 WordPress 多網站網站，請將記錄新增至網域的 DNS。DNS 記錄通常會在您註冊網域的註冊商處進行管理和託管。不過，我們建議您將網域 DNS 記錄的管理權限轉移至 Lightsail，以便您可以使用 Lightsail 主控台進行管理。

在 Lightsail 主控台首頁的 [網域和 DNS] 索引標籤下，選擇 [建立 DNS 區域]，然後依照頁面上的指示進行。如需詳細資訊，請參閱 [在 Lightsail 中建立 DNS 區域以管理網域的 DNS 記錄](#)。

在您的網域名稱將流量路由到執行個體之後，您必須完成下列程序，以 WordPress 瞭解網域名稱。

1. 在執行個體管理頁面的 Connect (連接) 索引標籤下，選擇 Connect using SSH (使用 SSH 連接)。



2. 連接後，請輸入以下命令。將 `< DomainName >` 取代為將流量路由到執行個體的網域名稱。

```
sudo /opt/bitnami/configure_app_domain --domain <DomainName>
```

範例：

```
sudo /opt/bitnami/configure_app_domain --domain www.example.com
```

您應該會看到類似於以下範例的回應。WordPress 多站點軟件現在應該知道域名。

```
bitnami@ip-172-31-0-197:~$ sudo /opt/bitnami/configure_app_domain --domain www.example.com
Configuring domain to www.example.com
2021-03-12T15:49:22.000Z - info: Saving configuration info to disk
prestashop 15:49:22.41 INFO ==> Trying to connect to the database server
prestashop 15:49:22.44 INFO ==> Updating hostname in database
prestashop 15:49:22.46 INFO ==> Purging cache
Disabling automatic domain update for IP address changes
```

如果該命令失敗，您可能正在使用較舊版本的 WordPress 多網站執行個體。改為嘗試執行下列命令。將 `< DomainName >` 取代為將流量路由到執行個體的網域名稱。

```
cd /opt/bitnami/apps/wordpress
sudo ./bnconfig --machine_hostname <DomainName>
```

在執行這些命令後，輸入以下命令，以防止 bnconfig 工具在伺服器每次重新啟動時自動執行。

```
sudo mv bnconfig bnconfig.disabled
```

如果您瀏覽至您為執行個體設定的網域名稱，您應該會被重新導向至 WordPress 多網站網站的主要部落格。接下來，您必須決定是否要將博客添加為域或子域添加到您的 WordPress 多站點網站。如需詳細資訊，請繼續參閱本指南的下一個[步驟 6：將部落格新增為網域或子網域至您的 WordPress 多網站網站](#)一節。

## 第 6 步：將博客作為域或子域添加到您的 WordPress 多站點網站

WordPress 多站點旨在在一個實例上託管多個博客網站。WordPress 當您將新的博客網站添加到 WordPress 多站點時，您可以將其配置為使用自己的域或 WordPress 多站點主域的子域。您可以將 WordPress 多網站設定為僅使用其中一個選項。例如：若您選擇將部落格網站新增為網域，則無法將其新增為子網域，反之亦然。若要設定其中一個選項，請參閱以下任一指南：

- 若要將部落格網站新增為網域，例如example1.com和example2.com，請參閱[在 Lightsail 中將部落格做為網域新增至您的 WordPress 多網站執行個體](#)。
- 若要將部落格網站新增為 WordPress 多網站主要網域的子網域，例如one.example.com和two.example.com，請參閱[將部落格作為子網域新增至 Lightsail 中的 WordPress 多網站執行個體](#)。

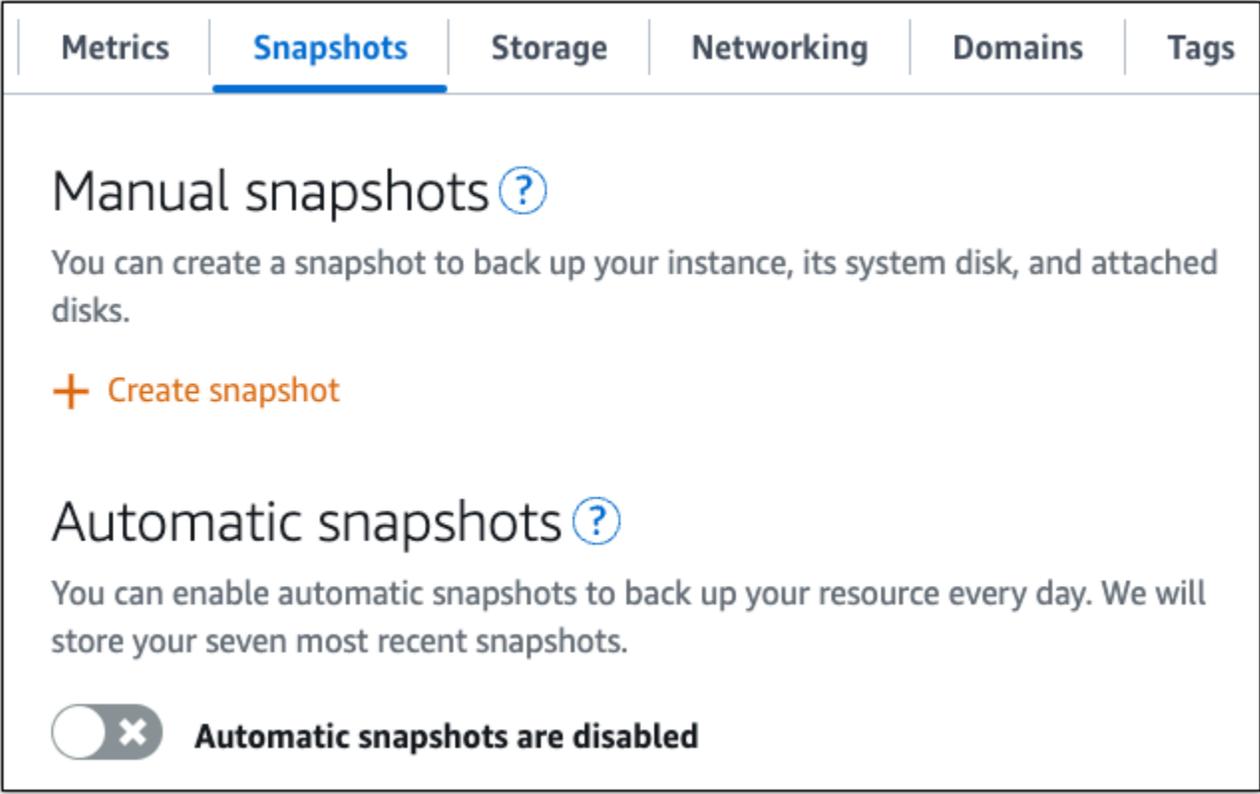
## 步驟 7：閱讀 WordPress 多站點文檔並繼續配置您的網站

閱讀 WordPress 多站點文檔以了解如何管理和自定義您的網站。如需詳細資訊，請參閱[WordPress 多站台網路管理文件](#)。

## 步驟 8：建立執行個體的快照

在您設定您的 WordPress 多網站網站您想要的方式之後，請建立執行個體的定期快照以備份它。您可以手動建立快照，或啟用自動快照，讓 Lightsail 為您建立每日快照。若執行個體出現問題，您可以使用快照建立新的替代執行個體。如需詳細資訊，請參閱[快照](#)。

在執行個體管理頁面的 Snapshot (快照) 索引標籤下，選擇 Create a snapshot (建立快照) 或選擇啟用自動快照。



Metrics | **Snapshots** | Storage | Networking | Domains | Tags

## Manual snapshots

You can create a snapshot to back up your instance, its system disk, and attached disks.

[+ Create snapshot](#)

## Automatic snapshots

You can enable automatic snapshots to back up your resource every day. We will store your seven most recent snapshots.

**Automatic snapshots are disabled**

如需詳細資訊，請參閱在 Amazon Lightsail 中建立 [Linux 或 Unix 執行個體的快照](#)或在 [Amazon Lightsail](#) 中[啟用或停用執行個體或磁碟的自動快照](#)。

## 在 Lightsail 上使用 Bitnami 應用程式和堆疊

本節涵蓋下列與 Amazon Lightsail 執行個體上的 Bitnami 應用程式相關主題：

### 主題

- [取得 Lightsail Bitnami 執行個體的預設應用程式使用者名稱和密碼](#)
- [從執行個體中移除比特納米橫幅](#)

## 取得 Lightsail Bitnami 執行個體的預設應用程式使用者名稱和密碼

Bitnami 提供許多應用程式執行個體映像或藍圖，您可以建立為 Amazon Lightsail 執行個體 (即虛擬私有伺服器)。這些藍圖在 Lightsail 主控台的執行個體建立頁面中描述為「由 Bitnami 封裝」。

在您使用 Bitnami 藍圖建立執行個體之後，即可登入及管理執行個體。若要這樣做，您必須取得預設的使用者名稱和密碼，才能讓應用程式和/或資料庫在執行個體上執行。本文說明如何取得登入及管理透過下列藍圖建立之 Lightsail 執行個體所需的資訊：

- WordPress 博客和內容管理應用程式
- WordPress 多站點博客和內容管理應用程式，支持同一實例上的多個網站
- Django 開發堆疊
- Ghost 部落格和內容管理應用程式
- LAMP開發堆棧 (PHP7)
- Node.js 開發堆疊
- Joomla 內容管理應用程式
- Magento 電子商務應用程式
- MEAN開發堆疊
- Drupal 內容管理應用程式
- GitLab CE 存儲庫應用
- Redmine 專案管理應用程式
- 尼金克斯 ( LEMP ) 開發堆棧

## 取得預設的 Bitnami 應用程式和資料庫使用者名稱

以下是使用 Bitnami 藍圖建立的 Lightsail 執行個體的預設應用程式和資料庫使用者名稱：

### Note

並非所有 Bitnami 藍圖皆包含應用程式或資料庫。當藍圖不包含應用程式或資料庫時，此使用者名稱將列為不適用 (N/A)。

- WordPress，包括 WordPress 多站點
  - 應用程式使用者名稱：user
  - 資料庫使用者名稱：root
- PrestaShop
  - 應用程式使用者名稱：user@example.com
  - 資料庫使用者名稱：root
- Django
  - 應用程式使用者名稱：N/A
  - 資料庫使用者名稱：root

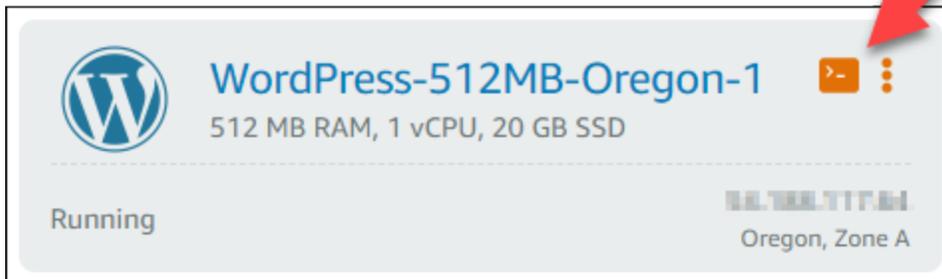
- Ghost
  - 應用程式使用者名稱 : `user@example.com`
  - 資料庫使用者名稱 : `root`
- LAMP堆疊 (PHP5 和 PHP 7)
  - 應用程式使用者名稱 : `N/A`
  - 資料庫使用者名稱 : `root`
- Node.js
  - 應用程式使用者名稱 : `N/A`
  - 資料庫使用者名稱 : `N/A`
- Joomla
  - 應用程式使用者名稱 : `user`
  - 資料庫使用者名稱 : `root`
- Magento
  - 應用程式使用者名稱 : `user`
  - 資料庫使用者名稱 : `root`
- MEAN
  - 應用程式使用者名稱 : `N/A`
  - 資料庫使用者名稱 : `root`
- Drupal
  - 應用程式使用者名稱 : `user`
  - 資料庫使用者名稱 : `root`
- GitLab 特首
  - 應用程式使用者名稱 : `user`
  - 資料庫使用者名稱 : `postgres`
- Redmine
  - 應用程式使用者名稱 : `user`
  - 資料庫使用者名稱 : `root`
- Nginx
  - 應用程式使用者名稱 : `N/A`
  - 資料庫使用者名稱 : `root`

## 取得預設的 Bitnami 應用程式和資料庫使用者密碼

預設應用程式和資料庫密碼存放在您的執行個體。您可以使用 Lightsail 主控台中的基於瀏覽器的SSH終端機連接到該終端並執行特殊命令來擷取它。

若要取得預設的 Bitnami 應用程式和資料庫使用者密碼

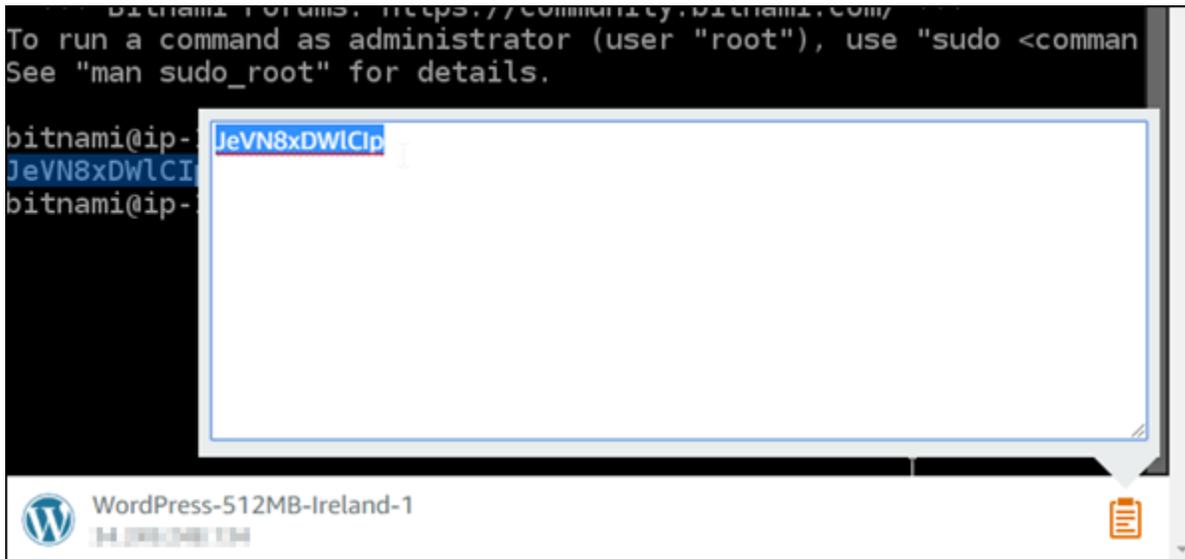
1. 登入主 [Lightsail](#) 台。
2. 如果您尚未建立，請使用 Bitnami 藍圖建立執行個體。如需詳細資訊，請參閱[建立 Amazon Lightsail VPS](#)
3. 在 Lightsail 首頁上，選擇您要連線之執行個體的快速連線圖示。



以瀏覽器為基礎的SSH用戶端視窗隨即開啟，如下列範例所示。



5. 在終端機畫面中，反白顯示密碼，然後選擇瀏覽器SSH用戶端視窗右下角的剪貼簿圖示。
6. 在剪貼簿文字方塊中，反白選取您要複製的文字，然後按下 Ctrl+C (Ctrl+C) 或 Cmd+C (Cmd+C)，將文字複製到本機的剪貼簿。



#### Important

此時請務必將您的密碼儲存至某個位置。您可以稍後登入您執行個體上的 Bitnami 應用程式來進行變更。

## 登入您執行個體上的 Bitnami 應用程式

對於透過 Joomla WordPress、Magento、Drupal、GitLab CE 和紅礦藍圖建立的執行個體，請瀏覽至執行個體的公用 IP 位址登入應用程式。

### 登入 Bitnami 應用程式

1. 在瀏覽器視窗中，導覽至您執行個體的公有 IP 地址。

Bitnami 應用程式首頁將會開啟。首頁會根據您為執行個體選擇的 Bitnami 藍圖而顯示。例如，這是 WordPress 應用程式首頁：

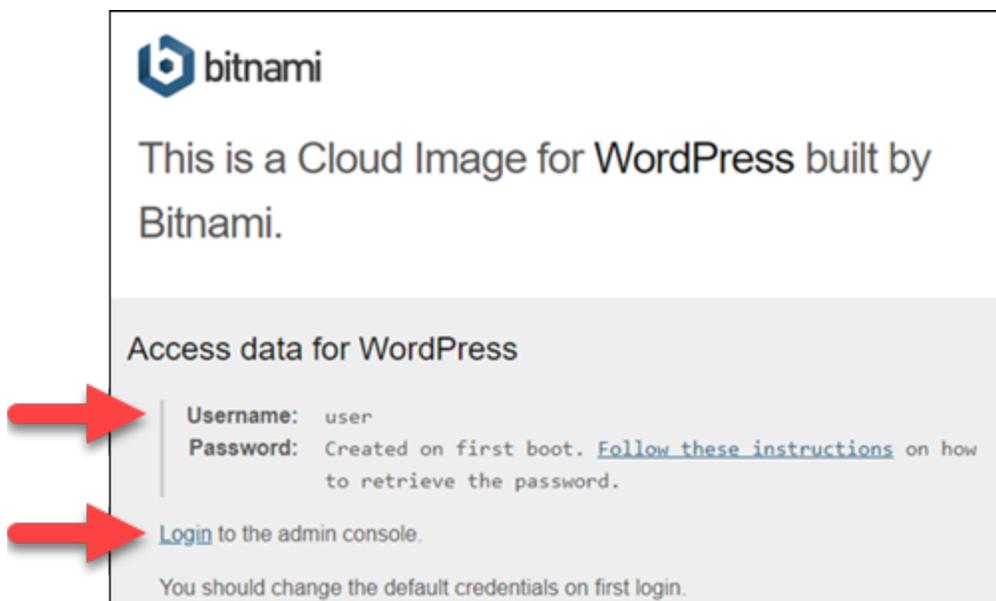


2. 選擇應用程式首頁右下角的 Bitnami 標誌，移至應用程式資訊頁面。

**Note**

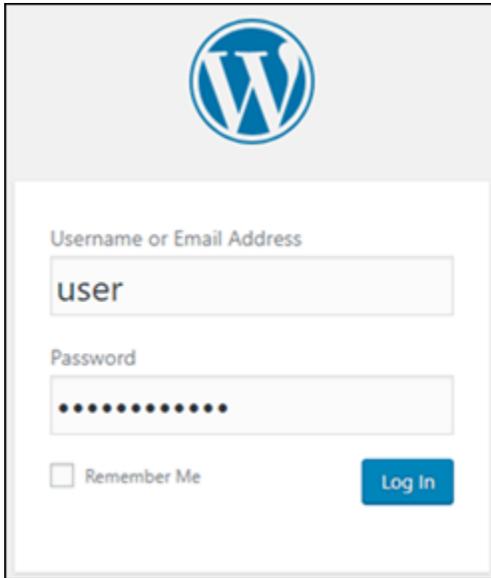
GitLab CE 應用程式不會顯示比特名稱標誌。請改用 GitLab CE 首頁上顯示的使用者名稱和密碼文字欄位登入。

應用程式資訊頁面包含預設的使用者名稱，以及您執行個體上的應用程式登入頁面的連結。



3. 選擇該頁面上的登入連結，移至您執行個體上的應用程式登入頁面。

4. 輸入您剛取得的使用者名稱和密碼，然後選擇 Log In (登入)。

A screenshot of the WordPress login interface. At the top center is the WordPress logo (a blue 'W' inside a circle). Below it, there are two input fields: the first is labeled 'Username or Email Address' and contains the text 'user'; the second is labeled 'Password' and contains ten black dots. Below the password field is a checkbox labeled 'Remember Me' which is unchecked. To the right of the checkbox is a blue button with the text 'Log In' in white.

## 後續步驟

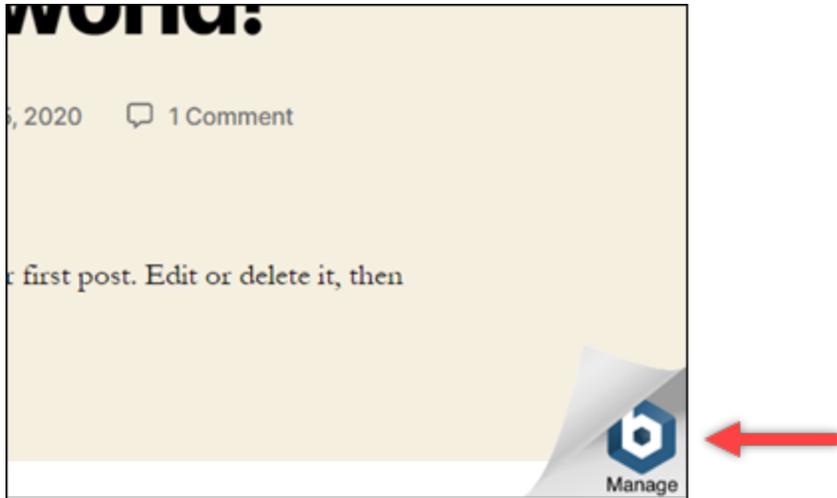
使用以下連結以進一步了解 Bitnami 藍圖並檢視教學課程。例如，您可以為 WordPress 執行個體[安裝外掛程式](#)或[啟用SSL憑證HTTPS支援](#)。

- [WordPress 用於 Amazon Web Services 的名稱](#)
- [Amazon Web Services 的比特名稱LAMP堆棧](#)
- [適用於 Amazon Web Services 的 Bitnami Node.js](#)
- [適用於 Amazon Web Services 的 Bitnami Joomla](#)
- [適用於 Amazon Web Services 的 Bitnami Magento](#)
- [Amazon Web Services 的比特名稱MEAN堆棧](#)
- [適用於 Amazon Web Services 的 Bitnami Drupal](#)
- [GitLab 用於 Amazon Web Services 的名稱](#)
- [適用於 Amazon Web Services 的 Bitnami Redmine](#)
- [Amazon Web Services 的比特名 \( LEMP堆棧 \)](#)

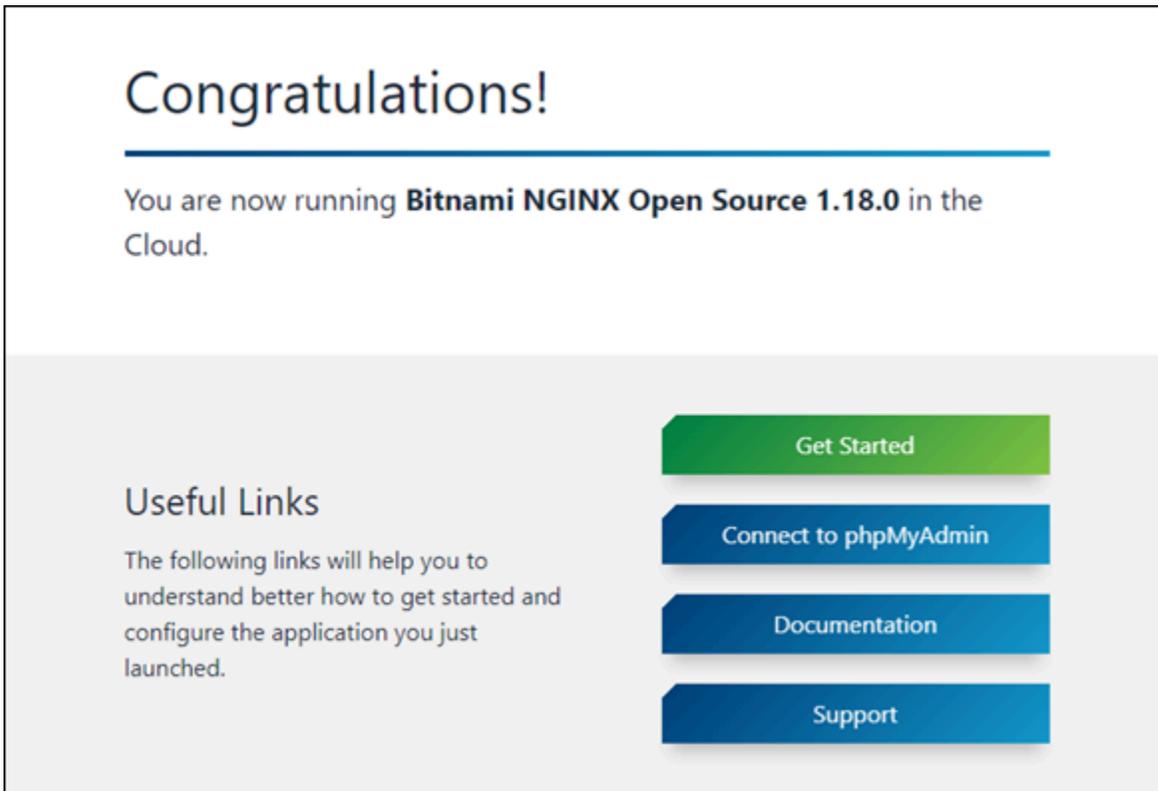
如需詳細資訊，請參閱使用 Amazon Lightsail [開始使用 Bitnami 應用程式或使用 Amazon Lightsail](#)。FAQ

## 從執行個體中移除比特納米橫幅

可以為 Amazon Lightsail 執行個體選取的某些 Bitnami 藍圖會在應用程式的首頁上顯示 Bitnami 橫幅。在下列「由 Bitnami 認證」WordPress 執行個體的範例中，Bitnami 橫幅會顯示在首頁的右下角。在本指南中，我們會為您介紹如何從執行個體上的應用程式首頁永久移除 Bitnami 圖示。



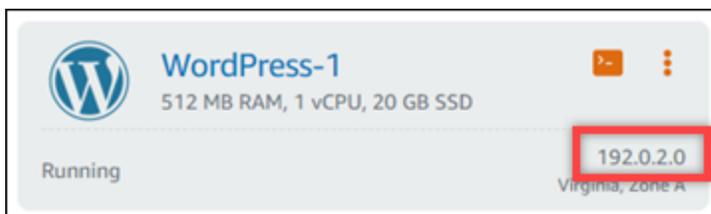
並非所有 Bitnami 藍圖應用程式都會在應用程式的首頁上顯示 Bitnami 橫幅。請造訪 Lightsail 執行個體的首頁，以判斷是否顯示 Bitnami 橫幅。在「由 Bitnami 封裝」Nginx 執行個體的以下範例中，頁面並未顯示 Bitnami 圖示，而是顯示預留位置資訊頁面，而該預留位置最終會由您選擇在執行個體上部署的應用程式所取代。若執行個體未顯示 Bitnami 橫幅，則不必遵循本指南中的程序。



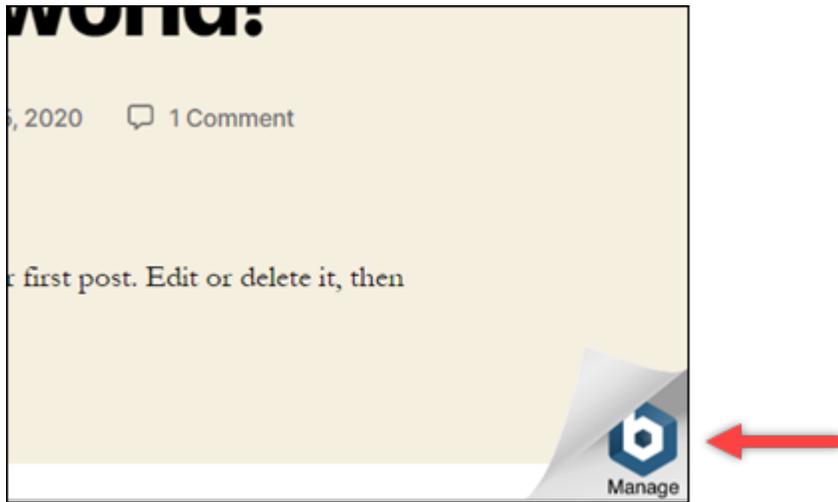
## 從執行個體移除 Bitnami 橫幅

請完成以下程序，以確認執行個體在應用程式首頁上顯示 Bitnami 圖示，並將其移除。

1. 登入主 [Lightsail](#) 台。
2. 在 Lightsail 首頁的 [執行個體] 索引標籤中，複製您要確認之執行個體的公用 IP 位址。



3. 開啓新瀏覽器索引標籤，將執行個體的公有 IP 地址輸入網址列，然後按下 Enter (確認)。
4. 請確認以下其中一個選項：
  1. 若頁面上未顯示 Bitnami 圖示，請停止遵循這些程序。您不需要從應用程式的首頁移除 Bitnami 圖示。
  2. 若 Bitnami 圖示顯示於頁面右下角 (如以下範例中所示)，請繼續執行以下一組步驟將其移除。



在下列步驟中，您將使用 Lightsail 瀏覽器型 SSH 用戶端連線至執行個體。連接之後，您需執行 Bitnami 組態工具 (bnconfig 工具)，以從應用程式首頁移除 Bitnami 圖示。bnconfig 工具是一種命令列工具，可允許您在 Bitnami 藍圖執行個體上設定應用程式。如需詳細資訊，請參閱 Bitnami 文件中的[了解 Bitnami 組態工具](#)。

5. 返回 Lightsail 首頁上的瀏覽器索引標籤。
6. 選擇您要連接之執行個體的名稱旁的瀏覽器型 SSH 用戶端圖示。



7. SSH 用戶端連接至執行個體後，請輸入以下命令之一：
  1. 若您的執行個體使用 Apache，請輸入下列命令其中之一。如果其中一個命令失敗，請嘗試另一個命令。這個命令的第一個部分會停用 Bitnami 橫幅，第二個部分會重新啟動 Apache 服務。

```
sudo /opt/bitnami/apps/wordpress/bnconfig --disable_banner 1 && sudo /opt/bitnami/ctlscript.sh restart apache
```

```
sudo /opt/bitnami/wordpress/bnconfig --disable_banner 1 && sudo /opt/bitnami/ctlscript.sh restart apache
```

您可以透過瀏覽至執行個體的公有 IP 地址，確認 Bitnami 圖示已消失，以確認程序已成功。

按照 step-by-step 說明了解如何檢索 Bitnami 應用程序和數據庫的默認憑據，登錄到應用程序的管理面板，並選擇性地從應用程序的首頁中刪除 Bitnami 商標橫幅。

該指南涵蓋了 Lightsail 中可用的各種比特名藍圖 WordPress，包括 Joomla，Drupal，幽靈，，LAMP，LEMPMEAN，Node.js 等。它提供了應用程序和數據庫的默認用戶名，以及安全地獲取默認密碼的命令。遵循本指南，您可以輕鬆存取和管理 Lightsail 執行個體上執行的 Bitnami 應用程式、根據您的需求進行自訂，並移除任何不需要的品牌元素。

## 設定和管理執行 WordPress 個體

本指南涵蓋下列與 Lightsail 中 WordPress 實體相關的主題：

### 主題

- [在 Lightsail 上啟動和設定 WordPress 執行個體](#)
- [使用 WP 卸載媒體將 Lightsail 上的 WordPress 網站 Connect 到 Amazon S3](#)
- [將 Lightsail WordPress 執行個體 Connect 到 Amazon Aurora 資料庫](#)
- [將 WordPress 資料傳輸 MySQL 受管理的資 Lightsail 庫](#)
- [將 WordPress 執行個體 Connect 至 Lightsail 值區以取得靜態內容](#)
- [WordPress 使用 Lightsail 內容傳遞網路進行設定](#)
- [在 Lightsail 中為 WordPress 實例啟用電子郵件](#)
- [使用 HTTPS 保護您 WordPress 的 Lightsail](#)
- [將您的 WordPress 部落格移 Lightsail](#)

## 在 Lightsail 上啟動和設定 WordPress 執行個體

Amazon Lightsail 是開始使用 Amazon Web Services ( AWS ) 的最簡單方法。Lightsail 包含快速啟動專案所需的一切，包括執行個體 (虛擬專用伺服器)、受管資料庫、SSD 儲存、備份 (快照)、資料傳輸、網域 DNS 管理、靜態 IP 和負載平衡器 — 價格**低廉**且可預測。

透過本教學課程，您將學習如何在 Lightsail 上啟動和設定 WordPress 執行個體。其中包括設定自訂網域名稱的步驟、使用 HTTPS 保護網際網路流量、使用 SSH 連線至執行個體，以及登入您的 WordPress 網站。完成本教學課程後，您將擁有讓執行個體在 Lightsail 上啟動並執行的基礎知識。

**Note**

作為 AWS 免費方案的一部分，您可以在特定執行個體套裝軟體上免費開始使用 Amazon Lightsail。如需詳細資訊，請參閱 [Amazon Lightsail 定價頁面](#) 上的 AWS 免費方案。

**目錄**

- [步驟 1：註冊 AWS](#)
- [步驟 2：建立 WordPress 執行個體](#)
- [步驟 3：設定您的 WordPress 執行個體](#)
- [步驟 4：獲取您 WordPress 網站的管理員密碼](#)
- [步驟 5：登入您 WordPress 網站的管理儀表板](#)
- [其他資訊](#)

**步驟 1：註冊 AWS**

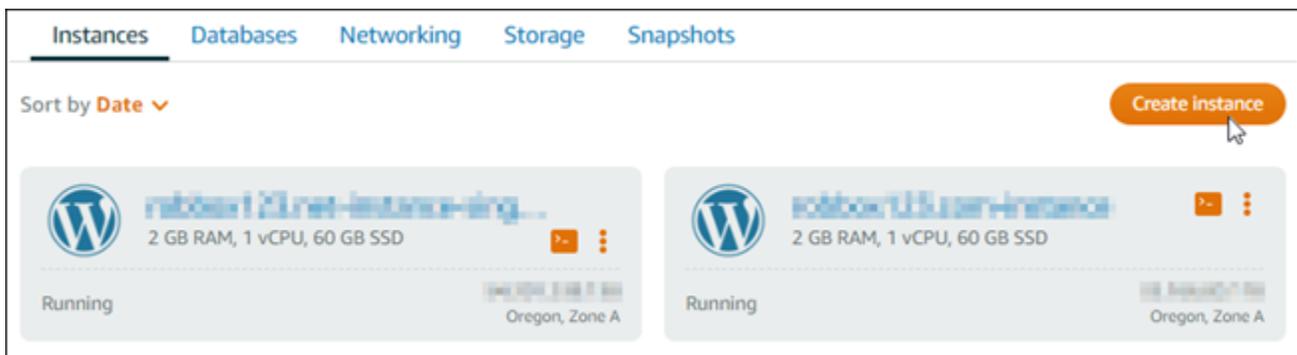
Amazon Lightsail 需要一個 AWS 帳戶。 [註冊 AWS](#)，或者 AWS 如果您已經有帳戶，請 [登入](#)。

**步驟 2：建立 WordPress 執行個體**

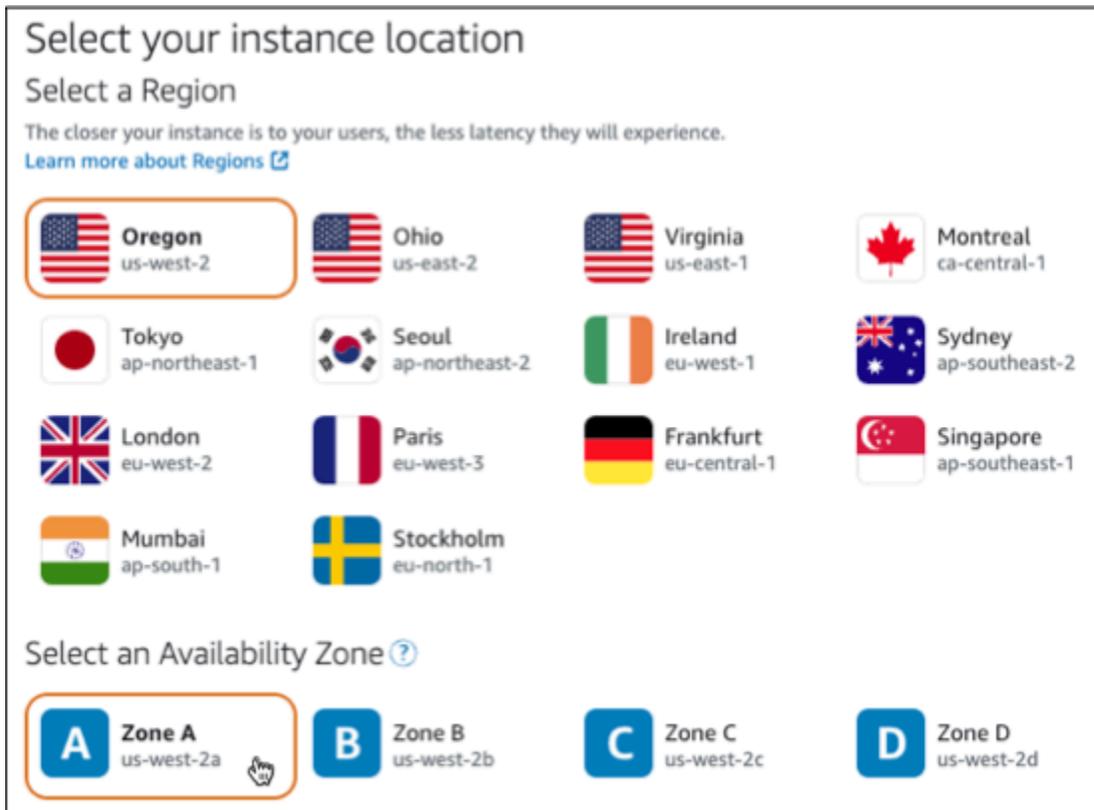
完成下列步驟，讓您的 WordPress 執行個體啟動並執行。如需詳細資訊，請參閱 [the section called “建立執行個體”](#)。

若要建立以下項 Lightsail 的實體 WordPress

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁的「實體」區段中，選擇「建立實體」。



3. 為您的執行個體選擇 AWS 區域 和可用區域。



4. 選擇執行個體的映像檔，如下所示：
  - a. 針對 [選取平台]，選擇 [Linux/Unix]。
  - b. 對於選取藍圖，請選擇WordPress。
5. 選擇執行個體方案。

計劃包括以低廉且可預測的成本的機器配置 ( RAM , SSD , vCPU ) 以及數據傳輸額度。

6. 輸入您執行個體的名稱。資源名稱：
  - 每個 Lightsail 帳戶 AWS 區域 中的每個項目都必須是唯一的。
  - 必須包含 2 至 255 個字元。
  - 開頭和結尾必須是英數字元或數字。
  - 可以包含英數字元、數字、句點、破折號和底線。
7. 選擇 建立執行個體。
8. 若要檢視測試部落格文章，請前往執行個體管理頁面，複製頁面右上角顯示的公用 IPv4 位址。將位址貼到連線至網際網路之網頁瀏覽器的位址欄位中。瀏覽器會顯示測試部落格文章。

### 步驟 3：設定您的 WordPress 執行個體

您可以使用引導式 step-by-step 工作流程來設定 WordPress 執行個體，也可以完成個別工作。使用任一選項，您將設定下列項目：

- 已註冊的網域名稱 — 您的 WordPress 網站需要一個容易記住的網域名稱。使用者將指定此網域名稱來存取您的 WordPress 網站。如需詳細資訊，請參閱 [域和 DNS](#)。
- DNS 管理 — 您必須決定如何管理網域的 DNS 記錄。DNS 記錄會告訴 DNS 伺服器與網域或子網域相關聯的 IP 位址或主機名稱。DNS 區域包含您網域的 DNS 記錄。如需詳細資訊，請參閱 [the section called “DNS 在 Lightsail”](#)。
- 靜態 IP 位址 — 如果您停止並啟動執行個體，WordPress 執行個體的預設公用 IP 位址就會變更。當您將靜態 IP 位址附加到執行個體時，即使您停止並啟動執行個體，它仍會保持不變。如需詳細資訊，請參閱 [the section called “IP 地址”](#)。
- SSL/TLS 憑證 — 建立驗證憑證並將其安裝在執行個體之後，您可以為網站啟用 HTTPS，以便透過註冊 WordPress 網域路由傳送至執行個體的流量會使用 HTTPS 加密。如需詳細資訊，請參閱 [the section called “啟用 HTTPS”](#)。

選項：引導式工作流

#### Tip

開始之前，請先檢閱下列秘訣。如需疑難排解的資訊，請參閱 [疑 WordPress 難排解](#)

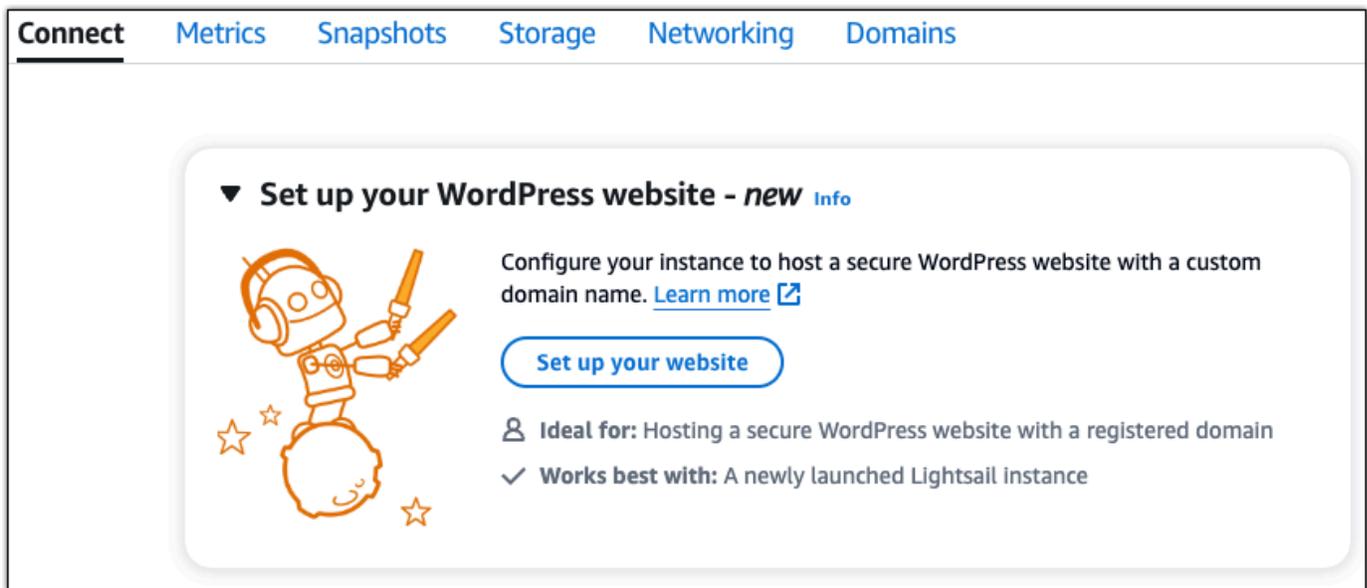
- 安裝程式支援在 2023 年 1 月 1 日之後建立的 WordPress 版本 6 及更新版本的 Lightsail 執行個體。
- 在安裝期間執行的 Certbot 相依性檔案、HTTPS 重新寫入指令碼和憑證更新指令碼會儲存在執行個體的 `/opt/bitnami/lightsail/scripts/` 目錄中。
- 您的執行個體必須處於執行中狀態。如果執行個體剛啟動，請等待幾分鐘的時間讓 SSH 連線準備就緒。
- 執行個體防火牆上的連接埠 22、80 和 443 必須允許在安裝程式執行時從任何 IP 位址進行 TCP 連線。如需詳細資訊，請參閱 [執行個體防火牆](#)。
- 當您新增或更新指向來自頂點網域 (example.com) 及其 www 子網域 (www.example.com) 流量的 DNS 記錄時，這些記錄必須在整個網際網路中傳播。您可以驗證您的 DNS 更改已經通過使用工具生效，或 [DNS 查找](#) 從 MxToolbox
- 在 2023 年 1 月 1 日之前創建的 WordPress 實例可能包含一個不推薦使用的 Certbot 個人 Package 存檔 (PPA) 存儲庫，這將導致網站設置失敗。如果此儲存庫在安裝期間存在，它

將從現有路徑中移除，並備份到執行個體上的下列位置：`~/opt/bitnami/lightsail/repo.backup`有關已過時 PPA 的更多信息，請參閱規範網站上的 [Certbot PPA](#)。

- 讓我們加密證書將每 60 到 90 天自動續訂一次。
- 進行安裝程序時，請勿停止或變更執行個體。設定執行個體最多可能需要 15 分鐘的時間。您可以在執行個體連線索引標籤中檢視每個步驟的進度。

## 使用網站設定精靈設定執行個體

1. 在執行個體管理頁面的 [Connect] 索引標籤上，選擇 [設定您的網站]。



2. 針對「指定網域名稱」，請使用現有的 Lightsail 受管理網域、向 Lightsail 註冊新網域，或使用您透過其他網域註冊機構註冊的網域。選擇 [使用此網域] 以前往下一個步驟。
3. 對於設定 DNS，請執行下列其中一個動作：
  - 選擇受管理的網域以使用 Lightsail DNS 區域。選擇 [使用此 DNS 區域] 以前往下一個步驟。
  - 選擇第三方網域以使用管理您網域 DNS 記錄的主機服務。請注意，如果您稍後決定使用，我們會在您的 Lightsail 帳戶中建立相符的 DNS 區域。選擇「使用第三方 DNS」以進行下一步。
4. 在 [建立靜態 IP 位址] 中，輸入靜態 IP 位址的名稱，然後選擇 [建立靜態 IP]。
5. 針對 [管理網域指派]，選擇 [新增指派]，選擇網域類型，然後選擇 [新增]。選擇「繼續」以前往下一個步驟。

- 在「建立 SSL/TLS 憑證」中，選擇您的網域和子網域、輸入電子郵件地址、選取「我授權 Lightsail 在我的執行個體上設定讓我們加密憑證」，然後選擇「建立憑證」。我們開始設定 Lightsail 資源。

進行安裝程序時，請勿停止或變更執行個體。設定執行個體最多可能需要 15 分鐘的時間。您可以在執行個體連線索引標籤中檢視每個步驟的進度。

- 網站設定完成後，請確認您在網域指派步驟中指定的 URL 是否開啟您的網 WordPress 站。

## 選項：個別任務

### 透過完成個別工作來設定執行個體

- 建立靜態 IP 地址

在執行個體管理頁面的 [網路] 索引標籤上，選擇 [建立靜態 IP]。系統會為您選取靜態 IP 位置和執行個體。指定靜態 IP 位址的名稱，然後選擇 [建立並連接]。

- 建立 DNS 區域

在功能窗格中，選擇 [網域和 DNS]。選擇 [建立 DNS 區域]，輸入您的網域，然後選擇 [建立 DNS 區域]。如果網路流量目前正在路由傳送至您的網域，請先確定 Lightsail DNS 區域中已存在所有現有 DNS 記錄，然後再變更網域目前 DNS 主控供應商的名稱伺服器。如此一來，在傳輸到 Lightsail DNS 區域後，流量會持續不間斷地流動

- 管理網域指派

在 DNS 區域的頁面上的 [指派] 索引標籤上，選擇 [新增指派]。選擇網域或子網域、選取您的執行個體、附加靜態 IP 位址，然後選擇 [指派]。

#### Tip

在您的網域開始將流量路由到 WordPress 執行個體之前，請預留一些時間將這些變更傳播到網際網路。

- 建立並安裝 SSL/TLS 憑證

如需 step-by-step 方向，請參閱[the section called “啟用 HTTPS”](#)。

- 確認您在網域指派步驟中指定的 URL 是否開啟您的 WordPress 網站。

## 步驟 4：獲取您 WordPress 網站的管理員密碼

登入 WordPress 網站管理儀表板的預設密碼會儲存在執行個體上。請完成以下步驟以取得密碼。

取得 WordPress 管理員的預設密碼

1. 開啟執行個體的執行 WordPress 個體管理頁面。
2. 在 WordPress 面板上，選擇「擷取預設密碼」。這會展開頁面底部的存取預設密碼。



3. 選擇 [啟動] CloudShell。這將在頁面底部打開一個面板。
4. 選擇「複製」，然後將內容貼到 CloudShell 視窗中。您可以將光標放在 CloudShell 提示符處並按 Ctrl+V，也可以右鍵單擊以打開菜單，然後選擇粘貼。
5. 記下 CloudShell 視窗中顯示的密碼。您需要此功能才能登入 WordPress 網站的管理儀表板。

```
[cloudshell-user@ip-10-11-11-11 ~]$ AWS_REGION=us-east-1 ~/lightsail_connect WordPress-1 cat bitnami_application_password
JKzh8wB5FAR!
```

## 步驟 5：登入您 WordPress 網站的管理儀表板

現在，您已經擁有 WordPress 網站管理儀表板的密碼，您可以登錄。在管理儀表板中，您可以變更您的使用者密碼、安裝外掛程式、變更網站的主題等。

完成下列步驟以登入您 WordPress 網站的管理儀表板。

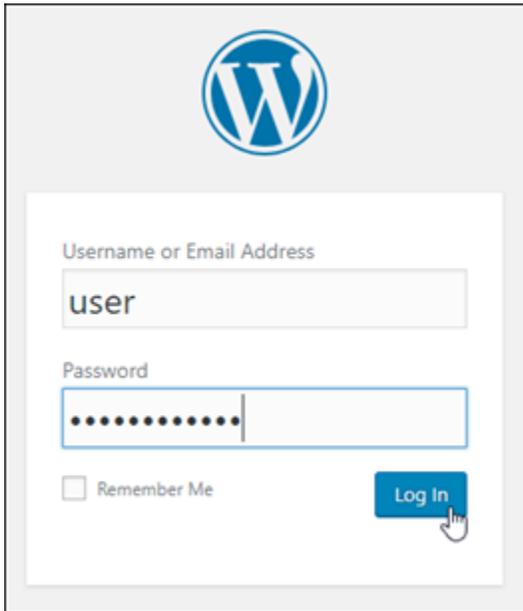
若要登入管理儀表板

1. 開啟執行個體的執行 WordPress 個體管理頁面。
2. 在 WordPress 面板上，選擇 [存取 WordPress 管理員]。

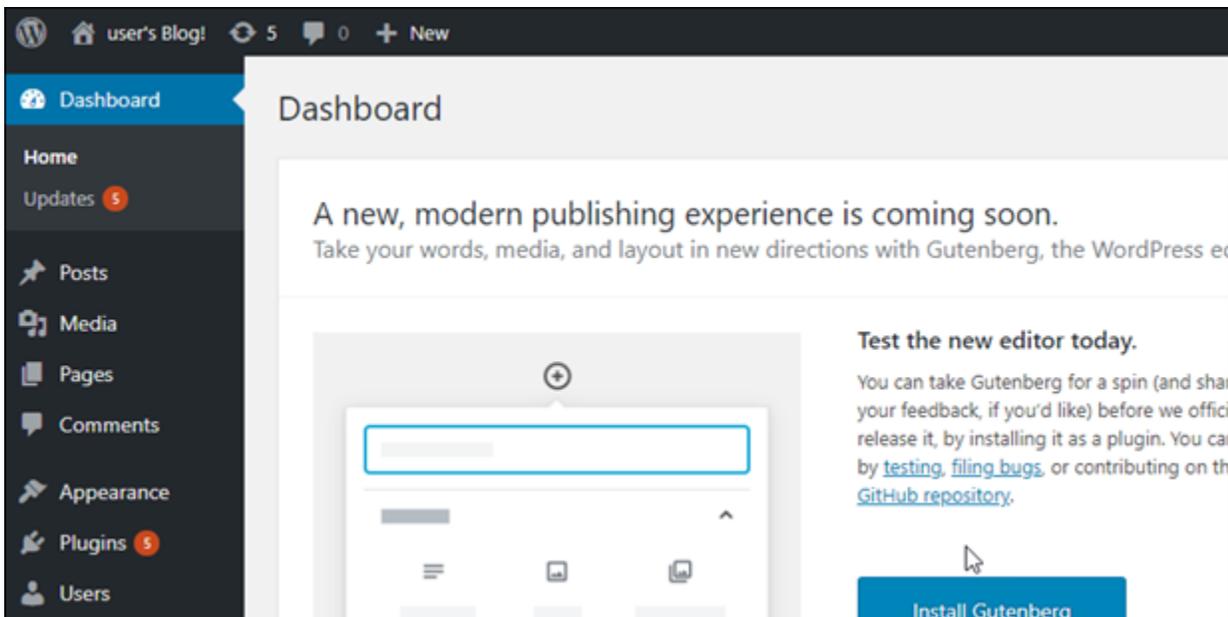
3. 在 [存取您的 WordPress 管理儀表板] 面板的 [使用公用 IP 位址] 下方，選擇具有此格式的連結：

HTTP : **://## IPV4** 地址。 /WP-管理員

4. 針對使用者名稱或電子郵件地址，輸入 **user**
5. 在「密碼」中，輸入在上一個步驟中取得的密碼。
6. 選擇 Log in (登入)。



您現在已登入 WordPress 網站的管理儀表板，您可以在其中執行管理動作。有關管理 WordPress 網站的更多信息，請參閱文檔中的 [WordPress Codex](#)。



## 其他資訊

以下是您在 Amazon Lightsail 中啟動執行個 WordPress 體之後可以執行的一些其他步驟：

- [the section called “配置一個 CDN”](#)
- [建立 Linux 或 Unix 執行個體快照](#)
- [啟用或停用執行個體或磁碟的自動快照](#)
- [建立額外的區塊儲存磁碟並將其附接至以 Linux 為基礎的執行個體](#)

## 使用 WP 卸載媒體將 Lightsail 上的 WordPress 網站 Connect 到 Amazon S3

本教學說明將您在 Amazon Lightsail 執行個體上執行的 WordPress 網站連接到 Amazon Simple Storage Service (Amazon S3) 貯體以存放網站影像和附件所需的步驟。為此，您可以使用一組 Amazon Web Services (AWS) 帳戶登入資料來設定 WordPress 外掛程式。外掛程式接著會為您建立 Amazon S3 儲存貯體，並將您的網站設定為使用儲存貯體，而不是執行個體的磁碟來存放網站影像和附件。

### 內容

- [步驟 1：完成先決條件](#)
- [步驟 2：在您 WordPress 的網站上安裝 WP 卸載媒體插件](#)
- [步驟 3：建立 IAM 使用者和策略](#)
- [步驟 4：編輯 WordPress 配置文件](#)
- [步驟 5：使用 WP Offload Media 外掛程式建立 Amazon S3 儲存貯體](#)
- [步驟 6：後續步驟](#)

### 步驟 1：完成先決條件

開始之前，請先在 Lightsail 中建立 WordPress 執行個體，並確定它處於執行中狀態。如需詳細資訊，請參閱[教學課程：啟動和設定 WordPress 執行個體](#)。

### 步驟 2：在您 WordPress 的網站上安裝 WP 卸載媒體插件

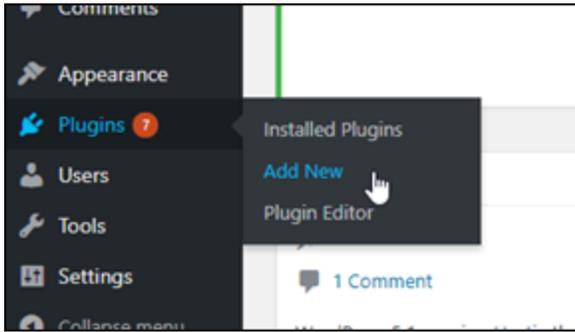
您必須使用外掛程式，將網站設定為使用 Amazon S3 儲存貯體。有許多外掛程式可用於設定此動作；[WP Offload Media Lite](#) 就是這類外掛程式之一。

完成以下步驟，在您的 WordPress 網站上安裝 WP 卸載媒體插件：

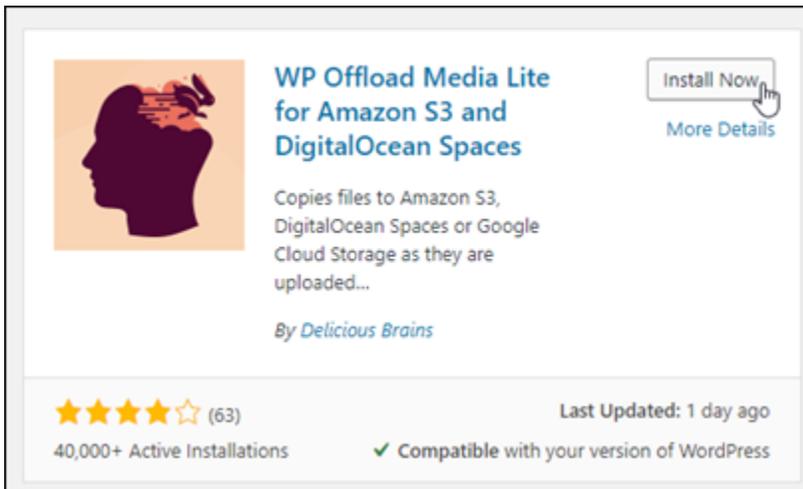
1. 以系統管理員身分登入 WordPress 儀表板。

如需詳細資訊，請參閱在 [Amazon Lightsail 中取得 Bitnami 執行個體的應用程式使用者名稱和密碼](#)。

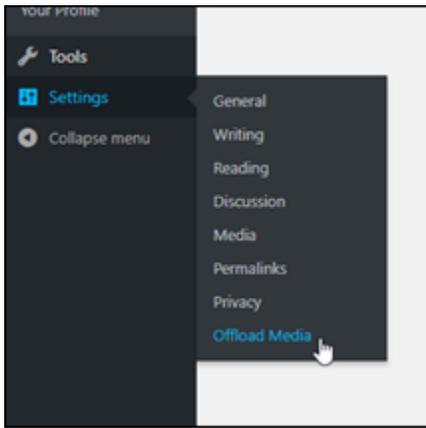
2. 將滑鼠游標移至左側導覽功能表中的 Plugins (外掛程式) 上，然後選擇 Add New (新增)。



3. 搜尋 WP Offload Media Lite。
4. 在搜尋結果中，選擇 WP Offload Media 外掛程式旁的 Install Now (立即安裝)。



5. 在外掛程式完成安裝後，選擇 Activate (啟用)。
6. 在左側導覽功能表中，選擇 Settings (設定)，然後選擇 Offload Media (卸載媒體)。



7. 在 Offload Media 頁面中，選擇 Amazon S3 作為儲存供應商，然後選擇定義 wp-config.php 中的存取金鑰。

使用此選項時，您必須將 AWS 帳戶認證新增至執行個體 wp-config.php 上的。本教學課程稍後將說明這些步驟。



將 Offload Media (卸載媒體) 頁面保持開啟，稍後您將在本教學課程中回到此頁面。請繼續閱讀本教學課程的 [〈步驟 3：建立 IAM 使用者和策略〉](#) 一節。

### 步驟 3：建立 IAM 使用者和策略

#### **⚠ Warning**

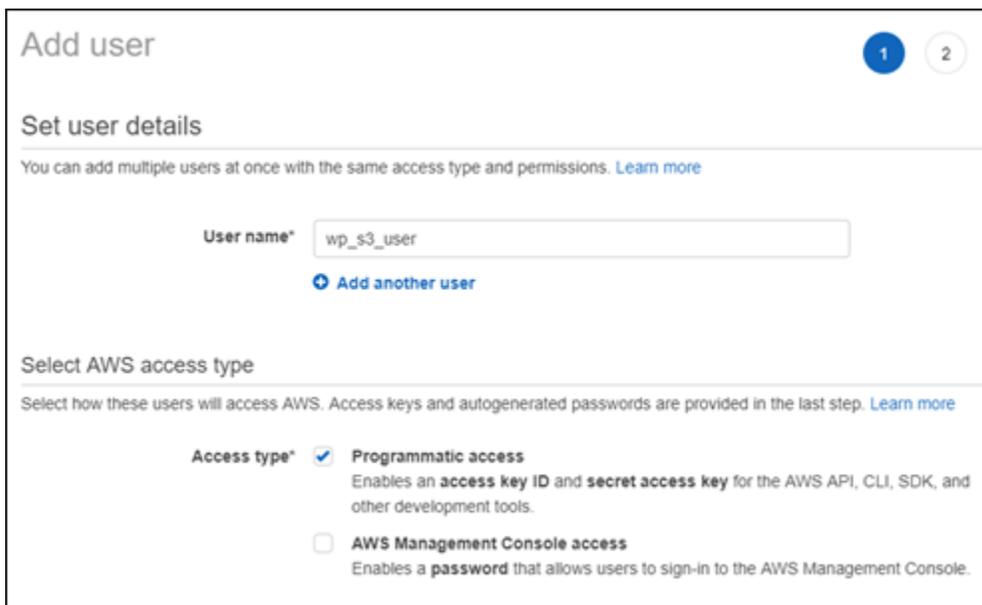
此案例需要具有程式設計存取和長期認證的 IAM 使用者，這會帶來安全性風險。為了減輕此風險，我們建議您僅向這些使用者提供執行工作所需的權限，並在不再需要這些使用者時移除這

些使用者。如有必要，可更新存取金鑰。如需詳細資訊，請參閱《IAM使用指南》中的〈[更新存取金鑰](#)〉。

WP 卸載媒體插件需要訪問您的 AWS 帳戶以創建 Amazon S3 存儲桶，並上傳您的網站圖像和附件。

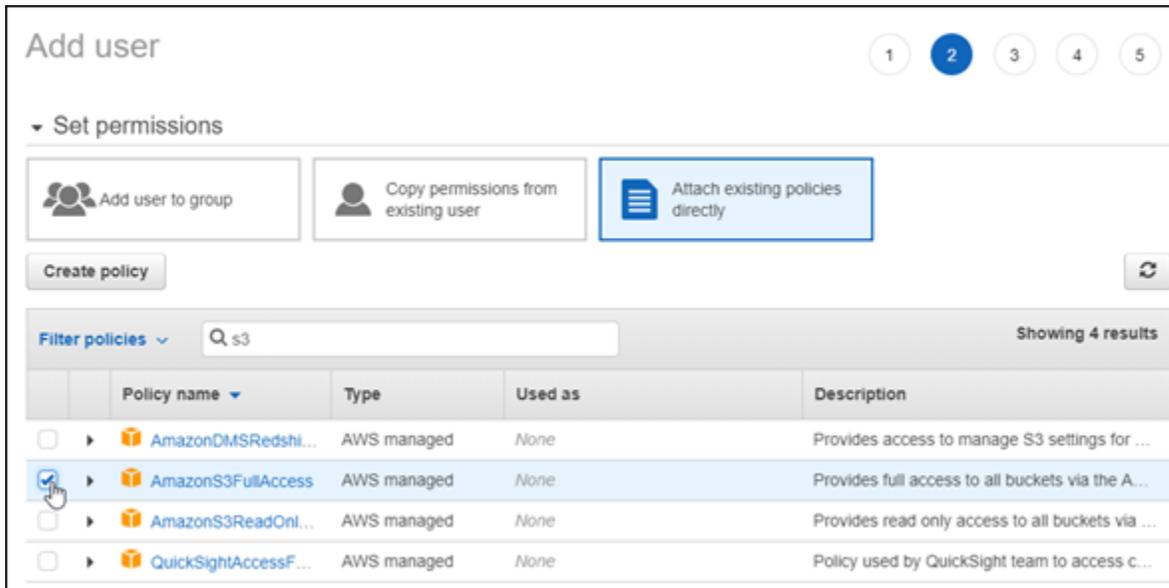
完成下列步驟，為 WP 卸載媒體外掛程式建立新的 AWS Identity and Access Management (IAM) 使用者和原則：

1. 開啟新的瀏覽器索引標籤，然後登入[IAM主控台](#)。
2. 在左側導覽功能表中，選擇 Roles (角色)。
3. 選擇 Add user (新增使用者)。
4. 在 User name (使用者名稱) 文字方塊中，輸入新使用者的名稱。輸入描述性內容，例如 wp\_s3\_user 或 wp\_offload\_media\_plugin\_user，以便您日後在執行維護時可以輕鬆識別它。
5. 在 Access type (存取類型) 部分，選擇 Programmatic access (程式設計存取)。



The screenshot shows the 'Add user' interface in the AWS IAM console. It is divided into two main sections: 'Set user details' and 'Select AWS access type'. In the 'Set user details' section, the 'User name\*' field contains 'wp\_s3\_user' and there is a blue '+ Add another user' button below it. The 'Select AWS access type' section has a heading and a sub-heading: 'Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. Learn more'. Underneath, there are two radio button options: 'Programmatic access' (which is selected with a blue checkmark) and 'AWS Management Console access'. The 'Programmatic access' option has a description: 'Enables an access key ID and secret access key for the AWS API, CLI, SDK, and other development tools.' The 'AWS Management Console access' option has a description: 'Enables a password that allows users to sign-in to the AWS Management Console.'

6. 選擇下一步：許可。
7. 選擇直接附加現有政策，搜尋 S3，然後在搜尋結果FullAccess中選擇 AmazonS3。



- 選擇 Next: Tags (下一步：標籤)，然後選擇 Next: Review (下一步：檢閱)。
- 檢閱頁面上顯示的使用者詳細資訊，然後選擇 Create user (建立使用者)。
- 記下使用者的 access key ID (存取金鑰 ID) 和 secret access key (私密存取金鑰)，或選擇 Download .csv (下載 .csv)，將這些值的複本儲存到本機磁碟機。在執行個體上編輯 wp-config.php 檔案時，在接下來的幾 WordPress 個步驟中，您將需要這些步驟。

#### 步驟 4：編輯 WordPress 配置文件

完成下列步驟，即可使用 Lightsail 主控台中的瀏覽器型用 SSH 戶端連線至 WordPress 執行個體，並編輯檔案。wp-config.php

wp-config.php 檔案包含您網站的基本組態詳細資訊，例如資料庫連線資訊。

#### Note

您也可以使用自己的用 SSH 戶端連線至執行個體。如需詳細資訊，請參閱 [下載並設定 PuTTY 以使用 Amazon Lightsail SSH 進行連線](#)。

- 登入主 [Lightsail 台](#)。
- 選擇 WordPress 執行個體的瀏覽器型 SSH 用戶端圖示。



3. 在出現的SSH客戶端窗口中，輸入以下命令以創建wp-config.php文件的備份，以防出現問題：

```
sudo cp /opt/bitnami/wordpress/wp-config.php /opt/bitnami/wordpress/wp-config.php.backup
```

4. 輸入下列命令，使用 wp-config.php (文字編輯器) 來開啟 nano 檔案：

```
nano /opt/bitnami/wordpress/wp-config.php
```

5. 在 /\* That's all, stop editing! Happy blogging. \*/ 文字上方輸入下列文字。

一定要更換 *AccessKeyID* 與訪問密鑰 ID 和 *SecretAccessKey* 使用您先前在這些步驟中創建的IAM用戶的秘密訪問密鑰。

```
define( 'AS3CF_SETTINGS', serialize( array(
    'provider' => 'aws',
    'access-key-id' => 'AccessKeyID',
    'secret-access-key' => 'SecretAccessKey',
) ) );
```

範例：

```
define( 'AS3CF_SETTINGS', serialize( array(
    'provider' => 'aws',
    'access-key-id' => 'AKIAIOSFODNN7EXAMPLE',
    'secret-access-key' => 'wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY',
) ) );
```

結果應如下範例所示：

```
/* Link: https://codex.wordpress.org/Debugging_in_WordPress */
define('WP_DEBUG', false);

define('AS3CF_SETTINGS', serialize( array(
    'provider' => 'aws',
    'access-key-id' => 'AKIAI44QH8D8DFK1L5M65',
    'secret-access-key' => 'a3cfd343f243b208b9ee7299b2832abd'
) ));

/* That's all, stop editing! Happy blogging. */

define('FS_METHOD', 'direct');
```

6. 按下 **Ctrl+X** 結束 Nano，然後按下 **Y** 和 **Enter**，以將您的編輯內容儲存至 wp-config.php 檔案。
7. 輸入下列命令，重新啟動執行個體上的服務：

```
sudo /opt/bitnami/ctlscript.sh restart
```

服務重新啟動後，您會看到如下的結果：

```
bitnami@ip-172-26-13-236:~$ sudo /opt/bitnami/ctlscript.sh restart
Syntax OK
/opt/bitnami/apache2/scripts/ctl.sh : httpd stopped
/opt/bitnami/php/scripts/ctl.sh : php-fpm stopped
/opt/bitnami/mysql/scripts/ctl.sh : mysql stopped
/opt/bitnami/mysql/scripts/ctl.sh : mysql started at port 3306
/opt/bitnami/php/scripts/ctl.sh : php-fpm started
Syntax OK
/opt/bitnami/apache2/scripts/ctl.sh : httpd started at port 80
bitnami@ip-172-26-13-236:~$
```

關閉SSH視窗並切換回您稍早在本教學課程中保持開啟狀態的「卸載媒體」頁面。您現在已準備好[使用 WP Offload Media 外掛程式建立 Amazon S3 儲存貯體](#)。

## 步驟 5：使用 WP Offload Media 外掛程式建立 Amazon S3 儲存貯體

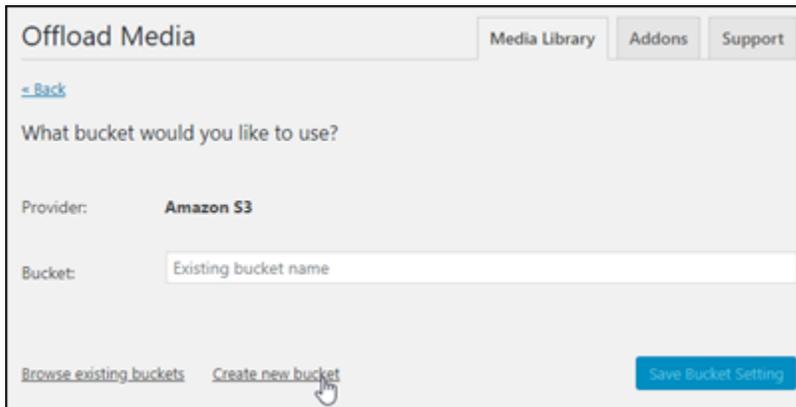
現在已使用AWS認證設定wp-config.php檔案，您可以返回「卸載媒體」頁面以完成程序。

完成下列步驟，使用 WP Offload Media 外掛程式來建立 Amazon S3 儲存貯體。

1. 重新整理 Offload Media (卸載媒體) 頁面，或選擇 Next (下一步)。

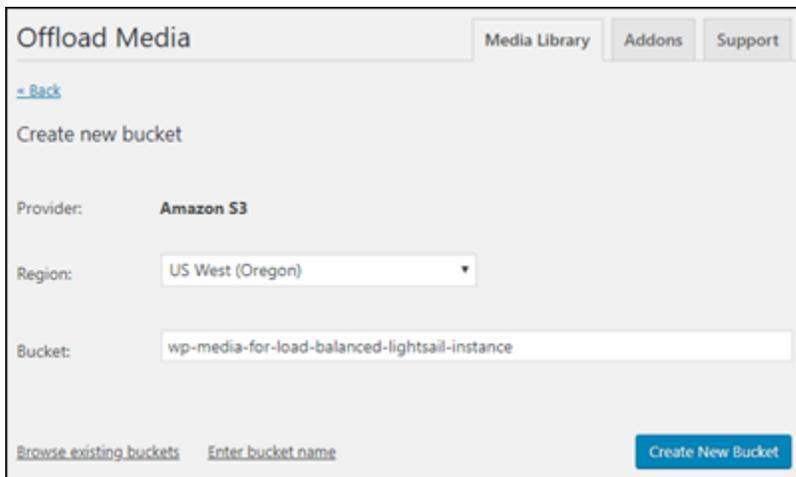
現在應該會看到 Amazon S3 供應商已完成設定。

2. 選擇 Create new bucket (建立新的儲存貯體)。



The screenshot shows the 'Offload Media' configuration interface. At the top, there are navigation tabs for 'Media Library', 'Addons', and 'Support'. Below the title, there is a '- Back' link. The main heading is 'What bucket would you like to use?'. The 'Provider' is set to 'Amazon S3'. The 'Bucket' field contains the text 'Existing bucket name'. At the bottom left, there are links for 'Browse existing buckets' and 'Create new bucket'. A blue button labeled 'Save Bucket Setting' is located at the bottom right.

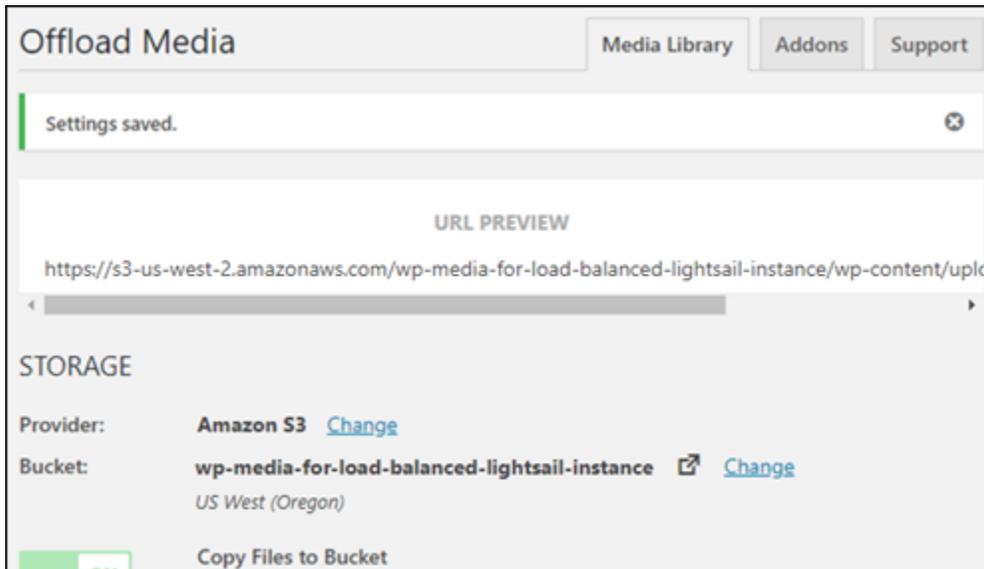
3. 在「地區」下拉式選單中，選擇所需的「AWS區域」。建議您選擇 WordPress 執行個體所在的相同區域。
4. 在 Bucket (儲存貯體) 文字方塊中，輸入新 S3 儲存貯體的名稱。



The screenshot shows the 'Offload Media' configuration interface for creating a new bucket. At the top, there are navigation tabs for 'Media Library', 'Addons', and 'Support'. Below the title, there is a '- Back' link. The main heading is 'Create new bucket'. The 'Provider' is set to 'Amazon S3'. The 'Region' dropdown menu is set to 'US West (Oregon)'. The 'Bucket' field contains the text 'wp-media-for-load-balanced-lightsail-instance'. At the bottom left, there are links for 'Browse existing buckets' and 'Enter bucket name'. A blue button labeled 'Create New Bucket' is located at the bottom right.

5. 選擇 Create New Bucket (建立新的儲存貯體)。

頁面會重新整理，確認已建立新的儲存貯體。查看出現的設置，並根據您希望 WordPress 網站的行為進行相應調整。



從現在開始，新增至部落格文章的影像和附件會自動上傳到您所建立的 Amazon S3 儲存貯體。

## 步驟 6：後續步驟

將 WordPress 網站連接到 Amazon S3 儲存貯體後，您應該建立 WordPress 執行個體快照以備份您所做的變更。如需詳細資訊，請參閱[建立 Linux 或 Unix 執行個體的快照](#)。

## 將 Lightsail WordPress 執行個體 Connect 到 Amazon Aurora 資料庫

貼文、頁面和使用者的網站資料會儲存在 Amazon Lightsail 執行個體上 WordPress 執行的資料庫中。如果執行個體發生故障，這些資料可能會無法復原。為避免這種情況，應該將網站資料轉移至 Amazon Relational Database Service (Amazon RDS) 中的 Amazon Aurora 資料庫。

Amazon Aurora 是針對雲端建置的 MySQL 和 PostgreSQL 相容關聯式資料庫。它將傳統企業資料庫的效能和可用性與開源資料庫的簡易性和有效性相結合。Aurora 作為 Amazon RDS 的一部分提供。Amazon RDS 是一項受管資料庫服務，可以讓雲端中關聯式資料庫的設定、操作和擴展更加簡單。如需詳細資訊，請參閱《[Amazon 關聯式資料庫服務使用者指南](#)》和《[Amazon Aurora 使用者指南](#)》。

在本教學中，我們將示範如何將網站資料庫從 Lightsail 中的 WordPress 執行個體連接到 Amazon RDS 中的 Aurora 受管資料庫。

### 內容

- [步驟 1：完成先決條件](#)

- [步驟 2：設定 Aurora 資料庫的安全群組](#)
- [步驟 3：從您的 Lightsail 執行個體 Connect 至您的 Aurora 資料庫](#)
- [步驟 4：將 MySQL 資料庫從 WordPress 執行個體傳輸到 Aurora 資料庫](#)
- [步驟 5：設定連線 WordPress 至 Aurora 管理的資料庫](#)

## 步驟 1：完成先決條件

開始之前，請先完成以下先決條件：

1. 在 Lightsail 中建立 WordPress 執行個體，並在其上設定您的應用程式。在繼續之前，執行個體應處於執行中狀態。如需詳細資訊，請參閱[教學課程：在 Amazon Lightsail 中啟動和設定 WordPress 執行個體](#)。
2. 在您的 Lightsail 帳戶中開啟 VPC 人雲端對等功能。如需詳細資訊，請參閱[設定對等互連以使用 Lightsail 以外的 AWS 資源](#)。
3. 在 Amazon RDS 中建立 Aurora 受管資料庫。資料庫必須位於與 WordPress 執行個體 AWS 區域相同的位置。在繼續之前，其亦應處於執行中狀態。如需詳細資訊，請參閱《Amazon Aurora 使用者指南》中的[Amazon Aurora 入門](#)。

## 步驟 2：設定 Aurora 資料庫的安全群組

安 AWS 全群組充當 AWS 資源的虛擬防火牆。它控制可以連接到 Amazon RDS 中 Aurora 資料庫的傳入和傳出流量。如需詳細資訊，請參閱《Amazon Virtual Private Cloud 使用者指南》中的[使用安全群組控制資源流量](#)。

請完成下列程序來設定安全群組，讓您的 WordPress 執行個體可以建立與 Aurora 資料庫的連線。

1. 登入 [Amazon RDS 主控台](#)。
2. 在導覽窗格中，選擇 Databases (資料庫)。
3. 選擇執行個體將連線到的 Aurora 資料庫的 Writer WordPress 執行個體。
4. 選擇 Connectivity & security (連線和安全) 索引標籤。
5. 在 Endpoint & port (端點與連接埠) 區段中，記下 Writer instance (寫入器執行個體) 的 Endpoint name (端點名稱) 和 Port (連接埠)。稍後將 Lightsail 執行個體設定為連線至資料庫時，您將需要這些項目。
6. 在 Security (安全) 區段中，選擇作用中的 VPC 安全群組連結。您會被重定引導至您資料庫的安全群組。

The screenshot shows the Amazon RDS console for an Aurora database instance named 'aurora-database-1-instance-1'. The instance is a 'Writer instance' in the 'us-west-2a' region, running on the 'db.r5.large' instance class. The 'Connectivity & security' section is expanded, showing the endpoint 'aurora-database-1-instance-1.us-west-2.rds.amazonaws.com' and port '3306'. The 'VPC security groups' section shows the instance is associated with the 'default (sg-...)' security group, which is active.

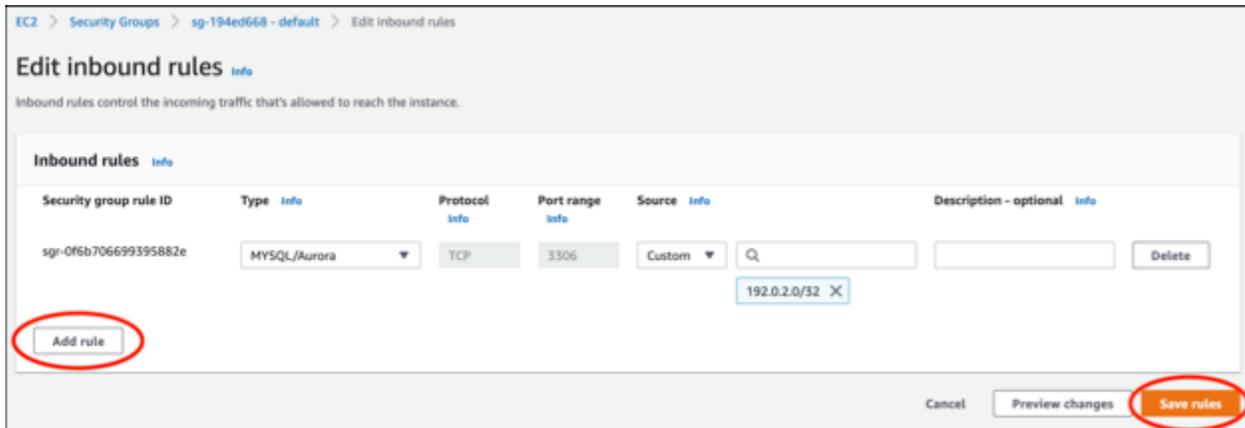
7. 確認已選取 Aurora 資料庫的安全群組。
8. 選擇 Inbound Rules (傳入規則) 索引標籤。
9. 選擇 Edit inbound Rules (編輯傳入規則)。

The screenshot shows the Amazon Security Groups console for a security group named 'sg-... - default'. The 'Inbound rules' tab is selected, showing a list of three inbound rules. The 'Edit inbound rules' button is circled in red.

Name	Security group rule...	IP version	Type	Protocol	Port range
-	sgr-...	IPv4	SSH	TCP	22
-	sgr-...	IPv4	MYSQL/Aurora	TCP	3306
-	sgr-...	IPv6	SSH	TCP	22

10. 在 Edit inbound rules (編輯傳入規則) 頁面中，選擇 Add rule (新增規則)。
11. 完成下列其中一個步驟：

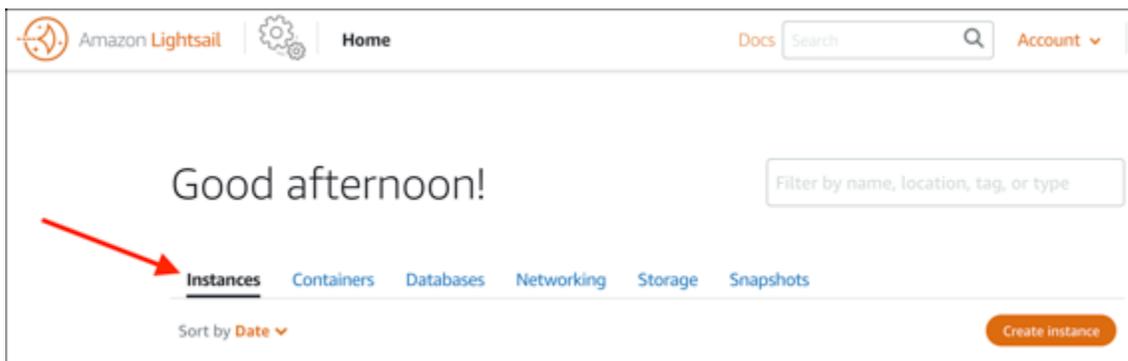
- 如果您是使用預設的 MySQL 連接埠 3306，則在 Type (類型) 下拉式選單中選擇 MySQL/Aurora。
  - 如果資料庫是使用自訂連接埠，則在 Type (類型) 下拉選單中選擇 Custom TCP (自訂 TCP)，並在 Port Range (連接埠範圍) 文字方塊中輸入連接埠編號。
12. 在 [來源] 文字方塊中，新增 WordPress 執行個體的私有 IP 位址。您必須以 CIDR 表示法輸入 IP 地址，這意味著您必須附加 /32。例如，若要允許 192.0.2.0，請輸入 192.0.2.0/32。
  13. 選擇儲存規則。



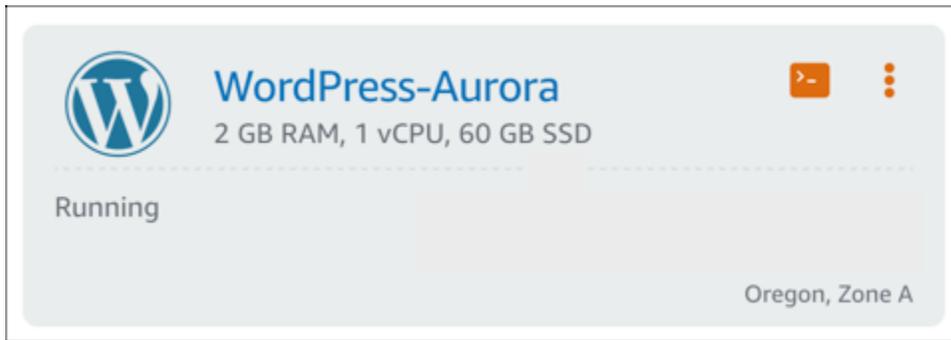
### 步驟 3：從您的 Lightsail 執行個體 Connect 至您的 Aurora 資料庫

請完成下列程序，以確認您可以從 Lightsail 執行個體連線至 Aurora 資料庫。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁上，選擇「實體」索引標籤。



3. 選擇以瀏覽器為基礎的 SSH 用戶端圖示，讓您的 WordPress 執行個體使用 SSH 連線。



4. 在連接至執行個體後，輸入以下命令以連接至 Aurora 資料庫。##### Aurora #####  
##### Port#DatabaseEndpointMyUserName 以建立資料庫時輸入的使用者名稱取代。

```
mysql -h DatabaseEndpoint -P Port -u MyUserName -p
```

您應該會看到類似以下範例的回應，其會確認您的執行個體可以存取並連接至 Aurora 資料庫。

```
bitnami@ip-...:~$ mysql -h database.cluster-... .us-west-2.rds.amazonaws.com -P 3306 -u admin -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 215
Server version: 5.6.10 MySQL Community Server (GPL)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> █
```

如果您沒有看到此回應，或收到錯誤訊息，則可能需要設定 Aurora 資料庫的安全性群組，以允許 Lightsail 執行個體的私有 IP 位址連線至該資料庫。如需詳細資訊，請參閱本指南的[設定 Aurora 資料庫的安全性群組](#)章節。

## 步驟 4：將資料庫從 WordPress 執行個體傳輸到 Aurora 資料庫

既然您已確認可以從執行個體連線到資料庫，您應該將 WordPress 網站資料傳輸到 Aurora 資料庫。

1. 登入主 [Lightsail](#) 台。
2. 在 [執行個體] 索引標籤中，選擇執行個體的瀏覽器型 SSH 用戶 WordPress 端。



- 在以瀏覽器為基礎的 SSH 用戶端連線到 WordPress 執行個體之後，輸入下列命令。該命令會轉移來自執行個體上 `bitnami_wordpress` 資料庫的資料，並將其移動到 Aurora 資料庫。在命令中，以 `DatabaseUserName` 您在建立 Aurora 資料庫時輸入的主要使用者名稱取代。 `DatabaseEndpoint` 以 Aurora 資料庫的端點位址取代。

```
sudo mysqldump -u root --databases bitnami_wordpress --single-transaction --
compress --order-by-primary -p$(cat /home/bitnami/bitnami_application_password) |
sudo mysql -u DatabaseUserName --host DatabaseEndpoint --password
```

#### 範例

```
sudo mysqldump -u root --databases bitnami_wordpress --single-transaction --
compress --order-by-primary -p$(cat /home/bitnami/bitnami_application_password)
| sudo mysql -u DBuser --host abc123exampleE67890.czowadgeezi.us-
west-2.rds.amazonaws.com --password
```

- 出現 `Enter password` 提示時，輸入 Aurora 資料庫的密碼，然後按下 Enter 鍵。

鍵入密碼時，您無法看到密碼。

```
bitnami@ip-172-26-7-200:~$ mysqldump -u root --databases bitnami_wordpress --single-transaction --co
mpress --order-by-primary -p$(cat /home/bitnami/bitnami_application_password) | mysql -u dbmasterus
er --host ls-a3420cc0b7a6b772af722d614e64e5c8298cf01c.czowadgeezi.us-west-2.rds.amazonaws.com --pas
sword
Enter password: mysqldump: [Warning] Using a password on the command line interface can be insecure.
█
```

如果資料轉移成功，即會顯示類似以下範例的回應。

```
Enter password: mysqldump: [Warning] Using a password on the command line interface can be insecure.
bitnami@ip-172-26-7-200:~$ █
```

如果出現錯誤，請確認您所使用的資料庫使用者名稱、密碼和端點正確無誤，然後再試一次。

## 步驟 5：設定連線 WordPress 至 Aurora 資料庫

將應用程式資料傳輸到 Aurora 資料庫後，您應該設定 WordPress 為連線至該資料庫。請完成下列程序來編輯 WordPress 組態檔 (wp-config.php)，讓您的網站連線至 Aurora 資料庫。

1. 在連線至 WordPress 執行個體的瀏覽器型 SSH 用戶端中，輸入下列指令以建立 wp-config.php 檔案備份：

```
cp /opt/bitnami/wordpress/wp-config.php /opt/bitnami/wordpress/wp-config.php-backup
```

2. 輸入以下命令讓 wp-config.php 檔案為可寫入：

```
sudo chmod 664 /opt/bitnami/wordpress/wp-config.php
```

3. 編輯 config 檔案中的資料庫使用者名稱，換成建立 Aurora 資料庫時輸入的主要使用者名稱。

```
sudo wp config set DB_USER DatabaseUserName
```

4. 編輯 config 檔案中的資料庫主機，換成 Aurora 資料庫的端點地址和連接埠編號。例如 abc123exampleE67890.czowadgeezqi.us-west-2.rds.amazonaws.com:3306。

```
sudo wp config set DB_HOST DatabaseEndpoint:Port
```

5. 編輯 config 檔案中的資料庫密碼，換成 Aurora 資料庫的密碼。

```
sudo wp config set DB_PASSWORD DatabasePassword
```

6. 輸入 wp config list 命令驗證您在 wp-config.php 檔案中輸入的資訊為正確。

```
sudo wp config list
```

會出現類似以下範例的結果，顯示出您組態的詳細資訊：

```
bitnami@ip-1 :~$ sudo wp config list
+-----+-----+-----+
| name   | value                                     | type   |
+-----+-----+-----+
| table_prefix | wp_                                       | variable |
| DB_NAME   | bitnami_wordpress                         | constant |
| DB_USER   | admin                                      | constant |
| DB_PASSWORD | Password1                                 | constant |
| DB_HOST   | database.cluster-                        .us-west-2.rds.amazonaws | constant |
|           | .com:3306                                 |           |
```

7. 輸入以下命令，重新啟動執行個體上的 Web 服務。

```
sudo /opt/bitnami/ctlscript.sh restart
```

服務重新啟動時，會顯示類似以下範例的結果：

```
bitnami@ip-172-26-13-236:~$ sudo /opt/bitnami/ctlscript.sh restart
Syntax OK
/opt/bitnami/apache2/scripts/ctl.sh : httpd stopped
/opt/bitnami/php/scripts/ctl.sh : php-fpm stopped
/opt/bitnami/mysql/scripts/ctl.sh : mysql stopped
/opt/bitnami/mysql/scripts/ctl.sh : mysql started at port 3306
/opt/bitnami/php/scripts/ctl.sh : php-fpm started
Syntax OK
/opt/bitnami/apache2/scripts/ctl.sh : httpd started at port 80
bitnami@ip-172-26-13-236:~$
```

恭喜您！您的 WordPress 網站現在已設定為使用 Aurora 資料庫。

#### Note

如果您需要還原原始 wp-config.php 檔案，則可輸入以下命令，使用先前在本教學課程中建立的備份來進行還原。

```
cp /opt/bitnami/wordpress/wp-config.php-backup /opt/bitnami/wordpress/wp-config.php
```

## 將 WordPress 資料傳輸 MySQL 受管理的資 Lightsail 庫

文章、頁面和使用者的重要 WordPress 網站資料會儲存在 Amazon Lightsail 執行個體上執行的 MySQL 資料庫中。如果執行個體發生故障，這些資料可能會無法復原。為避免這種情況，您應該將網站資料轉移至 MySQL 受管資料庫。

在本教程中，我們將向您展示如何將 WordPress 網站數據傳輸到 Lightsail 中的 MySQL 管理數據庫。我們也會示範如何編輯執行個體上的 configure (wp-config.php) 檔案，讓您的網站連線到受管理的資料庫，並停止連線至執行個體上執行的資料庫。WordPress

### 內容

- [步驟 1：完成先決條件](#)
- [第 2 步：將 WordPress 數據庫傳輸到您的 MySQL 託管數據庫](#)
- [第 3 步：配置連接 WordPress 到您的 MySQL 託管數據庫](#)
- [步驟 4：完成後續步驟](#)

## 步驟 1：完成先決條件

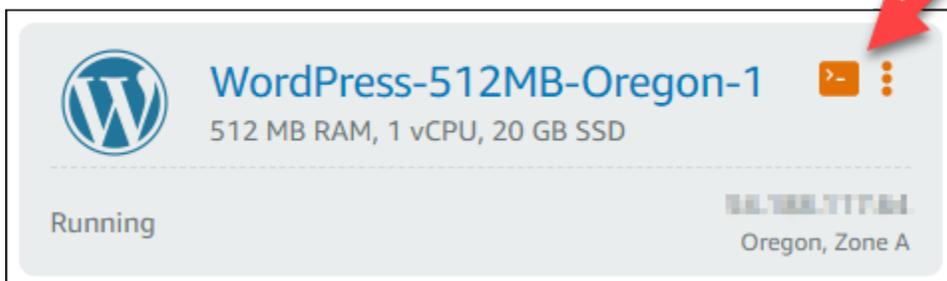
開始之前，請先完成以下先決條件：

- 在 Light WordPress sail 中建立實體，並確定它處於執行中狀態。如需詳細資訊，請參閱[教學課程：在 Amazon Lightsail 中啟動和設定 WordPress 執行個體](#)。
- 在 Lightsail 中與執行個體相同的 AWS 區域中建立 MySQL 受管資料庫，並確認資料庫處於 WordPress 執行中狀態。WordPress 適用於所有可用的 MySQL 資料庫 Lightsail。如需詳細資訊，請參閱[在 Amazon Lightsail 中建立資料庫](#)。
- 啟用 MySQL 受管資料庫的公有模式和資料匯入模式。您可以在完成本教學課程中的步驟後停用這些模式。如需詳細資訊，請參閱[設定資料庫的公有模式](#)以及[設定資料庫的資料匯入模式](#)。

## 第 2 步：將 WordPress 資料庫傳輸到您的 MySQL 託管資料庫

請完成下列程序，將您的 WordPress 網站資料傳輸至 Lightsail 中的 MySQL 受管理資料庫。

1. 登入主 [Lightsail 台](#)。
2. 在 [執行個體] 索引標籤中，選擇執行個體的 WordPress 瀏覽器型 SSH 用戶端圖示。



3. 在以瀏覽器為基礎的 SSH 用戶端連線到 WordPress 執行個體之後，輸入下列指令，將執行個體上資料bitnami\_wordpress庫中的資料傳輸到 MySQL 受管資料庫。請務必以受管理資料庫的使用者名稱取代 *DbEndpoint*，並以受管理資料庫的端點位址取代 *DbUserName*

```
sudo mysqldump -u root --databases bitnami_wordpress --single-transaction --
compress --order-by-primary -p$(cat /home/bitnami/bitnami_application_password) |
sudo mysql -u DbUserName --host DbEndpoint --password
```

### 範例

```
sudo mysqldump -u root --databases bitnami_wordpress --single-transaction --compress --order-by-primary -p$(cat /home/bitnami/bitnami_application_password) | sudo mysql -u dbmasteruser --host ls-abc123exampleE67890.czowadgeezqi.us-west-2.rds.amazonaws.com --password
```

4. 出現系統提示時，輸入 MySQL 受管資料庫的密碼，然後按下 Enter 鍵。

在輸入密碼的期間，您將無法看到該密碼。

```
bitnami@ip-172-26-7-200:~$ mysqldump -u root --databases bitnami_wordpress --single-transaction --compress --order-by-primary -p$(cat /home/bitnami/bitnami_application_password) | mysql -u dbmasteruser --host ls-a3420cc0b7a6b772af722d614e64e5c8298cf01c.czowadgeezqi.us-west-2.rds.amazonaws.com --password
Enter password: mysqldump: [Warning] Using a password on the command line interface can be insecure.
```

5. 如果資料轉移成功，即會顯示類似下列範例的回應。

如果發生錯誤，請確認您所使用的資料庫使用者名稱、密碼或端點正確無誤，然後再試一次。

```
Enter password: mysqldump: [Warning] Using a password on the command line interface can be insecure.
bitnami@ip-172-26-7-200:~$
```

### 第 3 步：配置連接 WordPress 到您的 MySQL 託管數據庫

完成下列程序來編輯 WordPress 組態檔案 (wp-config.php)，讓您的網站連線到您的 MySQL 受管理的資料庫。

1. 在連線至 WordPress 執行個體的瀏覽器 SSH 用戶端中，輸入下列指令建立 wp-config.php 檔案備份，以防發生問題。

```
cp /opt/bitnami/wordpress/wp-config.php /opt/bitnami/wordpress/wp-config.php-backup
```

2. 輸入下列命令，以使用 Nano 文字編輯器來開啟 wp-config.php 檔案。

```
nano /opt/bitnami/wordpress/wp-config.php
```

3. 向下捲動，直到您找到 DB\_USER、DB\_PASSWORD、DB\_HOST 的值，如下列範例所示。

```
// ** MySQL settings - You can get this info from your web host ** //  
/** The name of the database for WordPress */  
define('DB_NAME', 'bitnami_wordpress');  
  
/** MySQL database username */  
define('DB_USER', 'bn_wordpress');  
  
/** MySQL database password */  
define('DB_PASSWORD', 'd6ab501583');  
  
/** MySQL hostname */  
define('DB_HOST', 'localhost:3306');
```

#### 4. 修改下列值：

- DB\_USER — 將此值編輯為相符的 MySQL 受管資料庫使用者名稱。Lightsail 受管理資料庫的預設主要使用者名稱為 `dbmasteruser`
- DB\_PASSWORD — 將此值編輯為相符的 MySQL 受管資料庫高強度密碼。如需詳細資訊，請參閱 [管理資料庫密碼](#)。
- DB\_HOST — 將此值編輯為相符的 MySQL 受管資料庫端點。請務必在主機地址的結尾處新增 `:3306` 連接埠號碼。例如 `ls-abc123exampleE67890.czowadgeezqi.us-west-2.rds.amazonaws.com:3306`。

結果應如下列範例所示。

```
// ** MySQL settings - You can get this info from your web host ** //  
/** The name of the database for WordPress */  
define('DB_NAME', 'bitnami_wordpress');  
  
/** MySQL database username */  
define('DB_USER', 'dbmasteruser');  
  
/** MySQL database password */  
define('DB_PASSWORD', 'Q+s) [redacted] ?1|jY');  
  
/** MySQL hostname */  
define('DB_HOST', 'ls-c6d76d20f14d2c [redacted] ca7a695e26.czow [redacted] qi.us-west-2.rds.amazonaws.com:3306');
```

5. 按下 `Ctrl+X` 退出 Nano，接著按 `Y` 鍵和 `Enter` 鍵以儲存編輯內容。
6. 輸入下列命令，重新啟動執行個體上的 Web 服務。

```
sudo /opt/bitnami/ctlscript.sh restart
```

系統重新啟動服務時，會顯示類似下列範例的結果。

```
bitnami@ip-172-26-13-236:~$ sudo /opt/bitnami/ctlscript.sh restart
Syntax OK
/opt/bitnami/apache2/scripts/ctl.sh : httpd stopped
/opt/bitnami/php/scripts/ctl.sh : php-fpm stopped
/opt/bitnami/mysql/scripts/ctl.sh : mysql stopped
/opt/bitnami/mysql/scripts/ctl.sh : mysql started at port 3306
/opt/bitnami/php/scripts/ctl.sh : php-fpm started
Syntax OK
/opt/bitnami/apache2/scripts/ctl.sh : httpd started at port 80
bitnami@ip-172-26-13-236:~$
```

恭喜您！您的 WordPress 網站現在已設定為使用 MySQL 管理的資料庫。

#### Note

若出於任何原因需要還原 wp-config.php 原始檔案，則可輸入下列命令，使用先前在本教學課程中建立的備份來進行還原。

```
cp /opt/bitnami/wordpress/wp-config.php-backup /opt/bitnami/wordpress/wp-config.php
```

## 步驟 4：完成後續步驟

將 WordPress 網站連接到 MySQL 受管理的資料庫後，您應該完成以下額外步驟：

- 建立執行個 WordPress 體的快照。如需詳細資訊，請參閱[建立 Linux 或 Unix 執行個體的快照](#)。
- 建立 MySQL 受管資料庫的快照。如需詳細資訊，請參閱[建立資料庫快照](#)。
- 停用 MySQL 受管資料庫的公有模式和資料匯入模式。如需詳細資訊，請參閱[設定資料庫的公有模式](#)以及[設定資料庫的資料匯入模式](#)。

## 將 WordPress 執行個體 Connect 至 Lightsail 值區以取得靜態內容

本教學說明將您在 Amazon Lightsail 執行個體上執行的 WordPress 網站連線到 Lightsail 值區所需的步驟。您可以使用儲存貯體來託管靜態內容，例如影像和附件。為此，您必須在 WordPress 網站上安裝 WP 卸載媒體精簡版插件，並將其配置為連接到 Lightsail 存儲桶。設定好外掛程式後，您上傳至 WordPress 網站的所有媒體都會自動新增至儲存貯體，而非執行個體的磁碟。

### 內容

- [步驟 1：完成先決條件](#)
- [步驟 2：修改儲存貯體許可](#)
- [第 3 步：在您的 WordPress 的網站上安裝 WP 卸載媒體精簡版插件](#)
- [步驟 4：測試您的 WordPress 網站與 Lightsail 儲存貯體之間的連線](#)

## 步驟 1：完成先決條件

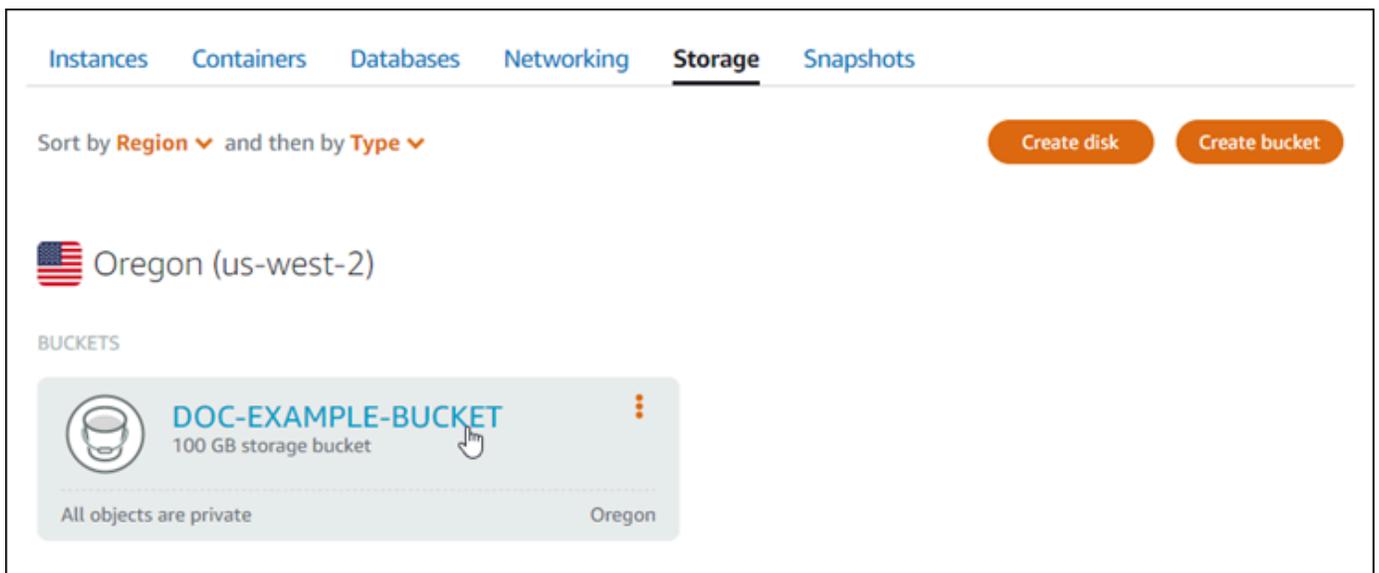
請先完成事前準備 (若尚未完成)：

- 在 Light WordPress sail 中建立實體。如需詳細資訊，請參閱[教學課程：在 Amazon Lightsail 中啟動和設定 WordPress 執行個體](#)。
- 在 Lightsail 物件儲存服務中建立值區。如需詳細資訊，請參閱[建立儲存貯體](#)。

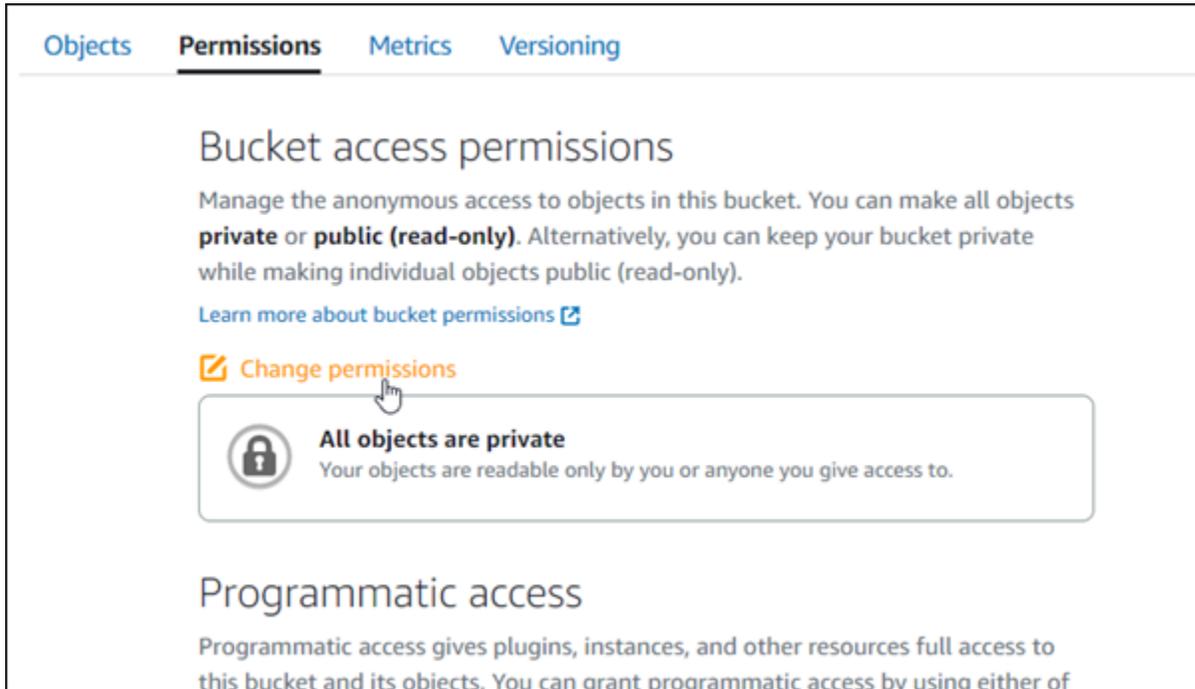
## 步驟 2：修改儲存貯體許可

請完成下列程序來變更值區的權限，以提供 WordPress 執行個體和卸載媒體精簡版外掛程式的存取權。儲存貯體的存取許可必須設為 Individual objects can be made public (read-only) (個別物件可設為公有 (唯讀))。您也必須將 WordPress 執行個體附加至值區的存取角色。如需有關儲存貯體許可的詳細資訊，請參閱[儲存貯體許可](#)。

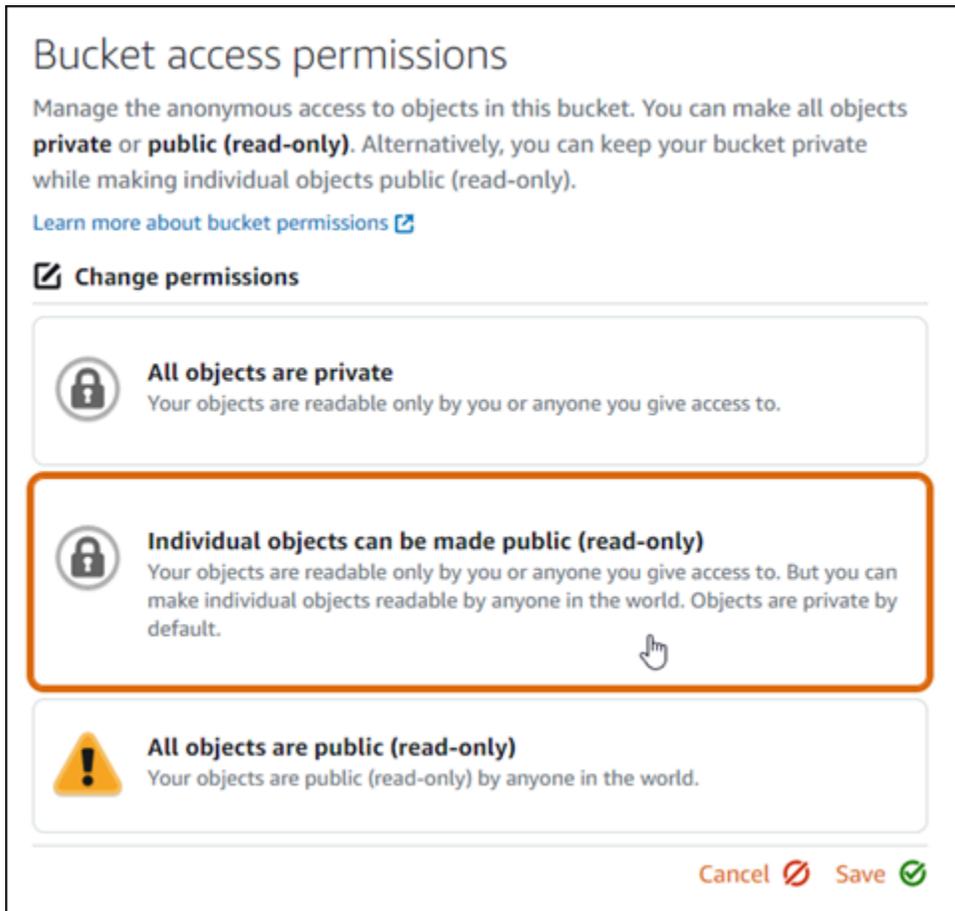
1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁上，選擇儲存空間索引標籤。
3. 選擇您要在 WordPress 網站上使用的值區名稱。



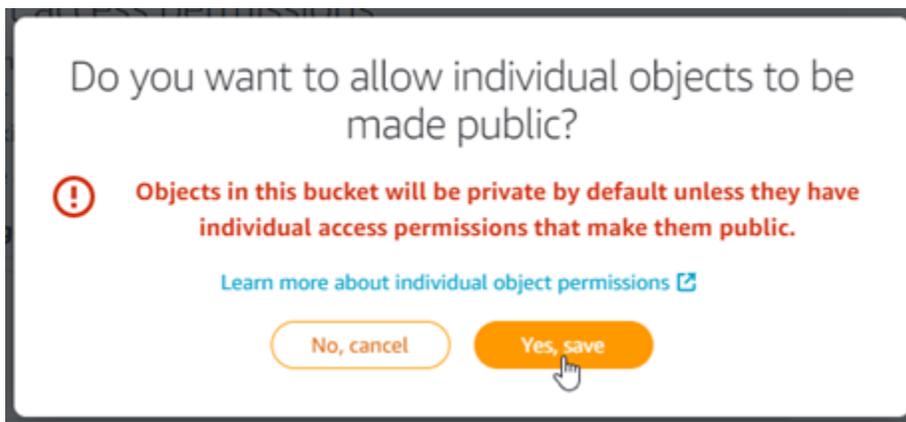
4. 選擇 Bucket management (儲存貯體管理) 頁面上的 Permissions (許可) 索引標籤。
5. 在頁面的 Bucket access permissions (儲存貯體存取許可) 區段下選擇 Change permissions (變更許可)。



6. 選擇 Individual objects can be made public and read only (可將個別物件設為公有和唯讀)。

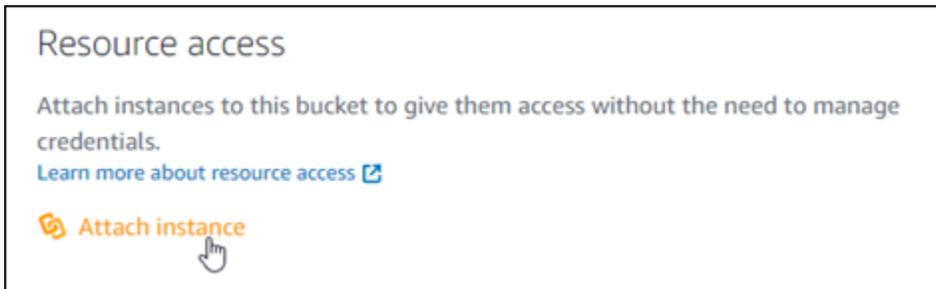


7. 選擇 Save (儲存)。
8. 在出現的確認提示中，選擇 Yes, save (是，儲存)。

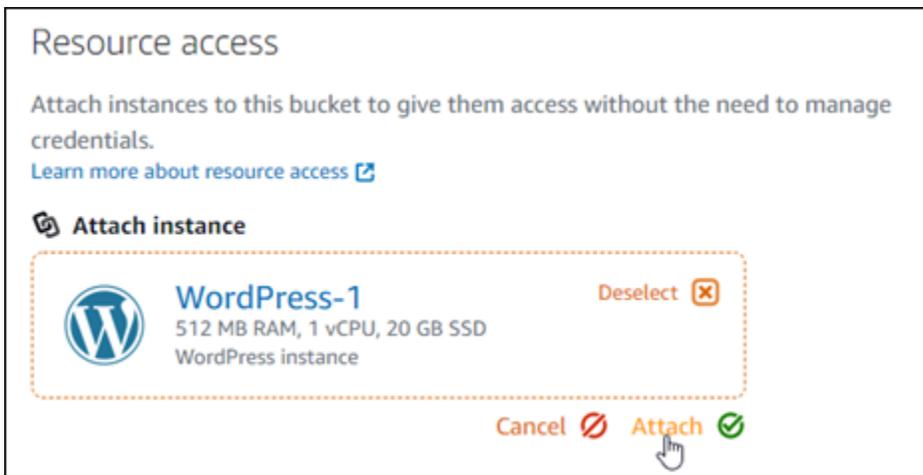


幾分鐘後，儲存貯體會設定為允許個別物件存取。如此可確保使用卸載 Media Lite 外掛程式從您的 WordPress 網站上傳至儲存貯體的物件可供客戶讀取。

9. 捲動至頁面的 Resource access (資源存取) 區段，然後選擇 Attach instance (連接執行個體)。



10. 在出現的下拉式清單中選擇 WordPress 執行個體的名稱，然後選擇 [連接]。



片刻之後，您的 WordPress 執行個體就會連接到儲存貯體。這可讓您的 WordPress 執行個體存取權以管理值區及其物件。

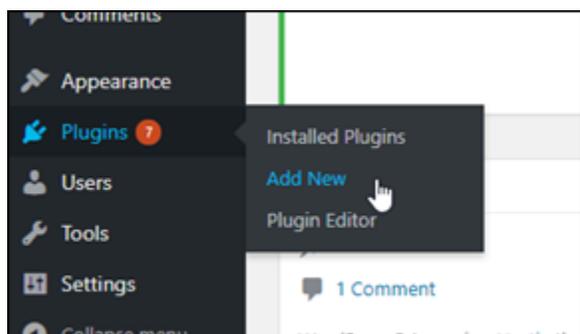
### 第 3 步：在您的 WordPress 的網站上安裝 WP 卸載媒體精簡版插件

完成以下步驟，在您的 WordPress 網站上安裝 WP 卸載媒體精簡版外掛程式。此插件會自動將通過媒體上傳器添加的圖像，視頻，文檔和任何其他 WordPress 媒體複製到 Lightsail 存儲桶中。有關更多信息，請參閱 [WP 卸載媒體精簡版](#) 在 WordPress 網站上。

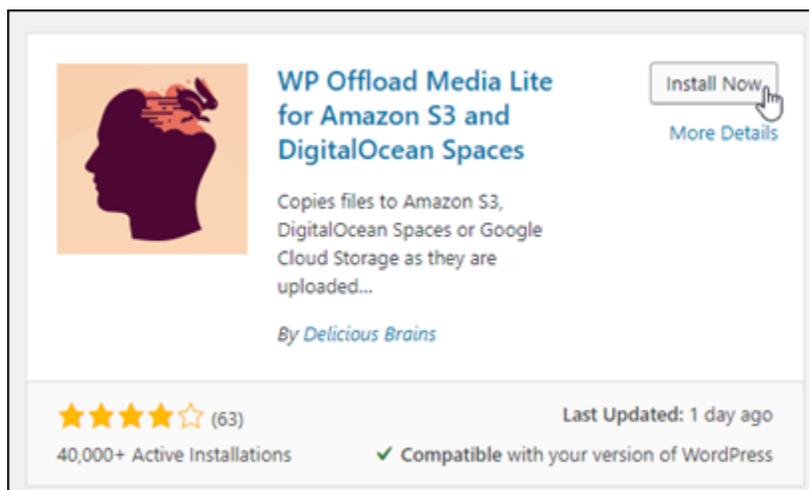
1. 以系統管理員身分登入您 WordPress 網站的儀表板。

如需詳細資訊，請參閱在 [Amazon Lightsail 中取得 Bitnami 執行個體的應用程式使用者名稱和密碼](#)。

2. 將滑鼠游標暫停在左側導覽選單中的 Plugins (外掛程式) 上，然後選擇 Add New (新增)。



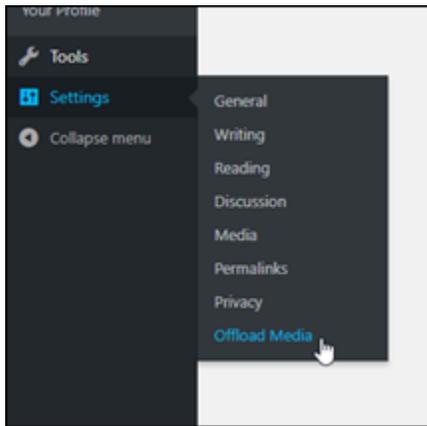
3. 搜尋 WP Offload Media Lite。
4. 在搜尋結果中，選擇 WP Offload Media 外掛程式旁的 Install Now (立即安裝)。



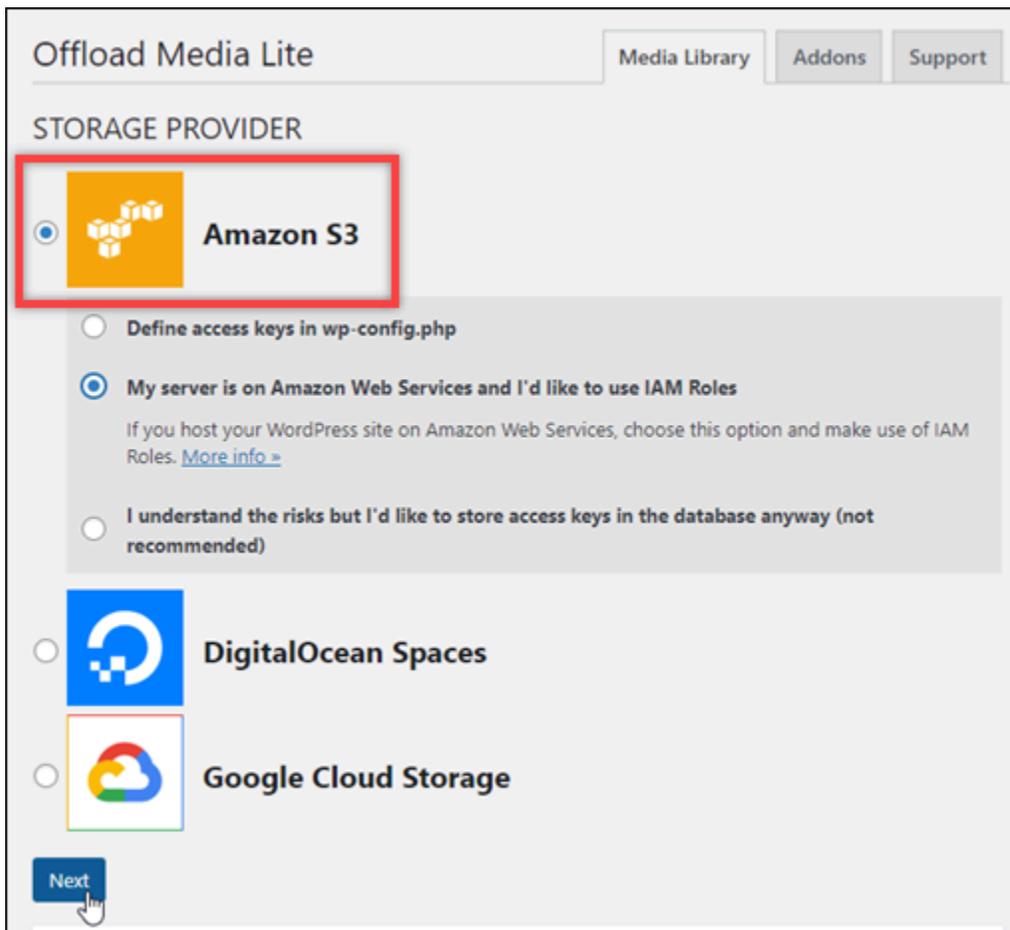
5. 在外掛程式完成安裝後，選擇 Activate (啟用)。



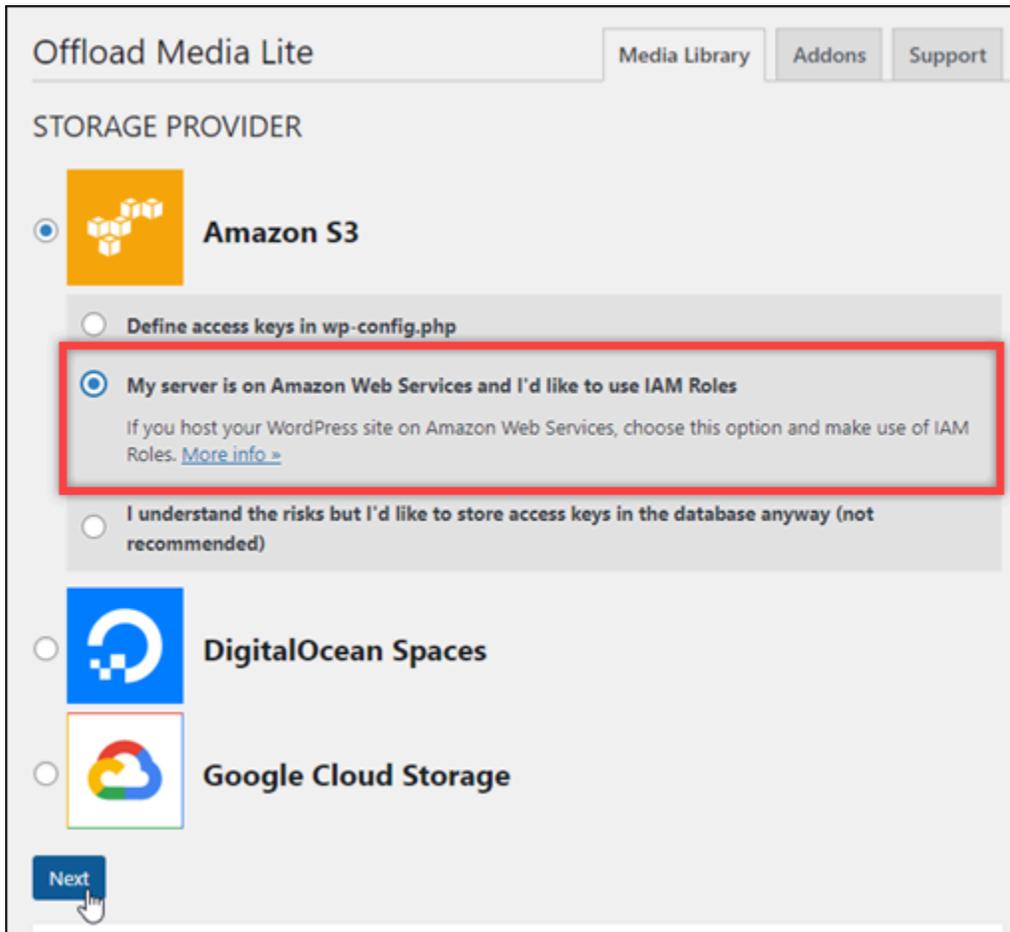
6. 在左側導覽功能表中，選擇 Settings (設定)，然後選擇 Offload Media (卸載媒體)。



7. 在 Offload Media (卸載媒體) 頁面中，選擇 Amazon S3 作為儲存供應商。

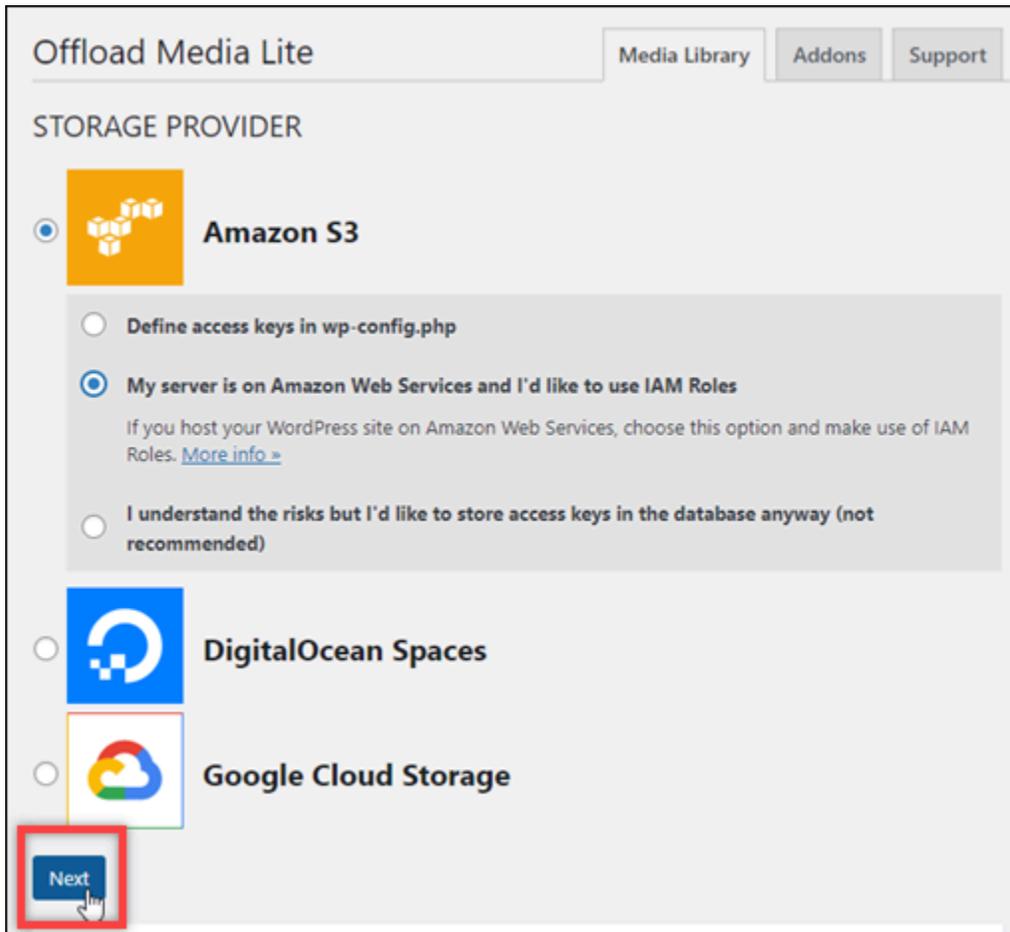


8. 選擇我的服務器在 Amazon Web Services 上，我想使用IAM角色。



The screenshot shows the 'Offload Media Lite' configuration interface. At the top, there are three tabs: 'Media Library', 'Addons', and 'Support'. Below the tabs, the 'STORAGE PROVIDER' section is visible. Under 'Amazon S3', three radio button options are listed. The second option, 'My server is on Amazon Web Services and I'd like to use IAM Roles', is selected and highlighted with a red rectangular box. Below this option, there is explanatory text and a link to 'More info'. The other two options are 'Define access keys in wp-config.php' and 'I understand the risks but I'd like to store access keys in the database anyway (not recommended)'. Below the Amazon S3 section, there are two other storage providers: 'DigitalOcean Spaces' and 'Google Cloud Storage'. At the bottom left of the configuration area, there is a blue 'Next' button with a mouse cursor pointing to it.

9. 選擇 Next (下一步)。



Offload Media Lite Media Library Addons Support

STORAGE PROVIDER

 **Amazon S3**

Define access keys in wp-config.php

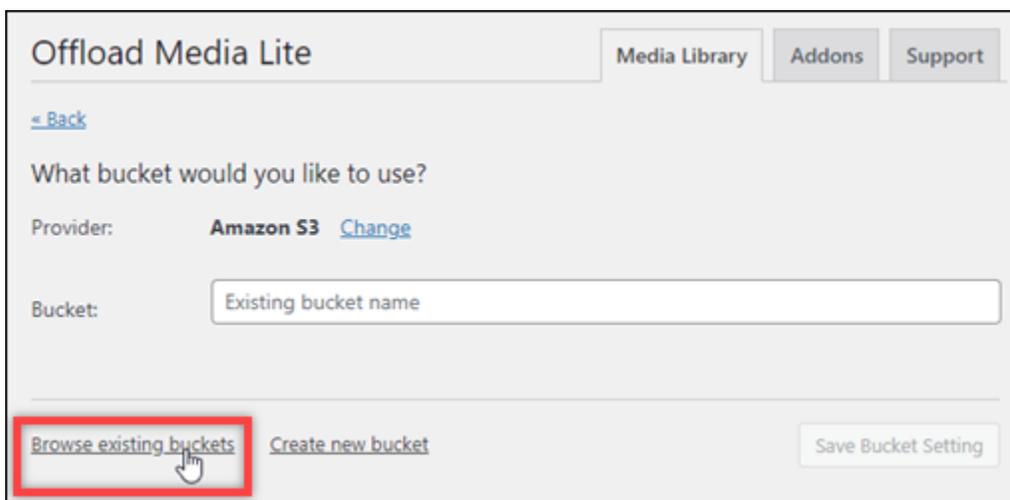
**My server is on Amazon Web Services and I'd like to use IAM Roles**  
If you host your WordPress site on Amazon Web Services, choose this option and make use of IAM Roles. [More info >](#)

I understand the risks but I'd like to store access keys in the database anyway (not recommended)

 **DigitalOcean Spaces**

 **Google Cloud Storage**

10. 在出現的 What bucket would you like to use (您要使用的儲存貯體) 頁面中，選擇 Browse existing buckets (瀏覽現有儲存貯體)。



Offload Media Lite Media Library Addons Support

[← Back](#)

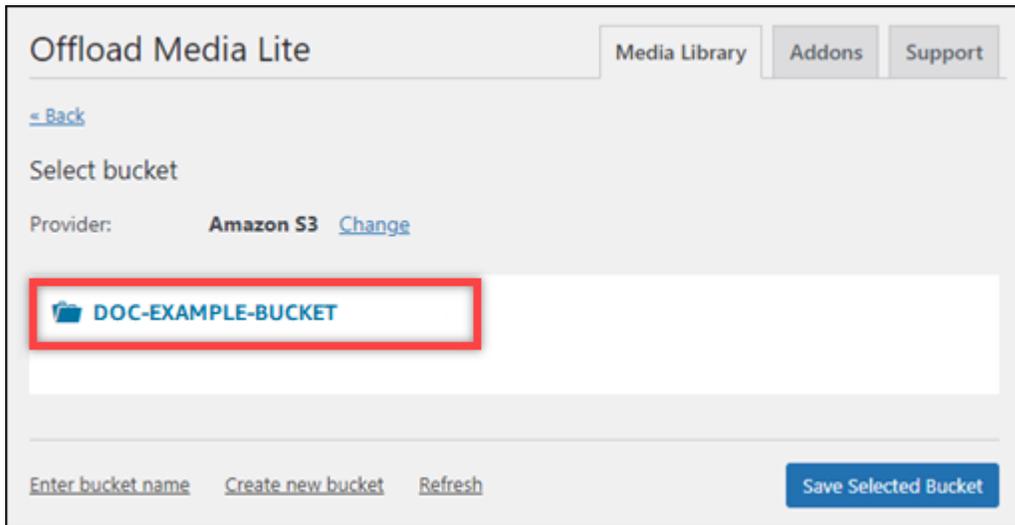
What bucket would you like to use?

Provider: **Amazon S3** [Change](#)

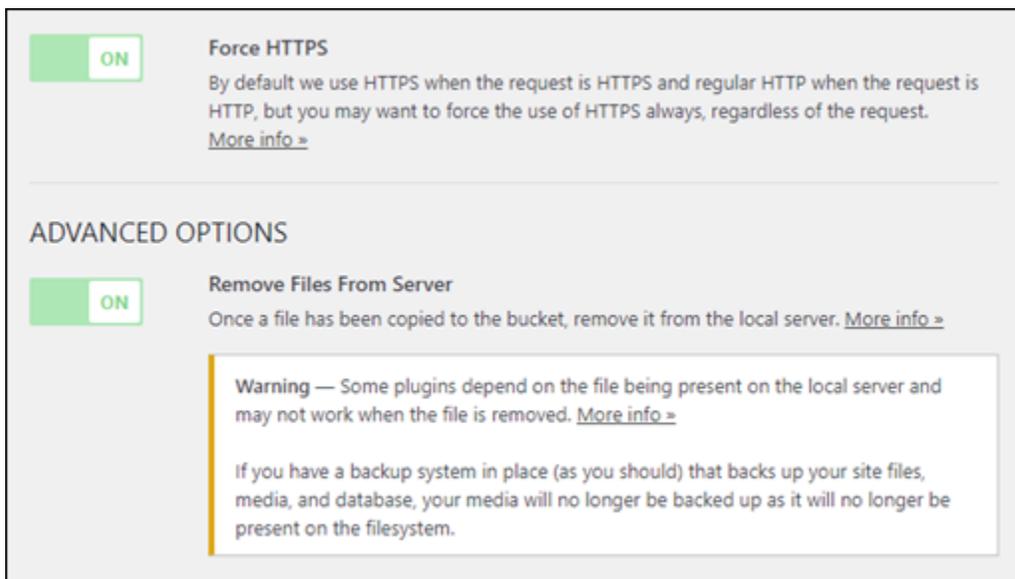
Bucket:

[Create new bucket](#)

11. 選擇您要搭配執行個體使用的值區名 WordPress 稱。



12. 在出現的「卸載媒體精簡版設定」頁面中，確定開啟「強制執行」HTTPS 和「從伺服器移除檔案」。
  - 必須開啟「強制」HTTPS 設定，因為 Lightsail 值區預設會使用 HTTPS 來提供媒體檔案。如果您未開啟此功能，從您的 WordPress 網站上傳至 Lightsail 儲存貯體的媒體檔案將無法正確提供給您的網站訪客。
  - 「從伺服器移除檔案」設定可確保上傳至 Lightsail 儲存貯體的媒體也不會儲存在執行個體的磁碟上。如果未開啟此功能，上傳至 Lightsail 儲存貯體的媒體檔案也會儲存在 WordPress 執行個體的本機儲存空間中。



13. 選擇 Save Changes (儲存變更)。

**Note**

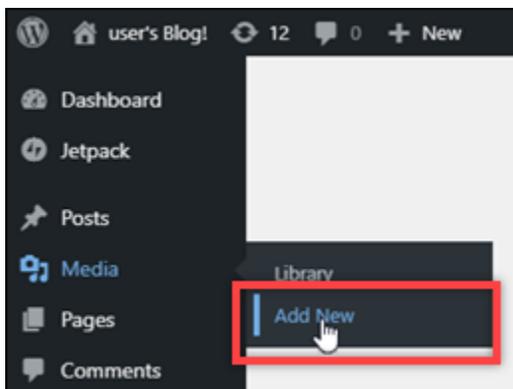
若要稍後返回 Offload Media Lite Settings (Offload Media Lite 設定) 頁面，請將滑鼠游標暫停在左側導覽選單中的 Settings (設定)，然後選擇 Offload Media Lite。

您的 WordPress 網站現在已設定為使用媒體精簡版外掛程式。下次您透過上傳媒體檔案時 WordPress，該檔案會自動上傳至您的 Lightsail 儲存貯體，並由值區提供。若要測試組態，請繼續前往本教學課程下一節。

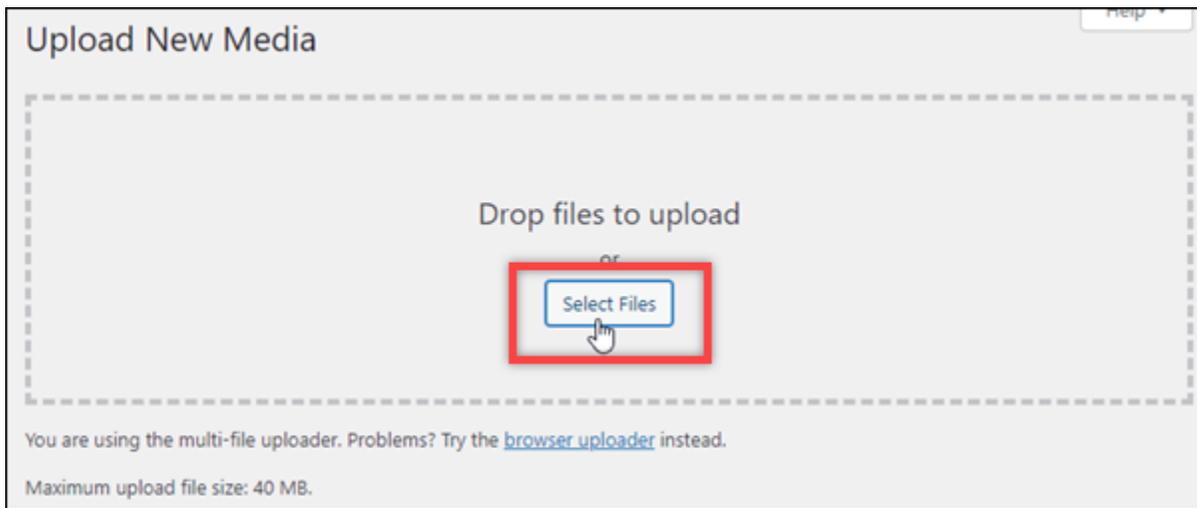
## 步驟 4：測試您的 WordPress 網站與 Lightsail 儲存貯體之間的連線

請完成下列程序，將媒體檔案上傳至您的 WordPress 執行個體，並確認該檔案已上傳至 Lightsail 儲存貯體，並從您的 Lightsail 儲存貯體提供。

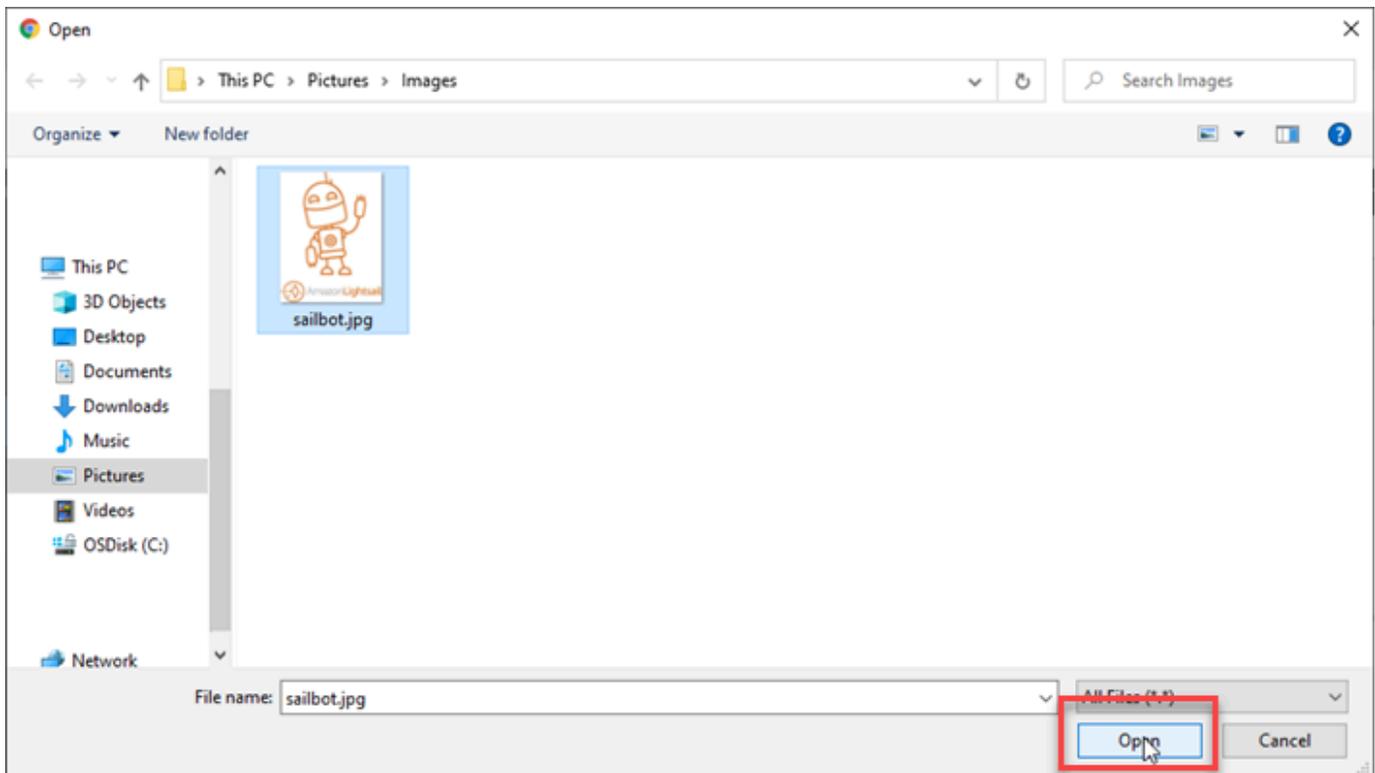
1. 暫停 WordPress 儀表板左側導覽功能表中的「媒體」，然後選擇「新增」。



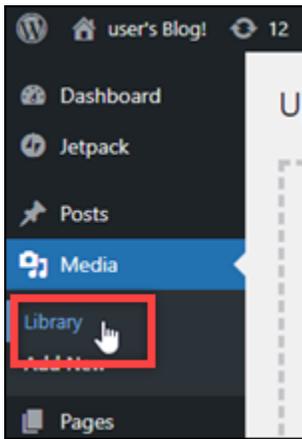
2. 在出現的 Upload New Media (上傳新媒體) 頁面上，選擇 Select Files (選取檔案)。



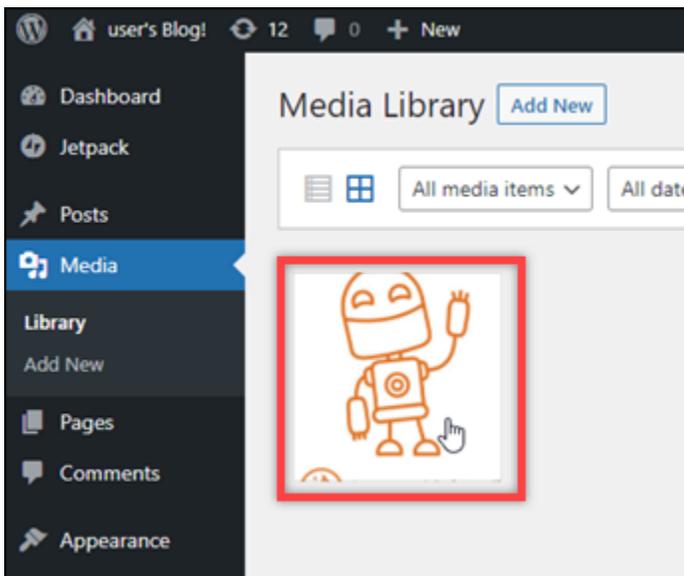
3. 選擇要從本機電腦上傳的媒體檔案，然後選擇 Open (開啟)。



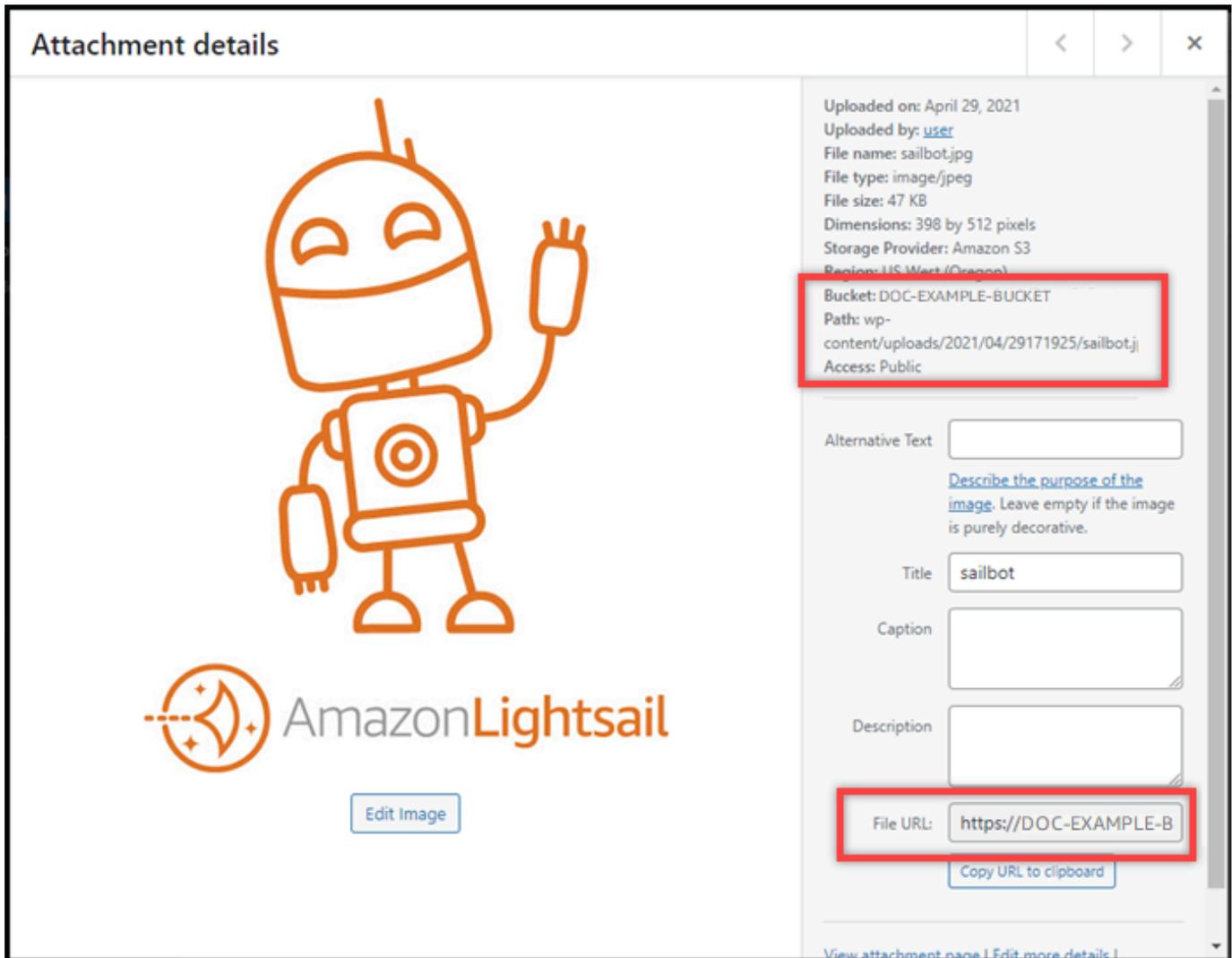
4. 檔案上傳完畢時，選擇左側導覽選單中 Media (媒體) 下方的 Library (程式庫)。



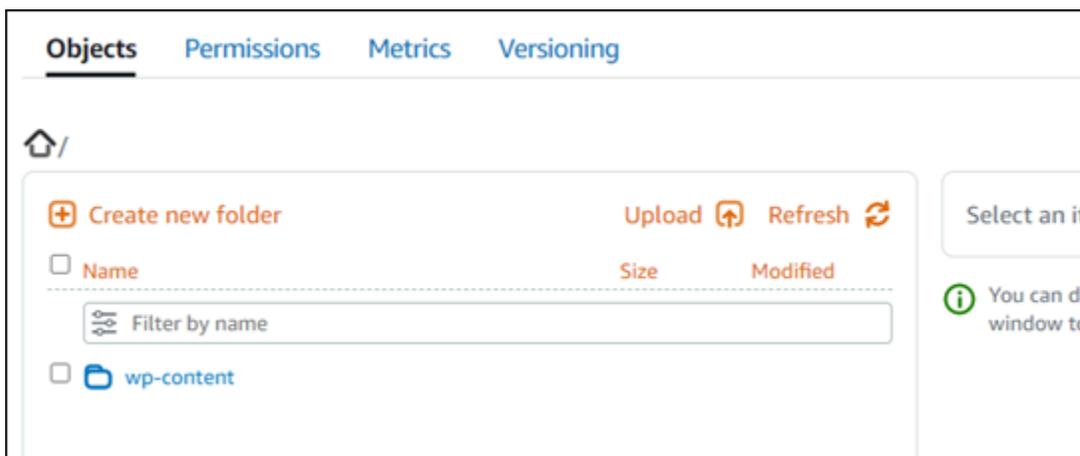
5. 選擇最近上傳的檔案。



6. 在檔案的詳細資料面板中，您應該會在「值區」和「檔案」URL 欄位中看到值區的名稱。



7. 當您前往 Lightsail 值區管理頁面的 [物件] 索引標籤時，應該會看到可濕性粉劑內容資料夾。此資料夾由 Offload Media Lite 外掛程式建立，用於存放上傳的媒體檔案。



## 管理儲存貯體和物件

以下是管理 Lightsail 物件儲存貯體的一般步驟：

1. 了解 Amazon Lightsail 物件儲存服務中的物件和值區。如需詳細資訊，請參閱 [Amazon Lightsail 中的物件儲存](#)。
2. 了解您可以在 Amazon Lightsail 中為您的儲存貯體提供哪些名稱。如需詳細資訊，請參閱 [Amazon Lightsail 中的儲存貯體命名規則](#)。
3. 透過建立值區開始使用 Lightsail 物件儲存服務。如需詳細資訊，請參閱 [在 Amazon Lightsail 中建立值區](#)。
4. 了解儲存貯體的安全最佳實務，以及可以為儲存貯體設定的存取許可。可以將儲存貯體中的所有物件設為公有或私有，也可以選擇將個別物件設為公有。您也可以建立存取金鑰、將執行個體附加至儲存貯體，以及授予其他AWS帳戶的存取權，以授予儲存貯體的存取權。如需詳細資訊，請參閱 [Amazon Lightsail 物件儲存的安全最佳實務和了解 Amazon Lightsail 中的儲存貯體許可](#)。

了解儲存貯體存取許可後，請參閱下列指南來授予對儲存貯體的存取權：

- [封鎖儲存貯體的公開存取](#)
  - [在 Amazon Lightsail 集團中設定儲存貯體存取權限](#)
  - [在 Amazon Lightsail 中為儲存貯體中的個別物件設定存取權限](#)
  - [在 Amazon Lightsail 中為存儲桶創建訪問密鑰](#)
  - [在 Amazon Lightsail 中設定儲存貯體的資源存取](#)
  - [在 Amazon Lightsail 中設定儲存貯體的跨帳戶存取](#)
5. 了解如何為儲存貯體啟用存取日誌記錄，以及如何使用存取日誌來稽核儲存貯體的安全性。如需詳細資訊，請參閱下列指南。
    - [Amazon Lightsail 物件儲存服務中儲存貯體的存取記錄](#)
    - [存取 Amazon Lightsail 物件儲存服務中儲存貯體的日誌格式](#)
    - [在 Amazon Lightsail 物件儲存服務中啟用儲存貯體的存取記錄](#)
    - [在 Amazon Lightsail 中使用儲存貯體的存取日誌來識別請求](#)
  6. 建立IAM政策以授與使用者在 Lightsail 中管理值區的能力。如需詳細資訊，請參閱 [在 Amazon Lightsail 中管理儲存貯體的IAM政策](#)。
  7. 了解儲存貯體中物件的標記和識別方式。如需詳細資訊，請參閱 [了解 Amazon Lightsail 中的物件金鑰名稱](#)。
  8. 了解如何在儲存貯體中上傳檔案及管理物件。如需詳細資訊，請參閱下列指南。
    - [將文件上傳到 Amazon Lightsail](#)

- [使用多部分上傳將檔案上傳到 Amazon Lightsail 中的儲存貯體](#)
  - [檢視儲存貯體中 Amazon Lightsail](#)
  - [在 Amazon Lightsail 中複製或移動值區中的物件](#)
  - [從儲存貯體下 Amazon Lightsail](#)
  - [在 Amazon Lightsail 中過濾儲存桶中的對象](#)
  - [標記儲存桶中 Amazon Lightsail](#)
  - [刪除儲存桶中 Amazon Lightsail](#)
9. 啟用物件版本控制功能來保留、擷取和恢復儲存貯體中所儲存每個物件的各個版本。如需詳細資訊，請參閱在 [Amazon Lightsail 中啟用和暫停儲存貯體中的物件版本控制](#)。
10. 啟用物件版本控制之後，可以還原儲存貯體中物件的先前版本。如需詳細資訊，請參閱在 [Amazon Lightsail 中還原儲存貯體中的舊版物件](#)。
11. 監控儲存貯體的使用率。如需詳細資訊，請參閱在 [Amazon Lightsail 中檢視儲存貯體的指標](#)。
12. 設定儲存貯體指標的警示，以便在儲存貯體的使用率超過閾值時收到通知。如需詳細資訊，請參閱在 [Amazon Lightsail 中建立儲存貯體指標警示](#)。
13. 如果儲存空間和網路傳輸不足，請變更儲存貯體的儲存計畫。如需詳細資訊，請參閱在 [Amazon Lightsail 中變更儲存貯體的計畫](#)。
14. 了解如何將儲存貯體連線至其他資源。如需詳細資訊，請參閱下列教學課程。
- [教學課程：將 WordPress 執行個體連接至 Amazon Lightsail 儲存貯體](#)
  - [教學課程：將 Amazon Lightsail 儲存貯體與 Lightsail 內容交付網路分發搭配使用](#)
15. 如果不再使用儲存貯體，請刪除它。如需詳細資訊，請參閱 [刪除儲存貯體](#)。

## WordPress 使用 Lightsail 內容傳遞網路進行設定

在本指南中，我們將說明如何將 WordPress 執行個體設定為與 Amazon Lightsail 分發搭配使用。

根據預設，所有 Lightsail 發行版都已為其預設網域啟用 HTTPS (例如，123456abcdef.cloudfront.net)。您的分發配置決定了分發和實例之間的連接是否已加密。

- 您的 WordPress 網站僅使用 HTTP — 如果您的網站僅使用 HTTP 作為發佈的來源，且未設定為使用 HTTPS，則您可以設定分發以終止 SSL/TLS，並使用未加密的連線將所有內容請求轉寄給執行個體。
- 您的 WordPress 網站使用 HTTPS — 如果您的網站使用 HTTPS 作為發佈的來源，您可以將分發設定為使用加密連線將所有內容請求轉寄至執行個體。此配置稱為 end-to-end 加密。

## 建立發行版

完成下列步驟，為您的執行個體設定 Lightsail 發 WordPress 行版。如需詳細資訊，請參閱 [the section called “建立分發”](#)。

### 先決條件

如中所述建立和設定 WordPress 執行個體 [the section called “WordPress”](#)。

若要為您的執行個 WordPress 體建立散發

1. 在 Lightsail 首頁上，選擇 [網路功能]。
2. 選擇 Create Distribution (建立分佈)。
3. 在 [選擇您的來源] 中，選擇 WordPress 執行個體的區域，然後選擇您的 WordPress 執行個體。我們會自動使用您連接到執行個體的靜態 IP 位址。
4. 對於「快取行為」，請選擇「最佳」WordPress。
5. (選擇性) 若要設定 end-to-end 加密，請將原始通訊協定原則變更為僅 HTTPS。如需詳細資訊，請參閱 [the section called “原始伺服器通訊協定政策”](#)。
6. 設定其餘選項，然後選擇 [建立分發]。
7. 在 [自訂網域] 索引標籤上選擇 [建立憑證]。輸入憑證的唯一名稱，輸入網域和子網域的名稱，然後選擇 [建立憑證]。
8. 選擇 Attach certificate (連接憑證)。
9. 在 [更新 DNS 記錄] 中，選擇 [我瞭解]。

## 更新 DNS 記錄

請完成下列步驟，以更新您的 DNS 區 Lightsail DNS 記錄。

若要更新您的散發的 DNS 記錄

1. 在首頁 Lightsail，選擇網域和 DNS。
2. 選擇您的 DNS 區域，然後選擇 DNS 記錄標籤。
3. 刪除您在憑證中指定之網域的 A 和 AAAA 記錄。
4. 選擇 [新增記錄]，然後建立 CNAME 記錄，將您的網域解析為您的分發網域 (例如，D2vbec9Example)。
5. 選擇儲存。

## 允許散發快取靜態內容

請完成下列程序來編輯 WordPress 執行個體中的 wp-config.php 檔案，使其與您的發行版本搭配使用。

### Note

建議您先建立執行個 WordPress 體的快照，然後再開始執行此程序。快照可用作備份，您可從中建立另一個執行個體，以防發生問題。如需詳細資訊，請參閱[建立 Linux 或 Unix 執行個體的快照](#)。

1. 登入主 [Lightsail](#) 台。
2. 在 Lightsail 首頁上，選擇顯示在執行個體旁邊的瀏覽器型 SSH 用戶端圖示。WordPress
3. 在您連線至執行個體後，請輸入以下命令來建立 wp-config.php 檔案的備份。如果發生問題，您可以使用備份來還原檔案。

```
sudo cp /opt/bitnami/wordpress/wp-config.php /opt/bitnami/wordpress/wp-config.php.backup
```

4. 輸入下列命令，以使用 Vim 來開啟 wp-config.php 檔案。

```
sudo vim /opt/bitnami/wordpress/wp-config.php
```

5. 在 Vim 中按 I 以進入插入模式。
6. 刪除檔案中以下幾行程式碼。

```
define('WP_SITEURL', 'http://' . $_SERVER['HTTP_HOST'] . '/');  
define('WP_HOME', 'http://' . $_SERVER['HTTP_HOST'] . '/');
```

7. 根據您使用的版本，將下列其中一程式碼新增至檔案：WordPress

- 如果使用的是版本 3.3 或更低版本，請將以下幾行程式碼新增至您先前刪除程式碼的位置。

```
define('WP_SITEURL', 'https://' . $_SERVER['HTTP_HOST'] . '/');  
define('WP_HOME', 'https://' . $_SERVER['HTTP_HOST'] . '/');  
if (isset($_SERVER['HTTP_CLOUDFRONT_FORWARDED_PROTO'])  
&& $_SERVER['HTTP_CLOUDFRONT_FORWARDED_PROTO'] === 'https') {  
    $_SERVER['HTTPS'] = 'on';  
}
```

```
}
```

- 如果使用的是版本 3.3.1-5 或更高版本，請將以下幾行程式碼新增至您先前刪除程式碼的位置。

```
define('WP_SITEURL', 'http://DOMAIN/');  
define('WP_HOME', 'http://DOMAIN/');  
if (isset($_SERVER['HTTP_CLOUDFRONT_FORWARDED_PROTO'])  
&& $_SERVER['HTTP_CLOUDFRONT_FORWARDED_PROTO'] === 'https') {  
    $_SERVER['HTTPS'] = 'on';  
}
```

8. 在 Vim 中按 Esc 鍵以離開插入模式，然後鍵入 :wq! 並按 Enter (輸入) 以儲存您的編輯 (寫入)，然後退出 Vim。
9. 輸入下列命令以重新啟動執行個體上的 Apache 服務。

```
sudo /opt/bitnami/ctlscript.sh restart apache
```

10. 稍候片刻，讓 Apache 服務重新啟動，然後測試分發是否正在快取您的內容。如需詳細資訊，請參閱[測試您的 Amazon Lightsail 分發](#)。
11. 如果發生問題，請使用瀏覽器型 SSH 用戶端重新連接至執行個體。使用您先前依本指南建立的備份，執行下列命令來還原 wp-config.php 檔案。

```
sudo cp /opt/bitnami/wordpress/wp-config.php.backup /opt/bitnami/wordpress/wp-config.php
```

還原檔案之後，請輸入下列命令以重新啟動 Apache 服務：

```
sudo /opt/bitnami/ctlscript.sh restart apache
```

## 分發的其他相關資訊

以下是一些可協助您在 Lightsail 中管理發行版的文章：

- [內容交付網路分發](#)
- [建立分發](#)
- [了解分發的請求和回應行為](#)
- [測試您的分發](#)
- [變更分發的原始伺服器](#)

- [變更分發的快取行為](#)
- [重設分發的快取](#)
- [變更分發計畫](#)
- [啟用分發的自訂域](#)
- [將域指向分發](#)
- [變更分發的自訂域](#)
- [停用分發的自訂域](#)
- [檢視分發指標](#)
- [刪除分發](#)

## 在 Lightsail 中為 WordPress 實例啟用電子郵件

您可以在 Amazon Lightsail 中的 WordPress 執行個體上啟用電子郵件。在 Amazon Simple Email Service (Amazon SES) 中設定 SMTP 服務。然後在執行個體上啟用和設定 WP 郵件 SMTP 外掛程式。啟用電子郵件後，您的 WordPress 管理員可以為其用戶配置文件請求密碼重置，並將發送博客文章，網站更新和其他插件消息的電子郵件通知。本指南說明如何使用 Amazon SES 在 Amazon Lightsail 中在 WordPress 執行個體上啟用電子郵件。

### 內容

- [步驟 1：檢閱限制](#)
- [步驟 2：完成事前準備](#)
- [步驟 3：在 Amazon SES 中建立 SMTP 憑證](#)
- [步驟 4：在 Amazon SES 中驗證域](#)
- [步驟 5：在 Amazon SES 中驗證電子郵件地址](#)
- [步驟 6：在您的 WordPress 實例上配置 WP 郵件 SMTP 插件](#)

如需詳細資訊，請參閱 Amazon SES 文件中的[使用 Amazon SES SMTP 介面來傳送電子郵件](#)。

### 步驟 1：檢閱限制

Amazon SES 沙盒中的新 Amazon Web Services (AWS) 帳戶可僅將電子郵件傳送至已驗證的地址和域。如果您的帳戶是這種情況，建議您驗證網站的網域，並驗證 WordPress 管理員的電子郵件地址。

要獲取他們的電子郵件地址，請登錄到您 WordPress 網站的儀表板，然後在左側導航菜單中選擇「用戶」。您將會看到在 Email (電子郵件) 欄中所列的管理員電子郵件地址，如下範例所示：

<input type="checkbox"/>	Username	Name	Email	Role
<input type="checkbox"/>	 Carlos	Carlos Salazar	user1@lightsail-demo.com	Administrator
<input type="checkbox"/>	 Jane	Jane Doe	user2@lightsail-demo.com	Administrator
<input type="checkbox"/>	 John	John Doe	user3@lightsail-demo.com	Administrator
<input type="checkbox"/>	 user	—	user@example.com	Administrator

### Note

預設 user 設定檔是使用 user@example.com 電子郵件地址設定。您應該將此地址變更為運作中的電子郵件地址。如需詳細資訊，請參閱 WordPress 文件中的[使用者設定檔畫面](#)。

若要將電子郵件傳送到任何地址和域，則必須請求將您的帳戶移出 Amazon SES 沙盒。如需詳細資訊，請參閱 Amazon SES 文件中的[移出 Amazon SES 沙盒](#)。

## 步驟 2：完成事前準備

您必須先完成下列工作，才能在 WordPress 執行個體上啟用電子郵件：

- 在 Light WordPress sail 中建立實體。如需詳細資訊，請參閱[教學課程：在 Amazon Lightsail 中啟動和設定 WordPress 執行個體](#)。
- 使用 Lightsail DNS 區域，將您註冊的網域指向您的 WordPress 執行個體。如需詳細資訊，請參閱[建立 DNS 區域以管理域的 DNS 記錄](#)。
- 註冊 Amazon SES 並進一步了解此服務。如需有關註冊 Amazon SES 的詳細資訊，請參閱 Amazon SES 文件中的[Amazon SES 快速入門](#)。如需有關 Amazon SES 的詳細資訊，請參閱 Amazon SES 文件中的以下指南：
  - [Amazon SES 開發人員指南](#)
  - [Amazon SES 常見問題](#)
  - [Amazon SES 定價](#)
  - [Amazon SES Service Quotas](#)

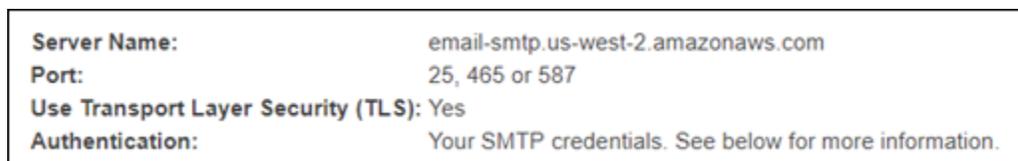
### 步驟 3：在 Amazon SES 中建立 SMTP 憑證

若要設定您在此指南稍後部分設定的 WP Mail SMTP 外掛程式，必須在 Amazon SES 帳戶中建立 SMTP 憑證。如需詳細資訊，請參閱 Amazon SES 文件中的[取得 Amazon SES SMTP 憑證](#)。

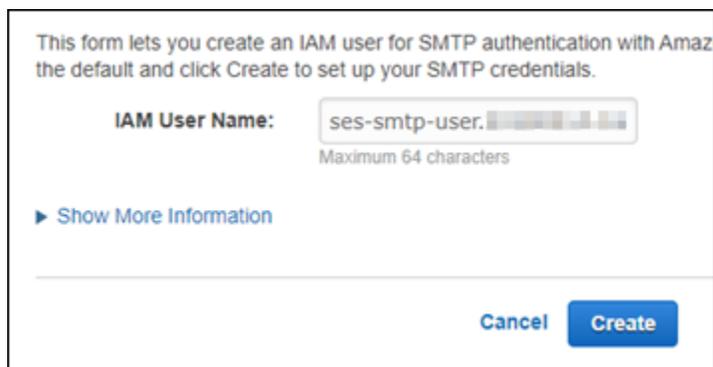
在 Amazon SES 中建立 SMTP 憑證

1. 登入 [Amazon SES 主控台](#)。
2. 從左側導覽功能表中，選擇 SMTP settings (SMTP 設定)。

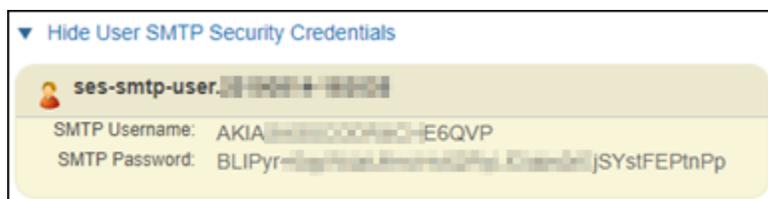
SMTP settings (SMTP 設定) 頁面會顯示您的 SMTP 伺服器名稱、連接埠和 TLS 設定。請注意這些值，因為在執行個體上設定 WP Mail SMTP 外掛程式時，在本指南中稍後需要這些 WordPress 值。



3. 選擇建立 SMTP 憑證。
4. 在 IAM 使用者名稱文字方塊中，保留預設使用者名稱，然後選擇建立。



5. 選擇 Show User SMTP Security Credentials (顯示使用者 SMTP 安全登入資料) 來檢視 SMTP 使用者名稱和密碼，或選擇 Download Credentials (下載登入資料)，來下載內含相同資訊的 CSV 檔案。稍後在 WordPress 執行個體上配置 WP Mail SMTP 外掛程式時，您需要這些憑據。



 Note

在 Amazon SES 主控台中建立的憑證會自動新增到您帳戶的 AWS Identity and Access Management (IAM)。

## 步驟 4：在 Amazon SES 中驗證域

Amazon SES 將要求您驗證域，以確認您擁有該域，並且防止他人使用。在驗證網域時，將驗證所有來自該網域的電子郵件地址，所以您不需要個別驗證該網域中的電子郵件地址。例如，如果您驗證網域 `example.com`，您可以從 `user1@example.com`、`user2@example.com` 或 `example.com` 的任何其他使用者傳送電子郵件。如需詳細資訊，請參閱 Amazon SES 文件中的[驗證 Amazon SES 中的網域](#)。

在 Amazon SES 中驗證域

1. 在 [Amazon SES 主控台](#) 中，從左側導覽功能表中選擇驗證身分。
2. 選擇 Create identity (建立身分)。
3. 輸入要驗證的網域，然後選擇建立身分。

您驗證的網域應與您在 Lightsail 中用於 WordPress 執行個體的網域相同。

 Important

### 舊版 TXT 記錄

Amazon SES 中的網域驗證現在以 DomainKeys 識別郵件 (DKIM) 為基礎，這是接收郵件伺服器用來驗證電子郵件真實性的電子郵件身份驗證標準。在網域的 DNS 設定中設定 DKIM 會向 SES 確認您是身分擁有者，因此不需要 TXT 記錄。使用 TXT 記錄驗證的網域身分不需要重新驗證；不過，我們仍建議您啟用 DKIM 簽章，以透過符合 DKIM 標準的電子郵件提供者提高郵件的可交付性。

# Create identity

A *verified identity* is a domain, subdomain, or email address you use to send email through Amazon SES. Identity verification at the domain level extends to all email addresses under one verified domain identity.

## Identity details [Info](#)

### Identity type

**Domain**

To verify ownership of a domain, you must have access to its DNS settings to add the necessary records.

**Email address**

To verify ownership of an email address, you must have access to its inbox to open the verification email.

### Domain

Domain name can contain up to 253 alphanumeric characters.

**Assign a default configuration set**

Enabling this option ensures that the assigned configuration set is applied to messages sent from this identity by default whenever a configuration set isn't specified at the time of sending.

**Use a custom MAIL FROM domain**

Configuring a custom MAIL FROM domain for messages sent from this identity enables the MAIL FROM address to align with the From address. Domain alignment must be achieved in order to be DMARC compliant.

## Verifying your domain

### DKIM-based domain verification

DomainKeys Identified Mail (DKIM) is an email authentication method that Amazon SES uses to verify domain ownership and that receiving mail servers use to validate email authenticity. You must configure DKIM as part of the domain verification process.

### Configuring DKIM

Following identity creation, Amazon SES will provide a set of DNS records. These records must be published to your domain's DNS server in order to successfully configure DKIM and verify ownership of your domain. For more information, see [Verifying a domain with Amazon SES](#).

**i** If your domain is registered with **Amazon Route 53**, Amazon SES will automatically update your domain's DNS server with the necessary records. This can be disabled by expanding the **Advanced DKIM settings** and unchecking **Publish DNS records to Route53** in the **Easy DKIM** selection.

### ▼ Advanced DKIM settings

### Identity type

**Easy DKIM**

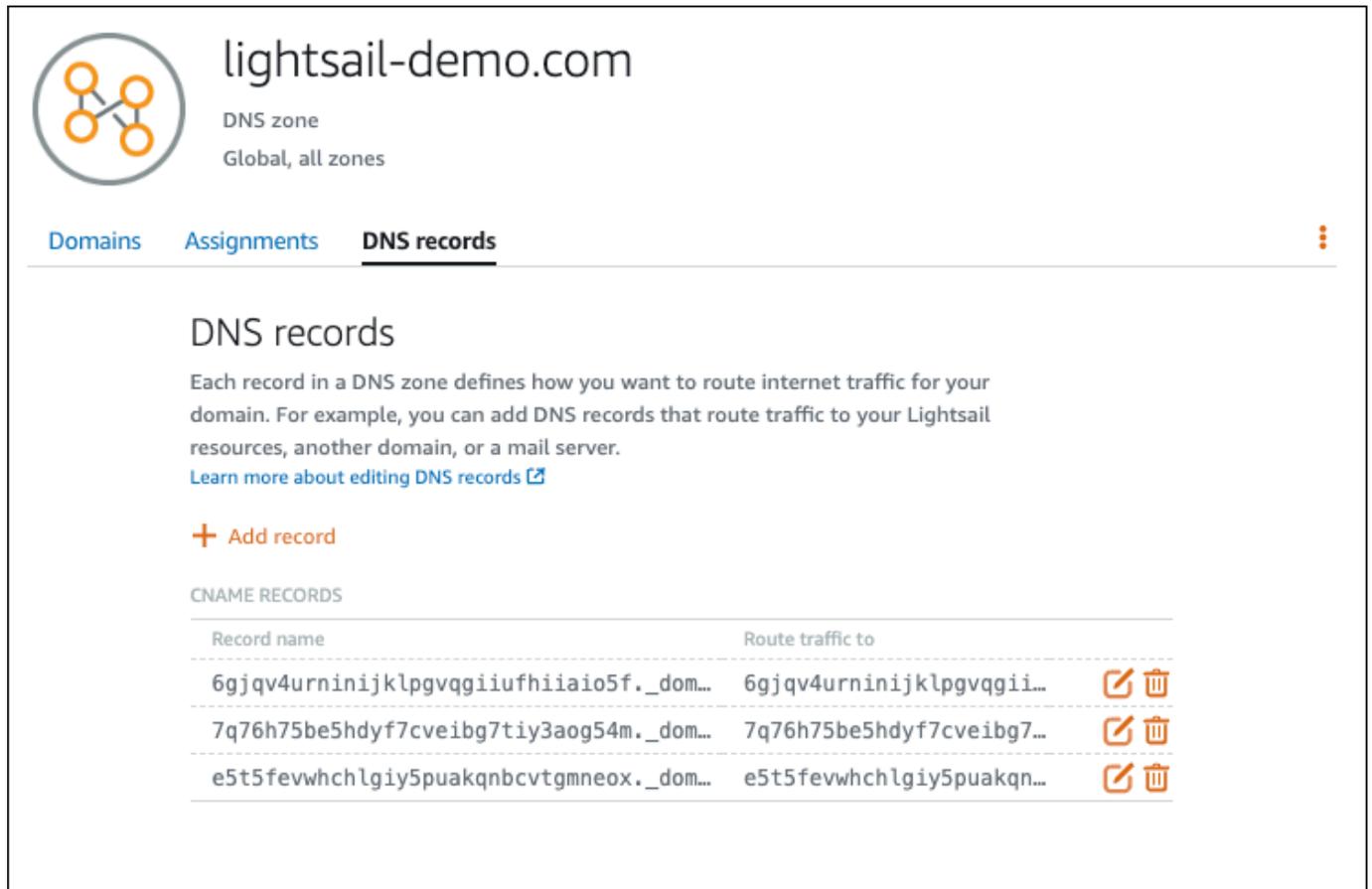
To set up Easy DKIM, you have to modify the DNS settings for your domain.

**Provide DKIM authentication token (BYODKIM)**

Configure DKIM for this domain by providing your own private key.

4. 使用 Easy DKIM 建立網域身分後，您必須透過 DKIM 身分驗證來完成驗證程序，方法是將下列產生要發佈的 CNAME 記錄複製到您網域的 DNS 提供者。這些記錄的偵測最多可能需要 72 小時。如需詳細資訊，請參閱[使用 DKIM 驗證網域身分](#)和 [Easy DKIM](#)
5. 開啟新的瀏覽器索引標籤，然後瀏覽至 [Lightsail 主控台](#)。
6. 在 Lightsail 首頁上，選擇網域和 DNS，然後選擇您網域的 DNS 區域。
7. 從 Amazon SES 主控台新增 DNS 記錄。如需有關在 Lightsail 中編輯 DNS 區域的詳細資訊，請參閱[編輯 DNS 區域](#)。

結果應如下列範例所示。



The screenshot displays the DNS records configuration for the domain 'lightsail-demo.com'. It includes a navigation menu with 'Domains', 'Assignments', and 'DNS records' (the active tab). Below the navigation, there is a section for 'DNS records' with a brief explanation and a link to learn more. An 'Add record' button is visible. A table lists three CNAME records, each with a record name and a route to traffic, along with edit and delete icons.

Record name	Route traffic to	
6gjv4urninijklpgvqgiufhiiiao5f._dom...	6gjv4urninijklpgvqgi...	 
7q76h75be5hdyf7cveibg7tiy3aog54m._dom...	7q76h75be5hdyf7cveibg7...	 
e5t5fevwhchlgiy5puakqncvtgmneox._dom...	e5t5fevwhchlgiy5puakqn...	 

#### Note

在 Subdomain (子網域) 文字方塊中輸入 @ 符號，以將網域的頂點用於 MX 記錄。此外，Amazon SES 提供的 MX 記錄值為 10 inbound-smtp.us-west-2.amazonaws.com。輸入 10 作為 Priority (優先順序) 與 inbound-smtp.us-west-2.amazonaws.com 作為 Maps to (映射到) 網域。

## 8. 在 [Amazon SES 主控台](#) 中，關閉驗證新域頁面。

幾分鐘後，Amazon SES 主控台中列出的域會標記為已驗證並已啟用可供傳送，如以下範例所示：

<input type="checkbox"/>	Domain Identities	Verification	DKIM Status	Enabled for
<input type="checkbox"/>	▶ lightsail-demo.com	verified	verified	Yes

Amazon SES 中的 SMTP 服務現在可以從域傳送電子郵件。

## 步驟 5：在 Amazon SES 中驗證電子郵件地址

身為新的 Amazon SES 客戶，您必須驗證電子郵件傳送目標的電子郵件地址。可以透過在 Amazon SES 主控台中新增電子郵件地址來完成此操作。如需詳細資訊，請參閱 Amazon SES 文件中的 [在 Amazon SES 中驗證電子郵件地址](#)。

我們建議您新增 WordPress 網站管理員的電子郵件地址。這麼做可讓 WordPress 管理員可以為他們的使用者描述檔請求密碼重設，並會收到部落格文章、網站更新和其他外掛程式訊息的電子郵件通知。

### Note

如果想要將電子郵件傳送到任何地址，而不需驗證，則必須請求將您的 Amazon SES 帳戶移出沙盒。如需詳細資訊，請參閱 Amazon SES 文件中的 [移出 Amazon SES 沙盒](#)。

若要建立電子郵件地址身分

1. 在 [Amazon SES 主控台](#) 中，從左側導覽功能表中選擇驗證身分。
2. 選擇 Create identity (建立身分)。
3. 選擇電子郵件地址。然後輸入想要驗證的電子郵件地址。
4. 選擇 Create identity (建立身分)。

對於想要驗證的每個電子郵件地址重複進行步驟 1 到 4。驗證電子郵件會傳送到您輸入的電子郵件地址。此地址會新增到驗證電子郵件身分清單，且狀態為「待驗證」。當使用者開啟電子郵件訊息並完成驗證程序時就會標示為「驗證」。

## 驗證電子郵件地址身分

1. 檢查用於創建身分的電子郵件地址的收件箱，然後查找來自 no-reply-aws@amazon .com 的電子郵件。
2. 開啟電子郵件，然後按一下連結，以完成電子郵件地址的驗證程序。完成之後，Identity status (身分狀態) 更新至 Verified (已驗證)。

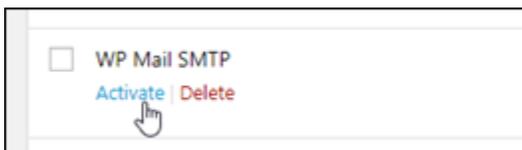
<input type="checkbox"/>	Email Address Identities	Verification Status
<input type="checkbox"/>	▶ user1@lightsail-demo.com	pending verification (resend)
<input type="checkbox"/>	▶ user2@lightsail-demo.com	verified
<input type="checkbox"/>	▶ user3@lightsail-demo.com	verified

## 步驟 6：在您的 WordPress 實例上配置 WP 郵件 SMTP 插件

最後一步是在您的 WordPress 實例上配置 WP 郵件 SMTP 插件。在 Amazon SES 主控台中使用此指南的前面部分中建立的 SMTP 憑證。

若要設定 WordPress 執行個體上的 WP 郵件 SMTP 外掛程式

1. 以系統管理員身分登入您 WordPress 網站的儀表板。
2. 從左側導覽功能表中，選擇 Plugins (外掛程式)，然後選擇 Installed Plugins (安裝的外掛程式)。
3. 向下捲動到 WP 郵件 SMTP 外掛程式，然後選擇 Activate (啟用)。如果有新版本的外掛程式，務必先進行更新，才能繼續進行下一個步驟。



4. 啟用 WP 郵件 SMTP 外掛程式後，選擇 Settings (設定)。您可能需要向下捲動來尋找該外掛程式。



5. 在 From Email Address (透過電子郵件地址) 文字方塊中，輸入您希望電子郵件發送者的電子郵件地址。必須使用此指南前面部分的步驟，在 Amazon SES 中確認您輸入的電子郵件地址。

- 選擇 Force From Email (強制透過電子郵件) 來強制使用您在 From Email Address (透過電子郵件地址) 文字方塊中輸入的電子郵件地址，並忽略其他外掛程式設定的「透過電子郵件地址」值。
- 在「寄件者名稱」文字方塊中，輸入您想要電子郵件來源的名稱，或保留原樣以使用部 WordPress 部落格名稱。
- 選擇 Force From Name (強制透過名稱) 來強制使用您在 From Name (透過名稱) 文字方塊中輸入的名稱。選擇此選項會忽略其他外掛程式所設定的「寄件者名稱」值，並強制 WordPress 使用您在「寄件者名稱」文字方塊中輸入的名稱。
- 在頁面的郵件程式區段，選擇 Other SMTP (其他 SMTP)。
- 選擇 Set the return-path to match the From Email (將傳回路徑設定為比對「透過電子郵件」) 來將未交付回條傳送到您在 From Email Address (透過電子郵件地址) 文字方塊中輸入的電子郵件地址。

**From Email**

*The email address which emails are sent from.  
If you using an email provider (Gmail, Yahoo, Outlook.com, etc) this should be your email address for that account.  
Please note that other plugins can change this, to prevent this use the setting below.*

Force From Email

*If checked, the From Email setting above will be used for all emails, ignoring values set by other plugins.*

**From Name**

*The name which emails are sent from.*

Force From Name

*If checked, the From Name setting above will be used for all emails, ignoring values set by other plugins.*

**Mailer**

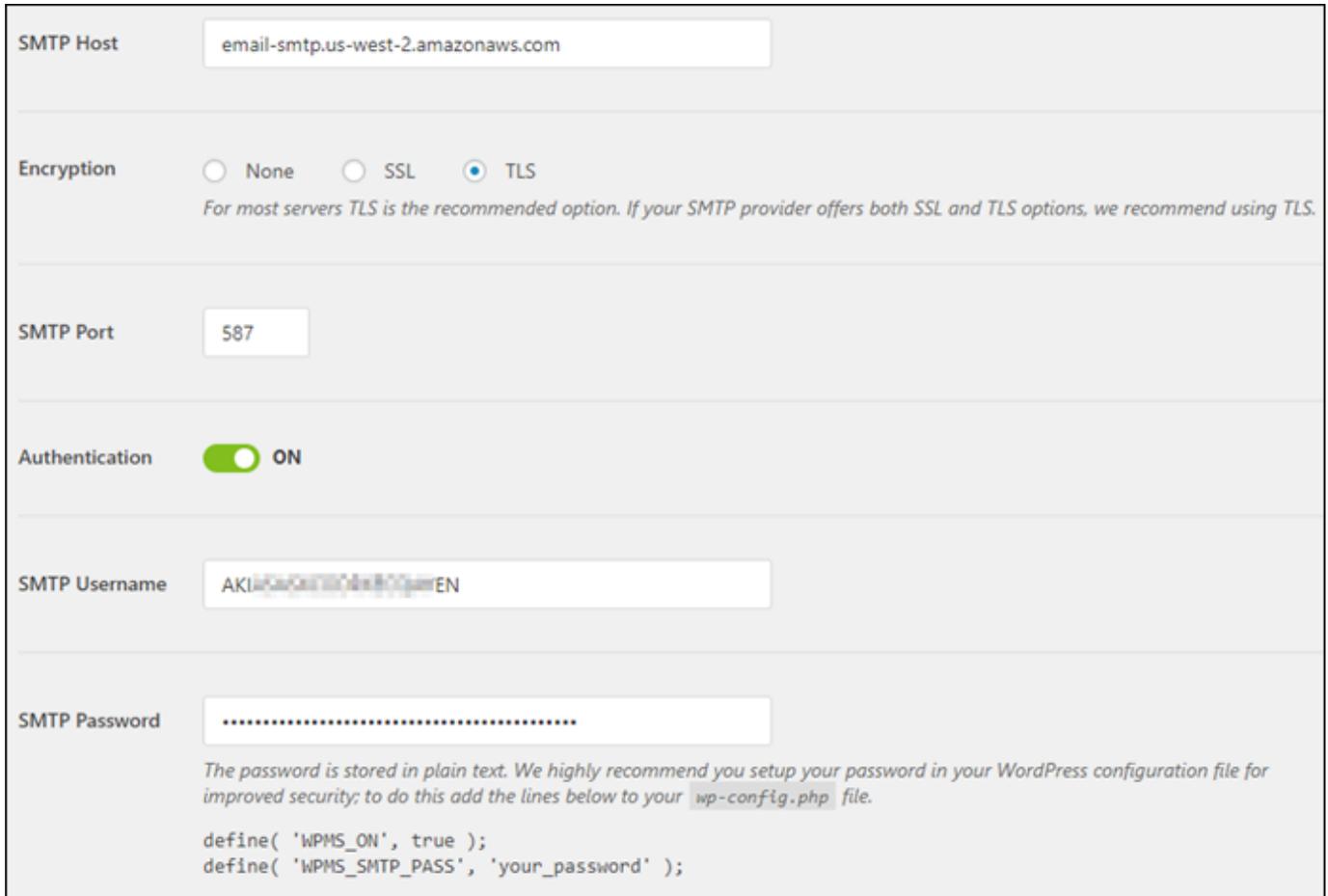
Default (none)  Gmail  Mailgun  SendGrid  Other SMTP

**Return Path**  Set the return-path to match the From Email

*Return Path indicates where non-delivery receipts - or bounce messages - are to be sent.  
If unchecked bounce messages may be lost.*

- 在 SMTP 主機文字方塊中，輸入您在此指南的前面部分中從 Amazon SES 主控台的 SMTP 設定頁面取得的 SMTP 伺服器名稱。

- 選擇該頁面的加密區段中的 TLS，以指定 Amazon SES 中的 SMTP 服務使用 TLS 加密。
- 在 SMTP Port (SMTP 連接埠) 文字方塊中，保留預設值 587。
- 將驗證切換為開啟，然後輸入在此指南前面部分中透過 Amazon SES 主控台取得的 SMTP 使用者名稱和密碼。



SMTP Host: email-smtp.us-west-2.amazonaws.com

Encryption:  None  SSL  TLS  
*For most servers TLS is the recommended option. If your SMTP provider offers both SSL and TLS options, we recommend using TLS.*

SMTP Port: 587

Authentication:  ON

SMTP Username: AKIA...@amazon.com

SMTP Password: .....

*The password is stored in plain text. We highly recommend you setup your password in your WordPress configuration file for improved security; to do this add the lines below to your `wp-config.php` file.*

```
define( 'WPMS_ON', true );  
define( 'WPMS_SMTP_PASS', 'your_password' );
```

- 選擇 Save Settings (儲存設定)。出現設定已成功儲存的確認提示。
- 選擇 Email Test (電子郵件測試) 索引標籤。

在接下來的步驟中，您傳送測試電子郵件，以確認電子郵件服務是否運作。

- 在 Send To (收件者) 文字方塊中輸入電子郵件地址，然後選擇 Send Email (傳送電子郵件)。必須使用此指南前面部分的步驟，在 Amazon SES 中確認您輸入的電子郵件地址。

您應該會看到兩種可能的結果。

- 如果您看到成功確認，則表示您的 WordPress 網站已啟用電子郵件功能。確認以下測試電子郵件送達指定的信箱：

Congrats, test email was sent successfully!

Thank you for trying out WP Mail SMTP. We're on a mission to make sure that your emails actually get delivered.

If you find this free plugin useful, please consider giving our sister plugin a try!

您現在可以選擇丟失密碼？在您的 WordPress 網站儀表板的登錄頁面上。如果 Amazon SES 確認 WordPress 使用者設定檔上的電子郵件地址，則會透過電子郵件傳送新密碼給您。

- 如果看到故障通知，請確認您在 WP Mail SMTP 外掛程式中輸入的 SMTP 設定與在 Amazon SES 帳戶中 SMTP 服務的 SMTP 設定相符。同時確認您使用的是在 Amazon SES 中驗證的電子郵件地址。

## 使用 HTTPS 保護您 WordPress 的 Lightsail

為您的 WordPress 網站啟用超文本傳輸協議安全 (HTTPS) 可確保訪問者您的網站是安全的，它正在發送和接收加密數據。非安全網站的地址開頭為 http，例如 <http://example.com>，而安全網站的地址開頭為 https，例如 <https://example.com>。即使您的網站主要為參考資訊，仍建議您啟用 HTTPS。這是因為若未啟用 HTTPS，大多數網頁瀏覽器都會通知網站訪客您的網站不安全，且您的網站在搜尋引擎結果中的排名也會較低。

### Tip

Lightsail 提供引導式工作流程，可自動執行個體上 SSL/TLS 讓我們加密憑證的安裝和設定。WordPress 我們強烈建議您使用工作流程，而不要遵循本教學課程中的手動步驟。如需詳細資訊，請參閱[啟動和設定 WordPress 執行個體](#)。

本指南說明如何使用 Bitnami HTTPS 設定工具 (bncert) 在 Amazon Lightsail 上經過 Bitnami 認證的 WordPress 執行個體上啟用 HTTPS。其可讓您在提出請求時，僅為指定的網域和子網域請求憑證。或者，您可以使用 Certbot 工具，其可讓您為網域請求憑證，以及為子網域請求萬用字元憑證。萬用字元憑證適用於網域的任何子網域，如果您不知道將使用哪些子網域將流量引導至執行個體，這將有所助益。但是，Certbot 不會像 bncert 工具一樣自動更新您的憑證。如果您使用 Certbot，就必須每 90 天手動更新您的憑證。如需有關使用 Certbot 啟用 HTTPS 的詳細資訊，請參閱[教學課程：使用執行個體加密 SSL 憑證](#)。WordPress

內容

- [步驟 1：了解程序](#)
- [步驟 2：完成事前準備](#)
- [步驟 3：連接到您的執行個體](#)
- [步驟 4：確認您的執行個體已安裝 bncert 工具](#)
- [步驟 5：在您的 WordPress 執行個體上啟用 HTTPS](#)
- [步驟 6：測試您的網站是否使用 HTTPS](#)

## 步驟 1：了解程序

### Note

在本節中，您將了解該程序的高階概觀。執行此程序的特定步驟包含於本指南的後續步驟中。

若要為您的 WordPress 網站啟用 HTTPS，請使用 SSH 連線至您的 Lightsail 執行個體，然後使用此 bncert 工具向 [讓我們加密憑證授權單位](#) 要求 SSL/TLS 憑證。在您請求憑證時，可以指定網站的主要網域 (example.com) 和替代網域 (www.example.com、blog.example.com 等) (如果有)。Let's Encrypt 會驗證您是否擁有網域，方法是要求您在網域的 DNS 中建立 TXT 記錄，或是驗證這些網域是否已將流量引導至您從中提出請求之執行個體的公有 IP 地址。

驗證您的憑證後，您可以設定 WordPress 網站自動將訪客從 HTTP 重新導向至 HTTPS (http://example.com 重新導向至 https://example.com)，以便強制訪客使用加密連線。您也可以設定網站以將 www 子網域自動重新引導至網域的頂點 (https://www.example.com 會重新引導至 https://example.com)，或反之亦然 (https://example.com 會重新引導至 https://www.example.com)。這些重新引導也是使用 bncert 工具來設定。

Let's Encrypt 會要求您每 90 天更新一次憑證，以維護網站上的 HTTPS。bncert 工具會自動為您更新憑證，讓您可以有更多時間專注於網站。

### bncert 工具的限制

bncert 工具具有下列限制：

- 建立時並未預先安裝在所有「由 Bitnami 認證」WordPress 執行個體上。WordPress 一段時間後在 Lightsail 上建立的執行個體將需要您手動安裝 bncert 工具。本指南的步驟 4 會說明如何確認是否已在您的執行個體上安裝該工具，以及未安裝時，如何安裝它。

- 當您提出請求時，只能請求指定的域和子域的憑證。這與 Certbot 工具不同，該工具可讓您為網域請求憑證，以及為子網域請求萬用字元憑證。萬用字元憑證適用於網域的任何子網域，如果您不知道將使用哪些子網域將流量引導至執行個體，這將有所助益。但是，Certbot 不會像 bncert 工具一樣自動更新您的憑證。如果您使用 Certbot，就必須每 90 天手動更新您的憑證。如需有關使用 Certbot 啟用 HTTPS 的詳細資訊，請參閱教學課程：[在 Amazon Lightsail 中使用 WordPress 執行個體加密 SSL 憑證](#)。

## 步驟 2：完成事前準備

請先完成事前準備 (若尚未完成)：

- 在 Lightsail 中建立 WordPress 執行個體，然後在執行個體上設定網站。如需詳細資訊，請參閱在 Amazon Lightsail 中[開始使用以 Linux /Unix 為基礎](#)的執行個體。
- 將靜態 IP 連接至執行個體。如果您停止和啟動執行個體，執行個體的公有 IP 地址將會改變。停止並啟動執行個體時，靜態 IP 不會變更。如需詳細資訊，請參閱[在 Amazon Lightsail 中建立靜態 IP 並將其連接至執行個體](#)。
- 設定完執行個 WordPress 體後，建立執行個體的快照，或啟用自動快照。快照可用作備份，您可從中建立另一個執行個體，以防原始執行個體發生問題。如需詳細資訊，請參閱[建立 Linux 或 Unix 執行個體的快照或在 Amazon Lightsail 中啟用或停用執行個體或磁碟的自動快照](#)。
- 將 DNS 記錄新增至您網域的 DNS，以便將網域頂點的流量 (example.com) 及其 www 子網域 (www.example.com) 的流量導向至 Lightsail 中 WordPress 執行個體的公用 IP 位址。您可以在網域目前的 DNS 託管提供者處完成這些動作。或者，如果您將網域 DNS 的管理權限轉移至 Lightsail，您可以使用 Lightsail 中的 DNS 區域來完成這些動作。若要進一步了解，請參閱[DNS](#)。

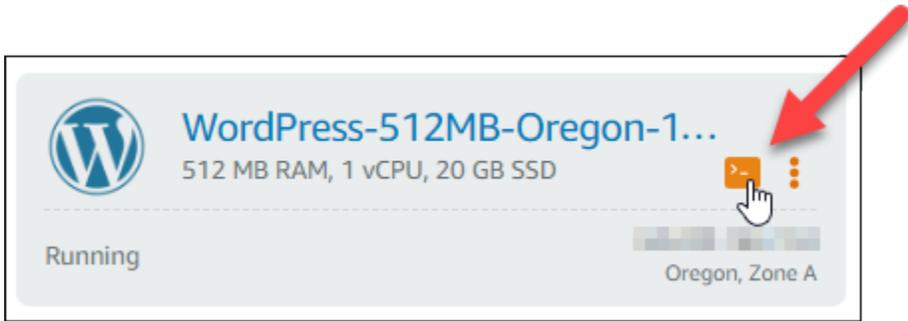
### Important

將 DNS 記錄新增至您要與網站搭配使用的所有 WordPress 網域的 DNS。所有這些域都應該將流量路由到您 WordPress 網站的公共 IP 地址。此工 bncert 具只會針對目前將流量導向至執行個體之公用 IP 位址的網域核發憑 WordPress 證。

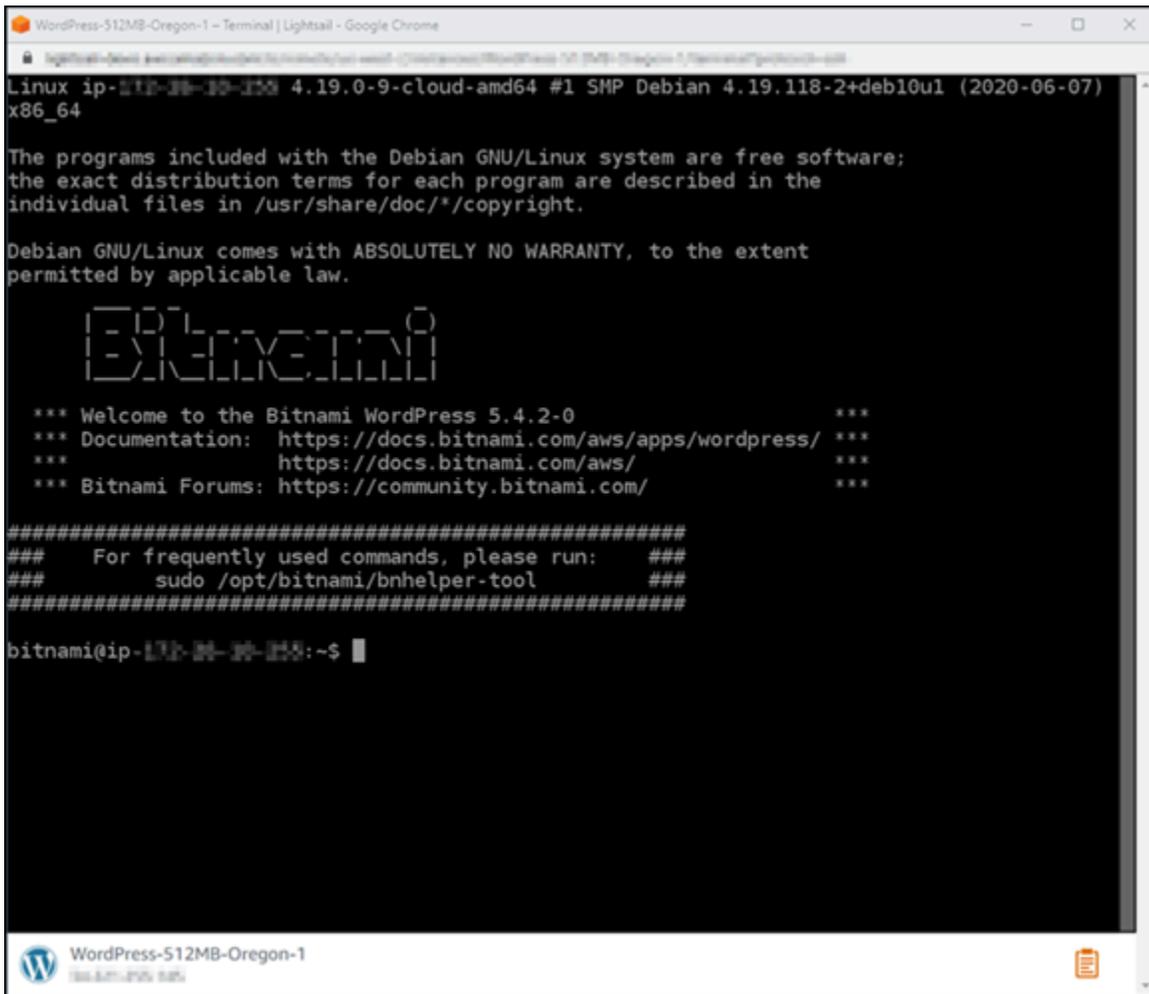
## 步驟 3：連接到您的執行個體

完成下列步驟，即可使用 Lightsail 主控台中以瀏覽器為基礎的 SSH 用戶端連線至執行個體。

- 登入主 [Lightsail 台](#)。
- 在 Lightsail 首頁上，選擇 WordPress 執行個體的安全殼層快速連線圖示。



瀏覽器型 SSH 用戶端終端機視窗將會開啟。如果您看到 Bitnami 標誌 (如以下範例所示)，即表示已透過 SSH 成功連接到執行個體。



## 步驟 4：確認您的執行個體已安裝 bncert 工具

請完成以下步驟，以確保 Bitnami HTTPS 組態工具 (bncert) 已安裝在您的執行個體上。建立時並未預先安裝在所有「由 Bitnami 認證」WordPress 執行個體上。WordPress 一段時間後在 Lightsail 上建立的執行個體將需要您手動安裝 bncert 工具。此程序包含安裝工具的步驟 (若尚未安裝)。

1. 輸入下列命令以執行 bncert 工具。

```
sudo /opt/bitnami/bncert-tool
```

- 如果您在回應中看到 `command not found`，如下列範例所示，則表示 bncert 工具尚未安裝在您的執行個體上。繼續此程序的下一個步驟以將 bncert 工具安裝在您的執行個體上。

### Important

此 bncert 工具只能在已通過 Bitnami 認證的 WordPress 執行個體上使用。或者，您也可以使用 Certbot 工具在執行個體上啟用 HTTPS。WordPress 如需詳細資訊，請參閱 [教學課程：搭配執行個體使用加密 SSL 憑 WordPress 證](#)。

```
bitnami@ip-172-28-13-141:~$ sudo /opt/bitnami/bncert-tool
sudo: /opt/bitnami/bncert-tool: command not found
bitnami@ip-172-28-13-141:~$
```

- 如果您在回應中看到 `Welcome to the Bitnami HTTPS configuration tool`，如下列範例所示，則表示 bncert 工具已安裝在您的執行個體上。請繼續閱讀本指南的「[步驟 5：在您的 WordPress 執行個體啟用 HTTPS](#)」一節。

```
bitnami@ip-172-28-13-141:~$ sudo /opt/bitnami/bncert-tool
-----
Welcome to the Bitnami HTTPS Configuration tool.
-----
Domains

Please provide a valid space-separated list of domains for which you wish to
configure your web server.

Domain list []:
```

2. 輸入以下命令以下載 bncert 執行檔案至您的執行個體。

```
wget -O bncert-linux-x64.run https://downloads.bitnami.com/files/bncert/latest/bncert-linux-x64.run
```

3. 輸入以下命令以便為執行個體上的 bncert 執行檔案建立目錄。

```
sudo mkdir /opt/bitnami/bncert
```

4. 輸入以下命令以將已下載的 bncert 執行檔案移至所建立的新目錄。

```
sudo mv bncert-linux-x64.run /opt/bitnami/bncert/
```

5. 輸入以下命令以讓 bncert 執行可作為程式執行的檔案。

```
sudo chmod +x /opt/bitnami/bncert/bncert-linux-x64.run
```

6. 輸入以下命令以在您輸入 `sudo /opt/bitnami/bncert-tool` 命令時建立執行 bncert 工具的符號連結。

```
sudo ln -s /opt/bitnami/bncert/bncert-linux-x64.run /opt/bitnami/bncert-tool
```

您現已在執行個體上安裝 bncert 工具。請繼續閱讀本指南的「[步驟 5：在您的 WordPress 執行個體啟用 HTTPS](#)」一節。

## 步驟 5：在您的 WordPress 執行個體上啟用 HTTPS

確認 WordPress 執行個體上已安裝 bncert 工具之後，請完成下列程序，以在執行個體上啟用 HTTPS。

1. 輸入下列命令以執行 bncert 工具。

```
sudo /opt/bitnami/bncert-tool
```

這時應該會出現類似以下範例的訊息。

```
bitnami@ip-172-31-1-81:~$ sudo /opt/bitnami/bncert-tool
-----
Welcome to the Bitnami HTTPS Configuration tool.
-----
Domains
Please provide a valid space-separated list of domains for which you wish to
configure your web server.
Domain list []: █
```

如果 bncert 工具已安裝至您的執行個體上一段時間，則您可能會看到說明該工具已有可用更新版本的訊息。如下列範例所示，選擇下載該工具，然後輸入 `sudo /opt/bitnami/bncert-tool` 命令以再次執行 bncert 工具。

```
bitnami@ip-172-31-11-55:~$ sudo /opt/bitnami/bncert-tool
An updated version is available. Would you like to download it? You would need to run it
manually later. [Y/n]: Y█
```

2. 輸入主要網域名稱和替代網域名稱，並以空格分隔，如以下範例所示。

如果您的網域未設為將流量路由至執行個體的公有 IP 地址，則 bncert 工具會要求您進行該設定，然後再繼續操作。您的網域必須將流量路由至執行個體的公有 IP 地址，而您需從該地址使用 bncert 工具來在執行個體上啟用 HTTPS。此舉措會確認您擁有該網域，並以此作為憑證的驗證。

```
-----
Welcome to the Bitnami HTTPS Configuration tool.
-----
Domains
Please provide a valid space-separated list of domains for which you wish to
configure your web server.
Domain list []: example.com www.example.com█
```

3. bncert 工具會詢問您要如何設定網站的重新引導。可用的選項如下：
  - Enable HTTP to HTTPS redirection (啟用 HTTP 至 HTTPS 重新引導) - 指定將瀏覽至網站 HTTP 版本 (即 `http://example.com`) 的使用者自動重新引導至 HTTPS 版本 (即 `https://example.com`)。由於此選項會強制所有訪客使用加密的連線，建議啟用此選項。輸入 Y，並按 Enter 以啟用。
  - Enable non-www to www redirection (啟用非 www 至 www 重新引導) - 指定將瀏覽至網域 (即 `https://example.com`) 頂點的使用者自動重新引導至您網域的 www 子網域 (即 `https://www.example.com`)。建議啟用此選項。不過，如果您已在搜索引擎工具 (如 Google 的網站管理員工具) 中將網域的頂點指定為您偏好的網站地址，或者如果您的頂點直接指向 IP，且 www

子網域透過 CNAME 記錄參考您的頂點，則您可能需要停用此選項並啟用替代選項 (啟用 `www` 至非 `www` 重新引導)。輸入 `Y`，並按 `Enter` 以啟用。

- Enable `www` to non-`www` redirection (啟用 `www` 至非 `www` 重新引導) - 指定將瀏覽至您網域 `www` 子網域 (即 `https://www.example.com`) 的使用者自動重新引導至網域的頂點 (即 `https://example.com`)。如果您已啟用非 `www` 重新引導至 `www`，我們建議您停用此選項。輸入 `N`，並按 `Enter` (確認) 以停用。

您的選取內容應看起來與下列範例類似。

```
Enable/disable redirections

Please select the redirections you wish to enable or disable on your Bitnami
installation.

Enable HTTP to HTTPS redirection [Y/n]: Y

Enable non-www to www redirection [Y/n]: Y

Enable www to non-www redirection [y/N]: N
```

4. 系統會列出即將進行的變更。輸入 `Y`，並按 `Enter` (確認) 以確認並繼續。

```
Changes to perform

The following changes will be performed to your Bitnami installation:

1. Stop web server
2. Configure web server to use a free Let's Encrypt certificate for the domains:
example.com www.example.com
3. Configure a cron job to automatically renew the certificate each month
4. Configure web server name to: example.com
5. Enable HTTP to HTTPS redirection (example: redirect http://example.com to
https://example.com)
6. Enable non-www to www redirection (example: redirect example.com to
www.example.com)
7. Start web server once all changes have been performed

Do you agree to these changes? [Y/n]: Y
```

5. 輸入您的電子郵件地址，以與您的 Let's Encrypt 憑證相關聯，然後按 `Enter`。

```
Create a free HTTPS certificate with Let's Encrypt

Please provide a valid e-mail address for which to associate your Let's Encrypt
certificate.

Domain list: example.com www.example.com

Server name: example.com

E-mail address []: █
```

6. 檢閱 Let's Encrypt 訂閱者協議。輸入 Y，並按 Enter (確認) 以接受該協議並繼續。

```
The Let's Encrypt Subscriber Agreement can be found at:
https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf

Do you agree to the Let's Encrypt Subscriber Agreement? [Y/n]: █
```

執行這些動作是為了在執行個體上啟用 HTTPS，包括請求憑證和設定您指定的重新引導。

```
Performing changes to your installation

The Bitnami HTTPS Configuration Tool will perform any necessary actions to your
Bitnami installation. This may take some time, please be patient.

█
```

系統已成功核發並驗證您的憑證，如果您看到類似以下範例的訊息，則表示已成功在執行個體上設定重新引導。

```
Success

The Bitnami HTTPS Configuration Tool succeeded in modifying your installation.

The configuration report is shown below.

Backup files:
* /opt/bitnami/apache2/conf/httpd.conf.back.202005290035
* /opt/bitnami/apache2/conf/bitnami/bitnami-apps-prefix.conf.back.202005290035
* /opt/bitnami/apache2/conf/bitnami/bitnami.conf.back.202005290035

Find more details in the log file:

/tmp/bncert-202005290035.log

If you find any issues, please check Bitnami Support forums at:

https://community.bitnami.com

Press [Enter] to continue:█
```

bncert 工具會在憑證過期前每 80 天執行自動續約一次。如果您要搭配執行個體使用其他網域和子網域，且要為這些網域啟用 HTTPS，請重複上述步驟。

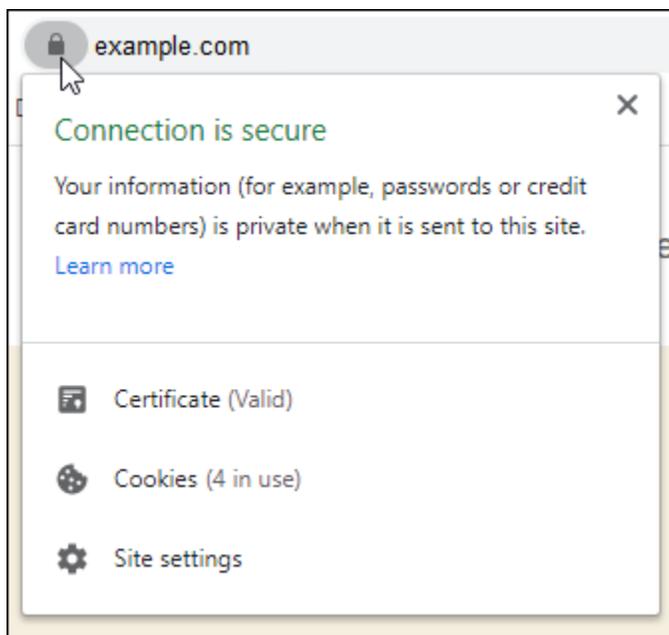
您現在已完成在 WordPress 執行個體上啟用 HTTPS。繼續前往本指南的[步驟 6：測試您的網站是否使用 HTTPS](#) 章節。

## 步驟 6：測試您的網站是否使用 HTTPS

在 WordPress 執行個體上啟用 HTTPS 之後，您應該瀏覽至使用 bncert 工具時指定的所有網域，以確認您的網站使用 HTTPS。在您前往每個網域時，應會看到其使用安全連線，如以下範例所示。

### Note

您可能必須重新整理，並清除瀏覽器的快取才能查看變更。



依據您在執行 bncert 工具時選取的選項而定，您可能還注意到非 www 地址會重新引導至您網域的 www 子網域，反之亦然。

## 將您的 WordPress 部落格移 Lightsail

想要更改您的 WordPress 託管服務提供商？Amazon Lightsail 是在 AWS 上運行 WordPress 網站的最簡單方法。

您可以選擇我們的定價計劃之一（USD每月 \$5 起），並完全控制您的 WordPress 安裝，包括插件，主題等。

建立 Lightsail WordPress 實體只需要幾分鐘的時間。請依照此教學課程備份您現有的 WordPress 部落格，並將其匯入 Lightsail 中執行的新執行個體。

下列為此程序的快速概觀：



繼續閱讀以開始使用。

## 必要條件

開始之前，您必須準備好以下事項：

1. 您將需要一個 AWS 帳戶。[註冊 AWS](#)，或者 AWS 如果您已經有帳戶，請[登入](#)。
2. 請確定您的帳戶已設定為使用 Lightsail。如果您建立帳戶已有一段時間，或者您尚未提供信用卡，您可能需要先登入 AWS Management Console 並更新您的帳戶。

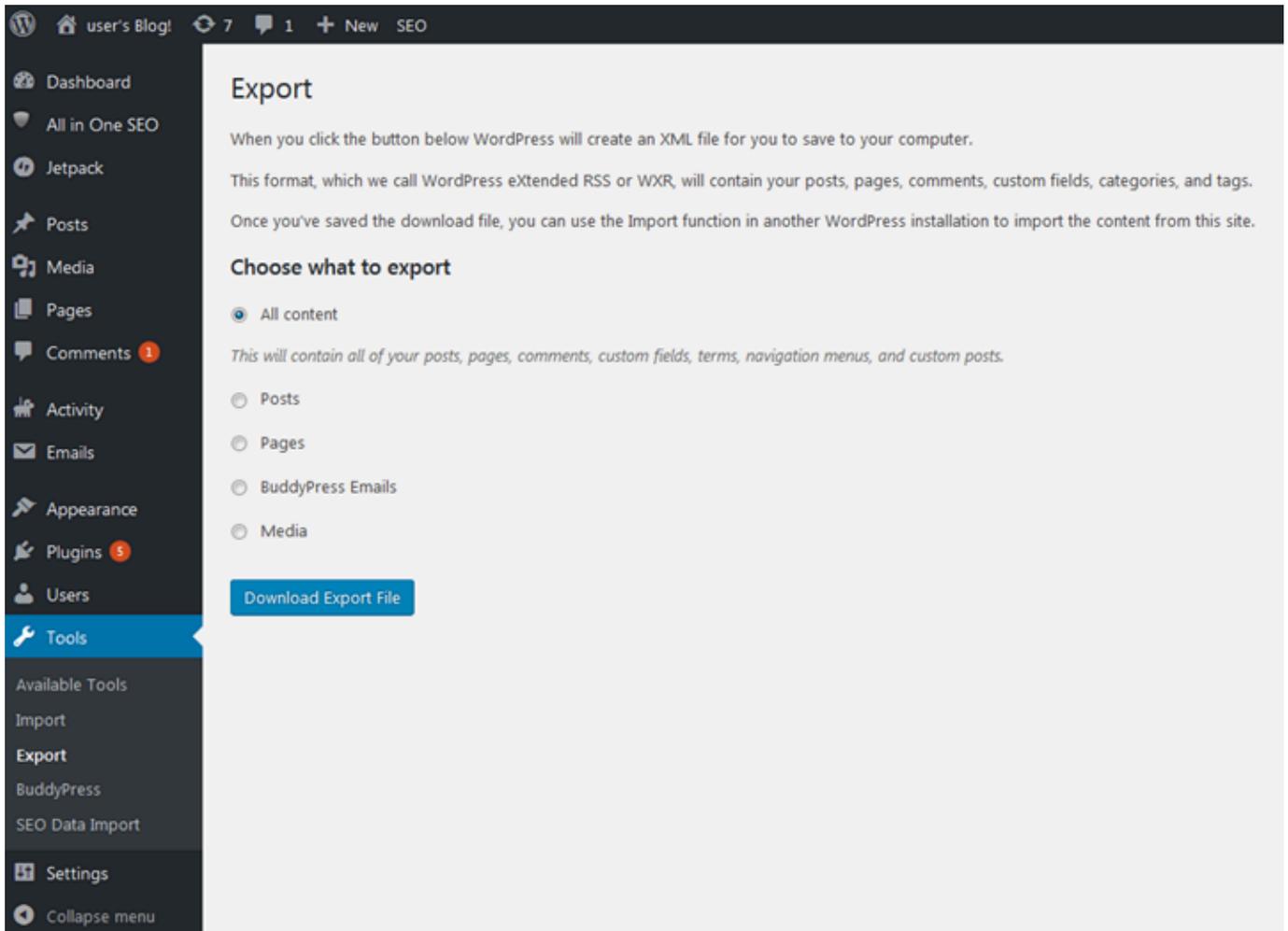
## 步驟 1：備份您現有的 WordPress 部落格

您可以用 WordPress 來備份現有的部落格。您只需要登入管理控制台並管理部落格即可。WordPress

1. 導覽至您的部落格，然後選擇 Manage (管理)。

如果未顯示 Manage (管理) 橫幅，您可以透過瀏覽至 `http://<PublicIP>/wp-login.php` 前往登入頁面。將 `<PublicIP>` 取代為您執行個體的公有 IP 地址。

2. 輸入您的使用者名稱和密碼以登入 WordPress 管理控制台。
3. 在 WordPress 儀表板上，選擇 [工具]，然後選擇 [匯出]。
4. 在「匯出」頁面上，選擇「所有內容」，將所有內容匯出為 XML 檔案。



5. 選擇「下載匯出檔案」，將舊部落格下載為XML檔案。

將XML檔案儲存在容易找到的位置。您將會在步驟 4 用到這些檔案。

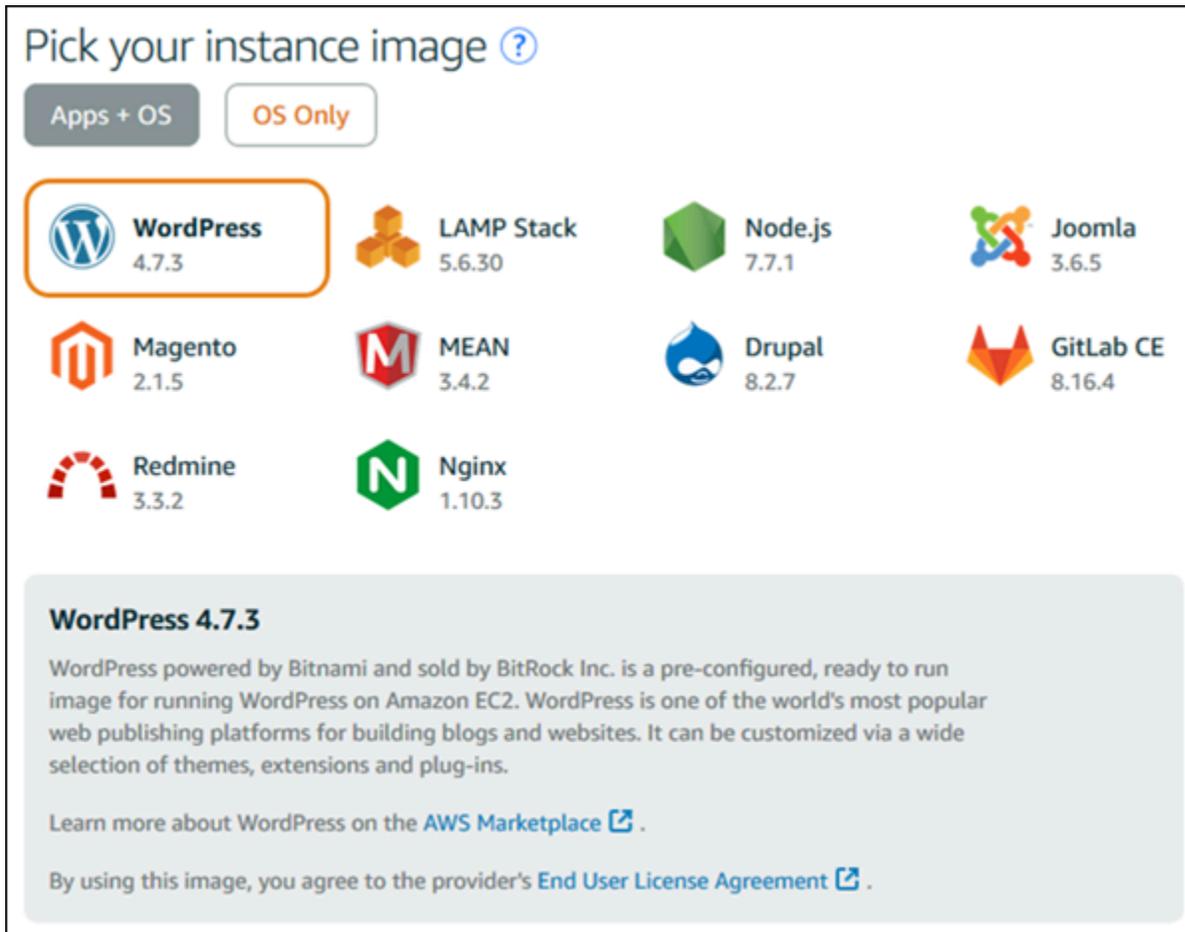
## 步驟 2：在 Lightsail 中建立新的 WordPress 執行個體

您可以在幾分鐘內在 Lightsail 中建立新的 WordPress 執行個體。方法如下：

1. 前往 [Lightsail](#) 並登入。
2. 選擇 建立執行個體。
3. 選取您 AWS 區域 要建立部落格的位置。

可以選擇預設的可用區域，或在選取 AWS 區域之後變更它。

4. 選取WordPress。



Pick your instance image [?](#)

Apps + OS OS Only

 <b>WordPress</b> 4.7.3	 <b>LAMP Stack</b> 5.6.30	 <b>Node.js</b> 7.7.1	 <b>Joomla</b> 3.6.5
 <b>Magento</b> 2.1.5	 <b>MEAN</b> 3.4.2	 <b>Drupal</b> 8.2.7	 <b>GitLab CE</b> 8.16.4
 <b>Redmine</b> 3.3.2	 <b>Nginx</b> 1.10.3		

**WordPress 4.7.3**

WordPress powered by Bitnami and sold by BitRock Inc. is a pre-configured, ready to run image for running WordPress on Amazon EC2. WordPress is one of the world's most popular web publishing platforms for building blogs and websites. It can be customized via a wide selection of themes, extensions and plug-ins.

Learn more about WordPress on the [AWS Marketplace](#) .

By using this image, you agree to the provider's [End User License Agreement](#) .

5. 選擇您的執行個體計劃 (或搭售套件)。

如有需要，您可以稍後升級您的 Lightsail 方案。[如需詳細資訊，請參閱在 Lightsail 中從快照建立實體。](#)

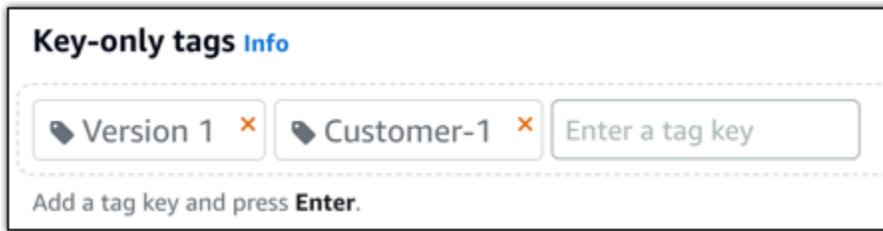
6. 輸入您執行個體的名稱。

資源名稱：

- 每個 Lightsail 帳戶 AWS 區域 中的每個項目都必須是唯一的。
- 必須包含 2 至 255 個字元。
- 必須以英數字元開頭和結尾。
- 可以包含英數字元、句號、破折號和底線。

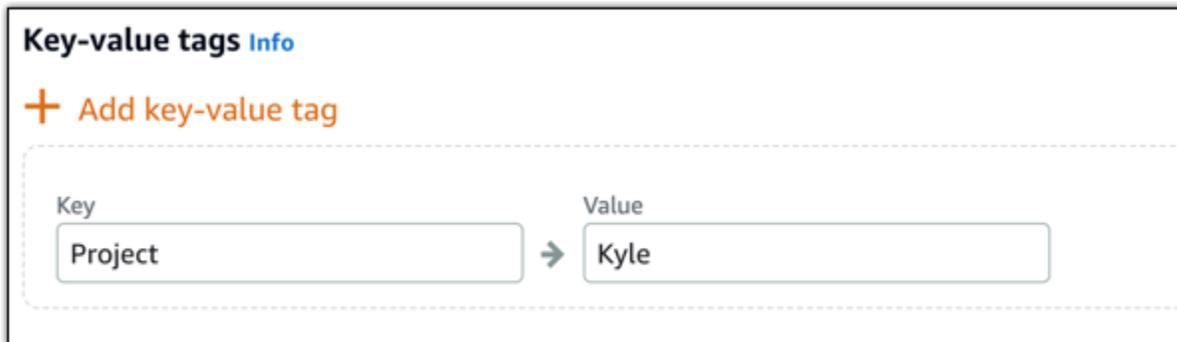
7. 選擇下列其中一個選項以新增標籤至您的執行個體：

- Add key-only tags (新增僅索引鍵標籤) 或 Edit key-only tags (編輯僅索引鍵標籤) (若標籤已新增)。在標籤索引鍵文字方塊中輸入新的標籤，接著按 Enter (輸入)。輸入標籤以新增之後，請選擇 Save (儲存)，如果不要新增則選擇 Cancel (取消)。



- Create a key-value tag (建立索引鍵值標籤)，接著將索引鍵輸入 Key (索引鍵) 文字方塊，將值輸入 Value (值) 文字方塊。完成輸入標籤後，請選擇 Save (儲存)，如果不要新增則選擇 Cancel (取消)。

鍵值標籤在儲存前一次只能新增一個。若要新增超過一個索引鍵值標籤，請重複之前的步驟。



#### Note

如需有關僅索引鍵和索引鍵值標籤的詳細資訊，請參閱[標籤](#)。

## 8. 選擇 建立執行個體。

### 步驟 3：登入您的新 Lightsail WordPress 格

現在您在 Lightsail 中有了新的部落格，您需要存取 WordPress 儀表板以匯入舊部落格資料。登入 WordPress 網站管理儀表板的預設密碼會儲存在執行個體上。請完成以下步驟以取得密碼。

取得 WordPress 管理員的預設密碼

1. 開啟執行個體的執行 WordPress 個體管理頁面。
2. 在 WordPress 面板上，選擇「擷取預設密碼」。這會展開頁面底部的存取預設密碼。

**WordPress-1** Info

1 GB RAM, 2 vCPUs, 40 GB SSD

**WordPress**  
6.3.2-12

**AWS Region**  
Virginia, Zone A  
(us-east-1a)

**Public IPv4 address**  
3.24.104.11

**Public IPv6**  
2600:1f18:1c00:800d:5e:300:51d:b:814

**Default WordPress admin user name**  
user

**Default WordPress admin password**  
Retrieve default password

**Instance status**  
Running

[Access WordPress Admin](#)

[Delete](#) [Reboot](#) [Stop](#)

- 選擇 [啟動] CloudShell。這將在頁面底部打開一個面板。
- 選擇「複製」，然後將內容貼到 CloudShell 視窗中。您可以將光標放在 CloudShell 提示符處並按 Ctrl+V，也可以右鍵單擊以打開菜單，然後選擇粘貼。
- 記下 CloudShell 視窗中顯示的密碼。您需要此功能才能登入 WordPress 網站的管理儀表板。

```
[cloudshell-user@ip-10-114-41-117 ~]$ AWS_REGION=us-east-1 ~/lightsail_connect WordPress-1 cat bitnami_application_password
JKzh8wB5FAR!
```

現在，您已經擁有 WordPress 網站管理儀表板的密碼，您可以登錄。在管理儀表板中，您可以變更您的使用者密碼、安裝外掛程式、變更網站的主題等。

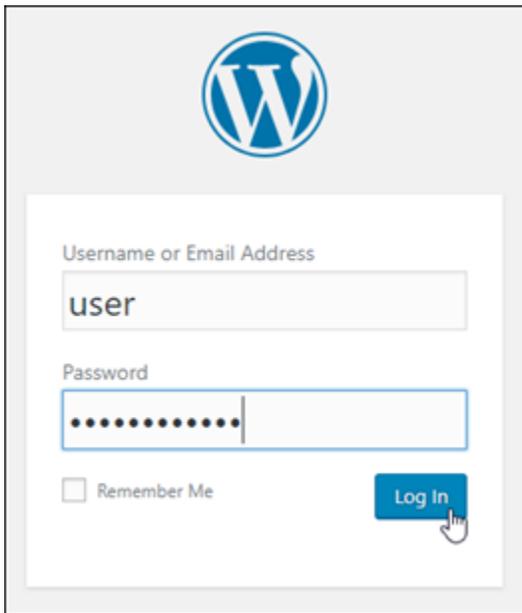
完成下列步驟以登入您 WordPress 網站的管理儀表板。

若要登入管理儀表板

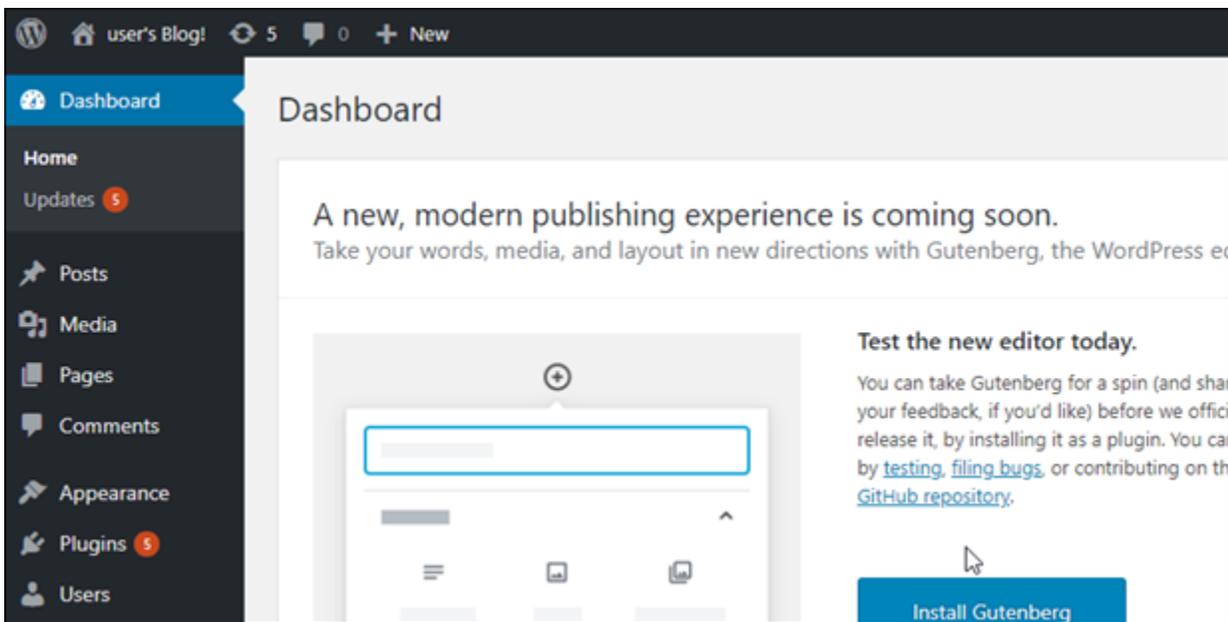
- 開啟執行個體的執行 WordPress 個體管理頁面。
- 在 WordPress 面板上，選擇 [存取 WordPress 管理員]。
- 在 [存取您的 WordPress 管理儀表板] 面板的 [使用公用 IP 位址] 下方，選擇具有此格式的連結：

`http://public-ipv4-address. /WP-管理員`

- 針對使用者名稱或電子郵件地址，輸入 **user**
- 在「密碼」中，輸入在上一個步驟中取得的密碼。
- 選擇 Log in (登入)。



您現在已登入 WordPress 網站的管理儀表板，您可以在其中執行管理動作。有關管理 WordPress 網站的更多信息，請參閱文檔中的 [WordPress Codex](#)。

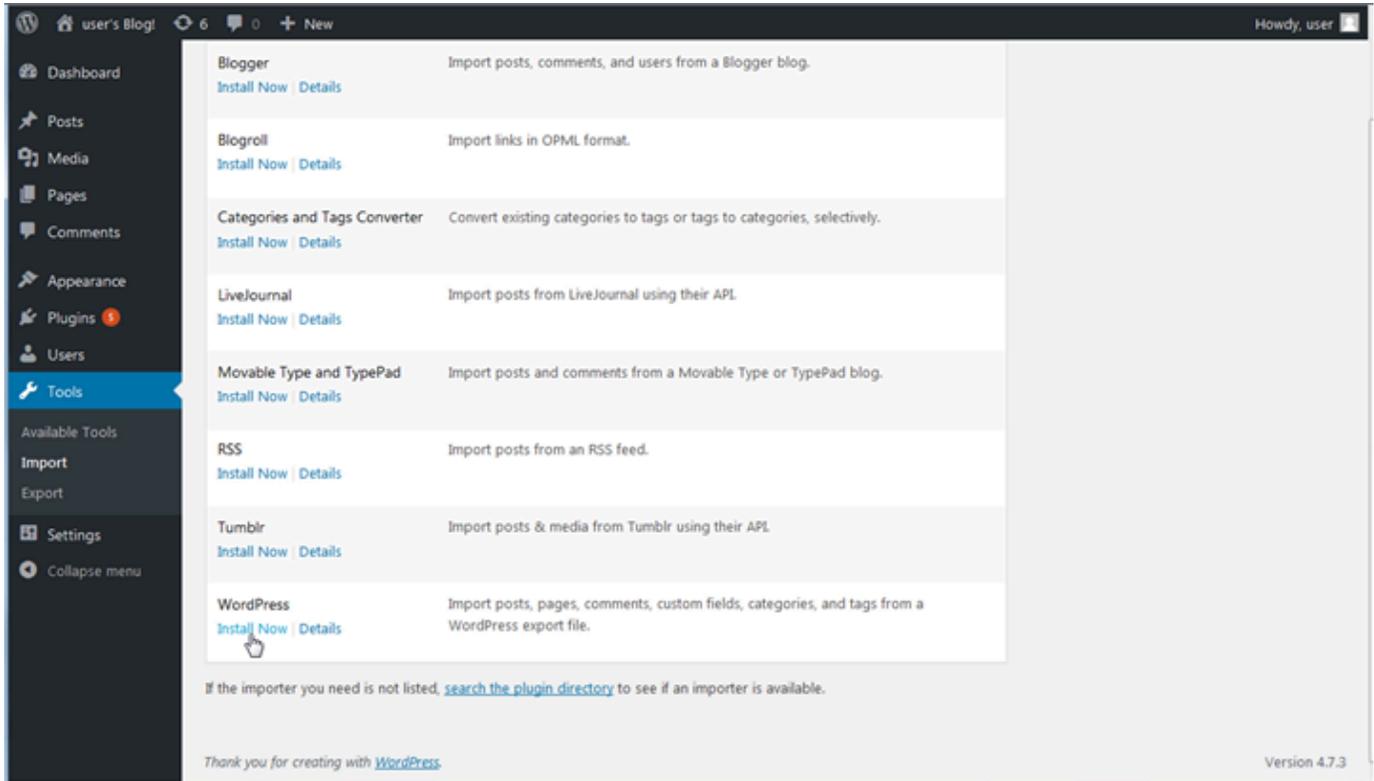


#### 步驟 4：將XML檔案匯入新的 Lightsail 部落格

在新的 Lightsail 執行個體上成功登入 WordPress 儀表板後，請依照下列步驟將XML檔案匯入新的 Lightsail 部落格。

1. 在新 Lightsail 實體上的「WordPress 控制面板」中，選擇「工具」。

## 2. 選擇 [匯入]，然後選擇 [立即安裝] 以安裝 WordPress 匯入工具。



## 3. 安裝工具完成之後，請選擇 Run Importer (執行匯入工具) 以執行匯入工具。

## 4. 在「匯入 WordPress」頁面上，選擇「瀏覽」。

## 5. 在「步驟 1：備份現有的 WordPress 部落格」中尋找您儲存的 XML 檔案，然後選擇「開啟」。

## 6. 選擇 Upload file and import (上傳檔案和匯入)。

接受其他預設值，然後選擇 Submit (提交)。

## 後續步驟

您可以選擇您的部落格 (位於「首頁」圖示旁)，然後從 WordPress 儀表板中選擇「造訪網站」，以確認一切正常。您也可以將 IP 地址輸入至瀏覽器，然後檢視部落格。

以下是一些後續步驟：

- 移轉您的網域名稱，DNS 讓您的網域名稱伺服器指向您的部落格的新版本。
- 自定義新博客的外觀和/或安裝一些 WordPress 插件。
- [啟用 SSL 憑證 HTTPS 支援](#)

依照 step-by-step 指示啟動和設定 WordPress 執行個體、保護執行個體的安全 HTTPS、連線至外部資料庫或儲存服務，以及將現有的部落格移轉至 Lightsail。這些教學涵蓋基本任務，例如取得 WordPress 管理員登入資料、安裝外掛程式、設定 DNS 和網域設定，以及與 Amazon S3、Amazon Aurora 和 Amazon AWS 服務等其他工作整合 SES。遵循本指南，您可以在 Lightsail 平台上輕鬆設定和管理安全、可擴充且高效能的 WordPress 網站。

## 在 Lightsail 上使用多站 WordPress 點管理多個網站

本節涵蓋下列與在 Amazon Lightsail 中管理 WordPress 多網站執行個體上的部落格相關主題：

### 主題

- [在 Lightsail 上將部落格作為網域新增至您的 WordPress 多網站](#)
- [在 Lightsail 上將部落格作為子網域新增至您的 WordPress 多網站](#)
- [在 Lightsail 上為您的 WordPress 多網站執行個體定義主要網域](#)

## 在 Lightsail 上將部落格作為網域新增至您的 WordPress 多網站

Amazon Lightsail 中的 WordPress 多網站執行個體旨在為您在該執行個體中建立的每個部落格網站使用多個網域或子網域。在本指南中，我們將向您展示如何在 WordPress 多站點實例上使用與主部落格主要網域不同的網域來新增部落格網站。例如，如果主要部落格的主要網域是 `example.com`，您所建立的新部落格站台可使用相同執行個體上的 `another-example.com` 和 `third-example.com` 網域。

### Note

您也可以將使用子網域的網站新增至 WordPress 多網站執行個體。如需詳細資訊，請參閱[將部落格新增為子網域至您的 WordPress 多網站執行個體](#)。

## 必要條件

依照下列順序完成先決條件：

1. 在 Lightsail 中建立 WordPress 多網站執行個體。如需詳細資訊，請參閱[建立執行個體](#)。
2. 建立靜態 IP，並將其附加至 Lightsail 中的 WordPress 多網站執行個體。如需詳細資訊，請參閱[建立靜態 IP 並將其附接至執行個體](#)。

3. 透過建立 DNS 區域，將您的網域新增至 Lightsail，然後將其指向您附加至 WordPress 多網站執行個體的靜態 IP。如需詳細資訊，請參閱[建立 DNS 區域以管理域的 DNS 記錄](#)。
4. 定義 WordPress 多網站執行個體的主要網域。如需詳細資訊，請參閱[定義 WordPress 多網站執行個體的主要網域](#)。

## 將部落格新增為網域至您的 WordPress 多網站執行個體

完成這些步驟，即可在您的 WordPress 多網站執行個體上建立部落格網站，該網站使用的網域與主要部落格的主要網域不同。

### ⚠ Important

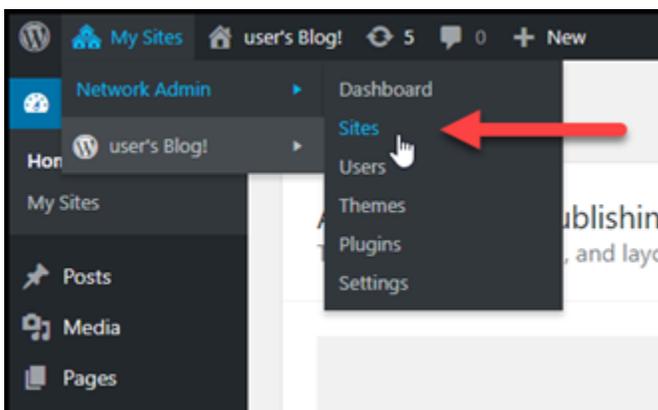
您必須先完成本指南先決條件小節所列的步驟 4，然後再執行這些步驟。

1. 登入 WordPress 多網站執行個體的管理儀表板。

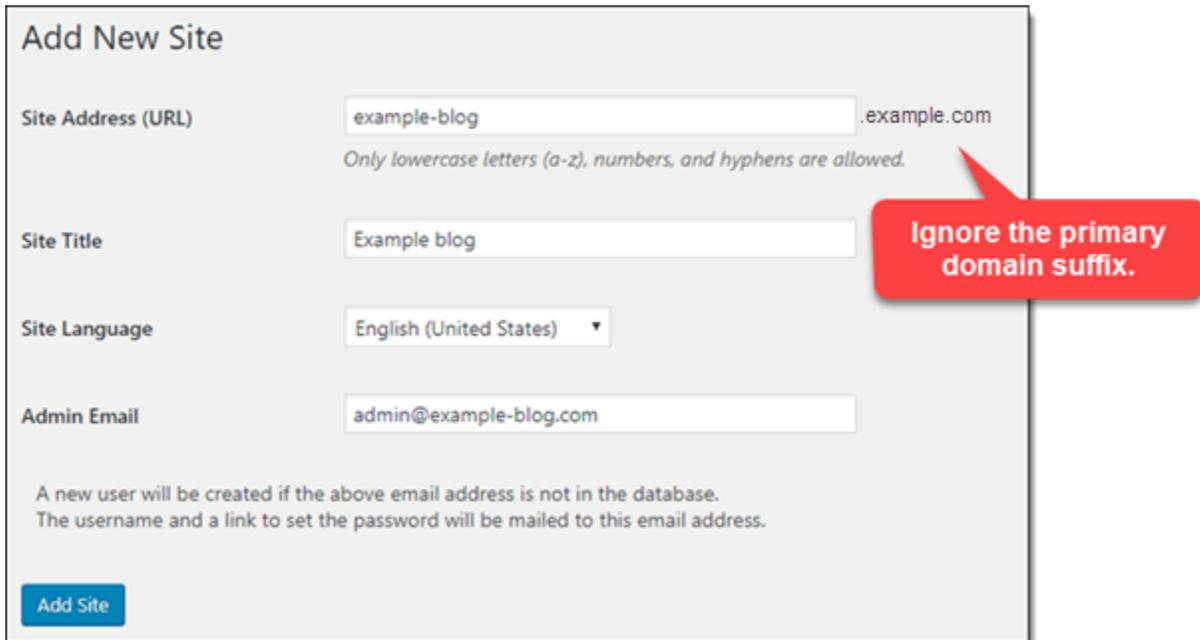
### 📌 Note

如需詳細資訊，請參閱[取得 Bitnami 執行個體的應用程式使用者名稱和密碼](#)。

2. 在頂部導覽窗格選擇 My Sites (我的網站)、Network Admin (網路管理) 和 Sites (網站)。



3. 選擇 Add New (新增) 來新增新的部落格網站。
4. 在 Site Address (URL) (網站地址 (URL)) 文字方塊中輸入網站地址。這是新部落格網站所用的網域。例如，若您的新部落格網站將使用 example-blog.com 作為網域，則在 Site Address (URL) (網站地址 (URL)) 文字方塊中輸入 example-blog。請忽略頁面顯示的主要網域字尾。



**Add New Site**

Site Address (URL)  .example.com  
*Only lowercase letters (a-z), numbers, and hyphens are allowed.*

Site Title

Site Language

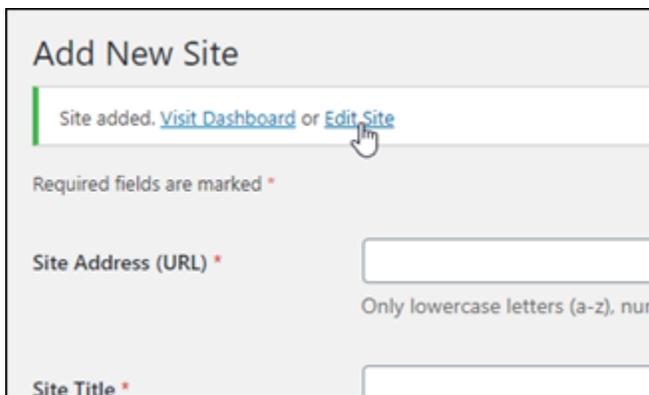
Admin Email

A new user will be created if the above email address is not in the database.  
The username and a link to set the password will be mailed to this email address.

[Add Site](#)

**Ignore the primary domain suffix.**

5. 輸入網站標題，選取語言，並輸入管理員電子郵件。
6. 選擇 Add Site (新增網站)。
7. 在頁面上顯示的確認橫幅中選擇 Edit Site (編輯網站)。這會將您重新引導至編輯您最近建立的網站的詳細資訊。



**Add New Site**

Site added. [Visit Dashboard](#) or [Edit Site](#)

Required fields are marked \*

Site Address (URL) \*

*Only lowercase letters (a-z), num*

Site Title \*

8. 在 Edit Site (編輯網站) 頁面中，將 Site Address (URL) (網站地址 (URL)) 文字方塊中列出的子網域變更為您要使用的 apex 網域。在此範例中，我們指定了 `http://example-blog.com`。

### Edit Site: Example Blog

[Visit](#) | [Dashboard](#)

**Info** | Users | Themes | Settings

Site Address (URL)

Registered

Last Updated

Attributes

- Public
- Archived
- Spam
- Deleted
- Mature

9. 選擇 Save Changes (儲存變更)。

此時，新的部落格網站已在您的 WordPress 多網站執行個體中建立，但網域尚未設定為路由到新的部落格網站。繼續下一個步驟，將地址記錄 (A 記錄) 新增至您網域的 DNS 區域。

Sites  Screen Options Help

All (2) | Public (2)

Bulk actions Apply 2 items

<input type="checkbox"/>	URL	Last Updated	Registered	Users
<input type="checkbox"/>	example.com — Main	Never	2020/12/10	1
<input type="checkbox"/>	example-blog.com	2021/01/25	2021/01/25	1

Bulk actions Apply 2 items

## 將地址記錄 (A 記錄) 新增至您網域的 DNS 區域

完成這些步驟，即可將新部落格網站的網域指向 WordPress 多網站執行個體。您必須針對在 WordPress 多網站執行個體上建立的每個部落格網站執行這些步驟。

為了進行示範，我們將使用 Lightsail DNS 區域。不過，通常網域註冊商託管的其他 DNS 區域也會採取類似步驟。

### Important

您最多可以在主控台中建立六個 DNS 區域。若您需要更多 DNS 區域，建議您使用 Amazon Route 53 來管理網域的 DNS 記錄。如需詳細資訊，請參閱 [將 Amazon Route 53 設定為現有域的 DNS 服務](#)。

1. 登入主 [Lightsail](#) 台。
2. 選擇 Lightsail 首頁上的 Domains & DNS (網域和 DNS) 索引標籤。
3. 在此頁的 DNS zones (DNS 區域) 部分底下，請選擇新部落格網站之網域的 DNS 區域。
4. 在 DNS 區域編輯器中，選擇 DNS records (DNS 記錄) 索引標籤。接著選擇 Add record (新增記錄)。



5. 在記錄類型下拉式功能表中選擇 A record (A 記錄)。
6. 在 Record name (記錄名稱) 文字方塊中，輸入 “@” 符號來建立網域根的記錄。
7. 在 [解析為] 文字方塊中，選擇附加至 WordPress 多網站執行個體的靜態 IP 位址。



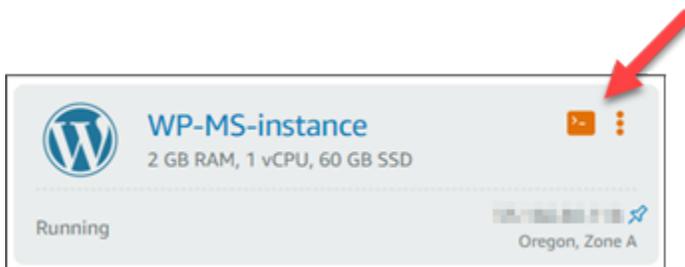
## 8. 選擇 Save (儲存) 圖示。

變更透過網際網路的 DNS 傳播之後，網域會將流量路由到您 WordPress 多網站執行個體上的新部落格網站。

## 啟用 Cookie 支援以允許登入部落格網站

當您將部落格網站新增為 WordPress 多網站執行個體時，您也必須更新執行個體上的 WordPress 設定 (wp-config) 檔案，以啟用 Cookie 支援。如果您不啟用 Cookie 支持，則用戶在嘗試登錄其博客網站的 WordPress 管理儀表板時可能會遇到「錯誤：阻止或不支持 Cookie」錯誤。

1. 登入主 [Lightsail](#) 台。
2. 在 Lightsail 首頁上，選擇 WordPress 多網站執行個體的安全殼層快速連線圖示。



3. 在您的 Lightsail 瀏覽器型 SSH 工作階段連線之後，請輸入下列指令，以使用 Vim 開啟及編輯執行個體的 wp-config.php 檔案：

```
sudo vim /opt/bitnami/wordpress/wp-config.php
```

**Note**

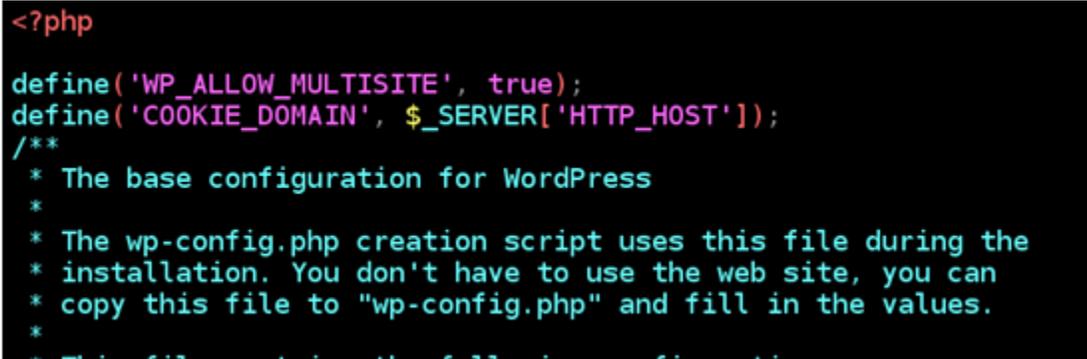
如果此命令失敗，您可能正在使用較舊版本的 WordPress 多網站執行個體。改為嘗試執行下列命令。

```
sudo vim /opt/bitnami/wordpress/wp-config.php
```

4. 在 Vim 中按 I 以進入插入模式。
5. 在 `define('WP_ALLOW_MULTISITE', true);` 文字行下方新增下列文字行。

```
define('COOKIE_DOMAIN', $_SERVER['HTTP_HOST']);
```

完成後，檔案會如下所示：



```
<?php
define('WP_ALLOW_MULTISITE', true);
define('COOKIE_DOMAIN', $_SERVER['HTTP_HOST']);
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the
 * installation. You don't have to use the web site, you can
 * copy this file to "wp-config.php" and fill in the values.
 *
 * This file is intended to be a base configuration for your WordPress installation.
```

6. 在 Vim 中按 Esc 鍵以離開插入模式，然後鍵入 `:wq!` 並按 Enter (輸入) 以儲存您的編輯 (寫入)，然後退出 Vim。
7. 輸入下列命令以重新啟動 WordPress 執行個體的基礎服務。

```
sudo /opt/bitnami/ctlscript.sh restart
```

現在應該在您的 WordPress 多站點實例上啟用 Cookie，並且嘗試登錄其博客網站的用戶不會遇到「錯誤：Cookie 被阻止或不支持」錯誤。

## 後續步驟

在您將部落格做為網域新增至 WordPress 多網站執行個體後，建議您熟悉 WordPress 多網站管理。如需詳細資訊，請參閱 WordPress 文件中的 [多站台網路管理](#)。

## 在 Lightsail 上將部落格作為子網域新增至您的 WordPress 多網站

Amazon Lightsail 中的 WordPress 多網站執行個體旨在為您在該執行個體中建立的每個部落格網站使用多個網域或子網域。在本指南中，我們將向您展示如何將部落格網站新增為 WordPress 多網站執行個體的子網域。例如，如果主要部落格的主要網域是 `example.com`，您可以建立新部落格站台，該站台會使用同一個執行個體上的 `earth.example.com` 和 `moon.example.com` 子網域。

### Note

您也可以將使用網域的網站新增至 WordPress 多網站執行個體。如需詳細資訊，請參閱[將部落格做為網域新增至您的 WordPress 多網站執行個體](#)。

### 必要條件

依照下列順序完成先決條件：

1. 建立 WordPress 多網站執行個體。如需詳細資訊，請參閱[建立執行個體](#)。
2. 建立靜態 IP 並將其附加至您的 WordPress 多網站執行個體。如需詳細資訊，請參閱[建立靜態 IP 並將其附接至執行個體](#)。
3. 透過建立 DNS 區域，將您的網域新增至 Lightsail，然後將其指向您附加至 WordPress 多網站執行個體的靜態 IP。如需詳細資訊，請參閱[建立 DNS 區域以管理域的 DNS 記錄](#)。
4. 定義 WordPress 多網站執行個體的主要網域。如需詳細資訊，請參閱[定義 WordPress 多網站執行個體的主要網域](#)。

### 將部落格新增為子網域至您的 WordPress 多網站執行個體

完成這些步驟，即可在您的 WordPress 多網站執行個體上建立新部落格，並使用您主要部落格主要網域的子網域。

### Important

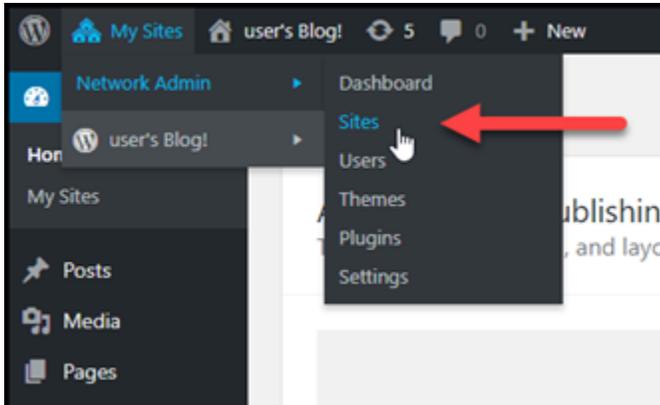
您必須先完成本指南先決條件小節所列的步驟 4，然後再執行這些步驟。

1. 登入 WordPress 多網站執行個體的管理儀表板。

**Note**

如需詳細資訊，請參閱[取得 Bitnami 執行個體的應用程式使用者名稱和密碼](#)。

- 在頂部導覽窗格選擇 My Sites (我的網站)、Network Admin (網路管理) 和 Sites (網站)。

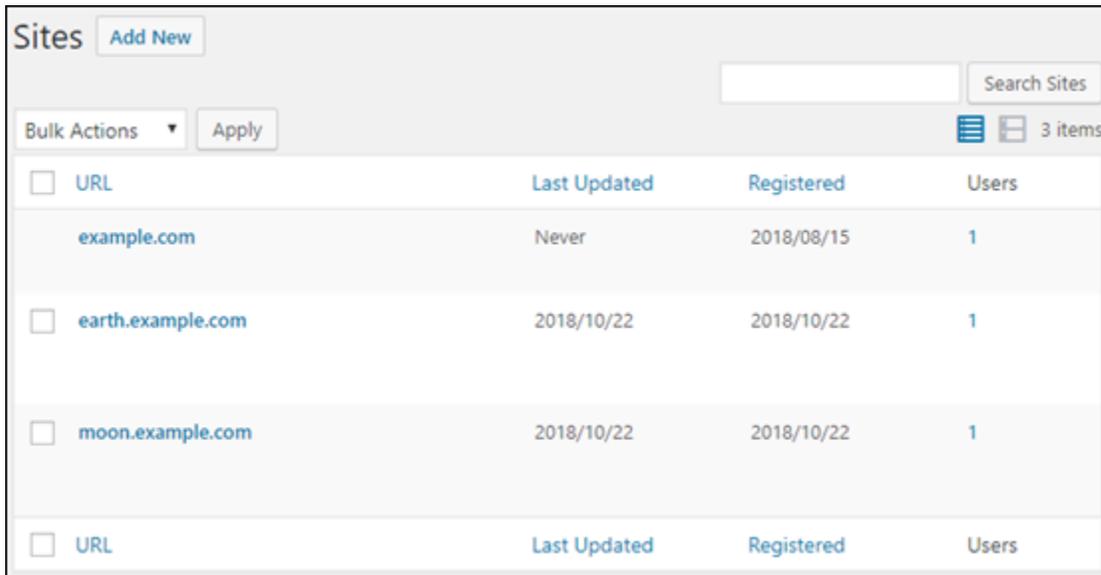


- 選擇 Add New (新增) 來新增新的部落格網站。
- 輸入站台地址，也就是在新部落格站台所用的子網域。

A screenshot of the 'Add New Site' form in the WordPress Network Admin dashboard. The form has four input fields: 'Site Address (URL)' with the value 'earth' and a '.example.com' suffix, 'Site Title' with the value 'Earth's Blog Site', 'Site Language' with a dropdown menu set to 'English (United States)', and 'Admin Email' with the value 'admin@example.com'. Below the fields is a note: 'A new user will be created if the above email address is not in the database. The username and a link to set the password will be mailed to this email address.' At the bottom left is a blue 'Add Site' button.

- 輸入網站標題，選取語言，並輸入管理員電子郵件。
- 選擇 Add Site (新增網站)。

此時，已在您的 WordPress 多網站執行個體中建立新的部落格網站，但子網域尚未設定為路由到新的部落格網站。繼續下一個步驟，將地址記錄 (A 記錄) 新增至您網域的 DNS 區域。



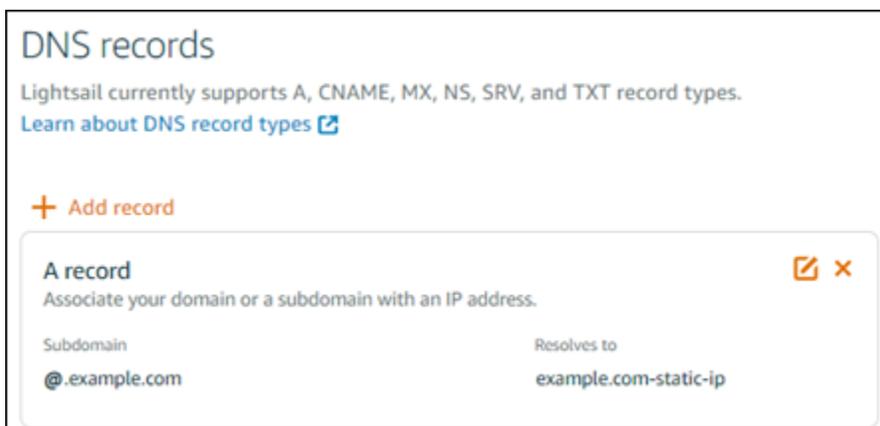
<input type="checkbox"/>	URL	Last Updated	Registered	Users
<input type="checkbox"/>	example.com	Never	2018/08/15	1
<input type="checkbox"/>	earth.example.com	2018/10/22	2018/10/22	1
<input type="checkbox"/>	moon.example.com	2018/10/22	2018/10/22	1
<input type="checkbox"/>	URL	Last Updated	Registered	Users

## 將地址記錄 (A 記錄) 新增至您網域的 DNS 區域

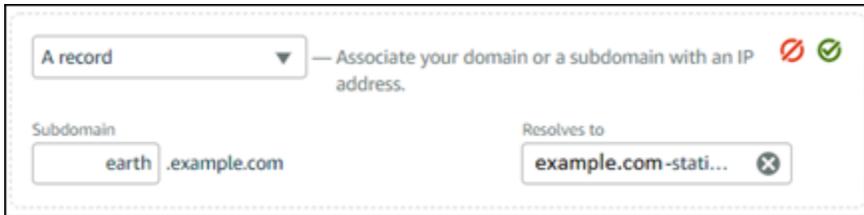
完成這些步驟，即可將新部落格網站的子網域指向 WordPress 多網站執行個體。您必須針對在 WordPress 多網站執行個體上建立的每個部落格網站執行這些步驟。

為了進行示範，我們將使用 Lightsail DNS 區域。不過，通常網域註冊商託管的其他 DNS 區域也會採取類似步驟。

1. 登入主 [Lightsail 台](#)。
2. 選擇 Lightsail 首頁上的 Domains & DNS (網域和 DNS) 索引標籤。
3. 在頁面的 DNS 區域區段下，選擇您定義為 WordPress 多網站執行個體主要網域的網域的 DNS 區域。
4. 在 DNS 區域編輯器中，選擇 DNS records (DNS 記錄) 索引標籤。接著選擇 Add record (新增記錄)。



5. 在記錄類型下拉式功能表中選擇 A record (A 記錄)。
6. 在 [記錄名稱] 文字方塊中，輸入在 WordPress 多網站執行個體上建立新部落格網站時指定為網站位址的子網域。
7. 在 [解析為] 文字方塊中，選擇附加至 WordPress 多網站執行個體的靜態 IP 位址。



8. 選擇 Save (儲存) 圖示。

您只需進行這些操作。變更透過網際網路的 DNS 傳播後，網域會重新導向至您 WordPress 多網站執行個體上的新部落格網站。

## 後續步驟

將部落格做為子網域新增至 WordPress 多網站執行個體後，建議您熟悉 WordPress 多網站管理。如需詳細資訊，請參閱 WordPress 文件中的[多站台網路管理](#)。

## 在 Lightsail 上為您的 WordPress 多網站執行個體定義主要網域

Amazon Lightsail 中的 WordPress 多網站執行個體旨在為您在該執行個體中建立的每個部落格網站使用多個網域或子網域。因此，您必須定義用於 WordPress 多網站執行個體主部落格的主要網域。

## 必要條件

依照下列順序完成先決條件：

1. 在 Lightsail 中建立 WordPress 多網站執行個體。如需詳細資訊，請參閱[建立執行個體](#)。
2. 建立靜態 IP 並將其附加至 Lightsail 中的 WordPress 多網站執行個體。如需詳細資訊，請參閱[建立靜態 IP 並將其附接至執行個體](#)。

### ⚠ Important

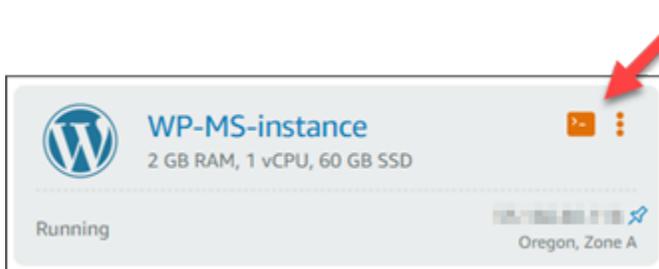
附加靜態 IP 後，您必須重新啟動 WordPress 多站台執行個體。這將允許執行個體識別其所連結的新靜態 IP。

3. 透過建立 DNS 區域，將您的網域新增至 Lightsail，然後將其指向您附加至 WordPress 多網站執行個體的靜態 IP。如需詳細資訊，請參閱[建立 DNS 區域以管理域的 DNS 記錄](#)。
4. 允許透過網際網路 DNS 傳播的 DNS 變更時間。接著，您可以繼續前往本指南的 [< 定義 WordPress 多網站執行個體的主要網域 >](#) 一節。

## 定義多網站執行個 WordPress 體的主要網域

完成這些步驟以確保您的網域 (例如 `example.com`，重新導向至 WordPress 多網站執行個體的主要部落格)。

1. 登入主 [Lightsail](#) 台。
2. 在 Lightsail 首頁上，選擇 WordPress 多網站執行個體的 SSH 快速連線圖示。



3. 輸入下列指令以定義 WordPress 多網站執行個體的主要網域名稱。請務必更換 `<domain>` 為您的 WordPress 多網站的正確網域名稱。

```
sudo /opt/bitnami/configure_app_domain --domain <domain>
```

範例：

```
sudo /opt/bitnami/configure_app_domain --domain example.com
```

### Note

如果此命令失敗，您可能正在使用較舊版本的 WordPress 多網站執行個體。嘗試運行以下命令，並確保替換 `<domain>` 為 WordPress 多站點的正確域名。

```
cd /opt/bitnami/apps/wordpress  
sudo ./bnconfig --machine_hostname <domain>
```

在執行該命令後，輸入以下命令，讓 `bnconfig` 工具不會在每次伺服器重新啟動時自動執行。

```
sudo mv bnconfig bnconfig.disabled
```

此時，瀏覽至您定義的網域應該會將您重新導向至 WordPress 多網站執行個體的主要部落格。

## 後續步驟

定義 WordPress 多網站執行個體的主要網域之後，請完成下一個步驟：

- [將部落格新增為子網域至您的 WordPress 多網站執行個體](#)
- [將部落格新增為網域至您的 WordPress 多網站執行個體](#)

請按照 step-by-step 指示瞭解如何使用不同的網域或子網域新增部落格網站，以及如何在 WordPress 多網站執行個體上為您的主要部落格定義主要網域。

本指南涵蓋建立 WordPress 多網站執行個體、附加靜態 IP、建立 DNS 區域，以及設定主要網域等先決條件。然後，它提供了將博客添加為域或子域，更新 DNS 記錄，啟用 cookie 支持以及執行其他必要配置的詳細步驟。按照本指南，您可以有效地管理和組織多 WordPress 站點實例中的多個博客，利用為每個博客網站使用單獨的域或子域的靈活性。

## 使用「讓我們加密」為 Lightsail 資源啟用加密通訊

本指南涵蓋下列與讓我們在 Amazon Lightsail 中加密相關的主題。開始之前，請確定您已完成下列先決條件：

### 必要條件

- [建立執行的 Lightsail 執行 LAMP 個體 WordPress](#)
- [註冊網域名稱並有權編輯其 DNS 記錄](#)
- [使用 Lightsail 瀏覽器式 SSH 終端機或您自己 SSH 的用戶端。](#)

### 主題

- [使用讓我們加密 SSL 憑證來保護您的 Lightsail LAMP 執行個體](#)

- [使用「讓我們加密 SSL/TLS」來保護您的 Lightsail 網站](#)
- [使用免費的讓我們加密 SSL 憑 WordPress 證來保護您的 Lightsail 執行個體](#)

## 使用讓我們加密 SSL 憑證來保護您的 Lightsail LAMP 執行個體

透過使用 Lightsail 負載平衡器，亞馬遜 Lightsail 可以透過 SSL/TLS 輕鬆保護您的網站和應用程式。但是，使用 Lightsail 負載平衡器通常不是正確的選擇。或許您的網站不需要負載平衡器提供的擴展能力或容錯能力，或者您是要最佳化成本。

在後者的情況中，您可能會考量使用 Let's Encrypt 以取得免費的 SSL 憑證。若是如此，則無問題。您可以將這些憑證與 Lightsail 執行個體整合。本教學課程說明如何使用 Certbot 請求 Let's Encrypt 萬用字元憑證，並將其與 LAMP 執行個體整合。

### Important

- Bitnami 執行個體所使用的 Linux 發行版本已在 2020 年 7 月從 Ubuntu 變更為 Debian。由於這項變更，本教學課程中的部分步驟會根據執行個體的 Linux 發行版本而有所不同。變更後才建立的所有 Bitnami 藍圖執行個體均會使用 Debian Linux 發行版本。在變更之前建立的執行個體將繼續使用 Ubuntu Linux 發行版本。若要檢查執行個體的分發，請執行 `uname -a` 命令。該回應會將執行個體的 Linux 發行版本顯示為 Ubuntu 或 Debian。
- Bitnami 正在修改其許多堆疊的檔案結構。本教學課程中的檔案路徑可能會根據您的 Bitnami 堆疊是否使用原生 Linux 系統套件 (方法 A)，或是否為獨立安裝 (方法 B) 而變更。若要識別您的 Bitnami 安裝類型以及要遵循的方法，請執行下列命令

```
test ! -f "/opt/bitnami/common/bin/openssl" && echo "Approach A: Using system packages." || echo "Approach B: Self-contained installation."
```

### 內容

- [步驟 1：完成先決條件](#)
- [步驟 2：在執行個體上安裝 Certbot](#)
- [步驟 3：請求 Let's Encrypt SSL 萬用字元憑證](#)
- [步驟 4：新增 TXT 記錄至域的 DNS 區域](#)
- [步驟 5：確認 TXT 記錄已傳播](#)

- [步驟 6：完成 Let's Encrypt SSL 憑證請求](#)
- [步驟 7：在 Apache 伺服器目錄中建立連結到 Let's Encrypt 憑證檔案](#)
- [步驟 8：為 Web 應用程式設定 HTTP 至 HTTPS 重新引導](#)
- [步驟 9：每 90 天續約 Let's Encrypt 憑證](#)

## 步驟 1：完成先決條件

請先完成事前準備 (若尚未完成)：

- 在 Lightsail 中建立 LAMP 執行個體。若要進一步了解，請參閱[建立執行個體](#)。
- 註冊網域名稱，並取得管理存取以編輯其 DNS 記錄。若要進一步了解，請參閱[Amazon Lightsail DNS](#)。

### Note

建議您使用 Lightsail DNS 區域管理網域的 DNS 記錄。若要進一步了解，請參閱[建立 DNS 區域以管理域的 DNS 記錄](#)。

- 使用 Lightsail 主控台中以瀏覽器為基礎的 SSH 終端機來執行本教學課程中的步驟。然而，您也可以使用自己的 SSH 用戶端，例如 PuTTY。若要進一步了解如何設定 PuTTY，請參閱[下載和設定 PuTTY 以使用 SSH 進行連線](#)。

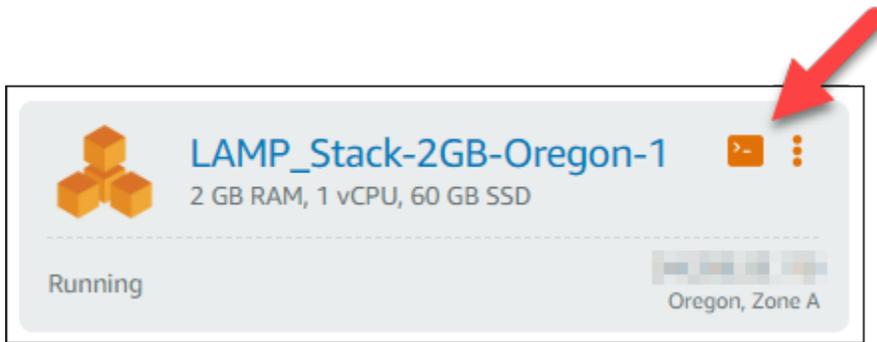
完成先決條件後，請繼續前往本教學課程的[下一節](#)。

## 步驟 2：在執行個體安裝 Certbot

Certbot 是一種用戶端，用於從 Let's Encrypt 請求憑證並將其部署至 Web 伺服器。Let's Encrypt 使用 ACME 協助發出憑證，而 Certbot 是一種啟用 ACME 的用戶端，可與 Let's Encrypt 互動。

若要在您的執行個體上安裝切爾特博特

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁上，針對您要連線的執行個體選擇安全殼層快速連線圖示。



3. 連線 Lightsail 瀏覽器型 SSH 工作階段之後，請輸入下列命令以更新執行個體上的套件：

```
sudo apt-get update
```

```
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-1069-aws x86_64)

 ████████
██ ████ ████ ████ ████
██ ████ ████ ████ ████
██ ████ ████ ████ ████
██ ████ ████ ████ ████

*** Welcome to the Bitnami LAMP 5.6.36-0 ***
*** Documentation: https://docs.bitnami.com/aws/infrastructure/lamp/ ***
***                    https://docs.bitnami.com/aws/ ***
*** Bitnami Forums: https://community.bitnami.com/ ***

Last login: Tue Oct 9 17:38:47 2018 from [REDACTED]
bitnami@ip-[REDACTED]:~$ sudo apt-get update
```

4. 輸入下列命令以安裝軟體屬性套件。Certbot 的開發人員使用個人套件存檔 (PPA) 分發 Certbot。軟體屬性套件可讓 PPA 的使用更有效率。

```
sudo apt-get install software-properties-common
```

#### Note

如果您在執行 `Could not get lock` 命令時遭遇 `sudo apt-get install` 錯誤，請等待大約 15 分鐘後再試一次。此錯誤可能是由使用 Apt 套件管理工具安裝自動升級的 cron 任務所引起的。

5. 輸入下列命令以新增 Certbot 至本機 apt 儲存庫：

**Note**

步驟 5 僅適用於使用 Ubuntu Linux 發行版本的執行個體。如果您的執行個體使用 Debian Linux 發行版本，請略過此步驟。

```
sudo apt-add-repository ppa:certbot/certbot -y
```

- 輸入下列命令更新 apt 以包含新的儲存庫：

```
sudo apt-get update -y
```

- 輸入下列命令以安裝 Certbot：

```
sudo apt-get install certbot -y
```

現在，Certbot 已安裝在您的執行個體上。

- 讓瀏覽器型 SSH 終端機視窗保持開啟 - 稍後您會在此教學課程中回到此處。繼續前往本教學課程的[下一節](#)。

### 步驟 3：請求 Let's Encrypt SSL 萬用字元憑證

開始從 Let's Encrypt 請求憑證的程序。使用 Certbot (請求萬用字元憑證) 可讓您針對網域及其子網域使用單一憑證。例如，單一萬用字元憑證適用於 example.com 頂層網域，以及 blog.example.com、stuff.example.com 子網域。

請求 Let's Encrypt SSL 萬用字元憑證

- 在與本教學課程[步驟 2](#)使用的相同瀏覽器型 SSH 終端機視窗中，輸入下列命令為您的網域設定環境變數。您現在可以更有效率複製和貼上命令以取得憑證。

```
DOMAIN=Domain
```

```
WILDCARD=*.$DOMAIN
```

在命令中，將 *Domain* 取代為您的註冊網域名稱。

範例：

```
DOMAIN=example.com
```

```
WILDCARD=*.$DOMAIN
```

2. 輸入下列命令確認變數傳回正確的值：

```
echo $DOMAIN && echo $WILDCARD
```

您應該會看到類似以下的結果：



```
bitnami@ip-172-31-1-144:~$ DOMAIN=example.com
bitnami@ip-172-31-1-144:~$ WILDCARD=*.$DOMAIN
bitnami@ip-172-31-1-144:~$ echo $DOMAIN && echo $WILDCARD
example.com
*.example.com
bitnami@ip-172-31-1-144:~$
```

A red arrow points to the first line of the terminal output, which is `example.com`.

3. 在互動式模式中輸入下列命令啟動 Certbot。此命令會通知 Certbot 使用手動授權方法搭配 DNS 查問以驗證網域所有權。這會為您的頂層網域及其子網域請求萬用字元憑證。

```
sudo certbot -d $DOMAIN -d $WILDCARD --manual --preferred-challenges dns certonly
```

4. 在提示時輸入您的電子郵件地址，這會用於續約和安全性注意事項。
5. 閱讀 Let's Encrypt 服務條款。完成時，如果您同意請按 A。如果您不同意，就無法取得 Let's Encrypt 憑證。
6. 根據分享您電子郵件地址的提示和關於您 IP 地址被記錄的警告做出回應。
7. Let's Encrypt 現在會提示您確認您擁有所指定的網域。要這麼做，請新增 TXT 記錄至網域的 DNS 記錄。這會提供一組 TXT 記錄值，如以下範例所示：

#### Note

Let's Encrypt 可能會提供一或多個必須用於驗證的 TXT 記錄。在此範例中，我們有兩個 TXT 記錄可用於驗證。

```
-----  
Please deploy a DNS TXT record under the name  
_acme-challenge.example.com with the following value:  
9vuaf232Bz0War8BUx3dTnBDpo6lm_4CDX4fpx4reoo  
Before continuing, verify the record is deployed.  
Press Enter to Continue  
-----  
Please deploy a DNS TXT record under the name  
_acme-challenge.example.com with the following value:  
BVkHW11a0Zhi2UB4BfoSmJV-B_fiSrWfdaf8eBA30dU  
Before continuing, verify the record is deployed.  
-----
```

8. 讓 Lightsail 瀏覽器型 SSH 工作階段保持開啟狀態，您稍後會在本教學課程中回到該工作階段。繼續前往本教學課程的[下一節](#)。

#### 步驟 4：新增 TXT 記錄至域的 DNS 區域

新增 TXT 記錄至網域的 DNS 區域可驗證您擁有網域。為了進行示範，我們會使用 Lightsail DNS 區域。然而，通常由網域註冊商託管的其他 DNS 區域可能會採取類似步驟。

##### Note

若要深入瞭解如何為您的網域建立 Lightsail DNS 區域，請參閱[在 Lightsail 中建立 DNS 區域以管理網域的 DNS 記錄](#)。

若要將 TXT 記錄新增至您網域的 DNS 區 Lightsail

1. 選擇 Lightsail 首頁上的 Domains & DNS (網域和 DNS) 索引標籤。
2. 在頁面的 DNS zones (DNS 區域) 部分，選擇您在 Certbot 憑證請求中所指定網域的 DNS 區域。
3. 在 DNS 區域編輯器中，選擇 DNS records (DNS 記錄)。
4. 選擇 Add record (新增記錄)。
5. 在 Record type (記錄類型) 下拉式選單中，選擇 TXT record (TXT 記錄)。

- 將 Let's Encrypt 憑證請求指定的值輸入 Record name (記錄名稱) 和 Responds with (回應內容) 欄位。

 Note

Lightsail 主控台會預先填入您網域的頂點部分。例如，如果您要新增 `_acme-challenge.example.com` 子網域，則只需在文字方塊中輸入 `_acme-challenge`，當您儲存記錄時，Lightsail 會新增 `.example.com` 部分。

- 選擇儲存。
- 重複步驟 4 到 7 以新增第二組由 Let's Encrypt 憑證請求指定的 TXT 記錄。
- 讓 Lightsail 主控台瀏覽器視窗保持開啟狀態，您稍後會在本教學課程中回到該視窗。繼續前往本教學課程的 [下一節](#)。

## 步驟 5：確認 TXT 記錄已傳播

使用此公用 MxToolbox 程式來確認 TXT 記錄已傳播至網際網路的 DNS。DNS 記錄傳輸可能需要一些時間，這取決於您的 DNS 託管提供者，以及設定的 DNS 記錄存留時間 (TTL)。在繼續 Certbot 憑證請求之前，請務必完成此步驟，並確認 TXT 記錄已傳播。否則，您的憑證請求會失敗。

確認 TXT 記錄已傳播至網際網路的 DNS

- 開啟新的瀏覽器視窗並前往 <https://mxtoolbox.com/TXTLookup.aspx>。
- 將以下文字輸入文字方塊。

```
_acme-challenge.Domain
```

將 *Domain* 取代您的註冊網域名稱。

範例：

```
_acme-challenge.example.com
```

**MX TOOLBOX®**

Home MX Lookup Blacklists Diagnostics Domain Health

## DNS Text Lookup

**Domain Name**

3. 選擇 TXT Lookup (TXT 查詢) 以執行檢查。
4. 這會產生以下其中一個回應：
  - 如果您的 TXT 記錄已傳播至網際網路的 DNS，您會看到類似以下螢幕擷取畫面的回應。關閉瀏覽器視窗，並繼續前往本教學課程的[下一節](#)。

**txt:\_acme-challenge.example.com**

Type	Domain Name	TTL	Record
TXT	<a href="#">_acme-challenge.example.com</a>	60 sec	9vuaf232Bz0War8BUx3dTnBDpo6lm_4CDX4fpx4reoo
TXT	<a href="#">_acme-challenge.example.com</a>	60 sec	BVkHW11aOZhi2UB4BfoSmJV-B_fiSrwfdaf8eBA30dU

	Test	Result
<input checked="" type="checkbox"/>	DNS Record Published	DNS Record found

Your DNS hosting provider is "Amazon Route 53" [Need Bulk Dns Provider Data?](#)

[dns lookup](#)
[smtp diag](#)
[blacklist](#)
[http test](#)
[dns propagation](#)

Reported by on 10/8/2018 at 8:53:50 PM (UTC 0), [just for you.](#) [Transcript](#)

- 如果 TXT 記錄未傳播至網際網路的 DNS，您會看見 DNS Record not found (找不到 DNS 記錄) 回應。確認您已新增正確 DNS 記錄至網域的 DNS 區域。如果您新增了正確記錄，請再等待片刻讓網域的 DNS 記錄傳播，接著再次執行 TXT 查詢。

## 步驟 6：完成 Let's Encrypt SSL 憑證請求

返回 LAMP 執行個體的 Lightsail 瀏覽器型 SSH 工作階段，並完成「讓我們加密」憑證要求。Certbot 會將 SSL 憑證、鏈及金鑰檔案儲存至 LAMP 執行個體上的特定目錄。

完成 Let's Encrypt SSL 憑證請求

1. 在 LAMP 執行個體的 Lightsail 瀏覽器型 SSH 工作階段中，按 Enter 繼續您的 [讓我們加密 SSL 憑證要求]。如果成功，則會顯示與以下螢幕擷取畫面類似的回應：

```
-----
Please deploy a DNS TXT record under the name
_acme-challenge.example.com with the following value:

9vuaf232Bz0War8BUx3dTnBDpo6lm_4CDX4fpx4reoo

Before continuing, verify the record is deployed.
-----
Press Enter to Continue

-----
Please deploy a DNS TXT record under the name
_acme-challenge.example.com with the following value:

BVkHwll1a0Zhi2UB4BfoSmJV-B_fiSrWfdaf8eBA30dU

Before continuing, verify the record is deployed.
-----
Press Enter to Continue
Waiting for verification...
Cleaning up challenges

IMPORTANT NOTES:
- Congratulations! Your certificate and chain have been saved at:
  /etc/letsencrypt/live/example.com/fullchain.pem
  Your key file has been saved at:
  /etc/letsencrypt/live/example.com/privkey.pem
  Your cert will expire on 2019-01-06. To obtain a new or tweaked
  version of this certificate in the future, simply run certbot
  again. To non-interactively renew *all* of your certificates, run
  "certbot renew"
- If you like Certbot, please consider supporting our work by:

  Donating to ISRG / Let's Encrypt:  https://letsencrypt.org/donate
  Donating to EFF:                  https://eff.org/donate-le

bitnami@ip-172-26-1-148:/$
```

訊息會確認您的憑證、鏈和金鑰檔案存放於 `/etc/letsencrypt/live/Domain/` 目錄。*Domain* 是您已註冊的網域名稱，例如，`/etc/letsencrypt/live/example.com/`。

2. 記下訊息中指定的過期日期。您可將其用於在該日期續約憑證。

**IMPORTANT NOTES:**

```

- Congratulations! Your certificate and chain have been saved at:
  /etc/letsencrypt/live/example.com/fullchain.pem
  Your key file has been saved at:
  /etc/letsencrypt/live/example.com/privkey.pem
  Your cert will expire on 2019-01-06. To obtain a new or tweaked
  version of this certificate in the future, simply run certbot
  again. To non-interactively renew *all* of your certificates, run
  "certbot renew"
- If you like Certbot, please consider supporting our work by:

  Donating to ISRG / Let's Encrypt: https://letsencrypt.org/donate
  Donating to EFF:                 https://eff.org/donate-le

```

- 既然您擁有 Let's Encrypt 憑證，就請繼續前往本教學課程的[下一節](#)。

### 步驟 7：在 Apache 伺服器目錄中建立連結到 Let's Encrypt 憑證檔案

在 LAMP 執行個體上的 Apache 伺服器目錄建立至 Let's Encrypt SSL 憑證檔案的連結。此外，請備份現有的憑證，以防您稍後需要用到。

若要在 Apache 伺服器目錄建立至 Let's Encrypt 憑證檔案的連結

- 在 LAMP 執行個體的 Lightsail 瀏覽器型 SSH 工作階段中，輸入下列命令以停止基礎 LAMP 堆疊服務：

```
sudo /opt/bitnami/ctlscript.sh stop
```

您應該會看到類似以下的回應：

```

bitnami@ip-172-31-0-144:~$ sudo /opt/bitnami/ctlscript.sh stop

Syntax OK
/opt/bitnami/apache2/scripts/ctl.sh : httpd stopped
/opt/bitnami/php/scripts/ctl.sh : php-fpm stopped
/opt/bitnami/mysql/scripts/ctl.sh : mysql stopped
bitnami@ip-172-31-0-144:~$

```

- 輸入下列命令以設定網域的環境變數。

```
DOMAIN=Domain
```

在命令中，將 *Domain* 取代為您的註冊網域名稱。

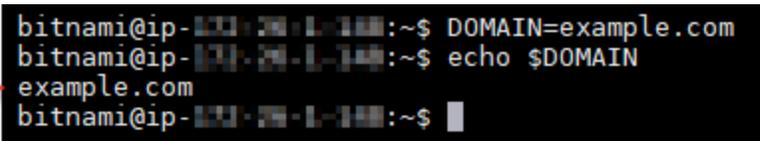
範例：

```
DOMAIN=example.com
```

3. 輸入下列命令確認變數傳回正確的值：

```
echo $DOMAIN
```

您應該會看到類似以下的結果：



```
bitnami@ip-172-31-1-100:~$ DOMAIN=example.com
bitnami@ip-172-31-1-100:~$ echo $DOMAIN
example.com
bitnami@ip-172-31-1-100:~$
```

A red arrow points to the output line 'example.com' in the terminal screenshot.

4. 個別輸入下列命令，以重新命名現有的憑證檔案做為備份。請參閱本教學課程開頭的重要區塊，以取得有關不同發行版本和檔案結構的資訊。

- Debian Linux 發行版本

方法 A (使用系統套件的 Bitnami 安裝)：

```
sudo mv /opt/bitnami/apache2/conf/bitnami/certs/server.crt /opt/bitnami/apache2/conf/bitnami/certs/server.crt.old
```

```
sudo mv /opt/bitnami/apache2/conf/bitnami/certs/server.key /opt/bitnami/apache2/conf/bitnami/certs/server.key.old
```

方法 B (獨立的 Bitnami 安裝)：

```
sudo mv /opt/bitnami/apache2/conf/server.crt /opt/bitnami/apache2/conf/server.crt.old
```

```
sudo mv /opt/bitnami/apache2/conf/server.key /opt/bitnami/apache2/conf/server.key.old
```

- 對於使用 Ubuntu Linux 發行版本的較舊執行個體：

```
sudo mv /opt/bitnami/apache/conf/bitnami/certs/server.crt /opt/bitnami/apache/conf/bitnami/certs/server.crt.old
```

```
sudo mv /opt/bitnami/apache/conf/bitnami/certs/server.key /opt/bitnami/apache/conf/bitnami/certs/server.key.old
```

5. 單獨輸入下列命令，在 apache2 伺服器目錄中建立 Let's Encrypt 憑證檔案的連結：請參閱本教學課程開頭的重要區塊，以取得有關不同發行版本和檔案結構的資訊。

- Debian Linux 發行版本

方法 A (使用系統套件的 Bitnami 安裝)：

```
sudo ln -sf /etc/letsencrypt/live/$DOMAIN/privkey.pem /opt/bitnami/apache2/conf/bitnami/certs/server.key
```

```
sudo ln -sf /etc/letsencrypt/live/$DOMAIN/fullchain.pem /opt/bitnami/apache2/conf/bitnami/certs/server.crt
```

方法 B (獨立的 Bitnami 安裝)：

```
sudo ln -sf /etc/letsencrypt/live/$DOMAIN/privkey.pem /opt/bitnami/apache2/conf/server.key
```

```
sudo ln -sf /etc/letsencrypt/live/$DOMAIN/fullchain.pem /opt/bitnami/apache2/conf/server.crt
```

- 對於使用 Ubuntu Linux 發行版本的較舊執行個體：

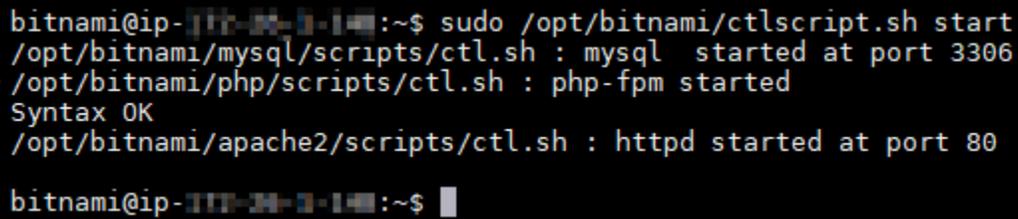
```
sudo ln -s /etc/letsencrypt/live/$DOMAIN/privkey.pem /opt/bitnami/apache/conf/bitnami/certs/server.key
```

```
sudo ln -s /etc/letsencrypt/live/$DOMAIN/fullchain.pem /opt/bitnami/apache/conf/bitnami/certs/server.crt
```

6. 輸入下列命令以啟動您先前停止的基礎 LAMP 堆疊服務：

```
sudo /opt/bitnami/ctlscript.sh start
```

您應該會看到類似以下的結果：

A terminal window showing the execution of a script to start LAMP services. A red arrow points to the first line of output. The output shows that MySQL, PHP-FPM, and Apache2 have started successfully.

```
bitnami@ip-10-10-10-10:~$ sudo /opt/bitnami/ctlscript.sh start
/opt/bitnami/mysql/scripts/ctl.sh : mysql started at port 3306
/opt/bitnami/php/scripts/ctl.sh : php-fpm started
Syntax OK
/opt/bitnami/apache2/scripts/ctl.sh : httpd started at port 80
bitnami@ip-10-10-10-10:~$
```

您的 LAMP 執行個體現在已設定為使用 SSL 加密。然而，流量不會從 HTTP 自動重新引導至 HTTPS。

7. 繼續前往本教學課程的[下一節](#)。

## 步驟 8：為 Web 應用程式設定 HTTP 至 HTTPS 重新引導

您可以為你的 LAMP 執行個體設定 HTTP 至 HTTPS 重新引導。從 HTTP 自動重新引導至 HTTPS 會讓客戶只能使用 SSL 存取網站，即使他們使用 HTTP 進行連線也是如此。

### 為 Web 應用程式設定 HTTP 至 HTTPS 重新引導

1. 在 LAMP 執行個體的 Lightsail 瀏覽器型 SSH 工作階段中，輸入下列命令，以使用 Vim 文字編輯器編輯 Apache 網頁伺服器設定檔：

```
sudo vim /opt/bitnami/apache2/conf/bitnami/bitnami.conf
```

#### Note

此教學課程使用 Vim 做為示範；然而，您可以在此步驟選擇任何文字編輯器。

2. 按 `i` 進入 Vim 編輯器的插入模式。
3. 在檔案中，於 `DocumentRoot "/opt/bitnami/apache2/htdocs"` 和 `<Directory "/opt/bitnami/apache2/htdocs">` 之間輸入以下文字：

```
RewriteEngine On
RewriteCond %{HTTPS} !=on
RewriteRule ^/(.*) https://%{SERVER_NAME}/$1 [R,L]
```

結果應如下列範例所示：

```
NameVirtualHost *:443
</IfVersion>

<VirtualHost _default_:80>
  DocumentRoot "/opt/bitnami/apache2/htdocs"
  RewriteEngine On
  RewriteCond %{HTTPS} !=on
  RewriteRule ^/(.*) https://%{SERVER_NAME}/$1 [R,L]
  <Directory "/opt/bitnami/apache2/htdocs">
    Options Indexes FollowSymLinks
    AllowOverride All
    <IfVersion < 2.3 >
      Order allow,deny
      Allow from all
    </IfVersion>
    <IfVersion >= 2.3 >
```

- 按 ESC (ESC) 鍵，接著輸入 :wq 以寫入 (儲存) 您的編輯，然後退出 Vim。
- 輸入下列命令重新啟動基礎 LAMP 堆疊服務並使您的編輯生效：

```
sudo /opt/bitnami/ctlscript.sh restart
```

您的 LAMP 執行個體現在已設定為自動將連線從 HTTP 重新引導至 HTTPS。當訪客前往 `http://www.example.com` 時，系統會自動重新引導至加密的 `https://www.example.com` 地址。

## 步驟 9：每 90 天續約 Let's Encrypt 憑證

Let's Encrypt 憑證有效期為 90 天。您可以憑證過期前 30 天內進行續約。若要更新 Let's Encrypt 憑證，請執行原始命令來取得憑證。重複本教學課程的[請求 Let's Encrypt SSL 萬用字元憑證](#)一節中的步驟。

## 使用「讓我們加密 SSL/TLS」來保護您的 Lightsail 網站

透過使用 Lightsail 負載平衡器，亞馬遜 Lightsail 可以透過 SSL/TLS 輕鬆保護您的網站和應用程式。但是，使用 Lightsail 負載平衡器通常不是正確的選擇。或許您的網站不需要負載平衡器提供的擴展能力或容錯能力，或者您是要最佳化成本。

在後者的情況中，您可能會考量使用 Let's Encrypt 以取得免費的 SSL 憑證。若是如此，則無問題。您可以將這些憑證與 Lightsail 執行個體整合。本教學課程會說明如何使用 Certbot 請求 Let's Encrypt 萬用字元憑證，並將該憑證與 Nginx 執行個體整合。

### ⚠ Important

- Bitnami 執行個體所使用的 Linux 發行版本已在 2020 年 7 月從 Ubuntu 變更為 Debian。由於這項變更，本教學課程中的部分步驟會根據執行個體的 Linux 發行版本而有所不同。變更後才建立的所有 Bitnami 藍圖執行個體均會使用 Debian Linux 發行版本。在變更之前建立的執行個體將繼續使用 Ubuntu Linux 發行版本。若要檢查執行個體的分發，請執行 `uname -a` 命令。該回應會將執行個體的 Linux 發行版本顯示為 Ubuntu 或 Debian。
- Bitnami 正在修改其許多堆疊的檔案結構。本教學課程中的檔案路徑可能會根據您的 Bitnami 堆疊是否使用原生 Linux 系統套件 (方法 A)，或是否為獨立安裝 (方法 B) 而變更。若要識別您的 Bitnami 安裝類型以及要遵循的方法，請執行下列命令

```
test ! -f "/opt/bitnami/common/bin/openssl" && echo "Approach A: Using system packages." || echo "Approach B: Self-contained installation."
```

## 內容

- [步驟 1：完成先決條件](#)
- [步驟 2：在您的執行個體上安裝 Certbot](#)
- [步驟 3：請求 Let's Encrypt SSL 萬用字元憑證](#)
- [步驟 4：新增 TXT 記錄至域的 DNS 區域](#)
- [步驟 5：確認 TXT 記錄已傳播](#)
- [步驟 6：完成 Let's Encrypt SSL 憑證請求](#)
- [步驟 7：在 Nginx 伺服器目錄中建立 Let's Encrypt 憑證檔案的連結](#)
- [步驟 8：為 Web 應用程式設定 HTTP 至 HTTPS 重新引導](#)
- [步驟 9：每 90 天續約 Let's Encrypt 憑證](#)

## 步驟 1：完成先決條件

請先完成事前準備 (若尚未完成)：

- 在 Lightsail 中創建一個 Nginx 實例。若要進一步了解，請參閱[建立執行個體](#)。
- 註冊網域名稱，並取得管理存取以編輯其 DNS 記錄。若要進一步了解，請參閱[DNS](#)。

**Note**

建議您使用 Lightsail DNS 區域管理網域的 DNS 記錄。若要進一步了解，請參閱[建立 DNS 區域以管理域的 DNS 記錄](#)。

- 使用 Lightsail 主控台中以瀏覽器為基礎的 SSH 終端機來執行本教學課程中的步驟。然而，您也可以使用自己的 SSH 用戶端，例如 PuTTY。若要進一步了解如何設定 PuTTY，請參閱[在 Amazon Lightsail 中下載和設定 PuTTY 以使用 SSH 進行連線](#)。

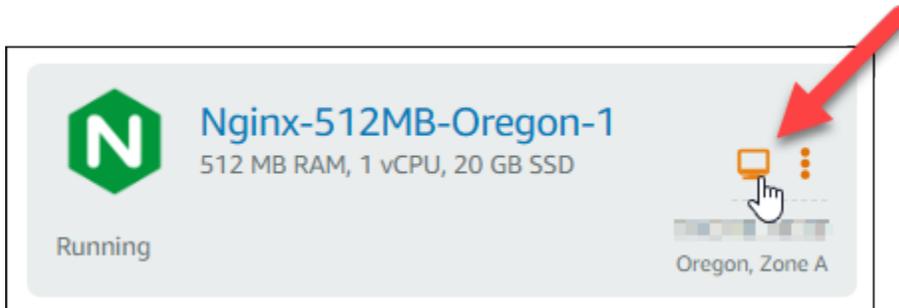
完成先決條件後，請繼續前往本教學課程的[下一節](#)。

## 步驟 2：在您的執行個體上安裝 Certbot

Certbot 是一種用戶端，用於從 Let's Encrypt 請求憑證並將其部署至 Web 伺服器。Let's Encrypt 使用 ACME 協助發出憑證，而 Certbot 是一種啟用 ACME 的用戶端，可與 Let's Encrypt 互動。

若要在您的執行個體上安裝切爾特博特

1. 登入主 [Lightsail](#) 台。
2. 在 Lightsail 首頁上，針對您要連線的執行個體選擇安全殼層快速連線圖示。



3. 連線 Lightsail 瀏覽器型 SSH 工作階段之後，請輸入下列命令來更新執行個體上的套件：

```
sudo apt-get update
```

```

Welcome to Ubuntu 16.04.5 LTS (GNU/Linux 4.4.0-1065-aws x86_64)
*** System restart required ***

          _ _              _ _
         | |_|_|           | |_|_| | |
         || |||           || |||
         || |||           || |||
         || |||           || |||
         || |||           || |||
         || |||           || |||
         || |||           || |||
         || |||           || |||
         || |||           || |||

*** Welcome to the Bitnami Nginx 1.14.0-1 ***
*** Documentation:  https://docs.bitnami.com/aws/infrastructure/nginx/ ***
***                  https://docs.bitnami.com/aws/ ***
*** Bitnami Forums: https://community.bitnami.com/ ***
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

bitnami@ip-...:~$ sudo apt-get update

```

4. 輸入下列命令以安裝軟體屬性套件。Certbot 的開發人員使用個人套件存檔 (PPA) 分發 Certbot。軟體屬性套件可讓 PPA 的使用更有效率。

```
sudo apt-get install software-properties-common
```

#### Note

如果您在執行 `Could not get lock` 命令時遭遇 `sudo apt-get install` 錯誤，請等待大約 15 分鐘後再試一次。此錯誤可能是由使用 Apt 套件管理工具安裝自動升級的 cron 任務所引起的。

5. 輸入下列命令以新增 Certbot 至本機 apt 儲存庫：

#### Note

步驟 5 僅適用於使用 Ubuntu Linux 發行版本的執行個體。如果您的執行個體使用 Debian Linux 發行版本，請略過此步驟。

```
sudo apt-add-repository ppa:certbot/certbot -y
```

6. 輸入下列命令更新 apt 以包含新的儲存庫：

```
sudo apt-get update -y
```

## 7. 輸入下列命令以安裝 Certbot :

```
sudo apt-get install certbot -y
```

現在，Certbot 已安裝在您的執行個體上。

## 8. 讓瀏覽器型 SSH 終端機視窗保持開啟 - 稍後您會在此教學課程中回到此處。繼續前往本教學課程的[下一節](#)。

### 步驟 3：請求 Let's Encrypt SSL 萬用字元憑證

開始從 Let's Encrypt 請求憑證的程序。使用 Certbot (請求萬用字元憑證) 可讓您針對網域及其子網域使用單一憑證。例如，單一萬用字元憑證適用於 `example.com` 頂層網域，以及 `blog.example.com`、`stuff.example.com` 子網域。

#### 請求 Let's Encrypt SSL 萬用字元憑證

1. 在與本教學課程[步驟 2](#) 使用的相同瀏覽器型 SSH 終端機視窗中，輸入下列命令為您的網域設定環境變數。您現在可以更有效率複製和貼上命令以取得憑證。請務必以註冊的網域名稱取代 *domain*。

```
DOMAIN=domain
```

```
WILDCARD=*.$DOMAIN
```

範例：

```
DOMAIN=example.com
```

```
WILDCARD=*.$DOMAIN
```

2. 輸入下列命令確認變數傳回正確的值：

```
echo $DOMAIN && echo $WILDCARD
```

您應該會看到類似以下的結果：

```
bitnami@ip-172-31-1-144:~$ DOMAIN=example.com
bitnami@ip-172-31-1-144:~$ WILDCARD=*. $DOMAIN
bitnami@ip-172-31-1-144:~$ echo $DOMAIN && echo $WILDCARD
example.com
*.example.com
bitnami@ip-172-31-1-144:~$
```

3. 在互動式模式中輸入下列命令啟動 Certbot。此命令會通知 Certbot 使用手動授權方法搭配 DNS 查問以驗證網域所有權。這會為您的頂層網域及其子網域請求萬用字元憑證。

```
sudo certbot -d $DOMAIN -d $WILDCARD --manual --preferred-challenges dns certonly
```

4. 在提示時輸入您的電子郵件地址，這會用於續約和安全性注意事項。
5. 閱讀 Let's Encrypt 服務條款。完成時，如果您同意請按 A。如果您不同意，就無法取得 Let's Encrypt 憑證。
6. 根據分享您電子郵件地址的提示和關於您 IP 地址被記錄的警告做出回應。
7. Let's Encrypt 現在會提示您確認您擁有所指定的網域。要這麼做，請新增 TXT 記錄至網域的 DNS 記錄。這會提供一組 TXT 記錄值，如以下範例所示：

#### Note

Let's Encrypt 可能會提供一或多個必須用於驗證的 TXT 記錄。在此範例中，我們有兩個 TXT 記錄可用於驗證。

```
-----
Please deploy a DNS TXT record under the name
_acme-challenge.example.com with the following value:
9vuaf232Bz0War8BUx3dTNBDpo6lm_4CDX4fpx4reoo
Before continuing, verify the record is deployed.
Press Enter to Continue
-----
Please deploy a DNS TXT record under the name
_acme-challenge.example.com with the following value:
BVkHWl1a0Zhi2UB4BfoSmJV-B_fiSrwfdaf8eBA30dU
Before continuing, verify the record is deployed.
-----
```

- 讓 Lightsail 瀏覽器型 SSH 工作階段保持開啟狀態，您稍後會在本教學課程中回到該工作階段。繼續前往本教學課程的[下一節](#)。

## 步驟 4：新增 TXT 記錄至域的 DNS 區域

新增 TXT 記錄至網域的 DNS 區域可驗證您擁有網域。為了進行示範，我們會使用 Lightsail DNS 區域。然而，通常由網域註冊商託管的其他 DNS 區域可能會採取類似步驟。

### Note

若要深入瞭解如何為您的網域建立 Lightsail DNS 區域，請參閱[在 Lightsail 中建立 DNS 區域以管理網域的 DNS 記錄](#)。

若要將 TXT 記錄新增至您網域的 DNS 區 Lightsail

- 選擇 Lightsail 首頁上的 Domains & DNS (網域和 DNS) 索引標籤。
- 在頁面的 DNS zones (DNS 區域) 部分，選擇您在 Certbot 憑證請求中所指定網域的 DNS 區域。
- 在 DNS 區域編輯器中，選擇 DNS records (DNS 記錄)。
- 選擇 Add record (新增記錄)。
- 在 Record type (記錄類型) 下拉式選單中，選擇 TXT record (TXT 記錄)。
- 將 Let's Encrypt 憑證請求指定的值輸入 Record name (記錄名稱) 和 Responds with (回應內容) 欄位。

### Note

Lightsail 主控台會預先填入您網域的頂點部分。例如，如果您要新增 `_acme-challenge.example.com` 子網域，則只需在文字方塊中輸入 `_acme-challenge`，當您儲存記錄時，Lightsail 會新增 `.example.com` 部分。

- 選擇儲存。
- 重複步驟 4 到 7 以新增第二組由 Let's Encrypt 憑證請求指定的 TXT 記錄。
- 讓 Lightsail 主控台瀏覽器視窗保持開啟狀態，您稍後會在本教學課程中回到該視窗。繼續前往本教學課程的[下一節](#)。

## 步驟 5：確認 TXT 記錄已傳播

使用此公用 MxToolbox 程式來確認 TXT 記錄已傳播至網際網路的 DNS。DNS 記錄傳輸可能需要一些時間，這取決於您的 DNS 託管提供者，以及設定的 DNS 記錄存留時間 (TTL)。在繼續 Certbot 憑證請求之前，請務必完成此步驟，並確認 TXT 記錄已傳播。否則，您的憑證請求會失敗。

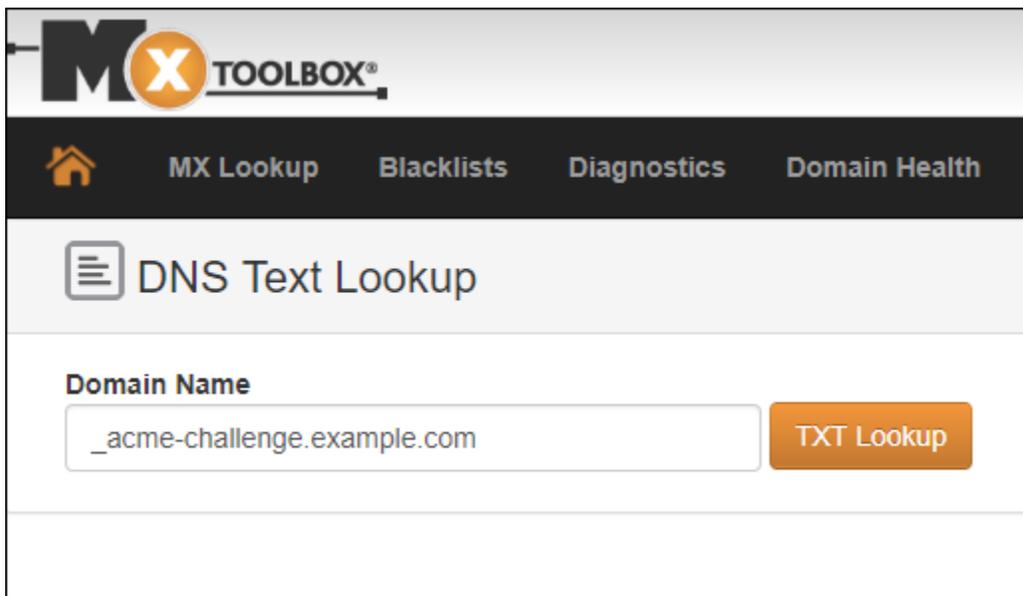
確認 TXT 記錄已傳播至網際網路的 DNS

1. 開啟新的瀏覽器視窗並前往 <https://mxtoolbox.com/TXTLookup.aspx>。
2. 將以下文字輸入文字方塊。請務必以您的網域取代 *domain*。

```
_acme-challenge.domain
```

範例：

```
_acme-challenge.example.com
```



3. 選擇 TXT Lookup (TXT 查詢) 以執行檢查。
4. 這會產生以下其中一個回應：
  - 如果您的 TXT 記錄已傳播至網際網路的 DNS，您會看到類似以下螢幕擷取畫面的回應。關閉瀏覽器視窗，並繼續前往本教學課程的[下一節](#)。

txt:\_acme-challenge.example.com [Find Problems](#) [txt](#)

Type	Domain Name	TTL	Record
TXT	_acme-challenge.example.com	60 sec	9vuaf232Bz0War8BUx3dTNBDpo6lm_4CDX4fpx4reoo
TXT	_acme-challenge.example.com	60 sec	BVkHW11a0Zhi2UB4BfoSmJV-B_fiSrwfdaf8eBA30dU

	Test	Result
✓	DNS Record Published	DNS Record found

Your DNS hosting provider is "Amazon Route 53" [Need Bulk Dns Provider Data?](#)

[dns lookup](#)
[smtp diag](#)
[blacklist](#)
[http test](#)
[dns propagation](#)

Reported by on 10/8/2018 at 8:53:50 PM (UTC 0), [just for you.](#) [Transcript](#)

- 如果 TXT 記錄未傳播至網際網路的 DNS，您會看見 DNS Record not found (找不到 DNS 記錄) 回應。確認您已新增正確 DNS 記錄至網域的 DNS 區域。如果您新增了正確記錄，請再等待片刻讓網域的 DNS 記錄傳播，接著再次執行 TXT 查詢。

## 步驟 6：完成 Let's Encrypt SSL 憑證請求

返回您的 Nginx 執行個體的 Lightsail 瀏覽器型 SSH 工作階段，並完成「讓我們加密」憑證要求。Certbot 將您的 SSL 憑證、鏈及金鑰檔案儲存至您 Nginx 執行個體上的特定目錄。

完成 Let's Encrypt SSL 憑證請求

1. 在您的 Nginx 執行個體的 Lightsail 瀏覽器型 SSH 工作階段中，按 Enter 鍵繼續您的 [讓我們加密 SSL 憑證要求]。如果成功，則會顯示與以下螢幕擷取畫面類似的回應：

```

-----
Please deploy a DNS TXT record under the name
_acme-challenge.example.com with the following value:

9vuaf232Bz0War8BUx3dTNBDpo6lm_4CDX4fpx4reoo

Before continuing, verify the record is deployed.
-----
Press Enter to Continue

-----
Please deploy a DNS TXT record under the name
_acme-challenge.example.com with the following value:

BVkHwll1a0Zhi2UB4BfoSmJV-B_fiSrWfdaf8eBA30dU

Before continuing, verify the record is deployed.
-----
Press Enter to Continue
Waiting for verification...
Cleaning up challenges

IMPORTANT NOTES:
- Congratulations! Your certificate and chain have been saved at:
  /etc/letsencrypt/live/example.com/fullchain.pem
  Your key file has been saved at:
  /etc/letsencrypt/live/example.com/privkey.pem
  Your cert will expire on 2019-01-06. To obtain a new or tweaked
  version of this certificate in the future, simply run certbot
  again. To non-interactively renew *all* of your certificates, run
  "certbot renew"
- If you like Certbot, please consider supporting our work by:

  Donating to ISRG / Let's Encrypt: https://letsencrypt.org/donate
  Donating to EFF:                 https://eff.org/donate-le

bitnami@ip-172-26-1-148:/$ █

```

訊息會確認您的憑證、鏈和金鑰檔案存放於 `/etc/letsencrypt/live/domain/` 目錄。務必以您的網域取代 *domain*，例如 `/etc/letsencrypt/live/example.com/`。

2. 記下訊息中指定的過期日期。您可將其用於在該日期續約憑證。

```

IMPORTANT NOTES:
- Congratulations! Your certificate and chain have been saved at:
  /etc/letsencrypt/live/example.com/fullchain.pem
  Your key file has been saved at:
  /etc/letsencrypt/live/example.com/privkey.pem
  Your cert will expire on 2019-01-06. To obtain a new or tweaked
  version of this certificate in the future, simply run certbot
  again. To non-interactively renew *all* of your certificates, run
  "certbot renew"
- If you like Certbot, please consider supporting our work by:

  Donating to ISRG / Let's Encrypt: https://letsencrypt.org/donate
  Donating to EFF:                 https://eff.org/donate-le

```

- 既然您擁有 Let's Encrypt 憑證，就請繼續前往本教學課程的[下一節](#)。

## 步驟 7：在 Nginx 伺服器目錄中建立 Let's Encrypt 憑證檔案的連結

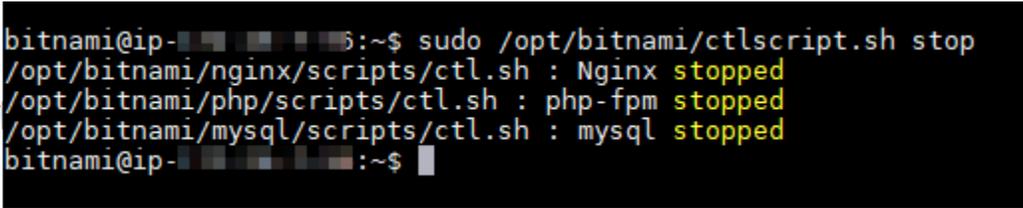
請在 Nginx 執行個體的 Nginx 伺服器目錄中建立 Let's Encrypt SSL 憑證檔案的連結。此外，請備份現有的憑證，以防您稍後需要用到。

若要在 Nginx 伺服器目錄中建立 Let's Encrypt 憑證檔案的連結

- 在 Nginx 執行個體的 Lightsail 瀏覽器型 SSH 工作階段中，輸入下列命令以停止基礎服務：

```
sudo /opt/bitnami/ctlscript.sh stop
```

您應該會看到類似以下的回應：



```
bitnami@ip-100-20-1-100:~$ sudo /opt/bitnami/ctlscript.sh stop
/opt/bitnami/nginx/scripts/ctl.sh : Nginx stopped
/opt/bitnami/php/scripts/ctl.sh : php-fpm stopped
/opt/bitnami/mysql/scripts/ctl.sh : mysql stopped
bitnami@ip-100-20-1-100:~$
```

A red arrow points to the first line of the terminal output, which is the command being executed.

- 輸入下列命令以設定網域的環境變數。您可以更有效率地複製和貼上命令，藉此連結至憑證檔案。請務必以註冊的網域名稱取代 *domain*。

```
DOMAIN=domain
```

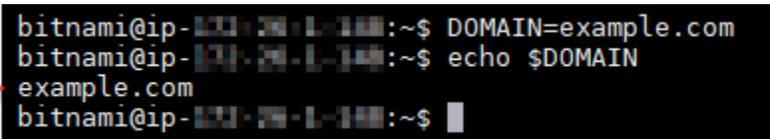
範例：

```
DOMAIN=example.com
```

- 輸入下列命令確認變數傳回正確的值：

```
echo $DOMAIN
```

您應該會看到類似以下的結果：



```
bitnami@ip-100-20-1-100:~$ DOMAIN=example.com
bitnami@ip-100-20-1-100:~$ echo $DOMAIN
example.com
bitnami@ip-100-20-1-100:~$
```

A red arrow points to the output of the echo command, which is example.com.

4. 個別輸入下列命令，以重新命名現有的憑證檔案做為備份。請參閱本教學課程開頭的重要區塊，以取得有關不同發行版本和檔案結構的資訊。

- Debian Linux 發行版本

方法 A (使用系統套件的 Bitnami 安裝)：

```
sudo mv /opt/bitnami/nginx/conf/bitnami/certs/server.crt /opt/bitnami/nginx/conf/bitnami/certs/server.crt.old
```

```
sudo mv /opt/bitnami/nginx/conf/bitnami/certs/server.key /opt/bitnami/nginx/conf/bitnami/certs/server.key.old
```

方法 B (獨立的 Bitnami 安裝)：

```
sudo mv /opt/bitnami/nginx/conf/server.crt /opt/bitnami/nginx/conf/server.crt.old
```

```
sudo mv /opt/bitnami/nginx/conf/server.key /opt/bitnami/nginx/conf/server.key.old
```

- 對於使用 Ubuntu Linux 發行版本的較舊執行個體：

```
sudo mv /opt/bitnami/nginx/conf/bitnami/certs/server.crt /opt/bitnami/nginx/conf/bitnami/certs/server.crt.old
```

```
sudo mv /opt/bitnami/nginx/conf/bitnami/certs/server.key /opt/bitnami/nginx/conf/bitnami/certs/server.key.old
```

5. 個別輸入下列命令，在 Nginx 伺服器目錄中建立 Let's Encrypt 憑證檔案的連結：請參閱本教學課程開頭的重要區塊，以取得有關不同發行版本和檔案結構的資訊。

- Debian Linux 發行版本

方法 A (使用系統套件的 Bitnami 安裝)：

```
sudo ln -sf /etc/letsencrypt/live/$DOMAIN/privkey.pem /opt/bitnami/nginx/conf/bitnami/certs/server.key
```

```
sudo ln -sf /etc/letsencrypt/live/$DOMAIN/fullchain.pem /opt/bitnami/nginx/conf/bitnami/certs/server.crt
```

方法 B (獨立的 Bitnami 安裝) :

```
sudo ln -sf /etc/letsencrypt/live/$DOMAIN/privkey.pem /opt/bitnami/nginx/conf/server.key
```

```
sudo ln -sf /etc/letsencrypt/live/$DOMAIN/fullchain.pem /opt/bitnami/nginx/conf/server.crt
```

- 對於使用 Ubuntu Linux 發行版本的較舊執行個體 :

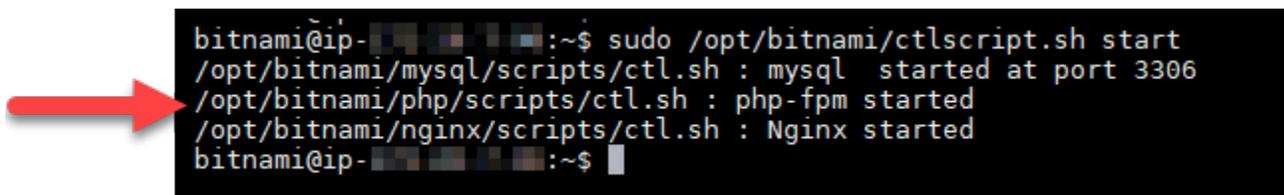
```
sudo ln -s /etc/letsencrypt/live/$DOMAIN/privkey.pem /opt/bitnami/nginx/conf/bitnami/certs/server.key
```

```
sudo ln -s /etc/letsencrypt/live/$DOMAIN/fullchain.pem /opt/bitnami/nginx/conf/bitnami/certs/server.crt
```

6. 輸入下列命令，啟動您稍早停止的基礎服務：

```
sudo /opt/bitnami/ctlscript.sh start
```

您應該會看到類似以下的結果：



```
bitnami@ip-...:~$ sudo /opt/bitnami/ctlscript.sh start
/opt/bitnami/mysql/scripts/ctl.sh : mysql started at port 3306
/opt/bitnami/php/scripts/ctl.sh : php-fpm started
/opt/bitnami/nginx/scripts/ctl.sh : Nginx started
bitnami@ip-...:~$
```

您的 Nginx 執行個體現在已設定為使用 SSL 加密。然而，流量不會從 HTTP 自動重新引導至 HTTPS。

7. 繼續前往本教學課程的[下一節](#)。

## 步驟 8：為 Web 應用程式設定 HTTP 至 HTTPS 重新引導

您可以為您的 Nginx 執行個體設定 HTTP 至 HTTPS 重新引導。從 HTTP 自動重新引導至 HTTPS 會讓客戶只能使用 SSL 存取網站，即使他們使用 HTTP 進行連線也是如此。請參閱本教學課程開頭的重要區塊，以取得有關不同發行版本和檔案結構的資訊。

此教學課程使用 Vim 做為示範；然而，您可以選擇使用任何文字編輯器。

對於 Debian Linux 發行版本 – 為 Web 應用程式設定 HTTP 至 HTTPS 重新導向

1. 在 Nginx 執行個體的 Lightsail 瀏覽器型 SSH 工作階段中，輸入下列命令以修改伺服器區塊設定檔。將 <ApplicationName> 取代為您應用程式的名稱。

```
sudo vim /opt/bitnami/nginx/conf/server_blocks/<ApplicationName>-server-block.conf
```

2. 按 i 進入 Vim 編輯器的插入模式。
3. 使用以下範例中的資訊來編輯檔案：

```
server {
    listen 80 default_server;
    root /opt/bitnami/APPNAME;
    return 301 https://$host$request_uri;
}
```

4. 按 ESC (ESC) 鍵，接著輸入 :wq 以寫入 (儲存) 您的編輯，然後退出 Vim。
5. 輸入以下命令來修改 Nginx 組態檔案的伺服器部分：

```
sudo vim /opt/bitnami/nginx/conf/nginx.conf
```

6. 按 i 進入 Vim 編輯器的插入模式。
7. 使用以下範例中的資訊來編輯檔案：

```
server {
    listen 80;
    server_name localhost;
    return 301 https://$host$request_uri;
}
```

8. 按 ESC (ESC) 鍵，接著輸入 :wq 以寫入 (儲存) 您的編輯，然後退出 Vim。
9. 輸入下列命令來重新啟動基礎服務，並讓您的編輯生效：

```
sudo /opt/bitnami/ctlscript.sh restart
```

方法 B (獨立的 Bitnami 安裝) :

1. 在您的 Nginx 執行個體的 Lightsail 瀏覽器型 SSH 工作階段中，輸入下列指令以修改 Nginx 設定檔的伺服器區段：

```
sudo vim /opt/bitnami/nginx/conf/nginx.conf
```

2. 按 `i` 進入 Vim 編輯器的插入模式。
3. 使用以下範例中的資訊來編輯檔案：

```
server {
    listen 80;
    server_name localhost;
    return 301 https://$host$request_uri;
}
```

4. 按 ESC (ESC) 鍵，接著輸入 `:wq` 以寫入 (儲存) 您的編輯，然後退出 Vim。
5. 輸入下列命令來重新啟動基礎服務，並讓您的編輯生效：

```
sudo /opt/bitnami/ctlscript.sh restart
```

對於使用 Ubuntu Linux 發行版本的舊版執行個體 - 為 Web 應用程式設定 HTTP 至 HTTPS 重新導向

1. 在您的 Nginx 執行個體的 Lightsail 瀏覽器型 SSH 工作階段中，輸入下列指令，以使用 Vim 文字編輯器編輯 Nginx 網頁伺服器設定檔：

```
sudo vim /opt/bitnami/nginx/conf/bitnami/bitnami.conf
```

2. 按 `i` 進入 Vim 編輯器的插入模式。
3. 在檔案中，於 `server_name localhost;` 和 `include "/opt/bitnami/nginx/conf/bitnami/bitnami-apps-prefix.conf";` 之間輸入以下文字：

```
return 301 https://$host$request_uri;
```

結果應如下列範例所示：

```
server {
    listen      80;
    server_name localhost;

    include "/opt/bitnami/nginx/conf/bitnami/phpfastcgi.conf";
    return 301 https://$host$request_uri;

    include "/opt/bitnami/nginx/conf/bitnami/bitnami-apps-prefix.conf";
}
```

4. 按 ESC (ESC) 鍵，接著輸入 :wq 以寫入 (儲存) 您的編輯，然後退出 Vim。
5. 輸入下列命令來重新啟動基礎服務，並讓您的編輯生效：

```
sudo /opt/bitnami/ctlscript.sh restart
```

您的 Nginx 執行個體現在已設定為自動將連線從 HTTP 重新引導至 HTTPS。當訪客前往 `http://www.example.com` 時，系統會自動重新引導至加密的 `https://www.example.com` 地址。

## 步驟 9：每 90 天續約 Let's Encrypt 憑證

Let's Encrypt 憑證有效期為 90 天。您可以憑證過期前 30 天內進行續約。若要更新 Let's Encrypt 憑證，請執行原始命令來取得憑證。重複本教學課程的[請求 Let's Encrypt SSL 萬用字元憑證](#)一節中的步驟。

## 使用免費的讓我們加密 SSL 憑 WordPress 證來保護您的 Lightsail 執行個體

### Tip

Amazon Lightsail 提供引導式工作流程，可自動執行個體上「讓我們加密」憑證的安裝和設定。WordPress 我們強烈建議您使用工作流程，而不要遵循本教學課程中的手動步驟。如需詳細資訊，請參閱[啟動和設定 WordPress 執行個體](#)。

透過使用 Lightsail 負載平衡器，Lightsail 可讓您輕鬆地透過 SSL/TLS 來保護您的網站和應用程式。但是，使用 Lightsail 負載平衡器通常不是正確的選擇。或許您的網站不需要負載平衡器提供的可擴展性或容錯能力，或者您是要最佳化成本。在後者的情況中，您可能會考量使用 Let's Encrypt 以取得免費的 SSL 憑證。若是如此，則無問題。您可以將這些憑證與 Lightsail 執行個體整合。

透過本指南，您將學習如何使用 Certbot 申請讓我們加密萬用字元憑證，並使用真正簡單的 SSL 外掛程式將其與您的 WordPress 執行個體整合。

- Bitnami 執行個體所使用的 Linux 發行版本已在 2020 年 7 月從 Ubuntu 變更為 Debian。由於這項變更，本教學課程中的部分步驟會根據執行個體的 Linux 發行版本而有所不同。變更後才建立的所有 Bitnami 藍圖執行個體均會使用 Debian Linux 發行版本。在變更之前建立的執行個體將繼續使用 Ubuntu Linux 發行版本。若要檢查執行個體的分發，請執行 `uname -a` 命令。該回應會將執行個體的 Linux 發行版本顯示為 Ubuntu 或 Debian。
- Bitnami 已經修改了許多堆棧的文件結構。本教學課程中的檔案路徑可能會根據您的 Bitnami 堆疊是否使用原生 Linux 系統套件 (方法 A)，或是否為獨立安裝 (方法 B) 而變更。若要識別您的 Bitnami 安裝類型以及要遵循的方法，請執行下列命令

```
test ! -f "/opt/bitnami/common/bin/openssl" && echo "Approach A: Using system packages." || echo "Approach B: Self-contained installation."
```

## 內容

- [開始之前](#)
- [步驟 1：完成先決條件](#)
- [步驟 2：在您的執行個體上安裝 Certbot](#)
- [步驟 3：請求 Let's Encrypt SSL 萬用字元憑證](#)
- [步驟 4：新增 TXT 記錄至域的 DNS 區域](#)
- [步驟 5：確認 TXT 記錄已傳播](#)
- [步驟 6：完成 Let's Encrypt SSL 憑證請求](#)
- [步驟 7：在 Apache 伺服器目錄中建立連結到 Let's Encrypt 憑證檔案](#)
- [步驟 8：使用非常簡單的 SSL 插件將 SSL 證書與您的 WordPress 網站集成](#)
- [步驟 9：每 90 天續約 Let's Encrypt 憑證](#)

## 開始之前

開始本教學課程之前，您應該考量下列事項：

### 改用 Bitnami HTTPS 組態 (**bncert**) 工具

本教學課程介紹了如何透過手動程序來實作 SSL/TLS 憑證。但是，Bitnami 提供了一個更自動化的過程，它使用了 Bitnami HTTPS 配置 (`bncert`) 工具，該工具通常預先安裝在 Lightsail 中的實例

上 WordPress。我們強烈建議您使用該工具，而非依照本教學課程中的手動步驟。本教學課程是在 bncert 工具可供使用之前完成。如需使用此 bncert 工具的詳細資訊，請參閱 [在您的 WordPress 執行個體上啟用 HTTPS](#)。

## 識別執行個體的 Linux 發行版本

Bitnami 執行個體所使用的 Linux 發行版本已在 2020 年 7 月從 Ubuntu 變更為 Debian。變更後才建立的所有 Bitnami 藍圖執行個體均會使用 Debian Linux 發行版本。在變更之前建立的執行個體將繼續使用 Ubuntu Linux 發行版本。由於這項變更，本教學課程中的部分步驟會根據執行個體的 Linux 發行版本而有所不同。您必須識別執行個體的 Linux 發行版本，以便您知道本教學課程中要使用哪些步驟。若要識別執行個體的 Linux 發行版本，請執行 `uname -a` 命令。該回應會將執行個體的 Linux 發行版本顯示為 Ubuntu 或 Debian。

## 確定適用於您的執行個體之教學課程

Bitnami 正在修改其許多堆疊的檔案結構。本教學課程中的檔案路徑可能會根據您的 Bitnami 堆疊是否使用原生 Linux 系統套件 (方法 A)，或是否為獨立安裝 (方法 B) 而變更。若要識別您的 Bitnami 安裝類型以及要遵循的方法，請執行下列命令

```
test ! -f "/opt/bitnami/common/bin/openssl" && echo "Approach A: Using system packages." || echo "Approach B: Self-contained installation."
```

## 步驟 1：完成先決條件

請先完成事前準備 (若尚未完成)：

- 在 Light WordPress sail 中建立實體。若要進一步了解，請參閱 [建立執行個體](#)。
- 註冊網域名稱，並取得管理存取以編輯其 DNS 記錄。若要進一步了解，請參閱 [DNS](#)。

建議您使用 Lightsail DNS 區域管理網域的 DNS 記錄。若要進一步了解，請參閱 [建立 DNS 區域以管理域的 DNS 記錄](#)。

- 使用 Lightsail 主控台中以瀏覽器為基礎的 SSH 終端機來執行本教學課程中的步驟。然而，您也可以使用自己的 SSH 用戶端，例如 PuTTY。若要進一步了解如何設定 PuTTY，請參閱 [在 Amazon Lightsail 中下載和設定 PuTTY 以使用 SSH 進行連線](#)。

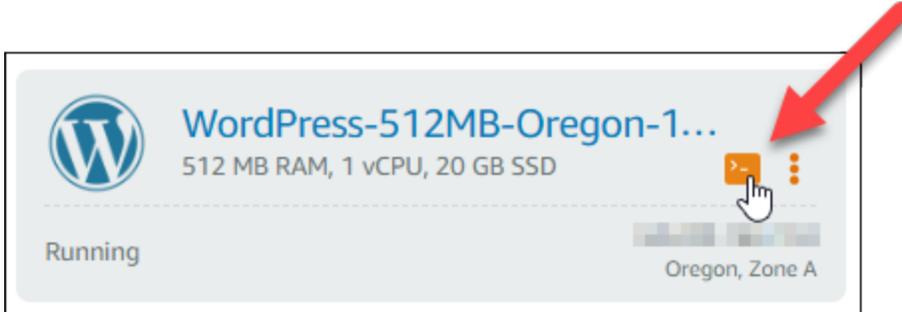
完成先決條件後，請繼續前往本教學課程的 [下一節](#)。

## 步驟 2：在您的執行個體上安裝 Certbot

Certbot 是一種用戶端，用於從 Let's Encrypt 請求憑證並將其部署至 Web 伺服器。Let's Encrypt 使用 ACME 協助發出憑證，而 Certbot 是一種啟用 ACME 的用戶端，可與 Let's Encrypt 互動。

若要在您的執行個體上安裝切爾特博特

1. 登入主 [Lightsail](#) 台。
2. 在 Lightsail 首頁上，針對您要連線的執行個體選擇安全殼層快速連線圖示。



3. 連線 Lightsail 瀏覽器型 SSH 工作階段之後，請輸入下列命令以更新執行個體上的套件：

```
sudo apt-get update
```

```
Welcome to Ubuntu 16.04.5 LTS (GNU/Linux 4.4.0-1070-aws x86_64)

   ____          _ _   ____ 
  /  _ \        / \  /  _ \
 | | | |       / _ \| | | |
 | |_| |      / ___ \| |_| |
  \___/      /_/  _\___/

*** Welcome to the Bitnami WordPress 4.9.8-0 ***
*** Documentation: https://docs.bitnami.com/aws/apps/wordpress/ ***
***                  https://docs.bitnami.com/aws/ ***
*** Bitnami Forums: https://community.bitnami.com/ ***
Last login: Tue Oct 30 14:22:03 2018 from [redacted]
bitnami@ip-[redacted]:~$ sudo apt-get update
```

4. 輸入下列命令以安裝軟體屬性套件。Certbot 的開發人員使用個人套件存檔 (PPA) 分發 Certbot。軟體屬性套件可讓 PPA 的使用更有效率。

```
sudo apt-get install software-properties-common
```

**Note**

如果您在執行 `Could not get lock` 命令時遭遇 `sudo apt-get install` 錯誤，請等待大約 15 分鐘後再試一次。此錯誤可能是由使用 Apt 套件管理工具安裝自動升級的 cron 任務所引起的。

5. 輸入下列命令以安裝 GPG 套件，並新增 Certbot 至本機 apt 儲存庫：

**Note**

步驟 5 僅適用於使用 Ubuntu Linux 發行版本的執行個體。如果您的執行個體使用 Debian Linux 發行版本，請略過此步驟。

```
sudo apt-get install gpg -y
```

```
sudo apt-add-repository ppa:certbot/certbot -y
```

6. 輸入下列命令更新 apt 以包含新的儲存庫：

```
sudo apt-get update -y
```

7. 輸入下列命令以安裝 Certbot：

```
sudo apt-get install certbot -y
```

現在，Certbot 已安裝在您的執行個體上。

8. 讓瀏覽器型 SSH 終端機視窗保持開啟 - 稍後您會在此教學課程中回到此處。繼續前往本教學課程的[下一節](#)。

### 步驟 3：請求 Let's Encrypt SSL 萬用字元憑證

開始從 Let's Encrypt 請求憑證的程序。使用 Certbot (請求萬用字元憑證) 可讓您針對網域及其子網域使用單一憑證。例如，單一萬用字元憑證適用於 `example.com` 頂層網域，以及 `blog.example.com`、`stuff.example.com` 子網域。

## 請求 Let's Encrypt SSL 萬用字元憑證

1. 在與本教學課程[步驟 2](#) 使用的相同瀏覽器型 SSH 終端機視窗中，輸入下列命令為您的網域設定環境變數。您現在可以更有效率複製和貼上命令以取得憑證。請務必以註冊的網域名稱取代 *domain*。

```
DOMAIN=domain
```

```
WILDCARD=*.$DOMAIN
```

範例：

```
DOMAIN=example.com
```

```
WILDCARD=*.$DOMAIN
```

2. 輸入下列命令確認變數傳回正確的值：

```
echo $DOMAIN && echo $WILDCARD
```

您應該會看到類似以下的結果：



```
bitnami@ip-172-31-1-141:~$ DOMAIN=example.com
bitnami@ip-172-31-1-141:~$ WILDCARD=*.$DOMAIN
bitnami@ip-172-31-1-141:~$ echo $DOMAIN && echo $WILDCARD
example.com
*.example.com
bitnami@ip-172-31-1-141:~$
```

3. 在互動式模式中輸入下列命令啟動 Certbot。此命令會通知 Certbot 使用手動授權方法搭配 DNS 查問以驗證網域所有權。這會為您的頂層網域及其子網域請求萬用字元憑證。

```
sudo certbot -d $DOMAIN -d $WILDCARD --manual --preferred-challenges dns certonly
```

4. 在提示時輸入您的電子郵件地址，這會用於續約和安全性注意事項。
5. 閱讀 Let's Encrypt 服務條款。完成時，如果您同意請按 A。如果您不同意，就無法取得 Let's Encrypt 憑證。
6. 根據分享您電子郵件地址的提示和關於您 IP 地址被記錄的警告做出回應。

- Let's Encrypt 現在會提示您確認您擁有所指定的網域。要這麼做，請新增 TXT 記錄至網域的 DNS 記錄。這會提供一組 TXT 記錄值，如以下範例所示：

**Note**

Let's Encrypt 可能會提供一或多個必須用於驗證的 TXT 記錄。在此範例中，我們有兩個 TXT 記錄可用於驗證。

```
-----  
Please deploy a DNS TXT record under the name  
_acme-challenge.example.com with the following value:  
9vuaf232Bz0War8BUx3dTnBDpo6lm_4CDX4fpx4reoo  
Before continuing, verify the record is deployed.  
Press Enter to Continue  
-----  
Please deploy a DNS TXT record under the name  
_acme-challenge.example.com with the following value:  
BvkHWl1a0Zhi2UB4BfoSmJV-B_fiSrwfdaf8eBA30dU  
Before continuing, verify the record is deployed.  
-----
```

- 保持以 Lightsail 瀏覽器為基礎的 SSH 工作階段開啟，您稍後會在本教學課程中返回。繼續前往本教學課程的[下一節](#)。

#### 步驟 4：新增 TXT 記錄至域的 DNS 區域

新增 TXT 記錄至網域的 DNS 區域可驗證您擁有網域。為了進行示範，我們使用 Lightsail DNS 區域。然而，通常由網域註冊商託管的其他 DNS 區域可能會採取類似步驟。

**Note**

若要深入瞭解如何為您的網域建立 Lightsail DNS 區域，請參閱[在 Lightsail 中建立 DNS 區域以管理網域的 DNS 記錄](#)。

## 若要將 TXT 記錄新增至您網域的 DNS 區 Lightsail

1. 選擇 Lightsail 首頁上的 Domains & DNS (網域和 DNS) 索引標籤。
2. 在頁面的 DNS zones (DNS 區域) 部分，選擇您在 Certbot 憑證請求中所指定網域的 DNS 區域。
3. 在 DNS 區域編輯器中，選擇 DNS records (DNS 記錄)。
4. 選擇 Add record (新增記錄)。
5. 在 Record type (記錄類型) 下拉式選單中，選擇 TXT record (TXT 記錄)。
6. 將 Let's Encrypt 憑證請求指定的值輸入 Record name (記錄名稱) 和 Responds with (回應內容) 欄位。

### Note

Lightsail 主控台會預先填入您網域的頂點部分。例如，如果您要新增 `_acme-challenge.example.com` 子網域，則只需在文字方塊中輸入 `_acme-challenge`，當您儲存記錄時，Lightsail 會新增 `.example.com` 部分。

7. 選擇儲存。
8. 重複步驟 4 到 7 以新增第二組由 Let's Encrypt 憑證請求指定的 TXT 記錄。
9. 讓 Lightsail 主控台瀏覽器視窗保持開啟，您稍後會在本教學課程中返回。繼續前往本教學課程的[下一節](#)。

## 步驟 5：確認 TXT 記錄已傳播

使用此公用 MxToolbox 程式來確認 TXT 記錄已傳播至網際網路的 DNS。DNS 記錄傳輸可能需要一些時間，這取決於您的 DNS 託管提供者，以及設定的 DNS 記錄存留時間 (TTL)。在繼續 Certbot 憑證請求之前，請務必完成此步驟，並確認 TXT 記錄已傳播。否則，您的憑證請求會失敗。

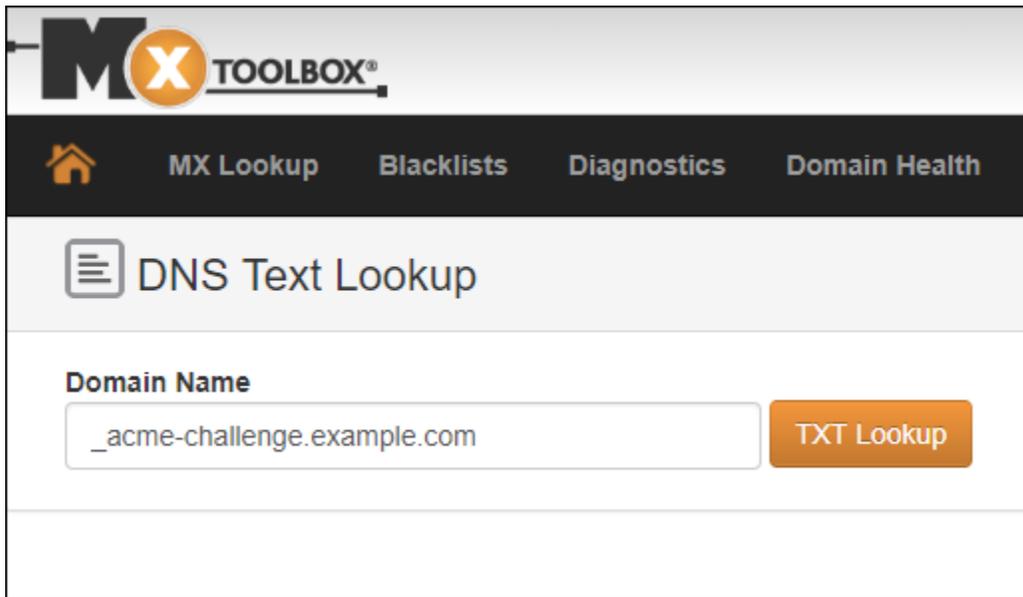
### 確認 TXT 記錄已傳播至網際網路的 DNS

1. 開啟新的瀏覽器視窗並前往 <https://mxtoolbox.com/TXTLookup.aspx>。
2. 將以下文字輸入文字方塊。請務必以您的網域取代 `domain`。

```
_acme-challenge.domain
```

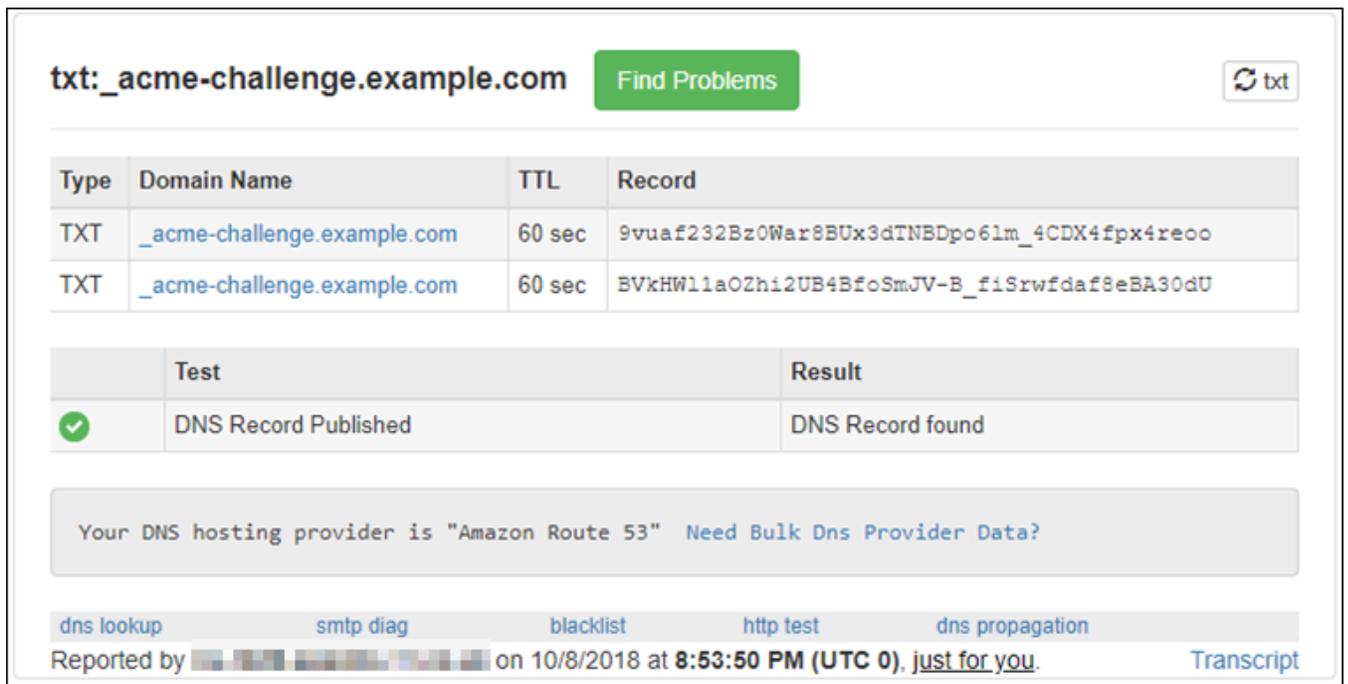
範例：

`_acme-challenge.example.com`



The screenshot shows the MX Toolbox website's 'DNS Text Lookup' page. At the top, there is a navigation bar with a home icon and links for 'MX Lookup', 'Blacklists', 'Diagnostics', and 'Domain Health'. Below this, the page title is 'DNS Text Lookup'. A form is present with a 'Domain Name' input field containing the text '\_acme-challenge.example.com' and an orange 'TXT Lookup' button to its right.

3. 選擇 TXT Lookup (TXT 查詢) 以執行檢查。
4. 這會產生以下其中一個回應：
  - 如果您的 TXT 記錄已傳播至網際網路的 DNS，您會看到類似以下螢幕擷取畫面的回應。關閉瀏覽器視窗，並繼續前往本教學課程的[下一節](#)。



The screenshot displays the results of a DNS lookup for the domain `txt:_acme-challenge.example.com`. At the top, there is a search bar with the domain name and a green 'Find Problems' button. Below the search bar is a table with the following data:

Type	Domain Name	TTL	Record
TXT	<a href="#">_acme-challenge.example.com</a>	60 sec	9vuaf232Bz0War8BUx3dTNBDpo6lm_4CDX4fpx4reoo
TXT	<a href="#">_acme-challenge.example.com</a>	60 sec	BVkhW11aOZhi2UB4BfoSmJV-B_fiSrwfdaf8eBA30dU

Below the table is another table with the following data:

	Test	Result
✓	DNS Record Published	DNS Record found

At the bottom of the screenshot, there is a message: "Your DNS hosting provider is 'Amazon Route 53' Need Bulk Dns Provider Data?". Below this message are several navigation links: "dns lookup", "smtp diag", "blacklist", "http test", and "dns propagation". At the very bottom, there is a footer that reads: "Reported by [blurred] on 10/8/2018 at 8:53:50 PM (UTC 0), just for you. Transcript".

- 如果 TXT 記錄未傳播至網際網路的 DNS，您會看見 DNS Record not found (找不到 DNS 記錄) 回應。確認您已新增正確 DNS 記錄至網域的 DNS 區域。如果您新增了正確記錄，請再等待片刻讓網域的 DNS 記錄傳播，接著再次執行 TXT 查詢。

## 步驟 6：完成 Let's Encrypt SSL 憑證請求

返回 WordPress 執行個體的 Lightsail 瀏覽器型 SSH 工作階段，並完成「讓我們加密」憑證要求。Certbot 會將您的 SSL 憑證、鏈結和金鑰檔案儲存到執行個體上的 WordPress 特定目錄中。

### 完成 Let's Encrypt SSL 憑證請求

1. 在 WordPress 執行個體的 Lightsail 瀏覽器型 SSH 工作階段中，按 Enter 繼續您的 [讓我們加密 SSL 憑證要求]。如果成功，則會顯示與以下螢幕擷取畫面類似的回應：

```
-----
Please deploy a DNS TXT record under the name
_acme-challenge.example.com  with the following value:

9vuaf232Bz0War8BUx3dTNBDpo6lm_4CDX4fpx4reoo

Before continuing, verify the record is deployed.
-----
Press Enter to Continue

-----
Please deploy a DNS TXT record under the name
_acme-challenge.example.com  with the following value:

BVkHwll1a0Zhi2UB4BfoSmJV-B_fiSrwdaf8eBA30dU

Before continuing, verify the record is deployed.
-----
Press Enter to Continue
Waiting for verification...
Cleaning up challenges

IMPORTANT NOTES:
- Congratulations! Your certificate and chain have been saved at:
  /etc/letsencrypt/live/example.com/fullchain.pem
  Your key file has been saved at:
  /etc/letsencrypt/live/example.com/privkey.pem
  Your cert will expire on 2019-01-06. To obtain a new or tweaked
  version of this certificate in the future, simply run certbot
  again. To non-interactively renew *all* of your certificates, run
  "certbot renew"
- If you like Certbot, please consider supporting our work by:

  Donating to ISRG / Let's Encrypt:  https://letsencrypt.org/donate
  Donating to EFF:                  https://eff.org/donate-le

bitnami@ip-172-26-1-148:/$
```

訊息會確認您的憑證、鏈和金鑰檔案存放於 `/etc/letsencrypt/live/domain/` 目錄。務必以您的網域取代 *domain*，例如 `/etc/letsencrypt/live/example.com/`。

2. 記下訊息中指定的過期日期。您可將其用於在該日期續約憑證。

```
IMPORTANT NOTES:
- Congratulations! Your certificate and chain have been saved at:
  /etc/letsencrypt/live/example.com/fullchain.pem
  Your key file has been saved at:
  /etc/letsencrypt/live/example.com/privkey.pem
  Your cert will expire on 2019-01-06. To obtain a new or tweaked
  version of this certificate in the future, simply run certbot
  again. To non-interactively renew *all* of your certificates, run
  "certbot renew"
- If you like Certbot, please consider supporting our work by:

  Donating to ISRG / Let's Encrypt:  https://letsencrypt.org/donate
  Donating to EFF:                  https://eff.org/donate-le
```

3. 既然您擁有 Let's Encrypt 憑證，就請繼續前往本教學課程的 [下一節](#)。

## 步驟 7：在 Apache 伺服器目錄中建立連結到 Let's Encrypt 憑證檔案

在 WordPress 執行個體上的 Apache 伺服器目錄中建立「讓我們加密 SSL 憑證檔案」的連結。此外，請備份現有的憑證，以防您稍後需要用到。

若要在 Apache 伺服器目錄建立至 Let's Encrypt 憑證檔案的連結

1. 在 WordPress 執行個體的 Lightsail 瀏覽器型 SSH 工作階段中，輸入下列命令以停止基礎服務：

```
sudo /opt/bitnami/ctlscript.sh stop
```

您應該會看到類似以下的回應：

```
bitnami@ip-172-31-0-141:~$ sudo /opt/bitnami/ctlscript.sh stop
Syntax OK
/opt/bitnami/apache2/scripts/ctl.sh : httpd stopped
/opt/bitnami/php/scripts/ctl.sh : php-fpm stopped
/opt/bitnami/mysql/scripts/ctl.sh : mysql stopped
bitnami@ip-172-31-0-141:~$
```

2. 輸入下列命令以設定網域的環境變數。您可以更有效率地複製和貼上命令，藉此連結至憑證檔案。請務必以註冊的網域名稱取代 *domain*。

```
DOMAIN=domain
```

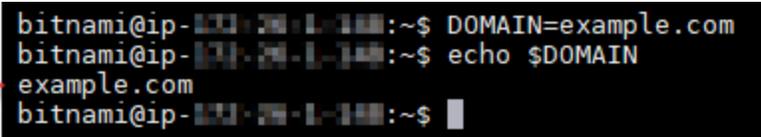
範例：

```
DOMAIN=example.com
```

3. 輸入下列命令確認變數傳回正確的值：

```
echo $DOMAIN
```

您應該會看到類似以下的結果：

A terminal window showing a user named bitnami at an IP address. The user sets the environment variable DOMAIN to example.com, then runs the command echo \$DOMAIN, which outputs example.com. A red arrow points to the output line.

```
bitnami@ip-172-31-1-100:~$ DOMAIN=example.com
bitnami@ip-172-31-1-100:~$ echo $DOMAIN
example.com
bitnami@ip-172-31-1-100:~$
```

4. 個別輸入下列命令，以重新命名現有的憑證檔案做為備份。請參閱本教學課程開頭的重要區塊，以取得有關不同發行版本和檔案結構的資訊。

- Debian Linux 發行版本

方法 A (使用系統套件的 Bitnami 安裝)：

```
sudo mv /opt/bitnami/apache2/conf/bitnami/certs/server.crt /opt/bitnami/apache2/conf/bitnami/certs/server.crt.old
```

```
sudo mv /opt/bitnami/apache2/conf/bitnami/certs/server.key /opt/bitnami/apache2/conf/bitnami/certs/server.key.old
```

方法 B (獨立的 Bitnami 安裝)：

```
sudo mv /opt/bitnami/apache2/conf/server.crt /opt/bitnami/apache2/conf/server.crt.old
```

```
sudo mv /opt/bitnami/apache2/conf/server.key /opt/bitnami/apache2/conf/server.key.old
```

- 對於使用 Ubuntu Linux 發行版本的較舊執行個體：

```
sudo mv /opt/bitnami/apache/conf/bitnami/certs/server.crt /opt/bitnami/apache/conf/bitnami/certs/server.crt.old
```

```
sudo mv /opt/bitnami/apache/conf/bitnami/certs/server.key /opt/bitnami/apache/conf/bitnami/certs/server.key.old
```

```
sudo mv /opt/bitnami/apache/conf/bitnami/certs/server.csr /opt/bitnami/apache/conf/bitnami/certs/server.csr.old
```

5. 個別輸入下列命令，以在 Apache 伺服器目錄中建立至您 Let's Encrypt 憑證檔案的連結：請參閱本教學課程開頭的重要區塊，以取得有關不同發行版本和檔案結構的資訊。

- Debian Linux 發行版本

方法 A (使用系統套件的 Bitnami 安裝)：

```
sudo ln -sf /etc/letsencrypt/live/$DOMAIN/privkey.pem /opt/bitnami/apache2/conf/bitnami/certs/server.key
```

```
sudo ln -sf /etc/letsencrypt/live/$DOMAIN/fullchain.pem /opt/bitnami/apache2/conf/bitnami/certs/server.crt
```

方法 B (獨立的 Bitnami 安裝)：

```
sudo ln -sf /etc/letsencrypt/live/$DOMAIN/privkey.pem /opt/bitnami/apache2/conf/server.key
```

```
sudo ln -sf /etc/letsencrypt/live/$DOMAIN/fullchain.pem /opt/bitnami/apache2/conf/server.crt
```

- 對於使用 Ubuntu Linux 發行版本的較舊執行個體：

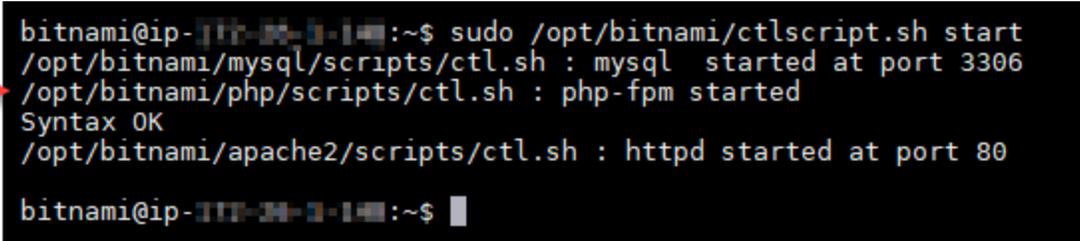
```
sudo ln -s /etc/letsencrypt/live/$DOMAIN/privkey.pem /opt/bitnami/apache/conf/bitnami/certs/server.key
```

```
sudo ln -s /etc/letsencrypt/live/$DOMAIN/fullchain.pem /opt/bitnami/apache/conf/bitnami/certs/server.crt
```

6. 輸入下列命令，啟動您先前停止的基礎服務：

```
sudo /opt/bitnami/ctlscript.sh start
```

您應該會看到類似以下的結果：



```
bitnami@ip-10-10-10-10:~$ sudo /opt/bitnami/ctlscript.sh start
/opt/bitnami/mysql/scripts/ctl.sh : mysql started at port 3306
/opt/bitnami/php/scripts/ctl.sh : php-fpm started
Syntax OK
/opt/bitnami/apache2/scripts/ctl.sh : httpd started at port 80
bitnami@ip-10-10-10-10:~$
```

您 WordPress 執行個體的 SSL 憑證檔案現在位於正確的目錄中。

7. 繼續前往本教學課程的[下一節](#)。

## 步驟 8：使用非常簡單的 SSL 插件將 SSL 證書與您的 WordPress 網站集成

將真正簡單的 SSL 插件安裝到您的 WordPress 網站，並使用它來集成 SSL 證書。Really Simple SSL 也會設定 HTTP 至 HTTPS 重新引導，以確保存取您網站的使用者一律在 HTTPS 連線上。

使用非常簡單的 SSL 外掛程式將 SSL 憑證與您的 WordPress 網站整合

1. 在 WordPress 執行個體的 Lightsail 瀏覽器型 SSH 工作階段中，輸入下列指令，將您的 wp-config.php 和 htaccess.conf 檔案設定為可寫入。Really Simple SSL 外掛程式將寫入 wp-config.php 檔案來設定您的憑證。

- 對於使用 Debian Linux 發行版本的較新執行個體：

```
sudo chmod 666 /opt/bitnami/wordpress/wp-config.php && sudo chmod 666 /opt/bitnami/apache/conf/vhosts/htaccess/wordpress-htaccess.conf
```

- 對於使用 Ubuntu Linux 發行版本的較舊執行個體：

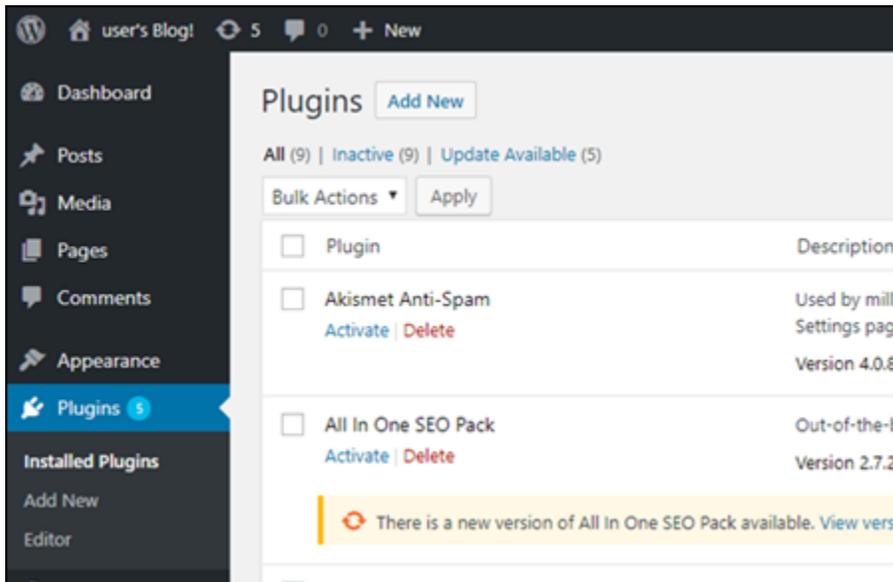
```
sudo chmod 666 /opt/bitnami/apps/wordpress/htdocs/wp-config.php && sudo chmod 666 /opt/bitnami/apps/wordpress/conf/htaccess.conf
```

2. 開啟新的瀏覽器視窗並登入執行個 WordPress 體的管理儀表板。

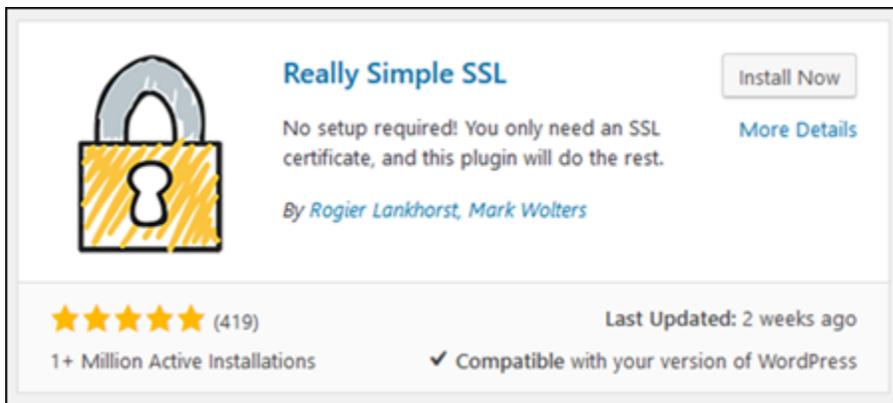
**Note**

如需詳細資訊，請參閱在 [Amazon Lightsail](#) 中取得 Bitnami 執行個體的應用程式使用者名稱和密碼。

3. 從左側導覽窗格中選擇 Plugins (外掛程式)。
4. 從外掛程式頁面最上方選擇 Add New (新增)。



5. 搜尋 Really Simple SSL (Really Simple SSL)。
6. 選擇搜尋結果中 Really Simple SSL 外掛程式旁邊的 Install Now (立即安裝)。



7. 完成安裝之後，選擇 Activate (啟用)。
8. 在系統提示時，選擇 Go ahead, activate SSL! (上吧，啟用 SSL!) 系統可能會將您重新導向至 WordPress 執行個體管理儀表板的登入頁面。

您的 WordPress 執行個體現已設定為使用 SSL 加密。此外，您的 WordPress 執行個體現在已設定為自動將連線從 HTTP 重新導向至 HTTPS。當訪客前往 <http://example.com> 時，系統會自動重新引導至加密的 HTTPS 連線 (也就是 <https://example.com>)。

## 步驟 9：每 90 天續約 Let's Encrypt 憑證

Let's Encrypt 憑證有效期為 90 天。您可以憑證過期前 30 天內進行續約。若要更新 Let's Encrypt 憑證，請執行原始命令來取得憑證。重複本教學課程的[請求 Let's Encrypt SSL 萬用字元憑證](#)一節中的步驟。

請依照您特定執行個體類型的 step-by-step 指示操作。每個主題都提供針對您執行個體的 Linux 發行版 (Ubuntu 或 Debian) 和 Bitnami 安裝類型 (系統套件或獨立套件) 量身打造的詳細指令和設定步驟。通過遵循此主題，您可以使用 Let's Encrypt 中的免費 SSL/TLS 證書來保護 Lightsail 網站和應用程序，從而確保加密的通信並改善訪問者的安全性。

## 為 Lightsail 執行個體設定 IPv6 網路

本節涵蓋下列與 IPv6 在 Lightsail 執行個體藍圖上進行設定的相關主題：

### 主題

- [設定 cPanel 執行個體的 IPv6 連線能力](#)
- [設定 Debian 8 個執行個體的 IPv6 連線能力](#)
- [在 Lightsail 中設定 GitLab 執行個體的 IPv6 連線](#)
- [設定 Nginx 執行個體的 IPv6 連線能力](#)
- [設定 Plesk 執行個體的 IPv6 連線能力](#)
- [設定 Ubuntu 16 執行個體的 IPv6 連線能力](#)

## 設定 cPanel 執行個體的 IPv6 連線能力

在預設情況下，Amazon Lightsail 中的所有執行個體都會指派一個公開和私有 IPv4 地址。您可以選擇 IPv6 為執行個體指派公用 IPv6 位址啟用。如需詳細資訊，請參閱 [Amazon Lightsail IP 地址](#) 和 [啟用或停用 IPv6](#)。

IPv6 針對使用 WHM 藍圖的執行個體啟用後，您必須執行一組額外的步驟，讓執行個體知道其 IPv6 位址。cPanel 在本指南中，我們將向您展示您必須對 WHM 實例 cPanel (& Instance) 執行的其他步驟。

## 必要條件

請先完成事前準備 (若尚未完成)：

- 在 Lightsail 中建立 WHM 實體 cPanel (P)。如需詳細資訊，請參閱[建立執行個體](#)。
- 設定 WHM 執行個體 cPanel (P)。有關更多信息，請參閱[快速入門指南：WHM 在 Amazon Lightsail 上](#)。

### ⚠ Important

請確保已執行所有軟體更新和所需的系統重新開機，然後再繼續執行本指南中的步驟。

- IPv6 為您的 WHM 執行個體啟用 cPanel (P)。如需詳細資訊，請參閱[啟用或停用 IPv6](#)。

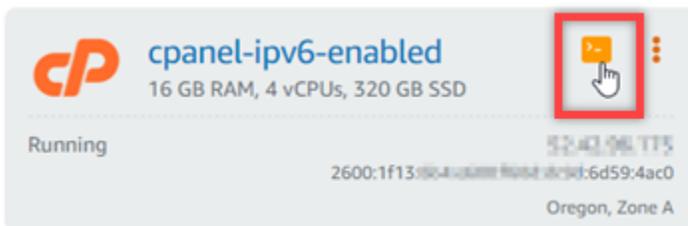
### 📘 Note

在 2021 年 1 月 12 日或之後建立的新 WHM 執行個體 cPanel (A) 在 Lightsail 主控台中建立時，預設會 IPv6 啟用這些執行個體。即使在建立執行個體時預設 IPv6 為啟用，您也必須完成本指南中的下列步驟，才能在執行個體 IPv6 上進行設定。

## 在執行個體 WHM 體 IPv6 上設定 cPanel (P)

請完成下列程序，以在 Lightsail 中的 WHM 執行個體 cPanel 行個體 IPv6 上進行設定。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁的「執行個體」區段中，找出您要設定的 cPanel & WHM 執行個體，然後選擇以瀏覽器為基礎的 SSH 用戶端圖示以使用連線。SSH



3. 連接到執行個體後，請輸入下列命令以使用 Nano 開啟 `ifcfg-eth0` 網路界面組態檔案。

```
sudo nano /etc/sysconfig/network-scripts/ifcfg-eth0
```

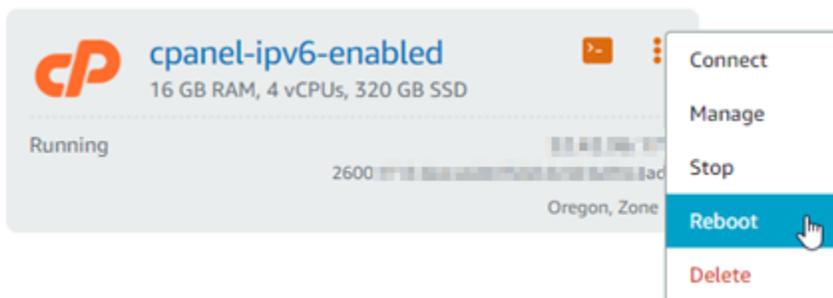
4. 將以下幾行文字新增至檔案 (如果其中尚無這些文字)。

```
IPV6INIT=yes  
IPV6_AUTOCONF=yes  
DHCPV6C=yes
```

結果應如下列範例所示。

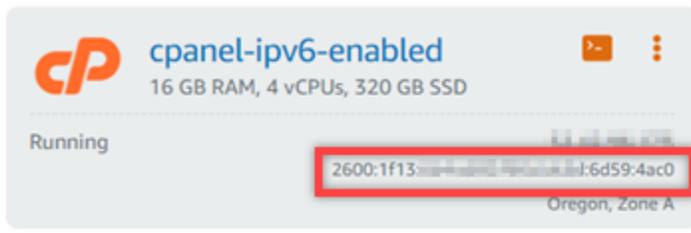
```
Automatically generated by the vm import process  
TYPE=Ethernet  
PROXY_METHOD=none  
BROWSER_ONLY=no  
BOOTPROTO=dhcp  
DEFROUTE=yes  
IPV4_FAILURE_FATAL=no  
NAME=eth0  
DEVICE=eth0  
ONBOOT=yes  
IPV6INIT=yes  
IPV6_FAILURE_FATAL=no  
DHCPV6C=yes  
IPV6_AUTOCONF=yes
```

5. 按鍵盤上的 CTRL+C 退出文件。
6. 出現提示時，按 Y 以儲存修改的緩衝區，然後按 Enter (確認) 以儲存至現有檔案。這樣會儲存您對 `ifcfg-eth0` 網路界面組態檔案進行的編輯。
7. 關閉以瀏覽器為基礎的SSH視窗，然後切換回 Lightsail 主控台。
8. 在 Lightsail 首頁的「執行個體」索引標籤中，選擇WHM執行個體的動作功能表 ( )，然後選擇「重新啟動」。cPanel

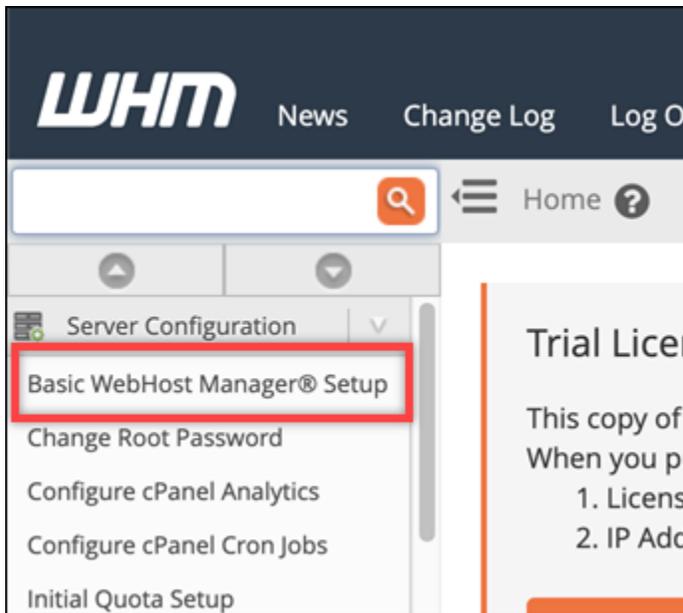


等待數分鐘讓執行個體重新啟動，再繼續進行下一個步驟。

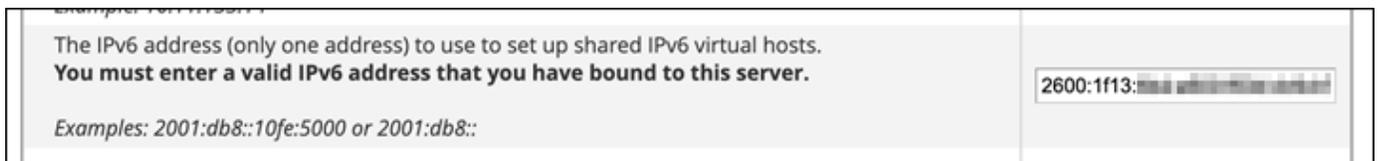
9. 在 Lightsail 首頁的「執行個體」索引標籤中，記下指派給WHM執行個體的IPv6位址。cPanel



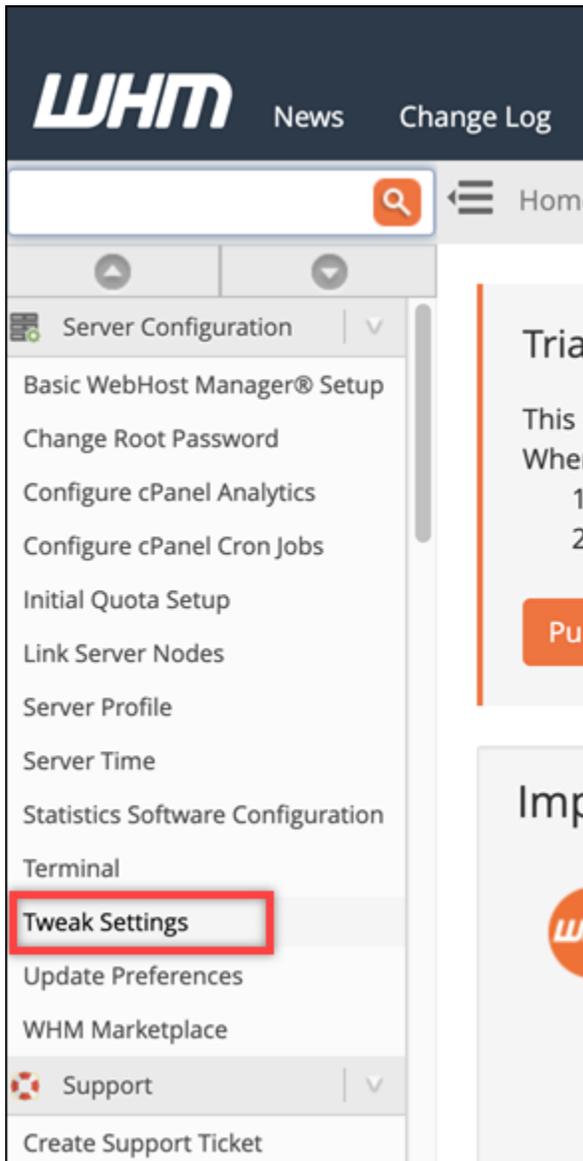
10. 開啟新的瀏覽器索引標籤，然後登入 cPanel & WHM 執行個體的 Web 主機管理員 (WHM)。
11. 在WHM主控台的左側導覽窗格中，選擇 [基本 WebHost 管理員安裝]。



12. 在「全部」索引標籤中，尋找要使用的IPv6地址文字，然後輸入指派給執行個體的IPv6位址。您應該記下本程序步驟 9 中指派給執行個體的IPv6位址。



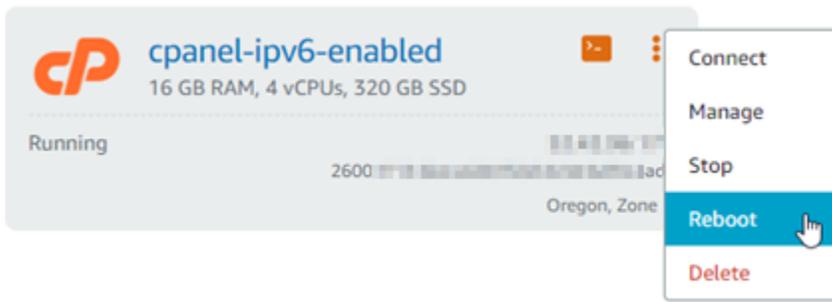
13. 請捲動至頁面底部並選擇 Save Changes (儲存變更)。
14. 在WHM主控台左側導覽窗格中，選擇「微調設定」。



15. 在 [全部] 索引標籤中，向下捲動以尋找 [依IPv6位址接聽] 設定，並將其設定為 [開啟]。

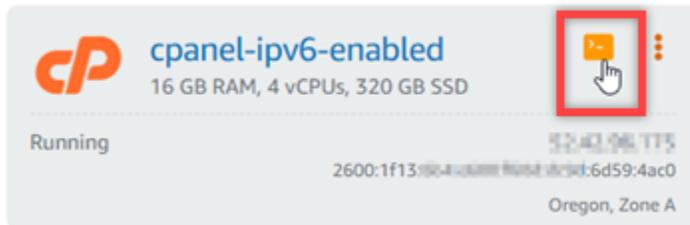


16. 捲動到頁面底部，然後選擇 Save (儲存)。
17. 切換回 Lightsail 主控台。
18. 在 Lightsail 首頁的「執行個體」索引標籤中，選擇WHM執行個體的動作功能表 ()，然後選擇「重新啟動」。cPanel



等待數分鐘讓執行個體重新啟動，再繼續進行下一個步驟。

19. 選擇以瀏覽器為基礎的用SSH戶端圖示，讓WHM執行個體使用SSH連線到它。 cPanel



20. 連線至執行個體後，請輸入下列指令以檢視在執行個體上設定的 IP 位址，並確認執行個體現在正在辨識其指派的位IPv6址。

```
ip addr
```

您將看到類似以下範例的回應。如果您的實例確實識別了它的IPv6地址，那麼您將看到它在響應中列出，並帶有全局範圍的標籤，如本示例所示。

```
[centos@52-42-96-175 ~]$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
   inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc mq state UP group default qlen 1000
   link/ether 02:9b:51:92:50:45 brd ff:ff:ff:ff:ff:ff
   inet 172.31.0.1/20 brd 172.31.0.255 scope global dynamic eth0
       valid_lft 2301sec preferred_lft 2301sec
   inet6 2600:1f13:804::6d59:4ac0/128 scope global dynamic
       valid_lft 112sec preferred_lft 112sec
   inet6 fe80::9015:3fff:f002:5045/64 scope link
       valid_lft forever preferred_lft forever
```

21. 輸入下列命令以確認您的執行個體能夠 ping IPv6 位址。

```
ping6 ipv6.google.com -c 6
```

結果應如下列範例所示，確認您的執行個體能夠 ping IPv6 位址。

```
[centos@52-42-54-173 ~]$ ping6 ipv6.google.com
PING ipv6.google.com(sea15s12-in-x0e.1e100.net (2607:f8b0:400a:809::200e)) 56 data bytes
64 bytes from sea15s12-in-x0e.1e100.net (2607:f8b0:400a:809::200e): icmp_seq=1 ttl=103 time=7.66 ms
64 bytes from sea15s12-in-x0e.1e100.net (2607:f8b0:400a:809::200e): icmp_seq=2 ttl=103 time=7.70 ms
64 bytes from sea15s12-in-x0e.1e100.net (2607:f8b0:400a:809::200e): icmp_seq=3 ttl=103 time=7.68 ms
64 bytes from sea15s12-in-x0e.1e100.net (2607:f8b0:400a:809::200e): icmp_seq=4 ttl=103 time=7.69 ms
64 bytes from sea15s12-in-x0e.1e100.net (2607:f8b0:400a:809::200e): icmp_seq=5 ttl=103 time=7.70 ms
64 bytes from sea15s12-in-x0e.1e100.net (2607:f8b0:400a:809::200e): icmp_seq=6 ttl=103 time=7.68 ms
^C
--- ipv6.google.com ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5008ms
rtt min/avg/max/mdev = 7.667/7.690/7.702/0.052 ms
```

## 設定 Debian 8 個執行個體的IPv6連線能力

在預設情況下，Amazon Lightsail 中的所有執行個體都會指派一個公開和私有IPv4地址。您可以選擇啟用IPv6用讓執行個體指派公用IPv6位址給執行個體。如需詳細資訊，請參閱 [Amazon Lightsail IP 地址](#) 和 [啟用或停用IPv6](#)。

IPv6為使用 Debian 8 藍圖的執行個體啟用後，您必須執行一組額外的步驟，讓執行個體知道其IPv6位址。在本指南中，我們會介紹您必須為 Debian 8 執行個體執行的其他步驟。

### 必要條件

請先完成事前準備 (若尚未完成)：

- 在 Lightsail 中建立一個 Debian 8 執行個體。如需詳細資訊，請參閱 [建立執行個體](#)。
- IPv6為您的 Debian 8 實例啟用。如需詳細資訊，請參閱 [啟用或停用IPv6](#)。

#### Note

在 2021 年 1 月 12 日或之後建立的新 Debian 執行個體在 Lightsail 主控台中建立時，預設會啟用IPv6這些執行個體。即使在建立執行個體時預設IPv6為啟用，您也必須完成本指南中的下列步驟，才能在執行個體IPv6上進行設定。

## IPv6在一個 Debian 8 實例上進行配置

請完成以下程序，以便IPv6在一個 Debian 8 執行個體上進 Lightsail 配置。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁的「實例」部分中，找到您要配置的 Debian 8 實例，然後選擇基於瀏覽器的SSH 客戶端圖標以使用連接到該實例。SSH



3. 連接至執行個體後，輸入下列命令來檢視執行個體上設定的 IP 地址。

```
ip addr
```

您將看到類似以下其中一個範例的回應：

- 如果您的執行個體無法辨識其IPv6位址，您就不會在回應中看到該位址。您應該繼續完成此程序的步驟 4 至 9。

```
admin@ip-172.31.0.1:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 02:9c:ad:11:00:01:00:00:00:00:00:00:ff:ff
    inet 172.31.0.1/20 brd 172.31.0.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::209c:ad11:0001::3df7/64 scope link
        valid_lft forever preferred_lft forever
```

- 如果您的執行個體確實辨識出其IPv6位址，您會看到它在回應中列出，並顯示此範例所示。您應該停在這裡；您不需要完成此程序的步驟 4 到 9，因為您的執行個體已設定為辨識其IPv6位址。

```
admin@ip-172-31-4-228:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 02:9c:84:1d:80:00:00:00:00:00:00:00:ff:ff
    inet 172.31.4.228/24 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 2600:1f13:1500:1000::f383:3212/64 scope global
        valid_lft forever preferred_lft forever
    inet6 fe80::841d:8000:0000:0000:3df7/64 scope link
        valid_lft forever preferred_lft forever
```

4. 輸入下列命令，即可使用 Nano 開啟 interfaces 組態檔案。

```
sudo nano /etc/network/interfaces
```

5. 在檔案的結尾新增下列文字行。

```
iface eth0 inet6 dhcp
```

完成後，檔案會如下所示：

```
GNU nano 2.2.6 File: /etc/network/interfaces
# interfaces(5) file used by ifup(8) and ifdown(8)
# Include files from /etc/network/interfaces.d:
source-directory /etc/network/interfaces.d
auto lo
iface lo inet loopback
auto eth0
iface eth0 inet dhcp

iface eth1 inet dhcp
iface eth2 inet dhcp
iface eth3 inet dhcp
iface eth4 inet dhcp
iface eth5 inet dhcp
iface eth6 inet dhcp
iface eth7 inet dhcp

iface eth0 inet6 dhcp
```

6. 按 Ctrl+Esc 鍵以退出 Nano。
7. 當系統詢問您是否要儲存修改後的緩衝區時，請按 Y，然後按 Enter (確認)，以儲存至現有界面組態檔案。
8. 輸入下列命令，以重新啟動執行個體的聯網服務。

```
sudo systemctl restart networking
```

重新啟動執行個體的網路服務後，您可能需要等待幾分鐘，讓執行個體辨識其IPv6位址。

9. 輸入下列命令以檢視在執行個體上設定的 IP 位址，並確認執行個體現在正在辨識其指派的位IPv6 址。

```
ip addr
```

您將看到類似以下範例的回應。如果您的執行個體確實辨識出其IPv6位址，您會在回應中看到該執行個體的位址，標籤scope global為如此範例所示。

```
admin@ip-172-31-1-22:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
     valid_lft forever preferred_lft forever
   inet6 ::1/128 scope host
     valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP group default qlen 1000
   link/ether 02:9c:42:1f:13:00 brd ff:ff:ff:ff:ff:ff
   inet 172.31.1.22/24 scope global eth0
     valid_lft forever preferred_lft forever
   inet6 2600:1f13:1000:1000:1000:1000:f383:3212/64 scope global
     valid_lft forever preferred_lft forever
   inet6 fe80::209c:42ff:fe1f:1300:3df7/64 scope link
     valid_lft forever preferred_lft forever
```

## 在 Lightsail 中設定 GitLab 執行個體的IPv6連線

在預設情況下，Amazon Lightsail 中的所有執行個體都會指派一個公開和私有IPv4地址。您可以選擇啟用IPv6用讓執行個體指派公用IPv6位址給執行個體。如需詳細資訊，請參閱 [Amazon Lightsail IP 地址](#) 和 [啟用或停用IPv6](#)。

IPv6針對使用 GitLab 藍圖的執行個體啟用後，您必須執行一組額外的步驟，讓執行個體知道其IPv6位址。在本指南中，我們將向您展示您必須針對執行 GitLab 個體執行的其他步驟。

### 必要條件

請先完成事前準備 (若尚未完成)：

- 在 Light GitLab sail 中建立實體。如需詳細資訊，請參閱[建立執行個體](#)。
- IPv6為您的 GitLab 執行個體啟用。如需詳細資訊，請參閱[啟用或停用IPv6](#)。

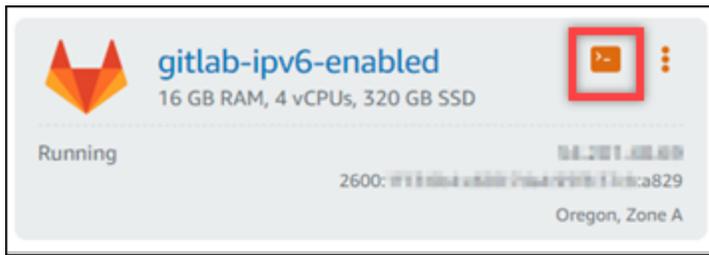
**Note**

在 2021 年 1 月 12 日或之後建立的新 GitLab 執行個體在 Lightsail 主控台中建立時，預設會 IPv6 啟用這些執行個體。即使在建立執行個體時預設 IPv6 為啟用，您也必須完成本指南中的下列步驟，才能在執行個體 IPv6 上進行設定。

## 在 GitLab 執行個體 IPv6 上設定

請完成下列程序，以在 Lightsail 中的 GitLab 執行個體 IPv6 上進行設定。

1. 登入主 [Lightsail](#) 台。
2. 在 Lightsail 首頁的「執行個體」區段中，找出您要設定的 GitLab 執行個體，然後選擇以瀏覽器為基礎的 SSH 用戶端圖示以連線至該執行個體。SSH



3. 連接至執行個體後，輸入下列命令來檢視執行個體上設定的 IP 地址。

```
ip addr
```

您將看到類似以下其中一個範例的回應：

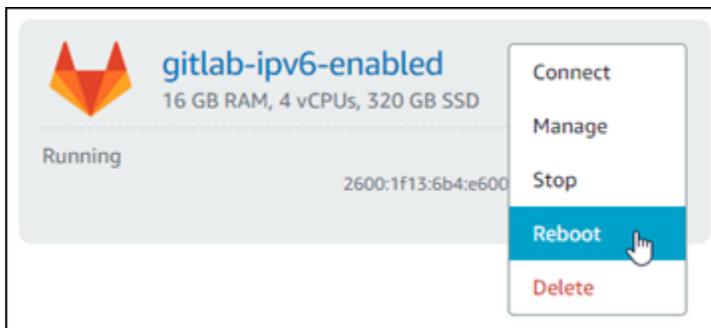
- 如果您的執行個體無法辨識其 IPv6 位址，您就不會在回應中看到該位址。您應該繼續完成此程序的步驟 4 至 9。

```
admin@ip-100-200-1-1:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
   inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP group default qlen 1000
   link/ether 02:9c:ad:11:00:00:00:00:00:00:00:00:ff:ff
   inet 100.200.1.1/24 brd 100.200.1.255 scope global eth0
       valid_lft forever preferred_lft forever
   inet6 fe80::209c:ad11:0000:0000:3df7/64 scope link
       valid_lft forever preferred_lft forever
```

- 如果您的執行個體 `scope global` 確實辨識出其 IPv6 位址，您會看到它在回應中列出，並顯示此範例中所示。您應該停在這裡；您不需要完成此程序的步驟 4 到 9，因為您的執行個體已設定為辨識其 IPv6 位址。

```
admin@ip-172-31-0-228:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 02:9c:84:14:00:00:00:00:00:00:00:00:ff:ff
    inet 172.31.0.228/20 brd 172.31.255.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 2600:1f13:154:1400::1:383:3212/64 scope global
        valid_lft forever preferred_lft forever
    inet6 fe80::8414:0000:0000:0000:3df7/64 scope link
        valid_lft forever preferred_lft forever
```

4. 切換回 Lightsail 主控台。
5. 在 Lightsail 首頁的「執行個體」索引標籤中，選擇 GitLab 執行個體的「動作」功能表 ()，然後選擇「重新開機」。



等待數分鐘讓執行個體重新啟動，再繼續進行下一個步驟。

6. 切換回 GitLab 執行個體的 SSH 工作階段。
7. 輸入下列命令以檢視在執行個體上設定的 IP 位址，並確認執行個體現在正在辨識其指派的位 IPv6 位址。

```
ip addr
```

您將看到類似以下範例的回應。如果您的執行個體確實辨識出其 IPv6 位址，您會在回應中看到該執行個體的位址，標籤 `scope global` 為如此範例所示。

```
admin@ip-172-31-0-23:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 02:9c:40:12:00:01 brd ff:ff:ff:ff:ff:ff
    inet 172.31.0.23/24 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 2600:1f13:1000:1000::f383:3212/64 scope global
        valid_lft forever preferred_lft forever
    inet6 fe80::209c:4012:0001::3df7/64 scope link
        valid_lft forever preferred_lft forever
```

## 設定 Nginx 執行個體的IPv6連線能力

在預設情況下，Amazon Lightsail 中的所有執行個體都會指派一個公開和私有IPv4地址。您可以選擇IPv6為執行個體指派公用IPv6位址啟用。如需詳細資訊，請參閱 [Amazon Lightsail IP 地址](#) 和 [啟用或停用IPv6](#)。

IPv6針對使用 Nginx 藍圖的執行個體啟用後，您必須執行一組額外的步驟，讓執行個體知道其IPv6位址。在本指南中，我們會介紹您必須為 Nginx 執行個體執行的其他步驟。

### 必要條件

請先完成事前準備 (若尚未完成)：

- 在 Lightsail 中建立一個 Nginx 執行個體。如需詳細資訊，請參閱 [建立執行個體](#)。
- IPv6為您的 Nginx 實例啟用。如需詳細資訊，請參閱 [啟用或停用IPv6](#)。

#### 📘 Note

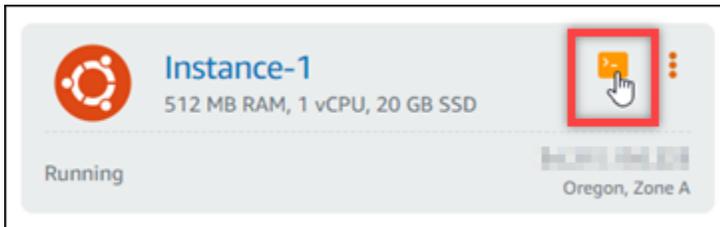
在 2021 年 1 月 12 日或之後建立的新 Nginx 執行個體在 Lightsail 主控台中建立時，預設會 IPv6 啟用這些執行個體。即使在建立執行個體時預設 IPv6 為啟用，您也必須完成本指南中的下列步驟，才能在執行個體 IPv6 上進行設定。

## 在 Nginx 實例IPv6上配置

請完成下列程序，以便在 Lightsail 中的 Nginx 實體 IPv6 上進行設定。

1. 登入主 [Lightsail 台](#)。

- 在 Lightsail 首頁的「執行個體」區段中，找出您要設定的 Ubuntu 16 執行個體，然後選擇瀏覽器型SSH用戶端圖示以使用連線。SSH



- 連線至執行個體後，請輸入下列指令，判斷執行個體是否正在接聽連接埠 80 的IPv6要求。一定要更換 *<IPv6Address>* 分配給您的實例的IPv6地址。

```
curl -g -6 'http://[<IPv6Address>]'
```

範例：

```
curl -g -6 'http://[2001:0db8:85a3:0000:0000:8a2e:0370:7334]'
```

您將看到類似以下其中一個範例的回應：

- 如果您的執行個體未透過連接埠 80 接聽IPv6要求，您會看到回應並顯示連線失敗的錯誤訊息。您應該繼續完成此程序的步驟 4 至 9。

```
bitnami@ip-172-31-1-104:~$ curl -g -6 'http://[2600:1f13:8000:0000:0000:985b:25d9]:80'
curl: (7) Failed to connect to 2600:1f13:8000:0000:0000:985b:25d9 port 80: Connection refused
```

- 如果您的執行個體透過連接埠 80 接聽IPv6要求，您會看到執行個體首頁HTML程式碼的回應，如下列範例所示。您應該在此停止；您不需要完成此程序的步驟 4 到 9，因為您的執行個體已設定為IPv6。

```
bitnami@ip-172-31-1-104:~$ curl -g -6 'http://[2600:1f13:8000:0000:0000:985b:25d9]:80'
<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <title>Bitnami NGINX Open Source</title>
    <meta name="description" content="Bitnami: Open Source. Simplified.">
    <meta name="author" content="Bitnami">
    <link rel="stylesheet" media="screen" href="//unpkg.com/@bitnami/hex/dist/hex.min.css">
  </head>
  <body>
    <main class="margin-t-huge">
      <section aria-labelledby="installation-title" aria-describedby="installation-desc" class="container container-tiny margin-b-gi">
        <h1 id="installation-title">Congratulations!</h1>
        <div aria-hidden="true" style="height: 4px; width: 100%;" class="gradient-135-brand"></div>
        <p id="installation-desc" class="type-big">You are now running <strong>Bitnami NGINX Open Source 1.18.0</strong> in the Clou
      </section>
      <section aria-labelledby="links-title" aria-describedby="links-desc" class="bg-light padding-v-bigger margin-v-enormous">
        <div class="container container-tiny">
          <div class="row row-collapse-b-tablet align-center ">
            <div class="col-6">
              <h3 id="links-title" class="margin-t-reset">Useful Links</h3>
              <p id="links-desc" class="margin-b-reset">The following links will help you to understand better how to get started an
            </div>
          </div>
        </div>
      </section>
    </main>
  </body>
</html>
```

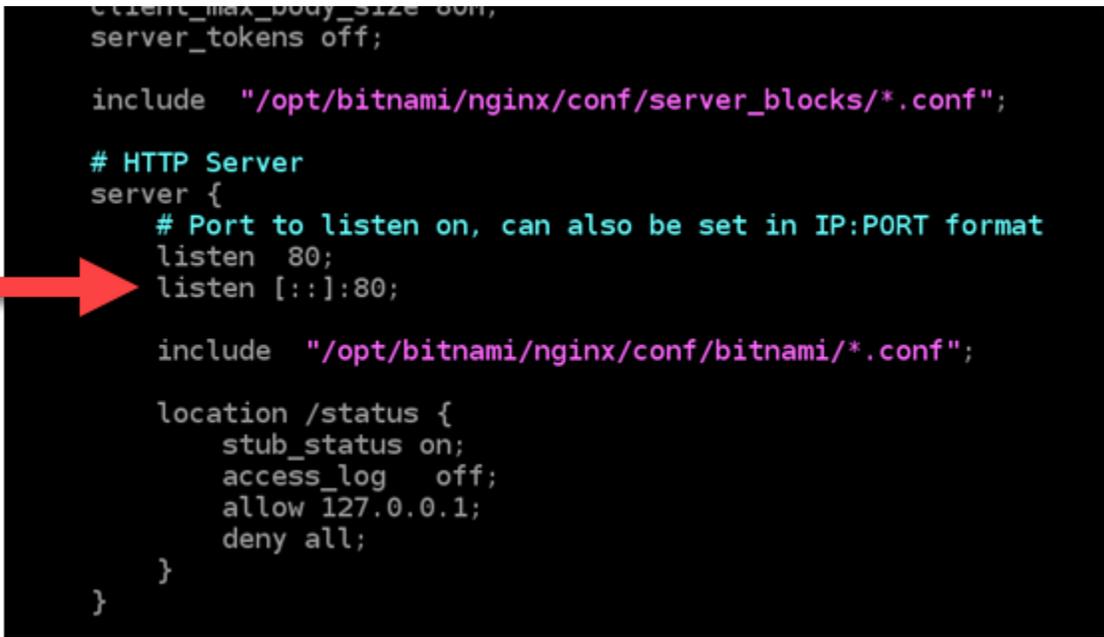
- 輸入下列命令，即可使用 Vim 開啟 nginx.conf 組態檔案。

```
sudo vim /opt/bitnami/nginx/conf/nginx.conf
```

- 在 Vim 中按 I 以進入插入模式。
- 在已經在檔案中的 `listen 80;` 文字下方新增下列文字。您可能需要在 Vim 中向下滾動，查看需要新增文字的部分。

```
listen [::]:80;
```

完成後，檔案會如下所示：



```
client_max_body_size 80m;
server_tokens off;

include "/opt/bitnami/nginx/conf/server_blocks/*.conf";

# HTTP Server
server {
    # Port to listen on, can also be set in IP:PORT format
    listen 80;
    listen [::]:80;

    include "/opt/bitnami/nginx/conf/bitnami/*.conf";

    location /status {
        stub_status on;
        access_log off;
        allow 127.0.0.1;
        deny all;
    }
}
```

- 在 Vim 中按 Esc 鍵以離開插入模式，然後鍵入 `:wq!` 並按 Enter (輸入) 以儲存您的編輯 (寫入)，然後退出 Vim。
- 輸入下列命令，以重新啟動執行個體的服務。

```
sudo /opt/bitnami/ctlscript.sh restart
```

- 輸入下列命令，判斷您的執行個體是否正在接聽通訊埠 80 的 IPv6 要求。一定要更換 `<IPv6Address>` 分配給您的實例的 IPv6 地址。

```
curl -g -6 'http://[<IPv6Address>]'
```

範例：

```
curl -g -6 'http://[2001:0db8:85a3:0000:0000:8a2e:0370:7334]'
```

您將看到類似以下範例的回應。如果您的執行個體透過連接埠 80 接聽IPv6要求，您會看到包含執行個體首頁HTML程式碼的回應。

```
bitnami@ip-10.0.0.1:~$ curl -g -6 'http://[2600:1208:1:2cd0::985b:25d9]:80'
<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <title>Bitnami NGINX Open Source</title>
    <meta name="description" content="Bitnami: Open Source. Simplified.">
    <meta name="author" content="Bitnami">
    <link rel="stylesheet" media="screen" href="//unpkg.com/@bitnami/hex/dist/hex.min.css">
  </head>
  <body>
    <main class="margin-t-huge">
      <section aria-labelledby="installation-title" aria-describedby="installation-desc" class="container container-tiny margin-b-gi
        <h1 id="installation-title">Congratulations!</h1>
        <div aria-hidden="true" style="height: 4px; width: 100%;" class="gradient-135-brand"></div>
        <p id="installation-desc" class="type-big">You are now running <strong>Bitnami NGINX Open Source 1.18.0</strong> in the Clou
      </section>
      <section aria-labelledby="links-title" aria-describedby="links-desc" class="bg-light padding-v-bigger margin-v-enormous">
        <div class="container container-tiny">
          <div class="row row-collapse-b-tablet align-center ">
            <div class="col-6">
              <h3 id="links-title" class="margin-t-reset">Useful Links</h3>
              <p id="links-desc" class="margin-b-reset">The following links will help you to understand better how to get started an
            </div>
          </div>
        </div>
      </section>
    </main>
  </body>
</html>
```

## 設定 Plesk 執行個體的IPv6連線能力

您必須執行一組額外的步驟，才能讓使用 Plesk 藍圖的執行個體感知其IPv6位址。在本指南中，我們會介紹您必須為 Plesk 執行個體執行的其他步驟。

### 必要條件

請先完成事前準備 (若尚未完成)：

- 在 Lightsail 中建立一個 Plesk 執行個體。如需詳細資訊，請參閱[建立執行個體](#)。
- IPv6為您的 Plesk 執行個體啟用。如需詳細資訊，請參閱[啟用或停用IPv6](#)。

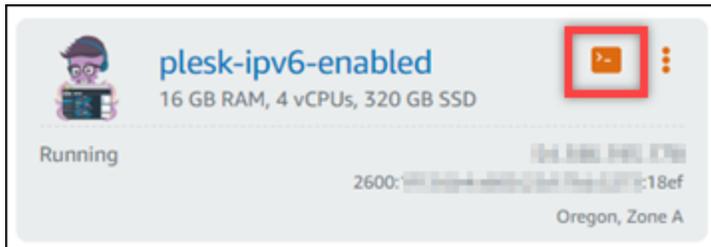
#### Note

在 2021 年 1 月 12 日當天或之後建立的 Lightsail Plesk 執行個體預設為IPv6啟用。即使在建立執行個體時預設IPv6為啟用，您也必須完成本指南中的下列步驟，才能在執行個體IPv6上進行設定。

## 在 Plesk IPv6 執行個體上進行設定

請完成下列程序，以在 Lightsail 中的 Plesk 執行個體 IPv6 上進行設定。

1. 登入主 [Lightsail](#) 台。
2. 在 Lightsail 首頁的「執行個體」區段中，找出您要設定的 Plesk 執行個體，然後選擇以瀏覽器為基礎的 SSH 用戶端圖示以連線至該執行個體。SSH



3. 連接至執行個體後，輸入下列命令來檢視執行個體上設定的 IP 地址。

```
ip addr
```

您將看到類似以下其中一個範例的回應：

- 如果您的執行個體無法辨識其 IPv6 位址，您就不會在回應中看到該位址。您應該繼續完成此程序的步驟 4 至 7。

```
admin@ip-100-200-100-100:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
   inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP group default qlen 1000
   link/ether 02:9c:ad:ff:fe:01:00:00:00:00:00:00:00:00:00:00:ff:ff
   inet 100.200.100.100 brd 100.200.100.255 scope global eth0
       valid_lft forever preferred_lft forever
   inet6 fe80::209c:adff:fe01::3df7/64 scope link
       valid_lft forever preferred_lft forever
```

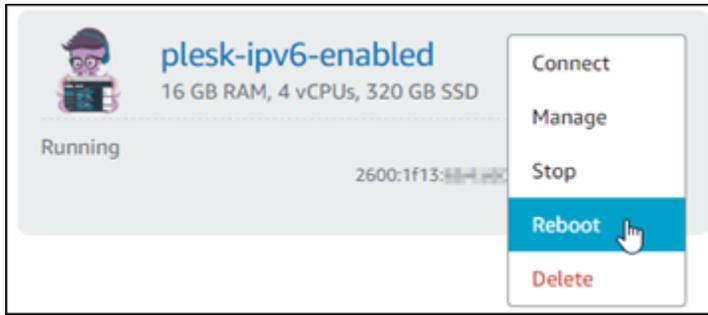
- 如果您的執行個體確實辨識出其 IPv6 位址，您會看到它在回應中列出，並顯示此範例所示。您應該停在這裡；您不需要完成此程序的步驟 4 到 7，因為您的執行個體已設定為辨識其 IPv6 位址。

```

admin@ip-172-31-1-22:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 02:9c:84:11:8a:11:ff:ff
    inet 172.31.1.22/24 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 2600:1f13:154:1000:154:1000:f383:3212/64 scope global
        valid_lft forever preferred_lft forever
    inet6 fe80::8411:8a11:ff:ff:3df7/64 scope link
        valid_lft forever preferred_lft forever

```

4. 切換回 Lightsail 主控台。
5. 在 Lightsail 首頁的 Instances (執行個體) 索引標籤中，為 Plesk 執行個體選擇動作選單 (:)，然後選擇 Reboot (重新啟動)。



等待數分鐘讓執行個體重新啟動，再繼續進行下一個步驟。

6. 切換回 Plesk 執行個體的 SSH 工作階段。
7. 輸入下列命令以檢視在執行個體上設定的 IP 位址，並確認執行個體現在正在辨識其指派的位 IPv6 位址。

```
ip addr
```

您將看到類似以下範例的回應。如果您的執行個體確實辨識出其 IPv6 位址，您會在回應中看到該執行個體的位址，標籤 `scope global` 為如此範例所示。

```
admin@ip-172-31-1-223:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 02:9c:84:1f:13:28 brd ff:ff:ff:ff:ff:ff
    inet 172.31.1.223/24 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 2600:1f13:2800::f383:3212/64 scope global
        valid_lft forever preferred_lft forever
    inet6 fe80::209c:841f:1328::3df7/64 scope link
        valid_lft forever preferred_lft forever
```

## 設定 Ubuntu 16 執行個體的IPv6連線能力

在預設情況下，Amazon Lightsail 中的所有執行個體都會指派一個公開和私有IPv4地址。您可以選擇啟用IPv6用讓執行個體指派公用IPv6位址給執行個體。如需詳細資訊，請參閱 [IP 地址](#)和[IPv6在 Amazon Lightsail 中啟用或停用](#)。

IPv6針對使用 Ubuntu 16 藍圖的執行個體啟用後，您必須執行一組額外的步驟，讓執行個體知道其IPv6位址。在本指南中，我們會介紹您必須為 Ubuntu 16 執行個體執行的其他步驟。

### 必要條件

請先完成事前準備 (若尚未完成)：

- 在 Lightsail 中建立一個 Ubuntu 16 執行個體。如需詳細資訊，請參閱[建立執行個體](#)。
- IPv6為您的 Ubuntu 16 執行個體啟用。如需詳細資訊，請參閱[啟用或停用IPv6](#)。

#### Note

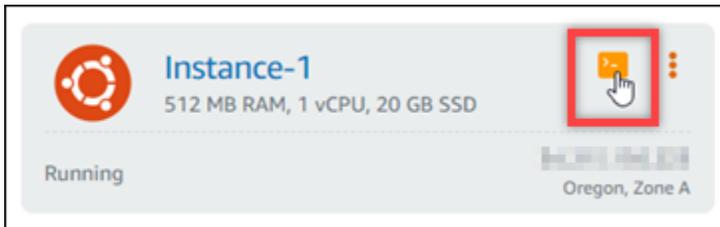
在 2021 年 1 月 12 日或之後建立的新 Ubuntu 執行個體在 Lightsail 主控台中建立時，預設會IPv6啟用這些執行個體。即使在建立執行個體時預設IPv6為啟用，您也必須完成本指南中的下列步驟，才能在執行個體IPv6上進行設定。

## 在 Ubuntu 16 執行個體上進行設定

請完成下列程序，以便在 Lightsail 中的 Ubuntu 16 執行個體IPv6上進行設定。

1. 登入主 [Lightsail](#) 台。

- 在 Lightsail 首頁的「執行個體」區段中，找出您要設定的 Ubuntu 16 執行個體，然後選擇瀏覽器型SSH用戶端圖示以使用連線至該執行個體。SSH



- 連接至執行個體後，輸入下列命令來檢視執行個體上設定的 IP 地址。

```
ip addr
```

您將看到類似以下其中一個範例的回應：

- 如果您的執行個體無法辨識其IPv6位址，您就不會在回應中看到該位址。您應該繼續完成此程序的步驟 4 至 9。

```
ubuntu@ip-172-30-4-4:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 02:af:fe:d3:16:bf brd ff:ff:ff:ff:ff:ff
    inet 172.30.4.4/20 brd 172.30.15.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::af:fe:d3:16bf/64 scope link
        valid_lft forever preferred_lft forever
```

- 如果您的執行個體確實辨識出其IPv6位址，您會看到它在回應中列出，並顯示此範例中所示。您應該停在這裡；您不需要完成此程序的步驟 4 到 9，因為您的執行個體已設定為辨識其IPv6位址。

```
ubuntu@ip-172-30-4-4:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 02:af:fe:d3:16:bf brd ff:ff:ff:ff:ff:ff
    inet 172.30.4.4/20 brd 172.30.15.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 2600:1f13:9b4:ee90:de77:120c:ed2c:91e2/128 scope global
        valid_lft forever preferred_lft forever
    inet6 fe80::af:fe:d3:16bf/64 scope link
        valid_lft forever preferred_lft forever
```

- 輸入下列命令，即可使用 Vim 開啟界面組態檔案。

```
sudo vim /etc/network/interfaces
```

5. 在 Vim 中按 I 以進入插入模式。
6. 在檔案的結尾新增下列文字行。

```
iface eth0 inet6 dhcp
```

完成後，檔案會如下所示：

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# Source interfaces
# Please check /etc/network/interfaces.d before changing this file
# as interfaces may have been defined in /etc/network/interfaces.d
# See LP: #1262951
source /etc/network/interfaces.d/*.cfg

iface eth0 inet6 dhcp
```

7. 在 Vim 中按 Esc 鍵以離開插入模式，然後鍵入 :wq! 並按 Enter (輸入) 以儲存您的編輯 (寫入)，然後退出 Vim。
8. 輸入下列命令，以重新啟動執行個體的聯網服務。

```
sudo service networking restart
```

重新啟動執行個體的網路服務後，您可能需要等待幾分鐘，讓執行個體辨識其IPv6位址。

9. 輸入下列命令以檢視在執行個體上設定的 IP 位址，並確認執行個體現在正在辨識其指派的位IPv6位址。

```
ip addr
```

您將看到類似以下範例的回應。如果您的執行個體確實辨識出其IPv6位址，您會在回應中看到該執行個體的位址，標籤scope global為如此範例所示。

```
ubuntu@ip-172-31-4-1:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 02:af:fe:d3:16:bf brd ff:ff:ff:ff:ff:ff
    inet 172.31.4.200/20 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 2600:1f13:404:4000::172:31:4:200/128 scope global
        valid_lft forever preferred_lft forever
    inet6 fe80::af:fe:d3:16bf/64 scope link
        valid_lft forever preferred_lft forever
```

按照 step-by-step 指示進行操作，了解如何在 Lightsail 執行個體藍圖 IPv6 上進行設定。

該指南涵蓋了各種實例藍圖，包括 DebianPanel，尼金克斯 GitLab，普萊斯克和 Ubuntu 16。這些程序包括透過連線至執行個體 SSH、修改網路設定檔、重新啟動服務，以及驗證執行個體是否能辨識其指派的 IPv6 位址。遵循本指南，您可以確保 Lightsail 執行個體已正確設定為同時使用 IPv4 和 IPv6 位址，提供更佳的連線能力，並為應用程式的 future 網際網路做好準備。

## 設定 AWS CLI 供 Lightsail 作業使用

AWS Command Line Interface (AWS CLI) 是一種工具，可讓進階使用者和開發人員透過在終端機 (Linux 和 Unix 上) 或命令提示字元 (在 Windows 上) 輸入命令來控制 Amazon Lightsail 服務。您也可以使用 Lightsail 主控台、圖形化使用者介面和 Lightsail 應用程式介面 () 來控制 Lightsail。API

在 Lightsail 中，您可以在本機桌面 AWS CLI 上安裝或將其安裝在 Lightsail 執行個體上。

若要取得有關的更多資訊 AWS CLI，請參閱 [AWS Command Line Interface 使用者指南](#)。您可以在命令 [參考中找到 Amazon Lightsail 命 AWS CLI 令](#)。

- 若要在本機桌面 AWS CLI 上安裝，請參閱 AWS Command Line Interface 說明文件 [AWS CLI 中的〈安裝〉](#)。
- 若要 AWS CLI 在您的 Ubuntu-Lightsail 執行個體上安裝，請連線至您的執行個體，然後輸入。sudo apt-get -y install awscli

### Note

AWS CLI 應該已經安裝在 Amazon 的 Lightsail 執行個體上。如果您需要重新安裝，請連接到您的執行個體，然後輸入 sudo yum install aws-cli。

安裝之後 AWS CLI，您需要取得存取金鑰，然後設定 AWS CLI 使用它們。如需詳細資訊，請參閱[建立存取金鑰以使用 Lightsail API 或 AWS Command Line Interface](#)

## 為 Lightsail API 和產生存取金鑰 AWS CLI

若要使用 Lightsail API 或 AWS Command Line Interface (AWS CLI)，您必須建立新的存取金鑰。存取金鑰包含 Access Key ID (存取金鑰 ID) 和 Secret Access Key (私密存取金鑰)。使用下列程序建立金鑰，並設定 AWS CLI 要撥打 Lightsail API 的電話。

### 步驟 1：建立新的存取金鑰

您可以在 AWS Identity and Access Management (IAM) 主控台中建立新的存取金鑰。

1. 登入主控IAM台。
2. 選擇您要為其建立存取金鑰之使用者的名稱。您選擇的使用者應具有 Lightsail 動作的完整存取權限或特定存取權限。
3. 選擇 Security credentials (安全憑證) 索引標籤。
4. 選擇頁面的 Access keys (存取金鑰) 區段下的 Create access key (建立存取金鑰)。

#### Note

每個使用者一次最多可以有兩種存取金鑰 (作用中或非作用中)。若您已有兩個存取金鑰，您必須先刪除其中一個，才能建立新的金鑰。請確定存取金鑰未在作用中，再將其刪除。

5. 記下列出的 Access key ID (存取金鑰 ID) 和 Secret access key (私密存取金鑰)。選擇 Secret access key (私密存取金鑰) 資料欄下的 Show (顯示)，以查看您的 Secret access key (私密存取金鑰)。

您可以從這個畫面複製金鑰，或選擇 Download Key File (下載金鑰檔案) 以下載包含存取存取金鑰 ID 和私密存取金鑰的 .csv 檔案。

#### Important

將您的存取金鑰存放在安全的地方。您應該將檔案名稱命名為類似 MyLightsailKeys.csv，以避免之後不易找到這些檔案。如果您已從IAM主機下載CSV檔案，請在完成步驟 2 之後將其刪除。如有必要，您可以稍後建立新的存取金鑰。

## 步驟 2：配置 AWS CLI

如果您尚未安裝 AWS CLI，您現在可以執行此操作。請參閱[安裝 AWS Command Line Interface](#)。安裝之後 AWS CLI，您需要對其進行配置，以便可以使用它。

1. 開啟終端機視窗或命令提示字元。
2. 類型 `aws configure`。
3. 從上一個步驟建立的 `.csv` 檔案中貼上 AWS 存取金鑰 ID。
4. 出現提示時，貼上您的 AWS 私密存取金鑰。
5. 輸入資源所 AWS 區域 在的位置。例如，如果您的資源主要位於俄亥俄州，請在提示輸入預設區域名稱時選擇 `us-east-2`。

如需有關使用選 AWS CLI `--region` 項的詳細資訊，請參閱 AWS CLI 參考中的 [一般選項](#)。

6. 選擇 Default output format (預設輸出格式)，例如 `json`。

### 後續步驟

- [安裝 SDK](#)
- [配置與 AWS Command Line Interface Amazon Lightsail 一起工作](#)
- [閱讀文API件](#)

## 在 Lightsail AMP 執行個體上部署 PHP 應用程式

如果您只需要虛擬私有伺服器，Amazon Lightsail 是開始使用亞馬遜網路服務 (AWS) 的最簡單方法。Lightsail 包含快速啟動專案所需的一切，包括虛擬機器、SSD 儲存、資料傳輸、DNS 管理和靜態 IP，價格低廉且可預測。

本教學課程說明如何在 Lightsail 上啟動和設定 LAMP 執行個體。它包含各項作業步驟，例如透過 SSH 連接到您的執行個體、為您的執行個體取得應用程式密碼、建立一個靜態 IP 並將它連接到您的執行個體，以及建立 DNS 區域並對應您的網域。完成本教學課程後，您將擁有讓執行個體在 Lightsail 上啟動並執行的基礎知識。

### 內容

- [步驟 1：註冊 AWS](#)
- [步驟 2：建立 LAMP 執行個體](#)

- [步驟 3：透過 SSH 連接至您的執行個體，並為您的 LAMP 執行個體取得應用程式密碼](#)
- [步驟 4：在您的 LAMP 執行個體上安裝應用程式](#)
- [步驟 5：建立靜態 IP 地址並將其附接至 LAMP 執行個體](#)
- [步驟 6：建立 DNS 區域並將域對應到 LAMP 執行個體](#)
- [後續步驟](#)

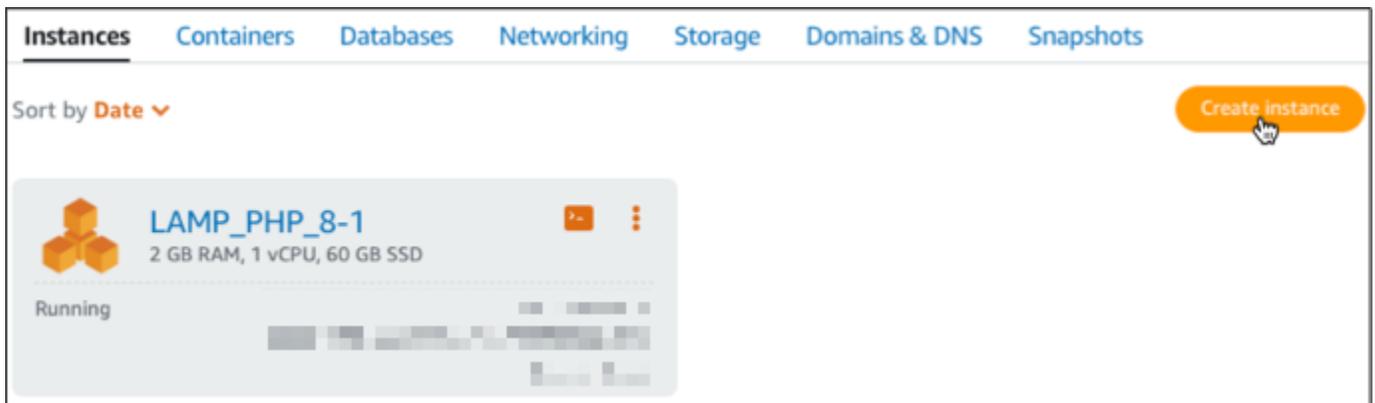
## 步驟 1：註冊 AWS

本教學課程需要一個 AWS 帳戶。[註冊 AWS](#)，或者 AWS 如果您已經有帳戶，請[登入](#)。

## 步驟 2：建立 LAMP 執行個體

讓您的 LAMP 執行個體在 Lightsail 中啟動並執行。如需在 Lightsail 中建立執行個體的詳細資訊，請參閱 Lightsail 文[件中的建立 Amazon Lightsail 執行個體](#)。

1. 登入主 [Lightsail](#) 台。
2. 在 Lightsail 首頁的「實體」索引標籤上，選擇「建立實體」。



3. 為您的執行個體選擇 AWS 區域 和可用區域。

## Select your instance location

### Select a Region

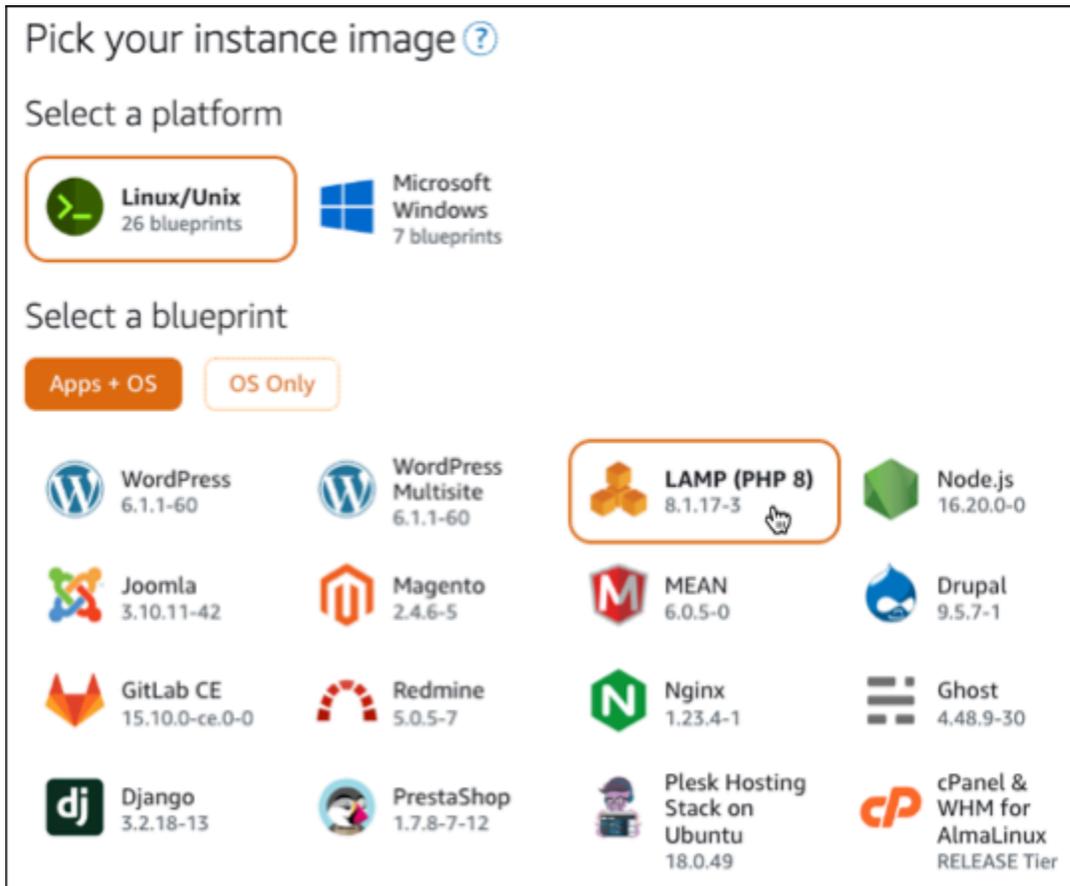
The closer your instance is to your users, the less latency they will experience.  
[Learn more about Regions](#)

 <b>Oregon</b> us-west-2	 <b>Ohio</b> us-east-2	 <b>Virginia</b> us-east-1	 <b>Montreal</b> ca-central-1
 <b>Tokyo</b> ap-northeast-1	 <b>Seoul</b> ap-northeast-2	 <b>Ireland</b> eu-west-1	 <b>Sydney</b> ap-southeast-2
 <b>London</b> eu-west-2	 <b>Paris</b> eu-west-3	 <b>Frankfurt</b> eu-central-1	 <b>Singapore</b> ap-southeast-1
 <b>Mumbai</b> ap-south-1	 <b>Stockholm</b> eu-north-1		

### Select an Availability Zone

 <b>Zone A</b> us-west-2a	 <b>Zone B</b> us-west-2b	 <b>Zone C</b> us-west-2c	 <b>Zone D</b> us-west-2d
---	---	---	---

4. 選擇您的執行個體映像。
  - a. 選擇 Linux/Unix (Linux/Unix) 做為平台。
  - b. 選擇 LAMP (PHP 8) 做為藍圖。



5. 選擇執行個體方案。

方案包含低且可預測的成本、機器組態 (RAM、SSD、vCPU) 及資料傳輸額度。您可以免費試用 5 美元的 Lightsail 計劃一個月 (最多 750 小時)。AWS 將一個月免費存入您的帳戶。

**Note**

作為 AWS 免費方案的一部分，您可以在特定執行個體套裝軟體上免費開始使用 Amazon Lightsail。如需詳細資訊，請參閱 [Amazon Lightsail 定價頁面](#) 上的 AWS 免費方案。

6. 輸入您執行個體的名稱。

資源名稱：

- 每個 Lightsail 帳戶 AWS 區域 中的每個項目都必須是唯一的。
- 必須包含 2 至 255 個字元。
- 開頭和結尾必須是英數字元或數字。

- 可以包含英數字元、數字、句點、破折號和底線。



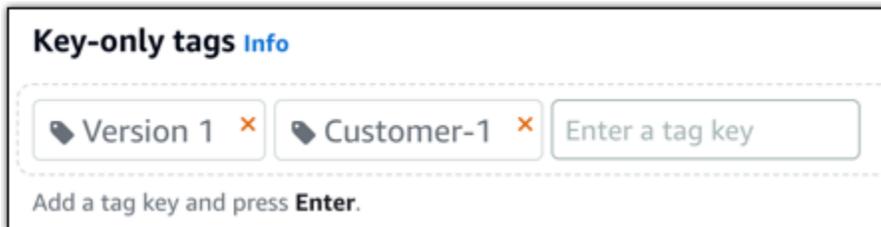
Name your instance

Your Lightsail resources must have unique names.

LAMP\_PHP\_5-512MB-Oregon-1 × 1

7. 選擇下列其中一個選項以新增標籤至您的執行個體：

- Add key-only tags (新增僅索引鍵標籤) 或 Edit key-only tags (編輯僅索引鍵標籤) (若標籤已新增)。在標籤索引鍵文字方塊中輸入新的標籤，接著按 Enter (輸入)。輸入標籤以新增之後，請選擇 Save (儲存)，如果不要新增則選擇 Cancel (取消)。



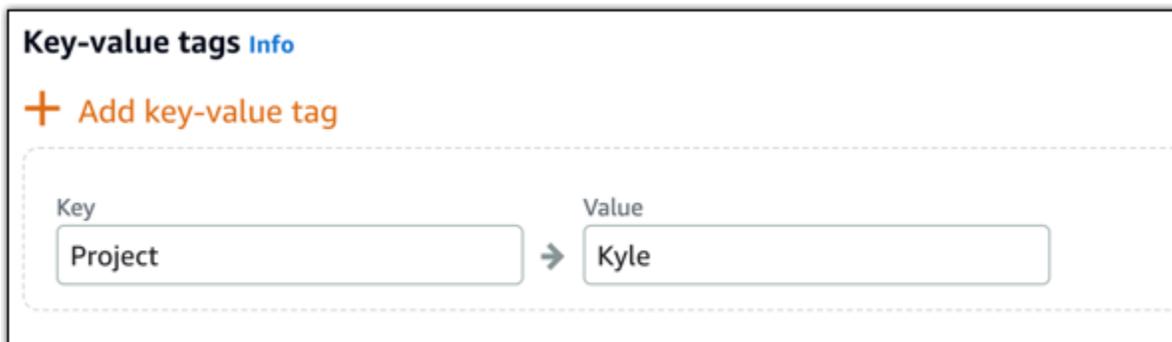
Key-only tags Info

Version 1 × Customer-1 × Enter a tag key

Add a tag key and press **Enter**.

- Create a key-value tag (建立索引鍵值標籤)，接著將索引鍵輸入 Key (索引鍵) 文字方塊，將值輸入 Value (值) 文字方塊。完成輸入標籤後，請選擇 Save (儲存)，如果不要新增則選擇 Cancel (取消)。

鍵值標籤在儲存前一次只能新增一個。若要新增超過一個索引鍵值標籤，請重複之前的步驟。



Key-value tags Info

+ Add key-value tag

Key Value

Project → Kyle

**Note**

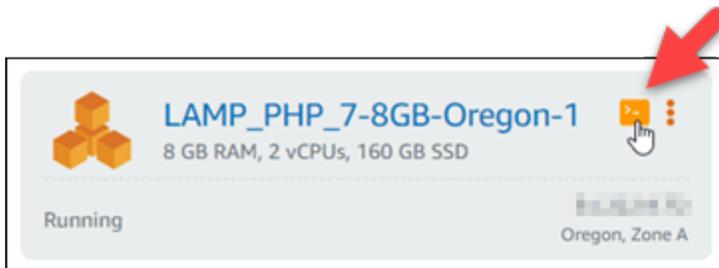
如需有關僅索引鍵和索引鍵值標籤的詳細資訊，請參閱[標籤](#)。

8. 選擇 Create instance (建立執行個體)。

### 步驟 3：透過 SSH 連接至您的執行個體，並為您的 LAMP 執行個體取得應用程式密碼

用於登入您在 LAMP 中的資料庫的預設密碼存放於您的執行個體。透過使用 Lightsail 主控台中的瀏覽器型 SSH 終端機連線至執行個體，並執行特殊命令來擷取該執行個體。如需詳細資訊，請參閱在[Amazon Lightsail 中取得 Bitnami 執行個體的應用程式使用者名稱和密碼](#)。

1. 在 Lightsail 首頁的 [執行個體] 索引標籤上，選擇 LAMP 執行個體的安全殼層快速連線圖示。



2. 在以瀏覽器為基礎的 SSH 用戶端視窗開啟後，請輸入下列命令來擷取預設的應用程式密碼：

```
cat bitnami_application_password
```

**Note**

若您是在使用者主目錄外的目錄中，則請輸入 `cat $HOME/bitnami_application_password`。

3. 請記下螢幕上顯示的密碼。之後您可使用此密碼在您的執行個體上安裝 Bitnami 應用程式，或以 root 的使用者名稱存取 MySQL 資料庫。

```
Welcome to Ubuntu 16.04.5 LTS (GNU/Linux 4.4.0-1065-aws x86_64)
*** System restart required ***

      BLUENIX

*** Welcome to the Bitnami LAMP 5.6.37-2 ***
*** Documentation: https://docs.bitnami.com/aws/infrastructure/lamp/ ***
***                 https://docs.bitnami.com/aws/ ***
*** Bitnami Forums: https://community.bitnami.com/ ***
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

bitnami@ip-10-10-10-10:~$ cat bitnami_application_password
pSAqtrn2l9nt
bitnami@ip-10-10-10-10:~$
```

## 步驟 4：在您的 LAMP 執行個體上安裝應用程式

在您的 LAMP 執行個體上部署 PHP 應用程式或安裝 Bitnami 應用程式。部署您 PHP 應用程式的主要目錄為 `/opt/bitnami/apache2/htdocs`。將您的 PHP 應用程式檔案複製至該目錄，並瀏覽至您執行個體的公有 IP 地址以存取應用程式。

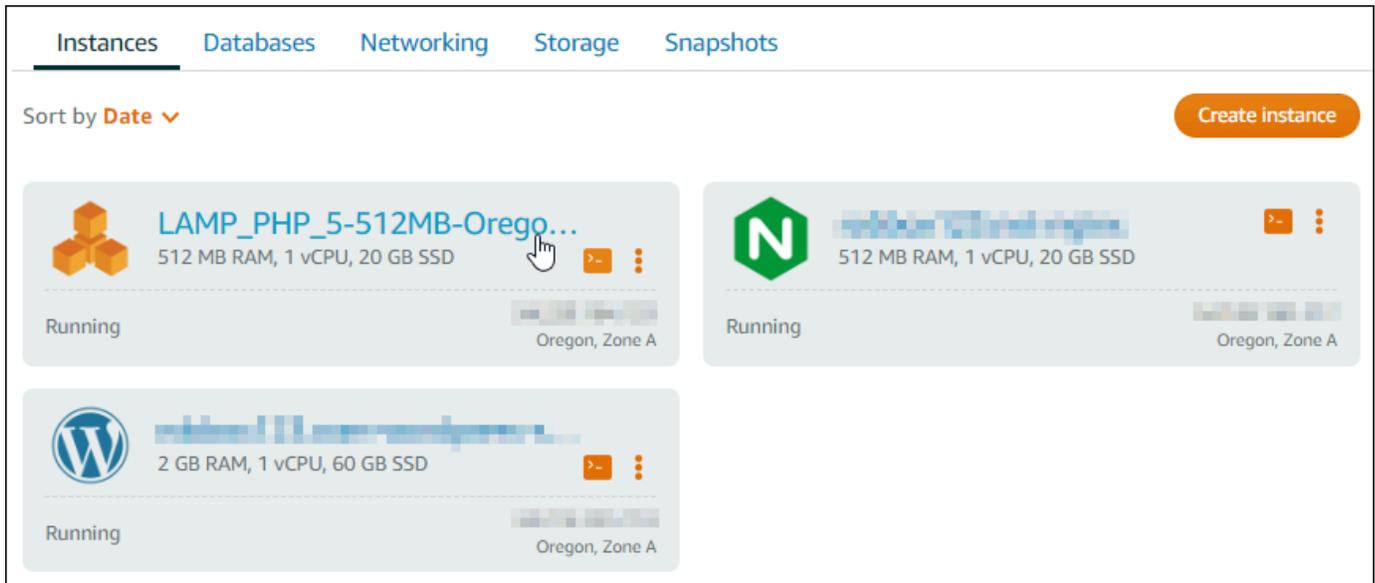
您也可以使用模組安裝程式來安裝 Bitnami 應用程式。下載 WordPress，Drupal 的，Magento 的，Moodle 的，從[比特納米網站](#)的其他應用程序和擴展服務器的功能。如需有關安裝 Bitnami 應用程式的詳細資訊，請參閱 Bitnami 文件中的[入門](#)指南。

## 步驟 5：建立靜態 IP 地址並將它連接到您的 LAMP 執行個體

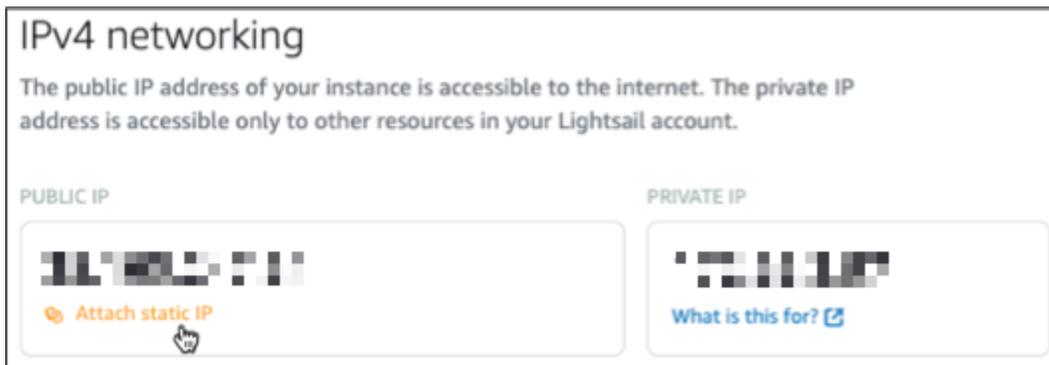
如果您停止和啟動執行個體，LAMP 執行個體的預設公有 IP 將會改變。連接到執行個體的靜態 IP 地址會保持不變，即使您停止和啟動您的執行個體。

建立靜態 IP 地址並將它連接到您的 LAMP 執行個體。如需詳細資訊，請參閱 Lightsail 文件中的[建立靜態 IP 並將其附加至執行個體](#)。

1. 在 Lightsail 首頁的「執行個體」索引標籤上，選擇執行中的 LAMP 執行個體。



2. 選擇聯網標籤，然後選擇建立靜態 IP。



3. 為靜態 IP 命名，然後選擇建立。

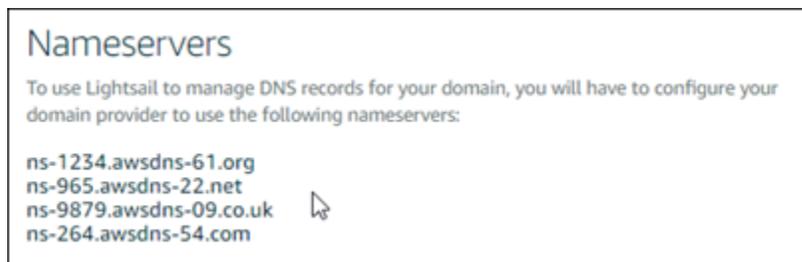


## 步驟 6：建立 DNS 區域並將域對應到 LAMP 執行個體

將您網域 DNS 記錄的管理作業移轉至 Lightsail。這可讓您更輕鬆地將網域對應至 LAMP 執行個體，並使用 Lightsail 主控台管理網站的所有資源。如需詳細資訊，請參閱[建立 DNS 區域以管理域的 DNS 記錄](#)。

1. 在首頁的 [網域和 DNS] 索引標籤上，選擇 [建立 DNS 區域]。
2. 輸入您的網域，然後選擇 Create DNS zone (建立 DNS 區域)。
3. 記下此頁面上列出的名稱伺服器地址。

您可以將這些名稱伺服器位址新增至網域名稱的註冊機構，以便將網域 DNS 記錄的管理轉移至 Lightsail。



4. 將網域的 DNS 記錄管理轉移至 Lightsail 之後，請新增 A 記錄，將網域頂點指向 LAMP 執行個體，如下所示：
  - a. 在 DNS 區域的 Assignments (指派) 索引標籤中，選擇 Add assignment (新增指派)。
  - b. 在 Select a domain (選取網域) 欄位中，選擇網域或子網域。
  - c. 在 Select a resource (選取資源) 下拉式清單中，選取您先前在本教學課程中建立的 LAMP 執行個體。
  - d. 選擇 Assign (指派)。

稍微等待一些時間，讓變更傳遞至整個網際網路的 DNS，之後您的網域才會開始將流量路由至您的 LAMP 執行個體。

## 後續步驟

在 Amazon Lightsail 中啟動 LAMP 執行個體後，您可以執行以下幾個其他步驟：

- [建立 Linux 或 Unix 執行個體快照](#)
- [建立額外的區塊儲存磁碟並將其附接至以 Linux 為基礎的執行個體](#)

## Connect Lightsail LAMP 執行個體連線至 Aurora 資料庫

貼文、頁面和使用者的應用程式資料會儲存在 Amazon Lightsail LAMP 執行個體上執行的 MariaDB 資料庫中。如果執行個體發生故障，這些資料可能會無法復原。為避免這種情況，您應該將應用程式資料轉移至 MySQL 受管資料庫。

Amazon Aurora 是針對雲端建置的 MySQL 和 PostgreSQL 相容關聯式資料庫。它將傳統企業資料庫的效能和可用性與開源資料庫的簡易性和有效性相結合。Aurora 是作為 Amazon Relational Database Service (Amazon RDS) 的一部分而提供。Amazon RDS 是一項受管資料庫服務，可以讓雲端中關聯式資料庫的設定、操作和擴展更加簡單。如需詳細資訊，請參閱 [《Amazon 關聯式資料庫服務使用者指南》](#) 和 [《Amazon Aurora 使用者指南》](#)。

在本教學中，我們將示範如何將應用程式資料庫從 Lightsail 中的 LAMP 執行個體連接到 Amazon RDS 中的 Aurora 受管資料庫。

### 內容

- [步驟 1：完成先決條件](#)
- [步驟 2：設定 Aurora 資料庫的安全群組](#)
- [步驟 3：從您的 Lightsail 執行個體 Connect 至您的 Aurora 資料庫](#)
- [步驟 4：將 MariaDB 資料庫從 LAMP 執行個體轉移至 Aurora 資料庫](#)
- [步驟 5：設定應用程式以連接至 Aurora 受管資料庫](#)

### 步驟 1：完成先決條件

開始之前，請先完成以下先決條件：

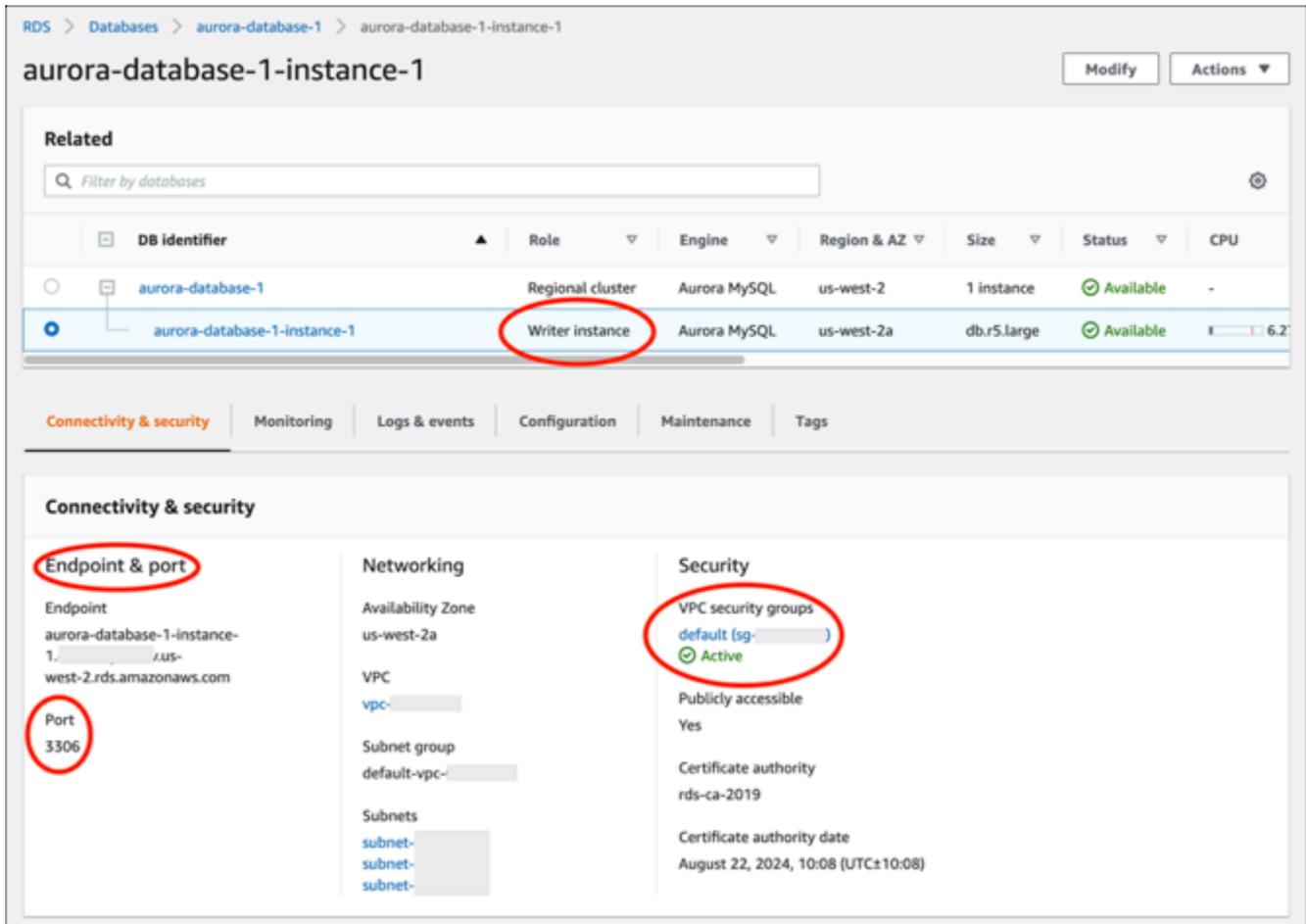
1. 在 Lightsail 中建立 LAMP 執行個體，並在其上設定您的應用程式。在繼續之前，執行個體應處於執行中狀態。如需詳細資訊，請參閱[教學課程：在 Lightsail 中啟動和設定 LAMP 執行個體](#)。
2. 在您的帳戶中開啟 VPC 人雲 Lightsail 功能。如需詳細資訊，請參閱[設定 Amazon VPC 對等互連以使用 Lightsail 以外的 AWS 資源](#)。
3. 在 Amazon RDS 中建立 Aurora 受管資料庫。資料庫應位於與您的 LAMP 執行個體相同的 AWS 區域中。在繼續之前，其亦應處於執行中狀態。如需詳細資訊，請參閱《Amazon Aurora 使用者指南》中的 [Amazon Aurora 入門](#)。

## 步驟 2：設定 Aurora 資料庫的安全群組

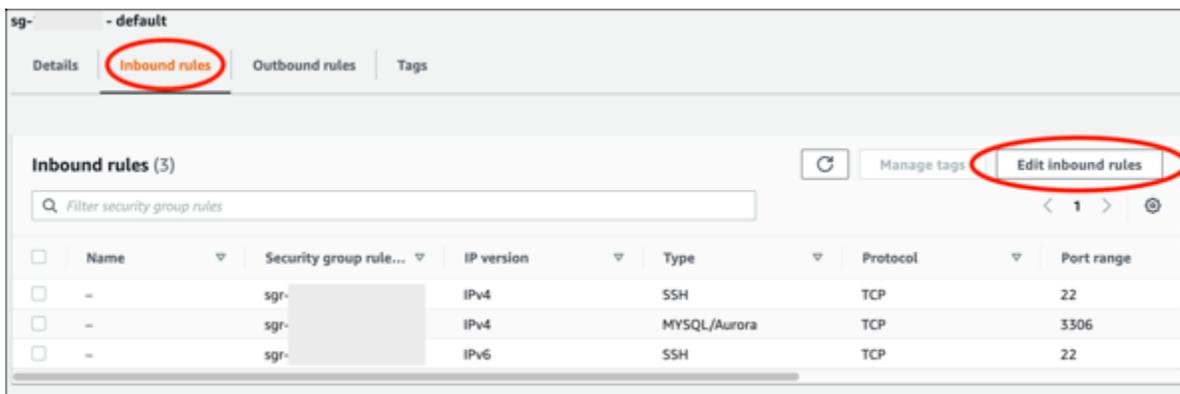
安 AWS 安全群組充當 AWS 資源的虛擬防火牆。它控制可以連接到 Amazon RDS 中 Aurora 資料庫的傳入和傳出流量。如需有關安全群組的詳細資訊，請參閱《Amazon Virtual Private Cloud 使用者指南》中的[使用安全群組控制資源流量](#)。

完成以下步驟來設定安全群組，以便 LAMP 執行個體可建立 Aurora 資料庫的連線。

1. 登入 [Amazon RDS 主控台](#)。
2. 在導覽窗格中，選擇 Databases (資料庫)。
3. 選擇 LAMP 執行個體要連接之 Aurora 資料庫的 Writer 執行個體。
4. 選擇 Connectivity & security (連線和安全) 索引標籤。
5. 在 Endpoint & port (端點與連接埠) 區段中，記下 Writer instance (寫入器執行個體) 的 Endpoint name (端點名稱) 和 Port (連接埠)。稍後將 Lightsail 執行個體設定為連線至資料庫時，您將需要這些項目。
6. 在 Security (安全) 區段中，選擇作用中的 VPC 安全群組連結。您會被重定引導至您資料庫的安全群組。

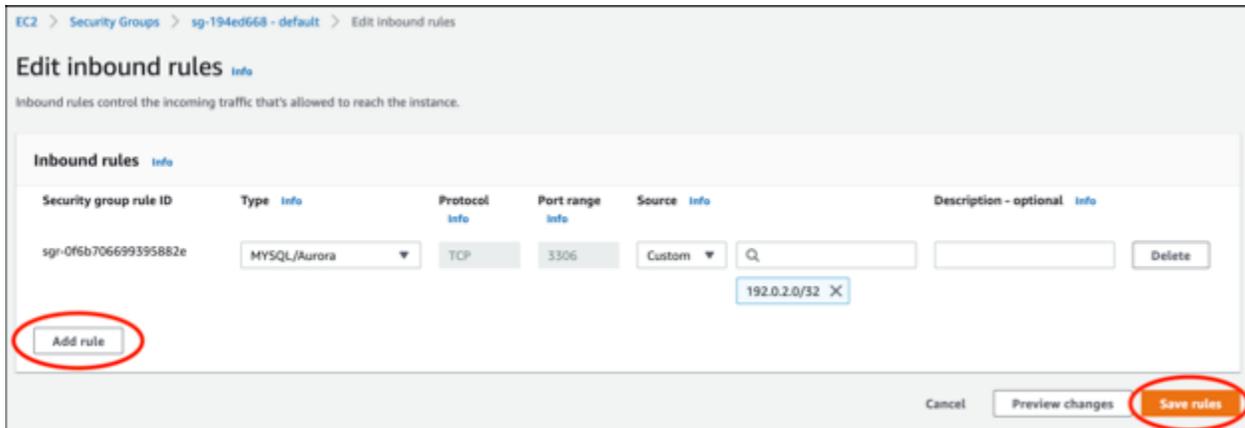


7. 確認已選取 Aurora 資料庫的安全群組。
8. 選擇 Inbound Rules (傳入規則) 索引標籤。
9. 選擇 Edit inbound Rules (編輯傳入規則)。



10. 在 Edit inbound rules (編輯傳入規則) 頁面中，選擇 Add rule (新增規則)。
11. 完成下列其中一個步驟：

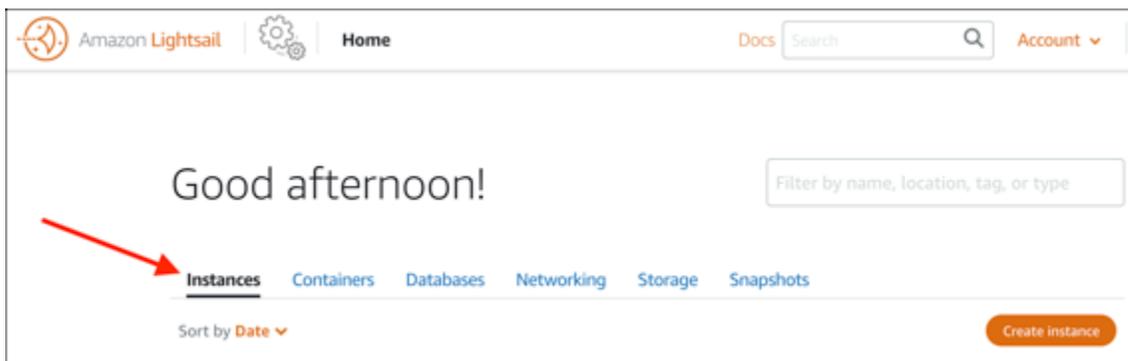
- 如果您是使用預設的 MySQL 連接埠 3306，則在 Type (類型) 下拉式選單中選擇 MySQL/Aurora。
  - 如果資料庫是使用自訂連接埠，則在 Type (類型) 下拉式選單中選擇 Custom TCP (自訂 TCP)，並在 Port Range (連接埠範圍) 文字方塊中輸入連接埠編號。
12. 在 Source (來源) 文字方塊中，新增您 LAMP 執行個體的私有 IP 地址。您必須以 CIDR 表示法輸入 IP 地址，這意味著您必須附加 /32。例如，若要允許 192.0.2.0，請輸入 192.0.2.0/32。
  13. 選擇儲存規則。



### 步驟 3：從您的 Lightsail 執行個體 Connect 至您的 Aurora 資料庫

請完成下列程序，以確認您可以從 Lightsail 執行個體連線至 Aurora 資料庫。

1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁上，選擇「實體」索引標籤。



3. 選擇瀏覽器型 SSH 用戶端圖示，讓 LAMP 執行個體使用 SSH 連接至用戶端。



4. 在連接至執行個體後，輸入以下命令以連接至 Aurora 資料庫。在命令中，以 Aurora 資料庫的端點位址取代 *DatabaseEndpoint*，並將 *Port* 取代為資料庫的連接埠。*MyUserName* 以建立資料庫時輸入的使用者名稱取代。

```
mysql -h DatabaseEndpoint -P Port -u MyUserName -p
```

您應該會看到類似以下範例的回應，其會確認您的執行個體可以存取並連接至 Aurora 資料庫。

```
bitnami@ip-... $ mysql -h database.cluster-...us-west-2.rds.amazonaws.com -P 3306 -u admin -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 215
Server version: 5.6.10 MySQL Community Server (GPL)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> █
```

如果您沒有看到此回應，或收到錯誤訊息，則可能需要設定資料庫的安全性群組，以允許 Lightsail 執行個體的私有 IP 位址連線至該資料庫。如需詳細資訊，請參閱本指南的[設定 Aurora 資料庫的安全群組](#)章節。

#### 步驟 4：將 MariaDB 資料庫從 LAMP 執行個體轉移至 Aurora 資料庫

現在您已確認能從執行個體連接至資料庫，接著應該將資料從 LAMP 執行個體遷移到 Aurora 資料庫。如需詳細資訊，請參閱《Amazon Aurora 使用者指南》中的[將資料遷移至 Amazon Aurora MySQL 資料庫叢集](#)。

#### 步驟 5：設定應用程式以連接至 Aurora 受管資料庫

將應用程式資料轉移到 Aurora 資料庫之後，應將在 LAMP 執行個體上執行的應用程式設定為連接至 Aurora 資料庫。使用 SSH 連接至您的 LAMP 執行個體，並存取應用程式的資料庫組態檔案。在組態檔案中，定義 Aurora 資料庫的端點地址、資料庫使用者名稱和密碼。以下是組態檔案範例。

```
bitnami@ip-          :~/htdocs$ cat connectvalues.php
<?php
$host      = 'database.cluster-          .us-west-2.rds.amazonaws.com';
$username  = 'admin';
$password  = 'Password1';
```

## 啟動並設定視窗伺服器 2016 年執行 Lightsail

如果您只需要虛擬私有伺服器，Amazon Lightsail 是開始使用亞馬遜網路服務 (AWS) 的最簡單方法。Lightsail 包含快速啟動專案所需的一切，包括虛擬機器、以 SSD 為基礎的儲存、資料傳輸、DNS 管理和靜態 IP，而且價格低廉且可預測。

本教學課程說明如何在 Lightsail 上啟動和設定視窗伺服器 2016 執行個體。它包含各項作業步驟，例如透過 RDP 連接到您的執行個體、建立一個靜態 IP 並將它連接到您的執行個體，以及建立 DNS 區域並對應您的網域。完成本教學課程後，您將擁有讓執行個體在 Lightsail 上啟動並執行的基礎知識。

### 內容

- [步驟 1：註冊 AWS](#)
- [步驟 2：建立 Windows Server 2016 執行個體](#)
- [步驟 3：透過 RDP 連接至您的 Windows Server 2016 執行個體](#)
- [步驟 4：建立靜態 IP 地址並將其附接至您的 Windows Server 2016 執行個體](#)
- [步驟 5：建立 DNS 區域並將域對應至您的 Windows Server 2016 執行個體](#)
- [後續步驟](#)

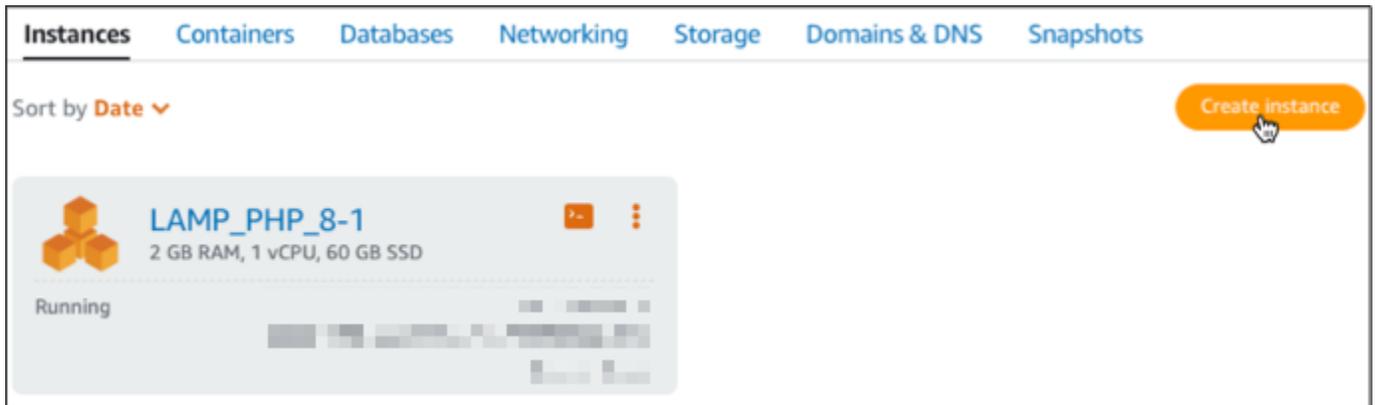
## 步驟 1：註冊 AWS

本教學課程需要一個 AWS 帳戶。[註冊 AWS](#)，或者 AWS 如果您已經有帳戶，請[登入](#)。

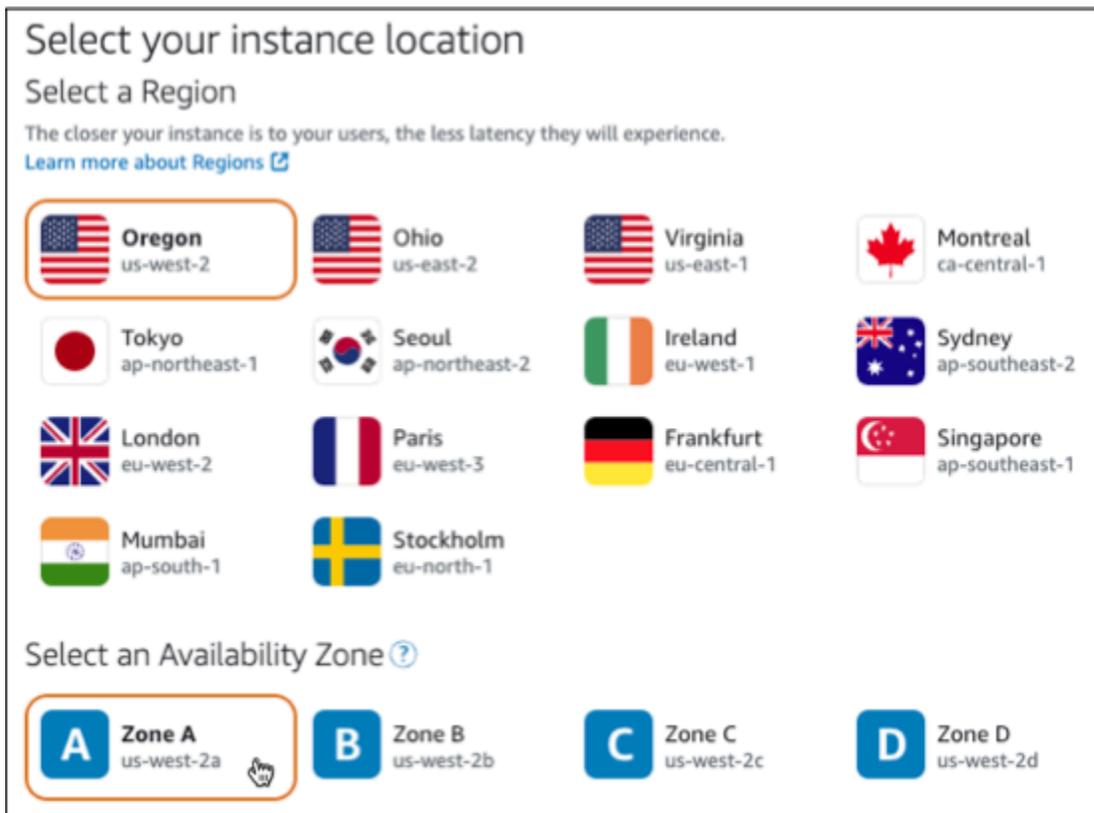
## 步驟 2：建立視窗伺服器 2016 年執行 Lightsail

讓您的視窗伺服器 2016 年執行個體在 Lightsail 中啟動並執行。如需詳細資訊，請參閱[開始使用以 Windows Server 為基礎的執行個體](#)。

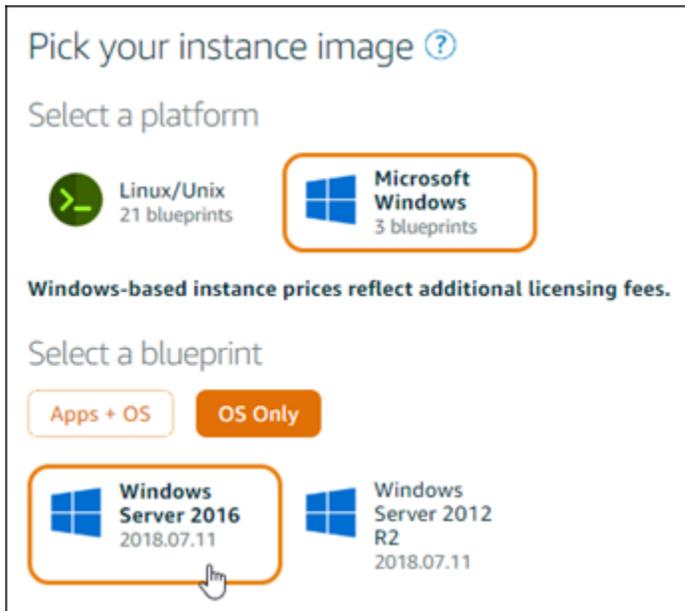
1. 登入主 [Lightsail 台](#)。
2. 在 Lightsail 首頁的「實體」索引標籤上，選擇「建立實體」。



3. 為您的執行個體選擇 AWS 區域 和可用區域。



4. 選擇您的執行個體映像。
  - a. 選擇 Microsoft Windows (Microsoft Windows) 做為平台。
  - b. 選擇 OS Only (僅作業系統) ，然後選擇 Windows Server 2016 (Windows Server 2016) 做為藍圖。



5. 選擇執行個體方案。

方案包含低且可預測的成本、機器組態 (RAM、SSD、vCPU) 及資料傳輸額度。您可以免費試用 9.50 美元的 Lightsail 計劃一個月 (最多 750 小時)。AWS 將一個月免費存入您的帳戶。

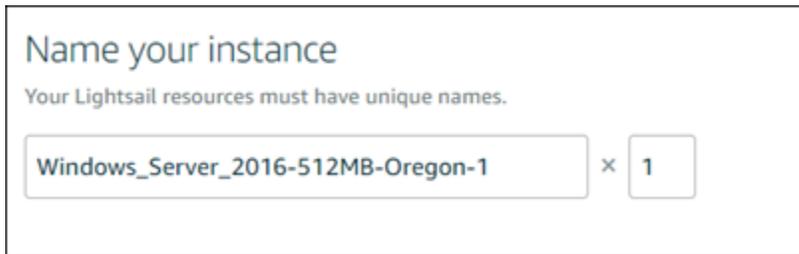
**Note**

作為 AWS 免費方案的一部分，您可以在特定執行個體套裝軟體上免費開始使用 Amazon Lightsail。如需詳細資訊，請參閱 [Amazon Lightsail 定價頁面](#) 上的 AWS 免費方案。

6. 輸入您執行個體的名稱。

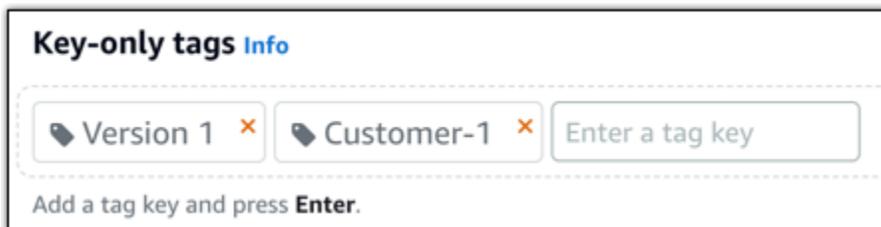
資源名稱：

- 每個 Lightsail 帳戶 AWS 區域 中的每個項目都必須是唯一的。
- 必須包含 2 至 255 個字元。
- 開頭和結尾必須是英數字元或數字。
- 可以包含英數字元、數字、句點、破折號和底線。



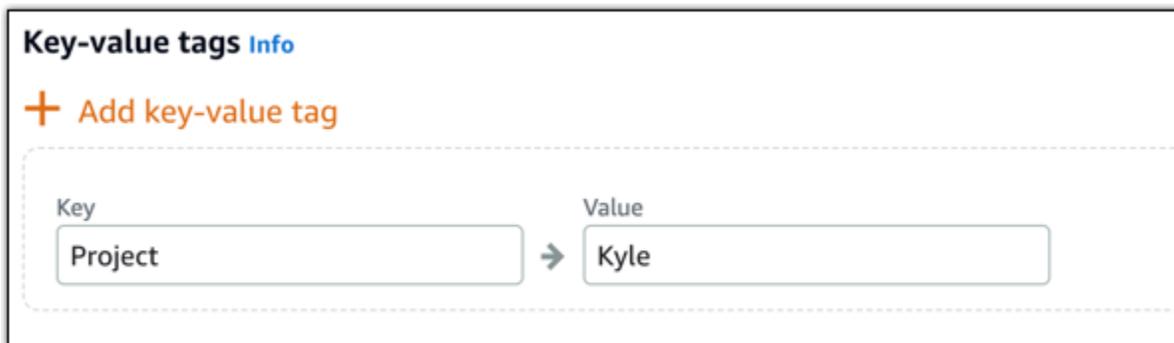
7. 選擇下列其中一個選項以新增標籤至您的執行個體：

- Add key-only tags (新增僅索引鍵標籤) 或 Edit key-only tags (編輯僅索引鍵標籤) (若標籤已新增)。在標籤索引鍵文字方塊中輸入新的標籤，接著按 Enter (輸入)。輸入標籤以新增之後，請選擇 Save (儲存)，如果不要新增則選擇 Cancel (取消)。



- Create a key-value tag (建立索引鍵值標籤)，接著將索引鍵輸入 Key (索引鍵) 文字方塊，將值輸入 Value (值) 文字方塊。完成輸入標籤後，請選擇 Save (儲存)，如果不要新增則選擇 Cancel (取消)。

鍵值標籤在儲存前一次只能新增一個。若要新增超過一個索引鍵值標籤，請重複之前的步驟。



#### Note

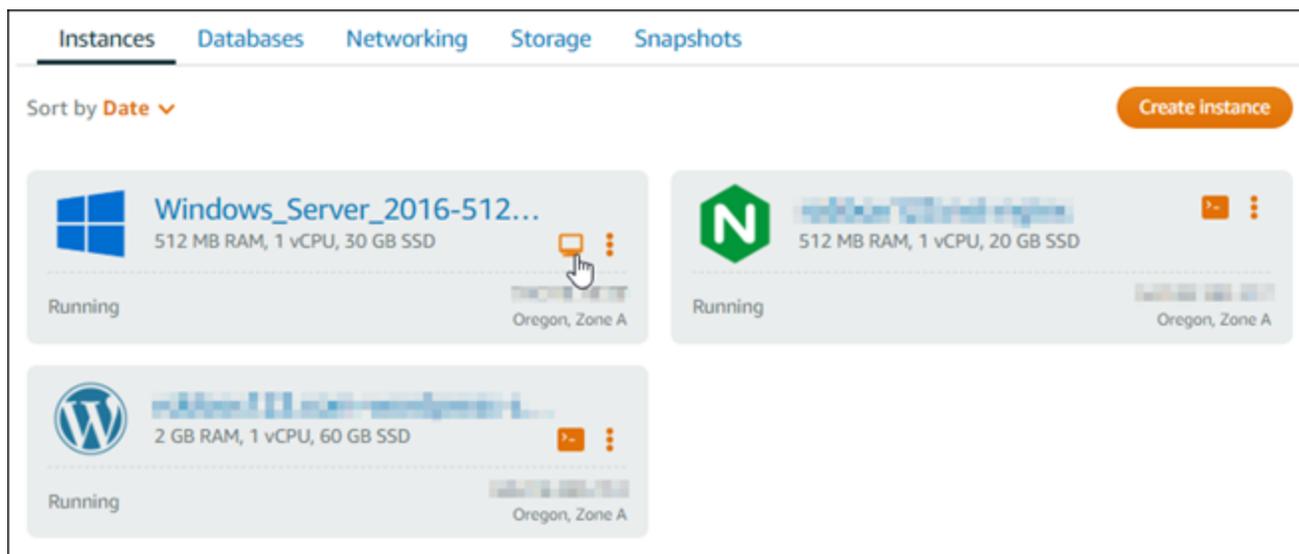
如需有關僅索引鍵和索引鍵值標籤的詳細資訊，請參閱[標籤](#)。

8. 選擇 建立執行個體。

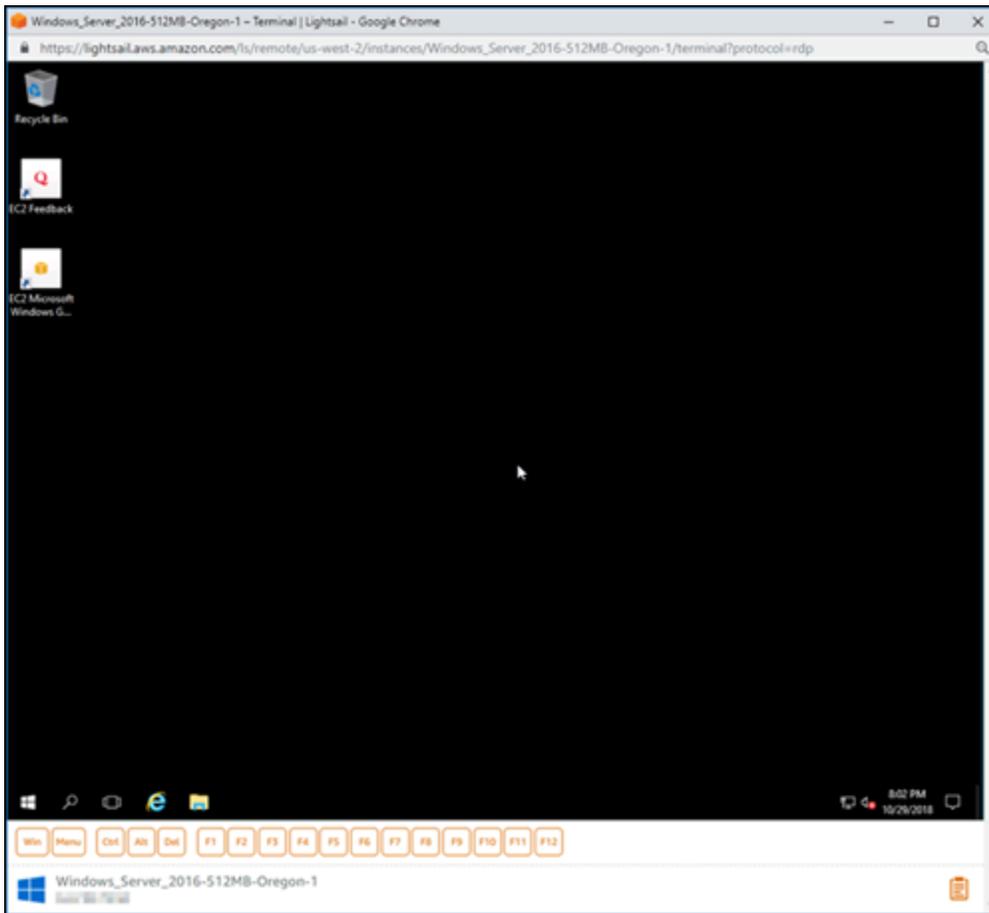
## 步驟 3：透過 RDP 連接至您的 Windows Server 2016 執行個體

使用 Lightsail 主控台中以瀏覽器為基礎的 RDP 用戶端，Connect 線至您的視窗伺服器 2016 執行個體。如需詳細資訊，請參閱[連線至您的 Windows 執行個體](#)。

1. 在 Lightsail 首頁的 [執行個體] 索引標籤上，為您的 Windows 伺服器 2016 年執行個體選擇 RDP 快速連線圖示。



2. 以瀏覽器為基礎的 RDP 用戶端視窗開啟之後，您就可以開始設定您的 Windows Server 2016 執行個體：

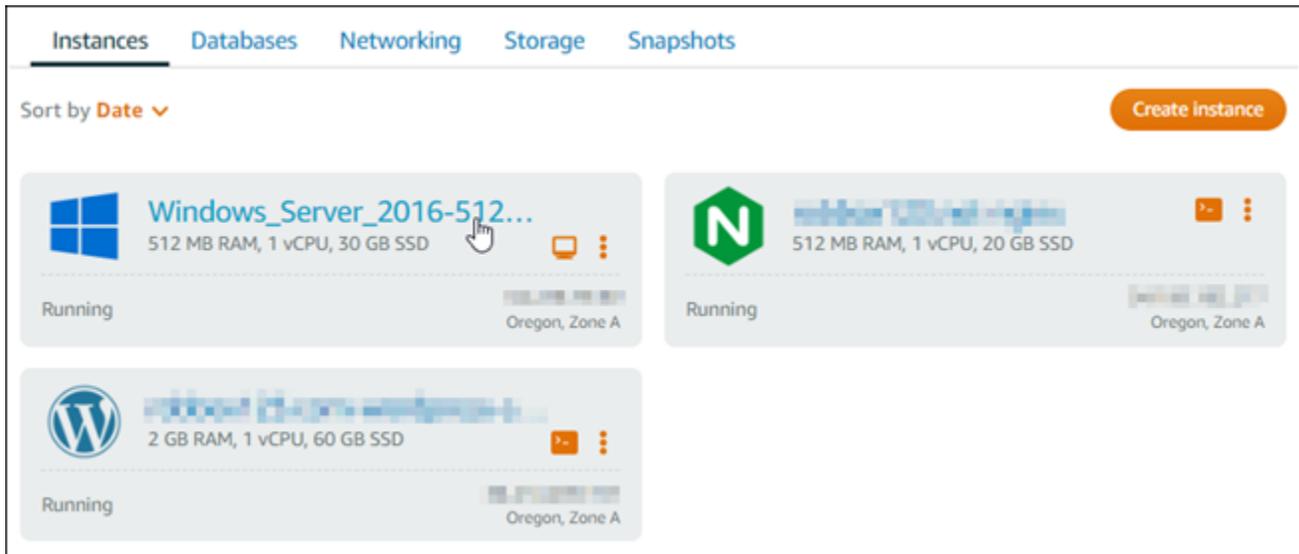


## 步驟 4：建立靜態 IP 地址並將它連接到您的 Windows Server 2016 執行個體

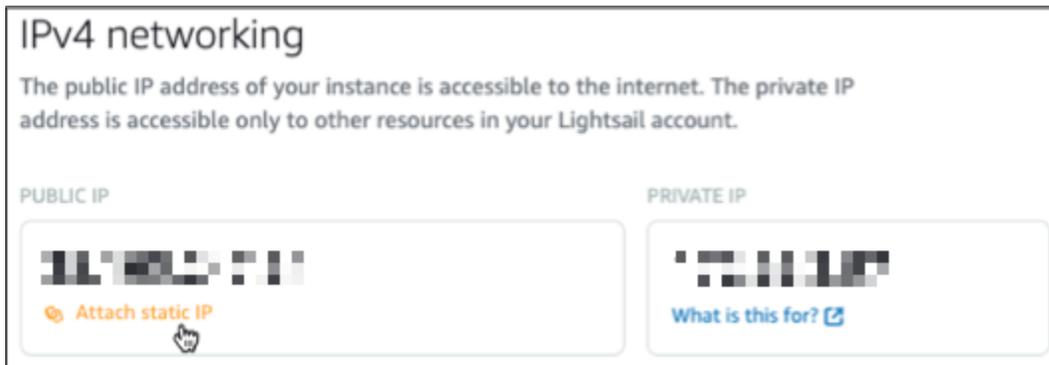
如果您停止和啟動執行個體，Windows Server 2016 執行個體的預設公有 IP 將會改變。連接到執行個體的靜態 IP 地址會保持不變，即使您停止和啟動您的執行個體。

建立靜態 IP 地址並將它連接到您的 Windows Server 2016 執行個體。如需詳細資訊，請參閱 Lightsail 文件中的 [建立靜態 IP 並將其附加至執行個體](#)。

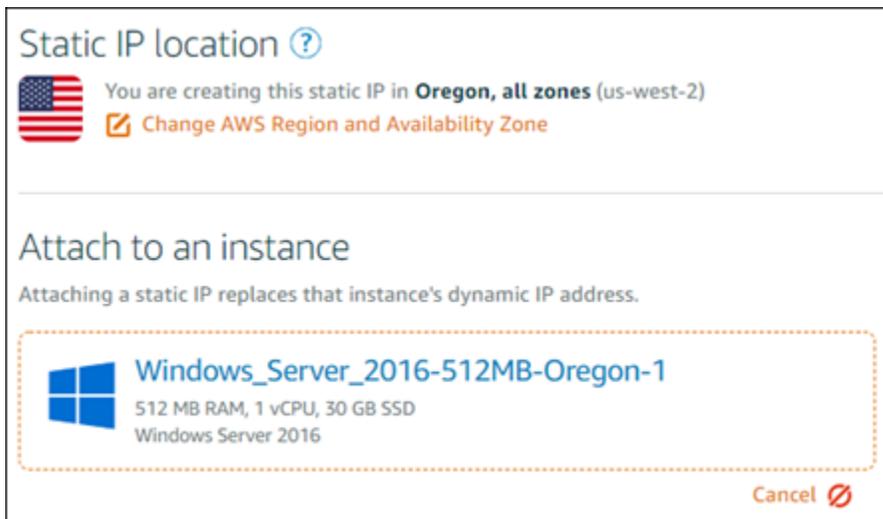
1. 在 Lightsail 首頁的 [執行個體] 索引標籤上，選擇執行中的 Windows 伺服器 2016 執行個體。



2. 選擇 Networking (聯網) 標籤，然後選擇 Create static IP (建立靜態 IP)。



3. 靜態 IP 位置，連接的執行個體是您之前在此教學課程中預先選取的。



4. 輸入靜態 IP 的名稱。

資源名稱：

- 每個 Lightsail 帳戶 AWS 區域 中的每個項目都必須是唯一的。
- 必須包含 2 至 255 個字元。
- 開頭和結尾必須是英數字元或數字。
- 可以包含英數字元、數字、句點、破折號和底線。

## 5. 選擇建立。



Create and attach a static IP

Create and attach a **Static IP** as a stable endpoint before assigning a domain to **LAMP\_PHP\_8-1**.

---

Identify your static IP

Your Lightsail resources must have unique names.

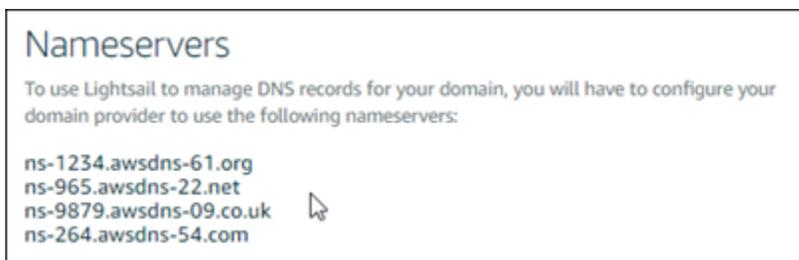
Name can contain letters and numbers; hyphen (-), period (.) and underscore (\_) characters can separate words.

## 步驟 5：建立 DNS 區域並將域對應至您的 Windows Server 2016 執行個體

將您網域 DNS 記錄的管理作業移轉至 Lightsail。這可讓您更輕鬆地將網域對應至 Windows 伺服器 2016 年執行個體，並使用 Lightsail 主控台管理您網站的所有資源。如需詳細資訊，請參閱 Lightsail 說明文件中的[建立 DNS 區域以管理網域的 DNS 記錄](#)。

1. 在首頁的 [網域和 DNS] 索引標籤上，選擇 [建立 DNS 區域]。
2. 輸入您的網域，然後選擇 Create DNS zone (建立 DNS 區域)。
3. 記下此頁面上列出的名稱伺服器地址。

您可以將這些名稱伺服器位址新增至網域名稱的註冊機構，以便將網域 DNS 記錄的管理轉移至 Lightsail。



Nameservers

To use Lightsail to manage DNS records for your domain, you will have to configure your domain provider to use the following nameservers:

- ns-1234.awsdns-61.org
- ns-965.awsdns-22.net
- ns-9879.awsdns-09.co.uk
- ns-264.awsdns-54.com

4. 將網域的 DNS 記錄管理轉移至 Lightsail 之後，請新增 A 記錄，將網域頂點指向 LAMP 執行個體，如下所示：
  - a. 在 DNS 區域的 Assignments (指派) 索引標籤中，選擇 Add assignment (新增指派)。
  - b. 在 Select a domain (選取網域) 欄位中，選擇網域或子網域。
  - c. 在 Select a resource (選取資源) 下拉式清單中，選取您先前在本教學課程中建立的 LAMP 執行個體。
  - d. 選擇 Assign (指派)。

稍微等待一些時間，讓變更傳遞至整個網際網路的 DNS，之後您的網域才會開始將流量路由至您的 LAMP 執行個體。

## 後續步驟

以下是您在 Amazon Lightsail 中啟動視窗伺服器 2016 年執行個體之後可以執行的一些其他步驟：

- [建立 Windows Server 執行個體的快照](#)
- [保護 Windows 伺服器型 Lightsail 執行個體的最佳做法](#)
- [建立區塊儲存磁碟並將其附接至 Windows Server 執行個體](#)
- [擴展 Windows Server 執行個體的儲存空間](#)

## 監控 Lightsail API 活動 AWS CloudTrail

Amazon Lightsail 與這項服務整合在一起 AWS CloudTrail，可提供 Lightsail 中使用者、角色或服務所採取的動作記錄的 AWS 服務。CloudTrail 將所有對 Lightsail 的 API 呼叫擷取為事件。擷取的呼叫包括來自 Lightsail 主控台的呼叫，以及對 Lightsail API 作業的程式碼呼叫。如果您建立追蹤，您可以啟用持續交付 CloudTrail 事件到 Amazon S3 儲存貯體，包括 Lightsail 的事件。如果您未設定追蹤，您仍然可以在 [事件歷程記錄] 中檢視 CloudTrail 主控台中最近的事件。使用收集的資訊 CloudTrail，您可以判斷向 Lightsail 提出的要求、提出要求的來源 IP 位址、提出要求的人員、提出要求的時間以及其他詳細資訊。

若要進一步了解 CloudTrail，請參閱使[AWS CloudTrail 用者指南](#)。

## Lightsail 資訊 CloudTrail

CloudTrail 在您創建 AWS 帳戶時，您的帳戶已啟用。當活動在 Lightsail 中發生時，該活動會與事件歷史記錄中的其他 AWS 服務 CloudTrail 事件一起記錄在事件中。您可以在帳戶中查看，搜索和下載最近的事 AWS 件。如需詳細資訊，請參閱[檢視具有事 CloudTrail 件記錄的事件](#)。

如需 AWS 帳戶中持續記錄事件 (包括 Lightsail 的活動)，請建立追蹤。追蹤可 CloudTrail 將日誌檔交付到 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。追蹤記錄來自 AWS 分區中所有區域的事件，並將日誌檔傳送到您指定的 Amazon S3 儲存貯體。此外，您還可以設定其他 AWS 服務，以進一步分析 CloudTrail 記錄中收集的事件資料並採取行動。如需詳細資訊，請參閱下列內容：

- [建立追蹤的概觀](#)
- [CloudTrail 支援的服務與整合](#)
- [設定 Amazon SNS 通知 CloudTrail](#)
- [從多個區域接收 CloudTrail 記錄檔並從多個帳戶接收 CloudTrail 記錄檔](#)

所有 Lightsail 動作都會記錄 CloudTrail 並記錄在 [Amazon Lightsail API 參考資料](#)中。例如，呼叫 GetInstance、AttachStaticIp 和 RebootInstance 區段會在 CloudTrail 記錄檔中產生項目。

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

- 要求是使用 root 或 AWS Identity and Access Management (IAM) 使用者認證提出的。
- 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](#)。

## 瞭解 Lightsail 記錄檔項目

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

# 建立 HAR 檔案以進 Lightsail 難排解

如果您在使用 Amazon Lightsail 主控台或 Lightsail 虛擬私人伺服器 (VPS) 時遇到問題，AWS Support 可能會要求您從網頁瀏覽器提交 HAR 檔案。HAR 檔案包含重要資訊，可協助疑難排解常見及難以診斷的問題。HAR 檔案還允許調 AWS Support 查或複製這些問題。

## Important

HAR 檔案可能會擷取敏感資訊，例如使用者名稱、密碼和金鑰。請務必移除 HAR 檔案中的任何敏感資訊再共用。

在本指南中，您會了解如何從網頁瀏覽器建立 HAR 檔案。HTTP 封存 (HAR) 檔案是 JSON 檔案，其中包含您瀏覽器記錄的最新網路活動。請依照此 step-by-step 程序建立 HAR 檔案。

## 內容

- [第 1 步：在瀏覽器中建立 HAR 檔案](#)
- [第 2 步：編輯 HAR 檔案以移除敏感資訊](#)
- [第 3 步：提交 HAR 檔案以供檢視](#)

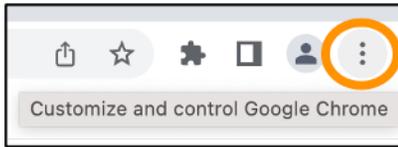
## 第 1 步：在瀏覽器中建立 HAR 檔案

### Note

下列指示最近一次是在 Google Chrome 101.0.4951.64 版、Microsoft Edge (Chromium) 101.0.1210.47 版，以及 Mozilla Firefox 91.9 版上測試。由於這些瀏覽器是第三方產品，因此這些指示可能與最新版本或您所使用版本中的體驗不符。在舊版 Microsoft Edge (EdgeHTML)，或適用於 macOS 的 Apple Safari 等其他瀏覽器中，產生 HAR 檔案的流程可能相似，但步驟會有所不同。

## Google Chrome

1. 在瀏覽器的右上角，選擇 **Customize and control Google Chrome** (自訂及管理 Google Chrome)。

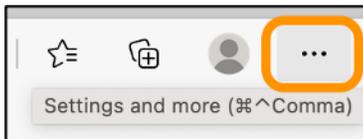


2. 停在 More tools (更多工具) 上，然後選擇 Developer tools (開發人員工具)。
3. 在瀏覽器中 DevTools 開啟時，選擇「網路」面板。
4. 選取 Preserve log (保留記錄) 核取方塊。
5. 選擇 Clear (清除) 以清除所有目前網路要求。
6. 重現您面臨的問題
7. 在中 DevTools，開啟任何網路要求的內容 (按一下滑鼠右鍵) 功能表。
8. 選擇 Save all as HAR with content (全部以 HAR 格式儲存內容)，然後儲存檔案。

如需詳細資訊，請參閱 Google [開發人員網站上的開啟 Chrome DevTools](#) 和將所有網路要求儲存至 [HAR 檔案](#)。

### Microsoft Edge (Chromium)

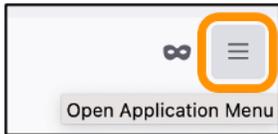
1. 在瀏覽器的右上角，選擇 Settings and more (設定及其他)。



2. 停在 More tools (更多工具) 上，然後選擇 Developer tools (開發人員工具)。
3. 在瀏覽器中 DevTools 開啟時，選擇「網路」面板。
4. 選取 Preserve log (保留記錄) 核取方塊。
5. 選擇 Clear (清除) 以清除所有目前網路要求。
6. 重現您面臨的問題
7. 在中 DevTools，開啟任何網路要求的內容 (按一下滑鼠右鍵) 功能表。
8. 選擇 Save all as HAR with content (全部儲存為內容 HAR)，然後儲存檔案。

### Mozilla Firefox

1. 在瀏覽器的右上角，選擇 Open Application Menu (開啟應用程式選單)。



2. 選擇 More tools (更多工具)，然後選擇 Web Developer tools (網頁開發者工具)。
3. 在 Web Developer (網頁開發者) 選單中，選擇 Network (網路)。(在部分 Firefox 版本中，Web Developer (網頁開發者) 選單位於 Tools (工具) 選單中。)
4. 選擇齒輪圖示，然後選取 Persist Logs (保留紀錄)。
5. 選擇垃圾桶圖示 (Clear (清除))，清除所有目前網路要求。
6. 重現您面臨的問題。
7. 在 Network Monitor (網路監控器) 中，開啟要求清單中任何網路要求的內容選單 (按一下右鍵)。
8. 選擇 Save All As HAR (用 HAR 格式儲存全部)，然後儲存檔案。

## 第 2 步：編輯 HAR 檔案以移除敏感資訊

1. 在文字編輯器應用程式中開啟 HAR 檔案。
2. 使用文字編輯器的 Find (尋找) 和 Replace (取代) 工具，找到並取代 HAR 檔案中擷取的所有敏感資訊。這包括您在建立檔案時，在瀏覽器中輸入的任何使用者名稱、密碼和金鑰。
3. 儲存移除敏感資訊的經編輯 HAR 檔案。

## 第 3 步：提交 HAR 檔案以供檢視

1. 在 [AWS Support Center Console](#) 的開啟支援案例中，選擇您的支援案例。
2. 在您的支援案例中，選擇您偏好的聯絡選項，附加編輯過的 HAR 檔案，然後提交。

## 使用 Prometheus 監控系統資源和應用程式

Prometheus 是一個開放原始碼的時間序列監控工具，用於管理各種系統資源和應用程式。其提供了多維度資料模型、查詢所收集資料的能力，以及透過 Grafana 進行詳細報告和資料視覺化的功能。

預設會啟用 Prometheus，以在其安裝所在的伺服器上收集指標。藉助節點匯出工具，您可以從其他資源 (例如 Web 伺服器、容器、資料庫、自訂應用程式和其他第三方系統) 收集指標。在本教程中，我們將向您展示如何在 Lightsail 實例上使用節點匯出器安裝和配置 Prometheus。如需可用匯出工具的完整清單，請參閱 Prometheus documentation (《Prometheus 文件》) 中的 [Exporters and integrations](#) (匯出工具和整合)。

## 內容

- [步驟 1：完成先決條件](#)
- [步驟 2：將使用者和本機系統目錄新增至 Lightsail 執行個體](#)
- [步驟 3：下載 Prometheus 二進位套件](#)
- [步驟 4：設定 Prometheus](#)
- [步驟 5：啟動 Prometheus](#)
- [步驟 6：啟動 Node Exporter](#)
- [步驟 7：使用 Node Exporter 資料收集器設定 Prometheus](#)

## 步驟 1：完成先決條件

您必須先執行下列動作，才能在 Amazon Lightsail 執行個體上安裝 Prometheus：

- 在 Lightsail 中建立實體。建議您為執行個體使用 Ubuntu 20.04 LTS 藍圖。如需詳細資訊，請參閱在 [Amazon Lightsail 中建立執行個體](#)。
- 建立靜態 IP 地址並將其連接到新的執行個體。如需詳細資訊，請參閱在 [Amazon Lightsail 中建立靜態 IP 位址](#)。
- 在新執行個體的防火牆上開啟連接埠 9090 和 9100。Prometheus 要求必須開啟連接埠 9090 和 9100。如需詳細資訊，請參閱在 [Amazon Lightsail 中新增和編輯執行個體防火牆規則](#)。

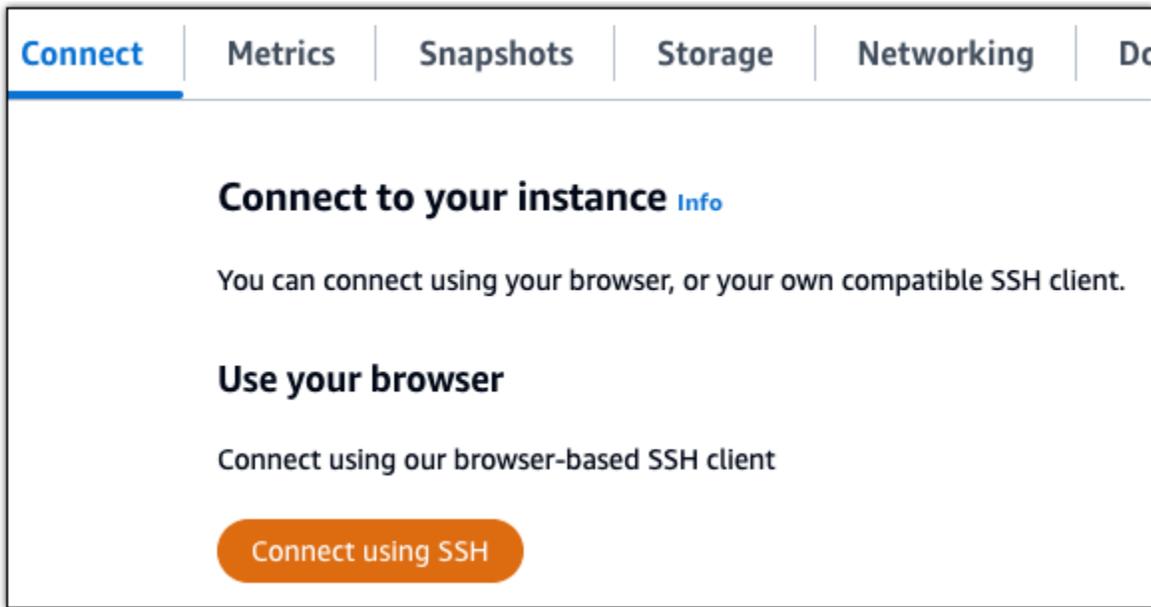
## 步驟 2：將使用者和本機系統目錄新增至 Lightsail 執行個體

請完成下列程序，以使用 SSH 連線至 Lightsail 執行個體，並新增使用者和系統目錄。此程序會建立下列 Linux 使用者帳戶：

- prometheus – 此帳戶用於伺服器環境的安裝和設定。
- exporter – 此帳戶用於設定 node\_exporter 延伸模組。

建立這些使用者帳戶的唯一目的是為了管理，因此不需要超出此設定範圍的其他使用者服務或許可。在此程序中，您還需建立目錄，用於存放和管理 Prometheus 用來監控資源的檔案、服務設定和資料。

1. 登入主 [Lightsail 台](#)。
2. 在執行個體管理頁面的 Connect (連接) 索引標籤下，選擇 Connect using SSH (使用 SSH 連接)。



3. 連接之後，請依序輸入下列命令以建立兩個 Linux 使用者帳戶：prometheus 和 exporter。

```
sudo useradd --no-create-home --shell /bin/false prometheus
```

```
sudo useradd --no-create-home --shell /bin/false exporter
```

4. 依序輸入下列命令以建立本機系統目錄。

```
sudo mkdir /etc/prometheus /var/lib/prometheus
```

```
sudo chown prometheus:prometheus /etc/prometheus
```

```
sudo chown prometheus:prometheus /var/lib/prometheus
```

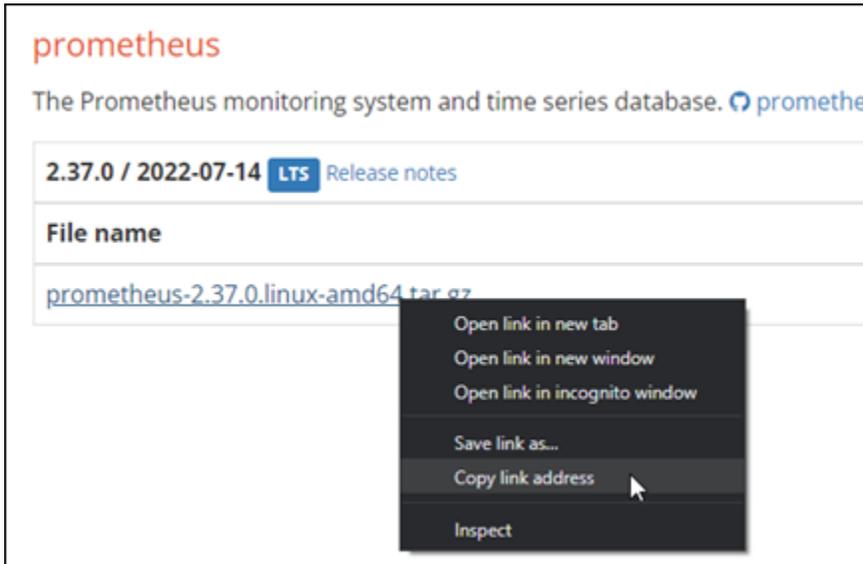
## 步驟 3：下載 Prometheus 二進位套件

請完成下列程序，將 Prometheus 二進位套件下載至您的 Lightsail 執行個體。

1. 在本機電腦上開啟 Web 瀏覽器，然後瀏覽至 [Prometheus 下載頁面](#)。
2. 在頁面頂端的 Operating system (作業系統) 下拉式選單中，選取 Linux。對於 Architecture (架構)，選取 amd64。



3. 選擇或以滑鼠右鍵按一下出現的 Prometheus 下載連結，並將連結地址複製到電腦上的文字檔案中。對於出現的 node\_exporter 下載連結重複一樣的步驟。您將在此程序的後續步驟中使用這兩個複製的地址。



4. 使用安全殼層 Connect 至您的 Lightsail 執行個體。
5. 輸入下列命令以將目錄變更為主目錄。

```
cd ~
```

6. 輸入下列命令以將 Prometheus 二進位套件下載至執行個體。

```
curl -LO prometheus-download-address
```

以您先前在此程序中複製的位址取 *prometheus-download-address* 代。此命令看起來應該像是您新增地址時的下列範例。

```
curl -LO https://github.com/prometheus/prometheus/releases/download/v2.37.0/prometheus-2.37.0.linux-amd64.tar.gz
```

7. 輸入下列命令以將 node\_exporter 二進位套件下載至執行個體。

```
curl -LO node_exporter-download-address
```

將 `node_exporter-download-address` 取代為您在此程序的上一個步驟中複製的位址。此命令看起來應該像是您新增地址時的下列範例。

```
curl -LO https://github.com/prometheus/node_exporter/releases/download/v1.3.1/node_exporter-1.3.1.linux-amd64.tar.gz
```

- 依序執行下列命令，擷取下載的 Prometheus 和 Node Exporter 檔案的內容。

```
tar -xvf prometheus-2.37.0.linux-amd64.tar.gz
```

```
tar -xvf node_exporter-1.3.1.linux-amd64.tar.gz
```

擷取下載檔案的內容後，系統便會建立數個子目錄。

- 依序輸入下列命令，將擷取的 prometheus 和 promtool 檔案複製到 `/usr/local/bin` 程式目錄。

```
sudo cp -p ./prometheus-2.37.0.linux-amd64/prometheus /usr/local/bin
```

```
sudo cp -p ./prometheus-2.37.0.linux-amd64/promtool /usr/local/bin
```

- 輸入下列命令，將 prometheus 和 promtool 檔案的擁有權變更為您先前在本教學課程中建立的 prometheus 使用者。

```
sudo chown prometheus:prometheus /usr/local/bin/prom*
```

- 依序輸入下列命令，將 `consoles` 和 `console_libraries` 子目錄複製到 `/etc/prometheus`。此 `-r` 選項會執行階層中所有目錄的遞迴副本。

```
sudo cp -r ./prometheus-2.37.0.linux-amd64/consoles /etc/prometheus
```

```
sudo cp -r ./prometheus-2.37.0.linux-amd64/console_libraries /etc/prometheus
```

- 依序輸入下列命令，將複製檔案的擁有權變更為您先前在本教學課程中建立的 prometheus 使用者。此 `-R` 選項會對階層中的所有檔案和目錄執行遞迴擁有權變更。

```
sudo chown -R prometheus:prometheus /etc/prometheus/consoles
```

```
sudo chown -R prometheus:prometheus /etc/prometheus/console_libraries
```

13. 依序輸入下列命令，將組態檔案 `prometheus.yml` 複製到 `/etc/prometheus` 目錄，並將複製檔案的擁有權變更為您先前在本教學課程中建立的 `prometheus` 使用者。

```
sudo cp -p ./prometheus-2.37.0.linux-amd64/prometheus.yml /etc/prometheus
```

```
sudo chown prometheus:prometheus /etc/prometheus/prometheus.yml
```

14. 輸入下列命令，將 `./node_exporter*` 子目錄中的 `node_exporter` 檔案複製到 `/usr/local/bin` 程式目錄。

```
sudo cp -p ./node_exporter-1.3.1.linux-amd64/node_exporter /usr/local/bin
```

15. 輸入下列命令，將檔案的擁有權變更為您先前在本教學課程中建立的 `exporter` 使用者。

```
sudo chown exporter:exporter /usr/local/bin/node_exporter
```

## 步驟 4：設定 Prometheus

請完成下列程序來設定 Prometheus。在此程序中，您需開啟並編輯 `prometheus.yml` 檔案，其中包含 Prometheus 工具的各種設定。Prometheus 會根據您在檔案中進行的設定來建立監控環境。

1. 使用安全殼層 Connect 至您的 Lightsail 執行個體。
2. 輸入下列命令來建立 `prometheus.yml` 檔案的備份複本，之後再開啟並進行編輯。

```
sudo cp /etc/prometheus/prometheus.yml /etc/prometheus/prometheus.yml.backup
```

3. 輸入下列命令，以使用 Vim 來開啟 `prometheus.yml` 檔案。

```
sudo vim /etc/prometheus/prometheus.yml
```

以下是一些您可能想要在 `prometheus.yml` 檔案中設定的重要參數：

- `scrape_interval` - 此參數位於 `global` 標頭下，可定義 Prometheus 針對指定目標將收集或湊集指標資料的時間間隔 (以秒為單位)。如 `global` 標籤所示，這個設定對 Prometheus 監

控的所有資源通用。除非個別匯出工具提供不同的值，而此值會覆寫全域值，否則此設定也適用於匯出工具。您可以保持將此參數設定為目前值：15 秒。

- `job_name` - 此參數是位於 `scrape_configs` 標頭下的標籤，用於識別資料查詢或視覺顯示結果集中的匯出工具。您可以指定任務名稱的值，以如實反映環境中正在被監控的資源。例如，您可以將用於管理網站的任務標示為 `business-web-app`，您也可以將資料庫標示為 `mysql-db-1`。在此初始設定中，您監控的只有 Prometheus 伺服器，因此您可以維持目前的 `prometheus` 值。
- `targets` - `targets` 設定位於 `static_configs` 標頭下，它使用 `ip_addr:port` 鍵值對來識別指定匯出工具的執行位置。將在此程序的步驟 4 - 7 中變更預設設定。

```
my global config
global:
  A scrape_interval: 15s # Set the scrape interval to every 15 seconds. Default is every 1 minute.
  evaluation_interval: 15s # Evaluate rules every 15 seconds. The default is every 1 minute.
  # scrape_timeout is set to the global default (10s).

# Alertmanager configuration
alerting:
  alertmanagers:
    - static_configs:
      - targets:
        # - alertmanager:9093

# Load rules once and periodically evaluate them according to the global 'evaluation_interval'.
rule_files:
  # - "first_rules.yml"
  # - "second_rules.yml"

# A scrape configuration containing exactly one endpoint to scrape:
# Here it's Prometheus itself.
scrape_configs:
  # The job name is added as a label 'job=<job_name>' to any timeseries scraped from this config.
  B - job_name: "prometheus"

  # metrics_path defaults to '/metrics'
  # scheme defaults to 'http'.

  C static_configs:
    - targets: ["localhost:9090"]
```

#### Note

對於此初始設定，您不需要設定 `alerting` 和 `rule_files` 參數。

4. 在您於 Vim 中開啟的 `prometheus.yml` 檔案中，請按 `I` 鍵以在 Vim 中進入插入模式。
5. 捲動並找到位於 `static_configs` 標頭下的 `targets` 參數。
6. 將預設設定變更為 `<ip_addr>:9090`。使用執行個體的靜態 IP 地址取代 `<ip_addr>`。修改後的參數看起來應該如下列範例所示。

```
static_configs:  
- targets: ["192.0.2.0:9090"]
```

- 按 ESC 鍵以退出插入模式，然後輸入 `:wq!` 以儲存您所做的變更並退出 Vim。
- (選用) 如果發生問題，請輸入下列命令，以使用您先前在此程序中建立的備份檔案取代 `prometheus.yml` 檔案。

```
sudo cp /etc/prometheus/prometheus.yml.backup /etc/prometheus/prometheus.yml
```

## 步驟 5：啟動 Prometheus

完成下列程序來啟動執行個體上的 Prometheus 服務。

- 使用安全殼層 Connect 至您的 Lightsail 執行個體。
- 輸入下列命令以啟動 Prometheus 服務。

```
sudo -u prometheus /usr/local/bin/prometheus --config.file /etc/prometheus/  
prometheus.yml --storage.tsdb.path /var/lib/prometheus --web.console.templates=  
etc/prometheus/conssoles --web.console.libraries=/etc/prometheus/console_libraries
```

此命令行會輸出有關啟動程序和其他服務的詳細資訊。其還應該表明該服務正在連接埠 9090 上接聽。

```
ts=2022-06-02T15:46:09.336Z caller=main.go:993 level=info fs_type=EXT4_SUPER_MAGIC  
ts=2022-06-02T15:46:09.336Z caller=main.go:996 level=info msg="TSDB started"  
ts=2022-06-02T15:46:09.336Z caller=main.go:1177 level=info msg="Loading configuration file" filename=/etc/prometheus/prometheus.yml  
ts=2022-06-02T15:46:09.345Z caller=main.go:1214 level=info msg="Completed loading of configuration file" filename=/etc/prometheus/prometheus.yml  
totalDuration=8.392805ms db_storage=1.681µs remote_storage=2.294µs web_handler=1.213µs query_engine=1.435µs scrape=7.967101ms scrape_sd=48.64µs n  
otify=1.931µs notify_sd=2.455µs rules=2.669µs tracing=6.382µs  
ts=2022-06-02T15:46:09.345Z caller=main.go:957 level=info msg="Server is ready to receive web requests."  
ts=2022-06-02T15:46:09.345Z caller=manager.go:937 level=info component="rule manager" msg="Starting rule manager..."
```

如果服務未啟動，請參閱本教學課程的 [Step 1: Complete the prerequisites](#) (步驟 1：完成先決條件) 一節，了解有關建立執行個體防火牆規則以允許此連接埠上流量的詳細資訊。若是其他錯誤，請檢閱 `prometheus.yml` 檔案以確認沒有語法錯誤。

- 驗證執行中的服務後，按 `Ctrl+C` 來停止服務。
- 輸入下列命令，即可在 Vim 中開啟 `systemd` 組態檔案。此檔案用於啟動 Prometheus。

```
sudo vim /etc/systemd/system/prometheus.service
```

- 在檔案中插入下列行。

```
[Unit]
```

```
Description=PromServer
Wants=network-online.target
After=network-online.target

[Service]
User=prometheus
Group=prometheus
Type=simple
ExecStart=/usr/local/bin/prometheus \
--config.file /etc/prometheus/prometheus.yml \
--storage.tsdb.path /var/lib/prometheus/ \
--web.console.templates=/etc/prometheus/consoles \
--web.console.libraries=/etc/prometheus/console_libraries

[Install]
WantedBy=multi-user.target
```

Linux systemd Service Manager 會使用先前的指令在伺服器上啟動 Prometheus。叫用時，Prometheus 會以 prometheus 使用者的身分執行和參照用於載入組態設定並將時間序列資料存放在 /var/lib/prometheus 目錄中的 prometheus.yml 檔案。您可以從命令列執行 man systemd 以查看關於服務的詳細資訊。

- 按 ESC 鍵以退出插入模式，然後輸入 :wq! 以儲存您所做的變更並退出 Vim。
- 輸入下列命令以將資訊載入 systemd Service Manager。

```
sudo systemctl daemon-reload
```

- 輸入下列命令以重新啟動 Prometheus。

```
sudo systemctl start prometheus
```

- 輸入下列命令以檢查 Prometheus 服務的狀態。

```
sudo systemctl status prometheus
```

如果此服務已正確啟動，您會收到類以下列範例的輸出。

```
ubuntu@ip-172-26-11-170:~$ sudo systemctl status prometheus
● prometheus.service - PrometheusServer
   Loaded: loaded (/etc/systemd/system/prometheus.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2022-06-02 16:03:33 UTC; 2s ago
     Main PID: 105938 (prometheus)
        Tasks: 6 (limit: 1164)
       Memory: 39.3M
      CGroup: /system.slice/prometheus.service
             └─105938 /usr/local/bin/prometheus --config.file /etc/prometheus/prometheus.yml --storage.tsdb.path /var/lib/prometheus/
```

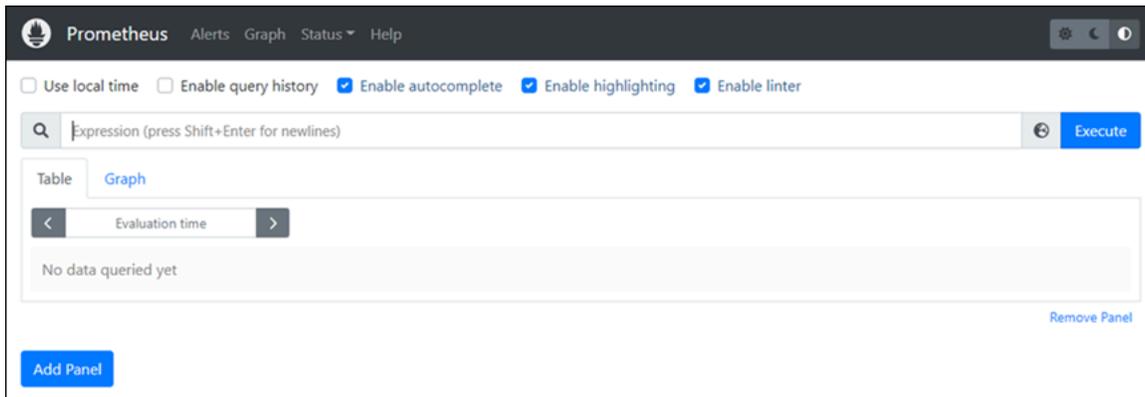
- 按 Q 以結束狀態命令。
- 在執行個體啟動時輸入下列命令以啟動 Prometheus。

```
sudo systemctl enable prometheus
```

- 在本機電腦上開啟 Web 瀏覽器，然後前往以下網址以檢視 Prometheus 管理介面。

```
http:<ip_addr>:9090
```

<ip\_addr>以您的 Lightsail 執行個體的靜態 IP 位址取代。您應該會看到類似以下範例的儀表板。



## 步驟 6：啟動 Node Exporter

請完成下列程序來啟動 Node Exporter 服務。

- 使用安全殼層 Connect 至您的 Lightsail 執行個體。
- 輸入下列命令，使用 Vim 為 node\_exporter 建立 systemd 服務檔案。

```
sudo vim /etc/systemd/system/node_exporter.service
```

- 按 I 鍵以在 Vim 中進入插入模式。
- 在檔案中新增下列文字行。這將為 node\_exporter 設定監控收集器的 CPU 負載、檔案系統使用情形和記憶體資源。

```
[Unit]
Description=NodeExporter
Wants=network-online.target
After=network-online.target
```

```
[Service]
User=exporter
Group=exporter
Type=simple
ExecStart=/usr/local/bin/node_exporter --collector.disable-defaults \
--collector.meminfo \
--collector.loadavg \
--collector.filesystem

[Install]
WantedBy=multi-user.target
```

### Note

這些指示會停用 Node Exporter 的預設機器指標。如需 Ubuntu 可用指標的完整清單，請參閱 Ubuntu documentation (《Ubuntu 文件》) 中的 [Prometheus node\\_exporter man page](#) (Prometheus node\_exporter 手冊頁)。

- 按 ESC 鍵以退出插入模式，然後輸入 :wq! 以儲存您所做的變更並退出 Vim。
- 輸入下列命令以重新載入 systemd 程序。

```
sudo systemctl daemon-reload
```

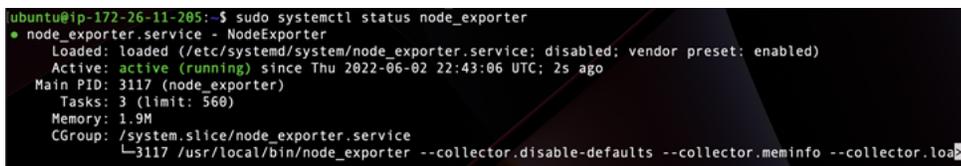
- 輸入下列命令以啟動 node\_exporter 服務。

```
sudo systemctl start node_exporter
```

- 輸入下列命令以檢查 node\_exporter 服務的狀態。

```
sudo systemctl status node_exporter
```

如果此服務成功啟動，您會收到類似下列範例的輸出。



```
ubuntu@ip-172-26-11-205:~$ sudo systemctl status node_exporter
● node_exporter.service - NodeExporter
   Loaded: loaded (/etc/systemd/system/node_exporter.service; disabled; vendor preset: enabled)
   Active: active (running) since Thu 2022-06-02 22:43:06 UTC; 2s ago
     Main PID: 3117 (node_exporter)
        Tasks: 3 (limit: 560)
       Memory: 1.9M
      CGroup: /system.slice/node_exporter.service
              └─3117 /usr/local/bin/node_exporter --collector.disable-defaults --collector.meminfo --collector.loa
```

- 按 Q 以結束狀態命令。
- 在執行個體啟動時輸入下列命令以啟用 Node Exporter。

```
sudo systemctl enable node_exporter
```

## 步驟 7：使用 Node Exporter 資料收集器設定 Prometheus

完成下列程序來使用 Node Exporter 資料收集器設定 Prometheus。您可以透過在 `prometheus.yml` 檔案中為 `node_exporter` 新增 `job_name` 參數來做到這一點。

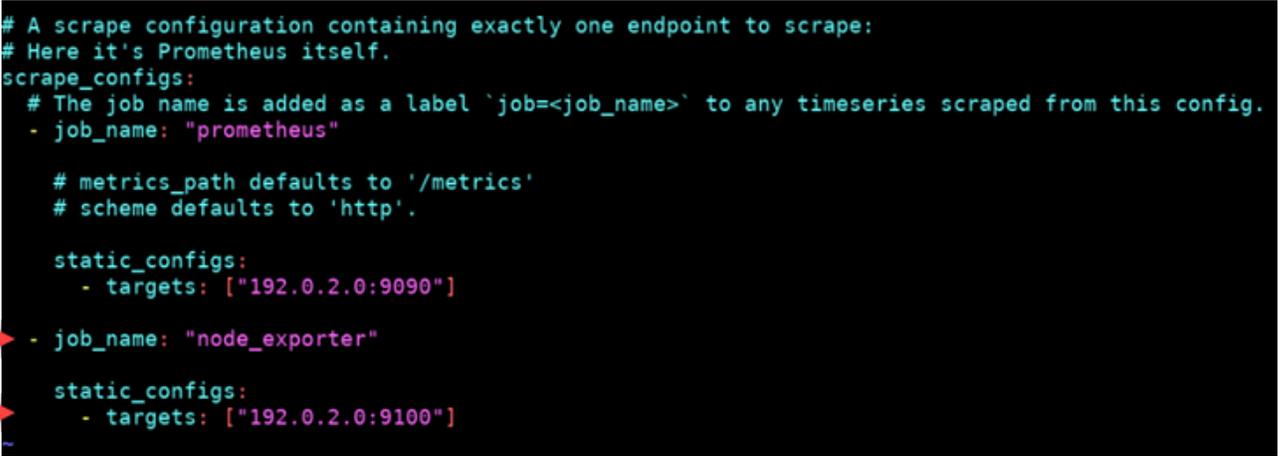
1. 使用安全殼層 Connect 至您的 Lightsail 執行個體。
2. 輸入下列命令，以使用 Vim 來開啟 `prometheus.yml` 檔案。

```
sudo vim /etc/prometheus/prometheus.yml
```

3. 按 `I` 鍵以在 Vim 中進入插入模式。
4. 將以下幾行文字新增到檔案中現有 `- targets: ["<ip_addr>:9090"]` 參數下方。

```
- job_name: "node_exporter"  
  
static_configs:  
- targets: ["<ip_addr>:9100"]
```

`prometheus.yml` 檔案中修改後的參數看起來應該如下列範例所示。



```
# A scrape configuration containing exactly one endpoint to scrape:  
# Here it's Prometheus itself.  
scrape_configs:  
  # The job name is added as a label `job=<job_name>` to any timeseries scraped from this config.  
  - job_name: "prometheus"  
  
    # metrics_path defaults to '/metrics'  
    # scheme defaults to 'http'.  
  
    static_configs:  
      - targets: ["192.0.2.0:9090"]  
  
  - job_name: "node_exporter"  
  
    static_configs:  
      - targets: ["192.0.2.0:9100"]
```

注意下列事項：

- Node Exporter 會接聽連接埠 9100，讓 prometheus 伺服器能夠湊集資料。如本教學課程的 [Step 1: Complete the prerequisites](#) (步驟 1：完成先決條件) 一節所述，確認您已遵循執行個體防火牆規則的建立步驟。
  - 如同的設定一樣 prometheusjob\_name，<ip\_addr>請以連接到 Lightsail 執行個體的靜態 IP 位址取代。
5. 按 ESC 鍵以退出插入模式，然後輸入 :wq! 以儲存您所做的變更並退出 Vim。
  6. 輸入下列命令以重新啟動 Prometheus 服務，如此對組態檔案所做的變更才會生效。

```
sudo systemctl restart prometheus
```

7. 輸入下列命令以檢查 Prometheus 服務的狀態。

```
sudo systemctl status prometheus
```

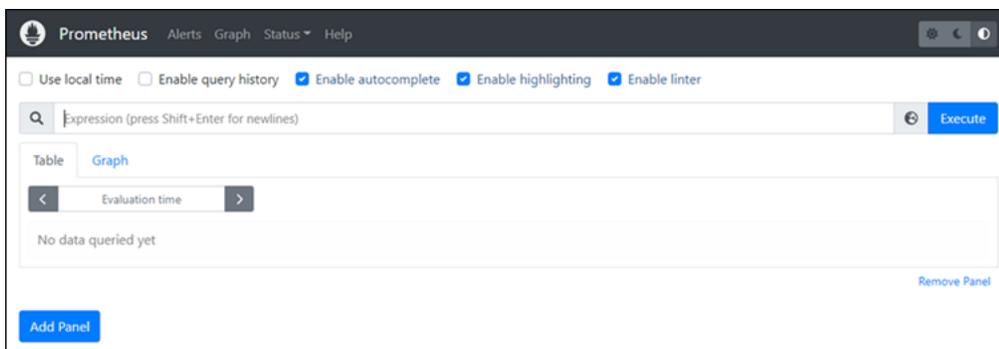
如果此服務已正確重新啟動，您會收到類似以下的輸出。

```
ubuntu@ip-172-26-11-178:~$ sudo systemctl status prometheus
● prometheus.service - PrometheusServer
   Loaded: loaded (/etc/systemd/system/prometheus.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2022-06-02 16:03:33 UTC; 2s ago
     Main PID: 105938 (prometheus)
       Tasks: 6 (Limit: 1164)
      Memory: 39.3M
   CGroup: /system.slice/prometheus.service
           └─105938 /usr/local/bin/prometheus --config.file /etc/prometheus/prometheus.yml --storage.tsdb.path /var/lib/prometheus/
```

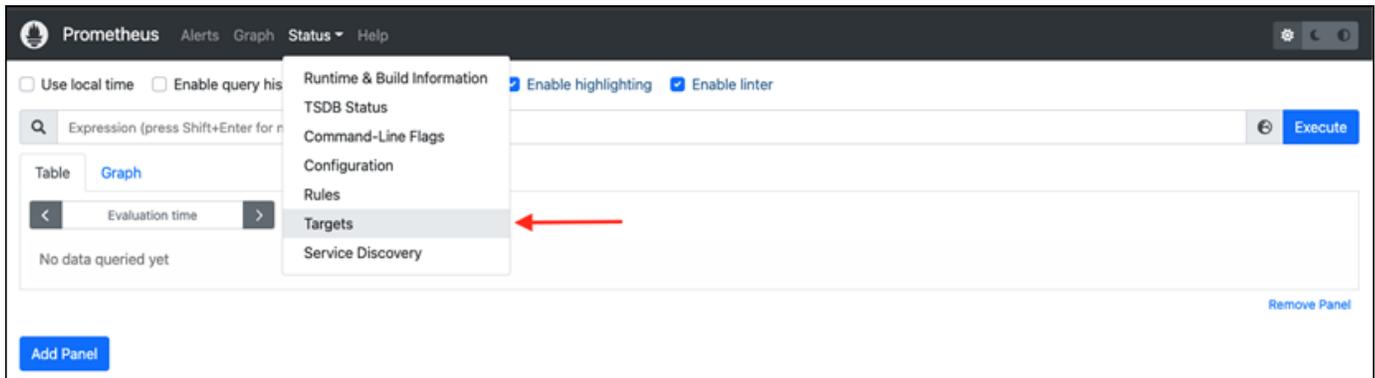
8. 按 Q 以結束狀態命令。
9. 在本機電腦上開啟 Web 瀏覽器，然後前往以下網址以檢視 Prometheus 管理介面。

```
http:<ip_addr>:9090
```

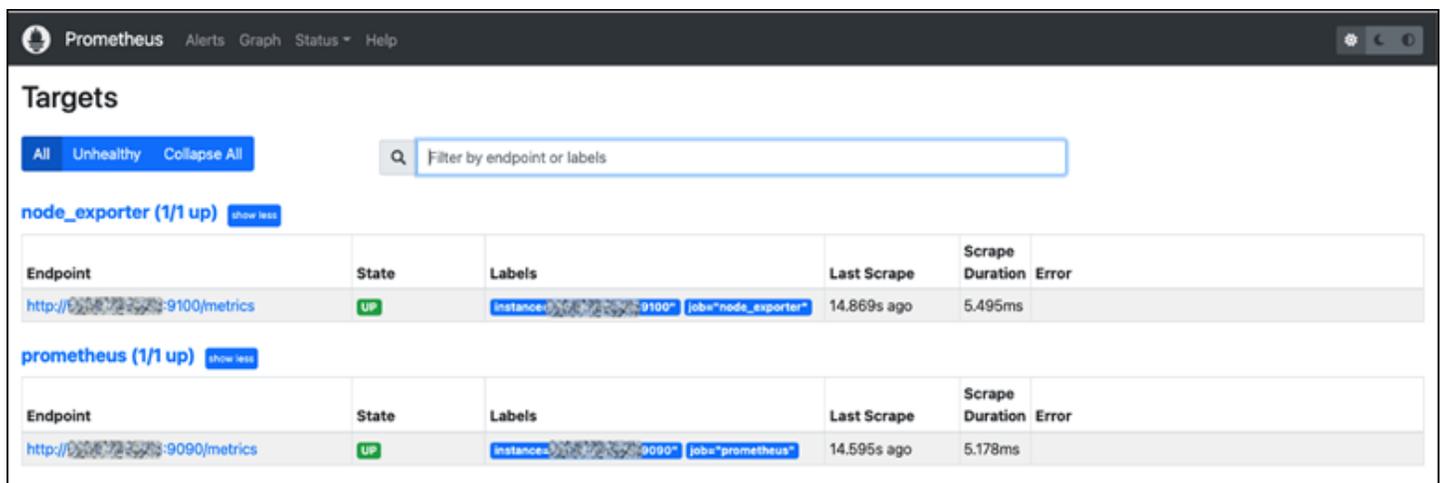
<ip\_addr>以您的 Lightsail 執行個體的靜態 IP 位址取代。您應該會看到類似以下範例的儀表板。



10. 在主選單中，選擇 Status (狀態) 下拉式選單並選取 Targets (目標)。



您應該會在下一個畫面上看到兩個目標。第一個目標適用於 `node_exporter` 指標收集器任務，第二個目標適用於 `prometheus` 任務。



現在已正確設定環境，可收集指標和監控伺服器。

## 使用 scp 在 Lightsail 上的 Linux 執行個體之間傳輸檔案

使用 Linux 中的安全複製 (`scp`) 命令，將檔案從本機電腦傳輸到 Linux 或 Unix 執行個體，並在 Amazon Lightsail 中從一個執行個體傳輸到另一個執行個體。要了解有關 `scp` 命令的更多信息，請參閱 [man 7 網站上的 `scp \( 1 \) -Linux 手冊頁面`](#)。

本教學課程將逐步引導您將檔案從一個 Lightsail 實體複製到另一個實體。

### 目錄

- [必要條件](#)
- [步驟 1：將私鑰 \( `.pem` \) 文件保存到本地計算機](#)
- [步驟 2：變更私密金鑰的權限](#)

- [步驟 3：將私密金鑰轉移到執行個體](#)
- [步驟 4：安全地在 Lightsail Linux 和 Unix 執行個體之間傳輸檔案](#)

## 必要條件

- 您有兩個 Lightsail 執行個體在執行中，而且兩個執行個體都有公用 IP 位址。取得執行個體的公用 IP 位址。登入 [Lightsail 主控台](#)，然後複製顯示在執行個體旁邊的公用 IP 位址。
- 您可以使用 SSH key pair 存取這兩個執行個體。如需詳細資訊，請參閱[連接至 Linux 執行個體](#)。

## 步驟 1：將私鑰 (.pem) 文件保存到本地計算機

完成下列步驟，將私密金鑰 (.pem) 檔案儲存到本機電腦。目標執行個體的私密金鑰檔案會用來安全地將檔案從一個執行個體傳輸到另一個執行個體。若要在同一個執行個體之間複製檔案 AWS 區域，您將使用該區域的預設金鑰。若要在不同區域的執行個體之間複製檔案，您需要針對目標執行個體所在的區域使用預設金鑰。若要深入瞭解金鑰配對，請參閱[SSH並連線至執行個體](#)。

### Note

如果您使用自己的金鑰組，或是使用 Lightsail 主控台建立 key pair，請找出您自己的私密金鑰，並使用該金鑰連線至執行個體。當您上傳自己的金鑰或使用 Lightsail 主控台建立 key pair 時，Lightsail 不會儲存您的私密金鑰。如果沒有私鑰，則無法使用 scp 將文件傳輸到實例。

將私密金鑰 (.pem) 儲存到本機電腦

1. 登入主 [Lightsail](#) 台。
2. 在頂部導航欄上選擇您的用戶名，然後選擇帳戶從下拉菜單中。
3. 選擇 [SSH金鑰] 索引標籤。
4. 向下捲動至頁面的 Default keys (預設金鑰) 區段。
5. 針對您要傳輸檔案的目標執行個體所 AWS 區域 在位置，選擇預設私密金鑰旁邊的 [下載]。

### Default keys

With default key pairs, you can connect to Linux instances using an SSH client, and retrieve administrator passwords for Windows instances.

You can download or delete your default key pairs. You can create one default key per AWS Region where you previously created resources.

[+ Create key pair](#)

Region name	Region code	Created		
Frankfurt	eu-central-1	April 27, 2018, 3:14 PM		
Ireland	eu-west-1	April 27, 2018, 3:14 PM		
Mumbai	ap-south-1	April 20, 2018, 2:54 PM		
Ohio	us-east-2	February 2, 2022, 4:17 PM		
Oregon	us-west-2	April 19, 2018, 9:11 AM		
Seoul	ap-northeast-2	August 23, 2018, 9:11 AM		
Singapore	ap-southeast-1	June 20, 2018, 3:45 PM		
Stockholm	eu-north-1	May 13, 2021, 10:03 AM		
Sydney	ap-southeast-2	April 30, 2019, 3:51 PM		

## 6. 將您的私有金鑰存放在本機磁碟上的安全位置。

您可能想要將下載的金鑰移至儲存所有SSH金鑰的目錄，例如使用者主目錄中的「金鑰」資料夾。您需要參考本指南下一節中儲存私有金鑰的目錄。如果私有金鑰嘗試儲存為 .pem 以外的格式，則應在儲存之前手動將格式更改為 .pem。

## 步驟 2：變更私密金鑰的權限

在下列程序中，您需變更私有金鑰檔案的許可，以確保只有您可讀取和寫入該檔案。

### 變更私密金鑰檔案的權限

1. 在您的本機電腦上開啟終端機視窗。
2. 輸入下列命令，讓金鑰對的私有金鑰只能由您讀取和寫入。這是某些作業系統所需的安全性最佳實務。

```
sudo chmod 400 /path/to/private-key.pem
```

在命令中，將 `/path/to/private-key` 取代為儲存執行個體正使用的金鑰對之私有金鑰的目錄路徑。

範例：

```
sudo chmod 400 /Users/user/Keys/LightsailDefaultKey-us-west-2.pem
```

### 步驟 3：將私密金鑰轉移到執行個體

在下列程序中，您會從本機電腦執行 `scp` 指令，將私密金鑰傳輸到來源執行個體。

使用 `scp` 將私密金鑰從電腦傳輸到來源執行個體

1. 判斷私密金鑰檔案在電腦上的位置，以及執行個體上的目標路徑。在下列範例中，私密金鑰檔案的名稱為 `private-key.pem`，來源執行環境的使用者名稱為 `ec2-user`，來源執行環境的IPv4地址為 `public-ipv4-address`，而來源執行環境的IPv6地址為 `public-ipv6-address`。該 `destination-path/` 是您要將私密金鑰移轉至的來源執行環境上的位置。

#### Note

您可以根據執行個體使用的藍圖指定下列其中一個使用者名稱：

- AlmaLinux 作業系統 9、Amazon Linux 2、Amazon Linux 2023、CentOS 串流 9、免費BSD和開放SUSE的執行個體：`ec2-user`
  - Debian 執行個體：`admin`
  - Ubuntu 執行個體：`ubuntu`
  - Bitnami 執行個體：`bitnami`
  - Plesk 執行個體：`ubuntu`
  - cPanel WHM實例 (E)：`centos`
- (IPv4) 若要將私密金鑰檔案傳輸至執行個體，請從您的電腦輸入下列指令。

```
scp -i /path/private-key.pem /path/private-key.pem ec2-user@public-ipv4-address:path/
```

- (IPv6) 若要在執行個體只有IPv6位址的情況下將私密金鑰檔案傳輸至執行個體，請從您的電腦輸入下列指令。地IPv6址必須用方括號 ( [ ] ) 括起來，必須轉義 ( \ )。

```
scp -i /path/private-key.pem /path/private-key.pem ec2-user@[public-ipv6-address]:path/
```

2. 如果您尚未使用連線至執行個體SSH，您會看到類似下列的回應：

```
The authenticity of host 'ec2-198-51-100-1.compute-1.amazonaws.com (10.254.142.33)'
can't be established.
RSA key fingerprint is 1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f.
Are you sure you want to continue connecting (yes/no)?
```

輸入 **yes**。

3. 如果傳輸成功，則回應會和下列內容相似：

```
Warning: Permanently added 'ec2-198-51-100-1.compute-1.amazonaws.com' (RSA)
to the list of known hosts.
private-key.pem                               100%  480    24.4KB/s   00:00
```

現在您已將私密金鑰傳輸到來源執行個體，您可以安全地連線到目標執行個體並將檔案傳輸到目標執行個體。繼續進行下一個步驟以了解操作方法。

## 步驟 4：安全地在 Lightsail Linux 和 Unix 執行個體之間傳輸檔案

在下列程序中，您將從一個執行處理 (來源執行環境) 執行 scp 命令，將檔案傳輸到另一個執行處理 (目標執行處理)。

使用 scp 在執行個體之間傳輸檔案

1. 使用 Connect 至來源執行個體SSH。您可以使用本機電腦上的終端機程式，或使用 Lightsail 中的瀏覽器型用SSH戶端進行連線。如需詳細資訊，請參閱[連接至 Linux 執行個體](#)。
2. 決定檔案在來源執行環境上的位置，以及目標執行處理上的目的地路徑。在下列範例中，私密金鑰檔案的名稱為 *private-key.pem*，執行個體的使用者名稱為 *ec2-user*，執行個體的IPv4位址為 *public-ipv4-address*，並且執行個體的IPv6位址為 *public-ipv6-address*。該 *destination-path/* 是您要將檔案傳送到目標執行個體上的位置。
  - (IPv4) 若要將檔案從來源執行環境傳輸至目標執行環境，請從來源執行環境輸入下列指令。

```
scp -i /path/private-key.pem /path/my-file.txt ec2-user@public-ipv4-address:destination-path/
```

- (IPv6) 若要將檔案從來源執行環境傳輸至目標執行環境，請從來源執行環境輸入下列指令。地 IPv6 址必須用方括號 ( [ ] ) 括起來，必須轉義 ( \ )。

```
scp -i /path/private-key.pem /path/my-file.txt ec2-user@[public-ipv6-address]:destination-path/
```

3. 如果您尚未使用連線至目標執行個體 SSH，您會看到類似下列的回應：

```
The authenticity of host 'ec2-198-51-100-1.compute-1.amazonaws.com (10.254.142.33)'
can't be established.
RSA key fingerprint is 1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f.
Are you sure you want to continue connecting (yes/no)?
```

輸入 **yes**。

4. 如果傳輸成功，則回應會和下列內容相似：

```
Warning: Permanently added 'ec2-198-51-100-1.compute-1.amazonaws.com' (RSA)
to the list of known hosts.
my-file.txt                               100%   480    24.4KB/s   00:00
```

## 透過對等互連功能將 Lightsail 與其他 AWS 服務整合 VPC

Amazon Lightsail 使用一組聚焦的 AWS 服務，例如 Amazon，EC2 並 AWS Identity and Access Management 使其更容易上手。但是，這並不表示您只能使用這些服務！

您可以透過 Amazon VPC 對等互連，將 Lightsail 資源與其他 AWS 服務整合。[瞭解如何設定 VPC 對等互連](#)。

點擊以下鏈接了解更多有關其他 AWS 服務的信息。

## 虛擬機器 (虛擬私有伺服器)

### Amazon EC2

Amazon 彈性運算雲 ( AmazonEC2 ) 是一種在雲中提供可調整大小的運算容量的 Web 服務。該服務旨在降低開發人員進行 Web 規模雲端運算的難度。

使用 Amazon，EC2 您可以以最小的摩擦來取得和設定容量。它可讓您完全控制運算資源，並讓您在經過驗證的 Amazon 運算環境中執行。Amazon 將取得和啟動新伺服器執行個體所需的時間縮

EC2短為數分鐘，因此您可以隨著運算需求的變化快速擴展和縮減容量。Amazon 讓您只需為實際使用的容量付費，從而EC2改變了運算的經濟效益。Amazon 為開發人員EC2提供各種工具來建置故障彈性應用程式，並將自己與常見故障案例隔離

[進一步了解 Amazon EC2。](#)

## Amazon VPC

Amazon Virtual Private Cloud (AmazonVPC) 可讓您佈建 AWS 雲端的邏輯隔離區段，您可以在定義的虛擬網路中啟動AWS資源。您可以完全掌控自己的虛擬聯網環境，包括選擇自己的 IP 地址範圍、建立子網路、設定路由表及網路閘道。

您可以輕鬆地為您的 Amazon 定制網絡配置VPC。例如，您可以為有權存取網際網路的 Web 伺服器建立公有子網路，然後將資料庫或應用程式伺服器等後端系統置於不能存取網際網路的私有子網路中。您可以利用多層安全性，包括安全群組和網路存取控制清單，協助控制每個子網路中 Amazon EC2 執行個體的存取。

此外，您可以在公司資料中心與您的資料中心之間建立硬體虛擬私人網路 (VPN) 連線，VPC並利用 AWS雲端做為公司資料中心的延伸。

[進一步了解 Amazon VPC。](#)

## 無伺服器運算

### AWS Lambda

AWS Lambda 可讓您執行程式碼，而無需佈建或管理伺服器。您只要按實際使用的運算時間付費即可，未執行程式碼時不必支付任何費用。使用 Lambda，您幾乎可以為任何類型的應用程式或後端服務執行程式碼，而且無須管理。您只需上傳程式碼，Lambda 就會處理執行程式碼及擴展所需的各項工作，藉此維持高可用性。您可以將程式碼設定為從其他AWS服務自動觸發，或直接從任何 Web 或行動應用程式呼叫程式碼。

[進一步了解 AWS Lambda。](#)

### Amazon API 网关

Amazon API Gateway 是一項全受管服務，可讓開發人員輕鬆地建立、發佈、維護、監控和APIs保護任何規模。只要在中按幾下 AWS Management Console，您就可以建立一API個「前門」，讓應用程式從後端服務存取資料、商務邏輯或功能。其中包括在 Amazon 上執行的工作負載EC2、在 Lambda 上執行的程式碼或任何 Web 應用程式。Amazon API Gateway 可處理接受和處理多達數

十萬個並行API呼叫所涉及的所有任務。其中包括流量管理、授權和存取控制、監控和API版本管理。Amazon API 網關沒有最低費用或啟動成本。您只需為接API聽的電話和傳出的資料量付費。

[進一步了解 Amazon API 網關。](#)

## 資料庫

### Amazon DynamoDB

Amazon DynamoDB 是一種快速且靈活的無SQL資料庫服務，適用於需要任何規模一致、10 毫秒延遲的所有應用程式。該服務為全受管的雲端資料庫，可支援文件和機碼值存放區模型。其具備彈性的資料模型與可靠的效能，是行動裝置、Web、遊戲、廣告技術、IoT 及其他眾多應用程式的不二之選。

[進一步了解 DynamoDB。](#)

### Amazon RDS

Amazon Relational Database Service (AmazonRDS) 可讓您輕鬆地在雲端中設定、操作和擴展關聯式資料庫。它既經濟實惠又可調整容量，還能用來處理耗時的資料庫管理任務，讓您得以專心開發應用程式和業務。Amazon 為您RDS提供了六個熟悉的數據庫引擎可供選擇，包括 Amazon Aurora，PostgreSQL，我的SQL，MariaDB 的，甲骨文和 Microsoft 服務器。SQL

[進一步了解 Amazon RDS。](#)

### Amazon Aurora

Amazon Aurora 是與我SQL相容的關聯式資料庫引擎，結合了高階商業資料庫的速度和可用性，以及開放原始碼資料庫的簡易性和成本效益。Aurora 以商業資料庫的安全性、可用性和可靠性提供比 My SQL 高五倍的效能，成本僅為十分之一。

[進一步了解 Amazon Aurora。](#)

## 負載平衡器

### Elastic Load Balancing

Elastic Load Balancing 可自動將傳入的應用程式流量分配到多個 Amazon EC2 執行個體 其可讓您落實應用程式容錯能力，同時無縫提供所需的負載平衡容量，以便路由應用程式流量。

Elastic Load Balancing 提供兩種負載平衡器。兩者皆具備高可用性、可自動擴展及穩健安全的特色。包括 Classic Load Balancer 和 Application Load Balancer，前者可依據應用程式或網路層級的

資訊來路由流量，而後者可依據包含請求內容的進階應用程式層級資訊來路由流量。Classic Load Balancer 非常適合在多個 Amazon EC2 執行個體之間進行簡單的流量負載平衡。Application Load Balancer 適合需要進階路由功能、微服務和容器型架構的應用程式。Application Load Balancer 可將流量路由到多個服務，或在同一 Amazon EC2 執行個體上的多個連接埠之間進行負載平衡。

[進一步了解 Elastic Load Balancing。](#)

## Application Load Balancer

應用程式負載平衡器是 Elastic Load Balancing 服務的負載平衡選項，該服務在應用程式層運作，可讓您根據多個服務或在一或多個 Amazon EC2 執行個體上執行的容器之間的內容來定義路由規則。

[進一步了解 Application Load Balancer。](#)

# 大數據

## Amazon Kinesis 服務

Amazon Kinesis 服務可讓您輕鬆使用 AWS 雲端中的即時串流資料。Amazon Kinesis 服務包括下列項目：可輕鬆將大量串流資料載入的 [Amazon 資料 Firehose](#) AWS、適用於 [Apache Flink 的亞馬遜受管服務](#) 以標準分析串流資料 SQL，以及 [Amazon Kinesis 資料串流](#) 來建置您自己的自訂應用程式來處理或分析串流資料。

[進一步了解 Amazon Kinesis 服務。](#)

## Amazon EMR

Amazon EMR 提供受管 Hadoop 架構，可讓您輕鬆、快速且符合成本效益，跨動態可擴展的 Amazon EC2 執行個體處理大量資料。您也可以亞馬遜中執行其他常用的分散式架構 HBase，例如 Apache Spark、普雷斯托和 Flink EMR，並與其他資料存放區 (例如 Amazon S3 和 DynamoDB) 中的 AWS 資料互動。

Amazon EMR 安全可靠地處理各種大數據使用案例，包括日誌分析、Web 索引、資料轉換 (ETL)、機器學習、財務分析、科學模擬和生物資訊學。

[進一步了解 Amazon EMR。](#)

## Amazon Redshift

Amazon Redshift 是一項快速的全受管 PB 級資料倉儲服務，可讓您使用現有的商業智慧工具來分析所有資料，操作簡單且符合成本效益。

[進一步了解 Amazon Redshift。](#)

## 儲存

### Amazon Simple Storage Service (Amazon S3)

Amazon S3 為開發人員和 IT 團隊提供安全、耐用、高度可擴展的雲端儲存空間。Amazon S3 是 easy-to-use 物件儲存，具有簡單的 Web 服務界面，可從 Web 上的任何位置存放和擷取任意數量的資料。使用 Amazon S3，只需按實際使用的儲存容量付費。無需支付最低費用和設定費。

Amazon S3 專門為不同使用案例提供了多種儲存類別，包括：Amazon S3 Standard，它適用於經常被存取資料的一般用途儲存；Amazon S3 Standard - Infrequent Access (Standard - IA)，它適用於長期存放但不常存取的資料；以及 S3 Glacier，它適用於長期存檔。Amazon S3 也提供可設定的生命週期政策，讓您在資料生命週期期間管理資料。一旦設定好政策，您無需對應用程式進行任何變更，系統即會自動將資料遷移至最適合的儲存類別。

Amazon S3 可單獨使用，也可以與其他AWS服務 (例如 Amazon EC2 和) 搭配使用IAM，也可以搭配雲端資料遷移服務和閘道來進行初始或持續的資料擷取。Amazon S3 提供符合成本效益的物件儲存服務，適合各種使用案例，包括備份與復原、近線性存檔、大數據分析、災難復原、雲端應用程式和內容分發。

[進一步了解 Amazon S3。](#)

### Amazon 彈性塊商店 ( AmazonEBS )

Amazon EBS 提供持久性區塊儲存磁碟區，可與AWS雲端中的 Amazon EC2 執行個體搭配使用。每個 Amazon EBS 磁碟區都會在其可用區域內自動複寫，以保護您不受元件故障影響，提供高可用性和耐用性。Amazon EBS 磁碟區提供執行工作負載所需的一致且低延遲效能。使用 AmazonEBS，您可以在幾分鐘內擴展或縮減使用量，同時只為佈建的內容支付低廉的價格。

[進一步了解 Amazon EBS。](#)

## 監控和警示

### Amazon CloudWatch

Amazon CloudWatch 是AWS雲端資源和您執行的應用程式的監控服務AWS。您可以用 CloudWatch 來收集和追蹤指標、收集和監控記錄檔、設定警示，以及自動回應AWS資源中的變更。CloudWatch 可以監控 Amazon EC2 執行個體、Amazon Dynamo RDS DB 表和 Amazon 資料庫執行個體等AWS資源，以及應用程式和服務產生的自訂指標，以及應用程式產生的任何日誌

檔。您可以用 CloudWatch 來取得整個系統的資源使用率、應用程式效能和作業狀態的可見度。您可以使用這些分析結果即時做出反應，並保持應用程式順暢運作。

[進一步了解 Amazon CloudWatch。](#)

## 應用程式部署

### AWS Elastic Beanstalk

AWS Elastic Beanstalk 是一種 easy-to-use 用於部署和擴展使用 Java 開發的 Web 應用程序和服務的服務，. NET, Node.js, PHP, Python, 紅寶石, 圍棋, 和碼頭工人熟悉的服務器，如阿帕奇, Nginx 的, 乘客, 和 IIS

您只要上傳程式碼，Elastic Beanstalk 即會自動處理部署作業；無論是容量佈建、負載平衡、自動調整規模或應用程式運作狀態監控，該服務都能滿足所需。同時，您可以完全控制為應用程式提供支援的 AWS 資源，並且可以隨時存取基礎資源。

[進一步了解 Elastic Beanstalk。](#)

## 應用程式容器

### Amazon 彈性容器服務 ( Amazon ECS )

Amazon ECS 是可高度擴展、高效能的容器管理服務，可支援 Docker 容器，並可讓您在 Amazon 執行個體的受管叢集上輕鬆 EC2 執行應用程式。ECS Amazon 無需安裝、操作和擴展自己的叢集管理基礎設施。透過簡單的 API 呼叫，您可以啟動和停止啟用 Docker 的應用程式、查詢叢集的完整狀態，以及存取許多熟悉的功能，例如安全群組、Elastic Load Balancing、Amazon EBS 磁碟區和 IAM 角色。您可以使用 Amazon ECS 根據資源需求和可用性需求，在叢集中排程容器的放置。而且，您還能整合自己的排程器或第三方排程器，以滿足商業或應用程式的特定需求。

[進一步了解 Amazon ECS。](#)

## 安全性和使用者登入功能

### AWS Identity and Access Management (IAM)

IAM 可讓您安全地控制使用者對 AWS 服務和資源的存取。使用時 IAM，您可以建立和管理使用 AWS 者和群組，並使用權限來允許和拒絕他們對 AWS 資源的存取。

[進一步了解 IAM。](#)

## Amazon Cognito 使用者集區

Amazon Cognito 可讓您輕鬆地將使用者註冊與登入功能新增至行動裝置和 Web 應用程式。透過 Amazon Cognito，您還可以選擇透過社交身分供應商 (例如 Facebook、Twitter 或 Amazon)、使用 SAML 身分解決方案或使用您自己的身分系統來驗證使用者。此外，Amazon Cognito 還可讓您在使用者的本機裝置上儲存資料。如此一來，即使裝置處於離線狀態，應用程式仍然可以運作。接著，您可以在使用者的多台裝置間同步資料，無論他們使用哪一台裝置，皆能維持一致的應用程式體驗。

透過 Amazon Cognito，您能夠專心建立絕佳的應用程式體驗，不用擔心如何建置、保護和擴展解決方案，即可有效處理使用者管理、身分驗證與跨裝置同步作業。

[進一步了解 Amazon Cognito。](#)

## 來源控制和應用程式生命週期管理

### AWS CodeCommit

AWS CodeCommit 是一項完全受管的原始檔控制服務，可讓公司輕鬆託管安全且可高度擴充的私有 Git 儲存庫。AWS CodeCommit 無需操作您自己的原始檔控制系統，也不必擔心擴展其基礎架構。您可以使用 AWS CodeCommit 安全地存儲從源代碼到二進製文件的任何內容，並且可以與現有的 Git 工具無縫配合使用。

[進一步了解 AWS CodeCommit。](#)

## 佇列和簡訊

### Amazon SQS

Amazon 簡單佇列服務 (AmazonSQS) 是一種快速、可靠、可擴展的全受管訊息佇列服務。Amazon SQS 讓分離雲端應用程式的元件變得簡單且符合成本效益。您可以使用 Amazon SQS 傳輸任何數量的數據，而不會丟失消息或要求其他服務始終可用。Amazon SQS 包括具有高輸送量和 at-least-once 處理能力的標準 FIFO 佇列，以及提供 FIFO (先進先出) 交付和僅處理一次的佇列。

使用 AmazonSQS，您可以減輕操作和擴展高可用性簡訊叢集的管理負擔，同時只針對您使用的項目支付低廉的價格。

[進一步了解 Amazon SQS。](#)

## Amazon SNS

Amazon 簡單通知服務 (AmazonSNS) 是一種快速、靈活、全受管的推播通知服務，可讓您傳送個別訊息或將訊息散播給大量收件人。Amazon SNS 讓傳送推播通知給行動裝置使用者或電子郵件收件者，甚至可以將訊息傳送到其他分散式服務，既簡單又符合成本效益。

使用 AmazonSNS，您可以將通知發送到蘋果推送通知服務 ( APNS )，谷歌雲消息傳遞 ( GCM )，消防操作系統和 Windows 設備，以及通過百度雲推送到中國的 Android 設備。您可以使用 Amazon SNS 向全球的移動設備用戶發送SMS消息。

除了這些端點之外，Amazon 還SNS可以將訊息傳遞到 Amazon SQS、AWS Lambda 功能或任何 HTTP端點。

[進一步了解 Amazon SNS。](#)

## Amazon SES

Amazon 簡單電子郵件服務 (AmazonSES) 是一種經濟高效的電子郵件服務，建立在 Amazon.com 開發的可靠且可擴展的基礎設施上，以服務自己的客戶群。使用 AmazonSES，您無需最低承諾即可傳送和接收電子郵件。該服務會依用量計費，您僅需按實際用量支付費用。

[進一步了解 Amazon SES。](#)

## 工作流程

### Amazon 簡單工作流服務 ( AmazonSWF )

Amazon SWF 可協助開發人員建置、執行和擴展具有 parallel 或連續步驟的背景任務。您可以將 Amazon SWF 視為雲端中的全受管狀態追蹤器和任務協調員。

如果應用程式的步驟需要 500 毫秒以上才能完成任務，您便需要追蹤處理狀態，並在任務失敗時復原或重試。Amazon SWF 可以幫助你。

[進一步了解 Amazon SWF。](#)

## 串流應用程式

### Amazon AppStream

Amazon AppStream 允許您將 Windows 應用程序交付到任何設備。

Amazon AppStream 可讓您從雲端串流現有的 Windows 應用程式，在更多裝置上觸及更多使用者，而無需修改程式碼。使用 Amazon AppStream，您的應用程式會在 AWS 基礎設施上部署和轉譯，並將輸出串流至大眾市場的裝置，例如個人電腦、平板電腦和行動電話。系統會在雲端中執行應用程式，因此無論客戶使用的裝置為何，您都可以擴展該應用程式，以處理大量的運算和儲存需求。Amazon AppStream 提供了一個用 SDK 於從雲流式傳輸您的應用程序。您可以將自己的自訂用戶端、訂閱、身分識別和儲存解決方案與 Amazon 整合，AppStream 以建立符合業務需求的自訂串流解決方案。

[進一步了解 Amazon AppStream。](#)

## 使用建立 Lightsail 資源 AWS CloudFormation

Amazon Lightsail 整合了這項服務 AWS CloudFormation，可協助您建立資源模型和設定 AWS 資源，以減少建立和管理資源和基礎設施的時間。您可以建立一個範本，說明所需的所有 AWS 資源 (例如執行個體和磁碟)，並為您 AWS CloudFormation 佈建和設定這些資源。

使用時 AWS CloudFormation，您可以重複使用範本，以一致且重複地設定 Lightsail 資源。描述您的資源一次，然後在多個區域中一遍又一遍地佈建相同 AWS 帳戶的資源。

## Lightsail 和 AWS CloudFormation 模板

若要佈建和設定 Lightsail 及相關服務的資源，您必須瞭解[AWS CloudFormation 範本](#)。範本是以 JSON 或 YAML 格式化的文本檔案。這些範本說明您要在 AWS CloudFormation 堆疊中佈建的資源。如果您不熟悉 JSON 或 YAML，可以使用 AWS CloudFormation 設計工具來協助您開始 AWS CloudFormation 使用範本。如需詳細資訊，請參閱[什麼是 AWS CloudFormation 設計師？](#) 在《AWS CloudFormation 使用者指南》中。

Lightsail 支援在 AWS AWS CloudFormation 中建立執行個體和磁碟。如需詳細資訊，請參閱 AWS CloudFormation 使用者指南中的 [Lightsail 資源類型參考](#) 資料。

## 進一步了解 AWS CloudFormation

若要進一步了解 AWS CloudFormation，請參閱下列資源：

- [AWS CloudFormation](#)
- [AWS CloudFormation 使用者指南](#)
- [AWS CloudFormation API 參考](#)

- [AWS CloudFormation 指令行介面使用者指南](#)

## 探索應用程式部署的 Lightsail 資源

下列清單包含未在 Lightsail 使用者指南中發佈的其他 Amazon Lightsail 資訊的連結。

### 內容

- [部落格](#)
- [教學課程](#)
- [影片](#)

### 部落格

- [使用資料多監控 Amazon Lightsail 執行個體的運作狀態](#)

2022 年 3 月 30 日 — 探索使用 Datadog 監控 Lightsail 工作負載如何協助您確保應用程式效能並控制成本。

- [如何設置銀河以進行有關 AWS 使用 Amazon Lightsail 的研究](#)

2022 年 1 月 13 日 — 在 Lightsail 上部署科學工作流程、資料整合和數位保存平台 Galaxy。

- [在瀏覽器中輸入 URL 會發生什麼情況](#)

2021 年 8 月 26 日 – 在瀏覽器中輸入 URL 並按下 Enter 鍵的話，會發生什麼情況？

- [監控 Amazon Lightsail 執行個體中的記憶體使用](#)

2021 年 6 月 14 日 — 將 Lightsail 執行個體設定為將記憶體使用量傳送至 Amazon 以 CloudWatch 進行監控、警示和通知。

- [使用 Amazon Lightsail 順暢無阻地託管容器化 ASP.NET 網路應用程式](#)

2021 年 6 月 10 日-如何使用容器化 ASP.NET 網頁應用程式，該應用程式會連線到 PostgreSQL 資料庫並將其部署到 Lightsail。

- [使用 Amazon Lightsail 集裝箱啟動 WordPress 網站](#)

2021 年 4 月 5 日 — 使用 Lightsail 容器和 Lightsail 資料庫啟動 WordPress 網站。

- [Lightsail 容器：在雲端中執行容器的簡單方法](#)

2020 年 11 月 13 日 — 在 Lightsail 上部署以容器為基礎的工作負載。

- [將網路服務從 Amazon Lightsail 遷移到 Amazon EC2](#)

2020 年 10 月 16 日 — 在 Amazon EC2 中設定生產環境，並將網路服務從 Lightsail 遷移到該環境中。

- [建置灰日誌伺服器以在 Amazon Lightsail 執行個體上執行](#)

2020 年 7 月 28 日 — 如何在 Lightsail 上建置灰日誌伺服器。

- [利用 Lightsail 內容傳遞網路改善網站效能](#)

2020 年 7 月 23 日 — 設定 Lightsail 發行版本，以便與標準網頁伺服器搭配使用 WordPress。

- [主動監控 Amazon Lightsail 執行個體的系統效能](#)

2020 年 6 月 4 日 – 設定容量劇增提醒，以便在系統效能問題影響使用者之前，率先預防問題發生。

- [利用全新的 Lightsail 防火牆功能強化網站安全](#)

2020 年 5 月 7 日 – 使用 SSH 限制遠端存取，僅允許單一來源 IP 地址的存取活動。

- [使用 CodeDeploy 和部署 CodePipeline 應用程式到 Amazon Lightsail](#)

2020 年 4 月 23 日 — 將 Lightsail 設定為在每次將變更推送 CodePipeline 至時使用 CodeDeploy 並自動部署 (或更新) 應用程式。GitHub

- [在 Amazon Lightsail 上使用負載平衡器](#)

2020 年 4 月 21 日 — 如何使用亞馬遜 Lightsail 負載平衡器對簡單的 Node.js 網路應用程式進行負載平衡。

- [用幽靈在 Amazon Lightsail 上建立照片日記](#)

2020 年 3 月 23 日 — 使用 Lightsail 上的幽靈開始照片日記。

- [Amazon Lightsail 數據庫提示和技巧](#)

2020 年 3 月 23 日 – 使用 Amazon Relational Database Service (Amazon RDS) 中找到的進階功能。

- [設定及使用監控和通知功能](#)

2020 年 2 月 27 日 – 建立通知聯絡人、建立新警示，並透過資源監控功能測試通知機制。

- [在 Amazon Lightsail 上部署高可用性的 WordPress 網站，第 1 部分：使用以下方式實施高可用性的 Lightsail 資料庫 WordPress](#)

2019 年 10 月 22 日 — 在 Lightsail 上建立一個高可用性的 WordPress 網站，第 1 部分。

- [在 Amazon Lightsail 上部署高可用性 WordPress 網站，第 2 部分：使用 Amazon S3 搭配安全交付媒體檔 WordPress 案](#)

2019 年 10 月 31 日 — 在 Lightsail 上建立高可用性 WordPress 網站，第 2 部分。

- [在 Amazon Lightsail 上部署高可用性 WordPress 網站，第 3 部分：使用 Amazon 提高安全性和性能 CloudFront](#)

2019 年 11 月 7 日 — 在 Lightsail 上建立高可用性 WordPress 網站，第 3 部分。

- [在 Amazon Lightsail 上部署高可用性的 WordPress 網站，第 4 部分：使用 Lightsail 負載平衡器提高效率 and 可擴展性](#)

2019 年 11 月 14 日 — 在 Lightsail 上建立一個高可用性的 WordPress 網站，第 4 部分。

- [使用 Amazon Lightsail 構建一個袖珍平台作為服務](#)

2019 年 10 月 8 日 — 在 Lightsail 上組裝一個袖珍平台。

- [使用 Amazon Lightsail 部署以 NGINX 為基礎的 HTTP/HTTPS 負載平衡器](#)

2019 年 7 月 8 日 — 在 Lightsail 執行個體內部設定以 NGINX 為基礎的負載平衡器。

- [新的 AWS 雲端？ Amazon Lightsail 可以提供幫助](#)

2019 年 3 月 27 日 — 開始使用 Amazon Lightsail。

- [新增 — 適用於 Amazon Lightsail 的受管資料庫](#)

2018 年 10 月 16 日 – 只需按幾下即可建立受管資料庫。

- [Amazon Lightsail 更新：更多執行個體大小和降低價格](#)

2018 年 8 月 23 日 — Lightsail 執行個體概觀。

- [Amazon Lightsail: 的力量 AWS, 一個 VPS 的簡單性](#)

2016 年 11 月 30 日 — Lightsail 啟動公告。

## 教學課程

前 5 名實作教學課程：

1. [建立負載平衡 WordPress 網站](#)

2021 年 9 月 8 日 — 透過 Lightsail 啟動高可用性 WordPress 網站。

## 2. [使用 Amazon Lightsail WordPress 網站遷移和管理](#)

2021 年 2 月 22 日 — 使用海馬軟體將您的 WordPress 網站複製到 Lightsail 上。

## 3. [啟動 Linux 虛擬機器](#)

2020 年 9 月 11 日 — 透過 Lightsail 啟動、設定及連線至 Linux 執行個體。

## 4. [啟動 Windows 虛擬機器](#)

2020 年 9 月 11 日 — 使用 Lightsail 啟動、設定及連線至 Windows 執行個體。

## 5. [在 Amazon Lightsail 上啟動一個交友面板和 WHM 實例](#)

2020 年 7 月 27 日 — 在您的 cPanel 和 WHM 執行個體在 Lightsail 上啟動並執行之後，本教學課程將逐步介紹幾個步驟。

- [如何在 Amazon Lightsail 上設置和配置 Magento](#)

2021 年 8 月 11 日 – 架設及執行電子商務網站。

- [如何將您的 WordPress 網站連接到物件儲存貯體](#)

2021 年 7 月 14 日 — 在 Lightsail 上設定您的網 WordPress 站，並將網站連線至 Lightsail 儲存貯體。

- [建立儲存物件的儲存貯體](#)

2021 年 7 月 14 日 — 在 Amazon Lightsail 中創建一個對象存儲桶。

- [將 WordPress 網站連接到 Amazon Lightsail 存儲桶並進行分發](#)

2021 年 7 月 14 日 — 將您的 Lightsail 儲存貯體設定為 Lightsail 內容交付網路 (CDN) 發佈的來源。

- [如何設定 Plesk](#)

2021 年 4 月 22 日 — 在 Lightsail 上啟動並運行一個普萊斯克託管堆棧。

- [如何設定 Prestashop 電子商務網站](#)

2021 年 4 月 1 日 — 使用 Bitnami PrestaShop 認證藍圖啟動和設定 Lightsail 執行個體。

- [如何將 Amazon EFS 與亞馬 Amazon Lightsail 一起使用](#)

2021 年 3 月 15 日 — 使用 VPC 擬私人雲端對等互連，從 Lightsail 執行個體建立並連接到 Amazon EFS 檔案系統。

- [如何設定 Nginx 反向代理](#)

2021 年 2 月 10 日 — 使用 Lightsail 容器設置 Nginx 反向代理。

- [如何為 Flask 應用程式提供服務](#)

2021 年 2 月 3 日 — 瞭解如何使用 Lightsail 容器為燒瓶應用程式提供服務。

- [使用 Amazon Lightsail 建立、推送和部署容器映像](#)

2020 年 11 月 11 日 – 使用 Dockerfile 在本機電腦上建立容器映像。

- [建置 Drupal 網站](#)

2020 年 9 月 11 日 — 在 Lightsail 上部署和託管可供生產使用的 Drupal 網站。

- [建置 LAMP 堆疊 Web 應用程式](#)

2020 年 9 月 9 日 — 在 Lightsail 上啟動並執行高可用性 PHP 網路應用程式。

- [設定您的 WordPress 執行個體以搭配您的發佈使用](#)

2020 年 7 月 16 日 — 將您的 WordPress 執行個體設定為使用您的 Lightsail 發行版本。

- [啟動一個 WordPress 網站](#)

2020 年 3 月 23 日 — 在 Lightsail 虛擬機器上 WordPress 安裝並啟動網站並運行。

- [託管 .NET 應用程式](#)

2020 年 3 月 20 日 — 使用 Lightsail 建置和部署 .NET 應用程式。

- [將您在 Amazon Route 53 上的域名映射到您的 Lightsail 資源](#)

將您網域的流量 (例如 .com) 路由至您的 Lightsail 資源。

## 影片

- [Amazon Lightsail 教程：部署 Django 應用程序](#)

2021 年 7 月 14 日 – 您會在此教學課程中建立 Django 應用程式。

- [Amazon Lightsail 教程：部署燒瓶應用程序](#)

2021 年 7 月 14 日 – 您會在此教學課程中建立 Flask 應用程式。

- [Amazon Lightsail 教程：部署 NGINX 反向代理](#)

2021 年 7 月 14 日 — 建立燒瓶應用程式、建置 Docker 容器、在 Lightsail 上建立容器服務，然後部署應用程式。

- [Amazon Lightsail 教程：部署電子商務網站](#)

2021 年 7 月 14 日 — 使用 Bitnami PrestaShop 認證藍圖啟動 Lightsail 執行個體，並進行設定。

- [在 Amazon Lightsail 上部署容器化應用程式](#)

2020 年 12 月 29 日 — 瞭解如何在 Lightsail 中部署容器化應用程式。

- [Amazon Lightsail 教程：建立一個 Drupal 網站](#)

2020 年 8 月 31 日 – 啟動和設定 Drupal 執行個體。

- [Amazon Lightsail 教程：部署 LAMP 堆疊應用程式](#)

2020 年 8 月 31 日 — 將燈具 (Linux 阿帕奇 MySQL) 堆疊應用程式部署到單一 Lightsail 執行個體。

- [Amazon Lightsail 教程：啟動一個 Linux 實例](#)

2020 年 8 月 31 日 – 了解如何啟動 Linux 執行個體。

- [Amazon Lightsail 教程：啟動視窗執行個體](#)

2020 年 8 月 31 日 – 了解如何啟動 Windows 執行個體。

- [Amazon Lightsail 教程：運行自己的我的世界服務器](#)

2020 年 8 月 31 日 – 了解如何設定專用的 Minecraft 伺服器。

- [Amazon Lightsail 教學簡介](#)

2020 年 8 月 31 日 — 立即使用 Lightsail 開始您的雲端旅程。

- [Amazon Lightsail：開始使用的最簡單方法 AWS](#)

2020 年 3 月 20 日 — Lightsail 是開始使用的最簡單方法。AWS 它能提供虛擬伺服器、儲存空間、資料庫和聯網服務，以及具備成本效益的每月計畫。

- [在 Amazon Lightsail 中設定 Plesk 執行個體](#)

2019 年 3 月 27 日 — 了解如何在 Lightsail 中設定 Plesk 執行個體。

- [在 Amazon Lightsail 中配置 WordPress 多站點](#)

2019 年 1 月 15 日 — 了解如何在 Lightsail 中設定 WordPress 多網站執行個體。

- [管理 Lightsail](#)

2018 年 10 月 9 日 — 快速瀏覽一下 Lightsail 的主要功能。

- [在 Amazon Lightsail 上部署平均堆疊應用程式](#)

2018 年 6 月 5 日 — 使用 Lightsail 的平均藍圖將自訂應用程式部署到雲端。

- [在 Amazon Light WordPress sail 上部署執行個體](#)

2018 年 6 月 5 日 — 在 Lightsail 上部署 WordPress 執行個體。

## 檢視 Lightsail 的帳單和用量

Amazon Lightsail 的計費是透過 Amazon Web Services (AWS) 計費處理。若要檢視 Lightsail 帳單，請移至「[AWS Billing and Cost Management 儀表板](#)」，或選擇 Lightsail 主控台頂端導覽列上的「帳單」。如需有關定價的詳細資訊，請參閱 [Lightsail 定價頁面](#)。

### 檢視您的詳細帳單

若要檢視每月 Lightsail 帳單的詳細明細，請執行下列步驟：

1. 登入 [AWS Billing and Cost Management 儀表板](#)。

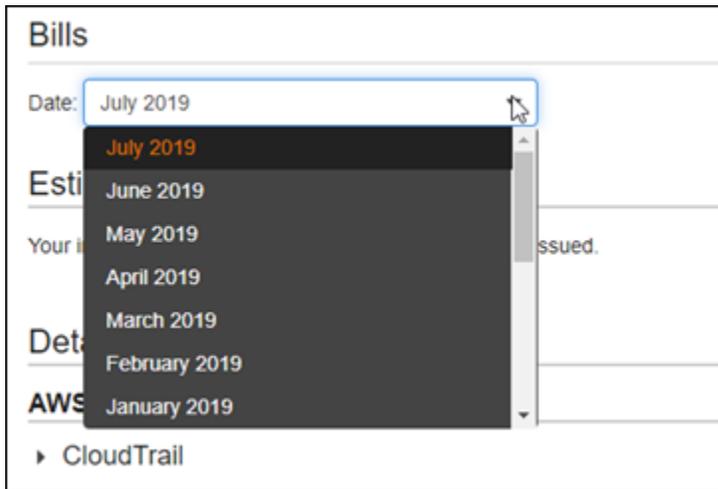
帳單控制面板首頁會顯示帳單的高階 month-to-date 明細。

2. 在儀表板首頁上選擇 Bill Details (帳單詳細資訊)，或選擇左側導覽窗格中的 Bills (帳單)，以檢視每月帳單的詳細版本。

The screenshot shows the AWS Billing & Cost Management Dashboard. On the left, the 'Bills' link is circled in red. In the main content area, the 'Month-to-Date Spend by Service' section has a 'Bill Details' button circled in red. The dashboard displays a 'Spend Summary' of \$198.33 for July 2019. Below this, a donut chart shows the proportion of costs spent for each service. The data is as follows:

Service	Amount
Lightsail	\$196.53
EC2	\$0.91
Route53	\$0.50
GuardDuty	\$0.26

3. 選擇 Date (日期) 下拉式選單，選取當月以外的月份。



- 在「帳單」頁面上向下捲動，然後展開 Lightsail 明細項目，以檢視每個區域的詳細用量。

▼ Lightsail		\$192.69
▶ US East (N. Virginia)		\$0.00
▼ US West (Oregon)		\$192.69
Amazon Lightsail Bundle:0.5GB		\$6.22
\$0.0047 / Hour of 0.5GB bundle Instance	1,323.603 Hrs	\$6.22
Amazon Lightsail Bundle:1GB		\$0.16
\$0.00672/ Hour of 1GB bundle Instance	23.073 Hrs	\$0.16
Amazon Lightsail Bundle:4GB		\$19.35
\$0.0269 / Hour of 4GB bundle Instance	720 Hrs	\$19.35
Amazon Lightsail Bundle:8GB		\$116.12
\$0.0538 / Hour of 8GB bundle Instance	2,160 Hrs	\$116.12

## 帳單用量類型

下列清單說明 Lightsail 帳單和用量報表中顯示的用量類型。這些用量類型有助於識別 Lightsail 資源的每月帳單上的費用。

### Note

如需下列指定區域代碼的用量類型，請參閱本指南的[帳單中的區域代碼](#)一節，來識別對應的 AWS 區域。

- Amazon Lightsail 套件：規模 B：使用的 Linux 或 Unix 執行個體計畫 (以小時為單位)。Size (大小) 定義所使用執行個體計畫的記憶體規格。例如，如果指定了 4GB 的記憶體，則會顯示 USD 每月 24 美元的 Linux 或 Unix 執行個體計畫的計費時數。

- Amazon Lightsail 套件：大小 B (視窗)：使用的 Windows 執行個體計劃 (以小時為單位)。Size (大小) 定義所使用執行個體計畫的記憶體規格。例如，如果指定 4GB 記憶體，則會顯示 Windows 執行個體計劃 USD 每月 44 美元的計費小時數。
- Amazon Lightsail：大小 B RelationalDatabase：使用的標準數據庫計劃 (以小時為單位)。Size (大小) 定義所使用資料庫計畫的記憶體規格。例如，如果指定 4GB 記憶體，則會顯示 USD 每月 \$60 美元標準資料庫計畫的計費小時數。
- Amazon LightSail：SizeGB RelationalDatabase (高可用性)：使用的高可用性資料庫計劃 (以小時為單位)。Size (大小) 定義所使用資料庫計畫的記憶體規格。例如，如果指定 4GB 記憶體，則會顯示 USD 每月 \$120 美元高可用性資料庫計畫的計費小時數。
- Amazon Lightsail 區域-DiskUsage：使用的區塊儲存磁碟數量 (每月 GB)。
- Amazon Lightsail DNS-查詢：該月查DNS詢的數量 (計數)。
- Amazon Lightsail Load Balancer：使用的負載平衡器數量 (以小時為單位)。
- Amazon Lightsail 區域SnapshotUsage：儲存的快照資料量 (每月 GB)。
- Amazon Lightsail 區域 UnusedStatic IP：未連接的靜態數量IPs (以小時為單位)。
- Amazon Lightsail 中TotalDataXfer位元組區域：以 GB 為單位傳輸的資料總量。
- Amazon Lightsail 區域 TotalDataXfer-輸出位元組：傳出的資料總量 (GB)。
- Amazon Lightsail 區域 DataXfer-輸出超量位元組：傳出至網際網路或公IPs有的資料超過所使用執行個體或資料庫計劃限額的資料量 (以 GB 為單位)。

## 帳單中的區域代碼

Lightsail 帳單和使用情況報告使用代碼和縮寫。例如，針對用量類型，區域會取代為下列其中一個縮寫：

- APN1: 亞太區域 (東京) (ap-northeast-1)
- APN2: 亞太區域 (首爾) (ap-northeast-2)
- APS1: 亞太區域 (新加坡) (ap-southeast-1)
- APS2: 亞太區域 (雪梨) (ap-southeast-2)
- APS3: 亞太區域 (孟買) (ap-south-1)
- CAN1: 加拿大 (中部) (ca-central-1)
- EU：歐洲 (愛爾蘭) (eu-west-1)
- EUC1: 歐洲 (法蘭克福) (eu-central-1)
- EUW2: 歐洲 (倫敦) (eu-west-2)

- EUW3: 歐洲 (巴黎) (eu-west-3)
- EUN1: 歐洲 (斯德哥爾摩) (eu-north-1)
- USE1: 美國東部 (維吉尼亞北部) (us-east-1)
- USE2 : 美國東部 (俄亥俄州) (us-east-2)
- USW2: 美國西部 (奧勒岡) (us-west-2)

# 取得常見問題的 Lightsail

本節涵蓋與 Lightsail 相關的常見問題和解答，分為以下類別。

## 主題

- [瞭解 Lightsail 及其全球可用性](#)
- [帳單和帳戶管理](#)
- [區塊儲存 \(磁碟\)](#)
- [憑證](#)
- [聯繫人和監控通知](#)
- [容器服務](#)
- [內容交付網路分發](#)
- [資料庫](#)
- [網域](#)
- [將 Lightsail 資源匯出至 Amazon 彈性運算雲端 \(AmazonEC2\)](#)
- [執行個體](#)
- [負載平衡器](#)
- [手動和自動快照](#)
- [資源健康指標和警示](#)
- [聯網](#)
- [物件儲存和儲存貯體](#)
- [Lightsail 中的標籤](#)

請按照每個類別中提供的連結，尋找有關 Lightsail 的這些常見問題的詳細解答。

## 瞭解 Lightsail 及其全球可用性

### 什麼是 Amazon Lightsail？

AWS 對於需要在雲端中建置和託管網站和 Web 應用程式的開發人員、小型企業、學生和其他使用者而言，Amazon Lightsail 是最簡單的入門方式。Lightsail 為開發人員提供運算、儲存和網路容量。Lightsail 包含快速啟動專案所需的一切，包括虛擬機器、容器、資料庫CDN、負載平衡器、DNS 管理等，而且每月價格低廉且可預測。

## 我可以使用 Lightsail 做什麼？

您可以建立預先設定的虛擬專用伺服器 (執行個體)，以便輕鬆部署和管理應用程式，或建立由 Lightsail 管理基礎架構和作業系統安全性與健康狀態的資料庫。Lightsail 最適合需要數十個執行個體或更少執行個體的專案，以及偏好簡單管理介面的開發人員。Lightsail 的常見使用案例包括執行網站、Web 應用程式、商業軟體、部落格、電子商務網站等。隨著專案的成長，您可以將負載平衡器和連接區塊儲存搭配執行個體使用，以增加備援和正常執行時間，並存取數十種其他 AWS 服務以新增功能。

## Lightsail 是否提供 API？

是。您在 Lightsail 主控台中所做的一切都是由公開提供 API 的支援。瞭解如何安裝 Lightsail CLI 用 [API](#)。

## 我要如何註冊成為 Lightsail？

若要開始使用 Lightsail，請選擇「[開始使用](#)」並登入。您可以使用 Amazon Web Services 帳戶存取 Lightsail；如果您還沒有帳戶，系統會提示您建立一個帳戶。

## Lightsail AWS 區域 有哪些可用？

Lightsail 提供以下產品：AWS 區域

### AWS 區域

- 美國東部 (俄亥俄) (us-east-2)
- 美國東部 (維吉尼亞北部) (us-east-1)
- 美國西部 (奧勒岡) (us-west-2)
- 亞太區域 (孟買) (ap-south-1)
- 亞太區域 (首爾) (ap-northeast-2)
- 亞太區域 (新加坡) (ap-southeast-1)
- 亞太區域 (雪梨) (ap-southeast-2)
- 亞太區域 (東京) (ap-northeast-1)
- 加拿大 (中部) (ca-central-1)
- 歐洲 (法蘭克福) (eu-central-1)
- 歐洲 (愛爾蘭) (eu-west-1)
- 歐洲 (倫敦) (eu-west-2)

- 歐洲 (巴黎) (eu-west-3)
- 歐洲 (斯德哥爾摩) (eu-north-1)

如需詳細資訊，請參閱 [Lightsail 中的AWS 區域 和可用區域](#)。

## 什麼是可用區域？

可用區域是資料中心的集合，這些資料中心在不同的獨立實體基礎設施上執行，而且具備高度可靠的設計。可用區域之間不會共用常見的故障點，如發電機和冷卻設備等。此外，可用區域各自分開，即使火災、風災或水災等極度罕見災難也只會影響其中一個可用區域。

## 什麼是 Lightsail 服務配額？

如需最新的 Lightsail 服務配額 (包括可增加哪些[配額](#))，請參閱 [AWS 一般參考](#) 若要增加服務配額，請使用 [AWS Support](#)。

## 如何獲得更多協助？

Lightsail 中的內容相關說明面板提供有關您在主控台中動作的即時實用提示。若要開啟說明面板，請選擇 Lightsail 主控台右上角的說明面板圖示 。您也可以從 Lightsail 主控台存取 [入門指南](#)、[概觀](#) 和 [操作](#) 主題的資料庫。如果您想要使用 Lightsail API，或者 AWS CLI，Lightsail 有所有支援的程式設計語言的完整 API 參考資料。您也可以使 Lightsail 援資源。

如果帳戶或帳單有問題，請線上聯絡 [AWS Support](#)。您可以使用您的 Lightsail 帳戶獲得全年無休的免費訪問權限。

如需有關如何使用 Lightsail 的一般問題，請搜尋 Lightsail 文件和 [支援論壇](#)。

此外，還 AWS Support 提供一系列付費計劃以滿足您的個人需求。

## 帳單和帳戶管理

### Lightsail 計劃的費用是多少？

Lightsail 方案以隨需小時費率計費，因此您只需按使用量付費。對於您使用的每個 Lightsail 計劃，我們會按固定小時收費，最高為每月計劃的最高費用。最便宜的 Lightsail 計劃的起價為每 USD 小時 0.0067 美元 (每月 5 美元)。USD 包含視窗伺服器授權的開始價格為每 USD 小時 0.0127 美元 (每月 9.50 美元)。USD

## 何時需要支付計劃的費用？

Lightsail 執行個體和受管資料庫會產生費用，直到刪除為止。如果您在月底之前刪除 Lightsail 執行個體或受管理的資料庫，我們只會根據您該月使用 Lightsail 執行個體或受管理資料庫的總時數，向您收取按比例分配的費用。例如，如果您在一個月內使用最便宜的 Lightsail 執行個體計劃 100 小時，則需支付 46 美分 (100\*0.0046) 的費用。

## 我可以免費試用 Lightsail 執行個體嗎？

是。無論您是現有客戶還是新 AWS 客戶，您都可以免費獲得 750 美元 USD Lightsail 計劃的免費使用時間。您也可以使用 9.50 美元 USD 的視窗方案免費試用包含視窗伺服器授權的 Lightsail 方案。

750 小時的用量可用於無限個執行個體。例如，您可以執行一個 Lightsail 執行個體一整個月，或執行 10 個 Lightsail 執行個體，持續 75 小時。免費試用優惠僅適用於註冊使用 Lightsail 起的第一個日曆月內的使用量。如果您的帳戶已連結至組織 (位於「組 Organ AWS izations」下)，則組織內只有一個帳戶可以從 AWS 免費方案優惠中受益。

### Note

作為 AWS 免費方案的一部分，您可以在特定執行個體套裝軟體上免費開始使用 Amazon Lightsail。如需詳細資訊，請參閱 [Amazon Lightsail 定價頁面](#) 上的 AWS 免費方案。

## 免費試用版何時開始？

Lightsail 免費試用權益會在第一個免費試用符合資格的資源推出時開始。

執行個體和資料庫的延長 90 天免費試用僅適用於特定方案 (套件)。此優惠適用於 2021 年 7 月 8 日或之後開始使用 Lightsail 的新 AWS 帳戶或現有帳戶。如需詳細資訊，請參閱 [Lightsail 定價頁面](#)。

## Lightsail 受管資料庫的成本為何？

Lightsail 受管理的資料庫有 4 種方案大小，對於具有 40 GB SSD 儲存空間和 100 GB 資料傳輸 USD 額度的 1GB 資料 RAM 庫執行個體，起始價格為每月 15 美元。高可用性計劃的費用是標準計劃價格的兩倍，因為它們在另一個可用區域中執行額外的資料庫執行個體和儲存磁碟，以提供冗餘。

## 我可以免費試用 Lightsail 受管理的資料庫嗎？

是! 新客戶可免費獲得 1 個月 15 美元的 USD Lightsail 計劃。

## 區塊儲存的 Lightsail 本是多少？

Lightsail 區塊儲存USD每月每 GB 的費用為 0.10 美元。

## Lightsail 負載平衡器的成本是多少？

Lightsail 負載平衡器每月花費 18 美元USD。

## 憑證管理費用是多少？

只要使用 Lightsail 負載平衡器，即可免費使用 Lightsail 憑證和憑證管理功能。

## 什麼是 Lightsail 靜態IPv4地址的成本？

靜態 IP 位址連接至 Lightsail 執行個體時，不會產生與其相關的費用。靜態IPs無法附加至IPv6僅執行個體。IPv4地址是一種稀缺的資源，Lightsail 致力於幫助有效地使用它們，因此我們針對靜態IPs未附加到執行個體超過 1 小時的時間收取 0.005 美元USD/小時的小時費用。

## 資料傳輸的費用是多少？

您的執行個體、資料庫和內容傳遞網路 (CDN) 發佈計劃包含資料傳輸額度。

對於 Lightsail 執行個體，執行個體的資料傳入和傳出資料都會計入您的資料傳輸額度。如果您超出資料傳輸額度，則只需支付使用執行個體公有 IP 位址OUT從 Lightsail 執行個體傳輸至網際網路或 AWS 資源的超額資料傳輸費用。您不需要支付多餘的資料傳輸至 Lightsail 執行個體的費用。資料傳入至 Lightsail 執行個體，以及在使用執行個體私有 IP 位址時OUT從 Lightsail 執行個體傳輸資料，都不會超出您的資料傳輸額度。

對於 Lightsail 受管理的資料庫，只有資料傳輸OUT才會計入您的額度。如果您超出資料傳輸額度，則只會針對OUT從 Lightsail 受管理的資料庫傳輸至網際網路的資料收費。

對於 Lightsail 發CDN佈，從您的發佈中傳出的所有資料都會計入您的額度。超過分發資料傳輸額度後，所有從分發中傳出的資料傳輸將會產生費用。

## 資料傳輸額度如何用於執行個體？

每個 Lightsail 執行個體計劃都包含資料傳輸額度。執行個體OUT的資料傳輸 IN 和資料傳輸都會計入您的資料傳輸額度。如果您超出資料傳輸額度，則只需支付OUT從 Lightsail 執行個體傳輸到網際網

路或使用執行個體公有 IP 位址傳輸至 AWS 資源的超額資料費用。您不需要支付多餘的資料傳輸至 Lightsail 執行個體的費用 (請參閱範例 1)。您的資料傳輸額度每個月都會重設，而且執行個體可以在當月需要時隨時使用。針對區域中相同套裝軟體 (bundleId) 的執行個體彙總資料傳輸額度 (請參閱範例 2 和範例 3)。也會針對相同大小的 IPv4 和 IPv6 執行個體彙總資料傳輸額度 (請參閱範例 4)。刪除執行個體和建立新執行個體並不會重設資料傳輸額度 (請參閱範例 5)。

如需 Lightsail 套裝軟體的詳細資訊，請參閱 Amazon Lightsail API 參考中的[套裝軟體](#)。

- 範例 1 — 您 USD 每月有一個 \$5 的執行個體套裝軟體 (bundleId nano\_3\_0)，每月 1 TB 的資料傳輸額度。如果您傳送 500 GB 的資料到網際網路 (資料傳輸 OUT)，並傳送 400 GB 的資料到執行個體 (資料傳輸 IN)，就會耗用 900 GB 的 1 TB 額度。如果您傳送另外 200 GB 的資料到網際網路，您的額度將超過 100 GB，並且需要支付 100 GB 的資料傳輸 OUT 超額費用。如果您接下來將 200 GB 的資料傳送至執行個體，則不會向您收取超額費用。
- 範例 2 — 如果您在一個區域中 USD 每月有兩個 \$5 的執行個體套裝軟體 (bundleId nano\_3\_0)，每個區域中每個月有 1 TB 的資料傳輸額度，您將獲得 2 TB 的資料傳輸額度合計。如果您使用第一個執行個體傳送 1.5 TB 的資料到網際網路，並使用第二個執行個體傳送 100 GB 的資料到網際網路，則在總容量 2 TB 以下仍然有 400 GB 的容量，而且不會向您收取任何資料傳輸 OUT 超額費用。
- 範例 3 — 您建立兩組執行個體套裝軟體：設定 A，USD 每月兩個 \$5 的執行個體套裝軟體 (bundleId nano\_3\_0)，以及將 B 設定為 USD 每月三個 \$7 的執行個體套裝軟體 (bundleId micro\_3\_0)，兩者皆位於美國西部 (奧勒岡) 區域。總而言之，這為組 A 提供 2 TB 的資料傳輸額度，組 B 的資料傳輸額度為 6 TB。如果您透過集 A 執行個體傳輸 3 TB 的資料到網際網路，並透過組 B 執行個體傳輸 4 TB 的資料傳輸額度，則會超過 Set A 執行個體的資料傳輸額度，並支付 1 TB 的資料傳輸 OUT 超額費用。您仍將在 Set B 執行個體的限額範圍內達到 2 TB。
- 範例 4 — 在帳單月份的前 20 天內，您已經使用了 USD 每月 3.50 USD 的 IPv6 執行個體套裝軟體 (bundleId nano\_ipv6\_3\_0)，佔總 1 TB 資料傳輸額度的 600 GB。您決定在第 21 天將執行個體的網路類型切換為雙堆疊 (以 USD 每月 \$5 美元的價格計 bundleId nano\_3\_0 費)。您當月的資料傳輸使用率不會重設，而且會維持 600 GB，剩餘 400 GB 額度。在帳單月份剩餘時間內，如果您傳送 500 GB 的資料到網際網路，就會產生 100 GB 的資料傳輸 OUT 超額費用。
- 範例 5 — 您 USD 每月有三個 \$5 的執行個體套裝軟體 (bundleId nano\_3\_0)，每個都有 1 TB 的每月資料傳輸額度。假設您在帳單月份內耗用了總共 3 TB 的 1 TB 資料傳輸額度，這會讓您剩下 2 TB 的資料傳輸額度。如果您在同一個帳單月份刪除所有執行個體，並在同一個地區建立了同一套裝軟體的三個新執行個體 (bundleId nano\_3\_0)，您的資料傳輸使用率仍將為 1 TB，而剩餘的資料傳輸額度仍為 2 TB。您可以在開始計算任何資料傳輸 OUT 超額費用之前的同一個月內，透過執行個體傳輸多達 2 TB 的資料。

## 資料傳輸額度如何與負載平衡器搭配使用？

負載平衡器不會佔用資料傳輸額度。系統會計算負載平衡器與目標執行個體或分發之間的流量，並計入執行個體或分發的資料傳輸額度，與從網際網路進出的流量計入不在負載平衡器後方的 Lightsail 執行個體的資料傳輸額度相同。負載平衡器到網際網路之間的進出流量不會計入執行個體的資料傳輸額度。

## 萬一超出資料傳輸計劃額度呢？

資料傳輸計劃的設計可涵蓋絕大部分客戶的全部傳輸量，不會產生任何額外費用。如果您的執行個體超過其計劃資料傳輸額度，則需要支付每 GB 資料傳輸使用的超額費用 (僅限資料傳輸OUT至網際網路)。

即使執行個體超出計劃資料傳輸額度，許多類型的資料傳輸也免費。將資料傳入至 Lightsail 執行個體和資料庫一律免費。OUT從 Lightsail 執行個體傳輸至另一個 Lightsail 執行個體、Lightsail 執行個體和 Lightsail 受管資料庫之間的資料傳輸，或者如果使用私有 IP 位址，也可免費將資料傳輸至相同區域中的 AWS 資源。

## 我需要支付哪種資料傳輸類型的費用？

當您超過執行個體方案的每月免費資料傳輸額度時，使用公有 IP 位址時，將會向您收取OUT從 Lightsail 執行個體傳輸至網際網路 AWS 區域 或其他執行個體或相同區域 AWS 資源的資料傳輸費用。這些類型的資料傳輸超過免費額度的費用如下。

- 美國東部 (俄亥俄州) (us-east-2) : 0.09 /GB USD
- 美國東部 (維吉尼亞北部) (us-east-1) : 0.09 /GB USD
- 美國西部 (奧勒岡) (us-west-2) : 0.09 /GB USD
- 亞太區域 (孟買) ( ap-south-1 ) : 每 GB 0.13 美元 USD
- 亞太區域 (首爾) (至 ap-northeast-2) : 0.13 /GB USD
- 亞太區域 (新加坡) (ap-southeast-1) : 每 GB 0.12 美元 USD
- 亞太區域 (雪梨) (ap-southeast-2) : 每 GB 0.17 美元 USD
- 亞太區域 (東京) ( ap-northeast-1 ) : 0.14 /GB USD
- 加拿大 (中部) ( ca-central-1 ) : 0.09 /GB USD
- 歐洲 (法蘭克福) ( eu-central-1 ) : 0.09 /GB USD
- 歐洲 (愛爾蘭) ( eu-west-1 ) : 0.09 /GB USD
- 歐洲 (倫敦) ( eu-west-2 ) : 0.09 /GB USD
- 歐洲 (巴黎) ( eu-west-3 ) : 0.09 /GB USD

- 歐洲 ( 斯德哥爾摩 ) ( eu-north-1 ) : 0.09 /GB USD

在不同可用區域建立的執行個體可私下進行區域之間的免費通訊，而且不太可能同時受到損害。可用區域讓您可以建立高度可用的應用程式和網站，而且不會增加資料傳輸的費用或危及應用程式的安全。

當您超出 Lightsail CDN 配送計劃的資料傳輸額度時，會向您收取所有資料傳輸OUT的費用。超過發佈額度的資料傳輸費用與 Lightsail 執行個體不同，如下所示。

- 亞太地區：每 GB 0.13 美元 USD
- 加拿大：每 GB 0.09 美元 USD
- 歐洲：每 GB 0.09 美元 USD
- 印度：每 GB 0.13 美元 USD
- 日本：每 GB 0.14 美元 USD
- 中東：每 GB 0.11 美元 USD
- 南非：每 GB 0.11 美元 USD
- 南美洲：每 GB 0.11 USD 美元
- 美國：每 GB 0.09 USD 美元

## 我的執行個體資料傳輸額度有何不同 AWS 區域？

您可以在 [Amazon Lightsail](#) 定價中找到 Lightsail 執行個體的區域資料傳輸額度。除了亞太區域 ( 孟買和雪梨 ) 地區外 AWS 區域，所有人的津貼都是相同的。孟買和雪梨地區的計劃包括其他區域的一半資料傳輸額度。

Lightsail 受管資料庫的資料傳輸額度完全 AWS 區域相同。

## Lightsail 網域的費用是多少？

連結的 .pdf 檔案中列出的價格適用於新的網域名稱註冊，以及 2021 年 12 月 22 日起續約的現有網域名稱註冊。所有價格均包括一個DNS區域和隱私保護。如需註冊域的費用資訊，請參閱 [Amazon Route 53 域註冊定價](#)和[域註冊](#)。

## Lightsail DNS 管理的成本是多少？

DNS管理是免 Lightsail。您最多可以為每DNS個DNS區域建立 6 個區域和任意數量的記錄。您還可以獲得每月 300 萬次DNS查詢的每月津貼給您的區域。除了一個月的 前 3 百萬個查詢之外，您需支付每 100 萬個DNS查詢 USD \$0.40 美元的費用。

## Lightsail 快照的費用是多少？

Lightsail 快照 (手動和自動) 的儲存費用為每月 0.05 USD USD。這表示如果您建立使用 28 GB 空間的執行個體快照，並將其保留一個月，則該月需支付 \$1.40 美元的USD費用。

當您為同一個執行個體拍攝多個連續快照時，Lightsail 會自動將快照成本最佳化。對於每個新建立的快照，只需針對資料變更的部分付費。在上述範例中，如果您的執行個體資料只變更 2 GB，則第二個執行個體快照USD每月僅需 0.10 USD。

## 如何管理我的 AWS 帳戶？

Lightsail 是一項在 AWS 受信任且經過驗證的雲端基礎架構上執行的 AWS 服務。您使用相同的 AWS 帳戶和認證來登入 Lightsail 和 AWS Management Console

您 AWS 可以從 Billing and [Cost Management 主控台管理 AWS 帳戶](#)，包括變更帳戶密碼、使用者名稱、聯絡資訊或帳AWS 單資訊。

## 什麼是 Lightsail 法律使用條款？

Lightsail 是 Amazon 網路服務，因此若要使用 Lightsail，您必須先同意[AWS 客戶協議和服務條款](#)。建立 Lightsail 執行個體時，您也同意您對軟體的使用也必須遵守賣家的一般使用者授權合約，您可以在建立執行個體頁面檢閱。

## 我該如何支付我的帳單？

您可以透過 Billing and Cost Management 主控台支付和管理 AWS 帳單。AWS 接受大多數主要信用卡。請在[這裡](#)進一步了解如何管理您的付款方式。

## 區塊儲存 (磁碟)

### 我可以使用 Lightsail 區塊儲存裝置做什麼？

Lightsail 區塊儲存空間提供額外的儲存磁碟區 (在 Lightsail 中稱為「連接的磁碟」)，您可以將其連接至 Lightsail 執行個體，類似於個別硬碟。連接磁碟非常適用於以下情況：當應用程式和軟體需要從核心服務區分特定的資料，以及保護應用程式資料不受執行個體和系統磁碟故障或其他問題影響時。連接磁碟為經常讀取存放資料的應用程式或軟體提供一致的效能和低延遲。

Lightsail 區塊儲存磁碟使用固態硬碟 (SSD)。這種類型的區塊儲存在低廉的價格和良好的效能之間取得平衡，旨在支援在 Lightsail 上執行的絕大多數工作負載。對於需要持續IOPS效能、每個磁碟大量輸

送量或執行 MongoDB、Cassandra 等大型資料庫的應用程式的客戶，我們建議您使用 Amazon EC2 搭配 GP2 或佈建 IOPS SSD 儲存，而不是 Lightsail。

## 連接的磁碟與 Lightsail 方案中包含的儲存空間有何不同？

Lightsail 方案隨附的系統磁碟就是執行個體的根裝置。如果您終止執行個體，系統磁碟也會被刪除。如果執行個體故障，系統磁碟可能會受到影響。您也無法分離您的系統磁碟或將其與您的執行個體分開備份。存放在連接磁碟上的資料與執行個體無關。連接的磁碟可在執行個體之間分離和移動。您可以建立磁碟的手動快照，以獨立於執行個體進行備份。為了保護您的資料，建議您僅將 Lightsail 執行個體的系統磁碟用於暫存資料。對於需要更高級別耐久性的資料，我們建議使用連接磁碟，並定期使用磁碟或執行個體快照備份磁碟。

## 連接磁碟可以有多大？

每個連接的磁碟最多可達 16 TB，而 Lightsail 帳戶中連接的區塊儲存空間總量不得超過 20 TB。

## 每個 Lightsail 執行個體可以連接多少個磁碟？

您最多可以將 15 個磁碟連接至 Lightsail 執行個體。

## 是否可將磁碟連接到多個執行個體？

否，磁碟一次只能連接一個執行個體。

## 磁碟是否一定要連接到執行個體？

否，您可以選擇不將磁碟連接到執行個體。磁碟在帳戶中將保持未連接的狀態。即使磁碟沒有連接執行個體，價格也都一樣。

## 是否可增加連接磁碟的大小？

是，如果想要增加磁碟的大小，可以建立磁碟快照，然後從該快照建立更大的新磁碟。

## Lightsail 區塊儲存是否提供加密功能？

是，為了保護資料安全，所有 Lightsail 連接的磁碟和磁碟快照預設都會使用 Lightsail 代表您管理的金鑰加密靜態。Lightsail 也會在資料在 Lightsail 執行個體和連接的磁碟之間移動時，提供資料加密功能。

## 我可以期待 Lightsail 區塊儲存裝置有哪些可用性？

Lightsail 區塊式儲存設計可提供高可用性和可靠性。每個連接的磁碟會在其可用區域內自動複寫，保護您免於任何組件故障的威脅。Lightsail 區塊儲存磁碟的設計可提供 99.99% 的可用性。Lightsail 也支援磁碟快照，以便定期備份資料。

## 如何備份連接磁碟？

您可以透過建立磁碟的手動快照來備份磁碟。您也可以建立執行個體的手動快照，或為已連接磁碟的執行個體啟用自動快照，藉此備份整個執行個體和任何連接的磁碟。連接至執行個體的磁碟包含在執行個體手動和自動快照中。

## 憑證

### 如何使用 Lightsail 建的憑證？

SSL/TLS 證書用來建立您的網站或應用程式的身份以及瀏覽器與您的網站之間的安全連接。Lightsail 提供可與負載平衡器搭配使用的已簽署憑證，而且負載平衡器會在透過安全 AWS 網路將已驗證的流量路由到目標執行個體之前提供 SSL/TLS 終止。Lightsail 憑證只能與 Lightsail 負載平衡器搭配使用，而不能與個別的 Lightsail 執行個體搭配使用。

### 如何驗證我的憑證？

Lightsail 憑證經過網域驗證，這表示您必須先驗證您擁有或可存取網站網域，以提供身分證明，才能由憑證授權單位佈建憑證。當您要求新的憑證時，Lightsail 會嘗試自動驗證憑證。如果憑證無法自動驗證，Lightsail 會提示您將 CNAME 記錄新增至您正在驗證的網域 DNS 區域。無論是 Lightsail DNS 管理或外部 DNS 主機服務供應商，無論是目前管理 DNS 區域的任何地方，您都有 72 小時的時間可以新增 CNAME 記錄。

### 如果無法驗證我的網域，會發生什麼情況？

為了安全起見，您必須證明自己擁有網域。這表示如果您或組織中的某人因任何原因無法新增 DNS 記錄來驗證憑證，您將無法透過 Lightsail 使用 HTTPS 已啟用的負載平衡器。

### 可以在憑證增加多少個網域和子網域？

每個憑證可以新增最多 10 個域或子域。Lightsail 不支援萬用字元網域。

## 如何變更與憑證關聯的網域？

若要變更與憑證關聯的網域 (新增/刪除)，您需要重新提交憑證並重新驗證網域擁有權。按照憑證管理畫面中的步驟重新產生憑證，並在出現提示時新增或移除網域。

## 如何續約憑證？

Lightsail 為您的 SSL/TLS 憑證提供受管理的續約服務。這表示 Lightsail 會嘗試在憑證到期前自動續約憑證，不需要您採取任何動作。您的 Lightsail 憑證必須與負載平衡器主動關聯，才能自動續訂。

## 刪除負載平衡器時，我的憑證會發生什麼狀況？

刪除負載平衡器時，您的憑證也會隨之刪除。如果將來需要針對相同的網域使用憑證，需申請並驗證新的憑證。

## 我可以下載我提供的憑證嗎？

否，Lightsail 憑證已綁定到您的 Lightsail 帳戶，無法在 Lightsail 之外移除和使用。

## 聯繫人和監控通知

### 什麼是通知？

您可在 Lightsail 中設定警示，以在其中一個執行個體、資料庫或負載平衡器的指標超過指定的閾值時通知您。通知可以採用 Lightsail 主控台中顯示的橫幅、傳送至您指定地址的電子郵件，或是傳送至您指定之行動電話號碼的 SMS 簡訊。若要透過電子郵件和 SMS 簡訊收到通知，您必須將您的電子郵件地址和行動電話號碼新增為通知聯絡人，並 AWS 區域 在每一個您想要監視資源的位置中。如需有關通知的詳細資訊，請參閱[通知](#)。

### 我可以新增多少個聯絡人？

您可以在每個要監控資源的 AWS 區域 方新增一個電子郵件地址和一個行動電話號碼。SMS 並非所有 AWS 區域可建立 Lightsail 資源的簡訊都支援，而且文字訊息無法傳送至世界上某些國家和地區。如需有關通知的詳細資訊，請參閱[通知](#)。

## 容器服務

### 我可以使用 Lightsail 貨櫃服務做什麼？

Lightsail 容器服務提供了一種在雲端中執行容器化應用程式的簡便方法。您可以在容器服務 (從簡單的 Web 應用程式到多個分級的微服務) 上執行各種應用程式。您只需指定容器服務所需的容器映像 CPU、Power (RAM) 和規模 (節點數目) 即可。Lightsail 負責執行容器服務，而無需管理任何基礎架構。Lightsail 將為您提供負載平衡 TLS 端點，以存取容器服務上執行的應用程式。

### Lightsail 容器服務是否可以執行碼頭集裝箱？

是。Lightsail 支持基於 Linux 的碼頭集裝箱。目前不支援 Windows 容器。

### 如何將我的公用容器映像檔與 Lightsail 容器服務搭配使用？

您可以使用線上公開登錄檔 (例如 Amazon ECR 公共登錄) 的容器映像檔，或建立自己的自訂映像檔，並使用幾個簡單的步驟將其推送至 Lightsail。AWS CLI 如需詳細資訊，請參閱 [推送和管理容器映像](#)。

### 我是否可以從私有容器登錄檔中提取容器映像？

目前，Lightsail 容器服務僅支援公用容器登錄。或者，您可以將自訂容器映像檔從本機電腦推送至 Lightsail，以保持其隱私。

### 我是否可以根據需求變更服務的能力和規模？

可以，即使在建立服務後，也可以隨時變更容器服務的能力和規模。

### 我可以自訂 Lightsail 容器服務所建立之 HTTPS 端點的名稱嗎？

Lightsail 會以該格式 `<service-name>.<random-guid>.<aws-region-name>.cs.amazonlightsail.com` 為每個容器服務提供 HTTPS 端點。只有服務名稱可自訂。或者，您可以使用自訂網域名稱。如需詳細資訊，請參閱 [啟用和管理自訂域](#)。

### 我可以將自訂網域用於 Lightsail 容器服務的 HTTPS 端點嗎？

是。您可以在 Lightsail 中建立含有自訂網域名稱的 SSL/TLS 憑證，並將其附加至您的容器服務。憑證必須經過網域驗證。如果您 DNS 的網域使用 Lightsail DNS 區域，您可以將網域頂點 (example.com)

或子網域 () 的流量路由到您的容器服務。www.example.com或者，您可以使用支援新增ALIAS記錄的DNS主機服務供應商，將網域頂點 (example.com) 對應至 Lightsail 容器服務的預設網域 (公用DNS)。如需詳細資訊，請參閱[啟用和管理自訂域](#)。

## Lightsail 集裝箱服務的費用是多少？

Lightsail 容器服務是以隨需小時費率計費，因此您只需按使用量付費。對於您使用的每個 Lightsail 容器服務，我們會按每小時固定價格向您收取費用，最高為每月服務價格。每月最高服務價格可以透過將服務能力的基本價格乘以服務規模來計算。例如，能力為 Micro 和規模為 2 的服務每月費用最多為 10 USD \* 2=20 USD。最便宜的 Lightsail 集裝箱服務起價為每USD小時 0.0094 美元 (每月 7 美元)。USD如果使用量超過每項服務每月 500 GB 的免費配額，可能需要支付額外的資料傳輸費。

## 即使我的容器服務執行時間只有幾天，我是否仍需要支付整個月的費用？

您的 Lightsail 容器服務只有在處於執行中或停用狀態時才會收費。如果您在月底之前刪除 Lightsail 容器服務，我們會根據您使用 Lightsail 容器服務的總時數，向您收取按比例分配的費用。例如，如果您在一個月內使用 Lightsail 容器服務，並且規模為 1，並且規模為 100 小時，您將需支付 1.34 美元的費用 (0.0134\*100 美元)

## 我是否需要為進出容器服務的資料傳輸量付費？

每項容器服務都有資料傳輸配額 (每月 500 GB)。這同時計入數據傳輸 IN 和您OUT的服務。當您超出配額時，使用公用 IP 位址時，將會向您收取OUT從 Lightsail 容器服務傳輸至網際網路 AWS 區域 或其他地區或相同區域 AWS 資源的資料傳輸費用。這些類型的資料傳輸超過免費額度的費用如下。

### 超出每月數據傳輸額度的收費

- 美國東部 (俄亥俄州) (us-east-2) : 0.09 /GB USD
- 美國東部 (維吉尼亞北部) (us-east-1) : 0.09 /GB USD
- 美國西部 (奧勒岡) (us-west-2) : 0.09 /GB USD
- 亞太區域 (孟買) ( ap-south-1 ) : 每 GB 0.13 美元 USD
- 亞太區域 (首爾) (至 ap-northeast-2) : 0.13 /GB USD
- 亞太區域 (新加坡) (ap-southeast-1) : 每 GB 0.12 美元 USD
- 亞太區域 (雪梨) (ap-southeast-2) : 每 GB 0.17 美元 USD
- 亞太區域 (東京) ( ap-northeast-1 ) : 0.14 /GB USD
- 加拿大 (中部) ( ca-central-1 ) : 0.09 /GB USD

- 歐洲 ( 法蘭克福 ) ( eu-central-1 ) : 0.09 /GB USD
- 歐洲 ( 愛爾蘭 ) ( eu-west-1 ) : 0.09 /GB USD
- 歐洲 ( 倫敦 ) ( eu-west-2 ) : 0.09 /GB USD
- 歐洲 ( 巴黎 ) ( eu-west-3 ) : 0.09 /GB USD
- 歐洲 ( 斯德哥爾摩 ) ( eu-north-1 ) : 0.09 /GB USD

## 停用和刪除容器服務有什麼區別？

停用容器服務時，容器節點處於停用狀態，且服務的公用端點會傳回HTTP狀態碼「503」。啟用服務會將其還原至上次作用中的部署。也會保留能力和規模組態。重新啟用後，公有端點名稱不會變更。會保留部署歷史記錄和容器映像。

刪除容器服務時，您是在進行一種破壞性的動作。服務的所有容器節點將被永久刪除。與您的服務相關聯的HTTPS公用端點位址、容器映像、部署歷程記錄和記錄也會永久刪除。您將無法復原端點地址。

## 如果我的容器服務處於停用狀態，系統是否會向我收取費用？

是，即使容器服務處於停用狀態，也會根據容器服務的能力和規模組態向您收費。

## 我可以將容器服務做為 Lightsail 內容傳遞網路 (CDN) 發佈的來源嗎？

目前不支援容器服務做為 Lightsail CDN 發行版的來源。

## 我可以將容器服務做為 Lightsail 負載平衡器的目標嗎？

沒有 容器服務目前無法做為 Lightsail 負載平衡器的目標使用。不過，容器服務的公有端點會隨附內建的負載平衡。

## 我可以將容器服務的公用端點設定為將HTTP要求重新導向至HTTPS嗎？

Lightsail 容器服務公用端點會自動重新導向所有HTTPHTTPS要求，以確保您的內容能夠安全地提供。

## 容器服務是否支援監控和提醒？

容器服務會針對服務節點的使用CPU率和記憶體使用率提供指標。目前不支援以這些指標為基礎的提醒。

## Lightsail 集裝箱服務是否支援IPv6？

Lightsail 容器服務HTTPS端點同時支援IPv4和IPv6。無法在容器服務上停用 IPv6。

## 內容交付網路分發

### 我可以使用 Lightsail CDN 發行版做什麼？

Lightsail 內容交付網路 (CDN) 分發可讓您在由 Amazon 提供支援的 Amazon 全球交付網路上儲存和提供內容，輕鬆地加速 Lightsail 資源上託管的內容的交付速度。CloudFront分發還可以HTTPS通過提供簡單的SSL證書創建和託管來幫助您使您的網站支持流量。最後，發行版可協助減少 Lightsail 資源的負載，並協助您的網站處理大量流量峰值。就像所有 Lightsail 的功能一樣，只需按幾下滑鼠即可完成設定，而且您只需支付每月簡單的價格。

### 我可以使用哪些類型的資源作為分發的原始伺服器？

Lightsail 發行版可讓您使用 Lightsail 執行個體和負載平衡器做為起源。Lightsail 容器目前不支援做為起源。不支援 Lightsail 以外的資源，例如 S3 儲存貯體。

### 我是否需要將靜態IPv4位址附加至 Lightsail 執行個體，才能將其用作 Lightsail 發行版本的來源？

是，靜態IPv4位址必須附加至指定為來源的執行個體。Lightsail 發行版目前不支援IPv6。

### 如何在我的 WordPress 網站上設定 Lightsail 發行版本？

建立您的發行版本、選取您的 WordPress 執行個體做為來源、選擇您的方案，就可以設定完畢。Lightsail 發行版會自動設定您的發佈設定，以最佳化大部分 WordPress 組態的效能。

### 我是否可以連接多個原始伺服器？

雖然您無法將多個來源連接至 Lightsail 發行版本，但是您可以將多個執行個體連接至 Lightsail 負載平衡器，並將其指定為發佈的原點。

### Lightsail 發行版是否支援憑證建立？

是。Lightsail 發行版可讓您直接從分發的管理頁面輕鬆建立、驗證和附加憑證。

## 是否需要憑證？

只有當您想要對分發使用自訂網域名稱時，才需要憑證。所有 Lightsail 發行版都是使HTTPS用已啟用的唯一 Amazon CloudFront 網域名稱建立的。但是，如果您想要將自訂網域與分發搭配使用，則需要將自訂網域的憑證連接到分發。

## 可建立的憑證數量是否有限？

是，如需詳細資訊，請參閱 [Lightsail 服務配額](#)。

## 如何配置我的分發以將HTTP請求重定向到HTTPS？

Lightsail 發佈會自動重新導向所有HTTP請求，HTTPS以確保您的內容能夠安全地提供。

## 如何將我的頂點網域設定為指向我的 Lightsail 發行版本？

為了將您的頂點域指向您的CDN分發，您必須在域的域名系統 ( DNS ) 中創建一個ALIAS記錄，將您的頂點域映射到分發的默認域。如果您的DNS主機服務供應商不支援ALIAS記錄，您可以使用 Lightsail DNS 區域輕鬆將 Apex 網域設定為指向分發網域。

## Lightsail 的執行個體資料傳輸配額和散發資料傳輸配額有何差異？

雖然資料傳入並OUT計入執行個體的資料傳輸配額，但只有資料傳輸OUT到原始伺服器 and 給檢視者的資料會計入您分發的配額中。此外，超出分發配額OUT的所有資料傳輸都會收取超額費用，而某些類型的資料傳輸對於執行個體則OUT是免費的。最後，Lightsail 發行版使用不同的區域超額費率模式，儘管大部分費率與針對執行個體超額收取的費率相同。

## 我是否可以變更與分發相關聯的計劃？

是，您每月可以變更分發計劃一次。如果您想再次變更計劃，您必須等到下個月初才能變更。

## 如何知道我的分發是否有效？

Lightsail 散發可為您提供各種追蹤散發績效的指標，包括分發已收到的請求總數、分發已傳送給客戶和來源的資料量，以及導致錯誤的請求百分比。此外，您可以建立與分發指標連結的提醒。

## 我可以刪除 Lightsail 發行版本上的快取內容嗎？

您可以刪除所有快取內容，但不能刪除特定的檔案或資料夾。

## 什麼時候應該使用 Lightsail 發行版與 Amazon 發行 CloudFront 版？

Lightsail 發行版是專為在 Lightsail 資源 (例如執行個體和負載平衡器) 上託管網站或 Web 應用程式的使用者所設計。如果您在中使用其他服務 AWS 來託管網站或應用程式、有複雜的組態需求，或者工作負載涉及大量每秒要求或大量視訊串流，我們建議您使用 Amazon CloudFront。

## 我可以將 Lightsail 內容交付網路 (CDN) 分發移到 Amazon CloudFront 嗎？

是的，您可以透過在 Amazon CloudFront 中建立類似設定的分發來移動 Lightsail 分發。您也可以可以在 Lightsail 發行版中設定的所有設定，也可以在發行版中進行設定 CloudFront。請完成下列步驟，將您的發行版本移至 CloudFront。

### 如何將您的 Lightsail 發行版本移至 CloudFront

- 拍攝設定為發行版本來源的 Lightsail 執行個體的快照。將快照匯出到 AmazonEC2，然後從 Amazon 中的快照建立新執行個體 EC2。如需詳細資訊，請參閱[將快照匯出到 Amazon EC2](#)。

#### Note

如果您需要對網站或 Web 應用程式進行負載平衡，請在 Elastic Load Balancing 中建立應用程式負載平衡器。如需詳細資訊，請參閱《[Elastic Load Balancing 使用者指南](#)》。

- 停用 Lightsail 發佈的自訂網域，以中斷連結您可能已附加的憑證。如需詳細資訊，請參閱[停用 Amazon Lightsail 分發的自訂網域](#)。
- 使用 AWS Command Line Interface (AWS CLI) 執行取得分發命令，以取得 Lightsail 發行版本的設定清單。如需詳細資訊，請參閱《AWS CLI 參考》中的 [get-distributions](#)。
- 登入[CloudFront主控台](#)，並使用與 Lightsail 發行版本相同的組態設定建立發行版。如需詳細資訊，請參閱 [Amazon CloudFront 開發人員指南中的建立分發](#)。
- 在 AWS Certificate Manager (ACM) 中創建一個證書，您將附加到您的 CloudFront發行版。如需詳細資訊，請參閱[ACM使用者指南中的要求公用憑證](#)。
- 更新您的 CloudFront 發行版以使用您建立的 ACM憑證。如需詳細資訊，請參閱[CloudFront 使用者指南中的更新 CloudFront 發行版](#)。

## 如何使用 LightsailCDN ？

Lightsail CDN 發行版是使用固定價格的資料傳輸組合來建立，以便讓使用服務的成本變得簡單且可預測。分發搭售套件是為了涵蓋一個月的使用量而設計。以避免產生超額費用的方式 (包括但不限於經

常升級或降級搭售套件，或對單一原始伺服器使用過多的分發) 使用分發搭售套件已超出預期的使用範圍，且這是不允許的做法。此外，不允許涉及大量每秒請求或大量影片串流的工作負載。進行這些行為可能會導致資料服務或帳戶的調節或暫停。

## Lightsail CDN 發行版是否支援IPv6？

依預設，所有 Lightsail CDN 發行版都已IPv6啟用。分發主機名稱會解析為IPv4和IPv6位址。IPv6您可以使用管理頁面的 [網路功能] 索引標籤上CDN的切換來停用。

## 是否需要IPv6啟用來源才能與 Lightsail CDN 發行版一起使用？

沒有 CDN分佈接受IPv6和IPv4流量，並在與後端的來源通信IPv4時將其無縫轉換為。因此，分佈背後的起源可以是雙堆棧或IPv4只。

## 資料庫

### 什麼是 Lightsail 資料庫？

Lightsail 受管資料庫是專用於執行資料庫的執行個體，而不是其他工作負載，例如 Web 伺服器、郵件伺服器。受管資料庫可以包含多個使用者建立的資料庫，可以使用您搭配獨立資料庫使用的相同工具和應用程式來進行存取。Lightsail 會維護資料庫基礎架構和作業系統的安全性和健全狀況，因此您無需深入的基礎架構管理專業知識即可執行資料庫。

與一般 Lightsail 執行個體一樣，Lightsail 受管資料庫在其計劃中具有固定數量的記憶體、運算能力和 SSD基礎儲存，可讓您隨時間擴充。Lightsail 會在建立時自動為您安裝並設定您選擇的資料庫。

### 我可以使用 Lightsail 受管資料庫做什麼？

Lightsail 受管資料庫提供簡單、低維護的方式，將資料儲存在雲端。您可以將受管理的資料庫當做新資料庫執行，也可以從現有的內部部署或託管資料庫移轉至 Lightsail 來執行。

其還可以讓您擴展應用程式，透過將資料庫分離為專用預留執行個體，可接受更大量的流量和更密集的負載。Lightsail 受管資料庫對於可設定狀態的應用程式 (例如 WordPress 最常見CMSs的應用程式) 特別有用，當您擴充超出單一執行個體時，這些應用程式需要保持同步的資料。受管理的資料庫可與 Lightsail 負載平衡器和兩個以上的 Lightsail 執行個體配對，以建立功能強大且可擴充的應用程式。透過使用 Lightsail 高可用性受管資料庫計劃，您也可以為資料庫新增備援，協助確保應用程式的高連續運作時間。

## Lightsail 為我管理什麼？

Lightsail 可管理受管理資料庫及其基礎架構的一系列維護活動和安全性。Lightsail 會自動備份您的資料庫，並允許使用資料庫還原工具從過去 7 天進行時間點還原，以協助防止資料遺失或元件故障。Lightsail 還會自動加密靜態和動態資料，以提高安全性，並儲存您的資料庫密碼，以便輕鬆安全地連接到資料庫。在維護方面，Lightsail 會在設定的維護時段期間對資料庫執行維護。此維護包含自動升級到最新的次要資料庫版本和基礎設施和作業系統的所有管理。

## Lightsail 支援哪些類型的資料庫以及這些資料庫的哪些版本？

Lightsail 受管理的資料庫支援最新的主要版本「我」SQL 和「Post SQL gre」。目前，這些版本是我的 SQL 5.7，我的 SQL 8.0，後者 SQL 9，後備 SQL 10，後者 SQL 11 和後格雷 12。SQL Lightsail 僅為每個主要版本選項提供最新的次要版本。

## Lightsail 提供哪些受管理的資料庫計劃？

Lightsail 在標準和高可用性計劃中提供 4 種大小的受管理資料庫。每個計劃都有固定的儲存數量和每月額度的資料傳輸。您也可以在這一段時間後，根據需要擴展到較大的計劃，並切換標準和高可用性計劃。高可用性計劃會鏡映與標準計劃相同的資源，且還包括在主要資料庫的單獨可用區域中執行的備用資料庫，來提供冗餘。

## 什麼是高可用性計劃？

Lightsail 受管理的資料庫提供標準和高可用性計劃。標準和高可用性計劃有相同的計劃資源 (包括記憶體、儲存和資料傳輸額度)。高可用性計劃透過在與主要資料庫不同的可用區域中自動建立待命資料庫、同步將資料複製到待命資料庫，以及在基礎結構故障和維護期間提供容錯移轉至待命資料庫，以便在 Lightsail 自動升級/維護資料庫時也能確保正常運作時間。將高可用性計劃用於需要高執行時間之生產應用程式或軟體的執行。

## 如何擴展或縮小 Lightsail 受管資料庫？

您可以透過拍攝 Lightsail 受管理資料庫的快照，並從快照建立新的、更大的資料庫計劃，或使用緊急還原功能建立新的、更大的資料庫，來擴展其規模。您也可以從標準切換到高可用性計劃，使用其中一種方法來反向操作。您不能縮減資料庫。如需詳細資訊，請參閱 [在 Lightsail 中從快照建立資料庫](#)。

## 如何備份受管理 Lightsail 料庫？

Lightsail 會自動備份您的資料，並允許將此資料從特定時間點還原至新資料庫。自動備份是適用於您資料庫的一種免費服務，但只會儲存最近 7 天的資料。如果您刪除資料庫，則會刪除所有自動備份記

錄，而且無法再進行 point-in-time 還原。以往若要在刪除資料庫後保留資料備份或將備份保留超過 7 天的時間，請使用手動快照。

您可以從資料庫管理頁面拍攝 Lightsail 受管理資料庫的手動快照。手動快照包含您資料庫的所有資料且可做為您想要永久存放的資料備份。您也可以使用手動快照來建立新的、較大的資料庫，或切換標準和高可用性計劃。手動快照會一直儲存，直到您刪除它們為止，並以每月 0.05 USD /GB 的費用計費。

## 如果我刪除 Lightsail 受管理的資料庫，我的資料會發生什麼情況？

如果您刪除 Lightsail 管理的資料庫，您的資料庫本身和所有自動備份都會遭到刪除。此資料無法恢復，除非您在刪除資料庫前先手動拍攝快照。在刪除資料庫期間，Lightsail 提供一鍵式選項，視需要擷取手動快照，以協助防止資料意外遺失。拍攝手動快照再刪除，這樣的作法是選擇性的，但我們強烈建議這麼做。您可以在未來您不再需要存放的資料時刪除手動快照。

## 是否可以將執行個體連線到在不同 AWS 區域 或不同可用區域中執行的 Lightsail 受管資料庫？

您無法將 Lightsail 受管資料庫用於執行不同 AWS 區域的執行個體。不過，您可以將資料庫用於與執行個體不同的可用區域。

## 如何將資料載入 Lightsail 受管理的資料庫？

若要將資料載入 Lightsail 受管理的資料庫，您應該先啟用資料匯入模式。啟用資料匯入模式之後，您可以繼續使用您偏好的資料庫用戶端來手動上傳資料。您完成載入資料的動作後，請記得關閉資料匯入模式，讓資料庫的自動備份和記錄可以繼續。如需詳細資訊，請參閱[將資料匯入我的資料SQL庫](#)和[將資料匯入 Postgre 資料SQL庫](#)。

## 如何存取 Lightsail 受管資料庫上的資料？

您可以連接到數據庫並使用任何標準SQL客戶端應用程序查詢數據。我們建議我的SQL工作台進行GUI基於管理和查詢。您可以在資料庫的資料庫管理畫面中找到連線資料，包括端點URL和DNS名稱。如需詳細資訊，請參閱在[Amazon Lightsail 中連 Connect 到我的資SQL料庫或連線到 Postgre 資SQL料庫](#)。

## Lightsail 受管資料庫如何與我的 Lightsail 執行個體搭配使用？

建立 Lightsail 受管理的資料庫之後，您可以立即開始使用 Lightsail 執行個體做為 Web 伺服器或應用程式的其他專用工作負載。若要將 Lightsail 執行個體連線至資料庫，請使用資料庫端點並參考安全儲

存的密碼，將資料庫設定為應用程式程式碼中的資料存放區。您可以在資料庫管理畫面中找到連線資料。資料庫組態檔案的檔案名稱和位置會隨著應用程式而不同。請注意，您可以擇一使用相同的資料表，或是使用不同的資料表將多個執行個體連接到單個資料庫。

## 如何將 Lightsail 受管資料庫連線到 AWS 帳戶中 EC2 執行的執行個體？

您可以透過公用網際網路連線，將 Lightsail 受管資料庫連線到 EC2 執行個體。請注意，連線到所有 AWS 服務都會消耗您的資料庫資料傳輸額度，而透過公用網際網路傳輸至超出資料傳輸額度的 AWS 服務，則會產生超額費用。您無法在 Lightsail 受管資料庫和 EC2 執行個體 VPC 之間使用對等互連。

## Lightsail 受管資料庫的公開和私有模式有何不同？

根據預設，您的 Lightsail 受管理資料庫是以私人模式建立的，只能由 Lightsail 執行個體存取，以保護資料庫的安全性。如果您需要透過公有網際網路連接到軟體或服務，您可以設定資料庫的公有模式。為確保資料的安全性，我們不建議將公有模式長期啟用。您可以從資料庫管理畫面中隨時變更公有和私有模式。

## 我可以管理 Lightsail 受管資料庫所使用的連接埠嗎？

否，Lightsail 會基於安全性考量自動管理您的連接埠，並在公用模式下為所有 Lightsail 受管理的 SQL 資料庫開啟連接埠 3306。如果您的資料庫處於私人模式，則您的資料庫僅開放給透過內部網路在 Lightsail 帳戶中執行的資源。

## 是否 Lightsail 受管資料庫服務 IPv6？

受管 Lightsail 的資料庫不支援 IPv6。

## 網域

### 我可以使用 Lightsail 網域做什麼？

Lightsail 網域可讓您註冊和管理網站或應用程式的網域。如果您擁有向其他供應商註冊的網域，則可以將這些網域的管理轉移至 Lightsail。您也可以將這些網域指向您的 Lightsail 資源。

### 我可以使用哪些頂層網域 (TLDs)？

Lightsail 使用與 Amazon Route 53 相同的通 TLDs 用。如果您想要註冊地理域，建議使用 Route 53 主控台。您的地理網域在使用 Route 53 註冊之後，就可以在 Lightsail 主控台中使用該網域。如需 [有關](#)

[Lightsail 支援的TLDs詳細資訊](#)，請參閱 [Amazon Route 53 開發人員指南](#)中的可向 [Amazon Route 53 註冊的網域](#)。

## 我可以讓 Lightsail 成為我現有網域的DNS服務嗎？

您可以將您使用其他DNS服務供應商註冊之網域的DNS管理權限轉移至 Lightsail。如需詳細資訊，請參閱[建立DNS區域以管理網域DNS記錄](#)。

## 如何開始在 Lightsail 中註冊網域？

登入 Lightsail 之後，您可以使用 [Lightsail 主控台](#)來建立和管理網域。如需詳細資訊，請參閱[域註冊](#)。

## 什麼時候應該在 Lightsail 和 Route 53 中註冊網域？

例如註冊網域、建立DNS區域，以及將網域的流量路由至 Lightsail 資源等工作，都可以在 Lightsail 中完成。建議您將 Route 53 用於進階任務，例如延長域註冊、轉移域 (包括流量政策) 以及建立私有託管區域。

## 我可以將我的網域轉移到我 Lightsail 嗎？

可以將域轉移至 Route 53。網域轉移完成後，您的網域就可以在 Lightsail 主控台中使用。如需詳細資訊，請參閱[在 Amazon Route 53 中管理 Lightsail 網域](#)。

## 我可以將哪些 Lightsail 資源和網域搭配使用？

在 Lightsail 中註冊網域之後，您可以將網域指向 Lightsail 執行個體、容器、負載平衡器、靜態 IP 或內容分發網路 ( ) CDN。

## 將 Lightsail 資源匯出至 Amazon 彈性運算雲端 (AmazonEC2)

### 什麼是出口到 AmazonEC2 ？

匯出到 Amazon EC2 是一項功能，可讓您在 Amazon EC2 上建立 Lightsail 執行個體的副本。匯出到 Amazon 時EC2，您可以在 Amazon EC2 提供的多種執行個體類型、組態和定價模式中進行挑選，並對您的聯網、儲存和運算環境進行更精細的控制。

### 我為什麼要出口到 AmazonEC2 ？

Lightsail 為您提供了一種簡單的方法，以捆綁式、可預測且低廉的價格執行和擴展各種雲端應用程式。Lightsail 也會自動設定您的雲端環境組態，例如網路和存取管理。

匯出至 Amazon EC2 可讓您在更廣泛的執行個體類型上執行應用程式，包括功CPU率更高的虛擬機器、記憶體和聯網功能，到具有FPGAs和的專業或加速執行個體GPUs。此外，Amazon EC2 執行的自動化管理和設定較少，可讓您更好地控制雲端環境的配置方式，例如VPC。

## 出口到 Amazon 如何EC2工作？

若要開始使用，您需要匯出 Lightsail 執行個體或區塊儲存磁碟的手動快照。接著，使用 Amazon 的客戶EC2可以使用 Amazon 建EC2立精靈或API建立新的 Amazon EC2 執行個體或 Amazon EBS 磁碟區，就像使用現有EC2AMI或磁EBS碟區一樣。此外，Lightsail 也提供引導式 Lightsail 主控台體驗，協助您輕鬆建立新EC2的執行個體。

### Note

cPanel & WHM (CentOS 7) 執行個體的快照不能匯出到 Amazon EC2。

## 如何計費？

使用導出到 Amazon EC2 功能是免費的。將手動快照匯出到 Amazon 後EC2，除了 Lightsail 手動快照外，還需要另外支付 Amazon EC2 映像的費用。您啟動的任何新 Amazon EC2 執行個體也將由 Amazon 計費EC2，包括其 Amazon EBS 儲存磁碟區和資料傳輸。如需新執行個體和資源[EC2定價的詳細資訊](#)，請參閱 [Amazon 定價頁面](#)。繼續在您的 Lightsail 帳戶中執行的 Lightsail 資源將繼續按一般費率計費，直到刪除資源為止。

## 是否可匯出受管資料庫或磁碟快照？

匯出功能可讓您匯出手動 Lightsail 磁碟快照，但目前不支援受管理資料庫的手動快照。您可以從 Amazon EC2 主控台將磁碟快照重新水分為 Amazon 磁碟EBS區或API。

## 我可以匯出哪些資源？

Lightsail 匯出至 Amazon EC2 功能旨在支援將 Linux 和 Windows 執行個體快照匯出到 Amazon EC2。它也支援將區塊儲存磁碟快照匯出至 Amazon EBS。它目前不支援資料庫、容器服務、內容傳遞網路 (CDN) 分發、負載平衡器IPs、靜態和DNS記錄的匯出。此外，Django，Ghost 和 cPanel & WHM 實例的快照目前無法導出到 Amazon EC2。

# 執行個體

## 什麼是執 Lightsail 體？

Lightsail 執行個體是位於中的虛擬私人伺服器 (VPS)。AWS 雲端使用 Lightsail 執行個體來儲存資料、執行程式碼，以及建置 Web 型應用程式或網站。您的執行個體可以透過公用 (網際網路) 和私有 () 網路連線到彼此，以及連線至其他 AWS 資源。VPC您可以直接從 Lightsail 主控台輕鬆建立、管理和連線至執行個體。

## 什麼是 Lightsail 計劃？

Lightsail 計劃也稱為服務包，包括具有固定數量的內存 (RAM) 和計算 ( )，SSD基於存儲 (磁盤 vCPUs) 的虛擬伺服器以及免費的數據傳輸額度。Lightsail 方案也提供靜態IPv4位址和DNS管理功能。Lightsail 方案是按小時隨需收費，因此您只需在使用方案時付費。

## 我可以在執行個體上執行什麼軟體？

Lightsail 提供一系列作業系統和應用程式範本，這些範本會在您建立新的 Lightsail 執行個體時自動安裝這些範本。應用程序模板包括 WordPress, WordPress 多站點, cPanel & WHM PrestaShop, Django 的, Drupal 的, 鬼, 的 Joomla!, Magento 的, 紅礦,LAMP, 尼金克斯 (LEMP)MEAN, 和 Node.js.

您可以使用瀏覽器內SSH或您自己的用SSH戶端，在執行個體上安裝其他軟體。

## 我可以搭配哪些作業系統使 Lightsail？

Lightsail 目前支援 7 個 Linux 或類 Unix 的發行版本：AlmaLinux 作業系統 9、Amazon Linux 2、Amazon Linux 2023、CentOS、Debian、免費BSD、開放和 UbuntuSUSE，以及三個視窗伺服器版本：2016 年、2019 年和 2022。

## 我是否需要攜帶自己的授權才能使用 Lightsail 執行個體？

Lightsail 上所有可用的執行個體藍圖都包含授權，但藍圖除外。cPanel WHM該藍圖包含 15 天試用授權。有關更多信息，請參閱[快速入 cPanel 門指南：WHM在 Amazon Lightsail](#) 上。對於所有其他執行個體藍圖，您不需要攜帶自己的授權 (BYOL)。

## 如何建立執 Lightsail 體？

登入 Lightsail 之後，您可以使用 Lightsail [主控台](#)、命令列介面 (CLI)，或API建立和管理執行個體。

首次登入主控台時，請選擇 Create Instance (建立執行個體)。您可以在建立執行個體頁面選擇執行個體的軟體、位置和名稱。選擇 Create (建立) 後，新的執行個體就會在幾分鐘內自動啟動。

## 執行個 Lightsail 如何執行？

Lightsail 執行個體專 AWS 為網頁伺服器、開發人員環境和小型資料庫使用案例而設計。這類工作負載不會 CPU 經常或一致地使用完整的工作負載，但偶爾需要突破效能。Lightsail 使用高載效能執行個體，可提供基準 CPU 效能，並提供超越基準線的額外功能。這種設計可在需要時提供您所需的效能，同時還可以保護您免受效能震盪的影響，或者在其他環境過度訂閱時常發生的其他常見負面影響。

如果您需要高度可設定的環境和執行個體，並且對於視訊編碼或應用程式等應用 HPC 程式具有一致的高 CPU 效能，我們建議您使用 [Amazon EC2](#)。

## 如何知道我的執行個體高載？

在執行個體的 CPU 使用率指標圖表上，您會看到永續區域和高載區域。您的 Lightsail 執行個體可以在永續區域中無限期地運作，而不會影響您的系統運作。當負載過重時，您的執行個體可能會開始在可高載區域中運作。在高載區域中操作時，您的執行個體會耗用更多 CPU 週期。因此，其只能於有限的時段內在此區域中運作。如需詳細資訊，請參閱 [在 Amazon Lightsail 中檢視執行個體指標](#)。

新增指標警示，以便在執行個體 CPU 使用率從可持續區域跨越爆發區域時收到通知。如需詳細資訊，請參閱 [在 Amazon Lightsail 中建立執行個體指標警示](#)。

## 如何連線至 Lightsail 執行個體？

Lightsail 提供直接從瀏覽器連線到執行個體終端機的一鍵式安全連線，支援 Linux/UNIX 型執行個體的 SSH 存取，以及 Windows 執行個體的存取權。RDP 若要使用一鍵式連線，請啟動執行個體管理畫面，選擇 [Connect 線方式] SSH 或 [Connect 線方式] RDP，就會開啟新的瀏覽器視窗並自動連線至您的執行個體。

如果您偏好使用自己的用戶端連線到 Linux/UNIX 執行個體，Lightsail 會為您執行 SSH 金鑰儲存和管理工作，並提供您在用戶端中使用的安全金鑰。SSH

## 如何備份執行個體？

如果您想要備份資料，可以使用 Lightsail 主控台或 API 建立執行個體的手動快照，或啟用自動快照，讓 Lightsail 為您建立每日快照。如果操作失敗或程式碼部署錯誤，可以稍後使用執行個體快照建立一個全新的執行個體。如需詳細資訊，請參閱 [快照](#)。

## 是否可以升級我的計劃？

是。您可以使用執行個體的快照來建立新的、更大的執行個體。如需詳細資訊，請參閱 [快照](#)。

## 如何將 Lightsail 執行個體連線到我 AWS 帳戶中的其他資源？

您可以使VPC用對等互連，私下將 Lightsail 執行個體連線到 AWS 帳戶中的 Amazon VPC 資源。只要在您的 Lightsail 帳戶頁面上選擇啟用VPC對等互連，Lightsail 就會為您完成工作。啟用VPC對等互連後，您可以使用其私IPs有 AWS 資源VPC來處理預設 Amazon 中的其他資源。在[這裡](#)尋找操作方法。

### Note

請注意，您必須在 AWS 帳戶中VPC設定預設 Amazon，才能與 Lightsail VPC 對等互連。AWS 在 2013 年 12 月之前建立的帳號沒有預設值VPC，因此您需要設定一個帳號。在這裡了解有關設置默認值的更多信VPC息。

## 停用執行個體和刪除執行個體有什麼區別？

停用執行個體時，它將在當前狀態下關閉，而且您隨時可以重新啟動。停止執行個體會釋放其公用位 IPv4 址，因此建議您針對在停止和啟動之後必須保留相同 IP 的執行個體使用靜態IPv4位址。請注意，即使執行個體停止並啟動，連接至執行個體的公開IPv6地址也不會變更。

刪除執行個體時，您是在進行一種破壞性的動作。除非您已經建立執行個體快照，否則所有執行個體資料都將消失，而且無法重新復原。自動快照也會隨執行個體刪除，除非複製為手動快照保留下來。執行個體的公有和私有 IP 地址也將被釋放。如果您在該執行個體上使用靜態IPv4位址，則靜態IPv4位址會分離，但仍保留在您的帳戶中。

## 負載平衡器

### 我可以使用 Lightsail 負載平衡器做什麼？

Lightsail 負載平衡器可讓您建置高可用性的網站和應用程式。Lightsail 負載平衡器可將流量分散到不同可用區域中的執行個體，並將流量指向運作良好的目標執行個體，藉此降低應用程式因執行個體發生問題或資料中心中斷而停機的風險。使用 Lightsail 負載平衡器和多個目標執行個體，您的網站或應用程式也可以因應 Web 流量的增加，並在尖峰載入時間為訪客保持良好的效能。

此外，您可以使用 Lightsail 負載平衡器來協助您建置安全的應用程式並接受HTTPS流量。Lightsail 消除了請求、佈建和維護SSL/TLS憑證的複雜性。內建憑證管理可代您請求並續約憑證，並自動將憑證新增到負載平衡器。

## 是否可以在不同 AWS 區域 或不同可用區域中的執行個體使用負載平衡器？

您無法在不 AWS 區域同的執行個體上使用負載平衡器。不過，負載平衡器可以用於不同可用區域中的目標執行個體。實際上，我們建議您將目標執行個體分散到各個可用區域，最大限度地提高應用程式可用性。

## 我的 Lightsail 負載平衡器如何處理流量尖峰？

Lightsail 負載平衡器會自動擴展以處理應用程式的流量尖峰，而無需手動調整它們。如果您的應用程式發生流量暫時性尖峰，Lightsail 負載平衡器將自動擴展並繼續有效率地將流量導向 Lightsail 執行個體。雖然 Lightsail 負載平衡器專為輕鬆管理流量尖峰而設計，但持續體驗非常高流量級別的應用程式可能會遇到效能降低或節流的情況。如果您希望應用程式持續管理每小時 5 GB 以上的資料，或持續擁有大量連線 (每小時 >400k 個新連線，超過 15k 個作用中的並行連線)，建議您改用 Amazon 搭配應用程式負載平衡。EC2

## Lightsail 負載平衡器如何將流量路由到我的目標執行個體？

Lightsail 負載平衡器會根據循環配置資源演算法，將流量導向運作良好的目標執行個體。

## Lightsail 如何知道我的目標執行個體是否健康？

建立負載平衡器並連接執行個體之後，Lightsail 會傳送健康狀態檢查要求至 Web 應用程式的根目錄。您可以指定 Lightsail 要偵測的路徑 (一般檔案或網頁 URL) 來自訂位置。如果可以使用此路徑到達目標執行個體，則 Lightsail 會將流量路由至該處。如果其中一個目標執行個體沒有回應，健康狀態檢查會失敗，且 Lightsail 不會將流量路由到該執行個體。[進一步了解運作狀態檢查](#)

## 負載平衡器可連接多少個執行個體？

您可以根據需要將任意數量的目標執行個體新增至負載平衡器，最多可達 Lightsail 帳戶執行個體配額。

## 是否可將一個執行個體指派給多個負載平衡器？

是，如有需要，Lightsail 支援將執行個體新增為多個負載平衡器的目標執行個體。

## 刪除負載平衡器時，目標執行個體會發生什麼狀況？

如果您刪除負載平衡器，連接的目標執行個體將繼續正常執行，並在 Lightsail 主控台中顯示為一般 Lightsail 執行個體。請注意，刪除負載平衡器後，您可能需要更新 DNS 記錄，以將流量導向到先前的其中一個目標執行個體。

## 什麼是工作階段持久性？

工作階段持久性讓負載平衡器能夠將訪客的工作階段連結到特定的目標執行個體。這樣能確保該工作階段期間所有的使用者請求都能傳送到相同的目標執行個體。對於需要訪客命中相同目標執行個體以確保資料一致性的應用程式，Lightsail 支援會話持續性。例如，許多需要使用者身分驗證的應用程式可受惠於工作階段持久性。建立負載平衡器之後，可以從負載平衡器管理畫面中，為特定負載平衡器啟用工作階段持久性。如需詳細資訊，請參閱[為負載平衡器啟用工作階段持續性](#)。

## Lightsail 負載平衡器支援哪些類型的連線？

Lightsail 平衡器支援HTTP和HTTPS連線。

## 是否支 Lightsail 負載平衡器？IPv6

在 2021 年 1 月 12 日之後建立的 Lightsail 負載平衡器預設會以雙堆疊模式運作 (也就是說，它們接受透過IPv4和IPv6通訊協定的用戶端流量)。IPv6您可以透過負載平衡器管理頁面的 [網路] 索引標籤上的切換，在此日期之前建立的負載平衡器上啟用。IPv6也可以使用此切換在任何負載平衡器上停用。

## 是否需要IPv6啟用負載平衡器後面的執行個體，才能使用已IPv6啟用的負載平衡器？

沒有 負載平衡器同時接受IPv4和IPv6流量，並在與後端執行個體通訊IPv4時將其無縫轉換為。因此，負載平衡器後面的實例可以是雙堆棧或IPv4僅。

## 手動和自動快照

### 什麼是快照？

快照是執行個體、資料庫或區塊儲存磁碟的 point-in-time 備份。您可以隨時建立資源的快照，也可以在執行個體和磁碟上啟用自動快照，讓 Lightsail 為您建立快照。您可以使用快照做為基準，以建立新資源或備份資料。快照包含還原資源所需的所有資料 (從建立快照的那一刻開始)。當您從快照建立資源以還原資源時，新的資源將開始做為用於建立快照之原始資源的確切複本。

您可以手動拍攝 Lightsail 執行個體、磁碟和資料庫的快照，也可以使用[自動快照](#)指示 Lightsail 自動為執行個體和磁碟建立每日快照。如需詳細資訊，請參閱[快照](#)。

## 什麼是自動快照？

自動快照是一種在 Amazon Lightsail 中安排 Linux/Unix 執行個體每日快照的方式。您可以選擇一天中的某個時間，Lightsail 會在您選擇的時間每天為您自動拍攝快照，並始終保留最新的七個自動快照。啟用快照是免費的，您只需支付快照使用的實際儲存用量費。

## 手動和自動快照有何不同？

自動快照無法標記或直接匯出至 Amazon EC2。不過，您可以複製自動快照，並將其轉換為手動快照。若要將自動快照複製為手動快照，請從自動快照的內容功能表中選擇 Keep (保留)，以將其複製為手動快照。

## 哪些資源支援快照？

您可以為執行個體、資料庫和磁碟建立手動快照。

您可以使用 Lightsail 主控台或 Lightsail 執行個體啟用自動快照，也可以針對僅使用 Lightsail API 或 AWS CLI 的磁碟啟用自動快照。API AWS CLI Windows 執行個體或受管資料庫目前不支援自動快照。

## 快照可以存放多長時間？

手動快照會存放到您選擇刪除為止。如需詳細資訊，請參閱[在 Amazon Lightsail 中刪除快照](#)。

自動快照會一直儲存，直到由較新的自動快照取代為止。Lightsail 會儲存最新的七個自動快照，然後再刪除最舊的快照，並以最新的快照取代。不過，您可以將特定的自動快照複製為手動快照以保留下來。如需詳細資訊，請參閱[在 Amazon Lightsail 中保留執行個體或磁碟的自動快照](#)。您需要針對存放在帳戶中的自動快照支付[快照儲存費用](#)。

## 如何啟用自動快照？

您可以使用 Lightsail 主控台、Lightsail 或建立 Linux 或 Unix 執行個體 AWS CLI 時 API，或稍後在執行個體執行後啟用自動快照。

您也可以在建​​立磁碟時或建立磁碟之後啟用自動快照；不過，您只能使用 Lightsail API 或 AWS CLI。

如需詳細資訊，請參閱[在 Amazon Lightsail 中啟用或停用執行個體或磁碟的自動快照](#)。

## 何時建立自動快照？

當您啟用自動快照時，會根據資源所在的 AWS 區域 設定預設時間。您可以將自動快照變更為您偏好的當日時間 (以每小時增量為單位)。如需詳細資訊，請參閱 [在 Amazon Lightsail 中變更執行個體或磁碟的自動快照時間](#)。

## 可以存放多少個快照？

您可以存放任意數量的手動快照。不過，在由最新快照取代最舊快照之前，只會儲存最新的七個自動快照。

## 快照如何計費？

您只需為 Lightsail 帳戶中儲存的快照付費。Lightsail 快照 (手動和自動) 的儲存費用為每月 0.05 USD USD。

## 如果停用自動快照，是否會遺失快照？

沒有 如果您停用自動快照，Lightsail 將停止建立每日快照，並保留現有的自動快照。當您重新啟用自動快照時，Lightsail 將繼續拍攝每日快照，刪除最舊的快照並將其替換為最新快照。

## 如果不想取代自動快照，該怎麼辦？

您可以將特定的自動快照複製為手動快照以保留下來。如需詳細資訊，請參閱 [在 Amazon Lightsail 中保留執行個體或磁碟的自動快照](#)。

## 是否可以刪除自動快照？

您可以隨時從自動快照內容功能表中選擇 Delete (刪除)，以刪除自動快照。如需詳細資訊，請參閱 [刪除自動執行個體快照](#)。

## 如何使用快照？

快照可做為基準，或在原始資源發生錯誤時建立新資源。如需詳細資訊，請參閱 [快照](#)。

快照也可以匯出到 Amazon，EC2 以在該服務中建立新資源。如需詳細資訊，請參閱 [將快照匯出到 Amazon EC2](#)。

## 資源健康指標和警示

### 什麼是指標？

Lightsail 會報告執行個體、資料庫和負載平衡器的指標資料。部分指標包括執行個體的CPU使用率百分比、輸入和輸出網路流量量、系統和執行個體錯誤計數、資料庫磁碟佇列深度、資料庫可用儲存空間、負載平衡器錯誤計數、負載平衡器回應時間等。指標可讓您監控及維護資源的可靠性、可用性與效能。定期監控並從您的資源收集指標資料，即可更輕鬆地進行多點失敗的偵錯。如需詳細資訊，請參閱[資源指標](#)。

### 什麼是警示？

您可以在 Lightsail 中建立警示，以監視執行個體、資料庫和負載平衡器的指標。您可將警示設定為根據您所指定閾值的相對指標值來通知您。如需詳細資訊，請參閱[警示](#)。

通知可以是 Lightsail 主控台中顯示的橫幅、傳送至您的電子郵件地址的電子郵件，以及傳送至您行動電話號碼的SMS簡訊。如需有關通知的詳細資訊，請參閱[通知](#)。

### 我可以新增多少個警示？

您可以為執行個體、資料庫和負載平衡器可用的每個指標設定兩個警示。如需詳細資訊，請參閱[警示](#)。

## 聯網

### 我要如何使用 IP Lightsail？

每個 Lightsail 執行個體都會自動取得私人IPv4地址、公用IPv4位址或公用IPv6位址 (IPv6必須針對2021年1月12日之前建立的執行個體手動啟用)。您可以免費使用私有 IP 在 Lightsail 執行個體和 AWS 資源之間私下傳輸資料。您可以使用公用 IP 從網際網路連線至執行個體，例如透過已註冊的網域名稱，或透過本機電腦的SSH或RDP連線。您也可以將靜態IPv4位址附加至執行個體，該IPv4位址會以即使執行個體停止並啟動也不會變更的IPv4位址來取代公用位址。IPv6指派給執行個體的位址會保持不變，直到執行個體遭到刪除，或在執行個體IPv6上停用以手動釋放位IPv6址為止。

### Lightsail 是否IPv6僅支援執行個體？

是，Lightsail 執行個體支援雙堆疊 (IPv4和IPv6) 和IPv6僅限設定。

## 什麼是靜態 IP ？

[靜態 IP](#) 是專用於您的 Lightsail 帳戶的固定公用 IP 位址。您可以將靜態IPv4位址指派給執行個體，取代其 public 位址IPv4。如果您決定將自己的執行個體換成另一個，您可以將靜態 IP 重新指派給新的執行個體。如此一來，每次想要取代執行個體時，就不必重新設定任何外部系統 (例如DNS記錄)，就能指向新的 IP 位址。目前 Lightsail IPv4 僅支援靜態IPs。靜態IPv6位址不可用。不過，指派給執行個體的IPv6位址會維持不變，直到執行個體遭到刪除，或在執行個體IPv6上停用以手動釋放位IPv6址為止。

## 我IPs可以將多少個靜態連接到一個實例？

您一次只能將一個靜態 IP 連接到執行個體。

## 什麼是DNS記錄？

DNS是一種全球分佈式服務，可將人類可讀的名稱 ( 例如www.example.com字母數字 IP 地址 ) 轉換為字母數字 IP 地址192.0.2.1，例如計算機用於相互連接。使用 Lightsail，您可以輕鬆地將註冊的網域名稱對應photos.example.com至 Lightsail 執行個體IPs的公開資訊。如此一來，當使用者在瀏覽器中輸example.com入人類可讀的名稱時，Lightsail 會自動將位址轉譯為您要將使用者導向至的執行個體 IP。這些翻譯中的每一個都稱為DNS查詢。

重要的是要知道，若要在 Lightsail 中使用網域，您必須先註冊該網域。您可以使用 [Lightsail](#) 或您偏好的註冊DNS商來註冊網域。

## 是否可以管理執行個體的防火牆設定？

是。您可以使用 Lightsail 防火牆控制執行個體的資料流量。在 Lightsail 主控台中，您可以設定執行個體的哪些連接埠可針對不同類型的流量公開存取的規則。

## 物件儲存和儲存貯體

### 我能用 Lightsail 物件儲存做什麼？

您可以將靜態內容 (例如影像、影片和HTML檔案) 儲存在 Lightsail 物件儲存服務的值區中。您可以將存放在儲存貯體中的物件與您的網站和應用程式搭配使用。只要按幾下滑鼠，Lightsail 物件儲存就能與 Lightsail CDN 發行版本建立關聯，讓您快速輕鬆地將內容交付給全球使用者。該舉措也可作為低成本、安全的備份解決方案。如需詳細資訊，請參閱[物件儲存](#)。

## Lightsail 物件儲存的費用是多少？

Lightsail 物件儲存裝置有三種不同的固定價格套件，可供使用 Lightsail 的所有 AWS 區域產品。第一個搭售套件是每月 1 USD，前 12 個月免費。此搭售套件包含 5 GB 儲存容量和 25 GB 的資料傳輸量。第二個搭售套件是每月 3 USD，包含 100 GB 儲存容量和 250 GB 的資料傳輸量。最後，第三個搭售套件是每月 5 USD，包含 250 GB 的儲存容量和 500 GB 的資料傳輸量。Lightsail 物件儲存包括在儲存貯體中無限的資料傳輸量，因為搭售套件的資料傳輸額度僅用於從儲存貯體中傳出的資料。

## Lightsail 物件儲存是否有超額費用？

當您超過個別儲存貯體的所選儲存計畫之每月儲存容量或資料傳輸額度時，您需支付多出數量的費用。如需詳細資訊，請參閱 [Lightsail 定價頁面](#)。

## 資料傳輸額度如何與物件儲存搭配使用？

您可以透過將資料傳入和傳出 Lightsail 物件儲存體來消耗資料傳輸額度，但下列情況除外。

- 從網際網路傳輸至 Lightsail 物件儲存空間的資料
- Lightsail 物件儲存資源之間的資料傳輸
- 資料從 Lightsail 物件儲存區傳出至相同的另一個 Lightsail 資源 AWS 區域 (包括至不同 AWS 帳戶中的資源，但相同) AWS 區域
- 從 Lightsail 物件儲存空間傳出至 Lightsail 發行版本的資料 CDN

## 我是否可以變更與 Lightsail 儲存貯體相關的計畫？

是，您可以在每月計 AWS 費週期內一次變更個別 Lightsail 儲存貯體的儲存空間計畫。

## 我是否可以將物件從 Lightsail 物件儲存複製到 Amazon S3？

可以，系統支援從 Lightsail 物件儲存到 Amazon S3 的複製。如需詳細資訊，請參閱《AWS Premium Support 知識中心》中的 [如何將一個 Amazon S3 儲存貯體中的所有物件複製到另一個儲存貯體？](#)。

## 如何開始使用 Lightsail 物件儲存？

若要使用 Lightsail 物件儲存，您必須先建立用於存放資料的儲存貯體。如需詳細資訊，請參閱 [建立儲存貯體](#)。儲存貯體啟動並運行後，您就可以透過使用 Lightsail 主控台上傳檔案，或透過設定應用程式

式，將日誌或其他應用程式資料等內容放入儲存貯體中，開始將物件新增至儲存貯體中。或者，您也可以透過使用 AWS Command Line Interface (AWS CLI) 開始使用 Lightsail 物件儲存。

## 如何將物件上傳到儲存貯體？

若要將物件上傳至儲存貯體 (例如影像或其他靜態檔案)，請從 Objects (物件) 頂端導覽索引標籤中選擇 Upload (上傳)，然後從電腦中選取正確的檔案或目錄。或者，將檔案和目錄從桌面拖放到 Lightsail 物件儲存主控台內的標記區域。

## 我是否可以封鎖對儲存貯體的公有存取？

Lightsail 儲存貯體和物件預設設定為私有，這意味著只有具有適當許可的使用者才能存取儲存貯體和物件。使用者可以變更此預設設定，並在私有儲存貯體中將個別物件設為公有且唯讀，或是選擇將整個儲存貯體設為公有且唯讀。當使用者將儲存貯體或物件設為公有時，世界上任何人都可以讀取其內容。如需詳細資訊，請參閱[儲存貯體許可](#)。

## 如何提供對儲存貯體的程式設計存取？

您可以使用存取金鑰或角色提供對儲存貯體的程式設計存取。首先，在 Lightsail 主控台中選取要以程式設計方式連接的儲存貯體。其次，在「權限」索引標籤下，建立存取金鑰或指派角色給 Lightsail 執行個體，然後設定您的網站或應用程式程式碼以使用值區。根據您計劃將物件儲存與網站或應用程式搭配使用的方式，此行為可能會有所不同。如需詳細資訊，請參閱[儲存貯體許可](#)。

## 如何與其他 AWS 帳戶共用儲存貯體？

Lightsail 允許您使用在值區管理頁面的「跨帳戶存取」區段中指定的 AWS 帳戶 ID 共用儲存貯體的存取權，讓跨帳戶共用變得更容易。指定 AWS 帳戶 ID 後，該帳戶將擁有值區的唯讀存取權。如需詳細資訊，請參閱[儲存貯體許可](#)。

## 什麼是版本控制？

版本控制允許您保留、擷取和恢復在儲存貯體中每個物件儲存的每個版本，從而提供額外的保護層級，避免意外覆寫和刪除。如需詳細資訊，請參閱[啟用和暫停儲存貯體物件版本控制](#)。

## 如何將我的 Lightsail 儲存貯體與我的發 Lightsail CDN 版本相關聯？

只要按幾下滑鼠，就能將 Lightsail 物件儲存與 Lightsail CDN 發行版產生關聯，讓您快速輕鬆地將內容交付給全球使用者。若要這麼做，請建立 Lightsail CDN 發行版本，然後只要選取 Lightsail 儲存貯體做為 Lightsail 發行版本的來源即可。CDN 如需詳細資訊，請參閱[使用具有 Lightsail 內容交付網路分發的 Amazon Lightsail 儲存貯體](#)。

## Lightsail 物件儲存服務有什麼限制？

您可以在 Lightsail 物件儲存服務中為每個帳戶建立最多 20 個儲存貯體。您可以在儲存貯體中儲存的物件數量沒有限制。您可以將所有物件存放在單一儲存貯體，或者可以整理到多個不同的儲存貯體中。

## Lightsail 物件儲存是否支援監控和提醒？

透過 Lightsail 物件儲存，客戶可以輕鬆檢視儲存貯體內所用空間總計以及儲存貯體內物件數目的指標。系統也支援以這些指標為基礎的提醒。如需詳細資訊，請參閱在 [Amazon Lightsail 中檢視儲存貯體的指標](#) 和 [建立儲存貯體指標警示](#)。

## Lightsail 中的標籤

### 什麼是標籤？

標籤是您指派給 Lightsail 資源的標籤。每個標記皆包含由您定義的索引鍵和值。標籤值是選擇性的，因此您可以選擇建立「僅限金鑰」標籤，以便在 Lightsail 主控台中篩選資源。

### 如何在 Lightsail 中使用標籤？

使用標籤，您可以在 Lightsail 主控台中分組和篩選資源 API，以及追蹤和整理帳單中的成本，以及透過存取管理規則管理誰可以查看或修改您的資源。您可以透過標記資源來執行以下動作：

- 整理 — 使用 Lightsail 主控台和 API 篩選器，根據您指派的標籤來檢視和管理資源。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。
- 成本分配 — 通過標記您的資源並在計費控制台中創建「成本分配標籤」來跟踪和分配不同項目或用戶的成本。例如，您可以將帳單拆開並依專案或用戶端了解成本。
- 管理存取權 — 使用 AWS Identity and Access Management 政策控制具有 AWS 帳戶存取權的使用者如何編輯、建立和刪除 Lightsail 資源。這可讓您更輕鬆地與其他人共同作業，而無需授予他們對 Lightsail 資源的完整存取權。

如需有關在 Lightsail 中使用標籤的詳細資訊，請參閱 [標籤](#)。

### 可以標記哪些資源？

Lightsail 目前支援下列資源的標記功能：

- 執行個體 (Linux 和視窗)

- 容器服務
- 區塊儲存磁碟
- 負載平衡器
- 資料庫
- DNS區域
- 執行個體、磁碟和資料庫的手動快照

手動快照支援標籤；不過，您必須使用 Lightsail API 或標 AWS CLI 記快照。如果您使用 Lightsail 主控台建立已標記執行個體、磁碟或資料庫的手動快照，手動快照會自動提供與來源資源相同的標記。當您使用 Lightsail 主控台從標籤化的手動快照建立新資源時，您可以編輯這些標籤。

自動快照無法加上標籤。

## 如何標記我的 Lightsail 照？

Lightsail 主控台會使用與其來源資源相同的標籤，自動標記手動快照。如果您使用 Lightsail API 或建 AWS CLI 立快照，您可以自行選擇快照的標籤。

### Important

帳單報告 (成本分配標籤) 目前不包含資料庫手動快照的標籤。

## 鍵值標籤和僅索引鍵標籤有何不同？

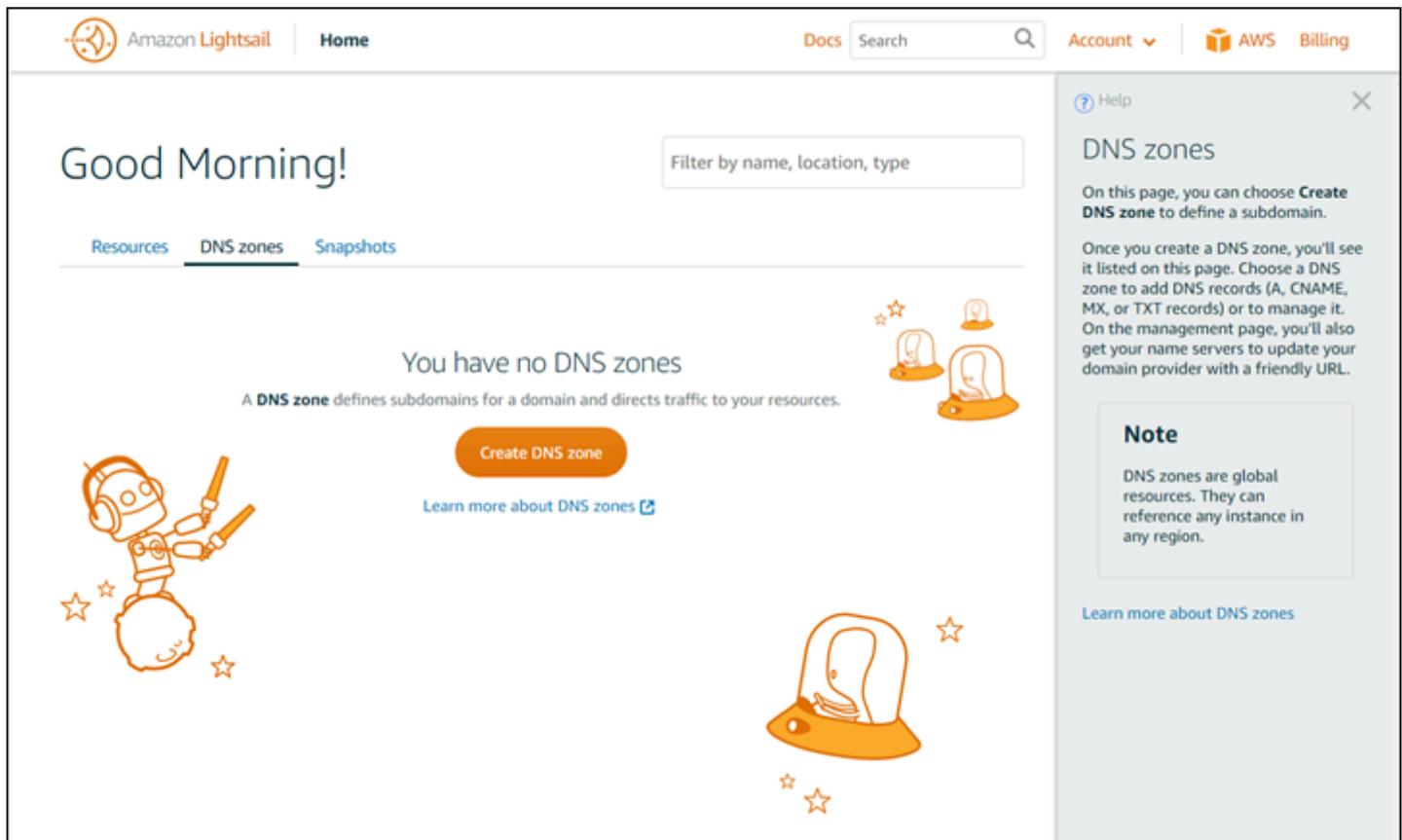
Lightsail 標籤是索引鍵值配對，可讓您組織不同類別的資源，例如執行個體 (例如專案：部落格、專案：遊戲、專案：測試)。這可讓您完全控制資源組織、帳單報告和存取管理之類的所有使用案例。Lightsail 主控台也可讓您使用僅限金鑰的標籤來標記資源，以便在主控台中快速篩選。

# 尋找有關 Lightsail 的實用資源

在 Amazon Lightsail 中，您可以通過多種方式找到幫助。

## 即時線上說明面板

Lightsail 在主控台的每個頁面上都有與內容相關的「說明」面板，其中包含您所在頁面專屬的其他提示和資訊。如果您對於頁面有任何問題，皆可隨時開啟說明面板，並在解決問題之後予以關閉。您可以在任何頁面選擇 Help (說明) 面板或選擇使用者界面中的任何小問號，以開啟說明面板。



The screenshot shows the Amazon Lightsail console interface. At the top, there's a navigation bar with the Amazon Lightsail logo, 'Home', 'Docs', a search bar, 'Account', 'AWS', and 'Billing'. The main content area is titled 'Good Morning!' and 'You have no DNS zones'. Below this, there's a 'Create DNS zone' button and a link to 'Learn more about DNS zones'. A 'Help' panel is open on the right, titled 'DNS zones', with a close button (X). The panel contains the following text: 'On this page, you can choose **Create DNS zone** to define a subdomain. Once you create a DNS zone, you'll see it listed on this page. Choose a DNS zone to add DNS records (A, CNAME, MX, or TXT records) or to manage it. On the management page, you'll also get your name servers to update your domain provider with a friendly URL.' Below this is a 'Note' section: 'DNS zones are global resources. They can reference any instance in any region.' At the bottom of the panel is a link: 'Learn more about DNS zones'.

## 關於使用者指南

Amazon Lightsail 使用者指南包含如何主題和概念概觀，可協助您在 Lightsail 中工作。例如，您可以 [建立一個執行個體](#)、[連接到您的執行個體](#)，或 [管理您的網域](#)。

## 使用搜尋

您可以使用每頁頂端的搜尋方塊，從 Lightsail 的任何頁面搜尋文件主題。為了更精確地進行搜尋，您可以從文件搜尋頁面再次進行搜尋。

沒有找到所需的資訊嗎？請傳送意見給我們，我們將設法改善。在 Lightsail 的每個頁面上，您都可以選擇 [提供意見反應] 並提交意見反應以提出建議。

## 使用 Lightsail CLI 和 API

您可以使用 AWS Command Line Interface (AWS CLI) 或 Lightsail REST API 來建立、讀取、更新及刪除 Lightsail 資源。除了 REST API，我們也有一個 SDK 在多種語言，包括 Java、紅寶石、JavaScript (Node.js)、圍棋 PHP、Python、.NET (C#) 和 C++。如需有關 Lightsail 的詳細資訊 API，請參閱 [Lightsail API 參考資料](#)。

### Note

您需要產生存取金鑰才能使用 Lightsail API。進一步瞭解如何設定存取鍵以使用 [Lightsail API](#)。

當您使用 AWS CLI 用 Lightsail 資源時，此功能會很有幫助。在中 AWS CLI，只輸入 `aws lightsail help` 即可瞭解可用的命令。如需特定 CLI 指令的說明，請輸入指令名稱，然後輸入命令名稱，`help` 以深入瞭解其參數和例外狀況。如需詳細資訊，請參閱 [Lightsail CLI 參考資料](#)。

## AWS 論壇和其他社群資源

您也可以在我们的 AWS 討論區中張貼您的問題：[AWS 論壇](#)。

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。