



管理指南

Amazon Redshift



Amazon Redshift: 管理指南

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 Amazon Redshift ?	1
您第一次使用 Amazon Redshift 嗎?	1
Amazon Redshift Serverless 功能概觀	2
Amazon Redshift 佈建叢集概觀	4
叢集管理	4
叢集存取和安全	5
監控叢集	6
資料庫	7
將 Amazon Redshift Serverless 與 Amazon Redshift 佈建資料倉儲進行比較	7
使用已佈建叢集的 Amazon Redshift 管理界面	25
使用 AWS 軟體開發套件	26
簽署 HTTP 請求	27
設定 Amazon Redshift CLI	31
Amazon Redshift Serverless	33
什麼是 Amazon Redshift Serverless ?	33
Amazon Redshift Serverless 主控台	33
使用 Amazon Redshift Serverless 時的考量	36
Amazon Redshift Serverless 的運算容量	39
了解 Amazon Redshift Serverless 容量	39
AI 驅動的擴展和最佳化 (預覽)	39
Amazon Redshift Serverless 的帳單	41
定價	41
運算容量的帳單	41
儲存的帳單	45
使用 Amazon Redshift Serverless 免費試用	45
帳單用量注意事項	45
連線至 Amazon Redshift Serverless	47
連線至 Amazon Redshift Serverless	47
透過 JDBC 驅動程式連線至 Amazon Redshift Serverless	47
使用資料 API 連線至 Amazon Redshift Serverless	49
使用 SSL 連線到 Amazon Redshift Serverless	49
從 Amazon Redshift 受管 VPC 端點連線至 Amazon Redshift Serverless	51
從其他帳戶或區域中的 Redshift VPC 端點連線至 Amazon Redshift Serverless	52
為 Amazon Redshift Serverless 設定適當的網路流量設定	56

在 Amazon Redshift Serverless 中定義要向聯合身分使用者授予的資料庫角色	56
其他資源	56
在 Amazon Redshift Serverless 中定義要向聯合身分使用者授予的資料庫角色	57
Amazon Redshift Serverless 中的身分和存取管理	59
授予許可給 Amazon Redshift Serverless	59
Amazon Redshift IAM 憑證入門	61
使用資料庫角色許可管理對 Amazon Redshift Serverless 資料庫物件的存取	62
將佈建的叢集遷移至 Amazon Redshift Serverless	63
建立已佈建叢集的快照	63
使用驅動程式連線至 Amazon Redshift Serverless	64
使用 Amazon Redshift Serverless SDK	66
Amazon Redshift Serverless 工作群組和命名空間的概觀	67
Amazon Redshift Serverless 工作群組和命名空間的概觀	67
使用主控台管理 Amazon Redshift Serverless	69
第一次設定 Amazon Redshift Serverless	69
使用工作群組	69
使用命名空間	73
管理用量限制、查詢限制及其他管理任務	76
使用 Amazon Redshift Serverless 監控查詢和工作負載	78
使用 Amazon Redshift Serverless 監控查詢和工作負載	78
Amazon Redshift Serverless 的稽核記錄	82
匯出日誌	82
使用快照和復原點	89
快照	90
復原點	92
排程快照	93
將備份複寫到另一個 AWS 區域	95
還原資料表	97
使用 AWS Command Line Interface 和 Amazon Redshift Serverless API	97
Amazon Redshift Serverless 中的資料共用	99
Amazon Redshift Serverless 中的資料共用	100
標記資源概觀	101
Amazon Redshift 佈建叢集	103
Amazon Redshift 概述	103
叢集和節點	103
在建立叢集時使用 EC2-VPC	108

EC2-VPC	109
預設磁碟空間警示	109
叢集狀態	110
使用 Amazon Redshift 佈建叢集的注意事項	111
區域與可用區域的考量	112
叢集維護	112
管理用量限制	117
RA3 節點支援的聯網功能	119
節點類型	120
叢集作業	125
調整叢集大小	125
暫停和繼續叢集	138
重新命名叢集	139
關閉及刪除叢集	140
重新定位叢集	141
快照和備份	145
設定多可用區部署	168
設定多可用區部署	168
管理多可用區部署	170
容錯移轉多可用區部署	177
多可用區的查詢監控	178
使用主控台管理叢集	180
建立叢集	181
建立預覽叢集	184
修改叢集	185
刪除叢集	186
重新啟動叢集	187
調整叢集大小	187
升級叢集的發行版本	188
取得叢集組態資訊	188
取得叢集狀態概觀	189
建立叢集快照	189
建立或編輯磁碟空間警示	189
使用叢集效能資料	190
使用 AWS CLI 和 Amazon Redshift API 管理叢集	190
管理 VPC 中的叢集	191

概觀	191
在 VPC 中建立叢集	193
管理叢集的 VPC 安全群組	194
設 Amazon Redshift 叢集或 Amazon Redshift Serverless 工作群組的安全群組通訊設定	195
Amazon Redshift 如何使用 VPC 共享資源 AWS	198
叢集子網路群組	199
叢集版本歷史記錄	201
使用零 ETL 整合	202
考量事項	204
開始使用零 ETL 整合	205
建立和設定目標 Amazon Redshift 資料倉儲	206
開啟區分大小寫功能	208
在 Amazon Redshift 中設定授權	209
後續步驟	213
建立目的地資料庫	213
在 Amazon Redshift 中建立目的地資料庫	213
新增資料至來源	215
以複寫的資料查詢和建立具體化視觀表	215
在 Amazon Redshift 中查詢複寫的資料	215
以複寫的資料建立具體化視觀表	216
管理零 ETL 整合	217
在 Amazon Redshift 中共用資料	219
零 ETL 整合的指標	220
對零 ETL 整合進行疑難排解	221
查詢資料庫	230
連線至 Amazon Redshift	230
使用 Amazon Redshift 查詢編輯器 v2 來查詢資料庫	231
配置您的 AWS 帳戶	232
使用查詢編輯器 v2	238
與查詢編輯器 v2 生成式 SQL 互動 (預覽)	253
將資料載入到資料庫	260
編寫和執行查詢	268
編寫和執行筆記本	273
查詢 AWS Glue Data Catalog	276
查詢資料湖	279
使用資料共用	281

排程查詢	284
將結果視覺化	293
以團隊的形式協作和共用	299
使用查詢編輯器來查詢資料庫	301
考量事項	302
啟用存取	302
使用查詢編輯器來連線	304
使用查詢編輯器	305
排程查詢	306
使用 SQL 用戶端工具連線至資料倉儲	311
連接用戶端工具的建議	311
在 Amazon Redshift 中設定連線	312
設定連線的安全選項	467
從用戶端工具和程式碼連線	475
使用 SQL Workbench/J 進行連線	519
以程式設計方式 Connect 到資料倉	520
使用身分驗證設定檔連線至 Amazon Redshift	520
針對 Amazon Redshift 中的連線問題進行疑難排解	523
使用資料 API	530
使用資料 API	530
呼叫資料 API 時的考量	531
執行含有等冪性字符的 SQL 陳述式	535
授權存取	537
呼叫資料 API	543
針對資料 API 問題進行故障診斷	567
使用 Amazon 排程資料 API 作業 EventBridge	567
監控資料 API	571
參數群組	574
概觀	574
關於參數群組	574
預設參數值	575
使用配置參數值 AWS CLI	576
設定工作負載管理	578
WLM 動態和靜態屬性	578
wlm_json_configuration 參數的屬性	578
使用以下方法配置 wlm_json_組態參數 AWS CLI	584

使用主控台來管理參數群組	592
建立參數群組	592
修改參數群組	592
使用主控台建立或更新查詢監控規則	595
刪除參數群組	596
將參數群組與叢集產生關聯	597
使用 AWS CLI 和 Amazon Redshift API 管理參數群組	597
與合 AWS 作夥伴整合	598
使用 Amazon Redshift 主控台與合 AWS 作夥伴整合	598
載入 AWS 合作夥伴的資料	599
購買預留節點	601
概觀	601
關於預留節點方案	601
比較預留節點方案間的定價	602
預留節點運作的方式	603
預留節點和合併帳單	603
預留節點範例	604
使用主控台購買預留節點優惠	605
升級保留節點 AWS CLI	606
使用 AWS CLI 和 Amazon Redshift API 購買預留節點方案	607
安全	609
資料保護	610
資料加密	611
資料字符化	625
網際網路流量隱私權	626
身分與存取管理	626
使用身分驗證	627
存取控制	629
管理存取概觀	630
使用以身分為基礎的政策 (IAM 政策)	635
Amazon Redshift 的原生身分提供者 (IdP) 聯合	685
將 Redshift 與 IAM Identity Center 連線，為使用者提供單一登入體驗	689
使用服務連結角色	703
使用 IAM 身分驗證產生資料庫使用者憑證	709
授權 Amazon Redshift 訪問服務 AWS	758
使用管理 Amazon Redshift 管理員密碼 AWS Secrets Manager	789

AWS Secrets Manager 整合所需的權限	790
輪換管理員密碼機密	791
在 Amazon Redshift 中擷取機密的 Amazon Resource Name (ARN)	791
建立資料庫連線認證的密碼	792
使用 Amazon Redshift AWS Secrets Manager 的注意事項	794
記錄和監控	795
資料庫稽核記錄日誌	795
使用記錄 CloudTrail	806
合規驗證	817
復原能力	818
基礎設施安全性	819
網路隔離	626
安全群組	820
使用界面 VPC 端點連線至 Amazon Redshift	820
組態與漏洞分析	826
網路工作	827
使用自訂網域名稱來進行用戶端連線	827
自訂網域名稱的安全	827
設定自訂網域名稱	828
使用 Redshift 管理的 VPC 端點	834
考量事項	835
使用 Redshift 主控台管理端點	836
使用管理 AWS CLI	837
使用 Amazon Redshift API 操作來進行管理	838
管理使用 AWS CloudFormation	838
增強型 VPC 路由	838
使用 VPC 端點	840
增強型 VPC 路由	841
Redshift Spectrum 和增強型 VPC 路由	842
監控叢集效能	847
概觀	847
效能資料	848
Amazon Redshift 指標	848
Amazon Redshift 指標的維度	857
Amazon Redshift 查詢和載入效能資料	859
使用效能資料	860

檢視叢集效能資料	861
檢視查詢歷史記錄資料	869
檢視資料庫效能資料	873
檢視工作負載並行和並行擴展資料	875
檢視查詢和載入	878
檢視載入操作期間的叢集指標	882
分析工作負載效能	882
管理警示	884
在 CloudWatch 主控台中使用效能指標	885
事件	887
叢集事件概觀	887
使用 Amazon Simple Notification Service	888
訂閱 Amazon Redshift 叢集事件通知	888
使用主控台檢視叢集事件	890
使用 AWS CLI 和 Amazon Redshift API 查看叢集事件	890
管理叢集事件通知	890
使用 Amazon Redshift 主控台管理叢集事件通知	891
使用 AWS CLI 和 Amazon Redshift API 管理叢集事件通知	891
Amazon Redshift 事件通知	892
Amazon Redshift 事件類別和事件訊息	892
Amazon Redshift 馬 Amazon 無服務器事件通知 EventBridge	907
透過 Amazon 進行零 ETL 整合事件通知 EventBridge	912
配額和限制	918
Amazon Redshift 物件的配額	918
Amazon Redshift Serverless 物件的配額	922
Amazon Redshift Data API 的配額	924
查詢編輯器 v2 物件的配額	925
Amazon Redshift Spectrum 物件的配額和限制	927
命名限制條件	928
標記	931
標記概觀	931
標記需求	932
使用主控台管理資源標籤	932
使用 Amazon Redshift API 來管理標籤	933
叢集版本	934
修補程式	934

新功能	935
修補程式 180	936
新功能	937
修補程式 179	937
新功能	938
修補程式 178	939
新功能	940
修補程式 177	942
新功能	942
修補程式 176	943
新功能	944
修補程式 175	945
新功能	945
修補程式 174	946
此版本的新功能	946
此版本的新功能	946
此版本的新功能	946
此版本的新功能	946
此版本的新功能	946
此版本的新功能	946
此版本的新功能	946
修補程式 173	947
此版本的新功能	947
此版本的新功能	947
此版本的新功能	947
此版本的新功能	947
此版本的新功能	947
此版本的新功能	947
此版本的新功能	947
此版本的新功能	947
此版本的新功能	947
此版本的新功能	947
修補程式 172	948
新功能	949
修補程式 171	949
新功能	950

修補程式 170	950
新功能	950
修補程式 169	950
新功能	950
修補程式 168	951
新功能	951
程式碼範例	952
動作	955
CreateCluster	955
CreateTable	962
DeleteCluster	965
DescribeClusters	969
DescribeStatement	976
GetStatementResult	978
Insert	980
ModifyCluster	982
Query	987
案例	989
開始使用 Amazon Redshift	989
跨服務範例	1015
建立用於追蹤 Amazon Redshift 資料的 Web 應用程式	1016
文件歷史紀錄	1017
.....	mxxxvii

什麼是 Amazon Redshift ？

歡迎使用《Amazon Redshift 管理指南》。Amazon Redshift 是一種在雲端中完全受管的 PB 級資料倉儲服務。Amazon Redshift Serverless 可讓您在沒有所佈建資料倉儲的所有組態的情況下，存取和分析資料。系統會自動佈建資源，並有智慧地擴展資料倉儲容量，即使是最嚴苛且無法預測的工作負載，也能為其提供快速的效能。資料倉儲閒置時不會產生費用，因此只需按實際用量支付費用。您可以在 Amazon Redshift 查詢編輯器 v2 或您最愛的商業智慧 (BI) 工具中立即載入資料並開始查詢。在零管理環境中享受最優惠的價格效能和熟悉的 SQL 功能。 easy-to-use

無論資料集大小為何，Amazon Redshift 都能使用您目前所用的相同 SQL 工具和商業智慧應用程式，提供快速的查詢效能。

您第一次使用 Amazon Redshift 嗎？

如果您是第一次使用 Amazon Redshift，建議您從閱讀下列章節開始：

- [服務特色和定價](#) — 此產品詳細資訊頁面提供 Amazon Redshift 的價值主張、服務特色和定價。
- [開始使用 Amazon Redshift Serverless](#) — 本主題會引導您完成設定無伺服器資料倉儲、建立資源和查詢範例資料的程序。
- [Amazon Redshift 資料庫開發人員指南](#) — 若您是資料庫開發人員，此指南會說明如何設計、建置、查詢和維護組成資料倉儲的資料庫。

如果您偏好手動管理 Amazon Redshift 資源，則可以針對資料查詢需求建立佈建叢集。如需詳細資訊，請參閱 [Amazon Redshift 叢集](#)。

身為應用程式開發人員，您可以使用 Amazon Redshift API 或 AWS 軟體開發套件 (SDK) 程式庫，以程式設計方式管理叢集。如果您使用 Amazon Redshift API，則必須透過簽署對 API 的每個 HTTP 或 HTTPS 請求進行驗證。如需簽署請求的相關資訊，請前往[簽署 HTTP 請求](#)。

如需 API、CLI 和 SDK 的資訊，請前往下列連結：

- [Amazon Redshift Serverless API 參考](#)
- [Amazon Redshift API 參考](#)
- [Amazon Redshift 資料 API API 參考](#)
- [AWS CLI 指令參考](#)
- [Amazon Web Services 的工具](#) 中的軟體開發套件參考。

Amazon Redshift Serverless 功能概觀

Amazon Redshift 佈建資料倉儲所支援的大部分功能也受到 Amazon Redshift Serverless 支援。以下是它的一些重要功能。

功能	描述
快照	您可以將 Amazon Redshift Serverless 或佈建資料倉儲的快照還原到 Amazon Redshift Serverless。如需詳細資訊，請參閱 使用快照和復原點 。
復原點	Amazon Redshift Serverless 會每 30 分鐘自動建立一個復原點。這些復原點會保留 24 小時。您可以在發生意外寫入或刪除後使用它們來進行還原。當您從復原點還原時，Amazon Redshift Serverless 資料庫中的所有資料都會還原到較早的時間點。如果您需要延長復原點的保留期間，則也可以從復原點建立快照。如需詳細資訊，請參閱 使用快照和復原點 。
基本 RPU 容量	您能以 Redshift 處理單元 (RPU) 為單位來設定基本容量。一個 RPU 可提供 16 GB 的記憶體。此設定可讓您控制使用中資源與工作負載成本之間的平衡。您可以增加此值以增加可用資源並改善查詢效能，或降低此值以限制支出。預設值是 128 個 RPU。您也可以設定用量限制 (例如每天使用的 RPU) 以控制成本。如需詳細資訊，請參閱 Amazon Redshift Serverless 的帳單 。
資料共用的用量限制	您可以使用主控台或 API 來限制從生產者區域傳輸到取用者區域的資料量。這些資料傳輸成本會有所不同 AWS 區域，且以 TB 為單位。如需資料共用的相關資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的 開始使用主控台來進行資料共用 。
使用者定義的函數 (UDF)	您可以在 Amazon Redshift Serverless 中執行使用者定義的函數 (UDF)。如需詳細資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的 建立使用者定義的函數 。
預存程序	您可以在 Amazon Redshift Serverless 中執行預存程序。如需詳細資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的 建立預存程序 。
具體化視觀表	您可以在 Amazon Redshift Serverless 中建立具體化視觀表。如需詳細資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的 建立具體化視觀表 。

功能	描述
空間函數	您可以在 Amazon Redshift Serverless 中執行空間函數。如需詳細資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的 查詢空間資料 。
聯合查詢	您可以從亞馬遜無伺服器執行查詢，以將資料與 Aurora 資料庫叢集和 Amazon RDS 資料庫連結。如需詳細資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的 使用聯合查詢來查詢資料 。
資料湖查詢	您可以執行查詢，將來自 Amazon S3 資料湖的資料與 Amazon Redshift Serverless 連結。如需詳細資訊，請參閱《Amazon Redshift 管理指南》中的 查詢資料湖 。
HyperLog日誌	您可以在亞馬遜無伺服器中執行 HyperLogLog 函數。如需詳細資訊，請參閱 Amazon Redshift 資料庫開發人員指南中的使用 HyperLogLog草圖 。
跨資料庫查詢資料	您可以使用 Amazon Redshift Serverless 來跨資料庫查詢資料。如需詳細資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的 跨資料庫查詢資料 。
資料共用	您可以使用 Amazon Redshift Serverless 存取所佈建資料倉儲上的資料共用。如需詳細資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的 跨叢集共用資料 。
半結構化資料查詢	您可以使用 Amazon Redshift Serverless 擷取和儲存 SUPER 資料類型的半結構化資料。如需詳細資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的 擷取和查詢半結構化資料 。
標記資源	您可以使用 AWS CLI 或 Amazon Redshift 無伺服器 API 來標記包含與資源相關的中繼資料的資源。如需詳細資訊，請參閱 標記資源 。
機器學習	您可以將 Amazon Redshift 機器學習與 Amazon Redshift Serverless 搭配使用。如需詳細資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的 使用機器學習 。
SQL 命令和函數	除了一些例外狀況 (例如 REBOOT_CLUSTER)，您可以將 Amazon Redshift SQL 命令和函數與 Amazon Redshift Serverless 搭配使用。如需詳細資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的 SQL 參考 。

功能	描述
CloudFormation 資源	您可以使用 CloudFormation 範本部署和更新 Amazon Redshift 無伺服器資源。這項整合意味著您可以減少管理資源的時間，並專注於應用程式。如需有關 Amazon Redshift 無伺服器 CloudFormation 資源的詳細資訊，請參閱 Amazon Redshift 無伺服器資源類型參考 。
CloudTrail 資源	Amazon Redshift 無伺服器已與整合，AWS CloudTrail 以提供在 Amazon Redshift 無伺服器中採取的動作記錄。CloudTrail 擷取 Amazon Redshift 無伺服器的所有 API 呼叫作為事件。如需詳細資訊，請參閱 CloudTrail 亞馬遜無伺服器相關資訊 。

Amazon Redshift 佈建叢集概觀

Amazon Redshift 服務會管理設定、操作和擴展資料倉儲的所有工作。這些工作包括佈建容量、監控和備份叢集，以及對 Amazon Redshift 引擎套用修補程式和升級。

以下影片說明如何使用 Amazon Redshift 查詢編輯器 v2 建立叢集和查詢資料。

叢集管理

Amazon Redshift 叢集是一組節點，其中包含一個領導者節點和一或多個運算節點。您需要的運算節點的類型和數量取決於您的資料的大小、將執行的查詢數量，以及您需要的查詢執行時間效能。

建立和管理叢集

取決於您的資料資料倉儲需求，您可以從小型的單一節點叢集開始，並隨著您的需求變更，輕鬆向上擴展至更大型的多節點叢集。您可以對叢集新增或移除運算節點而不會中斷服務。如需詳細資訊，請參閱 [Amazon Redshift 佈建叢集](#)。

預留運算節點

如果想要讓叢集執行一年以上，可以透過預留一年或三年期間的運算節點來節省金錢。相較於隨需佈建運算節點時的每小時費率，預留運算節點可大幅節省成本。如需詳細資訊，請參閱 [購買 Amazon Redshift 預留節點](#)。

建立叢集快照

快照是叢集的 point-in-time 備份。有兩種類型的快照：自動和手動。Amazon Redshift 會透過使用加密的 Secure Sockets Layer (SSL) 連線，將這些快照儲存在 Amazon Simple Storage Service (Amazon S3) 內部。如果您必須從快照還原，Amazon Redshift 會建立新的叢集並從您指定的快照匯入資料。如需快照的相關資訊，請參閱 [Amazon Redshift 快照和備份](#)。

叢集存取和安全

有數個功能與 Amazon Redshift 中的叢集存取和安全性相關。這些功能有助於控制對您的叢集的存取、定義連線規則，以及加密資料與連線。這些是 Amazon Redshift 中的資料庫存取和安全性相關功能以外的功能。如需資料庫安全的相關資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的 [管理資料庫安全](#)。

AWS 帳戶和 IAM 登入資料

根據預設，只有建立叢集的 AWS 帳戶才能存取 Amazon Redshift 叢集。叢集會遭鎖定以防止他人存取。在您的 AWS 帳戶中，您可以使用 AWS Identity and Access Management (IAM) 服務建立使用者帳戶並管理這些帳戶的許可，以控制叢集作業。如需詳細資訊，請參閱 [Amazon Redshift 中的安全](#)。如需如何管理 IAM 身分的相關資訊 (包括 IAM 角色的指引和最佳實務)，請參閱 [Amazon Redshift 中的身分和存取管理](#)。

安全群組

根據預設，您建立的叢集會對所有人關閉。IAM 憑證只能控制對 Amazon Redshift API 相關資源的存取：Amazon Redshift 主控台、命令列介面 (CLI)、API 和 SDK。若要啟用透過 JDBC 或 ODBC 從 SQL 用戶端工具對叢集的存取，您可以使用安全群組：

- 如果對您的 Amazon Redshift 叢集使用 EC2-VPC 平台，您必須使用 VPC 安全群組。建議您在 EC2-VPC 平台中啟動叢集。

叢集若已搭配 EC2-Classic 完成啟動，則您無法將該叢集移動至 VPC。不過，您可以使用 Amazon Redshift 主控台將 EC2-Classic 快照還原至 EC2-VPC 叢集。如需詳細資訊，請參閱 [從快照還原叢集](#)。

- 如果您對您的 Amazon Redshift 叢集使用 EC2-Classic 平台，則必須使用 Amazon Redshift 安全群組。

在任一情況下，如果您的 SQL 用戶端在 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體上執行，則可以新增規則至安全群組，以授予明確的輸入存取給特定範圍的 CIDR/IP 地址或 Amazon EC2 安全群組。如需詳細資訊，請參閱 [Amazon Redshift 叢集安全群組](#)。

除了輸入存取規則，您可以建立資料庫使用者來提供登入資料，向叢集本身的資料庫進行驗證。如需詳細資訊，請參閱此主題中的 [資料庫](#)。

加密

佈建叢集時，您可以選擇性地加密叢集來獲得額外的安全性。啟用加密時，Amazon Redshift 會將所有資料以加密格式儲存在使用者建立的資料表中。您可以使用 AWS Key Management Service (AWS KMS) 來管理您的 Amazon Redshift 加密金鑰。

加密是叢集不可變的屬性。從加密叢集切換至未加密叢集的唯一方式，是卸載資料，再將資料重新載入至新的叢集。加密會套用至叢集和任何備份。從加密的快照還原叢集時，新的叢集也會加密。

如需加密、金鑰和硬體安全性模組的相關資訊，請參閱 [Amazon Redshift 資料庫加密](#)。

SSL 連線

您可以使用 Secure Sockets Layer (SSL) 加密來加密您的 SQL 用戶端和您的叢集之間的連線。如需詳細資訊，請參閱 [設定連線的安全選項](#)。

監控叢集

有數個功能與 Amazon Redshift 中的監控相關。您可使用資料庫稽核記錄產生活動紀錄、設定事件和通知訂閱，以追蹤感興趣的資訊。使用 Amazon Redshift 和 Amazon 中的指標 CloudWatch 來了解叢集和資料庫的運作狀態和效能。

資料庫稽核記錄日誌

您可以使用資料庫稽核記錄功能來追蹤身分驗證嘗試、連線、中斷連線、對資料庫使用者定義的變更，以及資料庫中所執行查詢的相關資訊。此資訊對於 Amazon Redshift 中的安全性和故障診斷目的很有幫助。日誌會儲存在 Amazon S3 儲存貯體中。如需詳細資訊，請參閱 [資料庫稽核記錄日誌](#)。

事件和通知

Amazon Redshift 會追蹤事件，並在您的 AWS 帳戶中保留數週的相關資訊。對於每個事件，Amazon Redshift 會報告相關的資訊，如事件發生的日期、描述、事件來源 (例如，叢集、參數群組或快照)，以及來源 ID。您可以建立指定一組事件篩選條件的 Amazon Redshift 事件通知訂閱。發生符合篩選條件的事件時，Amazon Redshift 便會使用 Amazon Simple Notification Service 來主動通知您已發生事件。如需事件和通知的相關資訊，請參閱 [Amazon Redshift 事件](#)。

效能

Amazon Redshift 提供您可以追蹤叢集和資料庫之運作狀態和效能的效能指標和資料。Amazon Redshift 使用 Amazon CloudWatch 指標來監控叢集的實體層面，例如 CPU 使用率、延遲和輸送量。Amazon Redshift 也會提供查詢和載入的效能資料，以協助您監控叢集中的資料庫活動。如需效能指標和監控的相關資訊，請參閱[監控 Amazon Redshift 叢集效能](#)。

資料庫

Amazon Redshift 會在您佈建叢集時建立一個資料庫。這是您用來載入資料並對資料執行查詢的資料庫。您可以視需要執行 SQL 命令來建立額外的資料庫。如需建立額外資料庫的相關資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的[步驟 1：建立資料庫](#)。

佈建叢集時，您會指定管理員使用者，其會具有叢集內所建立一切資料庫的存取權。這個管理員使用者是超級使用者，他是最初可存取資料庫的唯一使用者，不過這個使用者可以建立其他的超級使用者和使用者。如需詳細資訊，請前往《Amazon Redshift 資料庫開發人員指南》中的[超級使用者](#)和[使用者](#)。

Amazon Redshift 使用參數群組來定義叢集中所有資料庫的行為，例如日期呈現樣式和浮點精確度。如果佈建叢集時不指定參數群組，Amazon Redshift 會將叢集與預設的參數群組建立關聯。如需詳細資訊，請參閱[Amazon Redshift 參數群組](#)。

如需 Amazon Redshift 中資料庫的相關資訊，請前往《Amazon Redshift 資料庫開發人員指南》<https://docs.aws.amazon.com/redshift/latest/dg/>。

將 Amazon Redshift Serverless 與 Amazon Redshift 佈建資料倉儲進行比較

Amazon Redshift Serverless 的某些概念和功能，和其所對應的 Amazon Redshift 佈建資料倉儲功能不同。例如，一個差異極大的比較是 Amazon Redshift Serverless 沒有叢集或節點的概念。下表描述 Amazon Redshift Serverless 中的功能和行為，並說明它們與佈建資料倉儲中的同等功能有何不同。

功能	描述	無伺服器	佈建
工作群組和命名空間	若要在 Amazon Redshift Serverless 中隔離工	命名空間是資料庫物件和使用者集合。 工作群組是	佈建叢集是您直接管理的運算節點和領導節點的集合。 如需詳細資訊，請參閱 Amazon Redshift 佈建叢集 。

功能	描述	無伺服器	佈建
	作負載並管理不同的資源，您可以建立命名空間和工作群組，以便將儲存和運算資源分開管理。	運算資源的集合。如需詳細資訊，請參閱 Amazon Redshift Serverless 以了解 Amazon Redshift Serverless 的設計。	

功能	描述	無伺服器	佈建
節點類型	當您使用 Amazon Redshift Serverless 時，不會像使用 Amazon Redshift 佈建叢集那樣地選擇節點類型或指定節點計數。	Amazon Redshift Serverless 會自動為您佈建和管理容量。您可以選擇性地指定基礎資料倉儲容量，以便為您的工作負載選擇合適的性價比。您也可以指定最大 RPU 時數來設定成本控制，以確保成本是可預測的。如需詳細資訊，請參閱 了解 Amazon Redshift Serverless 容量 。	您可以使用符合成本和效能規格的節點類型來建置叢集。如需詳細資訊，請參閱 Amazon Redshift 佈建叢集 。

功能	描述	無伺服器	佈建
工作負載管理和並行擴展	Amazon Redshift 可以在負載繁重時進行擴展。Amazon Redshift Serverless 也可以進行擴展以滿足間歇性高負載時段。	Amazon Redshift Serverless 會在成本控制的閾值內，自動根據工作負載有效率地管理資源並進行擴展。如需詳細資訊，請參閱 運算容量的帳單 。	使用佈建資料倉儲時，您可以在叢集上啟用並行擴展，以應付負載繁重的期間。如需詳細資訊，請參閱 並行擴展 。
連接埠	您用來連線的連接埠號碼。	使用 Amazon Redshift Serverless 時，您可以變更為連接埠範圍 5431 至 5455 或 8191 至 8215 內的另一個連接埠。如需詳細資訊，請參閱 連線至 Amazon Redshift Serverless 。	使用佈建資料倉儲時，您可以選擇任何連接埠來連線。

功能	描述	無伺服器	佈建
調整大小	新增或移除運算資源，以便有良好的工作負載執行效能。	調整大小不適用於 Amazon Redshift Serverless。不過，您可以根據您的價格和效能要求，變更基礎的資料倉儲 RPU 容量。如需詳細資訊，請參閱 了解 Amazon Redshift Serverless 容量 。	使用佈建叢集時，您可以執行叢集調整大小以新增節點或移除節點。如需詳細資訊，請參閱 在 Amazon Redshift 中管理叢集的概觀 。
暫停和繼續	您可以在沒有要執行的工作負載時暫停佈建叢集，以節省成本。	使用 Amazon Redshift Serverless 時，您只需就執行的查詢付費，因此無需暫停或繼續。如需詳細資訊，請參閱 運算容量的帳單 。	您根據不同時間的工作負載評估，手動暫停和繼續叢集。如需詳細資訊，請參閱 在 Amazon Redshift 中管理叢集的概觀 。

功能	描述	無伺服器	佈建
使用 Spectrum 查詢來查詢外部資料	您可以使用各種格式 (例如 JSON) 查詢 Amazon S3 儲存貯體中的資料。	運算資源在處理工作負載時會產生費用。此外，如同任何其他交易一樣，查詢外部 Redshift Spectrum 資料時，也會產生費用。如需詳細資訊，請參閱 運算容量的帳單 。	使用佈建資料倉儲時，Amazon Redshift Spectrum 容量存在於從 Amazon Redshift 叢集查詢的個別伺服器上。如需詳細資訊，請參閱 使用 Amazon Redshift Spectrum 查詢外部資料 。

功能	描述	無伺服器	佈建
運算資源計費	Amazon Redshift 與 Amazon Redshift Serverless 的計費方式。	使用 Amazon Redshift Serverless 時，您只需就所執行的工作負載支付費用，計費基礎為每秒 RPU 小時，最低費用為 60 秒。這包括在 Amazon S3 中存取開放檔案格式資料的查詢。如需詳細資訊，請參閱 運算容量的帳單 。	使用佈建叢集時，如果叢集未暫停，則會按秒計費。

功能	描述	無伺服器	佈建
Maintenance window (維護時段)	伺服器維護的運作方式。	使用 Amazon Redshift Serverless 時，不會有維護時段。系統會以無縫方式處理更新。如需詳細資訊，請參閱 什麼是 Amazon Redshift Serverless?	使用佈建叢集時，則會在進行修補時指定維護時段。(一般來說，您可以選擇低使用量的週期性時間。)
加密	您可以啟用資料庫加密。	Amazon Redshift 無伺服器一律使 AWS KMS 用受管金鑰或客戶受 AWS 管金鑰加密。	佈建資料倉儲中的資料可以使用 AWS KMS (使用受管金鑰或客戶 AWS 管理金鑰) 加密，也可以未加密。請參閱 Amazon Redshift 資料庫加密 。

功能	描述	無伺服器	佈建
儲存計費	儲存的計費方式。	若為 Amazon Redshift Serverless。會根據每月 GB 數來計算費率。請參閱 運算容量的帳單 。	針對具有 RA3 節點的佈建叢集，儲存以及運算資源都會計費。

功能	描述	無伺服器	佈建
使用者管理	管理使用者的方式。	<p>對於 Amazon Redshift 無伺服器，使用者是 IAM 或 Redshift 使用者。如需詳細資訊，請參閱 Amazon Redshift Serverless 中的身分和存取管理。</p> <p>如需如何管理 IAM 身分的相關資訊 (包括 IAM 角色的最佳實務)，請參閱 Amazon Redshift 中的身分和存取管理。</p>	<p>對於佈建的資料倉儲，使用者是 IAM 或 Redshift 使用者。如需詳細資訊，請參閱 Amazon Redshift 資料庫開發人員指南中的管理資料庫安全性。</p> <p>如需如何管理 IAM 身分的相關資訊 (包括 IAM 角色的最佳實務)，請參閱 Amazon Redshift 中的身分和存取管理。</p>

功能	描述	無伺服器	佈建
JDBC 和 ODBC 工具與相容性	用戶端連線的運作方式。	Amazon Redshift 無伺服器與任何 JDBC 或 ODBC 相容的工具或用戶端應用程式相容。如需驅動程式的相關資訊，請參閱《Amazon Redshift 管理指南》中的 設定連線 。如需連線至 Amazon Redshift 無伺服器的相關資訊，請參閱 連線至無伺服器 。	佈建的 Amazon Redshift 與任何 JDBC 或 ODBC 相容的工具或用戶端應用程式相容。如需驅動程式的相關資訊，請參閱《Amazon Redshift 管理指南》中的 設定連線 。如需連線到叢集的相關資訊，請參閱 使用 SQL 用戶端工具連線至 Amazon Redshift 資料倉儲 。

功能	描述	無伺服器	佈建
登入時的憑證要求	憑證的處理方式。	若為 Amazon Redshift Serverless，您不必在每個執行個體中輸入憑證。如需詳細資訊，請參閱 連線至 Amazon Redshift Serverless 。	想要存取 Amazon Redshift 就需要與 IAM 角色相關聯的使用者所提供的登入憑證。IAM 角色會針對佈建資料倉儲附加特定許可。經過驗證之後，使用者就可以直接連線到資料庫、Redshift 主控台，以及查詢編輯器 v2。

功能	描述	無伺服器	佈建
Data API (資料 API)	您可以從 Web 服務和其他應用程式存取資料。	Amazon Redshift Serverless 支援 Amazon Redshift 資料 API。使用 Amazon Redshift Serverless 時，您會使用 workgroup-name 參數而不是 cluster-identity 參數。如需呼叫資料 API 的相關資訊，請參閱 使用 Amazon Redshift 資料 API 。	Amazon Redshift 佈建支援 Amazon Redshift 資料 API。使用 Amazon Redshift 叢集時，您可以使用 cluster-identity 參數而不是 workgroup-name 參數。如需呼叫資料 API 的相關資訊，請參閱 使用 Amazon Redshift 資料 API 。

功能	描述	無伺服器	佈建
快照	提供 point-in-time 恢復。	Amazon Redshift Serverless 支援快照和復原點。如需命名空間的快照和復原點的相關資訊，請參閱 使用快照和復原點 。	佈建叢集支援快照。如需詳細資訊，請參閱 使用主控台管理快照 。
資料共用	提供在相同帳戶或不同帳戶中的資料庫之間共用資料的能力。	Amazon Redshift Serverless 支援佈建資料倉儲所具備的所有資料共用功能。其也可在 Amazon Redshift Serverless 和佈建資料倉儲、工具或用戶端應用程式之間支援資料共用。	佈建的叢集支援跨資料庫、跨帳戶、跨區域和 AWS Data Exchange 資料共用。如需詳細資訊，請參閱在 Amazon Redshift 中跨叢集共用資料 。

功能	描述	無伺服器	佈建
追蹤	提供軟體更新的排程。	Amazon Redshift Serverless 沒有追蹤的概念。版本和更新會由服務處理。如需 Amazon Redshift Serverless 設計的相關資訊，請參閱 使用快照和復原點 。	佈建叢集支援在目前的追蹤和隨後的追蹤之間進行切換。

功能	描述	無伺服器	佈建
系統資料表和檢視	提供監控資源和系統中繼資料的方法。	Amazon Redshift Serverless 支援新的系統資料表和檢視。如需系統資料表的相關資訊，請參閱 監控檢視 。如需如何將查詢從使用舊版的佈建系統資料表和檢視遷移至新檢視的相關資訊，請參閱 遷移至 SYS 監控檢視 。	佈建資料倉儲支援一組現有的系統資料表和檢視，可用於監控以及其他需要系統中繼資料的任務。
參數群組	這是套用至叢集中所建立所有資料庫的一組參數。這些參數用於設定查詢逾時和日期樣式等資料庫設定。	Amazon Redshift Serverless 沒有參數群組的概念。	佈建資料倉儲支援參數群組。如需佈建叢集之參數群組的相關資訊，請參閱 Amazon Redshift 參數群組 。

功能	描述	無伺服器	佈建
查詢監控	提供以時間為基礎的查詢執行檢視。	Amazon Redshift Serverless 中的查詢監控需要使用者連線到資料庫才能使用系統資料表。如此一來，查詢監控和系統資料表才會同步。Amazon Redshift Serverless 中的系統資料表查詢會使用映射至 IAM 使用者的資料庫使用者來使用查詢監控。如需監控查詢的相關資訊，請參閱 使用 Amazon Redshift Serverless 監控查詢和工作負載 。	佈建叢集中的查詢監控不會顯示系統資料表中的所有資料。

功能	描述	無伺服器	佈建
稽核記錄	提供資料庫中連線和使用者活動的相關資訊。	使用 Amazon Redshift 無伺服器，CloudWatch 是稽核日誌的目的地。Amazon Redshift Serverless 不支援以 Amazon S3 為基礎的稽核日誌交付。如需詳細資訊，請參閱 Amazon Redshift Serverless 的稽核記錄 。	若為佈建叢集，以 Amazon S3 為基礎的稽核日誌交付已成為常態。現在，將稽核記錄的傳遞 CloudWatch 延伸至涵蓋佈建的資料倉儲。

功能	描述	無伺服器	佈建
事件通知	Amazon EventBridge 是一種無伺服器事件匯流排服務，可用來連接應用程式與來自各種來源的事件資料。	Amazon Redshift 無伺服器使用 Amazon EventBridge 來管理事件通知，讓您 up-to-date 掌握資料倉儲中的變更。如需詳細資訊，請參閱 Amazon Redshift 馬 Amazon 無服務器事件通知 EventBridge 。	若為佈建叢集，您會使用 Amazon Redshift 主控台建立事件訂閱，以管理事件通知。如需更多詳細資訊，請參閱 管理叢集事件通知 。

使用已佈建叢集的 Amazon Redshift 管理界面

Note

本主題著重於已佈建叢集的 Amazon Redshift 管理界面。亞馬遜 Redshift 無伺服器和亞馬 Amazon Redshift 資料 API 也有類似的管理界面。

Amazon Redshift 支援多種管理界面，您可以用來建立、管理和刪除 Amazon Redshift 叢集：AWS 開發套件、AWS Command Line Interface (AWS CLI) 和 Amazon Redshift 管理 API。

Amazon Redshift API — 您可以透過提交請求來呼叫此 Amazon Redshift 管理 API。請求是使用 HTTP 動詞 GET 或 POST 及 Action 參數的 HTTP 或 HTTPS 請求。呼叫 Amazon Redshift API 是存取

Amazon Redshift 服務最直接的方式。不過，這需要您的應用程式處理低階詳細資訊，例如錯誤處理和產生雜湊以簽署請求。

- 如需有關建置與簽署 Amazon Redshift API 請求的詳細資訊，請參閱[簽署 HTTP 請求](#)。
- 如需有關 Amazon Redshift API 動作和 Amazon Redshift 資料類型的資訊，請參閱 [Amazon Redshift API 參考](#)。

AWS 開發套件 — 您可以使用 AWS 開發套件來執行與 Amazon Redshift 叢集相關的操作。多種軟體開發套件程式庫包裝了底層的 Amazon Redshift API。它們整合了 API 功能到特定的程式設計語言，並處理許多低階詳細資訊，例如計算簽章、處理請求重試和錯誤處理。在軟體開發套件程式庫中呼叫包裝器函式，可以大幅簡化撰寫 Amazon Redshift 叢集管理應用程式的流程。

- Amazon Redshift 是由 Java，網 AWS 絡，PHP，Python，紅寶石和 Node.js 的開發套件支持。Amazon Redshift 包裝器函式記錄在每個軟體開發套件的參考手冊中。如需開 AWS 發套件的清單及其文件的連結，請參閱 [Amazon Web Services 的工具](#)。
- 本指南提供透過 Java 開發套件使用 Amazon Redshift 的範例。如需更多一般 AWS SDK 程式碼範例，請參閱[使 AWS 用軟體開發套件的 Amazon Redshift 程式碼範例](#)。

AWS CLI— CLI 提供了一組命令列工具，您可以使用這些工具從 Windows、Mac 和 Linux 電腦管理 AWS 服務。AWS CLI 包含以 Amazon Redshift API 動作為基礎的命令。

- 如需有關安裝和設定 Amazon Redshift CLI 的資訊，請參閱[設定 Amazon Redshift CLI](#)。
- 如需有關 Amazon Redshift CLI 命令的參考資料，請參閱《AWS CLI 參考》中的 [Amazon Redshift](#)。

搭配 AWS SDK 使用此服務

AWS 軟體開發套件 (SDK) 可用於許多流行的編程語言。每個 SDK 都提供 API、程式碼範例和說明文件，讓開發人員能夠更輕鬆地以偏好的語言建置應用程式。

SDK 文件	代碼範例
AWS SDK for C++	AWS SDK for C++ 程式碼範例
AWS CLI	AWS CLI 程式碼範例

SDK 文件	代碼範例
AWS SDK for Go	AWS SDK for Go 程式碼範例
AWS SDK for Java	AWS SDK for Java 程式碼範例
AWS SDK for JavaScript	AWS SDK for JavaScript 程式碼範例
適用於 Kotlin 的 AWS SDK	適用於 Kotlin 的 AWS SDK 程式碼範例
AWS SDK for .NET	AWS SDK for .NET 程式碼範例
AWS SDK for PHP	AWS SDK for PHP 程式碼範例
AWS Tools for PowerShell	PowerShell 程式碼範例的工具
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto3) 程式碼範例
AWS SDK for Ruby	AWS SDK for Ruby 程式碼範例
適用於 Rust 的 AWS SDK	適用於 Rust 的 AWS SDK 程式碼範例
適用於 SAP ABAP 的 AWS SDK	適用於 SAP ABAP 的 AWS SDK 程式碼範例
適用於 Swift 的 AWS SDK	適用於 Swift 的 AWS SDK 程式碼範例

可用性範例

找不到所需的內容嗎？請使用本頁面底部的提供意見回饋連結申請程式碼範例。

簽署 HTTP 請求

Amazon Redshift 要求您傳送至管理 API 的每個請求都必須經過簽章驗證。本主題將說明如何簽署請求。

如果您使用其中一個 AWS 軟體開發套件 (SDK) 或 AWS Command Line Interface，系統會自動處理要求簽署，您可以略過本節。如需使用 AWS SDK 的詳細資訊，請參閱[使用已佈建叢集的 Amazon Redshift 管理界面](#)。如需使用 Amazon Redshift 命令列界面的相關資訊，請前往[Amazon Redshift 命令列參考](#)。

若要簽署請求，請使用加密雜湊函數來計算數位簽章。加密雜湊是一個函數，其根據輸入傳回一個唯一的雜湊值。此雜湊函數的輸入包含請求和私密存取金鑰 (可從暫時憑證取得) 的文字。雜湊函數會傳回一個雜湊值，您將此值包含在請求中做為簽章。該簽章是請求 Authorization 標頭中的一部分。

Note

如果使用者想要與 AWS 之外互動，則需要程式設計存取 AWS Management Console。授與程式設計存取 AWS 取權的方式取決於正在存取的使用者類型。若要授與使用者程式設計存取權，請選擇下列其中一個選項。

哪個使用者需要程式設計存取權？	到	By
人力身分 (IAM Identity Center 中管理的使用者)	使用臨時登入資料來簽署對 AWS CLI、AWS SDK 或 AWS API 的程式設計要求。	請依照您要使用的介面所提供的指示操作。 <ul style="list-style-type: none"> 如需詳細資訊 AWS CLI，請參閱 《使 AWS CLI 用 AWS Command Line Interface 者指南》 AWS IAM Identity Center 中的〈配置使用〉。 如需 AWS SDK、工具和 AWS API，請參閱 AWS SDK 和工具參考指南中的 IAM 身分中心身分驗證。
IAM	使用臨時登入資料來簽署對 AWS CLI、AWS SDK 或 AWS API 的程式設計要求。	遵循 《IAM 使用者指南》 中的〈 將臨時登入資料搭配 AWS 資源使用 〉中的指示
IAM	(不建議使用) 使用長期認證來簽署對 AWS CLI、AWS SDK 或 AWS API 的程式設計要求。	請依照您要使用的介面所提供的指示操作。 <ul style="list-style-type: none"> 如需相關資訊 AWS CLI，請參閱使用指南中的 使用 IAM 使用者登入資料進行

哪個使用者需要程式設計存取權？

到

By

[驗證](#)。AWS Command Line Interface

- 對於 AWS SDK 和工具，請參閱 AWS SDK 和工具參考指南中的[使用長期憑據進行身份驗證](#)。
- 如需 AWS API，請參閱 IAM 使用者指南中的[管理 IAM 使用者的存取金鑰](#)。

Amazon Redshift 收到請求後，其會使用您原先用來簽署請求的相同雜湊函數與輸入來重新計算簽章。若產生的簽章與請求中的簽章相符，Amazon Redshift 會處理該請求，否則請求會遭到拒絕。

Amazon Redshift 支援使用 [AWS Signature 第 4 版](#) 進行身分驗證。計算簽章的程序由三個任務組成。這些任務如下圖說明。

- [任務 1：建立標準請求](#)

將 HTTP 請求重新編排為正式格式。必須使用正式格式，因為 Amazon Redshift 在比較您傳送的簽章來建立簽章時會使用相同的正式格式。

- [任務 2：建立登入字串](#)

建立一個字串，您會使用此字串做為密碼編譯雜湊函數的其中一個輸入值。此字串，稱為登入字串，是雜湊演算法的名稱、請求日期、登入資料範圍字串和前一個任務的正式請求的串連。登入資料範圍字串本身是日期、區域和服務資訊的串連。

- [任務 3：計算簽章](#)

使用接受兩個輸入字串的密碼編譯雜湊函數來計算請求的簽章：您的登入字串和衍生金鑰。藉由從您的私密存取金鑰開始來計算此衍生金鑰和使用登入資料範圍字串來建立一系列雜湊型訊息身分驗證代碼 (HMAC-SHA256)。

範例簽章計算

下列範例會逐步引導您建立 [CreateCluster](#) 要求簽名的詳細資訊。您可以使用此範例做為檢查自身簽章計算方法的參考。其他參考計算包含在《IAM 使用者指南》的 [請求簽章範例章節](#) 中。

您可以使用 GET 或 POST 請求，將請求傳送至 Amazon Redshift。此兩者的差異在於，若是 GET 要求，會以查詢字串參數的形式來傳送您的參數。若是 POST 請求，它們會包含在請求的內文中。下列範例說明 POST 請求。

該範例假設如下：

- 請求的時間戳記為 Fri, 07 Dec 2012 00:00:00 GMT。
- 端點是美國東部 (維吉尼亞北部) 區域 (us-east-1)。

一般的請求語法是：

```
https://redshift.us-east-1.amazonaws.com/  
  ?Action=CreateCluster  
  &ClusterIdentifier=examplecluster  
  &MasterUsername=masteruser  
  &MasterUserPassword=12345678Aa  
  &NumberOfNode=2  
  &NodeType=dc2.large  
  &Version=2012-12-01  
  &x-amz-algorithm=AWS4-HMAC-SHA256  
  &x-amz-credential=AKIAIOSFODNN7EXAMPLE/20121207/us-east-1/redshift/aws4_request  
  &x-amz-date=20121207T000000Z  
  &x-amz-signedheaders=content-type;host;x-amz-date
```

對於 [任務 1：建立正式請求](#) 計算的請求的正式形式是：

```
POST  
/  
  
content-type:application/x-www-form-urlencoded; charset=utf-8  
host:redshift.us-east-1.amazonaws.com  
x-amz-date:20121207T000000Z  
  
content-type;host;x-amz-date  
55141b5d2aff6042ccd9d2af808fdf95ac78255e25b823d2dbd720226de1625d
```

正式請求的最後一行是請求內文的雜湊值。正式請求中的第三行是空的，因為此 API 沒有查詢參數。

「[任務 2：建立登入字串](#)」的登入字串是：

```
AWS4-HMAC-SHA256
20121207T000000Z
20121207/us-east-1/redshift/aws4_request
06b6bef4f4f060a5558b60c627cc6c5b5b5a959b9902b5ac2187be80cbac0714
```

登入字串的第一行是演算法，第二行是時間戳記，第三行是登入資料範圍，最後一行是來自[任務 1：建立正式請求](#)的正式請求的雜湊。在憑證範圍內使用的服務名稱是 redshift。

對於[任務 3：計算簽章](#)，衍生金鑰可以表示為：

```
derived key = HMAC(HMAC(HMAC(HMAC("AWS4" + YourSecretAccessKey, "20121207"), "us-
east-1"), "redshift"), "aws4_request")
```

衍生金鑰是以湊雜函數的方式計算。從上述公式中的內部 HMAC 陳述式開始，您可以串連片語 **AWS4** 與私密存取金鑰並使用此做為金鑰來對資料 "us-east-1" 進行雜湊。此雜湊的結果都會變成下一個雜湊函數的金鑰。

在計算衍生金鑰後，您會在雜湊函數中使用它，該函數會接受兩個輸入字串：您的登入字串和衍生金鑰。例如，如果您使用私密存取金鑰 wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY 和先前提提供的登入字串，則已計算的簽章如下：

```
9a6b557aa9f38dea83d9215d8f0eae54100877f3e0735d38498d7ae489117920
```

最後步驟是建立 Authorization 標頭。對於示範存取金鑰 AKIAIOSFODNN7EXAMPLE，標頭 (為了可讀性而新增了換行) 是：

```
Authorization: AWS4-HMAC-SHA256 Credential=AKIAIOSFODNN7EXAMPLE/20121207/us-east-1/
redshift/aws4_request,
SignedHeaders=content-type;host;x-amz-date,
Signature=9a6b557aa9f38dea83d9215d8f0eae54100877f3e0735d38498d7ae489117920
```

設定 Amazon Redshift CLI

本節說明如何設定和執行 AWS CLI 命令列工具，以使用於管理 Amazon Redshift。Amazon Redshift 命令行工具上運行 AWS Command Line Interface (AWS CLI)，這反過來又使用 Python (<https://www.python.org/>)。AWS CLI 可以在任何支援 Python 的作業系統上執行。

安裝說明

若要開始使用 Amazon Redshift 命令列工具，請先設定 AWS CLI，然後新增定義 Amazon Redshift CLI 選項的組態檔案。

如果您已經安裝並設定 AWS CLI 其他 AWS 服務，則可以略過此程序。

若要安裝 AWS Command Line Interface

1. 移至 [\[安裝或更新至最新版本的\]](#) AWS CLI，然後依照指示安裝 AWS CLI。

對於 CLI 存取，您需要存取金鑰 ID 和私密存取金鑰。盡可能使用臨時憑證，而不是長期存取金鑰。臨時憑證包含存取金鑰 ID、私密存取金鑰，以及指出憑證何時到期的安全符記。如需詳細資訊，請參閱 IAM 使用者指南中的[將臨時登入資料與 AWS 資源搭配使用](#)。

2. 建立包含組態資訊 (例如您的存取金鑰、預設區域和命令輸出格式) 的檔案。然後設定 `AWS_CONFIG_FILE` 環境變數來參考該檔案。如需詳細指示，請參閱 [《AWS Command Line Interface 使用指南》](#) 中的 [〈配置指 AWS 命令行介面〉](#)。
3. 執行測試命令以確認 AWS CLI 介面是否正常運作。例如，下列命令應會顯示 AWS CLI 協助資訊：

```
aws help
```

下列命令應會顯示 Amazon Redshift 協助資訊：

```
aws redshift help
```

如需 Amazon Redshift CLI 命令的參考資料，請前往參考資料中的 [Amazon Redshift](#)。AWS CLI

Amazon Redshift Serverless

Amazon Redshift Serverless 可讓您輕鬆地執行和擴展分析，而不必佈建和管理資料倉儲。透過 Amazon Redshift Serverless，資料分析師、開發人員和資料科學家現在可以使用 Amazon Redshift 將資料載入到資料倉儲以及從資料倉儲查詢記錄，在幾秒鐘內從資料中獲得洞察。Amazon Redshift 會自動佈建和擴展資料倉儲容量，為嚴苛且無法預測的工作負載提供快速的效能。您只需支付實際使用容量的費用。不必變更現有的分析和商業智慧應用程式，就能透過這項簡易性獲得好處。

什麼是 Amazon Redshift Serverless ？

Amazon Redshift Serverless 會自動佈建資料倉儲容量，並有智慧地擴展基礎資源。Amazon Redshift Serverless 可在幾秒鐘內調整容量，即使面對最苛刻、最不穩定的工作負載，也能持續提供高效能和簡化的操作機制。

透過 Amazon Redshift Serverless，您可以從下列功能獲得好處：

- 存取和分析資料，而不必設定、微調和管理 Amazon Redshift 佈建的叢集。
- 使用優異的 Amazon Redshift SQL 功能、領先業界的效能和資料湖整合，以在資料倉儲、資料湖和操作資料來源之間無縫地進行查詢。
- 透過智慧型自動擴展功能，為最嚴苛、最不穩定的工作負載持續提供高效能和簡化的操作機制。
- 使用工作群組和命名空間，透過精細的成本控制來組織運算資源和資料。
- 僅在資料倉儲處於使用狀態時才需要付費。

透過 Amazon Redshift Serverless，您可以使用主控台介面連線至無伺服器資料倉儲或 API 以建置應用程式。透過資料倉儲，您可以存取 Amazon Redshift 受管儲存和 Amazon S3 資料湖。

此影片會向您展示 Amazon Redshift Serverless 如何讓您輕鬆地執行和擴展分析，而不必管理資料倉儲基礎設施：

Amazon Redshift Serverless 主控台

若要開始使用 Amazon Redshift Serverless 主控台，請觀看以下影片：[開始使用 Amazon Redshift Serverless](#)。

Serverless 儀表板

在 Serverless 儀表板頁面上，您可以檢視資源摘要和用量圖表。

- 命名空間概觀 — 此區段會顯示命名空間內的快照和資料共用數量。
- 工作群組 — 此區段會顯示 Amazon Redshift Serverless 內的所有工作群組。
- 查詢指標 — 此區段會顯示過去 1 小時的查詢活動。
- 使用的 RPU 容量 — 此區段會顯示過去 1 小時使用的容量。
- 免費試用 — 此區段會顯示 AWS 帳戶中剩餘的免費試用抵用金。這涵蓋了同一帳戶下 Amazon Redshift Serverless 資源和操作 (包括快照、儲存、工作群組等) 的所有用量。
- 警示 — 此區段會顯示您在 Amazon Redshift Serverless 中所設定的警示。

資料備份

在資料備份索引標籤上，您可以使用以下項目：

- 快照 — 您可以建立、刪除和管理 Amazon Redshift Serverless 資料的快照。預設保留期間為 indefinitely，但您可以將保留期間設定為 1 到 3653 天之間的任何值。您可以授權 AWS 帳戶從快照還原命名空間。
- 復原點 — 顯示系統所自動建立、可讓您從過去 24 小時內的意外寫入或刪除情況中復原的復原點。若要復原資料，您可以將復原點還原至任何可用的命名空間。如果您想要延長復原點的保留期間，則可以從復原點建立快照。預設保留期間為 indefinitely，但您可以將保留期間設定為 1 到 3653 天之間的任何值。

資料存取

在資料存取索引標籤上，您可以使用下列項目：

- 網路和安全設定 — 您可以檢視 VPC 相關的、AWS KMS 加密值和稽核記錄值。您只能更新稽核記錄。如需使用主控台來設定網路和安全設定的相關資訊，請參閱[管理用量限制、查詢限制及其他管理任務](#)。
- AWS KMS key— AWS KMS key 用於加密 Amazon Redshift 無服務器資源。
- 許可 — 您可以管理 Amazon Redshift Serverless 所能擔任以代表您使用資源的 IAM 角色。如需詳細資訊，請參閱[Amazon Redshift Serverless 中的身分和存取管理](#)。
- Redshift 受管 VPC 端點 — 您可以從其他 VPC 或子網路存取您的 Amazon Redshift Serverless 執行個體。如需詳細資訊，請參閱[從其他 VPC 端點連線至 Amazon Redshift Serverless](#)。

限制

在限制索引標籤上，您可以使用以下項目：

- 以 Redshift 處理單元 (RPU) 為單位的基本容量設定 — 您可以設定用來處理工作負載的基本容量。若要改善查詢效能，請增加您的 RPU 值。
- 用量限制 — Amazon Redshift Serverless 執行個體可在動作啟動前的期間內使用的運算資源上限。您可以限制 Amazon Redshift Serverless 用來執行工作負載的資源數量。用量的測量單位是 Redshift 處理單元 (RPU) 小時。RPU 小時是一小時內所使用的 RPU 數量。您可以決定在達到所設定的限制值時會發生的動作，如下所示：
 - 傳送提醒。
 - 在系統資料表中記錄項目。
 - 關閉使用者查詢。

您最多可以設定四個限制。

- 查詢限制 — 您可以新增限制以監控效能和限制。如需查詢監控限制的相關資訊，請參閱 [WLM 查詢監控規則](#)。

如需詳細資訊，請參閱 [了解 Amazon Redshift Serverless 容量](#)。

資料共用

在資料共用索引標籤上，您可以使用以下項目：

- 我的命名空間中建立的資料共用設定 — 您可以建立資料共用，並與其他命名空間和 AWS 帳戶共用。
- 來自其他命名空間的 Datashares 和 AWS 帳戶 — 您可以從其他命名空間和 AWS 帳戶

如需資料共用的相關資訊，請參閱 [Amazon Redshift Serverless 中的資料共用](#)。

查詢和資料庫監控

在查詢和資料庫監控頁面上，您可以檢視查詢歷史記錄和資料庫效能的圖表。

在查詢歷史記錄索引標籤上，您會看到下列圖表 (您可以在查詢清單和資源指標之間進行選擇)：

- 查詢執行期 — 此圖表會顯示在相同時間範圍內執行的查詢。選擇圖表中的長條可檢視更多的查詢執行詳細資訊。
- 查詢與載入 — 此區段會依查詢 ID 列出查詢和載入。
- 已使用的 RPU 容量 — 此圖表會顯示以 Redshift 處理單元 (RPU) 為單位的整體容量。
- 資料庫連線數 — 此圖表會顯示作用中資料庫連線的數目。

資料庫效能

在資料庫效能索引標籤上，您會看到下列圖表：

- 每秒完成的查詢數 — 此圖表會顯示每秒完成的平均查詢數目。
- 查詢持續時間 — 此圖表會顯示完成查詢的平均時間長度。
- 資料庫連線數 — 此圖表會顯示作用中資料庫連線的數目。
- 執行中的查詢數 — 此圖表會顯示給定時間的執行中查詢總數。
- 排入佇列的查詢數 — 此圖表會顯示給定時間的已排入佇列查詢總數。
- 查詢執行時間明細 — 此圖表會顯示依查詢類型的查詢所花執行時間總數。

資源監控

在資源監控頁面上，您可以檢視已取用資源的圖表。您可以根據數個面向來篩選資料。

- 指標篩選條件 — 您可以使用指標篩選條件來選取特定工作群組的篩選條件，以及選擇時間範圍和時間間隔。
- 已使用的 RPU 容量 — 此圖表會顯示以 Redshift 處理單元 (RPU) 為單位的整體容量。
- 運算用量 — 此圖表會顯示所選時間範圍內，依期間分類的 RPU 時數用量。對於少於 6 小時的時間範圍，RPU 時數會以精確的時間顯示。對於 6 小時或以上的時間範圍，RPU 時數會顯示為平均值。

在資料共用頁面上，您可以管理在我的帳戶中和從其他帳戶資料共用。如需資料共用的相關資訊，請參閱 [Amazon Redshift Serverless 中的資料共用](#)。

使用 Amazon Redshift Serverless 時的考量

如需提供 Amazon Redshift 無伺服器的位 AWS 區域 置清單，請參閱中列出的 [Redshift 無伺服器 API 端點](#)。Amazon Web Services 一般參考

Amazon Redshift Serverless 所使用的某些資源會受到配額限制。如需詳細資訊，請參閱 [Amazon Redshift Serverless 物件的配額](#)。

當您 DECLARE (宣告) 游標時，系統會在 [DECLARE](#) 中指定 Amazon Redshift Serverless 的結果集大小規格。

維護時段 — Amazon Redshift Serverless 沒有維護時段。系統會自動套用軟體版本更新。當 Amazon Redshift 切換版本時，現有的連線或查詢執行不會中斷。新連線則一律會立即連線並與 Amazon Redshift Serverless 搭配運作。

可用區域 ID — 在設定 Amazon Redshift Serverless 執行個體時，請開啟其他考量，並確保子網路中提供的子網路 ID 至少包含三個支援的可用區域 ID。若要查看子網路與可用區域 ID 的對應，請移至 VPC 主控台，然後選擇子網路以查看子網路 ID 及其可用區域 ID 的清單。請確認您的子網路有對應至支援的可用區域 ID。若要建立子網路，請參閱《Amazon VPC 使用者指南》中的[在 VPC 中建立子網路](#)。

三個子網路 — 您必須有至少三個子網路，而且這些子網路必須跨越三個可用區域。例如，您可以使用三個分別對應至可用區域 us-east-1a、us-east-1b 和 us-east-1c 的子網路。美國西部 (加利佛尼亞北部) 區域是例外。這個區域和其他區域一樣需要三個子網路，但這些子網路只要跨越兩個可用區域即可。條件是所跨越的其中一個可用區域必須包含兩個子網路。

免費 IP 地址要求 — 當您建立 Amazon Redshift 無伺服器工作群組時，您必須擁有可用的免費 IP 地址。IP 位址的最小數目會隨著工作群組的 Redshift 處理單元 (RPU) 數量增加而提高。具體來說，工作群組 VPC 中的每個子網路都需要最少數量的 IP 位址。如需配置 IP 地址的相關資訊，請參閱《Amazon VPC 使用者指南》中的[IP 定址](#)。

建立工作群組時所需的最低可用 IP 位址數目如下：

每個子網路所需的可用 IP 位址數目

Redshift 處理單元 (RPU)	所需的可用 IP 地址	最小的 CIDR 大小
8	9	/27
16	15	/27
32	13	/27
64	21	/27
128	37	/26
256	69	/25
512	133	/24

將工作群組更新為使用更多 RPU 時，也需要可用的 IP 地址。更新工作群組的子網路時所需的可用 IP 位址數目如下：

更新子網路時所需的可用 IP 地址數量

Redshift 處理單元 (RPU)	更新後的 Redshift 處理單元 (RPU)	所需的可用 IP 地址
8	16	10
16	32	13
32	64	16
64	128	28
128	256	52
256	512	100

遷移後的儲存空間 — 將 Amazon Redshift 佈建的小型叢集遷移到 Amazon Redshift Serverless 時，您可能會發現遷移後的儲存空間配置有所增加。這是儲存空間配置經過最佳化，進而預先配置儲存空間的結果。隨著 Amazon Redshift Serverless 中的資料增加，此空間可使用一段時間。

Amazon Redshift Serverless 和 Amazon Redshift 佈建的叢集之間的資料共用 — 當有 Amazon Redshift Serverless 為生產者且已佈建的叢集是取用者的資料共用時，已佈建叢集的版本必須是 1.0.38214 之後的叢集版本。如果您使用此版本之前的叢集版本，則會在執行查詢時發生錯誤。您可以在 Amazon Redshift 主控台上的維護索引標籤上檢視叢集版本。您也可以執行 `SELECT version();`。

查詢執行時間上限 — 查詢所經歷的執行時間 (以秒為單位)。執行時間不包括在佇列中等待所花的時間。如果查詢超過設定的執行時間，Amazon Redshift Serverless 會停止查詢。有效值為 0 至 86,399。

具有交錯排序索引鍵的資料表遷移 — 將 Amazon Redshift 佈建的叢集遷移至 Amazon Redshift Serverless 時，Redshift 會將具有交錯排序索引鍵和 `DISTSTYLE KEY` 的資料表轉換為複合排序索引鍵。`DiSTSTYLE` 則不會變更。如需分佈樣式的相關資訊，請參閱《Amazon Redshift 開發人員指南》中的[使用資料分佈樣式](#)。如需排序索引鍵的相關資訊，請參閱[使用排序索引鍵](#)。

VPC 共用 — 您可以在共用的 VPC 中建立 Amazon Redshift Serverless 工作群組。如果您這麼做，建議您不要刪除資源共用，因為這會導致工作群組變得無法使用。

Amazon Redshift Serverless 的運算容量

了解 Amazon Redshift Serverless 容量

RPU

Amazon Redshift Serverless 會以 Redshift 處理單元 (RPU) 為單位來測量資料倉儲的容量。RPU 是用來處理工作負載的資源。

基本容量

此設定會指定 Amazon Redshift 用來為查詢提供服務的基本資料倉儲容量。基本容量會以 RPU 為單位來指定。您能以 Redshift 處理單元 (RPU) 為單位來設定基本容量。一個 RPU 可提供 16 GB 的記憶體。設定較高的基本容量可改善查詢效能，對於會取用大量資源的資料處理任務來說更是如此。Amazon Redshift Serverless 的預設基本容量為 128 個 RPU。您可以使用 AWS 主控台、UpdateWorkgroup API 作業或中的作業，將基本容量設定從 8 個 RPU 調整為 512 個單位 (8,16,24... 512)。update-workgroup AWS CLI

使用最小容量 8 個 RPU 時，您現在可以根據效能要求，更彈性地執行更複雜的工作負載。8 個、16 個和 24 個 RPU 的基本 RPU 容量的適用目標是需要少於 128 TB 資料的工作負載。如果您的資料要求大於 128 TB，則必須使用至少 32 個 RPU。如果工作負載的資料表有大量資料行且並行數量較高，建議您使用 32 個以上的 RPU。

Amazon Redshift Serverless 容量的考量和限制

以下是 Amazon Redshift Serverless 容量的考量和限制。

- 8 個或 16 個 RPU 的組態最多可支援 128 TB 的 Redshift 受管儲存容量。如果您要使用超過 128 TB 的受管儲存，則無法降級為少於 32 個 RPU。
- 編輯工作群組的基本容量，如此可能會取消工作群組上執行的某些查詢。

AI 驅動的擴展和最佳化 (預覽)

這是有關 Amazon Redshift Serverless 中 AI 驅動的擴展和優化的發行前版本文件，而該文件為預覽版。文件和功能會隨時變更。我們建議僅在測試環境中使用此功能，不要在生產環境中使用。如需預覽版條款和條件，請參閱 [AWS 服務條款](#) 中的 Beta 版和預覽版。

此預覽可在下列項目中使用 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 (東京) (ap-northeast-1)
- 歐洲 (愛爾蘭) (eu-west-1)
- 歐洲 (斯德哥爾摩) (eu-north-1)

您可以建立預覽工作群組來測試 Amazon Redshift Serverless 的新功能。您無法在生產環境中使用這些功能，以將工作群組移至另一個工作群組。如需了解預覽版條款和條件，請參閱 [AWS 服務條款](#) 中的 Beta 版和預覽版。如需如何建立預覽工作群組的指示，請參閱 [建立預覽工作群組](#)。

您也可以為工作群組設定價格效能目標，好讓 Redshift 可以自動對您的資源進行 AI 驅動的最佳化。透過這種方式，您可以在發揮最佳成本效益的同時，滿足您的價格績效目標。如果您不知道要為工作負載設定哪些基本容量，或是工作負載的某些部分可能會受益於更多配置的資源，則此自動定價效能優化特別有用。

例如，若您的組織通常執行的工作負載只需要 32 RPU，但突然導入了更複雜的查詢，您可能不知道應該要多少基本容量才算適當。設定較高的基本容量可產生較佳的價格效能，但也會產生較高的成本，因此成本可能不符合您的預期。Amazon Redshift Serverless 使用 AI 驅動的擴展和資源最佳化功能，可自動調整 RPU 以符合您的價格效能目標，同時為您的組織最佳化成本把關。無論工作負載大小是多少，此自動最佳化都很有效用。如果您有任何數量的複雜查詢，自動最佳化可協助您達成組織的價格績效目標。

價格效能目標是特定於工作群組的設定。不同的工作群組可以有不同的價格績效目標。

為了保持成本的可預測性，請設定允許 Amazon Redshift Serverless 配置給工作負載的最大容量限制。

若要設定價格效能目標，請使用 AWS 主控台。依預設，當您建立新工作群組並設定為平衡時，便會啟用價格效能目標。若要為工作群組設定不同的價格效能目標或指定基本容量，請在建立工作群組時使用自訂設定。若要取得有關建立工作群組的詳細資訊，請參閱 [使用命名空間建立工作群組](#)。

若要編輯工作群組的價格效能目標：

1. 在 Amazon Redshift Serverless 主控台上，選擇工作群組組態。

2. 選擇您要為其編輯價格效能目標的工作群組。選擇效能索引標籤，然後選擇編輯。
3. 選擇價格效能目標，然後根據您要設定之工作群組目標調整滑桿。
4. 選擇儲存變更。

若要更新 Amazon Redshift Serverless 可分配給工作負載的 RPU 數量上限，請前往工作群組組態的限制索引標籤。

若要深入了解 AI 驅動最佳化和資源擴展，請觀看以下影片。

Amazon Redshift Serverless 的帳單

定價

如需定價資訊，請參閱 [Amazon Redshift 定價](#)。

運算容量的帳單

基本容量及其對帳單的影響

執行查詢時，系統會根據指定期間內使用的容量來計費 (以每秒 RPU 小時進行計算)。沒有執行任何查詢時，則不會向您收取運算容量的費用。系統也會根據所存放的資料量向您收取 Redshift 受管儲存 (RMS) 的費用。

在建立工作群組時，您可以選擇設定運算的基本容量。若要符合工作群組層級的工作負載性價比要求，請將現有工作群組的基本容量調高或調低。從工作群組組態中選取工作群組，然後選擇限制索引標籤，以使用主控台變更基本容量。

隨著查詢數量的增加，Amazon Redshift Serverless 會自動擴展以提供一致的效能。

最大 RPU 時數使用限制

為了讓 Amazon Redshift Serverless 的成本保持可預測性，您可以設定每天、每週或每月能夠使用的 RPU 時數上限。使用主控台或透過 API 即可設定此限制。達到限制時，您可以指定要在系統資料表中寫入日誌項目、接收警示或關閉使用者查詢。設定 RPU 時數上限有助於控制成本。RPU 時數上限的設定會同時在存取資料倉儲資料的查詢和存取外部資料 (例如 Amazon S3 中的外部資料表) 的查詢兩方面適用於工作群組。

以下是範例：

假設您每週設定 100 小時的限制。若要在主控台上執行此操作，請執行下列步驟：

1. 選擇您的工作群組，然後在限制標籤下選擇管理用量限制。
2. 新增用量限制，選擇每週頻率、持續時間為 100 小時，並將動作設定為關閉使用者查詢。

在此範例中，如果您達到一週 100 RPU 小時限制，則關閉查詢。

設定工作群組的 RPU 時數上限並不會限制工作群組的效能或運算資源。您可以隨時調整設定值，而不會中斷查詢作業。設定最大 RPU 時數的目標，是協助您符合價格和效能需求。如需無伺服器帳單的詳細資訊，請參閱 [Amazon Redshift 定價](#)。

想要保持 Amazon Redshift Serverless 成本可預測的另一種方法，是使用 AWS [成本異常偵測](#) 來減少帳單中的意外情況，並提升控制能力。

Note

[Amazon Redshift 定價計算器](#) 有助於估算定價。只要輸入所需的運算資源，其便會提供成本預覽。

設定最大容量以控制運算資源的成本

最大容量設定可作為 Amazon Redshift Serverless 可縱向擴展的 RPU 上限。此有助於控制運算資源的成本。與基本容量設定最小可用運算資源的方式類似，最大容量會設定 RPU 用量上限。這樣就能幫助您的支出符合您的計劃。最大容量特別適用於每個工作群組，並且隨時都會限制運算用量。

最大容量與 RPU 時數用量限制有何不同

最大 RPU 時數限制和最大容量設定的目的在於控制成本。但他們透過不同的方式達成這個目標。以下幾點說明了不同之處：

- **最大容量** — 此設定建立 Amazon Redshift Serverless 用於擴展目的之最高 RPU 數量。當需要自動運算擴展時，最大容量值較高可增強查詢輸送量。達到最大容量限制時，工作群組不會進一步縱向擴展資源。
- **最大 RPU 時數用量限制** — 與最大容量不同，此設定不會設定容量上限。不過，此設定會確實執行其他動作來幫助您限制成本。其中包括將項目新增至記錄檔、通知您，或停止執行查詢 (如果您選擇的話)。

您可以專門使用最大容量，或者您可以使用 RPU 時數最大用量限制中的動作來補充容量。

最大容量使用案例

每個工作群組都可以有不同的最大容量設定。它可以幫助您執行預算編列要求。下列範例說明其運作方式：

- 您的工作群組的基本容量設定為 256 個 RPU。整個月的大部分時間您的工作負載穩定在 256 RPU 以上。
- 最大容量設定為 512 RPU。

假設您在三天期間內有非預期的大量使用率來產生臨機操作統計報告。在此情況下，您已設定最大容量來避免超過 512 RPU 的運算成本。執行此操作時，您可以確定運算容量不會超過此上限。

最大容量的使須知

這些使用須知可協助您正確設定最大容量：

- 每個 Amazon Redshift Serverless 工作群組都可以有不同的最大容量設定。
- 如果您在一段時間內資源使用率非常高，並且最大容量設定為較低的 RPU 級別，如此可能會延遲工作負載處理，並導致使用者體驗不佳。
- 設定最大容量設定並不會干擾執行查詢，即使在 RPU 用量很高時也是如此。它不會像用量限制一樣地運作，可以阻止查詢執行。它只會限制工作群組可用的運算資源。您可以在 Amazon Redshift Serverless 儀表板上檢視一段時間內使用的容量。如需有關檢視摘要資料的詳細資訊，請參閱[使用儀表板檢查 Amazon Redshift Serverless 摘要資料](#)。
- 最大容量設定為 5632 RPU。

如何設定最大容量

您可以在主控台設定最大容量。對於既有的工作群組，您可以變更工作群組組態下的設定。您也可以使用 CLI 執行下列範例所示的命令來設定：

```
aws redshift-serverless update-workgroup --workgroup-name myworkgroup --max-capacity 512
```

這會為具有指定名稱的工作群組設定最大容量設定。設定完成後，您可以在主控台上檢查該值以進行驗證。您也可以使用 CLI 執行 `get-workgroup` 命令來檢查值。

您可以透過設定為 `-1` 來關閉最大容量設定，如下所示：

```
aws redshift-serverless update-workgroup --workgroup-name myworkgroup --max-capacity -1
```

監控 Amazon Redshift Serverless 用量和成本

有數種方式可以估算 Amazon Redshift Serverless 的用量和帳單。系統檢視可能很有幫助，因為系統中繼資料 (包括查詢和使用情況資料) 是及時的，而且您不需要進行任何設定即可查詢。CloudWatch 對於監控 Amazon Redshift 無伺服器執行個體的使用情況也很有用，並具有提供見解和設定動作的其他功能。

透過查詢系統檢視將用量視覺化

查詢 `SYS_SERVERLESS_USAGE` 系統資料表即可追蹤用量並取得查詢費用：

```
select trunc(start_time) "Day",
(sum(charged_seconds)/3600::double
precision) * <Price for 1 RPU> as cost_incurred
from sys_serverless_usage
group by 1
order by 1
```

此查詢會根據用量，提供 Amazon Redshift Serverless 每天產生的費用。

用於決定用量和成本的用量注意事項

- 您只需就所執行的工作負載支付費用，計費基礎為每秒 RPU 小時，最低費用為 60 秒。
- `sys_serverless_usage` 系統資料表中的記錄會顯示以 1 分鐘的時間間隔產生的成本。了解下列資料欄很重要：

`charged_seconds` 資料欄：

- 提供在時間間隔內收費的運算單位 (RPU) 秒數。結果裡面包括 Amazon Redshift Serverless 中的任何最低費用。
- 具有交易完成後運算資源用量的相關資訊。因此，如果交易尚未完成，此資料欄的值可能會是 0。

`compute_seconds` 資料欄：

- 提供即時運算用量資訊。這不包括 Amazon Redshift Serverless 中的任何最低費用。因此，其可能會與間隔期間所計費的收費秒數有某種程度上的不同。
- 顯示每筆交易期間的用量資訊 (即使交易尚未結束)，因此所提供的資料為即時資料。

- 在某些情況下，compute_seconds 為 0，但 charged_seconds 大於 0，反之亦然。這是由於在系統檢視中記錄資料的方式所產生的正常行為。若要更準確地呈現無伺服器使用情況詳細資訊，建議您彙總 SYS_SERVERLESS_USAGE 中的資料。

如需有關監控資料表和檢視的詳細資訊，請參閱[使用 Amazon Redshift Serverless 監控查詢和工作負載](#)。

視覺化使用 CloudWatch

您可以使用中提供的指標 CloudWatch 來追蹤使用情況。產生的指標 CloudWatch 為 ComputeSeconds，指出目前分鐘使用的總 RPU 秒數 ComputeCapacity，並指出該分鐘的總計運算容量。您也可以 Redshift Serverless 儀表板上的 Redshift 主控台上找到用量指標。如需詳細資訊 CloudWatch，請參閱[什麼是 Amazon CloudWatch？](#)

儲存的帳單

主要儲存容量會以 Redshift 受管儲存 (RMS) 來計費。儲存會按每月 GB 數計費。儲存帳單不同於運算容量帳單。視用量方案而定，用於使用者快照的儲存會以標準備份帳單費率計費。

資料傳輸成本和機器學習 (ML) 成本會分開收取，情況與佈建叢集相同。跨 AWS 區域的快照複寫和資料共用會以定價頁面上列出的傳輸費率計費。如需詳細資訊，請參閱[Amazon Redshift 定價](#)。

視覺化帳單使用 CloudWatch

系統會產生追蹤快照儲存使用量 SnapshotStorage 的量度，並將其傳送至 CloudWatch。如需詳細資訊 CloudWatch，請參閱[什麼是 Amazon CloudWatch？](#)

使用 Amazon Redshift Serverless 免費試用

Amazon Redshift Serverless 會提供免費試用。如果您參與免費試用，便可在 Redshift 主控台中檢視免費試用額度餘額，並在 [SYS_SERVERLESS_USAGE](#) 系統檢視中查看免費試用用量。請注意，免費試用用量的帳單詳細資訊不會出現在帳單主控台中。免費試用結束後，您只能在帳單主控台中檢視用量。如需 Amazon Redshift Serverless 免費試用的詳細資訊，請參閱[Amazon Redshift Serverless 免費試用](#)。

帳單用量注意事項

- 記錄用量 — 查詢或交易只會在交易完成、回復或停止後才進行計量和記錄。例如，如果交易執行兩天，系統便會在交易完成後記錄 RPU 用量。您可以透過查詢 sys_serverless_usage 即時監控

持續的使用情況。系統可能會以特定小時和每日使用的 RPU 用量變化和效果成本的形式來反映交易記錄。

- 寫入明確交易 — 請務必將結束交易作為最佳實務。如果您沒有結束或回復開啟的交易，Amazon Redshift Serverless 會繼續使用 RPU。例如，如果你寫入明確的 BEGIN TRAN，則務必要有相應的 COMMIT 和 ROLLBACK 陳述式。
- 已取消的查詢 — 如果您執行查詢並在查詢完成前將其取消，系統仍會就查詢執行過的時間向您收費。
- 擴展 — Amazon Redshift Serverless 執行個體可能會啟動擴展來處理負載較高的時段，以維持一致的效能。您的 Amazon Redshift Serverless 帳單包含相同 RPU 費率的基本運算容量和擴展的容量。
- 縮減規模 — Amazon Redshift Serverless 會從其基本 RPU 容量縱向擴展，以處理負載較高的時段。在某些情況下，RPU 容量可能會在查詢負載下降後於一段時間內保持較高的設定。建議您在主控台中設定 RPU 時數上限，以免產生意外成本。
- 系統資料表 — 當您查詢系統資料表時，系統會就查詢時間計費。
- Redshift Spectrum — 當您有 Amazon Redshift Serverless 並執行查詢時，資料湖查詢不需要另外付費。對存放在 Amazon S3 中的資料所進行的查詢，按交易時間計算的費用與查詢本機資料時相同。
- 聯合查詢 — 聯合查詢會以特定時間間隔內所使用的 RPU 來收費，方式與資料倉儲或資料湖上的查詢相同。
- 儲存 — 儲存會以每月 GB 數另外計費。
- 最低費用 — 最低費用為 60 秒的資源用量，以每秒為單位來計量。
- 快照帳單 — 快照帳單不會變更。系統會根據儲存來收費，並以每月 GB 費率計費。您可以免費地將資料倉儲還原到過去 24 小時內的特定時間點 (可達 30 分鐘的精細程度)。如需詳細資訊，請參閱 [Amazon Redshift 定價](#)。

保持帳單可預測性的 Amazon Redshift Serverless 最佳實務

以下是有助於保持帳單一致性的最佳實務和內建設定。

- 確實結束每個交易。當您使用 BEGIN 開始交易時，請務必也將其 END。
- 使用最佳實務錯誤處理來適當地回應錯誤並結束每個交易。盡量減少開啟的交易有助於避免不必要的 RPU 用量。
- 使用 SESSION TIMEOUT 來協助結束開啟的交易和閒置的工作階段。其會導致任何閒置或非作用中時間超過 3600 秒 (1 小時) 的工作階段逾時。其會導致任何保持開啟和非作用中狀態超過 21600 秒 (6 小時) 的交易逾時。您可以針對特定使用者明確變更此逾時設定，例如當您想要為長時間執行的查詢保持工作階段開啟狀態時。[CREATE USER](#) 主題會顯示如何調整使用者的 SESSION TIMEOUT。

- 在大多數情況下，建議您不要延長 SESSION TIMEOUT 值，除非您有特別需要這麼做的使用案例。如果工作階段仍處於閒置狀態，具有開啟中的交易，則可能會導致系統使用 RPU，直到工作階段關閉為止。這會導致不必要的成本。
- Amazon Redshift Serverless 的執行中查詢時間上限為 86,399 秒 (24 小時)。開啟中交易的非作用中期間上限為六小時，超過之後，Amazon Redshift Serverless 就會結束與交易相關聯的工作階段。如需詳細資訊，請參閱 [Amazon Redshift Serverless 物件的配額](#)。

連線至 Amazon Redshift Serverless

在設定 Amazon Redshift Serverless 執行個體後，便可以使用以下概述的各種方法連線到該執行個體。如果您有多個團隊或專案，並且想要分開管理成本，則可以使用不同的 AWS 帳戶。

如需提供 Amazon Redshift 無伺服器位 AWS 區域 置清單，請參閱中列出的 [Redshift 無伺服器 API 端點](#)。Amazon Web Services 一般參考

Amazon Redshift 無伺服器連線到您目前環境中的 AWS 帳戶 無伺服器環境。AWS 區域 Amazon Redshift Serverless 會在連接埠範圍為 5431 至 5455 和 8191 至 8215 的連接埠範圍內的 VPC 中執行。預設值為 5439。目前，您只能使用 API 操作 UpdateWorkgroup 和操作更改端口 update-workgroup。AWS CLI

連線至 Amazon Redshift Serverless

您可以使用下列語法連線到 Amazon Redshift Serverless 中的資料庫 (名為 dev)。

```
workgroup-name.account-number.aws-region.redshift-serverless.amazonaws.com:port/dev
```

例如，下列連線字串會指定區域 us-east-1。

```
default.123456789012.us-east-1.redshift-serverless.amazonaws.com:5439/dev
```

透過 JDBC 驅動程式連線至 Amazon Redshift Serverless

您可以使用下列其中一種方法，透過 Amazon RedShift 所提供的 JDBC 驅動程式第 2 版驅動程式，以偏好的 SQL 用戶端連線至 Amazon Redshift Serverless。

若要透過 JDBC 驅動程式 2.1.x 版或更新版本，使用登入憑證驗證資料庫以進行連線，請使用下列語法。您可以選擇是否使用連接埠號碼；如果未包含，Amazon Redshift Serverless 會預設為連接埠號碼

5439。您可以變更為 5431 至 5455 或 8191 至 8215 之連接埠範圍內的其他連接埠。若要變更無伺服器端點的預設連接埠，請使用 AWS CLI 和 Amazon Redshift API。

```
jdbc:redshift://workgroup-name.account-number.aws-region.redshift-serverless.amazonaws.com:5439/dev
```

例如，下列連線字串會指定工作群組預設值、帳戶 ID 123456789012 以及 us-east-2 區域。

```
jdbc:redshift://default.123456789012.us-east-2.redshift-serverless.amazonaws.com:5439/dev
```

若要使用 JDBC 驅動程式 2.1.x 版或更新版本來與 IAM 連線，請使用下列語法。您可以選擇是否使用連接埠號碼；如果未包含，Amazon Redshift Serverless 會預設為連接埠號碼 5439。您可以變更為 5431 至 5455 或 8191 至 8215 之連接埠範圍內的其他連接埠。若要變更無伺服器端點的預設連接埠，請使用 AWS CLI 和 Amazon Redshift API。

```
jdbc:redshift:iam://workgroup-name.account-number.aws-region.redshift-serverless.amazonaws.com:5439/dev
```

例如，下列連線字串會指定工作群組預設值、帳戶 ID 123456789012 以及 us-east-2 區域。

```
jdbc:redshift:iam://default.123456789012.us-east-2.redshift-serverless.amazonaws.com:5439/dev
```

若為 ODBC，請使用下列語法。

```
Driver={Amazon Redshift (x64)}; Server=workgroup-name.account-number.aws-region.redshift-serverless.amazonaws.com; Database=dev
```

如果您使用的是 2.1.0.9 之前的 JDBC 驅動程式版本，並使用 IAM 來連線，則需要使用下列語法。

```
jdbc:redshift:iam://redshift-serverless-<name>:aws-region/database-name
```

例如，下列連接字串指定工作群組預設值和 AWS 區域 us-east-1。

```
jdbc:redshift:iam://redshift-serverless-default:us-east-1/dev
```

如需驅動程式的相關資訊，請參閱在 [Amazon Redshift 中設定連線](#)。

尋找 JDBC 和 ODBC 連線字串

若要使用 SQL 用戶端工具來連線至工作群組，您必須有 JDBC 或 ODBC 連線字串。您可以在 Amazon Redshift Serverless 主控台的工作群組詳細資訊頁面上找到連線字串。

尋找工作群組的連線字串

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽選單上，選擇 Redshift Serverless。
3. 在導覽選單上，選擇工作群組組態，然後從清單中選擇工作群組名稱以開啟其詳細資訊。
4. General information (一般資訊) 區段中提供了 JDBC URL 和 ODBC URL 連線字串，以及其他詳細資訊。每個字串均以工作群組執行的 AWS 區域為基礎。選擇適當連線字串旁邊的圖示以複製連線字串。

使用資料 API 連線至 Amazon Redshift Serverless

您也可以使用 Amazon Redshift 資料 API 來連線至 Amazon Redshift Serverless。在 AWS CLI 呼叫中 `workgroup-name` 使用 `cluster-identifier` 參數而不是參數。

如需資料 API 的相關資訊，請參閱 [使用 Amazon Redshift 資料 API](#)。如需 [使用 Python 呼叫資料 API 的範例程式碼和其他範例](#)，請參閱 [Redshift 資料 API 入門 quick-start](#) 並 [use-cases](#) 查看。GitHub

使用 SSL 連線到 Amazon Redshift Serverless

設定與 Amazon Redshift Serverless 的安全連線

為了支援 SSL 連線，Redshift 無伺服器會為每個工作群組建立並安裝 [AWS Certificate Manager \(ACM\)](#) 核發的 SSL 憑證。ACM 憑證受到大多數作業系統、網頁瀏覽器和用戶端公開信任。如果您的 SQL 用戶端或應用程式使用 SSL 連線到 Redshift 無伺服器 `require`，`verify-ca` 且 `sslmode` 連線選項設為、或，您可能需要下載憑證服務包。`verify-full` 如果您的用戶端需要憑證，Redshift 無伺服器會提供組合憑證，如下所示：

- 請從以下位置下載套件 [amazon-trust-ca-bundle](#)。 <https://s3.amazonaws.com/redshift-downloads/>
 - 預期的 MD5 檢查總和碼為 418dea9b6d5d5de7a8f1ac42e164cdcf。
 - sha256 檢查總和碼為 36dba8e4b8041cd14b9d60158893963301bcbb92e1c456847784de2acb5bd550。

請勿使用位於 <https://s3.amazonaws.com/redshift-downloads/redshift-ca-bundle.crt> 的先前憑證套件。

- 在中國 AWS 區域，請從以下位置下載該軟件包 [amazon-trust-ca-bundle. redshift-downloads-cn](https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn) <https://s3.cn-north-1.amazonaws.com.cn/>
 - 預期的 MD5 檢查總和碼為 418dea9b6d5d5de7a8f1ac42e164cdcf。
 - sha256 檢查總和碼為 36dba8e4b8041cd14b9d60158893963301bcbb92e1c456847784de2acb5bd550。

請勿使用位於 <https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/redshift-ca-bundle.crt> 和 <https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/redshift-ssl-ca-cert.pem> 的先前憑證套件。

Important

Redshift 無伺服器已經改變了 SSL 憑證的管理方式。您可能需要更新目前的信任根 CA 憑證，才能繼續使用 SSL 連線到您的工作群組。如需 SSL 連線之 ACM 憑證的詳細資訊，請參閱 [將 SSL 連線轉換為使用 ACM 憑證](#)。

依預設，無論是否使用 SSL，工作群組資料庫都會接受連線。

若要建立僅接受 SSL 連線的新工作群組，請使用 `create-workgroup` 指令並將 `require_ssl` 參數設定為 `true`。若要使用下列範例，請 *yourNamespaceName* 以命名空間的名稱取代，並 *yourWorkgroupName* 以工作群組的名稱取代。

```
aws redshift-serverless create-workgroup \  
--namespace-name yourNamespaceName \  
--workgroup-name yourWorkgroupName \  
--config-parameters parameterKey=require_ssl,parameterValue=true
```

若要將現有工作群組更新為僅接受 SSL 連線，請使用 `update-workgroup` 指令並將 `require_ssl` 參數設定為 `true`。請注意，Redshift 無伺服器會在 `require_ssl` 您更新參數時重新啟動工作群組。若要使用下列範例，請 *yourWorkgroupName* 以工作群組的名稱取代。

```
aws redshift-serverless update-workgroup \  
--workgroup-name yourWorkgroupName \  
--config-parameters parameterKey=require_ssl,parameterValue=true
```

Amazon Redshift 支援 Elliptic Curve Diffie—Hellman Ephemeral (ECDHE) 金鑰協議通訊協定。使用 ECDHE 時，用戶端和伺服器各有橢圓曲線公有-私有金鑰對，用於透過不安全通道建立共用秘密。您不需要在 Amazon Redshift 中設定任何項目來啟用 ECDHE。如果您從 SQL 用戶端工具連線，而此工具使用 ECDHE 來加密用戶端和伺服器之間的通訊，Amazon Redshift 會使用提供的密碼清單來建立適當的連線。如需詳細資訊，請參閱 Wikipedia 上的 [Elliptic curve diffie—hellman](#) 和 OpenSSL 網站上的 [Ciphers](#)。

設定與 Amazon Redshift 無伺服器的 FIPS 相容 SSL 連線

若要建立使用 FIPS 相容 SSL 連線的新工作群組，請使用 `create-workgroup` 指令並將 `use_fips_ssl` 參數設定為 `true`。若要使用下列範例，請將 `yourNamespaceName` 以命名空間的名稱取代，並將 `yourWorkgroupName` 以工作群組的名稱取代。

```
aws redshift-serverless create-workgroup \  
--namespace-name yourNamespaceName \  
--workgroup-name yourWorkgroupName \  
--config-parameters parameterKey=use_fips_ssl,parameterValue=true
```

若要更新既有工作群組以使用 FIPS 相容的 SSL 連線，請使用 `update-workgroup` 指令並將 `use_fips_ssl` 參數設定為 `true`。請注意，Redshift 無伺服器會在您更新參數時重新啟動工作群組。若要使用下列範例，請將 `yourWorkgroupName` 以工作群組的名稱取代。

```
aws redshift-serverless update-workgroup \  
--workgroup-name yourWorkgroupName \  
--config-parameters parameterKey=use_fips_ssl,parameterValue=true
```

如需設定無伺服器以使用 FIPS 相容連線的詳細資訊，請參閱 Amazon Redshift 資料庫開發人員指南中的 [use_fips_ssl](#)。

從 Amazon Redshift 受管 VPC 端點連線至 Amazon Redshift Serverless

從其他 VPC 端點連線至 Amazon Redshift Serverless

如需為 Amazon Redshift 無伺服器工作群組設定或設定受管虛擬私人雲端端點的詳細資訊，請參閱 [使用 RedShift 管理的 VPC 端點](#)。

從其他帳戶或區域中的 Redshift VPC 端點連線至 Amazon Redshift Serverless

從跨 VPC 端點連線至 Amazon Redshift Serverless

Amazon Redshift Serverless 會佈建在 VPC 中。您可以授予對其他帳戶中 VPC 的存取權，以存取帳戶中的 Amazon Redshift Serverless。這類似於來自受管理 VPC 端點的連線，但在此情況下，連線起始於另一個帳戶中的資料庫用戶端。您可以執行幾項作業：

- 資料庫擁有者可以將包含 Amazon Redshift Serverless 的 VPC 的存取權授予相同區域中的其他帳戶。
- 資料庫擁有者可以撤銷 Amazon Redshift Serverless 存取權。

跨帳戶存取的主要優點是允許更輕鬆的資料庫協同作業。不必在包含資料庫的帳戶中佈建使用者即可存取資料庫，這樣可減少設定步驟並節省時間。

授予對其他帳戶中 VPC 的存取

若要授予存取權或變更允許的存取權，授予者需要具有下列權限的已指派權限政策：

- 無紅移伺服器：PutResourcePolicy
- 無紅移伺服器：GetResourcePolicy
- 無紅移伺服器：DeleteResourcePolicy
- ec2：CreateVpcEndpoint
- ec2：ModifyVpcEndpoint

您可能需要 AWS 受管理策略中指定的其他權限 AmazonRedshiftFullAccess。如需詳細資訊，請參閱[授予 Amazon Redshift Serverless 的權限](#)。

承授者需要具有下列權限的已指派權限政策：

- 無紅移伺服器：ListWorkgroups
- 無紅移伺服器：CreateEndpointAccess
- 無紅移伺服器：UpdateEndpointAccess
- 無紅移伺服器：GetEndpointAccess

- 無紅移伺服器：ListEndpointAccess
- 無紅移伺服器：DeleteEndpointAccess

我們建議的最佳實務是，將許可政策附加到 IAM 角色，然後根據需要將其指派給使用者和群組。如需詳細資訊，請參閱 [Amazon Redshift 中的身分和存取管理](#)。

這是用來設定跨 VPC 存取權的範例資源政策：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CrossAccountCrossVPCAccess",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "123456789012",
          "234567890123"
        ]
      },
      "Action": [
        "redshift-serverless:CreateEndpointAccess",
        "redshift-serverless:UpdateEndpointAccess",
        "redshift-serverless>DeleteEndpointAccess",
        "redshift-serverless:GetEndpointAccess"
      ],
      "Condition": {
        "ArnLike": {
          "redshift-serverless:AuthorizedVpc": [
            "arn:aws:ec2:us-east-1:123456789012:vpc/*",
            "arn:aws:ec2:us-east-1:234567890123:vpc/vpc-456",
            "arn:aws:ec2:us-east-1:234567890123:vpc/vpc-987"
          ]
        }
      }
    }
  ]
}
```

本節接下來的程序假設執行這些權限的使用者具有適當的指派權限，例如，透過具有列出權限的已指派 IAM 角色。這些程序還假設工作群組具有附加適當資源權限的 IAM 角色。

使用主控台授予其他帳戶的 VPC 存取權

此程序顯示當您是資料庫擁有者且想要授予存取權時，用於設定資料庫存取權的步驟。

從擁有者帳戶授予存取權

1. 在 Amazon Redshift Serverless 工作群組的屬性中，在資料存取索引標籤上有一份名為已授予的帳戶清單。它會顯示授予工作群組存取權的帳戶和 VPC。找到清單，然後選擇授予存取權，將帳戶新增至清單。
2. 出現一個視窗，您可以在其中新增承授者資訊。輸入 AWS 帳戶的 ID，其為您要授予存取權的帳戶的 12 位數 ID。
3. 授予承授者的所有 VPC 或特定 VPC 的存取權。如果僅授予特定 VPC 的存取權，則可以透過輸入每個 VPC 並選擇新增 VPC 來為這些 VPC 新增 ID。
4. 完成後，選擇儲存變更。

當您儲存變更時，帳戶會出現在已授予的帳戶清單中。此項目會顯示帳戶 ID 和授予存取權的 VPC 清單。

資料庫擁有者也可以撤銷帳戶的存取權。您可以隨時撤消存取權。

撤銷帳戶存取權

1. 您可以從授予的帳戶清單開始。首先，選取一或多個帳戶。
2. 選擇撤銷存取權。

授予存取權之後，承授者的資料庫管理員可以檢查主控台，以判斷他們是否具有存取權。

使用主控台確認已授予存取其他帳戶的存取權

1. 在 Amazon Redshift Serverless 工作群組屬性的資料存取索引標籤上，有一份名為授權的帳戶清單。它顯示可以從此工作組存取的帳戶。承授者無法使用工作群組的端點 URL 直接存取工作群組。若要存取工作組，身為承授者的您移至端點區段，然後選擇建立端點。
2. 然後，身為承授者，您可以提供端點名稱和 VPC 來存取工作群組。
3. 成功建立端點後，它會出現在端點區段中，並且有端點 URL。您可以使用此端點 URL 來存取工作群組。

使用 CLI 命令授予其他帳戶的存取權

授予存取權的帳戶必須先授予其他帳戶的存取權，才能使用連線 `put-resource-policy`。資料庫擁有者可以呼叫 `put-resource-policy` 以授權其他帳戶，建立與工作群組的連線。接著，承授者帳戶便可透過其允許的 VPC，使用 `create-endpoint-authorization` 以建立與工作群組的連線。

以下顯示的內容適用於 `put-resource-policy`，您可以呼叫這些內容以允許存取特定帳戶和 VPC。

```
aws redshift-serverless put-resource-policy
--resource-arn <value>
--policy <value>
```

呼叫命令後，您可以呼叫 `get-resource-policy`，並指定 `resource-arn` 以查看允許哪些帳戶和 VPC 存取資源。

承授者可以進行以下呼叫。它顯示有關授予存取權的資訊。具體而言，它會傳回一份包含授予存取權的 VPC 清單。

```
aws redshift-serverless list-workgroups
--owner-account <value>
```

這樣做的目的是讓承授者從授予帳戶取得有關端點授權的資訊。`owner-account` 是共用帳戶。當您執行此項目時，它會傳回每個工作群組的 `CrossAccountVpcs`，即為允許的 VPC 清單。以下內容展示了工作群組可用的所有屬性以做為參考：

```
Output: workgroup (Object)
workgroupId String,
workgroupArn String,
workgroupName String,
status: String,
namespaceName: String,
baseCapacity: Integer, (Not-applicable)
enhancedVpcRouting: Boolean,
configParameters: List,
securityGroupIds: List,
subnetIds: List,
endpoint: String,
publiclyAccessible: Boolean,
creationDate: Timestamp,
```

```
port: Integer,  
CrossAccountVpcs: List
```

Note

提醒您，[叢集重新定位](#)不是設定其他 Redshift 網路功能的先決條件。您也不需要將其開啟才能啟用下列功能：

- 從跨帳戶或跨區域 VPC 連線至 Redshift — 您可以從一個 AWS 虛擬私人雲端 (VPC) 連線到包含 Redshift 資料庫的另一個虛擬私有雲端 (VPC)，如本節所述。
- 設定自訂網域名稱 — 您可以為 Amazon Redshift 叢集或 Amazon Redshift Serverless 工作群組建立自訂網域名稱 (也稱為自訂 URL)，以使端點名稱更加簡單易記。如需詳細資訊，請參閱[使用自訂網域名稱來進行用戶端連線](#)。

為 Amazon Redshift Serverless 設定適當的網路流量設定

在可公開存取時連線到 Amazon Redshift Serverless

您可以在[具有預設或自訂安全性群組組態的「公用存取性」](#)中找到設定網路流量設定的指示。這包括叢集可公開存取的使用案例。

在無法公開存取時連線到 Amazon Redshift Serverless

如需設定網路流量設定的指示，請參閱[具有預設或自訂安全性群組組態的私人存取功能](#)。這包括叢集無法供網際網路使用的使用案例。

在 Amazon Redshift Serverless 中定義要向聯合身分使用者授予的資料庫角色

您可以在組織中定義角色，以此決定要在 Amazon Redshift Serverless 中授予哪些資料庫角色。如需詳細資訊，請參閱 [在 Amazon Redshift Serverless 中定義要向聯合身分使用者授予的資料庫角色](#)。

其他資源

如需 Amazon Redshift Serverless 安全連線的相關資訊 (包括授予許可、授權其他服務的存取權，以及建立 IAM 角色)，請參閱 [Amazon Redshift Serverless 中的身分和存取管理](#)。

在 Amazon Redshift Serverless 中定義要向聯合身分使用者授予的資料庫角色

當您是組織的一分子時，您會有一組相關聯的角色。例如，你有你工作職能的角色，如程式設計人員和管理員。您的角色決定了您可以存取哪些應用程式和資料。大多數組織會使用身分提供者 (例如 Microsoft Active Directory) 將角色指派給使用者和群組。使用角色來控制資源存取的情況變多了，因為組織不必花太多時間管理個別使用者。

Amazon Redshift Serverless 最近引進了角色型存取控制功能。您可以使用資料庫角色來保護對於資料和物件 (例如結構描述或資料表) 的存取。或者，您也可以使用角色來定義一組提升的許可，例如針對系統監控或資料庫管理員來定義。但在向資料庫角色授予資源許可後，還要再進行一個步驟，那就是將使用者的角色從組織連線到資料庫角色。您可以透過執行 SQL 陳述式，在每個使用者初次登入時向其指派資料庫角色，但這需要大量工作。比較簡單的方法是定義要向其授予的資料庫角色，並將其傳遞至 Amazon Redshift Serverless。這麼做的好處是可以簡化初始登入程序。

您可以使用 `GetCredentials` 將角色傳遞至 Amazon Redshift Serverless。當使用者第一次登入 Amazon Redshift Serverless 資料庫時，系統會建立相關聯的資料庫使用者，並將其對應至相符的資料庫角色。本主題會詳細說明將角色傳遞至 Amazon Redshift Serverless 的機制。

傳遞資料庫角色有幾個主要的使用案例：

- 當使用者透過第三方身分提供者 (一般皆已設定聯合功能) 來登入，並透過工作階段標籤傳遞角色時。
- 當使用者透過 IAM 登入憑證來登入，並透過標籤索引鍵和值傳遞其角色時。

如需角色型存取控制的相關資訊，請參閱 [角色型存取控制 \(RBAC\)](#)。

設定資料庫角色

您必須先在資料庫中設定資料庫角色，並向其授予適當的資料庫資源許可，然後才能將角色傳遞至 Amazon Redshift Serverless。例如，在簡單的案例中，您可以建立名為 `sales` 的資料庫角色，並向其授予有銷售資料之資料表的查詢存取權。如需如何建立資料庫角色和授予許可的相關資訊，請參閱 [CREATE ROLE](#) 和 [GRANT](#)。

定義要向聯合身分使用者授予之資料庫角色的使用案例

以下各節概述了將資料庫角色傳遞至 Amazon Redshift Serverless 可以簡化資料庫資源存取方式的幾個使用案例。

使用身分提供者來登入

第一個使用案例假設您的組織在身分與存取管理服務中具有使用者身分。這項服務可以是基於雲，例 JumpCloud 如 Okta，或內部部署，如 Microsoft 活動目錄。目標是在使用者登入用戶端 (例如查詢編輯器 V2) 或使用 JDBC 用戶端時，自動將使用者得自身分提供者的角色對應至資料庫角色。若要進行這方面的設定，您必須先完成幾個組態任務。這些索引標籤包括以下項目：

1. 使用信任關係設定與身分提供者 (IdP) 的聯合整合。這是先決條件。當您完成設定時，身分提供者便會負責透過 SAML 聲明驗證使用者並提供登入憑證。如需詳細資訊，請參閱[將第三方 SAML 解決方案提供者與 AWS](#)。您也可以[在將 Amazon Redshift 查詢編輯器 V2 的存取與 Active Directory Federation Services \(AD FS\) 聯合](#)或[將 Amazon Redshift 查詢編輯器 v2 的單一登入存取與 Okta 聯合](#)中找到更多資訊。
2. 使用者必須具有下列政策許可：
 - `GetCredentials` — 提供憑證以供臨時授權登入 Amazon Redshift Serverless。
 - `sts:AssumeRoleWithSAML` — 提供將企業識別身分存放區或目錄繫結至以角色為基礎 AWS 的存取的機制。
 - `sts:TagSession` — 身分提供者主體上的標籤工作階段動作許可。

在這種情況下，`AssumeRoleWithSAML` 會透過 SAML 驗證回應，針對已驗證過的使用者傳回一組安全憑證。此作業提供一種機制，可將識別身分存放區或目錄連結至以角色為基礎的 AWS 存取，而無需使用者特定認證。對於具有 `AssumeRoleWithSAML` 許可的使用者，身分提供者會負責管理用來傳遞角色資訊的 SAML 聲明。

我們建議的最佳實務是，將許可政策連接到 IAM 角色，然後根據需要將其指派給使用者和群組。如需詳細資訊，請參閱 [Amazon Redshift 中的身分和存取管理](#)。

3. 您可以 `role1:role2` 格式的冒號分隔角色值來設定 `RedshiftDbRoles` 標籤。例如，`manager:engineer`。這些項目可以從身分提供者中所設定的 `session-tag` 實作來擷取。SAML 驗證請求會以程式設計方式傳遞角色。如需傳遞工作階段標籤的相關資訊，請參閱[在 AWS STS 中傳遞工作階段標籤](#)。

如果您傳遞的角色名稱不存在於資料庫中，系統會將其忽略。

在這個使用案例中，當使用者使用聯合身分登入時，系統會透過工作階段標籤的索引鍵和值在授權請求中傳遞其角色。緊接在授權之後，`GetCredentials` 便會將角色傳遞至資料庫。連線成功後，資料庫角色便會對應，而且使用者可以執行與其角色對應的資料庫任務。操作的基本部分是系統會在初始授權請求中向 `RedshiftDbRoles` 工作階段標籤指派角色。如需有關傳遞工作階段標籤的詳細資訊，請參閱[使用 AssumeRoleWith SAML 傳遞工作階段標籤](#)

使用 IAM 憑證進行登入

在第二個使用案例中，我們可以向使用者傳遞角色，讓其透過 IAM 憑證存取資料庫的用戶端應用程式。

1. 在此情況下登入的使用者必須獲派下列動作的政策許可：

- `tag:GetResources` — 傳回與指定標籤相關聯的已標記資源。
- `tag:GetTagKeys` — 傳回目前使用中的標籤索引鍵。

我們建議的最佳實務是，將許可政策連接到 IAM 角色，然後根據需要將其指派給使用者和群組。如需詳細資訊，請參閱 [Amazon Redshift 中的身分和存取管理](#)。

2. 我們也需要用來存取資料庫服務 (例如 Amazon Redshift Serverless) 的允許許可。

3. 對於此使用案例，請在中配置角色的標籤值 AWS Identity and Access Management。您可以選擇編輯標籤並建立名為 RedshiftDbRoles 的標籤鍵，其中包含角色的隨附標籤值字串。例如，`manager:engineer`。

當使用者登入時，系統會將其角色新增至授權請求並傳遞給資料庫。其會對應至現有的資料庫角色。

其他資源

如使用案例所述，您可以設定 IdP 和 AWS 之間的信任關係。如需詳細資訊，請參閱 [使用依賴方信任設定您的 SAML 2.0 IdP 並新增宣告](#)。

Amazon Redshift Serverless 中的身分和存取管理

存取 Amazon Redshift 需要 AWS 可用來驗證您的請求的登入資料。這些登入資料必須具有存取 AWS 資源的許可，例如 Amazon Redshift 無伺服器。

以下各節提供有關如何使用 AWS Identity and Access Management (IAM) 和 Amazon Redshift 的詳細資訊，透過控制可存取資源的人員來協助保護資源的安全。如需詳細資訊，請參閱 [Amazon Redshift 中的身分和存取管理](#)。

授予許可給 Amazon Redshift Serverless

若要存取其他 AWS 服務，Amazon Redshift 無伺服器需要許可。

授權 Amazon Redshift 無伺服器為您存取其他 AWS 服務

某些 Amazon Redshift 功能需要 Amazon Redshift 代表您存取其他 AWS 服務。為了讓 Amazon Redshift Serverless 執行個體為您服務，請為其提供安全憑證。提供安全登入資料的慣用方法是指定 AWS Identity and Access Management (IAM) 角色。您也可以透過 Amazon Redshift 主控台建立 IAM 角色，並將其設定為預設值。如需詳細資訊，請參閱 [建立 IAM 角色做為 Amazon Redshift 的預設角色](#)。

若要存取其他 AWS 服務，請建立具有適當權限的 IAM 角色。您還需要將該角色與 Amazon Redshift Serverless 相關聯。此外，您可以在執行 Amazon Redshift 命令時指定角色的 Amazon Resource Name (ARN)，或指定關鍵字 default。

在 <https://console.aws.amazon.com/iam/> 中變更 IAM 角色的信任關係時，請確定該角色包含 redshift-serverless.amazonaws.com 和 redshift.amazonaws.com 作為主要服務名稱。如需如何管理 IAM 角色以代表您存取其他 AWS 服務的相關資訊，請參閱 [授權 Amazon Redshift 代表您訪問其他 AWS 服務](#)。

建立 IAM 角色做為 Amazon Redshift 的預設角色

當您透過 Amazon Redshift 主控台建立 IAM 角色時，Amazon Redshift 會以程式設計方式在您的 AWS 帳戶 Amazon Redshift 也會自動將現有的 AWS 受管政策附加到這些政策。此方法意味著您可以保留在 Amazon Redshift 主控台內，而不必切換到 IAM 主控台來建立角色。

您透過主控台為叢集建立的 IAM 角色會自動附加 AmazonRedshiftAllCommandsFullAccess 受管政策。這個 IAM 角色可讓 Amazon Redshift 針對 IAM 帳戶中的資源複製、卸載、查詢和分析 AWS 資料。相關命令包括 COPY、UNLOAD、CREATE EXTERNAL FUNCTION、CREATE EXTERNAL TABLE、CREATE EXTERNAL SCHEMA、CREATE MODEL 和 CREATE LIBRARY。如需如何建立 IAM 角色作為 Amazon Redshift 預設值的相關資訊，請參閱 [建立 IAM 角色做為 Amazon Redshift 的預設角色](#)。

若要開始為 Amazon Redshift 建立 IAM 角色做為預設值，請開啟 AWS Management Console，選擇 Amazon Redshift 主控台，然後在功能表中選擇 Redshift 無伺服器角色。您可以從無伺服器儀表板建立新工作群組。建立步驟會引導您選取 IAM 角色或設定新的 IAM 角色。

當您擁有現有的 Amazon Redshift 無伺服器工作群組且想要為其設定 IAM 角色時，請開啟 AWS Management Console 選擇 Amazon Redshift 主控台，然後選擇紅移無伺服器。在 Amazon Redshift 無伺服器主控台上，為現有工作群組選擇命名空間組態。在 [安全性和加密] 下，您可以編輯權限。

指派 IAM 角色給命名空間

每個 IAM 角色都是具有許可政策的 AWS 身分識別，可決定每個角色可以在其中執行哪些動作 AWS。角色旨在可由任何需要它的使用者擔任。此外，每個命名空間都是物件的集合，例如資料表和結構描述，以及使用者。當您使用 Amazon Redshift Serverless 時，您可以將多個 IAM 角色與命名空間相關聯。這樣可以讓您更輕鬆地為資料庫物件集合建構適當的許可，以便角色可以對內部和外部資料執行動作。例如，您因此可以在 Amazon Redshift 資料庫中執行 COPY 命令，以從 Amazon S3 擷取資料並填入 Redshift 資料表。

您可以使用主控台將多個角色與命名空間相關聯，如本節先前所述。您也可以使用 API 命令 `CreateNamespace` 或 CLI 命令 `create-namespace`。使用 API 或 CLI 命令時，您可以透過為 `IAMRoles` 填入一或多個角色，將 IAM 角色指派給命名空間。具體而言，您會將特定角色的 ARN 新增至集合。

管理命名空間關聯的 IAM 角色

在上，AWS Management Console 您可以管理中角色的權限原則 AWS Identity and Access Management。您可以使用命名空間組態下的可用設定來管理命名空間的 IAM 角色。如需命名空間及其在 Amazon Redshift Serverless 中的使用方式的相關資訊，請參閱 [Amazon Redshift Serverless 工作群組和命名空間的概觀](#)。

Amazon Redshift IAM 憑證入門

當您第一次登入 Amazon Redshift 主控台並首次嘗試使用 Amazon Redshift Serverless 時，建議您使用已附加 IAM 角色，且該角色具有所需政策的使用者身分來登入。在您開始建立 Amazon Redshift Serverless 執行個體之後，Amazon Redshift 會記錄您用來登入的 IAM 角色名稱。您可以使用相同的憑證登入 Amazon Redshift 主控台和 Amazon Redshift Serverless 主控台。

在建立 Amazon Redshift Serverless 執行個體時，您可以建立資料庫。使用查詢編輯器 v2 透過暫時憑證選項連線至資料庫。

若要新增會針對資料庫保留下來的新管理員使用者名稱和密碼，請選擇自訂管理員使用者憑證，然後輸入新的管理員使用者名稱和管理員使用者密碼。

若要開始使用 Amazon Redshift Serverless，並首次在主控台中建立工作群組和命名空間，請使用已附加許可政策的 IAM 角色。請確定此角色具有管理員許可 `arn:aws:iam::aws:policy/AdministratorAccess` 或已附加至 IAM 政策的完整 Amazon Redshift 許可 `arn:aws:iam::aws:policy/AmazonRedshiftFullAccess`。

下列案例概述您開始使用 Amazon Redshift Serverless 主控台時，Amazon Redshift Serverless 會如何使用您的 IAM 憑證：

- 如果您選擇使用預設設定 — Amazon Redshift Serverless 會將您目前的 IAM 身分轉譯為資料庫超級使用者。您可以將相同的 IAM 身分與 Amazon Redshift Serverless 主控台搭配使用，以在 Amazon Redshift Serverless 的資料庫中執行超級使用者動作。
- 如果您選擇自訂設定而未指定管理員使用者名稱和密碼，則 Amazon Redshift Serverless 會使用您目前的 IAM 憑證作為預設管理員使用者憑證。
- 如果您選擇自訂設定並指定管理員使用者名稱和密碼 Amazon Redshift Serverless — Amazon Redshift Serverless 會將您目前的 IAM 身分轉譯為資料庫超級使用者。Amazon Redshift Serverless 也會建立另一個長期登入使用者名稱和密碼組作為超級使用者。您可以使用目前的 IAM 身分或已建立的使用者名稱和密碼組，以超級使用者身分登入資料庫。

使用資料庫角色許可管理對 Amazon Redshift Serverless 資料庫物件的存取

此程序會說明如何透過 [Amazon Redshift 資料庫角色](#) 授予用來查詢資料表的許可。角色會透過附加至 IAM 中使用者的標籤來指派，並在使用者登入時傳遞至 Amazon Redshift。這是在 [Amazon Redshift Serverless 中定義要向聯合身分使用者授予的資料庫角色](#) 中的概念範例說明。完成這些步驟的好處是，您可以將使用者與資料庫角色相關聯，避免為每個資料庫物件設定其許可。它可讓您更輕鬆地管理使用者查詢、修改或新增資料到資料表以及執行其他動作的能力。

此程序假設您已經設定 Amazon Redshift Serverless 資料庫，而且您可以在資料庫中授予許可。它還假設您具有在 AWS 主控台中建立 IAM 使用者、建立 IAM 角色以及指派政策許可的許可。

1. 使用 IAM 主控台建立 IAM 使用者 稍後，您會使用此使用者連線到資料庫。
2. 使用查詢編輯器 v2 或其他 SQL 用戶端建立 Redshift 資料庫角色。如需建立資料庫角色的相關資訊，請參閱 [CREATE ROLE](#)。

```
CREATE ROLE urban_planning;
```

查詢 [SVV_ROLES](#) 系統檢視，以檢查角色是否已建立。它也會傳回系統角色。

```
SELECT * from SVV_ROLES;
```

3. 授予您建立的資料庫角色，以便從資料表中選取。(您建立的 IAM 使用者最終會透過資料庫角色登入並從資料表中選取記錄。) 下列程式碼範例中的角色名稱和資料表名稱為範例。這裡會授予從名為 `cities` 的資料表中進行選取的許可。

```
GRANT SELECT on TABLE cities to ROLE urban_planning;
```

4. 使用 AWS Identity and Access Management 主控台建立 IAM 角色。此角色會授予使用查詢編輯器 v2 的許可。建立新的 IAM 角色，然後針對信任的實體類型選擇 AWS 帳戶。然後選擇此帳戶。為該角色提供下列政策許可：
 - AmazonRedshiftReadOnlyAccess
 - tag:GetResources
 - tag:GetTagKeys
 - sqlworkbench 的所有動作，包括 sqlworkbench:ListDatabases 和 sqlworkbench:UpdateConnection。
5. 在 IAM 主控台中，將具有索引鍵 RedshiftDbRoles 的標籤新增至您先前建立的 IAM 使用者。標籤的值應與您在第一個步驟中建立的資料庫角色相符。在範例中，值為 urban_planning。

完成這些步驟後，請指派 IAM 角色給您在 IAM 主控台中建立的使用者。當使用者使用查詢編輯器 v2 登入資料庫時，其在標籤中的資料庫角色名稱會傳遞至 Amazon Redshift 並與其相關聯。因此，其可以透過資料庫角色查詢適當的資料表。為了說明，此範例中的使用者可以透過 urban_planning 資料庫角色查詢 cities 資料表。

將佈建的叢集遷移至 Amazon Redshift Serverless

若要從已佈建的叢集遷移至 Amazon Redshift Serverless，請參閱下列步驟。

建立已佈建叢集的快照

若要將資料從已佈建的叢集傳輸到 Amazon Redshift Serverless，請建立已佈建叢集的快照，然後在 Amazon Redshift Serverless 中還原快照。當您將已佈建叢集的快照還原到無伺服器命名空間時，Amazon Redshift 會自動將交錯索引鍵轉換為複合索引鍵。

Note

在將資料遷移到無伺服器工作群組之前，請先確保已佈建的叢集需求與您在 Amazon Redshift Serverless 中選擇的 RPU 數量相容。

建立已佈建叢集的快照

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。

2. 在導覽選單中，選擇叢集、快照，然後選擇建立快照。
3. 輸入快照定義屬性，然後選擇建立快照。可能要等一會兒才能使用此快照。

若要將已佈建叢集的快照還原至無伺服器命名空間：

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 從 Amazon Redshift 已佈建的叢集主控台開始，然後導覽至叢集、快照頁面。
3. 選擇要使用的快照。
4. 選擇還原快照、還原至無伺服器命名空間。
5. 選擇要作為快照還原目的地的命名空間。
6. 確認您要從快照還原。此動作會使用已佈建叢集中的資料取代無伺服器端點中的所有資料庫。選擇 Restore (還原)。

如需已佈建叢集快照的相關資訊，請參閱 [Amazon Redshift 快照](#)。

使用驅動程式連線至 Amazon Redshift Serverless

若要以偏好的 SQL 用戶端連線至 Amazon Redshift Serverless，您可以使用 Amazon RedShift 所提供的 JDBC 驅動程式第 2 版驅動程式。建議您使用 JDBC 驅動程式 2.1.x 版或更新版本進行連線。連接埠號碼是選用的。如果未包含，Amazon Redshift Serverless 會預設為連接埠號碼 5439。您可以變更為 5431 至 5455 或 8191 至 8215 之連接埠範圍內的其他連接埠。若要變更無伺服器端點的預設連接埠，請使用 AWS CLI 和 Amazon Redshift API。

若要尋找用於 JDBC、ODBC 或 Python 驅動程式的確切端點，請參閱 Amazon Redshift Serverless 中的工作群組組態。您也可以使用 Amazon Redshift 無伺服器 API 作業 `GetWorkgroup` 或作業 `get-workgroups` 來傳回 AWS CLI 作群組的相關資訊，然後進行連線。

使用密碼型驗證進行連線

若要使用密碼型驗證進行連線，請使用下列語法。

```
jdbc:redshift://<workgroup-name>.<account-number>.<aws-region>.redshift-serverless.amazonaws.com:5439/?username=enter a username&password=enter a password
```

若要使用 Amazon Redshift Python 驅動程式進行連線，請使用下列語法。

```
import redshift_connector
with redshift_connector.connect(
    host='<workgroup-name>.<account-number>.<aws-region>.redshift-
serverless.amazonaws.com',
    database='<database-name>',
    user='enter a user',
    password='enter a password'
    # port value of 5439 is specified by default
) as conn:
    pass
```

使用 IAM 進行連線

如果您偏好使用 IAM 進行登入，請使用下列驅動程式端點。此驅動程式端點可讓您連線到特定資料庫，並使用 Amazon Redshift Serverless [GetCredentials](#) API 操作。

```
jdbc:redshift:iam://<workgroup-name>.<account-number>.<aws-region>.redshift-
serverless.amazonaws.com:5439/<database-name>
```

此驅動程式端點不支援自訂 dbUser、dbGroup 和 auto-create。根據預設，驅動程式會在登入時自動建立資料庫使用者，並根據您在 IAM 中定義的群組將這些使用者指派給群組。注意：您在 IAM 中指定的群組名稱必須只包含小寫字母、數字、底線 ('_')、加號 ('+')、句點 (.)、at 符號 (@) 或連字號 ('-')。否則，驅動程式可能無法連線到 dbGroup。

確保您的 AWS 身分具有 RedshiftServerlessGetCredentials 動作的正確 IAM 政策。以下是 IAM 政策範例，授與 AWS 身分識別的正确許可以連線到 Amazon Redshift 無伺服器。如需 IAM 許可的相關資訊，請參閱 [新增 IAM 身分許可](#)。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Action": "redshift-serverless:GetCredentials",
      "Resource": "*"
    }
  ]
}
```

使用 IAM 與 dbUser 和 dbGroups 進行連線

如果您想要使用自訂 dbUser 和 dbGroups 連線選項，請使用下列驅動程式端點。與其他 Amazon Redshift Serverless 驅動程式端點一樣，此語法會在登入時自動建立資料庫使用者。此驅動程式端點會使用 Amazon Redshift Serverless [GetCredentials](#) API 操作。dbUser 必須以字母開頭、只能包含英數字元、底線 ('_')、加號 ('+')、句點 ('.')、at ('@') 或連字號 ('-')，且必須少於 128 個字元。dbGroups 只能包含小寫字母、數字、底線 ('_')、加號 ('+')、句點 ('.')、at 符號 ('@') 或連字號。

```
jdbc:redshift:iam://redshift-serverless-<workgroup-name>:<aws-region>/<database-name>
```

若要使用 Amazon Redshift Python 驅動程式進行連線，請使用下列語法。

```
import redshift_connector
with redshift_connector.connect(
    iam=True,
    host='<workgroup-name>.<account-number>.<aws-region>.redshift-
serverless.amazonaws.com',
    database='<database-name>',
    db_user='enter a user',
    password='enter a password',
    db_groups='<db-groups>'
    # port value of 5439 is specified by default
) as conn:
    pass
```

使用 ODBC 進行連線

若要使用 ODBC 進行連線，請使用下列語法。

```
Driver={Amazon Redshift (x64)}; Server=<workgroup-name>.<account-number>.<aws-
region>.redshift-serverless.amazonaws.com; Database=dev
```

使用 Amazon Redshift Serverless SDK

如果您使用 Amazon Redshift SDK 撰寫了任何管理指令碼，則必須使用新的 Amazon Redshift Serverless SDK 來管理 Amazon Redshift Serverless 和相關資源。如需可用 API 操作的相關資訊，請參閱《[Amazon Redshift Serverless API 參考指南](#)》。

Amazon Redshift Serverless 工作群組和命名空間的概觀

若要在 Amazon Redshift Serverless 中隔離工作負載並管理不同的資源，您可以建立命名空間和工作群組，並將儲存和運算資源分開管理。

Amazon Redshift Serverless 工作群組和命名空間的概觀

命名空間是資料庫物件和使用者的集合。儲存體相關的命名空間會將結構描述、資料表、使用者或 AWS Key Management Service 金鑰群組在一起，以便加密資料。儲存屬性包括管理員使用者的資料庫名稱和密碼、許可以及加密與安全。群組到命名空間底下的其他資源包括資料共用、復原點和用量限制。您可以使用 Amazon Redshift 無伺服器主控台、或針對特定資源的 AWS Command Line Interface Amazon Redshift 無伺服器 API 來設定這些儲存屬性。

工作群組是運算資源的集合。運算相關的工作群組會將運算資源 (例如 RPU、VPC 子網路群組和安全群組) 群組在一起。工作群組的屬性包括網路和安全設定。群組到工作群組底下的其他資源包括存取和用量限制。您可以使用 Amazon Redshift 無伺服器主控台、或亞馬遜 Redshift 無伺服器 API 來設定這些運算屬性。AWS Command Line Interface

您可以建立一或多個命名空間與工作群組。每個命名空間只能有一個與其相關聯的工作群組。相反地，每個工作群組只能與一個命名空間相關聯。

使用主控台來開始使用 Amazon Redshift Serverless

設定 Amazon Redshift Serverless 需要逐步完成數個組態步驟。當您遵循步驟來設定 Amazon Redshift Serverless 時，您會建立命名空間和工作群組，並讓其彼此建立關聯。若要使用 Amazon Redshift Serverless 主控台開始設定 Amazon Redshift Serverless 組態，您可以選擇開始使用 Amazon Redshift Serverless 以設定 Amazon Redshift Serverless 並開始與其互動。您可以選擇具有預設設定的環境以加快設定速度，或根據組織的要求明確進行設定。在此過程中，您會指定工作群組和命名空間的設定。

在設定環境後，[工作群組屬性](#)和[命名空間屬性](#)可協助您熟悉設定。

使用和 Amazon Redshift 無伺服器 API 管理工作群組 AWS Command Line Interface 和命名空間

除了使用 AWS 主控台之外，您也可以使用 AWS CLI 或 Amazon Redshift 無伺服器 API 與工作群組和命名空間互動。下表列出可用來管理快照和復原點的 API 和 CLI 作業。

API 操作	CLI 命令	描述
CreateNamespace	建立命名空間	建立命名空間。根據預設，Amazon Redshift 無伺服器會使用預設 AWS Key Management Service 金鑰建立命名空間，但您可以指定另一個金鑰來加密資料。您也可以透過還原快照建立命名空間。如需詳細資訊，請參閱 使用快照和復原點 。
UpdateNamespace	更新命名空間	更新命名空間。
GetNamespace	獲取命名空間	擷取命名空間的相關資訊。
ListNamespaces	清單命名空間	擷取有關命名空間清單的資訊。
DeleteNamespace	刪除命名空間	刪除命名空間。
CreateWorkgroup	建立工作群組	建立工作群組。建立工作群組時，請確定您具有可與工作群組關聯的現有命名空間。您可以在建立工作群組時指定任何運算資源，例如子網路、安全群組或 RPU。
UpdateWorkgroup	更新工作群組	更新工作群組。
GetWorkgroup	取得工作群組	擷取有關工作群組的資訊。
ListWorkgroups	工作群組清單	擷取有關工作群組清單的資訊。
DeleteWorkgroup	刪除工作群組	刪除工作群組。

使用主控台管理 Amazon Redshift Serverless

若要建立、編輯和刪除 Amazon Redshift Serverless 資料倉儲，請使用 Amazon Redshift 主控台上的 Serverless 儀表板。能否存取個別主控台的設定取決於 IAM 角色和許可。

如需有關設定 Amazon Redshift Serverless 的資訊，請參閱[第一次設定 Amazon Redshift Serverless](#)。如需有關建立和設定工作群組的資訊，請參閱[使用工作群組](#)。如需有關設定命名空間的資訊，請參閱[使用命名空間](#)。

第一次設定 Amazon Redshift Serverless

第一次選取 Serverless 儀表板時，其會引導您完成設定 Amazon Redshift Serverless 的步驟。在開始使用無伺服器體驗下，您可以使用範例資料集設定 Amazon Redshift Serverless 資料倉儲。Amazon Redshift Serverless 會在建立過程中自動載入範例資料集。在建立資料倉儲之後，便可以立即查詢資料。如需有關如何第一次設定 Amazon Redshift 無伺服器的詳細資訊，請參閱 [Red](#) shift 無伺服器。

使用工作群組

若要在 Amazon Redshift Serverless 中隔離工作負載並管理資源，您可以建立工作群組和命名空間。運算相關的工作群組會將運算資源 (例如 RPU 和 VPC 子網路群組) 群組在一起。如果您尚未建立工作群組和命名空間，而且正在尋找說明如何開始使用 Amazon Redshift Serverless 的指示，請參閱[第一次設定 Amazon Redshift Serverless](#)。

使用命名空間建立工作群組

以下步驟假設您已完成 Amazon Redshift Serverless 的初始組態設定。如果您尚未建立工作群組和命名空間，而且正在尋找說明如何開始使用 Amazon Redshift Serverless 的指示，請參閱[第一次設定 Amazon Redshift Serverless](#)。

請完成以下步驟以建立工作群組：

1. 選擇 Serverless 儀表板。選擇建立工作群組。
2. 輸入工作群組名稱。
3. 選擇 Amazon Redshift Serverless 的虛擬私有雲端 (VPC)。這會將工作群組指定給您 AWS 環境中的特定虛擬網路。如需 VPC 的相關資訊，請參閱[VPC 和子網路概觀](#)。
4. 選擇一或多個 VPC 安全群組。如需詳細資訊，請參閱[使用安全群組控制資源的流量](#)。
5. 在子網路下，指定要與資料庫相關聯的一或多個子網路。這些子網路會包含在您先前選擇的 VPC 中，且必須位於三個不同的可用區域中。如需詳細資訊，請參閱[使用 Amazon Redshift Serverless 時的考量](#)。

6. 選取符合您要求的基本 RPU 容量。

選擇命名空間

1. 選擇建立新的命名空間，然後輸入命名空間名稱，或選擇新增至現有的命名空間，然後從下拉式清單中選取命名空間。
2. 對於資料庫名稱和密碼，指定第一個資料庫的名稱。您也可以透過編輯管理員使用者憑證來指定預設主控台管理員以外的管理員。
3. 對於許可，請選擇關聯 IAM 角色，以將特定 IAM 角色與命名空間和工作群組建立關聯。如需將 IAM 角色與 Amazon Redshift 建立關聯的相關資訊，請參閱 [Amazon Redshift 中的身分和存取管理](#)。
4. 您可以透過建立新的金鑰或選擇預設金鑰以外的金鑰來自訂加密設定。對於稽核記錄，選擇要匯出的日誌。每種日誌類型會指定不同的中繼資料 選擇繼續以檢閱您的選擇。

檢閱工作群組選取項目

1. 在檢閱和建立下方檢閱您的設定。其會顯示您在先前步驟中選擇的設定。
2. 選擇儲存。

在建立工作群組後，該工作群組會新增至工作群組清單。

建立預覽工作群組

若要測試新的 Amazon Redshift Serverless 功能，請建立預覽的 Amazon Redshift Serverless 工作群組。您無法在生產環境中使用這些功能，也無法將預覽工作群組移至生產工作群組。如需了解預覽條款和條件，請參閱 [AWS 服務條款](#) 中的 Beta 版和預覽版。

預覽工作群組中目前可以使用以下功能：

- [使用零 ETL 整合](#)

建立預覽工作群組

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽選單上，選擇 Serverless 儀表板，然後選擇工作群組組態。AWS 區域 會列出目前帳戶中帳戶的工作群組。每個工作群組的屬性子集會在清單中分欄顯示。

3. 工作群組組態頁面上的橫幅會介紹預覽工作群組。選擇建立預覽工作群組按鈕以開啟 [建立工作群組] 頁面。
4. 輸入工作群組的屬性。建議您為工作群組輸入可表示其為預覽版的名稱。針對您要測試的功能選擇工作群組選項，包括標記為 -preview 的選項。繼續瀏覽頁面，為您的工作群組和命名空間輸入選項。如需有關建立工作群組的一般資訊，請參閱[the section called “使用命名空間建立工作群組”](#)。
5. 選擇建立以建立預覽工作群組。
6. 當您的預覽工作群組可用時，請使用 SQL 用戶端載入和查詢資料。

如需有關已佈建叢集中預覽版的資訊，請參閱[建立預覽叢集](#)。

檢視工作群組的屬性

在 Amazon Redshift Serverless 中，工作群組是可用資源的集合。選擇 Amazon Redshift 無伺服器時，您可以在 AWS 主控台中從導覽功能表選擇工作群組組態以檢視清單。您可以使用搜尋方塊來尋找符合搜尋條件的工作群組。每個工作群組項目都會顯示一些屬性：

- 工作群組 — 工作群組名稱。您可以選取此項目來檢視和編輯工作群組的屬性。
- 狀態 — 顯示工作群組是否可供使用。
- 命名空間 — 與工作群組相關聯的命名空間。每個工作群組都會與一個命名空間相關聯。
- 建立日期 — 工作群組的建立日期。
- 標籤 - 與工作群組相關聯的標籤。

工作群組屬性

您可以透過選擇左側選單中的工作群組組態來列出工作群組。然後，您可以從清單中選擇工作群組。有數個面板會顯示工作群組的屬性。您也可以執行動作。一般資訊會顯示下列項目：

- 工作群組 — 工作群組名稱。
- 命名空間 — 與工作群組相關聯的命名空間。您可以選擇此項目來檢視其屬性。工作群組會與單一命名空間相關聯。
- 建立日期 — 工作群組的建立時間。
- 狀態 — 指出工作群組資源是否可供使用。如果可供使用，您可以透過用戶端連線至 Amazon Redshift Serverless 執行個體，以查詢資料或建立資料庫資源，或者，您也可以使用查詢編輯器 v2 來連線。
- 端點 — URL。

- JDBC URL — 用來建立 JDBC 用戶端連線的 URL。您可以使用此 URL 來與 Amazon Redshift 的 JDBC 驅動程序進行連線。如需詳細資訊，請參閱[設定 Amazon Redshift JDBC 驅動程式 2.1 版的連線](#)。
- ODBC URL — 用來建立 ODBC 用戶端連線的 URL。此項目包含資料庫和使用者 ID 等屬性以及這些屬性的值。
- 工作群組版本和修補程式版本 - Amazon Redshift Serverless 會定期發行新版本和修補程式。您可以使用工作群組版本和修補程式版本號碼，追蹤 Amazon Redshift Serverless 工作群組的軟體更新。如需特定修補程式中變更和功能的詳細資訊，請參閱[Amazon Redshift 的叢集版本](#)。

資料存取索引標籤包含數個面板：

- 網路和安全 — 您可以查看網路屬性，例如虛擬私有雲端 (VPC) 識別碼、VPC 安全群組清單、增強型 VPC 路由，以及可公開存取設定。如果您選擇編輯，則可以變更這些設定。此外，您也可以選取開啟增強型 VPC 路由，透過 VPC 來路由傳送無伺服器資料庫和資料儲存庫之間的網路流量，以增強隱私和安全。您也可以選取開啟公開存取，這會讓資料庫可供從 VPC 外部公開存取，讓執行個體和裝置得以連線。
- Redshift 受管 VPC 端點 — 您可以建立受管 VPC 端點，以便從其他 VPC 存取 Amazon Redshift Serverless。

限制索引標籤具有用於控制 Amazon Redshift Serverless 容量和使用限制的設定。其包含以下面板：

- 以 Redshift 處理單元 (RPU) 為單位的基本容量 — 您可以設定用來處理工作負載的運算資源基本容量。如需詳細資訊，請參閱[了解 Amazon Redshift Serverless 容量](#)。
- 用量限制 - 您最多可以為 Amazon Redshift Serverless 執行個體在一段時間內使用的運算資源上限設定四個限制，並選取 Amazon Redshift Serverless 在達到這些限制時要執行的動作。例如，您可以將工作群組設定為兩個限制：500 RPU 小時之一，以及 900 RPU 小時之一。您可以讓 Amazon Redshift Serverless 在達到 500 RPU 小時的第一個限制時傳送警示給您，然後在達到 900 小時的第二個限制時關閉使用者查詢。這些限制有助於控制成本，而更能夠預測成本。
- 查詢限制 — 您可以設定查詢限制，例如逾時設定。這些限制可協助您將成本和效能最佳化。

定位點頁籤具有標籤面板，展示您為工作群組建立的任何標籤。如需標記資源的詳細資訊，請參閱[標記資源概觀](#)。

刪除工作群組

您可以使用主控台刪除工作群組。在執行此操作之前，請確定您已備份資料並備妥快照。在許多情況下，您無法擷取隨工作群組一起刪除的資源。

請完成下列步驟：

1. 選擇 Amazon Redshift Serverless、選擇工作群組組態，然後選擇刪除 Amazon Redshift Serverless 執行個體。
2. 隨即會開啟對話方塊。當您選擇刪除工作群組時，系統會移除所有用量限制、移除所有 VPC 端點，並移除對 VPC 端點的存取權。

輸入刪除，然後選取刪除來進行確認。

完成這些步驟後，工作群組的狀態會是正在刪除，橫幅則會指出正在刪除工作群組。刪除程序進行期間，Serverless 儀表板下的某些功能會遭到停用。但是，您可以在佈建叢集儀表板上設定已佈建的叢集。

刪除工作群組後，該工作群組就不會與命名空間一起顯示。您可以選擇建立工作群組按鈕來建立新的工作群組。

您可以刪除現有工作群組，並將具有不同組態的新工作群組與相同的命名空間建立關聯。在建立新的工作群組時，請選擇能與命名空間的相關聯資料大小搭配運作的基本容量。

您可以將工作群組與使用客戶自管金鑰 (CMK) 所建立的命名空間建立關聯。如需詳細資訊 AWS KMS，請參閱[AWS KMS 概念](#)。

使用命名空間

在 Amazon Redshift Serverless 中，命名空間會定義資料庫物件的邏輯容器。其可以包含資料表、工作群組和其他資料庫資源。如果您尚未建立工作群組和命名空間，而且正在尋找如何開始使用 Amazon Redshift Serverless 的指示，請參閱[第一次設定 Amazon Redshift Serverless](#)。

搜尋命名空間

在 Amazon Redshift 選單中，您可以從命名空間清單中進行選擇，以檢視或編輯命名空間的屬性。主控台上的資訊包括命名空間名稱、管理員名稱和其他屬性。

命名空間的設定和屬性位於多個索引標籤上。這些索引標籤包括以下項目：

- 工作群組 — 顯示與命名空間相關聯的工作群組。
- 資料備份 — 您可以設定和建立快照，以及設定復原點。
- 安全和加密 — 您可以管理 IAM 角色許可，以及檢視或編輯安全和加密設定。這些項目包括您的加密金鑰狀態和稽核記錄設定。
- 資料共用 — 顯示資料共用。

命名空間屬性

在 Amazon Redshift Serverless 中，命名空間會定義資料庫物件的容器。您可以從導覽清單中選擇命名空間組態、從清單中選擇命名空間，然後編輯其設定。

命名空間的一般資訊包括以下項目：

- 命名空間 — 名稱。
- 命名空間 ID — 唯一識別碼。
- ARN-用於指定跨 AWS 資源的唯一標識符。其包含區域和服務等屬性。
- 狀態 — 即狀態，例如可用。
- 建立日期 — 命名空間的建立日期。
- 使用的儲存 — 命名空間及其所有物件所使用的儲存空間。
- 管理員使用者名稱 — 管理員帳戶。這一般是用來建立命名空間的帳戶。
- 資料庫名稱 — 命名空間所含資料庫的名稱。
- 資料表總數 — 所有結構描述中的資料表計數。

命名空間的其他設定和屬性位於數個索引標籤上。這些索引標籤包括以下項目：

- 工作群組 — 顯示與命名空間相關聯的工作群組。
- 資料備份 — 在這個面板上，您可以設定和建立快照，以及設定復原點。
- 安全和加密 — 您可以管理 IAM 角色許可，以及檢視或編輯安全和加密設定。這些項目包括您的加密金鑰狀態，以及用來開啟稽核記錄的設定。如需 Amazon Redshift Serverless 稽核記錄的相關資訊，請參閱 [Amazon Redshift Serverless 的稽核記錄](#)。
- 資料共用 — 顯示資料共用。透過資料共用，您不必複製或移動資料即可提供資料存取權。如需資料共用的相關資訊，請參閱 [Amazon Redshift Serverless 中的資料共用](#)。

編輯安全和加密

Amazon Redshift Serverless 會透過 KMS 加密的方式來獲得保護。您可以透過主控台更新加密設定：

1. 從主控台的主選單選擇命名空間組態、選擇要編輯的命名空間，然後在安全和加密索引標籤上選擇編輯。隨即會出現對話方塊。
2. 您可以選取 [自訂加密設定]，然後選取 [選擇 AWS 客戶管理的金鑰]，以變更新用來加密資源的金鑰。
3. 對於稽核記錄，選擇要匯出的日誌。每種日誌類型會指定不同的中繼資料
4. 若要完成組態更新，請選擇儲存變更。

更改命名空間的 AWS KMS 密鑰

在 Amazon Redshift 中，加密可保護靜態資料。Amazon Redshift 無伺服器會自動使用 AWS KMS 金鑰加密來加密您的 Amazon Redshift 無伺服器資源和快照。作為最佳實務，大多數組織會檢閱其儲存的資料類型，並且會規劃安排程輪換加密金鑰。視您的資料安全政策而定，輪換金鑰的頻率可能會有所不同。Amazon Redshift 無伺服器支援變更命名空間的 AWS KMS 金鑰，讓您能夠遵守組織的安全政策。

當您變更 AWS KMS 索引鍵時，資料會保持不變。

使用主控台變更 AWS KMS 金鑰

在 Amazon Redshift 中，加密可保護靜態資料。Amazon Redshift 無伺服器會使用 AWS KMS 金鑰加密自動加密，同時加密 Amazon Redshift 無伺服器和快照。作為最佳實務，大多數組織會檢閱其儲存的資料類型，並且會規劃安排程輪換加密金鑰。視您的資料安全政策而定，輪換金鑰的頻率可能會有所不同。Amazon Redshift 無伺服器支援變更命名空間的 AWS KMS 金鑰，讓您能夠遵守組織的安全政策。

當您變更 AWS KMS 索引鍵時，資料會保持不變。

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽選單中，選擇命名空間組態。從清單中選擇您的命名空間。
3. 從安全和加密索引標籤中，選擇編輯。
4. 選擇自訂加密設定，然後選擇命名空間的金鑰。您可以選擇建立新的金鑰。

使用變更 AWS KMS 加密金鑰 AWS CLI

用 `update-namespace` 於變更命名空間的 AWS KMS 金鑰。下列內容顯示命令的語法：

```
aws redshift-serverless update-namespace
--namespace-name
[--kms-key-id <id-of-kms-key>]
// other parameters omitted here
```

您必須已建立命名空間，否則 CLI 命令會導致錯誤。

變更金鑰所需的時間取決於 Amazon Redshift Serverless 中的資料量。每 8 TB 的儲存資料一般需要 15 分鐘的時間。

限制

您無法從客戶管理的 KMS 金鑰變更為金 AWS KMS 鑰。在此案例中，您必須建立新的命名空間。

金鑰變更期間，您無法執行其他動作。

刪除命名空間

如果要刪除具有關聯工作群組的命名空間，則必須先刪除該工作群組。

在 Amazon Redshift Serverless 主控台上，完成下列步驟：

1. 從左側選單中選擇命名空間組態，然後從清單中選擇要刪除的命名空間。
2. 選擇動作，然後選取刪除命名空間。
3. 隨即會開啟對話方塊。您可以透過在完成刪除操作之前手動建立快照來保留資料。

輸入刪除，然後選取刪除來進行確認。

管理用量限制、查詢限制及其他管理任務

您可以在主控台中進行設定，以控制用量並限制成本。

管理用量限制，包括設定 RPU 限制

在工作群組的限制索引標籤下，您可以新增一或多個用量限制，以控制您在給定期間內使用的 RPU 上限，或設定資料共用用量限制。

1. 選擇管理用量限制。限制區段會顯示在按期間計算用量面板的底部。
2. 以小時為單位設定用量限制。
3. 首先，選擇頻率，即每日、每週或每月。這會設定用量限制的期間。在這種情況下，選擇每日可提供更詳細的控制能力。
4. 以小時數為單位設定用量限制。
5. 設定動作。這些項目如下：
 - 記錄至系統資料表-將記錄新增至系統檢視 [SYS_QUERY](#) 歷史記錄。您可以查詢此檢視中的 `usage_limit` 資料行，以判斷查詢是否超過限制。
 - 提醒 — 使用 Amazon SNS 設定通知訂閱，並在超出限制時傳送通知。您可以選擇現有的 Amazon SNS 主題，或建立新的主題。
 - 關閉使用者查詢 — 停用查詢以停止 Amazon Redshift Serverless 的使用。其也會傳送通知。

前兩個動作會提供參考資訊，最後一個動作則會關閉查詢的處理。

6. 您可以選擇性地設定跨區域資料共用用量限制，以限制取用者可查詢多少從生產者區域傳輸至取用者區域的資料。若要這麼做，請選擇新增限制，然後遵循步驟來進行。
7. 在頁面底部選擇儲存變更以儲存您限制。
8. 視需要設定最多 3 個限制。

如需更多有關 RPU 和帳單的概念性資訊，請參閱 [Amazon Redshift Serverless 的帳單](#)。

管理查詢限制

在工作群組的限制索引標籤下，您可以新增限制以監控效能和限制。如需查詢監控限制的相關資訊，請參閱 [WLM 查詢監控規則](#)。

1. 選擇管理查詢限制。在管理查詢限制對話方塊上選擇新增新的限制。
2. 選擇您要設定的限制類型，然後輸入其對應限制的值。
3. 選擇儲存變更以儲存限制。

當您變更查詢限制和組態參數時，資料庫將會重新啟動。

篩選查詢

您可以使用 Serverless 儀表板上提供的篩選條件。若要篩選查詢，請執行以下步驟。

1. 在查詢摘要面板的左側，選取下拉式清單，以依已完成的查詢、失敗的查詢或兩者進行篩選。
2. 在查詢摘要面板的右側，選取下拉式清單，以透過執行查詢、排入佇列的查詢或兩者進行篩選。

變更管理員密碼

1. 選擇命名空間組態。接著選擇變更管理員密碼。隨即會出現對話方塊。
2. 您可以指定新的管理員使用者名稱和新的管理員使用者密碼。
3. 選擇儲存。

使用儀表板檢查 Amazon Redshift Serverless 摘要資料

Amazon Redshift 無伺服器儀表板包含一組面板，其中顯示有關工作群組和命名空間的 at-a-glance 指標和資訊。這些面板包括下列項目：

- 資源摘要 — 顯示有關 Amazon Redshift Serverless 的高階資訊，例如已使用的儲存和其他指標。
- 查詢摘要 — 顯示有關查詢的資訊，包括已完成的查詢和執行中的查詢。選擇檢視詳細資訊以移至具有其他篩選條件的畫面。
- 已使用的 RPU 容量 — 顯示給定期間內已使用的整體容量，例如前 10 個小時。
- 資料共用 — 顯示用來在 (舉例) AWS 帳戶之間共用資料的資料共用計數。這個指標會顯示哪些資料共用需要授權以及其他資訊。
- 總運算用量 - 顯示所選時間範圍內所選工作群組的總使用 RPU 時數 (最多過去 7 天)。

您可以從儀表板快速深入了解這些可用指標，以查看有關 Amazon Redshift Serverless 的詳細資訊，或是檢閱查詢或追蹤工作項目。

使用 Amazon Redshift Serverless 監控查詢和工作負載

使用 Amazon Redshift Serverless 監控查詢和工作負載

您可以使用所提供的系統檢視來監控 Amazon Redshift Serverless 查詢和工作負載。

授予用來監控查詢的存取權

超級使用者可以為非超級使用者的使用者提供存取權，讓非超級使用者可以針對所有使用者執行查詢監控。首先，請為使用者或角色新增政策，以提供查詢監控存取權。然後，向使用者或角色授予查詢監控許可。

新增查詢監控政策

1. 選擇 <https://console.aws.amazon.com/iam/>。
2. 在 Access management (存取管理) 下，請選擇 Policies (政策)。
3. 選擇建立政策。
4. 選擇 JSON，並貼上下列政策定義。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "redshift-data:ExecuteStatement",
        "redshift-data:DescribeStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:ListDatabases"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "redshift-serverless:GetCredentials",
      "Resource": "*"
    }
  ]
}
```

5. 選擇檢閱政策。
6. 對於 Name (名稱)，輸入政策的名稱，例如 query-monitoring。
7. 選擇建立政策。

建立政策後，就可以授予適當許可。

若要提供存取權，請新增權限至您的使用者、群組或角色：

- 使用者和群組位於 AWS IAM Identity Center：

建立權限合集。請按照 AWS IAM Identity Center 使用者指南 中的 [建立權限合集](#) 說明進行操作。

- 透過身分提供者在 IAM 中管理的使用者：

建立聯合身分的角色。請按照 IAM 使用者指南的 [為第三方身分提供者 \(聯合\) 建立角色](#) 中的指示進行操作。

- IAM 使用者：
 - 建立您的使用者可擔任的角色。請按照 IAM 使用者指南的 [為 IAM 使用者建立角色](#) 中的指示進行操作。
 - (不建議) 將政策直接附加至使用者，或將使用者新增至使用者群組。請遵循 IAM 使用者指南的 [新增許可到使用者 \(主控台\)](#) 中的指示。

向使用者授予查詢監控許可

具有 `sys:monitor` 許可的使用者可以檢視所有查詢。此外，具有 `sys:operator` 許可的使用者可以取消查詢、分析查詢歷史記錄，以及執行清空操作。

1. 輸入下列命令來提供系統監控存取權，其中 `user-name` 是您想要為其提供存取權之使用者的名稱。

```
grant role sys:monitor to "IAM:user-name";
```

2. (選擇性) 輸入下列命令來提供系統操作人員存取權，其中 `user-name` 是您想要為其提供存取權之使用者的名稱。

```
grant role sys:operator to "IAM:user-name";
```

向角色授予查詢監控許可

使用者若有具有 `sys:monitor` 許可的角色，便可以檢視所有查詢。此外，使用者若有具有 `sys:operator` 許可的角色，便可以取消查詢、分析查詢歷史記錄，以及執行清空操作。

1. 輸入下列命令來提供系統監控存取權，其中 `role-name` 是您想要為其提供存取權之角色的名稱。

```
grant role sys:monitor to "IAMR:role-name";
```

2. (選擇性) 輸入下列命令來提供系統操作人員存取權，其中 `role-name` 是您想要為其提供存取權之角色的名稱。

```
grant role sys:operator to "IAMR:role-name";
```

監控檢視

監控檢視是 Amazon Redshift Serverless 中用來監控查詢和工作負載用量的系統檢視。這些檢視位於 `pg_catalog` 結構描述中。可用的系統檢視旨在為您提供要監控 Amazon Redshift Serverless 所需的資訊，這比已佈建叢集所需的資訊簡單得多。SYS 系統檢視旨在與 Amazon Redshift Serverless 搭配運作。若要顯示這些檢視所提供的資訊，請執行 SQL SELECT 陳述式。

定義系統檢視是為了支援下列監控目標。

工作負載監控

您可以監控一段時間內的查詢活動，以便執行下列操作：

- 了解工作負載模式，以知道什麼是正常 (基準) 以及商業服務水準協議 (SLA) 中的內容。
- 快速識別偏離正常的情況，這可能是短暫的問題或需要採取進一步行動的事件。

資料載入與卸載的監控

將資料移入和移出 Amazon Redshift Serverless 是一項關鍵功能。您可以使用 COPY 和 UNLOAD 來載入或卸載資料，而且您必須密切監控每一傳輸資料列的位元組和已完成檔案的進度，以追蹤商業 SLA 的遵循情況。這一般會透過頻繁 (即每分鐘) 執行系統資料表查詢來追蹤進度，並在偵測到重大偏差時提出調查/糾正行動的提醒。

失敗和問題診斷

在某些情況下，您必須針對查詢或執行期的失敗採取行動。開發人員依賴系統資料表來自我診斷問題並確定正確的補救措施。

效能調校

您可能需要針對從一開始就不符合 SLA 要求的查詢，或是隨時間降級的查詢進行微調。若要微調，您必須具有執行期的詳細資訊，包括執行計劃、統計資料、持續時間和資源取用。您需要有違規查詢的基準資料，以判斷偏差的原因，並指導您如何改善效能。

使用者物件事件監控

您需要監控使用者物件上的動作和活動，例如重新整理具體化視觀表、清空和分析。這包括系統管理的事件，如具體化視觀表的自動重新整理。您會想要監控使用者啟動的事件何時結束，或是系統啟動的最後一次成功執行。

帳單的用量追蹤

您可以監控一段時間內的用量趨勢，以便執行下列操作：

- 了解預算規劃和業務擴展估算。
- 找出潛在的成本節約機會，例如移除冷資料。

使用 SYS 系統檢視以監控 Amazon Redshift Serverless。如需 SYS 監控視觀表的相關資訊，請參閱 [SYS 監督視觀表](#)。

Amazon Redshift Serverless 的稽核記錄

匯出日誌

您可以設定 Amazon Redshift 無伺服器，將連線、使用者和使用者活動日誌資料匯出到 Amazon 日誌中的日誌群組。CloudWatch 使用 Amazon CloudWatch Logs，您可以對日誌資料執行即時分析，並用 CloudWatch 來建立警示和檢視指標。您可以使用 CloudWatch 日誌將日誌記錄存儲在耐久存儲中。

您可以使用 Amazon Redshift 主控台建立 CloudWatch 警示來追蹤您的指標。如需建立警示的相關資訊，請參閱 [管理警示](#)。

若要將產生的日誌資料匯出至 Amazon CloudWatch 日誌，您必須在主控台的 Amazon Redshift 無伺服器組態設定中選取要匯出的相應日誌。您可以選擇安全和加密底下的命名空間組態設定來執行此操作。

監視記錄事件 CloudWatch

選取要匯出的 Redshift 日誌後，您可以監控 Amazon CloudWatch 日誌中的事件。系統會自動為 Amazon Redshift Serverless 建立新的日誌群組，其中 log_type 代表日誌類型。

```
/aws/redshift/<namespace>/<log_type>
```

當您建立第一個工作群組和命名空間時，預設值是命名空間名稱。日誌群組名稱會根據您命名空間的名稱而有所不同。

例如，如果您匯出連線日誌，則日誌資料會儲存在下列日誌群組中。

```
/aws/redshift/default/connectionlog
```

日誌事件會使用無伺服器日誌串流匯出至日誌群組。該行為取決於下列哪個條件為真：

- 具指定名稱的日誌群組存在。Redshift 會使用現有的日誌群組匯出日誌資料。若要使用預先定義的記錄保留期間、指標篩選器和客戶存取權來建立記錄群組，您可以使用自動化設定，例如提供的設定。AWS CloudFormation
- 具指定名稱的日誌群組不存在。在執行個體的日誌中偵測到符合的日誌項目時，Amazon Redshift 無伺服器會自動在 Amazon 日誌中建立新的 CloudWatch 日誌群組。日誌群組會使用永不過期的預

設日誌保留期間。若要變更記錄保留期，請使用 Amazon CloudWatch 日誌主控台 AWS CLI、或 Amazon CloudWatch 日誌 API。如需有關在記錄檔中變更記錄保留期間的詳細資訊，請參閱使用 [CloudWatch 記錄群組和記錄串流中的變更記錄資料保留](#)。

若要搜尋日誌事件中的資訊，請使用 Amazon CloudWatch 日誌主控台 AWS CLI、或 Amazon CloudWatch 日誌 API。如需搜尋和篩選日誌資料的相關資訊，請參閱 [搜尋和篩選日誌資料](#)。

Amazon Redshift Serverless 指標

Amazon Redshift Serverless 指標分為運算指標以及資料和儲存指標，兩者分別屬於工作群組和命名空間維度集。如需工作群組和命名空間的相關資訊，請參閱 [Amazon Redshift Serverless 工作群組和命名空間的概觀](#)。

CloudWatch 運算指標如下：

CloudWatch 運算指標

指標名稱	單位	描述	維度集
QueriesCompletedPerSecond	查詢數量	每秒完成的查詢次數。	{資料庫 LatencyRange, 工作群組}, {LatencyRange, 工作群組}
QueryDuration	微秒	完成查詢的平均時間。	{資料庫 LatencyRange, 工作群組}, {LatencyRange, 工作群組}
QueriesRunning	查詢數量	某個時間點的執行中查詢數目。	{資料庫 QueryType, 工作群組}, {QueryType, 工作群組}
QueriesQueued	查詢數量	佇列中某個時間點的查詢數目。	{資料庫 QueryType, 工作群組}, {QueryType, 工作群組}

指標名稱	單位	描述	維度集
DatabaseConnections	連線數量	某個時間點的資料庫連線數目。	{Database, Workgroup}, {Workgroup}
QueryRuntimeBreakdown	毫秒	依查詢階段的查詢所花費總執行時間。	{Database, Stage, Workgroup}, {Stage, Workgroup}
ComputeCapacity	RPU	過去 30 分鐘內配置的運算單元平均數量，四捨五入至最接近的整數。	{Workgroup}
ComputeSeconds	RPU-秒	過去 30 分鐘內使用的累計運算單元秒數。	{Workgroup}
QueriesSucceeded	查詢數量	過去 5 分鐘內成功的查詢數目。	{資料庫 QueryType, 工作群組}, {QueryType, 工作群組}
QueriesFailed	查詢數量	過去 5 分鐘內失敗的查詢數目。	{資料庫 QueryType, 工作群組}, {QueryType, 工作群組}

指標名稱	單位	描述	維度集
UsageLimitAvailable	RPU-小時或 TB	<p>根據 UsageType , 傳 UsageLimitAvailable 回下列內容 :</p> <ul style="list-style-type: none"> • 如果 UsageType 是 SERVERLESS_COMPUTE , 則會 UsageLimitAvailable 傳回工作群組可以在指定限制內查詢的剩餘 RPU 小時數。 • 如果 UsageType 是交叉_區域資料共享 , 則 UsageLimitAvailable 傳回客戶可以在給定限制內掃描的剩餘 TB 數。 	{UsageLimitId, UsageType, 工作群組}

指標名稱	單位	描述	維度集
UsageLimitConsumed	RPU-小時或 TB	<p>根據 UsageType , 傳 UsageLimitConsumed 回下列內容 :</p> <ul style="list-style-type: none"> • 如果 UsageType 是 SERVERLESS_COMPUTE , 則會 UsageLimitConsumed 傳回工作群組在指定限制內已查詢的 RPU 小時數。 • 如果 UsageType 是「交叉_區域資料共享」, 則 UsageLimitConsumed 傳回客戶已用於在指定限制內掃描的 TB 數。 	{UsageLimitId, UsageType, 工作群組}

CloudWatch 資料和儲存指標如下 :

CloudWatch 資料和儲存指標

指標名稱	單位	描述	維度集
TotalTableCount	資料表數目	某個時間點所存在的使用者資料表數目。這個總計不包括 Amazon Redshift Spectrum 資料表。	{Database, Namespace}
DataStorage	MB	在磁碟或儲存空間中用於 Redshift 資料的 MB 數。	{Namespace}

此 SnapshotStorage 量度不受命名空間和工作群組無關。CloudWatch 的 SnapshotStorage 量度如下：

CloudWatch SnapshotStorage 公制

指標名稱	單位	描述	維度集
SnapshotStorage	MB	在磁碟或儲存空間中用於快照的 MB 數。	{}

維度集是套用至指標的分組維度。您可以使用這些維度群組來指定擷取統計資料的方式。

下表詳細說明特定指標的維度和維度值：

CloudWatch 標註和尺寸值

維度	描述和值
DatabaseName	資料庫的名稱。自訂值。

維度	描述和值
Latency	<p>可能的值如下：</p> <ul style="list-style-type: none"> • 短 — 少於 10 秒 • 中 — 介於 10 秒到 10 分鐘 • 長 — 超過 10 分鐘
QueryType	<p>可能值為 INSERT、DELETE、UPDATE、UNLOAD、LOAD、SELECT 及 OTHER。</p>
stage	<p>查詢的執行階段。可能的值如下：</p> <ul style="list-style-type: none"> • QueryPlanning：剖析和最佳化 SQL 敘述句所花費的時間。 • QueryWaiting：在 WLM 佇列中等待所花費的時間。 • QueryExecutingRead：執行讀取查詢所花費的時間。 • QueryExecutingInsert：執行插入查詢所花費的時間。 • QueryExecutingDelete：執行刪除查詢所花費的時間。 • QueryExecutingUpdate：執行更新查詢所花費的時間。 • QueryExecutingCtas：執行建立資料表做為查詢所花費的時間。 • QueryExecutingUnload：執行卸載查詢所花費的時間。 • QueryExecutingCopy：執行複製查詢所花費的時間。 • QueryCommit：承諾所花費的時間。
Namespace	命名空間的名稱。自訂值。

維度	描述和值
Workgroup	工作群組的名稱。自訂值。
UsageLimitId	用量限制的識別碼。
UsageType	Amazon Redshift Serverless 功能會受限。可能的值如下： <ul style="list-style-type: none">• SERVERLESS_COMPUTE• CROSS_REGION_DATASHARING

使用快照和復原點

Amazon Redshift 無伺服器中的備份 point-in-time 代表命名空間中的物件和資料。備份類型有兩種：手動建立的快照和 Amazon Redshift Serverless 自動為您建立的復原點。每 30 分鐘會建立一次復原點，並保留 24 小時。

如果您發現要擷取快照或復原點中的資料，您可以將快照還原至無伺服器命名空間或已佈建的叢集。您可以在三種情況下還原快照：

- 將無伺服器快照還原至無伺服器命名空間。
- 將無伺服器快照還原至已佈建的叢集。
- 將已佈建叢集的快照還原至無伺服器命名空間。

當您將無伺服器快照還原到已佈建的叢集時，請選擇要使用的節點類型 (例如 RA3) 和節點數目，以便控制叢集或節點層級的設定。

若要將已佈建叢集的快照還原至無伺服器命名空間，請從 Redshift 佈建的主控制台開始、選擇要還原的快照，然後選擇從快照還原、還原至無伺服器命名空間。當您將已佈建叢集的快照還原到無伺服器命名空間時，Amazon Redshift 會將具有交錯索引鍵的資料表轉換為複合索引鍵。如需排序索引鍵的詳細資訊，請參閱[使用排序索引鍵](#)。

如果您要新增其他內容，可以使用會提供中繼資料和資訊給快照和復原點的鍵值組來標記快照和復原點。如需有關標記資源的詳細資訊，請參閱[標記資源概觀](#)。

最後，您還可以與其他 AWS 帳戶共用快照，讓其可以存取快照內的資料並執行查詢。

快照

您可以將您在 Amazon Redshift Serverless 主控台上建立的快照，還原到與工作群組相關聯的可用命名空間。一旦命名空間準備好而可進行查詢和/或修改，便會立即可供使用。您可以將使用 AWS 受管 KMS 金鑰加密的快照還原至無伺服器命名空間。

若要查看所有快照的清單，請在 Amazon Redshift Serverless 主控台上選擇資料備份。

建立快照

1. 在 Amazon Redshift Serverless 主控台上，選擇資料備份。
2. 選擇建立快照。
3. 選擇要為其建立快照的命名空間。
4. 輸入快照識別符。
5. (選擇性) 選擇保留期間。如果您選擇自訂值，請選擇天數。您選擇的天數必須在 1 至 3653 天 (含) 之間。預設值為無限期保留。
6. 選擇建立。

從命名空間組態建立快照

1. 在 Amazon Redshift Serverless 主控台上，選擇命名空間組態。
2. 選擇要為其建立快照的命名空間。您只能為與工作群組相關聯且狀態為「可用」的命名空間建立快照。
3. 選擇資料備份索引標籤。
4. 選擇建立快照。
5. 輸入快照識別符。
6. (選擇性) 選擇保留期間。如果您選擇自訂值，請選擇天數。您選擇的天數必須在 1 至 3653 天 (含) 之間。
7. 選擇建立。

更新快照的保留期間

1. 在 Amazon Redshift Serverless 主控台上，選擇資料備份。
2. 選擇要更新的快照。

3. 選擇動作、設定手動快照設定。
4. 選擇保留期間。如果您選擇自訂值，請選擇天數。
5. 選擇儲存變更。

刪除快照

Note

您無法刪除已和其他帳戶共用的快照。您必須先移除該帳戶對快照的存取權，然後才能刪除快照。

1. 在 Amazon Redshift Serverless 主控台上，選擇資料備份。
2. 選擇要刪除的快照。
3. 選擇動作、刪除。
4. 選擇 刪除。

在刪除命名空間之前，先建立命名空間內所有資料的最終快照。

1. 在 Amazon Redshift Serverless 主控台上，選擇命名空間組態。
2. 選擇要刪除的命名空間。
3. 選擇動作、刪除。
4. 選擇建立最終快照。
5. 輸入快照的名稱。
6. 輸入刪除。
7. 選擇刪除。

與其他 AWS 帳戶共用快照或移除帳戶對快照的存取權

1. 在 Amazon Redshift Serverless 主控台上，選擇資料備份。
2. 選擇要共用的快照。
3. 選擇動作、管理存取權。
4. 若要與其他帳戶共用快照，請輸入 AWS 帳戶 ID。若要移除帳戶的存取權，請選擇移除。

5. 選擇儲存變更。

還原快照

將快照還原至無伺服器命名空間後，會將資料庫替換為快照中的資料庫。

將快照還原至無伺服器命名空間會分兩個階段來完成。第一個階段會在幾分鐘內完成、將資料還原至您的命名空間，並使其可用於查詢。還原的第二個階段是微調資料庫，這可能會造成輕微的效能問題。第二個階段可以持續幾小時到幾天，在某些情況下，甚至會持續幾週。時間長短取決於資料大小，但隨著資料庫進行微調，效能會逐步改善。這個階段結束時，您的無伺服器命名空間會徹底完成微調，而且您可以提交查詢而不會出現效能問題。

將快照還原至無伺服器命名空間

1. 在 Amazon Redshift Serverless 主控台上，選擇資料備份。
2. 選擇要還原的快照。您一次只能還原一個快照。
3. 選擇動作、還原至無伺服器命名空間。
4. 選擇要作為還原目的地的可用命名空間。您只能還原至狀態為「可用」的命名空間。
5. 選擇 Restore (還原)。

將快照還原至已佈建的叢集

1. 在 Amazon Redshift Serverless 主控台上，選擇資料備份。
2. 選擇要還原的快照。
3. 選擇動作、還原至佈建叢集。
4. 輸入叢集識別符。
5. 選擇節點類型。節點數取決於節點類型。
6. 遵循主控台頁面上的頁面說明以輸入叢集組態的屬性。如需詳細資訊，請參閱[建立叢集](#)。

如需已佈建叢集快照的詳細資訊，請參閱 [Amazon Redshift 快照和備份](#)。

復原點

系統大約每 30 分鐘會在 Amazon Redshift Serverless 中建立一個復原點，並儲存 24 小時。

在 Amazon Redshift Serverless 主控台上，選擇資料備份以管理復原點。您可以執行下列操作：

- 將復原點還原至無伺服器命名空間。
- 將復原點轉換為快照。

將復原點還原至無伺服器命名空間

1. 在 Amazon Redshift Serverless 主控台上，選擇資料備份。
2. 在復原點底下，選擇您要還原之復原點的建立時間。
3. 選擇 Restore (還原)。您只能還原至狀態為「可用」的命名空間。
4. 在文字輸入欄位中輸入還原，然後選擇還原。

將復原點轉換為快照

1. 在 Amazon Redshift Serverless 主控台上，選擇資料備份。
2. 在復原點底下，選擇您要轉換為快照之復原點的建立時間。
3. 選擇從復原點建立快照。
4. 輸入快照識別符。
5. 選擇建立。

排程快照

若要精確控制拍攝快照的時間，您可以為特定的命名空間集建立快照排程。建立排程快照時，您可以建立一次性事件或使用 Unix cron 運算式來建立週期性排程。Cron 表達式支援三個欄位，並以空格隔開。

```
cron(Minutes Hours Day-of-month Month Day-of-week Year)
```

欄位	Values (數值)	Wildcards (萬用字元)
分鐘	0–59	, - * /
小時	0–23	, - * /
Day-of-month	1–31	, - * ? / L W
月	1-12 或 JAN-DEC	, - * /

欄位	Values (數值)	Wildcards (萬用字元)
Day-of-week	1-7 或 SUN-SAT	, - * ? L #
年	1970-2199	, - * /

萬用字元

- ,(逗號) 萬用字元包含額外的值。在 Day-of-week 欄位，MON,WED,FRI 包括週一、週二和週三。每個欄位的總數值限制為 24。
- -(破折號) 萬用字元用於指定範圍。在 Hour 欄位中，1-15 會包含指定日的 1 至 15 時。
- *(星號) 包含欄位中所有的值。在 Hours 欄位，* 包含每個小時。
- /(斜線) 萬用字元用於指定增量。在 Hours 欄位，您可以輸入 **1/10** 指定每第 10 小時，從一天的第一小時開始 (例如 01:00、11:00 和 21:00)。
- ?(問號) 萬用字元用於表示不限定任何一個。在該Day-of-month字段中，您可以輸入 7，如果您不在乎第七週的哪一天，您可以輸入？在 Day-of-week 段中。
- L 萬用字元在 Day-of-month 或 Day-of-week 欄位可指定月份或週的最後一天。
- W 萬用字元在 Day-of-month 欄位可指定任務日。在 Day-of-month 欄位，3W 指定的是月份中最接近第三個任務日的日子。
- Day-of-week 欄位中的 # 萬用字元會指定一個月內星期中指定日期的特定執行個體。例如，3#2 代表則該月的第二個星期二：3 是指星期二，因為它是每週的第三天，2 指的是一個月內該類型的第二天。

Note

如果您使用 '#' 字元，則只能在 day-of-week 欄位中定義一個運算式。例如："3#1,6#3" 是無效的，因為它被轉譯為兩個表達式。

限制

- 您無法在同一個 cron 表達式中指定 Day-of-month 和 Day-of-week 欄位。如果您在其中一個欄位指定了數值，就必須在另一個欄位中使用？(問號)。
- 快照排程不支援下列頻率：
 - 快照排程頻率超過每小時 1 次。

- 快照排程頻率低於每天 (24 小時) 1 次。

如果您有重疊的排程，導致 1 個小時內有多個排程快照，將會產生驗證錯誤。

下表包含一些 cron 字串範例。

分鐘	小時	週中的日	意義
0	14-20/1	TUE	週二下午 2 點至 8 點，每小時一次。
0	21	MON-FRI	週一至週五每天晚上 9 點。
30	0/6	SAT-SUN	週六和週日每 6 小時增量，從當日午夜後 30 分鐘開始 (00:30)。結果是在每天 [00:30、06:30、12:30 和 18:30] 進行快照。
30	12/4	*	每天 12:30 開始每 4 小時增量。這解析為 [12:30、16:30、20:30]。

下列範例說明如何建立可從每天 15:15 開始以 2 小時增量執行的排程。

```
cron(15 15/2 *)
```

目前您只能使用 Amazon Redshift Serverless API 或 AWS CLI 建立快照排程。如需這些操作的詳細資訊，請參閱 [使用 AWS CLI 和 Amazon Redshift Serverless API](#)。

將備份複寫到另一個 AWS 區域

您可以將 Amazon Redshift Serverless 設定為自動將快照和復原點複製到另一個 AWS 區域快照和復原點。當您在來源 AWS 區域中建立快照時，它會複製到目的地區域。您可以設定命名空間，以便一次只

將快照和復原點複製到一個目的地 AWS 區域。如需有提供 Amazon Redshift Serverless 的 AWS 區域清單，請參閱《Amazon Web Services 一般參考》中針對 [Redshift Serverless API](#) 所列出的端點。

設定複製備份時，您也可以指定 Amazon Redshift Serverless 應保留複製快照的時間長度的保留期。您無法變更復原點的保留期間 (必須為 1 天)。目標區域中快照的保留期與來源區域中快照的保留期是不同的。依預設，保留期會無限期保留快照。如果您選擇自訂值，請選擇天數。您選擇的天數必須在 1 至 3653 天 (含) 之間。

若要變更複製快照的目的地區域，請先停用複製備份，然後在重新啟用複製時指定新的目的地區域。

將快照或復原點複製到目的地區域後，您可以使用該快照或復原點將資料還原到該區域。

預設情況下，您的資料會經由 AWS 為您管理的金鑰進行加密。若要使用不同的金鑰，請在來源 AWS 區域中設定備份複製時選擇要使用的金鑰，Amazon Redshift Serverless 會自動建立授權，以便在目的地 AWS 區域啟用快照加密。

若要將備份複製到另一個區域，請確定您有下列 IAM 許可：

```
redshift-serverless:CreateSnapshotCopyConfiguration
redshift-serverless:UpdateSnapshotCopyConfiguration
redshift-serverless:ListSnapshotCopyConfigurations
redshift-serverless>DeleteSnapshotCopyConfiguration
```

如果您使用自己的 KMS 金鑰加密備份，您還需要下列權限：

```
kms:CreateGrant
kms:DescribeKey
```

設定將快照或復原點複製到另一個快照或復原點 AWS 區域

1. 在 Amazon Redshift Serverless 主控台上，選擇要為其設定複製快照或復原點的命名空間。
2. 選擇動作，設定跨區域備份。
3. 選擇要複製快照的目的地 AWS 區域。
4. (選用) 選擇保留快照的時間長度。如果您選擇自訂值，請選擇天數，您選擇的數量必須在 1-3653 天之間 (包括在內)。預設值為無限期保留。
5. (選用) 選擇不同的 AWS KMS 金鑰，以用於在目的地區域內進行加密。
6. 選擇 Save configuration (儲存組態)。

還原資料表

您也可以從快照或復原點還原特定資料表。這樣做時，您可以指定來源快照或復原點、資料庫、結構描述、資料表、目標資料庫、結構描述和新資料表名稱。這個新資料表的名稱不能與現有資料表相同。若您想要透過還原資料表來取代現有資料表，則必須先重新命名或捨棄現有資料表，然後再還原資料表。

已使用資料表的欄位定義、資料表屬性和欄位屬性 (外部索引鍵除外) 建立目標資料表。為避免因相依性而導致的衝突，目標資料表不會從來源資料表繼承外部索引鍵。任何相依性，例如檢視或來源資料表上授予的許可，都不會套用至目標資料表。

若來源資料表存在擁有者，則該使用者是已還原資料表的擁有者，前提是該使用者有足夠的許可可以成為指定資料庫和結構描述中關係的擁有者。否則，還原的資料表將由啟動叢集時建立的管理員使用者所擁有。

還原的資料表會恢復到備份時所處的狀態。這包括由 Amazon Redshift 符合 [可序列化的隔離](#) 所定義的交易可見度規則，這表示在備份後開始傳送的交易中立刻可看見該資料。

您可以使用 Amazon Redshift Serverless 主控台從快照還原資料表。

以下為從資料備份還原資料表的限制：

- 您一次只能還原一個資料表。
- 任何相依性，例如檢視或來源資料表上授予的許可，都不會套用至目標資料表。
- 如果為要還原的資料表開啟了資料列層級安全，Amazon Redshift Serverless 會在開啟資料列層級安全的情況下還原資料表。

使用 Amazon Redshift Serverless 主控台還原資料表

1. 在 Amazon Redshift Serverless 主控台上，選擇資料備份。
2. 選擇具有要還原之資料表的快照或復原點。
3. 選擇動作、從快照還原資料表或從復原點還原資料表。
4. 輸入來源快照或復原點和目標資料表的相關資訊，然後選擇還原資料表。

使用 AWS Command Line Interface 和 Amazon Redshift Serverless API

除了使用 AWS 主控台外，您也可以使用 AWS CLI 或 Amazon Redshift Serverless API 來與快照和復原點互動。下表列出可用來管理快照和復原點的 API 和 CLI 作業。

API 操作	CLI 命令	描述
CreateSnapshot	建立快照	建立快照。快照必須與命名空間相關聯，因此您必須在請求中包含命名空間的名稱。根據預設，Amazon Redshift Serverless 會無限期保留快照，但您可以指定保留期。
RestoreFromSnapshot	restore-from-snapshot	將快照中的資料庫還原至您的命名空間。如果要將快照從 Amazon Redshift Serverless 還原到已佈建的叢集，則必須指定要還原之快照的 <code>snapshotArn</code> 。否則，如果您要從無伺服器還原至無伺服器，則可以指定 <code>snapshotArn</code> 或 <code>snapshotName</code> ，但不能同時指定兩者。
RestoreTableFromSnapshot	restore-table-from-snapshot	將資料表從快照還原到您的 Amazon Redshift Serverless 命名空間。您無法使用此作業來還原具有交錯排序索引鍵的資料表。
GetSnapshot	get-snapshot	擷取有關快照的資訊。
ListSnapshots	list-snapshots	擷取有關多個快照的資訊。
DeleteSnapshot	delete-snapshot	刪除快照。
RestoreFromRecoveryPoint	restore-from-recovery-point	將復原點內的資料還原至您的命名空間。
RestoreTableFromRecoveryPoint	restore-table-from-recovery-point	將資料表從復原點還原到您的 Amazon Redshift Serverless 命名空間。您無法使用此作業

API 操作	CLI 命令	描述
		來還原具有交錯排序索引鍵的資料表。
ConvertRecoveryPointToSnapshot	convert-recovery-point-to-快照	將復原點轉換為快照。
GetRecoveryPoint	get-recovery-point	擷取復原點的相關資訊。
ListRecoveryPoints	list-recovery-points	擷取多個復原點的相關資訊。

若要排定建立快照，請使用下列 API 操作。

API 操作	CLI 命令	描述
CreateScheduledAction	create-scheduled-action	建立排程動作，包含排程和 Amazon Redshift Serverless 動作。例如，您可以建立何時要執行 CreateSnapshot API 操作的排程。
DeleteScheduledAction	delete-scheduled-action	刪除排程動作。
GetScheduledAction	get-scheduled-action	擷取排定動作的相關資訊。
ListScheduledActions	list-scheduled-actions	擷取排定動作清單的相關資訊。
UpdateScheduledAction	update-scheduled-action	更新排程動作。

Amazon Redshift Serverless 中的資料共用

在 Amazon Redshift 無伺服器中更新時，使用資料共用來共用最多 up-to-date 且一致的資訊。

Amazon Redshift Serverless 中的資料共用

透過資料共用，您可以即時存取資料，讓您的使用者可以在 Amazon Redshift 無伺服器中看到資訊更新時最 up-to-date 為一致的資訊。

在 Amazon Redshift Serverless 中開始使用資料共用

您可以在 AWS 帳戶內部或之間的不同 Amazon Redshift Serverless 執行個體之間共用資料以供讀取。

您可以透過使用 SQL 介面或 Amazon Redshift 主控台開始使用資料共用功能。如需詳細資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的[使用 SQL 介面開始使用資料共用](#)或[使用主控台開始使用資料共用](#)。

透過資料共用，Amazon Redshift 無伺服器命名空間和佈建的叢集可以彼此共用即時資料，無論它們位於跨境或 AWS 帳戶 跨越 AWS 帳戶。AWS 區域如需詳細資訊，請參閱[可使用資料共用的區域](#)。

若要開始在中共用資料 AWS 帳戶，請開啟 AWS Management Console，然後選擇 Amazon Redshift 主控台。選擇命名空間組態，然後選擇資料共用。遵循《Amazon Redshift 資料庫開發人員指南》中的[使用主控台開始使用資料共用](#)內的程序進行操作。

若要開始共用資料 AWS 帳戶，請開啟 AWS Management Console，然後選擇 Amazon Redshift 主控台。選擇資料共用。遵循《Amazon Redshift 資料庫開發人員指南》中的[使用主控台開始使用資料共用](#)內的程序進行操作。

若要開始查詢資料共用中的資料，請在具有相關聯工作群組的命名空間中建立資料庫。從指定的資料共用中，選擇具有相關聯工作群組的命名空間，然後建立用來查詢資料的資料庫。遵循[從資料共用建立資料庫](#)中的程序。

使用主控台授予檢視資料共用的存取權

超級使用者可以為非超級使用者的使用者提供存取權，讓非超級使用者可以檢視所有使用者建立的資料共用。

若要為使用者授予資料共用存取權，請使用以下命令為使用者提供資料共用存取權，其中 `datashare_name` 是資料共用的名稱，`user-name` 則是您要為其提供存取權之使用者的名稱。

```
grant share on datashare datashare_name to "IAM:test_user";
```

若要為使用者群組授予資料共用存取權，請先建立具有使用者的使用者群組。如需如何建立使用者群組的資訊，請參閱 [CREATE GROUP](#)。然後，使用以下命令向使用者授予資料共用存取權，其中 `datashare_name` 是資料共用的名稱，`user-group` 則是您要向其授予存取權之使用者群組的名稱。


```
grant share on datashare datashare_name to group user_group;
```

如需如何使用 GRANT 陳述式的資訊，請參閱 [GRANT](#)。

Amazon Redshift Serverless 中的資料共用考量

以下是在 Amazon Redshift Serverless 中使用資料共用的考量：

- Amazon Redshift 僅支援將執行個體類型為 ra3.16xlarge、ra3.4xlarge 和 ra3.xplus 的已佈建叢集以及無伺服器端點作為資料共用生產者或取用者。
- Amazon Redshift Serverless 預設會進行加密。

如需資料共用限制 (包括支援的資料庫物件、加密要求和排序索引鍵要求) 的清單，請參閱《Amazon Redshift 資料庫開發人員指南》中的 [在 Amazon Redshift 中使用資料共用時的考量](#)。

標記資源概觀

在 AWS 中，標籤是由鍵值對組成的使用者定義的標籤。Amazon Redshift Serverless 支援標記功能，以讓您一目了然地查看資源的中繼資料。

資源不需要標籤，但標籤可以協助提供內容。您可能會想要使用具有資源相關資訊的中繼資料來標記資源。例如，假設您想要追蹤哪些資源屬於測試環境和生產環境。您可以建立名為 environment 的索引鍵，並提供值 (test 或 production) 來識別每個環境中使用的資源。如果您在其他 AWS 服務中使用標記或擁有適用於業務的標準類別，我們建議您為了一致性起見，為資源建立相同的鍵值對。

如果您刪除資源，任何關聯的標籤也會遭到刪除。AWS CLI 和 Amazon Redshift Serverless 主控台都可用來標記無伺服器資源。可用的 API 操作有 TagResource、UntagResource 和 ListTagsForResource。

每個資源皆有一個標籤集，此為指派給該資源之一或多個標籤的集合。每個資源每個標籤集最多可擁有 50 個標籤。在您建立資源時與資源建立後，您可以新增標籤。您可以將標籤新增至以下無伺服器資源類型：

- 工作群組
- 命名空間
- 快照
- 復原點

標籤均擁有以下要求：

- 索引鍵字首不能是 `aws:`。
- 索引鍵在標籤集內必須是唯一的。
- 索引鍵必須介於 1 到 128 個允許的字元之間。
- 值必須介於 0 到 256 個允許的字元之間。
- 值在每個標籤集中不需要是唯一的。
- 索引鍵和值的允許字元為 Unicode 字母、數字、空格和下列任何符號：`_ . : / = + - @`。
- 金鑰和值會區分大小寫。

管理 Amazon Redshift Serverless 資源的標籤

1. 在 Amazon Redshift Serverless 主控台上，選擇管理標籤。
2. 輸入要搜尋的資源類型，然後選擇搜尋資源。選擇您要管理標籤的資源，然後選擇管理標籤。
3. 指定您要新增至資源的索引鍵和選用值。修改標籤時可以變更標籤的值，但無法變更索引鍵。
4. 在完成標籤的新增、移除或修改後，請選擇儲存變更，然後選擇套用以儲存變更。

Amazon Redshift 佈建叢集

在以下各節中，您可以了解經由啟動稱為 Amazon Redshift 叢集的一組運算節點，以建立資料倉儲的基礎概念。

主題

- [Amazon Redshift 概述](#)
- [在建立叢集時使用 EC2-VPC](#)
- [預設磁碟空間警示](#)
- [叢集狀態](#)
- [使用 Amazon Redshift 佈建叢集的注意事項](#)
- [叢集作業](#)
- [設定多可用區部署](#)
- [使用主控台管理叢集](#)
- [使用 AWS CLI 和 Amazon Redshift API 管理叢集](#)
- [管理 VPC 中的叢集](#)
- [叢集版本歷史記錄](#)

Amazon Redshift 概述

Amazon Redshift 資料倉儲是稱為節點的運算資源的集合，組織成稱為叢集的群組。每個叢集皆執行 Amazon Redshift 引擎並包含一或多個資料庫。

Note

目前，可用的是 Amazon Redshift 1.0 版引擎。但是，等引擎更新後，會有多個 Amazon Redshift 引擎版本可供選擇。

Amazon Redshift 中的叢集和節點

Amazon Redshift 叢集由節點組成。每個叢集會擁有一個領導節點和一或多個運算節點。領導節點接收來自用戶端應用程式的查詢，剖析查詢，並制定查詢執行計畫。領導節點會協調在運算節點上平行執行這些計畫，並彙總這些節點傳回的中間結果，最後將結果傳回用戶端應用程式。

運算節點會執行查詢執行計畫，並在它們之間傳輸資料以服務這些查詢。中繼結果在傳回用戶端應用程式之前，會傳給領導節點進行彙總。如需領導節點和運算節點的相關資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的[資料倉儲系統架構](#)。

Note

在 Amazon Redshift 主控台 (<https://console.aws.amazon.com/redshiftv2/>) 上建立叢集時，您可以根據資料大小和查詢特性取得叢集組態的建議。若要使用此大小計算器，請在支援 RA3 節點類型的 AWS 區域中尋找主控台上的 [協助我選擇]。如需詳細資訊，請參閱 [建立叢集](#)。

啟動叢集時，其中一個要指定的選項為節點類型。節點類型會決定每個節點的 CPU、RAM、儲存容量和儲存磁碟機類型。

Amazon Redshift 提供了不同的節點類型，可滿足您的工作負載需求，並且我們建議根據所需的效能、資料大小及預期的資料增長情況選擇 RA3 或 DC2。

RA3 節點搭配受管儲存，可讓您透過分別擴展運算和受管儲存並分別付費，來優化資料倉儲。使用 RA3 時，您可以根據效能需求來選擇節點數目，並只需為您使用的受管儲存付費。請根據每日處理的資料量調整 RA3 叢集的大小。您可以在虛擬私有雲端 (VPC) 中啟動使用 RA3 節點類型的叢集。您無法在 EC2-Classical 中啟動 RA3 叢集。如需詳細資訊，請參閱 [在 VPC 中建立叢集](#)。

Amazon Redshift 受管儲存會在每個 RA3 節點中使用大型、高效能的 SSD 以獲得快速的本機儲存，並使用 Amazon S3 來獲得長期的耐用儲存。如果節點中的資料成長到超過大型本機 SSD 的大小，Amazon Redshift 受管儲存會自動將資料卸載到 Amazon S3。無論資料是在高效能 SSD 或 Amazon S3 中，您都只需要支付與 Amazon Redshift 受管儲存相同的低費率。對於需要不斷增長儲存的工作負載，受管儲存可讓您自動擴充資料倉儲儲存容量，以獨立於運算節點。

DC2 節點讓您建立包含本機 SSD 儲存的運算密集型資料倉儲。您可以根據資料大小和效能需求來選擇所需的節點數目。DC2 節點將資料儲存在本機以提高效能，並且隨著資料大小的增長，您可以新增更多運算節點來增加叢集的儲存容量。針對 1 TB (壓縮) 以下資料集，我們建議使用 DC2 節點，以便以最低的價格獲得最佳效能。如果您預期資料會增長，我們建議使用 RA3 節點，這樣您就可以獨立調整運算和儲存的大小，以獲得改善的價格效能比。使用 DC2 節點類型的叢集需在虛擬私有雲端 (VPC) 中啟動。您無法在 EC2-Classical 中啟動 DC2 叢集。如需詳細資訊，請參閱 [在 VPC 中建立叢集](#)。

節點類型具備不同的大小。節點大小和節點數量決定了叢集的總儲存量。如需詳細資訊，請參閱 [節點類型詳細資訊](#)。

部分節點類型允許一個節點 (單節點) 或兩個以上的節點 (多節點)。某些節點類型叢集節點的數量下限是兩個節點。在單節點叢集上，節點由領導者和運算功能共享。不建議執行生產工作負載時使用單一節

點叢集。在多節點叢集上，領導節點與運算節點各自獨立。領導節點與運算節點的節點類型相同。您只需支付運算節點的費用。

Amazon Redshift 會將配額套用至每個 AWS 區域中每個 AWS 帳戶的資源。配額限制會限制您的帳號可針對某個 AWS 區域內的特定資源類型 (例如節點或快照) 建立的資源數量。如需套用至 Amazon Redshift 資源之預設配額的相關資訊，請參閱《Amazon Web Services 一般參考》中的 [Amazon Redshift 限制](#)。如需申請提高配額，請提交 [Amazon Redshift 限制提高表單](#)。

叢集的成本取決於 AWS 區域、節點類型、節點數目，以及節點是否預先保留。如需節點成本的相關資訊，請參閱 [Amazon Redshift 定價](#) 頁面。

節點類型詳細資訊

下表摘要說明各節點類型和大小的節點規格。表格中的標頭具有下列意義：

- vCPU 為各節點的虛擬 CPU 數量。
- RAM 為各節點的記憶體容量，以 GiB 為單位。
- 「每個節點的配量數」是在建立叢集或使用傳統調整大小進行大小調整時，運算節點分割成的配量數。

如果叢集使用彈性調整來調整大小，則每一節點的配量數目可能會改變。不過，在彈性調整大小之後，叢集中所有運算節點上的切片總數仍然相同。

當您使用來自快照操作的還原建立叢集時，如果您變更了節點類型，結果叢集的配量數可能會與原始叢集不同。

- 儲存為各節點的儲存容量與類型。
- 節點範圍是 Amazon Redshift 針對節點類型和大小所支援的最小和最大節點數量。

Note

您可能只能使用較少的節點，具體取決於您在所選 AWS 區域中套用至您 AWS 帳戶的配額。如需申請提高配額，請提交 [Amazon Redshift 限制提高表單](#)。

- 總容量是叢集的總儲存容量，假如您部署了節點範圍中所指定的節點最大數量。

RA3 節點類型

節點類型	vCPU	RAM (GiB)	每個節點的預設配量	每個節點的受管儲存限制 ¹	具有建立叢集的節點範圍	受管儲存總容量 ²
ra3.xlplus (單節點)	4	32	2	4 TB	1	4 TB ³
ra3.xlplus (多節點)	4	32	2	32 TB	2–16 ⁴	1024 TB ⁴
ra3.4xlarge	12	96	4	128 TB	2–32 ⁵	8192 TB ⁵
ra3.16xlarge	48	384	16	128 TB	2–128	16,384 TB

¹ Amazon Redshift 受管儲存的儲存限制。此為硬性限制。

² 受管儲存總限制是節點數目上限乘以每個節點的受管儲存限制。

³ 若要將單節點叢集的大小調整為多節點，則只支援傳統調整大小。

⁴ 您可以使用具有多達 16 個節點的 ra3.xlplus (多節點) 節點類型來建立叢集。至於多節點叢集，則可以使用彈性調整大小來將大小調整為最多 32 個節點。

⁵ 您可以使用具有多達 32 個節點的 ra3.4xlarge 節點類型來建立叢集。您可以使用彈性調整大小將其大小調整為最多 64 個節點。

密集運算節點類型

節點類型	vCPU	RAM (GiB)	每個節點的預設配量	每個節點的儲存體	節點範圍	總容量
dc2.large	2	15	2	160 GB NVMe-SSD	1–32	5.12 TB
dc2.8xlarge	32	244	16	2.56 TB NVMe-SSD	2–128	326 TB

Note

密集化儲存 (DS2) 節點類型已不再可用。

先前的節點類型名稱

在先前的 Amazon Redshift 版本中，特定節點類型具有不同的名稱。您可以在亞 Amazon Redshift API 和 AWS CLI。但我們建議您升級任何參考這些名稱的指令碼，使用最新的名稱。目前名稱和先前名稱如下所示。

目前名稱	先前名稱
ds2.xlarge	ds1.xlarge、dw.hs1.xlarge、dw1.xlarge
ds2.8xlarge	ds1.8xlarge、dw.hs1.8xlarge、dw1.8xlarge
dc1.large	dw2.large
dc1.8xlarge	dw2.8xlarge

決定節點數目

Amazon Redshift 會將查詢平行分配到所有叢集的運算節點上執行，因此只要在叢集中新增節點，即可提高查詢效能。執行包含至少兩個運算節點的叢集時，每個節點上的資料會鏡射至另一節點的磁碟上，如此可降低資料遺失的風險。

您可以在 Amazon Redshift 主控台和亞馬遜 CloudWatch 指標中監控查詢效能。您也可以視需要新增或移除節點，在價格與效能間為您的叢集取得平衡。要求增加節點時，Amazon Redshift 會處理關於部署、負載平衡和資料維護的所有詳細資訊。如需叢集效能的相關資訊，請參閱 [監控 Amazon Redshift 叢集效能](#)。

預留節點適合穩定狀態的生產工作負載，且提供較隨需節點更多的折扣。您可以在執行實驗後購買預留節點，並 proof-of-concepts 驗證您的生產組態。如需詳細資訊，請參閱 [購買 Amazon Redshift 預留節點](#)。

暫停叢集時，可讓您在叢集暫停期間暫停隨需帳單。在此暫停期間，您只需支付備份儲存的費用。這樣就不必在需求出現之前預先規劃和購買資料倉儲容量，並讓您能在開發或測試時，以經濟實惠的方式管理環境。

如需隨需節點和預留節點的定價相關資訊，請參閱 [Amazon Redshift 定價](#)。

在建立叢集時使用 EC2-VPC

Amazon Redshift 叢集會在針對您所選 Amazon Redshift 節點類型和大小所設定的 Amazon EC2 執行個體中執行。使用 EC2-VPC 建立叢集。如果您仍在使用 EC2-Classical，我們建議您使用 EC2-VPC 來改善效能和安全。如需有關這些聯網平台的詳細資訊，請參閱 Amazon EC2 使用者指南中的 [支援平台](#)。您的 AWS 帳戶設定會決定您是否可以使用 EC2-VPC 或 EC2-典型版。

Note

為避免 SQL 用戶端工具和 Amazon Redshift 資料庫之間發生連線問題，建議您採取下列兩項動作其中之一。設定傳入規則，允許主機協調封包大小。或者，在 Amazon EC2 執行個體的網路界面 (NIC) 上將最大傳輸單位 (MTU) 設定為 1500，停用 TCP/IP 巨型訊框。如需這些方法的相關資訊，請參閱 [查詢似乎沒有回應且有時無法觸達叢集](#)。

EC2-VPC

使用 EC2-VPC 時，您的叢集會在邏輯上與您的 AWS 帳戶隔離的虛擬私有雲 (VPC) 中執行。如果您在 EC2-VPC 中佈建叢集，您可將一或多個 VPC 安全群組與叢集建立關聯，以控制叢集的存取。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的 [VPC 的安全群組](#)。

若要在 VPC 中建立叢集，您必須提供 VPC 的子網路資訊，然後在叢集啟動時提供子網路群組，先建立 Amazon Redshift 叢集子網路群組。如需詳細資訊，請參閱 [Amazon Redshift 叢集子網路群組](#)。

如需 Amazon Virtual Private Cloud (Amazon VPC) 的相關資訊，請參閱 [Amazon VPC 產品詳細資訊 頁面](#)。

預設磁碟空間警示

建立 Amazon Redshift 叢集時，您可以選擇性地設定 Amazon CloudWatch 警示，以監控叢集中所有節點使用的平均磁碟空間百分比。我們將此警示稱為預設磁碟空間警示。

預設磁碟空間警示的作用是幫助您監控叢集的儲存容量。您可依據資料倉儲需求設定此警示。例如，您可用警告做為需要調整叢集大小的指示。您可調整叢集大小為不同的節點類型，或新增節點，或是購買預留節點以供日後擴充。

當磁碟使用量達到或超過指定百分比經過一定的次數和指定持續期間，便會觸發預設磁碟空間警示。根據預設，此警示會在達到指定百分比時觸發，並保持在該百分比之上超過五分鐘。您可在啟動叢集後編輯預設值。

觸發 CloudWatch 警示時，Amazon Simple Notification Service (Amazon SNS) 會傳送通知給指定的收件人，以警告他們達到百分比閾值。Amazon SNS 會使用主題來指定收件人和要在通知中傳送的訊息。您可用現有的 Amazon SNS 主題，或在啟動叢集時依指定設定建立主題。您可在啟動叢集後編輯此警示的主題。如需建立 Amazon SNS 主題的相關資訊，請參閱 [開始使用 Amazon Simple Notification Service](#)。

啟動叢集之後，您可以從叢集的 [狀態] 視窗 [CloudWatch 警示] 下檢視和編輯警示。名稱為 `percentage-disk-space-used-default-<string>`。您可開啟警示，以檢視與其相關聯的 Amazon SNS 主題並編輯警示設定。如果您未選取要使用的現有 Amazon SNS 主題，則為您建立的主題會命名為 `<####>-預設警示 (<###>)`；例如 `(notify@example.com).examplecluster-default-alarms`

如需設定及編輯預設磁碟空間警示的相關資訊，請參閱 [建立叢集](#) 和 [建立或編輯磁碟空間警示](#)。

Note

如果刪除叢集，與叢集相關聯的警示將不會刪除，但也不會觸發。如果您不再需要警報，可以從 CloudWatch 主控台刪除鬧鐘。

叢集狀態

叢集狀態顯示叢集的目前狀態。下表提供各叢集狀態的說明。

狀態	描述
available	叢集正在執行且可使用。
available, prep-for-resize	叢集正在準備進行彈性調整大小。叢集在執行中且可用於讀取和寫入查詢，但無法使用某些叢集操作，例如建立快照。
available, resize-cleanup	彈性調整大小操作正在完成將資料傳輸到新叢集節點。叢集在執行中且可用於讀取和寫入查詢，但無法使用某些叢集操作，例如建立快照。
cancelling- resize	調整大小的作業正在取消。
creating	Amazon Redshift 正在建立叢集。如需詳細資訊，請參閱 建立叢集 。
deleting	Amazon Redshift 正在刪除叢集。如需詳細資訊，請參閱 刪除叢集 。
final-snapshot	Amazon Redshift 正在刪除叢集之前為其建立最後快照。如需詳細資訊，請參閱 刪除叢集 。
hardware- failure	叢集發生硬體故障。 如果您有一個單一節點的叢集，該節點將無法替換。若要恢復叢集，請還原快照。如需詳細資訊，請參閱 Amazon Redshift 快照和備份 。
incompatible- hsm	Amazon Redshift 無法連線到硬體安全模組 (HSM)。請檢查叢集和 HSM 之間的 HSM 組態。如需詳細資訊，請參閱 使用硬體安全模組的 Amazon Redshift 加密 。

狀態	描述
incompatible-network	基本網路組態發生問題。確認您啟動叢集所在的 VPC 存在且其設定正確。如需詳細資訊，請參閱 管理 VPC 中的叢集 。
incompatible-parameters	相關聯參數群組中有一或多個參數值發生問題，且無法套用參數值或數值。請修改參數群組並更新任何無效的值。如需詳細資訊，請參閱 Amazon Redshift 參數群組 。
incompatible-restore	從快照還原叢集時發生問題。請再次嘗試從其他快照還原叢集。如需詳細資訊，請參閱 Amazon Redshift 快照和備份 。
modifying	Amazon Redshift 正在套用變更至叢集。如需詳細資訊，請參閱 修改叢集 。
paused	叢集已暫停。如需詳細資訊，請參閱 暫停和繼續叢集 。
rebooting	Amazon Redshift 正在重新啟動叢集。如需詳細資訊，請參閱 重新啟動叢集 。
renaming	Amazon Redshift 正在套用新名稱至叢集。如需詳細資訊，請參閱 重新命名叢集 。
resizing	Amazon Redshift 正在調整叢集的大小。如需詳細資訊，請參閱 調整叢集大小 。
rotating-keys	Amazon Redshift 正在輪換叢集的加密金鑰。如需詳細資訊，請參閱 Amazon Redshift 中的加密金鑰輪換 。
storage-full	叢集已達到其儲存容量。請調整叢集的大小，以新增節點或選擇不同的節點大小。如需詳細資訊，請參閱 調整叢集大小 。
updating-hsm	Amazon Redshift 正在更新 HSM 組態。

使用 Amazon Redshift 佈建叢集的注意事項

建立叢集之後，您可以在本節中找到有關可用功能的區域、維護工作、節點類型和使用限制的相關資訊。

主題

- [區域與可用區域的考量](#)
- [叢集維護](#)
- [管理 Amazon Redshift 中的用量限制](#)
- [RA3 節點支援的聯網功能](#)
- [節點類型](#)

區域與可用區域的考量

Amazon Redshift 在多個 AWS 區域提供。根據預設，Amazon Redshift 會在您選擇的區 AWS 域內隨機選取的可用區域 (AZ) 佈建叢集。所有叢集節點將佈建在相同的可用區域中。

如果該區域可使用 Amazon Redshift，您可以選擇請求該特定可用區域。例如，若您有一個 Amazon EC2 執行個體在一個可用區域內執行，您可能會想將 Amazon Redshift 叢集建立在相同的區域內，以降低延遲。另一方面，您可能會想選擇其他可用區域以獲得更高的可用性。某 AWS 個區域內的所有可用區域可能無法使用 Amazon Redshift。

如需可在其中佈建 Amazon Redshift 叢集的受支援 AWS 區域清單，請參閱[中的](#) Amazon Web Services 一般參考

叢集維護

Amazon Redshift 會定期執行維護，以套用升級至您的叢集。在這些更新期間，您的 Amazon Redshift 叢集無法執行正常的操作。您有多種方法可以控制我們如何維護您的叢集。例如，您可以控制我們何時將更新部署到您的叢集。您也可以選擇是否讓叢集一律執行最新發行的版本，或在最新發行版本之前發行的版本。最後，您可以選擇將非強制的維護更新延遲為一段期間。

主題

- [維護時段](#)
- [延遲維護](#)
- [選擇叢集維護軌道](#)
- [管理叢集版本](#)
- [轉返叢集版本](#)
- [判斷叢集維護版本](#)

維護時段

Amazon Redshift 會隨機指派 30 分鐘的維護時段，為每個區域 8 小時的時間 AWS 區塊隨機指派，發生在一週中的隨機日期 (包括週一至週日)。

預設維護時段

下列清單顯示指定預設維護時段之每個「AWS 區域」的時間區塊：

- 美國東部 (維吉尼亞北部) 區域：03:00–11:00 UTC
- 美國東部 (俄亥俄) 區域：03:00–11:00 UTC
- 美國西部 (加利佛尼亞北部) 區域：06:00–14:00 UTC
- 美國西部 (奧勒岡) 區域：06:00–14:00 UTC
- 非洲 (開普敦) 區域：20:00–04:00 UTC
- 亞太區域 (香港) 區域：13:00–21:00 UTC
- 亞太區域 (海德拉巴) 區域：16:30–00:30 UTC
- 亞太區域 (雅加達) 區域：15:00–23:00 UTC
- 亞太區域 (墨爾本) 區域：12:00–20:00 UTC
- 亞太區域 (孟買) 區域：16:30–00:30 UTC
- 亞太區域 (大阪) 區域：13:00–21:00 UTC
- 亞太區域 (首爾) 區域：13:00–21:00 UTC
- 亞太區域 (新加坡) 區域：14:00–22:00 UTC
- 亞太區域 (雪梨) 區域：12:00–20:00 UTC
- 亞太區域 (東京) 區域：13:00–21:00 UTC
- 加拿大 (中部) 區域：03:00–11:00 UTC
- 加拿大西部 (卡加利) 區域：04:00–12:00 UTC
- 中國 (北京) 區域：13:00–21:00 UTC
- 中國 (寧夏) 區域：13:00–21:00 UTC
- 歐洲 (法蘭克福) 區域：06:00–14:00 UTC
- 歐洲 (愛爾蘭) 區域：22:00–06:00 UTC
- 歐洲 (倫敦) 區域：22:00–06:00 UTC
- 歐洲 (米蘭) 區域：21:00–05:00 UTC

- 歐洲 (巴黎) 區域 : 23:00–07:00 UTC
- 歐洲 (斯德哥爾摩) 區域 : 23:00–07:00 UTC
- 歐洲 (蘇黎世) 區域 : 20:00–04:00 UTC
- 以色列 (特拉維夫) 區域 : 20:00–04:00 UTC
- 歐洲 (西班牙) 區域 : 21:00–05:00 UTC
- 中東 (巴林) 區域 : 13:00–21:00 UTC
- 中東 (阿拉伯聯合大公國) 區域 : 18:00–02:00 UTC
- 南美洲 (聖保羅) 區域 : 19:00–03:00 UTC

如果在特定週排程維護事件，事件會在指定的 30 分鐘維護時段內啟動。Amazon Redshift 執行維護時，會終止任何查詢或其他進行中的操作。多數的維護會在 30 分鐘維護時段內完成，但部分的維護作業可能會在時段結束後繼續執行。如果排程的維護時段內沒有要執行的維護作業，叢集將繼續正常運作，直到下次排程的維護時段。

您可以透過程式設計的方式或使用 Amazon Redshift 主控台修改叢集，以變更排程的維護時段。您可以在 [維護] 索引標籤下找到維護時段，並設定叢集發生的日期和時間。

叢集有可能在維護時段外重新啟動。有幾個原因會導致這種情況發生。還有一個常見原因是叢集偵測到問題，因此系統執行維護操作以使叢集恢復良好狀態。如需詳細資訊，請參閱[為何我的 Amazon Redshift 叢集在維護時段外重新啟動？](#)一文，其中會提供有關為何會發生這種情況的詳細資訊。

延遲維護

若要重新排程叢集的維護時段，您可以將維護延遲最多 45 天。例如，如果叢集的維護時段設為星期三 08:30 – 09:00 UTC，而您需要在這個時間存取叢集，則可以將維護時段延後。

如果您延後維護時段，Amazon Redshift 仍會對叢集套用硬體更新或其他強制性的安全更新。在這些更新期間，您的叢集無法使用。

如果在維護時段即將到來時排定了硬體更新或其他強制性的安全更新，Amazon Redshift 會在待分類別下傳送預先通知給您。若要進一步了解待定事件通知，請參閱[Amazon Redshift 事件通知](#)。

您也可以選擇從 Amazon Simple Notification Service (Amazon SNS) 接收事件通知。如需訂閱 Amazon SNS 事件通知的相關資訊，請參閱[訂閱 Amazon Redshift 叢集事件通知](#)。

如果您延遲叢集的維護，就無法再將所延遲時段後的下一個維護時段延遲。

Note

維護開始後就不能延遲。

如需叢集維護的相關資訊，請參閱以下文件：

- [維護時段](#)
- [使用主控台管理叢集](#)
- [修改叢集](#)

選擇叢集維護軌道

當 Amazon Redshift 發行新的叢集版本時，叢集會在維護時段內更新。您可控制是否要將叢集更新至最新核准的版本或先前的版本。

維護軌道可控制在維護時段內套用什麼叢集版本。當 Amazon Redshift 發行新的叢集版本時，該版本會指派到「目前」軌道，而先前版本會指派到「追蹤」軌道。若要設定叢集的維護軌道，請指定下列其中一個值：

- 目前 — 使用最新核准的叢集版本。
- 追蹤 — 使用目前版本之前的叢集版本。
- 預覽 — 使用包含可供預覽之新功能的叢集版本。

例如，假設您的叢集目前執行 1.0.2762 版，而 Amazon Redshift 目前版本是 1.0.3072。如果您將維護軌道值設為 Current (目前)，叢集會在下次維護時段更新為 1.0.3072 版 (下一個核准版本)。如果您將維護軌道值設為 Trailing (追蹤)，則叢集要直到 1.0.3072 版之後有新版本時才會更新。

預覽軌道

您不一定可以選擇 Preview (預覽) 軌道。當您選擇 Preview (預覽) 軌道時，必須選取軌道名稱。預覽軌道及其相關資源是暫時性的、具有功能限制，而且可能不會包含其他軌道中可用的所有目前 Amazon Redshift 功能。使用預覽軌道時：

- 使用預覽追蹤時，請使用新的 Amazon Redshift 主控台。例如，當您建立叢集以使用預覽功能時。
- 您無法將叢集從某個預覽軌道切換至另一個。
- 您無法將叢集從目前或追蹤軌道切換至預覽軌道。

- 您無法將叢集從預覽軌道切換至目前或追蹤軌道。
- 您無法從透過不同預覽軌道建立的快照還原。
- 您只能在建立新的叢集或從快照還原時，使用預覽軌道。
- 您無法從透過不同預覽軌道建立的快照還原，或使用比預覽軌道叢集版本更新的叢集維護版本進行還原。例如，當您將叢集還原至預覽軌道時，您只能使用從比預覽軌道更舊的叢集維護版本建立的快照。

切換維護軌道

變更叢集的軌道通常為一次性的決定。變更軌道時請務必謹慎。如果您將維護軌道從 Trailing (追蹤) 變更為 Current (目前)，我們會在下次維護時段將叢集更新為 Current (目前) 軌道發行版本。不過，如果您將叢集的維護軌道變更為 Trailing (追蹤)，我們會等到 Current (目前) 軌道發行版本之後有新版本時才更新您的叢集。

維護軌道和還原

快照繼承來源叢集的維護軌道。如果您在建立快照之後變更來源叢集的維護軌道，則快照和來源叢集會在不同的軌道上。從快照還原時，新叢集會在繼承自來源叢集的維護軌道上。您可在還原操作完成後變更維護軌道。調整叢集的大小不會影響叢集的維護軌道。

管理叢集版本

維護軌道是一系列的版本。您可以決定叢集是在目前軌道還是追蹤軌道上。如果您將叢集放在目前軌道上，則叢集在維護時段內一律會升級到最新的叢集發行版本。如果您將叢集放在追蹤軌道上，則叢集一律會執行就在/最新發行版本前發行的叢集發行版本。

Amazon Redshift 主控台叢集清單中的發行狀態資料欄會指出您的其中一個叢集是否可供升級。

轉返叢集版本

如果您的叢集是最新的叢集版本，您可以選擇將它轉返為之前的版本。

如需每個叢集版本所包含之功能和改善的詳細資訊，請參閱 [叢集版本歷史記錄](#)。

轉返為先前的叢集版本

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽選單上，選擇叢集。
3. 選擇要轉返的叢集。

4. 針對 Actions (動作)，選擇 Roll back cluster version (轉返叢集版本)。Roll back cluster version (轉返叢集版本) 頁面隨即出現。
5. 如有可供轉返的版本，請遵循頁面說明以進行操作。
6. 選擇 Roll back now (立即轉返)。

判斷叢集維護版本

您可以使用 Amazon Redshift 主控台判斷 Amazon Redshift 引擎和資料庫版本。

尋找叢集的版本

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽功能表上，選擇叢集，然後從清單中選擇叢集名稱以開啟其詳細資訊。隨即顯示叢集的詳細資訊，包含叢集效能、查詢監控、資料庫、資料共用、排程、維護和屬性標籤。
3. 選擇維護索引標籤以取得詳細資訊。
4. 在 Maintenance (維護) 區段中，尋找 Current cluster version (目前的叢集版本)。

Note

雖然主控台將此資訊顯示在同一個欄位中，但這些其實是 Amazon Redshift API 中的兩個參數：ClusterVersion 和 ClusterRevisionNumber。如需詳細資訊，請參閱《Amazon Redshift API 參考》中的[叢集](#)。

管理 Amazon Redshift 中的用量限制

您可以定義限制以限制及控制某些 Amazon Redshift 功能的用量和相關成本。您可以建立每日、每週和每月用量限制，並定義達到這些限制時 Amazon Redshift 會自動採取的動作。動作包括將事件記錄到系統資料表，以記錄超過定義限制的用量。其他可能動作包括向 Amazon SNS 和 Amazon CloudWatch 提出警示，以通知管理員並停用進一步的使用，以控制成本。

您可以定義每個叢集的用量限制。建立叢集之後，您可以定義下列功能的用量限制：

- Amazon Redshift Spectrum
- Amazon Redshift 並行擴展

- Amazon Redshift 跨區域資料共用

在 Amazon Redshift Spectrum 和 Amazon Redshift 並行擴展可用的 AWS 區域中，用量限制可用於發行版本 1.0.14677 或更高版本。

Redshift Spectrum 限制以 1 TB 的增量指定掃描資料總數的閾值。並行擴展限制以 1 分鐘為增量，指定並行擴展所使用的總時間量閾值。跨區域資料共用限制以 1 TB 的增量指定掃描資料總數的閾值。

您可以為每日、每週或每月期間指定一個限制 (使用 UTC 來確定期間的開始和結束)。如果您在期間中建立一個限制，則該限制會從該時間點算到該期間結束。例如，如果您在 3 月 15 日建立每月限制，則第一個每月期間是從 3 月 15 日算到 3 月 31 日。

您可以為每個功能定義多個用量限制。每個限制可以有不同的動作。可能的動作包括下列各項：

- 記錄至系統資料表 — 這是預設動作。資訊會記錄到 STL_USAGE_CONTROL 資料表。評估過去的用量和決定未來的用量限制時，記錄會很有幫助。如需所記錄項目的詳細資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的 [STL_USAGE_CONTROL](#)。
- 警示 — Amazon Redshift 會針對可用和已使用的用量發出 CloudWatch 指標。您最多可以為每個功能定義三個用量限制。如果您使用 Amazon Redshift 主控台啟用警示動作，CloudWatch 會在這些指標上自動建立警示。您可以選擇性地將 Amazon SNS 訂閱連接至該警示。如果您使用 AWS CLI 或 API 操作，請務必手動建立 CloudWatch 警示。達到閾值時，也會將事件記錄到系統資料表中。
- 停用功能 — 達到閾值時，Amazon Redshift 會停用功能，直到下一個時段 (每日、每週或每月) 重新整理配額為止。每個功能只能有一個限制可以執行停用動作。也會將事件記錄到系統資料表，而且會發出警示。

用量限制將一直持續到刪除用量限制定義本身或叢集為止。

您可以使用新的 Amazon Redshift 主控台、AWS CLI 或 Amazon Redshift API 操作，定義及管理用量限制。若要在 Amazon Redshift 主控台上定義限制，請導覽至叢集，並針對動作選擇設定用量限制。若要針對您的叢集檢視先前定義的用量限制，請導覽至您的叢集，並依序選擇維護索引標籤、用量限制區段。若要針對您的叢集檢視可使用量和已使用量，請導覽至您的叢集。選擇叢集效能索引標籤，然後查看圖表以了解功能的已使用量。

您可以使用下列 Amazon Redshift CLI 操作來管理用量限制。如需詳細資訊，請參閱《AWS CLI 命令參考》。

- [create-usage-limit](#)
- [describe-usage-limits](#)

- [modify-usage-limit](#)
- [delete-usage-limit](#)

您可以使用下列 Amazon Redshift API 操作來管理用量限制。如需詳細資訊，請參閱《Amazon Redshift API 參考》。

- [CreateUsageLimit](#)
- [DescribeUsageLimits](#)
- [ModifyUsageLimit](#)
- [DeleteUsageLimit](#)

觀看以下影片以了解如何使用 Amazon Redshift 主控台建立和監控用量限制：[Amazon Redshift Spectrum 和並行擴展的成本控制](#)。

RA3 節點支援的聯網功能

RA3 節點支援其他節點類型無法使用的網路功能集合。本節提供每個功能的簡要說明以及其他文件的連結：

- 已佈建的叢集 VPC 人雲端端點 — 當您建立或還原 RA3 叢集時，Amazon Redshift 會使用範圍在 5431-5455 或 8191-8215 範圍內的連接埠。將叢集設定為其中一個範圍內的連接埠時，Amazon Redshift 會在您的 AWS 帳戶中為叢集自動建立 VPC 端點，並在其中附加私有 IP 地址。如果您將叢集設定為可公開存取，Redshift 會在您的 AWS 帳戶中建立彈性 IP 位址，並將其附加到 VPC 端點。如需詳細資訊，請參閱 [Amazon Redshift 叢集或 Amazon Redshift 無伺服器工作群組設定安全群組通訊設定](#)。
- 單一子網路 RA3 叢集 — 您可以建立具有單一子網路的 RA3 叢集，但其無法使用災難復原功能。如果您在子網路沒有多個可用區域 (AZ) 時啟用叢集重新定位，就會發生例外狀況。
- 多重子網路 RA3 叢集和子網路群組 — 您可以在虛擬私人雲端 (VPC) 中佈建叢集時建立子網路群組，藉此建立具有多個子網路的 RA3 叢集。叢集子網路群組可讓您在 VPC 中指定一組子網路，而 Amazon Redshift 則會在其中一個子網路中建立叢集。建立子網路群組後，您可以移除先前新增的子網路，或新增其他子網路。如需詳細資訊，請參閱 [Amazon Redshift 叢集子網路群組](#)。
- 跨帳戶或跨 VPC 端點存取 — 您可以透過設定 RedShift 管理的 VPC 端點，存取佈建的叢集或 Amazon Redshift 無伺服器工作群組。例如，您可以將其設定為包含叢集或工作群組的 VPC 和執行用戶端工具的 VPC 之間的私人連線。這樣，您就可以存取資料倉儲，而無需使用公用 IP 位址，也不需要透過網際網路路由傳送流量。如需詳細資訊，請參閱 [使用由 RedShift 管理的 VPC 端點](#)。

- 叢集重新定位 — 當服務中斷時，您可以將叢集移至另一個可用區域 (AZ)，而不會遺失任何資料。您可以在主控台上啟用此功能。如需詳細資訊，請參閱 [重新定位叢集](#)。
- 自訂網域名稱 — 您可以為 Amazon Redshift 叢集建立自訂網域名稱 (也稱為自訂 URL)。它是將 SQL 用戶端連線路由到叢集端點的 easy-to-read DNS 記錄。如需詳細資訊，請參閱 [使用自訂網域名稱來進行用戶端連線](#)。

節點類型

這些章節詳細說明了各種節點類型可用的工作。

主題

- [節點](#)
- [DC2 節點類型](#)

節點

這些章節詳細說明 RA3 節點可用的工作。

主題

- [概觀](#)
- [升級至 RA3 節點類型](#)

概觀

RA3 節點提供下列優點：

- 其具備彈性，可在不增加儲存成本的情況下增加您的運算容量。且其可在不過度佈建運算容量的情況下擴展您的儲存體。
- 其針對您的熱資料使用高效能 SSD，針對冷資料則使用 Amazon S3。因此，這些節點提供了易於使用且符合成本效益的儲存體及高查詢效能。
- 他們使用 AWS Nitro 系統上建置的高頻寬聯網，進一步減少將資料卸載到 Amazon S3 和從 Amazon S3 擷取所需的時間。

請考慮在這些案例中選擇 RA3 節點類型：

- 您需要與儲存體分開擴展運算及為其支付費用的彈性時。

- 您只查詢總資料的一小部分。
- 您的資料量正在迅速成長或預期會快速成長。
- 您希望靈活地根據您的效能需求調整叢集大小。

若要使用 RA3 節點類型，您的 AWS 地區必須支援 RA3。如需詳細資訊，請參閱 [區域中 RA3 節點型態可用性 AWS](#)。

Important

您只能搭配 1.0.21262 或更新版本的叢集版本使用 ra3.xlplus 節點類型。您可以使用 Amazon Redshift 主控台檢視現有叢集的版本。如需詳細資訊，請參閱 [判斷叢集維護版本](#)。

請務必在使用 RA3 節點類型時使用新的 Amazon Redshift 主控台。

此外，如要搭配使用維護追蹤的 Amazon Redshift 操作使用 RA3 節點類型，維護追蹤的值必須設為支援 RA3 的叢集版本。如需維護追蹤的相關資訊，請參閱 [選擇叢集維護軌道](#)。

在使用單節點 RA3 節點類型時，請考量下列事項。

- 支援資料共用生產者和取用者。
- 若要變更節點類型，則只支援傳統調整大小。不支援使用彈性調整大小或快照還原來變更節點類型。支援以下情況：
 - 透過傳統調整大小將單節點 dc2.xlarge 變更為單節點 ra3.xlplus，反之亦然。
 - 透過傳統調整大小將單節點 dc2.xlarge 變更為多節點 ra3.xlplus，反之亦然。
 - 透過傳統調整大小將多節點 dc2.xlarge 變更為單節點 ra3.xlplus，反之亦然。

使用 Amazon Redshift 受管儲存

透過 Amazon Redshift 受管儲存，您可以在 Amazon Redshift 中儲存和處理您所有的資料，同時取得更大的彈性來分別擴展運算和儲存容量。您可以繼續使用 COPY 或 INSERT 命令來擷取資料。為了最佳化效能和管理不同儲存層的自動資料置放，Amazon Redshift 會利用最佳化 (例如資料區塊溫度、資料區塊年齡和工作負載模式)。當需要時，Amazon Redshift 或自動將儲存擴展至 Amazon S3，無須任何手動動作。

如需有關儲存成本的資訊，請參閱 [Amazon Redshift 定價](#)。

管理 RA3 節點類型

如要利用將運算與儲存分開的優勢，您可以使用 RA3 節點類型建立或升級您的叢集。如要使用 RA3 節點類型，請在虛擬私有雲端 (EC2-VPC) 中建立您的叢集。

如要變更 RA3 節點類型之 Amazon Redshift 叢集的節點數，請執行以下其中一項作業：

- 使用彈性調整大小操作新增或移除節點。在某些情況下，不允許使用彈性調整大小從 RA3 叢集移除節點。例如，當 2:1 節點計數升級將每個節點的配量數設為 32 時。如需詳細資訊，請參閱 [調整叢集大小](#)。如果無法使用彈性調整大小，請使用傳統調整大小。
- 使用傳統調整大小操作新增或移除節點。當您調整大小至無法透過彈性調整大小來使用的組態時，請選擇此選項。彈性調整大小比傳統調整大小更快。如需詳細資訊，請參閱 [調整叢集大小](#)。

區域中 RA3 節點型態可用性 AWS

RA3 節點類型僅適用於下列 AWS 區域：

- 美國東部 (維吉尼亞北部) 區域 (us-east-1)
- 美國東部 (俄亥俄) 區域 (us-east-2)
- 美國西部 (加利佛尼亞北部) 區域 (us-west-1)
- 美國西部 (奧勒岡) 區域 (us-west-2)
- 非洲 (開普敦) 區域 (af-south-1)
- 亞太區域 (香港) 區域 (ap-east-1)
- 亞太區域 (海德拉巴) 區域 (ap-south-2)
- 亞太區域 (雅加達) 區域 (ap-southeast-3)
- 亞太區域 (墨爾本) 區域 (ap-southeast-4)
- 亞太區域 (孟買) 區域 (ap-south-1)
- 亞太區域 (大阪) 區域 (ap-northeast-3)
- 亞太區域 (首爾) 區域 (ap-northeast-2)
- 亞太區域 (新加坡) 區域 (ap-southeast-1)
- 亞太區域 (雪梨) 區域 (ap-southeast-2)
- 亞太區域 (東京) 區域 (ap-northeast-1)
- 加拿大 (中部) 區域 (ca-central-1)
- 加拿大西部 (卡加利) 區域 (ca-west-1)
- 中國 (北京) 區域 (cn-north-1)

- 中國 (寧夏) 區域 (cn-northwest-1)
- 歐洲 (法蘭克福) 區域 (eu-central-1)
- 歐洲 (蘇黎世) 區域 (eu-central-2)
- 歐洲 (愛爾蘭) 區域 (eu-west-1)
- 歐洲 (倫敦) 區域 (eu-west-2)
- 歐洲 (米蘭) 區域 (eu-south-1)
- 歐洲 (西班牙) 區域 (eu-south-2)
- 歐洲 (巴黎) 區域 (eu-west-3)
- 歐洲 (斯德哥爾摩) 區域 (eu-north-1)
- 以色列 (特拉維夫) 區域 (il-central-1)
- 中東 (巴林) 區域 (me-south-1)
- 中東 (阿拉伯聯合大公國) 區域 (me-central-1)
- 南美洲 (聖保羅) 區域 (sa-east-1)
- AWS GovCloud (美國東部) (美國往東 1)
- AWS GovCloud (美國西部) (美國-往西 -1)

升級至 RA3 節點類型

如要將現有節點類型升級為 RA3，您可以使用下列選項來變更節點類型：

- 從快照還原 — Amazon Redshift 會使用叢集的最新快照並將其還原以建立新的 RA3 叢集。在叢集建立完成時 (通常在數分鐘內)，RA3 節點類型便已準備就緒，可執行您完整的生產工作負載。由於運算與儲存體分開，熱資料可受益於大型的聯網頻寬，快速地傳入本機快取。如果您從最新的 DC2 快照還原，RA3 會保留 DC2 工作負載的熱區塊資訊，並以最熱門的區塊填入其本機快取。如需詳細資訊，請參閱 [從快照還原叢集](#)。

若要為應用程式和使用者保持相同的端點，您可以使用與原始 DC2 叢集相同的名稱重新命名新 RA3 叢集。若要為此叢集重新命名，請在 Amazon Redshift 主控台或 `ModifyCluster` API 操作中修改叢集。如需詳細資訊，請參閱《Amazon Redshift API 參考》中的 [重新命名叢集](#) 或 [ModifyCluster API 操作](#)。

- 彈性調整大小 — 使用彈性調整大小調整叢集的大小。當您使用彈性調整大小來變更節點類型時，Amazon Redshift 會自動建立快照、建立新叢集、刪除舊叢集，並重新命名新的叢集。彈性調整大小操作可隨時執行，或排程在未來特定的時間執行。您可以透過彈性調整大小，快速將現有 DC2 節點類型叢集升級為 RA3。如需詳細資訊，請參閱 [彈性調整大小](#)。

下表顯示升級至 RA3 節點類型時的建議事項。(這些建議也適用於預留節點。)

此表格中的建議為啟動叢集節點類型和大小，但取決於工作負載的運算需求。為了更好地估計您的需求，請考慮進行使用「[試用方案](#)」執行潛在組態的概念驗證 (POC)。為您的 POC 資料倉儲佈建叢集，而不是 Redshift 無伺服器。如需有關[進行概念驗證的詳細資訊](#)，請參閱亞馬遜 Redshift 資料庫開發人員指南中的[針對亞馬 Amazon Redshift 執行概念驗證 \(POC\)](#)。

現有節點類型	現有節點數目	建議的新節點類型	升級動作
dc2.8xlarge	2–15	ra3.4xlarge	為每 1 個 dc2.8xlarge 節點建立 2 個 ra3.4xlarge 節點 ¹ 。
dc2.8xlarge	16–128	ra3.16xlarge	為每 2 個 dc2.8xlarge 節點建立 1 個 ra3.16xlarge 節點 ¹ 。
dc2.large	1–4	無	保留現有的 dc2.large 叢集。
dc2.large	5–15	ra3.xlplus	為每 8 個 dc2.large 節點建立 3 個 ra3.xlplus 節點 ¹ 。
dc2.large	16–32	ra3.4xlarge	為每 8 個 dc2.large 節點建立 1 個 ra3.4xlarge 節點 ^{1,2} 。

¹視工作負載需求而定，可能需要額外的節點。根據所需查詢效能的運算需求新增或移除節點。

²具有 dc2.large 節點類型的叢集會限制只能有 32 個節點。

某些 RA3 節點類型的節點數量下限是 2 個節點。在建立 RA3 叢集時，請考慮這一點。

DC2 節點類型

這些章節詳細說明 DC2 節點類型可用的工作。

叢集作業

建立叢集之後，您可以在叢集上執行數項操作。這些操作包括調整大小、暫停、繼續、重新命名和刪除。

主題

- [調整叢集大小](#)
- [暫停和繼續叢集](#)
- [重新命名叢集](#)
- [關閉及刪除叢集](#)
- [重新定位叢集](#)
- [Amazon Redshift 快照和備份](#)

調整叢集大小

當您的資料倉儲容量和效能需要變更時，您可以調整叢集大小，以充分利用 Amazon Redshift 的運算和儲存選項。

調整大小操作有兩種類型：

- 彈性調整大小 — 您可以在叢集中新增或移除節點。您也可以變更節點類型，例如從 DC2 節點變更為 RA3 節點。彈性調整大小通常會很快完成，平均需要十分鐘。因此，建議您將其作為第一個選項。當您執行彈性調整大小時，它會重新分散資料配量，這些資料配量是在每個節點中配置記憶體和磁碟空間的分割區。當您要進行下列操作時，就適合使用彈性調整大小：
 - 在現有叢集中新增或減少節點，但不變更節點類型 — 這通常稱為「就地」調整大小。當您執行此類型的調整大小時，某些執行中的查詢會成功完成，但其他查詢可能會在操作中遭到捨棄。
 - 變更叢集的節點類型 — 當您變更節點類型時，系統會建立快照，並將資料從來源叢集重新分散至包含新節點類型的叢集。完成後，執行中的查詢會遭到捨棄。和「就地」調整大小一樣，其也會快速完成。

- 傳統調整大小 — 您可以透過類似於彈性調整大小的方式來變更節點類型和 (或) 節點數目。傳統調整大小需要更多時間來完成，但是如果節點計數的變化或要遷移到的節點類型不在彈性調整大小的範圍內，傳統調整大小可能會很有用。例如，當節點計數的變化非常大時，就適用這種方式。

主題

- [彈性調整大小](#)
- [Elastic resize \(傳統調整大小\)](#)

彈性調整大小

當您新增或移除相同類型的節點時，彈性調整大小操作具有下列階段：

1. 彈性調整大小會取得叢集快照。此快照一律會包含節點的[不備份資料表](#) (如適用)。(RA3 等某些節點類型沒有不備份資料表。) 如果您的叢集因為您停用了自動快照而沒有最新的快照，備份操作會需要較長時間。(若要將調整大小操作開始之前的時間最小化，建議您啟用自動快照或在開始調整大小之前建立手動快照。) 當您啟動彈性調整大小且快照操作正在進行時，如果快照操作未在幾分鐘內完成，則調整大小可能會失敗。如需詳細資訊，請參閱 [Amazon Redshift 快照和備份](#)。
2. 此操作會遷移叢集中繼資料。叢集會有幾分鐘的時間無法使用。大多數查詢會暫時暫停，且會保持連線。但是，某些查詢則可能遭到捨棄。這個階段很快就會結束。
3. 工作階段連線會重新起始，並且查詢會繼續。
4. 彈性調整大小會在背景中將資料重新分散給節點配量。叢集可供讀寫操作，但有些查詢可能需要較長時間來執行。
5. 操作完成後，Amazon Redshift 會傳送事件通知。

當您使用彈性調整大小變更節點類型時，其運作方式與您新增或減少相同類型的節點時相似。首先，系統會建立快照。使用快照中的最新資料佈建新的目標叢集，並在背景中將資料傳輸到新的叢集。在此期間，資料是唯讀狀態。當調整大小操作接近完成時，Amazon Redshift 會更新端點以指向新的叢集，並中斷與來源叢集的所有連線。

彈性調整大小不太可能會失敗。但是，在發生故障的情況下，在大多數情況下都會自動進行復原，而無需任何手動介入。

如果您有保留節點 (例如 DC2 保留節點)，則可以在執行調整大小時升級至 RA3 保留節點。您可以在執行彈性調整大小或使用主控台從快照進行還原時進行升級。主控台會引導您完成此程序。如需升級至 RA3 節點的相關資訊，請參閱[升級至 RA3 節點類型](#)。

彈性調整大小不會排序資料表或回收磁碟空間，因此不是清空操作的替代方案。如需詳細資訊，請參閱[清空資料表](#)。

彈性調整大小有下列限制：

- 彈性調整大小和資料共用叢集 — 當您在作為資料共用生產者的叢集上新增或減少節點時，您無法在 Amazon Redshift 遷移叢集中繼資料時從取用者連線至該叢集。同樣地，如果您執行彈性調整大小並選擇新的節點類型，則在連線中斷並傳輸到新的目標叢集時，便無法使用資料共用。在這兩種類型的彈性調整大小中，生產者都會有幾分鐘的時間無法使用。
- 從共用快照傳輸資料 — 若要在從共用快照傳輸資料的叢集上執行彈性調整大小，必須至少有一個備份可供叢集使用。您可以在 Amazon Redshift 主控台快照清單、describe-cluster-snapshots CLI 命令或 DescribeClusterSnapshots API 操作上檢視備份。
- 平台限制 — 彈性調整大小僅供使用 EC2-VPC 平台的叢集使用。如需詳細資訊，請參閱[在建立叢集時使用 EC2-VPC](#)。
- 儲存考量 — 請確定新節點的組態有足夠的儲存可儲存現有資料。您可能必須新增其他節點或變更組態。
- 來源叢集與目標叢集的大小 — 彈性調整大小可以調整大小的節點數目和節點類型，取決於來源叢集中的節點數目和針對已調整大小的叢集所選擇的節點類型。若要判斷可用的組態，您可以使用主控台。或者，您可以將命令 describe-node-configuration-options AWS CLI 命令與 action-type resize-cluster 選項搭配使用。如需使用 Amazon Redshift 主控台來調整大小的相關資訊，請參閱[調整叢集大小](#)。

下列範例 CLI 命令會描述可用的組態選項。在此範例中，名為 mycluster 的叢集是一個 dc2.large 8 節點的叢集。

```
aws redshift describe-node-configuration-options --cluster-identifier mycluster --region eu-west-1 --action-type resize-cluster
```

此命令會傳回一個具有所建議節點類型的選項清單、節點數，以及每個選項的磁碟使用率。傳回的組態會因為特定的輸入叢集而不同。當您指定 resize-cluster CLI 命令的選項時，您可以選擇其中一個所傳回的組態。

- 其他節點的上限 — 彈性調整大小會限制您可以新增至叢集的節點數目。例如，dc2 叢集支援進行最多兩倍節點數目的彈性調整大小。為了說明，您可以在 4 節點的 dc2.8xlarge 叢集中新增一個節點，使其成為五節點的叢集，或新增更多節點，直到達到八個節點為止。

Note

增加和減少的限制取決於原始節點類型和原始叢集中的節點數目或其上次的傳統調整大小。如果彈性調整大小會超過增加或減少的限制，請使用傳統調整大小。

對於某些 ra3 節點類型，您最多可以將節點數目增加到現有計數的四倍。具體來說，假設您的叢集由 ra3.4xlarge 或 ra3.16xlarge 節點組成。然後，您可以使用彈性調整大小，將 8 節點的叢集中的節點數目增加到 32 個。或者，您也可以選擇低於限制的值。(請記住，將叢集增加 4 倍的能力取決於來源叢集的大小。) 如果您的叢集具有 ra3.xlplus 節點，則限制為兩倍。

所有 ra3 節點類型都支援將節點數目減少到現有計數的四分之一。例如，您可以將具有 ra3.4xlarge 節點的叢集大小從 12 個節點減少到 3 個，或減少到高於下限的數目。

下表列出每個支援彈性調整大小之節點類型的增加和減少限制。

原始節點類型	增加限制	減少限制
ra3.16xlarge	4 倍 (例如，從 4 個節點到 16 個節點)	減少到四分之一的數目 (例如，從 16 個節點到 4 個節點)
ra3.4xlarge	4 倍	減少到四分之一的數目
ra3.xlplus	2 倍 (例如，從 4 個節點到 8 個節點)	減少到四分之一的數目
dc2.8xlarge	2 倍	減少到二分之一的數目 (例如，從 16 個節點到 8 個節點)
dc2.large	2 倍	減少到二分之一的數目

Note

在調整 RA3 叢集大小時選擇舊版節點類型 — 如果您嘗試從具有 RA3 節點的叢集調整為其他節點類型 (例如 DC2)，則主控台中會顯示驗證警告訊息，且調整大小作業將無法完成。發

生這種情況是因為系統不支援調整大小為舊版節點類型。這是為了防止客戶調整大小為已棄用或即將棄用的節點類型。這同時適用於彈性調整大小和傳統調整大小。

Elastic resize (傳統調整大小)

傳統調整大小會處理彈性調整大小不支援的叢集大小變更或節點類型變更的使用案例。當您執行傳統調整大小時，Amazon Redshift 會建立目標叢集，並將資料和中繼資料從來源叢集遷移到目標叢集。

以 RA3 為目標的傳統調整大小可以提供更好的可用性

當目標節點類型為 RA3 時，傳統調整大小已獲得增強。其會在來源叢集與目標叢集之間使用備份和還原操作來做到這一點。調整大小開始進行時，來源叢集會重新啟動，並有幾分鐘的時間無法使用。之後，叢集便可用於讀取和寫入操作，同時調整大小會在背景中繼續進行。

檢查叢集

為了確保您在執行目標為 RA3 叢集的傳統調整大小時能獲得最佳效能和結果，請完成這份檢查清單。如果您不遵循這份檢查清單，可能就無法獲得使用 RA3 節點進行傳統調整大小的一些好處，例如執行讀取和寫入操作的能力。

1. 資料的大小必須低於 2 PB。(PB 等於 1,000 TB)。若要驗證資料的大小，請建立快照並檢查其大小。您也可以執行以下查詢來檢查大小：

```
SELECT
sum(case when lower(diststyle) like ('%key%') then size else 0 end) distkey_blocks,
sum(size) as total_blocks,
((distkey_blocks/(total_blocks*1.00)))*100 as Blocks_need_redist
FROM svv_table_info;
```

只有超級使用者才能看到 `svv_table_info` 資料表。

2. 在啟動傳統調整大小之前，請確定您已建立不超過 10 小時的手動快照。如果沒有，請建立快照。
3. 用於執行傳統調整大小的快照不能用於還原資料表或其他目的。
4. 叢集必須在 VPC 中。

目標為 RA3 的傳統調整大小所產生的排序和分散操作

在為 RA3 進行傳統調整大小期間，具 KEY 分佈 (移轉為 EVEN 分佈) 的資料表會轉換回其原始的分佈樣式。這種情況的持續時間取決於資料大小以及叢集的忙碌程度。查詢工作負載的執行優先順序高過資

料遷移。如需詳細資訊，請參閱[分散樣式](#)。在此移轉過程中，對資料庫的讀取和寫入都會運作，但查詢可能需要更長的時間才能完成。不過，在這段期間，並行擴展可以透過為查詢工作負載新增資源來提升效能。您可以檢視來自 [SYS_RESTORE_STATE](#) 和 [SYS_RESTORE_LOG](#) 視觀表的結果，查看資料移轉的進度。後面有關於監控的詳細資訊。

叢集調整大小徹底完成後，會發生下列排序行為：

- 如果調整大小導致叢集有更多的配量，KEY 分佈資料表會變成部分未排序的狀態，但平均分散資料表會保持排序狀態。此外，在調整大小剛完成時，有關已排序資料數量的資訊可能不是最新的。在復原索引鍵後，自動清空功能會隨著時間的推移對資料表進行排序。
- 如果調整大小導致叢集有較少的配量，則 KEY 分佈資料表和平均分散資料表都會變成部分未排序的狀態。自動清空功能會隨著時間的推移對資料表進行排序。

如需自動清空資料的相關資訊，請參閱[清空資料表](#)。如需運算節點中配量的相關資訊，請參閱[資料倉儲系統架構](#)。

目標叢集為 RA3 時的傳統調整大小步驟

當目標叢集類型為 RA3 且您已符合上一節中詳述的先決條件時，傳統調整大小包含下列步驟。

1. 啟動從來源叢集到目標叢集的遷移。佈建新的目標叢集時，Amazon Redshift 會傳送調整大小已開始的事件通知。它會重新啟動您現有的叢集，而這會關閉所有連線。如果您現有的叢集是資料共用生產者叢集，則與取用者叢集的連線也會關閉。重新啟動會進行幾分鐘的時間。

請注意，在傳統調整大小進行期間，系統不會保留使用 BACKUP NO 所建立的任何資料庫關聯，例如資料表或具體化視觀表。如需詳細資訊，請參閱 [CREATE MATERIALIZED VIEW](#)。

2. 重新啟動之後，資料庫便可進行讀取和寫入。此外，資料共用也會繼續進行，這另外需要幾分鐘的時間來完成。
3. 資料會遷移至目標叢集。當目標節點類型為 RA3 時，系統可在資料遷移期間進行讀取和寫入。
4. 當調整大小程序接近完成時，Amazon Redshift 會更新目標叢集的端點，而且與來源叢集的所有連線都會中斷。目標叢集會成為資料共用的生產者。
5. 調整大小完成。Amazon Redshift 傳送事件通知。

您可以在 Amazon Redshift 主控台上檢視調整大小進度。調整叢集大小所需的時間取決於資料量。

Note

在調整 RA3 叢集大小時選擇舊版節點類型 — 如果您嘗試從具有 RA3 節點的叢集調整為其他節點類型 (例如 DC2)，則主控台中會顯示驗證警告訊息，且調整大小作業將無法完成。發生這種情況是因為系統不支援調整大小為舊版節點類型。這是為了防止客戶調整大小為已棄用或即將棄用的節點類型。這同時適用於彈性調整大小和傳統調整大小。

在目標叢集為 RA3 時監控傳統調整大小

若要監控正在進行傳統調整大小的佈建叢集 (包括 KEY 分佈)，請使用 [SYS_RESTORE_STATE](#)。其會顯示正在轉換的資料表的完成百分比。您必須是超級使用者才能存取該資料。

當您執行傳統調整大小時，請捨棄不需要的資料表。如果您這麼做，就可以更快速地分散現有資料表。

目標叢集不是 RA3 時的傳統調整大小步驟

例如，當目標節點類型是 RA3 以外的任何內容時，傳統調整大小由以下內容組成。

1. 啟動從來源叢集到目標叢集的遷移。佈建新的目標叢集時，Amazon Redshift 會傳送調整大小已開始的事件通知。它會重新啟動您現有的叢集，而這會關閉所有連線。如果您現有的叢集是資料共用生產者叢集，則與取用者叢集的連線也會關閉。重新啟動會進行幾分鐘的時間。

請注意，在傳統調整大小進行期間，系統不會保留使用 BACKUP NO 所建立的任何資料庫關聯，例如資料表或具體化視觀表。如需詳細資訊，請參閱 [CREATE MATERIALIZED VIEW](#)。

2. 重新啟動之後，資料庫會是唯讀狀態。資料共用會繼續進行，這另外需要幾分鐘的時間來完成。
3. 資料會遷移至目標叢集。資料庫會保持唯讀狀態。
4. 當調整大小程序接近完成時，Amazon Redshift 會更新目標叢集的端點，而且與來源叢集的所有連線都會中斷。目標叢集會成為資料共用的生產者。
5. 調整大小完成。Amazon Redshift 傳送事件通知。

您可以在 Amazon Redshift 主控台上檢視調整大小進度。調整叢集大小所需的時間取決於資料量。

Note

當目標叢集不是 RA3 時，或者其不符合上一節所述 RA3 目標叢集的先決條件時，可能需要數天甚至數週的時間，才能為包含大量資料的叢集調整大小。

另請注意，叢集所使用的儲存容量在進行傳統調整大小後可能會上升。當叢集因為傳統調整大小產生了額外的資料配量時，這是正常的系統行為。即使叢集中的節點數目保持不變，也可能會像這樣使用額外的容量。

彈性調整大小與傳統調整大小

下表會比較這兩種調整大小類型的行為。

彈性調整大小與傳統調整大小

Behavior (行為)	彈性調整大小	Elastic resize (傳統調整大小)	說明				
系統資料保留	彈性調整大小會保留系統日誌資料。	傳統調整大小不會保留系統資料表和資料。	如果您已在來源叢集中啟用稽核記錄，則可以在調整大小後繼續存取 Amazon S3 或 CloudWatch 的日誌。您可以依				

Behavior (行為)	彈性調整大小	Elastic resize (傳統調整大小)	說明				
			照資料政策所指定的，來保留或刪除這些日誌。				
變更節點類型	<p>當節點類型未變更時的彈性調整大小：就地調整大小，並保留大多數查詢。</p> <p>選取新節點類型時的彈性調整大小：建立新叢集。當調整大小程序完成時，查詢會遭到捨棄。</p>	傳統調整大小：建立新叢集。調整大小程序進行期間，查詢會遭到捨棄。					

Behavior (行為)	彈性調整大小	Elastic resize (傳統調整大小)	說明				
工作階段和查詢保留	當來源叢集和目標叢集中的節點類型相同時，彈性調整大小會保留工作階段和查詢。如果您選擇新的節點類型，查詢會遭到捨棄。	傳統調整大小不會保留工作階段和查詢。查詢會遭到捨棄。	當查詢遭到捨棄時，效能應該會降低。最好的辦法是在使用量不大時執行調整大小操作。				

Behavior (行為)	彈性調整大小	Elastic resize (傳統調整大小)	說明				
取消調整大小操作	您無法取消彈性調整大小。	您可以在 Amazon Redshift 主控台中，從叢集詳細資訊選擇取消調整大小，以在傳統調整大小操作完成前將其取消。	取消調整大小所需的時間量，取決於取消時調整大小操作的階段。如果您這麼做，則要等到取消操作完成後，叢集才可供使用。如果調整大小操				

Behavior (行為)	彈性調整大小	Elastic resize (傳統調整大小)	說明				
			<p>作處於最終階段，即無法取消。</p> <p>若為目標為 RA3 叢集的傳統調整大小，您無法加以取消。</p>				

排定調整大小

您可以為叢集排定調整大小操作，縱向擴展以應付預期的高使用量，或縮減規模以節省成本。排程同時適用於彈性調整大小和傳統調整大小。您可以在 Amazon Redshift 主控台上設定排程。如需詳細資訊，請參閱使用主控台管理叢集下的[調整叢集大小](#)。您也可以使用 AWS CLI 或 Amazon Redshift API 操作來安排調整大小。如需詳細資訊，請參閱 AWS CLI 命令參考中的[建立排程動作](#)或 Amazon Redshift API 參考中的[CreateScheduled動作](#)。

快照、還原和調整大小

[彈性調整大小](#)是調整 Amazon Redshift 叢集大小最快的方法。如果彈性調整大小不是您的其中一個選擇，並且您需要對叢集進行近乎不變的寫入存取，則可以使用下節所述的快照和還原操作搭配傳統調整大小。此方法需要在擷取快照之後寫入至來源叢集的任何資料必須在切換之後手動複製到目標叢集。根

據複製所需時間，您可能需要重複此動作數次，直到您在這兩個叢集中具有相同的資料。然後可以切換至目標叢集。此程序可能對現有查詢具有負面影響，直到可在目標叢集中提供完整資料集。但它的確會將您無法寫入至資料庫的時間量降至最低。

快照、還原和傳統調整大小方法使用下列程序：

1. 擷取現有叢集的快照。現有叢集是來源叢集。
2. 記下快照所花費的時間。這麼做表示稍後您可以識別將需要在哪個時間點重新執行擷取、交易和載入 (ETL) 程序，以將任何後置快照資料載入至目標資料庫。
3. 將快照還原至新叢集。這個新叢集是目標叢集。驗證目標叢集中有範例資料。
4. 調整目標叢集大小。為目標叢集選擇新的節點類型、節點數量和其他設定。
5. 檢閱在您擷取來源叢集快照之後發生之 ETL 程序中的載入。務必依照相同順序將相同資料重新載入至目標叢集。如果您有資料持續載入，請重複此程序數次，直到來源叢集和目標叢集中的資料相同。
6. 停止來源叢集上執行的所有佇列。若要這樣做，您可以重新啟動叢集，或以超級使用者身分登入，並使用 [PG_CANCEL_BACKEND](#) 和 [PG_TERMINATE_BACKEND](#) 命令。重新啟動叢集是確定叢集無法使用的最簡便方法。
7. 重新命名來源叢集。例如，將它從 `examplecluster` 重新命名為 `examplecluster-source`。
8. 重新命名目標叢集，以使用重新命名之前的來源叢集名稱。例如，將前述的目標叢集重新命名為 `examplecluster`。從此時起，使用包含 `examplecluster` 之端點的任何應用程式都會連接至目標叢集。
9. 在切換至目標叢集之後刪除來源叢集，並驗證所有程序都如預期般運作。

或者，您可以在將資料重新載入目標叢集之前重新命名來源和目標叢集。如果您不需要任何相依系統和報告立即與目標叢集的系統和報告一樣最新，則可採用此方法。在此情況下，步驟 6 將移至上述程序尾端。

只在您想要應用程式繼續使用相同端點連接至叢集時，才需要重新命名程序。如果不需要這樣做，則您可以改為更新任何連接至叢集的應用程式，以使用目標叢集的端點，而無需重新命名叢集。

重複使用叢集名稱有一些優勢。首先，您不需要更新應用程式連線字串，因為端點不會變更，即使基礎叢集變更也一樣。其次，相關項目，例如 Amazon CloudWatch 警報和亞馬遜簡單通知服務 (Amazon SNS) 通知與叢集名稱繫結。這個連結表示您可以繼續使用您為叢集設定的相同警示和通知。這種持續使用主要是生產環境中的疑慮，而您想要在這個環境中能夠靈活地調整群集模範，而無需重新配置相關項目，例如警示和通知。

暫停和繼續叢集

如果您有只需要在特定時間可用的叢集，則可以暫停叢集，稍後再繼續該叢集。叢集暫停時，隨需計費也會暫停。只有叢集的儲存才會產生費用。如需定價的相關資訊，請參閱 [Amazon Redshift 定價頁面](#)。

當您暫停叢集時，Amazon Redshift 會建立快照、開始終止查詢，並將叢集置於暫停狀態。如果您在未請求最終快照的情況下刪除暫停的叢集，則無法還原叢集。啟動暫停或繼續操作後，您無法取消或回復該操作。

您可以使用或使用亞馬遜紅移 API 操作，在亞馬遜紅移主控台上暫停和恢復叢集。AWS CLI

您可以排定暫停和繼續叢集的動作。當您使用新的 Amazon Redshift 主控台建立經常性排程以暫停和繼續時，系統會針對您選擇的日期範圍建立兩個排程動作。排程動作名稱的字尾為 `-pause` 和 `-resume`。名稱的總長度必須符合排程動作名稱的大小上限。

您無法暫停下列類型的叢集：

- EC2-Classic 叢集。
- 未作用中的叢集，例如目前正在修改的叢集。
- 硬體安全模組 (HSM) 叢集。
- 已關閉自動快照的叢集。

決定暫停叢集時，請考慮下列事項：

- 無法連線或查詢叢集。
- 您無法在 Amazon Redshift 主控台上查看暫停叢集的查詢監控資訊。
- 您無法修改暫停的叢集。叢集上的任何排程動作都不會執行。其中包括建立快照、調整叢集大小，以及叢集維護操作。
- 不會建立硬體指標。如果您 CloudWatch 已針對遺失的指標設定警示，請更新警示。
- 您無法將暫停叢集的最新自動快照複製到手動快照。
- 當叢集暫停時，它無法繼續，直到暫停操作完成為止。
- 當您暫停叢集時，計費即會暫停。不過，暫停操作通常會在 15 分鐘內完成，視叢集的大小而定。
- 稽核日誌會進行存檔，而且繼續時不會還原這些稽核日誌。
- 叢集暫停後，就可能沒有追蹤和日誌可供用於針對暫停之前所發生的問題進行故障診斷。

- 繼續時，叢集上的不備份資料表不會還原。如需不備份資料表的相關資訊，請參閱[在快照中排除資料表](#)。
- 如果您使用 AWS Secrets Manager 並暫停叢集來管理您的管理員認證，則不會刪除叢集的密碼，而且會繼續向您收取該密碼的費用。如需使用管理 Redshift 管理員密碼的詳細資訊 AWS Secrets Manager，請參閱[使用管理 Amazon Redshift 管理員密碼 AWS Secrets Manager](#)。

當您繼續叢集時，請考慮下列事項：

- 繼續叢集的叢集版本會根據叢集的維護時段更新為維護版本。
- 如果您刪除與暫停叢集相關聯的子網路，則可能會有不相容的網路。在此情況下，請從最新的快照還原叢集。
- 如果您在叢集暫停時刪除彈性 IP 地址，則會請求新的彈性 IP 地址。
- 如果 Amazon Redshift 無法使用先前的彈性網路界面繼續叢集，則 Amazon Redshift 嘗試配置新的叢集。
- 當您繼續叢集時，您的節點 IP 地址可能會變更。您可能需要更新 VPC 設定，以支援這些新的 IP 地址，適用於來自 Secure Shell (SSH) 的 COPY，或來自 Amazon EMR 的 COPY。
- 如果您嘗試繼續未暫停的叢集，則繼續操作會傳回錯誤。如果繼續操作是排程動作的一部分，請修改或刪除排程動作，以防止未來發生錯誤。
- 根據叢集的大小，可能需要幾分鐘的時間來繼續叢集，然後才能處理查詢。此外，在繼續完成之後，叢集重新化合時，查詢效能可能會有一段時間受到影響。

重新命名叢集

如果想讓叢集使用不同的名稱，您可重新命名叢集。由於叢集的端點包含叢集名稱 (亦稱為叢集識別碼)，因此重新命名後端點將使用新名稱。例如，如果您擁有名為 `examplecluster` 的叢集，並將其重新命名為 `newcluster`，端點會變更為使用 `newcluster` 識別碼。連線至該叢集的任何應用程式都應更新為新端點。

如果您想變更應用程式所連線到的叢集，卻不想變更應用程式中的端點，則可以重新命名叢集。但在此情況下，您必須先重新命名原始叢集，接著變更第二個叢集，以重新使用原始叢集在重新命名之前的名稱。這樣做有其必要性，因為叢集識別碼在帳戶和區域中必須是唯一的，原始叢集和第二個叢集不得使用相同的名稱。假如您要從快照還原叢集，且不想變更任何相依應用程式的連線屬性，或許可這樣做。

Note

如果要刪除原始叢集，您也必須負責刪除任何不想要的叢集快照。

重新命名叢集時，叢集狀態會變更為 `renaming`，直到流程結束。叢集所用的舊 DNS 名稱會立即刪除，但其會保留在快取內幾分鐘。重新命名的叢集的新 DNS 名稱會在大約 10 分鐘內生效。重新命名的叢集必須等到新名稱生效後才可使用。叢集將重新啟動，且任何與叢集的現有連線將會被捨棄。完成後，端點將變更為使用新名稱。因此，您應在開始重新命名之前停止執行查詢，並在重新命名完成後重新啟動查詢。

叢集快照將保留，且與叢集相關聯的所有快照在重新命名後仍會保持與該叢集的關聯。例如，假設您有一個為生產資料庫服務的叢集，且該叢集有多個快照。如果您命名叢集，接著在生產環境中將叢集換成快照，重新命名後的叢集仍有與其相關聯的現有快照。

Amazon CloudWatch 警示和亞馬遜簡單通知服務 (Amazon SNS) 事件通知與叢集名稱相關聯。如果您重新命名叢集，就必須進行對應的更新。您可以在 CloudWatch 主控台中更新 CloudWatch 警示，也可以在「事件」窗格的 Amazon Redshift 主控台中更新 Amazon SNS 事件通知。叢集的負載與查詢資料會繼續顯示重新命名之前和之後的資料。但重新命名流程結束後，效能資料將重設。

如需詳細資訊，請參閱 [修改叢集](#)。

關閉及刪除叢集

如果想讓叢集停止執行且不再產生費用，可關閉叢集。關閉叢集時，您可選擇性建立最後快照。若您建立最後快照，Amazon Redshift 會在叢集關閉前手動建立叢集的快照。如果想繼續執行叢集並查詢資料，您稍後可以還原快照。

如果您不再需要叢集和其資料，則不用建立最後快照，然後關閉叢集。在此情況下，叢集和資料將被永久刪除。如需關閉及刪除叢集的相關資訊，請參閱 [刪除叢集](#)。

無論關閉叢集時是否手動建立最後快照，所有與叢集相關聯的自動化快照都會在叢集關閉後被刪除。但與叢集相關聯的任何手動快照則會保留。如果您在關閉叢集時已無其他執行中的叢集，或如果您超過提供給執行中 Amazon Redshift 叢集的免費可用儲存空間，任何保留的手動快照 (包括選擇性的最後快照) 將依 Amazon Simple Storage Service 儲存費率計費。如需快照儲存費用的相關資訊，請參閱 [Amazon Redshift 定價頁面](#)。

刪除叢集也會刪除所有關聯的 AWS Secrets Manager 密碼。

重新定位叢集

透過在 Amazon Redshift 中使用重新定位功能，您可以讓 Amazon Redshift 將叢集移至另一個可用區域 (AZ)，而不會遺失任何資料或導致應用程式發生變更。透過重新定位，您可以在叢集上發生服務中斷時繼續操作，將所受影響降到最低。

開啟叢集重新定位時，Amazon Redshift 可能會在某些情況下選擇將叢集重新定位。特別是，當目前的可用區域中所發生的問題讓您無法達到最佳化的叢集操作，或是為了改善服務可用性，就會發生這種情況。如果指定可用區域中的資源限制會中斷叢集操作，您也可以叫用重新定位功能。其中一個範例是繼續執行叢集或調整叢集大小的能力。Amazon Redshift 提供重新定位功能，無需額外付費。

將 Amazon Redshift 叢集重新定位到新的可用區域時，新叢集的端點會與原始叢集的端點相同。您的應用程式可以重新連線到該端點並繼續操作，而不會修改或遺失資料。但是，由於指定可用區域中的資源可能有限制，因此不一定可以重新定位。

Amazon Redshift 叢集重新定位功能僅支援 RA3 執行個體類型，例如 ra3.16xlarge、ra3.4xlarge 和 ra3.xplus。RA3 執行個體類型會使用 Redshift 受管儲存 (RMS) 作為耐用儲存層。叢集資料的最新副本永遠可在區域中的其他可用區 AWS 域中使用。換句話說，您可以將 Amazon Redshift 叢集重新定位到另一個可用區域，而不會遺失任何資料。

當您開啟叢集的重新定位功能時，Amazon Redshift 會將您的叢集遷移到代理後面。這樣做有助於實作與位置無關的叢集運算資源存取權。遷移會導致叢集重新開機。將叢集重新定位到另一個可用區域時，當新叢集在新的可用區域中重新上線時，會發生中斷情形。不過，您不需要對應用程式進行任何變更，因為即使在叢集重新定位至新的可用區域後，叢集端點仍會維持不變。

所有 RA3 叢集都預設停用叢集重新定位功能。在建立佈建叢集時，Amazon Redshift 會指派 5439 作為預設連接埠。您可以變更為 5431 至 5455 或 8191 至 8215 之連接埠範圍內的其他連接埠。(請勿變更為範圍以外的連接埠。這會導致錯誤。) 若要變更已佈建叢集的預設連接埠，請使用 Amazon Redshift 主控 AWS CLI 台或 Amazon Redshift API。若要變更無伺服器工作群組的預設連接埠，請使用 AWS CLI 或 Amazon Redshift 無伺服器 API。

如果您開啟重新定位功能，而您目前使用領導節點 IP 地址來存取叢集，請務必變更該存取權。請改為使用與叢集的虛擬私有雲端 (VPC) 端點相關聯的 IP 地址。若要尋找此叢集的 IP 地址，請在叢集詳細資訊頁面的網路和安全區段中尋找並使用 VPC 端點。若要取得 VPC 端點的詳細資訊，請登入 Amazon VPC 主控台。

您也可以使用 AWS Command Line Interface (AWS CLI) 指令 `describe-vpc-endpoints` 取得與端點相關聯的 `elastic network interface`。您可以使用 `describe-network-interfaces` 命令來取得相關聯的 IP 地址。如需 Amazon Redshift 命 AWS CLI 令的詳細資訊，請參閱 AWS CLI 命令參考中的 [可用命令](#)。

Note

提醒您，叢集重新定位不是設定其他 Redshift 網路功能的先決條件。例如，您可以使用[跨區域快照複製](#)來補充，以便為您的環境提供更高的彈性，但這並非必要。您也不需要將其開啟才能啟用下列功能：

- 從跨帳戶或跨區域 VPC 連線至 Redshift — 您可以從一個 AWS 虛擬私人雲端 (VPC) 連線到包含 Redshift 資料庫的另一個虛擬私有雲端。這樣可以更輕鬆地管理，例如：從不同的帳戶或 VPC 進行用戶端存取，而不必提供本機 VPC 存取權限來連線至資料庫的身分識別。如需詳細資訊，請參閱[從其他帳戶或區域中的 Redshift VPC 端點連線至 Amazon Redshift Serverless](#)。
- 設定自訂網域名稱 — 您可以為 Amazon Redshift 叢集或 Amazon Redshift Serverless 工作群組建立自訂網域名稱 (也稱為自訂 URL)，以使端點名稱更加簡單易記。如需詳細資訊，請參閱[使用自訂網域名稱來進行用戶端連線](#)。

限制

使用 Amazon Redshift 重新定位功能時，請注意下列限制：

- 由於指定可用區域中的資源可能有限制，因此並非所有情況下都能進行叢集重新定位。如果發生這種情況，Amazon Redshift 不會變更原始叢集。
- 產品的 DC2 執行個體系列不支援重新定位。
- 您無法跨 AWS 區域執行重新定位。
- Amazon Redshift 重新定位預設使用連接埠號碼 5439。您也可以變更為 5431-5455 或 8191-8215 之連接埠範圍內的其他連接埠。

開啟叢集重新定位

您可以從亞馬遜紅移主控台和亞馬 Amazon Redshift API 開啟和管理叢集重新定位。AWS CLI

若要開啟叢集重新定位功能，請定義包含多個可用區域的子網路群組。如果 Amazon Redshift 識別出多個可存取的可用區域，Amazon Redshift 會自動從可存取的可用區域清單中進行選擇以重新定位叢集。

重新定位完成後，請使用相同端點來存取叢集。Amazon Redshift 會刪除原始叢集的運算資源，並將其歸還資源集區。

使用主控台管理重新定位

您可以使用 Amazon Redshift 主控台來管理叢集重新定位的設定。

建立新叢集時開啟重新定位

使用下列程序在建立新叢集時開啟重新定位功能。

開啟新叢集的重新定位功能

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽功能表上，選擇叢集。
3. 選擇建立叢集以建立新叢集。如需有關如何建立叢集的詳細資訊，請參閱 [Amazon Redshift 佈建的叢集](#)，其中包含 Amazon Redshift 入門指南。
4. 在備份下，對於叢集重新定位選擇已啟用。預設會關閉重新定位。
5. 選擇建立叢集。

修改現有叢集的重新定位

使用下列程序變更現有叢集的重新定位設定。

修改現有叢集的重新定位設定

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽選單上，選擇叢集。會列出目前 AWS 區域中您帳戶的叢集。每個叢集的屬性子集會在清單中分欄顯示。
3. 從清單中選擇您要修改之叢集的名稱。隨即會出現叢集詳細資訊頁面。
4. 選擇維護索引標籤，然後在備份詳細資訊區段中選擇編輯。
5. 在備份下，選擇已啟用。預設會關閉重新定位。
6. 選擇修改叢集。

重新定位叢集

使用下列程序將叢集手動重新定位到其他可用區域。當您要測試次要可用區域中的網路設定，或當您在目前的可用區域中即將遇到資源限制時，此功能特別有用。

將叢集重新定位到其他可用區域

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽選單上，選擇叢集。會列出目前 AWS 區域中您帳戶的叢集。每個叢集的屬性子集會在清單中分欄顯示。
3. 從清單中選擇您要移動之叢集的名稱。隨即會出現叢集詳細資訊頁面。
4. 針對動作，選擇重新定位。重新定位叢集頁面隨即出現。
5. (選擇性) 選擇可用區域。如果您未選擇可用區域，Amazon Redshift 會為您選擇。

Amazon Redshift 會啟動重新定位功能，並將叢集顯示為正在重新定位。重新定位完成後，叢集狀態會變更為「可用」。

使用 Amazon Redshift CLI 管理重新定位

您可以使用 AWS 命令列介面 (CLI) 管理叢集重新定位的設定。

使用 AWS CLI 時，下列範例命令會建立名為已開啟重新定位 **mycluster** 的 Amazon Redshift 叢集。

```
aws redshift create-cluster --cluster-identifier mycluster --number-of-nodes 2 --
master-username enter a username --master-user-password enter a password --node-type
ra3.4xlarge --port 5439 --availability-zone-relocation
```

如果您目前的叢集使用不同的連接埠，您必須先將其修改為使用 5431-5455 或 8191-8215 的連接埠範圍，然後再將其修改為開啟重新定位。預設值為 5439。下列範例命令會修改連接埠，以防您的叢集未使用指定範圍中的連接埠。

```
aws redshift modify-cluster --cluster-identifier mycluster --port 5439
```

下列範例命令包含 Amazon Redshift 叢集上的 `availability-zone-relocation` 參數。

```
aws redshift modify-cluster --cluster-identifier mycluster --availability-zone-
relocation
```

下列範例命令會關閉 Amazon Redshift 叢集上的 `availability-zone-relocation` 參數。

```
aws redshift modify-cluster --cluster-identifier mycluster --no-availability-zone-
relocation
```

下列範例命令會叫用 Amazon Redshift 叢集上的重新定位。

```
aws redshift modify-cluster --cluster-identifier mycluster --availability-zone us-east-1b
```

Amazon Redshift 快照和備份

主題

- [快照的概觀](#)
- [自動快照](#)
- [自動快照排程](#)
- [快照排程格式](#)
- [手動快照](#)
- [管理快照儲存](#)
- [從快照排除資料表](#)
- [將快照複製到另一個 AWS 區域](#)
- [從快照還原叢集](#)
- [從快照還原資料表](#)
- [共用快照](#)
- [使用主控台管理快照](#)
- [使用 AWS CLI 和 Amazon Redshift API 管理快照](#)
- [使用 AWS Backup](#)

快照的概觀

快照是叢集的 point-in-time 備份。有兩種類型的快照：自動和手動。Amazon Redshift 會透過使用加密的 Secure Sockets Layer (SSL) 連線，將這些快照儲存在 Amazon S3 內部。

Amazon Redshift 會自動取得增量快照，以追蹤自上一個自動快照以來對叢集的變更。自動快照會保留所有需要的資料以從快照還原叢集。您可以建立快照排程以控制何時進行自動快照，或隨時手動進行快照。

當您從快照進行還原時，Amazon Redshift 會建立一個新的叢集，並在所有資料載入之前讓新叢集可供使用，以便您立即查詢新叢集。叢集會隨需從快照中串流資料以回應活動查詢，然後在背景載入剩餘資料。

當您啟動叢集時，您可以為自動和手動快照設定保留期間。您可以經由修改叢集，以變更自動和手動快照的預設保留期間。您可以在建立快照時，或經由修改快照，以變更手動快照的保留期間。

[您可以檢視中的快照詳細資訊 AWS Management Console](#)，或在 CLI 中呼叫[描述叢集快照或快照 API 動作來監控快照的進度](#)。[DescribeCluster](#)有關正在進行的快照，這些資訊顯示了例如增量快照的大小、傳輸速率、經過時間和預估剩餘時間。

為了確保您的備份永遠可供叢集使用，Amazon Redshift 會將快照儲存在由 Amazon Redshift 管理的內部受管 Amazon S3 儲存貯體中。若要管理儲存費用，請評估您需要保留自動快照的天數，並相應地設定其保留期。刪除您不再需要的任何手動快照。如需備份儲存成本的相關資訊，請參閱 [Amazon Redshift 定價](#) 頁面。

在 Amazon Redshift 無伺服器中使用快照和備份

Amazon Redshift 無伺服器與佈建的叢集一樣，可讓您將備份作為命名空間中物件和資料的 point-in-time 表示形式。Amazon Redshift 無伺服器中有兩種備份類型：手動建立的快照和 Amazon Redshift 無伺服器自動建立的復原點。如需使用 Amazon Redshift 無伺服器快照的詳細資訊，請參閱 [使用快照和復原點](#)。

您也可以將快照從佈建的叢集還原至無伺服器命名空間。如需詳細資訊，請參閱 [從快照還原無伺服器命名空間](#)。

自動快照

當叢集的自動快照已啟用時，Amazon Redshift 將定期為該叢集建立快照。Amazon Redshift 預設約每 8 小時或每節點資料變更 5 GB 時拍攝一次，以先到者為準。如果您的資料大於 5 GB * 節點數，則兩次自動建立快照之間的最短間隔時間為 15 分鐘。或者，您可以建立快照排程以控制何時進行自動快照。如果您使用自訂排程，則兩次自動快照之間的最短間隔時間為一小時。依據預設，當您建立叢集時，將會啟用自動快照。

在保留期間結束後，自動快照將永久刪除。預設保留期間為一日，但您可以使用 Amazon Redshift 主控台或使用 Amazon Redshift API 或 CLI 以程式設計方式進行修改。

若要停用自動快照，請將保留期間設定為 zero (零)。若您停用了自動快照，Amazon Redshift 將停止拍攝快照並刪除叢集的任何現有自動快照。您無法停用 RA3 節點類型的自動快照。您可以設定 1 到 35 天的 RA3 節點類型自動保留期。

只有 Amazon Redshift 可以刪除自動快照；您無法手動刪除自動快照。在自動快照的保留期結束時、停用叢集的自動快照時，或當您刪除叢集時，Amazon Redshift 會刪除自動快照。[Amazon Redshift 會保留最新的自動快照，直到您停用自動快照或刪除叢集為止。](#)

如果想要讓自動快照保留期間更長，請建立該快照複本以做為手動快照。自動快照會保留到保留期間結束為止，但對應的手動快照會保留到您手動刪除它為止，或直到保留期間結束為止。

自動快照排程

若要精確控制何時進行快照，您可以建立快照排程，並將它連接至一或多個叢集。當您修改快照排程時，所有相關聯叢集的排程都會修改。如果叢集沒有連接快照排程，將會使用預設的自動快照排程。

快照排程是一組排程規則。您可以指定時間間隔來定義簡單的排程規則，例如每 8 小時或每 12 小時。您也可以新增規則，在特定的週中的日、指定的時間或特定期間進行快照。您也可以使用類似 Unix 的 cron 運算式來定義規則。

快照排程格式

您可以在 Amazon Redshift 主控台建立快照排程。然後，您可以將排程連接至叢集以觸發系統快照的建立。一個排程可連接至多個叢集，而且您可以在一個排程中建立多個 cron 定義來觸發快照。

您可以使用 cron 語法為您的快照定義排程。這些排程的定義使用經過修改且類似 Unix 的 [cron](#) 語法。您以[國際標準時間 \(UTC\)](#) 指定時間。您可以用最大頻率 1 小時以及最小單位 1 分鐘來建立排程。

Amazon Redshift 修改的 cron 運算式有 3 個必要欄位，並且會以空格隔開。

語法

```
cron(Minutes Hours Day-of-month Month Day-of-week Year)
```

欄位	Values (數值)	萬用字元
分鐘	0-59	, - * /
小時	0-23	, - * /
月中的日	1-31	, - * ? / L W
月	1-12 或 JAN-DEC	, - * /
週中的日	1-7 或 SUN-SAT	, - * ? L #
年	1970-2199	, - * /

萬用字元

- , (逗號) 萬用字元包含額外的值。在 Day-of-week 欄位，MON, WED, FRI 包括週一、週二和週三。每個欄位的總數值限制為 24。
- - (破折號) 萬用字元用於指定範圍。在 Hour 欄位中，1-15 會包含指定日的 1 至 15 時。
- * (星號) 包含欄位中所有的值。在 Hours 欄位，* 包含每個小時。
- / (斜線) 萬用字元用於指定增量。在 Hours 欄位，您可以輸入 **1/10** 指定每第 10 小時，從一天的第一小時開始 (例如 01:00、11:00 和 21:00)。
- ? (問號) 萬用字元用於表示不限定任何一個。在該 Day-of-month 字段中，您可以輸入 7，如果您不在乎第七週的哪一天，您可以輸入 ? 在 Day-of-week 欄位中。
- L 萬用字元在 Day-of-month 或 Day-of-week 欄位可指定月份或週的最後一天。
- W 萬用字元在 Day-of-month 欄位可指定任務日。在 Day-of-month 欄位，3W 指定的是月份中最接近第三個任務日的日子。
- Day-of-week 欄位中的 # 萬用字元會指定一個月內星期中指定日期的特定執行個體。例如，3#2 代表則該月的第二個星期二：3 是指星期二，因為它是每週的第三天，2 指的是一個月內該類型的第二天。

Note

如果您使用 '#' 字元，則只能在 day-of-week 欄位中定義一個運算式。例如："3#1,6#3" 是無效的，因為它被轉譯為兩個表達式。

限制

- 您無法在同一個 cron 表達式中指定 Day-of-month 和 Day-of-week 欄位。如果您在其中一個欄位指定了數值，就必須在另一個欄位中使用 ? (問號)。
- 快照排程不支援下列頻率：
 - 快照排程頻率超過每小時 1 次。
 - 快照排程頻率低於每天 (24 小時) 1 次。

如果您有重疊的排程，導致 1 個小時內有多個排程快照，將會產生驗證錯誤。

建立排程時，您可以使用下列 cron 字串範例。

分鐘	小時	週中的日	意義
0	14-20/1	TUE	週二下午 2 點至 8 點，每小時一次。
0	21	MON-FRI	週一至週五每天晚上 9 點。
30	0/6	SAT-SUN	週六和週日每 6 小時增量，從當日午夜後 30 分鐘開始 (00:30)。結果是在每天 [00:30、06:30、12:30 和 18:30] 進行快照。
30	12/4	*	每天 12:30 開始每 4 小時增量。這解析為 [12:30、16:30、20:30]。

舉例來說，如果要執行排程，在每天的 15:15 開始每 2 小時增量。這解析為 [15:15、17:15、19:15、21:15、23:15]，指定：

```
cron(15 15/2 *)
```

您可以在排程中建立多個 cron 排程定義。例如，下列 AWS CLI 指令在一個排程中包含兩個 cron 排程。

```
create-snapshot-schedule --schedule-identifier "my-test" --schedule-definition "cron(0 17 SAT,SUN)" "cron(0 9,17 MON-FRI)"
```

手動快照

您可以隨時建立手動快照。在預設情況下，即使刪除叢集，手動快照也會無限期地保留。您可以在建立手動快照時指定保留期間，或經由修改快照以變更保留期間。如需變更保留期的相關資訊，請參閱[變更手動快照保留期間](#)。

若刪除快照，您便無法開始任何參考該快照的新操作。不過，若一個還原操作正在處理中，該還原操作將會繼續執行至完成為止。

Amazon Redshift 的配額限制了您可以建立的手動快照總數；此配額是每個 AWS 區域的每個 AWS 帳戶。[Amazon Redshift 中的配額和限制](#)中會列出預設配額。

管理快照儲存

由於快照會產生儲存費用，當您不再需要快照時，務必刪除它們。Amazon Redshift 會在各自的快照保留期結束時刪除自動和手動快照。您也可以使用 AWS Management Console 或搭配[批次](#)刪除叢集-快照 CLI 指令來刪除手動快照。

您可以修改手動快照設定，以變更手動快照的保留期間。

您可以使用 Amazon Redshift 主控台或使用 [describe-storage](#) CLI 命令，以取得您的快照耗用多少儲存的相關資訊。

從快照排除資料表

依預設，所有使用者定義的永久資料表都包含在快照中。如果不需要備份資料表 (例如臨時資料表)，則可以大幅減少建立快照和從快照還原所需的時間。您也可以使用不備份資料表以在 Amazon S3 上減少儲存空間。若要建立不備份資料表，請在建立資料表時使用 BACKUP NO 參數。如需詳細資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的 [CREATE TABLE](#) 和 [CREATE TABLE AS](#)。

將快照複製到另一個 AWS 區域

您可以將 Amazon Redshift 設定為自動將叢集的快照 (自動或手動) 複製到其他 AWS 區域。在叢集的主要 AWS 區域中建立快照時，會將其複製到次要 AWS 區域。這兩個 AWS 區域分別稱為來源 AWS 區域和目的地 AWS 區域。如果您將快照副本儲存在另一個 AWS 區域，則可以在任何影響主要 AWS 區域的情況下，從最近的資料還原叢集。您可以將叢集設定為一次只將快照複製到一個目的地 AWS 區域。如需 Amazon Redshift 區域的清單，請參閱《Amazon Web Services 一般參考》中的[區域與端點](#)。

當您啟用 Amazon Redshift 自動將快照複製到其他 AWS 區域時，您可以指定要將快照複製到的目的地 AWS 區域。對於自動化快照，您也可以指定將快照保留在目的地 AWS 區域中的保留期間。將自動快

照複製到目的地 AWS 區域並達到該區域的保留期間之後，就會從目的地 AWS 區域刪除該快照。執行此動作讓您的快照保持低使用率。若要在目的地區域中保留自動快照的時間較短或更長時 AWS 間，請變更此保留期間。

您為複製到目的地區域的自動快照所設定的保留期間，與來源 AWS 區域中自動快照的保留期間不同。預設快照複本的保留期間為 7 天。該 7 日的保留期間僅適用於自動快照。在來源和目的地 AWS 區域中，手動快照會在快照保留期間結束時刪除，或您手動將它們刪除。

您可隨時停用叢集的自動快照複製。停用此功能時，快照不會再從來源 AWS 區域複製到目的地 AWS 區域。除非您建立手動快照複本，否則複製到目的地 AWS 區域的任何自動快照都會在達到保留期限時予以刪除。這些手動快照以及從目的地 AWS 區域複製的任何手動快照都會保留在目的地 AWS 區域中，直到您手動刪除它們為止。

若要變更將快照複製到的目標 AWS 區域，請先停用自動複製功能。然後，重新啟用它，同時指定新的目的地 AWS 區域。

將快照複製到目的地 AWS 區域後，它會變為作用中並可用於還原目的。

若要將 AWS KMS 已加密叢集的快照複製到另一個 AWS 區域，請為 Amazon Redshift 建立授權，以便在目的地區域使用客戶受管金鑰。然後在來源 AWS 區域中啟用複製快照時，選擇該授權。如需設定跨區域快照複本授權的相關資訊，請參閱 [複製 AWS KMS— 加密的快照到另一個 AWS 區域](#)。

從快照還原叢集

快照包含的資料來自正在您叢集上執行的任何資料庫。它也包含叢集的相關資訊，包括節點數、節點類型及管理員使用者名稱。如果您從快照還原叢集，則 Amazon Redshift 會使用叢集資訊來建立新的叢集。然後，它會從快照資料還原所有資料庫。

若為從原始快照建立的新叢集，您可以選擇組態，例如節點類型及節點數。除非您在請求中指定另一個可用區域，否則該叢集將在同一個 AWS 區域和系統隨機選擇的可用區域中還原。從快照還原叢集時，您可以選擇性地為新叢集選擇相容的維護軌道。

Note

搭配不同組態將快照還原至叢集時，必須已在版本為 1.0.10013 或更新版本的叢集上取得快照。

當還原正在進行時，系統通常會以下列順序發出事件：

1. 還原程序開始時，會傳送 RESTORE_STARTED – REDSHIFT-EVENT-2008。

2. 建立了新叢集時，會傳送 `RESTORE_SUCCEEDED – REDSHIFT-EVENT-3003`。

叢集可供查詢使用。

3. 當資料傳輸完成時，會傳送 `DATA_TRANSFER_COMPLETED – REDSHIFT-EVENT-3537`。

Note

RA3 叢集只會發出 `RESTORE_STARTED` 和 `RESTORE_SUCCEEDED` 事件。`RESTORE` 成功後不需要進行明確的資料傳輸，因為 RA3 節點類型會將資料儲存在 Amazon Redshift 受管儲存中。使用 RA3 節點時，資料會在一般查詢的處理過程中，於 RA3 節點和 Amazon Redshift 受管儲存之間持續傳輸。RA3 節點會在本機快取熱資料，並在 Amazon Redshift 受管儲存中自動保留較不常查詢的區塊。

您可以透過呼叫 [DescribeClusters](#) API 作業或檢視中的叢集詳細資料來監視還原進度 AWS Management Console。有關正在進行的還原，這些資訊顯示了例如快照資料的大小、傳輸速率、經過時間和預估剩餘時間。如需這些測量結果的說明，請參閱 [RestoreStatus](#)。

您不得使用快照將作用中的叢集還原至上一個狀態。

Note

當您還原快照至新叢集時，除非您指定了不同的值，否則將會使用預設安全群組與參數群組。

基於下列原因，您可能想要搭配不同組態將快照還原至叢集：

- 當叢集是由更小的節點類型組成，而且您想要將其合併成更大的節點類型，而節點更少時。
- 當您已監控工作負載並判定需要移至 CPU 及儲存空間更多的節點類型時。
- 當您想要利用不同節點類型來測量測試工作負載的效能時。

「還原」有下列限制：

- 新節點組態必須具有足夠儲存體可放置現有資料。即使在新增節點時，您的新組態可能因為資料的重新配送方式而沒有足夠儲存體。
- 還原操作會檢查快照是否建立在與新叢集的叢集版本相容的叢集版本上。如果新叢集的版本層級太早，則還原操作會失敗，並且會在錯誤訊息中報告詳細資訊。

- 您可以還原的可能組態 (節點數目和節點類型) 取決於原始叢集中的節點數目，以及新叢集的目標節點類型。若要判斷可用的組態，您可以使用 Amazon Redshift 主控台或搭 `action-type restore-cluster` 配使用 `describe-node-configuration-options` AWS CLI 命令。如需使用 Amazon Redshift 主控台還原的相關資訊，請參閱 [從快照還原叢集](#)。

下列步驟會使用 AWS CLI 取得具有許多節點的叢集，並將其合併為更大的節點類型，而節點數更小。在此範例中，我們從 24 個節點構成的來源叢集開始。在此情況下，假設我們已建立此叢集的快照，而且想要將其還原至更大的節點類型。

1. 執行下列命令來取得我們 24 節點 叢集的詳細資訊。

```
aws redshift describe-clusters --region eu-west-1 --cluster-identifier
mycluster-123456789012
```

2. 執行下列命令來取得快照的詳細資訊。

```
aws redshift describe-cluster-snapshots --region eu-west-1 --snapshot-identifier
mycluster-snapshot
```

3. 執行下列命令來描述可供此快照使用的選項。

```
aws redshift describe-node-configuration-options --snapshot-identifier mycluster-
snapshot --region eu-west-1 --action-type restore-cluster
```

此命令會傳回一個具有所建議節點類型的選項清單、節點數，以及每個選項的磁碟使用率。在此範例中，上述命令列出下列可能的節點組態。我們選擇還原至三節點 叢集。

```
{
  "NodeConfigurationOptionList": [
    {
      "EstimatedDiskUtilizationPercent": 65.26134808858235,
      "NodeType": "dc2.large",
      "NumberOfNodes": 24
    },
    {
      "EstimatedDiskUtilizationPercent": 32.630674044291176,
      "NodeType": "dc2.large",
      "NumberOfNodes": 48
    }
  ]
}
```

```

    "EstimatedDiskUtilizationPercent": 65.26134808858235,
    "NodeType": "dc2.8xlarge",
    "NumberOfNodes": 3
  },
  {
    "EstimatedDiskUtilizationPercent": 48.94601106643677,
    "NodeType": "dc2.8xlarge",
    "NumberOfNodes": 4
  },
  {
    "EstimatedDiskUtilizationPercent": 39.156808853149414,
    "NodeType": "dc2.8xlarge",
    "NumberOfNodes": 5
  },
  {
    "EstimatedDiskUtilizationPercent": 32.630674044291176,
    "NodeType": "dc2.8xlarge",
    "NumberOfNodes": 6
  }
]
}

```

- 執行下列命令，將快照還原至我們選擇的叢集組態。在還原叢集之後，我們具有與來源叢集相同的內容，但資料已合併為三個 dc2.8xlarge 節點。

```

aws redshift restore-from-cluster-snapshot --region eu-west-1 --snapshot-identifier
mycluster-snapshot --cluster-identifier mycluster-123456789012-x --node-type
dc2.8xlarge --number-of-nodes 3

```

如果您有預留節點 (例如 DC2 保留節點)，則可以升級至 RA3 保留節點。您可以在從快照還原時或在執行彈性調整大小時進行此升級。您可以使用主控台來引導您完成此程序。如需升級至 RA3 節點的相關資訊，請參閱[升級至 RA3 節點類型](#)。

從快照還原資料表

您可以從快照來還原單一資料表，而無須還原整個叢集。當您自快照還原單一資料表時，您將指定來源快照、資料庫、結構描述與資料表名稱，以及還原的資料表目標資料庫、結構描述和新名稱。

新資料表名稱不能與現有資料表名稱重複。若您要將從快照還原的資料表取代現有資料表，請在從快照還原之前先重新命名或刪除現有資料表。

已使用資料表的欄位定義、資料表屬性和欄位屬性 (外部索引鍵除外) 建立目標資料表。為避免因相依性而導致的衝突，目標資料表不會從來源資料表繼承外部索引鍵。任何相依性，例如檢視或來源資料表上授予的許可，都不會套用至目標資料表。

若來源資料表存在擁有者，則該資料庫使用者是已還原資料表的擁有者，前提是該使用者有足夠的許可可以成為指定資料庫和結構描述中關係的擁有者。否則，還原的資料表將由啟動叢集時建立的管理員使用者所擁有。

還原的資料表會恢復到備份時所處的狀態。這包括由 Amazon Redshift 符合 [可序列化的隔離](#) 所定義的交易可見度規則，這表示在備份後開始傳送的交易中立刻可看見該資料。

以下為從快照還原資料表的限制：

- 您只能將資料表還原至目前、活動執行中的叢集；以及從該叢集拍攝的快照中還原資料表。
- 您一次只能還原一個資料表。
- 您無法從叢集調整大小前拍攝的叢集快照還原資料表。例外情況是，如果節點類型沒有變更，您可以在彈性調整大小之後還原資料表。
- 任何相依性，例如檢視或來源資料表上授予的許可，都不會套用至目標資料表。
- 如果為要還原的資料表開啟了資料列層級安全，Amazon Redshift 會在開啟資料列層級安全的情況下還原資料表。

從快照還原資料表

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽功能表上，選擇叢集，然後選擇用以還原資料表的叢集。
3. 針對 Actions (動作)，選擇 Restore table (還原資料表) 以顯示 Restore table (還原資料表) 頁面。
4. 輸入要使用的快照、來源資料表和目標資料表資訊，然後選擇 Restore table (還原資料表)。

Example 範例：使用 AWS CLI

下列範例會使用 `restore-table-from-cluster-snapshot` AWS CLI 命令，從中的 `sample-database` 結構描述還原資料 `my-source-table` 表 `my-snapshot-id`。您可以使用 AWS CLI 指令 `describe-table-restore-status` 來檢閱還原作業的狀態。此範例透過名為 `mycluster-example` 的新資料表還原快照至 `my-new-table` 叢集。

```
aws redshift restore-table-from-cluster-snapshot --cluster-identifier mycluster-
example
--new-table-name my-new-table
--snapshot-identifier my-snapshot-id
--source-database-name sample-
database
--source-table-name my-source-table
```

共用快照

您可以授權存取快照，與其他 AWS 客戶帳戶共用現有的手動快照。每個快照最多可授權 20 個，每個 AWS Key Management Service (AWS KMS) 金鑰最多可授權 100 個。也就是說，如果您有 10 個使用單一 KMS 金鑰加密的快照，則您可以授權 10 個 AWS 帳戶還原每個快照，或是其他組合 (最多可加入 100 個帳戶且每個快照的帳戶不超過 20 個帳戶)。在其中一個已授權帳戶登入為使用者的人員，接下來可以描述快照或將其還原，以在其帳戶下建立新的 Amazon Redshift 叢集。例如，如果您使用不同的 AWS 客戶帳戶進行生產和測試，則使用者可以使用生產帳戶登入，並與測試帳戶中的使用者共用快照。某人若以測試帳戶使用者身分登入，他接下來可以還原快照以建立由測試帳戶所擁有的新叢集，以進行測試或診斷工作。

建立手動快照的 AWS 客戶帳戶永久擁有。僅有在帳戶中擁有快照的使用者，方可授權或撤銷其他帳戶存取該快照。在已授權帳戶中的使用者僅可描述或還原任何與他們分享的快照；他們不得複製或刪除與他們分享的快照。授權將持續生效，除非快照擁有者撤銷之。若授權被撤銷，之前授權的使用者將無法看見該快照，也不能啟動任何參考該快照的新動作。若存取權被撤銷時帳戶正在還原該快照，則該還原會持續進執行至完成。您不得刪除有主動授權的快照；您必須先撤銷所有的授權。

AWS 客戶帳戶一律獲得授權，可存取該帳戶擁有的快照。試圖授權或撤銷擁有者帳戶的存取權將會收到錯誤。您無法還原或描述非作用中 AWS 客戶帳戶所擁有的快照。

授權存取客戶帳戶後，該帳 AWS 戶中的任何使用者都無法對快照執行任何動作，除非他們擔任具有允許他們執行此動作的原則的角色。

- 只有當快照擁有者帳戶中的使用者所擔任的角色有 IAM 政策允許他們執行使用包含快照的資源規格動作，他們才可授權或撤銷快照的存取權。例如，以下策略允許 AWS 帳戶 012345678912 中的使用者或角色授權其他帳戶存取名為的快照 my-snapshot20130829：

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



```

    "Effect": "Allow",
    "Action": [
        "redshift:AuthorizeSnapshotAccess",
        "redshift:RevokeSnapshotAccess"
    ],
    "Resource": [
        "arn:aws:redshift:us-east-1:012345678912:snapshot:*/my-snapshot20130829"
    ]
  }
]
}

```

- 已共用快照的 AWS 帳戶中的使用者無法對該快照執行動作，除非他們具有允許這些動作的權限。您可以透過將政策指派給某個角色並擔任該角色來執行此操作。
- 列出或描述快照；他們必須擁有允許 DescribeClusterSnapshots 動作的 IAM 政策。下列代碼顯示了範例：

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "redshift:DescribeClusterSnapshots"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}

```

- 若要還原快照，使用者所擔任的角色必須擁有允許 RestoreFromClusterSnapshot 動作的 IAM 政策，並擁有涵蓋嘗試建立的叢集與快照的資源元素。例如，若帳戶 012345678912 中的使用者已經與帳戶 my-snapshot20130829 分享快照 219876543210，以透過還原快照來建立叢集，則帳戶 219876543210 中的使用者所擔任的角色必須擁有的政策如下所示：

```

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

```

```
"Action":[
  "redshift:RestoreFromClusterSnapshot"
],
"Resource":[
  "arn:aws:redshift:us-east-1:012345678912:snapshot:*/my-
snapshot20130829",
  "arn:aws:redshift:us-east-1:219876543210:cluster:from-another-account"
]
}
]
}
```

- 從帳戶撤銷對快照的存取權後，該 AWS 帳戶中的任何使用者都無法存取快照。即使這些帳戶有 IAM 政策允許對之前共用的快照資源執行動作也一樣。

使用主控台管理快照

Amazon Redshift 會定期對資料建立自動增量快照，並將快照儲存至 Amazon S3。此外，您隨時都可以手動建立資料快照。本節說明如何從 Amazon Redshift 主控台管理快照。如需快照的相關資訊，請參閱 [Amazon Redshift 快照和備份](#)。

Amazon Redshift 主控台所有的快照作業都從快照清單中啟動。您可使用時間範圍、快照類型，以及與快照相關聯的叢集來篩選快照清單。此外，您可以依日期、大小和快照類型排序清單。快照上可用的選項各不相同，視所選的快照類型而定。

主題

- [建立快照排程](#)
- [建立手動快照](#)
- [變更手動快照保留期間](#)
- [刪除手動快照](#)
- [複製自動化快照](#)
- [從快照還原叢集](#)
- [從快照還原無伺服器命名空間](#)
- [共用叢集快照](#)
- [設定未加密叢集的跨區域快照複本](#)
- [為已 AWS KMS加密的叢集設定跨區域快照副本](#)
- [修改跨區域快照複本的保留期間](#)

建立快照排程

若要精確控制何時進行快照，您可以建立快照排程，並將它連接至一或多個叢集。您可以在建立叢集時附加排程，或修改叢集來附加排程。如需詳細資訊，請參閱 [自動快照排程](#)。

建立快照排程

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽功能表中，選擇叢集、快照，然後選擇快照排程索引標籤。快照排程即會出現。
3. 選擇 Add schedule (新增排程) 以顯示新增排程的頁面。
4. 輸入排程定義的屬性，然後選擇 Add schedule (新增排程)。
5. 在出現的頁面中，您可將叢集連接至新的快照排程，然後選擇 OK (確定)。

建立手動快照

您可從快照清單手動建立叢集的快照，方式如下。或者，您也可從叢集組態窗格建立叢集快照。如需詳細資訊，請參閱 [建立叢集快照](#)。

建立手動快照

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽功能表中，選擇叢集、快照，然後選擇建立快照。建立手動快照的快照頁面即會出現。
3. 輸入快照定義屬性，然後選擇建立快照。可能要等一會兒才能使用此快照。

變更手動快照保留期間

您可變更手動快照的保留期間，只要修改快照設定即可。

變更手動快照保留期間

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽功能表中，選擇叢集、快照，然後選擇要變更的手動快照。
3. 針對 Actions (動作)，選擇 Manual snapshot settings (手動快照設定) 以顯示手動快照的屬性。
4. 輸入快照定義的修訂屬性，然後選擇 Save (儲存)。

刪除手動快照

您可以透過選取快照清單中的一或多個快照來刪除手動快照。

刪除手動快照

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽功能表中，選擇叢集、快照，然後選擇要刪除的快照。
3. 針對 Actions (動作)，選擇 Delete snapshot (刪除快照) 以刪除快照。
4. 確認刪除列出的快照，然後選擇 Delete (刪除)。

複製自動化快照

當快照的保留期間結束，當您停用自動快照，或當您刪除叢集時，系統會自動刪除自動快照。如果想要保留自動快照，可將其複製到手動快照。

複製自動快照

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽功能表上，選擇叢集、快照，然後選擇要複製的快照。
3. 針對 Actions (動作)，選擇 Copy automated snapshot (複製自動快照) 以複製快照。
4. 更新新快照的屬性，然後選擇 Copy (複製)。

從快照還原叢集

當您從快照還原叢集時，Amazon Redshift 會建立新的叢集，並將所有快照資料匯入新叢集。

從快照還原叢集

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽功能表中，選擇叢集、快照，然後選擇要還原的快照。
3. 選擇 Restore from snapshot (從快照還原) 以檢視要使用快照資訊建立之新叢集的 Cluster configuration (叢集組態) 和 Cluster details (叢集詳細資訊) 值。
4. 更新新叢集的屬性，然後選擇 Restore cluster from snapshot (從快照還原叢集)。

如果 AWS Secrets Manager 不管理叢集的管理員密碼，您可以在 AWS Secrets Manager [叢集配置] 區段中選擇 [管理管理認證]，並指定 KSM 金鑰，讓叢集管理還原的叢集。否則，叢集會使用建立快照時擁有的管理員憑證來還原叢集。您可以在還原叢集之後，在叢集詳細資訊頁面中更新叢集的管理員憑證。

如果在擷取螢幕擷取畫面時 AWS Secrets Manager 管理叢集的管理員密碼，您必須繼續使用 AWS Secrets Manager 來管理管理員密碼。您可以在還原叢集之後，透過在叢集詳細資訊頁面中更新叢集的管理員憑證，以選擇不使用機密。

如果您有預留節點 (例如 DC2 保留節點)，則可以升級至 RA3 保留節點。您可以在從快照還原時或在執行彈性調整大小時進行此升級。您可以使用主控台來引導您完成此程序。如需升級至 RA3 節點的相關資訊，請參閱[升級至 RA3 節點類型](#)。

從快照還原無伺服器命名空間

從快照還原無伺服器命名空間會將所有命名空間的資料庫替換為快照中的資料庫。如需無伺服器快照的相關資訊，請參閱[使用快照和復原點](#)。當您將佈建的叢集快照還原到 Amazon Redshift 無伺服器命名空間時，Amazon Redshift 會自動將包含交錯金鑰的表格轉換為複合金鑰。如需排序索引鍵的相關資訊，請參閱[使用排序索引鍵](#)。

若要將佈建叢集的快照還原至無伺服器命名空間。

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽功能表中，選擇叢集、快照，然後選擇要使用的快照。
3. 選擇從快照還原、還原至無伺服器命名空間。
4. 選擇想要還原至的命名空間。
5. 確認您要從快照還原。選擇還原。此動作會使用佈建叢集中的資料取代無伺服器命名空間中的所有資料庫。

共用叢集快照

您可授權其他使用者存取您所擁有的手動快照，之後不需要時也可撤銷存取權。

與其他帳戶共用快照

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。

2. 在導覽功能表上，選擇叢集、快照，然後選擇要共用的手動快照。
3. 針對 Actions (動作)，選擇 Manual snapshot settings (手動快照設定) 以顯示手動快照的屬性。
4. 在 Manage access (管理存取) 區段輸入要共用的一或多個帳戶，然後選擇 Save (儲存)。

共用加密快照時的安全考量

當您提供加密快照的存取權時，Redshift 要求用於建立快照的 AWS KMS 客戶受管金鑰與執行還原的帳戶共用。如果金鑰未共用，嘗試還原快照會導致存取遭拒錯誤。接收帳戶不需要任何額外權限即可還原共用快照。當您授權快照存取權並共用金鑰時，授權存取權的身分必須具有用來加密快照之金鑰的 `kms:DescribeKey` 許可。[AWS KMS 權限](#) 中有此許可的更詳細描述。如需詳細資訊，請參閱 Amazon Redshift API 參考文件 [DescribeKey](#) 中的。

客戶受管金鑰政策可透過程式設計方式或在 AWS Key Management Service 主控台中更新。

允許存取加密快照的 AWS KMS 金鑰

若要共用加密快照的 AWS KMS 客戶受管金鑰，請執行下列步驟來更新金鑰原則：

1. 使用您要共用的 AWS 帳戶的 Amazon 資源名稱 (ARN) 更新 KMS 金鑰政策，如 Principal 同 KMS 金鑰政策一樣。
2. 允許 `kms:Decrypt` 動作。

在以下金鑰政策範例中，使用者 111122223333 是 KMS 金鑰的擁有者，使用者 444455556666 是與其共用該金鑰的帳戶。此金鑰原則可讓 AWS 帳戶存取範例 KMS 金鑰，方法是包含使用者根 AWS 帳號識別的 ARN 444455556666 做 Principal 為原則，並允許 `kms:Decrypt` 動作。

```
{
  "Id": "key-policy-1",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow use of the key",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::111122223333:user/KeyUser",
          "arn:aws:iam::444455556666:root"
        ]
      }
    }
  ],
}
```

```
        "Action": [  
            "kms:Decrypt"  
        ],  
        "Resource": "*" ]  
    }  
}
```

將存取權授與客戶受管 KMS 金鑰後，還原加密快照的帳戶必須建立 AWS Identity and Access Management (IAM) 角色或使用者 (如果尚未有) 角色。此外，該 AWS 帳戶還必須將 IAM 政策附加到該 IAM 角色或使用者，以允許他們使用您的 KMS 金鑰還原加密的資料庫快照。

如需有關授予金 AWS KMS 鑰存取權的詳細資訊，請參閱 [AWS Key Management Service 開發人員指南](#) 中的 [允許其他帳戶中的使用者使用 KMS 金鑰](#)。

如需關鍵政策的概觀，請參閱 [Amazon Redshift 如何使用 AWS KMS](#)。

設定未加密叢集的跨區域快照複本

您可以將 Amazon Redshift 設定為將叢集的快照複製到另一個 AWS 區域。若要設定跨區域快照複製，您需要為每個叢集啟用此複製功能，並設定複製快照的位置，以及在目的地 AWS 區域中保留複製自動或手動快照的時間長度。為叢集啟用跨區域複製時，所有新的手動和自動快照都會複製到指定的 AWS 區域。複製的快照名稱前面會加上 **copy:**。

設定跨區域快照

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽功能表上，選擇叢集，然後選擇您要移動快照的叢集。
3. 針對動作，選擇設定跨區域快照。

隨即會出現 [設定跨區域] 對話方塊。

4. 針對複製快照，選擇是。
5. 在目的地 AWS 區域中，選擇要複製快照的目標 AWS 區域。
6. 在自動快照保留期間 (天) 中，選擇要在刪除自動快照之前保留在目的地 AWS 區域中的天數。
7. 在 [手動快照保留期間] 中，選擇代表手動快照在刪除前保留在目的地 AWS 區域中的天數值。如果您選擇自訂值，則保留期必須介於 1 到 3653 天之間。
8. 選擇儲存。

為已 AWS KMS 加密的叢集設定跨區域快照副本

當您啟動 Amazon Redshift 叢集時，您可以選擇使用 AWS Key Management Service (AWS KMS) 中的根金鑰加密該叢集。AWS KMS 鍵是特定於一個 AWS 區域。如果您想要為 AWS KMS—encrypted 叢集啟用跨區域快照複製，您必須為目 AWS 的地區域中的根金鑰設定快照副本授權。如此，即可讓 Amazon Redshift 在目標 AWS 區域中執行加密操作。

下列程序說明為 AWS KMS 加密叢集啟用跨區域快照副本的程序。如需 Amazon Redshift 中的加密和快照複製權限授予的相關資訊，請參閱[複製 AWS KMS—加密的快照到另一個 AWS 區域](#)。

設定已 AWS KMS 加密叢集的跨區域快照

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽功能表上，選擇叢集，然後選擇您要移動快照的叢集。
3. 針對動作，選擇設定跨區域快照。

隨即會出現 [設定跨區域] 對話方塊。

4. 針對複製快照，選擇是。
5. 在目的地 AWS 區域中，選擇要複製快照的目標 AWS 區域。
6. 在自動快照保留期間 (天) 中，選擇要在刪除自動快照之前保留在目的地 AWS 區域中的天數。
7. 在 [手動快照保留期間] 中，選擇代表手動快照在刪除前保留在目的地 AWS 區域中的天數值。如果您選擇自訂值，則保留期必須介於 1 到 3653 天之間。
8. 選擇儲存。

修改跨區域快照副本的保留期間

設定跨區域快照副本後，您也許會想變更設定。您可輕易變更保留期間，只要選取新的天數，並儲存變更即可。

Warning

設定跨 AWS 區域快照副本之後，您無法修改目的地區域。

如果您要將快照複製到不同的 AWS 區域，請先停用跨區域快照複製。然後使用新的目的地 AWS 區域和保留期間重新啟用它。在您停用跨區域快照副本後，所有複製的自動化快照都會遭到刪除。因此，建議您判斷是否有想要保留的項目，以便先將其複製到手動快照，再停用跨區域快照副本。

修改跨區域快照

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽功能表上，選擇叢集，然後選擇您要修改快照的叢集。
3. 對於 Actions (動作)，選擇 Configure cross-region snapshot (設定跨區域快照) 以顯示快照的屬性。
4. 輸入快照定義的修訂屬性，然後選擇 Save (儲存)。

使用 AWS CLI 和 Amazon Redshift API 管理快照

您可以使用下列 Amazon Redshift CLI 操作來管理快照。

- [authorize-snapshot-access](#)
- [copy-cluster-snapshot](#)
- [create-cluster-snapshot](#)
- [delete-cluster-snapshot](#)
- [describe-cluster-snapshots](#)
- [disable-snapshot-copy](#)
- [enable-snapshot-copy](#)
- [modify-snapshot-copy-retention-period](#)
- [restore-from-cluster-snapshot](#)
- [revoke-snapshot-access](#)

您可以使用下列 Amazon Redshift API 動作來管理快照。

- [AuthorizeSnapshot存取](#)
- [CopyCluster快照](#)
- [CreateCluster快照](#)
- [DeleteCluster快照](#)
- [DescribeCluster快照](#)
- [DisableSnapshot複製](#)
- [EnableSnapshot複製](#)

- [ModifySnapshotCopyRetention期間](#)
- [RestoreFromClusterSnapshot](#)
- [RevokeSnapshot存取](#)

如需 Amazon Redshift 快照的相關資訊，請參閱 [Amazon Redshift 快照和備份](#)。

使用 AWS Backup

AWS Backup 是一項全受管的服務，可協助您跨 AWS 服務、在雲端中和在內部部署環境內，集中管理並自動化資料保護。

使用 Amazon Redshift 的 AWS Backup，您可以設定資料保護政策，並集中監控不同 Amazon Redshift 資源的活動。您也可以 Amazon Redshift 佈建叢集上建立和存放快照。這可讓您自動化並整合之前必須單獨執行的備份任務，而不必進行任何手動程序。

備份 (亦稱為復原點) 表示某個特定時間的資源內容，例如 Amazon Redshift 叢集。備份通常是指 AWS 服務中的不同備份，例如 Amazon Redshift 快照。AWS Backup 會將備份儲存在備份保存庫中，您可以根據業務需求組織備份。復原點和備份這兩個詞可互換使用。如需 AWS Backup 的詳細資訊，請參閱 [使用備份](#)。

Amazon Redshift 與 AWS Backup 原生整合。這可讓您定義備份計劃，並將 Amazon Redshift 資源指派給備份計劃。AWS Backup 會自動建立 Amazon Redshift 手動快照，並安全地將這些快照存放在您於備份計劃中指定的加密備份保存庫中。如需保存庫的相關資訊，請參閱 [使用備份保存庫](#)。在備份計劃中，您可以定義備份頻率、備份時段、生命週期或備份保存庫。如需備份計劃的相關資訊，請參閱 [使用備份計劃管理備份](#)。

主題

- [搭配 Amazon Redshift 使用 AWS Backup 時的考量](#)
- [使用 Amazon Redshift 管理 AWS Backup](#)

搭配 Amazon Redshift 使用 AWS Backup 時的考量

以下各節描述搭配 Amazon Redshift 使用 AWS Backup 時的考量和限制。

搭配 Amazon Redshift 使用 AWS Backup 時的考量

搭配 Amazon Redshift 使用 AWS Backup 時的考量如下：

- Amazon Redshift 的 AWS Backup 是可供使用的，AWS Backup 和 Amazon Redshift 都會在相同的 AWS 區域中可供使用。如需有關 AWS Backup 在哪些區域可供使用的資訊，請參閱[各 AWS 區域的功能可用性](#)。
- 若要開始使用 AWS Backup，請確認您已符合所有先決條件。如需詳細資訊，請參閱[先決條件](#)。
- 選擇加入 AWS Backup 服務。選擇加入選項適用於特定帳戶和 AWS 區域。您可能必須使用相同帳戶選擇加入多個區域。如需詳細資訊，請參閱[入門 1：選擇加入服務](#)。
- 您可以從 Amazon Redshift 主控台建立手動和自動快照。AWS Backup 目前僅支援手動快照。
- 使用 AWS Backup 管理快照設定後，就無法再使用 Amazon Redshift 繼續管理手動快照設定。相反地，您可以繼續使用 AWS Backup 計劃來管理設定。如需詳細資訊，請參閱[使用備份計劃管理備份](#)。
- 若要在備份已啟用版本控制的 Amazon S3 儲存貯體時節省儲存成本，建議您設定生命週期到期規則。如需有關指定生命週期規則的資訊，請參閱[範例 6：為已啟用版本控制的儲存貯體指定生命週期規則](#)。如果您沒有設定生命週期過期期間，則 Amazon Redshift 儲存成本可能會增加，因為 AWS Backup 會保留所有版本的 Amazon Redshift 資料。

限制

以下是在 Amazon Redshift 中使用 AWS Backup 的限制：

- 您無法使用 AWS Backup 來管理 Amazon Redshift 自動快照。若要管理自動快照，請使用標籤。如需有關標記資源的資訊，請參閱[在 Amazon Redshift 中標記資源](#)。
- AWS Backup 不支援 Amazon Redshift Serverless。

使用 Amazon Redshift 管理 AWS Backup

若要保護 Amazon Redshift 佈建叢集上的資源，您可以使用 AWS Backup 主控台，或以程式設計方式使用 AWS Backup API 或 AWS Command Line Interface (AWS CLI)。當您需要復原資源時，即可使用 AWS Backup 主控台或 AWS CLI 來尋找並復原所需資源。如需更多詳細資訊，請參閱[AWS Command Line Interface](#)。

您可以在使用適用於 Amazon Redshift 的 AWS Backup 時執行下列動作：

- 建立會自動啟動 Amazon Redshift 快照的定期備份。定期備份對於滿足您的長期資料保留需求非常有用。如需詳細資訊，請參閱[Amazon Redshift 備份](#)。
- 集中設定備份計劃，將備份排程與保留自動化。

- 將叢集還原至您選擇的已儲存備份。您必須設定備份資源的頻率。如需詳細資訊，請參閱[還原 Amazon Redshift 叢集](#)。

設定多可用區部署

針對 RA3 佈建叢集，Amazon Redshift 支援多個可用區域 (多可用區) 部署。透過使用多可用區部署，Amazon Redshift 資料倉儲可以在可用區域發生意外事件時，於失敗情況下繼續運作。多可用區部署會在兩個可用區域 (AZ) 中部署運算資源，而這些運算資源可透過單一端點來存取。如果整個可用區域發生故障，便可使用第二個可用區域中的剩餘運算資源繼續處理工作負載。在執行多可用區資料倉儲時，Amazon Redshift 會針對 RA3 收取相同的每小時運算費率。儲存成本保持不變，因為會在所有可用區域內部和 AWS 區域共用。

目前，Amazon Redshift 支援零復原點目標 (RPO)，可讓資料 up-to-date 在發生故障時保持最新狀態。透過多可用區部署，Amazon Redshift 可進一步增強其現有的復原功能，並減少其復原時間點目標 (RTO)。這是因為多可用區部署可以更快地從故障或災難中復原，進而將 Amazon Redshift 服務水準協議 (SLA) 提升到 99.99%，相較之下，單一可用區資料倉儲只有 99.9%。

設定多可用區部署

若要設定多可用區部署，請選取多可用區選項，並指定要在每個可用區域中佈建的運算節點數目。Amazon Redshift 會在兩個可用區域自動部署相同的運算資源，而且在正常操作期間，所有運算資源始終可用於進行讀取和寫入處理。這可讓多可用區部署作為具有單一端點的單一資料倉儲，而不需要在發生災難時變更應用程式。雖然多可用區部署只會使用一個可用區域的運算資源來處理個別查詢，但它可以自動將多個同時查詢的處理分配到兩個可用區域，以提升高並行工作負載數量的整體輸送量。

您也可以將現有的單一可用區資料倉儲轉換為多可用區資料倉儲，反之亦然。除了在第二個可用區域中會佈建額外的運算資源外，其他的部署都相同。從現有的單一可用區叢集遷移至多可用區時，您可能需要將所需的叢集節點數目加倍，以便維持單一查詢效能。大多數工作負載都會發現多可用區資料倉儲的整體查詢處理輸送量會增加，因為可用的運算資源數量是兩倍。

如果可用區域發生故障，Amazon Redshift 會自動使用剩餘可用區域中的資源繼續運作。不過，使用者連線可能會中斷，而且必須重新建立。此外，在失敗的可用區域中執行的查詢可能會失敗，必須重試。不過，您可以立即重新連線到叢集並為查詢重新排程，Amazon Redshift 則會處理剩餘可用區域中的查詢。在多可用區資料倉儲復原時，於故障發生當下起所發出的查詢可能會發生執行時間延遲。

Note

為了獲得更好的效能和更高的可用性，建議您對多可用區叢集使用 SNAPSHOT ISOLATION。如需詳細資訊，請參閱 [CREATE DATABASE](#)。

限制

多可用區資料倉儲具有與單一可用區資料倉儲相同的功能，但下列適用於多可用區資料倉儲的限制除外：

- 您無法建立未加密的多可用區資料倉儲。在建立新的多可用區資料倉儲、將單一可用區資料倉儲轉換為多可用區資料倉儲，或將單一可用區資料倉儲轉換為多可用區資料倉儲時，請務必新增加密。
- 您無法為任何 RA3 執行個體類型建立單一節點多可用區部署。在建立多可用區部署時，請為每個可用區域選擇 2 個以上的節點。
- Amazon Redshift 不支援可支援少於三個可用區域的子網路組態。換句話說，所設定的子網路群組需要另外三個子網路。
- 多可用區部署無法重新放置到其他可用區域。使用多可用區部署時，Amazon Redshift 會自動判斷和執行重新放置。
- 您無法暫停或繼續多可用區部署。
- 您無法在支援的連接埠範圍 5431 至 5455 和 8191 至 8215 之外執行多可用區部署。
- 您無法將 STL、SVCS、SVL、SVV、STV 檢視與多可用區部署搭配使用，因為它們只支援系統監控檢視 (SYS_* 檢視)。請變更監控查詢以使用系統監控檢視 (SYS_* 檢視)。
- 您無法將彈性 IP 位址附加到已啟用異地同步備份的現有叢集。
- 您無法將具有連接彈性 IP 位址的叢集從單一同步備份轉換為異地同步備份。
- Amazon Redshift 地同步備份部署提供以下服務：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)
 - 非洲 (開普敦) (af-south-1)
 - 亞太區域 (香港) (ap-east-1)
 - 亞太區域 (海德拉巴) (ap-south-2)
 - 亞太區域 (雅加達) (ap-southeast-3)

- 亞太區域 (墨爾本) (ap-southeast-4)
- 亞太區域 (孟買) (ap-south-1)
- 亞太區域 (大阪) (ap-northeast-3)
- 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 (米蘭) (eu-south-1)
- 歐洲 (巴黎) (eu-west-3)
- 歐洲 (西班牙) (eu-south-2)
- 歐洲 (斯德哥爾摩) (eu-north-1)
- 歐洲 (蘇黎世) (eu-central-2)
- 以色列 (特拉維夫) (il-central-1)
- 中東 (巴林) (me-south-1)
- 中東 (阿拉伯聯合大公國) (me-central-1)

主題

- [管理多可用區部署](#)
- [容錯移轉多可用區部署](#)
- [多可用區的查詢監控](#)

管理多可用區部署

Amazon Redshift 多可用區一次支援兩個可用區域。Amazon Redshift 會自動根據選取的子網路群組組態來選取可用區域。您可以將現有的單一可用區域資料倉儲轉換為多可用區資料倉儲，或從快照還原以將其設定為多可用區資料倉儲。

您可以使用 Amazon Redshift 主控台輕鬆建立新的多可用區部署。若要使用 Amazon Redshift 主控台 建立新的多可用區部署，請在建立資料倉儲時選取多可用區選項。指定單一可用區域中所需的運算節

點數量，Amazon Redshift 便會在兩個可用區域中各自部署該數量的節點。在正常操作期間，所有節點都會用於讀取和寫入工作負載的處理。您也可以使用 AWS CLI `create-cluster` 指令，使用 `multi-az` 參數建立新的異地同步備份資料倉儲。

您可以將現有的單一可用區資料倉儲轉換為異地同步備份資料倉儲，也可以使用 Amazon Redshift 主控台或使用該參數的 AWS CLI `modify-cluster` 命令。 `multi-az` 或者，您可以使用 Amazon Redshift 主控台或使用參數從快照還原，將單一可用區資料倉儲設定為異地同步備份 AWS CLI `restore-from-cluster-snapshot` 資料倉儲。 `multi-az`

多可用區部署僅支援使用 Amazon Redshift 受管儲存 (RMS) 的 RA3 節點類型。Amazon Redshift 會將資料存放在 RMS 中，該 RMS 使用 Amazon S3，而且可以在中的所有可用區域中存取 AWS 區域，而不必在 Amazon Redshift 層級複寫資料。

在建立新叢集時設定多可用區

您可以使用 Amazon Redshift 主控台或 AWS Command Line Interface 在建立新叢集時設定多可用區部署。

使用主控台

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽功能表上，選擇佈建叢集儀表板，然後選擇叢集。AWS 區域 會列出目前帳戶的叢集。每個叢集的屬性子集會在清單中分欄顯示。
3. 選擇建立叢集按鈕以開啟 [建立叢集] 頁面。
4. 輸入叢集的屬性。如需有關建立叢集的一般資訊，請參閱 [建立叢集](#)。
5. 從節點類型下拉式清單中選擇其中一種 RA3 節點類型。AZ 組態選項只會在選擇了 RA3 節點類型時才可供使用。
6. 在 AZ 組態下，選擇多可用區。
7. 在每個可用區域的節點數量下，為叢集輸入至少兩個節點。
8. 您可以選擇載入範例資料或帶入自己的資料：
 - 在範例資料中，選擇載入範例資料，將範例資料集載入 Amazon Redshift 叢集。Amazon Redshift 會將範例資料集 Tickit 載入預設 dev 資料庫和 public 結構描述。Amazon Redshift 會自動將範例資料集載入您的 Amazon Redshift 叢集。您可以開始使用查詢編輯器 v2 來查詢資料。
 - 若要將自己的資料帶入您的 Amazon Redshift 叢集，請按照 [將自己的資料帶入 Amazon Redshift](#) 中的步驟進行操作。

9. 向下捲動至其他組態、展開網路和安全，並務必接受預設的叢集子網路群組，或選擇另一個群組。如果您選擇另一個叢集子網路群組，請確定您選取的子網路群組中有 3 個可用區域。
10. 在其他組態下，展開資料庫組態。
11. 若要使用自訂 AWS KMS 金鑰而非預設金 AWS Key Management Service 鑰，請按一下 [資料庫加密] 底下的 [自訂加密設定]。
12. 在 [選擇 KMS 金鑰] 底下，您可以選擇金 AWS Key Management Service 鑰或輸入 ARN。或者，您也可以按一下 AWS Key Management Service 主控台中的 [建立 AWS Key Management Service 金鑰]。如需建立 KMS 金鑰的相關資訊，請參閱《AWS Key Management Service 開發人員指南》中的[建立金鑰](#)。
13. 按一下建立叢集。叢集建立成功時，您可以在叢集詳細資訊頁面中檢視詳細資訊。您可以使用 SQL 用戶端來載入和查詢資料。

使用 AWS Command Line Interface

使用建立叢集時設定異地同步備份 AWS Command Line Interface

- 從使 AWS CLI 用命 `create-cluster` 令和 `multi-az` 參數如下。

```
aws redshift create-cluster
  --port 5439
  --master-username master
  --master-user-password #####
  --node-type ra3.4xlarge
  --number-of-nodes 2
  --profile maz-test
  --endpoint-url https://redshift.eu-west-1.amazonaws.com
  --region eu-west-1
  --cluster-identifier test-maz
  --multi-az
  --maintenance-track-name CURRENT
  --encrypted
```

將單一可用區資料倉儲轉換為多可用區資料倉儲

透過將單一可用區資料倉儲轉換為多可用區資料倉儲，您的資料倉儲將具備 99.99% SLA 保證的高可用性。即使使用多可用區資料倉儲，個別查詢的效能仍會保持不變。對於較高的並行工作負載數量，由於 Amazon Redshift 可以使用兩個可用區域中的運算資源來執行請求，因此整體輸送量會有所提升。

Note

Amazon Redshift 不允許您在從單一可用區轉換為多可用區時分割現有的運算資源，反之亦然。不支援透過此操作來維持一致的個別查詢效能。

使用主控台

使用主控台將單一可用區叢集轉換為多可用區資料倉儲

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽功能表上，選擇佈建叢集儀表板，然後選擇叢集。AWS 區域 會列出目前帳戶的叢集。每個叢集的屬性子集會在清單中分欄顯示。
3. 選擇您要轉換為多可用區部署的叢集。隨即會出現叢集詳細資訊頁面。
4. 對於動作，選擇啟用多可用區。隨即會出現修改摘要。按一下啟用多可用區。
5. 發生錯誤時，請執行下列其中一項動作，然後按一下啟用多可用區。
 - 叢集加密 — 選擇屬性可在叢集詳細資訊頁面之 [屬性] 索引標籤底下的 [資料庫組態] 區段中編輯加密設定。
 - 子網路群組 — 選擇子網路群組，可透過按一下子網路群組連結來編輯叢集子網路群組設定。如果您選擇另一個叢集子網路群組，請確定您選取的子網路群組中有 3 個可用區域。
 - 連接埠設定 — 選擇屬性可在叢集詳細資訊頁面之 [屬性] 索引標籤底下的 [資料庫組態] 區段中編輯連接埠設定。
6. 您可以使用 SQL 用戶端來載入和查詢資料。

使用 AWS Command Line Interface

- 在中 AWS CLI，使用指 `modify-cluster` 令和 `multi-az` 參數，如下所示。

```
aws redshift modify-cluster
  --profile maz-test
  --endpoint-url https://redshift.eu-west-1.amazonaws.com
  --region eu-west-1
  --cluster-identifier test-maz-11
  --multi-az
```

將多可用區資料倉儲轉換為單一可用區資料倉儲

透過將多可用區資料倉儲轉換為單一可用區資料倉儲，您的資料倉儲將不會獲得多可用區所提供的 99.99% SLA 保證。個別查詢的效能會保持不變，但是整體輸送量會受到影響，因為無法使用第二個可用區域中的運算資源。您可以選擇啟用並行擴展，自動擴展輸送量以在使用單一可用區時仍可獲得一致的效能。

Note

Amazon Redshift 不允許您在從單一可用區轉換為多可用區時分割現有的運算資源，反之亦然。不支援透過此操作來維持一致的個別查詢效能。

使用主控台

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽功能表上，選擇佈建叢集儀表板，然後選擇叢集。AWS 區域 會列出目前帳戶的叢集。每個叢集的屬性子集會在清單中分欄顯示。
3. 選擇您要轉換為多可用區部署的叢集。隨即會出現叢集詳細資訊頁面。
4. 對於動作，選擇停用多可用區。隨即會出現修改摘要。按一下停用多可用區。

使用 AWS Command Line Interface

- 在中 AWS CLI，使用指 `modify-cluster` 令和 `no-multi-az` 參數，如下所示。

```
aws redshift modify-cluster
  --profile maz-test
  --endpoint-url https://redshift.eu-west-1.amazonaws.com
  --region eu-west-1
  --cluster-identifier test-maz-11
  --no-multi-az
```

一旦您的資料倉儲轉換為單一可用區，就會失去 99.99 的 SLA 保證。整體輸送量也會受到影響。儲存變更後，便可以在叢集詳細資訊頁面中檢視詳細資訊。

調整多可用區資料倉儲的大小

您可以調整多可用區資料倉儲的大小，並指定與目前的資料倉儲組態不同的節點數量或節點類型。

使用主控台

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽功能表上，選擇佈建叢集儀表板，然後選擇叢集。AWS 區域 會列出目前帳戶的叢集。每個叢集的屬性子集會在清單中分欄顯示。
3. 選擇您要調整多可用區資料倉儲大小的叢集。隨即會出現叢集詳細資訊頁面。
4. 針對 Actions (動作)，選擇 Resize (調整大小)。Resize cluster (調整叢集大小) 頁面隨即出現。
5. 遵循頁面說明以進行操作。您可以在特定時間立即重新調整叢集的大小一次，或是根據排程增加或減少您叢集的大小。
6. 在新增組態底下，從 [節點類型] 下拉式清單中選擇其中一種 RA3 節點類型。
7. 按一下調整叢集大小。

使用 AWS Command Line Interface

使用重新調整異地同步備份資料倉儲的大小 AWS Command Line Interface

- 在中 AWS CLI，使用命 `resize-cluster` 令來變更單一可用區域的節點數目，如下所示。

```
aws redshift resize-cluster \  
  --cluster-identifier test-maz-11  
  --cluster-type multi-node  
  --node-type ra3.4xlarge  
  --number-of-nodes 6
```

為從快照還原的資料倉儲設定多可用區

您也可以透過從快照還原來建立新的多可用區叢集。

使用主控台

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。

2. 在導覽功能表上，選擇叢集、快照，然後選擇要使用的快照。
3. 選擇還原快照、還原至佈建叢集。
4. 輸入叢集的屬性。如需有關建立叢集的一般資訊，請參閱[建立叢集](#)。
5. 從節點類型下拉式清單中選擇其中一種 RA3 節點類型。AZ 組態選項只會在選擇了 RA3 節點類型時才可供使用。
6. 在 AZ 組態下，選擇多可用區。
7. 在每個可用區域的節點數量下，為叢集輸入至少兩個節點。
8. 您可以選擇載入範例資料或帶入自己的資料：
 - 在範例資料中，選擇載入範例資料，將範例資料集載入 Amazon Redshift 叢集。Amazon Redshift 會將範例資料集 Tickit 載入預設 dev 資料庫和 public 結構描述。Amazon Redshift 會自動將範例資料集載入您的 Amazon Redshift 叢集。您可以開始使用查詢編輯器 v2 來查詢資料。
 - 若要將自己的資料帶到您的 Amazon Redshift 叢集，請按照將[資料從 Amazon S3 載入到亞馬 Amazon Red shift](#) 中的步驟進行操作。
9. 向下捲動至其他組態、展開網路和安全，並務必接受預設的叢集子網路群組，或選擇另一個群組。如果您選擇另一個叢集子網路群組，請確定您選取的子網路群組中有 3 個可用區域。
10. 在其他組態下，展開資料庫組態。
11. 在 [資料庫加密] 底下，若要使用預設金鑰以外的自訂 KMS 金 AWS Key Management Service 鑰，請按一下 [自訂加密設定]。預設會取消選取此選項。
12. 在 [選擇 KMS 金鑰] 底下，您可以選擇金 AWS Key Management Service 鑰或輸入 ARN。或者，您也可以按一下 AWS Key Management Service 主控台中的 [建立 AWS Key Management Service 金鑰]。如需建立 KMS 金鑰的相關資訊，請參閱《AWS Key Management Service 開發人員指南》中的[建立金鑰](#)。
13. 按一下從快照還原叢集。叢集還原成功時，您可以在叢集詳細資訊頁面中檢視詳細資訊。

使用 AWS Command Line Interface

- 在中 AWS CLI，使用 `restore-from-cluster-snapshot` 指令，如下所示。

```
aws redshift restore-from-cluster-snapshot
--region eu-west-1
--multi-az
--snapshot-identifier test-snap1
--cluster-identifier test-saz-11
```

```
--endpoint-url https://redshift.eu-west-1.amazonaws.com/
```

容錯移轉多可用區部署

多可用區資料倉儲是同時部署在兩個可用區域中的集合運算資源。部署在主要可用區域中的運算資源稱為主要運算，部署在次要可用區域中的運算資源則稱為次要運算。在可用區域或基礎設施發生故障等罕見事件時，多可用區資料倉儲不必使用者介入即可自動復原。復原程序包括從主要運算容錯移轉到次要運算，以及將次要運算資源指定為主要運算資源。此外，新的次要運算資源也會佈建到第三個可用區域。自動復原程序會根據 RTO 和 RPO 來進行測量。

- 復原時間點目標 (RTO) — 系統在災難發生後恢復運作狀態所需的時間。換言之，RTO 會測量停機時間。
- 復原點目標 (RPO) — 可能遺失的資料量 (以時間為單位)。對於 Amazon Redshift 多可用區資料倉儲而言，RPO 一般是零，因為所有資料都儲存在 Amazon Redshift 受管儲存 (RMS) 中，並由 Amazon Simple Storage Service 提供支援，其預設具有高耐用性和高可用性。

Note

發生容錯移轉之後，個別查詢的效能不會發生變化。由於其中一個可用區域中的運算資源無法使用，因此資料倉儲的整體輸送量會短暫降低。不過，Amazon Redshift 會自動取得另一個可用區域中的容量，確保系統會恢復相同的資料倉儲處理容量。

除了自動復原程序外，您也可以使用容錯移轉主要運算選項，針對資料倉儲手動觸發此程序。您可以使用此方法來測試多可用區對於讓應用程式獲得更高的高可用性和更好的連續性有多大幫助。

使用主控台

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 執行以下任意一項：
 - 在導覽功能表上，選擇叢集。在叢集底下，選擇叢集。隨即會出現叢集詳細資訊頁面。
 - 從叢集儀表板中選擇叢集。
3. 從動作中，選擇容錯移轉主要運算。
4. 出現提示時，按一下確認。

使用 AWS Command Line Interface

- 在中 AWS CLI，使用 `failover-primary-compute` 指令，如下所示。

```
aws redshift failover-primary-compute
  --profile maz-test
  --endpoint-url https://redshift.eu-west-1.amazonaws.com
  --region eu-west-1
  --cluster-identifier test-maz-11
```

確認上述操作後，Amazon Redshift 便會執行與從可用區域或基礎設施故障自動復原時相同的步驟。此程序會導致主要可用區域中的運算節點無法使用，並將次要可用區域中的運算資源指定為主要運算。成功完成叢集復原後，多可用區部署便會可供使用。多可用區資料倉儲也會在別的第三個可用區域可供使用時自動在其中佈建新的次要運算。

在這個過程中，當叢集自動復原並重新設定回多可用區部署設定時，主控台上的叢集狀態會在整個時間都顯示為正在修改。叢集可以立即接受新的連線。現有連線和執行中的查詢可能會遭到捨棄。您可以立即重試這些項目。

多可用區的查詢監控

無論叢集的類型、大小和狀態 (暫停或繼續) 為何，您都可以檢視過去 7 天所執行之查詢的相關資訊。

檢視多可用區資料倉儲的查詢和載入

[查詢和載入] 頁面上顯示的資訊會填入來自 Amazon Redshift 系統資料表 (SYS_* 檢視) 的資訊。此資訊可讓您顯示有關查詢的其他資訊，並提供滾動 7 天的保留期。查詢診斷會變得更快，可讓您依資料庫、使用者名稱或 SQL 陳述式類型來篩選資料。若要查看這些額外的篩選條件和所有已執行查詢的資訊，請注意下列先決條件：

- 您必須選擇連線至資料庫來連線至資料庫。
- 資料庫使用者必須具有 `sys:operator` 或 `sys:monitor` 角色和許可，才能執行查詢監控。如需有關系統角色的資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的 [Amazon Redshift 系統定義角色](#)。

在連線至資料庫後，便會看到這些額外的篩選條件和查詢資訊。

顯示來自查詢和載入的查詢效能資料

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽功能表上，選擇查詢和載入以顯示帳戶的查詢清單。
3. 您可能必須連線至資料庫才能查看其他篩選條件。如有必要，請按一下連線至資料庫，然後依照提示進行來連線至資料庫。

根據預設，此清單會顯示過去 24 小時您所有叢集的查詢。您可在主控台中變更顯示日期的範圍。

顯示來自查詢監控的查詢效能資料

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽功能表上，選擇叢集。在叢集底下，選取叢集。
3. 選擇查詢監控。
4. 視叢集的組態或版本而定，您可能必須連線至資料庫才能看到其他篩選條件。如有必要，請按一下連線至資料庫，然後依照提示進行來連線至資料庫。

監控多可用區部署中的查詢

多可用區部署會使用同時部署在兩個可用區域的運算資源，並可在指定可用區域中的資源無法使用時繼續運作。系統隨時會使用所有運算資源。這可讓系統以主動-主動的方式跨兩個可用區域進行完整操作，以便執行讀取和寫入操作。

您可以在 `pg_catalog` 結構描述中查詢 `SYS_` 檢視，以監控多可用區部署中的查詢執行時間。`SYS_` 檢視會顯示主要和次要叢集的查詢執行時間活動或統計資料。如需監控檢視的清單，請參閱[監控檢視](#)。

請依照下列步驟監控多可用區部署內每個可用區域的查詢執行時間：

1. 導覽至 Amazon Redshift 主控台，並連線到多可用區部署中的資料庫，然後透過查詢編輯器執行查詢。
2. 在多可用區 Amazon Redshift 部署上執行任何範例查詢。
3. 對於多可用區部署，您可以透過使用 `SYS_QUERY_HISTORY` 資料表中的 `compute_type` 資料欄來識別查詢和用來執行查詢的可用區域。「主要」代表在多可用區部署中的主要叢集上執行的查詢，「次要」代表在多可用區部署中的次要叢集上執行的查詢。

下列查詢會使用 `compute_type` 資料欄來監控查詢。

```
select (compute_type) as compute_type, left(query_text, 50) query_text from
sys_query_history order by start_time desc;

compute_type | query_text
-----+-----
secondary | select count(*) from t1;
```

終止叢集的查詢

終止叢集的查詢

此程序同時適用於多可用區叢集和單一可用區叢集。

終止查詢

您也可以使用 Queries (查詢) 頁面終止目前正在進行的查詢。

資料庫使用者必須具有 `sys:operator` 角色和許可，才能結束執行中的查詢。如需有關系統角色的資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的 [Amazon Redshift 系統定義角色](#)。

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽功能表上，選擇查詢和載入以顯示帳戶的查詢清單。
3. 選擇清單中要終止的執行中查詢，然後選擇 Terminate query (終止查詢)。

使用主控台管理叢集

若要建立、修改、調整大小、刪除、重新啟動和備份叢集，請使用 Amazon Redshift 主控台內的叢集區段。

檢視叢集

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽選單上，選擇叢集。會列出目前 AWS 區域中您帳戶的叢集。每個叢集的屬性子集會在清單中分欄顯示。如果您沒有任何叢集，請選擇 Create cluster (建立叢集) 以建立一個叢集。

3. 選擇清單中的叢集名稱以檢視該叢集的詳細資訊。

主題

- [建立叢集](#)
- [建立預覽叢集](#)
- [修改叢集](#)
- [刪除叢集](#)
- [重新啟動叢集](#)
- [調整叢集大小](#)
- [升級叢集的發行版本](#)
- [取得叢集組態資訊](#)
- [取得叢集狀態概觀](#)
- [建立叢集快照](#)
- [建立或編輯磁碟空間警示](#)
- [使用叢集效能資料](#)

建立叢集

建立叢集之前，請閱讀[Amazon Redshift 概述](#)和 [Amazon Redshift 中的叢集和節點](#)。

建立叢集

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽選單上，選擇叢集。會列出目前 AWS 區域中您帳戶的叢集。每個叢集的屬性子集會在清單中分欄顯示。
3. 選擇 Create cluster (建立叢集) 以建立叢集。
4. 遵循主控台頁面說明以輸入 Cluster configuration (叢集組態) 的屬性。

下列步驟說明在支援 RA3 節點類型的下列項目中執行 AWS 區域的 Amazon Redshift 主控台。如需支援 RA3 節點類型 AWS 區域的清單，請參閱 Amazon Redshift 管理指南中的 [RA3 節點類型概觀](#)。

如果您不知道要將叢集的大小調整到多大，請選擇協助我選擇。這樣做會啟動調整大小計算器，詢問您有關計劃儲存在資料倉儲中之資料的大小和查詢特性的問題。如果您知道叢集的所需大小（也就是節點類型和節點數目），請選擇我會選擇。然後選擇節點類型和節點數量來調整叢集的大小以進行概念驗證。

Note

如果您的組織符合資格，而且您的叢集是在無法使用 Amazon Redshift 無伺服器的 AWS 區域 地方建立，您也許可以在 Amazon Redshift 免費試用計劃下建立叢集。選擇生產或免費試用來回答問題您打算將此叢集用於什麼目的？選擇免費試用時，您可以使用 dc2.large 節點類型建立組態。如需選擇免費試用的相關資訊，請參閱 [Amazon Redshift 免費試用版](#)。如需提供 Amazon Redshift 無伺服器的位 AWS 區域 置清單，請參閱中針對 [Redshift 無伺服器](#) API 列出的端點。Amazon Web Services 一般參考

- 在資料庫組態區段中，指定管理員使用者名稱的值。針對管理員密碼，您可以從下列選項中選擇：
 - 產生密碼 - 使用 Amazon Redshift 產生的密碼。
 - 手動新增管理員密碼 - 使用您自己的密碼。
 - 在中管理管理登入資料 AWS Secrets Manager — Amazon Redshift 會用 AWS Secrets Manager 來產生和管理您的管理員密碼。用 AWS Secrets Manager 於生成和管理密碼的秘密需要支付費用。如需 AWS Secrets Manager 定價的詳細資訊，請參閱 [AWS Secrets Manager 定價](#)。
- (選用) 遵循主控台頁面說明以輸入 Cluster permissions (叢集許可) 的屬性。如果您的叢集需要為您存取其他 AWS 服務，例如從 Amazon S3 載入資料，請提供叢集許可。
- 選擇 Create cluster (建立叢集) 以建立叢集。該叢集可能需要幾分鐘方可使用。

其他組態

當您建立叢集時，您可以指定其他屬性進行自訂。您可以在下列清單中找到部分屬性的詳細資訊。

IP 地址類型

選擇叢集的 IP 地址類型。您可以選擇讓資源僅透過 IPv4 定址通訊協定進行通訊，或選擇雙堆疊模式，讓資源同時透過 IPv4 和 IPv6 進行通訊。此功能僅適用於 AWS GovCloud (美國東部) 和 AWS GovCloud (美國西部) 區域。如需區 AWS 域的詳細資訊，請參閱 [區域和可用區域](#)。

Virtual Private Cloud (VPC) (虛擬私有雲端 (VPC))

選擇具有叢集子網路群組的 VPC。建立叢集後，就無法變更叢集子網路群組。

參數群組


選擇要與該叢集建立關聯的叢集參數群組。如果您沒有選擇，則該叢集會使用預設參數群組。

加密

選擇您是否要加密叢集及其快照內的所有資料。如果您保留預設設定為 None (無)，加密將不會啟用。如果您想啟用加密，請選擇您是否要使用 AWS Key Management Service (AWS KMS) 或硬體安全模組 (HSM)，然後設定相關的設定。如需 Amazon Redshift 中加密的相關資訊，請參閱 [Amazon Redshift 資料庫加密](#)。

- KMS

如果您要啟用加密並使用來管理加密金鑰，請選擇使用 AWS Key Management Service AWS KMS (AWS KMS)。此外，也請選擇要使用的金鑰。您可以選擇預設金鑰、目前帳戶的金鑰或其他帳戶的金鑰。

 Note

如果您想要使用其他 AWS 帳戶的金鑰，請輸入要使用的金鑰的 Amazon 資源名稱 (ARN)。您必須擁有許可才能使用該金鑰。如需中金鑰存取權的詳細資訊 AWS KMS，請參閱《AWS Key Management Service 開發人員指南》中的 [「控制金鑰存取」](#)。

如需在 Amazon Redshift 中使用 AWS KMS 加密金鑰的詳細資訊，請參閱 [使用 AWS KMS 的 Amazon Redshift 資料庫加密](#)。

- HSM

如果您想啟用加密並使用硬體安全模組 (HSM) 來管理您的加密金鑰，請選擇 HSM (HSM)。

若您選擇 HSM，請從 HSM Connection (HSM 連線) 與 HSM Client Certificate (HSM 用戶端憑證) 選擇值。Amazon Redshift 和 HSM 需要這些值才能構建可傳遞叢集金鑰的信任連線。您必須在啟動叢集前先在 Amazon Redshift 中設定 HSM 連線與用戶端憑證。如需設定 HSM 連線與用戶端憑證的相關資訊，請參閱 [使用硬體安全模組的 Amazon Redshift 加密](#)。

維護軌道

您可以選擇所使用的叢集版本是否為 Current (目前)、Trailing (追蹤) 或 (有時) Preview (預覽) 軌道。

監控

您可以選擇是否要建立 CloudWatch 鬧鐘。

設定跨區域快照

您可以選擇是否啟用跨區域快照。

自動快照保留期

您可以在 35 天的範圍內選擇這些快照的保留天數。如果節點類型為 DC2，您可以選擇零 (0) 天來不建立自動快照。

手動快照保留期

您可以選擇天數或 Indefinitely 來保留這些快照。

建立預覽叢集

您可以在預覽版中建立 Amazon Redshift 叢集，以測試 Amazon Redshift 的新功能。您無法在生產環境中使用這些功能，也無法將預覽叢集移至生產叢集或其他軌道上的叢集。如需了解預覽版條款和條件，請參閱 [AWS 服務條款](#) 中的 Beta 版和預覽版。

建立預覽版叢集

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽功能表上，選擇佈建叢集儀表板，然後選擇叢集。AWS 區域 會列出目前帳戶的叢集。每個叢集的屬性子集會在清單中分欄顯示。
3. 叢集清單頁面上會顯示一個介紹預覽版的橫幅。選擇建立預覽叢集按鈕以開啟 [建立叢集] 頁面。
4. 輸入叢集的內容。選擇預覽軌道，其中包含您想要測試的功能。建議您輸入叢集名稱，以表示叢集位於預覽軌道上。針對您要測試的功能選擇叢集選項，包括標記為 -preview 的選項。如需有關建立叢集的一般資訊，請參閱《Amazon Redshift 管理指南》中的 [建立叢集](#)。
5. 選擇建立叢集按鈕以建立預覽叢集。

Note

preview_2023 軌跡是最近可用的預覽軌跡。此軌跡僅支援使用 RA3 節點類型建立叢集。不支援節點類型 DC2 和任何較舊的節點類型。

6. 當您的預覽叢集可用時，請使用 SQL 用戶端載入和查詢資料。

如需 Redshift Serverless 工作群組中預覽的相關資訊，請參閱[建立預覽工作群組](#)。

修改叢集

當您修改叢集時，以下選項變更會立即套用：

- VPC security groups (VPC 安全群組)
- 可公開存取
- 管理員使用者密碼
- HSM 連接
- HSM Client Certificate (HSM 用戶端憑證)
- 維護詳細資訊
- Snapshot preferences (快照偏好設定)

只有重新啟動叢集才能使以下選項的變更生效：

- 叢集識別碼

當您變更叢集識別碼時，Amazon Redshift 會自動重新啟動叢集。

- 增強型 VPC 路由

當您變更增強型 VPC 路由時，Amazon Redshift 會自動重新啟動叢集。

- 叢集參數群組
- IP 地址類型

此功能僅適用於 AWS GovCloud (美國東部) 和 AWS GovCloud (美國西部) 區域。如需區 AWS 域的詳細資訊，請參閱[區域和可用區域](#)。

若您縮短自動快照保留期間，設定落在新保留期間以外的現有自動快照將被刪除。如需詳細資訊，請參閱[Amazon Redshift 快照和備份](#)。

如需叢集屬性的相關資訊，請參閱[其他組態](#)。

修改叢集

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。

2. 在導覽功能表上，選擇叢集。
3. 選擇要修改的叢集。
4. 選擇編輯。編輯叢集頁面隨即出現。
5. 更新叢集屬性。您可以修改的一些屬性包括：
 - 叢集識別碼
 - 快照保留
 - 叢集重新定位

為了編輯網路和安全、維護和資料庫組態的設定，主控台會提供適當叢集詳細資訊索引標籤的連結。

6. 選擇儲存變更。

刪除叢集

若您不再需要您的叢集，您可以刪除它。若打算使用您要刪除的相同資料和組態來佈建新的叢集，您需要手動快照。您在稍後可以使用手動快照來還原快照，並繼續使用該叢集。如果您刪除叢集，但未建立最終手動快照，則會刪除叢集資料。在這兩種情況下，自動快照將在叢集刪除後一併刪除，但手動快照則會保留下來，直到您將它們刪除。您可能需要支付手動快照的 Amazon Simple Storage Service 儲存費用，這取決於叢集的 Amazon Redshift 快照可用的儲存量。如需詳細資訊，請參閱 [關閉及刪除叢集](#)。

刪除叢集也會刪除所有關聯的 AWS Secrets Manager 密碼。

刪除叢集

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽功能表上，選擇叢集。
3. 選擇要刪除的叢集。
4. 對於 Actions (動作)，請選擇 Delete (刪除)。Delete cluster (刪除叢集) 頁面隨即出現。
5. 選擇 Delete cluster (刪除叢集)。

Note

刪除叢集並選擇建立最終快照時，如果叢集上正在進行還原操作，Amazon Redshift 將停止刪除請求。如果發生這種情況，您可以在沒有最終快照的情況下刪除叢集，也可以在還原完成後使用最終快照刪除叢集。

重新啟動叢集

當您重新啟動叢集時，叢集狀態會設為 `rebooting`，當重新啟動完成時也會建立叢集事件。任何等待中的叢集修改都會套用在這次的重新啟動上。

重新啟動叢集

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽功能表上，選擇叢集。
3. 選擇要重新啟動的叢集。
4. 針對 Actions (動作)，選擇 Reboot cluster (重新啟動叢集)。Reboot cluster (重新啟動叢集) 頁面隨即出現。
5. 選擇 Reboot cluster (重新啟動叢集)。

調整叢集大小

當您重新調整叢集規模時，您將指定與目前叢集組態不同的節點數量或節點類型。當叢集正在進行重新規模調整時，您無法對該叢集執行任何寫入或讀寫查詢；您僅能執行讀取查詢。

如需重新調整叢集規模的相關資訊，包括使用不同方法的逐步解說資訊，請參閱 [調整叢集大小](#)。

重新調整叢集規模

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽功能表上，選擇叢集。
3. 選擇要調整大小的叢集。
4. 針對 Actions (動作)，選擇 Resize (調整大小)。Resize cluster (調整叢集大小) 頁面隨即出現。

5. 遵循頁面說明以進行操作。您可以在特定時間立即重新調整叢集的大小一次，或是根據排程增加或減少您叢集的大小。
6. 根據您的選擇，選擇 Resize now (立即調整大小) 或 Schedule resize (排程調整大小)。

如果您有保留節點，則可以升級至 RA3 保留節點。您可以在使用主控台從快照還原時或執行彈性調整大小時進行此升級。您可以使用主控台來引導您完成此程序。如需升級至 RA3 節點的相關資訊，請參閱 [升級至 RA3 節點類型](#)。

升級叢集的發行版本

您可以將發行維護版本 Release Status (發行狀態) 值為 New release available (新發行版本已推出) 的叢集升級。升級維護版本時，您可以選擇立即升級或在下一次的維護時段升級。

Important

如果您立即升級，則在升級完成前，您的叢集均會離線。

將叢集升級至新的發行版本

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽功能表上，選擇叢集。
3. 選擇要升級的叢集。
4. 針對 Actions (動作)，選擇 Upgrade cluster version (升級叢集版本)。Upgrade cluster version (升級叢集版本) 頁面隨即出現。
5. 遵循頁面說明以進行操作。
6. 選擇 Upgrade cluster version (升級叢集版本)。

取得叢集組態資訊

顯示叢集的相關資訊

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。

2. 在導覽功能表上，選擇叢集，然後從清單中選擇叢集名稱以開啟其詳細資訊。隨即顯示叢集的詳細資訊，包含叢集效能、查詢監控、資料庫、資料共用、排程、維護和屬性標籤。
3. 選擇每個標籤以檢視詳細資訊。

取得叢集狀態概觀

檢視叢集的狀態

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽功能表上，選擇叢集。
3. 在 Status (狀態) 欄中檢視叢集的狀態。

建立叢集快照

建立叢集快照

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽功能表上，選擇叢集。
3. 選擇要對其建立快照的叢集。
4. 針對 Actions (動作)，選擇 Create snapshot (建立快照)。Create snapshot (建立快照) 頁面隨即出現。
5. 遵循頁面說明以進行操作。
6. 選擇建立快照。

建立或編輯磁碟空間警示

為叢集建立磁碟空間使用量警示

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽功能表上，選擇警示。
3. 針對 Actions (動作)，選擇 Create alarm (建立警示)。Create alarm (建立警示) 頁面隨即出現。

4. 遵循頁面說明以進行操作。
5. 選擇 Create alarm (建立警示)。

使用叢集效能資料

在主控台中，您可以透過叢集詳細資訊頁面的叢集效能索引標籤來使用叢集效能資料。

使用 AWS CLI 和 Amazon Redshift API 管理叢集

您可以使用下列 AWS CLI 操作來管理 Amazon Redshift 中的叢集。

- [cancel-resize](#)
- [create-cluster](#)
- [delete-cluster](#)
- [describe-clusters](#)
- [describe-cluster-versions](#)
- [describe-node-configuration-options](#)
- [describe-orderable-cluster-options](#)
- [describe-resize](#)
- [modify-cluster](#)
- [pause-cluster](#)
- [reboot-cluster](#)
- [resize-cluster](#)
- [resume-cluster](#)

您可以使用下列 Amazon Redshift API 操作來管理叢集。

- [CancelResize](#)
- [CreateCluster](#)
- [DeleteCluster](#)
- [DescribeClusters](#)
- [DescribeCluster版本](#)

- [DescribeNodeConfigurationOptions](#)
- [DescribeResize](#)
- [DescribeOrderableClusterOptions](#)
- [ModifyCluster](#)
- [PauseCluster](#)
- [RebootCluster](#)
- [ResizeCluster](#)
- [ResumeCluster](#)

管理 VPC 中的叢集

主題

- [概觀](#)
- [在 VPC 中建立叢集](#)
- [管理叢集的 VPC 安全群組](#)
- [設 Amazon Redshift 叢集或 Amazon Redshift Serverless 工作群組的安全群組通訊設定](#)
- [Amazon Redshift 如何使用 VPC 共享資源 AWS](#)
- [Amazon Redshift 叢集子網路群組](#)

概觀

Amazon Redshift 支援使用 EC2-VPC 和 EC2-Classic 平台，在以 Amazon VPC 服務為基礎的虛擬私有雲端 (VPC) 中啟動叢集。如需詳細資訊，請參閱 [在建立叢集時使用 EC2-VPC](#)。

Note

Amazon Redshift 不支援將叢集啟動至專用租用 VPC。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的 [專用執行個體](#)。

在 VPC 中佈建叢集時，您需要執行下列動作：

- 提供 VPC 資訊。

當您要求 Amazon Redshift 在 VPC 中建立叢集時，您必須建立叢集子網路群組以提供 VPC 資訊。此資訊包括 VPC ID 和 VPC 中的子網路清單。當您啟動叢集時，需要提供叢集子網路群組，讓 Amazon Redshift 可以在 VPC 裡的一個子網路中佈建您的叢集。如需在 Amazon Redshift 中建立子網路群組的相關資訊，請參閱 [Amazon Redshift 叢集子網路群組](#)。如需設定 VPC 的相關資訊，請參閱《Amazon VPC 入門指南》中的 [Amazon VPC 入門](#)。

- 選擇性設定可公開存取選項。

如果您將叢集設定為可公開存取，Amazon Redshift 會針對外部 IP 地址使用彈性 IP 地址。彈性 IP 地址是靜態 IP 地址。其可讓您變更基礎組態，而不會影響用戶端用於連線到叢集的 IP 地址。這個方法對於諸如故障後復原等情況很有幫助。是否建立彈性 IP 地址取決於您的可用區域重新定位設定。有兩個選項：

1. 如果您已開啟可用區域重新定位，且想要啟用公開存取，則不要指定彈性 IP 地址。系統會指派由 Amazon Redshift 管理的彈性 IP 地址。它與您的 AWS 帳戶相關聯。
2. 如果您已關閉可用區域重新定位，且想要啟用公開存取，則可以在啟動 Amazon Redshift 叢集之前，選擇在 Amazon EC2 中為 VPC 建立彈性 IP 地址。如果您不建立 IP 地址，Amazon Redshift 會提供已設定的彈性 IP 地址以用於 VPC。這個彈性 IP 地址是由 Amazon Redshift 管理，不會與您的 AWS 帳戶相關聯。

如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的 [彈性 IP 地址](#)。

在某些情況下，您的 VPC 中可能有可公開存取的叢集，而您想要從 VPC 內使用私有 IP 地址與之連線。若是如此，請將下列 VPC 參數設定為 true：

- DNS resolution
- DNS hostnames

假設您的 VPC 中有可公開存取的叢集，但未在 VPC 中將這些參數設定為 true。在這些情況下，從 VPC 內部建立的連線會解析為叢集的彈性 IP 地址，而不是私有 IP 地址。建議您在從 VPC 內部連線時，將這些參數設為 true，並讓可公開存取的叢集使用私有 IP 地址。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的 [將 DNS 用於您的 VPC](#)。

Note

如果您的 VPC 中有可公開存取的現有叢集，來自 VPC 內部的連線會繼續使用彈性 IP 地址來連線至叢集，直到您調整叢集大小為止。即使已設定上述參數，也會發生此情況。任何新叢集皆會遵守新的行為，也就是在從相同 VPC 內部連線至可公開存取的叢集時，使用私有 IP 地址。

彈性 IP 地址是用來存取 VPC 外部叢集的外部 IP 地址。其與顯示在 Amazon Redshift 主控台連線詳細資訊底下的叢集節點公有 IP 地址和私有 IP 地址無關。不論叢集是不是可公開存取，都會出現公有和私有叢集節點 IP 地址。這些地址只能用於在特定情況下設定遠端主機上的傳入規則。當您從 Amazon EC2 執行個體或其他使用安全殼層 (SSH) 連線的遠端主機載入資料時，就會發生這些情況。如需詳細資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的[步驟 1：擷取叢集公有金鑰和叢集節點 IP 地址](#)。

您可以在建立叢集或從快照還原叢集時，選擇將叢集和彈性 IP 地址相關聯。在某些情況下，您可能想要將叢集與彈性 IP 地址相關聯，或是變更與叢集相關聯的彈性 IP 地址。若要在建立叢集後連接彈性 IP 地址，請先更新叢集，使其無法公開存取，然後將其同時設為可公開存取，並在同一個操作中新增靜態 IP 地址。

- 與 VPC 安全群組建立關聯

然後，您要使用 VPC 安全群組授予傳入存取。此 VPC 安全群組必須允許透過叢集的資料庫連接埠進行存取，這樣您才可以使用 SQL 用戶端工具進行連線。您可以事先進行這項設定，或在啟動叢集後新增規則。如需詳細資訊，請參閱[設定 Amazon Redshift 叢集的安全群組通訊設定](#)，其中會提供在用戶端與佈建叢集或 Amazon Redshift Serverless 工作群組之間設定傳入和傳出規則的指引。另一個可協助您了解安全群組的資源是《Amazon VPC 使用者指南》中的[VPC 中的安全](#)。請注意，您不能使用 Amazon Redshift 叢集安全群組授予對叢集的傳入存取。

如需在 VPC 中使用叢集的相關資訊，請參閱[在 VPC 中建立叢集](#)。

還原 VPC 中叢集的快照

VPC 中叢集的快照只能在 VPC 中還原，不能在 VPC 外還原。您可以在相同 VPC 中還原，或在帳戶的其他 VPC 中還原。如需快照的相關資訊，請參閱[Amazon Redshift 快照和備份](#)。

在 VPC 中建立叢集

以下是在虛擬私有雲端 (VPC) 中部署叢集的一般步驟。

在 VPC 中建立叢集

1. 設定 VPC。

您可以在帳戶的預設 VPC 中建立叢集 (如果帳戶有預設 VPC)，或是在您已建立的 VPC 中建立叢集。如需詳細資訊，請參閱[在建立叢集時使用 EC2-VPC](#)。若要建立 VPC，請參閱《Amazon

VPC 使用者指南》中的[建立 VPC](#)。請記下 VPC 識別碼、子網路和子網路的可用區域。當您啟動叢集時需要此資訊。

Note

您至少必須在 VPC 中定義一個子網路，才能在下一個步驟將其新增至叢集子網路群組。如需在您的 VPC 中新增子網路的相關資訊，請參閱《Amazon VPC 使用者指南》中的[在您的 VPC 中新增子網路](#)。

2. 建立 Amazon Redshift 叢集子網路群組，以指定您的 Amazon Redshift 叢集可用於 VPC 的子網路。

您可以使用 Amazon Redshift 主控台或以程式設計的方式建立叢集子網路群組。如需詳細資訊，請參閱 [Amazon Redshift 叢集子網路群組](#)。

3. 在您將與叢集相關聯的 VPC 安全群組中，授權傳入連線的存取權。

您可以允許 VPC 外部的用戶端 (在公有網際網路上) 連線至叢集。若要執行此作業，請將叢集與 VPC 安全群組相關聯，以授權啟動叢集時所用連接埠的傳入存取權。如需安全群組規則的範例，請參閱《Amazon VPC 使用者指南》中的[安全群組規則](#)。

4. 請遵循亞 [Amazon Redshift 佈建叢集](#) 中的步驟，建立叢集。請在建立叢集時進行下列修改：
 - 若要顯示 Additional configurations (其他組態) 區段，請關閉 Use defaults (使用預設值)。
 - 在 Network and security (網路與安全) 區段中，指定您所設定的 Virtual private cloud (VPC) (虛擬私有雲端 (VPC))、Cluster subnet group (叢集子網路群組) 和 VPC security group (VPC 安全群組)。

您現在已經可以使用叢集。您可以遵循「入門」中的步驟，上傳範例資料並執行範例查詢來測試叢集。

管理叢集的 VPC 安全群組

當您佈建 Amazon Redshift 叢集時，依預設它會遭鎖定，以便沒有人可以存取它。若要授予其他使用者 Amazon Redshift 叢集的傳入存取，您可使叢集與安全群組建立關聯。如果您是在 EC2-VPC 平台上，則可以使用現有的 Amazon VPC 安全群組，或定義新的安全群組。然後，您可以將其與叢集相關聯，如下所述。如果您是在 EC2-Classical 平台上，則可以定義叢集安全群組，並使它與叢集建立關聯。如需在 EC2-Classical 平台上使用叢集安全群組的相關資訊，請參閱 [Amazon Redshift 叢集安全群組](#)。

VPC 安全群組包含一組規則，用來控制對 VPC 上執行個體 (例如您的叢集) 的存取。個別規則設定存取是依據 IP 地址的範圍或依據其他 VPC 安全群組。當您將 VPC 安全群組與叢集建立關聯時，VPC 安全群組中定義的規則即會控制對叢集的存取。

您在 EC2-VPC 平台上佈建的每個叢集都有一個或多個 Amazon VPC 安全群組與其相關聯。Amazon VPC 會提供名為預設的 VPC 安全群組，系統會在您建立 VPC 時自動建立此群組。若您未在建立叢集時指定其他 VPC 安全群組，您在 VPC 中啟動的每個叢集都會自動與預設 VPC 安全群組建立關聯。您可以在建立叢集時將 VPC 安全群組與叢集建立關聯，也可以在稍後修改叢集，將 VPC 安全群組與其建立關聯。

下表說明預設 VPC 安全群組的預設規則。

Inbound			
Source	Protocol	Port Range	Comments
The security group ID (sg-xxxxxxx)	All	All	Allow inbound traffic from instances assigned to the same security group
Outbound			
Destination	Protocol	Port Range	Comments
0.0.0.0/0	All	All	Allow all outbound traffic

您可以依 Amazon Redshift 叢集的需要，變更預設 VPC 安全群組的規則。

如果預設 VPC 安全群組夠您使用，則您無需再建立更多 VPC 安全群組。不過，您可以選擇性地建立額外的 VPC 安全群組，以妥善管理叢集的傳入存取。例如，假設您是在 Amazon Redshift 叢集上執行服務，而且為您的客戶提供幾個不同的服務層級。如果不想讓所有服務層級具有相同的存取，則您可能需要建立個別的 VPC 安全群組，每個服務層級一個。然後，您可將這些 VPC 安全群組與您的叢集建立關聯。

您可以為 VPC 建立多達 100 個 VPC 安全群組，且可以將 VPC 安全群組與多個叢集相關聯。不過，一個指定的叢集最多只能與五個 VPC 安全群組相關聯。

Amazon Redshift 會立即套用對 VPC 安全群組所做的變更。因此，如果您已將 VPC 安全群組與叢集建立關聯，則已更新之 VPC 安全群組中的傳入叢集存取規則會立即套用。

您可以在 <https://console.aws.amazon.com/vpc/> 建立和修改 VPC 安全群組。您也可以使用 AWS CLI、Amazon EC2 CLI 和 AWS Tools for Windows PowerShell 如需使用 VPC 安全群組的相關資訊，請參閱《Amazon VPC 使用者指南》中的 [VPC 的安全群組](#)。

設 Amazon Redshift 叢集或 Amazon Redshift Serverless 工作群組的安全群組通訊設定

本主題可協助您設定安全群組，以適當地路由和接收網路流量。幾個常見的使用案例如下：

- 您開啟 Amazon Redshift 叢集或 Amazon Redshift Serverless 工作群組的公開存取性，但其未接收流量。為此，您必須設定傳入規則，以允許流量從網際網路抵達該項目。
- 您的叢集或工作群組無法公開存取，而且您使用 Redshift 預先設定的預設 VPC 安全群組來允許傳入流量。但是您必須使用預設安全群組以外的安全群組，而且這個自訂安全群組不允許傳入流量。您必須將其設定為允許通訊。

下列各節可協助您為每個使用案例選擇正確的回應，並向您說明如何根據您的要求來設定網路流量。您可以選擇性地使用這些步驟來設定來自其他私有安全群組的通訊。

Note

大多數情況下，系統不會在 Amazon Redshift 中自動設定網路流量設定。這是因為這些設定在精細層級上可能會有所不同 (具體取決於流量來源是網際網路還是私有安全群組)，以及因為安全要求有所不同。

具有預設或自訂安全群組組態的公開存取性

如果您要建立叢集或工作群組，或您已經有叢集或工作群組，請執行下列組態步驟，以將其設為可公開存取。當您選擇預設安全群組或自訂安全群組時，都請這麼做：

1. 尋找網路設定：
 - 對於 Amazon Redshift 佈建叢集，請選擇屬性索引標籤，然後在網路和安全設定下選取叢集的 VPC。
 - 對於 Amazon Redshift Serverless 工作群組，請選擇工作群組組態。從清單中選擇工作群組。然後，在資料存取下的網路和安全面板中，選擇編輯。
2. 設定 VPC 的網際網路閘道和路由表。您可以透過依名稱選擇 VPC 來啟動組態。其會開啟 VPC 儀表板。若要從網際網路連線到可公開存取的叢集或工作群組，就必須將網際網路閘道附加至路由表。您可以透過在 VPC 儀表板中選擇路由表來進行此設定。確認已為網際網路閘道的目標設定來源 0.0.0.0/0 或公開 IP CIDR。路由表必須與叢集所在的 VPC 相關聯。如需為 VPC 設定網際網路存取的相關資訊 (如此處所述)，請參閱 Amazon VPC 文件中的[啟用網際網路存取](#)。如需設定路由表的相關資訊，請參閱[設定路由表](#)。
3. 在設定網際網路閘道和路由表之後，請返回 Redshift 的網路設定。透過先選擇安全群組，再選擇傳入規則來開啟傳入存取。選擇 Edit inbound Rules (編輯傳入規則)。

4. 根據您的要求，為一或多個傳入規則選擇通訊協定和連接埠，以允許來自用戶端的流量。若為 RA3 叢集，請選取 5431-5455 或 8191-8215 範圍內的連接埠。完成時，請儲存每個規則。
5. 編輯可公開存取設定來加以啟用。您可以從叢集或工作群組的動作功能表執行此操作。

當您開啟可公開存取設定時，Redshift 會建立彈性 IP 地址。這是與您的帳戶相關聯的靜態 IP 位 AWS 址。在 VPC 外的用戶端可以使用此地址進行連線。

如需設定安全群組的相關資訊，請參閱 [Amazon Redshift 叢集安全群組](#)。

您可以透過與用戶端連線來測試規則，如果您要連線到 Amazon Redshift Serverless，請執行以下操作。完成網路組態後，請與您的用戶端工具連線，例如 [Amazon Redshift RSQL](#)。使用您的 Amazon Redshift Serverless 網域作為主機，輸入以下內容：

```
rsql -h workgroup-name.account-id.region.amazonaws.com -U admin -d dev -p 5439
```

具有預設或自訂安全群組組態的私有存取性

如果在與叢集或工作群組通訊時未透過網際網路，這種方式便稱為可私有存取。如果您在建立安全群組時選擇了預設安全群組，安全群組中便會包含下列預設通訊規則：

- 一個傳入規則，允許指派給安全群組的所有資源所傳來的流量。
- 一個傳出規則，允許所有傳出流量。此規則的目的地是 0.0.0.0/0。在無類別域間路由 (CIDR) 標記法中，其代表所有可能的 IP 地址。

您可以透過選取叢集或工作群組的安全群組，在主控台中檢視規則。

如果您的叢集或工作群組和用戶端都使用預設安全群組，則不需要設定任何額外的組態來允許網路流量。但是，如果您刪除或變更 Redshift 或用戶端的預設安全群組中的任何規則，此做法就不再適用。在此情況下，您必須設定規則以允許傳入和傳出通訊。常見的安全群組組態如下：

- 針對用戶端 Amazon EC2 執行個體：
 - 傳入規則，允許用戶端的 IP 地址。
 - 傳出規則，允許針對 Redshift 用途所提供之所有子網路的 IP 地址範圍 (CIDR 區塊)。或者，您也可以指定 0.0.0.0/0，這是所有 IP 地址範圍。
- 針對您的 Redshift 叢集或工作群組：
 - 傳入規則，允許用戶端安全群組。

- 傳出規則，允許流向 0.0.0.0/0 的流量。一般來說，傳出規則會允許所有傳出流量。您可以選擇性地新增傳出規則，允許流量流向用戶端安全群組。在這個選擇性案例中，不一定要有傳出規則，因為每個請求的回應流量都可以抵達執行個體。如需有關請求和回應行為的詳細資訊，請參閱《Amazon VPC 使用者指南》中的[安全群組](#)。

如果您變更針對 Redshift 用途指定的任何子網路或安全群組的組態，則可能需要相應地變更流量規則，以確保通訊能持續開啟。如需建立傳入和傳出規則的相關資訊，請參閱《Amazon VPC 使用者指南》中的[VPC CIDR 區塊](#)。如需從用戶端連線至 Amazon Redshift 的相關資訊，請參閱在[Amazon Redshift 中設定連線](#)。

Amazon Redshift 如何使用 VPC 共享資源 AWS

VPC 共用可讓您在共用、集中管理的虛擬私有雲 (VPC) 中建立 AWS 應用程式資源，例如 Amazon EC2 執行個體和其他 AWS 服務。擁有 VPC (擁有者) 的帳戶與屬於同一組織的其他帳戶 (參與者) 共用一或多個子網路。AWS 本文描述如何在共用 VPC 中建立和使用 Amazon Redshift 叢集或 Amazon Redshift Serverless 工作群組。

VPC 共用的好處包括您不必管理那麼多 VPC，而且它還可以協助您簡化網路。對於 Amazon Redshift 管理員和使用者來說，優點則是 Redshift 資源可以在共用的 VPC 中以高效率的方式運作。如需 VPC 共用的相關資訊，請參閱[與其他帳戶共用 VPC](#)，其中會詳細介紹 VPC 共用的優點及其運作方式。

如何在共用 VPC 中使用 Amazon Redshift 資料倉儲資源

首先，請務必了解共用子網路中的參與者無法看到 Amazon Redshift 叢集或 Amazon Redshift Serverless 工作群組。但這並不會讓參與者無法在共用 VPC 中使用擁有者的資料庫。下面的步驟中會更詳細地說明這一點。

在共用 VPC 中建立 Amazon Redshift 佈建叢集之前，您必須先建立要用於 Amazon Redshift 的子網路群組。這應該包括您要使用的共用 VPC 中的子網路。在建立 Amazon Redshift 叢集時，您必須選擇這個子網路，並且還要指定共用 VPC 的安全群組。同樣地，在建立 Amazon Redshift Serverless 工作群組和資料庫時，也必須指定共用子網路和您在共用 VPC 中建立的安全群組。在設定子網路後，請執行下列步驟以在共用環境中設定 Redshift 資源：

1. VPC 擁有者會使用共用 VPC 中的子網路建立 Amazon Redshift 叢集或 Amazon Redshift Serverless 工作群組。
2. VPC 擁有者可讓叢集或工作群組在跨 VPC 案例中使用。相關步驟的描述請見在[Amazon Redshift 中使用 Redshift 受管的 VPC 端點](#) (若為佈建叢集) 或從[Amazon Redshift 受管 VPC 端點連線至](#)

[Amazon Redshift Serverless](#) (若為 Amazon Redshift Serverless)。藉由啟用跨 VPC 可用性，他們可以讓相同 AWS 帳戶或其他帳戶中的使用者可以使用資料庫。

- 相反地，透過 VPC 共用的方式，擁有者可以與參與者共用子網路，而且參與者可以在子網路中建立 Amazon Redshift 叢集或 Amazon Redshift Serverless 工作群組。但是，在這種情況下，擁有者無法檢視參與者所建立的 Amazon Redshift 資源。您必須透過與以上步驟所述的相同方式啟用跨 VPC 可用性，讓叢集或工作群組可供存取。

在共用 VPC 中使用 Amazon Redshift 資源的使用須知

請注意下列有關在共用子網路中使用 Amazon Redshift 的行為：

- 如上一節所述，VPC 擁有者無法透過 VPC 共用與參與者共用 Amazon Redshift 叢集或 Amazon Redshift Serverless 工作群組。但參與者可以在擁有者的子網路中建立叢集或 Amazon Redshift Serverless 工作群組。在這種情況下，擁有者無法透過 VPC 共用看到 Amazon Redshift。
- VPC 擁有者無法檢視、更新或刪除參與者在共用子網路中建立的 Amazon Redshift 佈建叢集或 Amazon Redshift Serverless 工作群組。
- 沒有可用的許可，因此其他 AWS 帳戶可以存取您在共用 VPC 中建立的 Amazon Redshift 資源。

Amazon Redshift 叢集子網路群組

概觀

如果要在虛擬私有雲端 (VPC) 中佈建叢集，需建立叢集子網路群組。如需 VPC 的相關資訊，請參閱 [Amazon VPC](#) 產品的詳細資訊頁面。

您的 VPC 可以有一個以上的子網路 (VPC 內 IP 地址組成的子網路)，讓您可以根據安全和操作的需要將資源分組。叢集子網路群組可讓您指定 VPC 中的子網路集合。佈建叢集時，您提供子網路群組，Amazon Redshift 便可以在群組的其中一個子網路中佈建叢集。

如需建立 VPC 的相關資訊，請前往 [Amazon VPC 使用者指南](#) 文件。

在建立子網路群組後，便可以移除先前新增的子網路或新增更多子網路。Amazon Redshift 會提供 API 操作供您建立、修改或刪除叢集子網路群組。您也可以在主控台中執行這些操作。

使用主控台管理叢集子網路群組

您可使用 Amazon Redshift 主控台管理叢集子網路群組。您可以建立叢集子網路群組、管理現有的群組，或刪除群組。這些作業都是從叢集的子網路群組清單開始。您必須選取要管理的叢集子網路群組。

您可在其中一個提供子網路群組的子網路中佈建叢集。叢集子網路群組可讓您指定 Virtual Private Cloud (VPC) 中的子網路集合。

建立叢集子網路群組

您至少必須定義一個叢集子網路群組，才能在 VPC 中佈建叢集。

建立叢集子網路群組

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽功能表上，選擇組態，然後選擇子網路群組。子網路群組清單即會出現。
3. 選擇 Create cluster subnet group (建立叢集子網路群組) 以顯示建立頁面。
4. 輸入子網路群組的資訊，包括要新增的子網路。
5. 選擇 Create cluster subnet group (建立叢集子網路群組)，使用您選擇的子網路建立群組。

修改叢集子網路群組

修改叢集子網路群組

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽功能表上，選擇組態，然後選擇子網路群組。子網路群組清單即會出現。
3. 選擇要修改的子網路群組。
4. 針對 Actions (動作)，選擇 Modify (修改) 以顯示子網路群組的詳細資訊。
5. 更新子網路群組的資訊。
6. 選擇 Save (儲存) 以修改群組。

若要在某些情況下變更或移除子網路，您需要進行額外的步驟。例如，本 AWS 知識中心文章：[如何將佈建的 Amazon Redshift 叢集移至不同的子網路？](#)，說明涵蓋移動叢集的使用案例。

刪除叢集子網路群組

您無法刪除叢集正在使用的叢集子網路群組。

刪除叢集子網路群組

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽功能表上，選擇組態，然後選擇子網路群組。子網路群組清單即會出現。
3. 選擇要刪除的子網路群組，再選擇 Delete (刪除)。

使用 AWS CLI 和 Amazon Redshift API 管理叢集子網路群組

您可以使用下列 Amazon Redshift CLI 操作來管理叢集子網路群組。

- [create-cluster-subnet-group](#)
- [delete-cluster-subnet-group](#)
- [describe-cluster-subnet-groups](#)
- [modify-cluster-subnet-group](#)

您可以使用下列 Amazon Redshift API 操作來管理叢集子網路群組。

- [CreateClusterSubnetGroup](#)
- [DeleteClusterSubnetGroup](#)
- [DescribeClusterSubnetGroups](#)
- [ModifyClusterSubnetGroup](#)

叢集版本歷史記錄

Amazon Redshift 會定期發行用來更新叢集的新叢集版本。

Important

如需有關可用 Amazon Redshift 叢集版本及其功能、改善和修正的資訊，請參閱 [適用於 Amazon Redshift 的叢集版本](#)。

使用零 ETL 整合

本主題包含與 Amazon Redshift 的 Aurora PostgreSQL 和 RDS for MySQL 零 ETL 整合的發行前版本文件(預覽版本)。文件和功能會隨時變更。建議僅在測試環境中使用 RDS for MySQL 和 Aurora PostgreSQL 零 ETL 整合，不要在生產環境中使用。如需預覽版條款和條件，請參閱 [AWS 服務條款](#) 中的 Beta 版和預覽版。

零 ETL 整合是可在 Amazon Redshift 中以近乎即時的速度提供交易或操作資料的全受管解決方案。透過這個解決方案，您可以設定從您的來源到 Amazon Redshift 資料倉儲的整合。您不需要維護擷取、轉換和載入 (ETL) 管道。我們會為您處理 ETL，方法是自動建立和管理將資料從資料來源複寫到 Amazon Redshift 叢集或 Redshift Serverless 命名空間的複寫操作。您可以繼續更新和查詢來源資料，同時使用 Amazon Redshift 來處理分析工作負載，例如報告和儀表板。

透過零 ETL 整合，您可以獲得更新的分析、AI/ML 和報告資料。您可以針對即時儀表板、最佳化遊戲體驗、資料品質監控和客戶行為分析等使用案例獲得更準確、及時的洞察。您可以更有信心地進行數據驅動的預測，改善客戶體驗，並在整個業務中推廣數據驅動的洞察。

零 ETL 整合目前支援下列來源：

- Aurora MySQL-Compatible Edition
- Amazon PostgreSQL-Compatible Edition (預覽版)
- RDS for MySQL (預覽版)

若要建立零 ETL 整合，您必須指定整合來源，並指定 Amazon Redshift 資料倉儲做為目標。這項整合會將來源資料倉儲中的資料複寫到目標資料倉儲。在幾秒鐘內，資料便能在 Amazon Redshift 中使用。整合會監控資料管道的運作狀態，並在可能的情況下從問題中復原。您可以建立從相同類型的來源至單一 Amazon Redshift 資料倉儲的整合，以便跨多個應用程式衍生整體洞察。

使用 Amazon Redshift 中的資料，您可以使用 Amazon Redshift 提供的分析。例如，內建機器學習 (ML)、具體化視觀表、資料共用，以及直接存取多個資料存放區和資料湖。零 ETL 整合可讓您的運算資源與資料資源隔離，讓您可以使用最有效的工具來處理資料。對於資料工程師而言，零 ETL 整合可讓您存取可能會因複雜的資料管道中所發生的間歇性錯誤而遭到延遲的時效性資料。您可以在交易資料上執行分析查詢和 ML 模型，以針對時效性事件和商業決策衍生近乎即時的洞察。

您可以建立 Amazon Redshift 事件通知訂閱，因此，當指定的零 ETL 整合發生事件時，您可以收到通知。。若要檢視與整合相關的事件通知清單，請參閱 [透過 Amazon 進行零 ETL 整合事件通知](#)

[EventBridge](#)。建立訂閱最簡單的方式是使用 Amazon SNS 主控台。如需建立和訂閱 Amazon SNS 主題的詳細資訊，請參閱《Amazon Simple Notification Service 開發人員指南》中的 [Amazon SNS 入門](#)。

當您開始使用零 ETL 整合時，請考慮下列概念：

- 來源資料庫是將其資料複製到 Amazon Redshift 的資料庫。
- 目標資料倉儲是資料複製到的 Amazon Redshift 佈建的叢集或 Redshift Serverless 工作群組。
- 目的地資料庫是您從目標資料倉儲中的零 ETL 整合建立的資料庫。

您也可以透過在 Amazon Redshift 中查詢下列系統檢視來監控零 ETL 整合。

- [SVV_INTEGRATION](#) 會提供零 ETL 整合之組態詳細資訊的相關資訊。
- [SYS_INTEGRATION_ACTIVITY](#) 會提供已完成之零 ETL 整合的相關資訊。
- [SVV_INTEGRATION_TABLE_STATE](#) 會提供整合狀態的相關資訊。
- [SY_整合_表狀態_變更](#) 提供有關整合的資料表狀態變更記錄檔的資訊。

如需零 ETL 整合的定價資訊，請參閱適當的定價頁面：

- [Amazon Redshift 定價](#)
- [Amazon Aurora 定價](#)
- [Amazon RDS 定價](#)

如需有關零 ETL 整合來源的詳細資訊，請參閱下列主題：

- 如需 Aurora 零 ETL 整合的詳細資訊，請參閱 Amazon Aurora 使用者指南中的零 ETL 整合的 [優點](#)、[重要概念](#)、[限制](#)、[配額](#) 和 [支援的區域](#)。
- 如需 RDS 零 ETL 整合，請參閱 Amazon RDS 使用者指南中的零 ETL 整合的 [優點](#)、[重要概念](#)、[限制](#)、[配額](#) 和 [支援的區域](#)。

主題

- [將零 ETL 整合與 Amazon Redshift 搭配使用的考量](#)
- [開始使用零 ETL 整合](#)
- [在 Amazon Redshift 中建立目的地資料庫](#)
- [以複製的資料查詢和建立具體化視觀表](#)

- [管理零 ETL 整合](#)
- [零 ETL 整合的指標](#)
- [對零 ETL 整合進行疑難排解](#)

將零 ETL 整合與 Amazon Redshift 搭配使用的考量

以下考量適用於 Amazon Redshift 的零 ETL 整合。

- 您的目標 Amazon Redshift 資料倉儲必須符合下列先決條件：
 - 執行 Amazon Redshift Serverless 或 RA3 節點類型 (ra3.16xlarge、ra3.4xlarge 和 ra3.xlplus)。
 - 已加密 (如果使用已佈建的叢集)。
 - 已啟用區分大小寫。
- 您無法在已設定整合的資料倉儲上啟用增強型 VPC 支援。
- 如果您刪除來源，而該來源是 Amazon Redshift 資料倉儲的授權整合來源，則所有相關聯的整合都會進入 FAILED 狀態。
- 目的地資料庫是唯讀的。您無法在目的地資料庫中建立資料表、視觀表或具體化視觀表。不過，您可以在目標資料倉儲中的其他資料表上使用具體化視觀表。
- 具體化視觀表在用於跨資料庫查詢時才會得到支援。使用從 Zero-ETL 整合複製的資料重新整理具體化視觀表，會導致檢視的完整重新整理。不支援累加式重新整理、自動查詢重新寫入、自動重新整理及自動具體化視觀表。如需使用透過零 ETL 整合複製之資料來建立具體化視觀表的相關資訊，請參閱 [以複製的資料建立具體化視觀表](#)。
- 您只能查詢目標資料倉儲中處於 Synced 狀態的資料表。如需詳細資訊，請參閱 [零 ETL 整合的指標](#)。
- Amazon Redshift 只接受 UTF-8 字元，因此可能不遵守您的來源中定義的定序。排序和比較規則可能會有所不同，這最後可能會變更查詢結果。
- Amazon Redshift VARCHAR 數據類型的最大長度為 65,535 字節。當來源的內容不符合此限制時，將不會繼續複製，且表格會進入失敗狀態。如需零 ETL 整合來源和 Amazon Redshift 資料庫之間資料類型差異的詳細資訊，請參閱亞馬遜 Aurora 使用者指南中的 [Aurora 和 Amazon Redshift 之間的資料類型差異](#)。
- 整合來源中的資料表必須具有主索引鍵。否則，您的資料表無法複製到 Amazon Redshift 中的目標資料倉儲。
- 對於 Amazon Redshift 的 Aurora PostgreSQL 和 RDS for MySQL 零 ETL 整合，請在預覽版中建立您的目標資料倉儲。如需詳細資訊，請參閱 [建立和設定目標 Amazon Redshift 資料倉儲](#)。

- 零 ETL 整合在將資料從交易資料存放區複製到 Amazon Redshift 時，不支援轉換。資料會從來源資料庫中依原樣複製。不過，您可以在 Amazon Redshift 中對複製的資料套用轉換。
- 可能會對在 Amazon Redshift 中執行的其他工作負載造成影響。若要消除零 ETL 整合對其他工作負載的影響，請考慮使用單獨的端點進行零 ETL 整合，並與需要使用資料共用存取此資料的其他端點共用資料。
- 零 ETL 整合可使用並行連線在 Amazon Redshift 中執行。它會使用從整合建立資料庫的使用者認證來執行。執行查詢時，並行擴展不會在同步 (寫入) 期間啟動這些連線。並行擴展讀取 (來自 Amazon Redshift 用戶端) 適用於同步物件。

如需也同樣適用於整合來源的考量，請參閱下列其中一個主題：

- 如需 Aurora 來源，請參閱 Amazon Aurora 使用者指南中的[限制](#)。
- 對於 Amazon RDS 來源，請參閱 Amazon RDS 使用者指南中的[限制](#)。

開始使用零 ETL 整合

在 Amazon Redshift 上設定零 ETL 整合之前，請設定您的整合來源組態，然後使用必要的參數和權限進行設定。然後，從 Amazon Redshift 控制台繼續進行初始設置的其餘部分。AWS CLI

建立與 Amazon Redshift 的 Aurora 零 ETL 整合

若要建立與 Amazon Redshift 的 Aurora 零 ETL 整合，請執行下列動作：

1. 如 Amazon Aurora 使用者指南所述，從 Amazon RDS 主控台[建立自訂資料庫叢集參數群組](#)。
2. 如 Amazon Aurora 使用者指南所述，從 Amazon RDS 主控台[建立來源 Amazon Aurora 資料庫叢集](#)。
3. 從 Amazon Redshift 主控台：[建立和設定目標 Amazon Redshift 資料倉儲](#)。
 - 從 AWS CLI 或 Amazon Redshift 控制台：[為資料倉儲開啟區分大小寫功能](#)。
 - 從 Amazon Redshift 主控台：[設定 Amazon Redshift 資料倉儲的授權](#)。
4. 如 Amazon Aurora 使用者指南中所述，從 Amazon RDS 主控台[建立零 ETL 整合](#)。
5. 從 Amazon Redshift 主控台或查詢編輯器 v2，[從您的整合建立 Amazon Redshift 資料庫](#)。

然後，[查詢並建立具有複製資料的具體化視觀表](#)。

建立與 Amazon Redshift 的 RDS 零 ETL 整合

若要建立與 Amazon Redshift 的 RDS 零 ETL 整合，請執行下列動作：

1. 如 Amazon RDS 使用者指南所述，從 Amazon RDS 主控台 [建立自訂資料庫參數群組](#)。
2. 如 Amazon Aurora 使用者指南所述，從 Amazon RDS 主控台 [建立來源 Amazon RDS 執行個體](#)。
3. 從 Amazon Redshift 主控台：[建立和設定目標 Amazon Redshift 資料倉儲](#)。
 - 從 AWS CLI 或 Amazon Redshift 控制台：[為資料倉儲開啟區分大小寫功能](#)。
 - 從 Amazon Redshift 主控台：[設定 Amazon Redshift 資料倉儲的授權](#)。
4. 如 Amazon RDS 使用者指南所述，從 Amazon RDS 主控台 [建立零 ETL 整合](#)。
5. 從 Amazon Redshift 主控台或查詢編輯器 v2，[從您的整合建立 Amazon Redshift 資料庫](#)。

然後，[查詢並建立具有複製資料的具體化視觀表](#)。

Amazon RDS 主控台提供 step-by-step 整合建立流程，您可以在其中指定來源資料庫和目標 Amazon Redshift 資料倉儲。如果發生問題，您可以選擇讓 Amazon RDS 為您修正問題，而不必在 Amazon RDS 或 Amazon Redshift 主控台上手動修復問題。

建立和設定目標 Amazon Redshift 資料倉儲

在此步驟之前，先建立整合來源，並設定 零 ETL 整合的來源類型所需的參數。

在這個步驟中，您會建立和設定目標 Amazon Redshift 資料倉儲，例如 Redshift Serverless 工作群組或佈建叢集。

您的目標資料倉儲必須有下列特性：

- 執行 Amazon Redshift Serverless 或執行個體類型為 ra3.16xlarge、ra3.4xlarge 或 ra3.xlplus 的佈建叢集。
- 已開啟區分大小寫功能 (enable_case_sensitive_identifier)。如需詳細資訊，請參閱 [為資料倉儲開啟區分大小寫功能](#)。
- 加密 (如果您的目標資料倉儲是 Amazon Redshift 佈建叢集的話)。如需詳細資訊，請參閱 [Amazon Redshift 資料庫加密](#)。
- 在與整合來源相同的 AWS 區域中建立。

Note

對於搭配 Amazon Redshift 的 Aurora PostgreSQL 和 RDS for MySQL 零 ETL 整合，也針對您的目標資料倉儲考慮下列事項：

- 您必須在 preview_2023 追蹤上的預覽中建立資料倉儲。您無法在生產環境中使用預覽功能，也無法將預覽資料倉儲移至生產部署。
- 如果您選擇建立 Amazon Redshift 佈建的叢集，則該叢集至少必須有兩個節點。
- 對於 Aurora PostgreSQL 來源，您必須在美國東部 (俄亥俄) AWS 區域建立目標資料倉儲。請注意，您必須使用 [Amazon RDS 資料庫預覽環境](#) 為 Aurora PostgreSQL 零 ETL 整合建立來源資料庫。

對於適用於 MySQL 的 RDS 來源，您必須在支援的 AWS 區域中建立目標資料倉儲。如需可使用 RDS for MySQL 零 ETL 整合的 AWS 區域清單，請參閱 Amazon RDS 使用者指南中的 [支援與 Amazon Redshift 進行零 ETL 整合的區域](#)。

若要在預覽版中為您的 Aurora PostgreSQL 和 RDS for MySQL 零 ETL 整合建立目標資料倉儲，請參閱下列其中一個主題，具體取決於您的部署類型：

- 若要建立預覽 Amazon Redshift 佈建的叢集，請參閱 [建立預覽叢集](#)。確保您選擇的 preview_2023 追蹤，以便使用零 ETL 整合。
- 若要建立預覽版 Amazon Redshift Serverless 工作群組，請參閱 [建立預覽工作群組](#)。

若要為您的 Aurora MySQL 零 ETL 整合建立目標資料倉儲，請參閱下列其中一個主題，具體取決於您的部署類型：

- 若要建立 Amazon Redshift 佈建的叢集，請參閱 [建立叢集](#)。
- 若要建立含命名空間的 Amazon Redshift Serverless 工作群組，請參閱 [使用命名空間建立工作群組](#)。

當您建立佈建叢集時，Amazon Redshift 也會建立預設參數群組。您無法編輯預設參數群組。但是，您可以在建立新叢集之前先建立自訂參數群組，然後將其與叢集建立關聯。或者，您可以編輯將與建立的叢集相關聯的參數群組。在建立自訂參數群組時，或在編輯目前的參數群組以使用零 ETL 整合時，也必須為參數群組開啟區分大小寫功能。

您可以使用 Amazon Redshift 主控台建立自訂參數群組，也可以使用下列方式建立自訂參數群組：
AWS CLI

- 使用 Amazon Redshift 主控台 — [使用主控台來管理參數群組](#)
- 使用 AWS CLI — [使用 AWS CLI 和 Amazon Redshift API 管理參數群組](#)

為資料倉儲開啟區分大小寫功能

您可以附加參數群組，並在建立期間啟用已佈建叢集的區分大小寫。但是，您只能在建立無伺服器工作群組之後，透過 AWS Command Line Interface (AWS CLI) 更新該工作群組。必須這麼做才能支援 MySQL 和 PostgreSQL 的區分大小寫功能。enable_case_sensitive_identifier 是決定資料庫、資料表和資料欄的名稱識別符是否區分大小寫的組態值。必須開啟這個參數才能在資料倉儲中建立零 ETL 整合。如需詳細資訊，請參閱 [enable_case_sensitive_identifier](#)。

若為 Amazon Redshift Serverless — [開啟亞馬遜無伺服器的區分大小寫 AWS CLI](#)。請注意，您只能從 AWS CLI 為 Amazon Redshift Serverless 開啟區分大小寫功能。

對於 Amazon Redshift 佈建的叢集，請使用下列其中一個主題為目標叢集啟用區分大小寫：

- [使用 Amazon Redshift 主控台為 Amazon Redshift 佈建叢集開啟區分大小寫功能](#)
- [開啟 Amazon Redshift 佈建叢集的區分大小寫，使用 AWS CLI](#)

開啟亞馬遜無伺服器的區分大小寫 AWS CLI

執行下列 AWS CLI 命令以開啟工作群組的區分大小寫。

```
aws redshift-serverless update-workgroup \  
    --workgroup-name target-workgroup \  
    --config-parameters  
    parameterKey=enable_case_sensitive_identifier,parameterValue=true
```

等待工作群組的狀態變為 Active 後，再繼續進行下一個步驟。

使用 Amazon Redshift 主控台為 Amazon Redshift 佈建叢集開啟區分大小寫功能

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在左側導覽窗格中，選擇佈建叢集儀表板。
3. 選擇您要將資料複製到其中的佈建叢集。
4. 在左側導覽窗格中，選擇組態 > 工作負載管理。
5. 在工作負載管理頁面上，選擇參數群組。
6. 選擇參數索引標籤。

7. 選擇編輯參數，然後將 `enable_case_sensitive_identifier` 變更為 `true`。
8. 然後選擇 Save (儲存)。

開啟 Amazon Redshift 佈建叢集的區分大小寫，使用 AWS CLI

1. 由於您無法編輯預設參數群組，因此請從終端機程式執行下列 AWS CLI 命令以建立自訂參數群組。稍後，您會為其與已佈建的叢集建立關聯。

```
aws redshift create-cluster-parameter-group \  
  --parameter-group-name zero-etl-params \  
  --parameter-group-family redshift-1.0 \  
  --description "Param group for zero-ETL integrations"
```

2. 執行下列 AWS CLI 命令以開啟參數群組的區分大小寫。

```
aws redshift modify-cluster-parameter-group \  
  --parameter-group-name zero-etl-params \  
  --parameters ParameterName=enable_case_sensitive_identifier,ParameterValue=true
```

3. 執行以下命令將參數群組與叢集相關聯。

```
aws redshift modify-cluster \  
  --cluster-identifier target-cluster \  
  --cluster-parameter-group-name zero-etl-params
```

4. 等待佈建叢集變為可用狀態。您可以使用 `describe-cluster` 命令檢查叢集的狀態。然後，執行以下命令重新啟動叢集。

```
aws redshift reboot-cluster \  
  --cluster-identifier target-cluster
```

設定 Amazon Redshift 資料倉儲的授權

若要將資料從整合來源複寫到您的 Amazon Redshift 資料倉儲，您最初必須新增下列兩個實體：

- 授權主體 — 識別可在資料倉儲中建立零 ETL 整合的使用者或角色。
- 授權的整合來源 — 識別可更新資料倉儲的來源資料庫。

您可以從 Amazon Redshift 主控台上的資源政策索引標籤或使用 Amazon Redshift PutResourcePolicy API 作業，設定授權的整合來源。

新增授權主體

若要在 Redshift Serverless 工作群組或佈建叢集中建立零 ETL 整合，請授權相關聯命名空間或佈建叢集的存取權。

如果下列兩個情況都成立，則可以略過此步驟：

- 擁 AWS 帳戶 有 Redshift 無伺服器工作群組或佈建叢集的擁有者也擁有來源資料庫。
- 該主體與以身分為基礎的 IAM 政策相關聯，且具有可在此 Redshift Serverless 命名空間或佈建叢集中建立零 ETL 整合的許可。

將授權主體新增至 Amazon Redshift Serverless 命名空間

1. 在 Amazon Redshift 主控台中，從左側導覽窗格中選擇 Redshift Serverless。
2. 選擇命名空間組態，然後選擇您的命名空間，然後移至資源政策索引標籤。
3. 選擇新增授權主體。
4. 針對您要新增的每個授權主體，輸入命名空間的 AWS 使用者或角色的 ARN，或 AWS 帳戶 是您要授與存取權以建立 Zero-ETL 整合的 ID。帳戶 ID 會儲存為 ARN。
5. 選擇儲存變更。

將授權主體新增至 Amazon Redshift 佈建叢集

1. 在 Amazon Redshift 主控台的左側導覽窗格中，選擇佈建叢集儀表板。
2. 選擇叢集，然後選擇叢集，接著前往資源政策索引標籤。
3. 選擇新增授權主體。
4. 針對您要新增的每個授權主體，輸入叢集中的 AWS 使用者或角色的 ARN，或您要授與存取權 AWS 帳戶 以建立 Zero-ETL 整合的 ID。帳戶 ID 會儲存為 ARN。
5. 選擇儲存變更。

新增授權的整合來源

若要允許來源更新 Amazon Redshift 資料倉儲，您必須以授權的整合來源的形式將其新增至命名空間。

將授權的整合來源新增至 Amazon Redshift Serverless 命名空間

1. 在 Amazon Redshift 主控台中，前往 無伺服器儀表板。
2. 選擇命名空間的名稱。
3. 前往資源政策索引標籤。
4. 選擇新增授權的整合來源。
5. 針對零 ETL 整合指定來源的 ARN。

Note

移除授權的整合來源會讓系統不再將資料複製至命名空間。此動作會停用從該來源到此命名空間的所有零 ETL 整合。

將授權的整合來源新增至 Amazon Redshift 佈建叢集

1. 在 Amazon Redshift 主控台中，前往佈建叢集儀表板。
2. 選擇佈建叢集的名稱。
3. 前往資源政策索引標籤。
4. 選擇新增授權的整合來源。
5. 指定屬於零 ETL 整合資料來源之來源的 ARN。

Note

移除授權的整合來源會讓系統不再將資料複製至佈建叢集。此動作會停用從該來源到此 Amazon Redshift 佈建叢集的所有零 ETL 整合。

使用 Amazon Redshift API 設定授權

您可以使用 Amazon Redshift API 操作來設定與零 ETL 整合搭配使用的資源政策。

若要控制可以在命名空間中建立傳入整合的來源，請建立資源政策，並將其附加至命名空間。使用資源政策，您可以指定具有整合存取權的來源。資源政策會附加至目標資料倉儲的命名空間，以允許來源建立傳入整合，將即時資料從來源複製到 Amazon Redshift。

以下是範例資源政策。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "redshift.amazonaws.com"
      },
      "Action": "redshift:AuthorizeInboundIntegration",
      "Condition": {
        "StringEquals": {
          "aws:SourceArn": "source_arn"
        }
      }
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "source_principal"
      },
      "Action": "redshift:CreateInboundIntegration"
    }
  ]
}
```

以下概述了適用於設定整合資源政策的 Amazon Redshift API 操作：

- 使用 [PutResource策略](#) API 作業來保留資源策略。當您提供其他資源政策時，會取代資源上先前的資源政策。使用上一個範本資源政策，該策略會授予下列動作的許可：
 - CreateInboundIntegration – 允許來源主體建立輸入整合，以便將資料從來源複製到目標資料倉儲。
 - AuthorizeInboundIntegration – 允許 Amazon Redshift 持續驗證目標資料倉儲是否可以接收從來源 ARN 複製的資料。
- 使用 [GetResource策略](#) API 操作是查看現有的資源策略。
- 使用 [DeleteResource策略](#) API 作業可從資源中移除資源策略。

若要更新資源策略，您也可以使用 [put-resource-policy](#) AWS CLI 命令。

後續步驟

現在，您已設定好目標 Amazon Redshift 資料倉儲的授權，接下來您可以建立零 ETL 整合並開始複寫資料。

根據您的來源，執行以下其中一項操作：

- 若要建立 Aurora 零 ETL 整合，請參閱 Amazon Aurora 使用者指南中的[使用 Amazon Redshift 建立 Amazon Aurora 零 ETL 整合](#)。
- 若要建立 RDS 零 ETL 整合，請參閱 Amazon Aurora 使用者指南中的[使用 Amazon Redshift 建立 Amazon RDS 零 ETL 整合](#)。

在 Amazon Redshift 中建立目的地資料庫

若要將資料從來源複製到 Amazon Redshift，您必須從 Amazon Redshift 中的整合建立資料庫。

請連線至您的目標 Redshift Serverless 工作群組或佈建叢集，並建立參考整合識別符的資料庫。此識別碼是當您查詢 [SVV_INTEGRATION](#) 檢視時針對 integration_id 所傳回的值。

Important

在從您的整合建立資料庫之前，您必須先在 Amazon RDS 或 Amazon Redshift 主控台上建立零 ETL 整合，並處於 Active 狀態。

在 Amazon Redshift 中建立目的地資料庫

在將資料從來源複製到 Amazon Redshift 之前，您必須從 Amazon Redshift 中的整合建立資料庫。您可以使用 Amazon Redshift 主控台或查詢編輯器 v2 來建立資料庫。

使用 Amazon Redshift 主控台建立目的地資料庫

1. 在左側導覽窗格中，選擇零 ETL 整合。
2. 從整合清單中選擇整合。
3. 如果您要使用佈建叢集，則必須先連線至資料庫。選擇 Connect to database (連接至資料庫)。您可以透過使用最近的連線或建立新連線來進行連線。
4. 若要從整合建立資料庫，請選擇從整合建立資料庫。

5. 輸入資料庫名稱。整合 ID 和資料倉儲名稱會預先填入。

對於 Aurora PostgreSQL 來源，也請輸入您在建立零 ETL 整合時指定的具名資料庫。

6. 選擇建立資料庫。

使用查詢編輯器 v2 建立目的地資料庫

1. 導覽至 Amazon Redshift 主控台，然後選擇查詢編輯器 v2。
2. 在左側面板中選擇 Amazon Redshift Serverless 工作群組或 Amazon Redshift 佈建叢集，然後與其連線。
3. 若要取得整合 ID，請導覽至 Amazon Redshift 主控台上的整合清單。

或者，執行下列命令來取得 `integration_id` 值：

```
SELECT integration_id FROM SVV_INTEGRATION;
```

4. 然後，執行下列命令以建立資料庫。透過指定整合 ID，您可以在資料庫與來源之間建立連線。

以上一個命令傳回的值替代 `integration_id`。

```
CREATE DATABASE destination_db_name FROM INTEGRATION 'integration_id';
```

對於 Aurora PostgreSQL 來源，您還必須在建立整合時指定的叢集中包含具名資料庫的參考。例如：

```
CREATE DATABASE destination_db_name FROM INTEGRATION 'integration_id'  
DATABASE named_db;
```

Note

只有您的整合來源可以更新您從整合建立的資料庫中的資料。若要變更資料表的結構定義，請針對來源中的資料表執行 DDL 或 DML 命令。您可以針對來源中的資料表執行 DDL 和 DML 命令，但您只能在目的地資料庫上執行 DDL 命令和唯讀查詢。

如需檢視目的地資料庫狀態的相關資訊，請參閱 [管理零 ETL 整合](#)。

新增資料至來源

在建立目的地資料庫後，您可以將資料新增至來源。若要將資料新增至來源，請參閱下列其中一個主題：

- 對於 Aurora 來源，請參閱 Amazon Aurora 使用者指南中的[將資料新增至來源資料庫叢集](#)。
- 對於 Amazon RDS 來源，請參閱 Amazon RDS 使用者指南中的[將資料新增到來源資料庫執行個體](#)。

以複寫的資料查詢和建立具體化視觀表

在 Amazon Redshift 中查詢複寫的資料

在將資料新增到來源後，資料會近乎即時地複寫到 Amazon Redshift 資料倉儲，並且可供查詢。如需有關整合指標和表格統計資訊的資訊，請參閱[零 ETL 整合的指標](#)。

Note

由於資料庫與 MySQL 中的結構描述相同，因此 MySQL 資料庫層級會映射至 Amazon Redshift 結構描述層級。當您查詢從 Amazon Aurora MySQL 或 RDS for MySQL 複寫過來的資料時，請注意這個映射上的差異。

查詢複製的資料

1. 導覽至 Amazon Redshift 主控台，然後選擇查詢編輯器 v2。
2. 連線至您的 Amazon Redshift Serverless 工作群組或 Amazon Redshift 佈建叢集，然後從下拉式清單中選擇您的資料庫。
3. 使用 SELECT 陳述式從您在來源中建立的結構描述和資料表選取所有資料：如需區分大小寫，請針對結構描述、資料表和資料欄名稱使用雙引號 (" ")。例如：

```
SELECT * FROM "schema_name"."table_name";
```

您也可以使用 Amazon Redshift CLI 來查詢資料。

以複寫的資料建立具體化視觀表

您可以在本機 Amazon Redshift 資料庫中建立具體化視觀表，以轉換透過零 ETL 整合所複寫的資料。請連線至本機資料庫，並使用跨資料庫查詢來存取目的地資料庫。您可以使用由三個部分組成的標記法 (destination-database-name.schema-name.table-name) 所表示的完整物件名稱，或建立參考目的地資料庫結構描述配對的外部結構描述，並使用由兩個部分組成的標記法 (external-schema-name.table-name)。如需跨資料庫查詢的相關資訊，請參閱[跨資料庫查詢資料](#)。

使用下列範例，從來源 *ticket_zetl* 建立範例資料，並將其插入至 *sales_zetl* 和 *event_zetl* 資料表。這兩個資料表會複寫到 Amazon Redshift 資料庫 *zetl_int_db*。

```
CREATE TABLE sales_zetl (
    salesid integer NOT NULL primary key,
    eventid integer NOT NULL,
    pricepaid decimal(8, 2)
);

CREATE TABLE event_zetl (
    eventid integer NOT NULL PRIMARY KEY,
    eventname varchar(200)
);

INSERT INTO sales_zetl VALUES(1, 1, 3.33);
INSERT INTO sales_zetl VALUES(2, 2, 4.44);
INSERT INTO sales_zetl VALUES(3, 2, 5.55);

INSERT INTO event_zetl VALUES(1, "Event 1");
INSERT INTO event_zetl VALUES(2, "Event 2");
```

您可以使用由三個部分組成的標記法建立具體化視觀表，以取得每個活動的總銷售額：

```
--three part notation zetl-database-name.schema-name.table-name
CREATE MATERIALIZED VIEW mv_transformed_sales_per_event_3p as
(SELECT eventname, sum(pricepaid) as total_price
FROM zetl_int_db.ticket_zetl.sales_zetl S, zetl_int_db.ticket_zetl.event_zetl E
WHERE S.eventid = E.eventid
GROUP BY 1);
```

您可以使用由兩個部分組成的標記法建立具體化視觀表，以取得每個活動的總銷售額：

```
--two part notation external-schema-name.table-name notation
CREATE EXTERNAL schema ext_ticket_zetl
```

```

FROM REDSHIFT
DATABASE zetl_int_db
SCHEMA tickit_zetl;

CREATE MATERIALIZED VIEW mv_transformed_sales_per_event_2p
AS
(
    SELECT eventname, sum(pricepaid) as total_price
    FROM   ext_tickit_zetl.sales_zetl S, ext_tickit_zetl.event_zetl E
    WHERE  S.eventid = E.eventid
    GROUP BY 1
);

```

若要檢視您建立的具體化視觀表，請使用下列範例。

```
SELECT * FROM mv_transformed_sales_per_event_3p;
```

```

+-----+-----+
| eventname | total_price |
+-----+-----+
| Event 1   | 3.33        |
| Event 2   | 9.99        |
+-----+-----+

```

```
SELECT * FROM mv_transformed_sales_per_event_2p;
```

```

+-----+-----+
| eventname | total_price |
+-----+-----+
| Event 1   | 3.33        |
| Event 2   | 9.99        |
+-----+-----+

```

管理零 ETL 整合

您可以在 Amazon Redshift 主控台上檢視零 ETL 整合的詳細資訊，以查看其組態資訊和狀態。

檢視零 ETL 整合的詳細資訊

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 從左側導覽窗格選擇無伺服器或佈建叢集儀表板。然後，選擇零 ETL 整合。

3. 選取您要檢視的零 ETL 整合。針對每個整合，系統會提供以下資訊：

- 整合 ID 是建立整合時傳回的識別碼。
- 狀態可以是下列其中之一：
 - Active— 零 ETL 整合會將交易資料傳送到目標 Amazon Redshift 資料倉儲。
 - Syncing— 零 ETL 整合發生可復原的錯誤，並正在重新植入資料。在完成重新同步之前，受影響的資料表無法在 Amazon Redshift 中進行查詢。
 - Failed— 零 ETL 整合遇到無法修正的無法復原的事件或錯誤。您必須刪除並重新建立零 ETL 整合。
 - Creating— 正在建立零 ETL 整合。
 - Deleting— 正在刪除零 ETL 整合。
 - Needs attention— 零 ETL 整合發生事件或錯誤，需要手動介入才能解決此問題。若要修正問題，請遵循錯誤訊息中的步驟。
- 來源 ARN 是來源資料的 ARN。
- 目的地是目標資料倉儲命名空間的 ARN。
- 資料庫可以是下列其中之一：
 - No database — 沒有用於整合的目的地資料庫。
 - Creating — Amazon Redshift 正在建立用於整合的目的地資料庫。
 - Active – 正在將資料從整合來源複製到 Amazon Redshift。
 - Error — 整合發生錯誤。
 - Recovering — 重新啟動資料倉儲後，整合正在復原。
 - Resyncing — Amazon Redshift 正在重新同步整合中的資料表。
- 目的地類型是 Amazon Redshift 資料倉儲的類型。
- 建立日期是建立整合時的日期和時間 (UTC)。

Note

若要檢視資料倉儲的整合詳細資訊，請選擇已佈建叢集或無伺服器命名空間的詳細資料頁面，然後選擇 Zero-ETL 整合索引標籤。

用雙引號括住結構描述、資料表和資料欄的名稱 ("`<name>`"). 如需在 Amazon Redshift 資料倉儲中查詢資料的相關資訊，請參閱[使用 Amazon Redshift 查詢編輯器 v2 來查詢資料庫](#)。

從零 ETL 整合清單中，您可以選擇共用資料以建立資料共用。遵循建立資料共用頁面上的指示，為 Amazon Redshift 資料庫建立資料共用。您必須先建立目的地資料庫，才能在 Amazon Redshift 資料庫中共用資料。如需資料共用的詳細資訊，請參閱[Amazon Redshift 的資料共用概念](#)。

若要重新整理整合，您可以使用 `ALTER DATABASE` 命令。這樣做會將整合來源中的所有資料複寫到目的地資料庫中。下列範例會重新整理零 ETL 整合中所有已同步處理和失敗的資料表。

```
ALTER DATABASE sample_integration_db INTEGRATION REFRESH ALL tables;
```

在 Amazon Redshift 中共用資料

在您將資料新增到來源之後，資料會立即複寫到 Amazon Redshift，並可透過建立資料共用來共用。

您必須先建立目的地資料庫才能共用資料。

Important

若要將來自 Amazon Redshift 預覽資料倉儲的資料分享至 Amazon Redshift 取用者資料倉儲，您的取用者資料倉儲必須在 `preview_2023` 軌跡上。如需有關資料共用的詳細資訊，請參閱 Amazon Redshift 資料庫開發人員指南中的[什麼是資料共用？](#)。

若要建立預覽版的目標資料倉儲，請根據您的部署類型，參閱下列其中一個主題：

- Amazon Redshift 佈建的叢集 – [建立預覽叢集](#)
- Redshift Serverless 工作群組 – [建立預覽工作群組](#)

使用 Amazon Redshift 主控台在 Amazon Redshift Serverless 中共用資料

1. 在 Amazon Redshift 主控台的左側導覽窗格中，選擇 Amazon Redshift Serverless > 無伺服器儀表板。
2. 從左側導覽窗格中，選擇零 ETL 整合。
3. 選擇 Share data (共用資料)。
4. 在建立資料共用頁面上，依照[建立資料共用](#)中的步驟執行。

使用 Amazon Redshift 主控台在 Amazon Redshift 佈建叢集中共用資料

1. 在 Amazon Redshift 主控台的左側導覽窗格中，選擇佈建叢集儀表板。
2. 從左側導覽窗格中，選擇零 ETL 整合。
3. 從整合清單中選擇整合。
4. 在整合詳細資訊頁面上，選擇連線至資料庫。
5. 在連線至資料庫頁面上，您可以建立新連線或使用最近的連線。請確定您已向目的地資料庫建立連線。
6. 如果您建立新的連線，請輸入資料庫的資料庫名稱。然後，按一下連線。
7. 在整合詳細資料頁面上，選擇共用資料。
8. 在建立資料共用頁面上，依照[建立資料共用](#)中的步驟執行。

零 ETL 整合的指標

您可以使用 Amazon Redshift 主控台和 Amazon 中的指標 CloudWatch 來了解零 ETL 整合的運作狀態和效能。您可以調整量度以顯示較短或更長持續時間的資料，或選擇在中檢視量度 CloudWatch。若要在 Amazon Redshift 主控台上檢視整合的指標，請在左側導覽窗格中選擇零 ETL 整合，然後選擇您的整合 ID。

對於 Aurora 和 Amazon RDS 零 ETL 整合，Amazon Redshift 會在整合詳細資料頁面上提供兩種類型的指標，以進行整合。指標類型如下所示：

- 從整合指標索引標籤中，可用的圖表如下：

指標	描述
Lag	<p>從資料遞交到您的來源的時間，到資料可供在 Amazon Redshift 中查詢的時間兩者之間的延遲。</p> <p>單位：秒</p> <p>維度：IntegrationLag</p>
Tables replicated	<p>已從來源資料庫複寫到 Amazon Redshift 的資料表數量。</p> <p>單位：計數</p>

指標	描述
	維度：IntegrationNumTablesReplicated
Tables failed	複寫失敗的資料表數量。
	單位：計數
	維度：IntegrationNumTablesFailedReplication

- 您可以從表格統計資訊索引標籤檢視目前作用中或發生錯誤的表格清單。此標籤上的統計資料如下所示：
 - 結構描述名稱 — 資料表所在的結構描述名稱。
 - 資料表名稱 — 來源資料庫中的資料表名稱。
 - 狀態 — 資料表的狀態。可能的值包括 Synced、Failed、Deleted、Resync Required 及 Resync Initiated。
 - 資料庫 — 資料表所在的 Amazon Redshift 資料庫。
 - 上次更新 — 上次對資料表進行更新的日期和時間 (UTC)。

對零 ETL 整合進行疑難排解

針對 Aurora MySQL 的零 ETL 整合進行故障診斷

使用下列資訊，針對 Aurora MySQL 的零 ETL 整合常見問題進行故障診斷。

主題

- [整合建立失敗](#)
- [資料表沒有主索引鍵](#)
- [資料表中有不支援的資料類型](#)
- [資料操作語言命令失敗](#)
- [資料來源之間的追蹤變更不相符](#)
- [授權失敗](#)
- [資料表數量超過 10 萬個或結構描述數量超過 4950 個](#)
- [Amazon Redshift 無法載入資料](#)
- [工作群組參數的設定不正確](#)

- [未建立資料庫來啟用零 ETL 整合](#)
- [資料表處於需要重新同步處理或重新同步處理已起始狀態](#)

整合建立失敗

如果零 ETL 整合建立失敗，則整合的狀態為 Inactive。請確定您的 Aurora 資料庫叢集符合下列敘述：

- 您已在 Amazon RDS 主控台中建立叢集。
- 您的來源 Aurora 資料庫叢集執行 MySQL 3.05 或更新版本。若要驗證此問題，請前往叢集的組態索引標籤，然後檢查引擎版本。
- 您已正確設定叢集的 binlog 參數設定。如果您的 Aurora MySQL binlog 參數未正確設定或未與來源 Aurora 資料庫叢集相關聯，則建立會失敗。請參閱[設定資料庫叢集參數](#)。

此外，請確定您的 Amazon Redshift 資料倉儲符合下列敘述：

- 已開啟區分大小寫功能。請參閱[為資料倉儲開啟區分大小寫功能](#)。
- 您已為命名空間新增正確的授權主體和整合來源。請參閱[設定 Amazon Redshift 資料倉儲的授權](#)。

資料表沒有主索引鍵

在目的地資料庫中，一或多個資料表沒有主索引鍵，因此無法同步。

若要解決此問題，請前往整合詳細資訊頁面上的表格統計資訊索引標籤，或使用 SVV_INTEGRATION_TABLE_STATE 來檢視失敗的資料表。您可以在資料表中新增主索引鍵，Amazon Redshift 便會重新同步資料表。或者，雖不建議，但您也可以捨棄 Aurora 上的這些資料表，並建立有主索引鍵的資料表。如需詳細資訊，請參閱[Amazon Redshift 的資料表設計最佳實務](#)。

資料表中有不支援的資料類型

在您從 Amazon Redshift 整合建立的資料庫中，以及從 Aurora 資料庫叢集複寫資料的目的地資料庫中，一或多個資料表有不支援的資料類型，因此無法同步。

若要解決此問題，請前往整合詳細資訊頁面上的表格統計資訊索引標籤，或使用 SVV_INTEGRATION_TABLE_STATE 來檢視失敗的資料表。然後，移除這些資料表，並在 Amazon RDS 上重新建立新的資料表。如需有關不受支援資料類型的詳細資訊，請參閱 Amazon Aurora 使用者指南中的[Aurora 和 Amazon Redshift 資料庫之間的資料類型差異](#)。

資料操作語言命令失敗

Amazon Redshift 無法在 Redshift 資料表上執行 DML 命令。若要解決此問題，請使用 `SVV_INTEGRATION_TABLE_STATE` 檢視失敗的資料表。Amazon Redshift 會自動重新同步資料表以解決此錯誤。

資料來源之間的追蹤變更不相符

當 Amazon Aurora 與 Amazon Redshift 之間的變更不相符，導致整合進入 Failed 狀態時，就會發生此錯誤。

若要解決此錯誤，請刪除零 ETL 整合，然後在 Amazon RDS 中重新建立整合。如需詳細資訊，請參閱 [建立零 ETL 整合](#) 和 [刪除零 ETL 整合](#)。

授權失敗

授權失敗，因為做為 Amazon Redshift 資料倉儲授權整合來源的來源 Aurora 資料庫叢集已遭到移除。

若要解決此錯誤，請刪除零 ETL 整合，然後在 Amazon RDS 上重新建立整合。如需詳細資訊，請參閱 [建立零 ETL 整合](#) 和 [刪除零 ETL 整合](#)。

資料表數量超過 10 萬個或結構描述數量超過 4950 個

對於目的地資料倉儲，資料表的數量超過 10 萬個或結構描述的數量超過 4950 個。Amazon Aurora 無法將資料傳送到 Amazon Redshift。資料表和結構描述的數量超過所設定的限制。若要解決此問題，請從來源資料庫中移除任何不必要的結構描述或資料表。

Amazon Redshift 無法載入資料

Amazon Redshift 無法將資料載入到零 ETL 整合。

若要解決此問題，請刪除 Amazon RDS 上的零 ETL 整合，然後重新建立整合。如需詳細資訊，請參閱 [建立零 ETL 整合](#) 和 [刪除零 ETL 整合](#)。

工作群組參數的設定不正確

您的工作群組未開啟區分大小寫功能。

若要解決此問題，請前往整合詳細資訊頁面上的屬性索引標籤、選擇參數群組，然後從屬性索引標籤開啟區分大小寫的識別碼。如果您沒有現有的參數群組，請建立一個已開啟區分大小寫識別碼的參數群組。然後，在 Amazon RDS 上建立新的零 ETL 整合。如需詳細資訊，請參閱 [建立零 ETL 整合](#)。

未建立資料庫來啟用零 ETL 整合

沒有建立可供零 ETL 整合來啟用的資料庫。

若要解決此問題，請為整合建立資料庫。如需詳細資訊，請參閱 [在 Amazon Redshift 中建立目的地資料庫](#)。

資料表處於需要重新同步處理或重新同步處理已起始狀態

您的資料表處於需要重新同步處理或重新同步處理已起始狀態。

若要收集有關資料表為何處於該狀態的更詳細錯誤資訊，請使用 [SYS_LOAD_ERROR_DETAIL](#) 系統檢視。

針對與 Aurora PostgreSQL 的零 ETL 整合進行故障診斷

使用下列資訊，針對 Aurora PostgreSQL 的零 ETL 整合常見問題進行故障診斷。

主題

- [整合建立失敗](#)
- [資料表沒有主索引鍵](#)
- [資料表中有不支援的資料類型](#)
- [資料操作語言命令失敗](#)
- [資料來源之間的追蹤變更不相符](#)
- [授權失敗](#)
- [資料表數量超過 10 萬個或結構描述數量超過 4950 個](#)
- [Amazon Redshift 無法載入資料](#)
- [工作群組參數的設定不正確](#)
- [未建立資料庫來啟用零 ETL 整合](#)
- [資料表處於需要重新同步處理或重新同步處理已起始狀態](#)

整合建立失敗

如果零 ETL 整合建立失敗，則整合的狀態為 Inactive。請確定您的 Aurora 資料庫叢集符合下列敘述：

- 您已在 Amazon RDS 主控台中建立叢集。

- 您的來源 Aurora 資料庫叢集執行 Aurora PostgreSQL 15.4.99 版或更高版本。若要驗證此問題，請前往叢集的組態索引標籤，然後檢查引擎版本。
- 您已正確設定叢集的 binlog 參數設定。如果您的 Aurora PostgreSQL binlog 參數未正確設定或未與來源 Aurora 資料庫叢集相關聯，則建立會失敗。請參閱[設定資料庫叢集參數](#)。

此外，請確定您的 Amazon Redshift 資料倉儲符合下列敘述：

- 已開啟區分大小寫功能。請參閱[為資料倉儲開啟區分大小寫功能](#)。
- 您已新增正確的授權主體和整合來源的終端項目 = 「使用 .redshift-iam.title」 />。

資料表沒有主索引鍵

在目的地資料庫中，一或多個資料表沒有主索引鍵，因此無法同步。

若要解決此問題，請前往整合詳細資訊頁面上的表格統計資訊索引標籤，或使用 SVV_INTEGRATION_TABLE_STATE 來檢視失敗的資料表。您可以在資料表中新增主索引鍵，Amazon Redshift 便會重新同步資料表。或者，雖不建議，但您也可以捨棄 Aurora 上的這些資料表，並建立有主索引鍵的資料表。如需詳細資訊，請參閱[Amazon Redshift 的資料表設計最佳實務](#)。

資料表中有不支援的資料類型

在您從 Amazon Redshift 整合建立的資料庫中，以及從 Aurora 資料庫叢集複寫資料的目的地資料庫中，一或多個資料表有不支援的資料類型，因此無法同步。

若要解決此問題，請前往整合詳細資訊頁面上的表格統計資訊索引標籤，或使用 SVV_INTEGRATION_TABLE_STATE 來檢視失敗的資料表。然後，移除這些資料表，並在 Amazon RDS 上重新建立新的資料表。如需有關不受支援資料類型的詳細資訊，請參閱 Amazon Aurora 使用者指南中的[Aurora 和 Amazon Redshift 資料庫之間的資料類型差異](#)。

資料操作語言命令失敗

Amazon Redshift 無法在 Redshift 資料表上執行 DML 命令。若要解決此問題，請使用 SVV_INTEGRATION_TABLE_STATE 檢視失敗的資料表。Amazon Redshift 會自動重新同步資料表以解決此錯誤。

資料來源之間的追蹤變更不相符

當 Amazon Aurora 與 Amazon Redshift 之間的變更不相符，導致整合進入 Failed 狀態時，就會發生此錯誤。

若要解決此錯誤，請刪除零 ETL 整合，然後在 Amazon RDS 中重新建立整合。如需詳細資訊，請參閱[建立零 ETL 整合](#)和[刪除零 ETL 整合](#)。

授權失敗

授權失敗，因為做為 Amazon Redshift 資料倉儲授權整合來源的來源 Aurora 資料庫叢集已遭到移除。

若要解決此錯誤，請刪除零 ETL 整合，然後在 Amazon RDS 上重新建立整合。如需詳細資訊，請參閱[建立零 ETL 整合](#)和[刪除零 ETL 整合](#)。

資料表數量超過 10 萬個或結構描述數量超過 4950 個

對於目的地資料倉儲，資料表的數量超過 10 萬個或結構描述的數量超過 4950 個。Amazon Aurora 無法將資料傳送到 Amazon Redshift。資料表和結構描述的數量超過所設定的限制。若要解決此問題，請從來源資料庫中移除任何不必要的結構描述或資料表。

Amazon Redshift 無法載入資料

Amazon Redshift 無法將資料載入到零 ETL 整合。

若要解決此問題，請刪除 Amazon RDS 上的零 ETL 整合，然後重新建立整合。如需詳細資訊，請參閱[建立零 ETL 整合](#)和[刪除零 ETL 整合](#)。

工作群組參數的設定不正確

您的工作群組未開啟區分大小寫功能。

若要解決此問題，請前往整合詳細資訊頁面上的屬性索引標籤、選擇參數群組，然後從屬性索引標籤開啟區分大小寫的識別碼。如果您沒有現有的參數群組，請建立一個已開啟區分大小寫識別碼的參數群組。然後，在 Amazon RDS 上建立新的零 ETL 整合。如需詳細資訊，請參閱[建立零 ETL 整合](#)。

未建立資料庫來啟用零 ETL 整合

沒有建立可供零 ETL 整合來啟用的資料庫。

若要解決此問題，請為整合建立資料庫。如需詳細資訊，請參閱[在 Amazon Redshift 中建立目的地資料庫](#)。

資料表處於需要重新同步處理或重新同步處理已起始狀態

您的資料表處於需要重新同步處理或重新同步處理已起始狀態。

若要收集有關資料表為何處於該狀態的更詳細錯誤資訊，請使用 [SYS_LOAD_ERROR_DETAIL](#) 系統檢視。

針對 RDS for MySQL 的零 ETL 整合進行故障診斷

使用下列資訊，針對與 RDS for MySQL 的零 ETL 整合常見問題進行故障診斷。

主題

- [整合建立失敗](#)
- [資料表沒有主索引鍵](#)
- [資料表中有不支援的資料類型](#)
- [資料操作語言命令失敗](#)
- [資料來源之間的追蹤變更不相符](#)
- [授權失敗](#)
- [資料表數量超過 10 萬個或結構描述數量超過 4950 個](#)
- [Amazon Redshift 無法載入資料](#)
- [工作群組參數的設定不正確](#)
- [未建立資料庫來啟用零 ETL 整合](#)
- [資料表處於需要重新同步處理或重新同步處理已起始狀態](#)

整合建立失敗

如果零 ETL 整合建立失敗，則整合的狀態為 Inactive。請確定您的來源 RDS DB 執行個體符合下列敘述：

- 您已在 Amazon RDS 主控台中建立執行個體。
- 您的來源 RDS 資料庫執行個體正在執行適用於 MySQL 的 RDS 版本 8.0.32 或更新版本。若要驗證此問題，請前往執行個體的組態索引標籤，然後檢查引擎版本。
- 您已正確設定執行個體的 binlog 參數設定。如果您的 RDS for MySQL binlog 參數未正確設定或未與來源 RDS 資料庫執行個體相關聯，則建立會失敗。請參閱[設定資料庫執行個體參數](#)。

此外，請確定您的 Amazon Redshift 資料倉儲符合下列敘述：

- 已開啟區分大小寫功能。請參閱[為資料倉儲開啟區分大小寫功能](#)。
- 您已為命名空間新增正確的授權主體和整合來源。請參閱[設定 Amazon Redshift 資料倉儲的授權](#)。

資料表沒有主索引鍵

在目的地資料庫中，一或多個資料表沒有主索引鍵，因此無法同步。

若要解決此問題，請前往整合詳細資訊頁面上的表格統計資訊索引標籤，或使用 `SVV_INTEGRATION_TABLE_STATE` 來檢視失敗的資料表。您可以在資料表中新增主索引鍵，Amazon Redshift 便會重新同步資料表。或者，雖不建議，但您也可以捨棄 RDS 上的這些資料表，並建立有主索引鍵的資料表。如需詳細資訊，請參閱 [Amazon Redshift 的資料表設計最佳實務](#)。

資料表中有不支援的資料類型

在您於 Amazon Redshift 建立的目的地資料庫中，以及從 RDS 資料庫執行個體複寫資料的目的地資料庫中，一或多個資料表有不支援的資料類型，因此無法同步。

若要解決此問題，請前往整合詳細資訊頁面上的表格統計資訊索引標籤，或使用 `SVV_INTEGRATION_TABLE_STATE` 來檢視失敗的資料表。然後，移除這些資料表，並在 Amazon RDS 上重新建立新的資料表。如需有關不受支援資料類型的詳細資訊，請參閱 Amazon RDS 使用者指南中的 [RDS 和 Amazon Redshift 資料庫之間的資料類型差異](#)。

資料操作語言命令失敗

Amazon Redshift 無法在 Redshift 資料表上執行 DML 命令。若要解決此問題，請使用 `SVV_INTEGRATION_TABLE_STATE` 檢視失敗的資料表。Amazon Redshift 會自動重新同步資料表以解決此錯誤。

資料來源之間的追蹤變更不相符

當 Amazon Aurora 與 Amazon Redshift 之間的變更不相符，導致整合進入 Failed 狀態時，就會發生此錯誤。

若要解決此錯誤，請刪除零 ETL 整合，然後在 Amazon RDS 中重新建立整合。如需詳細資訊，請參閱 [建立零 ETL 整合](#) 和 [刪除零 ETL 整合](#)。

授權失敗

授權失敗，因為做為 Amazon Redshift 資料倉儲授權整合來源的來源 RDS 資料庫執行個體已遭到移除。

若要解決此錯誤，請刪除零 ETL 整合，然後在 Amazon RDS 上重新建立整合。如需詳細資訊，請參閱 [建立零 ETL 整合](#) 和 [刪除零 ETL 整合](#)。

資料表數量超過 10 萬個或結構描述數量超過 4950 個

對於目的地資料倉儲，資料表的數量超過 10 萬個或結構描述的數量超過 4950 個。Amazon Aurora 無法將資料傳送到 Amazon Redshift。資料表和結構描述的數量超過所設定的限制。若要解決此問題，請從來源資料庫中移除任何不必要的結構描述或資料表。

Amazon Redshift 無法載入資料

Amazon Redshift 無法將資料載入到零 ETL 整合。

若要解決此問題，請刪除 Amazon RDS 上的零 ETL 整合，然後重新建立整合。如需詳細資訊，請參閱[建立零 ETL 整合](#)和[刪除零 ETL 整合](#)。

工作群組參數的設定不正確

您的工作群組未開啟區分大小寫功能。

若要解決此問題，請前往整合詳細資訊頁面上的屬性索引標籤、選擇參數群組，然後從屬性索引標籤開啟區分大小寫的識別碼。如果您沒有現有的參數群組，請建立一個已開啟區分大小寫識別碼的參數群組。然後，在 Amazon RDS 上建立新的零 ETL 整合。如需詳細資訊，請參閱[建立零 ETL 整合](#)。

未建立資料庫來啟用零 ETL 整合

沒有建立可供零 ETL 整合來啟用的資料庫。

若要解決此問題，請為整合建立資料庫。如需詳細資訊，請參閱[在 Amazon Redshift 中建立目的地資料庫](#)。

資料表處於需要重新同步處理或重新同步處理已起始狀態

您的資料表處於需要重新同步處理或重新同步處理已起始狀態。

若要收集有關資料表為何處於該狀態的更詳細錯誤資訊，請使用 [SYS_LOAD_ERROR_DETAIL](#) 系統檢視。

查詢資料庫

若要查詢由 Amazon Redshift 叢集所託管的資料庫，您有兩個選項：

- AWS Management Console 使用查詢編輯器 Connect 到您的叢集並在上執行查詢。

如果在 Amazon Redshift 主控台中使用查詢編輯器，您即不必下載和設定 SQL 用戶端應用程式。

- 透過 SQL 用戶端工具連接到您的叢集，例如 SQL Workbench/J。

Amazon Redshift 可支援 SQL 用戶端工具透過 Java 資料庫連線 (JDBC) 和開放式資料庫連線 (ODBC) 進行連線。Amazon Redshift 不會提供或安裝任何 SQL 用戶端工具或程式庫，因此您必須在用戶端電腦或 Amazon EC2 執行個體上加以安裝才能使用。您可以使用支援 JDBC 或 ODBC 驅動程式的大多數 SQL 用戶端工具。

Note

當您撰寫預存程序時，我們建議您採用保護敏感值的最佳作法：

不要在預存程序邏輯中對任何敏感資訊進行硬式編碼。例如，請勿在預存程序主體的 CREATE USER 陳述式中指派使用者密碼。這會造成安全性風險，因為硬式編碼值可以記錄為目錄資料表中的結構描述資料。應改為透過參數將敏感值 (例如密碼) 當做引數傳遞給預存程序。

如需預存程序的相關資訊，請參閱 [CREATE PROCEDURE](#) 和在 [Amazon Redshift 中建立預存程序](#)。如需目錄資料表的相關資訊，請參閱 [系統目錄資料表](#)。

主題

- [連線至 Amazon Redshift](#)
- [使用 Amazon Redshift 查詢編輯器 v2 來查詢資料庫](#)
- [使用查詢編輯器來查詢資料庫](#)
- [使用 SQL 用戶端工具連接至 Amazon Redshift 資料倉儲](#)
- [使用 Amazon Redshift 資料 API](#)

連線至 Amazon Redshift

您可以使用以下語法連接到數據庫。

```
cluster-name.account-number.aws-region.redshift.amazonaws.com/database-name
```

語法元素定義如下。

- `cluster-name`

您叢集的名稱。

- `account-number`

在給定的 AWS 帳戶號碼相關聯的唯一識別碼 AWS 區域。指定帳戶在指定帳戶建立的所有叢集都 AWS 區域 具有相同的資訊 `account-number`。

- `aws-region`

叢集所在 AWS 區域 的程式碼。

- `database-name`

您的資料庫名稱。

例如，下列連接字串會指定 `us-east-1` AWS 區域 `st-1 my-cluster` 叢集中的 `my-db` 資料庫。

```
my-cluster.123456789012.us-east-1.redshift.amazonaws.com/my-db
```

使用 Amazon Redshift 查詢編輯器 v2 來查詢資料庫

查詢編輯器 v2 是另外一種網頁式 SQL 用戶端應用程式，可用來在 Amazon Redshift 資料倉儲上編寫和執行查詢。您可以將查詢結果視覺化為圖表，並透過與團隊中的其他人共用您的查詢來進行協作。查詢編輯器 v2 會取代先前的查詢編輯器。

Note

查詢編輯器 v2 可在商業上使用 AWS 區域。如需查詢編輯器 v2 可用位 AWS 區域 置的清單，請參閱中針對 [Redshift 查詢編輯器 v2](#) 列出的端點。Amazon Web Services 一般參考

如需查詢編輯器 v2 的示範，請觀看下列影片。[Amazon Redshift 查詢編輯器 v2](#)。

如需資料分析的示範，請觀看下列影片。[使用 Amazon Redshift 查詢編輯器 v2 進行資料分析](#)。

如需使用查詢編輯器 v2 透過隔離或共用連線來執行多個查詢的示範，請觀看下列影片。[使用查詢編輯器 v2 執行並行查詢](#)。

查詢編輯器 v2 有一組豐富的功能可供您管理和執行 SQL 陳述式。以下各節中的主題可協助您開始使用其中的許多功能。請自行探索查詢編輯器 v2 以熟悉其功能。

主題

- [配置您的 AWS 帳戶](#)
- [使用查詢編輯器 v2](#)
- [與查詢編輯器 v2 生成式 SQL 互動 \(預覽\)](#)
- [將資料載入到資料庫](#)
- [編寫和執行查詢](#)
- [編寫和執行筆記本](#)
- [查詢 AWS Glue Data Catalog](#)
- [查詢資料湖](#)
- [使用資料共用](#)
- [使用查詢編輯器 v2 來排程查詢](#)
- [將查詢結果視覺化](#)
- [以團隊的形式協作和共用](#)

配置您的 AWS 帳戶

當您從 Amazon Redshift 主控台選擇查詢編輯器 v2 時，瀏覽器中會開啟一個新的標籤，內有查詢編輯器 v2 的介面。有了適當的許可，您就可以存取 Amazon Redshift 叢集中的資料，或目前 AWS 區域叢集中您所擁有 AWS 帳戶 的工作群組中的資料。

系統管理員第一次為您設定查詢編輯器 v2 時 AWS 帳戶，他們會選擇用 AWS KMS key 來加密查詢編輯器 v2 資源的。默認情況下，AWS 擁有的密鑰用於加密資源。或者，管理員也可以在組態頁面中選擇金鑰的 Amazon Resource Name (ARN)，以使用客戶受管金鑰。設定帳戶後，無法變更 AWS KMS 加密設定。如需以查詢編輯器 v2 建立和使用客戶受管金鑰的相關資訊，請參閱[建立要與查詢編輯器搭配使用的 AWS KMS 客戶管理金鑰 v2](#)。管理員也可以選擇性地選擇用於某些功能 (例如，從檔案載入資料) 的 S3 儲存貯體和路徑。如需詳細資訊，請參閱[從本機檔案設定和工作流程載入資料](#)。

Amazon Redshift 查詢編輯器 v2 支援身分驗證、加密、隔離和合規功能，以確保靜態資料和傳輸中的資料安全無虞。如需資料安全和查詢編輯器 v2 的相關資訊，請參閱下列內容：

- [靜態加密](#)
- [傳輸中加密](#)
- [Amazon Redshift 中的組態與漏洞分析](#)

AWS CloudTrail 擷取由您或代表您發出的 API 呼叫和相關事件，AWS 帳戶 並將日誌檔傳遞到您指定的 Amazon S3 儲存貯體。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。若要進一步了解查詢編輯器 v2 在 AWS CloudTrail 上的執行方式，請參閱 [使用記錄 CloudTrail](#)。若要取得有關的更多資訊 CloudTrail，請參閱 [AWS CloudTrail 使用者指南](#)。

查詢編輯器 v2 對其某些資源具有可調整的配額。如需詳細資訊，請參閱 [Amazon Redshift 物件的配額](#)。

使用查詢編輯器 v2 所建立的資源

在查詢編輯器 v2 內，您可以建立儲存的查詢和圖表等資源。查詢編輯器 v2 中的所有資源都會與 IAM 角色或使用者相關聯。建議您將政策連接至 IAM 角色，並將該角色指派給使用者。

在查詢編輯器 v2 中，您可以為儲存的查詢和圖表新增及移除標籤。您可以在設定自訂 IAM 政策或搜尋資源時使用這些標籤。您也可以使用「AWS Resource Groups 標籤編輯器」來管理標籤。

您可以使用 IAM 政策設定 IAM 角色，以便與中的其他人共用查詢 AWS 區域。AWS 帳戶

建立要與查詢編輯器搭配使用的 AWS KMS 客戶管理金鑰 v2

若要建立對稱加密的客戶受管金鑰：

您可以建立對稱加密客戶受管金鑰，使用 AWS KMS 主控台或 AWS KMS API 作業來加密查詢編輯器 v2 資源。如需有關建立金鑰的指示，請參閱 AWS Key Management Service 開發人員指南中的 [建立對稱加密 AWS KMS 金鑰](#)。

金鑰政策

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

若要將客戶受管金鑰與 Amazon Redshift 查詢編輯器 v2 搭配使用，就必須在金鑰政策中允許下列 API 操作：

- kms:GenerateDataKey — 產生唯一一個用來加密資料的對稱資料金鑰。
- kms:Decrypt — 解密使用客戶受管金鑰所加密的資料。
- kms:DescribeKey — 提供客戶受管金鑰的詳細資訊，以便服務可以驗證金鑰。

以下是的範例 AWS KMS 政策 AWS 帳戶 111122223333。在第一部分中，kms:ViaService 會限制金鑰只能用於查詢編輯器 v2 服務 (在政策中名為 sqlworkbench.*region*.amazonaws.com)。使 AWS 帳戶 用密鑰必須是111122223333。在第二節中，的 root 使用者和金鑰管理員 AWS 帳戶 111122223333 可以存取金鑰。

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。如需這些任務的完整清單，了解需以根使用者登入的任務，請參閱 IAM 使用者指南中的[需要根使用者憑證的任務](#)。

```
{
  "Version": "2012-10-17",
  "Id": "key-consolepolicy",
  "Statement": [
    {
      "Sid": "Allow access to principals authorized to use Amazon Redshift Query Editor V2",
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt",
        "kms:DescribeKey"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "kms:ViaService": "sqlworkbench.region.amazonaws.com",
          "kms:CallerAccount": "111122223333"
        }
      }
    },
    {
      "Sid": "Allow access for key administrators",
```

```
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::111122223333:root"
    },
    "Action": [
      "kms:*"
    ],
    "Resource": "arn:aws:kms:region:111122223333:key/key_ID"
  }
]
```

下列資源提供有關 AWS KMS 金鑰的詳細資訊：

- 如需有關原 AWS KMS 則的詳細資訊，請參閱AWS Key Management Service 開發人員指南中的[指定原則中的權限](#)。
- 如需疑難排解 AWS KMS 原則的相關資訊，請參閱AWS Key Management Service 開發人員指南中的「[疑難排解金](#)」。
- 如需金鑰的相關資訊，請參閱《AWS Key Management Service 開發人員指南》中的 [AWS KMS 金鑰](#)。

存取查詢編輯器 v2

若要存取查詢編輯器 v2，您需要獲得許可。系統管理員可以將下列其中一個 AWS 受管理的原則附加至角色，以授與權限。(建議您將政策連接至 IAM 角色，並將該角色指派給使用者。) 這些 AWS 受管理的政策使用不同的選項撰寫，可控制標記資源允許共用查詢的方式。您可以使用 IAM 主控台 (<https://console.aws.amazon.com/iam/>) 來連接 IAM 政策。

- AmazonRedshiftQueryEditorV2 FullAccess — 授予對 Amazon Redshift 查詢編輯器 v2 操作和資源的完整存取權。此政策也會授予其他必要服務的存取權。
- AmazonRedshiftQueryEditorV2 NoSharing — 授予在不共用資源的情況下使用 Amazon Redshift 查詢編輯器 v2 的能力。此政策也會授予其他必要服務的存取權。
- AmazonRedshiftQueryEditorV2 ReadSharing — 授予在有限資源共用的情況下使用 Amazon Redshift 查詢編輯器 v2 的能力。獲得授予的主體可以讀取與其團隊共用的資源，但無法更新這些資源。此政策也會授予其他必要服務的存取權。
- AmazonRedshiftQueryEditorV2 ReadWrite 共用 — 授與 Amazon Redshift 查詢編輯器 v2 搭配使用資源共用的能力。獲得授予的主體可以讀取和更新與其團隊共用的資源。此政策也會授予其他必要服務的存取權。

您也可以根據所提供受控政策中允許和拒絕的許可來建立自己的政策。如果您使用 IAM 主控台政策編輯器建立自己的政策，請選擇 SQL Workbench 作為您在視覺化編輯器中為其建立政策的服務。查詢編輯器 v2 會在視覺化編輯器和 IAM 政策模擬器中使用服務名稱 AWS SQL Workbench。

若要讓主體 (已獲派 IAM 角色的使用者) 能夠連線到 Amazon Redshift 叢集，就需要其中一個查詢編輯器 v2 受管政策中的許可。他們也需要叢集的 `redshift:GetClusterCredentials` 許可。若要獲得此許可，具有系統管理許可的人員可以使用臨時憑證，將政策連接至用來連線到叢集的 IAM 角色。您可以將政策的範圍限定在特定叢集或更為普遍的範圍。如需有關使用臨時登入資料之權限的詳細資訊，請參閱 [建立 IAM 角色或具有呼叫權限的使用者 GetClusterCredentials](#)。

若要讓主體 (一般是已獲派 IAM 角色的使用者) 能夠在帳戶設定頁面中為帳戶中的其他使用者開啟匯出結果集的功能，他們需要該角色連接的 `sqlworkbench:UpdateAccountExportSettings` 許可。此權限包含在 `AmazonRedshiftQueryEditorV2FullAccess` AWS 受管理的策略中。

當新功能新增至查詢編輯器 v2 時，AWS 受管理的政策會視需要更新。如果您根據所提供受管策略中允許和拒絕的許可建立自己的政策，請編輯您的政策，讓政策隨著受管政策的變更進行更新以保持在最新狀態。如需 Amazon Redshift 中受管政策的相關資訊，請參閱 [AWS Amazon Redshift 的受管政策](#)。

若要提供存取權，請新增權限至您的使用者、群組或角色：

- 使用者和群組位於 AWS IAM Identity Center：

建立權限合集。請按照 AWS IAM Identity Center 使用者指南 中的 [建立權限合集](#) 說明進行操作。

- 透過身分提供者在 IAM 中管理的使用者：

建立聯合身分的角色。請按照 IAM 使用者指南 的 [為第三方身分提供者 \(聯合\) 建立角色](#) 中的指示進行操作。

- IAM 使用者：

- 建立您的使用者可擔任的角色。請按照 IAM 使用者指南 的 [為 IAM 使用者建立角色](#) 中的指示進行操作。
- (不建議) 將政策直接附加至使用者，或將使用者新增至使用者群組。請遵循 IAM 使用者指南的 [新增許可到使用者 \(主控台\)](#) 中的指示。

Note

如果 AWS IAM Identity Center 管理員移除整個帳戶中特定許可集的所有許可集關聯，使用者便無法再存取原本與已移除許可集相關聯之任何查詢編輯器資源的存取權。如果之後重新建立了相同的許可，系統會建立新的內部識別碼。由於內部識別碼已變更，因此使用者無法再存取

其先前擁有之查詢編輯器資源的存取權。我們的建議是，在管理員刪除許可集之前，該許可集的使用者先將查詢編輯器資源 (例如筆記本和查詢) 匯出為備份。

設定主體標籤以從查詢編輯器 v2 連接叢集或工作群組

若要使用聯合身分使用者選項連線到叢集或工作群組，請使用主體標籤設定 IAM 角色或使用者。或者，也可以設定身分提供者 (IdP) 以傳入 RedshiftDbUser 和 (選擇性) RedshiftDbGroups。如需使用 IAM 來管理標籤的相關資訊，請參閱《IAM 使用者指南》中的 [在 AWS Security Token Service 中傳遞工作階段標籤](#)。若要使用設定存取權 AWS Identity and Access Management，管理員可以使用 IAM 主控台 (<https://console.aws.amazon.com/iam/>) 新增標籤。

將主體標籤新增至 IAM 角色

1. 登入 AWS Management Console 並開啟身分與存取權管理主控台，網址為 <https://console.aws.amazon.com/iam/>。
2. 在導覽窗格中，選擇 Roles (角色)。
3. 選擇需要使用聯合身分使用者存取查詢編輯器 v2 的角色。
4. 選擇 Tags (標籤) 索引標籤。
5. 選擇管理標籤。
6. 選擇新增標籤，並將索引鍵輸入為 RedshiftDbUser，然後輸入聯合身分使用者名稱的值。
7. 選擇性地選擇新增標籤，並將索引鍵輸入為 RedshiftDbGroups，然後輸入要與使用者產生關聯之群組名稱的值。
8. 選擇儲存變更以檢視與所選擇的 IAM 角色相關聯的標籤清單。傳播變更的過程可能需要幾秒鐘的時間。
9. 若要使用聯合身分使用者，請在變更傳播完成後重新整理查詢編輯器 v2 的頁面。

設定您的身分提供者 (IdP) 以傳遞主體標籤

使用身分提供者 (IdP) 設定標籤的程序隨 IdP 而異。如需如何將使用者和群組資訊傳遞至 SAML 屬性的指示，請參閱您的 IdP 文件。正確設定後，下列屬性會顯示在您的 SAML 回應中，由用 AWS Security Token Service 來填入和的主參 RedshiftDbUser 與 RedshiftDbGroups 者標籤中。

```
<Attribute Name="https://aws.amazon.com/SAML/Attributes/PrincipalTag:RedshiftDbUser">
  <AttributeValue>db-user-name</AttributeValue>
</Attribute>
```

```
<Attribute Name="https://aws.amazon.com/SAML/Attributes/PrincipalTag:RedshiftDbGroups">
  <AttributeValue>db-groups</AttributeValue>
</Attribute>
```

選擇性的 `db_group` 必須是以冒號分隔的清單，例如 `group1:group2:group3`。

此外，您也可以設定 `TransitiveTagKeys` 屬性以在鏈結角色期間保留標籤。

```
<Attribute Name="https://aws.amazon.com/SAML/Attributes/TransitiveTagKeys">
  <AttributeValue>RedshiftDbUser</AttributeValue>
  <AttributeValue>RedshiftDbGroups</AttributeValue>
</Attribute>
```

如需設定查詢編輯器 v2 的相關資訊，請參閱 [要使用查詢編輯器 v2 所需的許可](#)。

Note

當您使用查詢編輯器 v2 的聯合身分使用者連線選項連線到叢集或工作群組時，身分提供者 (IdP) 可以為 `RedshiftDbUser` 和 `RedshiftDbGroups` 提供自訂主體標籤。目前，AWS IAM Identity Center 不支援將自訂主要標籤直接傳遞至查詢編輯器 v2。

使用查詢編輯器 v2

查詢編輯器 v2 主要用來編輯和執行查詢、將查詢結果視覺化，以及與團隊共用您的工作。透過查詢編輯器 v2，您可以建立資料庫、結構描述、資料表和使用使用者定義的函數 (UDF)。在樹狀檢視面板中，您可以針對每個資料庫檢視其結構描述。對於每個結構描述，您可以檢視其資料表、檢視、UDF 和預存程序。

主題

- [開啟查詢編輯器 v2](#)
- [連線至 Amazon Redshift 資料庫](#)
- [瀏覽 Amazon Redshift 資料庫](#)
- [建立資料庫物件](#)
- [檢視查詢和標籤歷史記錄](#)
- [使用查詢編輯器 v2 時的考量](#)
- [變更帳戶設定](#)

開啟查詢編輯器 v2

開啟查詢編輯器 v2

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 從導覽器選單中選擇編輯器，然後選擇查詢編輯器 V2。查詢編輯器 v2 便會在新的瀏覽器標籤中開啟。

查詢編輯器頁面會有一個導覽器選單可供您選擇檢視，如下所示：

編輯器



您可以管理和查詢組織為資料表並包含在資料庫中的資料。資料庫可以包含儲存的資料，也可以包含儲存在其他地方 (例如 Amazon S3) 之資料的參考。您可以連線到包含在叢集或無伺服器工作群組內的資料庫。

在編輯器檢視中工作時，您可以使用下列控制項：

- 叢集或工作群組欄位會顯示您目前所連線項目的名稱。資料庫欄位會顯示叢集或工作群組內的資料庫。您在資料庫檢視中執行的動作預設會對您選取的資料庫採取行動。
- 叢集或工作群組、資料庫和結構描述的樹狀檢視階層式檢視。在結構描述下，您可以處理您的資料表、檢視、函數和預存程序。樹狀檢視中的每個物件都支援可針對物件執行相關動作 (例如重新整理或捨棄) 的內容選單。



建立動作可建立資料庫、結構描述、資料表和函數。



載入資料動作可將資料從 Amazon S3 或從本機檔案載入到資料庫。



儲存圖示可儲存查詢。



捷徑圖示可顯示編輯器的鍵盤快速鍵。

- ...

更多圖示可在編輯器中顯示更多動作。例如：

- 與我的團隊共用可與團隊共用查詢或筆記本。如需詳細資訊，請參閱 [以團隊的形式協作和共用](#)。
- 捷徑可顯示編輯器的鍵盤快速鍵。
- 標籤歷史記錄可在編輯器中顯示標籤的歷史記錄。
- 重新整理自動完成可在編寫 SQL 時重新整理所顯示的建議。

- +

編輯器區域，可供您輸入和執行查詢。

執行查詢後會出現結果標籤，內有查詢結果。您可以在此開啟圖表以將結果視覺化。您也可以匯出結果。

- +

筆記本區域，可供您新增區段以便輸入和執行 SQL 或新增 Markdown。

執行查詢後會出現結果標籤，內有查詢結果。您可以在此匯出結果。

查詢



查詢包含用來管理和查詢資料庫中所含資料的 SQL 命令。當您使用查詢編輯器 v2 載入範例資料時，其也會為您建立並儲存範例查詢。

當您選擇已儲存的查詢時，您可以使用內容 (右鍵) 選單來將其開啟、重新命名和刪除。您可以選擇查詢詳細資訊來檢視已儲存查詢的屬性，例如查詢 ARN。您還可以檢視其版本歷史記錄、編輯連接至查詢的標籤，以及將其與您的團隊共用。

筆記本



SQL 筆記本包含 SQL 和 Markdown 儲存格。使用筆記本可在單一文件中組織、註釋和共用多個 SQL 命令。

當您選擇已儲存的筆記本時，您可以使用內容 (右鍵) 選單來將其開啟、重新命名、複製和刪除。您可以選擇筆記本詳細資訊來檢視已儲存筆記本的屬性，例如筆記本 ARN。您還可以檢視其版本歷史記錄、編輯連接至筆記本的標籤、匯出筆記本，以及將其與您的團隊共用。如需詳細資訊，請參閱 [編寫和執行筆記本](#)。

圖表



圖表會以視覺化方式呈現資料。查詢編輯器 v2 提供了工具供您建立多種類型的圖表並將其儲存起來。

當您選擇已儲存的圖表時，您可以使用內容 (右鍵) 選單來將其開啟、重新命名和刪除。您可以選擇圖表詳細資訊來檢視已儲存圖表的屬性，例如圖表 ARN。您也可以編輯連接至圖表的標籤，並將其匯出。如需詳細資訊，請參閱 [將查詢結果視覺化](#)。

歷史記錄



查詢歷史記錄會列出您使用 Amazon Redshift 查詢編輯器 v2 執行的查詢。這些查詢會以個別查詢的形式執行，或是作為 SQL 筆記本的一部分來執行。如需詳細資訊，請參閱 [檢視查詢和標籤歷史記錄](#)。

已排程的查詢



已排程的查詢是設定為在特定時間啟動的查詢。

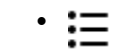
所有查詢編輯器 v2 檢視都有下列圖示：



視覺化模式圖示可在淺色模式和深色模式之間進行切換。



設定圖示可顯示不同設定畫面的選單。



編輯器偏好設定圖示可讓您在編輯器 v2 時編輯您的偏好設定。您可以在編輯工作區設定，以變更字型大小、標籤大小和其他顯示設定。您也可以開啟 (或關閉) 自動完成，以在您輸入 SQL 時顯示建議。



連線圖示可檢視編輯器標籤所使用的連線。

連線可用來擷取資料庫中的資料。連線會針對特定資料庫來建立。使用隔離連線時，在某個編輯器標籤中會變更資料庫的 SQL 命令 (例如建立暫存資料表) 結果，並無法在另一個編輯器標籤中看到。當您在查詢編輯器 v2 中開啟編輯器標籤時，預設會使用隔離連線。當您建立共用連線時 (也就是如果您關閉隔離工作階段切換開關的話)，相同資料庫的共用連線彼此能看到其他共用連線的結果。但是，使用資料庫共用連線的編輯器標籤並不會平行執行。使用相同連線的查詢必須等到連線為可用狀態時才能執行。某個資料庫的連線不能與另一個資料庫共用，因此無法在不同的資料庫連線中看見 SQL 結果。

帳戶中的任何使用者可以擁有的作用中連線數目會由查詢編輯器 v2 管理員控制。



帳戶設定圖示可讓管理員變更帳戶中所有使用者的某些設定。如需詳細資訊，請參閱 [變更帳戶設定](#)。

連線至 Amazon Redshift 資料庫

若要連線至資料庫，請在樹狀檢視面板中選擇叢集或工作群組的名稱。若出現提示，請輸入連線參數。

在連線至叢集或工作群組及其資料庫時，通常會提供資料庫名稱。您也可以提供下列其中一種身分驗證方法所需的參數：

IAM Identity Center

若使用此方法，您可以使用身分提供者 (IdP) 提供的單一登入憑證連線到 Amazon Redshift 資料倉儲。您的叢集或工作群組必須針對 Amazon Redshift 主控台內的 IAM Identity Center 來啟用。如需設定 IAM 身分中心連線的說明，請參閱 [將 Redshift 與 IAM Identity Center 連線，為使用者提供單一登入體驗](#)。

聯合身分使用者

使用此方法時，IAM 角色或使用者的主體標籤必須提供連線詳細資訊。您可以在 AWS Identity and Access Management 或您的身分識別提供者 (IdP) 中設定這些標籤。查詢編輯器 v2 依賴以下標籤。

- RedshiftDbUser — 此標籤會定義查詢編輯器 v2 所使用的資料庫使用者。這是必要標籤。
- RedshiftDbGroups — 此標籤會定義在連線至查詢編輯器 v2 時所加入的資料庫群組。這是選擇性標籤，其值必須是以冒號分隔的清單，例如 group1:group2:group3。系統會忽略空白值，也就是說，會將 group1:::group2 解譯為 group1:group2。

這些標籤會轉送至 `redshift:GetClusterCredentials` API，以取得叢集的憑證。如需詳細資訊，請參閱 [設定主體標籤以從查詢編輯器 v2 連接叢集或工作群組](#)。

使用資料庫使用者名稱的臨時憑證

只有在連線至叢集時才能使用此選項。使用此方法時，查詢編輯器 v2 會為資料庫提供使用者名稱。查詢編輯器 v2 會產生能以資料庫使用者名稱的身分連線到資料庫的臨時密碼。使用此方法來連線的使用者必須已被允許 `redshift:GetClusterCredentials` 的 IAM 許可。若要防止使用者使用此方法，請修改其 IAM 使用者或角色以拒絕此許可。

使用 IAM 身分的臨時憑證

只有在連線至叢集時才能使用此選項。使用此方法時，查詢編輯器 v2 會將使用者名稱對應到您的 IAM 身分，並產生能以 IAM 身分連線到資料庫的臨時密碼。使用此方法來連線的使用者必須已被允許 `redshift:GetClusterCredentialsWithIAM` 的 IAM 許可。若要防止使用者使用此方法，請修改其 IAM 使用者或角色以拒絕此許可。

資料庫使用者名稱和密碼

使用此方法時，也會為您要連線的資料庫提供使用者名稱和密碼。查詢編輯器 v2 會在 AWS Secrets Manager 中代表您建立秘密。此秘密包含用來連線至資料庫的憑證。

AWS Secrets Manager

使用此方法而不是資料庫名稱時，請提供儲存在 Secrets Manager、包含資料庫和登入憑證的祕密。如需有關建立密碼的資訊，請參閱 [建立資料庫連線認證的密碼](#)。

當您使用查詢編輯器 v2 選取叢集或工作群組時，視內容而定，您可以使用內容 (右鍵) 選單來建立、編輯和刪除連線。您可以透過選擇連線詳細資訊，檢視連線的連線 ARN 等屬性。您也可以編輯連接至連線的標籤。


































瀏覽 Amazon Redshift 資料庫

在資料庫內，您可於樹狀檢視面板中管理結構描述、資料表、檢視、函數和預存程序。檢視中的每個物件在內容 (右鍵) 選單中都有與其相關聯的動作。

階層式樹狀檢視面板會顯示資料庫物件。若要重新整理樹狀檢視面板，以顯示上次顯示樹狀檢視之後可能已建立的資料庫物件，請選擇



圖示。開啟物件的內容 (右鍵) 選單即可查看您能夠執行的動作。

▼  redshift-cluster-tickit	
▼  dev	
▼  public	
▼  Tables	11
 accommodations	
 category	
 customer_activity	
 date	
 event	
 listing	
 sales	
 sales2	
 users	
 venue	
 zipcode	
▼  Views	1
 myevent	
▼  Functions	2
<i>fx</i> f_py_greater(float8,float8)	
<i>fx</i> f_sql_greater(float8,float8)	
▼  Stored procedures	1
<i>fx</i> test_sp1(int4,varchar)	
>  testschema	
>  testschema2	
▼  sample_data_dev	
▼  tickit	
>  Tables	7
>  Views	0
>  Functions	0
>  Stored procedures	0
>  tpch	
>  tpcds	
>  testdb	

在選擇資料表後，您可以執行下列操作：

- 若要使用會查詢資料表中所有資料欄的 SELECT 陳述式在編輯器中開始查詢，請使用選取資料表。
- 若要查看屬性或資料表，請使用顯示資料表定義。使用此選項可查看資料欄名稱、資料欄類型、編碼、分佈索引鍵、排序索引鍵，以及資料欄是否可以包含 Null 值。如需資料表屬性的相關資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的 [CREATE TABLE](#)。
- 若要刪除資料表，請使用刪除。您可以使用截斷資料表刪除資料表中的所有資料列，或使用捨棄資料表從資料庫中移除資料表。如需詳細資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的 [TRUNCATE](#) 和 [DROP TABLE](#)。

選擇要重新整理的結構描述或捨棄結構描述。

選擇要顯示檢視定義的檢視或捨棄檢視。

選擇要顯示函數定義的函數或捨棄函數。

選擇要顯示程序定義的預存程序或捨棄程序。

建立資料庫物件

您可以建立資料庫物件，包括資料庫、結構描述、資料表和使用使用者定義函數 (UDF)。您必須連線至叢集或工作群組和資料庫，才能建立資料庫物件。

建立資料庫

您可以使用查詢編輯器 v2 在叢集或工作群組中建立資料庫。

若要建立資料庫

如需有關資料庫的資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的 [CREATE DATABASE](#)。

1. 選



擇立，然後選擇資料庫。

2. 輸入資料庫名稱。

3. (選擇性) 選取使用者和群組，然後選擇資料庫使用者。

建

4. (選擇性) 您可以從資料共用或 AWS Glue Data Catalog 建立資料庫。如需有關的詳細資訊 AWS Glue，請參閱 [什麼是 AWS Glue？](#) 在 AWS Glue 開發人員指南中。
 - (選擇性) 選取使用資料共用建立，然後選擇選取資料共用。此清單包含可用來在目前的叢集或工作群組中建立取用者資料共用的生產者資料共用。
 - (選擇性) 選取建立方式 AWS Glue Data Catalog，然後選擇選擇 AWS Glue 資料庫。在資料目錄結構描述中，輸入在參考由三個部分組成的名稱 (database.schema.table) 中的資料時，會用於結構描述的名稱。
5. 選擇建立資料庫。

樹狀檢視面板中隨即會顯示新的資料庫。

當您選擇選擇性步驟來查詢從資料共用建立的資料庫時，請連線到叢集或工作群組中的 Amazon Redshift 資料庫 (例如，預設資料庫 dev)，並使用由三個部分組成的標記法 (database.schema.table) (其會參考您選取使用資料共用建立時所建立的資料庫名稱)。資料共用資料庫會列在查詢編輯器 v2 的編輯器標籤中，但未啟用直接連線功能。

選擇可選步驟查詢從建立的資料庫時 AWS Glue Data Catalog，請連線到叢集或工作群組中的 Amazon Redshift 資料庫 (例如，預設資料庫 dev)，並使用參考您選取建立使 AWS Glue Data Catalog 用時建立的資料庫名稱、在資料目錄結構描述中命名的結構描述以及在中表格的三部分標記法 (database.schema.table)。AWS Glue Data Catalog 類似於：

```
SELECT * FROM glue-database.glue-schema.glue-table
```

Note

確認您已使用連線方法連線至預設資料庫，使用 IAM 身分識別的臨時登入資料，並且您的 IAM 登入資料已獲授與 AWS Glue 資料庫的使用權限。

```
GRANT USAGE ON DATABASE glue-database to "IAM:MyIAMUser"
```

資 AWS Glue 料庫會列在查詢編輯器 v2 編輯器索引標籤中，但未啟用直接連線。

[如需有關查詢的詳細資訊 AWS Glue Data Catalog](#)，請參閱以消費者身分使用 Lake 格式化管理的 [資料庫](#) 和 Amazon Redshift 資料庫開發人員指南中以生產者身分使用 Lake 格式化管理的 [資料庫](#)。

以資料共用取用者身分建立資料庫的範例

下列範例描述的是所使用的一個特定案例，目的是使用查詢編輯器 v2 從資料共用建立資料庫。請檢閱此案例，以了解如何在環境中從資料共用建立資料庫。此案例使用兩個叢集，分別是 cluster-base (生產者叢集) 和 cluster-view (取用者叢集)。

1. 使用 Amazon Redshift 主控台在叢集 cluster-base 中為資料表 category2 建立資料共用。生產者資料共用會命名為 datashare_base。

如需有關建立資料共用的資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的[在 Amazon Redshift 中跨叢集共用資料](#)。

2. 使用 Amazon Redshift 主控台接受資料共用 datashare_base 作為叢集 cluster-view 中資料表 category2 的取用者。
3. 檢視查詢編輯器 v2 中的樹狀檢視面板，該面板會將 cluster-base 的階層顯示為：

- 叢集：cluster-base
 - 資料庫：dev
 - 結構描述：public
 - 資料表：category2

4. 選



擇立，然後選擇資料庫。

5. 在資料庫名稱中輸入 see_datashare_base。
6. 選取使用資料共用建立，然後選擇選取資料共用。選擇 datashare_base 作為您要建立之資料庫的來源。

查詢編輯器 v2 中的樹狀檢視面板會將 cluster-view 的階層顯示為：

- 叢集：cluster-view
 - 資料庫：see_datashare_base
 - 結構描述：public
 - 資料表：category2

7. 當您查詢資料時，請連線到叢集 cluster-view 的預設資料庫 (名稱一般是 dev)，但在 SQL 中請參考資料共用資料庫 see_datashare_base。

Note

在查詢編輯器 v2 的編輯器檢視中，所選取的叢集為 `cluster-view`。所選取的資料庫為 `dev`。資料庫 `see_datashare_base` 會列出，但未啟用直接連線功能。您選擇 `dev` 資料庫，並在執行的 SQL 中參考 `see_datashare_base`。

```
SELECT * FROM "see_datashare_base"."public"."category2";
```

查詢會從叢集 `cluster_base` 中的資料共用 `datashare_base` 擷取資料。

從一個創建數據庫的示例 AWS Glue Data Catalog

下列範例說明用來從 AWS Glue Data Catalog 使用查詢編輯器 v2 建立資料庫的特定案例。檢閱此案例，瞭解如何從環境 AWS Glue Data Catalog 中建立資料庫。這個案例會使用 `cluster-view` 這個叢集來包含您建立的資料庫。

1. 選



擇 **+** 立，然後選擇資料庫。

2. 在資料庫名稱中輸入 `data_catalog_database`。

3. 選取 [使用建立] AWS Glue Data Catalog，然後選擇 [選擇資 AWS Glue 料庫]。選擇 `glue_db` 作為您要建立之資料庫的來源。

選擇資料目錄結構描述，並輸入 `myschema` 作為要在由三個部分組成的標記法中使用的結構描述名稱。

查詢編輯器 v2 中的樹狀檢視面板會將 `cluster-view` 的階層顯示為：

- 叢集：`cluster-view`
 - 資料庫：`data_catalog_database`
 - 結構描述：`myschema`
 - 資料表：`category3`
4. 當您查詢資料時，請連線到叢集 `cluster-view` 的預設資料庫 (名稱一般是 `dev`)，但在 SQL 中請參考資料庫 `data_catalog_database`。

Note

在查詢編輯器 v2 的編輯器檢視中，所選取的叢集為 `cluster-view`。所選取的資料庫為 `dev`。資料庫 `data_catalog_database` 會列出，但未啟用直接連線功能。您選擇 `dev` 資料庫，並在執行的 SQL 中參考 `data_catalog_database`。

```
SELECT * FROM "data_catalog_database"."myschema"."category3";
```

查詢會擷取由 AWS Glue Data Catalog 分類的資料。

建立結構描述

您可以使用查詢編輯器 v2 在叢集或工作群組中建立結構描述。

建立結構描述

如需有關結構描述的資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的 [結構描述](#)。

1. 選



擇 **+** 立，然後選擇結構描述。

2. 輸入結構描述名稱。

3. 選擇本機或外部作為結構描述類型。

如需本機結構描述的相關資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的 [CREATE SCHEMA](#)。如需外部結構描述的相關資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的 [CREATE EXTERNAL SCHEMA](#)。

4. 如果您選擇外部，則會有下列外部結構描述選項。

- Glue Data Catalog — 可在 Amazon Redshift 中建立會參考 AWS Glue 中資料表的外部結構描述。除了選擇資料 AWS Glue 庫之外，請選擇與叢集關聯的 IAM 角色以及與資料目錄相關聯的 IAM 角色。
- PostgreSQL — 可在 Amazon Redshift 中建立會參考 Amazon RDS for PostgreSQL 或 Amazon Aurora PostgreSQL 相容版本資料庫的外部結構描述。也請提供連線資訊給資料庫。如需聯合

查詢的相關資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的[使用聯合查詢來查詢資料](#)。

- MySQL — 可在 Amazon Redshift 中建立會參考 Amazon RDS for MySQL 或 Amazon Aurora MySQL 相容版本資料庫的外部結構描述。也請提供連線資訊給資料庫。如需聯合查詢的相關資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的[使用聯合查詢來查詢資料](#)。

5. 選擇建立結構描述。

樹狀檢視面板中便會出現新的結構描述。

建立資料表

您可以使用查詢編輯器 v2 在叢集或工作群組中建立資料表。

若要建立資料表

您可以根據指定的逗號分隔值 (CSV) 檔案來建立資料表，也可以定義資料表的每個資料欄。如需有關資料表的資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的[設計資料表](#)和 [CREATE TABLE](#)。

請選擇在編輯器中開啟查詢，先檢視及編輯 CREATE TABLE 陳述式，再執行查詢以建立資料表。

1. 選



擇立，然後選擇資料表。

2. 選擇結構描述。

3. 輸入資料表名稱。

4. 選擇



新增欄位以新增資料欄。

5. 使用 CSV 檔案作為資料表定義的範本：

- a. 選擇從 CSV 載入。
- b. 瀏覽至檔案位置。

如果您使用 CSV 檔案，請確定檔案的第一個資料列包含資料欄標題。

- c. 選擇檔案，然後選擇開啟。確認資料欄名稱和資料類型符合所需。

建

6. 針對每一個資料欄，請選擇該資料欄，然後選擇您想要的選項：
 - 為編碼選擇一個值。
 - 選擇預設值。
 - 如果您希望資料欄的值遞增，請開啟自動遞增。然後指定自動遞增種子和自動遞增步長的值。
 - 如果資料欄一律應該包含值，請開啟非 NULL。
 - 輸入資料欄的大小值。
 - 如果您想讓資料欄成為主索引鍵，請開啟主索引鍵。
 - 如果您想讓資料欄成為唯一索引鍵，請開啟唯一索引鍵。
7. (選擇性) 選擇資料表詳細資訊，然後選擇下列任何選項：
 - 分佈索引鍵資料欄和樣式。
 - 排序索引鍵資料欄和排序類型。
 - 開啟備份，以將資料表包含在快照中。
 - 開啟暫存資料表以將資料表建立為暫存資料表。
8. 選擇在編輯器中開啟查詢以繼續指定用來定義資料表的選項，或選擇建立資料表以建立資料表。


建立函數

您可以使用查詢編輯器 v2 在叢集或工作群組中建立函數。

建立 函數

1. 選



擇  立，然後選擇函數。

2. 在類型中，選擇 SQL 或 Python。
3. 選擇結構描述的值。
4. 輸入函數名稱的值。
5. 輸入函數波動的值。
6. 以輸入參數的順序，依資料類型選擇參數。
7. 在傳回中，選擇資料類型。
8. 輸入函數的 SQL 程式或 Python 程式的程式碼。

9. 選擇建立。

如需使用者定義函數 (UDF) 的相關資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的[建立使用者定義函數](#)。

檢視查詢和標籤歷史記錄

您可以使用查詢編輯器 v2 檢視查詢歷史記錄。只有使用查詢編輯器 v2 執行的查詢才會出現在查詢歷史記錄中。使用編輯器標籤或筆記本標籤所執行的查詢都會顯示出來。您可以依期間 (例如 This week) 篩選所顯示的清單，其中一週會定義為星期一至星期日。查詢清單一次會擷取 25 列符合篩選條件的查詢。選擇載入更多便可查看下一組。選擇查詢，然後從動作選單中選擇。可用的動作取決於所選擇的查詢是否已儲存。您可以選擇下列操作：

- 檢視查詢詳細資訊 — 顯示查詢詳細資訊頁面，其中包含已執行之查詢的詳細資訊。
- 在新標籤中開啟查詢 — 開啟新的編輯器標籤，並使用所選擇的查詢讓其做好準備。如果仍然連線，則系統會自動選取叢集或工作群組和資料庫。若要執行查詢，請先確認是否已選擇正確的叢集或工作群組和資料庫。
- 開啟來源標籤 — 如果仍開啟，請導覽至查詢在執行時所屬的編輯器或筆記本標籤。查詢執行後，編輯器或筆記本的內容可能已有所變更。
- 開啟儲存的查詢 — 導覽至編輯器或筆記本標籤，並開啟查詢。

您也可以檢視在編輯器標籤中執行之查詢的歷史記錄，或檢視在筆記本標籤中執行之查詢的歷史記錄。若要查看標籤中的查詢歷史記錄，請選擇標籤歷史記錄。在標籤歷史記錄內，您可以執行下列操作：

- 複製查詢 — 將查詢版本的 SQL 內容複製到剪貼簿。
- 在新標籤中開啟查詢 — 開啟新的編輯器標籤，並使用所選擇的查詢讓其做好準備。若要執行查詢，您必須選擇叢集或工作群組和資料庫。
- 檢視查詢詳細資訊 — 顯示查詢詳細資訊頁面，其中包含已執行之查詢的詳細資訊。

使用查詢編輯器 v2 時的考量

在使用查詢編輯器 v2 時，請考量下列事項：

- 查詢結果大小上限為 5 MB 或 100,000 個資料列 (視何者較小)。
- 您可以執行長度最多 300,000 個字元的查詢。
- 您可以儲存長度最多 30,000 個字元的查詢。

- 根據預設，查詢編輯器 v2 會自動遞交每個執行的個別 SQL 命令。在提供了 BEGIN 陳述式時，BEGIN-COMMIT 或 BEGIN-ROLLBACK 區塊內的陳述式會以單一交易的形式來執行。如需交易的相關資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的 [BEGIN](#)。
- 在執行 SQL 陳述式時，查詢編輯器 v2 可顯示的警告數量上限為 10 個。例如，在執行預存程序時，不會顯示超過 10 個 RAISE 陳述式。
- 查詢編輯器 v2 不支援包 RoleSessionName 含逗號 (,) 的 IAM。您可能會看到類似下列內容的錯誤訊息：「'aroa123456789 範例：myText，您的文字」不是有效的值 TagValue -它包含非法字元」當您定義包含逗號的 IAM，然後使用具有該 IAM RoleSessionName 角色的查詢編輯器 v2 時，就會出現此問題。

如需 IAM 的詳細資訊 RoleSessionName，請參閱 IAM 使用者指南中的 [RoleSessionName SAML 屬性](#)。

變更帳戶設定

具有正確 IAM 許可的使用者可以檢視和變更相同 AWS 帳戶中其他使用者的帳戶設定。此管理員可以檢視或設定下列項目：

- 帳戶中每一使用者的最大並行資料庫連線數。這包括隔離工作階段的連線。當您變更此值時，其可能需要 10 分鐘才會生效。
- 允許帳戶中的使用者將 SQL 命令的整個結果集匯出至檔案。
- 載入並顯示包含一些相關聯之已儲存查詢的範例資料庫。
- 指定帳戶使用者用來從本機檔案載入資料的 Amazon S3 路徑。
- 檢視用來加密查詢編輯器 v2 資源的 KMS 金鑰 ARN。

與查詢編輯器 v2 生成式 SQL 互動 (預覽)

這是預覽版本中的查詢編輯器 v2 生成式 SQL 的發行前版本文件。文件和功能會隨時變更。我們建議僅在測試環境中使用此功能，不要在生產環境中使用。如需預覽版條款與條件，請參閱 [AWS 服務條款](#) 中的 Beta 版服務參與。

Note

目前，產生式 SQL 支援僅適用於下列項目 AWS 區域：

- 美國東部 (維吉尼亞北部) 區域 (us-east-1)
- 美國西部 (奧勒岡) 區域 (us-west-2)
- 歐洲 (法蘭克福) 區域 (eu-central-1)

您可以在 Amazon Redshift 查詢編輯器 v2 中與 Amazon Q 生成式 SQL 功能互動。這是一個編碼助理，可根據您的提示和資料庫模式產生 SQL 陳述式。當您在查詢編輯器 v2 中編寫筆記本時，可以使用此編碼助理。

與生成式 SQL 互動時，請提出特定問題，在有複雜的請求時反覆運算，並驗證答案的準確性。

以自然語言提供分析請求時，請盡量具體地協助編碼助理了解您需要的內容。而不是詢問「尋找售出最多門票的熱門會場」，而是提供更多詳細資訊，例如「尋找 2008 年售出最多門票的前三個會場的名稱/ID」。使用資料庫中一致的物件名稱，例如資料庫中定義的結構描述、資料表和資料欄名稱，而不是以不同的方式參考相同的物件，這會造成助理混淆。

將複雜的請求分解為多個簡單的陳述式，這些陳述式更容易讓助理解譯。反覆提出後續問題，以從助理那裡獲得更詳細的分析。例如，首先要問「哪個州的場地最多？」然後根據回應，詢問「哪個是這個州最受歡迎的會場？」。

執行產生的 SQL 之前，請先檢閱產生的 SQL 以確保準確性。如果產生的 SQL 查詢有錯誤或不符合您的意圖，請提供指示給助理，說明如何更正，而不是改寫整個請求。例如，如果查詢缺少年份的述詞子句，請詢問「從 2008 年提供會場」。

與生成式 SQL 互動時的考量

在聊天面板中工作時，請考慮以下幾點。

- 您帳戶的查詢編輯器 v2 管理員必須已在生成式 SQL 設定頁面中開啟聊天功能。
- 若要使用查詢編輯器 v2 生成式 SQL，除了查詢編輯器 v2 AWS 受管政策中指定的其他許可 `sqlworkbench:GetQSqlRecommendations` 外，您還需要 IAM 政策中的許可。如需有關 AWS 受管理策略的詳細資訊，請參閱 [存取查詢編輯器 v2](#)。
- 您的問題必須以英文撰寫。
- 您的問題必須參考叢集或工作群組中已連接的資料庫。為了避免空白狀態錯誤，應該有至少一個資料表和資料庫中的一些資料。
- 您的問題必須參照儲存在連線資料庫中的資料。但無法參考外部結構描述。如需受支援之結構描述的詳細資訊，請參閱 Amazon Redshift 資料庫開發人員指南中的 [建立結構描述](#)。

- 任何導致 SQL 變更連線資料庫的問題,都可能會產生警告。
- 生成式 AI 技術是一種新穎的技術,在反應中可能會出現錯誤,有時也稱為幻覺。在您的環境或工作負載中使用之前,請先測試並檢閱所有程式碼是否有錯誤和漏洞。
- 您可以透過帳戶中其他使用者執行來分享 SQL 查詢,以改善建議。您的帳戶管理員可以執行下列 SQL 命令,以允許存取帳戶的查詢歷程記錄。

```
GRANT ROLE SYS:MONITOR to "IAMR:role-name";  
GRANT ROLE SYS:MONITOR to "IAM:user-name";  
GRANT ROLE SYS:MONITOR to "database-username";
```

如需有關 SYS:MONITOR 的詳細資訊,請參閱 Amazon Redshift 資料庫開發人員指南中的 [Amazon Redshift 系統定義角色](#)。

- 您的資料是安全和私有的。您的資料不會跨帳戶共用。您的查詢、資料和資料庫結構描述不會用於訓練生成式 AI 基礎模型 (FM)。您的輸入會用作 FM 的上下文提示詞,僅做為對您的查詢的回答。

使用生成式 SQL

設定正確的許可權後,在查詢編輯器 v2 中使用筆記本時,您可以選擇圖示來開始對話。

若要與查詢編輯器 v2 生成式 SQL 聊天功能進行互動以產生 SQL

1. 在查詢編輯器 v2 的編輯器索引標籤中,開啟筆記本。
2. 選擇



生成式 SQL 圖示,然後按照指令在聊天面板中詢問您對 Amazon Redshift 查詢編輯器 v2 生成式 SQL 的問題。

您在提示欄位中提供問題,查詢編輯器 v2 會使用建議的 SQL 來回應。遇到的任何錯誤,都會在聊天面板中傳回給您。

3. 選擇新增至筆記本,新增 Markdown 儲存格與您的提示,以及含有建議 SQL 的 SQL 儲存格以加入至您的筆記本。
4. (選用) 選擇重新產生 SQL,為相同的提示產生另一個回應。您可以選擇為目前的提示重新產生 SQL 一次。
5. (選用) 在生成式 SQL 聊天面板中,選擇



更多圖示，然後選擇重新整理資料庫以重新整理描述已連線之資料庫的中繼資料。此中繼資料包括資料庫中結構描述定義、資料表和欄的定義。

以管理員身分更新生成式 SQL 設定

具有正確 IAM 許可的使用者可以檢視和變更相同 AWS 帳戶中其他使用者的生成式 SQL 設定。除了查詢編輯器 v2 的受管政策中指定的其他許可 `sqlworkbench:UpdateAccountQSqlSettings` 外，此 AWS 管理員還必須在其 IAM 政策中擁有權限。如需受管政策的詳細資訊，請參閱 [要使用查詢編輯器 v2 所需的許可](#)。

讓系統管理員為帳戶中的所有使用者開啟生成式 SQL 聊天

1. 選擇



設定圖示以顯示不同設定畫面的選單。

2. 然後選擇



生成式 SQL 設定圖示，以顯示生成式 SQL 設定頁面。

3. 選取生成式 SQL，為帳戶中的使用者開啟生成式 SQL 功能。

搭配 TICKIT 資料使用 Amazon Q 生成式 SQL 功能的範例

若要撰寫生成式 SQL 的有效提示詞，您必須了解您的資料庫結構描述和資料。TICKIT 資料包含七個資料表：兩個事實資料表和五個維度資料表。範例資料包含 2008 年發生之娛樂活動服務員銷售的相關記錄。如需 TICKIT 資料結構描述的詳細資訊，請參閱 Amazon Redshift 資料庫開發人員指南中的 [範例資料庫](#)。您可以透過 Amazon Redshift 主控台和查詢編輯器 v2 中的各種方法，將 TICKIT 資料載入資料庫。查詢編輯器 v2 提供一種將 TICKIT 資料載入資料庫 `sample_data_dev` 的方法。如需相關資訊，請參閱 [載入範例資料](#)。查詢編輯器 v2 也提供 TICKIT 資料的範例提示。下列案例說明與生成式 SQL 的對話，以產生有關 TICKIT 範例資料的 SQL。在這個案例中，TICKIT 範例資料已經建立於 Amazon Redshift 叢集的 dev 資料庫中。

Note

這個範例是有關對話的圖解。生成式 SQL 的回應可能不符合使用相同提示詞的結果。

與查詢編輯器 v2 生成式 SQL 對話的範例

1. 在編輯器中，連接至包含 TICKIT 範例資料的叢集或工作群組。
2. 建立空白筆記本，然後選擇



生成式 SQL 圖示以開啟聊天面板。

3. 輸入以下提示以產生 SQL，以驗證 VENUE 資料表中的記錄數：

```
How many venues are there?
```

```
SELECT
  COUNT(*) AS num_venues
FROM
  tickit.venue
```

選擇新增至筆記本，新增兩個儲存格至開啟的筆記本。一個 Markdown 儲存格「有多少個會場？」和一個包含生成式 SQL。

在 SQL 儲存格中，選擇執行以接收結果：

```
count
-----
202
```

4. 若要請求其他版本的 SQL，請選擇重新產生 SQL 並接收下列答案：

```
SELECT
  venuestate,
  COUNT(*) AS num_venues
FROM
  tickit.venue
GROUP BY
  venuestate
```

選擇新增至筆記本，多新增兩個儲存格至開啟的筆記本。一個 Markdown 儲存格「有多少個會場？」和一個包含生成式 SQL。

在 SQL 儲存格中，選擇執行以按編號接收列出會場狀態的結果：

```

venuestate num_venues
-----
MA          4
OH          8
MI          5
...

```

5. 生成式 SQL 助理可以假設您請求的內容。儘管資料庫中沒有小工具，但您仍然可以詢問。在這種情況下，它會提供你一條訊息，表示無法產生 SQL。

```
How many widgets are there?
```

```
I was not able to generate any SQL
```

6. 當您了解更多有關資料庫的資訊時，可以提出更具體的問題來產生 SQL。例如，您知道資料庫包含 2008 年中幾個月份的銷售資料。輸入下列提示詞以產生 SQL，尋找 2008 年 11 月的銷售數量：

```
How many sales were there in November 2008?
```

```

SELECT
  COUNT(*) AS num_sales
FROM
  tickit.sales s
  JOIN tickit.date d ON s.dateid = d.dateid
WHERE
  d.month = 'November'
  AND d.year = 2008

```

選擇新增至筆記本，新增兩個儲存格至開啟的筆記本。一個 Markdown 儲存格「2008 年 11 月有多少銷量？」和一個包含生成式 SQL。

在 SQL 儲存格中，選擇執行以接收結果：

```

num_sales
-----

```

```
0
```

您了解到這不是您期望的結果。

7. 您注意到述詞 `date.month='November'` 預期 DATE 資料表中的月份會以月份名稱縮寫來表示。您可以將述詞變更為 `d.month='NOV'` 並重新執行 SQL。

```
SELECT
  COUNT(*)
FROM
  sales
  JOIN date ON sales.dateid = date.dateid
WHERE
  date.month = 'NOV'
  AND date.year = 2008
```

在 SQL 儲存格中，選擇執行以取得新結果。

```
count
-----
14261
```

8. 如果您問的問題會嘗試變更連線的資料庫，則會傳回警告訊息以及任何建議的 SQL。輸入下列提示詞以產生 SQL，將資料插入資料表：

```
Insert 1 into the venue table.
```

```
INSERT
,
UPDATE
  OR delete data
FROM
  the database AS that could potentially change the data.Please provide a query
  that ONLY selects data
```

```
I was not able to generate the correct SQL code. I generated SQL, but you'll have
to edit it to work with your database.
```

如果您選擇新增至筆記本，將兩個儲存格新增至開啟的筆記本，並執行 SQL，然後 SQL 會失敗。

```
ERROR: syntax error at or near "," Position: 132 [ErrorId:
1-6546764a-011df2691778846219ce6ec2]
```

這個案例只說明了與查詢編輯器 v2 生成式 SQL 互動的一些基本方法。您可以使用這種生成式 AI 技術進行更多實驗，幫助您開始編寫 SQL 來查詢資料庫。

將資料載入到資料庫

您可以使用查詢編輯器 v2 將資料載入到 Amazon Redshift 叢集或工作群組中的資料庫。

載入範例資料

查詢編輯器 v2 隨附範例資料和筆記本，可供您載入到範例資料庫和對應的結構描述。

若要載入範例資料，請選擇與您要載入的範例資料相關聯的



圖示。然後，查詢編輯器 v2 便會將資料載入到資料庫 `sample_data_dev` 中的結構描述，並在 Notebooks 資料夾中建立已儲存筆記本的資料夾。

以下是可用的範例資料集。

tickit

Amazon Redshift 文件中的多數範例都使用名為 `tickit` 的範本資料。這份資料包含七個資料表：兩個事實資料表和五個維度資料表。在載入這份資料時，系統便會以範例資料更新結構描述 `tickit`。如需 `tickit` 資料的相關資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的 [範例資料庫](#)。

tpch

這份資料會用於決策支援基準。在載入這份資料時，系統便會以範例資料更新結構描述 `tpch`。如需 `tpch` 資料的相關資訊，請參閱 [TPC-H](#)。

tpcds

這份資料會用於決策支援基準。在載入這份資料時，系統便會以範例資料更新結構描述 `tpcds`。如需 `tpcds` 資料的相關資訊，請參閱 [TPC-DS](#)。

從 Amazon S3 載入資料

您可以將 Amazon S3 資料載入到現有資料表或新的資料表。

將資料載入到現有資料表

查詢編輯器 v2 會使用 COPY 命令從 Amazon S3 載入資料。在查詢編輯器 v2 載入資料精靈中產生和使用的 COPY 命令，支援許多可供 COPY 命令語法從 Amazon S3 進行複製的參數。如需 COPY 命令及其用於從 Amazon S3 載入資料之選項的詳細資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的[從 Amazon Simple Storage Service 進行 COPY](#)。

1. 確認您要將資料載入到其中的資料庫內已建立資料表。
2. 確認您已連線至查詢編輯器 v2 的樹狀檢視面板中的目標資料庫後再繼續。您可以使用內容功能表 (按一下滑鼠右鍵) 對要在其中載入資料的叢集或工作群組建立連線。

選擇



載入資料。

3. 對於資料來源，選擇從 S3 儲存貯體載入。
4. 在 S3 URI 中選擇瀏覽 S3，以尋找要載入的資料所在的 Amazon S3 儲存貯體。
5. 如果指定的 Amazon S3 儲存貯體與目標資料表不同 AWS 區域，請選擇資料所在位 AWS 區域 置的 S3 檔案位置。
6. 如果 Amazon S3 檔案實際上是包含多個 Amazon S3 儲存貯體 URI 的資訊清單，請選擇此檔案是資訊清單檔案。
7. 為要上傳的檔案選擇檔案格式。支援的資料格式有 CSV、JSON、DELIMITER、FIXEDWIDTH、SHAPEFILE、AVRO、PARQUET 和 ORC。根據指定的檔案格式，您可以選擇相應的檔案選項。如果資料有加密，您也可以選取資料已加密，然後輸入用來加密資料之 KMS 金鑰的 Amazon Resource Name (ARN)。

如果您選擇 CSV 或 DELIMITER」，則也可以選擇分隔符號字元，以及是否要忽略標頭資料列 (如果指定的資料列數目實際上是資料欄名稱而非要載入的資料)。

8. 選擇壓縮方法來壓縮檔案。預設為沒有壓縮。
9. (選擇性) 進階設定支援各種資料轉換參數和載入操作。視需要為您的檔案輸入此資訊。

如需資料轉換和資料載入參數的相關資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的[資料轉換參數](#)和[資料載入操作](#)。

10. 選擇下一步。

11. 選擇載入現有資料表。
12. 確認或選擇在其中載入資料的目標資料表的位置，包括叢集或工作群組、資料庫、結構描述以及資料表名稱。
13. 選擇具有從 Amazon S3 載入資料所需許可的 IAM 角色。
14. (選擇性) 選擇資料欄名稱，在資料欄映射中輸入以依照輸入資料檔案的順序映射資料欄。
15. 選擇載入資料以開始載入資料。

當載入完成時，查詢編輯器會顯示所產生來載入資料的 COPY 命令。系統會顯示 COPY 的結果。如果成功，您便可立即使用 SQL 從所載入的資料表中選取資料。如果發生錯誤，請查詢系統檢視 STL_LOAD_ERRORS 以取得更多詳細資訊。如需有關 COPY 命令錯誤的資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的 [STL_LOAD_ERRORS](#)。

當您將資料載入到新的資料表時，查詢編輯器 v2 會先在資料庫中建立資料表，再於相同工作流程中以個別動作的形式載入資料。

將資料載入到新的資料表

查詢編輯器 v2 會使用 COPY 命令從 Amazon S3 載入資料。在查詢編輯器 v2 載入資料精靈中產生和使用的 COPY 命令，支援許多可供 COPY 命令語法從 Amazon S3 進行複製的參數。如需 COPY 命令及其用於從 Amazon S3 載入資料之選項的詳細資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的 [從 Amazon Simple Storage Service 進行 COPY](#)。

1. 確認您已連線至查詢編輯器 v2 的樹狀檢視面板中的目標資料庫後再繼續。您可以使用內容功能表 (按一下滑鼠右鍵) 對要在其中載入資料的叢集或工作群組建立連線。

選擇



載入資料。

2. 對於資料來源，選擇從 S3 儲存貯體載入。
3. 在 S3 URI 中選擇瀏覽 S3，以尋找要載入的資料所在的 Amazon S3 儲存貯體。
4. 如果指定的 Amazon S3 儲存貯體與目標資料表不同 AWS 區域，請選擇資料所在位 AWS 區域 置的 S3 檔案位置。
5. 如果 Amazon S3 檔案實際上是包含多個 Amazon S3 儲存貯體 URI 的資訊清單，請選擇此檔案是 資訊清單檔案。
6. 為要上傳的檔案選擇檔案格式。支援的資料格式有 CSV、JSON、DELIMITER、FIXEDWIDTH、SHAPEFILE、AVRO、PARQUET 和 ORC。根據

指定的檔案格式，您可以選擇相應的檔案選項。如果資料有加密，您也可以選取資料已加密，然後輸入用來加密資料之 KMS 金鑰的 Amazon Resource Name (ARN)。

如果您選擇 CSV 或 DELIMITER」，則也可以選擇分隔符號字元，以及是否要忽略標頭資料列 (如果指定的資料列數目實際上是資料欄名稱而非要載入的資料)。

7. 選擇壓縮方法來壓縮檔案。預設為沒有壓縮。
8. (選擇性) 進階設定支援各種資料轉換參數和載入操作。視需要為您的檔案輸入此資訊。

如需資料轉換和資料載入參數的相關資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的[資料轉換參數](#)和[資料載入操作](#)。

9. 選擇下一步。
10. 選擇載入新資料表。

資料表資料欄會從輸入資料推斷而來。您可以透過新增資料欄和資料表詳細資訊，修改資料表結構描述的定義。若要還原至查詢編輯器 v2 推斷的資料表結構描述，請選擇還原為預設值。

11. 確認或選擇在其中載入資料的目標資料表的位置，包括叢集或工作群組、資料庫和結構描述。輸入要建立的資料表名稱。
12. 選擇具有從 Amazon S3 載入資料所需許可的 IAM 角色。
13. 選擇建立資料表，使用所顯示的定義建立資料表。

此時會顯示資料表定義的檢閱摘要。資料表會建立到資料庫中。稍後若要刪除資料表，請執行 DROP TABLE SQL 命令。如需詳細資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的[DROP TABLE](#)。

14. 選擇載入資料以開始載入資料。

當載入完成時，查詢編輯器會顯示所產生來載入資料的 COPY 命令。系統會顯示 COPY 的結果。如果成功，您便可立即使用 SQL 從所載入的資料表中選取資料。如果發生錯誤，請查詢系統檢視 STL_LOAD_ERRORS 以取得更多詳細資訊。如需有關 COPY 命令錯誤的資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的[STL_LOAD_ERRORS](#)。

從本機檔案設定和工作流程載入資料

您可以將資料從本機檔案載入到現有資料表或新的資料表。

從本機檔案載入資料的管理員設定

您的查詢編輯器 v2 管理員必須在帳戶設定視窗中指定常用的 Amazon S3 儲存貯體。您必須已為帳戶使用者設定適當的許可。

- 必要的 IAM 許可 — 從本機檔案載入資料的使用者必須具有 `s3:ListBucket`、`s3:GetBucketLocation`、`s3:putObject`、`s3:getObject` 和 `s3:deleteObject` 許可。您可以指定 *optional-prefix*，以限制只有具有此字首的物件能透過查詢編輯器 v2 使用此儲存貯體。如果您透過查詢編輯器 v2 以外的工具使用這個相同的 Amazon S3 儲存貯體，便可以使用此選項。如需儲存貯體和字首的相關資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的[管理使用者對特定資料夾的存取](#)。為了確保系統不會允許跨使用者的資料存取，建議查詢編輯器 v2 管理員使用 Amazon S3 儲存貯體政策來根據 `aws:userid` 限制物件的存取。下列範例會向字首為 `aws:userid` 的 Amazon S3 物件允許具有唯讀/唯寫存取權限的 *<staging-bucket-name>* Amazon S3 許可。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource": [
        "arn:aws:s3:::<staging-bucket-name>"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource": [
        "arn:aws:s3:::<staging-bucket-name>[/<optional-prefix>]/"
        "${aws:userid}/*"
      ]
    }
  ]
}
```

```
}

```

- 資料分隔 — 建議不要讓使用者擁有存取彼此資料的權限 (即使很短暫也不行)。從本機檔案載入的方式會使用查詢編輯器 v2 管理員所設定的暫存 Amazon S3 儲存貯體。請設定暫存儲存貯體的儲存貯體政策，以在使用者之間提供資料分隔機制。下列範例顯示的儲存貯體政策會在 *<staging-bucket-name>* 的使用者之間分隔資料。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "userIdPolicy",
      "Effect": "Deny",
      "Principal": "*",
      "Action": ["s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"],
      "NotResource": [
        "arn:aws:s3:::<staging-bucket-name>[/<optional-prefix>]/
        ${aws:userid}/*"
      ]
    }
  ]
}
```

從本機檔案載入資料

將本機檔案的資料載入到現有資料表

查詢編輯器 v2 管理員必須在帳戶設定視窗中指定通用的 Amazon S3 儲存貯體。查詢編輯器 v2 會自動將本機檔案上傳到您帳戶使用的通用 Amazon S3 儲存貯體，然後使用 COPY 命令載入資料。查詢編輯器 v2 的載入本機檔案視窗所產生和執行的 COPY 命令，支援許多可供 COPY 命令語法從 Amazon S3 進行複製的參數。如需 COPY 命令及其用於從 Amazon S3 載入資料之選項的詳細資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的[從 Amazon S3 進行 COPY](#)。

1. 確認您要將資料載入到其中的資料庫內已建立資料表。
2. 確認您已連線至查詢編輯器 v2 的樹狀檢視面板中的目標資料庫。您可以使用內容功能表 (按一下滑鼠右鍵) 對要在其中載入資料的叢集或工作群組建立連線。

3. 選擇



載入資料。

4. 對於資料來源，選擇從本機檔案載入。
5. 選擇瀏覽以尋找包含要載入檔案之資料的檔案。依預設，系統會顯示副檔名為 .csv、.avro、.parquet 和 .orc 的檔案，但您也可以選擇其他檔案類型。檔案大小上限為 100 MB。
6. 為要上傳的檔案選擇檔案格式。支援的資料格式有 CSV、JSON、DELIMITER、FIXEDWIDTH、SHAPEFILE、AVRO、PARQUET 和 ORC。根據指定的檔案格式，您可以選擇相應的檔案選項。如果資料有加密，您也可以選取資料已加密，然後輸入用來加密資料之 KMS 金鑰的 Amazon Resource Name (ARN)。

如果您選擇 CSV 或 DELIMITER，則也可以選擇分隔符號字元，以及是否要忽略標頭資料列 (如果指定的資料列數目實際上是資料欄名稱而非要載入的資料)。

7. (選擇性) 進階設定支援各種資料轉換參數和載入操作。視需要為您的檔案輸入此資訊。

如需資料轉換和資料載入參數的相關資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的[資料轉換參數](#)和[資料載入操作](#)。

8. 選擇下一步。
9. 選擇載入現有資料表。
10. 確認或選擇在其中載入資料的目標資料表的位置，包括叢集或工作群組、資料庫、結構描述以及資料表名稱。
11. (選擇性) 您可以選擇資料欄名稱，在資料欄映射中輸入以依照輸入資料檔案的順序映射資料欄。
12. 選擇載入資料以開始載入資料。


載入完成時，無論載入是否成功，系統都會顯示訊息。如果成功，您便可立即使用 SQL 從所載入的資料表中選取資料。如果發生錯誤，請查詢系統檢視 STL_LOAD_ERRORS 以取得更多詳細資訊。如需有關 COPY 命令錯誤的資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的[STL_LOAD_ERRORS](#)。

用來載入資料的 COPY 命令範本會出現在您的查詢歷史記錄中。此 COPY 命令範本會顯示一些已使用的參數，但其無法直接在編輯器索引標籤中執行。如需查詢歷史記錄的相關資訊，請參閱[檢視查詢和標籤歷史記錄](#)。

當您將資料載入到新的資料表時，查詢編輯器 v2 會先在資料庫中建立資料表，再於相同工作流程中以個別動作的形式載入資料。

將本機檔案資料載入到新的資料表

您的查詢編輯器 v2 管理員必須在帳戶設定視窗中指定常用的 Amazon S3 儲存貯體。本機檔案會自動上傳到您帳戶使用的通用 Amazon S3 儲存貯體，然後查詢編輯器 v2 會使用 COPY 命令載入資料。查詢編輯器 v2 的載入本機檔案視窗所產生和執行的 COPY 命令，支援許多可供 COPY 命令語法從 Amazon S3 進行複製的參數。如需 COPY 命令及其用於從 Amazon S3 載入資料之選項的詳細資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的[從 Amazon S3 進行 COPY](#)。

1. 確認您已連線至查詢編輯器 v2 的樹狀檢視面板中的目標資料庫。您可以使用內容功能表 (按一下滑鼠右鍵) 對要在其中載入資料的叢集或工作群組建立連線。
2. 選擇  載入資料。
3. 對於資料來源，選擇從本機檔案載入。
4. 選擇瀏覽以尋找包含要載入檔案之資料的檔案。依預設，系統會顯示副檔名為 .csv、.avro、.parquet 和 .orc 的檔案，但您也可以選擇其他檔案類型。檔案大小上限為 100 MB。
5. 為要上傳的檔案選擇檔案格式。支援的資料格式有 CSV、JSON、DELIMITER、FIXEDWIDTH、SHAPEFILE、AVRO、PARQUET 和 ORC。根據指定的檔案格式，您可以選擇相應的檔案選項。如果資料有加密，您也可以選取資料已加密，然後輸入用來加密資料之 KMS 金鑰的 Amazon Resource Name (ARN)。如果您選擇 CSV 或 DELIMITER，則也可以選擇分隔符號字元，以及是否要忽略標頭資料列 (如果指定的資料列數目實際上是資料欄名稱而非要載入的資料)。
6. (選擇性) 進階設定支援各種資料轉換參數和載入操作。視需要為您的檔案輸入此資訊。如需資料轉換和資料載入參數的相關資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的[資料轉換參數](#)和[資料載入操作](#)。
7. 選擇下一步。
8. 選擇載入新資料表。
9. 確認或選擇在其中載入資料的目標資料表的位置，包括叢集或工作群組、資料庫和結構描述。輸入要建立的資料表名稱。
10. 選擇建立資料表，使用所顯示的定義建立資料表。

此時會顯示資料表定義的檢閱摘要。資料表會建立到資料庫中。稍後若要刪除資料表，請執行 `DROP TABLE SQL` 命令。如需詳細資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的 [DROP TABLE](#)。

11. 選擇載入資料以開始載入資料。

載入完成時，會顯示訊息以指出載入是否成功。如果成功，您便可立即使用 SQL 從所載入的資料表中選取資料。如果發生錯誤，請查詢系統檢視 `STL_LOAD_ERRORS` 以取得更多詳細資訊。如需有關 `COPY` 命令錯誤的資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的 [STL_LOAD_ERRORS](#)。

用來載入資料的 `COPY` 命令範本會出現在您的查詢歷史記錄中。此 `COPY` 命令範本會顯示一些已使用的參數，但其無法直接在編輯器索引標籤中執行。如需查詢歷史記錄的相關資訊，請參閱[檢視查詢和標籤歷史記錄](#)。

編寫和執行查詢

您可以在編輯器中輸入查詢，或從查詢清單中選取已儲存的查詢，然後選擇執行。

系統預設會設定限制 100 個以將結果限制為 100 個資料列。您可以關閉此選項，以傳回較大的結果集。如果您關閉這個選項，又想要避免結果集太大，則可以在 SQL 陳述式中包含 `LIMIT` 選項。如需詳細資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的 [ORDER BY 子句](#)。

若要在結果區域中顯示查詢計劃，請開啟解釋。開啟解釋圖形，讓結果也顯示以圖形表示的解釋計劃。

若要將查詢儲存至查詢資料夾，請選擇儲存。

如果查詢成功，則會出現成功訊息。如果查詢傳回資訊，結果會顯示在結果區段中。如果結果數目超過顯示區域，結果區域的頂端會出現數字。您可以選擇數字以顯示連續的結果頁面。

您可以為每個資料欄篩選和排序結果。若要在結果資料欄標頭中輸入篩選條件，請將游標暫留在該資料欄上，以查看可供您輸入資料欄篩選條件的選單

()。

如果查詢中包含錯誤，查詢編輯器 v2 會在結果區域中顯示錯誤訊息。該訊息會提供有關如何更正查詢的資訊。

您可以在結果區域中使用內容 (右鍵) 選單來匯出或複製查詢結果，如下所示：

- 選擇匯出結果集和 JSON 或 CSV，以將整組資料列結果下載至檔案。結果集內的資料列數目可能會受限於查詢中的限制選項或 SQL limit 子句。所下載結果集的大小上限為 5 MB。
- 如果未選取任何資料列，請選擇匯出目前頁面和 JSON 或 CSV，以將資料列從目前頁面下載至檔案。
- 如果已選取資料列，請選擇匯出選取的資料列和 JSON 或 CSV，以將選取的資料列下載至檔案。
- 如果已選取資料列，則請選擇複製資料列，以將選取的資料列複製到剪貼簿。
- 如果已選取資料列，則請選擇複製具有標頭的資料列，以將具有資料欄標頭的所選資料列複製到剪貼簿。

您也可以使用 Windows 上的快速鍵 Ctrl+C 或 macOS 上的 Cmd+C 將資料從目前的結果頁面複製到剪貼簿。如果未選取任何資料列，則會將焦點所在的儲存格複製到剪貼簿。如果已選取資料列，則會將選取的資料列複製到剪貼簿。

若要新增查詢標籤，請選擇



圖示，然後選擇編輯器，其會出現在具有查詢標籤的資料列中。查詢標籤不一定會使用 Isolated session。使用隔離工作階段時，SQL 命令的結果 (例如，在某個編輯器標籤中建立暫存資料表) 無法在另一個編輯器標籤中看到。當您在查詢編輯器 v2 中開啟編輯器標籤時，預設會使用隔離工作階段。

若要執行查詢

1. 在查詢區域中，執行以下其中一項操作：
 - 輸入查詢。
 - 貼上您複製的查詢。
 - 選擇查詢資料夾、開啟內容選單 (右鍵) 儲存的查詢，然後選擇開啟查詢。
2. 確認您已為打算執行的 SQL 選擇了正確的叢集或工作群組和資料庫值。

最初，您可以在樹狀檢視中選擇叢集或工作群組。也請在樹狀檢視中選擇資料庫。

您可以使用每個編輯器標籤的隔離工作階段標頭附近的下拉式控制項，在每個編輯器標籤內變更叢集或工作群組和資料庫。

對於每個編輯器標籤，您要選擇是否要在隔離工作階段中執行 SQL。隔離工作階段有自己的資料庫連線。請使用該連線來執行與其他查詢編輯器工作階段隔離的 SQL。如需連線的相關資訊，請參閱[開啟查詢編輯器 v2](#)。

3. 選擇執行。

隨即會開啟結果區域，並顯示查詢結果。

顯示查詢的解釋計劃

1. 選取查詢。
2. 開啟解釋。

預設也會開啟解釋圖形。

3. 選擇執行。

查詢便會開始執行，解釋計劃則會顯示在查詢的結果區域中。

查詢編輯器 v2 支援以下功能：

- 您可以在一個查詢標籤中使用多個 SQL 陳述式編寫查詢。系統會依序執行查詢，並針對每個查詢開啟多個結果標籤。
- 您可以使用工作階段變數和暫存資料表編寫查詢。
- 您可以使用以 `${parameter}` 指定的可取代參數來編寫查詢。您可以使用多個可取代參數來編寫 SQL 查詢，並在 SQL 陳述式中的多個位置使用相同的參數。

在執行查詢時，系統會顯示一個視窗供您輸入參數值。每次執行查詢時，系統都會顯示視窗供您輸入參數值。

如需範例，請參閱[範例：銷售額大於特定參數](#)。

- 系統會自動為查詢建立版本。您可以選擇較早的查詢版本來執行。
- 不需要等待查詢完成，就能繼續您的工作流程。即使您關閉查詢編輯器，查詢仍會繼續執行。
- 在編寫查詢時，系統支援自動完成結構描述、資料表和資料欄名稱。

SQL 編輯器支援以下功能：

- SQL 中使用的開始和結束括號具有相符的顏色。編輯器中會顯示垂直線以幫助您讓括號相符。
- 您可以收合和展開 SQL 的各個部分。
- 您可以搜尋和取代 SQL 中的文字。
- 您可以使用快速鍵來執行數個常見的編輯任務。
- 編輯器中會反白顯示 SQL 錯誤，以方便您找到問題所在區域。

如需編輯功能的示範，請觀看下列影片：[Amazon Redshift 查詢編輯器 v2 中的全新和增強編輯體驗](#)。

查詢範例

您可以在下面找到可以執行的各種查詢類型的描述。

其中許多查詢所使用的資料來自 tickit 範例結構描述。如需載入範例 tickit 資料的相關資訊，請參閱[載入範例資料](#)。如需 tickit 範例資料的相關資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的[範例資料庫](#)。

當您執行這些範例查詢時，請確認您在編輯器中選擇了正確的資料庫，例如 sample_data_dev。

主題

- [範例：設定工作階段變數](#)
- [範例：按總銷售額排序的最佳活動](#)
- [範例：銷售額大於特定參數](#)
- [範例：建立暫存資料表](#)
- [範例：從暫存資料表中選取](#)

範例：設定工作階段變數

下列命令會針對工作階段將 search_path 伺服器組態參數設定為「public」。如需詳細資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的[SET](#) 和 [search_path](#)。

```
set search_path to public;
```

範例：按總銷售額排序的最佳活動

下列查詢會尋找銷售額最多的活動。

```
select eventname, count(salesid) totalorders, sum(pricepaid) totalsales
from sales, event
where sales.eventid=event.eventid
group by eventname
order by 3;
```

以下是結果的部分清單。

eventname	totalorders	totalsales
-----------	-------------	------------

White Christmas	20	9352
Joshua Radin	38	23469
Beach Boys	58	30383
Linda Ronstadt	56	35043
Rascal Flatts	76	38214
Billy Idol	67	40101
Stephenie Meyer	72	41509
Indigo Girls	57	45399
...		

範例：銷售額大於特定參數

下列查詢會尋找銷量大於 `${numberoforders}` 所指定參數的銷售額。當參數值為 7 時，結果有 60 列。當您執行查詢時，查詢編輯器 v2 會顯示執行查詢表單視窗，以收集 SQL 陳述式中的參數值。

```
select salesid, qtysold
from sales
where qtysold > ${numberoforders}
order by 2;
```

以下是結果的部分清單。

```
salesid qtysold
20005 8
21279 8
130232 8
42737 8
74681 8
67103 8
105533 8
91620 8
121552 8
...
```

範例：建立暫存資料表

下列陳述式會透過選取「sales」和「event」資料表中的資訊來建立暫存資料表「eventsalestemp」。

```
create temporary table eventsalestemp as
select eventname, count(salesid) totalorders, sum(pricepaid) totalsales
from sales, event
where sales.eventid=event.eventid
```

```
group by eventname;
```

範例：從暫存資料表中選取

下列陳述式會從按訂單總量排序的暫存資料表「eventsalestemp」中選取活動、訂單總量和銷售總額。

```
select eventname, totalorders, totalsales
from eventsalestemp
order by 2;
```

以下是結果的部分清單。

eventname	totalorders	totalsales
White Christmas	20	9352
Joshua Radin	38	23469
Martina McBride	50	52932
Linda Ronstadt	56	35043
Indigo Girls	57	45399
Beach Boys	58	30383
...		

編寫和執行筆記本

您可以使用筆記本在單一文件中組織、註釋和共用多個 SQL 查詢。您可以將多個 SQL 查詢和 Markdown 儲存格新增至筆記本。筆記本可讓您透過使用多個查詢和 Markdown 儲存格，將與資料分析相關聯的查詢和說明分組到單一文件中。您可以使用 Markdown 語法新增文字並設定外觀格式，以提供資料分析任務的內容和其他資訊。您可以與團隊成員共用筆記本。

若要使用筆記本，您必須將筆記本的許可新增至 IAM 主體 (IAM 使用者或 IAM 角色)。我們建議的最佳實務是，將許可政策附加到 IAM 角色，然後根據需要將其指派給使用者和群組。如需詳細資訊，請參閱 [Amazon Redshift 中的身分和存取管理](#)。您可以將許可新增至其中一個查詢編輯器 v2 受管政策。如需詳細資訊，請參閱 [存取查詢編輯器 v2](#)。

您可以循序執行筆記本的所有儲存格。筆記本的 SQL 查詢儲存格與查詢編輯器索引標籤的功能大多相同。如需詳細資訊，請參閱 [編寫和執行查詢](#)。以下是查詢編輯器索引標籤與筆記本中的 SQL 儲存格之間的差異。

- 沒有控制項可以在筆記本中的 SQL 陳述式上執行 Explain。
- 在筆記本中，每個 SQL 儲存格只能建立一個圖表。

您可以將筆記本匯出和匯入至使用查詢編輯器 v2 建立的檔案。檔案的副檔名為 .ipynb，檔案大小最多可以為 5 MB。SQL 和 Markdown 儲存格會存放在檔案中。叢集或工作群組與資料庫不會存放在匯出的筆記本中。當您開啟匯入的筆記本時，您要選擇叢集或工作群組，以及要在其中執行叢集或工作群組的資料庫。執行 SQL 儲存格之後，您便可以在結果索引標籤中選擇是否要將目前的結果頁面顯示為圖表。查詢的結果集不會存放在筆記本中。

當您使用全部執行或執行以執行筆記本時，執行狀態面板就會變成可用的狀態。選擇



圖示開啟面板。此面板包含筆記本中 SQL 儲存格的最新全部執行或執行狀態摘要。如果您執行多個 SQL 儲存格，您可以一目了然地檢視狀態、歷經時間以及有關執行的一些詳細資訊。您可以根據狀態篩選顯示的儲存格：All、Succeeded、Error、In progress 或 Canceled。您也可以使用此面板導覽至編輯器中的 SQL 儲存格。

若要建立筆記本

1. 從導覽器功能表中選擇



編輯器。

2. 選擇



然後選擇筆記本。

根據預設，SQL 查詢儲存格會出現在筆記本中。

3. 在 SQL 查詢儲存格中，執行以下其中一項操作：

- 輸入查詢。
- 貼上您複製的查詢。

4. (選擇性) 選擇



圖示，然後選擇 Markdown 以新增 Markdown 儲存格，您可以在其中使用標準 Markdown 語法提供描述性或說明性的文字。

5. (選擇性) 選擇



圖示，然後選擇 SQL 以插入 SQL 儲存格。

您可以使用



(鉛筆) 圖示重新命名筆記本。

從



(更多) 功能表中，您也可以在此筆記本上執行下列操作：



與我的團隊共用 — 依標籤所定義與您的團隊共用筆記本。如需更多資訊，請參閱 [共用查詢](#)



匯出 — 將筆記本匯出至副檔名為 `.ipynb` 的本機檔案。



儲存版本 — 建立筆記本的版本。若要查看筆記本的版本，請導覽至已儲存的筆記本，然後開啟版本歷史記錄。



複製 — 建立筆記本的副本，並在新的筆記本索引標籤中開啟它。



捷徑 — 在編寫筆記本時顯示可用的捷徑。

開啟已儲存的筆記本

1. 從導覽器功能表中選擇



筆記本。隨即會顯示您儲存的筆記本和筆記本資料夾。

2. 選擇您想要開啟的筆記本，然後按兩下該筆記本。

您可以在筆記本索引標籤中顯示我的筆記本、由我共用的筆記本，以及共用給我的團隊的筆記本。

若要將筆記本從本機檔案匯入我的筆記本，請選擇



匯入，然後導覽至包含筆記本的 .ipynb 檔案。筆記本會匯入到目前開啟的筆記本資料夾。您接著可以在筆記本編輯器中開啟筆記本。

您可以從筆記本的內容功能表 (按一下滑鼠右鍵) 執行下列操作：

- 開啟筆記本 — 在編輯器中開啟筆記本。
- 儲存版本 — 儲存筆記本的版本。
- 版本歷史記錄 — 顯示筆記本的版本。您可以從版本歷史記錄視窗中刪除和還原版本。您也可以從目前選取的版本建立筆記本。
- 編輯標籤 — 在筆記本上建立和編輯標籤。
- 與我的團隊共用 — 與您的團隊共用筆記本。

若要與團隊共用筆記本，請確定您已將主體標籤 `sqlworkbench-team` 設定為與帳戶中其他團隊成員相同的值。例如，管理員可以針對會計部門中的每個人，將值設定為 `accounting-team`。如需範例，請參閱 [要使用查詢編輯器 v2 所需的許可](#)。

- 匯出 — 將筆記本匯出至本機檔案。
- 重新命名 — 重新命名筆記本。
- 複製 — 製作筆記本的副本。
- 刪除 — 刪除筆記本。

如需筆記本的示範，請觀看下列影片：[查詢編輯器 v2 中的 Amazon Redshift SQL 筆記本](#)。

查詢 AWS Glue Data Catalog

您可以使用查詢編輯器 v2 來查詢 AWS Glue Data Catalog 中所編目的資料。依預設，會列 AWS Glue Data Catalog 為名為的查詢編輯器 v2 資料庫 `awsdatacatalog`。並非所有 Amazon Redshift AWS 區域都提供查詢。AWS Glue Data Catalog 請使用 `SHOW` 命令來判斷此功能是否可用。如需有關的詳細資訊 AWS Glue，請參閱 [什麼是 AWS Glue?](#) 在 AWS Glue 開發人員指南中。

Note

只有在 Amazon Redshift RA3 節點類型叢集和亞 Amazon Redshift 無伺服器中才支援查詢。
AWS Glue Data Catalog

您可以設定資料倉儲，並檢視使用下列 SQL 命令編目的資料 AWS Glue 庫物件：

- SHOW — 顯示目前連線的資料倉儲是否已掛載 awsdatalog。例如，若要顯示 data_catalog_auto_mount 參數值，請執行：

```
SHOW data_catalog_auto_mount;
```

如需詳細資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的 [SHOW](#)。

- ALTER SYSTEM — 變更 data_catalog_auto_mount 的系統層級組態。例如，若要將 data_catalog_auto_mount 參數值變更為 on，請執行：

```
ALTER SYSTEM SET data_catalog_auto_mount = on;
```

當佈建叢集重新啟動或無伺服器工作群組自動暫停並繼續時，變更便會生效。如需詳細資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的 [ALTER SYSTEM](#)。

- SHOW SCHEMAS — 顯示結構描述的清單。名為的 AWS Glue 資料庫中的結構描述 awsdatalog 代表中目錄的 AWS Glue Data Catalog 資料庫。例如，若要顯示這些結構描述，請執行：

```
SHOW SCHEMAS FROM DATABASE awsdatalog;
```

如需詳細資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的 [SHOW SCHEMAS](#)。

- SHOW TABLES — 顯示結構描述中的資料表清單。例如，要顯示 AWS Glue Data Catalog 數據庫中名為模式中 awsdatalog 的表，請 myglue 運行：

```
SHOW TABLES FROM SCHEMA awsdatalog.myschema;
```

如需詳細資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的 [SHOW TABLES](#)。

- SHOW COLUMNS — 顯示資料表中的資料欄清單。例如，要顯示數 AWS Glue Data Catalog 數據庫中名為 awsdatalog 為模式 myglue 和表格 mytable 運行的列：

```
SHOW COLUMNS FROM TABLE awsdatalog.myglue.mytable;
```

如需詳細資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的 [SHOW COLUMNS](#)。

若要授與 IAM 使用者或角色查詢權限 AWS Glue Data Catalog，請依照下列步驟執行

1. 在樹狀檢視窗格中，使用資料庫使用者名稱和密碼身分驗證方法，連線至佈建叢集或無伺服器工作群組中的初始資料庫。例如，使用您在建立叢集或工作群組時使用的管理員使用者和密碼連線至 dev 資料庫。
2. 在編輯器索引標籤中，執行下列 SQL 陳述式以向 IAM 使用者授予 AWS Glue Data Catalog 的存取權。

```
GRANT USAGE ON DATABASE awsdatalog to "IAM:myIAMUser"
```

其中 *IAM:myIAMUser* 是您想要向其授予 AWS Glue Data Catalog 使用權限的 IAM 使用者。或者，您也可以將 *IAM:myIAMRole* 的使用權限授予 IAM 角色。

3. 在樹狀檢視窗格中，編輯或刪除先前建立的叢集或工作群組連線。使用下列其中一種方式連線至叢集或工作群組：
 - 若要從叢集存取 awsdatalog 資料庫，您必須使用身分驗證方法使用您的 IAM 身分的暫時憑證。如需此身分驗證方法的相關資訊，請參閱[連線至 Amazon Redshift 資料庫](#)。您的查詢編輯器 v2 管理員可能需要設定帳戶的帳戶設定，才能在連線視窗上顯示此身分驗證方法。
 - 若要從工作群組存取 awsdatalog 資料庫，您必須使用身分驗證方法聯合身分使用者。如需此身分驗證方法的相關資訊，請參閱[連線至 Amazon Redshift 資料庫](#)。
4. 透過所授予的權限，您可以使用 IAM 身分來針對您的 AWS Glue Data Catalog 執行 SQL。

連線後，您可以使用查詢編輯器 v2 來查詢 AWS Glue Data Catalog 中所編目的資料。在查詢編輯器 v2 的樹狀檢視窗格上，選擇叢集或工作群組和 awsdatalog 資料庫。在編輯器或筆記本窗格中，確認您已選擇正確的叢集或工作群組。所選擇的資料庫應該是初始的 Amazon Redshift 資料庫，例如 dev。如需有關編寫查詢的資訊，請參閱[編寫和執行查詢](#)和[編寫和執行筆記本](#)。系統會保留名為 awsdatalog 的資料庫，以參考帳戶中的外部 Data Catalog 資料庫。對 awsdatalog 資料庫所進行的查詢只能是唯讀的。請使用由三個部分組成的標記法來參考 SELECT 陳述式中的資料表。其中第一部分是數據庫名稱，第二部分是 AWS Glue 數據庫名稱，第三部分是 AWS Glue 表名。

```
SELECT * FROM awsdatalog.<aws-glue-db-name>.<aws-glue-table-name>;
```

您可以執行讀取 AWS Glue Data Catalog 資料並填入 Amazon Redshift 表格的各種案例。

下列範例 SQL 連接中定義的兩個資料表 AWS Glue。

```
SELECT pn.emp_id, alias, role, project_name
FROM "awsdatacatalog"."empl_db"."project_name_table" pn,
"awsdatacatalog"."empl_db"."project_alias_table" pa
WHERE pn.emp_id = pa.emp_id;
```

下列範例 SQL 會建立 Amazon Redshift 表格，並使用兩個 AWS Glue 資料表聯結中的資料填入資料。

```
CREATE TABLE dev.public.glue AS
SELECT pn.emp_id, alias, role, project_name
FROM "awsdatacatalog"."empl_db"."project_name_table" pn,
"awsdatacatalog"."empl_db"."project_alias_table" pa
WHERE pn.emp_id = pa.emp_id;
```

查詢資料湖

您可以查詢 Amazon S3 資料湖中的資料。首先，建立外部結構描述以參考 [AWS Glue Data Catalog](#) 中的外部資料庫。然後，您就可以查詢 Amazon S3 資料湖中的資料。

示範：查詢資料湖

如需如何查詢資料湖的示範，請觀看以下影片。[從 Amazon Redshift 查詢編輯器 v2 查詢資料湖。](#)

先決條件

在查詢編輯器 v2 中使用資料湖之前，請先確認您已在 Amazon Redshift 環境中設定以下項目：

- 使用 AWS Glue 來為 Amazon S3 資料編目，並為 AWS Lake Formation 啟用 Data Catalog。
- 使用已為 AWS Lake Formation 啟用 Data Catalog 的 AWS Glue 來為 Amazon Redshift 建立 IAM 角色。如需此程序的詳細資訊，請參閱[使用為 AWS Lake Formation 啟用的 AWS Glue Data Catalog，為 Amazon Redshift 建立 IAM 角色](#)。如需有關使用 Redshift Spectrum 和 Lake Formation 的詳細資訊，請參閱[使用 Redshift Spectrum 搭配 AWS Lake Formation](#)。
- 授予資料表的 SELECT 許可，以在 Lake Formation 資料庫中進行查詢。如需有關此程序的詳細資訊，請參閱[授予資料表的 SELECT 許可，以在 Lake Formation 資料庫中進行查詢](#)。

您可以在 Lake Formation 主控台 (<https://console.aws.amazon.com/lakeformation/>)、許可區段、資料湖許可頁面中驗證 IAM 角色、AWS Glue 資料庫和資料表是否具有適當許可。

- 確認已連線的使用者擁有在 Amazon Redshift 資料庫中建立結構描述和存取資料湖中資料的許可。當您在查詢編輯器 v2 中連線到資料庫時，您要選擇包含憑證 (可以是資料庫使用者或 IAM 使用者)

的驗證方法。已連線的使用者必須具備適當的許可和資料庫權限，例如 `superuser`。建立叢集或工作群組的 Amazon Redshift `admin` 使用者擁有 `superuser` 權限，而且可以建立結構描述和管理 Redshift 資料庫。如需有關使用查詢編輯器 v2 來連線至資料庫的詳細資訊，請參閱[連線至 Amazon Redshift 資料庫](#)。

建立外部結構描述

若要查詢 Amazon S3 資料湖中的資料，請先建立外部結構描述。外部結構描述會參考 [AWS Glue Data Catalog](#) 中的外部資料庫。

1. 在查詢編輯器 v2 的編輯器檢視中，選擇



建立，然後選擇結構描述。

2. 輸入結構描述名稱。
3. 對於結構描述類型，選擇外部。
4. 在 Data Catalog 詳細資訊內，區域會預設為 Redshift 資料庫所在的 AWS 區域。
5. 選擇外部結構描述要映射到、且包含 AWS Glue 資料表參考的 AWS Glue 資料庫。
6. 選擇具有在 Amazon S3 上查詢資料所需許可的 Amazon Redshift IAM 角色。
7. 選擇性地選擇具有 Data Catalog 許可的 IAM 角色。
8. 選擇建立結構描述。

結構描述會出現在樹狀檢視面板中的資料庫下方。

在建立結構描述時，如果您收到資料庫的許可遭拒錯誤，請檢查已連線的使用者是否具有建立結構描述的資料庫權限。

在 Amazon S3 資料湖中查詢資料

請使用您在上一個程序中建立的結構描述。

1. 在樹狀檢視面板中，選擇結構描述。
2. 若要檢視資料表定義，請選擇資料表。隨即會顯示資料表資料欄和資料類型。
3. 若要查詢資料表，請選擇該資料表，然後在內容功能表 (按一下滑鼠右鍵) 中，選擇選取資料表以產生查詢。
4. 在編輯器中執行查詢。

4. 設定您要共用之資料庫物件的許可。例如：

```
alter datashare mysource add schema public;
```

```
alter datashare mysource add table public.event;
```

5. 在取用者叢集命名空間上設定用來存取資料共用的許可。例如：

```
grant usage on datashare mysource to namespace '2b12345-1234-5678-9012-  
bb1234567890';
```

顯示資料共用

您可以顯示已在生產者叢集上建立的資料共用。

1. 選擇生產者叢集。
2. 顯示資料共用。例如：

```
show datashares;
```

```
share_name share_owner source_database consumer_database share_type createdate  
is_publicaccessible share_acl producer_account producer_namespace  
test_datashare 100 db_producer NULL OUTBOUND 2/15/2022 FALSE admin  
123456789012 p1234567-8765-4321-p10987654321
```

建立取用者資料庫

在取用者叢集上，您必須從資料共用建立資料庫。這些步驟會描述如何在同一帳戶的兩個叢集之間共用資料。如需跨 AWS 帳戶共用資料的相關資訊，請參閱 [Amazon Redshift 資料庫開發人員指南中的跨 AWS 帳戶共用資料](#)。

您可以使用 SQL 命令或查詢編輯器 v2 樹狀檢視面板來建立資料庫。

使用 SQL

1. 從您帳戶的資料共用和生產者叢集的命名空間建立資料庫。例如：

```
create database share_db from datashare mysource of account '123456789012'  
namespace 'p1234567-8765-4321-p10987654321';
```

2. 設定許可，以便使用者可以存取資料庫和結構描述。例如：

```
grant usage on database share_db to usernames;
```

```
grant usage on schema public to usernames;
```

使用查詢編輯器 v2 樹狀檢視面板

1. 選



擇，然後選擇資料庫。

2. 輸入資料庫名稱。
3. (選擇性) 選取使用者和群組，然後選擇資料庫使用者。
4. 選擇使用資料共用建立。
5. 選擇資料共用。
6. 選擇建立資料庫。

新的



料共用資料庫便會顯示在查詢編輯器 v2 的樹狀檢視面板中。

7. 設定許可，以便使用者可以存取資料庫和結構描述。例如：

```
grant usage on database share_db to usernames;
```

```
grant usage on schema public to usernames;
```

查詢資料共用物件

在取用者叢集上，您可以使用由三個部分組成的標記法表示的完全合格物件名稱來查詢資料共用物件：資料庫、結構描述和物件名稱。

1. 在查詢編輯器 v2 的樹狀檢視面板中，選擇結構描述。
2. 若要檢視資料表定義，請選擇資料表。

隨即會顯示資料表資料欄和資料類型。

3. 若要查詢資料表，請選擇該資料表，然後使用內容選單 (右鍵) 選擇選取資料表。
4. 使用 SELECT 命令查詢資料表。例如：

```
select top 10 * from test_db.public.event;
```

使用查詢編輯器 v2 來排程查詢

您可以使用 Amazon Redshift 查詢編輯器 v2 建立排程來執行 SQL 陳述式。您可以建立排程，以符合您業務需求的時間間隔執行 SQL 陳述式。當需要執行排程查詢時，查詢會由 Amazon 啟動，EventBridge 並使用 Amazon Redshift 資料 API。

建立排程以執行 SQL 陳述式

1. 在編輯器



檢視中，選擇



排程以建立排程來執行 SQL 陳述式。

2. 在定義排程時，您會提供下列資訊。
 - 擔任執行查詢所需許可的 IAM 角色。此 IAM 角色也會附加至您的叢集或工作群組。
 - 用於授權存取叢集 AWS Secrets Manager 或工作群組的認證值或臨時認證。資料 API 支援這些身分驗證方法。如需詳細資訊，請參閱 [驗證已排程的查詢](#)。
 - 資料庫所在的叢集或工作群組。
 - 所要查詢的資料所在資料庫的名稱。
 - 已排程查詢的名稱及其描述。查詢編輯器 v2 會在您提供的已排程查詢名稱前面加上「QS2-」。查詢編輯器 v1 會在其已排程查詢的名稱前面加上「QS-」。
 - 要依排程執行的 SQL 陳述式。

- 排程頻率和重複選項，或定義排程的 cron 格式值。如需詳細資訊，請參閱 Amazon CloudWatch 事件使用者指南中的 [Cron 運算式](#)。
 - 您也可以選擇啟用標準 Amazon SNS 通知來監控所排程的查詢。您可能需要確認提供給 Amazon SNS 通知的電子郵件地址。檢查您的電子郵件是否有用來確認 Amazon SNS 通知電子郵件地址的連結。如需詳細資訊，請參閱《Amazon Simple Notification Service 開發人員指南》中的 [電子郵件通知](#)。如果您的查詢正在執行中，但您沒有看到 SNS 主題中發佈的訊息，請參閱 [我的規則執行，但在 Amazon EventBridge 使用者指南中看不到發佈到 Amazon SNS 主題中的任何訊息](#)。
3. 選擇排程查詢以儲存並啟用排程，並將排程新增至已排程的查詢檢視中的查詢清單。

已排程的查詢



檢視會列出叢集和工作群組的已排程查詢。使用此檢視時，您可以顯示排程查詢詳細資訊、啟用或停用排程、編輯排程，以及刪除已排程的查詢。當您檢視查詢詳細資訊時，您也可以檢視依排程執行查詢的歷史記錄。

Note

排程查詢執行只會在排程歷史記錄清單中存在 24 小時。依排程執行的查詢未出現在查詢編輯器 v2 的查詢歷史記錄檢視中。

設定用來排程查詢的許可

若要排程查詢，定義排程和與排程相關聯的 IAM 角色的 AWS Identity and Access Management (IAM) 使用者必須設定 IAM 許可，才能使用 Amazon EventBridge 和 Amazon Redshift 資料 API。若要接收來自已排程查詢的電子郵件，則還必須設定您選擇性指定的 Amazon SNS 通知。

以下說明使用 AWS 受管理原則來提供權限的工作，但視您的環境而定，您可能會想要縮減允許的權限範圍。

若為已登入查詢編輯器 v2 的 IAM 使用者，請使用 IAM 主控台 (<https://console.aws.amazon.com/iam/>) 編輯 IAM 使用者。

- 除了執行 Amazon Redshift 和查詢編輯器 v2 操作的許可外，還可以將 AmazonEventBridgeFullAccess 和受 AmazonRedshiftDataFullAccess AWS 管政策附加到 IAM 使用者。

- 或者，請將許可指派給角色，然後將角色指派給使用者。

將允許 `sts:AssumeRole` 許可的政策附加到您在定義已排程查詢時所指定 IAM 角色的資源 ARN。如需有關擔任角色的相關資訊，請參閱《IAM 使用者指南》中的[向使用者授予切換角色的許可](#)。

下列範例顯示在帳戶 123456789012 中擔任 IAM 角色 `myRedshiftRole` 的許可政策。IAM 角色 `myRedshiftRole` 也是附加至已排程查詢執行所在叢集或工作群組的 IAM 角色。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AssumeIAMRole",
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": [
        "arn:aws:iam::123456789012:role/myRedshiftRole"
      ]
    }
  ]
}
```

更新用於排程查詢的 IAM 角色信任政策，以允許 IAM 使用者擔任該角色。

```
{
  "Sid": "AssumeRole",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::123456789012:user/myIAMUsername"
  },
  "Action": "sts:AssumeRole"
}
```

針對您指定要允許已排程的查詢執行的 IAM 角色，請使用 IAM 主控台 (<https://console.aws.amazon.com/iam/>) 編輯 IAM 角色。

- 將 `AmazonRedshiftDataFullAccess` 和 `AmazonEventBridgeFullAccess` AWS 管政策附加到 IAM 角色。 `AmazonRedshiftDataFullAccess` 受管政策只會針對標記了

索引鍵 `RedshiftDataFullAccess` 的 Redshift Serverless 工作群組允許 `redshift-serverless:GetCredentials` 許可。

驗證已排程的查詢

在排程查詢時，您會在 SQL 執行時使用下列其中一種身分驗證方法。每種方法都需要在查詢編輯器 v2 上使用不同的輸入組合。用於執行 SQL 陳述式的資料 API 支援這些身分驗證方法。

用於執行查詢的資料庫使用者或角色必須具備必要的資料庫權限。例如，若要授予資料表 `mytable` 的 `IAMR:MyRedshiftQEv2Scheduler` 權限，請執行下列 SQL 命令。

```
GRANT all ON TABLE mytable TO "IAMR:MyRedshiftQEv2Scheduler";
```

若要檢視叢集或工作群組中的資料庫使用者清單，請查詢系統檢視 `PG_USER_INFO`。

Note

您為其排程查詢的任何 Redshift 無伺服器工作群組都會使用關鍵字加上標籤。RedshiftDataFullAccess 如需詳細資訊，請參閱 [授權 Amazon Redshift 資料 API 的存取](#)。

若要替代標記工作群組的做法，您也可以將內嵌政策新增至允許 `redshift-serverless:GetCredentials` 的 IAM 角色 (隨排程指定)。例如：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "UseTemporaryCredentialsForAllServerlessWorkgroups",
      "Effect": "Allow",
      "Action": "redshift-serverless:GetCredentials",
      "Resource": [
        "arn:aws:redshift-serverless:*:*:workgroup/*"
      ]
    }
  ]
}
```

AWS Secrets Manager

使用此方法時，請為儲存在 AWS Secrets Manager 中的 secret-arn 提供機密值。此秘密包含用來連線至資料庫的憑證。建立叢集或工作群組時，您可能已使用適當的認證建立密碼。此機密必須標記了索引鍵 RedshiftDataFullAccess。如果標籤鍵不存在，請使用 AWS Secrets Manager 控制台將其添加。如需有關建立密碼的資訊，請參閱[建立資料庫連線認證的密碼](#)。

如需最基本許可的相關資訊，請參閱《AWS Secrets Manager 使用者指南》中的[使用 AWS Secrets Manager 建立和管理機密](#)。

臨時憑證

使用此方法時，請在連線到叢集中的資料庫時提供您的資料庫名稱和資料庫使用者值。您只需要在連線至工作群組中的資料庫時提供資料庫名稱。

在連線至叢集時，AmazonRedshiftDataFullAccess 政策會允許名為 redshift_data_api_user 的資料庫使用者獲得 redshift:GetClusterCredentials 的許可。如果您想要使用不同的資料庫使用者來執行 SQL 陳述式，請在附加至叢集的 IAM 角色中新增政策以允許 redshift:GetClusterCredentials。下列範例政策會允許資料庫使用者 awsuser 和 myuser。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "UseTemporaryCredentialsForAllDbUsers",
      "Effect": "Allow",
      "Action": "redshift:GetClusterCredentials",
      "Resource": [
        "arn:aws:redshift:*:*:dbuser:*/awsuser",
        "arn:aws:redshift:*:*:dbuser:*/myuser"
      ]
    }
  ]
}
```

設定用來檢視排程查詢歷史記錄的許可

若要允許使用者檢視排程查詢歷史記錄，請編輯 IAM 角色 (隨排程指定) 信任關係以新增許的。

以下是 IAM 角色中的信任政策範例，該政策允許 IAM 使用者 *myIAMUsername* 檢視排程查詢歷史記錄。您不必允許 IAM 使用者獲得 `sts:AssumeRole` 許可，而是可以選擇允許 IAM 角色獲得此許可。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "redshift.amazonaws.com",
          "redshift-serverless.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "events.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    },
    {
      "Sid": "AssumeRole",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/myIAMUsername"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

監控已排程的查詢

對於您指定要傳送電子郵件通知的 Amazon SNS 主題，請透過導覽至 SNS 通知區段、開啟監控，然後使用建立 SNS 主題建立主題，以使用查詢編輯器 v2 建立 Amazon SNS 主題。查詢編輯器 v2 會建立 Amazon SNS 主題，並將服務主體新增至 Amazon 的存取政策 EventBridge。以下是在 Amazon SNS 主題中建立的存取政策範例。在此範例中，使用了 AWS 區域 `#### -2`、AWS 帳戶 `1234567890 12` 和 Amazon SNS 主題。`select-version-pdx-testunload`

```
{
  "Version": "2008-10-17",
  "Id": "__default_policy_ID",
  "Statement": [
    {
      "Sid": "Allow_Publish_Events",
      "Effect": "Allow",
      "Principal": {
        "Service": "events.amazonaws.com"
      },
      "Action": "sns:Publish",
      "Resource": "arn:aws:sns:us-west-2:123456789012:select-version-pdx-testunload"
    }
  ]
}
```

排程查詢執行時，Amazon SNS 會傳送 AWS 通知電子郵件。#####
 myemail@example.com ##### 12345678 9012 ### Amazon SNS ### May25 AWS
 ## A-SNS # AWS ## ##### -1 ###

```
{"version":"0","id":"8e4323ec-5258-7138-181b-91290e30ff9b","detail-type":"Scheduled
Event","source":"aws.events","account":"123456789012","time":"2023-05-25T15:22:00Z",
  "region":"eu-north-1","resources":["arn:aws:events:eu-
north-1:123456789012:rule/QS2-may25a"],"detail":{}}
```

--
 If you wish to stop receiving notifications from this topic, please click or visit the link below to unsubscribe:
<https://sns.eu-north-1.amazonaws.com/unsubscribe.html?SubscriptionArn=arn:aws:sns:eu-north-1:123456789012:may25a-SNS:0c1a3d05-39c2-4507-bc3d-47250513d7b0&Endpoint=myemail@example.com>

Please do not reply directly to this email. If you have any questions or comments regarding this email, please contact us at <https://aws.amazon.com/support>

針對排程查詢的設定進行故障診斷

如果您在排程查詢時遇到問題，請考慮下列事項。

查詢未執行

檢查排程中使用的 IAM 角色是否有可取得暫時叢集憑證的許可。已佈建叢集的許可為 `redshift:GetClusterCredentialsWithIAM`。Redshift Serverless 工作群組的許可為 `redshift-serverless:GetCredentials`。

已排程歷史記錄未顯示

用於登入 AWS 主控台的 IAM 使用者或 IAM 角色未新增到用於排程查詢的 IAM 角色的信任政策中。

使用用 AWS Secrets Manager 於排程查詢連線時，請確認密碼已使用金鑰加上標籤 `RedshiftDataFullAccess`。

如果排程查詢使用 AWS Secrets Manager 連線，用於排程查詢的 IAM 角色必須 `SecretsManagerReadWrite` 附加至該角色的對等受管政策。

查詢歷史記錄狀態為 **Failed**

如需查詢失敗原因的詳細資訊，請檢視 `SYS_QUERY_HISTORY` 系統檢視。常見問題是用來執行查詢的資料庫使用者或角色可能沒有要執行 SQL 所需的權限。如需詳細資訊，請參閱 [驗證已排程的查詢](#)。

下列 SQL 會查詢 `SYS_QUERY_HISTORY` 檢視以傳回失敗的查詢。

```
SELECT user_id, query_id, transaction_id, session_id, database_name, query_type,
       status, error_message, query_text
FROM sys_query_history
WHERE status = 'failed';
```

若要了解特定的失敗已排程查詢的詳細資訊，請參閱 [尋找已排程查詢的詳細資料 AWS CloudShell](#)。

尋找已排程查詢的詳細資料 AWS CloudShell

您可以使用 AWS CloudShell 來尋找有關排程查詢的詳細資訊。您必須擁有適當的權限才能執行下列程序中顯示的 AWS CLI 命令。

檢視已排程查詢的結果

1. 在 AWS 主控台上，開啟 AWS CloudShell 命令提示字元。若要取得有關的更多資訊 AWS CloudShell，請參閱《AWS CloudShell 使用指南》AWS CloudShell 中的 [內容](#)。

2. 擔任已排程查詢的 IAM 角色。若要擔任該角色，請在查詢編輯器 v2 中尋找與排程查詢相關聯的 IAM 角色，並在中的 AWS CLI 命令中使用該角色 AWS CloudShell。例如，針對角色，scheduler 輸入 AWS STS 指令來承擔排程查詢所使用的角色。

```
aws sts assume-role --role-arn "arn:aws:iam::123456789012:role/scheduler" --role-session-name "scheduler-test"
```

傳回的憑證類似以下內容。

```
"Credentials": {
  "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
  "SecretAccessKey": "wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY",
  "SessionToken": "je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY...",
  "Expiration": "2023-08-18T18:19:44+00:00"
},
"AssumedRoleUser": {
  "AssumedRoleId": "AROA35B2NH6WBTP70NL4E:scheduler-test",
  "Arn": "arn:aws:sts::123456789012:assumed-role/scheduler/scheduler-test"
}
}
```

3. AWS CLI 使用假設 IAM 角色所顯示的登入資料，在中建立環境變數。您必須使用這些字符，直到其到期。例如，您可以在中輸入下列內容 AWS CloudShell。

```
export AWS_ACCESS_KEY_ID=AKIAIOSFODNN7EXAMPLE
export AWS_SECRET_ACCESS_KEY=wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY
export AWS_SESSION_TOKEN=je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY...
```

4. 若要檢視失敗查詢的錯誤，請執行 AWS CLI 命令來描述陳述式。SQL 陳述式的 ID 來自查詢編輯器 v2 中已排程查詢之排程歷史記錄區段中顯示的 ID。

```
aws redshift-data describe-statement --id 130d2620-05d2-439c-b7cf-815d9767f513
```

在此範例中，已排程的 SQL `select * from users limit 100` 會導致 `users` 資料表不存在的 SQL 錯誤。

```
{
  "CreatedAt": "2023-08-18T17:39:15.563000+00:00",
  "Duration": -1,
```



```
"Error": "ERROR: relation \"users\" does not exist",
"HasResultSet": false,
"Id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
"QueryString": "select * from users limit 100\n-RequestID=a1b2c3d4-5678-90ab-cdef-EXAMPLE22222; TraceID=1-633c5642-4039308d03f3a0ba53dbdf6f",
"RedshiftPid": 1073766651,
"RedshiftQueryId": 0,
"ResultRows": -1,
"ResultSize": -1,
"Status": "FAILED",
"UpdatedAt": "2023-08-18T17:39:16.116000+00:00",
"WorkgroupName": "default"
}
```

排程查詢的示範

如需排程查詢的示範，請觀看下列影片。[排程查詢的影片示範](#)。

將查詢結果視覺化

在執行查詢並顯示結果後，您可以開啟圖表來顯示透過圖形加以視覺化的目前結果頁面。您可以使用下列控制項來定義圖表的內容、結構和外觀：

+

追蹤

代表圖表中的一組相關圖形標記。您可以在圖表中定義多個追蹤。

Type

您可以定義追蹤類型以將資料表示為下列其中一項：

- 散佈圖或氣泡圖。
- 長條圖，以垂直或水平長條表示資料類別。
- 區域圖，以定義填充區域。
- 直方圖，以使用長條表示頻率的分佈。
- 圓餅圖，以圓形表示資料，其中的每個切片各表示在整體中所佔的百分比。
- 漏斗圖或漏斗區域圖，以透過各個程序階段表示資料。
- OHLC (開盤-最高-最低-收盤) 圖，通常用於財務資料，以沿著 x 軸 (通常代表時間間隔) 表示開盤價、最高價、最低價和收盤價。

- 蠟燭圖，在時間線上表示某個類別一系列的值得。
- 瀑布圖，透過一系列中間值來表示初始值的增減變化。這些值可以表示時間間隔或類別。
- 折線圖，表示值隨著時間推移的變化情形。

X 軸

您必須指定要沿著 X 軸繪製、含有值的資料表資料欄。包含描述性值的資料欄通常代表維度資料。包含量化值的資料欄通常代表事實資料。

Y 軸

您必須指定要沿著 Y 軸繪製、含有值的資料表資料欄。包含描述性值的資料欄通常代表維度資料。包含量化值的資料欄通常代表事實資料。

子圖

您可以定義圖表資料的其他呈現方式。

轉換

您可以定義轉換以篩選追蹤資料。您必須使用分割轉換以顯示來自單一來源追蹤的多個追蹤。您必須使用彙總轉換以將追蹤顯示為平均值或最小值。您必須使用排序轉換來排序追蹤。

一般外觀

您可以針對下列項目設定預設值：背景顏色、邊界顏色、用來設計色盤的色階、文字樣式和大小、標題樣式和大小，以及模式列。您可以定義拖曳、點按和暫留的互動效果。您可以定義中繼文字。您可以定義追蹤、軸、圖例和註釋的預設外觀。

選擇追蹤以將結果顯示為圖表。對於類型，將圖表的樣式選為長條、折線等等。對於方向，您可以選擇垂直或水平。對於 X，請選擇要用於水平軸的資料表資料欄。對於 Y，請選擇要用於垂直軸的資料表資料欄。

選擇重新整理以更新圖表顯示。選擇全螢幕以展開圖表顯示。

建立圖表

1. 執行查詢並取得結果。
2. 開啟圖表。
3. 選擇追蹤並開始將資料視覺化。
4. 從下列其中一個選項中選擇圖表樣式：

- 散佈圖
 - 長條圖
 - 區域圖
 - 直方圖
 - 圓餅圖
 - 漏斗圖
 - 漏斗區域圖
 - OHLC (開盤-最高-最低-收盤) 圖
 - 蠟燭圖
 - 瀑布圖
 - 折線圖
5. 選擇樣式以自訂外觀，包括顏色、軸、圖例和註釋。您可以新增文字、形狀和圖像。
 6. 選擇註釋以新增文字、形狀和圖像。

儲存圖表

1. 選擇儲存圖表。
2. 為圖表輸入名稱。
3. 選擇儲存。

匯出圖表

1. 選擇 Export (匯出)。
2. 選擇 PNG 或 JPEG。
3. 設定圖表的寬度和高度。
4. 選擇 Export (匯出)。
5. 選擇要在預設的圖形應用程式中開啟檔案，還是使用預設名稱儲存檔案。

瀏覽並開啟已儲存的圖表

1. 選擇圖表標籤。
2. 開啟您想要的圖表。

將圖表組織到資料夾內

1. 從導覽窗格選擇圖表。
2. 選擇新增資料夾並為資料夾命名。
3. 選擇建立以在圖表標籤中建立資料夾。

您可以使用將圖表移入和移出文件夾 drag-and-drop。

範例：建立圓餅圖以將查詢結果視覺化

下列範例會使用範例資料庫的「Sales」資料表。如需詳細資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的[範例資料庫](#)。

以下是您為了提供圓餅圖資料所執行的查詢。

```
select top 5 eventname, count(salesid) totalorders, sum(pricepaid) totalsales
from sales, event
where sales.eventid=event.eventid group by eventname
order by 3;
```

為按總銷售額排序的最佳活動建立圓餅圖

1. 執行查詢。
2. 在查詢結果區域中，開啟圖表。
3. 選擇追蹤。
4. 對於類型，選擇圓餅圖。
5. 對於值，選擇 totalsales。
6. 對於標籤，選擇 eventname。
7. 選擇樣式，然後選擇一般。
8. 在色階底下，選擇分類，然後選擇 Pastel2。



範例：建立用於比較營收與銷售額的組合圖表

執行此範例中的步驟，以建立由營收資料的長條圖與銷售額資料的折線圖組合而成的圖表。下列範例會使用 tickit 範例資料庫的「Sales」資料表。如需詳細資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的[範例資料庫](#)。

以下是您為了提供圖表資料所執行的查詢。

```
select eventname, total_price, total_qty_sold
from (select eventid, total_price, total_qty_sold, ntile(1000) over(order by
total_price desc) as percentile
      from (select eventid, sum(pricepaid) total_price, sum(qtysold) total_qty_sold
            from tickit.sales
            group by eventid)) Q, tickit.event E
where Q.eventid = E.eventid
and percentile = 1
order by total_price desc;
```

建立用於比較營收與銷售額的組合圖表

1. 執行查詢。
2. 在查詢結果區域中，開啟圖表。
3. 在追蹤 o 底下，對於類型，選擇長條圖。
4. 對於 X，選擇 eventname。
5. 對於 Y，請選擇 total_price。

長條圖會沿著 X 軸顯示活動名稱。

6. 在樣式底下，選擇追蹤。

7. 對於名稱，輸入營收。
8. 在樣式底下，選擇軸。
9. 對於標題，選擇 Y 並輸入營收。

營收標籤隨即會顯示在左側 Y 軸上。

10. 在結構底下，選擇追蹤。
11. 選擇
+
追蹤。

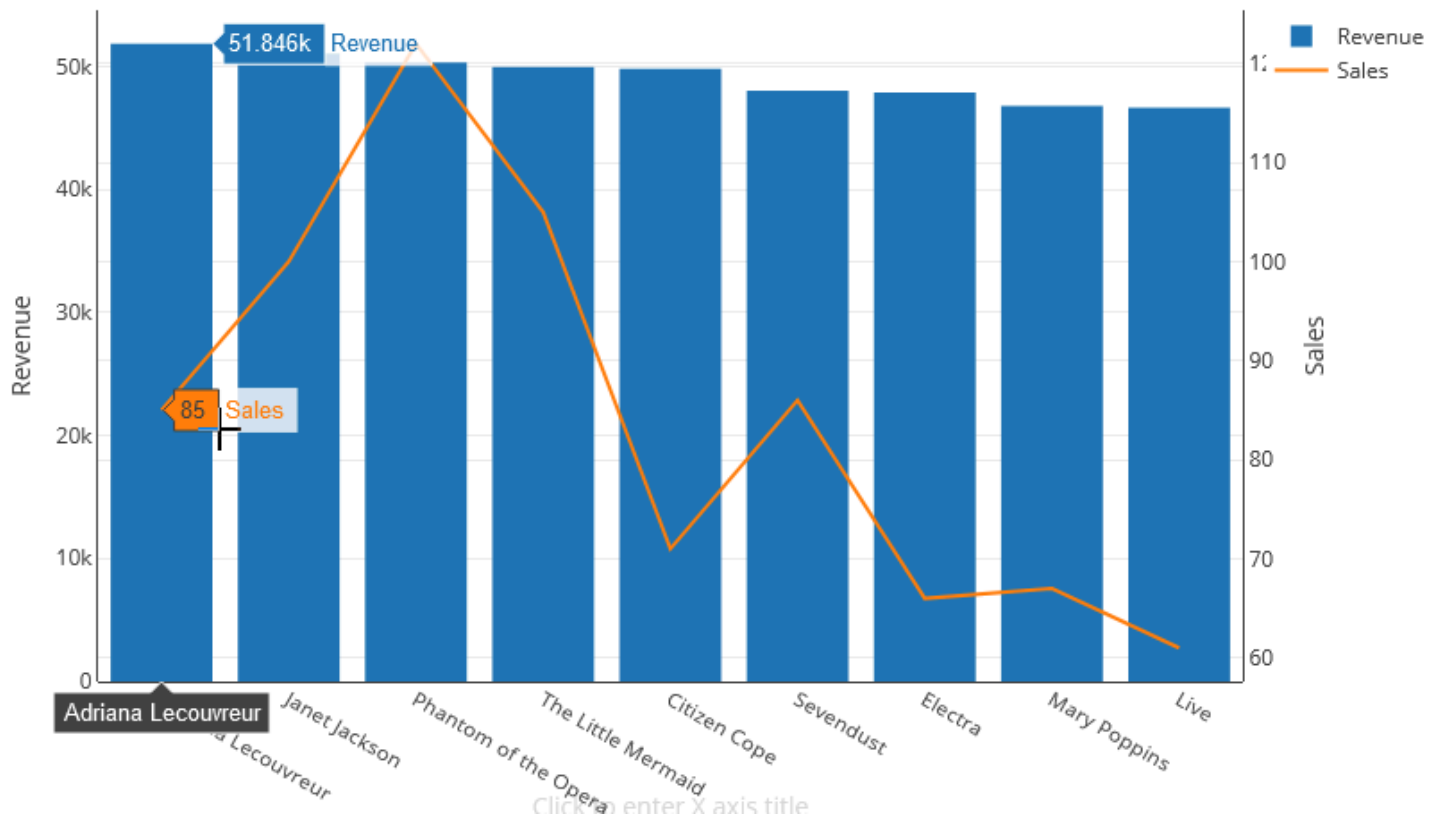
追蹤 1 的選項隨即會顯示出來。

12. 對於類型，選擇折線圖。
13. 對於 X，選擇 eventname。
14. 對於 Y，選擇 total_qty_sold。
15. 在要使用的軸底下，對於 Y 軸選擇
+

Y 軸便會顯示 Y2。

16. 在樣式底下，選擇軸。
17. 在標題底下，選擇 Y2。
18. 對於名稱，輸入 Sales。
19. 在折線圖底下，選擇 Y:Sales。
20. 在軸線底下，選擇顯示，然後對於位置，選擇右。

Revenue and Sales



示範：使用 Amazon Redshift 查詢編輯器 v2 建置視覺效果

如需如何建置視覺效果的示範，請觀看下列影片。[使用 Amazon Redshift 查詢編輯器 v2 建置視覺效果](#)。

以團隊的形式協作和共用

您可以與團隊共用查詢。

您可以為一組會協作和共用查詢編輯器 v2 資源的使用者定義團隊。管理員可以透過將標籤新增至 IAM 角色來建立團隊。如需詳細資訊，請參閱 [要使用查詢編輯器 v2 所需的許可](#)。

儲存、瀏覽及刪除查詢

在與團隊共用查詢前，請先儲存查詢。您可以檢視和刪除已儲存的查詢。

儲存查詢

1. 準備您的查詢並選擇儲存。

2. 為查詢輸入標題。
3. 選擇儲存。

瀏覽已儲存的查詢

1. 從導覽窗格選擇查詢。
2. 您可以檢視屬於我的查詢、由我共用或共用給我的團隊的查詢。這些查詢能以個別查詢的形式出現，也能出現在您建立的資料夾內。

若要刪除已儲存的查詢

1. 為已儲存的查詢開啟內容 (右鍵) 選單。
2. 選擇刪除，然後確認動作。

將已儲存的查詢組織到資料夾內

1. 從導覽窗格選擇查詢。
2. 選擇新增資料夾並為資料夾命名。
3. 選擇建立以在查詢標籤中建立資料夾。

您現在可以使用將查詢移入和移出資料夾 drag-and-drop。

共用查詢

您可以與團隊共用查詢。您也可以檢視已儲存查詢的歷史記錄並管理查詢版本。

若要與團隊共用查詢，請確定您已將主體標籤 `sqlworkbench-team` 設定為與帳戶中其他團隊成員相同的值。例如，管理員可以針對會計部門中的每個人，將值設定為 `accounting-team`。如需範例，請參閱[要使用查詢編輯器 v2 所需的許可](#)。

與團隊共用查詢

1. 從導覽窗格選擇查詢。
2. 開啟您要共用之查詢的內容 (右鍵) 選單，然後選擇與我的團隊共用。
3. 選擇您要與其共用查詢的團隊，然後選擇儲存共用選項。

每次儲存 SQL 查詢時，查詢編輯器 v2 都會將其儲存為新的版本。您可以瀏覽較舊的查詢版本、儲存查詢的複本或還原查詢。

管理查詢版本

1. 從導覽窗格選擇查詢。
2. 開啟您要使用之查詢的內容 (右鍵) 選單。
3. 選擇版本歷史記錄以開啟查詢的版本清單。
4. 在版本歷史記錄頁面上，您可以執行下列操作：
 - 回復為選取項 — 回復為選取的版本，並繼續使用此版本。
 - 另存選取項 — 在編輯器中建立新查詢。

使用查詢編輯器來查詢資料庫

若要在 Amazon Redshift 叢集託管的資料庫上執行查詢，簡單的辦法是使用查詢編輯器。建立叢集後，您可以在 Amazon Redshift 主控台中使用查詢編輯器，立即執行查詢。

Note

您無法使用這個原始查詢編輯器在 Amazon Redshift Serverless 中查詢資料。請改用 Amazon Redshift 查詢編輯器 v2。

2021 年 2 月，我們部署了更新的查詢編輯器，並變更了可使用查詢編輯器的授權許可。新的查詢編輯器會使用 Amazon Redshift 資料 API 來執行查詢。該 AmazonRedshiftQueryEditor 政策是 AWS 受管 AWS Identity and Access Management (IAM) 政策，已更新為包含必要的許可。如果您有自訂 IAM 政策，請務必加以更新。請使用 AmazonRedshiftQueryEditor 作為指南。AmazonRedshiftQueryEditor 的變更包括下列內容：

- 可管理查詢編輯器陳述式結果的許可需要陳述式擁有者使用者。
- 已新增使用 Secrets Manager 連線至資料庫的許可。

如需詳細資訊，請參閱 [要使用 Amazon Redshift 主控台查詢編輯器所需的許可](#)。

當您從新的查詢編輯器連線到叢集時，您可以使用下列兩種身分驗證方法的其中一種，如 [使用查詢編輯器來連線](#) 中所述。

您可以使用查詢編輯器執行下列作業：

- 執行單一 SQL 陳述式查詢。
- 將最大 100 MB 的結果集下載到逗號分隔值 (CSV) 檔案。
- 儲存查詢供重複使用。您無法在歐洲 (巴黎) 區域、亞太區域 (大阪) 區域、亞太區域 (香港) 區域或中東 (巴林) 區域儲存查詢。
- 檢視使用者定義資料表的查詢執行時間詳細資訊。
- 將查詢排程在未來的時間執行。
- 檢視您在查詢編輯器中所建立查詢的歷史記錄。
- 使用增強的 VPC 路由對叢集執行查詢。

查詢編輯器考量

在使用查詢編輯器時，請考慮下列有關使用查詢的事項：

- 查詢的持續時間上限為 24 小時。
- 查詢結果大小上限為 100 MB。如果呼叫傳回的回應資料超過 100 MB，系統會終止呼叫。
- 查詢結果的保留時間上限為 24 小時。
- 查詢陳述式的大小上限為 100 KB。
- 叢集必須位於以 Amazon VPC 服務為基礎的虛擬私有雲端 (VPC) 中。
- 您不能在查詢編輯器中使用交易。如需交易的相關資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的 [BEGIN](#)。
- 您可以儲存長度最多 3,000 個字元的查詢。

啟用對查詢編輯器的存取

您需要許可才能存取查詢編輯器。若要啟用存取權，建議您將 IAM 許可的 AmazonRedshiftQueryEditor 和 AmazonRedshiftReadOnlyAccess AWS 受管政策附加到用於存取叢集的 IAM 角色。然後，您可以將該角色指派給使用者。您可以使用 IAM 主控台 (<https://console.aws.amazon.com/iam/>) 來連接 IAM 政策。如需詳細資訊，請參閱 [針對 Amazon Redshift 使用以身分為基礎的政策 \(IAM 政策\)](#)。

如果您已經建立用於存取 Amazon Redshift 的使用者，則可以透過指派的角色將 AmazonRedshiftQueryEditor 和 AmazonRedshiftReadOnlyAccess AWS 受管政策附加到該

使用者。如果您尚未建立使用者，則請建立使用者，並將政策附加到 IAM 角色，然後指派角色給該使用者。

AWS 受管理的原則 AmazonRedshiftQueryEditor 允許動

作 `redshift:GetClusterCredentials`，依預設會提供超級使用者對資料庫的存取權。若要限制存取，您可以執行下列其中一項操作：

- 建立自訂政策，讓這個政策允許呼叫 `redshift:GetClusterCredentials`，並將資源限制在 `DbUser` 的指定值。
- 新增會拒絕 `redshift:GetClusterCredentials` 許可的政策。任何獲派已附加此許可之角色的使用者，都必須使用暫時憑證登入查詢編輯器。此拒絕政策說明了範例。

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Deny",
    "Action": "redshift:GetClusterCredentials",
    "Resource": "*"
  }
}
```

如需建立具有所需許可之角色的相關資訊，請參閱 [建立具有呼叫權限的 IAM 角色 GetClusterCredentials](#)。

任何透過 AWS 受管政策授與 Amazon Redshift 查詢編輯器存取權的使用者

都 AmazonRedshiftQueryEditor 可以列出所有密碼。不過，此政策只允許建立和擷取標記了金鑰 `RedshiftQueryOwner` 和值 `${aws:userid}` 的機密。如果您從 Amazon Redshift 查詢編輯器建立金鑰，則系統會自動標記金鑰。若要使用不是使用 Amazon Redshift 查詢編輯器所建立的機密，請確認機密已標記金鑰 `RedshiftQueryOwner` 和唯一 IAM 使用者識別碼的值，例如 `AIDACKCEVSQ6C2EXAMPLE`。

使用 Amazon Redshift 查詢編輯器所需的許可

是 `AmazonRedshiftQueryEditor` 和 `AmazonRedshiftReadOnlyAccess`。

若要提供存取權，請新增權限至您的使用者、群組或角色：

- 使用者和群組位於 AWS IAM Identity Center：

建立權限合集。請按照 AWS IAM Identity Center 使用者指南 中的 [建立權限合集](#) 說明進行操作。

- 透過身分提供者在 IAM 中管理的使用者：

建立聯合身分的角色。請按照 IAM 使用者指南的 [為第三方身分提供者 \(聯合\) 建立角色](#) 中的指示進行操作。

- IAM 使用者：

- 建立您的使用者可擔任的角色。請按照 IAM 使用者指南的 [為 IAM 使用者建立角色](#) 中的指示進行操作。
- (不建議) 將政策直接附加至使用者，或將使用者新增至使用者群組。請遵循 IAM 使用者指南的 [新增許可到使用者 \(主控台\)](#) 中的指示。

使用查詢編輯器來連線

當您使用查詢編輯器連線到叢集時，您會使用下列其中一種身分驗證方法。每種方法需要來自 Amazon Redshift 主控台的不同輸入組合。

AWS Secrets Manager

使用此方法時，請為儲存在 AWS Secrets Manager 中的 secret-arn 提供機密值。此秘密包含用來連線至資料庫的憑證。

臨時憑證

使用此方法時，請提供您的資料庫和 db-user 值。

將資料庫認證儲存於 AWS Secrets Manager

當您呼叫查詢編輯器時，您可以在 AWS Secrets Manager 中使用機密來傳遞叢集的憑證。若要以這種方式傳遞憑證，請指定機密的名稱或 Amazon Resource Name (ARN)。

如需最基本許可的相關資訊，請參閱《AWS Secrets Manager 使用者指南》中的 [使用 AWS Secrets Manager 建立和管理機密](#)。

將憑證儲存在 Amazon Redshift 叢集的機密中

1. 用 AWS Secrets Manager 於建立包含叢集認證的密碼。當您選擇儲存新的機密時，請選擇 Redshift 叢集的憑證。將使用者名稱 (資料庫使用者)、密碼和資料庫叢集 (叢集識別碼) 的值儲存在機密中。

如需說明，請參閱《AWS Secrets Manager 使用者指南》中的 [建立基本秘密](#)。

2. 使用主 AWS Secrets Manager 控制台檢視您建立之密碼的詳細資料，或執行 `aws secretsmanager describe-secret` AWS CLI 命令。

如果您選擇使用叢集的管理員認證 AWS Secrets Manager，您可以使用 Secrets Manager 儲存的管理員認證連線到資料庫。

使用查詢編輯器

在以下範例中，您可以使用查詢編輯器來執行下列任務：

- 執行 SQL 命令。
- 檢視查詢執行詳細資訊。
- 儲存查詢。
- 下載查詢結果集。

若要完成以下範例，您需要一個現有的 Amazon Redshift 叢集。如果您還沒有叢集，請使用[建立叢集](#)中說明的程序來建立叢集。

在 Amazon Redshift 主控台上使用查詢編輯器

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽選單中，選擇查詢編輯器，然後連線至您叢集的資料庫。
3. 針對 Schema (結構描述)，選擇 public (公有)，以根據結構描述建立新的資料表。
4. 在查詢編輯器視窗中輸入以下命令，然後選擇 Run (執行) 建立新資料表。

```
create table shoes(  
    shoetype varchar (10),  
    color varchar(10));
```

5. 選擇 Clear (清除)。
6. 在查詢編輯器視窗中輸入以下命令，然後選擇 Run (執行) 來將資料列新增至資料表。

```
insert into shoes values  
( 'loafers', 'brown'),  
( 'sandals', 'black');
```

7. 選擇 Clear (清除)。

- 在查詢編輯器視窗中輸入以下命令，然後選擇 Run (執行) 查詢新資料表。

```
select * from shoes;
```

Query results (查詢結果) 即會顯示結果。

鞋子類型	顏色
sandals	black
loafers	brown

- 選擇 Execution (執行) 檢視執行的詳細資訊。
- 選擇 Data (資料)，再選擇 Export (匯出)，將查詢結果下載為檔案。

排程查詢

Important

Amazon Redshift 查詢編輯器 v2 現在支援排程查詢。建議您使用查詢編輯器 v2。如需詳細資訊，請參閱 [使用查詢編輯器 v2 來排程查詢](#)。

若要建立執行 SQL 陳述式的排程，您可以使用 Amazon Redshift 主控台上的查詢編輯器。您可以建立排程，以符合您業務需求的時間間隔執行 SQL 陳述式。當排程查詢執行時，Amazon EventBridge 會啟動查詢。

建立排程以執行 SQL 陳述式

- 開啟主控台和查詢編輯器，如[使用查詢編輯器](#)中所述。此查詢編輯器只能與佈建叢集搭配使用。
- 選擇排程以建立用來執行 SQL 陳述式的排程。

在定義排程時，您會提供下列資訊：

- 用來擔任執行查詢時所需許可的 IAM 角色。如需詳細資訊，請參閱 [設定用來排程查詢的許可](#)。
- 用於授權存取叢集的驗證值 AWS Secrets Manager 或臨時認證。如需詳細資訊，請參閱 [驗證已排程的查詢](#)。
- 已排程查詢的名稱以及要執行的單一 SQL 陳述式。

- 排程頻率和重複選項或 cron 格式值。
- 您也可以選擇啟用 Amazon SNS 通知來監控所排程的查詢。如果您的查詢正在執行中，但您沒有看到 SNS 主題中發佈的訊息，請參閱 Amazon EventBridge 使用者指南中的「我的規則已觸發，但我看不到任何訊息發佈到 Amazon [SNS 主題](#)中」。

您也可以使用 Amazon Redshift 主控台來管理和更新已排程的查詢。視主控台的版本而定，已排程的查詢可能會列在下列位置：

- 叢集詳細資訊頁面的排程索引標籤上。
- 查詢編輯器的已排程的查詢索引標籤上。

如果您從這兩個位置的其中一個選擇排程名稱，便可以檢視和編輯已排程查詢的定義。

設定用來在 Amazon Redshift 主控台上排程查詢的許可

若要排程查詢，定義排程的 AWS Identity and Access Management (IAM) 使用者和與排程相關聯的 IAM 角色必須設定如下。

對於已登入 Amazon Redshift 主控台的 IAM 使用者，請執行以下操作：

- 將受 AmazonEventBridgeFullAccess AWS 管政策附加到 IAM 角色。
- 為政策附加您在定義已排程的 SQL 陳述式時所指定 IAM 角色的 `sts:AssumeRole` 許可。

以下範例顯示擔任指定 IAM 角色的政策。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AssumeIAMRole",
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws:iam::account-id:role/sql-statement-iam-role"
    }
  ]
}
```

若要讓您指定的 IAM 角色可以啟用排程器以執行查詢，請執行下列操作：

- 確保此 IAM 角色指定了 EventBridge 服務主體 (events.amazonaws.com)。信任關係範例如下。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "events.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

如需如何為事件建立 IAM 角色的詳細資訊，請參閱[使用 Amazon EventBridge 排程器所需的許可](#)。

- 將受AmazonRedshiftDataFullAccess AWS 管政策附加到 IAM 角色。
- 若要允許使用者檢視排程歷史記錄，請編輯 IAM 角色以新增 sts:AssumeRole 權限。

IAM 角色中的信任政策範例如下。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "events.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```


驗證已排程的查詢

在排程查詢時，您會在查詢 SQL 執行時使用下列其中一種身分驗證方法。每種方法需要來自 Amazon Redshift 主控台的不同輸入組合。

AWS Secrets Manager

使用此方法時，請為儲存在 AWS Secrets Manager 中的 secret-arn 提供機密值。此秘密包含用來連線至資料庫的憑證。此機密必須標記了索引鍵 RedshiftDataFullAccess。

如需最基本許可的相關資訊，請參閱《AWS Secrets Manager 使用者指南》中的[使用 AWS Secrets Manager 建立和管理機密](#)。

臨時憑證

使用此方法時，請提供您的資料庫和 db-user 值。

AmazonRedshiftDataFullAccess 政策允許名為 redshift_data_api_user 的資料庫使用者獲得 redshift:GetClusterCredentials 的許可。如果您想要使用不同的資料庫使用者來執行 SQL 陳述式，請在 IAM 角色中新增政策以允許 redshift:GetClusterCredentials。下列範例政策會允許資料庫使用者 awsuser 和 myuser。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "UseTemporaryCredentialsForAllDbUsers",
      "Effect": "Allow",
      "Action": "redshift:GetClusterCredentials",
      "Resource": [
        "arn:aws:redshift:*:*:dbuser:*/awsuser",
        "arn:aws:redshift:*:*:dbuser:*/myuser"
      ]
    }
  ]
}
```

創建一個在查詢完成時運行的 Amazon EventBridge 規則

您可以建立事件規則以在查詢完成時傳送通知。如需使用 Amazon EventBridge 主控台的程序，請參閱[Amazon 使用 EventBridge 者指南中的建立可對事件做出反應的 Amazon EventBridge 規則](#)。如有

關事件模式的詳細資訊，請參閱 [Amazon EventBridge 使用者指南中的 Amazon EventBridge 事件模式](#)。

例如，當查詢為 FINISHED 時，系統會傳送下列範例事件。

```
{
  "version": "0",
  "id": "6a7e8feb-b491-4cf7-a9f1-bf3703467718",
  "detail-type": "Redshift Data Statement Status Change",
  "source": "aws.redshift-data",
  "account": "123456789012",
  "time": "2020-12-22T17:00:00Z",
  "region": "us-west-1",
  "resources": [
    "arn:aws:redshift:us-east-2:123456789:cluster:t1"
  ],
  "detail": {
    "statementId": "01bdaca2-8967-4e34-ae3f-41d9728d5644",
    "clusterId": "test-dataapi",
    "statementName": "awesome query",
    "state": "FINISHED",
    "pages": 5,
    "expireAt": "2020-12-22T18:43:48Z",
    "principal": "arn:aws:sts::123456789012:assumed-role/any",
    "queryId": 123456
  }
}
```

您可以建立事件模式規則來篩選事件。

```
{
  "source": [
    "aws.redshift-data"
  ],
  "detail-type": [
    "Redshift Data Statement Status Change"
  ],
  "detail": {
    "state": [
      "FINISHED"
    ]
  }
}
```

使用 SQL 用戶端工具連接至 Amazon Redshift 資料倉儲

您可以透過 Java 資料庫連線 (JDBC)、Python 和開放式資料庫連線 (ODBC) 連線，從 SQL 用戶端工具連線到 Amazon Redshift 資料倉儲。Amazon Redshift 不會提供或安裝任何 SQL 用戶端工具或程式庫。若要使用這些工具或程式庫來處理資料倉儲中的資料，請將它們安裝在用戶端電腦或 Amazon EC2 執行個體上。您可以使用支援 JDBC、Python 或 ODBC 驅動程式的大多數 SQL 用戶端工具。

使用本主題結尾的章節清單，協助您逐步完成設定用戶端電腦或 Amazon EC2 執行個體以使用 JDBC、Python 或 ODBC 連線的程序。這些主題也會討論用戶端與伺服器之間連線的相關安全性選項。此外，也請尋找有關從 SQL 用戶端工具 (例如 SQL Workbench/J (第三方工具) 和 [Amazon Redshift RSQL](#)) 進行設定和連線的資訊。如果您還沒有可用的商業智慧工具，可以嘗試使用這些工具。您也可以使用本節瞭解如何以程式設計方式連線到資料倉儲。最後，如果您在嘗試連線到資料倉儲時遇到問題，您可以檢閱疑難排解資訊以找出解決方案。

連接用戶端工具的建議

如果您使用 IP 位址連線至 Redshift 叢集，當發生中斷或連線中斷，且叢集在新的可用區域 (AZ) 中線時，可能會導致額外的停機時間。不過，如果您仍希望應用程式使用 IP 位址連線至 Redshift，請使用連接至叢集 virtual-private-cloud (VPC) 端點的私有 IP 位址。您可以在「內容」選項卡下的「網絡和安全性」中的集群詳細信息中找到此信息。

Note

如果您的應用程式使用領導節點的 IP 位址來存取 Redshift 叢集，建議的最佳做法是將其變更為使用叢集端點 URL。如需詳細資訊，請參閱在 [Amazon Redshift 中設定連線](#)。

主題

- [在 Amazon Redshift 中設定連線](#)
- [設定連線的安全選項](#)
- [從用戶端工具和程式碼連線](#)
- [使用 SQL Workbench/J 進行連線](#)
- [以程式設計方式 Connect 到資料倉](#)
- [使用身分驗證設定檔連線至 Amazon Redshift](#)
- [針對 Amazon Redshift 中的連線問題進行疑難排解](#)

在 Amazon Redshift 中設定連線

在下一節中，您會了解如何設定 JDBC、Python 和 ODBC 連線，以從 SQL 用戶端工具連線至叢集。本節描述如何設定 JDBC、Python 和 ODBC 連線。也描述如何使用 Secure Sockets Layer (SSL) 和伺服器憑證，以加密用戶端與伺服器之間的通訊。

適用於 Amazon Redshift 的 JDBC、Python 和 ODBC 驅動程式

若要處理叢集中的資料，您必須具有 JDBC、Python 或 ODBC 驅動程式，以便從用戶端電腦或執行個體來連線。將應用程式編寫為使用 JDBC、Python 或 ODBC 資料存取 API 操作，並使用支援 JDBC、Python 或 ODBC 的 SQL 用戶端工具。

Amazon Redshift 提供了 JDBC、Python 和 ODBC 驅動程式供您下載。這些驅動程式有獲得 AWS Support 的支援。PostgreSQL 驅動程式未經過測試，因此未獲得 Amazon Redshift 團隊的支援。在連線至 Amazon Redshift 叢集時，請使用 Amazon Redshift 特定的驅動程式。Amazon Redshift 驅動程式有下列優點：

- 支援 IAM、SSO 和聯合身分驗證。
- 支援新的 Amazon Redshift 資料類型。
- 支援身分驗證設定檔。
- 與 Amazon Redshift 增強功能搭配使用而提升了效能。

如需如何下載 JDBC 和 ODBC 驅動程式及設定叢集連線的相關資訊，請參閱 [設定 Amazon Redshift JDBC 驅動程式 2.1 版的連線](#)、[設定 Amazon Redshift Python 連接器](#) 和 [設定 ODBC 連線](#)。

如需如何管理 IAM 身分的相關資訊 (包括 IAM 角色的最佳實務)，請參閱 [Amazon Redshift 中的身分和存取管理](#)。

尋找叢集連線字串

若要使用 SQL 用戶端工具來連線至叢集，您必須有叢集連線字串。您可以在 Amazon Redshift 主控台的叢集詳細資訊頁面上找到叢集連線字串。

尋找叢集的連線字串

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽功能表上，選擇叢集，然後從清單中選擇叢集名稱以開啟其詳細資訊。

3. General information (一般資訊) 區段中提供了 JDBC URL 和 ODBC URL 連線字串，以及其他詳細資訊。每個字串都以叢集執行的 AWS 區域為基礎。按一下適當連線字串旁邊的圖示以複製連線字串。

若要連線至叢集端點，您可以使用 [DescribeClusters API 要求](#) 中的叢集端點 URL。以下是叢集端點 URL 的範例。

```
mycluster.cmeaswqeuae.us-east-2.redshift.amazonaws.com
```

如果您已經為叢集設定了自訂網域名稱，您也可以使用該名稱來連線至叢集。如需建立自訂網域名稱的相關資訊，請參閱 [設定自訂網域名稱](#)。

Note

連線時，請勿使用叢集節點的 IP 地址或 VPC 端點的 IP 地址。請一律使用 Redshift 端點，以避免發生不必要的中斷。唯一會使用端點 URL 的例外狀況是當您使用自訂網域名稱時。如需詳細資訊，請參閱 [使用自訂網域名稱來進行用戶端連線](#)。

設定 Amazon Redshift JDBC 驅動程式 2.1 版的連線

您可以從許多第三方 SQL 用戶端工具使用 JDBC 驅動程式 2.1 版的連線來連線至 Amazon Redshift 叢集。Amazon Redshift JDBC 連接器會提供開放原始碼的解決方案。您可以瀏覽原始碼、請求增強功能、回報問題並提供貢獻。

若要使用 JDBC 連線，請參閱下列各節。

主題

- [下載 Amazon Redshift JDBC 驅動程式 2.1 版](#)
- [安裝 Amazon Redshift JDBC 驅動程式 2.1 版](#)
- [取得 JDBC URL](#)
- [建置連線 URL](#)
- [為 JDBC 連線設定 TCP 保持連線](#)
- [使用 Apache Maven 設定 JDBC 連線](#)
- [設定身分驗證和 SSL](#)

- [設定 記錄](#)
- [轉換資料類型](#)
- [使用預備陳述式支援](#)
- [2.1 版和 1.x 版 JDBC 驅動程式之間的差異](#)
- [建立 JDBC 驅動程式 2.1 版的初始化 \(.ini\) 檔案](#)
- [JDBC 驅動程式 2.1 版組態的選項](#)
- [JDBC 驅動程式 2.1 版之前的版本](#)

下載 Amazon Redshift JDBC 驅動程式 2.1 版

Amazon Redshift 為與 JDBC 4.2 API 相容的工具提供了驅動程式。此驅動程式的類別名稱為 `com.amazon.redshift.Driver`。

如需如何安裝 JDBC 驅動程式、參考 JDBC 驅動程式庫，以及註冊驅動程式類別的詳細資訊，請參閱下列主題。

對於您使用 Amazon Redshift JDBC 驅動程式 2.1 版的每部電腦，請確定其已安裝 Java 執行階段環境 (JRE) 8.0。

如果您使用 Amazon Redshift JDBC 驅動程式進行資料庫身分驗證，請確定您在 Java 類別路徑中具有 AWS SDK for Java 1.11.118 或更新版本。如果您尚未 AWS SDK for Java 安裝，請下載包含與 SDK 兼容 JDBC 4.2 的驅動程序和驅動程序相關庫的 ZIP 文件：AWS

- [JDBC 4.2 相容的驅動程式 2.1 版和 AWS SDK 驅動程式相關程式庫](#)

此 ZIP 檔案包含 JDBC 4.2 相容的驅動程式 2.1 版和 AWS SDK for Java 1.x 驅動程式 — 相關程式庫檔案。將相依 jar 檔案解壓縮到與 JDBC 驅動程式相同的位置。只有 JDBC 驅動程式需要在 CLASSPATH 中。

此 ZIP 檔案不包含適用於 Java 1.x 的完整 AWS 開發套件。不過，它包含適用於 Java 1.x 驅動程式的 AWS SDK，也就是 AWS Identity and Access Management (IAM) 資料庫驗證所需的相依程式庫。

將此 Amazon Redshift JDBC 驅動程式與 IAM 資料庫身份驗證所需的 AWS 開發套件搭配使用。

若要安裝適用於 Java 1.x 的完整開發 AWS 套件，請參閱開發人員指南中的[適用於 Java 1.x 的 AWS SDK for Java 開發 AWS 套件](#)。

- [JDBC 4.2 相容驅動程式 2.1 版 \(不含 AWS SDK\) 在中國 \(北京\) \(不含 SDK\) AWS](#)

檢閱 JDBC 驅動程式 2.1 版軟體授權和變更日誌檔案：

- [JDBC 驅動程式 2.1 版授權](#)
- [JDBC 驅動程式 2.1 版變更日誌](#)

JDBC 驅動程式 1.2.27.1051 版和更新版本支援 Amazon Redshift 預存程序。如需詳細資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的[在 Amazon Redshift 中建立預存程序](#)。

安裝 Amazon Redshift JDBC 驅動程式 2.1 版

若要安裝適用於 AWS 開發套件的 Amazon Redshift JDBC 4.2 相容驅動程式版本和驅動程式相依程式庫，請將檔案從 ZIP 存檔解壓縮到您選擇的目錄中。

若要安裝與 Amazon Redshift JDBC 4.2 相容的驅動程式 2.1 版 (不含 AWS 開發套件)，請將 JAR 檔案複製到您選擇的目錄。

若要使用 Amazon Redshift JDBC 驅動程式存取 Amazon Redshift 資料存放區，您需要如下所述地執行組態。

主題

- [參考 JDBC 驅動程式庫](#)
- [註冊驅動程式類別](#)

參考 JDBC 驅動程式庫

您用來連線至資料的 JDBC 應用程式或 Java 程式碼必須存取驅動程式 JAR 檔案。請在應用程式或程式碼中，指定您從 ZIP 封存檔中解壓縮的所有 JAR 檔案。

在 JDBC 應用程式中使用驅動程式

JDBC 應用程式通常會提供一組用於新增驅動程式庫檔案清單的組態選項。請使用所提供的選項，將 ZIP 封存檔中的所有 JAR 檔案納入為應用程式中驅動程式組態的一部分。如需詳細資訊，請參閱 DNS 應用程式的文件。

在 Java 程式碼中使用驅動程式

您必須在類別路徑中包含所有驅動程式庫檔案。Java 執行階段環境會在此路徑中搜尋類別和其他資源檔案。如需詳細資訊，請參閱適當的 Java SE 文件，以便為您的作業系統設定類別路徑。

- Windows : <https://docs.oracle.com/javase/7/docs/technotes/tools/windows/classpath.html>

- Linux 和 Solaris : <https://docs.oracle.com/javase/7/docs/technotes/tools/solaris/classpath.html>
- MacOS : 默認的 MacOS 類路徑是安裝 JDBC 驅動程序的目錄。

註冊驅動程式類別

請務必為您的應用程式註冊適當的類別。您可以使用下列類別將 Amazon Redshift JDBC 驅動程式連線到 Amazon Redshift 資料存放區：

- Driver 類別會擴展 `java.sql.Driver`。
- DataSource 類別會擴展 `javax.sql.DataSource` 和 `javax.sql.ConnectionPoolDataSource`。

該驅動程式支援下列完整類別名稱 (與 JDBC 版本無關)：

- `com.amazon.redshift.jdbc.Driver`
- `com.amazon.redshift.jdbc.DataSource`

下面的例子演示了如何使用 `DriverManager` 類別來建立 JDBC 4.2 的連接。

```
private static Connection connectViaDM() throws Exception
{
    Connection connection = null;
    connection = DriverManager.getConnection(CONNECTION_URL);
    return connection;
}
```

下列範例示範如何使用 `DataSource` 類別建立連線。

```
private static Connection connectViaDS() throws Exception
{
    Connection connection = null;
    11
    Amazon Redshift JDBC Driver Installation and Configuration Guide
    DataSource ds = new com.amazon.redshift.jdbc.DataSource
    ();
    ds.setURL(CONNECTION_URL);
}
```



```
connection = ds.getConnection();
return connection;
}
```

取得 JDBC URL

您需要先知道叢集的 JDBC URL，才能從 SQL 用戶端工具連線至 Amazon Redshift 叢集。JDBC URL 採用下列格式：`jdbc:redshift://endpoint:port/database`

前面格式的欄位具有下列值。

欄位	Value
<code>jdbc</code>	連線的通訊協定。
<code>redshift</code>	子通訊協定，指定使用 Amazon Redshift 驅動程式來連線至資料庫。
<code><i>endpoint</i></code>	Amazon Redshift 叢集的端點。
<code><i>port</i></code>	您啟動叢集時指定的連接埠號碼。如果有防火牆，請確定此連接埠已開放給您使用。
<code><i>database</i></code>	您為叢集建立的資料庫。

以下是 JDBC URL 範例：`jdbc:redshift://examplecluster.abc123xyz789.us-west-2.redshift.amazonaws.com:5439/dev`

請務必以 URL 編碼格式輸入 URL SessionToken 值，例如值。

如需如何取得 JDBC 連線的資訊，請參閱[尋找叢集連線字串](#)。

如果用戶端電腦無法連線至資料庫，您可以對可能的問題進行疑難排解。如需詳細資訊，請參閱[針對 Amazon Redshift 中的連線問題進行疑難排解](#)。

建置連線 URL

使用連線 URL 為您要存取的資料存放區提供連線資訊。以下是 Amazon Redshift JDBC 驅動程式 2.1 版的連線 URL 格式。在這裡，[Host] 是 Amazon Redshift 伺服器的端點，[Port] 是伺服器用來接聽用戶端請求的傳輸控制通訊協定 (TCP) 連接埠號碼。

```
jdbc:redshift://[Host]:[Port]
```

以下是會指定某些選擇性設定的連線 URL 格式。

```
jdbc:redshift://[Host]:[Port]/[database];[Property1]=[Value];  
[Property2]=[Value];
```

例如，假設您想要連線至 AWS 上美國西部 (加利佛尼亞北部) 區域中 Amazon Redshift 叢集上的連接埠 9000。您也想要存取名為 dev 的資料庫，並使用資料庫的使用者名稱和密碼來驗證連線。在此情況下，您會使用下列連線 URL。

```
jdbc:redshift://redshift.company.us-west-1.redshift.amazonaws.com:9000/  
dev;UID=amazon;PWD=amazon
```

您可以使用下列字元將組態選項與 URL 字串的其餘部分隔開：

- ;
- ?

例如，下面兩個 URL 字串是相等的：

```
jdbc:redshift://my_host:5439/dev;ssl=false;defaultRowFetchSize=100
```

```
jdbc:redshift://my_host:5439/dev?ssl=false;defaultRowFetchSize=100
```

您可以使用下列字元將 URL 字串中的組態選項彼此隔開：

- ;
- &

例如，下面兩個 URL 字串是相等的：

```
jdbc:redshift://my_host:5439/dev;ssl=false;defaultRowFetchSize=100
```

```
jdbc:redshift://my_host:5439/dev;ssl=false&defaultRowFetchSize=100
```

下列 URL 範例會指定日誌層級 6 以及日誌的路徑。

```
jdbc:redshift://redshift.amazonaws.com:5439/dev;DSILogLevel=6;LogPath=/home/user/logs;
```

請勿複製連線 URL 中的屬性。

如需可指定之組態選項的完整清單，請參閱 [JDBC 驅動程式 2.1 版組態的選項](#)。

Note

連線時，請勿使用叢集節點的 IP 地址或 VPC 端點的 IP 地址。請一律使用 Redshift 端點，以避免發生不必要的中斷。唯一會使用端點 URL 的例外狀況是當您使用自訂網域名稱時。如需詳細資訊，請參閱 [使用自訂網域名稱來進行用戶端連線](#)。

為 JDBC 連線設定 TCP 保持連線

依預設，Amazon Redshift JDBC 驅動程式會設定為使用 TCP 保持連線，以防止連線逾時。您可以指定驅動程式何時開始傳送保持連線封包，或在連線 URL 中設定相關屬性來關閉此功能。如需連線 URL 語法的相關資訊，請參閱 [建置連線 URL](#)。

屬性	描述
TCPKeepAlive	若要關閉 TCP 保持連線，請將此屬性設定為 FALSE。

使用 Apache Maven 設定 JDBC 連線

Apache Maven 是軟體專案管理和理解工具。該 AWS SDK for Java 支持阿帕奇 Maven 的項目。如需詳細資訊，請參閱《AWS SDK for Java 開發人員指南》中的 [搭配使用 SDK 與 Apache Maven](#)。

如果您使用 Apache Maven，您可以將專案設定和建置為使用 Amazon Redshift JDBC 驅動程式來連線至 Amazon Redshift 叢集。若要執行此作業，請在專案的 pom.xml 檔案中，將 JDBC 驅動程式新增為相依性。如果您使用 Maven 來建置專案，且想要使用 JDBC 連線，請採取下節中的步驟。

將 JDBC 驅動程式設定為 Maven 相依性

將 JDBC 驅動程式設定為 Maven 相依性

1. 將 Amazon 儲存庫或 Maven Central 儲存庫新增到 pom.xml 檔案的儲存庫區段。

Note

下列程式碼範例中的 URL 在瀏覽器中使用時會傳回錯誤。僅在 Maven 項目的內容中使用此 URL。

若為 Amazon Maven 儲存庫，請使用以下內容。

```
<repositories>
  <repository>
    <id>redshift</id>
    <url>http://redshift-maven-repository.s3-website-us-east-1.amazonaws.com/
release</url>
  </repository>
</repositories>
```

若要使用 Secure Sockets Layer (SSL) 來連線，請將下列儲存庫新增至 pom.xml 檔案。

```
<repositories>
  <repository>
    <id>redshift</id>
    <url>https://s3.amazonaws.com/redshift-maven-repository/release</url>
  </repository>
</repositories>
```

若為 Maven Central 儲存庫，請將以下內容新增到 pom.xml 檔案。

```
<repositories>
  <repository>
    <id>redshift</id>
    <url>https://repo1.maven.org/maven2</url>
  </repository>
</repositories>
```

2. 在 pom.xml 檔案的相依性區段中，宣告您要使用的驅動程式版本。

Amazon Redshift 為與 JDBC 4.2 API 相容的工具提供了驅動程式。如需這些驅動程式所支援功能的相關資訊，請參閱[下載 Amazon Redshift JDBC 驅動程式 2.1 版](#)。

新增驅動程式的相依性，如下所示。

以您的驅動程式版本取代下列範例中的 *driver-version*，例如 2.1.0.1。

若為 JDBC 4.2 相容驅動程式，請使用以下內容。

```
<dependency>
  <groupId>com.amazon.redshift</groupId>
  <artifactId>redshift-jdbc42</artifactId>
  <version>driver-version</version>
</dependency>
```

此驅動程式的類別名稱為 `com.amazon.redshift.Driver`。

當您使用 IAM 資料庫身分驗證時，Amazon Redshift Maven 驅動程式需要下列選擇性相依性。

```
<dependency>
  <groupId>com.amazonaws</groupId>
  <artifactId>aws-java-sdk-core</artifactId>
  <version>1.12.23</version>
  <scope>runtime</scope>
  <optional>>true</optional>
</dependency>
<dependency>
  <groupId>com.amazonaws</groupId>
  <artifactId>aws-java-sdk-redshift</artifactId>
  <version>1.12.23</version>
  <scope>runtime</scope>
  <optional>>true</optional>
</dependency>
<dependency>
  <groupId>com.amazonaws</groupId>
  <artifactId>aws-java-sdk-sts</artifactId>
  <version>1.12.23</version>
  <scope>runtime</scope>
  <optional>>true</optional>
</dependency>
```

將驅動程式升級到最新版本

若要將 Amazon Redshift JDBC 驅動程式升級或變更為最新版本，請先將相依性的版本區段修改為驅動程式的最新版本。然後以 Maven Clean Plugin 來清理專案，如下所示。

```
mvn clean
```

設定身分驗證和 SSL

為了防止有人未經授權就存取資料，Amazon Redshift 資料存放區會要求所有連線使用使用者憑證進行身分驗證。某些資料存放區還會要求必須透過 Secure Sockets Layer (SSL) 通訊協定來進行連線 (無論是否使用單向身分驗證)。

Amazon Redshift JDBC 驅動程式 2.1 版會針對這些身分驗證通訊協定提供完整支援。

驅動程式支援的 SSL 版本取決於您使用的 JVM 版本。如需每個 Java 版本所支援之 SSL 版本的相關資訊，請參閱 Java Platform Group Product Management 部落格上的[診斷 TLS、SSL 和 HTTPS](#)。

用於連線的 SSL 版本是驅動程式和伺服器支援的最高版本，而這會在連線時確定。

將 Amazon Redshift JDBC 驅動程式 2.1 版設定為根據您要連線之 Redshift 伺服器的安全需求驗證您的連線。

您一律必須提供 Redshift 使用者名稱和密碼來驗證連線。根據伺服器上是否啟用且需要 SSL，您可能還需要將驅動程式設定為透過 SSL 連接。或者，您也可以使用單向 SSL 身分驗證，以使用戶端 (驅動程式本身) 驗證伺服器的身分。

您要在連線 URL 中提供組態資訊給驅動程式。如需連線 URL 語法的相關資訊，請參閱[建置連線 URL](#)。

SSL 表示 TLS/SSL，兩者分別是 Transport Layer Security 和 Secure Sockets Layer。此驅動程式支援業界標準的 TLS/SSL 版本。

僅使用使用者名稱和密碼

如果您要連線的伺服器未使用 SSL，您只需要提供 Redshift 使用者名稱和密碼即可驗證連線。

僅使用 Redshift 使用者名稱和密碼來設定身分驗證

1. 將 UID 屬性設定為用於存取 Amazon Redshift 伺服器的 Redshift 使用者名稱。
2. 將 PWD 屬性設定為與 Redshift 使用者名稱對應的密碼。

使用 SSL 但不進行身分驗證

如果您要連線的伺服器使用 SSL，但不需要進行身分驗證，則您可以將驅動程式設定為使用非驗證 SSL Factory。

設定沒有身分驗證的 SSL 連線

1. 將 UID 屬性設定為用於存取 Amazon Redshift 伺服器的 Redshift 使用者名稱。
2. 將 PWD 屬性設定為與 Redshift 使用者名稱對應的密碼。
3. 將 SSLFactory 屬性設定為 `com.amazon.redshift.ssl.NonValidatingFactory`。

使用單向 SSL 身分驗證

如果您要連線的伺服器使用 SSL 且具有憑證，則您可以將驅動程式設定為使用單向身分驗證來驗證伺服器的身分。

單向身分驗證需要已簽署的受信任 SSL 憑證來驗證伺服器的身分。您可以將驅動程式設定為使用特定憑證，或存取包 TrustStore 含適當憑證的憑證。如果您未指定憑證或 TrustStore，則驅動程式會使用預設 Java TrustStore (通常是 `jssecacerts` 或 `cacerts`)。

設定單向 SSL 身分驗證

1. 將 UID 屬性設定為用於存取 Amazon Redshift 伺服器的 Redshift 使用者名稱。
2. 將 PWD 屬性設定為與 Redshift 使用者名稱對應的密碼。
3. 將 SSL 屬性設為 `true`。
4. 將 SSL RootCert 屬性設定為根 CA 憑證的位置。
5. 如果您沒有使用預設 Java 之一 TrustStores，請執行下列其中一個動作：
 - 若要指定伺服器憑證，請將 SSL RootCert 屬性設定為憑證的完整路徑。
 - 若要指定 TrustStore，請執行下列動作：
 - a. 使用 `keytool` 程式將伺服器憑證新增至您 TrustStore 要使用的憑證。
 - b. 指定使用驅動程式啟動 Java 應用程式時要使用的密碼 TrustStore 和密碼。例如：

```
-Djavax.net.ssl.trustStore=[TrustStoreName]
-Djavax.net.ssl.trustStorePassword=[TrustStorePassword]
-Djavax.net.ssl.trustStoreType=[TrustStoreType]
```

6. 選擇一項：
 - 若要驗證憑證，請將 SSLMode 屬性設定為 `verify-ca`。
 - 若要驗證憑證並驗證憑證中的主機名稱，請將 SSLMode 屬性設定為 `verify-full`。

設定 IAM 身分驗證

如果您要使用 IAM 身分驗證連線至 Amazon Redshift 伺服器，請將以下屬性設定為資料來源連線字串的一部分。

如需 IAM 身分驗證的相關資訊，請參閱 [Amazon Redshift 中的身分和存取管理](#)。

若要使用 IAM 身分驗證，請使用下列其中一種連線字串格式：

連接字串	描述
<code>jdbc:redshift:iam:// [host]:[port]/[db]</code>	一般連線字串。驅動程式會從主機推斷 ClusterID 和 Region。
<code>jdbc:redshift:iam:// [cluster-id]: [region]/[db]</code>	驅動程式會擷取主機資訊 (在給定 ClusterID 和 Region 的情況下)。
<code>jdbc:redshift:iam:// [host]/[db]</code>	驅動程式會預設為連接埠 5439，並從主機推斷 ClusterID 和 Region。根據您在建立、修改或遷移叢集時所選取的連接埠而定，允許存取選取的連接埠。

指定設定檔

如果您要使用 IAM 身分驗證，則可以在設定檔名稱下指定任何其他必要或選擇性的連線屬性。這樣做可讓您避免將某些資訊直接放在連線字串中。您可以使用 Profile 屬性在連線字串中指定設定檔名稱。

可以將設定檔新增至 AWS 認證檔案。此檔案的預設位置是：`~/.aws/credentials`。

您可以在下列環境變數中設定路徑來變更預設值：`AWS_CREDENTIAL_PROFILES_FILE`

如需設定檔的相關資訊，請參閱《AWS SDK for Java》中的 [使用 AWS 憑證](#)。

使用執行個體設定檔憑證

如果您要在與 IAM 角色關聯的 Amazon EC2 執行個體上執行應用程式，您可以使用執行個體設定檔憑證進行連線。

若要這麼做，請使用前面資料表中的其中一種 IAM 連線字串格式，並將 `dbuser` 連線屬性設定為您要用來連線的 Amazon Redshift 使用者名稱。

如需執行個體設定檔的相關資訊，請參閱《IAM 使用者指南》中的[存取管理](#)。

使用憑證提供者

此驅動程式也支援下列服務的憑證提供者外掛程式：

- Active Directory Federation Service (ADFS)
- JSON Web 權杖 (JWT) 服務
- Microsoft Azure Active Directory (AD) 服務和瀏覽器 Microsoft Azure Active Directory (AD) 服務
- Okta 服務
- PingFederate 服務
- 適用於 SAML 服務的瀏覽器 SAML，例如 Okta、Ping 或 ADFS

如果您使用這些服務的其中一個，連線 URL 必須指定下列屬性：

- Plugin_Name — 憑證提供者外掛程式類別的完整類別路徑。
- IDP_Host — 您用來對 Amazon Redshift 進行身分驗證的服務主機。
- IdP_Port — 用於身分驗證服務的主機監聽的連接埠。Okta 不需要此屬性。
- User — idp_host 伺服器的使用者名稱。
- Password — 與 idp_host 使用者名稱相關聯的密碼。
- DbUser — 您正在連接的 Amazon Redshift 用戶名。
- SSL_Insecure — 指出是否應驗證 IDP 伺服器憑證。
- Client_ID — 與 Azure AD 入口網站中的使用者名稱相關聯的用戶端 ID。僅用於 Azure AD。
- Client_Secret — 與 Azure AD 入口網站中的用戶端 ID 相關聯的用戶端祕密。僅用於 Azure AD。
- IdP_Tenant — Amazon Redshift 應用程式的 Azure AD 租用戶 ID。僅用於 Azure AD。
- App_ID — Amazon Redshift 應用程式的 Okta 應用程式 ID。僅用於 Okta。
- App_Name — Amazon Redshift 應用程式的 Okta 應用程式名稱 (選擇性)。僅用於 Okta。
- Partner_SPID — 選擇性的合作夥伴 SPID (服務提供者 ID) 值。僅用於 PingFederate。

如果您使用這些服務其中之一的瀏覽器外掛程式，連線 URL 也可以包括：

- Login_URL — 透過瀏覽器外掛程式使用安全性聲明標記語言 (SAML) 或 Azure AD 服務時，身分提供者網站上資源的 URL。如果您使用瀏覽器外掛程式，則必須要有此參數。

- Listn_Port — 透過瀏覽器外掛程式使用 SAML 或 Azure AD 服務時，驅動程式用來向身分提供者取得 SAML 回應的連接埠。
- IdP_Response_Timeout — 透過瀏覽器外掛程式使用 SAML 或 Azure AD 服務時，驅動程式等待身分提供者傳回 SAML 回應的時間長度 (以秒為單位)。

如需其他連線字串屬性的資訊，請參閱 [JDBC 驅動程式 2.1 版組態的選項](#)。

設定 記錄

您可以在驅動程式中開啟日誌記錄功能，以協助診斷問題。

您可以使用下列方法記錄驅動程式資訊：

- 若要將記錄的資訊儲存在 .log 檔案中，請參閱[使用日誌檔案](#)。
- 若要將記錄的資訊傳送至中 LogWriter 指定的 LogStream 或 DriverManager，請參閱[使用 LogStream 或 LogWriter](#)。

您要在連線 URL 中提供組態資訊給驅動程式。如需連線 URL 語法的相關資訊，請參閱[建置連線 URL](#)。

使用日誌檔案

日誌記錄功能應該要開啟到足以找到問題的時間長度就好。日誌記錄功能會降低效能，而且還會消耗大量磁碟空間。

在連線 URL 中設定金 LogLevel 鑰以開啟記錄功能，並指定記錄檔中包含的詳細資料量。下表列出 Amazon Redshift JDBC 驅動程式 2.1 版所提供的日誌記錄層級 (排序方式為最不詳細到最詳細)。

LogLevel 價值	描述
1	記錄會導致驅動程式中止的嚴重錯誤事件。
2	記錄可能允許驅動程式繼續執行的錯誤事件。
3	未採取動作時可能會導致錯誤的日誌事件。這個層級的日誌記錄和這個層級以上的日誌記錄層級也會記錄使用者的查詢。

LogLevel 價值	描述
4	記錄用於描述驅動程式進展的一般資訊。
5	記錄有助於偵錯驅動程式的詳細資訊。
6	記錄所有驅動程式活動。

設定會使用日誌檔案的日誌記錄功能

1. 將內 LogLevel 容設定為要包含在記錄檔中的所需資訊層級。
2. 將 LogPath 屬性設定為您要儲存記錄檔之資料夾的完整路徑。

例如，下列連線 URL 會啟用日誌記錄層級 3，並將日誌檔案儲存在 C:\temp 資料夾：

```
jdbc:redshift://redshift.company.us-west-1.redshift.amazonaws.com:9000/Default;DSILogLevel=3; LogPath=C:\temp
```

3. 若要確保新設定生效，請重新啟動 JDBC 應用程式並重新連線至伺服器。

Amazon Redshift JDBC 驅動程式會在屬性中指定的位置產生下列記錄檔：LogPath

- redshift_jdbc.log 檔案，會記錄非連線特定的驅動程式活動。
- redshift_jdbc_connection_[Number].log 檔案，會針對向資料庫建立的每個連線產生此檔案，其中 [Number] 是用來識別每個日誌檔案的編號。此檔案會記錄連線特定的驅動程式活動。

如果該 LogPath 值無效，則驅動程序將記錄的信息發送到標準輸出流 (System.out)

使用 LogStream 或 LogWriter

日誌記錄功能應該要開啟到足以找到問題的時間長度就好。日誌記錄功能會降低效能，而且還會消耗大量磁碟空間。

在連線 URL 中設定金 LogLevel 鑰以開啟記錄功能，並指定傳送至 LogStream 或中 LogWriter 指定的詳細資料量 DriverManager。

若要開啟使用 LogStream 或的記錄 LogWriter：

1. 若要設定驅動程式以記錄描述驅動程式進度的一般資訊，請將內 LogLevel 容設定為 1 或 INFO。
2. 若要確保新設定生效，請重新啟動 JDBC 應用程式並重新連線至伺服器。

若要關閉使用 LogStream 或的記錄 LogWriter：

1. 從連線 URL 移除 LogLevel 屬性。
2. 若要確保新設定生效，請重新啟動 JDBC 應用程式並重新連線至伺服器。

轉換資料類型

Amazon Redshift JDBC 驅動程式 2.1 版支援許多常見的資料格式，可在 Amazon Redshift、SQL 和 Java 資料類型之間進行轉換。

下表列出支援的資料類型對應。

Amazon Redshift 類型	SQL 類型	Java 類型
BIGINT	SQL_BIGINT	Long
BOOLEAN	SQL_BIT	Boolean
CHAR	SQL_CHAR	字串
DATE	SQL_TYPE_DATE	java.sql.Date
DECIMAL	SQL_NUMERIC	BigDecimal
DOUBLE PRECISION	SQL_DOUBLE	Double
GEOMETRY	SQL_LONGVARBINARY	byte[]
INTEGER	SQL_INTEGER	Integer
OID	SQL_BIGINT	Long
SUPER	SQL_LONGVARCHAR	字串
REAL	SQL_REAL	Float
SMALLINT	SQL_SMALLINT	Short
TEXT	SQL_VARCHAR	字串
TIME	SQL_TYPE_TIME	java.sql.Time

Amazon Redshift 類型	SQL 類型	Java 類型
TIMETZ	SQL_TYPE_TIME	java.sql.Time
TIMESTAMP	SQL_TYPE_TIMESTAMP	java.sql.Timestamp
TIMESTAMPTZ	SQL_TYPE_TIMESTAMP	java.sql.Timestamp
VARCHAR	SQL_VARCHAR	字串

使用預備陳述式支援

Amazon Redshift JDBC 驅動程式支援預備陳述式。您可以使用預備陳述式來改善需要在相同連線期間執行多次的參數化查詢效能。

預備陳述式是在伺服器端編譯但不會立即執行的 SQL 陳述式。編譯後的陳述式會以 PreparedStatement 物件的形式儲存在伺服器上，直到您關閉物件或連線為止。當該物件存在時，您可以視需要使用不同的參數值執行預備陳述式多次，而不必重新編譯陳述式。由於額外負荷降低，因此該組查詢的執行速度會變快。

如需預備陳述式的相關資訊，請參閱《Oracle 提供的 JDBC 基本概念教學課程》<https://docs.oracle.com/javase/tutorial/jdbc/basics/prepared.html>中的 < 使用預備陳述式 >。

您可以準備包含多個查詢的陳述式。例如，下列預備陳述式包含兩個 INSERT 查詢：

```
PreparedStatement pstmt = conn.prepareStatement("INSERT INTO
MyTable VALUES (1, 'abc'); INSERT INTO CompanyTable VALUES
(1, 'abc');");
```

請注意，這些查詢不會依賴相同預備陳述式中所指定其他查詢的結果。由於準備步驟期間不會執行查詢，因此系統尚未傳回結果，因此沒有結果可供相同預備陳述式中的其他查詢使用。

例如，系統不會允許下列會先建立資料表，然後將值插入該新建資料表的預備陳述式：

```
PreparedStatement pstmt = conn.prepareStatement("CREATE
TABLE MyTable(col1 int, col2 varchar); INSERT INTO myTable
VALUES (1, 'abc');");
```

如果您嘗試準備這個陳述式，伺服器會傳回錯誤，指出目的地資料表 (myTable) 尚不存在。必須先執行 CREATE 查詢，才可以準備 INSERT 查詢。

2.1 版和 1.x 版 JDBC 驅動程式之間的差異

本節說明 2.1 版和 1.x 版 JDBC 驅動程式所傳回資訊的差異。JDBC 驅動程式 1.x 版已停止使用。

下表列出 `getDatabaseProductName()` 和 `Version()` 函數針對每個 `getDatabaseProduct` 版本 JDBC 驅動程式所傳回的 `DatabaseMetadata` 資訊。JDBC 驅動程式 2.1 版會在建立連線時取得值。JDBC 驅動程式 1.x 版會從查詢結果取得值。

JDBC 驅動程式版本	得到 <code>DatabaseProduct</code> 名稱 () 結果	獲取 <code>DatabaseProduct</code> 版本 () 結果
2.1	Redshift	8.0.2
1.x	PostgreSQL	08.00.0002

下表列出 `getTypeInfo` 函數針對每個版本 JDBC 驅動程式傳回的 `DatabaseMetadata` 資訊。

JDBC 驅動程式版本	<code>getTypeInfo</code> 結果
2.1	與 Redshift 資料類型一致
1.x	與 PostgreSQL 資料類型一致

建立 JDBC 驅動程式 2.1 版的初始化 (.ini) 檔案

透過使用 Amazon Redshift JDBC 驅動程式 2.1 版的初始化 (.ini) 檔案，您可以指定系統層級的組態參數。例如，每個應用程式的聯合 IdP 身分驗證參數可能會有所不同。 .ini 檔案會提供通用位置讓 SQL 用戶端取得所需的組態參數。

您可以建立包含 SQL 用戶端組態選項的 JDBC 驅動程式 2.1 版初始化 (.ini) 檔案。檔案的預設名稱為 `rsjdbc.ini`。JDBC 驅動程式 2.1 版會在下列位置 (依優先順序列出) 檢查 .ini 檔案：

- 連線 URL 或 SQL 用戶端的連線屬性對話方塊中的 `IniFile` 參數。請確定 `IniFile` 參數包含 .ini 檔案的完整路徑 (包括檔案名稱)。如需 `IniFile` 參數的詳細資訊，請參閱 [IniFile](#)。如果 `IniFile` 參數未正確指定 .ini 檔案的位置，則會顯示錯誤。
- 具有完整路徑 (包括檔案名稱在內) 的環境變數，例如 `AMAZON_REDSHIFT_JDBC_INI_FILE`。您可以使用 `rsjdbc.ini` 或指定檔案名稱。如果 `AMAZON_REDSHIFT_JDBC_INI_FILE` 環境變數未正確指定 .ini 檔案的位置，則會顯示錯誤。

- 驅動程式 JAR 檔案所在的目錄。
- 使用者主目錄。
- 系統的臨時目錄。

您可以將 .ini 檔案組織為多個驅動，例如 [DRIVER]。每個區段包含指定各種連線參數的鍵值對。您可以使用 IniSection 參數來指定 .ini 檔案中的區段。如需 IniSection 參數的詳細資訊，請參閱 [IniSection](#)。

以下是 .ini 檔案格式的範例，其中包含 [DRIVER]、[DEV]、[QA] 和 [PROD] 區段。[DRIVER] 區段可套用到任何連線。

```
[DRIVER]
key1=val1
key2=val2

[DEV]
key1=val1
key2=val2

[QA]
key1=val1
key2=val2

[PROD]
key1=val1
key2=val2
```

JDBC 驅動程式 2.1 版會從下列位置 (依優先順序列出) 載入組態參數：

- 應用程式程式碼中的預設組態參數。
- .ini 檔案中的 [DRIVER] 區段屬性 (如果包含的話)。
- 自訂區段組態參數 (如果有在連線 URL 或 SQL 用戶端的連線屬性對話方塊中提供 IniSection 選項的話)。
- 來自 getConnection 呼叫中所指定連線屬性物件的屬性。
- 連線 URL 中所指定的組態參數。

JDBC 驅動程式 2.1 版組態的選項

接下來，您可以找到可為 Amazon Redshift JDBC 驅動程式 2.1 版指定的選項描述。組態選項不區分大小寫。

您可以使用連線 URL 設定組態屬性。如需詳細資訊，請參閱 [建置連線 URL](#)。

主題

- [AccessKey 身份證](#)
- [允許分貝 UserOverride](#)
- [App_ID](#)
- [App_Name](#)
- [ApplicationName](#)
- [AuthProfile](#)
- [AutoCreate](#)
- [Client_ID](#)
- [Client_Secret](#)
- [ClusterID \(ClusterID\)](#)
- [壓縮](#)
- [connectTimeout](#)
- [connectionTimezone](#)
- [資料庫 MetadataCurrent DbOnly](#)
- [DbUser](#)
- [DbGroups](#)
- [DBNAME](#)
- [預設RowFetch大小](#)
- [DisableIsValidQuery](#)
- [啟用FetchRing緩衝區](#)
- [啟用 S MultiSql support](#)
- [獲取RingBuffer大小](#)
- [ForceLowercase](#)

- [groupFederation](#)
- [HOST](#)
- [IAM DisableCache](#)
- [IAMDuration](#)
- [Identity_Namespace](#)
- [IdP_Host](#)
- [IdP_Port](#)
- [IdP_Tenant](#)
- [IdP_Response_Timeout](#)
- [IniFile](#)
- [IniSection](#)
- [isServerless](#)
- [Login_URL](#)
- [loginTimeout](#)
- [登錄 ToRp](#)
- [LogLevel](#)
- [LogPath](#)
- [OverrideSchemaPatternType](#)
- [Partner_SPID](#)
- [密碼](#)
- [Plugin_Name](#)
- [PORT](#)
- [Preferred_Role](#)
- [設定檔](#)
- [PWD](#)
- [queryGroup](#)
- [readOnly](#)
- [區域](#)

- [重新WriteBatched插入](#)
- [重新 WriteBatched InsertsSize](#)
- [roleArn](#)
- [角色 SessionName](#)
- [scope](#)
- [SecretAccess](#) 關鍵
- [SessionToken](#)
- [無伺服器 AcctId](#)
- [無伺服器 WorkGroup](#)
- [socketFactory](#)
- [socketTimeout](#)
- [SSL](#)
- [SSL_Insecure](#)
- [SSLCert](#)
- [SSLFactory](#)
- [SSLKey](#)
- [SSLMode](#)
- [SSLPassword](#)
- [SSL RootCert](#)
- [StsEndpoint](#) 網址
- [TCP KeepAlive](#)
- [token](#)
- [令牌類型](#)
- [UID](#)
- [使用者](#)
- [網頁 IdentityToken](#)

AccessKey 身份證

- 預設值 — 無

- 資料類型 — 字串

您可以指定此參數以輸入使用者或角色的 IAM 存取金鑰。您通常可以透過查看和現有字串或使用者設定檔來找到金鑰。如果您指定此參數，則還必須指定 `SecretAccessKey` 參數。如果在 JDBC 網址中傳遞，則 `AccessKey` 識別碼必須經過 URL 編碼。

此為選用參數。

允許分貝 `UserOverride`

- 預設值 — 0
- 資料類型 — 字串

此選項會指定驅動程式是使用 SAML 聲明中的 `DbUser` 值，還是使用連線 URL 中 `DbUser` 連線屬性所指定的值。

此為選用參數。

1

驅動程式會使用 SAML 聲明中的 `DbUser` 值。

如果 SAML 聲明未針對 `DBUser` 指定值，則驅動程式會使用 `DBUser` 連線屬性中指定的值。如果連線屬性也未指定值，則驅動程式會使用連線設定檔中指定的值。

0

驅動程式會使用 `DBUser` 連線屬性中指定的 `DBUser` 值。

如果 `DBUser` 連線屬性未指定值，則驅動程式會使用連線設定檔中指定的值。如果連線設定檔也未指定值，則驅動程式會使用 SAML 聲明中的值。

`App_ID`

- 預設值 — 無
- 資料類型 — 字串

與您的 Amazon Redshift 應用程式相關聯、Okta 所提供的唯一 ID。

如果透過 Okta 服務進行驗證，則需要此參數。

App_Name

- 預設值 — 無
- 資料類型 — 字串

您用來驗證與 Amazon Redshift 之連線的 Okta 應用程式名稱。

此為選用參數。

ApplicationName

- 預設值 — Null
- 資料類型 — 字串

要傳遞給 Amazon Redshift 以進行稽核的應用程式名稱。

此為選用參數。

AuthProfile

- 預設值 — 無
- 資料類型 — 字串

用於連線至 Amazon Redshift 的身分驗證設定檔名稱。

此為選用參數。

AutoCreate

- 預設值 — false
- 資料類型 — 布林值

此選項會指定當指定的使用者不存在時，驅動程式是否要導致系統建立新的使用者。

此為選用參數。

true

如果 DBUser 或唯一 ID (UID) 指定的使用者不存在，則系統會建立具有該名稱的新使用者。

false

驅動程式不會導致系統建立新的使用者。如果指定的使用者不存在，則身分驗證會失敗。

Client_ID

- 預設值 — 無
- 資料類型 — 字串

使用 Azure AD 服務來驗證連線時要使用的用戶端 ID。

如果透過 Azure AD 服務進行驗證，則需要此參數。

Client_Secret

- 預設值 — 無
- 資料類型 — 字串

使用 Azure AD 服務來驗證連線時要使用的用戶端秘密。

如果透過 Azure AD 服務進行驗證，則需要此參數。

ClusterID (ClusterID)

- 預設值 — 無
- 資料類型 — 字串

您要連線至的 Amazon Redshift 叢集的名稱。驅動程式會嘗試從給定的主機偵測此參數。如果您使用 Network Load Balancer (NLB) 並透過 IAM 進行連線，則驅動程式無法偵測此參數，因此您可以使用此連線選項設定此參數。

此為選用參數。

壓縮

- 預設值 — 關閉
- 資料類型 — 字串

用於 Amazon Redshift 伺服器與用戶端或驅動程式之間的有線通訊協定通訊的壓縮方法。

此為選用參數。

您可以指定下列值：

- lz4

將用於與 Amazon Redshift 進行有線通訊協定通訊的壓縮方法設定為 lz4。

- off

不要對與 Amazon Redshift 進行的有線通訊協定通訊使用壓縮。

connectTimeout

- 預設值 — 10
- 資料類型 — 整數

用於通訊端連線操作的逾時值。如果建立 Amazon Redshift 連線所需的時間超過此值，系統就會將此連線視為無法使用。逾時會以秒為單位來指定。值為 0 表示未指定逾時。

此為選用參數。

connectionTimezone

- 預設值 — LOCAL
- 資料類型 — 字串

工作階段層級時區。

此為選用參數。

您可以指定下列值：

LOCAL

將工作階段層級時區設定為 LOCAL JVM 時區。

SERVER

將工作階段層級時區設定為在 Amazon Redshift 伺服器上為使用者設定的時區。您可以使用以下命令為使用者設定工作階段層級時區：

```
ALTER USER  
[...]  
SET TIMEZONE TO [...];
```

資料庫 MetadataCurrent DbOnly

- 預設值 — true
- 資料類型 — 布林值

此選項指定中繼資料 API 會從所有可存取的資料庫擷取資料，還是僅從已連線的資料庫擷取資料。

此為選用參數。

您可以指定下列值：

true

應用程式會從單一資料庫擷取中繼資料。

false

應用程式會從所有可存取的資料庫擷取中繼資料。

DbUser

- 預設值 — 無
- 資料類型 — 字串

要與您的 Amazon Redshift 帳戶搭配使用的使用者 ID。如果您已啟用 AutoCreate 屬性，則可以使用目前不存在的 ID。

此為選用參數。

DbGroups

- 預設值 — PUBLIC
- 資料類型 — 字串

DBUser 針對目前的工作階段所加入之現有資料庫群組名稱的逗號分隔清單。

此為選用參數。

DBNAME

- 預設值 — Null
- 資料類型 — 字串

要連線到之資料庫的名稱。您可以使用此選項在 JDBC 連線 URL 中指定資料庫名稱。

此為必要參數。您必須在連線 URL 或用戶端應用程式的連線屬性中指定資料庫名稱。

預設RowFetch大小

- 預設值 — 0
- 資料類型 — 整數

此選項指定的預設值 `getFetchSize`。

此為選用參數。

您可以指定下列值：

0

在單一操作中擷取所有資料列。

正整數

每次擷取反覆運算時，要從資料庫擷取的資料列數目 `ResultSet`。

DisableIsValidQuery

- 預設值 — False
- 資料類型 — 布林值

此選項會指定驅動程式在使用 `Connection.isValid()` 方法判斷資料庫連線是否處於作用中狀態時，是否要提交新的資料庫查詢。

此為選用參數。

true

驅動程式在使用 `Connection.isValid()` 判斷資料庫連線是否處於作用中狀態時，不會提交查詢。如果資料庫伺服器意外關閉，這可能會造成驅動程式錯誤地將資料庫連線識別為作用中狀態。

false

驅動程式在使用 `Connection.isValid()` 判斷資料庫連線是否處於作用中狀態時，會提交查詢。

啟用FetchRing緩衝區

- 預設值 — true
- 資料類型 — 布林值

此選項指定驅動程式會在個別執行緒上使用環形緩衝器來擷取資料列。S `fetchRingBufferSize` 參數指定環形緩衝區的大小。

如果交易偵測到包含多個以分號分隔的 SQL 命令的陳述式，則該交易的擷取環緩衝區會設定為 false。enableFetchRing緩衝區的值不會改變。

此為選用參數。

啟用 S MultiSql support

- 預設值 — true
- 資料類型 — 布林值

此選項會指定是否要在陳述式中處理以分號分隔的多個 SQL 命令。

此為選用參數。

您可以指定下列值：

true

驅動程式會在陳述式物件中處理以分號分隔的多個 SQL 命令。

false

驅動程式會在單一陳述式中傳回多個 SQL 命令的錯誤。

獲取RingBuffer大小

- 預設值 — 1G
- 資料類型 — 字串

此選項會指定在擷取結果集時使用的環形緩衝區大小。您可以指定以位元組為單位的大小，例如 1K 表示 1 KB、5000 表示 5,000 個位元組、1M 表示 1 MB、1G 表示 1 GB，依此類推。您也可以指定堆積記憶體의百分比。驅動程式會在達到限制時停止擷取資料列。當應用程式讀取資料列並釋放環形緩衝區中的空間時，擷取操作便會繼續。

此為選用參數。

ForceLowercase

- 預設值 — false
- 資料類型 — 布林值

此選項指定在使用單一登入身分驗證時，驅動程式是否將從身分提供者傳送至 Amazon Redshift 的所有資料庫群組 (DbGroups) 減少其大小寫。

此為選用參數。

true

驅動程式會將從身分提供者傳送的所有資料庫群組轉換為小寫。

false

驅動程式不會變更資料庫群組。

groupFederation

- 預設值 — false
- 資料類型 — 布林值

此選項會指定是否使用 Amazon Redshift IDP 群組。這是由 GetClusterCredentials V2 API 所支援。

此為選用參數。

true

使用 Amazon Redshift 身分提供者 (IdP) 群組。

false

使用 STS API 和使 GetClusterCredentials 用者聯合，並明確指定 DbGroups 連線。

HOST

- 預設值 — Null
- 資料類型 — 字串

要連線到之 Amazon Redshift 伺服器的主機名稱。您可以使用此選項在 JDBC 連線 URL 中指定主機名稱。

此為必要參數。您必須在連線 URL 或用戶端應用程式的連線屬性中指定主機名稱。

IAM DisableCache

- 預設值 — false
- 資料類型 — 布林值

此選項會指定是否快取 IAM 憑證。

此為選用參數。

true

不快取 IAM 憑證。

false

快取 IAM 憑證。例如，當對於 API 閘道的請求遭到限流時，這可以提高效能。

IAMDuration

- 預設值 — 900
- 資料類型 — 整數

臨時 IAM 憑證到期之前的時間長度 (以秒為單位)。

- 最小值 — 900
- 最大值 — 3,600

此為選用參數。

Identity_Namespace

- 預設值 — 無
- 資料類型 — 字串

使用驗證時要使用的 IdpTokenAuthPlugin 識別名稱空間。它可協助 Redshift 判斷要使用哪個 IAM Identity Center 執行個體。

如果只存在一個 IAM Identity Center 執行個體，或者已設定預設身分命名空間，則此參數為選用參數，否則為必要參數。

IdP_Host

- 預設值 — 無
- 資料類型 — 字串

您用來對 Amazon Redshift 進行身分驗證的 IdP (身分提供者) 主機。這可以在連線字串或設定檔中指定。

此為選用參數。

IdP_Port

- 預設值 — 無
- 資料類型 — 字串

IdP (身分提供者) 使用的連接埠。您可以在連線字串或設定檔中指定連接埠。預設連接埠為 5439。根據您在建立、修改或遷移叢集時所選取的連接埠而定，允許存取選取的連接埠。

此為選用參數。

IdP_Tenant

- 預設值 — 無
- 資料類型 — 字串

Amazon Redshift 應用程式的 Azure AD 租用戶 ID。

如果透過 Azure AD 服務進行驗證，則需要此參數。

IdP_Response_Timeout

- 預設值 — 120
- 資料類型 — 整數

透過瀏覽器外掛程式使用 SAML 或 Azure AD 服務時，驅動程式等待身分提供者傳回 SAML 回應的時間長度 (以秒為單位)。

此為選用參數。

IniFile

- 預設值 — 無
- 資料類型 — 字串

.ini 檔案的完整路徑 (包括檔案名稱)。例如：

```
IniFile="C:\tools\rjdbc.ini"
```

如需 .ini 檔案的相關資訊，請參閱[建立 JDBC 驅動程式 2.1 版的初始化 \(.ini\) 檔案](#)。

此為選用參數。

IniSection

- 預設值 — 無
- 資料類型 — 字串

.ini 檔案中包含組態選項之區段的名稱。如需 .ini 檔案的相關資訊，請參閱[建立 JDBC 驅動程式 2.1 版的初始化 \(.ini\) 檔案](#)。

下列範例會指定 .ini 檔案的 [Prod] 區段：

```
IniSection="Prod"
```

此為選用參數。

isServerless

- 預設值 — false
- 資料類型 — 布林值

此選項會指定 Amazon Redshift 端點主機是否為無伺服器執行個體。驅動程式會嘗試從給定的主機偵測此參數。如果您使用 Network Load Balancer (NLB)，則驅動程式無法偵測此參數，因此您可以在此設定此參數。

此為選用參數。

true

Amazon Redshift 端點主機是無伺服器執行個體。

false

Amazon Redshift 端點主機是已佈建的叢集。

Login_URL

- 預設值 — 無
- 資料類型 — 字串

透過瀏覽器外掛程式使用 SAML 或 Azure AD 服務時，身分提供者網站上資源的 URL。

如果透過瀏覽器外掛程式向 SAML 或 Azure AD 服務進行驗證，則需要此參數。

loginTimeout

- 預設值 — 0
- 資料類型 — 整數

連線至伺服器並進行驗證時，逾時之前等待的秒數。如果建立連線所花的時間超過此臨界值，連線會中止。

當此屬性設為 0 時，連線不會逾時。

此為選用參數。

登錄 ToRp

- 預設值 — `urn:amazon:webservices`
- 資料類型 — 字串

您要用於 AD FS 身分驗證類型的依賴方信任。

此為選用參數。

LogLevel

- 預設值 — 0
- 資料類型 — 整數

使用此屬性可在驅動程式中開啟或關閉日誌記錄，以及指定日誌檔案中包含的詳細資訊數量。

日誌記錄功能應該要啟用到足以找到問題的時間長度就好。日誌記錄功能會降低效能，而且還會消耗大量磁碟空間。

此為選用參數。

將此參數設為以下其中一個值：

0

停用所有日誌記錄功能。

1

在 FATAL 層級上啟用日誌記錄功能，這會記錄會導致驅動程式中止的極嚴重錯誤事件。

2

在 ERROR 層級上啟用日誌記錄功能，這會記錄可能仍允許驅動程式繼續執行的錯誤事件。

3

在 WARNING 層級上啟用日誌記錄功能，這會記錄如果未採取動作可能會導致錯誤的事件。

4

在 INFO 層級上啟用日誌記錄功能，這會記錄描述驅動程式進度的一般資訊。

5

在 DEBUG 層級上啟用日誌記錄功能，這會記錄有助於偵錯驅動程式的詳細資訊。

6

在 TRACE 層級上啟用日誌記錄功能，這會記錄所有驅動程式活動。

在啟用日誌記錄功能時，驅動程式會在 LogPath 屬性所指定的位置產生下列日誌檔案：

- **redshift_jdbc.log** — 記錄非連線特定驅動程式活動的檔案。
- **redshift_jdbc_connection_[Number].log** — 向資料庫建立的每個連線的檔案，其中 [Number] 是用來區別每個日誌檔案的編號。此檔案會記錄連線特定的驅動程式活動。

如果該 LogPath 值無效，驅動程序將記錄的信息發送到標準輸出流，System.out。

LogPath

- 預設值 — 目前的工作目錄。
- 資料類型 — 字串

啟用 DSI LogLevel 內容時，驅動程式儲存記錄檔之資料夾的完整路徑。

為了確定連線 URL 會與所有 JDBC 應用程式相容，建議您輸入另一個反斜線來逸出檔案路徑中的反斜線 (\)。

此為選用參數。

OverrideSchemaPatternType

- 預設值 — Null
- 資料類型 — 整數

此選項會指定是否要覆寫 getTables 呼叫中使用的查詢類型。

0

無結構描述通用查詢

1

本機結構描述查詢

2

外部結構描述查詢

此為選用參數。

Partner_SPID

- 預設值 — 無
- 資料類型 — 字串

使用服務驗證連線時要使用的夥伴 SPID (服務提供者 ID) 值。 PingFederate

此為選用參數。

密碼

- 預設值 — 無
- 資料類型 — 字串

透過 IDP 使用 IAM 身分驗證進行連線時，這是 IDP_Host 伺服器的密碼。使用標準身分驗證時，這可以用於 Amazon Redshift 資料庫密碼，而不是 PWD。

此為選用參數。

Plugin_Name

- 預設值 — 無
- 資料類型 — 字串

用來實作特定憑證提供者外掛程式的完整類別名稱。

此為選用參數。

支援的提供者選項如下：

- **AdfsCredentialsProvider**— 作用中目錄聯合服務。
- **AzureCredentialsProvider**— Microsoft Azure 活動目錄 (AD) 服務。
- **BasicJwtCredentialsProvider**— JSON 網絡令牌 (JWT) 服務。
- **BasicSamlCredentialsProvider** — 可與許多 SAML 服務提供者搭配使用的安全性聲明標記語言 (SAML) 憑證。
- **BrowserAzureCredentialsProvider**— 瀏覽器 Microsoft Azure 活動目錄 (AD) 服務。
- **BrowserAzureOAuth2CredentialsProvider**— 瀏覽器 Microsoft Azure 活動目錄 (AD) 本機身份驗證服務。
- **BrowserSamlCredentialsProvider**— 用於 SAML 服務的瀏覽器 SAML，例如 Okta，Ping 或 ADFS。
- **IdpTokenAuthPlugin**-一種授權插件，可從鏈接到 IAM 身份中心的任何 Web 身份提供商中接受 IAM 身份中心令牌或 OpenID Connect (OIDC) 基於 JSON 的身份令牌 (JWT)。
- **OktaCredentialsProvider**— 確定服務。
- **PingCredentialsProvider**— PingFederate 服務。

PORT

- 預設值 — Null
- 資料類型 — 整數

要連線到之 Amazon Redshift 伺服器的連接埠。您可以使用此選項在 JDBC 連線 URL 中指定連接埠。

此為選用參數。

Preferred_Role

- 預設值 — 無
- 資料類型 — 字串

您要在連線到 Amazon Redshift 期間擔任的 IAM 角色。

此為選用參數。

設定檔

- 預設值 — 無
- 資料類型 — 字串

要用於 IAM 身分驗證之設定檔的名稱。此設定檔包含未在連線字串中指定的任何其他連線屬性。

此為選用參數。

PWD

- 預設值 — 無
- 資料類型 — 字串

與您使用屬性 UID 提供的 Amazon Redshift 使用者名稱對應的密碼。

此為選用參數。

queryGroup

- 預設值 — Null
- 資料類型 — 字串

此選項會在執行期將查詢指派給適當的查詢群組，以便將查詢指派給佇列。系統會針對工作階段設定查詢群組。在連線上執行的所有查詢都屬於此查詢群組。

此為選用參數。

readOnly

- 預設值 — false
- 資料類型 — 布林值

此屬性會指定驅動程式是否處於唯讀模式。

此為選用參數。

true

連線處於唯讀模式，且無法寫入到資料存放區。

false

連線不處於唯讀模式，可以寫入到資料存放區。

區域

- 預設值 — Null
- 資料類型 — 字串

此選項指定叢集所在的 AWS 區域。如果您指定選 StsEndPoint 項，則會忽略「區域」選項。Redshift GetClusterCredentials API 操作也會使用區域選項。

此為選用參數。

重新WriteBatched插入

- 預設值 — false
- 資料類型 — 布林值

此選項可實現最佳化，以重寫相容的 INSERT 陳述式並將這些陳述式合併為批次。

此為選用參數。

重新 WriteBatched InsertsSize

- 預設值 — 128
- 資料類型 — 整數

此選項可實現最佳化，以重寫相容的 INSERT 陳述式並將這些陳述式合併為批次。此值必須以 2 的冪呈指數增加。

此為選用參數。

roleArn

- 預設值 — 無

- 資料類型 — 字串

角色的 Amazon Resource Name (ARN)。當您 BasicJwtCredentialsProvider 為 Plugin_Name 選項指定時，請務必指定此參數。請以下列格式指定 ARN：

```
arn:partition:service:region:account-id:resource-id
```

如果您 BasicJwtCredentialsProvider 為「外掛程式名稱」選項指定此參數，則必須使用此參數。

角色 SessionName

- 預設值 — jwt_redshift_session
- 資料類型 — 字串

擔任角色工作階段的識別碼。一般來說，您會傳遞與應用程式使用者相關聯的名稱或識別碼。應用程式使用的臨時安全憑證會與該使用者相關聯。當您 BasicJwtCredentialsProvider 為外掛程式名稱選項指定時，您可以指定此參數。

此為選用參數。

scope

- 預設值 — 無
- 資料類型 — 字串

使用者可以同意的範圍清單 (以空格分隔)。指定這個參數可讓您的 Microsoft Azure 應用程式針對您想要呼叫的 API 取得同意。當您 CredentialsProvider 為外掛程式名稱選項指定 BrowserAzure OAuth2 時，您可以指定此參數。

BrowserAzureOAuth2 CredentialsProvider 外掛程式需要此參數。

SecretAccessKey 關鍵

- 預設值 — 無
- 資料類型 — 字串

使用者或角色的 IAM 存取金鑰。如果指定，則還必須指定 AccessKey ID。如果在 JDBC 網址中傳遞，則 SecretAccessKey 必須進行 URL 編碼。

此為選用參數。

SessionToken

- 預設值 — 無
- 資料類型 — 字串

與您用來驗證的 IAM 角色相關聯的臨時 IAM 工作階段權杖。如果在 JDBC URL 中傳遞，則臨時 IAM 工作階段權杖必須經過 URL 編碼。

此為選用參數。

無伺服器 AcctId

- 預設值 — Null
- 資料類型 — 字串

Amazon Redshift Serverless 帳戶 ID。驅動程式會嘗試從給定的主機偵測此參數。如果您使用 Network Load Balancer (NLB)，則驅動程式無法偵測此參數，因此您可以在此設定此參數。

此為選用參數。

無伺服器 WorkGroup

- 預設值 — Null
- 資料類型 — 字串

Amazon Redshift Serverless 工作群組名稱。驅動程式會嘗試從給定的主機偵測此參數。如果您使用 Network Load Balancer (NLB)，則驅動程式無法偵測此參數，因此您可以在此設定此參數。

此為選用參數。

socketFactory

- 預設值 — Null
- 資料類型 — 字串

此選項會指定用於建立通訊端的通訊端 Factory。

此為選用參數。

socketTimeout

- 預設值 — 0
- 資料類型 — 整數

在通訊端讀取操作期間，逾時之前等待的秒數。如果操作所花的時間超過此臨界值，連線會關閉。當此屬性設為 0 時，連線不會逾時。

此為選用參數。

SSL

- 預設值 — TRUE
- 資料類型 — 字串

使用此屬性可開啟或關閉連線的 SSL。

此為選用參數。

您可以指定下列值：

TRUE

驅動程式會透過 SSL 連線到伺服器。

FALSE

驅動程式會以不使用 SSL 的方式連線到伺服器。IAM 身分驗證不支援此選項。

或者，您可以配置 AuthMech 屬性。

SSL_Insecure

- 預設值 — true
- 資料類型 — 字串

此屬性會指出是否應驗證 IDP 主機伺服器憑證。

此為選用參數。

您可以指定下列值：

true

驅動程式不會檢查 IDP 伺服器憑證的真實性。

false

驅動程式會檢查 IDP 伺服器憑證的真實性。

SSLCert

- 預設值 — 無
- 資料類型 — 字串

包含可在使用 SSL 時驗證 Amazon Redshift 伺服器執行個體之其他受信任 CA 憑證的 .pem 或 .crt 檔案的完整路徑。

如果指定 SSLKey，則需要此參數。

SSLFactory

- 預設值 — 無
- 資料類型 — 字串

在不使用伺服器憑證的情況下，透過 TLS/SSL 連線至伺服器時要使用的 SSL Factory。

SSLKey

- 預設值 — 無
- 資料類型 — 字串

包含用於驗證 SSLCert 中所指定憑證的 PKCS8 金鑰檔案的 .der 檔案完整路徑。

如果指定 SSLCert，則需要此參數。

SSLMode

- 預設值 — verify-ca
- 資料類型 — 字串

使用此屬性可指定在已啟用 TLS/SSL 時，驅動程式會如何驗證憑證。

此為選用參數。

您可以指定下列值：

verify-ca

驅動程式會驗證憑證是否來自受信任的憑證授權機構 (CA)。

verify-full

驅動程式會驗證憑證是否來自受信任的 CA，以及憑證中的主機名稱是否符合連線 URL 中指定的主機名稱。

SSLPassword

- 預設值 — 0
- 資料類型 — 字串

SSLKey 中所指定已加密金鑰檔案的密碼。

如果指定了 SSLKey 且金鑰檔案已加密，則需要此參數。

SSL RootCert

- 預設值 — 無
- 資料類型 — 字串

包含可在使用 SSL 時驗證 Amazon Redshift 伺服器執行個體之根 CA 憑證的 .pem 或 .crt 檔案的完整路徑。

StsEndpoint网址

- 預設值 — Null
- 資料類型 — 字串

您可以指定 AWS Security Token Service (AWS STS) 端點。如果您指定此選項，系統會忽略區域選項。您只能為此端點指定安全的通訊協定 (HTTPS)。

TCP KeepAlive

- 預設值 — TRUE
- 資料類型 — 字串

使用此屬性可開啟或關閉 TCP 保持連線。

此為選用參數。

您可以指定下列值：

TRUE

驅動程式會使用 TCP 保持連線來防止連線逾時。

FALSE

驅動程式不會使用 TCP 保持連線。

token

- 預設值 — 無
- 資料類型 — 字串

IAM 身分中心提供的存取權杖或 OpenID Connect (OIDC) JSON 網頁權杖 (JWT)，由與 IAM 身分中心連結的網路身分提供者所提供。您的應用程式必須透過 IAM 身分中心或與 IAM 身分中心連結的身分提供者驗證應用程式的使用者，以產生此權杖。

此參數可搭配使用 `IdpTokenAuthPlugin`。

令牌類型

- 預設值 — 無
- 資料類型 — 字串

正在中使用的權杖類型 `IdpTokenAuthPlugin`。

您可以指定下列值：

訪問令牌

如果您使用 IAM 身分中心提供的存取權杖，請輸入此選項。

EXT_JWT

如果您使用 OpenID Connect (OIDC) JSON 網頁權杖 (JWT)，這是由與 IAM 身分中心整合的網頁型身分提供者所提供的，請輸入此選項。

此參數可搭配使用 IdpTokenAuthPlugin。

UID

- 預設值 — 無
- 資料類型 — 字串

您用來存取資料庫的資料庫使用者名稱。

此為必要參數。

使用者

- 預設值 — 無
- 資料類型 — 字串

透過 IDP 使用 IAM 身分驗證進行連線時，這是 idp_host 伺服器的使用者名稱。使用標準身分驗證時，這可以用於 Amazon Redshift 資料庫使用者名稱。

此為選用參數。

網頁 IdentityToken

- 預設值 — 無
- 資料類型 — 字串

由身分提供者提供的 OAuth 2.1 存取權杖或 OpenID Connect ID 權杖。您的應用程式必須透過使用 Web 身分提供者對應用程式的使用者進行身分驗證來獲取此權杖。當您 BasicJwtCredentialsProvider 為 Plugin_Name 選項指定時，請務必指定此參數。

如果您 BasicJwtCredentialsProvider 為「外掛程式名稱」選項指定此參數，則必須使用此參數。

JDBC 驅動程式 2.1 版之前的版本

請在您的工具需要特定版本的驅動程式時，才下載 Amazon Redshift JDBC 驅動程式 2.1 版之前的版本。

下列是之前的 JDBC 4.2 相容 JDBC 驅動程式 2.1 版驅動程式：

- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.28/redshift-jdbc42-2.1.0.28.zip>
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.26/redshift-jdbc42-2.1.0.26.zip>
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.25/redshift-jdbc42-2.1.0.25.zip>
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.24/redshift-jdbc42-2.1.0.24.zip>
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.23/redshift-jdbc42-2.1.0.23.zip>
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.22/redshift-jdbc42-2.1.0.22.zip>
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.21/redshift-jdbc42-2.1.0.21.zip>
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.20/redshift-jdbc42-2.1.0.20.zip>
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.19/redshift-jdbc42-2.1.0.19.zip>
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.18/redshift-jdbc42-2.1.0.18.zip>
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.17/redshift-jdbc42-2.1.0.17.zip>
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.16/redshift-jdbc42-2.1.0.16.zip>
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.15/redshift-jdbc42-2.1.0.15.zip>
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.14/redshift-jdbc42-2.1.0.14.zip>
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.13/redshift-jdbc42-2.1.0.13.zip>
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.12/redshift-jdbc42-2.1.0.12.zip>
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.11/redshift-jdbc42-2.1.0.11.zip>
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.10/redshift-jdbc42-2.1.0.10.zip>
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.9/redshift-jdbc42-2.1.0.9.zip>
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.8/redshift-jdbc42-2.1.0.8.zip>
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.7/redshift-jdbc42-2.1.0.7.zip>

設定 Amazon Redshift Python 連接器

透過使用適用於 Python 的 Amazon Redshift 連接器，您可以將工作與 [AWS SDK for Python \(Boto3\)](#)，以及熊貓和數字 Python () 整合。NumPy 有關熊貓的更多信息，請參閱 [熊貓存儲庫 GitHub](#)。如需有關的詳細資訊 NumPy，請參閱 [NumPy GitHub 存放庫](#)。

Amazon Redshift Python 連接器提供了一個開放原始碼的解決方案。您可以瀏覽原始碼、請求增強功能、回報問題並提供貢獻。

若要使用 Amazon Redshift Python 連線器，請確定您的 Python 是 3.6 版或更新版本。如需詳細資訊，請參閱 [Amazon Redshift Python 驅動程式授權合約](#)。

Amazon Redshift Python 連接器可提供以下功能：

- AWS Identity and Access Management (IAM) 身份驗證。如需詳細資訊，請參閱 [Amazon Redshift 中的身分和存取管理](#)。
- 使用聯合 API 存取的身分提供者身分驗證。以下企業身分提供者可支援聯合 API 存取：
 - Azure AD。如需詳細資訊，請參閱 AWS 大數據部落格文章與 [Microsoft Azure AD 單一登入聯合 Amazon Redshift 存取](#)。
 - Active Directory Federation Services。如需詳細資訊，請參閱 AWS 大數據部落格文章與 [使用中目錄同盟服務 \(AD FS\) 聯合存取 Amazon Redshift 叢集：第 1 部分](#)。
 - Okta。如需詳細資訊，請參閱 AWS 大數據部落格文章與 [身分供應商身分供應商身分與 Okta 聯合存取 Amazon Redshift](#)。
 - PingFederate。如需詳細資訊，請參閱 [PingFederate 網站](#)。
 - JumpCloud。如需詳細資訊，請參閱 [JumpCloud 網站](#)。
- Amazon Redshift 資料類型。

Amazon Redshift Python 連接器會實作 Python Database API Specification 2.0。如需詳細資訊，請參閱 Python 網站上的 [PEP 249—Python Database API Specification v2.0](#)。

主題

- [安裝 Amazon Redshift Python 連接器](#)
- [Amazon Redshift Python 連接器的組態選項](#)
- [匯入 Python 連接器](#)
- [整合 Python 連接器 NumPy](#)
- [將 Python 連接器與 pandas 進行整合](#)
- [使用身分提供者外掛程式](#)
- [使用 Amazon Redshift Python 連接器的範例](#)
- [Amazon Redshift Python 連接器的 API 參考](#)

安裝 Amazon Redshift Python 連接器

您可以使用下列任一方法來安裝 Amazon Redshift Python 連線器：

- Python Package Index (PyPI)
- Conda
- 複製存 GitHub 放庫

從 PyPI 安裝 Python 連接器

若要從 Python Package Index (PyPI) 安裝 Python 連線器，您可以使用 pip。若要進行這項動作，請執行以下命令。

```
>>> pip install redshift_connector
```

您可以在虛擬環境內安裝連接器。若要進行這項動作，請執行以下命令。

```
>>> pip install redshift_connector
```

或者，您可以安裝熊貓和 NumPy 連接器。

```
>>> pip install "redshift_connector[full]"
```

如需 pip 的相關資訊，請參閱 [pip 網站](#)。

從 Conda 安裝 Python 連接器

您可以從 Anaconda.org 安裝 Python 連接器。

```
>>>conda install -c conda-forge redshift_connector
```

透過從中複製 GitHub 儲存庫來安裝 Python 連接器 AWS

若要從來源安裝 Python 連接器，請從複製 GitHub 儲存庫 AWS。在安裝 Python 和 virtualenv 後，請透過執行以下命令來設定環境並安裝所需的相依性。

```
$ git clone https://github.com/aws/amazon-redshift-python-driver.git
$ cd RedshiftPythonDriver
```

```
$ virtualenv venv
$ . venv/bin/activate
$ python -m pip install -r requirements.txt
$ python -m pip install -e .
$ python -m pip install redshift_connector
```

Amazon Redshift Python 連接器的組態選項

接下來，您可以找到可為 Amazon Redshift Python 連接器指定之選項的描述。

access_key_id

- 預設值 — 無
- 資料類型 — 字串

針對 IAM 資料庫身分驗證而設定之 IAM 角色或使用者的存取金鑰。

此為選用參數。

allow_db_user_override

- 預設值 — False
- 資料類型 — 布林值

True

指定連接器會使用安全性聲明標記語言 (SAML) 聲明中的 DbUser 值。

False

指定使用 DbUser 連線參數中的值。

此為選用參數。

app_name

- 預設值 — 無
- 資料類型 — 字串

用於身分驗證之身分提供者 (IdP) 應用程式的名稱。

此為選用參數。

auth_profile

- 預設值 — 無
- 資料類型 — 字串

具有 JSON 形式連線屬性之 Amazon Redshift 身分驗證設定檔的名稱。如需有關命名連線參數的詳細資訊，請參閱 RedshiftProperty 類別。RedshiftProperty 類別會儲存最終使用者提供的連線參數，以及 (適用的話) 在 IAM 身分驗證程序 (例如臨時 IAM 憑證) 進行期間產生的連線參數。如需詳細資訊，請參閱[RedshiftProperty 類別](#)。

此為選用參數。

auto_create

- 預設值 — False
- 資料類型 — 布林值

此值會指出是否要在使用者不存在時建立使用者。

此為選用參數。

client_id

- 預設值 — 無
- 資料類型 — 字串

來自 Azure IdP 的用戶端 ID。

此為選用參數。

client_secret

- 預設值 — 無
- 資料類型 — 字串

來自 Azure IdP 的用戶端祕密。

此為選用參數。

`cluster_identifier`

- 預設值 — 無
- 資料類型 — 字串

Amazon Redshift 叢集的叢集識別碼。

此為選用參數。

`credentials_provider`

- 預設值 — 無
- 資料類型 — 字串

用於以 Amazon Redshift 進行驗證的 IdP。有效值如下：

- `AdfsCredentialsProvider`
- `AzureCredentialsProvider`
- `BrowserAzureCredentialsProvider`
- `BrowserAzureOAuth2CredentialsProvider`
- `BrowserSamlCredentialsProvider`
- `IdpTokenAuthPlugin`-一種授權插件，可從鏈接到 IDC 的任何 Web 身份提供程序接受身份中心 (IdC) 令牌或 OpenID Connect (OIDC) 基於 JSON 的身份令牌 (JWT)。
- `PingCredentialsProvider`
- `OktaCredentialsProvider`

此為選用參數。

`database`

- 預設值 — 無
- 資料類型 — 字串

要連線到之資料庫的名稱。

此為必要參數。

database_metadata_current_db_only

- 預設值 — True
- 資料類型 — 布林值

此值會指出應用程式是否支援多資料庫資料共用型錄。預設值 True 會指出應用程式不會為了回溯相容性而支援多資料庫資料共用型錄。

此為選用參數。

db_groups

- 預設值 — 無
- 資料類型 — 字串

以逗號分隔的現有資料庫群組名稱清單，由目前階段作業的 DbUser 聯結指示使用者。

此為選用參數。

db_user

- 預設值 — 無
- 資料類型 — 字串

要與 Amazon Redshift 搭配使用的使用者 ID。

此為選用參數。

endpoint_url

- 預設值 — 無
- 資料類型 — 字串

Amazon Redshift 端點的 URL。此選項僅供 AWS 內部使用。

此為選用參數。

group_federation

- 預設值 — False
- 資料類型 — 布林值

此選項會指定是否使用 Amazon Redshift IDP 群組。

此為選用參數。

true

使用 Amazon Redshift 身分提供者 (IdP) 群組。

false

使用 STS API 和使 GetClusterCredentials 用者聯合，並為連線指定資料庫群組。

託管

- 預設值 — 無
- 資料類型 — 字串

Amazon Redshift 叢集的主機名稱。

此為選用參數。

iam

- 預設值 — False
- 資料類型 — 布林值

會啟用 IAM 身分驗證。

此為必要參數。

iam_disable_cache

- 預設值 — False
- 資料類型 — 布林值

此選項會指定是否快取 IAM 憑證。預設會快取 IAM 憑證。當對於 API 閘道的請求遭到限流時，這可以提高效能。

此為選用參數。

識別名稱空間

- 默認值-空
- 資料類型 — 字串

使 IdpTokenAuthPlugin 用進行驗證時使用的身份名稱空間。它可協助 Redshift 決定要使用哪個身分識別中心執行個體。

如果只有一個 Identity Center 執行個體現有或已設定預設身分識別命名空間，則此參數為選擇性參數。否則該項目為必要項目。

idpPort

- 預設值 — 7890
- 資料類型 — 整數

IdP 會將 SAML 聲明傳送到的接聽連接埠。

此為必要參數。

idp_response_timeout

- 預設值 — 120
- 資料類型 — 整數

從 IdP 擷取 SAML 聲明的逾時。

此為必要參數。

idp_tenant

- 預設值 — 無
- 資料類型 — 字串

IdP 租用戶。

此為選用參數。

listen_port

- 預設值 — 7890
- 資料類型 — 整數

IdP 會將 SAML 聲明傳送到的接聽連接埠。

此為選用參數。

login_url

- 預設值 — 無
- 資料類型 — 字串

IdP 的單一登入 Url。

此為選用參數。

max_prepared_statements

- 預設值 — 1000
- 資料類型 — 整數

可同時開啟的預備陳述式數量上限。

此為必要參數。

numeric_to_float

- 預設值 — False
- 資料類型 — 布林值

此選項指定連接器是否會將數值資料類型值從 decimal.Decimal 轉換為浮點數。依預設，連接器會接收 decimal.Decimal 形式的數值資料類型值，且不會對值進行轉換。

對於需要精確度的使用案例，不建議您啟用 `numeric_to_float`，因為得到的結果可能會經過四捨五入。

如需 `decimal.Decimal` 以及其與浮點數之間權衡的相關資訊，請參閱 Python 網站上的 [小數 — 固定小數點和浮點數](#)。

此為選用參數。

`partner_sp_id`

- 預設值 — 無
- 資料類型 — 字串

針對以 Ping 進行的身分驗證所使用的合作夥伴 SP ID。

此為選用參數。

密碼

- 預設值 — 無
- 資料類型 — 字串

用於身分驗證的密碼。

此為選用參數。

`port`

- 預設值 — 5439
- 資料類型 — 整數

Amazon Redshift 叢集的連接埠號碼。

此為必要參數。

`preferred_role`

- 預設值 — 無
- 資料類型 — 字串

目前連線偏好的 IAM 角色。

此為選用參數。

principal_arn

- 預設值 — 無
- 資料類型 — 字串

要為其產生政策之使用者或 IAM 角色的 Amazon Resource Name (ARN)。建議您將政策連接至角色，然後將角色指派給您的使用者以提供存取權。

此為選用參數。

profile

- 預設值 — 無
- 資料類型 — 字串

認證檔案中包含 AWS 身分 AWS 證明的設定檔名稱。

此為選用參數。

provider_name

- 預設值 — 無
- 資料類型 — 字串

Redshift 原生身分驗證提供者的名稱。

此為選用參數。

region

- 預設值 — 無
- 資料類型 — 字串

叢集所 AWS 區域 在的位置。

此為選用參數。

role_arn

- 預設值 — 無
- 資料類型 — 字串

呼叫者所擔任角色的 Amazon Resource Name (ARN)。JwtCredentialsProvider 所指出的提供者會使用此參數。

若為 JwtCredentialsProvider 提供者，此為必要參數。否則，此為選擇性參數。

role_session_name

- 預設值 — jwt_redshift_session
- 資料類型 — 字串

擔任角色工作階段的識別碼。一般來說，您會傳遞與應用程式使用者相關聯的名稱或識別碼。應用程式使用的臨時安全憑證會與該使用者相關聯。JwtCredentialsProvider 所指出的提供者會使用此參數。

此為選用參數。

scope

- 預設值 — 無
- 資料類型 — 字串

使用者可以同意的範圍清單 (以空格分隔)。指定這個參數可讓您的應用程式針對您想要呼叫的 API 取得同意。當 CredentialsProvider 為認證 _ 提供者選項指定 BrowserAzure OAuth2 時，您可以指定此參數。

BrowserAzureOAuth2 CredentialsProvider 外掛程式需要此參數。

secret_access_key_id

- 預設值 — 無
- 資料類型 — 字串

針對 IAM 資料庫身分驗證而設定之 IAM 角色或使用者的私密存取金鑰。

此為選用參數。

session_token

- 預設值 — 無
- 資料類型 — 字串

針對 IAM 資料庫身分驗證而設定之 IAM 角色或使用者的存取金鑰。如果使用臨時 AWS 認證，則需要此參數。

此為選用參數。

serverless_acct_id

- 預設值 — 無
- 資料類型 — 字串

Amazon Redshift Serverless 帳戶 ID。

此為選用參數。

serverless_work_group

- 預設值 — 無
- 資料類型 — 字串

Amazon Redshift Serverless 工作群組名稱。

此為選用參數。

ssl

- 預設值 — True
- 資料類型 — 布林值

會啟用 Secure Sockets Layer (SSL)。

此為必要參數。

ssl_insecure

- 預設值 — True
- 資料類型 — 布林值

此值會指定是否要驗證 IdP 主機伺服器憑證。

此為選用參數。

sslmode

- 預設值 — verify-ca
- 資料類型 — 字串

連線至 Amazon Redshift 的安全。您可以指定下列任一項：

- verify-ca
- verify-full

此為必要參數。

timeout

- 預設值 — 無
- 資料類型 — 整數

對伺服器的連線在逾時前要經過的秒數。

此為選用參數。

token

- 預設值 — 無
- 資料類型 — 字串

IAM 身分中心提供的存取權杖或 OpenID Connect (OIDC) JSON 網頁權杖 (JWT)，由與 IAM 身分中心連結的網路身分提供者所提供。您的應用程式必須透過 IAM 身分中心或與 IAM 身分中心連結的身分提供者驗證應用程式的使用者，以產生此權杖。

此參數可搭配使用 `IdpTokenAuthPlugin`。

令牌類型

- 預設值 — 無
- 資料類型 — 字串

正在中使用的權杖類型 `IdpTokenAuthPlugin`。

您可以指定下列值：

訪問令牌

如果您使用 IAM 身分中心提供的存取權杖，請輸入此選項。

EXT_JWT

如果您使用 OpenID Connect (OIDC) JSON 網頁權杖 (JWT)，這是由與 IAM 身分中心整合的網頁型身分提供者所提供的，請輸入此選項。

此參數可搭配使用 `IdpTokenAuthPlugin`。

使用者

- 預設值 — 無
- 資料類型 — 字串

用於身分驗證的使用者名稱。

此為選用參數。

web_identity_token

- 預設值 — 無
- 資料類型 — 字串

由身分提供者提供的 OAuth 2.0 存取權杖或 OpenID Connect ID 權杖。請確保您的應用程式會透過以 Web 身分提供者對應用程式的使用者進行驗證來取得此權杖。`JwtCredentialsProvider` 所指出的提供者會使用此參數。

若為 `JwtCredentialsProvider` 提供者，此為必要參數。否則，此為選擇性參數。

匯入 Python 連接器

若要匯入 Python 連接器，請執行以下命令。

```
>>> import redshift_connector
```

導入 NumPy 並連接到 Amazon Redshift

若要匯入 Amazon Redshift Python 連接器和數字 Python (NumPy)，請執行下列命令。

```
import redshift_connector
import numpy
```

若要使用 AWS 登入資料連線到 Amazon Redshift 叢集，請執行下列命令。

```
conn = redshift_connector.connect(
    host='examplecluster.abc123xyz789.us-west-1.redshift.amazonaws.com',
    port=5439,
    database='dev',
    user='awsuser',
    password='my_password'
)
```

整合 Python 連接器 NumPy

以下是與 Python 連接器集成的一個例子 NumPy。

```
>>> import numpy
#Connect to the cluster
>>> import redshift_connector
>>> conn = redshift_connector.connect(
    host='examplecluster.abc123xyz789.us-west-1.redshift.amazonaws.com',
    port=5439,
    database='dev',
    user='awsuser',
    password='my_password'
)
```

```
# Create a Cursor object
>>> cursor = conn.cursor()

# Query and receive result set
cursor.execute("select * from book")

result: numpy.ndarray = cursor.fetch_numpy_array()
print(result)
```

結果如下。

```
[['One Hundred Years of Solitude' 'Gabriel García Márquez']
 ['A Brief History of Time' 'Stephen Hawking']]
```

將 Python 連接器與 pandas 進行整合

以下是將 Python 連接器與 pandas 進行整合的範例。

```
>>> import pandas

#Connect to the cluster
>>> import redshift_connector
>>> conn = redshift_connector.connect(
    host='examplecluster.abc123xyz789.us-west-1.redshift.amazonaws.com',
    port=5439,
    database='dev',
    user='awsuser',
    password='my_password'
)

# Create a Cursor object
>>> cursor = conn.cursor()

# Query and receive result set
cursor.execute("select * from book")
result: pandas.DataFrame = cursor.fetch_dataframe()
print(result)
```

使用身分提供者外掛程式

如需如何使用身分提供者外掛程式的一般資訊，請參閱[提供 IAM 登入資料的選項](#)。如需如何管理 IAM 身分的相關資訊 (包括 IAM 角色的最佳實務)，請參閱 [Amazon Redshift 中的身分和存取管理](#)。

使用 ADFS 身分提供者外掛程式進行身分驗證

以下是使用 Active Directory Federation Service (ADFS) 身分提供者外掛程式來針對連線至 Amazon Redshift 資料庫的使用者進行驗證的範例。

```
>>> con = redshift_connector.connect(
    iam=True,
    database='dev',
    host='my-testing-cluster.abc.us-east-2.redshift.amazonaws.com',
    cluster_identifier='my-testing-cluster',
    credentials_provider='AdfsCredentialsProvider',
    user='brooke@myadfshostname.com',
    password='Hunter2',
    idp_host='myadfshostname.com'
)
```

使用 Azure 身分提供者外掛程式進行身分驗證

以下是使用 Azure 身分提供者外掛程式進行身分驗證的範例。您可以為 Azure 企業應用程式建立 `client_id` 和 `client_secret` 的值，如下所示。

```
>>> con = redshift_connector.connect(
    iam=True,
    database='dev',
    host='my-testing-cluster.abc.us-east-2.redshift.amazonaws.com',
    cluster_identifier='my-testing-cluster',
    credentials_provider='AzureCredentialsProvider',
    user='brooke@myazure.org',
    password='Hunter2',
    idp_tenant='my_idp_tenant',
    client_id='my_client_id',
    client_secret='my_client_secret',
    preferred_role='arn:aws:iam:123:role/DataScientist'
)
```

使用 Azure Browser 身分提供者外掛程式進行身分驗證

以下是使用 Azure Browser 身分提供者外掛程式來針對連線至 Amazon Redshift 資料庫的使用者進行驗證的範例。

由使用者提供登入憑據的瀏覽器會進行多重要素驗證。

```
>>>con = redshift_connector.connect(
```

```
iam=True,  
database='dev',  
host='my-testing-cluster.abc.us-east-2.redshift.amazonaws.com',  
cluster_identifier='my-testing-cluster',  
credentials_provider='BrowserAzureCredentialsProvider',  
idp_tenant='my_idp_tenant',  
client_id='my_client_id',  
)
```

使用 Okta 身分提供者外掛程式進行身分驗證

以下是使用 Okta 身分提供者外掛程式進行身分驗證的範例。您可以透過 Okta 應用程式取得 `idp_host`、`app_id` 和 `app_name` 的值。

```
>>> con = redshift_connector.connect(  
    iam=True,  
    database='dev',  
    host='my-testing-cluster.abc.us-east-2.redshift.amazonaws.com',  
    cluster_identifier='my-testing-cluster',  
    credentials_provider='OktaCredentialsProvider',  
    user='brooke@myazure.org',  
    password='hunter2',  
    idp_host='my_idp_host',  
    app_id='my_first_appetizer',  
    app_name='dinner_party'  
)
```

使用通用 JumpCloud 用 SAML 瀏覽器身分識別提供者外掛程式的驗證

以下是使用通用 JumpCloud SAML 瀏覽器身分識別提供者外掛程式進行驗證的範例。

密碼是必要參數。但是，您不必輸入此參數，因為瀏覽器會進行多重要素驗證。

```
>>> con = redshift_connector.connect(  
    iam=True,  
    database='dev',  
    host='my-testing-cluster.abc.us-east-2.redshift.amazonaws.com',  
    cluster_identifier='my-testing-cluster',  
    credentials_provider='BrowserSamlCredentialsProvider',  
    user='brooke@myjumpcloud.org',  
    password='',  
    login_url='https://sso.jumpcloud.com/saml2/plustwo_melody'  
)
```

使用 Amazon Redshift Python 連接器的範例

以下是如何使用 Amazon Redshift Python 連接器的範例。若要執行這些範例，您必須先安裝 Python 連接器。如需安裝 Amazon Redshift Python 連接器的相關資訊，請參閱[安裝 Amazon Redshift Python 連接器](#)。如需可與 Python 連接器搭配使用之組態選項的相關資訊，請參閱[Amazon Redshift Python 連接器的組態選項](#)。

主題

- [使用登入資料連接和查詢 Amazon Redshift 叢集 AWS](#)
- [啟用自動遞交](#)
- [設定游標 paramstyle](#)
- [使用 COPY 從 Amazon S3 儲存貯體複寫資料，然後使用 UNLOAD 將資料寫入至 Amazon S3 儲存貯體](#)

使用登入資料連接和查詢 Amazon Redshift 叢集 AWS

下列範例會引導您使用登入資料連線至 Amazon Redshift 叢集，然後查詢 AWS 資料表並擷取查詢結果。

```
#Connect to the cluster
>>> import redshift_connector
>>> conn = redshift_connector.connect(
    host='examplecluster.abc123xyz789.us-west-1.redshift.amazonaws.com',
    database='dev',
    port=5439,
    user='awsuser',
    password='my_password'
)

# Create a Cursor object
>>> cursor = conn.cursor()

# Query a table using the Cursor
>>> cursor.execute("select * from book")

#Retrieve the query result set
>>> result: tuple = cursor.fetchall()
>>> print(result)
>> (['One Hundred Years of Solitude', 'Gabriel García Márquez'], ['A Brief History of Time', 'Stephen Hawking'])
```


啟用自動遞交

自動遞交屬性會預設為關閉，以遵循 Python Database API Specification。執行復原命令後，您可以使用以下命令開啟連線的 `autocommit` 屬性，以確保沒有進行中的交易。

```
#Connect to the cluster
>>> import redshift_connector
>>> conn = redshift_connector.connect(...)

# Run a rollback command
>>> conn.rollback()

# Turn on autocommit
>>> conn.autocommit = True
>>> conn.run("VACUUM")

# Turn off autocommit
>>> conn.autocommit = False
```

設定游標 paramstyle

游標的 `paramstyle` 可透過 `cursor.paramstyle` 進行修改。所使用的預設 `paramstyle` 是 `format`。此參數的有效值為 `qmark`、`numeric`、`named`、`format` 和 `pyformat`。

以下是使用各種 `paramstyle` 將參數傳遞至範例 SQL 陳述式的範例。

```
# qmark
redshift_connector.paramstyle = 'qmark'
sql = 'insert into foo(bar, jar) VALUES(?, ?)'
cursor.execute(sql, (1, "hello world"))

# numeric
redshift_connector.paramstyle = 'numeric'
sql = 'insert into foo(bar, jar) VALUES(:1, :2)'
cursor.execute(sql, (1, "hello world"))

# named
redshift_connector.paramstyle = 'named'
sql = 'insert into foo(bar, jar) VALUES(:p1, :p2)'
cursor.execute(sql, {"p1":1, "p2":"hello world"})
```

```
# format
redshift_connector.paramstyle = 'format'
sql = 'insert into foo(bar, jar) VALUES(%s, %s)'
cursor.execute(sql, (1, "hello world"))

# pyformat
redshift_connector.paramstyle = 'pyformat'
sql = 'insert into foo(bar, jar) VALUES(%(bar)s, %(jar)s)'
cursor.execute(sql, {"bar": 1, "jar": "hello world"})
```

使用 COPY 從 Amazon S3 儲存貯體複寫資料，然後使用 UNLOAD 將資料寫入至 Amazon S3 儲存貯體

下列範例顯示如何將資料從 Amazon S3 儲存貯體複製到資料表，然後從該資料表卸載回儲存貯體。

名為 category_csv.txt 且包含下列資料的文字檔案會上傳至 Amazon S3 儲存貯體：

```
12,Shows,Musicals,Musical theatre
13,Shows,Plays,"All ""non-musical"" theatre"
14,Shows,Opera,"All opera, light, and ""rock"" opera"
15,Concerts,Classical,"All symphony, concerto, and choir concerts"
```

以下是 Python 程式碼範例，其會先連線至 Amazon Redshift 資料庫。然後，會建立名為 category 的資料表，並將 S3 儲存貯體中的 CSV 資料複製到資料表中。

```
#Connect to the cluster and create a Cursor
>>> import redshift_connector
>>> with redshift_connector.connect(...) as conn:
>>> with conn.cursor() as cursor:

#Create an empty table
>>> cursor.execute("create table category (catid int, cargroup varchar, catname
  varchar, catdesc varchar)")

#Use COPY to copy the contents of the S3 bucket into the empty table
>>> cursor.execute("copy category from 's3://testing/category_csv.txt' iam_role
  'arn:aws:iam::123:role/RedshiftCopyUnload' csv;")

#Retrieve the contents of the table
>>> cursor.execute("select * from category")
>>> print(cursor.fetchall())

#Use UNLOAD to copy the contents of the table into the S3 bucket
```

```
>>> cursor.execute("unload ('select * from category') to 's3://testing/
unloaded_category_csv.txt' iam_role 'arn:aws:iam::123:role/RedshiftCopyUnload' csv;")

#Retrieve the contents of the bucket
>>> print(cursor.fetchall())
>> ([12, 'Shows', 'Musicals', 'Musical theatre'], [13, 'Shows', 'Plays', 'All "non-
musical" theatre'], [14, 'Shows', 'Opera', 'All opera, light, and "rock" opera'], [15,
'Concerts', 'Classical', 'All symphony, concerto, and choir concerts'])
```

如果您未將 `autocommit` 設定為 `true`，請在執行 `execute()` 陳述式後使用 `conn.commit()` 遞交。

資料會卸載到 S3 儲存貯體中的 `unloaded_category_csv.text0000_part00` 檔案中，其內容如下：

```
12,Shows,Musicals,Musical theatre
13,Shows,Plays,"All ""non-musical"" theatre"
14,Shows,Opera,"All opera, light, and ""rock"" opera"
15,Concerts,Classical,"All symphony, concerto, and choir concerts"
```

Amazon Redshift Python 連接器的 API 參考

接下來，您可以找到 Amazon Redshift Python 連線器 API 操作的描述。

`redshift_connector`

接下來，您可以找到 `redshift_connector` API 操作的描述。

```
connect(user, database, password[, port, ...])
```

建立對 Amazon Redshift 叢集的連線。此函數會驗證使用者輸入、選擇性地使用身分提供者外掛程式進行驗證，然後建構連線物件。

```
apilevel
```

支援 DBAPI 層級，目前為「2.0」。

```
paramstyle, str(object='') -> str str(bytes_or_buffer[, encoding[, errors]])
-> str
```

要全域使用的資料庫 API 參數樣式。

連線

接下來，您可以找到 Amazon Redshift Python 連接器的連線 API 操作描述。

```
__init__(user, password, database[, host, ...])
```

將原始連線物件初始化。

```
cursor
```

建立繫結至此連線的游標物件。

```
commit
```

遞交目前的資料庫交易。

```
rollback
```

復原目前的資料庫交易。

```
close
```

關閉資料庫連線。

```
execute(cursor, operation, vals)
```

執行指定的 SQL 命令。根據 `redshift_connector.paramstyle` 的值，您可以提供序列或映射形式的參數。

```
run(sql[, stream])
```

執行指定的 SQL 命令。您可以選擇性提供與 COPY 命令搭配使用的串流。

```
xid(format_id, global_transaction_id, ...)
```

建立交易 ID。只有 `global_transaction_id` 參數會用於 postgres。 `format_id` 和 `branch_qualifier` 不會用於 postgres。 `global_transaction_id` 可以是由傳回元組 (`format_id, global_transaction_id, branch_qualifier`) 的 postgres 支援的任何字串識別碼。

```
tpc_begin(xid)
```

使用由格式 ID、全域交易 ID 和分支限定詞組成的交易 ID `xid` 來開始 TPC 交易。

```
tpc_prepare
```

執行以 `.tpc_begin` 開始之交易的第一個階段。

```
tpc_commit([xid])
```

以無引數方式呼叫時，`.tpc_commit` 會遞交先前使用 `.tpc_prepare()` 所準備的 TPC 交易。

```
tpc_rollback([xid])
```

以無引數方式呼叫時，`.tpc_rollback` 會復原 TPC 交易。

tpc_recover

傳回適合與 `.tpc_commit(xid)` 或 `.tpc_rollback(xid)` 搭配使用的待定交易 ID 清單。

游標

接下來，您可以找到游標 API 操作的描述。

```
__init__(connection[, paramstyle])
```

將原始游標物件初始化。

```
insert_data_bulk(filename, table_name, parameter_indices, column_names,
delimiter, batch_size)
```

執行大量 INSERT 陳述式。

```
execute(operation[, args, stream, ...])
```

執行資料庫操作。

```
executemany(operation, param_sets)
```

準備資料庫操作，然後針對所提供的所有參數序列或映射執行此操作。

```
fetchone
```

擷取查詢結果集的下一列。

```
fetchmany([num])
```

擷取下一組查詢結果資料列。

```
fetchall
```

擷取查詢結果的所有剩餘資料列。

```
close
```

立即關閉游標。

```
__iter__
```

可對游標物件進行迭代以從查詢中擷取資料列。

```
fetch_dataframe([num])
```

傳回上次查詢結果的資料框。

```
write_dataframe(df, table)
```

將相同結構資料框寫入到 Amazon Redshift 資料庫。

```
fetch_numpy_array([num])
```

返回最後一個查詢結果的 NumPy 數組。

```
get_catalogs
```

Amazon Redshift 不支援來自單一連線的多個型錄。Amazon Redshift 只會傳回目前的型錄。

```
get_tables([catalog, schema_pattern, ...])
```

傳回系統內使用者定義的唯一公有資料表。

```
get_columns([catalog, schema_pattern, ...])
```

傳回 Amazon Redshift 資料庫中特定資料表內所有資料欄的清單。

AdfsCredentialsProvider 插件

以下是 Amazon Redshift Python 連接器 AdfsCredentialsProvider 插件 API 操作的語法。

```
redshift_connector.plugin.AdfsCredentialsProvider()
```

AzureCredentialsProvider 插件

以下是 Amazon Redshift Python 連接器 AzureCredentialsProvider 插件 API 操作的語法。

```
redshift_connector.plugin.AzureCredentialsProvider()
```

BrowserAzureCredentialsProvider 插件

以下是 Amazon Redshift Python 連接器 BrowserAzureCredentialsProvider 插件 API 操作的語法。

```
redshift_connector.plugin.BrowserAzureCredentialsProvider()
```

BrowserSamlCredentialsProvider 插件

以下是 Amazon Redshift Python 連接器 BrowserSamlCredentialsProvider 插件 API 操作的語法。

```
redshift_connector.plugin.BrowserSamlCredentialsProvider()
```

OktaCredentialsProvider 插件

以下是 Amazon Redshift Python 連接器 OktaCredentialsProvider 插件 API 操作的語法。

```
redshift_connector.plugin.OktaCredentialsProvider()
```

PingCredentialsProvider 插件

以下是 Amazon Redshift Python 連接器 PingCredentialsProvider 插件 API 操作的語法。

```
redshift_connector.plugin.PingCredentialsProvider()
```

SamlCredentialsProvider 插件

以下是 Amazon Redshift Python 連接器 SamlCredentialsProvider 插件 API 操作的語法。

```
redshift_connector.plugin.SamlCredentialsProvider()
```

Apache Spark 的 Amazon Redshift 整合

[Apache Spark](#) 是一種分散式處理架構和程式設計模型，可協助您執行機器學習、串流處理或圖形分析。與 Apache Hadoop 類似，Spark 是一種開放原始碼、分散式處理系統，通常用於大數據的工作負載。Spark 具有經過最佳化的有向無環圖 (DAG) 執行引擎，並且會主動快取記憶體中的資料。這可以提高效能，對於某些算法和互動式查詢來說更是如此。

這項整合可為您提供 Spark 連接器，讓您用於建置在 Amazon Redshift 和 Amazon Redshift Serverless 中讀取和寫入資料的 Apache Spark 應用程式。這些應用程式不會影響應用程式效能或資料的交易一致性。這項整合會自動納入到 [Amazon EMR](#) 和 [AWS Glue](#)，因此您可以立即執行會在資料擷取和轉換管道中存取資料並將資料載入到 Amazon Redshift 的 Apache Spark 任務。

目前，您可以搭配這項整合使用 Spark 3.3.0、3.3.1、3.3.2 和 3.4.0 版。

這項整合會提供下列功能：

- AWS Identity and Access Management (IAM) 身分驗證。如需詳細資訊，請參閱 [Amazon Redshift 中的身分和存取管理](#)。
- 述詞和查詢下推，以提升效能。
- Amazon Redshift 資料類型。
- 對 Amazon Redshift 和 Amazon Redshift Serverless 的連線。

使用 Spark 連接器時的考量和限制

- tempdir URI 會指向 Amazon S3 位置。此臨時目錄不會自動清理，因此可能會增加額外的費用。建議您使用《Amazon Simple Storage Service 使用者指南》中的 [Amazon S3 生命週期政策](#) 來定義 Amazon S3 儲存貯體的保留規則。
- 根據預設，如果 S3 儲存貯體和 Redshift 叢集位於不同的 AWS 區域，Amazon S3 和 Redshift 之間便無法進行複製操作。若要使用不同的 AWS 區域，請將 tempdir_region 參數設定為用於 tempdir 的 S3 儲存貯體區域。
- 如果使用 tempformat 參數寫入 Parquet 資料，則會在 S3 和 Redshift 之間進行跨區域寫入。
- 建議您使用 [Amazon S3 伺服器端加密](#) 來加密所用的 Amazon S3 儲存貯體。
- 建議您 [封鎖對 Amazon S3 儲存貯體的公開存取](#)。
- 建議您不要將 Amazon Redshift 叢集設為可公開存取。
- 建議您開啟 [Amazon Redshift 稽核記錄](#)。
- 建議您開啟 [Amazon Redshift 靜態加密](#)。
- 建議您針對從 Amazon EMR 上的 Spark 到 Amazon Redshift 的 JDBC 連線開啟 SSL。
- 建議您使用 Amazon Redshift 身分驗證參數的 aws_iam_role 參數傳遞 IAM 角色。

使用 Spark 連接器進行身分驗證

下圖描述了 Amazon S3、Amazon Redshift、Spark 驅動程式和 Spark 執行程式之間的身分驗證。

Redshift 和 Spark 之間的身分驗證

您可以使用 Amazon Redshift 提供的 JDBC 驅動程式第 2 版，透過指定登入憑證使用 Spark 連接器連線到 Amazon Redshift。若要使用 IAM，請 [設定 JDBC url 以使用 IAM 身分驗證](#)。若要從 Amazon EMR 或 AWS Glue 連線到 Redshift 叢集，請確定您的 IAM 角色有可用來擷取暫時 IAM 憑證的必要許可。下列清單描述 IAM 角色要擷取憑證和執行 Amazon S3 操作所需的所有許可。

- [Redshift:GetClusterCredentials](#) (適用於佈建的 Redshift 叢集)
- [Redshift:DescribeClusters](#) (適用於佈建的 Redshift 叢集)
- [Redshift:GetWorkgroup](#) (適用於 Amazon Redshift Serverless 工作群組)
- [Redshift:GetCredentials](#) (適用於 Amazon Redshift Serverless 工作群組)
- [s3:ListBucket](#)
- [s3:GetBucket](#)
- [s3:GetObject](#)
- [s3:PutObject](#)
- [s3:GetBucketLifecycleConfiguration](#)

如需 GetClusterCredentials 的詳細資訊，請參閱 [GetClusterCredentials 的資源政策](#)。

您還必須確保 Amazon Redshift 可以在 COPY 和 UNLOAD 操作期間擔任 IAM 角色。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "redshift.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

如果您使用的是最新的 JDBC 驅動程式，該驅動程式會自動管理從 Amazon Redshift 自我簽署憑證到 ACM 憑證的轉換。但是，您必須[指定 JDBC url 的 SSL 選項](#)。

以下是如何指定 JDBC 驅動程式 URL 和 `aws_iam_role` 以連線到 Amazon Redshift 的範例。

```
df.write \
  .format("io.github.spark_redshift_community.spark.redshift ") \
  .option("url", "jdbc:redshift:iam://<the-rest-of-the-connection-string>") \
  .option("dbtable", "<your-table-name>") \
  .option("tempdir", "s3a://<your-bucket>/<your-directory-path>") \
  .option("aws_iam_role", "<your-aws-role-arn>") \
```

```
.mode("error") \  
.save()
```

Amazon S3 和 Spark 之間的身分驗證

如果您使用 IAM 角色在 Spark 和 Amazon S3 之間進行驗證，請使用下列其中一種方法：

- 適用於 Java 的 AWS SDK 會自動嘗試使用 DefaultAWSCredentialsProviderChain 類別所實作的預設憑證提供者鏈結來尋找 AWS 憑證。如需詳細資訊，請參閱[使用預設憑證提供者鏈結](#)。
- 您可以透過 [Hadoop 組態屬性](#)來指定 AWS 金鑰。例如，如果您的 tempdir 組態指向 s3n:// 檔案系統，請在 Hadoop XML 組態檔案中設定 fs.s3n.awsAccessKeyId 和 fs.s3n.awsSecretAccessKey 屬性，或呼叫 sc.hadoopConfiguration.set() 以變更 Spark 的全域 Hadoop 組態。

例如，假設您使用 s3n 檔案系統，請新增：

```
sc.hadoopConfiguration.set("fs.s3n.awsAccessKeyId", "YOUR_KEY_ID")  
sc.hadoopConfiguration.set("fs.s3n.awsSecretAccessKey", "YOUR_SECRET_ACCESS_KEY")
```

若為 s3a 檔案系統，請新增：

```
sc.hadoopConfiguration.set("fs.s3a.access.key", "YOUR_KEY_ID")  
sc.hadoopConfiguration.set("fs.s3a.secret.key", "YOUR_SECRET_ACCESS_KEY")
```

如果您使用 Python，請使用下列操作：

```
sc._jsc.hadoopConfiguration().set("fs.s3n.awsAccessKeyId", "YOUR_KEY_ID")  
sc._jsc.hadoopConfiguration().set("fs.s3n.awsSecretAccessKey",  
"YOUR_SECRET_ACCESS_KEY")
```

- 在 tempdir URL 中編碼身分驗證金鑰。例如，URI s3n://ACCESSKEY:SECRETKEY@bucket/path/to/temp/dir 會編碼金鑰對 (ACCESSKEY,SECRETKEY)。

Redshift 和 Amazon S3 之間的身分驗證

如果您在查詢中使用 COPY 和 UNLOAD 命令，則也必須向 Amazon S3 授予 Amazon Redshift 的存取權，以代表您執行查詢。若要這麼做，請先[授權 Amazon Redshift 存取其他 AWS 服務](#)，然後授權[使用 IAM 角色進行 COPY 和 UNLOAD 操作](#)。

我們建議的最佳實務是，將許可政策附加到 IAM 角色，然後根據需要將其指派給使用者和群組。如需詳細資訊，請參閱 [Amazon Redshift 中的身分和存取管理](#)。

與 AWS Secrets Manager 的整合

您可以從 AWS Secrets Manager 中儲存的機密擷取 Redshift 的使用者名稱和密碼憑證。若要自動提供 Redshift 憑證，請使用 `secret.id` 參數。如需有關如何建立 Redshift 憑證機密的詳細資訊，請參閱 [建立 AWS Secrets Manager 資料庫機密](#)。

GroupID	ArtifactID	支援的修訂	描述
com.amazonaws.secretsmanager	aws-secretsmanager-jdbc	1.0.12	適用於 Java 的 AWS Secrets Manager SQL 連線庫可讓 Java 開發人員使用 AWS Secrets Manager 中儲存的機密輕鬆連線到 SQL 資料庫。

Note

確認：本文件包含由 [Apache Software Foundation](#) 根據 [Apache 2.0 授權](#) 所開發的範例程式碼和語言。

透過下推功能改善效能

Spark 連接器會自動套用述詞和查詢下推功能，以針對效能進行最佳化。這項支援表示，如果您在查詢中使用受支援的函數，Spark 連接器便會將該函數轉換為 SQL 查詢，並在 Amazon Redshift 中執行該查詢。此最佳化可減少所擷取的資料，因此 Apache Spark 可以處理較少的資料，獲得較好的效能。依預設，系統會自動啟動下推功能。若要加以停用，請將 `autopushdown` 設定為 `false`。

```
import sqlContext.implicits._val
sample= sqlContext.read
  .format("io.github.spark_redshift_community.spark.redshift")
  .option("url",jdbcURL )
  .option("tempdir", tempS3Dir)
  .option("dbtable", "event")
```

```
.option("autopushdown", "false")  
.load()
```

下推功能支援下列函數。如果您使用的函數不在此清單中，Spark 連接器會在 Spark 中執行此函數，而不是在 Amazon Redshift 中執行，因此無法獲得最佳效能。如需 Spark 中函數的完整清單，請參閱[內建函數](#)。

- 彙總函數
 - avg
 - count
 - max
 - 分鐘
 - sum
 - stddev_samp
 - stddev_pop
 - var_samp
 - var_pop
- 布林值運算子
 - in
 - isnull
 - isnotnull
 - contains
 - endswith
 - startswith
- 邏輯運算子
 - 以及
 - 或
 - not (or !)
- 數學函式
 - +
 - -
 - *

- /
- - (unary)
- abs
- acos
- asin
- atan
- ceil
- cos
- exp
- floor
- greatest
- least
- log10
- pi
- pow
- round
- sin
- sqrt
- tan
- 其他函數
 - cast
 - coalesce
 - decimal
 - 如
 - in
- 關係運算子
 - !=
 - =
 - >
 - >=

- <
- <=
- 字串函數
 - ascii
 - lpad
 - rpad
 - translate
 - upper
 - lower
 - length
 - trim
 - ltrim
 - rtrim
 - like
 - substring
 - concat
- 日期和時間函數
 - add_months
 - date
 - date_add
 - date_sub
 - date_trunc
 - timestamp
 - trunc
- 數學運算
 - CheckOverflow
 - PromotePrecision
- 關係運算
 - Aliases (例如 AS)
 - CaseWhen

- Distinct
- InSet
- Joins 和 cross joins
- 限制
- Unions, union all
- ScalarSubquery
- Sorts (遞增和遞減)
- UnscaledValue

其他組態選項

變更字串資料欄的大小上限

在建立儲存為 VARCHAR(256) 的資料表時，Redshift 會將字串資料欄建立為文字資料欄。如果你想要支援更大尺寸的資料欄，則可以使用 maxlength 來指定字串資料欄的最大長度。以下範例說明如何指定 maxlength。

```
columnLengthMap.foreach { case (colName, length) =>
  val metadata = new MetadataBuilder().putLong("maxlength", length).build()
  df = df.withColumn(colName, df(colName).as(colName, metadata))
}
```

設定資料欄類型

若要設定資料欄類型，請使用 redshift_type 欄位。

```
columnTypeMap.foreach { case (colName, colType) =>
  val metadata = new MetadataBuilder().putString("redshift_type", colType).build()
  df = df.withColumn(colName, df(colName).as(colName, metadata))
}
```

在資料欄上設定壓縮編碼

若要在資料欄上使用特定的壓縮編碼，請使用編碼欄位。如需支援壓縮編碼的完整清單，請參閱[壓縮編碼](#)。

設定資料欄的描述

若要設定描述，請使用 description 欄位。

Redshift 和 Amazon S3 之間的身分驗證

根據預設，結果會以 parquet 格式卸載到 Amazon S3。若要將結果卸載為以豎線分隔的文字檔案，請指定下列選項。

```
.option("unload_s3_format", "TEXT")
```

延遲執行下推陳述式

參數	必要	預設	描述
spark.datasource.redshiftcommunity.autopushdown.lazyMode	否	True	<p>指定連接器是否應延遲執行下推陳述式 Redshift。</p> <p>如果為 true，則 Spark 連接器會在執行查詢之前先擷取所有相關模型和資訊，這通常會產生較佳的效能。</p> <p>如果為 false，則 Spark 連接器會立即在主 Spark 驅動程式執行緒中執行下推陳述式，並跨運算式序列化。</p>

連接器參數

Spark SQL 中的參數映射或 OPTIONS 支援以下設定。

參數	必要	預設	描述
dbtable	是，除非指定查詢	N/A	要在 Redshift 中建立或讀取的資料表。將

參數	必要	預設	描述
			資料儲存回 Redshift 時，需要此參數。
query	是，除非指定 dbtable	N/A	要在 Redshift 中讀取的查詢。
使用者	否	N/A	Redshift 的使用者名稱。必須與密碼參數搭配使用。只有在使用者和密碼不是 URL 中的參數時才有效。同時使用兩者會導致錯誤。
密碼	否	N/A	Redshift 的密碼。必須與使用者參數搭配使用。只有在使用者和密碼不是 URL 中的參數時才有效。同時使用兩者會導致錯誤。

參數	必要	預設	描述
url	否	N/A	<p>JDBC URL。格式為 <code>jdbc:subprotocol://host:port/database?user=username&password=password</code>。</p> <p>視您已載入的 JDBC 驅動程序而定，子通訊協定可以是 <code>postgresql</code> 或 <code>Redshift</code>。請注意，一個與 Redshift 相容的驅動程式必須位於類別路徑中，並符合此 URL。</p> <p>主機和連接埠應指向 Redshift 主節點，因此您必須將安全群組和/或 VPC 設定為允許從驅動程式應用程式存取。</p> <p>資料庫是 Redshift 的資料庫名稱。</p> <p>使用者和密碼是用來存取資料庫的憑證，必須內嵌在 JDBC 的這個 URL 中，而且資料庫使用者必須具備用來存取資料表的必要許可。</p>

參數	必要	預設	描述
aws_iam_role	只有在使用 IAM 角色來授權 Redshift COPY/UNLOAD 操作時	N/A	附加至 Redshift 叢集之 IAM 角色的完整指定 ARN。
forward_spark_s3_credentials	否	False	指出此程式庫是否應自動探索 Spark 用來連線到 Amazon S3 的憑證，以及是否透過 JDBC 驅動程式將這些憑證轉送至 Redshift。這些憑證會在 JDBC 查詢中傳送。因此，建議您在使用此選項時，為 JDBC 連線啟用 SSL 加密。
temporary_aws_access_key_id	否	N/A	AWS 存取金鑰。必須具有 S3 儲存貯體的寫入許可。
temporary_aws_secret_access_key	否	N/A	對應至存取金鑰的 AWS 私密存取金鑰。
temporary_aws_session_token	否	N/A	對應至所提供存取金鑰的 AWS 工作階段權杖。

參數	必要	預設	描述
tempdir	否	N/A	Amazon S3 中的可寫入位置。用於在讀取時卸載資料，並在寫入時將 Avro 資料載入到 Redshift。如果您在一般 ETL 管道中使用適用於 Spark 的 Redshift 資料來源，則在儲存貯體上設定 生命週期政策 並將其作為此資料的暫存位置會很有用。
jdbcdriver	否	由 JDBC URL 的子通訊協定決定	要使用之 JDBC 驅動程式的類別名稱。這個類別必須在類別路徑上。在大多數情況下，應該不需要指定此選項，因為 JDBC URL 的子通訊協定應該會自動決定適當的驅動程式類別名稱。
diststyle	否	Even	在建立資料表時要使用的 Redshift 分散樣式 。有效選項為 EVEN、KEY 或 ALL。使用 KEY 時，也必須使用 distkey 選項設定分散索引鍵。
distkey	否，除非使用 DISTSTYLE_KEY	N/A	要在建立資料表時作為分散索引鍵的資料表資料欄名稱。

參數	必要	預設	描述
sortkeyspec	否	N/A	完整的 Redshift 排序索引鍵 定義。
include_column_list	否	False	指出此程式庫是否應根據 資料欄映射選項 ，自動從結構描述擷取資料欄，並將其新增至 COPY 命令。
description	否	N/A	資料表的描述。 描述可使用 SQL COMMENT 命令加以設定，並且會出現在大多數查詢工具中。 請參閱 <code>description</code> 中繼資料以設定個別資料欄的描述。

參數	必要	預設	描述
preactions	否	N/A	要在載入 COPY 命令前執行的分號分隔 SQL 命令清單。在載入新資料前先執行 DELETE 命令或類似命令可能會很有用。如果命令中包含 %s，則系統會在執行期之前先將資料表名稱格式化 (如果您使用的是暫存資料表)。如果此命令失敗，則系統會將其視為例外狀況。如果您使用的是暫存資料表，且預先處理失敗，則系統會回復變更並還原備份資料表。
extracopyoptions	否	N/A	<p>載入資料時要附加至 Redshift COPY 命令的額外選項清單 (例如 TRUNCATECOLUMNS 或 MAXERROR n)。</p> <p>如需可用參數的完整清單，請參閱選用參數。</p> <p>請注意，由於這些選項會附加到 COPY 命令的結尾，因此您只能使用在命令結尾上具有意義的選項。這應該涵蓋大多數可能的使用案例。</p>

參數	必要	預設	描述
sse_kms_key	否	N/A	要在 Redshift UNLOAD 操作期間用於 S3 中伺服器端加密的 AWS KMS 金鑰 ID (而非 AWS 預設加密)。Redshift IAM 角色必須具有 KMS 金鑰的存取權才能使用該金鑰來進行寫入，而 Spark IAM 角色必須具有該金鑰的存取權才能進行讀取操作。只要 Spark 的 IAM 角色具有適當存取權，讀取加密資料就不需要變更 (AWS 會負責處理)。
tempformat	否	AVRO	在寫入到 Redshift 時，用來在 Amazon S3 中儲存暫存檔案的格式。有效值為 AVRO、CSV 和 CSV GZIP (壓縮 CSV)。
csvnullstring (實驗性)	否	Null	使用 CSV tempformat 時為 Null 值寫入的字串值。這應該是不會出現在實際資料中的值。

參數	必要	預設	描述
autopushdown	否	True	指出是否要透過擷取和分析 SQL 操作的 Spark 邏輯計畫，以套用述詞和查詢下推。這些操作會轉換成 SQL 查詢，然後在 Redshift 中執行以提高效能。
autopushdown.s3_result_cache	否	False	快取查詢 SQL 以在記憶體中卸載 Amazon S3 路徑映射資料，因此不需要在相同的 Spark 工作階段中再次執行相同的查詢。只有在開啟 autopushdown 時才支援。在混合讀取和寫入操作時，不建議使用這個參數，因為快取的結果可能包含過時的資訊。
unload_s3_format	否	Parquet	用來卸載查詢結果的格式。有效選項為 Parquet 和文字，其會指定以豎線分隔的文字格式卸載查詢結果。

參數	必要	預設	描述
extraunloadoptions	否	N/A	要附加至 Redshift UNLOAD 命令的額外選項。並非所有選項都能保證運作，因為某些選項可能會與連接器內設定的其他選項衝突。
copydelay	否	30000	Redshift COPY 操作重試之間的延遲時間 (以毫秒為單位)。
copyretrycount	否	2	要重試 Redshift COPY 操作的次數。

參數	必要	預設	描述
tempdir_region	否	N/A	<p>tempdir 所在的 AWS 區域。設定此選項可改善連接器與 tempdir 互動時的效能，並且會在連接器的讀取和寫入操作期間，自動於 COPY 和 UNLOAD 操作中提供此值。</p> <p>建議在以下情況使用此設定：</p> <ol style="list-style-type: none">1) 當連接器在 AWS 外部執行時，因為自動探索區域的功能會失敗，並對連接器的效能造成負面影響。2) 當 tempdir 位於與 Redshift 叢集不同的區域時，因為使用此設定就比較不需要使用 extracopy options 和 extraunload options 參數手動提供區域。使用 PARQUET 做為 tempformat 時，即使使用此參數，tempdir 也不能位於與 Redshift 叢集不同的區域。

參數	必要	預設	描述
			3) 當連接器在與 tempdir 不同的區域中執行時，因為其會改善連接器對於 tempdir 的存取效能。
secret.id	否	N/A	儲存在 AWS Secrets Manager 之機密的名稱或 ARN。您可以使用此參數自動提供 Redshift 憑證，但前提是使用者、密碼和 DbUser 憑證未傳遞到 JDBC URL 或做為其他選項來傳遞。

參數	必要	預設	描述
secret.region	否	N/A	<p>要搜尋 secret.id 值的主要 AWS 區域，例如美國東部 (維吉尼亞北部)。</p> <p>如果未指定此區域，連接器會嘗試使用 預設憑證提供者鏈結 來解析 secret.id 的區域。在某些情況下，例如您使用外部的連接器的話，連接器便找不到該區域。建議在以下情況使用此設定：</p> <p>1) 當連接器在 AWS 外部執行時，因為自動探索區域的功能會失敗，而無法向 Redshift 進行身分驗證。</p> <p>當連接器在與 secret.id 不同的區域中執行時，因為其會改善連接器對於機密的存取效能。</p>
secret.vpcEndpointUrl	否	N/A	<p>在覆寫 預設憑證提供者鏈結 時，AWS Secrets Manager 的 PrivateLink DNS 端點 URL。</p>

參數	必要	預設	描述
secret.vpcEndpoint Region	否	N/A	在覆寫 預設憑證提供者鏈結 時，AWS Secrets Manager 的 PrivateLink DNS 端點區域。
jdbc.*	否	N/A	要傳遞給基礎 JDBC 驅動程式的其他參數，其中萬用字元是 JDBC 參數的名稱，例如 jdbc.ssl。請注意，在傳遞給 JDBC 驅動程序之前，會先刪除 jdbc 字首。若要查看 Redshift JDBC 驅動程式的所有可能選項，請參閱 JDBC 驅動程式 2.1 版組態的選項 。

參數	必要	預設	描述
label	否	" "	<p>使用連接器執行查詢時，要包含在查詢群組集內的識別符。必須在 100 個字元以下，且所有字元都必須是有效的 unicodeIdentifierParts。如果您的識別符有超過 100 個字元，系統會移除超過的部分。使用連接器執行查詢時，查詢群組會設定為 JSON 格式字串，例如</p> <pre> {"spark-redshift-connector": {"svc": "", "ver": "5.1.0-amzn-1-spark_3.3", "op": "Read", "lbl": ""}}` </pre> <p>。此選項會取代 lbl 索引鍵的值。</p>

Note

確認：本文件包含由 [Apache Software Foundation](#) 根據 [Apache 2.0 授權](#) 所開發的範例程式碼和語言。

支援的資料類型

Spark 連接器支援 Amazon Redshift 中的下列資料類型。如需 Amazon Redshift 中支援的資料類型完整清單，請參閱[資料類型](#)。如果資料類型不在下表中，則表示 Spark 連接器不支援該資料類型。

資料類型	別名
SMALLINT	INT2
INTEGER	INT、INT4
BIGINT	INT8
DECIMAL	NUMERIC
REAL	FLOAT4
DOUBLE PRECISION	FLOAT8、FLOAT
BOOLEAN	BOOL
CHAR	CHARACTER、NCHAR、BPCHAR
VARCHAR	CHARACTER VARYING、NVARCHAR、TEXT
DATE	
TIMESTAMP	不含時區的時間戳記
TIMESTAMPTZ	含時區的時間戳記
SUPER	
TIME	不含時區的時間
TIMETZ	含時區的時間
VARBYTE	VARBINARY、BINARY VARYING

複雜資料類型

您可以使用 Spark 連接器在 Redshift SUPER 資料類型資料欄中讀取和寫入 Spark 複雜資料類型 (例如 `ArrayType`、`MapType` 和 `StructType`)。如果您在讀取操作期間提供結構描述，資料欄中的資料會轉換為其在 Spark 中對應的複雜類型，包括任何巢狀類型。此外，如果已啟用 `autopushdown`，則巢狀屬性、映射值和陣列索引的投影會向下推送至 Redshift，在只存取一部分資料時，就不再需要卸載整個巢狀資料結構。

當您從連接器寫入 DataFrames 時，任何類型為 `MapType` (使用 `StringType`)、`StructType`、或 `ArrayType` 的資料欄都會寫入到 Redshift SUPER 資料類型資料欄。在撰寫這些巢狀資料結構時，`tempformat` 參數的類型必須是 CSV、CSV GZIP 或 PARQUET。使用 AVRO 會導致例外狀況。撰寫具有 `StringType` 以外索引鍵類型的 `MapType` 資料結構也會導致例外狀況。

StructType

下列範例會示範如何建立具有 SUPER 資料類型且包含以下結構的資料表

```
create table contains_super (a super);
```

然後，您可以使用連接器，在使用如下列範例中的結構描述的資料表中，從 SUPER 資料欄 `a` 查詢 `StringType` 欄位 `hello`。

```
import org.apache.spark.sql.types._

val sc = // existing SparkContext
val sqlContext = new SQLContext(sc)

val schema = StructType(StructField("a", StructType(StructField("hello",
  StringType) :: Nil)) :: Nil)

val helloDF = sqlContext.read
  .format("io.github.spark_redshift_community.spark.redshift")
  .option("url", jdbcURL )
  .option("tempdir", tempS3Dir)
  .option("dbtable", "contains_super")
  .schema(schema)
  .load().selectExpr("a.hello")
```

下列範例會示範如何將結構寫入到資料欄 `a`。

```
import org.apache.spark.sql.types._
```



```
import org.apache.spark.sql._

val sc = // existing SparkContext
val sqlContext = new SQLContext(sc)

val schema = StructType(StructField("a", StructType(StructField("hello",
  StringType) :: Nil)) :: Nil)
val data = sc.parallelize(Seq(Row(Row("world"))))
val mydf = sqlContext.createDataFrame(data, schema)

mydf.write.format("io.github.spark_redshift_community.spark.redshift").
  option("url", jdbcUrl).
  option("dbtable", tableName).
  option("tempdir", tempS3Dir).
  option("tempformat", "CSV").
  mode(SaveMode.Append).save
```

MapType

如果您偏好使用 MapType 來表示資料，則可以在結構描述中使用 MapType 資料結構，並擷取映射中與索引鍵對應的值。請注意，MapType 資料結構中的所有索引鍵都必須是字串類型，並且所有值都必須是相同類型，例如 int。

下列範例會示範如何取得資料欄 a 中索引鍵 hello 的值。

```
import org.apache.spark.sql.types._

val sc = // existing SparkContext
val sqlContext = new SQLContext(sc)

val schema = StructType(StructField("a", MapType(StringType, IntegerType))::Nil)

val helloDF = sqlContext.read
  .format("io.github.spark_redshift_community.spark.redshift")
  .option("url", jdbcURL )
  .option("tempdir", tempS3Dir)
  .option("dbtable", "contains_super")
  .schema(schema)
  .load().selectExpr("a['hello']")
```

ArrayType

如果資料欄包含陣列而不是結構，您可以使用連接器來查詢陣列中的第一個元素。

```
import org.apache.spark.sql.types._

val sc = // existing SparkContext
val sqlContext = new SQLContext(sc)

val schema = StructType(StructField("a", ArrayType(IntegerType)):: Nil)

val helloDF = sqlContext.read
  .format("io.github.spark_redshift_community.spark.redshift")
  .option("url", jdbcURL )
  .option("tempdir", tempS3Dir)
  .option("dbtable", "contains_super")
  .schema(schema)
  .load().selectExpr("a[0]")
```

限制

搭配 Spark 連接器使用複雜資料類型時有下列限制：

- 所有巢狀的結構欄位名稱和映射索引鍵都必須小寫。如果要查詢包含大寫字母的複雜欄位名稱，因應措施是您可以嘗試省略結構描述，並使用 `from_json` Spark 函數在本機轉換傳回的字串。
- 讀取或寫入操作中使用的任何映射欄位都必須只有 `StringType` 索引鍵。
- 只有 CSV、CSV GZIP 和 PARQUET 才是支援將複雜類型寫入到 Redshift 的 `tempformat` 值。嘗試使用 AVRO 會擲回例外狀況。

設定 Amazon Redshift ODBC 驅動程式 2.x 版連線

您可以從許多第三方 SQL 用戶端工具和應用程式使用 ODBC 連線來連線至 Amazon Redshift 叢集。如果用戶端工具支援 JDBC，您可以選擇使用這種連線，而非 ODBC，因為 JDBC 的設定簡單。不過，如果您的用戶端工具不支援 JDBC，您可以按照本節中的步驟，在用戶端電腦或 Amazon EC2 執行個體上設定 ODBC 連線。

Amazon Redshift 會提供適用於 Linux 和 Windows 作業系統的 64 位元 ODBC 驅動程式；32 位元 ODBC 驅動程式已停用。目前不支援 macOS X。除了緊急的安全修補程式外，不會再針對 32 位元 ODBC 驅動程式發佈其他更新。若要下載並安裝適用於 macOS X 和 32 位元作業系統的 ODBC 驅動程式，請參閱[設定 ODBC 連線](#)。

如需 ODBC 驅動程式變更的最新資訊，請參閱[變更日誌](#)。

主題

- [取得 ODBC URL](#)
- [在 Microsoft Windows 上安裝並設定 Amazon Redshift ODBC 驅動程式](#)
- [在 Linux 上安裝並設定 Amazon Redshift ODBC 驅動程式](#)
- [設定身分驗證](#)
- [轉換資料類型](#)
- [設定 ODBC 驅動程式選項](#)
- [先前的 ODBC 驅動程式版本](#)

取得 ODBC URL

Amazon Redshift 會在 Amazon Redshift 主控台中顯示叢集的 ODBC URL。此 URL 包含要在用戶端電腦和資料庫之間設定連線所需的資訊。

ODBC URL 採用下列格式：

```
Driver={driver}; Server=endpoint_host; Database=database_name; UID=user_name;  
PWD=password; Port=port_number
```

前面格式的欄位具有下列值：

ODBC URL 欄位值

欄位	Value
<i>Driver</i>	要使用的 64 位元 ODBC 驅動程式的名稱：Amazon Redshift ODBC 驅動程式 (x64)。
<i>Server</i>	Amazon Redshift 叢集的端點主機。
<i>Database</i>	您為叢集建立的資料庫。
<i>UID</i>	有許可而可連線至資料庫之資料庫使用者帳戶的使用者名稱。雖然這個值是資料庫層級的許可而非叢集層級的許可，但您可以使用您在啟動叢集時所設定的 Redshift 管理員使用者帳戶。
<i>PWD</i>	用來連線至資料庫之資料庫使用者帳戶的密碼。

欄位	Value
<i>Port</i>	您啟動叢集時指定的連接埠號碼。如果有防火牆，請確定此連接埠已開放給您使用。

以下是 ODBC URL 範例：

```
Driver={Amazon Redshift ODBC Driver (x64)}; Server=examplecluster.abc123xyz789.us-west-2.redshift.amazonaws.com; Database=dev; UID=adminuser; PWD=insert_your_admin_user_password_here; Port=5439
```

如需有關可在何處找到 ODBC URL 的資訊，請參閱[尋找叢集連線字串](#)。

在 Microsoft Windows 上安裝並設定 Amazon Redshift ODBC 驅動程式

系統要求

您必須在存取 Amazon Redshift 資料倉儲的用戶端電腦上安裝 Amazon Redshift ODBC 驅動程式。針對安裝驅動程式的每一台電腦，有下列最低要求：

- 機器上的管理員權限。
- 機器符合下列系統要求：
 - 下列其中一個操作系統：
 - Windows 10 或 8.1。
 - Windows Server 2019、2016 或 2012。
 - 100 MB 的可用磁碟空間。
 - 已安裝 Visual C++ Redistributable for Visual Studio 2015，適用於 64 位元。您可以在 Microsoft 網站上的[下載適用於 Visual Studio 2022 的 Visual C++ 可轉散發套件](#)下載安裝套件。


安裝 Amazon Redshift ODBC 驅動程式

使用下列程序來下載並安裝適用於 Windows 作業系統的 Amazon Redshift ODBC 驅動程式。僅在您執行的第三方應用程式經認證可與 Amazon Redshift 搭配使用，且該應用程式需要特定驅動程式時，才使用不同的驅動程式。

若要下載並安裝 ODBC 驅動程式：

1. 下載以下驅動程序：[64 位 ODBC 驅動程序 2.1.2.0 版本](#) BC 驅動程序版本 2.1.2.0

此驅動程式的名稱是 Amazon Redshift ODBC 驅動程式 (x64)。

 Note


32 位元的 ODBC 驅動程式已停用。除了緊急的安全修補程式外，不會再發佈其他更新。若要下載並安裝適用於 32 位元作業系統的 ODBC 驅動程式，請參閱[在 Microsoft Windows 上安裝和設定 Amazon Redshift ODBC 驅動程式](#)。

2. 檢閱 [Amazon Redshift ODBC 驅動程式 2.x 版授權](#)。
3. 按兩下 .msi 檔案，然後遵循精靈中的步驟來安裝驅動程式。

建立 ODBC 連線的系統 DSN 項目

在下載並安裝 ODBC 驅動程式之後，請將資料來源名稱 (DSN) 項目新增至用戶端電腦或 Amazon EC2 執行個體。SQL 用戶端工具可以使用此資料來源以連線至 Amazon Redshift 資料庫。

建議您建立系統 DSN，而不是使用者 DSN。部分應用程式會使用不同資料庫使用者帳戶載入資料，而且可能無法偵測到在其他資料庫使用者帳戶下建立的使用者 DSN。

 Note

對於使用 AWS Identity and Access Management (IAM) 登入資料或身分提供者 (IdP) 登入資料的身分驗證，則需要執行其他步驟。如需詳細資訊，請參閱[設定 JDBC 或 ODBC 連線以使用 IAM 憑證](#)。

若要建立 ODBC 連線的系統 DSN 項目：

1. 在開始功能表中，輸入「ODBC 資料來源」。選擇 ODBC 資料來源。

確定您選擇的 ODBC 資料來源管理員具有與您要用來連線到 Amazon Redshift 的用戶端應用程式相同的位元。

2. 在 ODBC 資料來源管理員中，選擇驅動程式索引標籤並尋找下列驅動程式資料夾：Amazon Redshift ODBC 驅動程式 (x64)。
3. 選擇系統 DSN 索引標籤，為電腦上的所有使用者設定驅動程式，或選擇使用者 DSN 索引標籤，只為您的資料庫使用者帳戶設定驅動程式。

4. 選擇新增。Create New Data Source (建立新的資料來源) 視窗會開啟。
5. 選擇 Amazon Redshift ODBC 驅動程式 (x64)，然後選擇完成。Amazon Redshift ODBC 驅動程式 DSN 設定視窗會開啟。
6. 在連線設定區段下，輸入下列資訊：

- Data Source Name (資料來源名稱)

輸入資料來源的名稱。例如，如果您遵循了《Amazon Redshift 入門指南》，則可能會輸入 `exampleclusterdsn`，以便輕鬆記住與此 DSN 建立關聯的叢集。

- Server

指定 Amazon Redshift 叢集的端點主機。您可以在 Amazon Redshift 主控台的叢集詳細資訊頁面上找到此資訊。如需詳細資訊，請參閱 [在 Amazon Redshift 中設定連線](#)。

- 連線埠

輸入資料庫使用的連接埠號碼。根據您在建立、修改或遷移叢集時所選取的連接埠而定，允許存取選取的連接埠。

- 資料庫

輸入 Amazon Redshift 資料庫的名稱。如果您在未指定資料庫名稱的情況下啟動了叢集，請輸入 `dev`。否則，請使用您在啟動過程選擇的名稱。如果您遵循了《Amazon Redshift 入門指南》，請輸入 `dev`。

7. 在身分驗證區段下，指定要設定標準或 IAM 身分驗證的組態選項。

8. 選擇 SSL 選項，並指定下列項目的值：

- 身分驗證方式

選擇用於處理 Secure Sockets Layer (SSL) 的模式。在測試環境中，您可以使用 `prefer`。不過，若為生產環境且需要交換安全資料時，請使用 `verify-ca` 或 `verify-full`。

- 最小 TLS

選擇性地選擇驅動程式允許資料存放區用於加密連線的 TLS/SSL 最低版本。例如，如果您指定 TLS 1.2，則無法使用 TLS 1.1 來加密連線。預設版本為 TLS 1.2。

9. 在代理索引標籤中，指定任何代理連線設定。

10. 在游標索引標籤中，指定有關如何將查詢結果傳回給 SQL 用戶端工具或應用程式的選項。

11. 在進階選項中，指定 `logLevel`、`logPathcompression`、和其他選項的值。

12 選擇 測試。如果用戶端電腦可以連線至 Amazon Redshift 資料庫，則會出現下列訊息：連線成功。如果用戶端電腦無法連線至資料庫，您可以透過產生記錄檔並連絡 AWS 支援人員來疑難排解可能的問題。如需有關產生日誌的資訊，請參閱 (LINK)。

13 選擇確定。

在 Linux 上安裝並設定 Amazon Redshift ODBC 驅動程式

系統要求

您必須在存取 Amazon Redshift 資料倉儲的用戶端電腦上安裝 Amazon Redshift ODBC 驅動程式。針對安裝驅動程式的每一台電腦，有下列最低要求：

- 機器上的根存取。
- 下列其中一個發行版本：
 - RHEL® 企業版 (RHEL) 8 或更新版本
 - CentOS 8 或以上版本。
- 150 MB 的可用磁碟空間
- unixODBC 2.2.14 或更新版本。
- glibc 2.26 或更新版本。

安裝 Amazon Redshift ODBC 驅動程式

若要下載並安裝適用於 Linux 的 Amazon Redshift ODBC 驅動程式 2.x 版：

1. 下載以下驅動程序：[64 位 RPM 驅動程序 2.1.2.0 版本](#) 驅動程序版本 2.1.2.0

Note

32 位元的 ODBC 驅動程式已停用。除了緊急的安全修補程式外，不會再發佈其他更新。

2. 移至您下載套件的位置，然後執行下列其中一個命令。使用與您的 Linux 發行版本相應的指令。

在 RHEL 和 CentOS 作業系統上，執行下列命令：

```
yum --nogpgcheck localinstall RPMFileName
```

將 *RPMFileName* 取代為 RPM 套件檔案名稱。例如，下列命令示範安裝 64 位元驅動程式：

```
yum --nogpgcheck localinstall AmazonRedshiftODBC-64-bit-2.x.xx.xxxx.x86_64.rpm
```

使用 ODBC 驅動程式管理員在 Linux 上設定 ODBC 驅動程式

在 Linux 上，您使用的是 ODBC 驅動程式管理員來設定 ODBC 連線設定。ODBC 驅動程式管理員使用組態檔案來定義及設定 ODBC 資料來源和驅動程式。您使用的 ODBC 驅動程式管理員視您使用的作業系統而定。

使用 unixODBC 驅動程式管理員來設定 ODBC 驅動程式

需要下列檔案才能設定 Amazon Redshift ODBC 驅動程式：

- amazon.redshiftdbc.ini
- odbc.ini
- odbcinst.ini

如果是安裝到預設位置，則 amazon.redshiftdbc.ini 組態檔案位於 /opt/amazon/redshiftdbcx64。

此外，在 /opt/amazon/redshiftdbcx64 下，您可以找到 odbc.ini 和 odbcinst.ini 範例檔案。您可以使用這些檔案做為設定 Amazon Redshift ODBC 驅動程式和資料來源名稱 (DSN) 的範例。

不建議使用 Amazon Redshift ODBC 驅動程式安裝目錄來存放組態檔案。所安裝目錄中的範例檔案僅供當作範例。如果您後來重新安裝 Amazon Redshift ODBC 驅動程式，或升級為更新版本，安裝目錄會遭到覆寫。您會遺失對安裝目錄中的檔案所做的任何變更。

若要避免這種情況，請將 amazon.redshiftdbc.ini 檔案複製到安裝目錄以外的目錄。如果您將此檔案複製到使用者的主目錄，請在檔案名稱開頭加上一點 (.)，將它變成隱藏檔。

對於 odbc.ini 和 odbcinst.ini 檔案，請使用位於使用者主目錄中的組態檔案，或在另一個目錄中建立新版本。根據預設，您的 Linux 作業系統應該在使用者的主目錄 (/home/\$USER 或 ~/.) 中具有 odbc.ini 檔案和 odbcinst.ini 檔案。這些預設檔案是隱藏檔，每個檔案名稱前面以點表示。僅當使用 -a 旗標來列出目錄內容時，才會顯示這些檔案。

無論對 odbc.ini 和 odbcinst.ini 檔案選擇何種選項，都會修改這些檔案來新增驅動程式和 DSN 組態資訊。如果建立新檔案，則還需要設定環境變數來指定這些組態檔案所在的位置。

根據預設，ODBC 驅動程式管理員會設定為使用隱藏版本的 `odbc.ini` 和 `odbcinst.ini` 組態檔 (命名為 `.odbc.ini` 和 `.odbcinst.ini`)，這些組態檔位於主目錄中。它們也會設定為使用驅動程式安裝目錄中的 `amazon.redshiftoDBC.ini` 檔案。如果您將這些組態檔儲存在其他位置，請設定如下所述的環境變數，以便驅動程式管理員可以找到這些檔案。

如果您使用 `unixODBC`，請執行以下操作：

- 將 `ODBCINI` 設定為 `odbc.ini` 檔案的完整路徑和檔案名稱。
- 將 `ODBCSYSINI` 設定為包含 `odbcinst.ini` 檔案之目錄的完整路徑。
- 將 `AMAZONREDSHIFTODBCINI` 設定為 `amazon.redshiftoDBC.ini` 檔案的完整路徑和檔案名稱。

以下是設定上述值的範例：

```
export ODBCINI=/usr/local/odbc/odbc.ini
export ODBCSYSINI=/usr/local/odbc
export AMAZONREDSHIFTODBCINI=/etc/amazon.redshiftoDBC.ini
```

在 Linux 上使用資料來源名稱 (DSN) 來設定連線

在使用資料來源名稱 (DSN) 連線至資料存放區時，請設定 `odbc.ini` 檔案來定義資料來源名稱 (DSN)。在 `odbc.ini` 檔案中設定屬性，以建立 DSN 來指定資料倉庫的連線資訊。

在 Linux 作業系統上使用下列格式：

```
[ODBC Data Sources]
driver_name=dsn_name

[dsn_name]
Driver=path/driver_file
Host=cluster_endpoint
Port=port_number
Database=database_name
locale=locale
```

以下範例示範 Linux 作業系統上使用 64 位元 ODBC 驅動程式的 `odbc.ini` 組態。

```
[ODBC Data Sources]
Amazon_Redshift_x64=Amazon Redshift ODBC Driver (x64)

[Amazon_Redshift_x64]
Driver=/opt/amazon/redshiftodbcx64/librsodbc64.so
Host=examplecluster.abc123xyz789.us-west-2.redshift.amazonaws.com
Port=5932Database=dev
locale=en-US
```

在 Linux 上設定不使用 DSN 的連線

若要透過沒有 DSN 的連線連接至您的資料存放區，請在 `odbcinst.ini` 檔案中定義驅動程式。然後，在應用程式中提供無 DSN 的連線字串。

在 Linux 作業系統上使用下列格式：

```
[ODBC Drivers]
driver_name=Installed
...

[driver_name]
Description=driver_description
Driver=path/driver_file
...


```

以下範例示範 Linux 作業系統上使用 64 位元 ODBC 驅動程式的 `odbcinst.ini` 組態。

```
[ODBC Drivers]
Amazon Redshift ODBC Driver (x64)=Installed

[Amazon Redshift ODBC Driver (x64)]
Description=Amazon Redshift ODBC Driver (64-bit)
Driver=/opt/amazon/redshiftodbcx64/librsodbc64.so
```

設定身分驗證

為了防止有人未經授權就存取資料，Amazon Redshift 資料存放區會要求所有連線使用使用者憑證進行身分驗證。

下表說明可用來連線至 Amazon Redshift ODBC 驅動程式 2.x 版之每種身分驗證方法的必要和選用連線選項：


ODBC 身分驗證方法的必要和選用連線選項

身分驗證方法	必要	選用
標準	<ul style="list-style-type: none"> 主機 連線埠 資料庫 UID 密碼 	
IAM 設定檔	<ul style="list-style-type: none"> 主機 連線埠 資料庫 IAM 設定檔 	<ul style="list-style-type: none"> ClusterID (ClusterID) 區域 AutoCreate EndpointURL StsEndpoint网址 InstanceProfile <div style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note 如果 ClusterID 和 Region 未單獨設定，則必須在 Host 中加以設定。</p> </div>
IAM 登入資料	<ul style="list-style-type: none"> 主機 連線埠 資料庫 IAM 	<ul style="list-style-type: none"> ClusterID (ClusterID) 區域 AutoCreate EndpointURL

身分驗證方法	必要	選用
	<ul style="list-style-type: none"> • AccessKey 身份證 • SecretAccess 關鍵 	<ul style="list-style-type: none"> • StsEndpoint 網址 • SessionToken • UID <div data-bbox="1068 436 1507 747" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note</p> <p>如果 ClusterID 和 Region 未單獨設定，則必須在 Host 中加以設定。</p> </div>
AD FS	<ul style="list-style-type: none"> • 主機 • 連線埠 • 資料庫 • IAM • plugin_name • UID • 密碼 • IdP_Host • IdP_Port 	<ul style="list-style-type: none"> • ClusterID (ClusterID) • 區域 • AutoCreate • EndpointUrl • StsEndpoint 網址 • Preferred_Role • 登錄 ToRp • SSL_Insecure <div data-bbox="1068 1297 1507 1608" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note</p> <p>如果 ClusterID 和 Region 未單獨設定，則必須在 Host 中加以設定。</p> </div>

身分驗證方法	必要	選用
Azure AD	<ul style="list-style-type: none"> • 主機 • 連線埠 • 資料庫 • IAM • plugin_name • UID • 密碼 • IdP_Tenant • Client_ID • Client_Secret 	<ul style="list-style-type: none"> • ClusterID (ClusterID) • 區域 • AutoCreate • EndpointUrl • StsEndpoint网址 • Preferred_Role • dbgroups_filter <div data-bbox="1068 678 1510 993" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note 如果 ClusterID 和 Region 未單獨設定，則必須在 Host 中加以設定。</p> </div>
JWT	<ul style="list-style-type: none"> • 主機 • 連線埠 • 資料庫 • IAM • plugin_name • web_identity_token 	<ul style="list-style-type: none"> • provider_name

身分驗證方法	必要	選用
Okta	<ul style="list-style-type: none"> • 主機 • 連線埠 • 資料庫 • IAM • plugin_name • UID • 密碼 • IdP_Host • App_Name • App_ID 	<ul style="list-style-type: none"> • ClusterID (ClusterID) • 區域 • AutoCreate • EndpointUrl • StsEndpoint网址 • Preferred_Role <div data-bbox="1068 621 1507 936" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note</p> <p>如果 ClusterID 和 Region 未單獨設定，則必須在 Host 中加以設定。</p> </div>
Ping Federate	<ul style="list-style-type: none"> • 主機 • 連線埠 • 資料庫 • IAM • plugin_name • UID • 密碼 • IdP_Host • IdP_Port 	<ul style="list-style-type: none"> • ClusterID (ClusterID) • 區域 • AutoCreate • EndpointUrl • StsEndpoint网址 • Preferred_Role • SSL_Insecure • partner_spid <div data-bbox="1068 1486 1507 1801" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note</p> <p>如果 ClusterID 和 Region 未單獨設定，則必須在 Host 中加以設定。</p> </div>

身分驗證方法	必要	選用
瀏覽器 Azure AD	<ul style="list-style-type: none"> • 主機 • 連線埠 • 資料庫 • IAM • plugin_name • IdP_Tenant • Client_ID • UID 	<ul style="list-style-type: none"> • ClusterID (ClusterID) • 區域 • AutoCreate • EndpointUrl • StsEndpoint网址 • Preferred_Role • dbgroups_filter • IdP_Response_Timeout • listen_port <div data-bbox="1068 793 1507 1108" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 20px;"> <p> Note</p> <p>如果 ClusterID 和 Region 未單獨設定，則必須在 Host 中加以設定。</p> </div>

身分驗證方法	必要	選用
瀏覽器 SAML	<ul style="list-style-type: none"> • 主機 • 連線埠 • 資料庫 • IAM • plugin_name • login_url • UID 	<ul style="list-style-type: none"> • ClusterID (ClusterID) • 區域 • AutoCreate • EndpointUrl • StsEndpoint网址 • Preferred_Role • dbgroups_filter • IdP_Response_Timeout • listen_port <div data-bbox="1068 793 1507 1108" style="border: 1px solid #add8e6; border-radius: 15px; padding: 10px; margin-top: 10px;"> <p> Note</p> <p>如果 ClusterID 和 Region 未單獨設定，則必須在 Host 中加以設定。</p> </div>
Auth Profile	<ul style="list-style-type: none"> • 主機 • 連線埠 • 資料庫 • AccessKey身份證 • SecretAccess關鍵 	

身分驗證方法	必要	選用
瀏覽器 Azure AD OAUTH2	<ul style="list-style-type: none"> • 主機 • 連線埠 • 資料庫 • IAM • plugin_name • IdP_Tenant • Client_ID • UID 	<ul style="list-style-type: none"> • ClusterID (ClusterID) • 區域 • EndpointUrl • IdP_Response_Timeout • listen_port • scope • provider_name <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note</p> <p>如果 ClusterID 和 Region 未單獨設定，則必須在 Host 中加以設定。</p> </div>

使用外部憑證服務

除了內建支援 AD FS、Azure AD 和 Okta 外，Windows 版本的 Amazon Redshift ODBC 驅動程式也支援其他憑證服務。驅動程式可以使用您選擇的任何 SAML 型憑證提供者外掛程式來驗證連線。

若要在 Windows 上設定外部憑證服務：

1. 建立會指定憑證提供者外掛程式和視需要指定其他身分驗證參數的 IAM 設定檔。設定檔必須採用 ASCII 編碼，且必須包含下列鍵值組，其中 PluginPath 是外掛程式應用程式的完整路徑：

```
plugin_name = PluginPath
```

例如：

```
plugin_name = C:\Users\kjson\myapp\CredServiceApp.exe
```

如需有關如何建立設定檔的資訊，請參閱《Amazon Redshift 叢集管理指南》中的[使用組態設定檔](#)。

2. 將驅動程式設定為使用此設定檔。驅動程式會偵測並使用設定檔中指定的驗證設定。

轉換資料類型

Amazon Redshift ODBC 驅動程式 2.x 版支援許多常見的資料格式，可在 Amazon Redshift 和 SQL 資料類型之間進行轉換。

下表列出支援的資料類型映射。

Amazon Redshift 類型	SQL 類型
BIGINT	SQL_BIGINT
BOOLEAN	SQL_BIT
CHAR	SQL_CHAR
DATE	SQL_TYPE_DATE
DECIMAL	SQL_NUMERIC
DOUBLE PRECISION	SQL_DOUBLE
GEOGRAPHY	SQL_LONGVARBINARY
GEOMETRY	SQL_LONGVARBINARY
INTEGER	SQL_INTEGER
REAL	SQL_REAL
SMALLINT	SQL_SMALLINT
SUPER	SQL_LONGVARCHAR
TEXT	SQL_LONGVARCHAR
TIME	SQL_TYPE_TIME
TIMETZ	SQL_TYPE_TIME

Amazon Redshift 類型	SQL 類型
TIMESTAMP	SQL_TYPE_TIMESTAMP
TIMESTAMPTZ	SQL_TYPE_TIMESTAMP
VARBYTE	SQL_LONGVARBINARY
VARCHAR	SQL_VARCHAR

設定 ODBC 驅動程式選項

您可以使用驅動程式組態選項來控制 Amazon Redshift ODBC 驅動程式的行為。驅動程式選項不區分大小寫。

在 Microsoft Windows 中，您通常於設定資料來源名稱 (DSN) 時設定驅動程式選項。您也可以在連接時以程式設計方式在連線字串中設定驅動程式選項，或在 HKEY_LOCAL_MACHINE\SOFTWARE\ODBC\ODBC.INI*your_DSN* 中新增或變更登錄機碼。如需設定 DSN 的相關資訊，請參閱 [在 Microsoft Windows 上安裝並設定 Amazon Redshift ODBC 驅動程式](#)。

在 Linux 中，您可以在 `odbc.ini` 和 `amazon.redshiftdbc.ini` 檔案中設定驅動程式組態選項，如 [使用 ODBC 驅動程式管理員來設定 Linux 和 macOS X 作業系統上的驅動程式](#) 中所述。在 `amazon.redshiftdbc.ini` 檔案中設定的組態選項會套用至所有連線。相反地，`odbc.ini` 檔案中設定的組態選項是針對某個連線。`odbc.ini` 中設定的組態選項優先於 `amazon.redshiftdbc.ini` 中設定的組態選項。

以下是您可以為 Amazon Redshift ODBC 2.x 版驅動程式指定之選項的描述。

AccessKey 身份證

- 預設值 — 無
- 資料類型 — 字串

使用者或角色的 IAM 存取金鑰。如果設定此參數，您還必須指定 `SecretAccessKey`。

此為選用參數。

app_id

- 預設值 — 無

- 資料類型 — 字串

與您的 Amazon Redshift 應用程式相關聯、Okta 所提供的唯一 ID。

此為選用參數。

app_name

- 預設值 — 無
- 資料類型 — 字串

您用來驗證與 Amazon Redshift 之連線的 Okta 應用程式名稱。

此為選用參數。

AuthProfile

- 預設值 — 無
- 資料類型 — 字串

用來管理連線設定的身分驗證設定檔。如果設定此參數，您還必須設定 AccessKeyID 和 SecretAccess 關鍵字。

此為選用參數。

AuthType

- 預設值 — 標準
- 資料類型 — 字串

此選項指定當您使用 [Amazon Redshift ODBC 驅動程式 DSN 設定] 對話方塊設定 DSN 時，驅動程式會使用的身分驗證模式：

- 標準：使用 Amazon Redshift 使用者名稱和密碼的標準身分驗證。
- AWS 設定檔：使用設定檔進行 IAM 身份驗證。
- AWS IAM 登入資料：使用 IAM 登入資料進行身分驗證
- 身分提供者：AD FS：使用 Active Directory Federation Services (AD FS) 進行 IAM 身分驗證。

- 身份提供者：身份驗證插件：一種授權插件，用於接受來自鏈接到 IAM 身份中心的任何 Web 身份提供者的 IAM 身份中心令牌或 OpenID Connect (OIDC) 基於 JSON 的身份令牌 (JWT)。
- 身分提供者：Azure AD：使用 Azure AD 入口網站進行 IAM 身分驗證。
- 身分提供者：JWT：使用 JSON Web 權杖 (JWT) 進行 IAM 身分驗證。
- 身分提供者：Okta：使用 Okta 進行 IAM 身分驗證。
- 身分識別提供者 PingFederate：IAM 身份驗證使用 PingFederate。

只有當您使用 Windows 驅動程式中的 [Amazon Redshift ODBC 驅動程式 DSN 設定] 對話方塊設定 DSN 時，才能使用此選項。當您使用連線字串或非 Windows 機器設定連線時，驅動程式會根據您指定的認證自動判斷是否要使用標準、設定 AWS 檔或 AWS IAM 登入資料驗證。若要使用身分提供者，您必須設定 plugin_name 屬性。

此為必要參數。

AutoCreate

- 預設值 — 0
- 資料類型 — 布林值

指定當所指定的使用者不存在時，驅動程式是否會建立新使用者的布林值。

- 1 | TRUE：如果透過 UID 指定的使用者不存在，驅動程式會建立新使用者。
- 0 | FALSE：驅動程式不會建立新使用者。如果指定的使用者不存在，則身分驗證會失敗。

此為選用參數。

CaFile

- 預設值 — 無
- 資料類型 — 字串

用於某些 IAM 身分驗證形式之 CA 憑證檔案的檔案路徑。

這個參數只能在 Linux 上使用。

此為選用參數。

client_id

- 預設值 — 無
- 資料類型 — 字串

與 Azure AD 中 Amazon Redshift 應用程式相關聯的用戶端 ID。

如果透過 Azure AD 服務進行驗證，則需要此參數。

client_secret

- 預設值 — 無
- 資料類型 — 字串

與 Azure AD 中 Amazon Redshift 應用程式相關聯的私密金鑰。

如果透過 Azure AD 服務進行驗證，則需要此參數。

ClusterId

- 預設值 — 無
- 資料類型 — 字串

您想要連線到之 Amazon Redshift 叢集的名稱。其會用於 IAM 身分驗證。伺服器參數中不會指定叢集 ID。

此為選用參數。

compression

- 預設值 — 關閉
- 資料類型 — 字串

用於 Amazon Redshift 伺服器與用戶端或驅動程式之間的有線通訊協定通訊的壓縮方法。

您可以指定下列值：

- lz4：將用於與 Amazon Redshift 進行有線通訊協定通訊的壓縮方法設定為。lz4
- zstd：將用於與 Amazon Redshift 進行有線通訊協定通訊的壓縮方法設定為。zstd

- 關閉：不使用壓縮來與 Amazon Redshift 進行有線通訊協定通訊。

此為選用參數。

資料庫

- 預設值 — 無
- 資料類型 — 字串

您想要存取之 Amazon Redshift 資料庫的名稱。

此為必要參數。

DatabaseMetadataCurrentDb 只有

- 預設值 — 1
- 資料類型 — 布林值

指定驅動程式是否會從多個資料庫和叢集傳回中繼資料的布林值。

- 1 | TRUE：驅動程式只會從目前的資料庫傳回中繼資料。
- 0 | FALSE。驅動程式會傳回多個 Amazon Redshift 資料庫和叢集的中繼資料。

此為選用參數。

dbgroups_filter

- 預設值 — 無
- 資料類型 — 字串

使用 Azure、瀏覽器 Azure 和瀏覽器 SAML 驗 DbGroups 證類型時，您可以指定用來篩選出從 Amazon Redshift 的 SAML 回應接收到的規則運算式。

此為選用參數。

驅動程式

- 預設值 — Amazon Redshift ODBC 驅動程式 (x64)

- 資料類型 — 字串

驅動程式的名稱。唯一支援的值是 Amazon Redshift ODBC 驅動程式 (x64)。

如果您未設定 DSN，則需要此參數。

DSN

- 預設值 — 無
- 資料類型 — 字串

驅動程式資料來源名稱的名稱。應用程式會在 SQL DriverConnect API 中指定 DSN。

如果您未設定驅動程式，則需要此參數。

EndpointUrl

- 預設值 — 無
- 資料類型 — 字串

用來與 Amazon Redshift Coral Service 通訊以進行 IAM 身分驗證的覆寫端點。

此為選用參數。

ForceLowercase

- 預設值 — 0
- 資料類型 — 布林值

一個布林值，指定在使用單一登入身分驗證時，驅動程式是否全部從身分提供者 DbGroups 傳送至 Amazon Redshift 的小寫字母。

- 1 | TRUE：驅動程式會將所 DbGroups 有從身分提供者傳送的資料都小寫。
- 0 | 錯誤：驅動程式不會變更 DbGroups。

此為選用參數。

group_federation

- 預設值 — 0
- 資料類型 — 布林值

一個布林值，指定是否使用 `getClusterCredentialsWithIAM` API 來取得已佈建叢集中的暫時叢集認證。此選項可讓 IAM 使用者與佈建叢集中的 Redshift 資料庫角色整合。請注意，此選項不適用於 Redshift 無伺服器命名空間。

- 1 | TRUE：驅動程式會使用 `getClusterCredentialsWithIAM` API 取得已佈建叢集中的暫時叢集認證。
- 0 | FALSE：驅動程式會使用預設 `getClusterCredentials` API 取得已佈建叢集中的暫存叢集認證。

此為選用參數。

https_proxy_host

- 預設值 — 無
- 資料類型 — 字串

您想要透過其通過 IAM 身分驗證程序之代理伺服器的主機名稱或 IP 地址。

此為選用參數。

https_proxy_password

- 預設值 — 無
- 資料類型 — 字串

您用來存取代理伺服器的密碼。其會用於 IAM 身分驗證。

此為選用參數。

https_proxy_port

- 預設值 — 無

- 資料類型 — 整數

代理伺服器用來接聽用戶端連線的連接埠號碼。其會用於 IAM 身分驗證。

此為選用參數。

https_proxy_username

- 預設值 — 無
- 資料類型 — 字串

您用來存取代理伺服器的使用者名稱。其會用於 IAM 身分驗證。

此為選用參數。

IAM

- 預設值 — 0
- 資料類型 — 布林值

指定驅動程式是否會使用 IAM 身分驗證方法來驗證連線的布林值。

- 1 | TRUE：驅動程式會使用其中一種 IAM 身分驗證方法 (使用存取金鑰和私密金鑰組、或設定檔或憑證服務)。
- 0 | FALSE。驅動程式會使用標準身分驗證 (使用資料庫使用者名稱和密碼)。

此為選用參數。

識別名稱空間

- 預設值 — 無
- 資料類型 — 字串

使 IdpTokenAuthPlugin 用進行驗證時使用的身份名稱空間。它可協助 Redshift 判斷要使用哪個 IAM Identity Center 執行個體。

如果只存在一個 IAM Identity Center 執行個體，或者已設定預設身分命名空間，則此參數為選用參數，否則為必要參數。

idp_host

- 預設值 — 無
- 資料類型 — 字串

您用來對 Amazon Redshift 進行身分驗證的 IdP (身分提供者) 主機。

此為選用參數。

idp_port

- 預設值 — 無
- 資料類型 — 整數

您用來對 Amazon Redshift 進行身分驗證的 IdP (身分提供者) 連接埠。根據您在建立、修改或遷移叢集時所選取的連接埠而定，允許存取選取的連接埠。

此為選用參數。

idp_response_timeout

- 預設值 — 120
- 資料類型 — 整數

透過瀏覽器外掛程式使用 SAML 或 Azure AD 服務時，驅動程式等待身分提供者所傳 SAML 回應的秒數。

此為選用參數。

idp_tenant

- 預設值 — 無
- 資料類型 — 字串

與 Amazon Redshift 應用程式相關聯的 Azure AD 租用戶 ID。

如果透過 Azure AD 服務進行驗證，則需要此參數。

idp_use_https_proxy

- 預設值 — 0
- 資料類型 — 布林值

指定驅動程式是否會透過代理伺服器來通過身分提供者 (IdP) 身分驗證程序的布林值。

- 1 | TRUE：驅動程式會透過代理伺服器來通過 IdP 身分驗證程序。
- 0 | FALSE。驅動程式不會透過代理伺服器來通過 IdP 身分驗證程序。

此為選用參數。

InstanceProfile

- 預設值 — 0
- 資料類型 — 布林值

指定驅動程式在設定為使用設定檔進行身分驗證時，是否會使用 Amazon EC2 執行個體設定檔的布林值。

- 1 | TRUE：驅動程式會使用 Amazon EC2 執行個體設定檔。
- 0 | FALSE。驅動程式會改用 [設定檔名稱] 選項 (設定檔) 所指定的鏈結角色設定檔。

此為選用參數。

KeepAlive

- 預設值 — 1
- 資料類型 — 布林值

指定驅動程式是否會使用 TCP 保持連線來防止連線逾時的布林值。

- 1 | TRUE：驅動程式會使用 TCP 保持連線來防止連線逾時。
- 0 | FALSE。驅動程式不會使用 TCP 保持連線。

此為選用參數。

KeepAlive伯爵

- 預設值 — 0
- 資料類型 — 整數

在認為連線已中斷之前可遺失的 TCP 保持連線封包數。此參數設為 0 時，驅動程式會使用此設定的系統預設值。

此為選用參數。

KeepAlive間隔

- 預設值 — 0
- 資料類型 — 整數

每一次 TCP 保持連線重新傳輸之間的秒數。此參數設為 0 時，驅動程式會使用此設定的系統預設值。

此為選用參數。

KeepAlive時間

- 預設值 — 0
- 資料類型 — 整數

驅動程式傳送 TCP 保持連線封包之前的閒置秒數。此參數設為 0 時，驅動程式會使用此設定的系統預設值。

此為選用參數。

listen_port

- 預設值 — 7890
- 資料類型 — 整數

透過瀏覽器外掛程式使用 SAML 或 Azure AD 服務時，驅動程式用來接收身分提供者所傳 SAML 回應的連接埠。

此為選用參數。

login_url

- 預設值 — 無
- 資料類型 — 字串

使用一般瀏覽器 SAML 外掛程式時，身分提供者網站上資源的 URL。

如果透過瀏覽器外掛程式向 SAML 或 Azure AD 服務進行驗證，則需要此參數。

登錄 ToRp

- 預設值 — urn:amazon:webservices
- 資料類型 — 字串

您要用於 AD FS 身分驗證類型的依賴方信任。

此為選用字串。

LogLevel

- 預設值 — 0
- 資料類型 — 整數

使用此屬性可在驅動程式中啟用或停用日誌記錄，以及指定日誌檔案中包含的詳細資訊數量。日誌記錄建議只啟用到足以擷取到問題就好，因為日誌記錄會降低效能，而且可能會耗用大量磁碟空間。

將此屬性設為以下其中一個值：

- 0 : OFF。停用所有日誌記錄功能。
- 1 : ERROR。記錄可能允許驅動程式繼續執行但會產生錯誤的錯誤事件。
- 2 : API_CALL。記錄 ODBC API 函數呼叫與函數引數值。
- 3 : INFO。記錄用於描述驅動程式進展的一般資訊。
- 4 : MSG_PROTOCOL。記錄驅動程式的訊息通訊協定詳細資訊。
- 5 : DEBUG。記錄所有驅動程式活動。
- 6 : DEBUG_APPEND。持續附加所有驅動程式活動的日誌。

啟用記錄時，驅動程式會在您在內LogPath容中指定的位置產生下列記錄檔：

- 記錄在連線交握期間發生之驅動程式活動的 `redshift_odbc.log.1` 檔案。
- 在與資料庫建立連線後所有驅動程式活動的 `redshift_odbc.log` 檔案。

此為選用參數。

LogPath

- 預設值 — 作業系統特定的 TEMP 目錄
- 資料類型 — 字串

當驅動程式儲存記錄檔大於 0 時，該資料夾LogLevel的完整路徑。

此為選用參數。

Min_TLS

- 預設值-1.2
- 資料類型 — 字串

驅動程式允許資料存放區用於加密連線的 TLS/SSL 最低版本。例如，如果指定 TLS 1.2，則無法使用 TLS 1.1 來加密連線。

Min_TLS 接受以下值：

- 1.0：連線必須至少使用 TLS 1.0。
- 1.1：連線必須至少使用 TLS 1.1。
- 1.2：連線至少必須使用 TLS 1.2。

此為選用參數。

partner_spid

- 預設值 — 無
- 資料類型 — 字串

使用服務驗證連線時要使用的夥伴 SPID (服務提供者 ID) 值。 PingFederate

此為選用參數。

Password | PWS

- 預設值 — 無
- 資料類型 — 字串

與您在 [使用者] 欄位 (UID | User | LogonID) 中所提供資料庫使用者名稱對應的密碼。

此為選用參數。

plugin_name

- 預設值 — 無
- 資料類型 — 字串

您想要用於身分驗證的憑證提供者外掛程式名稱。

支援下列值：

- ADFS：使用 Active Directory Federation Services 進行身分驗證。
- AzureAD：使用 Microsoft Azure Active Directory (AD) Service 進行身分驗證。
- BrowserAzureAD：使用 Microsoft Azure Active Directory (AD) Service 的瀏覽器外掛程式進行身分驗證。
- BrowserSAML：使用 SAML 服務 (例如 Okta 或 Ping) 的瀏覽器外掛程式進行身分驗證。
- IdpTokenAuthPlugin：一種授權外掛程式，可從任何連結至 IAM 身分中心的網路身分提供者接受 IAM 身分中心權杖或 OpenID Connect (OIDC) JSON 型身分權杖 (JWT)。
- JWT：使用 JSON Web 權杖 (JWT) 進行身分驗證。
- Ping：使用該 PingFederate 服務進行身份驗證。
- Okta：使用 Okta 服務進行身分驗證。

此為選用參數。

連接埠 | PortNumber

- 預設值 — 5439

- 資料類型 — 整數

Amazon Redshift 伺服器用來接聽用戶端連線的 TCP 連接埠號碼。

此為選用參數。

preferred_role

- 預設值 — 無
- 資料類型 — 字串

您要在連線到 Amazon Redshift 期間擔任的角色。其會用於 IAM 身分驗證。

此為選用參數。

設定檔

- 預設值 — 無
- 資料類型 — 字串

用於在 Amazon Redshift 中進行驗證的使用者 AWS 設定檔名稱。

- 如果使用執行個體設定檔參數 (InstanceProfile屬性) 設為 1 | TRUE，則該設定優先順序，而驅動程式改用 Amazon EC2 執行個體設定檔。
- 包含設定檔之憑證檔案的預設位置為 ~/.aws/Credentials。可使用 AWS_SHARED_CREDENTIALS_FILE 環境變數以指向不同的憑證檔案。

此為選用參數。

provider_name

- 預設值 — 無
- 資料類型 — 字串

使用者使用 CREATE IDENTITY PROVIDER 查詢所建立的身分驗證提供者。其會用於原生 Amazon Redshift 身分驗證。

此為選用參數。

ProxyHost

- 預設值 — 無
- 資料類型 — 字串

您想要透過其進行連線之代理伺服器的主機名稱或 IP 地址。

此為選用參數。

ProxyPort

- 預設值 — 無
- 資料類型 — 整數

代理伺服器用來接聽用戶端連線的連接埠號碼。

此為選用參數。

ProxyPwd

- 預設值 — 無
- 資料類型 — 字串

您用來存取代理伺服器的密碼。

此為選用參數。

ProxyUid

- 預設值 — 無
- 資料類型 — 字串

您用來存取代理伺服器的使用者名稱。

此為選用參數。

ReadOnly

- 預設值 — 0

- 資料類型 — 布林值

指定驅動程式是否處於唯讀模式的布林值。

- 1 | TRUE：連線處於唯讀模式，無法寫入到資料存放區。
- 0 | FALSE：連接不處於唯讀模式，可以寫入到資料存放區。

此為選用參數。

region

- 預設值 — 無
- 資料類型 — 字串

叢集所在的 AWS 區域。

此為選用參數。

SecretAccess 關鍵

- 預設值 — 無
- 資料類型 — 字串

使用者或角色的 IAM 私密金鑰。如果設定此參數，您也必須設定 AccessKeyID。

此為選用參數。

SessionToken

- 預設值 — 無
- 資料類型 — 字串

與您用來驗證的 IAM 角色相關聯的臨時 IAM 工作階段權杖。

此為選用參數。

伺服器 | HostName | 主機

- 預設值 — 無

- 資料類型 — 字串

要連線到的端點伺服器。

此為必要參數。

ssl_insecure

- 預設值 — 0
- 資料類型 — 布林值

指定驅動程式是否會檢查 IdP 伺服器憑證真確性的布林值。

- 1 | TRUE : 驅動程式不會檢查 IdP 伺服器憑證的真確性。
- 0 | FALSE : 驅動程式會檢查 IdP 伺服器憑證的真確性。

此為選用參數。

SSLMode

- 預設值 — verify-ca
- 資料類型 — 字串

連線到 Amazon Redshift 時要使用的 SSL 憑證驗證模式。可能的值如下：

- verify-full : 僅使用 SSL、受信任的憑證授權機構和符合憑證的伺服器名稱進行連線。
- verify-ca : 僅使用 SSL 和受信任的憑證授權機構進行連線。
- require : 僅使用 SSL 進行連線。
- prefer : 使用 SSL (如果可用) 進行連線。否則，以不使用 SSL 的方式進行連線。
- allow : 預設會以不使用 SSL 的方式進行連線。如果伺服器需要 SSL 連線，則使用 SSL。
- disable : 以不使用 SSL 的方式進行連線。

此為選用參數。

StsConnection逾時

- 預設值 — 0

- 資料類型 — 整數

IAM 連線的等待時間上限 (以秒為單位)。如果設定為 0 或未指定，驅動程式會等待每次 AWS STS 呼叫 60 秒。

此為選用參數。

StsEndpoint网址

- 預設值 — 無
- 資料類型 — 字串

此選項指定用於與 AWS Security Token Service (AWS STS) 通訊的覆寫端點。

此為選用參數。

token

- 預設值 — 無
- 資料類型 — 字串

IAM 身分中心提供的存取權杖或 OpenID Connect (OIDC) JSON 網頁權杖 (JWT)，由與 IAM 身分中心連結的網路身分提供者所提供。您的應用程式必須透過 IAM 身分中心或與 IAM 身分中心連結的身分提供者驗證應用程式的使用者，以產生此權杖。

此參數可搭配使用 `IdpTokenAuthPlugin`。

令牌類型

- 預設值 — 無
- 資料類型 — 字串

正在中使用的權杖類型 `IdpTokenAuthPlugin`。

您可以指定下列值：

訪問令牌

如果您使用 IAM 身分中心提供的存取權杖，請輸入此選項。

EXT_JWT

如果您使用 OpenID Connect (OIDC) JSON 網頁權杖 (JWT) ，這是由與 IAM 身分中心整合的網頁型身分提供者所提供的，請輸入此選項。

此參數可搭配使用 `IdpTokenAuthPlugin`。

UID | User | LogonID

- 預設值 — 無
- 資料類型 — 字串

您用來存取 Amazon Redshift 伺服器的使用者名稱。

若您使用資料庫身分驗證，則此為必要參數。

web_identity_token

- 預設值 — 無
- 資料類型 — 字串

身分提供者所提供的 OAUTH 權杖。其會用於 JWT 外掛程式。

如果您將 `plugin_name` 參數設定為 `BasicJwtCredentialsProvider`

先前的 ODBC 驅動程式版本

請在您的工具需要特定版本的驅動程式時，才下載 Amazon Redshift ODBC 驅動程式 2.x 版之前的版本。

使用先前的 ODBC 驅動程式版本 (適用於 Microsoft Windows)

以下是適用於 Microsoft Windows 的舊版 Amazon Redshift ODBC 驅動程式 2.x 版：

- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.1.0/> AmazonRedshift 在中 AWS 國地區，請使用以
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.0.0/> AmazonRedshift 在中 AWS 國地區，請使用以
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.1.0/> AmazonRedshift 在中 AWS 國地區，請使用以

- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.11/> AmazonRedshift 在中 AWS 國地區，請使用以
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.9/> AmazonRedshift 在中 AWS 國地區，請使用以
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.8/> AmazonRedshift 在中 AWS 國地區，請使用以
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.7/> AmazonRedshift 在中 AWS 國地區，請使用以
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.6/> AmazonRedshift 在中 AWS 國地區，請使用以
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.5/> AmazonRedshift 在中 AWS 國地區，請使用以
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.3/> AmazonRedshift 在中 AWS 國地區，請使用以
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.1/> AmazonRedshift 在中 AWS 國地區，請使用以

使用先前的 ODBC 驅動程式版本 (適用於 Linux)

以下是適用於 Linux 的舊版 Amazon Redshift ODBC 驅動程式 2.x 版：

- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.1.0/> AmazonRedshift 在中國地區，請使用以下連結
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.0.0/> AmazonRedshift 在中國地區，請使用以下連結
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.1.0/> AmazonRedshift 在中國地區，請使用以下連結
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.11/> AmazonRedshift 在中國地區，請使用以下
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.9/> AmazonRedshift 在中國地區，請使用以下
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.8/> AmazonRedshift 在中國地區，請使用以下連結

- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.7/> AmazonRedshift 在中國地區，請使用以下連結
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.6/> AmazonRedshift 在中國地區，請使用以下
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.5/> AmazonRedshift 在中國地區，請使用以下
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.3/> AmazonRedshift 在中國地區，請使用以下連結
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.1/> AmazonRedshift 在中國地區，請使用以下連結

設定 ODBC 連線

您可以從許多第三方 SQL 用戶端工具和應用程式使用 ODBC 連線來連線至 Amazon Redshift 叢集。若要這麼做，請在用戶端電腦或 Amazon EC2 執行個體上設定連線。如果用戶端工具支援 JDBC，您可能選擇使用這種連線，而非 ODBC，因為 JDBC 的設定簡單。但是，如果用戶端工具不支援 JDBC，請遵循本節的步驟來設定 ODBC 連線。

Amazon Redshift 會提供適用於 Linux、Windows 和 macOS X 作業系統的 64 位元 ODBC 驅動程式。32 位元的 ODBC 驅動程式已停止使用。除了緊急的安全修補程式外，不會再發佈其他更新。

如需 ODBC 驅動程式功能和先決條件的最新資訊，請參閱 [Amazon Redshift ODBC 驅動程式版本備註](#)。

如需 Amazon Redshift ODBC 驅動程式的安裝與組態資訊，請參閱 [Amazon Redshift ODBC 連接器安裝和組態指南](#)。

如果想要使用 ODBC 連線，請採取以下步驟。

主題

- [取得叢集的 ODBC URL](#)
- [在 Microsoft Windows 上安裝並設定 Amazon Redshift ODBC 驅動程式](#)
- [在 Linux 上安裝 Amazon Redshift ODBC 驅動程式](#)
- [在 macOS X 上安裝 Amazon Redshift ODBC 驅動程式](#)
- [使用 ODBC 驅動程式管理員來設定 Linux 和 macOS X 作業系統上的驅動程式](#)
- [設定 ODBC 驅動程式選項](#)

- [先前的 ODBC 驅動程式版本](#)

取得叢集的 ODBC URL

Amazon Redshift 會在 Amazon Redshift 主控台中顯示叢集的 ODBC URL。此 URL 包含要在用戶端電腦和資料庫之間設定連線的資訊。

ODBC URL 採用下列格

式：`Driver={driver};Server=endpoint;Database=database_name;UID=user_name;PWD=pass`

前面顯示的格式欄位具有下列值。

欄位	Value
Driver	要使用的 64 位元 ODBC 驅動程式的名稱：Amazon Redshift (x64)。 32 位元 ODBC 驅動程式的名稱：Amazon Redshift (x86)。
Server	Amazon Redshift 叢集的端點。
Database	您為叢集建立的資料庫。
UID	有許可連接至資料庫之使用者帳戶的使用者名稱。雖然可使用啟動叢集時所設定的管理員使用者帳戶，但此值是資料庫許可，不是 Amazon Redshift 許可。
PWD	用於連接至資料庫之使用者帳戶的密碼。
Port	您啟動叢集時指定的連接埠號碼。如果有防火牆，請確定此連接埠已開放給您使用。

上述資料表中的欄位可包含下列特殊字元：

```
[ ] { } ( ) , ; ? * = ! @
```

如果您使用這些特殊字元，則必須用大括號括住值。例如，連線字串中的密碼值 `Your;password123` 會表示為 `PWD={Your;password123};`。

由於 `Field=value` 配對會以分號分隔，因此 `}` 與 `;` 的組合中間若有任意數量的空格，將會被視為是 `Field={value};` 配對的結尾。建議您避免在欄位值中使用連續的 `};`。例如，如果您將密碼值設定

為 PWD={This is a passwor} ;d}; , 則密碼會是 This is a passwor} ; , 因此 URL 會發生錯誤。

以下是 ODBC URL 範例。

```
Driver={Amazon Redshift (x64)};  
        Server=examplecluster.abc123xyz789.us-  
west-2.redshift.amazonaws.com;  
        Database=dev;  
        UID=adminuser;  
        PWD=insert_your_admin_user_password_here;  
        Port=5439
```

如需如何取得 ODBC 連線的資訊，請參閱[尋找叢集連線字串](#)。

在 Microsoft Windows 上安裝並設定 Amazon Redshift ODBC 驅動程式

系統要求

請在存取 Amazon Redshift 資料倉儲的用戶端電腦上安裝 Amazon Redshift ODBC 驅動程式。您安裝驅動程式的每一台電腦必須符合最低系統需求清單：如需最低系統要求的相關資訊，請參閱[Amazon Redshift ODBC 連接器安裝和組態指南](#)。

在 Windows 作業系統上安裝 Amazon Redshift 驅動程式

使用下列程序來下載適用於 Windows 作業系統的 Amazon Redshift ODBC 驅動程式。僅在您執行的第三方應用程式經認證可與 Amazon Redshift 搭配使用，且需要有特定驅動程式時，才使用不同於以下的驅動程式。

安裝 ODBC 驅動程式

1. 根據 SQL 用戶端工具或應用程式的系統架構，下載下列其中一個項目：

- [64 位元 ODBC 驅動程式版本 1.5.9](#) 版本 1.5.9。

這個驅動程式的名稱是 Amazon Redshift (x64)。

- [32 位元 ODBC 驅動程式版本 1.4.52](#) BC 驅動程式版本 1.4.52

這個驅動程式的名稱是 Amazon Redshift (x86)。32 位元的 ODBC 驅動程式已停止使用。除了緊急的安全修補程式外，不會再發佈其他更新。

Note

下載對應於 SQL 用戶端工具或應用程式之系統架構的 MSI 套件。例如，假設 SQL 用戶端工具是 64 位元，請安裝 64 位元驅動程式。

然後下載並檢閱 [Amazon Redshift ODBC 和 JDBC 驅動程式授權合約](#)。

- 按兩下 .msi 檔案，然後遵循精靈中的步驟來安裝驅動程式。

在 Microsoft Windows 上建立 ODBC 連線的系統 DSN 項目

在下載並安裝 ODBC 驅動程式之後，請將資料來源名稱 (DSN) 項目新增至用戶端電腦或 Amazon EC2 執行個體。SQL 用戶端工具會使用此資料來源以連線至 Amazon Redshift 資料庫。

建議您建立系統 DSN，而不是使用者 DSN。某些應用程式會使用不同的使用者帳戶載入資料。這些應用程式可能無法偵測在另一個使用者帳戶下建立的使用者 DSN。

Note

對於使用 AWS Identity and Access Management (IAM) 登入資料或身分提供者 (IdP) 登入資料的身分驗證，則需要其他步驟。如需詳細資訊，請參閱 [設定 JDBC 或 ODBC 連線使用 IAM 登入資料](#)。

如需如何建立系統 DSN 項目的相關資訊，請參閱 [Amazon Redshift ODBC 連接器安裝和組態指南](#)。

在 Windows 上建立 ODBC 連線的系統 DSN 項目

- 在 Start (開啟) 功能表中，開啟 ODBC Data Sources (ODBC 資料來源)。

確定您選擇的 ODBC 資料來源管理員具有與您要用來連線到 Amazon Redshift 的用戶端應用程式相同的位元。

- 在 ODBC 資料來源管理員中，選擇驅動程式索引標籤並尋找驅動程式資料夾：
 - Amazon Redshift ODBC 驅動程式 (64 位元)
 - Amazon Redshift ODBC 驅動程式 (32 位元)

3. 選擇 System DSN (系統 DSN) 標籤，為電腦上的所有使用者設定驅動程式，或選擇 User DSN (使用者 DSN) 標籤，只為您的使用者帳戶設定驅動程式。
4. 選擇新增。Create New Data Source (建立新的資料來源) 視窗會開啟。
5. 選擇 Amazon Redshift ODBC 驅動程式，然後選擇完成。Amazon Redshift ODBC 驅動程式 DSN 設定視窗會開啟。
6. 在 Connection Settings (連線設定) 下，輸入下列資訊：

Data Source Name (資料來源名稱)

輸入資料來源的名稱。您可以使用稍後建立叢集連線時要用來識別資料來源的任何名稱。例如，如果您遵循了《Amazon Redshift 入門指南》，則可能會輸入 `exampleclusterdsn`，以便輕鬆記住與此 DSN 建立關聯的叢集。

Server

指定 Amazon Redshift 叢集的端點。您可以在 Amazon Redshift 主控台的叢集詳細資訊頁面上找到此資訊。如需詳細資訊，請參閱 [在 Amazon Redshift 中設定連線](#)。

連線埠

輸入資料庫使用的連接埠號碼。請使用在叢集啟動或修改時設定給叢集使用的連接埠。

資料庫

輸入 Amazon Redshift 資料庫的名稱。如果您在未指定資料庫名稱的情況下啟動了叢集，請輸入 `dev`。否則，請使用您在啟動過程選擇的名稱。如果您遵循了《Amazon Redshift 入門指南》，請輸入 `dev`。

7. 在 Authentication (身分驗證) 下，指定要設定標準或 IAM 身分驗證的組態選項。如需不同身分驗證選項的相關資訊，請參閱《Amazon Redshift ODBC 連接器安裝和組態指南》中的「在 Windows 上設定身分驗證」。
8. 在 SSL Settings (SSL 設定) 下，指定下列這一項的值：

SSL authentication (SSL 身分驗證)

選擇用於處理 Secure Sockets Layer (SSL) 的模式。在測試環境中，您可以使用 `prefer`。不過，若為生產環境且需要交換安全資料時，請使用 `verify-ca` 或 `verify-full`。如需在 Windows 上使用 SSL 的相關資訊，請參閱《Amazon Redshift ODBC 連接器安裝和組態指南》中的「在 Windows 上設定 SSL 驗證」。

9. 在 Additional Options (其他選項) 下，指定如何將查詢結果傳回給 SQL 用戶端工具或應用程式的選項。如需詳細資訊，請參閱《Amazon Redshift ODBC 連接器安裝和組態指南》中的「在 Windows 上設定其他選項」。

10. 在 Logging Options (記錄選項) 中，指定記錄選項的值：如需詳細資訊，請參閱《Amazon Redshift ODBC 連接器安裝和組態指南》中的「在 Windows 上設定記錄選項」。

然後選擇 OK (確定)。

11. 在 Data Type Options (資料類型選項) 下，指定資料類型的值。如需詳細資訊，請參閱《Amazon Redshift ODBC 連接器安裝和組態指南》中的「在 Windows 上設定資料類型選項」。

然後選擇 OK (確定)。

12. 選擇測試。如果用戶端電腦可以連線至 Amazon Redshift 資料庫，您會看到下列訊息：連線成功。

如果用戶端電腦無法連線至資料庫，您可以對可能的問題進行疑難排解。如需詳細資訊，請參閱[針對 Amazon Redshift 中的連線問題進行疑難排解](#)。

13. 在 Windows 上設定 TCP 保持連線，以防止連線逾時。如需如何在 Windows 上設定 TCP 保持連線的相關資訊，請參閱《Amazon Redshift ODBC 連接器安裝和組態指南》。

14. 若要協助疑難排解，請設定記錄。如需如何在 Windows 上設定記錄的相關資訊，請參閱《Amazon Redshift ODBC 連接器安裝和組態指南》。

在 Linux 上安裝 Amazon Redshift ODBC 驅動程式

系統要求

請在存取 Amazon Redshift 資料倉儲的用戶端電腦上安裝 Amazon Redshift ODBC 驅動程式。您安裝驅動程式的每一台電腦必須符合最低系統需求清單：如需最低系統要求的相關資訊，請參閱[Amazon Redshift ODBC 連接器安裝和組態指南](#)。

在 Linux 作業系統上安裝 Amazon Redshift 驅動程式

使用本節的步驟來下載 Amazon Redshift ODBC 驅動程式並安裝在 Linux 發行版本上。安裝程序會將驅動程式檔案安裝在下列目錄中：

- /opt/amazon/redshiftodbc/lib/64 (適用於 64 位元驅動程式)
- /opt/amazon/redshiftodbc/ErrorMessage
- /opt/amazon/redshiftodbc/Setup
- /opt/amazon/redshiftodbc/lib/32 (適用於 32 位元驅動程式)

安裝 Amazon Redshift ODBC 驅動程式

1. 根據 SQL 用戶端工具或應用程式的系統架構，下載下列其中一個項目：

- [64 位元 RPM 驅動程式版本 1.5.9](#) 5.9。
- [64 位元 Debian 驅動程式 1.5.9 版](#) 5.9。
- [32 位元 RPM 驅動程式版本 1.4.52](#) 版本 1.4.52
- [32 位元 Debian 驅動程式 1.4.52 版](#) 版本 1.4.52

其中每一個驅動程式的名稱都是 Amazon Redshift ODBC 驅動程式。32 位元的 ODBC 驅動程式已停止使用。除了緊急的安全修補程式外，不會再發佈其他更新。

Note

下載對應於 SQL 用戶端工具或應用程式之系統架構的套件。例如，假設用戶端工具是 64 位元，請安裝 64 位元驅動程式。

然後下載並檢閱 [Amazon Redshift ODBC 和 JDBC 驅動程式授權合約](#)。

2. 移至您下載套件的位置，然後執行下列其中一個命令。使用與您的 Linux 發行版本相應的指令。

- 在 RHEL 和 CentOS 作業系統上，執行下列命令。

```
yum --nogpgcheck localinstall RPMFileName
```

將 *RPMFileName* 取代為 RPM 套件檔案名稱。例如，下列命令示範安裝 64 位元驅動程式。

```
yum --nogpgcheck localinstall AmazonRedshiftODBC-64-bit-1.x.xx.xxxx-x.x86_64.rpm
```

- 在 SLES 上，執行下列命令。

```
zypper install RPMFileName
```

將 *RPMFileName* 取代為 RPM 套件檔案名稱。例如，下列命令示範安裝 64 位元驅動程式。

```
zypper install AmazonRedshiftODBC-1.x.x.xxxx-x.x86_64.rpm
```

- 在 Debian 上，執行下列命令。

```
sudo apt install ./DEBFileName.deb
```

將 *DEBFileName.deb* 取代為 Debian 套件檔案名稱。例如，下列命令示範安裝 64 位元驅動程式。

```
sudo apt install ./AmazonRedshiftODBC-1.x.x.xxxx-x.x86_64.deb
```

Important

驅動程式安裝完成時，請設定來用於您的系統。如需驅動程式組態的相關資訊，請參閱[使用 ODBC 驅動程式管理員來設定 Linux 和 macOS X 作業系統上的驅動程式](#)。

在 macOS X 上安裝 Amazon Redshift ODBC 驅動程式

系統要求

請在存取 Amazon Redshift 資料倉儲的用戶端電腦上安裝驅動程式。您安裝驅動程式的每一台電腦必須符合最低系統需求清單：如需最低系統要求的相關資訊，請參閱 [Amazon Redshift ODBC 連接器安裝和組態指南](#)。

在 macOS X 上安裝 Amazon Redshift ODBC 驅動程式

使用本節的步驟來下載 Amazon Redshift ODBC 驅動程式並安裝在支援的 macOS X 版本上。安裝程序會將驅動程式檔案安裝在下列目錄中：

- /opt/amazon/redshift/lib/universal
- /opt/amazon/redshift/ErrorMessage
- /opt/amazon/redshift/Setup

在 macOS X 上安裝 Amazon Redshift ODBC 驅動程式

1. 如果 macOS X 系統使用 Intel 架構，請下載 [macOS X Intel 驅動程式 1.5.9 版](#)。如果系統使用 ARM 架構，請下載 [macOS X ARM 驅動程式 1.5.9 版](#)。在這兩種情況下，此驅動程式的名稱都是 Amazon Redshift ODBC 驅動程序。

然後下載並檢閱 [Amazon Redshift ODBC 和 JDBC 驅動程式授權合約](#)。

2. 按兩下 AmazonRedshiftODBC.dmg 以掛載磁碟映像檔。
3. 按兩下 AmazonRedshiftODBC.pkg 以執行安裝程式。
4. 依照安裝程式中的步驟完成驅動程式安裝程序。若要執行安裝，請同意授權合約的條款。

Important

驅動程式安裝完成時，請設定來用於您的系統。如需驅動程式組態的相關資訊，請參閱[使用 ODBC 驅動程式管理員來設定 Linux 和 macOS X 作業系統上的驅動程式](#)。

使用 ODBC 驅動程式管理員來設定 Linux 和 macOS X 作業系統上的驅動程式

在 Linux 和 macOS X 作業系統上，您使用的是 ODBC 驅動程式管理員來設定 ODBC 連線設定。ODBC 驅動程式管理員使用組態檔案來定義及設定 ODBC 資料來源和驅動程式。您使用的 ODBC 驅動程式管理員視您使用的作業系統而定：

- unixODBC 驅動程式管理員 (適用於 Linux 作業系統)
- iODBC 驅動程式管理員 (適用於 macOS X 作業系統)

如需支援用來設定 Amazon Redshift ODBC 驅動程式的 ODBC 驅動程式管理員的相關資訊，請參閱 Linux 作業系統的 [系統要求](#) 和 macOS X 作業系統的 [系統要求](#)。另請參閱 [Amazon Redshift ODBC 連接器安裝和組態指南](#) 中的「在非 Windows 機器上指定 ODBC 驅動程式管理員」。

設定 Amazon Redshift ODBC 驅動程式需要三個檔案：`amazon.redshiftdbc.ini`、`odbc.ini` 和 `odbcinst.ini`。

如果是安裝到預設位置，則 `amazon.redshiftdbc.ini` 組態檔案位於下列其中一個目錄：

- `/opt/amazon/redshiftdbc/lib/64` (適用於 Linux 作業系統上的 64 位元驅動程式)
- `/opt/amazon/redshiftdbc/lib/32` (適用於 Linux 作業系統上的 32 位元驅動程式)
- `/opt/amazon/redshift/lib` (適用於 macOS X 上的驅動程式)

此外，在 Linux 上的 `/opt/amazon/redshiftdbc/Setup` 下，或在 macOS X 上的 `/opt/amazon/redshift/Setup` 下，有範例 `odbc.ini` 和 `odbcinst.ini` 檔案。您可以使用這些檔案做為設定 Amazon Redshift ODBC 驅動程式和資料來源名稱 (DSN) 的範例。

不建議使用 Amazon Redshift ODBC 驅動程式安裝目錄來存放組態檔案。Setup 目錄中的範例檔案僅供當作範例。如果您後來重新安裝 Amazon Redshift ODBC 驅動程式，或升級為更新版本，安裝目錄會遭到覆寫。然後，您對這些檔案可能做的任何變更都會遺失。

若要避免這種情況，請將 `amazon.redshiftdbc.ini` 檔案複製到安裝目錄以外的目錄。如果您將此檔案複製到使用者的主目錄，請在檔案名稱開頭加上一點 (`.`)，將它變成隱藏檔。

對於 `odbc.ini` 和 `odbcinst.ini` 檔案，請使用位於使用者主目錄中的組態檔案，或在另一個目錄中建立新版本。根據預設，您的 Linux 或 macOS X 作業系統應該在使用者的主目錄 (`/home/$USER` 或 `~/`) 中具有 `odbcinst.ini` 檔案和 `odbc.ini` 檔案。這些預設檔案是隱藏檔，每個檔案名稱前面以點表示。僅當使用 `-a` 旗標來列出目錄內容時，才會顯示這些檔案。

無論對 `odbc.ini` 和 `odbcinst.ini` 檔案選擇何種選項，都會修改這些檔案來新增驅動程式和 DSN 組態資訊。如果建立新檔案，則還需要設定環境變數來指定這些組態檔案所在的位置。

根據預設，ODBC 驅動程式管理員會設定為使用隱藏版本的 `odbc.ini` 和 `odbcinst.ini` 組態檔 (命名為 `.odbc.ini` 和 `.odbcinst.ini`)，這些組態檔位於主目錄中。它們也會設定為使用驅動程式安裝目錄的 `/lib` 子資料夾中的 `amazon.redshiftdbc.ini` 檔案。如果您將這些組態檔儲存在其他位置，請設定如下所述的環境變數，以便驅動程式管理員可以找到這些檔案。如需詳細資訊，請參閱 [Amazon Redshift ODBC 連接器安裝和組態指南](#) 中的「指定驅動程式組態檔案的位置」。

在 Linux 和 macOS X 作業系統上建立資料來源名稱

使用資料來源名稱 (DSN) 連接至資料倉庫時，請設定 `odbc.ini` 檔案來定義 DSN。在 `odbc.ini` 檔案中設定屬性，以建立 DSN 來指定資料倉庫的連線資訊。

如需有關如何設定 `odbc.ini` 檔案的詳細資訊，請參閱 [Amazon Redshift ODBC 連接器安裝和組態指南](#) 中的「在非 Windows 電腦上建立資料來源名稱」在 [中國 AWS 地區](#)，請使用下列 [連接器安裝和組態指南](#)

在 Linux 作業系統上使用下列格式。

```
[ODBC Data Sources]
driver_name=dsn_name

[dsn_name]
Driver=path/driver_file

Host=cluster_endpoint
Port=port_number
Database=database_name
```

```
locale=locale
```

以下範例示範 Linux 作業系統上使用 64 位元 ODBC 驅動程式的 odbc.ini 組態。

```
[ODBC Data Sources]
Amazon_Redshift_x64=Amazon Redshift (x64)

[Amazon Redshift (x64)]
Driver=/opt/amazon/redshiftdbc/lib/64/libamazonredshiftdbc64.so
Host=examplecluster.abc123xyz789.us-west-2.redshift.amazonaws.com
Port=5932
Database=dev
locale=en-US
```

以下範例示範 Linux 作業系統上使用 32 位元 ODBC 驅動程式的 odbc.ini 組態。

```
[ODBC Data Sources]
Amazon_Redshift_x32=Amazon Redshift (x86)

[Amazon Redshift (x86)]
Driver=/opt/amazon/redshiftdbc/lib/32/libamazonredshiftdbc32.so
Host=examplecluster.abc123xyz789.us-west-2.redshift.amazonaws.com
Port=5932
Database=dev
locale=en-US
```

在 macOS X 作業系統上使用下列格式。

```
[ODBC Data Sources]
driver_name=dsn_name

[dsn_name]
Driver=path/lib/amazonredshiftdbc.dylib

Host=cluster_endpoint
Port=port_number
Database=database_name
locale=locale
```

以下範例示範 macOS X 作業系統上的 odbc.ini 組態。

```
[ODBC Data Sources]
Amazon_Redshift_dylib=Amazon Redshift DSN for macOS X

[Amazon Redshift DSN for macOS X]
Driver=/opt/amazon/redshift/lib/amazonredshiftodbc.dylib
Host=examplecluster.abc123xyz789.us-west-2.redshift.amazonaws.com
Port=5932
Database=dev
locale=en-US
```

在 Linux 和 macOS X 作業系統上設定沒有 DSN 的連線

若要透過沒有 DSN 的連線連接至您的資料存放區，請在 `odbcinst.ini` 檔案中定義驅動程式。然後，在應用程式中提供無 DSN 的連線字串。

如需如何在此情況下設定 `odbcinst.ini` 檔案的相關資訊，請參閱 [Amazon Redshift ODBC 連接器安裝和組態指南](#) 中的「在非 Windows 機器上設定無 DSN 的連線」。

在 Linux 作業系統上使用下列格式。

```
[ODBC Drivers]
driver_name=Installed
...

[driver_name]
Description=driver_description
Driver=path/driver_file
...
```

以下範例針對 Linux 作業系統上安裝於預設目錄中的 64 位元驅動程式示範 `odbcinst.ini` 組態。

```
[ODBC Drivers]
Amazon Redshift (x64)=Installed

[Amazon Redshift (x64)]
Description=Amazon Redshift ODBC Driver (64-bit)
Driver=/opt/amazon/redshiftodbc/lib/64/libamazonredshiftodbc64.so
```

以下範例針對 Linux 作業系統上安裝於預設目錄中的 32 位元驅動程式示範 `odbcinst.ini` 組態。

```
[ODBC Drivers]
```

```
Amazon Redshift (x86)=Installed
```

```
[Amazon Redshift (x86)]
```

```
Description=Amazon Redshift ODBC Driver (32-bit)
```

```
Driver=/opt/amazon/redshiftodbc/lib/32/libamazonredshiftodbc32.so
```

在 macOS X 作業系統上使用下列格式。

```
[ODBC Drivers]
```

```
driver_name=Installed
```

```
...
```

```
[driver_name]
```

```
Description=driver_description
```

```
Driver=path/lib/amazonredshiftodbc.dylib
```

```
...
```

以下範例針對 macOS X 作業系統上安裝於預設目錄中的驅動程式，示範 `odbcinst.ini` 組態。

```
[ODBC Drivers]
```

```
Amazon RedshiftODBC DSN=Installed
```

```
[Amazon RedshiftODBC DSN]
```

```
Description=Amazon Redshift ODBC Driver for macOS X
```

```
Driver=/opt/amazon/redshift/lib/amazonredshiftodbc.dylib
```

設定環境變數

使用正確的 ODBC 驅動程式管理員來載入正確的驅動程式。若要這樣做，請設定程式庫路徑環境變數。如需詳細資訊，請參閱 [Amazon Redshift ODBC 連接器安裝和組態指南](#) 中的「在非 Windows 機器上指定 ODBC 驅動程式管理員」。

根據預設，ODBC 驅動程式管理員會設定為使用隱藏版本的 `odbc.ini` 和 `odbcinst.ini` 組態檔 (命名為 `.odbc.ini` 和 `.odbcinst.ini`)，這些組態檔位於主目錄中。它們也會設定為使用驅動程式安裝目錄的 `/lib` 子資料夾中的 `amazon.redshiftodbc.ini` 檔案。如果您將這些組態檔儲存在其他位置，請設定環境變數，以便驅動程式管理員可以找到這些檔案。如需詳細資訊，請參閱《Amazon Redshift ODBC 連接器安裝和組態指南》中的「指定驅動程式組態檔案的位置」。

設定連線功能

您可以將下列連線功能設定給 ODBC 設定：

- 設定 ODBC 驅動程式以提供憑證，並驗證 Amazon Redshift 資料庫的連線。
- 設定 ODBC 驅動程式，以連線到啟用 Secure Sockets Layer (SSL) 的通訊端 (如果您連線到已啟用 SSL 的 Amazon Redshift 伺服器)。
- 設定 ODBC 驅動程式，以透過 Proxy 伺服器連線到 Amazon Redshift。
- 將 ODBC 驅動程式設定為使用查詢處理模式，以防止查詢耗用太多記憶體。
- 設定 ODBC 驅動程式，以透過代理伺服器傳遞 IAM 身分驗證程序。
- 設定 ODBC 驅動程式，以使用 TCP 保持連線來防止連線逾時。

如需這些連線功能的相關資訊，請參閱 [Amazon Redshift ODBC 連接器安裝和組態指南](#)。

設定 ODBC 驅動程式選項

您可以使用組態選項來控制 Amazon Redshift ODBC 驅動程式的行為。

在 Microsoft Windows 中，您通常於設定資料來源名稱 (DSN) 時設定驅動程式選項。您也可以在連接時以程式設計方式在連線字串中設定驅動程式選項，或在 HKEY_LOCAL_MACHINE\SOFTWARE\ODBC\ODBC.INI*your_DSN* 中新增或變更登錄機碼。如需設定 DSN 的相關資訊，請參閱 [在 Microsoft Windows 上安裝並設定 Amazon Redshift ODBC 驅動程式](#)。

在 Linux 和 macOS X 中，您可以在 `odbc.ini` 和 `amazon.redshiftdbc.ini` 檔案中設定驅動程式組態選項，如 [使用 ODBC 驅動程式管理員來設定 Linux 和 macOS X 作業系統上的驅動程式](#) 中所述。在 `amazon.redshiftdbc.ini` 檔案中設定的組態選項會套用至所有連線。相反地，`odbc.ini` 檔案中設定的組態選項是針對某個連線。`odbc.ini` 中設定的組態選項優先於 `amazon.redshiftdbc.ini` 中設定的組態選項。

如需如何設定 ODBC 驅動程式組態選項的相關資訊，請參閱 [Amazon Redshift ODBC 連接器安裝和組態指南](#)。

先前的 ODBC 驅動程式版本

只有在您的工具需要特定版本的驅動程式時，才需要下載舊版的 Amazon Redshift ODBC 驅動程式。

使用先前的 ODBC 驅動程式版本 (適用於 Windows)

以下是 64 位元驅動程式：

- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.5.7.1007/> AmazonRedshift 在中國地區，請使用以下
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.65.1000/> AmazonRedshift 在中國地區，請使用以下
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.62.1000/> AmazonRedshift 在中國地區，請使用以下
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.59.1000/> AmazonRedshift 在中國地區，請使用以下
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.56.1000/> AmazonRedshift 在中國地區，請使用以下
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.53.1000/> AmazonRedshift 在中國地區，請使用以下
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.52.1000/> AmazonRedshift 在中國地區，請使用以下

32 位元的驅動程式已停止使用，先前的版本已不受支援。

使用先前的 ODBC 驅動程式版本 (適用於 Linux)

以下是 64 位元驅動程式版本：

- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.5.7.1007/> AmazonRedshift 在中國地區，請使用以下連結。AWS
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.65.1000/> AmazonRedshift 在中國地區，請使用以下連結<https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/drivers/odbc/1.4.65.1000/> 64 位 AmazonRedshift 元轉
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.62.1000/> AmazonRedshift 在中國地區，請使用以下連結
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.59.1000/> AmazonRedshift 在中國地區，請使用以下連結
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.59.1000/> AmazonRedshift 在中國地區，請使用以下連結<https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/drivers/odbc/1.4.59.1000/> AmazonRedshift 奧德布 -64 位元 -1.4.59.1000-1.x86_64.deb
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.56.1000/> AmazonRedshift 在中國地區，請使用下列連結

- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.56.1000/> AmazonRedshift 在中國地區，請使用下列連結<https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/drivers/odbc/1.4.56.1000/> AmazonRedshift 奧德布 -64 位元 -1.4.56.1000-1.x86_64.deb
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.52.1000/> AmazonRedshift 在中國地區，請使用以下連結
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.52.1000/> AmazonRedshift 在中國地區，請使用以下連結<https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/drivers/odbc/1.4.52.1000/> AmazonRedshift 奧德布 -64 位元 -1.4.52.1000-1.x86_64.deb

32 位元的驅動程式已停止使用，先前的版本已不受支援。

使用先前的 ODBC 驅動程式版本 (適用於 macOS X)

以下是適用於 macOS X 的 Amazon Redshift ODBC 驅動程式版本：

- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.5.7.1007/> AmazonRedshift 在中國地區，請使用以下鏈接。AWS
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.65.1000/> AmazonRedshift 在中國地區，使用以下鏈接
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.62.1000/> AmazonRedshift 在中國地區，使用以下鏈接
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.59.1000/> AmazonRedshift 在中國地區，使用以下鏈接
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.56.1000/> AmazonRedshift 在中國地區，使用以下鏈接
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.52.1000/> AmazonRedshift 在中國地區，使用以下鏈接

設定連線的安全選項

Amazon Redshift 支援 Secure Sockets Layer (SSL) 連線，可將資料和伺服器憑證加密，以驗證用戶端所連線的伺服器憑證。

使用 SSL 連線

為了支援 SSL 連線，Amazon Redshift 會在每一個叢集上建立並安裝 [AWS Certificate Manager \(ACM\)](#) 發行的 SSL 憑證。ACM 憑證受到大多數作業系統、網頁瀏覽器和用戶端公開信任。如果

SQL 用戶端或應用程式在 `sslmode` 連線選項設為 `require`、`verify-ca` 或 `verify-full` 的情況下，使用 SSL 連線到 Amazon Redshift，您可能需要下載憑證套件。如果用戶端需要憑證，Amazon Redshift 會提供如下的憑證套件：

- 從 <https://s3.amazonaws.com/redshift-downloads/amazon-trust-ca-bundle.crt> 下載套件。
 - 預期的 MD5 檢查總和碼為 418dea9b6d5d5de7a8f1ac42e164cdcf。
 - sha256 檢查總和碼為
36dba8e4b8041cd14b9d60158893963301bcbb92e1c456847784de2acb5bd550。

請勿使用位於 `https://s3.amazonaws.com/redshift-downloads/redshift-ca-bundle.crt` 的先前憑證套件。

- 在中國 AWS 區域，請從以下位置下載此套件：<https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/amazon-trust-ca-bundle.crt>。
 - 預期的 MD5 檢查總和碼為 418dea9b6d5d5de7a8f1ac42e164cdcf。
 - sha256 檢查總和碼為
36dba8e4b8041cd14b9d60158893963301bcbb92e1c456847784de2acb5bd550。

請勿使用位於 `https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/redshift-ca-bundle.crt` 和 `https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/redshift-ssl-ca-cert.pem` 的先前憑證套件。

Important

Amazon Redshift 已變更 SSL 憑證的管理方式。您可能需要更新目前的信任根 CA 憑證，才能繼續使用 SSL 連線到叢集。如需詳細資訊，請參閱 [將 SSL 連線轉換為使用 ACM 憑證](#)。

根據預設，不論連線是否使用 SSL，叢集資料庫都接受連線。若要將叢集設為需要 SSL 連線，請在與叢集相關聯的參數群組中，將 `require_ssl` 參數設為 `true`。

Amazon Redshift 支援符合美國聯邦資訊處理標準 (FIPS) 140-2 的 SSL 模式。符合 FIPS 的 SSL 模式預設為停用。

Important

只在系統需要符合 FIPS 時啟用與 FIPS 相容的 SSL 模式。

若要啟用 FIPS 相容的 SSL 模式，請 `true` 在與 Amazon Redshift 叢集或 Redshift 無伺服器工作群組關聯的參數群組中將參數和參數設定為 `use_fips_ssl require_ssl`。如需有關修改叢集上參數群組的資訊，請參閱 [Amazon Redshift 參數群組](#)。若要取得有關在工作群組上修改參數群組的資訊，請參閱 [設定與 Amazon Redshift 無伺服器的 FIPS 相容 SSL 連線](#)。

Amazon Redshift 支援 Elliptic Curve Diffie—Hellman Ephemeral (ECDHE) 金鑰協議通訊協定。使用 ECDHE 時，用戶端和伺服器各有橢圓曲線公有-私有金鑰對，用於透過不安全通道建立共用秘密。您不需要在 Amazon Redshift 中設定任何項目來啟用 ECDHE。如果您從 SQL 用戶端工具連線，而此工具使用 ECDHE 來加密用戶端和伺服器之間的通訊，Amazon Redshift 會使用提供的密碼清單來建立適當的連線。如需詳細資訊，請參閱 Wikipedia 上的 [Elliptic curve diffie—hellman](#) 和 OpenSSL 網站上的 [Ciphers](#)。

在 ODBC 中使用 SSL 和信任 CA 憑證

如果您使用最新的 Amazon Redshift ODBC 驅動程式 (1.3.7.1000 版或更新版本) 來連接，則可略過本節。若要下載最新的驅動程式，請參閱 [設定 ODBC 連線](#)。

您可能需要更新目前的信任根 CA 憑證，才能繼續使用 SSL 連線到叢集。如需詳細資訊，請參閱 [使用 SSL 連線](#)。

您可以驗證您下載的憑證是否符合預期的 MD5 檢查總和碼。若要執行此動作，您可以在 Linux 作業系統上使用 `Md5sum` 程式，或在 Windows 和 macOS X 作業系統上使用其他工具。

ODBC DSN 包含 `sslmode` 設定，可決定如何處理用戶端連線和伺服器憑證驗證的加密。Amazon Redshift 支援來自用戶端連線的下列 `sslmode` 值：

- `disable`

停用 SSL，不加密連線。

- `allow`

如果伺服器需要，就使用 SSL。

- `prefer`

如果伺服器支援，就使用 SSL。Amazon Redshift 支援 SSL，因此當您將 `sslmode` 設定為 `prefer` 時，系統會使用 SSL。

- `require`

需要 SSL。

- `verify-ca`

必須使用 SSL 且必須驗證伺服器憑證。

- `verify-full`

必須使用 SSL。必須驗證伺服器憑證，且伺服器主機名稱必須符合憑證上的主機名稱屬性。

您可以判斷用戶端和伺服器之間的連線是否使用 SSL 及是否驗證伺服器憑證。若要執行此作業，您需要在用戶端檢閱 ODBC DSN 的 `sslmode` 設定，並在伺服器上檢閱 Amazon Redshift 叢集的 `require_SSL` 設定。下表描述各種用戶端和伺服器設定組合的加密結果：

sslmode (用戶端)	require_SSL (伺服器)	結果
<code>disable</code>	<code>false</code>	不加密連線。
<code>disable</code>	<code>true</code>	無法建立連線，因為伺服器需要 SSL，但用戶端對連線停用 SSL。
<code>allow</code>	<code>true</code>	加密連線。
<code>allow</code>	<code>false</code>	不加密連線。
<code>prefer</code> 或 <code>require</code>	<code>true</code>	加密連線。
<code>prefer</code> 或 <code>require</code>	<code>false</code>	加密連線。
<code>verify-ca</code>	<code>true</code>	加密連線且驗證伺服器憑證。
<code>verify-ca</code>	<code>false</code>	加密連線且驗證伺服器憑證。
<code>verify-full</code>	<code>true</code>	加密連線且驗證伺服器憑證，並驗證主機名稱。
<code>verify-full</code>	<code>false</code>	加密連線且驗證伺服器憑證，並驗證主機名稱。

在 Microsoft Windows 上搭配 ODBC 使用伺服器憑證進行連線

如果您想要使用 SSL 和伺服器憑證連線到叢集，請先將憑證下載到用戶端電腦或 Amazon EC2 執行個體。然後，設定 ODBC DSN。

1. 將 Amazon Redshift 憑證授權機構套件下載到用戶端電腦驅動程式安裝目錄中的 lib 資料夾，並將檔案儲存為 root.crt。如需下載資訊，請參閱 [使用 SSL 連線](#)。
2. 開啟 ODBC 資料來源管理員，然後新增或編輯 ODBC 連線的系統 DSN 項目。在 SSL 模式中，選取 verify-full (除非您使用 DNS 別名)。如果您使用 DNS 別名，請選取 verify-ca。然後選擇 Save (儲存)。

如需設定 ODBC DSN 的相關資訊，請參閱 [設定 ODBC 連線](#)。

在 Java 中使用 SSL 和伺服器憑證

SSL 會將用戶端和伺服器之間移動的資料加密，多一道安全性。使用伺服器憑證可透過驗證叢集是否為 Amazon Redshift 叢集來提供額外一層的安全。在作法上是檢查您佈建的所有叢集上自動安裝的伺服器憑證。如需搭配 JDBC 使用伺服器憑證的相關資訊，請前往 PostgreSQL 文件中的 [Configuring the client](#)。

在 Java 中使用信任 CA 憑證進行連線

Important

Amazon Redshift 已變更 SSL 憑證的管理方式。您可能需要更新目前的信任根 CA 憑證，才能繼續使用 SSL 連線到叢集。如需詳細資訊，請參閱 [使用 SSL 連線](#)。

使用信任 CA 憑證來連接

您可以使用該 redshift-keytool.jar 檔案將 Amazon Redshift 憑證授權單位服務包中的 CA 憑證匯入 Java TrustStore 或您的私 TrustStore 有憑證。

1. 如果您使用 Java 命令列 -Djavax.net.ssl.trustStore 選項，可能的話，請從命令列中移除。
2. 下載 [redshift-keytool.jar](#)。
3. 執行以下任意一項：
 - 若要將 Amazon Redshift 憑證授權單位服務包匯入 Java TrustStore，請執行下列命令。

```
java -jar redshift-keytool.jar -s
```

- 若要將 Amazon Redshift 憑證授權單位服務包匯入您的私有伺服器 TrustStore，請執行下列命令：

```
java -jar redshift-keytool.jar -k <your_private_trust_store> -  
p <keystore_password>
```

將 SSL 連線轉換為使用 ACM 憑證

Amazon Redshift 將會以 [AWS Certificate Manager \(ACM\)](#) 發行的憑證取代您叢集上的 SSL 憑證。ACM 是大多數現行系統信任的公有憑證授權機構 (CA)。您可能需要更新目前的信任根 CA 憑證，才能繼續使用 SSL 連線到叢集。

只有在下列所有情況都存在時，此變更才會影響您：

- SQL 用戶端或應用程式使用 SSL 來連接至 Amazon Redshift 叢集，且 `sslMode` 連線選項設為 `require`、`verify-ca` 或 `verify-full` 組態選項。
- 您不使用 Amazon Redshift ODBC 或 JDBC 驅動程式，或使用的 Amazon Redshift 驅動程式是 ODBC 1.3.7.1000 版或 JDBC 1.2.8.1005 版以前。

如果此變更會在 Amazon Redshift 商業區域影響到您，則您必須在 2017 年 10 月 23 日之前更新目前的信任根 CA 憑證。Amazon Redshift 會從現在開始到 2017 年 10 月 23 日之前，將您的叢集轉換為使用 ACM 憑證。此變更對叢集效能或可用性的影響應該非常小，或完全不影響。

如果此變更在 AWS GovCloud (US) (美國) 區域影響您，則您必須在 2020 年 4 月 1 日之前更新目前的信任根 CA 憑證，以避免服務中斷。從這個日期起，使用 SSL 加密連線連線至 Amazon Redshift 叢集的用戶端需要額外的受信任憑證授權單位 (CA)。用戶端在連線到 Amazon Redshift 叢集時，會使用受信任的憑證授權單位來確認該叢集的身分。您必須採取動作，才能更新 SQL 用戶端和應用程式，以使用包含新信任 CA 的更新憑證套件。

Important

在 2021 年 1 月 5 日的中國區域，Amazon Redshift 將以 AWS Certificate Manager (ACM) 核發的憑證取代叢集上的 SSL 憑證。如果此變更會在中國 (北京) 區域或中國 (寧夏) 區域影響到您，則您必須在 2021 年 1 月 5 日之前更新目前的信任根 CA 憑證，以避免服務中斷。從這個日期起，使用 SSL 加密連線連線至 Amazon Redshift 叢集的用戶端需要額外的受信任憑證授

權單位 (CA)。用戶端在連線到 Amazon Redshift 叢集時，會使用受信任的憑證授權單位來確認該叢集的身分。您必須採取動作，才能更新 SQL 用戶端和應用程式，以使用包含新信任 CA 的更新憑證套件。

- [使用最新的 Amazon Redshift ODBC 或 JDBC 驅動程式](#)
- [使用較舊的 Amazon Redshift ODBC 或 JDBC 驅動程式](#)
- [使用其他 SSL 連線類型](#)

使用最新的 Amazon Redshift ODBC 或 JDBC 驅動程式

建議使用最新的 Amazon Redshift ODBC 或 JDBC 驅動程式。從 ODBC 1.3.7.1000 版和 JDBC 1.2.8.1005 版開始的 Amazon Redshift 驅動程式，將會自動處理從 Amazon Redshift 自簽憑證轉換到 ACM 憑證。若要下載最新的驅動程式，請參閱[設定 ODBC 連線](#)或[設定 Amazon Redshift JDBC 驅動程式 2.1 版的連線](#)。

如果您使用最新的 Amazon Redshift JDBC 驅動程式，最好不要在 JVM 選項中使用 `-Djavax.net.ssl.trustStore`。如果您必須使用 `-Djavax.net.ssl.trustStore`，請將 Redshift 憑證授權機構套件匯入其指向的信任憑證庫。如需下載資訊，請參閱[使用 SSL 連線](#)。如需詳細資訊，請參閱[將 Amazon Redshift 證書授權單位服務包導入 TrustStore](#)。

使用較舊的 Amazon Redshift ODBC 或 JDBC 驅動程式

- 如果 ODBC DSN 設定為 `SSLCertPath`，請覆寫指定路徑中的憑證檔案。
- 如果未設定 `SSLCertPath`，請覆寫驅動程式 DLL 位置中名為 `root.crt` 的憑證檔案。

如果您必須使用的 1.2.8.1005 版以前的 Amazon Redshift JDBC 驅動程式，請執行下列其中一個動作：

- 如果 JDBC 連線字串使用 `sslCert` 選項，請移除 `sslCert` 選項。然後將 Redshift 憑證授權單位套件匯入您的 Java TrustStore。如需下載資訊，請參閱[使用 SSL 連線](#)。如需詳細資訊，請參閱[將 Amazon Redshift 證書授權單位服務包導入 TrustStore](#)。
- 如果您使用 Java 命令列 `-Djavax.net.ssl.trustStore` 選項，可能的話，請從命令列中移除。然後將 Redshift 憑證授權單位套件匯入您的 Java TrustStore。如需下載資訊，請參閱[使用 SSL 連線](#)。如需詳細資訊，請參閱[將 Amazon Redshift 證書授權單位服務包導入 TrustStore](#)。

將 Amazon Redshift 證書授權單位服務包導入 TrustStore

您可以使用 `redshift-keytool.jar` 將 Amazon Redshift 憑證授權單位服務包中的 CA 憑證匯入 Java TrustStore 或您的私有信任存放區。

若要將 Amazon Redshift 憑證授權單位服務包匯入 TrustStore

1. 下載 [redshift-keytool.jar](#)。
2. 執行以下任意一項：
 - 若要將 Amazon Redshift 憑證授權單位服務包匯入 Java TrustStore，請執行下列命令。

```
java -jar redshift-keytool.jar -s
```

- 若要將 Amazon Redshift 憑證授權單位服務包匯入您的私有伺服器 TrustStore，請執行下列命令：

```
java -jar redshift-keytool.jar -k <your_private_trust_store> -  
p <keystore_password>
```

使用其他 SSL 連線類型

如果您使用下列任何一項來連接，請遵循本節的步驟：

- 開放原始碼 ODBC 驅動程式
- 開放原始碼 JDBC 驅動程式
- [Amazon Redshift RSQL](#) 命令列界面
- 任何以 `libpq` 為基礎的語言繫結，例如 `psycopg2` (Python) 和 `ruby-pg` (Ruby)

若要對其他 SSL 連線類型使用 ACM 憑證，請執行下列動作：

1. 下載 Amazon Redshift 憑證授權機構套件。如需下載資訊，請參閱 [使用 SSL 連線](#)。
2. 將套件中的憑證放入 `root.crt` 檔案中。
 - 在 Linux 和 macOS X 作業系統上，此檔案是 `~/.postgresql/root.crt`。
 - 在 Microsoft Windows 上，此檔案是 `%APPDATA%\postgresql\root.crt`。

從用戶端工具和程式碼連線

Amazon Redshift 提供了 Amazon Redshift 查詢編輯器 v2 供您連線到叢集和工作群組。如需詳細資訊，請參閱 [使用 Amazon Redshift 查詢編輯器 v2 來查詢資料庫](#)。

本節提供一些可供第三方工具進行連線的選項。此外，還描述如何以程式設計方式連接至叢集。

主題

- [使用 Amazon Redshift RSQL 進行連線](#)
- [使用 Amazon Redshift RSQL 連線至叢集](#)
- [Amazon Redshift RSQL 中繼命令](#)
- [Amazon Redshift RSQL 變數](#)
- [Amazon Redshift RSQL 錯誤代碼](#)
- [Amazon Redshift RSQL 環境變數](#)

使用 Amazon Redshift RSQL 進行連線

Amazon Redshift RSQL 是用於與 Amazon Redshift 叢集和資料庫互動的命令列用戶端。您可以連線到 Amazon Redshift 叢集、描述資料庫物件、查詢資料，以及檢視各種輸出格式的查詢結果。

Amazon Redshift RSQL 支援 PostgreSQL psql 命令列工具的功能，以及一組專屬於 Amazon Redshift 的額外功能。這些索引標籤包括以下項目：

- 您可以使用 ADFS、Okta、PingIdentity Azure ADM 或其他以 SAML/JWT 為基礎的身分識別提供者來使用單一登入驗證。您也可以使用以瀏覽器為基礎的 SAML 身分供應商來進行多重要素驗證 (MFA)。
- 您可以描述 Amazon Redshift 物件的屬性，例如資料表分佈索引鍵、資料表排序索引鍵、晚期繫結視觀表 (LBV) 和具體化視觀表。您也可以針對 AWS Glue 目錄或 Apache Hive 中繼存放區中的外部資料表、Amazon RDS for PostgreSQL 中的外部資料庫、Amazon Aurora PostgreSQL-Compatible Edition、RDS for MySQL (預覽) 和 Amazon Aurora MySQL-Compatible Edition (預覽)，以及使用 Amazon Redshift 資料共用所共用的資料表，來描述其屬性。
- 您也可以使用增強的控制流程命令，例如 IF (\ELSEIF、\ELSE、\ENDIF)、\GOTO 和 \LABEL。

透過 Amazon Redshift RSQL 批次模式 (該模式會執行以輸入參數形式傳遞的指令碼)，您可以執行同時包含 SQL 和複雜商業邏輯的指令碼。如果您有現有的自我管理內部部署資料倉儲，則可以使用

Amazon Redshift RSQL 取代現有的擷取、轉換、載入 (ETL) 和自動化指令碼，例如 Teradata BTEQ 指令碼。使用 RSQL 可以幫助您避免在程序語言中手動重新實作指令碼。

Amazon Redshift RSQL 適用於 Linux、Windows 和 macOS X 作業系統。

若要報告 Amazon Redshift RSQL 的問題，請寫信至 <redshift-rsql-support@amazon.com>。

主題

- [開始使用 Amazon Redshift RSQL](#)
- [Amazon Redshift RSQL 變更日誌](#)

開始使用 Amazon Redshift RSQL

在搭載 Linux、macOS 或 Microsoft Windows 作業系統的電腦上安裝 Amazon Redshift RSQL。

下載 RSQL

- Linux 64 位元 RPM : [RSQL 1.0.8 版](#)
- Mac OS 64 位元 DMG : [RSQL 1.0.8 版](#)
- Windows 64 位元 MSI : [RSQL 1.0.8 版](#)

若要查看舊版的變更日誌和下載，請瀏覽 [Amazon Redshift RSQL 變更日誌](#)。

安裝適用於 Linux 的 RSQL

請遵循下列步驟以安裝適用於 Linux 的 RSQL。

1. 使用以下命令安裝驅動程式管理員：

```
sudo yum install unixODBC openssl
```

Linux 發行版本需要 OpenSSL。OpenSSL 程式庫位於 [Linux OpenSSL Github 儲存庫](#)。如需 OpenSSL 的相關資訊，請參閱 [OpenSSL](#)。

2. 安裝 ODBC 驅動程式：[在 Linux 作業系統上安裝 Amazon Redshift 驅動程式](#)。
3. 將 ini 檔案複製到主目錄：

```
cp /opt/amazon/redshiftodbc/Setup/odbc.ini ~/.odbc.ini
```

4. 將環境變數設定為指向檔案的位置：


```
export ODBCINI=~/.odbc.ini
export OBCSYSINI=/opt/amazon/redshiftodbc/Setup
export AMAZONREDSHIFTODBCINI=/opt/amazon/redshiftodbc/lib/64/
amazon.redshiftodbc.ini
```

如需設定 ODBC 環境變數的相關資訊，請參閱 [設定環境變數](#)。

5. 您現在可以執行下列命令來安裝 RSQL。

```
sudo rpm -i AmazonRedshiftRsql-<version>-1.x86_64.rpm
```

安裝適用於 Mac 的 RSQL

請遵循下列步驟以安裝適用於 Mac OSX 的 RQL。

1. 使用以下命令安裝驅動程式管理員：

```
brew install unixodbc openssl@1.1 --build-from-source
```

2. 安裝 ODBC 驅動程式：[在 macOS X 上安裝 Amazon Redshift ODBC 驅動程式](#)。
3. 將 ini 檔案複製到主目錄：

```
cp /opt/amazon/redshift/Setup/odbc.ini ~/.odbc.ini
```

4. 將環境變數設定為指向檔案的位置：

```
export ODBCINI=~/.odbc.ini
export OBCSYSINI=/opt/amazon/redshift/Setup
export AMAZONREDSHIFTODBCINI=/opt/amazon/redshift/lib/amazon.redshiftodbc.ini
```

如需設定 ODBC 環境變數的相關資訊，請參閱 [設定環境變數](#)。

5. 將 DYLD_LIBRARY_PATH 設定為 libodbc.dylib 的位置 (如果它不在 /usr/local/lib 的話)。

```
export DYLD_LIBRARY_PATH=$DYLD_LIBRARY_PATH:/usr/local/lib
```

6. 按兩下 dmg 檔案以掛載磁碟映像。
7. 按兩下 pkg 檔案來執行安裝程式。
8. 依照安裝程式中的步驟完成安裝。同意授權合約中的條款。

安裝適用於 Windows 的 RSQL

請遵循 [在 Microsoft Windows 上安裝並設定 Amazon Redshift ODBC 驅動程式](#) 上的指示來安裝驅動程式。Windows 不需要驅動程式管理員。

Windows 上的 Amazon Redshift RSQL 需要 OpenSSL。視窗 OpenSSL 程式庫位於 [視窗 OpenSSL GitHub 儲存庫](#) 中。如需 OpenSSL 的相關資訊，請參閱 [OpenSSL](#)。

按兩下 RSQL 下載檔案以執行安裝程式，然後遵循提示以完成安裝。

Amazon Redshift RSQL 變更日誌

1.0.8 (2023-06-19)

錯誤修正

- 修正了使用 SHOW 命令會截斷輸出的問題。
- 已新增對用於描述外部 Kinesis 串流和 Kafka 主題之 \de 的支援。

1.0.7 (2023-03-22)

錯誤修正

- 修正了 RSQL 無法描述具體化視觀表的問題。
- 修正了使用 Amazon Redshift Serverless 時，stl_connection_log 上的許可遭拒錯誤。
- 修正了 RSQL 可能無法正確處理 \GOTO 標籤的問題。
- 修正了 SSL 訊息會以靜音模式列印的問題。
- 修正了描述預存程序時會顯示隨機字元的問題。
- 修正了會列印重複 ERROR/INFO 訊息的問題。

新增

- RSQL 現在會直接從 ODBC 驅動程式取得 SSL 資訊。

1.0.6 (2023-02-21)

錯誤修正

- 在 Redshift 修補程式 1.0.46086 (P173) 上修正了 \d 會擲出錯誤 (整數的輸入語法無效: "xid") 的問題。

新增

- 已重新命名安裝檔案以反映支援的架構。

1.0.5 (2022-06-27)

錯誤修正

- 將 SQL 錯誤訊息傳送到標準錯誤 (stderr)。
- 修正了使用 ON_ERROR_STOP 時結束代碼所發生的問題。指令碼現在會在遇到錯誤後結束，並返回正確的結束代碼。
- Maxerror 現在不區分大小寫。

新增

- 已新增對 ODBC 2.x 驅動程式的支援。

1.0.4 (2022-03-19)

- 新增對 RSPASSWORD 環境變數的支援。設定密碼以連線到 Amazon Redshift。例如 export RSPASSWORD=TestPassw0rd。

1.0.3 (2021-12-08)

錯誤修正

- 修正了在 Windows 作業系統中使用 \c 或 \logon 在資料庫之間進行切換時的快顯對話方塊。
- 修正了檢查 ssl 資訊時的損毀問題。

Amazon Redshift RSQL 的先前版本

請根據您的作業系統選擇其中一個連結，以下載您需要的 Amazon Redshift RSQL 版本。

Linux 64 位元 RPM

- [RSQL 1.0.7 版](#)
- [RSQL 1.0.6 版](#)
- [RSQL 1.0.5 版](#)
- [RSQL 1.0.4 版](#)
- [RSQL 1.0.3 版](#)
- [RSQL 1.0.1 版](#)

Mac OS 64 位元 DMG

- [RSQL 1.0.7 版](#)
- [RSQL 1.0.6 版](#)
- [RSQL 1.0.5 版](#)
- [RSQL 1.0.4 版](#)
- [RSQL 1.0.3 版](#)
- [RSQL 1.0.1 版](#)

Windows 64 位元 MSI

- [RSQL 1.0.7 版](#)
- [RSQL 1.0.6 版](#)
- [RSQL 1.0.5 版](#)
- [RSQL 1.0.4 版](#)
- [RSQL 1.0.3 版](#)
- [RSQL 1.0.1 版](#)

使用 Amazon Redshift RSQL 連線至叢集

在不使用 DSN 的情況下進行連線

1. 在 Amazon Redshift 主控台上，選擇要連線到的叢集，並記下端點、資料庫和連接埠。
2. 在命令提示字元中，使用命令列參數指定連線資訊。

```
rsql -h <endpoint> -U <username> -d <databasename> -p <port>
```

這裡會套用下列項目：

- *<endpoint>* 是您在前一步驟中記錄的 Endpoint (端點)。
- *<username>* 是有許可而可以連線至叢集的使用者名稱。
- *<databasename>* 是您在前一步驟中記錄的 Database Name (資料庫名稱)。
- *<port>* 是您在上一個步驟中記錄的連接埠。*<port>* 是選用參數。

範例如下。

```
rsql -h testcluster.example.amazonaws.com -U user1 -d dev -p 5439
```

3. 在密碼提示中，輸入 *<username>* 使用者的密碼。

成功連線的回應看起來如下。

```
% rsql -h testcluster.example.com -d dev -U user1 -p 5349
Password for user user1:
DSN-less Connected
DBMS Name: Amazon Redshift
Driver Name: Amazon Redshift ODBC Driver
Driver Version: 1.4.27.1000
Rsql Version: 1.0.1
Redshift Version: 1.0.29306
Type "help" for help.

(testcluster) user1@dev=#
```

用來連線的命令在 Linux、Mac OS 和 Windows 上具有相同的參數。

使用 DSN 進行連線

您可以使用資料來源名稱 (DSN) 將 RSQL 連線到 Amazon Redshift，以簡化連線屬性的組織工作。如需詳細資訊，請參閱 [設定連線功能](#)。本主題包含 ODBC 驅動程式安裝的指示，以及 DSN 屬性的描述。例如，下一節在 [Microsoft Windows 上安裝和設定 Amazon Redshift ODBC 驅動程式](#) 會示範如何在 Windows 上使用 DSN 進行連線。

使用具有密碼的 DSN 連線

以下示範使用密碼的 DSN 連線組態範例。Mac OSX 的預設 <path to driver> 是 /opt/amazon/redshift/lib/libamazonredshiftodbc.dylib，Linux 的則是 /opt/amazon/redshiftodbc/lib/64/libamazonredshiftodbc64.so。

```
[testuser]
Driver=/opt/amazon/redshiftodbc/lib/64/libamazonredshiftodbc64.so
SSLMode=verify-ca
Min_TLS=1.2
boolsaschar=0
Host=<server endpoint>
Port=<database port>
Database=<dbname>
UID=<username>
PWD=<password>
sslmode=prefer
```

以下輸出來自成功的連線。

```
% rsql -D testuser
DSN Connected
DBMS Name: Amazon Redshift
Driver Name: Amazon Redshift ODBC Driver
Driver Version: 1.4.27.1000
Rsql Version: 1.0.1
Redshift Version: 1.0.29306
Type "help" for help.

(testcluster) user1@dev=#
```

使用單一登入 DSN

您可以設定 DSN 以進行單一登入身分驗證。以下示範使用 Okta 單一登入的 DSN 連線組態範例。

```
[testokta]
Driver=<path to driver>
SSLMode=verify-ca
Min_TLS=1.2
boolsaschar=0
Host=<server endpoint>
clusterid=<cluster id>
```

```

region=<region name>
Database=<dbname>
locale=en-US
iam=1
plugin_name=<plugin name>
uid=<okta username>
pwd=<okta password>
idp_host=<idp endpoint>
app_id=<app id>
app_name=<app name>
preferred_role=<role arn>

```

成功連線的範例輸出。

```

% rsql -D testokta
DSN Connected
DBMS Name: Amazon Redshift
Driver Name: Amazon Redshift ODBC Driver
Driver Version: 1.4.27.1000
Rsql Version: 1.0.1
Redshift Version: 1.0.29306
Type "help" for help.

(testcluster) user1@dev=#

```

以下範例示範使用 Azure 單一登入的 DSN 連線組態範例。

```

[testazure]
Driver=<path to driver>
SSLMode=verify-ca
Min_TLS=1.2
boolsaschar=0
Host=<server endpoint>
Port=<cluster port>
clusterid=<cluster id>
region=<region name>
Database=<dbname>
locale=en-us
iam=1
plugin_name=<plugin name>
uid=<azure username>
pwd=<azure password>
idp_tenant=<Azure idp tenant uuid>

```

```
client_id=<Azure idp client uuid>
client_secret=<Azure idp client secret>
```

搭配 IAM 設定檔使用 DSN 連線

您可以使用所設定的 IAM 設定檔連線到 Amazon Redshift。IAM 設定檔必須具有呼叫 `GetClusterCredentials` 的權限。以下範例示範要使用的 DSN 屬性。只有在 Host 不是 Amazon 提供的端點 (例如 `examplecluster.abc123xyz789.us-west-2.redshift.amazonaws.com`) 時，才需要 `ClusterID` 和 `Region` 參數。

```
[testiam]
Driver=Default
Host=testcluster.example.com
Database=dev
DbUser=testuser
ClusterID=rsqltestcluster
Region=us-east-1
IAM=1
Profile=default
```

`Profile` 金鑰的值是您從 AWS CLI 認證中選擇的具名設定檔。本範例示範名為 `default` 之設定檔的憑證。

```
$ cat .aws/credentials
[default]
aws_access_key_id = ASIAIOSFODNN7EXAMPLE
aws_secret_access_key = wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY
```

以下示範連線回應。

```
$ rsql -D testiam
DSN Connected
DBMS Name: Amazon Redshift
Driver Name: Amazon Redshift ODBC Driver
Driver Version: 1.4.27.1000
Rsql Version: 1.0.1
Redshift Version: 1.0.29306
Type "help" for help.

(testcluster) testuser@dev=>
```


搭配執行個體設定檔使用 DSN 連線

您可以使用 Amazon EC2 執行個體設定檔連線到 Amazon Redshift。執行個體設定檔必須具有呼叫 `GetClusterCredentials` 的權限。如需要使用的 DSN 屬性，請參閱以下範例。只有在 Host 不是 Amazon 提供的端點 (例如 `examplecluster.abc123xyz789.us-west-2.redshift.amazonaws.com`) 時，才需要 `ClusterID` 和 `Region` 參數。

```
[testinstanceprofile]
Driver=Default
Host=testcluster.example.com
Database=dev
DbUser=testuser
ClusterID=rsqltestcluster
Region=us-east-1
IAM=1
Instanceprofile=1
```

以下示範連線回應。

```
$ rsql -D testinstanceprofile
DSN Connected
DBMS Name: Amazon Redshift
Driver Name: Amazon Redshift ODBC Driver
Driver Version: 1.4.27.1000
Rsql Version: 1.0.1
Redshift Version: 1.0.29306
Type "help" for help.

(testcluster) testuser@dev=>
```

搭配使用 DSN 連線與預設憑證提供者鏈結

若要使用預設登入資料提供者鏈結進行連線，請僅指定 IAM 屬性，Amazon Redshift RSQL 就會嘗試依照使用 AWS SDK for Java 中的登入資料中所述的[順序取得 AWS 登入資料](#)。鏈結中至少要有一個提供者必須具有 `GetClusterCredentials` 許可。這對於從 ECS 容器進行連線 (舉例來說) 非常有用。

```
[iamcredentials]
Driver=Default
Host=testcluster.example.com
Database=dev
DbUser=testuser
```

```
ClusterID=rsqltestcluster
Region=us-east-1
IAM=1
```

Amazon Redshift RSQL 中繼命令

Amazon Redshift RSQL 中繼命令會傳回有關資料庫或特定資料庫物件的資訊記錄。結果中可以包含各種資料行和中繼資料。其他命令會執行特定動作。這些命令的前面會加上反斜線。

`\d[S+]`

列出本機使用者建立的資料表、一般視觀表、晚期繫結視觀表及具體化視觀表。`\dS` 也會列出資料表和視觀表 (例如 `\d`)，但系統物件包含在傳回的記錄中。`+` 會導致所有列出的物件產生額外的中繼資料資料行 `description`。以下示範執行命令所傳回的範例記錄。

```
List of relations
 schema |   name   | type | owner
-----+-----+-----+-----
 public | category | table | awsuser
 public | date     | table | awsuser
 public | event    | table | awsuser
 public | listing  | table | awsuser
 public | sales    | table | awsuser
 public | users    | table | awsuser
 public | venue    | table | awsuser
(7 rows)
```

`\d[S+] NAME`

描述資料表、視觀表或索引。包括資料行名稱和類型。其還會提供 `diststyle`、備份組態、建立日期 (2018 年 10 月之後建立的資料表) 和限制。例如，`\dS+ sample` 會傳回物件屬性。附加 `S+` 會導致所傳回的記錄中包含額外資料行。

```
Table "public.sample"
 Column |          Type          | Collation  | Nullable | Default Value |
 Encoding | DistKey | SortKey
-----+-----+-----+-----+-----
+-----+-----+-----+-----+-----
 col1   | smallint                |             | NO       |                |
 none   | t                      |             |          |                |
 col2   | character(100)         | case_sensitive | YES      |                |
 none   | f                      |             |          |                |
```

```

col3 | character varying(100) | case_sensitive | YES | |
text32k | f | 3
col4 | timestamp without time zone | | YES | |
runlength | f | 0
col5 | super | | YES | |
zstd | f | 0
col6 | bigint | | YES | |
az64 | f | 0

```

Diststyle: KEY

Backup: YES

Created: 2021-07-20 19:47:27.997045

Unique Constraints:

"sample_pkey" PRIMARY KEY (col1)

"sample_col2_key" UNIQUE (col2)

Foreign-key constraints:

"sample_col2_fkey" FOREIGN KEY (col2) REFERENCES lineitem(l_orderkey)

資料表的分佈樣式 (簡稱 Diststyle) 可以是 KEY、AUTO、EVEN 或 ALL。

Backup 會指出在擷取快照時是否有備份資料表。有效值為 YES 或 NO。

Created 是建立資料表時的時間戳記。建立日期不適用於 2018 年 11 月之前建立的 Amazon Redshift 資料表。在此日期之前建立的資料表會顯示 n/a (不適用)。

Unique Constraints 會列出資料表上唯一的和主索引鍵的限制。

Foreign-key constraints 會列出資料表上的外部索引鍵限制。

\dC[+] [PATTERN]

列出轉換。包括來源類型、目標類型，以及轉換是否為隱含。

以下示範 \dC+ 的結果子集。

```

List of casts
      source type          |          target type          |          function          |
implicit? | description
-----+-----+-----
"char"    | character                    | bpchar                    | in
assignment |

```

"char" assignment	character varying	text	in
"char" 	integer	int4	no
"char" 	text	text	yes
"path" 	point	point	no
"path" assignment	polygon	polygon	in
abstime assignment	date	date	in
abstime 	integer	(binary coercible)	no
abstime assignment	time without time zone	time	in
abstime 	timestamp with time zone	timestamptz	yes
abstime 	timestamp without time zone	timestamp	yes
bigint 	bit	bit	no
bigint 	boolean	bool	yes
bigint assignment	character	bpchar	in
bigint assignment	character varying	text	in
bigint 	double precision	float8	yes
bigint assignment	integer	int4	in
bigint 	numeric	numeric	yes
bigint 	oid	oid	yes
bigint 	real	float4	yes
bigint 	regclass	oid	yes
bigint 	regoper	oid	yes
bigint 	regoperator	oid	yes

```

bigint          | regproc          | oid            | yes
|
bigint          | regprocedure     | oid            | yes
|
bigint          | regtype          | oid            | yes
|
bigint          | smallint         | int2           | in
assignment |
bigint          | super            | int8_partiql   | in
assignment |

```

`\dd[S] [PATTERN]`

顯示其他地方未顯示的物件描述。

`\de`

列出外部資料表。這包括 AWS Glue 資料目錄中的資料表、蜂巢中繼存放區和來自 Amazon RDS/Aurora MySQL、Amazon RDS/Aurora PostgreSQL 和 Amazon Redshift 資料清理表的聯合資料表。

`\de NAME`

描述外部資料表。

下面的例子顯示了一個 AWS Glue 外部表。

```

# \de spectrum.lineitem
                                Glue External table "spectrum.lineitem"
      Column      | External Type | Redshift Type | Position | Partition Key | Nullable
-----+-----+-----+-----+-----+-----
l_orderkey       | bigint        | bigint         | 1        | 0              |
l_partkey        | bigint        | bigint         | 2        | 0              |
l_suppkey        | int           | int            | 3        | 0              |
l_linenumbers    | int           | int            | 4        | 0              |
l_quantity       | decimal(12,2) | decimal(12,2) | 5        | 0              |
l_extendedprice  | decimal(12,2) | decimal(12,2) | 6        | 0              |
l_discount       | decimal(12,2) | decimal(12,2) | 7        | 0              |
l_tax            | decimal(12,2) | decimal(12,2) | 8        | 0              |
l_returnflag     | char(1)       | char(1)        | 9        | 0              |
l_linestatus     | char(1)       | char(1)        | 10       | 0              |
l_shipdate       | date          | date           | 11       | 0              |

```

l_commitdate	date	date	12	0	
l_receiptdate	date	date	13	0	
l_shipinstruct	char(25)	char(25)	14	0	
l_shipmode	char(10)	char(10)	15	0	
l_comment	varchar(44)	varchar(44)	16	0	

Location: s3://redshiftbucket/kfhose2019/12/31

Input_format: org.apache.hadoop.mapred.TextInputFormat

Output_format: org.apache.hadoop.hive.q1.io.HiveIgnoreKeyTextOutputFormat

Serialization_lib: org.apache.hadoop.hive.serde2.lazy.LazySimpleSerDe

Serde_parameters: {"field.delim": "|", "serialization.format": "|"}

Parameters:

{"EXTERNAL": "TRUE", "numRows": "178196721475", "transient_lastDdlTime": "1577771873"}

Hive Metastore 資料表。

```
# \de emr.lineitem
```

Hive Metastore External Table "emr.lineitem"

Column	External Type	Redshift Type	Position	Partition Key	Nullable
l_orderkey	bigint	bigint	1	0	
l_partkey	bigint	bigint	2	0	
l_suppkey	int	int	3	0	
l_linenumber	int	int	4	0	
l_quantity	decimal(12,2)	decimal(12,2)	5	0	
l_extendedprice	decimal(12,2)	decimal(12,2)	6	0	
l_discount	decimal(12,2)	decimal(12,2)	7	0	
l_tax	decimal(12,2)	decimal(12,2)	8	0	
l_returnflag	char(1)	char(1)	9	0	
l_linestatus	char(1)	char(1)	10	0	
l_commitdate	date	date	11	0	
l_receiptdate	date	date	12	0	
l_shipinstruct	char(25)	char(25)	13	0	
l_shipmode	char(10)	char(10)	14	0	
l_comment	varchar(44)	varchar(44)	15	0	
l_shipdate	date	date	16	1	

Location: s3://redshiftbucket/cetas

Input_format: org.apache.hadoop.hive.q1.io.parquet.MapredParquetInputFormat

Output_format: org.apache.hadoop.hive.q1.io.parquet.MapredParquetOutputFormat

Serialization_lib: org.apache.hadoop.hive.q1.io.parquet.serde.ParquetHiveSerDe

Serde_parameters: {"serialization.format": "1"}

```
Parameters: {"EXTERNAL":"TRUE", "numRows":"4307207",
"transient_lastDdlTime":"1626990007"}
```

PostgreSQL 外部資料表。

```
# \de pgrsql.alltypes
Postgres Federated Table "pgrsql.alltypes"
Column | External Type | Redshift Type | Position |
Partition Key | Nullable
-----+-----+-----+-----+
+-----+-----+-----+-----+
col1 | bigint | bigint | 1 | 0
|
col2 | bigint | bigint | 2 | 0
|
col5 | boolean | boolean | 3 | 0
|
col6 | box | varchar(65535) | 4 | 0
|
col7 | bytea | varchar(65535) | 5 | 0
|
col8 | character(10) | character(10) | 6 | 0
|
col9 | character varying(10) | character varying(10) | 7 | 0
|
col10 | cidr | varchar(65535) | 8 | 0
|
col11 | circle | varchar(65535) | 9 | 0
|
col12 | date | date | 10 | 0
|
col13 | double precision | double precision | 11 | 0
|
col14 | inet | varchar(65535) | 12 | 0
|
col15 | integer | integer | 13 | 0
|
col16 | interval | varchar(65535) | 14 | 0
|
col17 | json | varchar(65535) | 15 | 0
|
```

col18	jsonb	varchar(65535)	16	0
col19	line	varchar(65535)	17	0
col20	lseg	varchar(65535)	18	0
col21	macaddr	varchar(65535)	19	0
col22	macaddr8	varchar(65535)	20	0
col23	money	varchar(65535)	21	0
col24	numeric	numeric(38,20)	22	0
col25	path	varchar(65535)	23	0
col26	pg_lsn	varchar(65535)	24	0
col28	point	varchar(65535)	25	0
col29	polygon	varchar(65535)	26	0
col30	real	real	27	0
col31	smallint	smallint	28	0
col32	smallint	smallint	29	0
col33	integer	integer	30	0
col34	text	varchar(65535)	31	0
col35	time without time zone	varchar(65535)	32	0
col36	time with time zone	varchar(65535)	33	0
col37	timestamp without time zone	timestamp without time zone	34	0
col38	timestamp with time zone	timestamp with time zone	35	0
col39	tsquery	varchar(65535)	36	0
col40	tsvector	varchar(65535)	37	0

col41	txid_snapshot	varchar(65535)	38	0
col42	uuid	varchar(65535)	39	0
col43	xml	varchar(65535)	40	0

\df[anptw][S+] [PATTERN]

列出各種類型的函數。例如，命令 `\df` 會傳回函數清單。結果包括名稱、傳回的資料類型、存取權限和其他中繼資料等屬性。函數類型可以包括觸發條件、預存程序、視窗函數和其他類型。當您附加 `S+` 至命令時 (例如 `\dfantS+`)，其中會包括其他中繼資料資料行，例如 `owner`、`security` 和 `access privileges`。

\dL[S+] [PATTERN]

列出與資料庫相關聯之程序語言的相關資料。資訊中會包括名稱 (例如 `plpgsql`) 和其他中繼資料，其中包括其是否受信任、存取權限和描述。例如，範例呼叫是會列出語言及其屬性的 `\dLS+`。當您附加 `S+` 至命令時，其中會包括其他中繼資料資料行，例如 `call handler` 和 `access privileges`。

範例結果：

```
List of languages
 name      | trusted | internal language |      call handler      |
 validator |         |                   | access privileges |      description
-----+-----+-----+-----+-----
+-----+-----+-----+-----+-----
+-----+-----+-----+-----+-----
 c          | f       | t                 | -                     |
 fmgr_c_validator(oid) |         |                   |                       |
 Dynamically-loaded C functions
 exfunc    | f       | f                 | exfunc_call_handler() | -
 | rdsdb=U/rdsdb      |                       |
 internal  | f       | t                 | -                     |
 fmgr_internal_validator(oid) |         |                   |                       |
 Built-in functions
 mlfunc    | f       | f                 | mlfunc_call_handler() | -
 | rdsdb=U/rdsdb      |                       |
 plpgsql   | t       | f                 | plpgsql_call_handler() |
 plpgsql_validator(oid) |         |                   |                       |
```

```

plpythonu | f          | f          | plpython_call_handler() |
plpython_compiler(cstring,cstring,cstring,cstring,cstring) | rdsdb=U/rdsdb |
sql       | t          | t          | -                        |
fmgr_sql_validator(oid) | =U/rdsdb   | SQL-
language functions

```

\dm[S+] [PATTERN]

列出具體化視觀表。例如，\dmS+ 會列出具體化視觀表及其屬性。當您附加 S+ 至命令時，其中會包括其他中繼資料資料行。

\dn[S+] [PATTERN]

列出結構描述。當您附加 S+ 至命令時 (例如 \dnS+)，其中會包括其他中繼資料資料行，例如 description 和 access privileges。

\dp [PATTERN]

列出資料表、視觀表和序列存取權限。

\dt[S+] [PATTERN]

列出資料表。當您附加 S+ 至命令時 (例如 \dtS+)，其中會包括其他中繼資料資料行，例如本案例中的 description。

\du

列出資料庫的使用者。包括其名稱及其角色 (例如超級使用者) 和屬性。

\dv[S+] [PATTERN]

列出視觀表。包括結構描述、類型和擁有者資料。當您附加 S+ 至命令時 (例如 \dvS+)，其中會包括其他中繼資料資料行。

\H

開啟 HTML 輸出。這對於快速傳回格式化結果非常有用。例如，select * from sales; \H 會以 HTML 格式傳回銷售資料表的結果。若要切換回表格式結果，請使用 \q 或靜音。

\i

從檔案執行命令。例如，假設工作目錄中有 `rsql_steps.sql`，以下內容會執行檔案中的命令：`\i rsql_steps.sql`。

\l[+] [PATTERN]

列出資料庫。包括擁有者、編碼和其他資訊。

\q

結束或 `\q` 命令會登出資料庫工作階段並結束 RSQL。

\sv[+] VIEWNAME

顯示視觀表的定義。

\timing

例如，顯示查詢的執行時間。

\z [PATTERN]

與 `\dp` 相同的輸出。

\?

顯示說明資訊。選用參數會指定要解釋的項目。

\EXIT

登出所有資料庫工作階段並結束 Amazon Redshift RSQL。此外，您也可以指定選用的結束代碼。例如，`\EXIT 15` 會結束 Amazon Redshift RSQL 終端並傳回結束代碼 15。

以下範例示範從連線輸出以及從 RSQL 結束。

```
% rsql -D testuser
DSN Connected
DBMS Name: Amazon Redshift
Driver Name: Amazon Redshift ODBC Driver
Driver Version: 1.4.34.1000
Rsql Version: 1.0.1
Redshift Version: 1.0.29306
Type "help" for help.

(testcluster) user1@dev=# \exit 15
```

```
% echo $?  
15
```

\EXPORT

指定 RSQL 用來儲存後續 SQL SELECT 陳述式所傳回之資料庫資訊的匯出檔案名稱。

export_01.sql

```
\export report file='E:\\accounts.out'  
\rset rformat off  
\rset width 1500  
\rset heading "General Title"  
\rset titledashes on  
select * from td_dwh.accounts;  
\export reset
```

主控台輸出

```
Rformat is off.  
Target width is 1500.  
Heading is set to: General Title  
Titledashes is on.  
(exported 40 rows)
```

\LOGON

連線至資料庫。您可以使用位置語法或連線字串形式指定連線參數。

命令語法如下：`\logon {[DBNAME]- USERNAME|- HOST|- PORT|- [PASSWORD]] | conninfo}`

DBNAME 是所連線的資料庫名稱。USERNAME 是連線時所用身分的使用者名稱。預設的 HOST 是 localhost。預設的 PORT 是 5439。

在 \LOGON 命令中指定主機名稱時，其會變成其他 \LOGON 命令的預設主機名稱。若要變更預設主機名稱，請在另外的 \LOGON 命令中指定新的 HOST。

來自 user1 之 \LOGON 命令的範例輸出如下。

```
(testcluster) user1@redshiftdb=# \logon dev  
DBMS Name: Amazon Redshift
```

```
Driver Name: Amazon Redshift ODBC Driver
Driver Version: 1.4.27.1000
Rsql Version: 1.0.1
You are now connected to database "dev" as user "user1".
(testcluster) user1@dev=#
```

user2 的範例輸出。

```
(testcluster) user1@dev=# \logon dev user2 testcluster2.example.com
Password for user user2:
DBMS Name: Amazon Redshift
Driver Name: Amazon Redshift ODBC Driver
Driver Version: 1.4.27.1000
Rsql Version: 1.0.1
You are now connected to database "dev" as user "user2" on host
"testcluster2.example.com" at port "5439".
(testcluster2) user2@dev=#
```

\REMARK

\echo 命令的延伸。 \REMARK 會將指定字串列印至輸出串流。 \REMARK 會透過新增將輸出換行到不同行的能力來延伸 \echo。

以下範例示範命令的輸出。

```
(testcluster) user1@dev=# \remark 'hello//world'
hello
world
```

\RSET

命令 \rset 會設定命令參數和變數。 \rset 同時具有互動式模式和批次模式。其不支援將選項作為 bash 選項，如 -x 或引數，例如 --<arg>。

其會設定變數，如下所示：

- ERRORLEVEL
- HEADING 和 RTITLE
- RFORMAT
- MAXERROR
- TITLEDASHES

- WIDTH

以下範例會指定標題。

```
\rset heading "Winter Sales Report"
```

如需更多如何使用 `\rset` 的範例，您可以在 [Amazon Redshift RSQL 變數](#) 主題中找到幾個。

\RUN

執行指定檔案中包含的 Amazon Redshift RSQL 指令碼。`\RUN` 會透過新增選項來擴展 `\i` 命令，以略過檔案中的標題行。

如果檔案名稱包含逗號、分號或空格，請以單引號將其括住。此外，如果檔案名稱後面有文字，請以引號將其括住。在 UNIX 中，檔案名稱會區分大小寫。在 Windows 中，檔案名稱不區分大小寫。

以下範例示範命令的輸出。

```
(testcluster) user1@dev=# \! cat test.sql
select count(*) as lineitem_cnt from lineitem;
select count(*) as customer_cnt from customer;
select count(*) as orders_cnt from orders;

(testcluster) user1@dev=# \run file=test.sql
  lineitem_cnt
-----
          4307207
(1 row)

  customer_cnt
-----
      37796166
(1 row)

  orders_cnt
-----
           0
(1 row)

(testcluster) user1@dev=# \run file=test.sql skip=2
```

```
2 records skipped in RUN file.
orders_cnt
-----
          0
(1 row)
```

\OS

\! 命令的別名。 \OS 會執行以參數的形式傳遞的作業系統命令。執行命令後，控制項會回到 Amazon Redshift RSQL。例如，您可以執行以下命令來列印目前的系統日期時間，並返回 RSQL 終端：\os date。

```
(testcluster) user1@dev=# \os date
Tue Sep 7 20:47:54 UTC 2021
```

\GOTO

Amazon Redshift RSQL 的新命令。 \GOTO 會略過所有中間命令，並在指定的 \LABEL 繼續處理。 \LABEL 必須是前向參照。你不能跳到詞法上在 \GOTO 之前的 \LABEL。

下面顯示了範例輸出。

```
(testcluster) user1@dev=# \! cat test.sql
select count(*) as cnt from lineitem \gset
select :cnt as cnt;
\if :cnt > 100
    \goto LABELB
\endif

\label LABELA
\remark 'this is label LABELA'
\label LABELB
\remark 'this is label LABELB'

(testcluster) user1@dev=# \i test.sql
cnt
-----
4307207
(1 row)

\label LABELA ignored
\label LABELB processed
```

```
this is label LABELB
```

\LABEL

Amazon Redshift RSQL 的新命令。**LABEL** 會建立用於執行程式的進入點，以作為 **GOTO** 命令的目標。

以下示範命令的範例輸出。

```
(testcluster) user1@dev=# \! cat test.sql
select count(*) from lineitem limit 5;
\goto LABELB
\remark "this step was skipped by goto label";
\label LABELA
\remark 'this is label LABELA'
\label LABELB
\remark 'this is label LABELB'
```

```
(testcluster) user1@dev=# \i testgoto.sql
  count
 4307193
(1 row)

\label LABELA ignored
\label LABELB processed
this is label LABELB
```

\IF (\ELSEIF, \ELSE, \ENDIF)

\IF 和相關命令會有條件地執行輸入指令碼的某些部分。PSQL `\if` (`\elif`、`\else`、`\endif`) 命令的延伸。**IF** 和 **ELSEIF** 支援布林運算式，包括 AND、OR 和 NOT 條件。

以下示範命令的範例輸出。

```
(testcluster) user1@dev=# \! cat test.sql
SELECT query FROM stv_inflight LIMIT 1 \gset
select :query as query;
\if :query > 1000000
  \remark 'Query id is greater than 1000000'
\elseif :query = 1000000
  \remark 'Query id is equal than 1000000'
```



```

\else
  \remark 'Query id is less than 1000000'
\endif

(testcluster) user1@dev=# \i test.sql
query
-----
 994803
(1 row)

Query id is less than 1000000

```

在您的分支邏輯中使用 `ERRORCODE`。

```

\if :'ERRORCODE' = '00000'
  \remark 'The statement was executed without error'
\else
  \remark :LAST_ERROR_MESSAGE
\endif

```

在 `\IF` 區塊內使用 `\GOTO` 來控制程式碼的執行方式。

Amazon Redshift RSQL 變數

某些關鍵字會作為 RSQL 中的變數。您可以將每個關鍵字設定為特定值，或重設該值。大多數關鍵字會使用具有互動式模式和批次模式的 `\rset` 來進行設定。命令可以用小寫或大寫來定義。

ACTIVITYCOUNT

指出上次提交的請求所影響的資料列數目。若為資料傳回請求，這是從資料庫傳回到 RSQL 的資料列數目。此值是 0 或正整數。最大值是 18,446,744,073,709,551,615。

特殊對待的變數 `ACTIVITYCOUNT` 類似於變數 `ROW_COUNT`。不過，`ROW_COUNT` 不會在 `SELECT`、`COPY` 或 `UNLOAD` 的命令完成時，向用戶端應用程式報告受影響的資料列計數。但 `ACTIVITYCOUNT` 會。

activitycount_01.sql :

```

select viewname, schemaname
from pg_views
where schemaname = 'not_existing_schema';
\if :ACTIVITYCOUNT = 0

```

```
\remark 'views do not exist'  
\endif
```

主控台輸出：

```
viewname | schemaname  
-----+-----  
(0 rows)  
  
views do not exist
```

ERRORLEVEL

指定錯誤的嚴重性等級。使用嚴重性等級可決定行動方式。如果尚未使用 ERRORLEVEL 命令，則其值預設會是 ON。

errorlevel_01.sql：

```
\rset errorlevel 42P01 severity 0  
  
select * from tbl;  
  
select 1 as col;  
  
\echo exit  
\quit
```

主控台輸出：

```
Errorlevel is on.  
rsql: ERROR: relation "tbl" does not exist  
(1 row)  
  
col  
1  
  
exit
```

HEADING 和 RTITLE

可讓使用者指定顯示在報告頂端的標頭。RSET RTITLE 命令指定的標頭會自動包含用戶端電腦的目前系統日期。

rset_heading_rtitle_02.rsq content :

```
\remark Starting...
\rset rtitle "Marketing Department||Confidential//Third Quarter//Chicago"
\rset width 70
\rset rformat on
select * from rsq_test.tbl_currency order by id limit 2;
\exit
\remark Finishing...
```

主控台輸出：

```
Starting...
Rtitle is set to: &DATE||Marketing Department||Confidential//Third Quarter//Chicago
(Changes will take effect after RFORMAT is
switched ON)
Target width is 70.
Rformat is on.
09/11/20      Marketing      Department Confidential
              Third Quarter
              Chicago
id | bankid | name |      start_date
100 |      1 | USD | 2020-09-11 10:51:39.106905
110 |      1 | EUR | 2020-09-11 10:51:39.106905
(2 rows)

Press any key to continue . . .
```

MAXERROR

指定 RSQL 會終止任務處理的最大錯誤嚴重性等級。傳回代碼是 RSQL 在完成每項任務之後傳回給用戶端作業系統的整數值。傳回代碼的值會指出任務的完成狀態。如果指令碼包含的陳述式所產生的錯誤嚴重性等級大於指定的 maxerror 值，則 RSQL 會立即結束。因此，若要讓 RSQL 在錯誤嚴重性等級為 8 時結束，請使用 RSET MAXERROR 7。

maxerror_01.sql content :

```
\rset maxerror 0

select 1 as col;
```

```
\quit
```

主控台輸出：

```
Maxerror is default.
(1 row)

col
1
```

RFORMAT

可讓使用者指定是否要套用格式化命令的設定。

rset_rformat.rsq1 content：

```
\remark Starting...
\pset border 2
\pset format wrapped
\pset expanded on
\pset title 'Great Title'
select * from rsq1_test.tbl_long where id = 500;
\rset rformat
select * from rsq1_test.tbl_long where id = 500;
\rset rformat off
select * from rsq1_test.tbl_long where id = 500;
\rset rformat on
select * from rsq1_test.tbl_long where id = 500;
\exit
\remark Finishing...
```

主控台輸出：

```
Starting...
Border style is 2. (Changes will take effect after RFORMAT is switched ON)
Output format is wrapped. (Changes will take effect after RFORMAT is switched ON)
Expanded display is on. (Changes will take effect after RFORMAT is switched ON)
Title is "Great Title". (Changes will take effect after RFORMAT is switched ON)
id | long_string
500 | In general, the higher the number the more borders and lines the tables will
    | have, but details depend on the particular
format.
```

```
(1 row)
```

```
Rformat is on.
```

```
Great Title
```

```
+-[ RECORD
```

```
1 ]+-----
```

```
-----+
```

```
| id          | 500
```

```
|
```

```
| long_string | In general, the higher the number the more borders and lines the tables  
will have, but details depend on the  
particular format. |
```

```
+-----
```

```
+-----
```

```
-----+
```

```
Rformat is off.
```

```
id |
```

```
long_string
```

```
500 | In general, the higher the number the more borders and lines the tables will  
have, but details depend on the particular format.
```

```
(1 row)
```

```
Rformat is on.
```

```
Great Title
```

```
+-[ RECORD
```

```
1 ]+-----
```

```
-----+
```

```
| id          | 500
```

```
|
```

```
| long_string | In general, the higher the number the more borders and lines the tables  
will have, but details depend on the  
particular format. |
```

```
+-----
```

```
+-----
```

```
-----+
```

```
Press any key to continue . . .
```

ROW_COUNT

取得受先前查詢影響的記錄數目。其通常用來檢查結果，如下面的程式碼片段：

```
SET result = ROW_COUNT;
```

```
IF result = 0
```

...

TITLEDASHES

此控制項可讓使用者指定是否要在針對 SQL 陳述式所傳回的資料行資料上方列印一行破折號字元。

範例：

```
\rset titledashes on
select dept_no, emp_no, salary from rsql_test.EMPLOYEE
where dept_no = 100;
\rset titledashes off
select dept_no, emp_no, salary from rsql_test.EMPLOYEE
where dept_no = 100;
```

主控台輸出：

```
dept_no      emp_no      salary
-----
100          1000346    1300.00
100          1000245    5000.00
100          1000262    2450.00

dept_no      emp_no      salary
100          1000346    1300.00
100          1000245    5000.00
100          1000262    2450.00
```

WIDTH

將輸出格式設定為換行，並指定報告中每一行的目標寬度。如果沒有參數，則會傳回格式和目標寬度的目前設定。

rset_width_01.rsq content：

```
\echo Starting...
\rset width
\rset width 50
\rset width
\quit
\echo Finishing...
```

主控台輸出：

```
Starting...
Target width is 75.
Target width is 50.
Target width is 50.
Press any key to continue . . .
```

有參數的範例：

```
\echo Starting...
\rset rformat on
\pset format wrapped
select * from rsql_test.tbl_long where id = 500;
\rset width 50
select * from rsql_test.tbl_long where id = 500;
\quit
\echo Finishing...
```

主控台輸出：

```
Starting...
Rformat is on.
Output format is wrapped.
id |                               long_string
500 | In general, the higher the number the more borders and lines the ta.
    | .bles will have, but details depend on the particular format.
(1 row)

Target width is 50.
id |                               long_string
500 | In general, the higher the number the more.
    | . borders and lines the tables will have, b.
    | .ut details depend on the particular format.
    | ..
(1 row)
Press any key to continue . . .
```

Amazon Redshift RSQL 錯誤代碼

成功訊息、警告和例外狀況：

錯誤程式碼	錯誤類別	狀況名稱
00000	類別 00 — 成功完成	successful_completion
01000	類別 01 — 警告	warning
0100C	類別 01 — 警告	dynamic_result_sets_returned
01008	類別 01 — 警告	implicit_zero_bit_padding
01003	類別 01 — 警告	null_value_eliminated_in_set_function
01007	類別 01 — 警告	privilege_not_granted
01006	類別 01 — 警告	privilege_not_revoked
01004	類別 01 — 警告	string_data_right_truncation
01P01	類別 01 — 警告	deprecated_feature
02000	類別 02 — 沒有資料	no_data
02001	類別 02 — 沒有資料	no_additional_dynamic_result_sets_returned
03000	類別 03 — SQL 陳述式尚未完成	sql_statement_not_yet_complete
08000	類別 08 — 連線例外狀況	connection_exception
08003	類別 08 — 連線例外狀況	connection_does_not_exist
08006	類別 08 — 連線例外狀況	connection_failure
08001	類別 08 — 連線例外狀況	sqlclient_unable_to_establish_sqlconnection
08004	類別 08 — 連線例外狀況	sqlserver_rejected_establishment_of_sqlconnection
08007	類別 08 — 連線例外狀況	transaction_resolution_unknown
08P01	類別 08 — 連線例外狀況	protocol_violation

錯誤程式碼	錯誤類別	狀況名稱
09000	類別 09 — 觸發的動作例外狀況	triggered_action_exception
0A000	類別 0A — 功能不受支援	feature_not_supported
0A000	類別 0A — 功能不受支援	feature_not_supported
0B000	類別 0B — 無效的交易啟動	invalid_transaction_initiation
0F000	類別 0F — 定位器例外狀況	locator_exception
0F001	類別 0F — 定位器例外狀況	invalid_locator_specification
0L000	類別 0L — 無效的授與者	invalid_grantor
0LP01	類別 0L — 無效的授與者	invalid_grant_operation
0P000	類別 0P — 無效的角色規格	invalid_role_specification
0Z000	類別 0Z — 診斷例外狀況	diagnostics_exception
0Z002	類別 0Z — 診斷例外狀況	stacked_diagnostics_accessed_without_active_handler
20000	類別 20 — 找不到案例	case_not_found
21000	類別 21 — 基數違規	cardinality_violation

資料例外狀況：

錯誤程式碼	錯誤類別	狀況名稱
22000	類別 22 — 資料例外狀況	data_exception
2202E	類別 22 — 資料例外狀況	array_subscript_error
22021	類別 22 — 資料例外狀況	character_not_in_repertoire

錯誤程式碼	錯誤類別	狀況名稱
22008	類別 22 — 資料例外狀況	datetime_field_overflow
22012	類別 22 — 資料例外狀況	division_by_zero
22005	類別 01 — 警告	error_in_assignment
2200B	類別 01 — 警告	escape_character_conflict
22022	類別 01 — 警告	indicator_overflow
22015	類別 01 — 警告	interval_field_overflow
2201E	類別 01 — 警告	invalid_argument_for_logarithm
2201F	類別 01 — 警告	invalid_argument_for_power_function
2201G	類別 01 — 警告	invalid_argument_for_width_bucket_function
22018	類別 01 — 警告	invalid_character_value_for_cast
22007	類別 01 — 警告	invalid_datetime_format
22019	類別 01 — 警告	invalid_escape_character
2200D	類別 01 — 警告	invalid_escape_octet
22025	類別 01 — 警告	invalid_escape_sequence
22P06	類別 01 — 警告	nonstandard_use_of_escape_character
22010	類別 01 — 警告	invalid_indicator_parameter_value
22023	類別 01 — 警告	invalid_parameter_value
2201B	類別 01 — 警告	invalid_regular_expression
22009	類別 01 — 警告	invalid_time_zone_displacement_value
2200C	類別 01 — 警告	invalid_use_of_escape_character

錯誤程式碼	錯誤類別	狀況名稱
2200G	類別 01 — 警告	most_specific_type_mismatch
22004	類別 01 — 警告	null_value_not_allowed
22002	類別 01 — 警告	null_value_no_indicator_parameter
22003	類別 01 — 警告	numeric_value_out_of_range
22026	類別 01 — 警告	string_data_length_mismatch
22001	類別 01 — 警告	string_data_right_truncation
22011	類別 01 — 警告	substring_error
22027	類別 01 — 警告	trim_error
22024	類別 01 — 警告	unterminated_c_string
2200F	類別 01 — 警告	zero_length_character_string
22P01	類別 01 — 警告	floating_point_exception
22P02	類別 01 — 警告	invalid_text_representation
22P03	類別 01 — 警告	invalid_binary_representation
22P04	類別 01 — 警告	bad_copy_file_format
22P05	類別 01 — 警告	untranslatable_character

完整性限制違規：

錯誤程式碼	錯誤類別	狀況名稱
23000	類別 23 — 完整性限制違規	integrity_constraint_violation
23001	類別 23 — 完整性限制違規	restrict_violation

錯誤程式碼	錯誤類別	狀況名稱
23502	類別 23 — 完整性限制違規	not_null_violation
23503	類別 23 — 完整性限制違規	foreign_key_violation
23505	類別 23 — 完整性限制違規	unique_violation
23514	類別 23 — 完整性限制違規	check_violation
24000	類別 24 — 無效的游標狀態	invalid_cursor_state
01004	類別 01 — 警告	string_data_right_truncation
25000	類別 25 — 無效的交易狀態	invalid_transaction_state
25001	類別 25 — 無效的交易狀態	active_sql_transaction
25002	類別 25 — 無效的交易狀態	invalid_transaction_state
25008	類別 25 — 無效的交易狀態	held_cursor_requires_same_isolation_level
25003	類別 25 — 無效的交易狀態	inappropriate_access_mode_for_branch_transaction
25004	類別 25 — 無效的交易狀態	inappropriate_isolation_level_for_branch_transaction
25005	類別 25 — 無效的交易狀態	no_active_sql_transaction_for_branch_transaction
25006	類別 25 — 無效的交易狀態	read_only_sql_transaction
25007	類別 25 — 無效的交易狀態	no_active_sql_transaction_for_branch_transaction
25P01	類別 25 — 無效的交易狀態	no_active_sql_transaction
25P02	類別 25 — 無效的交易狀態	in_failed_sql_transaction

錯誤程式碼	錯誤類別	狀況名稱
26000	類別 26 — 無效的 SQL 陳述式名稱	invalid_sql_statement_name
28000	類別 28 — 無效的授權規格	invalid_authorization_specification
2B000	類別 2B — 仍存在相依權限描述項	dependent_privilege_descriptors_still_exist
2BP01	類別 2B — 仍存在相依權限描述項	dependent_objects_still_exist
2D000	類別 2D — 無效的交易終止	invalid_transaction_termination
2F000	類別 2F — SQL 常式例外狀況	sql_routine_exception
2F005	類別 2F — SQL 常式例外狀況	function_executed_no_return_statement
2F002	類別 2F — SQL 常式例外狀況	modifying_sql_data_not_permitted
2F003	類別 2F — SQL 常式例外狀況	prohibited_sql_statement_attempted
2F004	類別 2F — SQL 常式例外狀況	reading_sql_data_not_permitted
34000	類別 34 — 無效的游標名稱	invalid_cursor_name
38000	類別 38 — 外部常式例外狀況	external_routine_exception
38001	類別 38 — 外部常式例外狀況	containing_sql_not_permitted
38002	類別 38 — 外部常式例外狀況	modifying_sql_data_not_permitted
38003	類別 38 — 外部常式例外狀況	prohibited_sql_statement_attempted
38004	類別 38 — 外部常式例外狀況	reading_sql_data_not_permitted
39000	類別 39 — 外部常式調用例外狀況	external_routine_invocation_exception

錯誤程式碼	錯誤類別	狀況名稱
39001	類別 39 — 外部常式調用例外狀況	invalid_sqlstate_returned
39004	類別 39 — 外部常式調用例外狀況	null_value_not_allowed
39P01	類別 39 — 外部常式調用例外狀況	trigger_protocol_violated
39P02	類別 39 — 外部常式調用例外狀況	srf_protocol_violated
3D000	類別 3D — 無效的目錄名稱	invalid_catalog_name
3F000	類別 3F — 無效的結構描述名稱	invalid_schema_name
42000	類別 42 — 語法錯誤或存取規則違規	syntax_error_or_access_rule_violation
42601	類別 42 — 語法錯誤或存取規則違規	syntax_error
42501	類別 42 — 語法錯誤或存取規則違規	insufficient_privilege
42846	類別 42 — 語法錯誤或存取規則違規	cannot_coerce
42803	類別 42 — 語法錯誤或存取規則違規	grouping_error
42830	類別 42 — 語法錯誤或存取規則違規	invalid_foreign_key
42602	類別 42 — 語法錯誤或存取規則違規	invalid_name

錯誤程式碼	錯誤類別	狀況名稱
42622	類別 42 — 語法錯誤或存取規則違規	name_too_long
42939	類別 42 — 語法錯誤或存取規則違規	reserved_name
42804	類別 42 — 語法錯誤或存取規則違規	datatype_mismatch
42P18	類別 42 — 語法錯誤或存取規則違規	indeterminate_datatype
42809	類別 42 — 語法錯誤或存取規則違規	wrong_object_type
42703	類別 42 — 語法錯誤或存取規則違規	undefined_column
42883	類別 42 — 語法錯誤或存取規則違規	undefined_function
42P01	類別 42 — 語法錯誤或存取規則違規	undefined_table
42P02	類別 42 — 語法錯誤或存取規則違規	undefined_parameter
42704	類別 42 — 語法錯誤或存取規則違規	undefined_object
42701	類別 42 — 語法錯誤或存取規則違規	duplicate_column
42P03	類別 42 — 語法錯誤或存取規則違規	duplicate_cursor
42P04	類別 42 — 語法錯誤或存取規則違規	duplicate_database

錯誤程式碼	錯誤類別	狀況名稱
42723	類別 42 — 語法錯誤或存取規則違規	duplicate_function
42P05	類別 42 — 語法錯誤或存取規則違規	duplicate_prepared_statement
42P06	類別 42 — 語法錯誤或存取規則違規	duplicate_schema
42P07	類別 42 — 語法錯誤或存取規則違規	duplicate_table
42712	類別 42 — 語法錯誤或存取規則違規	duplicate_alias
42710	類別 42 — 語法錯誤或存取規則違規	duplicate_object
42702	類別 42 — 語法錯誤或存取規則違規	ambiguous_column
42725	類別 42 — 語法錯誤或存取規則違規	ambiguous_function
42P08	類別 42 — 語法錯誤或存取規則違規	ambiguous_parameter
42P09	類別 42 — 語法錯誤或存取規則違規	ambiguous_alias
42P10	類別 42 — 語法錯誤或存取規則違規	invalid_column_reference
42611	類別 42 — 語法錯誤或存取規則違規	invalid_column_definition
42P11	類別 42 — 語法錯誤或存取規則違規	invalid_cursor_definition

錯誤程式碼	錯誤類別	狀況名稱
42P12	類別 42 — 語法錯誤或存取規則違規	invalid_database_definition
42P13	類別 42 — 語法錯誤或存取規則違規	invalid_function_definition
42P14	類別 42 — 語法錯誤或存取規則違規	invalid_prepared_statement_definition
42P15	類別 42 — 語法錯誤或存取規則違規	invalid_schema_definition
42P16	類別 42 — 語法錯誤或存取規則違規	invalid_table_definition
42P17	類別 42 — 語法錯誤或存取規則違規	invalid_object_definition
44000	類別 44 — WITH CHECK OPTION 違規	with_check_option_violation
53000	類別 53 — 資源不足	insufficient_resources
53100	類別 53 — 資源不足	disk_full
53200	類別 53 — 資源不足	out_of_memory
53300	類別 53 — 資源不足	too_many_connections
54000	類別 54 — 超過計劃限制	program_limit_exceeded
54001	類別 54 — 超過計劃限制	statement_too_complex
54011	類別 54 — 超過計劃限制	too_many_columns
54023	類別 54 — 超過計劃限制	too_many_arguments
55000	類別 55 — 物件未處於先決條件狀態	object_not_in_prerequisite_state

錯誤程式碼	錯誤類別	狀況名稱
55006	類別 55 — 物件未處於先決條件狀態	object_in_use
55P02	類別 55 — 物件未處於先決條件狀態	cant_change_runtime_param
55P03	類別 55 — 物件未處於先決條件狀態	lock_not_available
57000	類別 57 — 操作員介入	operator_intervention
57014	類別 57 — 操作員介入	query_canceled
57P01	類別 57 — 操作員介入	admin_shutdown
57P02	類別 57 — 操作員介入	crash_shutdown
57P03	類別 57 — 操作員介入	cannot_connect_now
58000	類別 58 — 系統錯誤 (PostgreSQL 外部的錯誤)	system_error
58030	類別 58 — 系統錯誤 (PostgreSQL 外部的錯誤)	io_error
58P01	類別 58 — 系統錯誤 (PostgreSQL 外部的錯誤)	undefined_file
58P02	類別 58 — 系統錯誤 (PostgreSQL 外部的錯誤)	duplicate_file
F0000	類別 F0 — 組態檔案錯誤	duplicate_file
F0001	類別 F0 — 組態檔案錯誤	lock_file_exists
P0000	類別 P0 — PL/pgSQL 錯誤	plpgsql_error
P0001	類別 P0 — PL/pgSQL 錯誤	raise_exception

錯誤程式碼	錯誤類別	狀況名稱
P0002	類別 P0 — PL/pgSQL 錯誤	no_data_found
P0003	類別 P0 — PL/pgSQL 錯誤	too_many_rows
XX000	類別 XX — 內部錯誤	internal_error
XX001	類別 XX — 內部錯誤	data_corrupted
XX002	類別 XX — 內部錯誤	index_corrupted

Amazon Redshift RSQL 環境變數

Amazon Redshift RSQL 可以使用環境變數來選取預設的參數值。

RSPASSWORD

Important

基於安全考量，不建議您使用此環境變數，因為某些作業系統會允許非系統管理使用者查看處理序環境變數。

設定 Amazon Redshift RSQL 在連線至 Amazon Redshift 時要使用的密碼。此環境變數需要 Amazon Redshift RSQL 1.0.4 及以上版本。

如果設定了 RSPASSWORD，RSQL 會優先使用 RSPASSWORD。如果未設定 RSPASSWORD，而且您使用 DSN 進行連線，則 RSQL 會從 DSN 檔案的參數中取得密碼。最後，如果未設定 RSPASSWORD，而且您沒有使用 DSN，則 RSQL 會在嘗試連線後提供密碼提示。

以下是設定 RSPASSWORD 的範例：

```
export RSPASSWORD=TestPassw0rd
```

使用 SQL Workbench/J 進行連線

您可以使用 SQL Workbench/J (免費、不需使用 DBMS、跨平台的 SQL 查詢工具) 來連線至資料庫。

Amazon Redshift 未提供或安裝任何第三方 SQL 用戶端工具或程式庫，因此您必須自行安裝想要用於資料庫的任何這類工具或程式庫。若要安裝 SQL Workbench/J，請遵循 SQL Workbench/J 文件 ([SQL Workbench/J](#)) 中的指示。一般而言，若要使用 SQL Workbench/J，請進行下列操作：

- 檢閱 SQL Workbench/J 軟體授權。
- 在用戶端電腦或 Amazon EC2 執行個體上，下載適合您作業系統的 SQL Workbench/J 套件。
- 在您的系統上安裝 SQL Workbench/J。

在您的系統上安裝 Java 執行階段環境 (JRE)。請確定您使用 SQL Workbench/J 用戶端所需的正確 JRE 版本。

- 在 SQL Workbench/J 中透過 JDBC 連線來連線至您的資料庫。

請確定用戶端電腦或 Amazon EC2 執行個體具有建議使用的 Amazon Redshift JDBC 驅動程式。如需可下載最新驅動程式的連結，請參閱[下載 Amazon Redshift JDBC 驅動程式 2.1 版](#)。此外，也請確定您已設定防火牆設定以允許存取您的資料庫。如需詳細資訊，請參閱《[Amazon Redshift 入門指南](#)》中的「[步驟 4：授權叢集的存取權](#)」。

- 在使用 Amazon Redshift 驅動程式的 SQL Workbench/J 中建立新的連線設定檔。

以程式設計方式 Connect 到資料倉

如需建置應用程式以連線到資料倉儲的工具的相關資訊，請參閱[建置在 AWS 上的工具](#)。

使用身分驗證設定檔連線至 Amazon Redshift

如果您有許多 Amazon Redshift 連線，則可能難以管理所有連線的設定。每個 JDBC 或 ODBC 連線通常會使用特定的組態選項。透過使用身分驗證設定檔，您可以將連線選項儲存在一起。如此一來，使用者就可以選擇要用來連線的設定檔，而不必管理個別選項的設定。設定檔可以套用至各種案例和使用者類型。

建立驗證設定檔之後，使用者可以將 ready-to-use 設定檔新增至連接字串。如此一來，其便可以使用每個角色和使用案例的正確設定來連線至 Amazon Redshift。

如需 Amazon Redshift API 的資訊，請參閱[CreateAuthentication設定檔](#)。

建立身分驗證設定檔

您可以 AWS CLI 使用 `create-authentication-profile` 指令建立驗證設定檔。這會假設您有現有的 Amazon Redshift 叢集和現有的資料庫。您的憑證必須具有可連線至 Amazon Redshift 資料庫的許

可，以及可擷取身分驗證設定檔的權限。您可以透過 JSON 字串的形式提供組態選項，也可以參考包含 JSON 字串的檔案。

```
create-authentication-profile --authentication-profile-name<value: String> --
authentication-profile-content<value: String>
```

以下範例會建立名為 `ExampleProfileName` 的設定檔。在這裡，您可以將定義叢集名稱和其他選項設定的金鑰和值新增為 JSON 字串。

```
create-authentication-profile --authentication-profile-name "ExampleProfileName"
--authentication-profile-content "{\"AllowDBUserOverride\" : \"1\", \"Client_ID
\": \"ExampleClientID\", \"App_ID\" : \"ExampleAppID\", \"AutoCreate\" : false,
\"enableFetchRingBuffer\" : true, \"databaseMetadataCurrentDbOnly\" : true}"
}
```

此命令會使用指定的 JSON 設定建立設定檔。系統會傳回以下內容，以指出您已建立設定檔。

```
{"AuthenticationProfileName": "ExampleProfileName",
"AuthenticationProfileContent": "{\"AllowDBUserOverride\" : \"1\",
\"Client_ID\" : \"ExampleClientID\", \"App_ID\" : \"ExampleAppID\",
\"AutoCreate\" : false, \"enableFetchRingBuffer\" : true,
\"databaseMetadataCurrentDbOnly\" : true}" }
```

建立身分驗證設定檔的限制和配額

每位客戶的配額為十 (10) 個身分驗證設定檔。

身分驗證設定檔可能會發生某些錯誤。例如，如果您使用現有名稱建立新的設定檔，或是您超過設定檔配額的話。如需詳細資訊，請參閱[CreateAuthentication設定檔](#)。

您無法在身分驗證設定檔存放區中儲存 JDBC、ODBC 和 Python 連線字串的某些選項金鑰和值：

- AccessKeyID
- access_key_id
- SecretAccessKey
- secret_access_key_id
- PWD
- Password

- password

您無法在設定檔存放區中儲存 JDBC 或 ODBC 連線字串的金鑰或值 AuthProfile。若為 Python 連線，您無法儲存 auth_profile。

身份驗證設定檔存放在 Amazon DynamoDB 中，並由其管理。AWS

使用身分驗證設定檔

在建立身分驗證設定檔後，便可以在 JDBC 2.0 版 AuthProfile 中將設定檔名稱納入為連線選項。使用此連線選項會擷取已儲存的設定。

```
jdbc:redshift:iam://endpoint:port/database?AuthProfile=<Profile-Name>&AccessKeyId=<Caller-Access-Key>&SecretAccessKey=<Caller-Secret-Key>
```

以下是 JDBC URL 字串範例。

```
jdbc:redshift:iam://examplecluster:us-west-2/dev?AuthProfile="ExampleProfile"&AccessKeyId="AKIAIOSFODNN7EXAMPLE"&SecretAccessKey="wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY"
```

在 JDBC URL 中指定 AccessKeyId 和 SecretAccessKey，以及身分驗證設定檔名稱。

您也可以使用分號分隔符號來分隔組態選項，例如以下範例 (其包含記錄的選項)。

```
jdbc:redshift:iam://my_redshift_end_point:5439/dev?LogLevel=6;LogPath=/tmp;AuthProfile=my_profile;AccessKeyId="AKIAIOSFODNN7EXAMPLE";SecretAccessKey="wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY"
```

Note

請勿將機密資訊新增至身分驗證設定檔。例如，請勿在身分驗證設定檔中儲存 AccessKeyId 或 SecretAccessKey 值。身分驗證設定檔存放區具有禁止儲存秘密金鑰的規則。如果您嘗試儲存與敏感資訊相關聯的金鑰和值，就會收到錯誤。

取得身分驗證設定檔

若要列出現有的身分驗證設定檔，請呼叫以下命令。

```
describe-authentication-profiles --authentication-profile-name <value: String>
```

以下範例示範所擷取的兩個設定檔。如果未指定設定檔名稱，則會傳回所有設定檔。

```
{ "AuthenticationProfiles": [ { "AuthenticationProfileName":  
"testProfile1", "AuthenticationProfileContent": "{\\"AllowDBUserOverride  
\\":\\"1\\",\\"Client_ID\\":\\"ExampleClientID\\",\\"App_ID\\":\\"ExampleAppID  
\\",\\"AutoCreate\\":false,\\"enableFetchRingBuffer\\":true,  
\\"databaseMetadataCurrentDbOnly\\":true}" }, { "AuthenticationProfileName":  
"testProfile2", "AuthenticationProfileContent": "{\\"AllowDBUserOverride  
\\":\\"1\\",\\"Client_ID\\":\\"ExampleClientID\\",\\"App_ID\\":\\"ExampleAppID  
\\",\\"AutoCreate\\":false,\\"enableFetchRingBuffer\\":true,  
\\"databaseMetadataCurrentDbOnly\\":true}" } ] }
```

針對 Amazon Redshift 中的連線問題進行疑難排解

如果從 SQL 用戶端工具連接至叢集時有問題，您可以檢查幾個項目來縮小問題的範圍。如果您使用 SSL 或伺服器憑證，對連線問題進行故障排除時，請先移除此複雜度。然後在找到解決方案之後加回來。如需詳細資訊，請參閱 [設定連線的安全選項](#)。

Important

Amazon Redshift 已變更 SSL 憑證的管理方式。如果您無法使用 SSL 來連接，您可能需要更新目前的信任根 CA 憑證。如需詳細資訊，請參閱 [將 SSL 連線轉換為使用 ACM 憑證](#)。

下一節提供連線問題的一些範例錯誤訊息及可能的解決方案。因為不同的 SQL 用戶端工具會提供不同的錯誤訊息，所以這不是完整的清單，但很適合作為問題疑難排解時的起點。

主題

- [從 Amazon EC2 外部進行連線 \(防火牆逾時問題\)](#)
- [連線遭拒或失敗](#)
- [用戶端和驅動程式不相容](#)
- [查詢似乎沒有回應且有時無法觸達叢集](#)
- [設定 JDBC 擷取大小參數](#)

從 Amazon EC2 外部進行連線 (防火牆逾時問題)

問題範例

執行長時間查詢 (例如 COPY 命令) 時，對資料庫的用戶端連線似乎懸置或逾時。在此情況下，您可能會發現 Amazon Redshift 主控台顯示查詢已完成，但用戶端工具本身仍似乎在執行查詢。取決於連線停止的時間，查詢的結果可能遺漏或不完整。

可能的解決方案

從 Amazon EC2 執行個體以外的機器連線到 Amazon Redshift 時，便會發生此問題。在此情況下，閒置連線會在閒置一段時間後，遭到中繼網路元件 (例如防火牆) 終止。當您從虛擬私有網路 (VPN) 或本機網路登入時，這是很典型的行為。

為了避免這些逾時，建議採取下列變更：

- 提高與 TCP/IP 逾時有關的用戶端系統值。請在您用來連接至叢集的電腦上進行這些變更。應該依您的用戶端和網路來調整逾時期間。如需詳細資訊，請參閱 [變更 TCP/IP 逾時設定](#)。
- (選用) 在 DSN 層級上設定保持連線行為。如需詳細資訊，請參閱 [變更 DSN 逾時設定](#)。

變更 TCP/IP 逾時設定

若要變更 TCP/IP 逾時設定，請根據您用於連接至叢集的作業系統來設定逾時設定。

- Linux — 如果用戶端在 Linux 上執行，請以根使用者身分執行下列命令，以變更目前工作階段的逾時設定：

```
/sbin/sysctl -w net.ipv4.tcp_keepalive_time=200 net.ipv4.tcp_keepalive_intvl=200  
net.ipv4.tcp_keepalive_probes=5
```

若要保留設定，請使用下列值建立或修改 `/etc/sysctl.conf` 檔案，然後重新啟動系統。

```
net.ipv4.tcp_keepalive_time=200  
net.ipv4.tcp_keepalive_intvl=200  
net.ipv4.tcp_keepalive_probes=5
```

- 視窗 — 如果您的用戶端在 Windows 上執行，請在 HKEY_LOCAL_ 機器\系統\設定\服務\Tcpip\ 參數下編輯下列登錄設定的值：CurrentControl

- KeepAlive時間：3 萬
- KeepAlive間隔：
- TcpMaxDataRetransmissions：十

這些設定使用 DWORD 資料類型。如果這些設定不存在於登錄路徑下，您可以建立設定並指定這些建議值。如需編輯 Windows 登錄的相關資訊，請參閱 Windows 文件。

設定這些值之後，請重新啟動電腦以讓變更改生效。

- Mac — 如果用戶端在 Mac 上執行，請執行下列命令，以變更目前工作階段的逾時設定：

```
sudo sysctl net.inet.tcp.keepintvl=200000
sudo sysctl net.inet.tcp.keepidle=200000
sudo sysctl net.inet.tcp.keepinit=200000
sudo sysctl net.inet.tcp.always_keepalive=1
```

若保留設定，請使用下列值建立或修改 `/etc/sysctl.conf` 檔案：

```
net.inet.tcp.keepidle=200000
net.inet.tcp.keepintvl=200000
net.inet.tcp.keepinit=200000
net.inet.tcp.always_keepalive=1
```

重新啟動電腦，然後執行下列命令，以驗證是否已設定這些值。

```
sysctl net.inet.tcp.keepidle
sysctl net.inet.tcp.keepintvl
sysctl net.inet.tcp.keepinit
sysctl net.inet.tcp.always_keepalive
```

變更 DSN 逾時設定

您可以在 DSN 層級上設定保持連線行為 (若選擇這麼做)。在作法上是在 `odbc.ini` 檔案中新增或修改下列參數：

KeepAlives伯爵

在認為連線已中斷之前可遺失的 TCP 保持連線封包數。

KeepAlives 閒置

驅動程式傳送 TCP 保持連線封包之前的閒置秒數。

KeepAlives 間隔

每一次 TCP 保持連線重新傳輸之間的秒數。

在 Windows 上，您可以在登錄中的 HKEY_LOCAL_MACHINE\SOFTWARE\ODBC\ODBC.INI *<your_DSN>* 中新增或變更機碼，以修改這些參數。在 Linux 和 macOS 上，您直接在 `odbc.ini` 檔案中的目標 DSN 項目中新增或修改這些參數。如需在 Linux 和 macOS 電腦上修改 `odbc.ini` 檔案的相關資訊，請參閱 [使用 ODBC 驅動程式管理員來設定 Linux 和 macOS X 作業系統上的驅動程式](#)。

如果這些參數不存在，或值為 0，系統會使用指定給 TCP/IP 的保持連線參數，以決定 DSN 保持連線行為。在 Windows 上，您可以在 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\ 的登錄中找到 TCP/IP 參數。在 Linux 和 macOS 上，您可以在 `sysctl.conf` 檔案中找到 TCP/IP 參數。

連線遭拒或失敗

錯誤範例

- 「無法對 *<endpoint>* 建立連線。」
- 「無法連接至伺服器：連線逾時。伺服器在主機 '*<endpoint>*' 上執行且在連接埠 '*<port>*' 上接受 TCP/IP 連線嗎？」
- 「連線遭拒。請檢查主機名稱和連接埠正確，且 postmaster 接受 TCP/IP 連線。」

可能的解決方案

一般來說，收到錯誤訊息指出無法建立連線時，表示存取叢集的許可有問題，或到達叢集的網路流量有問題。

若要從叢集所在網路外部的用戶端工具連線至叢集，請在叢集的安全群組中新增傳入規則。規則組態取決於 Amazon Redshift 叢集是否建立於虛擬私有雲端 (VPC)：

- 如果您在以 Amazon VPC 為基礎的虛擬私有雲端 (VPC) 中建立了 Amazon Redshift 叢集，請在 Amazon VPC 中於 VPC 安全群組內新增會指定用戶端 CIDR/IP 地址的傳入規則。如需為叢集設定 VPC 安全群組以及可公開存取選項的相關資訊，請參閱 [管理 VPC 中的叢集](#)。

- 如果在 VPC 外部建立了 Amazon Redshift 叢集，請在 Amazon Redshift 中將用戶端 CIDR/IP 地址新增至叢集安全群組。如需設定叢集安全群組的相關資訊，請參閱 [Amazon Redshift 叢集安全群組](#)。

如果您嘗試從在 Amazon EC2 執行個體上執行的用戶端工具連線至叢集，您也會新增傳入規則。在此情況下，請在叢集安全群組中新增規則。此規則必須指定與用戶端工具的 Amazon EC2 執行個體相關聯的 Amazon EC2 安全群組。

在某些情況下，您的用戶端與伺服器之間可能有一層，例如防火牆。在這些情況下，請確定防火牆透過您為叢集設定的連接埠接受傳入連線。

用戶端和驅動程式不相容

錯誤範例

「指定 DSN 所包含的驅動程式和應用程式之間的架構不符。」

可能的解決方案

當您嘗試連接並得到有關架構不符的錯誤時，這表示用戶端工具和驅動程式不相容。原因是它們的系統架構不相符。例如，假設您有 32 位元用戶端工具，但卻安裝 64 位元版本的驅動程式，就可能發生此錯誤。有時，64 位元用戶端工具可以使用 32 位元驅動程式，但 32 位元應用程式不能搭配 64 位元驅動程式一起使用。請確定驅動程式和用戶端工具使用相同版本的系統架構。

查詢似乎沒有回應且有時無法觸達叢集

問題範例

您遇到查詢完成方面的問題，查詢似乎正在執行，但在 SQL 用戶端工具中無回應。有時，查詢無法出現在叢集，例如系統資料表或 Amazon Redshift 主控台。

可能的解決方案

由於封包捨棄，可能發生此問題。在兩個網際網路通訊協定 (IP) 主機之間的網路路徑中，最大傳輸單位 (MTU) 出現差異。MTU 大小決定網路連線上的一個乙太網路訊框中可傳輸的封包大小上限 (位元組)。在中 AWS，某些 Amazon EC2 執行個體類型支援 1500 的 MTU (乙太網路 v2 框架)，而其他執行個體類型則支援 MTU 9001 (TCP/IP 巨型框架)。

為了避免因為 MTU 大小不同而發生問題，建議採取下列其中一個動作：

- 如果叢集使用 EC2-VPC 平台，請以傳回 Destination Unreachable 的傳入自訂「網際網路控制訊息通訊協定 (ICMP)」規則來設定 Amazon VPC 安全群組。此規則會藉以指示原始主機沿著網路路徑使用最低的 MTU 大小。如需此方法的詳細資訊，請參閱[將安全群組設為允許 ICMP「無法觸達目標」](#)。
- 如果叢集使用 EC2-Classic 平台，或您無法允許 ICMP 傳入規則，請停用 TCP/IP 巨型訊框，以便使用乙太網路 v2 訊框。如需此方法的詳細資訊，請參閱[設定執行個體的 MTU](#)。

將安全群組設為允許 ICMP「無法觸達目標」

在兩個主機之間的網路中，當 MTU 大小出現差異時，首先請確定網路設定並未禁止路徑 MTU 探索 (PMTUD)。PMTUD 可讓接收端主機向原始主機回應下列 ICMP 訊息：Destination Unreachable: fragmentation needed and DF set (ICMP Type 3, Code 4)。此訊息指示原始主機沿著網路路徑，使用最低的 MTU 大小來重新傳送請求。如果不這樣協議，可能會因為請求太大，使得接收端主機無法接受，而發生封包捨棄。如需此 ICMP 訊息的相關資訊，請前往網際網路工程任務組 (IETF) 網站上的 [RFC792](#)。

如果您沒有明確為 Amazon VPC 安全群組設定此 ICMP 傳入規則，則會封鎖 PMTUD。在中 AWS，安全群組是指定執行個體輸入和輸出流量規則的虛擬防火牆。如需 Amazon Redshift 叢集安全群組的相關資訊，請參閱 [Amazon Redshift 叢集安全群組](#)。對於使用 EC2-VPC 平台的叢集，Amazon Redshift 會使用 VPC 安全群組來允許或拒絕流量進入叢集。根據預設，安全群組會鎖定並拒絕所有傳入流量。如需如何為 EC2-Classic 或 EC2-VPC 執行個體設定輸入和輸出規則的詳細資訊，請參閱 Amazon EC2 使用者指南中的 [EC2-Classic 中的執行個體與 VPC 之間的差異](#)。

如需如何將規則新增至 VPC 安全群組的相關資訊，請參閱[管理叢集的 VPC 安全群組](#)。如需有關此規則所需之特定 PMTUD 設定的詳細資訊，請參閱 Amazon EC2 使用者指南中的[路徑 MTU 探索](#)。

設定執行個體的 MTU

在某些情況下，您的叢集可能會使用 EC2-Classic 平台，或您無法允許傳入流量的自訂 ICMP 規則。在這些情況下，我們建議您將連線到 Amazon Redshift 叢集之 EC2 執行個體的網路界面 (NIC) 上的 MTU 調整為 1500。此調整會停用 TCP/IP 巨型訊框，以確保連線始終使用相同的封包大小。不過，此選項會完全地降低執行個體的最大網路輸送量，而不只是 Amazon Redshift 的連線而已。如需詳細資訊，請參閱下列程序。

在 Microsoft Windows 作業系統上設定 MTU

如果用戶端在 Microsoft Windows 作業系統中執行，您可以使用 netsh 命令來檢閱並設定乙太網路卡的 MTU 值。

1. 執行下列命令來判斷目前的 MTU 值：

```
netsh interface ipv4 show subinterfaces
```

2. 在輸出中檢閱 MTU 界面卡的 Ethernet 值。
3. 如果值不是 1500，請執行下列命令來設定此值：

```
netsh interface ipv4 set subinterface "Ethernet" mtu=1500 store=persistent
```

設定此值之後，請重新啟動電腦以讓變更生效。

在 Linux 作業系統上設定 MTU

如果用戶端在 Linux 作業系統中執行，您可以使用 ip 命令來檢閱並設定 MTU 值。

1. 執行下列命令來判斷目前的 MTU 值：

```
$ ip link show eth0
```

2. 在輸出中檢閱 mtu 後面的值。
3. 如果值不是 1500，請執行下列命令來設定此值：

```
$ sudo ip link set dev eth0 mtu 1500
```

在 Mac 作業系統上設定 MTU

- 遵循 MacOS 支援網站上有關 [How to change the MTU for troubleshooting purposes](#) 的指示進行操作。如需詳細資訊，請搜尋 [支援網站](#)。

設定 JDBC 擷取大小參數

依預設，JDBC 驅動程式會一次收集查詢的所有結果。因此，當您嘗試透過 JDBC 連線擷取大型結果集時，可能會遇到用戶端 out-of-memory 錯誤。若要讓用戶端能夠批次擷取結果集，而非單一 all-or-nothing 擷取，請在用戶端應用程式中設定 JDBC fetch size 參數。

Note

ODBC 不支援擷取大小。

為求最佳效能，請將擷取大小設定為不會導致記憶體不足錯誤的最高值。較低的擷取大小值會造成更多伺服器來回行程，進而延長執行時間。伺服器會預留資源，包括 WLM 查詢位置和關聯的記憶體，直到用戶端擷取整個結果集或查詢取消為止。適當地調校擷取大小時，那些資源會更快速釋出，使得它們可供其他查詢使用。

Note

如果您需要擷取大型資料集，建議您使用 [UNLOAD](#) 陳述式將資料傳輸到 Amazon S3。使用 UNLOAD 時，運算節點會平行運作，以加速資料的傳輸。

如需設定 JDBC 擷取大小參數的相關資訊，請前往 PostgreSQL 文件中的[根據游標取得結果](#)。

使用 Amazon Redshift 資料 API

您可以使用內建的 Amazon Redshift 資料 API 存取 Amazon Redshift 資料庫。使用此 API，您可以使用以網路服務為基礎的應用程式 (包括 AWS Lambda Amazon SageMaker 筆記本和 AWS Cloud9) 如需這些應用程式的詳細資訊 [AWS Lambda](#)，請參閱 [Amazon SageMaker](#) 和 [AWS Cloud9](#)。

資料 API 不需要與資料庫持續連線。相反，它提供了一個安全的 HTTP 端點，並與 AWS SDK 的集成。您可以使用端點來執行 SQL 陳述式，而不需管理連線。對資料 API 的呼叫是非同步的。

資料 API 使用儲存在資料庫認證 AWS Secrets Manager 或臨時資料庫認證中的認證。不管是哪一種授權方法，都不需要在 API 呼叫中傳遞密碼。如需有關的詳細資訊 AWS Secrets Manager，請參閱[什麼是 AWS Secrets Manager？](#) 在《AWS Secrets Manager 使用者指南》中。

如需資料 API 操作的相關資訊，請參閱 [Amazon Redshift 資料 API 參考](#)。

使用 Amazon Redshift 資料 API

在使用 Amazon Redshift 資料 API 之前，請先檢閱下列步驟：

1. 確定身為資料 API 呼叫者的您是否已獲得授權。如需授權的相關資訊，請參閱 [授權 Amazon Redshift 資料 API 的存取](#)。

2. 確定您打算使用來自 Secrets Manager 的驗證憑證還是使用暫時憑證來呼叫資料 API。如需詳細資訊，請參閱 [在呼叫 Amazon Redshift 資料 API 時選擇資料庫身分驗證憑證](#)。
3. 如果您使用 Secrets Manager 來取得驗證憑證，請設定機密。如需詳細資訊，請參閱 [將資料庫認證儲存於 AWS Secrets Manager](#)。
4. 在呼叫資料 API 時，檢閱考量和限制。如需詳細資訊，請參閱 [呼叫 Amazon Redshift 資料 API 時的考量](#)。
5. 從 AWS Command Line Interface (AWS CLI)、您自己的程式碼或使用 Amazon Redshift 主控台內的查詢編輯器呼叫資料 API。如需從呼叫的範例 AWS CLI，請參閱 [呼叫資料 API](#)。

呼叫 Amazon Redshift 資料 API 時的考量

在呼叫資料 API 時，請考量下列事項：

- Amazon Redshift 資料 API 可以存取 Amazon Redshift 所佈建的叢集和 Redshift Serverless 工作群組中的資料庫。如需可用 Redshift 資料 API 的 AWS 區域清單，請參閱中針對 [Redshift 資料 API](#) 列出的端點。Amazon Web Services 一般參考
- 查詢的持續時間上限為 24 小時。
- 每個 Amazon Redshift 叢集的作用中查詢 (STARTED 和 SUBMITTED 查詢) 數目上限為 200 個。
- 查詢結果大小上限為 100 MB (在 gzip 壓縮之後)。如果呼叫傳回的回應資料超過 100 MB，系統就會結束呼叫。
- 查詢結果的保留時間上限為 24 小時。
- 查詢陳述式的大小上限為 100 KB。
- 資料 API 可用於查詢以下節點類型的單節點和多節點叢集：
 - dc2.large
 - dc2.8xlarge
 - ra3.xlplus
 - ra3.4xlarge
 - ra3.16xlarge
- 叢集必須位於以 Amazon VPC 服務為基礎的虛擬私有雲端 (VPC) 中。
- 根據預設，其 IAM 角色或 IAM 許可與 ExecuteStatement 或 BatchExecuteStatement API 操作的執行者相同的使用者，可以使用 CancelStatement、DescribeStatement、GetStatementResult 和 ListStatements API 操作來處理相同的陳述式。若要處理其他使用者的相同 SQL 陳述式，使用者必須能夠擔任執行了

SQL 陳述式之使用者的 IAM 角色。如需擔任角色的相關資訊，請參閱 [授權 Amazon Redshift 資料 API 的存取](#)。

- 在 BatchExecuteStatement API 操作的 Sqls 參數中，SQL 陳述式會以單一交易的形式來執行。其會依陣列順序循序執行。後續的 SQL 陳述式要等到陣列中的前一個陳述式完成後才會啟動。如果有任何 SQL 陳述式失敗，由於其以單一交易的形式執行，因此所有工作都會復原。
- ExecuteStatement 或 BatchExecuteStatement API 操作中所使用的用戶端字符保留時間上限為 8 小時。
- 在限流請求之前，Redshift Data API 中的每個 API 都有每秒交易配額。如需配額的相關資訊，請參閱 [Amazon Redshift Data API 的配額](#)。如果請求的速率超過配額，則傳回附帶 HTTP 狀態碼：400 的 ThrottlingException。若要回應限流，請使用重試策略，如 AWS SDK 和工具參考指南中的 [重試行為](#) 中所述。此策略會自動實作，以便在某些 AWS SDK 中進行節流錯誤。

Note

依預設 AWS Step Functions，在中，不會啟用重試。如果您需要在 Step Functions 狀態機器中呼叫 Redshift Data API，請在 Redshift Data API 呼叫中包含 ClientToken 等冪性參數。ClientToken 的值需要在重試之間持續存在。在 ExecuteStatement API 請求的下列範例片段中，表達式 States.ArrayGetItem(States.StringSplit(\$\$.Execution.Id, ':'), 7) 會使用內部函數來擷取 \$\$.Execution.Id 的 UUID 部分，這對於狀態機器的每次執行而言都是唯一的。如需詳細資訊，請參閱 AWS Step Functions 開發人員指南中的 [內部函數](#)。

```
{
  "Database": "dev",
  "Sql": "select 1;",
  "ClusterIdentifier": "MyCluster",
  "ClientToken.$": "States.ArrayGetItem(States.StringSplit($$.Execution.Id,
  ':'), 7)"
}
```

在呼叫 Amazon Redshift 資料 API 時選擇資料庫身分驗證憑證

當您呼叫資料 API 時，您會對部分 API 操作使用下列其中一種身分驗證方法。每種方法都需要不同的參數組合。

AWS Secrets Manager

使用此方法，提供存儲在 AWS Secrets Manager 中具有username和secret-arn的密碼password。指定的機密包含用來連線至所指定 database 的憑證。當您連線至叢集時，您也會提供資料庫名稱，如果您提供叢集識別碼 (dbClusterIdentifier)，則其必須符合儲存在機密中的叢集識別碼。當您連線至無伺服器工作群組時，您也會提供資料庫名稱。如需詳細資訊，請參閱[將資料庫認證儲存於 AWS Secrets Manager](#)。

臨時憑證

使用此方法時，請選擇下列其中一個選項：

- 在連線至無伺服器工作群組時，請指定工作群組名稱和資料庫名稱。資料庫的使用者名稱會衍生自 IAM 身分。例如，arn:iam::123456789012:user:foo 的資料庫使用者名稱為 IAM:foo。此外，也需要用來呼叫 redshift-serverless:GetCredentials 操作的許可。
- 以 IAM 身分連線至叢集時，請指定叢集識別碼和資料庫名稱。資料庫的使用者名稱會衍生自 IAM 身分。例如，arn:iam::123456789012:user:foo 的資料庫使用者名稱為 IAM:foo。此外，也需要用來呼叫 redshift:GetClusterCredentialsWithIAM 操作的許可。
- 以資料庫使用者身分連線至叢集時，請指定叢集識別碼、資料庫名稱和資料庫使用者名稱。此外，也需要用來呼叫 redshift:GetClusterCredentials 操作的許可。如需有關在使用此方法進行連線時要如何加入資料庫群組的資訊，請參閱[連線到叢集時加入資料庫群組](#)。

使用這些方法，您也可以提供指定資料所 AWS 區域 在位置的region值。

在呼叫 Amazon Redshift 資料 API 時映射 JDBC 資料類型

下表會將 Java Database Connectivity (JDBC) 資料類型對應至您在資料 API 呼叫中指定的資料類型。

JDBC 資料類型	資料 API 資料類型
INTEGER, SMALLINT, BIGINT	LONG
FLOAT, REAL, DOUBLE	DOUBLE
DECIMAL	STRING
BOOLEAN, BIT	BOOLEAN
BLOB, BINARY, LONGVARBINARY	BLOB

JDBC 資料類型	資料 API 資料類型
VARBINARY	STRING
CLOB	STRING
其他類型 (包含與日期和時間相關的類型)	STRING

字串值會傳遞至 Amazon Redshift 資料庫，並以隱含方式轉換為資料庫的資料類型。

Note

目前，資料 API 不支援通用唯一識別碼 (UUID) 的陣列。

在呼叫 Amazon Redshift 資料 API 時執行含有參數的 SQL 陳述式

您可以透過對 SQL 陳述式的各個部分使用參數來呼叫資料 API 操作，以控制提交給資料庫引擎的 SQL 文字。具名參數可讓您靈活地傳遞參數，而不必以硬式編碼的方式將其寫入 SQL 文字內。其可協助您重複使用 SQL 文字，並避免 SQL 隱碼攻擊問題。

下列範例顯示命 `execute-statement` AWS CLI 令 `parameters` 欄位的具名參數。

```
--parameters "[{"name": "id", "value": "1"}, {"name": "address", "value": "Seattle"}]"
```

在使用具名參數時，請考量下列事項：

- 具名參數只能用來取代 SQL 陳述式中的值。
 - 您可以取代 INSERT 陳述式中的值，例如 `INSERT INTO mytable VALUES (:val1)`。

具名參數可以是任何順序，並且可以在 SQL 文字中使用多次。前面範例中顯示的參數選項，1 和 Seattle 值會插入到資料表資料欄 id 和 address。在 SQL 文字中，您可以依下列方式指定具名參數：

```
--sql "insert into mytable values (:id, :address)"
```

- 您可以取代條件子句中的值，例如 `WHERE attr >= :val1`、`WHERE attr BETWEEN :val1 AND :val2` 和 `HAVING COUNT(attr) > :val`。

- 您無法取代 SQL 陳述式中的資料欄名稱，例如 SELECT column-name、ORDER BY column-name 或 GROUP BY column-name。

例如，下列 SELECT 陳述式會因為語法無效而失敗。

```
--sql "SELECT :colname, FROM event" --parameters "[{"name": "colname", "value": "eventname"}]"
```

如果使用錯誤的語法描述 (describe-statement 操作) 陳述式，則傳回的 QueryString 不會替代參數的資料欄名稱 ("QueryString": "SELECT :colname, FROM event")，並且會回報錯誤 (錯誤：在 "FROM"\n Position: 12 或附近有語法錯誤)。

- 您無法取代彙總函數中的資料欄名稱，例如 COUNT(column-name)、AVG(column-name) 或 SUM(column-name)。
- 您無法取代 JOIN 子句中的資料欄名稱。
- 當 SQL 執行時，資料會以隱含方式轉換為資料類型。如需資料類型轉換的相關資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的[資料類型](#)。
- 您無法將值設定為 NULL。資料 API 會將其解譯為常值字串 NULL。下列範例會將 id 取代為常值字串 null。不是 SQL NULL 值。

```
--parameters [{"name": "id", "value": "null"}]"
```

- 您無法設定零長度的值。資料 API SQL 陳述式會失敗。下列範例會嘗試使用零長度的值來設定 id，並導致 SQL 陳述式失敗。

```
--parameters [{"name": "id", "value": ""}]"
```

- 您無法使用參數在 SQL 陳述式中設定資料表名稱。資料 API 會遵循 JDBC PreparedStatement 的規則。
- describe-statement 操作的輸出會傳回 SQL 陳述式的查詢參數。
- 只有 execute-statement 操作會支援含有參數的 SQL 陳述式。

在呼叫 Amazon Redshift 資料 API 時執行含有等冪性字符的 SQL 陳述式

當您提出變動的 API 請求時，該請求一般會在操作的非同步工作流程完成之前傳回結果。即使請求已傳回結果，操作還是可能會在完成前就逾時或發生其他伺服器問題。這可能會讓您難以判斷請求是否成

功，而且可能導致系統多次重試以確保操作能成功完成。但是，如果原始請求和後續的重試有成功，則操作會完成多次。這表示您可能會更新比預期數量還多的資源。

等冪性可確保 API 請求不會完成超過一次。使用等冪請求時，如果原始請求成功完成，則任何後續的重試都會成功完成，而不必執行任何進一步的動作。資料 API `ExecuteStatement` 和 `BatchExecuteStatement` 操作具有選用的 `ClientToken` 等冪參數。`ClientToken` 會在 8 小時後到期。

Important

如果您從 AWS SDK 調用 `ExecuteStatement` 和 `BatchExecuteStatement` 操作，它會自動生成客戶端令牌以在重試時使用。在這種情況下，我們不建議將 `client-token` 參數與 `ExecuteStatement` 和 `BatchExecuteStatement` 操作搭配使用。檢視 CloudTrail 記錄以查看 `ClientToken`。如需記 CloudTrail 錄範例，請參閱 [Amazon Redshift 資料 API 範例](#)。

下面的 `execute-statement` AWS CLI 命令說明了冪等的可選 `client-token` 參數。

```
aws redshift-data execute-statement
  --region us-west-2
  --secret arn:aws:secretsmanager:us-west-2:123456789012:secret:myuser-secret-hKgPwn
  --cluster-identifier mycluster-test
  --sql "select * from stl_query limit 1"
  --database dev
  --client-token b855dced-259b-444c-bc7b-d3e8e33f94g1
```

下表顯示您可能會從等冪 API 請求得到的一些常見回應，並提供重試建議。

回應	建議	說明
200 (OK)	請勿重試	原始請求已成功完成。任何後續的重試都會成功傳回。
400 系列的回應碼	請勿重試	請求有下列方面的問題： <ul style="list-style-type: none"> 其包含無效的參數或參數組合。 其使用您沒有許可的動作或資源。 其使用處於變更狀態過程的資源。

回應	建議	說明
		如果請求涉及處於變更狀態過程的資源，則重試請求有可能會成功。
500 系列的回應碼	重試	該錯誤是由 AWS 服務器端問題引起的，通常是短暫的。請使用適當的退避策略來重複請求。

如需有關 Amazon Redshift 回應碼的資訊，請參閱《Amazon Redshift API 參考》中的[常見錯誤](#)。

授權 Amazon Redshift 資料 API 的存取

若要存取資料 API，使用者必須獲得授權。您可以透過將受管政策 (即預先定義的 AWS Identity and Access Management (IAM) 政策) 新增至該使用者，來授權其存取資料 API。我們建議的最佳實務是，將許可政策附加到 IAM 角色，然後根據需要將其指派給使用者和群組。如需詳細資訊，請參閱[Amazon Redshift 中的身分和存取管理](#)。若要查看受管政策允許和拒絕的許可，請參閱 IAM 主控台 (<https://console.aws.amazon.com/iam/>)。

Amazon Redshift 會提供 AmazonRedshiftDataFullAccess 受管政策。此政策可提供 Amazon Redshift 資料 API 操作的完整存取權。此政策還允許範圍存取特定的 Amazon Redshift 和 IAM API 操作 AWS Secrets Manager，以驗證和存取 Amazon Redshift 叢集或 Redshift 無伺服器工作群組所需的 IAM API 操作。

您也可以建立自己的 IAM 政策，以允許存取特定資源。若要建立您的政策，請使用 AmazonRedshiftDataFullAccess 政策作為起始範本。建立政策後，將它新增給每一位需要資料 API 存取的使用者。

請考量與使用者相關聯之 IAM 政策的下列要求：

- 如果您使 AWS Secrets Manager 用驗證，請確認政策允許使用 `secretsmanager:GetSecretValue` 動作擷取標記為金鑰的密碼 `RedshiftDataFullAccess`。
- 如果您使用暫時憑證對叢集進行身分驗證，請確認政策允許對叢集中任何資料庫的資料庫使用者名稱 `redshift_data_api_user` 使用 `redshift:GetClusterCredentials` 動作。此使用者名稱必須已建立在資料庫中。
- 如果您使用暫時憑證向無伺服器工作群組進行身分驗證，請確認政策允許使用 `redshift-serverless:GetCredentials` 動作來擷取以索引鍵 `RedshiftDataFullAccess` 標記的工作群組。資料庫使用者會將 1:1 對應至來源 AWS Identity and Access Management (IAM) 身分識別。

例如，使用者 `sample_user` 會映射至資料庫使用者 `IAM:sample_user`，而 IAM 角色 `sample_role` 會映射至 `IAMR:sample_role`。如需 IAM 身分的相關資訊，請參閱《IAM 使用者指南》中的 [IAM 身分 \(使用者、使用者群組和角色\)](#)。

若要在另一個帳戶擁有的叢集上執行查詢，擁有端帳戶必須提供資料 API 可在呼叫端帳戶中擔任的 IAM 角色。例如，假設帳戶 B 擁有帳戶 A 需要存取的叢集。帳戶 B 可將受 AWS 管政策附加 `AmazonRedshiftDataFullAccess` 到帳戶 B 的 IAM 角色。然後，帳戶 B 會使用信任政策來信任帳戶 A，如下所示：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::accountID-of-account-A:role/someRoleA"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

最後，帳戶 A 的 IAM 角色必須能夠擔任帳戶 B 的 IAM 角色。

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "sts:AssumeRole",
    "Resource": "arn:aws:iam::accountID-of-account-B:role/someRoleB"
  }
}
```

以下連結提供 IAM 使用者指南 AWS Identity and Access Management 中的詳細資訊。

- 如需有關建立 IAM 角色的資訊，請參閱 [建立 IAM 角色](#)。

- 如需有關建立 IAM 政策的資訊，請參閱[建立 IAM 政策](#)。
- 如需有關將 IAM 政策新增給使用者的資訊，請參閱[新增和移除 IAM 身分許可](#)。

將資料庫認證儲存於 AWS Secrets Manager

當您呼叫資料 API 時，您可以透過在 AWS Secrets Manager 中使用機密來傳遞叢集或無伺服器工作群組的憑證。若要這樣傳遞登入資料，請指定秘密的名稱或秘密的 Amazon Resource Name (ARN)。

若要使用 Secrets Manager 來儲存憑證，您需要 SecretManagerReadWrite 受管政策許可。如需有關最低權限的詳細資訊，請參閱 AWS Secrets Manager 使用指南中的使用 AWS [Secrets Manager 建立和管理密碼](#)。

將憑證儲存在 Amazon Redshift 叢集的機密中

1. 使用 AWS Secrets Manager 主控台建立包含叢集認證的密碼：
 - 當您選擇儲存新的機密時，請選擇 Redshift 叢集的憑證。
 - 將使用者名稱 (資料庫使用者)、密碼和資料庫叢集 (叢集識別碼) 的值儲存在機密中。
 - 使用索引鍵 RedshiftDataFullAccess 標記機密。AWS 受管政策 AmazonRedshiftDataFullAccess 只允許針對使用索引鍵 RedshiftDataFullAccess 標記的機密執行動作 `secretsmanager:GetSecretValue`。

如需說明，請參閱《AWS Secrets Manager 使用者指南》中的[建立基本秘密](#)。

2. 使用主 AWS Secrets Manager 控制台檢視您建立之密碼的詳細資料，或執行 `aws secretsmanager describe-secret` AWS CLI 命令。

記下秘密的名稱和 ARN。您可以在呼叫資料 API 時使用這些資料。

將憑證儲存在無伺服器工作群組的機密中

1. 使用 AWS Secrets Manager AWS CLI 命令儲存包含無伺服器工作群組認證的密碼：
 - 在檔案中建立您的秘密，例如名為 `mycreds.json` 的 JSON 檔案。在檔案中提供使用者名稱 (資料庫使用者) 和密碼的值。

```
{
  "username": "myusername",
  "password": "mypassword"
```

```
}
```

- 將值儲存在機密中，並使用索引鍵 `RedshiftDataFullAccess` 標記機密。

```
aws secretsmanager create-secret --name MyRedshiftSecret --tags
  Key="RedshiftDataFullAccess",Value="serverless" --secret-string file://
mycreds.json
```

以下將顯示輸出。

```
{
  "ARN":
  "arn:aws:secretsmanager:region:accountId:secret:MyRedshiftSecret-mvLHxf",
  "Name": "MyRedshiftSecret",
  "VersionId": "a1603925-e8ea-4739-9ae9-e509eEXAMPLE"
}
```

如需詳細資訊，請參閱《AWS Secrets Manager 使用者指南》中的[使用 AWS CLI 建立基本機密](#)。

2. 使用主 AWS Secrets Manager 控制台檢視您建立之密碼的詳細資料，或執行 `aws secretsmanager describe-secret` AWS CLI 命令。

記下秘密的名稱和 ARN。您可以在呼叫資料 API 時使用這些資料。

建立資料 API 的 Amazon VPC 端點 (AWS PrivateLink)

Amazon Virtual Private Cloud (Amazon VPC) 可讓您將 AWS 資源 (例如 Amazon Redshift 叢集和應用程式) 啟動到虛擬私有雲端 (VPC) 中。AWS PrivateLink 在 Amazon 網路上安全地在虛擬私有雲 (VPC) 和 AWS 服務之間提供私有連線。您可以使用 AWS PrivateLink 建立 VPC 端點，這能讓您根據 Amazon VPC 連線至不同帳戶與 VPC 的服務。如需有關的詳細資訊 AWS PrivateLink，請參閱 Amazon Virtual Private Cloud 使用者指南中的[VPC 端點服務 \(AWS PrivateLink\)](#)。

您可以使用 Amazon VPC 端點呼叫資料 API。使用 Amazon VPC 端點可保留 Amazon VPC 中的應用程式與 AWS 網路中的資料 API 之間的流量，而無需使用公有 IP 地址。Amazon VPC 端點能協助您符合與限制公有網際網路連線相關的合規和法律需求。舉例來說，若使用 Amazon VPC 端點，就能讓在 Amazon EC2 執行個體上執行之應用程式和資料 API 的流量，只在包含兩者的 VPC 中傳送。

建立 Amazon VPC 端點之後就能開始使用，而不需要在應用程式中進行任何程式碼或組態變更。

建立資料 API 的 Amazon VPC 端點

1. 登入 AWS Management Console 並開啟 Amazon VPC 主控台，網址為 <https://console.aws.amazon.com/vpc/>。
2. 選擇 Endpoints (端點)，然後選擇 Create Endpoint (建立端點)。
3. 在 Create Endpoint (建立端點) 頁面上，針對 Service category (服務類別) 選擇 AWS services (服務)。針對服務名稱，選擇 redshift-data (com.amazonaws.*region*.redshift-data)。
4. 針對 VPC，選擇要在其中建立端點的 VPC。

選擇包含進行資料 API 呼叫之應用程式的 VPC。

5. 對於子網路，請為執行應用程式的 AWS 服務所使用的每個可用區域 (AZ) 選擇子網路。

若要建立 Amazon VPC 端點，請指定可存取端點的私有 IP 地址範圍。若要執行此作業，請選擇每個可用區域的子網路。這麼做會將 VPC 端點限制為每個可用區域專屬的私有 IP 地址範圍，並且也會在每個可用區域中建立 Amazon VPC 端點。

6. 針對 Enable DNS name (啟用 DNS 名稱)，選取 Enable for this endpoint (為此端點啟用)。

私有 DNS 會將標準資料 API DNS 主機名稱 ([https://redshift-data.*region*.amazonaws.com](https://redshift-data.<i>region</i>.amazonaws.com)) 解析為與您 Amazon VPC 端點專用 DNS 主機名稱相關的私有 IP 地址。因此，您可以使用 AWS CLI 或 AWS SDK 存取資料 API VPC 人雲端節點，而無需進行任何程式碼或組態變更以更新資料 API 端點 URL。

7. 針對 Security group (安全群組)，選擇要與 Amazon VPC 端點建立關聯的安全群組。

選擇允許存取執行應用程式之 AWS 服務的安全性群組。舉例來說，若有 Amazon EC2 執行個體在執行您的應用程式，請選擇要允許存取 Amazon EC2 執行個體的安全群組。安全群組能讓您控制 VPC 中，資源流向 Amazon VPC 端點的流量。

8. 選擇建立端點。

建立端點後，選擇中的連結 AWS Management Console 以檢視端點詳細資訊。

端點 Details (詳細資訊) 標籤會顯示建立 Amazon VPC 端點時產生的 DNS 主機名稱。

您可以使用標準端點 ([redshift-data.*region*.amazonaws.com](https://redshift-data.<i>region</i>.amazonaws.com)) 或其中一個 VPC 專用端點，來在 Amazon VPC 中呼叫資料 API。標準資料 API 端點會自動路由至 Amazon VPC 端點。因為私有 DNS 主機名稱在 Amazon VPC 端點建立時已啟用，所以會發生此路由。

當您在資料 API 呼叫中使用 Amazon VPC 端點時，應用程式與資料 API 間的所有流量都會維持在包含兩者的 Amazon VPC 中。您可以使用 Amazon VPC 端點進行任何類型的資料 API 呼叫。如需呼叫資料 API 的詳細資訊，請參閱[呼叫 Amazon Redshift 資料 API 時的考量](#)。

連線到叢集時加入資料庫群組

資料庫群組是資料庫使用者的集合。您可以向群組授予資料庫權限。管理員可以設定 IAM 角色，以便在使用資料 API 執行 SQL 時將這些資料庫群組納入考量。如需資料庫群組的相關資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的[群組](#)。

您可以設定資料 API 呼叫者的 IAM 角色，以便在資料 API 連線到叢集時，呼叫中指定的資料庫使用者會加入資料庫群組。只有在連線至已佈建的叢集時才支援此功能。連線至 Redshift Serverless 工作群組時則不支援。資料 API 呼叫者的 IAM 角色也必須允許 `redshift:JoinGroup` 動作。

請透過向 IAM 角色新增標籤來進行此設定。呼叫者 IAM 角色的管理員會新增標籤，標籤中包含資料庫群組清單的索引鍵 `RedshiftDbGroups` 和索引鍵值。此值是以冒號 (:) 分隔的資料庫群組名稱清單，總長度最多可有 256 個字元。您必須之前就已在連線的資料庫中定義好資料庫群組。如果在資料庫中找不到任何指定的群組，則會忽略該群組。例如，對於資料庫群組 `accounting` 和 `retail`，索引鍵-值為 `accounting:retail`。資料 API 會使用標籤索引鍵-值組 `{"Key": "RedshiftDbGroups", "Value": "accounting:retail"}` 來判斷在呼叫資料 API 時，哪些資料庫群組會與所提供的資料庫使用者相關聯。

以標籤的形式將資料庫群組新增至 IAM 角色

1. 登入 AWS Management Console 並開啟 IAM 主控台，網址為 <https://console.aws.amazon.com/iam/>。
2. 在主控台導覽窗格中，選擇 Roles (角色)，然後選擇您要編輯的角色名稱。
3. 選擇標籤索引標籤，然後選擇管理標籤。
4. 選擇新增標記，然後新增索引鍵 `RedshiftDbGroups`，以及以冒號分隔的 `###` 群組清單的值。
5. 選擇儲存變更。

現在，當 IAM 主體 (附加了此 IAM 角色) 呼叫資料 API 時，指定的資料庫使用者便會加入 IAM 角色中指定的資料庫群組。

如需如何將標籤附加到主體 (包括 IAM 角色和 IAM 使用者) 的相關資訊，請參閱《IAM 使用者指南》中的[標記 IAM 資源](#)。

呼叫資料 API

您可以呼叫資料 API 或在叢集或無伺服器工作群組上執行 SQL 陳述式。AWS CLI 在《Amazon Redshift 資料 API 參考》中，用來執行 SQL 陳述式的主要操作是 [ExecuteStatement](#) 和 [BatchExecuteStatement](#)。資料 API 支援 AWS SDK 支援的程式設計語言。如需這些語言的相關資訊，請參閱[用來在 AWS 上進行建置的工具](#)。

若要查看呼叫資料 API 的程式碼範例，請參閱 [GitHub](#) 此儲存庫提供使用 AWS Lambda 從 Amazon EC2 和 Amazon SageMaker 執行階段存取亞馬遜 Redshift 資料的範例。AWS Glue Data Catalog 範例程式設計語言包括 Python、Go、Java 和 Javascript。

您可以使用 AWS CLI 呼叫資料 API。

下列範例使 AWS CLI 用呼叫資料 API。若要執行範例，請編輯參數值以符合您的環境。許多範例會提供 `cluster-identifier` 來針對叢集執行。當您針對無伺服器工作群組執行時，請改為提供 `workgroup-name`。這些範例會示範一些資料 API 操作。如需詳細資訊，請參閱 AWS CLI 命令參考。

下列範例中的命令已經過分割和格式化，以方便您閱讀。

執行 SQL 陳述式

若要執行 SQL 陳述式，請使用 `aws redshift-data execute-statement` AWS CLI 指令。

下列 AWS CLI 命令會針對叢集執行 SQL 陳述式，並傳回識別碼以擷取結果。此範例使用 AWS Secrets Manager 驗證方法。

```
aws redshift-data execute-statement
  --region us-west-2
  --secret arn:aws:secretsmanager:us-west-2:123456789012:secret:myuser-secret-hKgPwn
  --cluster-identifier mycluster-test
  --sql "select * from stl_query limit 1"
  --database dev
```

以下是回應的範例。

```
{
  "ClusterIdentifier": "mycluster-test",
  "CreatedAt": 1598323175.823,
  "Database": "dev",
  "Id": "c016234e-5c6c-4bc5-bb16-2c5b8ff61814",
```

```
"SecretArn": "arn:aws:secretsmanager:us-west-2:123456789012:secret:yanruiz-secret-
hKgPwn"
}
```

下列 AWS CLI 命令會針對叢集執行 SQL 陳述式，並傳回識別碼以擷取結果。此範例使用暫時憑證身分驗證方法。

```
aws redshift-data execute-statement
  --region us-west-2
  --db-user myuser
  --cluster-identifier mycluster-test
  --database dev
  --sql "select * from stl_query limit 1"
```

以下是回應的範例。

```
{
  "ClusterIdentifier": "mycluster-test",
  "CreatedAt": 1598306924.632,
  "Database": "dev",
  "DbUser": "myuser",
  "Id": "d9b6c0c9-0747-4bf4-b142-e8883122f766"
}
```

下列 AWS CLI 命令會針對無伺服器工作群組執行 SQL 陳述式，並傳回識別碼以擷取結果。此範例使用暫時憑證身分驗證方法。

```
aws redshift-data execute-statement
  --database dev
  --workgroup-name myworkgroup
  --sql "select 1;"
```

以下是回應的範例。

```
{
  "CreatedAt": "2022-02-11T06:25:28.748000+00:00",
  "Database": "dev",
  "DbUser": "IAM:RoleName",
  "Id": "89dd91f5-2d43-43d3-8461-f33aa093c41e",
}
```

```
"WorkgroupName": "myworkgroup"
}
```

下列 AWS CLI 命令會針對叢集執行 SQL 陳述式，並傳回識別碼以擷取結果。此範例使用 AWS Secrets Manager 驗證方法和冪等權杖。

```
aws redshift-data execute-statement
  --region us-west-2
  --secret arn:aws:secretsmanager:us-west-2:123456789012:secret:myuser-secret-hKgPwn
  --cluster-identifier mycluster-test
  --sql "select * from stl_query limit 1"
  --database dev
  --client-token b855dced-259b-444c-bc7b-d3e8e33f94g1
```

以下是回應的範例。

```
{
  "ClusterIdentifier": "mycluster-test",
  "CreatedAt": 1598323175.823,
  "Database": "dev",
  "Id": "c016234e-5c6c-4bc5-bb16-2c5b8ff61814",
  "SecretArn": "arn:aws:secretsmanager:us-west-2:123456789012:secret:yanruiz-secret-hKgPwn"
}
```

執行含有參數的 SQL 陳述式

若要執行 SQL 陳述式，請使用 `aws redshift-data execute-statement` AWS CLI 指令。

下列 AWS CLI 命令會針對叢集執行 SQL 陳述式，並傳回識別碼以擷取結果。此範例使用 AWS Secrets Manager 驗證方法。SQL 文字有具名參數 `distance`。在此案例中，述詞中使用的距離是 5。在 SELECT 陳述式中，資料欄名稱的具名參數只能在述詞中使用。SQL 陳述式的具名參數值會於 `parameters` 選項中指定。

```
aws redshift-data execute-statement
  --region us-west-2
  --secret arn:aws:secretsmanager:us-west-2:123456789012:secret:myuser-secret-hKgPwn
  --cluster-identifier mycluster-test
  --sql "SELECT ratecode FROM demo_table WHERE trip_distance > :distance"
  --parameters "[{\"name\": \"distance\", \"value\": \"5\"}]"
```

```
--database dev
```

以下是回應的範例。

```
{
  "ClusterIdentifier": "mycluster-test",
  "CreatedAt": 1598323175.823,
  "Database": "dev",
  "Id": "c016234e-5c6c-4bc5-bb16-2c5b8ff61814",
  "SecretArn": "arn:aws:secretsmanager:us-west-2:123456789012:secret:yanruiz-secret-
hKgPwn"
}
```

下列範例會使用來自範例資料庫的 EVENT 資料表。如需詳細資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的 [EVENT 資料表](#)。

如果資料庫中還沒有 EVENT 資料表，您可以使用資料 API 加以建立，如下所示：

```
aws redshift-data execute-statement
--database dev
--cluster-id my-test-cluster
--db-user awsuser
--sql "create table event( eventid integer not null distkey,
                           venueid smallint not null,
                           catid smallint not null,
                           dateid smallint not null sortkey,
                           eventname varchar(200),
                           starttime timestamp)"
```

下列命令會在 EVENT 資料表中插入一個資料列。

```
aws redshift-data execute-statement
--database dev
--cluster-id my-test-cluster
--db-user awsuser
--sql "insert into event
values(:eventid, :venueid::smallint, :catid, :dateid, :eventname, :starttime)"
--parameters "[{"name": "eventid", "value": "1"}, {"name": "venueid",
"value": "1"},
{"name": "catid", "value": "1"},
```

```
{\"name\": \"dateid\", \"value\": \"1\"},
{\"name\": \"eventname\", \"value\": \"event 1\"},
{\"name\": \"starttime\", \"value\": \"2022-02-22\"}]"
```

下列命令會在 EVENT 資料表中插入第二個資料列。此範例示範下列操作：

- 名為 id 的參數會在 SQL 文字中使用四次。
- 在插入參數 starttime 時會自動套用隱含類型轉換。
- venueid 資料欄是轉換為 SMALLINT 資料類型的類型。
- 代表 DATE 資料類型的字元字串會隱含地轉換成 TIMESTAMP 資料類型。
- 您可以在 SQL 文字中使用註解。

```
aws redshift-data execute-statement
--database dev
--cluster-id my-test-cluster
--db-user awsuser
--sql "insert into event values(:id, :id::smallint, :id, :id, :eventname, :starttime) /
*this is comment, and it won't apply parameterization for :id, :eventname or :starttime
here*/"
--parameters "[{\"name\": \"eventname\", \"value\": \"event 2\"},
                {\"name\": \"starttime\", \"value\": \"2022-02-22\"},
                {\"name\": \"id\", \"value\": \"2\"}]"
```

下列範例顯示所插入的兩個資料列：

eventid	venueid	catid	dateid	eventname	starttime
1	1	1	1	event 1	2022-02-22 00:00:00
2	2	2	2	event 2	2022-02-22 00:00:00

下列命令會在 WHERE 子句中使用具名參數來擷取 eventid 是 1 的資料列。

```
aws redshift-data execute-statement
--database dev
```

```
--cluster-id my-test-cluster
--db-user awsuser
--sql "select * from event where eventid=:id"
--parameters "[{"name": "id", "value": "1"}]"
```

執行下列命令以取得上一個 SQL 陳述式的 SQL 結果：

```
aws redshift-data get-statement-result --id 7529ad05-b905-4d71-9ec6-8b333836eb5a
```

提供下列結果：

```
{
  "Records": [
    [
      {
        "longValue": 1
      },
      {
        "longValue": 1
      },
      {
        "longValue": 1
      },
      {
        "longValue": 1
      },
      {
        "stringValue": "event 1"
      },
      {
        "stringValue": "2022-02-22 00:00:00.0"
      }
    ]
  ],
  "ColumnMetadata": [
    {
      "isCaseSensitive": false,
      "isCurrency": false,
      "isSigned": true,
      "label": "eventid",
    }
  ]
}
```



```
    "length": 0,
    "name": "eventid",
    "nullable": 0,
    "precision": 10,
    "scale": 0,
    "schemaName": "public",
    "tableName": "event",
    "typeName": "int4"
  },
  {
    "isCaseSensitive": false,
    "isCurrency": false,
    "isSigned": true,
    "label": "venueid",
    "length": 0,
    "name": "venueid",
    "nullable": 0,
    "precision": 5,
    "scale": 0,
    "schemaName": "public",
    "tableName": "event",
    "typeName": "int2"
  },
  {
    "isCaseSensitive": false,
    "isCurrency": false,
    "isSigned": true,
    "label": "catid",
    "length": 0,
    "name": "catid",
    "nullable": 0,
    "precision": 5,
    "scale": 0,
    "schemaName": "public",
    "tableName": "event",
    "typeName": "int2"
  },
  {
    "isCaseSensitive": false,
    "isCurrency": false,
    "isSigned": true,
    "label": "dateid",
    "length": 0,
    "name": "dateid",
```

```
        "nullable": 0,
        "precision": 5,
        "scale": 0,
        "schemaName": "public",
        "tableName": "event",
        "typeName": "int2"
    },
    {
        "isCaseSensitive": true,
        "isCurrency": false,
        "isSigned": false,
        "label": "eventname",
        "length": 0,
        "name": "eventname",
        "nullable": 1,
        "precision": 200,
        "scale": 0,
        "schemaName": "public",
        "tableName": "event",
        "typeName": "varchar"
    },
    {
        "isCaseSensitive": false,
        "isCurrency": false,
        "isSigned": false,
        "label": "starttime",
        "length": 0,
        "name": "starttime",
        "nullable": 1,
        "precision": 29,
        "scale": 6,
        "schemaName": "public",
        "tableName": "event",
        "typeName": "timestamp"
    }
],
"TotalNumRows": 1
}
```

執行多個 SQL 陳述式

若要使用一個命令執行多個 SQL 陳述式，請使用 `aws redshift-data batch-execute-statement` AWS CLI 命令。

下列 AWS CLI 命令會針對叢集執行三個 SQL 陳述式，並傳回識別碼以擷取結果。此範例使用暫時憑證身分驗證方法。

```
aws redshift-data batch-execute-statement
  --region us-west-2
  --db-user myuser
  --cluster-identifier mycluster-test
  --database dev
  --sqls "set timezone to BST" "select * from mytable" "select * from another_table"
```

以下是回應的範例。

```
{
  "ClusterIdentifier": "mycluster-test",
  "CreatedAt": 1598306924.632,
  "Database": "dev",
  "DbUser": "myuser",
  "Id": "d9b6c0c9-0747-4bf4-b142-e8883122f766"
}
```

列出有關 SQL 陳述式的中繼資料

若要列出有關 SQL 陳述式的中繼資料，請使用 `aws redshift-data list-statements` AWS CLI 指令。執行此命令的授權取決於呼叫者的 IAM 許可。

下列 AWS CLI 命令會列出執行的 SQL 陳述式。

```
aws redshift-data list-statements
  --region us-west-2
  --status ALL
```

以下是回應的範例。

```
{
  "Statements": [
    {
      "CreatedAt": 1598306924.632,
      "Id": "d9b6c0c9-0747-4bf4-b142-e8883122f766",
      "QueryString": "select * from stl_query limit 1",
    }
  ]
}
```

```

    "Status": "FINISHED",
    "UpdatedAt": 1598306926.667
  },
  {
    "CreatedAt": 1598311717.437,
    "Id": "e0ebd578-58b3-46cc-8e52-8163fd7e01aa",
    "QueryString": "select * from stl_query limit 1",
    "Status": "FAILED",
    "UpdatedAt": 1598311719.008
  },
  {
    "CreatedAt": 1598313683.65,
    "Id": "c361d4f7-8c53-4343-8c45-6b2b1166330c",
    "QueryString": "select * from stl_query limit 1",
    "Status": "ABORTED",
    "UpdatedAt": 1598313685.495
  },
  {
    "CreatedAt": 1598306653.333,
    "Id": "a512b7bd-98c7-45d5-985b-a715f3cfde7f",
    "QueryString": "select 1",
    "Status": "FINISHED",
    "UpdatedAt": 1598306653.992
  }
]
}

```

描述有關 SQL 陳述式的中繼資料

若要取得 SQL 陳述式中繼資料的描述，請使用 `aws redshift-data describe-statement` AWS CLI 指令。執行此命令的授權取決於呼叫者的 IAM 許可。

下面的 AWS CLI 命令描述了一個 SQL 語句。

```

aws redshift-data describe-statement
  --id d9b6c0c9-0747-4bf4-b142-e8883122f766
  --region us-west-2

```

以下是回應的範例。

```
{
```

```
"ClusterIdentifier": "mycluster-test",
"CreatedAt": 1598306924.632,
"Duration": 1095981511,
"Id": "d9b6c0c9-0747-4bf4-b142-e8883122f766",
"QueryString": "select * from stl_query limit 1",
"RedshiftPid": 20859,
"RedshiftQueryId": 48879,
"ResultRows": 1,
"ResultSize": 4489,
"Status": "FINISHED",
"UpdatedAt": 1598306926.667
}
```

以下是在執行含有多個 SQL 陳述式的 `batch-execute-statement` 命令後的 `describe-statement` 回應範例。

```
{
  "ClusterIdentifier": "mayo",
  "CreatedAt": 1623979777.126,
  "Duration": 6591877,
  "HasResultSet": true,
  "Id": "b2906c76-fa6e-4cdf-8c5f-4de1ff9b7652",
  "RedshiftPid": 31459,
  "RedshiftQueryId": 0,
  "ResultRows": 2,
  "ResultSize": 22,
  "Status": "FINISHED",
  "SubStatements": [
    {
      "CreatedAt": 1623979777.274,
      "Duration": 3396637,
      "HasResultSet": true,
      "Id": "b2906c76-fa6e-4cdf-8c5f-4de1ff9b7652:1",
      "QueryString": "select 1;",
      "RedshiftQueryId": -1,
      "ResultRows": 1,
      "ResultSize": 11,
      "Status": "FINISHED",
      "UpdatedAt": 1623979777.903
    },
    {
      "CreatedAt": 1623979777.274,
      "Duration": 3195240,
```

```

        "HasResultSet": true,
        "Id": "b2906c76-fa6e-4cdf-8c5f-4de1ff9b7652:2",
        "QueryString": "select 2;",
        "RedshiftQueryId": -1,
        "ResultRows": 1,
        "ResultSize": 11,
        "Status": "FINISHED",
        "UpdatedAt": 1623979778.076
    }
],
"UpdatedAt": 1623979778.183
}

```

擷取 SQL 陳述式的結果

若要從執行的 SQL 陳述式擷取結果，請使用 `redshift-data get-statement-result` AWS CLI 指令。您可以提供所收到的 `Id` 以回應 `execute-statement` 或 `batch-execute-statement`。由 `batch-execute-statement` 執行的 SQL 陳述式的 `Id` 值可以在 `describe-statement` 的結果中擷取，並且會加上由冒號和序號組成的字尾 (例如 `b2906c76-fa6e-4cdf-8c5f-4de1ff9b7652:2`)。如果您使用 `batch-execute-statement` 執行多個 SQL 陳述式，則每個 SQL 陳述式都會有一個 `Id` 值，如 `describe-statement` 中所示。執行此命令的授權取決於呼叫者的 IAM 許可。

下列陳述式會傳回由 `execute-statement` 執行的 SQL 陳述式的結果。

```

aws redshift-data get-statement-result
  --id d9b6c0c9-0747-4bf4-b142-e8883122f766
  --region us-west-2

```

下列陳述式會傳回由 `batch-execute-statement` 執行的第二個 SQL 陳述式的結果。

```

aws redshift-data get-statement-result
  --id b2906c76-fa6e-4cdf-8c5f-4de1ff9b7652:2
  --region us-west-2

```

以下是對於 `get-statement-result` 呼叫的回應範例。

```

{
  "ColumnMetadata": [

```

```
{
  "isCaseSensitive": false,
  "isCurrency": false,
  "isSigned": true,
  "label": "userid",
  "length": 0,
  "name": "userid",
  "nullable": 0,
  "precision": 10,
  "scale": 0,
  "schemaName": "",
  "tableName": "stll_query",
  "typeName": "int4"
},
{
  "isCaseSensitive": false,
  "isCurrency": false,
  "isSigned": true,
  "label": "query",
  "length": 0,
  "name": "query",
  "nullable": 0,
  "precision": 10,
  "scale": 0,
  "schemaName": "",
  "tableName": "stll_query",
  "typeName": "int4"
},
{
  "isCaseSensitive": true,
  "isCurrency": false,
  "isSigned": false,
  "label": "label",
  "length": 0,
  "name": "label",
  "nullable": 0,
  "precision": 320,
  "scale": 0,
  "schemaName": "",
  "tableName": "stll_query",
  "typeName": "bpchar"
},
{
  "isCaseSensitive": false,
```

```
    "isCurrency": false,
    "isSigned": true,
    "label": "xid",
    "length": 0,
    "name": "xid",
    "nullable": 0,
    "precision": 19,
    "scale": 0,
    "schemaName": "",
    "tableName": "stll_query",
    "typeName": "int8"
  },
  {
    "isCaseSensitive": false,
    "isCurrency": false,
    "isSigned": true,
    "label": "pid",
    "length": 0,
    "name": "pid",
    "nullable": 0,
    "precision": 10,
    "scale": 0,
    "schemaName": "",
    "tableName": "stll_query",
    "typeName": "int4"
  },
  {
    "isCaseSensitive": true,
    "isCurrency": false,
    "isSigned": false,
    "label": "database",
    "length": 0,
    "name": "database",
    "nullable": 0,
    "precision": 32,
    "scale": 0,
    "schemaName": "",
    "tableName": "stll_query",
    "typeName": "bpchar"
  },
  {
    "isCaseSensitive": true,
    "isCurrency": false,
    "isSigned": false,
```



```
    "label": "querytxt",
    "length": 0,
    "name": "querytxt",
    "nullable": 0,
    "precision": 4000,
    "scale": 0,
    "schemaName": "",
    "tableName": "stll_query",
    "typeName": "bpchar"
  },
  {
    "isCaseSensitive": false,
    "isCurrency": false,
    "isSigned": false,
    "label": "starttime",
    "length": 0,
    "name": "starttime",
    "nullable": 0,
    "precision": 29,
    "scale": 6,
    "schemaName": "",
    "tableName": "stll_query",
    "typeName": "timestamp"
  },
  {
    "isCaseSensitive": false,
    "isCurrency": false,
    "isSigned": false,
    "label": "endtime",
    "length": 0,
    "name": "endtime",
    "nullable": 0,
    "precision": 29,
    "scale": 6,
    "schemaName": "",
    "tableName": "stll_query",
    "type": 93,
    "typeName": "timestamp"
  },
  {
    "isCaseSensitive": false,
    "isCurrency": false,
    "isSigned": true,
    "label": "aborted",
```

```
    "length": 0,
    "name": "aborted",
    "nullable": 0,
    "precision": 10,
    "scale": 0,
    "schemaName": "",
    "tableName": "stll_query",
    "typeName": "int4"
  },
  {
    "isCaseSensitive": false,
    "isCurrency": false,
    "isSigned": true,
    "label": "insert_pristine",
    "length": 0,
    "name": "insert_pristine",
    "nullable": 0,
    "precision": 10,
    "scale": 0,
    "schemaName": "",
    "tableName": "stll_query",
    "typeName": "int4"
  },
  {
    "isCaseSensitive": false,
    "isCurrency": false,
    "isSigned": true,
    "label": "concurrency_scaling_status",
    "length": 0,
    "name": "concurrency_scaling_status",
    "nullable": 0,
    "precision": 10,
    "scale": 0,
    "schemaName": "",
    "tableName": "stll_query",
    "typeName": "int4"
  }
],
"Records": [
  [
    {
      "longValue": 1
    },
    {
```

```

        "longValue": 3
      },
      {
        "stringValue": "health"
      },
      {
        "longValue": 1023
      },
      {
        "longValue": 15279
      },
      {
        "stringValue": "dev"
      },
      {
        "stringValue": "select system_status from stv_gui_status;"
      },
      {
        "stringValue": "2020-08-21 17:33:51.88712"
      },
      {
        "stringValue": "2020-08-21 17:33:52.974306"
      },
      {
        "longValue": 0
      },
      {
        "longValue": 0
      },
      {
        "longValue": 6
      }
    ]
  ],
  "TotalNumRows": 1
}

```

描述資料表

若要取得描述資料表的中繼資料，請使用 `aws redshift-data describe-table` AWS CLI 指令。

下列 AWS CLI 命令會針對叢集執行 SQL 陳述式，並傳回描述資料表的中繼資料。此範例使用 AWS Secrets Manager 驗證方法。

```
aws redshift-data describe-table
  --region us-west-2
  --cluster-identifier mycluster-test
  --database dev
  --schema information_schema
  --table sql_features
  --secret arn:aws:secretsmanager:us-west-2:123456789012:secret:myuser-secret-hKgPwN
```

以下是回應的範例。

```
{
  "ColumnList": [
    {
      "isCaseSensitive": false,
      "isCurrency": false,
      "isSigned": false,
      "length": 2147483647,
      "name": "feature_id",
      "nullable": 1,
      "precision": 2147483647,
      "scale": 0,
      "schemaName": "information_schema",
      "tableName": "sql_features",
      "typeName": "character_data"
    },
    {
      "isCaseSensitive": false,
      "isCurrency": false,
      "isSigned": false,
      "length": 2147483647,
      "name": "feature_name",
      "nullable": 1,
      "precision": 2147483647,
      "scale": 0,
      "schemaName": "information_schema",
      "tableName": "sql_features",
      "typeName": "character_data"
    }
  ]
}
```

下列 AWS CLI 命令會針對描述資料表的叢集執行 SQL 陳述式。此範例使用暫時憑證身分驗證方法。

```
aws redshift-data describe-table
  --region us-west-2
  --db-user myuser
  --cluster-identifier mycluster-test
  --database dev
  --schema information_schema
  --table sql_features
```

以下是回應的範例。

```
{
  "ColumnList": [
    {
      "isCaseSensitive": false,
      "isCurrency": false,
      "isSigned": false,
      "length": 2147483647,
      "name": "feature_id",
      "nullable": 1,
      "precision": 2147483647,
      "scale": 0,
      "schemaName": "information_schema",
      "tableName": "sql_features",
      "typeName": "character_data"
    },
    {
      "isCaseSensitive": false,
      "isCurrency": false,
      "isSigned": false,
      "length": 2147483647,
      "name": "feature_name",
      "nullable": 1,
      "precision": 2147483647,
      "scale": 0,
      "schemaName": "information_schema",
      "tableName": "sql_features",
      "typeName": "character_data"
    },
    {
      "isCaseSensitive": false,
```

```
    "isCurrency": false,
    "isSigned": false,
    "length": 2147483647,
    "name": "sub_feature_id",
    "nullable": 1,
    "precision": 2147483647,
    "scale": 0,
    "schemaName": "information_schema",
    "tableName": "sql_features",
    "typeName": "character_data"
  },
  {
    "isCaseSensitive": false,
    "isCurrency": false,
    "isSigned": false,
    "length": 2147483647,
    "name": "sub_feature_name",
    "nullable": 1,
    "precision": 2147483647,
    "scale": 0,
    "schemaName": "information_schema",
    "tableName": "sql_features",
    "typeName": "character_data"
  },
  {
    "isCaseSensitive": false,
    "isCurrency": false,
    "isSigned": false,
    "length": 2147483647,
    "name": "is_supported",
    "nullable": 1,
    "precision": 2147483647,
    "scale": 0,
    "schemaName": "information_schema",
    "tableName": "sql_features",
    "typeName": "character_data"
  },
  {
    "isCaseSensitive": false,
    "isCurrency": false,
    "isSigned": false,
    "length": 2147483647,
    "name": "is_verified_by",
    "nullable": 1,
```

```
    "precision": 2147483647,
    "scale": 0,
    "schemaName": "information_schema",
    "tableName": "sql_features",
    "typeName": "character_data"
  },
  {
    "isCaseSensitive": false,
    "isCurrency": false,
    "isSigned": false,
    "length": 2147483647,
    "name": "comments",
    "nullable": 1,
    "precision": 2147483647,
    "scale": 0,
    "schemaName": "information_schema",
    "tableName": "sql_features",
    "typeName": "character_data"
  }
]
}
```

列出叢集中的資料庫

若要列出叢集中的資料庫，請使用 `aws redshift-data list-databases` AWS CLI 指令。

下列 AWS CLI 命令會針對叢集執行 SQL 陳述式，以列出資料庫。此範例使用 AWS Secrets Manager 驗證方法。

```
aws redshift-data list-databases
  --region us-west-2
  --secret arn:aws:secretsmanager:us-west-2:123456789012:secret:myuser-secret-hKgPwn
  --cluster-identifier mycluster-test
  --database dev
```

以下是回應的範例。

```
{
  "Databases": [
    "dev"
  ]
}
```

```
}
```

下列 AWS CLI 命令會針對叢集執行 SQL 陳述式，以列出資料庫。此範例使用暫時憑證身分驗證方法。

```
aws redshift-data list-databases
  --region us-west-2
  --db-user myuser
  --cluster-identifier mycluster-test
  --database dev
```

以下是回應的範例。

```
{
  "Databases": [
    "dev"
  ]
}
```

列出資料庫中的結構描述

若要列出資料庫中的結構描述，請使用 `aws redshift-data list-schemas` AWS CLI 指令。

下列 AWS CLI 命令會針對叢集執行 SQL 陳述式，以列出資料庫中的結構描述。此範例使用 AWS Secrets Manager 驗證方法。

```
aws redshift-data list-schemas
  --region us-west-2
  --secret arn:aws:secretsmanager:us-west-2:123456789012:secret:myuser-secret-hKgPwn
  --cluster-identifier mycluster-test
  --database dev
```

以下是回應的範例。

```
{
  "Schemas": [
    "information_schema",
    "pg_catalog",
  ]
}
```



```
    "pg_internal",
    "public"
  ]
}
```

下列 AWS CLI 命令會針對叢集執行 SQL 陳述式，以列出資料庫中的結構描述。此範例使用暫時憑證身分驗證方法。

```
aws redshift-data list-schemas
  --region us-west-2
  --db-user mysuser
  --cluster-identifier mycluster-test
  --database dev
```

以下是回應的範例。

```
{
  "Schemas": [
    "information_schema",
    "pg_catalog",
    "pg_internal",
    "public"
  ]
}
```

列出資料庫中的資料表

若要列出資料庫中的表格，請使用 `aws redshift-data list-tables` AWS CLI 指令。

下列 AWS CLI 命令會針對叢集執行 SQL 陳述式，以列出資料庫中的表格。此範例使用 AWS Secrets Manager 驗證方法。

```
aws redshift-data list-tables
  --region us-west-2
  --secret arn:aws:secretsmanager:us-west-2:123456789012:secret:mysuser-secret-hKgPwN
  --cluster-identifier mycluster-test
  --database dev
  --schema information_schema
```

以下是回應的範例。

```
{
  "Tables": [
    {
      "name": "sql_features",
      "schema": "information_schema",
      "type": "SYSTEM TABLE"
    },
    {
      "name": "sql_implementation_info",
      "schema": "information_schema",
      "type": "SYSTEM TABLE"
    }
  ]
}
```

下列 AWS CLI 命令會針對叢集執行 SQL 陳述式，以列出資料庫中的表格。此範例使用暫時憑證身分驗證方法。

```
aws redshift-data list-tables
  --region us-west-2
  --db-user myuser
  --cluster-identifier mycluster-test
  --database dev
  --schema information_schema
```

以下是回應的範例。

```
{
  "Tables": [
    {
      "name": "sql_features",
      "schema": "information_schema",
      "type": "SYSTEM TABLE"
    },
    {
      "name": "sql_implementation_info",
      "schema": "information_schema",
      "type": "SYSTEM TABLE"
    }
  ]
}
```

```
]
}
```

針對 Amazon Redshift 資料 API 的問題進行故障診斷

請使用下列標題包含常見錯誤訊息的章節，協助針對您在使用資料 API 時所發生的問題進行故障診斷。

主題

- [查詢封包過大](#)
- [資料庫回應超過大小上限](#)

查詢封包過大

如果您看到錯誤，內容指出查詢的封包太大，這一般是因為針對資料列傳回的結果集太大。針對資料庫傳回結果集中的每個資料列，資料 API 的大小上限為每個資料列 64 KB。

若要解決此問題，請確定結果集的每個資料列都是 64 KB 或更小。

資料庫回應超過大小上限

如果您看到錯誤，內容指出資料庫回應超過大小限制，這一般是因為資料庫傳回的結果集大小太大。針對資料庫傳回的結果集，資料 API 的大小上限為 100 MB。

若要解決此問題，請確認對資料 API 呼叫傳回的資料小於或等於 100 MB。若您需要傳回超過 100 MB，您可以在查詢中搭配 LIMIT 子句使用多個陳述式呼叫。

使用 Amazon 排程亞馬遜紅移資料 API 操作 EventBridge

您可以建立會比對所選事件並將其路由到目標以採取行動的規則。您也可以使用規則對預定的排程採取行動。如需詳細資訊，請參閱 [Amazon EventBridge 使用者指南](#)。

若要使用排程資料 API 作業 EventBridge，相關聯的 IAM 角色必須信任事件的主體 (CloudWatch 事件 .amazonaws.com)。此角色應該要有已附加之受管政策 AmazonEventBridgeFullAccess 的對等項目。其也應該要有由資料 API 管理的 AmazonRedshiftDataFullAccess 政策許可。您可以在 IAM 主控台上使用這些許可建立 IAM 角色。在 IAM 主控台上建立角色時，請為 CloudWatch 事件選擇 AWS 服務受信任實體。在 EventBridge 目標的 RoleArn JSON 值中指定 IAM 角色。如需建立 IAM 角色的詳細資訊，請參閱 IAM 使用者指南中的 [建立 AWS 服務角色 \(主控台\)](#)。

您在 Amazon 中創建的規則 EventBridge 必須與 StatementName 中的 RedshiftDataParameters.name

下列範例顯示使用單一或多個 SQL 陳述式建立 EventBridge 規則，以及使用 Amazon Redshift 叢集或 Amazon Redshift 無伺服器工作群組做為資料倉儲來建立規則的變化。

使用單一 SQL 陳述式和叢集來進行呼叫

下列範例會使 AWS CLI 用建立 EventBridge 規則，該規則用來針對 Amazon Redshift 叢集執行 SQL 陳述式。

```
aws events put-rule
--name test-redshift-cluster-data
--schedule-expression "rate(1 minute)"
```

然後會建立一個 EventBridge 目標，以按照規則中指定的排程執行。

```
aws events put-targets
--cli-input-json file://data.json
```

data.json 輸入檔案如下。Sql JSON 索引鍵表示有單一 SQL 陳述式。Arn JSON 值包含叢集識別碼。RoleArn JSON 值包含用來執行 SQL 的 IAM 角色，如先前所述。

```
{
  "Rule": "test-redshift-cluster-data",
  "EventBusName": "default",
  "Targets": [
    {
      "Id": "2",
      "Arn": "arn:aws:redshift:us-east-1:123456789012:cluster:mycluster",
      "RoleArn": "arn:aws:iam::123456789012:role/Administrator",
      "RedshiftDataParameters": {
        "Database": "dev",
        "DbUser": "root",
        "Sql": "select 1;",
        "StatementName": "test-redshift-cluster-data",
        "WithEvent": true
      }
    }
  ]
}
```

使用單一 SQL 陳述式和工作群組來進行呼叫

下列範例會使 AWS CLI 用建立 EventBridge 規則，以針對 Amazon Redshift 無伺服器工作群組執行 SQL 陳述式。

```
aws events put-rule
--name test-redshift-serverless-workgroup-data
--schedule-expression "rate(1 minute)"
```

然後會建立一個 EventBridge 目標，以按照規則中指定的排程執行。

```
aws events put-targets
--cli-input-json file://data.json
```

data.json 輸入檔案如下。Sql JSON 索引鍵表示有單一 SQL 陳述式。Arn JSON 值包含工作群組名稱。RoleArn JSON 值包含用來執行 SQL 的 IAM 角色，如先前所述。

```
{
  "Rule": "test-redshift-serverless-workgroup-data",
  "EventBusName": "default",
  "Targets": [
    {
      "Id": "2",
      "Arn": "arn:aws:redshift-serverless:us-east-1:123456789012:workgroup/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
      "RoleArn": "arn:aws:iam::123456789012:role/Administrator",
      "RedshiftDataParameters": {
        "Database": "dev",
        "Sql": "select 1;",
        "StatementName": "test-redshift-serverless-workgroup-data",
        "WithEvent": true
      }
    }
  ]
}
```

使用多個 SQL 陳述式和叢集進行呼叫

下列範例使用建 AWS CLI 立 EventBridge 規則，該規則用於對 Amazon Redshift 叢集執行多個 SQL 陳述式。

```
aws events put-rule
```

```
--name test-redshift-cluster-data
--schedule-expression "rate(1 minute)"
```

然後會建立一個 EventBridge 目標，以按照規則中指定的排程執行。

```
aws events put-targets
--cli-input-json file://data.json
```

data.json 輸入檔案如下。Sqls JSON 索引鍵表示有多個 SQL 陳述式。Arn JSON 值包含叢集識別碼。RoleArn JSON 值包含用來執行 SQL 的 IAM 角色，如先前所述。

```
{
  "Rule": "test-redshift-cluster-data",
  "EventBusName": "default",
  "Targets": [
    {
      "Id": "2",
      "Arn": "arn:aws:redshift:us-east-1:123456789012:cluster:mycluster",
      "RoleArn": "arn:aws:iam::123456789012:role/Administrator",
      "RedshiftDataParameters": {
        "Database": "dev",
        "Sqls": ["select 1;", "select 2;", "select 3;"],
        "StatementName": "test-redshift-cluster-data",
        "WithEvent": true
      }
    }
  ]
}
```

使用多個 SQL 陳述式和工作群組進行呼叫

下列範例使用建立 EventBridge 規則，該規則用於對 Amazon Redshift 無伺服器工作群組執行多個 SQL 陳述式。AWS CLI

```
aws events put-rule
--name test-redshift-serverless-workgroup-data
--schedule-expression "rate(1 minute)"
```

然後會建立一個 EventBridge 目標，以按照規則中指定的排程執行。

```
aws events put-targets
```

```
--cli-input-json file://data.json
```

data.json 輸入檔案如下。Sqls JSON 索引鍵表示有多個 SQL 陳述式。Arn JSON 值包含工作群組名稱。RoleArn JSON 值包含用來執行 SQL 的 IAM 角色，如先前所述。

```
{
  "Rule": "test-redshift-serverless-workgroup-data",
  "EventBusName": "default",
  "Targets": [
    {
      "Id": "2",
      "Arn": "arn:aws:redshift-serverless:us-east-1:123456789012:workgroup/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
      "RoleArn": "arn:aws:iam::123456789012:role/Administrator",
      "RedshiftDataParameters": {
        "Database": "dev",
        "Sqls": ["select 1;", "select 2;", "select 3;"],
        "StatementName": "test-redshift-serverless-workgroup-data",
        "WithEvent": true
      }
    }
  ]
}
```

監控資料 API

監控是維持 Data API 和其他 AWS 解決方案的可靠性、可用性和效能的重要組成部分。AWS 提供下列監控工具來觀看 Data API、在發生錯誤時報告，並在適當時採取自動動作：

- Amazon EventBridge 可用於自動化 AWS 服務並自動回應系統事件，例如應用程式可用性問題或資源變更。來自 AWS 服務的事件會以近乎即時 EventBridge 的方式傳遞到。您可編寫簡單的規則，來指示您在意的事件，以及當事件符合規則時所要自動執行的動作。如需詳細資訊，請參閱 [Amazon EventBridge 使用者指南](#)。
- AWS CloudTrail 擷取您帳戶或代表您 AWS 帳戶發出的 API 呼叫和相關事件，並將日誌檔傳送到您指定的 Amazon S3 儲存貯體。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。若要進一步了解 Amazon Redshift 與之整合的方式 AWS CloudTrail，請參閱 [使用 CloudTrail](#)。若要取得有關的更多資訊 CloudTrail，請參閱 [AWS CloudTrail 使用者指南](#)。

主題

- [在 Amazon 中監控 Amazon Redshift 數據 API 的事件 EventBridge](#)

在 Amazon 中監控 Amazon Redshift 數據 API 的事件 EventBridge

您可以監控中的 Data API 事件 EventBridge，從您自己的應用程式、software-as-a-service (SaaS) 應用程式和 AWS 服務提供即時資料串流。EventBridge 將資料路由到目標 (例如 AWS Lambda 和 Amazon SNS)。這些事件與 Events 中出現的 CloudWatch 事件相同，它提供了描述資源變更的系統事件的近乎即時 AWS 資料流。事件會傳送至包含 Amazon Redshift 資料庫的帳戶。例如，如果您在另一個帳戶中擔任某個角色，事件便會傳送至該帳戶。如需詳細資訊，請參閱 [Amazon EventBridge 使用者指南中的 Amazon EventBridge 事件](#)。

當 ExecuteStatement 或 BatchExecuteStatement API 操作將 WithEvents 選項設定為 true 時，系統就會傳送資料 API 事件。事件的 state 欄位會包含下列其中一個值：

- 已中止 — 使用者已停止執行查詢。
- 失敗 — 查詢執行失敗。
- 已完成 — 查詢已執行完成。

系統保證會提供事件。如需詳細資訊，請參閱 Amazon EventBridge 使用者指南中的 [來自 AWS 服務的事件](#)。

資料 API 的已完成事件範例

下列範例顯示當 ExecuteStatement API 操作完成時的資料 API 事件。在此範例中，名為 test.testtable 的陳述式已執行完成。

```
{
  "version": "0",
  "id": "18e7079c-dd4b-dd64-caf9-e2a31640dab0",
  "detail-type": "Redshift Data Statement Status Change",
  "source": "aws.redshift-data",
  "account": "123456789012",
  "time": "2020-10-01T21:14:26Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:redshift:us-east-1:123456789012:cluster:redshift-cluster-1"
  ],
  "detail": {
    "principal": "arn:aws:iam::123456789012:user/myuser",
    "statementName": "test.testtable",
```



```
    "statementId": "dd2e1ec9-2ee3-49a0-819f-905fa7d75a4a",
    "redshiftQueryId": -1,
    "state": "FINISHED",
    "rows": 1,
    "expireAt": 1601673265
  }
}
```

Amazon Redshift 參數群組

概觀

在 Amazon Redshift 中，您可以將參數群組與您建立的每個叢集建立關聯。參數群組為參數的群組，這些參數會套用至您在叢集中建立的所有資料庫。這些參數用於設定查詢逾時和日期樣式等資料庫設定。

關於參數群組

每個參數群組都有多個參數，用於設定資料庫的設定。可用的參數群組清單視參數群組所屬的參數群組系列而定。參數群組系列為參數群組中參數所套用的 Amazon Redshift 引擎版本。參數群組系列名稱的格式為 `redshift-version`，其中 *version* 是引擎版本。例如，組態的目前版本是 `redshift-1.0`。

Amazon Redshift 為每個參數群組系列提供一個預設的參數群組。預設參數群組的每個參數都有預設的數值，無法修改。預設參數群組名稱的格式為 `default.parameter_group_family`，其中 *parameter_group_family* 為參數群組所屬引擎的版本。舉例來說，`redshift-1.0` 版本的預設參數群組名稱為 `default.redshift-1.0`。

Note

目前，`redshift-1.0` 為 Amazon Redshift 引擎的唯一版本。因此，`default.redshift-1.0` 為唯一的預設參數群組。

如果您想使用非預設參數群組的其他參數值，您必須建立自訂參數群組，然後將叢集與群組相關聯。自訂參數群組中的參數值一開始與預設參數群組中的相同。所有參數的初始 `source` 是 `engine-default`，因為值是由 Amazon Redshift 預設。變更參數值後，`source` 將變更為 `user`，表示數值經過修改，不同於預設值。

Note

Amazon Redshift 主控台不會顯示每個參數的 `source`。您必須使用 Amazon Redshift API、AWS CLI、或其中一個 AWS 開發套件來檢視 `source`。

如為您建立的參數群組，您可以隨時修改其參數值，或將所有參數值重設為預設值。也可將不同的參數群組與叢集相關聯。在某些情況下，您可能修改已與叢集相關聯的參數群組中的參數值，或將不同參數群組與叢集建立關聯。在這些情況下，您可能需要重新啟動叢集，更新的參數值才會生效。如果叢集失敗，而且 Amazon Redshift 重新啟動叢集，變更將在此時套用。如果叢集在維護期間重新啟動，則不會套用變更。如需詳細資訊，請參閱 [WLM 動態和靜態屬性](#)。

預設參數值

下表顯示預設參數值的概覽，包含各參數深入資訊的連結。這些是 redshift-1.0 參數群組系列的預設值。

參數名稱	Value	其他資訊
auto_analyze	true	《Amazon Redshift 資料庫開發人員指南》中的 auto_analyze
auto_mv	true	《Amazon Redshift 資料庫開發人員指南》中的 自動具體化視觀表
datestyle	ISO、MDY	《Amazon Redshift 資料庫開發人員指南》中的 datestyle
enable_case_sensitive_identifier	false	《Amazon Redshift 資料庫開發人員指南》中的 enable_case_sensitive_identifier
enable_user_activity_logging	false	本指南中的 資料庫稽核記錄日誌
extra_float_digits	0	《Amazon Redshift 資料庫開發人員指南》中的 extra_float_digits
max_concurrency_scaling_clusters	1	《Amazon Redshift 資料庫開發人員指南》中的 max_concurrency_scaling_clusters
query_group	預設	《Amazon Redshift 資料庫開發人員指南》中的 query_group
require_ssl	false	本指南中的 設定連線的安全選項

參數名稱	Value	其他資訊
search_path	\$user、public	《Amazon Redshift 資料庫開發人員指南》中的 search_path
statement_timeout	0	《Amazon Redshift 資料庫開發人員指南》中的 statement_timeout
wlm_json_configuration	[{"auto_wlm":true}]	本指南中的 設定工作負載管理
use_fips_ssl	false	只在系統需要符合 FIPS 時啟用與 FIPS 相容的 SSL 模式。

Note

max_cursor_result_set_size 參數已棄用。如需游標結果集大小的相關資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的 [游標限制條件](#)。

您可在資料庫中使用 SET 命令暫時覆寫參數。SET 命令僅覆寫表示目前工作階段持續時間的參數。除了上表列出的參數，您也可設定資料庫中的 wlm_query_slot_count 來暫時調整槽計數。wlm_query_slot_count 參數不適用於參數群組中的組態。如需調整插槽計數的相關資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的 [wlm_query_slot_count](#)。如需暫時覆寫其他參數的相關資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的 [修改伺服器組態](#)。

使用配置參數值 AWS CLI

若要使用設定 Amazon Redshift 參數 AWS CLI，您可以針對特定參數群組使用 modify-cluster-parameter-group 命令。在 parameter-group-name 中指定要修改的參數群組。您可用 parameters 參數 (用於 modify-cluster-parameter-group 命令) 指定參數群組中您想要修改之各參數的名稱/值對。

Note

使用 AWS CLI 設定 `wlm_json_configuration` 參數時有特殊考量。本節中的範例適用於除了 `wlm_json_configuration` 之外的所有參數。若要取得有關使用 `wlm_json_configuration` 行配置的更多資訊 AWS CLI，請參閱 [設定工作負載管理](#)。

修改參數值後，您必須重新啟動與修改過的參數群組相關聯的任何叢集。applying 的叢集狀態在套用值時會顯示 `ParameterApplyStatus`，套用結束後則顯示 `pending-reboot`。重新啟動後，叢集內的資料庫便會開始使用新的參數值。如需重新啟動叢集的相關資訊，請參閱 [重新啟動叢集](#)。

Note

`wlm_json_configuration` 參數包含部分的動態屬性，因此不需為了套用變更而重新啟動相關聯的叢集。如需動態和靜態屬性的相關資訊，請參閱 [WLM 動態和靜態屬性](#)。

語法

下列語法圖表顯示如何使用 `modify-cluster-parameter-group` 命令設定參數。您可指定 `parameter_group_name`，並將 `parameter_name` 和 `parameter_value` 換成要修改的實際參數和該參數的值。如果想同時修改一個以上的參數，請用空格分隔各個參數和值組。

```
aws redshift modify-cluster-parameter-group --parameter-group-name parameter_group_name
--parameters ParameterName=parameter_name,ParameterValue=parameter_value
```

範例

下列範例說明如何設定 `statement_timeout` 參數群組的 `enable_user_activity_logging` 和 `myclusterparametergroup` 參數。

Note

為了便於閱讀，該示例顯示在幾行上，但實際上 AWS CLI 這是一行。

```
aws redshift modify-cluster-parameter-group
--parameter-group-name myclusterparametergroup
```

```
--parameters ParameterName=statement_timeout,ParameterValue=20000  
ParameterName=enable_user_activity_logging,ParameterValue=true
```

您可以使用主控台管理參數群組。如需詳細資訊，請參閱 [使用主控台來管理參數群組](#)。

設定工作負載管理

您可在 Amazon Redshift 中用工作負載管理 (WLM) 定義可用的查詢佇列數量，以及查詢如何路由至佇列進行處理。WLM 為參數群組組態的一部分。叢集將使用在其相關聯參數群組中指定的 WLM 組態。

建立參數群組時，預設的 WLM 組態將包含一個佇列，其最多可同時執行五個查詢。如果您想更有效地控制查詢處理功能，可新增其他佇列並設定其各自的 WLM 屬性。您所新增的每個佇列都會擁有相同的預設 WLM 組態，除非您設定其屬性。

新增額外的佇列時，組態中最後一個佇列為預設佇列。除非查詢依照 WLM 組態中的條件路由至其他佇列，否則皆由預設佇列處理。您可以為預設佇列指定模式和並行層級 (查詢槽)，但無法指定預設佇列的使用者群組或查詢群組。

如同其他參數，您也無法修改預設參數群組中的 WLM 組態。與預設參數群組相關聯的叢集永遠使用預設的 WLM 組態。若要修改 WLM 組態，請建立新的參數群組，然後將該參數群組與需要自訂 WLM 組態的任何叢集相關聯。

WLM 動態和靜態屬性

WLM 屬性分為動態和靜態兩種。您可在不重新啟動叢集的情形下，將動態屬性套用至資料庫，但靜態屬性需要重新啟動叢集才能讓變更生效。如需動態和靜態組態屬性的相關資訊，請參閱 [WLM 動態和靜態組態屬性](#)。

wlm_json_configuration 參數的屬性

您可以使用 Amazon Redshift 主控台、亞馬 Amazon Redshift API 或其中一個開發套件來設定 WLM。AWS CLI AWS WLM 組態使用多項屬性定義佇列行為，例如跨佇列的記憶體配置、佇列中可同時執行的查詢數量等。

Note

以下顯示屬性將同時在說明中列出其 Amazon Redshift 主控台名稱，以及對應的 JSON 屬性名稱。

下表摘要顯示屬性適用於自動 WLM 或是手動 WLM。

WLM 屬性	自動 WLM	手動 WLM
Auto WLM (自動 WLM)	是	是
啟用短期查詢加速	是	是
短期查詢最長執行時間	是	是
優先順序	是	否
佇列類型	是	是
佇列名稱	是	是
並行擴展模式	是	是
並行數量	否	是
使用者群組	是	是
使用者群組萬用字元	是	是
查詢群組	是	是
查詢群組萬用字元	是	是
使用者角色	是	是
使用者角色萬用字元	是	是
逾時	否	已棄用
記憶體	否	是
查詢監控規則	是	是

下列清單說明您可以設定的 WLM 屬性。

Auto WLM (自動 WLM)

Auto WLM (自動 WLM) 設為 `true` 可啟用自動 WLM。自動 WLM 會將主體的並行和記憶體 (%) 的值設為 `Auto`。Amazon Redshift 可管理查詢並行和記憶體配置。預設值為 `true`。

JSON 屬性：`auto_wlm`

Enable short query acceleration (啟用短期查詢加速)

短期查詢加速 (SQA) 可排定讓短期執行的查詢優先於長期執行的查詢。SQA 會在專用佇列中執行短期查詢，所以 SQA 查詢不會被迫在佇列中排在長期查詢後面等待。SQA 可讓短期執行的查詢更快開始執行，使用者會更快看到結果。啟用 SQA 時，您也可以指定短期查詢的最長執行時間。若要啟用 SQA，請使用 `true`。預設值為 `false`。此設定適用於每個參數群組，而不是佇列。

JSON 屬性：`short_query_queue`

短期查詢最長執行時間

啟用 SQA 時，您可指定 0，讓 WLM 動態設定短期查詢的最長執行時間。或者，您也可以指定 1–20 秒 (以毫秒為單位) 的值。預設值為 0。

JSON 屬性：`max_execution_time`

優先順序

優先順序設定在佇列中執行之查詢的優先順序。若要設定優先順序，WLM mode (WLM 模式) 必須設定為 Auto WLM (自動 WLM)；也就是說，`auto_wlm` 必須是 `true`。優先順序值可以是 `highest`、`high`、`normal`、`low` 和 `lowest`。預設值為 `normal`。

JSON 屬性：`priority`

佇列類型

佇列類型指定佇列由 Auto WLM (自動 WLM) 或 Manual WLM (手動 WLM) 使用。將 `queue_type` 設定為 `auto` 或 `manual`。若沒有指定，則預設為 `manual`。

JSON 屬性：`queue_type`

佇列名稱

佇列的名稱。您可以根據商業需求設定佇列名稱。佇列名稱在 WLM 組態內必須是唯一的，最多可包含 64 個英數字元、底線或空格，且不能包含引號。例如，如果您有 ETL 查詢的佇列，則可以將其命名為 `ETL queue`。此名稱用於指標、系統資料表值和 Amazon Redshift 主控台中，以

識別佇列。使用來自這些來源之名稱的查詢和報告必須能夠處理名稱的變更。先前，佇列名稱是由 Amazon Redshift 產生的。佇列的預設名稱是 Queue 1、Queue 2 到最後一個名為 Default queue 的佇列。

Important

如果您變更佇列名稱，WLM 佇列測量結果 (例如 WLM、WLM QueueWait 時間 QueueLength、WLM、WLM、WLM QueriesCompleted PerSecond 等) 的 QueueName 維度值也會變更。QueryDuration RunningQueries 因此，如果您變更佇列的名稱，您可能需要變更已設定的 CloudWatch 警示。

JSON 屬性：name

Concurrency Scaling mode (並行擴展模式)

若要啟用佇列的並行擴展，請將 Concurrency Scaling mode (並行擴展模式) 設定為 auto。當路由至佇列的查詢數量超過佇列設定的並行時，合格查詢將前往擴展叢集。當有可用的空位時，查詢會執行於主要叢集。預設值為 off。

JSON 屬性：concurrency_scaling

並行數量

手動 WLM 佇列中可同時執行的查詢數量。此屬性僅適用於手動 WLM。如果並行擴展已啟用，當佇列達到並行層級 (查詢槽) 時，合格查詢將前往擴展叢集。如果並行擴展未啟用，查詢會在佇列中等待，直到有空位為止。範圍介於 1 與 50 之間。

JSON 屬性：query_concurrency

User Groups (使用者群組)

逗號分隔的使用者群組名稱清單。使用者群組的成員在資料庫內執行查詢時，其查詢會路由至與其使用者群組相關聯的佇列。

JSON 屬性：user_group

User Group Wildcard (使用者群組萬用字元)

布林值類型，用以指示是否啟用使用者群組的萬用字元。如果為 0，表示萬用字元為停用；如果為 1，表示萬用字元為啟用。當萬用字元啟用時，您可以在執行查詢時使用 "*" 或 "?" 來指定多個使用者群組。如需詳細資訊，請參閱 [萬用字元](#)。

JSON 屬性：user_group_wild_card

Query Groups (查詢群組)

逗號分隔的查詢群組清單。查詢群組的成員在資料庫內執行查詢時，其查詢會路由至與其查詢群組相關聯的佇列。

JSON 屬性：query_group

Query Group Wildcard (查詢群組萬用字元)

布林值類型，用以指示是否啟用查詢群組的萬用字元。如果為 0，表示萬用字元為停用；如果為 1，表示萬用字元為啟用。當萬用字元啟用時，您可以在執行查詢時使用 "*" 或 "?" 來指定多個查詢群組。如需詳細資訊，請參閱[萬用字元](#)。

JSON 屬性：query_group_wild_card

使用者角色

逗號分隔的使用者角色清單。具有該使用者角色的成員在資料庫內執行查詢時，其查詢會路由至與其使用者角色相關聯的佇列。如需使用者角色的相關資訊，請參閱[角色型存取控制 \(RBAC\)](#)。

JSON 屬性：user_role

使用者角色萬用字元

布林值類型，用以指示是否啟用查詢群組的萬用字元。如果為 0，表示萬用字元為停用；如果為 1，表示萬用字元為啟用。當萬用字元啟用時，您可以在執行查詢時使用 "*" 或 "?" 來指定多個查詢群組。如需詳細資訊，請參閱[萬用字元](#)。

JSON 屬性：user_role_wild_card

Timeout (ms) (逾時 (毫秒))

WLM 逾時 (max_execution_time) 已作廢。使用自動 WLM 時無法使用此功能。這時請改成使用 query_execution_time 建立查詢監控規則 (QMR)，以限制查詢的經歷執行時間。如需詳細資訊，請參閱[WLM 查詢監控規則](#)。

查詢遭取消前所能執行的最長時間 (毫秒)。在某些情況下，唯讀查詢 (例如 SELECT 陳述式) 可能因為 WLM 逾時而被取消。在這些情況下，WLM 會嘗試根據 WLM 佇列指派規則，將查詢路由至下一個相符的佇列。如果查詢不符合任何的佇列定義，此查詢將取消；不會指派給預設佇列。如需詳細資訊，請參閱[WLM 查詢佇列跳轉](#)。WLM 逾時不會套用到已達到 returning 狀態的查詢。若要檢視查詢的狀態，請參閱[STV_WLM_QUERY_STATE](#) 系統資料表。

JSON 屬性：max_execution_time


Memory (%) (記憶體 (%))

配置給佇列的記憶體百分比。若您要為至少一個佇列指定記憶體百分比，您必須為所有其他佇列指定總共 100% 的記憶體。如果所有佇列合計的記憶體配置低於 100%，則未配置的記憶體由該服務管理。該服務可將未配置的記憶體，暫時提供給需要更多記憶體來處理的佇列。

JSON 屬性：memory_percent_to_use

查詢監控規則

您可以使用 WLM 查詢監控規則依照指定的條件或述詞持續監控查詢的 WLM 佇列。例如，您可監控經常使用過多系統資源的查詢，並在查詢超過指定的效能邊界時啟動指定動作。

 Note

如果您選擇以程式設計方式建立規則，強烈建議您使用主控台來產生 JSON，再加入參數群組定義中。

您需將查詢監控規則與特定的查詢佇列相關聯。每個佇列最多可以有 25 個規則，而全部佇列合計最多 25 規則。

JSON 屬性：rules

JSON 屬性階層：

```
rules
  rule_name
  predicate
    metric_name
    operator
    value
  action
    value
```

針對每個規則，您指定下列屬性：

- rule_name — 規則名稱在 WLM 組態內必須是唯一的。規則名稱最多為 32 個英數字元或底線，且不可含有空格和問號。
- predicate — 每個規則最多可以有三個述詞。針對每個述詞，您指定下列屬性。

- `metric_name` — 如需指標清單，請參閱《Amazon Redshift 資料庫開發人員指南》中的[查詢監控指標](#)。
- `operator` — 運算子為 =、< 和 >。
- `value` — 觸發動作之指定指標的閾值。
- `action` — 每個規則都與一個動作相關聯。有效的動作為：
 - `log`
 - `hop` (僅適用於手動 WLM)
 - `abort`
 - `change_query_priority` (僅適用於自動 WLM)

以下範例顯示名為 `rule_1`、含有兩個述詞和 `hop` 動作之 WLM 查詢監控規則的 JSON。

```
"rules": [  
  {  
    "rule_name": "rule_1",  
    "predicate": [  
      {  
        "metric_name": "query_execution_time",  
        "operator": ">",  
        "value": 100000  
      },  
      {  
        "metric_name": "query_blocks_read",  
        "operator": ">",  
        "value": 1000  
      }  
    ],  
    "action": "hop"  
  }  
]
```

如需這些屬性和用於設定查詢佇列的策略的相關資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的[實作工作負載管理](#)。

使用以下方法配置 `wlm_json_組態參數` AWS CLI

若要設定 WLM，您必須修改 `wlm_json_configuration` 參數。`wlm_json_configuration` 屬性值的大小上限為 8000 個字元。該值以「JavaScript 物件標記法」(JSON) 格式化。如果您使用

Amazon Redshift API 或其中 AWS CLI 一個 AWS 開發套件來設定 WLM，請使用本節的其餘部分來了解如何建構參數的 JSON 結構。wlm_json_configuration

Note

如果您使用 Amazon Redshift 主控台來設定 WLM，則不需要了解 JSON 格式，因為該主控台提供更簡單的方式來新增佇列及設定屬性。如需使用主控台來設定 WLM 的相關資訊，請參閱 [修改參數群組](#)。

範例

以下範例是以自動 WLM 定義一個佇列的預設 WLM 組態。

```
{
  "auto_wlm": true
}
```

範例

以下範例為自訂的 WLM 組態，其定義一個並行層級 (查詢槽) 為 5 的手動 WLM 佇列。

```
{
  "query_concurrency":5
}
```

語法

預設的 WLM 組態非常簡單，只有一個佇列和一個屬性。您可以新增更多佇列，並為 JSON 結構的每個佇列設定多重屬性。以下語法代表用於設定有多重屬性之多重佇列的 JSON 結構：

```
[
  {
    "ParameterName": "wlm_json_configuration", "ParameterValue":
      "[
        {
          "q1_first_property_name": "q1_first_property_value",
          "q1_second_property_name": "q1_second_property_value",
          ...
        },
      ],
```

```
    {
      "q2_first_property_name": "q2_first_property_value",
      "q2_second_property_name": "q2_second_property_value",
      ...
    }
    ...
  ]"
}
]
```

在上述範例中，開頭為 q1 的代表性屬性為第一個佇列陣列中的物件。這些物件中每個均有名稱/值對；name 和 value 共同設定了第一個佇列的 WLM 屬性。開頭為 q2 的代表性屬性為第二個佇列陣列中的物件。如果您需要更多佇列，可為其他的每個佇列新增額外的陣列，並設定各物件的屬性。

修改 WLM 組態時，即使您只需要變更佇列中的一個屬性，仍必須加入佇列的完整結構。因為整個 JSON 結構會與 `wlm_json_configuration` 參數值一起以字串傳入。

將 AWS CLI 命令格式化

使用 AWS CLI 時，`wlm_json_configuration` 參數需要特定格式。使用的格式需視用戶端作業系統而定。作業系統會使用不同方式來包圍 JSON 結構，以從命令列正確傳送。如需如何在 Linux、Mac OS X 和 Windows 作業系統中建構合適命令的詳細資訊，請參閱下列各節。如需一般而言，封閉 JSON 資料結構差異的詳細資訊，請參閱使用指南中的 [引 AWS Command Line Interface 用字串](#)。

AWS CLI

範例

下列命令範例為名為 `example-parameter-group` 的參數群組設定手動 WLM。該組態啟用短期查詢加速，短期查詢的最長執行時間設為 0，指示 WLM 動態設定數值。ApplyType 設定為 `dynamic`。此設定表示對參數中動態屬性進行的任何變更將立即套用，除非組態有任何其他靜態變更。該組態定義三個佇列，內容如下：

- 第一個佇列可讓使用者指定 `report` 為佇列中的標籤 (如 `query_group` 屬性中所指定)，以協助將查詢路由至該佇列。`report*` 標籤將啟用萬用字元搜尋，因此不需要精確指定要路由至佇列的查詢。例如，`reports` 和 `reporting` 皆符合此查詢群組。佇列將從所有佇列的總記憶體中分配到 25%，且最多可同時執行四個查詢。查詢限制的最長時間為 20000 毫秒 (ms)。模式設定為自動，因此當佇列的查詢空位已滿時，合格查詢將傳送到擴展叢集。
- 第二個佇列可讓屬於資料庫中 `admin` 或 `dba` 群組成員的使用者將其查詢路由至佇列，以進行處理。使用者群組不可用萬用字元搜尋，因此使用者必須與資料庫中的群組精確相符，其查詢才會路由至佇列。

列。佇列將從所有佇列的總記憶體中分配到 40%，且最多可同時執行五個查詢。模式設為關閉，因此 admin 或 dba 群組成員傳送的所有查詢都會在主要叢集上執行。

- 組態中的最後一個佇列為預設佇列。此佇列將從所有佇列的總記憶體中分配到 35%，且一次最多可處理五個查詢。模式設為自動。

Note

範例以多行顯示，做為示範之用。實際的命令不應包含分行符號。

```
aws redshift modify-cluster-parameter-group
--parameter-group-name example-parameter-group
--parameters
'[
  {
    "query_concurrency": 4,
    "max_execution_time": 20000,
    "memory_percent_to_use": 25,
    "query_group": ["report"],
    "query_group_wild_card": 1,
    "user_group": [],
    "user_group_wild_card": 0,
    "user_role": [],
    "user_role_wild_card": 0,
    "concurrency_scaling": "auto",
    "queue_type": "manual"
  },
  {
    "query_concurrency": 5,
    "memory_percent_to_use": 40,
    "query_group": [],
    "query_group_wild_card": 0,
    "user_group": [
      "admin",
      "dba"
    ],
    "user_group_wild_card": 0,
    "user_role": [],
    "user_role_wild_card": 0,
    "concurrency_scaling": "off",
    "queue_type": "manual"
  }
]
```

```

},
{
  "query_concurrency": 5,
  "query_group": [],
  "query_group_wild_card": 0,
  "user_group": [],
  "user_group_wild_card": 0,
  "user_role": [],
  "user_role_wild_card": 0,
  "concurrency_scaling": "auto",
  "queue_type": "manual"
},
{"short_query_queue": true}
]'

```

以下是為自動 WLM 組態設定 WLM 查詢監控規則的範例。下列範例建立名為 `example-monitoring-rules` 的參數群組。此組態定義與先前範例中相同的三個佇列，但不再指定 `query_concurrency` 和 `memory_percent_to_use`。組態還新增了以下規則和查詢優先順序：

- 第一個佇列定義名為 `rule_1` 的規則。規則有兩個述詞：`query_cpu_time > 10000000` 和 `query_blocks_read > 1000`。規則動作為 `log`。此佇列的優先順序為 `Normal`。
- 第二個佇列定義名為 `rule_2` 的規則。規則有兩個述詞：`query_execution_time > 600000000` 和 `scan_row_count > 1000000000`。規則動作為 `abort`。此佇列的優先順序為 `Highest`。
- 組態中的最後一個佇列為預設佇列。此佇列的優先順序為 `Low`。

Note

範例以多行顯示，做為示範之用。實際的命令不應包含分行符號。

```

aws redshift modify-cluster-parameter-group
--parameter-group-name example-monitoring-rules
--parameters
'[ {
  "query_group" : [ "report" ],
  "query_group_wild_card" : 1,
  "user_group" : [ ],
  "user_group_wild_card" : 0,
  "user_role": [ ],

```



```

"user_role_wild_card": 0,
"concurrency_scaling" : "auto",
"rules" : [{
  "rule_name": "rule_1",
  "predicate": [{
    "metric_name": "query_cpu_time",
    "operator": ">",
    "value": 1000000 },
    { "metric_name": "query_blocks_read",
    "operator": ">",
    "value": 1000
  } ],
  "action" : "log"
} ],
"priority": "normal",
"queue_type": "auto"
}, {
  "query_group" : [ ],
  "query_group_wild_card" : 0,
  "user_group" : [ "admin", "dba" ],
  "user_group_wild_card" : 0,
  "user_role": [ ],
  "user_role_wild_card": 0,
  "concurrency_scaling" : "off",
  "rules" : [ {
    "rule_name": "rule_2",
    "predicate": [
      {"metric_name": "query_execution_time",
      "operator": ">",
      "value": 600000000},
      {"metric_name": "scan_row_count",
      "operator": ">",
      "value": 1000000000}],
    "action": "abort"}],
  "priority": "high",
  "queue_type": "auto"
}, {
  "query_group" : [ ],
  "query_group_wild_card" : 0,
  "user_group" : [ ],
  "user_group_wild_card" : 0,
  "user_role": [ ],
  "user_role_wild_card": 0,

```

```
"concurrency_scaling" : "auto",
"priority": "low",
"queue_type": "auto",
"auto_wlm": true
}, {
  "short_query_queue" : true
} ]'
```

透過在命令列 AWS CLI 中搭配 JSON 檔案使用來設定 WLM

您可以使用修改 `wlm_json_configuration` 參數，AWS CLI 並將 `parameters` 引數的值當做 JSON 檔案傳遞。

```
aws redshift modify-cluster-parameter-group --parameter-group-name
myclusterparaametergroup --parameters file://modify_pg.json
```

`--parameters` 的引數會儲存在 `modify_pg.json` 檔案中。檔案位置會以您的作業系統的格式指定。如需詳細資訊，請參閱 [從檔案載入參數](#)。以下顯示 `modify_pg.json` JSON 檔案內容的範例。

```
[
  {
    "ParameterName": "wlm_json_configuration",
    "ParameterValue": "[{\"user_group\": \"example_user_group1\", \"query_group\": \"example_query_group1\", \"query_concurrency\": 7}, {\"query_concurrency\": 5}]"
  }
]
```

```
[
  {
    "ParameterName": "wlm_json_configuration",
    "ParameterValue": "[{\"query_group\": [\"reports\"], \"query_group_wild_card\": 0, \"query_concurrency\": 4, \"max_execution_time\": 20000, \"memory_percent_to_use\": 25}, {\"user_group\": [\"admin\", \"dba\"], \"user_group_wild_card\": 1, \"query_concurrency\": 5, \"memory_percent_to_use\": 40}, {\"query_concurrency\": 5, \"memory_percent_to_use\": 35}, {\"short_query_queue\": true, \"max_execution_time\": 5000 }]",
    "ApplyType": "dynamic"
  }
]
```

使用 Linux 和 macOS X 作業系統上 AWS CLI 的命令列中的設定 WLM 的規則

請遵循下列規則，在一行上執行含有參數的 AWS CLI 命令：

- 整個 JSON 結構必須包圍在單引號 (') 和一組括號 ([]) 內。
- 所有參數名稱和參數值必須包圍在雙引號 (") 內。
- ParameterValue 值內的整個巢狀結構必須包圍在雙引號 (") 和括號 ([]) 內。
- 巢狀結構內每個佇列的每個屬性和值必須包圍在大括號 ({ }) 內。
- 巢狀結構內的每個雙引號 (") 前必須使用反斜線 (\) 逸出字元。
- 如為名稱/值對，冒號 (:) 可分隔每個屬性與值。
- 每個名稱/值對用逗號 (,) 區隔。
- 多重佇列在佇列結束大括號 (}) 和下一個佇列起始大括號 ({) 之間用逗號 (,) 分隔。

在 Microsoft 視窗作業系統 PowerShell 上使用視窗 AWS CLI 中的設定 WLM 的規則

請遵循下列規則，在一行上執行含有參數的 AWS CLI 命令：

- 整個 JSON 結構必須包圍在單引號 (') 和一組括號 ([]) 內。
- 所有參數名稱和參數值必須包圍在雙引號 (") 內。
- ParameterValue 值內的整個巢狀結構必須包圍在雙引號 (") 和括號 ([]) 內。
- 巢狀結構內每個佇列的每個屬性和值必須包圍在大括號 ({ }) 內。
- 巢狀結構內的每個雙引號 (") 和其反斜線 (\) 逸出字元前必須使用反斜線 (\) 逸出字元。此需求意味著您將使用三個反斜線和一個雙引號，以確定用正確方式傳送屬性 (\\")。
- 如為名稱/值對，冒號 (:) 可分隔每個屬性與值。
- 每個名稱/值對用逗號 (,) 區隔。
- 多重佇列在佇列結束大括號 (}) 和下一個佇列起始大括號 ({) 之間用逗號 (,) 分隔。

在 Windows 作業系統上使用命令提示設定 WLM 的規則

請遵循下列規則，在一行上執行含有參數的 AWS CLI 命令：

- 整個 JSON 結構必須包圍在雙引號 (") 和一組括號 ([]) 內。
- 所有參數名稱和參數值必須包圍在雙引號 (") 內。
- ParameterValue 值內的整個巢狀結構必須包圍在雙引號 (") 和括號 ([]) 內。

- 巢狀結構內每個佇列的每個屬性和值必須包圍在大括號 ({}) 內。
- 巢狀結構內的每個雙引號 (") 和其反斜線 (\) 逸出字元前必須使用反斜線 (\) 逸出字元。此需求意味著您將使用三個反斜線和一個雙引號，以確定用正確方式傳送屬性 (\\")。
- 如為名稱/值對，冒號 (:) 可分隔每個屬性與值。
- 每個名稱/值對用逗號 (,) 區隔。
- 多重佇列在佇列結束大括號 (}) 和下一個佇列起始大括號 ({) 之間用逗號 (,) 分隔。

使用主控台來管理參數群組

您可以在 Amazon Redshift 主控台上檢視、建立、修改和刪除參數群組。

您可以檢視所有的參數群組，以查看參數值摘要和工作負載管理 (WLM) 組態。Group parameters (群組參數) 顯示於 Parameters (參數) 標籤中，而 Workload queues (工作負載佇列) 則顯示於 Workload Management (工作負載管理) 標籤中。

建立參數群組

如果想要設定不同於預設參數群組的參數值，您可以建立自己的參數群組。

建立參數群組

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽選單中，選擇組態，然後選擇工作負載管理以顯示工作負載管理頁面。
3. 選擇 Create (建立) 以顯示 Create parameter group (建立參數群組) 視窗。
4. 針對 Parameter group name (參數群組名稱) 和 Description (描述) 輸入值。
5. 請選擇 Create (建立) 以建立參數群組。

修改參數群組

您可以修改參數來變更參數設定和 WLM 組態屬性。

Note

您無法修改預設參數群組。

修改參數群組

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽選單中，選擇組態，然後選擇工作負載管理以顯示工作負載管理頁面。
3. 選擇您要修改的參數群組以顯示詳細資訊頁面及 Parameters (參數) 和 Workload management (工作負載管理) 標籤。
4. 選擇 Parameters (參數) 標籤以檢視目前的參數設定。
5. 選擇 Edit parameters (編輯參數) 以變更這些參數的設定：

- auto_analyze
- auto_mv
- datestyle
- enable_case_sensitive_identifier
- enable_user_activity_logging
- extra_float_digits
- max_concurrency_scaling_clusters
- max_cursor_result_set_size
- query_group
- require_ssl
- search_path
- statement_timeout
- use_fips_ssl

如需這些參數的相關資訊，請參閱 [Amazon Redshift 參數群組](#)。

6. 輸入您的變更，然後選擇 Save (儲存) 以更新參數群組。

修改參數群組的 WLM 組態

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽選單中，選擇組態，然後選擇工作負載管理以顯示工作負載管理頁面。

3. 選擇您要修改的參數群組以顯示詳細資訊頁面及 Parameters (參數) 和 Workload management (工作負載管理) 標籤。
4. 選擇 Workload management (工作負載管理) 標籤以檢視目前的 WLM 組態。
5. 選擇 Edit workload queues (編輯工作負載佇列) 以編輯 WLM 組態。
6. (選用) 請選取 Enable short query acceleration (啟用短期查詢加速)，以啟用短期查詢加速 (SQA)。

啟用 SQA 時，預設會將 Maximum run time for short queries (1 to 20 seconds) (短期查詢 (1 到 20 秒) 的最長執行時間) 設為 Dynamic (動態)。若要將最長執行時間設為固定值，請選擇 1–20 的值。

7. 執行下列其中一個動作來修改佇列組態：
 - 選擇 Switch WLM mode (切換 WLM 模式)，以選擇 Auto WLM (自動 WLM) 或 Manual WLM (手動 WLM)。

使用 Automatic WLM (自動 WLM) 時，Memory (記憶體) 和 Concurrency on main (主要叢集的並行) 值會設為 auto (自動)。

- 若要建立佇列，請選擇 Edit workload queues (編輯工作負載佇列)，再選擇 Add Queue (新增佇列)。
- 若要修改佇列，請變更資料表中的屬性值。依據佇列類型而定，屬性可能包括：
 - 可以變更 Queue name (佇列名稱)。
 - Memory (%) (記憶體 (%))
 - Concurrency on main (主要叢集的並行)
 - Concurrency scaling mode (並行擴展模式) 可以是 off (關閉) 或 auto (自動)
 - Timeout (ms) (逾時 (毫秒))
 - User groups (使用者群組)
 - Query groups (查詢群組)
 - 使用者角色

如需這些屬性的相關資訊，請參閱[wlm_json_configuration 參數的屬性](#)。

Important

如果您變更佇列名稱，WLM 佇列測量結果 (例如 WLM、WLM

QueueLength、WLM、WLM QueueWaitTime、WLM QueriesCompletedPerSecond

等) 的 QueueName 維度值也會變更。QueryDuration RunningQueries 因此，如果您變更佇列的名稱，您可能需要變更已設定的 CloudWatch 警示。

- 若要變更佇列的順序，請選擇 Up (向上) 和 Down (向下) 箭頭按鈕。
 - 若要刪除佇列，請在資料表中選擇佇列那一系列的 Delete (刪除)。
8. (選用) 請選取 Defer dynamic changes until reboot (延遲動態變更直至重開機)，在下次重新開機之後將變更套用至叢集。

Note

不論此設定如何，某些變更需要將叢集重新開機。如需詳細資訊，請參閱 [WLM 動態和靜態屬性](#)。

9. 選擇 Save (儲存)。

使用主控台建立或更新查詢監控規則

您可以使用 Amazon Redshift 主控台建立及修改 WLM 查詢監控規則。查詢監控規則是參數群組中之 WLM 組態參數的一部分。如果您修改查詢監控規則 (QMR)，則變更會自動進行，而不需要修改叢集。如需詳細資訊，請參閱 [WLM 查詢監控規則](#)。

建立規則時，您可以定義規則名稱、一或多個述詞和一個動作。

儲存含有規則的 WLM 組態時，您可以將規則定義的 JSON 程式碼視為 WLM 組態參數的一部分 JSON。

建立查詢監控規則

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽選單中，選擇組態，然後選擇工作負載管理以顯示工作負載管理頁面。
3. 選擇您要修改的參數群組以顯示詳細資訊頁面及 Parameters (參數) 和 Workload management (工作負載管理) 標籤。
4. 選擇 Workload management (工作負載管理) 標籤，再選擇 Edit workload queues (編輯工作負載佇列) 編輯 WLM 組態。
5. 使用預先定義的範本新增規則，或從頭開始新增規則。

若要使用預先定義的範本，執行以下作業：

1. 選擇查詢監控規則群組中的從範本新增規則。規則範本清單即會出現。
2. 選擇一個或多個規則範本。當您選擇 Save (儲存) 時，WLM 會為您選擇的每個範本建立一條規則。
3. 輸入或確認該規則的值，包括 Rule names (規則名稱)、Predicates (述詞) 和 Actions (動作)。
4. 選擇儲存。

若要從頭開始新增規則，請執行下列作業：

1. 若要新增其他述詞，請選擇 Add predicate (新增述詞)。每項規則最多可有三個述詞。如果符合所有述詞，WLM 會觸發相關聯的動作。
2. 選擇 Action (動作)。每一個規則有一個動作。
3. 選擇儲存。

Amazon Redshift 會產生 JSON 格式的 WLM 組態參數，並顯示於 JSON 區段。

刪除參數群組

您可以刪除已不需要且沒有任何相關聯叢集的參數群組。您只能刪除自訂參數群組。

刪除參數群組

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽選單中，選擇組態，然後選擇工作負載管理以顯示工作負載管理頁面。
3. 在 Parameter groups (參數群組) 中，選擇您要修改的參數群組。

Note

您無法刪除預設參數群組。

4. 選擇 Delete (刪除)，然後確認您要刪除該參數群組。

將參數群組與叢集產生關聯

啟動叢集時，必須將此叢集與參數群組建立關聯。如果稍後想要變更參數群組，您可以修改叢集並選擇不同的參數群組。

使用 AWS CLI 和 Amazon Redshift API 管理參數群組

您可以使用中的下列 Amazon Redshift 操作 AWS CLI 來管理參數群組。

- [create-cluster-parameter-group](#)
- [delete-cluster-parameter-group](#)
- [describe-cluster-parameters](#)
- [describe-cluster-parameter-groups](#)
- [describe-default-cluster-parameters](#)
- [modify-cluster-parameter-group](#)
- [reset-cluster-parameter-group](#)

您可以使用下列 Amazon Redshift API 操作來管理參數群組。

- [CreateClusterParameterGroup](#)
- [DeleteClusterParameterGroup](#)
- [DescribeCluster](#) 參數
- [DescribeClusterParameterGroups](#)
- [DescribeDefaultClusterParameters](#)
- [ModifyClusterParameterGroup](#)
- [ResetClusterParameterGroup](#)

將 Amazon Redshift 與合作 AWS 夥伴整合

透過使用 Amazon Redshift，您可以從 Amazon Redshift 主控台上的叢集詳細資料頁面與合作 AWS 夥伴整合。透過叢集詳細資料頁面，您可以透過 AWS 合作夥伴應用程式加快資料上線至 Amazon Redshift 資料倉儲的速度。您也可以將來自不同來源的資料與叢集中的現有資料聯結起來並進行分析。在完成與 Informatica 的整合之前，您必須先將合作夥伴的 IP 地址新增至傳入流量的允許清單。下列合作 AWS 夥伴可以與 Amazon Redshift 整合：

- [Datacoral](#)
- [Etleap](#)
- [Fivetran](#)
- [SnapLogic](#)
- [Stitch](#)
- [Upsolver](#)
- [Matillion \(預覽\)](#)
- [Sisense \(預覽\)](#)
- [Thoughtspot](#)

AWS 合作夥伴可以使用 AWS CLI 或 Amazon Redshift API 操作與 Amazon Redshift 集成。如需詳細資訊，請參閱《AWS CLI 命令參考》和《Amazon Redshift API 參考》。

使用 Amazon Redshift 主控台與合作 AWS 夥伴整合

請使用下列程序來整合叢集與合作 AWS 夥伴。

若要整合亞 Amazon Redshift 叢集與合作 AWS 夥伴

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽功能表上，選擇叢集。
3. 選擇您要整合的叢集。
4. 選擇新增合作夥伴整合。隨即開啟 [選擇合作夥伴] 頁面，其中包含可用 AWS 合作夥伴
5. 選擇 AWS 合作夥伴，然後選擇「下一步」。

此時會顯示有關所選合 AWS 作夥伴的更多詳細資訊，以及您要整合之叢集的詳細資訊。[叢集詳細資料] 區段包含您在 AWS 夥伴網站上提供的資訊，例如叢集識別碼、端點、資料庫名稱和使用名稱 (資料庫使用者名稱)。此資訊會傳送給您選擇的合作夥伴。

6. 選擇 [新增合作夥伴] 以開啟 AWS 合作夥伴的網站。
7. 在合作夥伴的網站上設定與 Amazon Redshift 叢集的整合。在合作夥伴的網站上，您可以選取並設定載入到 Amazon Redshift 叢集的資料來源。您還可以定義其他的擷取、載入和轉換 (ELT) 轉換，以處理業務資料、將業務資料與其他資料集聯結，以及建置用於分析和報告的合併檢視。

您可以從叢集詳細資料屬性索引標籤檢視和管理合 AWS 作夥伴整合。「整合」區段會列出可用來連結至合 AWS 作夥伴網站的合作夥伴名稱、整合的狀態、接收資料的資料庫，以及可能更新叢集的「上次成功連線」。

可能的狀態值如下：

- 作用中 — 合作 AWS 夥伴可以連線到叢集並完成設定的工作。
- 非作用中 — 合 AWS 作夥伴整合不存在。
- 執行階段失敗 — 合作 AWS 夥伴可以連線到叢集，但無法完成設定的工作。
- 連線失敗 — 合 AWS 作夥伴無法連線至叢集。

從 Amazon Redshift 刪除合 AWS 作夥伴整合後，資料會繼續流入您的叢集。請在合作夥伴的網站上完成刪除。

載入 AWS 合作夥伴的資料

除了將合作夥伴與 Amazon Redshift 叢集整合之外，您還可以使用我們合作夥伴的資料載入工具，將資料從 30 多個來源移至 Amazon Redshift 叢集。在執行此操作之前，您必須將合作夥伴的 IP 地址 (如下所示) 新增至傳入規則的允許清單。如需將規則新增至 Amazon EC2 安全群組的詳細資訊，請參閱 Amazon EC2 使用者指南中的[授權執行個體的入站流量](#)。請注意，雖然 Information Data Loader 工具是免費的，但視您選擇的資料來源和目標而定，可能會收取資料傳入費用。

您可以從下列合作夥伴載入資料：

- [Informatica](#) — [IP 地址](#)

將 Amazon Redshift 叢集與 Informatica 進行整合

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在瀏覽功能表上，選擇合 AWS 作夥伴整合，然後選擇您要與叢集整合的合作夥伴。
3. 選擇完成 <partner-name> 整合。系統會將您重新導向至合作夥伴的整合網站。
4. 在合作夥伴的網站上輸入必要的詳細資訊，然後完成整合。

購買 Amazon Redshift 預留節點

概觀

在中 AWS，您使用 Amazon Redshift 所產生的費用是以運算節點為基礎。每個運算節點會以小時的費率來計費。小時費率會根據區域、節點類型以及節點是否接收隨需節點定價或預留節點定價之類的因素而定。

隨需節點定價是 Amazon Redshift 中最昂貴，但最具彈性的選項。透過隨需費率，只會對在執行叢集中擁有的運算節點向您收費。如果您將叢集關機或將其刪除，將不會針對曾在該叢集中的運算節點向您收費。只會對您使用的運算節點向您收費，僅此而已。針對每個運算節點而計費的小時費率會根據區域與節點類型之類的因素而有所不同。

預留節點定價較隨需定價便宜，因為運算節點是以打折的小時費率來計費。然而，若要接收這些打折的費率，您必須購買預留節點方案。當您購買方案時，即進行保留。保留會為您在保留期間預留的每個節點設定折扣費率。方案中的折扣費率會根據區域、節點類型、期間和付費選項之類的因素而有所不同。

您可以呼叫 `PurchaseReservedNodeOffering` API 作業或在 Amazon Redshift 主控台上選擇 `Purchase reserved nodes` (購買預留節點)，將節點指定為預留節點。購買預留節點時，必須為適用的預留節點類型指定「AWS 區域」、節點類型、期限、節點數量及提供項目類型。保留節點只能在指定的 AWS 區域中使用。

此主題會討論預留節點方案為何與您可以購買的方式，以降低 Amazon Redshift 叢集的執行成本。此主題會討論費率以隨需或折扣形式的一般概念，讓您能夠了解定價的概念與定價影響計費的方式。如需特定費率的相關資訊，請前往 [Amazon Redshift 定價](#)。

關於預留節點方案

如果想要讓 Amazon Redshift 叢集持續執行很長一段期間，您應考慮購買預留節點方案。這些方案可省下的金額大幅超過隨需定價，但您需要預留運算節點並承諾為那些節點支付一年或三年期的費用。

預留節點是一種計費概念，將嚴格用來判斷會使用何種費率來向您收取節點費用。預留節點實際上並不會為您建立任何節點。不論使用情形為何，都會向您收取預留節點的費用，也就是說，您必須為在保留期間預留的每個節點支付費用，不論您在執行叢集中是否有任何節點，而這些叢集是否適用折扣費率。

在專案的評估階段時，或是您正在構思概念驗證，隨需定價可以提供彈性，讓您只需為使用的量而隨需付費，並透過關閉或刪除叢集，即可隨時停止付費。在您確認生產環境的需求並開始實作階段，您應透過購買一或多個方案來考量預留運算節點。

任何方案都可適用於一或多個運算節點。您會在購買方案時指定要預留的運算節點數。您可以為多個運算節點選擇購買一個方案，或者可以選擇購買多個方案，並在每個方案中指定某個數量的運算節點。

例如，下列是為三個運算節點購買方案的方法，任一種皆為有效：

- 購買一個方案並指定三個運算節點。
- 購買兩個方案，並將一個運算節點指定給第一個方案，將兩個運算節點指定給第二個方案。
- 購買三個方案，並為每個方案指定一個運算節點。

比較預留節點方案間的定價

Amazon Redshift 提供方案的數種付費選項。您選擇的付費選項會影響付費排程以及針對保留向您收費所使用的折扣費率。您為保留所支付的預付費用越多，整體所省下的費用越多。

下列付款選項可用於方案。方案是按照隨需費率時所省下費用由少至多來排列。

Note

無論您是否使用預留節點，都會針對在保留指定期間中的每小時以適用的小時費率向您收費。付費選項僅決定所適用的付費頻率與折扣。如需詳細資訊，請參閱 [關於預留節點方案](#)。

比較預留節點方案

付款選項	付款排程	節省費用比較	持續時間	預付費用	經常性每月費用
不預付	保留期間的每月分期付款。無預付款項。	約隨需費率的 20% 折扣。	一年或三年	無	是
部分預付	保留期間的部分預付款和每月分期付款。	高達 41% 到 73% 折扣 (視期間而定)。	一年或三年	是	是
全額預付	保留的完整預付款。無每月費用。	高達 42% 到 76% 折扣 (視期間而定)。	一年或三年	是	無

特定選項和持續時間不一定都可供使用。

Note

如果您之前購買過 Amazon Redshift 的重度使用方案，則類似的方案為部分預付方案。

預留節點運作的方式

透過預留節點方案，您會根據先前章節中所述的付費期限來付款。不論您是否已有執行中的叢集，或在擁有保留後啟動叢集，付費方式都是如此。

購買方案時，保留的狀態為 payment-pending (待付款)，直到保留進行處理為止。如果無法處理保留，狀態會顯示為 payment-failed (付款失敗) 且您可以再次嘗試該程序。在保留順利處理後，其狀態即會變成 active (作用中)。保留中的適用折扣費率在狀態變成 active (作用中) 前都不會加以套用。在保留期間過後，狀態會變更為 retired (淘汰)，但您可以基於查證目的繼續存取保留的相關資訊。在保留為 retired (淘汰) 後，叢集會繼續執行，且系統可能會以隨需費率向您收費，除非您有另一個將打折定價套用至節點的保留。

預留節點專屬於您購買方案的區域。如果您使用 Amazon Redshift 主控台購買產品，請選取您要購買供應項目的 AWS 區域，然後完成預訂程序。如果您透過程式設計方式購買方案，會由您連接的 Amazon Redshift 端點來決定區域。如需 Amazon Redshift 區域的相關資訊，請前往《Amazon Web Services 一般參考》中的[區域與端點](#)。

為了確保折扣費率會在您啟動叢集時套用至所有節點，請確保您選取的區域、節點類型和節點數符合一或多個作用中的保留。否則，將針對不符合作用中保留的節點以隨需費率向您收費。

如果您在執行中叢集的節點數超出了您所預留的數量，將會以隨需費率向您收取那些其他節點的累積費用。此累積費用表示相同叢集內節點的計費費率可能會因您預留的節點數量而有所不同。如果您購買另一個方案來涵蓋那些其他節點，則在保留狀態變為 active (可用) 時即會為剩餘期間向那些節點套用折扣費率。

如果您將叢集的大小重新調整為另一個節點類型，且您沒有預留該類型的節點，將會以隨需費率向您收取費用。如果您想要為重新調整大小的叢集接收折扣費率，您可以購買另一個方案搭配新的節點類型。然而，您也繼續支付原本的保留直到其期間結束。如果您在期限過期前需要變更保留，請使用[AWS 主控台](#)建立支援案例。

預留節點和合併帳單

若購買帳戶是在單一合併帳單付款人帳戶下一組帳戶的一部分，則會共用預留節點的計費利益。所有子帳戶的小時用量每個月都會彙總到付款人的帳戶中。這通常對有不同功能團隊或群組的公司來說非常有

用；然後，會套用標準預留節點邏輯計算帳單。如需詳細資訊，請參閱 AWS Billing 使用指南中的[合併帳單](#)。

預留節點範例

此章節的使用案例會示範節點如何使用下列保留詳細資訊來根據隨需和折扣費率來累積費用：

- 區域：美國西部 (奧勒岡)
- 節點類型：加
- 付款選項：無預付款
- 期間：一年期
- 預留節點數目：16

範例 1

您在美國西部 (奧勒岡) 區域中有一個叢集，其中包含 20 個節點。

在此使用案例中，16 個節點會接收保留中的折扣費率，而叢集中其他 4 個節點會以隨需費率向您收費。

範例 2

您在美國西部 (奧勒岡) 區域中有一個叢集，其中包含 12 個節點。

在此使用案例中，叢集中所有 12 個節點會從保留中接收折扣費率。然而，即使您目前沒有保留中剩餘預留節點適用的執行中叢集，您也仍需為它們支付費用。

範例 3

您在美國西部 (奧勒岡) 區域中有一個叢集，其中包含 12 個節點。您使用此組態執行叢集數月的時間，接著您需要將節點新增至叢集。您會重新調整叢集大小，選擇相同的節點類型並指定節點總數 16。

在此使用案例中，會針對 16 個節點以折扣費率向您收費。因為您在叢集中擁有的節點數與您預留的節點數相等，因此在全年期中對您的收費向保持相同。

範例 4

您在美國西部 (奧勒岡) 區域中有一個叢集，其中包含 16 個節點。您使用此組態執行叢集數月的時間，接著您需要新增節點。您會重新調整叢集大小，選擇相同的節點類型並指定節點總數 20。

在此使用案例中，在重新調整大小之前，會針對所有節點以折扣費率向您收費。在重新調整大小後，會在一年中剩下的時間針對 16 個節點以折扣費率向您收費，而針對您在叢集中新增的其他 4 個節點則會以隨需費率向您收費。

範例 5

您在美國西部 (奧勒岡) 區域有兩個叢集。其中一個叢集有 6 個節點，另一個叢集有 10 個節點。

在此使用案例中，因為兩個叢集中的節點總數與您預留的節點數相同，因此會以折扣費率針對所有節點向您收費。

範例 6

您在美國西部 (奧勒岡) 區域有兩個叢集。其中一個叢集有 4 個節點，另一個叢集有 6 個節點。

在此使用案例中，會針對您在執行中叢集中擁有的 10 個節點以折扣費率向您收費，而您也需為您預留的其他 6 個節點支付折扣費率 (即使您目前沒有它們所適用的執行中叢集)。

使用 Amazon Redshift 主控台購買預留節點優惠

您可以使用 Amazon Redshift 主控台內的預留節點頁面來購買預留節點方案，以及檢視目前和過去的預留。

購買後，Reserved Node (預留節點) 清單會顯示您的預留節點以及各節點的詳細資訊，像是節點類型、節點數量、預留狀態。如需預留節點的相關資訊，請參閱[預留節點運作的方式](#)。

購買預留節點

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽功能表中，選擇叢集，然後選擇預留節點以顯示預留節點清單。
3. 選擇 Purchase reserved nodes (購買預留節點) 以顯示頁面，供您選擇要購買的節點屬性。
4. 輸入節點屬性，然後選擇 Purchase reserved nodes (購買預留節點)。

若要升級預留節點，請使用 AWS CLI。

您無法將所有節點類型轉換為預留節點，而且現有的預留節點也可能無法續約。這可能是因為節點類型已停用。請聯絡客戶支援以續約已停用的節點類型。

升級保留節點 AWS CLI

若要升級保留的節點保留區，請使用 AWS CLI

1. 取得符合您付款類型、期限和費用需求之供應項目的 ReservedNodeOffering ID 清單。以下範例示範這個步驟。

```
aws redshift get-reserved-node-exchange-offerings --reserved-node-id xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx
{
  "ReservedNodeOfferings": [
    {
      "Duration": 31536000,
      "ReservedNodeOfferingId": "yyyyyyyyy-yyyy-yyyy-yyyy-yyyyyyyyyyyyy",
      "UsagePrice": 0.0,
      "NodeType": "dc2.large",
      "RecurringCharges": [
        {
          "RecurringChargeFrequency": "Hourly",
          "RecurringChargeAmount": 0.2
        }
      ],
      "CurrencyCode": "USD",
      "OfferingType": "No Upfront",
      "ReservedNodeOfferingType": "Regular",
      "FixedPrice": 0.0
    }
  ]
}
```

2. 呼叫 `accept-reserved-node-exchange` 並提供您要交換之 DC1 保留節點的 ID，以及您在上一個步驟中取得的 ReservedNodeOffering ID。

以下範例示範這個步驟。

```
aws redshift accept-reserved-node-exchange --reserved-node-id xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx --target-reserved-node-offering-id yyyyyyyyyy-yyyy-yyyy-yyyy-yyyyyyyyyyyyy
{
  "ExchangedReservedNode": {
```

```
    "UsagePrice": 0.0,
    "OfferingType": "No Upfront",
    "State": "exchanging",
    "FixedPrice": 0.0,
    "CurrencyCode": "USD",
    "ReservedNodeId": "zzzzzzzz-zzzz-zzzz-zzzz-zzzzzzzzzzzzz",
    "NodeType": "dc2.large",
    "NodeCount": 1,
    "RecurringCharges": [
      {
        "RecurringChargeFrequency": "Hourly",
        "RecurringChargeAmount": 0.2
      }
    ],
    "ReservedNodeOfferingType": "Regular",
    "StartTime": "2018-06-27T18:02:58Z",
    "ReservedNodeOfferingId": "yyyyyyyyy-yyyy-yyyy-yyyy-yyyyyyyyyyyyyy",
    "Duration": 31536000
  }
}
```

您可以呼叫[describe-reserved-nodes](#)並檢查的值，以確認交換已完成Node type。

使用 AWS CLI 和 Amazon Redshift API 購買預留節點方案

您可以使用下列 AWS CLI 操作來購買預留節點方案。

- [purchase-reserved-node-offering](#)
- [describe-reserved-node-offerings](#)
- [describe-orderable-cluster-options](#)

您可以使用下列 Amazon Redshift API 操作來購買預留節點方案。

- [PurchaseReservedNodeOffering](#)
- [DescribeReservedNodeOfferings](#)
- [DescribeOrderableClusterOptions](#)

您無法將所有節點類型轉換為預留節點，而且現有的預留節點也可能無法續約。這可能是因為節點類型已停用。

Amazon Redshift 中的安全

雲端安全是 AWS 最重視的一環。身為 AWS 客戶的您，將能從資料中心和網路架構的建置中獲益，以滿足組織最為敏感的安全要求。

安全是 AWS 與您共同的責任。[共同的責任模型](#) 將此描述為雲端本身的安全和雲端內部的安全：

- 雲端本身的安全：AWS 負責保護在 AWS Cloud 中執行 AWS 服務的基礎設施。AWS 也提供您可安全使用的服務。第三方稽核人員定期檢測及驗證安全的效率也是我們 [AWS 合規計劃](#) 的一部分。若要了解適用於 Amazon Redshift 的合規計畫，請參閱 [合規計畫範圍內的 AWS 服務](#)。
- 雲端內部的安全 – 您的責任取決於所使用的 AWS 服務。您也必須對其他因素負責，包括資料的敏感度、您組織的需求和適用的法律及法規。

對 Amazon Redshift 資源的存取會以四個層級控制：

- 叢集管理 — 建立、設定和刪除叢集的功能是透過提供給予 AWS 安全性登入資料關聯的使用者或帳戶的許可來控制。具有適當許可的使用者可以使用 AWS Management Console、AWS Command Line Interface (CLI) 或 Amazon Redshift 應用程式介面 (API) 來管理其叢集。此存取透過使用 IAM 政策來管理。

Important

Amazon Redshift 集合了用於管理許可、身分和安全存取的最佳實務。建議您在開始使用 Amazon Redshift 時熟悉這些內容。如需詳細資訊，請參閱 [Amazon Redshift 中的身分和存取管理](#)。

- 叢集連線 — Amazon Redshift 安全性群組會指定 AWS 執行個體，其獲授權可連線至格式為無類別網域間路由 (CIDR) 的 Amazon Redshift 叢集。如需建立 Amazon Redshift、Amazon EC2 和 Amazon VPC 安全群組以及將它們與叢集建立關聯的詳細資訊，請參閱 [Amazon Redshift 叢集安全群組](#)。
- 資料庫存取 — 存取資料庫物件 (例如資料表和檢視) 的功能是透過 Amazon Redshift 資料庫中的資料庫使用者帳戶控制。使用者只能存取其使用者帳戶已獲存取許可之資料庫中的資源。您可以透過使用 [CREATE USER](#)、[CREATE GROUP](#)、[GRANT](#) 和 [REVOKE](#) SQL 陳述式來建立這些 Amazon Redshift 使用者帳戶並管理許可。如需詳細資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的 [管理資料庫安全](#)。

- 暫時資料庫登入資料和單一登入 — 除了使用 SQL 命令 (例如 CREATE USER 和 ALTER USER) 來建立和管理資料庫使用者，您可以使用自訂 Amazon Redshift JDBC 或 ODBC 驅動程式 (可在資料庫登入程序中管理資料庫使用者的建立程序和暫時密碼)，來設定 SQL 用戶端。這些驅動程式會管理隨著資料庫登入的一部分建立使用者資料庫和暫時密碼的程序。

該驅動程式會根據 AWS Identity and Access Management (IAM) 身分驗證來驗證資料庫使用者。如果您已管理 AWS 外的使用者身分，便可使用符合 SAML 2.0 的身分提供者 (IdP) 來管理 Amazon Redshift 資源的存取。您可以使用 IAM 角色來設定您的 IdP 和 AWS，以允許您的聯合身分使用者產生暫時資料庫登入資料和登入 Amazon Redshift 資料庫。如需詳細資訊，請參閱[使用 IAM 身分驗證產生資料庫使用者憑證](#)。

本文件有助於您了解如何在使用 Amazon Redshift 時套用共同責任模型。下列主題說明如何將 Amazon Redshift 設定為符合您的安全與合規目標。您也將了解如何使用其他 AWS 服務，幫助您監控並保護 Amazon Redshift 資源。

主題

- [Amazon Redshift 中的資料保護](#)
- [Amazon Redshift 中的身分和存取管理](#)
- [使用管理 Amazon Redshift 管理員密碼 AWS Secrets Manager](#)
- [在 Amazon Redshift 中記錄和監控](#)
- [Amazon Redshift 的合規驗證](#)
- [Amazon Redshift 中的復原能力](#)
- [Amazon Redshift 的基礎設施安全](#)
- [Amazon Redshift 中的組態與漏洞分析](#)

Amazon Redshift 中的資料保護

AWS [共同的責任模型](#)適用於 Amazon Redshift 中的資料保護。如此模型所述，AWS 負責保護執行所有 AWS 雲端 的全球基礎設施。您負責維護在此基礎設施上託管內容的控制權。您也必須負責您所使用 AWS 服務 的安全組態和管理任務。如需有關資料隱私權的更多相關資訊，請參閱[資料隱私權常見問答集](#)。如需有關歐洲資料保護的相關資訊，請參閱 AWS 安全性部落格上的 [AWS 共同的責任模型和 GDPR](#) 部落格文章。

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

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用 AWS CloudTrail 設定 API 和使用者活動日誌記錄。
- 使用 AWS 加密解決方案，以及 AWS 服務內的所有預設安全控制項。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果您在透過命令列介面或 API 存取 AWS 時，需要 FIPS 140-2 驗證的加密模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的更多相關資訊，請參閱[聯邦資訊處理標準 \(FIPS\) 140-2 概觀](#)。

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的文字欄位中，例如 Name (名稱) 欄位。這包括當您使用 Amazon Redshift 或其他使用主控台、API、AWS CLI 或 AWS SDK 的 AWS 服務時。您在標籤或自由格式文字欄位中輸入的任何資料都可能用於計費或診斷日誌。如果您提供外部伺服器的 URL，我們強烈建議請勿在驗證您對該伺服器請求的 URL 中包含憑證資訊。

資料加密

資料保護是指保護往返 Amazon Redshift 的傳輸中資料，以及存放在 Amazon Redshift 資料中心內磁碟的靜態資料。您可以透過 SSL 或用戶端加密來保護傳輸中的資料。在 Amazon Redshift 中保護靜態資料有下列選項。

- 使用伺服器端加密 — 您可以請求 Amazon Redshift 來加密資料，再將它儲存至其資料中心內的磁碟，然後在您下載時解密物件。
- 使用用戶端加密 — 您可以在用戶端加密資料，再將加密的資料上傳至 Amazon Redshift。在這種情況下，您可以管理加密程序、加密金鑰和相關工具。

靜態加密

伺服器端加密與靜態資料加密有關；亦即，Amazon Redshift 會選擇性地在將資料寫入資料中心時將其加密，以及在您存取該資料時將其解密。只要您有驗證請求並具備存取許可，存取加密資料或未加密資料的方式並無不同。

Amazon Redshift 會透過加密保護靜態資料。您可以選擇性地使用進階加密標準 AES-256 來保護存放在叢集內磁碟上的所有資料和 Amazon S3 中的所有備份。

若要管理用於加密和解密 Amazon Redshift 資源的金鑰，請使用 [AWS Key Management Service \(AWS KMS\)](#)。AWS KMS 結合了安全且高可用軟硬體的服務，可提供針對雲端擴展的金鑰管理系統。您可以使用 AWS KMS 建立加密金鑰，並定義控制這些金鑰使用方式的策略。AWS KMS 支援 AWS CloudTrail，因此您可稽核金鑰使用情況，以確認金鑰的使用方式是否正確。您可將 AWS KMS 金鑰與 Amazon Redshift 及受支援的 AWS 服務搭配使用。如需支援 AWS KMS 的服務清單，請參閱《AWS Key Management Service 開發人員指南》中的 [AWS 服務如何使用 AWS KMS](#)。

如果您選擇使用 AWS Secrets Manager 管理佈建叢集或無伺服器命名空間的管理員密碼，Amazon Redshift 也會接受 AWS Secrets Manager 用來加密憑證的其他 AWS KMS 金鑰。這個額外金鑰可以是從 AWS Secrets Manager 自動產生的金鑰，也可以是您提供的自訂金鑰。

Amazon Redshift 查詢編輯器 v2 會安全地存放輸入到查詢編輯器中的資訊，如下所示：

- 用來加密查詢編輯器 v2 資料的 KMS 金鑰 Amazon Resource Name (ARN)。
- 資料庫連線資訊。
- 檔案和資料夾的名稱與內容。

Amazon Redshift 查詢編輯器 v2 會搭配您的 KMS 金鑰或服務帳戶 KMS 金鑰，使用區塊層級加密來加密資訊。Amazon Redshift 資料的加密會由 Amazon Redshift 叢集屬性來控制。

主題

- [Amazon Redshift 資料庫加密](#)

Amazon Redshift 資料庫加密

在 Amazon Redshift 中，您可以為您的叢集啟用資料庫加密，以協助保護靜態資料。啟用叢集的加密時，叢集和其快照的資料區塊和系統中繼資料會加密。

您可以在啟動叢集時啟用加密，也可以修改未加密的叢集以使用 AWS Key Management Service (AWS KMS) 加密。若要這麼做，您可以使用 AWS-managed 金鑰或客戶管理的金鑰。當您修改叢集以啟用 AWS KMS 加密時，Amazon Redshift 會自動將資料遷移到新的加密叢集。從加密叢集建立的快照也會加密。您也可以修改叢集和變更 Encrypt database (加密資料庫) 選項，將加密的叢集遷移到未加密的叢集。如需詳細資訊，請參閱 [變更叢集加密](#)。

雖然 Amazon Redshift 中的加密是選擇性設定，我們仍建議您為包含敏感資料的叢集啟用加密。此外，根據控管您的資料的指導方針或規範，可能會要求您使用加密。例如，支付卡產業資料安全標準 (PCI DSS)、沙賓法案 (SOX)、健康保險流通與責任法案 (HIPAA) 和其他這類法規可提供用於處理特定資料類型的指導方針。

Amazon Redshift 使用加密金鑰的階層來加密資料庫。您可以使用 AWS Key Management Service (AWS KMS) 或硬體安全模組 (HSM) 來管理此階層中最上層的加密金鑰。Amazon Redshift 用於加密的程序會因您管理金鑰的方式而有所不同。Amazon Redshift 會自動與 HSM 集成，AWS KMS 但不與 HSM 集成。使用 HSM 時，您必須使用用戶端和伺服器憑證來設定 Amazon Redshift 與您的 HSM 之間的信任連線。

可提升效能與可用性的加密程序改善

使用 RA3 節點進行加密

RA3 節點加密程序的更新讓使用體驗變得更好了。加密程序進行期間，讀取和寫入查詢在執行時的效能比較不會因加密而受到影響了。此外，加密完成的速度也快了許多。已更新的程序步驟包括還原操作，以及將叢集中繼資料遷移至目標叢集的操作。改進的體驗適用於加密類型 AWS KMS，例如。當您擁有 PB 規模的資料磁碟區時，操作已從幾週減少為幾天。

在加密叢集之前，如果您打算繼續執行資料庫工作負載，則可以透過新增具有彈性調整大小功能的節點來改善效能並加快程序的進行速度。加密進行期間中，您無法使用彈性調整大小功能，因此請在加密之前執行此操作。請注意，新增節點一般會導致成本上升。

使用其他節點類型進行加密

使用 DC2 節點加密叢集時，您無法執行寫入查詢，就像使用 RA3 節點一樣。您只能執行讀取查詢。

使用 RA3 節點進行加密的使用須知

下列洞察和資源可協助您為加密做好準備並監控加密程序。

- 在啟動加密後執行查詢 — 啟動加密後，可在大約 15 分鐘內執行讀取和寫入操作。整個加密程序所需的完成時間取決於叢集上的資料量和工作負載層級。
- 加密需要多久時間？ — 加密資料所需的時間取決於幾個因素：這些因素包括執行的工作負載數量、使用的運算資源、節點數目及節點類型。建議您一開始先在測試環境中執行加密。根據經驗，如果您要處理數 PB 的資料磁碟區，則可能需要 1 至 3 天才能完成加密。
- 我如何知道加密已完成？ — 啟用加密之後，完成第一個快照會確認加密已完成。
- 復原加密 — 如果您需要復原加密操作，最好的方法是從在啟動加密前所製作的最新備份進行還原。您必須重新套用在上次備份後所做過的任何新更新 (更新/刪除/插入)。
- 執行資料表還原 — 請注意，您無法將資料表從未加密的叢集還原至已加密的叢集。
- 加密單一節點叢集 — 加密單一節點叢集有效能限制。其所需時間比加密多節點叢集還要久。

- 在加密後建立備份 — 當您加密叢集中的資料時，要等到整個叢集完成加密後，才會建立備份。此操作所需的時間會有所不同。視叢集大小而定，備份所需的時間從幾小時到幾天不等。加密完成後，會延遲一段時間才能建立備份。

請注意，由於 backup-and-restore 作業會在加密程序期間發生，所以BACKUP NO不會保留使用建立的任何表格或具體化視觀表。如需詳細資訊，請參閱 [CREATE TABLE](#) 或 [CREATE MATERIALIZED VIEW](#)。

主題

- [使用 AWS KMS的 Amazon Redshift 資料庫加密](#)
- [使用硬體安全模組的 Amazon Redshift 加密](#)
- [Amazon Redshift 中的加密金鑰輪換](#)
- [變更叢集加密](#)
- [使用主控台設定資料庫加密](#)
- [使用 Amazon Redshift API 和 AWS CLI 設定資料庫加密](#)

使用 AWS KMS的 Amazon Redshift 資料庫加密

當您選擇使用 Amazon Redshift AWS KMS 進行金鑰管理時，會有四層加密金鑰階層。這些金鑰按層次順序列出為根金鑰、叢集加密金鑰 (CEK)、資料庫加密金鑰 (DEK) 和資料加密金鑰。

當您啟動叢集時，Amazon Redshift 會傳回您 AWS 帳戶已建立或有權在中 AWS KMS使用的帳戶清單。AWS KMS keys 您可以選取 KMS 金鑰作為您在加密階層中的根金鑰。

依預設，Amazon Redshift 會選取您的預設金鑰作為根金鑰。您的預設金鑰是為您的 AWS 帳戶所建立的 AWS受管金鑰，以便在 Amazon Redshift 中使用。AWS KMS 在您第一次在 AWS 區域中啟動加密叢集時建立此金鑰，並選擇預設金鑰。

如果您不想使用預設金鑰，則必須先在 Amazon Redshift 中啟動叢集 AWS KMS 之前，分別擁有 (或建立) 客戶管理的 KMS 金鑰。客戶受管金鑰可為您提供更多彈性，包含建立、輪換、停用、定義存取控制，以及稽核用於協助保護您資料之加密金鑰的能力。如需建立 KMS 金鑰的相關資訊，請參閱《AWS Key Management Service 開發人員指南》中的[建立金鑰](#)。

如果您想要使用其他 AWS 帳戶的 AWS KMS 金鑰，您必須擁有使用金鑰的權限，並在 Amazon Redshift 中指定其亞馬遜資源名稱 (ARN)。如需中金鑰存取權的詳細資訊 AWS KMS，請參閱《AWS Key Management Service 開發人員指南》中的[「控制金鑰存取」](#)。

選擇根金鑰後，Amazon Redshift 會請求 AWS KMS 產生資料金鑰，並使用選取的根金鑰加密該金鑰。此資料金鑰在 Amazon Redshift 中用作 CEK。AWS KMS 會將加密的 CEK 匯出至 Amazon Redshift，其中，它會與 KMS 金鑰的授予和 CEK 的加密內容一併儲存在與叢集分開的網路磁碟內。只有加密的 CEK 會匯出至 Amazon Redshift；KMS 金鑰會保留在 AWS KMS 中。Amazon Redshift 也會透過安全通道將加密的 CEK 傳遞到叢集，並將其載入到記憶體。然後，Amazon Redshift 調用 AWS KMS 解密 CEK 並將解密的 CEK 加載到內存中。如需授權、加密內容和其他 AWS KMS 相關概念的詳細資訊，請參閱 AWS Key Management Service 開發人員指南中的 [概念](#)。

接下來，Amazon Redshift 會隨機產生金鑰來用作 DEK，並在叢集中將它載入記憶體。解密的 CEK 可用來加密 DEK，然後透過安全管道從 Amazon Redshift 要在內部儲存的叢集，傳遞至與叢集不同網路中的磁碟。如同 CEK，加密和解密版本的 DEK 會在叢集中載入記憶體。接著使用 DEK 的解密版本來加密為資料庫中每個資料區塊隨機產生的個別加密金鑰。

叢集重新啟動時，Amazon Redshift 會從內部儲存的 CEK 和 DEK 加密版本開始，將它們重新載入記憶體，然後呼叫 AWS KMS 再次使用 KMS 金鑰解密 CEK，以便將其載入記憶體。然後使用解密的 CEK 來再次解密，而解密的 DEK 會載入記憶體，並視需要用來加密和解密資料區塊金鑰。

如需建立使用 AWS KMS 金鑰加密的 Amazon Redshift 叢集的相關資訊，請參閱 [建立叢集](#) 和 [使用 AWS CLI 和 Amazon Redshift API 管理叢集](#)。

複製 AWS KMS— 加密的快照到另一個 AWS 區域

AWS KMS 鍵是特定於一個 AWS 區域。如果您啟用將 Amazon Redshift 快照複製到另一個 AWS 區域，且來源叢集及其快照已使用根金鑰加密 AWS KMS，則需要設定授權讓 Amazon Redshift 在目標 AWS 的地區域使用根金鑰。這項授權可讓 Amazon Redshift 加密目標 AWS 區域中的快照。如需跨區域快照複製的相關資訊，請參閱 [將快照複製到另一個 AWS 區域](#)。

Note

如果您啟用從加密叢集複製快照並用 AWS KMS 於根金鑰，則無法重新命名叢集，因為叢集名稱是加密內容的一部分。如果必須重新命名叢集，您可以停用來源 AWS 區域中的快照複製、重新命名叢集，然後再次設定和啟用快照複製。

為複製快照設定授予的程序如下所示。

1. 在目的地 AWS 區域中，執行下列動作來建立快照副本授權：
 - 如果您還沒有要使用的 AWS KMS 金鑰，請建立一個金鑰。如需有關建立 AWS KMS 金鑰的詳細資訊，請參閱 AWS Key Management Service 開發人員指南中的 [建立金鑰](#)。

- 指定快照複製授予的名稱。此名稱在您 AWS 帳戶的該 AWS 地區中必須是唯一的。
 - 指定您 AWS KMS 要為其建立授權的金鑰 ID。如果您不指定金鑰 ID，該授予即會套用至您的預設金鑰。
2. 在來源 AWS 區域中，啟用快照複製，並指定您在目的地 AWS 區域中建立的快照副本授權的名稱。

只有當您使用 Amazon Redshift API 或軟體開發套件啟用快照複製時 AWS CLI，才需要執行上述程序。如果是使用主控台，在啟用跨區域快照複製時，Amazon Redshift 會提供適當的工作流程來設定授予。如需使用主控台來為 AWS KMS 加密叢集設定跨區域快照複製的相關資訊，請參閱 [為已 AWS KMS 加密的叢集設定跨區域快照副本](#)。

在將快照複製到目的地 AWS 區域之前，Amazon Redshift 會使用來源 AWS 區域中的根金鑰將快照解密，並使用 Amazon Redshift 內部管理的隨機產生的 RSA 金鑰對其進行臨時加密。然後，Amazon Redshift 會透過安全通道將快照複製到目的地 AWS 區域，使用內部管理的 RSA 金鑰解密快照，然後使用目標區域中的根金鑰重新加密快照。AWS

如需針對 AWS KMS 已加密叢集設定快照複製授權的詳細資訊，請參閱 [使用 Amazon Redshift API 和 AWS CLI 將 Amazon Redshift 設定為使用 AWS KMS 加密金鑰](#)。

使用硬體安全模組的 Amazon Redshift 加密

如果您不用 AWS KMS 於金鑰管理，您可以使用硬體安全模組 (HSM) 透過 Amazon Redshift 進行金鑰管理。

⚠ Important

DC2 和 RA3 節點類型不支援 HSM 加密。

HSM 為可針對金鑰產生和管理提供直接控制的裝置。其會透過將金鑰管理與應用程式資料庫層分開以提供更好的安全性。Amazon Redshift 支持 AWS CloudHSM 經典的密鑰管理。此加密程序與使用 HSM 而非 AWS KMS 來管理您的加密金鑰時不同。

⚠ Important

Amazon Redshift 只支持 AWS CloudHSM 經典。我們不支援較新版的 AWS CloudHSM 服務。

AWS CloudHSM 經典對新客戶不開放。如需詳細資訊，請參閱 [CloudHSM 傳統定價](#)。AWS CloudHSM 並非所有 AWS 地區都提供經典版。如需有關可用區 AWS 域的詳細資訊，請參閱 [AWS 區域表](#)。

設定您的叢集使用 HSM 時，Amazon Redshift 會將請求傳送至 HSM 以產生和儲存要用作 CEK 的金鑰。但是 AWS KMS，與 HSM 不同的是，不會將 CEK 匯出到 Amazon Redshift。Amazon Redshift 會改為在叢集中隨機產生 DEK，並將它傳遞至 HSM 供 CEK 加密。HSM 會將已加密的 DEK 傳回給 Amazon Redshift，在此處使用隨機產生的內部根金鑰進行進一步加密，然後儲存在與叢集位於不同網路的磁碟內。Amazon Redshift 也會將 DEK 的解密版本載入到叢集的記憶體中，以便使用 DEK 來加密和解密資料區塊的個別金鑰。

如果叢集重新開機，Amazon Redshift 會使用內部根金鑰來解密內部儲存、雙重加密的 DEK，以讓在內部儲存的 DEK 回到 CEK 加密的狀態。然後將 CEK 加密的 DEK 傳遞至要解密的 HSM，並傳回 Amazon Redshift，在該處可將它再次載入記憶體，以搭配個別資料區塊金鑰使用。

設定 Amazon Redshift 與 HSM 之間的信任連線

選擇使用 HSM 管理您的叢集金鑰時，您必須在 Amazon Redshift 與您的 HSM 之間設定信任的網路連結。要這麼做需要對用戶端和伺服器憑證進行組態。信任的連線可用來於加密和解密操作期間，在 HSM 與 Amazon Redshift 之間傳遞加密金鑰。

Amazon Redshift 會從隨機產生的私有和公有金鑰對建立公有用戶端憑證。這些憑證會經過加密並在內部儲存。您可以在您的 HSM 中下載和註冊公有用戶端憑證，並將它指派至適用的 HSM 分割區。

您可以提供 Amazon Redshift 相關的 HSM IP 地址、HSM 分割區名稱、HSM 分割區密碼和公有 HSM 伺服器憑證 (其使用內部根金鑰進行加密)。Amazon Redshift 會完成組態程序，並驗證它可連線至 HSM。如果它無法連線，則會讓叢集處於 INCOMPATIBLE_HSM 狀態，並且不會建立叢集。在此情況下，您必須刪除不完整的叢集並重試。

Important

修改您的叢集以使用不同的 HSM 分割區時，Amazon Redshift 會驗證它可以連線至新的分割區，但無法驗證存在有效的加密金鑰。使用新的分割區之前，您必須將金鑰複寫至新的分割區。如果叢集已重新啟動，並且 Amazon Redshift 找不到有效的金鑰，重新啟動會失敗。如需詳細資訊，請參閱 [跨 HSM 複寫金鑰](#)。

初始組態之後，如果 Amazon Redshift 無法連線至 HSM，即會記錄事件。如需這些事件的相關資訊，請參閱 [Amazon Redshift 事件通知](#)。

Amazon Redshift 中的加密金鑰輪換

在 Amazon Redshift 中，您可以輪換加密的叢集的加密金鑰。當您啟動金鑰輪換程序時，Amazon Redshift 會為指定叢集以及叢集的任何自動或手動快照輪換 CEK。Amazon Redshift 也會為指定叢集輪換 DEK，但是當快照儲存在 Amazon Simple Storage Service (Amazon S3) 內並使用現有 DEK 進行加密時，則無法輪換快照的 DEK。

在輪換進行中時，叢集會處於 ROTATING_KEYS 狀態直到完成為止，完成時叢集會回到 AVAILABLE 狀態。Amazon Redshift 會在金鑰輪換程序期間處理解密和重新加密。

Note

您無法為沒有來源叢集的快照輪換金鑰。刪除叢集之前，請考慮其快照是否仰賴於金鑰輪換。

由於叢集金鑰輪換程序期間暫時無法使用，您應該只在您的資料需求或當您懷疑金鑰可能已遭到盜用時才輪換金鑰。做為最佳實務，您應該檢閱儲存的資料類型，並計畫輪換加密該資料之金鑰的頻率。輪換金鑰的頻率因對於資料安全性的公司政策，以及有關敏感資料和法規合規的任何產業標準而有所不同。確保您的計畫可平衡您的叢集對於可用性考量的安全性需求。

如需輪換金鑰的相關資訊，請參閱[使用 Amazon Redshift 主控台輪換加密金鑰](#)和[使用 Amazon Redshift API 和 AWS CLI 輪換加密金鑰](#)。

變更叢集加密

您可以使用 AWS-managed 金鑰或客戶管理的金鑰，修改未加密的叢集以使用 AWS Key Management Service (AWS KMS) 加密。當您修改叢集以啟用 AWS KMS 加密時，Amazon Redshift 會自動將資料遷移到新的加密叢集。您也可以經由修改叢集，將未加密的叢集遷移到加密的叢集。

在遷移操作期間，只能以唯讀模式使用您的叢集，而且叢集的狀態會顯示為 resizing (調整大小)。

如果您的叢集設定為啟用跨AWS 區域快照副本，您必須在變更加密之前停用它。如需詳細資訊，請參閱[將快照複製到另一個 AWS 區域](#)及[為已 AWS KMS加密的叢集設定跨區域快照副本](#)。您無法經由修改叢集來啟用硬體安全模組 (HSM) 加密。反之，請建立新的 HSM 加密叢集，然後將您的資料遷移至新叢集。如需詳細資訊，請參閱[遷移至 HSM 加密的叢集](#)。

修改叢集上的資料庫加密

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽功能表上，選擇叢集，然後選擇您要修改加密的叢集。
3. 選擇 Properties (屬性)。
4. 在資料庫組態區段中，選擇編輯，然後選擇編輯加密。
5. 選擇其中一個加密選項，然後選擇儲存變更。

使用 CLI 變更叢集加密

若要修改要使用的未加密叢集 AWS KMS，請執行 `modify-cluster` CLI 命令並指定 `--encrypted`，如下所示。在預設情況下會使用預設 KMS 金鑰。若要指定客戶受管金鑰，請包含 `--kms-key-id` 選項。

```
aws redshift modify-cluster --cluster-identifier <value> --encrypted --kms-key-id <value>
```

若要從叢集移除加密，請執行下列 CLI 命令。

```
aws redshift modify-cluster --cluster-identifier <value> --no-encrypted
```

遷移至 HSM 加密的叢集

若要將未加密的叢集遷移至使用硬體安全模組 (HSM) 加密的叢集，請建立新的加密叢集，然後將您的資料移至新叢集。您無法經由修改叢集來遷移 HSM 加密的叢集。

若要從未加密的叢集遷移至 HSM 加密的叢集，請先從現有的來源叢集卸載您的資料。然後在新的目標叢集中，使用所選的加密設定將資料重新載入。如需啟動加密的叢集的相關資訊，請參閱 [Amazon Redshift 資料庫加密](#)。

遷移程序期間，您的來源叢集可供唯讀查詢，直到最後一個步驟為止。最後一個步驟是重新命名目標和來源叢集，這會切換端點，使得所有流量會路由至新的目標叢集。在您重新命名後重新開機之前，目標叢集將無法使用。在資料傳送時，請暫停來源叢集上的所有資料載入和其他寫入操作。

準備遷移

1. 識別與 Amazon Redshift 互動的所有相依系統，例如商業智慧 (BI) 工具和擷取、轉換和載入 (ETL) 系統。

2. 識別驗證查詢以測試遷移。

例如，您可以使用下列查詢來尋找使用者定義資料表的數目。

```
select count(*)
from pg_table_def
where schemaname != 'pg_catalog';
```

下列查詢會傳回所有使用者定義資料表的清單，和每個資料表中資料列的數目。

```
select "table", tbl_rows
from svv_table_info;
```

3. 選擇適合遷移的好時機。若要了解叢集使用率何時最低，請監控叢集指標，例如 CPU 使用率和資料庫連線數目。如需詳細資訊，請參閱 [檢視叢集效能資料](#)。
4. 捨棄未使用的資料表。

若要建立資料表的清單和查詢每個資料表的次數，請執行下列查詢。

```
select database,
schema,
table_id,
"table",
round(size::float/(1024*1024)::float,2) as size,
sortkey1,
nvl(s.num_qs,0) num_qs
from svv_table_info t
left join (select tbl,
perm_table_name,
count(distinct query) num_qs
from stl_scan s
where s.userid > 1
and s.perm_table_name not in ('Internal worktable','S3')
group by tbl,
perm_table_name) s on s.tbl = t.table_id
where t."schema" not in ('pg_internal');
```

5. 啟動新的加密叢集。

對目標叢集使用與來源叢集相同的連線埠號碼。如需啟動加密的叢集的相關資訊，請參閱 [Amazon Redshift 資料庫加密](#)。

6. 設定卸載和載入程序。

您可以使用 [Amazon Redshift Unload/Copy Utility](#) 來幫助您在叢集之間遷移資料。該公用程式會從來源叢集匯出資料至 Amazon S3 上的位置。資料會使用加密 AWS KMS。然後該公用程式會將資料自動匯入至目標。您可以在遷移完成之後，選擇性地使用該公用程式來清理 Amazon S3。

7. 執行測試以驗證您的程序並估計寫入操作必須暫停的時間長度。

在卸載和載入操作期間，透過暫停資料載入和其他寫入操作來保有資料一致性。使用您的其中一個最大的資料表，執行卸載和載入程序來幫助您估計時間。

8. 建立資料庫物件，例如結構描述、檢視和資料表。若要協助您產生必要的資料定義語言 (DDL) 陳述式，您可以在 AWS GitHub 儲存庫 [AdminViews](#) 中使用指令碼。

遷移叢集

1. 停止來源叢集上的所有 ETL 處理。

若要確認程序中沒有寫入操作，請使用 Amazon Redshift 管理主控台來監控寫入 IOPS。如需詳細資訊，請參閱 [檢視叢集效能資料](#)。

2. 執行您稍早識別的驗證查詢，以在遷移之前收集未加密的來源叢集的相關資訊。

3. (選用) 建立一個工作負載管理 (WLM) 佇列以使用來源和目標叢集中最大可用的資源。例如，建立名為 data_migrate 的佇列，並設定具有 95% 記憶體和並行 4 的佇列。如需詳細資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的 [根據使用者群組和查詢群組將查詢路由至佇列](#)。

4. 使用 data_migrate 佇列，執行 UnloadCopyUtility。

使用 Amazon Redshift 主控台監控 UNLOAD 和 COPY 程序。

5. 再次執行驗證查詢，並驗證該結果符合來源叢集的結果。

6. 重新命名您的來源和目標叢集以交換端點。為了避免干擾，請在上班時間以外執行此操作。

7. 驗證您可以使用您的所有 SQL 用戶端 (例如 ETL 和報表工具) 連線至目標叢集。

8. 關閉未加密的來源叢集。

使用主控台設定資料庫加密

您可以使用 Amazon Redshift 主控台，將 Amazon Redshift 設定為使用 HSM 和輪換加密金鑰。如需如何使用 AWS KMS 加密金鑰建立叢集的詳細資訊，請參閱 [建立叢集](#) 和 [使用 AWS CLI 和 Amazon Redshift API 管理叢集](#)。

修改叢集上的資料庫加密

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽功能表上，選擇叢集，然後選擇您要移動快照的叢集。
3. 針對 Actions (動作)，選擇 Modify (修改) 以顯示組態頁面。
4. 在 Database configuration (資料庫組態) 區段中，選擇 Encryption (加密) 的設定，然後選擇 Modify cluster (修改叢集)。

使用 Amazon Redshift 主控台輪換加密金鑰

您可以使用下列程序，藉由使用 Amazon Redshift 主控台來輪換加密金鑰。

輪換叢集的加密金鑰

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽功能表上，選擇叢集，然後選擇您要更新加密金鑰的叢集。
3. 針對 Actions (動作)，選擇 Rotate encryption (輪換加密) 以顯示 Rotate encryption keys (輪換加密金鑰) 頁面。
4. 在 Rotate encryption keys (輪換加密金鑰) 頁面上，選擇 Rotate encryption keys (輪換加密金鑰)。

使用 Amazon Redshift API 和 AWS CLI 設定資料庫加密

使用 Amazon Redshift API 和 AWS Command Line Interface (AWS CLI) 設定 Amazon Redshift 資料庫的加密金鑰選項。如需資料庫加密的詳細資訊，請參閱 [Amazon Redshift 資料庫加密](#)。

使用 Amazon Redshift API 和 AWS CLI 將 Amazon Redshift 設定為使用 AWS KMS 加密金鑰。

您可以使用下列 Amazon Redshift API 動作將 Amazon Redshift 設定為使用 AWS KMS 加密金鑰。

- [CreateCluster](#)
- [CreateSnapshotCopyGrant](#)
- [DescribeSnapshotCopyGrants](#)
- [DeleteSnapshotCopyGrant](#)
- [DisableSnapshotCopy](#)

- [EnableSnapshotCopy](#)

您可以使用下列 Amazon Redshift CLI 操作將 Amazon Redshift 設定為使用 AWS KMS 加密金鑰。

- [create-cluster](#)
- [create-snapshot-copy-grant](#)
- [describe-snapshot-copy-grants](#)
- [delete-snapshot-copy-grant](#)
- [disable-snapshot-copy](#)
- [enable-snapshot-copy](#)

使用 Amazon Redshift API 和 AWS CLI 將 Amazon Redshift 設定為使用 HSM。

您可以使用下列 Amazon Redshift API 動作來管理硬體安全模組。

- [CreateHsmClientCertificate](#)
- [CreateHsmConfiguration](#)
- [DeleteHsmClientCertificate](#)
- [DeleteHsmConfiguration](#)
- [DescribeHsmClientCertificates](#)
- [DescribeHsmConfigurations](#)

您可以使用下列 AWS CLI 操作來管理硬體安全模組。

- [create-hsm-client-certificate](#)
- [create-hsm-configuration](#)
- [delete-hsm-client-certificate](#)
- [delete-hsm-configuration](#)
- [describe-hsm-client-certificates](#)
- [describe-hsm-configurations](#)

使用 Amazon Redshift API 和 AWS CLI 輪換加密金鑰

您可以使用下列 Amazon Redshift API 動作來輪換加密金鑰。

- [RotateEncryptionKey](#)

您可以使用下列 AWS CLI 操作來輪換加密金鑰。

- [rotate-encryption-key](#)

傳輸中加密

您可以設定您的環境以保護傳輸中資料的機密性及完整性。

加密 Amazon Redshift 叢集與透過 JDBC/ODBC 的 SQL 用戶端之間的傳輸中資料：

- 您可以從 SQL 用戶端工具透過 Java 資料庫連線 (JDBC) 和開放式資料庫連線 (ODBC) 來連線至 Amazon Redshift 叢集。
- Amazon Redshift 支援 Secure Sockets Layer (SSL) 連線，可將資料和伺服器憑證加密，以驗證用戶端所連線的伺服器憑證。用戶端會連線到 Amazon Redshift 叢集的領導節點。如需詳細資訊，請參閱[設定連線的安全選項](#)。
- 為了支援 SSL 連線，Amazon Redshift 會在每一個叢集上建立並安裝 AWS Certificate Manager (ACM) 發行的 SSL 憑證。如需詳細資訊，請參閱[將 SSL 連線轉換為使用 ACM 憑證](#)。
- 為了保護在 AWS 雲端中傳輸中的資料，Amazon Redshift 會使用硬體加速的 SSL 來與 Amazon S3 或 Amazon DynamoDB 通訊，以進行 COPY、UNLOAD、備份和還原操作。

加密 Amazon Redshift 叢集與 Amazon S3 或 DynamoDB 之間的傳輸中資料：

- Amazon Redshift 使用硬體加速的 SSL 來與 Amazon S3 或 DynamoDB 通訊，以進行 COPY、UNLOAD、備份和還原操作。
- Redshift Spectrum 支援使用您帳戶預設金鑰的 Amazon S3 伺服器端加密 (SSE)。該預設金鑰是由 AWS Key Management Service (KMS) 進行管理。
- 使用 Amazon S3 和 AWS KMS 來加密 Amazon Redshift 負載。如需詳細資訊，請參閱[使用 Amazon S3 和 AWS KMS 來加密 Amazon Redshift 負載](#)。

AWS CLI、SDK 或 API 用戶端與 Amazon Redshift 端點之間傳輸中資料的加密和簽署：

- Amazon Redshift 會提供 HTTPS 端點用於加密傳輸中資料。

- 為了保護向 Amazon Redshift 發出之 API 請求的完整性，必須由發起人簽署 API 呼叫。根據 Signature 第 4 版簽署程序 (Sigv4)，呼叫會由 X.509 憑證或客戶的 AWS 私密存取金鑰簽署。如需詳細資訊，請參閱《AWS 一般參考》中的 [Signature 第 4 版簽署程序](#)。
- 使用 AWS CLI 或其中一個 AWS SDK 來向 AWS 進行請求。這些工具會自動使用您設定工具時指定的存取金鑰，替您簽署請求。

加密 Amazon Redshift 叢集與 Amazon Redshift 查詢編輯器 v2 之間的傳輸中資料

- 資料會透過 TLS 加密的通道在查詢編輯器 v2 和 Amazon Redshift 叢集之間傳輸。

金鑰管理

您可以設定您的環境以使用金鑰保護資料：

- Amazon Redshift 會自動與 AWS Key Management Service (AWS KMS) 整合以進行金鑰管理。AWS KMS 會使用封套加密。如需詳細資訊，請參閱[信封加密](#)。
- 在 AWS KMS 中加密金鑰時，Amazon Redshift 會使用四個階層的金鑰式架構進行加密。架構包含隨機產生的 AES-256 資料加密金鑰、資料庫金鑰、叢集金鑰和根金鑰。如需詳細資訊，請參閱[Amazon Redshift 如何使用 AWS KMS](#)。
- 您可以在 AWS KMS 中建立您自己的客戶受管金鑰。如需詳細資訊，請參閱[建立金鑰](#)。
- 您也可以為新 AWS KMS keys 匯入您自己的金鑰材料。如需詳細資訊，請參閱[在 AWS Key Management Service \(AWS KMS\) 中匯入金鑰材料](#)。
- Amazon Redshift 支援在外部硬體安全模組 (HSM) 中加密金鑰的管理。HSM 可以是內部部署，也可以是 AWS CloudHSM。使用 HSM 時，您必須使用用戶端和伺服器憑證來設定 Amazon Redshift 與您的 HSM 之間的信任連線。Amazon Redshift 僅支援使用 AWS CloudHSM Classic 來管理金鑰。如需詳細資訊，請參閱[使用硬體安全模組的 Amazon Redshift 加密](#)。如需 AWS CloudHSM 的相關資訊，請參閱[什麼是 AWS CloudHSM ?](#)
- 您可以輪換加密的叢集的加密金鑰。如需詳細資訊，請參閱[Amazon Redshift 中的加密金鑰輪換](#)。

資料字符化

字符化是出於資料安全目的，用不透明值替換實際值的程序。對安全敏感的應用程式會使用字符化，以字符替換敏感資料 (例如，個人身分識別資訊 (PII) 或受保護的醫療資訊 (PHI)) 來降低安全風險。去字符化會為授權使用者使用適當的安全政策將字符逆轉為實際值。

若要與第三方字符化服務整合，您可以使用您透過 [AWS Lambda](#) 建立的 Amazon Redshift 使用者定義函數 (UDF)。如需詳細資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的 [Lambda 使用者定義的函數](#)。例如，請參閱 [Protegrity](#)。

Amazon Redshift 會將字符化請求傳送至透過 REST API 或預先定義的端點所存取的字符化伺服器。有兩個以上免費的 Lambda 函數會處理字符化和去字符化請求。對於此處理，您可以使用第三方字符化提供者所提供的 Lambda 函數。您也可以使用在 Amazon Redshift 中註冊為 Lambda UDF 的 Lambda 函數。

例如，假設您提交的查詢會在資料欄叫用字符化或去字符化 UDF。Amazon Redshift 叢集會對適用的引數資料列進行多工緩衝處理，並以批次方式將這些資料列平行傳送至 Lambda 函數。資料會在 Amazon Redshift 運算節點與 Lambda 之間另外以用戶端無法存取的隔離網路連線進行傳輸。Lambda 函數會將資料傳遞至字符化伺服器端點。字符化伺服器會根據需要對資料進行字符化或去字符化，並將其傳回。然後，Lambda 函數會將結果傳輸到 Amazon Redshift 叢集以進行進一步處理 (如有必要)，然後傳回查詢結果。

網際網路流量隱私權

若要在 Amazon Redshift 與企業網路上的用戶端和應用程式之間路由流量：

- 在虛擬私有雲端 (VPC) 和公司網路之間設定私有連線。設定透過網際網路的 IPsec VPN 連線，或使用 AWS Direct Connect 連線的私有實體連線。AWS Direct Connect 可讓您在您的內部部署網路與 Amazon VPC 之間直接建立一個專用虛擬界面，在您的網路和 VPC 之間提供一個私有的高頻寬網路連線。您可使用多個虛擬界面，甚至能與多個 VPC 建立私有連線，同時保持網路隔離性。如需詳細資訊，請參閱 [什麼是 AWS Site-to-Site VPN ?](#) 和 [什麼是 AWS Direct Connect ?](#)

若要在 VPC 中的 Amazon Redshift 叢集與相同 AWS 區域中的 Amazon S3 儲存貯體之間路由流量：

- 設定 Amazon S3 私有 VPC 端點，以私密地存取來自 ETL 載入或卸載的 Amazon S3 資料。如需詳細資訊，請參閱 [Amazon S3 的端點](#)。
- 為 Amazon Redshift 叢集啟用「增強型 VPC 路由」，指定目標 Amazon S3 VPC 端點。然後 Amazon Redshift COPY、UNLOAD 或 CREATE LIBRARY 命令產生的流量會透過私有端點路由。如需詳細資訊，請參閱 [增強型 VPC 路由](#)。

Amazon Redshift 中的身分和存取管理

存取 Amazon Redshift 需要 AWS 可用來驗證您的請求的登入資料。這些登入資料必須具有存取 AWS 資源的權限，例如 Amazon Redshift 叢集。以下章節提供關於如何使用 [AWS Identity and Access](#)

[Management \(IAM\)](#) 與 Amazon Redshift 的詳細資訊，藉由控制可存取的人員，協助保護您資源的安全：

- [使用身分驗證](#)
- [存取控制](#)

Important

本主題集合了用於管理許可、身分和安全存取的最佳實務。建議您熟悉將 IAM 與 Amazon Redshift 搭配使用的最佳實務。這些實務包括使用用於套用許可的 IAM 角色。充分了解這些部分會可助您保持更安全的 Amazon Redshift 資料倉儲。

使用身分驗證

驗證是您 AWS 使用身分認證登入的方式。您必須以 IAM 使用者身分或假設 IAM 角色進行驗證 (登入 AWS)。AWS 帳戶根使用者

您可以使用透過 AWS 身分識別來源提供的認證，以聯合身分識別身分登入。AWS IAM Identity Center (IAM 身分中心) 使用者、貴公司的單一登入身分驗證，以及您的 Google 或 Facebook 登入資料都是聯合身分識別的範例。您以聯合身分登入時，您的管理員先前已設定使用 IAM 角色的聯合身分。當您使 AWS 用同盟存取時，您會間接擔任角色。

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

如果您 AWS 以程式設計方式存取，請 AWS 提供軟體開發套件 (SDK) 和命令列介面 (CLI)，以使用您的認證以加密方式簽署您的要求。如果您不使用 AWS 工具，則必須自行簽署要求。如需使用建議的方法自行簽署請求的詳細資訊，請參閱 IAM 使用者指南中的[簽署 AWS API 請求](#)。

無論您使用何種身分驗證方法，您可能都需要提供額外的安全性資訊。例如，AWS 建議您使用多重要素驗證 (MFA) 來增加帳戶的安全性。如需更多資訊，請參閱 AWS IAM Identity Center 使用者指南中的[多重要素驗證](#)和 IAM 使用者指南中的[在 AWS 中使用多重要素驗證 \(MFA\)](#)。

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。如需這些任務的完整清單，了解需以根使用者登入的任務，請參閱《IAM 使用者指南》中的[需要根使用者憑證的任務](#)。

IAM 使用者和群組

[IAM 使用者](#)是您內部的身份，具 AWS 帳戶有單一人員或應用程式的特定許可。建議您盡可能依賴暫時憑證，而不是擁有建立長期憑證 (例如密碼和存取金鑰) 的 IAM 使用者。但是如果特定使用案例需要擁有長期憑證的 IAM 使用者，建議您輪換存取金鑰。如需更多資訊，請參閱 [IAM 使用者指南](#) 中的為需要長期憑證的使用案例定期輪換存取金鑰。

[IAM 群組](#)是一種指定 IAM 使用者集合的身份。您無法以群組身份簽署。您可以使用群組來一次為多名使用者指定許可。群組可讓管理大量使用者許可的程序變得更為容易。例如，您可以擁有一個名為 IAMAdmins 的群組，並給予該群組管理 IAM 資源的許可。

使用者與角色不同。使用者只會與單一人員或應用程式建立關聯，但角色的目的是在由任何需要它的人員取得。使用者擁有永久的長期憑證，但角色僅提供暫時憑證。如需進一步了解，請參閱 IAM 使用者指南中的[建立 IAM 使用者 \(而非角色\) 的時機](#)。

IAM 角色

[IAM 角色](#)是您 AWS 帳戶 內部具有特定許可的身份。它類似 IAM 使用者，但不與特定的人員相關聯。您可以[切換角色，在中暫時擔任 IAM 角色](#)。AWS Management Console 您可以透過呼叫 AWS CLI 或 AWS API 作業或使用自訂 URL 來擔任角色。如需使用角色的方法詳細資訊，請參閱 IAM 使用者指南中的[使用 IAM 角色](#)。

使用暫時憑證的 IAM 角色在下列情況中非常有用：

- 聯合身份使用者存取 — 如需向聯合身份指派許可，請建立角色，並為角色定義許可。當聯合身份進行身份驗證時，該身份會與角色建立關聯，並獲授予由角色定義的許可。如需有關聯合角色的相關資訊，請參閱 [IAM 使用者指南](#) 中的為第三方身份提供者建立角色。如果您使用 IAM Identity Center，則需要設定許可集。為控制身份驗證後可以存取的內容，IAM Identity Center 將許可集與 IAM 中的角色相關聯。如需有關許可集的資訊，請參閱 AWS IAM Identity Center 使用者指南中的[許可集](#)。
- 暫時 IAM 使用者許可 – IAM 使用者或角色可以擔任 IAM 角色來暫時針對特定任務採用不同的許可。
- 跨帳戶存取權：您可以使用 IAM 角色，允許不同帳戶中的某人 (信任的主體) 存取您帳戶的資源。角色是授予跨帳戶存取權的主要方式。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)。若要了解跨帳戶存取角色和以資源為基礎的政策之間的差異，請參閱 IAM 使用者指南中的 [IAM 中的跨帳戶資源存取](#)。

- 跨服務訪問 — 有些 AWS 服務 使用其他 AWS 服務功能。例如，當您在服務中進行呼叫時，該服務通常會在 Amazon EC2 中執行應用程式或將物件儲存在 Amazon Simple Storage Service (Amazon S3) 中。服務可能會使用呼叫主體的許可、使用服務角色或使用服務連結角色來執行此作業。
- 轉寄存取工作階段 (FAS) — 當您使用 IAM 使用者或角色在中執行動作時 AWS，您會被視為主體。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 會使用主體呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。只有當服務收到需要與其 AWS 服務 他資源互動才能完成的請求時，才會發出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的政策詳細資訊，請參閱 [《轉發存取工作階段》](#)。
- 服務角色 – 服務角色是服務擔任的 [IAM 角色](#)，可代表您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需詳細資訊，請參閱 IAM 使用者指南中的 [建立角色以委派許可給 AWS 服務服務](#)。
- 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，但不能編輯服務連結角色的許可。
- 在 Amazon EC2 上執行的應用程式 — 您可以使用 IAM 角色來管理在 EC2 執行個體上執行的應用程式以及發出 AWS CLI 或 AWS API 請求的臨時登入資料。這是在 EC2 執行個體內儲存存取金鑰的較好方式。若要將 AWS 角色指派給 EC2 執行個體並提供給其所有應用程式，請建立連接至執行個體的執行個體設定檔。執行個體設定檔包含該角色，並且可讓 EC2 執行個體上執行的程式取得暫時憑證。如需詳細資訊，請參閱 IAM 使用者指南中的 [利用 IAM 角色來授予許可給 Amazon EC2 執行個體上執行的應用程式](#)。

若要了解是否要使用 IAM 角色或 IAM 使用者，請參閱《IAM 使用者指南》中的 [建立 IAM 角色 \(而非使用者\) 的時機](#)。

存取控制

您可以持有效憑證來驗證請求，但還須具備許可，才能建立或存取 Amazon Redshift 資源。例如，您必須具備許可，才能建立 Amazon Redshift 叢集、建立快照、新增事件訂閱及其他動作。

以下章節描述如何管理 Amazon Redshift 的許可。我們建議您先閱讀概觀。

- [管理 Amazon Redshift 資源存取許可的概觀](#)
- [將以身分為基礎的政策 \(IAM 政策\) 用於 Amazon Redshift](#)

管理 Amazon Redshift 資源存取許可的概觀

每個 AWS 資源都由一個 AWS 帳號擁有，建立或存取資源的權限由權限原則控制。帳戶管理員可以將許可政策附加到 IAM 身分 (即使用者、群組和角色)，而某些服務 (例如 AWS Lambda) 也支援將權限政策附加至資源。

Note

帳戶管理員 (或管理員使用者) 是具有管理員權限的使用者。如需詳細資訊，請參閱 [《IAM 使用者指南》](#) 中的 IAM 最佳實務。

授予許可時，您會決定誰取得這些許可、取得哪些資源的許可，以及可以對那些資源進行的特定動作。

Amazon Redshift 資源和操作

Amazon Redshift 提供服務特有的資源、動作和條件內容索引鍵，可用於 IAM 許可政策。

Amazon Redshift、Amazon Redshift Serverless、Amazon Redshift 資料 API 和 Amazon Redshift 查詢編輯器 v2 的存取許可

當設定 [存取控制](#) 時，您要編寫可附加到 IAM 身分的許可政策 (身分型政策)。如需詳細的參考資訊，請參閱 [《服務授權參考》](#) 中的下列主題：

- 若為 Amazon Redshift，請參閱使用 redshift: 前置詞的 [Amazon Redshift 的動作、資源和條件索引鍵](#)。
- 若為 Amazon Redshift Serverless，請參閱使用 redshift-serverless: 前置詞的 [Amazon Redshift Serverless 的動作、資源和條件索引鍵](#)。
- 若為 Amazon Redshift 資料 API，請參閱使用 redshift-data: 前置詞的 [Amazon Redshift 資料 API 的動作、資源和條件索引鍵](#)。
- 如需 Amazon Redshift 查詢編輯器 v2，請參閱使用該前置詞的 [AWS SQL 工作台 \(Amazon Redshift 查詢編輯器 v2\) 的動作、資源和條件金鑰](#)。sqlworkbench:

查詢編輯器 v2 包含非直接對應至 API 操作的僅限許可動作。《服務授權參考》中會使用 [permission only] 指出這些動作。

《服務授權參考》包含了可在 IAM 政策中使用哪些 API 操作的相關資訊。它還包括您可以授與權限的 AWS 資源，以及可包含用於精細存取控制的條件金鑰。如需條件的相關資訊，請參閱 [使用 IAM 政策條件進行精細定義存取控制](#)。

您可以在政策的 Action 欄位中指定動作、在政策的 Resource 欄位中指定資源值，以及在政策的 Condition 欄位中指定條件。若要指定 Amazon Redshift 的動作，請使用後接 API 操作名稱的 redshift: 前置詞 (例如，redshift:CreateCluster)。

了解資源所有權

資源擁有者是建立資源的 AWS 帳號。也就是說，資源擁有者是驗證建立資源之請求的主體實體 (根帳戶、IAM 使用者或 IAM 角色) 的帳戶。AWS 下列範例說明其如何運作：

- 如果您使用帳戶的根帳戶登入資料建立資料庫叢集，您的 AWS 帳戶就是 Amazon Redshift 資源的擁有者。AWS
- 如果您在 AWS 帳戶中建立具有建立 Amazon Redshift 資源許可的 IAM 角色，則任何可以擔任該角色的人都可以建立 Amazon Redshift 資源。您的 AWS 帳戶 (即角色所屬帳戶) 會擁有 Amazon Redshift 資源。
- 如果您在 AWS 帳戶中建立 IAM 使用者，並將建立 Amazon Redshift 資源的許可授與該使用者，則該使用者可以建立 Amazon Redshift 資源。不過，您的 AWS 帳戶 (該使用者所屬的帳戶) 擁有 Amazon Redshift 資源。在大多數情況下，不建議您使用此方法。建議您建立 IAM 角色並將許可附加到該角色，然後將角色指派給使用者。

管理資源存取

許可政策會描述誰可以存取什麼資源。下面這節會說明用於建立許可政策的可用選項。

Note

本節著重討論如何在 Amazon Redshift 的環境中使用 IAM。它不提供 IAM 服務的詳細資訊。如需完整的 IAM 文件，請參閱《IAM 使用者指南》中的[什麼是 IAM?](#)。如需有關 IAM 政策語法和說明的資訊，請參閱《IAM 使用者指南》中的[AWS IAM 政策參考](#)。

連接到 IAM 身分的政策稱為身分類型政策 (IAM 政策)，而連接到資源的政策參考資源類型政策。Amazon Redshift 僅支援以身分為基礎的政策 (IAM 政策)。

身分類型政策 (IAM 政策)

您可以透過將政策附加到 IAM 角色，然後將該角色指派給使用者或群組來指派許可。以下是範例政策，其中包含為您的 AWS 帳戶建立、刪除、修改和重新啟動 Amazon Redshift 叢集的許可。

```
{
```

```
"Version": "2012-10-17",
"Statement": [
  {
    "Sid": "AllowManageClusters",
    "Effect": "Allow",
    "Action": [
      "redshift:CreateCluster",
      "redshift>DeleteCluster",
      "redshift:ModifyCluster",
      "redshift:RebootCluster"
    ],
    "Resource": "*"
  }
]
```

如需將以身分為基礎的政策與 Amazon Redshift 搭配使用的相關資訊，請參閱[將以身分為基礎的政策 \(IAM 政策\) 用於 Amazon Redshift](#)。如需使用者、群組、角色和許可的相關資訊，請參閱《IAM 使用者指南》中的[身分 \(使用者、群組和角色\)](#)。

資源型政策

其他服務 (例如 Amazon S3) 也支援以資源為基礎的許可政策。例如，您可以將政策連接至 S3 儲存貯體，以管理該儲存貯體的存取許可。Amazon Redshift 不支援資源型政策。

指定政策元素：動作、效果、資源和主體

針對每一個 Amazon Redshift 資源 (請參閱[Amazon Redshift 資源和操作](#))，服務會定義一組 API 操作 (請參閱[動作](#))。Amazon Redshift 會定義一組您可在政策中指定的動作，以授予這些 API 操作的許可。執行一項 API 操作可能需要多個動作的許可。

以下是基本的政策元素：

- 資源 – 在政策中，您可以使用 Amazon Resource Name (ARN) 來識別要套用政策的資源。如需詳細資訊，請參閱[Amazon Redshift 資源和操作](#)。
- 動作：使用動作關鍵字識別您要允許或拒絕的資源操作。例如，`redshift:DescribeClusters` 許可會讓使用者獲得執行 Amazon Redshift `DescribeClusters` 操作的許可。
- 效果 - 您可以指定使用者要求特定動作時會有什麼效果；可為允許或拒絕。如果您未明確授予存取 (允許) 資源，則隱含地拒絕存取。您也可以明確拒絕資源存取，這樣做可確保使用者無法存取資源，即使不同政策授予存取也是一樣。

- 委託人：在以身分為基礎的政策 (IAM 政策) 中，政策所連接的使用者就是隱含委託人。對於資源型政策，您可以指定想要收到許可的使用者、帳戶、服務或其他實體 (僅適用於資源型政策)。Amazon Redshift 不支援資源型政策。

如需進一步了解有關 IAM 政策語法和說明的詳細資訊，請參閱《IAM 使用者指南》中的 [AWS IAM 政策參考](#)。

如需詳列所有 Amazon Redshift API 動作及適用資源的表格，請參閱 [Amazon Redshift、Amazon Redshift Serverless、Amazon Redshift 資料 API 和 Amazon Redshift 查詢編輯器 v2 的存取許可](#)。

在政策中指定條件

當您授予許可時，可以使用存取政策語言來指定政策應該何時生效的條件。例如，建議只在特定日期之後套用政策。如需以存取政策語言指定條件的相關資訊，請參閱《IAM 使用者指南》中的 [IAM JSON 政策元素：條件](#)。

若要識別許可政策適用的條件，請在您的 IAM 許可政策中包含 Condition 元素。例如，您可以建立允許使用者使用 `redshift:CreateCluster` 動作來建立叢集的政策，並且可以新增 Condition 元素，將該使用者限制在僅限於特定區域中建立叢集。如需詳細資訊，請參閱 [使用 IAM 政策條件進行精細定義存取控制](#)。如需呈現所有條件索引鍵值以及 Amazon Redshift 動作和其套用之資源的清單，請參閱 [Amazon Redshift、Amazon Redshift Serverless、Amazon Redshift 資料 API 和 Amazon Redshift 查詢編輯器 v2 的存取許可](#)。

使用 IAM 政策條件進行精細定義存取控制

在 Amazon Redshift 中，您可以使用兩個條件索引鍵，根據那些資源的標籤來限制對資源的存取權限。下列是常見的 Amazon Redshift 條件索引鍵。

條件金鑰	描述
<code>aws:RequestTag</code>	每當使用者建立資源時，都會要求使用者包括標籤索引鍵 (名稱) 和值。如需詳細資訊，請參閱 IAM 使用者指南RequestTag中的 aws: 。
<code>aws:ResourceTag</code>	根據特定標籤索引鍵和值，限制使用者對資源的存取。如需詳細資訊，請參閱 IAM 使用者指南ResourceTag中的 aws: 。
<code>aws:TagKeys</code>	使用此鍵來將請求中的標籤鍵與您在政策中所指定的鍵進行比較。如需詳細資訊，請參閱 IAM 使用者指南TagKeys中的 aws: 。

如需標籤的詳細資訊，請參閱[標記概觀](#)。

如需支援 `redshift:RequestTag` 和 `redshift:ResourceTag` 條件索引鍵的 API 動作清單，請參閱[Amazon Redshift](#)、[Amazon Redshift Serverless](#)、[Amazon Redshift 資料 API](#) 和 [Amazon Redshift 查詢編輯器 v2 的存取許可](#)。

下列條件金鑰可與 Amazon Redshift `GetClusterCredentials` 動作搭配使用。

條件金鑰	描述
<code>redshift:DurationSeconds</code>	限制可為持續時間指定的秒數。
<code>redshift:DbName</code>	限制可以指定的資料庫名稱。
<code>redshift:DbUser</code>	限制可以指定的資料庫使用者名稱。

範例 1：使用 `aws:ResourceTag` 條件金鑰限制存取

使用下列 IAM 政策，讓使用者僅針對 `us-west-2` 區域中具有標籤值命名 `environment` 的特定 AWS 帳戶修改 Amazon Redshift 叢集。test

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "AllowModifyTestCluster",
    "Effect": "Allow",
    "Action": "redshift:ModifyCluster",
    "Resource": "arn:aws:redshift:us-west-2:123456789012:cluster:*",
    "Condition": {
      "StringEquals": {
        "aws:ResourceTag/environment": "test"
      }
    }
  }
}
```

範例 2：使用 aws: RequestTag 條件金鑰限制存取

使用下列 IAM 政策可讓使用者僅在建立叢集的命令包含名為 usage 的標籤和標籤值為 production 時建立 Amazon Redshift 叢集。aws:TagKeys 和 ForAllValues 修飾符的條件指定您在請求中只能指定金鑰 costcenter 和 usage。

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "AllowCreateProductionCluster",
    "Effect": "Allow",
    "Action": [
      "redshift:CreateCluster",
      "redshift:CreateTags"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:RequestTag/usage": "production"
      },
      "ForAllValues:StringEquals": {
        "aws:TagKeys": [
          "costcenter",
          "usage"
        ]
      }
    }
  }
}
```

將以身分為基礎的政策 (IAM 政策) 用於 Amazon Redshift

這個主題提供以身分為基礎的政策範例，在該政策中帳戶管理員可以將許可政策連接至 IAM 身分 (即使用者、群組和角色)。

Important

建議您先檢閱簡介主題，其中說明基本概念及有何選項可供您管理對 Amazon Redshift 資源的存取。如需詳細資訊，請參閱 [管理 Amazon Redshift 資源存取許可的概觀](#)。

以下顯示許可政策範例。此原則可讓使用者建立、刪除、修改和重新啟動所有叢集，然後拒絕刪除或修改叢集識別碼以 production in AWS 區域 us-west-2 和 AWS 帳戶 123456789012 開頭的任何叢集的權限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowClusterManagement",
      "Action": [
        "redshift:CreateCluster",
        "redshift>DeleteCluster",
        "redshift:ModifyCluster",
        "redshift:RebootCluster"
      ],
      "Resource": [
        "*"
      ],
      "Effect": "Allow"
    },
    {
      "Sid": "DenyDeleteModifyProtected",
      "Action": [
        "redshift>DeleteCluster",
        "redshift:ModifyCluster"
      ],
      "Resource": [
        "arn:aws:redshift:us-west-2:123456789012:cluster:production*"
      ],
      "Effect": "Deny"
    }
  ]
}
```

此政策具有兩個陳述式：

- 第一個陳述式會將某使用者的許可授予給另一位使用者，讓該使用者得以建立、刪除、修改叢集和將它們重新開機。該陳述式會指定萬用字元 (*) 做為 Resource 值，以便該政策適用於根 AWS 帳戶擁有的所有 Amazon Redshift 資源。
- 第二個陳述式會拒絕對叢集的刪除或修改許可。此陳述式會為包含萬用字元 (*) 的 Resource 值指定叢集 Amazon Resource Name (ARN)。因此，此陳述式適用於叢集識別碼開頭為根 AWS 帳戶所擁有的所有 Amazon Redshift 叢集。production

AWS Amazon Redshift 的受管政策

AWS 透過提供由建立和管理的獨立 IAM 政策來解決許多常見使用案例 AWS。受管政策授與常見使用案例中必要的許可，讓您免於查詢需要哪些許可。如需詳細資訊，請參閱《IAM 使用者指南》中的 [AWS 受管政策](#)。

您也能建立專屬的自訂 IAM 政策，以允許 Amazon Redshift API 操作與資源的相關許可。您可以將這些自訂政策附加至需要這些許可的 IAM 角色或群組。

以下各節說明 AWS 受管政策，您可以將這些政策附加到帳戶中的使用者，並且特定於 Amazon Redshift。

AmazonRedshiftReadOnly存取

授予 AWS 帳戶所有 Amazon Redshift 資源的唯讀存取權。

您可以在 IAM 主控台上找到 [AmazonRedshiftReadOnly存取](#) 政策，並在 AWS 受管政策參考指南中找到 [AmazonRedshiftReadOnlyAccess](#)。

AmazonRedshiftFullAccess

授予 AWS 帳戶所有 Amazon Redshift 資源的完整存取權。此外，這個政策還會授予所有 Amazon Redshift Serverless 資源的完整存取權。

您可以在 IAM 主控台和 AWS 受管 [AmazonRedshiftFullAccess](#) 政策參考指南 [AmazonRedshiftFullAccess](#) 中找到該政策。

AmazonRedshiftQueryEditor

授予 Amazon Redshift 主控台上查詢編輯器的完整存取權。

您可以在 IAM 主控台和 AWS 受管 [AmazonRedshiftQueryEditor](#) 政策參考指南 [AmazonRedshiftQueryEditor](#) 中找到該政策。

AmazonRedshiftDataFull存取

授予 AWS 帳戶對 Amazon Redshift 資料 API 操作和資源的完整存取權。

您可以在 IAM 主控台上找到 [AmazonRedshiftDataFull存取](#) 政策，並在 AWS 受管政策參考指南中找到 [AmazonRedshiftDataFullAccess](#)。

AmazonRedshiftQueryEditorV2 FullAccess

授予 Amazon Redshift 查詢編輯器 v2 操作和資源的完整存取權。此政策也會授予其他必要服務的存取權。

您可以FullAccess在 IAM 主控台和 [AmazonRedshiftQueryEditorV2](#) 上找到 [AmazonRedshiftQueryEditorV2 FullAccess](#) 政策，請參閱受AWS 管政策參考指南。

AmazonRedshiftQueryEditorV2 NoSharing

授予使用 Amazon Redshift 查詢編輯器 v2 的能力，而不共用資源。此政策也會授予其他必要服務的存取權。使用此政策的主體無法標記其資源 (例如查詢)，以便與相同 AWS 帳戶中的其他主體共用。

您可以NoSharing在 IAM 主控台和 [AmazonRedshiftQueryEditorV2](#) 上找到 [AmazonRedshiftQueryEditorV2 NoSharing](#) 政策，請參閱受AWS 管政策參考指南。

AmazonRedshiftQueryEditorV2 ReadSharing

授予使用 Amazon Redshift 查詢編輯器 v2 的能力，並可有限度地共用資源。此政策也會授予其他必要服務的存取權。使用此政策的主體可以標記其資源 (例如查詢)，以便與相同 AWS 帳戶中的其他主體共用。獲得授予的主體可以讀取與其團隊共用的資源，但無法更新這些資源。

您可以ReadSharing在 IAM 主控台和 [AmazonRedshiftQueryEditorV2](#) 上找到 [AmazonRedshiftQueryEditorV2 ReadSharing](#) 政策，請參閱受AWS 管政策參考指南。

AmazonRedshiftQueryEditor第二版ReadWrite分享

授予使用 Amazon Redshift 查詢編輯器 v2 的能力，並可共用資源。此政策也會授予其他必要服務的存取權。使用此政策的主體可以標記其資源 (例如查詢)，以便與相同 AWS 帳戶中的其他主體共用。獲得授予的主體可以讀取和更新與其團隊共用的資源。

您可以在 IAM 主控台上找到 [AmazonRedshiftQueryEditorV2 ReadWrite 共用](#) 政策，並在AWS 受管政策參考指南中找到 [AmazonRedshiftQueryEditorV2 ReadWrite 共用](#) 政策。

AmazonRedshiftServiceLinkedRolePolicy

您無法附加 AmazonRedshiftServiceLinkedRolePolicy 到 IAM 實體。此政策會附加至服務連結角色，可讓 Amazon Redshift 存取帳戶資源。如需詳細資訊，請參閱 [為 Amazon Redshift 使用服務連結角色](#)。

您可以在 IAM 主控台和AWS 受管 [AmazonRedshiftServiceLinkedRolePolicy](#) 政策參考指南 [AmazonRedshiftServiceLinkedRolePolicy](#) 中找到該政策。

AmazonRedshiftAllCommandsFullAccess

授予相關能力，而能夠使用從 Amazon Redshift 主控台建立的 IAM 角色，並將其設定為叢集的預設值，以便執行 COPY (從 Amazon S3)、UNLOAD、CREATE EXTERNAL SCHEMA、CREATE EXTERNAL FUNCTION 和 CREATE MODEL 命令。該政策還授予對相關服務 (例如 Amazon S3、CloudWatch 日誌、Amazon 或) 執行 SELECT 陳述式的許可 AWS Glue。 SageMaker

您可以在 IAM 主控台和AWS 受管[AmazonRedshiftAllCommandsFullAccess](#)政策參考指南[AmazonRedshiftAllCommandsFullAccess](#)中找到該政策。

您也能建立專屬的自訂 IAM 政策，以允許 Amazon Redshift API 操作與資源的相關許可。您可以將這些自訂政策附加至需要這些許可的 IAM 角色或群組。

Amazon Redshift 對 AWS 受管政策的更新

檢視有關 Amazon Redshift AWS 受管政策更新的詳細資訊，因為此服務開始追蹤這些變更。如需有關此頁面變更的自動提醒，請訂閱 Amazon Redshift 文件歷史記錄頁面上的 RSS 摘要。

變更	描述	日期
AmazonRedshiftQueryEditorV2 FullAccess – 更新現有政策	redshift-serverless:ListNamespaces 和 redshift-serverless:ListWorkgroups 動作的許可已新增至受管政策。新增它們會授予在 Amazon Redshift 資料倉儲中列出無伺服器命名空間和無伺服器工作群組的權限。	2024年2月21 日
AmazonRedshiftQueryEditorV2 NoSharing – 更新現有政策	redshift-serverless:ListNamespaces 和 redshift-serverless:ListWorkgroups 動作的許可已新增至受管政策。新增它們會授予在 Amazon	2024年2月21 日

變更	描述	日期
	Redshift 資料倉儲中列出無伺服器命名空間和無伺服器工作群組的權限。	
AmazonRedshiftQueryEditorV2 ReadSharing – 更新現有政策	redshift-serverless:ListNamespaces 和 redshift-serverless:ListWorkgroups 動作的許可已新增至受管政策。新增它們會授予在 Amazon Redshift 資料倉儲中列出無伺服器命名空間和無伺服器工作群組的權限。	2024年2月21 日
AmazonRedshiftQueryEditor第二版ReadWrite分享 – 更新現有政策	redshift-serverless:ListNamespaces 和 redshift-serverless:ListWorkgroups 動作的許可已新增至受管政策。新增它們會授予在 Amazon Redshift 資料倉儲中列出無伺服器命名空間和無伺服器工作群組的權限。	2024年2月21 日
AmazonRedshiftReadOnly存取 – 更新現有政策	redshift:ListRecommendations 動作的許可已新增至受管政策。這將授予列出 Amazon Redshift 顧問建議的權限。	2024年2月7日
AmazonRedshiftServiceLinkedRolePolicy – 更新現有政策	ec2:AssignIpv6Addresses 和 ec2:UnassignIpv6Addresses 動作的許可已新增至受管政策。新增這兩個動作可准許指派和取消指派 IP 地址。	2023 年 10 月 31 日

變更	描述	日期
AmazonRedshiftQueryEditorV2 NoSharing – 更新現有政策	sqlworkbench:GetAutocompletionMetadata 和 sqlworkbench:GetAutocompletionResource 動作的許可已新增至受管政策。新增這兩個動作可准許產生和擷取資料庫資訊，以便在編輯查詢時自動完成 SQL。	2023 年 8 月 16 日
AmazonRedshiftQueryEditorV2 ReadSharing – 更新現有政策	sqlworkbench:GetAutocompletionMetadata 和 sqlworkbench:GetAutocompletionResource 動作的許可已新增至受管政策。新增這兩個動作可准許產生和擷取資料庫資訊，以便在編輯查詢時自動完成 SQL。	2023 年 8 月 16 日
AmazonRedshiftQueryEditor 第二版ReadWrite分享 – 更新現有政策	sqlworkbench:GetAutocompletionMetadata 和 sqlworkbench:GetAutocompletionResource 動作的許可已新增至受管政策。新增這兩個動作可准許產生和擷取資料庫資訊，以便在編輯查詢時自動完成 SQL。	2023 年 8 月 16 日

變更	描述	日期
AmazonRedshiftServiceLinkedRolePolicy – 更新現有政策	<p>建立和管理密碼 AWS Secrets Manager 的動作權限會新增至受管理的策略。已新增的許可如下：</p> <ul style="list-style-type: none">• <code>secretsmanager:GetRandomPassword</code>• <code>secretsmanager:DescribeSecret</code>• <code>secretsmanager:PutSecretValue</code>• <code>secretsmanager:UpdateSecret</code>• <code>secretsmanager:UpdateSecretVersionStage</code>• <code>secretsmanager:RotateSecret</code>• <code>secretsmanager>DeleteSecret</code>	2023 年 8 月 14 日

變更	描述	日期
AmazonRedshiftServiceLinkedRolePolicy – 更新現有政策	<p>Amazon EC2 上用來建立和管理安全群組與路由規則的動作許可已從受管政策中移除。這些許可與建立子網路和 VPC 有關。已移除的許可如下：</p> <ul style="list-style-type: none"> • ec2:AuthorizeSecurityGroupEgress • ec2:AuthorizeSecurityGroupIngress • ec2:UpdateSecurityGroupRuleDescriptionsEgress • ec2:ReplaceRouteTableAssociation • ec2:CreateRouteTable • ec2:AttachInternetGateway • ec2:UpdateSecurityGroupRuleDescriptionsIngress • ec2:AssociateRouteTable • ec2:RevokeSecurityGroupIngress • ec2:CreateRoute • ec2:CreateSecurityGroup • ec2:RevokeSecurityGroupEgress 	2023 年 5 月 8 日

變更	描述	日期
	<ul style="list-style-type: none"> • ec2:ModifyVpcAttribute • ec2:CreateSubnet • ec2:CreateInternetGateway • ec2:CreateVpc <p>這些與目的:RedshiftMigrateToVpc資源標籤相關聯。這個標籤將許可的適用範圍限制在 Amazon EC2 Classic 到 Amazon EC2 VPC 的遷移任務。如需資源標籤的相關資訊，請參閱使用標籤來控制 AWS 資源的存取權。</p>	
AmazonRedshiftDataFull存取 – 更新現有政策	redshift:GetClusterCredentialsWithIAM 動作的許可已新增至受管政策。新增此項目可准許取得增強型臨時憑證，讓指定的 AWS 帳戶存取 Amazon Redshift 資料庫。	2023 年 4 月 7 日
AmazonRedshiftServiceLinkedRolePolicy – 更新現有政策	Amazon EC2 上用於建立和管理安全群組規則的動作許可已新增至受管政策。這些安全群組和規則特別與 Amazon Redshift aws:RequestTag/Redshift 資源標籤相關聯。這會將許可的適用範圍限制在特定的 Amazon Redshift 資源。	2023 年 4 月 6 日

變更	描述	日期
AmazonRedshiftQueryEditorV2 NoSharing – 更新現有政策	sqlworkbench:GetSchemaInference 動作的許可已新增至受管政策。新增此項目可准許取得從檔案中推斷出的資料欄和資料類型。	2023 年 3 月 21 日
AmazonRedshiftQueryEditorV2 ReadSharing – 更新現有政策	sqlworkbench:GetSchemaInference 動作的許可已新增至受管政策。新增此項目可准許取得從檔案中推斷出的資料欄和資料類型。	2023 年 3 月 21 日
AmazonRedshiftQueryEditor第二版ReadWrite分享 – 更新現有政策	sqlworkbench:GetSchemaInference 動作的許可已新增至受管政策。新增此項目可准許取得從檔案中推斷出的資料欄和資料類型。	2023 年 3 月 21 日
AmazonRedshiftQueryEditorV2 NoSharing – 更新現有政策	sqlworkbench:AssociateNotebookWithTab 動作的許可已新增至受管政策。新增此項目可准許建立和更新連結至使用者自有筆記本的標籤。	2023 年 2 月 2 日
AmazonRedshiftQueryEditorV2 ReadSharing – 更新現有政策	sqlworkbench:AssociateNotebookWithTab 動作的許可已新增至受管政策。新增此項目可准許建立和更新連結至使用者自有筆記本或連結至與其共用之筆記本的標籤。	2023 年 2 月 2 日

變更	描述	日期
AmazonRedshiftQueryEditor第二版ReadWrite分享 – 更新現有政策	sqlworkbench:AssociateNotebookWithTab 動作的許可已新增至受管政策。新增此項目可准許建立和更新連結至使用者自有筆記本或連結至與其共用之筆記本的標籤。	2023 年 2 月 2 日

變更	描述	日期
AmazonRedshiftQueryEditorV2 NoSharing – 更新現有政策	<p>為了授予使用筆記本的許可，Amazon Redshift 已新增下列動作的許可：</p> <ul style="list-style-type: none"> • sqlworkbench:ListNotebooks • sqlworkbench:CreateNotebook • sqlworkbench:DuplicateNotebook • sqlworkbench:CreateNotebookFromVersion • sqlworkbench:ImportNotebook • sqlworkbench:GetNotebook • sqlworkbench:UpdateNotebook • sqlworkbench>DeleteNotebook • sqlworkbench:CreateNotebookCell • sqlworkbench>DeleteNotebookCell • sqlworkbench:UpdateNotebookCellContent • sqlworkbench:UpdateNotebookCellLayout 	2022 年 10 月 17 日

變更	描述	日期
	<ul style="list-style-type: none">• <code>sqlworkbench:BatchGetNotebookCell</code>• <code>sqlworkbench:ListNotebookVersions</code>• <code>sqlworkbench:CreateNotebookVersion</code>• <code>sqlworkbench:GetNotebookVersion</code>• <code>sqlworkbench>DeleteNotebookVersion</code>• <code>sqlworkbench:RestoreNotebookVersion</code>• <code>sqlworkbench:ExportNotebook</code>	

變更	描述	日期
AmazonRedshiftQueryEditorV2 ReadSharing – 更新現有政策	<p>為了授予使用筆記本的許可，Amazon Redshift 已新增下列動作的許可：</p> <ul style="list-style-type: none"> • sqlworkbench:ListNotebooks • sqlworkbench:CreateNotebook • sqlworkbench:DuplicateNotebook • sqlworkbench:CreateNotebookFromVersion • sqlworkbench:ImportNotebook • sqlworkbench:GetNotebook • sqlworkbench:UpdateNotebook • sqlworkbench>DeleteNotebook • sqlworkbench:CreateNotebookCell • sqlworkbench>DeleteNotebookCell • sqlworkbench:UpdateNotebookCellContent • sqlworkbench:UpdateNotebookCellLayout 	2022 年 10 月 17 日

變更	描述	日期
	<ul style="list-style-type: none">• <code>sqlworkbench:BatchGetNotebookCell</code>• <code>sqlworkbench:ListNotebookVersions</code>• <code>sqlworkbench:CreateNotebookVersion</code>• <code>sqlworkbench:GetNotebookVersion</code>• <code>sqlworkbench>DeleteNotebookVersion</code>• <code>sqlworkbench:RestoreNotebookVersion</code>• <code>sqlworkbench:ExportNotebook</code>	

變更	描述	日期
AmazonRedshiftQueryEditor第二版ReadWrite分享 – 更新現有政策	<p>為了授予使用筆記本的許可，Amazon Redshift 已新增下列動作的許可：</p> <ul style="list-style-type: none"> • sqlworkbench:ListNotebooks • sqlworkbench:CreateNotebook • sqlworkbench:DuplicateNotebook • sqlworkbench:CreateNotebookFromVersion • sqlworkbench:ImportNotebook • sqlworkbench:GetNotebook • sqlworkbench:UpdateNotebook • sqlworkbench>DeleteNotebook • sqlworkbench:CreateNotebookCell • sqlworkbench>DeleteNotebookCell • sqlworkbench:UpdateNotebookCellContent • sqlworkbench:UpdateNotebookCellLayout 	2022 年 10 月 17 日

變更	描述	日期
	<ul style="list-style-type: none"> • sqlworkbench:BatchGetNotebookCell • sqlworkbench:ListNotebookVersions • sqlworkbench:CreateNotebookVersion • sqlworkbench:GetNotebookVersion • sqlworkbench>DeleteNotebookVersion • sqlworkbench:RestoreNotebookVersion • sqlworkbench:ExportNotebook 	
AmazonRedshiftServiceLinkedRolePolicy – 更新現有政策	Amazon Redshift 添加了命名空間，AWS/Redshift 以允許將指標發佈到 CloudWatch.	2022 年 9 月 7 日
AmazonRedshiftQueryEditorV2 NoSharing – 更新現有政策	Amazon Redshift 已新增動作 sqlworkbench:ListQueryExecutionHistory 和 sqlworkbench:GetQueryExecutionHistory 的許可。這可准許查看查詢歷史記錄。	2022 年 8 月 30 日
AmazonRedshiftQueryEditorV2 ReadSharing – 更新現有政策	Amazon Redshift 已新增動作 sqlworkbench:ListQueryExecutionHistory 和 sqlworkbench:GetQueryExecutionHistory 的許可。這可准許查看查詢歷史記錄。	2022 年 8 月 30 日

變更	描述	日期
AmazonRedshiftQueryEditor第二版ReadWrite分享 – 更新現有政策	Amazon Redshift 已新增動作 <code>sqlworkbench:ListQueryExecutionHistory</code> 和 <code>sqlworkbench:GetQueryExecutionHistory</code> 的許可。這可准許查看查詢歷史記錄。	2022 年 8 月 30 日
AmazonRedshiftFullAccess – 更新現有政策	Amazon Redshift 無伺服器的許可會新增至現有的 <code>AmazonRedshiftFullAccess</code> 受管政策。	2022 年 7 月 22 日
AmazonRedshiftDataFull存取 – 更新現有政策	Amazon Redshift 已將標籤 <code>aws:ResourceTag/RedshiftDataFullAccess</code> 許可的 <code>redshift-serverless:GetCredentials</code> 預設範圍條件從 <code>StringEquals</code> 更新為 <code>StringLike</code> ，以授予標記了標籤索引鍵 <code>RedshiftDataFullAccess</code> 和任何標籤值之資源的存取權。	2022 年 7 月 11 日
AmazonRedshiftDataFull存取 – 更新現有政策	Amazon Redshift 已新增新的許可，以允許使用 <code>redshift-serverless:GetCredentials</code> 獲得 Amazon Redshift Serverless 的臨時憑證。	2022 年 7 月 8 日

變更	描述	日期
AmazonRedshiftQueryEditorV2 NoSharing – 更新現有政策	Amazon Redshift 已增加動作 <code>sqlworkbench:GetAccountSettings</code> 的許可。這可准許取得帳戶設定。	2022 年 6 月 15 日
AmazonRedshiftQueryEditorV2 ReadSharing – 更新現有政策	Amazon Redshift 已增加動作 <code>sqlworkbench:GetAccountSettings</code> 的許可。這可准許取得帳戶設定。	2022 年 6 月 15 日
AmazonRedshiftQueryEditor 第二版ReadWrite分享 – 更新現有政策	Amazon Redshift 已增加動作 <code>sqlworkbench:GetAccountSettings</code> 的許可。這可准許取得帳戶設定。	2022 年 6 月 15 日
AmazonRedshiftServiceLinkedRolePolicy – 更新現有政策	為了能夠公開存取新的 Amazon Redshift Serverless 端點，Amazon Redshift 會將彈性 IP 地址配置並關聯到客戶帳戶中 VPC 端點的彈性網路介面。其會透過服務連結角色所提供的許可來執行此操作。為了實現這個使用案例，用來配置和釋放彈性 IP 地址的動作已新增至 Amazon Redshift Serverless 服務連結角色。	2022 年 5 月 26 日
AmazonRedshiftQueryEditorV2 FullAccess – 更新現有政策	動作 <code>sqlworkbench:ListTaggedResources</code> 的許可。其具體的適用範圍是 Amazon Redshift 查詢編輯器 v2 資源。此政策更新提供了只能透過查詢編輯器 v2 呼叫 <code>tag:GetResources</code> 的權利。	2022 年 2 月 22 日

變更	描述	日期
AmazonRedshiftQueryEditorV2 NoSharing – 更新現有政策	動作 <code>sqlworkbench:ListTaggedResources</code> 的許可。其具體的適用範圍是 Amazon Redshift 查詢編輯器 v2 資源。此政策更新提供了只能透過查詢編輯器 v2 呼叫 <code>tag:GetResources</code> 的權利。	2022 年 2 月 22 日
AmazonRedshiftQueryEditorV2 ReadSharing – 更新現有政策	動作 <code>sqlworkbench:ListTaggedResources</code> 的許可。其具體的適用範圍是 Amazon Redshift 查詢編輯器 v2 資源。此政策更新提供了只能透過查詢編輯器 v2 呼叫 <code>tag:GetResources</code> 的權利。	2022 年 2 月 22 日
AmazonRedshiftQueryEditor第二版ReadWrite分享 – 更新現有政策	動作 <code>sqlworkbench:ListTaggedResources</code> 的許可。其具體的適用範圍是 Amazon Redshift 查詢編輯器 v2 資源。此政策更新提供了只能透過查詢編輯器 v2 呼叫 <code>tag:GetResources</code> 的權利。	2022 年 2 月 22 日
AmazonRedshiftQueryEditorV2 ReadSharing – 更新現有政策	<code>sqlworkbench:AssociateQueryWithTab</code> 動作的許可已新增至受管政策。新增此項目讓客戶得以建立會連結至與其共用之查詢的編輯器標籤。	2022 年 2 月 22 日

變更	描述	日期
AmazonRedshiftServiceLinkedRolePolicy – 更新現有政策	Amazon Redshift 已新增新動作的許可，以允許管理 Amazon Redshift 網路和 VPC 資源。	2021 年 11 月 22 日
AmazonRedshiftAllCommandsFullAccess – 新政策	Amazon Redshift 已新增一項新政策，以允許使用從 Amazon Redshift 主控台建立的 IAM 角色，並將其設定為叢集的預設值，以便執行 COPY (從 Amazon S3)、UNLOAD、CREATE EXTERNAL SCHEMA、CREATE EXTERNAL FUNCTION、CREATE MODEL 或 CREATE LIBRARY 命令。	2021 年 11 月 18 日
AmazonRedshiftServiceLinkedRolePolicy – 更新現有政策	Amazon Redshift 為新動作新增了許可，以允許管理 Amazon Redshift CloudWatch 日誌群組和日誌串流，包括稽核日誌匯出。	2021 年 11 月 15 日
AmazonRedshiftFullAccess – 更新現有政策	Amazon Redshift 已新增新的許可，以允許模型可解釋性、DynamoDB、Redshift Spectrum 和 Amazon RDS 聯合。	2021 年 10 月 7 日
AmazonRedshiftQueryEditorV2 FullAccess – 新政策	Amazon Redshift 已新增一項新政策，以允許 Amazon Redshift 查詢編輯器 v2 的完整存取權。	2021 年 9 月 24 日

變更	描述	日期
AmazonRedshiftQueryEditorV2 NoSharing – 新政策	Amazon Redshift 已新增一項新政策，以允許在不共用資源的情況下使用 Amazon Redshift 查詢編輯器 v2。	2021 年 9 月 24 日
AmazonRedshiftQueryEditorV2 ReadSharing – 新政策	Amazon Redshift 已新增一項新政策，以允許在 Amazon Redshift 查詢編輯器 v2 內進行讀取共用。	2021 年 9 月 24 日
AmazonRedshiftQueryEditor 第二版ReadWrite分享 – 新政策	Amazon Redshift 已新增一項新政策，以允許在 Amazon Redshift 查詢編輯器 v2 內進行讀取和更新共用。	2021 年 9 月 24 日
AmazonRedshiftFullAccess – 更新現有政策	Amazon Redshift 已新增新的許可，以允許 sagemaker : *Job* 。	2021 年 8 月 18 日
AmazonRedshiftDataFull存取 – 更新現有政策	Amazon Redshift 已新增新的許可，以允許 Authorize DataShare 。	2021 年 8 月 12 日
AmazonRedshiftDataFull存取 – 更新現有政策	Amazon Redshift 已新增新的許可，以允許 BatchExecuteStatement 。	2021 年 7 月 27 日
Amazon Redshift 已開始追蹤變更	Amazon Redshift 開始追蹤其 AWS 受管政策的變更。	2021 年 7 月 27 日

要使用 Redshift Spectrum 所需的許可

Amazon Redshift Spectrum 需要其他 AWS 服務的許可才能存取資源。如需有關 Redshift Spectrum IAM 政策中許可的詳細資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的 [Amazon Redshift Spectrum 的 IAM 政策](#)。

要使用 Amazon Redshift 主控台所需的許可

若要讓使用者使用 Amazon Redshift 主控台，該使用者必須擁有一組最低限度的許可，才能讓使用者描述其 AWS 帳戶的 Amazon Redshift 資源。這些許可還必須允許使用者描述其他相關資訊，包括 Amazon EC2 安全性 CloudWatch、Amazon、Amazon SNS 和網路資訊。

如果您建立比最基本必要許可更嚴格的 IAM 政策，則對於採取該 IAM 政策的使用者而言，主控台就無法如預期運作。為確保這些使用者仍可使用 Amazon Redshift 主控台，也請將 `AmazonRedshiftReadOnlyAccess` 受管政策附加至使用者。若要了解如何執行這項操作，請參閱 [AWS Amazon Redshift 的受管政策](#)。

如需有關向使用者提供 Amazon Redshift 主控台上查詢編輯器存取權的資訊，請參閱 [要使用 Amazon Redshift 主控台查詢編輯器所需的許可](#)。

您不需要為只對 AWS CLI 或 Amazon Redshift API 進行呼叫的使用者允許最低主控台許可。

要使用 Amazon Redshift 主控台查詢編輯器所需的許可

使用者若要使用 Amazon Redshift 查詢編輯器，就必須擁有一組包含 Amazon Redshift 和 Amazon Redshift 資料 API 操作的最基本許可。若要使用機密連線到資料庫，您也必須擁有 Secrets Manager 許可。

若要讓使用者在 Amazon Redshift 主控台上存取查詢編輯器，請附加 `AmazonRedshiftQueryEditor` 和受 `AmazonRedshiftReadOnlyAccess` AWS 管政策。 `AmazonRedshiftQueryEditor` 政策會讓使用者獲得僅擷取自己 SQL 陳述式結果的許可。也就是說，由 `AmazonRedshiftQueryEditor` AWS 受管理策略的這一 `aws:userid` 部分所示提交的陳述式。

```
{
  "Sid": "DataAPIIAMSessionPermissionsRestriction",
  "Action": [
    "redshift-data:GetStatementResult",
    "redshift-data:CancelStatement",
    "redshift-data:DescribeStatement",
    "redshift-data:ListStatements"
  ],
  "Effect": "Allow",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "redshift-data:statement-owner-iam-userid": "${aws:userid}"
    }
  }
}
```

```
}  
}
```

若要允許使用者擷取有相同 IAM 角色之其他人的 SQL 陳述式結果，請建立您自己的政策，但不要有用來限制目前使用者存取權的條件。同時，請限制只有管理員能獲得變更政策的存取權。

要使用查詢編輯器 v2 所需的許可

若要讓使用者使用 Amazon Redshift 查詢編輯器 v2，該使用者必須擁有 Amazon Redshift、查詢編輯器 v2 操作以及其他 AWS 服務 (例如 AWS Key Management Service AWS Secrets Manager、和標記服務) 的最低許可集。

若要讓使用者擁有查詢編輯器 v2 的完整存取權，請附加

受 AmazonRedshiftQueryEditorV2FullAccess AWS 管理的原

則。AmazonRedshiftQueryEditorV2FullAccess 政策會讓使用者獲得與同一團隊中的其他成員共用查詢編輯器 v2 資源 (例如查詢) 的許可。如需查詢編輯器 v2 資源存取權控制方式的詳細資訊，請參閱 IAM 主控台中查詢編輯器 v2 特定受管政策的定義。

某些 Amazon Redshift 查詢編輯器 v2 AWS 受管政策會在條件範圍內使用 AWS 標籤來設定對資源的存取範圍。在查詢編輯器 v2 內，會以附加至主體 (IAM 角色) 的 IAM 政策中的標籤索引鍵和值 "aws:ResourceTag/sqlworkbench-team": "\${aws:PrincipalTag/sqlworkbench-team}" 為基礎來共用查詢。AWS 帳戶 具有相同標籤值 (例如 accounting-team) 的相同主參與者位於查詢編輯器 v2 中的相同專案團隊中。您一次只能與一個團隊相關聯。具有管理許可的使用者可以透過為所有團隊成員提供相同的 sqlworkbench-team 標籤值，以在 IAM 主控台中設定團隊。如果 IAM 使用者或 IAM 角色的 sqlworkbench-team 標籤值發生變更，則可能要等一段時間，共用資源才會反映此變更。如果資源 (例如查詢) 的標籤值發生變更，則一樣可能要等一段時間才會反映此變更。團隊成員還必須擁有 tag:GetResources 許可才能共用。

範例：新增 IAM 角色的 **accounting-team** 標籤

1. 登入 AWS Management Console 並開啟身分與存取權管理主控台，[網址為 https://console.aws.amazon.com/iam/](https://console.aws.amazon.com/iam/)。
2. 在主控台導覽窗格中，選擇 Roles (角色)，然後選擇您要編輯的角色名稱。
3. 選擇標籤索引標籤，然後選擇新增標籤。
4. 新增標籤索引鍵 sqlworkbench-team 和值 accounting-team。
5. 選擇儲存變更。

現在，當 IAM 主體 (附加了此 IAM 角色) 與團隊共用查詢時，具有相同 accounting-team 標籤值的其他主體都可以檢視該查詢。

如需如何將標籤附加到主體 (包括 IAM 角色和 IAM 使用者) 的相關資訊，請參閱《IAM 使用者指南》中的[標記 IAM 資源](#)。

您也可以使用身分提供者 (IdP) 在工作階段層級設定團隊。這可讓使用相同 IAM 角色的多個使用者擁有不同的團隊。IAM 角色的信任政策必須允許 `sts:TagSession` 操作。如需詳細資訊，請參閱《IAM 使用者指南》中的[新增工作階段標籤所需的許可](#)。將主體標籤屬性新增至 IdP 提供的 SAML 聲明。

```
<Attribute Name="https://aws.amazon.com/SAML/Attributes/PrincipalTag:sqlworkbench-team">
  <AttributeValue>accounting-team</AttributeValue>
</Attribute>
```

遵循身分提供者 (IdP) 的指示，將來自目錄的內容填入到 SAML 屬性。如需身分識別供應商 (IdPs) 和 Amazon Redshift 的詳細資訊，請參閱 IAM 使用者指南中的[使用 IAM 身分驗證產生資料庫使用者憑證和身分識別供應商和聯合](#)。

`sqlworkbench>CreateNotebookVersion` 可准許在帳戶上取得筆記本儲存格的目前內容並建立筆記本版本。這意味著，在建立版本時，筆記本的目前內容會與版本的內容相同。之後，當目前的筆記本更新時，版本中的儲存格內容會保持不變。`sqlworkbench:GetNotebookVersion` 可准許取得筆記本的版本。在筆記本上沒有 `sqlworkbench:BatchGetNotebookCell` 許可但有 `sqlworkbench>CreateNotebookVersion` 和 `sqlworkbench:GetNotebookVersion` 許可的使用者可以存取版本中的筆記本儲存格。這位沒有 `sqlworkbench:BatchGetNotebookCell` 許可的使用者仍然可以透過先建立版本，然後取得所建立的這個版本，以擷取筆記本儲存格的內容。

要使用 Amazon Redshift 排程器所需的許可

使用 Amazon Redshift 排程器時，您要設定與 Amazon Redshift 排程器 (**`scheduler.redshift.amazonaws.com`**) 有信任關係的 IAM 角色，讓排程器代您取得許可。您也要將政策 (許可) 附加到您想排程之 Amazon Redshift API 操作的角色。

以下範例示範 JSON 格式的政策文件，以設定與 Amazon Redshift 排程器和 Amazon Redshift 的信任關係。

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



```

                "scheduler.redshift.amazonaws.com",
                "redshift.amazonaws.com"
            ]
        },
        "Action": "sts:AssumeRole"
    }
]
}

```

如需有關信任實體的詳細資訊，請參閱《IAM 使用者指南》中的[建立角色以將許可委派給 AWS 服務](#)。

您也必須新增要排程之 Amazon Redshift 操作的許可。

為使用 `ResizeCluster` 操作的排程器，在您的 IAM 政策中新增類似以下的許可。是否需要加強政策限制，視環境而定。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "redshift:ResizeCluster",
      "Resource": "*"
    }
  ]
}

```

如需為 Amazon Redshift 排程器建立角色的步驟，請參閱 IAM 使用者指南中的[建立 AWS 服務角色 \(主控台\)](#)。在 IAM 主控台中建立角色時，選擇以下項目：

- 針對 Choose the service that will use this role (選擇將使用此角色的服務)：選擇 Redshift。
- 針對 Select your use case (選取您的使用案例)：選擇 Redshift - Scheduler (Redshift - 排程器)。
- 建立政策，或將政策附加到允許排程 Amazon Redshift 操作的角色。選擇 Create policy (建立政策) 或修改角色以連接政策。輸入要排程之操作的 JSON 政策。
- 建立角色之後，編輯 IAM 角色的 Trust Relationship (信任關係) 以納入服務 `redshift.amazonaws.com`。

您建立的 IAM 角色有信任的 `scheduler.redshift.amazonaws.com` 和 `redshift.amazonaws.com` 實體。且附加了允許受支援 Amazon Redshift API 動作的政策，例如 `"redshift:ResizeCluster"`。

使用 Amazon EventBridge 排程器所需的許可

使用 Amazon EventBridge 排程器時，您可以設定與排程器 (**events.amazonaws.com**) 具有信任關係的 EventBridge IAM 角色，以允許排程器代表您執行許可。您也可以將政策 (許可) 附加到要排程之 Amazon Redshift 資料 API 操作的角色，以及 Amazon EventBridge 操作的政策。

使用主控台上的 Amazon Redshift 查詢編輯器建立 EventBridge 排程查詢時，可以使用排程器。

您可以建立 IAM 角色，以便在 IAM 主控台上執行已排程的查詢。在此 IAM 角色中，請附加 AmazonEventBridgeFullAccess 和 AmazonRedshiftDataFullAccess。

下列範例顯示 JSON 格式的原則文件，以設定與 EventBridge 排程器之間的信任關係。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "events.amazonaws.com",
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

如需有關信任實體的詳細資訊，請參閱《IAM 使用者指南》中的[建立角色以將許可委派給 AWS 服務](#)。

如需為 EventBridge 排程器建立角色的步驟，請參閱 IAM 使用者指南中的[建立 AWS 服務角色 \(主控台\)](#)。在 IAM 主控台中建立角色時，選擇以下項目：

- 對於 [選擇將使用此角色的服務]：選擇 [CloudWatch 事件]。
- 對於選取您的使用案例：選擇 CloudWatch 事件。
- 附加以下許可政策：AmazonEventBridgeFullAccess 和 AmazonRedshiftDataFullAccess。

您建立的 IAM 角色有信任的 **events.amazonaws.com** 實體。且附加了允許受支援 Amazon Redshift 資料 API 動作的政策，例如 "redshift-data:*"。

要使用 Amazon Redshift 機器學習 (ML) 所需的許可

接下來，您可以找到要針對不同使用案例使用 Amazon Redshift 機器學習 (ML) 所需之許可的描述。

若要讓您的使用者將 Amazon Redshift ML 與 Amazon 搭配使用 SageMaker，請使用比預設政策更嚴格的政策來建立 IAM 角色。您可以使用下列政策。您也可以修改此政策以因應您的需求。

下列政策顯示使用 Amazon Redshift 提供的模型說明功能執行 SageMaker 自動輔助駕駛所需的許可。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateAutoMLJob",
        "sagemaker:CreateCompilationJob",
        "sagemaker:CreateEndpoint",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeCompilationJob",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeTransformJob",
        "sagemaker:ListCandidatesForAutoMLJob",
        "sagemaker:StopAutoMLJob",
        "sagemaker:StopCompilationJob",
        "sagemaker:StopTrainingJob",
        "sagemaker:DescribeEndpoint",
        "sagemaker:InvokeEndpoint",
        "sagemaker:StopProcessingJob",
        "sagemaker:CreateModel",
        "sagemaker:CreateProcessingJob"
      ],
      "Resource": [
        "arn:aws:sagemaker:*:*:model/*redshift*",
        "arn:aws:sagemaker:*:*:training-job/*redshift*",
        "arn:aws:sagemaker:*:*:automl-job/*redshift*",
        "arn:aws:sagemaker:*:*:compilation-job/*redshift*",
        "arn:aws:sagemaker:*:*:processing-job/*redshift*",
        "arn:aws:sagemaker:*:*:transform-job/*redshift*",
        "arn:aws:sagemaker:*:*:endpoint/*redshift*"
      ]
    }
  ],
}
```

```
{
  "Effect": "Allow",
  "Action": [
    "logs:CreateLogGroup",
    "logs:CreateLogStream",
    "logs:DescribeLogStreams",
    "logs:PutLogEvents"
  ],
  "Resource": [
    "arn:aws:logs:*:*:log-group:/aws/sagemaker/Endpoints/*redshift*",
    "arn:aws:logs:*:*:log-group:/aws/sagemaker/ProcessingJobs/*redshift*",
    "arn:aws:logs:*:*:log-group:/aws/sagemaker/TrainingJobs/*redshift*",
    "arn:aws:logs:*:*:log-group:/aws/sagemaker/TransformJobs/*redshift*"
  ]
},
{
  "Effect": "Allow",
  "Action": [
    "cloudwatch:PutMetricData"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "cloudwatch:namespace": [
        "SageMaker",
        "/aws/sagemaker/Endpoints",
        "/aws/sagemaker/ProcessingJobs",
        "/aws/sagemaker/TrainingJobs",
        "/aws/sagemaker/TransformJobs"
      ]
    }
  }
},
{
  "Effect": "Allow",
  "Action": [
    "ecr:BatchCheckLayerAvailability",
    "ecr:BatchGetImage",
    "ecr:GetAuthorizationToken",
    "ecr:GetDownloadUrlForLayer"
  ],
  "Resource": "*"
},
{
```

```

    "Effect": "Allow",
    "Action": [
        "s3:GetObject",
        "s3:GetBucketAcl",
        "s3:GetBucketCors",
        "s3:GetEncryptionConfiguration",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:ListMultipartUploadParts",
        "s3:ListBucketMultipartUploads",
        "s3:PutObject",
        "s3:PutBucketAcl",
        "s3:PutBucketCors",
        "s3>DeleteObject",
        "s3:AbortMultipartUpload",
        "s3:CreateBucket"
    ],
    "Resource": [
        "arn:aws:s3:::redshift-downloads",
        "arn:aws:s3:::redshift-downloads/*",
        "arn:aws:s3::*:redshift*",
        "arn:aws:s3::*:redshift/*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "s3:GetObject",
        "s3:GetBucketAcl",
        "s3:GetBucketCors",
        "s3:GetEncryptionConfiguration",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:ListMultipartUploadParts",
        "s3:ListBucketMultipartUploads",
        "s3:PutObject",
        "s3:PutBucketAcl",
        "s3:PutBucketCors",
        "s3>DeleteObject",
        "s3:AbortMultipartUpload",
        "s3:CreateBucket"
    ],

```

```

    "Resource": "*",
    "Condition": {
      "StringEqualsIgnoreCase": {
        "s3:ExistingObjectTag/Redshift": "true"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "iam:PassRole"
    ],
    "Resource": "arn:aws:iam::*:role/*",
    "Condition": {
      "StringEquals": {
        "iam:PassedToService": [
          "redshift.amazonaws.com",
          "sagemaker.amazonaws.com"
        ]
      }
    }
  }
]
}

```

下列政策顯示可允許存取 Amazon DynamoDB、Redshift Spectrum 和 Amazon RDS 聯合的完整最基本許可。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateAutoMLJob",
        "sagemaker:CreateCompilationJob",
        "sagemaker:CreateEndpoint",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeCompilationJob",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeTransformJob",

```

```

        "sagemaker:ListCandidatesForAutoMLJob",
        "sagemaker:StopAutoMLJob",
        "sagemaker:StopCompilationJob",
        "sagemaker:StopTrainingJob",
        "sagemaker:DescribeEndpoint",
        "sagemaker:InvokeEndpoint",
        "sagemaker:StopProcessingJob",
        "sagemaker:CreateModel",
        "sagemaker:CreateProcessingJob"
    ],
    "Resource": [
        "arn:aws:sagemaker:*:*:model/*redshift*",
        "arn:aws:sagemaker:*:*:training-job/*redshift*",
        "arn:aws:sagemaker:*:*:automl-job/*redshift*",
        "arn:aws:sagemaker:*:*:compilation-job/*redshift*",
        "arn:aws:sagemaker:*:*:processing-job/*redshift*",
        "arn:aws:sagemaker:*:*:transform-job/*redshift*",
        "arn:aws:sagemaker:*:*:endpoint/*redshift*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
    ],
    "Resource": [
        "arn:aws:logs:*:*:log-group:/aws/sagemaker/Endpoints/*redshift*",
        "arn:aws:logs:*:*:log-group:/aws/sagemaker/ProcessingJobs/*redshift*",
        "arn:aws:logs:*:*:log-group:/aws/sagemaker/TrainingJobs/*redshift*",
        "arn:aws:logs:*:*:log-group:/aws/sagemaker/TransformJobs/*redshift*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "cloudwatch:PutMetricData"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "cloudwatch:namespace": [

```

```

        "SageMaker",
        "/aws/sagemaker/Endpoints",
        "/aws/sagemaker/ProcessingJobs",
        "/aws/sagemaker/TrainingJobs",
        "/aws/sagemaker/TransformJobs"
    ]
}
},
{
    "Effect": "Allow",
    "Action": [
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": [
        "s3:GetObject",
        "s3:GetBucketAcl",
        "s3:GetBucketCors",
        "s3:GetEncryptionConfiguration",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:ListMultipartUploadParts",
        "s3:ListBucketMultipartUploads",
        "s3:PutObject",
        "s3:PutBucketAcl",
        "s3:PutBucketCors",
        "s3>DeleteObject",
        "s3:AbortMultipartUpload",
        "s3>CreateBucket"
    ],
    "Resource": [
        "arn:aws:s3:::redshift-downloads",
        "arn:aws:s3:::redshift-downloads/*",
        "arn:aws:s3:::*redshift*",
        "arn:aws:s3:::*redshift/*"
    ]
}
]

```



```

    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetBucketAcl",
        "s3:GetBucketCors",
        "s3:GetEncryptionConfiguration",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:ListMultipartUploadParts",
        "s3:ListBucketMultipartUploads",
        "s3:PutObject",
        "s3:PutBucketAcl",
        "s3:PutBucketCors",
        "s3>DeleteObject",
        "s3:AbortMultipartUpload",
        "s3:CreateBucket"
      ],
      "Resource": "*",
      "Condition": {
        "StringEqualsIgnoreCase": {
          "s3:ExistingObjectTag/Redshift": "true"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "dynamodb:Scan",
        "dynamodb:DescribeTable",
        "dynamodb:Getitem"
      ],
      "Resource": [
        "arn:aws:dynamodb:*:*:table/*redshift*",
        "arn:aws:dynamodb:*:*:table/*redshift*/index/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "elasticmapreduce:ListInstances"
      ],

```

```
    "Resource": [
      "arn:aws:elasticmapreduce:*:*:cluster/*redshift*"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "elasticmapreduce:ListInstances"
    ],
    "Resource": "*",
    "Condition": {
      "StringEqualsIgnoreCase": {
        "elasticmapreduce:ResourceTag/Redshift": "true"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "lambda:InvokeFunction"
    ],
    "Resource": "arn:aws:lambda:*:*:function:*redshift*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "glue:CreateDatabase",
      "glue>DeleteDatabase",
      "glue:GetDatabase",
      "glue:GetDatabases",
      "glue:UpdateDatabase",
      "glue:CreateTable",
      "glue>DeleteTable",
      "glue:BatchDeleteTable",
      "glue:UpdateTable",
      "glue:GetTable",
      "glue:GetTables",
      "glue:BatchCreatePartition",
      "glue:CreatePartition",
      "glue>DeletePartition",
      "glue:BatchDeletePartition",
      "glue:UpdatePartition",
      "glue:GetPartition",
      "glue:GetPartitions",
    ]
  }
}
```

```

        "glue:BatchGetPartition"
    ],
    "Resource": [
        "arn:aws:glue:*:*:table/*redshift*/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*redshift*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecretVersionIds"
    ],
    "Resource": [
        "arn:aws:secretsmanager:*:*:secret:*redshift*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "secretsmanager:GetRandomPassword",
        "secretsmanager:ListSecrets"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "secretsmanager:ResourceTag/Redshift": "true"
        }
    }
},
{
    "Effect": "Allow",
    "Action": [
        "iam:PassRole"
    ],
    "Resource": "arn:aws:iam:*:*:role/*",
    "Condition": {
        "StringEquals": {
            "iam:PassedToService": [
                "redshift.amazonaws.com",
                "glue.amazonaws.com",
            ]
        }
    }
}

```



```
}

```

在上文中，Amazon S3 儲存貯體 `redshift-downloads/redshift-ml/` 是用於其他步驟和範例之範例資料的儲存所在位置。如果您不需要從 Amazon S3 載入資料，則可以移除此儲存貯體。或者，也可以將其取代為您用來將資料載入 Amazon Redshift 的其他 Amazon S3 儲存貯體。

your-account-id、**your-role** 和 **your-s3-bucket** 值是您在 CREATE MODEL 命令中所指定的帳戶 ID、角色和儲存貯體。

或者，如果您指定 AWS KMS 要與 Amazon Redshift ML 搭配使用的 AWS KMS 金鑰，您也可以使用範例政策的金鑰區段。**your-kms-key** 值是您用來作為 CREATE MODEL 命令一部分的金鑰。

當您為 hyperparameter 調校任務指定私有虛擬私有雲端 (VPC) 時，請新增下列許可。

```
{
    "Effect": "Allow",
    "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2>DeleteNetworkInterface",
        "ec2>DeleteNetworkInterfacePermission",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
    ]
}
```

若要使用模型說明，請確定您具有呼叫 SageMaker API 作業的權限。建議您使用 `AmazonSageMakerFullAccess` 受管政策。如果您想要建立具有更嚴格政策的 IAM 角色，請使用以下政策。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "sagemaker::CreateEndpoint",
        "sagemaker::CreateEndpointConfig",
        "sagemaker::DeleteEndpoint",

```

```

    "sagemaker::DeleteEndpointConfig",
    "sagemaker::DescribeEndpoint",
    "sagemaker::DescribeEndpointConfig",
    "sagemaker::DescribeModel",
    "sagemaker::InvokeEndpoint",
    "sagemaker::ListTags"
  ],
  "Resource": "*"
}
]
}

```

如需有關AmazonSageMakerFullAccess受管政策的詳細資訊，請參閱[AmazonSageMakerFullAccess](#) Amazon SageMaker 開發人員指南中的存取。

如果您想要建立 Forecast 模型，建議您使用 AmazonForecastFullAccess 受管政策。如果您想要使用更嚴格的政策，請新增以下政策至 IAM 角色。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "forecast:CreateAutoPredictor",
        "forecast:CreateDataset",
        "forecast:CreateDatasetGroup",
        "forecast:CreateDatasetImportJob",
        "forecast:CreateForecast",
        "forecast:CreateForecastExportJob",
        "forecast>DeleteResourceTree",
        "forecast:DescribeAutoPredictor",
        "forecast:DescribeDataset",
        "forecast:DescribeDatasetGroup",
        "forecast:DescribeDatasetImportJob",
        "forecast:DescribeForecast",
        "forecast:DescribeForecastExportJob",
        "forecast:StopResource",
        "forecast:TagResource",
        "forecast:UpdateDatasetGroup"
      ],
      "Resource": "*"
    }
  ]
}

```

```
]
}
```

如需 Amazon Redshift ML 的相關資訊，請參閱[在 Amazon Redshift 中使用機器學習](#)或 [CREATE MODEL](#)。

串流擷取的許可

串流擷取可與兩個服務搭配運作。這兩個服務是 Kinesis Data Streams 和 Amazon MSK。

要搭配 Kinesis Data Streams 使用串流擷取所需的許可

您可以在[開始從 Amazon Kinesis Data Streams 擷取串流](#)中找到包含受管政策範例的程序。

要搭配 Amazon MSK 使用串流擷取所需的許可

您可以在[開始從 Amazon Managed Streaming for Apache Kafka 擷取串流](#)中找到包含受管政策範例的程序。

要使用資料共用 API 操作所需的許可

若要控制資料共用 API 操作的存取權，請使用 IAM 動作型政策。如需有關如何管理 IAM 政策的資訊，請參閱《IAM 使用者指南》中的[管理 IAM 政策](#)。

具體而言，假設生產者叢集管理員需要使用 `AuthorizeDataShare` 呼叫來為 AWS 帳戶外部的資料共用授權輸出。在此情況下，您需要設定 IAM 動作型政策以授予此許可。使用 `DeauthorizeDataShare` 呼叫以撤銷輸出。

使用 IAM 動作型政策時，您也可以指定 IAM 資源，例如 `DataShareARN`。以下內容會顯示 `DataShareARN` 的格式和範例。

```
arn:aws:redshift:region:account-id:datashare:namespace-guid/datashare-name
arn:aws:redshift:us-east-1:555555555555:datashare:86b5169f-01dc-4a6f-9fbb-e2e24359e9a8/
SalesShare
```

您可以在 IAM 政策中指定資料共用名稱，以限制特定資料共用的 `AuthorizeDataShare` 存取權。

```
{
  "Statement": [
    {
      "Action": [
        "redshift:AuthorizeDataShare",
```

```

    ],
    "Resource": [
      "arn:aws:redshift:us-east-1:555555555555:datashare:86b5169f-01dc-4a6f-9fbb-
e2e24359e9a8/SalesShare"
    ],
    "Effect": "Deny"
  }
]
}

```

您也可以將 IAM 政策的範圍限制在特定生產者叢集擁有的所有資料共用。若要這麼做，請使用萬用字元或星號來取代政策中的 **datashare-name** 值。保留叢集的 namespace-guid 值。

```
arn:aws:redshift:us-east-1:555555555555:datashare:86b5169f-01dc-4a6f-9fbb-e2e24359e9a8/
*
```

以下是可防止實體呼叫特定生產者叢集所擁有資料共用上 AuthorizeDataShare 的 IAM 政策。

```

{
  "Statement": [
    {
      "Action": [
        "redshift:AuthorizeDataShare",
      ],
      "Resource": [
        "arn:aws:redshift:us-east-1:555555555555:datashare:86b5169f-01dc-4a6f-9fbb-
e2e24359e9a8/*"
      ],
      "Effect": "Deny"
    }
  ]
}

```

DataShareARN 會根據資料共用名稱和擁有端叢集命名空間的全域唯一 ID (GUID) 來限制存取權。其會透過將名稱指定為星號來進行此操作。

的資源策略 GetClusterCredentials

若要以 IAM 資料庫登入資料使用 JDBC 或 ODBC 連線來連線至叢集資料庫，或是以程式設計方式呼叫 GetClusterCredentials 動作，您需要基本的一組許可。您至少需要呼叫 redshift:GetClusterCredentials 動作的許可，該動作具有 dbuser 資源的存取權。

如果您使用 JDBC 或 ODBC 連線，而不是 server 和 port，您可以指定 `cluster_id` 和 `region`，但要這麼做，您的政策必須允許具有 `redshift:DescribeClusters` 資源存取的 `cluster` 動作。

如果您使用選用參數 `Autocreate`、`DbGroups` 和 `DbName` 來呼叫 `GetClusterCredentials`，請務必也允許動作並允許下表所列資源的存取權。

GetClusterCredentials 參數	動作	資源
Autocreate	redshift:dbuser CreateClusterUser	
DbGroups	redshift:dbgroup JoinGroup	
DbName	NA	dbname

如需資源的相關資訊，請參閱 [Amazon Redshift 資源和操作](#)。

您也可以在政策包含下列條件：

- `redshift:DurationSeconds`
- `redshift:DbName`
- `redshift:DbUser`

如需條件的相關資訊，請參閱 [在政策中指定條件](#)。

客戶受管政策範例

在本節中，您可以找到授予各種 Amazon Redshift 動作之許可的使用者政策範例。當您使用 Amazon Redshift API、AWS 開發套件或 AWS CLI

Note

所有範例皆使用美國西部 (奧勒岡) 區域 (`us-west-2`) 及虛構帳戶 ID。

範例 1：允許使用者對所有 Amazon Redshift 動作和資源的完整存取權

下列政策允許存取處理所有資源的所有 Amazon Redshift 動作。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowRedshift",
      "Action": [
        "redshift:*"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Action 元素中的值 redshift:* 指出 Amazon Redshift 中的所有動作。

範例 2：拒絕使用者存取一組 Amazon Redshift 動作

預設會拒絕所有的許可。不過，有時您必須明確拒絕對特定動作或動作集的存取權。下列政策允許對所有 Amazon Redshift 動作的存取權，並明確拒絕對名稱開頭為 Delete 之任何 Amazon Redshift 動作的存取權。此政策適用於 us-west-2 中的所有 Amazon Redshift 資源。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowUSWest2Region",
      "Action": [
        "redshift:*"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:redshift:us-west-2:*"
    },
    {
      "Sid": "DenyDeleteUSWest2Region",
      "Action": [
        "redshift:Delete*"
      ],

```

```
    "Effect": "Deny",
    "Resource": "arn:aws:redshift:us-west-2:*"
  }
]
}
```

範例 3：允許使用者管理叢集

下列政策允許使用者建立、刪除、修改所有叢集和將它們重新開機，然後拒絕刪除叢集名稱開頭為 `protected` 之任何叢集的許可。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowClusterManagement",
      "Action": [
        "redshift:CreateCluster",
        "redshift>DeleteCluster",
        "redshift:ModifyCluster",
        "redshift:RebootCluster"
      ],
      "Resource": [
        "*"
      ],
      "Effect": "Allow"
    },
    {
      "Sid": "DenyDeleteProtected",
      "Action": [
        "redshift>DeleteCluster"
      ],
      "Resource": [
        "arn:aws:redshift:us-west-2:123456789012:cluster:protected*"
      ],
      "Effect": "Deny"
    }
  ]
}
```

範例 4：允許使用者授權和撤銷快照存取

下列政策允許使用者 (例如使用者 A) 來執行下列動作：

- 授予對透過名為 shared 之叢集建立的任何快照的存取權。
- 撤銷對透過 shared 叢集建立、快照名稱開頭為 revokable 之任何快照的快照存取權。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSharedSnapshots",
      "Action": [
        "redshift:AuthorizeSnapshotAccess"
      ],
      "Resource": [
        "arn:aws:redshift:us-west-2:123456789012:shared/*"
      ],
      "Effect": "Allow"
    },
    {
      "Sid": "AllowRevokableSnapshot",
      "Action": [
        "redshift:RevokeSnapshotAccess"
      ],
      "Resource": [
        "arn:aws:redshift:us-west-2:123456789012:snapshot:*/revokable*"
      ],
      "Effect": "Allow"
    }
  ]
}
```

如果使用者 A 已允許使用者 B 存取快照，使用者 B 必須具備以下這類的政策以允許使用者 B 從快照還原叢集。下列政策允許使用者 B 從快照描述和還原，以及建立叢集。這些叢集名稱的開頭必須是 from-other-account。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowDescribeSnapshots",
      "Action": [
        "redshift:DescribeClusterSnapshots"
      ],

```

```

    "Resource": [
      "*"
    ],
    "Effect": "Allow"
  },
  {
    "Sid": "AllowUserRestoreFromSnapshot",
    "Action": [
      "redshift:RestoreFromClusterSnapshot"
    ],
    "Resource": [
      "arn:aws:redshift:us-west-2:123456789012:snapshot:*/**",
      "arn:aws:redshift:us-west-2:444455556666:cluster:from-other-account*"
    ],
    "Effect": "Allow"
  }
]
}

```

範例 5：允許使用者複製叢集快照和從快照還原叢集

下列政策允許使用者複製透過名為 `big-cluster-1` 之叢集建立的任何快照，以及還原快照名稱開頭為 `snapshot-for-restore` 的任何快照。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowCopyClusterSnapshot",
      "Action": [
        "redshift:CopyClusterSnapshot"
      ],
      "Resource": [
        "arn:aws:redshift:us-west-2:123456789012:snapshot:big-cluster-1/*"
      ],
      "Effect": "Allow"
    },
    {
      "Sid": "AllowRestoreFromClusterSnapshot",
      "Action": [
        "redshift:RestoreFromClusterSnapshot"
      ],
      "Resource": [

```

```

        "arn:aws:redshift:us-west-2:123456789012:snapshot:*/snapshot-for-restore*",
        "arn:aws:redshift:us-west-2:123456789012:cluster:*"
    ],
    "Effect": "Allow"
}
]
}

```

範例 6：允許使用者存取 Amazon Redshift，和相關 AWS 服務的一般動作和資源

下列範例政策允許存取 Amazon Redshift、亞馬遜簡單通知服務 (Amazon SNS) 和亞馬遜的所有動作和資源。CloudWatch 它也會允許在該帳戶下於所有相關 Amazon EC2 資源上的指定動作。

Note

此範例政策中指定的 Amazon EC2 動作不支援資源層級許可。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowRedshift",
      "Effect": "Allow",
      "Action": [
        "redshift:*"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "AllowSNS",
      "Effect": "Allow",
      "Action": [
        "sns:*"
      ],
      "Resource": [
        "*"
      ]
    }
  ],
  {

```

```

    "Sid": "AllowCloudWatch",
    "Effect": "Allow",
    "Action": [
      "cloudwatch:*"
    ],
    "Resource": [
      "*"
    ]
  },
  {
    "Sid": "AllowEC2Actions",
    "Effect": "Allow",
    "Action": [
      "ec2:AllocateAddress",
      "ec2:AssociateAddress",
      "ec2:AttachNetworkInterface",
      "ec2:DescribeAccountAttributes",
      "ec2:DescribeAddresses",
      "ec2:DescribeAvailabilityZones",
      "ec2:DescribeInternetGateways",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeSubnets",
      "ec2:DescribeVpcs"
    ],
    "Resource": [
      "*"
    ]
  }
]
}

```

範例 7：允許使用者使用 Amazon Redshift 主控台標記資源

以下範例政策可讓使用者使用 AWS Resource Groups 透過 Amazon Redshift 主控台標記資源。此政策可附加至會叫用新的或原始 Amazon Redshift 主控台的使用者角色。如需標記的相關資訊，請參閱 [在 Amazon Redshift 中標記資源](#)。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Tagging permissions",
      "Effect": "Allow",

```

```

    "Action": [
      "redshift:DeleteTags",
      "redshift:CreateTags",
      "redshift:DescribeTags",
      "tag:UntagResources",
      "tag:TagResources"
    ],
    "Resource": "*"
  }
]
}

```

使用政策範例 GetClusterCredentials

以下範例政策使用這些範例參數值：

- 區域: us-west-2
- AWS 帳號 : 123456789012
- 叢集名稱: examplecluster

以下策略启用 GetCredentials、CreateClusterUser 和 JoinGroup 操作。此原則會使用條件金鑰，僅在使用 AWS 者識別碼相符時允許GetClusterCredentials和CreateClusterUser動作"AIDIODR4TAW7CSEXAMPLE:\${redshift:DbUser}@yourdomain.com"。僅會對 "testdb" 資料庫請求 IAM 存取權。此政策也允許使用者加入名為 "common_group" 的群組。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "GetClusterCredsStatement",
      "Effect": "Allow",
      "Action": [
        "redshift:GetClusterCredentials"
      ],
      "Resource": [
        "arn:aws:redshift:us-west-2:123456789012:dbuser:examplecluster/
        ${redshift:DbUser}",
        "arn:aws:redshift:us-west-2:123456789012:dbname:examplecluster/testdb",
        "arn:aws:redshift:us-west-2:123456789012:dbgroup:examplecluster/common_group"
      ],
      "Condition": {

```



```
        "StringEquals": {
          "aws:userid": "AIDIODR4TAW7CSEXAMPLE:${redshift:DbUser}@yourdomain.com"
        }
      },
    {
      "Sid": "CreateClusterUserStatement",
      "Effect": "Allow",
      "Action": [
        "redshift:CreateClusterUser"
      ],
      "Resource": [
        "arn:aws:redshift:us-west-2:123456789012:dbuser:examplecluster/
${redshift:DbUser}"
      ],
      "Condition": {
        "StringEquals": {
          "aws:userid": "AIDIODR4TAW7CSEXAMPLE:${redshift:DbUser}@yourdomain.com"
        }
      }
    },
    {
      "Sid": "RedshiftJoinGroupStatement",
      "Effect": "Allow",
      "Action": [
        "redshift:JoinGroup"
      ],
      "Resource": [
        "arn:aws:redshift:us-west-2:123456789012:dbgroup:examplecluster/common_group"
      ]
    }
  ]
}
```

Amazon Redshift 的原生身分提供者 (IdP) 聯合

使用原生身分提供者聯合可以更輕鬆地管理 Amazon Redshift 的身分和許可，因為它可以運用您現有的身分提供者來簡化身分驗證和管理許可。它會透過將身分中繼資料從您的身分提供者共用至 Redshift 來達成此目的。對於此功能的第一個迭代，支援的身分提供者是 [Microsoft Azure Active Directory \(Azure AD\)](#)。

若要設定 Amazon Redshift 以便能夠從第三方身分提供者進行身分驗證，請向 Amazon Redshift 註冊身分提供者。這樣做可讓 Redshift 驗證身分提供者所定義的使用者和角色。因此，您就不必在第三方身分提供者和 Amazon Redshift 中執行精細的身分管理，因為身分資訊會共用。

如需有關使用從身分提供者 (IdP) 群組傳輸而來之工作階段角色的資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的 [PG_GET_SESSION_ROLES](#)。

在 Amazon Redshift 上設定身分提供者

本節說明用來設定身分提供者和 Amazon Redshift 以便為原生身分提供者聯合建立通訊的步驟。您需要身分提供者的作用中帳戶。在設定 Amazon Redshift 之前，您必須向身分提供者將 Redshift 註冊為應用程式，並授予管理員同意。

在 Amazon Redshift 中完成以下步驟：

1. 執行 SQL 陳述式以註冊識別提供者，包括 Azure 應用程式中繼資料的描述。若要在 Amazon Redshift 中建立身分提供者，請在取代 issuer、client_id、client_secret 和 audience 參數值後執行下列命令。這些參數是 Microsoft Azure AD 的特有參數。請將身分提供者名稱取代為您選擇的名稱，並以唯一名稱取代命名空間，以包含您身分提供者目錄中的使用者和角色。

```
CREATE IDENTITY PROVIDER oauth_standard TYPE azure
NAMESPACE 'aad'
PARAMETERS '{
  "issuer": "https://sts.windows.net/2sdfdsf-d475-420d-b5ac-667adad7c702/",
  "client_id": "<client_id>",
  "client_secret": "BUAH~ewrqewrqwerUUY^%tHe1oNZShoiU7",
  "audience": ["https://analysis.windows.net/powerbi/connector/AmazonRedshift"]
}'
```

azure 類型表示提供者具體來說有利於與 Microsoft Azure AD 進行通訊。這是目前唯一支援的第三方身分提供者。

- issuer — 收到字符時要信任的發行者 ID。發行者會附加 tenant_id 的唯一識別碼。
- client_id — 向身分提供者註冊之應用程式的唯一公共識別碼。這可以稱為應用程式 ID。
- client_secret — 只有身分提供者和已註冊的應用程式才知道的機密識別碼或密碼。
- audience — 指派給 Azure 中應用程式的應用程式 ID。

您可以在建立身分提供者時設定參數以指定憑證、私有金鑰和私有金鑰密碼，而不是使用共用用戶端機密。

```
CREATE IDENTITY PROVIDER example_idp TYPE azure
NAMESPACE 'example_aad'
PARAMETERS '{"issuer":"https://sts.windows.net/2sdfdsf-d475-420d-
b5ac-667adad7c702/",
"client_id":"<client_id>",
"audience":["https://analysis.windows.net/powerbi/connector/AmazonRedshift"],
"client_x5t":"<certificate thumbprint>",
"client_pk_base64":"<private key in base64 encoding>",
"client_pk_password":"test_password"}';
```

私有金鑰密碼 `client_pk_password` 是選擇性的。

2. 選擇性：在 Amazon Redshift 中執行 SQL 命令以預先建立使用者和角色。這有助於事先授予許可。在 Amazon Redshift 中的角色名稱如下所示：`< GroupName 在 Azure AD <Namespace>>`。例如，當您在 Microsoft Azure AD 中建立名為 `rsgroup` 的群組和名為 `aad` 的命名空間時，角色名稱會是 `aad:rsgroup`。Amazon Redshift 中的使用者和角色名稱，這些名稱是根據身分提供者命名空間中的這些使用者和群組成員資格定義的。

角色和使用者的映射包括驗證其 `external_id` 值，以確保它是最新的。外部 ID 會映射至身分提供者中群組或使用者的識別碼。例如，角色的外部 ID 會映射至對應的 Azure AD 群組 ID。同樣地，每個使用者的外部 ID 會映射至身分提供者中的 ID。

```
create role "aad:rsgroup";
```

3. 根據您的要求向角色授予相關許可。例如：

```
GRANT SELECT on all tables in schema public to role "aad:rsgroup";
```

4. 您也可以向特定使用者授予許可。

```
GRANT SELECT on table foo to aad:alice@example.com
```

請注意，聯合的外部使用者的角色成員資格只能在該使用者在工作階段中使用。這會對建立資料庫物件造成影響。例如，當聯合的外部使用者建立任何檢視或預存程序時，同一使用者便無法將這些物件的許可委派給其他使用者和角色。

命名空間的解釋

命名空間會將使用者或角色映射至特定身分提供者。例如，在 AWS IAM 中建立的使用者前置詞為 iam:。此前置詞可防止使用者名稱發生衝突，並可實現對於多個身分存放區的支援。如果使用 aad 命名空間註冊之身分來源的使用者 alice@example.com 登入，則系統會在 Redshift 中建立使用者 aad:alice@example.com (如果該使用者尚未存在)。請注意，使用者和角色命名空間的功能與 Amazon Redshift 叢集命名空間 (這是與叢集相關聯的唯一識別碼) 的功能不同。

使用原生身分提供者 (IdP) 聯合時的登入運作方式

若要完成身分提供者和 Amazon Redshift 之間的初步設定，請執行幾個步驟：首先，向身分提供者將 Amazon Redshift 註冊為第三方應用程式，以請求必要的 API 許可。然後，在身分提供者中建立使用者和群組。最後，使用會設定身分提供者專屬身分驗證參數的 SQL 陳述式向 Amazon Redshift 註冊身分提供者。在向 Redshift 註冊身分提供者時，指派命名空間以確保使用者和角色會正確分組。

透過向 Amazon Redshift 註冊的身分提供者，可以在 Redshift 與身分提供者之間設定通訊。然後，用戶端可以傳遞字符並以身分提供者實體的身分向 Redshift 進行驗證。Amazon Redshift 會使用 IdP 群組成員資格資訊以映射至 Redshift 角色。如果使用者先前不存在於 Redshift 中，系統會建立該使用者。系統會建立映射至身分提供者群組的角色 (如果它們不存在)。Amazon Redshift 管理員在角色上授予許可，使用者可以執行查詢和執行其他資料庫任務。

下列步驟概述使用者登入時，原生身分提供者聯合的運作方式：

1. 當使用者從用戶端使用原生 IdP 選項登入時，身分提供者字符會從用戶端傳送至驅動程式。
2. 使用者會進行身分驗證。如果該使用者還未存在於 Amazon Redshift 中，系統便會建立新使用者。Redshift 會將使用者的身分提供者群組映射至 Redshift 角色。
3. 系統會根據使用者的 Redshift 角色指派許可。這些許可會由管理員授予給使用者和角色。
4. 使用者可以查詢 Redshift。

使用桌面用戶端工具連線到 Amazon Redshift

如需如何使用原生身分提供者聯合透過 Power BI 連線到 Amazon Redshift 的指示，請參閱部落格文章 [整合 Amazon Redshift 原生 IdP 聯合與 Microsoft Azure Active Directory \(AD\) 和 Power BI](#)。它描述了使用 Azure AD 的 Amazon Redshift 原生 IdP 安裝程序的 step-by-step 實現。其內容會詳細說明用來為 Power BI 桌面版或 Power BI 服務設定用戶端連線的步驟。這些步驟包括註冊應用程式、設定許可和設定憑證。

若要了解如何使用 Power BI 桌面版和 JDBC 用戶端 SQL Workbench/J 來整合 Amazon Redshift 原生 IdP 聯合，請觀看以下影片：

如需如何使用原生身分提供者聯合透過 SQL 用戶端 (具體來說是 DBeaver 或 SQL Workbench/J) 連線至 Amazon Redshift 的指示，請參閱部落格文章[使用 SQL 用戶端將 Amazon Redshift 原生 IdP 聯合與 Microsoft Azure AD 進行整合](#)。

將 Redshift 與 IAM Identity Center 連線，為使用者提供單一登入體驗

您可以透過信任身分傳播來管理使用者和群組對 Amazon Redshift 資料倉儲的存取。這可透過 Redshift 和 AWS IAM 身分中心之間的連線運作，讓您的使用者享有單一登入體驗。這樣您就可以從目錄導入使用者和群組，並直接將權限指派給他們。隨後此連線會支援繫結其他工具和服務。為了說明一個 end-to-end 案例，您可以使用 Amazon QuickSight 儀表板或 Amazon Redshift 查詢編輯器 v2 來存取 Redshift。在此情況下，存取權限是以 IAM Identity Center 群組為基礎。Redshift 可以判斷使用者的身分及其群組成員資格。IAM 身分中心也可讓您透過第三方身分提供者 (IdP) (例如 Okta 或) 來連接和管理身分識別。PingOne

管理員設定 Redshift 和 IAM Identity Center 之間的連線後，他們可以根據身分提供者群組設定精細的存取權限，以授予資料存取權給使用者。

Redshift 與 AWS IAM 身分中心整合的好處

搭配 Redshift 使用 IAM Identity Center 可使您的組織透過下列方式受益：

- 中的儀表板作者 Amazon QuickSight 可以連線到 Redshift 資料來源，無需重新輸入密碼或要求管理員設定具有複雜許可的 IAM 角色。
- IAM Identity Center 為您的員工使用者在 AWS 提供中央位置。您可以直接在 IAM 身分中心建立使用者和群組，PingOne 或連接您在標準型身分識別提供者 (例如 Okta 或 Microsoft Entra ID (Azure AD) 中管理的現有使用者和群組。IAM Identity Center 會將身分驗證導向您選擇的使用者和群組的事實來源，並維護使用者和群組的目錄以供 Redshift 存取。如需詳細資訊，請參閱 AWS IAM Identity Center 使用者指南中的[管理身分來源](#)和[支援的身分提供者](#)。
- 您可以透過簡單的自動探索和連線功能，與多個 Redshift 叢集和工作群組共用一個 IAM Identity Center 執行個體。這可讓您快速新增叢集，而無需為每個叢集設定 IAM Identity Center 連線的額外工作，並確保所有叢集和工作群組都有一致的使用者、使用者屬性和群組視觀表。請注意，您組織的 IAM Identity Center 執行個體必須與您要連線的任何 Redshift 資料共用位於相同的區域。
- 由於使用者身分是已知且會隨著資料存取而被記錄，因此您可以更輕鬆地透過稽核中的使用者存取權來符合法規 AWS CloudTrail。

設定 IAM Identity Center 與 Amazon Redshift 整合

您的 Amazon Redshift 叢集管理員或 Amazon Redshift Serverless 管理員必須執行幾個步驟，才能將 Redshift 設定為啟用 IAM Identity Center 的應用程式。這使得 Redshift 可以自動發現並連接 IAM Identity Center，以接收登入和使用者目錄服務。在此之後，當您的 Redshift 管理員建立叢集或工作群組時，他們可以讓新的資料倉儲使用 IAM Identity Center 來管理資料庫存取。

啟用 Redshift 做為 IAM Identity Center 受管應用程式的重點在於，您可以從 IAM Identity Center 內，或從與之整合的第三方身分提供者來控制使用者和群組權限。當您的資料庫使用者登入 Redshift 資料庫 (例如分析師或資料科學家) 時，它會在 IAM Identity Center 檢查其群組，而這些群組與 Redshift 中的角色名稱相符。以這種方式定義 Redshift 資料庫角色名稱的群組，可以存取一組用於銷售分析的資料表。下列各節展示如何設定此項。

必要條件

以下是將 IAM Identity Center 與 Amazon Redshift 整合的先決條件：

- 帳戶設定 — 如果您打算擁有跨帳戶使用案例，或者在具有相同 IAM 身分中心執行個體的不同帳戶中使用 Redshift 叢集，則必須在 AWS 組織的管理帳戶中設定 IAM 身分中心。這包括設定您的身分識別來源。如需詳細資訊，請參閱 AWS IAM Identity Center 使用者指南中的[入門](#)、[員工身分識別](#)和[支援的身分提供者](#)。您必須確定已在 IAM Identity Center 中建立使用者或群組，或從身分識別來源同步處理使用者和群組，然後才能將使用者和群組指派給 Redshift 中的資料。

Note

您可以選擇使用 IAM 身分中心的帳戶執行個體，前提是 Redshift 和 IAM 身分中心位於同一個帳戶中。當您建立和設定 Redshift 叢集或工作群組時，可以使用小工具建立此執行個體。

- 設定受信任的字符發行者 — 在某些情況下，您可能需要使用受信任的字符簽發者，這是一個可以發出和驗證信任字符的實體。在設定 IAM Identity Center 整合的 Redshift 管理員可以選取受信任的字符發行者，並新增必要的屬性以完成組態設定之前，必須先執行初步的步驟。這包括設定外部身分提供者做為受信任的字符發行者，以及在 IAM Identity Center 主控台新增其屬性。若要完成這些步驟，請參閱[搭配受信任憑證發行者使用應用程式](#)。

Note

並非所有外部連線都需要設定受信任的字符發行者。使用 Amazon Redshift 查詢編輯器 v2 連線到 Redshift 資料庫，並不需要受信任的字符發行者組態。但可以套用於第三方應用程式，例如透過您的身分提供者進行驗證的儀表板或自訂應用程式。

- 設定 IAM 角色 — 必須設定後續提及權限的區段。您必須依據 IAM 最佳實務新增許可權。下列程序會詳細說明特定權限。

如需詳細資訊，請參閱 [IAM Identity Center 入門](#)。

設定身分提供者，以使用 IAM Identity Center

控制使用者和群組身分管理的第一步是連線到 IAM Identity Center，並設定您的身分提供者。您可以使用 IAM Identity Center 本身做為身分提供者，也可以連接第三方身分存放區 (例如 Okta)。如需有關設定連線和設定身分提供者的詳細資訊，請參閱 IAM Identity Center 使用者指南中的 [連線至外部身分提供者](#)。請務必在此程序結束時將少數使用者和群組新增至 IAM Identity Center，以達測試之目的。

管理許可

紅移/IAM 身分中心應用程式生命週期管理所需的權限

您必須建立身分與存取權管理員，Redshift 管理員使用此身分識別身分來設定 Redshift，以便與 IAM 身分中心搭配使用。最常見的是，您可以建立具有許可的 IAM 角色，並根據需要將其指派給其他身分。它必須具有列出的權限才能執行下列動作。

建立紅移/IAM 身分識別中心應用程式

- `sso:PutApplicationAssignmentConfiguration`— 用於安全性。
- `sso:CreateApplication`— 用於建立 IAM Identity Center 應用程式。
- `sso:PutApplicationAuthenticationMethod`— 授予 Redshift 驗證存取權。
- `sso:PutApplicationGrant`— 用於變更受信任的字符發行者資訊。
- `sso:PutApplicationAccessScope`— 適用於 Redshift IAM Identity Center 應用程式設定。這包括適用於 AWS Lake Formation 和適用於 [Amazon S3 存取授權](#)。
- `redshift:CreateRedshiftIdcApplication`— 用於建立 Redshift IDC 應用程式。

描述紅移/IAM 身分識別中心應用程式

- `sso:GetApplicationGrant`— 用於列出受信任的字符發行者資訊。
- `sso:ListApplicationAccessScopes`— 針對 Redshift IAM 身分中心應用程式設定，以列出下游整合，例如針對 AWS Lake Formation 和 S3 存取授權。
- `redshift:DescribeRedshiftIdcApplications`— 用於描述現有的 IAM 身分中心應用程式。

變更紅移/IAM 身分中心應用程式

- `redshift:ModifyRedshiftIdcApplication`— 用於變更現有的 Redshift 應用程式。
- `sso:UpdateApplication`— 用於更新 IAM Identity Center 應用程式。
- `sso:GetApplicationGrant`— 獲取信任令牌發行者信息。
- `sso:ListApplicationAccessScopes`— 適用於 Redshift IAM Identity Center 應用程式設定。
- `sso>DeleteApplicationGrant`— 刪除信任權杖發行者資訊。
- `sso:PutApplicationGrant`— 用於變更受信任的字符發行者資訊。
- `sso:PutApplicationAccessScope`— 適用於 Redshift IAM Identity Center 應用程式設定。這包括適用於 AWS Lake Formation 和適用於 [Amazon S3 存取授權](#)。
- `sso>DeleteApplicationAccessScope`— 用於刪除 Redshift IAM 身份中心應用程序設置。這包括適用於 AWS Lake Formation 和適用於 [Amazon S3 存取授權](#)。

刪除紅移/IAM 身分中心應用程式

- `sso>DeleteApplication`— 用於刪除 IAM Identity Center 應用程式。
- `redshift>DeleteRedshiftIdcApplication`— 提供刪除現有 Redshift IDC 應用程式的功能。

紅移/查詢編輯器v2 應用程式生命週期管理所需的權限

您必須建立身分與存取權管理員，Redshift 管理員使用此身分識別身分來設定 Redshift，以便與 IAM 身分中心搭配使用。最常見的是，您可以建立具有許可的 IAM 角色，並根據需要將其指派給其他身分。它必須具有列出的權限才能執行下列動作。

創建查詢編輯器 v2 應用程序

- `redshift>CreateQev2IdcApplication`— 用於建立 QEV2 應用程式。
- `sso:CreateApplication`— 提供建立 IAM 身分中心應用程式的功能。
- `sso:PutApplicationAuthenticationMethod`— 授予 Redshift 驗證存取權。
- `sso:PutApplicationGrant`— 用於變更受信任的字符發行者資訊。
- `sso:PutApplicationAccessScope`— 適用於 Redshift IAM Identity Center 應用程式設定。這包括查詢編輯器第 2 版。
- `sso:PutApplicationAssignmentConfiguration`— 用於安全性。

描述查詢編輯器 v2 應用

- `redshift:DescribeQev2IdcApplications`— 用來描述 IAM 身分中心 QEV2 應用程式。

更改查詢編輯器 v2 應用程式

- `redshift:ModifyQev2IdcApplication`— 用於變更 IAM 身分中心 QEV2 應用程式。
- `sso:UpdateApplication`— 用於變更 IAM 身分中心 QEV2 應用程式。

刪除查詢編輯器 v2 應用程式

- `redshift>DeleteQev2IdcApplication`— 用於刪除 QEV2 應用程式。
- `sso>DeleteApplication`— 用於刪除 QEV2 應用程式。

Note

在 Amazon Redshift 開發套件中，以下 API 不可用：

- `CreateQev2 IdcApplication`
- `DescribeQev2 IdcApplications`
- `ModifyQev2 IdcApplication`
- `DeleteQev2 IdcApplication`

這些動作專門針對在主控台中與 Redshift QEV2 執行身分識別中心整合。AWS 如需詳細資訊，請參閱 [Amazon Redshift 定義的動作](#)。

資料庫管理員在主控台中連線新資源所需的權限

在建立過程中，需要這些權限才能連接新的佈建叢集或 Amazon Redshift Serverless 工作群組。如果您具有這些權限，主控台會顯示選項，供您選擇連線至適用於 Redshift 的 IAM Identity Center 受管應用程式。

- `redshift:DescribeRedshiftIdcApplications`
- `sso:ListApplicationAccessScopes`
- `sso:GetApplicationAccessScope`
- `sso:GetApplicationGrant`

我們建議的最佳實務是，將許可政策附加到 IAM 角色，然後根據需要將其指派給使用者和群組。如需詳細資訊，請參閱 [Amazon Redshift 中的身分和存取管理](#)。

使用 IAM 身分中心將 Redshift 設定為 AWS 受管應用程式

在 IAM Identity Center 可以管理 Amazon Redshift 佈建的叢集或 Amazon Redshift Serverless 工作群組的身分之前，Redshift 管理員必須先完成以下步驟，讓 Redshift 成為 IAM Identity Center 受管應用程式：

1. 在 Amazon Redshift 或 Amazon Redshift Serverless 主控台功能表中選取 IAM Identity Center 整合，然後選取連線至 IAM Identity Center。您可以從那裡逐步執行一系列選項，以填入 IAM Identity Center 整合的屬性。
2. 為 Redshift 的 IDC 受管應用程式選擇顯示名稱和唯一名稱。
3. 指定組織的命名空間。這通常是組織名稱的縮寫版。它會新增為 Redshift 資料庫中 IDC 管理的使用者和角色的字首。
4. 選取要使用的 IAM 角色。此 IAM 角色應與用於 Redshift 的其他角色分開，建議您不要將其用於其他用途。需要的特定政策許可如下所示：
 - `sso:DescribeApplication`— 在目錄中建立身分提供者 (IdP) 項目時需要。
 - `sso:DescribeInstance`— 用於手動建立 IdP 聯合角色或使用者。
5. 設定用戶端連線和受信任的字符發行者。藉由設定與外部身分提供者的關係，設定受信任的字符發行者有助於信任的身分傳播。身分傳播可讓使用者登入一個應用程式的同時，存取另一個應用程式中的特定資料。這可讓使用者更順暢地從不同位置收集資料。在此步驟中，您可以在主控台為每個受信任的字符發行者設定屬性。這些屬性包括名稱和受眾聲明 (或 `aud claim`)，您可能必須從工具或服務的組態屬性中取得這些聲明。您可能還需要提供第三方工具的 JSON Web 字符 (JWT) 應用程式名稱。

Note

根據字符類型，每個第三方工具或服務的 `aud claim` 需求可能會有所不同，字符類型可以是身分提供者發行的存取字符或另一種類型 (例如 ID 字符)。每個廠商可以有所不同。當您實作信任的身分傳播並與 Redshift 整合時，需要為第三方工具傳送給 AWS 的字符類型提供正確的 `aud` 值。查看您的工具或服務廠商的建議。

如需有關信任的身分傳播的詳細資訊，請參閱 [信任的身分傳播的運作方式](#)。另外，請參閱本文件隨附的 IAM Identity Center 測試版文件。

Redshift 管理員完成這些步驟並儲存設定之後，IAM Identity Center 屬性就會顯示在 Redshift 主控台中。您也可以查詢系統檢視 [SVV_IDENTITY_PROVIDERS](#)，以驗證應用程式的屬性。其中包括應用程式名稱和命名空間。您可以使用命名空間做為與應用程式相關聯之 Redshift 資料庫物件的字首。完成這些任務，使 Redshift 成為已啟用 IAM Identity Center 的應用程式。主控台內的屬性包括整合狀態。當整合完成時，會顯示已啟用。完成此程序後，可以在每個新叢集上啟用 IAM Identity Center 整合。

設定好組態之後，您可以透過選擇使用者或群組索引標籤，並選擇指派，在 Redshift 中包含 IAM Identity Center 的使用者和群組。

為新 Amazon Redshift 叢集或 Amazon Redshift Serverless 工作群組啟用 IAM Identity Center 整合

您的資料庫管理員會設定新的 Redshift 資源，以便與 IAM Identity Center 一致運作，使登入和資料存取操作更加輕鬆。這是建立已佈建叢集或 Serverless 工作群組的步驟的一部分來執行。任何具有建立 Redshift 資源權限的人，都可以執行這些 IAM Identity Center 整合任務。建立佈建的叢集時，請先在 Amazon Redshift 主控台選擇建立叢集。後續步驟說明如何為資料庫啟用 IAM Identity Center 管理。(不包括建立叢集的所有步驟。)

1. 在建立叢集步驟中的 IAM Identity Center 整合區段中選擇啟用 <您的叢集名稱>。
2. 啟用整合時，處理程序依照步驟。您可以在主控台選擇啟用 IAM Identity Center 整合以執行此操作。
3. 對於新的叢集或工作群組，請使用 SQL 命令在 Redshift 中建立資料庫角色。以下是命令：

```
CREATE ROLE <idcnamespac:rolename>;
```

命名空間和角色名稱如下所示：

- IAM Identity Center 命名空間字首 — 這是您在設定 IAM Identity Center 與 Redshift 之間的連線時定義的命名空間。
- 角色名稱 — 此 Redshift 資料庫角色必須與 IAM Identity Center 中的群組名稱相符。

Redshift 會與 IAM Identity Center 連線，並擷取建立資料庫角色，並將資料庫角色對應至 IAM Identity Center 群組所需的資訊。

請注意，建立新的資料倉儲時，針對 IDC 整合指定的 IAM 角色會自動附加到佈建的叢集或 Amazon Redshift Serverless 工作群組。完成輸入所需的叢集中繼資料並建立資源後，您可以在屬性中檢查 IAM Identity Center 整合的狀態。如果 IAM Identity Center 中的群組名稱有空格，則在建立相符角色時，必須在 SQL 中使用引號。

啟用 Redshift 資料庫並建立角色之後，您就可以使用 Amazon Redshift 查詢編輯器 v2 或 Amazon QuickSight 連線到資料庫。接下來章節中會進一步提供詳細資訊。

使用 API 設定預設值 `RedshiftIdcApplication`

設定作業由您的身分管理員執行。您可以使用 API 建立並填入 `RedshiftIdcApplication`，其代表 IAM Identity Center 內的 Redshift 應用程式。

1. 若要開始，您可以在 IAM Identity Center 中建立使用者，並將其加入至群組。您可以在 IAM 身分中心 (IDC) 的 AWS 主控台中執行此操作。
2. 呼叫 `create-redshift-idc-application` 以建立 IDC 應用程式，並使其與 Redshift 相容。您可以填入必要的值來建立應用程式。顯示名稱是指要在 IDC 儀表板上顯示的名稱。IAM 角色 ARN 是具有 IAM Identity Center 許可權限的 ARN，也可由 Redshift 確認。

```
aws redshift create-redshift-idc-application
--idc-instance-arn 'arn:aws:sso:::instance/ssoins-1234a01a1b12345d'
--identity-namespace 'MYCO'
--idc-display-name 'TEST-NEW-APPLICATION'
--iam-role-arn 'arn:aws:redshift:us-east-1:012345678901:role/TestRedshiftRole'
--redshift-idc-application-name 'myredshiftidcapplication'
```

下列範例顯示從呼叫 `create-redshift-idc-application` 傳回的範例 `RedshiftIdcApplication` 回應。

```
"RedshiftIdcApplication": {
  "IdcInstanceArn": "arn:aws:sso:::instance/ssoins-1234a01a1b12345d",
  "RedshiftIdcApplicationName": "test-application-1",
  "RedshiftIdcApplicationArn": "arn:aws:redshift:us-east-1:012345678901:redshiftidcapplication:12aaa111-3ab2-3ab1-8e90-b2d72aea588b",
  "IdentityNamespace": "MYCO",
  "IdcDisplayName": "Redshift-Idc-Application",
  "IamRoleArn": "arn:aws:redshift:us-east-1:012345678901:role/TestRedshiftRole",
  "IdcManagedApplicationArn": "arn:aws:sso:::012345678901:application/ssoins-1234a01a1b12345d/apl-12345678910",
  "IdcOnboardStatus": "arn:aws:redshift:us-east-1:123461817589:redshiftidcapplication",
  "RedshiftIdcApplicationArn": "Completed",
  "AuthorizedTokenIssuerList": [
    "TrustedTokenIssuerArn": ...,
    "AuthorizedAudiencesList": [...]]...
```

```
  ]}
```

3. 您可以使用 `create-application-assignment` 將特定群組或個別使用者指派給 IAM Identity Center 中的受管應用程式。這樣一來，您就可以指定要透過 IAM Identity Center 管理的群組。如果資料庫管理員在 Redshift 中建立資料庫角色，IAM Identity Center 中的群組名稱會對應至 Redshift 中的角色名稱。那些角色可以控制資料庫中的權限。如需詳細資訊，請參閱 [在 IAM Identity Center 主控台中指派應用程式的使用者存取權](#)。
4. 啟用應用程式後，請從 IAM Identity Center 呼叫 `create-cluster`，並加入 Redshift 受管應用程式 ARN。這樣做會使叢集與 IAM Identity Center 中的受管應用程式產生關聯。

為 IAM Identity Center 應用程式與現有叢集或工作群組建立關聯

如果您有要啟用 IAM Identity Center 整合的現有叢集或工作群組，則可以執行 SQL 命令來執行此作業。您會執行下列命令以啟用整合。資料庫管理員必須執行查詢，且 Redshift 和 IAM Identity Center 之間的連線已經設定完成。設定 `ENABLE` 後，它可讓 IAM Identity Center 為叢集或工作群組提供身分管理。

```
ALTER IDENTITY PROVIDER
<idp_name> | NAMESPACE <namespace> | IAM_ROLE default | 'arn:aws:iam::<AWS account-id-1>:role/<role-name>' | [DISABLE | ENABLE]
```

您可以捨棄現有身分提供者。以下範例顯示 `CASCADE` 如何刪除附加至身分提供者的使用者和角色。

```
DROP IDENTITY PROVIDER
<provider_name> [ CASCADE ]
```

設定使用者權限

管理員可根據使用者的身分屬性和群組成員資格，在其身分提供者內或在 IAM Identity Center 內直接設定各種資源的權限。例如，身分提供者管理員可以將資料庫工程師新增至適合其角色的群組。此群組名稱會對應至 Redshift 資料庫角色名稱。此角色可提供或限制 Redshift 中特定資料表或視觀表的存取權。

連接應用程式的管理員角色

以下是將分析應用程式連接到適用於 Redshift 的 IAM Identity Center 受管應用程式的關鍵角色：

- 應用程式管理員 — 建立應用程式，並設定應用程式將啟用哪些服務來交換身分字符。此管理員也會指定哪些使用者或群組可存取應用程式。

- 資料管理員 — 設定對資料的精細存取權限。IAM Identity Center 中的使用者和群組可對應至特定權限。

透過 IAM 身分中心連線至 Amazon Redshift Amazon QuickSight

以下內容顯示如何使用 Amazon 在 Redshift 連接 QuickSight 到 Redshift 進行身份驗證，並通過 IAM 身分中心進行訪問：[授權從 Amazon QuickSight 到亞馬 Amazon Redshift 集群的連接](#)。這些步驟也適用於 Amazon Redshift Serverless。

使用 IAM Identity Center，透過 Amazon Redshift 查詢編輯器第 2 版連線至 Amazon Redshift

在完成設定與 Redshift 的 IAM Identity Center 連線的操作步驟後，使用者可以透過以 IAM Identity Center 為基礎的命名空間前綴的身分，存取資料庫和資料庫中的適當物件。如需有關使用查詢編輯器 v2 登入以連線至 Redshift 資料庫的詳細資訊，請參閱[使用查詢編輯器 v2](#)。

透過查詢資料 AWS Lake Formation

使用可 AWS Lake Formation 讓您更輕鬆地集中控管和保護您的資料湖，並提供資料存取。透過 IAM Identity Center 和 Redshift 將身分傳播至 Lake Formation，如此管理員可以根據組織的身分提供者 (IdP) 群組，允許對 Amazon S3 資料湖進行更精細的存取。這些群組是透過 IAM Identity Center 進行管理。本節說明如何設定幾個使用案例、從資料湖查詢以及從資料共用進行查詢，以展示如何利用 IAM Identity Center 搭配 Redshift 連線至 Lake Formation 控管的資源。

使用 IAM Identity Center 和 Redshift 連線查詢資料湖

這些步驟涵蓋使用案例，您可以在其中使用連接到 Redshift 的 IAM Identity Center，查詢由 Lake Formation 管理的資料湖。

先決條件

此程序有幾個先決條件步驟：

1. 必須先設定 IAM Identity Center 才能透過 Redshift 支援身分驗證和身管理。您可以從主控台啟用 IAM Identity Center，然後選取身分提供者 (IdP) 來源。之後，將一組 IdP 使用者與 IAM Identity Center 同步處理。您也必須依照本文件先前詳述的步驟，設定 IAM Identity Center 和 Redshift 之間的連線。
2. 在組態設定步驟中建立新的 Amazon Redshift 叢集，並透過 IAM Identity Center 啟用身管理。

3. 建立 Lake Formation 的受管 IAM Identity Center 應用程式，並進行組態設定。這是接在設定 IAM Identity Center 和 Redshift 之間連線之後的步驟。步驟如下：
 - a. 在 AWS CLI 中，使用 `modify-redshift-idc-application` 命令促成 Lake Formation 服務與適用於 Redshift 的 IAM Identity Center 受管應用程式的整合。此呼叫包含 `service-integrations` 參數，該參數設定為啟用 Lake Formation 授權的組態字串值。
 - b. 使用 `create-lake-formation-identity-center-configuration` 命令設定 Lake Formation。這會建立適用於 Lake Formation 的 IAM Identity Center 應用程式，該應用程式會顯示在 IAM Identity Center 入口網站中。管理員必須設定 `--cli-input-json` 引數，其值是 JSON 檔案的路徑，該檔案的路徑使用所有 AWS CLI API 呼叫的標準格式。您可以包含下列各值：
 - `CatalogId`— Lake Formation 目錄 ID。
 - `InstanceArn`— IAM Identity Center 執行個體 ARN 值。

管理員完成必要條件組態之後，資料庫管理員可以建立外部結構描述以查詢資料湖。

1. 管理員建立外部結構描述 — Redshift 資料庫管理員使用下列 SQL 陳述式連線到資料庫，並建立外部結構描述：

```
CREATE EXTERNAL SCHEMA if not exists my_external_schema from DATA CATALOG database
'my_lf_integrated_db' catalog_id '12345678901234';
```

請注意，在這種情況下不需要指定 IAM 角色，因為存取權是透過 IAM Identity Center 進行管理。

2. 系統管理員授予權限 — 管理員會將使用權授予 IAM Identity Center 群組，該群組會授予 Redshift 資源的使用權。這是透過執行 SQL 陳述式來完成，如下所示：

```
GRANT USAGE ON SCHEMA "my_external_schema" to "MYCO:sales";
```

隨後，系統管理員會根據組織的需求，使用 AWS CLI 授與物件的 Lake Formation 權限：

```
aws lakeformation grant-permissions ...
```

3. 使用者執行查詢 — 此時，屬於銷售群組一部分的 IAM Identity Center 使用者，可以透過查詢編輯器 v2 登入 Redshift 資料庫。然後，他們可以執行存取外部結構描述中資料表的查詢，如以下範例所示：

```
SELECT * from my_external_schema.table1;
```

使用 IAM Identity Center 和 Redshift 連線連線至資料共用

透過 IAM Identity Center 管理存取權時，您可以從不同的 Redshift 資料倉儲存取資料共用。若要這麼做，您可以執行查詢來設定外部資料庫。在完成這些步驟之前，假設您已經在 Redshift 和 IAM 身分中心之間設定了連線，而且您已建立 AWS Lake Formation 應用程式，如先前程序所述。

1. 建立外部資料庫 — 管理員建立外部資料庫以進行資料共用，並透過其 ARN 參考該資料庫。以下是展示如何執行此操作的範例：

```
CREATE DATABASE "redshift_external_db" FROM ARN 'arn:aws:glue:us-east-1:123456789012:database/redshift_external_db-iad' WITH NO DATA CATALOG SCHEMA;
```

在此使用案例中，如果您搭配 Redshift 使用 IAM Identity Center 進行身管理，則不包含 IAM 角色。

2. 管理員設定許可 — 建立資料庫後，管理員會將使用權授予 IAM Identity Center 群組。這會授予 Redshift 資源的權限：

```
GRANT USAGE ON DATABASE "my_external_db" to "MYC0:sales";
```

系統管理員還會使用 AWS CLI 授予物件的 Lake Formation 權限：

```
aws lakeformation grant-permissions ...
```

3. 使用者執行查詢 — 來自銷售群的使用者可以根據指派的權限，查詢資料庫中的資料表：

```
select * from redshift_external_db.public.employees;
```

如需有關授予資料湖權限以及授予資料共用權限的詳細資訊，請參閱[將權限授予使用者和群組](#)。如需將使用權授予結構描述或資料庫的詳細資訊，請參閱[GRANT](#)。

使用信任的字符發行者將您的應用程式或工具與 OAuth 整合

您可以透過 IAM 身分中心連線，將功能新增至您建立的用戶端工具以連線至 Redshift。如果您已將 Redshift 整合設定為 IAM 身分中心，請使用本節中詳述的屬性來設定連線。

身份驗證插件，用於使用 IAM 身份中心連接到 Redshift

IdpTokenAuthPlugin 透過 IAM 身分中心提供連線屬性並促進身份驗證。它接受來自與 IAM 身分中心 Connect 的任何網絡身份提供商的 OpenID 連接 (OIDC) JSON 網絡令牌 (JWT)。

如果您使用的是 Amazon Redshift 驅動程式，則可以透過 IAM 身分中心使 IdpTokenAuthPlugin 用紅移進行身份驗證。該插件接受來自與 IAM 身分中心連接的任何 Web 身份提供商的 OIDC JWT。下表詳細說明要用於成功驗證的連線選項。

驅動程式	連線選項鍵	Value	備註
JDBC	plugin_name	。亞馬遜。。。IdpTokenAuthPlugin	連線時，您必須輸入外掛程式的完整類別名稱。
ODBC	plugin_name	IdpTokenAuthPlugin	
Python	credential_provider	IdpTokenAuthPlugin	沒有可用於 Python 驅動程式的 plugin_name 選項。請改用 credential_provider 。

該插件具有以下附加連接選項：

- 令牌 — 由與 IAM 身分中心 Connect 的網絡身份提供商提供的 OpenID 連接 (OIDC) JSON 網絡令牌 (JWT)。您的應用程式必須透過與 IAM 身分中心連線的身分提供者驗證應用程式使用者來產生此權杖。
- 權杖類型 — 用於的權杖類型。IdpTokenAuthPlugin 您可以指定下列選項的值：
 - EXT_JWT — 如果您使用 OpenID Connect (OIDC) JSON 網絡令牌 (JWT)，由與 IAM 身分中心連接的基於 Web 的身份提供商提供，請提供此選項。

您必須在建立並連接的工具的連接屬性中輸入這些值。如需詳細資訊，請參閱各個驅動程式的連線選項說明文件：

- [JDBC 驅動程式 2.1 版組態的選項](#)
- [設定 ODBC 驅動程式選項](#)
- [Amazon Redshift Python 連接器的組態選項](#)

疑難排解來自 Amazon Redshift 查詢編輯器 v2 的連

此清單詳細說明常發生的錯誤，並可協助您使用 IAM 身分中心身分，透過查詢編輯器 v2 連線至 Redshift 資料庫。

- 錯誤：連線問題：沒有可用的身分中心工作階段資訊。— 發生此錯誤時，請檢查瀏覽器的安全性和隱私設定。這些瀏覽器設定，特別是安全 Cookie 的設定，例如 Firefox 的完整 Cookie 保護功能，可能會導致從亞馬遜 Redshift 查詢編輯器 v2 到 Redshift 資料庫的連線嘗試遭到封鎖。請依照您瀏覽器的詳細修復步驟進行：
 - 火狐 — 當前，第三方 cookie 默認情況下被阻止。按一下瀏覽器網址列中的盾牌，然後切換開關以關閉查詢編輯器 v2 的增強型追蹤保護。
 - Chrome 無痕模式 — 在預設情況下，Chrome 無痕模式會封鎖第三方 Cookie。按一下網址列中的眼睛圖示，以允許第三方 Cookie 用於查詢編輯器 v2。將設定變更為允許 Cookie 後，網址列上可能看不到眼睛圖示。
 - 野生動物園 — 在 Mac 上，打開 Safari 瀏覽器應用程式。選擇設定，然後選擇進階。切換為關閉：封鎖所有 Cookie。
 - 邊緣 — 選擇「設定」，然後選擇「Cookie 和網站權限」。然後選取 [管理和刪除 Cookie 和網站資料]，然後關閉 [封鎖第三方 Cookie]。

如果您在變更設定後嘗試連線，並繼續收到錯誤訊息連線問題：沒有可用的身分中心工作階段資訊，建議您重新整理與 IAM Identity Center 的連線。若要這麼做，請在 Redshift 資料庫執行個體上按一下滑鼠右鍵，然後選擇 [這時系統顯示一個新窗口，您可以使用該窗口進行驗證。

- 錯誤：連線問題：身分識別中心工作階段已過期或無效。— 在將 Redshift 佈建的叢集或無伺服器工作群組與 IAM 身分中心整合之後，使用者嘗試從查詢編輯器 v2 連線至 Redshift 資料庫時，可能會收到此錯誤訊息。這可以跟隨成功的連接嘗試。在這種情況下，我們建議您重新驗證。若要這麼做，請在 Redshift 資料庫執行個體上按一下滑鼠右鍵，然後選擇 [這時系統顯示一個新窗口，您可以使用該窗口進行驗證。
- 錯誤：無效的範圍。使用者身份證明未獲得連線至 Redshift 的授權。— 在將 Redshift 佈建的叢集或無伺服器工作群組與 IAM 身分識別中心進行身分管理整合之後，使用者嘗試從查詢編輯器 v2 連線至 Redshift 資料庫時，可能會收到此錯誤訊息。在這種情況下，為了使查詢編輯器 v2 能夠透過 IAM 身分中心成功連線和驗證使用者以存取正確的資源，系統管理員必須透過 Redshift 主控台將使用者指派給 Redshift IAM 身分中心應用程式。這是在 IAM 身分中心連線下完成的。在此之後，使用者可以在一小時後建立成功的連線，這是 IAM Identity Center 工作階段快取的限制。
- 錯誤：無法列出資料庫。致命：群集 auto 暫停時查詢失敗。— 當 Amazon Redshift 無伺服器資料庫處於閒置狀態而未處理任何工作負載時，當您與 IAM 身分中心身分連線時，該資料庫可能會保持暫

停狀態。若要解決此問題，請使用其他驗證方法登入以繼續無伺服器工作群組。然後使用您的 IAM 身分中心身分連線到資料庫。

- 錯誤：嘗試與 IAM 身分中心聯合時發生錯誤。Amazon Redshift 管理員必須使用紅移主控台刪除和重新建立 IAM 身分中心 QEV2 應用程式。— 刪除與查詢編輯器 v2 相關聯的 IAM 身分中心應用程式執行個體時，通常會發生此錯誤。若要解決此問題，Amazon Redshift 管理員必須刪除並重新建立適用於 IAM 身分中心的 Redshift 和查詢編輯器 v2 應用程式。這可以在 Redshift 控制台上執行，也可以使用 <https://docs.aws.amazon.com/cli/latest/reference/redshift/delete-redshift-idc-application.html> CLI 命令執行。

限制

這些限制均適用：

- 使用 IAM 身分中心搭配 Redshift 驅動程式 — 當您使用可透過目前 Redshift 驅動程式取得的身分識別中心時，用戶端應用程式必須產生身份驗證權杖。IdpTokenAuthPlugin 但請注意，AWS IAM 身分中心目前不支援為 Redshift 產生存取權杖。因此，不支援使用 IAM 身分中心存取權杖。目前可以透過與 IAM 身分中心整合的外部網路身分提供者 (例如 Okta 或 Microsoft 恩特拉 ID (Azure AD) IdpTokenAuthPlugin 來連接 Amazon Redshift 資料庫。PingOne 在這種情況下，客戶端負責從網路身份提供商生成 OpenID Connect (OIDC) JSON Web 令牌 (JWT)，並將其作為輸入提供給驅動程序。IdpTokenAuthPlugin 該插件在上一節中描述。如果您想直接使用 IAM 身分中心授權和身份驗證，也可以使用查詢編輯器 v2 進行連線。
- 不支援增強型 VPC — 使用 IAM 身分中心設定 Redshift 受信任身分傳播時，不支援增強型 VPC。如需有關增強型 VPC 的詳細資訊，請參閱 [Amazon Redshift 中的增強型 VPC 路由](#)。
- IAM 身分中心快取 — IAM 身分中心快取工作階段資訊。當您嘗試透過 Redshift 查詢編輯器 v2 連線至 Redshift 資料庫時，這可能會造成無法預期的存取問題。這是因為即使在資料庫使用者登出 AWS 主控台的情況下，查詢編輯器 v2 中關聯的 IAM 身分中心工作階段仍然有效。快取會在一小時後過期，這通常會修正任何問題。

使用 Amazon Redshift 的服務連結角色

Amazon Redshift 使用 AWS Identity and Access Management (IAM) [服務連結](#) 角色。服務連結角色是直接連結至 Amazon Redshift 的一種特殊 IAM 角色類型。服務連結角色是由 Amazon Redshift 預先定義的，並包含該服務代表 Amazon Redshift 叢集呼叫 AWS 服務所需的所有許可。

服務連結角色可讓設定 Amazon Redshift 變得更加簡單，因為您不必手動新增必要的許可。角色已連結到 Amazon Redshift 使用案例並且具備預先定義的許可。只有 Amazon Redshift 可以擔任此角色，

且只有服務連結角色可以使用預先定義的許可政策。當您第一次建立叢集或由 RedShift 管理的 VPC 端點時，Amazon Redshift 會在您的帳戶中建立服務連結角色。只有在刪除帳戶中的所有 Amazon Redshift 叢集或由 RedShift 管理的虛擬私人雲端端點之後，才能刪除服務連結角色。因為您不會不小心移除存取資源所需的許可，這可保護您的 Amazon Redshift 資源。

Amazon Redshift 在所有提供服務的區域中支援使用服務連結的角色。如需詳細資訊，請參閱 [AWS 區域與端點](#)。

如需關於支援服務連結角色的其他服務資訊，請參閱 [《可搭配 IAM 運作的 AWS 服務》](#)，並尋找在服務連結角色欄中顯示為是的服務。選擇具有連結的是，以檢視該服務的服務連結角色文件。

Amazon Redshift 的服務連結角色許可

Amazon Redshift 使用名為的服務連結角色 `AWSServiceRoleForRedshift`— 允許 Amazon Redshift 代表您呼叫 AWS 服務。此服務連結角色連接至下列受管政策：`AmazonRedshiftServiceLinkedRolePolicy`。如需此政策的更新，請參閱 [Amazon Redshift 的 AWS 受管 \(預先定義\) 政策](#)。

`AWSServiceRoleForRedshift` 服務連結角色只 `redshift.amazonaws.com` 信任擔任該角色。

`AWSServiceRoleForRedshift` 服務連結的角色許可政策允許 Amazon Redshift 在所有相關資源上完成下列操作：

- `ec2:DescribeVpcs`
- `ec2:DescribeSubnets`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeAddress`
- `ec2:AssociateAddress`
- `ec2:DisassociateAddress`
- `ec2:CreateNetworkInterface`
- `ec2>DeleteNetworkInterface`
- `ec2:ModifyNetworkInterfaceAttribute`
- `ec2:CreateVpcEndpoint`
- `ec2>DeleteVpcEndpoints`
- `ec2:DescribeVpcEndpoints`
- `ec2:ModifyVpcEndpoint`
- `ec2:DescribeVpcAttribute`

- `ec2:DescribeSecurityGroups`
- `ec2:DescribeInternetGateways`
- `ec2:DescribeSecurityGroupRules`
- `ec2:DescribeAvailabilityZones`
- `ec2:DescribeNetworkAcls`
- `ec2:DescribeRouteTables`
- `ec2:AssignIpv6Addresses`
- `ec2:UnassignIpv6Addresses`

網路資源的許可

下列許可允許在 Amazon EC2 上執行動作，以建立和管理安全群組規則。這些安全群組和規則特別與 Amazon Redshift `aws:RequestTag/Redshift` 資源標籤相關聯。這會將許可的適用範圍限制在特定的 Amazon Redshift 資源。

- `ec2:CreateSecurityGroup`
- `ec2:AuthorizeSecurityGroupEgress`
- `ec2:AuthorizeSecurityGroupIngress`
- `ec2:RevokeSecurityGroupEgress`
- `ec2:RevokeSecurityGroupIngress`
- `ec2:ModifySecurityGroupRules`
- `ec2>DeleteSecurityGroup`

稽核記錄的動作

列出 `logs` 字首的動作與稽核記錄和相關功能有關。具體而言是日誌群組和日誌串流的建立與管理。

- `logs:CreateLogGroup`
- `logs:PutRetentionPolicy`
- `logs:CreateLogStream`
- `logs:PutLogEvents`
- `logs:DescribeLogStreams`
- `logs:GetLogEvents`

下列 JSON 會向 Amazon Redshift 顯示動作和資源範圍，以進行稽核記錄。

```
[
  {
    "Sid": "EnableCreationAndManagementOfRedshiftCloudwatchLogGroups",
    "Effect": "Allow",
    "Action": [
      "logs:CreateLogGroup",
      "logs:PutRetentionPolicy"
    ],
    "Resource": [
      "arn:aws:logs:*:*:log-group:/aws/redshift/*"
    ]
  },
  {
    "Sid": "EnableCreationAndManagementOfRedshiftCloudwatchLogStreams",
    "Effect": "Allow",
    "Action": [
      "logs:CreateLogStream",
      "logs:PutLogEvents",
      "logs:DescribeLogStreams",
      "logs:GetLogEvents"
    ],
    "Resource": [
      "arn:aws:logs:*:*:log-group:/aws/redshift/*:log-stream:*"
    ]
  }
]
```

如需有關服務連結角色及其用途的詳細資訊 AWS，請參閱[使用服務連結](#)角色。如需 Amazon Redshift 的特定動作和其他 IAM 資源的相關資訊，請參閱 [Amazon Redshift 的動作、資源和條件索引鍵](#)。

管理管理員認證的動作 AWS Secrets Manager

列出 secretsmanager 字首的動作與使用 Amazon Redshift 來管理管理員憑證有關。這些動作可讓 Amazon Redshift 用 AWS Secrets Manager 來建立和管理您的管理登入資料密碼。

以下 JSON 向 Amazon Redshift 顯示了用 AWS Secrets Manager 於管理管理登入資料的動作和資源範圍。

```
[
  {
```

```

    "Effect": "Allow",
    "Action": [
      "secretsmanager:DescribeSecret",
      "secretsmanager>DeleteSecret",
      "secretsmanager:PutSecretValue",
      "secretsmanager:UpdateSecret",
      "secretsmanager:UpdateSecretVersionStage",
      "secretsmanager:RotateSecret"
    ],
    "Resource": [
      "arn:aws:secretsmanager:*:*:secret:redshift!*"
    ],
    "Condition": {
      "StringEquals": {
        "secretsmanager:ResourceTag/aws:secretsmanager:owningService":
"redshift"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "secretsmanager:GetRandomPassword"
    ],
    "Resource": "*"
  }
]

```

允許 IAM 實體建立 AWSServiceRoleForRedshift 服務連結角色

```

{
  "Effect": "Allow",
  "Action": [
    "iam:CreateServiceLinkedRole"
  ],
  "Resource": "arn:aws:iam::<AWS-account-ID>:role/aws-service-role/
redshift.amazonaws.com/AWSServiceRoleForRedshift",
  "Condition": {"StringLike": {"iam:AWSServiceName": "redshift.amazonaws.com"}}
}

```

允許 IAM 實體刪除 AWSServiceRoleForRedshift 服務連結角色

將以下政策陳述式新增到該 IAM 實體的許可中：

```
{
  "Effect": "Allow",
  "Action": [
    "iam:DeleteServiceLinkedRole",
    "iam:GetServiceLinkedRoleDeletionStatus"
  ],
  "Resource": "arn:aws:iam::<AWS-account-ID>:role/aws-service-role/redshift.amazonaws.com/AWSServiceRoleForRedshift",
  "Condition": {"StringLike": {"iam:AWSServiceName": "redshift.amazonaws.com"}}
}
```

或者，您也可以使用受 AWS 管政策來[提供對 Amazon Redshift 的完整存取權](#)。

建立 Amazon Redshift 的服務連結角色

您不需要手動建立 AWSServiceRoleForRedshift 服務連結角色。Amazon Redshift 會為您建立服務連結角色。如果 AWSServiceRoleForRedshift 服務連結角色已從您的帳戶中刪除，Amazon Redshift 會在您啟動新的 Amazon Redshift 叢集時建立該角色。

Important

如果您在 2017 年 9 月 18 日之前使用 Amazon Redshift 服務，那麼該服務開始支援服務連結角色時，Amazon Redshift 就會在您的帳戶中建立該 AWSServiceRoleForRedshift 角色。若要進一步了解，請參閱[顯示在我的 IAM 帳戶中的新角色](#)。

編輯 Amazon Redshift 的服務連結角色

Amazon Redshift 不允許您編輯 AWSServiceRoleForRedshift 服務連結的角色。因為可能有各種實體會參考服務連結角色，所以您無法在建立角色之後變更其名稱。不過，您可以使用 IAM 主控台、AWS Command Line Interface (AWS CLI) 或 IAM API 編輯角色的說明。如需詳細資訊，請參閱《IAM 使用者指南》中的[修改角色](#)。

刪除 Amazon Redshift 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。

您必須先關閉和刪除帳戶中的任何叢集，才能刪除帳戶的服務連結角色。如需詳細資訊，請參閱[關閉及刪除叢集](#)。

您可以使用 IAM 主控台 AWS CLI、或 IAM API 刪除服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的[刪除服務連結角色](#)。

使用 IAM 身分驗證產生資料庫使用者憑證

您可依 AWS Identity and Access Management (IAM) 許可政策所授予的許可產生暫時性資料庫憑證，以管理使用者對 Amazon Redshift 資料庫的存取。

Amazon Redshift 資料庫使用者通常會使用資料庫使用者名稱和密碼來登入資料庫。但是，您不必維護 Amazon Redshift 資料庫中的使用者名稱和密碼。另一種方法是，您可以將系統設定為允許使用者建立使用者登入資料，並根據其 IAM 登入資料登入資料庫。

如需詳細資訊，請參閱《IAM 使用者指南》中的[身分提供者與聯合](#)。

主題

- [概觀](#)
- [建立暫時性 IAM 憑證](#)
- [提供 IAM 登入資料的選項](#)

概觀

Amazon Redshift 提供 [GetClusterCredentials](#) API 操作來產生臨時資料庫使用者登入資料。您可以使用 Amazon Redshift JDBC 或 ODBC 驅動程式來設定 SQL 用戶端，以便管理呼叫 `GetClusterCredentials` 操作的程序。其作法是擷取資料庫使用者憑證，然後在 SQL 用戶端和 Amazon Redshift 資料庫之間建立連線。但您也可以使用資料庫應用程式，以程式設計的方式呼叫 `GetClusterCredentials` 操作，擷取資料庫使用者登入資料，然後連線至資料庫。

如果您已在外部管理使用者身分 AWS，則可以使用符合安全聲明標記語言 (SAML) 2.0 的身分提供者 (IdP) 來管理對 Amazon Redshift 資源的存取。您需設定 IdP，允許聯合身分使用者存取 IAM 角色。您可利用該 IAM 角色產生暫存資料庫憑證，並登入 Amazon Redshift 資料庫。

您的 SQL 用戶端需要許可，才能為您呼叫 `GetClusterCredentials` 操作。若要管理這些許可，您需建立 IAM 角色並連接 IAM 許可政策，以授予或限制對 `GetClusterCredentials` 操作和相關動作的存取。我們建議的最佳實務是，將許可政策附加到 IAM 角色，然後根據需要將其指派給使用者和群組。如需詳細資訊，請參閱 [Amazon Redshift 中的身分和存取管理](#)。

政策也會授予或限制特定資源的存取，例如 Amazon Redshift 叢集、資料庫、資料庫使用者名稱和使用群組名稱。

Note

我們建議使用 Amazon Redshift JDBC 或 ODBC 驅動程式來管理呼叫 `GetClusterCredentials` 操作及登入資料庫的程序。為簡化程序，我們假設您在本主題中都透過 JDBC 或 ODBC 驅動程式使用 SQL 用戶端。如需使用 `GetClusterCredentials` 作業或 `parallel get-cluster-credentials` CLI 指令的特定詳細資訊和範例，請參閱 [GetClusterCredentials](#) 和 [get-cluster-credentials](#)。

為了集中管理身分驗證和授權，Amazon Redshift 支援使用 IAM 進行資料庫身分驗證，可讓您透過企業聯合進行使用者身分驗證。您可以使用 AWS Directory Service、企業使用者目錄或 Web 身分提供者的現有身分，而不需要建立使用者。這些稱為聯合使用者。AWS 透過 IdP 要求存取時，會將角色指派給聯合身分使用者。

若要為組織使用者或用戶端應用程式提供同盟存取以呼叫 Amazon Redshift API 操作，您也可以使用具有 SAML 2.0 支援的 JDBC 或 ODBC 驅動程式，向組織 IdP 請求身分驗證。在這種情況下，組織的使用者無法直接存取 Amazon Redshift。

建立暫時性 IAM 憑證

您將在本節中了解如何設定系統以產生暫時性 IAM 型資料庫使用者登入資料，並使用新的登入資料來登入資料庫。

高階的程序流程如下：

1. [步驟 1：建立適用於 IAM 單一登入存取的 IAM 角色](#)

(選用) 您可整合 IAM 身分驗證和第三方身分提供者 (IdP)，對存取 Amazon Redshift 資料庫的使用者進行驗證。

2. [步驟 2：設定 IdP 的 SAML 聲明](#)

(選用) 若要利用 IdP 使用 IAM 身分驗證，您需要在 IdP 應用程式中定義宣告規則，將組織中的使用者或群組映射到 IAM 角色。您也可選擇性加入屬性元素，以設定 `GetClusterCredentials` 參數。

3. [步驟 3：建立具有呼叫權限的 IAM 角色 `GetClusterCredentials`](#)

SQL 用戶端應用程式在呼叫 `GetClusterCredentials` 操作時會擔任使用者。如果已建立用於身分提供者存取的 IAM 角色，您可為該角色新增必要的許可。

4. [步驟 4：建立資料庫使用者和資料庫群組](#)

(選用) 根據預設，如果使用者名稱不存在，GetClusterCredentials 會傳回登入資料以建立新的使用者。您也可以選擇指定使用者登入時會加入的使用者群組。根據預設，資料庫使用者將加入 PUBLIC 群組。

5. [步驟 5：設定 JDBC 或 ODBC 連線使用 IAM 登入資料](#)

若要連線至 Amazon Redshift 資料庫，請將 SQL 用戶端設定為使用 Amazon Redshift JDBC 或 ODBC 驅動程式。

步驟 1：建立適用於 IAM 單一登入存取之 IAM 角色

如果您未使用身分提供者進行單一登入存取，可略過此步驟。

如果您已在以外管理使用者身分識別 AWS，則可以透過整合 IAM 身分驗證和第三方 SAML-2.0 身分識別提供者 (IdP) 來驗證使用者以存取 Amazon Redshift 資料庫。

如需詳細資訊，請參閱《IAM 使用者指南》中的[身分提供者與聯合](#)。

在您可以使用 Amazon Redshift IdP 身分驗證之前，請先建立 AWS SAML 身分識別提供者。您可以在 IAM 主控台中建立 IdP，以通 AWS 知 IdP 及其設定。這樣做會在您的 AWS 帳戶和 IdP 之間建立信任。如需建立角色的步驟，請參閱《IAM 使用者指南》中的[為 SAML 2.0 聯合建立角色 \(主控台\)](#)。

步驟 2：設定 IdP 的 SAML 聲明

建立 IAM 身分後，請在 IdP 應用程式中定義宣告規則，以將組織中的使用者或群組映射到 IAM 角色。如需詳細資訊，請參閱《IAM 使用者指南》中的[為身分驗證回應設定 SAML 聲明](#)。

如果您選擇使用選用的 GetClusterCredentials 參數 DbUser、AutoCreate、和 DbGroups，則有兩個選項。您可以使用 JDBC 或 ODBC 連線來設定參數值，或將 SAML 屬性元素新增至 IdP 以設定數值。如需 DbUser、AutoCreate 和 DbGroups 參數的詳細資訊，請參閱[步驟 5：設定 JDBC 或 ODBC 連線使用 IAM 登入資料](#)。

Note

如果您使用 IAM 政策變數 `${redshift:DbUser}`，如[資源策略 GetClusterCredentials](#)中所述，則會以 API 操作的請求內容所擷取的值取代 DbUser 的值。Amazon Redshift 驅動程式使用連線 URL 提供的 DbUser 變數的值，而非提供作為 SAML 屬性的值。

為了協助保護此組態的安全，建議您在 IAM 政策中使用條件，以使用 RoleSessionName 來驗證 DbUser 值。您可以在[使用政策範例 GetClusterCredentials](#)中找到如何使用 IAM 政策來設定條件的範例。

若要設定 IdP 以設定 DbUser、AutoCreate 和 DbGroups 參數，請包含下列 Attribute 元素：

- Name 屬性設定為 "https://redshift.amazon.com/SAML/Attributes/DbUser" 的 Attribute 元素

將 AttributeValue 設定為即將連線至 Amazon Redshift 資料庫的使用者名稱。

AttributeValue 元素中的值長度必須為小寫，開頭需為英文字母，只能包含英數字元、底線 (「_」)、加號 (「+」)、點號 (「.」)、At (「@」) 或連字號 (「-」)，且不得超過 128 個字元。使用者名稱的通常為使用者 ID (例如，bobsmith) 或電子郵件地址 (例如，bobsmith@example.com)。該值不能包含空格 (例如，Bob Smith 之類的使用者顯示名稱)。

```
<Attribute Name="https://redshift.amazon.com/SAML/Attributes/DbUser">
  <AttributeValue>user-name</AttributeValue>
</Attribute>
```

- 與名稱屬性設置為 "https://redshift.amazon.com/SAML/Attributes/AutoCreate" 的屬性元素

將 AttributeValue 元素設置為 true 以創建一個新的數據庫用戶 (如果不存在)。將設定 AttributeValue 為 false 以指定資料庫使用者必須存在於 Amazon Redshift 資料庫中。

```
<Attribute Name="https://redshift.amazon.com/SAML/Attributes/AutoCreate">
  <AttributeValue>true</AttributeValue>
</Attribute>
```

- Name 屬性設定為 "https://redshift.amazon.com/SAML/Attributes/DbGroups" 的 Attribute 元素

此元素包含一或多個 AttributeValue 元素。將每個 AttributeValue 元素設定為 DbUser 在連線至 Amazon Redshift 資料庫之工作階段期間將加入的資料庫群組名稱。

```
<Attribute Name="https://redshift.amazon.com/SAML/Attributes/DbGroups">
  <AttributeValue>group1</AttributeValue>
  <AttributeValue>group2</AttributeValue>
  <AttributeValue>group3</AttributeValue>
</Attribute>
```

步驟 3：建立具有呼叫權限的 IAM 角色 GetClusterCredentials

您的 SQL 用戶端需要授權，才能代替您呼叫 GetClusterCredentials 操作。若要提供授權，您應建立使用者或角色，並附加授予必要許可的政策。

建立具有呼叫權限的 IAM 角色 GetClusterCredentials

1. 使用 IAM 服務建立使用者或角色。也可使用現有的使用者或角色，例如，如果已建立用於身分提供者存取的 IAM 角色，您可將必要的 IAM 政策連接至該角色。
2. 連接具有呼叫 `redshift:GetClusterCredentials` 操作許可的許可政策。根據指定的選用參數而定，您也能在政策中允許或限制其他動作和資源：
 - 若要允許您的 SQL 用戶端擷取叢集 ID、AWS 區域和連接埠，請包含使用 Redshift 叢集資源呼叫 `redshift:DescribeClusters` 作業的權限。
 - 如果使用 `AutoCreate` 選項，請在 `dbuser` 資源中包含呼叫 `redshift>CreateClusterUser` 的許可。以下 Amazon Resource Name (ARN) 會指定 Amazon Redshift `dbuser`。將 `regionaccount-id`、和 `cluster-name` 取代為您的 AWS 地區、帳戶和叢集的值。針對 `dbuser-name`，指定用來登入叢集資料庫的使用者名稱。

```
arn:aws:redshift:region:account-id:dbuser:cluster-name/dbuser-name
```

- (選用) 新增 ARN 以指定 Amazon Redshift `dbname` 資源，格式如下。將 `regionaccount-id`、和 `cluster-name` 取代為您的 AWS 地區、帳戶和叢集的值。針對 `database-name`，指定使用者將登入的資料庫名稱。

```
arn:aws:redshift:region:account-id:dbname:cluster-name/database-name
```

- 如果您使用 `DbGroups` 選項，請包含對 Amazon Redshift `dbgroup` 資源呼叫 `redshift:JoinGroup` 操作的許可，格式如下。將 `regionaccount-id`、和 `cluster-name` 取代為您的 AWS 地區、帳戶和叢集的值。針對 `dbgroup-name`，指定使用者登入時要加入的使用者群組名稱。

```
arn:aws:redshift:region:account-id:dbgroup:cluster-name/dbgroup-name
```

如需詳細資訊和範例，請參閱 [資源策略 GetClusterCredentials](#)。

下面的範例顯示允許 IAM 角色呼叫 `GetClusterCredentials` 操作的政策。指定 Amazon Redshift `dbuser` 資源會將角色存取授予名為 `examplecluster` 的叢集上的資料庫使用者名稱 `temp_creds_user`。

```
{
```

```

"Version": "2012-10-17",
"Statement": {
  "Effect": "Allow",
  "Action": "redshift:GetClusterCredentials",
  "Resource": "arn:aws:redshift:us-west-2:123456789012:dbuser:examplecluster/
temp_creds_user"
}
}

```

您可以使用萬用字元 (*) 來取代全部或一部分的叢集名稱、使用者名稱和資料庫群組名稱。以下範例允許指定帳戶中任何叢集任何開頭為 temp_ 的使用者名稱。

Important

下列範例中的陳述式指定萬用字元 (*) 做為資源的部分值，因此政策允許任何開頭為指定字元的資源。在 IAM 政策中使用萬用字元可能會授予過多許可，根據最佳實務，建議使用適用於您商業應用程式最嚴苛的政策。

```

{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "redshift:GetClusterCredentials",
    "Resource": "arn:aws:redshift:us-west-2:123456789012:dbuser:*/temp_*"
  }
}

```

以下範例顯示允許 IAM 角色呼叫 GetClusterCredentials 操作的策略，且選項將自動建立新使用者並指定使用者於登入時加入的群組。"Resource": "*" 子句授予角色任何資源的存取權，包括叢集、資料庫使用者或使用者群組。

```

{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "redshift:GetClusterCredentials",
      "redshift:CreateClusterUser",
      "redshift:JoinGroup"
    ],

```

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

如需詳細資訊，請參閱 [Amazon Redshift ARN 語法](#)。

步驟 4：建立資料庫使用者和資料庫群組

您可選擇性建立資料庫使用者，以用來登入叢集資料庫。如果您為現有的使用者建立暫時性使用者登入資料，您可停用使用者的密碼，以強制使用者用暫時性密碼登入。或者，您也可使用 `GetClusterCredentials Autocreate` 選項自動建立新的資料庫使用者。

您可建立資料庫使用者群組並加入允許 IAM 資料庫使用者於登入時加入的許可。呼叫 `GetClusterCredentials` 操作時，您可指定新使用者於登入時加入的使用者群組名稱清單。這些群組成員資格僅適用於使用指定請求產生之登入資料所建立的工作階段。

建立資料庫使用者和資料庫群組

1. 登入 Amazon Redshift 資料庫並使用 [CREATE USER](#) 建立資料庫使用者，或使用 [ALTER USER](#) 來變更現有的使用者。
2. 選擇性地指定 `PASSWORD DISABLE` 選項，防止使用者使用密碼。停用使用者密碼後，使用者只能使用暫時性憑證登入。如果未停用密碼，使用者可用其密碼或暫時性憑證登入。您無法停用超級使用者的密碼。

如果使用者想要與 AWS 之外的 AWS Management Console 授與程式設計存取 AWS 取權的方式取決於正在存取的使用者類型。

若要授與使用者程式設計存取權，請選擇下列其中一個選項。

哪個使用者需要程式設計存取權？	到	By
人力身分 (IAM Identity Center 中管理的使用者)	使用臨時登入資料來簽署對 AWS CLI、AWS SDK 或 AWS API 的程式設計要求。	請依照您要使用的介面所提供的指示操作。 <ul style="list-style-type: none"> • 如需詳細資訊 AWS CLI，請參閱 《使 AWS CLI 用 AWS Command Line Interface 者指南》 AWS

哪個使用者需要程式設計存取權？	到	By
		IAM Identity Center中的〈配置使用〉。 <ul style="list-style-type: none"> 如需 AWS SDK、工具和 AWS API，請參閱 AWS SDK 和工具參考指南中的 IAM 身分中心身分驗證。
IAM	使用臨時登入資料來簽署對 AWS CLI、AWS SDK 或 AWS API 的程式設計要求。	遵循《IAM 使用者指南 》中的〈 將臨時登入資料搭配 AWS 資源 使用〉中的指示
IAM	(不建議使用) 使用長期認證來簽署對 AWS CLI、AWS SDK 或 AWS API 的程式設計要求。	請依照您要使用的介面所提供的指示操作。 <ul style="list-style-type: none"> 如需相關資訊 AWS CLI，請參閱使用指南中的 使用 IAM 使用者登入資料進行驗證。AWS Command Line Interface 對於 AWS SDK 和工具，請參閱 AWS SDK 和工具參考指南中的 使用長期憑據進行身份驗證。 如需 AWS API，請參閱 IAM 使用者指南中的管理 IAM 使用者的存取金鑰。

以下範例會建立停用密碼的使用者。

```
create user temp_creds_user password disable;
```

以下範例會停用現有使用者的密碼。


```
alter user temp_creds_user password disable;
```

3. 使用 [CREATE GROUP](#) 建立資料庫使用者群組。
4. 使用 [GRANT](#) 命令定義群組的存取權限。

步驟 5：設定 JDBC 或 ODBC 連線使用 IAM 登入資料

您可以使用 Amazon Redshift JDBC 或 ODBC 驅動程序設定您的 SQL 用戶端。此驅動程式會管理建立資料庫使用者憑證，然後在 SQL 用戶端與 Amazon Redshift 資料庫之間建立連線的程序。

如果您使用身分提供者進行身分驗證，請指定登入資料供應商外掛程式的名稱。Amazon Redshift JDBC 和 ODBC 驅動程式包含下列以 SAML 為基礎之身分提供者的外掛程式：

- Active Directory Federation Services (AD FS)
- PingOne
- Okta
- Microsoft Azure AD

如需將 Microsoft Azure AD 設定為身分提供者的步驟，請參閱 [設定 JDBC 或 ODBC 單一登入身分驗證搭配 Microsoft Azure AD](#)。

設定 JDBC 連線使用 IAM 登入資料

1. 從 [設定 Amazon Redshift JDBC 驅動程式 2.1 版的連線](#) 頁面下載最新的 Amazon Redshift JDBC 驅動程式。
2. 使用下列其中一種格式的 IAM 登入資料選項建立 JDBC URL。若要使用 IAM 身分驗證，請將 iam: 新增至 Amazon Redshift JDBC URL 的 jdbc:redshift: 後方，如下列範例所示。

```
jdbc:redshift:iam://
```

新增 cluster-name、region 和 account-id。JDBC 驅動程式會使用您的 IAM 帳戶資訊和叢集名稱來擷取叢集 ID 和 AWS 區域。若要這樣做，您的使用者或角色必須具備為指定叢集呼叫 redshift:DescribeClusters 操作的許可。如果您的使用者或角色沒有呼叫 redshift:DescribeClusters 作業的權限，請包含叢集 ID、AWS Region 和連接埠，如下列範例所示。連接埠號碼是選用的。

```
jdbc:redshift:iam://examplecluster.abc123xyz789.us-west-2.redshift.amazonaws.com:5439/dev
```

3. 新增 JDBC 選項，以提供 IAM 登入資料。您可使用不同的 JDBC 選項組合來提供 IAM 登入資料。如需詳細資訊，請參閱 [用於建立資料庫使用者登入資料的 JDBC 和 ODBC 選項](#)。

下面的 URL 指定 AccessKey ID 和 SecretAccessKey 用戶。

```
jdbc:redshift:iam://examplecluster:us-west-2/dev?AccessKeyID=AKIAIOSFODNN7EXAMPLE&SecretAccessKey=wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
```

以下範例指定包含 IAM 登入資料的命名設定檔。

```
jdbc:redshift:iam://examplecluster:us-west-2/dev?Profile=user2
```

4. 新增 JDBC 驅動程式用來呼叫 GetClusterCredentials API 操作的 JDBC 選項。如果您用程式設計的方式呼叫 GetClusterCredentials API 操作，請勿加入這些選項。

下列範例包含 JDBC GetClusterCredentials 選項。

```
jdbc:redshift:iam://examplecluster:us-west-2/dev?plugin_name=com.amazon.redshift.plugin.AzureCredentialsProvider&UID=user&PWD=password&idp_t
```

設定 ODBC 連線使用 IAM 登入資料

在以下程序中，您只能尋找設定 IAM 身分驗證的步驟。如需使用標準身分驗證 (使用資料庫使用者名稱和密碼) 的步驟，請參閱 [設定 ODBC 連線](#)。

1. 安裝並設定您的作業系統適用的 Amazon Redshift ODBC 驅動程式。如需詳細資訊，請參閱 [設定 ODBC 連線](#) 頁面。

Important

Amazon Redshift ODBC 驅動程式必須為 1.3.6.1000 版或更新版本。

2. 依照您作業系統適用的步驟，設定連線設定。

如需詳細資訊，請參閱下列其中一個項目：

- [在 Microsoft Windows 上安裝並設定 Amazon Redshift ODBC 驅動程式](#)
 - [使用 ODBC 驅動程式管理員來設定 Linux 和 macOS X 作業系統上的驅動程式](#)
3. 在 Microsoft Windows 作業系統中，存取 Amazon Redshift ODBC Driver DSN Setup 視窗。
- a. 在 Connection Settings (連線設定) 下，輸入下列資訊：
- Data Source Name (資料來源名稱)
 - Server (伺服器) (選用)
 - Port (連接埠) (選用)
 - 資料庫

如果您的使用者或角色具有呼叫 `redshift:DescribeClusters` 操作的許可，則只需要資料來源名稱和資料庫。Amazon Redshift 使用 `ClusterId` 和區域通過調用 `DescribeCluster` 操作來獲取服務器和端口。

如果您的使用者或角色不具有呼叫 `redshift:DescribeClusters` 操作的許可，請指定伺服器 and 連接埠。

- b. 在 Authentication (身分驗證) 下方，選擇 Auth Type (驗證類型) 的值。

針對每個驗證類型，輸入下列的值：

AWS 設定檔

輸入下列資訊：

- ClusterID (ClusterID)
- 區域
- Profile name (設定檔名稱)

在包含 ODBC 連線選項值的 AWS 組態檔中輸入設定檔的名稱。如需詳細資訊，請參閱 [使用組態設定檔](#)。

(選用) 提供 ODBC 驅動程式用來呼叫 `GetClusterCredentials` API 操作之選項的詳細資訊：

- DbUser
- 使用者 AutoCreate
- DbGroups

如需詳細資訊，請參閱 [用於建立資料庫使用者登入資料的 JDBC 和 ODBC 選項](#)。

IAM 登入資料

輸入下列資訊：

- ClusterID (ClusterID)
- 區域
- AccessKey 身份證和 SecretAccessKey

IAM 資料庫身分驗證所設定之 IAM 角色或使用者的存取金鑰 ID 和私密存取金鑰。

- SessionToken

SessionToken 具有臨時登入資料的 IAM 角色是必需的。如需詳細資訊，請參閱 [暫時性安全登入資料](#)。

提供 ODBC 驅動程式用來呼叫 GetClusterCredentials API 操作之選項的詳細資訊：

- DbUser(必填)
- 使用者 AutoCreate (選擇性)
- DbGroups (可選)

如需詳細資訊，請參閱 [用於建立資料庫使用者登入資料的 JDBC 和 ODBC 選項](#)。

身分提供者：AD FS

針對使用 AD FS 的 Windows 整合式身分驗證，請讓 User (使用者) 和 Password (密碼) 保持空白。

提供 IdP 詳細資訊：

- IdP Host (IdP 主機)

企業身分提供商主機的名稱。該名稱不得包含任何斜線 (/)。

- IdP Port (IdP 連接埠) (選用)

身分提供者使用的連接埠。預設為 443。

- Preferred Role (偏好的角色)

IAM 角色的 Amazon Resource Name (ARN)，來自 SAML 聲明中 Role 屬性的多值 AttributeValue 元素。若要尋找偏好角色適用的值，請洽詢 IdP 管理員。如需詳細資訊，請參閱 [設定 IdP 的 SAML 聲明](#)。

(選用) 提供 ODBC 驅動程式用來呼叫 GetClusterCredentials API 操作之選項的詳細資訊：

- DbUser
- 使用者 AutoCreate
- DbGroups

如需詳細資訊，請參閱 [用於建立資料庫使用者登入資料的 JDBC 和 ODBC 選項](#)。

身份提供者：PingFederate

針對 User (使用者) 和 Password (密碼)，輸入 IdP 的使用者名稱和密碼。

提供 IdP 詳細資訊：

- IdP Host (IdP 主機)

企業身分提供商主機的名稱。該名稱不得包含任何斜線 (/)。

- IdP Port (IdP 連接埠) (選用)

身分提供者使用的連接埠。預設為 443。

- Preferred Role (偏好的角色)

IAM 角色的 Amazon Resource Name (ARN)，來自 SAML 聲明中 Role 屬性的多值 AttributeValue 元素。若要尋找偏好角色適用的值，請洽詢 IdP 管理員。如需詳細資訊，請參閱 [設定 IdP 的 SAML 聲明](#)。

(選用) 提供 ODBC 驅動程式用來呼叫 GetClusterCredentials API 操作之選項的詳細資訊：

- DbUser
- 使用者 AutoCreate
- DbGroups

如需詳細資訊，請參閱 [用於建立資料庫使用者登入資料的 JDBC 和 ODBC 選項](#)。

身分提供者：Okta

針對 User (使用者) 和 Password (密碼)，輸入 IdP 的使用者名稱和密碼。

提供 IdP 詳細資訊：

- IdP Host (IdP 主機)

企業身分提供商主機的名稱。該名稱不得包含任何斜線 (/)。

- IdP Port (IdP 連接埠)

Okta 不會使用此值。

- Preferred Role (偏好的角色)

IAM 角色的 Amazon Resource Name (ARN)，來自 SAML 聲明中 Role 屬性的 AttributeValue 元素。若要尋找偏好角色適用的值，請洽詢 IdP 管理員。如需詳細資訊，請參閱 [設定 IdP 的 SAML 聲明](#)。

- Okta App ID (Okta 應用程式 ID)

Okta 應用程式的 ID。Okta 應用程式嵌入連結中「amazon_aws」後方的 App ID 值。請洽詢 IdP 管理員，以取得此值。

(選用) 提供 ODBC 驅動程式用來呼叫 GetClusterCredentials API 操作之選項的詳細資訊：

- DbUser
- 使用者 AutoCreate
- DbGroups

如需詳細資訊，請參閱 [用於建立資料庫使用者登入資料的 JDBC 和 ODBC 選項](#)。

身分提供者：Azure AD

針對 User (使用者) 和 Password (密碼)，輸入 IdP 的使用者名稱和密碼。

針對叢集 ID 和區域，輸入您的 Amazon Redshift 叢集的叢集 ID 和 AWS 區域。

針對資料庫，輸入您為 Amazon Redshift 叢集建立的資料庫。

提供 IdP 詳細資訊：

- IdP Tenant (IdP 租用戶)

用於 Azure AD 的租用戶。

- Azure Client Secret (Azure 用戶端密碼)

Azure 中 Amazon Redshift 企業應用程式的用戶端密碼。

- Azure Client ID (Azure 用戶端 ID)

Azure 中 Amazon Redshift 企業應用程式的用戶端 ID (應用程式 ID)。

(選用) 提供 ODBC 驅動程式用來呼叫 GetClusterCredentials API 操作之選項的詳細資訊：

- DbUser
- 使用者 AutoCreate
- DbGroups

如需詳細資訊，請參閱 [用於建立資料庫使用者登入資料的 JDBC 和 ODBC 選項](#)。

提供 IAM 登入資料的選項

若要提供 JDBC 或 ODBC 連線的 IAM 登入資料，請選擇下列選項之一。

- AWS profile

做為以 JDBC 或 ODBC 設定形式提供登入資料值的替代方案，您可將值放入命名設定檔。如需詳細資訊，請參閱 [使用組態設定檔](#)。

- IAM 登入資料

以 JDBC 或 ODBC 設定的形式，SessionToken 選擇性地提供 AccessKey ID、和的值。SecretAccessKey SessionToken 只有具有臨時登入資料的 IAM 角色才需要。如需詳細資訊，請參閱 [提供 IAM 登入資料的 JDBC 和 ODBC 選項](#)。

- 身分提供者聯合

當您使用身分提供者聯合，讓來自身分提供者的使用者向 Amazon Redshift 進行驗證時，請指定憑證供應商外掛程式的名稱。如需詳細資訊，請參閱 [使用登入資料供應商外掛程式](#)。

Amazon Redshift JDBC 和 ODBC 驅動程式包含下列以 SAML 為基礎之聯合身分憑證供應商的外掛程式：

- Microsoft Active Identity Federation Services (AD FS)
- PingOne
- Okta
- Microsoft Azure Active Directory (Azure AD)

您可用 JDBC 或 ODBC 設定形式或使用設定檔提供外掛程式名稱和相關值。如需詳細資訊，請參閱 [JDBC 驅動程式 2.1 版組態的選項](#) 及 [設定 ODBC 驅動程式選項](#)。

如需詳細資訊，請參閱 [設定 JDBC 或 ODBC 連線使用 IAM 登入資料](#)。

使用組態設定檔

您可以提供 IAM 登入資料選項和 GetClusterCredentials 選項，做為設定檔中具名設定檔中的 AWS 設定。若要提供設定檔名稱，請使用設定檔 JDBC 選項。組態儲存於主目錄內名為 `.aws` 之資料夾中名為 `config` 的檔案或名為 `credentials` 的檔案中。

針對具有 Amazon Redshift JDBC 或 ODBC 驅動程式之以 SAM 為基礎的憑證供應商外掛程式，您可以使用先前在 [使用登入資料供應商外掛程式](#) 中所述的設定。如果 `plugin_name` 未使用，則會忽略其他選項。

下列範例顯示具有兩個設定檔的 `~/.aws/credentials` 檔案：

```
[default]
aws_access_key_id=AKIAIOSFODNN7EXAMPLE
aws_secret_access_key=wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY

[user2]
aws_access_key_id=AKIAI44QH8DHBEXAMPLE
aws_secret_access_key=je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY
session_token=AQoDYXdzEPT/////////
wEXAMPLEtc764bNrC9SAPBSM22wD0k4x4HIZ8j4FZTWdQWLwsKWHGBuFqwAeMicRXmxfpSPfIeoIYRqTf1fKD8YUuwthAx7
qkPpKPi/kMcGd
QrmGdeehM4IC1NtBmUpp2wUE8phUZampKsburEDy0KPkyQDYwT7WZ0wq5V5XDvp75YU
9HFv1Rd8Tx6q6fE8YQcHNvXAKiY9q6d+xo0rKwT38xVqr7ZD0u0iPPkUL64lIZbqBAz
+scqKmlzm8FDrypNC9Yjc8fP0Ln9FX9KSYvKTr4rvx3iS1lTJabIQwj2ICCR/oLxBA==
```


若要使用 user2 範例的登入資料，請在 JDBC URL 中指定 Profile=user2。

如需有關使用設定檔的詳細資訊，請參閱使 AWS Command Line Interface 用指南中的[組態和認證檔案設定](#)。

如需為 JDBC 驅動程式使用設定檔的相關資訊，請參閱[指定設定檔](#)。

如需為 ODBC 驅動程式使用設定檔的相關資訊，請參閱[設定身分驗證](#)。

提供 IAM 登入資料的 JDBC 和 ODBC 選項

下表列出提供 IAM 登入資料的 JDBC 和 ODBC 選項。

選項	描述
Iam	僅使用於 ODBC 連線字串。設為 1 以使用 IAM 身分驗證。
AccessKey ID	針對 IAM 資料庫身份驗證設定的 IAM 角色或使用者的存取金鑰 ID 和秘密存取金鑰。SessionToken 只有具有臨時登入資料的 IAM 角色才需要。SessionToken 不適用於使用者。如需詳細資訊，請參閱 暫時性安全登入資料 。
SecretAccessKey	
SessionToken	
plugin_name	實作登入資料供應商之類別的完全合格名稱。Amazon Redshift JDBC 驅動程式包含以 SAML 為基礎的憑證供應商外掛程式。如果您提供 plugin_name，您也可以提供其他相關選項。如需詳細資訊，請參閱 使用登入資料供應商外掛程式 。
Profile	AWS 證明資料或組態檔中的設定檔名稱，其中包含 JDBC 連線選項的值。如需詳細資訊，請參閱 使用組態設定檔 。

使用登入資料供應商外掛程式

Amazon Redshift 使用憑證供應商外掛程式進行單一登入身分驗證。

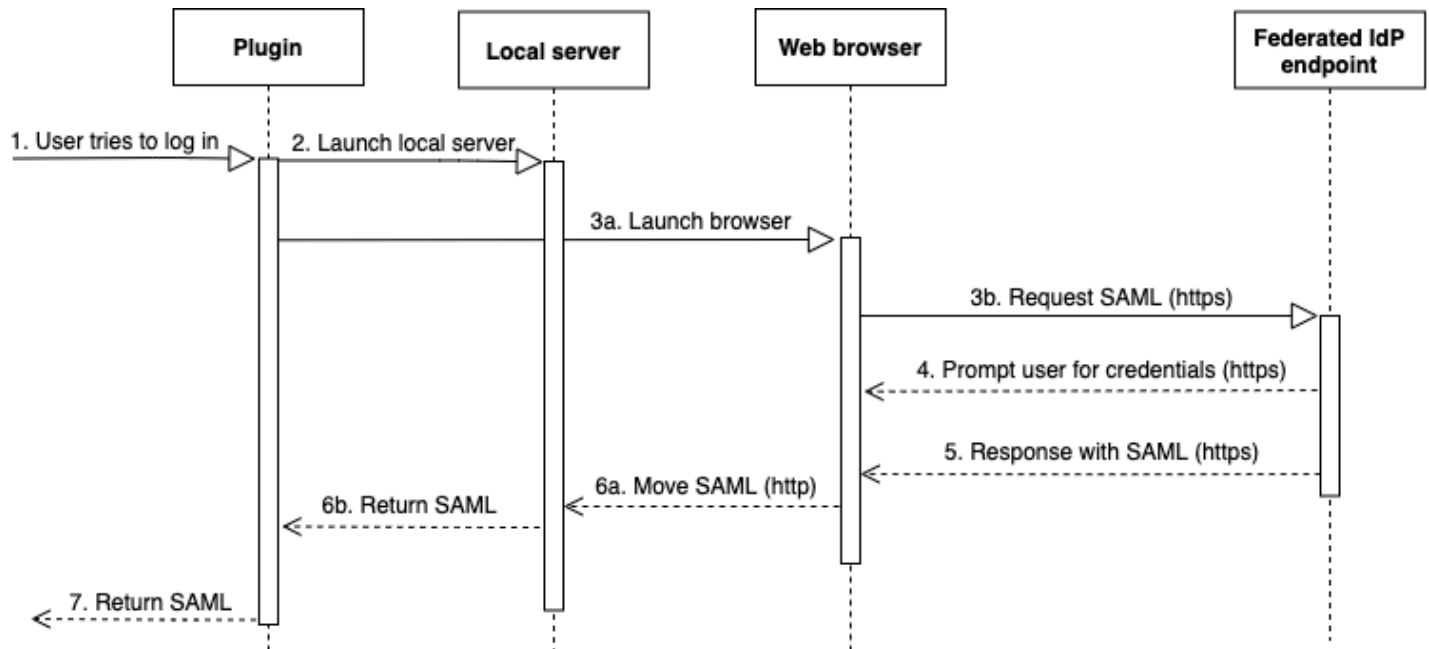
為了支援單一登入身分驗證，Amazon Redshift 提供適用於 Microsoft Azure Active Directory 的 Azure AD 外掛程式。如需如何設定此外掛程式的資訊，請參閱[設定 JDBC 或 ODBC 單一登入身分驗證搭配 Microsoft Azure AD](#)。

設定多重因素認證

設定多重因素認證

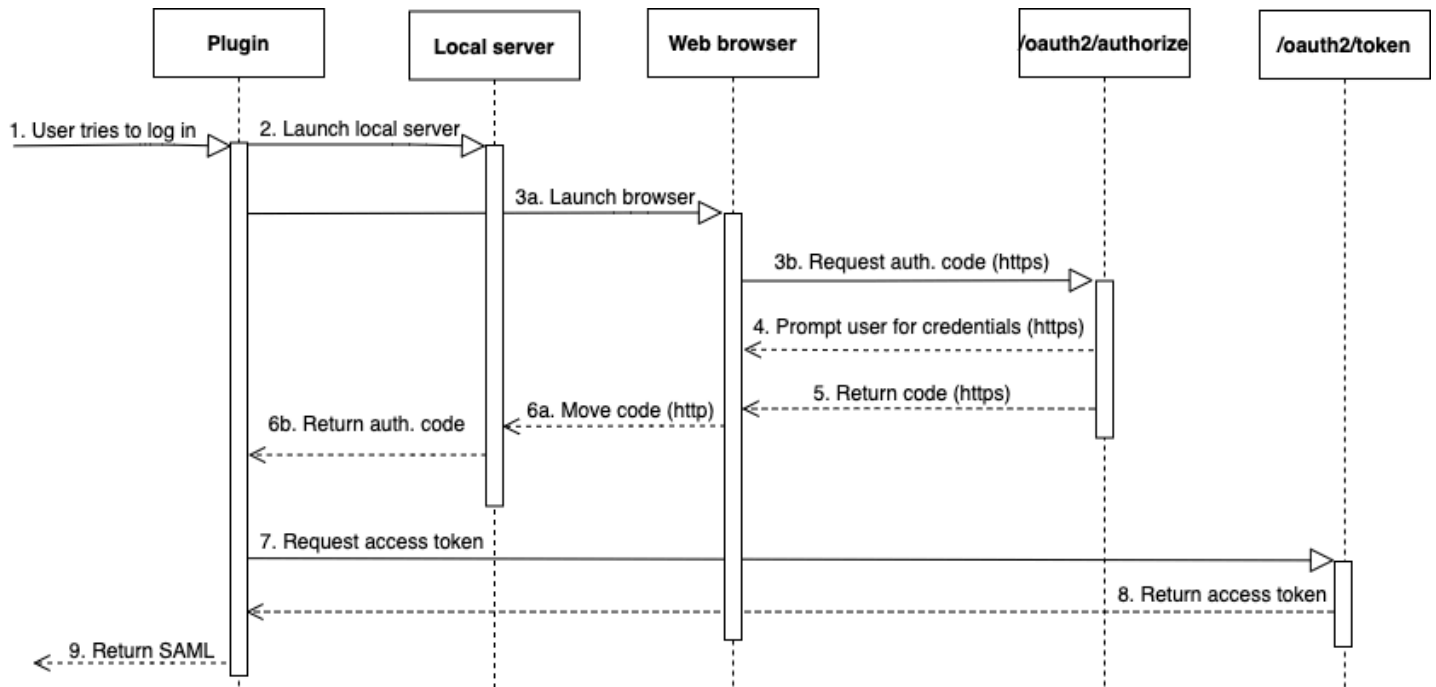
為了支援多重要素驗證 (MFA)，Amazon Redshift 提供瀏覽器型的外掛程式。使用瀏覽器 SAML 外掛程式確認 PingOne, 和瀏覽器 Azure AD 外掛程式 Microsoft Azure 活動目錄。

使用瀏覽器 SAML 外掛程式時，SAML 身分驗證的流程如下：



1. 使用者嘗試登入。
2. 外掛程式會啟動本機伺服器來接聽 localhost 上的傳入連線。
3. 外掛程式會啟動 web 瀏覽器，從指定的單一登入 URL 聯合身分識別供應商端點透過 HTTPS 請求 SAML 回應。
4. web 瀏覽器會遵循連結，並提示使用者輸入登入資料。
5. 在使用者驗證並授予同意後，聯合身分提供者端點會透過 HTTPS 將 SAML 回應傳回由 `redirect_uri` 指定的 URI。
6. web 瀏覽器會將回應訊息與 SAML 回應移至指定的 `redirect_uri`。
7. 本機伺服器會接受傳入的連線，而外掛程式會擷取 SAML 回應並將其傳遞給 Amazon Redshift。

使用瀏覽器 Azure AD 外掛程式時，SAML 身分驗證的流程如下：



1. 使用者嘗試登入。
2. 外掛程式會啟動本機伺服器來接聽 localhost 上的傳入連線。
3. 外掛程式會啟動 web 瀏覽器，以從 Azure AD `oauth2/authorize` 端點請求授權碼。
4. web 瀏覽器會透過 HTTPS 遵循所產生的連結，並提示使用者輸入登入資料。連結是使用組態屬性 (例如租用戶和 `client_id`) 所產生的。
5. 在使用者進行驗證並授予同意後，Azure AD `oauth2/authorize` 端點會傳回，並透過 HTTPS 將包含授權碼的回應傳送至指定 `redirect_uri`。
6. web 瀏覽器會將回應訊息與 SAML 回應移至指定的 `redirect_uri`。
7. 本機伺服器會接受傳入的連線和外掛程式請求並擷取授權碼，然後將 POST 請求傳送至 Azure AD `oauth2/token` 端點。
8. Azure AD `oauth2/token` 端點會將包含存取權杖的回應傳回指定 `redirect_uri`。
9. 外掛程式會擷取 SAML 回應並將其傳遞給 Amazon Redshift。

請參閱以下章節：

- Active Directory Federation Services (AD FS)

如需詳細資訊，請參閱 [設定 JDBC 或 ODBC 單一登入身分驗證搭配 AD FS。](#)

- PingOne (坪)

只有使用表單驗證的預先決定的 PingOne IdP 轉接器才支援 Ping。

如需詳細資訊，請參閱 [設定 JDBC 或 ODBC 單一登入身分驗證搭配 Ping Identity](#)。

- Okta

Okta 只有在使用 Okta 提供用於 AWS Management Console 的應用程式時受到支援。

如需詳細資訊，請參閱 [設定 JDBC 或 ODBC 單一登入身分驗證搭配 Okta](#)。

- Microsoft Azure Active Directory

如需詳細資訊，請參閱 [設定 JDBC 或 ODBC 單一登入身分驗證搭配 Microsoft Azure AD](#)。

設定外掛程式選項

設定外掛程式選項

若要使用以 SAML 為基礎的憑證供應商外掛程式，請使用 JDBC 或 ODBC 選項或在命名設定檔中指定下列選項。如果未指定 `plugin_name`，則會忽略其他選項。

選項	描述
<code>plugin_name</code>	<p>針對 JDBC，為實作登入資料供應商的類別名稱。請指定下列其中一項：</p> <ul style="list-style-type: none"> • 針對 Active Directory Federation Services <div style="border: 1px solid #ccc; border-radius: 10px; padding: 5px; margin: 5px 0;"><code>com.amazon.redshift.plugin.AdfsCredentialsProvider</code></div> • 針對 Okta <div style="border: 1px solid #ccc; border-radius: 10px; padding: 5px; margin: 5px 0;"><code>com.amazon.redshift.plugin.OktaCredentialsProvider</code></div> • 對於 PingFederate <div style="border: 1px solid #ccc; border-radius: 10px; padding: 5px; margin: 5px 0;"><code>com.amazon.redshift.plugin.PingCredentialsProvider</code></div> • 針對 Microsoft Azure Active Directory <div style="border: 1px solid #ccc; border-radius: 10px; padding: 5px; margin: 5px 0;"><code>com.amazon.redshift.plugin.AzureCredentialsProvider</code></div> • 針對 SAML MFA

選項	描述
	<pre>com.amazon.redshift.plugin.BrowserSamlCredentialsProvider</pre> <ul style="list-style-type: none"> 針對 Microsoft Azure Active Directory 單一登入與 MFA <pre>com.amazon.redshift.plugin.BrowserAzureCredentialsProvider</pre> <p>針對 ODBC，請指定下列其中一項：</p> <ul style="list-style-type: none"> 針對 Active Directory Federation Services：adfs 針對 Okta：okta 對於 PingFederate：ping 針對 Microsoft Azure Active Directory：azure 針對 SAML MFA：browser saml 針對 Microsoft Azure Active Directory 單一登入與 MFA：browser azure ad
idp_host	企業身分提供商主機的名稱。該名稱不得包含任何斜線（「/」）。針對 Okta 身分提供者，idp_host 的值應以 .okta.com 結尾。
idp_port	身分提供者使用的連接埠。預設為 443。Okta 會忽略此連接埠。
preferred_role	Amazon Resource Name (ARN) 角色，來自 SAML 聲明中 Role 屬性的 Attribute Value 元素。若要尋找偏好角色適用的值，請洽詢 IdP 管理員。如需詳細資訊，請參閱 設定 IdP 的 SAML 聲明 。
user	企業使用者名稱，包括網域 (如適用)。例如，在 Active Directory 中，網域名稱為必填，使用格式為網域\使用者名稱。
密碼	企業使用者的密碼。我們建議不要使用此選項。請改用 SQL 用戶端提供密碼。
app_id	Okta 應用程式的 ID。僅搭配 Okta 使用。Okta 應用程式嵌入連結中 app_id 後方的 amazon_aws 值。若要取得此值，請洽詢 IdP 管理員。以下為應用程式嵌入連結的範例： <code>https://example.okta.com/home/amazon_aws/0oa2hylwrpM8UGehd1t7/272</code>

選項	描述
idp_tenant	用於 Azure AD 的租用戶。僅搭配 Azure 使用。
client_id	Azure AD 中 Amazon Redshift 企業應用程式的用戶端 ID。僅搭配 Azure 使用。

設定 JDBC 或 ODBC 單一登入身分驗證搭配 Microsoft Azure AD

您可以使用 Microsoft Azure AD 作為身分提供者 (IdP) 來存取您的 Amazon Redshift 叢集。接著，您可以尋找描述如何就此目的設定信任關係的程序。如需 [有關設定 AWS 為 IdP 服務提供者的詳細資訊](#)，請參閱「IAM 使用者指南」中的「[使用信賴方信任設定 SAML 2.0 IdP](#)」和「[新增宣告](#)」。

Note

若要使用 Azure AD 搭配 JDBC，Amazon Redshift JDBC 驅動程式必須為 1.2.37.1061 版或更新版本。若要使用 Azure AD 搭配 ODBC，Amazon Redshift ODBC 驅動程式必須為 1.4.10.1000 版或更新版本。

觀看以下影片，了解如何搭配 Microsoft Azure AD 單一登入來聯合 Amazon Redshift 存取：[搭配 Microsoft Azure AD 單一登入來聯合 Amazon Redshift 存取](#)。

若要將 Azure AD 和您的 AWS 帳戶設定為彼此信任

1. 建立或使用現有的 Amazon Redshift 叢集，以供 Azure AD 使用者連線。若要設定連線，則需要此叢集的特定屬性，例如叢集識別碼。如需詳細資訊，請參閱[建立叢集](#)。
2. 設置 Azure 活動目錄，組，用於 Microsoft Azure 門戶網站 AWS 上的用戶。
3. 在 Microsoft Azure 入口網站上將 Amazon Redshift 新增為企業應用程式，以使用於單一登入 AWS 主控台，以及聯合登入 Amazon Redshift。選擇 Enterprise application (企業應用程式)。
4. 選擇 +New application (新增應用程式)。新增應用程式頁面隨即顯示。
5. 在搜尋欄位中搜尋 **AWS**。
6. 選擇 Amazon Web Services (AWS)，然後選擇新增。這將創建 AWS 應用程序。
7. 在 Manage (管理) 下方，選擇 Single sign-on (單一登入)。
8. 選擇 SAML。Amazon Web Services (AWS) | 以 SAML 為基礎的登入頁面隨即顯示。

9. 選擇 Yes (是)，繼續進行「使用 SAML 頁面設定單一登入」。此頁面會顯示預先設定的單一登入相關屬性清單。
10. 在 Basic SAML Configuration (基本 SAML 組態) 中，選擇編輯圖示並選擇 Save (儲存)。
11. 設定超過一個應用程式時，請提供識別碼值。例如，輸入 ***https://signin.aws.amazon.com/saml#2***。請注意，從第二個應用程式開始，請使用此格式搭配 # 符號來指定唯一的 SPN 值。
12. 在 User Attributes and Claims (使用者屬性和宣告) 區段中選擇編輯圖示。

根據預設，會預先設定唯一使用者識別碼 (UID) RoleSessionName、角色和 SessionDuration 宣告。

13. 選擇 + Add new claim (新增宣告) 來新增資料庫使用者的宣告。

針對名稱，輸入 **DbUser**。

針對 Namespace (命名空間)，輸入 ***https://redshift.amazon.com/SAML/Attributes***。

針對 Source (來源)，選擇 Attribute (屬性)。

針對 Source attribute (來源屬性)，選擇 `user.userprincipalname`。然後選擇 Save (儲存)。

14. 選擇 [+ 新增聲明] 以新增索賠 AutoCreate。

針對名稱，輸入 **AutoCreate**。

針對 Namespace (命名空間)，輸入 ***https://redshift.amazon.com/SAML/Attributes***。

針對 Source (來源)，選擇 Attribute (屬性)。

針對 Source attribute (來源屬性)，選擇 "true"。然後選擇 Save (儲存)。

在此，***123456789012*** 是您的 AWS 帳戶，***AzureSSO*** 是您建立的 IAM 角色，而 ***AzureADProvider*** 是 IAM 提供者。

宣告名稱	Value
唯一使用者識別碼 (名稱 ID)	<code>user.userprincipalname</code>
<code>https://aws.amazon.com/SAML/Attributes/SessionDuration</code>	"900"

宣告名稱	Value
https://aws.amazon.com/SAML/Attributes/Role	arn:aws:iam:: <i>123456789012</i> :role/ <i>AzureSSO</i> ,arn:aws:iam:: <i>123456789012</i> :saml-provider/ <i>AzureADProvider</i>
https://aws.amazon.com/SAML/Attributes/RoleSessionName	user.userprincipalname
https://redshift.amazon.com/SAML/Attributes/AutoCreate	"true"
https://redshift.amazon.com/SAML/Attributes/DbGroups	user.assignedroles
https://redshift.amazon.com/SAML/Attributes/DbUser	user.userprincipalname

- 在 App Registration (應用程式註冊) > ***your-application-name*** > Authentication (身分驗證) 下方，新增 Mobile And Desktop Application (行動和桌面應用程式)。將 URL 指定為 http://localhost/redshift。
- 在 SAML Signing Certificate (SAML 簽署憑證) 區段中，選擇 Download (下載) 以下載並儲存聯合中繼資料 XML 檔案，以便在建立 IAM SAML 身分提供者時使用。此檔案用於建立單一登入聯合身分。
- 在 IAM 主控台上建立 IAM SAML 身分提供者。您所提供的中繼資料文件，是您在設定 Azure 企業應用程式時儲存的聯合中繼資料 XML 檔案。如需詳細步驟，請參閱《IAM 使用者指南》中的[建立和管理 IAM 身分提供者 \(主控台\)](#)。
- 在 IAM 主控台上建立 SAML 2.0 聯合的 IAM 角色。如需詳細步驟，請參閱《IAM 使用者指南》中的[為 SAML 建立角色](#)。
- 建立 IAM 政策，您可將其附加至您在 IAM 主控台上為 SAML 2.0 聯合建立的 IAM 角色。如需詳細步驟，請參閱《IAM 使用者指南》中的[建立 IAM 政策 \(主控台\)](#)。

為您的環境修改下列政策 (JSON 格式)：

- 以叢集的 AWS 區域取代 *us-west-1*。
- 將您的 AWS 帳戶替換為 *123456789012*。
- 以您的叢集識別碼 (或 * 代表所有叢集) 代替 *cluster-identifier*。

- 以您的資料庫 (或 * 代表所有資料庫) 代替 *dev*。
- 以 IAM 角色的唯一識別碼代替 *AROAJ2UCCR6DPCEXAMPLE*。
- 以您的租用戶或公司電子郵件網域代替 *example.com*。
- 以您計劃為其指派使用者的資料庫群組代替 *my_dbgroup*。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "redshift:GetClusterCredentials",
      "Resource": [
        "arn:aws:redshift:us-west-1:123456789012:dbname:cluster-identifier/dev",
        "arn:aws:redshift:us-west-1:123456789012:dbuser:cluster-identifier/  
${redshift:DbUser}",
        "arn:aws:redshift:us-west-1:123456789012:cluster:cluster-identifier"
      ],
      "Condition": {
        "StringEquals": {
          "aws:userid": "AROAJ2UCCR6DPCEXAMPLE:  
${redshift:DbUser}@example.com"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "redshift:CreateClusterUser",
      "Resource": "arn:aws:redshift:us-west-1:123456789012:dbuser:cluster-identifier/  
${redshift:DbUser}"
    },
    {
      "Effect": "Allow",
      "Action": "redshift:JoinGroup",
      "Resource": "arn:aws:redshift:us-west-1:123456789012:dbgroup:cluster-identifier/  
my_dbgroup"
    },
    {
      "Effect": "Allow",
      "Action": [
```

```
        "redshift:DescribeClusters",
        "iam:ListRoles"
    ],
    "Resource": "*"
}
]
```

此政策會授與許可，如下所示：

- 第一個區段會授與 GetClusterCredentials API 操作的許可，以取得所指定叢集的暫時性登入資料。在此範例中，資源是 *cluster-identifier*，其具有資料庫 *dev*、位於帳戶 *123456789012*、並位於 AWS 區域 *us-west-1*。\${redshift:DbUser} 子句只允許符合 Azure AD 中指定 DbUser 值的使用者連線。
- 條件子句會強制只有特定使用者會取得臨時登入資料。這些是依據貴公司電子郵件網域中的電子郵件地址所識別的 IAM 帳戶中，具備角色唯一 ID *AR0AJ2UCCR6DPCEXAMPLE* 所指定角色的使用者。如需唯一 ID 的相關資訊，請參閱《IAM 使用者指南》中的[唯一 ID](#)。

您所設定的 IdP (在此案例中為 Azure AD) 會決定條件子句的撰寫方式。如果您的員工電子郵件是 johndoe@example.com，請先將 \${redshift:DbUser} 設定為符合員工使用者名稱 johndoe 的超級欄位。然後將 AWS SAML RoleSessionName 欄位設定為符合員工電子郵件 johndoe@example.com 的超級欄位，讓此條件發揮作用。當您採取這種方法時，請考慮下列事項：

- 如果您將 \${redshift:DbUser} 設定為員工的電子郵件，然後移除範例 JSON 中符合 RoleSessionName 的 @example.com。
- 如果您將 RoleSessionId 設定為員工的使用者名稱，然後移除範例中符合 RoleSessionName 的 @example.com。
- 在範例 JSON 中，\${redshift:DbUser} 和 RoleSessionName 均設定為員工的電子郵件。此範例 JSON 會使用 Amazon Redshift 資料庫使用者名稱搭配 @example.com，讓使用者登入以存取叢集。
- 第二個區段會授與許可，以在指定的叢集中建立 dbuser 名稱。在此範例 JSON 中，其會將建立限制於 \${redshift:DbUser}。
- 第三個區段會授與許可，以指定使用者可以加入的 dbgroup。在此範例 JSON 中，使用者可以加入指定叢集中的 my_dbgroup 群組。
- 第四個區段會授予使用者可對所有資源執行動作的許可。在此範例 JSON 中，它可讓使用者呼叫 redshift:DescribeClusters 以取得叢集資訊，例如叢集端點、AWS 區域和連接埠。此外，還可允許使用者呼叫 iam:ListRoles，以檢查使用者可以擔任哪些角色。

設定 JDBC 以對 Microsoft Azure AD 進行身分驗證

- 將資料庫用戶端設定為使用 Azure AD 單一登入，透過 JDBC 連線到您的叢集。

您可使用任何採用 JDBC 驅動程式的用戶端使用 Azure AD 單一登入進行連線，或使用 Java 之類的語言透過指令碼進行連線。如需安裝和組態資訊，請參閱 [設定 Amazon Redshift JDBC 驅動程式 2.1 版的連線](#)。

例如，您可以使用 SQLWorkbench/J 作為用戶端。當您設定 SQLWorkbench /J 時，您的資料庫 URL 會使用下列格式。

```
jdbc:redshift:iam://cluster-identifier:us-west-1/dev
```

如果您使用 SQLWorkbench /J 作為用戶端，請執行下列步驟：

- 啟動 SQL Workbench/J。在選取連線設定檔頁面上，新增名為 **AzureAuth** 的設定檔群組。
- 針對 Connection Profile (連線設定檔)，輸入 **Azure**。
- 選擇 Manage Drivers (管理驅動程式)，然後選擇 Amazon Redshift。選擇程式庫旁邊的開啟資料夾圖示，然後選擇適當的 JDBC .jar 檔案。
- 在 Select Connection Profile (選取連線設定檔) 頁面上，將資訊新增至連線設定檔，如下所示：
 - 針對 User (使用者)，輸入您的 Microsoft Azure 使用者名稱。這是您用於單一登入之 Microsoft Azure 帳戶的使用者名稱，該帳戶具有您嘗試驗證之叢集的許可。
 - 針對 Password (密碼)，輸入您的 Microsoft Azure 密碼。
 - 針對 Drivers (驅動程式)，選擇 Amazon Redshift (com.amazon.redshift.jdbc.Driver)。
 - 針對 URL，輸入 **`jdbc:redshift:iam://your-cluster-identifier:your-cluster-region/your-database-name`**。
- 選擇 Extended Properties (擴充屬性) 以將其他資訊新增至連線屬性，如下所述。

針對 Azure AD 單一登入組態新增其他資訊，如下所示：

- 針對 plugin_name，輸入 **`com.amazon.redshift.plugin.AzureCredentialsProvider`**。此值會指定驅動程式使用 Azure AD 單一登入做為身分驗證方法。
- 針對 idp_tenant，輸入 **`your-idp-tenant`**。僅用於 Microsoft Azure AD。這是您在 Azure AD 上設定的公司租用戶名稱。此值可以是租用戶名稱或租用戶唯一 ID (含連字號)。

- 針對 `client_secret`，輸入 ***your-azure-redshift-application-client-secret***。僅用於 Microsoft Azure AD。這是您在設定 Azure 單一登入組態時所建立之 Amazon Redshift 應用程式的用戶端秘密。這僅適用於亞馬遜。AzureCredentialsProvider 插件。
- 針對 `client_id`，輸入 ***your-azure-redshift-application-client-id***。僅用於 Microsoft Azure AD。這是您在設定 Azure 單一登入組態時所建立之 Amazon Redshift 應用程式的用戶端 ID (含連字號)。

針對具有 MFA 的 Azure AD 單一登入組態，將其他資訊新增至連線屬性，如下所示：

- 針對 `plugin_name`，輸入 **`com.amazon.redshift.plugin.BrowserAzureCredentialsProvider`**。此值會指定驅動程式使用具有 MFA 的 Azure AD 單一登入做為身分驗證方法。
- 針對 `idp_tenant`，輸入 ***your-idp-tenant***。僅用於 Microsoft Azure AD。這是您在 Azure AD 上設定的公司租用戶名稱。此值可以是租用戶名稱或租用戶唯一 ID (含連字號)。
- 針對 `client_id`，輸入 ***your-azure-redshift-application-client-id***。此選項僅用於 Microsoft Azure AD。這是您在設定具有 MFA 的 Azure AD 單一登入組態時所建立之 Amazon Redshift 應用程式的用戶端 ID (含連字號)。
- 針對 `listen_port`，輸入 ***your-listen-port***。這是本機伺服器接聽的連接埠。預設值為 7890。
- 針對 `idp_response_timeout`，輸入 ***the-number-of-seconds***。這是 IdP 伺服器傳回回應時，在逾時之前等待的秒數。秒數的下限必須為 10。如果建立連線所花的時間超過此臨界值，連線會中止。

設定 ODBC 以對 Microsoft Azure AD 進行身分驗證

- 將資料庫用戶端設定為使用 Azure AD 單一登入，透過 ODBC 連線到您的叢集。

Amazon Redshift 會提供適用於 Linux、Windows 和 macOS 作業系統的 ODBC 驅動程式。安裝 ODBC 驅動程式之前，查明 SQL 用戶端工具是 32 位元或 64 位元。安裝符合 SQL 用戶端工具需求的 ODBC 驅動程式。

此外，為您的作業系統安裝和設定最新的 Amazon Redshift ODBC 驅動程式，如下所示：


- 若為 Windows，請參閱 [在 Microsoft Windows 上安裝並設定 Amazon Redshift ODBC 驅動程式](#)。
- 如需有關 macOS 的資訊，請參閱 [在 macOS X 上安裝 Amazon Redshift ODBC 驅動程式](#)。

- 若為 Linux，請參閱 [在 Linux 上安裝 Amazon Redshift ODBC 驅動程式](#)。

在 Windows 上，於 Amazon Redshift ODBC Driver DSN Setup (Amazon Redshift ODBC 驅動程式 DSN 設定) 頁面的 Connection Settings (連線設定) 之下，輸入下列資訊：

- 針對 Data source name (資料來源名稱)，輸入 ***your-DSN***。這會指定作為 ODBC 設定檔名稱的資料來源名稱。
- 針對 Azure AD 單一登入組態的驗證類型，請選擇 **Identity Provider: Azure AD**。這是 ODBC 驅動程式使用 Azure 單一登入來進行驗證的身分驗證方法。
- 針對具有 MFA 的 Azure AD 單一登入組態的驗證類型，請選擇 **Identity Provider: Browser Azure AD**。這是 ODBC 驅動程式使用具有 MFA 之 Azure 單一登入來進行驗證的身分驗證方法。
- 針對 Cluster ID (叢集 ID)，輸入 ***your-cluster-identifier***。
- 針對 Region (區域)，輸入 ***your-cluster-region***。
- 針對 Database (資料庫)，輸入 ***your-database-name***。
- 針對 User (使用者)，輸入 ***your-azure-username***。這是您用於單一登入之 Microsoft Azure 帳戶的使用者名稱，該帳戶具有您嘗試驗證之叢集的許可。僅在 Auth Type (驗證類型) 為 Identity Provider: Azure AD (身分提供者：Azure AD) 的情況下使用此項目。
- 針對 Password (密碼)，輸入 ***your-azure-password***。僅在 Auth Type (驗證類型) 為 Identity Provider: Azure AD (身分提供者：Azure AD) 的情況下使用此項目。
- 針對 IdP Tenant (IdP 租用戶)，輸入 ***your-idp-tenant***。這是您在 IdP (Azure) 上設定的公司租用戶名稱。此值可以是租用戶名稱或租用戶唯一 ID (含連字號)。
- 針對 Azure Client Secret (Azure 用戶端密碼)，輸入 ***your-azure-redshift-application-client-secret***。這是您在設定 Azure 單一登入組態時所建立之 Amazon Redshift 應用程式的用戶端秘密。
- 針對 Azure Client ID (Azure 用戶端 ID)，輸入 ***your-azure-redshift-application-client-id***。這是您在設定 Azure 單一登入組態時所建立之 Amazon Redshift 應用程式的用戶端 ID (含連字號)。
- 針對 Listen Port (接聽連接埠)，輸入 ***your-listen-port***。這是本機伺服器接聽的預設接聽連接埠。預設值為 7890。這僅適用於瀏覽器 Azure AD 外掛程式。
- 針對 Response Timeout (回應逾時)，輸入 ***the-number-of-seconds***。這是 IdP 伺服器傳回回應時，在逾時之前等待的秒數。秒數的下限必須為 10。如果建立連線所花的時間超過此臨界值，連線會中止。此選項僅適用於瀏覽器 Azure AD 外掛程式。

在 macOS 和 Linux 上，編輯 `odbc.ini` 檔案，如下所示：

 Note

所有項目都不區分大小寫。

- 針對 `clusterid`，輸入 ***your-cluster-identifier***。這是所建立 Amazon Redshift 叢集的名稱。
- 針對 `region` (區域)，輸入 ***your-cluster-region***。這是所建 AWS 立的 Amazon Redshift 叢集的區域。
- 針對 `database` (資料庫)，輸入 ***your-database-name***。這是您嘗試在 Amazon Redshift 叢集上存取的資料庫名稱。
- 針對 `locale`，輸入 ***en-us***。這是錯誤訊息的顯示語言。
- 針對 `iam`，輸入 ***1***。此值指定驅動程式使用 IAM 登入資料進行身分驗證。
- 如需 Azure AD 單一登入組態的 `plugin_name`，請輸入 ***AzureAD***。這會指定驅動程式使用 Azure 單一登入作為身分驗證方法。
- 如需具有 MFA 的 Azure AD 單一登入組態的 `plugin_name`，請輸入 ***BrowserAzureAD***。這會指定驅動程式使用具有 MFA 的 Azure 單一登入做為身分驗證方法。
- 針對 `uid`，輸入 ***your-azure-username***。這是您用於單一登入之 Microsoft Azure 帳戶的使用者名稱，該帳戶具有您嘗試驗證之叢集的許可。僅在 `plugin_name` 為 `AzureAD` 的情況下使用此項目。
- 針對 `pwd`，輸入 ***your-azure-password***。僅在 `plugin_name` 為 `AzureAD` 的情況下使用此項目。
- 針對 `idp_tenant`，輸入 ***your-idp-tenant***。這是您在 IdP (Azure) 上設定的公司租用戶名稱。此值可以是租用戶名稱或租用戶唯一 ID (含連字號)。
- 針對 `client_secret`，輸入 ***your-azure-redshift-application-client-secret***。這是您在設定 Azure 單一登入組態時所建立之 Amazon Redshift 應用程式的用戶端秘密。
- 針對 `client_id`，輸入 ***your-azure-redshift-application-client-id***。這是您在設定 Azure 單一登入組態時所建立之 Amazon Redshift 應用程式的用戶端 ID (含連字號)。
- 針對 `listen_port`，輸入 ***your-listen-port***。這是本機伺服器接聽的連接埠。預設值為 7890。這適用於瀏覽器 Azure AD 外掛程式。

- 針對 `idp_response_timeout`，輸入 ***the-number-of-seconds***。這是等待 Azure 回應的指定時間期間 (秒)。此選項適用於瀏覽器 Azure AD 外掛程式。

在 macOS 和 Linux 上，同時編輯設定檔設定以新增下列匯出：

```
export ODBCINI=/opt/amazon/redshift/Setup/odbc.ini
```

```
export ODBCINSTINI=/opt/amazon/redshift/Setup/odbcinst.ini
```

疑難排解瀏覽器 Azure AD 外掛程式的問題

1. 若要使用瀏覽器 Azure AD 外掛程式，您必須設定請求中指定的回覆 URL，以符合為您的應用程式設定的回覆 URL。

瀏覽至 Microsoft Azure 入口網站上的 Set up Single Sign-On with SAML (使用 SAML 設定單一登入) 頁面。然後檢查回覆網址 是否設定為 `http://localhost/redshift/`。

2. 如果您收到 IdP 租用戶錯誤，請確認 IdP 租用戶名稱與您最初用來設定 Microsoft Azure 中使用中目錄的網域名稱相符。

在 Windows 上，導覽至 Amazon Redshift ODBC DSN 設定頁面的連線設定區段。接著檢查您在 IdP (Azure) 上設定的公司租用戶名稱是否與您最初用來在 Microsoft Azure 中設定使用中目錄的網域名稱相符。

在 macOS 和 Linux 上，找到這個 `odbc.ini` 檔案。接著檢查您在 IdP (Azure) 上設定的公司租用戶名稱是否與您最初用來在 Microsoft Azure 中設定使用中目錄的網域名稱相符。

3. 如果您收到請求中指定的回覆 URL 與為應用程式設定的回覆 URL 不相符的錯誤，請確認重新導向 URI 與回覆 URL 相同。

瀏覽至 Microsoft Azure 入口網站上應用程式的 App registration (應用程式註冊) 頁面。然後檢查重新導向 URI 與回覆 URL 是否相符。

4. 如果您收到未經授權的回應：未經授權的錯誤，請確認您已完成行動裝置和桌面應用程式組態。

瀏覽至 Microsoft Azure 入口網站上應用程式的 App registration (應用程式註冊) 頁面。然後瀏覽至 Authentication (驗證)，並檢查您已將行動裝置和桌面應用程式設定為使用 `http://localhost/redshift/` 做為重新導向 URI。

設定 JDBC 或 ODBC 單一登入身分驗證搭配 AD FS

您可以使用 AD FS 做為身分提供者 (IdP) 來存取您的 Amazon Redshift 叢集。接著，您可以尋找描述如何就此目的設定信任關係的程序。如需有關設定 AWS 為 AD FS 服務提供者的詳細資訊，請參閱「IAM 使用者指南」中的「[使用信賴方信任設定 SAML 2.0 IdP](#)」和「[新增宣告](#)」。

若要設定 AD FS 和您的 AWS 帳戶互相信任

1. 建立或使用現有的 Amazon Redshift 叢集，以供 AD FS 使用者連線。若要設定連線，則需要此叢集的特定屬性，例如叢集識別碼。如需詳細資訊，請參閱[建立叢集](#)。
2. 設定 AD FS 以控制 Microsoft 管理主控台上的 Amazon Redshift 存取：
 1. 選擇 ADFS 2.0，然後選擇 Add Relying Party Trust (新增信賴方信任)。在 Add Relying Party Trust Wizard (新增信賴方信任精靈) 頁面上，選擇 Start (開始)。
 2. 在 Select Data Source (選取資料來源) 頁面上，選擇 Import data about the relying party published online or on a local network (匯入關於在線上或本機網路上發佈信賴方的資料)。
 3. 針對 Federation metadata address (host name or URL) (聯合中繼資料地址 (主機名稱或 URL))，輸入 **https://signin.aws.amazon.com/saml-metadata.xml**。中繼資料 XML 檔案是描述 AWS 為信賴憑證者的標準 SAML 中繼資料文件。
 4. 在 Specify Display Name (指定顯示名稱) 頁面上，輸入 Display name (顯示名稱) 的值。
 5. 在 Choose Issuance Authorization Rules (選擇發行授權規則) 頁面上，選擇允許或拒絕所有使用者存取此信賴方的發行授權規則。
 6. 在 Ready to Add Trust (準備新增信任) 頁面上檢閱您的設定。
 7. 在 Finish (完成) 頁面上，選擇 Open the Edit Claim Rules dialog for this relying party trust when the wizard closes (當精靈關閉時，開啟此信賴方信任的「編輯宣告規則」對話方塊)。
 8. 在內容 (按一下滑鼠右鍵) 功能表上，選擇 Relying Party Trusts (依賴方信任)。
 9. 針對您的信賴方，開啟內容 (按一下滑鼠右鍵) 功能表，然後選擇 Edit Claim Rules (編輯宣告規則)。在 Edit Claim Rules (編輯宣告規則) 頁面上，選擇 Add Rule (新增規則)。
 10. 針對宣告規則範本，選擇 [轉換內送宣告]，然後在 [編輯規則-] NameId 頁面上執行下列動作：
 - 針對宣告規則名稱，輸入NameId。
 - 針對 Incoming claim name (傳入宣告名稱)，選擇 Windows Account Name (Windows 帳戶名稱)。
 - 針對 Outgoing claim name (傳出宣告名稱)，選擇 Name ID (名稱 ID)。
 - 針對 Outgoing name ID format (傳出名稱 ID 格式)，選擇 Persistent Identifier (持久性標識符)。

- 選擇 Pass through all claim values (傳遞所有宣告值)。

11. 在 Edit Claim Rules (編輯宣告規則) 頁面上，選擇 Add Rule (新增規則)。在 Select Rule Template (選取規則範本) 頁面上，針對 Claim rule template (宣告規則範本)，選擇 Send LDAP Attributes as Claims (將 LDAP 屬性傳送為宣告)。

12. 在 Configure Rule (設定規則) 頁面上，執行下列作業：

- 針對 Claim rule name (宣告規則名稱)，輸入 RoleSessionName。
- 針對 Attribute store (屬性存放區)，選擇 Active Directory。
- 針對 LDAP Attribute (LDAP 屬性)，選擇 Email Addresses (電子郵件地址)。
- 針對 傳出宣告類型，選擇 https://aws.amazon.com/SAML/Attributes/RoleSessionName。

13. 在 Edit Claim Rules (編輯宣告規則) 頁面上，選擇 Add Rule (新增規則)。在 Select Rule Template (選取規則範本) 頁面上，針對 Claim rule template (宣告規則範本)，選擇 Send Claims Using a Custom Rule (使用自訂規則傳送宣告)。

14. 在 Edit Rule – Get AD Groups (編輯規則 – 取得 AD 群組) 頁面上，針對 Claim rule name (宣告規則名稱)，輸入 Get AD Groups (取得 AD 群組)。

15. 針對 Custom rule (自訂規則)，輸入下列內容。

```
c:[Type ==
                                "http://schemas.microsoft.com/ws/2008/06/
identity/claims/windowsaccountname",
                                Issuer == "AD AUTHORITY"] => add(store =
"Active Directory",
                                types = ("http://temp/variable"), query =
";tokenGroups;{0}";,
                                param = c.Value);
```

16. 在 Edit Claim Rules (編輯宣告規則) 頁面上，選擇 Add Rule (新增規則)。在 Select Rule Template (選取規則範本) 頁面上，針對 Claim rule template (宣告規則範本)，選擇 Send Claims Using a Custom Rule (使用自訂規則傳送宣告)。

17. 在 Edit Rule – Roles (編輯規則 – 角色) 頁面上，針對 Claim rule name (宣告規則名稱)，輸入 Roles (角色)。

18. 針對 Custom rule (自訂規則)，輸入下列內容。

```
c:[Type == "http://temp/variable", Value =~ "(?i)^AWS-"] =>
issue(Type = "https://aws.amazon.com/SAML/Attributes/Role", Value =
RegExReplace(c.Value, "AWS-", "arn:aws:iam::123456789012:saml-provider/
ADFS,arn:aws:iam::123456789012:role/ADFS-"));
```

請記下 SAML 供應商的 ARN，以及要扮演的角色。在此範例中，arn:aws:iam:123456789012:saml-provider/ADFS 是 SAML 供應商的 ARN，arn:aws:iam:123456789012:role/ADFS- 是角色的 ARN。

- 請確定您已下載 federationmetadata.xml 檔案。檢查文件內容沒有無效的字元。這是您在設定信任關係時使用的中繼資料檔案 AWS。
- 在 IAM 主控台上建立 IAM SAML 身分提供者。您所提供的中繼資料文件，是您在設定 Azure 企業應用程式時儲存的聯合中繼資料 XML 檔案。如需詳細步驟，請參閱《IAM 使用者指南》中的[建立和管理 IAM 身分提供者 \(主控台\)](#)。
- 在 IAM 主控台上建立 SAML 2.0 聯合的 IAM 角色。如需詳細步驟，請參閱《IAM 使用者指南》中的[為 SAML 建立角色](#)。
- 建立 IAM 政策，您可將其附加至您在 IAM 主控台上為 SAML 2.0 聯合建立的 IAM 角色。如需詳細步驟，請參閱《IAM 使用者指南》中的[建立 IAM 政策 \(主控台\)](#)。如需 Azure AD 範例，請參閱[設定 JDBC 或 ODBC 單一登入身分驗證搭配 Microsoft Azure AD](#)。

設定 JDBC 以對 AD FS 進行身分驗證

- 將資料庫用戶端設定為使用 AD FS 單一登入，透過 JDBC 連線到您的叢集。

您可使用任何採用 JDBC 驅動程式的用戶端使用 AD FS 單一登入進行連線，或使用 Java 之類的語言透過指令碼進行連線。如需安裝和組態資訊，請參閱[設定 Amazon Redshift JDBC 驅動程式 2.1 版的連線](#)。

例如，您可以使用 SQLWorkbench/J 作為用戶端。當您設定 SQLWorkbench /J 時，您的資料庫 URL 會使用下列格式。

```
jdbc:redshift:iam://cluster-identifier:us-west-1/dev
```

如果您使用 SQLWorkbench /J 作為用戶端，請執行下列步驟：

- 啟動 SQL Workbench/J。在選取連線設定檔頁面中，新增設定檔群組，例如 **ADFS**。
- 針對 Connection Profile (連線設定檔)，輸入您的連線設定檔名稱，例如 **ADFS**。
- 選擇 Manage Drivers (管理驅動程式)，然後選擇 Amazon Redshift。選擇程式庫旁邊的開啟資料夾圖示，然後選擇適當的 JDBC .jar 檔案。
- 在 Select Connection Profile (選取連線設定檔) 頁面上，將資訊新增至連線設定檔，如下所示：

- 針對 User (使用者)，輸入您的 AD FS 使用者名稱。這是您用於單一登入之帳戶的使用者名稱，該帳戶具有您嘗試驗證之叢集的許可。
 - 針對 Password (密碼)，輸入您的 AD FS 密碼。
 - 針對 Drivers (驅動程式)，選擇 Amazon Redshift (com.amazon.redshift.jdbc.Driver)。
 - 針對 URL，輸入 **`jdbc:redshift:iam://your-cluster-identifier:your-cluster-region/your-database-name`**。
- e. 選擇延伸屬性。針對 plugin_name，輸入 **`com.amazon.redshift.plugin.AdfsCredentialsProvider`**。此值會指定驅動程式使用 AD FS 單一登入做為身分驗證方法。

設定 ODBC 以對 AD FS 進行身分驗證

- 將資料庫用戶端設定為使用 AD FS 單一登入，透過 ODBC 連線到您的叢集。

Amazon Redshift 會提供適用於 Linux、Windows 和 macOS 作業系統的 ODBC 驅動程式。安裝 ODBC 驅動程式之前，查明 SQL 用戶端工具是 32 位元或 64 位元。安裝符合 SQL 用戶端工具需求的 ODBC 驅動程式。

此外，為您的作業系統安裝和設定最新的 Amazon Redshift ODBC 驅動程式，如下所示：


- 若為 Windows，請參閱 [在 Microsoft Windows 上安裝並設定 Amazon Redshift ODBC 驅動程式](#)。
- 如需有關 macOS 的資訊，請參閱 [在 macOS X 上安裝 Amazon Redshift ODBC 驅動程式](#)。
- 若為 Linux，請參閱 [在 Linux 上安裝 Amazon Redshift ODBC 驅動程式](#)。

在 Windows 上，於 Amazon Redshift ODBC Driver DSN Setup (Amazon Redshift ODBC 驅動程式 DSN 設定) 頁面的 Connection Settings (連線設定) 之下，輸入下列資訊：

- 針對 Data source name (資料來源名稱)，輸入 **`your-DSN`**。這會指定作為 ODBC 設定檔名稱的資料來源名稱。
- 針對驗證類型，選擇身分提供者：SAML。這是 ODBC 驅動程式使用 AD FS 單一登入來進行驗證的身分驗證方法。
- 針對 Cluster ID (叢集 ID)，輸入 **`your-cluster-identifier`**。
- 針對 Region (區域)，輸入 **`your-cluster-region`**。
- 針對 Database (資料庫)，輸入 **`your-database-name`**。

- 針對 User (使用者)，輸入 ***your-adfs-username***。這是您用於單一登入之 AD FS 帳戶的使用者名稱，該帳戶具有您嘗試驗證之叢集的許可。僅在 Auth Type (驗證類型) 為 Identity Provider: SAML (身分提供者：SAML) 的情況下使用此項目。
- 針對 Password (密碼)，輸入 ***your-adfs-password***。僅在 Auth Type (驗證類型) 為 Identity Provider: SAML (身分提供者：SAML) 的情況下使用此項目。

在 macOS 和 Linux 上，編輯 `odbc.ini` 檔案，如下所示：

 Note

所有項目都不區分大小寫。

- 針對 `clusterid`，輸入 ***your-cluster-identifier***。這是所建立 Amazon Redshift 叢集的名稱。
- 針對 `region` (區域)，輸入 ***your-cluster-region***。這是所建 AWS 立的 Amazon Redshift 叢集的區域。
- 針對 `database` (資料庫)，輸入 ***your-database-name***。這是您嘗試在 Amazon Redshift 叢集上存取的資料庫名稱。
- 針對 `locale`，輸入 **`en-us`**。這是錯誤訊息的顯示語言。
- 針對 `iam`，輸入 **`1`**。此值指定驅動程式使用 IAM 登入資料進行身分驗證。
- 針對 `plugin_name`，執行下列其中一項作業：
 - 若為具有 MFA 的 AD FS 單一登入組態，請輸入 **`BrowserSAML`**。這是 ODBC 驅動程式用來驗證 AD FS 的身分驗證方法。
 - 若為 AD FS 單一登入組態，請輸入 **`ADFS`**。這是 ODBC 驅動程式使用 Azure AD 單一登入來進行驗證的身分驗證方法。
- 針對 `uid`，輸入 ***your-adfs-username***。這是您用於單一登入之 Microsoft Azure 帳戶的使用者名稱，該帳戶具有您嘗試驗證之叢集的許可。僅在 `plugin_name` 為 ADFS 的情況下使用此項目。
- 針對 `pwd`，輸入 ***your-adfs-password***。僅在 `plugin_name` 為 ADFS 的情況下使用此項目。

在 macOS 和 Linux 上，同時編輯設定檔設定以新增下列匯出：

```
export ODBCINI=/opt/amazon/redshift/Setup/odbc.ini
```

```
export ODBCINSTINI=/opt/amazon/redshift/Setup/odbcinst.ini
```

設定 JDBC 或 ODBC 單一登入身分驗證搭配 Ping Identity

您可以使用 Ping 身分做為身分提供者 (IdP) 來存取您的 Amazon Redshift 叢集。接下來，您可以找到描述如何使用 PingOne 入口網站為此目的設定信任關係的程序。如需[有關設定 AWS 為 Ping 身分識別服務提供者的詳細資訊](#)，請參閱在 IAM 使用者指南中設定 SAML 2.0 IdP 和新增宣告。

設置 Ping 身份和您的 AWS 帳戶以相互信任

1. 建立或使用現有的 Amazon Redshift 叢集，以供 Ping Identity 使用者連線。若要設定連線，則需要此叢集的特定屬性，例如叢集識別碼。如需詳細資訊，請參閱[建立叢集](#)。
2. 將 Amazon Redshift 新增為入口網站上的新 SAML 應用程式 PingOne。如需詳細步驟，請參閱[Ping 身分文件](#)。
 1. 前往 My Applications (我的應用程式)。
 2. 在 Add Application (新增應用程式) 下方，選擇 New SAML Application (新增 SAML 應用程式)。
 3. 針對 Application Name (應用程式名稱)，輸入 **Amazon Redshift**。
 4. 針對 Protocol Version (通訊協定版本)，選擇 SAML v2.0。
 5. 針對 Category (類別)，選擇 ***your-application-category***。
 6. 針對 Assertion Consumer Service (ACS) (聲明消費者服務 (ACS))，輸入 ***your-redshift-local-host-url***。這是 SAML 聲明會重新導向至的本機主機與連接埠。
 7. 針對 Entity ID (實體 ID)，輸入 urn:amazon:webservices。
 8. 針對 Signing (簽署)，選擇 Sign Assertion (簽署聲明)。
 9. 在 SSO Attribute Mapping (SSO 屬性映射) 區段中，建立如下表所示的宣告。

應用程式屬性	常值的身分橋接屬性
https://aws.amazon.com/SAML/Attributes/Role	<i>ARN: AWN: IAM:: 123456789012: # #/#, ##:AWN: IAM:: 123 456789012 : #####/ PingProvider</i>

應用程式屬性	常值的身分橋接屬性
https://aws.amazon.com/SAML/Attributes/RoleSessionName	email
https://redshift.amazon.com/SAML/Attributes/AutoCreate	“true”
https://redshift.amazon.com/SAML/Attributes/DbUser	email
https://redshift.amazon.com/SAML/Attributes/DbGroups	「DbGroups」屬性中的群組包含 @directory 前置詞。若要移除此項目，請在 Identity Bridge 中輸入 memberOf。在函數中，選擇 ExtractByRegularExpression。在運算式中，輸入 (.*)[\@](?:.*)。

- 針對 Group Access (群組存取)，視需要設定下列群組存取：
 - https://aws.amazon.com/SAML/Attributes/Role
 - https://aws.amazon.com/SAML/Attributes/RoleSessionName
 - https://redshift.amazon.com/SAML/Attributes/AutoCreate
 - https://redshift.amazon.com/SAML/Attributes/DbUser
- 檢閱您的設定並進行變更 (如有必要)。
- 使用 Initiate Single Sign-On (SSO) URL (啟動單一登入 (SSO) URL) 做為瀏覽器 SAML 外掛程式的登入 URL。
- 在 IAM 主控台上建立 IAM SAML 身分提供者。您所提供的中繼資料文件，是您在設定 Ping 身分時儲存的聯合中繼資料 XML 檔案。如需詳細步驟，請參閱《IAM 使用者指南》中的[建立和管理 IAM 身分提供者 \(主控台\)](#)。
- 在 IAM 主控台上建立 SAML 2.0 聯合的 IAM 角色。如需詳細步驟，請參閱《IAM 使用者指南》中的[為 SAML 建立角色](#)。
- 建立 IAM 政策，您可將其附加至您在 IAM 主控台上為 SAML 2.0 聯合建立的 IAM 角色。如需詳細步驟，請參閱《IAM 使用者指南》中的[建立 IAM 政策 \(主控台\)](#)。如需 Azure AD 範例，請參閱[設定 JDBC 或 ODBC 單一登入身分驗證搭配 Microsoft Azure AD](#)。

設定 JDBC 以對 Ping 身分進行驗證

- 將資料庫用戶端設定為使用 Ping Identity 單一登入，透過 JDBC 連線到您的叢集。

您可使用任何採用 JDBC 驅動程式的用戶端使用 Ping Identity 單一登入進行連線，或使用 Java 之類的語言透過指令碼進行連線。如需安裝和組態資訊，請參閱 [設定 Amazon Redshift JDBC 驅動程式 2.1 版的連線](#)。

例如，您可以使用 SQLWorkbench/J 作為用戶端。當您設定 SQLWorkbench /J 時，您的資料庫 URL 會使用下列格式。

```
jdbc:redshift:iam://cluster-identifier:us-west-1/dev
```

如果您使用 SQLWorkbench /J 作為用戶端，請執行下列步驟：

- 啟動 SQL Workbench/J。在選取連線設定檔頁面中，新增設定檔群組，例如 **Ping**。
- 針對 Connection Profile (連線設定檔)，輸入 ***your-connection-profile-name***，例如 **Ping**。
- 選擇 Manage Drivers (管理驅動程式)，然後選擇 Amazon Redshift。選擇程式庫旁邊的開啟資料夾圖示，然後選擇適當的 JDBC .jar 檔案。
- 在 Select Connection Profile (選取連線設定檔) 頁面上，將資訊新增至連線設定檔，如下所示：
 - 在使用者中，輸入您的 PingOne 使用者名稱。這是您用於單一登入之 PingOne 帳戶的使用者名稱，該帳戶具有您嘗試使用驗證之叢集權限的使用者名稱。
 - 在「密碼」中，輸入您的 PingOne 密碼。
 - 針對 Drivers (驅動程式)，選擇 Amazon Redshift (com.amazon.redshift.jdbc.Driver)。
 - 針對 URL，輸入 ***jdbc:redshift:iam://your-cluster-identifier:your-cluster-region/your-database-name***。
- 選擇 Extended Properties (延伸屬性)，然後執行下列任一項：
 - 針對 login_url，輸入 ***your-ping-sso-login-url***。此值會指定 URL 使用單一登入做為登入的身分驗證。
 - 若為 Ping 身分，請針對 plugin_name 輸入 **com.amazon.redshift.plugin.PingCredentialsProvider**。此值指定驅動程式使用 Ping Identity 單一登入作為身分驗證方法。

- 若為具有單一登入的 Ping Identity，請針對 `plugin_name` 輸入 **`com.amazon.redshift.plugin.BrowserSamlCredentialsProvider`**。此值會指定驅動程式使用 Ping Identity PingOne 搭配單一登入作為驗證方法。

設定 ODBC 以對 Ping 身分進行身分驗證

- 將您的資料庫用戶端設定為使用 Ping 身分 PingOne 單一登入透過 ODBC 連線到叢集。

Amazon Redshift 會提供適用於 Linux、Windows 和 macOS 作業系統的 ODBC 驅動程式。安裝 ODBC 驅動程式之前，查明 SQL 用戶端工具是 32 位元或 64 位元。安裝符合 SQL 用戶端工具需求的 ODBC 驅動程式。

此外，為您的作業系統安裝和設定最新的 Amazon Redshift ODBC 驅動程式，如下所示：


- 若為 Windows，請參閱 [在 Microsoft Windows 上安裝並設定 Amazon Redshift ODBC 驅動程式](#)。
- 如需有關 macOS 的資訊，請參閱 [在 macOS X 上安裝 Amazon Redshift ODBC 驅動程式](#)。
- 若為 Linux，請參閱 [在 Linux 上安裝 Amazon Redshift ODBC 驅動程式](#)。

在 Windows 上，於 Amazon Redshift ODBC Driver DSN Setup (Amazon Redshift ODBC 驅動程式 DSN 設定) 頁面的 Connection Settings (連線設定) 之下，輸入下列資訊：

- 針對 Data source name (資料來源名稱)，輸入 ***your-DSN***。這會指定作為 ODBC 設定檔名稱的資料來源名稱。
- 針對 Auth Type (驗證類型)，執行下列其中一項操作：
 - 針對 Ping 身分組態，選擇 Identity Provider: Ping Federate (身分提供者：Ping 聯合)。這是 ODBC 驅動程式使用 Ping Identity 單一登入用來驗證的身分驗證方法。
 - 針對具有單一登入的 Ping Identity 組態，選擇身分提供者：瀏覽器 SAML。這是 ODBC 驅動程式透過具有單一登入的 Ping Identity 用來進行身分驗證的身分驗證方法。
- 針對 Cluster ID (叢集 ID)，輸入 ***your-cluster-identifier***。
- 針對 Region (區域)，輸入 ***your-cluster-region***。
- 針對 Database (資料庫)，輸入 ***your-database-name***。
- 針對 User (使用者)，輸入 ***your-ping-username***。這是您用於單一登入的 PingOne 帳戶的使用者名稱，該帳戶具有您嘗試使用驗證之叢集的權限。僅將其用於身份驗證類型是身份提供者：PingFederate。

- 針對 Password (密碼), 輸入 ***your-ping-password***。僅將其用於身份驗證類型是身份提供者: PingFederate。
- 針對 Listen Port (接聽連接埠), 輸入 ***your-listen-port***。這是本機伺服器接聽的連接埠。預設值為 7890。這僅適用於瀏覽器 SAML 外掛程式。
- 針對 Response Timeout (回應逾時), 輸入 ***the-number-of-seconds***。這是 IdP 伺服器傳回回應時, 在逾時之前等待的秒數。秒數的下限必須為 10。如果建立連線所花的時間超過此臨界值, 連線會中止。這僅適用於瀏覽器 SAML 外掛程式。
- 針對 Login URL (登入 URL), 輸入 ***your-login-url***。這僅適用於瀏覽器 SAML 外掛程式。

在 macOS 和 Linux 上, 編輯 `odbc.ini` 檔案, 如下所示:

 Note

所有項目都不區分大小寫。

- 針對 clusterid, 輸入 ***your-cluster-identifier***。這是所建立 Amazon Redshift 叢集的名稱。
- 針對 region (區域), 輸入 ***your-cluster-region***。這是所建 AWS 立的 Amazon Redshift 叢集的區域。
- 針對 database (資料庫), 輸入 ***your-database-name***。這是您嘗試在 Amazon Redshift 叢集上存取的資料庫名稱。
- 針對 locale, 輸入 ***en-us***。這是錯誤訊息的顯示語言。
- 針對 iam, 輸入 ***1***。此值指定驅動程式使用 IAM 登入資料進行身分驗證。
- 針對 plugin_name, 執行下列其中一項作業:
 - 針對 Ping 身分組態, 輸入 ***BrowserSAML***。這是 ODBC 驅動程式用來驗證具有 MFA 之 Ping 身分 SSO 的身分驗證方法。
 - 對於具有單一登入的 Ping Identity 組態, 請輸入 ***Ping***。這是 ODBC 驅動程式透過具有單一登入的 Ping Identity 用來進行身分驗證的身分驗證方法。
- 針對 uid, 輸入 ***your-ping-username***。這是您用於單一登入之 Microsoft Azure 帳戶的使用者名稱, 該帳戶具有您嘗試驗證之叢集的許可。僅在 plugin_name 為 Ping 的情況下使用此項目。
- 針對 pwd, 輸入 ***your-ping-password***。僅在 plugin_name 為 Ping 的情況下使用此項目。

- 針對 `login_url`，輸入 ***your-login-url***。這是會傳回 SAML 回應的初始單一登入 URL。這僅適用於瀏覽器 SAML 外掛程式。
- 針對 `idp_response_timeout`，輸入 ***the-number-of-seconds***。這是等待 PingOne Identity 回應的指定時間 (以秒為單位)。這僅適用於瀏覽器 SAML 外掛程式。
- 針對 `listen_port`，輸入 ***your-listen-port***。這是本機伺服器接聽的連接埠。預設值為 7890。這僅適用於瀏覽器 SAML 外掛程式。

在 macOS 和 Linux 上，同時編輯設定檔設定以新增下列匯出：

```
export ODBCINI=/opt/amazon/redshift/Setup/odbc.ini
```

```
export ODBCINSTINI=/opt/amazon/redshift/Setup/odbcinst.ini
```

設定 JDBC 或 ODBC 單一登入身分驗證搭配 Okta

您可以使用 Okta 做為身分提供者 (IdP) 來存取您的 Amazon Redshift 叢集。接著，您可以尋找描述如何就此目的設定信任關係的程序。如需有關設定 AWS 為 Okta 服務提供者的詳細資訊，請參閱 [「IAM 使用者指南」](#) 中的 [「使用信賴方信任設定 SAML 2.0 IdP」](#) 和 [「新增宣告」](#)。

設定 Okta 與您的 AWS 帳戶以互相信任

1. 建立或使用現有的 Amazon Redshift 叢集，以供 Okta 使用者連線。若要設定連線，則需要此叢集的特定屬性，例如叢集識別碼。如需詳細資訊，請參閱 [建立叢集](#)。
2. 在 Okta 入口網站上將 Amazon Redshift 新增為新的應用程式。如需詳細步驟，請參閱 [Okta 文件](#)。
 - 選擇 Add Application (新增應用程式)。
 - 在 Add Application (新增應用程式) 下方，選擇 Create New App (建立新的應用程式)。
 - 在 Create a New Add Application Integration (建立新的新增應用程式整合) 頁面上，針對 Platform (平台) 選擇 Web。
 - 針對 Sign on method (登入方法)，選擇 SAML v2.0。
 - 在 General Settings (一般設定) 頁面上，針對 App name (應用程式名稱) 輸入 ***your-redshift-saml-ssso-name***。這是您的應用程式名稱。

- 在 SAML Settings (SAML 設定) 頁面上，針對 Single sign on URL (單一登入 URL)，輸入 ***your-redshift-local-host-url***。這是 SAML 聲明會重新導向至的本機主機與連接埠，例如 `http://localhost:7890/redshift/`。
3. 使用單一登入 URL 值做為收件人 URL 和目標 URL。
 4. 針對 Signing (簽署)，選擇 Sign Assertion (簽署聲明)。
 5. 針對對象 URI (SP 實體 ID)，針對宣告輸入 **`urn:amazon:webservices`**，如下表所示。
 6. 在進階設定區段中，針對 SAML 發行者 ID 輸入 ***your-Identity-Provider-Issuer-ID***，您可以在檢視設定指示區段中找到此值。
 7. 在 Attribute Statements (屬性陳述式) 區段中，建立如下表所示的宣告。

宣告名稱	Value
<code>https://aws.amazon.com/SAML/Attributes/Role</code>	<code>arn:aws:iam::<i>123456789012</i> :role/<i>Okta</i>,arn:aws:iam::<i>123456789012</i> :saml-provider/<i>Okta</i></code>
<code>https://aws.amazon.com/SAML/Attributes/RoleSessionName</code>	<code>user.email</code>
<code>https://redshift.amazon.com/SAML/Attributes/AutoCreate</code>	<code>"true"</code>
<code>https://redshift.amazon.com/SAML/Attributes/DbUser</code>	<code>user.email</code>

8. 在 App Embed Link (應用程式內嵌連結) 區段中，尋找您可以用來做為瀏覽器 SAML 外掛程式登入 URL 的 URL。
9. 在 IAM 主控台上建立 IAM SAML 身分提供者。您所提供的中繼資料文件，是您在設定 Okta 時儲存的聯合中繼資料 XML 檔案。如需詳細步驟，請參閱《IAM 使用者指南》中的[建立和管理 IAM 身分提供者 \(主控台\)](#)。
10. 在 IAM 主控台上建立 SAML 2.0 聯合的 IAM 角色。如需詳細步驟，請參閱《IAM 使用者指南》中的[為 SAML 建立角色](#)。
11. 建立 IAM 政策，您可將其附加至您在 IAM 主控台上為 SAML 2.0 聯合建立的 IAM 角色。如需詳細步驟，請參閱《IAM 使用者指南》中的[建立 IAM 政策 \(主控台\)](#)。如需 Azure AD 範例，請參閱[設定 JDBC 或 ODBC 單一登入身分驗證搭配 Microsoft Azure AD](#)。

設定 JDBC 以對 Okta 進行身分驗證

- 將資料庫用戶端設定為使用 Okta 單一登入，透過 JDBC 連線到您的叢集。

您可使用任何採用 JDBC 驅動程式的用戶端使用 Okta 單一登入進行連線，或使用 Java 之類的語言透過指令碼進行連線。如需安裝和組態資訊，請參閱 [設定 Amazon Redshift JDBC 驅動程式 2.1 版的連線](#)。

例如，您可以使用 SQLWorkbench/J 作為用戶端。當您設定 SQLWorkbench /J 時，您的資料庫 URL 會使用下列格式。

```
jdbc:redshift:iam://cluster-identifier:us-west-1/dev
```

如果您使用 SQLWorkbench /J 作為用戶端，請執行下列步驟：

- 啟動 SQL Workbench/J。在選取連線設定檔頁面中，新增設定檔群組，例如 **Okta**。
- 針對 Connection Profile (連線設定檔)，輸入 ***your-connection-profile-name***，例如 **Okta**。
- 選擇 Manage Drivers (管理驅動程式)，然後選擇 Amazon Redshift。選擇程式庫旁邊的開啟資料夾圖示，然後選擇適當的 JDBC jar 檔案。
- 在 Select Connection Profile (選取連線設定檔) 頁面上，將資訊新增至連線設定檔，如下所示：
 - 在 User (使用者) 輸入您的 Okta 使用者名稱。這是您用於單一登入之 Okta 帳戶的使用者名稱，該帳戶具有您嘗試驗證之叢集的許可。
 - 在 Password (密碼) 輸入您的 Okta 密碼。
 - 針對 Drivers (驅動程式)，選擇 Amazon Redshift (com.amazon.redshift.jdbc.Driver)。
 - 針對 URL，輸入 ***jdbc:redshift:iam://your-cluster-identifier:your-cluster-region/your-database-name***。
- 選擇 Extended Properties (延伸屬性)，然後執行下列任一項：
 - 針對 login_url，輸入 ***your-okta-sso-login-url***。此值會指定 URL 使用單一登入做為登入 Okta 的身分驗證。
 - 針對 Okta 單一登入，請為 plugin_name 輸入 **com.amazon.redshift.plugin.OktaCredentialsProvider**。此值指定驅動程式使用 Okta 單一登入作為身分驗證方法。

- 針對具有 MFA 的 Okta 單一登入，請為 `plugin_name` 輸入 **`com.amazon.redshift.plugin.BrowserSamlCredentialsProvider`**。此值會指定驅動程式使用具有 MFA 的 Okta 單一登入做為身分驗證方法。

設定 ODBC 以對 Okta 進行身分驗證

- 將資料庫用戶端設定為使用 Okta 單一登入，透過 ODBC 連線到您的叢集。

Amazon Redshift 會提供適用於 Linux、Windows 和 macOS 作業系統的 ODBC 驅動程式。安裝 ODBC 驅動程式之前，查明 SQL 用戶端工具是 32 位元或 64 位元。安裝符合 SQL 用戶端工具需求的 ODBC 驅動程式。

此外，為您的作業系統安裝和設定最新的 Amazon Redshift ODBC 驅動程式，如下所示：


- 若為 Windows，請參閱 [在 Microsoft Windows 上安裝並設定 Amazon Redshift ODBC 驅動程式](#)。
- 如需有關 macOS 的資訊，請參閱 [在 macOS X 上安裝 Amazon Redshift ODBC 驅動程式](#)。
- 若為 Linux，請參閱 [在 Linux 上安裝 Amazon Redshift ODBC 驅動程式](#)。

在 Windows 上，於 Amazon Redshift ODBC Driver DSN Setup (Amazon Redshift ODBC 驅動程式 DSN 設定) 頁面的 Connection Settings (連線設定) 之下，輸入下列資訊：

- 針對 Data source name (資料來源名稱)，輸入 ***your-DSN***。這會指定作為 ODBC 設定檔名稱的資料來源名稱。
- 針對 Auth Type (驗證類型)，執行下列其中一項操作：
 - 針對 Okta 單一登入組態，請選擇 **Identity Provider: Okta**。這是 ODBC 驅動程式使用 Okta 單一登入來進行驗證的身分驗證方法。
 - 針對具有 MFA 的 Okta 單一登入組態，請選擇 **Identity Provider: Browser SAML**。這是 ODBC 驅動程式使用具有 MFA 之 Okta 單一登入來進行驗證的身分驗證方法。
- 針對 Cluster ID (叢集 ID)，輸入 ***your-cluster-identifier***。
- 針對 Region (區域)，輸入 ***your-cluster-region***。
- 針對 Database (資料庫)，輸入 ***your-database-name***。
- 針對 User (使用者)，輸入 ***your-okta-username***。這是您用於單一登入之 Okta 帳戶的使用者名稱，該帳戶具有您嘗試驗證之叢集的許可。僅在 Auth Type (驗證類型) 為 Identity Provider: Okta (身分提供者：Okta) 的情況下使用此項目。

- 針對 Password (密碼)，輸入 ***your-okta-password***。僅在 Auth Type (驗證類型) 為 Identity Provider: Okta (身分提供者：Okta) 的情況下使用此項目。

在 macOS 和 Linux 上，編輯 `odbc.ini` 檔案，如下所示：

 Note

所有項目都不區分大小寫。

- 針對 `clusterid`，輸入 ***your-cluster-identifier***。這是所建立 Amazon Redshift 叢集的名稱。
- 針對 `region` (區域)，輸入 ***your-cluster-region***。這是所建 AWS 立的 Amazon Redshift 叢集的區域。
- 針對 `database` (資料庫)，輸入 ***your-database-name***。這是您嘗試在 Amazon Redshift 叢集上存取的資料庫名稱。
- 針對 `locale`，輸入 ***en-us***。這是錯誤訊息的顯示語言。
- 針對 `iam`，輸入 ***1***。此值指定驅動程式使用 IAM 登入資料進行身分驗證。
- 針對 `plugin_name`，執行下列其中一項作業：
 - 若為具有 MFA 的 Okta 單一登入組態，請輸入 ***BrowserSAML***。這是 ODBC 驅動程式用來驗證具有 MFA 之 Okta 單一登入的身分驗證方法。
 - 針對 Okta 單一登入組態，請輸入 ***Okta***。這是 ODBC 驅動程式使用 Okta 單一登入來進行驗證的身分驗證方法。
- 針對 `uid`，輸入 ***your-okta-username***。這是您用於單一登入之 Okta 帳戶的使用者名稱，該帳戶具有您嘗試驗證之叢集的許可。僅在 `plugin_name` 為 Okta 的情況下使用此項目。
- 針對 `pwd`，輸入 ***your-okta-password***。僅在 `plugin_name` 為 Okta 的情況下使用此項目。
- 針對 `login_url`，輸入 ***your-login-url***。這是會傳回 SAML 回應的初始單一登入 URL。這僅適用於瀏覽器 SAML 外掛程式。
- 針對 `idp_response_timeout`，輸入 ***the-number-of-seconds***。這是等待回應的指定時間 (以秒為單位) PingOne。這僅適用於瀏覽器 SAML 外掛程式。
- 針對 `listen_port`，輸入 ***your-listen-port***。這是本機伺服器接聽的連接埠。預設值為 7890。這僅適用於瀏覽器 SAML 外掛程式。

在 macOS 和 Linux 上，同時編輯設定檔設定以新增下列匯出：

```
export ODBCINI=/opt/amazon/redshift/Setup/odbc.ini
```

```
export ODBCINSTINI=/opt/amazon/redshift/Setup/odbcinst.ini
```

用於建立資料庫使用者登入資料的 JDBC 和 ODBC 選項

若要使用 Amazon Redshift JDBC 或 ODBC 驅動程式建立資料庫使用者憑證，請以 JDBC 或 ODBC 選項提供資料庫使用者名稱。如果資料庫使用者不存在，您也可選擇性讓驅動程式建立新的資料庫使用者，此外也可指定使用者於登入時加入的資料庫使用者群組清單。

如果您使用身分提供者 (IdP)，請洽詢 IdP 管理員，以決定這些選項的正確值。IdP 管理員也可設定您的 IdP，以提供這些選項，如此您便不用透過 JDBC 或 ODBC 選項提供。如需詳細資訊，請參閱 [設定 IdP 的 SAML 聲明](#)。

Note

如果您使用 IAM 政策變數 `${redshift:DbUser}`，如 [資源策略 GetClusterCredentials](#) 中所述，則會以 API 操作的請求內容所擷取的值取代 `DbUser` 的值。Amazon Redshift 驅動程式使用連線 URL 提供的 `DbUser` 變數的值，而非提供作為 SAML 屬性的值。

為了協助保護此組態的安全，建議您在 IAM 政策中使用條件，配合 `RoleSessionName` 來驗證 `DbUser` 值。您可以在 [使用政策範例 GetClusterCredentials](#) 中找到如何使用 IAM 政策來設定條件的範例。

下表列出提供用於建立資料庫使用者登入資料的選項。

選項	描述
DbUser	資料庫使用者的名稱。如果資料庫中 DbUser 存在名為的使用者，則臨時使用者認證會與現有使用者具有相同的權限。如果資料庫中 DbUser 不存在且 <code>AutoCreate</code> 為 <code>true</code> ，則會建立名 <code>DbUser</code> 為的新使用者。您也可選擇性停用現有使用者的密碼。如需詳細資訊，請參閱 ALTER_USER

選項	描述
AutoCreate	如果資料庫使用者不存在，請指定使用指 DbUser 定的名稱 true 來建立資料庫使用者。預設值為 false。
DbGroups	資料庫使用者在目前工作階段中加入之一或多個現有資料庫群組名稱的逗號分隔清單。根據預設，新使用者只會加入 PUBLIC。

使用 Amazon Redshift CLI 或 API 產生 IAM 身分的資料庫登入資料

為了以程式設計方式產生臨時資料庫使用者登入資料，Amazon Redshift 會提供 AWS Command Line Interface (AWS CLI) 和 [GetClusterCredentials](#) API 作業的 `get-cluster-credentials` 命令。或者，您可以使用 Amazon Redshift JDBC 或 ODBC 驅動程式來設定 SQL 用戶端，以管理呼叫 `GetClusterCredentials` 操作、擷取資料庫使用者憑證，以及在 SQL 用戶端和 Amazon Redshift 資料庫之間建立連接的程序。如需詳細資訊，請參閱 [用於建立資料庫使用者登入資料的 JDBC 和 ODBC 選項](#)。

Note

我們建議使用 Amazon Redshift JDBC 或 ODBC 驅動程式產生資料庫使用者憑證。

在本節中，您可以找到以程式設計方式呼叫 `GetClusterCredentials` 作業或 `get-cluster-credentials` 命令、擷取資料庫使用者認證，以及連線至資料庫的步驟。

產生及使用暫時性資料庫登入資料

1. 建立或修改具有必要許可的使用者或角色。如需 IAM 許可的相關資訊，請參閱 [建立具有呼叫權限的 IAM 角色](#) `GetClusterCredentials`。
2. 身為您在上一個步驟中授權的使用者或角色，執行 `get-cluster-credentials` CLI 命令或呼叫 `GetClusterCredentials` API 作業，並提供下列值：
 - 叢集識別碼 — 包含資料庫之叢集的名稱。
 - 資料庫使用者名稱 — 現有或新資料庫使用者的名稱。
 - 如果使用者不存在於資料庫中且 `AutoCreate` 為真，則會在停用 `PASSWORD` 的情況下建立新使用者。
 - 如果使用者不存在且 `AutoCreate` 為 false，則要求會失敗。

- 針對此範例，資料庫使用者名稱為 `temp_creds_user`。
 - 自動建立 — (選用) 如果資料庫使用者名稱不存在，則建立新使用者。
 - 資料庫名稱 — (選用) 使用者授權登入之資料庫的名稱。如果未指定資料庫名稱，使用者將可登入任何的叢集資料庫。
 - 資料庫群組 — (選用) 現有資料庫使用者群組的清單。成功登入後，資料庫使用者將新增至指定的使用者群組。如果未指定群組，使用者只會具有 PUBLIC 許可。使用者群組名稱必須符合附加至使用者或角色之 IAM 政策中指定的 `dbgroup` 資源 ARN。
 - 過期時間 — (選用) 暫時性憑證過期前經過的時間 (以秒計)。您可指定 900 秒 (15 分鐘) 至 3600 秒 (60 分鐘) 之間的值。預設為 900 秒。
3. Amazon Redshift 會確定使用者具備用指定資源呼叫 `GetClusterCredentials` 操作的許可。
 4. Amazon Redshift 將傳回暫時性密碼和資料庫使用者名稱。

下列範例使用 Amazon Redshift CLI 為名為 `temp_creds_user` 的現有使用者產生暫時性資料庫憑證。

```
aws redshift get-cluster-credentials --cluster-identifier examplecluster --db-user
temp_creds_user --db-name exampledb --duration-seconds 3600
```

結果如下所示。

```
{
  "DbUser": "IAM:temp_creds_user",
  "Expiration": "2016-12-08T21:12:53Z",
  "DbPassword": "EXAMPLEjArE3hcnQj8zt4XQj9Xtma8oxYEM80yxpdHwXVPyJYBDm/
gqX2Eeaq6P3DgTzgPg=="
}
```

下列範例使用 Amazon Redshift CLI 與 `autocreate` 為新使用者產生暫時性資料庫憑證，並將使用者加入到 `example_group` 群組。

```
aws redshift get-cluster-credentials --cluster-identifier examplecluster --db-user
temp_creds_user --auto-create --db-name exampledb --db-groups example_group --
duration-seconds 3600
```

結果如下所示。

```
{
```

```
"DbUser": "IAMA:temp_creds_user:example_group",
"Expiration": "2016-12-08T21:12:53Z",
"DbPassword": "EXAMPLEjArE3hcnQj8zt4XQj9Xtma8oxYEM80yxpDHwXVPyJYBDm/
gqX2Eeaq6P3DgTzgPg=="
}
```

5. 建立與 Amazon Redshift 叢集的 Secure Socket Layer (SSL) 身分驗證連線，並用來自 GetClusterCredentials 回應中的使用者名稱和密碼傳送登入請求。請在使用者名稱中加入 IAM: 或 IAMA: 字首，例如，IAM:temp_creds_user 或 IAMA:temp_creds_user。

Important

設定 SQL 用戶端要求 SSL。否則，如果您的 SQL 用戶端自動嘗試使用 SSL 連線，發生任何類型的故障時其將切換為非 SSL。在此情況下，第一個連線嘗試可能會因為登入資料過期或失效而失敗，而第二個連線嘗試可能會因連線不是 SSL 而失敗。此時，可能會跳過第一個錯誤訊息。如需使用 SSL 連接至叢集的相關資訊，請參閱 [設定連線的安全選項](#)。

6. 如果連線不使用 SSL，連線嘗試將失敗。
7. 叢集會傳送 authentication 請求至 SQL 用戶端。
8. 接著 SQL 用戶端會傳送暫時性密碼至叢集。
9. 如果密碼為有效且尚未過期，叢集將完成連線。

授權 Amazon Redshift 代表您訪問其他 AWS 服務

某些 Amazon Redshift 功能需要 Amazon Redshift 代表您存取其他 AWS 服務。例如，[COPY](#) 和 [UNLOAD](#) 命令可在使用 Amazon S3 儲存貯體的 Amazon Redshift 叢集上載入或卸載資料。[創建外部函數](#)命令可以使用標量 AWS Lambda 用戶定義函數 (UDF) 調用 Lambda 函數。Amazon Redshift Spectrum 可以在 Amazon Athena 使用數據目錄或 AWS Glue。若要讓 Amazon Redshift 叢集代替您執行作業，您需為叢集提供安全憑證。提供安全憑證的建議方式為指定 AWS Identity and Access Management (IAM) 角色。對於 COPY 和 UNLOAD，您可以提供臨時憑證。

如果使用者想要與 AWS 之外的 AWS Management Console 授與程式設計存取 AWS 取權的方式取決於正在存取的使用者類型。

若要授與使用者程式設計存取權，請選擇下列其中一個選項。

哪個使用者需要程式設計存取權？	到	By
人力身分 (IAM Identity Center 中管理的使用者)	使用臨時登入資料來簽署對 AWS CLI、AWS SDK 或 AWS API 的程式設計要求。	請依照您要使用的介面所提供的指示操作。 <ul style="list-style-type: none"> • 如需詳細資訊 AWS CLI，請參閱 《使 AWS CLI 用 AWS Command Line Interface 者指南》 AWS IAM Identity Center 中的〈配置使用〉。 • 如需 AWS SDK、工具和 AWS API，請參閱 AWS SDK 和工具參考指南中的 IAM 身分中心身分驗證。
IAM	使用臨時登入資料來簽署對 AWS CLI、AWS SDK 或 AWS API 的程式設計要求。	遵循 《IAM 使用者指南》 中的〈 將臨時登入資料搭配 AWS 資源使用 〉中的指示
IAM	(不建議使用) 使用長期認證來簽署對 AWS CLI、AWS SDK 或 AWS API 的程式設計要求。	請依照您要使用的介面所提供的指示操作。 <ul style="list-style-type: none"> • 如需相關資訊 AWS CLI，請參閱使用指南中的 使用 IAM 使用者登入資料進行驗證。AWS Command Line Interface • 對於 AWS SDK 和工具，請參閱 AWS SDK 和工具參考指南中的 使用長期憑據進行身份驗證。 • 如需 AWS API，請參閱 IAM 使用者指南 中的 管理 IAM 使用者的存取金鑰。

接下來，瞭解如何建立具有適當權限的 IAM 角色，以存取其他 AWS 服務。您也需要在執行 Amazon Redshift 命令時將角色與您的叢集相關聯，並指定角色的 Amazon Resource Name (ARN)。如需詳細資訊，請參閱 [使用 IAM 角色授權 COPY、UNLOAD、CREATE EXTERNAL FUNCTION 和 CREATE EXTERNAL SCHEMA 操作](#)。

此外，超級使用者可以將 ASSUMEROLE 權限授予特定使用者和群組，以提供 COPY 和 UNLOAD 操作角色的存取權。如需詳細資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的 [GRANT](#)。

建立 IAM 角色以允許您的 Amazon Redshift 叢集存取 AWS 服務

若要建立 IAM 角色以允許 Amazon Redshift 叢集代表您與其他 AWS 服務進行通訊，請採取下列步驟。本節中使用的值是範例，您可以根據需要選擇值。

若要建立 IAM 角色以允許 Amazon Redshift 存取 AWS 服務

1. 開啟 [IAM 主控台](#)。
2. 在導覽窗格中，選擇 Roles (角色)。
3. 選擇 Create Role (建立角色)。
4. 選擇 AWS 服務，然後選擇 Redshift。
5. 在選取您的使用案例下，選擇 Redshift – 可自訂，然後選擇下一步：許可。連接許可政策頁面隨即出現。
6. 舉例來說，若要使用 COPY 存取 Amazon S3，您可以使用 **AmazonS3ReadOnlyAccess** 和 **append**。若要使用 COPY 或 UNLOAD 存取 Amazon S3，我們建議您建立受管政策，以便相應地限制對所需儲存貯體和字首的存取。對於讀取和寫入操作，我們建議您強制執行最低權限並僅限用於 Amazon Redshift 所需的 Amazon S3 儲存貯體和索引鍵字首。

如需為 CREATE EXTERNAL FUNCTION 命令調用 Lambda 函數的存取權，請新增 **AWSLambdaRole**。

對於 Redshift Spectrum，除了 Amazon S3 存取之外，另請新增 **AWSGlueConsoleFullAccess** 或 **AmazonAthenaFullAccess**。

選擇下一步：標籤。

7. Add tags (新增標籤) 頁面隨即出現。您可以選擇性地新增標籤。選擇下一步：檢閱。
8. 針對 Role name (角色名稱)，輸入您的角色名稱，例如 **RedshiftCopyUnload**。選擇建立角色。
9. 新角色適用於叢集上使用該角色的所有使用者。若要限制只有特定叢集上的特定使用者或特定區域中的叢集可存取，請編輯角色的信任關係。如需詳細資訊，請參閱 [限制對 IAM 角色的存取](#)。

10. 將角色與叢集相關聯。您可在建立叢集或新增角色至現有叢集時將 IAM 角色與叢集相關聯。如需詳細資訊，請參閱 [將 IAM 角色與叢集建立關聯](#)。

Note

若要限制對特定資料的存取權，請使用授予所需最低權限的 IAM 角色。

限制對 IAM 角色的存取

根據預設，Amazon Redshift 叢集上可用的 IAM 角色適用於該叢集上所有的使用者。但您可以選擇將 IAM 角色限制為只有特定叢集上的特定 Amazon Redshift 資料庫使用者或特定區域可存取。

若只要允許特定資料庫使用者使用 IAM 角色，請遵循以下步驟。

識別可存取 IAM 角色的特定資料庫使用者

1. 識別 Amazon Redshift 叢集中資料庫使用者的 Amazon Resource Name (ARN)。資料庫使用者的 ARN 格式如下：`arn:aws:redshift:region:account-id:dbuser:cluster-name/user-name`。

對於 Amazon Redshift Serverless，請使用以下 ARN 格式。`arn:aws:redshift:region:account-id:dbuser:workgroup-name/user-name`

2. 開啟 [IAM 主控台](#)。
3. 在導覽窗格中，選擇 Roles (角色)。
4. 選擇您想要限制只有特定 Amazon Redshift 資料庫使用者可存取的 IAM 角色。
5. 選擇 Trust Relationships (信任關係) 索引標籤，然後選擇 Edit Trust Relationship (編輯信任關係)。可讓 Amazon Redshift 代表您存取其他 AWS 服務的新 IAM 角色具有信任關係，如下所示：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "redshift.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

```

]
}

```

6. 新增條件至信任關係的 `sts:AssumeRole` 動作區段，將 `sts:ExternalId` 欄位限制在您所指定的值。包含您想要授予角色存取之各資料庫使用者的 ARN。外部 ID 可以是任何唯一的字串。

例如，以下的信任關係指定只有 `user1` 區域中 `user2` 叢集上的 `my-cluster` 和 `us-west-2` 資料庫使用者有使用此 IAM 角色的許可。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "redshift.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "sts:ExternalId": [
            "arn:aws:redshift:us-west-2:123456789012:dbuser:my-cluster/user1",
            "arn:aws:redshift:us-west-2:123456789012:dbuser:my-cluster/user2"
          ]
        }
      }
    }
  ]
}

```

7. 選擇 Update Trust Policy (更新信任政策)。

將 IAM 角色限制在 AWS 區域

您可以限制 IAM 角色只能在特定 AWS 區域中存取。根據預設，Amazon Redshift 的 IAM 角色不受限於任何單一區域。

若要限制區域可使用的 IAM 角色，請遵循以下步驟。

識別 IAM 角色的允許區域

1. 在 <https://console.aws.amazon.com/> 開啟 [身分與存取管理主控台](#)。
2. 在導覽窗格中，選擇角色。

3. 選擇您想要針對特定區域修改的角色。
4. 選擇 Trust Relationships (信任關係) 索引標籤，然後選擇 Edit Trust Relationship (編輯信任關係)。可讓 Amazon Redshift 代表您存取其他 AWS 服務的新 IAM 角色具有信任關係，如下所示：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "redshift.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

5. 搭配您想要允許使用角色的特定區域清單，修改 Service 的 Principal 清單。Service 清單中的各區域必須使用下列格式：`redshift.region.amazonaws.com`。

例如，以下經編輯後的信任關係僅允許在 `us-east-1` 和 `us-west-2` 區域使用 IAM 角色。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "redshift.us-east-1.amazonaws.com",
          "redshift.us-west-2.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

6. 選取 Update Trust Policy (更新信任政策)

在 Amazon Redshift 中鏈結 IAM 角色

將角色附加到叢集時，您的叢集可以擔任該角色來存取 Amazon S3、Amazon Athena AWS Glue，並 AWS Lambda 代表您存取。如果連接至叢集的角色無法存取必要資源，您可鏈結其他角色，該角色甚至可以來自其他帳戶。您的叢集接著會暫時擔任鏈結的角色，以存取資料。您也可以用鏈結角色的方式來授予跨帳戶存取。鏈結中的每個角色都會擔任鏈結中的下一個角色，直到叢集擔任鏈結尾端的角色為止。您可建立關聯的 IAM 角色數量上限需符合配額。如需詳細資訊，請參閱中的配額「讓 Amazon Redshift 存取其他 AWS 服務的叢集 IAM 角色」。 [Amazon Redshift 物件的配額](#)

例如，假設 A 公司想要存取屬於 B 公司的 Amazon S3 儲存貯體中的資料，為命名的 Amazon Redshift 建立 AWS 服務角色，RoleA 並將其附加到其叢集。B 公司應建立一個名為 RoleB 的角色，允許其存取 B 公司儲存貯體內的資料。若要存取 B 公司儲存貯體內的資料，A 公司應使用鏈結 iam_role 和 RoleA 的 RoleB 參數執行 COPY 命令。在 COPY 操作期間，RoleA 會暫時擔任 RoleB，以存取 Amazon S3 儲存貯體。

若要鏈結角色，您應建立角色間的信任關係。擔任其他角色的角色 (例如 RoleA) 必須擁有許可政策，允許其擔任下一個鏈結的角色 (例如 RoleB)。另一方面，要傳送許可的角色 (RoleB) 必須擁有信任政策，允許其將許可傳送給上一個鏈結的角色 (RoleA)。如需詳細資訊，請參閱《IAM 使用者指南》中的 [使用 IAM 角色](#)。

鏈結中的第一個角色必須為連接至叢集的角色。第一個角色，以及擔任鏈結中下一個角色的每個後續角色，必須擁有加入特定陳述式的政策。此陳述式對 Allow 動作和 sts:AssumeRole 元素中下一個角色的 Amazon Resource Name (ARN) 有 Resource 的效果。在我們的範例中，RoleA 具有下列許可政策，允許其擔任 AWS 帳戶 210987654321 的 RoleB。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1487639602000",
      "Effect": "Allow",
      "Action": [
        "sts:AssumeRole"
      ],
      "Resource": "arn:aws:iam::210987654321:role/RoleB"
    }
  ]
}
```


傳遞給其他角色的角色必須與擔任該角色的角色或擁有該角色的 AWS 帳戶建立信任關係。在我們的範例中，RoleB 擁有下列與 RoleA 建立信任關係的信任政策。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Principal": {
        "AWS": "arn:aws:iam::role/RoleA"
      }
    }
  ]
}
```

下列信任原則會與 AWS 帳戶的RoleA擁有人建立信任關係123456789012。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:root"
      }
    }
  ]
}
```

Note

若要將角色鏈結授權限制為特定使用者，請定義條件。如需詳細資訊，請參閱 [限制對 IAM 角色的存取](#)。

執行 UNLOAD、COPY、CREATE EXTERNAL FUNCTION 或 CREATE EXTERNAL SCHEMA 命令時，您應將逗號分隔的角色 ARN 清單加入到 iam_role 參數內，以鏈結角色。以下顯示 iam_role 參數中鏈結角色的語法。

```
unload ('select * from venue limit 10')
to 's3://acmedata/redshift/venue_pipe_'
IAM_ROLE 'arn:aws:iam::<aws-account-id-1>:role/<role-name-1>[,arn:aws:iam::<aws-account-id-2>:role/<role-name-2>][,...]';
```

Note

整個角色鏈結用單引號括住，且不得包含空格。

在下列範例中，RoleA 連接到屬於 AWS 帳戶 123456789012 的叢集。RoleB (屬於帳戶 210987654321) 具備許可存取名為 s3://companyb/redshift/ 的儲存貯體。下列範例鏈結 RoleA 和 RoleB，將資料 UNLOAD (卸載) 到 s3://companyb/redshift/ 儲存貯體。

```
unload ('select * from venue limit 10')
to 's3://companyb/redshift/venue_pipe_'
iam_role 'arn:aws:iam::123456789012:role/RoleA,arn:aws:iam::210987654321:role/RoleB';
```

以下範例使用 COPY 命令載入在上一範例中卸載的資料。

```
copy venue
from 's3://companyb/redshift/venue_pipe_'
iam_role 'arn:aws:iam::123456789012:role/RoleA,arn:aws:iam::210987654321:role/RoleB';
```

在以下範例中，CREATE EXTERNAL SCHEMA 使用鏈結的角色來擔任 RoleB 角色。

```
create external schema spectrumexample from data catalog
database 'exampledb' region 'us-west-2'
iam_role 'arn:aws:iam::123456789012:role/RoleA,arn:aws:iam::210987654321:role/RoleB';
```

在以下範例中，CREATE EXTERNAL FUNCTION 使用鏈結的角色來擔任 RoleB 角色。

```
create external function lambda_example(varchar)
returns varchar
volatile
lambda 'exampleLambdaFunction'
iam_role 'arn:aws:iam::123456789012:role/RoleA,arn:aws:iam::210987654321:role/RoleB';
```

其他資訊

如需詳細資訊，另請參閱[使用 IAM 角色授權 COPY、UNLOAD、CREATE EXTERNAL FUNCTION 和 CREATE EXTERNAL SCHEMA 操作](#)。

使用 IAM 角色授權 COPY、UNLOAD、CREATE EXTERNAL FUNCTION 和 CREATE EXTERNAL SCHEMA 操作

您可以用 [COPY](#) 命令將資料載入 (或匯入) Amazon Redshift，也能使用 [UNLOAD](#) 命令從 Amazon Redshift 卸載 (或匯出) 資料。您可以使用「建立外部函數」指令來建立使用者定義的函數，從中叫用函數 AWS Lambda。

使用 Amazon Redshift Spectrum 時，您可以使用 [CREATE EXTERNAL SCHEMA](#) 命令指定 Amazon S3 儲存貯體的位置 (其中包含您資料)。執行 COPY、UNLOAD 或 CREATE EXTERNAL SCHEMA 命令時，您必須提供安全憑證。這些憑證會授權 Amazon Redshift 叢集對您的目標目的地 (例如 Amazon S3 儲存貯體) 讀取或寫入資料。

執行 CREATE EXTERNAL FUNCTION 時，您可以使用 IAM 角色參數提供安全憑證。這些登入資料會授權您的 Amazon Redshift 叢集從中 AWS Lambda 叫用 Lambda 函數。提供安全登入資料的慣用方法是指定 AWS Identity and Access Management (IAM) 角色。對於 COPY 和 UNLOAD，您可以提供臨時憑證。如需有關建立 IAM 角色的詳細資訊，請參閱[授權 Amazon Redshift 代表您訪問其他 AWS 服務](#)。

如果使用者想要與 AWS 之外的 AWS Management Console 授與程式設計存取 AWS 取權的方式取決於正在存取的使用者類型。

若要授與使用者程式設計存取權，請選擇下列其中一個選項。

哪個使用者需要程式設計存取權？	到	By
人力身分 (IAM Identity Center 中管理的使用者)	使用臨時登入資料來簽署對 AWS CLI、AWS SDK 或 AWS API 的程式設計要求。	請依照您要使用的介面所提供的指示操作。 <ul style="list-style-type: none"> 如需詳細資訊 AWS CLI，請參閱《使 AWS CLI 用 AWS Command Line Interface 者指南》 AWS IAM Identity Center 中的〈配置使用〉。

哪個使用者需要程式設計存取權？	到	By
		<ul style="list-style-type: none"> 如需 AWS SDK、工具和 AWS API，請參閱 AWS SDK 和工具參考指南中的 IAM 身分中心身分驗證。
IAM	使用臨時登入資料來簽署對 AWS CLI、AWS SDK 或 AWS API 的程式設計要求。	遵循《IAM 使用者指南 》中的 〈將臨時登入資料搭配 AWS 資源使用〉 中的指示
IAM	(不建議使用) 使用長期認證來簽署對 AWS CLI、AWS SDK 或 AWS API 的程式設計要求。	<p>請依照您要使用的介面所提供的指示操作。</p> <ul style="list-style-type: none"> 如需相關資訊 AWS CLI，請參閱使用指南中的 使用 IAM 使用者登入資料進行驗證。AWS Command Line Interface 對於 AWS SDK 和工具，請參閱 AWS SDK 和工具參考指南中的 使用長期憑據進行身份驗證。 如需 AWS API，請參閱 IAM 使用者指南中的 管理 IAM 使用者的存取金鑰。

使用 IAM 角色的步驟如下：

- 建立要用於 Amazon Redshift 叢集的 IAM 角色。
- 將 IAM 角色與叢集相關聯。
- 呼叫 COPY、UNLOAD、CREATE EXTERNAL SCHEMA 或 CREATE EXTERNAL FUNCTION 命令時，請加入 IAM 角色的 ARN。

在本主題中，您將了解如何將 IAM 角色與 Amazon Redshift 叢集相關聯。

將 IAM 角色與叢集建立關聯

建立 IAM 角色來授權 Amazon Redshift 代表您存取其他 AWS 服務後，您必須將該角色與 Amazon Redshift 叢集相關聯。您必須執行這項作業，才能使用該角色來載入或卸載資料。

將 IAM 角色與叢集建立關聯所需的許可

若要將 IAM 角色與叢集相關聯，使用者必須擁有該 IAM 角色的 `iam:PassRole` 許可。管理員可以運用此許可，限制使用者可將哪些 IAM 角色與 Amazon Redshift 叢集相關聯。我們建議的最佳實務是，將許可政策連接到 IAM 角色，然後根據需要將其指派給使用者和群組。如需詳細資訊，請參閱 [Amazon Redshift 中的身分和存取管理](#)。

以下範例顯示可連接到使用者的 IAM 政策，以允許使用者採取下列動作：

- 取得該使用者帳戶所擁有之所有 Amazon Redshift 叢集的詳細資訊。
- 將任何三個 IAM 角色與兩個 Amazon Redshift 叢集中的任一個相關聯。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "redshift:DescribeClusters",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "redshift:ModifyClusterIamRoles",
        "redshift:CreateCluster"
      ],
      "Resource": [
        "arn:aws:redshift:us-east-1:123456789012:cluster:my-redshift-cluster",
        "arn:aws:redshift:us-east-1:123456789012:cluster:my-second-redshift-
cluster"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": [
        "arn:aws:iam::123456789012:role/MyRedshiftRole",
```

```
        "arn:aws:iam::123456789012:role/SecondRedshiftRole",
        "arn:aws:iam::123456789012:role/ThirdRedshiftRole"
    ]
}
]
```

使用者取得適當的許可後，該使用者可以將 IAM 角色與 Amazon Redshift 叢集相關聯。然後，IAM 角色就能使用 COPY 或 UNLOAD 命令，或是其他 Amazon Redshift 命令。

如需 IAM 政策的相關資訊，請參閱《IAM 使用者指南》中的 [IAM 政策概觀](#)。

管理 IAM 角色與叢集的關聯

您可以在建立叢集時將 IAM 角色與 Amazon Redshift 叢集相關聯。您也可以修改現有的叢集，並新增或移除一或多個 IAM 角色關聯。

請注意以下事項：

- 您可建立關聯的 IAM 角色數量上限需符合配額。
- IAM 角色可以與多個 Amazon Redshift 叢集相關聯。
- 只有當 IAM 角色和叢集都屬於同一個 AWS 帳戶時，IAM 角色才能與 Amazon Redshift 叢集建立關聯。

使用主控台管理 IAM 角色關聯

您可在主控台中使用下列程序管理叢集的 IAM 角色關聯。

管理 IAM 角色關聯

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽功能表上，選擇叢集，然後選擇您要更新的叢集。
3. 針對 Actions (動作)，選擇 Manage IAM roles (管理 IAM 角色) 以顯示與叢集相關聯的目前 IAM 角色清單。
4. 在 Manage IAM roles (管理 IAM 角色) 頁面上，選擇要新增的可用 IAM 角色，然後選擇 Add IAM role (新增 IAM 角色)。
5. 選擇 Done (完成) 以儲存變更。

使用管 AWS CLI 理 IAM 角色關聯

您可以使用下列方法 AWS CLI 來管理叢集的 IAM 角色關聯。

使用將 IAM 角色與叢集產生關聯 AWS CLI

若要在建立叢集時將 IAM 角色與叢集相關聯，請用 `--iam-role-arns` 命令的 `create-cluster` 參數指定 IAM 角色的 Amazon Resource Name (ARN)。您在呼叫 `create-cluster` 命令時可新增的 IAM 角色數量上限需符合配額。

IAM 角色與 Amazon Redshift 叢集的相關聯和取消關聯是非同步的程序。您可呼叫 `describe-clusters` 命令，以取得所有 IAM 角色叢集關聯的狀態。

以下範例將兩個 IAM 角色與名為 `my-redshift-cluster` 的新建立叢集相關聯。

```
aws redshift create-cluster \  
  --cluster-identifier "my-redshift-cluster" \  
  --node-type "ra3.4xlarge" \  
  --number-of-nodes 16 \  
  --iam-role-arns "arn:aws:iam::123456789012:role/RedshiftCopyUnload" \  
                  "arn:aws:iam::123456789012:role/SecondRedshiftRole"
```

若要將 IAM 角色與現有的 Amazon Redshift 叢集建立關聯，請在 `modify-cluster-iam-roles` 命令的 `--add-iam-roles` 參數中，指定 IAM 角色的 Amazon Resource Name (ARN)。您在呼叫 `modify-cluster-iam-roles` 命令時可新增的 IAM 角色數量上限需符合配額。

以下範例將一個 IAM 角色與名為 `my-redshift-cluster` 的現有叢集相關聯。

```
aws redshift modify-cluster-iam-roles \  
  --cluster-identifier "my-redshift-cluster" \  
  --add-iam-roles "arn:aws:iam::123456789012:role/RedshiftCopyUnload"
```

使用取消 IAM 角色與叢集的關聯 AWS CLI

若要將 IAM 角色與叢集取消關聯，請用 `modify-cluster-iam-roles` 命令的 `--remove-iam-roles` 參數指定 IAM 角色的 ARN。您在呼叫 `modify-cluster-iam-roles` 命令時可移除的 IAM 角色數量上限需符合配額。

下列範例會從名為的叢集中移除123456789012 AWS 帳戶 IAM 角色的關聯`my-redshift-cluster`。

```
aws redshift modify-cluster-iam-roles \  
  --cluster-identifier "my-redshift-cluster" \  
  --remove-iam-roles "arn:aws:iam::123456789012:role/RedshiftCopyUnload"
```

列出叢集的 IAM 角色關聯 AWS CLI

若要列出與 Amazon Redshift 叢集相關聯的所有 IAM 角色，以及 IAM 角色關聯的狀態，請呼叫 `describe-clusters` 命令。IamRoles 清單會傳回與叢集關聯之每個 IAM 角色的 ARN，如下列輸出範例所示。

已經與叢集相關聯的角色狀態會顯示為 `in-sync`。正在與叢集相關聯的角色狀態會顯示為 `adding`。正在與叢集取消關聯的角色狀態會顯示為 `removing`。

```
{  
  "Clusters": [  
    {  
      "ClusterIdentifier": "my-redshift-cluster",  
      "NodeType": "ra3.4xlarge",  
      "NumberOfNodes": 16,  
      "IamRoles": [  
        {  
          "IamRoleArn": "arn:aws:iam::123456789012:role/MyRedshiftRole",  
          "IamRoleApplyStatus": "in-sync"  
        },  
        {  
          "IamRoleArn": "arn:aws:iam::123456789012:role/SecondRedshiftRole",  
          "IamRoleApplyStatus": "in-sync"  
        }  
      ],  
      ...  
    },  
    {  
      "ClusterIdentifier": "my-second-redshift-cluster",  
      "NodeType": "ra3.4xlarge",  
      "NumberOfNodes": 10,  
      "IamRoles": [  
        {  
          "IamRoleArn": "arn:aws:iam::123456789012:role/MyRedshiftRole",  
          "IamRoleApplyStatus": "in-sync"  
        },  
        {
```



```
        "IamRoleArn": "arn:aws:iam::123456789012:role/SecondRedshiftRole",
        "IamRoleApplyStatus": "in-sync"
    },
    {
        "IamRoleArn": "arn:aws:iam::123456789012:role/ThirdRedshiftRole",
        "IamRoleApplyStatus": "in-sync"
    }
],
...
}
]
```

若要取得有關使用的更多資訊 AWS CLI，請參閱[AWS CLI 使用指南](#)。

建立 IAM 角色做為 Amazon Redshift 的預設角色

當您透過 Redshift 主控台建立 IAM 角色時，Amazon Redshift 會以程式設計方式在您的角色中建立角色，AWS 帳戶 並自動將現有的 AWS 受管政策附加到這些角色。此方法意味著您可以保留在 Redshift 主控台內，而不必切換到 IAM 主控台來建立角色。若要對在 Amazon Redshift 主控台中建立的現有 IAM 角色進行更精細的許可控制，您可以將自訂的受管政策連接到 IAM 角色。

在主控台中建立的 IAM 角色概觀

當您使用 Amazon Redshift 主控台建立 IAM 角色時，Amazon Redshift 會追蹤透過主控台建立的所有 IAM 角色。Amazon Redshift 會預先選取最新的預設 IAM 角色，以建立所有新叢集和從快照還原叢集。

您可以透過主控台建立 IAM 角色，該角色有權執行 SQL 命令的政策。這些命令包括 COPY、UNLOAD、CREATE EXTERNAL FUNCTION、CREATE EXTERNAL TABLE、CREATE EXTERNAL SCHEMA、CREATE MODEL 或 CREATE LIBRARY。或者，您可以透過建立自訂政策並將其連接到 IAM 角色，進而更精細地控制使用者對 AWS 資源的存取權限。

使用主控台建立 IAM 角色並將其設定為叢集預設值時，您不必提供 IAM 角色的 Amazon Resource Name (ARN) 即可執行驗證和授權。

使用在主控台中建立的 IAM 角色

您透過主控台為叢集建立的 IAM 角色會自動連接 AmazonRedshiftAllCommandsFullAccess 受管政策。這個 IAM 角色可讓 Amazon Redshift 針對 IAM 帳戶中的資源複製、卸載、查詢和分析

AWS 資料。受管政策可讓您存取 [COPY](#)、[UNLOAD](#)、[CREATE EXTERNAL FUNCTION](#)、[CREATE EXTERNAL SCHEMA](#)、[CREATE MODEL](#) 和 [CREATE LIBRARY](#) 操作。該政策還授予對相關 AWS 服務執行 SELECT 陳述式的許可，例如 Amazon S3、Amazon CloudWatch 日誌 SageMaker、Amazon 和 AWS Glue。

CREATE EXTERNAL FUNCTION、CREATE EXTERNAL SCHEMA、CREATE MODEL 和 CREATE LIBRARY 命令有 default 關鍵字。對於這些命令的這個關鍵字，Amazon Redshift 會使用設定為預設值且在命令執行時與叢集關聯的 IAM 角色。您可以執行 [DEFAULT_IAM_ROLE](#) 命令來檢查目前已連接到叢集的 IAM 角色。

若要控制建立的 IAM 角色的存取權限，並將其設定為 Redshift 叢集的預設值，請使用 ASSUMEROLE 權限。此存取控制適用於資料庫使用者和群組執行命令 (例如前面列出的命令)。將 ASSUMEROLE 權限授予 IAM 角色的使用者或群組之後，使用者或群組就可以在執行這些命令時擔任該角色。透過使用 ASSUMEROLE 權限，您可以視需要授予適當命令的存取權。

使用 Amazon Redshift 主控台，您可以執行以下操作：

- [建立 IAM 角色做為預設角色](#)
- [從叢集移除 IAM 角色](#)
- [將 IAM 角色與叢集建立關聯](#)
- [將 IAM 角色設定為預設角色](#)
- [讓 IAM 角色不再是叢集的預設角色](#)

AmazonRedshiftAllCommandsFullAccess 受管理策略的權限

下列範例顯示 AmazonRedshiftAllCommandsFullAccess 受管政策中的許可，這些許可允許針對設定為叢集預設的 IAM 角色執行某些動作。連接了許可政策的 IAM 角色授權使用者或群組可以執行和不能執行的操作。有了這些許可，您可以從 Amazon S3 執行 COPY 命令、執行 UNLOAD，然後使用 CREATE MODEL 命令。

```
{
    "Effect": "Allow",
    "Action": [
        "s3:GetObject",
        "s3:GetBucketAcl",
        "s3:GetBucketCors",
        "s3:GetEncryptionConfiguration",
        "s3:GetBucketLocation",
```

```

        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:ListMultipartUploadParts",
        "s3:ListBucketMultipartUploads",
        "s3:PutObject",
        "s3:PutBucketAcl",
        "s3:PutBucketCors",
        "s3:DeleteObject",
        "s3:AbortMultipartUpload",
        "s3:CreateBucket"
    ],
    "Resource": [
        "arn:aws:s3:::redshift-downloads",
        "arn:aws:s3:::redshift-downloads/*",
        "arn:aws:s3::*redshift*",
        "arn:aws:s3::*redshift/*"
    ]
}

```

下列範例顯示 AmazonRedshiftAllCommandsFullAccess 受管政策中的許可，這些許可允許針對設定為叢集預設的 IAM 角色執行某些動作。連接了許可政策的 IAM 角色授權使用者或群組可以執行和不能執行的操作。根據下列許可，您可以執行 CREATE EXTERNAL FUNCTION 命令。

```

{
  "Action": [
    "lambda:InvokeFunction"
  ],
  "Resource": "arn:aws:lambda:*:*:function:*redshift*"
}

```

下列範例顯示 AmazonRedshiftAllCommandsFullAccess 受管政策中的許可，這些許可允許針對設定為叢集預設的 IAM 角色執行某些動作。連接了許可政策的 IAM 角色授權使用者或群組可以執行和不能執行的操作。有了下列許可，您就可以執行 Amazon Redshift Spectrum 所需的 CREATE EXTERNAL SCHEMA 和 CREATE EXTERNAL TABLE 命令。

```

{
  "Effect": "Allow",
  "Action": [
    "glue:CreateDatabase",
    "glue>DeleteDatabase",
    "glue:GetDatabase",
    "glue:GetDatabases",

```

```

        "glue:UpdateDatabase",
        "glue:CreateTable",
        "glue>DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:GetTable",
        "glue:GetTables",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue>DeletePartition",
        "glue:BatchDeletePartition",
        "glue:UpdatePartition",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:BatchGetPartition"
    ],
    "Resource": [
        "arn:aws:glue:*:*:table/*redshift*/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*redshift*"
    ]
}

```

下列範例顯示 AmazonRedshiftAllCommandsFullAccess 受管政策中的許可，這些許可允許針對設定為叢集預設的 IAM 角色執行某些動作。連接了許可政策的 IAM 角色授權使用者或群組可以執行和不能執行的操作。有了下列許可，您就可以使用聯合查詢執行 CREATE EXTERNAL SCHEMA 命令。

```

{
    "Effect": "Allow",
    "Action": [
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecretVersionIds"
    ],
    "Resource": [
        "arn:aws:secretsmanager:*:*:secret:*Redshift*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "secretsmanager:GetRandomPassword",

```

```
        "secretsmanager:ListSecrets"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "secretsmanager:ResourceTag/Redshift": "true"
        }
    }
},
```

使用主控台管理為叢集建立的 IAM 角色

若要建立、修改和移除從 Amazon Redshift 主控台建立的 IAM 角色，請使用主控台內的叢集區段。

建立 IAM 角色做為預設角色

在主控台上，您可以為叢集建立自動連接 AmazonRedshiftAllCommandsFullAccess 政策的 IAM 角色。您建立的新 IAM 角色可讓 Amazon Redshift 複製、載入、查詢和分析 IAM 帳戶中 Amazon 資源中的資料。

只能將一個 IAM 角色設定為叢集的預設角色。如果在目前將現有 IAM 角色指派為預設值時，建立另一個 IAM 角色做為叢集預設角色，則新的 IAM 角色會取代另一個角色作為預設角色。

建立新叢集和設定為新叢集預設值的 IAM 角色

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽選單上，選擇叢集。AWS 區域 會列出目前帳戶的叢集。每個叢集的屬性子集會在清單中分欄顯示。
3. 選擇 Create cluster (建立叢集) 以建立叢集。
4. 遵循主控台頁面說明以輸入 Cluster configuration (叢集組態) 的屬性。如需此步驟的相關資訊，請參閱 [建立叢集](#)。
5. (選用) 選擇載入範例資料將範例資料集載入 Amazon Redshift 叢集，以開始使用查詢編輯器查詢資料。

如果您在防火牆後，則資料庫連接埠必須是接受傳入連線的開放連接埠。

6. 遵循主控台頁面說明以輸入資料庫組態的屬性。
7. 在叢集許可下，從管理 IAM 角色中選擇建立 IAM 角色。
8. 選擇下列其中一種方法來指定 IAM 角色要存取的 Amazon S3 儲存貯體：

- 選擇不使用其他 Amazon S3 儲存貯體來建立 IAM 角色，而無需指定特定的 Amazon S3 儲存貯體。
 - 選擇任何 Amazon S3 儲存貯體，允許擁有 Amazon Redshift 叢集存取權的使用者也可以存取您的任何 Amazon S3 儲存貯體及其中的 AWS 帳戶內容。
 - 選擇特定的 Amazon S3 儲存貯體，以指定要建立的 IAM 角色具有存取許可的一或多個 Amazon S3 儲存貯體。然後從資料表中選擇一或多個 Amazon S3 儲存貯體。
9. 選擇建立 IAM 角色作為預設值。Amazon Redshift 會自動建立 IAM 角色，並將其設定為叢集的預設角色。
 10. 選擇 Create cluster (建立叢集) 以建立叢集。該叢集可能需要幾分鐘方可使用。

從叢集移除 IAM 角色

您可以從叢集移除一或多個 IAM 角色。

從叢集移除 IAM 角色

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽選單上，選擇叢集。AWS 區域 會列出目前帳戶的叢集。每個叢集的屬性子集會在清單中分欄顯示。
3. 選擇您要從中移除 IAM 角色的叢集。
4. 在叢集許可下，選擇一或多個要從叢集移除的 IAM 角色。
5. 在管理 IAM 角色中，選擇移除 IAM 角色。

將 IAM 角色與叢集建立關聯

您可以將一或多個 IAM 角色與叢集建立關聯。

將 IAM 角色與叢集產生關聯

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽選單上，選擇叢集。AWS 區域 會列出目前帳戶的叢集。每個叢集的屬性子集會在清單中分欄顯示。
3. 選擇您要與 IAM 角色建立關聯的叢集。

4. 在叢集許可下，選擇一或多個要與叢集建立關聯的 IAM 角色。
5. 從管理 IAM 角色中，選擇關聯 IAM 角色。
6. 選擇一個或多個 IAM 角色來與您的叢集建立關聯。
7. 選擇關聯 IAM 角色。

將 IAM 角色設定為預設角色

您可以將 IAM 角色設定為叢集的預設角色。

將 IAM 角色設為叢集的預設角色

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽選單上，選擇叢集。AWS 區域 會列出目前帳戶的叢集。每個叢集的屬性子集會在清單中分欄顯示。
3. 選擇您要設定預設 IAM 角色的叢集。
4. 在叢集許可下，從關聯的 IAM 角色中，選擇要設為叢集預設的 IAM 角色。
5. 在設定預設值下，選擇設為預設。
6. 出現提示時，選擇設定預設值以確認將指定的 IAM 角色設為預設角色。

讓 IAM 角色不再是叢集的預設角色

您可以讓 IAM 角色不再做為叢集的預設角色。

清除 IAM 角色不再做為叢集預設的預設角色

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽選單上，選擇叢集。AWS 區域 會列出目前帳戶的叢集。每個叢集的屬性子集會在清單中分欄顯示。
3. 選擇您要與 IAM 角色建立關聯的叢集。
4. 在叢集許可下，從關聯的 IAM 角色中選擇預設 IAM 角色。
5. 在設定預設值下，選擇清除預設值
6. 出現提示時，選擇清除預設值以確認清除指定的 IAM 角色不再做為預設角色。

使用管理在叢集上建立的 IAM 角色 AWS CLI

您可以使用 AWS CLI 管理在叢集上建立的 IAM 角色。

建立 Amazon Redshift 叢集並將 IAM 角色設定為預設角色

若要使用 IAM 角色建立 Amazon Redshift 叢集，請將其設定為叢集的預設值，請使用以下 `aws redshift create-cluster` AWS CLI 命令。

以下 AWS CLI 命令會建立一個 Amazon Redshift 叢集和名為 `myrole1` 的 IAM 角色。此指 AWS CLI 命令也會將 `myrole1` 設定為叢集的預設值。

```
aws redshift create-cluster \  
  --node-type dc2.large \  
  --number-of-nodes 2 \  
  --master-username adminuser \  
  --master-user-password TopSecret1 \  
  --cluster-identifier mycluster \  
  --iam-roles 'arn:aws:iam::012345678910:role/myrole1'  
'arn:aws:iam::012345678910:role/myrole2' \  
  --default-iam-role-arn 'arn:aws:iam::012345678910:role/myrole1'
```

下列程式碼片段為回應範例。

```
{  
  "Cluster": {  
    "ClusterIdentifier": "mycluster",  
    "NodeType": "dc2.large",  
    "MasterUsername": "adminuser",  
    "DefaultIamRoleArn": "arn:aws:iam::012345678910:role/myrole1",  
    "IamRoles": [  
      {  
        "IamRoleArn": "arn:aws:iam::012345678910:role/myrole1",  
        "ApplyStatus": "adding"  
      },  
      {  
        "IamRoleArn": "arn:aws:iam::012345678910:role/myrole2",  
        "ApplyStatus": "adding"  
      }  
    ]  
    ...  
  }  
}
```



```
}
```

將一或多個 IAM 角色新增至 Amazon Redshift 叢集

若要新增與叢集相關聯的一或多個 IAM 角色，請使用 `aws redshift modify-cluster-iam-roles` AWS CLI 指令。

下列 AWS CLI 命令會將 `myrole3` 和新增 `myrole4` 至叢集。

```
aws redshift modify-cluster-iam-roles \  
  --cluster-identifier mycluster \  
  --add-iam-roles 'arn:aws:iam::012345678910:role/myrole3'  
  'arn:aws:iam::012345678910:role/myrole4'
```

下列程式碼片段為回應範例。

```
{  
  "Cluster": {  
    "ClusterIdentifier": "mycluster",  
    "NodeType": "dc2.large",  
    "MasterUsername": "adminuser",  
    "DefaultIamRoleArn": "arn:aws:iam::012345678910:role/myrole1",  
    "IamRoles": [  
      {  
        "IamRoleArn": "arn:aws:iam::012345678910:role/myrole1",  
        "ApplyStatus": "in-sync"  
      },  
      {  
        "IamRoleArn": "arn:aws:iam::012345678910:role/myrole2",  
        "ApplyStatus": "in-sync"  
      },  
      {  
        "IamRoleArn": "arn:aws:iam::012345678910:role/myrole3",  
        "ApplyStatus": "adding"  
      },  
      {  
        "IamRoleArn": "arn:aws:iam::012345678910:role/myrole4",  
        "ApplyStatus": "adding"  
      }  
    ],  
    ...  
  }  
}
```

```
}
```

從 Amazon Redshift 叢集移除一或多個 IAM 角色

若要移除與叢集相關聯的一或多個 IAM 角色，請使用 `aws redshift modify-cluster-iam-roles` AWS CLI 指令。

下列 AWS CLI 命令會從叢集 `myrole4` 中移除 `myrole3` 和 `myrole4`。

```
aws redshift modify-cluster-iam-roles \  
  --cluster-identifier mycluster \  
  --remove-iam-roles 'arn:aws:iam::012345678910:role/myrole3'  
  'arn:aws:iam::012345678910:role/myrole4'
```

下列程式碼片段為回應範例。

```
{  
  "Cluster": {  
    "ClusterIdentifier": "mycluster",  
    "NodeType": "dc2.large",  
    "MasterUsername": "adminuser",  
    "DefaultIamRoleArn": "arn:aws:iam::012345678910:role/myrole1",  
    "IamRoles": [  
      {  
        "IamRoleArn": "arn:aws:iam::012345678910:role/myrole1",  
        "ApplyStatus": "in-sync"  
      },  
      {  
        "IamRoleArn": "arn:aws:iam::012345678910:role/myrole2",  
        "ApplyStatus": "in-sync"  
      },  
      {  
        "IamRoleArn": "arn:aws:iam::012345678910:role/myrole3",  
        "ApplyStatus": "removing"  
      },  
      {  
        "IamRoleArn": "arn:aws:iam::012345678910:role/myrole4",  
        "ApplyStatus": "removing"  
      }  
    ],  
    ...  
  }  
}
```

```
}
```

將關聯的 IAM 角色設定為叢集的預設角色

若要將關聯的 IAM 角色設定為叢集的預設角色，請使用 `aws redshift modify-cluster-iam-roles` AWS CLI 指令。

下列 AWS CLI 指令會設定 `myrole2` 為叢集的預設值。

```
aws redshift modify-cluster-iam-roles \  
  --cluster-identifier mycluster \  
  --default-iam-role-arn 'arn:aws:iam::012345678910:role/myrole2'
```

下列程式碼片段為回應範例。

```
{  
  "Cluster": {  
    "ClusterIdentifier": "mycluster",  
    "NodeType": "dc2.large",  
    "MasterUsername": "adminuser",  
    "DefaultIamRoleArn": "arn:aws:iam::012345678910:role/myrole2",  
    "IamRoles": [  
      {  
        "IamRoleArn": "arn:aws:iam::012345678910:role/myrole1",  
        "ApplyStatus": "in-sync"  
      },  
      {  
        "IamRoleArn": "arn:aws:iam::012345678910:role/myrole2",  
        "ApplyStatus": "in-sync"  
      }  
    ],  
    ...  
  }  
}
```

將未關聯的 IAM 角色設定為叢集的預設角色

若要將未關聯的 IAM 角色設定為叢集的預設角色，請使用 `aws redshift modify-cluster-iam-roles` AWS CLI 指令。

下列 AWS CLI 命令會新增 `myrole2` 至 Amazon Redshift 叢集，並將其設定為叢集的預設值。

```
aws redshift modify-cluster-iam-roles \  
  --cluster-identifier mycluster \  
  --add-iam-roles 'arn:aws:iam::012345678910:role/myrole3' \  
  --default-iam-role-arn 'arn:aws:iam::012345678910:role/myrole3'
```

下列程式碼片段為回應範例。

```
{  
  "Cluster": {  
    "ClusterIdentifier": "mycluster",  
    "NodeType": "dc2.large",  
    "MasterUsername": "adminuser",  
    "DefaultIamRoleArn": "arn:aws:iam::012345678910:role/myrole3",  
    "IamRoles": [  
      {  
        "IamRoleArn": "arn:aws:iam::012345678910:role/myrole1",  
        "ApplyStatus": "in-sync"  
      },  
      {  
        "IamRoleArn": "arn:aws:iam::012345678910:role/myrole2",  
        "ApplyStatus": "in-sync"  
      },  
      {  
        "IamRoleArn": "arn:aws:iam::012345678910:role/myrole3",  
        "ApplyStatus": "adding"  
      }  
    ],  
    ...  
  }  
}
```

從快照還原叢集並將 IAM 角色設定為其預設值

從快照還原叢集時，您可以關聯現有的 IAM 角色，也可以建立新的 IAM 角色並將其設定為叢集的預設角色。

若要從快照還原 Amazon Redshift 叢集，並將 IAM 角色設定為叢集預設值，請使用以下 `aws redshift restore-from-cluster-snapshot` AWS CLI 命令。

下列 AWS CLI 指令會從快照還原叢集，並將其設定 `myrole2` 為叢集的預設值。

```
aws redshift restore-from-cluster-snapshot \  
  --cluster-identifier mycluster \  
  --iam-role-arn 'arn:aws:iam::012345678910:role/myrole2'
```

```
--cluster-identifier mycluster-clone \  
--snapshot-identifier my-snapshot-id  
--iam-roles 'arn:aws:iam::012345678910:role/myrole1'  
'arn:aws:iam::012345678910:role/myrole2' \  
--default-iam-role-arn 'arn:aws:iam::012345678910:role/myrole1'
```

下列程式碼片段為回應範例。

```
{  
  "Cluster": {  
    "ClusterIdentifier": "mycluster-clone",  
    "NodeType": "dc2.large",  
    "MasterUsername": "adminuser",  
    "DefaultIamRoleArn": "arn:aws:iam::012345678910:role/myrole1",  
    "IamRoles": [  
      {  
        "IamRoleArn": "arn:aws:iam::012345678910:role/myrole1",  
        "ApplyStatus": "adding"  
      },  
      {  
        "IamRoleArn": "arn:aws:iam::012345678910:role/myrole2",  
        "ApplyStatus": "adding"  
      }  
    ],  
    ...  
  }  
}
```

使用聯合身分來管理 Amazon Redshift 對本機資源和 Amazon Redshift Spectrum 外部資料表的存取。

將聯合身分 AWS 與提供的認證一起使用 `GetDatabaseCredentials` 可以簡化對本機資料和外部資料的授權和存取。目前，為了讓使用者能夠存取 Amazon S3 中的外部資料，您可以使用許可政策中定義的許可來建立 IAM 角色。然後，具有連接角色的使用者可以存取外部資料。這是可行的，但如果您想提供精細的規則，例如讓特定使用者無法使用特定的欄，您可能必須對外部結構描述進行其他設定。在本主題中，我們將說明如何透過 AWS 身分聯合提供資源的存取權，而不是使用特定 IAM 角色。聯合身分識別 (透過提供的登入資料) 可透過更易於指定 AWS Glue 和變更的精細 IAM 規則 `GetDatabaseCredentials`，提供對 Redshift Spectrum 資源的存取權。這可讓您更輕鬆地應用符合業務規則的存取權限。

使用聯合憑證的好處如下：

- 您無需為 Redshift Spectrum 管理叢集連接的 IAM 角色。
- 叢集管理員可以建立具有不同 IAM 內容的消費者可存取的外部結構描述。舉例來說，這對於在資料表上執行欄篩選非常有用，其中不同的消費者查詢相同的外部結構描述，並在傳回的記錄中取得不同的欄位。
- 您可以使用具有 IAM 許可的使用者來查詢 Amazon Redshift，而不是僅使用某個角色。

準備身分以使用聯合身分登入

使用聯合身分登入之前，您必須先執行幾個初步步驟。這些說明假設您有一個現有的 Redshift Spectrum 外部結構描述，該結構描述參考儲存在 Amazon S3 儲存貯體中的資料檔案，且該儲存貯體與您的 Amazon Redshift 叢集或 Amazon Redshift Serverless 資料倉儲位於同一帳戶中。

1. 建立 IAM 身分。這可以是使用者或 IAM 角色。使用 IAM 支援的任何名稱。
2. 將許可政策連接至身分。指定下列任一項：
 - `redshift:GetClusterCredentialsWithIAM` (適用於 Amazon Redshift 佈建的叢集)
 - `redshift-serverless:GetCredentials` (適用於 Amazon Redshift Serverless)

您可以使用 IAM 主控台透過政策編輯器新增許可。

IAM 身分還需要許可才能存取外部資料。直接新增下列 AWS 受管政策，以授予對 Amazon S3 的存取權限：

- `AmazonS3ReadOnlyAccess`
- `AWSGlueConsoleFullAccess`

如果您使 AWS Glue 用準備外部資料，則需要最後一個受管理的政策。如需授予 Amazon Redshift Spectrum 存取權的步驟相關資訊，請參閱 [為 Amazon Redshift 建立 IAM 角色](#)，這是 Amazon Redshift 和 Redshift Spectrum 入門指南的一部分。它顯示了新增 IAM 政策以存取 Redshift Spectrum 的步驟。

3. 設定您的 SQL 用戶端以連接到 Amazon Redshift。使用 Amazon Redshift JDBC 驅動器，並將使用者的憑證新增至工具的憑證屬性。像 SQL Workbench/J 這樣的用戶端非常適合此目的。設定下列用戶端連線延伸屬性：
 - `AccessKeyID` — 您的存取金鑰識別碼。
 - `SecretAccessKey` 金鑰 — 您的秘密存取金鑰。(如果不使用加密，請注意傳輸金鑰的安全風險。)

- SessionToken— IAM 角色的一組臨時登入資料。
 - groupFederation - 如果您要為已佈建的叢集設定聯合身分，則設定為 true。如果您使用的是 Amazon Redshift Serverless，請勿設定此參數。
 - LogLevel— 整數記錄層級值。這是選用的。
4. 將 URL 設定為在 Amazon Redshift 或 Amazon Redshift Serverless 主控台中找到的 JDBC 端點。將您的 URL 結構描述替換為 jdbc:redshift:iam: 並使用以下格式：

- Amazon Redshift 佈建叢集的格式：`jdbc:redshift:iam://<cluster_id>.<unique_suffix>.<region>.redshift.amazonaws.com:<port>/<database_name>`

範例：`jdbc:redshift:iam://test1.12345abcdefg.us-east-1.redshift.amazonaws.com:5439/dev`

- Amazon Redshift Serverless 的格式：`jdbc:redshift:iam://<workgroup-name>.<account-number>.<aws-region>.redshift-serverless.amazonaws.com:5439:<port>/<database_name>`

範例：`jdbc:redshift:iam://default.123456789012.us-east-1.redshift-serverless.amazonaws.com:5439/dev`

在您第一次使用 IAM 身分連線到資料庫之後，Amazon Redshift 會自動建立具有相同名稱的 Amazon Redshift 身分，並為使用者加上 IAM: 字首或為 IAM 角色加上 IAMR: 字首。本主題中的其餘步驟顯示使用者的範例。

如果未自動建立 Redshift 使用者，您可以使用管理員帳戶執行 CREATE USER 陳述式，並以格式 IAM:<user name> 指定使用者名稱來建立一個使用者。

5. 身為 Amazon Redshift 叢集管理員，請授予 Redshift 使用者存取外部結構描述所需的許可。

```
GRANT ALL ON SCHEMA my_schema to "IAM:my_user";
```

若要授予 Redshift 使用者在外部結構描述中建立資料表的能力，他們必須是結構描述擁有者。例如：

```
ALTER SCHEMA my_schema owner to "IAM:my_user";
```

6. 若要驗證組態，請在授予許可之後，使用 SQL 用戶端以使用者身分執行查詢。此查詢範例會從外部資料表擷取資料。

```
SELECT * FROM my_schema.my_table;
```

開始將身分和授權傳播到 Redshift Spectrum

若要傳遞聯合身分來查詢外部資料表，請將 SESSION 設定為 CREATE EXTERNAL SCHEMA 的 IAM_ROLE 查詢參數值。下列步驟說明如何設定及運用 SESSION 來授權對外部結構描述進行查詢。

1. 建立本機資料表和外部資料表。為此編目的 AWS Glue 工作的外部表格。
2. 使用您的 IAM 身分連接到 Amazon Redshift。如上一節所述，當身分連接到 Amazon Redshift 時，便會建立一個 Redshift 資料庫使用者。如果先前不存在，則會建立使用者。如果使用者是新使用者，管理員必須授予他們在 Amazon Redshift 中執行任務 (例如查詢和建立資料表) 的許可。
3. 使用您的管理員帳戶連接到 Redshift。執行命令以使用 SESSION 值建立外部結構描述。

```
create external schema spectrum_schema from data catalog
database '<my_external_database>'
region '<my_region>'
iam_role 'SESSION'
catalog_id '<my_catalog_id>;'
```

請注意，在這種情況下會設定 catalog_id。這是與功能一起新增的設定，因為 SESSION 會取代特定角色。

在此範例中，查詢中的值模擬真實值的顯示方式。

```
create external schema spectrum_schema from data catalog
database 'spectrum_db'
region 'us-east-1'
iam_role 'SESSION'
catalog_id '123456789012'
```

在這種情況下，catalog_id 值是您的 AWS 帳戶 ID。

4. 使用您在步驟 2 中連接的 IAM 身分，執行查詢以存取外部資料。例如：

```
select * from spectrum_schema.table1;
```

在這種情況下，table1 可以是 Amazon S3 儲存貯體中檔案中的 JSON 格式資料。

5. 如果您已經擁有使用叢集連接 IAM 角色的外部結構描述 (指向外部資料庫或結構描述)，則可以取代現有結構描述並使用這些步驟中詳述的聯合身分，或建立新的結構描述。

SESSION 表示聯合身分憑證用於查詢外部結構描述。當您使用 SESSION 查詢參數時，請務必設定 `catalog_id`。這是必要的，因為它指向用於結構描述的資料目錄。先前，`catalog_id` 是從指派給 `iam_role` 的值中擷取。當您以這種方式設定身分識別和授權傳播時，例如，透過使用聯合憑證查詢外部結構描述，就不需要透過 IAM 角色進行授權。

使用須知

一個常見的連線錯誤如下：IAM 擷取臨時憑證時發生錯誤：無法使用提供的解組器取消封送異常回應。此錯誤是具有舊版 JDBC 驅動器的結果。聯合身分所需的最低驅動程式版本為 2.1.0.9。您可以從[下載 Amazon Redshift JDBC 驅動器 2.1 版](#)取得 JDBC 驅動器。

其他資源

這些連結提供管理外部資料存取權的其他資訊。

- 您仍然可以使用 IAM 角色存取 Redshift Spectrum 資料。如需詳細資訊，請參閱 [授權 Amazon Redshift 代表您訪問其他 AWS 服務](#)。
- 當您使用管理對外部資料表的存取時 AWS Lake Formation，您可以使用具有聯合身分識別身分的 Redshift Spectrum 來查詢外部資料表。您不再需要為 Redshift 頻譜管理叢集連接的 IAM 角色，就能查詢註冊的資料。AWS Lake Formation 如需詳細資訊，請參閱 [AWS Lake Formation 搭配 Amazon Redshift Spectrum 使用](#)。

使用管理 Amazon Redshift 管理員密碼 AWS Secrets Manager

Amazon Redshift 可與 AWS Secrets Manager 之整合，在加密密碼內產生和管理您的管理員登入資料。使用 AWS Secrets Manager，您可以使用 API 呼叫取代管理員密碼，以便在需要時以程式設計方式擷取密碼。使用機密而非硬式編碼憑證可降低這些憑證遭到洩露或遭到入侵的風險。若要取得有關的更多資訊 AWS Secrets Manager，請參閱 [AWS Secrets Manager 使用者指南](#)。

您可以指定 Amazon Redshift 在執行下列其中一項操作 AWS Secrets Manager 時使用管理員密碼來管理您的管理員密碼：

- 建立佈建叢集或無伺服器命名空間
- 從快照還原叢集或無伺服器命名空間

當您指定 Amazon Redshift 管理中的管理員密碼時 AWS Secrets Manager，Amazon Redshift 會生成密碼並將其存儲在 Secrets Manager 中。您可以直接在中存取密碼，AWS Secrets Manager 以擷取管理員使用者的認證。或者，如果您需要從其他帳戶存取密碼，您也可以指定客 AWS 戶管理的金鑰來加密密碼。您也可以使用 AWS Secrets Manager 提供的 KMS 金鑰。

Amazon Redshift 會管理機密的設定，並依預設每 30 天輪換一次密碼。您可以隨時手動輪換機密。如果您刪除管理密碼的佈建叢集或無伺服器命名空間 AWS Secrets Manager，則密碼及其關聯的中繼資料也會一併刪除。

若要使用機密管理的憑證來連線到叢集或無伺服器命名空間，您可以使用 Secrets Manager 主控台或 GetSecretValue Secrets Manager API 呼叫從 AWS Secrets Manager 擷取機密。如需詳細資訊，請參閱《AWS Secrets Manager 使用指南》中的使用[密 AWS Secrets Manager 碼中的認證從 SQL 資料庫擷取密碼 AWS Secrets Manager 和 Connect 到 SQL 資料庫](#)。

AWS Secrets Manager 整合所需的權限

使用者必須擁有必要的權限，才能執行與 AWS Secrets Manager 整合相關的作業。建立 IAM 政策，授予對其需要的指定資源執行特定 API 操作的許可。然後，將這些政策附加至需要這些許可的 IAM 許可集或角色。如需詳細資訊，請參閱 [Amazon Redshift 中的身分和存取管理](#)。

指定 Amazon Redshift 管理中管理管理員密碼的使用者 AWS Secrets Manager 必須具有執行下列操作的許可：

- `secretsmanager:CreateSecret`
- `secretsmanager:RotateSecret`
- `secretsmanager:DescribeSecret`
- `secretsmanager:UpdateSecret`
- `secretsmanager>DeleteSecret`
- `secretsmanager:GetRandomPassword`
- `secretsmanager:TagResource`

如果使用者想要在佈建叢集的 `MasterPasswordSecretKmsKeyId` 參數中傳遞 KMS 金鑰，或在無伺服器命名空間的 `AdminPasswordSecretKmsKeyId` 參數中傳遞 KMS 金鑰，除了上面所列的許可外，其還需要下列許可。

- `kms:Decrypt`
- `kms:GenerateDataKey`

- kms:CreateGrant
- kms:RetireGrant

輪換管理員密碼機密

根據預設，Amazon Redshift 會每 30 天自動輪換您的機密，以確保您的憑證不會長時間保持不變。當 Amazon Redshift 輪換管理員密碼密碼時，請 AWS Secrets Manager 更新現有密碼以包含新的管理員密碼。Amazon Redshift 會變更叢集的管理員密碼，以符合已更新之機密中的密碼。

您可以使用 AWS Secrets Manager 立即輪換機密，而無需等待排程的輪換。如需旋轉密碼的詳細資訊，請參閱《AWS Secrets Manager 使用指南》中的 [〈旋轉 AWS Secrets Manager 密碼〉](#)。

在 Amazon Redshift 中擷取機密的 Amazon Resource Name (ARN)

您可以使用 Amazon Redshift 主控台，檢視由 AWS Secrets Manager 管理之任何機密的 Amazon Resource Name (ARN)。獲得秘密的 ARN 後，您可以使 AWS Secrets Manager 用查看有關秘密和秘密中的加密數據的詳細信息。如需使用 ARN 擷取機密的相關資訊，請參閱《AWS Secrets Manager 使用者指南》中的 [擷取機密](#)。

檢視 Amazon Redshift 佈建叢集之機密的詳細資訊

請透過下列程序，使用 Amazon Redshift 主控台檢視叢集機密的 Amazon Resource Name (ARN)：

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台。
2. 在叢集概觀窗格中，選擇您要檢視其機密的叢集。
3. 選擇屬性索引標籤。
4. 在管理員憑證 ARN 下檢視機密的 ARN。此 ARN 是密碼的標識符，您可以在中使用它 AWS Secrets Manager 來查看密碼的詳細信息。

檢視 Amazon Redshift Serverless 命名空間之機密的詳細資訊

請透過下列程序，使用 Amazon Redshift 主控台檢視無伺服器命名空間機密的 Amazon Resource Name (ARN)：

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台。
2. 從佈建叢集儀表板中，選擇頁面右上角的前往無伺服器。
3. 在 Serverless 儀表板中，捲動至命名空間/工作群組窗格，然後選擇您要檢視其機密的命名空間。

4. 在一般資訊窗格中，於管理員憑證 ARN 下檢視機密的 ARN。此 ARN 是密碼的標識符，您可以在中使用它 AWS Secrets Manager 來查看密碼的詳細信息。

建立資料庫連線認證的密碼

您可以建立 Secrets Manager 碼來儲存用於連線至 Amazon Redshift 佈建叢集或 Redshift 無伺服器命名空間和工作群組的登入資料。您也可以 Amazon Redshift 查詢編輯器 v2 中排程查詢時使用此密碼。

使用秘密管理員主控台為 Amazon Redshift 佈建叢集中的資料庫建立密碼

1. 開啟 Secrets Manager 主控台 (<https://console.aws.amazon.com/secretsmanager/>)。
2. 瀏覽至密碼清單，然後選擇 [儲存新密碼]。
3. 選擇 Amazon Redshift 資料倉儲的登入資料。在建立密碼的步驟中輸入您的資訊，如下所示：
 - 在使用者名稱的認證中，輸入資料倉儲的管理使用者名稱。
 - 在密碼認證中，輸入使用者名稱的密碼。
 - 對於加密金鑰，請選擇您的加密金鑰。
 - 對於資料倉儲，請選擇包含您資料的 Amazon Redshift 佈建叢集。
 - 在密碼名稱中，輸入密碼的名稱。
 - 在說明中，輸入密碼的說明。
 - 在「標籤」中，輸入含有文字的標籤鍵 **Redshift**。當您嘗試使用 Amazon Redshift 查詢編輯器 v2 連線到資料倉儲時，需要此標籤金鑰才能列出機密。密碼必須具有標籤金鑰，該標籤金鑰必須以字串 **Redshift** 開頭，以便 AWS Secrets Manager 在管理主控台下列出密碼。
4. 透過數個步驟繼續輸入密碼的相關資訊，直到您在「檢閱」步驟中儲存變更為止。

認證、引擎、主機、連接埠和叢集識別碼的特定值會儲存在機密中。此外，秘密還使用標籤鍵標記 **Redshift**。

使用 Redshift 無伺服器主控台為 Redshift 無伺服器命名空間中的資料庫建立密碼

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 選擇 Redshift 無伺服器並瀏覽至命名空間組態。
3. 選擇要為其建立秘密證明資料的命名空間。

4. 打開操作，編輯管理員憑據。
5. 對於管理員密碼，請在中選擇管理員認證 AWS Secrets Manager。
6. 選擇儲存變更，以儲存您所做的變更。

確認出現密碼已成功變更的訊息。您也可以 Secret 管理員主控台中檢視密碼。您可以使用此密碼，使用連線方法連線至 Redshift 無伺服器主控台和 Amazon Redshift 查詢編輯器 v2 中工作群組中的 AWS Secrets Manager 資料庫。密碼必須具有以字串「Redshift」開頭的標籤金鑰，密碼才能在查詢編輯器 v2 Web 應用程式上列出。密碼必須具有標籤金鑰，該標籤金鑰必須以字串**Redshift**開頭，以便 AWS Secrets Manager 在管理主控台下列出密碼。

使用秘密管理員主控台為 Redshift 無伺服器命名空間中的資料庫建立密碼

1. 開啟 Secrets Manager 主控台 (<https://console.aws.amazon.com/secretsmanager/>)。
2. 瀏覽至密碼清單，然後選擇 [儲存新密碼]。
3. 選擇 Amazon Redshift 資料倉儲的登入資料。在建立密碼的步驟中輸入您的資訊，如下所示：
 - 在使用者名稱的認證中，輸入資料倉儲的管理使用者名稱。
 - 在密碼認證中，輸入使用者名稱的密碼。
 - 對於加密金鑰，請選擇您的加密金鑰。
 - 對於資料倉儲，請選擇包含資料的 Redshift 無伺服器命名空間。
 - 在密碼名稱中，輸入密碼的名稱。
 - 在說明中，輸入密碼的說明。
 - 在「標籤」中，輸入含有文字的標籤鍵**Redshift**。當您嘗試使用 Amazon Redshift 查詢編輯器 v2 連線到資料倉儲時，需要此標籤金鑰才能列出機密。密碼必須具有標籤金鑰，該標籤金鑰必須以字串**Redshift**開頭，以便 AWS Secrets Manager 在管理主控台下列出密碼。
4. 透過數個步驟繼續輸入密碼的相關資訊，直到您在「檢閱」步驟中儲存變更為止。

您的認證、資料庫名稱、主機、連接埠、命名空間和引擎的特定值會儲存在機密中。此外，秘密還使用標籤鍵標記**Redshift**。

若要在 Redshift 無伺服器命名空間中建立資料庫密碼，請使用 AWS CLI

您可以使 AWS CLI 用建立密碼。一種方法是使用 AWS CloudShell 如下運行 Secrets Manager AWS CLI 命令。您必須擁有適當的權限才能執行下列程序中顯示的 AWS CLI 命令。

1. 在 AWS 主控台上，開啟 AWS CloudShell 命令提示字元。若要取得有關的更多資訊 AWS CloudShell，請參閱《AWS CloudShell 使用指南》AWS CloudShell 中的內容。
2. 例如，對於密碼，MyTestSecret 請輸入 Secrets Manager 命令來儲存用於連線到資料庫或排程 Amazon Redshift 查詢編輯器 v2 查詢的密碼。將指令中的下列值取代為您環境的值：
 - `admin` 是資料倉儲的管理員使用者名稱。
 - `#`碼是管理員的密碼。
 - `dev` 是數據倉庫中的初始數據庫名稱。
 - `##`是包 AWS 區域 含數據倉庫。例如：`us-east-1`。
 - `123456789012` 是一個 AWS 帳戶
 - 命 `###-id ###` 於的命名空間標識符。 `c3928f0e-c889-4d2b-97a5-5738324d5d3e` 您可以在無伺服器命名空間的 Amazon Redshift 主控台詳細資訊頁面上找到此識別碼。

```
aws secretsmanager create-secret \  
--name MyTestSecret \  
--description "My test secret created with the CLI." \  
--secret-string "{\"username\":\"admin\",\"password\":\"password\",\"dbname\":\  
\"dev\",\"engine\":\"redshift\"}" \  
--tags "[{\"Key\":\"redshift-serverless:namespaceArn\",\"Value\":\  
\"arn:aws:redshift-serverless:region:123456789012:namespace/namespace-id\"}]"
```

使用 Amazon Redshift AWS Secrets Manager 的注意事項

使用 AWS Secrets Manager 來管理佈建的叢集或無伺服器命名空間的管理員認證時，請考慮下列事項：

- 當您暫停其管理認證由其管理員認證的叢集時 AWS Secrets Manager，不會刪除叢集的密碼，並繼續向您收取該密碼的費用。只有刪除叢集時才會刪除機密。
- 如果您的叢集在 Amazon Redshift 嘗試輪換其附加的機密時暫停了，輪換會失敗。在這種情況下，即使您繼續叢集，Amazon Redshift 還是會停止自動輪換，而且不會嘗試再次輪換。您必須使用 `secretsmanager:RotateSecret` API 呼叫重新啟動自動輪換排程，才能繼續 AWS Secrets Manager 自動輪替密碼。
- 如果在 Amazon Redshift 嘗試輪換其附加的機密時，您的無伺服器命名空間沒有相關聯的工作群組，則輪換會失敗，且不會嘗試再次輪換，即使在您附加工作群組之後也是如此。您必須使用

secretsmanager:RotateSecret API 呼叫重新啟動自動輪換排程，才能繼續 AWS Secrets Manager 自動輪替密碼。

在 Amazon Redshift 中記錄和監控

監控是維護 Amazon Redshift 及 AWS 解決方案的可靠性、可用性和效能所不可或缺。您可以從 AWS 解決方案各個部分收集監控資料，以便在發生多點失敗時，可更輕鬆地偵錯。AWS 提供多種工具，讓您監控 Amazon Redshift 資源及回應潛在的事件：

Amazon CloudWatch 警示

使用 Amazon CloudWatch 警示，您可在自己指定的一段時間內監看單一指標。如果指標超過指定的閾值，會傳送一則通知至 Amazon SNS 主題或 AWS Auto Scaling 政策。CloudWatch 警示不會因為處於特定狀態而叫用動作。必須是狀態已變更並維持了所指定的時間長度，才會呼叫動作。如需更多詳細資訊，請參閱 [管理警示](#)。如需指標的清單，請參閱 [使 CloudWatch 用指標監控 Amazon Redshift](#)。

AWS CloudTrail 日誌

對於使用者、IAM 角色或 AWS 服務在 Amazon Redshift 中採取的 API 操作，CloudTrail 會提供記錄。您可以利用 CloudTrail 所收集的資訊來判斷向 Amazon Redshift 發出的請求，以及發出請求的 IP 地址、人員、時間和其他詳細資訊。如需更多詳細資訊，請參閱 [使用記錄 CloudTrail](#)。

資料庫稽核記錄日誌

Amazon Redshift 會記錄您資料庫中連線和使用者活動的相關資訊。這些日誌可協助您基於安全和故障診斷之目的監控資料庫，此程序稱為資料庫稽核。日誌可以儲存在：

- Amazon S3 儲存貯體 — 這會讓負責監控資料庫中活動的使用者能夠存取資料安全功能。
- Amazon CloudWatch-您可以使用內建的功能 (例如視覺化功能和設定動 CloudWatch 作) 來檢視稽核記錄資料。

Note

[SYS_CONNECTION_LOG](#) 會收集 Amazon Redshift Serverless 的連線日誌資料。請注意，當您收集 Amazon Redshift 無伺服器的稽核記錄資料時，無法將資料傳送至記錄檔，只能傳送給 CloudWatch

主題

- [Amazon Redshift 日誌](#)
- [啟用記錄](#)
- [將稽核日誌傳送到 Amazon CloudWatch](#)
- [在 Amazon S3 中管理日誌檔案](#)
- [針對 Amazon S3 中的 Amazon Redshift 稽核記錄進行故障診斷](#)
- [使用記錄 Amazon Redshift API 呼叫 AWS CloudTrail](#)
- [使用主控台設定稽核](#)
- [使用 AWS CLI 和 Amazon Redshift API 設定記錄](#)

Amazon Redshift 日誌

Amazon Redshift 會將資訊記錄在下列日誌檔中：

- 連線日誌 — 記錄身分驗證嘗試、連線和中斷連線。
- 使用者日誌 — 記錄對資料庫使用者定義所做之變更的相關資訊。
- 使用者活動日誌 — 在每個查詢於資料庫上執行之前先行記錄。

連線和使用者日誌主要用於安全目的。您可以使用連線日誌，來監控正在連線至資料庫的使用者相關資訊，以及相關的連線資訊。此資訊可能是使用者的 IP 地址、使用者何時提出請求、使用者使用哪種類型的身分驗證等等。您可以利用使用者日誌，來監控對資料庫使用者之定義所做的變更。

使用者活動日誌主要用於故障診斷目的。它會追蹤使用者和系統在資料庫中執行之查詢類型的相關資訊。

連線日誌和使用者日誌對應至儲存在資料庫中系統資料表的資訊。您可以使用系統資料表來取得相同資訊，但是日誌檔提供更簡單的擷取和檢閱機制。日誌檔依賴 Amazon S3 許可而非資料庫許可，針對資料表執行查詢。此外，藉由檢視日誌檔中的資訊，而非查詢系統資料表，您可以減少與資料庫互動的任何影響。

Note

日誌檔不如系統日誌資料表 [STL_USERLOG](#) 和 [STL_CONNECTION_LOG](#) 一樣新。比最新記錄舊的記錄 (但不含最新記錄) 會複製到日誌檔。

Note

若為 Amazon Redshift Serverless，[SYS_CONNECTION_LOG](#) 會收集連線日誌資料。當您收集 Amazon Redshift 無伺服器的稽核記錄資料時，只能將資料傳送到記錄檔。CloudWatch

連線日誌

記錄身分驗證嘗試以及連線和中斷連線。下表說明連線日誌中的資訊。如需這些欄位的相關資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的 [STL_CONNECTION_LOG](#)。如需 Amazon Redshift Serverless 所收集連線日誌資料的相關資訊，請參閱 [SYS_CONNECTION_LOG](#)。

資料欄名稱	描述
事件	連線或身分驗證事件。
recordtime	發生事件的時間。
remotehost	遠端主機的名稱或 IP 地址。
remoteport	遠端主機的連接埠號碼。
pid	與陳述式相關聯的處理程序 ID。
dbname	資料庫名稱。
使用者名稱	使用者名稱。
authmethod	身分驗證方法。
持續時間	連線的持續時間，以微秒為單位。
sslversion	Secure Sockets Layer (SSL) 版本。
sslcipher	SSL 密碼。
mtu	最大傳輸單位 (MTU)。
sslcompression	SSL 壓縮類型。
sslexpansion	SSL 擴展類型。

資料欄名稱	描述
iamauthguid	請求的 AWS Identity and Access Management (IAM) 身份驗證識別 AWS CloudTrail 碼。這是 GetClusterCredentials API 呼叫的識別碼，用來建立用於指定連線的認證。
application_name	工作階段應用程式的初始名稱或已更新名稱。
os_version	連線到 Amazon Redshift 叢集之用戶端機器上的作業系統版本。
driver_version	從第三方 SQL 用戶端工具連線到 Amazon Redshift 叢集的 ODBC 或 JDBC 驅動器版本。
plugin_name	連接至您的 Amazon Redshift 叢集時使用的外掛程式名稱。
protocol_version	Amazon Redshift 驅動程式在建立與伺服器的連線時使用的內部通訊協定版本。
sessionid	目前工作階段的全域唯一識別碼。
compression	用於連線的壓縮演算法。

使用者日誌

記錄資料庫使用者之下列變更的詳細資訊：

- 建立使用者
- 捨棄使用者
- 更改使用者 (重新命名)
- 更改使用者 (更改屬性)

資料欄名稱	描述
userid	受到變更影響之使用者的 ID。
使用者名稱	受到變更影響之使用者的使用者名稱。

資料欄名稱	描述
oldusername	若為重新命名動作，這是原始使用者名稱。若是任何其他動作，此欄位空白。
動作	發生的動作。有效值： <ul style="list-style-type: none"> • Alter • 建立 • Drop • 重新命名
usecreatedb	若為 true (1)，表示使用者具備建立資料庫許可。
usesuper	若為 true (1)，表示使用者是超級使用者。
usecatupd	若為 true (1)，表示使用者可以更新系統目錄。
valuntil	密碼到期日。
pid	處理程序 ID。
xid	交易 ID。
recordtime	查詢開始的時間，以 UTC 表示。

查詢 [SYS_USERLOG](#) 系統檢視可尋找有關使用者變更的其他資訊。此檢視包含來自 Amazon Redshift Serverless 的日誌資料。

使用者活動日誌

在每個查詢於資料庫上執行之前先行記錄。

資料欄名稱	描述
recordtime	發生事件的時間。
db	資料庫名稱。
使用者	使用者名稱。

資料欄名稱	描述
pid	與陳述式相關聯的處理程序 ID。
userid	使用者 ID。
xid	交易 ID。
query	日誌的字首：後面跟著查詢的文字，包括換行字元。

啟用記錄

根據預設，Amazon Redshift 不會開啟稽核記錄。當您在叢集上開啟日誌記錄功能時，Amazon Redshift 會將日誌匯出到 Amazon CloudWatch，或是建立日誌並將日誌上傳到 Amazon S3，從啟用稽核記錄到目前為止擷取資料。每個記錄更新都會接續先前的日誌。

向 Amazon S3 CloudWatch 或傳送到 Amazon S3 的稽核記錄是選擇性的程序。目標為系統資料表的記錄則非選用，而且會自動發生。如需目標為系統資料表之記錄的相關資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的[系統資料表參考](#)。

連線日誌、使用者日誌和使用者活動日誌可透過使用 Amazon Redshift API 參考或 AWS Command Line Interface (AWS CLI) 一起啟用。AWS Management Console 對於使用者活動日誌，您也須啟用 `enable_user_activity_logging` 資料庫參數。如果您只啟用稽核記錄功能，但未啟用相關聯參數，則資料庫稽核日誌將只記錄連線日誌和使用者日誌的日誌資訊，但不記錄使用者活動日誌的日誌資訊。預設不會啟用 `enable_user_activity_logging` 參數 (`false`)。您可以將其設為 `true` 來啟用使用者活動日誌。如需詳細資訊，請參閱 [Amazon Redshift 參數群組](#)。

將稽核日誌傳送到 Amazon CloudWatch

當您啟用記錄功能時 CloudWatch，Amazon Redshift 會將叢集連線、使用者和使用者活動日誌資料匯出到 Amazon CloudWatch 日誌群組。記錄檔資料在結構描述方面不會變更。CloudWatch 專為監控應用程式而建置，您可以使用它來執行即時分析或將其設定為採取行動。您也可以使用 Amazon CloudWatch 日誌將日誌記錄存放在耐用儲存中。

建議 CloudWatch 使用檢視日誌檔案在 Amazon S3 中存放日誌檔案的替代方法。其不需要太多的組態設定，並可能適合您的監控要求，特別是如果您已經使用它來監控其他服務和應用程式的話。

Amazon 中的日誌群組和日誌事件 CloudWatch

選取要匯出的 Amazon Redshift 日誌後，您可以在 Amazon 日誌中監控 CloudWatch 日誌事件。系統會自動在下列字首下，為 Amazon Redshift Serverless 建立新的日誌群組，其中 `log_type` 代表日誌類型。

```
/aws/redshift/cluster/<cluster_name>/<log_type>
```

例如，如果您選擇匯出連線日誌，則日誌資料會儲存在下列日誌群組中。

```
/aws/redshift/cluster/cluster1/connectionlog
```

日誌事件會使用日誌串流匯出至日誌群組。若要在無伺服器端點的日誌事件中搜尋資訊，請使用 Amazon CloudWatch 日誌主控台 AWS CLI、或 Amazon CloudWatch 日誌 API。如需有關搜尋和篩選日誌資料的資訊，請參閱[使用篩選條件從日誌事件建立指標](#)。

在中 CloudWatch，您可以使用提供精細度和彈性的查詢語法來搜尋記錄資料。如需詳細資訊，請參閱[CloudWatch 記錄檔見解查詢語法](#)。

遷移至 Amazon CloudWatch 稽核記錄

在任何情況下，當您將日誌傳送到 Amazon S3 並變更組態 (例如要將日誌傳送到) 時 CloudWatch，保留在 Amazon S3 中的日誌都不會受到影響。您仍可在日誌資料所在的 Amazon S3 儲存貯體中查詢日誌資料。

在 Amazon S3 中管理日誌檔案

Amazon S3 中 Amazon Redshift 日誌檔案的數目和大小極度取決於叢集中的活動。如果您有作用中叢集，正在產生大量日誌，則 Amazon Redshift 可能更頻繁地產生日誌檔案。對於相同類型的活動，您可能具有一系列日誌檔案，例如在同一小時內具有多個連線日誌。

當 Amazon Redshift 使用 Amazon S3 來儲存日誌時，您在 Amazon S3 中使用的儲存會產生費用。在設定目標為 Amazon S3 的記錄之前，請計劃您需要儲存日誌檔案多長時間。這包括根據您的稽核需求，決定何時可刪除或封存日誌檔案。您建立的計劃極度取決於您儲存的資料類型，例如受制於合規或法規需求的資料。如需 Amazon S3 定價的相關資訊，請前往 [Amazon Simple Storage Service \(Amazon S3\) 定價](#)。

啟用目標為 Amazon S3 的記錄時的限制

稽核記錄有下列限制：

- 您只能使用 Amazon S3 受管金鑰 (SSE-S3) 加密 (AES-256)。
- Amazon S3 儲存貯體必須關閉 S3 物件鎖定功能。

Amazon Redshift 稽核記錄的儲存貯體許可

當您開啟目標為 Amazon S3 的記錄功能時，Amazon Redshift 會收集記錄資訊，並將其上傳到儲存在 Amazon S3 的日誌檔案。您可以使用現有的儲存貯體，或建立新的儲存貯體。Amazon Redshift 需要儲存貯體的以下 IAM 許可：

- `s3:GetBucketAcl` 服務對 Amazon S3 儲存貯體需有讀取許可，才能識別儲存貯體擁有者。
- `s3:PutObject` 服務需有放置物件許可，才能上傳物件。此外，開啟記錄功能的使用者或 IAM 角色還必須具有 Amazon S3 儲存貯體的 `s3:PutObject` 許可。每次上傳日誌，服務就會判斷目前儲存貯體擁有者是否符合啟用記錄時的儲存貯體擁有者。如果這些擁有者不相符，您會收到錯誤。

當您啟用稽核記錄時，如果您選取建立新儲存貯體的選項，系統便會為其套用正確的許可。不過，如果您在 Amazon S3 建立自己的儲存貯體，或使用現有的儲存貯體，則請務必新增包含儲存貯體名稱的儲存貯體政策。日誌會使用服務主體憑證來傳送。##### AWS ##### Redshift ##### ##

儲存貯體政策會使用以下格式。*ServiceName* 並且 *BucketName* 是您自己的價值觀的佔位符。此外，還要在儲存貯體政策中指定相關聯的動作和資源。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Put bucket policy needed for audit logging",
      "Effect": "Allow",
      "Principal": {
        "Service": "ServiceName"
      },
      "Action": [
        "s3:PutObject",
        "s3:GetBucketAcl"
      ],
      "Resource": [
        "arn:aws:s3:::BucketName",
        "arn:aws:s3:::BucketName/*"
      ]
    }
  ]
}
```

```
]
}
```

下列範例是美國東部 (維吉尼亞北部) 區域的儲存貯體政策，以及名為 AuditLogs 的儲存貯體。

```
{
  "Version": "2008-10-17",
  "Statement": [
    {
      "Sid": "Put bucket policy needed for audit logging",
      "Effect": "Allow",
      "Principal": {
        "Service": "redshift.amazonaws.com"
      },
      "Action": [
        "s3:PutObject",
        "s3:GetBucketAcl"
      ],
      "Resource": [
        "arn:aws:s3:::AuditLogs",
        "arn:aws:s3:::AuditLogs/*"
      ]
    }
  ]
}
```

預設未啟用的區域 (也稱為「選擇加入」區域) 需要區域特定的服務主體名稱。對於這些區域，服務主體名稱會包含 `redshift.region.amazonaws.com` 格式的區域。例如，對於亞太區域 (香港) 區域，名稱是 `redshift.ap-east-1.amazonaws.com`。如需預設未啟用的區域清單，請參閱《AWS 一般參考》中的[管理 AWS 區域](#)。

Note

區域特定服務主體名稱會對應到叢集所在的區域。

日誌檔案的最佳實務

當 Redshift 將日誌檔案上傳到 Amazon S3 時，大型檔案可以分段上傳。如果分段上傳不成功，檔案的這些分段可能會留在 Amazon S3 儲存貯體中。這可能會導致額外的儲存成本，因此請務必了解分段上

傳失敗時會發生什麼情況。如需有關稽核日誌分段上傳的詳細說明，請參閱[使用分段上傳來上傳和複製物件](#)和[中止分段上傳](#)。

如需建立 S3 儲存貯體和新增儲存貯體政策的相關資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的[建立儲存貯體](#)和[編輯儲存貯體許可](#)。

Amazon Redshift 稽核記錄的儲存貯體結構

依預設，Amazon Redshift 會使用下列儲存貯體和物件結構來組織 Amazon S3 儲存貯體中的日誌檔案：

`AWSLogs/AccountID/ServiceName/Region/Year/Month/Day/AccountID_ServiceName_Region`

範例為：`AWSLogs/123456789012/redshift/us-east-1/2013/10/29/123456789012_redshift_us-east-1_mycluster_userlog_2013-10-29T18:01.gz`

如果您提供 Amazon S3 金鑰字首，請將字首置於金鑰開頭處。

例如，如果您指定 myprefix 的字首：`myprefix/AWSLogs/123456789012/redshift/us-east-1/2013/10/29/123456789012_redshift_us-east-1_mycluster_userlog_2013-10-29T18:01.gz`

Amazon S3 金鑰字首不能超過 512 個字元。它不能包含空格 ()、雙引號 (")、單引號 (')、反斜線 (\)。也有一些不允許的特殊字元和控制字元。這些字元的十六進位碼如下：

- x00 到 x20
- x22
- x27
- x5c
- x7f 或更大

針對 Amazon S3 中的 Amazon Redshift 稽核記錄進行故障診斷

Amazon Redshift 稽核記錄可能會由於下列原因而中斷：

- Amazon Redshift 沒有將日誌上傳至 Amazon S3 儲存貯體的許可。驗證儲存貯體是使用正確 IAM 政策設定的。如需詳細資訊，請參閱[Amazon Redshift 稽核記錄的儲存貯體許可](#)。

- 儲存貯體擁有者已變更。當 Amazon Redshift 上傳日誌時，其會驗證儲存貯體擁有者是否與啟用記錄時的儲存貯體擁有者相同。如果儲存貯體擁有者已變更，則 Amazon Redshift 無法上傳日誌，直到您設定另一個用於稽核記錄的儲存貯體為止。
- 找不到儲存貯體。如果在 Amazon S3 中刪除該儲存貯體，Amazon Redshift 便無法上傳日誌。您必須重建儲存貯體，或設定 Amazon Redshift 以將日誌上傳至不同的儲存貯體。

使用記錄 Amazon Redshift API 呼叫 AWS CloudTrail

Amazon Redshift 與這項服務整合在一起 AWS CloudTrail，該服務可提供使用者、角色或 AWS 服務在 Amazon Redshift 中所採取的動作記錄。CloudTrail 以事件形式擷取 Amazon Redshift 的所有 API 呼叫。如需與 Amazon Redshift 整合的詳細資訊 AWS CloudTrail，請參閱[使用 CloudTrail](#)。

您可以在 Amazon Redshift 資料庫稽核記錄之外 CloudTrail 獨立使用，也可以在 Amazon Redshift 資料庫稽核

若要進一步了解 CloudTrail，請參閱使[AWS CloudTrail 用者指南](#)。

使用主控台設定稽核

設定 Amazon Redshift 以匯出稽核日誌資料。日誌可以匯出到 Amazon S3 儲存貯體 CloudWatch，或以檔案形式匯出至 Amazon S3 儲存貯體

使用主控台啟用稽核記錄日誌

主控台步驟

啟用叢集的稽核記錄

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽功能表上，選擇叢集，然後選擇您要更新的叢集。
3. 選擇屬性索引標籤。在資料庫組態面板上，選擇編輯，然後選擇編輯稽核記錄。
4. 在 [編輯稽核記錄] 頁面上，選擇 [開啟]，然後選取 S3 儲存貯體或 CloudWatch。我們建議您使用，CloudWatch 因為管理很簡單，並且具有用於資料視覺化的實用功能。
5. 選擇要匯出的日誌。
6. 若要儲存您的選擇，請選擇儲存變更。

使用 AWS CLI 和 Amazon Redshift API 設定記錄

您可以使用下列 Amazon Redshift CLI 操作來設定稽核記錄：

- [describe-logging-status](#)
- [disable-logging](#)
- [enable-logging](#)

您可以使用下列 Amazon Redshift API 操作來設定稽核記錄：

- [DescribeLoggingStatus](#)
- [DisableLogging](#)
- [EnableLogging](#)

使用記錄 CloudTrail

使用 AWS CloudTrail 記錄呼叫

Amazon Redshift，數據共享，Amazon Redshift 無服務器，Amazon Redshift 數據 API 和查詢編輯器 v2 都與 AWS CloudTrail CloudTrail 這是一項服務，可提供 Amazon Redshift 中使用者、角色或 AWS 服務所採取的動作記錄。CloudTrail 以事件形式擷取 Amazon Redshift 的所有 API 呼叫。擷取的呼叫包括從 Redshift 主控台進行的呼叫，以及針對 Redshift 操作的程式碼呼叫。

如果您建立 CloudTrail 追蹤，您可以持續將 CloudTrail 事件傳遞到 Amazon S3 儲存貯體，包括 Redshift 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。使用收集的信息 CloudTrail，您可以確定某些事情。這些事情包括向 Redshift 提出的請求、提出請求的 IP 地址、提出請求的人員、提出請求的時間，以及其他詳細資訊。

您可以在 Amazon Redshift 資料庫稽核記錄之外 CloudTrail 獨立使用，也可以除了使用。

若要進一步了解 CloudTrail，請參閱使 [AWS CloudTrail 用者指南](#)。

使用中的資訊 CloudTrail

CloudTrail 當您建立 AWS 帳戶時，會在您的帳戶中開啟。當活動發生時，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。您可以檢視、搜尋和下載 AWS 帳戶的最新事件。如需詳細資訊，請參閱 AWS CloudTrail 使用指南中的 [檢視具有 CloudTrail 事件歷程記錄](#) 的事件。

如需AWS帳戶中持續記錄事件 (包括 Redshift 的事件)，請建立追蹤。CloudTrail 使用追蹤將日誌檔傳送到 Amazon S3 儲存貯體。根據預設，當您在主控台建立線索時，線索會套用到所有 AWS 區域。該追蹤會記錄來自 AWS 分割區中所有區域的事件，並將日誌檔案交付到您指定的 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《AWS CloudTrail 使用者指南》中的下列主題：

- [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 Amazon Redshift、Amazon Redshift 無伺服器、資料 API、資料共用和查詢編輯器 v2 動作均由記錄。CloudTrail例如，呼叫AuthorizeDatashare、CreateNamespaceExecuteStatement、和CreateConnection動作會在 CloudTrail 記錄檔中產生項目。

每一筆事件或日誌項目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：

- 該請求是否使用根或使用者憑證提出。
- 提出該請求時，是否使用了特定角色或聯合身分使用者的暫時安全憑證。
- 該請求是否由另一項 AWS 服務提出。

若要取得更多資訊，請參閱AWS CloudTrail使用者指南中的使用者 CloudTrail [userIdentity 元素](#)。

了解日誌檔案項目

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。一個事件為任何來源提出的單一請求，並包含請求動作、請求的日期和時間、請求參數等資訊。CloudTrail 日誌文件不是公共 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。

Amazon Redshift 資料共用範例

下列範例顯示說明AuthorizeDataShare作業的 CloudTrail 記錄項目。

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

```
"principalId": "AKIAIOSFODNN7EXAMPLE:janedoe",
"arn": "arn:aws:sts::111122223333:user/janedoe",
"accountId": "111122223333",
"accessKeyId": "AKIAI44QH8DHBEXAMPLE",
"sessionContext": {
  "sessionIssuer": {
    "type": "Role",
    "principalId": "AKIAIOSFODNN7EXAMPLE:janedoe",
    "arn": "arn:aws:sts::111122223333:user/janedoe",
    "accountId": "111122223333",
    "userName": "janedoe"
  },
  "attributes": {
    "creationDate": "2021-08-02T23:40:45Z",
    "mfaAuthenticated": "false"
  }
},
},
"eventTime": "2021-08-02T23:40:58Z",
"eventSource": "redshift.amazonaws.com",
"eventName": "AuthorizeDataShare",
"awsRegion": "us-east-1",
"sourceIPAddress": "3.227.36.75",
"userAgent": "aws-cli/1.18.118 Python/3.6.10
Linux/4.9.217-0.1.ac.205.84.332.metal1.x86_64 boto3/1.17.41",
"requestParameters": {
  "dataShareArn": "arn:aws:redshift:us-
east-1:111122223333:datashare:4c64c6ec-73d5-42be-869b-b7f7c43c7a53/testshare",
  "consumerIdentifier": "555555555555"
},
"responseElements": {
  "dataShareArn": "arn:aws:redshift:us-
east-1:111122223333:datashare:4c64c6ec-73d5-42be-869b-b7f7c43c7a53/testshare",
  "producerNamespaceArn": "arn:aws:redshift:us-
east-1:123456789012:namespace:4c64c6ec-73d5-42be-869b-b7f7c43c7a53",
  "producerArn": "arn:aws:redshift:us-
east-1:111122223333:namespace:4c64c6ec-73d5-42be-869b-b7f7c43c7a53",
  "allowPubliclyAccessibleConsumers": true,
  "dataShareAssociations": [
    {
      "consumerIdentifier": "555555555555",
      "status": "AUTHORIZED",
      "createdDate": "Aug 2, 2021 11:40:56 PM",
      "statusChangeDate": "Aug 2, 2021 11:40:57 PM"
    }
  ]
}
```

```

    }
  ]
},
"requestID": "87ee1c99-9e41-42be-a5c4-00495f928422",
"eventID": "03a3d818-37c8-46a6-aad5-0151803bdb09",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "111122223333",
"eventCategory": "Management"
}

```

Amazon Redshift Serverless 範例

Amazon Redshift 無伺服器已與整合，AWS CloudTrail 以提供在 Amazon Redshift 無伺服器中採取的動作記錄。CloudTrail 擷取 Amazon Redshift 無伺服器的所有 API 呼叫作為事件。如需 Amazon Redshift Serverless 功能的詳細資訊，請參閱 [Amazon Redshift Serverless 功能概觀](#)。

下列範例顯示示範 CreateNamespace 動作的 CloudTrail 記錄項目。

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AAKEOFPINEXAMPLE",
    "arn": "arn:aws:sts::111111111111:assumed-role/admin/admin",
    "accountId": "111111111111",
    "accessKeyId": "AAKEOFPINEXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AAKEOFPINEXAMPLE",
        "arn": "arn:aws:iam::111111111111:role/admin",
        "accountId": "111111111111",
        "userName": "admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "creationDate": "2022-03-21T20:51:58Z",
        "mfaAuthenticated": "false"
      }
    }
  },
},

```

```

"eventTime": "2022-03-21T23:15:40Z",
"eventSource": "redshift-serverless.amazonaws.com",
"eventName": "CreateNamespace",
"awsRegion": "us-east-1",
"sourceIPAddress": "56.23.155.33",
"userAgent": "aws-cli/2.4.14 Python/3.8.8 Linux/5.4.181-109.354.amzn2int.x86_64
exe/x86_64.amzn.2 prompt/off command/redshift-serverless.create-namespace",
"requestParameters": {
  "adminUserPassword": "HIDDEN_DUE_TO_SECURITY_REASONS",
  "adminUsername": "HIDDEN_DUE_TO_SECURITY_REASONS",
  "dbName": "dev",
  "namespaceName": "testnamespace"
},
"responseElements": {
  "namespace": {
    "adminUsername": "HIDDEN_DUE_TO_SECURITY_REASONS",
    "creationDate": "Mar 21, 2022 11:15:40 PM",
    "defaultIamRoleArn": "",
    "iamRoles": [],
    "logExports": [],
    "namespaceArn": "arn:aws:redshift-serverless:us-
east-1:111111111111:namespace/befa5123-16c2-4449-afca-1d27cb40fc99",
    "namespaceId": "8b726a0c-16ca-4799-acca-1d27cb403599",
    "namespaceName": "testnamespace",
    "status": "AVAILABLE"
  }
},
"requestID": "ed4bb777-8127-4dae-aea3-bac009999163",
"eventID": "1dbee944-f889-4beb-b228-7ad0f312464",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "111111111111",
"eventCategory": "Management",
}

```

Amazon Redshift 資料 API 範例

下列範例顯示示範ExecuteStatement動作的 CloudTrail 記錄項目。

```

{
  "eventVersion": "1.05",
  "userIdentity": {

```

```

    "type": "IAMUser",
    "principalId": "AKIAIOSFODNN7EXAMPLE:janedoe",
    "arn": "arn:aws:sts::123456789012:user/janedoe",
    "accountId": "123456789012",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "userName": "janedoe"
  },
  "eventTime": "2020-08-19T17:55:59Z",
  "eventSource": "redshift-data.amazonaws.com",
  "eventName": "ExecuteStatement",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "aws-cli/1.18.118 Python/3.6.10
Linux/4.9.217-0.1.ac.205.84.332.metal1.x86_64 boto3/1.17.41",
  "requestParameters": {
    "clusterIdentifier": "example-cluster-identifier",
    "database": "example-database-name",
    "dbUser": "example_db_user_name",
    "sql": "***OMITTED***"
  },
  "responseElements": {
    "clusterIdentifier": "example-cluster-identifier",
    "createdAt": "Aug 19, 2020 5:55:58 PM",
    "database": "example-database-name",
    "dbUser": "example_db_user_name",
    "id": "5c52b37b-9e07-40c1-98de-12ccd1419be7"
  },
  "requestID": "00c924d3-652e-4939-8a7a-cd0612eeb8ac",
  "eventID": "c1fb7076-102f-43e5-9ec9-40820bcc1175",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "recipientAccountId": "123456789012"
}

```

下列範例顯示了一個 CloudTrail 記錄項目，該記錄項目示範了clientToken用於冪等性的ExecuteStatement動作。

```

{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AKIAIOSFODNN7EXAMPLE:janedoe",
    "arn": "arn:aws:sts::123456789012:user/janedoe",

```

```

    "accountId": "123456789012",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "userName": "janedoe"
  },
  "eventTime": "2020-08-19T17:55:59Z",
  "eventSource": "redshift-data.amazonaws.com",
  "eventName": "ExecuteStatement",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "aws-cli/1.18.118 Python/3.6.10
Linux/4.9.217-0.1.ac.205.84.332.metal1.x86_64 boto3/1.17.41",
  "requestParameters": {
    "clusterIdentifier": "example-cluster-identifier",
    "database": "example-database-name",
    "dbUser": "example_db_user_name",
    "sql": "****OMITTED****",
    "clientToken": "32db2e10-69ac-4534-b3fc-a191052616ce"
  },
  "responseElements": {
    "clusterIdentifier": "example-cluster-identifier",
    "createdAt": "Aug 19, 2020 5:55:58 PM",
    "database": "example-database-name",
    "dbUser": "example_db_user_name",
    "id": "5c52b37b-9e07-40c1-98de-12ccd1419be7"
  },
  "requestID": "00c924d3-652e-4939-8a7a-cd0612eeb8ac",
  "eventID": "c1fb7076-102f-43e5-9ec9-40820bcc1175",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "recipientAccountId": "123456789012"
}

```

Amazon Redshift 查詢編輯器 v2 範例

下列範例顯示示範CreateConnection動作的 CloudTrail 記錄項目。

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AAKE0FPINEXAMPLE:session",
    "arn": "arn:aws:sts::123456789012:assumed-role/MyRole/session",
    "accountId": "123456789012",

```



```
"accessKeyId": "AKIAI44QH8DHBEXAMPLE",
"sessionContext": {
  "sessionIssuer": {
    "type": "Role",
    "principalId": "AAKEOFPINEXAMPLE",
    "arn": "arn:aws:iam::123456789012:role/MyRole",
    "accountId": "123456789012",
    "userName": "MyRole"
  },
  "webIdFederationData": {},
  "attributes": {
    "creationDate": "2022-09-21T17:19:02Z",
    "mfaAuthenticated": "false"
  }
}
},
"eventTime": "2022-09-21T22:22:05Z",
"eventSource": "sqlworkbench.amazonaws.com",
"eventName": "CreateConnection",
"awsRegion": "ca-central-1",
"sourceIPAddress": "192.2.0.2",
"userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:102.0)
Gecko/20100101 Firefox/102.0",
"requestParameters": {
  "password": "****",
  "databaseName": "****",
  "isServerless": false,
  "name": "****",
  "host": "redshift-cluster-2.c8robpbxvbf9.ca-central-1.redshift.amazonaws.com",
  "authenticationType": "****",
  "clusterId": "redshift-cluster-2",
  "username": "****",
  "tags": {
    "sqlworkbench-resource-owner": "AAKEOFPINEXAMPLE:session"
  }
},
"responseElements": {
  "result": true,
  "code": "",
  "data": {
    "id": "arn:aws:sqlworkbench:ca-central-1:123456789012:connection/ce56b1be-
dd65-4bfb-8b17-12345123456",
    "name": "****",
    "authenticationType": "****",
```

```

    "databaseName": "****",
    "secretArn": "arn:aws:secretsmanager:ca-
central-1:123456789012:secret:sqlworkbench!7da333b4-9a07-4917-b1dc-12345123456-qTCoFm",
    "clusterId": "redshift-cluster-2",
    "dbUser": "****",
    "userSettings": "****",
    "recordDate": "2022-09-21 22:22:05",
    "updatedAt": "2022-09-21 22:22:05",
    "accountId": "123456789012",
    "tags": {
      "sqlworkbench-resource-owner": "AAKEOFPINEXAMPLE:session"
    },
    "isServerless": false
  }
},
"requestID": "9b82f483-9c03-4cdd-bb49-a7009e7da714",
"eventID": "a7cdd442-e92f-46a2-bc82-2325588d41c3",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "123456789012",
"eventCategory": "Management"
}

```

AWS CloudTrail 日誌中的 Amazon Redshift 帳戶 ID

當 Amazon Redshift 代表您呼叫另一個 AWS 服務時，即會使用屬於 Amazon Redshift 的帳戶 ID 來記錄呼叫。而不會使用您的帳戶 ID 來記錄呼叫。例如，假設 Amazon Redshift 呼叫 AWS Key Management Service (AWS KMS) 操作 (例如 CreateGrant、Decrypt、Encrypt 和 RetireGrant) 來管理叢集上的加密。在此情況下，AWS CloudTrail 會使用 Amazon Redshift 帳戶 ID 來記錄呼叫。

呼叫其他 AWS 服務時，Amazon Redshift 會使用下表中的帳戶 ID。

區域	區域	帳戶 ID
美國東部 (維吉尼亞北部) 區域	us-east-1	368064434614
美國東部 (俄亥俄) 區域	us-east-2	790247189693
美國西部 (加利佛尼亞北部) 區域	us-west-1	703715109447

區域	區域	帳戶 ID
美國西部 (奧勒岡) 區域	us-west-2	473191095985
非洲 (開普敦) 區域	af-south-1	420376844563
亞太區域 (香港) 區域	ap-east-1	651179539253
亞太區域 (海德拉巴)	ap-south-2	297058826802
亞太區域 (雅加達)	ap-southeast-3	623197973179
亞太區域 (墨爾本) 區域	ap-southeast-4	945512339897
亞太 (孟買) 區域	ap-south-1	408097707231
亞太 (大阪) 區域	ap-northeast-3	398671365691
亞太 (首爾) 區域	ap-northeast-2	713597048934
亞太 (新加坡) 區域	ap-southeast-1	960118270566
亞太 (雪梨) 區域	ap-southeast-2	485979073181
亞太 (東京) 區域	ap-northeast-1	615915377779
加拿大 (中部) 區域	ca-central-1	764870610256
加拿大西部 (卡加利) 區域	ca-west-1	830903446466
歐洲 (法蘭克福) 區域	eu-central-1	434091160558
歐洲 (愛爾蘭) 區域	eu-west-1	246478207311
歐洲 (倫敦) 區域	eu-west-2	885798887673
Europe (Milan) Region	eu-south-1	041313461515
歐洲 (巴黎) 區域	eu-west-3	694668203235
歐洲 (西班牙) 區域	eu-south-2	028811157404

區域	區域	帳戶 ID
歐洲 (斯德哥爾摩) 區域	eu-north-1	553461782468
歐洲 (蘇黎世) 區域	eu-central-2	668912161003
以色列 (特拉維夫) 區域	il-central-1	901883065212
Middle East (Bahrain) Region	me-south-1	051362938876
中東 (阿拉伯聯合大公國) 區域	me-central-1	595013617770
南美洲 (聖保羅) 區域	sa-east-1	392442076723

下列範例顯示 Amazon Redshift 所呼叫之「AWS KMS解密」作業的 CloudTrail 日誌項目。

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAI5QPCMKLTL4VHFCYY:i-0f53e22dbe5df8a89",
    "arn": "arn:aws:sts::790247189693:assumed-role/prod-23264-role-wp/i-0f53e22dbe5df8a89",
    "accountId": "790247189693",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2017-03-03T16:24:54Z"
      }
    },
    "sessionIssuer": {
      "type": "Role",
      "principalId": "AROAI5QPCMKLTL4VHFCYY",
      "arn": "arn:aws:iam::790247189693:role/prod-23264-role-wp",
      "accountId": "790247189693",
      "userName": "prod-23264-role-wp"
    }
  }
},
"eventTime": "2017-03-03T17:16:51Z",
"eventSource": "kms.amazonaws.com",
```

```
"eventName": "Decrypt",
"awsRegion": "us-east-2",
"sourceIPAddress": "52.14.143.61",
"userAgent": "aws-internal/3",
"requestParameters": {
  "encryptionContext": {
    "aws:redshift:createtime": "20170303T1710Z",
    "aws:redshift:arn": "arn:aws:redshift:us-east-2:123456789012:cluster:my-dw-
instance-2"
  }
},
"responseElements": null,
"requestID": "30d2fe51-0035-11e7-ab67-17595a8411c8",
"eventID": "619bad54-1764-4de4-a786-8898b0a7f40c",
"readOnly": true,
"resources": [
  {
    "ARN": "arn:aws:kms:us-east-2:123456789012:key/f8f4f94f-e588-4254-
b7e8-078b99270be7",
    "accountId": "123456789012",
    "type": "AWS::KMS::Key"
  }
],
"eventType": "AwsApiCall",
"recipientAccountId": "123456789012",
"sharedEventID": "c1daefea-a5c2-4fab-b6f4-d8eaa1e522dc"
}
```

Amazon Redshift 的合規驗證

在多個 AWS 合規計劃中，第三方稽核人員會評估 Amazon Redshift 的安全與合規。這些計劃包括 SOC、PCI、FedRAMP、HIPAA 等等。

如需特定合規計劃範圍內的 AWS 服務清單，請參閱[合規計劃內的 AWS 服務](#)。如需一般資訊，請參閱[AWS 合規計劃](#)。

您可使用 AWS Artifact 下載第三方稽核報告。如需詳細資訊，請參閱[在 AWS Artifact 中下載報告](#)。

使用 Amazon Redshift 時的合規責任會取決於資料的敏感度、組織的合規目標，以及適用法律和法規。若您使用的 Amazon Redshift 必須遵循特定標準 (如 HIPAA、PCI 或 FedRAMP)，AWS 會提供資源予以協助：

- [安全與合規快速入門指南](#)會討論在 AWS 上部署以安全及合規為重心之基準環境的架構考量和步驟。
- [HIPAA 安全與合規架構白皮書](#)，說明公司可如何運用 AWS 來建立 HIPAA 合規的應用程式。
- [AWS 合規資源](#)，可能適用於您的產業和位置的手冊和指南。
- [AWS Config](#)，一項 AWS 服務，可評定資源組態與內部實務、業界準則和法規的合規狀態。
- [AWS Security Hub](#)，此 AWS 服務可供您檢視 AWS 中的安全狀態，可助您檢查是否符合安全產業標準和最佳實務。Security Hub 會透過安全控制來評估資源組態和安全標準，協助您遵守各種合規架構。如需有關使用 Security Hub 評估 Amazon Redshift 資源的詳細資訊，請參閱《AWS Security Hub 使用者指南》中的 [Amazon Redshift 控制項](#)。

下列合規和安全性文件涵蓋 Amazon Redshift，並且可視需求透過 AWS Artifact 取得。如需更多詳細資訊，請參閱 [AWS Artifact](#)。

- Cloud Computing Compliance Controls Catalogue (C5)
- ISO 27001:2013 適用性聲明 (SoA)
- ISO 27001:2013 認證
- ISO 27017:2015 適用性聲明 (SoA)
- ISO 27017:2015 認證
- ISO 27018:2015 適用性聲明 (SoA)
- ISO 27018:2014 認證
- ISO 9001:2015 認證
- PCI DSS 合規聲明文件 (AOC) 與責任摘要
- 服務組織控制 (SOC) 1 報告
- 服務組織控制 (SOC) 2 報告
- 服務組織控制 (SOC) 2 報告，針對機密性

Amazon Redshift 中的復原能力

AWS 全球基礎設施是以 AWS 區域與可用區域 (AZ) 為中心建置的。AWS 區域提供多個分開且隔離的實際可用區域，並以具備低延遲、高輸送量和高度備援特性的聯網相互連結。透過可用區域，您所設計與操作的應用程式和資料庫，就能夠在可用區域之間自動容錯移轉，而不會發生中斷。可用區域的可用性、容錯能力和擴展性都比傳統單一或多個資料中心的基礎設施高。

幾乎所有 AWS 區域都有多個可用區域和資料中心。您可以在相同區域中的多個可用區域間部署應用程式，以提供容錯能力與低延遲效能。

若要將叢集移至另一個可用區域，而不遺失任何資料或應用程式變更，您可以為叢集設定重新定位。透過重新定位，您可以在叢集上發生服務中斷時繼續操作，將所受影響降到最低。開啟叢集重新定位時，Amazon Redshift 可能會在某些情況下選擇將叢集重新定位。如需 Amazon Redshift 中重新定位的詳細資訊，請參閱[重新定位叢集](#)。

在可用區域發生意外事件的故障案例中，您可以設定多個可用區域 (多可用區) 部署，以確保 Amazon Redshift 資料倉儲能夠繼續運作。Amazon Redshift 會在可透過單一端點存取的兩個可用區域中部署相等的運算資源。如果整個可用區域發生故障，便可使用第二個可用區域中的剩餘運算資源繼續處理工作負載。如需異地同步備份部署的詳細資訊，請參閱[設定多可用區部署](#)。

如需 AWS 區域與可用區域的詳細資訊，請參閱[AWS 全球基礎設施](#)。

Amazon Redshift 的基礎設施安全

Amazon Redshift 是一項受管服務，受到 AWS 全球網路安全的保護。如需有關 AWS 安全服務以及 AWS 如何保護基礎設施的詳細資訊，請參閱[AWS 雲端安全](#)。若要使用基礎設施安全性的最佳實務來設計您的 AWS 環境，請參閱安全性支柱 AWS 架構良好的框架中的[基礎設施保護](#)。

您可使用 AWS 發佈的 API 呼叫，透過網路存取 Amazon Redshift。用戶端必須支援下列項目：

- 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，請求必須使用存取索引鍵 ID 和與 IAM 主體相關聯的私密存取索引鍵來簽署。或者，您可以使用[AWS Security Token Service](#) (AWS STS) 來產生暫時安全憑證來簽署請求。

網路隔離

以 Amazon VPC 服務為基礎的虛擬私有雲端 (VPC) 為您在 AWS 雲端中的私有、邏輯上隔離的網路。您可以執行下列步驟，在 VPC 內部署 Amazon Redshift 叢集：

- 在 AWS 區域中建立 VPC。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的[什麼是 Amazon VPC ?](#)。
- 建立兩個或多個私有 VPC 子網路。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的[VPC 和子網路](#)。
- 部署 Amazon Redshift 叢集。如需更多詳細資訊，請參閱[Amazon Redshift 叢集子網路群組](#)。

依預設會在佈建時鎖定 Amazon Redshift 叢集。若要允許來自 Amazon Redshift 用戶端的傳入網路流量，請將 VPC 安全群組與 Amazon Redshift 叢集相關聯。如需更多詳細資訊，請參閱 [Amazon Redshift 叢集子網路群組](#)。

若要僅允許往返特定 IP 位址範圍的流量，請更新您的 VPC 的安全群組。一個例子是僅允許往返您的企業網路的流量。

針對用來標記 Amazon Redshift 叢集的子網路，在設定與這個子網路相關聯的網路存取控制清單時，請務必將個別 AWS 區域的 S3 CIDR 範圍新增至傳入和傳出規則的允許清單中。這樣做可讓您執行以 S3 為基礎的操作，例如 Redshift Spectrum、COPY 和 UNLOAD，而不會造成中斷。

以下範例命令會在 us-east-1 區域中剖析 Amazon S3 所使用的所有 IPv4 地址的 JSON 回應。

```
curl https://ip-ranges.amazonaws.com/ip-ranges.json | jq -r '.prefixes[] |
  select(.region=="us-east-1") | select(.service=="S3") | .ip_prefix'

54.231.0.0/17

52.92.16.0/20

52.216.0.0/15
```

如需如何取得特定區域之 S3 IP 範圍的指示，請參閱 [AWS IP 地址範圍](#)。

Amazon Redshift 支援將叢集部署至專用租用 VPC。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的 [專用預留執行個體](#)。

Amazon Redshift 叢集安全群組

當您佈建 Amazon Redshift 叢集時，依預設它會遭鎖定，以便沒有人可以存取它。若要授予其他使用者 Amazon Redshift 叢集的傳入存取，您可使叢集與安全群組建立關聯。如果您是在 EC2-VPC 平台上，則可以使用現有的 Amazon VPC 安全群組，或定義新的安全群組，然後使它與叢集建立關聯。如需在 EC2-VPC 平台上管理叢集的相關資訊，請參閱 [管理 VPC 中的叢集](#)。

使用界面 VPC 端點連線至 Amazon Redshift

您可以使用虛擬私有雲端 (VPC) 中的界面 VPC 端點 (AWS PrivateLink) 直接連線至 Amazon Redshift API 服務，而非透過網際網路進行連線。如需 Amazon Redshift API 動作的相關資訊，請參閱《Amazon Redshift API 參考》中的 [動作](#)。如需有關的詳細資訊 AWS PrivateLink，請參閱 Amazon

VPC 使用者指南中的[介面虛擬私人雲端端點 \(AWS PrivateLink\)](#)。請注意，叢集的 JDBC/ODBC 連線不屬於 Amazon Redshift API 服務的一部分。

當您使用介面虛擬私人雲端端點時，VPC 和 Amazon Redshift 之間的通訊完全在 AWS 網路內進行，因此可提供更高的安全性。每個 VPC 端點皆會由一個或多個具私有 IP 地址彈性網路界面來表示，而該界面位於 VPC 子網路中。如需彈性網路界面的詳細資訊，請參閱 Amazon EC2 使用者指南中的[彈性網路界面](#)。

介面 VPC 端點會將 VPC 直接連線到 Amazon Redshift。它不使用網際網路閘道、網路位址轉譯 (NAT) 裝置、虛擬私人網路 (VPN) 連線或 AWS Direct Connect 連線。VPC 中的執行個體不需要公有 IP 地址，就能與 Amazon Redshift API 進行通訊。

若要透過 VPC 使用 Amazon Redshift，您有兩個選項。一個是從 VPC 內部的執行個體進行連線。另一種方法是使用 AWS VPN 選項或 AWS Direct Connect 將私人網絡連接到 VPC。如需有關 AWS VPN 選項的詳細資訊，請參閱 Amazon VPC 使用者指南中的[VPN 連線](#)。如需有關 AWS Direct Connect 的資訊，請參閱《AWS Direct Connect 使用者指南》中的[建立連線](#)。

您可以使用 AWS Management Console 或 AWS Command Line Interface (AWS CLI) 命令建立介面 VPC 人雲端端點，以連接到 Amazon Redshift。如需詳細資訊，請參閱[建立介面端點](#)。

在您建立介面 VPC 端點後，您可以為該端點啟用私有 DNS 主機名稱。啟用後，預設 Amazon Redshift 端點 (<https://redshift.Region.amazonaws.com>) 會解析為您的 VPC 端點。

如果您未啟用私有 DNS 主機名稱，Amazon VPC 會透過下列格式提供 DNS 端點名稱供您使用。

```
VPC_endpoint_ID.redshift.Region.vpce.amazonaws.com
```

如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的[介面 VPC 端點 \(AWS PrivateLink\)](#)。

Amazon Redshift 支援在您的 VPC 內呼叫其所有 [API 操作](#)。

可以將 VPC 端點政策附接至某個 VPC 端點，以控制 AWS Identity and Access Management (IAM) 主體的存取權。您也可以將安全群組與 VPC 端點建立關聯，以根據網路流量的來源和目的地來控制傳入和傳出存取。範例是 IP 地址範圍。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的[使用 VPC 端點控制服務的存取](#)。

為 Amazon Redshift 建立 VPC 端點政策

您可以為 Amazon Redshift 的 VPC 端點建立政策，以指定下列各項：

- 可執行或不可執行動作的主體

- 可執行的動作
- 可在其中執行動作的資源

如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的[使用 VPC 端點控制對服務的存取](#)。

接下來，您可以找到 VPC 端點政策的範例。

主題

- [範例：拒絕來自指 AWS 定帳戶的所有存取的 VPC 端點策略](#)
- [範例：可用來只向指定 IAM 角色允許 VPC 存取的 VPC 端點政策](#)
- [範例：可用來只向指定 IAM 主體 \(使用者\) 允許 VPC 存取的 VPC 端點政策](#)
- [範例：可用來允許唯讀 Amazon Redshift 操作的 VPC 端點政策](#)
- [範例：拒絕指定叢集存取的 VPC 端點政策](#)

範例：拒絕來自指 AWS 定帳戶的所有存取的 VPC 端點策略

下列 VPC 端點策略會拒絕 AWS 帳戶對使用此端點的資源進行`123456789012`所有存取。

```
{
  "Statement": [
    {
      "Action": "*",
      "Effect": "Allow",
      "Resource": "*",
      "Principal": "*"
    },
    {
      "Action": "*",
      "Effect": "Deny",
      "Resource": "*",
      "Principal": {
        "AWS": [
          "123456789012"
        ]
      }
    }
  ]
}
```

範例：可用來只向指定 IAM 角色允許 VPC 存取的 VPC 端點政策

下列 VPC 私人雲端端點政策只允許完整存取 AWS 帳戶 **123 456789012** *redshiftrrole* 中的 IAM 角色。所有其他 IAM 主體均無法存取該端點。

```
{
  "Statement": [
    {
      "Action": "*",
      "Effect": "Allow",
      "Resource": "*",
      "Principal": {
        "AWS": [
          "arn:aws:iam::123456789012:role/redshiftrrole"
        ]
      }
    }
  ]
}
```

這只是範例。在大多數使用案例中，建議您附加特定動作的許可，以縮小許可範圍。

範例：可用來只向指定 IAM 主體 (使用者) 允許 VPC 存取的 VPC 端點政策

下列 VPC 端點政策只允許 AWS 帳戶 **123 456789012** *redshiftadmin* 中的 IAM 使用者進行完整存取。所有其他 IAM 主體均無法存取該端點。

```
{
  "Statement": [
    {
      "Action": "*",
      "Effect": "Allow",
      "Resource": "*",
      "Principal": {
        "AWS": [
          "arn:aws:iam::123456789012:user/redshiftadmin"
        ]
      }
    }
  ]
}
```

```
}
```

這只是範例。在大多數使用案例中，建議您先附加許可給某個角色，再指派給使用者。此外，也建議您使用特定動作來縮小許可範圍。

範例：可用來允許唯讀 Amazon Redshift 操作的 VPC 端點政策

下列 VPC 端點政策只允許 AWS 帳戶執 **123456789012** 行指定的 Amazon Redshift 動作。

指定的動作會為 Amazon Redshift 提供等效的唯讀存取權。拒絕指定的帳戶存取在該 VPC 上的所有其他動作。此外，也會拒絕所有其他帳戶的任何存取。如需 Amazon Redshift 動作的清單，請參閱《IAM 使用者指南》中的 [Amazon Redshift 的動作、資源和條件金鑰](#)。

```
{
  "Statement": [
    {
      "Action": [
        "redshift:DescribeAccountAttributes",
        "redshift:DescribeClusterParameterGroups",
        "redshift:DescribeClusterParameters",
        "redshift:DescribeClusterSecurityGroups",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeClusterSubnetGroups",
        "redshift:DescribeClusterVersions",
        "redshift:DescribeDefaultClusterParameters",
        "redshift:DescribeEventCategories",
        "redshift:DescribeEventSubscriptions",
        "redshift:DescribeHsmClientCertificates",
        "redshift:DescribeHsmConfigurations",
        "redshift:DescribeLoggingStatus",
        "redshift:DescribeOrderableClusterOptions",
        "redshift:DescribeQuery",
        "redshift:DescribeReservedNodeOfferings",
        "redshift:DescribeReservedNodes",
        "redshift:DescribeResize",
        "redshift:DescribeSavedQueries",
        "redshift:DescribeScheduledActions",
        "redshift:DescribeSnapshotCopyGrants",
        "redshift:DescribeSnapshotSchedules",
        "redshift:DescribeStorage",
        "redshift:DescribeTable",
        "redshift:DescribeTableRestoreStatus",
```

```

        "redshift:DescribeTags",
        "redshift:FetchResults",
        "redshift:GetReservedNodeExchangeOfferings"
    ],
    "Effect": "Allow",
    "Resource": "*",
    "Principal": {
        "AWS": [
            "123456789012"
        ]
    }
}
]
}

```

範例：拒絕指定叢集存取的 VPC 端點政策

下列 VPC 端點政策會允許所有帳戶和主體擁有完整存取權。同時，它會拒絕任何 AWS 帳戶 **123456789012** 存取具有叢集 ID 的 Amazon Redshift 叢集上執行的動作。*my-redshift-cluster* 仍然允許其他不支援叢集資源層級許可的 Amazon Redshift 動作。如需 Amazon Redshift 動作及其對應資源類型的清單，請參閱《IAM 使用者指南》中的 [Amazon Redshift 的動作、資源和條件金鑰](#)。

```

{
  "Statement": [
    {
      "Action": "*",
      "Effect": "Allow",
      "Resource": "*",
      "Principal": "*"
    },
    {
      "Action": "*",
      "Effect": "Deny",
      "Resource": "arn:aws:redshift:us-east-1:123456789012:cluster:my-redshift-cluster",
      "Principal": {
        "AWS": [
            "123456789012"
        ]
      }
    }
  ]
}

```

```
    }  
  ]  
}
```

Amazon Redshift 中的組態與漏洞分析

AWS 會處理訪客作業系統 (OS) 和資料庫修補、防火牆組態和災難復原 (DR) 等基本安全任務。這些程序已由認證的第三方進行檢閱。如需詳細資訊，請參閱 [Amazon Redshift 的合規驗證](#)、[共同責任模式與安全、身分和合規的最佳實務](#)。

Amazon Redshift 會自動套用升級並修補資料倉儲，這樣您就能專注於應用程式本身，而不是管理。修補和升級會在可設定的維護時間期間套用。如需更多詳細資訊，請參閱 [維護時段](#)。

Amazon Redshift 查詢編輯器 v2 是 AWS 受管應用程式。所有修補程式和更新都會視需要由 AWS 套用。

網路工作

您可以執行網路工作，例如自訂與 Redshift 資料庫的連線。您也可以執行 DNS 相關工作，例如設定自訂網域名稱。如果您擁有 Amazon Redshift 佈建的叢集或 Amazon Redshift 無伺服器工作群組，您就可以使用這些組態任務。

主題

- [使用自訂網域名稱來進行用戶端連線](#)
- [使用 Redshift 管理的 VPC 端點](#)
- [Amazon Redshift 中的增強型 VPC 路由](#)

使用自訂網域名稱來進行用戶端連線

您可以為 Amazon Redshift 叢集和 Amazon Redshift Serverless 工作群組建立自訂網域名稱 (也稱為自訂 URL)。這是將 SQL 用戶端連線路由到您的端點的 easy-to-read DNS 記錄。您可以隨時為現有叢集或工作群組設定此項目。其提供了數種優勢：

- 自訂網域名稱比預設 URL 更簡單的字串，通常包括叢集名稱或工作群組名稱和區域。其更容易召回和使用。
- 例如，在容錯移轉案例中，您可以快速將流量路由至新叢集或工作群組。這會讓用戶端不必在重新連線時變更組態。連線可以集中地重新路由，而且中斷情況最少。
- 您可以避免在連線 URL 中共用私人資訊，例如同伺服器名稱。您可以將其隱藏在自訂 URL 中。

當您使用 CNAME 設定自訂網域名稱時，Amazon Redshift 不會產生任何額外費用。如果您建立新的網域名稱，DNS 供應商可能會向您收取相關費用，但金額通常很小。如需詳細資訊，請參閱[設定自訂網域名稱](#)。

自訂網域名稱的安全

Amazon Redshift 或 Amazon Redshift Serverless 需要經過驗證的 Secure Sockets Layer (SSL) 憑證，才能讓自訂端點確保通訊安全並驗證網域名稱的擁有權。您可以將您的 AWS Certificate Manager 帳戶與一起使用，以 AWS KMS key 進行安全的憑證管理。安全驗證包括完整的主機名稱驗證 (sslmode=verify-full)。

續約憑證

只有在選擇 DNS 驗證 (而非電子郵件驗證) 時，Amazon Redshift 才會管理憑證的續約。如果您使用電子郵件驗證，您還是可以使用憑證，但必須在憑證到期前自行續約。建議您為憑證選擇 DNS 驗證。您可以在 AWS Certificate Manager 中監控所匯入憑證的到期日期。

設定自訂網域名稱

設定自訂網域名稱包含幾項任務：其中包括向 DNS 提供者註冊網域名稱以及建立憑證。執行這些工作後，您可以在 Amazon Redshift 主控台或 Amazon Redshift 無伺服器主控台中設定自訂網域名稱，或使用命令進行設定。AWS CLI 下列各節會詳細說明這些步驟。

註冊網域名稱並選取憑證

您必須有已註冊的網際網路網域名稱，才能在 Amazon Redshift 中設定自訂網域名稱。您可以使用 Route 53 或第三方網域註冊提供商來註冊網際網路網域。您會在 Amazon Redshift 主控台之外完成這些任務。想要完成剩餘程序以便建立自訂網域，先決條件是要有已註冊的網域。。

Note


若您正在使用佈建的叢集，在執行相關步驟以設定自訂網域名稱之前，您必須先啟用重新定位。如需詳細資訊，請參閱 [重新定位叢集](#)。Amazon Redshift Serverless 不需要此步驟。

自訂網域名稱通常包括根網域和子網域，例如 `mycluster.example.com`。若要進行設定，請執行下列步驟：

為自訂網域名稱建立 DNS CNAME 項目

1. 註冊根網域，例如 `example.com`。您可以選擇使用現有網域。自訂名稱可能會受限於特定字元限制或其他命名驗證。如需使用 Route 53 註冊網域的相關資訊，請參閱 [註冊新網域](#)。
2. 針對您的叢集或工作群組，新增會將自訂網域指向 Redshift 端點的 DNS CNAME 記錄。您可以在叢集或工作群組的屬性、Redshift 主控台或 Amazon Redshift Serverless 主控台尋找端點。在一般資訊底下的叢集或工作群組屬性中複製可用的 JDBC URL。URL 顯示如下：
 - 對於 Amazon Redshift 叢集：`redshift-cluster-sample.abc123456.us-east-1.redshift.amazonaws.com`
 - 對於 Amazon Redshift Serverless 工作群組：`endpoint-name.012345678901.us-east-1-dev.redshift-serverless-dev.amazonaws.com`

如果 URL 具有 JDBC 字首，請將其移除。

 Note

DNS 記錄不一定都可供使用，因為每個名稱都必須是唯一的，並且可在您的組織中使用。

限制


為自訂網域建立 CNAME 記錄有幾項限制：

- 不支援為相同佈建的叢集或 Amazon Redshift Serverless 工作群組建立多個自訂網域名稱。您僅能為一個 CNAME 記錄建立關聯性。
- 不支援使 CNAME 記錄與多個叢集或工作群組產生關聯。每個 Redshift 資源的 CNAME 必須是唯一的。

在註冊網域並建立 CNAME 記錄後，您就要選取新的憑證或現有憑證。您可使用 AWS Certificate Manager 下列方式執行此步驟

向 ACM 請求網域名稱的憑證

1. 登入 AWS Management Console 並開啟 ACM 主控台，網址為 <https://console.aws.amazon.com/acm/>。
2. 選擇 Request a certificate (請求憑證)。
3. 在網域名稱欄位中輸入您的自訂網域名稱。

 Note

除了憑證網域外，您還可以指定許多字首，以便將單一憑證用於多個自訂網域記錄。若要說明，您可以搭配相同憑證來使用其他記錄，例如 `one.example.com`、`two.example.com` 或萬用字元 DNS 記錄如 `*.example.com`。

4. 選擇 Review and request (檢閱和請求)。
5. 選擇 Confirm and request (確認和請求)。
6. 針對有效的請求，在 ACM 發出憑證之前，網際網路網域的註冊擁有者必須先同意請求。完成這些步驟後，請確定狀態在 ACM 主控台中顯示為已發行。

我們建議您建立符合受管續約資格的 [DNS 驗證憑證](#)，此憑證適用於 AWS Certificate Manager。受管續約的意思是 ACM 會自動續約您的憑證，或在即將到期時傳送電子郵件通知給您。如需詳細資訊，請參閱 [ACM 憑證的受管續約](#)。

建立自訂網域

您可以使用 Amazon Redshift 或 Amazon Redshift Serverless 主控台來建立自訂網域 URL。如果您尚未設定，在一般資訊底下，自訂網域名稱屬性會顯示為破折號 (-)。建立 CNAME 記錄和憑證之後，為叢集或工作群組的自訂網域名稱建立關聯。

若要建立自訂網域關聯，您必須有下列 IAM 許可：

- `redshift:CreateCustomDomainAssociation` — 您可以透過新增特定叢集的 ARN 來限制特定叢集的許可。
- `redshiftServerless:CreateCustomDomainAssociation` — 您可以透過新增 ARN 來限制特定工作群組的許可。
- `acm:DescribeCertificate`

我們建議的最佳實務是，將許可政策附加到 IAM 角色，然後根據需要將其指派給使用者和群組。如需詳細資訊，請參閱 [Amazon Redshift 中的身分和存取管理](#)。

您可以透過執行下列步驟來指派自訂網域名稱。

1. 在 Amazon Redshift 主控台選擇叢集，或在 Amazon Redshift Serverless 主控台選擇工作群組，然後在動作功能表下選擇建立自訂網域名稱。隨即會出現對話方塊。
2. 輸入自訂網域名稱。
3. AWS Certificate Manager 針對 ACM 憑證，從中選取 ARN。確認變更。根據建立憑證所採取步驟中的指引，我們建議您選擇符合受管續約資格的 DNS 驗證憑證 AWS Certificate Manager。
4. 在叢集屬性中確認自訂網域名稱和自訂網域憑證 ARN 已填入您的項目。其中也會列出自訂網域憑證到期日。

設定好自訂網域後，使用 `sslmode=verify-full` 只會對新的自訂網域起作用。其不會對預設端點起作用。但是您仍然可以透過使用其他 ssl 模式 (例如 `sslmode=verify-ca`) 來連線到預設端點。

Note

提醒您，[叢集重新定位](#)不是設定其他 Redshift 網路功能的先決條件。您不需要開啟此功能即可啟用下列項目：

- 從跨帳戶或跨區域 VPC 連線至 Redshift — 您可以從一個 AWS 虛擬私人雲端 (VPC) 連線到包含 Redshift 資料庫的另一個虛擬私有雲端。這樣可以更輕鬆地管理，例如：從不同的帳戶或 VPC 進行用戶端存取，而不必提供本機 VPC 存取權限來連線至資料庫的身分識別。如需詳細資訊，請參閱[從其他帳戶或區域中的 Redshift VPC 端點連線至 Amazon Redshift Serverless](#)。
- 設定自訂網域名稱 — 您可以建立自訂網域名稱 (如本主題所述)，讓端點名稱更相關且簡單。

使用主控台重新命名已指派自訂網域的叢集

Note

這一系列步驟不適用於 Amazon Redshift Serverless 工作群組。您無法變更工作群組名稱。

若要重新命名具有自訂網域名稱的叢集，就必須有 `acm:DescribeCertificate` IAM 許可。

1. 前往 Amazon Redshift 主控台，然後選擇要變更其名稱的叢集。選擇編輯以編輯叢集屬性。
2. 叢集叢集識別碼。您也可以變更叢集的其他屬性。接著選擇 Save changes (儲存變更)。
3. 重新命名叢集之後，您必須更新 DNS 記錄，將自訂網域的 CNAME 項目變更為指向更新後的 Amazon Redshift 端點。

使用 CLI 命令描述自訂網域關聯

使用本節中的命令可取得與特定佈建叢集或 Amazon Redshift Serverless 工作群組相關聯的自訂網域名稱清單。

您需要具備下列許可：

- 針對已佈建的叢集：`redshift:DescribeCustomDomainAssociations`
- 對於 Amazon Redshift Serverless 工作群組：`redshiftServerless:ListCnameAssociations`

我們建議的最佳實務是，將許可政策附加到 IAM 角色，然後根據需要將其指派給使用者和群組。如需詳細資訊，請參閱 [Amazon Redshift 中的身分和存取管理](#)。

以下是列出指定 Amazon Redshift 叢集之自訂網域名稱的範例命令：

```
aws redshift describe-custom-domain-associations --custom-domain-name customdomainname
```

您可以在啟用自訂網域名稱時執行此命令，以判斷與叢集相關聯的自訂網域名稱。如需用來描述自訂網域關聯之 CLI 指令的詳細資訊，請參閱[describe-custom-domain-associations](#)。

同樣的，以下顯示範例命令以列出指定 Amazon Redshift Serverless 工作群組的自訂網域名稱。有幾種不同的方法可以做到這一點。您只能提供自訂網域名稱：

```
aws redshift-serverless list-custom-domain-associations --custom-domain-name customdomainname
```

您也可以透過僅提供憑證 ARN 來取得關聯：

```
aws redshift-serverless list-custom-domain-associations --custom-domain-certificate-arn certificatearn
```

當啟用自訂網域名稱以決定與工作群組相關聯的自訂網域名稱時，您可以執行這些命令。您也可以執行命令來取得自訂網域關聯的內容。若要這麼做，您必須提供自訂網域名稱和工作群組名稱做為參數。系統會傳回憑證 ARN、工作群組名稱和自訂網域的憑證到期時間：

```
aws redshift-serverless get-custom-domain-association --workgroup-name workgroupname --custom-domain-name customdomainname
```

如需適用於 Amazon Redshift Serverless 的 CLI 參考命令的詳細資訊，請參閱[redshift-serverless](#)。

使自訂網域與不同的憑證產生關聯

若要變更自訂網域名稱的憑證關聯，需要下列 IAM 許可：

- `redshift:ModifyCustomDomainAssociation`
- `acm:DescribeCertificate`

我們建議的最佳實務是，將許可政策附加到 IAM 角色，然後根據需要將其指派給使用者和群組。如需詳細資訊，請參閱[Amazon Redshift 中的身分和存取管理](#)。

使用下列命令以利用不同憑證與自訂網域建立關聯。`--custom-domain-name` 和 `custom-domain-certificate-arn` 引數是強制性的。新憑證的 ARN 必須與現有 ARN 不同。

```
aws redshift modify-custom-domain-association --cluster-id redshiftcluster --custom-domain-name customdomainname --custom-domain-certificate-arn certificatearn
```

以下範例顯示如何為自訂網域與 Amazon Redshift Serverless 工作群組的不同憑證建立關聯。

```
aws redshift-serverless modify-custom-domain-association --workgroup-name redshiftworkgroup --custom-domain-name customdomainname --custom-domain-certificate-arn certificatearn
```

連線到叢集之前，最多會延遲 30 秒。部分延遲發生在 Amazon Redshift 叢集更新其屬性時，並且在 DNS 更新時也會有一些額外的延遲。如需 API 和每個屬性設定的詳細資訊，請參閱 [ModifyCustomDomainAssociation](#)。

刪除自訂網域

若要刪除自訂網域名稱，使用者必須具有下列動作的許可：

- 針對已佈建的叢集：redshift>DeleteCustomDomainAssociation
- 對於 Amazon Redshift Serverless 工作群組：redshiftServerless>DeleteCustomDomainAssociation

在主控台上

您可以透過選取動作按鈕並選擇刪除自訂網域名稱來刪除自訂網域名稱。執行此操作之後，您仍然可以透過更新工具以使用主控台列出的端點來連接伺服器。

使用 CLI 指令

以下範例顯示如何刪除自訂網域名稱。刪除作業需要您提供叢集的現有自訂網域名稱。

```
aws redshift delete-custom-domain-association --cluster-id redshiftcluster --custom-domain-name customdomainname
```

以下範例顯示如何刪除 Amazon Redshift Serverless 工作群組的自訂網域名稱。自訂網域名稱是必要的參數。

```
aws redshift-serverless delete-custom-domain-association --workgroup-name workgroupname --custom-domain-name customdomainname
```

如需詳細資訊，請參閱 [DeleteCustomDomainAssociation](#)。

使用 SQL 用戶端連線至具有自訂網域名稱的叢集或工作群組

若要以自訂網域名稱的叢集連線，必須有下列 IAM 許可才能使用佈建的叢集：`redshift:DescribeCustomDomainAssociations`。對於 Amazon Redshift Serverless 伺服器，您不需新增許可。

我們建議的最佳實務是，將許可政策附加到 IAM 角色，然後根據需要將其指派給使用者和群組。如需詳細資訊，請參閱 [Amazon Redshift 中的身分和存取管理](#)。

在主控台完成建立 CNAME 並將其指派給叢集的步驟後，您可以在 SQL 用戶端的連線屬性中提供自訂 URL。請注意，建立 CNAME 記錄之後，系統會立即因為 DNS 傳播而發生延遲。

1. 開啟 SQL 用戶端。例如，您可以使用 SQL/Workbench J。開啟連線的屬性，並新增連線字串的自訂網域名稱。例如 `jdbc:redshift://mycluster.example.com:5439/dev?sslmode=verify-full`。在此範例中，`dev` 會指定預設資料庫。
2. 新增資料庫使用者的使用者名稱和密碼。
3. 測試連線。根據向資料庫使用者授予的許可或向所指派的 Amazon Redshift 資料庫角色授予的許可，您查詢資料庫資源 (例如特定資料表) 的能力會有所不同。

請注意，如果在 VPC 中，您可能必須將叢集或工作群組設定為可公開存取，才能連線到叢集或工作群組。您可以在網路屬性中變更此設定。

Note

JDBC 和 Python 驅動程式支援與自訂網域名稱的連線。不支援 ODBC 連線。

使用 Redshift 管理的 VPC 端點

根據預設，Amazon Redshift 叢集或 Amazon Redshift 無伺服器工作群組會佈建在虛擬私有雲端 (VPC) 中。當您允許公用存取或設定網際網路閘道、NAT 裝置或將流量路由到 VPC 的 AWS Direct Connect 連線時，可以從其他 VPC 或子網路存取 VPC。您也可以透過設定 RedShift 管理的 VPC 端點 (由支援) 來存取叢集或工作群組。AWS PrivateLink

您可以將 RedShift 管理的 VPC 端點設定為包含叢集或工作群組的 VPC 與執行用戶端工具的 VPC 之間的私人連線。如果叢集或工作群組位於其他帳戶中，則帳戶擁有者 (授與者) 必須授與連線帳戶 (受權者) 的存取權。使用這種方法，您可以存取資料倉儲，而無需使用公用 IP 位址或透過網際網路路由傳送流量。

以下是允許使用 RedShift 管理的 VPC 端點進行存取的常見原因：

- AWS 帳戶 A 想要允許 AWS 帳戶 B 中的 VPC 存取叢集或工作群組。
- AWS 帳戶 A 想要允許也在 AWS 帳戶 A 中的 VPC 具有叢集或工作群組的存取權。
- AWS 帳戶 A 想要允許 AWS 帳戶 A 內 VPC 中的不同子網路存取叢集或工作群組。

設定 RedShift 管理的 VPC 端點以存取其他帳戶中的叢集或工作群組的工作流程如下：

1. 擁有者帳戶將存取權授予其他帳戶，並指定受權者的 AWS 帳戶 ID 和 VPC 識別碼 (或所有 VPC)。
2. 被授予者帳戶收到通知，指出其已擁有建立 Redshift 管理的 VPC 端點的許可。
3. 被授予者帳戶建立 Redshift 管理的 VPC 端點。
4. 受權者帳戶會使用 RedShift-管理的 VPC 端點存取擁有者帳戶的叢集或工作群組。

您可以使用 Amazon Redshift 控制台，或亞 Amazon Redshift API 來執行此操作。AWS CLI

使用 Redshift 管理的 VPC 端點時的考量

Note

若要建立或修改 RedShift-託管的 VPC 端點，除了 `ec2:ModifyVpcEndpoint` 在受管政策中指定的其他許可外，您還需要在 IAM 政策中獲得許可 `ec2:CreateVpcEndpoint` 或存取權管理政策。AWS `AmazonRedshiftFullAccess`

在使用 Redshift 管理的 VPC 端點時，請記住以下事項：

- 確定要存取的叢集是 RA3 節點類型。亞 Amazon Redshift 無服務器工作組也適用於此。
- 對於佈建的叢集，請確定叢集已啟用叢集重新定位或異地同步備份。如需開啟叢集重新定位要求的相關資訊，請參閱 [重新定位叢集](#)。如需啟用異地同步備份的資訊，請參閱 [在建立新叢集時設定多可用區](#)。
- 請確定要透過其安全性群組存取的叢集或工作群組可在有效連接埠範圍 5431-5455 和 8191-8215 內使用。預設值為 5439。
- 您可以修改與現有 Redshift 管理的 VPC 端點相關聯的 VPC 安全群組。若要修改其他設定，請刪除目前的 Redshift 管理的 VPC 端點並建立新端點。
- 您可建立的 Redshift 管理的 VPC 端點數目受限於 VPC 端點的配額。

- Redshift 管理的 VPC 端點無法從網際網路存取。RedShift 管理的 VPC 端點只能在佈建端點的 VPC 內存取，或從任何與 VPC 對等的 VPC 存取 (該端點是在路由表和安全群組允許的情況下佈建端點)。
- 您無法使用 Amazon VPC 主控台來管理 Redshift 管理的 VPC 端點。
- 當您為已佈建的叢集建立 RedShift 管理的 VPC 端點時，您選擇的 VPC 必須具有子網路群組。若要建立子網路群組，請參閱[使用主控台管理叢集子網路群組](#)。
- 如果可用區域關閉，Amazon Redshift 就不會在另一個可用區域中建立新的 elastic network interface。在此情況下，您可能需要建立新端點。

如需有關配額和命名限制的資訊，請參閱 [Amazon Redshift 中的配額和限制](#)。

如需定價的詳細資訊，請參閱 [AWS PrivateLink 定價](#)。

使用主控台管理由 RedShift 管理的 VPC 人雲端端點

您可以透過使用 Amazon Redshift 主控台來設定 Redshift 管理的 VPC 端點的使用。

授與 存取權

如果您要存取叢集或工作群組的 VPC 位於其他 AWS 帳戶中，請確定從擁有者 (授與者) 帳戶授權該 VPC。

允許其他 AWS 帳戶中的 VPC 存取您的叢集或工作群組

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽選單上，選擇叢集。對於 Amazon Redshift 無伺服器，請選擇無伺服器儀表板。
3. 對於您要允許存取的叢集，請選擇叢集名稱來檢視詳細資訊。選擇叢集的屬性索引標籤。

已授予的帳戶區段會顯示可存取您叢集的帳戶和對應的 VPC。如果是 Amazon Redshift 無伺服器工作群組，請選擇工作群組。授與的帳戶可在「資料存取」標籤下找到。

4. 選擇授予存取權以顯示表單，供您輸入要新增帳戶的被授予者資訊。
5. 對於 AWS 帳戶 ID，輸入您要授予存取權之帳戶的 ID。您可以授予存取權給指定帳戶中的特定 VPC 或所有 VPC。
6. 選擇授予存取權以授予存取權。

建立 Redshift 管理的 VPC 端點

如果您擁有叢集或工作群組，或者您已獲得管理叢集或工作群組的存取權，則可以為其建立由 RedShift 管理的 VPC 端點。

建立 Redshift 管理的 VPC 端點

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽功能表上，選擇組態。

組態頁面會顯示已建立的 Redshift 管理的 VPC 端點。若要檢視端點的詳細資訊，請選擇其名稱。對於 Amazon Redshift 無伺服器，當您選擇工作群組時，VPC 端點位於「資料存取」索引標籤下。

3. 選擇建立端點以顯示表單，供您輸入要新增之端點的相關資訊。
4. 輸入端點名稱、12 位數 AWS 帳號識別碼、端點所在的虛擬私人雲端 (VPC)、子網路和 VPC 安全性群組的值。

子網路中的子網路會定義 Amazon Redshift 在其中部署端點的子網路和 IP 位址。Amazon Redshift 會選擇具有 IP 地址可供與該端點相關聯之網路介面使用的子網路。

VPC 安全群組中的安全群組規則會定義您為端點授權之入站流量的連接埠、通訊協定和來源。您允許透過安全性群組或工作負載執行的 CIDR 範圍存取所選連接埠。

5. 選擇建立端點以建立端點。

建立端點之後，您可以透過 RedShift 管理的 VPC 端點組態設定中端點 URL 中顯示的 URL 存取叢集或工作群組。

使用管理 RedShift 管理的 VPC 人雲端端點 AWS CLI

您可以使用下列 Amazon Redshift CLI 操作來使用 Redshift 管理的 VPC 端點。如需詳細資訊，請參閱《AWS CLI 命令參考》。

- [authorize-endpoint-access](#)
- [revoke-endpoint-access](#)
- [create-endpoint-access](#)
- [modify-endpoint-access](#)

- [delete-endpoint-access](#)
- [describe-endpoint-access](#)
- [describe-endpoint-authorization](#)

使用 Amazon Redshift API 操作來管理 Redshift 管理的 VPC 端點

您可以使用下列 Amazon Redshift API 操作來使用 Redshift 管理的 VPC 端點。如需詳細資訊，請參閱《Amazon Redshift API 參考》。

- [AuthorizeEndpointAccess](#)
- [RevokeEndpointAccess](#)
- [CreateEndpointAccess](#)
- [ModifyEndpointAccess](#)
- [DeleteEndpointAccess](#)
- [DescribeEndpointAccess](#)
- [DescribeEndpointAuthorization](#)

使用以下方式管理 RedShift 管理的 VPC 端點 AWS CloudFormation

如需用來建立 RedShift-管理的 VPC 端點之 AWS CloudFormation 資源類型的相關資訊 AWS CloudFormation，請參閱使用者指南[AWS::Redshift::EndpointAccess](#)中的。AWS CloudFormation

Amazon Redshift 中的增強型 VPC 路由

當您使用 Amazon Redshift 增強型 VPC 路由時，Amazon Redshift 會根據 Amazon VPC 服務來強制叢集與資料儲存庫之間所有的 [COPY](#) 與 [UNLOAD](#) 流量通過您的虛擬私有雲端 (VPC)。使用增強型 VPC 路由時，您可以使用標準 VPC 功能，例如 [VPC 安全群組](#)、[網路存取控制清單 \(ACL\)](#)、[VPC 端點](#)、[VPC 端點政策](#)、[網際網路閘道](#)，以及 [網域名稱系統 \(DNS\)](#) 伺服器，如《Amazon VPC 使用者指南》中所述。您可以使用這些功能來密切管理 Amazon Redshift 叢集與其他資源之間的資料流動。當您使用增強型 VPC 路由以透過 VPC 路由流量時，亦可使用 [VPC 流程日誌](#) 來監控 COPY 與 UNLOAD 流量。

Amazon Redshift 叢集和 Amazon Redshift Serverless 工作群組支援增強型 VPC 路由。您無法搭配 Redshift Spectrum 使用增強型 VPC 路由。如需詳細資訊，請參閱 [Redshift Spectrum 和增強型 VPC 路由](#)。

如果未開啟增強型 VPC 路由，Amazon Redshift 會透過網際網路路由流量，包括網路內其他服務的 AWS 流量。

⚠ Important

由於增強型 VPC 路由會影響 Amazon Redshift 存取其他資源的方式，COPY 與 UNLOAD 命令可能會失敗，除非您正確設定 VPC。您必須在叢集的 VPC 與資料資源之間特別建立網路路徑，如下所述。

當您在已開啟增強型 VPC 路由的叢集上執行 COPY 或 UNLOAD 命令時，您的 VPC 會使用「最嚴格」（或最獨特）可用的網路路徑，將流量路由至指定的資源。

例如，您可以在 VPC 中設定下列路徑：

- VPC 端點 — 對於流量到與叢集位於相同 AWS 區域的 Amazon S3 儲存貯體，您可以建立 VPC 端點以將流量直接導向儲存貯體。當您使用 VPC 端點時，可以連接端點政策以管理 Amazon S3 的存取。如需將端點與 Amazon Redshift 搭配使用的相關資訊，請參閱[使用 VPC 端點](#)。如果您使用 Lake Formation，您可以找到有關在 AWS VPC 和湖泊形成的 AWS Lake Formation 和接[口 VPC 端點之間建立私人連接的更多信息 \(\) AWS PrivateLink](#)。

📘 Note

當您將 Redshift VPC 端點與 Amazon S3 虛擬私人 VPC 端閘道端點搭配使用時，必須在 Redshift 中啟用增強型 VPC 雲端路由。如需詳細資訊，請參閱[Amazon S3 的閘道端點](#)。

- NAT 閘道 — 您可以連接到另一個 AWS 區域的 Amazon S3 儲存貯體，也可以連線到 AWS 網路中的其他服務。您也可以存取 AWS 網路外部的主機執行個體。若要這麼做，請設定[網路位址轉譯 \(NAT\) 閘道](#)，如《Amazon VPC 使用者指南》中所述。
- 網際網路閘道 — 若要連線至 VPC 外的 AWS 服務，您可以將[網際網路閘道](#)附加至您的 VPC 子網路，如《Amazon VPC 使用者指南》中所述。若要使用網際網路閘道，您的叢集必須有公有 IP，以便讓其他服務與您的叢集進行通訊。

如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的[VPC 端點](#)。

使用增強型 VPC 路由無需額外付費。某些操作可能需要額外的數據傳輸費。這些操作包括在不同 AWS 區域中卸載到 Amazon S3 之類的操作。從 Amazon EMR 或 Secure Shell (SSH) 透過公有 IP 地址 COPY。如需定價的相關資訊，請參閱[Amazon EC2 定價](#)。

主題

- [使用 VPC 端點](#)
- [增強型 VPC 路由](#)
- [Redshift Spectrum 和增強型 VPC 路由](#)

使用 VPC 端點

您可以使用 VPC 端點，在 VPC 中的 Amazon Redshift 叢集與 Amazon Simple Storage Service (Amazon S3) 之間建立受管連線。當您這麼做時，資料庫與 Amazon S3 上的資料之間的 COPY 與 UNLOAD 流量會停留在 Amazon VPC 中。您可以將端點政策連接至您的端點，更緊密地管理您資料的存取。例如，您可以將政策新增至您的 VPC 端點，僅允許資料上傳至您帳戶中特定的 Amazon S3 儲存貯體。

若要使用 VPC 端點，請為資料倉儲所在的 VPC 建立 VPC 端點，然後開啟增強型 VPC 路由。您可以在建立叢集或工作群組時開啟增強型 VPC 路由，也可以修改 VPC 中的叢集或工作群組以使用增強型 VPC 路由。

VPC 端點使用路由表來控制 VPC 中的叢集或工作群組與 Amazon S3 之間流量的路由。與指定之路由表關聯之子網路中的所有叢集和工作群組會自動使用該端點來存取服務。

您的 VPC 使用最具體或最嚴格且匹配您流量的路由，以判斷如何路由流量。例如，假設您的路由表中有路由處理指向網際網路閘道和 Amazon S3 端點的所有網際網路流量 (0.0.0.0/0)。在此情況下，端點路由會優先處理所有以 Amazon S3 為目的地的流量。這是因為 Amazon S3 服務的 IP 地址比 0.0.0.0/0 更明確。在此範例中，所有其他網際網路流量會流向網際網路閘道，包括以其他 AWS 區域區域中的 Amazon S3 儲存貯體為目的地的流量。

如需建立端點的相關資訊，請參閱《Amazon VPC 使用者指南》中的[建立 VPC 端點](#)。

您使用端點政策，控制從您的叢集或工作群組對於存有您資料檔案之 Amazon S3 儲存貯體的存取。如需更精確的控制，您可以選擇連接自訂端點政策。如需詳細資訊，請參閱《AWS PrivateLink 指南》中的[使用端點政策控制對服務的存取](#)。

Note

AWS Database Migration Service (AWS DMS) 是一種雲端服務，可讓您移轉關聯式資料庫、資料倉儲和其他類型的資料存放區。它可以連接到任何 AWS 來源或目標資料庫，包括已啟用 VPC 的 Amazon Redshift 資料庫，但有一些組態限制。支援 Amazon VPC 端點可讓 AWS DMS 您更輕鬆地維護複寫任務的 end-to-end 網路安全。如需有關[搭配使用 Redshift 的詳細](#)

資訊 AWS DMS，請參閱《使用手冊》中的〈將 VPC 端點設定為 AWS DMS 來源和目標端點 AWS Database Migration Service〉。

使用端點無需額外付費。需支付標準數據傳輸與資源使用費。如需有關定價的詳細資訊，請參閱 [Amazon EC2 定價](#)。

增強型 VPC 路由

您可以在建立或修改叢集時，以及建立或修改 Amazon Redshift Serverless 工作群組時，開啟增強型 VPC 路由。

若要針對叢集使用增強型 VPC 路由，叢集必須符合以下要求與限制條件：

- 您的叢集必須在 VPC 中。

如果您連接 Amazon S3 VPC 端點，則叢集只會使用 VPC 端點來存取相同 AWS 區域中的 Amazon S3 儲存貯體。若要存取其他 AWS 區域中的值區 (不使用 VPC 端點) 或存取其他 AWS 服務，請讓叢集可公開存取，或使用 [網路位址轉譯 \(NAT\) 閘道](#)。如需詳細資訊，請參閱 [在 VPC 中建立叢集](#)。

- 您必須在 VPC 中啟用網域名稱服務 (DNS) 解析。或者，如果您使用自己的 DNS 伺服器，請確定對 Amazon S3 提出的 DNS 請求可正確解析為 AWS 所維護的 IP 地址。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的 [使用 DNS 與您的 VPC 搭配](#)。
- 您的 VPC 必須啟用 DNS 主機名稱。DNS 主機名稱預設為啟用。
- 您的 VPC 端點政策必須允許存取 Amazon Redshift 中的 COPY、UNLOAD 或 CREATE LIBRARY 呼叫所使用的任何 Amazon S3 儲存貯體，包括存取任何涉及的資訊清單檔案。對於來自遠端主機的 COPY，您的端點政策必須允許存取每個主機機器。如需詳細資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的 [COPY、UNLOAD 和 CREATE LIBRARY 的 IAM 許可](#)。

建立具有增強型 VPC 路由的叢集

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽功能表上，選擇佈建叢集儀表板，然後選擇建立叢集並輸入叢集詳細資訊屬性。
3. 若要顯示 Additional configurations (其他組態) 區段，請選擇關閉 Use defaults (使用預設值)。
4. 導覽至網路和安全區段。
5. 若要開啟增強型 VPC 路由，請選擇開啟以強制透過 VPC 傳輸叢集流量。

6. 選擇 Create cluster (建立叢集) 以建立叢集。該叢集可能需要幾分鐘方可使用。

透過增強型 VPC 路由建立 Amazon Redshift Serverless 工作群組

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽功能表上，選擇 Serverless 儀表板，然後選擇建立工作群組並輸入工作群組的屬性。
3. 導覽至網路和安全區段。
4. 選取開啟增強型 VPC 路由以透過 VPC 來路由網路流量。
5. 選擇下一步並完成工作群組屬性的輸入，直到您建立工作群組為止。

Redshift Spectrum 和增強型 VPC 路由

Amazon Redshift Spectrum 不支援使用已佈建叢集的增強型 VPC 路由。Amazon Redshift 增強型 VPC 路由會將特定流量路由通過您的 VPC。叢集與 Amazon S3 儲存貯體之間的所有流量都會強制通過您的 Amazon VPC。Redshift 頻譜在 Amazon Redshift 擁有的 AWS 受管資源上執行。因為這些資源位於 VPC 外，所以 Redshift Spectrum 不會使用增強型 VPC 路由。

Redshift 頻譜和 Amazon S3 之間的流量會透過虛擬 AWS 私人網路安全地路由到 VPC 之外。傳輸中的流量是使用 Amazon Signature 第 4 版通訊協定 (SIGv4) 來簽署，並使用 HTTPS 來加密。此流量是根據連接到 Amazon Redshift 叢集的 IAM 角色而獲得授權。若要進一步管理 Redshift Spectrum 流量，您可以修改叢集的 IAM 角色和已連接到 Amazon S3 儲存貯體的政策。您可能還需要將 VPC 設定為允許叢集存取 AWS Glue 或 Athena，如下所述。

請注意，由於增強型 VPC 路由會影響 Amazon Redshift 存取其他資源的方式，查詢可能會失敗，除非您正確設定 VPC。如需詳細資訊，請參閱 [Amazon Redshift 中的增強型 VPC 路由](#)，其中會詳細討論如何建立 VPC 端點、NAT 閘道和其他網路資源，以將流量導向 Amazon S3 儲存貯體。

Note

Amazon Redshift Serverless 支援將增強型 VPC 路由用於 Amazon S3 上外部資料表的查詢。

使用 Amazon Redshift Spectrum 時的考量

以下是使用 Redshift Spectrum 時的考量：

- [儲存貯體存取政策](#)

- [叢集 IAM 角色](#)
- [記錄和稽核 Amazon S3 存取](#)
- [訪問 AWS Glue 或 Amazon Athena](#)

儲存貯體存取政策

您可以使用連接到儲存貯體的儲存貯體政策，以及使用連接到叢集的 IAM 角色，以控制存取 Amazon S3 儲存貯體中的資料。

如果 Amazon S3 儲存貯體使用的儲存貯體政策僅限於存取指定的 VPC 端點，佈建叢集上的 Redshift Spectrum 便無法存取該儲存貯體中儲存的資料。請改用儲存貯體策略來限制只能存取特定主體，例如特定 AWS 帳戶或特定使用者。

對於獲授權存取儲存貯體的 IAM 角色，請使用只允許由 Amazon Redshift 服務主體擔任該角色的信任關係。連接到叢集時，該角色只能用於 Amazon Redshift 的內容中，不能在叢集外共用。如需詳細資訊，請參閱 [限制對 IAM 角色的存取](#)。服務控制政策 (SCP) 也可用於進一步限制角色，請參閱《AWS Organizations 使用者指南》中的 [防止 IAM 使用者和角色進行指定變更，且指定的管理員角色除外](#)。

Note

若要使用 Redshift 頻譜，則無法制定任何 IAM 政策阻止使用 Amazon S3 預先簽署的 URL。Amazon Redshift Spectrum 產生的預先簽署網址有效期為 1 小時，因此亞馬遜 Redshift 有足夠的時間從 Amazon S3 儲存貯體載入所有檔案。Redshift 頻譜掃描的每個檔案都會產生一個唯一的預先簽署 URL。對於包含 `s3:signatureAge` 動作的值區政策，請務必將值設定為至少 3,600,000 毫秒。

下列範例值區政策只允許從 AWS 帳戶 123456789012 所擁有的 Redshift Spectrum 產生的流量存取指定值區。

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "BucketPolicyForSpectrum",
    "Effect": "Allow",
    "Principal": {
      "AWS": ["arn:aws:iam::123456789012:role/redshift"]
    },
    "Action": ["s3:GetObject", "s3:List*"],
```

```

"Resource": ["arn:aws:s3:::examplebucket/*"],
"Condition": {
  "StringEquals": {
    "aws:UserAgent": "AWS Redshift/Spectrum"
  }
}
]]
}

```

叢集 IAM 角色

連接到叢集的角色應該具有只允許 Amazon Redshift 服務擔任該角色的信任關係，如下所示。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "redshift.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}

```

您可以將政策新增至叢集角色，以防止 COPY 和 UNLOAD 存取特定的貯體政策。以下政策僅允許來自 Redshift Spectrum 的流量才能流向指定的儲存貯體。

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": ["s3:Get*", "s3:List*"],
    "Resource": "arn:aws:s3:::myBucket/*",
    "Condition": {"StringEquals": {"aws:UserAgent": "AWS Redshift/
Spectrum"}}
  ]
}

```

如需詳細資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的 [Redshift Spectrum 的 IAM 政策](#)。

記錄和稽核 Amazon S3 存取

使用 Amazon Redshift 增強型 VPC 路由的一項好處是所有 COPY 和 UNLOAD 流量都記錄在 VPC 流程日誌中。源自 Redshift Spectrum 到 Amazon S3 的流量不會通過 VPC，所以沒有記錄在 VPC 流程日誌中。當 Redshift 頻譜存取 Amazon S3 中的資料時，它會根據 AWS 帳戶的內容和個別的角色權限執行這些操作。您可以在 AWS CloudTrail 和 Amazon S3 中使用伺服器存取日誌記錄，以記錄和稽核 Amazon S3。

確定 S3 IP 範圍已新增至您的允許清單。若要進一步了解所需的 S3 IP 範圍，請參閱[網路隔離](#)。

AWS CloudTrail 日誌

若要追蹤 Amazon S3 中物件的所有存取權限 (包括 Redshift 頻譜存取)，請啟用 Amazon S3 物件的 CloudTrail 記錄功能。

您可以用 CloudTrail 來檢視、搜尋、下載、封存、分析和回應 AWS 基礎結構中的帳戶活動。如需詳細資訊，請參閱[入門 CloudTrail](#)。

依預設，只會 CloudTrail 追蹤值區層級的動作。若要追蹤物件層級的動作 (例如 GetObject)，請對每一個已記錄的儲存貯體啟用資料和管理事件。

Amazon S3 伺服器存取記錄

伺服器存取記錄日誌，應儲存貯體要求，提出的詳細記錄。存取記錄資訊在安全與存取稽核中相當實用。如需詳細資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的[如何啟用伺服器存取記錄](#)。

如需詳細資訊，請參閱 AWS 安全部落格文章[如何使用儲存貯體政策和套用深度防禦來協助保護 Amazon S3 資料的安全](#)。

訪問 AWS Glue 或 Amazon Athena

Redshift 頻譜可存取您在 AWS Glue 或 Athena 的資料目錄。另一個選項是使用專用的 Hive 中繼存放區來處理資料目錄。

若要啟用對 AWS Glue 或 Athena 的存取，請使用網際網路閘道或 NAT 閘道來設定您的 VPC。設定您的 VPC 安全群組，以允許 AWS Glue 和 Athena 的公用端點輸出流量。或者，您可以設定介面 VPC 端點 AWS Glue 以存 AWS Glue Data Catalog。當您使用 VPC 介面端點時，VPC 之間的通訊會 AWS Glue 在網路內進行。AWS 如需詳細資訊，請參閱[建立介面端點](#)。

您可以在 VPC 中設定下列路徑：

- 網際網路閘道 — 若要連接到 VPC 外部的 AWS 服務，您可以將[網際網路閘道](#)連接到 VPC 子網路，如 Amazon VPC 使用者指南中所述。若要使用網際網路閘道，您的叢集必須有公有 IP 地址，以便讓其他服務與您的叢集進行通訊。
- NAT 閘道 — 若要連線至其他 AWS 區域中的 Amazon S3 儲存貯體或 AWS 網路內的其他服務，請按照 Amazon VPC 使用者指南中所述設定[網路位址轉譯 \(NAT\) 閘道](#)。您也可以使用此組態來存取 AWS 網路外的主機執行個體。

如需更多詳細資訊，請參閱 [Amazon Redshift 中的增強型 VPC 路由](#)。

監控 Amazon Redshift 叢集效能

Amazon Redshift 提供您可以追蹤叢集和資料庫之運作狀態和效能的效能指標和資料。在本節中，我們討論您可在 Amazon Redshift (特別是 Amazon Redshift 主控台) 中處理的資料類型。

主題

- [概觀](#)
- [使 CloudWatch 用指標監控 Amazon Redshift](#)
- [在 Amazon Redshift 主控台中使用效能資料](#)

概觀

您可以在 Amazon Redshift 主控台中使用的效能資料之種類有兩種：

- **Amazon CloudWatch 指標** — Amazon CloudWatch 指標可協助您監控叢集的實體層面，例如 CPU 使用率、延遲和輸送量。Amazon Redshift 主控台中將直接顯示指標資料。您也可以 CloudWatch 控制台中查看它。或者，您可以使用任何其他方式使用指標，例如使用 AWS CLI 或其中一個 AWS SDK。
- **查詢/載入效能資料** — 效能資料可協助您監控資料庫活動和效能。此資料彙總在 Amazon Redshift 主控台中，以協助您輕鬆地將 CloudWatch 指標中看到的內容與特定資料庫查詢和載入事件建立關聯。您也可以建立自己的自訂效能查詢，並在資料庫上執行他們。Amazon Redshift 主控台中僅顯示查詢和載入效能資料。它不會以 CloudWatch 量度的形式發佈。

效能資料會整合至 Amazon Redshift 主控台中，以下列方式帶來更豐富的體驗：

- 在您檢視叢集，而您可以需要進行如重新調整大小之與叢集有關的決定時，與叢集關聯的效能資料會隨之顯示。
- 相較於 Amazon Redshift 主控台，部分效能指標會以 CloudWatch 更適當調整的單位顯示。例如 WriteThroughput，以 GB/s 顯示 (與中的位元組相比 CloudWatch)，這是節點典型儲存空間的相關單位。
- 您可以輕鬆在相同圖表上一起顯示某叢集之節點的效能資料。您可以透過此方式來監控叢集之所有節點的效能。您也可以檢視每個節點的效能資料。

Amazon Redshift 提供效能資料 (包括 CloudWatch 指標、查詢和載入資料)，無需額外付費。效能資料會每秒記錄。您可以在 Amazon Redshift 主控台中存取效能資料的歷史值。如需有關使用存取

CloudWatch 以 CloudWatch 指標形式公開的 Amazon Redshift 效能資料的詳細資訊，請參閱 [什麼是 CloudWatch ?](#) 在 Amazon 用 CloudWatch 戶指南。

使 CloudWatch 用指標監控 Amazon Redshift

使用 Amazon Redshift 的 CloudWatch 指標，您可以取得叢集運作狀態和效能的相關資訊，並查看節點層級的資訊。使用這些指標時，請謹記每個指標都有一或多個與其關聯的維度。您可透過這些維度來知道指標適用的項目，也就是指標的範圍。Amazon Redshift 具有以下兩個維度：

- 具有 NodeID 維度的指標即為提供叢集的節點之效能資料的指標。這組指標包含領導與運算節點。這些指標的範例包括：CPUUtilization、ReadIOPS、WriteIOPS。
- 僅具有 ClusterIdentifier 維度的指標即為提供叢集之效能資料的指標。這些指標的範例包括：HealthStatus 和 MaintenanceMode。

Note

在這些指標案例中，叢集特定指標代表的是節點行為的彙總。在這些案例中，請留意指標值的解譯，因為領導節點的行為會透過運算節點來彙總。

有關指 CloudWatch 標和維度的一般資訊，請參閱 Amazon CloudWatch 使用者指南中的 [CloudWatch 概念](#)。

如需 Amazon Redshift CloudWatch 指標的進一步說明，請參閱以下各節。

主題

- [Amazon Redshift 指標](#)
- [Amazon Redshift 指標的維度](#)
- [Amazon Redshift 查詢和載入效能資料](#)

Amazon Redshift 指標

AWS/Redshift 命名空間包含下列指標。除非另有說明，否則會每隔 1 分鐘收集指標。

Title

指標	描述
CommitQueueLength	<p>在指定時間點等待認可的交易數目。</p> <p>單位：計數</p> <p>維度：ClusterIdentifier</p>
ConcurrencyScaling ActiveClusters	<p>在任何指定時間主動處理查詢的並行擴展叢集數量。</p> <p>單位：計數</p> <p>維度：ClusterIdentifier</p>
ConcurrencyScaling Seconds	<p>有主動查詢處理活動的並行擴展叢集所使用的秒數。</p> <p>單位：計數</p> <p>維度：ClusterIdentifier</p>
CPUUtilization	<p>CPU 使用率。以叢集而言，此指標代表所有節點 (領導者與運算) CPU 使用值的彙整。</p> <p>單位：百分比</p> <p>尺寸: ClusterIdentifier , NodeID</p> <p>維度：ClusterIdentifier</p>
DatabaseConnections	<p>叢集的資料庫連線數量。</p> <p>單位：計數</p> <p>維度：ClusterIdentifier</p>
HealthStatus	<p>表示叢集運作狀態。叢集每分鐘連線至其資料庫並執行建議查詢。如果成功執行此操作，該叢集將被視為運作正常。否則，表示該叢集運作不良。不良狀態可能會發生於資料庫處於極高負載，或叢集上的資料庫有組態的問題。</p>

指標	描述
	<p>Note</p> <p>在 Amazon 中 CloudWatch，此指標報告為 1 或 0，而在 Amazon Redshift 控制台中，此指標與文字一起顯示 HEALTHY 或 UNHEALTHY 為了方便起見。此指標顯示於 Amazon Redshift 主控台時，將忽略取樣平均值，只會顯示 HEALTHY 或 UNHEALTHY。在 Amazon 中 CloudWatch，由於採樣問題，可能會出現與 1 和 0 不同的值。小於 1 的任何 HealthStatus 值都將回報為 0 (UNHEALTHY)。</p> <p>單位：計數 (1/0) (在 Amazon Redshift 主控台中為 HEALTHY/UNHEALTHY)</p> <p>維度：ClusterIdentifier</p>
MaintenanceMode	<p>表示叢集是否處於維護模式。</p> <p>Note</p> <p>在 Amazon 中 CloudWatch，此指標報告為 1 或 0，而在 Amazon Redshift 控制台中，此指標與文字一起顯示 ON 或 OFF 為了方便起見。此指標顯示於 Amazon Redshift 主控台時，將忽略取樣平均值，只會顯示 ON 或 OFF。在 Amazon 中 CloudWatch，由於採樣問題，可能會出現與 1 和 0 不同的值。大於 0 的任何 MaintenanceMode 值都將回報為 1 (ON)。</p> <p>單位：計數 (1/0) (在 Amazon Redshift 主控台中為 ON/OFF)。</p> <p>維度：ClusterIdentifier</p>

指標	描述
MaxConfiguredConcurrencyScalingClusters	<p>從參數群組設定檔最大並行擴展叢集數量。如需詳細資訊，請參閱 Amazon Redshift 參數群組。</p> <p>單位：計數</p> <p>維度：ClusterIdentifier</p>
NetworkReceiveThroughput	<p>節點或叢集接收資料的速率。</p> <p>單位：位元組/秒 (在 Amazon Redshift 主控台中為 MB/秒)</p> <p>尺寸: ClusterIdentifier , NodeID</p> <p>維度：ClusterIdentifier</p>
NetworkTransmitThroughput	<p>節點或叢集寫入資料的速率。</p> <p>單位：位元組/秒 (在 Amazon Redshift 主控台中為 MB/秒)</p> <p>尺寸: ClusterIdentifier , NodeID</p> <p>維度：ClusterIdentifier</p>
PercentageDiskSpaceUsed	<p>已使用的磁碟空間的百分比。</p> <p>單位：百分比</p> <p>維度：ClusterIdentifier</p> <p>尺寸: ClusterIdentifier , NodeID</p>
QueriesCompletedPerSecond	<p>平均每秒完成的查詢次數。每隔 5 分鐘回報。單節點叢集不支援此指標。</p> <p>單位：計數/秒</p> <p>尺寸: ClusterIdentifier , latency</p> <p>尺寸: ClusterIdentifier , wlmid</p>

指標	描述
QueryDuration	<p>完成查詢的平均時間。每隔 5 分鐘回報。單節點叢集不支援此指標。</p> <p>單位：微秒</p> <p>維度：ClusterIdentifier、NodeID、latency</p> <p>尺寸：ClusterIdentifier、latency</p> <p>維度：ClusterIdentifier、NodeID、wlmid</p>
QueryRuntimeBreakdown	<p>查詢階段執行所花費的查詢總時間。每隔 5 分鐘回報。</p> <p>單位：毫秒</p> <p>尺寸：ClusterIdentifier、NodeID、階段</p> <p>尺寸：ClusterIdentifier、舞台</p>
ReadIOPS	<p>磁碟讀取操作的每秒平均次數。</p> <p>單位：計數/秒</p> <p>尺寸：ClusterIdentifier、NodeID</p> <p>維度：ClusterIdentifier</p>
ReadLatency	<p>用於磁碟讀取 I/O 操作的平均時間量。</p> <p>單位：秒</p> <p>尺寸：ClusterIdentifier、NodeID</p> <p>維度：ClusterIdentifier</p>

指標	描述
ReadThroughput	<p>平均每秒從磁碟讀取的位元組數目。</p> <p>單位：位元組 (在 Amazon Redshift 主控台中為 GB/秒)</p> <p>尺寸: ClusterIdentifier , NodeID</p> <p>維度：ClusterIdentifier</p>
RedshiftManagedStorageTotalCapacity	<p>受管儲存總容量。</p> <p>單位：MB</p> <p>維度：ClusterIdentifier</p>
TotalTableCount	<p>在特定時間點開啟的使用者資料表數。這個總計不包括 Amazon Redshift Spectrum 資料表。</p> <p>單位：計數</p> <p>維度：ClusterIdentifier</p>
WLMQueueLength	<p>等候進入工作負載管理 (WLM) 佇列中的查詢數量。</p> <p>單位：計數</p> <p>尺寸: ClusterIdentifier , service class</p> <p>尺寸: ClusterIdentifier , QueueName</p>
WLMQueueWaitTime	<p>查詢在工作負載管理 (WLM) 佇列中等待的總時間。每隔 5 分鐘回報。</p> <p>單位：毫秒。</p> <p>尺寸: ClusterIdentifier , QueryPriority</p> <p>尺寸: ClusterIdentifier , wlmid</p> <p>尺寸: ClusterIdentifier , QueueName</p>

指標	描述
WLMQueriesCompletedPerSecond	<p>工作負載管理 (WLM) 佇列平均每秒完成的查詢次數。每隔 5 分鐘回報。單節點叢集不支援此指標。</p> <p>單位：計數/秒</p> <p>尺寸: ClusterIdentifier , wlmid</p> <p>尺寸: ClusterIdentifier , QueueName</p>
WLMQueryDuration	<p>工作負載管理 (WLM) 佇列完成查詢的平均時間長度。每隔 5 分鐘回報。單節點叢集不支援此指標。</p> <p>單位：微秒</p> <p>尺寸: ClusterIdentifier , wlmid</p> <p>尺寸: ClusterIdentifier , QueueName</p>
WLMRunningQueries	<p>每個 WLM 佇列從主要叢集和並行擴展叢集執行的查詢數。</p> <p>單位：計數</p> <p>尺寸: ClusterIdentifier , wlmid</p> <p>尺寸: ClusterIdentifier , QueueName</p>
WriteIOPS	<p>寫入操作的每秒平均次數。</p> <p>單位：計數/秒</p> <p>尺寸: ClusterIdentifier , NodeID</p> <p>維度：ClusterIdentifier</p>

指標	描述
WriteLatency	<p>用於磁碟寫入 I/O 操作的平均時間量。</p> <p>單位：秒</p> <p>尺寸: ClusterIdentifier , NodeID</p> <p>維度：ClusterIdentifier</p>
WriteThroughput	<p>平均每秒寫入磁碟的位元組數目。</p> <p>單位：位元組 (在 Amazon Redshift 主控台中為 GB/秒)</p> <p>尺寸: ClusterIdentifier , NodeID</p> <p>維度：ClusterIdentifier</p>
SchemaQuota	<p>所設定的結構描述配額。</p> <p>單位：MB</p> <p>維度：ClusterIdentifier 、 Database、 Schema</p> <p>定期/推送：Periodic</p> <p>頻率：5 minutes</p> <p>停止條件：已捨棄結構描述或已移除配額</p>
NumExceededSchemaQuotas	<p>超出配額的結構描述數目。</p> <p>單位：計數</p> <p>維度：ClusterIdentifier</p> <p>定期/推送：Periodic</p> <p>頻率：5 minutes</p> <p>停止條件：無</p>

指標	描述
StorageUsed	<p>結構描述使用的磁碟或儲存空間。</p> <p>單位：MB</p> <p>維度：ClusterIdentifier、Database、Schema</p> <p>定期/推送：Periodic</p> <p>頻率：5 minutes</p> <p>停止條件：已捨棄結構描述或已移除配額</p>
PercentageQuotaUsed	<p>已使用的磁碟或儲存空間相對於已設定的結構描述配額的百分比。</p> <p>單位：百分比</p> <p>維度：ClusterIdentifier、Database、Schema</p> <p>定期/推送：Periodic</p> <p>頻率：5 minutes</p> <p>停止條件：已捨棄結構描述或已移除配額</p>

指標	描述
UsageLimitAvailable	<p>根據 FeatureType，傳 UsageLimitAvailable 回下列內容：</p> <ul style="list-style-type: none"> • 如果 FeatureType 是CONCURRENCY_SCALING，則 UsageLimitAvailable 傳回以 1 分鐘為增量的並行縮放可使用的總時間量。 • 如果 FeatureType 是CROSS_REGION_DATASHARING，則 UsageLimitAvailable 傳回可以以 1 TB 為增量掃描的資料總量。 • 如果 FeatureType 是SPECTRUM，則 UsageLimitAvailable 傳回可以以 1 TB 為增量掃描的資料總量。 <p>單位：分鐘或 TB</p> <p>維度：ClusterIdentifier、FeatureType、UsageLimitId</p>
UsageLimitConsumed	<p>根據 FeatureType，傳 UsageLimitConsumed 回下列內容：</p> <ul style="list-style-type: none"> • 如果 FeatureType 是CONCURRENCY_SCALING，則 UsageLimitAvailable 傳回並行縮放所使用的總時間量 (以 1 分鐘為增量)。 • 如果 FeatureType 是CROSS_REGION_DATASHARING，則 UsageLimitAvailable 傳回以 1 TB 為增量掃描的資料總量。 • 如果 FeatureType 是SPECTRUM，則 UsageLimitAvailable 傳回以 1 TB 為增量掃描的資料總量。 <p>單位：分鐘或 TB</p> <p>維度：ClusterIdentifier、FeatureType、UsageLimitId</p>

Amazon Redshift 指標的維度

Amazon Redshift 資料可依下表中任何維度進行篩選。

維度	描述
latency	<p>可能的值如下：</p> <ul style="list-style-type: none"> • 短 — 少於 10 秒 • 中 — 介於 10 秒到 10 分鐘 • 長 — 超過 10 分鐘
NodeID	<p>篩選專屬於某個叢集的節點的資料。NodeID 可以是「Leader」、「Shared」或「Compute-N」，其中的 N 是 0, 1, ...，亦即叢集中的節點數量。「Shared」表示該叢集只有一個節點，例如領導節點與運算節點結合。</p> <p>領導者節點與運算節點回報的指標只有 CPUUtilization、NetworkTransmitThroughput 及 ReadIOPS。只有運算節點會回報使用 NodeId 維度的其他指標。</p>
ClusterIdentifier	<p>篩選專屬於某個叢集的資料。專屬於叢集的指標包括 HealthStatus、MaintenanceMode 及 DatabaseConnections。通常，此維度中的指標 (例如 ReadIOPS) 也是代表節點指標資料彙總的節點指標。在解譯這些指標時應特別注意，因為它們彙整了領導與運算節點的行為。</p>
service class	WLM 服務類別的識別碼。
stage	<p>查詢的執行階段。可能的值如下：</p> <ul style="list-style-type: none"> • QueryPlanning：剖析和最佳化 SQL 敘述句所花費的時間。 • QueryWaiting：在 WLM 佇列中等待所花費的時間。 • QueryExecutingRead：執行讀取查詢所花費的時間。 • QueryExecutingInsert：執行插入查詢所花費的時間。 • QueryExecutingDelete：執行刪除查詢所花費的時間。 • QueryExecutingUpdate：執行更新查詢所花費的時間。 • QueryExecutingCtas：執行建立資料表做為查詢所花費的時間。 • QueryExecutingUnload：執行卸載查詢所花費的時間。

維度	描述
	<ul style="list-style-type: none"> QueryExecutingCopy：執行複製查詢所花費的時間。 QueryCommit：承諾所花費的時間。
wlmid	工作負載管理佇列的識別碼。
QueryPriority	查詢的優先順序。可能值為 CRITICAL、HIGHEST、HIGH、NORMAL、LOW 以及 LOWEST。
QueueName	工作負載管理佇列的名稱。
FeatureType	受限於使用限制值的功能。可能值為 CONCURRENCY_SCALING、CROSS_REGION_DATASHARING 及 SPECTRUM。
UsageLimitId	用於限制用量的識別符。

Amazon Redshift 查詢和載入效能資料

除了 CloudWatch 指標之外，Amazon Redshift 還提供查詢和載入效能資料。查詢和載入效能資料可用來協助您了解資料庫效能和叢集指標間的關係。例如，如果您注意到叢集的 CPU 用量高升，您可以在叢集 CPU 圖形上找到峰值並查看在當時執行中的查詢。或者，您可以檢閱特定的查詢，指標資料 (例如 CPU) 會顯示在內容中，讓您可以了解查詢對叢集指標的影響。

查詢和載入效能資料不會以 CloudWatch 指標形式發佈，只能在 Amazon Redshift 主控台中檢視。查詢和載入效能資料會透過查詢資料庫的系統資料表來產生 (如需詳細資訊，請參閱《Amazon Redshift 開發人員指南》中的[系統資料表參考](#))。您也可以產生自己的自定資料庫效能查詢，但我們建議開始從在主控台中呈現的查詢和載入效能資料開始。如需自行測量和監控資料庫效能的相關資訊，請參閱《Amazon Redshift 開發人員指南》中的[管理效能](#)。

以下資料表說明您可以在 Amazon Redshift 主控台中存取之查詢和載入資料的不同層面。

查詢/載入資料	描述
查詢摘要	在特定期間的查詢清單。可以根據查詢 ID、查詢執行時間和狀態等值排序清單。請在叢集詳細資訊頁面的 Query monitoring (查詢監控) 標籤中檢視此資料。
查詢詳細資訊	提供包含以下項目之特定查詢的詳細資訊：

查詢/載入資料	描述
	<ul style="list-style-type: none"> 查詢 ID、類型、執行查詢的叢集和執行時間等查詢屬性。 查詢狀態和錯誤數之類的詳細資訊。 執行的 SQL 陳述式。 解釋計畫 (如果有)。 查詢執行期間的叢集效能資料 (如需詳細資訊，請參閱 檢視查詢歷史記錄資料)。
載入摘要	列出在特定期間的所有載入。可以根據查詢 ID、查詢執行時間和狀態等值排序清單。請在叢集詳細資訊頁面的 Query monitoring (查詢監控) 標籤中檢視此資料。
載入詳細資訊	<p>提供包含以下項目之特定載入操作的詳細資訊：</p> <ul style="list-style-type: none"> 查詢 ID、類型、執行查詢的叢集和執行時間等載入屬性。 載入狀態和錯誤數之類的詳細資訊。 執行的 SQL 陳述式。 載入檔案清單。 載入操作期間的叢集效能資料 (如需詳細資訊，請參閱 檢視查詢歷史記錄資料)。

在 Amazon Redshift 主控台中使用效能資料

本節說明如何在 Amazon Redshift 主控台中檢視效能資料，包括叢集和查詢效能的資訊。此外，您可以透過 Amazon Redshift 主控台來直接建立對叢集指標的警示。

當您在 Amazon Redshift 主控台中檢視效能資料時，您可以依叢集來進行檢視。叢集的效能資料圖形旨在讓您存取可回答您最常見效能問題的資料。有關某些效能資料 (請參閱 [使 CloudWatch 用指標監控 Amazon Redshift](#))，您也可以使用 CloudWatch 進一步自訂量度圖表。例如，您可以選擇更長的時間，或是合併叢集的指標。如需使用 CloudWatch 主控台的詳細資訊，請參閱 [在 CloudWatch 主控台中使用效能指標](#)。

觀看以下影片，了解如何使用 Amazon Redshift 主控台上的查詢監控功能來監控、隔離和優化您的查詢：[Amazon Redshift 中的查詢監控](#)。

主題

- [檢視叢集效能資料](#)
- [檢視查詢歷史記錄資料](#)
- [檢視資料庫效能資料](#)
- [檢視工作負載並行和並行擴展資料](#)
- [檢視查詢和載入](#)
- [檢視載入操作期間的叢集指標](#)
- [分析工作負載效能](#)
- [管理警示](#)
- [在 CloudWatch 主控台中使用效能指標](#)

檢視叢集效能資料

使用 Amazon Redshift 中的叢集指標，您可執行以下常見的效能任務：

- 判斷叢集指標在特定時間範圍內是否不正常，以及若是不正常，則辨識影響效能的查詢。
- 確認歷史或目前查詢是否對叢集效能造成影響。如果您發現有問題的查詢，您可以檢視其相關詳細資訊，包含查詢執行期間的叢集效能。您可以使用此資訊來診斷查詢緩慢的原因以及可以執行的事項來改善其效能。

檢視效能資料

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽功能表上，選擇叢集，然後從清單中選擇叢集名稱以開啟其詳細資訊。隨即顯示叢集的詳細資訊，包含叢集效能、查詢監控、資料庫、資料共用、排程、維護和屬性標籤。
3. 選擇 Cluster performance (叢集效能) 標籤，取得包括下列項目的效能資訊：
 - CPU 使用率
 - 使用的磁碟空間百分比
 - 資料庫連線
 - 運作狀態
 - 查詢期間
 - 查詢輸送量

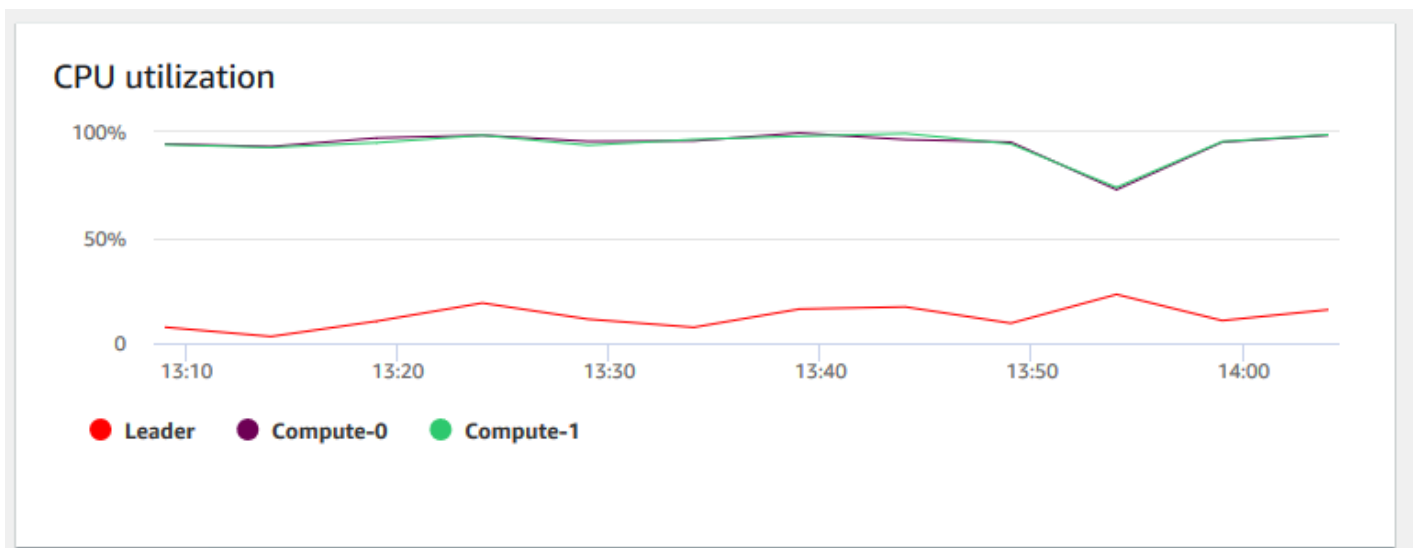
- Concurrency scaling activity (並行擴展活動)

另有更多指標可用。若要查看可用的指標並選擇要顯示的指標，請選擇 Preferences (偏好設定) 圖示。

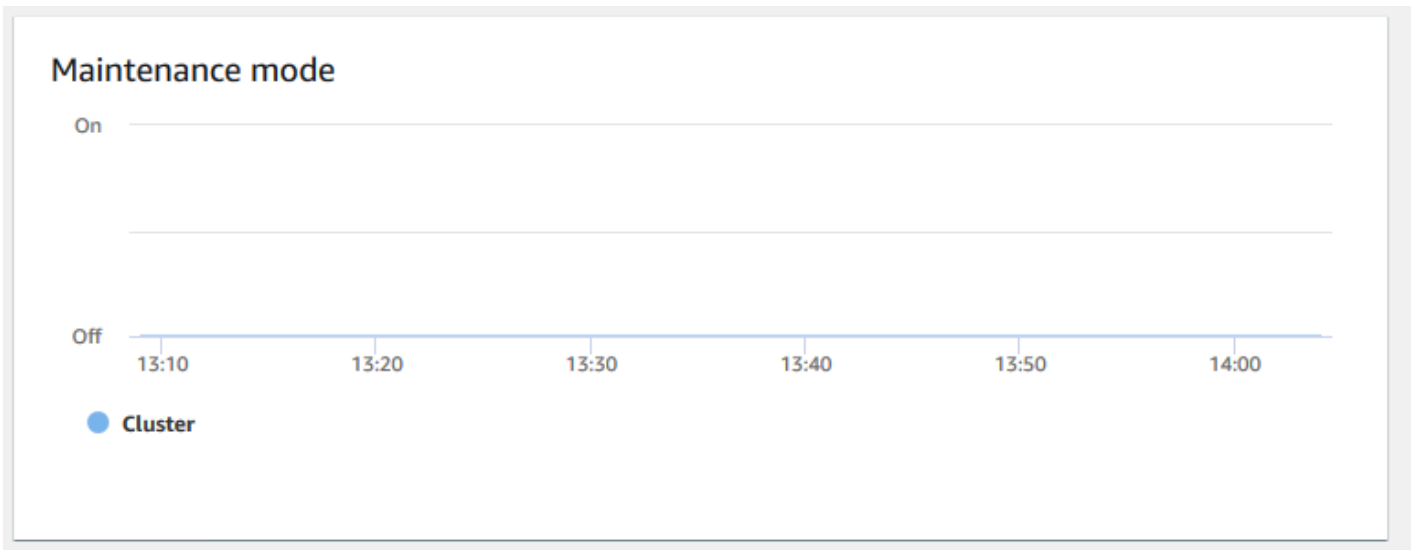
叢集效能圖表

下列範例顯示一些在全新 Amazon Redshift 主控台中顯示的圖表。

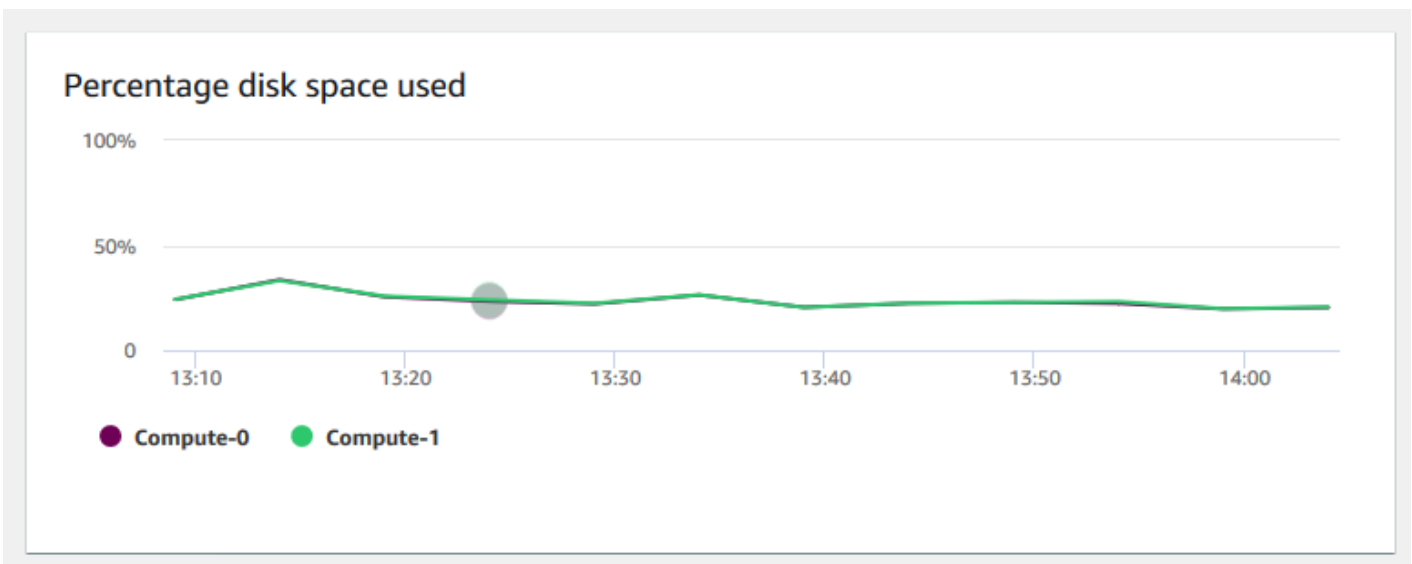
- CPU 使用率 — 顯示所有節點的 CPU 使用率百分比 (領導和運算)。如要在排程叢集遷移或其他資源使用操作前尋找叢集用量最低的時間，請監控此圖表來查看個別或所有節點的 CPU 使用率。



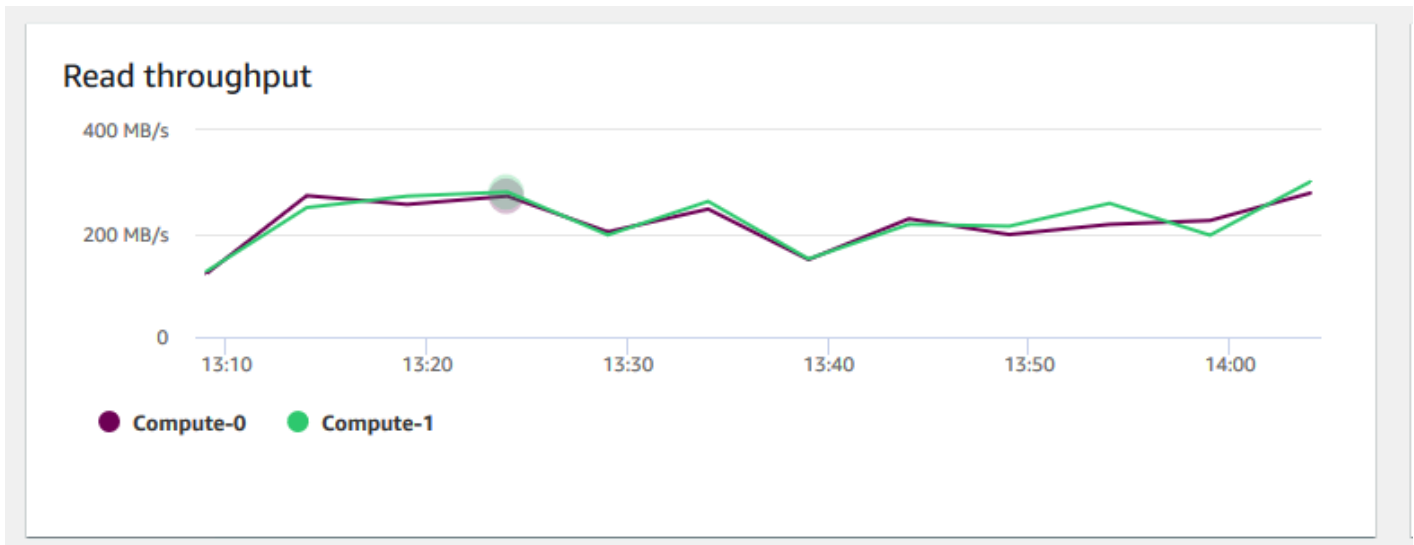
- 維護模式 — 使用 On 和 Off 指標，顯示叢集在指定時間是否處於維護模式。您可以查看叢集正在進行維護的時間。然後，您可以將此時間與叢集完成的操作產生關聯，以估計其未來在發生經常性事件時的停機時間。



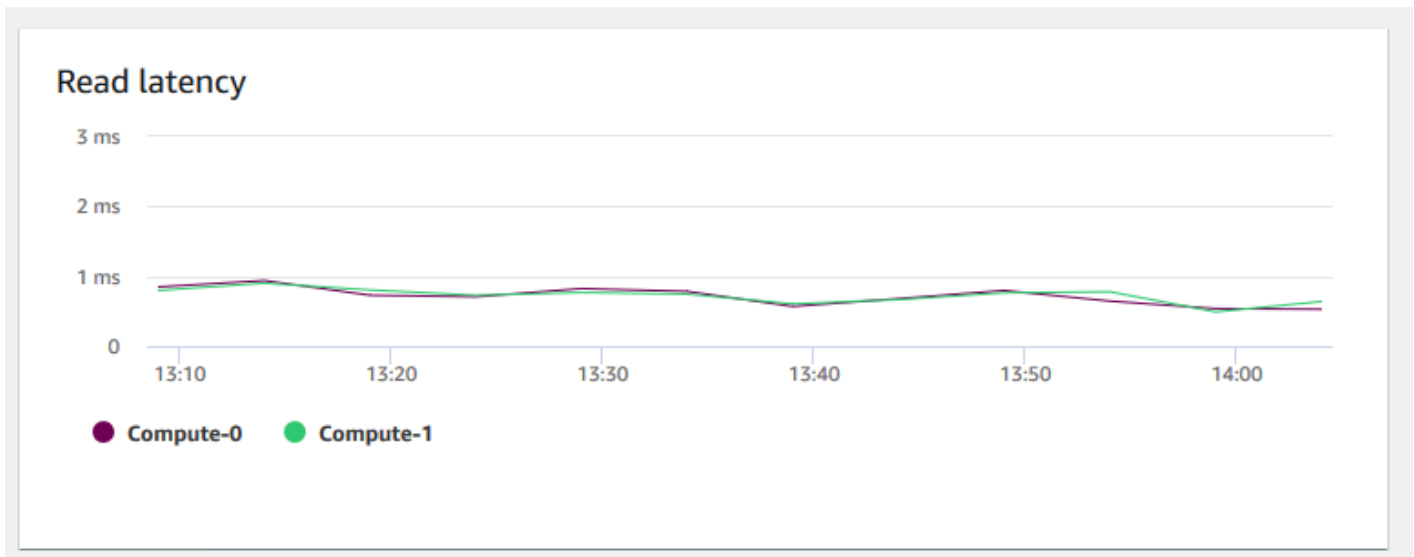
- 使用的磁碟空間百分比 — 顯示每個運算節點磁碟空間的用量百分比，而非叢集整體的用量。您可以探索此圖表來監控磁碟使用率。VACUUM 和 COPY 等維護操作會使用中繼暫時儲存空間來進行排序操作，因此預期會在磁碟用量中出現尖峰。



- 讀取輸送量 — 顯示每秒從磁碟讀取的平均 MB 數。您可以評估此圖表，監控叢集的對應實體方面。此輸送量不包含叢集中執行個體及其磁碟區之間的網路流量。



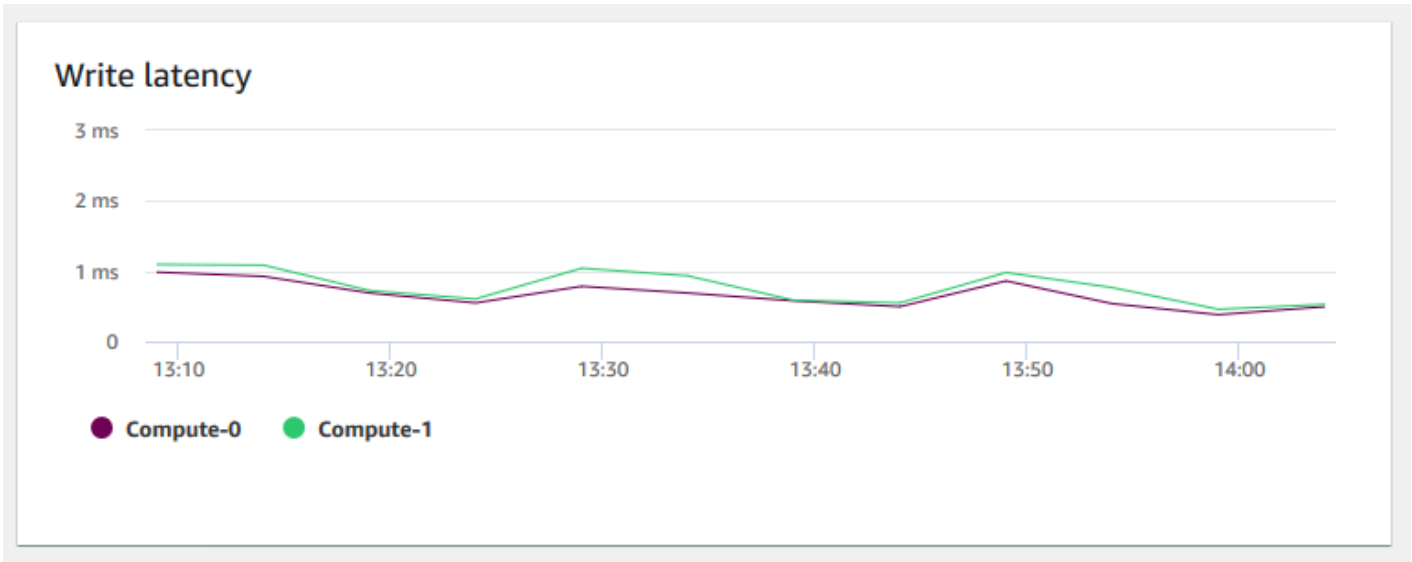
- **讀取延遲** — 顯示每毫秒磁碟讀取 I/O 操作所花費的平均時間長度。您可以檢視要傳回資料的回應時間。當延遲相當高時，這表示寄件者花費較多時間閒置 (而非傳送任何新的封包)，降低輸送量成長的速度。



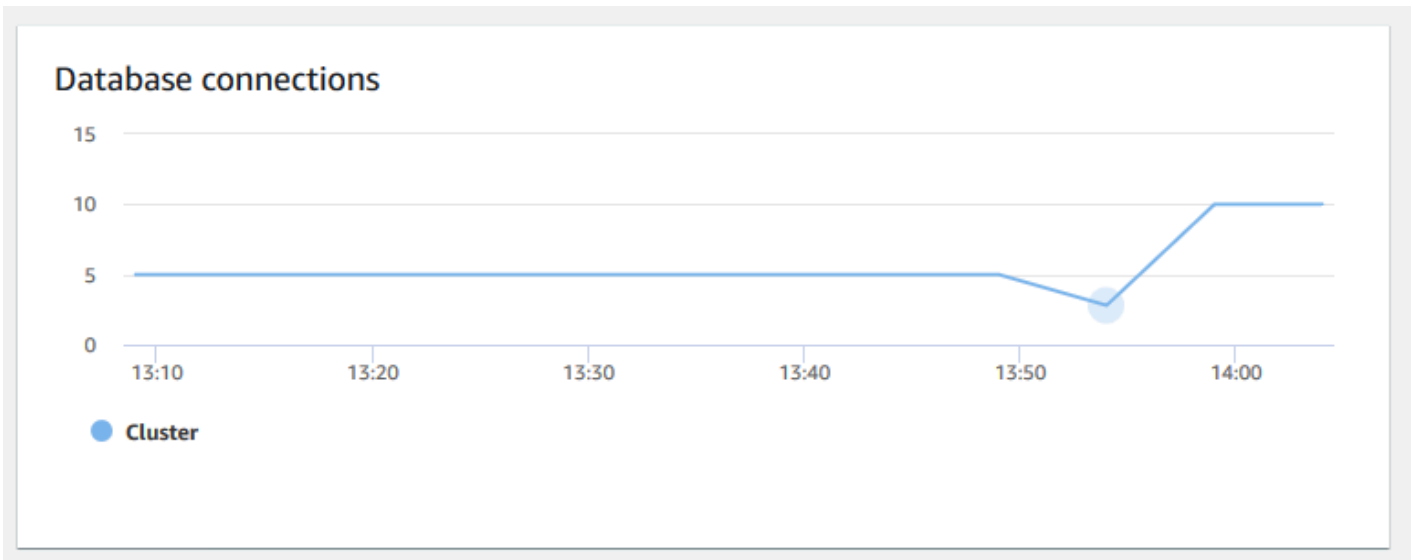
- **寫入輸送量** — 顯示每秒寫入磁碟的平均 MB 數。您可以評估此指標來監控叢集的對應實體方面。此輸送量不包含叢集中執行個體及其磁碟區之間的網路流量。



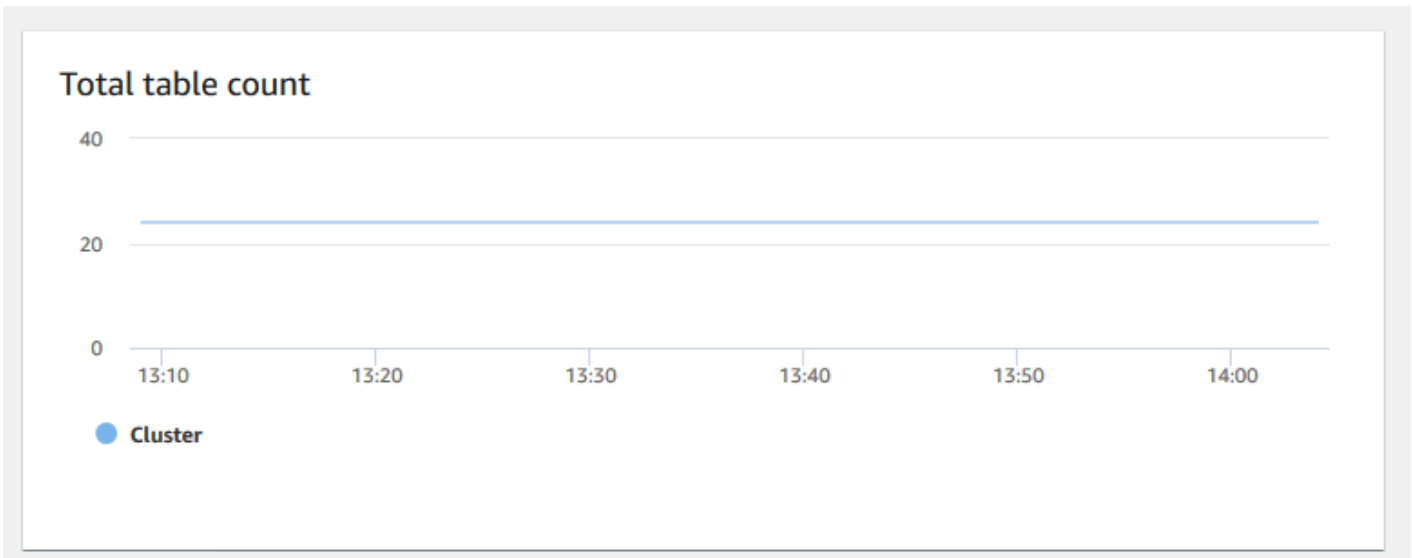
- **寫入延遲** — 顯示磁碟寫入 I/O 操作花費的平均時間長度 (毫秒)。您可以評估傳回寫入確認的時間。當延遲相當高時，這表示寄件者花費較多時間閒置 (而非傳送任何新的封包)，降低輸送量成長的速度。



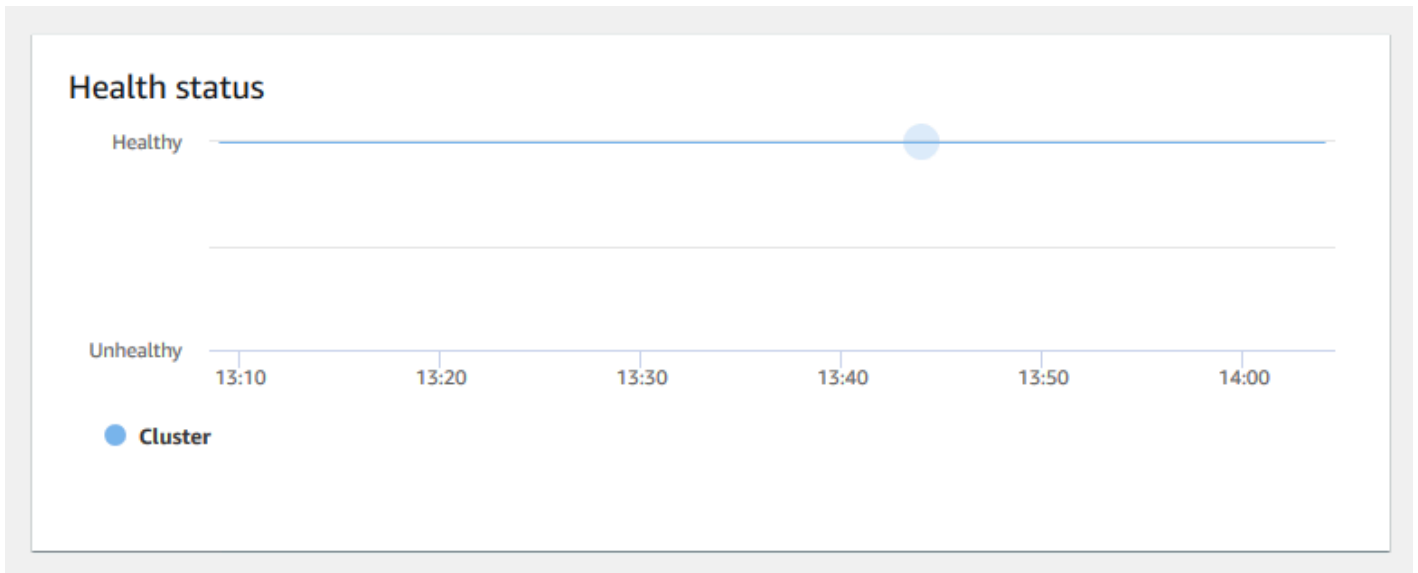
- **資料庫連線** — 顯示叢集的資料庫連線數。您可以使用此圖表來查看與資料庫建立的連線數，並尋找叢集用量最低的時間。



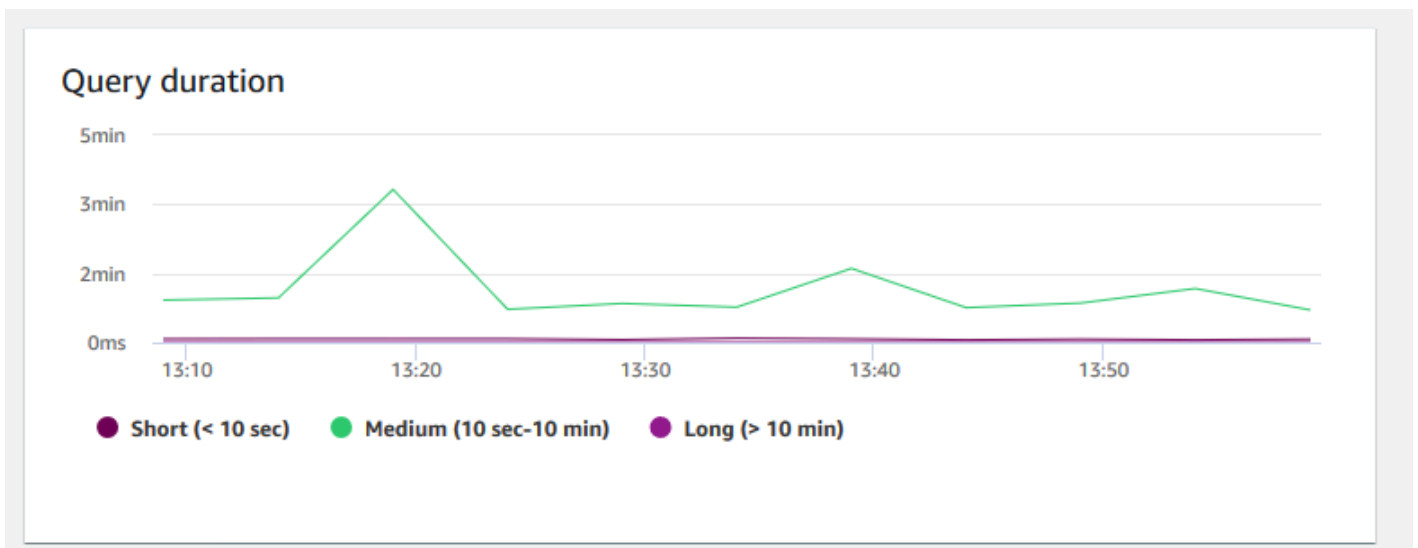
- **總資料表計數** — 顯示叢集內於特定時間點開啟的使用者資料表數。您可以監控開啟資料表計數較高時的叢集效能。



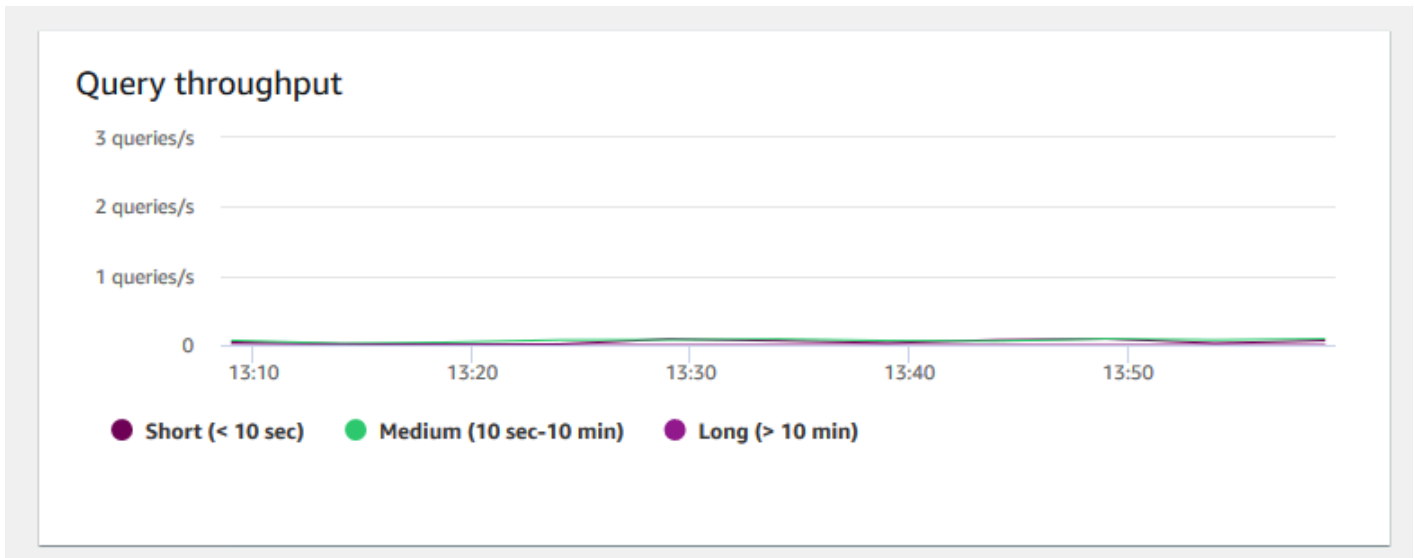
- **運作狀態** — 指出叢集的運作狀態為 **Healthy** 或 **Unhealthy**。如果叢集可以連線到其資料庫及成功執行簡易查詢，便會將叢集視為運作狀態良好。否則，表示該叢集運作不良。不良狀態可能會發生於資料庫處於極高負載，或叢集上的資料庫有組態的問題。



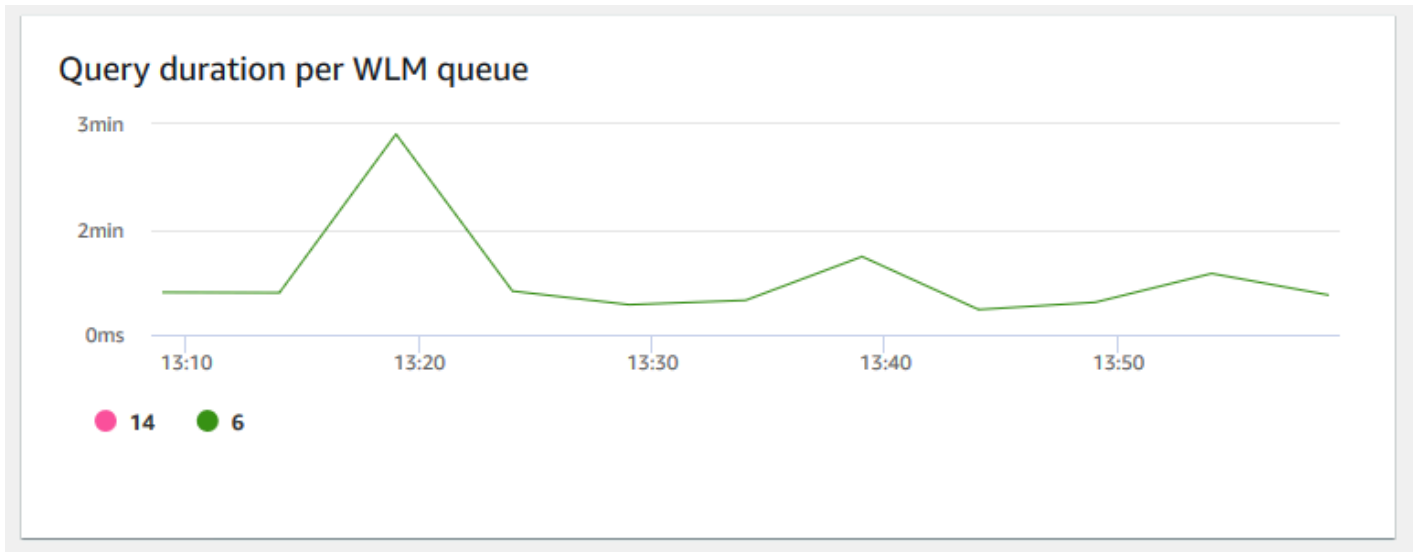
- **查詢持續時間** — 顯示完成查詢的平均時間長度 (微秒)。您可以針對此圖表上的資料進行基準測試，測量叢集內的 I/O 效能，並視需要調校最耗費時間的查詢。



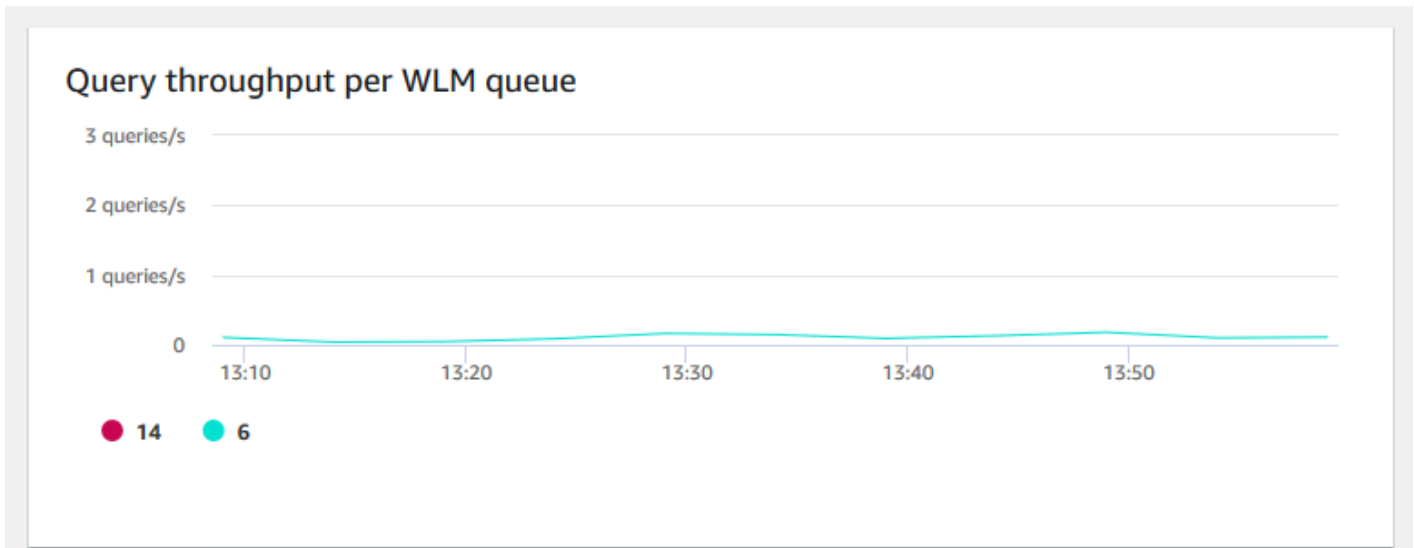
- **查詢輸送量** — 顯示每秒完成的平均查詢數。您可以分析此圖表上的資料，測量資料庫效能，並說明系統以平衡方式支援多使用者的能力。



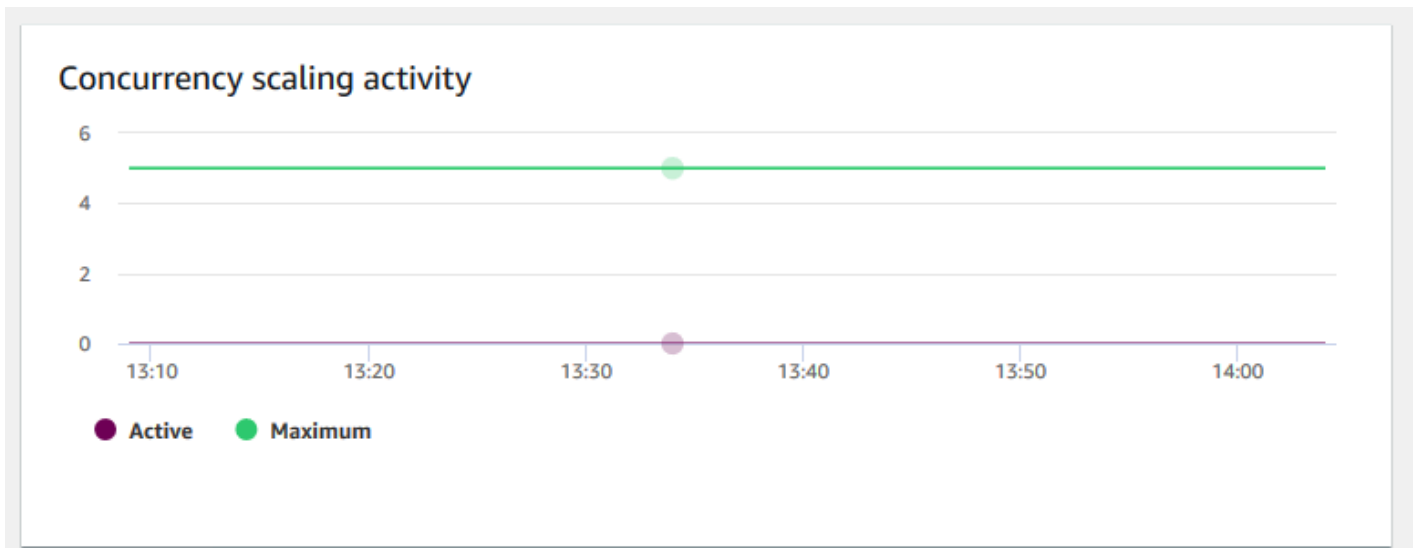
- 每個 WLM 佇列的查詢持續時間 — 顯示完成查詢的平均時間長度 (微秒)。您可以針對此圖表上的資料進行基準測試，測量每個 WLM 佇列的 I/O 效能，並視需要調校最耗費時間的查詢。



- 每個 WLM 佇列的查詢輸送量 — 顯示每秒完成的平均查詢數。您可以分析此圖表上的資料，測量每個 WLM 佇列的資料庫效能。



- 並行擴展活動 — 顯示作用中並行擴展叢集的數量。當並行擴展啟用時，當您需要更多叢集容量以執行增加的並行讀取查詢時，Amazon Redshift 將會自動新增額外的叢集容量。



檢視查詢歷史記錄資料

您可以在 Amazon Redshift 中使用查詢歷史記錄指標來執行以下作業：

- 隔離和診斷查詢效能問題。
- 比較相同時間軸上的查詢執行時間指標和叢集效能指標，查看兩個指標可能的相關情況。您可以透過這麼做來找出執行狀況不佳的查詢、尋找瓶頸查詢並判斷您是否需要重新調整工作負載的叢集大小。

- 在時間軸上選擇，以向下切入特定查詢的詳細資訊。當 Query ID (查詢 ID) 和其他屬性顯示在圖表下方的資料列時，您可以選擇查詢來查看查詢詳細資訊。詳細資訊包括查詢的 SQL 陳述式、執行詳細資訊和查詢計畫。如需詳細資訊，請參閱 [檢視查詢詳細資訊](#)。
- 判斷您的載入任務是否成功完成，以及滿足您的服務水準協議 (SLA)。

顯示查詢歷史記錄資料

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽功能表上，選擇叢集，然後從清單中選擇叢集名稱以開啟其詳細資訊。隨即顯示叢集的詳細資訊，包含叢集效能、查詢監控、資料庫、資料共用、排程、維護和屬性標籤。
3. 選擇與查詢有關的指標 Query monitoring (查詢監控) 標籤。
4. 在 Query monitoring (查詢監控) 區段中，選擇 Query history (查詢歷史記錄) 標籤。

使用視窗上的控制項，您可以在 Query list (查詢清單) 和 Cluster metrics (叢集指標) 之間進行切換。

當您選擇 Query list (查詢清單) 時，標籤會包含下列圖表：

- 查詢執行時間 — 時間軸上的查詢活動。使用此圖表以查看在相同時間範圍內執行的查詢。選擇查詢以檢視更多查詢執行詳細資訊。x 軸會顯示選取的期間。您可以透過正在執行、已完成、載入等篩選圖表化查詢。每個長條都代表一個查詢，且長條的長度代表其從長條開始到結束的執行時間。查詢可以包含 SQL 資料處理陳述式 (例如 SELECT、INSERT、DELETE) 和載入 (例如 COPY)。根據預設，會顯示所選取時間期間中前 100 個執行時間最長的查詢。
- 查詢和載入 — 在該叢集上執行的查詢和載入清單。如果查詢目前正在執行中，視窗便會包含 Terminate query (終止查詢) 選項。

當您選擇 Cluster metrics (叢集指標) 時，標籤會包含下列圖表：

- 查詢執行時間 — 時間軸上的查詢活動。使用此圖表以查看在相同時間範圍內執行的查詢。選擇查詢以檢視更多查詢執行詳細資訊。
- CPU 使用率 — 領導節點和運算節點平均的叢集 CPU 使用率。
- 已使用的儲存體容量 — 已使用的儲存體容量百分比。
- 作用中資料庫連線 — 叢集上作用中的資料庫連線數。

請在使用查詢歷史記錄圖表時，請考慮下列事項：

- 在 Query runtime (查詢執行時間) 圖表上選擇代表特定查詢的橫條，以查看該查詢的詳細資訊。您也可以從 Queries and loads (查詢和載入) 清單上選擇查詢 ID 來查看其詳細資訊。
- 您可以滑動以選取 Query runtime (查詢執行時間) 圖表的區段，以放大顯示特定時間期間。
- 在 Query runtime (查詢執行時間) 圖表上，如要查看您所選擇篩選條件考慮的所有資料，請向前翻到所有列在 Queries and loads (查詢和載入) 清單上的頁面。
- 您可以使用顯示在 settings gear icon (設定齒輪圖示) 旁邊的偏好設定視窗，變更在 Queries and loads (查詢和載入) 清單上顯示的資料列數和欄位。
- 您也可以從左側導覽器的查詢圖示、查詢和載入進行瀏覽，以顯示查詢和載入清單。如需詳細資訊，請參閱 [檢視查詢和載入](#)。

查詢歷史記錄圖表

下列範例顯示在全新 Amazon Redshift 主控台中顯示的圖表。

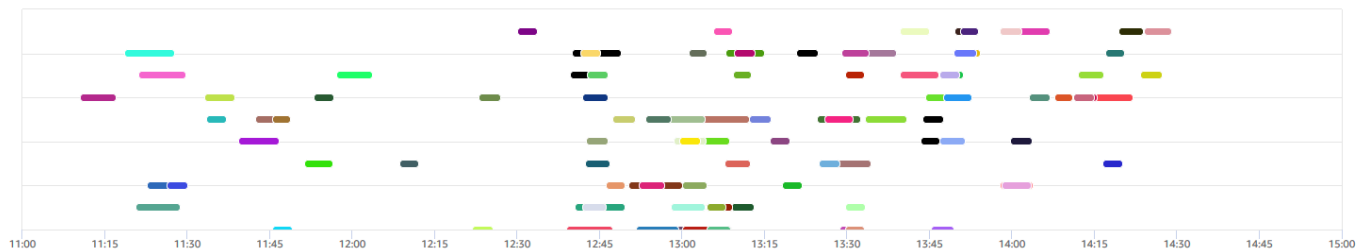
Note

Amazon Redshift 主控台圖表只包含最近 100,000 筆查詢的資料。

Query runtime (查詢執行時間)

Query runtime

The query activity on a timeline. Use this graph to see which queries are running in the same timeframe. Choose a query to view more query execution details.



Queries and loads (查詢和載入)

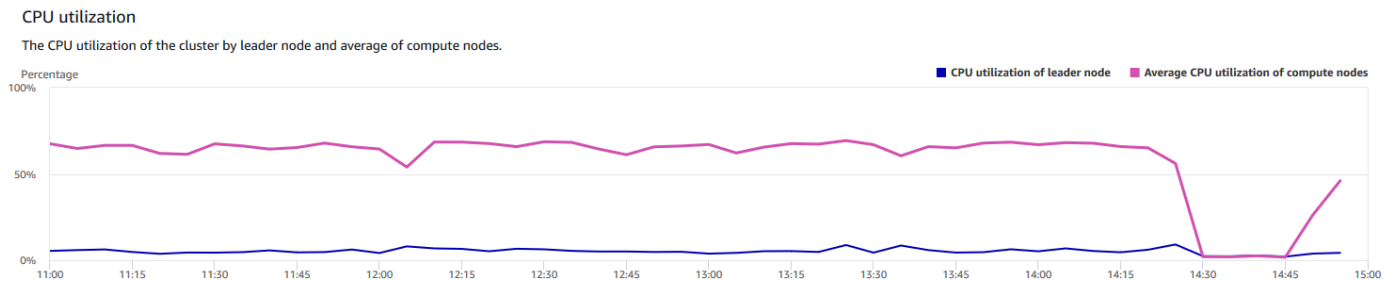
Queries and loads(100)

Filter queries

Terminate query

Start time	Query	Status	Duration	SQL	Copy SQL	User	Transaction ID
Apr 13th, 2020 01:00:55 PM 8 days ago	69248	Completed	11 min	with /* query_templates/query67.tpLO ICF:IR-09c6a4cc-6ec8-11e a-8047-06872b3fecc8.stream_10cu_run01_nocache.stream-quer ...	Copy	rsperf	105501
Apr 13th, 2020 12:58:07 PM 8 days ago	69199	Completed	11 min	with /* query_templates/query67.tpLO ICF:IR-09c6a4cc-6ec8-11e a-8047-06872b3fecc8.stream_10cu_run01_nocache.stream-quer ...	Copy	rsperf	105414
Apr 13th, 2020 12:54:15 PM 8 days ago	69111,69265,69253	Completed	10 min	with /* query_templates/query22.tpLO ICF:IR-09c6a4cc-6ec8-11e a-8047-06872b3fecc8.stream_10cu_run01_nocache.stream-quer ...	Copy	rsperf	105283
Apr 13th, 2020 12:50:17 PM 8 days ago	68976	Completed	10 min	with /* query_templates/query67.tpLO ICF:IR-09c6a4cc-6ec8-11e a-8047-06872b3fecc8.stream_10cu_run01_nocache.stream-quer ...	Copy	rsperf	105128
Apr 13th, 2020 01:29:23 PM 8 days ago	70089	Completed	10 min	with /* query_templates/query67.tpLO ICF:IR-09c6a4cc-6ec8-11e a-8047-06872b3fecc8.stream_10cu_run01_nocache.stream-quer ...	Copy	rsperf	106659
Apr 13th, 2020 11:18:35 AM 8 days ago	65543	Completed	9 min	with /* query_templates/query67.tpLO ICF:IR-09c6a4cc-6ec8-11e a-8047-06872b3fecc8.stream_05cu_run01_nocache.stream-quer ...	Copy	rsperf	101092
Apr 13th, 2020 12:40:30 PM 8 days ago	68729	Completed	9 min	with /* query_templates/query67.tpLO ICF:IR-09c6a4cc-6ec8-11e a-8047-06872b3fecc8.stream_10cu_run01_nocache.stream-quer ...	Copy	rsperf	104789

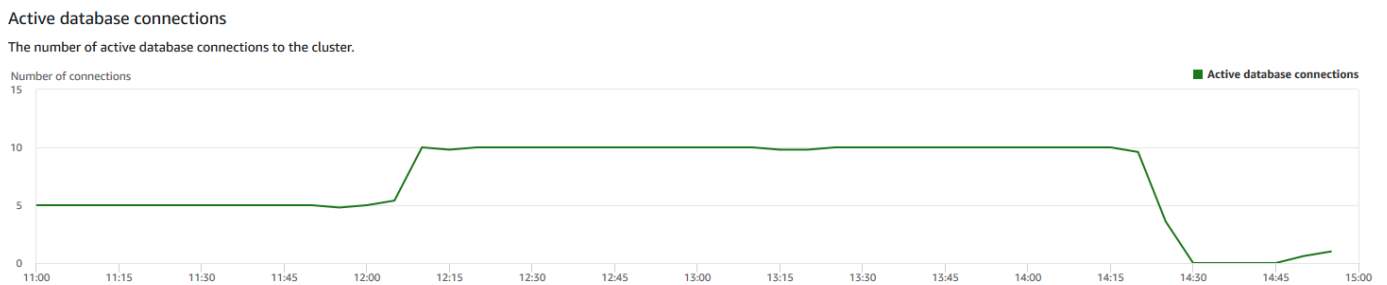
• CPU 使用率



• Storage capacity used (已使用的儲存體容量)



• Active database connections (作用中的資料庫連線)



檢視資料庫效能資料

您可以使用 Amazon Redshift 中的資料庫效能指標來執行以下作業：

- 透過處理階段來分析查詢所花費的時間。您可以尋找在某階段所花費時間中不尋常的趨勢。
- 根據持續時間範圍 (短、中、長) 來分析查詢數、持續時間和查詢的輸送量。
- 根據查詢優先順序 (最低、低、一般、高、最高、關鍵) 尋找查詢等待時間中的趨勢。
- 尋找查詢持續時間、輸送量，或是 WLM 佇列等待時間中的趨勢。

顯示資料庫效能資料

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽功能表上，選擇叢集，然後從清單中選擇叢集名稱以開啟其詳細資訊。隨即顯示叢集的詳細資訊，包含叢集效能、查詢監控、資料庫、資料共用、排程、維護和屬性標籤。
3. 選擇與查詢有關的指標 Query monitoring (查詢監控) 標籤。
4. 在 Query monitoring (查詢監控) 區段中，選擇 Database performance (資料庫效能) 標籤。

使用視窗上的控制項，您可以在 Cluster metrics (叢集指標) 和 WLM queue metrics (WLM 佇列指標) 之間進行切換。

當您選擇 Cluster metrics (叢集指標) 時，標籤會包含下列圖表：

- 工作負載執行明細項目 — 在查詢處理階段所耗費的時間。
- 查詢 (依持續時間範圍) — 短、中、長時間的查詢數。
- 查詢輸送量 — 每秒完成的平均查詢數。
- 查詢持續時間 — 完成查詢的平均時間長度。
- 平均佇列等待時間 (依優先順序) — 查詢在 WLM 佇列中所耗費的總時間 (依查詢優先順序)。

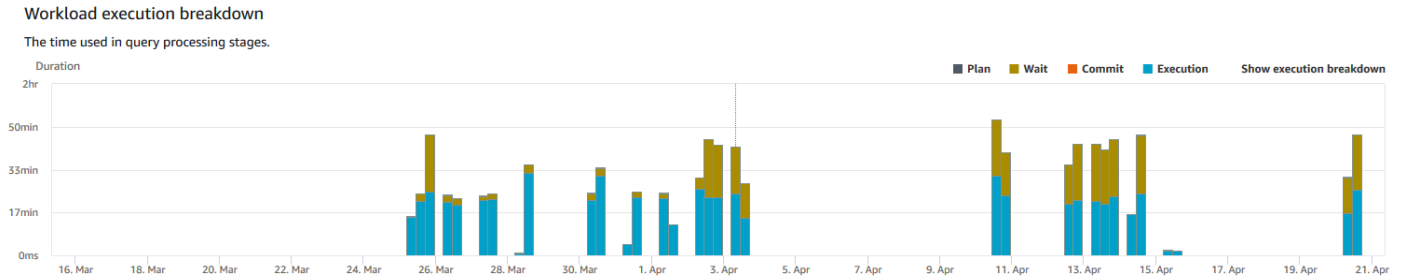
當您選擇 WLM queue metrics (WLM 佇列指標) 時，標籤會包含下列圖表：

- 查詢持續時間 (依佇列) — WLM 佇列的平均查詢持續時間。
- 查詢輸送量 (依佇列) — WLM 佇列每秒完成的平均查詢數。
- 查詢等待時間 (依佇列) — 查詢在 WLM 佇列耗費的平均持續時間。

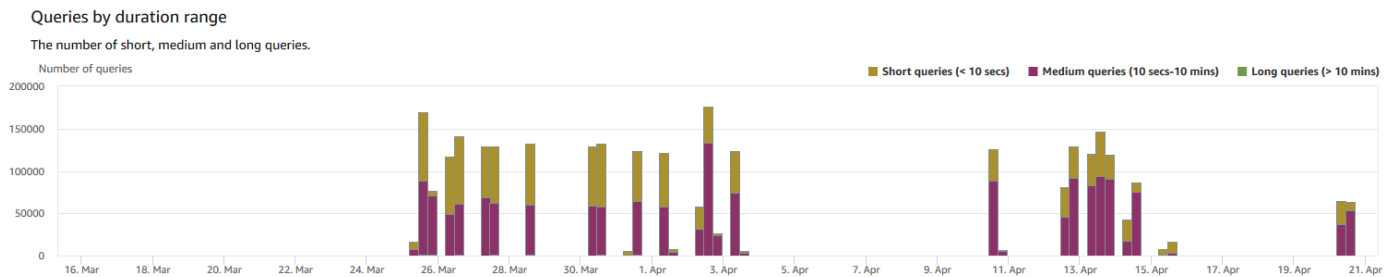
資料庫效能圖表

下列範例顯示在全新 Amazon Redshift 主控台中顯示的圖表。

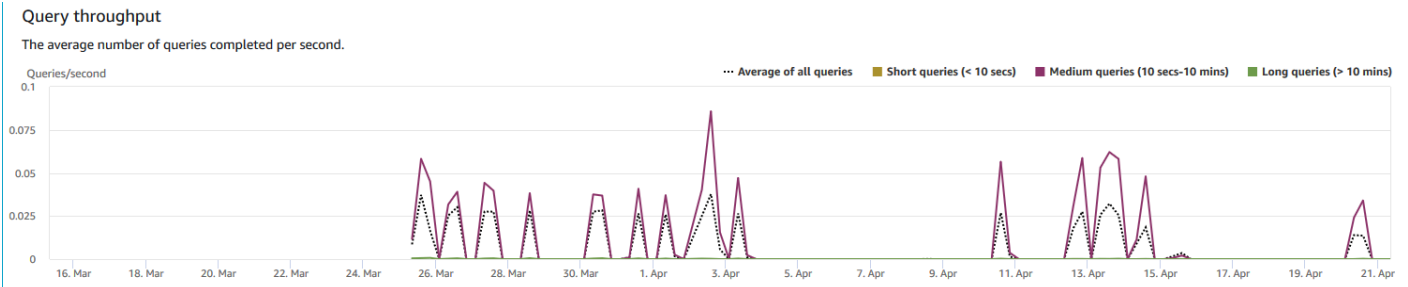
- Workload execution breakdown (工作負載執行明細項目)



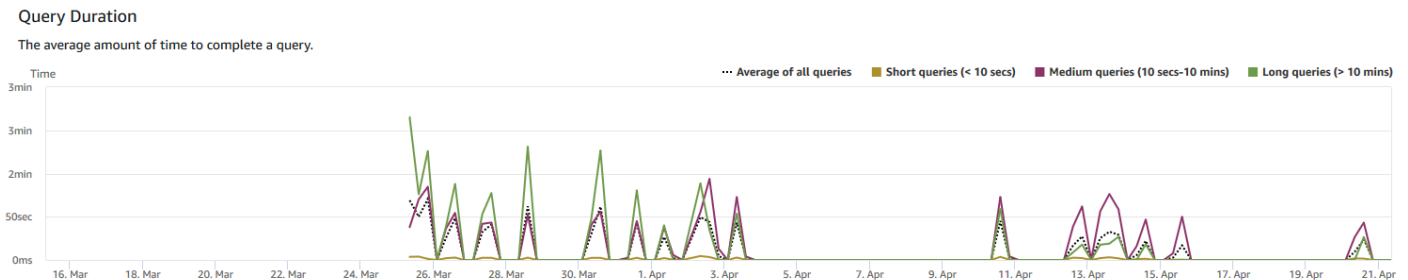
- Queries by duration range (查詢 (依持續時間範圍))



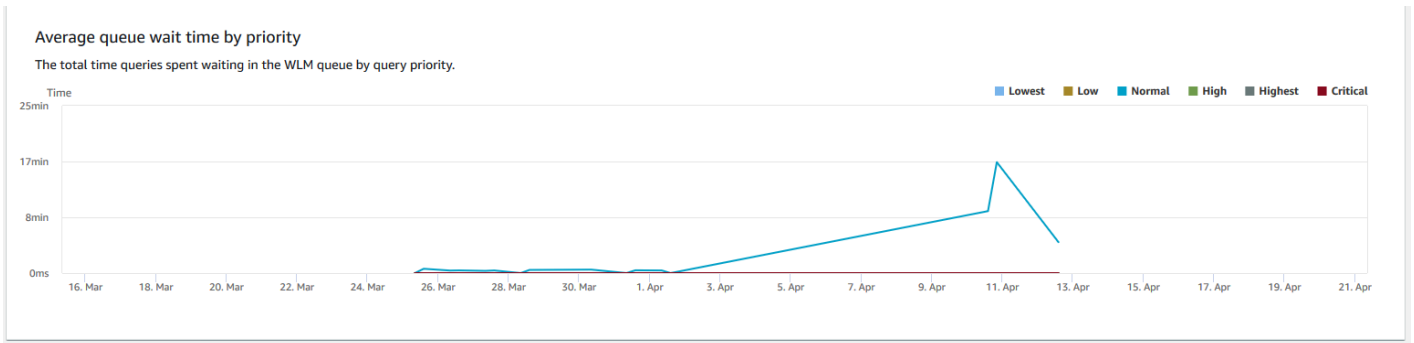
- 查詢輸送量



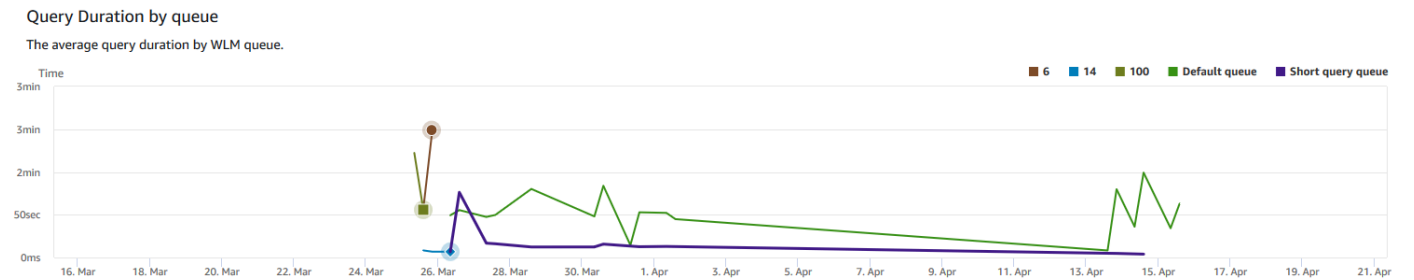
- 查詢期間



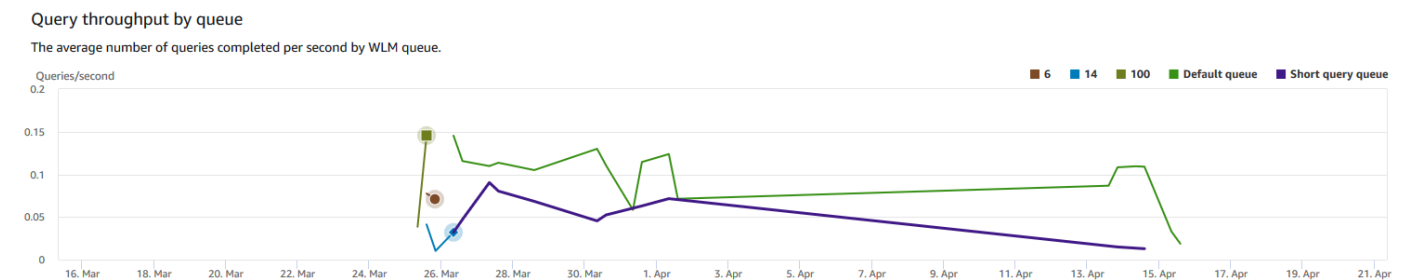
- Average queue wait time by priority (平均佇列等待時間 (依優先順序))



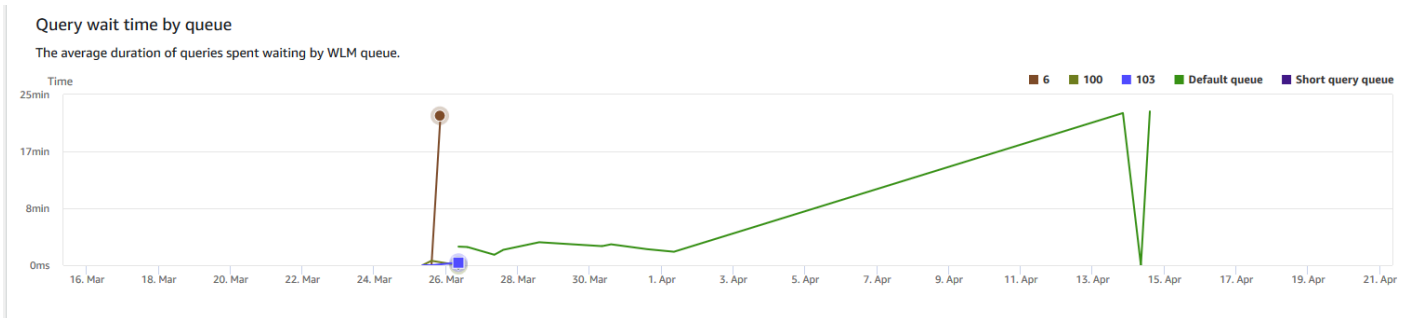
• Query duration by queue (查詢持續時間 (依佇列))



• Query throughput by queue (查詢輸送量 (依佇列))



• Query wait time by queue (查詢等待時間 (依佇列))



檢視工作負載並行和並行擴展資料

透過在 Amazon Redshift 中使用並行擴展指標，您可以執行以下操作：

- 分析您是否可以透過啟用並行擴展來降低排入佇列的查詢數。您可以依 WLM 佇列進行比較，或是針對所有 WLM 佇列進行比較。
- 檢視並行擴展叢集中的並行擴展活動。如此可讓您了解並行擴展是否受限於 `max_concurrency_scaling_clusters`。如果是，您可以選擇提高 DB 參數中的 `max_concurrency_scaling_clusters`。
- 檢視所有並行擴展叢集合計的並行擴展總用量。

顯示並行擴展資料

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽功能表上，選擇叢集，然後從清單中選擇叢集名稱以開啟其詳細資訊。隨即顯示叢集的詳細資訊，包含叢集效能、查詢監控、資料庫、資料共用、排程、維護和屬性標籤。
3. 選擇與查詢有關的指標 Query monitoring (查詢監控) 標籤。
4. 在 Query monitoring (查詢監控) 區段中，選擇 Workload concurrency (工作負載並行) 標籤。

標籤包括下列圖表：

- 排入佇列的查詢和正在叢集上執行的查詢 — 正在執行查詢數 (來自主要叢集和並行擴展叢集) 和叢集中所有 WLM 佇列內正在等待查詢數的比較。
- 每個佇列上排入佇列和正在執行的查詢 — 正在執行查詢數 (來自主要叢集和並行擴展叢集) 和正在每個 WLM 佇列中等待查詢數的比較。
- 並行擴展活動 — 正在處理查詢的並行擴展叢集數。
- 並行擴展用量 — 具備作用中查詢處理活動的並行擴展叢集用量。

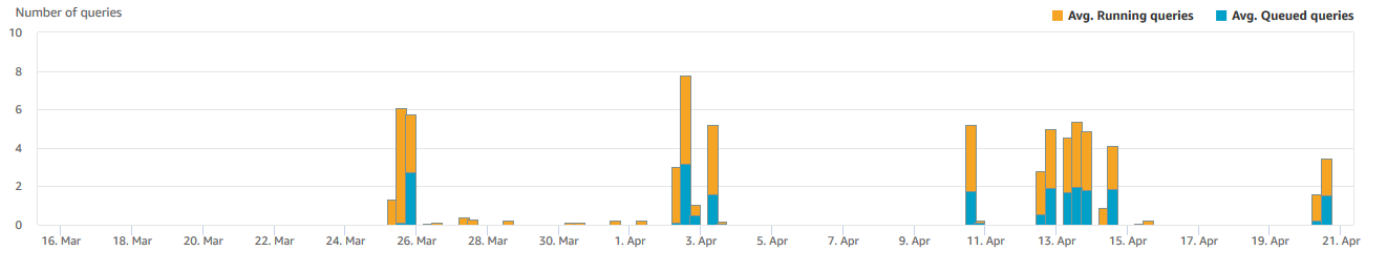
工作負載並行圖表

下列範例顯示在全新 Amazon Redshift 主控台中顯示的圖表。要在 Amazon 中創建類似的圖形 CloudWatch，您可以使用並發擴展和 WLM CloudWatch 指標。如需有關 Amazon Redshift CloudWatch 指標的詳細資訊，請參閱 [使 CloudWatch 用指標監控 Amazon Redshift](#)。

- 排入佇列的查詢和正在叢集上執行的查詢

Queued vs. Running queries on the cluster

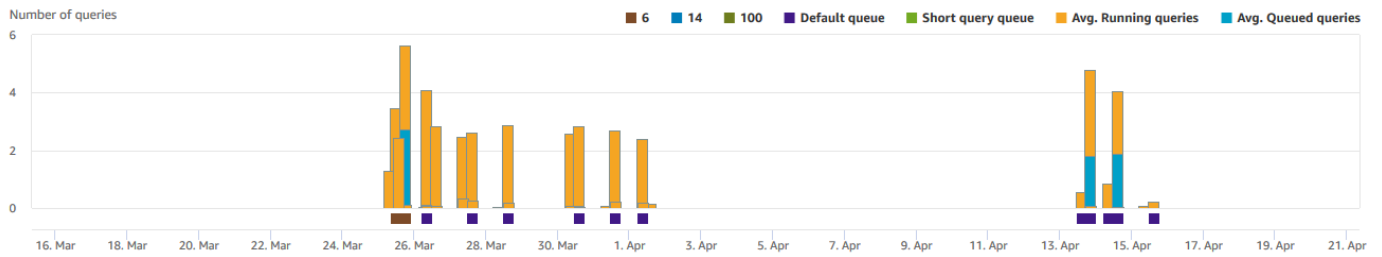
The number of queries running (from the main cluster and concurrency scaling cluster) compared to the number of queries waiting in all WLM queues in the cluster.



- 每個佇列上排入佇列和正在執行的查詢

Queued vs. Running queries per queue

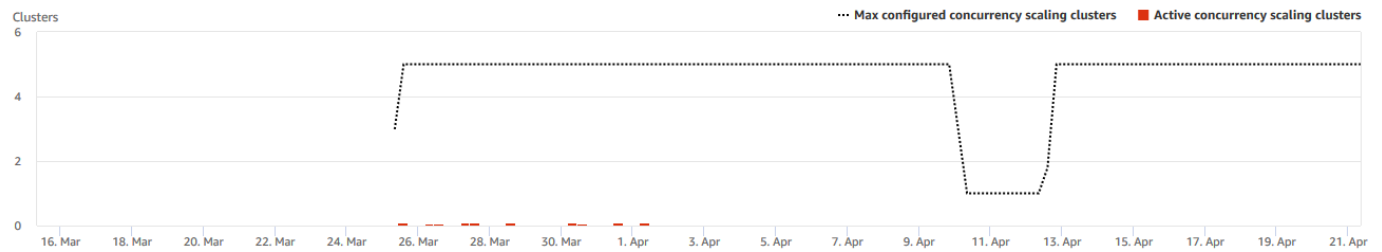
The number of queries running (from the main cluster and concurrency scaling cluster) compared to the number of queries waiting in each WLM queue.



- Concurrency scaling activity (並行擴展活動)

Concurrency scaling activity

The number of concurrency scaling clusters that are actively processing queries.

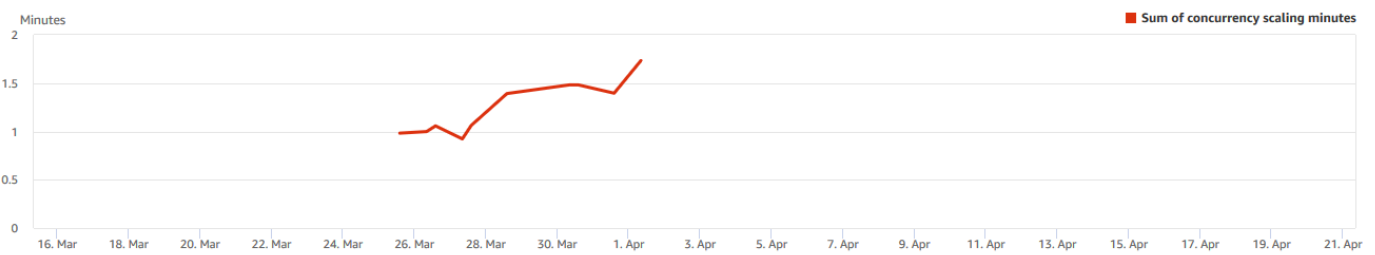


- 並行擴展模式

Concurrency scaling usage

The usage of concurrency scaling clusters that have active query processing activity.

Total usage: 12.51 mins ⓘ



檢視查詢和載入

Amazon Redshift 主控台提供在資料庫中執行的查詢和載入資訊。您可以使用此資訊，來找出花長時間處理和對其他查詢造成瓶頸而無法有效處理的查詢並對其進行疑難排解。您可在 Amazon Redshift 主控台中使用查詢資訊監控查詢處理過程。

顯示查詢效能資料

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽功能表上，選擇查詢和載入以顯示帳戶的查詢清單。

根據預設，此清單會顯示過去 24 小時您所有叢集的查詢。您可在主控台中變更顯示日期的範圍。

Important

Queries and loads (查詢和負載) 清單顯示系統中執行時間最長的查詢，最多 100 個查詢。

終止執行中的查詢

您也可以使用 Queries (查詢) 頁面終止目前正在進行的查詢。

Note

在 Amazon Redshift 主控台終止查詢和載入的功能需要特定的許可。如果您希望使用者能夠終止查詢和載入，請務必將 `redshift:CancelQuerySession` 動作新增至您的 AWS Identity and Access Management (IAM) 政策。無論您是選取 Amazon Redshift 唯讀 AWS 受管政策還是在 IAM 中建立自訂政策，都適用此要求。具有 Amazon Redshift 完整存取政策之使用者已擁有必要的許可，可終止查詢和載入。如需 Amazon Redshift 之 IAM 政策中動作的相關資訊，請參閱 [管理資源存取](#)。

終止執行中的查詢

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽功能表上，選擇查詢和載入以顯示帳戶的查詢清單。

3. 選擇清單中要終止的執行中查詢，然後選擇 Terminate query (終止查詢)。

檢視查詢詳細資訊

您可以在 Amazon Redshift 主控台上分析查詢詳細資訊。您可以使用查詢識別碼檢視查詢的詳細資訊。詳細資訊可以包括查詢的完成狀態、持續時間、SQL 陳述式，以及它是否為使用者查詢或由 Amazon Redshift 重寫的查詢。使用者查詢是從 SQL 用戶端提交至 Amazon Redshift 的查詢，或是由商業智慧工具產生的查詢。Amazon Redshift 可能會重寫查詢以進行最佳化，這可能會導致多個重寫的查詢。雖然程序是由 Amazon Redshift 完成的，但您會在查詢詳細資訊頁面上同時看到這類查詢和使用者查詢。

檢視查詢

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽功能表上，選擇查詢和載入以顯示帳戶的查詢清單。您可能需要變更此頁面的設定，才能找到您的查詢。
3. 在清單中選擇 Query (查詢) 識別碼，以顯示 Query details (查詢詳細資訊)。

Query details (查詢詳細資訊) 頁面包括附有查詢指標的 Query details (查詢詳細資訊) 和 Query plan (查詢計畫) 標籤。

指標包括查詢的詳細資訊，例如開始時間、查詢 ID、狀態和持續時間。其他詳細資訊包括查詢是否在主叢集或並行擴展叢集上執行，以及它是否為父系或重新寫入的查詢。

分析查詢執行

分析查詢

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽功能表上，選擇查詢和載入以顯示帳戶的查詢清單。您可能需要變更此頁面的設定，才能找到您的查詢。
3. 在清單中選擇 Query (查詢) 識別碼，以顯示 Query details (查詢詳細資訊)。

Query details (查詢詳細資訊) 頁面包括附有查詢指標的 Query details (查詢詳細資訊) 和 Query plan (查詢計畫) 標籤。

Note

當您向下切入查詢執行時間圖表中的查詢時，您也可以從叢集詳細資訊頁面的查詢歷史記錄索引標籤瀏覽至查詢詳細資訊頁面。

Query details (查詢詳細資訊) 頁面包含下列各節：

- Rewritten queries (重新撰寫的查詢) 清單，如以下螢幕擷取畫面所示。

Rewritten queries (5)							
This query was rewritten by Amazon Redshift for optimization							
	Start time ▲	Query ▼	Status ▼	Duration ▼	Executed on ▼	Query type ▼	
<input type="radio"/>	Apr 15th, 2020 01:44:44 PM 6 days ago	122927,122928,122929...	✔ Completed	5 min		Parent query	
<input checked="" type="radio"/>	Apr 15th, 2020 01:44:44 PM 6 days ago	122927	✔ Completed	4 sec	Main	Rewritten query	
<input type="radio"/>	Apr 15th, 2020 01:44:48 PM 6 days ago	122928	✔ Completed	22 ms	Main	Rewritten query	
<input type="radio"/>	Apr 15th, 2020 01:44:48 PM 6 days ago	122929	✔ Completed	19 ms	Main	Rewritten query	
<input type="radio"/>	Apr 15th, 2020 01:44:48 PM 6 days ago	122931	✔ Completed	5 min	Main	Rewritten query	

- Query details (查詢詳細資訊) 區段，如以下螢幕擷取畫面所示。

Query details				
Query ID 122927	Cluster ✔ dnd-sudhare-qa	User [redacted]	Type Rewritten query	Status ✔ Completed
From April 15, 2020 at 01:44:44 PM To April 15, 2020 at 01:44:48 PM				Total runtime 4sec

- Query details (查詢詳細資訊) 標籤，包含執行的 SQL 和執行的 Execution details (執行詳細資訊)。
- Query plan (查詢計劃) 標籤，包含 Query plan (查詢計劃) 步驟和其他查詢計劃的相關資訊。此表格也包含執行查詢的叢集相關圖表。
- Cluster health status (叢集運作狀態)

Cluster health status

Cluster health during the workload.

■ Healthy ■ Unhealthy



- CPU 使用率

CPU utilization

The CPU utilization of the cluster by leader node and average of compute nodes.



- Storage capacity used (已使用的儲存體容量)

Storage capacity used

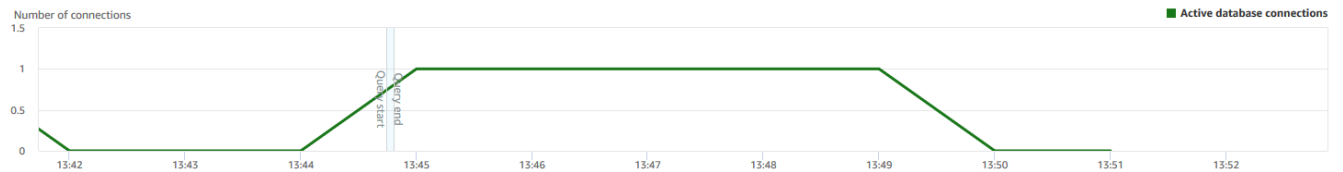
The percent of the storage capacity used.



- Active database connections (作用中的資料庫連線)

Active database connections

The number of active database connections to the cluster.



在查詢執行時檢視叢集效能

在查詢執行時顯示叢集效能

- 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
- 在導覽功能表上，選擇叢集，然後從清單中選擇叢集名稱以開啟其詳細資訊。隨即顯示叢集的詳細資訊，包含叢集效能、查詢監控、資料庫、資料共用、排程、維護和屬性標籤。
- 選擇 Query monitoring (查詢監控) 標籤以取得詳細資訊。

如需詳細資訊，請參閱 [檢視查詢歷史記錄資料](#)。

檢視載入操作期間的叢集指標

檢視載入操作期間叢集效能時，您可以辨識正在耗用資源的查詢並採取動作來降低它們的影響。如果您不希望某個載入的執行完成，可以將其終止。

Note

在 Amazon Redshift 主控台終止查詢和載入的功能需要特定的許可。如果您希望使用者能夠終止查詢和載入，請務必將 `redshift:CancelQuerySession` 動作新增至您的 AWS Identity and Access Management (IAM) 政策。無論您是選取 Amazon Redshift 唯讀 AWS 受管政策，還是在 IAM 中建立自訂政策，都適用此要求。具有 Amazon Redshift 完整存取政策之使用者已擁有必要的許可，可終止查詢和載入。如需 Amazon Redshift 之 IAM 政策中動作的相關資訊，請參閱 [管理資源存取](#)。

顯示載入操作期間的叢集效能

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽功能表上，選擇叢集，然後從清單中選擇叢集名稱以開啟其詳細資訊。隨即顯示叢集的詳細資訊，包含叢集效能、查詢監控、資料庫、資料共用、排程、維護和屬性標籤。
3. 選擇 Query monitoring (查詢監控) 標籤以取得詳細資訊。
4. 在 Queries and loads (查詢和載入) 區段中，選擇 Loads (載入) 檢視叢集的載入操作。如果載入正在執行，您可選擇 Terminate query (終止查詢) 以終止此作業。

分析工作負載效能

您可以取得工作負載效能的詳細檢視，方法是查看主控台的工作負載執行明細項目圖表。我們使用 QueryRuntimeBreakdown 指標提供的數據構建圖表。利用此圖表，您可以查看您的查詢花費各種處理階段 (例如等候和規劃) 的時間。

Note

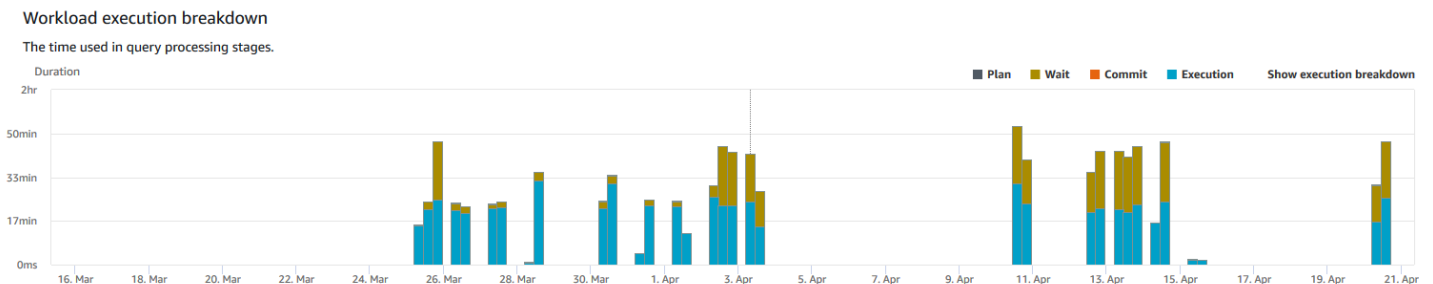
工作負載執行明細項目圖表不會對單一節點叢集顯示。

以下指標清單說明各種處理階段：

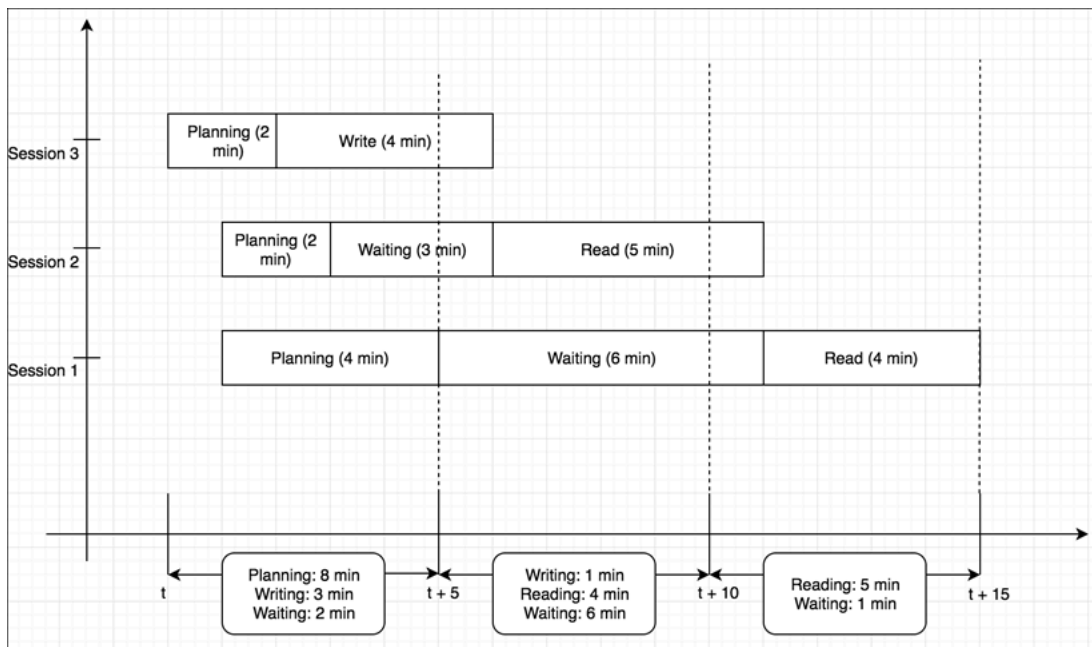
- QueryPlanning：剖析與最佳化 SQL 陳述式花費的時間。
- QueryWaiting：花費在工作負載管理 (WLM) 佇列中等待的時間。
- QueryExecutingRead：執行讀取查詢所花費的時間。
- QueryExecutingInsert：執行插入查詢所花費的時間。
- QueryExecutingDelete：執行刪除查詢所花費的時間。
- QueryExecutingUpdate：執行更新查詢所花費的時間。
- QueryExecutingCtas：執行 CREATE TABLE AS 查詢所花費的時間。
- QueryExecutingUnload：執行卸載查詢所花費的時間。
- QueryExecutingCopy：執行複製查詢所花費的時間。

例如，在 Amazon Redshift 主控台的下列圖示表示查詢在計畫、等待、讀取和寫入階段中所花的時間。您可以將此圖形中的發現與其他指標相結合，以進一步分析。在某些情況下，您的圖表可能顯示較短期間的查詢 (量測方式為 QueryDuration 指標) 在等待階段的所花費時間較長。在這些情況下，您可以為特定佇列增加 WLM 並行率，以增加傳輸量。

以下是工作負載執行細分圖表的範例。在圖表中，y 軸值是指每個階段在指定時間的平均持續時間，以堆疊長條圖顯示。



下圖說明 Amazon Redshift 如何為並行工作階段彙總查詢的處理。



顯示叢集工作負載明細表

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽功能表上，選擇叢集，然後從清單中選擇叢集名稱以開啟其詳細資訊。隨即顯示叢集的詳細資訊，包含叢集效能、查詢監控、資料庫、資料共用、排程、維護和屬性標籤。
3. 選擇與查詢有關的指標 Query monitoring (查詢監控) 標籤。
4. 在 Query monitoring (查詢監控) 區段中，選擇 Database performance (資料庫效能) 及選擇 Cluster metrics (叢集指標)。

下列指標已建立所選時間範圍的堆疊長條圖：

- Plan (計畫) 階段
- Wait (等待) 階段
- Commit (遞交) 時間
- Execution (執行) 時間

管理警示

您在 Amazon Redshift 主控台中建立的 CloudWatch 警示是警示。因為它們可協助您針對叢集和無伺服器執行個體做出主動的決定，因此很有用。您可以對 [使 CloudWatch 用指標監控 Amazon Redshift](#)

中所列的任何指標設定一或多個警示。例如，在叢集節點上設定高 CPUUtilization 的警示，可協助指出節點過度使用的時機。DataStorage 偏高的警示會追蹤無伺服器命名空間用於資料的儲存空間。

您可以從動作中修改或刪除警示。您也可以透過指定 Slack 或 Amazon Chime 網路掛鉤網址，建立響鈴或鬆弛警示，CloudWatch 將警示從 Slack 或亞馬遜鈴聲傳送到 Slack 或亞馬遜鈴聲。

您可以在本節中找到如何使用 Amazon Redshift 主控台來建立警示。您可以使用 CloudWatch 控制台或使用指標的任何其他方式（例如使用 AWS CLI 或 AWS SDK）來建立警示。

若要使用 Amazon Redshift 主控台建立 CloudWatch 警示

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。

如果您使用的是 Amazon Redshift Serverless，請選擇儀表板右上角的前往無伺服器。

2. 在導覽功能表上，選擇警示，然後選擇建立警示。
3. 在 [建立警示] 頁面上，輸入要建立 CloudWatch 警示的內容。
4. 選擇 Create alarm (建立警示)。

在 CloudWatch 主控台中使用效能指標

在 CloudWatch 主控台中使用 Amazon Redshift 指標時，請記住以下幾點：

- 僅在 Amazon Redshift 主控台中才可使用查詢和載入效能資料。
- 中的某些指標的 CloudWatch 單位與 Amazon Redshift 主控台中使用的單位不同。例如，WriteThroughput 以 GB/s 顯示（與中的位元組/秒相比 CloudWatch），這是節點典型儲存空間的相關單位。

在 CloudWatch 主控台、命令列工具或 Amazon 開發套件中使用 Amazon Redshift 指標時，請牢記以下概念：

1. 首先，指定要處理的指標維度。維度是一組用來單獨辨識指標的名稱值組。Amazon Redshift 的維度是 ClusterIdentifier 和 NodeID。在 CloudWatch 主控台中，提供 Redshift Cluster 和 Redshift Node 檢視以便輕鬆選取叢集和節點特定維度。如需維度的詳細資訊，請參閱 CloudWatch 開發人員指南中的 [維度](#)。
2. 接著，指定指標名稱，例如 ReadIOPS。

下表摘要說明可供您使用之 Amazon Redshift 指標維度的類型。視指標而定，每隔 1 分鐘或 5 分鐘可免費取得資料。如需詳細資訊，請參閱 [Amazon Redshift 指標](#)。

CloudWatch 名稱 區	維度	描述
AWS/Redshift	NodeID	篩選專屬於某個叢集的節點的資料。NodeID 可以是「Leader」、「Shared」或「Compute-N」，其中的 N 是 0, 1, ...，亦即叢集中的節點數量。「Shared」表示該叢集只有一個節點，例如領導節點與運算節點結合。
	ClusterIdentifier	篩選專屬於某個叢集的資料。專屬於叢集的指標包括 HealthStatus、MaintenanceMode 及 DatabaseConnections。通常，此維度中的指標 (例如 ReadIOPS) 也是代表節點指標資料彙總的節點指標。在解譯這些指標時應特別注意，因為它們彙整了領導與運算節點的行為。

閘道和磁碟區指標的使用類似於其他服務指標的使用。CloudWatch 文件中概述了許多常見工作，包括下列項目：

- [檢視可用的指標](#)
- [取得指標的統計資訊](#)
- [建立 CloudWatch 警示](#)

Amazon Redshift 事件

主題

- [叢集事件概觀](#)
- [使用 Amazon Simple Notification Service](#)
- [訂閱 Amazon Redshift 叢集事件通知](#)
- [使用主控台檢視叢集事件](#)
- [使用 AWS CLI 和 Amazon Redshift API 查看叢集事件](#)
- [管理叢集事件通知](#)
- [Amazon Redshift 事件通知](#)
- [Amazon Redshift 馬 Amazon 無服務器事件通知 EventBridge](#)
- [透過 Amazon 進行零 ETL 整合事件通知 EventBridge](#)

叢集事件概觀

Amazon Redshift 會追蹤叢集事件，並在您的 AWS 帳戶中保留數週的相關資訊。對於每個事件，Amazon Redshift 會報告相關的資訊，如事件發生的日期、描述、事件來源 (例如，叢集、參數群組或快照)，以及來源 ID。

Amazon Redshift 會事先提供某些事件的通知。這些事件的事件類別為 pending。例如，如果叢集的其中一個節點要硬體更新，我們會傳送事先通知。如同其他 Amazon Redshift 事件一樣，您也可以訂閱待定事件。如需詳細資訊，請參閱 [訂閱 Amazon Redshift 叢集事件通知](#)。

您可以使用 Amazon Redshift 管理主控台、Amazon Redshift API 或 AWS 開發套件來取得事件資訊。您可以取得事件清單或套用篩選條件，例如事件持續時間或開始與結束日期，以取得特定期間的事件資訊。

您可以取得特定來源類型所產生的事件，例如叢集事件或參數群組事件。「來源」資料欄會顯示觸發指定動作的資源名稱和資源類型。

您可以建立指定一組事件篩選條件的 Amazon Redshift 事件通知訂閱。發生符合篩選條件的事件時，Amazon Redshift 便會使用 Amazon Simple Notification Service 來主動通知您已發生事件。

如需依照來源類型與類別分組的 Amazon Redshift 事件清單，請參閱 [the section called “Amazon Redshift 事件類別和事件訊息”](#)。

使用 Amazon Simple Notification Service

Amazon Redshift 會使用 Amazon Simple Notification Service (Amazon SNS) 來傳達 Amazon Redshift 事件的通知。建立 Amazon Redshift 事件訂閱，即可啟用通知。在 Amazon Redshift 訂閱中，您需要指定 Amazon Redshift 事件的一組篩選條件和 Amazon SNS 主題。每當發生符合篩選條件的事件時，Amazon Redshift 就會向 Amazon SNS 主題發佈通知訊息。然後，Amazon SNS 會將訊息傳送給任何已有該主題之 Amazon SNS 訂閱的 Amazon SNS 取用者。傳送給 Amazon SNS 取用者的訊息可以採用 Amazon SNS 針對某個 AWS 區域支援的任何形式，例如電子郵件、文字訊息或呼叫 HTTP 端點。例如，所有區域均支援電子郵件通知，但簡訊通知只能針對美國東部 (維吉尼亞北部) 來建立。

Note

目前，您只能建立 Amazon SNS 標準主題的事件訂閱 (而非 Amazon SNS FIFO 主題的事件訂閱)。如需詳細資訊，請參閱《Amazon Simple Notification Service 開發人員指南》中的 [Amazon SNS 事件來源](#)。

當您建立事件通知訂閱時，您需要指定一或多個事件篩選條件。只要發生符合所有篩選條件的事件，Amazon Redshift 就會透過訂閱傳送通知。篩選條件包含來源類型 (例如叢集或快照)、來源 ID (例如叢集或快照的名稱)、事件類別 (例如監控或安全性) 和事件嚴重性 (例如 INFO 或 ERROR)。

您可以在中將「已啟用」選項按鈕設定為，或將 Enabled 參數設定為 false 使用 Amazon Redshift CLI AWS Management Console 或 API，即可輕鬆關閉通知，而不刪除訂閱。

Amazon Redshift 事件通知的帳單會透過 Amazon Simple Notification Service (Amazon SNS) 來傳送。使用事件通知時需支付 Amazon SNS 費用；如需 Amazon SNS 帳單的相關資訊，請前往 [Amazon Simple Notification Service 定價](#)。

您亦可使用管理主控台來檢視發生的 Amazon Redshift 事件。如需詳細資訊，請參閱 [Amazon Redshift 事件](#)。

訂閱 Amazon Redshift 叢集事件通知

您可以建立 Amazon Redshift 事件通知訂閱，在指定的叢集、快照、安全群組或參數群組發生事件時收到通知。建立訂閱最簡單的方式是使用 Amazon SNS 主控台。如需建立和訂閱 Amazon SNS 主題的詳細資訊，請參閱 [Amazon SNS 入門](#)。

您可以建立 Amazon Redshift 事件通知訂閱，在指定的叢集、快照、安全群組或參數群組發生事件時收到通知。建立訂閱最簡單的方式是使用 AWS Management Console 主控台。如果您選擇使用 CLI 或 API 建立事件通知訂閱，您必須建立 Amazon Simple Notification Service 主題，並使用 Amazon SNS 主控台或 Amazon SNS API 訂閱該主題。您也將必須保留主題的 Amazon Resource Name (ARN)，因為在提交 CLI 命令或 API 動作時會用到它。如需建立和訂閱 Amazon SNS 主題的詳細資訊，請參閱 [Amazon SNS 入門](#)。

Amazon Redshift 事件訂閱可指定這些事件條件：

- 來源類型，其值包括叢集、快照、參數群組和安全群組。
- 資源的來源 ID，例如 `my-cluster-1` 或 `my-snapshot-20130823`。ID 必須是與事件訂閱位於相同 AWS 區域的資源。
- 事件類別，其值包括組態、管理、監控、安全與待定。
- 事件嚴重性，其值包括 INFO 或 ERROR。

事件條件可單獨指定，但您必須先指定來源類型，才能在主控台中指定來源 ID。例如，您可指定事件類別，但不需指定來源類型、來源 ID 或嚴重性。雖然您可以為非來源類型所指定類型的資源指定來源 ID，但將不會針對這些資源傳送事件通知。例如，如果您指定來源類型為叢集，ID 為安全群組，而該安全群組發生的事件均與來源類型篩選條件不符，將不會傳送這些事件的通知。

發生符合訂閱指定之所有條件的任何事件時，Amazon Redshift 便會傳送通知。傳回之事件集合的一些範例：

- 訂閱指定來源類型為叢集，來源 ID 為 `my-cluster-1`，類別為監控，嚴重性為 ERROR。訂閱將針對來自 `my-cluster-1`、嚴重性為 ERROR 的監控事件傳送通知。
- 訂閱指定來源類型為叢集，類別為組態，嚴重性為 INFO。訂閱會從 AWS 帳戶中的任何 Amazon Redshift 叢集傳送嚴重性為 INFO 之組態事件的通知。
- 訂閱指定類別為組態，嚴重性為 INFO。訂閱會從 AWS 帳戶中的任何 Amazon Redshift 資源傳送嚴重性為 INFO 的組態事件通知。
- 訂閱指定嚴重性為 ERROR。訂閱會從 AWS 帳戶中的任何 Amazon Redshift 資源傳送嚴重程度為錯誤的所有事件的通知。

如果刪除或移除名稱在現有訂閱中做為來源 ID 參考的物件，訂閱將保持作用中，但不會傳送該物件的任何事件。如果之後建立新物件，且物件使用訂閱來源 ID 中所參考的相同名稱，訂閱將開始傳送新物件的事件通知。

Amazon Redshift 會將事件通知發佈至以 Amazon Resource Name (ARN) 識別的 Amazon SNS 主題。使用 Amazon Redshift 主控台建立事件訂閱時，您可指定現有的 Amazon SNS 主題，或要求主控台在建立訂閱時建立主題。傳送至 Amazon SNS 主題的所有 Amazon Redshift 事件通知，接著會傳送給所有訂閱該主題的 Amazon SNS 取用者。使用 Amazon SNS 主控台來變更 Amazon SNS 主題，例如新增或移除取用者對主題的訂閱。如需建立和訂閱 Amazon SNS 主題的相關資訊，請前往 [Amazon Simple Notification Service 入門](#)。

以下幾節會列出您可以收到通知的所有類別和事件。亦提供有關訂閱和使用 Amazon Redshift 事件訂閱的資訊。

使用主控台檢視叢集事件

檢視事件

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽功能表上，選擇事件。

使用 AWS CLI 和 Amazon Redshift API 查看叢集事件

您可以使用下列 Amazon Redshift CLI 操作來檢視事件。

- [describe-events](#)

Amazon Redshift 提供以下 API 以檢視事件。

- [DescribeEvents](#)

管理叢集事件通知

您可以建立 Amazon Simple Notification Service (Amazon SNS) 事件通知訂閱，在指定的 Amazon Redshift 叢集、快照、安全群組或參數群組發生事件時傳送通知。這些通知將傳送至 SNS 主題，接著再傳送訊息給訂閱該主題的任何 SNS 消費者。傳送給取用者的 SNS 訊息可以採用 Amazon SNS 針對某個 AWS 區域支援的任何通知形式，例如電子郵件、文字訊息或 HTTP 端點的呼叫。例如，所有區域均支援電子郵件通知，但簡訊通知只能針對美國東部 (維吉尼亞北部) 來建立。如需詳細資訊，請參閱 [Amazon Redshift 事件通知](#)。

使用 Amazon Redshift 主控台管理叢集事件通知

建立事件通知訂閱

建立事件訂閱

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽功能表上，選擇事件。
3. 選擇 Event subscription (事件訂閱) 標籤，然後選擇 Create event subscriptions (建立事件訂閱)。
4. 輸入事件訂閱的屬性，例如名稱、來源類型、類別和嚴重性。您也可以啟用 Amazon SNS 主題來接收事件通知。
5. 選擇 Create event subscriptions (建立事件訂閱) 以建立訂閱。

使用 AWS CLI 和 Amazon Redshift API 管理叢集事件通知

您可以使用下列 Amazon Redshift CLI 操作來管理叢集事件通知。

- [create-event-subscription](#)
- [delete-event-subscription](#)
- [describe-event-categories](#)
- [describe-event-subscriptions](#)
- [describe-events](#)
- [modify-event-subscription](#)

您可以使用下列 Amazon Redshift API 動作來管理事件通知。

- [CreateEventSubscription](#)
- [DeleteEventSubscription](#)
- [DescribeEventCategories](#)
- [DescribeEventSubscriptions](#)
- [DescribeEvents](#)
- [ModifyEventSubscription](#)

如需 Amazon Redshift 事件通知的相關資訊，請參閱 [Amazon Redshift 事件通知](#)。

Amazon Redshift 事件通知

Amazon Redshift 事件類別和事件訊息

本節將告訴您各 Amazon Redshift 來源類型的事件 ID 和類別。

下表顯示來源類型為叢集時的事件類別和事件清單。

Amazon Redshift 類別	事件 ID	事件嚴重性	描述
組態	REDSHIFT-EVENT-1000	INFO	參數群組 [參數群組名稱] 於 [時間] 更新。如果您只變更動態參數，則現在正在修改相關聯的叢集。如果您變更靜態參數，則會在您重新啟動相關聯的叢集時套用所有更新，包括動態參數。
組態	REDSHIFT-EVENT-1001	INFO	您的 Amazon Redshift 叢集 [叢集名稱] 於 [時間] 修改為使用參數群組 [參數群組名稱]。
組態	REDSHIFT-EVENT-1500	ERROR	Amazon VPC [VPC 名稱] 不存在。您對叢集 [叢集名稱] 的組態變更尚未套用。請造訪 AWS Management Console 以修正此問題。
組態	REDSHIFT-EVENT-1501	ERROR	您為 Amazon VPC [VPC 名稱] 指定的客戶子網路 [子網路名稱] 不存在或無效。您對叢集 [叢集名稱] 的組態變更尚未套用。請造訪 AWS Management Console 以修正此問題。
組態	REDSHIFT-EVENT-1502	ERROR	叢集子網路群組 [子網路群組名稱] 中的子網路沒有可用的 IP 地址。無法建立叢集 [叢集名稱]。
組態	REDSHIFT-EVENT-1503	ERROR	Amazon VPC [VPC 名稱] 未連接網際網路閘道。您對叢集 [叢集名稱] 的組態變更尚未套用。

Amazon Redshift 類別	事件 ID	事件嚴重性	描述
			請造訪 AWS Management Console 以更正問題。
組態	REDSHIFT-EVENT-1504	ERROR	叢集 [叢集名稱] 的 HSM 無法連線。
組態	REDSHIFT-EVENT-1505	ERROR	叢集 [叢集名稱] 的 HSM 無法註冊。請嘗試不同的組態。
組態	REDSHIFT-EVENT-1506	ERROR	Amazon Redshift 已超過您帳戶的彈性網路界面限制。刪除最多 [彈性網路介面的最大數量] 彈性網路介面，或要求增加 EC2 區域中每個 AWS 區域的網路介面數量限制。
組態	REDSHIFT-EVENT-1509	ERROR	<p>無法建立 Amazon Redshift 叢集 [叢集名稱]，因為您的帳戶已達到 VPC 端點限制。刪除未使用的 VPC 端點，或請求提高 VPC 端點的限制。</p> <p>如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的 VPC 端點。</p>
組態	REDSHIFT-EVENT-1510	ERROR	<p>我們偵測到在 Amazon Redshift 叢集 [叢集名稱] 上載入範例資料的嘗試失敗。若要載入範例資料，請先設定 VPC 以便能夠存取 Amazon S3 儲存貯體，然後再建立新叢集並載入範例資料。</p> <p>如需詳細資訊，請參閱《Amazon Redshift 管理指南》中的 啟用增強型 VPC 路由。</p>
組態	REDSHIFT-EVENT-1511	ERROR	無法建立 Amazon Redshift 叢集 [叢集名稱]，因為您已超過帳戶的彈性 IP 地址限制。使用 Amazon EC2 刪除未使用的彈性 IP 地址或請求提高限制。

Amazon Redshift 類別	事件 ID	事件嚴重性	描述
管理	REDSHIFT-EVENT-2000	INFO	您的 Amazon Redshift 叢集 [叢集名稱] 已建立且已就緒可供使用。
管理	REDSHIFT-EVENT-2001	INFO	您的 Amazon Redshift 叢集 [叢集名稱] 於 [時間] 刪除。最後的快照 [已/未] 儲存。
管理	REDSHIFT-EVENT-2002	INFO	叢集 [叢集名稱] 的 VPC 安全群組已於 [UTC 時間] 更新。
管理	REDSHIFT-EVENT-2003	INFO	叢集 [叢集名稱] 於 [UTC 時間] 開始維護。
管理	REDSHIFT-EVENT-2004	INFO	叢集 [叢集名稱] 於 [UTC 時間] 完成維護。
管理	REDSHIFT-EVENT-2006	INFO	叢集 [叢集名稱] 於 [UTC 時間] 開始調整大小。叢集為唯讀模式。
管理	REDSHIFT-EVENT-2007	INFO	已確認叢集 [叢集名稱] 的調整大小請求。
管理	REDSHIFT-EVENT-2008	INFO	建立新 Amazon Redshift 叢集 [叢集名稱] 快照 [快照名稱] 的還原操作於 [時間] 開始。若要監控還原流程，請造訪 AWS Management Console。
管理	REDSHIFT-EVENT-2013	INFO	您的 Amazon Redshift 叢集 [叢集名稱] 於 [時間] 重新命名。
管理	REDSHIFT-EVENT-2014	INFO	已收到 Amazon Redshift 叢集 [叢集名稱] 的資料表還原要求。
管理	REDSHIFT-EVENT-2015	INFO	Amazon Redshift 叢集 [叢集名稱] 於 [時間] 取消資料表還原。

Amazon Redshift 類別	事件 ID	事件嚴重性	描述
管理	REDSHIFT-EVENT-2016	INFO	您的 Amazon Redshift 叢集 [叢集名稱] 於 [時間] 開始替換。
管理	REDSHIFT-EVENT-2017	INFO	您的 Amazon Redshift 叢集 [叢集名稱] 已於 [時間] 開始客戶所啟動的維護。叢集在維護期間可能無法使用。
管理	REDSHIFT-EVENT-2018	INFO	您的 Amazon Redshift 叢集 [叢集名稱] 已於 [時間] 完成客戶所啟動的維護。
管理	REDSHIFT-EVENT-2019	ERROR	您的 Amazon Redshift 叢集 [叢集名稱] 於 [時間] 執行客戶所啟動的維護失敗。正在將叢集返回其原始狀態。
管理	REDSHIFT-EVENT-2020	INFO	您的 Amazon Redshift 叢集 [叢集名稱] 追蹤已從 [舊追蹤] 修改為 [新追蹤]。
管理	REDSHIFT-EVENT-2021	ERROR	從容量集區取得容量時，Amazon Redshift 叢集 [叢集名稱] 的 [操作] 未成功。我們正在設法取得容量，但現在，我們已取消您的請求。刪除此叢集，稍後再試。
管理	REDSHIFT-EVENT-2022	ERROR	從容量集區取得容量時，Amazon Redshift 叢集 [叢集名稱] 的 [操作] 未成功。我們正在設法取得容量，但現在，我們已取消您的請求。[替代可用區域] 中有可用容量。請刪除此叢集，並在替代可用區域中重試。

Amazon Redshift 類別	事件 ID	事件嚴重性	描述
管理	REDSHIFT-EVENT-2023	ERROR	我們偵測到您的單一節點 Amazon Redshift 叢集 [叢集名稱] 發生硬體故障，這可能已導致查詢失敗，或叢集的可用性不穩定。從容量集區取得容量時，取代叢集未成功。您將需要從快照還原新叢集。刪除此叢集，選取最新可用的快照，然後從該快照還原新叢集。這將會自動佈建在狀況良好的硬體上。
管理	REDSHIFT-EVENT-2024	ERROR	我們偵測到您的單一節點 Amazon Redshift 叢集 [叢集名稱] 發生硬體故障，這可能已導致查詢失敗，或叢集的可用性不穩定。從容量集區取得容量時，取代叢集未成功。可用區域 [替代可用區域] 中有可用容量。刪除此叢集，選取最新可用的快照，然後從該快照還原新叢集。這將會自動佈建在狀況良好的硬體上。
管理	REDSHIFT-EVENT-3011	INFO	Amazon Redshift 叢集「[叢集名稱]」的彈性調整大小於 [時間] 開始。我們在調整大小期間會保持資料庫連線。在此操作期間，部分查詢和連線可能終止或逾時。
管理	REDSHIFT-EVENT-3012	INFO	我們收到叢集 '[叢集名稱]' 在 [時間] 開始的彈性調整大小請求。調整大小開始時，我們會提供事件通知。
待定	REDSHIFT-EVENT-2025	INFO	叢集 <叢集名稱> 的資料庫將在 <開始時間> 和 <結束時間> 之間更新。將無法存取您的叢集。請妥善規劃。
待定	REDSHIFT-EVENT-2026	INFO	叢集 <叢集名稱> 將在 <開始時間> 和 <結束時間> 之間更新。將無法存取您的叢集。請妥善規劃。

Amazon Redshift 類別	事件 ID	事件嚴重性	描述
監控	REDSHIFT-EVENT-2050	INFO	在 Amazon Redshift 叢集 [叢集名稱] 上偵測到硬體問題。已於 [時間] 啟動替換要求。
監控	REDSHIFT-EVENT-3000	INFO	您的 Amazon Redshift 叢集 [叢集名稱] 於 [時間] 重新開機。
監控	REDSHIFT-EVENT-3001	INFO	您的 Amazon Redshift 叢集 [叢集名稱] 上的某一節點於 [時間] 自動替換，叢集目前正常運作中。
監控	REDSHIFT-EVENT-3002	INFO	您的 Amazon Redshift 叢集 [叢集名稱] 已完成調整規模，叢集目前可供讀寫。該規模調整於 [時間] 啟動，並花了 [小時數] 小時完成。
監控	REDSHIFT-EVENT-3003	INFO	已成功從快照 [快照名稱] 建立 Amazon Redshift 叢集 [叢集名稱]，且叢集目前可供使用。
監控	REDSHIFT-EVENT-3007	INFO	您的 Amazon Redshift 快照 [快照名稱] 已在 [時間] 從 [來源 AWS 區域] 成功複製到 [目的地 AWS 區域]。
監控	REDSHIFT-EVENT-3008	INFO	Amazon Redshift 叢集 [叢集名稱] 於 [時間] 開始資料表還原。
監控	REDSHIFT-EVENT-3009	INFO	Amazon Redshift 叢集 [叢集名稱] 於 [時間] 成功完成資料表還原。
監控	REDSHIFT-EVENT-3010	ERROR	Amazon Redshift 叢集 [叢集名稱] 於 [時間] 執行資料表還原失敗。
監控	REDSHIFT-EVENT-3013	ERROR	由於 [原因]，對 Amazon Redshift 叢集 [叢集名稱] 所要求的彈性調整大小操作於 [時間] 失敗。

Amazon Redshift 類別	事件 ID	事件嚴重性	描述
監控	REDSHIFT-EVENT-3014	INFO	Amazon Redshift 叢集 [叢集名稱] 於 [時間] 重新開機。
監控	REDSHIFT-EVENT-3500	ERROR	您的 Amazon Redshift 叢集 [叢集名稱] 調整大小失敗。幾分鐘後會自動重試調整規模。
監控	REDSHIFT-EVENT-3501	ERROR	從快照 [快照名稱] 建立 Amazon Redshift 叢集 [叢集名稱] 的還原操作於 [時間] 執行失敗。請重試操作。
監控	REDSHIFT-EVENT-3504	ERROR	Amazon S3 儲存貯體 [儲存貯體名稱] 無法用於叢集 [叢集名稱] 的記錄。
監控	REDSHIFT-EVENT-3505	ERROR	Amazon S3 儲存貯體 [儲存貯體名稱] 未擁有叢集 [叢集名稱] 的正確 IAM 政策。
監控	REDSHIFT-EVENT-3506	ERROR	Amazon S3 儲存貯體 [儲存貯體名稱] 不存在。叢集 [叢集名稱] 無法繼續記錄。
監控	REDSHIFT-EVENT-3507	ERROR	Amazon Redshift 叢集 [叢集名稱] 無法用 EIP [IP 地址] 建立。該 EIP 已被使用。
監控	REDSHIFT-EVENT-3508	ERROR	Amazon Redshift 叢集 [叢集名稱] 無法用 EIP [IP 地址] 建立。找不到該 EIP。
監控	REDSHIFT-EVENT-3509	ERROR	跨區域快照複本未針對叢集 [叢集名稱] 啟用。
監控	REDSHIFT-EVENT-3510	ERROR	Amazon Redshift 叢集 [叢集名稱] 於 [時間] 啟動資料表還原失敗。原因：[原因]。
監控	REDSHIFT-EVENT-3511	ERROR	Amazon Redshift 叢集 [叢集名稱] 於 [時間] 執行資料表還原失敗。

Amazon Redshift 類別	事件 ID	事件嚴重性	描述
監控	REDSHIFT-EVENT-3512	ERROR	Amazon Redshift 叢集 [叢集名稱] 因硬體問題而失敗。正自動從 [時間] 建立的最新快照 [快照名稱] 還原叢集。
監控	REDSHIFT-EVENT-3513	ERROR	Amazon Redshift 叢集 [叢集名稱] 因硬體問題而失敗。正自動從 [時間] 建立的最新快照 [快照名稱] 還原叢集。在此時間後進行的任何資料庫變更將需要重新提交。
監控	REDSHIFT-EVENT-3514	ERROR	Amazon Redshift 叢集 [叢集名稱] 因硬體問題而失敗。叢集目前為硬體故障狀態。請刪除叢集，並從 [時間] 建立的最新快照 [快照名稱] 還原。
監控	REDSHIFT-EVENT-3515	ERROR	Amazon Redshift 叢集 [叢集名稱] 因硬體問題而失敗。叢集目前為硬體故障狀態。請刪除叢集，並從 [時間] 建立的最新快照 [快照名稱] 還原。在此時間後進行的任何資料庫變更將需要重新提交。
監控	REDSHIFT-EVENT-3516	ERROR	Amazon Redshift 叢集 [叢集名稱] 因硬體問題而故障，且該叢集沒有備份。叢集目前為硬體故障狀態，可以刪除。
監控	REDSHIFT-EVENT-3519	INFO	叢集 [叢集名稱] 於 [時間] 開始重新啟動。
監控	REDSHIFT-EVENT-3520	INFO	叢集 [叢集名稱] 於 [時間] 完成重新啟動。
監控	REDSHIFT-EVENT-3521	INFO	我們在叢集「[叢集名稱]」上偵測到連線問題。已於 [時間] 啟動自動診斷檢查。

Amazon Redshift 類別	事件 ID	事件嚴重性	描述
監控	REDSHIFT-EVENT-3522	INFO	「[叢集名稱]」叢集的復原動作於 [時間] 失敗。Amazon Redshift 團隊正在尋找解決方案。
監控	REDSHIFT-EVENT-3533	ERROR	'[叢集名稱]' 上的叢集調整大小已在 [時間] 取消。已取消操作，因為 [原因]。[需要的動作]。
監控	REDSHIFT-EVENT-3534	INFO	Amazon Redshift 叢集「[叢集名稱]」的彈性調整大小在 [時間] 完成。當我們傳輸資料時，叢集現在可用於讀取和寫入操作。完成資料傳輸前，部分查詢可能需要較長的時間才會完成。
監控	REDSHIFT-EVENT-3537	INFO	叢集「[叢集名稱]」資料傳輸已於 [UTC 時間] 完成。
監控	REDSHIFT-EVENT-3600	INFO	對 Amazon RedShift 叢集 '[叢集名稱]' 要求的調整大小操作已在過去取消。轉返在 [時間] 完成。
待定	REDSHIFT-EVENT-3601	INFO	叢集 <叢集名稱> 上的節點將在 <開始時間> 和 <結束時間> 之間取代。您無法延遲此維護。請妥善規劃。
待定	REDSHIFT-EVENT-3602	INFO	叢集 <叢集名稱> 上的節點已排定在 <開始時間> 和 <結束時間> 之間取代。將無法存取您的叢集。請妥善規劃。
管理	REDSHIFT-EVENT-3603	INFO	從快照 [快照名稱] 建立叢集 [叢集名稱] 的還原操作因內部錯誤而失敗。叢集目前不相容還原狀態，因此可以刪除。請嘗試以不同組態，將快照還原成叢集。
管理	REDSHIFT-EVENT-3614	INFO	排程動作 [已排程的動作名稱] 已在 [UTC 時間] 建立。第一次呼叫已排程在 [UTC 時間] 進行。

Amazon Redshift 類別	事件 ID	事件嚴重性	描述
管理	REDSHIFT-EVENT-3615	INFO	排程動作 [已排程的動作名稱] 已排程在 [UTC 時間] 進行。
監控	REDSHIFT-EVENT-3616	INFO	排程動作 [已排程的動作名稱] 已在 [UTC 時間] 完成，其狀態為 'SUCCEEDED' (成功)。
監控	REDSHIFT-EVENT-3617	ERROR	排程動作 [已排程的動作名稱] 已在 [UTC 時間] 因延遲而跳過。
監控	REDSHIFT-EVENT-3618	INFO	叢集 [叢集名稱] 暫停操作已在 [UTC 時間] 開始。已開始暫停
監控	REDSHIFT-EVENT-3619	INFO	Amazon Redshift 叢集 [叢集名稱] 已在 [UTC 時間] 成功暫停。
管理	REDSHIFT-EVENT-3626	INFO	排程動作 [已排程的動作名稱] 已在 [UTC 時間] 修改。第一次呼叫已排程在 [UTC 時間] 進行。
管理	REDSHIFT-EVENT-3627	INFO	排程動作 [已排程的動作名稱] 已在 [UTC 時間] 遭到刪除。
監控	REDSHIFT-EVENT-3628	ERROR	排程動作 [已排程的動作名稱] 已在 [UTC 時間] 完成，其狀態為 'FAILED' (失敗)。
管理	REDSHIFT-EVENT-3629	INFO	Amazon Redshift [叢集名稱] 已收到您的重新定位請求。當可用區域重新定位完成時，Amazon Redshift 會傳送事件通知。
管理	REDSHIFT-EVENT-3630	INFO	Amazon Redshift 叢集 [叢集名稱] 已成功從 [可用區域] 重新定位到 [可用區域]。您現在可以使用該叢集了。
管理	REDSHIFT-EVENT-3631	INFO	Amazon Redshift 已成功將 Amazon Redshift 叢集 [叢集名稱] 從 [可用區域] 重新定位到 [可用區域] 以進行復原。

Amazon Redshift 類別	事件 ID	事件嚴重性	描述
管理	REDSHIFT-EVENT-3632	INFO	由於組態變更，Amazon Redshift 已暫時停用 Amazon Redshift 叢集 [叢集名稱] 的叢集重新定位功能。請稍後再嘗試重新定位叢集。
監控	REDSHIFT-EVENT-3658	ERROR	Redshift 叢集 [叢集 ID] 的 EC2-Classic 至 EC2-VPC 遷移失敗。
監控	REDSHIFT-EVENT-3659	INFO	Redshift 叢集 [叢集 ID] 的 EC2-Classic 至 EC2-VPC 遷移成功。
監控	REDSHIFT-EVENT-3660	INFO	叢集目前為硬體故障狀態。請刪除 EC2-Classic 叢集，並從 [UTC 時間] 建立的最新快照 [快照名稱] 還原至 EC2-VPC 叢集。
管理	REDSHIFT-EVENT-3666	INFO	Amazon Redshift 異地同步備份叢集 [叢集名稱] 已在 [UTC 時間] 偵測到故障，並觸發自動復原。
管理	REDSHIFT-EVENT-3667	INFO	Amazon Redshift 異地同步備份叢集 [叢集名稱] 在 [UTC 時間] 成功復原，並可用於 [第一個可用區域]。另一個 AZ 中的次要運算即將推出。
監控	REDSHIFT-EVENT-3668	ERROR	Amazon Redshift 異地同步備份叢集 [叢集名稱] 無法在 [UTC 時間] 復原。
管理	REDSHIFT-EVENT-3669	INFO	Amazon Redshift 異地同步備份叢集 [叢集名稱] 在 [UTC 時間] 成功復原，並可與 [第一個可用區域] 和 [第二個可用區域] 的運算資源搭配使用。
管理	REDSHIFT-EVENT-3670	INFO	Amazon Redshift 叢集的維護 [叢集名稱] 已於 [UTC 時間] 完成，並可與 [第一個可用區域] 中的運算資源搭配使用。另一個 AZ 中的次要運算即將推出。

Amazon Redshift 類別	事件 ID	事件嚴重性	描述
管理	REDSHIFT-EVENT-3671	INFO	在 Amazon Redshift 叢集上調整大小 [叢集名稱] 已於 [UTC 時間] 完成，並可在 [第一個可用區域] 中使用。另一個 AZ 中的次要運算即將推出。
管理	REDSHIFT-EVENT-3672	INFO	Amazon Redshift 異地同步備份叢集 [叢集名稱] 在 [UTC 時間] 偵測到 [第二個可用性區域] 中的故障，並觸發了自動復原。
管理	REDSHIFT-EVENT-3673	INFO	為 Amazon Redshift 叢集啟用異地同步備份 [叢集名稱] 的作業已於 [UTC 時間] 開始。
管理	REDSHIFT-EVENT-3674	INFO	為 Amazon Redshift 叢集啟用異地同步備份 [叢集名稱] 的作業已在 [UTC 時間] 順利完成。
監控	REDSHIFT-EVENT-3675	ERROR	為 Amazon Redshift 叢集啟用異地同步備份 [叢集名稱] 的作業在 [UTC 時間] 失敗。
管理	REDSHIFT-EVENT-3676	INFO	停用 Amazon Redshift 異地同步備份叢集 [叢集名稱] 的異地同步備份作業已於 [UTC 時間] 開始。
管理	REDSHIFT-EVENT-3677	INFO	停用 Amazon Redshift 叢集 [叢集名稱] 的異地同步備份作業已在 [UTC 時間] 順利完成。
監控	REDSHIFT-EVENT-3678	ERROR	為 Amazon Redshift 叢集 [叢集名稱] 停用異地同步備份的作業在 [UTC 時間] 失敗。
組態	REDSHIFT-EVENT-3679	INFO	已成功修改 Amazon Redshift 叢集 [叢集名稱] 的連接埠。
組態	REDSHIFT-EVENT-3680	ERROR	Amazon Redshift 無法建立叢集 [叢集名稱]，因為無法存取此操作所需的服務連結角色 (SLR)。請嘗試從 Amazon Redshift 主控台再次建立。Amazon Redshift 會自動建立 SLR。

Amazon Redshift 類別	事件 ID	事件嚴重性	描述
監控	REDSHIFT-EVENT-3684	ERROR	您的 Amazon S3 儲存貯體 [儲存貯體名稱] 已使用未知或無法存取的 AWS KMS 金鑰加密。請修改您 Amazon S3 儲存貯體的加密。
管理	REDSHIFT-EVENT-3685	ERROR	叢集 [叢集名稱] 上的還原作業失敗，因為它沒有足夠的可用磁碟空間。正在復原作業。嘗試使用不同的配置還原到叢集。
管理	REDSHIFT-EVENT-3686	ERROR	叢集 [叢集名稱] 上的調整大小作業失敗，因為它沒有足夠的可用磁碟空間。正在復原作業。嘗試使用不同配置調整叢集的大小。
安全	REDSHIFT-EVENT-4000	INFO	您 Amazon Redshift 叢集 [叢集名稱] 的管理員憑證已於 [時間] 更新。
安全	REDSHIFT-EVENT-4001	INFO	安全群組 [安全群組名稱] 於 [時間] 修改。變更將自動套用到所有相關聯的叢集。
安全	REDSHIFT-EVENT-4500	ERROR	您提供的安全群組 [安全群組名稱] 無效。您對叢集 [叢集名稱] 的組態變更尚未套用。請造訪 AWS Management Console 以更正問題。
安全	REDSHIFT-EVENT-4501	ERROR	找不到叢集安全群組 [叢集安全群組名稱] 中指定的安全群組 [安全群組名稱]。無法完成授權。
安全	REDSHIFT-EVENT-4502	ERROR	由於並行活動，Amazon Redshift 叢集 [叢集名稱] 的管理員憑證無法在 [時間] 更新。請允許目前的工作負載以完成或減少作用中的工作負載，然後重試該操作。
安全	REDSHIFT-EVENT-4503	ERROR	Amazon Redshift 無法存取叢集的秘密 [叢集名稱]。

Amazon Redshift 類別	事件 ID	事件嚴重性	描述
安全	REDSHIFT-EVENT-4504	ERROR	Amazon Redshift 無法存取用來加密叢集 [叢集名稱] 的管理員登入資料密碼的 KMS 金鑰 [KMS 金鑰]。
安全	REDSHIFT-EVENT-4505	ERROR	Amazon Redshift 無法輪換叢集 [叢集名稱] 的密碼，因為叢集上有正在進行的作業。
安全	REDSHIFT-EVENT-4506	ERROR	您的 Amazon Redshift 叢集 [叢集名稱] 已暫停。Amazon Redshift 無法輪換已暫停叢集的秘密。

下表顯示當參數群組為來源類型時的事件類別和事件清單。

參數群組來源類型的類別和事件

Amazon Redshift 類別	事件 ID	事件嚴重性	描述
組態	REDSHIFT-EVENT-1002	INFO	參數 [參數名稱] 於 [時間] 從 [數值] 更新為 [數值]。
組態	REDSHIFT-EVENT-1003	INFO	已建立 [群組名稱] 叢集參數群組。
組態	REDSHIFT-EVENT-1004	INFO	已刪除 [群組名稱] 叢集參數群組。
組態	REDSHIFT-EVENT-1005	INFO	叢集參數群組 [名稱] 於 [時間] 更新。如果您只變更動態參數，則現在正在修改相關聯的叢集。如果您變更靜態參數，則會在您重新啟動相關聯的叢集時套用所有更新，包括動態參數。

下表顯示當安全群組為來源類型時的事件類別和事件清單。

安全群組來源類型的類別和事件

Amazon Redshift 類別	事件 ID	事件嚴重性	描述
安全	REDSHIFT-EVENT-4002	INFO	已建立 [群組名稱] 叢集安全群組。
安全	REDSHIFT-EVENT-4003	INFO	已刪除 [群組名稱] 叢集安全群組。
安全	REDSHIFT-EVENT-4004	INFO	叢集安全群組 [群組名稱] 於 [時間] 變更。變更將自動套用到所有相關聯的叢集。

下表顯示當快照為來源類型時的事件類別和事件清單。

快照來源類型的類別和事件

Amazon Redshift 類別	事件 ID	事件嚴重性	描述
管理	REDSHIFT-EVENT-2009	INFO	Amazon Redshift 叢集 [叢集名稱] 的使用者快照 [快照名稱] 於 [時間] 開始。若要監控快照流程，請造訪 AWS Management Console。
管理	REDSHIFT-EVENT-2010	INFO	Amazon Redshift 叢集 [叢集名稱] 的使用者快照 [快照名稱] 於 [時間] 取消。
管理	REDSHIFT-EVENT-2011	INFO	Amazon Redshift 叢集 [叢集名稱] 的使用者快照 [快照名稱] 於 [時間] 刪除。
管理	REDSHIFT-EVENT-2012	INFO	Amazon Redshift 叢集 [叢集名稱] 最後的快照 [快照名稱] 於 [時間] 開始。
監控	REDSHIFT-EVENT-3004	INFO	Amazon Redshift 叢集 [叢集名稱] 的使用者快照 [快照名稱] 於 [時間] 成功完成。

Amazon Redshift 類別	事件 ID	事件嚴重性	描述
監控	REDSHIFT-EVENT-3005	INFO	Amazon Redshift 叢集 [叢集名稱] 最後的快照 [快照名稱] 於 [時間] 成功完成。
監控	REDSHIFT-EVENT-3006	INFO	Amazon Redshift 叢集 [叢集名稱] 最後的快照 [快照名稱] 於 [時間] 取消。
監控	REDSHIFT-EVENT-3502	ERROR	Amazon Redshift 叢集 [叢集名稱] 最後的快照 [快照名稱] 於 [時間] 失敗。團隊正在調查問題。請造訪 AWS Management Console 以重試該作業。
監控	REDSHIFT-EVENT-3503	ERROR	Amazon Redshift 叢集 [叢集名稱] 的使用者快照 [快照名稱] 於 [時間] 失敗。團隊正在調查問題。請造訪 AWS Management Console 以重試該作業。

Amazon Redshift 馬 Amazon 無服務器事件通知 EventBridge

Amazon Redshift 無伺服器使用 Amazon EventBridge 來管理事件通知，讓您 up-to-date 掌握資料倉儲中的變更。Amazon EventBridge 是一種無伺服器事件匯流排服務，可用來連接應用程式與來自各種來源的資料。在這種情況下，事件來源是 Amazon Redshift。事件 (受監控環境中的變更) 會自動 EventBridge 從 Amazon Redshift 資料倉儲傳送到這些事件。系統會以接近即時的速度傳送事件。

功能 EventBridge 包括提供編寫事件規則的環境，這些環境可以指定要針對特定事件採取的動作。您也可以設定目標，這些目標是 EventBridge 可以將事件傳送至的資源。目標可以包括 API 目的地、Amazon CloudWatch 日誌群組和其他目標。如需有關規則的詳細資訊，請參閱 [Amazon EventBridge 規則](#)。如需有關目標的詳細資訊，請參閱 [Amazon EventBridge 目標](#)。

事件可以分為嚴重性和類別兩種。可用的篩選條件如下：

- 資源篩選 — 根據事件所關聯的資源來接收訊息。資源包括工作群組和快照等項目。
- 時段篩選 — 將範圍限定在特定時段內的事件。
- 類別篩選 — 接收指定類別中所有事件的事件通知。

下表包含 Amazon Redshift Serverless 事件，以及其他中繼資料：

Amazon Redshift 類別	外部事件 ID	事件嚴重性	訊息描述
RateChange	REDSHIFT-SERVERLESS-EVENT-1001	INFO	工作群組基礎 RPU 變更已於 <UTC 時間> 成功完成。
RateChange	REDSHIFT-SERVERLESS-EVENT-1002	ERROR	工作群組基礎 RPU 變更無法於 <UTC 時間> 完成。
監控	REDSHIFT-SERVERLESS-EVENT-1003	INFO	Amazon Redshift 資料倉儲 <端點名稱> 上的軟體已於 <UTC 時間> 更新。
組態	REDSHIFT-SERVERLESS-EVENT-1011	ERROR	Amazon Redshift Serverless 無法建立工作群組 [工作群組名稱]，因為無法存取此操作所需的服務連結角色 (SLR)。請嘗試在 Amazon Redshift 主控台上再次建立。Amazon Redshift 會自動建立 SLR。
監控	紅移-無服務器事件 -1029	ERROR	工作群組基礎 RPU 變更無法在 [UTC 時間] 完成，因為它沒有足夠的可用磁碟空間。請使用不同的組態再試一次。

Amazon Redshift 類別	外部事件 ID	事件嚴重性	訊息描述
監控	REDSHIFT-SERVERLESS-EVENT-1500	ERROR	無法建立或更新工作群組 <工作群組名稱>，因為您已超過帳戶的彈性 IP 地址限制。使用 Amazon EC2 刪除未使用的彈性 IP 地址或請求提高限制。
監控	REDSHIFT-SERVERLESS-EVENT-1501	ERROR	子網路 <子網路 ID> 沒有可用的 IP 地址。這會讓下列查詢類型無法在工作群組 <工作群組名稱> 上成功執行：EMR、聯合查詢、從 Amazon EC2 進行的 COPY/UNLOAD。若要修正此問題，請刪除 ENI 以在子網路中釋放 IP。

Amazon Redshift 類別	外部事件 ID	事件嚴重性	訊息描述
監控	REDSHIFT-SERVERLESS-EVENT-1502	ERROR	子網路 <子網路 ID> 沒有可用的 IP 地址。這會讓 Amazon EMR、Redshift 聯合查詢、Redshift COPY/UNLOAD、Redshift ML 查詢類型無法在工作群組 <工作群組名稱> 上成功執行。若要修正此問題，請刪除未使用的彈性網路界面 (ENI) 以在子網路中釋放 IP。
管理	REDSHIFT-SERVERLESS-EVENT-1008	INFO	您的 Amazon Redshift 工作群組 <工作群組名稱> 已建立並可供使用。
管理	REDSHIFT-SERVERLESS-EVENT-1009	INFO	您的 Amazon Redshift 工作群組 <工作群組名稱> 已於 <UTC 時間> 刪除。
監控	REDSHIFT-SERVERLESS-EVENT-1000	INFO	快照 <快照名稱> 已於 <UTC 時間> 成功完成。
管理	REDSHIFT-SERVERLESS-EVENT-1004	INFO	已於 <UTC 時間> 成功完成從命名空間 <命名空間名稱> 上的快照還原。

Amazon Redshift 類別	外部事件 ID	事件嚴重性	訊息描述
管理	REDSHIFT-SERVERLESS-EVENT-1005	ERROR	從命名空間 <命名空間名稱> 上的快照還原的操作已於 <UTC 時間> 失敗。
管理	REDSHIFT-SERVERLESS-EVENT-1006	INFO	已於 <UTC 時間> 成功完成從命名空間 <命名空間名稱> 上的復原點還原。
管理	REDSHIFT-SERVERLESS-EVENT-1007	INFO	從命名空間 <命名空間名稱> 上的復原點還原的操作已於 <UTC 時間> 失敗。
安全	REDSHIFT-SERVERLESS-EVENT-1012	ERROR	<namespace name>Amazon Redshift 無法存取您的命名空間 <namespace name> 的秘密。
安全	REDSHIFT-SERVERLESS-EVENT-1013	ERROR	Amazon Redshift 無法存取用來加密命名空間<namespace name>之管理員登入資料秘密的 KMS 金鑰。
安全	REDSHIFT-SERVERLESS-EVENT-1014	ERROR	Amazon Redshift 無法輪換命名空間<namespace name>的秘密，因為工作群組正在進行操作。

Amazon Redshift 類別	外部事件 ID	事件嚴重性	訊息描述
安全	REDSHIFT-SERVERLESS-EVENT-1015	ERROR	您的命名空間<namespace name>沒有附加工作群組。Amazon Redshift 只能輪換已連接工作群組之命名空間的秘密。
安全	REDSHIFT-SERVERLESS-EVENT-1016	INFO	針對您的命名空間<namespace name>在<time in UTC>更新的管理員憑證。

透過 Amazon 進行零 ETL 整合事件通知 EventBridge

Zero-ETL 整合使用 Amazon EventBridge 來管理事件通知，讓您掌握整合中 up-to-date 的變更。Amazon EventBridge 是一種無伺服器事件匯流排服務，可用來連接應用程式與來自各種來源的資料。在這種情況下，事件來源是 Amazon Redshift。事件 (受監控環境中的變更) 會自動 EventBridge 從 Amazon Redshift 資料倉儲傳送到這些事件。系統會以接近即時的速度傳送事件。

EventBridge 提供您撰寫事件規則的環境，此環境可指定要針對特定事件採取的動作。您也可以設定目標，這些目標是 EventBridge 可以將事件傳送至的資源。目標可以包括 API 目的地、Amazon CloudWatch 日誌群組和其他目標。如需有關規則的詳細資訊，請參閱 [Amazon EventBridge 規則](#)。如需有關目標的詳細資訊，請參閱 [Amazon EventBridge 目標](#)。

事件可以分為嚴重性和類別兩種。可用的篩選條件如下：

- 資源篩選 — 根據事件所關聯的資源來接收訊息。資源包括工作群組或快照。
- 時段篩選 — 將範圍限定在特定時段內的事件。
- 類別篩選 — 接收指定類別中所有事件的事件通知。

下表包含零 ETL 整合事件，以及其他中繼資料：

Amazon Redshift 類別	外部事件 ID	事件嚴重性	訊息描述
監控	REDSHIFT-INTEGRATION-EVENT-0000	INFO	零 ETL 整合 <整合名稱> 已建立，現在處於 ACTIVE 狀態。
監控	REDSHIFT-INTEGRATION-EVENT-0001	INFO	零 ETL 整合 <整合名稱> 已於 <UTC 時間> 刪除。
監控	REDSHIFT-INTEGRATION-EVENT-0002	INFO	已於 <UTC 時間> 起始零 ETL 整合 <整合名稱> 的刪除。
監控	REDSHIFT-INTEGRATION-EVENT-0003	INFO	零 ETL 整合 <整合名稱> 正在將交易資料同步到目標資料倉儲。
監控	REDSHIFT-INTEGRATION-EVENT-0004	WARNING	一或多個資料表沒有主索引鍵，無法同步。在 Amazon RDS 上進行備份、刪除這些表格，然後按照 Amazon Redshift 設計資料表的最佳實務重新建立這些資料表。
監控	REDSHIFT-INTEGRATION-EVENT-0005	WARNING	一或多個資料表無法同步，因為它們包含不受支援的資料類型或長度。請修正資料表，然後重試。如不需支援的資料類型，

Amazon Redshift 類別	外部事件 ID	事件嚴重性	訊息描述
			請參閱 不支援的資料類型 。
監控	REDSHIFT-INTEGRATION-EVENT-0006	ERROR	無法建立整合。請刪除並重新建立整合。
監控	REDSHIFT-INTEGRATION-EVENT-0007	ERROR	由於內部失敗而無法載入資料。請刪除並重新建立整合。
監控	REDSHIFT-INTEGRATION-EVENT-0008	ERROR	授權失敗，因為來源 Aurora DB 叢集資料庫叢集的權限已撤銷。請刪除並重新建立整合。
監控	REDSHIFT-INTEGRATION-EVENT-0009	ERROR	無法將資料傳送至 Amazon Redshift，因為資料表和結構描述的數目超過 Amazon Redshift 的限制。請刪除並重新建立整合。
監控	REDSHIFT-INTEGRATION-EVENT-0012	ERROR	已在目的地無伺服器命名空間上叫用從復原點還原。請刪除並重新建立整合。
監控	REDSHIFT-INTEGRATION-EVENT-0013	INFO	零 ETL 整合 <整合名稱> 現在處於 ACTIVE 狀態。

Amazon Redshift 類別	外部事件 ID	事件嚴重性	訊息描述
監控	REDSHIFT-INTEGRATION-EVENT-0014	ERROR	整合 <整合名稱> 失敗，因為有內部錯誤而無法加以修改。請刪除並重新建立整合。如果錯誤仍然存在，請聯絡 Sup AWS port 部門。
作業	REDSHIFT-INTEGRATION-EVENT-0015	INFO	DDL 變更 <DDL 變更> 已套用至資料表 <schema.name>。
作業	REDSHIFT-INTEGRATION-EVENT-0016	INFO	您的零 ETL 整合 <整合名稱> 正在使用下列引數處理修改請求：<請求引數的複本>。
作業	REDSHIFT-INTEGRATION-EVENT-0017	INFO	已套用您對零 ETL 整合 <整合名稱> 的修改。
作業	REDSHIFT-INTEGRATION-EVENT-0018	WARNING	目標 Amazon Redshift 叢集正在暫停。等待叢集暫停，然後讓其繼續執行，以繼續串流資料。
作業	REDSHIFT-INTEGRATION-EVENT-0019	WARNING	目標 Amazon Redshift 叢集正在暫停。繼續叢集以繼續串流資料。

Amazon Redshift 類別	外部事件 ID	事件嚴重性	訊息描述
作業	REDSHIFT-INTEGRATION-EVENT-0020	WARNING	目標 Amazon Redshift 叢集正在繼續。等待叢集處於作用中狀態，以繼續串流資料。
組態	REDSHIFT-INTEGRATION-EVENT-1000	ERROR	來源 Aurora 資料庫叢集資料庫叢集上的一或多個參數設定錯誤。請修正參數群組，並重新啟動叢集以套用變更，然後重新建立整合。
組態	REDSHIFT-INTEGRATION-EVENT-1001	ERROR	整合失敗，因為 <code>enable_case_sensitive_identifier</code> 參數的值不正確。將來源 Aurora 資料庫叢集資料庫叢集的值設為 <code>true</code> ，然後刪除並重新建立整合。
組態	REDSHIFT-INTEGRATION-EVENT-1002	ERROR	整合失敗，因為 <code>cdc_insert_enabled</code> 參數的值不正確。將來源 Aurora 資料庫叢集資料庫叢集的值設為 <code>true</code> ，然後刪除並重新建立整合。

Amazon Redshift 類別	外部事件 ID	事件嚴重性	訊息描述
組態	REDSHIFT-INTEGRATION-EVENT-1003	ERROR	來源資料庫叢集參數群組中的 <code>binlog_format</code> 參數必須設定為 <code>ROW</code> 。請修正參數群組，並重新啟動叢集以套用變更，然後重新建立整合。
組態	REDSHIFT-INTEGRATION-EVENT-1004	ERROR	無法載入資料，因為已啟用 <code>binlog_transaction_compression</code> 叢集參數。將參數值設定為 <code>OFF</code> ，並重新啟動寫入器執行個體以套用變更，然後重新建立整合。
組態	REDSHIFT-INTEGRATION-EVENT-1005	ERROR	無法載入資料，因為 <code>binlog_row_value_options</code> 叢集參數設定為不支援的 <code>PARTIAL_JSON</code> 。請修正參數群組，並重新啟動寫入器執行個體以套用變更，然後重新建立整合。
組態	REDSHIFT-INTEGRATION-EVENT-1006	WARNING	無法剖析整合篩選條件。請修正篩選條件語法。

Amazon Redshift 中的配額和限制

Amazon Redshift 的配額限制了您 AWS 帳戶中每個 AWS 區域中多個資源的使用情況。每個配額都有預設值，而且有些配額可以調整。對於可調配額，您可以透過提交 [Amazon Redshift 限制增加表單](#) 來 [申請增加](#) 某個 AWS 區域中的 AWS 帳戶。

Amazon Redshift 物件的配額

Amazon Redshift 的配額會限制數種物件類型的使用。每個類型都有預設值。

配額名稱	AWS 預設值	可調整	描述
AWS 您可以授權還原每個快照的快照的帳戶	20	否	每個快照可授權還原快照的 AWS 帳戶數目上限。
AWS 您可以授權還原快照的帳戶 AWS KMS key	100	否	每個 KMS 金鑰可授權還原快照的 AWS 帳戶數目上限。換言之，如果您有 10 個以單一 KMS 金鑰加密的快照，那麼您可以授權 10 個 AWS 帳戶還原每個快照，或者是合計最多 100 個帳戶、每個快照不超過 20 個帳戶的其他組合。
適用於 Amazon Redshift 的叢集 IAM 角色，以存取其他 AWS 服務	50 ¹	否	您可以與叢集建立關聯的 IAM 角色數目上限，以授權 Amazon Redshift 存取擁有叢集和 IAM 角色的使用者的其他 AWS 服務。 ¹ 在下列各項中，配額為 10 AWS 區域：us-iso-east-1、us-iso-west-1、us-isob-east-1。
所有使用者定義手動 WLM 佇列的並行層級 (查詢槽)	50	否	手動工作負載管理定義之所有使用者定義佇列的查詢槽上限。

配額名稱	AWS 預設值	可調整	描述
並行擴展叢集	10	是	並行擴展叢集的數目上限。
叢集中的 DC2 節點	128	是	您可以配置給叢集的 DC2 節點數目上限。如需每個節點類型之節點限制的相關資訊，請參閱 Amazon Redshift 中的叢集和節點 。
事件訂閱	20	是	目前 AWS 區域中此帳戶的活動訂閱數目上限。
節點	200	是	目前 AWS 區域中此帳戶所有資料庫執行個體的節點數目上限。
參數群組	20	否	目前「AWS 區域」中此帳戶的參數群組數目上限。
叢集中的 RA3 節點	128	是	您可以配置給叢集的 RA3 節點數目上限。如需每個節點類型之節點限制的相關資訊，請參閱 Amazon Redshift 中的叢集和節點 。
已連線至叢集的 RedShift 受管 VPC 端點	30	是	您可以連線至叢集的 RedShift 受管 VPC 端點數目上限。如需 RedShift 受管 VPC 端點的相關資訊，請參閱 使用 Redshift 管理的 VPC 端點 。
透過 RedShift 受管 VPC 端點存取之叢集的被授予者	5	是	叢集擁有者可授權其為叢集建立 RedShift 受管 VPC 端點的被授予者數目上限。如需 RedShift 受管 VPC 端點的相關資訊，請參閱 使用 Redshift 管理的 VPC 端點 。
每個授權的 RedShift 受管 VPC 端點數目	5	是	每個授權可建立的 RedShift 受管 VPC 端點數目上限。如需 RedShift 受管 VPC 端點的相關資訊，請參閱 使用 Redshift 管理的 VPC 端點 。

配額名稱	AWS 預設值	可調整	描述
預留節點	200	是	目前 AWS 區域中此帳戶的預留節點數目上限。
各叢集中每個資料庫中的結構描述	9,900	否	各叢集中可在每個資料庫中建立的結構描述數目上限。然而，pg_temp_* 結構描述不會計入此配額。
安全群組	20	是	目前 AWS 區域中此帳戶的安全性群組數目上限。
使用 COPY 載入時的單一資料列大小	4	否	使用 COPY 命令載入時的單一資料列大小上限 (單位 MB)。
快照	700	是	目前 AWS 區域中此帳戶的使用者快照數目上限。
子網路群組	20	是	目前 AWS 區域中此帳戶的子網路群組數目上限。
子網路群組中的子網路	20	是	子網路群組的子網路數目上限。
large 叢集節點類型的資料表	9,900	否	大型叢集節點類型的資料表數量上限。此限制包括永久資料表、暫存資料表、資料共用資料表和具體化視觀表。外部資料表會計為暫存資料表。暫存資料表包括使用者定義的暫存資料表，以及 Amazon Redshift 在查詢處理或系統維護期間建立的暫存資料表。檢視和系統暫存資料表不包含在此限制中。
xlarge 叢集節點類型的資料表	9,900	否	xlarge 叢集節點類型的資料表數目上限。此限制包括永久資料表、暫存資料表、資料共用資料表和具體化視觀表。外部資料表會計為暫存資料表。暫存資料表包括使用者定義的暫存資料表，以及 Amazon Redshift 在查詢處理或系統維護期間建立的暫存資料表。檢視和系統暫存資料表不包含在此限制中。

配額名稱	AWS 預設值	可調整	描述
具有單節點叢集之 x1plus 叢集節點類型的資料表。	9,900	否	具有單節點叢集之 x1plus 叢集節點類型的資料表數目上限。此限制包括永久資料表、暫存資料表、資料共用資料表和具體化視觀表。外部資料表會計為暫存資料表。暫存資料表包括使用者定義的暫存資料表，以及 Amazon Redshift 在查詢處理或系統維護期間建立的暫存資料表。檢視和系統暫存資料表不包含在此限制中。
具有多節點叢集之 x1plus 叢集節點類型的資料表。	20,000	否	具有多節點叢集之 x1plus 叢集節點類型的資料表數目上限。此限制包括永久資料表、暫存資料表、資料共用資料表和具體化視觀表。外部資料表會計為暫存資料表。暫存資料表包括使用者定義的暫存資料表，以及 Amazon Redshift 在查詢處理或系統維護期間建立的暫存資料表。檢視和系統暫存資料表不包含在此限制中。
4xlarge 叢集節點類型的資料表	200,000	否	4xlarge 叢集節點類型的資料表數目上限。此限制包括永久資料表、暫存資料表、資料共用資料表和具體化視觀表。外部資料表會計為暫存資料表。暫存資料表包括使用者定義的暫存資料表，以及 Amazon Redshift 在查詢處理或系統維護期間建立的暫存資料表。檢視和系統暫存資料表不包含在此限制中。
8xlarge 叢集節點類型的資料表	200,000	否	8xlarge 叢集節點類型的資料表數目上限。此限制包括永久資料表、暫存資料表、資料共用資料表和具體化視觀表。外部資料表會計為暫存資料表。暫存資料表包括使用者定義的暫存資料表，以及 Amazon Redshift 在查詢處理或系統維護期間建立的暫存資料表。檢視和系統暫存資料表不包含在此限制中。
16xlarge 叢集節點類型的資料表	200,000	否	16xlarge 叢集節點類型的資料表數目上限。此限制包括永久資料表、暫存資料表、資料共用資料表和具體化視觀表。外部資料表會計為暫存資料表。暫存資料表包括使用者定義的暫存資料表，以及 Amazon Redshift 在查詢處理或系統維護期間建立的暫存資料表。檢視和系統暫存資料表不包含在此限制中。

配額名稱	AWS 預設值	可調整	描述
資料庫數目	60	否	Amazon Redshift 叢集中允許的資料庫計數上限。這會排除從資料共用建立的資料庫。
閒置或非作用中工作階段的逾時	4 小時	否	此設定適用於叢集。如需有關為使用者設定閒置工作階段逾時值的資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的 ALTER USER 。使用者設定的優先順序高於叢集設定。
閒置交易的逾時	6 小時	否	開啟中交易的非作用中期間上限，超過之後，Amazon Redshift 就會結束與交易相關聯的工作階段。此設定的優先順序高於任何使用者定義的閒置逾時設定。其適用於叢集。
資料庫中的預存程序	10,000	否	預存程序的數目上限。若要了解更多限制，請參閱 預存程序支援的限制和差異 。
RA3 節點的連線數上限	2,000	否	RA3 叢集的連線數目上限。(這特別適用於 ra3.xlplus、ra3.4xlarge 和 ra3.16xlarge 節點類型。) 允許的連線數目上限會隨節點類型而異。
DC2 節點的最大連線數	各有不同	否	與 dc2. 大型叢集的連線數目上限為 500 個。一個 DC2.8 大型叢集的收集數目上限是 2000。
叢集中的 Amazon Redshift 角色數目	1,000	是	您可以為每個叢集建立的 Amazon Redshift 角色數目上限。如需角色型存取控制 (RBAC) 角色的相關資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的 角色型存取控制 (RBAC) 。

Amazon Redshift Serverless 物件的配額

Amazon Redshift 的配額會限制 Amazon Redshift Serverless 執行個體中數個物件類型的使用。每個類型都有預設值。

配額名稱	AWS 預設值	可調整	描述
資料庫數目	100	否	Amazon Redshift Serverless 命名空間中允許的資料庫計數上限。這會排除從資料共用建立的資料庫。
結構描述數目	9,900	否	Amazon Redshift Serverless 執行個體中允許的結構描述計數上限。
資料表數目	200,000	否	Amazon Redshift Serverless 執行個體中允許的資料表計數上限。
閒置或非作用中工作階段的逾時	1 小時	否	如需有關為使用者設定閒置工作階段逾時值的資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的 ALTER USER 。會優先採用使用者設定。
執行中查詢的逾時	86,399 秒 (24 小時)	否	執行中的查詢在遭到 Amazon Redshift 結束前的執行時間上限。
閒置交易的逾時	6 小時	否	開啟中交易的非作用中期間上限，超過之後，Amazon Redshift Serverless 就會結束與交易相關聯的工作階段。此設定的優先順序高於任何使用者定義的閒置逾時設定。
連線數目上限	2000	否	允許連線至工作群組的連線數目上限。
工作群組數目	25	是	支援的工作群組數目。
命名空間數目	25	是	支援的命名空間數目。
工作群組中的 Amazon Redshift 角色數目	1,000	是	您可以為每個工作群組建立的 Amazon Redshift 角色數目上限。如需角色型存取控制 (RBAC) 角色的相關資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的 角色型存取控制 (RBAC) 。

如需 Amazon Redshift Serverless 計費如何受逾時組態影響的相關資訊，請參閱 [Amazon Redshift Serverless 的帳單](#)。

Amazon Redshift Data API 的配額

Amazon Redshift 的配額限制了 Redshift Data API 的使用。每個類型都有預設值。如需 Amazon Redshift Data API 的詳細資訊，請參閱 [使用 Amazon Redshift 資料 API](#)。

配額名稱	AWS 預設值	可調整	描述
BatchExecuteStatement API 每秒交易數 (TPS)	20	否	您每秒可以提出而不受限制的操作請求數量上限。
CancelStatement API 每秒交易數 (TPS)	3	否	您每秒可以提出而不受限制的操作請求數量上限。
DescribeStatement API 每秒交易數 (TPS)	100	否	您每秒可以提出而不受限制的操作請求數量上限。
DescribeTable API 每秒交易數 (TPS)	3	否	您每秒可以提出而不受限制的操作請求數量上限。
ExecuteStatement API 每秒交易數 (TPS)	30	否	您每秒可以提出而不受限制的操作請求數量上限。

配額名稱	AWS 預設值	可調整	描述
GetStatementResult API 每秒交易數 (TPS)	20	否	您每秒可以提出而不受限制的操作請求數量上限。
ListDatabases API 每秒交易數 (TPS)	3	否	您每秒可以提出而不受限制的操作請求數量上限。
ListSchemas API 每秒交易數 (TPS)	3	否	您每秒可以提出而不受限制的操作請求數量上限。
ListStatements API 每秒交易數 (TPS)	3	否	您每秒可以提出而不受限制的操作請求數量上限。
ListTables API 每秒交易數 (TPS)	3	否	您每秒可以提出而不受限制的操作請求數量上限。

查詢編輯器 v2 物件的配額

Amazon Redshift 的配額會限制 Amazon Redshift 查詢編輯器 v2 中數個物件類型的使用。每個類型都有預設值。

配額名稱	AWS 預設值	可調整	描述
連線	500	是	目前區域中，您可以在此帳戶中使用查詢編輯器 v2 建立的連線數目上限。
每個帳戶的作用中主體	50	是	目前「區域」中可在此帳戶中使用查詢編輯器 v2 的同時主參與者的最大數目。
已儲存的查詢	2,500	是	目前區域中，您可以在此帳戶中使用查詢編輯器 v2 建立的已儲存查詢數目上限。
查詢版本	20	是	目前區域中，您可以在此帳戶中使用查詢編輯器 v2 為每一查詢建立的版本數目上限。
已儲存的圖表	500	是	目前區域中，您可以在此帳戶中使用查詢編輯器 v2 建立的已儲存圖表數目上限。
每一查詢擷取的資料列數目	100,000	否	目前區域中，可在此帳戶中由查詢編輯器 v2 為每一查詢擷取的資料列數目上限。
每一查詢擷取的資料大小	5	否	目前區域中，可在此帳戶中由查詢編輯器 v2 為每一查詢擷取的資料大小上限 (以 MB 為單位)。
每一主體的同時通訊端連線數目	10	是	單一主體可在目前區域中建立的查詢編輯器 v2 同時通訊端連線數目上限。如果您收到錯誤，內容指出通訊端連線超過限制，請評估是否要提高此配額。
每一帳戶的同時通訊端連線數目	250	是	帳戶中的所有主體可在目前區域中建立的查詢編輯器 v2 同時通訊端連線數目上限。如果您收到錯誤，內容指出通訊端連線超過限制，請評估是否要提高此配額。
並行連線數目上限	3	否	每一使用者的資料庫連線數目上限 (包括隔離的工作階段)。此值可由查詢編輯器 v2 管理員在帳戶設定中設定為 1–10。如果達到管理員所設的限制，請考慮在執行 SQL 時使用共用工作階段而非隔離的工作階段。如需連

配額名稱	AWS 預設值	可調整	描述
			線的相關資訊，請參閱 開啟查詢編輯器 v2 。如需設定限制的相關資訊，請參閱 變更帳戶設定 。

Amazon Redshift Spectrum 物件的配額和限制

Amazon Redshift Spectrum 具有以下配額和限制：

- 使用時，每個 AWS 帳戶的資料庫數目上限 AWS Glue Data Catalog。如需此值，請參閱《Amazon Web Services 一般參考》中的 [AWS Glue 服務配額](#)。
- 使用 AWS Glue Data Catalog 時，每個資料庫的資料表數目上限。如需此值，請參閱《Amazon Web Services 一般參考》中的 [AWS Glue 服務配額](#)。
- 使用 AWS Glue Data Catalog 時，每個資料保的分割區數目上限。如需此值，請參閱《Amazon Web Services 一般參考》中的 [AWS Glue 服務配額](#)。
- 使用時，每個 AWS 帳戶的分割區數目上限 AWS Glue Data Catalog。如需此值，請參閱《Amazon Web Services 一般參考》中的 [AWS Glue 服務配額](#)。
- 使用時外部資料表的最大資料行數目，啟用虛擬資料行時為 1,597 個 AWS Glue Data Catalog，未啟用虛擬資料行時的資料行數目上限為 1,600。
- 使用時，ION 或 JSON 文件中的字符串值的最大大小 AWS Glue Data Catalog 為 16 KB。如果達到此限制，則可以截斷字串。
- 您可以使用單一 ALTER TABLE 陳述式新增最多 100 個分割區。
- 所有 S3 資料必須位於與 Amazon Redshift 叢集相同的 AWS 區域。
- ION 和 JSON 中的時間戳記必須使用 [ISO8601](#) 格式。
- 不支援 ORC 檔案的外部壓縮。
- Text、OpenCSV 和 Regex SERDE 不支援大於 '\177' 的八進位分隔符號。
- 您可以在分割欄指定述詞，以避免讀取所有分割區。

例如，下列述詞會篩選資料欄 ship_dtm，但不會將篩選條件套用至分割區資料欄 ship_yyyymm：

```
WHERE ship_dtm > '2018-04-01'.
```

若要略過不需要的分割區，您需要新增述詞 WHERE ship_yyyymm = '201804'。此述詞會將讀取操作限於分割區 \ship_yyyymm=201804\。

這些限制不適用於 Apache Hive 中繼存放區。

命名限制條件

下表說明 Amazon Redshift 中的命名限制。

叢集識別碼	<ul style="list-style-type: none">叢集識別碼必須僅包含小寫字母。他們必須包含 1–63 個英數字元或連字號。第一個字元必須是字母。不能以一個連字號結尾或是連續包含兩個連字號。它在 AWS 帳戶的所有叢集中必須是唯一的。
資料庫名稱	<ul style="list-style-type: none">資料庫名稱必須包含 1–64 個英數字元。它只能包含小寫字母。它不能是保留字。如需保留字清單，請參閱《Amazon Redshift 資料庫開發人員指南》中的保留字。
RedShift 受管 VPC 端點的端點名稱	<ul style="list-style-type: none">端點名稱必須包含 1–30 個字元。有效字元為 A-Z、a-z、0-9 和連字號 (-)。第一個字元必須是字母。名稱不能包含兩個連續連字號或以連字號結尾。
管理員使用者名稱	<ul style="list-style-type: none">管理員使用者名稱必須僅包含小寫字母。其必須包含 1–128 個英數字元。第一個字元必須是字母。

	<ul style="list-style-type: none">• 它不能是保留字。如需保留字清單，請參閱《Amazon Redshift 資料庫開發人員指南》中的保留字。
管理員密碼	<ul style="list-style-type: none">• 管理員密碼必須包含 8–64 個字元。• 必須包含至少一個大寫字母。• 必須包含至少一個小寫字母。• 它必須包含一個數字。• <p>它可以使用的任何 ASCII 字元 (ASCII 碼 33–126)，但 ' (單引號)、" (雙引號)、\、/ 或 @ 除外。</p>
參數群組名稱	<ul style="list-style-type: none">• 參數群組名稱必須包含 1–255 個英數字元或連字號。• 它只能包含小寫字元。• 第一個字元必須是字母。• 不能以一個連字號結尾或是連續包含兩個連字號。
叢集安全群組名稱	<ul style="list-style-type: none">• 叢集安全群組名稱必須包含 255 個以內的英數字元或連字號。• 它只能包含小寫字元。• 它不得為 Default。• 對於您的 AWS 帳戶所建立的所有安全性群組，它必須是唯一的。

子網路群組名稱

- 子網路安全群組名稱必須包含 255 個以內的英數字元或連字號。
- 它只能包含小寫字元。
- 它不得為 **Default**。
- 對於您的 AWS 帳戶所建立的所有子網路群組，它必須是唯一的。

叢集快照識別碼

- 叢集快照識別碼必須包含 255 個以內的英數字元或連字號。
- 它只能包含小寫字元。
- 它不得為 **Default**。
- 對於您的 AWS 帳戶所建立的所有快照識別碼，其必須是唯一的。

在 Amazon Redshift 中標記資源

主題

- [標記概觀](#)
- [使用主控台管理資源標籤](#)
- [使用 Amazon Redshift API 來管理標籤](#)

標記概觀

在中 AWS，標籤是由鍵值配對組成的使用者定義標籤。Amazon Redshift 支援標記功能，以讓您一目了然地查看資源的中繼資料，並根據成本分配來對帳單報告進行分類。若要使用標籤進行成本分配，您必須先在 AWS Billing and Cost Management 服務中啟用這些標記。如需設定和使用標籤供計費使用的相關資訊，請參閱[將成本分配標籤用於自訂帳單報告](#)和[設定每月成本分配報告](#)。

在 Amazon Redshift 中的資源不須標籤，但它們可協助提供內容。您可能希望使用與成本中心、專案名稱和其他與資源之相關資訊的中繼資料來為資源加上標籤。例如，假設您想要追蹤哪些資源屬於測試環境和生產環境。您可以建立名為 `environment` 的索引鍵並提供值 `test` 或 `production` 來辨識每個環境中使用的資源。如果您在其他 AWS 服務中使用標記，或為您的業務使用標準類別，建議您在 Amazon Redshift 中為資源建立相同的鍵值對，以保持一致性。

在您重新調整叢集的大小後與在相同區域內復原叢集的快照後，系統會保留資源的標籤。然而，如果您將快照複製到另一個區域，系統就不會保留標籤，因此您必須在該新區域中重新建立標籤。如果您刪除資源，任何關聯的標籤也會遭到刪除。

每個資源皆有一個標籤集，此為指派給該資源之一或多個標籤的集合。每個資源每個標籤集最多可擁有 50 個標籤。在您建立資源時與資源建立後，您可以新增標籤。您可以將標籤新增至 Amazon Redshift 中的以下資源類型：

- CIDR/IP
- 叢集
- 叢集安全群組
- 叢集安全群組傳入規則
- Amazon EC2 安全群組
- 硬體安全模組 (HSM) 連線

- HSM 用戶端憑證
- 參數群組
- 快照
- 子網路群組

若要從 Amazon Redshift 主控台使用標記功能，使用者可以附加 AWS 受管政策 AmazonRedshiftFullAccess。如需可附加至 Amazon Redshift 主控台使用者、具有有限標記許可的 IAM 政策範例，請參閱[範例 7：允許使用者使用 Amazon Redshift 主控台標記資源](#)。如需有關標記的詳細資訊，請參閱[什麼是 AWS Resource Groups？](#)。

標記需求

標籤均擁有以下要求：

- 索引鍵字首不能是 aws:。
- 索引鍵在標籤集內必須是唯一的。
- 索引鍵必須介於 1 到 128 個允許的字元之間。
- 值必須介於 0 到 256 個允許的字元之間。
- 值在每個標籤集中不需要是唯一的。
- 索引鍵和值的允許字元為 Unicode 字母、數字、空格和下列任何符號：_ . : / = + - @。
- 金鑰和值會區分大小寫。

使用主控台管理資源標籤

管理 Amazon Redshift 資源上的標籤

1. 登入 AWS Management Console 並開啟 Amazon Redshift 主控台，網址為 <https://console.aws.amazon.com/redshiftv2/>。
2. 在導覽功能表上，選擇組態，然後選擇管理標籤。
3. 輸入您選擇的資源，並選擇要新增、修改或刪除的標籤。然後選擇 Manage tags of the resources that you chose (管理所選資源的標籤)。

您可標記的資源包括叢集、參數群組、子網路群組、HSM 用戶端憑證、HSM 連線和快照。

4. 在管理標籤導覽窗格上，選擇檢閱和套用標籤變更，然後選擇套用以儲存變更。

使用 Amazon Redshift API 來管理標籤

您可以使用下列 AWS CLI 操作來管理 Amazon Redshift 中的標籤。

- [create-tags](#)
- [delete-tags](#)
- [describe-tags](#)

您可以使用下列 Amazon Redshift API 操作來管理標籤：

- [CreateTags](#)
- [DeleteTags](#)
- [DescribeTags](#)
- [標籤](#)
- [TaggedResource](#)

此外，您也可以使用下列 Amazon Redshift API 操作來管理和檢視特定資源的標籤：

- [CreateCluster](#)
- [CreateClusterParameterGroup](#)
- [CreateClusterSecurityGroup](#)
- [CreateClusterSnapshot](#)
- [CreateClusterSubnetGroup](#)
- [CreateHsmClientCertificate](#)
- [CreateHsmConfiguration](#)
- [DescribeClusters](#)
- [DescribeClusterParameterGroups](#)
- [DescribeClusterSecurityGroups](#)
- [DescribeClusterSnapshots](#)
- [DescribeClusterSubnetGroups](#)
- [DescribeHsmClientCertificates](#)
- [DescribeHsmConfigurations](#)

適用於 Amazon Redshift 的叢集版本

Amazon Redshift 會定期發行叢集版本。您的 Amazon Redshift 叢集會在系統維護時段進行修補。修補程式的時間取決於您 AWS 區域 和維護時段的設定。您可以從 Amazon Redshift 檢視或變更維護時段設定。如需維護的相關資訊，請參閱[叢集維護](#)。

您可以在 Amazon Redshift 主控台上，於叢集詳細資訊的維護索引標籤上檢視您叢集的叢集版本。或者，您也可以從 SQL 命令的輸出中查看叢集版本：

```
SELECT version();
```

主題

- [Amazon Redshift 補丁 181](#)
- [Amazon Redshift 修補程式 180](#)
- [Amazon Redshift 修補程式 179](#)
- [Amazon Redshift 修補程式 178](#)
- [Amazon Redshift 修補程式 177](#)
- [Amazon Redshift 修補程式 176](#)
- [Amazon Redshift 修補程式 175](#)
- [Amazon Redshift 修補程式 174](#)
- [Amazon Redshift 修補程式 173](#)
- [Amazon Redshift 修補程式 172](#)
- [Amazon Redshift 修補程式 171](#)
- [Amazon Redshift 修補程式 170](#)
- [Amazon Redshift 修補程式 169](#)
- [Amazon Redshift 修補程式 168](#)

Amazon Redshift 補丁 181

此修補程式中的叢集版本：

- 1.0.69497 — Amazon Redshift 無伺服器版本 — 於 2024 年 6 月 18 日發行

- 1.0.69451 — 目前的曲目版本 — 於二零二四年六月十八日發行
- 1.0.69076 — Amazon Redshift 無伺服器版本 — 於 2024 年 6 月 14 日發行
- 1.0.69065 — 目前的曲目版本 — 於二零二四年六月十四日發行
- 1.0.68555 — Amazon Redshift 無伺服器版本 — 於 2024 年 5 月 31 日發行
- 1.0.68540 — 目前的曲目版本 — 於二零二四年五月三十一日發行
- 1.0.68328 — Amazon Redshift 無伺服器版本 — 於 2024 年 5 月 23 日發行
- 1.0.68205 — 目前的曲目版本 — 於二零二四年五月二十三日發佈
- 1.0.67796 — Amazon Redshift 無伺服器版本 — 於 2024 年 5 月 15 日發行
- 1.0.67788 — 目前的曲目版本 — 於二零二四年五月十五日發行
- 1.0.67308 — Amazon Redshift 無伺服器版本 — 於 2024 年 5 月 1 日發行
- 1.0.67305 — 目前的曲目版本 — 於二零二四年五月一日發佈

此修補程式中的新功能和改善

- 引入更改具體化視觀表的發佈索引鍵和排序索引鍵的支援。
- 引入了對「降低屬性名稱 ()」和「上限屬性名稱 ()」函數的支持，該函數修改了 SUPER 對象值的屬性名稱的大小寫。
- 修復了使用標識列時創建表類似的問題。之前，新資料表會繼承來源資料表的識別碼。如果來源資料表稍後遭到捨棄，這會造成問題，因為新資料表中的識別碼會變成無效。
- 修正了防止某些外部表格在 SVV_ALL_TABLE 中顯示的問題。
- 改善叢集啟動程序時間，並加快高並行工作負載的查詢初始化速度。
- 修正了將 split_part () 函數傳遞至同盟來源至 RDS 和 Aurora MySQL 時造成錯誤的聯合查詢問題
- 支援使用者透過 ALTER TABLE... 在佈建的並行擴展叢集和無伺服器自動調度資源運算上透過 ALTER TABLE KEY KEY DISTKEY 命令對發佈金鑰所做的變更。
- 支援手動重新整理的具體化視觀表，這些視觀表涉及已佈建並行擴展和無伺服器自動調度資源
- 添加對零 ETL 的支援，以處理大小最大 16 MB 的記錄，並支援高達 16 MB 的超級值。
- 透過提供結構描述和資料表名稱等其他詳細資料，從 Aurora MySQL 以零 ETL 進行初始同步期間增強錯誤訊息。
- 引入了對使用 Amazon Redshift ML 創建模型進行標記的支持。通過這項改進，您現在可以標記 Amazon Redshift ML 使用的亞馬遜 SageMaker 資源。標記可協助您管理、識別、組織、搜尋和篩選資源。
- 透過使用最佳化資料處理，改善涉及 Lambda 使用者定義函數 (UDF) 的查詢效能。AWS Lambda

- 在彈性調整大小和無伺服器叢集的排序表格中，減少資料擷取期間的記憶體使用率。
- 添加對視圖 SYS_QUERY_歷史記錄列中的換行符 (\n) 和 query_text 視圖 SYS_QUERY_TEXT 中的列的支持。text

Amazon Redshift 修補程式 180

此修補程式中的叢集版本：

- 1.0.68870 — 追蹤追蹤版本 — 於二零二四年六月三日發佈
- 1.0.68520 — 追蹤追蹤版本 — 於二零二四年五月二十八日發佈
- 1.0.67699 — 追蹤追蹤版本 — 於二零二四年五月十五日發佈
- 1.0.66960 — 追蹤追蹤版本 — 於二零二四年四月二十一日發佈
- 1.0.66954 — 目前的曲目版本 — 於二零二四年四月二十一日發行
- 1.0.66276 — 目前的曲目版本 — 於二零二四年四月十二日發佈
- 1.0.66290 — Amazon Redshift 無伺服器版本 — 於二零二四年四月十日發行
- 1.0.63590 — 目前曲目版本 — 於二零二四年二月十九日發佈
- 1.0.63567 — Amazon Redshift 無伺服器版本 — 於 2024 年 2 月 16 日發行
- 1.0.63282 — Amazon Redshift 無伺服器版本 — 於 2024 年 2 月 13 日發行
- 1.0.63269 — 目前的曲目版本 — 於二零二四年二月十三日發行
- 1.0.63215 — Amazon Redshift 無伺服器版本 — 於 2024 年 2 月 12 日發行
- 1.0.63205 — 目前的曲目版本 — 於二零二四年二月十二日發佈
- 1.0.63030 — Amazon Redshift 無伺服器版本 — 於 2024 年 2 月 7 日發行
- 1.0.62913 — 目前的曲目版本 — 於二零二四年二月七日發佈
- 1.0.62922 — Amazon Redshift 無伺服器版本 — 於 2024 年 2 月 5 日發行
- 1.0.62878 — 目前的曲目版本 — 於二零二四年二月五日發佈
- 1.0.62698 — Amazon Redshift 無伺服器版本 — 於 2024 年 1 月 31 日發行
- 1.0.62614 — 目前的曲目版本 — 於二零二四年一月三十一日發佈
- 1.0.61687 — Amazon Redshift Serverless 版本 — 於 2024 年 1 月 5 日發行
- 1.0.61678 — 目前的追蹤版本 — 於 2024 年 1 月 5 日發行
- 1.0.61567 — Amazon Redshift Serverless 版本 — 於 2023 年 12 月 31 日發行
- 1.0.61559 — 目前的追蹤版本 — 於 2023 年 12 月 31 日發行

- 1.0.61430 — Amazon Redshift Serverless 版本 — 於 2023 年 12 月 29 日發行
- 1.0.61395 — 目前的追蹤版本 — 於 2023 年 12 月 29 日發行

此修補程式中的新功能和改善

- 將 CURRENT_USER 變更為不再將傳回的使用者名稱截斷為 64 個字元。
- 新增在標準檢視和近期繫結視觀表上套用資料遮罩政策的功能。
- 新增會將動態資料遮罩 (DDM) 套用至 SUPER 資料類型資料欄中的純量屬性的功能。
- 新增 OBJECT_TRANSFORM SQL 函數。如需詳細資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的 [OBJECT_TRANSFORM 函數](#)。
- 新增將 AWS Lake Formation 精細存取控制套用至巢狀資料的功能，並使用 Amazon Redshift 資料湖分析進行查詢。
- 新增 INTERVAL 資料類型。
- 新增 CONTINUE_HANDLER，這是一種例外狀況處理常式，可控制預存程序的流程。若使用該處理常式，您就可以掌握和處理例外狀況，而不會結束現有的陳述式區塊。
- 除了個別物件外，還新增定義限定範圍 (結構描述或資料庫) 權限的功能。這可讓使用者和角色獲得限定範圍內所有目前和未來物件的權限。
- 新增從具有權限的資料共用建立資料庫的功能，讓取用者端管理員將共用資料庫物件的個別權限授予取用者端使用者和角色。
- 新增對來自遠端 BYOM 模型的 SUPER 傳回資料類型的支援。這將擴大接受的 SageMaker 模型範圍，以包括那些具有更複雜的返回格式。
- 將外部函數變更為現在隱含將含或不含小數部分的數字轉換為資料欄的數字資料類型。對於 int2、int4 和 int8 資料欄，除非數字超出範圍，否則具有小數位數的數字可以截斷至被接受。對於 float4 和 float8 資料欄，數字被接受，沒有小數位數。
- 加入與 H3 階層式空間索引格線系統搭配使用的三個空間函數：H3_FromLong 緯度、H3_ 和 H3_FromPoint_Polyfill。

Amazon Redshift 修補程式 179

此修補程式中的叢集版本：

- 1.0.62317 — Amazon Redshift 無伺服器版本 — 於 2024 年 1 月 29 日發行
- 1.0.62312 — 追蹤追蹤版本 — 於二零二四年一月二十九日發佈

- 1.0.61631 — Amazon Redshift Serverless 版本 — 於 2024 年 1 月 5 日發行
- 1.0.61626 — 目前的追蹤版本 — 於 2024 年 1 月 5 日發行
- 1.0.61191 — 目前的追蹤版本 — 於 2023 年 12 月 16 日發行
- 1.0.61150 — Amazon Redshift Serverless 版本 — 於 2023 年 12 月 16 日發行
- 1.0.60982 — Amazon Redshift Serverless 版本 — 於 2023 年 12 月 13 日發行
- 1.0.60854 — 目前的追蹤版本 — 於 2023 年 12 月 10 日發行
- 1.0.60354 — Amazon Redshift Serverless 版本 — 於 2023 年 11 月 22 日發行
- 1.0.60353 — 目前的追蹤版本 — 於 2023 年 11 月 21 日發行
- 1.0.60293 — Amazon Redshift Serverless 版本 — 於 2023 年 11 月 21 日發行
- 1.0.60292 — 目前的追蹤版本 — 於 2023 年 11 月 22 日發行
- 1.0.60161 — Amazon Redshift Serverless 版本 — 於 2023 年 11 月 18 日發行
- 1.0.60140 — 目前的追蹤版本 — 於 2023 年 11 月 18 日發行
- 1.0.60139 — Amazon Redshift Serverless 版本 — 於 2023 年 11 月 18 日發行
- 1.0.59947 — Amazon Redshift Serverless 版本 — 於 2023 年 11 月 16 日發行
- 1.0.59945 — 目前的追蹤版本 — 於 2023 年 11 月 16 日發行
- 1.0.59118 — Amazon Redshift Serverless 版本 — 於 2023 年 11 月 9 日發行
- 1.0.59117 — 目前的追蹤版本 — 於 2023 年 11 月 9 日發行

此修補程式中的新功能和改善

- 新增支援，讓具有適當權限的聯合使用者可以檢視資料列層級安全性和動態資料遮罩系統檢視，包括：
 - SVV_ATTACHED_MASKING_POLICY
 - SVV_MASKING_POLICY
 - SVV_RLS_ATTACHED_POLICY
 - SVV_RLS_POLICY
 - SVV_RLS_RELATION
- 新增功能，查詢只包含 FROM 子句中的純量函數，現在就會產生錯誤。新增功能，使得 FROM 子句中僅包含純量函數的查詢產生錯誤。
- 將具有永久目標資料表功能的 CREATE TABLE AS (CTAS) 陳述式新增至並行擴展叢集。並行擴展叢集目前支援更多查詢。

- 在 RA3 叢集上執行傳統調整大小後，新增下列系統資料表以追蹤資料表重新分佈狀態：
 - SYS_RESTORE_STATE 系統資料表會顯示資料表層級的重新分佈進度。
 - SYS_RESTORE_LOG 系統資料表會顯示資料重新分佈的歷史輸送量。
- 改善在 RA3 節點類型上執行傳統調整大小之後，EVEN 表上的配量偏斜最小化。這也適用於執行傳統調整大小的 178 個叢集的修補程式。
- 在並行擴展叢集上新增對具有 EXTENSION 的 UNLOAD 支援。
- 改善包含 UDF 的查詢 HashJoins 和 NestLoop 連接的效能。
- 提升 RA3 節點類型上彈性調整大小的效能。
- 提升資料共用查詢的效能。
- 提升在彈性調整大小的佈建叢集和無伺服器工作群組中手動起啟分析查詢的效能。
- 透過更好的工作負載管理資源預測功能，提升自動 WLM 查詢效能。
- 移除將叢集啟動到專用租用 VPC 的功能。此變更不會影響 VPC 中任何 EC2 執行個體的租用。您可以使用 `modify-vpc-tenancy` AWS CLI 命令將 VPC 的租用修改為預設值。
- 已佈建的並行擴展叢集和無伺服器自動擴展運算現在支援具體化視觀表手動重新整理。
- 將對 INTERVAL 逐字的支援新增到 EXTRACT 函數。例如，`EXTRACT('hours' from Interval '50 hours')` 傳回 2 因為 50 小時被解譯為 2 天和 2 小時，並擷取 2 的小時分量。

Amazon Redshift 修補程式 178

此修補程式中的叢集版本：

- 1.0.63327-目前的曲目版本 — 於二零二四年二月九日發佈
- 1.0.63313-追蹤追蹤版本 — 於二零二四年二月九日發佈
- 1.0.60977 — 隨後的追蹤版本 — 於 2023 年 12 月 15 日發行
- 1.0.59596 — 目前的追蹤版本 — 於 2023 年 11 月 9 日發行
- 1.0.58593 — Amazon Redshift Serverless 版本 — 已於 2023 年 10 月 23 日發行
- 1.0.58558 — 目前的追蹤版本 — 已於 2023 年 10 月 23 日發行
- 1.0.57864 — 目前的追蹤版本 — 已於 2023 年 10 月 12 日發行
- 1.0.57850 — Amazon Redshift Serverless 版本 — 已於 2023 年 10 月 12 日發行
- 1.0.56952 — 目前的追蹤版本 — 已於 2023 年 9 月 25 日發行
- 1.0.56970 — Amazon Redshift Serverless 版本 — 已於 2023 年 9 月 25 日發行

此修補程式中的新功能和改善

- Amazon Redshift 現已改善了資料共用查詢效能，所憑借的方法是在生產者執行個體上發生並行資料變更時，以更快的速度重新整理取用者執行個體上的中繼資料。
- 新增了相關支援，可在具體化視觀表的基本資料表參考共用的資料時，以自動和增量的方式重新整理 Amazon Redshift 資料共用取用者執行個體上的具體化視觀表。
- 新增了相關支援，可在 SUPER 資料類型中存放最多 16 MB 大小的大型物件。從 JSON、PARQUET、TEXT 和 CSV 來源檔案擷取時，您可以將半結構化資料或文件載入為 SUPER 資料類型的值，最多 16 MB。
- 新增了相關支援，可彈性地調整大小，以便擴展為單節點 Amazon Redshift RA3 叢集或從單節點 Amazon Redshift RA3 叢集進行擴展。
- 單節點 Amazon Redshift RA3 叢集現在可以受益於加密功能的增強，減少整體加密時間，並改善加密程序進行期間的資料倉儲可用性。
- 改善了將儲存在 SUPER 資料類型的資料解除巢狀化和取消樞紐時，對於查詢的支援。
- 改善了以 SUPER 資料類型重新整理具體化視觀表的效能。
- 新增了對於使用 ANY_VALUE 函數來彙總 INTERVAL 常值的支援。
- 串流擷取現在支援使用下列新的 SQL 命令清除串流資料：DELETE FROM streaming_materialized_views WHERE <where filter clause>。
- 視等式條件的結果而定，DECODE 函數會將特定值取代為另一個特定值或預設值。DECODE 現在需要以下三個參數：
 - expression
 - search
 - result
- 對預存程序新增功能，以允許補捉資料溢位資料類型轉換錯誤，並在例外狀況處理區塊內進行處理。
- 現在，如果您將 enable_case_sensitive_identifier 變更為與工作階段預設設定不同，則會在查詢資料列層級安全或動態資料遮罩保護的關係時收到錯誤。此外，當您在佈建叢集或無伺服器命名空間中套用資料列層級安全或動態資料遮罩政策時，下列組態會遭到封鎖：

```
ALTER USER <current_user> SET case-sensitive identifier.
```

- MERGE 命令現在支援只需要目標和來源資料表的簡化語法。如需詳細資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的 [MERGE](#)。
- 新增了相關支援，可將相同的動態資料遮罩政策附加到具有相同優先順序或不指定優先順序的多個使用者或角色。

- 您現在可以在透過 ALTER TABLE ADD COLUMN 新增新的資料欄時指定 COLLATION。
- 修正了會延遲對並行擴展叢集和 Amazon Redshift Serverless 強制執行 QMR 規則的問題。
- Amazon Redshift 聯合查詢已在 Amazon RDS for PostgreSQL 和 Amazon Aurora PostgreSQL 上擴大了對時區與時間戳記的下推支援。
- 您現在可以在聯合查詢中使用以數字開頭的 Amazon RDS for MySQL 和 Aurora MySQL 資料庫名稱。
- 新增 SYS_ANALYZE_HISTORY 檢視，其中包含 ANALYZE 操作的記錄詳細資訊。
- 新增 SYS_ANALYZE_COMPRESSION_HISTORY 檢視，其中包含 COPY 或 ANALYZE COMPRESSION 命令執行期間的壓縮分析操作記錄詳細資訊。
- 新增 SYS_SESSION_HISTORY 檢視，其中包含與作用中工作階段、歷史工作階段和重新啟動的工作階段相關的記錄詳細資訊。
- 新增 SYS_TRANSACTION_HISTORY 檢視，其中包含與交易層級分析相關的記錄詳細資訊，可提供遞交所花時間、遞交的 datasha 區塊數量和隔離層級。
- 新增 SVV_REDSHIFT_SCHEMA_QUOTA 檢視，其中包含與資料庫中每個結構描述之配額和目前的磁碟用量相關的記錄。
- 使用 SYS_PROCEDURE_CALL 檢視，其中包含與預存程序呼叫相關的記錄，包括開始時間、結束時間、預存程序呼叫的狀態，以及巢狀預存程序呼叫的呼叫階層。
- 新增 SYS_CROSS_REGION_DATASHARING_USAGE 檢視，其中包含與追蹤跨區域資料共用用量相關的記錄。
- 新增 SYS_PROCEDURE_MESSAGES 檢視，其中包含與關於所記錄預存程序訊息之追蹤資訊相關的記錄。
- 新增 SYS_UDF_LOG 檢視，其中包含與使用者定義函數的呼叫、錯誤、警告或追蹤 (如果適用) 的追蹤系統日誌訊息相關的記錄。
- 在 SYS_EXTERNAL_QUERY_DETAIL 中新增了新的資料欄 IS_RECURSIVE、IS_NESTED、S3LIST_TIME 和 GET_PARTITION_TIME。
- 新增 MaxRPU，這是適用於 Redshift Serverless 的新運算成本控制設定。若使用 MaxRPU，您可以選擇性地指定較高的運算閾值，以控制不同時間點的資料倉儲成本，方法是選取 Redshift Serverless 可以在每個工作群組調整的最大運算層級。
- 使用數值間隔字串更正 INTERVAL 常值的輸出。例如，指定為 INTERVAL '1' YEAR 的間隔現在會傳回 1 YEAR 而不是 "00:00:00。此外，INTERVAL 常值的輸出會截斷為指定的最小 INTERVAL 元件。例如，INTERVAL '1 day 1 hour 1 minute 1.123 seconds' HOUR TO MINUTE 會截斷至 1 day 01:01:00。

Amazon Redshift 修補程式 177

此修補程式中的叢集版本：

- 1.0.57922 — 隨後的追蹤版本 — 已於 2023 年 10 月 12 日發行
- 1.0.57799 — Amazon Redshift Serverless 版本 — 已於 2023 年 10 月 10 日發行
- 1.0.57798 — 目前的追蹤版本 — 已於 2023 年 10 月 10 日發行
- 1.0.57085 — 隨後的追蹤版本 — 已於 2023 年 9 月 26 日發行
- 1.0.56899 — Amazon Redshift Serverless 版本 — 已於 2023 年 9 月 21 日發行
- 1.0.56754 — 目前的追蹤版本 — 已於 2023 年 9 月 21 日發行
- 1.0.56242 — 目前的追蹤版本 — 已於 2023 年 9 月 11 日發行
- 1.0.55539 — Amazon Redshift Serverless 版本 — 已於 2023 年 8 月 28 日發行
- 1.0.55524 — 目前的追蹤版本 — 已於 2023 年 8 月 28 日發行
- 1.0.54899 — 目前的追蹤版本 — 已於 2023 年 8 月 15 日發行
- 1.0.54899 — 目前的追蹤版本 — 已於 2023 年 8 月 14 日發行
- 1.0.54899 — 目前的追蹤版本 — 已於 2023 年 8 月 15 日發行
- 1.0.54239 — 目前的追蹤版本 — 已於 2023 年 8 月 3 日發行
- 1.0.54321 — Amazon Redshift Serverless 版本 — 已於 2023 年 8 月 3 日發行

此修補程式中的新功能和改善

- 新增 SYS_MV_STATE 檢視，其中包含具體化視觀表每個狀態轉換的資料列。SYS_MV_STATE 可用於 Amazon Redshift Serverless 和 Amazon Redshift 佈建的執行個體的 MV 重新整理監控。
- 新增 SYS_USERLOG 檢視，其中會記錄 Create user、Drop user、Alter user (重新命名)、Alter user (更改屬性) 的資料庫使用者變更詳細資訊。
- 新增 SYS_COPY_REPLACEMENTS 檢視，其中會顯示一個日誌，日誌內記錄了搭配 ACCEPTINVCHARS 選項的 COPY 命令何時取代無效的 UTF-8 字元。
- 新增 SYS_SPATIAL_SIMPLIFY 檢視，其中包含使用 COPY 命令取得有關簡化空間幾何物件的資訊。
- 新增 SYS_VACUUM_HISTORY 檢視，可用來查看 VACUUM 操作的詳細資訊和結果。
- 新增 SYS_SCHEMA_QUOTA_VIOLATIONS 檢視，以記錄超過結構描述配額時的出現次數、時間戳記、XID 和其他有用的資訊。

- 新增 SYS_RESTORE_STATE 檢視，可用來在非同步傳統調整大小期間，監控叢集中每個資料表的重新分佈進度。
- 新增 SYS_EXTERNAL_QUERY_ERROR 檢視，其會傳回有關 Redshift Spectrum 掃描錯誤的資訊。
- 對 CREATE MODEL 命令新增了標籤參數，因此您現在可以使用自動駕駛訓練工作來追蹤訓練成本。
- 為 Amazon Redshift 叢集新增自訂網域名稱 (CNAME)。
- 新增 Apache Iceberg 的預覽支援，讓客戶能夠在 Amazon Redshift 內的 Apache Iceberg 資料表上執行分析查詢。
- 新增在工作負載管理 (WLM) 中搭配使用使用者角色與參數群組的支援。
- 添加對自動掛載的支援 AWS Glue Data Catalog，使客戶可以更輕鬆地在其資料湖中執行查詢。
- 新增一些功能，以便在使用不含 GROUP BY 子句的分組函數或在 WHERE 子句中使用分組操作時導致錯誤。
- 對預存程序新增功能，以允許補捉除以零錯誤，並在例外狀況處理區塊內進行處理。
- 修正當來源資料表是資料共用資料表時，查詢無法使用並行擴展以將資料寫入到資料表的錯誤。
- 將記錄在 enable_case_sensitive_identifier 的區分大小寫識別碼修正為現在可與 MERGE 陳述式搭配運作。
- 修正在函數 pg_get_late_binding_view_cols() 上的查詢偶爾會被忽略的錯誤。您現在可以隨時取消這類查詢。
- 改善在生產者上執行清空任務時，於取用者上執行的資料共用查詢的效能。
- 改善資料共用和並行擴展查詢的效能，尤其是生產者上的並行資料變更，或卸載至附加到取用者的並行擴展執行個體時。

Amazon Redshift 修補程式 176

此修補程式中的叢集版本：

- 1.0.56738 — 隨後的追蹤版本 — 已於 2023 年 9 月 21 日發行
- 1.0.55837 — 隨後的追蹤版本 — 已於 2023 年 9 月 11 日發行
- 1.0.54776 — 目前的追蹤版本 — 已於 2023 年 8 月 15 日發行
- 1.0.54052 — 目前的追蹤版本 — 已於 2023 年 7 月 26 日發行
- 1.0.53642 — Amazon Redshift Serverless 版本 — 已於 2023 年 7 月 20 日發行
- 1.0.53301 — 目前的追蹤版本 — 已於 2023 年 7 月 20 日發行

- 1.0.52943 — Amazon Redshift Serverless 版本 — 已於 2023 年 7 月 7 日發行
- 1.0.52931 — 目前的追蹤版本 — 已於 2023 年 7 月 7 日發行
- 1.0.52194 — Amazon Redshift Serverless 版本 — 已於 2023 年 6 月 21 日發行
- 1.0.51986 — 目前的追蹤版本 — 已於 2023 年 6 月 16 日發行
- 1.0.51594 — 目前的追蹤版本 — 已於 2023 年 6 月 9 日發行

此修補程式中的新功能和改善

- 改善為空白分組集寫入 GROUP BY () 時的錯誤處理。這之前會被忽略，現在則會傳回剖析器錯誤。
- 增強以增量方式重新整理有 SUPER 資料欄之具體化視觀表時的效能
- ALTER TABLE <target_tbl> APPEND FROM <streaming_mv> – (ATA) SQL 命令現在支援將所有記錄從做為來源的串流具體化視觀表 (MV) (除了以資料表做為來源外) 移動到目標資料表。串流 MV 上的 ATA 支援可讓使用者將串流 MV 中的所有記錄移至另一個資料表來管理資料成長，藉此快速清除串流 MV 中的所有記錄。
- TRUNCATE <streaming_mv> – SQL 命令現在支援截斷串流具體化視觀表 (MV) (除了資料表外) 中的所有記錄。TRUNCATE 會刪除串流 MV 中的所有記錄，同時讓串流 MV 的結構保持不變。在串流 MV 上執行 TRUNCATE 可讓客戶快速清除串流 MV 中的所有記錄，以管理資料成長。
- 在 SELECT 命令中新增了 QUALIFY 子句的功能。
- 透過與 Amazon Forecast 整合，Redshift 機器學習支援時間序列預測。
- AWS Glue Data Catalog 支援 auto 裝載以簡化資料湖的查詢，無需額外的步驟即可建立外部結構描述參考。
- 現已支援更改 RLS 政策。如需詳細資訊，請參閱文件中的 [ALTER RLS POLICY](#)。
- Lambda UDF 現在可在 CREATE FUNCTION 陳述式中支援 STABLE 函數波動參數。當 CREATE FUNCTION 陳述式中使用了 STABLE 參數，且使用相同引數多次呼叫 Lambda UDF 時，預期的 Lambda UDF 函數叫用次數會減少。[CREATE FUNCTION 參數](#)中有 STABLE 函數波動類別的更詳細解釋。
- 多個 Lambda UDF 效能改善。具體而言，已改善在查詢受資料列層級安全 (RLS) 政策保護的資料表時的記錄批次處理支援。
- 減少 Amazon Redshift RA3 叢集的整體加密時間，並改善加密期間資料倉儲的可用性。如需詳細資訊，請參閱 [Amazon Redshift 資料庫加密](#)。
- Redshift 中已新增新的系統檢視 SYS_MV_REFRESH_HISTORY。針對具體化視觀表的重新整理活動，SYS_MV_REFRESH_HISTORY 檢視會包含一個資料列。您可以使用 SYS_MV_REFRESH_HISTORY 檢查具體化視觀表的重新整理歷史記錄。所有使用者都可看見

SYS_MV_REFRESH_HISTORY。超級使用者可以看見所有資料列；一般使用者只能看見自己的資料。

系統檢視 SYS_QUERY_DETAIL 中已新增一個新的資料欄 SPILLED_BLOCK_LOCAL_DISK。新資料欄 SPILLED_BLOCK_LOCAL_DISK 可協助客戶判斷溢寫到本機磁碟的區塊。您可以使用 SYS_QUERY_DETAIL 來檢視步驟層級的查詢詳細資訊。所有使用者都可看見 SYS_QUERY_DETAIL。超級使用者可以看見所有資料列；一般使用者只能看見它們有權存取的中繼資料。

- 佈建的 Amazon Redshift Serverless 和 Amazon Redshift 中已新增新的系統檢視 SYS_QUERY_TEXT。SYS_QUERY_TEXT 檢視類似於佈建叢集的 [SVL_STATEMENTTEXT](#)。使用 SYS_QUERY_TEXT 檢視中的 sequence 資料欄可取得完整的 SQL 陳述式文字。

Amazon Redshift 修補程式 175

此修補程式中的叢集版本：

- 1.0.53064 — 目前的追蹤版本 — 已於 2023 年 7 月 7 日發行
- 1.0.51973 — 目前的追蹤版本 — 已於 2023 年 6 月 16 日發行
- 1.0.51781 — 目前的追蹤版本 — 已於 2023 年 6 月 10 日發行
- 1.0.51314 — Amazon Redshift Serverless 版本 — 已於 2023 年 6 月 3 日發行
- 1.0.51304 — 目前的追蹤版本 — 已於 2023 年 6 月 2 日發行
- 1.0.50708 — 目前的追蹤版本 — 已於 2023 年 5 月 19 日發行
- 1.0.50300 — 目前的追蹤版本 — 已於 2023 年 5 月 8 日發行
- 1.0.49710 — Amazon Redshift Serverless 版本 — 已於 2023 年 4 月 28 日發行
- 1.0.49676 — 目前的追蹤版本 — 已於 2023 年 4 月 28 日發行

此修補程式中的新功能和改善

- 次要錯誤修正。
- Amazon Redshift 串流擷取現在支援跨區域串流擷取，您的來源 Amazon Kinesis Data Streams (KDS) 或適用於 Apache Kafka 的亞馬遜受管串流 (MSK) 主題可以位於與 Amazon Redshift 資料倉儲所在 AWS 區域不同的 AWS 區域。[開始從 Amazon Kinesis Data Streams 擷取串流](#) 的文件已進行修訂，會說明 REGION 關鍵字的使用方式。
- 埃及日光節約時間調整。

- 已改善 RA3 叢集加密的整體時間。

Amazon Redshift 修補程式 174

1.0.51296 — 已於 2023 年 6 月 2 日發行

發行至隨後的追蹤。無版本備註。

1.0.50468 — 已於 2023 年 5 月 12 日發行

維護版本。無版本備註。

1.0.49780、1.0.49868 和 1.0.49997 – 已於 2023 年 4 月 28 日發行

此版本的版本備註：

- 已改善 Lambda UDF 的批次處理支援。
- Lambda UDF 的增量批次處理。
- 有新的 MERGE SQL 命令，可將來源資料變更套用至 Amazon Redshift 資料表。
- 有新的動態資料遮罩功能，可簡化 Amazon Redshift 資料倉儲中敏感資料的保護程序。
- 透過 Lake Formation 進行資料共用的全新集中式存取控制，可讓您使用 Lake Formation API 和主控台管理權限授與、檢視存取控制，以及稽核 Amazon Redshift 資料庫中的資料表和檢視上的許可。
AWS
- 埃及日光節約時間調整。

1.0.49087 – 已於 2023 年 4 月 12 日發行

維護版本。無版本備註。

1.0.48805 – 已於 2023 年 4 月 5 日發行

此版本的版本備註：

- Amazon Redshift 針對使用 BYTEDICT、有大量字串的查詢引入了額外的效能增強功能，其中 BYTEDICT 是 Amazon Redshift 中的新壓縮編碼，相較於替代壓縮編碼 (例如 LZ0 或 ZSTD)，可將字串式資料的處理速度提升 5 倍到 63 倍。如需此功能的相關資訊，請參閱《Amazon Redshift 資料庫開發人員指南》中的 [Byte-dictionary 編碼](#)。

1.0.48004 – 已於 2023 年 3 月 17 日發行

維護版本。無版本備註。

1.0.47470 – 已於 2023 年 3 月 11 日發行

此版本的版本備註：

- 改善 `pg_catalog.svv_table_info` 的查詢效能 此外，也新增了新的資料欄 `create_time`。在建立資料表時，這個資料欄會以 UTC 儲存日期/時間戳記。
- 新增對於在聯合查詢上指定工作階段層級逾時的支援。

Amazon Redshift 修補程式 173

1.0.49788 – 已於 2023 年 4 月 28 日發行

此版本的版本備註：

- 埃及日光節約時間調整。

1.0.49074 – 已於 2023 年 4 月 12 日發行

此版本的版本備註：

- 時區組態已更新為 IANA 程式庫版本 2022g。

1.0.48766 – 已於 2023 年 4 月 5 日發行

維護版本。無版本備註。

1.0.48714 – 已於 2023 年 4 月 5 日發行

維護版本。無版本備註。

1.0.48022 – 已於 2023 年 3 月 17 日發行

維護版本。無版本備註。

1.0.47357 – 已於 2023 年 3 月 7 日發行

維護版本。無版本備註。

1.0.46987 – 已於 2023 年 2 月 24 日發行

維護版本。無版本備註。

1.0.46806 – 已於 2023 年 2 月 18 日發行

維護版本。無版本備註。

1.0.46607 – 已於 2023 年 2 月 13 日發行

此版本的版本備註：

- 現在，如果具有手動設定之交錯排序索引鍵的資料表將其分散樣式設定為 DISTSTYLE KEY，我們會自動將該資料表轉換為複合排序索引鍵，以改善這些資料表的效能。這會在將快照還原到 Amazon Redshift Serverless 時完成。

1.0.45698 – 已於 2023 年 1 月 20 日發行

此版本的版本備註：

- 在 UNLOAD 命令中新增了副檔名參數，以便在檔案名稱後自動新增副檔名。
- 可在將受 RLS 保護的物件新增到資料共用時，或是這些物件已是資料共用的一部分時，支援保護這些物件。管理員現在可以關閉資料共用的 RLS，以允許取用者存取受保護的物件。
- 新增用於監控的新系統資料表：SVV_ML_MODEL_INFO、SVV_MV_DEPENDENCY 和 SYS_LOAD_DETAIL。此外，也在系統資料表 SYS_QUERY_DETAIL 中新增資料欄 data_skewness 和 time_skewness。

Amazon Redshift 修補程式 172

此修補程式中的叢集版本：

- 1.0.46534 – 已於 2023 年 2 月 18 日發行
- 1.0.46523 – 已於 2023 年 2 月 13 日發行

- 1.0.46206 – 已於 2023 年 2 月 1 日發行
- 1.0.45603 – 已於 2023 年 1 月 20 日發行
- 1.0.44924 – 已於 2022 年 12 月 19 日發行
- 1.0.44903 – 已於 2022 年 12 月 18 日發行
- 1.0.44540 – 已於 2022 年 12 月 13 日發行
- 1.0.44126 – 已於 2022 年 11 月 23 日發行
- 1.0.43980 – 已於 2022 年 11 月 17 日發行

此修補程式中的新功能和改善

- 依預設，由 CTAS 建立的資料表為 AUTO。
- 新增對於具體化視觀表的資料列層級安全 (RLS) 支援。
- 增加 S3 的逾時以改善跨區域資料共用。
- 新增了新的空間函數 ST_GeomFromGeohash。
- 改進了從複合主鍵中自動選擇分配鍵以提高 out-of-the-box 性能。
- 將自動主索引鍵新增至具有複合主索引鍵的資料表的分配索引鍵，以改善 out-of-the-box 效能。
- 改善並行擴展功能，以允許更多查詢在資料發生變更時也能擴展。
- 改善資料共用查詢效能。
- 為分類模型新增 Machine Learning 機率指標。
- 新增用於監控的新系統資料表：SVV_USER_INFO、SVV_MV_INFO、SYS_CONNECTION_LOG、SYS_DATASHARE_USAGE_PRODUCER 和 SYS_DATASHARE_CHANGE_LOG。
- 新增對於在 Parquet 和 ORC 檔案類型的外部資料表中查詢 VARBYTE 資料欄的支援。

Amazon Redshift 修補程式 171

此修補程式中的叢集版本：

- 1.0.43931 – 已於 2022 年 11 月 16 日發行
- 1.0.43551 – 已於 2022 年 11 月 5 日發行
- 1.0.43331 – 已於 2022 年 9 月 29 日發行
- 1.0.43029 – 已於 2022 年 9 月 26 日發行

此修補程式中的新功能和改善

- CONNECT BY 支援：新增對 CONNECT BY SQL 建構模組的支援，可讓您根據該資料集內的父子關係遞迴查詢資料倉儲中的階層式資料。

Amazon Redshift 修補程式 170

此修補程式中的叢集版本：

- 1.0.43922 – 已於 2022 年 11 月 21 日發行
- 1.0.43573 – 已於 2022 年 11 月 7 日發行
- 1.0.41881 – 已於 2022 年 9 月 20 日發行
- 1.0.41465 – 已於 2022 年 9 月 7 日發行
- 1.0.40325 – 已於 2022 年 7 月 27 日發行

此修補程式中的新功能和改善

- ST_GeomfromGeo JSON：在 GeoJSON 表示形式中從 VARCHAR 構造一個 Amazon Redshift 空間幾何對象。

Amazon Redshift 修補程式 169

此修補程式中的叢集版本：

- 1.0.41050 – 已於 2022 年 9 月 7 日發行
- 1.0.40083 – 已於 2022 年 7 月 16 日發行
- 1.0.39734 – 已於 2022 年 7 月 7 日發行
- 1.0.39380 – 已於 2022 年 6 月 23 日發行
- 1.0.39251 – 已於 2022 年 6 月 15 日發行
- 1.0.39009 – 已於 2022 年 6 月 8 日發行

此修補程式中的新功能和改善

- 將角色新增為 Alter Default Privileges 命令的參數，以支援角色型存取控制。

- 新增 ACCEPTINVCHARS 參數，以支援在從 Parquet 和 ORC 檔案進行複製時取代無效的 UTF-8 字元。
- 新增 OBJECT(k,v) 函數以從鍵值組建構 SUPER 物件。

Amazon Redshift 修補程式 168

此修補程式中的叢集版本：

- 1.0.38698 – 已於 2022 年 5 月 25 日發行
- 1.0.38551 – 已於 2022 年 5 月 20 日發行
- 1.0.38463 – 已於 2022 年 5 月 18 日發行
- 1.0.38361 – 已於 2022 年 5 月 13 日發行
- 1.0.38199 – 已於 2022 年 5 月 9 日發行
- 1.0.38112 – 已於 2022 年 5 月 6 日發行
- 1.0.37684 – 已於 2022 年 4 月 20 日發行

此修補程式中的新功能和改善

- 在 Amazon Redshift ML 中新增對於線性學習程式模型類型的支援。
- 為 SQL 交易隔離層級新增 SNAPSHOT 選項。
- 新增 farmhashFingerprint64 做為 VARBYTE 和 VARCHAR 資料的新雜湊演算法。
- 在具體化視觀表的增量重新整理中支援 AVG 函數。
- 在 Redshift Spectrum 中對外部資料表支援相互關聯的子查詢。
- 為了改善 out-of-the-box 查詢效能，Amazon Redshift 會針對特定資料表自動選擇單一欄主索引鍵做為分配金鑰。

使 AWS 用軟體開發套件的 Amazon Redshift 程式碼範例

下列程式碼範例說明如何搭配 AWS 軟體開發套件 (SDK) 使用 Amazon Redshift。

Actions 是大型程式的程式碼摘錄，必須在內容中執行。雖然動作會告訴您如何呼叫個別服務函數，但您可以在其相關情境和跨服務範例中查看內容中的動作。

Scenarios (案例) 是向您展示如何呼叫相同服務中的多個函數來完成特定任務的程式碼範例。

Cross-service examples (跨服務範例) 是跨多個 AWS 服務執行的應用程式範例。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱[搭配 AWS SDK 使用此服務](#)。此主題也包含入門相關資訊和舊版 SDK 的詳細資訊。

開始使用

你好 Amazon Redshift

下列程式碼範例顯示如何開始使用 Amazon Redshift。

Java

適用於 Java 2.x 的 SDK

Note

還有更多關於 GitHub。尋找完整範例，並了解如何在[AWS 設定和執行程式碼範例儲存庫](#)。

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.redshift.RedshiftClient;
import
    software.amazon.awssdk.services.redshift.paginators.DescribeClustersIterable;

/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
```

```
*
* https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
*/
public class HelloRedshift {

    public static void main(String[] args) {
        Region region = Region.US_EAST_1;
        RedshiftClient redshiftClient = RedshiftClient.builder()
            .region(region)
            .build();

        listClustersPaginator(redshiftClient);
    }

    public static void listClustersPaginator(RedshiftClient redshiftClient) {
        DescribeClustersIterable clustersIterable =
redshiftClient.describeClustersPaginator();
        clustersIterable.stream()
            .flatMap(r -> r.clusters().stream())
            .forEach(cluster -> System.out
                .println(" Cluster identifier: " + cluster.clusterIdentifier() +
" status = " + cluster.clusterStatus()));
    }
}
```

- 如需 API 詳細資訊，請參閱 AWS SDK for Java 2.x API 參考中的[叢集說明](#)。

Python

適用於 Python (Boto3) 的 SDK

Note

還有更多關於 GitHub。尋找完整範例，並了解如何在[AWS 設定和執行程式碼範例儲存庫](#)。

```
import boto3
```

```
def hello_redshift(redshift_client):
    """
    Use the AWS SDK for Python (Boto3) to create an Amazon Redshift client and
    list
    the clusters in your account. This list might be empty if you haven't created
    any clusters.
    This example uses the default settings specified in your shared credentials
    and config files.

    :param redshift_client: A Boto3 Redshift Client object.
    """
    print("Hello, Redshift! Let's list your clusters:")
    paginator = redshift_client.get_paginator("describe_clusters")
    clusters = []
    for page in paginator.paginate():
        clusters.extend(page["Clusters"])

    print(f"{len(clusters)} cluster(s) were found.")

    for cluster in clusters:
        print(f" {cluster['ClusterIdentifier']}")

if __name__ == "__main__":
    hello_redshift(boto3.client("redshift"))
```

- 如需 API 詳細資訊，請參閱 [AWS SDK 中的叢集](#)，以供 Python (Boto3) API 參考使用。

程式碼範例

- [使 AWS 用 SDK 執行 Amazon Redshift 的操作](#)
 - [搭CreateCluster配 AWS 開發套件或 CLI 使用](#)
 - [搭CreateTable配 AWS 開發套件或 CLI 使用](#)
 - [搭DeleteCluster配 AWS 開發套件或 CLI 使用](#)
 - [搭DescribeClusters配 AWS 開發套件或 CLI 使用](#)
 - [搭DescribeStatement配 AWS 開發套件或 CLI 使用](#)
 - [搭GetStatementResult配 AWS 開發套件或 CLI 使用](#)
 - [搭Insert配 AWS 開發套件或 CLI 使用](#)
 - [搭ModifyCluster配 AWS 開發套件或 CLI 使用](#)

- [搭Query配 AWS 開發套件或 CLI 使用](#)
- [使用軟體開發套件的 Amazon Redshift 案 AWS 例](#)
 - [開始使用 Amazon Redshift 表格、項目和查詢](#)
- [使用軟體開發套件的 Amazon Redshift 跨服務範例 AWS](#)
 - [建立 Amazon Redshift 項目追蹤器](#)

使 AWS 用 SDK 執行 Amazon Redshift 的操作

下列程式碼範例示範如何使用 AWS 開發套件執行個別的 Amazon Redshift 動作。這些摘錄會呼叫 Amazon Redshift API，而且是大型程式的程式碼摘錄，這些程式必須在內容中執行。每個範例都包含一個連結 GitHub，您可以在其中找到設定和執行程式碼的指示。

下列範例僅包含最常使用的動作。如需完整清單，請參閱 [Amazon Redshift API 參考](#)。

範例

- [搭CreateCluster配 AWS 開發套件或 CLI 使用](#)
- [搭CreateTable配 AWS 開發套件或 CLI 使用](#)
- [搭DeleteCluster配 AWS 開發套件或 CLI 使用](#)
- [搭DescribeClusters配 AWS 開發套件或 CLI 使用](#)
- [搭DescribeStatement配 AWS 開發套件或 CLI 使用](#)
- [搭GetStatementResult配 AWS 開發套件或 CLI 使用](#)
- [搭Insert配 AWS 開發套件或 CLI 使用](#)
- [搭ModifyCluster配 AWS 開發套件或 CLI 使用](#)
- [搭Query配 AWS 開發套件或 CLI 使用](#)

搭CreateCluster配 AWS 開發套件或 CLI 使用

下列程式碼範例會示範如何使用CreateCluster。

CLI

AWS CLI

以最小的 ParametersThis 範例建立叢集會建立具有最少組參數的叢集。默認情況下，輸出為 JSON 格式。命令：

```
aws redshift create-cluster --node-type dw.hs1.xlarge --number-of-nodes 2 --
master-username adminuser --master-user-password TopSecret1 --cluster-identifier
mycluster
```

結果：

```
{
  "Cluster": {
    "NodeType": "dw.hs1.xlarge",
    "ClusterVersion": "1.0",
    "PubliclyAccessible": "true",
    "MasterUsername": "adminuser",
    "ClusterParameterGroups": [
      {
        "ParameterApplyStatus": "in-sync",
        "ParameterGroupName": "default.redshift-1.0"
      }
    ],
    "ClusterSecurityGroups": [
      {
        "Status": "active",
        "ClusterSecurityGroupName": "default"
      }
    ],
    "AllowVersionUpgrade": true,
    "VpcSecurityGroups": [],
    "PreferredMaintenanceWindow": "sat:03:30-sat:04:00",
    "AutomatedSnapshotRetentionPeriod": 1,
    "ClusterStatus": "creating",
    "ClusterIdentifier": "mycluster",
    "DBName": "dev",
    "NumberOfNodes": 2,
    "PendingModifiedValues": {
      "MasterUserPassword": "\\*****"
    }
  },
  "ResponseMetadata": {
    "RequestId": "7cf4bcfc-64dd-11e2-bea9-49e0ce183f07"
  }
}
```

- 如需 API 詳細資訊，請參閱AWS CLI 命令參考[CreateCluster](#)中的。

Java

適用於 Java 2.x 的 SDK

Note

還有更多關於 GitHub。尋找完整範例，並了解如何在[AWS 設定和執行程式碼範例儲存庫](#)。

建立 叢集

```
public static void createCluster(RedshiftClient redshiftClient, String
clusterId, String masterUsername,
                                String masterUserPassword) {
    try {
        CreateClusterRequest clusterRequest = CreateClusterRequest.builder()
            .clusterIdentifier(clusterId)
            .masterUsername(masterUsername)
            .masterUserPassword(masterUserPassword)
            .nodeType("ra3.4xlarge")
            .publiclyAccessible(true)
            .numberOfNodes(2)
            .build();

        CreateClusterResponse clusterResponse =
redshiftClient.createCluster(clusterRequest);
        System.out.println("Created cluster " +
clusterResponse.cluster().clusterIdentifier());

    } catch (RedshiftException e) {

        System.err.println(e.getMessage());
        System.exit(1);
    }
}
```

- 如需 API 詳細資訊，請參閱 AWS SDK for Java 2.x API 參考[CreateCluster](#)中的。

JavaScript

適用於 JavaScript (v3) 的開發套件

Note

還有更多關於 GitHub。尋找完整範例，並了解如何在[AWS 設定和執行程式碼範例儲存庫](#)。

建立用戶端。

```
import { RedshiftClient } from "@aws-sdk/client-redshift";
// Set the AWS Region.
const REGION = "REGION";
//Set the Redshift Service Object
const redshiftClient = new RedshiftClient({ region: REGION });
export { redshiftClient };
```

建立叢集

```
// Import required AWS SDK clients and commands for Node.js
import { CreateClusterCommand } from "@aws-sdk/client-redshift";
import { redshiftClient } from "../libs/redshiftClient.js";

const params = {
  ClusterIdentifier: "CLUSTER_NAME", // Required
  NodeType: "NODE_TYPE", //Required
  MasterUsername: "MASTER_USER_NAME", // Required - must be lowercase
  MasterUserPassword: "MASTER_USER_PASSWORD", // Required - must contain at least
  one uppercase letter, and one number
  ClusterType: "CLUSTER_TYPE", // Required
  IAMRoleARN: "IAM_ROLE_ARN", // Optional - the ARN of an IAM role with
  permissions your cluster needs to access other AWS services on your behalf, such
  as Amazon S3.
  ClusterSubnetGroupName: "CLUSTER_SUBNET_GROUPNAME", //Optional - the name of a
  cluster subnet group to be associated with this cluster. Defaults to 'default'
  if not specified.
  DBName: "DATABASE_NAME", // Optional - defaults to 'dev' if not specified
  Port: "PORT_NUMBER", // Optional - defaults to '5439' if not specified
};
```

```
const run = async () => {
  try {
    const data = await redshiftClient.send(new CreateClusterCommand(params));
    console.log(
      "Cluster " + data.Cluster.ClusterIdentifier + " successfully created",
    );
    return data; // For unit tests.
  } catch (err) {
    console.log("Error", err);
  }
};
run();
```

- 如需 API 詳細資訊，請參閱 AWS SDK for JavaScript API 參考 [CreateCluster](#) 中的。

Kotlin

適用於 Kotlin 的 SDK

Note

還有更多關於 GitHub。尋找完整範例，並了解如何在 [AWS 設定和執行程式碼範例儲存庫](#)。

建立 叢集

```
suspend fun createCluster(
  clusterId: String?,
  masterUsernameVal: String?,
  masterUserPasswordVal: String?,
) {
  val clusterRequest =
    CreateClusterRequest {
      clusterIdentifier = clusterId
      masterUsername = masterUsernameVal
      masterUserPassword = masterUserPasswordVal
      nodeType = "ds2.xlarge"
      publiclyAccessible = true
      numberOfNodes = 2
    }
}
```

```
    }

    RedshiftClient { region = "us-east-1" }.use { redshiftClient ->
        val clusterResponse = redshiftClient.createCluster(clusterRequest)
        println("Created cluster ${clusterResponse.cluster?.clusterIdentifier}")
    }
}
```

- 有關 API 的詳細信息，請參閱 AWS SDK [CreateCluster](#) 中的 Kotlin API 參考。

Python

適用於 Python (Boto3) 的 SDK

Note

還有更多關於 GitHub。尋找完整範例，並了解如何在 [AWS 設定和執行程式碼範例儲存庫](#)。

```
class RedshiftWrapper:
    """
    Encapsulates Amazon Redshift cluster operations.
    """

    def __init__(self, redshift_client):
        """
        :param redshift_client: A Boto3 Redshift client.
        """
        self.client = redshift_client

    def create_cluster(
        self,
        cluster_identifier,
        node_type,
        master_username,
        master_user_password,
        publicly_accessible,
        number_of_nodes,
    ):
```

```
"""
Creates a cluster.

:param cluster_identifier: The name of the cluster.
:param node_type: The type of node in the cluster.
:param master_username: The master username.
:param master_user_password: The master user password.
:param publicly_accessible: Whether the cluster is publicly accessible.
:param number_of_nodes: The number of nodes in the cluster.
:return: The cluster.
"""

try:
    cluster = self.client.create_cluster(
        ClusterIdentifier=cluster_identifier,
        NodeType=node_type,
        MasterUsername=master_username,
        MasterUserPassword=master_user_password,
        PubliclyAccessible=publicly_accessible,
        NumberOfNodes=number_of_nodes,
    )
    return cluster
except ClientError as err:
    logging.error(
        "Couldn't create a cluster. Here's why: %s: %s",
        err.response["Error"]["Code"],
        err.response["Error"]["Message"],
    )
    raise
```

下面的代碼實例化對 RedshiftWrapper 象。

```
client = boto3.client("redshift")
redshift_wrapper = RedshiftWrapper(client)
```

- 如需 API 的詳細資訊，請參閱AWS 開發套件[CreateCluster](#)中的 Python (博托 3) API 參考。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱[搭配 AWS SDK 使用此服務](#)。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

搭CreateTable配 AWS 開發套件或 CLI 使用

下列程式碼範例會示範如何使用CreateTable。

Java

適用於 Java 2.x 的 SDK

Note

還有更多關於 GitHub。尋找完整範例，並了解如何在[AWS 設定和執行程式碼範例儲存庫](#)。

```
public static void createTable(RedshiftDataClient redshiftDataClient, String
clusterId, String databaseName, String userName) {
    try {
        ExecuteStatementRequest createTableRequest =
ExecuteStatementRequest.builder()
        .clusterIdentifier(clusterId)
        .dbUser(userName)
        .database(databaseName)
        .sql("CREATE TABLE Movies ("
            + "id INT PRIMARY KEY, "
            + "title VARCHAR(100), "
            + "year INT)")
        .build();

        redshiftDataClient.executeStatement(createTableRequest);
        System.out.println("Table created: Movies");

    } catch (RedshiftDataException e) {
        System.err.println("Error creating table: " + e.getMessage());
        System.exit(1);
    }
}
```

- 如需 API 詳細資訊，請參閱 AWS SDK for Java 2.x API 參考[CreateTable](#)中的。

Python

適用於 Python (Boto3) 的 SDK

Note

還有更多關於 GitHub。尋找完整範例，並了解如何在[AWS 設定和執行程式碼範例儲存庫](#)。

```
def create_table(self, cluster_id, database, username):
    self.redshift_data_wrapper.execute_statement(
        cluster_identifier=cluster_id,
        database_name=database,
        user_name=username,
        sql="CREATE TABLE Movies (statement_id INT PRIMARY KEY, title
VARCHAR(100), year INT)",
    )

    print("Table created: Movies")
```

包裝器對象調用 ExecuteStatement。

```
class RedshiftDataWrapper:
    """Encapsulates Amazon Redshift data."""

    def __init__(self, client):
        """
        :param client: A Boto3 RedshiftDataWrapper client.
        """
        self.client = client

    def execute_statement(
        self, cluster_identifier, database_name, user_name, sql,
        parameter_list=None
    ):
        """
        Executes a SQL statement.
```

```
:param cluster_identifier: The cluster identifier.
:param database_name: The database name.
:param user_name: The user's name.
:param sql: The SQL statement.
:param parameter_list: The optional SQL statement parameters.
:return: The SQL statement result.
"""

try:
    kwargs = {
        "ClusterIdentifier": cluster_identifier,
        "Database": database_name,
        "DbUser": user_name,
        "Sql": sql,
    }
    if parameter_list:
        kwargs["Parameters"] = parameter_list
    response = self.client.execute_statement(**kwargs)
    return response
except ClientError as err:
    logging.error(
        "Couldn't execute statement. Here's why: %s: %s",
        err.response["Error"]["Code"],
        err.response["Error"]["Message"],
    )
    raise
```

下面的代碼實例化對 RedshiftDataWrapper 象。

```
client = boto3.client("redshift-data")
redshift_data_wrapper = RedshiftDataWrapper(client)
```

- 如需 API 的詳細資訊，請參閱AWS 開發套件[CreateTable](#)中的 Python (博托 3) API 參考。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱[搭配 AWS SDK 使用此服務](#)。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

搭DeleteCluster配 AWS 開發套件或 CLI 使用

下列程式碼範例會示範如何使用DeleteCluster。

CLI

AWS CLI

刪除沒有最終叢集的叢集 SnapshotThis 範例會刪除叢集，強制刪除資料，因此不會建立最終叢集快照。命令：

```
aws redshift delete-cluster --cluster-identifier mycluster --skip-final-cluster-snapshot
```

刪除叢集，允許最終叢集 SnapshotThis 範例刪除叢集，但指定最終的叢集快照。命令：

```
aws redshift delete-cluster --cluster-identifier mycluster --final-cluster-snapshot-identifier myfinalsnapshot
```

- 如需 API 詳細資訊，請參閱AWS CLI 命令參考[DeleteCluster](#)中的。

Java

適用於 Java 2.x 的 SDK

Note

還有更多關於 GitHub。尋找完整範例，並了解如何在[AWS 設定和執行程式碼範例儲存庫](#)。

刪除叢集。

```
public static void deleteRedshiftCluster(RedshiftClient redshiftClient,
String clusterId) {
    try {
        DeleteClusterRequest deleteClusterRequest =
DeleteClusterRequest.builder()
            .clusterIdentifier(clusterId)
            .skipFinalClusterSnapshot(true)
            .build();
```

```
        DeleteClusterResponse response =
redshiftClient.deleteCluster(deleteClusterRequest);
        System.out.println("The status is " +
response.cluster().clusterStatus());

    } catch (RedshiftException e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}
```

- 如需 API 詳細資訊，請參閱 AWS SDK for Java 2.x API 參考 [DeleteCluster](#) 中的。

JavaScript

適用於 JavaScript (v3) 的開發套件

Note

還有更多關於 GitHub。尋找完整範例，並了解如何在 [AWS 設定和執行程式碼範例儲存庫](#)。

建立用戶端。

```
import { RedshiftClient } from "@aws-sdk/client-redshift";
// Set the AWS Region.
const REGION = "REGION";
//Set the Redshift Service Object
const redshiftClient = new RedshiftClient({ region: REGION });
export { redshiftClient };
```

建立叢集

```
// Import required AWS SDK clients and commands for Node.js
import { DeleteClusterCommand } from "@aws-sdk/client-redshift";
import { redshiftClient } from "../libs/redshiftClient.js";
```

```
const params = {
  ClusterIdentifier: "CLUSTER_NAME",
  SkipFinalClusterSnapshot: false,
  FinalClusterSnapshotIdentifier: "CLUSTER_SNAPSHOT_ID",
};

const run = async () => {
  try {
    const data = await redshiftClient.send(new DeleteClusterCommand(params));
    console.log("Success, cluster deleted. ", data);
    return data; // For unit tests.
  } catch (err) {
    console.log("Error", err);
  }
};

run();
```

- 如需 API 詳細資訊，請參閱 AWS SDK for JavaScript API 參考[DeleteCluster](#)中的。

Kotlin

適用於 Kotlin 的 SDK

Note

還有更多關於 GitHub。尋找完整範例，並了解如何在[AWS 設定和執行程式碼範例儲存庫](#)。

刪除叢集。

```
suspend fun deleteRedshiftCluster(clusterId: String?) {
    val request =
        DeleteClusterRequest {
            clusterIdentifier = clusterId
            skipFinalClusterSnapshot = true
        }

    RedshiftClient { region = "us-west-2" }.use { redshiftClient ->
        val response = redshiftClient.deleteCluster(request)
        println("The status is ${response.cluster?.clusterStatus}")
    }
}
```

```
}  
}
```

- 有關 API 的詳細信息，請參閱 AWS SDK [DeleteCluster](#) 中的 Kotlin API 參考。

Python

適用於 Python (Boto3) 的 SDK

Note

還有更多關於 GitHub。尋找完整範例，並了解如何在 [AWS 設定和執行程式碼範例儲存庫](#)。

```
class RedshiftWrapper:  
    """  
    Encapsulates Amazon Redshift cluster operations.  
    """  
  
    def __init__(self, redshift_client):  
        """  
        :param redshift_client: A Boto3 Redshift client.  
        """  
        self.client = redshift_client  
  
    def delete_cluster(self, cluster_identifier):  
        """  
        Deletes a cluster.  
  
        :param cluster_identifier: The cluster identifier.  
        """  
        try:  
            self.client.delete_cluster(  
                ClusterIdentifier=cluster_identifier,  
                SkipFinalClusterSnapshot=True  
            )  
        except ClientError as err:  
            logging.error(  
                "Couldn't delete a cluster. Here's why: %s: %s",
```

```
        err.response["Error"]["Code"],
        err.response["Error"]["Message"],
    )
    raise
```

下面的代碼實例化對 RedshiftWrapper 象。

```
client = boto3.client("redshift")
redshift_wrapper = RedshiftWrapper(client)
```

- 如需 API 的詳細資訊，請參閱AWS 開發套件[DeleteCluster](#)中的 Python (博托 3) API 參考。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱[搭配 AWS SDK 使用此服務](#)。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

搭 DescribeClusters 配 AWS 開發套件或 CLI 使用

下列程式碼範例會示範如何使用 DescribeClusters。

CLI

AWS CLI

[取得全部說明] ClustersThis 範例會傳回該帳戶之所有叢集的說明。默認情況下，輸出為 JSON 格式。命令：

```
aws redshift describe-clusters
```

結果：

```
{
  "Clusters": [
    {
      "NodeType": "dw.hs1.xlarge",
      "Endpoint": {
        "Port": 5439,
        "Address": "mycluster.coqoarplqhsn.us-east-1.redshift.amazonaws.com"
      },
    },
  ],
}
```

```

"ClusterVersion": "1.0",
"PubliclyAccessible": "true",
"MasterUsername": "adminuser",
"ClusterParameterGroups": [
  {
    "ParameterApplyStatus": "in-sync",
    "ParameterGroupName": "default.redshift-1.0"
  } ],
"ClusterSecurityGroups": [
  {
    "Status": "active",
    "ClusterSecurityGroupName": "default"
  } ],
"AllowVersionUpgrade": true,
"VpcSecurityGroups": \[],
"AvailabilityZone": "us-east-1a",
"ClusterCreateTime": "2013-01-22T21:59:29.559Z",
"PreferredMaintenanceWindow": "sat:03:30-sat:04:00",
"AutomatedSnapshotRetentionPeriod": 1,
"ClusterStatus": "available",
"ClusterIdentifier": "mycluster",
"DBName": "dev",
"NumberOfNodes": 2,
"PendingModifiedValues": {}
} ],
"ResponseMetadata": {
  "RequestId": "65b71cac-64df-11e2-8f5b-e90bd6c77476"
}
}

```

您也可以使用 `--output text` 選項以文字格式取得相同的資訊。指令：

`--output text` 選項。命令：

選項。命令：

```
aws redshift describe-clusters --output text
```

結果：

```

dw.hs1.xlarge      1.0      true      adminuser      True      us-east-1a
2013-01-22T21:59:29.559Z      sat:03:30-sat:04:00      1      available
mycluster         dev      2

```

```

ENDPOINT      5439      mycluster.coqoarplqhsn.us-east-1.redshift.amazonaws.com
in-sync      default.redshift-1.0
active       default
PENDINGMODIFIEDVALUES
RESPONSEMETADATA  934281a8-64df-11e2-b07c-f7fbdd006c67

```

- 如需 API 詳細資訊，請參閱AWS CLI 命令參考[DescribeClusters](#)中的。

Java

適用於 Java 2.x 的 SDK

Note

還有更多關於 GitHub。尋找完整範例，並了解如何在[AWS 設定和執行程式碼範例儲存庫](#)。

描述叢集。

```

public static void waitForClusterReady(RedshiftClient redshiftClient, String
clusterId) {
    boolean clusterReady = false;
    String clusterReadyStr;
    System.out.println("Waiting for cluster to become available. This may
take a few mins.");
    try {
        DescribeClustersRequest clustersRequest =
DescribeClustersRequest.builder()
            .clusterIdentifier(clusterId)
            .build();
        long startTime = System.currentTimeMillis();

        // Loop until the cluster is ready.
        while (!clusterReady) {
            DescribeClustersResponse clusterResponse =
redshiftClient.describeClusters(clustersRequest);
            List<Cluster> clusterList = clusterResponse.clusters();
            for (Cluster cluster : clusterList) {
                clusterReadyStr = cluster.clusterStatus();
                if (clusterReadyStr.contains("available"))
                    clusterReady = true;
            }
        }
    }
}

```

```
        else {
            long elapsedTimeMillis = System.currentTimeMillis() -
startTime;

            long elapsedSeconds = elapsedTimeMillis / 1000;
            long minutes = elapsedSeconds / 60;
            long seconds = elapsedSeconds % 60;

            System.out.printf("Elapsed Time: %02d:%02d - Waiting for
cluster... %n", minutes, seconds);
            TimeUnit.SECONDS.sleep(5);
        }
    }

    long elapsedTimeMillis = System.currentTimeMillis() - startTime;
    long elapsedSeconds = elapsedTimeMillis / 1000;
    long minutes = elapsedSeconds / 60;
    long seconds = elapsedSeconds % 60;

    System.out.println(String.format("Cluster is available! Total Elapsed
Time: %02d:%02d", minutes, seconds));

    } catch (RedshiftException | InterruptedException e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}
```

- 如需 API 詳細資訊，請參閱 AWS SDK for Java 2.x API 參考[DescribeClusters](#)中的。

JavaScript

適用於 JavaScript (v3) 的開發套件

Note

還有更多關於 GitHub。尋找完整範例，並了解如何在[AWS 設定和執行程式碼範例儲存庫](#)。

建立用戶端。


```
import { RedshiftClient } from "@aws-sdk/client-redshift";
// Set the AWS Region.
const REGION = "REGION";
//Set the Redshift Service Object
const redshiftClient = new RedshiftClient({ region: REGION });
export { redshiftClient };
```

描述您的叢集。

```
// Import required AWS SDK clients and commands for Node.js
import { DescribeClustersCommand } from "@aws-sdk/client-redshift";
import { redshiftClient } from "../libs/redshiftClient.js";

const params = {
  ClusterIdentifier: "CLUSTER_NAME",
};

const run = async () => {
  try {
    const data = await redshiftClient.send(new DescribeClustersCommand(params));
    console.log("Success", data);
    return data; // For unit tests.
  } catch (err) {
    console.log("Error", err);
  }
};
run();
```

- 如需 API 詳細資訊，請參閱 AWS SDK for JavaScript API 參考[DescribeClusters](#)中的。

Kotlin

適用於 Kotlin 的 SDK

Note

還有更多關於 GitHub。尋找完整範例，並了解如何在[AWS 設定和執行程式碼範例儲存庫](#)。

描述叢集。

```
suspend fun describeRedshiftClusters() {
    RedshiftClient { region = "us-west-2" }.use { redshiftClient ->
        val clusterResponse =
            redshiftClient.describeClusters(DescribeClustersRequest {})
        val clusterList = clusterResponse.clusters

        if (clusterList != null) {
            for (cluster in clusterList) {
                println("Cluster database name is ${cluster.dbName}")
                println("Cluster status is ${cluster.clusterStatus}")
            }
        }
    }
}
```

- 有關 API 的詳細信息，請參閱 AWS SDK [DescribeClusters](#) 中的 Kotlin API 參考。

Python

適用於 Python (Boto3) 的 SDK

Note

還有更多關於 GitHub。尋找完整範例，並了解如何在 [AWS 設定和執行程式碼範例儲存庫](#)。

```
class RedshiftWrapper:
    """
    Encapsulates Amazon Redshift cluster operations.
    """

    def __init__(self, redshift_client):
        """
        :param redshift_client: A Boto3 Redshift client.
        """
        self.client = redshift_client
```

```
def describe_clusters(self, cluster_identifier):
    """
    Describes a cluster.

    :param cluster_identifier: The cluster identifier.
    :return: A list of clusters.
    """
    try:
        kwargs = {}
        if cluster_identifier:
            kwargs["ClusterIdentifier"] = cluster_identifier

        paginator = self.client.get_paginator("describe_clusters")
        clusters = []
        for page in paginator.paginate(**kwargs):
            clusters.extend(page["Clusters"])

        return clusters

    except ClientError as err:
        logging.error(
            "Couldn't describe a cluster. Here's why: %s: %s",
            err.response["Error"]["Code"],
            err.response["Error"]["Message"],
        )
        raise
```

下面的代碼實例化對 RedshiftWrapper 象。

```
client = boto3.client("redshift")
redshift_wrapper = RedshiftWrapper(client)
```

- 如需 API 的詳細資訊，請參閱AWS 開發套件[DescribeClusters](#)中的 Python (博托 3) API 參考。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱[搭配 AWS SDK 使用此服務](#)。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

搭DescribeStatement配 AWS 開發套件或 CLI 使用

下列程式碼範例會示範如何使用DescribeStatement。

Java

適用於 Java 2.x 的 SDK

Note

還有更多關於 GitHub。尋找完整範例，並了解如何在[AWS 設定和執行程式碼範例儲存庫](#)。

```
public static void checkStatement(RedshiftDataClient redshiftDataClient,
String sqlId) {
    try {
        DescribeStatementRequest statementRequest =
DescribeStatementRequest.builder()
            .id(sqlId)
            .build();

        String status;
        while (true) {
            DescribeStatementResponse response =
redshiftDataClient.describeStatement(statementRequest);
            status = response.statusAsString();
            System.out.println("..." + status);

            if (status.compareTo("FAILED") == 0 ) {
                System.out.println("The Query Failed. Ending program");
                System.exit(1);

            } else if (status.compareTo("FINISHED") == 0) {
                break;
            }
            TimeUnit.SECONDS.sleep(1);
        }

        System.out.println("The statement is finished!");
    } catch (RedshiftDataException | InterruptedException e) {
```

```
        System.err.println(e.getMessage());
        System.exit(1);
    }
}
```

- 如需 API 詳細資訊，請參閱 AWS SDK for Java 2.x API 參考[DescribeStatement](#)中的。

Python

適用於 Python (Boto3) 的 SDK

Note

還有更多關於 GitHub。尋找完整範例，並了解如何在[AWS 設定和執行程式碼範例儲存庫](#)。

```
class RedshiftDataWrapper:
    """Encapsulates Amazon Redshift data."""

    def __init__(self, client):
        """
        :param client: A Boto3 RedshiftDataWrapper client.
        """
        self.client = client

    def describe_statement(self, statement_id):
        """
        Describes a SQL statement.

        :param statement_id: The SQL statement identifier.
        :return: The SQL statement result.
        """
        try:
            response = self.client.describe_statement(Id=statement_id)
            return response
        except ClientError as err:
            logging.error(
                "Couldn't describe statement. Here's why: %s: %s",
                err.response["Error"]["Code"],
```

```
        err.response["Error"]["Message"],
    )
    raise
```

下面的代碼實例化對 RedshiftDataWrapper 象。

```
client = boto3.client("redshift-data")
redshift_data_wrapper = RedshiftDataWrapper(client)
```

- 如需 API 的詳細資訊，請參閱AWS 開發套件[DescribeStatement](#)中的 Python (博托 3) API 參考。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱[搭配 AWS SDK 使用此服務](#)。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

搭GetStatementResult配 AWS 開發套件或 CLI 使用

下列程式碼範例會示範如何使用GetStatementResult。

Java

適用於 Java 2.x 的 SDK

Note

還有更多關於 GitHub。尋找完整範例，並了解如何在[AWS 設定和執行程式碼範例儲存庫](#)。

檢查語句結果。

```
public static void getResults(RedshiftDataClient redshiftDataClient, String
statementId) {
    try {
        GetStatementResultRequest resultRequest =
        GetStatementResultRequest.builder()
```

```

        .id(statementId)
        .build();

        // Extract and print the field values using streams.
        GetStatementResultResponse response =
redshiftDataClient.getStatementResult(resultRequest);
        response.records().stream()
            .flatMap(List::stream)
            .map(Field::stringValue)
            .filter(value -> value != null)
            .forEach(value -> System.out.println("The Movie title field is "
+ value));

    } catch (RedshiftDataException e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}

```

- 如需 API 詳細資訊，請參閱 AWS SDK for Java 2.x API 參考中的[GetStatement結果](#)。

Python

適用於 Python (Boto3) 的 SDK

Note

還有更多關於 GitHub。尋找完整範例，並了解如何在[AWS 設定和執行程式碼範例儲存庫](#)。

```

class RedshiftDataWrapper:
    """Encapsulates Amazon Redshift data."""

    def __init__(self, client):
        """
        :param client: A Boto3 RedshiftDataWrapper client.
        """
        self.client = client

```

```
def get_statement_result(self, statement_id):
    """
    Gets the result of a SQL statement.

    :param statement_id: The SQL statement identifier.
    :return: The SQL statement result.
    """
    try:
        result = {
            "Records": [],
        }
        paginator = self.client.get_paginator("get_statement_result")
        for page in paginator.paginate(Id=statement_id):
            if "ColumnMetadata" not in result:
                result["ColumnMetadata"] = page["ColumnMetadata"]
            result["Records"].extend(page["Records"])
        return result
    except ClientError as err:
        logging.error(
            "Couldn't get statement result. Here's why: %s: %s",
            err.response["Error"]["Code"],
            err.response["Error"]["Message"],
        )
        raise
```

下面的代碼實例化對 RedshiftDataWrapper 象。

```
client = boto3.client("redshift-data")
redshift_data_wrapper = RedshiftDataWrapper(client)
```

- 如需 API 的詳細資訊，請參閱AWS 開發套件中的[GetStatement結果](#) (Boto3) API 參考。


如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱[搭配 AWS SDK 使用此服務](#)。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

搭Insert配 AWS 開發套件或 CLI 使用

下列程式碼範例會示範如何使用Insert。

Java

適用於 Java 2.x 的 SDK

 Note

還有更多關於 GitHub。尋找完整範例，並了解如何在[AWS 設定和執行程式碼範例儲存庫](#)。

```
public static void popTable(RedshiftDataClient redshiftDataClient, String
clusterId, String databaseName, String userName, String fileName, int number)
throws IOException {
    JsonParser parser = new JsonFactory().createParser(new File(fileName));
    com.fasterxml.jackson.databind.JsonNode rootNode = new
ObjectMapper().readTree(parser);
    Iterator<JsonNode> iter = rootNode.iterator();
    ObjectNode currentNode;
    int t = 0;
    while (iter.hasNext()) {
        if (t == number)
            break;
        currentNode = (ObjectNode) iter.next();
        int year = currentNode.get("year").asInt();
        String title = currentNode.get("title").asText();

        // Use SqlParameter to avoid SQL injection.
        List<SqlParameter> parameterList = new ArrayList<>();
        String sqlStatement = "INSERT INTO Movies
VALUES( :id , :title, :year);";

        // Create the parameters.
        SqlParameter idParam = SqlParameter.builder()
            .name("id")
            .value(String.valueOf(t))
            .build();

        SqlParameter titleParam= SqlParameter.builder()
            .name("title")
            .value(title)
            .build();
```

```
SqlParameter yearParam = SqlParameter.builder()
    .name("year")
    .value(String.valueOf(year))
    .build();
parameterList.add(idParam);
parameterList.add(titleParam);
parameterList.add(yearParam);

try {
    ExecuteStatementRequest insertStatementRequest =
ExecuteStatementRequest.builder()
    .clusterIdentifier(clusterId)
    .sql(sqlStatement)
    .database(databaseName)
    .dbUser(userName)
    .parameters(parameterList)
    .build();

    redshiftDataClient.executeStatement(insertStatementRequest);
    System.out.println("Inserted: " + title + " (" + year + ")");
    t++;

} catch (RedshiftDataException e) {
    System.err.println("Error inserting data: " + e.getMessage());
    System.exit(1);
}
}
System.out.println(t + " records were added to the Movies table. ");
}
```

- 如需 API 詳細資訊，請參閱在 [AWS SDK for Java 2.x API 參考](#) 中 [插入](#)。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱 [搭配 AWS SDK 使用此服務](#)。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

搭 `ModifyCluster` 配 AWS 開發套件或 CLI 使用

下列程式碼範例會示範如何使用 `ModifyCluster`。

CLI

AWS CLI

將「安全群組」與 ClusterThis 範例產生關聯，顯示如何將叢集安全性群組與指定的叢集產生關聯。命令：

```
aws redshift modify-cluster --cluster-identifier mycluster --cluster-security-groups mysecuritygroup
```

修改「維護時段」，以 ClusterThis 顯示如何將叢集的每週偏好維護時段變更為從星期日晚上 11:15 開始至少 4 小時的時段，並在星期一凌晨 3:15 結束。命令：

```
aws redshift modify-cluster --cluster-identifier mycluster --preferred-maintenance-window Sun:23:15-Mon:03:15
```

變更主要密碼的 ClusterThis 範例顯示如何變更叢集的主要密碼。命令：

```
aws redshift modify-cluster --cluster-identifier mycluster --master-user-password A1b2c3d4
```

- 如需 API 詳細資訊，請參閱AWS CLI 命令參考[ModifyCluster](#)中的。

Java

適用於 Java 2.x 的 SDK

Note

還有更多關於 GitHub。尋找完整範例，並了解如何在[AWS 設定和執行程式碼範例儲存庫](#)。

修改叢集。

```
public static void modifyCluster(RedshiftClient redshiftClient, String
clusterId) {
    try {
        ModifyClusterRequest modifyClusterRequest =
ModifyClusterRequest.builder()
```

```
        .clusterIdentifier(clusterId)
        .preferredMaintenanceWindow("wed:07:30-wed:08:00")
        .build();

        ModifyClusterResponse clusterResponse =
redshiftClient.modifyCluster(modifyClusterRequest);
        System.out.println("The modified cluster was successfully modified
and has "
            + clusterResponse.cluster().preferredMaintenanceWindow() + " as
the maintenance window");

    } catch (RedshiftException e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}
```

- 如需 API 詳細資訊，請參閱 AWS SDK for Java 2.x API 參考[ModifyCluster](#)中的。

JavaScript

適用於 JavaScript (v3) 的開發套件

Note

還有更多關於 GitHub。尋找完整範例，並了解如何在[AWS 設定和執行程式碼範例儲存庫](#)。

建立用戶端。

```
import { RedshiftClient } from "@aws-sdk/client-redshift";
// Set the AWS Region.
const REGION = "REGION";
//Set the Redshift Service Object
const redshiftClient = new RedshiftClient({ region: REGION });
export { redshiftClient };
```

修改叢集。

```
// Import required AWS SDK clients and commands for Node.js
import { ModifyClusterCommand } from "@aws-sdk/client-redshift";
import { redshiftClient } from "../libs/redshiftClient.js";

// Set the parameters
const params = {
  ClusterIdentifier: "CLUSTER_NAME",
  MasterUserPassword: "NEW_MASTER_USER_PASSWORD",
};

const run = async () => {
  try {
    const data = await redshiftClient.send(new ModifyClusterCommand(params));
    console.log("Success was modified.", data);
    return data; // For unit tests.
  } catch (err) {
    console.log("Error", err);
  }
};
run();
```

- 如需 API 詳細資訊，請參閱 AWS SDK for JavaScript API 參考[ModifyCluster](#)中的。

Kotlin

適用於 Kotlin 的 SDK

Note

還有更多關於 GitHub。尋找完整範例，並了解如何在[AWS 設定和執行程式碼範例儲存庫](#)。

修改叢集。

```
suspend fun modifyCluster(clusterId: String?) {
    val modifyClusterRequest =
        ModifyClusterRequest {
            clusterIdentifier = clusterId
            preferredMaintenanceWindow = "wed:07:30-wed:08:00"
```

```
    }

    RedshiftClient { region = "us-west-2" }.use { redshiftClient ->
        val clusterResponse = redshiftClient.modifyCluster(modifyClusterRequest)
        println(
            "The modified cluster was successfully modified and has
            ${clusterResponse.cluster?.preferredMaintenanceWindow} as the maintenance
            window",
        )
    }
}
```

- 有關 API 的詳細信息，請參閱 AWS SDK [ModifyCluster](#) 中的 Kotlin API 參考。

Python

適用於 Python (Boto3) 的 SDK

Note

還有更多關於 GitHub。尋找完整範例，並了解如何在 [AWS 設定和執行程式碼範例儲存庫](#)。

```
class RedshiftWrapper:
    """
    Encapsulates Amazon Redshift cluster operations.
    """

    def __init__(self, redshift_client):
        """
        :param redshift_client: A Boto3 Redshift client.
        """
        self.client = redshift_client

    def modify_cluster(self, cluster_identifier, preferred_maintenance_window):
        """
        Modifies a cluster.

        :param cluster_identifier: The cluster identifier.
```

```
:param preferred_maintenance_window: The preferred maintenance window.
"""
try:
    self.client.modify_cluster(
        ClusterIdentifier=cluster_identifier,
        PreferredMaintenanceWindow=preferred_maintenance_window,
    )
except ClientError as err:
    logging.error(
        "Couldn't modify a cluster. Here's why: %s: %s",
        err.response["Error"]["Code"],
        err.response["Error"]["Message"],
    )
    raise
```

下面的代碼實例化對 RedshiftWrapper 象。

```
client = boto3.client("redshift")
redshift_wrapper = RedshiftWrapper(client)
```

- 如需 API 的詳細資訊，請參閱AWS 開發套件[ModifyCluster](#)中的 Python (博托 3) API 參考。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱[搭配 AWS SDK 使用此服務](#)。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

搭Query配 AWS 開發套件或 CLI 使用

下列程式碼範例會示範如何使用Query。

Java

適用於 Java 2.x 的 SDK

Note

還有更多關於 GitHub。尋找完整範例，並了解如何在[AWS 設定和執行程式碼範例儲存庫](#)。

查詢資料表。

```
public static String queryMoviesByYear(RedshiftDataClient redshiftDataClient,
                                       String database,
                                       String dbUser,
                                       int year,
                                       String clusterId) {

    try {
        String sqlStatement = " SELECT * FROM Movies WHERE year = :year";
        SqlParameter yearParam= SqlParameter.builder()
            .name("year")
            .value(String.valueOf(year))
            .build();

        ExecuteStatementRequest statementRequest =
ExecuteStatementRequest.builder()
            .clusterIdentifier(clusterId)
            .database(database)
            .dbUser(dbUser)
            .parameters(yearParam)
            .sql(sqlStatement)
            .build();

        ExecuteStatementResponse response =
redshiftDataClient.executeStatement(statementRequest);
        return response.id();

    } catch (RedshiftDataException e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
    return "";
}
```

- 如需 API 的詳細資訊，請參閱《AWS SDK for Java 2.x API 參考》中的 [Query](#)。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱[搭配 AWS SDK 使用此服務](#)。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

使用軟體開發套件的 Amazon Redshift 案 AWS 例

下列程式碼範例說明如何在具有 AWS 開發套件的 Amazon Redshift 中實作常見案例。這些案例說明如何透過在 Amazon Redshift 中呼叫多個函數來完成特定任務。每個案例都包含一個連結 GitHub，您可以在其中找到如何設定和執程式碼的指示。

範例

- [開始使用 Amazon Redshift 表格、項目和查詢](#)

開始使用 Amazon Redshift 表格、項目和查詢

下列程式碼範例說明如何使用 Amazon Redshift 資料表、項目和查詢。

Java

適用於 Java 2.x 的 SDK

Note

還有更多關於 GitHub。尋找完整範例，並了解如何在[AWS 設定和執程式碼範例儲存庫](#)。

```
import com.fasterxml.jackson.core.JsonFactory;
import com.fasterxml.jackson.databind.JsonNode;
import com.fasterxml.jackson.databind.ObjectMapper;
import com.fasterxml.jackson.databind.node.ObjectNode;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.redshift.RedshiftClient;
import software.amazon.awssdk.services.redshift.model.Cluster;
import software.amazon.awssdk.services.redshift.model.CreateClusterRequest;
import software.amazon.awssdk.services.redshift.model.CreateClusterResponse;
import software.amazon.awssdk.services.redshift.model.DeleteClusterRequest;
import software.amazon.awssdk.services.redshift.model.DeleteClusterResponse;
import software.amazon.awssdk.services.redshift.model.DescribeClustersRequest;
import software.amazon.awssdk.services.redshift.model.DescribeClustersResponse;
import software.amazon.awssdk.services.redshift.model.ModifyClusterRequest;
import software.amazon.awssdk.services.redshift.model.ModifyClusterResponse;
import software.amazon.awssdk.services.redshift.model.RedshiftException;
import software.amazon.awssdk.services.redshiftdata.RedshiftDataClient;
```

```
import
    software.amazon.awssdk.services.redshiftdata.model.DescribeStatementRequest;
import
    software.amazon.awssdk.services.redshiftdata.model.DescribeStatementResponse;
import
    software.amazon.awssdk.services.redshiftdata.model.ExecuteStatementRequest;
import
    software.amazon.awssdk.services.redshiftdata.model.ExecuteStatementResponse;
import software.amazon.awssdk.services.redshiftdata.model.Field;
import
    software.amazon.awssdk.services.redshiftdata.model.GetStatementResultRequest;
import
    software.amazon.awssdk.services.redshiftdata.model.GetStatementResultResponse;
import software.amazon.awssdk.services.redshiftdata.model.ListDatabasesRequest;
import software.amazon.awssdk.services.redshiftdata.model.RedshiftDataException;
import software.amazon.awssdk.services.redshiftdata.model.SqlParameter;
import
    software.amazon.awssdk.services.redshiftdata.paginators.ListDatabasesIterable;
import com.fasterxml.jackson.core.JsonParser;
import java.io.File;
import java.io.IOException;
import java.util.ArrayList;
import java.util.Iterator;
import java.util.List;
import java.util.Scanner;
import java.util.concurrent.TimeUnit;

/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-started.html
 *
 * This Java example performs these tasks:
 *
 * 1. Prompts the user for a unique cluster ID or use the default value.
 * 2. Creates a Redshift cluster with the specified or default cluster Id value.
 * 3. Waits until the Redshift cluster is available for use.
 * 4. Lists all databases using a pagination API call.
 * 5. Creates a table named "Movies" with fields ID, title, and year.
```

- * 6. Inserts a specified number of records into the "Movies" table by reading the Movies JSON file.
 - * 7. Prompts the user for a movie release year.
 - * 8. Runs a SQL query to retrieve movies released in the specified year.
 - * 9. Modifies the Redshift cluster.
 - * 10. Prompts the user for confirmation to delete the Redshift cluster.
 - * 11. If confirmed, deletes the specified Redshift cluster.
- */

```
public class RedshiftScenario {
    public static final String DASHES = new String(new char[80]).replace("\0",
"-");
    public static void main(String[] args) throws Exception {
        final String usage = ""

            Usage:
                <jsonFilePath>\s

            Where:
                jsonFilePath - The path to the Movies JSON file (you can locate
that file in ../../../../resources/sample_files/movies.json)
                """;

        if (args.length != 1) {
            System.out.println(usage);
            System.exit(1);
        }

        String jsonFilePath = args[0];
        String userName;
        String userPassword;
        String databaseName = "dev" ;
        Scanner scanner = new Scanner(System.in);

        Region region = Region.US_EAST_1;
        RedshiftClient redshiftClient = RedshiftClient.builder()
            .region(region)
            .build();

        RedshiftDataClient redshiftDataClient = RedshiftDataClient.builder()
            .region(region)
            .build();

        System.out.println(DASHES);
    }
}
```

```
System.out.println("Welcome to the Amazon Redshift SDK Getting Started
scenario.");
System.out.println("""
This Java program demonstrates how to interact with Amazon Redshift by
using the AWS SDK for Java (v2).\s
Amazon Redshift is a fully managed, petabyte-scale data warehouse service
hosted in the cloud.

The program's primary functionalities include cluster creation,
verification of cluster readiness,\s
list databases, table creation, data population within the table, and
execution of SQL statements.
Furthermore, it demonstrates the process of querying data from the Movie
table.\s

Upon completion of the program, all AWS resources are cleaned up.
""");

System.out.println("Lets get started...");
System.out.println("Please enter your user name (default is awsuser)");
String user = scanner.nextLine();
userName = user.isEmpty() ? "awsuser" : user;
System.out.println(DASHES);
System.out.println("Please enter your user password (default is
AwsUser1000)");
String userpass = scanner.nextLine();
userPassword = userpass.isEmpty() ? "AwsUser1000" : userpass;
System.out.println(DASHES);

System.out.println(DASHES);
System.out.println("A Redshift cluster refers to the collection of
computing resources and storage that work together to process and analyze large
volumes of data.");
System.out.println("Enter a cluster id value (default is redshift-
cluster-movies): ");
String userClusterId = scanner.nextLine();
String clusterId = userClusterId.isEmpty() ? "redshift-cluster-movies" :
userClusterId;
createCluster(redshiftClient, clusterId, userName, userPassword);
System.out.println(DASHES);

System.out.println(DASHES);
System.out.println("Wait until "+clusterId+" is available.");
System.out.print("Press Enter to continue...");
```

```
scanner.nextLine();
waitForClusterReady(redshiftClient, clusterId);
System.out.println(DASHES);

System.out.println(DASHES);
String databaseInfo = ""
    When you created $clusteridD, the dev database is created by default
and used in this scenario.\s

    To create a custom database, you need to have a CREATEDB privilege.\s
    For more information, see the documentation here: https://docs.aws.amazon.com/redshift/latest/dg/r\_CREATE\_DATABASE.html.
    """.replace("$clusteridD", clusterId);

System.out.println(databaseInfo);
System.out.print("Press Enter to continue...");
scanner.nextLine();
System.out.println(DASHES);

System.out.println(DASHES);
System.out.println("List databases in "+clusterId);
System.out.print("Press Enter to continue...");
scanner.nextLine();
listAllDatabases(redshiftDataClient, clusterId, userName, databaseName);
System.out.println(DASHES);

System.out.println(DASHES);
System.out.println("Now you will create a table named Movies.");
System.out.print("Press Enter to continue...");
scanner.nextLine();
createTable(redshiftDataClient, clusterId, databaseName, userName);
System.out.println(DASHES);

System.out.println(DASHES);
System.out.println("Populate the Movies table using the Movies.json
file.");
System.out.println("Specify the number of records you would like to add
to the Movies Table.");
System.out.println("Please enter a value between 50 and 200.");
int numRecords;
do {
    System.out.print("Enter a value: ");
    while (!scanner.hasNextInt()) {
```

```
        System.out.println("Invalid input. Please enter a value between
50 and 200.");
        System.out.print("Enter a year: ");
        scanner.next();
    }
    numRecords = scanner.nextInt();
} while (numRecords < 50 || numRecords > 200);
popTable(redshiftDataClient, clusterId, databaseName, userName,
jsonFilePath, numRecords);
System.out.println(DASHES);

System.out.println(DASHES);
System.out.println("Query the Movies table by year. Enter a value between
2012-2014.");
int movieYear;
do {
    System.out.print("Enter a year: ");
    while (!scanner.hasNextInt()) {
        System.out.println("Invalid input. Please enter a valid year
between 2012 and 2014.");
        System.out.print("Enter a year: ");
        scanner.next();
    }
    movieYear = scanner.nextInt();
    scanner.nextLine();
} while (movieYear < 2012 || movieYear > 2014);

String id = queryMoviesByYear(redshiftDataClient, databaseName, userName,
movieYear, clusterId);
System.out.println("The identifier of the statement is " + id);
checkStatement(redshiftDataClient, id);
getResults(redshiftDataClient, id);
System.out.println(DASHES);

System.out.println(DASHES);
System.out.println("Now you will modify the Redshift cluster.");
System.out.print("Press Enter to continue...");
scanner.nextLine();
modifyCluster(redshiftClient, clusterId);
System.out.println(DASHES);

System.out.println(DASHES);
System.out.println("Would you like to delete the Amazon Redshift cluster?
(y/n)");
```

```
String delAns = scanner.nextLine().trim();
if (delAns.equalsIgnoreCase("y")) {
    System.out.println("You selected to delete " +clusterId);
    System.out.print("Press Enter to continue...");
    scanner.nextLine();
    deleteRedshiftCluster(redshiftClient, clusterId);
} else {
    System.out.println("The "+clusterId +" was not deleted");
}
System.out.println(DASHES);

System.out.println(DASHES);
System.out.println("This concludes the Amazon Redshift SDK Getting
Started scenario.");
System.out.println(DASHES);
}

public static void listAllDatabases(RedshiftDataClient redshiftDataClient,
String clusterId, String dbUser, String database) {
    try {
        ListDatabasesRequest databasesRequest =
ListDatabasesRequest.builder()
            .clusterIdentifier(clusterId)
            .dbUser(dbUser)
            .database(database)
            .build();

        ListDatabasesIterable listDatabasesIterable =
redshiftDataClient.listDatabasesPaginator(databasesRequest);
        listDatabasesIterable.stream()
            .flatMap(r -> r.databases().stream())
            .forEach(db -> System.out
                .println("The database name is : " + db));

    } catch (RedshiftDataException e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}

public static void deleteRedshiftCluster(RedshiftClient redshiftClient,
String clusterId) {
    try {
```

```

        DeleteClusterRequest deleteClusterRequest =
DeleteClusterRequest.builder()
        .clusterIdentifier(clusterId)
        .skipFinalClusterSnapshot(true)
        .build();

        DeleteClusterResponse response =
redshiftClient.deleteCluster(deleteClusterRequest);
        System.out.println("The status is " +
response.cluster().clusterStatus());

    } catch (RedshiftException e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}

public static void popTable(RedshiftDataClient redshiftDataClient, String
clusterId, String databaseName, String userName, String fileName, int number)
throws IOException {
    JsonParser parser = new JsonFactory().createParser(new File(fileName));
    com.fasterxml.jackson.databind.JsonNode rootNode = new
ObjectMapper().readTree(parser);
    Iterator<JsonNode> iter = rootNode.iterator();
    ObjectNode currentNode;
    int t = 0;
    while (iter.hasNext()) {
        if (t == number)
            break;
        currentNode = (ObjectNode) iter.next();
        int year = currentNode.get("year").asInt();
        String title = currentNode.get("title").asText();

        // Use SqlParameter to avoid SQL injection.
        List<SqlParameter> parameterList = new ArrayList<>();
        String sqlStatement = "INSERT INTO Movies
VALUES( :id , :title, :year);";

        // Create the parameters.
        SqlParameter idParam = SqlParameter.builder()
            .name("id")
            .value(String.valueOf(t))
            .build();

```



```
        SqlParameter titleParam= SqlParameter.builder()
            .name("title")
            .value(title)
            .build();

        SqlParameter yearParam = SqlParameter.builder()
            .name("year")
            .value(String.valueOf(year))
            .build();
        parameterList.add(idParam);
        parameterList.add(titleParam);
        parameterList.add(yearParam);

        try {
            ExecuteStatementRequest insertStatementRequest =
ExecuteStatementRequest.builder()
                .clusterIdentifier(clusterId)
                .sql(sqlStatement)
                .database(databaseName)
                .dbUser(userName)
                .parameters(parameterList)
                .build();

            redshiftDataClient.executeStatement(insertStatementRequest);
            System.out.println("Inserted: " + title + " (" + year + ")");
            t++;

        } catch (RedshiftDataException e) {
            System.err.println("Error inserting data: " + e.getMessage());
            System.exit(1);
        }
    }
    System.out.println(t + " records were added to the Movies table. ");
}

public static void checkStatement(RedshiftDataClient redshiftDataClient,
String sqlId) {
    try {
        DescribeStatementRequest statementRequest =
DescribeStatementRequest.builder()
            .id(sqlId)
            .build();

        String status;
```

```
        while (true) {
            DescribeStatementResponse response =
redshiftDataClient.describeStatement(statementRequest);
            status = response.statusAsString();
            System.out.println("..." + status);

            if (status.compareTo("FAILED") == 0 ) {
                System.out.println("The Query Failed. Ending program");
                System.exit(1);

            } else if (status.compareTo("FINISHED") == 0) {
                break;
            }
            TimeUnit.SECONDS.sleep(1);
        }

        System.out.println("The statement is finished!");

    } catch (RedshiftDataException | InterruptedException e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}

public static void modifyCluster(RedshiftClient redshiftClient, String
clusterId) {
    try {
        ModifyClusterRequest modifyClusterRequest =
ModifyClusterRequest.builder()
            .clusterIdentifier(clusterId)
            .preferredMaintenanceWindow("wed:07:30-wed:08:00")
            .build();

        ModifyClusterResponse clusterResponse =
redshiftClient.modifyCluster(modifyClusterRequest);
        System.out.println("The modified cluster was successfully modified
and has "
            + clusterResponse.cluster().preferredMaintenanceWindow() + " as
the maintenance window");

    } catch (RedshiftException e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}
```

```
}

public static String queryMoviesByYear(RedshiftDataClient redshiftDataClient,
                                       String database,
                                       String dbUser,
                                       int year,
                                       String clusterId) {

    try {
        String sqlStatement = " SELECT * FROM Movies WHERE year = :year";
        SqlParameter yearParam= SqlParameter.builder()
            .name("year")
            .value(String.valueOf(year))
            .build();

        ExecuteStatementRequest statementRequest =
ExecuteStatementRequest.builder()
            .clusterIdentifier(clusterId)
            .database(database)
            .dbUser(dbUser)
            .parameters(yearParam)
            .sql(sqlStatement)
            .build();

        ExecuteStatementResponse response =
redshiftDataClient.executeStatement(statementRequest);
        return response.id();

    } catch (RedshiftDataException e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
    return "";
}

public static void getResults(RedshiftDataClient redshiftDataClient, String
statementId) {
    try {
        GetStatementResultRequest resultRequest =
GetStatementResultRequest.builder()
            .id(statementId)
            .build();

        // Extract and print the field values using streams.
```

```
        GetStatementResultResponse response =
redshiftDataClient.getStatementResult(resultRequest);
        response.records().stream()
            .flatMap(List::stream)
            .map(Field::stringValue)
            .filter(value -> value != null)
            .forEach(value -> System.out.println("The Movie title field is "
+ value));

    } catch (RedshiftDataException e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}

public static void waitForClusterReady(RedshiftClient redshiftClient, String
clusterId) {
    boolean clusterReady = false;
    String clusterReadyStr;
    System.out.println("Waiting for cluster to become available. This may
take a few mins.");
    try {
        DescribeClustersRequest clustersRequest =
DescribeClustersRequest.builder()
            .clusterIdentifier(clusterId)
            .build();
        long startTime = System.currentTimeMillis();

        // Loop until the cluster is ready.
        while (!clusterReady) {
            DescribeClustersResponse clusterResponse =
redshiftClient.describeClusters(clustersRequest);
            List<Cluster> clusterList = clusterResponse.clusters();
            for (Cluster cluster : clusterList) {
                clusterReadyStr = cluster.clusterStatus();
                if (clusterReadyStr.contains("available"))
                    clusterReady = true;
                else {
                    long elapsedTimeMillis = System.currentTimeMillis() -
startTime;

                    long elapsedSeconds = elapsedTimeMillis / 1000;
                    long minutes = elapsedSeconds / 60;
                    long seconds = elapsedSeconds % 60;
```

```
        System.out.printf("Elapsed Time: %02d:%02d - Waiting for
cluster... %n", minutes, seconds);
        TimeUnit.SECONDS.sleep(5);
    }
}

long elapsedTimeMillis = System.currentTimeMillis() - startTime;
long elapsedSeconds = elapsedTimeMillis / 1000;
long minutes = elapsedSeconds / 60;
long seconds = elapsedSeconds % 60;

System.out.println(String.format("Cluster is available! Total Elapsed
Time: %02d:%02d", minutes, seconds));

} catch (RedshiftException | InterruptedException e) {
    System.err.println(e.getMessage());
    System.exit(1);
}

}

public static void createTable(RedshiftDataClient redshiftDataClient, String
clusterId, String databaseName, String userName) {
    try {
        ExecuteStatementRequest createTableRequest =
ExecuteStatementRequest.builder()
            .clusterIdentifier(clusterId)
            .dbUser(userName)
            .database(databaseName)
            .sql("CREATE TABLE Movies ("
                + "id INT PRIMARY KEY, "
                + "title VARCHAR(100), "
                + "year INT)")
            .build();

        redshiftDataClient.executeStatement(createTableRequest);
        System.out.println("Table created: Movies");

    } catch (RedshiftDataException e) {
        System.err.println("Error creating table: " + e.getMessage());
        System.exit(1);
    }
}
```

```
public static void createCluster(RedshiftClient redshiftClient, String
clusterId, String masterUsername,
                                String masterUserPassword) {
    try {
        CreateClusterRequest clusterRequest = CreateClusterRequest.builder()
            .clusterIdentifier(clusterId)
            .masterUsername(masterUsername)
            .masterUserPassword(masterUserPassword)
            .nodeType("ra3.4xlarge")
            .publiclyAccessible(true)
            .numberOfNodes(2)
            .build();

        CreateClusterResponse clusterResponse =
redshiftClient.createCluster(clusterRequest);
        System.out.println("Created cluster " +
clusterResponse.cluster().clusterIdentifier());

    } catch (RedshiftException e) {

        System.err.println(e.getMessage());
        System.exit(1);
    }
}
}
```

- 如需 API 詳細資訊，請參閱《AWS SDK for Java 2.x API 參考》中的下列主題。
 - [createCluster](#)
 - [描述叢集](#)
 - [描述聲明](#)
 - [執行陳述式](#)
 - [得到 StatementResult](#)
 - [列表 DatabasesPaginator](#)
 - [修改叢集](#)

Python

適用於 Python (Boto3) 的 SDK

Note

還有更多關於 GitHub。尋找完整範例，並了解如何在[AWS 設定和執行程式碼範例儲存庫](#)。

```
class RedshiftScenario:
    """Runs an interactive scenario that shows how to get started with
    Redshift."""

    def __init__(self, redshift_wrapper, redshift_data_wrapper):
        self.redshift_wrapper = redshift_wrapper
        self.redshift_data_wrapper = redshift_data_wrapper

    def redshift_scenario(self, json_file_path):
        database_name = "dev"

        print(DASHES)
        print("Welcome to the Amazon Redshift SDK Getting Started example.")
        print(
            """
            This Python program demonstrates how to interact with Amazon Redshift
            using the AWS SDK for Python (Boto3).

            Amazon Redshift is a fully managed, petabyte-scale data warehouse
            service hosted in the cloud.

            The program's primary functionalities include cluster creation,
            verification of cluster readiness, listing databases, table creation,
            populating data within the table, and executing SQL statements.

            It also demonstrates querying data from the Movies table.

            Upon completion, all AWS resources are cleaned up.
            """
        )
        if not os.path.isfile(json_file_path):
            logging.error(f"The file {json_file_path} does not exist.")
```

```
        return

    print("Let's get started...")
    user_name = q.ask("Please enter your user name (default is awsuser):")
    user_name = user_name if user_name else "awsuser"

    print(DASHES)
    user_password = q.ask(
        "Please enter your user password (default is AwsUser1000):"
    )
    user_password = user_password if user_password else "AwsUser1000"

    print(DASHES)
    print(
        """A Redshift cluster refers to the collection of computing resources
and storage that work
        together to process and analyze large volumes of data."""
    )
    cluster_id = q.ask(
        "Enter a cluster identifier value (default is redshift-cluster-
movies): "
    )
    cluster_id = cluster_id if cluster_id else "redshift-cluster-movies"

    self.redshift_wrapper.create_cluster(
        cluster_id, "ra3.4xlarge", user_name, user_password, True, 2
    )

    print(DASHES)
    print(f"Wait until {cluster_id} is available. This may take a few
minutes...")
    q.ask("Press Enter to continue...")

    self.wait_cluster_available(cluster_id)

    print(DASHES)

    print(
        f"""
        When you created {cluster_id}, the dev database is created by default and
used in this scenario.

        To create a custom database, you need to have a CREATEDB privilege.
For more information, see the documentation here:
```



```
https://docs.aws.amazon.com/redshift/latest/dg/r_CREATE_DATABASE.html.
"""
)
q.ask("Press Enter to continue...")
print(DASHES)

print(DASHES)
print(f"List databases in {cluster_id}")
q.ask("Press Enter to continue...")
databases = self.redshift_data_wrapper.list_databases(
    cluster_id, database_name, user_name
)
print(f"The cluster contains {len(databases)} database(s).")
for database in databases:
    print(f"    Database: {database}")
print(DASHES)

print(DASHES)
print("Now you will create a table named Movies.")
q.ask("Press Enter to continue...")

self.create_table(cluster_id, database_name, user_name)

print(DASHES)

print("Populate the Movies table using the Movies.json file.")
print(
    "Specify the number of records you would like to add to the Movies
Table."
)
print("Please enter a value between 50 and 200.")

while True:
    try:
        num_records = int(q.ask("Enter a value: ", q.is_int))
        if 50 <= num_records <= 200:
            break
        else:
            print("Invalid input. Please enter a value between 50 and
200.")
    except ValueError:
        print("Invalid input. Please enter a value between 50 and 200.")

self.populate_table(
```

```
        cluster_id, database_name, user_name, json_file_path, num_records
    )

    print(DASHES)
    print("Query the Movies table by year. Enter a value between 2012-2014.")

    while True:
        movie_year = int(q.ask("Enter a year: ", q.is_int))
        if 2012 <= movie_year <= 2014:
            break
        else:
            print("Invalid input. Please enter a valid year between 2012 and
2014.")

    # Function to query database
    sql_id = self.query_movies_by_year(
        database_name, user_name, movie_year, cluster_id
    )

    print(f"The identifier of the statement is {sql_id}")

    print("Checking statement status...")
    self.wait_statement_finished(sql_id)
    result = self.redshift_data_wrapper.get_statement_result(sql_id)

    self.display_movies(result)

    print(DASHES)

    print(DASHES)
    print("Now you will modify the Redshift cluster.")
    q.ask("Press Enter to continue...")

    preferred_maintenance_window = "wed:07:30-wed:08:00"
    self.redshift_wrapper.modify_cluster(cluster_id,
preferred_maintenance_window)

    print(DASHES)

    print(DASHES)
    delete = q.ask("Do you want to delete the cluster? (y/n) ", q.is_yesno)

    if delete:
        print(f"You selected to delete {cluster_id}")
```

```
        q.ask("Press Enter to continue...")
        self.redshift_wrapper.delete_cluster(cluster_id)
    else:
        print(f"Cluster {cluster_id}cluster_id was not deleted")

    print(DASHES)
    print("This concludes the Amazon Redshift SDK Getting Started scenario.")
    print(DASHES)

def create_table(self, cluster_id, database, username):
    self.redshift_data_wrapper.execute_statement(
        cluster_identifier=cluster_id,
        database_name=database,
        user_name=username,
        sql="CREATE TABLE Movies (statement_id INT PRIMARY KEY, title
VARCHAR(100), year INT)",
    )

    print("Table created: Movies")

def populate_table(self, cluster_id, database, username, file_name, number):
    with open(file_name) as f:
        data = json.load(f)

    i = 0
    for record in data:
        if i == number:
            break

        statement_id = i
        title = record["title"]
        year = record["year"]
        i = i + 1
        parameters = [
            {"name": "statement_id", "value": str(statement_id)},
            {"name": "title", "value": title},
            {"name": "year", "value": str(year)},
        ]

        self.redshift_data_wrapper.execute_statement(
            cluster_identifier=cluster_id,
            database_name=database,
            user_name=username,
```

```
        sql="INSERT INTO Movies VALUES(:statement_id, :title, :year)",
        parameter_list=parameters,
    )

    print(f"{i} records inserted into Movies table")

def wait_cluster_available(self, cluster_id):
    """
    Waits for a cluster to be available.

    :param cluster_id: The cluster identifier.

    Note: The cluster_available waiter can also be used.
    It is not used in this case to allow an elapsed time message.
    """
    cluster_ready = False
    start_time = time.time()

    while not cluster_ready:
        time.sleep(30)
        cluster = self.redshift_wrapper.describe_clusters(cluster_id)
        status = cluster[0]["ClusterStatus"]
        if status == "available":
            cluster_ready = True
        elif status != "creating":
            raise Exception(
                f"Cluster {cluster_id} creation failed with status {status}."
            )

        elapsed_seconds = int(round(time.time() - start_time))
        minutes = int(elapsed_seconds // 60)
        seconds = int(elapsed_seconds % 60)

        print(f"Elapsed Time: {minutes}:{seconds:02d} - status {status}...")

        if minutes > 30:
            raise Exception(
                f"Cluster {cluster_id} is not available after 30 minutes."
            )

def query_movies_by_year(self, database, username, year, cluster_id):
    sql = "SELECT * FROM Movies WHERE year = :year"

    params = [{"name": "year", "value": str(year)}]
```

```
response = self.redshift_data_wrapper.execute_statement(
    cluster_identifier=cluster_id,
    database_name=database,
    user_name=username,
    sql=sql,
    parameter_list=params,
)

return response["Id"]

@staticmethod
def display_movies(response):
    metadata = response["ColumnMetadata"]
    records = response["Records"]

    title_column_index = None
    for i in range(len(metadata)):
        if metadata[i]["name"] == "title":
            title_column_index = i
            break

    if title_column_index is None:
        print("No title column found.")
        return

    print(f"Found {len(records)} movie(s).")
    for record in records:
        print(f"    {record[title_column_index]['stringValue']}")

def wait_statement_finished(self, sql_id):
    while True:
        time.sleep(1)
        response = self.redshift_data_wrapper.describe_statement(sql_id)
        status = response["Status"]
        print(f"Statement status is {status}.")

        if status == "FAILED":
            print(f"The query failed because {response['Error']}. Ending
program")
            raise Exception("The Query Failed. Ending program")
        elif status == "FINISHED":
            break
```

顯示場景實現的主要功能。

```
def main():
    redshift_client = boto3.client("redshift")
    redshift_data_client = boto3.client("redshift-data")
    redshift_wrapper = RedshiftWrapper(redshift_client)
    redshift_data_wrapper = RedshiftDataWrapper(redshift_data_client)
    redshift_scenario = RedshiftScenario(redshift_wrapper, redshift_data_wrapper)
    redshift_scenario.redshift_scenario(
        f"{os.path.dirname(__file__)}/../../resources/sample_files/
movies.json"
    )
```

在場景中使用的包裝函數。

```
def create_cluster(
    self,
    cluster_identifier,
    node_type,
    master_username,
    master_user_password,
    publicly_accessible,
    number_of_nodes,
):
    """
    Creates a cluster.

    :param cluster_identifier: The name of the cluster.
    :param node_type: The type of node in the cluster.
    :param master_username: The master username.
    :param master_user_password: The master user password.
    :param publicly_accessible: Whether the cluster is publicly accessible.
    :param number_of_nodes: The number of nodes in the cluster.
    :return: The cluster.
    """

    try:
```

```
        cluster = self.client.create_cluster(
            ClusterIdentifier=cluster_identifier,
            NodeType=node_type,
            MasterUsername=master_username,
            MasterUserPassword=master_user_password,
            PubliclyAccessible=publicly_accessible,
            NumberOfNodes=number_of_nodes,
        )
        return cluster
    except ClientError as err:
        logging.error(
            "Couldn't create a cluster. Here's why: %s: %s",
            err.response["Error"]["Code"],
            err.response["Error"]["Message"],
        )
        raise

def describe_clusters(self, cluster_identifier):
    """
    Describes a cluster.

    :param cluster_identifier: The cluster identifier.
    :return: A list of clusters.
    """
    try:
        kwargs = {}
        if cluster_identifier:
            kwargs["ClusterIdentifier"] = cluster_identifier

        paginator = self.client.get_paginator("describe_clusters")
        clusters = []
        for page in paginator.paginate(**kwargs):
            clusters.extend(page["Clusters"])

        return clusters

    except ClientError as err:
        logging.error(
            "Couldn't describe a cluster. Here's why: %s: %s",
            err.response["Error"]["Code"],
            err.response["Error"]["Message"],
        )
        raise
```

```
def execute_statement(
    self, cluster_identifier, database_name, user_name, sql,
    parameter_list=None
):
    """
    Executes a SQL statement.

    :param cluster_identifier: The cluster identifier.
    :param database_name: The database name.
    :param user_name: The user's name.
    :param sql: The SQL statement.
    :param parameter_list: The optional SQL statement parameters.
    :return: The SQL statement result.
    """

    try:
        kwargs = {
            "ClusterIdentifier": cluster_identifier,
            "Database": database_name,
            "DbUser": user_name,
            "Sql": sql,
        }
        if parameter_list:
            kwargs["Parameters"] = parameter_list
        response = self.client.execute_statement(**kwargs)
        return response
    except ClientError as err:
        logging.error(
            "Couldn't execute statement. Here's why: %s: %s",
            err.response["Error"]["Code"],
            err.response["Error"]["Message"],
        )
        raise

def describe_statement(self, statement_id):
    """
    Describes a SQL statement.

    :param statement_id: The SQL statement identifier.
    :return: The SQL statement result.
    """
```



```
    try:
        response = self.client.describe_statement(Id=statement_id)
        return response
    except ClientError as err:
        logging.error(
            "Couldn't describe statement. Here's why: %s: %s",
            err.response["Error"]["Code"],
            err.response["Error"]["Message"],
        )
        raise

def get_statement_result(self, statement_id):
    """
    Gets the result of a SQL statement.

    :param statement_id: The SQL statement identifier.
    :return: The SQL statement result.
    """
    try:
        result = {
            "Records": [],
        }
        paginator = self.client.get_paginator("get_statement_result")
        for page in paginator.paginate(Id=statement_id):
            if "ColumnMetadata" not in result:
                result["ColumnMetadata"] = page["ColumnMetadata"]
            result["Records"].extend(page["Records"])
        return result
    except ClientError as err:
        logging.error(
            "Couldn't get statement result. Here's why: %s: %s",
            err.response["Error"]["Code"],
            err.response["Error"]["Message"],
        )
        raise

def modify_cluster(self, cluster_identifier, preferred_maintenance_window):
    """
    Modifies a cluster.

    :param cluster_identifier: The cluster identifier.
    :param preferred_maintenance_window: The preferred maintenance window.
```

```
"""
try:
    self.client.modify_cluster(
        ClusterIdentifier=cluster_identifier,
        PreferredMaintenanceWindow=preferred_maintenance_window,
    )
except ClientError as err:
    logging.error(
        "Couldn't modify a cluster. Here's why: %s: %s",
        err.response["Error"]["Code"],
        err.response["Error"]["Message"],
    )
    raise

def list_databases(self, cluster_identifier, database_name, database_user):
    """
    Lists databases in a cluster.

    :param cluster_identifier: The cluster identifier.
    :param database_name: The database name.
    :param database_user: The database user.
    :return: The list of databases.
    """
    try:
        paginator = self.client.get_paginator("list_databases")
        databases = []
        for page in paginator.paginate(
            ClusterIdentifier=cluster_identifier,
            Database=database_name,
            DbUser=database_user,
        ):
            databases.extend(page["Databases"])

        return databases
    except ClientError as err:
        logging.error(
            "Couldn't list databases. Here's why: %s: %s",
            err.response["Error"]["Code"],
            err.response["Error"]["Message"],
        )
        raise
```

```
def delete_cluster(self, cluster_identifier):
    """
    Deletes a cluster.

    :param cluster_identifier: The cluster identifier.
    """
    try:
        self.client.delete_cluster(
            ClusterIdentifier=cluster_identifier,
            SkipFinalClusterSnapshot=True
        )
    except ClientError as err:
        logging.error(
            "Couldn't delete a cluster. Here's why: %s: %s",
            err.response["Error"]["Code"],
            err.response["Error"]["Message"],
        )
        raise
```

- 如需 API 的詳細資訊，請參閱《適用於 Python (Boto3) 的 AWS SDK API 參考資料》中的下列主題。
 - [createCluster](#)
 - [描述叢集](#)
 - [描述聲明](#)
 - [執行陳述式](#)
 - [得到 StatementResult](#)
 - [列表 DatabasesPaginator](#)
 - [修改叢集](#)

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱[搭配 AWS SDK 使用此服務](#)。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

使用軟體開發套件的 Amazon Redshift 跨服務範例 AWS

下列範例應用程式使用 AWS 開發套件將 Amazon Redshift 與其他應用程式結合在一起。AWS 服務每個範例都包含一個連結 GitHub，您可以在其中找到如何設定和執行應用程式的指示。

範例

- [建立 Amazon Redshift 項目追蹤器](#)

建立 Amazon Redshift 項目追蹤器

下列程式碼範例說明如何使用 Amazon Redshift 資料庫建立可追蹤和報告工作項目的 Web 應用程式。

Java

適用於 Java 2.x 的 SDK

說明如何建立可追蹤和報告存放在 Amazon Redshift 資料庫中的工作項目的 Web 應用程式。

如需有關如何設定 Spring REST API 以查詢 Amazon Redshift 資料以及供 React 應用程式使用的完整原始程式碼和說明，請參閱上[GitHub](#)的完整範例。

此範例中使用的服務

- Amazon Redshift
- Amazon SES

Kotlin

適用於 Kotlin 的 SDK

說明如何建立可追蹤和報告存放在 Amazon Redshift 資料庫中的工作項目的 Web 應用程式。

如需有關如何設定 Spring REST API 以查詢 Amazon Redshift 資料以及供 React 應用程式使用的完整原始程式碼和說明，請參閱上[GitHub](#)的完整範例。

此範例中使用的服務

- Amazon Redshift
- Amazon SES

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱[搭配 AWS SDK 使用此服務](#)。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

文件歷史紀錄

Note

如需 Amazon Redshift 中新功能的說明，請參閱[新增功能](#)。

下表說明在 2018 年 6 月之後對 Amazon Redshift 管理指南進行的重要文件變更。如需有關此文件更新的通知，您可以訂閱 RSS 訂閱源。

API 版本：2012-12-01

如需《Amazon Redshift 資料庫開發人員指南》的變更清單，請參閱[Amazon Redshift 資料庫開發人員指南文件歷史記錄](#)。

如需新功能的相關資訊，包括每個版本的修正清單以及關聯的叢集版本號碼，請參閱[叢集版本歷史記錄](#)。

變更	描述	日期
Amazon Redshift 補丁 181 發布。	我們即將部署新的 Amazon Redshift 修補程式。新版本需要幾週的時間才能在所有支援 AWS 區域的 Amazon Redshift 中使用。如需有關此版本的詳細資訊，請參閱 Amazon Redshift 修補程式 181 。	2024年5月1日
更新查詢編輯器 v2 受管政策	更新AmazonRedshiftQueryEditorV2FullAccess、AmazonRedshiftQueryEditorV2NoSharing、AmazonRedshiftQueryEditorV2ReadSharing、和AmazonRedshiftQueryEditorV2ReadWrite	2024年2月21日

Sharing 受管理的策略，具有權限 `redshift-serverless:ListNamespaces` 和 `redshift-serverless:ListWorkgroups`。

[更新 Amazon Redshift 讀存取受管政策](#)

AmazonRedshiftReadOnlyAccess 受管政策的更新具有列 `redshift:ListRecommendations` 出 Amazon Redshift 顧問建議的權限。

2024年2月7日

[Amazon Redshift 修補程式 180 已發行。](#)

我們即將部署新的 Amazon Redshift 修補程式。新版本需要幾週的時間才能在所有支援 AWS 區域的 Amazon Redshift 中使用。如需此版本的詳細資訊，請參閱 [Amazon Redshift 修補程式 180](#)。

2023 年 12 月 29 日

[Amazon Redshift 修補程式 179 已發行。](#)

我們即將部署新的 Amazon Redshift 修補程式。新版本需要幾週的時間才能在所有支援 AWS 區域的 Amazon Redshift 中使用。如需此版本的詳細資訊，請參閱 [Amazon Redshift 修補程式 179](#)。

2023 年 11 月 9 日

[更新 Amazon Redshift 受管政策](#)

更新具有 `ec2:AssignIpv6Addresses` 和 `ec2:UnassignIpv6Addresses` 許可的 `AmazonRedshiftServiceLinkedRolePolicy` 受管政策。

2023 年 10 月 31 日

[Amazon Redshift 修補程式 178 已發行。](#)

我們即將部署新的 Amazon Redshift 修補程式。新版本需要幾週的時間才能在所有支援 AWS 區域的 Amazon Redshift 中使用。如需此版本的相關資訊，請參閱 [Amazon Redshift 修補程式 178](#)。

2023 年 9 月 25 日

[更新查詢編輯器 v2 受管政策](#)

更新具有 `sqlworkbench:GetAutocompletionMetadata` 和 `sqlworkbench:GetAutocompletionResource` 許可的 `AmazonRedshiftQueryEditorV2NoSharing`、`AmazonRedshiftQueryEditorV2ReadSharing` 和 `AmazonRedshiftQueryEditorV2ReadWriteSharing` 受管政策。

2023 年 8 月 16 日

[更新 Amazon Redshift 受管政策](#)

`AmazonRedshiftServiceLinkedRolePolicy` 受管理原則的更新，以授與建立和管理系統管理認證密碼的權限。AWS Secrets Manager

2023 年 8 月 14 日

[Amazon Redshift 修補程式 177 已發行。](#)

我們即將部署新的 Amazon Redshift 修補程式。新版本需要幾週的時間才能在所有支援 AWS 區域的 Amazon Redshift 中使用。如需此版本的相關資訊，請參閱 [Amazon Redshift 修補程式 177](#)。

2023 年 8 月 3 日

[Amazon Redshift 修補程式 176 已發行。](#)

我們即將部署新的 Amazon Redshift 修補程式。新版本需要幾週的時間才能在所有支援 AWS 區域的 Amazon Redshift 中使用。如需此版本的相關資訊，請參閱 [Amazon Redshift 修補程式 176](#)。

2023 年 6 月 8 日

[Amazon Redshift 修補程式 175 已發行。](#)

我們即將部署新的 Amazon Redshift 修補程式。新版本需要幾週的時間才能在所有支援 AWS 區域的 Amazon Redshift 中使用。如需此版本的相關資訊，請參閱 [Amazon Redshift 修補程式 175](#)。

2023 年 4 月 28 日

[更新 Amazon Redshift 受管政策](#)

更新 AmazonRedshiftServiceLinkedRolePolicy 受管政策，以移除 ec2 網路相關動作的許可。這些特別與目的:RedshiftMigrateToVpc 資源標籤相關聯。

2023 年 4 月 27 日

[更新 Amazon Redshift 資料 API 受管政策](#)

更新具有 redshift:GetClusterCredentialsWithIAM 許可的 AmazonRedshiftDataFullAccess 受管政策。

2023 年 4 月 7 日

[更新查詢編輯器 v2 受管政策](#)

更新具有 sqlworkbench:GetSchemaInference 許可的 AmazonRedshiftQueryEditorV2NoSharing 、AmazonRedshiftQueryEditorV2ReadSharing 和 AmazonRedshiftQueryEditorV2ReadWriteSharing 受管政策。

2023 年 3 月 21 日

[Amazon Redshift 修補程式 174 已發行。](#)

我們即將部署新的 Amazon Redshift 修補程式。新版本需要幾週的時間才能在所有支援 AWS 區域的 Amazon Redshift 中使用。如需此版本的相關資訊，請參閱 [Amazon Redshift 修補程式 174](#)。

2023 年 3 月 11 日

[更新查詢編輯器 v2 受管政策](#)

更新具有 sqlworkbench:AssociateNotebookWithTab 許可的 AmazonRedshiftQueryEditorV2NoSharing 、AmazonRedshiftQueryEditorV2ReadSharing 和 AmazonRedshiftQueryEditorV2ReadWriteSharing 受管政策。

2023 年 2 月 2 日

[Amazon Redshift 修補程式 173 已發行。](#)

我們即將部署新的 Amazon Redshift 修補程式。新版本需要幾週的時間才能在所有支援 AWS 區域的 Amazon Redshift 中使用。如需此版本的相關資訊，請參閱 [Amazon Redshift 修補程式 173](#)。

2023 年 1 月 20 日

[Amazon Redshift 修補程式 172 已發行。](#)

我們即將部署新的 Amazon Redshift 修補程式。新版本需要幾週的時間才能在所有支援 AWS 區域的 Amazon Redshift 中使用。如需此版本的相關資訊，請參閱 [Amazon Redshift 修補程式 172](#)。

2022 年 11 月 17 日

[Amazon Redshift 修補程式 171 已發行。](#)

我們即將部署新的 Amazon Redshift 修補程式。新版本需要幾週的時間才能在所有支援 AWS 區域的 Amazon Redshift 中使用。如需此版本的相關資訊，請參閱 [Amazon Redshift 修補程式 171](#)。

2022 年 11 月 9 日

[Amazon Redshift 修補程式 170 已發行。](#)

我們即將部署新的 Amazon Redshift 修補程式。新版本需要幾週的時間才能在所有支援 AWS 區域的 Amazon Redshift 中使用。如需此版本的相關資訊，請參閱 [Amazon Redshift 修補程式 170](#)。

2022 年 7 月 20 日

[Amazon Redshift 修補程式 169 已發行。](#)

我們即將部署新的 Amazon Redshift 修補程式。新版本需要幾週的時間才能在所有支援 AWS 區域的 Amazon Redshift 中使用。如需此版本的相關資訊，請參閱 [Amazon Redshift 修補程式 169](#)。

2022 年 6 月 8 日

[Amazon Redshift 修補程式 168 已發行。](#)

我們即將部署新的 Amazon Redshift 修補程式。新版本需要幾週的時間才能在所有支援 AWS 區域的 Amazon Redshift 中使用。如需此版本的相關資訊，請參閱 [Amazon Redshift 修補程式 168](#)。

2022 年 4 月 19 日

[針對 Amazon Redshift 驅動程式支援身分驗證設定檔](#)

您現在可以使用身分驗證設定檔來連線至 Amazon Redshift。

2021 年 8 月 2 日

[Support 跨 VPC 端點的 Amazon Redshift \(由下列項目提供支援\) AWS PrivateLink](#)

您現在可以將 Redshift 管理的 VPC 端點與 Amazon Redshift 搭配使用。

2021 年 4 月 1 日

[支援 Amazon Redshift 查詢編輯器增強功能](#)

您現在可以使用具有增強的 VPC 路由、更長的查詢執行時間和更多叢集節點類型的查詢編輯器。

2021 年 2 月 17 日

[支援與合作夥伴進行主控台整合](#)

您可以使用 Amazon Redshift 主控台來與合作夥伴進行整合。

2020 年 12 月 9 日

[支援在可用區域之間移動叢集的功能](#)

您現在可以在可用區域之間移動 RA3 叢集。

2020 年 12 月 9 日

[支援 ra3.xlplus 節點類型](#)

您現在可以建立 ra3.xlplus 節點類型。

2020 年 12 月 9 日

支援 JDBC 驅動程式 2.0	您現在可以設定 JDBC 驅動程式 2.0 版了。	2020 年 11 月 5 日
支援 Lambda UDF 和字符化	您現在可以撰寫 Lambda UDF 來啟用資料的外部記號化。	2020 年 10 月 26 日
支援排程 SQL 陳述式的執行	您現在可以在 Amazon Redshift 主控台上排程查詢。	2020 年 10 月 22 日
支援 Amazon Redshift 資料 API	您現在可以使用內建的資料 API 來存取 Amazon Redshift。文件更新包括《Amazon Redshift 資料 API 參考》。	2020 年 9 月 10 日
支援 Amazon Redshift 主控台查詢監控	更新指南，描述新的查詢監控圖表。	2020 年 5 月 7 日
支援用量限制	更新指南，說明用量限制。	2020 年 4 月 23 日
多重要素驗證	更新指南，描述多重要素驗證支援。	2020 年 4 月 20 日
彈性調整大小現在支援節點類型變更	更新彈性調整大小說明。	2020 年 4 月 6 日
支援具有受管儲存的 ra3.4xlarge 節點類型	更新指南，加入 ra3.4xlarge 節點類型。	2020 年 4 月 2 日
支援暫停和繼續	更新指南以描述暫停和繼續叢集操作。	2020 年 3 月 11 日
支援 Microsoft Azure AD 作為身分提供者	已更新指南，說明以 Microsoft Azure AD 作為身分提供者的步驟。	2020 年 2 月 10 日
支援 RA3 節點類型	更新指南，說明新的 RA3 節點類型。	2019 年 12 月 3 日

支援新主控台	更新指南以說明新的 Amazon Redshift 主控台。	2019 年 11 月 11 日
安全資訊更新	更新安全資訊文件。	2019 年 6 月 24 日
快照增強功能	Amazon Redshift 現可支援多項增強功能以管理和排程快照。 。	2019 年 4 月 4 日
並行擴展	您可以設定工作負載管理 (WLM) 以啟用並行擴展模式。如需詳細資訊，請參閱 設定工作負載管理 。	2019 年 3 月 21 日
已更新 JDBC 和 ODBC 驅動程式	Amazon Redshift 現在支援 JDBC 和 ODBC 驅動程式的新版本。如需詳細資訊，請參閱 設定 JDBC 連線 和 設定與 ODBC 連線 。	2019 年 2 月 4 日
延遲維護	如果您需要重新排程叢集的維護時段，您可以選擇將維護延遲最多 14 天。在延遲期間，如果我們需要更新硬體或進行必要的更新，我們會通知您並進行所需的變更。在這些更新期間，您的叢集無法使用。如需詳細資訊，請參閱 延遲維護 。	2018 年 11 月 20 日

[事先通知](#)

Amazon Redshift 會事先提供某些事件的通知。這些事件的事件類別為 pending。例如，如果叢集的其中一個節點要硬體更新，我們會傳送事先通知。如同其他 Amazon Redshift 事件一樣，您也可以訂閱待定事件。如需詳細資訊，請參閱[訂閱 Amazon Redshift 事件通知](#)。

2018 年 11 月 20 日

[彈性調整大小](#)

彈性調整大小是調整叢集大小最快的方法。彈性調整大小會在現有叢集上新增或移除節點，然後自動將資料重新配送到新節點。彈性調整大小操作不會建立新叢集，通常在幾分鐘之內就很快完成。如需詳細資訊，請參閱[調整叢集大小](#)。

2018 年 11 月 15 日

[新的 ODBC 驅動程式](#)

Amazon Redshift ODBC 驅動程式已更新為 1.4.3.1000 版。如需詳細資訊，請參閱[設定 ODBC 連線](#)。

2018 年 11 月 8 日

[取消調整大小操作](#)

您現在可以取消正在進行的調整大小操作。如需詳細資訊，請參閱[調整大小操作概觀](#)。

2018 年 11 月 2 日

[修改叢集來變更加密](#)

您可以使用 AWS-managed 金鑰或客戶管理的金鑰，修改未加密的叢集以使用 AWS Key Management Service (AWS KMS) 加密。當您修改叢集以啟用 KMS 加密時，Amazon Redshift 會自動將資料遷移到新的加密叢集。您也可以經由修改叢集，將未加密的叢集遷移到加密的叢集。

2018 年 10 月 16 日

[Amazon Redshift Spectrum 支援增強型 VPC 路由](#)

您現在可以針對叢集使用已啟用增強型 VPC 路由的 Redshift Spectrum。您可能需要執行額外的設定步驟。如需詳細資訊，請參閱[使用 Amazon Redshift Spectrum 搭配增強型 VPC 路由](#)。

2018 年 10 月 10 日

[查詢編輯器](#)

您現在可以從 Amazon Redshift 管理主控台執行 SQL 查詢。

2018 年 10 月 4 日

[工作負載執行明細圖表](#)

您現在可以在主控台查看工作負載執行明細圖表，以取得工作負載效能的詳細檢視。如需詳細資訊，請參閱[分析工作負載效能](#)。

2018 年 7 月 30 日

[維護追蹤](#)

您現在可以選擇維護追蹤，以查明您的叢集一律會更新為最新版的 Amazon Redshift 或以前的版本。如需詳細資訊，請參閱[選擇叢集維護軌道](#)。

2018 年 7 月 26 日

下表描述 2018 年 7 月前《Amazon Redshift 管理指南》的重要變更。

變更	描述	發行日期
新 CloudWatch 量度	添加了用於監視查詢性能的新 CloudWatch 指標。如需更多資訊，請參閱 使 CloudWatch 用指標監控 Amazon Redshift	2018 年 5 月 17 日
HSM 加密	Amazon Redshift 僅支援硬體 AWS CloudHSM 安全模組 (HSM) 金鑰管理。如需詳細資訊，請參閱 Amazon Redshift 資料庫加密 。	2018 年 3 月 6 日
IAM 角色鏈結	如果連接至叢集的 IAM 角色無法存取必要資源，您可鏈結其他角色，該角色甚至可以來自其他帳戶。您的叢集接著會暫時擔任鏈結的角色，以存取資料。您也可以用鏈結角色的方式來授予跨帳戶存取。鏈結中的每個角色都會擔任鏈結中的下一個角色，直到叢集擔任鏈結尾端的角色為止。您最多可以鏈結 10 個角色。如需詳細資訊，請參閱 在 Amazon Redshift 中鏈結 IAM 角色 。	2018 年 2 月 23 日
新的 DC2 節點類型	新一代的密集運算 (DC) 節點類型提供比 DC1 更好的效能，且價格不變。若要利用這項效能提升，可以將 DC1 叢集遷移到較新的 DC2 節點類型。如需詳細資訊，請參閱 Amazon Redshift 中的叢集和節點 。	2017 年 10 月 17 日
ACM 憑證	Amazon Redshift 正在使用 AWS Certificate Manager (ACM) 發行的憑證取代叢集上的 SSL 憑證。ACM 是大多數現行系統信任的公有憑證授權機構 (CA)。您可能需要更新目前的信任根 CA 憑證，才能繼續使用 SSL 連線到叢集。如需詳細資訊，請參閱 將 SSL 連線轉換為使用 ACM 憑證 。	2017 年 9 月 18 日
服務連結角色	服務連結角色是直接連結至 Amazon Redshift 的一種特殊 IAM 角色類型。服務連結角色是由 Amazon Redshift 預先定義的，並包含該服務代表 Amazon Redshift 叢集呼叫 AWS 服務所需的所有許可。如需詳細資訊，請參閱 使用 Amazon Redshift 的服務連結角色 。	2017 年 9 月 18 日
IAM 資料庫使用者身分驗證	您可以將系統設定為允許使用者建立使用者登入資料，並根據其 IAM 登入資料登入資料庫。您也可以設定系統	2017 年 8 月 11 日

變更	描述	發行日期
	<p>，讓使用者透過符合 SAML 2.0 的身分提供者使用聯合單一登入進行登入。如需詳細資訊，請參閱 使用 IAM 身分驗證產生資料庫使用者憑證。</p>	
資料表層級還原支援增強型 VPC 路由	<p>使用 增強型 VPC 路由 的叢集現在支援資料表層級的還原。如需詳細資訊，請參閱 從快照還原資料表。</p>	2017 年 7 月 19 日
查詢監控規則	<p>使用 WLM 查詢監控規則，您可以為 WLM 查詢定義以指標為基礎的效能邊界，並指定在查詢超出那些邊界時 (日誌記錄、跳轉或中止)，要採取何種動作。請將查詢監控規則定義為工作負載管理 (WLM) 組態的一部分。如需詳細資訊，請參閱 設定工作負載管理。</p>	2017 年 4 月 21 日
增強型 VPC 路由	<p>當您使用 Amazon Redshift 增強型 VPC 路由時，Amazon Redshift 會強制叢集與資料儲存庫之間所有的 COPY 與 UNLOAD 流量通過您的 Amazon VPC。如需詳細資訊，請參閱 Amazon Redshift 中的增強型 VPC 路由。</p>	2016 年 9 月 15 日
新的連線日誌欄位	<p>連線日誌 稽核日誌有兩個新的欄位可追蹤 SSL 連線。如果您定期將稽核日誌載入 Amazon Redshift 資料表，則需要將以下新欄位新增到目標資料表：sslcompression 和 ssllexpansion。</p>	2016 年 5 月 5 日
新的 ODBC 驅動程式	<p>Amazon Redshift ODBC 驅動程式已更新為 1.2.7.1007 版。如需詳細資訊，請參閱 設定 ODBC 連線。</p>	2016 年 3 月 30 日
可進行 COPY 和 UNLOAD 的 IAM 角色	<p>您現在可以指定叢集可用於驗證以存取其他 AWS 服務的一或多個 AWS Identity and Access Management (IAM) 角色。IAM 角色提供更安全的替代方法，可利用 COPY、UNLOAD 或 CREATE LIBRARY 命令提供身分驗證。如需詳細資訊，請參閱 授權 Amazon Redshift 代表您訪問其他 AWS 服務 及 使用 IAM 角色授權 COPY、UNLOAD、CREATE EXTERNAL FUNCTION 和 CREATE EXTERNAL SCHEMA 操作。</p>	2016 年 3 月 29 日

變更	描述	發行日期
從資料表還原	您可以從叢集快照將資料表還原至作用中叢集的新資料表。如需詳細資訊，請參閱 從快照還原資料表 。	2016 年 3 月 10 日
在政策中使用 IAM 條件	您可以在 IAM 政策中使用 Condition 元素，進一步限制對資源的存取。如需詳細資訊，請參閱 使用 IAM 政策條件進行精細定義存取控制 。	2015 年 12 月 10 日
修改是否可公開存取	您可以修改 VPC 中的現有叢集，變更是否可公開存取該叢集。如需詳細資訊，請參閱 修改叢集 。	2015 年 11 月 20 日
文件修正	發佈多項文件修正。	2015 年 8 月 28 日
文件更新	已更新有關網路設定的故障排除指南，以確保具有不同最大傳輸單位 (MTU) 大小的主機，可以決定連線的封包大小。如需詳細資訊，請參閱 查詢似乎沒有回應且有時無法觸達叢集 。	2015 年 8 月 25 日
文件更新	已修訂有關參數群組的整個小節，使內容更有組織也更清楚。如需詳細資訊，請參閱 Amazon Redshift 參數群組 。	2015 年 8 月 17 日
WLM 動態屬性	WLM 組態參數現在支援動態套用部分屬性。其他屬性仍然是靜態變更，需要將關聯的叢集重新啟動才會套用組態變更。如需詳細資訊，請參閱 WLM 動態和靜態屬性 及 Amazon Redshift 參數群組 。	2015 年 8 月 3 日
將 KMS 加密叢集複製到其他 AWS 區域	已新增有關設定快照複製授權以允許將 AWS KMS 加密叢集複製到另一個 AWS 區域的內容。如需詳細資訊，請參閱 複製 AWS KMS— 加密的快照到另一個 AWS 區域 。	2015 年 7 月 28 日
文件更新	更新了資料庫加密部分，以更好地說明 Amazon Redshift 如何使用 AWS KMS 或 HSM 來管理金鑰，以及加密程序如何與這些選項搭配使用。如需詳細資訊，請參閱 Amazon Redshift 資料庫加密 。	2015 年 7 月 28 日

變更	描述	發行日期
新的節點類型	Amazon Redshift 現在提供了新的節點類型：DS2。已更新對現有節點類型的文件參考，以使用此版本中介紹的新名稱。也已修訂節點類型組合的小節，不但解釋更清楚，並闡明預設配額限制。如需詳細資訊，請參閱 Amazon Redshift 中的叢集和節點 。	2015 年 6 月 9 日
預留節點優惠	新增有關新的預留節點方案的內容。也已修訂可用方案的小節，更清楚解釋並加以比較，同時提供範例來示範隨需和預留節點定價如何影響計費。如需詳細資訊，請參閱 概觀 。	2015 年 6 月 9 日
新的 ODBC 驅動程式	Amazon Redshift ODBC 驅動程式已更新。新增小節來說明這些驅動程式的先前版本，以及這些驅動程式的版本備註連結。如需詳細資訊，請參閱 設定 ODBC 連線 。	2015 年 6 月 5 日
文件修正	發佈多項文件修正。	2015 年 4 月 30 日
新功能	此版本的 Amazon Redshift 引進最適合與 Amazon Redshift 搭配使用的新的 ODBC 和 JDBC 驅動程式。如需詳細資訊，請參閱 使用 SQL 用戶端工具連接至 Amazon Redshift 資料倉儲 。	2015 年 2 月 26 日
新功能	此版本的 Amazon Redshift 引進叢集效能指標，可讓您檢視及分析查詢執行的詳細資訊。如需詳細資訊，請參閱 檢視查詢和載入 。	2015 年 2 月 26 日
文件更新	新增範例政策，示範授與 Amazon Redshift 所依賴的常見 AWS 服務動作和資源的權限。如需詳細資訊，請參閱 客戶受管政策範例 。	2015 年 1 月 16 日
文件更新	已更新有關設定最大傳輸單位 (MTU) 以停用 TCP/IP 巨型訊框的指南。如需詳細資訊，請參閱 在建立叢集時使用 EC2-VPC 及查詢似乎沒有回應且有時無法觸達叢集 。	2015 年 1 月 16 日

變更	描述	發行日期
文件更新	已修訂有關 <code>wlm_json_configuration</code> 參數的內容，並提供範例語法，以便在 Linux、Mac OS X 和 Microsoft 視窗作業系統 AWS CLI 上使用來設定此參數。如需詳細資訊，請參閱 設定工作負載管理 。	2015 年 1 月 13 日
文件更新	新增遺失事件通知和說明的內容。如需詳細資訊，請參閱 Amazon Redshift 事件類別和事件訊息 。	2015 年 1 月 8 日
文件更新	更新有關 Amazon Redshift 動作和資源的 IAM 政策指導。已修訂該小節使內容更有組織更清楚。如需詳細資訊，請參閱 Amazon Redshift 中的安全 。	2014 年 11 月 21 日
新功能	這個版本的 Amazon Redshift 引入了使用加密金鑰 AWS Key Management Service (AWS KMS) 來加密叢集的功能。AWS KMS 結合安全、高可用性的硬體和軟體，提供專為雲端擴充的金鑰管理系統。如需有關 Amazon Redshift AWS KMS 和加密選項的詳細資訊，請參閱 Amazon Redshift 資料庫加密 和 使用主控台管理叢集 。	2014 年 11 月 12 日
新功能	此版本 Amazon Redshift 引進可以標記資源 (如叢集、快照) 的功能。標記可讓您提供用戶定義的中繼資料，能根據成本分配來分類帳單報告，並幫助您更容易快速識別資源。如需詳細資訊，請參閱 在 Amazon Redshift 中標記資源 。	2014 年 11 月 4 日
新功能	已將 <code>dw1.8xlarge</code> 和 <code>dw2.8xlarge</code> 節點大小的節點上限增加到 128 個節點。如需詳細資訊，請參閱 Amazon Redshift 中的叢集和節點 。	2014 年 10 月 30 日
文件更新	新增 Microsoft Visual C ++ 2010 可轉散發套件的連結，它是 Amazon Redshift 使用 PostgreSQL ODBC 驅動程式所需的元件。如需詳細資訊，請參閱 在 Microsoft Windows 上安裝並設定 Amazon Redshift ODBC 驅動程式 。	2014 年 10 月 30 日

變更	描述	發行日期
新功能	新增從 Amazon Redshift 主控台終止查詢和載入的功能。如需詳細資訊，請參閱 檢視查詢和載入 及 檢視載入操作期間的叢集指標 。	2014 年 10 月 28 日
文件修正	發佈多項文件修正。	2014 年 10 月 17 日
新內容	新增有關關閉叢集和刪除叢集的內容。如需詳細資訊，請參閱 關閉及刪除叢集 及 刪除叢集 。	2014 年 8 月 14 日
文件更新	闡明叢集 Allow Version Upgrade (允許版本升級) 設定的行為。如需詳細資訊，請參閱 Amazon Redshift 概述 。	2014 年 8 月 14 日
文件更新	已修訂在 Amazon Redshift 主控台中處理叢集的程序、螢幕擷取畫面和主題組織。如需詳細資訊，請參閱 使用主控台管理叢集 。	2014 年 7 月 11 日
新內容	新增有關調整 Amazon Redshift 叢集大小的新教學課程，包括如何在調整叢集大小的同時，使叢集處於唯讀模式的時間縮到最短。如需詳細資訊，請參閱 調整叢集大小 。	2014 年 6 月 27 日
新功能	新增重新命名叢集的功能。如需詳細資訊，請參閱 重新命名叢集 及 修改叢集 。	2014 年 6 月 2 日
文件更新	已更新 .NET 程式碼範例，以便在使用 .NET 以程式設計方式連線到叢集時，使用 ODBC 資料提供者。如需詳細資訊，請參閱 以程式設計方式 Connect 到資料倉 。	2014 年 5 月 15 日
新功能	新增選項，可在從快照還原叢集時，選取不同的參數群組和安全群組。如需詳細資訊，請參閱 從快照還原叢集 。	2014 年 5 月 12 日

變更	描述	發行日期
新功能	已新增新章節，說明如何設定預設 Amazon CloudWatch 警示，以監控 Amazon Redshift 叢集中使用的磁碟空間百分比。此警示是叢集建立程序中的新選項。如需詳細資訊，請參閱 預設磁碟空間警示 。	2014 年 4 月 28 日
文件更新	闡明 Amazon Redshift 中的 Elliptic curve Diffie—Hellman Exchange (ECDHE) 支援的相關資訊。如需詳細資訊，請參閱 使用 SSL 連線 。	2014 年 4 月 22 日
新功能	新增有關 Amazon Redshift 對 Elliptic curve Diffie—Hellman (ECDH) 金鑰協議通訊協定的支援敘述。如需詳細資訊，請參閱 使用 SSL 連線 。	2014 年 4 月 18 日
文件更新	修訂並重新組織 使用 SQL 用戶端工具連接至 Amazon Redshift 資料倉儲 小節中的主題。新增有關 JDBC 和 ODBC 連線的更多資訊，並新增小節來描述連線問題的故障排除。	2014 年 4 月 15 日
文件更新	在指南中的 IAM 政策範例新增版本。	2014 年 4 月 3 日
文件更新	新增有關調整叢集大小時定價如何計算的資訊。如需詳細資訊，請參閱 購買 Amazon Redshift 預留節點 。	2014 年 4 月 2 日
新功能	新增介紹新參數 max_cursor_result_set_size 的小節，它可設定每個游標可以儲存的結果集大小上限 (以 MB 為單位)。此參數值也會影響叢集的並行作用中游標的數量。如需詳細資訊，請參閱 Amazon Redshift 參數群組 。	2014 年 3 月 28 日
新功能	新增有關 Cluster Version 欄位的說明，現在包括叢集引擎版本和資料庫修訂版號碼。如需詳細資訊，請參閱 Amazon Redshift 佈建叢集 。	2014 年 3 月 21 日
新功能	已更新調整大小程序，在叢集的 Status (狀態) 標籤上會顯示新的調整大小進度資訊。如需詳細資訊，請參閱 調整叢集大小 。	2014 年 3 月 21 日

變更	描述	發行日期
文件更新	重新組織並更新 什麼是 Amazon Redshift ? ，以及已修訂 Amazon Redshift 佈建叢集概觀 。發佈多項文件修正。	2014 年 2 月 21 日
新功能	為 Amazon Redshift 叢集新增新的節點類型和大小，並根據意見回饋重寫相關的叢集概觀主題，使內容更有組織更清楚。如需詳細資訊，請參閱 Amazon Redshift 佈建叢集 。	2014 年 1 月 23 日
新功能	新增新的資訊，有關虛擬私有雲端中的可公開存取 Amazon Redshift 叢集使用彈性 IP (EIP) 地址。如需 Amazon Redshift 中 EIP 的相關資訊，請參閱 管理 VPC 中的叢集 和 在 VPC 中建立叢集 。	2013 年 20 月 12 日
新功能	已新增有關 Amazon Redshift AWS CloudTrail 日誌的資訊。如需有關的 Amazon Redshift 支援的詳細資訊 CloudTrail，請參閱 使用記錄 CloudTrail 。	2013 年 13 月 12 日
新功能	新增有關新的使用者活動日誌及 Amazon Redshift 中資料庫稽核日誌記錄功能的 enable_user_activity_logging 資料庫參數的資訊。如需資料庫稽核日誌的相關資訊，請參閱 資料庫稽核記錄日誌 。如需這資料庫參數的相關資訊，請參閱 Amazon Redshift 參數群組 。	2013 年 6 月 12 日
新功能	已更新，說明將 Amazon Redshift 設定為自動將自動和手動快照複製到次要 AWS 區域。如需設定跨區域快照複本的相關資訊，請參閱 將快照複製到另一個 AWS 區域 。	2013 年 11 月 14 日
新功能	新增小節來描述 Amazon Redshift 對於連線和使用者活動的稽核記錄，以及將這些日誌存放在 Amazon S3 中。如需資料庫稽核日誌的相關資訊，請參閱 資料庫稽核記錄日誌 。	2013 年 11 月 11 日

變更	描述	發行日期
新功能	新增描述 Amazon Redshift 加密新功能的小節，包括管理硬體安全模組 (HSM) 中的加密金鑰和輪換加密金鑰。如需加密、HSM、金鑰輪換的相關資訊，請參閱 Amazon Redshift 資料庫加密 、 使用硬體安全模組的 Amazon Redshift 加密 及 Amazon Redshift 中的加密金鑰輪換 。	2013 年 11 月 11 日
新功能	更新來描述使用 Amazon SNS 發佈 Amazon Redshift 事件通知。如需 Amazon Redshift 事件通知的相關資訊，請參閱 Amazon Redshift 事件通知 。	2013 年 11 月 11 日
新功能	已更新內容，描述 IAM 資源層級許可。如需 Amazon Redshift IAM 許可的相關資訊，請參閱 Amazon Redshift 中的安全 。	2013 年 8 月 9 日
新功能	已更新內容，描述還原流程指標。如需詳細資訊，請參閱 從快照還原叢集 。	2013 年 8 月 9 日
新功能	已更新內容，描述叢集快照共用以及建立快照流程指標。如需詳細資訊，請參閱 共用快照 。	2013 年 7 月 17 日
文件修正	發佈多項文件修正。	2013 年 7 月 8 日
新的主控台畫面	更新了《Amazon Redshift 管理指南》以符合 Amazon Redshift 主控台的變更。	2013 年 22 月 4 日
新指南	這是《Amazon Redshift 管理指南》的第一版。	2013 年 2 月 14 日

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。