Oracle Database@AWS 使用者指南

Oracle Database@AWS

Oracle Database@AWS: Oracle Database@AWS 使用者指南

Table of Contents

什麼是 Oracle Database@AWS？

Oracle Database@AWS 是一項產品，可讓您存取 AWS 資料中心內由 Oracle Cloud Infrastructure (OCI) 管理的 Oracle Exadata 基礎設施。您可以遷移 Oracle Exadata 工作負載、與 上執行的應用程式建立低延遲連線 AWS，以及與 AWS 服務整合。您透過 取得單一發票 AWS Marketplace，這將計入 AWS 承諾和 Oracle Support 獎勵。

下圖顯示與託管 Oracle Exadata 基礎設施的 AWS 資料中心繫結的 OCI 區域的高階概觀。在 AWS 可用區域 (AZ) 中，您可以將 Amazon VPC 對等至繫結至資料中心的私有網路。透過對等這些網路，VPC 中的應用程式伺服器可以存取在 Oracle Exadata 基礎設施上執行的 Oracle 資料庫。

的功能 Oracle Database@AWS

透過 Oracle Database@AWS，您可以受益於下列功能：

將 Oracle Exadata 資料庫工作負載遷移至 AWS

使用 Oracle Database@AWS，您可以輕鬆地將 Oracle Exadata 工作負載遷移至 Oracle Exadata Database Service on Dedicated Infrastructure 或 Oracle Autonomous Database on Dedicated Exadata Infrastructure AWS。遷移提供最小的變更、完整的功能可用性、架構相容性，以及與內部部署 Exadata 部署相同的效能。您可以使用標準 Oracle 資料庫遷移工具，例如 Recovery Manager (RMAN)、Oracle Data Guard、可傳輸資料表空間、Oracle Data Pump、Oracle GoldenGate、AWS Database Migration Service 和 Oracle 零停機時間遷移。

減少應用程式延遲

您可以在 Oracle Exadata 與在 上執行的應用程式之間建立低延遲連線 AWS。中託管的應用程式鄰近性 AWS 可確保將網路延遲降至最低並改善效能。

透過資料統一進行創新

您可以使用零 ETL 整合來跨 Oracle 統一您的資料，並 AWS 進行分析、機器學習和生成式 AI，進而產生更深入的洞見並開發新的創新。透過使用 Amazon Redshift 進行零 ETL 整合，您可以對存放於 的交易資料啟用近乎即時的分析和機器學習 (ML) Oracle Database@AWS。

簡化管理和操作

您可以受益於 Oracle 與 之間的統一體驗 AWS ，以及協作支援、購買、管理和操作。您使用 Oracle Database 服務符合現有 AWS 承諾和 Oracle 授權利益的資格，例如 Oracle Support

Rewards。您可以使用熟悉 AWS 的工具和界面來購買、佈建和管理 Oracle Database@AWS 資源。您可以使用 AWS APIs、CLI 或 SDKs 來佈建和管理 資源。 AWS APIs 會呼叫佈建和管理資源所需的對應 OCI APIs。

與 AWS 服務的無縫整合

您可以與在相同環境中執行的 AWS 其他服務和應用程式整合。例如， 與 Amazon EC2、Amazon VPC 和 IAM Oracle Database@AWS 整合。您也可以 Oracle Database@AWS 整合 AWS 服務，例如用於監控的 Amazon CloudWatch 和用於事件管理的 Amazon EventBridge。對於資料庫備份，您可以使用 Amazon S3，其設計旨在超過 11 9 秒的耐用性。

相關 AWS 服務

Oracle Database@AWS 使用下列 服務來改善 Oracle 資料庫應用程式的可用性和可擴展性：

- Amazon EC2 — 提供可做為 Oracle 應用程式伺服器的虛擬伺服器。您可以設定負載平衡器，將流量路由到 EC2 應用程式伺服器。如需詳細資訊，請參閱《Amazon EC2 使用者指南》。
- Amazon Virtual Private Cloud (VPC) — 可讓您在已定義的邏輯隔離虛擬網路中啟動 AWS 資源。Oracle Exadata 基礎設施位於稱為 ODB 網路的特殊網路中，您可以對等至 VPC。然後，您可以在 VPC 中執行應用程式伺服器，並存取 Exadata 資料庫。如需詳細資訊，請參閱 Amazon VPC 使用者指南。
- Amazon VPC Lattice — 從 ODB 網路提供 Amazon S3 和 Oracle 受管備份等 AWS 服務的原生存取權。如需詳細資訊，請參閱什麼是 Amazon VPC Lattice？。
- Amazon CloudWatch — 提供 的監控服務 Oracle Database@AWS。OCI 會收集 Oracle Exadata 系統的指標資料，並將其傳送至 CloudWatch。如需詳細資訊，請參閱Oracle Database@AWS 使用 Amazon CloudWatch 進行監控。
- AWS Identity and Access Management (IAM) — 協助您安全地控制使用者對 Oracle Database@AWS 資源的存取。使用 IAM 控制誰可以使用您的 AWS 資源 （身分驗證），以及使用者可以使用哪些資源 （授權）。如需詳細資訊，請參閱的身分和存取管理 Oracle Database@AWS。
- AWS 分析服務 — 提供一組廣泛且符合成本效益的分析服務，協助您更快地從 Exadata 資料庫取得洞見。每個服務都是專為各種分析使用案例而打造，例如互動式分析、大數據處理、資料倉儲、即時分析、操作分析、儀表板和視覺化。如需詳細資訊，請參閱 上的分析 AWS。

存取 Oracle Database@AWS

您可以使用 建立、存取和管理 Oracle Database@AWS AWS 管理主控台。它提供您可以用來存取的 Web 界面 Oracle Database@AWS。

的定價 Oracle Database@AWS

您可以從 購買 Oracle Database@AWS 方案 AWS Marketplace。您首先會聯絡 Oracle 銷售代表。然後，Oracle AWS Marketplace 會根據私有定價協議，在 中為您提供優惠。您的 AWS 帳單會根據您的用量顯示費用。

當您的 Oracle 應用程式和 Oracle 資料庫託管在相同的可用區域 (AZ) 時，不會收取資料傳輸費用。標準資料傳輸費用適用於 AZs 之間的通訊。

使用零 ETL、Oracle 受管備份和 Amazon S3 等 Oracle Database@AWS 受管整合時，需要支付透過 VPC Lattice 共用和存取資源的標準資料處理費用。 Oracle Database@AWS 受管整合不收取每小時費用。如需詳細資訊，請參閱 Amazon VPC Lattice 定價。

後續步驟？

您現在可以開始建立您的 Oracle Database@AWS 資源。

1. 了解 Oracle Database@AWS 的運作方式。如需詳細資訊，請參閱Oracle Database@AWS 運作方式。

   > **Note**
   >
   > 如果您熟悉 AWS 和 Oracle Exadata，並想要立即開始使用，請略過此步驟。

2. Oracle Database@AWS 透過 請求 的私有優惠 AWS 管理主控台，然後接受優惠。如需詳細資訊，請參閱請求 Oracle Database@ 的私有優惠AWS。

   > **Note**
   >
   > 若要在此預覽中請求私有優惠，您必須聯絡 AWS ，將 AWS 帳戶 新增至允許清單。

3. 使用 AWS 主控台建立 ODB 網路、Oracle Exadata 基礎設施和 Exadata VM 叢集。使用 OCI 工具建立 Exadata 資料庫。如需詳細資訊，請參閱Oracle Database@ 入門AWS。

4. 與 AWS Resource Access Manager () 共用跨帳戶的資源AWS RAM。如需詳細資訊，請參閱使用信任帳戶中的共用 Oracle Database@AWS 資源。

Oracle Database@AWS 運作方式

Oracle Database@AWS 整合 Oracle Cloud Infrastructure (OCI) 與 AWS 雲端。在下列各節中，您可以了解此多雲端架構的關鍵元件。

Oracle Exadata Database Service on Dedicated Infrastructure 是一種提供 Exadata Database Machine 的 OCI 服務。Oracle Exadata Database Machine 是一種整合、預先設定和預先測試的完整堆疊平台，可用於企業資料中心。您可以使用 AWS 主控台、CLI 或 APIs，在 AWS 可用區域 (AZ) 中建立 Oracle Exadata 基礎設施和 VM 叢集。

在 中建立資源之後 AWS，您可以使用 OCI APIs來建立和管理 Oracle Exadata 資料庫。您互連至 Amazon VPC 的 ODB 網路可讓 Amazon EC2 應用程式伺服器存取您的 Exadata 資料庫。如此一來，Oracle Exadata 資料庫就會整合到環境中 AWS 。

下圖顯示 Oracle Database@AWS 架構。

OCI 子網站

Oracle Cloud Infrastructure 託管於 OCI 區域和可用性網域。OCI 區域由 OCI 可用性網域 (ADs) 組成，這些網域是 OCI 區域內隔離的資料中心叢集。OCI 子網站是將 OCI 可用性網域延伸到 AWS 區域中可用區域 (AZ) 的資料中心。Exadata 基礎設施邏輯上位於 OCI 區域，實際位於 AWS 區域。

的 OCI 子網站 Oracle Database@AWS 實際位於 AWS 資料中心。 AWS 託管 Exadata 基礎設施，而 OCI 會在資料中心內佈建和維護 Exadata 基礎設施硬體。您可以使用 AWS 主控台、CLI 或 APIs 來設定 Exadata 基礎設施、私有網路和 VM 叢集。您可以使用 Amazon EC2 和 Amazon VPC 等 AWS 服務，允許應用程式存取在基礎設施上執行的 Oracle Exadata 資料庫。

Oracle Exadata 基礎設施

Oracle Exadata 基礎設施是執行 Oracle Exadata 資料庫的資料庫伺服器和儲存伺服器的基礎架構。基礎設施位於 AWS 可用區域 (AZ)。若要在 Exadata 基礎設施上建立 VM 叢集，您可以使用 AWS 主控台、CLI 或 APIs。

Oracle Exadata 基礎設施分散在稱為資料庫伺服器的實體機器上。這些伺服器提供運算資源，類似於 Amazon EC2 專用伺服器。每個資料庫伺服器都會託管在 Hypervisor 上執行的一或多個虛擬機器 VMs)。如需說明這些關係的架構圖，請參閱專用基礎設施技術架構上的 Exadata Database Service。

當您在 Oracle Database@ 中建立 Exadata 基礎設施時AWS，您可以指定下列資訊：

- 資料庫伺服器總數
- 儲存伺服器總數
- Exadata 系統模型 (X11M)
- 託管基礎設施的 AZ （ 請參閱 支援的 區域 Oracle Database@AWS)

若要了解如何建立 Oracle Exadata 基礎設施，請參閱 步驟 2：在 中建立 Oracle Exadata 基礎設施 Oracle Database@AWS。

ODB 網路

ODB 網路是在 AWS 可用區域 (AZ) 中託管 OCI 基礎設施的私有隔離網路。ODB 網路包含 IP 地址的 CIDR 範圍。ODB 網路會直接映射至 OCI 子網站中存在的網路，因此可做為 AWS 和 OCI 之間的通訊方式。建立 Exadata VM 叢集時，您必須指定 ODB 網路 （ 請參閱 步驟 3：在 中建立 Exadata VM 叢集或自治 VM 叢集 Oracle Database@AWS)。

您可以使用 Oracle Database@AWS APIs 在 ODB 網路中佈建資源。ODB 網路由 管理 AWS，但您可以設定 ODB 互連連線，將 Amazon VPC 連線至 ODB 網路。如需詳細資訊，請參閱 enODB 對等互連。

當您建立 ODB 網路時，您可以指定下列資訊：

- 可用區域 — ODB 網路專屬於 AZ。

  您可以在下列 Oracle Database@AWS 中使用 AWS 區域：

  美國東部 (維吉尼亞北部)

  您可以使用 AZs 搭配實體 IDsuse1-az4和 use1-az6。

  美國西部 (奧勒岡)

  您可以使用 AZs 搭配實體 IDsusw2-az3和 usw2-az4。

  亞太地區 (東京)

  您可以使用 AZs 搭配實體 IDsapne1-az1和 apne1-az4。

美國東部 (俄亥俄)

您可以使用 AZs 搭配實體 IDsuse2-az1和 use2-az2。

歐洲 (法蘭克福)

您可以使用 AZs 搭配實體 IDseuc1-az1和 euc1-az2。

加拿大 (中部)

您可以使用 AZ 搭配實體 ID cac1-az4。

亞太地區 (悉尼)

您可以使用 AZ 搭配實體 ID apse2-az4。

若要尋找您帳戶中對應到上述實體 AZ IDs邏輯 AZ 名稱，請執行下列命令。

```
aws ec2 describe-availability-zones \
  --region us-east-1 \
  --query "AvailabilityZones[*].{ZoneName:ZoneName, ZoneId:ZoneId}" \
  --output table
```

- 用戶端 CIDR 地址 — ODB 網路需要 Exadata VM 叢集和自治 VM 叢集的用戶端子網路 CIDR。
- 備份 CIDR 地址 — ODB 網路需要備份子網路 CIDR，才能進行 VM 叢集的受管資料庫備份。Exadata VM 叢集可選擇備份子網路。
- AWS 服務整合 — 您可以設定 AWS 服務整合的網路路徑，例如 Amazon S3 和 Amazon Redshift 的零 ETL。如需詳細資訊，請參閱AWS 服務整合。

如需詳細資訊，請參閱步驟 1：在 中建立 ODB 網路 Oracle Database@AWS。

Virtual Private Cloud (VPC)

Virtual Private Cloud (VPC) 是您在 AWS 雲端中建立的虛擬網路。它在邏輯上與 AWS 雲端中的其他虛擬網路隔離，可讓您完全控制虛擬聯網環境，包括選擇您自己的 IP 地址範圍、建立子網路，以及路由表和網路閘道的組態。如需詳細資訊，請參閱什麼是 Amazon VPC？

您可以在 Amazon VPC 中啟動 Amazon EC2 執行個體。EC2 執行個體可以託管與 Oracle Exadata 資料庫通訊的應用程式伺服器。您可以管理和啟動應用程式伺服器，就像 VPC 中的任何其他 EC2 執行個體一樣。如需詳細資訊，請參閱什麼是 Amazon EC2？

根據預設，ODB 網路沒有與 VPCs連線。若要將 ODB 網路連接到現有的 AWS 基礎設施，請在 ODB 網路和一個 VPC 之間建立對等連線。您可以在建立 ODB 網路時指定 VPC。如需詳細資訊，請參閱步驟 1：在 中建立 ODB 網路 Oracle Database@AWS。

ODB 對等互連

ODB 對等互連是使用者建立的網路連線，可讓流量在 Amazon VPC 和 ODB 網路之間私下路由。VPC 與 ODB 網路之間有 1：1 的關係。在對等互連之後，VPC 中的 Amazon EC2 執行個體可以與 ODB 網路中的 Oracle Exadata 資料庫進行通訊，就像在相同的網路中一樣。

> **Note**
>
> ODB 對等互連與 VPC 對等互連不同，後者是兩個 VPCs的對等互連。

您可以在一個帳戶中對等 ODB 網路，並在另一個帳戶中對等 VPC AWS RAM。如果您與其他帳戶共用 ODB 網路，信任帳戶可以直接啟動對等互連。啟動 ODB 互連連線的帳戶擁有和管理連線。

您可以在建立或更新 ODB 互連連線時指定對等網路 CIDRs。透過這種方式，您可以控制對等 VPC 中的哪些子網路可以存取您的 ODB 網路。VPC 帳戶可以更新 CIDR 範圍，而不需要擁有 ODB 網路。如需詳細資訊，請參閱在 中設定 ODB 對等互連至 Amazon VPC Oracle Database@AWS。

VPC 中的資源可以跨越可用區域 (AZs)。在 ODB 網路中，資源繫結至單一 AZ。您可以在建立 ODB 網路時定義此可用區。

建立 ODB 對等互連

ODB 對等互連不是 ODB 網路的特徵，而是具有自己的 ID （字首為 `odbpcx-`) 和生命週期的獨立資源。您可以使用一組專用 APIs來管理對等連線。例如，您可以使用 Oracle Database@AWS console 或 `CreateOdbPeeringConnection` API 建立現有 ODB 網路的 ODB 對等互連。如需詳細資訊，請參閱在 Oracle Database@ 中建立 ODB 對等互連AWS。

當您建立 ODB 對等互連時，Oracle Database@ 會自動AWS 執行下列動作：

1. 驗證網路組態，包括檢查是否有與 Oracle VCN CIDR 重疊的 CIDR 區塊
2. 設定基礎網路對等互連基礎設施

3. 使用 VPC CIDR 地址設定 ODB 網路 （ 而非 VPC) 路由表

建立 ODB 對等互連後，請使用 Amazon EC2 `create-route`命令手動更新 VPC 路由表。如需詳細資訊，請參閱設定 ODB 對等互連的 VPC 路由表。

AWS 服務整合

為了為您的 Oracle 資料庫提供增強的功能和連線選項，Oracle Database@ AWS 服務 使用 Amazon VPC Lattice 與AWS 整合。您可以 AWS 服務 設定直接從 ODB 網路到 的網路路徑，而不需要額外的 VPCs或複雜的聯網設定。

Oracle Database@AWS 支援下列 AWS 受管服務整合：

Amazon S3

您可以透過AWS 下列方式將 Amazon S3 與 Oracle Database@ 整合：

- Oracle 受管自動備份至 Amazon S3 – Oracle Database@AWS 自動啟用自動備份的網路存取。無法停用此整合。如果您在 OCI 主控台中將 Amazon S3 設定為受管備份目標，則 OCI 會將自動備份上傳到 S3 儲存貯體。
- 從 ODB 網路直接存取 Amazon S3 – 您可以啟用對 S3 的直接 ODB 網路存取，然後將指令碼、匯入和匯出檔案以及相關檔案儲存在 S3 儲存貯體中。您可以停用此存取。此設定獨立於 Oracle 受管自動備份的自動網路存取。

與 Amazon Redshift 的零 ETL 整合

您可以啟用 ODB 網路與 Amazon Redshift 的零 ETL 整合。此整合可讓您從 Oracle Database@ 中執行的 Oracle 資料庫將資料複寫至 Amazon Redshift，AWS 而不需要傳統的擷取、轉換和載入 (ETL) 程序。此整合可透過自動同步 Oracle 資料與 Amazon Redshift，來啟用即時分析和 AI 工作負載。

除了 AWS 服務的受管整合之外，您也可以使用 VPC Lattice 來存取其他 VPCs中託管的服務和資源，或從 VPC 存取 ODB 網路執行個體。您可以使用 VPC Lattice 主控台、CLI 和 APIs 來管理存取和資源。如需詳細資訊，請參閱下列資源：

- 在 Oracle Database@ 中備份AWS
- Oracle Database@AWS Zero-ETL 與 Amazon Redshift 整合
- 什麼是 Amazon VPC Lattice？ 和 VPC Lattice for Oracle Database@AWS

從多個 VPCs路由流量

若要允許多個 VPCs 存取一個 ODB 網路中的 Oracle Database@AWS 資源，您可以使用 AWS Transit Gateway 或 AWS Cloud WAN。

AWS Transit Gateway

Amazon VPC 傳輸閘道是一種用於互連 VPCs和內部部署網路的網路傳輸中樞。ODB 網路僅支援 one-to-one直接對等互連。您可以將 ODB 網路對等至 VPC，然後將此 VPC 連接至傳輸閘道。閘道可以連接到多個 VPCs。使用此傳輸閘道組態，您可以將多個 VPC 子網路之間的流量路由到單一 ODB 網路。

如需詳細資訊，請參閱設定 的 Amazon VPC Transit Gateway Oracle Database@AWS。

AWS 雲端 WAN

AWS Cloud WAN 是一項受管廣域聯網 (WAN) 服務，可讓您建置、管理和監控跨雲端和內部部署環境的統一全球網路連線資源。使用中央儀表板，您可以連接 AWS 全球網路的內部部署分支辦公室、資料中心和 VPCs。

您可以將 ODB 網路對等至 VPC，然後將此 VPC 連接至 Cloud WAN 核心網路。透過此組態，您可以使用 Cloud WAN 在多個 VPCs或內部部署網路與 ODB 網路之間路由流量。如需詳細資訊，請參閱設定 的 AWS 雲端 WAN Oracle Database@AWS。

Exadata VM 叢集

Exadata VM 叢集是一組緊密耦合的 Exadata VMs。每個 VM 都有完整的 Oracle 資料庫安裝，其中包含 Oracle Enterprise Edition 的所有功能，包括 Oracle Real Application Clusters (Oracle RAC) 和 Oracle Grid Infrastructure。您可以在 VM 叢集上建立一或多個 Oracle Exadata 資料庫。如需顯示 VMs 和 VM 叢集架構的圖表，請參閱專用基礎設施技術架構上的 Exadata Database Service。

當您建立 VM 叢集時，您可以指定包含下列項目的資訊：

- ODB 網路
- Oracle Exadata 基礎設施
- 要在叢集中放置 VMs 的資料庫伺服器
- 可用的 Exadata 儲存總量

您可以為 VM 叢集中的每個 VM 設定 CPU 核心、記憶體和本機儲存。如需詳細資訊，請參閱步驟 3：在 中建立 Exadata VM 叢集或自治 VM 叢集 Oracle Database@AWS。

自治 VM 叢集

自治 VM 叢集是全受管資料庫，可使用機器學習和 AI 自動化金鑰管理任務。與傳統資料庫不同，自動資料庫會自動佈建、安全、更新、備份和調整資料庫，無需人工介入。

您可以設定每個 VM 的 ECPU 核心計數、每個 CPU 的資料庫記憶體、資料庫儲存，以及自動容器資料庫的最大數量。如需詳細資訊，請參閱步驟 3：在 中建立 Exadata VM 叢集或自治 VM 叢集 Oracle Database@AWS。

Oracle Exadata 資料庫

Oracle Exadata 是一種工程化系統，可提供執行 Oracle 資料庫的高效能平台。透過 Oracle Database@AWS，您可以使用 AWS 主控台來建立託管 Exadata 資料庫的 Oracle Exadata 基礎設施和 VM 叢集。然後，您可以使用 OCI APIs來建立和管理 Oracle 資料庫。如需詳細資訊，請參閱步驟 4：在 Oracle Cloud Infrastructure 中建立 Oracle Exadata 資料庫。

加入 Oracle Database@AWS

在您開始使用 之前 Oracle Database@AWS，請確定您已註冊 AWS 並建立必要的使用者。然後，您可以透過AWS AWS Marketplace 接受 Oracle 的私有優惠，從 購買 Oracle Database@。

註冊 AWS 帳戶

如果您沒有 AWS 帳戶，請完成下列步驟來建立一個。

註冊 AWS 帳戶

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

   部分註冊程序需接收來電或簡訊，並在電話鍵盤輸入驗證碼。

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

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

建立具有管理存取權的使用者

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

保護您的 AWS 帳戶根使用者

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

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

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

建立具有管理存取權的使用者

1. 啟用 IAM Identity Center。

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

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

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

以具有管理存取權的使用者身分登入

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

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

指派存取權給其他使用者

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

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

2. 將使用者指派至群組，然後對該群組指派單一登入存取權。

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

請求 Oracle Database@ 的私有優惠AWS

AWS Marketplace 賣方私有優惠功能可讓您向 Oracle 請求和接收 Oracle Database@AWS pricing 和 EULA 條款。您與 Oracle 協商定價和條款，然後 Oracle 為您 AWS 帳戶 指定的 建立私有優惠。您接受私有優惠，並收到協議價格和使用條款。此時，您可以使用 Oracle Database@AWS 儀表板。當私有優惠協議到期時，您會自動移至產品的公有定價，或取消訂閱 Oracle Database@AWS。如需私有優惠的詳細資訊，請參閱 中的私有優惠 AWS Marketplace。

請求和接受 的私有優惠 Oracle Database@AWS

1. 登入 AWS 管理主控台。

2. 搜尋 ，然後選擇 Oracle Database@AWS。
3. 選擇請求私有優惠。

> **Note**
>
> 在您接受私有優惠之前， Oracle Database@AWS 儀表板無法使用。

4. 在 Oracle Cloud Infrastructure (OCI) 網站上，指定區域和聯絡資訊等詳細資訊。
5. 等待 OCI 代表與您聯絡，並提供私有優惠。
6. 在 中 AWS 管理主控台，選擇檢視私有優惠。
7. 選擇優惠，然後選擇檢視優惠。
8. 選擇建立合約並回應後續提示以接受私有優惠。
9. 接受私有優惠後，您需要啟用 OCI 帳戶。您可以直接從 存取 Oracle 啟用連結 AWS 管理主控台。
    1. 在 主控台中，導覽至入門區段。
    2. 按一下 主控台中提供的 Oracle 啟用連結。或者，您也可以使用透過電子郵件傳送給您的啟用連結。
    3. 在 Oracle 啟用頁面上，選擇是否建立新的 Oracle 雲端帳戶或新增至現有帳戶。
    4. 依照畫面上的指示完成啟用程序。
    5. 提交啟用請求後，您會在 中看到啟用進行中狀態 AWS 管理主控台，而且儀表板會暫時停用，並顯示原因。
    6. 啟用完成後，Oracle Database@AWS dashboard 即可供使用，可讓您管理 資源。
10. 在 中 AWS 管理主控台，選擇儀表板。

在AWS 多個區域中訂閱 Oracle Database@

當您 Oracle Database@AWS 透過 訂閱 AWS Marketplace 並完成加入時，您的 AWS 帳戶 會連結至您的 OCI 租用。此連結以及相關資源會自動複寫到 Oracle Database@AWS 可用 的所有 AWS 區域。您訂閱並加入一次，而不是為每個區域重複此程序。

若要 Oracle Database@AWS 在多個區域中使用 ，請執行下列步驟：

1. 透過 訂閱 Oracle Database@AWS AWS Marketplace 並完成加入程序。

    當您第一次訂閱 Oracle Database@ 時AWS，您的帳戶會在主區域中啟用。您可以在 Oracle Cloud Infrastructure (OCI) 中指定主要區域。

2. 透過 OCI 主控台啟用您偏好的區域。

   如果您未在 OCI 中啟用區域，然後在 Oracle Database@AWS 主控台中切換到此區域，您會收到錯誤，指出您尚未訂閱。在此情況下，您必須先在 OCI 中啟用此區域，才能使用此區域中的 Oracle Database@AWS 儀表板。

3. Oracle Database@AWS 在任何支援的 AWS 區域中存取 ，無需重複訂閱程序。

Oracle Database@ 入門AWS

若要開始使用 Oracle Database@AWS，您可以使用 Oracle Database@AWS 主控台、CLI 或 APIs 建立下列資源：

1. ODB 網路
2. Oracle Exadata 基礎設施
3. Exadata VM 叢集或自治 VM 叢集
4. ODB 對等互連

若要在基礎設施上建立 Oracle Exadata 資料庫，您必須使用 Oracle Cloud Infrastructure (OCI) 主控台或 APIs而非 Oracle Database@AWS 儀表板。因此，您會在兩個雲端環境中部署資源：網路和基礎設施資源位於 AWS，而資料庫管理控制平面位於 OCI。如需詳細資訊，請參閱 Oracle Cloud Infrastructure 文件Oracle Database@AWS中的 。

設定 的先決條件 Oracle Database@AWS

在設定 Oracle Exadata 基礎設施之前，請務必執行下列動作：

- 請執行 加入 Oracle Database@AWS 中的步驟。您必須已接受要使用的私有優惠 Oracle Database@AWS。
- 授予 IAM 主體 中列出的政策許可允許使用者佈建 Oracle Database@AWS 資源。這些許可是使用的必要許可 Oracle Database@AWS。

上支援的 OCI 服務 Oracle Database@AWS

Oracle Database@AWS 支援下列 Oracle Cloud Infrastructure (OCI) 服務：

- Oracle Exadata Database Service on Dedicated Infrastructure – 提供可在其中存取的全受管專用 Exadata 環境 AWS。如需詳細資訊，請參閱 OCI 文件中的 Oracle Cloud Exadata Database Service on Dedicated Infrastructure。
- 專用 Exadata 基礎設施上的自治資料庫 – 提供高度自動化、全受管的資料庫環境，在 OCI 中執行，並具有遞交的硬體和軟體資源。如需詳細資訊，請參閱 OCI 文件中的關於專用 Exadata 基礎設施上的自治資料庫。

支援的 區域 Oracle Database@AWS

您可以在下列 Oracle Database@AWS 內容中使用 AWS 區域：

美國東部 (維吉尼亞北部)

您可以使用 AZs 搭配實體 IDsuse1-az4和 use1-az6。

美國西部 (奧勒岡)

您可以使用 AZs 搭配實體 IDsusw2-az3和 usw2-az4。

亞太地區 (東京)

您可以使用 AZs 搭配實體 IDsapne1-az1和 apne1-az4。

美國東部 (俄亥俄)

您可以使用 AZs 搭配實體 IDsuse2-az1和 use2-az2。

歐洲 (法蘭克福)

您可以使用 AZs 搭配實體 IDseuc1-az1和 euc1-az2。

加拿大 (中部)

您可以使用 AZ 搭配實體 ID cac1-az4。

亞太地區 (悉尼)

您可以使用 AZ 搭配實體 ID apse2-az4。

若要尋找您帳戶中對應到上述實體 AZ IDs邏輯 AZ 名稱，請執行下列命令。

```
aws ec2 describe-availability-zones \
  --region us-east-1 \
  --query "AvailabilityZones[*].{ZoneName:ZoneName, ZoneId:ZoneId}" \
  --output table
```

在 中規劃 IP 地址空間 Oracle Database@AWS

仔細規劃 IP 地址空間 Oracle Database@AWS。根據 VM 叢集的數量考慮 IP 地址使用，包括您可以佈建到 ODB 網路的每個叢集的 VMs 數量。如需詳細資訊，請參閱 Oracle Cloud Infrastructure 立方體中的 ODB 網路設計。

主題

ODB 網路中 IP 地址的限制

請注意有關 ODB 網路中 CIDR 範圍的下列限制：

- 您無法在建立 ODB 網路之後修改其用戶端或備份子網路 CIDR 範圍。
- 您無法在 IPv4 CIDR 區塊關聯限制的資料表中的受限制關聯欄中使用 VPC CIDR 範圍。 IPv4
- 對於 Exadata X9M，IP 地址 100.106.0.0/16 和 100.107.0.0/16 保留給由 OCI 自動化互連的叢集，因此您無法執行下列動作：
  - 將這些範圍指派給 ODB 網路的用戶端或備份 CIDR 範圍。
  - 針對用於連線至 ODB 網路的 VPC CIDR，請使用這些範圍。
- 下列 CIDR 範圍保留給 Oracle Cloud Infrastructure，無法用於 ODB 網路：
  - Oracle Cloud 預留範圍 CIDR 169.254.0.0/16
  - 預留類別 D 224.0.0.0 — 239.255.255.255
  - 預留類別 E 240.0.0.0 — 255.255.255.255
- 您無法重疊用戶端和備份子網路的 IP 地址 CIDR 範圍。
- 您無法將針對用戶端和備份子網路配置的 IP 地址 CIDR 範圍與用於連線至 ODB 網路的 VPC CIDR 範圍重疊。
- 您無法將 VMs 叢集中的 VM 佈建到不同的 ODB 網路。網路是 VM 叢集的屬性，這表示您只能將 VMs 叢集中的 VM 佈建至相同的 ODB 網路。

ODB 網路的用戶端子網路 CIDR 需求

在下表中，您可以找到 服務和基礎設施針對用戶端子網路 CIDR 使用的 IP 地址數量。用戶端子網路的最小 CIDR 大小為 /27，最大大小為 /16。

IP 地址數量	使用者	備註
6	Oracle Database@AWS	無論您在 ODB 網路中佈建多少 VM 叢集，都會保留這些 IP 地址。 Oracle Database@AWS 會使用下列項目： • 為 中的 ODB 網路資源預留的 3 個 IP 地址 AWS • 為 OCI 聯網服務保留的 3 個 IP 地址
3	每個 VM 叢集	無論每個 VMs有多少 VM，這些 IP 地址都會保留給單一用戶端存取名稱 (SCANs)。
4	每個 VM	這些 IP 地址僅取決於基礎設施中的 VMs 數量。

ODB 網路的備份子網路 CIDR 需求

在下表中，您可以找到 服務和基礎設施針對備份子網路 CIDR 使用的 IP 地址數量。備份子網路的最小 CIDR 大小為 /28，最大大小為 /16。

IP 地址數量	使用者	備註
3	Oracle Database@AWS	無論您在 ODB 網路中佈建多少 VM 叢集，都會保留這些 IP 地址。 Oracle Database@AWS 會使用下列項目： • CIDR 範圍開頭的 2 個 IP 地址 • CIDR 範圍結束時的 1 個 IP 地址
3	每個 VM	這些 IP 地址僅取決於基礎設施中的 VMs 數量。

ODB 網路的 IP 使用案例

在下表中，您可以查看 ODB 網路中用於不同 VM 叢集組態的 IP 地址。/28 是用戶端子網路 CIDR 部署 1 個具有 2 個 VM VMs 叢集的技術最低 CIDR 範圍，我們建議您至少使用 /27 CIDR 範圍。在此情況下，VM 叢集不會完全使用 IP 範圍，並允許配置其他 IP 地址。

Configuration	使用的用戶端 IPs	用戶端 IPs下限	使用的備份 IPs	備份 IPs下限
1 個具有 2 個 VM VMs 叢集	17 (6 個服務 + 3 個叢集 + 4*2)	32 (/27 CIDR 範圍)	9 (3 個服務 + 3*2)	16 (/28 CIDR 範圍)
1 個具有 3 個 VM VMs 叢集	21 (6 個服務 + 3 個叢集 + 4*3)	32 (/27 CIDR 範圍)	12 (3 個服務 + 3*3)	16 (/28 CIDR 範圍)
1 個具有 4 個 VM VMs 叢集	25 (6 個服務 + 3 個叢集 + 4*4)	32 (/27 CIDR 範圍)	15 (3 個服務 + 3*4)	16 (/28 CIDR 範圍)
1 個具有 8 個 VM VMs 叢集	41 (6 個服務 + 3 個叢集 + 4*8)	64 (/26 CIDR 範圍)	27 (3 個服務 + 3*8)	32 (/27 CIDR 範圍)

下表顯示針對特定用戶端 CIDR 範圍，每個組態的執行個體數量是可能的。例如，具有 4 個 VM 的 1 個 VMs 叢集會使用用戶端子網路中的 24 個 IP 地址。如果 CIDR 範圍為 /25，則有 128 個 IP 地址可用。因此，您可以在子網路中佈建 5 個 VM 叢集。

VM 叢集組態	具有 /27 的數字 (32 IPs)	具有 /26 (64 個 IPs數字	具有 /25 的數字 (128 IPs)	具有 /24 的數字 (256 IPs)	/23 (512 個 IPs時的數字	/22 (1024 個 IPs時的數字
1 個 VM 叢集與 2 VMs (16 IPs)	1	3	7	15	30	60
1 個 VM 叢集與 3 VMs (20 IPs)	1	3	6	12	24	48
1 個具有 4 個 VM 的 VMs 叢集 (24 IPs)	1	2	5	10	20	40
2 個 VM 叢集，每個 2 VMs (27 IPs)	1	2	4	9	18	36
2 個 VM 叢集，每個 3 VMs (35 IPs)	0	1	3	7	14	28

VM 叢集組態	具有 /27 的數字 (32 IPs)	具有 /26 (64 個 IPs數字	具有 /25 的數字 (128 IPs)	具有 /24 的數字 (256 IPs)	/23 (512 個 IPs時的數字	/22 (1024 個 IPs時的數字
2 個 VM 叢集，每個 4 VMs (43 IPs)	0	1	2	5	11	23

步驟 1：在 中建立 ODB 網路 Oracle Database@AWS

ODB 網路是在可用區域 (AZ) 中託管 OCI 基礎設施的私有隔離網路。ODB 網路和 Oracle Exadata 基礎設施是佈建 VM 叢集和建立 Exadata 資料庫的先決條件。您可以依任一順序建立 ODB 網路和 Oracle Exadata 基礎設施。如需詳細資訊，請參閱ODB 網路及ODB 對等互連。

此任務假設您已讀取 在 中規劃 IP 地址空間 Oracle Database@AWS。若要稍後修改或刪除 ODB 網路，請參閱 管理 Oracle Database@AWS。

建立 ODB 網路

1. 登入 AWS 管理主控台 ，並在 https：//https://console.aws.amazon.com/odb/ 開啟 Oracle Database@AWS 主控台。
2. 選擇右上角 AWS 的區域。如需詳細資訊，請參閱支援的 區域 Oracle Database@AWS。
3. 從左側窗格中，選擇 ODB 網路。
4. 選擇建立 ODB 網路。
5. 針對 ODB 網路名稱，輸入網路名稱。名稱必須為 1–255 個字元，並以字母字元或底線開頭。它不能包含連續連字號。
6. 針對可用區域，選擇 AZ 名稱。如需支援的 AZs，請參閱 支援的 區域 Oracle Database@AWS。
7. 針對用戶端子網路 CIDR，指定用戶端連線的 CIDR 範圍。如需詳細資訊，請參閱ODB 網路的用戶端子網路 CIDR 需求。
8. 針對備份子網路 CIDR，指定備份連線的 CIDR 範圍。若要隔離備份流量並改善彈性，建議您不要與備份 CIDR 和用戶端 CIDR 重疊。如需詳細資訊，請參閱ODB 網路的備份子網路 CIDR 需求。
9. 針對 DNS 組態，選擇下列其中一個選項：

預設

對於網域名稱字首，輸入要用作網域字首的名稱。網域名稱固定為 oraclevcn.com。例如，如果您輸入 **myhost**，則完整網域名稱為 myhost.oraclevcn.com。

自訂網域名稱

針對網域名稱，輸入完整的網域名稱。例如，您可以輸入 myhost.myodb.com。

10. （選用）對於服務整合，選擇使用 VPC Lattice 與您的網路整合的服務。Oracle Database@ 與各種AWS 整合 AWS 服務 ，為您的 Oracle 資料庫提供增強的功能和連線選項。選取下列任一整合：

    Amazon S3

    啟用 Amazon S3 的直接 ODB 網路存取。您的資料庫可以存取 S3 以進行資料匯入/匯出或自訂備份。您可以輸入 JSON 政策。如需詳細資訊，請參閱使用者受管備份至 Oracle Database@ 中的 Amazon S3 AWS。

    零 ETL

    使用 Amazon Redshift 啟用交易資料的即時分析和機器學習。如需詳細資訊，請參閱Oracle Database@AWS Zero-ETL 與 Amazon Redshift 整合。

    > **Note**
    >
    > 當您建立 ODB 網路時，Oracle Database@AWS 會自動預先設定 Oracle 受管備份對 Amazon S3 的網路存取。您無法啟用或停用此整合。如需詳細資訊，請參閱AWS 服務整合。

11. （選用）針對標籤，為網路輸入最多 50 個標籤。標籤是可用於組織和追蹤資源的鍵/值對。
12. 選擇建立 ODB 網路。

建立 ODB 網路之後，您可以將其對等至 VPC。ODB 對等互連是使用者建立的網路連線，可讓流量在 Amazon VPC 和 ODB 網路之間私下路由。對等互連後，VPC 內的 Amazon EC2 執行個體可以與 ODB 網路中的資源通訊，就像在相同的網路中一樣。如需詳細資訊，請參閱在 Oracle Database@ 中設定 ODB 對等互連至 Amazon VPC AWS。

步驟 2：在 中建立 Oracle Exadata 基礎設施 Oracle Database@AWS

Oracle Exadata 基礎設施是執行 Oracle Exadata 資料庫的資料庫伺服器、儲存伺服器和聯網的基礎架構。選擇 Exadata X9M 或 X11M 做為系統模型。然後，您可以使用 AWS 主控台在 Exadata 基礎設施上建立 VM 叢集。

您可以依任一順序建立 Oracle Exadata 基礎設施和 ODB 網路。建立基礎設施時，您不需要指定聯網資訊。

您無法在建立 Oracle Exadata 基礎設施之後對其進行修改。若要刪除 Exadata 基礎設施，請參閱 在中刪除 Oracle Exadata 基礎設施 Oracle Database@AWS。

建立 Exadata 基礎設施

1. 登入 AWS 管理主控台 並在 https：//https://console.aws.amazon.com/odb/ 開啟 Oracle Database@AWS 主控台。
2. 從左側窗格中，選擇 Exadata 基礎設施。
3. 選擇建立 Exadata 基礎設施。
4. 針對 Exadata 基礎設施名稱，輸入名稱。名稱必須為 1–255 個字元，並以字母字元或底線開頭。它不能包含連續連字號。
5. 針對可用區域，選擇其中一個支援的AZs。然後選擇下一步。
6. 針對 Exadata 系統模型，選擇 Exadata.X9M 或 Exadata.X11M。對於 Exadata.X11M，也請選擇下列伺服器類型：
   - 針對資料庫伺服器類型，選擇 Exadata 基礎設施的資料庫伺服器模型類型。目前，唯一的選擇是 X11M。
   - 針對儲存伺服器類型，選擇 Exadata 基礎設施的儲存伺服器模型類型。目前，唯一的選擇是 X11M-HC。
7. 對於資料庫伺服器，保留預設值 2 或移動滑桿以選擇最多 32 個伺服器。若要指定超過 2 個，請從 OCI 請求提高限制。

   每個 Exadata X9M 資料庫伺服器都支援 126 OCPUs。每個 Exadata X11M 資料庫伺服器都支援 760 ECPUs。總運算計數會隨著您變更伺服器的數量而變更。如需 OCPUs和 ECPUs 的詳細資訊，請參閱 Oracle 文件中的自治資料庫中的運算模型。

8. 對於儲存伺服器，保留預設值 3 或移動滑桿以選擇最多 64 個伺服器。若要指定超過 3 個，請從 OCI 請求提高限制。每個 X9M 儲存伺服器提供 64 TB。每個 X11m 儲存伺服器提供 80 TB。當您變更伺服器數量時，儲存體的總 TB 會變更。然後選擇下一步。
9. 針對維護時段，設定何時可以進行系統維護：
   a. 針對排程偏好設定，選取下列其中一個選項：
      - Oracle 受管排程 - Oracle 決定維護活動的最佳時間。
      - 客戶受管排程 - 您可以指定何時可進行維護活動。
   b. 針對修補模式，選取下列其中一個選項：
      - 滾動 - 一次將更新套用至一個節點，讓資料庫在修補期間保持可用。
      - 非滾動 - 更新會同時套用至所有節點，這可能需要停機時間。
   c. 如果您選取了客戶受管排程，請設定下列其他設定：
      - 針對維護月份，選取可執行維護的月份。
      - 針對當月的一週，選取當月的哪一週可以執行維護（第一個、第二個、第三個、第四個或最後一個）。
      - 對於星期幾，選取可以執行維護的日期（週一至週日）。
      - 針對開始時間，選取維護時段開始時的小時。時間是 UTC。
      - 針對通知前置時間，選取您希望提前幾天收到即將進行維護的通知。

   > **Note**
   >
   > Oracle Cloud Infrastructure 會在此時段執行系統維護。在維護期間，您的 Exadata 基礎設施仍然可用，但您可能會經歷短暫的較高延遲。

10. （選用）對於 OCI 維護通知聯絡人，輸入最多 10 個電子郵件地址。 AWS 然後輸入這些電子郵件地址到 OCI。更新發生時，OCI 會將通知傳送到列出的地址。
11. （選用）針對標籤，為基礎設施輸入最多 50 個標籤。標籤是可用於組織和追蹤資源的鍵/值對。
12. 選擇下一步並檢閱您的基礎設施設定。
13. 選擇建立 Exadata 基礎設施。

步驟 3：在 中建立 Exadata VM 叢集或自治 VM 叢集 Oracle Database@AWS

Exadata VM 叢集是一組 VMs，您可以在其中建立 Oracle Exadata 資料庫。您可以在 Exadata 基礎設施上建立 VM 叢集。您可以在相同的 ODB 網路中部署具有不同 Oracle Exadata 基礎設施的多個 VM 叢集。您可以完全管理控制在 Exadata VM 叢集上建立的資料庫。

自治 VM 叢集是預先配置的 Oracle Exadata 運算和儲存資源集區，在 VM 層級虛擬化，可執行自治資料庫 (ADB)。與您在 Exadata VM 叢集上建立的使用者受管資料庫不同，自動資料庫是由 Oracle 而非資料庫管理員進行自我調校、自我修補和管理。

當您建立 VM 叢集時，請考慮下列限制：

- 您只能將 VM 叢集部署到您建立 ODB 網路和 Oracle Exadata 基礎設施的 AZ。
- 如果您不跨帳戶共用 VM 叢集，它必須與 Oracle Exadata 基礎設施 AWS 帳戶 位於相同的 中。如果您使用 從具有信任 AWS 帳戶的帳戶 AWS RAM 共用 ODB 網路和 Oracle Exadata 基礎設施，信任帳戶可以在自己的帳戶中建立 VM 叢集。
- 您只能在 ODB 網路中部署 VM 叢集。不允許使用其他資源。
- 您無法在建立 VM 叢集之後變更儲存配置。

> **Important**
>
> 建立程序可能需要超過 6 小時，取決於 VM 叢集的大小。

Exadata VM cluster

建立 Exadata VM 叢集

1. 登入 AWS 管理主控台 ，並在 https：//https://console.aws.amazon.com/odb/ 開啟 Oracle Database@AWS 主控台。
2. 從左側窗格中，選擇 Exadata VM 叢集。
3. 選擇建立 VM 叢集。
4. 針對 VM 叢集名稱，輸入名稱。名稱必須為 1–255 個字元，並以字母字元或底線開頭。它不能包含連續連字號。

5. （選用）對於網格基礎設施叢集名稱，輸入與您正在使用的 Oracle 資料庫版本相符的 VM 叢集網格基礎設施版本。名稱必須為 1–11 個字元，且不能包含連字號。
6. 針對時區，輸入時區。
7. 針對授權選項，選擇自帶授權 (BYOL) 或包含授權，然後選擇下一步。此授權是由 Oracle 提供的 OCI 授權，而不是由 提供的授權 AWS。
8. 設定 Exadata 基礎設施設定，如下所示：

   a. 針對基礎設施，選擇下列項目：

      - 對於 Exadata 基礎設施名稱，選擇要用於此 VM 叢集的基礎設施。
      - 對於網格基礎設施版本，選擇要用於此 VM 叢集的版本。
      - 對於 Exadata 映像版本，選擇要用於此 VM 叢集的版本。我們建議您選擇顯示的版本，這是可用的最高版本。

   b. 針對資料庫伺服器，選取一或多個資料庫伺服器來託管您的 VM 叢集。

   c. 對於組態，請執行下列動作：

      - 選擇每個 VM 的 CPU 核心計數、記憶體和本機儲存體，或接受預設值。
      - 選擇 VM 叢集的 Exadata 儲存總量，或接受預設值。

   d. （選用）針對儲存配置，選取下列任一選項：

      - 啟用 Exadata 稀疏快照的儲存配置
      - 啟用本機備份的儲存配置

      當您選取選項時，可用的儲存配置會變更。您稍後無法變更此儲存配置。檢閱您的選擇，然後選擇下一步。
9. 設定連線，如下所示：

   a. 針對 ODB 網路，選擇現有的 ODB 網路。

   b. 針對主機名稱字首，輸入 VM 叢集的字首。請確定不要包含網域名稱。字首會形成 Oracle Exadata VM 叢集主機名稱的第一個部分。

      > **Note**
      >
      > 主機網域名稱固定為 oraclevcn.com。

c. 針對 SCAN 接聽程式連接埠 (TCP/IP)，輸入 TCP 存取單一用戶端存取名稱 (SCAN) 接聽程式的連接埠號碼。預設連接埠為 1521。或者，您可以輸入 1024–8999 範圍內的自訂 SCAN 連接埠，不包括下列連接埠號碼：2484、6100、6200、7060、7070、7085 和 7879。然後選擇下一步。

d. 對於 SSH 金鑰對，輸入用於 SSH 存取 VM 叢集的一或多個金鑰對的公有金鑰部分。然後選擇下一步。

10. （選用）選擇診斷和標籤，如下所示：

a. 選擇是否要為診斷事件、運作狀態監控和事件日誌和追蹤收集啟用診斷收集。 Oracle 可以使用此診斷資訊來識別、追蹤和解決問題。

b. 針對標籤，輸入 VM 叢集最多 50 個標籤。標籤是可用於組織和追蹤資源的鍵/值對。然後選擇下一步。

11. 檢閱您的設定。然後選擇建立 VM 叢集。

Autonomous VM cluster

建立自治 VM 叢集

1. 登入 AWS 管理主控台 並在 https：//https://console.aws.amazon.com/odb/ 開啟 Oracle Database@AWS 主控台。
2. 從左側窗格中，選擇自治 VM 叢集。
3. 選擇建立自治 VM 叢集。
4. 針對 VM 叢集名稱，輸入名稱。名稱必須為 1–255 個字元，並以字母字元或底線開頭。它不能包含連續連字號。
5. 針對時區，輸入時區。
6. 針對授權選項，選擇自攜授權 (BYOL) 或包含授權，然後選擇下一步。此授權是由 Oracle 提供的 OCI 授權，而不是由 提供的授權 AWS。
7. 設定 Exadata 基礎設施設定，如下所示：

a. 對於 Exadata 基礎設施名稱，選擇要用於此自治 VM 叢集的基礎設施。

b. 針對資料庫伺服器，選取一或多個資料庫伺服器來託管您的自治 VM 叢集。

c. 針對組態，請執行下列動作：

- 選擇每個 VM 的 ECPU 核心計數、每個 CPU 的資料庫記憶體、資料庫儲存，以及自治容器資料庫的數量上限，或接受預設值。

- 選擇自治 VM 叢集的 Exadata 儲存總量，或接受預設值。

8. 設定連線，如下所示：

   a. 針對 ODB 網路，選擇現有的 ODB 網路。

   b. 針對 SCAN 接聽程式連接埠 (TCP/IP)，輸入連接埠的連接埠號碼（非 TLS)。預設連接埠為 1521。或者，您可以輸入範圍為 1024–8999 的 Port(TLS)，不包括下列連接埠號碼：2484、6100、6200、7060、7070、7085 和 7879。然後選擇下一步。

      選取啟用交互 TLS (mTLS) 身分驗證，以允許交互 TLS 身分驗證。

9. （選用）選擇診斷和標籤，如下所示：

   a. 選擇是否要將修改組態排程至 Oracle 受管排程或客戶受管排程。如果您選擇客戶受管排程，請設定維護月份、當月週數、星期幾和開始時間 (UTC)。

   b. 針對標籤，輸入自治 VM 叢集最多 50 個標籤。標籤是可用於組織和追蹤資源的鍵/值對。然後選擇下一步。

10. 檢閱您的設定。然後選擇建立自治 VM 叢集。

步驟 4：在 Oracle Cloud Infrastructure 中建立 Oracle Exadata 資料庫

在 中 Oracle Database@AWS，您可以使用 AWS 主控台、CLI 或 APIs 建立和管理下列資源：

- ODB 網路
- Oracle Exadata 基礎設施
- Exadata VM 叢集和自治 VM 叢集
- ODB 對等互連

若要在您建立的基礎設施上建立和管理 Oracle Exadata 資料庫，您必須使用 Oracle Cloud Infrastructure 主控台，而不是 Oracle Database@AWS 儀表板。您可以在 Exadata VM 叢集上建立使用者管理的 Exadata 資料庫，並在 Autonomous Exadata VM 叢集上建立自治資料庫。如需有關在 OCI 中建立 Oracle 資料庫的資訊，請參閱 Oracle Cloud Infrastructure 文件中的 Exadata Database。

建立 Oracle Exadata 資料庫

1. 登入 AWS 管理主控台 ，並在 https：//https://console.aws.amazon.com/odb/ 開啟 Oracle Database@AWS 主控台。
2. 從左側窗格中，選擇 Exadata VM 叢集或自治 VM 叢集。
3. 選擇 VM 叢集以查看詳細資訊頁面。
4. 選擇在 OCI 中管理，以重新導向至 Oracle Cloud Infrastructure 主控台。
5. 在 OCI 中建立使用者受管 Exadata 資料庫或自治資料庫。

在 Oracle Database@ 中設定 ODB 對等互連至 Amazon VPC AWS

ODB 對等互連是使用者建立的網路連線，可讓流量在 Amazon VPC 和 ODB 網路之間私下路由。VPC 與 ODB 網路之間有one-to-one的關係。使用主控台、CLI 或 API 建立對等連線後，請務必更新您的 VPC 路由表並設定 DNS 解析。如需 ODB 對等互連的概念概觀，請參閱 ODB 對等互連。

在 Oracle Database@ 中建立 ODB 對等互連AWS

透過 ODB 互連連線，您可以在 Oracle Exadata 基礎設施與 Amazon VPCs 中執行的應用程式之間建立私有網路連線。每個 ODB 互連連線都是獨立的資源，您可以獨立於 ODB 網路來建立、檢視和刪除。

建立 ODB 互連連線時，您可以指定對等網路 CIDR 範圍。此技術會限制對所需子網路的網路存取、減少攻擊的潛在目標，並針對合規要求啟用更精細的網路分段。

您可以建立下列類型的 ODB 互連連線：

相同帳戶 ODB 對等互連

您可以在相同 AWS 帳戶中的 ODB 網路和 Amazon VPC 之間建立 ODB 對等互連。

跨帳戶 ODB 對等互連

使用 ODB 網路共用後，您可以在一個帳戶中的 ODB 網路與不同帳戶中的 Amazon VPC 之間建立 ODB 對等互連 AWS RAM。VPC 擁有者帳戶可以管理互連連線中指定的 CIDR 範圍，而不需要擁有 ODB 網路。

VPC 與 ODB 網路之間有 1：1 的關係。您無法在 VPC 和多個 ODB 網路之間或 ODB 網路和多個 VPCs 之間建立 ODB 對等互連。

主控台

1. 登入 AWS 管理主控台 ，並在 https：//https://console.aws.amazon.com/odb/ 開啟 Oracle Database@AWS 主控台。
2. 在導覽窗格中，選擇 ODB 互連連線。
3. 選擇建立 ODB 對等互連。

4. （選用）針對 ODB 對等互連名稱，輸入連線的唯一名稱。
5. 針對 ODB 網路，選擇要對等的 ODB 網路。
6. 針對對等網路，選擇要與 ODB 網路對等的 Amazon VPC。
7. （選用）對於對等網路 CIDRs，請從可存取 ODB 網路的對等 VPC 指定其他 CIDR 區塊。如果您未指定 CIDRs，則允許來自對等 VPC 的所有 CIDRs存取。
8. （選用）在標籤中，新增索引鍵和值對。
9. 選擇建立 ODB 對等互連。

建立 ODB 對等互連之後，請設定 Amazon VPC 路由表，將流量路由至對等 ODB 網路。如需詳細資訊，請參閱設定 ODB 對等互連的 VPC 路由表。請注意，Oracle Database@AWS 會自動設定 ODB 網路路由表。

AWS CLI

若要建立 ODB 對等互連，請使用 `create-odb-peering-connection`命令。

```
aws odb create-odb-peering-connection \
    --odb-network-id odbnet-1234567890abcdef \
    --peer-network-id vpc-abcdef1234567890
```

若要將 ODB 網路的存取限制在特定 CIDR 範圍，請使用 `--peer-network-cidrs-to-be-added` 參數。如果您未指定 CIDR 範圍，則所有範圍都可以存取。

```
aws odb create-odb-peering-connection \
    --odb-network-id odbnet-1234567890abcdef \
    --peer-network-id vpc-abcdef1234567890 \
    --peer-network-cidrs-to-be-added "10.0.1.0/24,10.0.2.0/24"
```

若要列出 ODB 對等互連，請使用 `list-odb-peering-connections`命令。

```
aws odb list-odb-peering-connections
```

若要取得特定 ODB 互連連線的詳細資訊，請使用 `get-odb-peering-connection`命令。

```
aws odb get-odb-peering-connection \
    --odb-peering-connection-id odbpcx-1234567890abcdef
```

更新 ODB 對等互連

您可以更新現有的 ODB 互連連線，以新增或移除對等網路 CIDRs。您可以控制對等 VPC 中哪些子網路可以存取您的 ODB 網路。

主控台

1. 登入 AWS 管理主控台 ，並在 https：//https://console.aws.amazon.com/odb/ 開啟 Oracle Database@AWS 主控台。
2. 在導覽窗格中，選擇 ODB 對等互連。
3. 選取您要更新的 ODB 互連連線。
4. 選擇動作，然後選擇更新對等連線。
5. 在對等網路 CIDRs區段中，視需要新增或移除 CIDR 區塊：
   - 若要新增 CIDRs，請選擇新增 CIDR，然後輸入 CIDR 區塊。
   - 若要移除 CIDRs，請選擇您要移除之 CIDR 區塊旁的 X。
6. 選擇更新對等連線。

AWS CLI

若要將對等網路 CIDRs 新增至 ODB 對等連線，請在 `update-odb-peering-connection`命令`--peer-network-cidrs-to-be-added`中指定 參數。

```
aws odb update-odb-peering-connection \
    --odb-peering-connection-id odbpcx-1234567890abcdef \
    --peer-network-cidrs-to-be-added "10.0.1.0/24,10.0.3.0/24"
```

若要從 ODB 對等連線中移除對等網路 CIDRs，請在 `update-odb-peering-connection`命令`--peer-network-cidrs-to-be-removed`中指定 參數。

```
aws odb update-odb-peering-connection \
    --odb-peering-connection-id odbpcx-1234567890abcdef \
    --peer-network-cidrs-to-be-removed "10.0.1.0/24,10.0.3.0/24"
```

設定 ODB 對等互連的 VPC 路由表

路由表包含一組名為路由的規則，可判斷來自子網或閘道之網路流量的方向。路由表中的目的地 CIDR 是您希望流量前往的 IP 地址範圍。如果您為 ODB 網路的 ODB 對等指定 VPC，請使用 ODB 網路中的目的地 IP 範圍更新您的 VPC 路由表。如需 ODB 對等互連的詳細資訊，請參閱 ODB 對等互連。

若要更新路由表，請使用 AWS CLI `ec2 create-route`命令。下列範例會更新 Amazon VPC 路由表。如需詳細資訊，請參閱設定 ODB 對等互連的 VPC 路由表。

```
aws ec2 create-route \
    --route-table-id rtb-1234567890abcdef \
    --destination-cidr-block 10.0.0.0/16 \
    --odb-network-arn arn:aws:odb:us-east-1:111111111111:odb-network/
odbnet_1234567890abcdef
```

ODB 網路路由表會自動更新為 VPC CIDRs。若要只允許存取特定子網路 CIDRs 的 ODB 網路，而不是 VPC 中的所有 CIDRs，您可以在建立 ODB 對等互連時指定對等網路 CIDRs，或更新現有的 ODB 對等互連連線以新增或移除對等 CIDR 範圍。如需詳細資訊，請參閱在 Oracle Database@ 中建立 ODB 對等互連AWS及更新 ODB 對等互連。

如需 VPC 路由表的詳細資訊，請參閱《Amazon Virtual Private Cloud 使用者指南》中的子網路路由表和《 AWS CLI 命令參考》中的 ec2 create-route。

設定 的 DNS Oracle Database@AWS

Amazon Route 53 是一種高可用性且可擴展的網域名稱系統 (DNS) Web 服務，可用於 DNS 路由。當您在 ODB 網路與 VPC 之間建立 ODB 對等互連時，您需要一種機制，才能從 VPC 內解析 ODB 網路資源的 DNS 查詢。您可以使用 Amazon Route 53 來設定下列資源：

- 傳出端點

  需要端點才能將 DNS 查詢傳送至 ODB 網路。

- 解析程式規則

  此規則會指定 Route 53 Resolver 轉送至 ODB 網路之 DNS 的 DNS 查詢網域名稱。

DNS 如何在 中運作 Oracle Database@AWS

Oracle Database@AWS 會自動管理 ODB 網路的網域名稱系統 (DNS) 組態。對於網域名稱，您可以指定預設網域名稱的自訂字首`oraclevcn.com`或完全自訂的網域名稱。如需詳細資訊，請參閱步驟 1：在 中建立 ODB 網路 Oracle Database@AWS。

當 Oracle Database@AWS 佈建 ODB 網路時，它會建立下列資源：

- 與 ODB 網路具有相同 CIDR 區塊的 Oracle Cloud Infrastructure (OCI) 虛擬雲端網路 (VCN)

  此 VCN 位於客戶連結的 OCI 租用中。ODB 網路與 OCI VCN 之間有 1：1 映射。每個 ODB 網路都與 OCI VCN 相關聯。
- OCI VCN 中的私有 DNS 解析程式

  此 DNS 解析程式會在 OCI VCN 中處理 DNS 查詢。OCI 自動化會建立 VM 叢集的記錄。掃描使用`*.oraclevcn.com`完整網域名稱 (FQDN)。
- 私有 DNS 解析程式的 OCI VCN 內 DNS 接聽端點

  您可以在 主控台的 ODB 網路詳細資訊頁面 Oracle Database@AWS 中找到 DNS 接聽端點。

在 中的 ODB 網路中設定傳出端點 Oracle Database@AWS

傳出端點允許 DNS 查詢從您的 VPC 傳送至網路或 IP 地址。端點會指定查詢來源的 IP 地址。若要將 DNS 查詢從 VPC 轉送到您的 ODB 網路，請使用 Route 53 主控台建立傳出端點。如需詳細資訊，請參閱轉送傳出 DNS 查詢到您的網路。

在 ODB 網路中設定傳出端點

1. 登入 AWS 管理主控台 並開啟 Route 53 主控台，網址為 https：//https://console.aws.amazon.com/route53/。
2. 從左側窗格中，選擇傳出端點。
3. 在導覽列上，選擇您要建立傳出端點的 VPC 區域。
4. 選擇 Create outbound endpoint (建立傳出端點)。
5. 完成傳出端點的一般設定區段，如下所示：

   a. 選擇允許傳出 TCP 和 UDP 連線至下列項目的安全群組：

      - 解析程式用於 ODB 網路上 DNS 查詢的 IP 地址

- 解析程式用於 ODB 網路上 DNS 查詢的連接埠

b. 針對端點類型，選擇 IPv4。

c. 針對此端點的通訊協定，選擇 Do53。

6. 在 IP 地址中，提供下列資訊：

- 指定 IP 地址，或讓 Route 53 Resolver 從子網路中的可用地址為您選擇 IP 地址。為 DNS 查詢選擇最少 2 個最多 6 個 IP 地址。我們建議您在至少兩個不同的可用區域中選擇 IP 地址。
- 針對子網路，選擇具有下列項目的子網路：
  - 包含路由到 ODB 網路上 DNS 接聽程式 IP 地址的路由表
  - 網路存取控制清單 ACLs)，允許 UDP 和 TCP 流量流向 IP 地址和解析程式用於 ODB 網路上 DNS 查詢的連接埠
  - 允許來自目的地連接埠範圍 1024-65535 上解析程式流量的網路 ACLs

7. （選用）針對標籤，指定端點的標籤。

8. 選擇提交。

在 中設定解析程式規則 Oracle Database@AWS

解析程式規則是一組條件，可決定如何路由 DNS 查詢。重複使用或建立規則，指定解析程式轉送至 ODB 網路 DNS 的 DNS 查詢網域名稱。

使用現有的解析程式規則

若要使用現有的解析程式規則，您的動作取決於規則的類型：

與 中 VPC 位於相同 AWS 區域中相同網域的規則 AWS 帳戶

將規則與 VPC 建立關聯，而不是建立新的規則。從規則儀表板中選擇規則，並將其與 AWS 區域中適用的 VPCs建立關聯。

與您的 VPC 位於相同區域中但位於不同帳戶中之相同網域的規則

使用 將規則從遠端帳戶 AWS Resource Access Manager 共用到您的帳戶。當您共用規則時，也會共用對應的傳出端點。在您與帳戶共用規則之後，請從規則儀表板中選擇規則，並將其與帳戶中 VPCs 建立關聯。如需詳細資訊，請參閱管理轉送規則。

建立新的解析程式規則

如果您無法重複使用現有的解析程式規則，請使用 Amazon Route 53 主控台建立新的規則。

建立新的解析程式規則

1. 登入 AWS 管理主控台 並開啟 Route 53 主控台，網址為 https：//https://console.aws.amazon.com/route53/。
2. 從左側窗格中，選擇規則。
3. 在導覽列上，選擇傳出端點所在的 VPC 區域。
4. 選擇建立規則。
5. 完成傳出流量區段的規則，如下所示：
   a. 針對規則類型，選擇轉送規則。
   b. 針對網域名稱，指定來自 ODB 網路的完整網域名稱。
   c. 對於使用此規則VPCs，請將它與轉送 DNS 查詢到您的 ODB 網路的 VPC 建立關聯。
   d. 針對傳出端點，選擇您在 中建立的傳出端點在 中的 ODB 網路中設定傳出端點 Oracle Database@AWS。

   > **Note**
   > 與此規則相關聯的 VPC 不需要與您建立傳出端點的 VPC 相同。

6. 完成目標 IP 地址區段，如下所示：
   a. 針對 IP 地址，指定 ODB 網路上 DNS 接聽程式 IP 的 IP 地址。
   b. 針對連接埠，指定 53。這是解析程式用於 DNS 查詢的連接埠。

   > **Note**
   > Route 53 Resolver 轉送符合此規則的 DNS 查詢，並且源自與此規則相關聯的 VPC 至參考的傳出端點。這些查詢會轉送到您在目標 IP 地址中指定的目標 IP 地址。

   c. 針對傳輸通訊協定，選擇 Do53。
7. （選用）針對標籤，指定規則的標籤。
8. 選擇提交。

在 中測試您的 DNS 組態 Oracle Database@AWS

在您建立傳出端點和解析程式規則之後，請測試 以確保 DNS 正確解析。在應用程式 VPC 中使用 Amazon EC2 執行個體，執行 DNS 解析，如下所示：

對於 Linux 或 MacOS

使用格式為 的命令`dig` *record-name record-type*。

適用於 Windows

使用格式為 的命令`nslookup -type=`*record-name record-type*。

設定 的 Amazon VPC Transit Gateway Oracle Database@AWS

Amazon VPC Transit Gateways 是一種網路傳輸中樞，可互連虛擬私有雲端 (VPCs) 和內部部署網路。hub-and-spoke架構中的每個 VPC 都可以連線至傳輸閘道，以取得其他連線 VPCs存取權。 AWS Transit Gateway 支援 IPv4 和 IPv6 的流量。

在 中 Oracle Database@AWS，ODB 網路僅支援對等互連至一個 VPC。如果您將傳輸閘道連接到對等至 ODB 網路的 VPC，您可以將多個 VPCs連接到此閘道。在這些不同 VPCs可以存取在您的 ODB 網路中執行的 Exadata VM 叢集。

下圖顯示連線至兩個 VPCs和一個內部部署網路的傳輸閘道。

在上圖中，一個 VPC 會對等至 ODB 網路。在此組態中，ODB 網路可以將流量路由到連接到傳輸閘道的所有 VPCs。每個 VPC 的路由表都包含本機路由，以及將目的地為 ODB 網路的流量傳送至傳輸閘道的路由。

在 中 AWS Transit Gateway，系統會針對您每小時對傳輸閘道進行的連線數，以及流經的流量，向您收費 AWS Transit Gateway。如需成本資訊，請參閱 AWS Transit Gateway 定價。

要求

請確定您的 Oracle Database@AWS 環境符合下列要求：

- 對等至 ODB 網路的 VPC 必須位於相同的 中 AWS 帳戶。如果對等 VPC 位於與 ODB 網路不同的帳戶中，無論共用組態為何，傳輸閘道附件都會失敗。
- 對等至 ODB 網路的 VPC 必須具有傳輸閘道連接。

> **Note**
>
> 如果傳輸閘道設定為共用，它可以位於任何帳戶中。因此，閘道本身不需要與 VPC 和 ODB 網路位於相同的帳戶中。

- 傳輸閘道連接必須位於與 ODB 網路相同的可用區域 (AZ)。

限制

請注意 Amazon VPC Transit Gateways 的下列限制 Oracle Database@AWS：

- Amazon VPC Transit Gateways 不提供原生整合，以使用 ODB 網路做為附件。因此，無法使用下列 VPC 功能：
  - 公有 DNS 主機名稱解析為私有 IP 地址
  - ODB 網路拓撲、路由和連線狀態變更的事件通知
- 不支援多點傳送流量到 ODB 網路。

設定傳輸閘道

您可以使用 Amazon VPC 主控台或`aws ec2`命令來建立和設定傳輸閘道。下列程序假設您的 中沒有與 VPC 對等的 ODB 網路 AWS 帳戶。如果 ODB 網路和 VPC 已在您的帳戶中對等，請略過步驟 1–3。

> **Note**
>
> 如果您在 VPC 上連接或重新連接附件，請務必將 CIDR 範圍重新輸入至 ODB ODB 網路。

設定 的傳輸閘道 Oracle Database@AWS

1. 建立 ODB 網路。如需詳細資訊，請參閱步驟 1：在 中建立 ODB 網路 Oracle Database@AWS。
2. 使用包含 ODB 網路的相同帳戶來建立 VPC。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的建立 VPC。
3. 在 ODB 網路和 VPC 之間建立 ODB 對等互連。如需詳細資訊，請參閱在 Oracle Database@ 中設定 ODB 對等互連至 Amazon VPC AWS。

4. 遵循使用 Amazon VPC Transit Gateways 開始使用中的步驟來設定傳輸閘道。閘道必須與 ODB 網路和 VPC 位於相同的 AWS 帳戶 中，或由另一個帳戶共用。

   > **Important**
   >
   > 在與 ODB 網路相同的 AZ 中建立傳輸閘道連接。

5. 針對您計劃連接到核心網路VPCs 和內部部署網路，將 CIDR 範圍新增至您的 ODB 網路。如需詳細資訊，請參閱在 中更新 ODB 網路 Oracle Database@AWS。

   如果您使用的是 CLI，請使用 `update-odb-network--peered-cidrs-to-be-added`和 執行命令`--peered-cidrs-to-be-removed`。如需詳細資訊，請參閱 AWS CLI 命令參考。

設定 的 AWS 雲端 WAN Oracle Database@AWS

AWS Cloud WAN 是一種受管廣域聯網 (WAN) 服務。您可以使用 AWS Cloud WAN 來建置、管理和監控統一的全域網路，以連接在雲端和內部部署環境中執行的資源。

在 AWS Cloud WAN 中，全域網路是單一的私有網路，可做為網路物件的高階容器。核心網路是 管理的全球網路的一部分 AWS。

AWS Cloud WAN 提供下列主要優點：

- 集中式網路管理，可簡化操作，同時跨多個區域維護安全性
- 具有內建分段的核心網路，可透過多個路由網域隔離流量
- 支援政策，以自動化網路管理和定義全球網路的一致組態

在 Oracle Database@ 中AWS，ODB 網路僅支援對等互連至一個 VPC。如果您將 AWS Cloud WAN 核心網路連接到對等 VPC，則會啟用全域流量路由。跨多個區域的連接 VPCs 中的應用程式可以存取 ODB 網路中的 Exadata VM 叢集。您可以在自己的區段中隔離 ODB 網路流量，或啟用對其他區段的存取。

下圖顯示連接到三個 VPCs和一個內部部署網路的 AWS Cloud WAN 核心網路。

AWS Cloud WAN 不提供原生整合，以使用 ODB 網路做為附件。因此，無法使用下列 VPC 功能：

- 公有 DNS 主機名稱解析為私有 IP 地址

- ODB 網路拓撲、路由和連線狀態變更的事件通知

在 AWS Cloud WAN 中，您需要按小時支付下列費用：

- 區域數目 （核心網路邊緣）
- 核心網路附件的數量
- 透過附件流經核心網路的流量

如需詳細的定價資訊，請參閱 AWS Cloud WAN 定價。

設定 的核心網路 Oracle Database@AWS

1. 針對您計劃連接到核心網路VPCs 和內部部署網路，將 CIDR 範圍新增至您的 ODB 網路。如需詳細資訊，請參閱在 中更新 ODB 網路 Oracle Database@AWS。

   > **Note**
   >
   > 如果您在 VPC 上連接或重新連接附件，請務必將 CIDR 範圍重新輸入至 ODB ODB 網路。

2. 請遵循建立 AWS Cloud WAN 全域網路和核心網路中的步驟。

Oracle Database@ 中的權利共用AWS

使用 Oracle Database@AWS，您可以共用 AWS 帳戶 同一 AWS 組織中 Oracle Database@AWS across 的 AWS Marketplace 權利。這可讓其他帳戶使用您的訂閱佈建自己的 Oracle Exadata 基礎設施和 ODB 網路資源。

共享方法

Oracle Database@AWS 支援兩種共用方法：

與 AWS License Manager 共用權限

- 授予其他帳戶佈建自己的 Oracle Exadata 基礎設施和 ODB 網路資源的能力
- 每個帳戶使用完整的資源生命週期控制獨立運作
- 最適合跨團隊或業務單位啟用自助式佈建

與 AWS Resource Access Manager (AWS RAM) 共用資源

- 共用已佈建的 Oracle Exadata 基礎設施和 ODB 網路資源
- 集中基礎設施管理，同時允許收件人帳戶建立 VM 叢集
- 讓多個帳戶使用相同的基礎設施來最佳化成本

您可以根據您的組織需求，同時使用這兩種共用方法。

Oracle Database@AWS entitlement 共用的限制

共用 Oracle Database@AWS entitlements 時，請記住下列限制：

- 您只能與 AWS 組織內 AWS 帳戶 的 共用
- 您無法與整個組織單位 (OU) 或整個組織共用
- 帳戶只能從一個買方帳戶 （從一個私有優惠） 接收權利
- 買方帳戶無法與其他買方帳戶共用權利
- 收件人帳戶必須先初始化 Oracle Database@AWS service，才能使用共用權利
- 權利授予操作只能從美國東部 （維吉尼亞北部） 區域執行

跨帳戶共用 Oracle Database@AWS entitlements

若要在最佳化成本的同時啟用協同合作，請將 Oracle Database@AWS entitlements AWS 帳戶 分享給同一 AWS 組織內的其他 。本主題說明如何使用 AWS License Manager 共用權利。

共用權利的先決條件

共用 Oracle Database@AWS entitlements 之前，請確定您有下列項目：

- 作用中的 Oracle Database@AWS subscription （您必須是透過 接受私有優惠的買方帳戶 AWS Marketplace)
- 您希望與之共用權利的組織中 AWS 的帳戶 IDs
- 授予者和承授者使用 AWS License Manager 資源和操作的必要許可 （如需詳細資訊，請參閱 AWS License Manager 使用者指南中的 License Manager 的 Identity and Access Management)
- 以下為您 （授權方） 和權利接收者 （授權方） 列出的許可

權利共用所需的許可

除了 AWS License Manager 許可之外，Oracle Database@AWS 還需要下列許可：

授予者許可

- `odb:CreateGrantShare`
- `odb:UpdateGrantShare`
- `odb:DeleteGrantShare`

承授者許可

- `odb:UpdateGrantShare`
- `odb:DeleteGrantShare`

使用 AWS License Manager 與其他帳戶共用 Oracle Database@AWS entitlements

若要與其他 AWS 帳戶共用權利，您可以使用 AWS License Manager 建立授予。如需詳細資訊，請參閱《 License Manager 使用者指南》中的分佈 License Manager 權限。 AWS

建立授予之後，收件人（承授者）必須：

- 接受並啟用授予。如需詳細資訊，請參閱《 License Manager 使用者指南》中的授權管理員中的授予接受和啟用。 AWS
- 遵循 Oracle Database@ 的初始化指示AWS。

初始化完成後，承授者可以使用共用權利佈建 Oracle Database@AWS resources。

Oracle Database@ 中的資源共用AWS

使用 Oracle Database@AWS，您可以在 AWS 帳戶 同一個 AWS 組織中跨多個 共用 Exadata 基礎設施和 ODB 網路。這可讓您佈建基礎設施一次，並在受信任的帳戶中重複使用，讓您在分離責任的同時降低成本。

當您共用資源時：

- 擁有資源的帳戶 （ 擁有者帳戶 ） 會維持對資源生命週期的控制。
- 接收共用資源 （ 受信任帳戶 ） 存取權的帳戶可以根據授予的許可來檢視和使用這些資源。
- 信任的帳戶可以在共用基礎設施上建立自己的資源，但無法刪除基礎共用資源。

Oracle Database@AWS integration 與 AWS RAM

Oracle Database@AWS uses AWS Resource Access Manager (AWS RAM) 可跨帳戶啟用安全、受控的資源共用。透過 AWS RAM，您可以安全地在同一個 AWS 組織內的多個 AWS 帳戶之間共用 Oracle Database@AWS resources。 AWS RAM 可簡化資源共用、降低營運開銷，並提供共用 Oracle Database@AWS resources 的安全性和可見性。

您可以透過建立資源共享 AWS RAM，與 共用您擁有的資源。資源共用會指定要共用的資源，以及要 AWS 帳戶 與其共用的資源。

Oracle Database@ 中資源共用的優點AWS

跨帳戶共用 Oracle Database@AWS resources 有下列優點：

- 成本最佳化 – 透過管理帳戶佈建一次昂貴的 Exadata 基礎設施，並與多個帳戶共用，從而降低整體成本。
- 職責分離 – 在允許協同合作的同時，維持基礎設施管理員和資料庫使用者之間的明確界限。
- 簡化管理 – 集中基礎設施佈建和管理，同時啟用分散式資料庫操作。
- 一致的控管 – 跨共用資源套用一致的政策和控制。

例如，管理員可以在其 中佈建 Oracle Exadata 基礎設施和 ODB 網路， AWS 帳戶 並與開發人員帳戶共用。然後，開發人員可以在此共用基礎設施上建立 VM 叢集，而不需要佈建自己的昂貴硬體。此方法可大幅降低成本，同時在帳戶之間維持適當的責任分離。

資源共用如何在 Oracle Database@ 中運作AWS

您可以共用下列 Oracle Database@AWS resources：

- Oracle Exadata 基礎設施
- ODB 網路

Oracle Database@ 透過下列程序AWS 共用上述資源：

1. 買方帳戶 （透過 AWS Marketplace 接受 Oracle Database@AWS private 優惠的帳戶） 會佈建 Oracle Database@AWS resources，例如 Exadata 基礎設施和 ODB 網路。
2. 買方帳戶使用 建立資源共用 AWS RAM，指定要共用的資源和要共用的信任帳戶。
3. 系統會自動接受同一組織內受信任帳戶的資源共用。
4. 在使用共用資源之前，受信任帳戶必須使用 `aws odb initialize-service`命令或在 Oracle Database@AWS console 中選擇啟用帳戶，在其帳戶中初始化 Oracle Database@AWS service。
5. 初始化後，信任的帳戶可以在共用基礎設施上建立自己的資源，例如共用 Exadata 基礎設施和 ODB 網路上的 VM 叢集。

受信任帳戶的共用資源許可

當您共用資源時，Oracle Database@AWS 會自動為每個資源類型選取特定動作 （受管許可）：

對於 Exadata 基礎設施

Oracle Database@AWS 授予受信任帳戶的下列許可：

- `odb:CreateCloudVmCluster`
- `odb:CreateCloudAutonomousVmCluster`
- `odb:GetCloudExadataInfrastructure`
- `odb:ListCloudExadataInfrastructures`
- `odb:GetCloudExadataInfrastructureUnallocatedResources`
- `odb:ListDbServers`
- `odb:GetDbServer`
- `odb:ListCloudVmClusters`
- `odb:ListCloudAutonomousVmClusters`

對於 ODB 網路

下列許可會授予信任的帳戶：

- odb:CreateCloudVmCluster
- odb:CreateCloudAutonomousVmCluster
- odb:GetOdbNetwork
- odb:ListOdbNetworks
- odb:CreateOdbPeeringConnection
- odb:ListOdbPeeringConnections

資源共用遵守 Oracle Database@AWS resources 的階層性質。例如，如果您共用 Exadata 基礎設施，受信任帳戶可以在此基礎設施上建立 VM 叢集，但無法修改或刪除 Exadata 基礎設施本身。

未共用資源時，信任的帳戶將無法在共用的基礎設施上建立新的資源。不過，他們已建立的任何資源仍然可以存取和運作。

Oracle Database@AWS resource 共用的限制

在共用資源之前，請記住下列限制。

共用資源的限制

共用 Oracle Database@AWS resources 時，請記住下列限制：

- 您只能使用 AWS 帳戶 IDs共用資源。
- 您只能在相同 AWS 帳戶 AWS 組織內共用 的資源。
- 您可以在特定 AWS 區域內共用資源。若要跨區域共用資源，您必須在每個區域中建立個別的資源共用。
- 當您建立資源共享時，會自動選取每個資源類型的動作 （受管許可），而且無法修改。
- 您無法使用 Oracle Database@AWS 做為資源並與其他資源共用 AWS 帳戶。
- 受信任帳戶只能使用來自一個買方帳戶的共用資源 （來自一個私有優惠）。因此，兩個買方帳戶無法與相同的信任帳戶共用資源。
- 買方帳戶無法與另一個買方帳戶共用資源。
- 與信任帳戶共用的資源必須先由買方所在區域的買方帳戶共用。
- 當您取消共用資源時，建議您等待約 15 分鐘，再與相同的信任帳戶重新共用相同的資源。

建立和使用共用資源的限制

建立或使用 Oracle Database@AWS resources 時，請記住下列限制：

- 只有買方帳戶可以建立 Exadata 基礎設施和 ODB 網路資源。買方帳戶是接受 Oracle Database@AWS private 優惠的帳戶。
- 信任的帳戶只能在買方帳戶共用的 Exadata 基礎設施上建立資源。
- 信任的帳戶必須先在其帳戶中初始化 Oracle Database@AWS service，才能使用共用資源。

刪除共用資源的限制

- 在移除這些 VM 叢集之前，您無法刪除具有信任帳戶所建立 VM 叢集的 Exadata 基礎設施。
- 在移除 ODB 互連連線之前，您無法刪除具有信任帳戶所建立 ODB 互連連線的 ODB 網路。
- 買方帳戶無法刪除信任帳戶建立的 Oracle Database@AWS resources。
- 信任的帳戶可以檢視共用資源，但無法修改或刪除買方帳戶擁有的 Oracle Database@AWS 資源。

跨帳戶共用 Oracle Database@AWS 資源

若要在最佳化成本的同時啟用協同合作，請將 Oracle Database@AWS resources AWS 帳戶 分享給同一 AWS 組織內的其他 。本主題說明如何使用 AWS Resource Access Manager () 共用資源AWS RAM。

主題

共用資源的先決條件

共用 Oracle Database@AWS resources 之前，請確定您有下列項目：

- 作用中的 Oracle Database@AWS subscription （您必須是透過 接受私有優惠的買方帳戶 AWS Marketplace)

- 您要共用的資源 IDs 或名稱，例如 Exadata 基礎設施或 ODB 網路
- 組織中您要與之共用資源 AWS 的帳戶 IDs
- 在 中建立資源共用的必要許可 AWS RAM
- 使用 與 共用資源的能力 AWS Organizations AWS RAM （ 如需詳細資訊，請參閱AWS Resource Access Manager 《 使用者指南》中的在 中啟用資源共用 AWS Organizations)

使用 與其他帳戶共用 Oracle Database@AWS resources AWS RAM

若要與其他 AWS 帳戶共用 Exadata 基礎設施或 ODB 網路，您可以使用 建立資源共用 AWS RAM。這可讓信任的帳戶在您的 Exadata 基礎設施上建立 VM 叢集。

主控台

1. 在 https：//https://console.aws.amazon.com/ram/ 開啟 AWS RAM 主控台。
2. 選擇 Create resource share (建立資源共用)。
3. 在名稱中，輸入資源共享的描述性名稱。
4. 在選取資源類型下，下列任一資源：
   - Oracle Database@AWS ODB 網路
   - Oracle Database@AWS Exadata 基礎設施
5. 選取您要共用的 Exadata 基礎設施資源。選擇下一步，直到您取得授予委託人的存取權為止。
6. 在主體下，選擇 AWS 帳戶，然後輸入 AWS 您要共用的帳戶 IDs。
7. 在受管許可下，選取下列許可，以允許信任的帳戶在共用 Exadata 基礎設施上建立 VM 叢集：
   - AWSRAMDefaultPermissionODBNetwork
   - AWSRAMDefaultPermissionODBCloudExadataInfrastructure
8. 選擇 Create resource share (建立資源共用)。

AWS CLI

若要使用 共用資源 AWS CLI，請使用 `aws ram create-resource-share`命令。下列範例會建立名為 的資源共享`ExadataInfraShare`，與帳戶 222222222222 共用指定的 Exadata 基礎設施，允許此帳戶在共用基礎設施上建立 VM 叢集。

```
aws ram create-resource-share --region us-east-1 \
    --name "ExadataInfraShare" \
```

```
    --resource-arns arn:aws:odb:us-east-1:111111111111:cloud-exadata-infrastructure/
exa_infra_1 \
    --principals 222222222222
```

檢視您的資源共用

若要檢視您已共用的資源和已共用這些資源的帳戶：

主控台

1. 在 https：//https://console.aws.amazon.com/ram/ 開啟 AWS RAM 主控台。
2. 選擇共用資源以檢視您與其他 帳戶共用的資源。
3. 選取資源共用以檢視其詳細資訊，包括共用的資源和共用的委託人。

AWS CLI

若要使用 檢視您的資源共享 AWS CLI，請使用 `get-resource-shares`命令：

```
aws ram get-resource-shares --resource-owner SELF
```

若要檢視特定資源共享中的資源，請使用 `list-resources`命令：

```
aws ram list-resources \
    --resource-owner SELF \
    --resource-share-arns arn:aws:ram:us-east-1:111111111111:resource-share/12345678-
abcd-1234-efgh-111111111111
```

若要檢視與資源共用共用共用的委託人（帳戶），請使用 `list-principals`命令：

```
aws ram list-principals \
    --resource-owner SELF \
    --resource-share-arns arn:aws:ram:us-east-1:111111111111:resource-share/12345678-
abcd-1234-efgh-111111111111
```

使用 更新或刪除資源共用 AWS RAM

若要使用 停止與信任的帳戶共用資源 AWS RAM，請採取下列任何動作：

- 從資源共用中移除資源。
- 從資源共用中移除信任的帳戶。

- 刪除資源共享。

在您撤銷存取或刪除共用資源之前，請考慮下列影響：

- 信任的帳戶無法再在未共用的基礎設施上建立新的資源。
- 在共用 Exadata 基礎設施上由受信任帳戶建立的現有資源會繼續運作，並可供這些資源存取 AWS 帳戶。
- 在移除這些 VM 叢集之前，您無法刪除具有信任帳戶所建立 VM 叢集的 Exadata 基礎設施。

在取消共用資源之前，我們建議您與信任的帳戶協調，以確保順利轉換。

如需詳細資訊，請參閱AWS Resource Access Manager 《 使用者指南》中的在 中更新資源共享 AWS RAM和在 中刪除資源共享 AWS RAM。

在信任 Oracle Database@AWS 的帳戶中初始化

信任帳戶是您指定為符合接收資源共享資格 AWS 帳戶 的 。它必須是 AWS 組織中 AWS 帳戶 的另一個個人。您必須先初始化服務，才能在信任的帳戶中使用共用的 Oracle Database@AWS resources。初始化會建立必要的中繼資料，並在您的 AWS 帳戶 和 Oracle Cloud Infrastructure 之間建立連線。

主題

什麼是 Oracle Database@AWS 初始化？

在與您的帳戶共用資源之後，您必須先初始化 Oracle Database@AWS service，才能存取或使用共用資源。如果您在未先初始化服務的情況下嘗試使用 Oracle Database@AWS APIs，您會收到錯誤。

初始化是一次性的程序。它會建立必要的中繼資料，並在您的 AWS 帳戶 和 Oracle Cloud Infrastructure 之間建立連線。

您可以使用 AWS 管理主控台或 來初始化服務 AWS CLI。

主控台

1. 在 https：//https://console.aws.amazon.com/odb/ 開啟 Oracle Database@AWS console。

2. 如果這是您第一次存取此帳戶中的 Oracle Database@AWS console，您會看到歡迎頁面。
3. 選擇啟用帳戶。
4. 服務初始化程序開始。此程序可能需要幾分鐘的時間才能完成。
5. 定期重新整理歡迎頁面，直到啟用帳戶按鈕變更為儀表板按鈕為止。
6. 選擇儀表板以開始使用 Oracle Database@AWS。

AWS CLI

若要使用AWS 在您的信任帳戶中初始化 Oracle Database@ AWS CLI，請使用 `initialize-service`命令。

```
aws odb initialize-service
```

若要檢查初始化狀態，請使用 `get-oci-onboarding-status`命令。

```
aws odb get-oci-onboarding-status
```

初始化完成時，輸出會顯示 狀態`ACTIVE_LIMITED`，表示您的帳戶可以存取共用資源，但無法建立新的 Exadata 基礎設施或 ODB 網路。

後續步驟

在信任AWS 的帳戶中初始化 Oracle Database@ 之後，您可以執行下列動作：

- 使用 `list`和 `get`命令或在 AWS 主控台中檢視共用資源。
- 在共用 Exadata 基礎設施和 ODB 網路上建立 VM 叢集和自治 VM 叢集。
- 在共用 ODB 網路上建立 ODB 對等互連。

如需使用共用資源的詳細資訊，請參閱 使用信任帳戶中的共用 Oracle Database@AWS 資源。

使用信任帳戶中的共用 Oracle Database@AWS 資源

與您的信任帳戶共用資源且初始化 Oracle Database@AWS service 後，您可以檢視和使用共用資源。本主題說明如何使用信任帳戶中的共用資源。

主題

- 受信任帳戶中共用資源的限制

- 在共用 Exadata 基礎設施上建立 VM 叢集
- 檢視信任帳戶中的共用資源
- 使用共用 ODB 網路設定 ODB 對等互連

受信任帳戶中共用資源的限制

使用共用的 Oracle Database@AWS resources 時，請注意下列限制：

- 僅在相同的 AWS 組織中支援資源共用。
- 只有買方帳戶（接受 Oracle Database@AWS private 優惠的帳戶）可以建立 Exadata 基礎設施和 ODB 網路資源。
- 您只能在共用基礎設施上建立資源，而且只有在您擁有必要的許可時才能建立資源。
- 建立資源共用期間會自動選取每個資源類型的特定動作（受管許可），而且無法修改。
- 您無法修改或刪除另一個帳戶擁有的資源。
- 您在共用基礎設施上建立的資源由您的帳戶擁有，並計入您的 OCI 配額。這同樣適用於父資源。
- 如果擁有者帳戶取消共用資源，您就無法再在此共用基礎設施上建立新的資源。不過，您現有的資源會繼續運作。
- 不支援跨區域資源共用。您只能在相同區域內共用資源 AWS 。
- 信任的帳戶資源會向 Oracle Database@AWS 訂閱的買方收費。
- 使用共用的資源時，您必須提供 Amazon Resource Name (ARN)。

在共用 Exadata 基礎設施上建立 VM 叢集

如果您的信任帳戶可以存取共用的 Exadata 基礎設施和 ODB 網路，您可以在此基礎設施上建立 Exadata VM 叢集、自治 VM 叢集或 ODB 對等互連。

> **Note**
>
> 使用與您共用的資源時，您必須指定 Amazon Resource Name (ARN)，而不是只指定資源 ID。

主控台

1. 在 https：//https://console.aws.amazon.com/odb/ 開啟 Oracle Database@AWS console。

2. 在導覽窗格中，選擇 Exadata VM 叢集或自治 VM 叢集。
3. 選擇建立 VM 叢集或建立自治 VM 叢集。
4. 針對 Exadata 基礎設施，選取您要在其中建立 VM 叢集的共用 Exadata 基礎設施。
5. 完成 VM 叢集組態所需的其餘欄位。
6. 選擇建立 VM 叢集或建立自治 VM 叢集。

AWS CLI

若要使用 在共用 Exadata 基礎設施上建立 VM 叢集 AWS CLI，請使用 `create-cloud-vm-cluster`命令：

```
aws odb create-cloud-vm-cluster --region us-east-1 \
    --cloud-exadata-infrastructure-id arn:aws:odb:us-east-1:111111111111:cloud-exadata-infrastructure/exa_aaaaaaaaaa \
    --odb-network-id arn:aws:odb:us-east-1:111111111111:odb-network/odbnet_aaaaaaaaaa \
    --cpu-core-count 4 \
    --display-name "Shared-VMC-1" \
    --gi-version "19.0.0.0" \
    --hostname "vmchost" \
    --ssh-public-keys "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQ..." \
```

若要使用 在共用 Exadata 基礎設施上建立自治 VM 叢集 AWS CLI，請使用 `create-cloud-vm-cluster`命令：

```
aws odb create-cloud-autonomous-vm-cluster --region us-east-1  \
    --cloud-exadata-infrastructure-id arn:aws:odb:us-east-1:111111111111:cloud-exadata-infrastructure/exa_aaaaaaaaaa \
    --odb-network-id arn:aws:odb:us-east-1:111111111111:odb-network/odbnet_aaaaaaaaaa\
    --display-name "Shared-AVMC-1" \
    --autonomous-data-storage-size-in-tbs 8 \
    --cpu-core-count-per-node 16
```

VM 叢集是在指定的共用 Exadata 基礎設施上建立，並由您的信任帳戶擁有。

檢視信任帳戶中的共用資源

您可以使用 管理主控台或 檢視已與您的帳戶 AWS 共用的資源 AWS CLI。

主控台

1. 在 https：//https://console.aws.amazon.com/odb/ 開啟 Oracle Database@AWS console。
2. 在導覽窗格中，選擇您要檢視的資源類型：Exadata 基礎設施或 ODB 網路。
3. 主控台會顯示與您共用的資源。
4. 選取共用資源以檢視其詳細資訊。

AWS CLI

若要使用 檢視共用資源 AWS CLI，請針對資源類型使用適當的`list`命令。例如，若要列出 Exadata 基礎設施：

```
aws odb list-cloud-exadata-infrastructures
```

回應會顯示與您共用的資源。

若要取得特定共用資源的詳細資訊，請使用具有資源 ID 的適當`get`命令：

```
aws odb get-cloud-exadata-infrastructure --cloud-exadata-infrastructure-id exa_infra_1
```

使用共用 ODB 網路設定 ODB 對等互連

若要在共用 ODB 網路上啟用應用程式和資料庫之間的通訊，您可以在 VPC 和共用 ODB 網路之間設定 ODB 對等互連。如需 ODB 對等互連的詳細資訊，請參閱 在 Oracle Database@ 中建立 ODB 對等互連AWS。

主控台

1. 在 https：//https://console.aws.amazon.com/odb/ 開啟 Oracle Database@AWS console。
2. 在導覽窗格中，選擇 ODB 對等互連。
3. 選擇建立 ODB 網路對等互連。
4. 針對 ODB 網路，選取您要對等的共用 ODB 網路。
5. 針對對等網路，選取您的 VPC。
6. 選擇建立 ODB 網路對等互連。

AWS CLI

若要使用 在 VPC 與共用 ODB 網路之間建立網路對等互連 AWS CLI，請使用 `create-odb-peering-connection`命令。

```
aws odb create-odb-peering-connection \
    --odb-network-id odbnet_1234567890abcdef \
    --peer-network-id vpc-abcdef1234567890
```

建立對等連線後，請更新您的路由表，以啟用對等網路之間的流量。

```
aws ec2 create-route \
    --route-table-id rtb-1234567890abcdef \
    --destination-cidr-block 10.0.0.0/16 \
    --odb-network-arn arn:aws:odb:us-east-1:111111111111:odb-network/
odbnet_1234567890abcdef
```

管理 Oracle Database@AWS

您可以在建立後修改和刪除一些 Oracle Database@AWS 資源。

在 中更新 ODB 網路 Oracle Database@AWS

您可以更新下列 ODB 網路資源：

- ODB 網路名稱
- 用來建立 ODB 網路對等互連的 Amazon VPC
- 可存取 ODB 網路中 Exadata 資源的 VPC CIDR 範圍

> **Note**
>
> 透過指定 CIDR 範圍，您可以限制與必要 VPC 子網路的連線，而不是讓整個 VPC 可供 ODB 網路使用。

本節假設您已在 中建立 ODB 網路步驟 1：在 中建立 ODB 網路 Oracle Database@AWS。

更新 ODB 網路

1. 登入 AWS 管理主控台 ，並在 https：//https://console.aws.amazon.com/odb/ 開啟 Oracle Database@AWS 主控台。
2. 從左側窗格中，選擇 ODB 網路。
3. 選取您要修改的網路。
4. 選擇 Modify (修改)。
5. （選用）針對 ODB 網路名稱，輸入新的網路名稱。名稱必須為 1–255 個字元，並以字母字元或底線開頭。它不能包含連續連字號。
6. （選用）對於對等 CIDRs，從需要連線至 ODB 網路的對等 VPC 指定 CIDR 範圍。若要限制存取，建議您指定所需的 CIDR 範圍下限。
7. （選用）對於設定服務整合，選取或取消選取 Amazon S3 或零 ETL。
8. 選擇繼續，然後選擇修改。

在 中刪除 ODB 網路 Oracle Database@AWS

您可以刪除 ODB 網路。本節假設您已在 中建立 ODB 網路步驟 1：在 中建立 ODB 網路 Oracle Database@AWS。您無法刪除 VM 叢集目前正在使用的 ODB 網路。

刪除 ODB 網路

1. 登入 AWS 管理主控台 ，並在 https：//https://console.aws.amazon.com/odb/ 開啟 Oracle Database@AWS 主控台。
2. 從左側窗格中，選擇 ODB 網路。
3. 選取您要刪除的網路。
4. 選擇 刪除。
5. （選用）選擇刪除相關聯的 OCI 資源，以刪除與 ODB 網路一起建立的 OCI 資源。
6. 在文字方塊中輸入 **`delete me`**。
7. 選擇 刪除。

在 中刪除 VM 叢集 Oracle Database@AWS

您可以刪除 Exadata VM 叢集或自治 VM 叢集。本節假設您已在 中建立 VM 叢集步驟 3：在 中建立 Exadata VM 叢集或自治 VM 叢集 Oracle Database@AWS。

刪除 VM 叢集

1. 登入 AWS 管理主控台 並在 https：//https://console.aws.amazon.com/odb/ 開啟 Oracle Database@AWS 主控台。
2. 從左側窗格中，選擇 Exadata VM 叢集或自治 VM 叢集。
3. 選擇要刪除的 VM 叢集。
4. 選擇 刪除。
5. 出現提示時，輸入 **`delete me`**，然後選擇刪除。

在 中刪除 Oracle Exadata 基礎設施 Oracle Database@AWS

您可以刪除 Oracle Exadata 基礎設施。本節假設您已在 中建立 Oracle Exadata 基礎設施步驟 2：在 中建立 Oracle Exadata 基礎設施 Oracle Database@AWS。您無法刪除 VM 叢集目前正在使用的 Exadata 基礎設施。

刪除 Oracle Exadata 基礎設施

1. 登入 AWS 管理主控台 並在 https：//https://console.aws.amazon.com/odb/ 開啟 Oracle Database@AWS 主控台。
2. 從左側窗格中，選擇 Exadata 基礎設施。
3. 選擇要刪除的 Exadata 基礎設施。
4. 選擇 刪除。
5. 出現提示時，輸入 **`delete me`**，然後選擇刪除。

刪除 ODB 對等互連

當您不再需要 ODB 對等互連時，您可以將其刪除。您必須刪除所有 ODB 對等互連，才能刪除 ODB 網路。

主控台

1. 登入 AWS 管理主控台 ，並在 https：//https://console.aws.amazon.com/odb/ 開啟 Oracle Database@AWS 主控台。
2. 在導覽窗格中，選擇 ODB 對等互連。
3. 選取要刪除的 ODB 對等互連。
4. 選擇 刪除。
5. 若要確認刪除，請輸入 **`delete me`** 並選擇刪除。

AWS CLI

若要刪除 ODB 對等互連，請使用 `delete-odb-peering-connection`命令。

```
aws odb delete-odb-peering-connection \
    --odb-peering-connection-id odbpcx-1234567890abcdef
```

在 Oracle Database@ 中備份AWS

Oracle Database@AWS 提供多個備份選項來保護您的 Oracle 資料庫。您可以使用與 Amazon S3 無縫整合的 Oracle 受管備份，或使用 Oracle Recovery Manager (RMAN) 建立自己的使用者受管備份。

Amazon S3 的 Oracle 受管備份

當您建立 ODB 網路時，Oracle Database@AWS 會自動設定 Oracle 受管備份對 Amazon S3 的網路存取。OCI 會設定必要的 DNS 項目和安全清單。這些組態允許 OCI Virtual Cloud Network (VCN) 和 Amazon S3 之間的流量。ODB 網路不會啟用或控制自動備份。

Oracle 受管備份完全由 OCI 管理。當您建立 Oracle Exadata 資料庫時，您可以選擇在 OCI 主控台中啟用自動備份，以啟用自動備份。選擇下列其中一個備份目的地：

- Amazon S3
- OCI 物件儲存
- 自主復原服務

如需詳細資訊，請參閱 OCI 文件中的備份 Exadata 資料庫。

使用者受管備份至 Oracle Database@ 中的 Amazon S3 AWS

使用 Oracle Database@AWS，您可以使用專用基礎設施上的 Exadata Database Service 建立資料庫的使用者受管備份。您可以使用 Oracle Recovery Manager (RMAN) 備份資料，並將其存放在 Amazon S3 儲存貯體中。您可以完全控制備份排程、保留政策和儲存成本，同時維護 Oracle Database@ 的受管服務優勢AWS。

> **Note**
>
> Oracle Database@AWS does 不支援專用基礎設施上自治資料庫的使用者受管備份。

使用者受管備份補充 Oracle Database@ 提供的 AWS 受管備份解決方案AWS。您可以使用手動備份來滿足合規要求、跨區域災難復原，或與現有備份管理工作流程整合。

您可以使用下列使用者受管備份技術：

Oracle Secure Backup

以最佳效能將備份直接串流至 Amazon S3。

Storage Gateway

使用 Storage Gateway 進行使用 NFS 共用的檔案型備份。

S3 掛載點

使用檔案用戶端將 Amazon S3 儲存貯體掛載為本機檔案系統。

使用者受管備份至 Oracle Database@ 中 Amazon S3 的先決條件AWS

在將 Oracle Exadata 資料庫備份至 Amazon S3 之前，請執行下列動作：

1. 啟用從您的 ODB 網路直接存取 Amazon S3。
2. 設定 Oracle Database@ 和 Amazon S3 之間的網路連線AWS 和路由。

啟用從 ODB 網路到 Amazon S3 的存取權

若要手動將資料庫備份至 Amazon S3，請啟用從您的 ODB 網路直接存取 S3。此技術可讓您的資料庫根據您的業務需求存取 Amazon S3，例如資料匯入/匯出或使用者管理的備份。您可以完全控制備份儲存的目標目的地，並使用 政策來限制使用 VPC Lattice 存取 Amazon S3。

預設不會啟用從您的 ODB 網路直接存取 Amazon S3。您可以在建立或修改 ODB 網路時啟用 S3 存取。

主控台

啟用從您的 ODB 網路直接存取 Amazon S3

1. 在 https：//https://console.aws.amazon.com/odb/ 開啟 Oracle Database@AWS console。
2. 在導覽窗格中，選擇 ODB 網路。
3. 選取您要啟用 Amazon S3 存取的 ODB 網路。
4. 選擇 Modify (修改)。
5. 選取 Amazon S3。
6. （選用）設定 Amazon S3 政策文件以控制對 Amazon S3 的存取。如果您未指定政策，預設政策會授予完整存取權。
7. 選擇繼續，然後選擇修改。

AWS CLI

若要從 ODB 網路啟用直接 Amazon S3 存取，請使用 `update-odb-network`命令搭配 `s3-access` 參數：

```
aws odb update-odb-network \
  --odb-network-id odb-network-id \
  --s3-access ENABLED
```

若要設定 Amazon S3 政策文件，請使用 `--s3-policy-document` 參數：

```
aws odb update-odb-network \
  --odb-network-id odb-network-id \
  --s3-policy-document file://s3-policy.json
```

啟用 Amazon S3 存取時，您可以使用區域 DNS 從您的 ODB 網路存取 Amazon S3`s3.region.amazonaws.com`。OCI 預設會設定此 DNS 名稱。若要使用自訂 DNS 名稱，請修改 VCN DNS，以確保自訂 DNS 解析為服務網路端點的 IP 地址。

設定 Oracle Database@AWS 與 Amazon S3 之間的網路連線

若要允許使用者受管備份至 Amazon S3，您的 VM 必須能夠存取 S3 Amazon VPC 端點。在 OCI 主控台中，您可以編輯網路安全群組 (NSG) 中的安全規則，以控制輸入和輸出流量。對於使用者受管備份，流量會流經用戶端子網路，而不是備份子網路。在下列步驟中，您會更新用戶端子網路NSGs，以新增 VPC 端點 IP 地址的輸出規則。

允許 VM 存取 Amazon S3 端點

1. 在 https：//https://console.aws.amazon.com/odb/ 開啟 Oracle Database@AWS console。
2. 選擇 ODB 網路。
3. 選擇 ODB 網路的名稱。
4. 選擇 OCI 資源。
5. 選擇服務整合索引標籤。
6. 在 Amazon S3 下，請注意下列資訊：

   - Amazon VPC S3 端點的 IPv4 地址。您稍後需要此資訊。例如，IP 地址可能是 `192.168.12.223`。
   - Amazon VPC S3 端點的網域名稱。您稍後需要此資訊。例如，網域名稱可能是 `s3.us-east-1.amazonaws.com`。

7. 在左側導覽窗格中，選擇 Exadata VM 叢集，然後選擇您的 VM 叢集名稱。
8. 在頁面頂端，選擇摘要索引標籤。
9. 選擇虛擬機器，然後選擇 VM 的名稱。
10. 請注意 DNS 名稱中的值。這是您使用 連線到 VM 時指定的主機名稱ssh。
11. 在右上角，選擇在 OCI 中管理。這會開啟 OCI 主控台。
12. 在虛擬雲端網路清單頁面上，選擇包含 ODB 網路用戶端子網路 () 網路安全群組 (NSG) 的 VCNexa_static_nsg。如需詳細資訊，請參閱 OCI 文件中的管理 NSG 的安全規則。
13. 在詳細資訊頁面上，根據您看到的選項執行下列其中一個動作：
    - 在安全索引標籤上，前往網路安全群組。
    - 在資源下，選擇網路安全群組。
14. 選擇用戶端子網路的 NSG (exa_static_nsg)。
15. 為您先前記下的 VPC 端點地址新增輸出規則。

從 VM 測試對 S3 的連線

1. 使用 ssh 將 root 連接至您先前取得 DNS 名稱的 VM。連線時，請使用 SSH 金鑰指定.pem檔案。
2. 執行下列命令，以確保 VM 可以存取 Amazon S3 Amazon VPC 端點。使用您先前記下的 S3 網域名稱。

```
# nslookup s3.us-east-1.amazonaws.com
# curl -v https://s3.us-east-1.amazonaws.com/
# aws s3 ls --endpoint-url https://s3.us-east-1.amazonaws.com
```

使用 Oracle Secure Backup 備份至 Amazon S3

Oracle Secure Backup 可做為搭配 Recovery Manager (RMAN) 使用的 SBT 界面。您可以使用 RMAN 搭配 Oracle Secure Backup，將 Oracle Database@AWS databases 直接備份至 Amazon S3。Oracle Secure Backup 提供下列優點：

- Oracle Secure Backup 可最佳化 RMAN 和 S3 之間的資料傳輸。
- 不需要中繼備份儲存。
- Oracle Secure Backup 會管理備份媒體的生命週期。

使用 Oracle Secure Backup 備份至 Amazon S3

1. 在 Exadata VM 伺服器上安裝 Oracle Secure Backup 模組。將預留位置值取代為您的 AWS 存取金鑰和私密存取金鑰。如需詳細資訊，請參閱 Backup to Cloud with Oracle Secure Backup Cloud Module 中的 Oracle 文件。

```
cd $ORACLE_HOME/lib
java -jar osbws_install.jar -AWSID aws-access-key-id -AWSKey aws-secret-access-
key -walletDir $ORACLE_HOME/dbs/osbws_wallet -location us-west-2 -useHttps -
awsEndPoint s3.us-west-2.amazonaws.com
```

2. 連線至 RMAN 並設定備份通道和預設裝置類型。

```
RMAN target /
RMAN> CONFIGURE CHANNEL DEVICE TYPE 'SBT_TAPE' PARMS 'SBT_LIBRARY=/u02/app/oracle/
product/19.0.0.0/dbhome_2/lib/libosbws.so, ENV=(OSB_WS_PFILE=/u02/app/oracle/
product/19.0.0.0/dbhome_2/dbs/osbwssmalikdb1.ora)';
RMAN> CONFIGURE DEFAULT DEVICE TYPE TO 'SBT_TAPE';
```

3. 驗證組態。

```
RMAN> SHOW ALL;
```

4. 備份資料庫。

```
RMAN> BACKUP DATABASE;
```

5. 確認備份已成功完成。

```
RMAN> LIST BACKUP OF DATABASE SUMMARY;
```

在 Amazon EC2 上使用 備份至 Amazon S3 AWS Storage Gateway Amazon EC2

AWS Storage Gateway 是一種混合式服務，可將您的現場部署環境連線至 AWS 雲端 儲存服務。對於 Oracle Database@AWS backups，您可以使用 Storage Gateway 建立直接寫入 Amazon S3 的檔案型備份工作流程。與 Oracle Secure Backup 技術不同，您可以管理備份的生命週期。

在此解決方案中，您會建立個別的 Amazon EC2 執行個體來設定 Storage Gateway。您也可以新增 Amazon EBS 磁碟區，以快取讀取和寫入 Amazon S3。

此技術提供下列優點：

- 您不需要 Oracle Secure Backup 等媒體管理員。
- 不需要中繼備份儲存。

部署 Storage Gateway 並建立檔案共享

1. AWS 管理主控台 在 https：//https://console.aws.amazon.com/storagegateway/home/ 開啟 ，然後選擇您要建立閘道 AWS 的區域。
2. 使用 Amazon EC2 執行個體做為中樞，部署和啟用 Amazon S3 檔案閘道。 Amazon EC2 遵循 Storage Gateway Gateway 使用者指南中部署 S3 File Gateway 的自訂 Amazon EC2 主機中的指示。

   當您設定檔案閘道時，請務必執行下列動作：

   - 為快取儲存新增至少一個 Amazon EBS 磁碟區，其大小至少為 150 GiB。
   - 開啟安全群組中 NFS 存取的 TCP/UDP 連接埠 2049。這可讓您建立 NFS 檔案共享。
   - 為傳入流量開啟 TCP 連接埠 80，以在閘道啟用期間允許一次性 HTTP 存取。啟用後，您可以關閉此連接埠。
3. 建立 Amazon VPC 端點，以便在 ODB 網路和 Storage Gateway 之間進行私有連線。如需詳細資訊，請參閱使用介面 VPC 端點存取 AWS 服務。
4. 透過 Storage Gateway 主控台建立 Amazon S3 儲存貯體的檔案共享。如需詳細資訊，請參閱建立檔案共享。

使用 Storage Gateway 將資料庫備份至 Amazon S3

1. 在終端機中，使用 ssh 連線到 Exadata VM 的 DNS 名稱。若要尋找 DNS 名稱，請參閱 使用者受管備份至 Oracle Database@ 中 Amazon S3 的先決條件AWS。
2. 在適用於 NFS 掛載的 Exadata VM 叢集伺服器上建立目錄。下列範例會建立 /home/oracle/sgw_mount/ 目錄。

   ```
   mkdir /home/oracle/sgw_mount/
   ```

3. 在您剛建立的目錄中掛載 NFS 共用。下列範例會在目錄 上建立共用/home/oracle/sgw_mount/。將 *SG-IP-address* 取代為您的 Storage Gateway IP 地址，並將 *your-bucket-name* 取代為您的 S3 儲存貯體名稱。

```
sudo mount -t nfs -o nolock,hard SG-IP-address:/your-bucket-name /home/oracle/
sgw_mount/
```

4. 連線至 RMAN 並將資料庫備份至掛載的目錄。下列範例會建立頻道rman_local_bkp，並使用掛載點路徑來格式化備份片段。

```
$ rman TARGET /
RMAN> ALLOCATE CHANNEL rman_local_bkp DEVICE TYPE DISK;
RMAN> BACKUP FORMAT '/home/oracle/sgw_mount/%U' DATABASE;
```

5. 確認已在掛載目錄中建立備份檔案。下列範例顯示兩個備份片段。

```
$ ls -lart /home/oracle/sgw_mount/
total 8569632
-rw-r----- 1 oracle asmdba 1112223334 Jul 10 20:51 1a2b34cd_1234_1_1
drwxrwxrwx 1 nobody nobody 0 Jul 10 20:56 .
-rw-r----- 1 oracle asmdba 5556667778 Jul 10 20:56 1a2b34cd_1235_1_1
```

使用 Amazon S3 S3

您可以使用 Amazon S3 掛載點先在本機建立備份，然後將其複製到 Amazon S3。此技術會在本機儲存體上建立備份，然後使用掛載點界面將其傳輸至 Amazon S3。備份時間比其他技術更長，因為您需要備份資料兩次。

> **Note**
>
> 不支援使用掛載點直接備份至 Amazon S3，無需預備。RMAN 需要與 Amazon S3 掛載點界面不相容的特定檔案系統許可。

此技術不需要您授權媒體管理員，例如 Oracle Secure Backup。您可以管理備份的生命週期。

使用 Amazon S3 S3

1. 在終端機中，使用 ssh 連線到 Exadata VM 的 DNS 名稱。若要尋找 DNS 名稱，請參閱 使用者受管備份至 Oracle Database@ 中 Amazon S3 的先決條件AWS。
2. 在 Exadata VM 叢集伺服器上安裝 Amazon S3 掛載點。如需安裝和組態的詳細資訊，請參閱《Amazon S3 使用者指南》中的適用於 Amazon S3 的掛載點。 Amazon S3

```
$ sudo yum install ./mount-s3.rpm
```

3. 執行 mount-s3命令來驗證安裝。

```
$ mount-s3 --version
mount-s3 1.19.0
```

4. 在 Exadata VM 叢集伺服器本機儲存體上建立中繼備份目錄。您將將資料庫備份至此本機目錄，然後將備份複製到 S3 儲存貯體。下列範例會建立目錄 /u02/rman_bkp_local。

```
mkdir /u02/rman_bkp_local
```

5. 建立 Amazon S3 掛載點的目錄。下列範例會建立目錄 /home/oracle/s3mount。

```
$ mkdir /home/oracle/s3mount
```

6. 使用掛載點掛載 Amazon S3 儲存貯體。下列範例會在目錄 上掛載 S3 儲存貯體/home/oracle/s3mount。以實際的 Amazon S3*3 ######## your-s3-bucket-*name。

```
$ mount-s3 s3://your-s3-bucket-name /home/oracle/s3mount
```

7. 確認您可以存取 Amazon S3 儲存貯體內容。

```
$ ls -lart /home/oracle/s3mount
```

8. 將 RMAN 連接到您的目標資料庫，並將其備份到本機預備目錄。下列範例會建立 頻道，rman_local_bkp並使用 路徑/u02/rman_bkp_local/來格式化備份片段。

```
$ rman TARGET /

RMAN> ALLOCATE CHANNEL rman_local_bkp DEVICE TYPE DISK;
RMAN> BACKUP FORMAT '/u02/rman_bkp_local/%U' DATABASE;
```

9. 確認已在本機目錄中建立備份：

```
$ cd /u02/rman_bkp_local/
$ ls -lart
total 4252128
drwxr-xr-x 8 oracle oinstall 4096 Jul 10 02:13 ..
-rw-r----- 1 oracle asmdba 1112223334 Jul 10 02:13 abcd1234_1921_1_1
drwxr-xr-x 2 oracle oinstall 4096 Jul 10 02:13 .
```

```
-rw-r----- 1 oracle asmdba 5556667778 Jul 10 02:14 abcd1234_1922_1_1
```

10. 將備份檔案從本機預備目錄複製到 Amazon S3 掛載點。

```
cp /u02/rman_bkp_local/* /home/oracle/s3mount/
```

11. 確認您已成功將檔案複製到 Amazon S3。

```
$ ls -lart /home/oracle/s3mount/
total 4252112
drwx------ 6 oracle oinstall 225 Jul 10 02:09 ..
drwxr-xr-x 2 oracle oinstall 0 Jul 10 02:24 .
-rw-r--r-- 1 oracle oinstall 1112223334 Jul 10 02:24 abcd1234_1921_1_1
-rw-r--r-- 1 oracle oinstall 5556667778 Jul 10 02:24 abcd1234_1922_1_1
```

停用直接存取 Amazon S3

如果您不再需要從 ODB 網路直接存取 Amazon S3，您可以停用它。啟用或停用對 S3 的直接網路存取不會影響對 Oracle 受管備份對 Amazon S3 的網路存取。

主控台

停用對 Amazon S3 的直接存取

1. 在 https：//https://console.aws.amazon.com/odb/ 開啟 Oracle Database@AWS console。
2. 在導覽窗格中，選擇 ODB 網路。
3. 選取您要停用 Amazon S3 存取的 ODB 網路。
4. 選擇 Modify (修改)。
5. 清除啟用 S3 存取核取方塊。
6. 選擇修改 ODB 網路。

AWS CLI

使用具有 `s3-access` 參數的 `update-odb-network` 命令。

```
aws odb update-odb-network \
  --odb-network-id odb-network-id \
  --s3-access DISABLED
```

Amazon S3 整合疑難排解

如果您遇到 Oracle 受管備份至 Amazon S3 或直接存取 Amazon S3 的問題，請考慮下列疑難排解步驟：

無法從您的資料庫存取 Amazon S3

請檢查以下內容：

- 確認您的 ODB 網路已啟用 Amazon S3 存取。使用 `GetOdbNetwork`動作來檢查`s3Access`狀態是否為 `Enabled`。
- 請確定您使用的是正確的區域 DNS 名稱：`s3.region.amazonaws.com`。
- 檢查您的 Oracle 資料庫是否具有存取 Amazon S3 的必要許可。

Oracle 受管備份失敗

請檢查以下內容：

- Amazon S3 的 Oracle 受管備份預設為啟用，無法停用。如果備份失敗，請檢查 Oracle 資料庫日誌是否有特定錯誤訊息。
- 檢視服務整合資源，確認 Amazon VPC Lattice 資源已正確設定。
- 如需 Oracle 受管自動備份問題的協助，請聯絡 Oracle Support。如需詳細資訊，請參閱取得 Oracle Database@ 的支援AWS。

Oracle Database@AWS Zero-ETL 與 Amazon Redshift 整合

零 ETL 整合是一種全受管解決方案，可讓 Amazon Redshift 從多個來源取得交易和操作資料。使用此解決方案，您可以從 Oracle Exadata 上執行的 Oracle 資料庫或專用 Exadata Infrastructure 上的自治資料庫，將資料複寫至 Amazon Redshift。自動同步可避免傳統擷取、轉換和載入 (ETL) 程序。它也可以啟用即時分析和 AI 工作負載。如需詳細資訊，請參閱《Amazon Redshift 管理指南》中的零 ETL 整合。

零 ETL 整合提供下列優點：

- 即時資料複寫 – 從 Oracle 資料庫持續資料同步至 Amazon Redshift，並將延遲降至最低
- 消除複雜的 ETL 管道 – 不需要建置和維護自訂資料整合解決方案
- 降低營運開銷 – 透過 AWS APIs 自動化設定和管理
- 簡化的資料整合架構 – Oracle Database@AWS 與 AWS 分析服務之間的無縫整合
- 增強安全性 – 內建加密和 AWS IAM 存取控制

Amazon Redshift 不會針對與 Oracle Database@ 的零 ETL 整合收取額外費用AWS。您支付用來建立和處理作為零 ETL 整合一部分所建立之變更資料的現有 Amazon Redshift 資源的費用。如需詳細資訊，請參閱 Amazon Redshift 定價。

Oracle Database@ 中零 ETL 整合支援的資料庫版本AWS

零 ETL 整合支援下列 Oracle 資料庫版本：

- Oracle Exadata – Oracle 資料庫 19c
- 專用基礎設施上的自治資料庫 – Oracle Database 19c 和 23ai

零 ETL 整合如何在 Oracle Database@ 中運作AWS

零 ETL 整合可讓 Oracle Database@AWS 將資料複寫至 Amazon Redshift。整合利用 Amazon VPC Lattice 來建立安全的網路連線。變更資料擷取 (CDC) 技術可確保即時資料同步。您可以透過 AWS Glue APIs管理整合。

零 ETL 整合架構包括下列項目：

- 安全連線 – 透過 TLS 連接埠 2484 使用 SSL/TLS 加密進行資料傳輸

- AWS Secrets Manager – 使用 AWS Key Management Service 安全地存放資料庫登入資料和憑證
- AWS Glue 整合 – 為零 ETL 整合提供統一的管理界面

複寫會繼續進行下列步驟：

1. 在連接埠 2484 上使用 SSL 建立 Oracle 資料庫的安全連線
2. 執行所選資料庫、結構描述和資料表的初始完整傾印
3. 設定變更資料擷取 (CDC) 以進行持續的即時複寫
4. 將複寫的資料寫入目標 Amazon Redshift 叢集

> **Important**
>
> 預設不會啟用零 ETL 整合。您必須使用 AWS Glue APIs進行設定。您無法直接使用 Oracle Database@AWS APIs 設定零 ETL 整合。

Oracle Database@ 中零 ETL 整合的先決條件AWS

設定零 ETL 整合之前，請確定您符合下列先決條件。

一般先決條件

- Oracle Database@AWS setup – 確認您至少已佈建並執行一個 VM 叢集。
- 與啟用零 ETL 的整合 – 確保您的 VM 叢集或自治 VM 叢集與啟用零 ETL 的 ODB 網路相關聯。
- 支援的 Oracle 資料庫版本 – 您必須使用 Oracle Database 19c (Oracle Exadata) 或 Oracle Database 19c/23ai （專用基礎設施上的自主資料庫）。
- 相同 AWS 區域 – 來源 Oracle 資料庫和目標 Amazon Redshift 叢集必須位於相同 AWS 區域。

Oracle 資料庫先決條件

您必須使用下列設定來設定 Oracle 資料庫。

複寫使用者設定

在您要複寫的每個可插入資料庫 (PDB) 中建立專用複寫使用者：

- 對於 Oracle Exadata – ODBZEROETLADMIN建立具有安全密碼的使用者。
- 對於專用基礎設施上的自治資料庫 – 使用現有GGADMIN使用者。

將下列許可授予複寫使用者。

```
-- For Autonomous Database on Dedicated Infrastructure only
ALTER USER GGADMIN ACCOUNT UNLOCK;
ALTER USER GGADMIN IDENTIFIED BY ggadmin-password;

-- For Oracle Exadata only
GRANT SELECT ON any-replicated-table TO "ODBZEROETLADMIN";
GRANT LOGMINING to "ODBZEROETLADMIN";

-- Grant the following permissions to all services.
-- For Oracle Exadata, use the ODBZEROETLADMIN user. For Autonomous Database on
 Dedicated Infrastructure,
-- use the GGADMIN user.
GRANT CREATE SESSION TO "ODBZEROETLADMIN";
GRANT SELECT ANY TRANSACTION TO "ODBZEROETLADMIN";
GRANT SELECT ON V_$ARCHIVED_LOG TO "ODBZEROETLADMIN";
GRANT SELECT ON V_$LOG TO "ODBZEROETLADMIN";
GRANT SELECT ON V_$LOGFILE TO "ODBZEROETLADMIN";
GRANT SELECT ON V_$LOGMNR_LOGS TO "ODBZEROETLADMIN";
GRANT SELECT ON V_$LOGMNR_CONTENTS TO "ODBZEROETLADMIN";
GRANT SELECT ON V_$DATABASE TO "ODBZEROETLADMIN";
GRANT SELECT ON V_$THREAD TO "ODBZEROETLADMIN";
GRANT SELECT ON V_$PARAMETER TO "ODBZEROETLADMIN";
GRANT SELECT ON V_$NLS_PARAMETERS TO "ODBZEROETLADMIN";
GRANT SELECT ON V_$TIMEZONE_NAMES TO "ODBZEROETLADMIN";
GRANT SELECT ON V_$TRANSACTION TO "ODBZEROETLADMIN";
GRANT SELECT ON V_$CONTAINERS TO "ODBZEROETLADMIN";
GRANT SELECT ON ALL_INDEXES TO "ODBZEROETLADMIN";
GRANT SELECT ON ALL_OBJECTS TO "ODBZEROETLADMIN";
GRANT SELECT ON ALL_TABLES TO "ODBZEROETLADMIN";
GRANT SELECT ON ALL_USERS TO "ODBZEROETLADMIN";
GRANT SELECT ON ALL_CATALOG TO "ODBZEROETLADMIN";
GRANT SELECT ON ALL_CONSTRAINTS TO "ODBZEROETLADMIN";
GRANT SELECT ON ALL_CONS_COLUMNS TO "ODBZEROETLADMIN";
GRANT SELECT ON ALL_TAB_COLS TO "ODBZEROETLADMIN";
GRANT SELECT ON ALL_IND_COLUMNS TO "ODBZEROETLADMIN";
GRANT SELECT ON ALL_ENCRYPTED_COLUMNS TO "ODBZEROETLADMIN";
GRANT SELECT ON ALL_LOG_GROUPS TO "ODBZEROETLADMIN";
```

```
GRANT SELECT ON ALL_TAB_PARTITIONS TO "ODBZEROETLADMIN";
GRANT SELECT ON SYS.DBA_REGISTRY TO "ODBZEROETLADMIN";
GRANT SELECT ON SYS.OBJ$ TO "ODBZEROETLADMIN";
GRANT SELECT ON DBA_TABLESPACES TO "ODBZEROETLADMIN";
GRANT SELECT ON DBA_OBJECTS TO "ODBZEROETLADMIN";
GRANT SELECT ON SYS.ENC$ TO "ODBZEROETLADMIN";
GRANT SELECT ON GV_$TRANSACTION TO "ODBZEROETLADMIN";
GRANT SELECT ON V_$DATAGUARD_STATS TO "ODBZEROETLADMIN";
GRANT SELECT ON V_$DATABASE_INCARNATION TO "ODBZEROETLADMIN";
GRANT EXECUTE ON SYS.DBMS_CRYPTO TO "ODBZEROETLADMIN";
GRANT SELECT ON SYS.DBA_DIRECTORIES TO "ODBZEROETLADMIN";
GRANT SELECT ON ALL_VIEWS TO "ODBZEROETLADMIN";
GRANT SELECT ON DBA_SEGMENTS TO "ODBZEROETLADMIN";
GRANT SELECT ON V_$TRANSPORTABLE_PLATFORM TO "ODBZEROETLADMIN";
GRANT CREATE ANY DIRECTORY TO "ODBZEROETLADMIN";
GRANT EXECUTE ON DBMS_FILE_TRANSFER TO "ODBZEROETLADMIN";
GRANT EXECUTE ON DBMS_FILE_GROUP TO "ODBZEROETLADMIN";
GRANT EXECUTE on DBMSLOGMNR to "ODBZEROETLADMIN";
GRANT SELECT on V_$LOGMNRLOGS to "ODBZEROETLADMIN";
GRANT SELECT on V_$LOGMNRCONTENTS to "ODBZEROETLADMIN";
GRANT LOGMINING to "ODBZEROETLADMIN";
GRANT SELECT ON GV_$CELL_STATE TO "ODBZEROETLADMIN";
```

補充記錄

在您的 Oracle 資料庫上啟用補充記錄，以擷取變更資料。

```
-- Check if supplemental logging is enabled
SELECT supplemental_log_data_min FROM v$database;

-- Enable supplemental logging if not already enabled.
-- For Oracle Exadata, enable supplemental logging on both the CDB and PDB.
-- For Autonomous Database on Dedicated Infrastructure, enable supplemental logging on
 the PDB only.
ALTER DATABASE ADD SUPPLEMENTAL LOG DATA;

-- For Autonomous Database on Dedicated Infrastructure only
ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (PRIMARY KEY) COLUMNS;

-- Archive current online redo log
ALTER SYSTEM ARCHIVE LOG CURRENT;
```

若要設定 Oracle Database@AWS 與 Amazon Redshift 之間的零 ETL 整合，您必須設定 SSL。

對於 Oracle Exadata 資料庫

您必須在連接埠 2484 上手動設定 SSL。此任務包含下列項目：

- 在 (PROTOCOL=tcps)(PORT=2484)中設定 listener.ora
- 使用 設定錢包 sqlnet.ora
- 產生和設定 SSL 憑證 （ 請參閱 My Oracle Support 文件中的如何設定 Exadata Cloud Database (ExaCC/ExaCS) （ 文件 ID 2947301.1))

對於自治資料庫

連接埠 2484 上的 SSL 預設為啟用。不需任何其他設定。

> **Important**
>
> SSL 連接埠固定為 2484。

AWS 服務先決條件

在設定零 ETL 整合之前，請設定 AWS Secrets Manager 並設定 IAM 許可。

設定 AWS Secrets Manager

將 Oracle 資料庫登入資料儲存在 AWS Secrets Manager 中，如下所示：

1. 在 Key Management Service 中建立客戶受管 AWS 金鑰 (CMK)。
2. 使用 CMK 將資料庫登入資料儲存在 AWS Secrets Manager 中。
3. 設定資源政策以允許 Oracle Database@AWS access。

若要取得 TDE 金鑰 ID 和密碼，請使用支援加密方法中所述的技術，以使用 Oracle 做為 AWS Database Migration Service 的來源。下列命令會產生 base64 錢包。

```
base64 -i cwallet.sso > wallet.b64
```

下列範例顯示 Oracle Exadata 的秘密。對於 *asm_service_name* ，*111.11.11.11* 代表 VM 節點的虛擬 IP。您也可以向 SCAN 註冊 ASM 接聽程式。

```
{
```

```
  "database_info": [
    {
      "name": "ODBDB_ZETLPDB",
      "service_name": "ODBDB_ZETLPDB.paas.oracle.com",
      "username": "ODBZEROETLADMIN",
      "password": "secure_password",
      "tde_key_id": "ORACLE.SECURITY.DB.ENCRYPTION.key_id",
      "tde_password": "tde_password",
      "certificateWallet": "base64_encoded_wallet_content"
    }
  ],
  "asm_info": {
    "asm_user": "odbzeroetlasm",
    "asm_password": "secure_password",
    "asm_service_name": "111.11.11.11:2484/+ASM"
  }
}
```

下列範例顯示專用基礎設施上自治資料庫的秘密。

```
{
  "database_info": [
    {
      "database_name": "ZETLACD_ZETLADBMORECPU",
      "service_name": "ZETLADBMORECPU_high.adw.oraclecloud.com",
      "username": "ggadmin",
      "password": "secure_password",
      "certificateWallet": "base64_encoded_wallet_content"
    }
  ]
}
```

設定 IAM 許可

建立允許零 ETL 整合操作的 IAM 政策。下列範例政策允許描述、建立、更新和刪除 Exadata VM 叢集的操作。對於自治 VM 叢集，請使用 值`cloud-autonomous-vm-cluster`，而不是資源 ARN `cloud-vm-cluster`的值。

Oracle Database@ 中零 ETL 整合的考量事項AWS

在 Oracle Database@AWS 和 Amazon Redshift 之間設定零 ETL 整合時，請考慮下列準則：

初始資料載入時間

初始完全載入時間取決於資料庫的大小。大型資料庫可能需要數小時或數天才能完成初始同步。

Oracle 資料庫效能

變更資料擷取可能會影響 Oracle 資料庫效能，尤其是在高交易量期間。啟用零 ETL 整合之後，請監控資料庫效能。

結構描述變更

來源 Oracle 資料庫中的資料定義語言 (DDL) 變更可能需要您手動介入以重新建立整合。仔細計劃結構描述變更。

如需一般考量，請參閱將零 ETL 整合與 Amazon Redshift 搭配使用時的考量。

Oracle Database@ 中零 ETL 整合的限制AWS

請注意下列一般限制：

每次整合單一 PDB

每個零 ETL 整合只能從一個可插入資料庫 (PDB) 複寫資料。`include: pdb1.*.*, include: pdb2.*.*` 不支援 等資料篩選條件。

每個自治資料庫或 Exadata 基礎設施的單一整合

每個零 ETL 整合只能從專用基礎設施上的一個自治資料庫複寫資料。

固定 SSL 連接埠

SSL 連線必須使用連接埠 2484。

相同的區域需求

來源 Oracle Database@AWS VM 叢集和目標 Amazon Redshift 叢集必須位於相同的 AWS 區域。不支援跨區域複寫。

沒有 mTLS 支援

不支援相互 TLS (mTLS)。如果您的 OCI 資料庫已啟用 mTLS，您必須停用它才能使用零 ETL 整合。

不可避免的整合設定

建立與整合相關聯的秘密 ARN 或 KMS 金鑰之後，您就無法修改它。您必須刪除並重新建立整合，才能變更這些設定。

TDE 資料欄層級加密

Oracle Exadata 資料庫不支援資料欄層級透明資料加密 (TDE)。僅支援資料表空間層級 TDE。

支援的資料類型

某些 Oracle 特定的資料類型可能未完全支援，或可能需要在複寫期間進行轉換。在將資料庫部署到生產環境之前，請徹底測試您的特定資料類型。

使用 Amazon Redshift 設定 Oracle Database@AWS integrations

若要設定 Oracle 資料庫與 Amazon Redshift 之間的零 ETL 整合，請完成下列步驟：

1. 在 ODB 網路上啟用零 ETL。
2. 設定 Oracle 資料庫先決條件。
3. 設定 AWS Secrets Manager 和 AWS Key Management Service。
4. 設定 IAM 許可。
5. 設定 Amazon Redshift 資源政策。
6. 建立零 ETL 整合。
7. 在 Amazon Redshift 中建立目標資料庫。

步驟 1：為您的 ODB 網路啟用零 ETL

您可以為與來源 VM 叢集相關聯的 ODB 網路啟用零 ETL 整合。預設會停用此整合。

主控台

啟用零 ETL 整合

1. 在 https：//https://console.aws.amazon.com/odb/ 開啟 Oracle Database@AWS console。
2. 在導覽窗格中，選擇 ODB 網路。
3. 選取您要啟用零 ETL 整合的 ODB 網路。
4. 選擇 Modify (修改)。

5. 選取零 ETL。
6. 選擇繼續，然後選擇修改。

AWS CLI

若要啟用零 ETL 整合，請使用 `update-odb-network`命令搭配 `--zero-etl-access` 參數：

```
aws odb update-odb-network \
  --odb-network-id odb-network-id \
  --zero-etl-access ENABLED
```

若要為與來源 VM 叢集相關聯的 ODB 網路啟用零 ETL 整合，請使用 `update-odb-network`命令。此命令會設定零 ETL 整合所需的網路基礎設施。

```
aws odb update-odb-network \
  --odb-network-id your-odb-network-id \
  --zero-etl-access ENABLED
```

步驟 2：設定 Oracle 資料庫

完成 Oracle 資料庫組態，如先決條件中所述：

- 建立複寫使用者並授予必要的許可。
- 啟用封存的重做日誌。
- 設定 SSL （僅限 Oracle Exadata)。
- 如果適用，請設定 ASM 使用者 （僅限 Oracle Exadata)。

步驟 3：設定 AWS Secrets Manager 和 AWS Key Management Service

建立客戶受管金鑰 (CMK) 並存放您的資料庫登入資料。

1. 使用 `create-key`命令在 AWS Key Management Service 中建立 CMK。

   ```
   aws kms create-key \
     --description "ODB Zero-ETL Integration Key" \
     --key-usage ENCRYPT_DECRYPT \
     --key-spec SYMMETRIC_DEFAULT
   ```

2. 將您的資料庫登入資料儲存在 AWS Secrets Manager 中。

```
aws secretsmanager create-secret \
  --name "ODBZeroETLCredentials" \
  --description "Credentials for Oracle Database@AWS Zero-ETL integration" \
  --kms-key-id your-cmk-key-arn \
  --secret-string file://secret-content.json
```

3. 將資源政策連接至秘密，以允許 Oracle Database@AWS access。

```
aws secretsmanager put-resource-policy \
  --secret-id "ODBZeroETLCredentials" \
  --resource-policy file://secret-resource-policy.json
```

在上述命令中， `secret-resource-policy.json`包含下列 JSON。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "zetl.odb.amazonaws.com"
      },
      "Action": [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret"
      ],
      "Resource": "*"
    }
  ]
}
```

4. 將資源政策連接至 CMK。CMK 資源政策必須包含 Oracle Database@AWS service 主體和 Amazon Redshift 服務主體的許可，以支援加密的零 ETL 整合。

```
aws kms put-key-policy \
  --key-id your-cmk-key-arn \
  --policy-name default \
  --policy file://cmk-resource-policy.json
```

cmk-resource-policy.json 檔案應包含下列政策陳述式。第一個陳述式允許 Oracle Database@AWS service 存取，第二個陳述式允許 Amazon Redshift 在 KMS 金鑰上為加密的資料操作建立授予。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "Allow ODB service access",
      "Effect": "Allow",
      "Principal": {
        "Service": "zetl.odb.amazonaws.com"
      },
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "kms:CreateGrant"
      ],
      "Resource": "*"
    },
    {
      "Sid": "Allows the Redshift service principal to add a grant to a KMS
 key",
      "Effect": "Allow",
      "Principal": {
        "Service": "redshift.amazonaws.com"
      },
      "Action": "kms:CreateGrant",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "kms:EncryptionContext:{context-key}": "{context-value}"
        },
        "ForAllValues:StringEquals": {
          "kms:GrantOperations": [
            "Decrypt",
            "GenerateDataKey",
            "CreateGrant"
          ]
```

```
        }
      }
    }
  ]
}
```

步驟 4：設定 IAM 許可

建立並連接允許零 ETL 整合操作的 IAM 政策。

```
aws iam create-policy \
  --policy-name "ODBZeroETLIntegrationPolicy" \
  --policy-document file://odb-zetl-iam-policy.json

aws iam attach-user-policy \
  --user-name your-iam-username \
  --policy-arn policy-arn
```

下列政策會授予必要的許可。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "ODBGlueIntegrationAccess",
      "Effect": "Allow",
      "Action": [
        "glue:CreateIntegration",
        "glue:ModifyIntegration",
        "glue:DeleteIntegration",
        "glue:DescribeIntegrations",
        "glue:DescribeInboundIntegrations"
      ],
      "Resource": "*"
    },
    {
      "Sid": "ODBZetlOperations",
      "Effect": "Allow",
      "Action": "odb:CreateOutboundIntegration",
```

```
      "Resource": "*"
    },
    {
      "Sid": "ODBRedshiftFullAccess",
      "Effect": "Allow",
      "Action": [
        "redshift:*",
        "redshift-serverless:*",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
        "sns:CreateTopic",
        "sns:Get*",
        "sns:List*",
        "cloudwatch:Describe*",
         "cloudwatch:Get*",
        "cloudwatch:List*",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:EnableAlarmActions",
        "cloudwatch:DisableAlarmActions",
        "tag:GetResources",
        "tag:UntagResources",
        "tag:GetTagValues",
        "tag:GetTagKeys",
        "tag:TagResources"
      ],
      "Resource": "*"
    },
    {
      "Sid": "ODBRedshiftDataAPI",
      "Effect": "Allow",
      "Action": [
        "redshift-data:ExecuteStatement",
        "redshift-data:CancelStatement",
        "redshift-data:ListStatements",
        "redshift-data:GetStatementResult",
        "redshift-data:DescribeStatement",
        "redshift-data:ListDatabases",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables",
```

```
        "redshift-data:DescribeTable"
      ],
      "Resource": "*"
    },
    {
      "Sid": "ODBKMSAccess",
      "Effect": "Allow",
      "Action": [
        "kms:CreateKey",
        "kms:DescribeKey",
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "kms:ListKeys",
        "kms:CreateAlias",
        "kms:ListAliases"
      ],
      "Resource": "*"
    },
    {
      "Sid": "ODBSecretsManagerAccess",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue",
        "secretsmanager:CreateSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecrets",
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:PutResourcePolicy",
        "secretsmanager:ValidateResourcePolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

步驟 5：設定 Amazon Redshift 資源政策

在 Amazon Redshift 叢集上設定資源政策，以授權傳入整合。

```
aws redshift put-resource-policy \
  --no-verify-ssl \
  --resource-arn "your-redshift-cluster-arn" \
  --policy '{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Principal": {
          "Service": "redshift.amazonaws.com"
        },
        "Action": [
          "redshift:AuthorizeInboundIntegration"
        ],
        "Condition": {
          "StringEquals": {
            "aws:SourceArn": "your-vm-cluster-arn"
          }
        }
      },
      {
        "Effect": "Allow",
        "Principal": {
          "AWS": "your-account-id"
        },
        "Action": [
          "redshift:CreateInboundIntegration"
        ]
      }
    ]
  }' \
  --region us-west-2
```

Tip

或者，您可以使用 主控台中的 AWS 「為我修正」選項。此選項會自動設定所需的 Amazon Redshift 政策，而不需要手動執行。

步驟 6：使用 建立零 ETL 整合 AWS Glue

使用 命令建立零 ETL AWS Glue `create-integration`整合。在此命令中，您可以指定來源 VM 叢集和目標 Amazon Redshift 命名空間。

下列範例會建立與名為 在 Exadata VM 叢集中`pdb1`執行之 PDB 的整合。您也可以在來源 ARN `cloud-autonomous-vm-cluster`中將 取代`cloud-vm-cluster`為 ，以建立自治 VM 叢集。指定 KMS 金鑰是選用的。如果您指定金鑰，它可以與您在 中建立的金鑰不同步驟 3：設定 AWS Secrets Manager 和 AWS Key Management Service。

```
aws glue create-integration \
  --integration-name "MyODBZeroETLIntegration" \
  --source-arn "arn:aws:odb:region:account:cloud-vm-cluster/cluster-id" \
  --target-arn "arn:aws:redshift:region:account:namespace/namespace-id" \
  --data-filter "include: pdb1.*.*" \
  --integration-config '{
      "RefreshInterval": "10",
      "IntegrationMode": "DEFAULT",
      "SourcePropertiesMap": {
        "secret-arn": "arn:aws:secretsmanager:region:account:secret:secret-name"
      }
    }' \
  --description "Zero-ETL integration for Oracle to Amazon Redshift" \
  --kms-key-id "arn:aws:kms:region:account:key/key-id"
```

命令會傳回整合 ARN，並將狀態設定為 `creating`。您可以使用 `describe-integrations`命令監控整合狀態。

```
aws glue describe-integrations \
  --integration-identifier integration-id
```

> **Important**
>
> 每個整合僅支援一個 PDB。資料篩選條件必須指定單一 PDB，例如 `include: pdb1.*.*`。來源必須位於建立整合的相同 AWS 區域和帳戶中。

步驟 7：在 Amazon Redshift 中建立目標資料庫

整合處於作用中狀態後，請在 Amazon Redshift 叢集中建立目標資料庫。

```
-- Connect to your Amazon Redshift cluster
psql -h your-redshift-endpoint -U username -d database

-- Create database from integration
CREATE DATABASE target_database_name
FROM INTEGRATION 'integration-id'
DATABASE "source_pdb_name";
```

建立目標資料庫之後，您可以查詢複寫的資料。

```
-- List databases to verify creation
\l

-- Connect to the new database
\c target_database_name

-- List tables to see replicated data
\dt
```

驗證零 ETL 整合

透過在 中查詢整合狀態， AWS Glue 並確保您的 Oracle 變更正在複寫至 Amazon Redshift 來驗證整合是否正常運作。

驗證您的零 ETL 整合是否正常運作

1. 檢查整合狀態。

   ```
   aws glue describe-integrations \
     --integration-identifier integration-id
   ```

   狀態應為 ACTIVE或 REPLICATING。
2. 在 Oracle 資料庫中進行變更並檢查資料複寫是否出現在 Amazon Redshift 中，以驗證資料複寫。
3. 在 Amazon CloudWatch 中監控複寫指標 （如果可用）。

中的零 ETL 整合資料篩選 Oracle Database@AWS

Oracle Database@AWS 零 ETL 整合支援資料篩選。您可以使用它來控制來源 Oracle Exadata 資料庫複寫到目標資料倉儲的資料。您可以套用一或多個篩選條件來選擇性地包含或排除特定資料表，而不是

複寫整個資料庫。這可協助您透過確保僅傳輸相關資料來最佳化儲存和查詢效能。篩選僅限於資料庫和資料表層級。不支援資料欄層級和資料列層級篩選。

Oracle Database 和 Amazon Redshift 以不同的方式處理物件名稱大小寫，這會影響資料篩選條件組態和目標查詢。注意下列事項：

- 除非在 CREATE 陳述式中明確加上引號，否則 Oracle Database 會以大寫形式儲存資料庫、結構描述和物件名稱。例如，如果您建立 mytable (無引號)，Oracle 資料字典會將資料表名稱儲存為 MYTABLE。如果您在建立陳述式中引用物件名稱，Oracle 資料字典會保留案例。
- 零 ETL 資料篩選條件區分大小寫，且必須符合物件名稱在 Oracle 資料字典中顯示的確切大小寫。例如，如果 Oracle 字典存放結構描述和資料表名稱 REINVENT.MYTABLE，則使用 建立篩選條件include: ORCL.REINVENT.MYTABLE。
- 除非明確加上引號，否則 Amazon Redshift 查詢預設為小寫物件名稱。例如，查詢 MYTABLE(無引號) 會搜尋 mytable。

當您建立 Amazon Redshift 篩選條件並查詢資料時，請注意大小寫差異。的篩選考量 Oracle Database@AWS 與 Amazon RDS for Oracle 相同。如需案例如何影響 Oracle 資料庫中資料篩選條件的範例，請參閱《Amazon Relational Database Service 使用者指南》中的 RDS for Oracle 範例。

監控零 ETL 整合

定期監控您的零 ETL 整合可確保最佳效能，並有助於及早識別問題。

整合狀態監控

使用 Glue APIs 監控零 ETL AWS 整合的狀態。

```
# Check status of a specific integration
aws glue describe-integrations \
  --integration-identifier integration-id

# List all integrations in your account
aws glue describe-integrations
```

整合狀態包括：

- 建立 – 正在設定整合
- 作用中 – 整合正在執行並複寫資料

- 修改 – 正在更新整合組態
- needs_attention – 整合需要手動介入
- 失敗 – 整合發生錯誤
- 刪除 – 正在移除整合

效能監控

監控零 ETL 整合效能的下列層面：

- 複寫延遲 – 在 Oracle 中發生變更與在 Amazon Redshift 中出現變更之間的時間差異
- 資料輸送量 – 每單位時間複寫的資料量
- 錯誤率 – 複寫錯誤或失敗的頻率
- 資源使用率 – 來源和目標系統的 CPU、記憶體和網路使用量

使用 Amazon CloudWatch 監控這些指標，並設定關鍵閾值的警示。

在 中管理零 ETL 整合 Oracle Database@AWS

建立零 ETL 整合之後，您可以執行各種管理操作，包括修改和刪除整合。本節涵蓋零 ETL 整合的持續管理。

修改零 ETL 整合

您只能修改支援的資料倉儲中零 ETL 整合的名稱、描述和資料篩選選項。您無法修改用來加密整合的 AWS Key Management Service 金鑰，或是來源或目標資料庫。

修改整合的先決條件

修改零 ETL 整合之前，請確定您有下列項目：

- 必要許可 – 除了標準`odb:UpdateOutboundIntegration`許可之外，您的 IAM 使用者或角色還必須具有 AWS Glue 許可。
- 處於作用中狀態的整合 – 整合必須處於 `ACTIVE` 狀態，而非 `CREATING`、`DELETING`、`MODIFYING`或 `FAILED`。
- 有效的資料篩選條件語法 – 新的資料篩選條件必須遵循支援的包含/排除模式語法。

修改資料篩選條件

您可以修改資料篩選條件來變更要複寫的資料表或結構描述。如此一來，您可以在複寫中新增或移除資料庫物件，而無需重新建立整個整合。

若要修改整合的資料篩選條件，請使用 `modify-integration`命令。

```
aws glue modify-integration \
  --integration-identifier integration-id \
  --data-filter "include: pdb1.new_schema.*"
```

您也可以同時修改整合名稱和描述。在下列範例中，您可以修改 中兩個結構描述的整合名稱、描述和篩選條件pdb1。

```
aws glue modify-integration \
  --integration-identifier integration-id \
  --data-filter "include: pdb1.schema1.*, pdb1.schema2.*" \
  --integration-name "Updated Integration Name" \
  --description "Updated integration description"
```

> **Important**
>
> 當您修改資料篩選條件時，整合會進入 `modifying` 狀態，並執行資料的重新同步。整合會停止複寫、套用新的篩選條件設定，並使用重新載入目標操作繼續複寫。監控整合狀態，以確保修改成功完成。

對零 ETL 整合進行資料篩選條件修改的考量

修改資料篩選條件時，請考慮下列事項：

- 單一 PDB 限制 – 每個整合只能指定一個插入式資料庫 (PDB)。`include: pdb1.*.*, include: pdb2.*.*` 不支援 等資料篩選條件
- 複寫中斷 – 資料複寫會在修改程序期間停止，並在套用新的篩選條件後繼續。
- 資料重新載入 – 整合會執行符合新篩選條件的完整資料重新載入。
- 效能影響 – 大型資料篩選條件變更可能需要很長的時間才能完成，並且可能會影響重新載入期間的來源資料庫效能。

修改零 ETL 整合設定的限制

建立零 ETL 整合後，您無法修改下列設定：

- 秘密 ARN – 包含資料庫登入資料的 AWS Secrets Manager 秘密
- KMS 金鑰 – 用於加密的客戶受管金鑰
- 來源 ARN – Oracle Database@AWS VM 叢集
- 目標 ARN – Amazon Redshift 叢集或命名空間

若要變更這些設定，請刪除現有的零 ETL 整合並建立新的整合。

刪除零 ETL 整合

當您不再需要零 ETL 整合時，您可以將其刪除以停止複寫並清除相關聯的資源。

使用 Glue AWS 刪除

使用 Glue API 刪除零 ETL AWS 整合。

```
aws glue delete-integration \
  --integration-identifier integration-id
```

您可以在下列狀態下刪除整合：

- 作用中
- needs_attention
- 失敗
- 同步

刪除的影響

當您刪除零 ETL 整合時，請考慮下列效果：

複寫會停止。

Oracle Database@AWS does 不會從 Amazon Redshift 複寫新變更。

保留現有資料。

已複寫至 Amazon Redshift 的資料仍然可用。

目標資料庫仍會保留。

從整合建立的 Amazon Redshift 資料庫不會自動刪除。

> **Important**
>
> 刪除是不可復原的。如果您需要在刪除後繼續複寫，請建立新的整合，以執行完整的初始載入。

零 ETL 管理的最佳實務

遵循這些最佳實務，以確保零 ETL 整合的最佳效能、安全性和成本效益。

操作最佳實務

這些操作實務有助於維持可靠且有效率的零 ETL 整合。

定期監控

設定 CloudWatch 警示來監控整合運作狀態和效能指標。

登入資料輪換

定期輪換資料庫密碼，並在 AWS Secrets Manager 中更新它們。

備份驗證

定期驗證您的 Oracle 資料庫備份是否包含災難復原所需的元件。

效能測試

測試零 ETL 整合對 Oracle 資料庫效能的影響，特別是在尖峰使用期間。

結構描述變更規劃

在將結構描述變更套用到生產環境之前，在開發環境中規劃和測試結構描述變更。

安全最佳實務

實作這些安全措施來保護您的零 ETL 整合和資料。

最低權限存取

僅授予複寫使用者和 IAM AWS 角色所需的最低許可。

網路安全

使用安全群組和 NACLs來限制網路只能存取必要的連接埠和來源。

靜態加密

確保 Oracle 資料庫和 Amazon Redshift 叢集都使用靜態加密。

稽核記錄

在 Oracle 和 Amazon Redshift 上啟用稽核記錄，以追蹤資料存取和變更。

秘密管理

盡可能使用 AWS Secrets Manager 自動輪換功能。

成本最佳化

套用這些策略來最佳化成本，同時維持有效的零 ETL 整合效能。

資料篩選

使用精確的資料篩選條件僅複寫您需要的資料，從而降低儲存和運算成本。

Amazon Redshift 最佳化

使用適當的 Amazon Redshift 節點類型並實作資料壓縮來最佳化成本。

監控用量

透過 AWS Cost Explorer 定期檢閱您的零 ETL 整合用量和成本。

清除未使用的整合

刪除不再需要的整合，以避免持續收費。

故障診斷零 ETL 整合

本節提供解決零 ETL 整合常見問題的指引。

零 ETL 整合設定失敗

身分驗證失敗

- 驗證複寫使用者是否存在，並在 AWS Secrets Manager 中具有正確的密碼。
- 確定所有必要的許可都已授予複寫使用者。
- 檢查秘密 ARN 是否正確且可由 Oracle Database@ 存取AWS。
- 確認 CMK 資源政策允許 Oracle Database@AWS service 主體存取。

網路連線問題

- 請確定您的 ODB 網路已啟用零 ETL 整合。
- 確認連接埠 2484 上已正確設定 SSL （僅限 Exadata)。
- 檢查 Oracle 資料庫接聽程式是否正在執行並接受連線。
- 確保網路安全群組和 NACLs連接埠 2484 上的流量。
- 確認秘密中的服務名稱符合實際的 Oracle 服務名稱。

許可錯誤

- 檢查您的 IAM 使用者或角色是否具有整合操作的必要許可 AWS Glue 。
- 確認 Amazon Redshift 資源政策允許來自 VM 叢集的傳入整合。
- 確保 Oracle Database@s AWS 已獲得存取您的秘密和 AWS Key Management Service 金鑰的權限。

複寫問題

初始載入失敗

- 確認 Oracle 資料庫有足夠的資源來支援完整載入操作。
- 確定已在來源資料庫上啟用補充記錄。
- 檢查是否有任何資料表層級鎖定或限制，可能阻止資料擷取。

變更資料擷取問題

- 確認 Oracle 資料庫有足夠的重做日誌空間和保留。
- 檢查複寫使用者是否有權存取封存的重做日誌。
- 對於啟用 ASM 的系統，請確保 ASM 使用者已正確設定。
- 監控 Oracle 資料庫效能，以確保 CDC 不會造成資源爭用。

高複寫延遲

- 在 CloudWatch 中監控複寫延遲指標。
- 檢查來源資料庫中是否有高交易量或大型交易。
- 確認 Amazon Redshift 叢集有足夠的容量來處理傳入的資料。

資料一致性問題

資料遺失或不完整

- 確認資料篩選條件包含所有必要的結構描述和資料表。
- 檢查可能導致複寫失敗的不支援資料類型。
- 確定複寫使用者具有所有必要資料表的 SELECT 許可。

資料類型轉換錯誤

- 檢閱 Oracle 和 Redshift 之間支援的資料類型映射。
- 檢查是否需要自訂處理的 Oracle 特定資料類型。
- 請考慮修改 Oracle 結構描述，以使用更相容的資料類型。

監控與除錯

使用下列方法來監控和偵錯零 ETL 整合問題：

- 整合狀態監控 – 使用 定期檢查整合狀態`aws glue describe-integrations`。
- CloudWatch 指標 – 監控可用的 CloudWatch 指標是否有複寫效能和錯誤。
- Oracle 資料庫監控 – 監控 Oracle 資料庫效能和資源使用率。
- Redshift 監控 – 監控 Amazon Redshift 叢集效能和儲存使用率。

對於無法使用此故障診斷指南解決的複雜問題，請聯絡 AWS 支援 並提供下列資訊：

- 整合 ARN 和目前狀態。
- 整合的錯誤訊息說明 操作。
- Oracle 資料庫和 Amazon Redshift 叢集組態。
- 問題開始發生的時間表。

中的安全性 Oracle Database@AWS

的雲端安全 AWS 是最高優先順序。身為 AWS 客戶，您可以受益於資料中心和網路架構，這些架構是為了滿足最安全敏感組織的需求而建置。

安全性是 OCI AWS與您之間的共同責任。共同責任模型將此描述為雲端安全性和雲端安全性：

- 雲端的安全性 – AWS 負責保護在 AWS 服務 中執行的基礎設施 AWS 雲端。 AWS 也為您提供可安全使用的服務。在 AWS 合規計劃中，第三方稽核員會定期測試並驗證我們的安全功效。
- 雲端的安全性 – 您的責任取決於您使用 AWS 的服務。您也必須負責其他因素，包括資料的敏感度、組織的需求，以及適用的法律和法規。

本文件可協助您了解如何在使用 時套用共同責任模型 Oracle Database@AWS。您也會了解如何使用其他 AWS 服務來協助您監控和保護 Oracle Database@AWS 資源。

您可以管理對 Oracle Database@AWS 資源的存取。您用來管理存取的方法取決於您需要執行的任務類型 Oracle Database@AWS：

- 使用 AWS Identity and Access Management (IAM) 政策來指派許可，以決定允許誰管理 Oracle Database@AWS 資源。例如，您可以使用 IAM 來判斷誰可以建立、描述、修改和刪除 Exadata 基礎設施、VM 叢集或標籤資源。
- 使用 Oracle 資料庫引擎的安全功能來控制誰可以登入資料庫執行個體上的資料庫。這項功能的運作方式就好像資料庫位在您的本機網路上。
- 搭配 Exadata 資料庫使用 Secure Socket Layers (SSL) 或 Transport Layer Security (TLS) 連線。如需詳細資訊，請參閱準備 TLS 無錢包連線。
- Oracle Database@AWS 無法從網際網路立即存取，而且 AWS 只能在 的私有子網路上部署。
- Oracle Database@AWS 使用許多預設傳輸控制通訊協定 (TCP) 連接埠進行各種操作。如需連接埠的完整清單，請參閱預設連接埠指派。
- 若要使用依預設啟用的透明資料加密 (TDE) 來存放和管理金鑰， Oracle Database@AWS 會使用 OCI 保存庫或 Oracle 金鑰保存庫。 Oracle Database@AWS 不支援 AWS Key Management Service。
- 根據預設，資料庫是使用 Oracle 管理的加密金鑰來設定。資料庫也支援客戶受管金鑰。
- 若要增強資料保護，請使用 Oracle Data Safe 搭配 Oracle Database@AWS。

下列主題說明如何設定 Oracle Database@AWS 以符合您的安全與合規目標。

主題

中的資料保護 Oracle Database@AWS

基於資料保護目的，我們建議您保護 AWS 帳戶 登入資料，並使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 設定個別使用者。如此一來，每個使用者都只會獲得授與完成其任務所必須的許可。我們也建議您採用下列方式保護資料：

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用 設定 API 和使用者活動記錄 AWS CloudTrail。如需有關使用 CloudTrail 追蹤擷取 AWS 活動的資訊，請參閱AWS CloudTrail 《 使用者指南》中的使用 CloudTrail 追蹤。
- 使用 AWS 加密解決方案，以及其中的所有預設安全控制 AWS 服務。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果您在 AWS 透過命令列界面或 API 存取 時需要 FIPS 140-3 驗證的密碼編譯模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的更多相關資訊，請參閱聯邦資訊處理標準 (FIPS) 140-3。

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的文字欄位中，例如名稱欄位。這包括當您使用主控台 AWS CLI、API AWS 或 AWS SDKs來使用 Oracle Database@ 或其他 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

Exadata 資料庫使用 Oracle 透明資料加密 (TDE) 來加密您的資料。您的資料也會在暫存資料表空間、復原區段、重做日誌和 JOIN 和 SORT 等內部資料庫操作期間受到保護。如需詳細資訊，請參閱資料安全。

傳輸中加密

Exadata 資料庫使用原生 Oracle Net Services 加密和完整性功能來保護資料庫的連線。如需詳細資訊，請參閱傳輸中資料的安全性。

金鑰管理

透明資料加密包括可安全存放主加密金鑰的金鑰存放區，以及可安全有效地管理金鑰存放區和執行金鑰維護操作的管理架構。如需詳細資訊，請參閱管理保存庫加密金鑰。

的身分和存取管理 Oracle Database@AWS

AWS Identity and Access Management (IAM) 是一種 AWS 服務，可協助管理員安全地控制對 AWS 資源的存取。IAM 管理員可控制誰可以進行身分驗證 （登入） 和授權 （具有許可），以使用 Oracle Database@AWS resources。IAM 是一項服務 AWS ，您可以免費使用。

主題

- 目標對象
- 使用身分驗證
- 使用政策管理存取權
- Oracle Database@AWS 如何使用 IAM
- 適用於 Oracle Database@AWS的身分型政策
- AWS 的 受管政策 Oracle Database@AWS
- Oracle Database@AWS OCI 中的身分驗證和授權
- 對 Oracle Database@AWS 身分和存取進行故障診斷

目標對象

使用方式 AWS Identity and Access Management (IAM) 會根據您的角色而有所不同：

- 服務使用者 — 若無法存取某些功能，請向管理員申請所需許可 (請參閱 對 Oracle Database@AWS 身分和存取進行故障診斷)
- 服務管理員 — 負責設定使用者存取權並提交相關許可請求 (請參閱 Oracle Database@AWS 如何使用 IAM)
- IAM 管理員 — 撰寫政策以管理存取控制 (請參閱 適用於 Oracle Database@AWS的身分型政策)

使用身分驗證

身分驗證是您 AWS 使用身分憑證登入 的方式。您必須驗證為 AWS 帳戶根使用者、IAM 使用者或擔任 IAM 角色。

您可以使用身分來源的登入資料，例如 AWS IAM Identity Center (IAM Identity Center)、單一登入身分驗證或 Google/Facebook 登入資料，以聯合身分的形式登入。如需有關登入的詳細資訊，請參閱《AWS 登入 使用者指南》中的如何登入您的 AWS 帳戶。

對於程式設計存取， AWS 提供 SDK 和 CLI 以密碼編譯方式簽署請求。如需詳細資訊，請參閱《IAM 使用者指南》中的 API 請求的AWS 第 4 版簽署程序。

AWS 帳戶 根使用者

當您建立 時 AWS 帳戶，您會從一個名為 AWS 帳戶 theroot 使用者的登入身分開始，該身分可完整存取所有 AWS 服務 和資源。強烈建議不要使用根使用者來執行日常任務。有關需要根使用者憑證的任務，請參閱《IAM 使用者指南》中的需要根使用者憑證的任務。

聯合身分

最佳實務是要求人類使用者使用聯合身分提供者，以 AWS 服務 使用臨時憑證存取 。

聯合身分是您企業目錄、Web 身分提供者的使用者，或是 AWS 服務 使用身分來源的憑證 Directory Service 存取的使用者。聯合身分會擔任角色，而該角色會提供臨時憑證。

若需集中化管理存取權限，建議使用 AWS IAM Identity Center。如需詳細資訊，請參閱 AWS IAM Identity Center 使用者指南中的什麼是 IAM Identity Center？。

IAM 使用者和群組

IAM 使用者https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users.html是一種身分具備單人或應用程式的特定許可權。建議以臨時憑證取代具備長期憑證的 IAM 使用者。如需詳細資訊，請參閱《IAM 使用者指南》中的要求人類使用者使用聯合身分提供者來 AWS 使用臨時憑證存取 。

IAM 群組會指定 IAM 使用者集合，使管理大量使用者的許可權更加輕鬆。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 使用者的使用案例。

IAM 角色

IAM 角色https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html的身分具有特定許可權，其可以提供臨時憑證。您可以透過從使用者切換到 IAM 角色 （主控台） 或呼叫 AWS CLI 或 AWS API 操作來擔任角色。如需詳細資訊，請參閱《IAM 使用者指南》中的擔任角色的方法。

IAM 角色適用於聯合身分使用者存取、臨時 IAM 使用者許可、跨帳戶存取權與跨服務存取，以及在 Amazon EC2 執行的應用程式。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 中的快帳戶資源存取。

使用政策管理存取權

您可以透過建立政策並將其連接到身分或資源 AWS 來控制 AWS 中的存取。政策定義與身分或資源相關聯的許可。當委託人提出請求時 AWS ， 會評估這些政策。大多數政策會以 JSON 文件 AWS 形式存放在 中。如需進一步了解 JSON 政策文件，請參閱《IAM 使用者指南》中的 JSON 政策概觀。

管理員會使用政策，透過定義哪些主體可在哪些條件下對哪些資源執行動作，以指定可存取的範圍。

預設情況下，使用者和角色沒有許可。IAM 管理員會建立 IAM 政策並將其新增至角色，供使用者後續擔任。IAM 政策定義動作的許可，無論採用何種方式執行。

身分型政策

身分型政策是附加至身分 (使用者、使用者群組或角色) 的 JSON 許可政策文件。這類政策控制身分可對哪些資源執行哪些動作，以及適用的條件。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的透過客戶管理政策定義自訂 IAM 許可。

身分型政策可分為內嵌政策 (直接內嵌於單一身分) 與受管政策 (可附加至多個身分的獨立政策)。如需了解如何在受管政策及內嵌政策之間做選擇，請參閱《IAM 使用者指南》中的在受管政策與內嵌政策之間選擇。

資源型政策

資源型政策是附加到資源的 JSON 政策文件。範例包括 IAM 角色信任政策與 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。您必須在資源型政策中指定主體。

資源型政策是位於該服務中的內嵌政策。您無法在資源型政策中使用來自 IAM 的 AWS 受管政策。

其他政策類型

AWS 支援其他政策類型，可設定更多常見政策類型授予的最大許可：

- 許可界限 — 設定身分型政策可授與 IAM 實體的最大許可。如需詳細資訊，請參閱《 IAM 使用者指南》中的 IAM 實體許可界限。

- 服務控制政策 (SCP) — 為 AWS Organizations中的組織或組織單位指定最大許可。如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的服務控制政策。
- 資源控制政策 (RCP) — 設定您帳戶中資源可用許可的上限。如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的資源控制政策 (RCP)。
- 工作階段政策 — 在以程式設計方式為角色或聯合身分使用者建立臨時工作階段時，以參數形式傳遞的進階政策。如需詳細資訊，請參《IAM 使用者指南》中的工作階段政策。

多種政策類型

當多種類型的政策適用於請求時，產生的許可會更複雜而無法理解。若要了解如何 AWS 在涉及多個政策類型時決定是否允許請求，請參閱《IAM 使用者指南》中的政策評估邏輯。

Oracle Database@AWS 如何使用 IAM

在您使用 IAM 管理 Oracle Database@ 的存取權之前AWS，請先了解哪些 IAM 功能可與 Oracle Database@ 搭配使用AWS。

IAM 功能	Oracle Database@AWS 支援
身分型政策	是
資源型政策	否
政策動作	是
政策資源	是
政策條件索引鍵	是
ACL	否
ABAC(政策中的標籤)	部分
臨時憑證	是
主體許可	是
服務角色	否

IAM 功能	Oracle Database@AWS 支援
服務連結角色	是

若要全面了解 Oracle Database@AWS 和其他 AWS 服務如何與大多數 IAM 功能搭配使用，請參閱《AWS IAM 使用者指南》中的與 IAM 搭配使用的 服務。

的身分型政策 Oracle Database@AWS

支援身分型政策：是

身分型政策是可以附加到身分 (例如 IAM 使用者、使用者群組或角色) 的 JSON 許可政策文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的透過客戶管理政策定義自訂 IAM 許可。

使用 IAM 身分型政策，您可以指定允許或拒絕的動作和資源，以及在何種條件下允許或拒絕動作。如要了解您在 JSON 政策中使用的所有元素，請參閱《IAM 使用者指南》中的 IAM JSON 政策元素參考。

的身分型政策範例 Oracle Database@AWS

若要檢視 Oracle Database@AWS identity 型政策的範例，請參閱 適用於 Oracle Database@AWS的身分型政策。

內的資源型政策 Oracle Database@AWS

支援資源型政策：否

資源型政策是附加到資源的 JSON 政策文件。資源型政策的最常見範例是 IAM 角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定主體。委託人可以包含帳戶、使用者、角色、聯合身分使用者或 AWS 服務。

如需啟用跨帳戶存取權，您可以在其他帳戶內指定所有帳戶或 IAM 實體作為資源型政策的主體。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 中的快帳戶資源存取。

的政策動作 Oracle Database@AWS

支援政策動作：是

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

JSON 政策的 `Action` 元素描述您可以用來允許或拒絕政策中存取的動作。政策會使用動作來授予執行相關聯動作的許可。

若要查看 Oracle Database@AWS 動作清單，請參閱《服務授權參考》中的 Oracle Database@ 定義的動作AWS。

中的政策動作在動作之前 Oracle Database@AWS 使用下列字首：

```
odb
```

若要在單一陳述式中指定多個動作，請用逗號分隔。

```
"Action": [
      "odb:action1",
      "odb:action2"
         ]
```

若要檢視 Oracle Database@AWS identity 型政策的範例，請參閱 適用於 Oracle Database@AWS的身分型政策。

的政策資源 Oracle Database@AWS

支援政策資源：是

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

`Resource` JSON 政策元素可指定要套用動作的物件。最佳實務是使用其 Amazon Resource Name (ARN) 來指定資源。若動作不支援資源層級許可，使用萬用字元 (*) 表示該陳述式適用於所有資源。

```
"Resource": "*"
```

若要查看 Oracle Database@AWS 資源類型及其 ARNs，請參閱《服務授權參考》中的 Oracle Database@ 定義的資源AWS。若要了解您可以使用哪些動作指定每個資源的 ARN，請參閱 Oracle Database@ 定義的動作AWS。

若要檢視 Oracle Database@AWS identity 型政策的範例，請參閱 適用於 Oracle Database@AWS的身分型政策。

的政策條件索引鍵 Oracle Database@AWS

支援服務特定政策條件金鑰：是

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

`Condition` 元素會根據定義的條件，指定陳述式的執行時機。您可以建立使用條件運算子的條件運算式 (例如等於或小於)，來比對政策中的條件和請求中的值。若要查看所有 AWS 全域條件索引鍵，請參閱《IAM 使用者指南》中的AWS 全域條件內容索引鍵。

若要查看 Oracle Database@AWS 條件金鑰清單，請參閱《服務授權參考》中的 Oracle Database@ 的條件金鑰AWS。若要了解您可以使用條件金鑰的動作和資源，請參閱 Oracle Database@ 定義的動作AWS。

若要檢視 Oracle Database@AWS identity 型政策的範例，請參閱 適用於 Oracle Database@AWS的身分型政策。

中的 ACLs Oracle Database@AWS

支援 ACL：否

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

ABAC 搭配 Oracle Database@AWS

支援 ABAC (政策中的標籤)：部分

屬性型存取控制 (ABAC) 是一種授權策略，根據稱為標籤的屬性定義許可權。您可以將標籤連接至 IAM 實體 AWS 和資源，然後設計 ABAC 政策，以便在委託人的標籤符合資源上的標籤時允許操作。

如需根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件索引鍵，在政策的條件元素中，提供標籤資訊。

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

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

搭配 使用臨時登入資料 Oracle Database@AWS

支援臨時憑證：是

臨時登入資料提供 AWS 資源的短期存取權，當您使用聯合或切換角色時，會自動建立。 AWS 建議您動態產生臨時登入資料，而不是使用長期存取金鑰。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 中的臨時安全憑證與可與 IAM 搭配運作的AWS 服務。

的跨服務主體許可 Oracle Database@AWS

支援轉寄存取工作階段 (FAS)：是

轉送存取工作階段 (FAS) 使用呼叫 AWS 服務的委託人許可，結合 請求 AWS 服務向下游服務提出請求。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。

Oracle Database@AWS的服務角色

支援服務角色：否

服務角色是服務擔任的 IAM 角色，可代您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需詳細資訊，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。

> **Warning**
>
> 變更服務角色的許可可能會中斷 Oracle Database@AWS 功能。只有在 Oracle Database@AWS 提供指引時，才能編輯服務角色。

的服務連結角色 Oracle Database@AWS

支援服務連結角色：是

服務連結角色是連結至 服務的一種 AWS 服務角色。服務可以擔任代表您執行動作的角色。服務連結角色會出現在您的 中 AWS 帳戶 ，並由服務擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

如需建立或管理 Oracle Database@AWS 服務連結角色的詳細資訊，請參閱 使用 的服務連結角色 Oracle Database@AWS。

適用於 Oracle Database@AWS的身分型政策

根據預設，使用者和角色沒有建立或修改 Oracle Database@AWS 資源的許可。若要授予使用者對其所需資源執行動作的許可，IAM 管理員可以建立 IAM 政策。

如需了解如何使用這些範例 JSON 政策文件建立 IAM 身分型政策，請參閱《IAM 使用者指南》中的建立 IAM 政策 (主控台)。

如需 Oracle Database@ 定義的動作和資源類型的詳細資訊AWS，包括每種資源類型的 ARNs 格式，請參閱服務授權參考中的 Oracle Database@ 的動作、資源和條件金鑰AWS。

主題

政策最佳實務

身分型政策會判斷您帳戶中的某個人員是否可以建立、存取或刪除 Oracle Database@AWS resources。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管政策並邁向最低權限許可 – 若要開始將許可授予您的使用者和工作負載，請使用將許可授予許多常見使用案例的 AWS 受管政策。它們可在您的 中使用 AWS 帳戶。我們建議您定義特定於使用案例 AWS 的客戶受管政策，以進一步減少許可。如需更多資訊，請參閱《IAM 使用者指南》中的 AWS 受管政策或任務職能的AWS 受管政策。
- 套用最低權限許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的許可。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的更多相關資訊，請參閱《IAM 使用者指南》中的 IAM 中的政策和許可。
- 使用 IAM 政策中的條件進一步限制存取權 – 您可以將條件新增至政策，以限制動作和資源的存取。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。如果透過特定服務使用服務動作，您也可以使用條件來授予存取 AWS 服務動作的權限，例如 CloudFormation。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM JSON 政策元素：條件。
- 使用 IAM Access Analyzer 驗證 IAM 政策，確保許可安全且可正常運作 – IAM Access Analyzer 驗證新政策和現有政策，確保這些政策遵從 IAM 政策語言 (JSON) 和 IAM 最佳實務。IAM Access

Analyzer 提供 100 多項政策檢查及切實可行的建議，可協助您撰寫安全且實用的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的使用 IAM Access Analyzer 驗證政策。

- 需要多重要素驗證 (MFA) – 如果您的案例需要 IAM 使用者或 中的根使用者 AWS 帳戶，請開啟 MFA 以提高安全性。如需在呼叫 API 操作時請求 MFA，請將 MFA 條件新增至您的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的透過 MFA 的安全 API 存取。

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

使用 Oracle Database@AWS 主控台

若要存取 Oracle Database@AWS console，您必須擁有一組最低許可。這些許可必須允許您列出和檢視 中 Oracle Database@AWS resources 的詳細資訊 AWS 帳戶。如果您建立比最基本必要許可更嚴格的身分型政策，則對於具有該政策的實體 (使用者或角色) 而言，主控台就無法如預期運作。

對於僅呼叫 AWS CLI 或 AWS API 的使用者，您不需要允許最低主控台許可。反之，只需允許存取符合他們嘗試執行之 API 操作的動作就可以了。

允許使用者佈建 Oracle Database@AWS 資源

此政策允許使用者完整存取佈建 Oracle Database@AWS 資源。若要從 VPC 設定 DNS 解析，請建立傳出 Route 53 解析程式，並新增規則，以使用 OCI 網域名稱將 DNS 流量轉送至 OCI DNS 接聽程式 IP。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowODBAndEC2Actions",
            "Effect": "Allow",
            "Action": [
                "odb:GetOciOnboardingStatus",
                "odb:CreateOdbNetwork",
                "odb:DeleteOdbNetwork",
                "odb:GetOdbNetwork",
                "odb:ListOdbNetworks",
                "odb:UpdateOdbNetwork",
                "odb:CreateOdbPeeringConnection",
                "odb:DeleteOdbPeeringConnection",
```

```
                "odb:GetOdbPeeringConnection",
                "odb:ListOdbPeeringConnections",
                "odb:PutResourcePolicy",
                "odb:GetResourcePolicy",
                "odb:DeleteResourcePolicy",
                "ec2:DescribeVpcs",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeVpcEndpointAssociations",
                "ec2:CreateVpcEndpoint",
                "ec2:DeleteVpcEndpoints",
                "ec2:DescribeVpcEndpoints"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowSLRActions",
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": [
                        "odb.amazonaws.com",
                        "vpc-lattice.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Sid": "AllowTaggingActions",
            "Effect": "Allow",
            "Action": [
                "odb:TagResource",
                "odb:UntagResource",
                "odb:ListTagsForResource"
            ],
            "Resource": "arn:aws:odb:*:*:odb-network/*"
        },
        {
            "Sid": "AllowOdbVpcLatticeActions",
            "Effect": "Allow",
            "Action": [
```

```
                "vpc-lattice:CreateServiceNetwork",
                "vpc-lattice:DeleteServiceNetwork",
                "vpc-lattice:GetServiceNetwork",
                "vpc-lattice:CreateServiceNetworkResourceAssociation",
                "vpc-lattice:DeleteServiceNetworkResourceAssociation",
                "vpc-lattice:GetServiceNetworkResourceAssociation",
                "vpc-lattice:CreateResourceGateway",
                "vpc-lattice:DeleteResourceGateway",
                "vpc-lattice:GetResourceGateway",
                "vpc-lattice:CreateServiceNetworkVpcEndpointAssociation"
            ],
            "Resource": "*"
        }
    ]
}
```

允許使用者檢視他們自己的許可

此範例會示範如何建立政策，允許 IAM 使用者檢視附加到他們使用者身分的內嵌及受管政策。此政策包含在主控台或使用 或 AWS CLI AWS API 以程式設計方式完成此動作的許可。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
```

```
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS 的 受管政策 Oracle Database@AWS

若要將許可新增至許可集和角色，使用 AWS 受管政策比自行撰寫政策更容易。建立 IAM 客戶受管政策需要時間和專業知識，而受管政策可為您的團隊提供其所需的許可。若要快速開始使用，您可以使用我們的 AWS 受管政策。這些政策涵蓋常見的使用案例，並可在您的 AWS 帳戶中使用。如需 AWS 受管政策的詳細資訊，請參閱《IAM 使用者指南》中的 AWS 受管政策。

AWS 服務 維護和更新 AWS 受管政策。您無法變更 AWS 受管政策中的許可。服務偶爾會將其他許可新增至 AWS 受管政策，以支援新功能。此類型的更新會影響已連接政策的所有身分識別 (許可集和角色)。當新功能啟動或新操作可用時，服務最有可能更新 AWS 受管政策。服務不會從 AWS 受管政策中移除許可，因此政策更新不會破壞您現有的許可。

此外， AWS 支援跨多個 服務之任務函數的受管政策。例如， `ReadOnlyAccess` AWS 受管政策提供所有 AWS 服務 和 資源的唯讀存取權。當服務啟動新功能時， 會為新操作和資源 AWS 新增唯讀許可。如需任務職能政策的清單和說明，請參閱 IAM 使用者指南中有關任務職能的AWS 受管政策。

主題

- AWS 受管政策：AmazonODBServiceRolePolicy

AWS 受管政策：AmazonODBServiceRolePolicy

您無法將 `AmazonODBServiceRolePolicy` 政策附加至 IAM 實體。此政策會連接到服務連結角色，Oracle Database@AWS 允許 代表您執行動作。如需詳細資訊，請參閱使用 的服務連結角色 Oracle Database@AWS。

若要檢視政策的詳細資訊，包括最新版本的 JSON 政策文件，請參閱《 AWS 受管政策參考指南》中的 AmazonODBServiceRolePolicy。

Oracle Database@AWS OCI 中的身分驗證和授權

當您使用 AWS APIs為 建立資源時 Oracle Database@AWS，這些資源邏輯上位於連結的 Oracle Cloud Infrastructure (OCI) 租用中。若要部署這些資源， AWS 會代表您與 OCI APIs通訊。為了緩解混淆代理人問題，OCI 和 Oracle Database@AWS 使用 AWS STS 做為信任的實體，並轉送存取工作階段，以授權您在連結租用中使用 OCI APIs意圖。因此，會從 AWS CloudTrail 追蹤和事件歷史記錄中的 OCI IP 空間記錄 `sts:getCallerIdentity` API 的事件。當您使用 Oracle Database@AWS APIs時，請預期這些事件。

對 Oracle Database@AWS 身分和存取進行故障診斷

使用以下資訊來協助您診斷和修正使用 Oracle Database@AWS and IAM 時可能遇到的常見問題。

主題

- 我無權在 中執行動作 Oracle Database@AWS
- 我未獲得執行 iam:PassRole 的授權
- 我想要允許 以外的人員 AWS 帳戶 存取我的 Oracle Database@AWS 資源

我無權在 中執行動作 Oracle Database@AWS

如果您收到錯誤，告知您未獲授權執行動作，您的政策必須更新，允許您執行動作。

下列範例錯誤會在`mateojackson` IAM 使用者嘗試使用主控台檢視一個虛構 *`my-example-widget`* 資源的詳細資訊，但卻無虛構 `odb:`*`GetWidget`* 許可時發生。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 odb:GetWidget on resource: my-example-widget
```

在此情況下，必須更新 `mateojackson` 使用者的政策，允許使用 `odb:`*`GetWidget`* 動作存取 *`my-example-widget`* 資源。

如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的簽署憑證。

我未獲得執行 iam:PassRole 的授權

如果您收到錯誤，告知您無權執行 `iam:PassRole`動作，您的政策必須更新，以允許您將角色傳遞至 Oracle Database@AWS。

有些 AWS 服務 可讓您將現有角色傳遞給該服務，而不是建立新的服務角色或服務連結角色。如需執行此作業，您必須擁有將角色傳遞至該服務的許可。

當名為 的 IAM `marymajor` 使用者嘗試使用主控台在 Oracle Database@ 中執行動作時，會發生下列範例錯誤AWS。但是，動作請求服務具備服務角色授予的許可。Mary 沒有將角色傳遞給服務的許可。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

在這種情況下，Mary 的政策必須更新，允許她執行 `iam:PassRole` 動作。

如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的簽署憑證。

我想要允許 以外的人員 AWS 帳戶 存取我的 Oracle Database@AWS 資源

您可以建立一個角色，讓其他帳戶中的使用者或您組織外部的人員存取您的資源。您可以指定要允許哪些信任物件取得該角色。針對支援基於資源的政策或存取控制清單 (ACL) 的服務，您可以使用那些政策來授予人員存取您的資源的許可。

如需進一步了解，請參閱以下內容：

- 若要了解 Oracle Database@ 是否AWS 支援這些功能，請參閱 Oracle Database@AWS 如何使用 IAM。
- 若要了解如何 AWS 帳戶 在您擁有的 資源之間提供存取權，請參閱《IAM 使用者指南》中的在您擁有 AWS 帳戶 的另一個 中為 IAM 使用者提供存取權。
- 若要了解如何將資源的存取權提供給第三方 AWS 帳戶，請參閱《IAM 使用者指南》中的將存取權提供給第三方 AWS 帳戶 擁有。
- 如需了解如何透過聯合身分提供存取權，請參閱《IAM 使用者指南》中的將存取權提供給在外部進行身分驗證的使用者 (聯合身分)。
- 如需了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱《IAM 使用者指南》中的 IAM 中的跨帳戶資源存取。

Oracle Database@ 的合規驗證AWS

您使用 Oracle Database@ 時的合規責任AWS 取決於資料的敏感度、您公司的合規目標，以及適用的法律和法規。Oracle 網站提供雲端合規的 Oracle 文件

中的彈性 Oracle Database@AWS

AWS 全球基礎設施是以 AWS 區域 和 可用區域為基礎建置。 AWS 區域 提供多個實體隔離和隔離的可用區域，這些可用區域與低延遲、高輸送量和高備援聯網連接。透過可用區域，您可以設計與操作的應用程式和資料庫，在可用區域之間自動容錯移轉而不會發生中斷。可用區域的可用性、容錯能力和擴展能力，均較單一或多個資料中心的傳統基礎設施還高。

如需 AWS 區域 和可用區域的詳細資訊，請參閱 AWS 全球基礎設施。

除了 AWS 全球基礎設施之外，Oracle Database@AWS 還提供數種功能，以協助支援您的資料彈性和備份需求。

使用 的服務連結角色 Oracle Database@AWS

Oracle Database@AWS use AWS Identity and Access Management (IAM) 服務連結角色。服務連結角色是直接連結至 的唯一 IAM 角色類型 Oracle Database@AWS。服務連結角色由 預先定義，Oracle Database@AWS 並包含該服務 AWS 服務 代表您呼叫其他 所需的所有許可。

服務連結角色可讓您更 Oracle Database@AWS 輕鬆地使用 ，因為您不必手動新增必要的許可。 Oracle Database@AWS 會定義其服務連結角色的許可，除非另有定義，否則只能 Oracle Database@AWS 擔任其角色。定義的許可包括信任政策和許可政策，並且該許可政策不能附加到任何其他 IAM 實體。

您必須先刪除角色的相關資源，才能刪除角色。這可保護您的 Oracle Database@AWS 資源，因為您不會不小心移除存取資源的許可。

的服務連結角色許可 Oracle Database@AWS

Oracle Database@AWS 使用名為 AWSServiceRoleForODB 的服務連結角色， Oracle Database@AWS 以允許 AWS 服務 代表您的資源呼叫 。

AWSServiceRoleForODB 服務連結角色信任下列服務擔任該角色：

- `odb.amazonaws.com`
- `vpc-lattice.amazonaws.com`

此服務連結角色具有名為 AmazonODBServiceRolePolicy 的許可政策，該政策會授予此角色在帳戶中操作的許可。如需詳細資訊，請參閱AWS 受管政策：AmazonODBServiceRolePolicy。

> **Note**
>
> 您必須設定許可，IAM 實體 (如使用者、群組或角色) 才可建立、編輯或刪除服務連結角色。如果您遇到下列錯誤訊息：
> 無法建立資源。確認您具有建立服務連結角色的許可。否則請等待，然後再試一次。
> 請確定您已啟用下列許可：
>
> ```
> {
>     "Action": "iam:CreateServiceLinkedRole",
>     "Effect": "Allow",
>     "Resource": "arn:aws:iam::*:role/aws-service-role/odb.amazonaws.com/
> AWSServiceRoleForODB",
>     "Condition": {
>         "StringLike": {
>             "iam:AWSServiceName":"odb.amazonaws.com",
>             "iam:AWSServiceName":"vpc-lattice.amazonaws.com"
>         }
>     }
> }
> ```
>
> 如需詳細資訊，請參閱《IAM 使用者指南》中的服務連結角色許可。

為 建立服務連結角色 Oracle Database@AWS

您不需要手動建立服務連結角色，當您建立 Exadata 資料庫時， 會為您 Oracle Database@AWS 建立服務連結角色。

若您刪除此服務連結角色，之後需要再次建立，您可以在帳戶中使用相同程序重新建立角色。當您建立 Exadata 資料庫時， 會再次為您 Oracle Database@AWS 建立服務連結角色。

編輯 的服務連結角色 Oracle Database@AWS

Oracle Database@AWS 不允許您編輯 AWSServiceRoleForODB 服務連結角色。因為有各種實體可能會參考服務連結角色，所以您無法在建立角色之後變更角色名稱。不過，您可以使用 IAM 編輯角色的描述。如需詳細資訊，請參閱《IAM 使用者指南》中的編輯服務連結角色。

刪除 的服務連結角色 Oracle Database@AWS

若您不再使用需要服務連結角色的功能或服務，我們建議您刪除該角色。如此一來，您就沒有未主動監控或維護的未使用實體。不過，您必須先刪除所有資源，才能刪除服務連結角色。

清除 的服務連結角色 Oracle Database@AWS

您必須先確認服務連結角色沒有作用中的工作階段，並移除該角色使用的資源，之後才能使用 IAM 將其刪除。

檢查服務連結角色是否於 IAM 主控台有作用中的工作階段

1. 登入 AWS 管理主控台 並開啟位於 https：//https://console.aws.amazon.com/iam/ 的 IAM 主控台。
2. 在 IAM 主控台的導覽窗格中，選擇角色。然後選擇 AWSServiceRoleForODB 角色的名稱 （ 而非核取方塊 ）。
3. 在所選角色的 Summary (摘要) 頁面中，選擇 Access Advisor (存取 Advisor) 分頁。
4. 在 Access Advisor (存取 Advisor) 分頁中，檢閱服務連結角色的近期活動。

> **Note**
>
> 如果您不確定 Oracle Database@AWS 是否使用 AWSServiceRoleForODB 角色，您可以嘗試刪除該角色。如果服務使用 角色，則刪除會失敗，而且您可以檢視使用該角色 AWS 區域 的 。如果服務正在使用該角色，您必須先等到工作階段結束，才能刪除該角色。您無法撤銷服務連結角色的工作階段。

如果您想要移除 AWSServiceRoleForODB 角色，您必須先刪除所有 Oracle Database@AWS 資源。

Oracle Database@AWS 服務連結角色支援的 區域

Oracle Database@AWS 支援在所有提供服務 AWS 區域 的 中使用服務連結角色。如需詳細資訊，請參閱 AWS 區域 和端點。

Oracle Database@AWSAWS 受管政策的更新

檢視自此服務開始追蹤這些變更 Oracle Database@AWS 以來， AWS 受管政策更新的詳細資訊。如需此頁面變更的自動提醒，請訂閱 Oracle Database@AWS 文件歷史記錄頁面上的 RSS 摘要。

變更	描述	Date
的服務連結角色許可 Oracle Database@AWS – 更新現有政策	Oracle Database@AWS 已將新許可新增至`AWSServiceRoleForODB` 服務連結角色`AmazonODBServiceRolePolicy` 的 。這些許可允許 Oracle Database@AWS 執行下列動作： • 描述 Amazon VPC Transit Gateways 附件 • 描述 Amazon EC2 連接 • 啟用 Amazon EventBridge 來源 如需詳細資訊，請參閱的服務連結角色許可 Oracle Database@AWS。	2025 年 6 月 30 日
的服務連結角色許可 Oracle Database@AWS – 更新現有政策	Oracle Database@AWS 已將新許可新增至`AWSServiceRoleForODB` 服務連結角色`AmazonODBServiceRolePolicy` 的 。這些許可允許 Oracle Database@AWS 執行下列動作： • 描述 Amazon EventBridge 來源 • 描述和建立事件匯流排 如需詳細資訊，請參閱的服務連結角色許可 Oracle Database@AWS。	2025 年 6 月 26 日
AWS 受管政策：AmazonODBServiceRolePolicy – 新的服務連結角色政策	Oracle Database@AWS `AmazonODBServiceRolePolicy` 已為`AWSServiceRoleForODB` 服務連結角色新增 。如需詳細資訊，請參閱AWS 受管政策：AmazonODBServiceRolePolicy。	2024 年 12 月 2 日
Oracle Database@AWS 開始追蹤變更	Oracle Database@AWS 已開始追蹤其 AWS 受管政策的變更。	2024 年 12 月 2 日

監控 Oracle Database@AWS

監控是維護 Oracle Database@AWS 和其他 AWS 解決方案的可靠性、可用性和效能的重要部分。AWS 提供下列監控工具，讓您監看 Oracle Database@AWS、回報錯誤，並適時採取自動動作：

- Amazon CloudWatch AWS 會即時監控您的 AWS 資源和您在 上執行的應用程式。您可以收集和追蹤指標、建立自訂儀板表，以及設定警示，在特定指標達到您指定的閾值時通知您或採取動作。例如，您可以讓 CloudWatch 追蹤 CPU 使用量或其他 Amazon EC2 執行個體指標，並在需要時自動啟動新的執行個體。如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南。
- Amazon CloudWatch Logs 可讓您監控、存放和存取來自 Amazon EC2 執行個體、CloudTrail 及其他來源的日誌檔案。CloudWatch Logs 可監控日誌檔案中的資訊，並在達到特定閾值時通知您。您也可以將日誌資料存檔在高耐用性的儲存空間。如需詳細資訊，請參閱 Amazon CloudWatch Logs 使用者指南。
- Amazon EventBridge 可用來自動化您的 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的方式交付至 EventBridge。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 會擷取由 AWS 您的帳戶或代表您的帳戶發出的 API 呼叫和相關事件，並將日誌檔案交付至您指定的 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 地址，以及呼叫的時間。如需詳細資訊，請參閱「AWS CloudTrail 使用者指南」。

Oracle Database@AWS 使用 Amazon CloudWatch 進行監控

您可以使用 Oracle Database@AWS CloudWatch 監控 ，這會收集原始資料並將其處理為可讀且近乎即時的指標。這些統計資料會保留 15 個月，以便您存取歷史資訊，並更清楚 Web 應用程式或服務的執行效能。您也可以設定留意特定閾值的警示，當滿足這些閾值時傳送通知或採取動作。如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南。

的 Amazon CloudWatch 指標 Oracle Database@AWS

Oracle Database@AWS 服務會在 VM 叢集、容器資料庫和可插入資料庫的AWS/ODB命名空間中，向 Amazon CloudWatch 報告指標。

主題

- 雲端 VM 叢集的指標

雲端 VM 叢集的指標

Oracle Database@AWS 服務會在雲端 VM 叢集的AWS/ODB命名空間中報告下列指標。

指標	Description	單位
ASMDiskgroupUtilization	磁碟群組中使用的可用空間百分比。可用空間是可供成長的空間。DATA 磁碟群組會儲存我們的 Oracle 資料庫檔案。RECO 磁碟群組包含用於復原的資料庫檔案，例如封存和回寫日誌。	百分比
CpuUtilization	CPU 使用率百分比。	百分比
FilesystemUtilization	佈建檔案系統的使用率百分比。	百分比
LoadAverage	系統平均負載超過 5 分鐘。	Integer
MemoryUtilization	可用於啟動新應用程式的記憶體百分比，無需交換。可用的記憶體可透過下列命令取得：cat /proc/meminfo	百分比
NodeStatus	指出主機是否可連線。	Integer
OcpusAllocated	配置OCPUs 數目。	Integer
SwapUtilization	總交換空間的使用率百分比。	百分比

容器資料庫的指標

Oracle Database@AWS 服務會在容器資料庫的AWS/ODB命名空間中報告下列指標。

指標	Description	單位
BlockChanges	每秒變更的平均區塊數。	每秒變更數
CpuUtilization	CPU 使用率以百分比表示，並彙總所有取用者群組。針對允許資料庫使用的 CPUs 數量報告使用率百分比，這是 OCPUs 數量的兩倍。	百分比
CurrentLogons	在所選間隔內成功登入的次數。	計數
ExecuteCount	在所選間隔內執行 SQL 陳述式的使用者和遞迴呼叫數目。	計數
ParseCount	所選間隔內的硬剖析和軟剖析數目。	計數
StorageAllocated	在收集時間配置給資料庫的儲存空間總量。	GB
StorageAllocatedBy Tablespace	集合時間分配給資料表空間的儲存空間總量。如果是容器資料庫，此指標會提供根容器資料表空間。	GB
StorageUsed	資料庫在收集時間使用的儲存空間總量。	GB
StorageUsedByTable space	收集時資料表空間使用的儲存空間總量。如果是容器資料庫，此指標會提供根容器資料表空間。	GB
StorageUtilization	目前正在使用的佈建儲存容量百分比。代表所有資料表空間的總配置空間。	百分比

指標	Description	單位
StorageUtilization ByTablespace	這表示收集時資料表空間使用的儲存空間百分比。如果是容器資料庫，此指標會提供根容器資料表空間。	百分比
TransactionCount	在所選間隔期間，使用者遞交和使用者轉返的合併數量。	計數
UserCalls	在所選間隔內登入、剖析和執行呼叫的合併數量。	計數

可插入資料庫的指標

Oracle Database@AWS 服務會在可插入資料庫的AWS/ODB命名空間中報告下列指標。

指標	Description	單位
AllocatedStorageUtilizationByTablespace	資料表空間在所有配置中所使用的空間百分比。對於容器資料庫，此指標提供根容器資料表空間的資料。（統計資料：平均值，間隔：30 分鐘）	百分比
AvgGCCRBlockReceiveTime	平均全域快取 CR（一致性讀取）區塊接收時間。僅適用於 RAC/叢集資料庫。（統計資料：平均值，間隔：5 分鐘）	毫秒
AvgGCCurrentBlockReceiveTime	平均全域快取目前區塊接收時間。統計資料會報告平均值。僅適用於 Real Application Cluster (RAC) 資料庫。（統計資料：平均值，間隔：5 分鐘）	毫秒

指標	Description	單位
BlockChanges	每秒變更的平均區塊數。（統計資料：平均值、間隔：1 分鐘）	每秒變更數
BlockingSessions	目前的封鎖工作階段。不適用於容器資料庫。（統計資料：最大值，間隔：15 分鐘）	計數
CPUTimeSeconds	在時間間隔內，根據資料庫執行個體中前景工作階段的 CPU 時間累積平均速率。平均作用中工作階段的 CPU 時間元件。（統計資料：平均值、間隔：1 分鐘）	每秒秒數
CpuCount	所選間隔期間的 CPUs 數量。	計數
CpuUtilization	CPU 使用率以百分比表示，並彙總所有取用者群組。針對允許資料庫使用的 CPUs 數量報告使用率百分比，這是 OCPUs 數量的兩倍。（統計資料：平均值、間隔：1 分鐘）	百分比
CurrentLogons	在所選間隔內成功登入的次數。（統計資料：總和，間隔：1 分鐘）	計數
DBTimeSeconds	資料庫執行個體中前景工作階段在時間間隔內累積資料庫時間 (CPU + 等待） 的平均速率。也稱為平均作用中工作階段。（統計資料：平均值、間隔：1 分鐘）	每秒秒數

指標	Description	單位
DbmgmtJobExecutionsCount	單一受管資料庫或資料庫群組上的 SQL 任務執行數量及其狀態。狀態維度可以是下列值：「成功」、「失敗」、「InProgress."（統計資料：總和，間隔：1 分鐘）	計數
ExecuteCount	在所選間隔內執行 SQL 陳述式的使用者和遞迴呼叫數目。（統計資料：總和，間隔：1 分鐘）	計數
FRASpaceLimit	快閃記憶體復原區域空間限制。不適用於可插入資料庫。（統計資料：最大值，間隔：15 分鐘）	GB
FRAUtilization	快閃記憶體復原區域使用率。不適用於可插入資料庫。（統計資料：平均值，間隔：15 分鐘）	百分比
GCCRBlocksReceived	每秒收到的全域快取 CR（一致性讀取）區塊。僅適用於 RAC/叢集資料庫。（統計資料：平均值，間隔：5 分鐘）	每秒區塊數
GCCurrentBlocksReceived	代表每秒收到的全域快取目前區塊。統計資料會報告平均值。僅適用於 Real Application Cluster (RAC) 資料庫。（統計資料：平均值，間隔：5 分鐘）	每秒區塊數

指標	Description	單位
IOPS	每秒輸入輸出操作的平均數量。（統計資料：平均值、間隔：1 分鐘）	每秒操作數
IOThroughputMB	每秒平均輸送量，以 MB 為單位。（統計資料：平均值、間隔：1 分鐘）	每秒 MB
InterconnectTrafficMB	平均內部節點資料傳輸率。僅適用於 RAC/叢集資料庫。（統計資料：平均值，間隔：5 分鐘）	每秒 MB
InvalidObjects	無效的資料庫物件計數。不適用於容器資料庫。（統計資料：最大值，間隔：24 小時）	計數
LogicalBlocksRead	每秒從 SGA/記憶體（緩衝快取）讀取的平均區塊數。（統計資料：平均值、間隔：1 分鐘）	每秒讀取數
MaxTablespaceSize	可能的資料表空間大小上限。對於容器資料庫，此指標提供根容器資料表空間的資料。（統計資料：最大值，間隔：30 分鐘）	GB
MemoryUsage	記憶體集區總大小，以 MB 為單位。（統計資料：平均值，間隔：15 分鐘）	MB
MonitoringStatus	資源的監控狀態。如果指標集合失敗，則會在此指標中擷取錯誤資訊。（統計資料：平均值，間隔：5 分鐘）	不適用

指標	Description	單位
NonReclaimableFRA	不可回收的快速復原區域。不適用於可插入資料庫。（統計資料：平均值，間隔：15 分鐘）	百分比
OcpusAllocated	服務在所選時間間隔內配置的實際 OCPUs 數量。（統計資料：計數、間隔：1 分鐘）	Integer
ParseCount	所選間隔內的硬剖析和軟剖析數目。（統計資料：總和，間隔：1 分鐘）	計數
ParsesByType	每秒硬或軟剖析的數量。（統計資料：平均值、間隔：1 分鐘）	每秒剖析數
ProblematicScheduledDBMSJobs	有問題的排程資料庫任務計數。不適用於容器資料庫。（統計資料：最大值，間隔：15 分鐘）	計數
ProcessLimitUtilization	程序限制使用率。不適用於可插入資料庫。（統計資料：平均值、間隔：1 分鐘）	百分比
Processes	資料庫會處理計數。不適用於可插入資料庫。（統計資料：最大值，間隔：1 分鐘）	計數
ReclaimableFRA	可回收的快速復原區域。不適用於可插入資料庫。（統計資料：平均值，間隔：15 分鐘）	百分比

指標	Description	單位
ReclaimableFRASpace	快閃記憶體復原區域可回收空間。不適用於可插入資料庫。（統計資料：平均值，間隔：15 分鐘）	GB
RedoSizeMB	產生的重做平均數量，以每秒 MB 為單位。（統計資料：平均值、間隔：1 分鐘）	每秒 MB
SessionLimitUtilization	工作階段限制使用率。不適用於可插入資料庫。（統計資料：平均值、間隔：1 分鐘）	百分比
Sessions	資料庫中的工作階段數目。（統計資料：平均值、間隔：1 分鐘）	計數
StorageAllocated	在間隔期間，資料表空間配置的空間上限。對於容器資料庫，此指標提供根容器資料表空間的資料。（統計資料：最大值，間隔：30 分鐘）	GB
StorageAllocatedByTablespace	在間隔期間，資料表空間配置的空間上限。對於容器資料庫，此指標提供根容器資料表空間的資料。（統計資料：最大值，間隔：30 分鐘）	GB
StorageUsed	間隔期間使用的最大空間量。（統計資料：最大值，間隔：30 分鐘）	GB

指標	Description	單位
StorageUsedByTablespace	資料表空間在間隔期間使用的最大空間量。對於容器資料庫，此指標提供根容器資料表空間的資料。（統計資料：最大值，間隔：30 分鐘）	GB
StorageUtilization	目前正在使用的佈建儲存容量百分比。代表所有資料表空間的總配置空間。（統計資料：平均值，間隔：30 分鐘）	百分比
StorageUtilizationByTablespace	使用的空間百分比，依資料表空間。對於容器資料庫，此指標提供根容器資料表空間的資料。（統計資料：平均值，間隔：30 分鐘）	百分比
TransactionCount	在所選間隔期間，使用者遞交和使用者轉返的合併數量。（統計資料：總和，間隔：1 分鐘）	計數
TransactionsByStatus	每秒遞交或復原的交易數量。（統計資料：平均值、間隔：1 分鐘）	每秒交易數
UnusableIndexes	資料庫結構描述中無法使用的索引計數。不適用於容器資料庫。（統計資料：最大值，間隔：24 小時）	計數
UsableFRA	可用的快速復原區域。不適用於可插入資料庫。（統計資料：平均值，間隔：15 分鐘）	百分比

指標	Description	單位
UsedFRASpace	快閃記憶體復原區域空間用量。不適用於可插入資料庫。（統計資料：最大值，間隔：15 分鐘）	GB
UserCalls	在所選間隔內登入、剖析和執行呼叫的合併數量。（統計資料：總和，間隔：1 分鐘）	計數
WaitTimeSeconds	由資料庫執行個體中前景工作階段在時間間隔內累積非閒置等待時間的平均速率。平均作用中工作階段的等待時間元件。（統計資料：平均值，間隔：5 分鐘）	每秒秒數

的 Amazon CloudWatch 維度 Oracle Database@AWS

您可以使用下表中的任何維度來篩選 Oracle Database@AWS 指標資料。

維度	篩選請求的資料 . . .
cloudVmClusterId	VM 叢集的識別符。
cloudExadataInfrastructureId	Exadata 基礎設施的識別符。
collectionName	集合的名稱。
deploymentType	基礎設施的類型。
diskgroupName	磁碟群組的名稱
errorCode	錯誤代碼。
errorSeverity	錯誤的嚴重性。

維度	篩選請求的資料 . . .
filesystemName	檔案系統的名稱。
hostName	主機機器的名稱。
instanceName	資料庫執行個體的名稱。
instanceNumber	資料庫執行個體的執行個體編號。
ioType	一種 I/O 操作類型。
jobId	任務的唯一識別符。
managedDatabaseGroupId	的識別符Managed Database Group。
managedDatabaseId	的識別符Managed Database。
memoryPool	記憶體集區的類型。
memoryType	一種記憶體類型。
ociCloudVmClusterId	VM 叢集的 OCI 識別符。
ociCloudExadataInfrastructureId	Exadata 基礎設施的 OCI 識別符。
parseType	剖析的類型。
resourceId	資源的識別符。
resourceId_Database	資料庫的識別符。
resourceId_DbNode	資料庫節點的識別符。
resourceName	資源的名稱。
resourceName_Database	資料庫的名稱。

維度	篩選請求的資料 . . .
resourceName_DbNode	資料庫節點的名稱。
resourceType	資料庫的類型。
schemaName	結構描述的名稱。
status	資料庫的狀態。
tablespaceContents	資料表空間的內容。
tablespaceName	資料表空間的名稱。
tablespaceType	資料表空間的類型。
transactionStatus	交易的狀態。
waitClass	等待事件的類別。

監控 Amazon EventBridge 中的 Oracle Database@AWS 事件

您可以在 EventBridge 中監控 Oracle Database@AWS 事件，從應用程式 AWS 和服務提供即時資料串流。EventBridge 將此資料路由到目標，例如 AWS Lambda 和 Amazon Simple Notification Service。

> **Note**
>
> EventBridge 之前被稱為 Amazon CloudWatch Events。如需詳細資訊，請參閱《Amazon EventBridge 使用者指南》中的 EventBridge 是 Amazon CloudWatch Events 的演變 Amazon CloudWatch。 EventBridge

Oracle Database@AWS 事件概觀

Oracle Database@AWS 事件是表示資源生命週期變更的結構化訊息。事件匯流排是接收事件並將其交付至零個或多個目的地或目標的路由器。 Oracle Database@AWS 事件可以從下列來源產生：

來自 的事件 AWS

這些事件是從 AWS 端 Oracle Database@AWS APIs 產生，並傳送到您 中的預設事件匯流排 AWS 帳戶。

來自 OCI 的事件

這些事件直接從 OCI 產生，例如與 Oracle Exadata 基礎設施或 VM 叢集相關的事件。當您訂閱 時 Oracle Database@AWS，`aws.partner/odb/`會在 中建立字首為 的事件匯流排 AWS 帳戶 ，以接收來自 OCI 的事件。

Oracle Database@AWS 來自 的事件 AWS

Oracle Database@AWS 事件 AWS 包括與建立和刪除期間 ODB 網路相關的生命週期變更。這些事件會交付至您 中的預設事件匯流排 AWS 帳戶。交付類型是最佳作法。

ODB 網路事件

事件	事件 ID	訊息
建立	ODB-EVENT-0001	成功建立 ODB 網路 odbnet_ID
建立失敗	ODB-EVENT-0011	無法建立 ODB 網路 odbnet_ID
刪除	ODB-EVENT-0002	成功刪除 ODB 網路 odbnet_ID
刪除失敗	ODB-EVENT-0012	無法刪除 ODB 網路 odbnet_ID

範例：ODB 網路建立事件

下列範例顯示成功建立 ODB 網路的事件。

```
{
  "version": "0",
  "id": "01234567-EXAMPLE",
  "detail-type": "ODB Network Event",
  "source": "aws.odb",
  "account": "123456789012",
  "time": "2025-06-12T10:23:43Z",
  "region": "us-east-1",
```

```
  "resources": [
    "arn:aws:odb:us-east-1:123456789012:odbnetwork/odbnet-1234567890abcdef"
  ],
  "detail": {
    "eventId": "ODB-EVENT-0001",
    "message": "Successfully created ODB network odbnet-1234567890abcdef"
  }
}
```

Oracle Database@AWS 來自 OCI 的事件

大多數事件都是直接從 OCI 產生。 會在 aws.partner/odb/中 Oracle Database@AWS 建立字首為的事件匯流排 AWS 帳戶 ，以接收來自 OCI 的事件。建議您不要刪除此事件匯流排。

OCI 提供完整的事件類型，包括下列項目：

- Oracle Exadata 基礎設施
- VM 叢集事件
- CDB 事件
- PDB 事件

如需 OCI 支援的特定事件類型和詳細資訊，請參閱 Oracle Exadata Database Service on Dedicated Infrastructure Events 和 Events for Autonomous Database on Dedicated Exadata Infrastructure。

篩選 Oracle Database@AWS 事件

您可以在 Amazon EventBridge 中的事件匯流排上遵循 EventBridge 建議的事件匯流排設定最佳實務。EventBridge 根據您的使用案例，您可以設定 EventBridge 規則來篩選事件和目標，以接收和使用事件。

從 篩選 ODB 網路事件 AWS

對於來自 的 ODB 網路事件 AWS，您可以使用下列事件模式進行篩選：

```
{
  "source": ["aws.odb"],
  "detail-type": ["ODB Network Event"]
}
```

您可以使用 EventBridge `put-rule` API 搭配預設事件匯流排來套用此模式。如需詳細資訊，請參閱《Amazon EventBridge API 參考》中的 PutRule。

從 OCI 篩選 Oracle Database@AWS 事件

對於來自 OCI Oracle Database@AWS 的事件，您可以使用類似於 Amazon EventBridge API 參考中 PutRule 中範例的命令來設定規則。請注意下列準則：

- 根據您要篩選的事件類型，使用自訂事件模式。
- 將 EventBusName 設定為 Oracle Database@AWS 建立的匯流排名稱。

如需如何篩選事件和跨帳戶設定 EventBridge 目標的詳細資訊，請參閱 Amazon EventBridge AWS 帳戶 中的在 之間傳送和接收事件。

對 Oracle Database@AWS 事件進行故障診斷

如果您遇到事件交付或事件內容的問題，請執行下列動作：

- 如需 ODB 網路事件，請聯絡 AWS 支援。
- 對於 ODB 網路 Oracle Database@AWS 事件以外的事件，請聯絡 Oracle Cloud Support。

如需詳細資訊，請參閱取得 Oracle Database@ 的支援AWS。

使用 記錄 Oracle Database@AWS API 呼叫 AWS CloudTrail

Oracle Database@AWS 已與 整合AWS CloudTrail，此服務提供使用者、角色或 所採取動作的記錄 AWS 服務。CloudTrail 會將 的所有 API 呼叫擷取 Oracle Database@AWS 為事件。擷取的呼叫包括來自 Oracle Database@AWS 主控台的呼叫，以及對 Oracle Database@AWS API 操作的程式碼呼叫。您可以使用 CloudTrail 所收集的資訊來判斷提出的請求 Oracle Database@AWS、提出請求的 IP 地址、提出請求的時間，以及其他詳細資訊。

每一筆事件或日誌專案都會包含產生請求者的資訊。身分資訊可協助您判斷下列事項：

- 該請求是使用根使用者還是使用者憑證提出。
- 請求是否代表 IAM Identity Center 使用者提出。
- 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 服務服務提出。

> **Note**
>
> Oracle Database@AWS 會在 CloudTrail 日誌中記錄來自 AWS Security Token Service (STS) 的 `GetCallerIdentity` API 呼叫。這些 STS API 呼叫會在代表您與 OCI 互動 Oracle Database@AWS 時驗證 的身分。它們是正常且安全 AWS 的操作部分，不會公開敏感資訊。

當您建立帳戶 AWS 帳戶 時CloudTrail 會在 中處於作用中狀態，而且您會自動存取 CloudTrail 事件歷史記錄。CloudTrail 事件歷史記錄為 AWS 區域中過去 90 天記錄的管理事件，提供可檢視、可搜尋、可下載且不可變的記錄。如需詳細資訊，請參閱「AWS CloudTrail 使用者指南」中的使用 CloudTrail 事件歷史記錄。檢視事件歷史記錄不會產生 CloudTrail 費用。

如需 AWS 帳戶 過去 90 天內持續記錄的事件，請建立線索或 CloudTrail Lake 事件資料存放區。

CloudTrail 追蹤

線索能讓 CloudTrail 將日誌檔案交付至 Amazon S3 儲存貯體。使用 建立的所有線索 AWS 管理主控台 都是多區域。您可以使用 AWS CLI建立單一或多區域追蹤。建議您建立多區域追蹤，因為您擷取 AWS 區域 帳戶中所有 的活動。如果您建立單一區域追蹤，您只能檢視追蹤 AWS 區域中記錄的事件。如需追蹤的詳細資訊，請參閱《AWS CloudTrail 使用者指南》中的為您的 AWS 帳戶建立追蹤和為組織建立追蹤。

您可以透過建立追蹤，免費將持續管理事件的一個複本從 CloudTrail 傳遞至您的 Amazon S3 儲存貯體，但這樣做會產生 Amazon S3 儲存費用。如需 CloudTrail 定價的詳細資訊，請參閱 AWS CloudTrail 定價。如需 Amazon S3 定價的相關資訊，請參閱 Amazon S3 定價。

CloudTrail Lake 事件資料存放區

CloudTrail Lake 讓您能夠對事件執行 SQL 型查詢。CloudTrail Lake 會將分列式 JSON 格式的現有事件轉換為 Apache ORC 格式。ORC 是一種單欄式儲存格式，針對快速擷取資料進行了最佳化。系統會將事件彙總到事件資料存放區中，事件資料存放區是事件的不可變集合，其依據為您透過套用進階事件選取器選取的條件。套用於事件資料存放區的選取器控制哪些事件持續存在並可供您查詢。如需 CloudTrail Lake 的詳細資訊，請參閱AWS CloudTrail 《 使用者指南》中的使用 AWS CloudTrail Lake。

CloudTrail Lake 事件資料存放區和查詢會產生費用。建立事件資料存放區時，您可以選擇要用於事件資料存放區的定價選項。此定價選項將決定擷取和儲存事件的成本，以及事件資料存放區的預設和最長保留期。如需 CloudTrail 定價的詳細資訊，請參閱 AWS CloudTrail 定價。

Oracle Database@AWS CloudTrail 中的管理事件

管理事件提供有關在 資源上執行的管理操作的資訊 AWS 帳戶。這些也稱為控制平面操作。根據預設，CloudTrail 記錄管理事件。

Oracle Database@AWS 會將所有 Oracle Database@AWS 控制平面操作記錄為管理事件。

Oracle Database@AWS 事件範例

一個事件代表任何來源提出的單一請求，並包含請求 API 操作的相關資訊、操作的日期和時間、請求參數等。CloudTrail 日誌檔案不是公有 API 呼叫的已排序堆疊追蹤，因此事件不會以任何特定順序顯示。

以下範例顯示的 CloudTrail 事件會示範 `CreateOdbNetwork` 操作。


```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AKIAIOSFODNN7EXAMPLE:yourRole",
        "arn": "arn:aws:sts::123456789012:assumed-role/Admin/yourRole",
        "accountId": "123456789012",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AKIAIOSFODNN7EXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/Admin",
                "accountId": "123456789012",
                "userName": "Admin"
            },
            "attributes": {
                "creationDate": "2024-11-06T21:17:29Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2024-11-06T21:17:44Z",
    "eventSource": "odb.amazonaws.com",
    "eventName": "CreateOdbNetwork",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "python-requests/2.28.2",
```

```
    "requestParameters": {
        "availabilityZoneId": "use1-az6",
        "backupSubnetCidr": "123.45.6.7/89",
        "clientSubnetCidr": "123.44.6.7/89",
        "clientToken": "testClientToken",
        "defaultDnsPrefix": "testLabel",
        "displayName": "yourOdbNetwork"
    },
    "responseElements": {
        "displayName": "yourOdbNetwork",
        "odbNetworkId": "odbnet_1234567",
        "status": "PROVISIONING"
    },
    "requestID": "daf2e3f5-96a3-4df7-a026-863f96db793e",
    "eventID": "797163d3-5726-441d-80a7-6eeb7464acd4",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "odb.us-east-1.amazonaws.com"
    }
}
```


如需有關 CloudTrail 記錄內容的資訊，請參閱《AWS CloudTrail 使用者指南》中的 CloudTrail record contents。

故障診斷 Oracle Database@AWS

使用下列各節來協助疑難排解使用 時可能遇到的網路問題 Oracle Database@AWS。

主題

建立 ODB 網路失敗

當您無法建立 ODB 網路時，以下是常見原因：

受限 CIDR 範圍

ODB 網路會針對用戶端和備份子網路使用特定的 CIDR 範圍。請確定您為這些子網路選擇的 CIDR 範圍不會與任何限制或預留 IP 地址範圍重疊。

下列 CIDR 範圍已保留，無法用於 ODB 網路：

- Oracle 雲端預留範圍：169.254.0.0/16
- 預留類別 D：224.0.0.0 - 239.255.255.255
- 預留類別 E：240.0.0.0 - 255.255.255.255
- 未來的 OCI 使用：100.105.0.0/16

請遵循 VPC 文件中所述的 CIDR 範圍 EC2 規則。若要進一步了解，請參閱 CIDR 區塊關聯限制。

此外，請避免指定 CIDR 範圍與用於 VPC 連線至 ODB 網路範圍之間的重疊。

重疊的 VPC CIDR

您為 ODB 網路指定的 CIDR 範圍不應與任何現有 VPCs 使用的 CIDR 範圍重疊。重疊 CIDR 範圍可能會導致路由衝突，並阻止成功建立 ODB 網路。檢查 ODB 對等 VPCs的 CIDR 範圍，並確保 ODB 網路 CIDR 是唯一且不重疊。

VPCs的擁有權

您連線的 ODB 網路和 VPC 必須由相同的 AWS 帳戶擁有。如果您嘗試將 ODB 網路對等至不同帳戶擁有的 VPC，則建立將會失敗。確認 ODB 網路和 VPC 都屬於同一個 AWS 帳戶。

缺少傳輸閘道

如果您將 CIDR 範圍新增至 ODB 網路對等 CIDR 清單，但未將傳輸閘道連接至 VPC，則建立或更新操作會失敗。不需要使用附件的 CIDR 範圍。

VPC 與 ODB 網路或 VM 叢集之間的連線問題

當您無法從 VPC 連線到 ODB 網路或其中的 VM 叢集時，以下是常見原因：

- 驗證 VPC 組態 – 在 Oracle Database@AWS 主控台中，找到與 ODB 網路對等的 VPC。確認 VPC ID 符合 ODB 網路詳細資訊中顯示的 VPC ID。
- 檢查路由表 – 在 Amazon VPC 主控台中，尋找連接至應用程式執行所在子網路的路由表。檢查路由的目的地 CIDR 是否與 ODB 網路的用戶端子網路 CIDR 相符。確認此路由指向正確的 ODB 網路 ARN。如果路由遺失，請將新的路由新增至 ODB 網路的用戶端子網路 CIDR。
- 驗證對等 CIDRs – 檢閱 ODB 網路詳細資訊中的 `Peered CIDRs`區段。確認列出 VPC 的所有相關 CIDR 區塊。如果缺少必要的 CIDR，請更新對等 CIDRs。
- 檢查安全群組規則 – 在 Amazon EC2 主控台中，尋找 VPC 中資源的安全群組。檢閱傳入和傳出規則，並視需要更新這些規則以允許必要的流量。
- 確認可用區域 – 在 Amazon VPC 主控台中，識別子網路的可用區域 (AZ)。確認 ODB 網路也與您的子網路部署在相同的 AZ 中。
- 避免多個 ODB 網路對等互連 – 在 Oracle Database@AWS 主控台中檢查您的 VPC 對等互連。請確定您只有一個與 ODB 網路的作用中連線。如果您看到多個 ODB 網路對等互連，請移除額外的對等互連。

從 VPC 無法解析的主機名稱或 VM 叢集的掃描名稱

如果 VM 叢集的主機名稱或掃描名稱無法從 VPC 解析，請在 VPC 上設定 DNS 轉送和下列資源，以解析 ODB 網路上託管的 DNS 記錄：

- 將 DNS 查詢傳送至 ODB 網路的傳出端點。如需詳細資訊，請參閱在 中的 ODB 網路中設定傳出端點 Oracle Database@AWS。
- 解析程式規則，用於指定解析程式轉送至 ODB 網路 DNS 的 DNS 查詢網域名稱。如需詳細資訊，請參閱在 中設定解析程式規則 Oracle Database@AWS。

取得 Oracle Database@ 的支援AWS

了解如何取得 Oracle Database@ 的資訊和支援AWS。

Oracle 支援範圍和聯絡資訊

Oracle Cloud Support 是所有 Oracle Database@AWS questions 的第一行支援。若要聯絡支援，請登入 Oracle Cloud Infrastructure (OCI) 主控台，然後選取生命週期移植圖示。如果您沒有 My Oracle Cloud Support 帳戶，請參閱 My Oracle Cloud Support 帳戶和存取權。

Oracle Support 可協助您處理的問題範例包括下列項目：

- 資料庫連線問題 (Oracle TNS)
- Oracle 資料庫效能問題
- Oracle 資料庫錯誤解決方案
- 與服務相關聯 OCI 租用通訊相關的聯網問題
- 配額（限制）增加以接收更多容量（如需詳細資訊，請參閱請求提高資料庫資源的限制)
- 擴展以將更多運算和儲存容量新增至 Oracle 資料庫基礎設施
- 新一代硬體升級
- 與 AWS Marketplace 費用相關的帳單問題

如果您需要在 OCI 主控台之外聯絡 Oracle Support，請告訴 Oracle Support 代理程式您的問題與 Oracle Database@ 有關AWS。這是因為此服務的請求是由專門處理這些部署的 OCI 支援團隊處理。

透過電話聯絡 Oracle 支援

1. 撥打 1-800-223-1711。如果您在美國境外，請造訪 Oracle Support Contacts Global Directory 尋找您所在國家或地區的聯絡資訊。
2. 選擇選項「2」以開啟新的服務請求 (SR)。
3. 針對「不確定」選擇選項「4」。
4. 讓客服人員知道您的多雲端系統發生問題，以及產品的名稱。內部服務請求將代表您開啟，OCI 支援工程師將直接與您聯絡。

您也可以將問題提交至 Oracle Cloud Customer Connect 社群中的多雲端論壇。此選項適用於所有客戶。

My Oracle Cloud Support 帳戶和存取權

若要建立 My Oracle Cloud Support 服務請求票證，組織的 Oracle Database@AWS service 管理員必須核准您的請求。如果您是 Oracle Database@AWS 管理員，請完成 Oracle Database@AWS service 啟用電子郵件中包含的 My Oracle Cloud Support 加入說明。

您可以在下列主題中找到加入 My Oracle Cloud Support 的指示：

- 設定您的 Oracle 支援帳戶
- 建立支援請求

如需核准使用者開啟 My Oracle Cloud Support 請求的說明，請參閱管理員支援任務。

AWS 支援 範圍和聯絡資訊

AWS 支援 是您對所有 AWS相關問題和問題的第一行支援。為您的問題建立 AWS 支援 案例，就像使用其他 AWS 服務一樣。 AWS 支援 團隊會視需要與 OCI Support 合作。

AWS 支援 可協助您處理 的 Oracle Database@AWS issues 範例包括下列項目：

- 虛擬網路問題，包括涉及網路位址轉譯 (NAT)、防火牆、DNS AWS 和流量管理和子網路的問題
- 堡壘和虛擬機器 (VM) 問題，包括資料庫主機連線、軟體安裝、延遲和主機效能
- Amazon CloudWatch 中的 Exadata VM 叢集指標報告
- AWS 與服務相關的帳單問題

如需 的資訊 AWS 支援，請參閱 入門 AWS 支援。

Oracle 服務水準協議

如果您對 Oracle Database@AWS Service Level Agreements (SLAs) 有任何疑問，或想要請求 SLA 違規的服務額度，請聯絡您的 Oracle 客戶經理。如需詳細資訊，請參閱服務水準協議。

Oracle Database@ 的配額AWS

Oracle Database@AWS 是多雲端方案。 AWS 不會設定或強制執行資源的 Oracle Database@AWS 配額。配額由 Oracle Cloud Infrastructure (OCI) 強制執行。如需 OCI 配額的詳細資訊，請參閱 Oracle Cloud Infrastructure 文件中的配額和服務限制。

Oracle Database@AWS 使用者指南的文件歷史記錄

下表說明 文件的發行版本 Oracle Database@AWS。

變更	描述	日期
Oracle Database@AWS 支援亞太區域（雪梨）區域和加拿大（中部）區域	您可以在這些區域中建立 Oracle Database@AWS 資源。如需詳細資訊，請參閱 支援的 區域 Oracle Database@AWS。	2026 年 2 月 2 日
Oracle Database@AWS 支援亞太區域（東京）區域、美國東部（俄亥俄）區域、歐洲（法蘭克福）區域	您可以在這些區域中建立 Oracle Database@AWS 資源。如需詳細資訊，請參閱 支援的 區域 Oracle Database@AWS。	2025 年 12 月 22 日
Oracle Database@AWS 支援跨 共用權利 AWS 帳戶	您現在可以使用 AWS License Manager AWS 帳戶 在同一個 AWS 組織中共用 Oracle Database@AWS across 的 AWS Marketplace 權利。如需詳細資訊，請參閱 Oracle Database@ 中的權限共用 AWS。	2025 年 12 月 19 日
Oracle Database@AWS 支援修改零 ETL 整合資料篩選條件	Oracle Database@AWS 支援修改與 Amazon Redshift 的現有零 ETL 整合的資料篩選條件。您可以更新資料篩選條件模式，以從資料複寫中包含或排除指定的結構描述和資料表。如需詳細資訊，請參閱管理零 ETL 整合。	2025 年 10 月 15 日

Oracle Database@AWS 支援對等連線的對等網路 CIDR 管理	您可以在建立或更新 ODB 互連連線時指定對等網路 CIDRs。您可以控制對等 VPC 中哪些子網路可以存取您的 ODB 網路。VPC 帳戶可以更新 CIDR 範圍，而不需要擁有 ODB 網路。如需詳細資訊，請參閱在 中設定 ODB 對等互連至 Amazon VPC Oracle Database@AWS。	2025 年 10 月 10 日
Oracle Database@AWS 支援與 Amazon Redshift 進行零 ETL 整合	Oracle Database@AWS 現在與 VPC Lattice 整合，以啟用與 Amazon Redshift 的零 ETL 整合。如需詳細資訊，請參閱 Oracle Database@ 的服務整合AWS。	2025 年 7 月 2 日
更新至 IAM 服務連結角色許可	`AmazonODBServiceRolePolicy` 政策現在授予其他許可來描述 VPC 傳輸閘道附件、描述 Amazon EC2 子網路，以及啟用 Amazon EventBridge 來源。如需詳細資訊，請參閱 Oracle Database@AWSAWS 受管政策的更新。	2025 年 6 月 30 日
更新至 IAM 服務連結角色許可	此`AmazonODBServiceRolePolicy` 政策現在授予其他許可，以描述 Amazon EventBridge 排程器中的事件，並建立或描述事件匯流排。如需詳細資訊，請參閱 Oracle Database@AWSAWS 受管政策的更新。	2025 年 6 月 26 日

Oracle Database@AWS 支援美國西部（奧勒岡）區域	您可以在美國西部（奧勒岡）區域中建立 Oracle Database@AWS 資源。支援的實體 AZ IDs為 usw2-az3和 usw2-az4。如需詳細資訊，請參閱 支援的 區域 Oracle Database@AWS。	2025 年 6 月 26 日
Oracle Database@AWS 支援跨 進行資源共用 AWS 帳戶	您現在可以使用 AWS Resource Access Manager () AWS 帳戶 與組織內的其他 共用 Exadata 基礎設施和 VM 叢集AWS RAM。您可以佈建基礎設施一次，並跨多個帳戶共用，降低成本，同時保持責任分離。如需詳細資訊，請參閱 Oracle Database@ 中的資源共用AWS。	2025 年 6 月 26 日
Oracle Database@AWS 支援 Amazon EventBridge 中的事件	Oracle Database@AWS 會將事件交付至 Amazon EventBridge，以監控資源生命週期變更。事件是從 AWS 和 OCI 來源產生，可讓您追蹤 ODB 網路、Exadata 基礎設施、VM 叢集和資料庫的變更。如需詳細資訊，請參閱監控 Oracle Database@AWS Amazon EventBridge 中的事件。	2025 年 6 月 26 日
Oracle Database@AWS 支援跨區域訂閱	Oracle Database@AWS 支援跨區域訂閱，可讓您訂閱一次，並在所有可用的 中使用服務 AWS 區域。如需詳細資訊，請參閱在AWS 多個區域中訂閱 Oracle Database@。	2025 年 6 月 26 日

Oracle Database@AWS 支援 ODB 對等互連做為個別資源	ODB 互連連線現在是具有專用 APIs的獨立資源，用於建立、檢視和刪除互連連線。您可以在相同帳戶或不同帳戶中的 ODB 網路與 Amazon VPC 之間建立對等連線。如需詳細資訊，請參閱使用 ODB 互連連線。	2025 年 6 月 26 日
Oracle Database@AWS 整合 ODB 網路與 Amazon S3	Oracle Database@AWS 現在與 VPC Lattice 整合，以啟用 Oracle 受管備份至 Amazon S3，並引導 ODB 網路存取 Amazon S3。如需詳細資訊，請參閱 Oracle Database@ 的服務整合AWS。	2025 年 6 月 26 日
Oracle Database@AWS 支援自治 VM 叢集	您現在可以在 Exadata 基礎設施上建立自治 VM 叢集。自治 VM 叢集是全受管資料庫，可使用機器學習和 AI 自動化金鑰管理任務。如需詳細資訊，請參閱步驟 3：在 中建立 Exadata VM 叢集或自治 VM 叢集 Oracle Database@AWS。	2025 年 5 月 28 日
Oracle Database@AWS 支援可自訂的維護時段	您現在可以使用 Oracle 受管或客戶受管排程的選項來設定 Exadata 基礎設施的維護時段。您也可以選取修補模式（滾動或非滾動），並指定維護時間偏好設定。如需詳細資訊，請參閱在 中建立 Oracle Exadata 基礎設施 Oracle Database@AWS。	2025 年 5 月 1 日

Oracle Database@AWS 支援新的可用區域 (AZ)	您現在可以使用實體 ID use1-az4或 在 AZ 中建立 ODB 網路use1-az6。如需詳細資訊，請參閱 Oracle Exadata 基礎設施。	2025 年 3 月 26 日
Oracle Database@AWS 支援 Amazon VPC Transit Gateways	如果您將傳輸閘道連接到對等至 ODB 網路的 VPC，您可以將多個 VPCs連接到此閘道。在這些 VPCs可以存取在您的 ODB 網路中執行的 Exadata VM 叢集。如需詳細資訊，請參閱設定 的 Amazon VPC 傳輸閘道 Oracle Database@AWS。	2025 年 3 月 26 日
Oracle Database@AWS 支援 Exadata X11M 的資料庫和儲存伺服器類型	您可以在使用 Exadata X11M 建立基礎設施時指定資料庫伺服器類型和儲存伺服器類型。如需詳細資訊，請參閱在 中建立 Oracle Exadata 基礎設施 Oracle Database@AWS。	2025 年 2 月 4 日
新的服務連結角色政策	Oracle Database@AWS 新增AmazonODBServiceRolePolicy AWSServiceRoleForODB 服務連結角色的新政策。如需詳細資訊，請參閱 AWS 受管政策的Oracle Database@AWS 更新項目。	2024 年 12 月 2 日
初始版本	Oracle Database@AWS 使用者指南的初始版本	2024 年 12 月 2 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。