Oracle Database@AWS 用户指南

Oracle Database@AWS

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Oracle Database@AWS: Oracle Database@AWS 用户指南

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商标和商业外观不得用于任何非 Amazon 的商品或服务，也不得以任何可能引起客户混淆、贬低或诋毁 Amazon 的方式使用。所有非 Amazon 拥有的其他商标均为各自所有者的财产，这些所有者可能附属于 Amazon、与 Amazon 有关联或由 Amazon 赞助，也可能不是如此。

Table of Contents

什么是 Oracle Database@AWS？ 1
功能 1
相关服务 2
访问 2
定价 3
接下来做什么？ 3
工作原理 4
OCI 子网站 4
甲骨文 Exadata 基础架构 4
ODB 网络 5
Virtual Private Cloud (VPC) 6
ODB 对等互连 7
创建 ODB 对等连接 7
AWS 服务集成 8
路由来自多个流量 VPCs 9
AWS Transit Gateway 9
AWS 云广域网 9
Exadata 虚拟机集群 9
自主虚拟机集群 10
甲骨文 Exadata 数据库 10
载入 11
注册获取 AWS 账户 11
创建具有管理访问权限的用户 11
申请私人报价 12
在多个地区订阅 13
开始使用 15
先决条件 15
支持的 OCI 服务 15
支持的区域： 16
规划 IP 地址空间 16
ODB 网络中对 IP 地址的限制 17
客户端子网 CIDR 要求 17
Backup 子网 CIDR 要求 18
IP 消费场景 18

步骤 1：创建 ODB 网络 20
步骤 2：创建 Oracle Exadata 基础架构 22
步骤 3：创建虚拟机集群 24
步骤 4：创建 Oracle Exadata 数据库 27
ODB 对等互连 29
设置 ODB 对等互连 29
更新 ODB 对等互连 31
为 ODB 对等互连配置 VPC 路由表 31
配置 DNS 32
DNS 的工作原理 Oracle Database@AWS 32
配置出站终端节点 33
配置解析器规则 34
测试你的 DNS 配置 35
配置 Amazon VPC 中转网关 Oracle Database@AWS 36
要求 36
限制 36
设置和配置传输网关 37
为以下 AWS 各项配置云 WAN Oracle Database@AWS 38
权利共享 40
共享方法 40
与 L AWS icense Manager 共享权限 40
与 AWS Resource Access Manager (AWS RAM) 共享资源 40
限制 40
在账户之间共享权利 41
共享权利的先决条件 41
权限共享所需的权限 41
共享权限 41
资源共享 43
AWS RAM 整合 43
优势 43
资源共享的工作原理 44
共享资源的权限 44
限制 45
共享资源的限制 45
创建和使用共享资源的限制 46
删除共享资源的限制 46

跨账号共享资源 46
共享资源的先决条件 46
共享资源 47
查看您的资源共享 48
更新或删除资源共享 48
初始化服务 49
什么是服务初始化？ 49
后续步骤 50
使用可信账户中的共享资源 50
可信账户的限制 51
创建虚拟机集群 51
查看共享资源 52
设置与共享 ODB 网络的 ODB 对等互连 53
管理 55
更新 ODB 网络 55
删除 ODB 网络 56
删除虚拟机集群 56
删除 Exadata 基础架构 56
删除 ODB 对等连接 57
正在备份 58
甲骨文托管备份 58
用户管理的备份 58
先决条件 59
Oracle Secure Backup 61
Storage Gateway 62
S3 挂载点 64
禁用对 S3 的访问权限 66
对 Amazon S3 集成进行故障排除 67
与 Redshift 的零 ETL 集成 68
支持的数据库版本 68
工作原理 68
先决条件 69
一般先决条 69
数据库先决条件 69
注意事项 73
限制 74

设置 75
第 1 步：为您的 ODB 网络启用零 ETL 75
步骤 2：配置您的 Oracle 数据库 76
第 3 步：设置 S AWS ecrets Manager 和 AWS 密钥管理服务 76
步骤 4：配置 IAM 权限 79
第 5 步：配置 Amazon Redshift 资源策略 81
步骤 6：使用创建零 ETL 集成 AWS Glue 83
第 7 步：在 Amazon Redshift 中创建目标数据库 83
验证零 ETL 集成 84
数据筛选 85
监控 85
集成状态监控 85
性能监控 86
管理 86
修改零 ETL 集成 86
删除零 ETL 集成 88
最佳实践 89
问题排查 90
集成设置失败 91
复制问题 91
数据一致性问题 92
监控和调试 92
安全性 93
数据保护 94
数据加密 95
传输中加密 95
密钥管理 95
Identity and access management 95
受众 95
使用身份进行身份验证 96
使用策略管理访问 97
如何 Oracle Database@AWS 与 IAM 配合使用 98
基于身份的策略 103
AWS 托管策略 107
Oracle Database@AWS OCI 中的身份验证和授权 108
问题排查 108

合规性验证 110
恢复能力 110
服务关联角色 110
的服务相关角色权限 Oracle Database@AWS 111
Oracle Database@AWS 服务相关角色支持的区域 113
策略更新 113
监控 115
使用监控 CloudWatch 115
CloudWatch 指标 115
CloudWatch 尺寸 125
监控事件 127
活动概述 127
活动来自 AWS 127
来自 OCI 的活动 128
筛选事件 129
Oracle Database@AWS 事件疑难解答 129
CloudTrail 日志 130
Oracle Database@AWS 中的管理事件 CloudTrail 131
Oracle Database@AWS 事件示例 131
问题排查 134
无法创建 ODB 网络 134
解决您的 VPC 和 ODB 网络或虚拟机集群之间的连接问题 135
无法解析的主机名或来自 VPC 的虚拟机集群的扫描名称 135
获取对 Oracle 数据库的支持@AWS 136
Oracle 支持范围和联系信息 136
我的 Oracle 云支持 Support 账户和访问权限 137
AWS 支持 范围和联系信息 137
甲骨文服务级别协议 137
配额 138
文档历史记录 139
..... cxliv

什么是 Oracle Database@AWS？

Oracle Database@AWS 该产品使您能够在数据中心内 AWS 访问由 Oracle 云基础架构 (OCI) 管理的 Oracle Exadata 基础架构。您可以迁移 Oracle Exadata 工作负载，与正在运行的应用程序建立低延迟连接 AWS，并与服务集成。 AWS 您将获得一张发票 AWS Marketplace，该发票计入 AWS 承诺和 Oracle Support 奖励。

下图显示了与托管 Oracle Exadata 基础架构 AWS 的数据中心相关的 OCI 区域的高级概述。在 AWS 可用区 (AZ) 内，您可以将 Amazon VPC 与与数据中心绑定的私有网络对等。通过对等这些网络，VPC 中的应用服务器可以访问在 Oracle Exadata 基础设施上运行的 Oracle 数据库。

的特点 Oracle Database@AWS

借助 Oracle Database@AWS，您可以从以下功能中受益：

将 Oracle Exadata 数据库工作负载迁移到 AWS

借助 Oracle Database@AWS，您可以轻松地将您的 Oracle Exadata 工作负载迁移到专用基础设施上的 Oracle Exadata 数据库服务或其中的专用 Exadata 基础设施上的 Oracle 自治数据库。AWS迁移提供了最少的更改、完整的功能可用性、架构兼容性以及与本地 Exadata 部署相同的性能。您可以使用标准的 Oracle 数据库迁移工具，例如恢复管理器 (RMAN)、Oracle Data Guard、可传输表空间、Oracle Data Pump、Oracle、 AWS 数据库迁移 GoldenGate服务和 Oracle 零停机迁移。

减少了应用程序延迟

您可以在 Oracle Exadata 和其上运行的应用程序之间建立低延迟连接。 AWS靠近托管的应用程序 AWS 可确保最大限度地减少网络延迟并提高性能。

通过数据统一进行创新

通过使用零 ETL 集成来统一整个 Oracle 以及分析、机器学习和生成式 AI 的数据，您可以生成更深入 AWS 的见解并开发新的创新。通过使用 Amazon Redshift 进行零 ETL 集成，您可以对存储在中的交易数据启用近乎实时的分析和机器学习 (ML)。 Oracle Database@AWS

简化的管理和操作

您可以从 Oracle 之间的统一体验以及 AWS 协作支持、采购、管理和运营中受益。您使用 Oracle 数据库服务即有资格享受现有 AWS 承诺和 Oracle 许可权益，例如 Oracle Support Rewards。您可以使用熟悉的 AWS 工具和界面来购买、配置和管理您的 Oracle Database@AWS 资源。您可以

使用 AWS APIs、CLI 或预置和管理您的资源 SDKs。 AWS APIs 调用相应的 OCI APIs 来配置和管理资源。

与 AWS 服务无缝集成

您可以与在同一环境中运行的其他 AWS 服务和应用程序集成。例如，与亚马逊 EC2、亚马逊 VPC 和 IAM Oracle Database@AWS 集成。您还可以 Oracle Database@AWS 与诸如 CloudWatch 用于监控的 Amazon 和 EventBridge 用于事件管理的 Amazon 等 AWS 服务集成。对于数据库备份，您可以使用 Amazon S3，其设计持久性超过 11 9 秒。

相关 AWS 服务

Oracle Database@AWS 与以下服务配合使用，以提高 Oracle 数据库应用程序的可用性和可扩展性：

- 亚马逊 EC2 — 提供充当 Oracle 应用程序服务器的虚拟服务器。您可以将负载均衡器配置为将流量路由到您的 EC2应用程序服务器。有关更多信息，请参阅 Amazon EC2 用户指南。
- Amazon Virtual Private Cloud (VPC) — 使您能够在您定义的逻辑隔离的虚拟网络中启动 AWS 资源。Oracle Exadata 基础设施位于一个名为 ODB 网络的特殊网络中，您可以通过该网络与 VPC 建立对等关系。然后，您可以在 VPC 中运行应用程序服务器并访问您的 Exadata 数据库。有关更多信息，请参阅《Amazon VPC 用户指南》。
- Amazon VPC Lattice — 提供从 ODB 网络对 Amazon S3 和 Oracle 托管备份等 AWS 服务的本地访问权限。有关更多信息，请参阅什么是 Amazon VPC Lattice？ 。
- Amazon CloudWatch — 为提供监控服务 Oracle Database@AWS。OCI 收集有关您的 Oracle Exadata 系统的指标数据并将其发送到。 CloudWatch有关更多信息，请参阅 Oracle Database@AWS 使用 Amazon 进行监控 CloudWatch。
- AWS Identity and Access Management (IAM) — 帮助您安全地控制用户对 Oracle Database@AWS 资源的访问权限。使用 IAM 控制谁可以使用您的 AWS 资源（身份验证）以及用户可以通过哪些方式使用哪些资源（授权）。有关更多信息，请参阅 的身份和访问管理 Oracle Database@AWS。
- AWS 分析服务 — 提供广泛且经济实惠的分析服务，帮助您更快地从 Exadata 数据库中获得见解。每项服务均专为各种分析用例而构建，例如交互式分析、大数据处理、数据仓库、实时分析、运营分析、仪表板和可视化。有关更多信息，请参阅上的 Analytics AWS。

正在访问 Oracle Database@AWS

您可以使用创建、访问和管理 Oracle Database@AWS AWS 管理控制台。它提供了一个可用于访问的 Web 界面 Oracle Database@AWS。

的定价 Oracle Database@AWS

您可以从中购买 Oracle Database@AWS 产品 AWS Marketplace。您首先要联系 Oracle 销售代表。然后，Oracle AWS Marketplace 根据私有定价协议向您提供该报价。您的 AWS 账单会根据您的使用量显示费用。

如果您的 Oracle 应用程序和 Oracle 数据库托管在同一个可用区 (AZ) 中，则无需支付数据传输费用。之间的通信收取标准数据传输费 AZs。

使用 Oracle Database@AWS 托管集成（例如零ETL、Oracle托管备份和Amazon S3）时，通过VPC Lattice共享和访问资源将收取标准数据处理费用。 Oracle Database@AWS 托管集成不按小时收费。有关更多信息，请参阅 Amazon VPC Lattice 定价。

接下来做什么？

现在，您可以开始创建 Oracle Database@AWS 资源了。

1. 了解 Oracle Database@AWS 工作原理。有关更多信息，请参阅 如何 Oracle Database@AWS 运作。

   > **Note**
   >
   > 如果您熟 AWS 悉 Oracle Exadata 并想立即开始使用，请跳过此步骤。

2. Oracle Database@AWS 通过申请私人报价 AWS 管理控制台，然后接受报价。有关更多信息，请参阅 申请 Oracle 数据库的私募报价@AWS。

   > **Note**
   >
   > 要在此预览版中申请私人报价，您必须联系 AWS 以将其 AWS 账户 添加到允许列表中。

3. 使用控制台创建 ODB 网络、Oracle Exadata 基础设施和 Exadata 虚拟机集群。 AWS 使用 OCI 工具创建 Exadata 数据库。有关更多信息，请参阅 Oracle 数据库入门@AWS。
4. 使用 AWS Resource Access Manager (AWS RAM) 跨账户共享您的资源。有关更多信息，请参阅 使用可信账户中的共享 Oracle Database@AWS 资源。

如何 Oracle Database@AWS 运作

Oracle Database@AWS 将 Oracle 云基础架构 (OCI) 与. AWS Cloud在以下各节中，您可以了解此多云架构的关键组件。

专用基础架构上的 Oracle Exadata 数据库服务是一项提供 Exadata 数据库机的 OCI 服务。Oracle Exadata 数据库机是一个集成、预配置和预先测试的全栈平台，适用于企业数据中心。您可以使用 AWS 控制台、CLI 或在 AWS 可用区 (AZ) 中创建 Oracle Exadata 基础设施和虚拟机集群。 APIs

在中创建资源后 AWS，可以使用 OCI 创建和管理 O APIs racle Exadata 数据库。与亚马逊 VPC 对等的 ODB 网络使亚马逊 EC2 应用程序服务器能够访问您的 Exadata 数据库。通过这种方式，Oracle Exadata 数据库可以集成到环境中。 AWS

下图显示了 Oracle Database@AWS 架构。

OCI 子网站

Oracle 云基础设施托管在 OCI 区域和可用性域中。OCI 区域由 OCI 可用性域 (ADs) 组成，这些域是 OCI 区域内的隔离数据中心集群。OCI 子站点是将 OCI 可用性域扩展到某个区域中的可用区 (AZ) 的数据中心。 AWS Exadata 基础架构在逻辑上驻留在 OCI 区域中，实际驻留在一个区域中。 AWS

的 OCI 子站点 Oracle Database@AWS 实际位于 AWS 数据中心中。 AWS 托管 Exadata 基础架构，OCI 在数据中心内部配置和维护 Exadata 基础架构硬件。您可以使用 AWS 控制台、CLI 或配置 Exadata 基础架构、私有网络和虚拟机集群。 APIs您可以使用诸如 Amazon EC2 和 Amazon VPC 之类的 AWS 服务来允许应用程序访问在基础设施上运行的 Oracle Exadata 数据库。

甲骨文 Exadata 基础架构

Oracle Exadata 基础架构是运行 Oracle Exadata 数据库的数据库服务器和存储服务器的底层架构。基础设施位于 AWS 可用区 (AZ) 中。要在 Exadata 基础架构上创建虚拟机集群，您可以使用 AWS 控制台、CLI 或。 APIs

Oracle Exadata 基础架构分布在称为数据库服务器的物理机上。这些服务器提供计算资源，类似于 Amazon EC2 专用服务器。每台数据库服务器都托管一个或多个在虚拟机管理程序上运行的虚拟机 (VMs)。有关说明这些关系的架构图，请参阅专用基础设施技术架构上的 Exadata 数据库服务。

在 Oracle Database@ 中创建 Exadata 基础架构时AWS，需要指定以下信息：

- 数据库服务器的总数
- 存储服务器的总数
- Exadata 系统型号 (X11M)
- 托管基础设施的可用区（请参阅支持的区域 Oracle Database@AWS）

要了解如何创建 Oracle Exadata 基础架构，请参阅。步骤 2：在中创建 Oracle Exadata 基础架构 Oracle Database@AWS

ODB 网络

ODB 网络是一个私有隔离网络，在 AWS 可用区 (AZ) 中托管 OCI 基础架构。ODB 网络由 CIDR 范围的 IP 地址组成。ODB 网络直接映射到 OCI 子站点中存在的网络，从而充当 AWS 和 OCI 之间的通信手段。在创建 Exadata 虚拟机集群时，必须指定 ODB 网络（请参阅）。步骤 3：在中创建 Exadata 虚拟机群集或自治虚拟机群集 Oracle Database@AWS

您可以使用 Oracle Databas AWS APIs e@ 在 ODB 网络中配置资源。ODB 网络由管理 AWS，但您可以设置 ODB 对等连接以将 Amazon VPC 连接到 ODB 网络。有关更多信息，请参阅 en ODB 对等互连。

创建 ODB 网络时，需要指定以下信息：

- 可用区 — ODB 网络特定于可用区。

  你可以在以下 Oracle Database@AWS 中使用 AWS 区域：

  美国东部（弗吉尼亚州北部）

  您可以将 AZs 与物理 IDs use1-az4和use1-az6.

  美国西部（俄勒冈州）

  您可以将 AZs 与物理 IDs usw2-az3和usw2-az4.

  亚太地区（东京）

  您可以将 AZs 与物理 IDs apne1-az1和apne1-az4.

  美国东部（俄亥俄州）

  您可以将 AZs 与物理 IDs use2-az1和use2-az2.

欧洲地区（法兰克福）

您可以将 AZs 与物理 IDs euc1-az1和euc1-az2.

加拿大（中部）

您可以使用带有物理 ID 的 AZ cac1-az4。

亚太地区（悉尼）

您可以使用带有物理 ID 的 AZ apse2-az4。

要在您的账户中查找映射到前面物理可用区的逻辑可用区名称 IDs，请运行以下命令。

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

- 客户端 CIDR 地址 — ODB 网络需要 Exadata 虚拟机群集和自治虚拟机群集的客户端子网 CIDR。
- 备份 CIDR 地址 — ODB 网络需要备份子网 CIDR 来对虚拟机群集进行托管数据库备份。对于 Exadata 虚拟机集群，备份子网是可选的。
- AWS 服务集成 — 您可以为 AWS 服务集成（例如 Amazon S3 和使用 Amazon Redshift 的 Zero-ETL）配置网络路径。有关更多信息，请参阅 AWS 服务集成。

有关更多信息，请参阅 步骤 1：在中创建 ODB 网络 Oracle Database@AWS。

Virtual Private Cloud (VPC)

虚拟私有云 (VPC) 是您在云中 AWS 创建的虚拟网络。它在逻辑上与 AWS 云中的其他虚拟网络隔离，使您可以完全控制虚拟网络环境，包括选择自己的 IP 地址范围、创建子网以及配置路由表和网络网关。有关更多信息，请参阅什么是 Amazon VPC？

您可以在您的亚马逊 VPC 中启动亚马逊 EC2 实例。这些 EC2 实例可以托管与 Oracle Exadata 数据库通信的应用程序服务器。您可以像 VPC 中的任何其他 EC2 实例一样管理和启动应用程序服务器。有关更多信息，请参阅什么是亚马逊 EC2？

默认情况下，ODB 网络无法连接。 VPCs要将 ODB 网络连接到您的现有 AWS 基础设施，请在 ODB 网络和一个 VPC 之间创建对等连接。您可以在创建 ODB 网络时指定 VPC。有关更多信息，请参阅 步骤 1：在中创建 ODB 网络 Oracle Database@AWS。

ODB 对等互连

ODB 对等互连是用户创建的网络连接，它允许在 Amazon VPC 和 ODB 网络之间私下路由流量。VPC 和 ODB 网络之间存在一对一的关系。对等互连后，VPC 内的 Amazon EC2 实例可以与 ODB 网络中的 Oracle Exadata 数据库进行通信，就像它们在同一个网络中一样。

> **Note**
>
> ODB 对等与 VPC 对等互连不同，后者是两者之间的对等连接，用于在两者之间路由流 VPCs 量。

您可以使用对等一个账户中的 ODB 网络和另一个账户中的 VPC。 AWS RAM如果您与其他账户共享 ODB 网络，则该信任账户可以直接启动对等互连。启动 ODB 对等连接的帐户拥有并管理该连接。

在创建或更新 ODB 对等连接 CIDRs 时，您可以指定对等网络。通过这种方式，您可以控制对等 VPC 中的哪些子网可以访问您的 ODB 网络。VPC 账户可以在不拥有 ODB 网络的情况下更新 CIDR 范围。有关更多信息，请参阅中的配置与 Amazon VPC 的 ODB 对等关系。 Oracle Database@AWS

VPC 中的资源可以跨越可用区 (AZs)。在 ODB 网络中，资源绑定到单个可用区。您在创建 ODB 网络时定义此可用区。

创建 ODB 对等连接

ODB 对等连接不是 ODB 网络的特征，而是具有自己的 ID（前缀为 ）和生命周期的独立资源。odbpcx-您可以使用一组专用的 APIs对等连接来管理对等连接。例如，您可以使用 Oracle Database@AWS 控制台或 API 创建与现有 ODB 网络的 ODB 对等连接。CreateOdbPeeringConnection有关更多信息，请参阅 在 Oracle 数据库中创建 ODB 对等连接@AWS。

创建 ODB 对等连接时，Oracle Database@AWS 会自动执行以下操作：

1. 验证网络配置，包括检查是否与 Oracle VCN CIDR 重叠的 CIDR 块
2. 设置底层网络对等互连基础架构
3. 使用 VPC CIDR 地址配置 ODB 网络（不是 VPC）路由表

创建 ODB 对等连接后，使用 Ama EC2 `create-route` zon 命令手动更新您的 VPC 路由表。有关更多信息，请参阅 为 ODB 对等互连配置 VPC 路由表。

AWS 服务集成

为了为您的 Oracle 数据库提供增强的功能和连接选项，Oracle Database@ 与使用 AWS 服务 Amazon VPC Lattice 进行了AWS 集成。您可以将网络路径配置为 AWS 服务 直接来自 ODB 网络，而无需进行额外 VPCs 或复杂的网络设置。

Oracle Database@AWS 支持以下 AWS 托管服务集成：

Amazon S3

您可以通过以下方式将 Amazon S3 与 Oracle Database@AWS 集成：

- Oracle 管理了对亚马逊 S3 的自动备份 — Oracle Database@AWS 自动启用网络访问以进行自动备份。无法禁用此集成。如果您在 OCI 控制台中将 Amazon S3 设置为托管备份目标，则 OCI 会将自动备份上传到 S3 存储桶。
- 从 ODB 网络直接访问 Amazon S3-您可以启用对 S3 的直接 ODB 网络访问，然后在 S3 存储桶中存储脚本、导入和导出文件以及相关文件。您可以禁用此访问权限。此设置与 Oracle 托管的自动备份的自动网络访问无关。

与 Amazon Redshift 的零 ETL 集成

您可以启用与 Amazon Redshift 的 ODB 网络的零 ETL 集成。这种集成使您能够将数据从在 Oracle Database@ 中运行的 Oracle 数据库复制到 Amazon Redshift，AWS 而无需传统的提取、转换和加载 (ETL) 流程。这种集成通过自动将您的 Oracle 数据与 Amazon Redshift 同步，实现实时分析和 AI 工作负载。

除了 AWS 服务的托管集成外，您还可以使用 VPC Lattice 访问托管在其他服务器中的服务和资源 VPCs，或者从您的 VPC 访问 ODB 网络实例。您可以使用VPC Lattice控制台、CLI和来管理访问和APIs资源。有关更多信息，请参阅以下资源：

- 在 Oracle 数据库中备份@AWS
- Oracle Database@AWS Zero-ETL 与亚马逊 Redshift 集成
- 什么是 Amazon VPC Lattice？ 还有适用于 Oracle 数据库的 VPC Lattice @AWS

路由来自多个流量 VPCs

VPCs 要允许多人访问一个 ODB 网络中的 Oracle Database@AWS 资源，您可以使用 AWS Transit Gateway 或 AWS Cloud WAN。

AWS Transit Gateway

Amazon VPC 传输网关是一个用于互连 VPCs 和本地网络的网络传输中心。ODB 网络仅支持 ODB 网络和单个 VPC 之间的 one-to-one直接对等。您可以将您的 ODB 网络与 VPC 对等，然后将此 VPC 连接到传输网关。网关可以连接到多个 VPCs。使用此传输网关配置，您可以将多个 VPC 子网之间的流量路由到单个 ODB 网络。

有关更多信息，请参阅 配置 Amazon VPC 中转网关 Oracle Database@AWS。

AWS 云广域网

AWS Cloud WAN 是一项托管广域网 (WAN) 服务，可让您构建、管理和监控统一的全球网络，连接云和本地环境中的资源。使用中央控制面板，您可以连接本地分支机构、数据中心和 VPCs AWS 全球网络。

您可以将您的 ODB 网络与 VPC 对等，然后将此 VPC 连接到云 WAN 核心网络。通过此配置，您可以使用 Cloud WAN 在多个 VPCs 或本地网络与您的 ODB 网络之间路由流量。有关更多信息，请参阅 为以下 AWS 各项配置云 WAN Oracle Database@AWS。

Exadata 虚拟机集群

Exadata 虚拟机群集是一组紧密耦合的 Exadata。 VMs每台虚拟机都安装了完整的 Oracle 数据库，其中包括 Oracle 企业版的所有功能，包括 Oracle Real Application Clusters (Oracle RAC) 和 Oracle 网格基础设施。您可以在虚拟机集群上创建一个或多个 Oracle Exadata 数据库。有关显示 VMs和虚拟机集群架构的图表，请参阅专用基础设施技术架构上的 Exadata 数据库服务。

创建虚拟机集群时，需要指定包含以下内容的信息：

- 一个 ODB 网络
- 甲骨文 Exadata 基础架构
- 要在集群中放置 VMs 的数据库服务器
- 可用 Exadata 存储空间的总量

您可以为虚拟机集群中的每个 VM 配置 CPU 内核、内存和本地存储。有关更多信息，请参阅 步骤 3：在中创建 Exadata 虚拟机群集或自治虚拟机群集 Oracle Database@AWS。

自主虚拟机集群

自治虚拟机集群是完全托管的数据库，可使用机器学习和 AI 自动执行关键管理任务。与传统数据库不同，自治数据库无需人工干预即可自动配置、保护、更新、备份和调整数据库。

您可以配置每个 VM 的 ECPU 核心数、每 CPU 的数据库内存、数据库存储空间和自治容器数据库的最大数量。有关更多信息，请参阅 步骤 3：在中创建 Exadata 虚拟机群集或自治虚拟机群集 Oracle Database@AWS。

甲骨文 Exadata 数据库

Oracle Exadata 是一个经过精心设计的系统，可为运行 Oracle 数据库提供高性能平台。使用 Oracle Database@AWS，您可以使用 AWS 控制台创建 Oracle Exadata 基础架构和托管 Exadata 数据库的虚拟机集群。然后，您可以使用 OCI APIs 来创建和管理 Oracle 数据库。有关更多信息，请参阅 步骤 4：在 Oracle 云基础设施中创建 Oracle Exadata 数据库。

加入 Oracle 数据库@AWS

在开始使用之前 Oracle Database@AWS，请确保您已注册 AWS 并创建必要的用户。然后，您可以 AWS Marketplace 通过接受 Oracle 的私人报价购买 Oracle Database@AWS 。

注册获取 AWS 账户

如果您没有 AWS 账户，请完成以下步骤来创建一个。

要注册 AWS 账户

1. 打开https://portal.aws.amazon.com/billing/注册。
2. 按照屏幕上的说明操作。

   在注册时，将接到电话或收到短信，要求使用电话键盘输入一个验证码。

   当您注册时 AWS 账户，就会创建AWS 账户根用户一个。根用户有权访问该账户中的所有 AWS 服务 和资源。作为最佳安全实践，请为用户分配管理访问权限，并且只使用根用户来执行需要根用户访问权限的任务。

AWS 注册过程完成后会向您发送一封确认电子邮件。您可以随时前往 https://aws.amazon.com/并选择“我的账户”，查看您当前的账户活动并管理您的账户。

创建具有管理访问权限的用户

注册后，请保护您的安全 AWS 账户 AWS 账户根用户 AWS IAM Identity Center，启用并创建管理用户，这样您就不会使用 root 用户执行日常任务。

保护你的 AWS 账户根用户

1. 选择 Root 用户并输入您的 AWS 账户 电子邮件地址，以账户所有者的身份登录。AWS 管理控制台在下一页上，输入您的密码。

   要获取使用根用户登录方面的帮助，请参阅《AWS 登录 用户指南》中的 Signing in as the root user。
2. 为您的根用户启用多重身份验证（MFA）。

   有关说明，请参阅 I A M 用户指南中的为 AWS 账户 根用户启用虚拟 MFA 设备（控制台）。

创建具有管理访问权限的用户

1. 启用 IAM Identity Center。

   有关说明，请参阅《AWS IAM Identity Center 用户指南》中的启用 AWS IAM Identity Center。

2. 在 IAM Identity Center 中，为用户授予管理访问权限。

   有关使用 IAM Identity Center 目录 作为身份源的教程，请参阅《用户指南》 IAM Identity Center 目录中的使用默认设置配置AWS IAM Identity Center 用户访问权限。

以具有管理访问权限的用户身份登录

- 要使用您的 IAM Identity Center 用户身份登录，请使用您在创建 IAM Identity Center 用户时发送到您的电子邮件地址的登录 URL。

  有关使用 IAM Identity Center 用户登录的帮助，请参阅AWS 登录 用户指南中的登录 AWS 访问门户。

将访问权限分配给其他用户

1. 在 IAM Identity Center 中，创建一个权限集，该权限集遵循应用最低权限的最佳做法。

   有关说明，请参阅《AWS IAM Identity Center 用户指南》中的 Create a permission set。

2. 将用户分配到一个组，然后为该组分配单点登录访问权限。

   有关说明，请参阅《AWS IAM Identity Center 用户指南》中的 Add groups。

申请 Oracle 数据库的私募报价@AWS

AWS Marketplace 卖家私下报价功能使您能够向甲骨文申请并接收 Oracle 的 Oracle Database@AWS 定价和最终用户许可协议条款。您与 Oracle 协商定价和条款，然后 Oracle 为您指定的报价创建私 AWS 账户 有报价。您接受私下报价，并收到议定的价格和使用条款。此时，您可以使用 Oracle Database@AWS 控制面板。当私募协议到期日时，您要么自动转到产品的公开定价，要么取消订阅 Oracle Database@。AWS有关私人优惠的更多信息，请参阅中的私人优惠 AWS Marketplace。

申请并接受私人报价 Oracle Database@AWS

1. 登录到 AWS 管理控制台。

2. 搜索然后选择 Oracle 数据库 @AWS。
3. 选择 “申请私人报价”。

> **Note**
>
> 在您接受私人报价后， Oracle Database@AWS 控制面板才可用。

4. 在 Oracle 云基础架构 (OCI) 网站上，指定详细信息，例如地区和您的联系信息。
5. 等待 OCI 代表与您联系并提供私人报价。
6. 在中 AWS 管理控制台，选择查看私人优惠。
7. 选择报价，然后选择 “查看报价”。
8. 选择 “创建合同”，然后根据后续提示接受私募报价。
9. 接受私人报价后，您需要激活您的OCI帐户。您可以直接从中访问 Oracle 激活链接 AWS 管理控制台。
    1. 在控制台中，导航至 “入门” 部分。
    2. 单击控制台中提供的 Oracle 激活链接。或者，您也可以使用通过电子邮件发送给您的激活链接。
    3. 在 Oracle 激活页面上，选择是创建新的 Oracle 云帐户还是向现有帐户添加帐户。
    4. 按照屏幕上的说明完成激活过程。
    5. 提交激活请求后，您将在中看到 “激活正在进行” 状态 AWS 管理控制台，控制面板将暂时禁用，并显示原因。
    6. 激活完成后，Oracle Database@AWS 控制面板将变为可用，允许您管理自己的资源。
10. 在中 AWS 管理控制台，选择控制面板。

在多个区域订阅 Oracle Database@AWS

当您订阅 AWS Marketplace 并 Oracle Database@AWS 完成入职后，您的租约将与您 AWS 账户 的 OCI 租约相关联。此链接以及相关资源会自动复制到所有 Oracle Database@AWS 可用的 AWS 区域。您只需订阅和注册一次，而不必为每个地区重复该过程。

要 Oracle Database@AWS 在多个区域中使用，请执行以下步骤：

1. 订阅 AWS Marketplace 并 Oracle Database@AWS 完成入职流程。

当您首次订阅 Oracle Database@ 时AWS，您的账户将在主区域激活。您可以在 Oracle 云基础架构 (OCI) 中指定主区域。

2. 通过 OCI 控制台启用您的首选区域。

   如果您未在 OCI 中启用某个区域，然后在 Oracle Database@AWS 控制台中切换到该区域，则会收到一条错误消息，指出您尚未订阅。在这种情况下，必须先在 OCI 中启用此区域，然后才能使用该区域中的 Oracle Database@AWS 控制面板。

3. 无需重复订阅流程即可访问 Oracle Database@AWS 任何受支持的 AWS 区域。

Oracle 数据库入门@AWS

要开始使用 Oracle Database@AWS，您可以使用 Oracle Database@AWS 控制台、CLI 或创建以下资源 APIs：

1. ODB 网络
2. 甲骨文 Exadata 基础架构
3. Exadata 虚拟机集群或自治虚拟机集群
4. ODB 对等连接

要在基础架构上创建 Oracle Exadata 数据库，必须使用 Oracle 云基础架构 (OCI) 控制台或控制面 APIs 板。 Oracle Database@AWS 因此，您可以在两个云环境中部署资源：网络和基础设施资源位于 OCI 中 AWS，而数据库管理控制平面位于 OCI 中。有关更多信息，请参阅 Oracle 云基础设施文档Oracle Database@AWS中的。

设置的先决条件 Oracle Database@AWS

在配置 Oracle Exadata 基础架构之前，请务必执行以下操作：

- 按照加入 Oracle 数据库@AWS中的步骤操作。您必须已接受私人报价才能使用 Oracle Database@AWS。
- 向您的 IAM 委托人授予中列出的策略权限允许用户配置 Oracle Database@AWS 资源。这些权限是使用所必需的 Oracle Database@AWS。

支持的 OCI 服务 Oracle Database@AWS

Oracle Database@AWS 支持以下 Oracle 云基础设施 (OCI) 服务：

- 专用基础架构上的 Oracle Exadata 数据库服务 — 提供可在其中访问的完全托管的专用 Exadata 环境。 AWS有关更多信息，请参阅 OCI 文档中关于专用基础设施的 Oracle Cloud Exadata 数据库服务。
- 专用 Exadata 基础架构上的自治数据库 — 提供高度自动化、完全托管的数据库环境，在 OCI 中运行，并提供已投入的硬件和软件资源。有关更多信息，请参阅 OCI 文档中的关于专用 Exadata 基础架构上的自治数据库。

支持的区域 Oracle Database@AWS

你可以在以下 Oracle Database@AWS 中使用 AWS 区域：

美国东部（弗吉尼亚州北部）

您可以将 AZs 与物理 IDs use1-az4和use1-az6.

美国西部（俄勒冈州）

您可以将 AZs 与物理 IDs usw2-az3和usw2-az4.

亚太地区（东京）

您可以将 AZs 与物理 IDs apne1-az1和apne1-az4.

美国东部（俄亥俄州）

您可以将 AZs 与物理 IDs use2-az1和use2-az2.

欧洲地区（法兰克福）

您可以将 AZs 与物理 IDs euc1-az1和euc1-az2.

加拿大（中部）

您可以使用带有物理 ID 的 AZ cac1-az4。

亚太地区（悉尼）

您可以使用带有物理 ID 的 AZ apse2-az4。

要在您的账户中查找映射到前面物理可用区的逻辑可用区名称 IDs，请运行以下命令。

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

规划 IP 地址空间 Oracle Database@AWS

仔细规划 IP 地址空间 Oracle Database@AWS。根据虚拟机群集的数量考虑 IP 地址消耗，包括可以配置到 ODB 网络的 VMs 每个集群的数量。有关更多信息，请参阅 Oracle 云基础设施文档中的 ODB 网络设计。

主题

- ODB 网络中对 IP 地址的限制
- ODB 网络的客户端子网 CIDR 要求
- ODB 网络的备份子网 CIDR 要求
- ODB 网络的 IP 使用场景

ODB 网络中对 IP 地址的限制

请注意以下有关 ODB 网络中 CIDR 范围的限制：

- 创建 ODB 网络后，您无法修改其客户端或备份子网 CIDR 范围。
- 您不能使用 CIDR 区块关联限制表中 “受限关联” 列中的 VPC IPv4 CIDR 范围。
- 对于 Exadata X9M，OCI 自动化将 IP 地址 100.106.0.0/16 和 100.107.0.0/16 保留给集群互连，因此您无法执行以下操作：
  - 将这些范围分配给 ODB 网络的客户端或备份 CIDR 范围。
  - 将这些范围用于连接到 ODB 网络的 VPC CIDR。
- 以下 CIDR 范围是为 Oracle 云基础设施保留的，不能用于 ODB 网络：
  - 甲骨文云保留范围 CIDR 169.254.0.0/16
  - D 类预留 224.0.0.0 — 239.255.255.255
  - 预留级 E 240.0.0.0 — 255.255.255.255
- 客户端子网和备份子网的 IP 地址 CIDR 范围不能重叠。
- 您不能将分配给客户端和备份子网的 IP 地址 CIDR 范围与用于连接 ODB 网络的 VPC CIDR 范围重叠。
- 您无法在虚拟机集群 VMs 中配置到不同的 ODB 网络。网络是虚拟机群集的属性，这意味着您只能将虚拟机集群 VMs 中的配置到同一 ODB 网络中。

ODB 网络的客户端子网 CIDR 要求

在下表中，您可以找到服务和基础设施为客户端子网 CIDR 消耗的 IP 地址数量。客户端子网的最小 CIDR 大小为 /27，最大大小为 /16。

IP 地址数	被消耗了	注意
6	Oracle Database@AWS	无论您在 ODB 网络中配置了多少虚拟机群集，这些 IP 地址都会被保留。 Oracle Database@AWS 消耗以下内容： • 3 个为 ODB 网络资源保留的 IP 地址 AWS • 3 个为 OCI 网络服务保留的 IP 地址
3	每个虚拟机集群	无论每个虚拟机群集中存在多少个 IP 地址，这些 IP 地址 VMs 都是为单一客户机访问名称 (SCANs) 保留的。
4	每台虚拟机	这些 IP 地址完全取决于基础架构 VMs 中的数量。

ODB 网络的备份子网 CIDR 要求

在下表中，您可以找到备份子网 CIDR 的服务和基础架构使用的 IP 地址数量。备份子网的最小 CIDR 大小为 /28，最大大小为 /16。

IP 地址数	被消耗了	注意
3	Oracle Database@AWS	无论您在 ODB 网络中配置了多少虚拟机群集，这些 IP 地址都会被保留。 Oracle Database@AWS 消耗以下内容： • 2 个 IP 地址位于 CIDR 范围的开头 • 1 个 IP 地址位于 CIDR 范围的末尾
3	每台虚拟机	这些 IP 地址完全取决于基础架构 VMs 中的数量。

ODB 网络的 IP 使用场景

在下表中，您可以看到 ODB 网络中用于不同虚拟机群集配置的 IP 地址。虽然 /28 是客户机子网 CIDR 部署 1 个虚拟机集群和 2 个虚拟机群集的技术上最低 CIDR 范围 VMs，但我们建议您至少使用 /27 CIDR 范围。在这种情况下，IP 范围未被虚拟机群集完全占用，因此允许分配额外的 IP 地址。

配置	客户机 IPs 已消费	客户 IPs 最低要求	IPs 已消耗的备份	Backup IPs 最低要求
1 个虚拟机集群和 2 个 VMs	17 (6 个服务 + 3 个集群 + 4*2)	32（/27 CIDR 范围）	9 (3 项服务 + 3*2)	16（/28 CIDR 范围）
1 个虚拟机集群有 3 个 VMs	21 (6 个服务 + 3 个集群 + 4*3)	32（/27 CIDR 范围）	12 (3 项服务 + 3*3)	16（/28 CIDR 范围）
1 个虚拟机集群有 4 个 VMs	25 (6 个服务 + 3 个集群 + 4*4)	32（/27 CIDR 范围）	15 (3 项服务 + 3*4)	16（/28 CIDR 范围）
1 个虚拟机集群有 8 个 VMs	41 (6 个服务 + 3 个集群 + 4*8)	64（/26 CIDR 范围）	27 (3 项服务 + 3*8)	32（/27 CIDR 范围）

下表显示了在给定特定客户端 CIDR 范围的情况下，每种配置可能有多少个实例。例如，1 个 VM 群集 4 VMs 占用客户端子网中的 24 个 IP 地址。如果 CIDR 范围为 /25，则有 128 个 IP 地址可用。因此，您可以在子网中配置 5 个虚拟机集群。

虚拟机集群配置	带有 /27 的数字 (32 IPs)	带有 /26 的数字 (64 IPs)	带有 /25 的数字 (128 IPs)	带有 /24 的数字 (256 IPs)	/23 时的数字 (512 IPs)	/22 时的数字 (1024 IPs)
1 个带有 2 VMs (16 IPs) 个虚拟机群集	1	3	7	15	30	60
1 个带有 3 VMs (20 IPs) 个虚拟机群集	1	3	6	12	24	48
1 个带有 4 VMs (24 IPs) 个虚拟机集群	1	2	5	10	20	40
2 个虚拟机群集， VMs 每个集群有 2 个 (27 IPs)	1	2	4	9	18	36

虚拟机集群配置	带有 /27 的数字 (32 IPs)	带有 /26 的数字 (64 IPs)	带有 /25 的数字 (128 IPs)	带有 /24 的数字 (256 IPs)	/23 时的数字 (512 IPs)	/22 时的数字 (1024 IPs)
2 个虚拟机群集， VMs 每个集群有 3 个 (35 IPs)	0	1	3	7	14	28
2 个虚拟机群集， VMs 每个集群有 4 个 (43 IPs)	0	1	2	5	11	23

步骤 1：在中创建 ODB 网络 Oracle Database@AWS

ODB 网络是一个私有隔离网络，在可用区 (AZ) 中托管 OCI 基础架构。ODB 网络和 Oracle Exadata 基础架构是配置虚拟机群集和创建 Exadata 数据库的先决条件。您可以按任一顺序创建 ODB 网络和 Oracle Exadata 基础架构。有关更多信息，请参阅ODB 网络和ODB 对等互连。

此任务假设您已阅读规划 IP 地址空间 Oracle Database@AWS。要稍后修改或删除 ODB 网络，请参阅管理 Oracle 数据库@AWS。

创建 ODB 网络

1. 登录 AWS 管理控制台 并打开 Oracle Database@AWS 控制台，网址为https://console.aws.amazon.com/odb/。
2. 在右上角选择您 AWS 所在的地区。有关更多信息，请参阅 支持的区域 Oracle Database@AWS。
3. 从左侧窗格中选择 ODB 网络。
4. 选择创建 ODB 网络。
5. 在 ODB 网络名称中，输入网络名称。名称必须为 1-255 个字符，并以字母字符或下划线开头。它不能包含连续的连字符。
6. 对于可用区，选择可用区名称。有关支持的内容 AZs，请参阅支持的区域 Oracle Database@AWS。
7. 对于客户端子网 CIDR，请为客户端连接指定 CIDR 范围。有关更多信息，请参阅 ODB 网络的客户端子网 CIDR 要求。

8. 对于 Backup 子网 CIDR，请为备份连接指定 CIDR 范围。为了隔离备份流量并提高弹性，我们建议您不要将备份 CIDR 和客户端 CIDR 重叠。有关更多信息，请参阅 ODB 网络的备份子网 CIDR 要求。
9. 对于 DNS 配置，请选择以下任一选项：

   默认

   在域名前缀中，输入一个用作域名前缀的名称。该域名固定为 orac levcn.com。例如，如果您输入**myhost**，则完全限定的域名为 myhost .oraclevcn.com。

   自定义域名

   在“域名”中，输入完整的域名。例如，你可以输入 myhost.myodb.com。
10. （可选）对于服务集成，请使用VPC Lattice选择要与您的网络集成的服务。Oracle Database@与各种数据库AWS 集成 AWS 服务 ，为您的 Oracle 数据库提供增强的功能和连接选项。选择以下任一集成：

    Amazon S3

    启用对 Amazon S3 的直接 ODB 网络访问。您的数据库可以访问 S3 以进行数据导入/导出或自定义备份。您可以输入 JSON 策略。有关更多信息，请参阅 在 Oracle 数据库中由用户管理的 Amazon S3 备份@AWS。

    零 ETL

    使用 Amazon Redshift 对交易数据启用实时分析和机器学习。有关更多信息，请参阅 Oracle Database@AWS Zero-ETL 与亚马逊 Redshift 集成。

    > **Note**
    >
    > 在创建 ODB 网络时，Oracle Database@AWS 会自动为 Oracle 托管的 Amazon S3 备份预配置网络访问权限。您无法启用或禁用此集成。有关更多信息，请参阅 AWS 服务集成。
11. （可选）在标签中，为网络输入最多 50 个标签。标签是一个键值对，你可以用它来组织和跟踪你的资源。
12. 选择创建 ODB 网络。

创建 ODB 网络后，您可以将其与 VPC 建立对等关系。ODB 对等互连是用户创建的网络连接，它允许在 Amazon VPC 和 ODB 网络之间私下路由流量。对等互连后，VPC 内的 Amazon EC2 实例可以与 ODB 网络中的资源进行通信，就像它们在同一个网络中一样。有关更多信息，请参阅 在 Oracle 数据库中配置与 Amazon VPC 的 ODB 对等连接@AWS。

步骤 2：在中创建 Oracle Exadata 基础架构 Oracle Database@AWS

Oracle Exadata 基础架构是运行 Oracle Exadata 数据库的数据库服务器、存储服务器和网络的底层架构。选择 Exadata X9M 或 X11M 作为系统型号。然后，您可以使用控制台在 Exadata 基础架构上创建虚拟机集群。 AWS

您可以按任一顺序创建 Oracle Exadata 基础架构和 ODB 网络。创建基础架构时，您无需指定网络信息。

创建 Oracle Exadata 基础架构后，您就无法对其进行修改。要删除 Exadata 基础架构，请参阅。在中删除 Oracle Exadata 基础架构 Oracle Database@AWS

创建 Exadata 基础架构

1. 登录 AWS 管理控制台 并打开 Oracle Database@AWS 控制台，网址为https://console.aws.amazon.com/odb/。
2. 从左侧窗格中选择 Exadata 基础架构。
3. 选择创建 Exadata 基础架构。
4. 在 E xadata 基础架构名称中，输入一个名称。名称必须为 1-255 个字符，并以字母字符或下划线开头。它不能包含连续的连字符。
5. 对于可用区，请选择一个支持的可用区 AZs。然后选择下一步。
6. 对于 Exadata 系统型号，请选择 Exadata .X9M 或 Exad ata.X11M。对于 Exadata.X11M，还要选择以下服务器类型：
   - 对于数据库服务器类型，选择 Exadata 基础架构的数据库服务器型号类型。目前，唯一的选择是 X11M。
   - 对于存储服务器类型，选择 Exadata 基础架构的存储服务器型号类型。目前，唯一的选择是 X11M-HC。
7. 对于数据库服务器，保留默认值 2 或移动滑块以选择最多 32 台服务器。要指定超过 2 个，请向 OCI 请求提高限额。

每台 Exadata X9M 数据库服务器支持 126 个。 OCPUs每台 Exadata X11M 数据库服务器都支持 760。 ECPUs服务器数量的变化会随着服务器数量的变化而变化。有关 OCPUs 和的更多信息 ECPUs，请参阅 Oracle 文档中的自治数据库中的计算模型。

8. 对于存储服务器，保留默认值 3 或移动滑块以选择最多 64 台服务器。要指定超过 3 个，请向 OCI 请求提高限额。每台 X9M 存储服务器提供 64 TB 的容量。每台 x11m 存储服务器提供 80 TB 的容量。随着服务器数量的变化，总存储容量 TB 也会发生变化。然后选择下一步。
9. 对于维护窗口，配置何时可以进行系统维护：

   a. 在“日程安排”首选项中，选择以下选项之一：

      - Oracle 管理的时间表-Oracle 确定维护活动的最佳时间。
      - 客户管理的时间表-您可以指定何时可以进行维护活动。

   b. 对于修补模式，请选择以下选项之一：

      - Rolling-一次只对一个节点进行更新，从而允许数据库在修补期间保持可用。
      - 非滚动-更新同时应用于所有节点，这可能需要停机时间。

   c. 如果您选择了客户管理的日程安排，请配置以下其他设置：

      - 对于维护月份，请选择可以执行维护的月份。
      - 对于本月的周，选择可以执行每月哪一周的维护（第一周、第二周、第三周、第四周或最后一周）。
      - 在“一周中的某一天”中，选择可以执行维护的日期（星期一至星期日）。
      - 在“开始时间”中，选择维护时段开始的时间。时间以 UTC 为单位。
      - 对于通知提前期，请选择您希望提前多少天收到有关即将到来的维护的通知。

   > **Note**
   >
   > Oracle 云基础设施在此窗口期间执行系统维护。在维护期间，您的 Exadata 基础架构仍可用，但您可能会遇到短暂的延迟。

10. （可选）对于 OCI 维护通知联系人，最多输入 10 个电子邮件地址。 AWS 将这些电子邮件地址转发给 OCI。更新发生时，OCI 会将通知发送到列出的地址。
11. （可选）在标签中，为基础架构输入最多 50 个标签。标签是一个键值对，你可以用它来组织和跟踪你的资源。
12. 选择下一步并查看您的基础架构设置。

13. 选择创建 Exadata 基础架构。

步骤 3：在中创建 Exadata 虚拟机群集或自治虚拟机群集 Oracle Database@AWS

Exadata 虚拟机集群是一组可以在其 VMs 上创建 Oracle Exadata 数据库的集合。您可以在 Exadata 基础架构上创建虚拟机集群。您可以在同一 ODB 网络中部署具有不同 Oracle Exadata 基础架构的多个虚拟机集群。您对在 Exadata 虚拟机集群上创建的数据库拥有完全的管理控制权。

自治虚拟机集群是预先分配的 Oracle Exadata 计算和存储资源池，在虚拟机级别进行虚拟化，用于运行自治数据库 (ADB)。与您在 Exadata 虚拟机集群上创建的用户管理的数据库不同，自治数据库可以自行调整、自行修补，并由 Oracle 而不是数据库管理员进行管理。

创建虚拟机集群时，请考虑以下限制：

- 您只能将虚拟机群集部署到您创建 ODB 网络和 Oracle Exadata 基础架构的可用区。
- 如果您不跨账户共享虚拟机集群，则该集群必须与 Oracle Exadata 基础架构 AWS 账户 相同。如果您使用 AWS RAM 一个 AWS 账户与可信账户共享 ODB 网络和 Oracle Exadata 基础架构，则该可信账户可以在自己的账户中创建虚拟机集群。
- 您只能在 ODB 网络中部署虚拟机集群。不允许使用其他资源。
- 创建虚拟机集群后，您无法更改存储分配。

> **Important**
>
> 创建过程可能需要 6 个多小时，具体取决于虚拟机集群的大小。

Exadata VM cluster

创建 Exadata 虚拟机集群

1. 登录 AWS 管理控制台 并打开 Oracle Database@AWS 控制台，网址为https://console.aws.amazon.com/odb/。
2. 从左侧窗格中选择 Exadata 虚拟机集群。
3. 选择创建虚拟机集群。

4. 在虚拟机群集名称中，输入一个名称。名称必须为 1-255 个字符，并以字母字符或下划线开头。它不能包含连续的连字符。
5. （可选）在网格基础设施集群名称中，输入与您正在使用的 Oracle 数据库版本相匹配的虚拟机群集的网格基础设施版本。名称必须为 1-11 个字符，并且不能包含连字符。
6. 在 “时区” 中，输入时区。
7. 对于许可证选项，选择 “自带许可证 (BYOL)” 或 “包含许可证”，然后选择 “下一步”。此许可证是 Oracle 提供的 OCI 许可证，而不是由 AWS提供的许可证。
8. 按如下方式配置 Exadata 基础架构设置：

   a. 对于基础架构，请选择以下选项：

      - 在 Exadata 基础架构名称中，选择要用于此虚拟机群集的基础架构。
      - 对于网格基础设施版本，请选择要用于此虚拟机集群的版本。
      - 对于 Exadata 映像版本，请选择要用于此虚拟机集群的版本。我们建议您选择显示的版本，即可用的最高版本。

   b. 对于数据库服务器，请选择一个或多个数据库服务器来托管您的虚拟机群集。

   c. 对于配置，请执行以下操作：

      - 为每个 VM 选择 CPU 核心数、内存和本地存储，或接受默认值。
      - 选择虚拟机集群的 Exadata 存储总量，或接受默认值。

   d. （可选）对于存储空间分配，请选择以下任一选项：

      - 为 Exadata 稀疏快照启用存储分配
      - 为本地备份启用存储分配

      在您选择选项时，可用存储分配会发生变化。您以后无法更改此存储分配。查看您的选择，然后选择 “下一步”。
9. 按如下方式配置连接：

   a. 对于 ODB 网络，请选择现有的 ODB 网络。

   b. 在主机名前缀中，输入虚拟机群集的前缀。确保不要包含域名。前缀构成 Oracle Exadata 虚拟机群集主机名的第一部分。

> **Note**
>
> 主机域名固定为 orac levcn.com。

c. 在 SC AN 侦听器端口 (TCP/IP) 中，输入一个端口号，用于 TCP 访问单个客户机访问名称 (SCAN) 侦听器。默认端口为 1521。或者你可以输入 1024—8999 范围内的自定义扫描端口，不包括以下端口号：248 4、6100、6200、706 0、7070、7070、70 8 5 和 7879。然后选择下一步。

d. 对于 SSH 密钥对，请输入一个或多个密钥对的公钥部分，该密钥对用于 SSH 访问虚拟机集群。然后选择下一步。

10. （可选）按如下方式选择诊断和标签：

a. 选择是否为诊断事件、Health monitor 以及事件日志和跟踪收集启用诊断收集。Oracle 可以使用此诊断信息来识别、跟踪和解决问题。

b. 在标签中，为虚拟机集群输入最多 50 个标签。标签是一个键值对，你可以用它来组织和跟踪你的资源。然后选择下一步。

11. 检视您的设置。然后选择创建虚拟机集群。

Autonomous VM cluster

创建自治虚拟机集群

1. 登录 AWS 管理控制台 并打开 Oracle Database@AWS 控制台，网址为https://console.aws.amazon.com/odb/。
2. 从左侧窗格中，选择自治虚拟机集群。
3. 选择创建自治虚拟机集群。
4. 在虚拟机群集名称中，输入一个名称。名称必须为 1-255 个字符，并以字母字符或下划线开头。它不能包含连续的连字符。
5. 在“时区”中，输入时区。
6. 对于许可证选项，选择“自带许可证 (BYOL)”或“包含许可证”，然后选择“下一步”。此许可证是 Oracle 提供的 OCI 许可证，而不是由 AWS提供的许可证。
7. 按如下方式配置 Exadata 基础架构设置：

a. 在 Exadata 基础架构名称中，选择要用于此自治虚拟机群集的基础架构。

b. 对于数据库服务器，请选择一个或多个数据库服务器来托管您的自治虚拟机群集。

c. 对于配置，请执行以下操作：

- 选择每个 VM 的 ECPU 核心数、每 CPU 的数据库内存、数据库存储空间和自治容器数据库的最大数目或接受默认值。
- 选择自治虚拟机群集的 Exadata 存储总量，或接受默认值。

8. 按如下方式配置连接：

a. 对于 ODB 网络，请选择现有的 ODB 网络。

b. 对于 SCAN 侦听器端口 (TCP/IP)，输入端口（非 TLS）的端口号。默认端口为 1521。或者你可以输入 1024—8999 范围内的端口 (TLS)，不包括以下端口号：2484、6100、6200、7060、7070、7070、7085 和 7879。然后选择下一步。

选择启用双向 TLS (mTLS) 身份验证以允许双向 TLS 身份验证。

9. （可选）按如下方式选择诊断和标签：

a. 选择是将修改配置安排为 Oracle 管理的计划还是客户管理的计划。如果您选择客户管理的时间表，请设置维护月份、每月周数、星期数和开始时间 (UTC)。

b. 在标签中，为自治虚拟机集群输入最多 50 个标签。标签是一个键值对，你可以用它来组织和跟踪你的资源。然后选择下一步。

10. 检视您的设置。然后选择创建自治虚拟机集群。

步骤 4：在 Oracle 云基础设施中创建 Oracle Exadata 数据库

在中 Oracle Database@AWS，您可以使用 AWS 控制台、CLI 或创建和管理以下资源 APIs：

- ODB 网络
- 甲骨文 Exadata 基础架构
- Exadata 虚拟机集群和自治虚拟机集群
- ODB 对等连接

要在您创建的基础架构上创建和管理 Oracle Exadata 数据库，必须使用 Oracle 云基础设施控制台而不是控制面 Oracle Database@AWS 板。您可以在 Exadata 虚拟机集群上创建用户管理的 Exadata 数据库，在自治 Exadata 虚拟机群集上创建自治数据库。有关在 OCI 中创建 Oracle 数据库的信息，请参阅 Oracle 云基础设施文档中的 Exadata 数据库。

创建 Oracle Exadata 数据库

1. 登录 AWS 管理控制台 并打开 Oracle Database@AWS 控制台，网址为https://console.aws.amazon.com/odb/。
2. 在左侧窗格中，选择 Exadata 虚拟机集群或自治虚拟机群集。
3. 选择虚拟机集群以查看详细信息页面。
4. 在 OCI 中选择 “管理”，将重定向到 Oracle 云基础设施控制台。
5. 在 OCI 中创建用户管理的 Exadata 数据库或自治数据库。

在 Oracle 数据库中配置与 Amazon VPC 的 ODB 对等连接@AWS

ODB 对等互连是用户创建的网络连接，它允许在 Amazon VPC 和 ODB 网络之间私下路由流量。VPC 和 ODB 网络之间存在 one-to-one关系。使用控制台、CLI 或 API 创建对等连接后，请务必更新您的 VPC 路由表并配置 DNS 解析。有关 ODB 对等互连的概念性概述，请参阅。ODB 对等互连

在 Oracle 数据库中创建 ODB 对等连接@AWS

通过 ODB 对等连接，您可以在 Oracle Exadata 基础设施和亚马逊上运行的应用程序之间建立私有网络连接。 VPCs每个 ODB 对等连接都是一个单独的资源，您可以独立于 ODB 网络创建、查看和删除该资源。

创建 ODB 对等连接时，您可以指定对等网络 CIDR 范围。这种技术限制了对所需子网的网络访问，减少了潜在的攻击目标，并支持更精细的网络分段以满足合规性要求。

您可以创建以下类型的 ODB 对等连接：

同账户 ODB 对等

您可以在同一个账户中的 ODB 网络和 Amazon VPC 之间创建 ODB 对等连接。 AWS

跨账户 ODB 对等

使用共享 ODB 网络后，您可以在一个账户中的 ODB 网络与另一个账户中的 Amazon VPC 之间创建 ODB 对等连接。 AWS RAM VPC 所有者账户可以管理对等连接中指定的 CIDR 范围，而无需拥有 ODB 网络。

VPC 和 ODB 网络之间存在一对一的关系。您无法在一个 VPC 和多个 ODB 网络之间或一个 ODB 网络与多个 ODB 网络之间创建 ODB 对等连接。 VPCs

控制台

1. 登录 AWS 管理控制台 并打开 Oracle Database@AWS 控制台，网址为https://console.aws.amazon.com/odb/。
2. 在导航窗格中，选择 ODB 对等连接。
3. 选择创建 ODB 对等连接。

4. （可选）对于 ODB 对等名称，请输入连接的唯一名称。
5. 对于 ODB 网络，请选择要对等的 ODB 网络。
6. 对于点对等网络，请选择要与您的 ODB 网络对等的 Amazon VPC。
7. （可选）对于对等网络 CIDRs，请指定来自可以访问 ODB 网络的对等 VPC 的其他 CIDR 块。如果您未指定 CIDRs，则允许所有 CIDRs 来自对等 VPC 的访问权限。
8. （可选）在“标签”中，添加密钥和值对。
9. 选择创建 ODB 对等连接。

创建 ODB 对等连接后，配置您的 Amazon VPC 路由表以将流量路由到对等 ODB 网络。有关更多信息，请参阅 为 ODB 对等互连配置 VPC 路由表。请注意，Oracle Database@AWS 会自动配置 ODB 网络路由表。

AWS CLI

要创建 ODB 对等连接，请使用命令。`create-odb-peering-connection`

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

要将对 ODB 网络的访问限制在特定 CIDR 范围内，请使用参数。`--peer-network-cidrs-to-be-added`如果您未指定 CIDR 范围，则所有范围都有访问权限。

```
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"
```

要列出您的 ODB 对等连接，请使用命令。`list-odb-peering-connections`

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

要获取有关特定 ODB 对等连接的详细信息，请使用命令。`get-odb-peering-connection`

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

更新 ODB 对等连接

您可以更新现有的 ODB 对等连接以添加或删除对等网络。 CIDRs您可以控制对等 VPC 中的哪些子网可以访问您的 ODB 网络。

控制台

1. 登录 AWS 管理控制台 并打开 Oracle Database@AWS 控制台，网址为https://console.aws.amazon.com/odb/。
2. 在导航窗格中，选择 ODB 对等连接。
3. 选择要更新的 ODB 对等连接。
4. 选择 “操作”，然后选择 “更新对等连接”。
5. 在 “对等网络 CIDRs” 部分，根据需要添加或删除 CIDR 块：
   - 要添加 CIDRs，请选择添加 CIDR 并输入 CIDR 块。
   - 要移除 CIDRs，请选择要移除的 CIDR 块旁边的 X。
6. 选择 “更新对等连接”。

AWS CLI

要向 ODB 对等连接添加对等网络 CIDRs ，请在命令`--peer-network-cidrs-to-be-added`中`update-odb-peering-connection`指定参数。

```
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"
```

要 CIDRs 从 ODB 对等连接中删除对等网络，请在命令`--peer-network-cidrs-to-be-removed`中`update-odb-peering-connection`指定参数。

```
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"
```

为 ODB 对等互连配置 VPC 路由表

路由表包含一组被称为路由的规则，决定了来自您的子网或网关的网络流量将指向何处。路由表中的目标 CIDR 是您希望流量到达的 IP 地址范围。如果您指定了 VPC 以便与 ODB 网络的 ODB 对等互连，

请使用 ODB 网络中的目标 IP 范围更新您的 VPC 路由表。有关 ODB 对等的更多信息，请参阅。ODB 对等互连

要更新路由表，请使用 AWS CLI `ec2 create-route`命令。以下示例更新了 Amazon VPC 路由表。有关更多信息，请参阅 为 ODB 对等互连配置 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 网络路由表会使用 VPC CIDRs 自动更新。要仅允许特定子网 CIDRs 而不是 VPC CIDRs 中的所有子网访问 ODB 网络，您可以在创建 ODB 对等连接 CIDRs 时指定对等网络，或者更新现有 ODB 对等连接以添加或删除对等 CIDR 范围。有关更多信息，请参阅在 Oracle 数据库中创建 ODB 对等连接 @AWS和更新 ODB 对等连接。

有关 VPC 路由表的更多信息，请参阅 Amazon Virtual Private Cloud 用户指南中的子网路由表和《AWS CLI 命令参考》中的 ec2 create- route。

配置 DNS Oracle Database@AWS

Amazon Route 53 是一项高度可用且可扩展的域名系统 (DNS) 网络服务，您可以将其用于 DNS 路由。在您的 ODB 网络和 VPC 之间创建 ODB 对等连接时，您需要一种机制来解析来自 VPC 内部的 ODB 网络资源的 DNS 查询。您可以使用 Amazon Route 53 配置以下资源：

- 出站终端节点

  需要使用终端节点才能向 ODB 网络发送 DNS 查询。
- 解析器规则

  此规则指定了 Route 53 解析器转发给 ODB 网络的 DNS 的 DNS 查询的域名。

DNS 的工作原理 Oracle Database@AWS

Oracle Database@AWS 自动管理 ODB 网络的域名系统 (DNS) 配置。对于域名，您可以为默认域名指定自定义前缀，也可以指定完全自定义的域名。`oraclevcn.com`有关更多信息，请参阅 步骤 1：在中创建 ODB 网络 Oracle Database@AWS。

置 Oracle Database@AWS 备 ODB 网络时，它会创建以下资源：

- 与 ODB 网络具有相同的 CIDR 块的 Oracle 云基础架构 (OCI) 虚拟云网络 (VCN)

  此 VCN 位于客户的关联 OCI 租赁中。ODB 网络和 OCI VCN 之间有 1:1 的映射。每个 ODB 网络都与 OCI VCN 相关联。
- OCI VCN 中的私有 DNS 解析器

  此 DNS 解析器处理 OCI VCN 中的 DNS 查询。OCI 自动化会为虚拟机集群创建记录。扫描使用`*.oraclevcn.com`完全限定域名 (FQDN)。
- OCI VCN 中专用 DNS 解析器的 DNS 监听端点

  您可以在 Oracle Database@AWS 控制台的 ODB 网络详细信息页面中找到 DNS 侦听端点。

在 ODB 网络中配置出站终端节点 Oracle Database@AWS

出站终端节点允许将 DNS 查询从您的 VPC 发送到网络或 IP 地址。端点指定查询来源的 IP 地址。要将 DNS 查询从您的 VPC 转发到您的 ODB 网络，请使用 Route 53 控制台创建出站终端节点。有关更多信息，请参阅将出站 DNS 查询转发到您的网络。

在 ODB 网络中配置出站终端节点

1. 登录 AWS 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 从左侧窗格中，选择出站终端节点。
3. 在导航栏上，为要创建出站终端节点的 VPC 选择区域。
4. 选择 Create outbound endpoint (创建出站端点)。
5. 按如下方式填写出站终端节点的常规设置部分：

   a. 选择一个允许出站 TCP 和 UDP 连接到以下内容的安全组：

      - 解析器在您的 ODB 网络上进行 DNS 查询时使用的 IP 地址
      - 解析器在您的 ODB 网络上用于 DNS 查询的端口

   b. 为终端节点类型选择 IPv4。

   c. 对于此端点的协议，请选择 Do53。
6. 在 IP 地址中，提供以下信息：

   - 要么指定 IP 地址，要么让 Route 53 解析器从子网中的可用地址中为您选择 IP 地址。选择 2 个至多 6 个 IP 地址进行 DNS 查询。我们建议您至少在两个不同的可用区中选择 IP 地址。

- 对于子网，请选择具有以下内容的子网：
  - 包含指向 ODB 网络上 DNS 侦听器 IP 地址的路由的路由表
  - 网络访问控制列表 (ACLs)，允许 UDP 和 TCP 流量到解析器在 ODB 网络上进行 DNS 查询时使用的 IP 地址和端口
  - 允许来自目标端口范围为 1024-65535 的解析器的流量的网络 ACLs

7. （可选）在“标签”中，为终端节点指定标签。
8. 选择提交。

在中配置解析器规则 Oracle Database@AWS

解析器规则是一组确定如何路由 DNS 查询的标准。要么重复使用，要么创建一个规则，指定解析器转发给 ODB 网络的 DNS 的 DNS 查询的域名。

使用现有的解析器规则

要使用现有的解析器规则，您的操作取决于规则的类型：

适用于与您的 VPC 位于相同 AWS 区域的相同域的规则 AWS 账户

将规则与您的 VPC 关联，而不是创建新规则。从规则控制面板中选择规则，并将其与该 VPCs AWS 地区的适用规则相关联。

适用于与您的 VPC 位于相同区域但账户不同的域的规则

用于 AWS Resource Access Manager 将远程账户中的规则共享到您的账户。共享规则时，您还会共享相应的出站终端节点。与您的账户共享规则后，从规则控制面板中选择该规则，然后将其与您账户 VPCs 中的相关联。有关更多信息，请参阅管理转发规则。

创建新的解析器规则

如果您无法重复使用现有的解析器规则，请使用 Amazon Route 53 控制台创建新规则。

创建新的解析器规则

1. 登录 AWS 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 从左侧窗格中选择“规则”。
3. 在导航栏上，为出站终端节点所在的 VPC 选择区域。

4. 选择 Create rule（创建规则）。
5. 按如下方式填写“出站流量规则”部分：
   a. 对于规则类型，选择转发规则。
   b. 在“域名”中，指定 ODB 网络中的完整域名。
   c. 为VPCs 此，请使用此规则，将其与 DNS 查询从中转发到您的 ODB 网络的 VPC 相关联。
   d. 对于出站终端节点，请选择您在中创建的出站终端节点[在 ODB 网络中配置出站终端节点 Oracle Database@AWS]。

      > **Note**
      > 与此规则关联的 VPC 不必与您在其中创建出站终端节点的 VPC 相同。

6. 按如下方式填写“目标 IP 地址”部分：
   a. 对于 IP 地址，请指定 ODB 网络上的 DNS 侦听器 IP 的 IP 地址。
   b. 对于“端口”，指定 53。这是解析器用于 DNS 查询的端口。

      > **Note**
      > Route 53 解析器将匹配此规则且来自与此规则关联的 VPC 的 DNS 查询转发到引用的出站终端节点。这些查询会转发到您在目标 IP 地址中指定的目标 IP 地址。

   c. 对于传输协议，请选择 Do53。
7. （可选）在“标签”中，为规则指定标签。
8. 选择提交。

在中测试您的 DNS 配置 Oracle Database@AWS

创建出站终端节点和解析器规则后，请进行测试以确保 DNS 解析正确。使用应用程序 VPC 中的 Amazon EC2 实例，按如下方式执行 DNS 解析：

适用于 Linux 或 macOS

使用表单命令`dig` *`record-name record-type`*。

对于 Windows：

使用表单命令`nslookup -type=`*`record-name record-type`*。

配置 Amazon VPC 中转网关 Oracle Database@AWS

Amazon VPC Transit Gateways 是一个网络传输中心，可将虚拟私有云 (VPCs) 和本地网络互连。hub-and-spoke架构中的每个 VPC 都可以连接到传输网关，从而访问其他连接的 VPC VPCs。 AWS Transit Gateway 支持 IPv4 和的流量 IPv6。

在中 Oracle Database@AWS，ODB 网络仅支持与一个 VPC 的对等连接。如果您将传输网关连接到与 ODB 网络对等的 VPC，则可以将多个传输网关 VPCs 连接到该网关。在这些不同环境中运行的应用程序 VPCs 可以访问在您的 ODB 网络中运行的 Exadata 虚拟机集群。

下图显示了连接到两个 VPCs 和一个本地网络的传输网关。

在上图中，一个 VPC 与 ODB 网络建立对等关系。在此配置中，ODB 网络可以将流量路由到所有 VPCs 连接到传输网关的网络。每个 VPC 的路由表包括本地路由和将发往 ODB 网络的流量发送到中转网关的路由。

在中 AWS Transit Gateway，您需要为每小时与公交网关建立的连接次数和流经的流量付费 AWS Transit Gateway。有关费用信息，请参阅AWS Transit Gateway 定价。

要求

确保您的 Oracle Database@AWS 环境满足以下要求：

- 与您的 ODB 网络对等的 VPC 必须位于相同的 VPC 中。 AWS 账户如果对等互连 VPC 的账户与 ODB 网络不同，则无论共享配置如何，传输网关连接都会失败。
- 与您的 ODB 网络对等的 VPC 必须具有传输网关连接。

> **Note**
>
> 如果将传输网关配置为共享，则它可以驻留在任何账户中。因此，网关本身不必与 VPC 和 ODB 网络位于同一个账户中。

- 传输网关连接必须与 ODB 网络位于同一个可用区 (AZ) 中。

限制

请注意 Amazon VPC 传输网关在以下方面的限制 Oracle Database@AWS：

- Amazon VPC Transit Gateways 不提供将 ODB 网络用作附件的原生集成。因此，诸如以下的 VPC 功能不可用：
  - 将公有 DNS 主机名解析为私有 IP 地址
  - ODB 网络拓扑、路由和连接状态变化的事件通知
- 不支持到 ODB 网络的多播流量。

设置和配置传输网关

您可以使用 Amazon VPC 控制台或`aws ec2`命令创建和配置传输网关。以下过程假设您中没有与 VPC 对等的 ODB 网络。 AWS 账户如果您的账户中已有 ODB 网络和 VPC 对等，请跳过步骤 1-3。

> **Note**
>
> 如果您在 VPC 上连接或重新连接附件，请确保重新输入 ODB ODB 网络的 CIDR 范围。

为以下目的设置和配置传输网关 Oracle Database@AWS

1. 创建 ODB 网络。有关更多信息，请参阅 步骤 1：在中创建 ODB 网络 Oracle Database@AWS。
2. 使用包含 ODB 网络的相同账户创建 VPC。有关更多信息，请参阅 Amazon VPC 用户指南中的创建 VPC。
3. 在您的 ODB 网络和 VPC 之间创建 ODB 对等连接。有关更多信息，请参阅 在 Oracle 数据库中配置与 Amazon VPC 的 ODB 对等连接@AWS。
4. 按照开始使用 Amazon VPC 传输网关中的步骤设置传输网关。网关必须与 ODB 网络和 VPC 处于 AWS 账户 相同状态，或者由其他账户共享。

   > **Important**
   >
   > 在 ODB 网络所在的可用区中创建传输网关附件。

5. 将 CIDR 范围添加到您计划连接到核心网络的 ODB 网络 VPCs 和本地网络。有关更多信息，请参阅 更新中的 ODB 网络 Oracle Database@AWS。

   如果您使用的是 CLI，请`update-odb-network`使用`--peered-cidrs-to-be-added`和运行命令`--peered-cidrs-to-be-removed`。有关更多信息，请参阅 AWS CLI 命令参考。

为以下 AWS 各项配置云 WAN Oracle Database@AWS

AWS 云广域网是一项托管广域网 (WAN) 服务。您可以使用 AWS Cloud WAN 来构建、管理和监控统一的全球网络，该网络连接在云端和本地环境中运行的资源。

在 AWS Cloud WAN 中，全球网络是一个单独的私有网络，它充当网络对象的高级容器。核心网络是您的全球网络中由管理的部分 AWS。

AWS 云广域网具有以下主要优势：

- 集中式网络管理，可简化操作，同时维护多个区域的安全
- 具有内置分段功能的核心网络，可隔离通过多个路由域的流量
- Support 支持策略以实现网络管理的自动化，并在您的全球网络中定义一致的配置

在 Oracle Database@ 中AWS，ODB 网络仅支持与一个 VPC 建立对等关系。如果您将 AWS Cloud WAN 核心网络连接到对等 VPC，则它会启用全球流量路由。 VPCs 跨多个区域连接的应用程序可以访问您的 ODB 网络中的 Exadata 虚拟机集群。您可以将 ODB 网络流量隔离在自己的分段中，也可以允许访问其他分段。

下图显示了连接到三个 VPCs 和一个本地网络的 AWS Cloud WAN 核心网络。

AWS Cloud WAN 不提供将 ODB 网络用作附件的原生集成。因此，诸如以下的 VPC 功能不可用：

- 将公有 DNS 主机名解析为私有 IP 地址
- ODB 网络拓扑、路由和连接状态变化的事件通知

在 AWS Cloud WAN 中，以下各项按小时收费：

- 区域数量（核心网络边缘）
- 核心网络连接数量
- 通过附件流经核心网络的流量量

有关详细定价信息，请参阅 AWS Cloud WAN 定价。

为配置核心网络 Oracle Database@AWS

1. 将 CIDR 范围添加到您计划连接到核心网络的 ODB 网络 VPCs 和本地网络。有关更多信息，请参阅 更新中的 ODB 网络 Oracle Database@AWS。

   > **Note**
   >
   > 如果您在 VPC 上连接或重新连接附件，请确保重新输入 ODB ODB 网络的 CIDR 范围。

2. 按照创建 AWS Cloud WAN 全球网络和核心网络中的步骤操作。

在 Oracle 数据库中共享权利@AWS

使用 Oracle Database@AWS，您可以在同一个组织 AWS 账户 中共享 Oracle Database@AWS 的 AWS Marketplace 权限。 AWS 这允许其他账户使用您的订阅配置自己的 Oracle Exadata 基础架构和 ODB 网络资源。

共享方法

Oracle 数据库 @AWS 支持两种共享方法：

与 L AWS icense Manager 共享权限

- 允许其他账户配置自己的 Oracle Exadata 基础架构和 ODB 网络资源
- 每个账户都独立运行，完全控制资源生命周期
- 最适合跨团队或业务部门实现自助配置

与 AWS Resource Access Manager (AWS RAM) 共享资源

- 共享已配置的 Oracle Exadata 基础架构和 ODB 网络资源
- 集中管理基础架构，同时允许收款人账户创建虚拟机集群
- 让多个账户使用同一个基础架构，从而优化成本

您可以根据组织需求同时使用两种共享方法。

Oracle Database@ 权限共享AWS 的限制

共享 Oracle Database@AWS 授权时，请记住以下限制：

- 您只能在 AWS 组织 AWS 账户 内部与他人共享
- 您不能与整个组织单位 (OU) 或整个组织共享
- 一个账户只能从一个买家账户获得权利（来自一个私人报价）
- 一个买家账户不能与其他买家账户共享权利
- 收件人帐户必须先初始化 Oracle Database@AWS 服务，然后才能使用共享授权
- 权利授予操作只能在美国东部（弗吉尼亚北部）地区执行

跨账户共享 Oracle Database@AWS 权限

要在优化成本的同时实现协作，请与同一 AWS 组织 AWS 账户 内的其他人共享 Oracle Database@AWS 权限。本主题介绍如何使用 License Manager 共享 AWS 授权。

共享权利的先决条件

在共享 Oracle Database@AWS 授权之前，请确保您具备以下条件：

- 有效的 Oracle Database@AWS 订阅（您必须是通过以下方式接受私募报价的买家账户） AWS Marketplace
- 组织中您想要与之共享权利的 AWS 账户 IDs
- 授予者和被授权者使用 AWS License Manager 资源和操作的必要权限（有关更多信息，请参阅《许可证管理器用户指南》AWS 中的 License Manager 身份和访问管理）
- 下面列出了您（授予者）和权利接收者（被授权者）的权限

权限共享所需的权限

除了 L AWS icense Manager 权限外，Oracle Database@ 还AWS 需要以下权限：

授予者权限

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

被授予者权限

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

使用 AWS License Manager 与其他账户共享 Oracle Database@AWS 权限

要与其他 AWS 账户共享授权，请使用 License Manager 创建授 AWS 权。有关更多信息，请参阅《许可证管理器用户指南》中的 “分发AWS许可证管理器授权”。

创建赠款后，接受者（被授权者）必须：

- 接受并激活授权。有关更多信息，请参阅《许可证管理器用户指南》中的 License Manager 中的 AWS 授权接受和激活。
- 按照 Oracle 数据库 AWS@ 的初始化说明进行操作。

初始化完成后，被授权者可以使用共享授权配置 Oracle Database@AWS 资源。

在 Oracle 数据库中共享资源@AWS

使用 Oracle Database@AWS，您可以在同一个组织中的多个 AWS 账户 组织之间共享 Exadata 基础架构和您的 ODB 网络。 AWS 这样，您只需预置一次基础设施即可在多个受信任账户中重复使用，从而在分离职责的同时降低成本。

共享资源时：

- 拥有资源的账户（所有者账户）保持对资源生命周期的控制。
- 获得共享资源访问权限的账户（可信账户）可以根据授予的权限查看和使用这些资源。
- 可信账户可以在共享基础架构上创建自己的资源，但不能删除底层共享资源。

Oracle Database@AWS 与 AWS RAM

Oracle Database@AWS 使用 AWS Resource Access Manager (AWS RAM) 实现跨账户安全、受控的资源共享。借助 AWS RAM，您可以安全地在同一 AWS 组织内的多个 AWS 账户之间共享您的 Oracle Database@AWS 资源。 AWS RAM 简化了资源共享，减少了运营开销，并提供了共享的 Oracle Database@AWS 资源的安全性和可见性。

使用 AWS RAM，您可以通过创建资源共享来共享您拥有的资源。资源共享指定要共享的资源以及 AWS 账户 与谁共享这些资源。

在 Oracle 数据库中共享资源的优势@AWS

跨账户共享 Oracle Database@AWS 资源具有以下好处：

- 成本优化 — 通过管理帐户一次配置昂贵的 Exadata 基础架构，然后与多个账户共享，从而降低总体成本。
- 职责分工 — 在允许协作的同时，保持基础架构管理员和数据库用户之间的明确界限。
- 简化管理-集中管理基础架构，同时支持分布式数据库操作。
- 一致的治理-对共享资源应用一致的策略和控制。

例如，管理员可以在其中配置 Oracle Exadata 基础架构和 ODB 网络， AWS 账户 并与开发者账户共享。然后，开发人员可以在此共享基础架构上创建虚拟机集群，而无需自己配置昂贵的硬件。这种方法可以显著降低成本，同时保持账户之间的适当责任分工。

资源共享在 Oracle 数据库中的工作原理@AWS

您可以共享以下 Oracle Database@ 资源AWS ：

- 甲骨文 Exadata 基础架构
- ODB 网络

Oracle Database@ 通过以下过程AWS 共享上述资源：

1. 买方账户（通过 M AWS arketplace 接受 Oracle Database@AWS 私募报价的账户）会配置 Oracle Database@AWS 资源，例如 Exadata 基础设施和 ODB 网络。
2. 买方账户使用创建资源共享 AWS RAM，指定要共享的资源以及要与之共享的受信任账户。
3. 系统会自动接受同一组织内可信账户的资源共享。
4. 在使用共享资源之前，可信账户必须使用`aws odb initialize-service`命令或在 Oracle Database@ 控制台中选择 “激活帐户”，在其账户中初始化 Oracle Datab AWS ase@AWS 服务。
5. 初始化后，可信账户可以在共享基础架构上创建自己的资源，例如共享 Exadata 基础架构和 ODB 网络上的虚拟机群集。

可信账户共享资源的权限

共享资源时，Oracle Database@AWS 会自动为每种资源类型选择特定的操作（托管权限）：

适用于 Exadata 基础架构

Oracle Database@AWS 向可信账户授予以下权限：

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

适用于 ODB 网络

向可信账户授予以下权限：

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

资源共享尊重 Oracle Database@AWS 资源的分层特性。例如，如果您共享 Exadata 基础架构，则可信账户可以在此基础架构上创建虚拟机集群，但他们无法修改或删除 Exadata 基础架构本身。

当资源被取消共享时，可信账户将失去在共享基础架构上创建新资源的能力。但是，他们已经创建的任何资源仍然可以访问且可以正常使用。

Oracle Database@ 资源共享AWS 的限制

在共享资源之前，请记住以下限制。

共享资源的限制

共享 Oracle Database@AWS 资源时，请记住以下限制：

- 您只能与共享资源 AWS 账户 IDs。
- 您只能在同一个 AWS 组织 AWS 账户 内共享资源。
- 您在特定 AWS 区域内共享资源。要跨区域共享资源，您必须在每个区域中创建单独的资源共享。
- 创建资源共享时，会自动选择每种资源类型的操作（托管权限），且无法修改。
- 您不能使用 Oracle Database@AWS 作为资源并与其他人共享。 AWS 账户
- 一个可信账户只能使用来自一个买家账户（来自一个私人报价）的共享资源。因此，两个买家账户不能与同一个可信账户共享资源。
- 一个买家账户不能与其他买家账户共享资源。
- 与可信账户共享的资源必须首先由买家所在地区的买家账户共享。
- 取消共享资源时，我们建议您等待大约 15 分钟，然后再与同一个可信账户重新共享同一资源。

创建和使用共享资源的限制

创建或使用 Oracle Database@AWS 资源时，请记住以下限制：

- 只有买家账户才能创建 Exadata 基础设施和 ODB 网络资源。买方账户是接受 Oracle Database@AWS 私募报价的账户。
- 可信账户只能在买方账户共享的 Exadata 基础架构上创建资源。
- 可信账户必须在其账户中初始化 Oracle Database@AWS 服务，然后才能使用共享资源。

删除共享资源的限制

- 在移除虚拟机集群之前，您无法删除由可信账户创建的虚拟机群集的 Exadata 基础架构。
- 在移除 ODB 对等连接之前，您无法删除具有由可信帐户创建的 ODB 对等连接的 ODB 网络。
- 买方账户无法删除由可信账户创建的 Oracle Database@AWS 资源。
- 可信账户可以查看共享资源，但不能修改或删除买方账户拥有的 Oracle Database@AWS 资源。

跨账号共享 Oracle Database@AWS 资源

要在优化成本的同时实现协作，请与同一 AWS 组织 AWS 账户 内的其他人共享 Oracle Database@AWS 资源。本主题介绍如何使用 AWS Resource Access Manager (AWS RAM) 共享资源。

主题

- 共享资源的先决条件
- 使用与其他账户共享 Oracle Database@AWS 资源 AWS RAM
- 查看您的资源共享
- 使用更新或删除资源共享 AWS RAM

共享资源的先决条件

在共享 Oracle Database@AWS 资源之前，请确保您具备以下条件：

- 有效的 Oracle Database@AWS 订阅（您必须是通过以下方式接受私募报价的买家账户） AWS Marketplace

- 您要共享的资源的 IDs 或名称，例如 Exadata 基础架构或 ODB 网络
- 组织中您想要与之共享资源的 AWS 账户 IDs
- 在中创建资源共享所需的权限 AWS RAM
- AWS Organizations 使用共享资源的功能 AWS RAM （有关更多信息，请参阅《AWS Resource Access Manager 用户指南》 AWS Organizations中的 “启用资源共享”）

使用与其他账户共享 Oracle Database@AWS 资源 AWS RAM

要与其他 AWS 账户共享 Exadata 基础架构或 ODB 网络，请使用创建资源共享。 AWS RAM这允许可信账户在您的 Exadata 基础架构上创建虚拟机集群。

控制台

1. 打开 AWS RAM 控制台，网址为https://console.aws.amazon.com/ram/。
2. 选择创建资源共享。
3. 在名称中，输入资源共享的描述性名称。
4. 在 “选择资源类型” 下，显示以下任一资源：
   - Oracle Database@AWS ODB 网络
   - Oracle 数据库 @ Exadata 基础架构AWS
5. 选择要共享的 Exadata 基础架构资源。选择 “下一步”，直到进入向委托人授予访问权限。
6. 在 “委托人” 下 AWS 账户，选择，然后输入 IDs 您要与之共享的 AWS 账户。
7. 在托管权限下，选择以下权限以允许可信账户在共享的 Exadata 基础架构上创建虚拟机集群：
   - AWSRAMDefault许可ODBNetwork
   - AWSRAMDefault许可ODBCloudExadataInfrastructure
8. 选择创建资源共享。

AWS CLI

要使用共享资源 AWS CLI，请使用`aws ram create-resource-share`命令。以下示例创建一个名为的资源共享`ExadataInfraShare`，该共享与账户 222222222222 共享指定的 Exadata 基础架构，从而允许该账户在共享基础架构上创建虚拟机群集。

```
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
```

查看您的资源共享

要查看您共享的资源以及与之共享的账户，请执行以下操作：

控制台

1. 打开 AWS RAM 控制台，网址为https://console.aws.amazon.com/ram/。
2. 选择共享资源以查看您与其他账户共享的资源。
3. 选择一个资源共享以查看其详细信息，包括共享的资源和与之共享的委托人。

AWS CLI

要使用查看您的资源共享 AWS CLI，请使用以下get-resource-shares命令：

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

要查看特定资源共享中的资源，请使用以下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
```

要查看与之共享资源共享的委托人（账户），请使用以下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
```

使用更新或删除资源共享 AWS RAM

要停止使用与可信账户共享资源 AWS RAM，请执行以下任一操作：

- 从资源共享中移除资源。
- 从资源共享中移除可信账户。

- 删除资源共享。

在撤消对共享资源的访问权限或删除共享资源之前，请考虑以下影响：

- 可信账户无法再在非共享基础架构上创建新资源。
- 由可信账户在共享 Exadata 基础架构上创建的现有资源继续发挥作用并可供这些用户访问。 AWS 账户
- 在移除虚拟机集群之前，您无法删除由可信账户创建的虚拟机群集的 Exadata 基础架构。

在取消共享资源之前，我们建议您与可信账户进行协调，以确保平稳过渡。

有关更多信息，请参阅《AWS Resource Access Manager 用户指南》中的 “更新资源共享” AWS RAM 和 “删除资源共享”。 AWS RAM

在可信账户 Oracle Database@AWS 中初始化

可信账户是 AWS 账户 指您指定有资格接收资源共享的账户。必须是您 AWS 组织 AWS 账户 中的另一个人。必须先初始化该服务，然后才能在可信账户中使用共享的 Oracle Database@AWS 资源。初始化会创建必要的元数据，并在您 AWS 账户 和 Oracle 云基础设施之间建立连接。

主题

- 什么是 Oracle Database@ 初始化AWS ？
- 后续步骤

什么是 Oracle Database@ 初始化AWS ？

与您的账户共享资源后，必须先初始化 Oracle Database@AWS 服务，然后才能访问或使用该共享资源。如果您在未先初始化服务的AWS APIs 情况下尝试使用 Oracle Database@，则会收到错误消息。

初始化是一个一次性的过程。它会创建必要的元数据，并在您 AWS 账户 和 Oracle 云基础设施之间建立连接。

您可以使用 AWS 管理控制台或初始化服务 AWS CLI。

控制台

1. 打开 Oracle Database@AWS 控制台，网址为。https://console.aws.amazon.com/odb/

2. 如果这是您首次使用此账户访问 Oracle Database@AWS 控制台，则会看到一个欢迎页面。
3. 选择 “激活账户”。
4. 服务初始化过程开始。此过程可能需要几分钟才能完成。
5. 定期刷新欢迎页面，直到 “激活账户” 按钮变为 “控制面板” 按钮。
6. 选择 “控制面板” 开始使用 Oracle 数据库 @AWS。

AWS CLI

要使用AWS 在您的可信账户中初始化 Oracle Database@ AWS CLI，请使用命令。`initialize-service`

```
aws odb initialize-service
```

要检查初始化状态，请使用`get-oci-onboarding-status`命令。

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

初始化完成后，输出显示状态为`ACTIVE_LIMITED`，表示您的账户可以访问共享资源，但无法创建新的 Exadata 基础架构或 ODB 网络。

后续步骤

在您的可信账户AWS 中初始化 Oracle Database@ 之后，您可以执行以下操作：

- 使用`list`和`get`命令或在 AWS 控制台中查看共享资源。
- 在共享的 Exadata 基础架构和 ODB 网络上创建虚拟机群集和自治虚拟机群集。
- 在共享 ODB 网络上创建 ODB 对等连接。

有关使用共享资源的更多信息，请参阅使用可信账户中的共享 Oracle Database@AWS 资源。

使用可信账户中的共享 Oracle Database@AWS 资源

在与您的可信账户共享资源并初始化 Oracle Database@AWS 服务后，您可以查看和使用该共享资源。本主题介绍如何使用可信账户中的共享资源。

主题

- 可信账户中共享资源的限制
- 在共享的 Exadata 基础架构上创建虚拟机集群
- 查看可信账户中的共享资源
- 设置与共享 ODB 网络的 ODB 对等互连

可信账户中共享资源的限制

使用共享的 Oracle Database@AWS 资源时，请注意以下限制：

- 仅在同一 AWS 组织内支持资源共享。
- 只有买方账户（接受 Oracle Database@AWS 私人报价的账户）才能创建 Exadata 基础架构和 ODB 网络资源。
- 您只能在共享基础架构上创建资源，并且必须具有必要的权限。
- 每种资源类型的特定操作（托管权限）都是在创建资源共享时自动选择的，并且无法修改。
- 您无法修改或删除其他账户拥有的资源。
- 您在共享基础架构上创建的资源归您的账户所有，并计入您的 OCI 配额。这同样适用于父资源。
- 如果所有者账户取消共享资源，则您将无法再在此共享基础架构上创建新资源。但是，您的现有资源可以继续运行。
- 不支持跨区域资源共享。您只能在同一 AWS 区域内共享资源。
- 可信账户资源向 Oracle Database AWS @ 订阅的购买者计费。
- 使用共享资源时，必须提供 Amazon 资源名称 (ARN)。

在共享的 Exadata 基础架构上创建虚拟机集群

如果您的可信账户可以访问共享的 Exadata 基础架构和 ODB 网络，则可以在此基础架构上创建 Exadata 虚拟机群集、自治虚拟机群集或 ODB 对等。

> **Note**
>
> 使用与您共享的资源时，您必须指定 Amazon 资源名称 (ARN)，而不仅仅是指定资源 ID。

控制台

1. 打开 Oracle Database@AWS 控制台，网址为。https://console.aws.amazon.com/odb/

2. 在导航窗格中，选择 Exadata 虚拟机集群或自治虚拟机集群。
3. 选择创建虚拟机集群或创建自治虚拟机集群。
4. 对于 Exadata 基础架构，请选择要在其上创建虚拟机集群的共享 Exadata 基础架构。
5. 根据需要填写虚拟机集群配置的其余字段。
6. 选择创建虚拟机集群或创建自治虚拟机集群。

AWS CLI

要使用在共享 Exadata 基础架构上创建虚拟机集群 AWS CLI，请使用以下`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..." \
```

要使用在共享 Exadata 基础架构上创建自治虚拟机群集 AWS CLI，请使用以下`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
```

虚拟机集群在指定的共享 Exadata 基础架构上创建，归您的可信账户所有。

查看可信账户中的共享资源

您可以使用 AWS 管理控制台或查看与您的账户共享的资源 AWS CLI。

控制台

1. 打开 Oracle Database@AWS 控制台，网址为。https://console.aws.amazon.com/odb/
2. 在导航窗格中，选择要查看的资源类型：Exadata 基础架构或 OD B 网络。
3. 控制台显示与您共享的资源。
4. 选择共享资源以查看其详细信息。

AWS CLI

要使用查看共享资源 AWS CLI，请使用与资源类型对应的`list`命令。例如，要列出 Exadata 基础架构，请执行以下操作：

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

响应中显示了与您共享的资源。

要获取有关特定共享资源的详细信息，请使用带有资源 ID 的相应`get`命令：

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

设置与共享 ODB 网络的 ODB 对等互连

要在共享 ODB 网络上实现应用程序和数据库之间的通信，您可以在 VPC 和共享 ODB 网络之间设置 ODB 对等关系。有关 ODB 对等的更多信息，请参阅。在 Oracle 数据库中创建 ODB 对等连接@AWS

控制台

1. 打开 Oracle Database@AWS 控制台，网址为。https://console.aws.amazon.com/odb/
2. 在导航窗格中，选择 ODB 对等。
3. 选择 “创建 ODB 网络对等”。
4. 对于 ODB 网络，请选择要与之建立对等关系的共享 ODB 网络。
5. 对于对等网络，请选择您的 VPC。
6. 选择 “创建 ODB 网络对等”。

AWS CLI

要使用在您的 VPC 和共享 ODB 网络之间创建网络对等连接 AWS CLI，请使用命令。`create-odb-peering-connection`

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

创建对等连接后，更新您的路由表以启用对等互连网络之间的流量。

```
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 数据库@AWS

在创建某些 Oracle Database@AWS 资源之后，您可以对其进行修改和删除。

更新中的 ODB 网络 Oracle Database@AWS

您可以更新以下 ODB 网络资源：

- ODB 网络名称
- 用于建立与 ODB 网络的 ODB 对等连接的 Amazon VPC
- 可以访问 ODB 网络中的 Exadata 资源的 VPC 网段范围

> **Note**
>
> 通过指定 CIDR 范围，您可以限制与必要 VPC 子网的连接，而不是让整个 VPC 可用于 ODB 网络。

本节假设您已经在中创建了 ODB 网络。步骤 1：在中创建 ODB 网络 Oracle Database@AWS

更新 ODB 网络

1. 登录 AWS 管理控制台 并打开 Oracle Database@AWS 控制台，网址为https://console.aws.amazon.com/odb/。
2. 从左侧窗格中选择 ODB 网络。
3. 选择要修改的网络。
4. 选择 Modify(修改)。
5. （可选）在 ODB 网络名称中，输入新的网络名称。名称必须为 1-255 个字符，并以字母字符或下划线开头。它不能包含连续的连字符。
6. （可选）对于对等连接 CIDRs，请指定需要连接到 ODB 网络的对等 VPC 的 CIDR 范围。要限制访问权限，我们建议您指定所需的最低 CIDR 范围。
7. （可选）对于配置服务集成，请选择或取消选择 Amazon S3 或零 ETL。
8. 选择 “继续”，然后选择 “修改”。

在中删除 ODB 网络 Oracle Database@AWS

您可以删除 ODB 网络。本节假设您已经在中创建了 ODB 网络。步骤 1：在中创建 ODB 网络 Oracle Database@AWS您无法删除虚拟机集群当前正在使用的 ODB 网络。

删除 ODB 网络

1. 登录 AWS 管理控制台 并打开 Oracle Database@AWS 控制台，网址为https://console.aws.amazon.com/odb/。
2. 从左侧窗格中选择 ODB 网络。
3. 选择要删除的网络。
4. 选择删除。
5. （可选）选择删除关联的 OCI 资源以删除与 ODB 网络一起创建的 OCI 资源。
6. 在文本框中输入 **`delete me`**。
7. 选择删除。

删除中的虚拟机集群 Oracle Database@AWS

您可以删除 Exadata 虚拟机群集或自治虚拟机群集。本节假设您已经在中创建了一个虚拟机集群步骤 3：在中创建 Exadata 虚拟机群集或自治虚拟机群集 Oracle Database@AWS。

删除虚拟机集群

1. 登录 AWS 管理控制台 并打开 Oracle Database@AWS 控制台，网址为https://console.aws.amazon.com/odb/。
2. 在左侧窗格中，选择 Exadata 虚拟机集群或自治虚拟机群集。
3. 选择要删除的虚拟机集群。
4. 选择删除。
5. 出现提示时，输入，**`delete me`**然后选择 “删除”。

在中删除 Oracle Exadata 基础架构 Oracle Database@AWS

您可以删除 Oracle Exadata 基础架构。本节假设您已经在中创建了 Oracle Exadata 基础架构。步骤 2：在中创建 Oracle Exadata 基础架构 Oracle Database@AWS您无法删除虚拟机集群当前正在使用的 Exadata 基础架构。

删除 Oracle Exadata 基础架构

1. 登录 AWS 管理控制台 并打开 Oracle Database@AWS 控制台，网址为https://console.aws.amazon.com/odb/。
2. 从左侧窗格中选择 Exadata 基础架构。
3. 选择要删除的 Exadata 基础架构。
4. 选择删除。
5. 出现提示时，输入，**`delete me`**然后选择 “删除”。

删除 ODB 对等连接

当您不再需要 ODB 对等连接时，可以将其删除。必须先删除所有 ODB 对等连接，然后才能删除 ODB 网络。

控制台

1. 登录 AWS 管理控制台 并打开 Oracle Database@AWS 控制台，网址为https://console.aws.amazon.com/odb/。
2. 在导航窗格中，选择 ODB 对等连接。
3. 选择要删除的 ODB 对等连接。
4. 选择删除。
5. 要确认删除，请输入**`delete me`**并选择删除。

AWS CLI

要删除 ODB 对等连接，请使用命令。`delete-odb-peering-connection`

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

在 Oracle 数据库中备份@AWS

Oracle Database@AWS 提供了多种备份选项来保护您的 Oracle 数据库。您可以使用与 Amazon S3 无缝集成的 Oracle 托管备份，也可以使用 Oracle 恢复管理器 (RMAN) 创建自己的用户管理备份。

甲骨文管理了对亚马逊 S3 的备份

创建 ODB 网络时，Oracle Database@AWS 会自动为 Oracle 托管的 Amazon S3 备份配置网络访问权限。OCI 配置必要的 DNS 条目和安全列表。这些配置允许 OCI 虚拟云网络 (VCN) 和 Amazon S3 之间的流量。ODB 网络不启用或控制自动备份。

Oracle 托管的备份完全由 OCI 管理。创建 Oracle Exadata 数据库时，您可以通过在 OCI 控制台中选择启用自动备份来启用自动备份。选择以下备份目标之一：

- Amazon S3
- OCI 对象存储
- 自主恢复服务

有关更多信息，请参阅 OCI 文档中的 Backup Exadata 数据库。

在 Oracle 数据库中由用户管理的 Amazon S3 备份@AWS

借助 Oracle Database@AWS，您可以使用专用基础架构上的 Exadata 数据库服务创建用户管理的数据库备份。您可以使用 Oracle 恢复管理器 (RMAN) 备份数据并将其存储在 Amazon S3 存储桶中。您可以完全控制备份计划、保留策略和存储成本，同时保持 Oracle Database AWS@ 的托管服务优势。

> **Note**
>
> Oracle Database@AWS 不支持在专用基础设施上对自治数据库进行用户管理的备份。

用户管理的备份与 Oracle Databas AWS e@ 提供的 AWS 托管备份解决方案相得益彰。您可以使用手动备份来满足合规性要求、跨区域灾难恢复或与现有备份管理工作流程的集成。

您可以使用以下用户管理的备份技术：

Oracle Secure Backup

以最佳性能将备份直接传输到 Amazon S3。

Storage Gateway

使用 Storage Gateway 进行使用 NFS 共享的基于文件的备份。

S3 挂载点

使用文件客户端将 Amazon S3 存储桶挂载为本地文件系统。

在 Oracle 数据库中由用户管理的 Amazon S3 备份的先决条件@AWS

在将 Oracle Exadata 数据库备份到 Amazon S3 之前，请执行以下操作：

1. 允许从您的 ODB 网络直接访问 Amazon S3。
2. 在 Oracle Database@ 和 Amazon S3 之间配置网络连接AWS 和路由。

允许从您的 ODB 网络访问 Amazon S3

要将数据库手动备份到 Amazon S3，请启用从 ODB 网络直接访问 S3。该技术允许您的数据库访问 Amazon S3以满足您的业务需求，例如数据导入/导出或用户管理的备份。您可以完全控制备份存储的目标位置，并且可以使用 VPC Lattice 使用策略来限制对 Amazon S3 的访问。

默认情况下，不启用从您的 ODB 网络直接访问 Amazon S3。您可以在创建或修改 ODB 网络时启用 S3 访问权限。

控制台

允许从您的 ODB 网络直接访问 Amazon S3

1. 打开 Oracle Database@AWS 控制台，网址为。https://console.aws.amazon.com/odb/
2. 在导航窗格中，选择 ODB 网络。
3. 选择您要为其启用 Amazon S3 访问权限的 ODB 网络。
4. 选择 Modify(修改)。
5. 选择 Amazon S3。
6. （可选）配置 Amazon S3 策略文档以控制对 Amazon S3 的访问权限。如果您未指定策略，则默认策略会授予完全访问权限。
7. 选择 “继续”，然后选择 “修改”。

AWS CLI

要允许从 ODB 网络直接访问 Amazon S3，请使用带`s3-access`参数的`update-odb-network`命令：

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

要配置 Amazon S3 策略文档，请使用以下`--s3-policy-document`参数：

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

启用 Amazon S3 访问后，您可以使用区域 DNS `s3.region.amazonaws.com` 从您的 ODB 网络访问 Amazon S3。默认情况下，OCI 会配置此 DNS 名称。要使用自定义 DNS 名称，请修改您的 VCN DNS 以确保自定义 DNS 解析为服务网络终端节点的 IP 地址。

在 Oracle Database@AWS 和 Amazon S3 之间配置网络连接

要允许用户管理备份到 Amazon S3，您的虚拟机必须能够访问 S3 Amazon VPC 终端节点。在 OCI 控制台中，您可以编辑网络安全组 (NSG) 中的安全规则以控制入口和出口流量。对于用户管理的备份，流量通过客户端子网而不是备份子网流动。在以下步骤中，您将更新客户端子网以添加 VPC 终端节点 IP 地址的出口规则。 NSGs

允许虚拟机访问 Amazon S3 终端节点

1. 打开 Oracle Database@AWS 控制台，网址为。https://console.aws.amazon.com/odb/
2. 选择 ODB 网络。
3. 选择 ODB 网络的名称。
4. 选择 OCI 资源。
5. 选择 “服务集成” 选项卡。
6. 在 Amazon S3 下，请注意以下信息：
   - 亚马逊 VPC S3 终端节点 IPv4 的地址。您稍后需要此信息。例如，IP 地址可能是`192.168.12.223`。
   - 亚马逊 VPC S3 终端节点的域名。您稍后需要此信息。例如，域名可能是`s3.us-east-1.amazonaws.com`。

7. 在左侧导航窗格中，选择 Exadata 虚拟机集群，然后选择您的虚拟机集群名称。
8. 在页面顶部，选择 “摘要” 选项卡。
9. 选择虚拟机，然后选择虚拟机的名称。
10. 注意 D NS 名称中的值。这是您在使用连接虚拟机时指定的主机名ssh。
11. 在右上角，选择在 OCI 中管理。这将打开 OCI 控制台。
12. 在虚拟云网络列表页上，选择包含 ODB 网络客户端子网 () 的网络安全组 (NSG) 的 VCN。exa_static_nsg有关更多信息，请参阅 OCI 文档中的管理 NSG 的安全规则。
13. 在详细信息页面上，根据您看到的选项执行以下操作之一：
    - 在 “安全” 选项卡上，转到 “网络安全组”。
    - 在资源下，选择网络安全组。
14. 为客户机子网选择 NSG (exa_static_nsg)。
15. 为您之前记下的 VPC 终端节点地址添加一条出口规则。

测试从您的虚拟机到 S3 的连接

1. ssh用于连接您之前root获得的 DNS 名称的虚拟机。连接时，请使用您的 SSH 密钥指定一个.pem文件。
2. 运行以下命令以确保虚拟机可以访问 Amazon S3 Amazon VPC 终端节点。使用您之前记下的 S3 域名。

```
# 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 备份到亚马逊 S3

Oracle Secure Backup 充当 SBT 接口，可与恢复管理器 (RMAN) 配合使用。你可以使用 RMAN 和 Oracle Secure Backup 将你的 Oracle Database@AWS 数据库直接备份到 Amazon S3。Oracle Secure Backup 具有以下优势：

- Oracle Secure Backup 优化了 RMAN 和 S3 之间的数据传输。
- 无需中间备份存储。
- Oracle Secure Backup 管理备份媒体的生命周期。

使用 Oracle Secure Backup 备份到亚马逊 S3

1. 在 Exadata 虚拟机服务器上安装 Oracle 安全备份模块。将占位符值替换为您的 AWS 访问密钥和私有访问密钥。有关更多信息，请参阅使用 Oracle 安全备份云模块备份到云上的 Oracle 文档。

```
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. 连接 RMAN 并配置备份通道和默认设备类型。

```
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. 验证配置。

```
RMAN> SHOW ALL;
```

4. 备份数据库。

```
RMAN> BACKUP DATABASE;
```

5. 验证备份是否成功完成。

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

在亚马逊上使用 AWS Storage Gateway 备份到亚马逊 S3 EC2

AWS Storage Gateway 是一项混合服务，可将您的本地环境与 AWS Cloud 存储服务连接起来。对于 Oracle Database@AWS 备份，您可以使用 Storage Gateway 创建直接写入 Amazon S3 的基于文件的备份工作流程。与 Oracle 安全备份技术不同，您可以管理备份的生命周期。

在此解决方案中，您可以创建一个单独的 Amazon EC2 实例来配置 Storage Gateway。您还可以添加一个 Amazon EBS 卷来缓存对 Amazon S3 的读取和写入。

此技术具有以下优点：

- 您不需要像 Oracle Secure Backup 这样的媒体管理器。
- 无需中间备份存储。

部署 Storage Gateway 并创建文件共享

1. 打开 AWS 管理控制台 at https://console.aws.amazon.com/storagegateway/home/，然后选择要在其中创建网关的 AWS 区域。
2. 使用亚马逊 EC2 实例作为中心，部署并激活 Amazon S3 文件网关。按照 Storage Gateway 用户指南中为 S3 文件网关部署自定义 Amazon EC2 主机中的说明进行操作。

   配置文件网关时，请确保执行以下操作：

   - 至少添加一个 Amazon EBS 卷作为缓存存储空间，其大小至少为 150 GiB。
   - 在您的安全组中打开 TCP/UDP 端口 2049 以进行 NFS 访问。这允许您创建 NFS 文件共享。
   - 为入站流量打开 TCP 端口 80，以便在网关激活期间允许一次性 HTTP 访问。激活后，您可以关闭此端口。
3. 为你的 ODB 网络和 Storage Gateway 之间的私有连接创建一个 Amazon VPC 终端节点。有关更多信息，请参阅使用接口 VPC 终端节点访问 AWS 服务。
4. 通过 Storage Gateway 控制台为您的 Amazon S3 存储桶创建文件共享。有关更多信息，请参阅创建文件共享。

使用 Storage Gateway 将数据库备份到 Amazon S3

1. 在终端中，使用连接ssh到 Exadata 虚拟机的 DNS 名称。要查找 DNS 名称，请参阅在 Oracle 数据库中由用户管理的 Amazon S3 备份的先决条件@AWS。
2. 在 Exadata 虚拟机群集服务器上为 NFS 挂载创建一个目录。以下示例会创建 `/home/oracle/sgw_mount/` 目录。

   ```
   mkdir /home/oracle/sgw_mount/
   ```
3. 将 NFS 共享挂载到您刚刚创建的目录上。以下示例在目录上创建共享`/home/oracle/sgw_mount/`。*`SG-IP-address`*替换为您的 Storage Gatew *`your-bucket-name`* ay IP 地址和 S3 存储桶的名称。

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

4. 连接到 RMAN 并将数据库备份到已装载的目录。以下示例创建通道`rman_local_bkp`并使用装入点路径来格式化备份片段。

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

5. 确认备份文件已在装载目录中创建。以下示例显示了两个备份片段。

```
$ 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 S3 挂载点备份到 Amazon S3

您可以使用 Amazon S3 挂载点先在本地创建备份，然后将其复制到 Amazon S3。此技术在本地存储上创建备份，然后使用挂载点接口将其传输到 Amazon S3。备份时间比其他技术长，因为您需要备份两次数据。

> **Note**
>
> 不支持使用挂载点直接备份到 Amazon S3，无需暂存。RMAN 需要与 Amazon S3 挂载点接口不兼容的特定文件系统权限。

此技术不需要您许可 Oracle Secure Backup 等媒体管理器。您可以管理备份的生命周期。

使用 S3 挂载点备份到 Amazon S3

1. 在终端中，使用连接`ssh`到 Exadata 虚拟机的 DNS 名称。要查找 DNS 名称，请参阅在 Oracle 数据库中由用户管理的 Amazon S3 备份的先决条件@AWS。
2. 在 Exadata 虚拟机群集服务器上安装 Amazon S3 挂载点。有关安装和配置的更多信息，请参阅《亚马逊 S3 用户指南》中的 Amazon S 3 安装点。

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

3. 通过运行`mount-s3`命令来验证安装。

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

4. 在 Exadata 虚拟机群集服务器的本地存储上创建中间备份目录。您将数据库备份到此本地目录，然后将备份复制到 S3 存储桶。以下示例创建目录/u02/rman_bkp_local。

```
mkdir /u02/rman_bkp_local
```

5. 为 Amazon S3 挂载点创建目录。以下示例创建目录/home/oracle/s3mount。

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

6. 使用挂载点挂载您的 Amazon S3 存储桶。以下示例在目录/home/oracle/s3mount上安装一个 S3 存储桶。*your-s3-bucket-name*替换为您实际的 Amazon S3 存储桶名称。

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

7. 确认您可以访问 Amazon S3 存储桶中的内容。

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

8. 将 RMAN 连接到您的目标数据库并将其备份到本地暂存目录。以下示例创建通道rman_local_bkp并使用该路径/u02/rman_bkp_local/格式化备份片段。

```
$ rman TARGET /

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

9. 确认备份是在本地目录中创建的：

```
$ 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. 将备份文件从本地暂存目录复制到 Amazon S3 挂载点。

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

11. 确认您已成功将文件复制到 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
```

禁止直接访问 Amazon S3

如果您不再需要从 ODB 网络直接访问 Amazon S3，则可以将其禁用。启用或禁用对 S3 的直接网络访问不会影响对 Oracle 托管的 Amazon S3 备份的网络访问。

控制台

禁用直接访问 Amazon S3

1. 打开 Oracle Database@AWS 控制台，网址为。https://console.aws.amazon.com/odb/
2. 在导航窗格中，选择 ODB 网络。
3. 选择您要禁用 Amazon S3 访问权限的 ODB 网络。
4. 选择 Modify(修改)。
5. 清除 “启用 S3 访问权限” 复选框。
6. 选择修改 ODB 网络。

AWS CLI

将 `update-odb-network` 命令与 `s3-access` 参数一起使用。

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

对 Amazon S3 集成进行故障排除

如果您在 Oracle 托管的 Amazon S3 备份或直接访问 Amazon S3 时遇到问题，请考虑以下故障排除步骤：

无法从您的数据库访问 Amazon S3

请检查以下事项：

- 确认您的 ODB 网络已启用 Amazon S3 访问权限。使用`GetOdbNetwork`操作来检查`s3Access`状态是否为`Enabled`。
- 确保您使用的是正确的区域 DNS 名称：`s3.`*`region`*`.amazonaws.com`。
- 检查您的 Oracle 数据库是否具有访问亚马逊 S3 所需的权限。

甲骨文管理的备份失败

请检查以下事项：

- 默认情况下，Oracle 对 Amazon S3 的托管备份处于启用状态，无法禁用。如果备份失败，请查看 Oracle 数据库日志中是否有特定的错误消息。
- 通过查看服务集成资源，验证 Amazon VPC Lattice 资源配置是否正确。
- 请联系 Oracle 支持部门，获取有关 Oracle 托管自动备份问题的帮助。有关更多信息，请参阅 获取对 Oracle 数据库的支持@AWS。

Oracle Database@AWS Zero-ETL 与亚马逊 Redshift 集成

零 ETL 集成是一种完全托管的解决方案，可在 Amazon Redshift 中提供来自多个来源的交易和运营数据。使用此解决方案，您可以将数据从在 Oracle Exadata 上运行的 Oracle 数据库或专用 Exadata 基础设施上的自治数据库复制到 Amazon Redshift。自动同步避免了传统的提取、转换和加载 (ETL) 过程。它还支持实时分析和 AI 工作负载。有关更多信息，请参阅《Amazon Redshift 管理指南》中的零 ETL 集成。

零 ETL 集成具有以下好处：

- 实时数据复制 — 将数据从 Oracle 数据库持续同步到 Amazon Redshift，延迟最小
- 省去复杂的 ETL 管道 — 无需构建和维护自定义数据集成解决方案
- 减少运营开销 — 通过以下方式实现自动设置和管理 AWS APIs
- 简化的数据集成架构 — Oracle Database@AWS 和 AWS 分析服务之间的无缝集成
- 增强安全性 — 内置加密和 AWS IAM 访问控制

对于与 Oracle Database@ 的零 ETL 集成，Amazon Redshift 不收取额外费用。AWS您需要为现有 Amazon Redshift 资源付费，这些资源用于创建和处理在零 ETL 集成中创建的变更数据。有关更多信息，请参阅 Amazon Redshift 定价。

Oracle Database@ 中支持零 ETL 集成的数据库版本AWS

零 ETL 集成支持以下 Oracle 数据库版本：

- 甲骨文 Exadata — 甲骨文数据库 19c
- 专用基础设施上的自治数据库 — Oracle 数据库 19c 和 23ai

零 ETL 集成在 Oracle 数据库中的工作原理@AWS

零 ETL 集成允许 Oracle Database@AWS 将数据复制到亚马逊 Redshift。该集成利用 Amazon VPC Lattice 来创建安全的网络连接。变更数据捕获 (CDC) 技术可确保实时数据同步。您可以通过管理集成 AWS Glue APIs。

零 ETL 集成架构包括以下内容：

- 安全连接-使用 TLS 端口 2484 上的 SSL/TLS 加密进行数据传输

- AWS S@@ ecrets Manager — 使用密 AWS 钥管理服务安全地存储数据库凭据和证书
- AWS Glue 集成 — 为零 ETL 集成提供统一的管理界面

复制过程将通过以下步骤进行：

1. 在端口 2484 上使用 SSL 建立与 Oracle 数据库的安全连接
2. 对选定的数据库、架构和表执行初始完整转储
3. 为持续的实时复制设置变更数据捕获 (CDC)
4. 将复制的数据写入目标 Amazon Redshift 集群

> **Important**
>
> 默认情况下，未启用零 ETL 集成。您必须使用对其进行配置 AWS Glue APIs。您无法使用 Oracle Database@ 直接设置零 ETL 集成。AWS APIs

在 Oracle 数据库中实现零 ETL 集成的先决条件@AWS

在设置零 ETL 集成之前，请确保满足以下先决条件。

一般先决条

- Oracle Database@AWS 设置 — 确保已配置并运行至少一个虚拟机集群。
- 已启用零 ETL 集成 — 确保您的虚拟机集群或自治虚拟机群集与启用了零 ETL 的 ODB 网络相关联。
- 支持的 Oracle 数据库版本 — 必须使用 Oracle Database 19c（Oracle Exadata）或 Oracle Database 19c/23ai（专用基础设施上的自治数据库）。
- 相同 AWS 区域 — 源 Oracle 数据库和目标 Amazon Redshift 集群必须位于同一 AWS 区域。

甲骨文数据库先决条件

您必须使用以下设置来配置 Oracle 数据库。

复制用户设置

在要复制的每个可插拔数据库 (PDB) 中创建一个专用的复制用户：

- 对于 Oracle Exadata — 使用安全ODBZEROETLADMIN密码创建用户。
- 对于专用基础架构上的自治数据库-使用现有GGADMIN用户。

向复制用户授予以下权限。

```
-- 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";
```

补充日志记录

在 Oracle 数据库上启用补充日志记录以捕获变更数据。

```
-- 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;
```

要在 Oracle Database@ 和 Amazon AWS Redshift 之间设置零 ETL 集成，您必须配置 SSL。

对于 Oracle Exadata 数据库

您必须在端口 2484 上手动配置 SSL。此任务涉及以下内容：

- `(PROTOCOL=tcps)(PORT=2484)`在中进行配置 `listener.ora`
- 使用设置钱包 `sqlnet.ora`
- 生成和配置 SSL 证书（请参阅 My Oracle Support 文档中的 “如何配置 SSL/TCPS Exadata 云数据库 (exacc/exacs)（文档 ID 2947301.1）”）

对于自治数据库

默认情况下，端口 2484 上的 SSL 处于启用状态。无需其他配置。

> **Important**
>
> SSL 端口固定为 2484。

AWS 服务先决条件

在设置零 ETL 集成之前，请设置 S AWS ecrets Manager 并配置 IAM 权限。

设置 S AWS ecrets Manager

将您的 Oracle 数据库凭据存储在 S AWS ecrets Manager 中，如下所示：

1. 在密钥管理服务中创建客户托管密 AWS 钥 (CMK)。
2. 使用 CMK 将数据库凭据存储在 S AWS ecrets Manager 中。
3. 配置资源策略以允许 Oracle Database@ 访问AWS 。

要获取 TDE 密钥 ID 和密码，请使用支持 Oracle 作为 AWS 数据库迁移服务来源的加密方法中描述的技术。以下命令生成 base64 钱包。

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

以下示例显示了 Oracle Exadata 的密钥。对于*asm_service_name*，*111.11.11.11*表示虚拟机节点的虚拟 IP。您也可以使用 SCAN 注册 ASM 监听器。

```
{
```

```
  "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"
  }
}
```

以下示例显示了专用基础设施上自治数据库的密钥。

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

配置 IAM 权限

创建允许零 ETL 集成操作的 IAM 策略。以下示例策略允许对 Exadata 虚拟机集群执行描述、创建、更新和删除操作。对于自治虚拟机群集，请使用该值`cloud-autonomous-vm-cluster`代`cloud-vm-cluster`替资源 ARN。

在 Oracle 数据库中集成零 ETL 的注意事项@AWS

在和 Amazon Redshift Oracle Database@AWS 之间设置零 ETL 集成时，请考虑以下指南：

初始数据加载时间

初始满载时间取决于数据库的大小。大型数据库可能需要几个小时或几天才能完成初始同步。

甲骨文数据库性能

更改数据捕获可能会影响 Oracle 数据库性能，尤其是在事务量大的情况下。启用零 ETL 集成后，监控您的数据库性能。

架构更改

源 Oracle 数据库中的数据定义语言 (DDL) 更改可能需要您手动干预才能重新创建集成。仔细规划架构变更。

有关一般注意事项，请参阅在 Amazon Redshift 中使用零 ETL 集成时的注意事项。

Oracle 数据库中零 ETL 集成的局限性@AWS

请注意以下一般限制：

每个集成只有一个 PDB

每个 Zero-ETL 集成只能从一个可插拔数据库 (PDB) 复制数据。`include: pdb1.*.*`, `include: pdb2.*.*`不支持诸如此类的数据过滤器。

每个自治数据库或 Exadata 基础架构均可进行单一集成

每个 Zero-ETL 集成只能从专用基础设施上的一个自治数据库复制数据。

固定 SSL 端口

SSL 连接必须使用端口 2484。

相同区域要求

源 Oracle Database@AWS 虚拟机集群和目标 Amazon Redshift 集群必须位于同一区域。 AWS 不支持跨区域复制。

不支持 mTLS

不支持双向 TLS (mTLS)。如果您的 OCI 数据库启用了 mTLS，则必须将其禁用才能使用零 ETL 集成。

不可变的集成设置

创建与集成关联的 ARN 或 KMS 密钥后，您无法对其进行修改。要更改这些设置，您必须删除并重新创建集成。

TDE 列级加密

Oracle Exadata 数据库不支持列级透明数据加密 (TDE)。仅支持表空间级别 TDE。

数据类型支持

某些特定于 Oracle 的数据类型可能不受完全支持，或者可能需要在复制期间进行转换。在将数据库部署到生产环境之前，请彻底测试您的特定数据类型。

设置 Oracle Database@ 与 Amazon Redshift AWS 的集成

要在您的 Oracle 数据库和 Amazon Redshift 之间设置零 ETL 集成，请完成以下步骤：

1. 在您的 ODB 网络上启用零 ETL。
2. 配置 Oracle 数据库先决条件。
3. 设置 S AWS ecrets Manager 和 AWS 密钥管理服务。
4. 配置 IAM 权限。
5. 设置 Amazon Redshift 资源政策。
6. 创建零 ETL 集成。
7. 在 Amazon Redshift 中创建目标数据库。

第 1 步：为您的 ODB 网络启用零 ETL

您可以为与源虚拟机集群关联的 ODB 网络启用零 ETL 集成。默认情况下，此集成处于禁用状态。

控制台

启用零 ETL 集成

1. 打开 Oracle Database@AWS 控制台，网址为。https://console.aws.amazon.com/odb/
2. 在导航窗格中，选择 ODB 网络。
3. 选择要为其启用零 ETL 集成的 ODB 网络。
4. 选择 Modify(修改)。

5. 选择零 ETL。
6. 选择 “继续”，然后选择 “修改”。

AWS CLI

要启用零 ETL 集成，请使用带参数的`update-odb-network`命令：`--zero-etl-access`

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

要为与源虚拟机集群关联的 ODB 网络启用零 ETL 集成，请使用命令。`update-odb-network`此命令配置零 ETL 集成所需的网络基础架构。

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

步骤 2：配置您的 Oracle 数据库

按照先决条件中所述完成 Oracle 数据库配置：

- 创建复制用户并授予必要的权限。
- 启用已存档的重做日志。
- 配置 SSL（仅限 Oracle Exadata）。
- 如果适用，请设置 ASM 用户（仅限 Oracle Exadata）。

第 3 步：设置 S AWS ecrets Manager 和 AWS 密钥管理服务

创建客户托管密钥 (CMK) 并存储您的数据库凭据。

1. 使用`create-key`命令在 AWS 密钥管理服务中创建 CMK。

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

2. 将您的数据库凭据存储在 S AWS ecrets 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. 为密钥附加资源策略以允许 Oracle Database@ 访问AWS 。

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

在前面的命令中，`secret-resource-policy.json`包含以下 JSON。

JSON

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

4. 将资源策略附加到 CMK。CMK 资源策略必须包括 Oracle Database@AWS 服务主体和 Amazon Redshift 服务主体的权限，才能支持加密的零 ETL 集成。

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

该cmk-resource-policy.json文件应包含以下政策声明。第一条语句允许 Oracle Database@AWS 服务访问，第二条语句允许 Amazon Redshift 为 KMS 密钥创建用于加密数据操作的授权。

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"
          ]
```

```
        }
      }
    }
  ]
}
```

步骤 4：配置 IAM 权限

创建并附加允许零 ETL 集成操作的 IAM 策略。

```
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
```

以下策略授予必要的权限。

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": "*"
    }
  ]
}
```

第 5 步：配置 Amazon Redshift 资源策略

在您的 Amazon Redshift 集群上设置资源策略以授权入站集成。

```
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，你可以使用 AWS 控制台中的 “为我修复” 选项。此选项可自动配置所需的 Amazon Redshift 策略，而无需您手动配置。

步骤 6：使用创建零 ETL 集成 AWS Glue

使用命令创建零 ETL 集成。 AWS Glue `create-integration`在此命令中，您可以指定源虚拟机集群和目标 Amazon Redshift 命名空间。

以下示例创建了与 Exadata 虚拟机群集中`pdb1`运行的名为 PDB 的集成。您也可以通过在源 ARN `cloud-autonomous-vm-cluster` 中`cloud-vm-cluster`替换为来创建自治虚拟机集群。指定 KMS 密钥是可选的。如果您指定密钥，则该密钥可能与您在中创建的密钥不同第 3 步：设置 S AWS ecrets Manager 和 AWS 密钥管理服务。

```
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"
```

该命令返回集成 ARN 并将状态设置为。`creating`您可以使用`describe-integrations`命令监控集成状态。

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

> **Important**
>
> 每个集成仅支持一个 PDB。例如，数据筛选器必须指定单个 PDB。`include: pdb1.*.*`来源必须位于创建集成的相同 AWS 区域和账户中。

第 7 步：在 Amazon Redshift 中创建目标数据库

集成激活后，在您的 Amazon Redshift 集群中创建目标数据库。

```
-- 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";
```

创建目标数据库后，您可以查询复制的数据。

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

-- Connect to the new database
\c target_database_name

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

验证零 ETL 集成

通过在中查询集成状态 AWS Glue 并确保您的 Oracle 更改已复制到 Amazon Redshift 来验证集成是否正常运行。

验证您的零 ETL 集成是否正常运行

1. 检查集成状态。

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

   状态应为ACTIVE或REPLICATING。
2. 通过在您的 Oracle 数据库中进行更改并检查更改是否显示在 Amazon Redshift 中，来验证数据复制。
3. 监控 Amazon 中的复制指标 CloudWatch （如果有）。

针对零 ETL 集成的数据过滤 Oracle Database@AWS

Oracle Database@AWS 零 ETL 集成支持数据过滤。您可以使用它来控制源 Oracle Exadata 数据库将哪些数据复制到目标数据仓库。您可以应用一个或多个筛选条件来有选择地包含或排除特定的表，而不是复制整个数据库。这可以通过确保只传输相关数据，来协助您优化存储和查询性能。筛选仅限于数据库和表级别。不支持列级和行级筛选。

Oracle Database 和 Amazon Redshift 对对象名称大小写的处理方式不同，这会影响数据筛选器配置和目标查询。注意以下几点：

- 除非 CREATE 语句中显式引用，否则 Oracle Database 以大写形式存储数据库、架构和对象名称。例如，如果您创建 mytable（不带引号），Oracle 数据字典会将表名存储为 MYTABLE。如果您在创建语句中引用对象名称，Oracle 数据字典将保留大小写。
- 零 ETL 数据筛选器区分大小写，并且必须与 Oracle 数据字典中显示的对象名称的大小写完全匹配。例如，如果 Oracle 字典存储架构和表名REINVENT.MYTABLE，则使用创建筛选器include: ORCL.REINVENT.MYTABLE。
- 除非被显式引用，否则 Amazon Redshift 查询默认为小写对象名称。例如，查询 MYTABLE（无引号）会搜索 mytable。

在创建 Amazon Redshift 筛选条件和查询数据时，请注意大小写差异。的筛选注意事项与适用于 Oracle Oracle Database@AWS 的 Amazon RDS 的筛选注意事项相同。有关案例如何影响 Oracle 数据库中的数据筛选器的示例，请参阅 Amazon Relational Database Service 用户指南中的 RDS f or Oracle 示例。

监控零 ETL 集成

定期监控您的零ETL集成可确保最佳性能，并有助于尽早发现问题。

集成状态监控

使用 Glue 监控您的零 ETL 集成的状态。 AWS APIs

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

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

集成状态包括：

- 创建-正在设置集成
- activ e — 集成正在运行并正在复制数据
- 正在@@ 修改-正在更新集成配置
- ne@@ eds_acten tion — 集成需要手动干预
- 失败-集成遇到错误
- 正在删除-正在移除集成

性能监控

监控您的零 ETL 集成性能的以下方面：

- 复制延迟 — Oracle 中发生更改的时间与更改出现在 Amazon Redshift 中的时间差
- 数据吞吐量-每单位时间内复制的数据量
- 错误率-复制错误或失败的频率
- 资源利用率 — 源系统和目标系统上的 CPU、内存和网络使用率

使用 Amazon CloudWatch 监控这些指标并为临界阈值设置警报。

在中管理零 ETL 集成 Oracle Database@AWS

创建 Zero-ETL 集成后，您可以执行各种管理操作，包括修改和删除集成。本节介绍零ETL集成的持续管理。

修改零 ETL 集成

您只能在受支持的数据仓库中修改零 ETL 集成的名称、描述和数据筛选选项。您无法修改用于加密集成、源数据库或目标数据库的密 AWS 钥管理服务密钥。

修改集成的先决条件

在修改零 ETL 集成之前，请确保满足以下条件：

- 必需权限-除了标准`odb:UpdateOutboundIntegration`权限外，您的 IAM 用户或角色还必须拥有该 AWS Glue 权限。

- 处于活动状态的集成-集成必须处于ACTIVE状态，而不是处于CREATINGMODIFYING、DELETING、或FAILED。
- 有效的数据筛选器语法-新的数据筛选器必须遵循支持的 include/exclude 模式语法。

修改数据筛选器

您可以通过修改数据筛选器来更改要复制的表或架构。通过这种方式，您无需重新创建整个集成，即可在复制中添加或移除数据库对象。

要修改集成的数据筛选器，请使用modify-integration命令。

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

您也可以同时修改集成名称和描述。在以下示例中，您将修改中两个架构的集成名称、描述和过滤器。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**
>
> 修改数据筛选器时，集成会进入modifying状态并对数据执行重新同步。该集成会停止复制，应用新的筛选器设置，并通过重新加载目标操作恢复复制。监控集成状态以确保修改成功完成。

将数据筛选器修改为零 ETL 集成的注意事项

修改数据筛选器时，请考虑以下几点：

- 单个 PDB 限制-每个集成只能指定一个可插拔数据库 (PDB)。include: pdb1.*.*, include: pdb2.*.*不支持诸如此类的数据过滤器
- 复制中断 — 数据复制在修改过程中停止，并在应用新筛选器后恢复。

- 数据重新加载-集成会对符合新筛选条件的数据进行完全重新加载。
- 性能影响-大型数据筛选器更改可能需要很长时间才能完成，并且可能会在重装期间影响源数据库的性能。

修改零 ETL 集成设置的限制

在创建零 ETL 集成后，您无法修改以下设置：

- S@@ ecret ARN — 包含数据库凭据的 Secrets Manager AWS 密钥
- KMS 密钥-用于加密的客户托管密钥
- 来源 ARN — Or acle Databas AWS e@ 虚拟机集群
- 目标 ARN — 亚马逊 Redshift 集群或命名空间

要更改这些设置，请删除现有的 Zero-ETL 集成并创建一个新的集成。

删除零 ETL 集成

当您不再需要零 ETL 集成时，可以将其删除以停止复制并清理关联的资源。

使用 AWS Glue 进行删除

使用 Glue API 删除零 ETL 集成 AWS 。

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

您可以删除处于以下状态的集成：

- 处于活动状态
- 需要注意
- failed
- 正在同步

删除的影响

删除零 ETL 集成时，请考虑以下影响：

复制停止。

Oracle Database@AWS 不会复制亚马逊 Redshift 中的新更改。
现有数据会被保留。

已经复制到亚马逊 Redshift 的数据仍然可用。
目标数据库仍然存在。

通过集成创建的 Amazon Redshift 数据库不会自动删除。

> **Important**
>
> 删除是不可逆的。如果您需要在删除后恢复复制，请创建一个新的集成，该集成将执行完整的初始加载。

零 ETL 管理的最佳实践

遵循这些最佳实践，确保零ETL集成具有最佳性能、安全性和成本效益。

运营最佳实践

这些操作实践有助于保持可靠、高效的零 ETL 集成。

定期监测

设置 CloudWatch 警报以监控集成运行状况和性能指标。
凭证轮换

定期轮换数据库密码并在 S AWS ecrets Manager 中更新密码。
Backup 验证

定期验证您的 Oracle 数据库备份是否包含灾难恢复所需的组件。
性能测试

测试零 ETL 集成对 Oracle 数据库性能的影响，尤其是在使用高峰期。
架构变更计划

在将架构更改应用于生产环境之前，在开发环境中对其进行规划和测试。

安全最佳实践

实施这些安全措施来保护您的零 ETL 集成和数据。

最低权限访问

仅向复制用户和 AWS IAM 角色授予必要的最低权限。

网络安全

使用安全组和 NACLs 将网络访问限制为仅限所需的端口和源。

静态加密

确保 Oracle 数据库和 Amazon Redshift 集群都使用静态加密。

审计日志记录

在 Oracle 和 Amazon Redshift 上启用审计日志以跟踪数据访问和更改。

密钥管理

尽可能使用 S AWS ecrets Manager 的自动轮换功能。

成本优化

应用这些策略来优化成本，同时保持有效的零 ETL 集成性能。

数据筛选

使用精确的数据筛选器仅复制您需要的数据，从而降低存储和计算成本。

亚马逊 Redshift 优化

使用适当的 Amazon Redshift 节点类型并实施数据压缩以优化成本。

监控使用情况

通过 AWS Cost Explorer 定期查看您的零 ETL 集成使用情况和成本。

清理未使用的集成

删除不再需要的集成，以避免持续收费。

对零 ETL 集成进行故障排除

本节为解决零 ETL 集成的常见问题提供了指导。

零 ETL 集成设置失败

身份验证失败次数

- 在 S AWS ecrets Manager 中验证复制用户是否存在且密码正确。
- 确保已向复制用户授予所有必需的权限。
- 检查密钥 ARN 是否正确且可通过 Oracle Database@ 访问。AWS
- 验证 CMK 资源策略是否允许 Oracle Database@AWS 服务主体进行访问。

网络连接问题

- 确保您的 ODB 网络已启用零 ETL 集成。
- 验证端口 2484 上的 SSL 配置是否正确（仅限 Exadata）。
- 检查 Oracle 数据库监听器是否正在运行并接受连接。
- 确保网络安全组并 NACLs 允许端口 2484 上的流量。
- 验证您的密钥中的服务名称是否与实际的 Oracle 服务名称相匹配。

权限错误

- 检查您的 IAM 用户或角色是否具有执行 AWS Glue 集成操作所需的权限。
- 验证 Amazon Redshift 资源策略是否允许从您的虚拟机集群进行入站集成。
- 确保 Oracle Database@AWS 已被授予访问您的密 AWS 钥和密钥管理服务密钥的权限。

复制问题

初始加载失败

- 验证 Oracle 数据库是否有足够的资源来支持满载操作。
- 确保在源数据库上启用了补充日志记录。
- 检查是否存在任何可能阻止数据提取的表级锁或约束。

更改数据捕获问题

- 验证 Oracle 数据库是否有足够的重做日志空间和保留期。
- 检查复制用户是否有权访问已存档的重做日志。
- 对于启用 ASM 的系统，请确保正确配置 ASM 用户。
- 监控 Oracle 数据库性能，确保 CDC 不会导致资源争用。

复制延迟高

- 监控中的复制延迟指标 CloudWatch。

- 检查源数据库中是否存在高事务量或大事务。
- 验证 Amazon Redshift 集群是否有足够的容量来处理传入的数据。

数据一致性问题

数据缺失或不完整

- 验证数据筛选器是否包含所有必需的架构和表。
- 检查是否存在可能导致复制失败的不支持的数据类型。
- 确保复制用户对所有必需的表具有 SELECT 权限。

数据类型转换错误

- 查看 Oracle 和 Redshift 之间支持的数据类型映射。
- 检查是否存在可能需要自定义处理的 Oracle 特定数据类型。
- 考虑修改您的 Oracle 架构以使用更兼容的数据类型。

监控和调试

使用以下方法来监控和调试零 ETL 集成问题：

- 集成状态监控 — 使用定期检查集成状态`aws glue describe-integrations`。
- CloudWatch 指标-监控复制性能和错误的可用 CloudWatch 指标。
- Oracle 数据库监控 — 监控 Oracle 数据库性能和资源利用率。
- Redshift 监控 — 监控 Amazon Redshift 集群性能和存储利用率。

对于使用本疑难解答指南无法解决的复杂问题，请联系 AWS 支持 并提供以下信息：

- 集成 ARN 和当前状态。
- 来自集成的错误消息描述了操作。
- 甲骨文数据库和 Amazon Redshift 集群配置。
- 问题开始发生的时间表。

安全性 Oracle Database@AWS

云安全 AWS 是重中之重。作为 AWS 客户，您可以受益于专为满足大多数安全敏感型组织的要求而构建的数据中心和网络架构。

安全是 OCI 和您共同承担的责任。 AWS责任共担模型将其描述为云的安全和云中的安全：

- 云安全 — AWS 负责保护在云 AWS 服务 中运行的基础架构 AWS Cloud。 AWS 还为您提供可以安全使用的服务。作为 AWS 合规性计划的一部分，第三方审核人员将定期测试和验证安全性的有效性。
- 云端安全-您的责任由您使用的 AWS 服务决定。您还需要对其他因素负责，包括您的数据的敏感性、您组织的要求以及适用的法律法规。

本文档可帮助您了解在使用分担责任模型时如何应用 Oracle Database@AWS。您还将学习如何使用其他 AWS 服务来帮助您监控和保护您的 Oracle Database@AWS 资源。

您可以管理对 Oracle Database@AWS 资源的访问权限。您用来管理访问权限的方法取决于您需要执行的任务类型 Oracle Database@AWS：

- 使用 AWS Identity and Access Management (IAM) 策略分配权限，以确定谁有权管理 Oracle Database@AWS 资源。例如，您可以使用 IAM 来确定允许谁创建、描述、修改和删除 Exadata 基础架构、虚拟机集群或标记资源。
- 使用 Oracle 数据库引擎的安全功能来控制谁可以登录数据库实例上的数据库。这些功能就像本地网络上的数据库一样工作。
- 对 Exadata 数据库使用安全套接层 (SSL) 或传输层安全 (TLS) 连接。有关更多信息，请参阅为 TLS 无钱包连接做准备。
- Oracle Database@AWS 无法立即从 Internet 访问， AWS 只能部署在私有子网上。
- Oracle Database@AWS 使用许多默认的传输控制协议 (TCP) 端口进行各种操作。有关端口的完整列表，请参阅默认端口分配。
- 要使用默认启用的透明数据加密 (TDE) 来存储和管理密钥，请 Oracle Database@AWS 使用 OCI 保管库或 O racle 密钥保管库。 Oracle Database@AWS 不支持 AWS Key Management Service。
- 默认情况下，使用 Oracle 管理的加密密钥配置数据库。该数据库还支持客户管理的密钥。
- 要增强数据保护，请将 Oracle Data Safe 与配合使用 Oracle Database@AWS。

以下主题向您介绍如何进行配置 Oracle Database@AWS 以满足您的安全和合规性目标。

主题

- 中的数据保护 Oracle Database@AWS
- 的身份和访问管理 Oracle Database@AWS
- Oracle 数据库的合规性验证@AWS
- 韧性在 Oracle Database@AWS
- 将服务相关角色用于 Oracle Database@AWS
- Oracle Database@AWS AWS 托管策略的更新

中的数据保护 Oracle Database@AWS

出于数据保护目的，我们建议您保护 AWS 账户 凭证并使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 设置个人用户。这样，每个用户只获得履行其工作职责所需的权限。还建议您通过以下方式保护数据：

- 对每个账户使用多重身份验证（MFA）。
- 用于 SSL/TLS 与 AWS 资源通信。我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 使用设置 API 和用户活动日志 AWS CloudTrail。有关使用 CloudTrail 跟踪捕获 AWS 活动的信息，请参阅《AWS CloudTrail 用户指南》中的使用跟 CloudTrail 踪。
- 使用 AWS 加密解决方案以及其中的所有默认安全控件 AWS 服务。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Amazon S3 中的敏感数据。
- 如果您在 AWS 通过命令行界面或 API 进行访问时需要经过 FIPS 140-3 验证的加密模块，请使用 FIPS 端点。有关可用的 FIPS 端点的更多信息，请参阅《美国联邦信息处理标准（FIPS）第 140-3 版》https://aws.amazon.com/compliance/fips/。

强烈建议您切勿将机密信息或敏感信息（如您客户的电子邮件地址）放入标签或自由格式文本字段（如名称字段）。这包括您使用控制台、API AWS 或 AWS 服务 使用 Oracle Database@ 或其他网站时。 AWS CLI AWS SDKs在用于名称的标签或自由格式文本字段中输入的任何数据都可能会用于计费或诊断日志。如果您向外部服务器提供 URL，强烈建议您不要在网址中包含凭证信息来验证对该服务器的请求。

数据加密

Exadata 数据库使用 Oracle 透明数据加密 (TDE) 来加密您的数据。在临时表空间、撤消段、重做日志以及内部数据库操作（例如 JOIN 和 SORT）期间，您的数据也会受到保护。有关更多信息，请参阅数据安全。

传输中加密

Exadata 数据库使用本机 Oracle 网络服务加密和完整性功能来保护与数据库的连接。有关更多信息，请参阅传输中数据的安全性。

密钥管理

透明数据加密包括用于安全存储主加密密钥的密钥库和用于安全高效地管理密钥库和执行密钥维护操作的管理框架。有关更多信息，请参阅管理保管库加密密钥。

的身份和访问管理 Oracle Database@AWS

AWS Identity and Access Management (IAM) 是一项 AWS 服务，可帮助管理员安全地控制对 AWS 资源的访问。IAM 管理员控制谁可以进行身份验证（登录）和授权（有权限）使用 Oracle Database@资源AWS 。IAM 是一项无需额外付费即可使用的 AWS 服务。

主题

- 受众
- 使用身份进行身份验证
- 使用策略管理访问
- 如何 Oracle Database@AWS 与 IAM 配合使用
- 适用于 Oracle Database@AWS的基于身份的策略
- AWS 的托管策略 Oracle Database@AWS
- Oracle Database@AWS OCI 中的身份验证和授权
- 对 Oracle Database@AWS 身份和访问进行故障排除

受众

您的使用方式 AWS Identity and Access Management (IAM) 因您的角色而异：

- 服务用户：如果您无法访问功能，请从管理员处请求权限（请参阅对 Oracle Database@AWS 身份和访问进行故障排除）
- 服务管理员：确定用户访问权限并提交权限请求（请参阅如何 Oracle Database@AWS 与 IAM 配合使用）
- IAM 管理员：编写用于管理访问权限的策略（请参阅适用于 Oracle Database@AWS的基于身份的策略）

使用身份进行身份验证

身份验证是您 AWS 使用身份凭证登录的方式。您必须以 IAM 用户身份进行身份验证 AWS 账户根用户，或者通过担任 IAM 角色进行身份验证。

您可以使用来自身份源的证书 AWS IAM Identity Center（例如（IAM Identity Center）、单点登录身份验证或 Google/Facebook 证书，以联合身份登录。有关登录的更多信息，请参阅《AWS 登录 用户指南》中的如何登录您的 AWS 账户。

对于编程访问， AWS 提供 SDK 和 CLI 来对请求进行加密签名。有关更多信息，请参阅《IAM 用户指南》中的适用于 API 请求的AWS 签名版本 4。

AWS 账户 root 用户

创建时 AWS 账户，首先会有一个名为 AWS 账户 root 用户的登录身份，该身份可以完全访问所有资源 AWS 服务 和资源。我们强烈建议不要使用根用户进行日常任务。有关需要根用户凭证的任务，请参阅《IAM 用户指南》中的需要根用户凭证的任务。

联合身份

作为最佳实践，要求人类用户使用与身份提供商的联合身份验证才能 AWS 服务 使用临时证书进行访问。

联合身份是指来自您的企业目录、Web 身份提供商的用户 Directory Service ，或者 AWS 服务 使用来自身份源的凭据进行访问的用户。联合身份代入可提供临时凭证的角色。

要集中管理访问权限，建议使用。 AWS IAM Identity Center有关更多信息，请参阅《AWS IAM Identity Center 用户指南》中的什么是 IAM Identity Center？。

IAM 用户和群组

IAM 用户是对某个人员或应用程序具有特定权限的一个身份。建议使用临时凭证，而非具有长期凭证的 IAM 用户。有关更多信息，请参阅 IAM 用户指南中的要求人类用户使用身份提供商的联合身份验证才能 AWS 使用临时证书进行访问。

IAM 组指定一组 IAM 用户，便于更轻松地对大量用户进行权限管理。有关更多信息，请参阅《IAM 用户指南》中的 IAM 用户使用案例。

IAM 角色

IAM 角色是具有特定权限的身份，可提供临时凭证。您可以通过从用户切换到 IAM 角色（控制台）或调用 AWS CLI 或 AWS API 操作来代入角色。有关更多信息，请参阅《IAM 用户指南》中的担任角色的方法。

IAM 角色对于联合用户访问、临时 IAM 用户权限、跨账户访问、跨服务访问以及在 Amazon 上运行的应用程序非常有用。 EC2有关更多信息，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。

使用策略管理访问

您可以 AWS 通过创建策略并将其附加到 AWS 身份或资源来控制中的访问权限。策略定义了与身份或资源关联时的权限。 AWS 在委托人提出请求时评估这些政策。大多数策略都以 JSON 文档的 AWS 形式存储在中。有关 JSON 策略文档的更多信息，请参阅《IAM 用户指南》中的 JSON 策略概述。

管理员使用策略，通过定义哪个主体可以在什么条件下对哪些资源执行哪些操作来指定谁有权访问什么。

默认情况下，用户和角色没有权限。IAM 管理员创建 IAM 策略并将其添加到角色中，然后用户可以担任这些角色。IAM 策略定义权限，与执行操作所用的方法无关。

基于身份的策略

基于身份的策略是您附加到身份（用户、组或角色）的 JSON 权限策略文档。这些策略控制身份可以执行什么操作、对哪些资源执行以及在什么条件下执行。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的使用客户管理型策略定义自定义 IAM 权限。

基于身份的策略可以是内联策略（直接嵌入到单个身份中）或托管策略（附加到多个身份的独立策略）。要了解如何在托管策略和内联策略之间进行选择，请参阅《IAM 用户指南》中的在托管策略与内联策略之间进行选择。

基于资源的策略

基于资源的策略是附加到资源的 JSON 策略文档。示例包括 IAM 角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。您必须在基于资源的策略中指定主体。

基于资源的策略是位于该服务中的内联策略。您不能在基于资源的策略中使用 IAM 中的 AWS 托管策略。

其他策略类型

AWS 支持其他策略类型，这些策略类型可以设置更常见的策略类型授予的最大权限：

- 权限边界 – 设置基于身份的策略可以授予 IAM 实体的最大权限。有关更多信息，请参阅《 IAM 用户指南》中的 IAM 实体的权限边界。
- 服务控制策略 (SCPs)-在中指定组织或组织单位的最大权限 AWS Organizations。有关更多信息，请参阅《AWS Organizations 用户指南》中的服务控制策略。
- 资源控制策略 (RCPs)-设置账户中资源的最大可用权限。有关更多信息，请参阅《AWS Organizations 用户指南》中的资源控制策略 (RCPs)。
- 会话策略 – 在为角色或联合用户创建临时会话时，作为参数传递的高级策略。有关更多信息，请参阅《IAM 用户指南》中的会话策略。

多个策略类型

当多个类型的策略应用于一个请求时，生成的权限更加复杂和难以理解。要了解在涉及多种策略类型时如何 AWS 确定是否允许请求，请参阅 IAM 用户指南中的策略评估逻辑。

如何 Oracle Database@AWS 与 IAM 配合使用

在使用 IAM 管理对 Oracle Database@ 的访问权限之前AWS，请先了解有哪些 IAM 功能可用于 Oracle Database@。AWS

IAM 功能	Oracle Database@AWS 支持
基于身份的策略	是
基于资源的策略	否

IAM 功能	Oracle Database@AWS 支持
策略操作	是
策略资源	是
策略条件键	是
ACLs	否
ABAC（策略中的标签）	部分
临时凭证	是
主体权限	是
服务角色	否
服务关联角色	是

要全面了解 Oracle Database@AWS 以及其他 AWS 服务如何与大多数 IAM 功能配合使用，请参阅 IAM 用户指南中的与 IAM 配合使用的AWS 服务。

基于身份的策略 Oracle Database@AWS

支持基于身份的策略：是

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的使用客户管理型策略定义自定义 IAM 权限。

通过使用 IAM 基于身份的策略，您可以指定允许或拒绝的操作和资源以及允许或拒绝操作的条件。要了解可在 JSON 策略中使用的所有元素，请参阅《IAM 用户指南》中的 IAM JSON 策略元素引用。

基于身份的策略示例 Oracle Database@AWS

要查看 Oracle Database@AWS 基于身份的策略的示例，请参阅。适用于 Oracle Database@AWS的基于身份的策略

内部基于资源的政策 Oracle Database@AWS

支持基于资源的策略：否

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定主体。委托人可以包括账户、用户、角色、联合用户或 AWS 服务。

要启用跨账户访问，您可以将整个账户或其他账户中的 IAM 实体指定为基于资源的策略中的主体。有关更多信息，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。

的政策行动 Oracle Database@AWS

支持策略操作：是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

JSON 策略的 `Action` 元素描述可用于在策略中允许或拒绝访问的操作。在策略中包含操作以授予执行关联操作的权限。

要查看 Oracle Database@AWS 操作列表，请参阅《服务授权参考》AWS中的 Oracle Database@ 定义的操作。

正在执行的策略操作在操作前 Oracle Database@AWS 使用以下前缀：

```
odb
```

要在单个语句中指定多项操作，请使用逗号将它们隔开。

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

要查看 Oracle Database@AWS 基于身份的策略的示例，请参阅。适用于 Oracle Database@AWS的基于身份的策略

的政策资源 Oracle Database@AWS

支持策略资源：是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

`Resource` JSON 策略元素指定要向其应用操作的一个或多个对象。作为最佳实践，请使用其 Amazon 资源名称（ARN）指定资源。对于不支持资源级权限的操作，请使用通配符 (*) 指示语句应用于所有资源。

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

要查看 Oracle Database@AWS 资源类型及其列表 ARNs，请参阅《服务授权参考》AWS中的 Oracle Database@ 定义的资源。要了解您可以使用哪些操作来指定每种资源的 ARN，请参阅 Or acle Database@ 定义的操作。AWS

要查看 Oracle Database@AWS 基于身份的策略的示例，请参阅。适用于 Oracle Database@AWS的基于身份的策略

的策略条件密钥 Oracle Database@AWS

支持特定于服务的策略条件键：是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

`Condition` 元素根据定义的条件指定语句何时执行。您可以创建使用条件运算符（例如，等于或小于）的条件表达式，以使策略中的条件与请求中的值相匹配。要查看所有 AWS 全局条件键，请参阅 IAM 用户指南中的AWS 全局条件上下文密钥。

要查看 Oracle Database@AWS 条件键列表，请参阅《服务授权参考》AWS中的 Oracle Database@ 的条件密钥。要了解可以使用条件键的操作和资源，请参阅 Oracle Database AWS@ 定义的操作。

要查看 Oracle Database@AWS 基于身份的策略的示例，请参阅。适用于 Oracle Database@AWS的基于身份的策略

ACLs in Oracle Database@AWS

支持 ACLs：否

访问控制列表 (ACLs) 控制哪些委托人（账户成员、用户或角色）有权访问资源。 ACLs 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

ABAC with Oracle Database@AWS

支持 ABAC（策略中的标签）：部分支持

基于属性的访问权限控制（ABAC）是一种授权策略，该策略基于称为标签的属性来定义权限。您可以将标签附加到 IAM 实体和 AWS 资源，然后设计 ABAC 策略以允许在委托人的标签与资源上的标签匹配时进行操作。

要基于标签控制访问，您需要使用 `aws:ResourceTag/key-name`aws:RequestTag/*key-name* 或 `aws:TagKeys` 条件键在策略的条件元素中提供标签信息。

如果某个服务对于每种资源类型都支持所有这三个条件键，则对于该服务，该值为是。如果某个服务仅对于部分资源类型支持所有这三个条件键，则该值为部分。

有关 ABAC 的更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权定义权限。要查看设置 ABAC 步骤的教程，请参阅《IAM 用户指南》中的使用基于属性的访问权限控制（ABAC）。

将临时凭证与 Oracle Database@AWS

支持临时凭证：是

临时证书提供对 AWS 资源的短期访问权限，并且是在您使用联合身份或切换角色时自动创建的。AWS 建议您动态生成临时证书，而不是使用长期访问密钥。有关更多信息，请参阅《IAM 用户指南》中的 IAM 中的临时安全凭证和使用 IAM 的。AWS 服务

的跨服务主体权限 Oracle Database@AWS

支持转发访问会话（FAS）：是

转发访问会话 (FAS) 使用调用 AWS 服务的委托人的权限以及请求 AWS 服务的权限，向下游服务发出请求。有关发出 FAS 请求时的策略详细信息，请参阅转发访问会话。

Oracle Database@AWS的服务角色

支持服务角色：否

服务角色是由一项服务担任、代表您执行操作的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅 IAM 用户指南中的创建角色以向 AWS 服务委派权限。

> **Warning**
>
> 更改服务角色的权限可能会中断 Oracle Database@AWS 功能。只有在 Oracle Database@AWS 提供操作指导时才编辑服务角色。

的服务相关角色 Oracle Database@AWS

支持服务关联角色：是

服务相关角色是一种与服务关联的 AWS 服务角色。服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 AWS 账户 ，并且归服务所有。IAM 管理员可以查看但不能编辑服务关联角色的权限。

有关创建或管理 Oracle Database@AWS 服务相关角色的详细信息，请参阅将服务相关角色用于 Oracle Database@AWS。

适用于 Oracle Database@AWS的基于身份的策略

默认情况下，用户和角色无权创建或修改 Oracle Database@ 资源AWS 。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。

要了解如何使用这些示例 JSON 策略文档创建基于 IAM 身份的策略，请参阅《IAM 用户指南》中的创建 IAM 策略（控制台）。

有关 Oracle Database@AWS定义的操作和资源类型（包括每种资源类型的格式）的详细信息，请参阅《服务授权参考》AWS中的 Oracle Database@ 的操作、资源和条件键。 ARNs

主题

- 策略最佳实践
- 使用 Oracle Database@AWS 控制台
- 允许用户配置 Oracle Database@AWS 资源
- 允许用户查看他们自己的权限

策略最佳实践

基于身份的策略决定了是否有人可以在您的账户中创建、访问或删除 Oracle Database@AWS 资源。这些操作可能会使 AWS 账户产生成本。创建或编辑基于身份的策略时，请遵循以下指南和建议：

- 开始使用 AWS 托管策略并转向最低权限权限 — 要开始向用户和工作负载授予权限，请使用为许多常见用例授予权限的AWS 托管策略。它们在你的版本中可用 AWS 账户。我们建议您通过定义针对您的用例的 AWS 客户托管策略来进一步减少权限。有关更多信息，请参阅《IAM 用户指南》中的AWS 托管策略或工作职能的AWS 托管策略。
- 应用最低权限：在使用 IAM 策略设置权限时，请仅授予执行任务所需的权限。为此，您可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限许可。有关使用 IAM 应用权限的更多信息，请参阅《IAM 用户指南》中的 IAM 中的策略和权限。
- 使用 IAM 策略中的条件进一步限制访问权限：您可以向策略添加条件来限制对操作和资源的访问。例如，您可以编写策略条件来指定必须使用 SSL 发送所有请求。如果服务操作是通过特定 AWS 服务（例如）使用的，则也可以使用条件来授予对这些操作的访问权限 CloudFormation。有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：条件。
- 使用 IAM Access Analyzer 验证您的 IAM 策略，以确保权限的安全性和功能性：IAM Access Analyzer 会验证新策略和现有策略，以确保策略符合 IAM 策略语言（JSON）和 IAM 最佳实践。IAM Access Analyzer 提供 100 多项策略检查和可操作的建议，以帮助您制定安全且功能性强的策略。有关更多信息，请参阅《IAM 用户指南》中的使用 IAM Access Analyzer 验证策略。
- 需要多重身份验证 (MFA)-如果 AWS 账户您的场景需要 IAM 用户或根用户，请启用 MFA 以提高安全性。若要在调用 API 操作时需要 MFA，请将 MFA 条件添加到您的策略中。有关更多信息，请参阅《IAM 用户指南》中的使用 MFA 保护 API 访问。

有关 IAM 中的最佳实操的更多信息，请参阅 IAM 用户指南中的 IAM 中的安全最佳实操。

使用 Oracle Database@AWS 控制台

要访问 Oracle Database@AWS 控制台，您必须拥有一组最低权限。这些权限必须允许您列出和查看有关您的 Oracle Database@AWS 资源的详细信息。 AWS 账户如果创建比必需的最低权限更为严格的基于身份的策略，对于附加了该策略的实体（用户或角色），控制台将无法按预期正常运行。

对于仅调用 AWS CLI 或 AWS API 的用户，您无需为其设置最低控制台权限。相反，只允许访问与其尝试执行的 API 操作相匹配的操作。

允许用户配置 Oracle Database@AWS 资源

此政策允许用户完全访问配置 Oracle Database@AWS 资源。要从您的 VPC 设置 DNS 解析，请创建出站 Route 53 解析器并添加规则，将带有 OCI 域名的 DNS 流量转发到 OCI DNS 侦听器 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": "*"
        }
    ]
}
```

允许用户查看他们自己的权限

该示例说明了您如何创建策略，以允许 IAM 用户查看附加到其用户身份的内联和托管式策略。此策略包括在控制台上或使用 AWS CLI 或 AWS API 以编程方式完成此操作的权限。

```
{
    "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 的托管策略 Oracle Database@AWS

要向权限集和角色添加权限，使用 AWS 托管策略比自己编写策略要容易得多。创建仅为团队提供所需权限的 IAM 客户管理型策略需要时间和专业知识。要快速入门，您可以使用我们的 AWS 托管策略。这些策略涵盖常见使用案例，可在您的 AWS 账户中使用。有关 AWS 托管策略的更多信息，请参阅 IAM 用户指南中的AWS 托管策略。

AWS 服务 维护和更新 AWS 托管策略。您无法更改 AWS 托管策略中的权限。服务偶尔会向 AWS 托管策略添加其他权限以支持新功能。此类型的更新会影响附加了策略的所有身份（权限集和角色）。当

推出新功能或有新操作可用时，服务最有可能更新 AWS 托管策略。服务不会从 AWS 托管策略中移除权限，因此策略更新不会破坏您的现有权限。

此外，还 AWS 支持跨多个服务的工作职能的托管策略。例如，ReadOnlyAccess AWS 托管策略提供对所有资源 AWS 服务 和资源的只读访问权限。当服务启动一项新功能时， AWS 会为新操作和资源添加只读权限。有关工作职能策略的列表和说明，请参阅 IAM 用户指南中的适用于工作职能的AWS 托管式策略。

主题

- AWS 托管策略：Amazon ODBService RolePolicy

AWS 托管策略：Amazon ODBService RolePolicy

无法将 AmazonODBServiceRolePolicy 策略附加到 IAM 实体。此策略附加到允许代表您执行操作 Oracle Database@AWS 的服务相关角色。有关更多信息，请参阅 将服务相关角色用于 Oracle Database@AWS。

要查看有关该政策的更多详细信息，包括最新版本的 JSON 策略文档，请参阅《AWS 托管策略参考指南》ODBServiceRolePolicy中的 Amazon。

Oracle Database@AWS OCI 中的身份验证和授权

当您使用 AWS APIs 为创建资源时 Oracle Database@AWS，这些资源在逻辑上驻留在您关联的 Oracle 云基础设施 (OCI) 租户中。要部署这些资源，请代表您 AWS 与 OCI APIs 沟通。为了缓解混乱的代理问题，OCI 并 Oracle Database@AWS 使用 AWS STS 作为可信实体和转发访问会话来授权你打算在关联租赁 APIs 中使用 OCI。因此，会将来自 OCI IP 空间的 sts:getCallerIdentity API 事件记录在您的 AWS CloudTrail 跟踪和事件历史记录中。使用时会发生这些事件 Oracle Database@AWS APIs。

对 Oracle Database@AWS 身份和访问进行故障排除

使用以下信息来帮助您诊断和修复在使用 Oracle Database@AWS 和 IAM 时可能遇到的常见问题。

主题

- 我无权在以下位置执行操作 Oracle Database@AWS
- 我无权执行 iam：PassRole
- 我想允许我以外的人 AWS 账户 访问我的 Oracle Database@AWS 资源

我无权在以下位置执行操作 Oracle Database@AWS

如果您收到错误提示，指明您无权执行某个操作，则必须更新策略以允许执行该操作。

当 mateojackson IAM 用户尝试使用控制台查看有关虚构 *my-example-widget* 资源的详细信息，但不拥有虚构 odb:*GetWidget* 权限时，会发生以下示例错误。

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

在此情况下，必须更新 mateojackson 用户的策略，以允许使用 odb:*GetWidget* 操作访问 *my-example-widget* 资源。

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

我无权执行 iam：PassRole

如果您收到一条错误消息，指出您无权执行该iam:PassRole操作，则必须更新您的策略以允许您将角色传递给 Oracle Database@AWS。

有些 AWS 服务 允许您将现有角色传递给该服务，而不是创建新的服务角色或服务相关角色。为此，您必须具有将角色传递到服务的权限。

当名为的 IAM 用户marymajor尝试使用控制台在 Oracle Database AWS@ 中执行操作时，会出现以下示例错误。但是，服务必须具有服务角色所授予的权限才可执行此操作。Mary 不具有将角色传递到服务的权限。

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

在这种情况下，必须更新 Mary 的策略以允许她执行 iam:PassRole 操作。

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

我想允许我以外的人 AWS 账户 访问我的 Oracle Database@AWS 资源

您可以创建一个角色，以便其他账户中的用户或您组织外的人员可以使用该角色来访问您的资源。您可以指定谁值得信赖，可以代入角色。对于支持基于资源的策略或访问控制列表 (ACLs) 的服务，您可以使用这些策略向人们授予访问您的资源的权限。

要了解更多信息，请参阅以下内容：

- 要了解 Oracle Database@ 是否AWS 支持这些功能，请参阅。如何 Oracle Database@AWS 与 IAM 配合使用
- 要了解如何提供对您拥有的资源的访问权限 AWS 账户 ，请参阅 IAM 用户指南中的向您拥有 AWS 账户 的另一个 IAM 用户提供访问权限。
- 要了解如何向第三方提供对您的资源的访问权限 AWS 账户，请参阅 IAM 用户指南中的向第三方提供访问权限。 AWS 账户
- 要了解如何通过身份联合验证提供访问权限，请参阅《IAM 用户指南》中的为经过外部身份验证的用户（身份联合验证）提供访问权限。
- 要了解使用角色和基于资源的策略进行跨账户访问之间的差别，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。

Oracle 数据库的合规性验证@AWS

您在使用 Oracle Databas AWS e@ 时的合规责任取决于数据的敏感性、贵公司的合规目标以及适用的法律和法规。Oracle 关于云端合规性的文档可在 Oracle 网站上找到

韧性在 Oracle Database@AWS

AWS 全球基础设施是围绕 AWS 区域 可用区构建的。 AWS 区域 提供多个物理隔离和隔离的可用区，这些可用区通过低延迟、高吞吐量和高度冗余的网络连接。利用可用区，您可以设计和操作在可用区之间无中断地自动实现失效转移的应用程序和数据库。与传统的单个或多个数据中心基础设施相比，可用区具有更高的可用性、容错能力和可扩展性。

有关 AWS 区域 和可用区的更多信息，请参阅AWS 全球基础设施。

除了 AWS 全球基础架构外，Oracle Database@ 还AWS 提供多项功能来帮助支持您的数据弹性和备份需求。

将服务相关角色用于 Oracle Database@AWS

Oracle Database@AWS 使用 AWS Identity and Access Management (IAM) 服务相关角色。服务相关角色是一种与之直接关联的 IAM 角色的独特类型。 Oracle Database@AWS服务相关角色由服务预定义 Oracle Database@AWS ，包括该服务代表您呼叫他人 AWS 服务 所需的所有权限。

由于您不必手动添加必要的权限，因此与服务相关的角色可以 Oracle Database@AWS 更轻松地使用。 Oracle Database@AWS 定义其服务相关角色的权限，除非另有定义，否则 Oracle

Database@AWS 只能担任其角色。定义的权限包括信任策略和权限策略，而且权限策略不能附加到任何其他 IAM 实体。

只有在首先删除角色的相关资源后，才能删除角色。这样可以保护您的 Oracle Database@AWS 资源，因为您不会无意中删除访问资源的权限。

的服务相关角色权限 Oracle Database@AWS

Oracle Database@AWS 使用名为 AWSService RoleFor ODB 的服务相关角色 Oracle Database@AWS 允许代表您的资源 AWS 服务 进行调用。

AWSServiceRoleForODB 服务相关角色信任以下服务来代入该角色：

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

此服务相关角色附加了一个名为 `AmazonODBServiceRolePolicy` 的权限策略，授予其在您的账户中操作的权限。有关更多信息，请参阅 AWS 托管策略：Amazon ODBService RolePolicy。

> **Note**
>
> 您必须配置权限，允许 IAM 实体（如用户、组或角色）创建、编辑或删除服务关联角色。如果您遇到以下错误消息：
> Unable to create the resource. 确认您有权创建服务相关角色。Otherwise wait and try again later.
> 确保您已启用以下权限：

```
{
    "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"
        }
    }
}
```

有关更多信息，请参阅《IAM 用户指南》中的服务相关角色权限。

为创建服务相关角色 Oracle Database@AWS

您无需手动创建服务关联角色。创建 Exadata 数据库时， Oracle Database@AWS 会为您创建服务相关角色。

如果您删除该服务关联角色，然后需要再次创建，您可以使用相同流程在账户中重新创建此角色。创建 Exadata 数据库时， Oracle Database@AWS 会再次为您创建服务相关角色。

编辑的服务相关角色 Oracle Database@AWS

Oracle Database@AWS 不允许您编辑 AWSService RoleFor ODB 服务相关角色。创建服务关联角色后，您将无法更改角色的名称，因为可能有多种实体引用该角色。但是，您可以使用 IAM 编辑角色的描述。有关更多信息，请参阅 I A M 用户指南中的编辑服务相关角色。

删除的服务相关角色 Oracle Database@AWS

如果您不再需要使用某个需要服务相关角色的功能或服务，我们建议您删除该角色。这样您就没有未被主动监控或维护的未使用实体。但是，必须先删除所有资源，然后才能删除服务相关角色。

正在清理的服务相关角色 Oracle Database@AWS

必须先确认服务相关角色没有活动会话并删除该角色使用的任何资源，然后才能使用 IAM 删除服务相关角色。

在 IAM 控制台中检查服务相关角色是否具有活动会话

1. 登录 AWS 管理控制台 并打开 IAM 控制台，网址为https://console.aws.amazon.com/iam/。
2. 在 IAM 控制台的导航窗格中，选择角色。然后选择 AWSService RoleFor ODB 角色的名称（不是复选框）。
3. 在所选角色的 Summary (摘要) 页面上，选择 Access Advisor (访问顾问) 选项卡。
4. 在 Access Advisor 选项卡上，查看服务相关角色的近期活动。

> **Note**
>
> 如果您不确定 Oracle Database@AWS 是否在使用 AWSService RoleFor ODB 角色，可以尝试删除该角色。如果服务正在使用该角色，则删除将失败，您可以查看该角色的使用 AWS 区

域 位置。如果该角色已被使用，则您必须等待会话结束，然后才能删除该角色。您无法撤销服务相关角色对会话的权限。

如果要移除 AWSService RoleFor ODB 角色，则必须先删除所有 Oracle Database@AWS 资源。

Oracle Database@AWS 服务相关角色支持的区域

Oracle Database@AWS 支持在所有提供服务 AWS 区域 的地方使用服务相关角色。有关更多信息，请参阅AWS 区域 和端点。

Oracle Database@AWS AWS 托管策略的更新

查看 Oracle Database@AWS 自该服务开始跟踪这些更改以来 AWS 托管策略更新的详细信息。要获得有关此页面更改的自动提醒，请订阅 “ Oracle Database@AWS 文档历史记录” 页面上的 RSS feed。

更改	描述	日期
的服务相关角色权限 Oracle Database@AWS – 对现有策略的更新	Oracle Database@AWS 为AWSServiceRoleForODB 服务相关角色添加AmazonODBServiceRolePolicy 了新权限。这些权限 Oracle Database@AWS 允许执行以下操作： • 描述 Amazon VPC 传输网关附件 • 描述亚马逊 EC2 附件 • 激活 Amazon EventBridge 来源 有关更多信息，请参阅 的服务相关角色权限 Oracle Database@AWS。	2025 年 6 月 30 日
的服务相关角色权限 Oracle Database@AWS - 对现有策略的更新	Oracle Database@AWS 为AWSServiceRoleForODB 服务相关角色添加AmazonODBServiceRolePolicy 了新权限。这些权限 Oracle Database@AWS 允许执行以下操作： • 描述亚马逊 EventBridge 来源	2025 年 6 月 26 日

更改	描述	日期
	• 描述和创建事件总线 有关更多信息，请参阅 的服务相关角色权限 Oracle Database@AWS。	
AWS 托管策略：Amazon ODBService RolePolicy— 新的服务相关角色策略	Oracle Database@AWS `AmazonODBServiceRolePolicy` 为`AWSServiceRoleForODB` 服务相关角色添加了。有关更多信息，请参阅 AWS 托管策略：Amazon ODBService RolePolicy。	2024 年 12 月 2 日
Oracle Database@AWS 开始跟踪更改	Oracle Database@AWS 开始跟踪其 AWS 托管策略的更改。	2024 年 12 月 2 日

监控 Oracle 数据库@AWS

监控是维护和其他 AWS 解决方案的可靠性、可用性和性能的重要组成部分。 Oracle Database@AWS AWS 提供以下监控工具 Oracle Database@AWS，供您监视、报告问题并在适当时自动采取措施：

- Amazon 会实时 CloudWatch监控您的 AWS 资源和您运行 AWS 的应用程序。您可以收集和跟踪指标，创建自定义的控制面板，以及设置警报以在指定的指标达到您指定的阈值时通知您或采取措施。例如，您可以 CloudWatch 跟踪您的 Amazon EC2 实例的 CPU 使用率或其他指标，并在需要时自动启动新实例。有关更多信息，请参阅 Amazon CloudWatch 用户指南。
- Amazon Lo CloudWatch gs 使您能够监控、存储和访问来自亚马逊 EC2 实例和其他来源的日志文件。 CloudTrail CloudWatch 日志可以监视日志文件中的信息，并在达到特定阈值时通知您。您还可以在高持久性存储中检索您的日志数据。有关更多信息，请参阅 Amazon CloudWatch 日志用户指南。
- Amazon EventBridge 可用于自动化您的 AWS 服务，并自动响应系统事件，例如应用程序可用性问题或资源更改。来自 AWS 服务的事件几乎实时 EventBridge 地传送到。您可以编写简单的规则来指示您关注的事件，并指示要在事件匹配规则时执行的自动化操作。有关更多信息，请参阅 Amazon EventBridge 用户指南。
- AWS CloudTrail捕获由您的账户或代表您的 AWS 账户进行的 API 调用和相关事件，并将日志文件传输到您指定的 Amazon S3 存储桶。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。有关更多信息，请参阅 AWS CloudTrail 《用户指南》。

Oracle Database@AWS 使用 Amazon 进行监控 CloudWatch

您可以使用 Oracle Database@AWS 进行监控 CloudWatch，它收集原始数据并将其处理为可读的近乎实时的指标。这些统计数据会保存 15 个月，从而使您能够访问历史信息，并能够更好地了解您的 Web 应用程序或服务的执行情况。此外，可以设置用于监测特定阈值的警报，并在达到相应阈值时发送通知或执行操作。有关更多信息，请参阅 Amazon CloudWatch 用户指南。

以下各项的亚马逊 CloudWatch 指标 Oracle Database@AWS

该 Oracle Database@AWS 服务在AWS/ODB命名空间 CloudWatch 中向 Amazon 报告虚拟机集群、容器数据库和可插拔数据库的指标。

主题

- 云虚拟机集群的指标

- 容器数据库的指标
- 可插拔数据库的指标

云虚拟机集群的指标

该 Oracle Database@AWS 服务在AWS/ODB命名空间中报告云虚拟机集群的以下指标。

指标	说明	单位
ASMDiskgroupUtilization	磁盘组中已用可用空间的百分比。可用空间是可用于增长的空间。数据磁盘组存储我们的 Oracle 数据库文件。RECO 磁盘组包含用于恢复的数据库文件，例如存档和闪回日志。	百分比
CpuUtilization	CPU 使用率百分比。	百分比
FilesystemUtilization	已配置文件系统的利用率百分比。	百分比
LoadAverage	系统平均负载超过 5 分钟。	整数
MemoryUtilization	无需交换即可启动新应用程序的内存百分比。可用内存可以通过以下命令获取：cat /proc/meminfo	百分比
NodeStatus	表示是否可以访问主机。	整数
OcpusAllocated	OCPUs 分配的数量。	整数
SwapUtilization	总交换空间的利用率百分比。	百分比

容器数据库的指标

该 Oracle Database@AWS 服务在容器数据库的AWS/ODB命名空间中报告以下指标。

指标	说明	单位
BlockChanges	平均每秒更改的方块数。	每秒变化次数
CpuUtilization	CPU 使用率以百分比表示，在所有使用者组中汇总。报告的利用率百分比与允许使用的数据库数量 CPUs 有关，该数量是允许使用的数据库数量的两倍 OCPUs。	百分比
CurrentLogons	在所选时间间隔内成功登录的次数。	计数
ExecuteCount	在所选时间间隔内执行 SQL 语句的用户和递归调用的数量。	计数
ParseCount	所选时间间隔内的硬解析和软解析次数。	计数
StorageAllocated	收集时分配给数据库的存储空间总量。	GB
StorageAllocatedByTablespace	收集时分配给表空间的存储空间总量。对于容器数据库，此指标提供根容器表空间。	GB
StorageUsed	收集时数据库使用的存储空间总量。	GB
StorageUsedByTablespace	收集时表空间使用的存储空间总量。对于容器数据库，此指标提供根容器表空间。	GB
StorageUtilization	当前正在使用的预配置存储容量的百分比。表示为所有表空间分配的总空间。	百分比

指标	说明	单位
StorageUtilization ByTablespace	这表示收集时表空间使用的存储空间百分比。对于容器数据库，此指标提供根容器表空间。	百分比
TransactionCount	在所选时间间隔内用户提交和用户回滚的总数。	计数
UserCalls	在所选时间间隔内登录、解析和执行呼叫的总数。	计数

可插拔数据库的指标

该 Oracle Database@AWS 服务在AWS/ODB命名空间中报告可插拔数据库的以下指标。

指标	说明	单位
AllocatedStorageUt ilizationByTablesp ace	表空间使用的空间占所有已分配空间的百分比。对于容器数据库，该指标提供根容器表空间的数据。（统计：平均值，间隔：30 分钟）	百分比
AvgGCCRBlockReceiv eTime	全局缓存 CR（一致读取）块的平均接收时间。仅适用于 RAC /集群数据库。（统计：均值，间隔：5 分钟）	毫秒
AvgGCCurrentBlockR eceiveTime	全局缓存当前区块的平均接收时间。统计数据报告平均值。仅适用于真实应用程序集群 (RAC) 数据库。（统计：均值，间隔：5 分钟）	毫秒

指标	说明	单位
BlockChanges	平均每秒更改的区块数。（统计：均值，间隔：1 分钟）	每秒的变化
BlockingSessions	当前封锁会话。不适用于容器数据库。（统计：最大，间隔：15 分钟）	计数
CPUTimeSeconds	在时间间隔内，数据库实例中前台会话累积的 CPU 时间的平均速率。平均活动会话数的 CPU 时间部分。（统计：均值，间隔：1 分钟）	每秒秒
CpuCount	所选时间间隔内的数量。CPUs	计数
CpuUtilization	CPU 使用率以百分比表示，在所有使用者组中汇总。报告的利用率百分比与允许使用的数据库数量 CPUs 有关，该数量是允许使用的数据库数量的两倍 OCPUs。（统计：均值，间隔：1 分钟）	百分比
CurrentLogons	在所选时间间隔内成功登录的次数。（统计：总和，间隔：1 分钟）	计数
DBTimeSeconds	在时间间隔内，数据库实例中前台会话累积数据库时间（CPU + Wait）的平均速率。也称为平均活跃会话数。（统计：均值，间隔：1 分钟）	每秒秒

指标	说明	单位
DbmgmtJobExecutionsCount	在单个托管数据库或数据库组上执行 SQL 作业的次数及其状态。状态维度可以是以下值：“成功”、“失败”、“InProgress。”（统计：求和，间隔：1 分钟）	计数
ExecuteCount	在所选时间间隔内执行 SQL 语句的用户和递归调用的数量。（统计：求和，间隔：1 分钟）	计数
FRASpaceLimit	快速恢复区空间限制。不适用于可插拔的数据库。（统计：最大，间隔：15 分钟）	GB
FRAUtilization	快速恢复区利用率。不适用于可插拔的数据库。（统计：平均值，间隔：15 分钟）	百分比
GCCRBlocksReceived	每秒接收的全局缓存 CR（一致读取）块。仅适用于 RAC / 集群数据库。（统计：均值，间隔：5 分钟）	每秒块数
GCCurrentBlocksReceived	表示每秒接收到的全局缓存当前块。统计数据报告平均值。仅适用于真实应用程序集群 (RAC) 数据库。（统计：均值，间隔：5 分钟）	每秒块数
IOPS	每秒输入输出操作的平均次数。（统计：均值，间隔：1 分钟）	每秒操作数

指标	说明	单位
IOThroughputMB	平均吞吐量，以 MB 每秒为单位。（统计：均值，间隔：1 分钟）	每秒 MB
InterconnectTraffi cMB	平均节点间数据传输速率。仅适用于 RAC /集群数据库。（统计：均值，间隔：5 分钟）	每秒 MB
InvalidObjects	数据库对象计数无效。不适用于容器数据库。（统计数据：最大，间隔：24 小时）	计数
LogicalBlocksRead	平均每秒从 SGA/Memory（缓冲区缓存）读取的块数。（统计：均值，间隔：1 分钟）	每秒读取次数
MaxTablespaceSize	可能的最大表空间大小。对于容器数据库，该指标提供根容器表空间的数据。（统计：最大，间隔：30 分钟）	GB
MemoryUsage	内存池总大小（以 MB 为单位）。（统计：平均值，间隔：15 分钟）	MB
MonitoringStatus	资源的监控状态。如果指标收集失败，则会在该指标中捕获错误信息。（统计：均值，间隔：5 分钟）	不适用
NonReclaimableFRA	不可回收的快速恢复区。不适用于可插拔的数据库。（统计：平均值，间隔：15 分钟）	百分比

指标	说明	单位
OcpusAllocated	在所选时间间隔内服务 OCPUs 分配的实际数量。（统计：计数，间隔：1 分钟）	整数
ParseCount	所选时间间隔内的硬解析和软解析次数。（统计：求和，间隔：1 分钟）	计数
ParsesByType	每秒硬解析或软解析的次数。（统计：均值，间隔：1 分钟）	每秒分析数
ProblematicScheduledDBMSJobs	有问题的定时数据库作业计数。不适用于容器数据库。（统计：最大，间隔：15 分钟）	计数
ProcessLimitUtilization	该过程限制了利用率。不适用于可插拔的数据库。（统计：均值，间隔：1 分钟）	百分比
Processes	数据库进程计数。不适用于可插拔的数据库。（统计：最大，间隔：1 分钟）	计数
ReclaimableFRA	可回收的快速恢复区。不适用于可插拔的数据库。（统计：平均值，间隔：15 分钟）	百分比
ReclaimableFRASpace	快速恢复区可回收空间。不适用于可插拔的数据库。（统计：平均值，间隔：15 分钟）	GB
RedoSizeMB	生成的平均重做量，以 MB 每秒为单位。（统计：均值，间隔：1 分钟）	每秒 MB

指标	说明	单位
SessionLimitUtilization	会话限制利用率。不适用于可插拔的数据库。（统计：均值，间隔：1 分钟）	百分比
Sessions	数据库中的会话数。（统计：均值，间隔：1 分钟）	计数
StorageAllocated	在时间间隔内表空间分配的最大空间量。对于容器数据库，该指标提供根容器表空间的数据。（统计：最大，间隔：30 分钟）	GB
StorageAllocatedByTablespace	在时间间隔内表空间分配的最大空间量。对于容器数据库，该指标提供根容器表空间的数据。（统计：最大，间隔：30 分钟）	GB
StorageUsed	间隔内使用的最大空间量。（统计：最大，间隔：30 分钟）	GB
StorageUsedByTablespace	时间间隔内表空间使用的最大空间量。对于容器数据库，该指标提供根容器表空间的数据。（统计：最大，间隔：30 分钟）	GB
StorageUtilization	当前正在使用的预配置存储容量的百分比。表示为所有表空间分配的总空间。（统计：平均值，间隔：30 分钟）	百分比

指标	说明	单位
StorageUtilization ByTablespace	按表空间划分的已用空间百分比。对于容器数据库，该指标提供根容器表空间的数据。（统计：平均值，间隔：30 分钟）	百分比
TransactionCount	在所选时间间隔内用户提交和用户回滚的总数。（统计：求和，间隔：1 分钟）	计数
TransactionsByStatus	每秒提交或回滚的事务数。（统计：均值，间隔：1 分钟）	每秒事务数
UnusableIndexes	不可用的索引计入数据库架构。不适用于容器数据库。（统计数据：最大，间隔：24 小时）	计数
UsableFRA	可用的快速恢复区。不适用于可插拔的数据库。（统计：平均值，间隔：15 分钟）	百分比
UsedFRASpace	快速恢复区空间使用情况。不适用于可插拔的数据库。（统计：最大，间隔：15 分钟）	GB
UserCalls	在所选时间间隔内登录、解析和执行呼叫的总数。（统计：求和，间隔：1 分钟）	计数
WaitTimeSeconds	在时间间隔内，数据库实例中前台会话的非空闲等待时间的平均累积速率。平均活动会话数的等待时间部分。（统计：均值，间隔：5 分钟）	每秒秒

Amazon 的 CloudWatch 尺寸 Oracle Database@AWS

您可以使用下表中的任何维度筛选 Oracle Database@AWS 指标数据。

维度	筛选为 . . 请求的数据
cloudVmClusterId	虚拟机集群的标识符。
cloudExadataInfrastructureId	Exadata 基础架构的标识符。
collectionName	集合的名称。
deploymentType	基础设施的类型。
diskgroupName	磁盘组的名称
errorCode	错误代码。
errorSeverity	错误的严重程度。
filesystemName	文件系统的名称。
hostName	主机的名称。
instanceName	数据库实例的名称。
instanceNumber	数据库实例的实例号。
ioType	一种 I/O 操作。
jobId	作业的唯一标识符。
managedDatabaseGroupId	a 的标识符Managed Database Group。
managedDatabaseId	a 的标识符Managed Database。
memoryPool	一种内存池。
memoryType	一种记忆。

维度	筛选为 . . 请求的数据
ociCloudVmClusterId	虚拟机集群的 OCI 标识符。
ociCloudExadataInfrastructureId	Exadata 基础架构的 OCI 标识符。
parseType	一种解析。
resourceId	资源的标识符。
resourceId_Database	数据库的标识符。
resourceId_DbNode	数据库节点的标识符。
resourceName	资源的名称。
resourceName_Database	数据库的名称。
resourceName_DbNode	数据库节点的名称。
resourceType	一种数据库。
schemaName	架构的名称。
status	数据库的状态。
tablespaceContents	表空间的内容。
tablespaceName	表空间的名称。
tablespaceType	一种表空间。
transactionStatus	交易的状态。
waitClass	一类等待事件。

监控 Amazon 中的 Oracle Database@AWS 事件 EventBridge

您可以在中监控 Oracle Database@AWS 事件 EventBridge，它会提供来自应用程序和 AWS 服务的实时数据流。 EventBridge 将此数据路由到目标，例如 AWS Lambda 和 Amazon 简单通知服务。

> **Note**
>
> EventBridge 以前被称为 Amazon Ev CloudWatch ents。有关更多信息，请参阅《亚马逊 EventBridge 用户指南》中的 Amazon Ev CloudWatch ent EventBridge s 的演变。

Oracle Database@AWS 活动概述

Oracle Database@AWS 事件是表示资源生命周期变化的结构化消息。事件总线是接收事件并将其传送到零个或多个目的地或目标的路由器。 Oracle Database@AWS 事件可以从以下来源生成：

活动来自 AWS

这些事件是从 Oracle Database@AWS APIs AWS 侧面生成的，并传送到您的默认事件总线 AWS 账户。

来自 OCI 的活动

这些事件直接从 OCI 生成，例如与 Oracle Exadata 基础架构或虚拟机集群相关的事件。订阅时 Oracle Database@AWS，将在中创建带有前缀`aws.partner/odb/`的事件总线， AWS 账户 用于接收来自 OCI 的事件。

Oracle Database@AWS 来自的事件 AWS

Oracle Database@AWS 中的事件 AWS 包括在创建和删除过程中与 ODB 网络相关的生命周期更改。这些事件将传送到您的默认事件总线 AWS 账户。配送类型是尽力而为。

ODB 网络活动

事件	事件 ID	Message
创建	ODB-EVENT-0001	成功创建 ODB 网络 odbnet_ID
创建失败	ODB-EVENT-0011	创建 ODB 网络 odbnet_ID 失败

事件	事件 ID	Message
删除	ODB-EVENT-0002	成功删除 ODB 网络 odbnet_ID
删除失败	ODB-EVENT-0012	删除 ODB 网络 odbnet_ID 失败

示例：ODB 网络创建事件

以下示例显示成功创建 ODB 网络的事件。

```
{
  "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 来自 OCI 的事件

大多数事件都是直接从 OCI 生成的。 Oracle Database@AWS 创建带有前缀的事件总线`aws.partner/odb/`， AWS 账户 用于接收来自 OCI 的事件。我们建议您不要删除此事件总线。

OCI 提供全面的事件类型，包括：

- 甲骨文 Exadata 基础架构
- 虚拟机集群事件
- 国开行活动
- PDB 活动

有关 OCI 支持的特定事件类型和详细信息的更多信息，请参阅 O racle Exadata 数据库服务关于专用 Exadata 基础设施上自治数据库的专用基础设施事件和事件。

筛选 Oracle Database@AWS 事件

您可以在 Amazon 的活动总线上遵循 EventBridge 建议的活动总线设置最佳实践 EventBridge。根据您的用例，您可以设置 EventBridge 规则来筛选事件和目标，以接收和使用事件。

筛选 ODB 网络事件来自 AWS

对于来自的 ODB 网络事件 AWS，您可以使用以下事件模式进行筛选：

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

您可以使用带有默认事件总线的 EventBridge `put-rule` API 来应用此模式。有关更多信息，请参阅 Amazon EventBridge API 参考PutRule中的。

筛选来自 OCI Oracle Database@AWS 的事件

对于来自 OCI Oracle Database@AWS 的事件，您可以使用与 Amazon EventBridge API 参考PutRule中的示例类似的命令来设置规则。请注意以下准则：

- 根据要过滤的事件类型，使用自定义事件模式。
- 设置EventBusName为 Oracle Database@AWS 创建的总线的名称。

有关如何筛选事件和跨账户设置 EventBridge 目标的更多信息，请参阅AWS 账户 在 Amazon 中发送和接收事件 EventBridge。

Oracle Database@AWS 事件疑难解答

如果您在活动交付或活动内容方面遇到问题，请执行以下操作：

- 如需了解 ODB 网络活动，请联系 AWS 支持。
- 如果 ODB 网络 Oracle Database@AWS 事件以外的事件，请联系 Oracle Cloud Support。

有关更多信息，请参阅 获取对 Oracle 数据库的支持@AWS。

使用记录 Oracle Database@AWS API 调用 AWS CloudTrail

Oracle Database@AWS 与AWS CloudTrail一项服务集成，该服务提供用户、角色或角色所执行操作的记录 AWS 服务。 CloudTrail 将所有 API 调用捕获 Oracle Database@AWS 为事件。捕获的调用包括来自 Oracle Database@AWS 控制台的调用和对 Oracle Database@AWS API 操作的代码调用。使用收集的信息 CloudTrail，您可以确定向哪个请求发出 Oracle Database@AWS、发出请求的 IP 地址、发出请求的时间以及其他详细信息。

每个事件或日志条目都包含有关生成请求的人员信息。身份信息有助于您确定以下内容：

- 请求是使用根用户凭证还是用户凭证发出的。
- 请求是否代表 IAM Identity Center 用户发出。
- 请求是使用角色还是联合用户的临时安全凭证发出的。
- 请求是否由其他 AWS 服务发出。

> **Note**
>
> Oracle Database@AWS 在您的 CloudTrail 日志中记录来自 AWS Security Token Service (STS) 的 `GetCallerIdentity` API 调用。这些 STS API 调用会验证代表您与 OCI 交互 Oracle Database@AWS 时的身份。它们是正常且安全的 AWS 操作部分，不会泄露敏感信息。

CloudTrail 在您创建账户 AWS 账户 时在您的账户中处于活动状态，并且您自动可以访问 CloudTrail 活动历史记录。 CloudTrail 事件历史记录提供了过去 90 天中记录的管理事件的可查看、可搜索、可下载且不可变的记录。 AWS 区域有关更多信息，请参阅《AWS CloudTrail 用户指南》中的 “使用 CloudTrail 事件历史记录”。查看活动历史记录不 CloudTrail收取任何费用。

要持续记录 AWS 账户 过去 90 天内的事件，请创建跟踪或 CloudTrailLake 事件数据存储。

CloudTrail 步道

跟踪允许 CloudTrail 将日志文件传输到 Amazon S3 存储桶。使用创建的所有跟踪 AWS 管理控制台 都是多区域的。您可以通过使用 AWS CLI创建单区域或多区域跟踪。建议创建多区域跟踪，因为您可以捕获账户 AWS 区域 中的所有活动。如果您创建单区域跟踪，则只能查看跟踪的 AWS 区域中记录的事件。有关跟踪的更多信息，请参阅《AWS CloudTrail 用户指南》中的为您的 AWS 账户创建跟踪和为组织创建跟踪。

通过创建跟踪，您可以免费将正在进行的管理事件的一份副本传送到您的 Amazon S3 存储桶，但会收取 Amazon S3 存储费用。 CloudTrail 有关 CloudTrail 定价的更多信息，请参阅AWS CloudTrail 定价。有关 Amazon S3 定价的信息，请参阅 Amazon S3 定价。

CloudTrail 湖泊事件数据存储

CloudTrail L@@ ak e 允许你对自己的事件运行基于 SQL 的查询。 CloudTrail Lake 将基于行的 JSON 格式的现有事件转换为 Apache ORC 格式。ORC 是一种针对快速检索数据进行优化的列式存储格式。事件将被聚合到事件数据存储中，它是基于您通过应用高级事件选择器选择的条件的不可变的事件集合。应用于事件数据存储的选择器用于控制哪些事件持续存在并可供您查询。有关 CloudTrail Lake 的更多信息，请参阅AWS CloudTrail 用户指南中的使用 AWS CloudTrail Lake。

CloudTrail 湖泊事件数据存储和查询会产生费用。创建事件数据存储时，您可以选择要用于事件数据存储的定价选项。定价选项决定了摄取和存储事件的成本，以及事件数据存储的默认和最长保留期。有关 CloudTrail 定价的更多信息，请参阅AWS CloudTrail 定价。

Oracle Database@AWS 中的管理事件 CloudTrail

管理事件提供有关对中的资源执行的管理操作的信息 AWS 账户。这些也称为控制面板操作。默认情况下， CloudTrail 记录管理事件。

Oracle Database@AWS 将所有 Oracle Database@AWS 控制平面操作记录为管理事件。

Oracle Database@AWS 事件示例

事件代表来自任何来源的单个请求，包括有关所请求的 API 操作、操作的日期和时间、请求参数等的信息。 CloudTrail 日志文件不是公共 API 调用的有序堆栈跟踪，因此事件不会按任何特定顺序出现。

以下示例显示了一个演示该`CreateOdbNetwork`操作 CloudTrail 的事件。

```
{
    "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"
    }
}
```

有关 CloudTrail 录音内容的信息，请参阅《AWS CloudTrail 用户指南》中的CloudTrail录制内容。

Oracle 数据库疑难解答@AWS

使用以下部分来帮助解决您可能遇到的网络问题 Oracle Database@AWS。

主题

- 创建 ODB 网络失败
- 您的 VPC 和 ODB 网络或虚拟机集群之间的连接问题
- 无法解析的主机名或来自 VPC 的虚拟机集群的扫描名
- 获取对 Oracle 数据库的支持@AWS

创建 ODB 网络失败

无法创建 ODB 网络时，常见原因如下：

受限的 CIDR 范围

ODB 网络对客户端和备份子网使用特定的 CIDR 范围。确保您为这些子网选择的 CIDR 范围不与任何受限或保留的 IP 地址范围重叠。

以下 CIDR 范围已保留，不能用于 ODB 网络：

- 甲骨文云预留范围：169.254.0.0/16
- D 类预留：224.0.0.0-239.255.255.255
- E 类预留：240.0.0.0-255.255.255.255
- OCI 的未来用途：100.105.0.0/16

遵守 VPC 文档中概述的 CIDR 范围 EC2 规则。要了解更多信息，请参阅 CIDR 区块关联限制。

此外，请避免指定的 CIDR 范围与用于 VPC 与 ODB 网络连接的 CIDR 范围重叠。

重叠的 VPC 网段

您为 ODB 网络指定的 CIDR 范围不应与任何现有网络使用的 CIDR 范围重叠。 VPCs重叠的 CIDR 范围可能会导致路由冲突并阻止 ODB 网络的成功创建。检查 ODB 对等互连的 CIDR 范围，确保 ODB 网络 CIDR 是唯一 VPCs 且不重叠的。

的所有权 VPCs

ODB 网络和您要连接的 VPC 必须归同一个 AWS 账户所有。如果您尝试将 ODB 网络与另一个账户拥有的 VPC 建立对等关系，则创建将失败。确认 ODB 网络和 VPC 均归同一个 AWS 账户所有。

缺少公交网关

如果您将 CIDR 范围添加到 ODB 网络对等 CIDR 列表中，但未将传输网关连接到 VPC，则创建或更新操作将失败。对使用该附件的 CIDR 范围没有要求。

您的 VPC 和 ODB 网络或虚拟机集群之间的连接问题

当您无法从 VPC 连接到 ODB 网络或其中的虚拟机集群时，常见原因如下：

- 验证 VPC 配置 — 在 Oracle Database@AWS 控制台中，找到与 ODB 网络建立对等关系的 VPC。确认 VPC ID 与 ODB 网络详细信息中显示的 ID 相匹配。
- 检查路由表-在 Amazon VPC 控制台中，找到附加到运行应用程序的子网的路由表。检查目的地 CIDR 与 ODB 网络的客户端子网 CIDR 匹配的路由。确认此路由指向正确的 ODB 网络 ARN。如果缺少路由，请在 ODB 网络的客户端子网 CIDR 中添加一条新路由。
- 验证对等互连 CIDRs-查看 ODB `Peered CIDRs` 网络详细信息中的部分。确认已列出您的 VPC 中的所有相关 CIDR 块。如果缺少必需的 CIDR，请更新对等设备。 CIDRs
- 检查安全组规则-在 Amazon EC2 控制台中，找到您的 VPC 中资源的安全组。查看入站和出站规则，根据需要对其进行更新以允许必要的流量。
- 确认可用区 — 在 Amazon VPC 控制台中，确定子网的可用区 (AZ)。验证 ODB 网络是否也部署在与您的子网相同的可用区中。
- 避免多个 ODB 网络对等连接 — 在控制台中检查您的 VPC 对等连接。 Oracle Database@AWS 确保与 ODB 网络只有一个活动连接。如果您看到多个 ODB 网络对等互连，请移除多余的 ODB 网络对等。

无法解析的主机名或来自 VPC 的虚拟机集群的扫描名

如果您的 VPC 无法解析虚拟机集群的主机名或扫描名，请在 VPC 上配置 DNS 转发和以下资源以解析 ODB 网络上托管的 DNS 记录：

- 用于向 ODB 网络发送 DNS 查询的出站终端节点。有关更多信息，请参阅 在 ODB 网络中配置出站终端节点 Oracle Database@AWS。

- 解析器规则，用于指定解析器转发到 DNS for ODB 网络的 DNS 查询的域名。有关更多信息，请参阅 在中配置解析器规则 Oracle Database@AWS。

获取对 Oracle 数据库的支持@AWS

了解如何获取 Oracle 数据库AWS@ 的信息和支持。

Oracle 支持范围和联系信息

Oracle Cloud Support 是为所有 Oracle Database@AWS 问题提供第一线支持。要联系支持人员，请登录 Oracle 云基础架构 (OCI) 控制台，然后选择救生筏图标。如果您没有 “我的 Oracle Cloud Support” 帐户，请参阅我的 Oracle 云支持 Support 账户和访问权限。

Oracle Support 可以帮助您解决的问题示例包括以下内容：

- 数据库连接问题 (Oracle TNS)
- 甲骨文数据库性能问题
- Oracle 数据库错误解决方案
- 与与服务相关的 OCI 租户通信相关的网络问题
- 增加配额（限制）以获得更多容量（有关更多信息，请参阅请求提高数据库资源的限制）
- 通过扩展为您的 Oracle 数据库基础架构增加更多计算和存储容量
- 新一代硬件升级
- 与您的 AWS Marketplace 费用相关的账单问题

如果您需要通过 OCI 控制台之外联系 Oracle 支持部门，请告知您的 Oracle 支持代理您的问题与 Oracle Databas AWS e@ 有关。这是因为对该服务的请求由专门负责这些部署的 OCI 支持团队处理。

通过电话联系 Oracle 支持人员

1. 致电 1-800-223-1711。如果您在美国境外，请访问 Oracle Support 联系人全球名录，查找您所在国家或地区的联系信息。
2. 选择选项 “2” 以打开新的服务请求 (SR)。
3. 为 “不确定” 选择选项 “4”。
4. 让代理知道您的多云系统存在问题，并告知产品名称。将代表您提出内部服务请求，OCI 支持工程师将直接与您联系。

您也可以向 Oracle 的 Cloud Cust omer Connect 社区中的多云论坛提交问题。此选项适用于所有客户。

我的 Oracle 云支持 Support 账户和访问权限

要创建 My Oracle Cloud Support 服务请求单，您所在组织的 Oracle Database@AWS 服务的管理员必须批准您的请求。如果你是 Oracle Database@AWS 管理员，请完成 Oracle Database@ 服务激活电子邮件中包含的 My Oracle Cloud S AWS upport 入职说明。

您可以在以下主题中找到有关使用 My Oracle Cloud Support 进行入门的说明：

- 配置您的 Oracle Support 账户
- 创建 Support 请求

有关批准用户打开 “我的 Oracle Cloud Support” 支持请求的说明，请参阅管理员支持任务。

AWS 支持 范围和联系信息

AWS 支持 是您为所有 AWS相关问题和问题提供第一线支持。像处理其他 AWS 服务一样，为你的问题提出 AWS 支持 理由。该 AWS 支持 团队根据需要与 OCI Support 合作。

AWS 支持 可以帮助您解决的 Oracle Database@AWS 问题示例包括以下内容：

- 虚拟网络问题，包括涉及网络地址转换 (NAT)、防火墙、DNS 和流量管理以及 AWS 子网的问题
- 堡垒和虚拟机 (VM) 问题，包括数据库主机连接、软件安装、延迟和主机性能
- 亚马逊内部的 Exadata 虚拟机集群指标报告 CloudWatch
- 与 AWS 服务相关的账单问题

有关信息 AWS 支持，请参阅入门 AWS 支持。

甲骨文服务级别协议

如果您对 Oracle Database@AWS 服务等级协议 (SLAs) 有疑问，或者想为违反 SLA 而申请服务积分，请联系您的 Oracle 客户经理。有关更多信息，请参阅服务级别协议。

Oracle 数据库的配额@AWS

Oracle Database@AWS 是一款多云产品。 AWS 不设置或强制执行 Oracle Database@AWS 资源配额。配额由 Oracle 云基础架构 (OCI) 强制执行。有关 OCI 配额的更多信息，请参阅 Oracle 云基础设施文档中的配额和服务限制。

《 Oracle Database@AWS 用户指南》的文档历史记录

下表描述了的文档版本 Oracle Database@AWS。

变更	说明	日期
Oracle Database@AWS 支持亚太地区（悉尼）地区和加拿大（中部）区域	您可以在这些区域创建您的 Oracle Database@AWS 资源。有关更多信息，请参阅支持的区域 Oracle Database@AWS。	2026年2月2日
Oracle Database@AWS 支持亚太地区（东京）区域、美国东部（俄亥俄州）区域、欧洲（法兰克福）区域	您可以在这些区域创建您的 Oracle Database@AWS 资源。有关更多信息，请参阅支持的区域 Oracle Database@AWS。	2025年12月22日
Oracle Database@AWS 支持跨权限共享 AWS 账户	现在，你可以使用 L AWS icens AWS e Manager 在同一个 AWS 组织 AWS 账户 中共享 Oracle Database@AWS 的 Marketplace 权限。有关更多信息，请参阅 Oracle 数据库 AWS中的授权共享 @。	2025 年 12 月 19 日
Oracle Database@AWS 支持修改零 ETL 集成数据过滤器	Oracle Database@AWS 支持修改与 Amazon Redshift 的现有零 ETL 集成的数据筛选器。您可以更新数据筛选模式，以便在数据复制中包括或排除指定的架构和表。有关更多信息，请参阅管理零 ETL 集成。	2025 年 10 月 15 日
Oracle Database@AWS 支持对等连接的对等网络 CIDR 管理	在创建或更新 ODB 对等连接 CIDRs 时，您可以指定对等网络。您可以控制对等 VPC 中	2025 年 10 月 10 日

	的哪些子网可以访问您的 ODB 网络。VPC 账户可以在不拥有 ODB 网络的情况下更新 CIDR 范围。有关更多信息，请参阅中的配置与 Amazon VPC 的 ODB 对等关系。 Oracle Database@AWS	
Oracle Database@AWS 支持与 Amazon Redshift 的零 ETL 集成	Oracle Database@AWS 现在已与 VPC Lattice 集成，实现与 Amazon Redshift 的零 ETL 集成。有关更多信息，请参阅 Oracle 数据库AWS的服务集成@。	2025 年 7 月 2 日
IAM 服务相关角色权限更新	现在，该AmazonODB ServiceRolePolicy 政策授予了描述 VPC 传输网关附件、描述亚马逊 EC2 子网和激活 Amazon EventBridge 来源的额外权限。有关更多信息，请参阅AWS 托管策略的Oracle Database@AWS 更新。	2025 年 6 月 30 日
IAM 服务相关角色权限更新	现在，该AmazonODB ServiceRolePolicy 策略授予了在 Amazon S EventBridge cheduler 中描述事件以及创建或描述事件总线的额外权限。有关更多信息，请参阅AWS 托管策略的Oracle Database@AWS 更新。	2025 年 6 月 26 日

Oracle Database@AWS 支持美国西部（俄勒冈）区域	您可以在美国西部（俄勒冈）区域创建您的 Oracle Database@AWS 资源。支持的物理 AZ IDs 是usw2-az3和usw2-az4。有关更多信息，请参阅支持的区域 Oracle Database@AWS。	2025 年 6 月 26 日
Oracle Database@AWS 支持跨资源共享 AWS 账户	现在，您可以使用 AWS Resource Access Manager ()AWS RAM与组织 AWS 账户内的其他人共享 Exadata 基础设施和虚拟机集群。您可以一次配置基础架构，然后在多个账户之间共享，从而在保持责任分工的同时降低成本。有关更多信息，请参阅 Oracle 数据库AWS中的资源共享 @。	2025 年 6 月 26 日
Oracle Database@AWS 支持 Amazon 中的活动 EventBridge	Oracle Database@AWS 向 Amazon 传送事件 EventBridge 以监控资源生命周期的变化。事件由两个源 AWS 和 OCI 源生成，允许您跟踪 ODB 网络、Exadata 基础架构、虚拟机群集和数据库的更改。有关更多信息，请参阅在 Amazon 中监控 Oracle Database@AWS 事件 EventBridge。	2025 年 6 月 26 日
Oracle Database@AWS 支持跨区域订阅	Oracle Database@AWS 支持跨区域订阅，允许您订阅一次即可使用所有可用 AWS 区域服务。有关更多信息，请参阅订阅多个区域的 Oracle Database@AWS。	2025 年 6 月 26 日

Oracle Database@AWS 支持 ODB 对等连接作为单独的资源	ODB 对等连接现在是一种单独的资源，专门 APIs 用于创建、查看和删除对等连接。您可以在同一个账户或不同账户中的 ODB 网络和 Amazon VPC 之间创建对等连接。有关更多信息，请参阅使用 ODB 对等连接。	2025 年 6 月 26 日
Oracle Database@AWS 将 ODB 网络与 Amazon S3 集成	Oracle Database@AWS 现在与 VPC Lattice 集成，允许 Oracle 托管备份到 Amazon S3，并可直接 ODB 网络访问亚马逊 S3。有关更多信息，请参阅 Oracle 数据库AWS的服务集成 @。	2025 年 6 月 26 日
Oracle Database@AWS 支持自主虚拟机集群	现在，您可以在 Exadata 基础架构上创建自治虚拟机集群。自治虚拟机集群是完全托管的数据库，可使用机器学习和 AI 自动执行关键管理任务。有关更多信息，请参阅中的步骤 3：创建 Exadata 虚拟机群集或自治虚拟机群集。 Oracle Database@AWS	2025 年 5 月 28 日
Oracle Database@AWS 支持可自定义的维护窗口	现在，您可以通过 Oracle 管理或客户管理的计划选项为 Exadata 基础架构配置维护窗口。您还可以选择修补模式（滚动或非滚动）并指定维护时间首选项。有关更多信息，请参阅中的创建 Oracle Exadata 基础架构。 Oracle Database@AWS	2025 年 5 月 1 日

Oracle Database@AWS 支持新的可用区 (AZ)	现在，您可以使用物理 ID `use1-az4` 或`use1-az6`在 AZ 中创建 ODB 网络。有关更多信息，请参阅 Oracle Exadata 基础架构。	2025 年 3 月 26 日
Oracle Database@AWS 支持 Amazon VPC 传输网关	如果您将传输网关连接到与 ODB 网络对等的 VPC，则可以将多个传输网关 VPCs 连接到该网关。在其中运行的应用程序 VPCs 可以访问在您的 ODB 网络中运行的 Exadata 虚拟机集群。有关更多信息，请参阅为其配置 Amazon VPC 传输网关 Oracle Database@AWS。	2025 年 3 月 26 日
Oracle Database@AWS 支持 Exadata X11M 的数据库和存储服务器类型	使用 Exadata X11M 创建基础架构时，可以指定数据库服务器类型和存储服务器类型。有关更多信息，请参阅中的创建 Oracle Exadata 基础架构。Oracle Database@AWS	2025 年 2 月 4 日
新的服务相关角色策略	Oracle Database@AWS `AmazonODBServiceRolePolicy` 为`AWSServiceRoleForODB` 服务相关角色添加了新策略。有关更多信息，请参阅 Oracle Database@AWS 对 AWS 托管式策略的更新。	2024 年 12 月 2 日
初始版本	《Oracle Database@AWS 用户指南》的初始版本	2024 年 12 月 2 日

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。