

# Oracle Cloud Infrastructureに Exadata DBシステムのデプロイ

ORACLE WHITE PAPER | 2018年8月

## 免責事項

下記事項は、弊社の一般的な製品の方向性に関する概要を説明するものです。また、情報提供を唯一の目的とするものであり、いかなる契約にも組み込むことはできません。マテリアルやコード、機能の提供をコミットメント(確約)するものではなく、購買を決定する際の判断材料になさらないで下さい。オラクルの製品に関して記載されている機能の開発、リリース、および時期については、弊社の裁量により決定されます。

## 改定履歴

このホワイト・ペーパーが初めて公開されて以降、次の改訂が加えられています。

| 日付         | 改訂内容 |
|------------|------|
| 2018年8月31日 | 初版公開 |

Oracle Cloud Infrastructureの最新版のホワイト・ペーパーは、

<https://cloud.oracle.com/iaas/technical-resources>にあります。

# 目次

|   |    |
|---|----|
| 概要  | 4  |
| Oracle Cloud Infrastructure上でのExadataの概要            | 4  |
| サポートされるデータベースのエディションとバージョン                          | 5  |
| Exadataデプロイのアクセス要件                                  | 5  |
| Oracle Cloud InfrastructureでExadata DBシステムを起動するステップ | 5  |
| ステップ1: VCNの作成                                       | 5  |
| ステップ2: インターネット・ゲートウェイの作成                            | 7  |
| ステップ3: サービス・ゲートウェイの作成                               | 7  |
| ステップ4: ルート表の作成                                      | 8  |
| ステップ5: セキュリティ・リストの作成                                | 10 |
| ステップ6: DHCPオプションの作成                                 | 12 |
| ステップ7: サブネットの作成                                     | 13 |
| ステップ8: セキュリティ・リストへのルールの追加                           | 17 |
| ステップ9: Exadata DBシステムの起動                            | 20 |
| ステップ10: コンソールからのExadata DBシステムへのアクセス                | 24 |
| ステップ11: Exadata DBシステムへの接続                          | 25 |
| サマリー  | 26 |

## 概要

このホワイト・ペーパーでは、Oracle Cloud InfrastructureへのExadata DBシステムのデプロイについて、順を追ってガイドラインを示します。このホワイト・ペーパーでは、一部のベスト・プラクティスの概要を説明します。Exadata実装の完全なリファレンス・ガイドとしての使用は意図していません。

このドキュメントでは、Oracle Cloud Infrastructureの様々なコンポーネントに関する基礎知識があると仮定します。

- [Oracle Cloud Infrastructureの基礎](#)
- [Oracle Cloud Infrastructure Networking](#) (特に、[仮想クラウド・ネットワーク \(VCN\)](#)、[サブネット](#)、[セキュリティ・リスト](#)および[ルート表](#))
- [Oracle Cloud Infrastructure Identity Access Management \(IAM\)](#)

## Oracle Cloud Infrastructure上のExadataの概要

Exadata DBシステムはクオータ・ラック、ハーフ・ラックまたはフル・ラックのコンピュート・ノードとストレージ・サーバーで構成されており、高速で低レイテンシのInfiniBandネットワークとインテリジェントなExadataソフトウェアで結び付けられています。自動バックアップの構成や、様々なワークロードの最適化、需要の増加に応じたシステムのスケール・アップが可能です。

各コンピュート・ノードには、仮想マシン(VM)が構成されています。コンピュート・ノードVMへのルート権限があるため、そこに追加のソフトウェアをロードして実行できます。ただし、物理的なコンピュート・ノード・ハードウェア、ネットワーク・スイッチ、配電ユニット(PDU)、Integrated Lights-Out Management (ILOM)インターフェース、Exadata Storage ServerなどのExadataインフラストラクチャ・コンポーネントに対する管理アクセス権はなく、すべてオラクル社が管理します。

データベースに対しては完全な管理権限があり、Oracle Net Servicesを使用して、Oracle Cloud Infrastructureの外からデータベースに接続できます。表領域の作成やデータベース・ユーザーの管理など、データベース管理タスクはお客様が行います。また、バックアップを含むデフォルトの自動メンテナンス設定のカスタマイズが可能で、データベース障害の発生時には、リカバリ・プロセスを完全に制御できます。

Oracle Cloud Infrastructureには、X6とX7という2つのバージョンのExadataがあり、どちらのバージョンにも3つのシェイプがあります。これらのシェイプの詳細は、Databaseサービスのドキュメントの「[Exadata DBシステム](#)」のトピックにある「[システム構成](#)」の項を参照してください。

---

**注意:** DATAディスク・グループの実際に使用可能なストレージは、Exadata DBシステムの起動時に選択するバックアップ・オプションによって異なります。詳細は、[Exadata DBシステムのドキュメント](#)を参照してください。

## サポートされるデータベースのエディションとバージョン

Exadata DBシステムには、Enterprise Edition - Extreme Performanceが必要です。このエディションでは、Oracle Database Enterprise Editionのすべての機能だけでなく、データベース・エンタープライズ管理パックすべてと、Oracle Database In-MemoryおよびOracle Real Application Clusters (RAC)などのEnterprise Editionのオプションすべてが提供されています。サポートされるソフトウェア・リリースのリストは、Databaseサービスのドキュメントの「[サポートされているデータベース・エディションおよびバージョン](#)」を参照してください。

## Exadataデプロイのアクセス要件

Oracle Cloud InfrastructureでExadataを起動するには、IAMポリシー経由で必要なアクセス権を付与されている必要があります。次に、テナント・レベルでグループDBAdminsに、このアクセス権を付与するサンプルのIAMポリシーを示します。特定コンパートメントのデータベース・システムのみにアクセス範囲を絞るには、テナントのかわりにそのコンパートメントを指定します。

```
Allow group DBAdmins to manage database-family in tenancy
```

また、SSH経由でDBシステムに接続する際に使用する公開鍵も必要です。

## Oracle Cloud InfrastructureでExadata DBシステムを起動するステップ

この項では、必要なネットワーキング・コンポーネントを作成し、Oracle Cloud InfrastructureでExadata DBシステムを起動するステップを説明します。Oracle Cloud Infrastructure NetworkingおよびDatabaseサービスのドキュメントの参照先で、詳細なステップを確認してください。

### ステップ1: VCNの作成

1. Oracle Cloud Infrastructureコンソールにサインインします。
2. 「[クラウド・ネットワークを作成するには](#)」のステップに従ってVCNを作成します。

この例では、「仮想クラウド・ネットワークの作成」ダイアログ・ボックスに次の値を入力しています。

- 「名前」に「ExaVCN」と入力します。
- 「仮想クラウド・ネットワークのみの作成」を選択します。

- 「CIDRブロック」に「10.0.0.0/16」と入力します。

**注意:** RFC 1918で指定されているプライベートIPアドレス範囲のいずれか(10.0.0.0/8、172.16/12および192.168/16)の使用をお薦めします。ただし、公にルーティング可能な範囲は使用できます。VCNのCIDRは、オンプレミスのネットワークやピアリングしている別のVCNとオーバーラップさせることはできません。詳細は、「[他のVCNへのアクセス: ピアリング](#)」を参照してください。

- 「このVCNでDNSホスト名を使用」チェック・ボックスを選択します。
- 「DNSラベル」に「exavcn」と入力します。

Create Virtual Cloud Network [help](#) [cancel](#)

CREATE IN COMPARTMENT [Nishant-POC](#)

NAME OPTIONAL

CREATE VIRTUAL CLOUD NETWORK ONLY  
 CREATE VIRTUAL CLOUD NETWORK PLUS RELATED RESOURCES

Creates a Virtual Cloud Network only. You'll still need to set up at least one Subnet, Gateway, and Route Rule to have a working Virtual Cloud Network.

CIDR BLOCK

Specified IP addresses: 10.0.0.0-10.0.255.255 (65,536 IP addresses)

DNS RESOLUTION [?](#)  
 USE DNS HOSTNAMES IN THIS VCN  
Allows assignment of DNS hostname when launching an Instance

DNS LABEL

Only letters and numbers, starting with a letter. 15 characters max.

DNS DOMAIN NAME (READ-ONLY)

TAGS

Tagging is a metadata system that allows you to organize and track resources within your tenancy. Tags are composed of keys and values which can be attached to resources.

[Learn more about tagging](#)

| TAG NAMESPACE   | TAG KEY              | VALUE                |
|---|----------------------|----------------------|
| <input type="text" value="None (apply a free-form tag)"/> | <input type="text"/> | <input type="text"/> |

View detail page after this resource is created

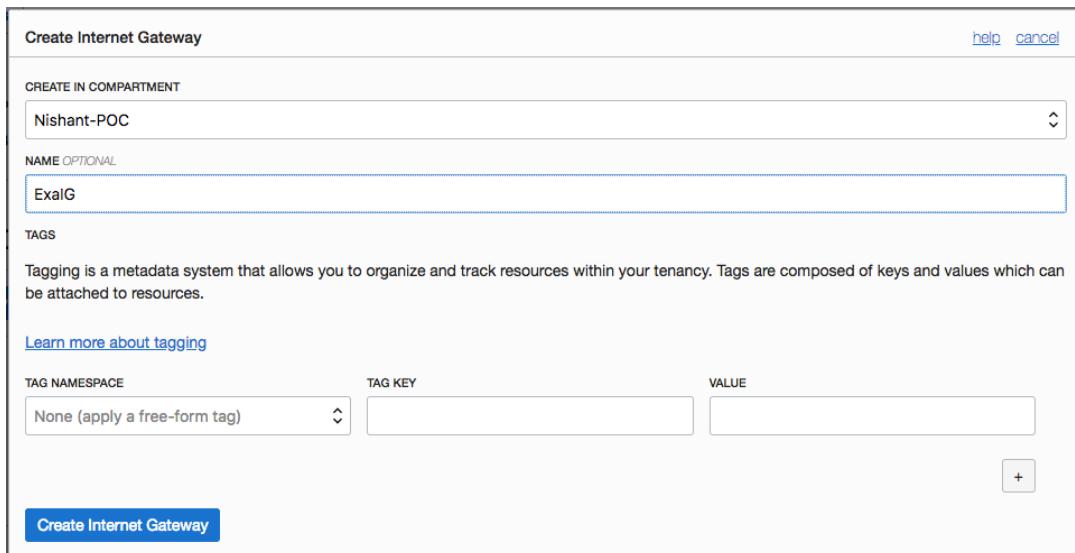
**Create Virtual Cloud Network**

VCNが作成されると、コンソールに表示されます。

## ステップ2: インターネット・ゲートウェイの作成

インターネット・ゲートウェイは、クラウド・ネットワークのエッジとインターネットを接続する仮想ルーターです。VCNで発生し、VCN外のパブリックIPアドレスを宛先とするトラフィックは、インターネット・ゲートウェイを通過します。

1. コンソールで、作成したVCNの名前をクリックします。
2. 「[インターネット・ゲートウェイを作成するには](#)」のステップに従って、インターネット・ゲートウェイを作成します。  
この例では、「インターネット・ゲートウェイの作成」ダイアログ・ボックスで、名前に「ExaIG」と入力しています。



The screenshot shows the 'Create Internet Gateway' dialog box. It has fields for 'CREATE IN COMPARTMENT' (set to 'Nishant-POC'), 'NAME OPTIONAL' (set to 'ExaIG'), and 'TAGS' (set to 'None (apply a free-form tag)'). A note about tagging is present, with a link to 'Learn more about tagging'. At the bottom is a 'Create Internet Gateway' button.

## ステップ3: サービス・ゲートウェイの作成

サービス・ゲートウェイを使用すると、VCN内のリソースがインターネット・ゲートウェイやNATを介さずに、Object StorageなどのOracle Cloud Infrastructureのパブリック・サービスにアクセスできます。サポートされているパブリック・サービスの1つを宛先とするVCNからのトラフィックは、ルーティングにはインスタンスのプライベートIPアドレスを使用し、Oracle Cloud Infrastructureのネットワーク・ファブリックを移動するため、インターネットを経由することはありません。そのため、サービス・ゲートウェイを作成し、それをバックアップ・ルート表に使用すれば、Exadataのバックアップは、Oracle Cloud Infrastructureのネットワーク・ファブリック経由でObject Storageに移動できます。

1. コンソールで、作成したVCNの名前をクリックします。
2. 「[タスク1: サービス・ゲートウェイの作成](#)」のステップに従って、サービス・ゲートウェイを作成します。この例では、「サービス・ゲートウェイの作成」ダイアログ・ボックスに次の値を入力しています。
  - 「名前」に「DemoSG」と入力します。

- 「サービス」で、「OCI LHRオブジェクト・ストレージ」を選択します。

Create Service Gateway

CREATE IN COMPARTMENT

Nishant-POC

NAME

DemoSG

SERVICES

OCI LHR Object Storage

Note: Make sure to add a route rule and security list rule for any subnet that needs to use the service gateway. [Learn more](#)

Create

## ステップ4: ルート表の作成

クラウド・ネットワークは仮想ルート表を使用して、VCNの外(インターネットやオンプレミスのネットワークなど)にトラフィックを送信します。これらの仮想ルート表には、すでに使い慣れている従来のネットワーク・ルート・ルールに、見かけも機能も類似しているルールがあります。各ルールは、宛先のCIDRブロックと、そのCIDRに一致する任意のトラフィックのターゲット(次のホップ)を指定します。Exadataでは、クライアント・トラフィックとバックアップ・トラフィック用に、2つのルート表を作成します。

- コンソールで、作成したVCNの名前をクリックします。
- 「ルート表を作成するには」のステップに従って、クライアント・トラフィックのルート表を作成します。クライアント・ルート表で、「ルート表の作成」ダイアログ・ボックスに次の値を入力します。
  - 「名前」に「Client\_RT」と入力します。
  - 「ルート・ルール」セクション:
    - ターゲット・タイプ: インターネット・ゲートウェイ
    - 宛先CIDRブロック: 0.0.0.0/0
    - コンパートメント名: インターネット・ゲートウェイが配置されているコンパートメント。
    - ターゲット・インターネット・ゲートウェイ: ステップ2で作成したインターネット・ゲートウェイ(この例ではExaIG)。

Create Route Table

CREATE IN COMPARTMENT

Nishant-POC

NAME

Client\_RT

Route Rules

Important: For a route rule that targets a Private IP, you must first enable "Skip Source/Destination Check" on the VNIC that the Private IP is assigned to.

| TARGET TYPE      | DESTINATION CIDR BLOCK | COMPARTMENT | TARGET INTERNET GATEWAY |
|------------------|------------------------|-------------|-------------------------|
| Internet Gateway | 0.0.0/0                | Nishant-POC | ExaIG                   |

Specified IP addresses: 0.0.0-255.255.255 (4,294,967,296 IP addresses)

+ Another Route Rule

TAGS

Tagging is a metadata system that allows you to organize and track resources within your tenancy. Tags are composed of keys and values which can be attached to resources.

[Learn more about tagging](#)

| TAG NAMESPACE                | TAG KEY | VALUE |
|------------------------------|---------|-------|
| None (apply a free-form tag) |         |       |

+ Create Route Table

3. 「ルート表を作成するには」のステップに従って、バックアップ・トラフィックのルート表を作成します。

バックアップ・ルート表で、「ルート表の作成」ダイアログ・ボックスに次の値を入力します。

- 「名前」に「Backup\_RT」と入力します。
- 「ルート・ルール」セクション:
  - ターゲット・タイプ: サービス・ゲートウェイ
  - 宛先サービス: OCI LHRオブジェクト・ストレージ
  - コンパートメント名: サービス・ゲートウェイが配置されているコンパートメント。
  - ターゲット・サービス・ゲートウェイ: ステップ3で作成したサービス・ゲートウェイ(この例ではDemoSG)。

Create Route Table

CREATE IN COMPARTMENT

Nishant-POC

NAME

Backup\_RT

Route Rules

Important: For a route rule that targets a Private IP, you must first enable "Skip Source/Destination Check" on the VNIC that the Private IP is assigned to.

| TARGET TYPE     | DESTINATION SERVICE  | COMPARTMENT | TARGET SERVICE GATEWAY |
|-----------------|----------------------|-------------|------------------------|
| Service Gateway | OCI LHR Object St... | Nishant-POC | DemoSG                 |

+ Another Route Rule

TAGS

Tagging is a metadata system that allows you to organize and track resources within your tenancy. Tags are composed of keys and values which can be attached to resources.

[Learn more about tagging](#)

| TAG NAMESPACE                | TAG KEY | VALUE |
|------------------------------|---------|-------|
| None (apply a free-form tag) |         |       |

+ Additional Tag

Create Route Table

## ステップ5: セキュリティ・リストの作成

セキュリティ・リストは、許可されるインバウンドとアウトバウンドのトラフィック・タイプを指定するイングレスとエグレスのルールを使用して、インスタンスの仮想ファイアウォールを提供します。各セキュリティ・リストは、インスタンス・レベルで強制されます。ただし、セキュリティ・リストを構成するのはサブネット・レベルで、指定されたサブネット内のすべてのインスタンスが同じルール・セットの対象になることを意味します。

各サブネットにアタッチできるセキュリティ・リストは最大で5つです。サブネットが作成されたら、セキュリティ・リストの追加や削除はできません。ただし、イングレス・ルールとエグレス・ルールは、いつでもセキュリティ・リストに追加できます。

Oracle Cloud Infrastructure上のExadataには、ユーザー・データ用のクライアント・サブネットと、バックアップ・トラフィック用のバックアップ・サブネットという、2つの別々のVCNサブネットが必要です(これらのサブネットを作成する手順はステップ7に記載されています)。このステップでは、サブネットで使用する、次の9つのセキュリティ・リストを作成します。9つすべてのセキュリティ・リストがすぐに必要なわけではありませんが、後からはサブネットにリストを追加できないため、許可されている最大数のセキュリティ・リストをサブネットにアタッチすることをお薦めします。

- **NodeTraffic:** Exadataノードと、クライアント・サブネットとバックアップ・サブネット間のTCPとICMPのトラフィック間の通信用。このセキュリティ・リストは、クライアント・サブネットとバックアップ・サブネットの両方で共有されます。

- **SSH\_Traffic:** SSH トライアック用。
- **SQLNet:** SQL Net トライアック用。
- **Client1:** クライアント・トライアック用。
- **Client2:** クライアント・トライアック用。
- **DB\_Backup1:** Object Storageへのバックアップ・トライアック。
- **DB\_Backup2:** Object Storageへのバックアップ・トライアック。
- **Flex1:** 将来使用するためのフレックス・セキュリティ・リスト。
- **Flex2:** 将来使用するためのフレックス・セキュリティ・リスト。

---

**注意:** VCNの作成時に作られたデフォルトのセキュリティ・リストの使用はお薦めしません。SQLNetトライアックを開くために、デフォルトのセキュリティ・リストにルールを追加すると、それらのルールは、デフォルトのセキュリティ・リストがアタッチされているすべてのサブネットに適用されます。

---

リストに先ほどの名前を使用して、9つの空のセキュリティ・リストを作成します。後続の項で、セキュリティ・リストにイングレス・ルールとエグレス・ルールを追加します。

1. コンソールで、作成したVCNの名前をクリックします。
2. 「[新しいセキュリティ・リストを作成するには](#)」のステップに従って、9つのセキュリティ・リストを作成します。

この例では、「[セキュリティ・リストの作成](#)」ダイアログ・ボックスに次の値を入力しています。

- セキュリティ・リストの名前を入力します。使用する名前は、先ほどのリストを参照してください。
- イングレス・ルールとエグレス・ルールのデフォルトのエントリを削除します。

次の図では、**NodeTraffic**セキュリティ・リストに入力する値の例を示しています。

Create Security List

CREATE IN COMPARTMENT

Nishant-POC

SECURITY LIST NAME

NodeTraffic

Allow Rules for Ingress

+ Add Rule

Allow Rules for Egress

+ Add Rule

TAGS

Tagging is a metadata system that allows you to organize and track resources within your tenancy. Tags are composed of keys and values which can be attached to resources.

[Learn more about tagging](#)

TAG NAMESPACE

None (apply a free-form tag)

TAG KEY

VALUE

+ Additional Tag

Create Security List

## ステップ6: DHCPオプションの作成

VCNはDHCPオプションを使用して、インスタンスの起動時に、構成情報を自動的にインスタンスに提供します。各VCNには、DHCPオプションのセットがデフォルトで組み込まれており、初期値は変更可能です。このステップでは、Exadata用に別のDHCPオプションを作成します。

1. コンソールで、作成したVCNの名前をクリックします。
2. 「[DHCPオプションの新しいセットを作成するには](#)」のステップに従って、DHCPオプションの新しいセットを作成します。

この例では、「**DHCPオプションの作成**」ダイアログ・ボックスに次の値を入力しています。

- 「名前」に「ExaDHCP」と入力します。
- 「DNSタイプ」で、「インターネットおよびVCNリゾルバ」を選択します。
- 「検索ドメイン」ボックスはブランクのままにするか、値(たとえば、oraclevcn.com)を入力します。

## ステップ7: サブネットの作成

サブネットはVCNの下位区分です。VCNの各サブネットは単一の可用性ドメインに存在し、クラウド・ネットワークの他のサブネットとオーバーラップしない、連続したIPアドレスの範囲で構成されます。VCNおよびサブネットの詳細は、「[VCNとサブネットの操作](#)」を参照してください。

次のステップに従って、クライアント・サブネットとバックアップ・サブネットを作成します。

1. コンソールで、作成したVCNの名前をクリックします。
2. 「リソース」セクションで、「サブネット」をクリックします。
3. 「サブネットの作成」をクリックします。
4. 「サブネットの作成」ダイアログ・ボックスに、次の値を入力してクライアント・サブネットを作成します。
  - サブネットの名前を入力します(この例では**Client\_Subnet\_AD1**)。
  - Exadata DBシステムを起動する可用性ドメインを選択します。
  - サブネットのCIDRブロックを入力します(この例では**10.0.3.0/24**)。
  - クライアント・トラフィック用に作成したルート表を選択します(この例では**Client\_RT**)。

- 「サブネット・アクセス」に、「パブリック・サブネット」を選択します。

**注意:** 本番環境では、「プライベート・サブネット」を選択します。

- 「DNS解決」チェック・ボックスが選択されていることを確認してください。
- 「DNSラベル」はデフォルト値のままにします。
- 「DHCPオプション」で、ステップ6で作成したDHCPオプション(ExaDHCPなど)を選択します。
- 次の5つのセキュリティ・リストを選択します。
  - NodeTraffic
  - Client1
  - Client2
  - SQLNet
  - Flex1

**Create Subnet**

If the Route Table, DHCP Options, or Security Lists are in a different Compartment than the Subnet, [click here](#) to enable Compartment selection for those resources.

**NAME (OPTIONAL)**  
Client\_Subnet\_AD1

**AVAILABILITY DOMAIN**  
eurR:UK-LONDON-1-AD-1

**CIDR BLOCK**  
10.0.3.0/24  
Specified IP addresses: 10.0.3.0-10.0.3.255 (256 IP addresses)

**ROUTE TABLE**  
Client\_RT

**SUBNET ACCESS**

PRIVATE SUBNET  
Prohibit public IP addresses for Instances in this Subnet

PUBLIC SUBNET  
Allow public IP addresses for Instances in this Subnet

**DNS RESOLUTION**  
 USE DNS HOSTNAMES IN THIS SUBNET  
Allows assignment of DNS hostname when launching an Instance

**DNS LABEL**  
clientsubnetad1  
Only letters and numbers, starting with a letter. 15 characters max.

**DNS DOMAIN NAME (READ-ONLY)**  
clientsubnetad1.exavcn.oraclevcn.com

**DHCP OPTIONS**  
ExaDHCP

DHCP OPTIONS

ExaDHCP

Security Lists

- NodeTraffic
- Client1
- Client2
- SQLNet
- Flex1

TAGS

Tagging is a metadata system that allows you to organize and track resources within your tenancy. Tags are composed of keys and values which can be attached to resources.

[Learn more about tagging](#)

| TAG NAMESPACE                | TAG KEY | VALUE |
|------------------------------|---------|-------|
| None (apply a free-form tag) |         |       |

+ Additional Tag

Create

- 「作成」をクリックします。
- ステップ3から5を繰り返してバックアップ・サブネットを作成し、「サブネットの作成」ダイアログ・ポックスに次の値を入力します。
  - サブネットの名前を入力します(この例では**Backup\_Subnet\_AD1**)。
  - Exadata DBシステムを起動する可用性ドメインを選択します。
  - サブネットのCIDRブロックを入力します(この例では**10.0.4.0/24**)。
  - バックアップ・トラフィック用に作成したルート表を選択します(この例では**Backup\_RT**)。
  - 「サブネット・アクセス」に、「パブリック・サブネット」を選択します。

**注意:** 本番環境では、「プライベート・サブネット」を選択します。

- 「DNS解決」チェック・ボックスが選択されていることを確認してください。
- 「DNSラベル」はデフォルト値のままにします。
- 「DHCPオプション」で、ステップ6で作成したDHCPオプション(**ExaDHCP**など)を選択します。

- 次の5つのセキュリティ・リストを選択します。

- NodeTraffic
- DB\_Backup1
- DB\_Backup2
- SSH\_Traffic
- Flex2

**Create Subnet** help cancel

If the Route Table, DHCP Options, or Security Lists are in a different Compartment than the Subnet, [click here](#) to enable Compartment selection for those resources.

**NAME (OPTIONAL)**  
Backup\_Subnet\_AD1

**AVAILABILITY DOMAIN**  
eurR:UK-LONDON-1-AD-1

**CIDR BLOCK**  
10.0.4.0/24  
Specified IP addresses: 10.0.4.0-10.0.4.255 (256 IP addresses)

**ROUTE TABLE**  
Backup\_RT

**SUBNET ACCESS**

**PRIVATE SUBNET**  
Prohibit public IP addresses for Instances in this Subnet

**PUBLIC SUBNET**  
Allow public IP addresses for Instances in this Subnet

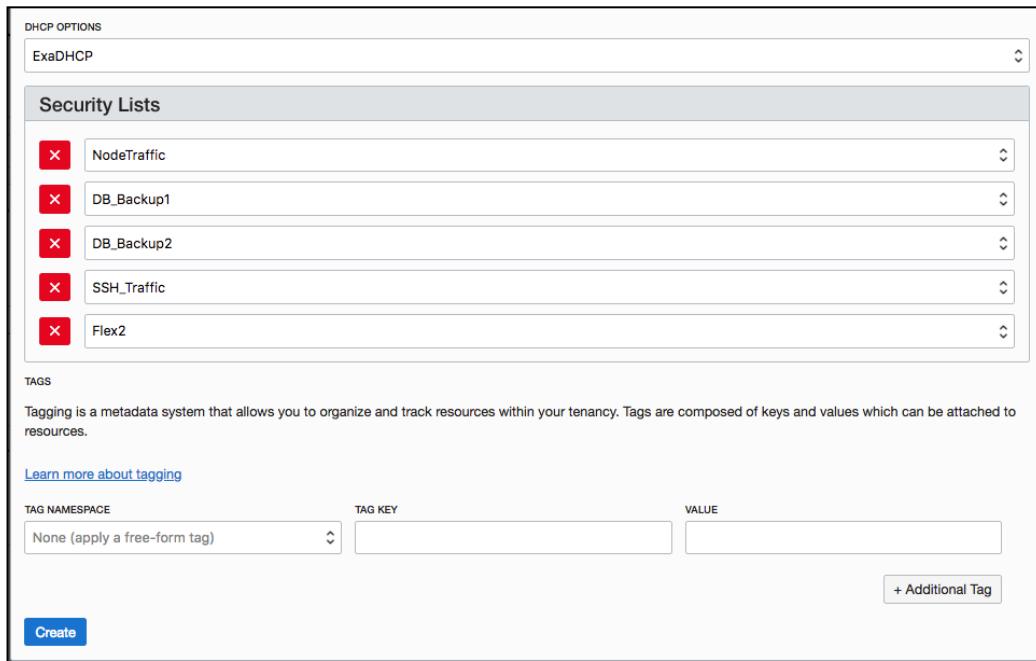
**DNS RESOLUTION**  
 **USE DNS HOSTNAMES IN THIS SUBNET** ?  
Allows assignment of DNS hostname when launching an Instance

**DNS LABEL**  
backupssubnetad1

Only letters and numbers, starting with a letter, 15 characters max.

**DNS DOMAIN NAME (READ-ONLY)**  
backupssubnetad1.exavcn.oraclevcn.com

**DHCP OPTIONS**  
ExaDHCP



## ステップ8: セキュリティ・リストへのルールの追加

これで、クライアントとバックアップの両方のサブネットにIP CIDRができたので、セキュリティ・リストを更新して、トライフィックを許可する適切なイングレス・ルールとエグレス・ルールを追加します。

1. コンソールで、作成したVCNの名前をクリックします。
2. 「リソース」セクションで、「セキュリティ・リスト」をクリックします。
3. 「NodeTraffic」セキュリティ・リストをクリックします。
4. 「すべてのルールの編集」をクリックします。
5. 次のイングレス・ルールを追加して、TCPおよびICMPトライフィックが両方のサブネット間を移動できるようにします。
  - CIDR 10.0.3.0/24 TCP すべて すべて
  - CIDR 10.0.3.0/24 ICMP すべて すべて
  - CIDR 10.0.4.0/24 TCP すべて すべて
  - CIDR 10.0.4.0/24 ICMP すべて すべて



Edit Security List Rules

SECURITY LIST NAME: NodeTraffic [help](#) [cancel](#)

**Allow Rules for Ingress**

|  |                   |                          |                   |                                   |  |
|--|-------------------|--------------------------|-------------------|-----------------------------------|--|
| <input checked="" type="checkbox"/> STATELESS  | SOURCE TYPE: CIDR | SOURCE CIDR: 10.0.3.0/24 | IP PROTOCOL: TCP  | SOURCE PORT RANGE (OPTIONAL): All | DESTINATION PORT RANGE (OPTIONAL): All |
| <small>(more information)</small><br><small>Allows TCP traffic for ports: all</small>            |                   |                          |                   |                                   |  |
| <input checked="" type="checkbox"/> STATELESS  | SOURCE TYPE: CIDR | SOURCE CIDR: 10.0.3.0/24 | IP PROTOCOL: ICMP | TYPE AND CODE (OPTIONAL): All     |  |
| <small>(more information)</small><br><small>Allows ICMP traffic for: all types and codes</small> |                   |                          |                   |                                   |  |
| <input checked="" type="checkbox"/> STATELESS  | SOURCE TYPE: CIDR | SOURCE CIDR: 10.0.4.0/24 | IP PROTOCOL: TCP  | SOURCE PORT RANGE (OPTIONAL): All | DESTINATION PORT RANGE (OPTIONAL): All |
| <small>(more information)</small><br><small>Allows TCP traffic for ports: all</small>            |                   |                          |                   |                                   |  |
| <input checked="" type="checkbox"/> STATELESS  | SOURCE TYPE: CIDR | SOURCE CIDR: 10.0.4.0/24 | IP PROTOCOL: ICMP | TYPE AND CODE (OPTIONAL): All     |  |
| <small>(more information)</small><br><small>Allows ICMP traffic for: all types and codes</small> |                   |                          |                   |                                   |  |

[+ Add Rule](#)

## 6. 次のエグレス・ルールを追加します。

- CIDR 10.0.3.0/24 TCP すべて すべて
- CIDR 10.0.3.0/24 ICMP すべて すべて
- CIDR 10.0.4.0/24 TCP すべて すべて
- CIDR 10.0.4.0/24 ICMP すべて すべて

Allow Rules for Egress

|  |      |                  |             |                              |                                   |
|--|------|------------------|-------------|------------------------------|-----------------------------------|
| DESTINATION TYPE                             | CIDR | DESTINATION CIDR | TCP         | SOURCE PORT RANGE (OPTIONAL) | DESTINATION PORT RANGE (OPTIONAL) |
| <input type="checkbox"/>                     | CIDR | 10.0.3.0/24      | TCP         | All                          | All                               |
| STATELESS<br>(more information)              |      |                  |             |                              |                                   |
| Allows TCP traffic for ports: all            |      |                  |             |                              |                                   |
| DESTINATION TYPE                             | CIDR | DESTINATION CIDR | IP PROTOCOL | TYPE AND CODE (OPTIONAL)     |                                   |
| <input type="checkbox"/>                     | CIDR | 10.0.3.0/24      | ICMP        | All                          |                                   |
| STATELESS<br>(more information)              |      |                  |             |                              |                                   |
| Allows ICMP traffic for: all types and codes |      |                  |             |                              |                                   |
| DESTINATION TYPE                             | CIDR | DESTINATION CIDR | IP PROTOCOL | SOURCE PORT RANGE (OPTIONAL) | DESTINATION PORT RANGE (OPTIONAL) |
| <input type="checkbox"/>                     | CIDR | 10.0.4.0/24      | TCP         | All                          | All                               |
| STATELESS<br>(more information)              |      |                  |             |                              |                                   |
| Allows TCP traffic for ports: all            |      |                  |             |                              |                                   |
| DESTINATION TYPE                             | CIDR | DESTINATION CIDR | IP PROTOCOL | TYPE AND CODE (OPTIONAL)     |                                   |
| <input type="checkbox"/>                     | CIDR | 10.0.4.0/24      | ICMP        | All                          |                                   |
| STATELESS<br>(more information)              |      |                  |             |                              |                                   |
| Allows ICMP traffic for: all types and codes |      |                  |             |                              |                                   |

+ Add Rule

Save Security List Rules

- 「セキュリティ・リスト・ルールの保存」をクリックします。
- 「SSH\_Traffic」セキュリティ・リストをクリックします。
- 「すべてのルールの編集」をクリックします。
- 次のイングレス・ルールの値を追加します。

CIDR 0.0.0.0/0 TCP 22 22

Edit Security List Rules

SECURITY LIST NAME

SSH\_Traffic

Allow Rules for Ingress

|  |             |             |                              |                                   |
|--|-------------|-------------|------------------------------|-----------------------------------|
| SOURCE TYPE  | SOURCE CIDR | IP PROTOCOL | SOURCE PORT RANGE (OPTIONAL) | DESTINATION PORT RANGE (OPTIONAL) |
| <input type="checkbox"/>                                   | CIDR        | TCP         | 22                           | 22                                |
| STATELESS<br>(more information)                            |             |             |                              |                                   |
| Allows TCP traffic for ports: 22 SSH Remote Login Protocol |             |             |                              |                                   |

+ Add Rule

Allow Rules for Egress

+ Add Rule

Save Security List Rules

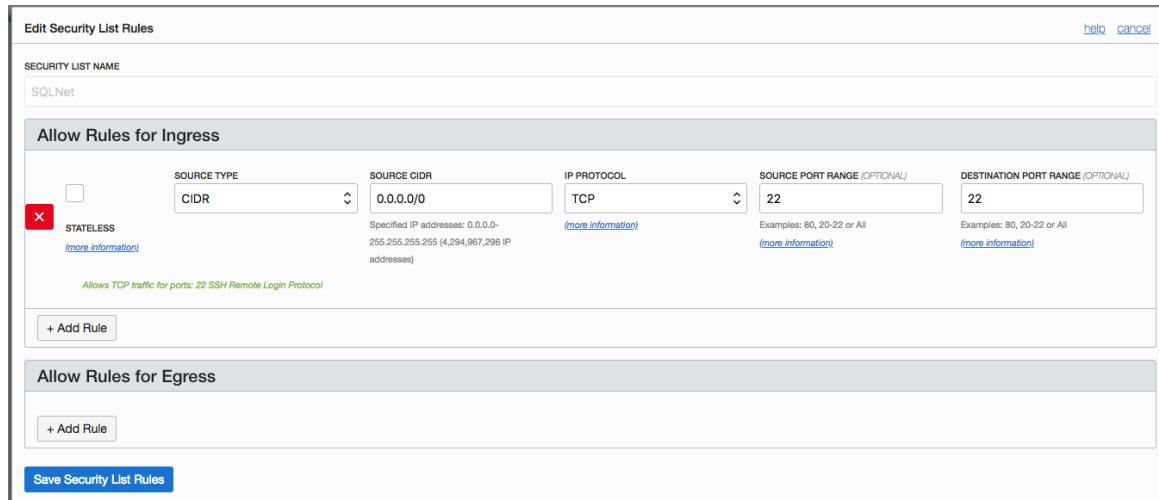
- 「セキュリティ・リスト・ルールの保存」をクリックします。

12. 「SQLNet」セキュリティ・リストをクリックします。

13. 「すべてのルールの編集」をクリックします。

14. 次のイングレス・ルールの値を追加します。

CIDR 0.0.0.0/0 TCP 22 22



Security List Name: SQLNet

Allow Rules for Ingress

| STATELESS                           | SOURCE CIDR | IP PROTOCOL | SOURCE PORT RANGE (OPTIONAL) | DESTINATION PORT RANGE (OPTIONAL) |
|-------------------------------------|-------------|-------------|------------------------------|-----------------------------------|
| <input checked="" type="checkbox"/> | 0.0.0.0/0   | TCP         | 22                           | 22                                |

Allows TCP traffic for ports: 22 SSH Remote Login Protocol

+ Add Rule

Allow Rules for Egress

+ Add Rule

Save Security List Rules

15. 「セキュリティ・リスト・ルールの保存」をクリックします。

**注意:** お客様の会社のセキュリティ・ポリシーで許可されているとおりに、イングレスとエグレスのセキュリティ・ルールを追加します。これらの例では0.0.0.0/0を使用していますが、これはデモ専用です。

## ステップ9: Exadata DBシステムの起動

これで、Exadata DBシステムとシステムの起動に必要なすべてのネットワーキング・コンポーネントが作成されました。

1. コンソールで、ナビゲーション・メニューを開きます。「データベース」の下で、「ペア・メタル、VMおよびExadata」をクリックします。
2. コンパートメントを選択します。
3. 「DBシステムの起動」をクリックします。
4. 「DBシステムの起動」ダイアログ・ボックスに、次の値を入力します。このダイアログ・ボックスのフィールドに関する詳細は、「[Exadata DBシステムを起動するには](#)」を参照してください。
  - Exadata DBシステムの表示名(DemoExaCSなど)を入力します。

- Exadata DBシステムを配置する可用性ドメインを選択します。
- 「シェイプ・タイプ」に、「ペア・メタル・マシン」を選択します。
- シェイプ(**Exadata.Quarter1.84**など)を選択します。
- クラスタ名(**ExaCluster**など)を入力します。
- CPUコア数(**22**など)を入力します。
- ライセンス・タイプを選択します。

Launch DB System help cancel

If the Virtual Cloud Network or Subnet is in a different Compartment than the DB System, [click here](#) to enable Compartment selection for those resources.

**DB System Information**

DISPLAY NAME

AVAILABILITY DOMAIN

SHAPE TYPE  VIRTUAL MACHINE  BARE METAL MACHINE

SHAPE

TOTAL NODE COUNT

ORACLE DATABASE SOFTWARE EDITION

CLUSTER NAME (Optional)

CPU CORE COUNT

The number of CPU cores to enable on the DB System. Specify a multiple of 2, up to 84.

LICENSE TYPE  LICENSE INCLUDED  
Includes the cost of Oracle Cloud Infrastructure and Oracle Database licenses.

BRING YOUR OWN LICENSE (BYOL)  
Includes the cost of Oracle Cloud Infrastructure but excludes Oracle Database licenses. You purchased your Database licenses directly from Oracle.

- SSH鍵(公開鍵)のアップロードまたは貼付けを選択します。
- データ・ストレージの割合(**80%**など)を選択します。
- 「仮想クラウド・ネットワーク」に、作成したVCN(**ExaVCN**など)を選択します。
- 「クライアント・サブネット」に、作成したクライアント・サブネット(**Client\_Subnet\_AD1**など)を選択します。
- 「バックアップ・サブネット」に、作成したバックアップ・サブネット(**Backup\_Subnet\_AD1**など)を選択します。
- ホスト名接頭辞(**exanode**など)を入力します。

BRING YOUR OWN LICENSE (BYOL)  
Includes the cost of Oracle Cloud Infrastructure but excludes Oracle Database licenses. You purchased your Database licenses directly from Oracle.

SSH PUBLIC KEY  
 CHOOSE SSH KEY FILES  
 PASTE SSH KEYS

Choose SSH Key files (.pub) from your computer:

DATA STORAGE PERCENTAGE  
80%

DISK REDUNDANCY  
High

High disk redundancy (3-way mirroring) is required for all Exadata shapes.

**Network Information**

VIRTUAL CLOUD NETWORK  
ExaVCN

CLIENT SUBNET  
Client\_Subnet\_AD1

BACKUP SUBNET  
Backup\_Subnet\_AD1

HOSTNAME PREFIX  
exanode

- データベース名(**exadb**など)を入力します。
- データベース・バージョン(**18.0.0.0**など)を選択します。
- Oracle Databaseバージョン12以降を選択した場合は、PDB名(**pdb1**など)を入力します。
- データベース管理パスワードを入力して確認します。
- データベース・ワーカロード(OLTPまたはDSS)を選択します。

HOSTNAME PREFIX  
exanode

HOST DOMAIN NAME  
clientsubnetad1.exavcn.oraclevcn.com

HOST AND DOMAIN URL  
exanode.clientsubnetad1.exavcn.oraclevcn.com

### Database Information

DATABASE NAME  
exadb

DATABASE VERSION  
18.0.0.0

PDB NAME (Optional)  
pdb1

DATABASE ADMIN PASSWORD  
\*\*\*\*\*  
Password must be 9 to 30 characters and contain at least 2 uppercase, 2 lowercase, 2 special, and 2 numeric characters. The special characters must be \_, #, or -.

CONFIRM DATABASE ADMIN PASSWORD  
\*\*\*\*\*  
Confirmation must match password above.

DATABASE WORKLOAD  
 ON-LINE TRANSACTION PROCESSING (OLTP)  
 Configure the database for a transactional workload, with bias towards high volumes of random data access.

DATABASE WORKLOAD  
 ON-LINE TRANSACTION PROCESSING (OLTP)  
 Configure the database for a transactional workload, with bias towards high volumes of random data access.

DECISION SUPPORT SYSTEM (DSS)  
 Configure the database for a decision support or data warehouse workload, with bias towards large data scanning operations.

[Hide Advanced Options](#)

CHARACTER SET  
AL32UTF8

NATIONAL CHARACTER SET  
AL16UTF16

TAGS  
Tagging is a metadata system that allows you to organize and track resources within your tenancy. Tags are composed of keys and values which can be attached to resources.

[Learn more about tagging](#)

| TAG NAMESPACE                | TAG KEY | VALUE |
|------------------------------|---------|-------|
| None (apply a free-form tag) |         |       |

+ Additional Tag

[Launch DB System](#)

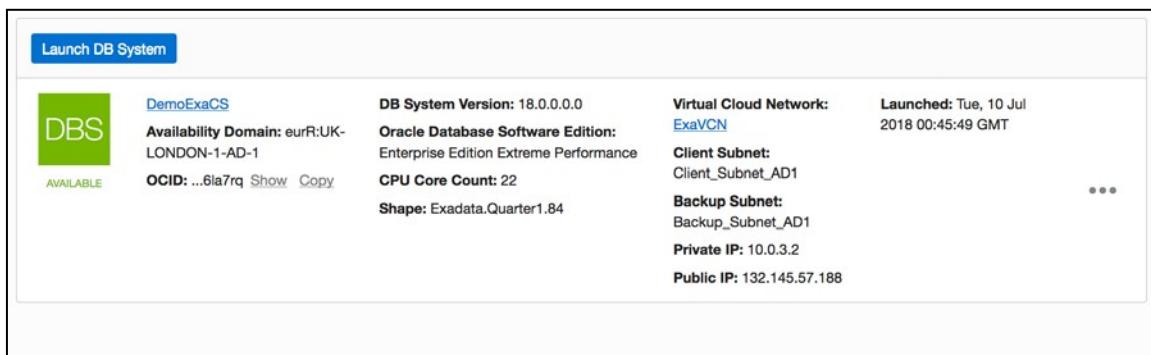
5. 「DBシステムの起動」をクリックします。

## ステップ10: コンソールからのExadata DBシステムへのアクセス

Exadata DBシステムにはOracle Cloud Infrastructureコンソールからアクセスし、ノードのIPアドレスやその他の情報を取得できます。追加のデータベースの作成や、ノードの停止と再起動を実行可能です。詳細は、「[Exadata DBシステムの管理](#)」を参照してください。

1. コンソールで、ナビゲーション・メニューを開きます。「データベース」の下で、「ペア・メタル、VMおよびExadata」をクリックします。
2. コンパートメントを選択します。

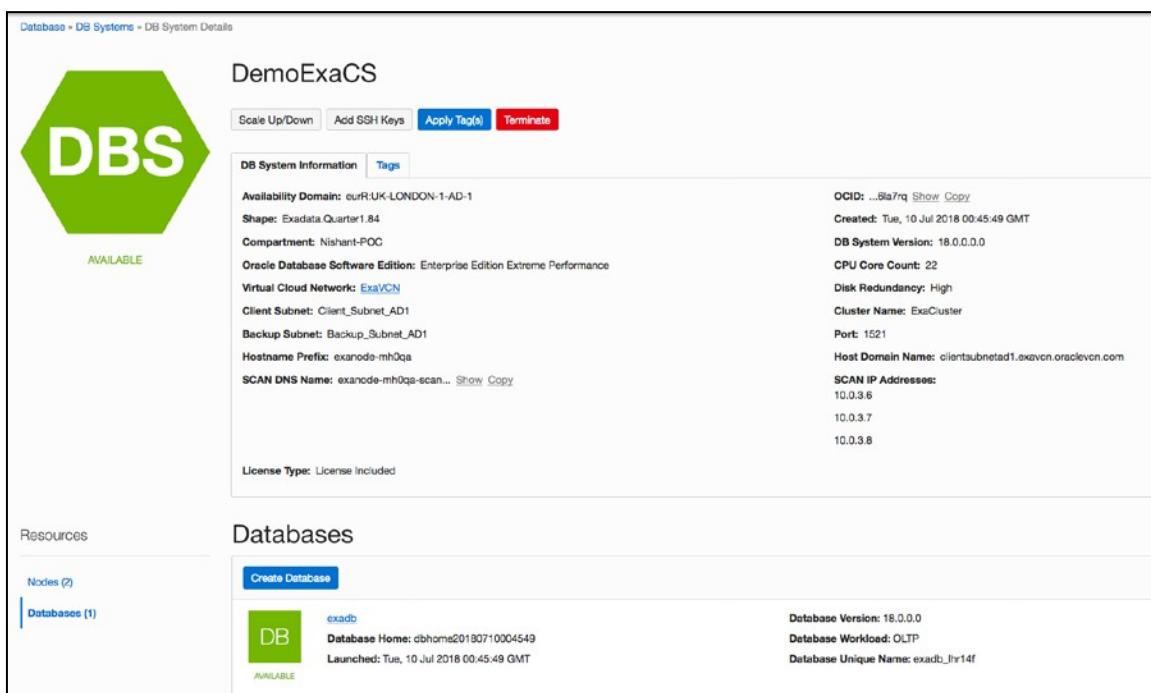
コンパートメント内のExadata DBシステムがリストされています。



The screenshot shows the 'Launch DB System' button at the top. Below it is a table with the following data:

|  |   |   |   |  |
|--|---|---|---|--|
| <br>AVAILABLE | <b>DemoExaCS</b><br>Availability Domain: eurR:UK-LONDON-1-AD-1<br>OCID: ...6la7rq <a href="#">Show</a> <a href="#">Copy</a> | <b>DB System Version:</b> 18.0.0.0.0<br><b>Oracle Database Software Edition:</b> Enterprise Edition Extreme Performance<br><b>CPU Core Count:</b> 22<br><b>Shape:</b> Exadata.Quarter1.84 | <b>Virtual Cloud Network:</b> ExaVCN<br><b>Client Subnet:</b> Client_Subnet_AD1<br><b>Backup Subnet:</b> Backup_Subnet_AD1<br><b>Private IP:</b> 10.0.3.2<br><b>Public IP:</b> 132.145.57.188 | <b>Launched:</b> Tue, 10 Jul 2018 00:45:49 GMT |
|--|---|---|---|--|

3. 詳細を表示するシステムの名前をクリックします。



The screenshot shows the 'DemoExaCS' system details. The top navigation bar includes 'Scale Up/Down', 'Add SSH Keys', 'Apply Tag(s)', and 'Terminate' buttons. The 'DB System Information' tab is selected, showing the following details:

|  |   |
|--|---|
| Availability Domain: eurR:UK-LONDON-1-AD-1                               | OCID: ...6la7rq <a href="#">Show</a> <a href="#">Copy</a> |
| Shape: Exadata.Quarter1.84   | Created: Tue, 10 Jul 2018 00:45:49 GMT                    |
| Compartment: Nishant-POC   | DB System Version: 18.0.0.0.0                             |
| Oracle Database Software Edition: Enterprise Edition Extreme Performance | CPU Core Count: 22  |
| Virtual Cloud Network: ExaVCN  | Disk Redundancy: High                                     |
| Client Subnet: Client_Subnet_AD1   | Cluster Name: ExaCluster                                  |
| Backup Subnet: Backup_Subnet_AD1   | Port: 1521  |
| Hostname Prefix: exanode-mh0qa   | Host Domain Name: clientsubnetad1.exavcn.oraclecloud.com  |
| SCAN DNS Name: exanode-mh0qa-scan...                                     | SCAN IP Addresses:<br>10.0.3.6<br>10.0.3.7<br>10.0.3.8    |

The 'License Type' is listed as 'License included'.

The 'Resources' section shows 'Nodes (2)' and 'Databases (1)'. The 'Databases' section shows a table with the following data:

|  |   |   |
|--|---|---|
| <br>AVAILABLE | <b>exadb</b><br>Database Home: dbhomes20180710004549<br>Launched: Tue, 10 Jul 2018 00:45:49 GMT | Database Version: 18.0.0.0<br>Database Workload: OLTP<br>Database Unique Name: exadb_jhr14f |
|--|---|---|

## ステップ11: Exadata DBシステムへの接続

Exadata DBシステムのコンピュート・ノードには、セキュア・シェル(SSH)接続を使用して接続できます。システムの起動時に使用された公開鍵に関連付けられている秘密鍵があるファイルへのフル・パスが必要です。

DBシステムのパブリックまたはプライベートのIPアドレスを使用して、Exadataノードに接続できます。

- オンプレミスのVPN、またはVCN内からDBシステムに接続する場合は、プライベートIPアドレスを使用します。
- クラウド(VPNなし)の外からシステムに接続する場合は、DBシステムのパブリックIPアドレスを使用します。

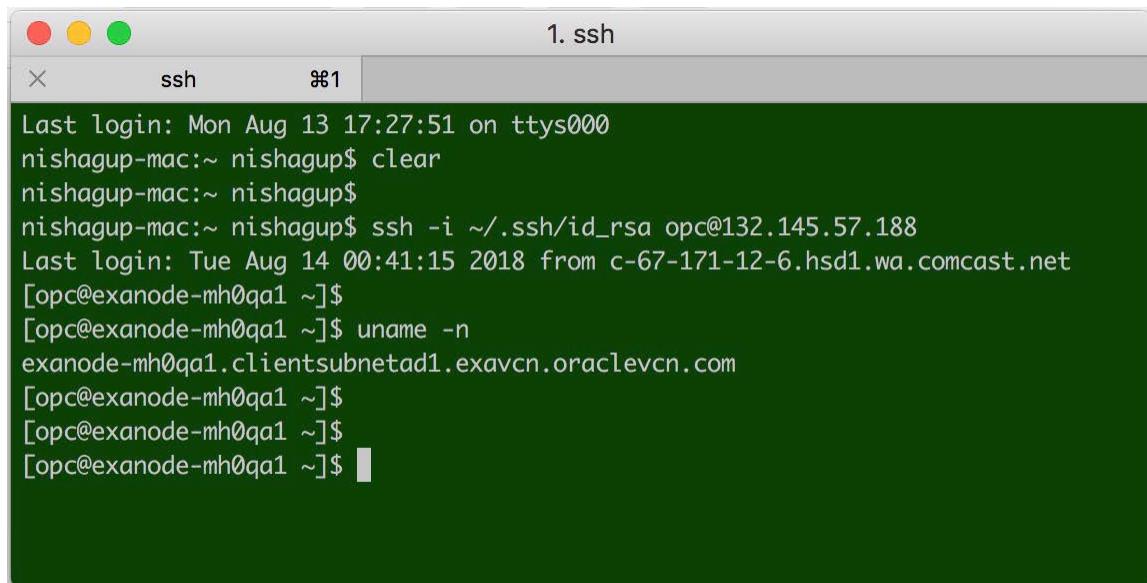
IPアドレスは、Oracle Cloud Infrastructureコンソールの「データベース」ページで見つけられます。

コンピュート・ノードにアクセスするには、次のSSHコマンドを使用します。

```
$ ssh -i <private_key> opc@<DB_system_IP_address>
```

<private key>は、アクセスするExadata DBシステムに関連付けられている秘密鍵があるファイルのフル・パスと名前です。次に例を示します。

```
ssh -i ~/.ssh/id_rsa opc@132.145.57.188
```



```
1. ssh
ssh    1. ssh
Last login: Mon Aug 13 17:27:51 on ttys000
nishagup-mac:~ nishagup$ clear
nishagup-mac:~ nishagup$ 
nishagup-mac:~ nishagup$ ssh -i ~/.ssh/id_rsa opc@132.145.57.188
Last login: Tue Aug 14 00:41:15 2018 from c-67-171-12-6.hsd1.wa.comcast.net
[opc@exanode-mh0qa1 ~]$ 
[opc@exanode-mh0qa1 ~]$ uname -n
exanode-mh0qa1.clientsubnetad1.exavcn.oraclevcn.com
[opc@exanode-mh0qa1 ~]$ 
[opc@exanode-mh0qa1 ~]$ 
[opc@exanode-mh0qa1 ~]$
```

詳細は、「[Exadata DBシステムへの接続](#)」を参照してください。

## サマリー

Exadataデータベース・マシンは高パフォーマンスのエンジニアド・ソリューションで、エンタープライズクラスのデータベースや関連付けられたワークロードに関する機能を最適化してユーザーに提供するよう設計されています。これらのステップに従って、簡単な選択を行うことで、Oracle Cloud InfrastructureにExadataをプロビジョニングできます。RMANやデータベース・コマンドライン・インターフェースなどの使い慣れたツールを使用して、お客様自身のデータ・センターと同じように、クラウドのデータベースを管理できます。



Oracle Corporation, World Headquarters  
500 Oracle Parkway  
Redwood Shores, CA 94065, USA

Worldwide Inquiries  
Phone: +1.650.506.7000  
Fax: +1.650.506.7200

---

CONNECT WITH US

- [blogs.oracle.com/oracle](http://blogs.oracle.com/oracle)
- [facebook.com/oracle](http://facebook.com/oracle)
- [twitter.com/oracle](http://twitter.com/oracle)
- [oracle.com](http://oracle.com)

**Integrated Cloud** Applications & Platform Services

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. 本文書は情報提供のみを目的として提供されており、ここに記載されている内容は予告なく変更されることがあります。本文書は一切間違いないことを保証するものではなく、さらに、口述による明示または法律による默示を問わず、特定の目的に対する商品性もしくは適合性についての默示的な保証を含み、いかなる他の保証や条件も提供するものではありません。オラクル社は本文書に関するいかなる法的責任も明確に否認し、本文書によって直接的または間接的に確立される契約義務はないものとします。本文書はオラクル社の書面による許可を前もって得ることなく、いかなる目的のためにも、電子または印刷を含むいかなる形式や手段によっても再作成または送信することはできません。

OracleおよびJavaはオラクルおよびその関連会社の登録商標です。その他の社名、商品名等は各社の商標または登録商標である場合があります。

Intel、Intel Xeonは、Intel Corporationの商標または登録商標です。すべてのSPARCの商標はライセンスをもとに使用し、SPARC International, Inc.の商標または登録商標です。AMD、Opteron、AMDロゴ、AMD Opteronロゴは、Advanced Micro Devices, Inc.の商標または登録商標です。UNIXは、The Open Groupの登録商標です。

Oracle Cloud InfrastructureにExadata DBシステムのデプロイ  
2018年8月  
著者: Nishant Gupta