

サービス・ゲートウェイを介したプライベートIPシリアル・コンソールへの接続

ORACLE WHITE PAPER | 2019年3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。以下の事項は、マテリアルやコード、機能を提供することをコミットメント（確約）するものではないため、購買決定を行う際の判断材料にならないで下さい。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。

改訂履歴

本ホワイトペーパーは、初版の公開後、次の改訂がありました。

日付	改訂内容
2019年3月26日	初版発行

Oracle Cloud Infrastructureホワイトペーパーの最新版は、
<https://cloud.oracle.com/iaas/technical-resources>でご覧いただけます。

目次

はじめに	4
サービス・ゲートウェイの概要	4
ルート表とセキュリティ・リストの構成	6
ルート表の構成	6
セキュリティ・リストの構成	8
パブリックおよびプライベート・インスタンスの作成	9
シリアル・コンソールの構成	9
プライベート・インスタンスのシリアル・コンソールへの接続	10
プライベート・インスタンスのシリアル・コンソール接続のテスト	12
結論	12

はじめに

シリアル・コンソールへの安全なアクセスは、長い間お客様から要望されていたサービスでした。Oracle Cloud Infrastructureで新しいサービス・ゲートウェイ機能がリリースされたことで、この機能を利用できるようになりました。サービス・ゲートウェイでは、インターネット・ゲートウェイやネットワーク・アドレス変換（NAT）デバイスを使用することなく、仮想クラウド・ネットワーク（VCN）のリソースがOracle Cloudにプライベートにアクセスできます。サービス・ゲートウェイを使用すると、プライベートIPアドレスを持つプライベート・サブネット上にあるVCNリソースに、インターネットを横断することなくパブリックIPアドレスからアクセスできます。このサービスに対する通信はすべて、Oracle Services Network上しか通過しないので、安全な通信パスが確保されるのです。

このホワイトペーパーでは、シリアル・コンソールを構成して、リモート接続から安全な形でそれにアクセスする方法を説明します。

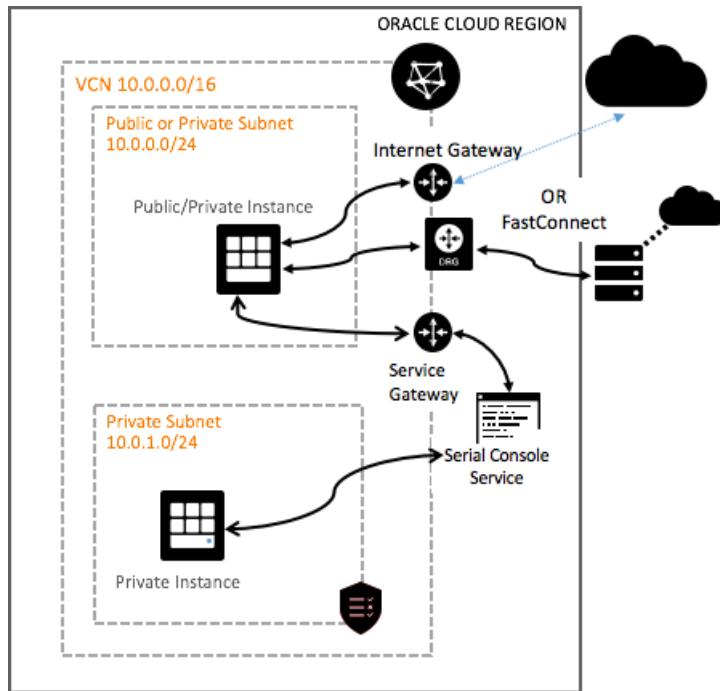
サービス・ゲートウェイの概要

各VCNには、ゲートウェイがいくつか関連付けられています。インターネット・ゲートウェイ、動的ルーティング・ゲートウェイ、NATゲートウェイ、そしてサービス・ゲートウェイです。これらのゲートウェイは、データ・プレーンとコントロール・プレーンの2種類に分類されます。インターネット・ゲートウェイ、動的ルーティング・ゲートウェイ、およびNATゲートウェイは、Oracle Cloud Infrastructureのテナントに出入りするデータ・プレーン・トラフィックのアクセス・ポイントです。サービス・ゲートウェイは、コントロール・プレーンに接続するので、Oracleの内部クラウド・サービス・ネットワークにアクセスできます。

1つのサービス・ゲートウェイには、1つのVCNしか関連付けられません。VCNを他のVCNとピア接続した場合、他のVCNにあるリソースはサービス・ゲートウェイにアクセスできなくなります。他のVCNからサービス・ゲートウェイにルーティングすることはできません。サービス・ゲートウェイのVCNにFastConnectまたはIPSec VPNで接続しているオンプレミス・ネットワーク上のリソースは、サービス・ゲートウェイを使用できません。

インターネット・ゲートウェイを通じてサービス・ゲートウェイに接続する、あるいはFastConnectを通じてパブリック・サブネットまたはプライベート・サブネット上にある内部インスタンスに接続することは可能です。その場合、そのインスタンスを使用してVCNに関連付けられたサービス・ゲートウェイにアクセスできます。

次の図は、パブリック・サブネットとプライベート・サブネットの両方があるVCNを示しています。プライベート・サブネットのリソースは、プライベートIPアドレスしか持たないため、直接インターネットと通信することはできません。



サービス・ゲートウェイの構成

サービス・ゲートウェイを構成するユース・ケースの例として、要塞またはDMZのジャンプボックス・サーバーから、プライベート・サブネット上の別のインスタンスに接続して再起動を実行することを考えてみます。

本書の例では、パブリック・サブネット1つとプライベート・サブネット1つを持ち、それぞれ1つのVMインスタンスがあるVCNを使用します。

注意：本書は、以前にリリースされたサービス・ゲートウェイの機能を使って執筆され、あくまでも1つの例として示されています。フェニックス（PHX）リージョンへの参照、サンプルのサービス・ラベル、利用可能なサービスは、最終的なGAリリースから変更されている場合があります。

1. Oracle Cloud InfrastructureコンソールでVCNに移動し、「リソース」の下にある「サービス・ゲートウェイ」をクリックします。
2. 「サービス・ゲートウェイの作成」をクリックして、接続を確立する名前とサービスを入力します。ここでは、「Oracle Services Networkの全PHXサービス」を選択します。
3. 「作成」をクリックします。

サービス・ゲートウェイが作成されると、その詳細が次のようにコンソールに表示されます。

The screenshot shows the 'Create Service Gateway' interface. At the top, there's a 'Sort by' dropdown set to 'Created Date (Desc)'. Below it, a service gateway named 'SGW Serial Console Test' is listed. It has an OCID of '...7uu7pq' and status 'AVAILABLE'. To the right, its creation date is listed as 'Tue, 19 Feb 2019 13:41:24 GMT' and services are listed as 'All PHX Services In Oracle Services Network'.

ルート表とセキュリティ・リストの構成

VCNからプライベート・サブネットへトラフィックが正しくルーティングされるためには、ルールとルートを追加する必要があります。インターネットからテナントにアクセスする場合は、インターネット・ルート0.0.0.0/0に対する通常のインターネット・ゲートウェイをVCNに追加します。

注意：外部接続用に、動的ルーティング・ゲートウェイを構成することもできます。インターネット・ゲートウェイは必須ではありません。

The screenshot shows the 'Route Table' configuration screen. It displays a table with columns for Destination CIDR Block (0.0.0.0/0), Target Type (Internet Gateway), and Target (Internet Gateway VCN_1). There are also 'Show' and 'Copy' buttons for each row.

ルート表の構成

サービス・ゲートウェイを使用するには、そこまでのルートを作成する必要があります。

1. VCNの詳細ページの「リソース」で、「ルート表」をクリックします。
2. ルート表を選択して、「ルート・ルールの編集」をクリックします。
3. サービス・ルートを追加し、このルート表にプライベート・サブネットを関連付けます。
 - A. ターゲット・タイプとして「サービス・ゲートウェイ」を選択します。
 - B. コンパートメントを選択します。
 - C. 宛先サービスとして「Oracle Services Networkの全PHXサービス」を選択します。
 - D. ターゲットとして作成したサービス・ゲートウェイを選択します。

Edit Route Rules

[help](#) [cancel](#)

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
Service Gateway	All PHX Services In Oracle Services Network x
COMPARTMENT	TARGET SERVICE GATEWAY
DCF_Sandbox	SGW Serial Console Test x
bmcsoutbound (root)/DCF_Sandbox	
TARGET TYPE	DESTINATION CIDR BLOCK
Internet Gateway	0.0.0.0/0 x
COMPARTMENT	TARGET INTERNET GATEWAY
DCF_Sandbox	Internet Gateway VCN_1 x
bmcsoutbound (root)/DCF_Sandbox	

+ Another Route Rule

[Save](#)

4. 「保存」をクリックします。

完了したときVCNのルート表ルールがどのように見えるか、例を以下に示します。

- **宛先サービス** : Oracle Services Networkの全PHXサービス
- **ターゲット・タイプ** : サービス・ゲートウェイ
- **ターゲット** : SGWシリアル・コンソール

Route Rules

Displaying 2 Route Rules

Edit Route Rules	
Destination Service: All PHX Services In Oracle Services Network	Target Type: Service Gateway Target: SGW Serial Console Test, ...7uu7pq Show Copy
Destination CIDR Block: 0.0.0.0/0	Target Type: Internet Gateway Target: Internet Gateway VCN_1 , ...lmjdia Show Copy

セキュリティ・リストの構成

セキュリティ・リストは、サブネットに関連付けられたファイアウォール・ルールの一般的なセットです。サブネットの内部で起動されたインスタンスすべてに適用され、そのインスタンスに出入りを許可されるトラフィックのタイプを指定するイングレス・ルールとエグレス・ルールを提供します。サービス・ゲートウェイを構成する際には、そのサービス・ゲートウェイを使用するサブネットのセキュリティ・リストで適切なポートが開かれている必要があります。たとえば、シリアル・コンソールはポート22 (SSH) を使用します。このポートは、他のインスタンスで使用できるようにあらかじめ開かれている必要があります。

1. サービス・ゲートウェイと通信する必要があるサブネットを決定します。
2. VCNの詳細ページの「リソース」で、「セキュリティ・リスト」をクリックします。
3. セキュリティ・リストを選択して、「すべてのルールの編集」をクリックします。
4. 次の値で、ステートフルなイングレス・ルールを追加します。
 - ソース : Oracle Services Networkの全PHXサービス
 - IPプロトコル : すべてのプロトコル（限定してプロトコルを選択することも可能）
 - 許可 : すべてのポートのすべてのトラフィック（限定してポートを選択することも可能）

Ingress Rules

Stateless Rules				
No Ingress Rules				
There are no stateless Ingress Rules for this Security List.				
Stateful Rules				
Source: 0.0.0.0/0	IP Protocol: TCP	Source Port Range: All	Destination Port Range: 22	Allows: TCP traffic for ports: 22 SSH Remote Login Protocol
Source: All PHX Services In Oracle Services Network	IP Protocol: All Protocols	Allows: all traffic for all ports		

5. 次の値で、エグレス・ルールを追加します。
 - 宛先 : Oracle Services Networkの全PHXサービス
 - IPプロトコル : TCP
 - ソース・ポート : すべて（限定してポートを選択することも可能）
 - 宛先ポート : 22、443（限定してポートを選択することも可能）

Egress Rules

Stateless Rules				
No Egress Rules				
There are no stateless Egress Rules for this Security List.				
Stateful Rules				
Destination: All PHX Services in Oracle Services Network	IP Protocol: TCP	Source Port Range: All	Destination Port Range: 22	Allows: TCP traffic for ports: 22 SSH Remote Login Protocol
Destination: All PHX Services in Oracle Services Network	IP Protocol: TCP	Source Port Range: All	Destination Port Range: 443	Allows: TCP traffic for ports: 443 HTTPS
Destination: 10.0.0.0/16	IP Protocol: TCP	Source Port Range: All	Destination Port Range: 22	Allows: TCP traffic for ports: 22 SSH Remote Login Protocol

パブリックおよびプライベート・インスタンスの作成

このユース・ケースでは、パブリック・サブネット上のVMインスタンスを、プライベート・サブネット上のVMインスタンスのシリアル・コンソールに接続します。どちらのインスタンスも、修正済のルート表とセキュリティ・リストを使用していることを確認してください。

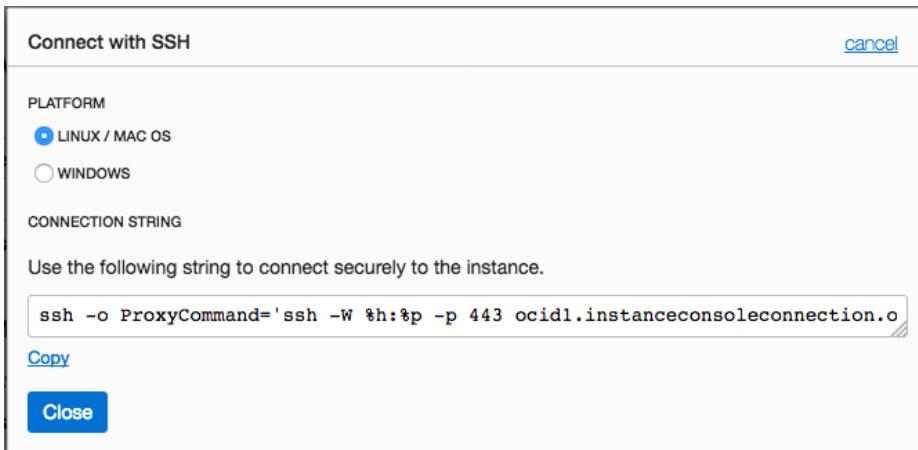
 RUNNING	VM_PRIV1 OCID: ...ghtzma Show Copy	Shape: VM.Standard2.1 Region: phx Availability Domain: eurR:PHX-AD-1 Fault Domain: FAULT-DOMAIN-1	Created: Tue, 19 Feb 2019 14:00:35 GMT Maintenance Reboot: -	•••
 RUNNING	VM_PUB1 OCID: ...swnkka Show Copy	Shape: VM.Standard2.1 Region: phx Availability Domain: eurR:PHX-AD-1 Fault Domain: FAULT-DOMAIN-1	Created: Tue, 19 Feb 2019 13:59:28 GMT Maintenance Reboot: -	•••

シリアル・コンソールの構成

このユース・ケースでは、サービス・ゲートウェイの宛先はプライベートVMインスタンスのシリアル・コンソールです。

1. Oracle Cloud Infrastructureコンソールで、接続しようとしているプライベートVMインスタンスの詳細ページに移動します。
2. 「リソース」で「コンソール接続」をクリックします。
3. 「コンソール接続の作成」をクリックします。

4. ダイアログ・ボックスで、SSH鍵を入力（貼り付けるか、ファイルを選択）し、「**コンソール接続の作成**」をクリックします。
5. コンパートメントのすべてのインスタンスがリストされるページで、接続しようとしているインスタンスの「アクション」メニュー（3つのドット）をクリックして「**SSHを使用して接続**」を選択します。
6. 「**SSHを使用して接続**」ダイアログ・ボックスで、接続しているプラットフォームを選択します。プライベート・インスタンスへの接続に必要な接続文字列が生成されます。



7. その接続文字列を、テキスト・ファイルにコピーします。次の項でこれを使用します。

プライベート・インスタンスのシリアル・コンソールへの接続

まず、パブリックVMインスタンスとプライベートVMインスタンスの間で接続をテストして設定する必要があります。

1. SSHを使用して、パブリック・インスタンスからプライベート・インスタンスへ接続します。

```
[opc@vm-pub1 ~]$ ssh -i ~/.ssh/oci -l opc 10.0.3.2
Warning: Identity file /home/opc/.ssh/oci not accessible: No such file or
directory.

The authenticity of host '10.0.3.2 (10.0.3.2)' can't be established.

ECDSA key fingerprint is
SHA256:qzbMWEY2Endh0oZqHGrMHCDdJKGMithl2nQ8KJuyqjs.

ECDSA key fingerprint is
MD5:0c:c4:11:13:83:d1:09:0c:3f:77:3b:65:5d:0c:8d:58.

Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.3.2' (ECDSA) to the list of known hosts.
```

2. SSH鍵ファイルを編集し、接続の必要なユーザーのソース秘密鍵ファイルを追加します。

```
[opc@vm priv1 ~]$ vi ~/.ssh/oci (add in the private key file)
```

3. SSH鍵ファイルで、セキュリティに必要な権限を変更します。

```
[opc@vm priv1 ~]$ chmod 400 ~/.ssh/oci
```

4. プライベート・インスタンスの接続セッションを終了します。

5. 前の項でコピーしておいた接続文字列を使用して、パブリック・インスタンスからプライベート・シリアル・コンソールに接続します。青色で強調表示されているテキスト (-i ~/.ssh/oci) は、インスタンスに固有のディレクトリ・パスに置き換えてください。

```
[opc@vm-pub1 ~]$ ssh -i ~/.ssh/oci -o ProxyCommand='ssh -i ~/.ssh/oci -W %h:%p -p 443  
ocid1.instanceconsoleconnection.oc1.phx.abyhqljsjfketfyf73rz7c6jcpbjpvla  
ewog4dyvbj3ueukjolsfrpjskq@instance-console.us-phoenix-1.oraclecloud.com'  
ocid1.instance.oc1.phx.abyhqljsjfw4hzv3dnduacavri2juvolznhqias4dwqbyi6xe  
e3vghtzma
```

```
Warning: Identity file /home/opc/.ssh/oci not accessible: No such file or  
directory.
```

```
Warning: Identity file /home/opc/.ssh/oci not accessible: No such file or  
directory.
```

```
The authenticity of host '[instance-console.us-phoenix-  
1.oraclecloud.com]:443 ([129.146.14.188]:443)' can't be established.
```

```
RSA key fingerprint is SHA256:Ghg/XkZv4W42u0xaqNhN7LMQcxrYuRTE+IYBD+kBxxx.
```

```
RSA key fingerprint is  
MD5:29:5e:e8:be:3c:8c:39:5c:29:d3:3a:9d:78:e9:7f:d3.
```

```
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added '[instance-console.us-phoenix-  
1.oraclecloud.com]:443, [129.146.14.188]:443' (RSA) to the list of known  
hosts.
```

```
The authenticity of host  
'ocid1.instance.oc1.phx.abyhqljsjfw4hzv3dnduacavri2juvolznhqias4dwqbyi6x  
ee3vghtzma (<no hostip for proxy command>)' can't be established.
```

```
RSA key fingerprint is SHA256:PhpxXIeD9OuKmi0ntmhePLW4Br8PRpu4oYMmuNvRAKk.
```

```
RSA key fingerprint is  
MD5:xx:xx:1c:dd:30:54:3f:68:bd:58:22:e4:65:64:9b:xx.
```

```
Are you sure you want to continue connecting (yes/no)? yes
```

```
Warning: Permanently added  
'ocid1.instance.oc1.phx.abyhqljsjfw4hzv3dnduacasvri2juvolznhqias4dwqbyi6x  
ee3vghtzma' (RSA) to the list of known hosts.
```

コンソール接続の確認画面が表示されます。

```
Oracle Linux Server 7.6  
Kernel 4.14.35-1844.1.3.el7uek.x86_64 on an x86_64
```

プライベート・インスタンスのシリアル・コンソール接続のテスト

シリアル・コンソール接続をテストするには、プライベートVMインスタンス・コンソールで再起動を実行し、接続が維持されるかどうか確認します。この時点で、プライベートVMインスタンスにログインできるか、あるいはコンソール経由で再起動コマンドを発行できます。まだプライベート・インスタンスのシリアル・コンソールに接続している状態で、再起動プロセス全体が表示されるはずです。

```
vmprivl login: [ OK ] Stopped Dump dmmsg to /var/log/dmmsg.  
      Stopping RPC bind service...  
[ OK ] Closed LVM2 poll daemon socket.  
[ OK ] Stopped target rpc_pipefs.target.  
[ OK ] Stopped target Multi-User System.  
[ OK ] Stopped Resets System Activity Logs.
```

```
Private VM instance rebooting.....
```

```
Welcome to Oracle Linux Server 7.6 dracut-033-554.0.3.el7 (Initramfs)!
```

```
[ OK ] Reached target Swap.  
[ OK ] Started Dispatch Password Requests to Console Directory Watch.  
[ OK ] Reached target Timers.  
[ OK ] Reached target Local Encrypted Volumes.  
[ OK ] Reached target Paths.
```

結論

このホワイトペーパーでは、Oracle Services Networkで分離性と安全性を保つためにサービス・ゲートウェイを使用するパブリック・ソース・ポイントから、プライベート・シリアル・コンソール接続を作成する方法について説明しました。

**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
- facebook.com/oracle
- twitter.com/oracle
- oracle.com

Integrated Cloud Applications & Platform Services

Copyright © 2019, 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、記載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暗示を問わず、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。0319

サービス・ゲートウェイを介したプライベートIPシリアル・コンソールへの接続
2019年3月
著者 : David Foster