Oracle® Cloud

Setting Up VPN from a Corente Services Gateway to an IP Network in Oracle Cloud

E68490-08
May 2020

Oracle Cloud Setting Up VPN from a Corente Services Gateway to an IP Network in Oracle Cloud,

E68490-08

Primary Author: Kumar Dhanagopal

Contributors: Kunal Rupani, Sylaja Kannan, Neeraj Sharma, George Sun, Henry Shen, Babu Suryanarayanan, Michael Fine, Bappan Dutta, Nagendran J, Anamika Mukherjee

Contents

Preface

Audience v
Conventions v

1 Solution Overview

2 Setting Up Corente Services Gateway in Your Data Center

Preparing Your Environment 2-1
Preparing Your Host 2-2
Setting Up Virtualization 2-2
Setting Up Networking 2-5
Downloading and Installing the Corente Services Gateway 2-9

3 Creating an IP Network

4 Creating a Cloud Gateway

5 Establishing Partnership Between Your On-Premises Gateway and Cloud Gateway

6 Configuring Your Guest Instances for VPN Access

7 Troubleshooting

Partner VPN Device Problems 7-1
Could Not Fit Range from Partner 7-1
IPsec Phase1 Failure Brings Down Tunnel 7-1

IPsec Phase2 Failure Brings Down Tunnel 7-2

Preface

This document describes how to set up VPN access from a Corente Services Gateway on-premises to an IP network in Oracle Cloud Infrastructure Compute Classic.

Topics

- Audience
- Conventions

Audience

This document is intended for administrators who want to set up VPN access through an third-party VPN gateway in their data center to an IP network in a multitenant Compute Classic site.

Conventions

This table describes the text conventions used in this document.

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1

Solution Overview

This document describes how to set up VPN access from a Corente Services Gateway in your data center to Compute Classic instances that are attached to an IP network defined by you in a multitenant Compute Classic site.

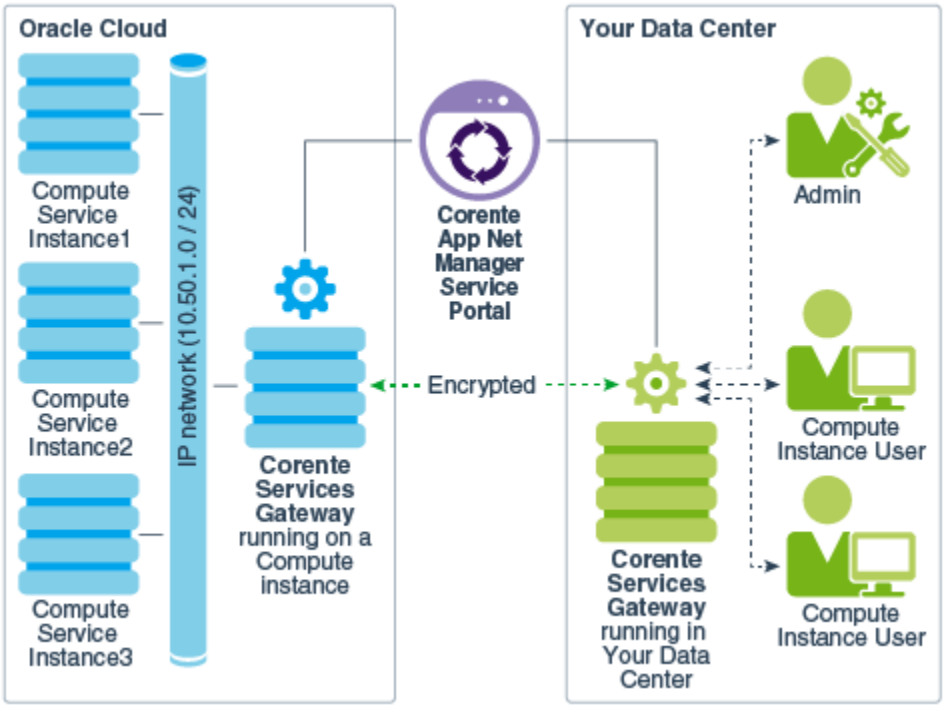
Topics

- Understanding the Architecture and Key Components of the Solution
- Workflow for Setting Up VPN

> **Note:**
>
> The following other VPN solutions are available for multitenant sites:
>
> - VPN access through a third-party gateway in your data center to instances attached to an IP network defined by you in the cloud. See *Setting Up VPN From a Third-Party Gateway to an IP Network in Oracle Cloud*.
> - VPN access through a third-party gateway or Corente Services Gateway in your data center to instances attached to the Oracle-provided shared network. See the following documentation:
>   - *Setting Up VPN from a Third-Party Gateway On-Premises to the Shared Network*
>   - *Setting Up VPN from Corente Services Gateway On-Premises to the Shared Network*

Understanding the Architecture and Key Components of the Solution

The following figure provides an overview of the solution:



The following are the key components of this solution:

- **App Net Manager Service Portal**: App Net Manager is a secure web portal that you use to create, configure, modify, delete, and monitor the components of your Corente-powered network. You can create, configure, modify, delete, and monitor the components of your Corente-powered network using the Compute Classic web console as well.
- **Corente Services Gateway**: Corente Services Gateway serves as a proxy that facilitates secure access and data transfer in the VPN solution.

  The solution consists of two separate installations of Corente Services Gateway:

  – The first gateway (referred to as *on-premises gateway*) is installed on a host in your on-premises data center. The gateway may be run as a guest VM on your physical host.

    Note that you should set up the on-premises gateway manually on a host with Internet access in your data center. One edge of this on-premises gateway connects to the Internet to establish connectivity with the Corente Services Gateway (the first one) installed in Oracle Cloud and the other edge of the on-premises gateway communicates with hosts or virtual machines of your users and administrators in your private network.

    You should manually set routes in your on-premises environment to direct packets with Oracle Cloud tunnel subnets to the Corente Services Gateway installed in your data center.

  – The second gateway (referred to as *cloud gateway*) is installed on an Compute Classic instance running in Oracle Cloud.

Workflow for Setting Up VPN

Task	More Information
Create and configure your account on Oracle Cloud	Getting an Oracle.com Account in *Getting Started with Oracle Cloud*
Obtain a trial or paid subscription to Compute Classic After you subscribe to Compute Classic, you will get your Corente credentials through email after you receive the Compute Classic welcome email. Note down the Corente account credentials that you received by email.	How to Begin with Compute Classic Subscriptions in *Using Oracle Cloud Infrastructure Compute Classic*
Set up a Corente Services Gateway (on-premises gateway) in your data center.	Setting Up Corente Services Gateway in Your Data Center
Create an IP network.	Creating an IP Network
Set up Corente Services Gateway (cloud gateway)	Creating a Cloud Gateway
Establish partnership between your on-premises gateway and the cloud gateway.	Establishing Partnership Between Your On-Premises Gateway and Cloud Gateway
Configure your guest instances for VPN access.	Configuring Your Guest Instances for VPN Access

2

Setting Up Corente Services Gateway in Your Data Center

You must set up Corente Services Gateway in your data center. This section provides steps to install Corente Services Gateway on a virtual machine in your data center. In this procedure, you're installing Corente Services Gateway to run as a guest VM on your host.

Topics

- Preparing Your Environment
- Preparing Your Host
- Setting Up Virtualization
- Setting Up Networking
- Downloading and Installing the Corente Services Gateway

Preparing Your Environment

Prepare your on-premises environment as follows:

1. Ensure that you have sudo privilege on the host where the gateway will be installed.
2. Run the following commands:
   a. `set path: PATH=$PATH:/usr/sbin:/sbin`
   b. If you're using a proxy, set the HTTP proxy and the HTTPS proxy, as in the following example:

```
export http_proxy=your_http_proxy_server:port
export https_proxy=your_https_proxy_server:port
```

> **Note:**
>
> Instructions are provided in this section are specific to Oracle Linux 6. For other versions of Linux, instructions may vary. For more information, see your operating system documentation.

Preparing Your Host

Prepare your host as follows:

- Verify that you have at least 40 GB of free disk space on the host where the on-premises gateway will be installed. If the partition used by `/var/lib/libvert/images/` is small, mount the directory to a large disk.
- If you're using a physical node/box, make sure that **virtualization** is enabled from BIOS. You can usually find this option under **Security** in BIOS.
- If you're using a virtual machine, verify support for virtualization as follows:

1. Log in as a root user.
2. Run the following command:

   ```
   modprobe -v kvm-intel
   ```

   If this command fails with fatal errors, it indicates some problem.
3. Run the following command:

   ```
   egrep '^flags.*(vmx|svm)' /proc/cpuinfo
   ```

   If this command produces no output, it indicates some problem.
4. Use the following command to see whether `/var/log/messages` contain messages such as "`KVM not supported by hardware/BIOS`":

   ```
   # cat /var/log/messages | grep -i kvm
   ```

5. If your hardware/BIOS does not support KVM, contact your IT administrator to enable nested virtualization on your VM.

Setting Up Virtualization

After preparing the host for the installation, you need to set up virtualization.

> **Note:**
>
> If you encounter fatal errors while preparing your host for the installation, contact your IT administrator to fix the errors before proceeding with virtualization.

1. If the `/etc/avahi/avahi-daemon.conf` file exists on your host, modify the file as follows:

   Change `#disallow-other-stacks=no` to `#disallow-other-stacks=yes`.

> **Note:**
>
> If the `/etc/avahi/avahi-daemon.conf` file is not present, you can do this step later during yum installation.

2. Check `/etc/login.defs`, and add the following lines if they are absent:

```
SYS_GID_MIN 2000


SYS_GID_MAX 9000
```

3. Verify the existence of group and user `qemu` with ID `107` by running the following commands:

```
grep qemu /etc/group


grep qemu /etc/passwd
```

   If the group and user are not found, create them:

   a. Add a group `qemu` if there isn't one:

```
# groupadd qemu
```

   b. Check `/etc/group`, and change the group ID of `qemu` to `107`.

```
# groupmod -g 107 qemu
```

> **Note:**
>
> If group ID `107` is taken, then assign a new ID to the application using it, and use group ID `107` for `qemu`.

   c. Add user `qemu` to group `qemu` if there isn't one:

```
# useradd qemu -g qemu
```

   d. Check `/etc/passwd`, and change the user ID of `qemu` to `107`.

```
# usermod -u 107 qemu
```

   e. Verify using the ID `qemu` that the user `qemu` has `107` as both user ID and group ID, as in the following:

```
-bash-4.1$ grep qemu /etc/group
qemu:x:107:
-bash-4.1$ grep qemu /etc/passwd
qemu:x:107:107::/:/sbin/nologin
```

4. Run `yum update` to get the latest versions of all packages.
5. Install `KVM`, `libvirt`, `qemu` and other packages required for the setup:

   ```
   # yum install kvm qemu-kvm python-virtinst libvirt libvirt-python virt-
   manager libguestfs-tools tunctl -y
   ```

   If the installation of the packages fails with an error "`invalid GPG key`", then do the following to import the GPG key and try to run `yum install` one more time:

   ```
   -bash-4.1$ locate GPG
   /etc/pki/rpm-gpg/RPM-GPG-KEY
   /etc/pki/rpm-gpg/RPM-GPG-KEY-fedora
   /etc/pki/rpm-gpg/RPM-GPG-KEY-fedora-test
   /etc/pki/rpm-gpg/RPM-GPG-KEY-oracle
   /usr/share/rhn/RPM-GPG-KEY
   -bash-4.1$ rpm --import /etc/pki/rpm-gpg/RPM-GPG-KEY-oracle
   ```

6. Run the following command to check the status of messagebus:

   ```
   # service messagebus status
   ```

   If the status is stopped, start messagebus by running the following command:

   ```
   # service messagebus start
   ```

7. If the avahi-daemon service is installed, verify its status by running the following command:

   ```
   # service avahi-daemon status
   ```

   If the status is stopped, start avahi-daemon:

   ```
   # service avahi-daemon start
   ```

8. Check the status of the libvirtd service:

   ```
   # service libvirtd status
   ```

   If the status is stopped, start the libvirtd service:

   ```
   # service libvirtd start
   ```

   If the status is dead with subsys lock, try to stop the service and restart:

   ```
   # service libvirtd stop
   # service libvirtd start
   ```

9. Add `/sbin/service avahi-daemon start` and `/sbin/service libvirtd start` to the `/etc/rc.d/rc.local` file, so these services will be started automatically whenever the host is rebooted.

10. Run the following command:

```
# modprobe -v kvm
# modprobe -v kvm-intel
```

Setting Up Networking

Topics

- Setting Up Virtual Bridge for NAT (virbr0)
- Configuring Bridge Interfaces

Setting Up Virtual Bridge for NAT (virbr0)

In this procedure, you're setting up a virtual bridge for NAT (`virbr0`).

1. Every standard libvirt installation provides out-of-the-box NAT-based connectivity to virtual machines. This network is referred to as the *default virtual network*. Verify this default network by running the following command:

   ```
   # virsh net-list –all
   ```

   If the default virtual network is present, you should see `virbr0` in the command output, as in the following example:

   ```
   # brctl show
   bridge name bridge id  STP enabled interfaces
   virbr0  8000.000000000000 yes
   ```

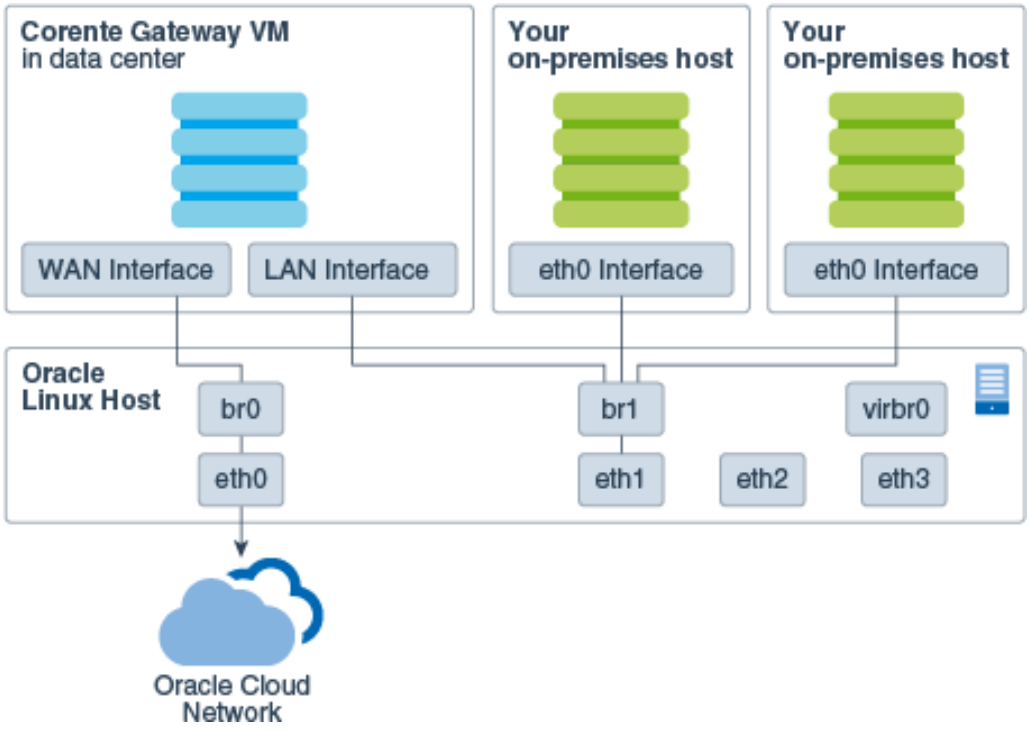
2. (Optional): If you don't see the default virtual network (`virbr0`), run the following commands:

   ```
   # virsh net-define /usr/share/libvirt/networks/default.xml
   # virsh net-autostart default
   # virsh net-start default
   ```

> **Note:**
>
> If you see the error "`dnsmasq: failed to set SO_REUSE{ADDR|PORT} on DHCP socket: Protocol not available`", then run the following commands to install a new version of `dnsmasq`:
>
> ```
> # wget http://www.thekelleys.org.uk/dnsmasq/dnsmasq-2.73.tar.gz
> # tar xvzf dnsmasq-2.73.tar.gz
> # cd dnsmasq-2.73
> # make install
> # cp /usr/local/sbin/dnsmasq /usr/sbin
> ```
>
> Now run steps 1 and 2 again.

Configuring Bridge Interfaces

The following diagram illustrates the configuration of bridge interfaces:



> **Note:**
>
> The names of network interfaces in the diagram are examples only.

Bridge interfaces are created in the host operating system to accommodate networking requirements of guest VMs.

Interface	Description
br0	Bridge for the Internet. The host's PHY interface for the Oracle Cloud Network connects to this bridge.
br1	Bridge for private networking between your on-premises Corente Services Gateway and your on-premises hosts.
virbr0	Backup bridge for NAT, and this may not be used.

You must create two bridges on the host and two virtual interfaces on your on-premises gateway and connect them, as illustrated in the diagram. The WAN interface connects to the Internet, and the LAN interface is for your internal network.

Complete the following steps:

1. If `NetworkManager` is present in `chkconfig`, disable `NetworkManager`, so that bridging can be supported using the classical framework:

   ```
   # chkconfig NetworkManager off
   # chkconfig network on
   # service NetworkManager stop
   # service network start
   ```

2. Create bridges and modify physical interfaces in the `/etc/sysconfig/network-scripts` directory as follows:

Bridge	How to Modify

`ifcfg-br0`	`DEVICE=br0`
	`TYPE=Bridge`
	`BOOTPROTO=static`
	`IPADDR=`
	`NETMASK=`
	`ONBOOT=yes`
	`DELAY=0`
	`NM_CONTROLLED=no`
	
	Note: Enter the IP address and the subnet mask of your host's Internet physical interface (eth0, in this example).

Bridge	How to Modify
ifcfg-eth0	DEVICE=eth0 HWADDR=90:E2:BA:80:40:34 ONBOOT=yes TYPE=Ethernet BRIDGE=br0 NM_CONTROLLED=no In addition, remove the following lines: IPADDR NETMASK BOOTPROTO
ifcfg-br1	DEVICE=br1 TYPE=Bridge IPADDR=192.168.37.10 NETMASK=255.255.255.0 BOOTPROTO=static ONBOOT=yes DELAY=0 NM_CONTROLLED=no
ifcfg-eth1	DEVICE=eth1 HWADDR=00:10:E0:5F:9A:B3 TYPE=Ethernet UUID=521fffed-8905-465a-a0ec-ea4739c62871 ONBOOT=yes NM_CONTROLLED=no BRIDGE=br1 Connection eth1 to br1 is optional.

3. Verify the bridge interfaces by running the following command:

```
# brctl show
```

You should see output, as in the following example:

```
bridge name     bridge id               STP enabled     interfaces
br0             8000.90e2ba804034       no              eth4
br1             8000.0010e05f9ab3       no              eth1
virbr0          8000.52540038e839       yes             virbr0-nic
```

Downloading and Installing the Corente Services Gateway

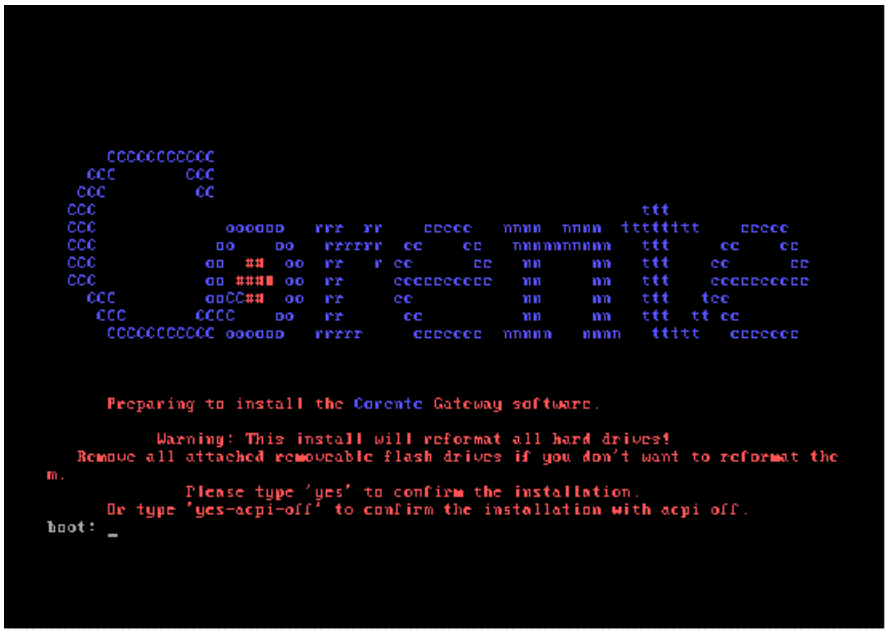
Download the Corente Gateway Image and use this image file to create a new virtual machine for your Corente Services Gateway (referred to as on-premises gateway).

Before you begin installing Corente Services Gateway, create a location-specific configuration file for your on-premises gateway. You'll use App Net Manager to perform the configuration of your *maiden* on-premises gateway (the first one in your data center domain). Log in to App Net Manager using the Corente credentials that you received in an email when you subscribed to Compute Classic. For more information about creating the location configuration file for your gateway, see Configuring the Corente Services Gateway in *Corente Services Gateway Deployment Guide*. The configuration file that you create is downloaded onto the on-premises gateway as part of the installation process.

Download and install Corente Services Gateway in your data center as follows:

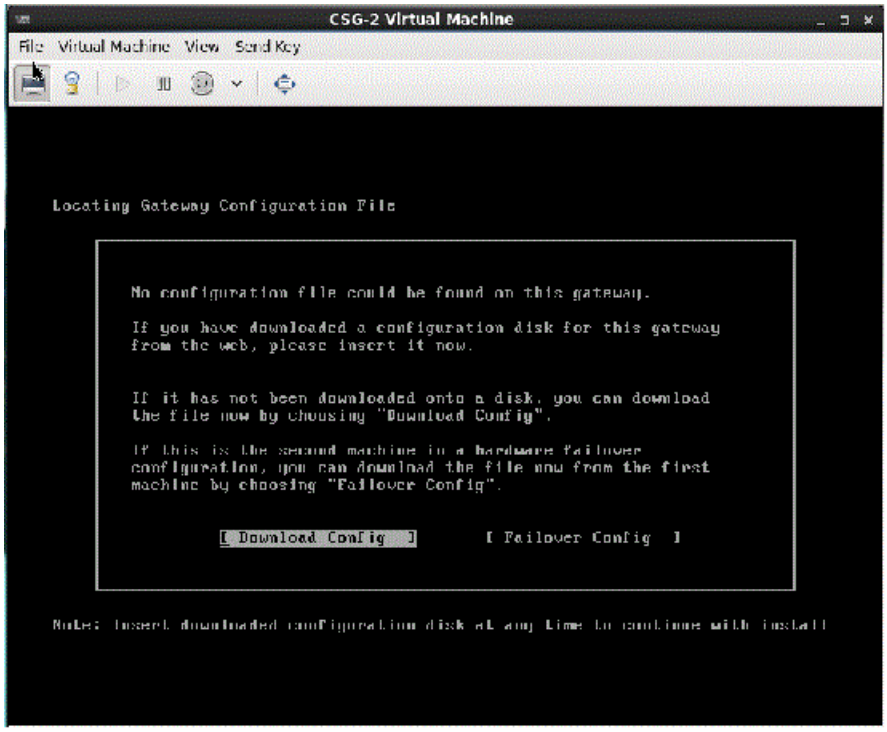
1. In your data center, identify the host you had prepared in the previous section.
2. Download the Corente Services Gateway software (Corente Gateway Image) from the following URL:

   http://www.oracle.com/technetwork/topics/cloud/downloads/network-cloud-service-2952583.html
3. Ensure that you have root access to the host where you want to install the on-premises Corente Services Gateway (referred to as on-premises gateway).
4. Create a new virtual machine for the on-premises gateway. Take care of the following points while creating the virtual machine:
   - Use the ISO image file of the Corente Gateway Image that you have downloaded to create the virtual machine.
   - Configure memory and CPU for the virtual machine being created.
   - Ensure that the size of the hard disk is more than 40 GB.
   - Configure two NICs for the on-premises gateway: one for br0 and another for br1. The virtual machine should have two network adapters or interfaces, one for WAN and another for LAN. One network interface or adapter is used for Internet connection and another one for internal communication with the Corente guest virtual machines.
5. When you create the virtual machine, the following virtual machine terminal screen is displayed:

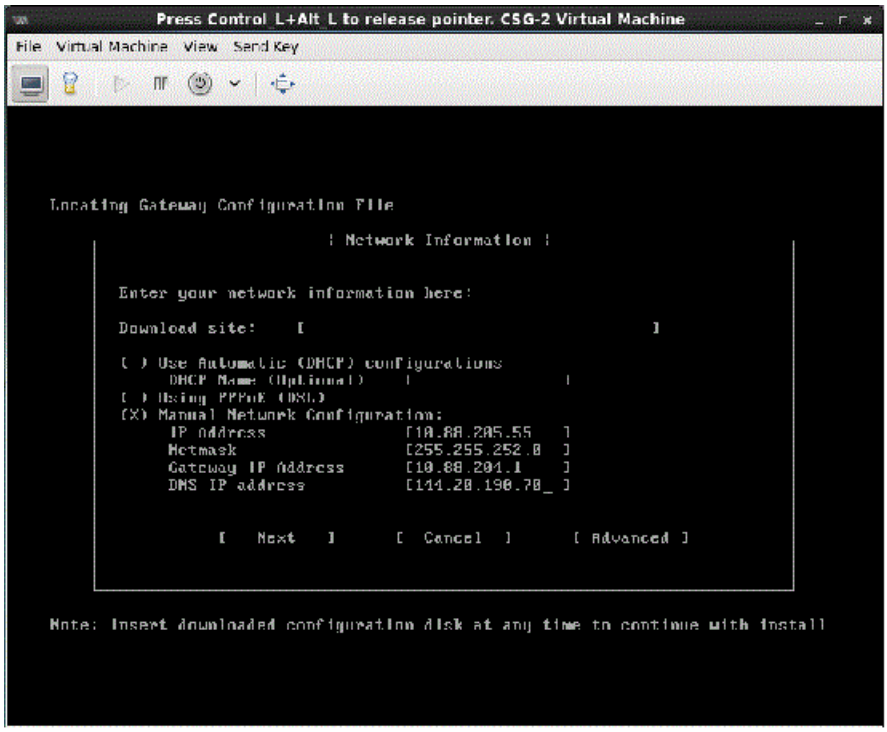


Enter yes, and then press **Enter** to proceed with the installation. The installation continues. Reboot the virtual machine, when prompted.

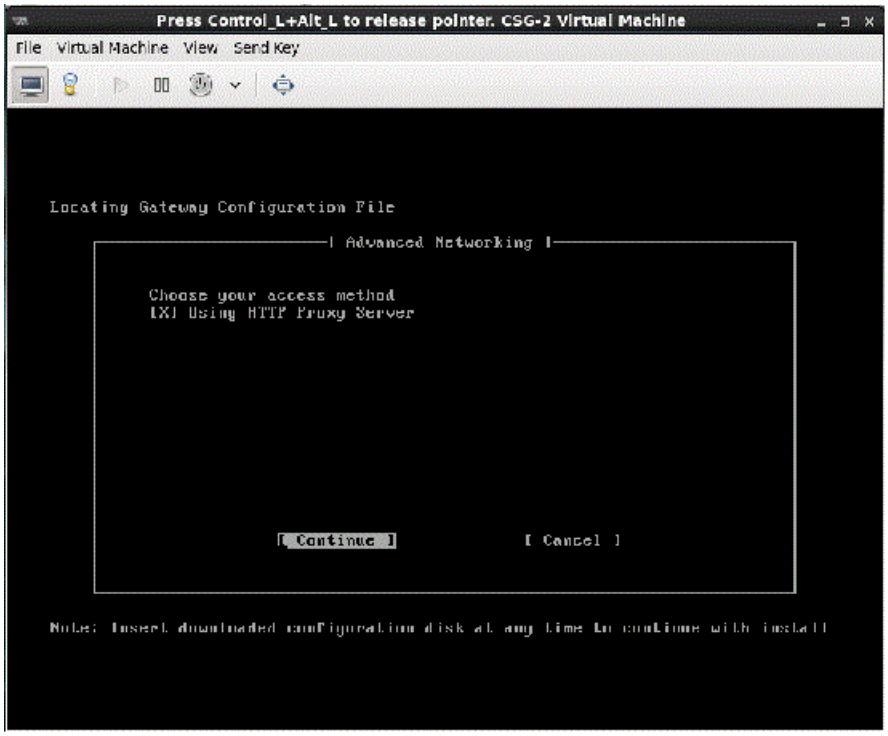
When the on-premises gateway virtual machine starts up, you'll see the following screen:



6. Select **Download Config** and press **Enter**. The network configuration screen is displayed, as in the following:

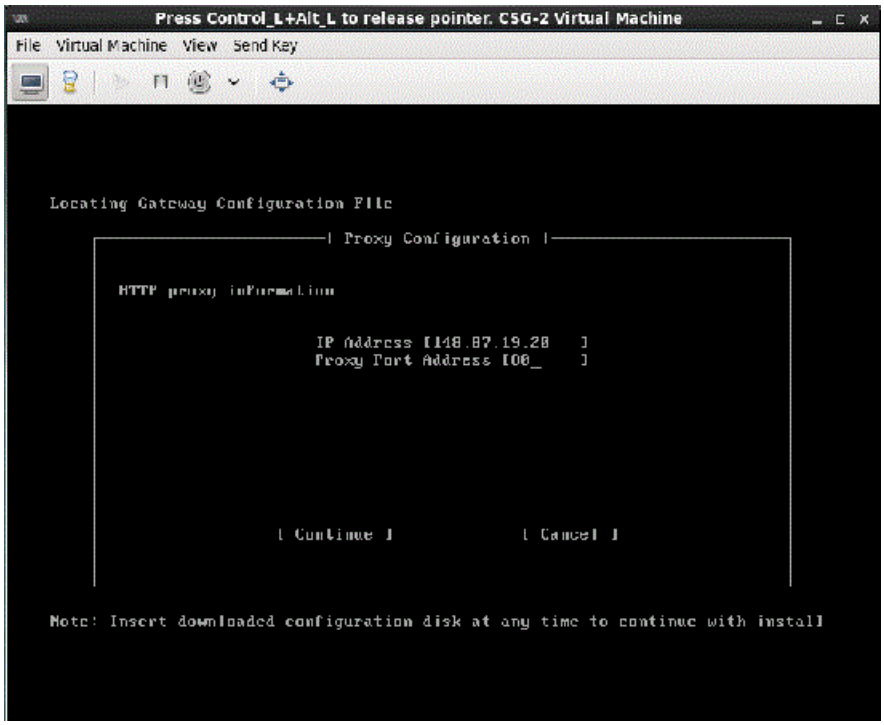


7. In this screen, enter information about your network interface facing Oracle Cloud (Internet). Move to **Advanced** to configure proxy.

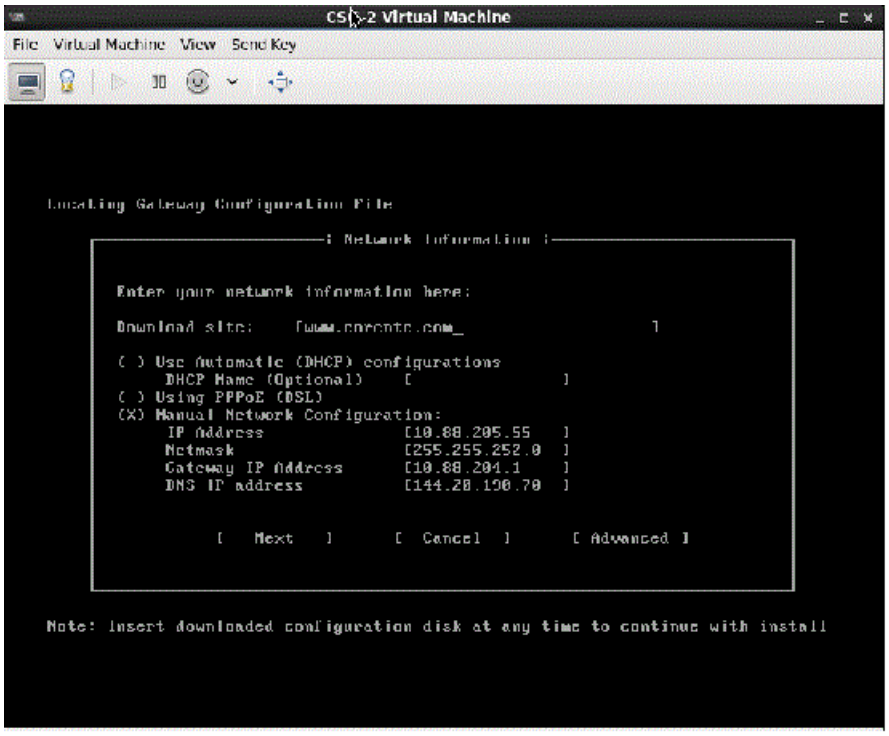


Select **Continue**.

8. Enter HTTP proxy information, as in the following:



9. In the next screen, enter `www.corente.com` as the **Download site**, and then select **Next**.



10. In the next screen, enter the username and password to log into the App Net Manager and the name of the gateway that you have created using App Net Manager as part of the prerequisite tasks. The location configuration file that you have created in App Net Manager is downloaded onto your on-premises gateway.

After the download is complete, your on-premises gateway reboots. When the gateway comes back up, you can't log into it due to security reasons. Your network administrator should use App Net Manager to start managing your on-premises gateway.

3

Creating an IP Network

To make your guest Compute Classic instances accessible over VPN, you should attach them *and* the Corente Services Gateway instance in the cloud to an IP network that you define in Compute Classic.

You can use an existing IP network or create a new one. For information about creating an IP network, see Creating an IP Network in *Using Oracle Cloud Infrastructure Compute Classic*. Note down the name of the IP network as you'll need to provide this name later while creating the Corente Services Gateway on the Cloud.

4 Creating a Cloud Gateway

If you want to establish a VPN connection to your Compute Classic instances, start by creating a Corente Services Gateway instance.

Prerequisites

- You must have already reserved the public IP address that you want to use with your gateway instance. See Reserving a Public IP Address in *Using Oracle Cloud Infrastructure Compute Classic*.
- You must have already created the IP network that you want to add your gateway instance to. See Creating an IP Network in *Using Oracle Cloud Infrastructure Compute Classic*.
- To complete this task, you must have the `Compute_Operations` role. If this role isn't assigned to you or you're not sure, then ask your system administrator to ensure that the role is assigned to you in Oracle Cloud Infrastructure Classic Console. See Modifying User Roles in *Managing and Monitoring Oracle Cloud*.

Procedure

1. Sign in to the Compute Classic console. If your domain spans multiple sites, select the appropriate site. To change the site, click the **Site** menu near the top of the page.
2. Click the **Network** tab.
3. In the **Network** drop-down list, expand **VPN**, expand **Corente**, and then click **VPN Gateways**.
4. Click **Create VPN Gateway**.
5. Select or enter the required information:
    - **Name:** Enter a name for the Corente Services Gateway instance.
    - **IP Reservation:** Select the IP reservation that you want to use with this instance. This is the public IP address of your VPN gateway.
    - **Image:** Select the machine image that you want to use to create the instance. You must select the most recent Corente Gateway image.
    - **Interface Type:** Select **Dual-homed**. Your gateway instance is added to an IP network as well as to the shared network. All instances that are on the same IP network as the Corente Services Gateway instance, as well as instances on IP networks that are connected to that IP network through an IP network exchange, can be accessed using VPN.
    - **IP Network:** Select the IP network that you want to add the Corente Services Gateway instance to.
    - **IP Network Address:** Select the IP address for your gateway instance. The IP address that you specify must belong to the subnet of the specified IP network. An available IP address is allocated by default. You can specify a different LAN IP address, if required.

- **Subnets:** Enter a comma-separated list of subnets (in CIDR format) that should be reachable using this gateway. The subnet of the IP network specified in the **IP Network** field is added by default. Don't modify or delete this subnet in this field.
- **Add reachable IP networks:** (Optional) You can select additional IP networks that should be reachable using this gateway. Ensure that the IP networks that you specify here, and the IP network that the Corente Services Gateway is added to, all belong to the same IP network exchange. See Adding an IP Network to an IP Network Exchange in *Using Oracle Cloud Infrastructure Compute Classic*.
  You must also add a route on the gateway to the subnet of each additional IP network. You can't do this using the web console. Use App Net Manager to add this route.

> **Note:**
>
> You must also add the subnets that you specify here to the list of destination IP addresses that you specify in your third-party device.

6. Click **Create**.

A Corente Services Gateway instance is created. The required orchestrations are created and started automatically. For example, if you specified the name of the Corente Gateway instance as **CSG1**, then the following orchestrations are created:

- **vpn–CSG1–launchplan:** This orchestration creates the instance using the specified image, and associates the instance interfaces with the shared network and the specified IP network.
- **vpn–CSG1–bootvol:** This orchestration creates the persistent bootable storage volume.
- **vpn–CSG1–secrules:** This orchestration creates the required security list, security applications, and security rules.
- **vpn–CSG1–master:** This orchestration specifies relationships between each of the nested orchestrations and starts each orchestration in the appropriate sequence.

While the Corente Services Gateway instance is being created, the instance status displayed in the **Instance** column on the VPN Gateways page is **Starting**. When the instance is created, its status changes to **Ready**.

You can also list the VPN gateways, update the gateway instance to modify the reachable routes, or delete the gateway instance if you no longer require this gateway. See Listing VPN Gateways, Modifying the Reachable Subnets for a VPN Gateway, or Deleting a VPN Gateway in *Using Oracle Cloud Infrastructure Compute Classic*.

> **Note:**
>
> You can list the gateway instance and view details on the Instances page, or view the corresponding orchestrations on the Orchestrations page. However, it is recommended that you always use the VPN Gateways page to manage your gateway instances.

5

Establishing Partnership Between Your On-Premises Gateway and Cloud Gateway

After verifying that your on-premises gateway and cloud gateway are running, you must add partnership between the two gateways.

Do the following:

1. Log in to App Net Manager.
2. In App Net Manager, in the Domains pane, click **Locations** to expand and show all of your gateways.
3. Select your Corente Services Gateway cloud instance and click to expand.
4. Click the **Partner** option under your Corente Services Gateway cloud instance in App Net Manager.
5. Click **New** at the top of the App Net Manager screen.
6. Select **Intranet** in the Connection to Partner panel, and then select your corporate gateway in the drop-down (right side of your selection).
7. Click **Add** at the bottom of the Tubes pane at the bottom of the Add Partner screen.
8. In the Local Side of Tube pane in the Add Tube screen, select **Default User Group** in the User Group selector.
9. In the Remote Side of Tube pane in the Add Tube screen, select **Default User Group** in the User Group selector.
10. Leave all other settings at the defaults.
11. Click **OK** in the Add Tube screen.
12. Click **OK** in the Add Partner screen.
13. Select your corporate Corente Services Gateway in the Locations in the Domains pane of App Net Manager.
14. Select **Partners** under your corporate Corente Services Gateway.
15. Click **New** at the top of the App Net Manager screen.
16. Select **Intranet** in the Connection to Partner panel, and then select your cloud gateway in the drop-down next to your selection.
17. Click **Add** at the bottom of the Tubes pane at the bottom of the Add Partner screen
18. In the Local Side of Tube pane in the Add Tube screen, select **Default User Group** in the User Group selector.
19. In the Remote Side of Tube pane in the Add Tube screen, select **Default User Group** in the User Group selector.
20. Leave all other settings at the defaults.

21. Click **OK** in the Add Tube screen.
22. Click **OK** in the Add Partner screen.
23. Click **Save** at the top of the App Net Manager screen.
24. Click **Start** in the Save screen.
25. Click **Finished** in the Save screen.

You should now see a connection line appear between the gateways in App Net Manager. You'll see a yellow line first. The line turns green as the tunnel becomes active.

6 Configuring Your Guest Instances for VPN Access

To make your guest Compute Classic instances accessible over VPN, you should attach them to the same IP network that the Corente Services Gateway instance is attached to.

1. Download the sample orchestration, `csg-sdn-guestinstance.json`, which is included in the `greconf_orchsamples.zip` file at the following location: http://www.oracle.com/technetwork/topics/cloud/downloads/network-cloud-service-2952583.html.
2. Open `csg-sdn-guestinstance.json` in a plain-text editor, and make the following changes:
   - Replace all occurrences of `myidentitydomain` with the ID of your identity domain.
   - Change all occurrences of `john.doe@example.com` to your user name.
3. Under the `launchplan` object type, update the following attributes:
   - Change the `name`, `ha_policy`, `label`, `imagelist`, and `shape` attributes to values of your choice. See Instance Attributes in *Using Oracle Cloud Infrastructure Compute Classic*.
   - Change `ipnetwork` to the name of the IP network that you created earlier and attached the Corente Services Gateway instance to. See Creating an IP Network.
     Here's a *partial* example of an instance orchestration showing the `networking` attribute.

     ```
     {
     "networking": {
       ...
       "eth1": {
         ipnetwork": "/Compute-acme/john@example.com/ipnet1",
         ...
        }
      }
     }
     ```
4. Save and close the orchestration JSON file.
5. Upload the orchestration to Compute Classic.

   See Uploading an Orchestration in *Using Oracle Cloud Infrastructure Compute Classic*.
6. Start the orchestration.

   See Starting an Orchestration in *Using Oracle Cloud Infrastructure Compute Classic*.
7. (Optional) If you specified multiple interfaces for the guest instance, and if one of those interfaces is attached to the Oracle-provided shared network, then you must

explicitly configure the Corente Services Gateway as the gateway to the on-premises subnet. You don't have to perform this additional step for instances that are only connected to the IP network and are not connected to the Oracle-provided shared network.

Here's a *partial* example of an instance orchestration showing the `networking` attribute with two interfaces: `eth1` attached to the IP network that the cloud gateway is attached to, and `eth0` attached to the Oracle-provided shared network with the IP address you had reserved earlier.

```
...
"networking": {
   "eth0": {
    "seclists": [
      "/Compute-acme/john@example.com/mySecList"
    ],
    "nat": "ipreservation:/Compute-acme/john@example.com/ipres1"
   },
   "eth1": {
     "ipnetwork": "/Compute-acme/john@example.com/ipnet1",
     ...
   }
}
```

On your guest instance, to configure the Corente Services Gateway as the gateway to the on-premises subnet, complete the following steps:

a. Log in to the instance.

b. Add a route:

> **Note:**
>
> You may need root or administrator privileges for this step.

- **Linux**:

  Command syntax: `ip route add` *`onprem_subnet`* `via` *`cloud_gateway_ip`*

  Example: `ip route add 10.248.64.176/28 via 172.31.200.1`

- **Windows**:

  Command syntax: `route add` *`onprem_subnet`* `mask` *`subnet_mask`* *`cloud_gateway_ip`*

  Example: `route add 192.168.49.0 mask 255.255.255.0 172.31.200.1`

When you run this command, set `cloud_gateway_ip` to the first address in the IP network that the cloud gateway instance is attached to, and set `onprem_subnet` to the subnet address of the on-premises network. For example, if `172.31.200.0/24` is the IP address prefix of the IP network that is attached to the cloud gateway instance, then the `cloud_gateway_ip` is `172.31.200.1`. If `192.168.0.128/25` is the IP address prefix of the IP network that is attached to the cloud gateway instance, then the `cloud_gateway_ip` is `192.168.0.129`.

> **Note:**
>
> You must add this route every time the instance is rebooted or re-created. You can also configure the route to persist across reboots. For detailed instructions to configure the route to persist across reboots, refer to documentation for your operating system.

7

Troubleshooting

This section describes common problems that you might encounter when setting up VPN and explains how to solve them. If you cannot find a solution in this section, raise a service request with My Oracle Support.

- If you encounter issues while setting up a cloud gateway by creating a Corente Services Gateway instance, see Orchestration Problems in *Using Oracle Cloud Infrastructure Compute Classic*.
- If you encounter issues while connecting the cloud gateway with the partner device, see Partner VPN Device Problems.

Partner VPN Device Problems

This section describes common problems that you might encounter while connecting the cloud gateway with the partner device.

When there are issues setting up the connection to the partner device, alarms are created in App Net Manager. See Working with Alarms and Events in *Oracle Corente Cloud Services Exchange Administration Guide*.

Could Not Fit Range from Partner

Description

When the tunnel is not set up between the CSG gateway and the partner gateway, the following message is displayed as an active tunnel alarm in App Net Manager.

```
Gateway [identity-domain.name-of-CSG-gateway] could not fit range [remote acl range
10.0.0.0-10/63.255.255] from Partner [name-of-partner-device] because it is nested
within committed range [local LAN range 10.18.7.112-10.18.7.115] from Gateway/
Partner [identity-domain.name-of-CSG-gateway]. Consequently, the secure subnet
tunnel between the two Partners has not been brought up. Please check the partners'
NAT policies and User Groups.
```

Solution

This error indicates that the subnets provided in `10.18.x.x` range are already nested in `10.0.0.x`.

To resolve this issue, remove the `10.0.0.0` subnet.

IPsec Phase1 Failure Brings Down Tunnel

Description

The following error message is displayed under the **Alarms** section in the App Net Manager.

```
The secure tunnel between [identity-domain.name-of-CSG-gateway] and [name-of-partner-
device] is DOWN. (IPsec Phase1 ISAKMP SA Failed).
```

Solution

This error indicates that there is IPsec Phase 1 failure and the connection between the cloud gateway and the partner device could not be set up. Such failures usually occur if you have provided incorrect information while establishing partnership between the two gateways.

To resolve this error, ensure that the information you have provided is correct.

IPsec Phase2 Failure Brings Down Tunnel

Description

When you add another subnet, the VPN tunnel (which was established previously) fails and the following error message is displayed under the **Alarms** section in the App Net Manager.

```
The secure tunnel between [identity-domain.name-of-CSG-gateway] and [name-of-partner-
device] is DOWN.
detail
[IPsec Phase2 Failed
192.128.0.0/16-10.50.0.0/16:UP
10.0.0.0/16-10.50.0.0/16:DOWN]
```

Solution

This error indicates that the IP addresses announced by Corente doesn't match with the IP addresses accepted or published by the partner device. In this example, the partner device is not configured to receive traffic from `10.0.0.0/16` subnet.

Add the new subnet to the firewall of the partner device.