Oracle® Cloud

Setting Up VPN from Corente Services Gateway On-Premises to the Shared Network

E72381-18
May 2020

Oracle Cloud Setting Up VPN from Corente Services Gateway On-Premises to the Shared Network,

E72381-18

Primary Author: Sylaja Kannan

Contributors: Anirban Ghosh, Kumar Dhanagopal, Kunal Rupani, Neeraj Sharma

Contents

Preface

This document describes how you can set up VPN access to your guest instances in Oracle Cloud by installing Corente Service Gateway, which is an Oracle-provided IPSec solution, in both your data center as well as in Oracle Cloud. You can use this VPN connection to securely access to your Oracle Cloud Infrastructure Compute Classic, Oracle Java Cloud Service, and Oracle Database Cloud Service instances.

Topics

- Audience
- Conventions

Audience

This document is intended for administrators of Oracle Cloud Infrastructure Compute Classic, Oracle Java Cloud Service, and Oracle Database Cloud Service.

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 About Setting Up VPN Using Corente Services Gateway

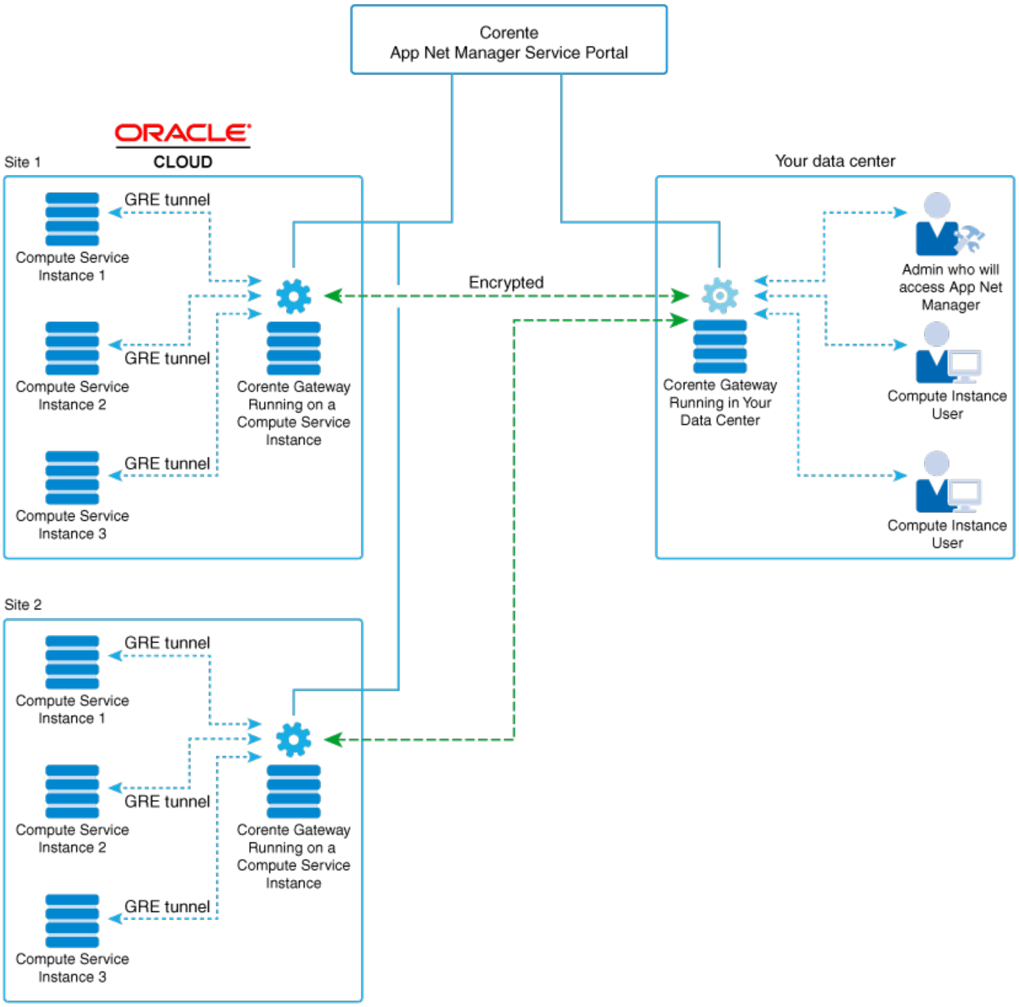
You can set up VPN access to Oracle Cloud Service instances by installing Corente Service Gateway, which is an Oracle-provided IPSec solution, in both your data center as well as in Oracle Cloud.

Topics

- Understanding the Architecture and Key Components of the Solution
- Workflow for Setting Up VPN Using Corente Services Gateway

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

Understanding the Architecture and Key Components of the Solution


Corente
App Net Manager Service Portal
ORACLE
CLOUD
Site 1
GRE tunnel
Compute Service Instance 1
GRE tunnel
Compute Service Instance 2
GRE tunnel
Compute Service Instance 3
Corente Gateway Running on a Compute Service Instance
Encrypted
Your data center
Corente Gateway Running in Your Data Center
Admin who will access App Net Manager
Compute Instance User
Compute Instance User
Site 2
GRE tunnel
Compute Service Instance 1
GRE tunnel
Compute Service Instance 2
GRE tunnel
Compute Service Instance 3
Corente Gateway Running on a Compute Service Instance

- **Corente Services Gateway**: Corente Services Gateway acts 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 GRE tunnel subnets (for example, 172.16.1.0/25 specified in Creating a New Linux Instance and Configuring a GRE Tunnel) to the Corente Services Gateway installed in your data center.

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

Your Compute Classic account can contain multiple sites. You must set up the cloud gateway on each site.

After setting up the cloud gateway, manually set up and configure a Generic Routing Encapsulation (GRE) tunnel from your OCompute Classic instances (virtual machines) to the Corente Services Gateway running on another Compute Classic instance.

On each site, create a GRE tunnel between Compute Classic instances and the cloud gateway on the same site.

- **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 also use the Compute Classic web console to manage the cloud gateway.

Workflow for Setting Up VPN Using Corente Services Gateway

Task	Component in the Architectural Diagram	For more Information
Create and configure your account on Oracle Cloud	It’s a prerequisite.	See 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 Classicwelcome email. Note down the Corente account credentials that you received by email.	It’s a prerequisite.	See 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	Corente Services Gateway running in your data center, as shown in the architecture diagram.	See Setting Up Corente Services Gateway in Your Data Center.
Set up Corente Services Gateway (cloud gateway) on Oracle Cloud	Corente Services Gateway running on a Compute Classic instance, as shown in the architecture diagram.	See Creating a Cloud Gateway.
Establish partnership between your on-premises gateway and cloud gateway	This is the dashed line between the two gateways, as shown in the architecture diagram.	See Establishing Partnership Between Your On-Premises Gateway and Cloud Gateway.

Task	Component in the Architectural Diagram	For more Information
Configure a GRE tunnel on your guest instances in Oracle Cloud	GRE tunnel from Compute Classic instances 1, 2, and 3 as shown in the architecture diagram.	See: • Creating a New Linux Instance and Configuring a GRE Tunnel • Configuring a GRE Tunnel on Running Linux Instances • Configuring a GRE Tunnel on a Windows Instance

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

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:

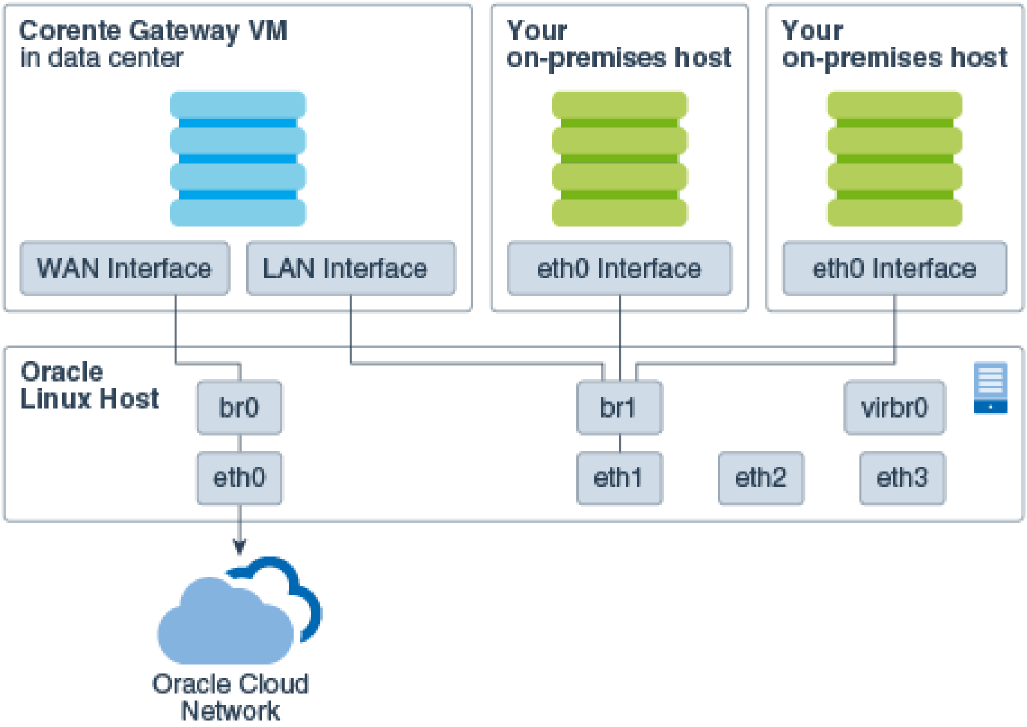
If you see the error “dnsmasq: failed to set SO_REUSE{ADDR|PORT} on DHCP socket: Protocol not available”, then run the following commands to install a new version of dnsmasq:

```
# 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

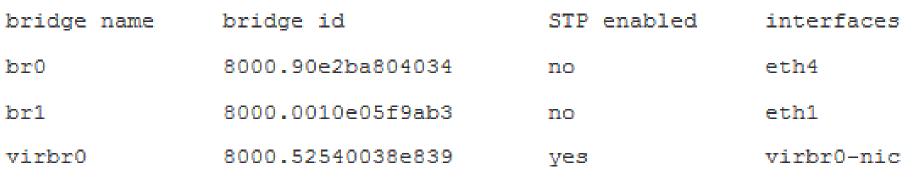
ifcfg-br1	DEVICE=br1
	TYPE=Bridge
	IPADDR=192.168.37.10
	NETMASK=255.255.255.0
	BOOTPROTO=static
	ONBOOT=yes
	DELAY=0
	NM_CONTROLLED=no

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

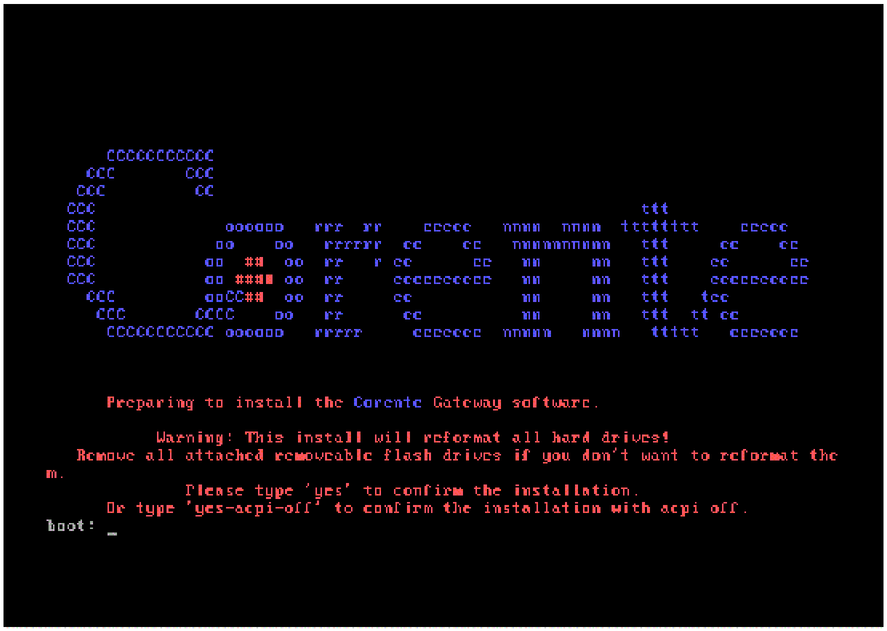
Download the Corente Gateway Image and use this image file to create a new virtual machine for your Corente Services Gateway (referred to as on-premises gateway).

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:

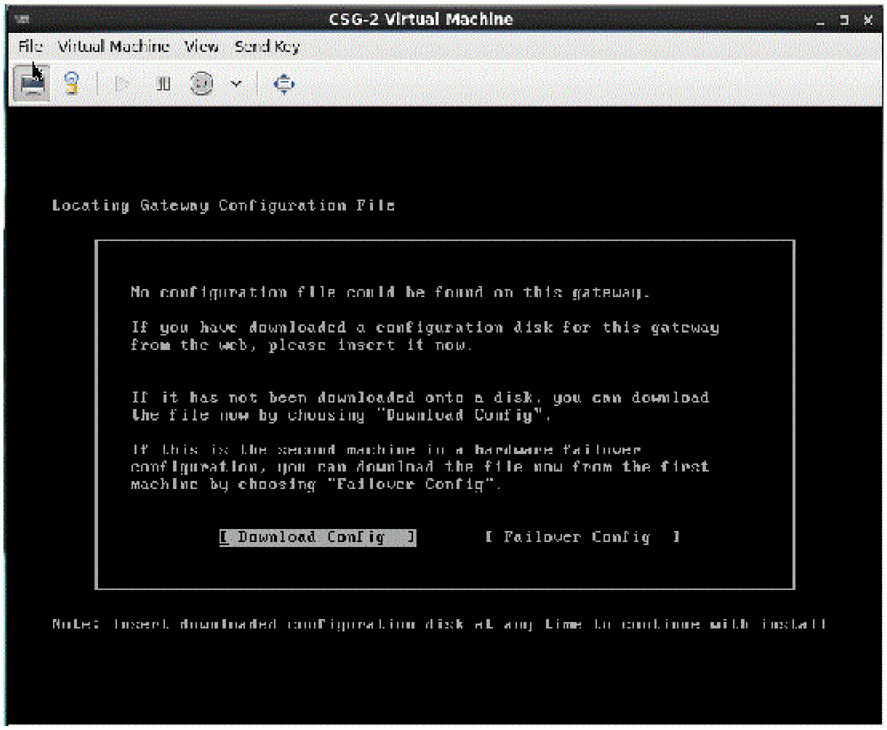
   http://www.oracle.com/technetwork/topics/cloud/downloads/network-cloud-service-2952583.html
3. Ensure that you have root access to the host where you want to install the on-premises Corente Services Gateway (referred to as on-premises gateway).
4. Create a new virtual machine for the on-premises gateway. 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:



```
          CCCCCCCCCCC
        CCC         CCC
       CCC           CC
      CCC                                                    ttt
      CCC            oooooo   rrr  rr    ccccc   nnnn  nnnn  ttttttt    ccccc
      CCC           oo    oo  rrrrrr  cc    cc   nnnnnnnnnn    ttt     cc    cc
      CCC          oo  ##  oo rr    r cc      cc  nn      nn   ttt    cc      cc
      CCC          oo ###■ oo rr      cccccccccc  nn      nn   ttt    cccccccccc
        CCC        ooCC##  oo rr      cc          nn      nn   ttt   tcc
         CCC      CCCC    oo  rr       cc         nn      nn   ttt  tt cc
          CCCCCCCCCCC oooooo  rrrrr     ccccccc  nnnnn   nnnn   ttttt   ccccccc


          Preparing to install the Corente Gateway software.

               Warning: This install will reformat all hard drives!
       Remove all attached removeable flash drives if you don't want to reformat the
    m.
                   Please type 'yes' to confirm the installation.
          Or type 'yes-acpi-off' to confirm the installation with acpi off.
    boot: _
```

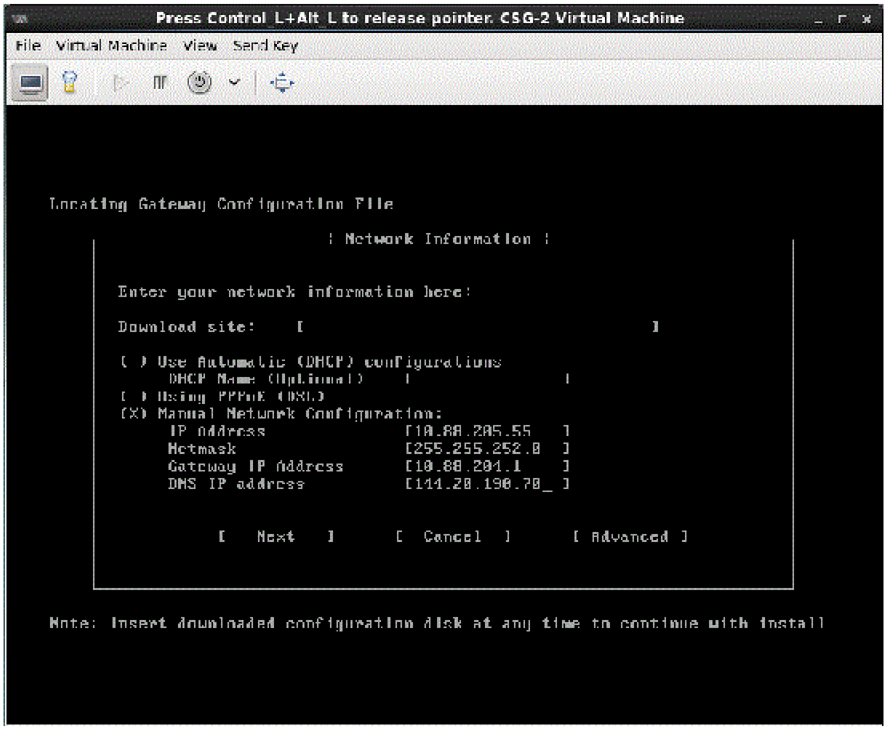
Enter yes, and then press **Enter** to proceed with the installation. The installation continues. Reboot the virtual machine, when prompted.

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



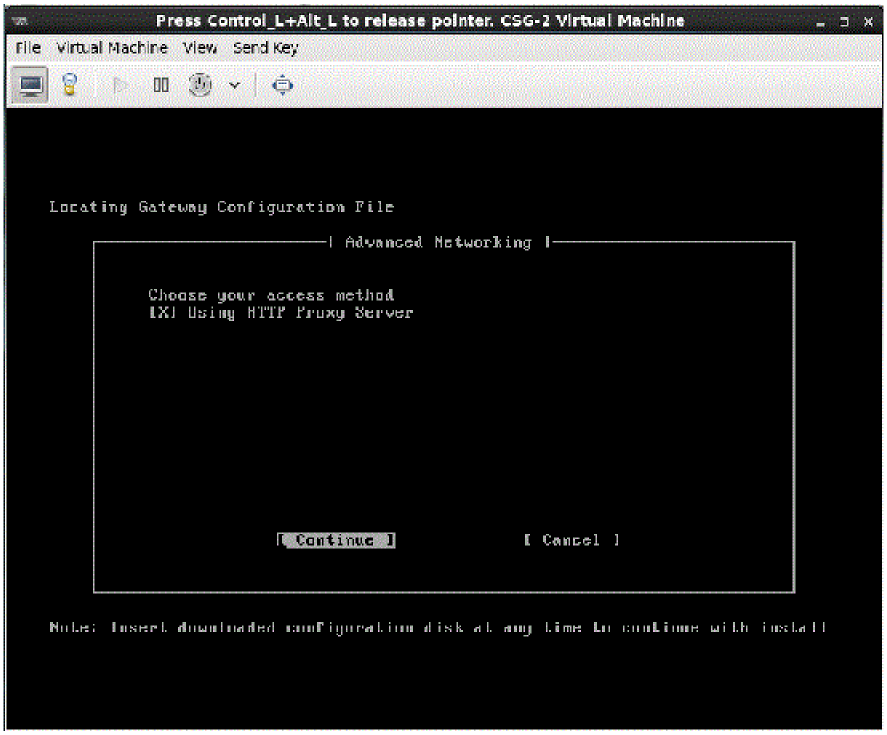
```
Locating Gateway Configuration File

    No configuration file could be found on this gateway.

    If you have downloaded a configuration disk for this gateway
    from the web, please insert it now.


    If it has not been downloaded onto a disk, you can download
    the file now by choosing "Download Config".

    If this is the second machine in a hardware failover
    configuration, you can download the file now from the first
    machine by choosing "Failover Config".


          [ Download Config  ]       [ Failover Config  ]


Note: Insert downloaded configuration disk at any time to continue with install
```

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


Press Control_L+Alt_L to release pointer. CSG-2 Virtual Machine
File
Virtual Machine
View
Send Key

```
Locating Gateway Configuration File

                        | Network Information |

   Enter your network information here:

   Download site:     [                                   ]

   ( ) Use Automatic (DHCP) configurations
        DHCP Name (Optional)     [                  ]
   ( ) Using PPPoE (DSL)
   (X) Manual Network Configuration:
        IP Address               [10.88.205.55    ]
        Netmask                  [255.255.252.0   ]
        Gateway IP Address       [10.88.201.1     ]
        DNS IP address           [144.20.190.70_  ]

             [   Next   ]      [  Cancel  ]      [ Advanced ]

Note: Insert downloaded configuration disk at any time to continue with install
```

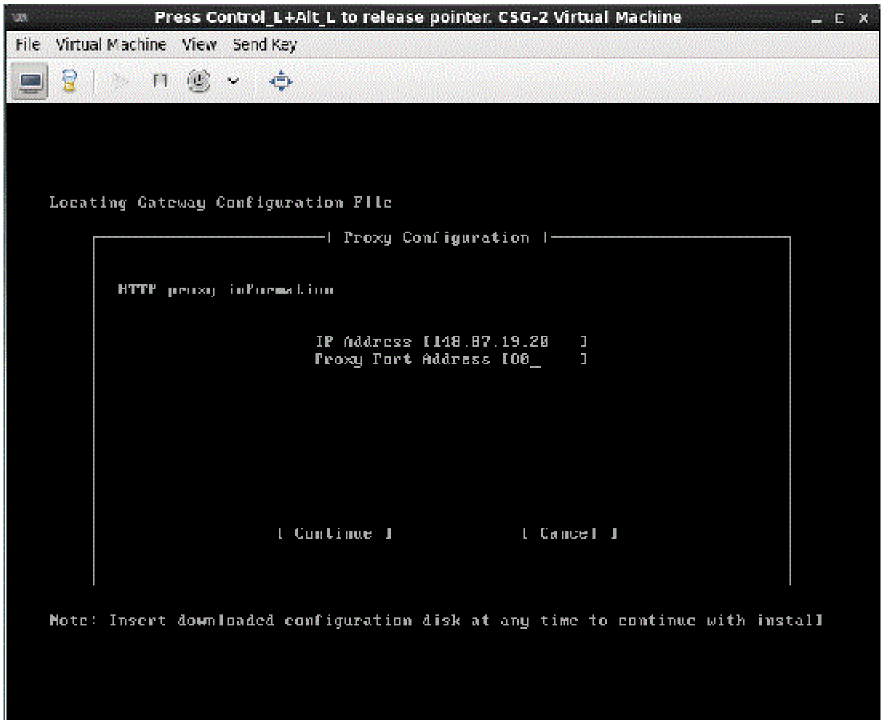
7. In this screen, enter information about your network interface facing Oracle Cloud (Internet). Move to **Advanced** to configure proxy.


Press Control_L+Alt_L to release pointer. CSG-2 Virtual Machine
File
Virtual Machine
View
Send Key

```
Locating Gateway Configuration File

                  ------------| Advanced Networking |------------

      Choose your access method
      [X] Using HTTP Proxy Server

                  [ Continue ]              [ Cancel ]

Note: Insert downloaded configuration disk at any time to continue with install
```

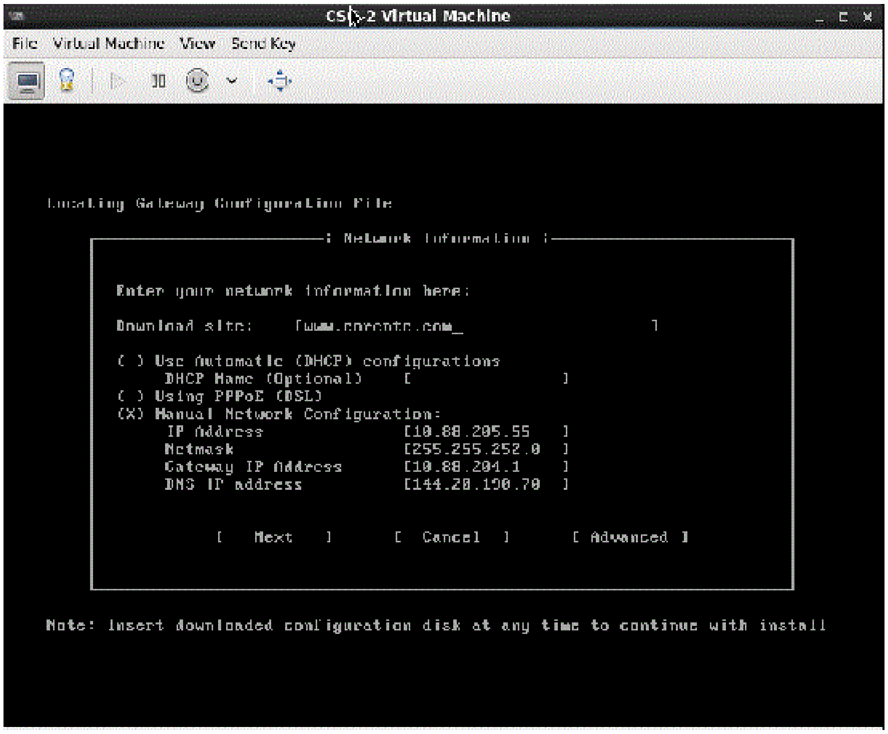
Select **Continue**.

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


Press Control_L+Alt_L to release pointer. CSG-2 Virtual Machine
File
Virtual Machine
View
Send Key

```
Locating Gateway Configuration File

      ----------------------| Proxy Configuration |----------------------

       HTTP proxy information


                            IP Address [148.87.19.20    ]
                            Proxy Port Address [80_     ]




                     [ Continue ]              [ Cancel ]


Note: Insert downloaded configuration disk at any time to continue with install
```

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



```
Locating Gateway Configuration File

      ----------------------: Network Information :----------------------

       Enter your network information here:

       Download site:    [www.corente.com_                     ]

       ( ) Use Automatic (DHCP) configurations
            DHCP Name (Optional)     [                  ]
       ( ) Using PPPoE (DSL)
       (X) Manual Network Configuration:
            IP Address               [10.88.205.55     ]
            Netmask                  [255.255.252.0    ]
            Gateway IP Address       [10.88.204.1      ]
            DNS IP address           [144.20.190.70    ]


              [   Next   ]      [  Cancel  ]      [ Advanced ]


Note: Insert downloaded configuration disk at any time to continue with install
```

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 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

- 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.
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–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.

4

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.

5

Configuring a GRE Tunnel on a Guest Instance in Oracle Cloud

To complete the VPN setup, configure a GRE tunnel between your guest instances in Oracle Cloud and your Corente Services Gateway instance in Oracle Cloud.

Topics

Oracle Cloud services certified to use Corente-based VPN solutions

You can configure a GRE tunnel only on instances of the following Oracle Cloud services:

- Oracle Cloud Infrastructure Compute Classic
- Oracle Database Cloud Service
- Oracle Java Cloud Service

Creating a New Linux Instance and Configuring a GRE Tunnel

You must configure a Generic Routing Encapsulation (GRE) tunnel on your Compute Classic instances to complete the VPN setup.

Follow the instructions provided in this section to create a guest instance using the provided `corente-guest-launchplan.json` template and configure a GRE tunnel on the newly created guest instance. To set up a GRE tunnel on running instances, see Configuring a GRE Tunnel on Running Linux Instances.

Create a Linux Client Compute Cloud Service Instance

Create your guest instance using the sample orchestration, `corente-guest-launchplan.json`.

1. Create a bootable storage volume. Use an image that is Oracle Linux 6.6 or later versions as only these versions support GRE tunneling. See Creating a Bootable Storage Volume in *Using Oracle Cloud Infrastructure Compute Classic*.

> **Note:**
>
> A persistent boot disk is required to retain data and patches that are applied to your instance.

2. Download the sample orchestration, `corente-guest-launchplan.json`, to create a guest instance. This sample orchestration 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

3. Modify values in the sample orchestration file based on your environment. While modifying `corente-guest-launchplan.json`, take care of the following requirements:

   - Ensure that you create the guest instance using the bootable storage volume you have created in step 1.
   - The client instance and the gateway instance should be in the same security list.

     In this example, a Compute instance in the Corente network is assigned to an internal security list, `vpn-CSG1-secrules`.
   - Ensure that the `ha_policy` of the orchestration is set to `active`.
   - The GRE tunnel addresses (both local and cloud gateway) should *not* be in the `10.x.x.x` subnet.
   - If you have set up the VPN connection using the Compute Classic user interface, specify the default value `172.16.254.1`.

4. Upload the modified orchestration to Compute Classic, and then start the orchestration. For information about uploading and starting an orchestration, see Managing Orchestrations in *Using Oracle Cloud Infrastructure Compute Classic*.

5. After creating the instance ensure that the instance is running.

6. Note the DNS hostname assigned to the cloud gateway instance. You will need this hostname later, when running the configuration script. This is needed for HA. The cloud gateway hostname is automatically populated, and should point to the private IP address of the cloud gateway.

Sample Orchestration with Corente Tunnel Arguments

```
{
  "name": "/Compute-myIdentityDomain/john.doe@example.com/corente-guest-
instance",
  "label": "corente-guest",
  "description": "Corente guest instance",
  "oplans": [
    {
      "obj_type": "launchplan",
      "label": "corente-guest-launchplan-1",
      "ha_policy: "active",
      "objects": [
        {
          "instances": [
      {
       "name": "/Compute-myIdentityDomain/john.doe@example.com/
corente-guest",
       "networking": {
        "eth0": {
         "model": "e1000",
         "dns": [
          "corente-guest"
         ],
         "seclists": [
          "/Compute-myIdentityDomain/john.doe@example.com/vpn-
CSG1-secrules"
         ],
         "nat": "ippool:/oracle/public/ippool"
        }
       },
       "boot_order": [
        1
       ],
       "storage_attachments": [
        {
         "index": 1,
         "volume": "/Compute-myIdentityDomain/
john.doe@example.com/corente-guest-boot-vol"
        }
       ],
       "label": "corente-guest",
       "shape": "oc3",
       "attributes": {
        "userdata": {
         "corente-tunnel-args": "--local-tunnel-
address=172.16.1.4 --csg-hostname=c9fcb5.compute-
acme.oraclecloud.internal. --csg-tunnel-address=172.16.254.1 --onprem-
subnets=10.2.3.0/24,10.3.2.0/24"
        }
       },
       "sshkeys": [
        "/Compute-myIdentityDomain/john.doe@example.com/adminkey"
       ]
      }
     ]
    }
   ]
  }
 ]
}
```

Create a GRE Tunnel

To create a GRE tunnel on your newly created Compute Classic instances:

1. SSH to the instance where you want to create a GRE tunnel.
2. Download the `oc-config-corente-tunnel` script onto this instance. This script is included in `Greconf_orchsamples.zip` file which is available at the following location:

http://www.oracle.com/technetwork/topics/cloud/downloads/network-cloud-service-2952583.html

3. Extract the contents of the `greconf_orchsamples.zip` file.
4. After extracting, copy the `oc-config-corente-tunnel` file from the `Config and Orchestration` directory to the `/usr/bin` directory.

> **Note:**
>
> You'll need superuser privileges to copy to `/usr/bin`.

5. Make the `oc-config-corente-tunnel` script executable:

```
sudo chmod 550 oc-config-corente-tunnel
```

6. Run the `oc-config-corente-tunnel` script:

```
sudo bash /usr/bin/oc-config-corente-tunnel
```

7. Add the following entry to `/etc/rc.local` so that the script runs automatically every time the instance boots:

```
bash /usr/bin/oc-config-corente-tunnel
```

About Configuration Script Arguments

The `oc-config-corente-tunnel` configuration script accepts arguments from the `userdata` attribute `corente-tunnel-args` in a launch plan (refer to `corente-guest-launchplan.json`). The value of that attribute should be in the form of a command line with the following syntax (showing only required arguments):

```
--local-tunnel-address=<addr> --csg-hostname=<hostname> --csg-tunnel-address=<addr> --onprem-subnets=<subnet_cidrs>
```

Parameter	Description	Example
`csg-hostname`	The host name of the cloud gateway instance is based on the value specified for the VPN gateway name while creating the cloud gateway. To identify this name, see the **Instances** page in the Compute Classic web console. Mandatory. No default value. No limit. The value for this parameter should follow the format: `*hostName*.compute-*myIdentityDomain*.oraclecloud.internal.`	`csg1.compute-acme.oraclecloud.internal.`

Parameter	Description	Example
`csg-tunnel-address`	If you have set up the VPN connection using theCompute Classic user interface, specify the default value `172.16.254.1`. Mandatory.	`172.16.254.1`
`local-tunnel-address`	GRE tunnel address of the Compute instance. Local address of the GRE tunnel to Corente Services Gateway instance on the Cloud. Specify the IP address that you want to assign to the GRE interface on the Linux instance. This IP address will be used to communicate with Corente Services Gateway, instances in your on-premise environment, and other IP addresses you define. Specify an IP address from the `172.16.1.0/24` subnet. Mandatory. No default value.	`172.16.1.4`
`onprem-subnets`	List of on-premise networks participating in VPN. This should be in the form of one or more comma-separated CIDRs. Mandatory. No default value. No limit.	`10.2.3.0/24,10.3.2.0/24`
`ping-count`	Number of pings of the cloud gateway tunnel end point in one iteration of health check. Optional. Default is 3. 2 is minimum.	5
`ping-timeout`	Timeout for each of the pings to the cloud gateway (in seconds). Optional. Default is 2. 1 is minimum.	1
`ping-interval`	Interval between pings to the cloud gateway (in seconds). Optional. Default is 10. 3 is minimum.	3

Configuring a GRE Tunnel on Running Linux Instances

You can set up a GRE tunnel to the Corente Services Gateway on existing instances of Compute Classic instances. You can use the procedure described in this chapter to set up a GRE tunnel on running Linux instances without having to restart orchestrations.

Ensure that the service instance on Oracle Cloud (where the GRE script runs) and the cloud gateway instance (the one it is paired with) are part of the same security list.

Do the following:

1. Install dig utility if it is not available. The dig utility is used for DNS resolution.

   ```
   yum install bind-utils
   ```

2. Create `opc-compute` directory in `/var/log` for Corente log files.

   ```
   cd /var/log
   mkdir opc-compute
   ```

3. Go to the `/usr/bin` directory.

   ```
   cd /usr/bin
   ```

4. Ensure that the script is executable. Run the following command:

   ```
   sudo chmod 550 oc-config-corente-tunnel
   ```

5. Run the following commands:

   ```
   $ sudo bash
   $ nohup ./oc-config-corente-tunnel --local-tunnel-address=172.16.2.2 --
   csg-hostname=csgdbaas-1.root.oraclecloud.internal --csg-tunnel-
   address=172.16.254.1 --onprem-subnets=192.168.39.0/24 &
   ```

   > **Note:**
   >
   > You may have to wait up to 1 minute before the GRE tunnel is up.

   For a description of the configuration parameters, see About Configuration Script Arguments.

   > **Note:**
   >
   > Customize the command-line parameters, as needed (same syntax as the `corente-tunnel-args userdata` attribute). You must run the script in background, as the script won't exit.

6. Verify that the GRE tunnel is functional by running the `ping` command to any live IP address within your data center network directly.

7. Add the following entry to the `/etc/rc.local` file.

   ```
   nohup bash /usr/bin/oc-config-corente-tunnel --local-tunnel-
   address=172.16.2.2 --csg-hostname=csgdbaas-1.root.oraclecloud.internal
   --csg-tunnel-address=172.16.254.1 --onprem-subnets=192.168.39.0/24 &
   ```

   > **Note:**
   >
   > Customize the command-line parameters, as needed. The values of the parameters should match what you entered in step 4.

Configuring a GRE Tunnel on a Windows Instance

To complete the VPN setup, configure a GRE tunnel between your Windows instance and Corente Services Gateway instance.

Topics

Creating a Windows Server 2012 R2 Client Instance

Follow the instructions provided in this section to create a Windows guest instance.

If you want to create a GRE tunnel on an existing Windows instance, skip this section and see Creating a GRE Tunnel on a Windows Guest Instance.

To create a guest Windows instance:

1. Identify the Windows image that you are going to use while creating the instance. Ensure that you use an image of Windows Server 2012 R2 as only Windows Server 2012 R2 with a hotfix applied supports GRE tunneling. Windows images are available in Oracle Cloud Marketplace.
2. Create your Windows guest instance from the Instances page. See Workflow for Creating Your First Windows Instance in *Using Oracle Cloud Infrastructure Compute Classic*. Take care of the following requirements:
   - By default, High Availability (HA) policy is set to `active`. Retain this value.
   - By default, RDP is enabled. Retain this value to use RDP to access your Windows instance.
   - By default, the Storage page shows the persistent boot disk that will be created and used to boot your instance. Retain this setting.

   > **Note:**
   >
   > A persistent boot disk is required to retain data and patches that are applied to your instance.

   If you are using the CLI tool or REST API for Compute Classic to automate instance creation, ensure that you use a bootable storage volume while creating your Windows instance.
3. After creating the instance, ensure that the instance is running.
4. Enable RDP access to your Windows instance. RDP access to your Windows instance is not enabled by default. See Accessing a Windows Instance Using RDP in *Using Oracle Cloud Infrastructure Compute Classic*.

After creating the instance, create a GRE tunnel on the instance. See Creating a GRE Tunnel on a Windows Guest Instance.

Creating a GRE Tunnel on a Windows Guest Instance

To complete the VPN setup, create a GRE tunnel between your guest Windows instance in Oracle Cloud and your Corente Services Gateway instance in Oracle Cloud. `oc-config-corente-tunnel.ps1` is a Windows PowerShell script which establishes the GRE tunnel between your Corente Services Gateway and your guest Windows instance in Oracle Cloud. The script continuously monitors the health of the GRE tunnel and re-establishes the tunnel on failure. You can schedule the script to run in a continuous loop on the instance and reconnects with the CSG instance when the CSG instance is restarted.

Before creating a GRE tunnel on your guest Windows instance, ensure that you complete the following prerequisites:

- The Windows guest instance and the Compute Classic instance on which you have set up Corente Services Gateway must be part of the `vpn-CSG1-secrules` security list. Add the Windows guest instance to the `vpn-CSG1-secrules` security list. For information about adding an instance to a security list, see Adding an Instance to a Security List in *Using Oracle Cloud Infrastructure Compute Classic*.
- Ensure that the registry key `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\TCPIP6\Parameters\DisabledComponents` exists and it’s value is set to 0.

  > **Caution:**
  >
  > Improper editing of registry keys can cause serious problems. For the instructions to edit registry keys, see the Windows documentation.

- Apply the hotfix provided by Microsoft to your Windows 2012 R2 server instance. For more information about downloading and applying the hotfix, see https://support.microsoft.com/en-us/kb/3022776.

  Ensure that the instance is running after applying the hotfix.
- Remote Access, a PowerShell module, should be available. Enter the following PowerShell command at the command prompt to display a list of all loaded modules.

  ```
  Get-Module -ListAvailable
  ```

  If you don't see Remote Access in the list, use the Server Manager tool to add Remote Access as a role. Select the Direct Access and VPN (RAS) role service while adding the Remote Access role.
- Ensure that you can RDP to your Windows instance. RDP access to your Windows instance is not enabled by default. To enable RDP access on your Windows instance, see Accessing a Windows Instance Using RDP in *Using Oracle Cloud Infrastructure Compute Classic*.

  Ensure that the Windows instance is running after enabling RDP access.

To create a GRE tunnel on your guest Windows instance after completing the prerequisites:

1. Download the `oc-config-corente-tunnel.ps1` script to your instance. You can either download the script directly on to the instance, or download the file elsewhere and copy the file to the instance. To download the file directly on to the instance, you should log in to the instance.

   You can download the script (included in `greconf_orchsamples.zip`) from the following location:

   http://www.oracle.com/technetwork/topics/cloud/downloads/network-cloud-service-2952583.html

2. Enter the following command at the command prompt to run the `oc-config-corente-tunnel.ps1` script. You must provide values for all the parameters. In the following example, it is considered that the `oc-config-corente-tunnel.ps1` script is available at `C:\`. When you run this command, specify the complete path of the location where you have downloaded the script file.

   Syntax

   ```
   powershell –File C:\oc-config-corente-tunnel.ps1 Name-of-tunnel CSG-hostname GRE-tunnel-destination-prefix GRE-local-IPAddress Remote-IPv4Subnet:Metric Prefix-length
   ```

   Example: Creating a GRE tunnel by specifying a single remote route

   ```
   powershell –File C:\oc-config-corente-tunnel.ps1 GREtoCSG
   csg1.compute-acme.oraclecloud.internal. 172.16.254.1/32 172.16.1.9
   192.168.10.0/24:100 24
   ```

   Example: Creating a GRE tunnel by specifying multiple remote routes

   ```
   powershell –File C:\oc-config-corente-tunnel.ps1 GREtoCSG
   c9fcb5.compute-acme.oraclecloud.internal. 172.16.254.1/32 172.16.1.9
   “192.168.10.0/24:100,192.168.133.0/24:100” 24
   ```

   The script runs checks to ensure that the prerequisites are met, and then establishes a GRE tunnel. The time taken to establish the tunnel varies depending on your environment. Do not close or quit the terminal window while the script is running.

   > **Note:**
   >
   > If you provide incorrect parameters, stop the script, and then enter the correct parameters to run the `oc-config-corente-tunnel.ps1` script.

   Parameter and descriptions

Parameter	Description	Example
`Name-of-tunnel`	An alphanumeric string representing a name for the GRE tunnel between the guest Windows instance in Oracle Cloud and the Corente Services Gateway instance in Oracle Cloud.	GREtoCSG

Parameter	Description	Example
CSG-hostname	The host name of the cloud gateway instance is based on the value specified for the VPN gateway name while creating the cloud gateway. You can find the DNS name on the instance information page in the Compute Classic web console. The value for this parameter should follow the format: *hostName*.compute-*myIdentityDomain*.oraclecloud.internal.	csg1.compute-acme.oraclecloud.internal.
GRE-tunnel-destination-prefix	Specify the default value 172.16.254.1/32, if you have not changed this value using App Net Manager.	172.16.254.1/32
GRE-local-IPAddress	Local address of GRE tunnel to Corente Services Gateway instance on Windows image side. This is also known as local-tunnel-address. Specify the IP address that you want to assign to the GRE interface on the Windows instance. This IP address will be used to communicate with Corente Services Gateway, instances in your on-premise environment, and other IP addresses you define. Specify an IP address from the 172.16.1.0/24 subnet.	172.16.1.9
Remote-IPv4Subnet:Metric	Remote-IPv4Subnet are customer reachable routes or on-premises subnets. You can also provide a comma-separated list of multiple remote subnets. Metric: Routing metrics are used for precedence when multiple routes exist to a single destination. In this case there is only one route. However, you must provide an integer value.	192.168.10.0/24:100 192.168.122.0/24:100, 192.168.133.0/24:100
Prefix-length	Prefix length for the subnet to which the GRE-local–IPAddress belongs.	If you specify 172.16.1.9 as the value for GRE-local–IPAddress and the IPv4Subnet to which GRE-local–IPAddress belongs is 172.16.1.0/24, then the Prefix-length is 24.

3. To automatically set up the GRE tunnel to Corente Services Gateway every time the system restarts, use the Task Scheduler in Windows to run the following

command on system restart. The example provided here is uses sample values. Specify values for the parameters based on your environment.

```
cmd /C powershell –File C:\oc-config-corente-tunnel.ps1 GREtoCSG c9fcb5.compute-
acme.oraclecloud.internal. 172.16.254.1/32 172.16.31.9 192.168.10.0/24:100 16>>c:
\corente.log 2>>&1cmd /C powershell –File C:\oc-config-corente-tunnel.ps1
GREtoCSG c9fcb5.compute-acme.oraclecloud.internal. 172.16.254.1/32 172.16.1.9
192.168.10.0/24:100 24>>c:\corente.log 2>>&1
```

For more information about using Task Scheduler to run a PowerShell script, see Windows documentation.

> **Note:**
>
> When the system restarts, the Remote Access service may not be available immediately. You might find a few error messages logged in the `C:\corente.log` file to indicate that Remote Access service is not available. However, the script runs continuously and the GRE tunnel is established when the Remote Access service becomes available.

6

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.

GRE Tunnel Problems

This section lists problems that you might encounter while configuring a GRE tunnel on a Guest Instance in Oracle Cloud.

Waiting for Remote Access Service

Description

The following error message is displayed when you run the run the `oc-config-corente-tunnel.ps1` script.

```
Waiting for Remote Access Service
get-vpns2sinterface : The term 'get-vpns2sinterface' is not recognized as the  name
of a cmdlet, function, script file, or operable program. Check the spelling of the
name, or if a path was included, verify that the path is  correct and try again.
```

Solution

This error indicates that the hotfix was applied on Windows Server 2012 R2 instance, but Remote Access, a PowerShell module, is not available.

To add Remote Access as a role using the Windows interface of the Server Manager console:

1. On the Server Manager Dashboard, under **Quick Start**, click **Add roles and features**.

   The Add Roles and Features Wizard appears.
2. On the Select role services page, under **Remote Access**, click **Role Services**.

   The Role services are listed.
3. Select the **DirectAccess and VPN (RAS)** check box, and then click **Next**.

   The Installation progress page appears. When the installation is complete, click **Close**.
4. On the Server Manager Dashboard, click **Tools**, and then click **Routing and Remote Access**.

   The Routing and Remote Access dialog box appears.
5. In the left pane, right-click the name of your Windows server, and then select **Configure and Enable Routing and Remote Access**.

   The Routing and Remote Access Server Setup Wizard is displayed.
6. On the Configuration page, select **Custom configuration**, and then click **Next**.
7. On the Custom Configuration page, select **VPN access**, and then click **Next.**
8. On the Completing the Routing and Remote Access Server Setup Wizard page, click **Finish**. The Routing and Remote Access dialog box appears.
9. Click **Start Service**, and then wait till the service is initialized.

GRE Script Fails with dig, nslookup

Description

When you run the GRE script, it fails and the following error message is displayed.

```
/bin/sh: dig: command not found
```

Solution

This error indicates that the Linux instance on which you are running the GRE script doesn’t have `bind-utils` installed.

Run the following command, and then rerun the GRE script.

```
sudo yum install bind-utils
```