Oracle® Cloud

Setting Up VPN from a Third-Party Gateway On-Premises to the Shared Network

E77625-14
May 2020

Oracle Cloud Setting Up VPN from a Third-Party Gateway On-Premises to the Shared Network,

E77625-14

Copyright © 2016, 2020, Oracle and/or its affiliates.

Primary Author: Sylaja Kannan

Contributing Authors: Kunal Rupani, Anirban Ghosh, Kumar Dhanagopal, Neeraj Sharma, Anamika Mukherjee

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or “commercial computer software documentation” pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government’s use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

Preface

This document describes how to set up VPN access from a third-party gateway to your guest instances in Oracle Cloud by installing Corente Service Gateway, which is an Oracle-provided IPSec solution, in your data center. 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

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 a Third-Party VPN Device

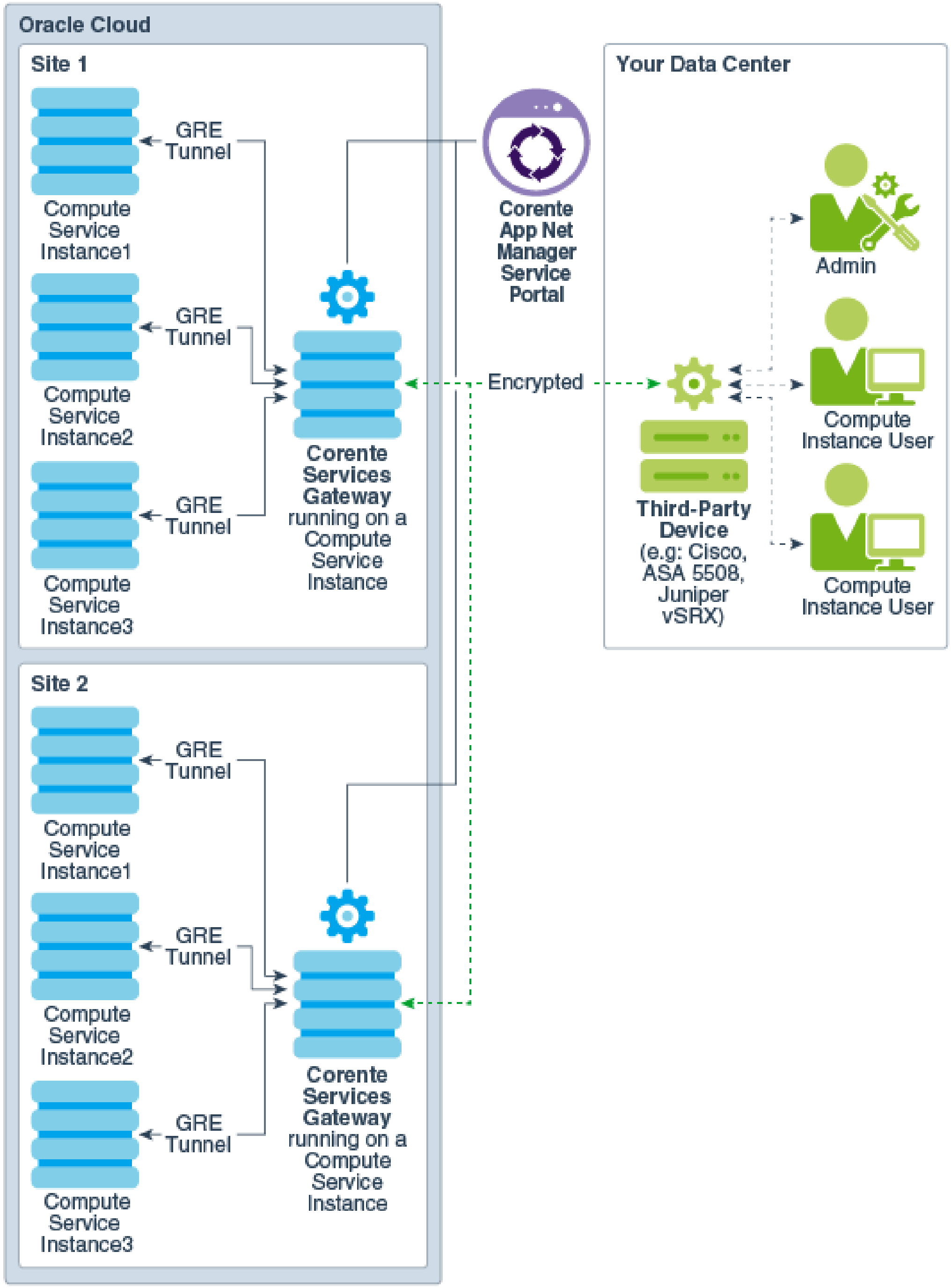
You can set up VPN access to Compute Classic instances by using Corente Services Gateway in Oracle Cloud and a certified third-party VPN device in your data center.

Topics

- Understanding the Architecture and Key Components of the Solution
- Certified Third-Party VPN Device Configurations
- Workflow for Setting Up VPN Using a Third-Party VPN Device

> **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 Corente Services Gateway in your data center to instances attached to the Oracle-provided shared network. See *Setting Up VPN from Corente Services 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 Services Gateway**: Corente Services Gateway is installed on a Compute Classic instance running on Oracle Cloud. It acts as a proxy that facilitates secure access and data transfer in the VPN solution.

  Your Compute Classic account can contain multiple sites. You must set up Corente Services Gateway on each site.

  After setting up the Corente Services Gateway, manually set up and configure a Generic Routing Encapsulation (GRE) tunnel from your Compute 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 Corente Services 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 components of your Corente-powered network.
- **Your own third-party VPN solution**: Any third-party VPN solution that allows interoperability with Corente Services Gateway.

Certified Third-Party VPN Device Configurations

The following table lists the third-party VPN device configurations that are supported in the Corente 9.4 release.

Certified Configurations	Devices
• Encryption AES256; Hash SHA-256 • DH phase 1 group 14 • No Perfect Forward Secrecy (PFS); so no Diffie-Hellman (DH) phase 2 group	Cisco 2921 Cisco ISR 4331 Checkpoint 3200 Palo Alto 3020 FortiGate-200D
• Encryption AES256; Hash SHA-256 • DH phase 1 group 14; DH phase 2 group 14	Cisco 2921 Cisco ISR 4331 Checkpoint 3200 Palo Alto 3020 FortiGate-200D
• Encryption AES128; Hash SHA-256 • DH phase 1 group 14; no PFS	Cisco 2921 Cisco ISR 4331 Checkpoint 3200 Palo Alto 3020 FortiGate-200D
• Encryption AES192; Hash SHA-1 • DH phase 1 group 2, DH phase 2 group 2	Cisco ASA5505
• Encryption AES256; Hash SHA-1 • DH phase 1 group 5; no PFS	Cisco ISR 4331 Checkpoint 3200 Palo Alto 3020 FortiGate-200D

Note:

Other devices may work if they are configured with the certified configurations.

The Corente Services Gateway uses IPSec and is behind a NAT, so network address translator traversal (NAT-T) is required. Ensure that the third-party device in your data center supports NAT-T.

Workflow for Setting Up VPN Using a Third-Party VPN Device

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 Classic welcome 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 Corente Services Gateway (cloud gateway) on Oracle Cloud.	Corente Services Gateway running on an Compute Classic instance, as shown in the architecture diagram.	See Creating a Cloud Gateway.
Add a third-party device and establish partnership between your third-party VPN device and the cloud gateway.	This is the dashed line between the third-party VPN device and the cloud gateway, as shown in the architecture diagram.	See Registering a Third-Party VPN Device See Connecting the Cloud Gateway with the Third-Party Device.
Configure a GRE tunnel on your Oracle Compute, Database, and Java Cloud Service instances.	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 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*.
- 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 **Single-homed**.
   - **Subnets:** Enter a comma-separated list of subnets (in CIDR format) that should be reachable using this gateway.

   > **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 with the shared 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**.

To use this gateway in a VPN connection, add a third-party device and then create a connection. See Registering a Third-Party VPN Device and Connecting the Cloud Gateway with the Third-Party Device.

You can also update the gateway instance to modify the reachable routes, or delete the gateway instance if you no longer require this gateway. See Modifying the Reachable Subnets for a VPN Gateway or Deleting a VPN Gateway.

> **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.

3 Registering a Third-Party VPN Device

To establish a VPN connection to your Compute Classic instances, after creating a Corente Services Gateway instance, register a VPN device to provide information about the third-party VPN gateway used in your data center.

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*.

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 **Customer Devices**.
4. Click **Create VPN Device**.
5. Select or enter the required information:
   - **Name:** Enter a name for the third-party VPN device.
   - **Type:** Select a supported third-party VPN device from the list.
   - **Model:** Enter the model of your third-party VPN device.
   - **WAN IP Address:** Enter the IP address of the WAN interface of your third-party VPN device.
   - **Visible IP Address:** Enter the public IP address of your third-party VPN device that the Corente Services Gateway should connect to. If you use network address translation (NAT), then this IP address would be different from the WAN IP address. Otherwise, the visible IP address would be the same as the WAN IP Address.
   - **Subnets:** Enter (in CIDR format) a comma-separated list of subnets in your data center that should be reachable using this third-party device.
   - **PFS:** This option is selected by default. If your third-party device supports Perfect Forward Secrecy (PFS), retain this setting to require PFS.
   - **DPD:** This option is selected by default. If your third-party device supports Dead Peer Detection (DPD), retain this setting to require DPD.
6. Click **Create**.

   A record of your third-party VPN device is created. Next, to use this VPN device to establish a VPN connection between your data center and your Compute Classic instances, create a VPN connection. See Connecting the Cloud Gateway with the Third-Party Device.

4 Connecting the Cloud Gateway with the Third-Party Device

After you've created a Corente Services Gateway instance and added a third-party device, to establish a VPN connection between your data center and your Compute Classic instances you must connect the cloud gateway with the third-party VPN device.

Prerequisites

- You must have already created the cloud gateway that you want to use. See Creating a Cloud Gateway.
- You must have already configured your third-party VPN device in your data center. See Certified Third-Party VPN Device Configurations.
- You must have already added the third-party VPN device that you want to connect to in your data center. See Registering a Third-Party VPN Device.
- 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 **Connections**.
4. Click **Create VPN Connection**.
5. Select or enter the required information:
   - **Gateway:** Select the Corente Services Gateway that you want to use. Each Corente Services Gateway can be used in multiple connections. However, each connection must reach distinct destination subnets.
   - **Device:** Select the third-party device that you want to use. Each device can be used in multiple connections. However, each connection must reach distinct destination subnets.
   - **IKE ID:** The Internet Key Exchange (IKE) ID. Only IKE v1 in Main Mode is supported. The IKE ID can be the name or IP address used to identify the Corente Services Gateway on the third-party device. Alternatively, you can specify a string that you want to use as the IKE ID.

     Select one of the following:

> **Note:**
>
> The third-party device that you use might not support all of the following options for IKE ID. Select the appropriate option for your device.

  - **Gateway Name:** The name of the Corente Services Gateway instance in the format `Corente_Domain_name.Corente_Services_Gateway_instance_name`. The name is auto-populated when you select this option.
  - **Gateway IP Address:** The private IP address (on the shared network) of the instance hosting the Corente Services Gateway. The IP address is auto-populated when you select this option. Note, however, that this address will change each time the instance is re-created.
  - **User-Defined IKE ID:** Enter text that you want to use as the IKE ID. You can specify either an alternative IP address, or any text string. If you specify a text string, you must prefix the string with `@`. For example, if you want to specify the text `IKEID-for-VPN1`, enter `@IKEID-for-VPN1`. If you specify an IP address, don't prefix it with `@`. The IKE ID is case sensitive and can contain a maximum of 255 ASCII alphanumeric characters including special characters, period (.), hyphen (-), and underscore (_). The IKE ID can't contain embedded space characters.

    > **Note:**
    >
    > If you specify the IKE ID, ensure that you specify the Peer ID type as **Domain Name** on the third-party device in your data center. Other Peer ID types, such as email address, firewall identifier or key identifier, aren't supported.

- **Shared Secret:** The shared secret, also called the pre-shared key (PSK) on some devices, is used while setting up the VPN connection to establish the authenticity of the Corente Services Gateway that is requesting the VPN connection. You must enter the same shared secret here and on your third-party device. The shared secret must contain only alphanumeric characters.

The VPN connection is created.

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
Managing VPN

Topics

> **Note:**
>
> You must have the `Compute_Operations` role to access the pages under the **VPN** tab. If you don't have this role, you won't be able to view these pages.

Listing VPN Gateways

After you've created one or more VPN gateways, you can see information about all your VPN gateways by using the web console.

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*.

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**.

The VPN Gateways page displays a list of all your Corente Services Gateways, along with information about each gateway such as the interface type and status of the gateway.

> **Note:**
>
> This page also displays Corente Services Gateways deployed on hosts outside of Compute Classic.

Each gateway can have any of the following statuses:

Status	Description
Active	The Corente Services Gateway instance is running.
Inactive	The Corente Services Gateway instance has been shut down or is being restarted. **Action:** If the instance is restarting, wait for it to return to the running state. If the instance has been shut down, start it to return to the Active state.
Download	The configuration file for the Corente Services Gateway is available to download, but hasn't been downloaded to the gateway instance. **Action:** Check that the required security rules or ACLs are in place and enabled, to allow the gateway instance to download the configuration file.
Downloaded	The configuration file for the Corente Services Gateway has been downloaded but not activated. This status usually indicates that the Corente Services Gateway is not yet installed or started. **Action:** Check that the gateway instance is running or restart the instance if required. Check that the required security rules or ACLs are in place and enabled.
Upgrade	A software upgrade is available for the Corente Services Gateway. **Action:** Schedule a maintenance time for the Corente Services Gateway in App Net Manager. The upgrade will occur automatically during the scheduled maintenance time. See the App Net Manager online help for more information.
Disconnected	The Corente Services Gateway has lost connectivity, without being powered off safely. **Action:** Check your network configuration to see if outbound connectivity has been blocked by firewall rules.
Denied	The Corente Services Gateway connection has been denied. **Action:** Contact Oracle Support.
New	A new Corente Services Gateway instance has been created using App Net Manager, but the configuration of this new gateway instance hasn't been completed. **Action:** Complete and save the configuration of the new gateway using App Net Manager. The new configuration will then be downloaded.
Unknown	The Corente Services Gateway is in an unknown state. **Action:** Check the status again after some time, or contact Oracle Support.

Modifying the Reachable Subnets for a VPN Gateway

You must specify the list of reachable subnets while creating a VPN gateway. If required, you can modify this list of subnets at any time after creating a VPN gateway.

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*.

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. Go to the VPN gateway for which you want to modify the set of subnets. From the menu, select **Update**.
5. Modify the list of subnets as required, and then click **Update**.

   The list of subnets reachable by the VPN gateway is updated.

> **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.

Deleting a VPN Gateway

If you no longer require a VPN connection, you can stop the connection and delete the VPN gateway instance. Each VPN gateway instance is managed by a master orchestration that can be used to start or stop several nested orchestrations. To delete a VPN gateway instance, go to the VPN Gateways page in the web console and stop the master orchestration.

Prerequisites

- The VPN gateway that you want to delete should not be connected to any device. If the gateway is used in a VPN connection, stop the connection first. See Deleting a VPN Connection.
- 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. Go to the Corente Services Gateway instance that you want to delete.
   - If you want to delete only the gateway instance, from the menu, select **Stop**. The orchestration that controls the gateway instance is stopped. This deletes the Corente Services Gateway instance.
   - If you want to delete the gateway instance as well as other associated resources, from the menu, select **Stop All**. The master orchestration that controls the gateway instance and its associated resources is stopped. This deletes the gateway instance as well as resources created by the nested orchestrations, such as the bootable storage volume and networking objects.

   > **Note:**
   >
   > Resources created outside the master orchestration, such as the public IP address reservation or IP networks, aren't deleted when you stop the master orchestration for the gateway instance. If you no longer need those resources, remember to delete them after you've stopped the master orchestration.

   After you've deleted a gateway instance, it continues to be listed on the VPN Gateways page, with the status **Stopped**. At any time, you can restart the master orchestration to re-create the cloud gateway instance and its associated resources.
5. If you want to delete the orchestrations associated with your gateway instance, go to the gateway instance and from the menu, select **Delete**.

   The master orchestration and the associated orchestrations for the instance, storage volumes, and security rules are deleted. The VPN gateway is no longer listed on the VPN Gateways page.

Listing Third-Party VPN Devices

After you've added third-party devices, you can see information about all your third-party devices by using the web console.

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*.

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 **Customer Devices**.

The Customer Devices page displays a list of all the third-party devices that you've added, along with information about each device such as its model and type and its IP address.

Updating a Third-Party Device

After you've added a third-party device, if required, you can modify the information associated with a third-party devices by using the web console.

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*.

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 **Customer Devices**.
4. Go to the device that you want to update. From the ☰ menu, select **Update**.
5. In the Update VPN Device dialog box, modify the information as required. Note that you can't change the device name or type. If you need to modify that information, add a new device. You can modify the following device information:
   - **Model:** The model of your third-party VPN device.
   - **WAN IP Address:** The IP address of the WAN interface of your third-party VPN device.
   - **Visible IP Address:** The public IP address of your third-party VPN device that the Corente Services Gateway should connect to. If you use network address translation (NAT), then this IP address would be different from the WAN IP address. Otherwise, the visible IP address would be the same as the WAN IP Address.
   - **Subnets:** A list of IP addresses or subnets in your data center that should be reachable by this third-party device.
   - **PFS:** Perfect Forward Secrecy.
   - **DPD:** Dead Peer Detection.
6. Click **Update**. The device information is updated.

Deleting a Third-Party Device

After you've added a third-party device, if you no longer want to use the device in a VPN connection, you can delete the device information by using the web console.

Prerequisites

- The device that you want to delete should not be used in a VPN connection. If the device is used in a VPN connection, stop the connection first. See Deleting a VPN Connection.
- 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 **Customer Devices**.
4. Go to the device that you want to delete. From the ☰ menu, select **Delete**.

   The information about the selected device is deleted and the device is no longer displayed on the Customer Devices page.

Listing VPN Connections

After you've created a connection between your VPN gateway and your third-party device, you can see a list of connections by using the web console.

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*.

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 **Connections**.

When a single-homed gateway is used in a connection, the **IP Route** column isn't used.

The Connections page also shows the status of each of your VPN connections. If a VPN connection has any status other than **Up**, check the status again after some time. If the status doesn't change to **Up**, then contact Oracle Support.

Updating a VPN Connection

After you've created a connection between a VPN gateway and a third-party device, if required, you can modify the IKE ID or the shared secret by updating the VPN connection.

The IKE ID and shared secret that you enter here must match the corresponding entries on the third-party device used in this connection. If you make any changes to these fields, ensure that the corresponding changes are made on the connected third-party device.

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*.

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 **Connections**.
4. Go to the connection that you want to modify. From the menu, select **Update**.
5. Update the IKE ID or modify the shared secret as required, and then click **Update**.

   The IKE ID or shared secret is updated.

> **Note:**
>
> The IKE ID and shared secret are used to identify and authenticate the Corente Services Gateway on the third-party device. If you modify these fields, ensure that the information you enter here matches the corresponding entries on the third-party device used in this connection.

Deleting a VPN Connection

After you've created a connection between a VPN gateway and a third-party device, if you no longer want to use this VPN connection, you can delete the connection.

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*.

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 **Connections**.
4. To delete a VPN connection, go to the connection that you want to delete. From the menu, select **Delete**.

   This ends the partnership between the specified VPN gateway and the third-party device and deletes the route orchestration. The VPN connection is no longer listed on the Connections page.

After deleting a VPN connection, you can also delete the gateway instance or delete the information about the third-party device used in this connection. See Deleting a VPN Gateway or Deleting a Third-Party Device.

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.
- If you encounter issues while setting up the GRE tunnel, see GRE Tunnel 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, such as incorrect **WAN IP Address** or **Visible IP Address** while registering the third-party VPN device. See Registering a Third-Party VPN Device. Such failures can also occur if you have provided incorrect pre-shared key (PSK) as the **Shared Secret**. See Connecting the Cloud Gateway with the Third-Party Device.

To resolve this error, ensure that the information you have provided is correct. For information about updating a third-party VPN device, see Updating a Third-Party Device. For information about updating the PSK, see Updating a VPN Connection.

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
```