



Pexip Infinity and Oracle Cloud Infrastructure

Deployment Guide

Software Version 33

Document Version 33.a

October 2023


] pexip[

Contents

Introduction	3
Deployment guidelines	4
Deployment options	4
Recommended instance types and call capacity guidelines	5
Security and SSH keys	5
Site-to-Site VPN for private/hybrid cloud deployments	6
IP addressing	6
Preparing your Oracle Cloud environment	7
Assumptions and prerequisites	7
Creating a compartment	7
Oracle Cloud Regions	8
Creating a Virtual Cloud Network (VCN)	8
Configuring the VCN Security List	9
Obtaining and preparing disk images for Oracle Cloud deployments	9
Deploying a Management Node in Oracle Cloud	13
Deploying the VM	13
Bootstrapping the Management Node	14
Running the installation wizard	15
Next steps	16
Initial platform configuration — Oracle Cloud	17
Accessing the Pexip Infinity Administrator interface	17
Configuring the Pexip Infinity platform	17
Next step	18
Deploying a Conferencing Node in Oracle Cloud	19
Deploying the VM	19
Generating, downloading and deploying the configuration file	21
Deploying Conferencing Nodes in additional Oracle Cloud regions	24
Managing Oracle Cloud Infrastructure VM instances	28
Temporarily removing (stopping) a Conferencing Node instance	28
Reinstating (restarting) a stopped Conferencing Node instance	28
Permanently removing a Conferencing Node instance	28

Introduction

The Oracle Cloud Infrastructure (OCI) service provides scalable computing capacity in the Oracle Cloud. Using Oracle Cloud eliminates your need to invest in hardware up front, so you can deploy Pexip Infinity even faster.

 Pexip Infinity deployments in Oracle Cloud Infrastructure is a technical preview feature.

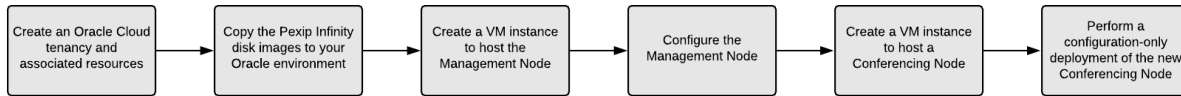
You can use Oracle Cloud to launch as many or as few virtual servers as you need, and use those virtual servers to host a Pexip Infinity Management Node and as many Conferencing Nodes as required for your Pexip Infinity platform.

Pexip publishes disk images for the Pexip Infinity Management Node and Conferencing Nodes. These images may be used to launch instances of each node type as required.

Deployment guidelines

This section summarizes the Oracle Cloud deployment options and limitations, and provides guidance on our recommended Oracle Cloud instance types, security groups and IP addressing options.

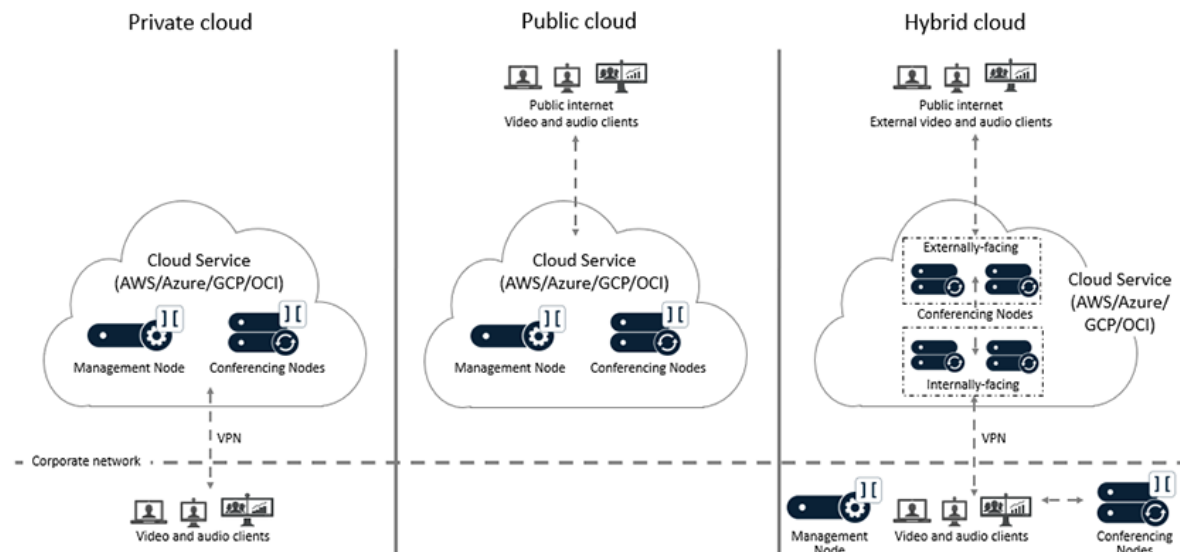
This flowchart provides an overview of the basic steps involved in deploying the Pexip Infinity platform on Azure:



Deployment options

There are three main deployment options for your Pexip Infinity platform when using the Oracle Cloud platform:

- **Private cloud:** all nodes are deployed within Oracle Cloud. Private addressing is used for all nodes and connectivity is achieved by configuring a VPN tunnel between the corporate network and Oracle Cloud. As all nodes are private, this is equivalent to an on-premises deployment which is only available to users internal to the organization.
- **Public cloud:** all nodes are deployed within Oracle Cloud. All nodes have a private address but, in addition, public IP addresses are allocated to each node. The node's private addresses are only used for inter-node communications. Each node's public address is then configured on the relevant node as a static NAT address. Access to the nodes is permitted from the public internet, or a restricted subset of networks, as required. Any systems or endpoints that will send signaling and media traffic to those Pexip Infinity nodes must send that traffic to the public address of those nodes. If you have internal systems or endpoints communicating with those nodes, you must ensure that your local network allows such routing.
- **Hybrid cloud:** the Management Node, and optionally some Conferencing Nodes, are deployed in the corporate network. A VPN tunnel is created between the corporate network and Oracle Cloud. Additional Conferencing Nodes are deployed in Oracle Cloud and are managed from the on-premises Management Node. The Oracle Cloud-hosted Conferencing Nodes can be either internally-facing, privately-addressed (private cloud) nodes; or externally-facing, publicly-addressed (public cloud) nodes; or a combination of private and public nodes (where the private nodes are in a different Pexip Infinity system location to the public nodes).



All of the Pexip nodes that you deploy in the cloud are completely dedicated to running the Pexip Infinity platform— you maintain full data ownership and control of those nodes.

Recommended instance types and call capacity guidelines

Oracle Cloud instances come in many different sizes. In general, Pexip Infinity Conferencing Nodes should be considered compute intensive and Management Nodes reflect a more general-purpose workload. Our [Server design recommendations](#) also apply to cloud-based deployments.

For deployments of up to 20 Conferencing Nodes, we recommend using the following shapes:

- **Management Node:** VM.Standard3.Flex (or VM.Standard2 if 3.Flex isn't available) with 2 OCPUs or larger.
- **Transcoding Conferencing Nodes:** VM.Standard3.Flex (or VM.Standard2 if 3.Flex isn't available) with a minimum of 2 OCPUs.
- **Proxying Edge Nodes:** VM.Standard3.Flex (or VM.Standard2 if 3.Flex isn't available) with 2 OCPUs.

Note that 1 OCPU gives 2 vCPUs, either because the hypervisor has available physical cores, or because of Hyper-Threading on a single physical core.

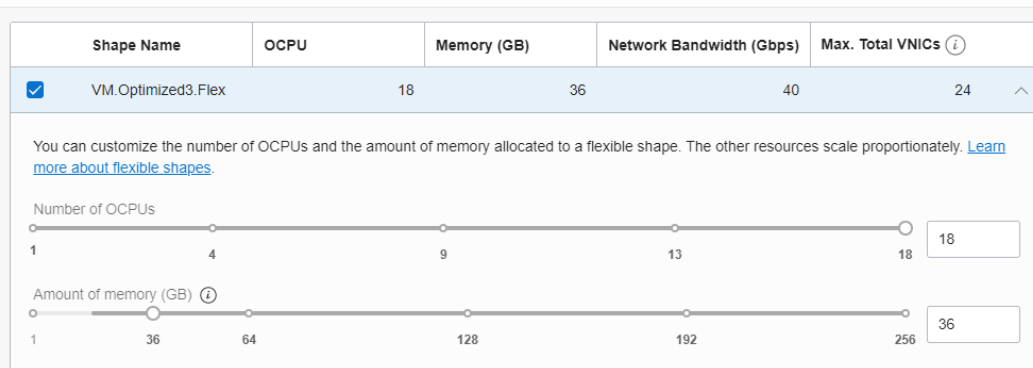
We have observed the following performance guidelines for HD call capacity per Transcoding Conferencing Node:

- VM.Standard.2 (Intel 8167M @ 2.0GHz)
 - 4 OCPUs: 12 HD
 - 8 OCPUs: 23 HD
 - 24 OCPUs: 63 HD
- VM.Optimized3.Flex (Intel Xeon Gold 6354 CPU @ 3.0GHz)
 - 4 OCPUs: 23 HD
 - 8 OCPUs: 44 HD
 - 18 OCPUs: 82 HD

For all available machine types see: <https://docs.oracle.com/en-us/iaas/Content/Compute/References/computeshapes.htm>.

Note that if you select an Optimized3.Flex Intel-shape you need to configure the number of OCPUs and memory (assign 2GB of memory for each OCPU):

Browse All Shapes



Security and SSH keys

SSH access to Oracle-hosted Pexip Infinity nodes/instances requires key-based authentication (password-based authentication is not supported). An SSH key pair must be assigned to each instance at launch time. You can create key pairs within Oracle Cloud while creating an instance, or use third-party tools such as PuTTYgen to generate a key pair and then import the public key while creating an instance.

Note that:

- Pexip Infinity node instances only support a single SSH key pair.
- If you are using a Linux or Mac SSH client to access your instance you must use the **chmod** command to make sure that your private key file on your local client (SSH private keys are never uploaded) is not publicly viewable. For example, if the name of your private key file is my-key-pair.pem, use the following command: `chmod 400 /path/my-key-pair.pem`

Site-to-Site VPN for private/hybrid cloud deployments

For a private or hybrid cloud deployment, you need to configure a site-to-site VPN to connect your on-premises network to the Oracle Cloud VCN.

See <https://docs.oracle.com/en-us/iaas/Content/Network/Tasks/overviewIPsec.htm> for information about using VPN Connect.

IP addressing

All Oracle VM instances are allocated a **Private IP address**. You can optionally also assign a static (reserved) **Public IP address** to a VM instance. You should assign a public address to all nodes in a public cloud deployment, and to any externally-facing nodes in a hybrid deployment, that you want to be accessible to conference participants located in the public internet.

Pexip Infinity nodes must always be configured with the private IP address associated with its instance, as it is used for all internal communication between nodes. To associate an instance's public IP address with the node, configure that public IP address as the node's **Static NAT address** (via **Platform > Conferencing Nodes**).

The private IP address should be used as the Conferencing Node address by users and systems connecting to conferences from the corporate network (via the site-to-site VPN) in a private or hybrid cloud deployment. When an instance has been assigned a public IP address and that address is configured on the Conferencing Node as its **Static Nat address**, all conference participants **must** use that external address to access conferencing services on that node.

Preparing your Oracle Cloud environment

This topic explains how to prepare your Oracle Cloud environment before installing Pexip Infinity. It covers:

- [Assumptions and prerequisites](#)
- [Creating a compartment](#)
- [Oracle Cloud Regions](#)
- [Creating a Virtual Cloud Network \(VCN\)](#)
- [Configuring the VCN Security List](#)
- [Obtaining and preparing disk images for Oracle Cloud deployments](#)

All configuration is performed via the Oracle Cloud Console.

A summary of the key terminology and concepts used in the Oracle Cloud Infrastructure (OCI) can be found at <https://docs.oracle.com/en-us/iaas/Content/GSG/Concepts/concepts.htm>.

Note that the images shown in this guide depict an example deployment. Unless explicitly stated, you should use your own resource names and address spaces etc. as appropriate for your own environment. Also, as the Oracle Cloud Console is regularly updated, some images and labels shown here may not directly match the currently available options.

Assumptions and prerequisites

The deployment instructions assume that within Oracle Cloud you have already:

- signed up to the Oracle Cloud Infrastructure platform and created a tenancy
- configured a VPN (for a private or hybrid cloud deployment)

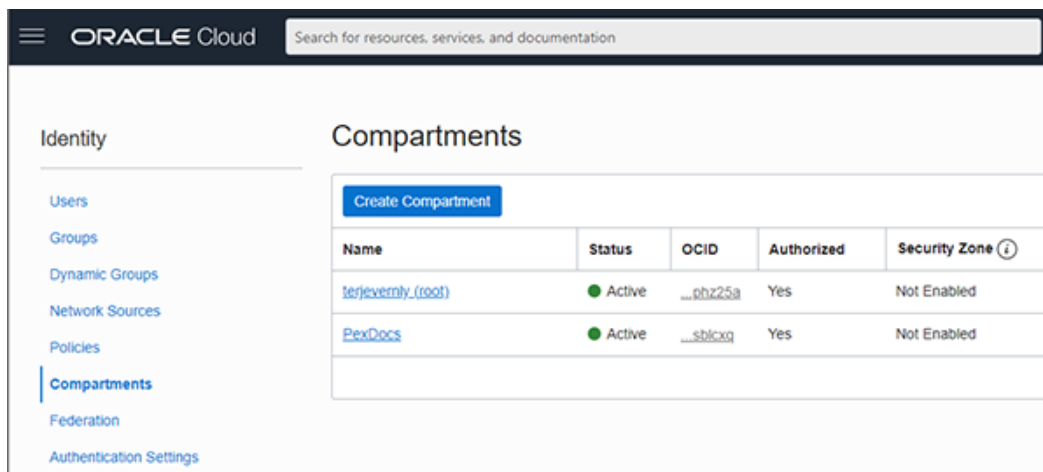
For more information on setting up your Oracle Cloud environment, see <https://docs.oracle.com/en-us/iaas/Content/GSG/Concepts/settinguptenancy.htm> and <https://docs.oracle.com/en-us/iaas/Content/Compute/Tasks/launchinginstance.htm> for more details.

Creating a compartment

A compartment is a logical container for the collection of resources used for your Pexip Infinity deployment. A compartment is not specific to a region.

You create a compartment via **Identity & Security > Compartments**.

We recommend creating a separate compartment for each Pexip Infinity deployment (e.g. production system, lab system). This example has created a "PexDocs" compartment within the root compartment.



Oracle Cloud Regions

When planning your installation you must decide in which Oracle Cloud Region(s) to deploy your nodes. You can deploy all of your nodes in one region or you can spread them across one or more regions.

A region is broadly equivalent to a Pexip Infinity location, although you could also map them to an Availability Domain within a region.

Note that when using the Oracle Cloud Console, your current region is displayed at the top of the Console. If your tenancy is subscribed to multiple regions, you can switch regions by selecting a different region from the Region menu.

See <https://docs.oracle.com/en-us/iaas/Content/General/Concepts/regions.htm> for more information.

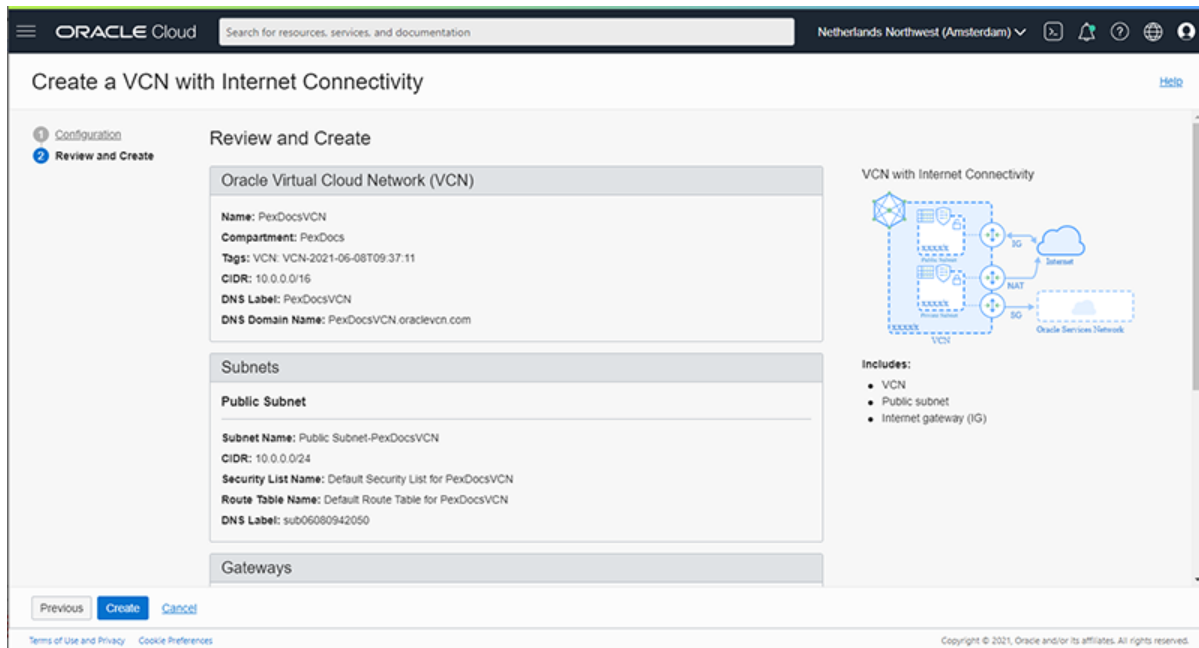
Creating a Virtual Cloud Network (VCN)

A Virtual Cloud Network (VCN) is a virtual, private network that you set up in Oracle data centers. It resembles a traditional network, with firewall rules and specific types of communication gateways that you can use. A VCN resides in a single OCI region and covers a single, contiguous IPv4 CIDR block of your choice.

i All regions to be included in the Pexip installation need non-overlapping CIDR ranges.

To create a VCN:

1. Go to **Networking > Virtual Cloud Networks**.
2. Ensure your **Compartment** is selected.
3. Select **Start VCN Wizard**.
4. Select **VCN with Internet Connectivity**.
5. Select **Start VCN Wizard**.
6. Enter a **VCN Name**.
7. Use the default CIDR blocks listed for the VCN and subnets, or specify a different range if required.
Remember to choose your CIDR blocks so that they don't overlap with any other region.
8. Ensure that **Use DNS Hostnames in the VCN** is selected.
9. Select **Next**.
10. Review the information and select **Previous** to make changes or select **Create** to create the VCN.



The default Security List for the VCN needs to be edited to allow administrative access to the Management Node, for the Pexip nodes to communicate, and for internet access for WebRTC and SIP with their respective UDP and TCP ports.

1. Go to **Networking > Virtual Cloud Networks** and select your VCN.
2. Select **Security Lists**.
3. Select the **Default Security List** for your VCN.
4. Use the Add and Edit options to modify the **Ingress** rules as shown below. All rules should not be stateless.

Where **0.0.0.0/0** implies any source/destination, **<management station IP address/subnet>** should be restricted to a single IP address or subnet for SSH access only, and **10.0.0.0/8** is for the internal communication between the Pexip nodes via their private IP addresses.

There is no need to modify the default Egress rules.

Your ingress rules should look similar to these:

Obtaining and preparing disk images for Oracle Cloud deployments

To deploy the Pexip Infinity software you need to create Oracle Custom Images from Pexip's generic Management Node and Conferencing Node OVA files.

If you intend to deploy Conferencing Nodes in multiple regions, you'll need to create a custom image of the Pexip generic Conferencing Node in every region, unless you have enabled replication.

To create your images:

- Download to your local PC the generic OVAs for the Pexip Infinity Management Node and Conferencing Nodes.
 - Go to <https://dl.pexip.com/infinity/index.html> and then select the appropriate directory for your software version.
 - Download the generic Management Node OVA (Pexip_Infinity_v<version>_generic_pxMgr_<build>.ova).
 - Download the generic Conferencing Node OVA (Pexip_Infinity_v<version>_generic_ConfNode_<build>.ova).
- Create a bucket in the Oracle Object Storage (Storage > Buckets). A bucket is a logical container used by Object Storage for storing your files.

You can use the default bucket properties.

In this example, "Pexip-images" was created:

The screenshot shows the Oracle Cloud console interface. On the left, there's a sidebar with 'Object Storage & Archive Storage' and 'Buckets' selected. The main area is titled 'Buckets in PexDocs Compartment'. Below the title, there's a 'Create Bucket' button and a table listing buckets. The table has columns for 'Name', 'Default Storage Tier', and 'Visibility'. One bucket named 'Pexip-images' is listed with a 'Standard' storage tier and 'Private' visibility.

Name	Default Storage Tier	Visibility
Pexip-images	Standard	Private

- Select the bucket and then Upload the two generic OVA files that you downloaded in step 1 into the bucket.

The screenshot shows the Oracle Cloud console interface for the 'Pexip-images' bucket. The top section shows bucket information: 'Visibility: Private', 'Namespace: axwgc69m6az', 'Default Storage Tier: Standard', 'Auto-Tiering: @ Disabled', 'Approximate Count: 1 objects', 'ETag: 3a5210d1-391d-408a-87fa-f9ce308e93ba', 'OCID: ...xgs6ppra', 'Encryption Key: Oracle managed key', 'Created: Tue, Jun 8, 2021, 16:01:15 UTC', 'Compartment: PexDocs', 'Approximate Size: 642.87 MiB', 'Emit Object Events: @ Disabled', and 'Object Versioning: @ Disabled'. Below this, the 'Objects' section shows two uploaded files: 'Pexip_Infinity_v25.4_generic_ConfNode_59565.ova' (642.87 MiB) and 'Pexip_Infinity_v25.4_generic_pxMgr_59565.ova' (1.33 GiB).

Name	Last Modified	Size	Storage Tier
<input type="checkbox"/> Pexip_Infinity_v25.4_generic_ConfNode_59565.ova	Tue, Jun 8, 2021, 16:25:25 UTC	642.87 MiB	Standard
<input type="checkbox"/> Pexip_Infinity_v25.4_generic_pxMgr_59565.ova	Tue, Jun 8, 2021, 16:37:27 UTC	1.33 GiB	Standard

- Create Oracle Custom Images from these two OVA files:
 - Go to Compute > Custom Images.
 - Select Import Image.
 - Enter a Name, for example "Pexip generic Management Node" or "Pexip generic Conferencing Node".
 - Select the Bucket (if necessary) and for Object name select the relevant OVA file.
You can use the default image settings provided by Oracle.
 - Select Import Image to start the import.

- f. Repeat the process for the second OVA file. You can start the second import while the first import is still in progress (they are asynchronous operations).

Import Image [Help](#)

Create in compartment

PexDocs

terjevemly (root)/PexDocs

Name

Pexip generic Mangement Node

Operating system

Linux

☒ Import from an Object Storage bucket

☐ Import from an Object Storage URL

Bucket in PexDocs [\(Change Compartment\)](#)

Pexip-images

Object name

Pexip_Infinity_v25.4_generic_pxMgr_59565.ova

Image type

☒ VMDK
Virtual machine disk file format. For disk images used in virtual machines.

☐ QCOW2
For disk image files used by QEMU.

☐ OCI
For images that were exported from Oracle Cloud Infrastructure. The launch mode is specified in the .oci file and can't be changed in the Console.

Launch mode

Firmware: BIOS

NIC attachment type: PV NIC

Boot volume type: PV

Remote data volume: PV

☒ Paravirtualized Mode
For virtual machines that [support paravirtualized drivers](#), created outside of Oracle Cloud Infrastructure.

☐ Emulated Mode
For virtual machines that [don't support paravirtualized drivers](#), created outside of Oracle Cloud Infrastructure from older on-premises physical or virtual machines.

☐ Native Mode
For images that were exported from Oracle Cloud Infrastructure.

[Show tagging options](#)

[Import Image](#) [Cancel](#)

This process takes 20-25 minutes per image and results in the two custom images you need for installation.

Compute

- Instances
- Dedicated Virtual Machine Hosts
- Instance Configurations
- Instance Pools
- Cluster Networks
- Autoscaling Configurations
- Capacity Reservations
- Custom Images**

Custom Images *in PexDocs Compartment*

An image is a template of a virtual hard drive. It determines the operating system and other software for an instance. You can [create custom images](#), regions, and [bring your own image](#) to the cloud.

[Import Image](#)

Name	State	Original Image	Billable Size (GB) ⓘ
Pexip_generic_Conferencing_Node	Available	-	2
Pexip_generic_Management_Node	Available	-	3

Custom images and instance shapes

Not all instance shapes are automatically available for a custom image. For example, if you want to use a VM.Optimized3.Flex shape you need to manually make it available:

1. Go to **Compute > Custom Images**.
2. Select the custom image.
3. Select **Edit Details**.
4. Select (tick) the shapes you want to make available, e.g. VM.Optimized3.Flex.
5. Select **Save Changes**.

Deploying a Management Node in Oracle Cloud

As with all Pexip Infinity deployments, you must first deploy the Management Node before deploying any Conferencing Nodes. In a hybrid cloud deployment the Management Node may be deployed in the corporate network or in Oracle Cloud. This section describes how to deploy the Management Node in Oracle Cloud.

Deploying the VM

To deploy a Management Node on an Oracle Cloud VM:

1. Prepare a Management Node disk image as described in [Obtaining and preparing disk images for Oracle Cloud deployments](#).
2. From the Oracle Console, go to **Compute > Instances**.
3. Select **Create Instance**.
4. Enter a **Name**, for example "pexmgr".
5. Ensure the correct **Compartment** is selected.
6. In the **Image and shape** section:
 - a. Change the Image to the previously created Custom Image for the Management Node. (Change the Image source to *Custom images* to see the options.)

Browse All Images

An image is a template of a virtual hard drive that determines the operating system and other software for an instance.

Image source
Custom images

Compartment
PexDocs

terjevemly (root)/PexDocs

Create or import [custom images](#) into your Oracle Cloud Infrastructure environment.

Custom Image Name	Created
<input type="checkbox"/> Pexip generic Conferencing Node	Wed, Jun 9, 2021, 09:02:36 UTC
<input checked="" type="checkbox"/> Pexip generic Mangement Node	Wed, Jun 9, 2021, 08:56:23 UTC

1 Selected Showing 2 Items < 1 of 1 >

- b. Select an appropriate shape for the Management Node. We recommend: VM.Standard3.Flex (or VM.Standard2 if 3.Flex isn't available) with 2 OCPUs or larger.

See [Recommended instance types and call capacity guidelines](#) for more information, and see [Custom images and instance](#)

[shapes](#) if your required shape is not available.

Browse All Shapes

Instance type

Virtual Machine
A virtual machine is an independent computing environment that runs on top of physical bare metal hardware. ✓

Bare Metal Machine
A bare metal compute instance gives you dedicated physical server access for highest performance and strong isolation.

Shape series

AMD
Flexible OCPU count. AMD processors.

Intel
Current generation Intel processors. ✓

Ampere
Arm-based processor.

Specialty and Previous Generation
Earlier generation AMD and Intel Standard shapes. Always Free, Dense I/O, GPU, and HPC shapes.

Image: Custom Custom

Shape Name	OCPU	Memory (GB)	Network Bandwidth (Gbps)	Max. Total VNICS
<input type="checkbox"/> VM.Standard2.1	1	15	1	2
<input checked="" type="checkbox"/> VM.Standard2.2	2	30	2	2
Local Disk: Block Storage Only				
<input type="checkbox"/> VM.Standard2.4	4	60	4.1	4
<input type="checkbox"/> VM.Standard2.8	8	120	8.2	8
<input type="checkbox"/> VM.Standard2.16	16	240	16.4	16
<input type="checkbox"/> VM.Standard2.24	24	320	24.6	24

Select Shape Cancel

7. In the **Networking** section:
 - a. Ensure the correct VCN is attached.
 - b. You only need to select **Assign a public IPv4 address** if you need to administer the Management Node via a public address.
 8. Add **SSH keys** to your instance. See [Security and SSH keys](#) for more information.
 9. Select **Create** to create the instance.
- The Management Node VM will be provisioned and spin up.

Bootstrapping the Management Node

To perform the initial setup of the Management Node, you need to set up an SSH console session to connect to the instance.

This involves creating a Console Connection for the instance (from the Instance details page, select **Console Connection**). Information about creating a Console Connection is at https://docs.oracle.com/en-us/iaas/Content/Compute/References/serialconsole.htm#Instance_Console_Connections.

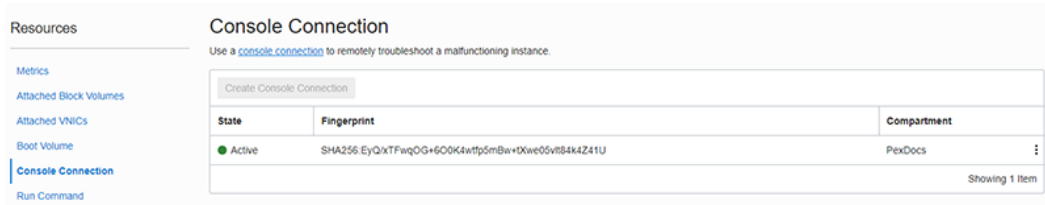
- We recommend using Oracle Cloud Shell to connect to the instance. To do this, follow the instructions at https://docs.oracle.com/en-us/iaas/Content/Compute/References/serialconsole.htm#Connecti2_cloudshell.
Note that we have observed (with Windows and Firefox) that if you subsequently use "Ctrl-V" to paste the passwords from Cloud shell into the Pexip Infinity installation wizard, the password will actually contain an (invisible) Ctrl-V at the start followed by the password. Right-click and "Paste" works correctly.
- Alternatively, you can set up a Console Connection by using your own keys and connecting via PowerShell plink, but this method can be more error-prone.

Connecting via PowerShell plink

Note that you use a keypair for the console connection itself, which is used separately from the keypair assigned to the instance. When using this method:

- You should use a key type of SSH-2 RSA, a key size of 2048 bits, and you need to use a .ppk key file.
- After creating the Console Connection, use the **Copy Serial Console Connection** option to connect to the instance via PowerShell (remember to edit the key file names and paths as appropriate).
- After the instance username is displayed you may need to press Enter to activate the console and bring up the `pexipmcumgr login:` prompt.
- If you experience "Network error: Connection refused" errors it could be because your version of plink and ppk files are not compatible — if you are using PuTTYgen to create or convert the key you can switch between version 2 and version 3 ppk files. Alternatively, ensure that you have the latest versions of PuTTYgen and plink installed.

When the connection is up you can run the installation wizard.



Running the installation wizard

When you open the console window on the Management Node VM, the following prompt appears:


```
pexipmcumgr login:
```

To run the installation wizard:

1. At the prompt, enter the username **admin**.
The display reads:
`You are required to change your password immediately (root enforced)`
`Enter new UNIX password:`
2. Create a password for the Management Node operating system by typing the password, pressing Enter, retyping the password, and pressing Enter again.
3. Ensure you record the password in a secure location. After you have finished running the installation wizard you will not need the password again unless you need to access the Management Node using SSH.
You are presented with another login prompt:
`[sudo] password for admin:`
4. Log in again with the password you just created.
The Pexip installation wizard starts.
5. Complete the installation wizard to apply basic configuration to the Management Node:

IP address	Accept the defaults for the IP address, Network mask and Gateway settings.
Network mask	
Gateway	
Hostname	Enter your required Hostname and Domain suffix for the Management Node.
Domain suffix	
DNS servers	Configure one or more DNS servers. You must override the default values if it is a private deployment.
NTP servers	Configure one or more NTP servers. You must override the default values if it is a private deployment.
Web administration username	Set the Web administration username and password.
Password	

Enable incident reporting	Select whether or not to Enable incident reporting .
Send deployment and usage statistics to Pexip	Select whether or not to Send deployment and usage statistics to Pexip .

-  The DNS and NTP servers at the default addresses are only accessible if your instance has a public IP address. The installation wizard will fail if the NTP server address cannot be resolved and reached.

The installation begins and the Management Node restarts using the values you have configured.

When the Management Node has restarted the console displays a login prompt:

```
<hostname> login:
```

At this point you can close the console. All further configuration should now be done (if you encounter SSL connection errors when using the Administrator interface, wait a few seconds to allow the relevant services to start before trying again).

Next steps

After you have run the installation wizard, you must perform some preliminary configuration before you can deploy a Conferencing Node. See [Initial platform configuration — Oracle Cloud](#) for more information.

Initial platform configuration — Oracle Cloud

After you have run the installation wizard, you must perform some preliminary configuration of the Pexip Infinity platform before you can deploy a Conferencing Node.

This section lists the configuration required, and provides a summary of each step with a link to further information.

All configuration should be done using the Pexip Infinity Administrator interface.

i **No changes** should be made to any Pexip VM via the terminal interface (other than as described when running the initial Pexip installation wizard) unless directed to do so by Pexip support. This includes (but is not limited to) changes to the time zone, changes to IP tables, configuration of Ethernet interfaces, or the installation of any third-party code/applications.

Accessing the Pexip Infinity Administrator interface

The Pexip Infinity Administrator interface is hosted on the Management Node. To access this:

1. Open a web browser and type in the IP address or DNS name that you assigned to the Management Node using the installation wizard (you may need to wait a minute or so after installation is complete before you can access the Administrator interface).
2. Until you have uploaded appropriate TLS certificates to the Management Node, your browser may present you with a warning that the website's security certificate is not trusted. You should proceed, but upload appropriate TLS certificates to the Management Node (and Conferencing Nodes, when they have been created) as soon as possible.

The **Pexip Infinity Conferencing Platform** login page will appear.

3. Log in using the web administration username and password you set using the installation wizard.

You are now ready to begin configuring the Pexip Infinity platform and deploying Conferencing Nodes.

As a first step, we strongly recommend that you configure at least 2 additional NTP servers or NTP server pools to ensure that log entries from all nodes are properly synchronized.

It may take some time for any configuration changes to take effect across the Conferencing Nodes. In typical deployments, configuration replication is performed approximately once per minute. However, in very large deployments (more than 60 Conferencing Nodes), configuration replication intervals are extended, and it may take longer for configuration changes to be applied to all Conferencing Nodes (the administrator log shows when each node has been updated).

Brief details of how to perform the initial configuration are given below. For complete information on how to configure your Pexip Infinity solution, see the Pexip Infinity technical documentation website at docs.pexip.com.

Configuring the Pexip Infinity platform

This table lists the Pexip Infinity platform configuration steps that are required before you can deploy Conferencing Nodes and make calls.

Configuration step	Purpose
1. Enable DNS (System > DNS Servers)	<p>Pexip Infinity uses DNS to resolve the hostnames of external system components including NTP servers, syslog servers, SNMP servers and web proxies. It is also used for call routing purposes — SIP proxies, gatekeepers, external call control and conferencing systems and so on. The address of at least one DNS server must be added to your system.</p> <p>You will already have configured at least one DNS server when running the install wizard, but you can now change it or add more DNS servers.</p>

Configuration step	Purpose
2. Enable NTP (System > NTP Servers)	<p>Pexip Infinity uses NTP servers to obtain accurate system time. This is necessary to ensure correct operation, including configuration replication and log timestamps.</p> <p>We strongly recommend that you configure at least three distinct NTP servers or NTP server pools on all your host servers and the Management Node itself. This ensures that log entries from all nodes are properly synchronized.</p> <p>You will already have configured at least one NTP server when running the install wizard, but you can now change it or add more NTP servers.</p>
3. Add licenses (Platform > Licenses)	<p>You must install a system license with sufficient concurrent call capacity for your environment before you can place calls to Pexip Infinity services.</p>
4. Add a system location (Platform > Locations)	<p>These are labels that allow you to group together Conferencing Nodes that are in the same datacenter. You must have at least one location configured before you can deploy a Conferencing Node.</p>
5. Upload TLS certificates (Certificates > TLS Certificates)	<p>You must install TLS certificates on the Management Node and — when you deploy them — each Conferencing Node. TLS certificates are used by these systems to verify their identity to clients connecting to them.</p> <p>All nodes are deployed with self-signed certificates, but we strongly recommend they are replaced with ones signed by either an external CA or a trusted internal CA.</p>
6. Add Virtual Meeting Rooms (Services > Virtual Meeting Rooms)	<p>Conferences take place in Virtual Meeting Rooms and Virtual Auditoriums. VMR configuration includes any PINs required to access the conference. You must deploy at least one Conferencing Node before you can call into a conference.</p>
7. Add an alias for the Virtual Meeting Room (done while adding the Virtual Meeting Room)	<p>A Virtual Meeting Room or Virtual Auditorium can have more than one alias. Conference participants can access a Virtual Meeting Room or Virtual Auditorium by dialing any one of its aliases.</p>

Next step

You are now ready to deploy a Conferencing Node. See [Deploying a Conferencing Node in Oracle Cloud](#) for more information.

Deploying a Conferencing Node in Oracle Cloud

After deploying the Management Node and completing the initial platform configuration you can deploy one or more Conferencing Nodes in Oracle Cloud to provide conferencing capacity.

Creating a new Conferencing Node is a two-step process:

1. Deploying a new VM instance in Oracle Cloud.
2. Configuring the VM with the details of the specific Conferencing Node being deployed, using a file generated from the Pexip Infinity Management Node.

Deploying the VM

To deploy a Conferencing Node on an Oracle Cloud VM:

1. Prepare a Conferencing Node disk image as described in [Obtaining and preparing disk images for Oracle Cloud deployments](#).
Note that if you have upgraded your Pexip Infinity software, you need a Conferencing Node disk image for the software version you are currently running.
2. From the Oracle Console, go to **Compute > Instances**.
3. Select **Create Instance**.
4. Enter a **Name**, for example "pexconf01".
5. Ensure the correct **Compartment** is selected.
6. In the **Image and shape** section:
 - a. Change the Image to the previously created Custom Image for the Conferencing Node. (Change the **Image source** to **Custom images** to see the options.)

Browse All Images

An image is a template of a virtual hard drive that determines the operating system and other software for an instance.

Image source
Custom images

Compartment
PexDocs

terjevemly (root)/PexDocs

Create or import [custom images](#) into your Oracle Cloud Infrastructure environment.

Custom Image Name	Created
<input checked="" type="checkbox"/> Pexip generic Conferencing Node	Wed, Jun 9, 2021, 09:02:36 UTC
<input type="checkbox"/> Pexip generic Management Node	Wed, Jun 9, 2021, 08:56:23 UTC

1 Selected

Showing 2 Items < 1 of 1 >

- b. Select an appropriate shape for the Conferencing Node. We recommend: VM.Standard3.Flex (or VM.Standard2 if 3.Flex isn't available) with a minimum of 2 OCPUs

See [Recommended instance types and call capacity guidelines](#) for more information, and see [Custom images and instance](#)

[shapes](#) if your required shape is not available.


Browse All Shapes


Instance type


Virtual Machine
A virtual machine is an independent computing environment that runs on top of physical bare metal hardware. ✓

Bare Metal Machine
A bare metal compute instance gives you dedicated physical server access for highest performance and strong isolation.

Shape series

AMD
 Flexible OCPU count. AMD processors.

Intel
 Current generation Intel processors. ✓

Ampere
 Arm-based processor.

Specialty and Previous Generation
Earlier generation AMD and Intel Standard shapes. Always Free, Dense I/O, GPU, and HPC shapes.

Image: Custom Custom

Shape Name	OCPU	Memory (GB)	Network Bandwidth (Gbps)	Max. Total VNICS
<input type="checkbox"/> VM.Standard2.1	1	15	1	2
<input checked="" type="checkbox"/> VM.Standard2.2	2	30	2	2
Local Disk: Block Storage Only				
<input type="checkbox"/> VM.Standard2.4	4	60	4.1	4
<input type="checkbox"/> VM.Standard2.8	8	120	8.2	8
<input type="checkbox"/> VM.Standard2.16	16	240	16.4	16
<input type="checkbox"/> VM.Standard2.24	24	320	24.6	24

Select Shape Cancel

7. In the **Networking** section:
 - a. Ensure the correct VCN is attached.
 - b. Ensure that **Assign a public IPv4 address** is selected, so that your Conferencing Nodes can receive calls from systems and endpoints on the public internet.
8. Add **SSH keys** to your instance. See [Security and SSH keys](#) for more information.
9. Select **Create** to create the instance.
The Conferencing Node VM will be provisioned and spin up.
10. Make a note of the public and private IP addresses from the Oracle Cloud management interface as you will need to enter them into the appropriate fields of the configuration file in Pexip Infinity in the next stage (the private IP address is used as the **IPv4 address**, and the public address is used as the **IPv4 static NAT address**).

Compute » Instances » Instance Details » Work Requests

pexconf01

Start Stop Reboot Edit More Actions

Instance Information Oracle Cloud Agent Tags

General Information

Availability Domain: AD-1

Fault Domain: FD-1

Region: eu-frankfurt-1

OCID: ...ug4ysq [Show](#) [Copy](#)

Launched: Tue, Jun 15, 2021, 10:43:34 UTC

Compartment: tenjevenly (root)/PexipInfinityPoC

Capacity type: On-demand

Instance Details

Virtual Cloud Network: [PxC](#)

Maintenance Reboot: -

Image: [Pexip_Generic_Conferencing_Node](#)

Launch Mode: PARAVIRTUALIZED

Instance Metadata Service: Versions 1 and 2 [Edit](#) ⓘ

Live Migration: Use recommended default ⓘ

Maintenance Recovery Action: Restore instance

Instance Access

The instance must be running before you can connect to it.

Public IP Address: 130.61.206.225 [Copy](#)

Primary VNIC

Private IP Address: 10.0.0.31

Network Security Groups: None [Edit](#) ⓘ

Subnet: [Public Subnet-PxC](#)

Private DNS record: Enable

Hostname: pexconf01

Internal FQDN: pexconf01... [Show](#) [Copy](#)

Launch Options

NIC Attachment Type: PARAVIRTUALIZED

Remote Data Volume: PARAVIRTUALIZED


Firmware: BIOS

Boot Volume Type: PARAVIRTUALIZED

Generating, downloading and deploying the configuration file

- From the Pexip Infinity Administrator interface, go to **Platform > Conferencing Nodes** and select **Add Conferencing Node**.
- You are now asked to provide the network configuration to be applied to the Conferencing Node, by completing the following fields:

Option	Description
Name	Enter the name to use when referring to this Conferencing Node in the Pexip Infinity Administrator interface.
Description	An optional field where you can provide more information about the Conferencing Node.
Role	<p>This determines the Conferencing Node's role:</p> <ul style="list-style-type: none"> ◦ Proxying Edge Node: a Proxying Edge Node handles all media and signaling connections with an endpoint or external device, but does not host any conferences — instead it forwards the media on to a Transcoding Conferencing Node for processing. ◦ Transcoding Conferencing Node: a Transcoding Conferencing Node handles all the media processing, protocol interworking, mixing and so on that is required in hosting Pexip Infinity calls and conferences. When combined with Proxying Edge Nodes, a transcoding node typically only processes the media forwarded on to it by those proxying nodes and has no direct connection with endpoints or external devices. However, a transcoding node can still receive and process the signaling and media directly from an endpoint or external device if required.
Hostname Domain	<p>Enter the hostname and domain to assign to this Conferencing Node. Each Conferencing Node and Management Node must have a unique hostname.</p> <p>The Hostname and Domain together make up the Conferencing Node's DNS name or FQDN. We recommend that you assign valid DNS names to all your Conferencing Nodes.</p>
IPv4 address	<p>Enter the IP address to assign to this Conferencing Node when it is created.</p> <p>This should be the Private IP Address of the instance.</p>
Network mask	<p>Enter the IP network mask to assign to this Conferencing Node.</p> <p>Typically, this is 255.255.255.0.</p> <p>Note that IPv4 address and Network mask apply to the eth0 interface.</p>

Option	Description
Gateway IPv4 address	<p>Enter the IP address of the default gateway to assign to this Conferencing Node.</p> <p>This the first host address in the CIDR of the instance's subnet.</p> <p>Note that the Gateway IPv4 address is not directly associated with a network interface, except that the address entered here lies in the subnet in which either eth0 or eth1 is configured to use. Thus, if the gateway address lies in the subnet in which eth0 lives, then the gateway will be assigned to eth0, and likewise for eth1.</p>
Secondary interface IPv4 address	<p>Leave this option blank as dual network interfaces are not supported on Conferencing Nodes deployed in public cloud services.</p>
Secondary interface network mask	<p>Leave this option blank as dual network interfaces are not supported on Conferencing Nodes deployed in public cloud services.</p> <p>Note that Secondary interface IPv4 address and Secondary interface network mask apply to the eth1 interface.</p>
System location	<p>Select the physical location of this Conferencing Node. A system location should not contain a mixture of proxying nodes and transcoding nodes.</p> <p>If the system location does not already exist, you can create a new one here by clicking  to the right of the field. This will open up a new window showing the Add System Location page.</p>
SIP TLS FQDN	<p>A unique identity for this Conferencing Node, used in signaling SIP TLS Contact addresses.</p>
TLS certificate	<p>The TLS certificate to use on this node. This must be a certificate that contains the above SIP TLS FQDN. Each certificate is shown in the format <subject name> (<issuer>).</p>
IPv6 address	<p>The IPv6 address for this Conferencing Node. Each Conferencing Node must have a unique IPv6 address.</p>
Gateway IPv6 address	<p>The IPv6 address of the default gateway.</p> <p>If this is left blank, the Conferencing Node listens for IPv6 Router Advertisements to obtain a gateway address.</p>
IPv4 static NAT address	<p>Configure the Conferencing Node's static NAT address, if you have assigned a public/external IP address to the instance.</p> <p>This should be the Public IP Address of the instance.</p>
Static routes	<p>From the list of Available Static routes, select the routes to assign to the node, and then use the right arrow to move the selected routes into the Chosen Static routes list.</p>
Enable distributed database	<p>This should usually be enabled (checked) for all Conferencing Nodes that are expected to be "always on", and disabled (unchecked) for nodes that are expected to only be powered on some of the time (e.g. nodes that are likely to only be operational during peak times).</p>
Enable SSH	<p>Determines whether this node can be accessed over SSH.</p> <p>Use Global SSH setting: SSH access to this node is determined by the global Enable SSH setting (Platform > Global Settings > Connectivity > Enable SSH).</p> <p>Off: this node cannot be accessed over SSH, regardless of the global Enable SSH setting.</p> <p>On: this node can be accessed over SSH, regardless of the global Enable SSH setting.</p> <p>Default: Use Global SSH setting.</p>

3. Select Save.

4. You are now asked to complete the following fields:

Option	Description
Deployment type	Select <i>Generic (configuration-only)</i> .
SSH password	<p>Enter the password to use when logging in to this Conferencing Node's Linux operating system over SSH. The username is always <i>admin</i>.</p> <p>Logging in to the operating system is required when changing passwords or for diagnostic purposes only, and should generally be done under the guidance of your Pexip authorized support representative. In particular, do not change any configuration using SSH — all changes should be made using the Pexip Infinity Administrator interface.</p>

5. Select **Download**.

A message appears at the top of the page: "The Conferencing Node image will download shortly or click on the following link".

After a short while, a file with the name **pexip-`<hostname>`.`<domain>`.xml** is generated and downloaded.

Note that the generated file is only available for your current session so you should download it immediately.

6. Browse to **<https://<conferencing-node-ip>:8443/>** and use the form provided to upload the configuration file to the Conferencing Node VM.

If you cannot access the Conferencing Node, check that you have allowed the appropriate source addresses in your security list for management traffic. In public deployments and where there is no virtual private network, you need to use the public address of the node.

The Conferencing Node will apply the configuration and reboot. After rebooting, it will connect to the Management Node in the usual way.

You can close the browser window used to upload the file.

After deploying a new Conferencing Node, it takes approximately 5 minutes before the node is available for conference hosting and for its status to be updated on the Management Node. Until it becomes available, the Management Node reports the status of the Conferencing Node as having a last contacted and last updated date of "Never". "Connectivity lost between nodes" alarms relating to that node may also appear temporarily.

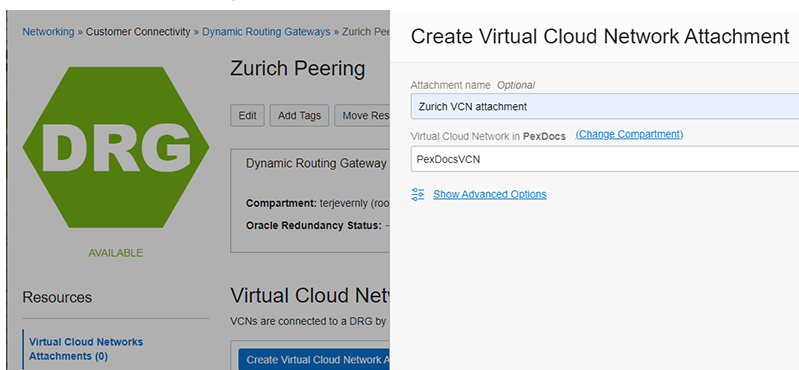
Deploying Conferencing Nodes in additional Oracle Cloud regions

In larger Pexip Infinity deployments you may want to deploy Conferencing Nodes across multiple OCI regions. This requires setting up Dynamic Routing Gateways (DRGs) for each region, and Remote Peering Connections and route tables between each region.

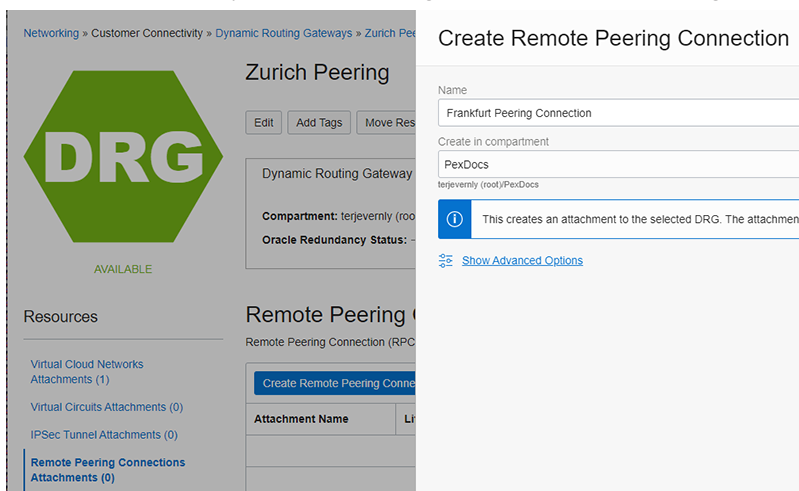
This example shows how to set up peering between Zurich and Frankfurt. It assumes you have already deployed your Conferencing Nodes in each region as described in [Deploying a Conferencing Node in Oracle Cloud](#).

To set up an peering between regions:

1. Select your region, for example Switzerland North (Zurich).
2. Create a Dynamic Routing Gateway (DRG) (**Networking > Dynamic Routing Gateway**) and name it appropriately e.g. "Zurich Peering".
3. Go to **Virtual Cloud Network Attachments** and select **Create Virtual Cloud Network Attachment** to attach a VCN to the DRG. Give it a name, for example "Zurich VCN attachment", select the VCN and create the VCN attachment.



4. Go to **Remote Peering Connections Attachments** and select **Create a Remote Peering Connection**. Give it a name, for example "Frankfurt Peering Connection" (based on the region we are peering with) and create the connection.



5. Select the Remote Peering Connection and take note of the Remote Peering OCID.

Networking » Customer Connectivity » Dynamic Routing Gateways » Zurich Peering » Remote Peering Connections » Frankfurt Peering Connection

Frankfurt Peering Connection

Establish Connection **Edit** **Terminate**

RPC
AVAILABLE

Remote Peering Connection Information

Compartment: terjevorny (root)/PexDocs
 DRG OCID: ...vmzadn6pa [Show](#) [Copy](#)
 Peer Status: ● New (not peered)
 Peer Region: —
 Peer Connection OCID: —

OCID: ...p73ltvxiuq [Show](#) [Copy](#)
 Created: Wed, Jun 16, 2021, 10:29:08 AM UTC
 Cross-Tenancy: No
 Peer Tenancy OCID: —

6. Switch to the Region you are peering with, in this case Germany Central (Frankfurt). That region should already have its own VCN set up.
7. Repeat the process as described above to set up a DRG, and then a peering connection from that region back to the first region:
 - a. Create a **Dynamic Routing Gateway** in that region, e.g. "Frankfurt Peering".
 - b. Create a **Virtual Cloud Network Attachment** (e.g. "Frankfurt VCN attachment") and attach the region's VCN to the DRG.
 - c. Create a **Remote Peering Connections Attachment** for the region you are peering with (e.g. "Zurich Peering Connection").

Networking » Customer Connectivity » Dynamic Routing Gateways » Frankfurt Peering

Frankfurt Peering

DRG
AVAILABLE

Dynamic Routing Gateway

Compartment: terjevorny (root)/PexDocs
 Oracle Redundancy Status: —

Resources

- Virtual Cloud Networks Attachments (0)
- Virtual Circuits Attachments (0)
- IPSec Tunnel Attachments (0)
- Remote Peering Connections Attachments (0)**

Create Remote Peering Connection

Name: Zurich Peering Connection

Create in compartment: PexDocs

terjevorny (root)/PexDocs

This creates an attachment to the selected DRG. The attachment will be created in the same compartment as the DRG.

[Show Advanced Options](#)

8. At this stage, the peering status shows as "New (not peered)" (it is also not peered in the other region).

Resources

- Virtual Cloud Networks Attachments (0)
- Virtual Circuits Attachments (0)
- IPSec Tunnel Attachments (0)
- Remote Peering Connections Attachments (1)**

Remote Peering Connections Attachments in PexDocs Compartment

Remote Peering Connection (RPC) attachments are automatically created when an RPC is created. You can't directly create additional attachments for an RPC.

[Create Remote Peering Connection](#)

Attachment Name	Lifecycle State	DRG Route Table	Remote Peering Connection	Peering Status	Created
DRG Attachment for RPC c. Zurich Peering Connection	Attached	Autogenerated Drg Route Table for DRG_VCN_3 not IPSec attachments	Zurich Peering Connection	● New (not peered)	Wed, Jun 16, 2021, 10:56:08 AM UTC

9. Establish the connection between the two regions:
 - a. Select the peering connection and select **Establish Connection**.
 - b. Select the Region for the remote peer (in our example we are in the Frankfurt region, so we would select Zurich).
 - c. Paste in the OCID you took note of in step 5 above (the OCID of the Remote Peering Connection in the other region).
 - d. Select **Establish Connection**.

10. The Peer status changes to "Pending", and then to "Peered" on both sides of the Peering Connection.

Remote Peering Connections Attachments *in* PexDocs *Compartment*

Remote Peering Connection (RPC) attachments are automatically created when an RPC is created. You can't directly create additional attachments for an RPC.

Create Remote Peering Connection					
Attachment Name	Lifecycle State	DRG Route Table	Remote Peering Connection	Peering Status	Created
DRG Attachment for RPC: Zurich Peering Connection	Attached	Autogenerated DRG Route Table for RPC: VCN_8 not IPsec attachments	Zurich Peering Connection	Peered	Wed, Jun 16, 2021, 10:56:08 AM UTC

11. Set up routing via the DRG between the regions:
- Switch back to the first Region (Zurich, in our example).
 - Go to **Networking > Virtual Cloud Networks**.
 - Select the appropriate VCN.
 - Select **Route Tables**.
 - Select the **Default Route Table** and add a new Route Rule, with:

Target Type: Dynamic Routing Gateway.

Destination CIDR Block: enter the CIDR block of Frankfurt.

Description: for example, "Zurich to Frankfurt".

Route Rules

Add Route Rules

Edit

Remove


<input type="checkbox"/>	Destination	Target Type	Target
<input type="checkbox"/>	0.0.0.0/0	Internet Gateway	Internet Gateway-PexDocsVCN
<input type="checkbox"/>	10.41.0.0/24	Dynamic Routing Gateways	Zurich Peering
0 Selected			

- f. Switch to the other Region (Frankfurt in this case) and repeat the process from the other side, where the destination CIDR

block in this example is Zurich's addresses.

Add Route Rules

[Help](#)

 Important:

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

Route Rule

TARGET TYPE

Dynamic Routing Gateway

DESTINATION CIDR BLOCK

10.0.1.0/24

Specified IP addresses: 10.0.1.0-10.0.1.255 (256 IP addresses)

TARGET DYNAMIC ROUTING GATEWAY

Name: Frankfurt Peering
Compartment: PexDocs

DESCRIPTION OPTIONAL

Frankfurt to Zurich

Maximum 255 characters

12. Repeat this process for all of your other regions, setting up Remote Peering Connections and route tables between each region.

Managing Oracle Cloud Infrastructure VM instances

This section describes the common maintenance tasks for [stopping](#), [restarting](#) and [permanently removing](#) Conferencing Node VM instances in the Oracle Cloud Infrastructure (OCI).

Temporarily removing (stopping) a Conferencing Node instance

At any time you can temporarily remove a Conferencing Node instance from your Pexip Infinity platform if, for example, you do not need all of your current conferencing capacity.

To temporarily remove a Conferencing Node instance:

1. Put the Conferencing Node into maintenance mode via the Pexip Infinity Administrator interface on the Management Node:
 - a. Go to **Platform > Conferencing Nodes**.
 - b. Select the Conferencing Node(s).
 - c. From the **Action** menu at the top left of the screen, select **Enable maintenance mode** and then select **Go**.
While maintenance mode is enabled, this Conferencing Node will not accept any new conference instances.
 - d. Wait until any existing conferences on that Conferencing Node have finished. To check, go to **Status > Live View**.
2. Stop the Conferencing Node instance on Oracle:
 - a. From the Oracle cloud console, select **Compute > Instances** to see the status of all of your instances.
 - b. Select the instance you want to shut down.
 - c. At the top of the Instance Details page, select **Stop**.

Reinstating (restarting) a stopped Conferencing Node instance

You can reinstate a Conferencing Node instance that has already been installed but has been temporarily shut down.

To restart a Conferencing Node instance:

1. Restart the Conferencing Node instance on Oracle:
 - a. From the Oracle cloud console, select **Compute > Instances** to see the status of all of your instances.
 - b. Select the instance you want to restart.
 - c. At the top of the Instance Details page, select **Start** to restart the instance.
2. Take the Conferencing Node out of maintenance mode via the Pexip Infinity Administrator interface on the Management Node:
 - a. Go to **Platform > Conferencing Nodes**.
 - b. Select the Conferencing Node.
 - c. Clear the **Enable maintenance mode** check box and select **Save**.

After reinstating a Conferencing Node, it takes approximately 5 minutes for the node to reboot and be available for conference hosting, and for its last contacted status to be updated on the Management Node.

Permanently removing a Conferencing Node instance

If you no longer need a Conferencing Node instance, you can permanently delete it from your Pexip Infinity platform.

To remove a Conferencing Node instance:

1. If you have not already done so, put the Conferencing Node into maintenance mode via the Pexip Infinity Administrator interface on the Management Node:
 - a. Go to **Platform > Conferencing Nodes**.
 - b. Select the Conferencing Node(s).
 - c. From the **Action** menu at the top left of the screen, select **Enable maintenance mode** and then select **Go**.

While maintenance mode is enabled, this Conferencing Node will not accept any new conference instances.

- d. Wait until any existing conferences on that Conferencing Node have finished. To check, go to **Status > Live View**.
2. Delete the Conferencing Node from the Management Node:
 - a. Go to **Platform > Conferencing Nodes** and select the Conferencing Node.
 - b. Select the check box next to the node you want to delete, and then from the **Action** drop-down menu, select **Delete selected Conferencing Nodes** and then select **Go**.
3. Terminate the Conferencing Node instance on Oracle:
 - a. From the Oracle cloud console, go to **Compute > Instances**.
 - b. Select the instance you want to permanently remove.
 - c. From the **More Actions** drop-down, select **Terminate** to remove the instance.

Note that the instance will terminate immediately, but it may take several hours for the terminated instance to be removed from the list of instances shown in the console.