

leostream

Remote Desktop Access Platform

Leostream Quick Start for OpenStack Clouds

Advanced Capacity Automation, Connection Management, and Remote Access

Version 202x
July 2023

Contacting Leostream

Leostream Corporation
77 Sleeper St.
PMB 02-123
Boston, MA 02210
USA

<http://www.leostream.com>
Telephone: +1 781 890 2019

To submit an enhancement request, email features@leostream.com.

To request product information or inquire about our future directions, email sales@leostream.com.

Copyright

© Copyright 2002-2023 by Leostream Corporation

This software program and documentation are copyrighted by Leostream. The software described in this document is provided under a license agreement and may be used or copied only under the terms of this agreement. No part of this manual may be copied or reproduced in any form without prior written consent from Leostream.

Trademarks

The following are trademarks of Leostream Corporation.

Leostream™

The Leostream graphical logo™

The absence of a product name or logo from this list does not constitute a waiver of the trademark or other intellectual property rights concerning that product, name, or logo by Leostream.

The OpenStack Word Mark and OpenStack Logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. Leostream is not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community. Linux is the registered trademark of Linus Torvalds in the U.S. and other countries. OpenLDAP is a trademark of The OpenLDAP Foundation. Microsoft, Active Directory and Windows are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Other brand and product names are trademarks or registered trademarks of their respective holders. Leostream claims no right to use of these marks.

Patents

Leostream software is protected by U.S. Patent 8,417,796.

Contents

CONTENTS	3
CHAPTER 1: INTRODUCTION	4
OVERVIEW OF OPENSTACK COMPONENTS FOR VDI	4
OVERVIEW OF THE LEOSTREAM PLATFORM	5
CHAPTER 2: PREPARING OPENSTACK IMAGES	6
SUPPORTED OPERATING SYSTEMS	6
INSTALLING THE LEOSTREAM AGENT	6
CHAPTER 3: INSTALLING LEOSTREAM IN OPENSTACK	8
REQUIRED OPENSTACK PERMISSIONS	8
SECURITY GROUP REQUIREMENTS	8
INSTALLING THE CONNECTION BROKER	9
ASSIGNING A FLOATING IP ADDRESS	10
LICENSING YOUR LEOSTREAM CONNECTION BROKER	11
CHAPTER 4: INTEGRATING WITH EXTERNAL SYSTEM	13
CONNECTING TO YOUR AUTHENTICATION SERVERS	13
CONNECTING TO YOUR OPENSTACK CLOUD	14
CHAPTER 5: POOLING AND PROVISIONING IN OPENSTACK	16
CREATING POOLS	16
PROVISIONING NEW INSTANCES	17
DISABLING PROVISIONING	20
JOINING INSTANCES TO A DOMAIN	20
CHAPTER 6: OFFERING OPENSTACK INSTANCES TO USERS	23
DEFINING POOL-BASED PLANS	23
<i>Protocol Plans</i>	23
<i>Power Control Plans</i>	24
<i>Release Plans</i>	26
BUILDING USER POLICIES	28
ASSIGNING POLICIES TO USERS	30
TESTING YOUR CONNECTION BROKER CONFIGURATION	32

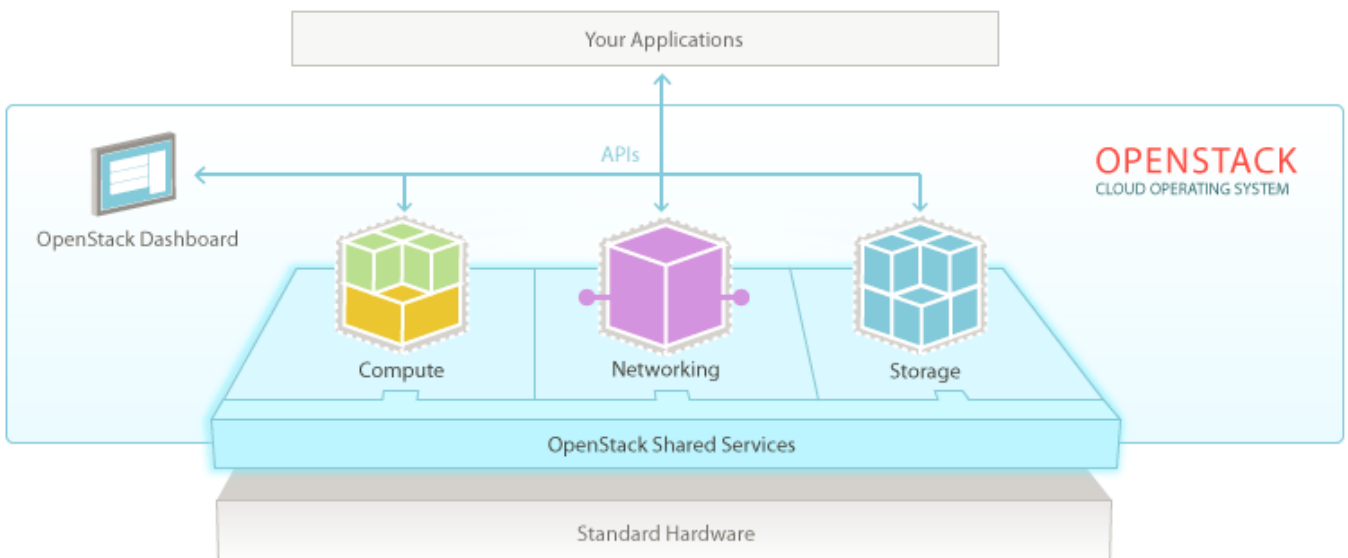
Chapter 1: Introduction

OpenStack cloud control software allows you to control pools of compute, storage, and networking in your data center, and turns your data center into a cloud that is ideal for hosting virtual desktops. In an OpenStack cloud, you can deliver virtual desktops and desktops-as-a-service that:

1. Provide on-demand availability – quickly on-board new employees by provisioning desktops for users from custom images created in OpenStack.
2. Support multi-tenancy – separate departments, customers, etc., by OpenStack project to provide isolated networks, set compute and storage quotas, and manage resources independently.
3. Improve security – isolate desktops using separate networks, including dedicated IP address ranges, subnets, and routers. Provision desktops into the appropriate virtual private cloud so that only instances within a given internal network, or those on subnets connected through interfaces, can access other instances in that network.
4. Lower costs – use open source software components to avoid the licensing fees associated with commercial VDI or DaaS stacks. Scale your data center seamlessly without acquiring additional licenses.

Overview of OpenStack Components for VDI

The OpenStack software consists of over 10 different projects, each with a focus on a particular aspect of the data center. The projects shown in the following figure are the most important for VDI deployments.



When working with Leostream, the relevant OpenStack projects are:

- **Keystone** = identity. The Connection Broker uses the Keystone API to gain access to the OpenStack API. Leostream supports OpenStack versions that use Keystone Identify API version 3.

- **Nova** = compute. The nova project is the heart of OpenStack. It runs the instances that are the desktops you deliver in your VDI and DaaS deployment. The instances may be stored as nova instances, or you may run nova instances with attach external volume storage.
- **Cinder** and **Swift** = storage. Desktop workloads should be retained in cinder block storage. Each desktop can be a persistent volume that can be attached to a running instance.
- **Glance** = imaging. Glance tools allow you to create a master image of a customer's desktop, and then quickly provision new on-demand instances from that image.
- **Neutron** = network. Neutron provides tools to build per-tenant private networks.
- **Horizon** = dashboard. Horizon provides a UI on top of your OpenStack cloud, where you can create images, instances, networks, and more.

You will not manage your VDI or DaaS deployment within the Horizon dashboard, however. Management is done within the Leostream Connection Broker.

Overview of the Leostream Platform

The Leostream Platform is comprised of a set of components, including the Connection Broker, Leostream Gateway, Leostream Agent, and Leostream Connect client.

- The Connection Broker lies at the heart of any hosted desktop deployment on OpenStack and is responsible for provisioning resources in your OpenStack cloud, assigning and connecting end users to those resources, and managing the end user's remote session.
- If you plan to isolate your OpenStack instances in a private network, the Leostream Gateway provides HTML5 and client-based access to those desktops, using a range of commodity and high-performance display protocols.
- The Leostream Agent installs on your OpenStack instances and provides the Connection Broker with critical information about the end user's session.
- The Leostream Connect client allows users to log in from any Windows, Linux, or macOS client device. Users can also log in using any PCoIP client device, or using the Leostream Web client.

The Connection Broker is configured using the Administrator Web interface, where you define the Leostream concepts that control your environment. For more information on Leostream concepts, or to learn more about the components that make up the Leostream Platform, see the [Introduction to the Leostream Platform](#) guide.

Leostream software is available from the [Leostream Downloads page](#). You must have a Leostream Serial Number to access the downloads.

Chapter 2: Preparing OpenStack Images

Leostream can manage connections to existing OpenStack instances, and provision new OpenStack instances from existing OpenStack images.

Currently, you cannot create new images within the Leostream interface. All images must be created using native OpenStack tools.

Supported Operating Systems

The Leostream Connection Broker can manage connections to OpenStack instances running Windows or Linux operating systems, including:

1. Any Microsoft Windows operating system version currently covered by Mainstream Support under the Microsoft Fixed Lifecycle Policy, or in service under the Microsoft Modern Lifecycle Policy.
2. Any of the following operating systems when running a Java Runtime Environment version 1.8, or later:
 - CentOS
 - Debian
 - Fedora
 - SUSE Linux Enterprise
 - Red Hat Enterprise Linux
 - Ubuntu
 - macOS

When creating instances within the Horizon Dashboard, ensure that you install the appropriate Leostream Agent onto the instance and register that agent with your Leostream Connection Broker, as described in the following section.

Any images that you want to use within Leostream to provision new instances must also include the Leostream Agent.

Installing the Leostream Agent

When installed on a desktop, the Leostream Agent provides the Connection Broker with additional information about the user's session, including:

- When the user logs into the remote desktop
- When the user disconnects from the remote session
- When the user logs off of the remote desktop
- When the user locks or unlocks their remote desktop
- When the user's session is idle

In addition, the Connection Broker requires the Leostream Agent to enforce certain role and policy options, including:

- Adding Local Users or adding users to the Remote Desktop Users group
- Taking actions when the user disconnects from their remote session
- Using release plan options to lock, disconnect, or log out the user after their session is idle
- Managing USB devices
- Attaching network printers specified by Connection Broker printer plans
- Using registry plans to modify or create registry keys on the remote desktop

Leostream provides a Leostream Agent version for Windows operating systems and a Java version of the Leostream Agent for Linux operating systems. Ensure that you download the appropriate Leostream Agent from the [Leostream Downloads](#) page. Consult the [Leostream Installation Guide](#) for instructions on how to install the Leostream Agent on your OpenStack instances.

The Connection Broker address can be specified when you install the Leostream Agent. If you need to specify or change the Connection Broker address after the Leostream Agent is installed, you can use the Leostream Control Panel dialog in Windows or set the address in the `leostreamagent.conf` file on Linux. See the [Leostream Agent Administrator's Guide](#) for more information.

If you plan to use Leostream to provision new Windows instances in OpenStack, and to have Leostream join these new Windows instances to your Microsoft Active Directory domain, please adhere to the following guidelines when building the master image to use for provisioning.

- The instance used to create the image must not be joined to the domain. Leostream only joins instances to a domain if they are currently part of a Workgroup.
- The instance must have an installed Leostream Agent that is registered with your Connection Broker. If the Leostream Agent cannot communicate with the Connection Broker, new instances will not be joined to the domain.

Chapter 3: Installing Leostream in OpenStack

The Leostream Connection Broker must be installed in a location where it has network access to the Leostream Agents installed on your OpenStack instances. The following procedure covers installing a single instance of the Leostream Connection Broker. For information on creating clusters of Connection Brokers for large-scale production environments, see the [Leostream Scalability Guide](#).



Depending on your OpenStack distribution, your Horizon Dashboard may appear differently than shown in the screen shots included in this chapter.

Required OpenStack Permissions

Leostream manages OpenStack clouds using the OpenStack APIs. Before you begin your Leostream deployment, ensure that you have access to a user account with the required permissions in OpenStack. In order to use all of the functionality in the Connection Broker, your user requires access to the following:

Nova permissions:

```
compute:get_all
compute:create
compute:start
compute:stop
compute:reboot
compute_extension:admin_actions:suspend
compute_extension:floating_ips
compute_extension:admin_actions:resume
network:associate_floating_ip
network:disassociate_floating_ip
os_compute_api:os-flavor-extra-specs:index
```

Glance permissions:

```
get_images
```

Cinder permissions

```
volume:create_from_image
volume:delete
volume_extension:type_get_all
```

Security Group Requirements

Before creating your Connection Broker instances, ensure that you have an appropriate security group configured in OpenStack. Leostream requires the following ports be open for incoming traffic.

Port	Required By	Purpose
22	Connection Broker	For SSH access to the Connection Broker. Alternatively, you can access the Connection Broker console via the Horizon Dashboard.
80 and 443	Connection Broker, Leostream Gateway	For access to the Connection Broker Web interface, and communication with the Leostream Agents and Leostream Connect. If you close port 80 on your Connection Broker, you may omit that port from the security group. The Leostream Gateway does not require port 80, only port 443.
20001 - 30000	Leostream Gateway	The Leostream Gateway uses this default port range to forward display protocol traffic from the user's client device to an instance isolated in a private OpenStack network. You may optionally change this port range using the Leostream Gateway CLI.
8080*	Leostream Agent on the OpenStack Instances	Port for communications from the Connection Broker to the Leostream Agent. * The Leostream Agent port may be changed using the Leostream Agent Control Panel dialog. If you change the default Leostream Agent port, ensure that you open the associated port in the security group
3389**	OpenStack Instances	For RDP access to the OpenStack VDI/DaaS instances ** If you use a display protocol other than RDP, ensure that you open any ports required by that display protocol.

Installing the Connection Broker

The Connection Broker can be installed on any virtual or physical machine running the latest Red Hat® Enterprise Linux® 8.x operating system and its derivatives such as Rocky Linux and AlmaLinux OS.



The Connection Broker does not install on CentOS 8, on any operating system based on Fedora, or any other Linux distribution.

When creating a virtual machine for the Connection Broker installation, ensure that the VM has, at least, the following resources.

- 2 CPU or vCPU
- 8.0 Gbytes of RAM
- At least 20 Gbytes of hard drive space
- One NIC, ideally with Internet connectivity

Prior to installing your Connection Broker, install the latest updates to the operating system. See the [Leostream Installation Guide](#) for information on obtaining and applying your license key, using the Leostream serial number you obtained from Leostream sales.

The Connection Broker uses the private IP address assigned by OpenStack on the network you selected when launching the instance. To access the Connection Broker Administrator Web interface, you must be able to access the Connection Broker from a Web browser, which may require you to assign a public floating IP address to the Connection Broker, as described in the following section.

Assigning a Floating IP Address

If you cannot access the private IP address assigned to the Connection Broker instance, you can use the OpenStack Horizon Dashboard to associate a floating IP address with your Connection Broker instance, as follows.

1. Go to the **Network > Floating IPs** page in the OpenStack project that contains your Connection Broker.
2. If you do not have an available floating IP address, click the **Allocate IP to Project** button. Otherwise, skip to step 5.
3. Select **public** from the **Pool** drop-down menu in the **Allocate Floating IP** form.
4. Click **Allocate IP**.
5. In the list of floating IPs, click the **Associate** button for an available IP address, for example:

Floating IPs

Floating IP Address =

Displaying 3 items

<input type="checkbox"/>	IP Address	Description	Mapped Fixed IP Address	Pool	Status	Actions
<input type="checkbox"/>	172.24.4.243		-	public	Down	Associate ▼
<input type="checkbox"/>	172.24.4.189		-	public	Down	Associate ▼
<input type="checkbox"/>	172.24.4.154		-	public	Down	Associate ▼

6. In the **Manage Floating IP Associations** form, select your Leostream Connection Broker instance from the **Port to be associated** drop-down menu, for example:

Manage Floating IP Associations

IP Address *

IP Address *

172.29.229.159 ▼ +

Port to be associated *

Leostream Connection Broker: 192.168.201 ▼

Select the IP address you wish to associate with the selected instance.

Cancel Associate

7. Click **Associate**.

You can now access the Connection Broker Administrator Web interface using the public floating IP address.

Licensing your Leostream Connection Broker

Your Connection Broker license is derived from the serial number you received from Leostream Sales. If you do not have a Leostream 9 serial number, please contact sales@leostream.com.

To obtain your license key:


1. Point a web browser at the IP address of the machine running the Connection Broker. The Connection Broker **Sign In** page opens.
2. Log into your Connection Broker using the following default administrator credentials:

`username=admin`
`password=leo`
3. On the **Leostream License** page, select **Enter manually** from the **How do you want to enter your license key** drop-down menu.
4. Below the drop-down, click the link to go to <https://license.leostream.com>. The installation code for your Connection Broker is automatically populated.
5. Enter the serial number you obtained from Leostream sales.
6. Enter the email address associated with that serial number.
7. Click **Generate a license**.
8. Click the **Apply to the broker** button above the generated license key. The browser returns to the **Leostream License** page.

9. Select the **I have read and accept the License Agreement** check box.
10. Click **Save**.

If your Connection Broker does not have internet access, you can obtain your license key from another computer with internet access. In this case, to obtain your license:

1. Note your Connection Broker installation code to the right of the form on the **Leostream License** page.
2. Go to <https://license.leostream.com> and manually enter your serial number, installation code, and email address.
3. Copy the license key to a text file.
4. Return to your Connection Broker and copy-and-paste the key into the **License key** field.

 The generated license key is linked to this Connection Broker installation or cluster. If you rebuild your Connection Broker or create a second Leostream environment, contact sales@leostream.com to obtain a new serial number for that environment.

Chapter 4: Integrating with External System

Connecting to Your Authentication Servers

The Connection Broker can authenticate users against Microsoft Active Directory and OpenLDAP authentication servers. You can also leverage any Identify Provider that supports the SAML Protocol. To authenticate users in Active Directory, you first register your domain with your Connection Broker.

1. Go to the **> Setup > Authentication Servers** menu.
2. Click the **Add Authentication Server** link.
3. In the **Add Authentication Server** form, Select **Active Directory** from the **Type** drop-down list.
4. Enter a name for this server in the Connection Broker in the **Authentication Server name** edit field.
5. In the **Domain** edit field, enter the domain name associated with this Active Directory server.
6. In the **Connection Settings** section, shown in the following figure, use the following procedure to integrate with your Active Directory authentication server.

The screenshot shows the 'Connection Settings' section of a web form. It includes a dropdown menu for 'Specify address using' with 'Hostnames or IP addresses' selected. Below this are two input fields: 'Hostname or IP address' and 'Port', with '389' entered in the port field. A note states: 'If using multiple addresses, separate each entry with spaces'. Below these is another dropdown for 'Algorithm for selecting from multiple addresses' with 'Random' selected. A note states: 'The sequential algorithm uses the first working address in the list'. There is a checkbox for 'Encrypt connection to the authentication server using SSL (LDAPS)' which is currently unchecked. At the bottom is an input field for 'AWS Directory ID' with a note: 'Enter the Directory ID if this is an AWS directory that will be used for a Amazon Workspaces'.

- a. From the **Specify address using** drop-down menu, select **Hostname or IP address**.
- b. Enter the authentication server hostname or IP address in the **Hostname or IP address** edit field.
- c. Enter the port number in the **Port** edit field.
- d. Check the **Encrypt connection to authentication server using SSL (LDAPS)** checkbox if you need a secure connection to the authentication server. The port number automatically changes to 636. Re-edit the **Port** edit field if you are not using port 636 for secure connections.

7. In the **Search Settings** section, shown in the following figure, enter the username and password for an account that has read access to the user records. Leostream does not need full administrator rights to your Active Directory authentication server.

Search Settings
Enter the credentials for a user who has the permissions to search for other users.
If you do not enter credentials an anonymous bind will be used.

Login name or DN
Administrator
Enter a fully qualified login name, e.g. Administrator@YOUR_DOMAIN.com or CN=Administrator;CN=Users;DC=YOUR_DOMAIN,DC=com

Password

8. In the **User Login Search** section, ensure that the **Match Login name against this field** edit field is set to **sAMAccountName**. This is the attribute that the Connection Broker uses to locate the user in the authentication server, based on the information the user enters when logging into Leostream.
9. Click **Save**.

Connecting to your OpenStack Cloud

In order to manage your OpenStack cloud, you create OpenStack *centers* in Leostream for each project you want to manage in your Connection Broker.

*Leostream defines **centers** as the external systems that inform the Connection Broker about desktops and other resources that are available for assignment to end users.*

Leostream uses the OpenStack APIs to inventory the instances and images in your OpenStack cloud. Ensure that you have a user account that has the appropriate permissions for the OpenStack projects you plan to manage in your Connection Broker (see [Required OpenStack Permissions](#)).

To create an OpenStack center:

1. Go to the **> Setup > Centers** page.
2. Click the **Add Center** link.
3. In the **Add Center** form, select **OpenStack** from the **Type** drop-down menu.

If you do not see OpenStack in your list of provided options, please contact sales@leostream.com to update your Leostream license key.

4. Enter a name for the center in the **Name** edit field.

5. In the **Auth URL** edit field, enter the public URL to the OpenStack Keystone identity service endpoint, for example:

http://external_openstack_ip:5000/v3.0

Where *external_openstack_ip* is the externally accessible IP address to your identity service.



Leostream supports only version 3 of the Keystone API.

6. If you are not using the default region, enter your OpenStack region in the **Region** edit field.
7. Enter the OpenStack domain that contains your project and user in the **Project Domain** edit field.
8. Specify the project you want to manage in the **Project** edit field.
9. Enter an administrator domain, username, and password into the **User Domain**, **Username** and **Password** edit fields, respectively.
10. Click **Save** to create the center.

The instances in the center's OpenStack project appear in the > **Resources** > **Desktops** page. The Connection Broker inventories all images and displays them on the > **Resources** > **Images** page. See the "Working with Desktops" section of the [Connection Broker Administrator's Guide](#) for information on viewing, editing, and controlling desktops from within the Connection Broker.

Chapter 5: Pooling and Provisioning in OpenStack

After you create your centers and the Connection Broker inventories your desktops, you can logically group the desktops into **pools**.

The Leostream Connection Broker defines a pool as any group of desktops. Pools can be nested within one another, to create sub-pools. Pools and sub-pools have three distinct functions in Leostream.

1. Organizing desktops on the > **Resources** > **Desktops** page
2. Provisioning new instances in OpenStack
3. Indicating the desktops that a user may connect to and how the Connection Broker manages the user's connection to those desktops

Creating Pools

When using Leostream to provision new instances in OpenStack, the key is to construct your pool in a way that ensures that newly provisioned desktops become members of that pool. One method is to set the pool to contain all instances in the OpenStack project associated with the center you created in the previous chapter.

If that pool definition is too broad, another easy way to ensure that new desktops become part of a pool is to define the pool based on the instance name, which you set during provisioning, for example:

1. Go to the > **Configuration** > **Pools** page.
2. Click the **Create Pool** link. The **Create Pool** form opens.
3. Enter a name for the pool in the **Name** edit field.
4. In the first row of the **Desktop Attribute Selection** section:
 - a. Select **Name** from the **Desktop attribute** drop-down menu.
 - b. Select **begins with** from the **Conditional** drop-down menu.
 - c. In the **Text value** field, enter the name you will use for all the instances in this pool.
5. Click **Save** to save the pool.

For a complete description of creating pools, including how to create a pool of all desktops in an OpenStack center, see the “Creating Desktop Pools” chapter in the [Connection Broker Administrator's Guide](#).

Provisioning New Instances



Your Connection Broker license determines if provisioning is enabled in your Connection Broker. If you do not see the options described in this section, contact sales@leostream.com to update your license key.

Provisioning allows you to generate new OpenStack instances when the number of desktops in a pool reaches a specified lower threshold. Before provisioning instances in an OpenStack environment, ensure your available images are displayed on the **> Resources > Images** page, and that your master images contain an installed Leostream Agent that is configured to communicate with your Connection Broker.

The **Provisioning** section of the **Edit Pool** page allows you to configure when and how the Connection Broker creates new instances in your OpenStack environment. To begin, check the **Provisioning enabled** checkbox, as shown in the following figure.

Provisioning

☐ Provisioning enabled

Provisioning Limits

Start provisioning when unassigned desktops in pool drops below

Stop provisioning when total desktops in pool reaches

☐ Enforce provisioning limits (automatically create and delete available machines to meet thresholds)

The Connection Broker determines when to create new instances by comparing the thresholds specified in the **Provisioning Limits** section to the current contents of the pool. If you edit an existing pool, the Connection Broker displays the current contents of the pool size to the right of the **Edit Pool** form, for example:

Pool size information (updated less than a minute ago) *

Total:	46
Available:	44
Unavailable:	1
Assigned:	1
Running:	17
Stopped:	29
Suspended:	0
Agent running:	7

The number entered into the **Start provisioning when unassigned desktops in pool drops below** field specifies a lower bound on the number of unassigned desktops in the pool, where the number of unassigned desktops is the total number of desktops minus the number of assigned desktops.

For example, the previous figure shows one assigned desktop and 46 total desktops. Therefore, there are 45 unassigned desktops. An unassigned desktop can have a desktop status of either available or unavailable.

The Connection Broker checks the provisioning limits, and creates new instances, at the following times

- When the pool is saved
- When a user is assigned to a desktop in this pool

- When any `pool_stats` or `pool_history_stats` job runs

The Connection Broker continues to provision new desktops whenever the lower threshold is crossed, until the upper threshold specified in the **Stop provisioning when total desktops in pool reaches** field is reached, indicated by the **Total** value in the pool size information.

Use the **Provisioning Parameters** section to configure how Leostream provisions new instances in OpenStack.

1. Select the OpenStack center to provision new machines into from the **Provision in center** drop-down menu. The remainder of the form updates based on the contents of your selection. The following figure shows an example of the **Provisioning Parameters** section.

PROVISIONING PARAMETERS

Provision in center
OpenStack

Virtual machine name
desktop-{SEQUENCE}

Display name

Optional sequence number for virtual machine name
0

Availability zone
Select ...

Flavor
Select ...

Deploy from image
Select ...

☐ Create new volume

Network
Select ...

☒ Associate floating IP (allocate new IP, if necessary)

Available security groups
default

Selected security groups

☐ Initialize newly-provisioned desktops as "deletable"

☐ Initialize newly-provisioned desktops as "unavailable"

2. Enter a name for the virtual machine in the **Virtual Machine Name** edit field. If the pool is defined using names that begin with a certain string, ensure that the **Virtual Machine Name** field starts with that string.
3. Optionally enter a user-friendly display name into the **Display name** edit field. You can specify in the

user's policy if the Connection Broker should display the desktop to the user with its display name instead of virtual machine name.

4. If either of the names contains a `{SEQUENCE}` dynamic tag, enter the starting number for the sequence in the **Optional sequence number for virtual machine name** edit field. The Connection Broker starts naming virtual machines at this number and increments the number for each machine created.
5. Select the availability zone to provision the new instance into from the **Availability zone** drop-down menu.
6. Select the instance size from the **Flavor** drop-down menu.
7. Select the image to use from the **Deploy from image** drop-down menu. This menu contains all the images available in the OpenStack project associated with the selected center.
8. By default, the Connection Broker creates an instance with ephemeral storage. To create a new volume from the image to use for the provisioned instance, select the **Create new volume** checkbox. The form expands to show the fields in the following figure.



The screenshot shows a form titled "Create new volume" with a purple header bar. Below the header, there is a checkbox labeled "Delete volume on instance delete". Underneath is a text input field labeled "Volume size (GB)". To the right of this field, a small note states "Overrides volume size specified in the selected flavor". At the bottom, there is a dropdown menu labeled "Volume type" with the text "Select ..." and a downward arrow.

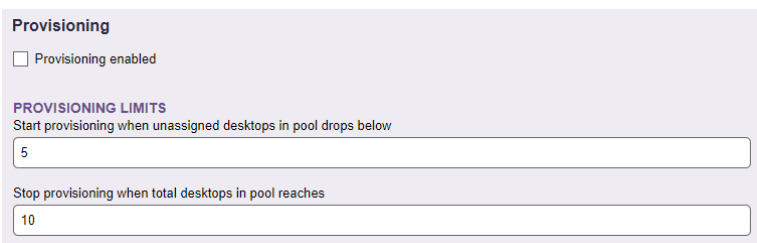
- a. If you are provisioning non-persistent virtual machines, select the **Delete volume on instance delete** checkbox to have the Connection Broker delete the volume along with the instance, when instructed to do so by the user's Release Plan.
 - b. If create a volume of a different size than that of the selected flavor, enter the desired volume size in the **Volume size** edit field.
 - c. Select the desired volume type from the **Volume type** drop-down menu.
 9. Select the network for the new instance from the **Network** drop-down menu.
- If you add the instance to a private network without associating a public IP address, you can use the Leostream Gateway to connect clients that are outside of the private network. See the [Leostream Gateway Guide](#) for more information.
10. Select the **Associate floating IP (allocate new IP, if necessary)** option if Leostream should assign a floating IP address to the new instance. If a floating IP address is not available, Leostream attempts to allocate a new address.

11. In the **Available security groups** field, select the security groups to assign to the new instance. Click the **Add item** button to place them into the **Selected security groups** field.
12. Select the **Initialize newly provisioned desktops as deletable** option to indicate that the Connection Broker is allowed to delete these instances. When this option selected, the **Edit Desktop** page for the newly provisioned VM has the **Allow this desktop to be deleted from disk** option selected. Use release plans to schedule VM deletion.

For more information on using release plans to terminate OpenStack instances, see the example on deleting virtual machines in the “Release Plans” section of Chapter 11 of the [Connection Broker Administrator’s Guide](#).
13. Select the **Initialize newly provisioned desktop as unavailable** option to set the desktop status to Unavailable. The Connection Broker will not offer a desktop to users if the desktop’s status is set to Unavailable, allowing you to perform post-provisioning actions on the desktop.
14. Click **Save**.

Disabling Provisioning

If you’ve set non-zero provisioning limits in your pool and need to temporarily disable provisioning, uncheck the **Provisioning enabled** check box, shown in the following figure.



Provisioning

☐ Provisioning enabled

PROVISIONING LIMITS

Start provisioning when unassigned desktops in pool drops below

5

Stop provisioning when total desktops in pool reaches

10

The Connection Broker may automatically disable provisioning in cases where provisioning is failing due to configuration errors in your pool. If this occurs, please check and correct your provisioning parameters before enabling provisioning.

Joining Instances to a Domain

You can use Leostream to join OpenStack Windows instance to an Active Directory domain. When enabled, the Connection Broker attempts to join a desktop to the domain when the Leostream Agent on the desktop registers with the Connection Broker, for example, when a desktop is provisioned or when you reboot the desktop.



Before configuring a pool to join desktops to a domain, you must define the Active Directory domain on the **> Setup > Authentication Servers** page.

To enable domain joining for a pool:

1. Select the **Join virtual machine to a domain** option in the **Domain Join** section, shown in the following figure.

The screenshot shows the 'Domain Join' configuration window. At the top, it says 'Domain Join' and 'Applies to desktops that are not already a member of a domain when the desktop registers with the Connection Broker.' Below this is a section titled 'Join machine to a domain' with a checked checkbox. Underneath, there is a 'Domain' dropdown menu with 'leodev.net (Leostream)' selected. A note below the dropdown states 'Contains all Active Directory domains registered on the > Setup > Authentication Servers page'. Below that is an 'Organizational Unit within "leodev.net (Leostream)"' dropdown menu with 'Select ...' chosen, and a small 'Optional' label to its right. The main area is divided into two columns. The left column is titled 'Available AD groups to join' and contains a list of groups: ADSyncAdmins, ADSyncBrowse, ADSyncOperators, ADSyncPasswordSet, Access Control Assistance Operators, Account Operators, Administrators, Allowed RODC Password Replication Group, Backup Operators, Cert Publishers, Certificate Service DCOM Access, and Cloneable Domain Controllers. Between the columns are four buttons: 'Add item', 'Add all', 'Remove item', and 'Remove all'. The right column is titled 'Selected AD groups to join' and is currently empty, with an 'Optional' label below it. At the bottom, there are two checkboxes: 'Set desktop hostname to machine name' (checked) and 'When virtual machine is permanently deleted, also remove it from the domain' (unchecked).

2. Select the domain from the **Domain** drop-down menu.
3. Optionally, from the **Organizational Unit** drop-down menu, select an OU for the desktops.
4. To add the desktop to one or more AD groups, select and move the groups from the **Available AD groups to join** to the **Selected AD groups to join** list.
5. To reset the desktops hostname when joining it to the domain, select the **Set desktop hostname to virtual machine name** check box. With this option selected, the Leostream Agent attempts to set the hostname to the value shown in the **Name** column on the > **Resources > Desktops** page.

If the pool provisions new desktops, this is the name found in the **Virtual machine name** edit field.

The **Name** field must contain a valid hostname, as follows:

- The name uses only the standard character set for Computer Name, which includes letters, numbers, and the following symbols: ! @ # \$ % ^ & ' (. - _ { } ~
 - Then name cannot be longer than 15 characters.
6. If you are provisioning non-persistent desktops, select the **When virtual machine is permanently deleted, also remove it from the domain** to instruct the Connection Broker to delete the Computer

record from your Active Directory server. If you do not select this option, the Computer record remains in AD after the VM is deleted.




Leostream performs the domain join for any desktop in the pool that is not already joined to a domain. Leostream does not have to provision the desktop to perform the domain join.

Chapter 6: Offering OpenStack Instances to Users

Defining Pool-Based Plans

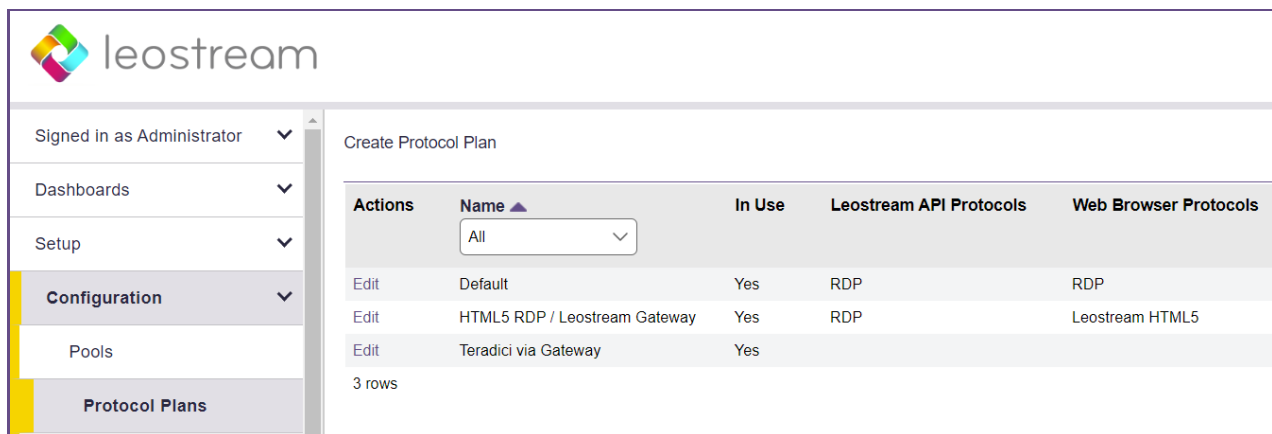
After you separate your desktops into pools, define the rules that control how the Connection Broker manages the user's connection to the desktops in those pools. To perform this step, ask yourself the following questions.

- What display protocols do I want to use to connect users to their desktops?
- How do I want to manage the power state of each desktop, for example, should it be powered off when the user logs out?
- How long can users remain assigned to a particular desktop? For example, if the user logs out, should they remain assigned to that desktop, or should another user be able to log in?

 The *Leostream Connection Broker* defines a **pool-based plan** as a set of rules that determine how the Connection Broker manages the connection to a desktop in a pool. This step describes three types of pool-based plans. 1) Protocol, 2) Power Control, and 3) Release. The Connection Broker also provides **location-based plans** for setting registry keys and attaching network printers to the remote desktop. See the *Connection Broker Administrator's Guide* for information on using location-based plans.

Protocol Plans

Protocol plans determine the display protocol the Connection Broker uses to connect a user to their desktop. The Connection Broker provides one default protocol plan, which is shown on the **> Configuration > Protocol Plans** page, shown in the following figure.




Actions	Name	In Use	Leostream API Protocols	Web Browser Protocols
Edit	Default	Yes	RDP	RDP
Edit	HTML5 RDP / Leostream Gateway	Yes	RDP	Leostream HTML5
Edit	Teradici via Gateway	Yes		

3 rows

The default Protocol Plan instructs the Connection Broker to connect to the remote desktops using Microsoft RDP.

To create a new Protocol Plan, click the **Create Protocol Plan** link. The **Create Protocol Plan** form is divided into sections based on the type of client device used to log into Leostream, for example, Leostream Connect or the Leostream Web client.

 *Your Connection Broker license determines which display protocols your Connection Broker can use. If the display protocol you want to use is not shown on the **Create Protocol Plan**, please contact sales@leostream.com to obtain an updated license key.*

In each section, indicate which protocol the Connection Broker should use to connect users to their desktops by selecting **1** from that protocol's **Priority** drop-down menu. Then, use the **Configuration file** and **Command line parameters** to determine how that connection is launched. For example, for RDP, the **Configuration file** is a list of RDP-file parameters that determine if, for example, the connection is launched in full screen.


 *See the Leostream Guide for [Working with Display Protocols](#) for more information on defining command line parameters and configuration files for each supported display protocol.*

For a complete description of protocol plans, see “Building Pool-Based Plans” in the [Connection Broker Administrator's Guide](#).

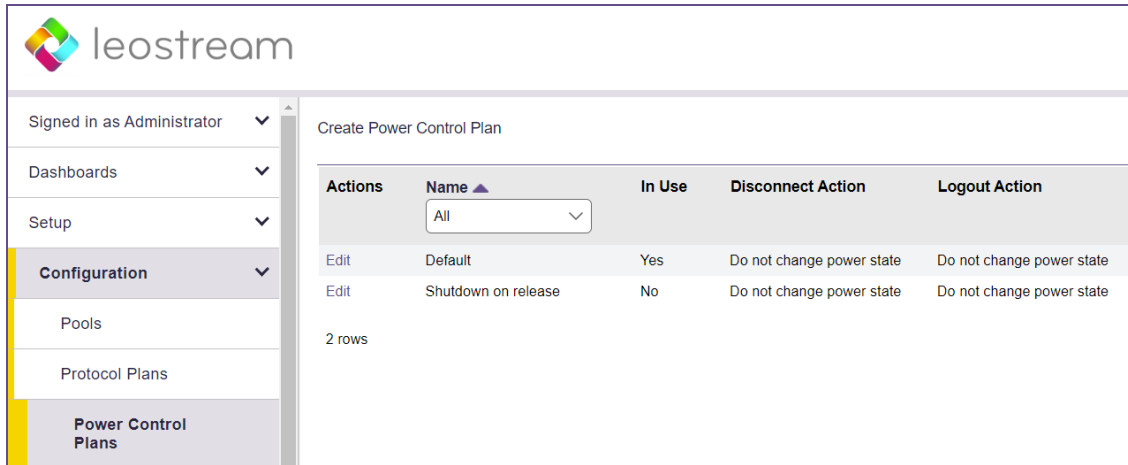
Power Control Plans

Power control and release plans allow you to take actions on the user's remote session based on different events, such as:

- When the user disconnects from their desktop
- When the user logs out of their desktop
- When the desktop is released to its pool
- When the user's session has been idle for a specified length of time

 *The remote desktop must have an installed and running Leostream Agent to allow the Connection Broker to distinguish between user logout and disconnect and to perform actions based on idle time.*

Power control plans define the power control action to take on a desktop. Available power control plans are shown on the **> Configuration > Power Control Plans** page, shown in the following figure.



New Connection Broker installations contain one default power control plan, called **Default**. You can create as many additional power control plans as needed for your deployment. To build a new power control plan:

1. Click the **Create Power Control Plan** link on the **> Configuration > Power Control Plans** page. The **Create Power Control Plan** form, shown in the following figure, opens.

Enter a descriptive name. You'll refer to this name when assigning the plan to a pool.

Select the amount of time to wait before changing the desktop's power state. A wait time of zero tells the Connection Broker to immediately execute the selected power control action.


Select the power control action to take after the wait time elapses. For the Connection Broker to take actions based on disconnect or idle-time events, you must install the Leostream Agent on that desktop.

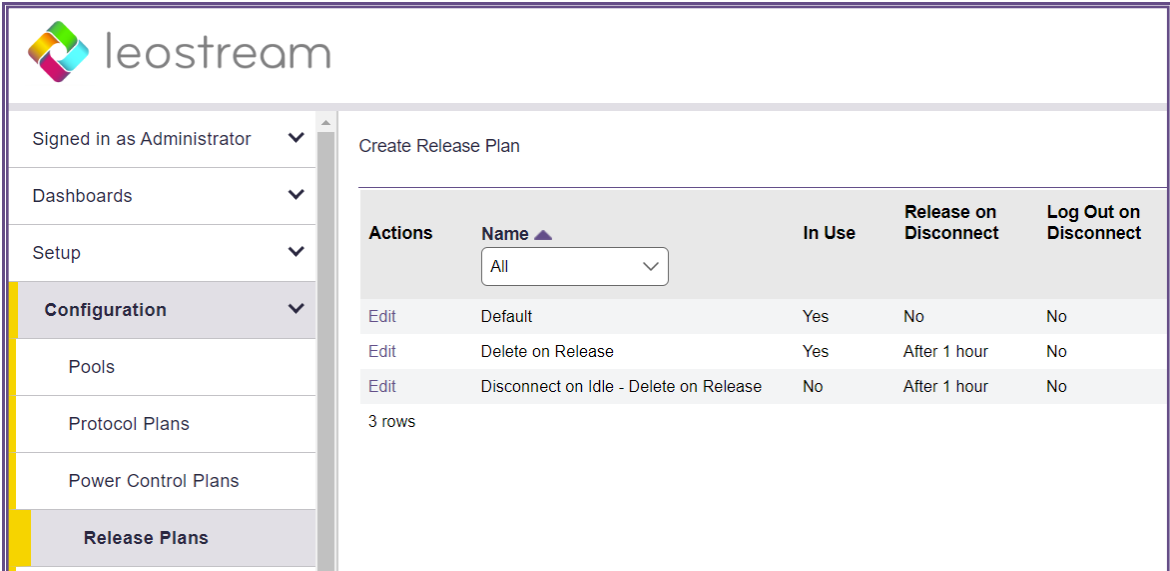
2. Enter a unique name for the plan in the **Plan name** edit field.
3. For each of the remaining sections:
 - a. From the **Wait** drop-down menu, select the time to wait before applying the power action.
 - b. From the **then** drop-down menu, select the power control action to apply. Selecting **Do not change power state** renders the setting in the **Wait** drop-down menu irrelevant, as no action is ever taken.

- Click **Save** to store the changes or **Cancel** to return to the > **Configuration > Power Control Plans** page without creating the plan.

Release Plans

Release plans determine how long a desktop remains assigned to a user. When the assignment is broken, the Connection Broker releases the desktop back to its pool, making it available for other users. Available release plans are shown on the > **Configuration > Release Plans** page, shown in the following figure.

 When a desktop is **assigned** to a user, the Connection Broker always offers that desktop to that user, regardless of where the user logs in, and to no other users. Desktops can be policy-assigned or hard-assigned. For a description of hard-assigned desktops, see the *Connection Broker Administrator's Guide*.



The screenshot shows the leostream web interface. On the left is a sidebar with navigation links: Signed in as Administrator, Dashboards, Setup, Configuration (highlighted), Pools, Protocol Plans, Power Control Plans, and Release Plans (highlighted). The main content area is titled 'Create Release Plan'. It contains a table with the following data:

Actions	Name ▲	In Use	Release on Disconnect	Log Out on Disconnect
Edit	Default	Yes	No	No
Edit	Delete on Release	Yes	After 1 hour	No
Edit	Disconnect on Idle - Delete on Release	No	After 1 hour	No

Below the table, it indicates '3 rows'. There is also a dropdown menu for 'Name' with 'All' selected.

New Connection Broker installations contain one default release plan. The default release plan is designed to keep the user assigned to their desktop until they log out. When the user logs out, the Connection Broker releases the desktop back to its pool. You can create as many additional release plans as needed for your deployment, using the **Create Release Plan** form shown in the following figure.

The screenshot shows the 'Create Release Plan' form with several sections and fields. Annotations with arrows point to specific fields:

- Plan name:** A text input field at the top.
- When User Disconnects from Desktop:** A section containing 'Release to pool:' and 'Log user out:' dropdown menus, both set to 'No'.
- When User Logs Out of Desktop:** A section containing 'Release to pool:' and 'URL to call' fields. 'Release to pool:' is set to 'Immediately'.
- When Connection is Closed:** A section with 'Execute actions for:' dropdown set to 'When User Logs Out of Desktop'. A note below states: 'This section of the plan executes when no Leostream Agent is installed or communicating on the remote desktop'.
- When Desktop is Idle:** A section with 'Lock desktop:', 'Disconnect:', and 'Log user out:' dropdown menus, all set to 'No'.
- When Desktop is First Assigned:** A section with 'Release to pool:' and 'Release if user does not log in:' dropdown menus, both set to 'No'. A note below states: 'When Desktop is Released actions will not be invoked'.
- When Desktop is Released:** A section with a checkbox 'Log user out of the desktop' (unchecked) and a 'Delete virtual machine from disk:' dropdown set to 'No'.

Enter a descriptive name for the plan. You'll refer to this name when selecting the plan in policies.

This section controls actions taken when the user disconnects, but remains logged into, their remote desktop.

To model Persistent desktops, set all "Release to pool" options to "No". The Connection Broker offers an assigned desktop only to its assigned user.

If the Leostream Agent is not installed on the remote desktop, the Connection Broker cannot distinguish a disconnect from a logout event. For these cases, configure how to interpret the Client Close event that is sent by Leostream Connect.

Idle-time is accumulated when there are no mouse or keyboard events. When performing logout actions, you can also monitor the CPU level to delay the logout.

Use this section to schedule a release action based on the time of day or at an allotted time after assignment

To avoid "rogue" users, forcefully log out the user when the desktop is released.

The "Edit Desktop" page must set the desktop as deletable to use this option.

For example, to build a release plan that schedules a logout one hour after the user disconnects from their desktop:


1. Enter a unique name for the plan in the **Plan name** edit field.
2. To build the Release Plan for our example, in the **When User Disconnects from Desktop** section, select **after 1 hour** from the **Forced Logout** drop-down menu.
3. Click **Save**.

In this release plan, the Connection Broker forcefully logs the user out an hour after they disconnect from their desktop. The logout event then triggers the **When User Logs Out of Desktop** section of the release plan, which releases the desktop back to its pool and removes the user's assignment to the desktop.

For more details on creating and using release plans, see the "Release Plans" section in Chapter 11 of the [Connection Broker Administrator's Guide](#).

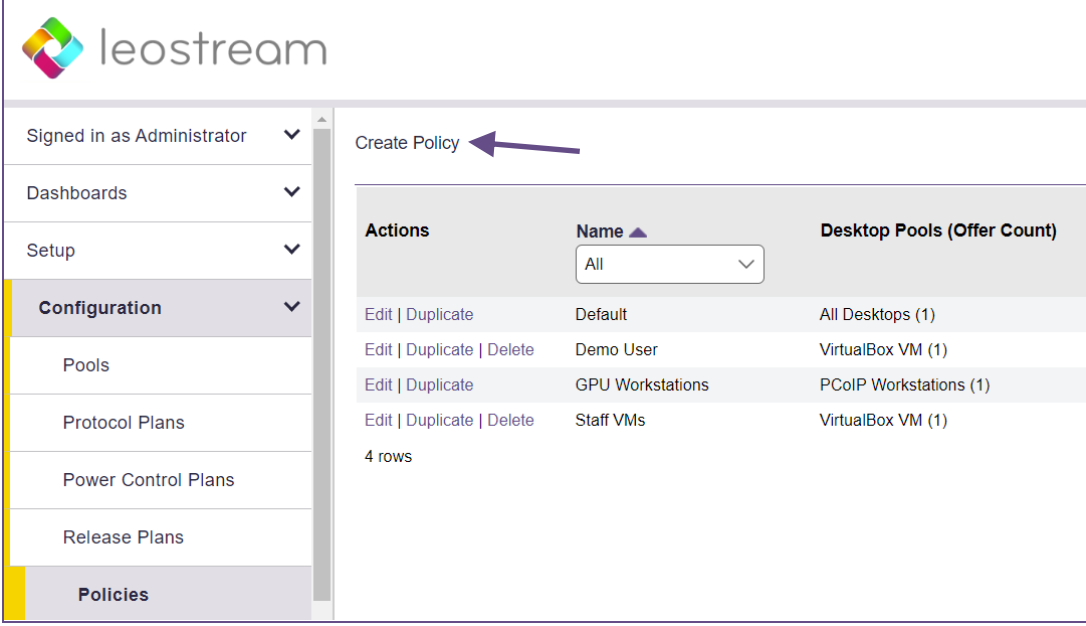
Building User Policies

After you define pools and plans, build policies.

 *The Leostream Connection Broker defines a **policy** as a set of rules that determine how desktops are offered, connected, and managed for a user, including what specific desktops are offered, which power control and release plans are applied to those desktops, what USB devices the user can access in their remote desktop, and more.*

The Connection Broker provides a **Default** policy that applies if no other policy exists or is applicable. The **Default** policy assigns one desktop from the **All Desktops** pool. You can create additional policies, as follows:

1. Navigate to the **> Configuration > Policies** menu.
2. Click the **Create Policy** link, shown in the following figure.



The screenshot shows the Leostream web interface. On the left is a sidebar menu with the following items: Signed in as Administrator, Dashboards, Setup, Configuration (expanded), Pools, Protocol Plans, Power Control Plans, Release Plans, and Policies. The 'Configuration' menu is expanded, showing sub-items: Pools, Protocol Plans, Power Control Plans, Release Plans, and Policies. The 'Policies' item is highlighted. In the main content area, there is a 'Create Policy' link with a blue arrow pointing to it. Below this link is a table with the following data:

Actions	Name ▲	Desktop Pools (Offer Count)
	All ▼	
Edit Duplicate	Default	All Desktops (1)
Edit Duplicate Delete	Demo User	VirtualBox VM (1)
Edit Duplicate	GPU Workstations	PCoIP Workstations (1)
Edit Duplicate Delete	Staff VMs	VirtualBox VM (1)

4 rows

The **Create Policy** form, shown in the following figure, opens.

Create Policy

General | Pool Assignments | Hard Assignments | Rogue User Assignments | Advanced Settings

Policy name

☐ Auto-launch remote viewer session if only one desktop is offered (Web client only)

☐ Launch HTML5 Viewer and External Viewer connections in new window (Web client only)

☐ Hide hover menu when any remote desktop is locked (Leostream Connect only)

☒ Allow multiple selections in Leostream Connect dialogs

☐ Inform user when a pool is out of resources

☐ Prompt user for alternate credentials before connecting to selected desktop (PCoIP only)

Store user-configured protocol parameters

Individually for each connection/client pair

Maximum number of desktops that can be assigned across all pools

<No Limit>

Expire user's resource offers and Connection Broker session after specified elapsed time

2 days

☐ Expire user's session as soon as a remote desktop is locked

☐ Send HTTP GET request at start of session

Notes

Save Cancel

3. In the **General** tab, enter a name for the policy in the **Policy name** edit field. For a discussion on the remaining general policy properties, see the [Connection Broker Administrator's Guide](#).
4. Click **Save** to continue building the policy.
5. Go to the **Pool Assignments** tab.
6. Click the **Add Pool Assignments** link. In the **Edit Pool Assignment** form:
 - a. In the **When User Logs into Connection Broker** section, use the **Number of desktops to offer** drop-down menu to indicate the number of desktops to offer to a user of this policy.
 - b. Use the **Pool** menu to select the pool to offer desktops from. When a user is offered this policy, the Connection Broker sorts the desktops in the selected pool based on the other policy settings, then offers the user the top n desktops from the pool, where n is the number selected in the **Number of desktops to offer** drop-down menu.
 - c. Scroll down to the **Plans** section and select the protocol, power control, and release plans to apply to desktops offered from this pool.

- d. Click **Save**.



In a simple proof-of-concept environment, many of these settings can be left at their default values. Note that, by default, the Connection Broker does not offer a desktop to the user if the desktop does not have an installed Leostream Agent. If you want to offer desktops that do not have a Leostream Agent, select the **Yes, regardless of Leostream Agent status** option from the **Offer running desktops** drop-down menu.

For a complete description of setting up policies, see “Configuring User Experience by Policy” in the [Connection Broker Administrator’s Guide](#).

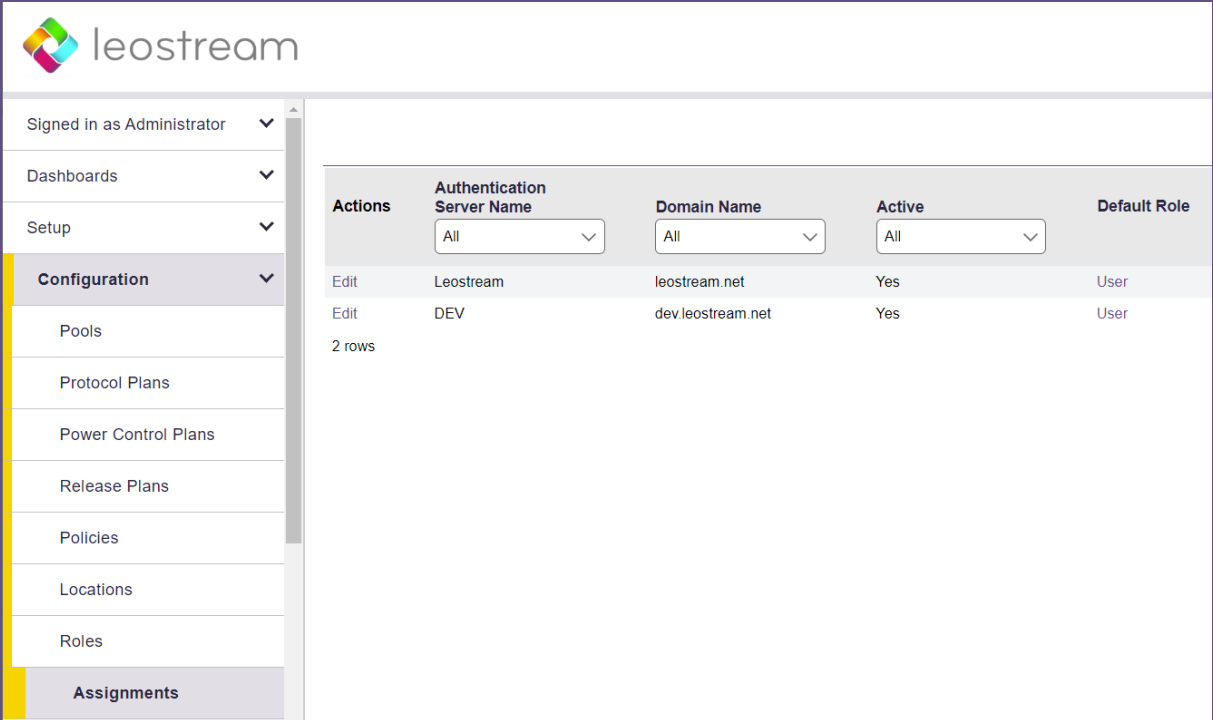


*A policy can offer desktops from multiple pools. To add additional pools, edit the policy and click the **Add Pool Assignment** link on the **Pool Assignments** tab as described in step six of the previous procedure.*

Assigning Policies to Users

When a user logs in to the Connection Broker, the Connection Broker searches the authentication servers you defined on the **> Setup > Authentication Servers** page for a user that matches the credentials provided by the user.

The Connection Broker then looks on the **> Configuration > Assignments** page, shown in the following figure, for the assignment rules associated with the user’s authentication server. For example, if the Connection Broker authenticated the user in the `LEOSTREAM` domain defined on the **> Setup > Authentication Servers** page, the Connection Broker would look in the `LEOSTREAM` assignment rules in the following figure.

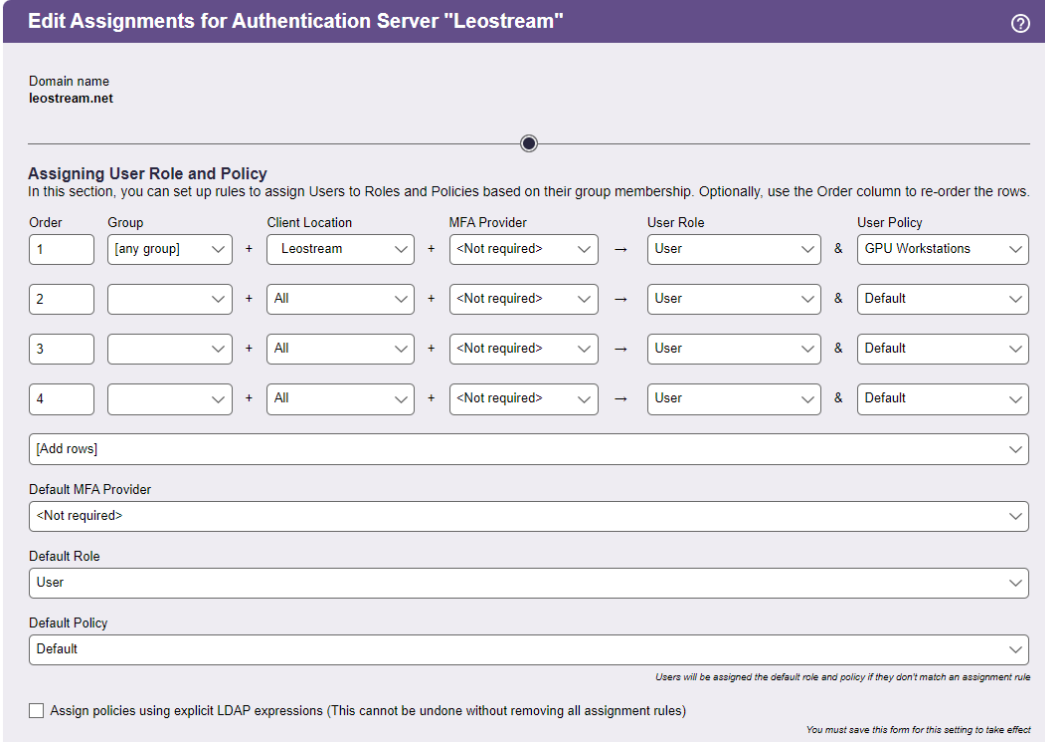


The screenshot shows the Leostream web interface. On the left is a navigation menu with the following items: Signed in as Administrator, Dashboards, Setup, Configuration (highlighted), Pools, Protocol Plans, Power Control Plans, Release Plans, Policies, Locations, Roles, and Assignments. The main content area displays a table of authentication servers.

Actions	Authentication Server Name	Domain Name	Active	Default Role
Edit	Leostream	leostream.net	Yes	User
Edit	DEV	dev.leostream.net	Yes	User

2 rows

To assign policies to users in a particular authentication server, click the **Edit** link associated with that authentication server on the **> Configuration > Assignments** tab, shown in the previous figure. The **Edit Assignment** form for this authentication server appears, shown in the following figure.



The screenshot shows the 'Edit Assignments for Authentication Server "Leostream"' form. The domain name is 'leostream.net'. The form is titled 'Assigning User Role and Policy' and includes instructions: 'In this section, you can set up rules to assign Users to Roles and Policies based on their group membership. Optionally, use the Order column to re-order the rows.'

Order	Group	Client Location	MFA Provider	User Role	User Policy
1	[any group]	Leostream	<Not required>	User	GPU Workstations
2		All	<Not required>	User	Default
3		All	<Not required>	User	Default
4		All	<Not required>	User	Default

[Add rows]

Default MFA Provider: <Not required>

Default Role: User

Default Policy: Default

Users will be assigned the default role and policy if they don't match an assignment rule

☐ Assign policies using explicit LDAP expressions (This cannot be undone without removing all assignment rules)

You must save this form for this setting to take effect

By default, the Connection Broker matches the selection in the **Group** drop-down menu to the user's `memberOf` attribute in Active Directory.



If you modified your groups in Active Directory after you last signed into your Connection Broker, you must sign out and sign back in to have your Connection Broker reflect the authentication server changes.

To assign policies based on the user's `memberOf` attribute:

1. Select the group from the **Group** drop-down menu.
2. If you are using locations, select a location from the **Client Location** drop-down menu.
3. Assign a role to this group and client location pair by selecting an item from the **User Role** drop-down menu.



*In Leostream, **roles** are permissions that control the actions an end user can take on their desktop and the level of access the user has to the Connection Broker Administrator Web interface. A **location** is a group of clients defined by attributes such as manufacturer, device type, OS version, IP address, etc. For more information on building roles and locations, see Chapters 10 and 13 in the [Connection Broker Administrator's Guide](#).*

4. Assign a policy to this group and client location pair by selecting an item from the **User Policy** drop-down menu.

If you need to assign roles and policies based on a different user attributes, see Step 12 under “Assigning Roles and Policies Based on any Attribute” in the [Connection Broker Administrator's Guide](#).



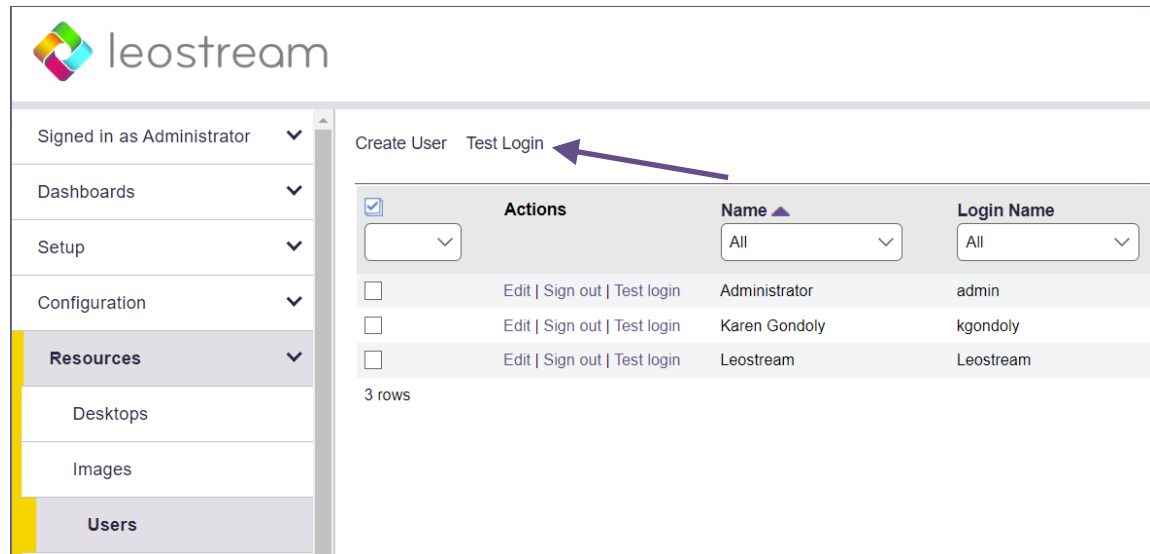
Leostream supports various different multi-factor authentication systems. If you require MFA, visit the Support Documents tab on the Leostream [Documentation](#) page for more information.

Testing Your Connection Broker Configuration

To test your Connection Broker, ensure that users are being assigned to the correct policy, and offered the correct desktops. You can test user logins before the user has ever logged into, and been loaded into, Leostream.

1. Navigate to the **> Resources > Users** menu. As users log into your Leostream environment, their user information is added to this page. You do not need to load users before they can log in.

2. Click the **Test Login** link at the top of the page, shown in the following figure.



3. In the **Test Login** form that opens, enter the name of the user to test in the **User Name** edit field.
4. If you are allowing the user to specify their domain, select a domain from the **Domain** drop-down.
5. Click **Run Test**. The Connection Broker searches the authentication server for your user, and then presents a report, for example:

Test Results

User name: Maybel
 Authentication server: Leostream
 Domain: leostream.net
 Client: Chrome/91.0 (Web Browser) at 10.110.3.40
 (This client is in these locations: Web browsers, All)

Looking up user "Maybel":
 in authentication server "Leostream" ← **found user** ([show Active Directory attributes](#))

Trying to match with Authentication Server Assignment rules: ([edit](#))

- 1: "memberOf" exactly matches "CN=Karen Test Sub Group,OU=Karen Test,OU=Karen Groups,DC=leostream,DC=net", location "All" ← no attribute match
- 2: "memberOf" exactly matches "CN=Students,OU=Security Groups,DC=leostream,DC=net", location "All" ← **matched**

User will have Role "User" and Policy "Default"

User must first successfully authenticate with RADIUS server "Okta RADIUS Agent" ← **PIN+token not provided**

User's role provides access to Web Client, only.

Policy: Default ([edit](#))

No hard-assigned desktops found

Pool "All Desktops" ([edit](#))

Including pool for all users

Looking for two desktops

Policy settings for this pool:

- follow-me mode
- do not allow users to change power state of offered desktops
- offer powered-on desktops without a running Leostream Agent
- do not offer stopped/suspended desktops
- favor previously-assigned desktops
- may offer desktops with pending reboot job
- do not confirm desktop power state
- do not power on stopped desktops
- do not log out rogue users
- do not attempt single sign-on into desktop console session
- allow manual release (but Maybel's role prevents it)
- Power control plan: Default
 - when user disconnects, do not change power state
 - when user logs out, do not change power state
 - when desktop is released, do not change power state
 - when desktop is idle, do not change power state
- Release plan: Default
 - handle unverified user state as disconnect
 - do not release on disconnect
 - do not log user out on disconnect
 - when user logs out, release immediately
 - do not lock desktop if idle
 - do not disconnect user if desktop is idle
 - do not log user out if desktop is idle
 - do not release after initial assignment
 - if user does not log in, release

(389 total, 383 in service, 18 policy filtered, 18 pool filtered, 18 available, 8 running, 8 with an IP address)

kdg-debian9 ← **available**, running, Leostream Agent v5.1.22.0, will offer as: "kdg-debian9", will connect via RDP ([show](#)) ← will use protocol plan "Default" associated with policy [Default](#)

kdg-1803 ← **available**, running, Leostream Agent v7.3.13.0, will offer as: "kdg-1803", will connect via RDP ([show](#)) ← will use protocol plan "Default" associated with policy [Default](#)

Offering two desktops with this policy.

See "Testing User Role and Policy Assignment" in the [Connection Broker Administrator's Guide](#) for information on interpreting test login results.



Please complete a login test before contacting Leostream Support.