



| Teradici Cloud
Access Software



The Leostream Connection Broker

Advanced Connection and Capacity Management for Hybrid Clouds

Version 9.0 – January 2019

Contacting Leostream

Leostream Corporation
271 Waverley Oaks Rd.
Suite 206
Waltham, MA 02452
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 2002-2019 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.

HPE is a trademark of Hewlett-Packard Enterprise Development, L.P. in the U.S. and other countries. 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, SQL Server, Hyper-V, 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: OVERVIEW	4
HIGH-LEVEL ARCHITECTURE	4
CLOUD INFRASTRUCTURE COMPONENTS	5
TERADICI CLOUD ACCESS PLATFORM COMPONENTS	5
USING PCOIP CLIENTS WITH LEOSTREAM	6
CHAPTER 2: BUILDING A PROOF-OF-CONCEPT	7
INSTALLING THE LEOSTREAM CONNECTION BROKER	7
INSTALLING THE TERADICI CONNECTION MANAGER AND SECURITY GATEWAY	7
CHAPTER 3: PREPARING DESKTOPS AND IMAGES	8
INSTALLING LEOSTREAM AGENTS	8
INSTALLING THE CLOUD ACCESS SOFTWARE	8
CHAPTER 4: CONFIGURING THE CONNECTION BROKER	9
STEP 1: ADDING AUTHENTICATION SERVERS	9
STEP 2: ADDING DESKTOPS	11
<i>Connecting Leostream to an OpenStack Cloud.....</i>	<i>11</i>
<i>Connecting Leostream to Amazon Web Services.....</i>	<i>12</i>
<i>Connecting Leostream to Microsoft Azure</i>	<i>13</i>
STEP 3: DEFINING POOLS AND PROVISIONING INSTANCES	14
<i>Pooling by Center</i>	<i>14</i>
<i>Provisioning New Desktops</i>	<i>15</i>
STEP 4: DEFINING PLANS	17
<i>Protocol Plans.....</i>	<i>17</i>
<i>Power Control Plans.....</i>	<i>17</i>
<i>Release Plans</i>	<i>19</i>
STEP 5: DEFINING USER POLICIES	21
STEP 6: ASSIGNING USER ROLES AND POLICIES	23
STEP 7: TESTING USER LOGIN	25
STEP 8: CONNECTING FROM A PCOIP CLIENT	26

Chapter 1: Overview

As a solution provider, you need to develop and evolve solutions that expand your portfolio and satisfy your customers' needs. You require tools that make it easier to manage the day-to-day operation of your solution, as well as provide the level of access and performance end users require. The combination of Leostream and the Teradici Cloud Access Software or Cloud Access Platform is the ideal solution.

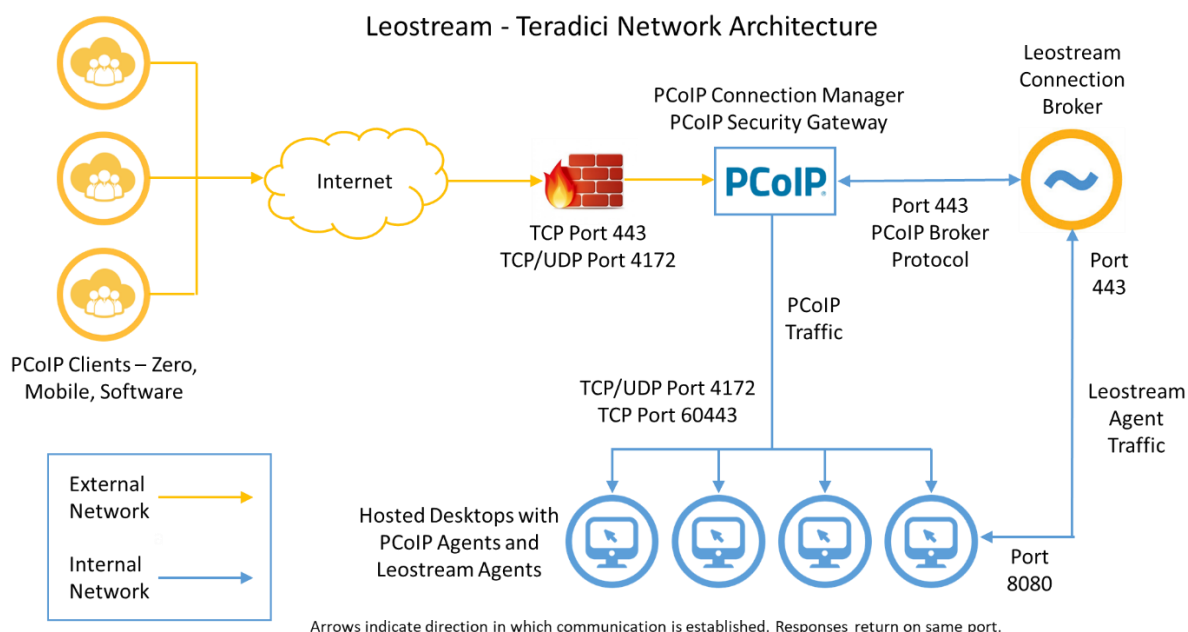
The Leostream Connection Broker helps you automate the lifecycle of your solution - including provisioning and deleting desktops and applications - and provides access management for your solutions, so end users have a seamless login to the correct resources. The Teradici Cloud Access Software and Cloud Access Platform utilize the industry-leading PCoIP technology, so your applications are delivered securely via a lossless protocol, ensuring uncompromised user experience – regardless of network conditions. And, with the built-in Teradici Security Gateway, your solutions are available anywhere, no matter where your users roam.

Using Leostream with the Teradici Cloud Access Platform, you can host solutions that provide secure, policy-based access to desktops and applications from any client device, including PCoIP Zero Clients and PCoIP Soft Clients and Mobile Clients (iOS and Android), from any hosting platform, including VMware, Amazon Web Service, Microsoft Azure, and Google Cloud Platform.

This document describes how to integrate Leostream with the Teradici Cloud Access Platform

High-Level Architecture

A high-level Leostream Connection Broker and Teradici Cloud Access Platform architecture is shown in the following figure.



The following sections give an overview of the Leostream and Teradici components. For more information and documentation on the Teradici Cloud Access Platform, visit <https://techsupport.teradici.com>.

Cloud Infrastructure Components

The Leostream Connection Broker and Teradici Cloud Access Platform can be installed into a number of cloud platforms, both public and private. Using Leostream with the Teradici Cloud Access Software and Cloud Access Platform, you can build solutions that are hosted on any of the following cloud/virtualization platforms.

- Amazon Web Services
- Microsoft Azure
- Google Cloud Platform
- OpenStack clouds, both public and hosted in your data center
- VMware vSphere and ESXi

Teradici Cloud Access Platform Components

A solution that integrates Leostream and the Teradici Cloud Access Platform includes the following Teradici components.

- **PCoIP Connection Manager and Security Gateway:** The PCoIP Connection Manager creates a PCoIP session between the PCoIP Client and remote desktop. The PCoIP Security Gateway allows WAN users to access their remote desktops from the Internet without having to set up a VPN connection. It is not required for LAN access. The Leostream Connection Broker communicates with the PCoIP Connection Manager using the PCoIP Broker Protocol, to offer the correct resources to the user based on their Leostream policy.
- **Teradici License Server (optional):** If the PCoIP Agents on your desktops cannot register with the Teradici automatic cloud licensing server, you can install your own license server to track your session licenses.
- **PCoIP Agents:** The PCoIP Security Gateway allows WAN users to securely access their remote desktops from the Internet without having to set up a VPN connection. It is not required for LAN access. Desktops with installed PCoIP Agents appear on the > **Resources > Desktops** page of the Connection Broker.
- **PCoIP Clients:** The PCoIP client is a device or application for the user to connect to their remote desktop. PCoIP clients decode the PCoIP Session and present the results to the user. A number of client vendors, such as Amulet Hotkey and Dell Wyse®, have embedded PCoIP processors into their end-point, zero client hardware. In addition, users can connect to their desktop using PCoIP Soft Clients and Mobile Clients (iOS and Android). PCoIP client devices appear in the > **Resources > Clients** page of the Connection Broker.

Using PCoIP Clients with Leostream

You can use any supported PCoIP software, mobile, or zero client to log into Leostream. The type of client you use, and whether the client communicates with Leostream or the PCoIP Connection Manager, determines what types of PCoIP resources can be connected. The following table describes the types of resources users can connect to from different types of PCoIP client.

If the user logs into	And the client communicates with	The client can connect to Virtual Machines	The client can connect to Physical Machines
PCoIP Software (Mac, Windows, ChromeOS)	PCoIP Connection Manager	Running the PCoIP Standard or Graphics Cloud Access Software	N/A
PCoIP Mobile			
PCoIP Zero			
PCoIP zero client	Leostream Connection Broker	Running the VMware Horizon View Direct Connection Plug-In	With an installed Remote Workstation Cards
Leostream Connect	Leostream Connection Broker	<ul style="list-style-type: none"> Running the VMware Horizon View Direct Connection Plug-In – Leostream Connect launches the VMware Horizon View Client to establish the connection Running the Teradici Cloud Access Software – Leostream Connect launches the PCoIP software client to establish the connection 	With an installed Remote Workstation Cards – Leostream Connect launches the PCoIP Software client to establish the connection

When using PCoIP zero clients, they must be running firmware version 5.x. Set the **Server URI** to either the PCoIP Connection Manager or to the Leostream Connection Broker, depending on what system the client needs to communicate with. As an example, with the **Server URI** set to PCoIP Connection Manager, you can connect to any virtual machine that is part of your Cloud Access Platform, however you cannot connect to workstations with installed PCoIP Remote Workstation Card.

Chapter 2: Building a Proof-of-Concept

Installing the Leostream Connection Broker

The Connection Broker runs on the latest 64-bit CentOS 7, Red Hat Enterprise Linux 7, Ubuntu 16.04, or SUSE Linux Enterprise Server 12 SP3 operating systems.

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

- 1 vCPU
- 2.0 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. After the updates are applied, if your Connection Broker instance has access to the internet, you can install the Connection Broker by logging into the instance's console and executing the following command.

```
curl http://downloads.leostream.com/broker.prod.sh | bash
```

If your Connection Broker instance does not have internet access, download the appropriate Connection Broker package from the following location and copy the file into the Connection Broker instance.

```
https://www.leostream.com/downloads/connection-broker
```

See the [Leostream Installation Guide](#) for the appropriate commands to use to finish the installation on your chosen operating system and obtain your Leostream license. For information regarding configuring an OpenStack, Amazon Web Services, or Microsoft Azure environment for use with the Leostream Connection Broker, please see the associated [Quick Start](#) guide for your platform.

Installing the Teradici Connection Manager and Security Gateway

The Connection Broker requires the PCoIP Connection Manager in order to communicate with the PCoIP clients. The PCoIP Connection Manager is installed on a separate Linux system. Please contact Teradici support for more information on downloading and installing the PCoIP Connection Manager.

For instructions on configuring the PCoIP Connection Manager to communicate with your Leostream Connection Broker, see the [Leostream Support Blog](#).

Chapter 3: Preparing Desktops and Images

The Leostream Connection Broker can manage connections to remote desktops running Microsoft Windows and Linux operating systems.

When using Leostream to provision new desktops in AWS, Azure, or OpenStack, ensure that the master images include an installed and configured Leostream Agent and PCoIP Agent, as described in the following sections. You can also use Leostream to provision new desktops in VMware vSphere and ESXi environments. Again, ensure that appropriate agents are installed on the template used for provisioning.

Installing Leostream Agents

See the [Leostream Installation Guide](#) for instructions on installing the Leostream Agent. During the installation, do *not* select the **Enable single sign-on for PCoIP and VNC** task. This task is used only when establishing PCoIP connections to a workstation with a PCoIP Remote Workstation Card. For more information on the Leostream Agent, see the [Leostream Agent Administrator's Guide](#).

The Leostream Agent can locate the Connection Broker through the `_connection_broker` DNS SRV record. For large installations, Leostream recommends using this DNS SRV record. If you do not have, or do not want to use, a DNS SRV record for the Connection Broker, enter the Connection Broker IP address when you install the agent.

Installing the Cloud Access Software

The Connection Broker can connect users to Windows and Linux desktops that run either the Standard or Graphics Cloud Access Software. Contact Teradici for more information on obtaining and licensing the Cloud Access Software.

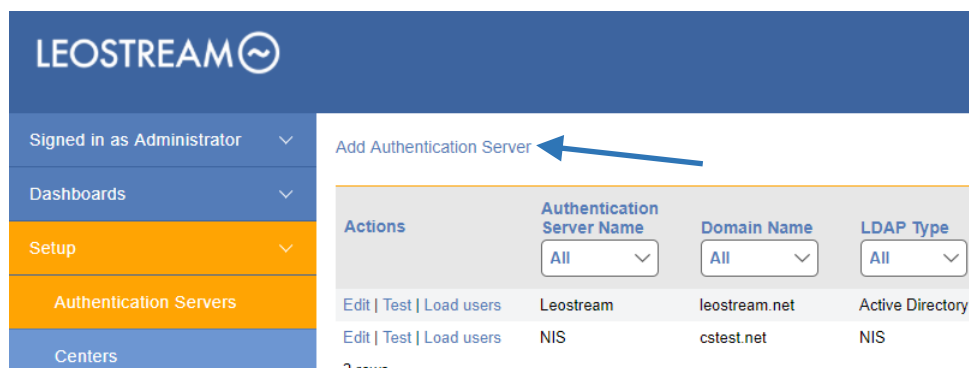
Chapter 4: Configuring the Connection Broker

Step 1: Adding Authentication Servers

The Connection Broker can authenticate users in standard LDAP systems, such as Active Directory, or OpenLDAP™, and with NIS authentication servers. In this example, we add an Active Directory authentication server, as follows. If you do not plan to use an authentication server, you can also define users locally in the Connection Broker. See “Locally Authenticated Users” in the [Connection Broker Administrator’s Guide](#) for more information.

Note: Any options not covered in the following procedure remain at their default values.

1. Navigate to the > **Setup > Authentication Servers** menu.
2. Click the **Add Authentication Server** link, shown in the following figure.



3. The **Add Authentication Server** form opens. In the **Authentication Server name** edit field, enter a name for this server in the Connection Broker.
4. In the **Domain** edit field, enter the domain name associated with this Active Directory server.
5. 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' configuration page. It includes a 'Type' dropdown menu set to 'Active Directory'. Below it is a 'Specify address using' dropdown menu set to 'Hostnames or IP addresses'. There are two input fields: 'Hostname or IP address' containing 'LEO-AD.leostream.net' and 'Port' containing '389'. A small note below these fields states: 'If using multiple addresses, separate each entry with spaces'. Below the input fields is an 'Algorithm for selecting from multiple addresses' dropdown menu set to 'Random'. A small note below this dropdown states: 'The sequential algorithm uses the first working address in the list'. At the bottom, there is a checkbox labeled 'Encrypt connection to the authentication server using SSL (LDAPS)' which is currently unchecked.

- a. Select **Active Directory** from the **Type** drop-down list.
 - b. From the **Specify address using** drop-down menu, select **Hostname or IP address**.
 - c. Enter the authentication server hostname or IP address in the **Hostname or IP address** edit field.
 - d. Enter the port number in the **Port** edit field.
 - e. Check on 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.
6. 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.

The screenshot shows the 'Search Settings' configuration page. It includes a heading 'Search Settings' followed by a description: '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.' Below this is a 'Login' input field containing 'Administrator@leostream.net'. A small note below this field states: 'Enter a fully qualified login name, e.g. Administrator@YOUR_DOMAIN.com or CN=Administrator,CN=Users,DC=YOUR_DOMAIN,DC=com'. Below the login field is a 'Password' input field which is currently empty.

7. 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.
8. Click **Save**.

For more detailed instructions, see the chapter “Authenticating Users” in the [Connection Broker Administrator’s Guide](#).

Step 2: Adding Desktops

To manage desktops, create centers that connect your Leostream Connect Broker to one or more hosting platforms.



*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. For a complete set of instructions for all center types, see “Chapter 6: Connecting to your Hosting Platforms” in the [Connection Broker Administrator’s Guide](#). The remainder of this step focuses on OpenStack clouds, and Microsoft Azure and Amazon Web Services environments.*



If you do not see a way to create a center for your hosting platform, please contact sales@leostream.com to update your Leostream license key.

Connecting Leostream to an OpenStack Cloud

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.

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.
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 an IP address to your identity service that is reachable by your Connection Broker.



Leostream supports only version 3 of the Keystone API.

6. Enter the OpenStack domain that contains your project and user in the **Domain** edit field.
7. Specify the project you want to manage in the **Project** edit field.
8. In the **Username** edit field, enter the name of a user with the necessary permissions for this project.
9. Enter this user's password into the **Password** edit field.
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.

Connecting Leostream to Amazon Web Services

The Connection Broker can inventory instances and images in your AWS account, and manage provisioning and terminating instances based on the pool, policy, and plan settings in your Connection Broker. To manage desktops hosted in AWS, you must install the Leostream Agent on your AWS instance and ensure that the Connection Broker has network access to the instances.

To create an AWS center:

1. Go to the **> Setup > Centers** page.
2. Click the **Add Center** link.
3. In the **Add Center** form, select **Amazon Web Services** from the **Type** drop-down menu.
4. Enter a name for the multi-user center in the **Name** edit field.
5. Select the AWS region you want to manage from the **Region** drop-down menu. Create separate centers for each region you want to manage in the Connection Broker.
6. Enter your AWS access key into the **Access Key ID** edit field. You can create an IAM user to use with Leostream. Ensure that user has sufficient privileges to access EC2.
7. Enter the secret key associated with your access key into the **Secret Access Key** field.
8. Select a time from the **Inventory refresh interval** drop-down menu. This setting tells the Connection Broker how often to refresh the desktops imported from this center. The refresh interval is the length of time between when one refresh action completes and the next refresh action begins.
9. Click **Save** to create the center.

The instances in the center's AWS region appear in the > **Resources** > **Desktops** page. The AMIs available for provisioning appear 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.

Connecting Leostream to Microsoft Azure

In order to manage Azure instances, you need to create an Azure center in your Leostream Connection Broker. To create the Azure center, you must first acquire the necessary IDs for your Azure Subscription. See the [Leostream Quick Start Guide for Azure Clouds](#) for information on how to obtain the necessary IDs.

After you have your IDs, to create the Azure center:

1. Go to the > **Setup** > **Centers** page.
2. Click the **Add Center** link.
3. In the **Add Center** form, select **Microsoft Azure** from the **Type** drop-down menu.
4. Enter a name for the multi-user center in the **Name** edit field.
5. Select the Azure region you want to manage from the **Region** drop-down menu. Create separate centers for each region you want to manage in the Connection Broker.
6. Enter your Azure subscription ID into the **Subscription ID** edit field.
7. Enter your tenant ID into the **Tenant ID** edit field.
8. Enter your client ID into the **Client ID** edit field.
9. Enter the secret key associated with your Leostream application into the **Secret Access Key** field.
10. Select a time from the **Inventory refresh interval** drop-down menu. This setting tells the Connection Broker how often to refresh the desktops imported from this center. The refresh interval is the length of time between when one refresh action completes and the next refresh action begins.
11. Click **Save** to create the center.

The instances in the center's Azure region appear on the > **Resources** > **Desktops** page. The images available for provisioning appear 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.

Step 3: Defining Pools and Provisioning Instances

After you create your centers and the Connection Broker inventories all desktops, you can combine the desktops into logical groups, or **pools**. Use pools to create sets of desktops that have similar attribute or are used by a particular group of users.



*The Leostream Connection Broker defines a **pool** as any group of desktops. Pools also control provisioning in Leostream.*

How you configure your pools depends on the services you plan to provide to end users and customers. You may pool desktops by customer, or by installed application. Leostream provides a variety of way to configure you pools. For a complete description of pools, see the “Creating Desktop Pools” chapter in the Connection Broker Administrator’s Guide.

Pooling by Center

If you want to group or provision desktops in a particular center, create your pool, as follows:

1. Go to the > **Configuration > Pools** page.
2. Click **Create Pool**, as shown in the following figure.

The screenshot shows the Leostream web interface. On the left is a navigation sidebar with the Leostream logo at the top. Below the logo, there are links for 'Signed in as Administrator', 'Dashboards', 'Setup', 'Configuration', and 'Pools'. The 'Configuration' link is highlighted in orange. To the right of the sidebar, there is a header bar with 'Create Pool', 'Refresh', and 'View as List' buttons. Below this header is a table with columns: 'Actions', 'Name', 'Total', 'In Use', and 'Available'. The table contains four rows of data:

Actions	Name	Total	In Use	Available
Edit	All Desktops	127	Yes	126
Edit	All Linux Desktops	66	No	66
Edit	Karen's Linux VMs	19	Yes	19
Edit	All Windows Desktops	46	No	45

3. Enter a unique name for this pool in the **Name** edit field.
4. Select **Centers** from the **Define pool using** drop-down menu.

For information on creating pools using desktop attributes or any other method, see the “Creating Desktop Pools” chapter in the Connection Broker Administrator’s Guide.

5. In the **Center Selection** section, select the appropriate center from the **Available centers** list, for example:

6. Click the **Add item** link to the right of the **Available centers** list.
7. Click **Save**.

The pool created in this example contains all of the instances already in the subscription associated with the selected Azure center. To instruct the Connection Broker to launch new instances, configure the **Provisioning Limits** and **Provisioning Parameters** sections in the **Edit Pool** page, as described in the next section.

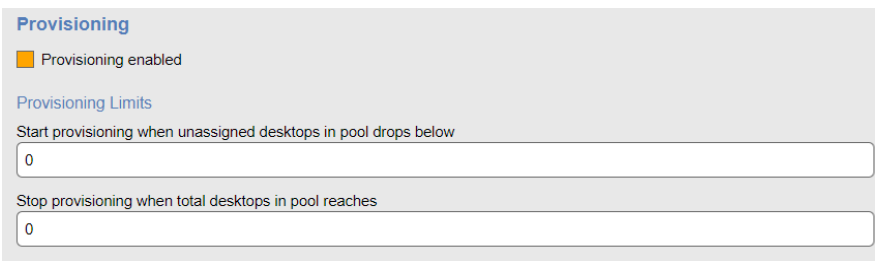
Provisioning New Desktops

Provisioning allows you to generate new OpenStack, AWS, Azure, or VMware instances when the number of desktop in a pool reaches a specified lower threshold. Before provisioning instances, ensure that you do the following:

1. Create master images. In OpenStack, the images are displayed on the images page associated with the project. In AWS, the images are the AMIs in your account. For VMware, use the templates or snapshots in vCenter. In Azure, the images can be created in the Azure Resource Manager or using the API. Ensure that your master images contain an installed Leostream Agent and PCoIP Agent.

2. For OpenStack, Azure, and AWS deployments, configure the network where newly provisioned desktops will exist. Ensure that the network ID for this network is included in the **Network UUID** field of your OpenStack center. When provisioning desktops into Azure and AWS, Leostream uses the network you select in the **Provisioning Parameters**.

The **Provisioning** section of the **Edit Pool** page allows you to configure when and how the Connection Broker creates new EC2 instances in your AWS account. By default, the **Provisioning enabled** checkbox is selected, as shown in the following figure, and provisioning is on for all your pools.



Provisioning

☒ Provisioning enabled

Provisioning Limits

Start provisioning when unassigned desktops in pool drops below

0

Stop provisioning when total desktops in pool reaches

0

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.

After defining provisioning limits, use the **Provisioning Parameters** section to configure provisioning. See “Chapter 9: Provisioning New Desktops” in the Connection Broker Administrator’s Guide for complete instructions on provisioning into the various platforms.

Step 4: Defining Plans

After you separate your desktops into pools, define plans that determine how the Connection Broker manages the user’s session.



*The Leostream Connection Broker defines a **plan** as a set of behaviors that can be applied to any number of pools. This step describes three types of plans: 1) Power Control, 2) Release, and 3) Protocol.*

Protocol Plans

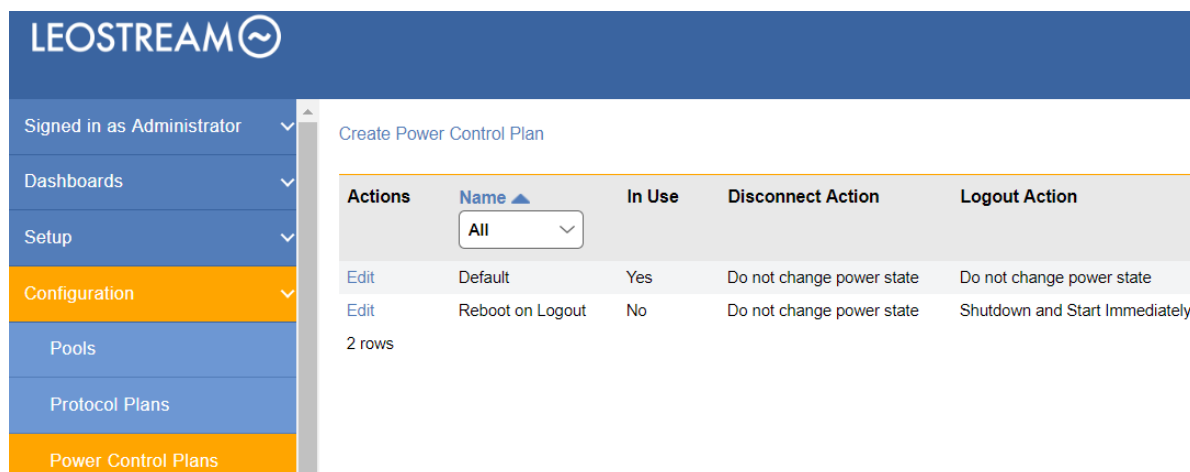
The Connection Broker always establishes a PCoIP connection when a user logs in at a PCoIP client device. When using the PCoIP protocol, the protocol plan is used only to configure the port to check when powering on the desktop or using backup pools or failover desktops. By default, the Connection Broker checks port 8080. If you want to change the default port:

1. Go to the **> Configuration > Protocol Plans** page.
2. Click the **Create Protocol Plan** at the top of the page. The **Create Protocol Plan** form opens.
3. Scroll down to the **Teradici PCoIP Client Configuration** section, shown in the following figure.

4. Enter the new port in the **Alternate port for remote viewer port check** edit field.
5. Click **Save** to save the form.

Power Control Plans

Power control plans define what power control action is taken on a desktop when the user disconnects or logs out of the desktop or when the desktop is released to its pool. 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 **Create Power Control Plan** 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.

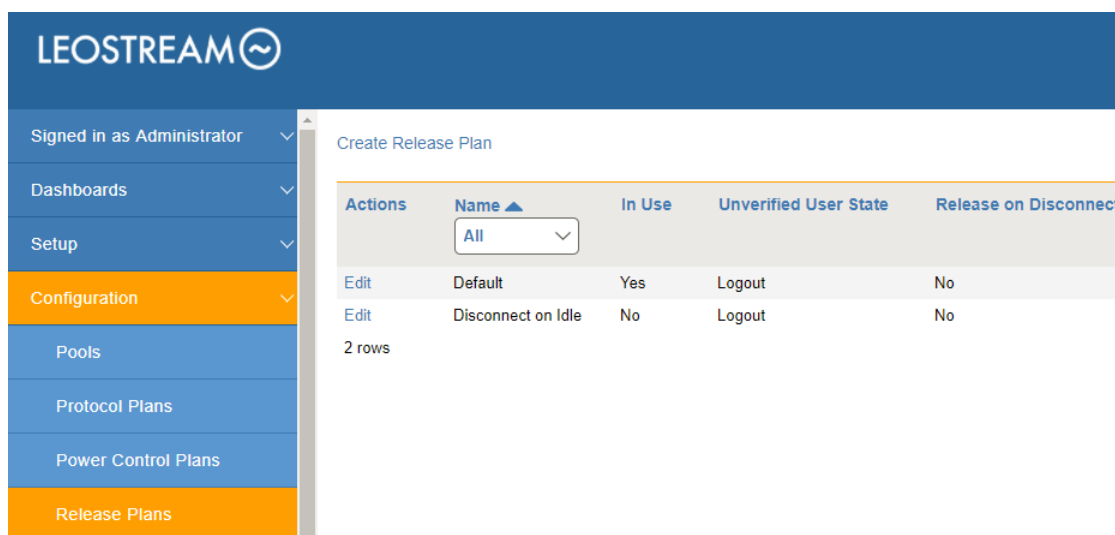
2. Enter a unique name for the plan in the **Plan name** edit field.
3. For each of the three remaining sections:
 - a. From the **Wait** drop-down menu, select a time period to wait before applying the power control action.

- 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.
4. Enter any optional **Notes**.
5. Click **Save** or **Cancel** to return to the **> Configuration > Power Control Plans** page without creating the plan.

 *The 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.*

Release Plans

Release plans define how long a desktop remains assigned to a user and when it is released to its pool, as well as if a user should be forcefully logged out of their desktop. Available release plans are shown on the **> Configuration > Release Plans** page, shown in the following figure.



Actions	Name	In Use	Unverified User State	Release on Disconnect
Edit	Default	Yes	Logout	No
Edit	Disconnect on Idle	No	Logout	No

2 rows

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

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

Create Release Plan

Plan name:

When User Disconnects from Desktop

Release to pool:

Forced logout:

URL to call:

When User Logs Out of Desktop

Release to pool:

URL to call:

When Connection is Closed

Execute actions for:

This section of the plan executes when no Leostream Agent is installed or communicating on the remote desktop

When Desktop is Idle

Lock desktop:

Disconnect:

Logout:

When Desktop is First Assigned

Release to pool:

Release if user does not log in:

"When Desktop is Released" actions will not be invoked

When Desktop is Released

☐ Log user out of the desktop

☐ Delete virtual machine from disk

Enter a descriptive name. Refer to this name when assigning this plan to pools.

To model a persistent desktop, ensure that the desktop is not released when the user disconnects or logs out.

If a Leostream Agent is not installed on the remote desktop, the Connection Broker cannot distinguish when the user disconnects or logs out of their desktop. If the user logs in using Leostream Connect, the client sends a Connection Close event, and you can determine if the Disconnect or Log out portion of the release plan should be executed.

You can perform actions on the desktop after the user's session is idle for the selected elapsed time. In addition, you can monitor the desktop's CPU levels to ensure that any processes the user is running come to completion before you forcefully log them out.

You can release a desktop back to its pool after a specified elapsed time since the desktop was initially assigned to the user. After the desktop is released, if the user remains logged in, the Connection Broker considers them to be **rogue**.


To avoid rogue users, forcefully log out the user when the desktop is released to its pool.

Select this option to have the Connection Broker completely delete the VM from disk as soon as the desktop is released to its pool. The Connection Broker deletes the VM only if the "Edit Desktop" page for that VM selects the "Allow this desktop to be deleted from disk" option.

2. Enter a unique name for the plan in the **Plan name** edit field.
3. In the **When User Logs Out from Desktop** section, select **No** from the **Release to pool** drop-down menu to create a release plan for persistent desktops. Otherwise, use the **Release to pool** drop-down menu to indicate how long the user is assigned to the desktop.
4. In the **When Desktop is Released** section, select the **Delete virtual machine from disk** option to have the Connection Broker terminate the virtual workspace when the desktop is released back to its pool.


The desktop must be marked as deletable on the **Edit Desktop** page or the Connection Broker will not perform the terminate action.

- Click **Save**.

 The **When Connection is Closed** section does not apply as PCoIP clients do not inform the Connection Broker when a connection is dropped.

Step 5: Defining User Policies

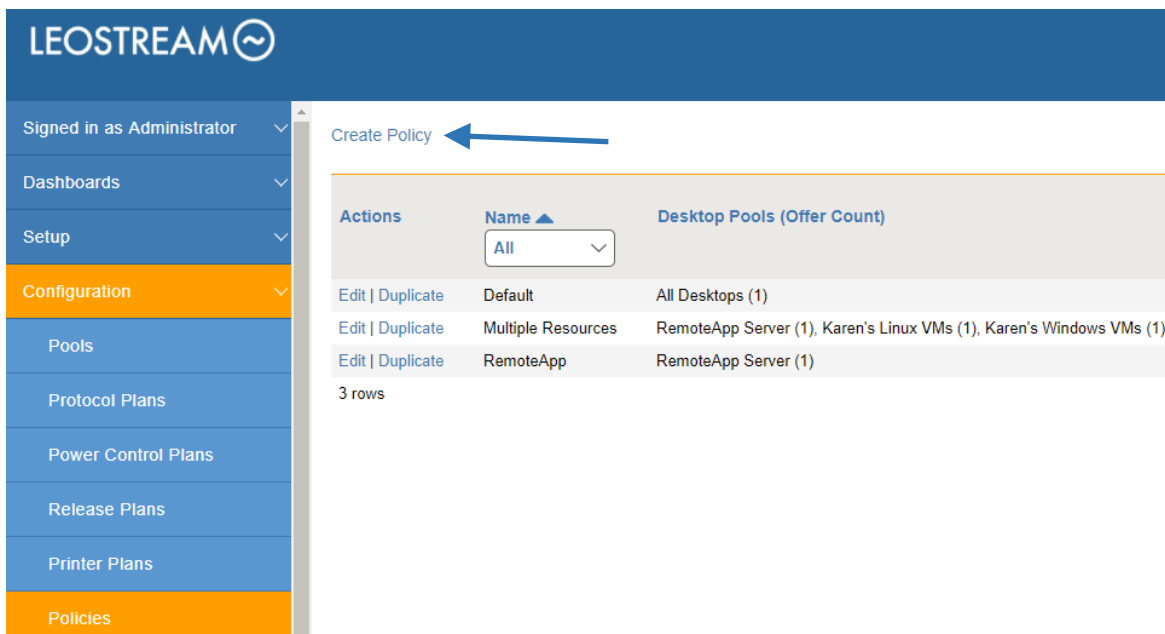
After you define pools and plans, build policies that assign the plans to desktops.

 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:

You can create additional policies, as follows:

- Go to the **> Configuration > Policies** page.
- Click **Create Policy**, as shown in the following figure.



The screenshot shows the Leostream web interface. The left sidebar contains the following menu items: Signed in as Administrator, Dashboards, Setup, Configuration (highlighted), Pools, Protocol Plans, Power Control Plans, Release Plans, Printer Plans, and Policies (highlighted). The main content area is titled 'Create Policy' with a blue arrow pointing to the button. Below the button is a table with the following data:

Actions	Name	Desktop Pools (Offer Count)
Edit Duplicate	Default	All Desktops (1)
Edit Duplicate	Multiple Resources	RemoteApp Server (1), Karen's Linux VMs (1), Karen's Windows VMs (1)
Edit Duplicate	RemoteApp	RemoteApp Server (1)

3 rows

3. In the **Create Policy** form, enter a name for the policy in the **Policy name** edit field. For a discussion of the remaining general policy properties, see the [Connection Broker Administrator's Guide](#).
4. In the **Desktop Assignment from Pools** section, select the pool to offer desktops from in the **Pool** drop-down menu.



*One policy can assign desktops from multiple pools. Use the **[Add Pools]** menu at the bottom of the **Desktop Assignment from Pools** section to add additional pools to the **Create Policy** form.*

5. Select the number of desktops to offer from this pool from the **Number of desktops to offer** drop-down menu.
6. For each pool, use the controls shown in the following figure to configure the policy options.

See the “Configuring User Experience by Policy” chapter of the [Connection Broker Administrator's Guide](#) for information on using the controls shown in the following figure.

The screenshot shows the 'Desktop Assignments from Pools' configuration form. It is divided into two main sections: 'When User Logs into Connection Broker' and 'When User is Assigned to Desktop'.

When User Logs into Connection Broker

- Number of desktops to offer: 1
- Pool: Select ...
- Backup pool: Select ...
- Offer desktops from this pool: To all users of this policy
- Select desktops to offer based on: User ("follow-me" mode)
- Display desktop to user as: Desktop name
- Allow users to restart offered desktops: No
- Offer running desktops: Yes, only if Leostream Agent is running
- Offer stopped and suspended desktops: No
- Offer desktops with pending reboot job: Yes
- Desktop selection preference: Favor desktops previously assigned to this user

When User is Assigned to Desktop

- ☐ Revert the desktop to its most-recent snapshot
- ☐ Confirm desktop's current power state
- ☒ Power on stopped or suspended desktops
- ☐ Log out any rogue users (also applies when reconnecting to assigned desktop)
- ☐ Enable single sign-on to desktop console (DCV, VNC, PCoIP, and HTML5, only)
- ☐ Prevent user from manually releasing desktop
- ☐ Adjust time zone to match client (Leostream Connect and HP SAM, only)
- ☐ Enable collaboration and session shadowing (NoMachine NX, HP RGS and Mechdyne TGX, only)
- ☐ View only shadowing, not interactive (NoMachine NX, only)

7. In the **Plans** section, select the protocol, power control, and release plans to use for desktops that are offered from this pool. For this getting started guide, use the Default plans.
8. Click **Save**.



*You do not need to select the **Enable single-sign-on to desktop console** option when using the Teradici Cloud Access Software or Cloud Access Platform. Users always experience single sign-on to their virtual workspace.*

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

Step 6: Assigning User Roles and Policies

When a user logs in to the Connection Broker, the Connection Broker searches the authentication servers 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.

LEOSTREAM						
Signed in as Administrator						
Dashboards						
Setup						
Configuration						
Pools						
Protocol Plans						
Power Control Plans						
Release Plans						
Printer Plans						
Policies						
Locations						
Roles						
Assignments						

Actions	Authentication Server Name	Domain Name	Active	Default Role	Default Policy	Position
	All	All	All			
Edit	DEV	dev.leostream.net	Yes	User	Default	2
Edit	LEOSTREAM	leostream.net	Yes	User	Default	1

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.

Edit Assignments for Authentication Server "LEOSTREAM"

Domain name
leostream.net

Assigning User Role and Policy
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	User Role	User Policy
1	[any group]	Leostream Connect	User	Multiple Resources
2	[any group]	All	User	RemoteApp
3		All	User	Default
4		All	User	Default
5		All	User	Default

[Add rows]

Default Role
User

Default Policy
Default

☐ Query for Active Directory Group information

Users will be assigned to this role if they do not match an assignment rule.

Users will be assigned to this policy if they don't match an assignment rule.

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.



*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](#).*

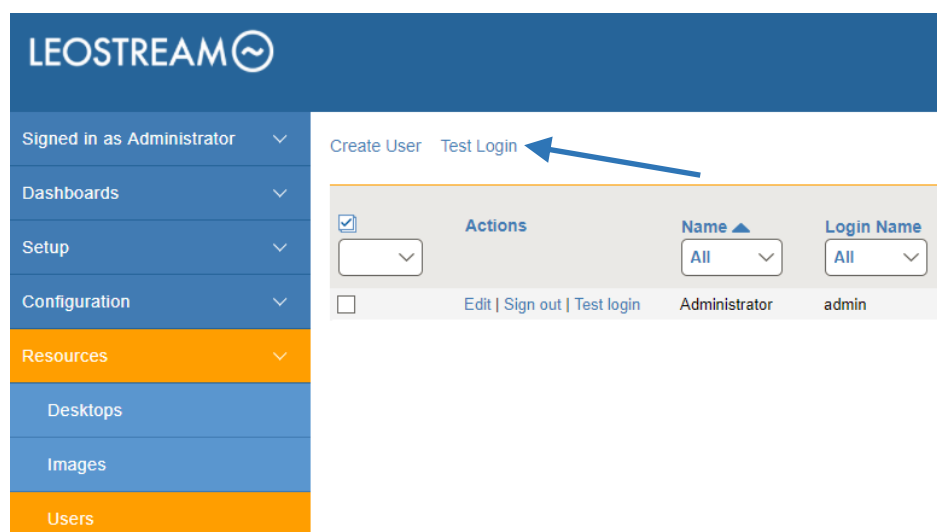
3. Assign a role to this group and client location pair by selecting an item from the **User Role** drop-down menu.
4. Assign a policy to this group and client location pair by selecting an item from the **User Policy** drop-down menu.

If you need to assign roles and policies based on a different user attributes, see “Assigning Roles and Policies Based on any Attribute” in Chapter 14 of the [Connection Broker Administrator’s Guide](#).

Step 7: Testing User Login

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** page. 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: laberie (Laura Aberle)
 Authentication server: Test authentication server
 RADIUS authentication server: disabled
 Domain: Leostream
 Client: Chrome/42.0 (Web Browser) at 172.29.229.35
 (This client is in this location: All)

Looking up user "laberie (Laura Aberle)":
 in authentication server "Test authentication server" — found user (show Active Directory attributes)
 This user's "memberOf" attribute:
 CN=Domain Users,CN=Users,DC=leostream,DC=net

Trying to match with Authentication Server Assignment rule: (edit)
 1: "memberOf" exactly matches [any group], location "All" — matched

User will have Role "Administrator" and Policy "Example Policy".

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

Policy: Example Policy (edit)

Hard-Assigned Desktops
 Protocol plan for hard-assigned desktops: Default (show details)
 No hard-assigned desktops found.


Pool "vSphere Windows Pool" (edit)
 Including pool for all users.
 Protocol plan for desktops in this pool: Microsoft RDP (show details)
 Looking for one desktop
 Policy settings for this pool:

- backup pool: All Desktops
- follow-me mode
- do not allow users to restart offered desktops
- offer powered-on desktops without a running Leostream Agent
- if not running, power on the desktop
- do not favor previously-assigned desktops
- may offer desktops with pending reboot job
- do not confirm desktop power state
- power on stopped desktops
- do not log out rogue users
- do not attempt single sign-on into desktop console session
- allow manual release
- Power control plan: Test 1
- when user disconnects, do not change power state
- when user logs out, immediately shutdown and Start
- 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 logout
- 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
- do not release if user does not log in

(70 total, 70 in service, 70 policy filtered, 70 pool filtered, 70 available, 19 running, 19 with an IP address)
 kdg-win10 — connecting via RDP (show) — available, running, Leostream Agent v6.2.1.0, will offer as: "kdg-win10"
 Leostream Agent check failed.
 Actual login will try backup pool "All Desktops".

Assignments from XenApp Services Site
 Not configured for this policy.

Offering one desktop and zero applications with this policy.

 Please complete a login test before contacting Leostream support.

The test login results show the role and policy assigned to the user, and what desktops the user will be offered

Step 8: Connecting from a PCoIP Client

When using a PCoIP zero client with Leostream and the Teradici Cloud Access Platform, ensure that you configure the client as follows.

1. Set the **Connection Type** to PCoIP Connection Manager
2. In the **Server URI** field, enter the `https` address of the PCoIP Connection Manager. Do not enter the Leostream Connection Broker address.

To connect to Leostream using a PCoIP soft or mobile client, enter the address of the PCoIP Connection Manager into the client. Do not enter the Leostream Connection Broker address.