leostream

Remote Desktop Access Platform

Using Leostream to Manage VDI in AWS EC2

Remote Access and Desktop Connection Management with Leostream

Version 2023
August 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.
For support, contact support@leostream.com. (See the Leostream Support Policy.)

Copyright

Trademarks

Patents

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

Contents

Chapter 1: Introduction

The Leostream Connection Broker makes it possible to manage virtual workstations on Amazon Web Services Elastic Compute Cloud (AWS EC2). Leostream provides the tools necessary to satisfy a wide range of use cases and maximize the utility of desktops and applications hosted in the public cloud. With the combination of Leostream and AWS, you can:

1. Provide desktops on-demand – provision virtual workspaces in minutes, preconfigured from customized images created in AWS

2. Support multi-tenancy – separate departments, customers, etc., using AWS virtual private clouds, to provide isolated networks and manage resources independently

3. Improve security – keep data off of the end user's client device, to ensure that sensitive data never leaves the cloud; leverage multifactor authentication for secure access; use the Leostream Gateway to connect users to EC2 instances in a virtual private cloud

4. Lower costs – avoid licensing fees associated with commercial VDI or DaaS stacks and pay low hourly usage fees in AWS.

A virtual desktop infrastructure leveraging Leostream can utilize a range of AWS services, as described below, allowing you to build a complete VDI solution in the cloud. This guide focuses on AWS EC2, Amazon Virtual Private Cloud, and Amazon Directory Services. For more information on using Leostream with NICE DCV, see the Leostream Guide for Using Display Protocols.

- AWS EC2 (required) provides the compute for your virtual desktop infrastructure. Leostream launches, terminates, power controls, and connects users to instances in EC2. Simplify management by using a single Connection Broker to manage instances across multiple AWS regions, or create a cluster of Connection Brokers across various regions to support a global workforce.

- NICE DCV (optional) securely connects users to EC2 instances from any device over varying network conditions, with the ability to deliver graphics-intense applications and HPC workloads. NICE DCV is available at no extra charge when used on Amazon EC2.

- AWS Relational Database Service (RDS) (optional) provides the database required to build a cluster of Leostream Connection Brokers for high availability. The Leostream Connection Broker includes a built-in PostgreSQL database for small environments and proof-of-concepts. In a production environment, or to support a large number of users, create a cluster of Connection Brokers that use a common database hosted in RDS.

   The Connection Broker database stores all of your Leostream configuration information and user login history. Leostream has no access to your sensitive information. All passwords and secret keys which are saved when creating Centers, Authentication Servers, etc. are stored encrypted in your Connection Broker database.

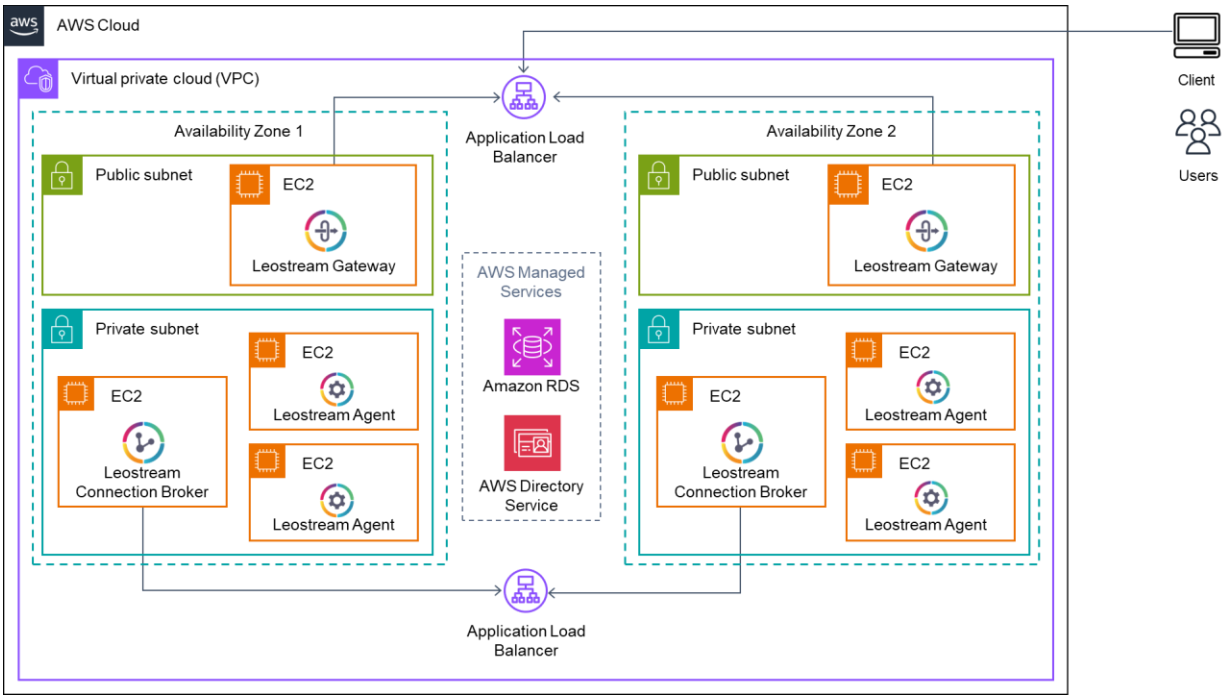
- AWS Elastic Load Balancing (optional) distributes user logins to different Connection Brokers in a cluster, to provide high availability and failover. Connection Brokers can be load balanced like any other application that uses HTTPS traffic.

- Amazon Virtual Private Cloud (VPC) (required) isolates EC2 instances in private networks. The Leostream Gateway can then be used in conjunction with the Connection Broker to provide secure access into the private network.

- Amazon Directory Services (optional) manages domain users and computers. Leostream can authenticate users and automatically join new EC2 instances to domains managed by either AWS Microsoft AD or Simple AD.

- Amazon Route 53 (optional) provides DNS load balancing and routes users to your Leostream login page.

A conceptual architectural diagram is shown in the following figure.



This document describes important aspects to consider when configuring your Amazon Web Services account for use with Leostream and describes how to configure the Leostream Connection Broker to manage capacity and user connections to compute hosted in AWS.

The document assumes a basic familiarity with AWS EC2, Amazon Virtual Private Cloud, and Amazon Directory Services concepts and use.

For an introduction to Leostream, including a description of key concepts and components, please reference the Getting Started with Leostream Concepts guide available on the Leostream web site.

If you have already configured your AWS EC2 infrastructure to support your VDI workloads, you can deploy a Leostream Proof of Concept, as described in this document, in less than a day. Additional time may be required to configure your Leostream environment to manage your specific business use cases.

For complete details on using the Leostream Connection Broker, download the Connection Broker Administrator's Guide.

Chapter 2: Configuring AWS for use with Leostream

This chapter discusses key requirements related to setting up your AWS account to use with Leostream.

Architecting Your Cloud Infrastructure

When architecting your VDI or DaaS deployment in AWS, Leostream recommends referencing the AWS Well-Architected framework. This framework includes guidelines and strategies for designing a VDI environment that satisfies the five pillars of a Well-Architected framework.

1. **Security** protects information and systems.
2. **Reliability** prevents and quickly recovers from failures.
3. **Performance Efficiency** uses computing resources efficiently, such as choosing the right instances sizes for your workloads.
4. **Cost Optimization** focuses on understanding and controlling costs.
5. **Operational Excellence** includes methods for continually improving processes and procedures.

For a complete description of the Well-Architected framework and to view the guidelines, please visit https://aws.amazon.com/architecture/well-architected/.

Defining Access Roles or Users for Your Leostream Environment

Leostream manages AWS using the AWS EC2 API. When using Leostream to manage instances in AWS, you may either attach an IAM Role to the Connection Broker instance or, if your Connection Broker is not hosted in AWS EC2, use the Access Key ID and Secret Access Key of an IAM user with the required permissions for EC2.

 Never use your AWS account root user for any Leostream operations.

Defining an Identity and Access Management (IAM) Policy for Leostream

Leostream requires only a subset of EC2 permissions to fully integrate with the AWS APIs. While you can choose to use the default `AmazonEC2FullAcess` policy, best practice is to create a new policy for Leostream that provides only the required access to EC2.

To create a new policy:

1. Go to the Identity and Access Management service in your AWS account.
2. Click on the **Policies** link in the Details Dashboard on the left.

3. Click **Create Policy**.

4. Click the **Select** button for the **Create Your Own Policy** option.

5. Enter a name in the **Policy Name** edit field, and an optional description.

6. In the **Policy Document** edit field, enter the following minimum permissions. These permissions are required for Leostream to inventory, launch, power control, terminate, and sync Leostream tags for instances in EC2.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "",
            "Effect": "Allow",
            "Action": [
                "ec2:Describe*",
                "ec2:DeleteTags",
                "ec2:CreateTags"
            ],
            "Resource": "*"
        },
        {
            "Sid": "",
            "Effect": "Allow",
            "Action": [
                "ec2:TerminateInstances",
                "ec2:StopInstances",
                "ec2:StartInstances",
                "ec2:RebootInstances"
            ],
            "Resource": "*"
        },
        {
            "Sid": "",
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": "*"
        }
    ]
}
```

   The policy above provides access to all instances in all region. Use the Resource parameter to restrict the IAM user, and therefore your Leostream Connection Broker, to certain instances, such as to a region or to instances with a certain tag. You can use the **Validate Policy** button to check if you entered the code correctly.

7. Click **Create Policy**.

Creating an IAM Role to use with Leostream

If your Connection Broker is hosted in AWS EC2, attach an IAM Role to that Connection Broker instance so it has permission to call the AWS EC2 APIs.

 If you have a cluster of Connection Brokers, you should attach an appropriate IAM Role to every Connection Broker in the cluster to optimize Leostream operation.

To create an appropriate IAM Role

1. Go to the Identity and Access Management service in your AWS account.
2. Click on the **Roles** link in the Details Dashboard on the left.
3. Click **Create role**.
4. On the **Select trusted entity** page, select **AWS service**.
5. In the **Use case** section, select **EC2**.
6. Click **Next**.
7. Search for and select either your Leostream policy or the `AmazonEC2FullAcess` policy in the **Permissions policies** section.
8. Click **Next**.
9. Enter a name in the **Role name** edit field.
10. Click **Create role**.

Adding an IAM User to use with Leostream

If you are building a hybrid environment and hosting your Connection Broker on a platform other than AWS EC2, you can use the Access Key ID and Secret Access Key of an IAM to integrate Leostream with AWS EC2.

If you plan to use an existing IAM user or group, skip to Attaching an IAM Policy to an Existing User. Otherwise, to create a new Leostream IAM user:

1. Go to the Identity and Access Management service in your AWS account.
2. Click on the **Users** link in the Details Dashboard on the left.
3. Click **Add users**.
4. In the **Specify user details** form, enter a username for your Leostream user.

5. Click **Next**.
6. Select the **Attach policies directly** option in the **Permissions options** section.
7. Search for and select either your Leostream policy or the `AmazonEC2FullAcess` policy in the **Permissions policies** section.
8. Click **Next**.
9. Review the user and click **Create user**.
10. After the user is created, click on the user's name in the list of users.
11. Click on the **Security credentials** tab.
12. In the **Access keys** section, click **Create access key**.
13. Select **Application running outside AWS** in the **Use case** section.
14. Click **Next**.
15. Optionally enter a describing tag and click **Create access key**
16. Make sure to note the **Access Key ID** and **Secret Access Key**.

     You cannot download the Secret Access Key after you leave this page. Ensure that you store your Access Key ID and Secret Access Key in a secure location for future use. You need these keys to connect Leostream to your AWS account.

17. Click **Done**.

Attaching an IAM Policy to an Existing User

To attach an IAM policy to an existing IAM user that you plan to use with Leostream:

1. Log into your AWS account as a user with full access to the Identity and Access Management service.
2. Click on the **Users** link in the Details Dashboard on the left.
3. Click on your Leostream user in the list of users.
4. When editing that user, in the **Permissions section**, select **Add Permissions** from the drop-down menu.
5. In the **Permissions options** section, select the **Attach policies directly** radio option.

6. Search for and select either your Leostream policy or the `AmazonEC2FullAcess` policy in the **Permissions policies** section.

7. Click **Next**.

8. Review your changes and click **Add Permissions**.

Setting up Security Groups

EC2 instances block all incoming traffic, by default. To ensure that the Connection Broker and desktop instances can communicate, you must create one or more security groups that open the required ports for incoming traffic. You can create a single security group to use for all components in your environment or create separate security groups for the Leostream Connection Broker and desktop instances.

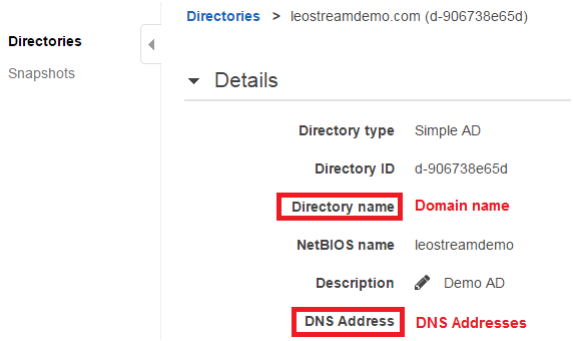
Port	Type	Required By	Purpose
22	TCP	Connection Broker	For SSH access to the Connection Broker
80	TCP	Connection Broker	For access to the Connection Broker web interface. If you close port 80 on your Connection Broker, you may omit that port from the security group.
443	TCP	Connection Broker, Leostream Gateway	For access to the Connection Broker web interface, and communication with the Leostream Agents and Leostream Connect.
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*	TCP	Leostream Agent on the AWS 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*	TCP	AWS Instances	For RDP access to the AWS VDI/DaaS instances ** If you use a display protocol other than RDP, ensure that you open any ports required by that display protocol.

Configuring a VPC

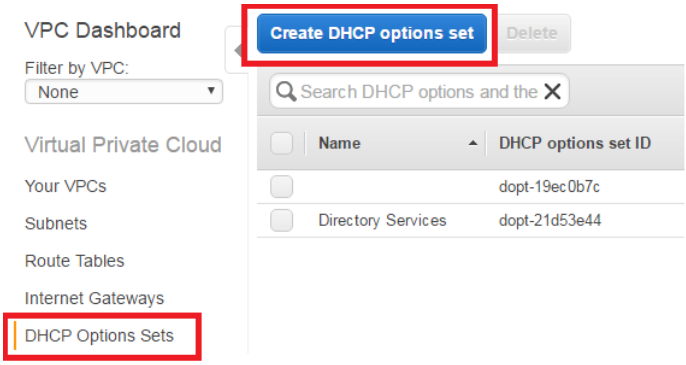
An Amazon Virtual Private Cloud (VPC) isolates EC2 instances on a virtual network within the AWS cloud, allowing you to secure and separate instances for different customers, use cases, etc. All VPC configuration must be done within the AWS Management Console. After you configure your VPCs, Leostream can launch and manage AWS instances in those VPCs.

If your VPC uses AWS Directory Services, you must create a DHCP option set that associates the **Domain name** and **Domain name servers** to the domain name and DNS addresses of your Directory Services. Any Leostream Connection Broker launched within the VPC uses the DNS information in the DHCP options set to resolve hostnames within the VPC.

To find the DNS addresses used by your Directory Services, open the Directory Services console in the AWS Management Console and click on the Directory ID for your Directory Services. The **Directory name** and **DNS Address** fields displays the domain name and DNS addresses you should use in your DHCP options set, for example:



To create a new DHCP option set, go to the **DHCP Options Set** page in the VPC service and click the **Create DHCP options set** button, highlighted in the following figure.

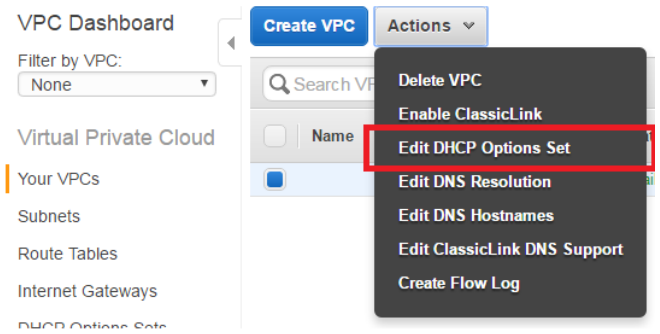


In the **Create DHCP options set** form, ensure that you complete the **Domain name** and **Domain name servers** information.

After creating the DHCP option set, you can associate it with your VPC, as follows.

1. On the **Your VPCs** page, select your VPC.

2. Select **Edit DHCP Options Set** from the **Actions** drop-down menu, for example:



3. In the **Edit DHCP Options Set** dialog, select the DHCP options set associated with your Directory Services.

4. Click **Save**.

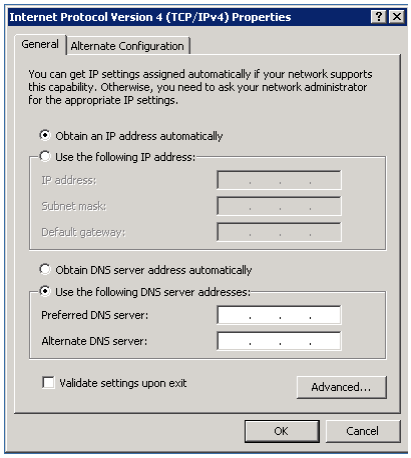
Working with AWS Directory Services

Leostream can use AWS Directory Services to authenticate users and to join new AWS instances to the associated domain. The VPC associated with the Directory Services must have a DHCP options set that associates the **Domain name** and **Domain name servers** to the domain name and DNS addresses of your Directory Services, as described in Configuring a VPC. By setting the DHCP option set, AWS automatically configures the Leostream Connection Broker instance with the appropriate network information.

In addition, in order for an AWS instance to join a Directory Services domain, the instance must point to the DNS servers used by the Directory Services. Before creating a desktop image to use in Leostream, ensure that you modify the instance's network configuration, as follows.

1. Get the DNS addresses used by your Directory Services, as described in Configuring a VPC.

2. Open the instance's **Internet Properties** dialog for the local area connection, shown in the following figure.



3. Select the **Use the following DNS server addresses** option.

4. In the **Preferred DNS server** and **Alternate DNS server** fields, enter in the primary and secondary DNS addresses used by your Directory Services.

5. Click **OK** to accept and close any open dialogs.

If you do not set the DNS addresses appropriately, the instance cannot join the Directory Services domain.

Chapter 3: Installing Leostream in AWS

You can quickly and easily install the Leostream Connection Broker using Leostream's offering in the AWS Marketplace.

Leostream currently provides AMIs based on Rocky Linux 8. For envrionments that require Red Hat Enterprise Linux 8, please see the Leostream Installation Guide for instructions on installing the Leostream components on AWS instances launched with that operating system. With the exception of this Chapter 3, the remainder of this Quick Start guide applies to Leostream versions 9.1 and 2023.

To run properly, the Connection Broker requires, at least, the following resources.

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

Leostream recommends launching the Connection Broker on a t2.large or t3.large instance type in order to adhere to the RAM requirement guidelines. The instance type used when launching the Leostream Gateway depends on your environment's requirements.

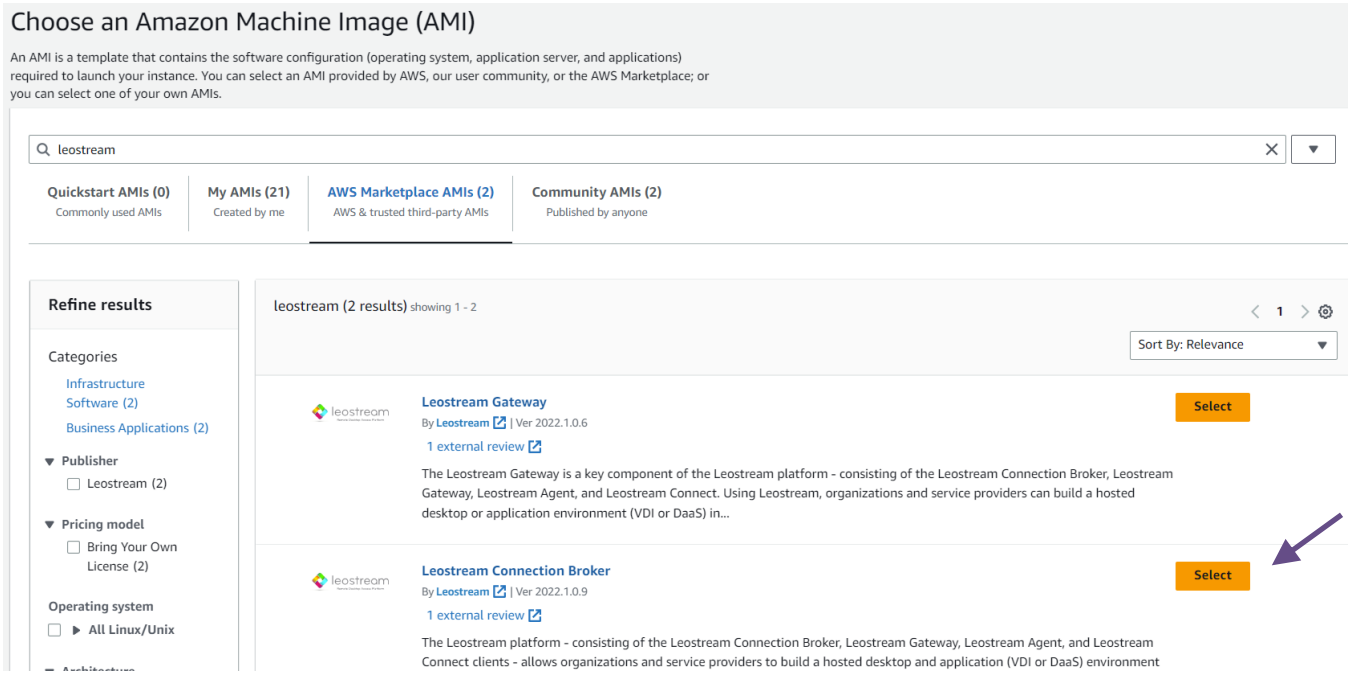
You can run the Connection Broker and Leostream Gateway on any virtual or physical machine with the required resources. If you are managing a hybrid cloud and need to install the Connection Broker on a platform outside of AWS, please consult the Leostream Installation Guide for complete instructions. The remainder of this guide covers installing the Connection Broker in your AWS account.

Launching a Connection Broker Instance

When launching a Connection Broker instance from the Leostream Connection Broker AMI in the AWS Marketplace, please adhere to the following guidelines:

1. Configure the instance name and tags according to your environment's requirements.

2. Search for an **Application and OS Images** that contains the name **Leostream.** Click the **Select** button for the Leostream Connection Broker AMI in the AWS Marketplace AMIs, shown in the following figure, then click **Continue** on the Leostream Connection Broker description dialog that opens.



3. For the **Instance type**, select a t2.large instance, or larger. Consider using a T2 Unlimited instance type to avoid CPU throttling.

4. In the **Key pair name** drop-down menu, select a key pair to use for the instance. You will need this key pair to SSH into the Connection Broker instance.

   Ensure that you rotate the SSH key used for your Connection Broker in accordance with your corporate standards for rotating SSH key pairs.

   The Linux user for SSH access to the instance console is `leostream`.

5. When configuring the **Network settings**:

   a. If you want to use the Connection Broker with an AWS Directory Services, use the **Network** drop-down menu to place the Connection Broker in the same VPC as the AWS Directory Services.

      The Connection Broker must be in the same VPC to communicate with the Directory Services. Also, ensure that the VPC's DHCP option set is configured to use the domain and DNS servers associated with the Directory Services (see Configuring a VPC.)

   b. The Connection Broker must be able to communicate with the Leostream Agents installed on your AWS instances. Therefore, place the Connection Broker in the VPC where you will host your desktops, or ensure your configuration supports Leostream Agent communication.

c. You must be able to access the Connection Broker Administrator Web interface to configure your Leostream environment, but you do not need to assign a public IP address to your Connection Broker to do so. The Leostream Gateway provides access to Connection Brokers that are isolated in a private network. See "Forwarding Connection Broker Logins through the Gateway" in the Leostream Gateway Guide for complete instructions.

a. The Leostream AMI suggests a security group with the following rules.

Type	Protocol	Port Range	Source
HTTPS	TCP	443	0.0.0.0/0
HTTP	TCP	80	0.0.0.0/0
SSH	TCP	22	0.0.0.0/0

These rules provide SSH, HTTP, and HTTPS access to the Connection Broker instance. If you want to restrict the Connection Broker to only HTTPS, remove the inbound rule for port 80. To limit SSH access, you can restrict the source to the IP address range of your clients.

6. In **Configure storage**, allocate at least 20 GB of storage to the Connection Broker.

7. Configure any **Advanced details** as required by your environment then click **Launch instance**.

Attaching an IAM Role to your Connection Broker

Before you can create a center in Leostream to manage your AWS EC2 environment, attach the IAM Role you defined for Leostream to your Connection Broker instance.

If you have a cluster of Connection Brokers, you should attach an appropriate IAM Role to every Connection Broker in the cluster to optimize Leostream operation.

1. Go to the EC2 service console in your AWS account.

2. Select your Connection Broker instance.

3. From the **Actions** drop-down menu, select **Security > Modify IAM role**.

4. Search for and select the IAM Role to use with Leostream from the **IAM role** drop-down menu.

5. Click **Update IAM role**.

Upgrading the Leostream Connection Broker

After launching your Connection Broker instance, update the underlying operating system and Connection Broker to the latest version.

To upgrade your Connection Broker, download the latest RPM file from the Leostream Downloads page, found at:

https://license.leostream.com/download.html

Ensure that you have your Leostream Serial Number and the email addresses associated with it, in order to log into the Leostream Downloads page.

Do not uninstall or stop your existing Connection Broker before performing the upgrade.
After downloading the latest RPM from the Leostream Downloads page, copy the file to your Connection Broker instance and run the following commands from the instance's terminal.

```
sudo dnf update
sudo dnf -y install RPM-FILE-NAME
sudo /sbin/reboot
```

If, at any time, you need to check the status of your Leostream Connection Broker, point a Web browser at the following URL, which will replay with `CB_IS_OKAY` if your Connection Broker is functioning nominally.

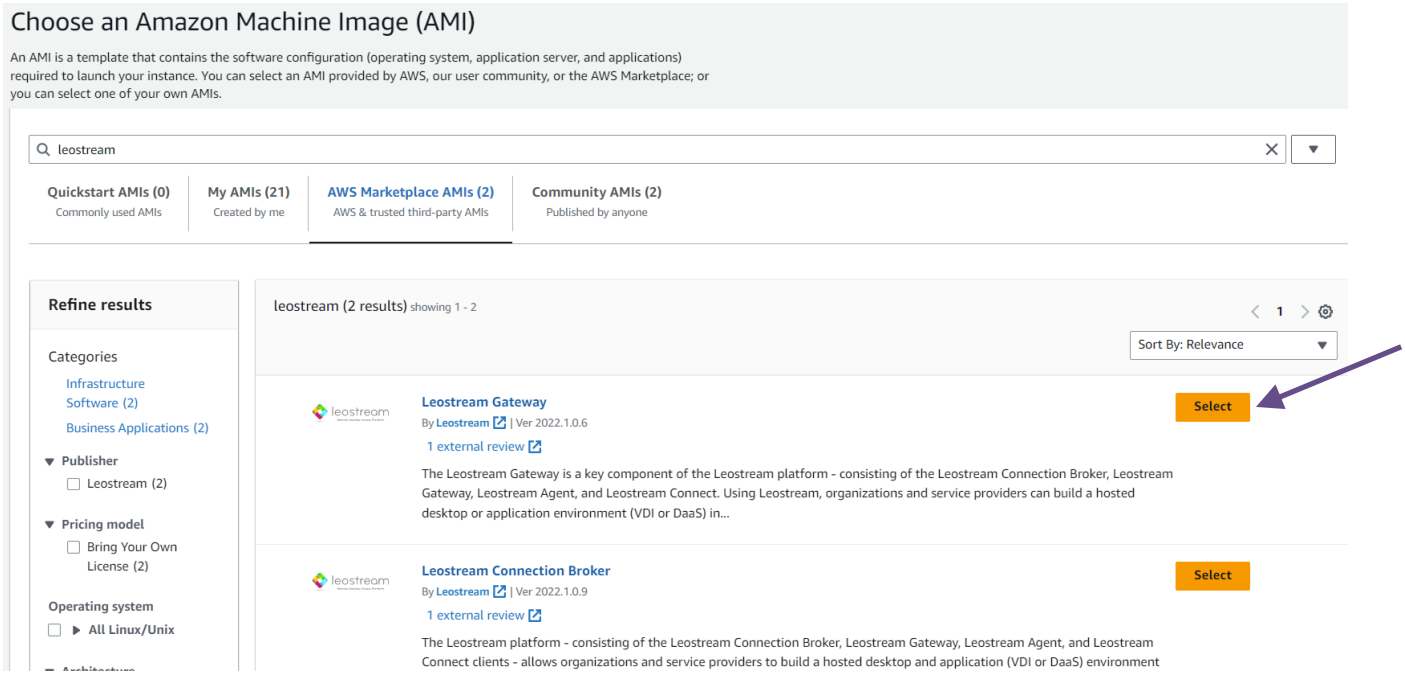
```
https://CB_ADDRESS/index.pl?action=is_alive
```

Launching a Leostream Gateway Instance

When launching a Leostream Gateway instance using the Leostream Gateway AMI in the AWS Marketplace, please adhere to the following guidelines:

1. Configure the instance name and tags according to your environment's requirements.

2. Search for an **Application and OS Images** that contains the name **Leostream.** Click the **Select** button for the Leostream Gateway AMI in the AWS Marketplace AMIs, shown in the following figure, then click **Continue** on the Leostream Gateway description dialog that opens.



3. For the **Instance type**, ensure you choose the appropriate instance type based on the size of your environment. Leostream recommends at least 4GB of RAM and 2 or more CPUs.

   The number of user connections that can be handled by the Leostream Gateway is determined by two key factors, the number of available ports for forwarding display protocol traffic and the amount of CPU. Ensure that you choose an instance type with adequate CPU, particularly if you are connecting users to their desktops with a high-performance protocol such as Mechdyne TGX.

4. In the **Key pair name** drop-down menu, select a key pair to use for the instance. You will need this key pair to SSH into the Leostream Gateway instance.

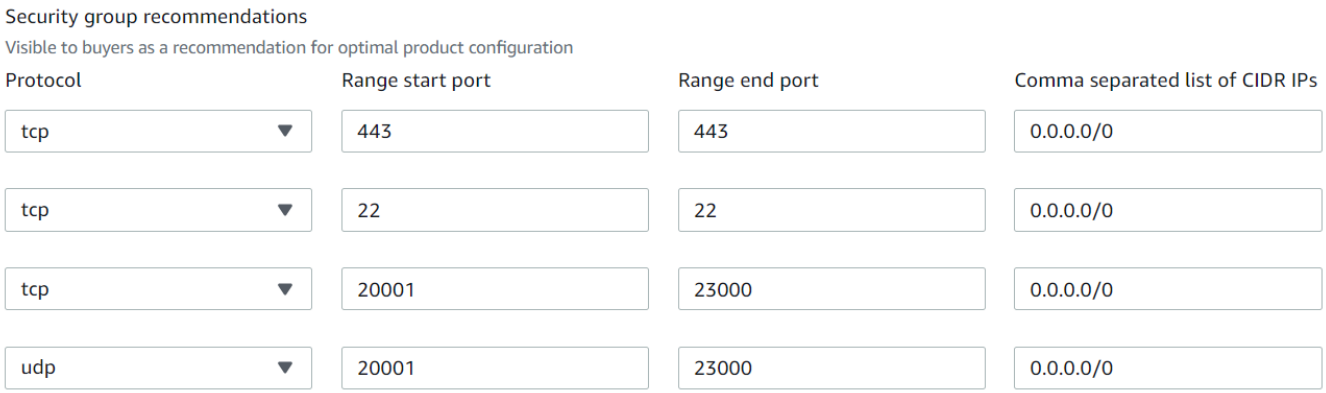
   Ensure that you rotate the SSH key used for your Leostream Gateway in accordance with your corporate standards for rotating SSH key pairs.

   The Linux user for SSH access to the instance console is `leostream`.

5. When configuring the **Network settings**:

   a. The Leostream Gateway must have network access to your AWS instances and must be reachable by the end user's client. Typically, that means locating the Leostream Gateway in the public network of the VPC that contains your instances and assigning an Elastic IP address to the gateway instance.

   b. The Leostream Gateway AMI suggests a security group with the following rules.



These rules provide SSH and HTTPS access to the Leostream Gateway instance, and open the default random port range required to forward client-based display protocol traffic. Add or modify the security group rules related to display protocol traffic based on the types of display protocols you plan to use and the forwarding rules you configure in your Leostream Connection Broker.

6. In **Configure storage**, allocate at least 20 GB of storage to the Leostream Gateway.

7. Configure any **Advanced details** as required by your environment then click **Launch instance**.

After launching your Leostream Gateway instance, update the underlying operating system and Leostream Gateway by running the following commands from the instance's terminal.

```
sudo dnf update
sudo dnf update leostream_gateway
```

If you need to use the Leostream Gateway to access your Connection Broker login page, SSH into the Leostream Gateway instance as a user with `sudo` privileges and execute the following command:

```
sudo leostream-gateway --broker <your-broker-private-IPaddress>
```

If, at any time, you need to check the status of your Leostream Gateway, point a Web browser at the following URL.

```
https://<your-gateway-address>/app/system/ping
```

Obtaining Your Leostream License

Leostream uses a BYOL model in AWS, purchased as an annual subscription either from Leostream or an approved reseller. After installing your Connection Broker, you must obtain your Leostream license key. Your Connection Broker license is derived from the serial number you received from Leostream Sales and indicates either the number of named users or AWS instances (desktop resources) you may manage within Leostream. If you did not receive your Leostream serial number, please contact sales@leostream.com.

You can generate the license key from the Connection Broker Administrator web interface if your Connection Broker has internet access, as follows.

1. Enter https://<broker-or-gateway-address> in your Web browser's URL edit field, depending on if you can access your Connection Broker or if you are using the Leostream Gateway to forward traffic. The Connection Broker **Sign In** page opens.

2. Sign into the Connection Broker Web interface using the following default credentials:

   - **User name**: admin
   - **Password**: leo

3. Click **Sign In**. The **Leostream license** page opens.

4. Select **Enter manually** from the **How do you want to enter your license key** drop-down menu.

5. If your Connection Broker has internet access, click the link to go to:

   `https://license.leostream.com`.

   The installation code for your Connection Broker is automatically populated. If your Connection Broker does not have internet access, note the **Installation code** to the right of the form and navigate to the Leostream license server from a device with internet access.

6. In the **Leostream license key generator**, enter the Serial number you received from Leostream. If you do not have a Leostream Serial number, contact sales@leostream.com.

7. If the **Installation code** is not automatically populated, enter the Installation code listed on your Connection Broker.

8. In the **Email address** form, enter your email address.

9. Click **Generate a license**.

10. If you navigated to the Leostream license generator from your Connection Broker, click **Apply to the broker** to copy the new license key into your Connection Broker. Otherwise, copy the key into a text file.

11. Back on your Connection Broker **Leostream License** form, enter the license key you obtained from the Leostream license generator. Ensure that you include the BEGIN and END lines.

12. Click on the **License Agreement** link to view the end user license agreement. Select the **I have read and accept the License Agreement** option if you agree to the terms of the Leostream end user license agreement.

13. Click **Save**. The **Welcome** page opens, giving you the option to check for any Connection Broker updates.

Chapter 4: Preparing AWS Instances and Images

Leostream can manage connections to existing Windows and Linux AWS instances, and can provision new AWS instances from existing AWS images, or AMIs. All instances manage by Leostream should have an installed Leostream Agent that can communicate with the Connection Broker. The Leostream Agents are available on the Leostream Product Downloads page. The Leostream Installation Guide contains complete instructions for installing the Leostream Agent.

During installation, you can specify the address of the Connection Broker that manages the instance. If the Connection Broker and instance are in the same VPC, you can point the Leostream Agent at the Connection Broker's private IP address. Otherwise, to ensure proper communication between the Connection Broker and Leostream Agents, use the Connection Broker public or elastic IP.

After the Leostream Agent is installed, you can use the **Test** button on the Leostream Agent Control Panel dialog to ensure that the Leostream Agent can contact the Connection Broker. To test if the Connection Broker can contact the Leostream Agent, go to the **> Resources > Desktops** page in the Connection Broker Administrator Web interface and click the **Status** link associated with the instance's record in the Connection Broker. Communication must work in both directions to use all Leostream functionality.

If you plan to use Leostream to provision new instances in AWS, and to have Leostream join the new instances to your Directory Services domain, please adhere to the following guidelines.

- 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.

After you create an image from an instance following the previous guidelines, you can configure Leostream pools that automatically provision new capacity in AWS (see Chapter 6: Pooling and Provisioning in AWS.)

Chapter 5: Integrating with Your AWS Infrastructure

In the **Setup** section of the Connection Broker Administrator Web interface, you integrate Leostream with the other components of your hosted desktop environment, such as your Amazon Directory Services and your AWS regions.

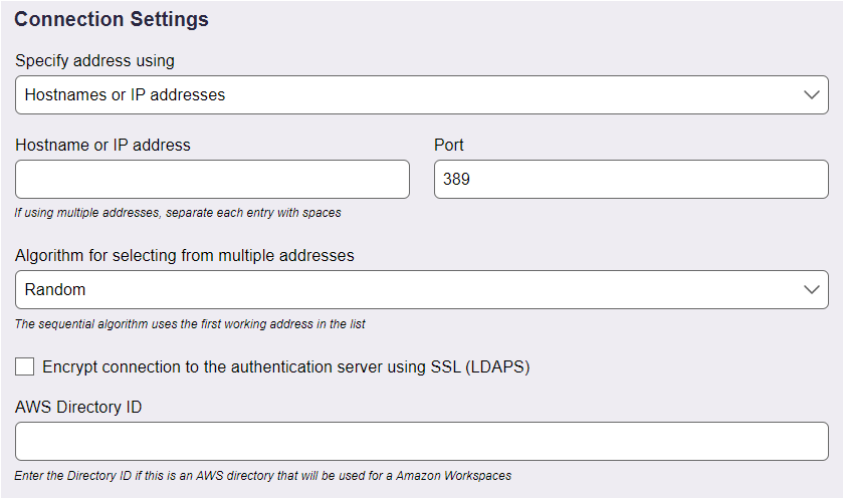
The **Setup** section is also used to integrate your Connection Broker with the Leostream Gateway. Note that this Quick Start guide does not cover using the Leostream Gateway. For more information on configuring your Connection Broker to work with the Leostream Gateway, see the Leostream Gateway Guide.

The Leostream Gateway may be required if your desktop instances are located in a VPC and not given publicly accessible IP addresses.

Connecting to Your Amazon Directory Services

To authenticate users with Amazon Directory Services, or other Microsoft Active Directory server, you must first register that domain with your Connection Broker, as follows.

1. Go to the **> Setup > Authentication Servers** menu.
2. Click the **Add Authentication Server** link.
3. In the **Add Authentication Server** form, enter a name for this server in the Connection Broker in the **Authentication Server name** edit field.
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.



   a. Select **Active Directory** from the **Type** drop-down list.

b. From the **Specify address using** drop-down menu, select **Hostname or IP address**.

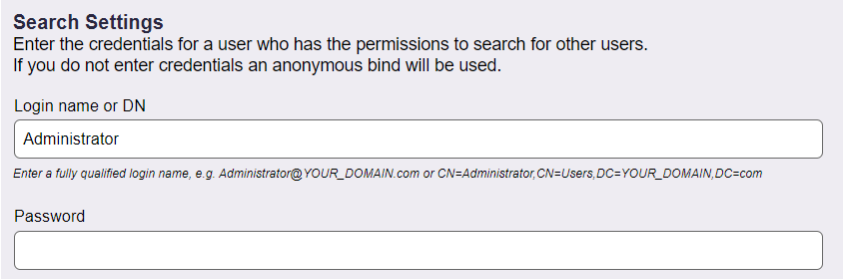
c. Enter the authentication server hostname or IP address in the **Hostname or IP address** edit field.

d. Enter the port number in the **Port** edit field.

e. Check 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.

f. The **AWS Directory ID** is not required to work with AWS EC2. Complete this field only if you plan to also manage Amazon WorkSpaces Core with Leostream.

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.



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**.

You do not need to load users into your Leostream environment prior to their first login. Instead, when a user logs in for the first time, the Connection Broker creates a record for that user in your Leostream database. Leostream does not store user password, but does store other user information that may be considered sensitive, such as personally identifiable information (PII). Ensure that you protect your Leostream database using your standard corporate procedures for databases that contain PII.

Connecting to Your AWS EC2 Regions

In order to manage EC2 instances in AWS, you need to create an Amazon Web Services center in your Leostream 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.

You can currently create centers for the following AWS regions:

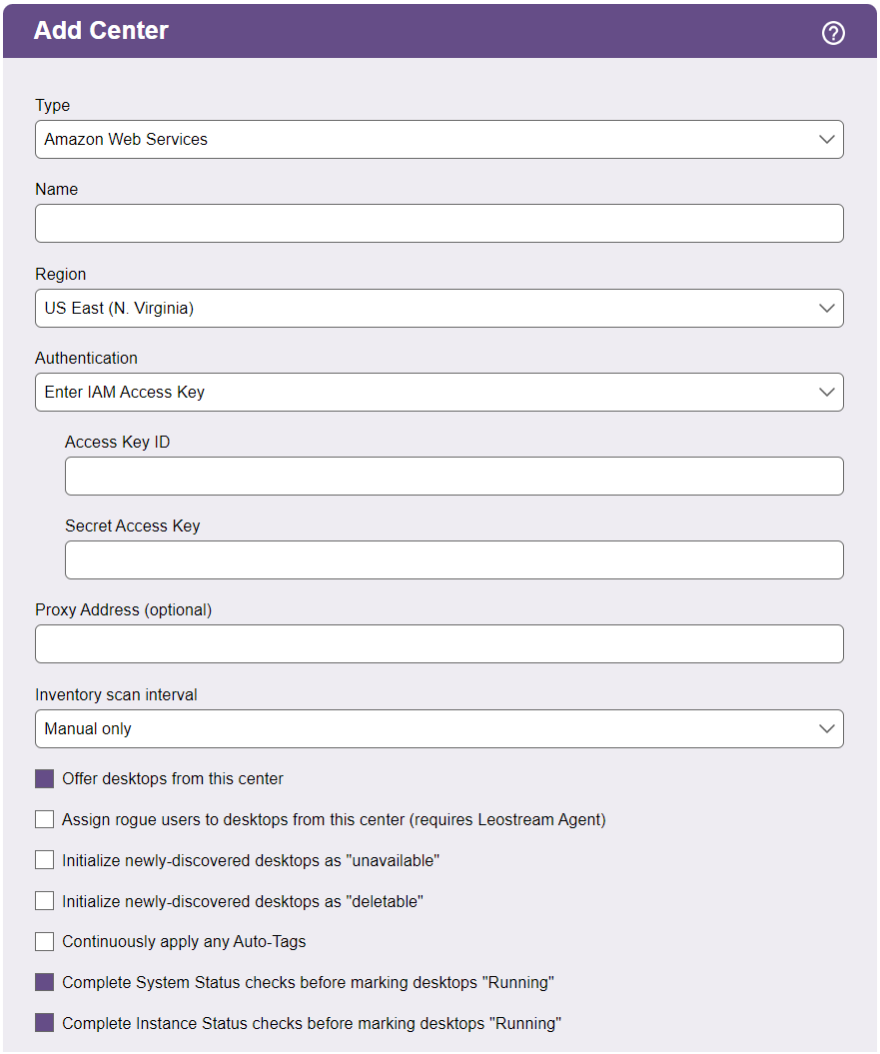
- US East (N. Virginia)
- US East (Ohio)
- US West (N. California)
- US West (Oregon)
- Africa (Cape Town)
- Asia Pacific (Hong Kong)
- Asia Pacific (Jakarta)
- Asia Pacific (Mumbai)
- Asia Pacific (Osaka-Local)
- Asia Pacific (Seoul)
- Asia Pacific (Singapore)
- Asia Pacific (Sydney)
- Asia Pacific (Tokyo)
- Canada (Central)
- EU (Frankfurt)
- EU (Ireland)
- EU (London)
- EU (Milan)
- EU (Paris)
- EU (Stockholm)
- Middle East (Bahrain)
- South America (São Paulo)
- China (Beijing)
- China (Ningxia)

For certain regions, such as Boston and Los Angeles, local zones are supported. 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. The **Add Center** form updates to display the fields shown in the following figure.



4. Enter a name for the 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. If your Connection Broker is installed on an AWS EC2 instance, you can use the **Authentication** drop-down menu to indicate how the Connection Broker authenticates against the AWS API.

   Select **Use attached IAM role** if your Connection Broker EC2 instance has an attached IAM role with appropriate permissions. Otherwise, select **Enter IAM Access Key** and enter the following information. If your Connection Broker is not installed in EC2, the **Authentication** drop-down menu is not available and you must specify the **Access Key ID** and **Secret Access Key**, as follows.

   a. 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.

   b. Enter the secret key associated with your access key into the **Secret Access Key** field.

7. If access to your AWS account must go through a proxy server, specify its address in the **Proxy Address (optional)** edit 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.

   If you are launching EC2 instances and creating new AMIs in the AWS Management Console, the Connection Broker finds these new items when the next refresh interval occurs.

9. Select the **Continuously apply any Auto-Tags** option to have the Connection Broker create Tags in AWS for the instances inventoried from this center. The Connection Broker creates tags in AWS for each Leostream Tag associated with the instance. See Tagging AWS Instances and Volumes for complete instructions.

10. Click **Save** to create the center.

All instances in all availability zones 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.

If you need to support a multi-region deployment, repeat the previous procedure to create a center for each region.

Chapter 6: Pooling and Provisioning in AWS

After you create your centers and the Connection Broker inventories your desktops, you 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 virtual machines in AWS EC2
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 AWS, 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 AWS region 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:

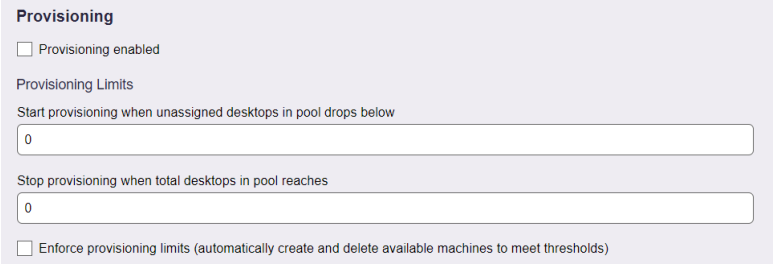
1. Go to the **> Configuration > Pools** page.
2. Click the **Create Pool** link. The **Create Pool** form opens.
3. Enter a name for the pool in the **Name** edit field.
4. In the first row of the **Desktop Attribute Selection** section:
    a. Select **Name** from the **Desktop attribute** drop-down 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 AWS center, see the "Creating Desktop Pools" chapter in the Connection Broker Administrator's Guide.

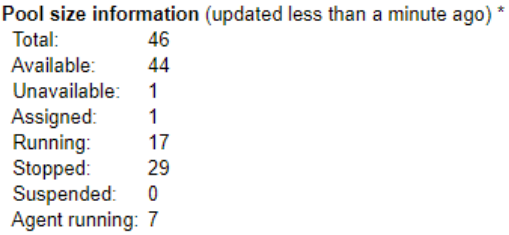
Provisioning New Instances

Your Leostream 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.

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. To begin, check the **Provisioning enabled** checkbox, as shown in the following figure.



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:



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.

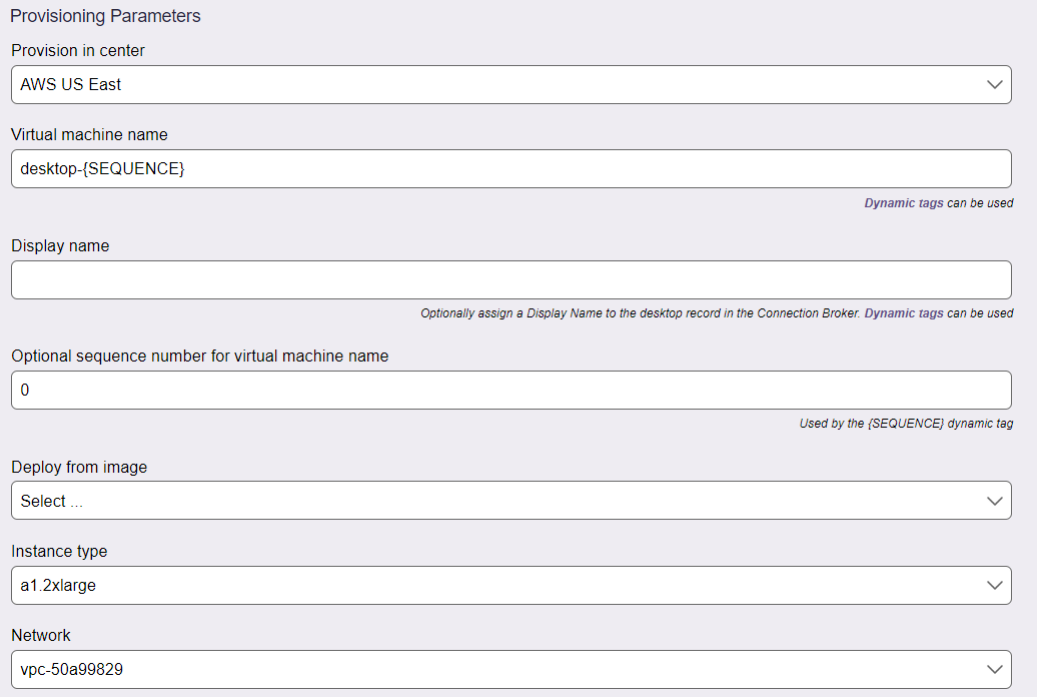
The Connection Broker checks the provisioning limits, and creates new instances, at the following times

- 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 AWS.

1. Select the AWS 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 a portion of the **Provisioning Parameters** section.



2. Enter a name for the virtual machine in the **Virtual machine name** edit field. If the pool is defined as instance 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 image to use from the **Deploy from image** drop-down menu. This menu contains all the AMIs available in your account in the AWS region associated with the selected center.

6. Select the instance size from the **Instance type** drop-down menu.

7. If you chose a T2 instance type, select the **Enable T2 Unlimited** option to indicate the instance is allowed to burst beyond its baseline CPU usage.

8. Select the VPC from the **Network** drop-down menu.

   If you add the instance to a VPC that does not provide public IP addresses, you can use the Leostream Gateway to connect clients that are outside of the private network. See the Leostream Gateway Guide for more information.

9. Indicate the Availability Zones where the Connection Broker should attempt to locate new instances by moving AZs from the **Available subnets/Availability Zones** list to the **Selected subnets/Availability Zones** list.

   Every time the Connection Broker needs to provision a virtual machine, it attempts to place it in the first Availability Zone in the list. If that Availability Zone no longer has capacity to provision an instance of the selected type, the Connection Broker looks through the remaining Availability Zones to find capacity. If the Connection Broker cannot find capacity in any of the selected Availability Zones, provisioning is disabled for the pool

10. Select the security group to assign to the instance from the **Security group** drop-down menu.

11. In the **IAM Instance Profile name** edit field, optionally enter the name of an IAM instance profile to attach to the provisioned instances. If you created your IAM role using the console, the instance profile has the same name as your IAM role.

12. Select the **Initialize newly provisioned desktops as deletable** option to indicate that the Connection Broker is allowed to delete this VM from disk. 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, by default. Use release plans to schedule VM deletion.

    For more information on using release plans to terminate AWS instances, see the example on deleting virtual machines in the “Release Plans” section of Chapter 10 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 at the top of the **Provisioning** section.

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. Typical errors to look for include:

- Your AWS account has reached its quota for the selected instance type
- The instance type is not available in your AWS region

If provisioning fails due to an issue with the AWS API that the Connection Broker is using, the Connection Broker does not disable provisioning. In these cases, the Connection Broker retries the provisioning command, until the AWS APIs become responsive.

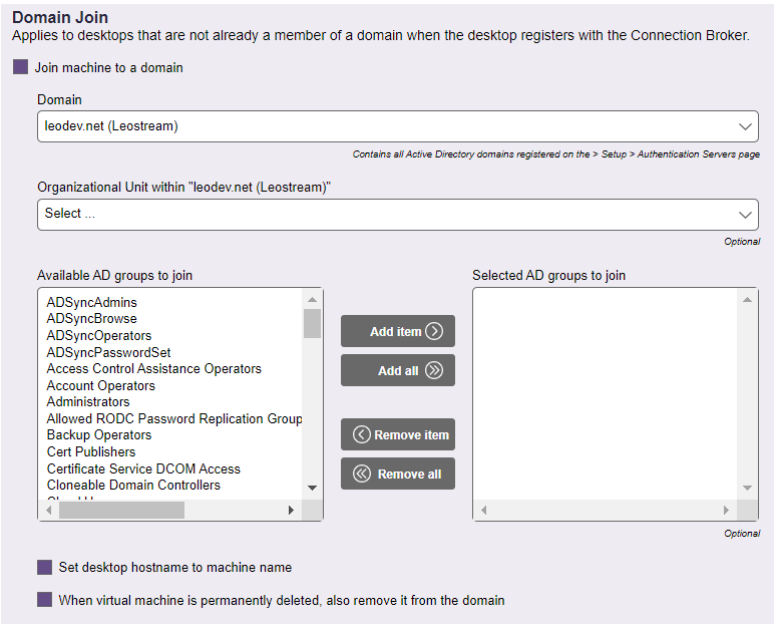
Joining Instances to a Domain

You can use Leostream to join AWS instance to a domain, include Amazon Directory Services. 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.

You 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.



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.

Tagging AWS Instances and Volumes

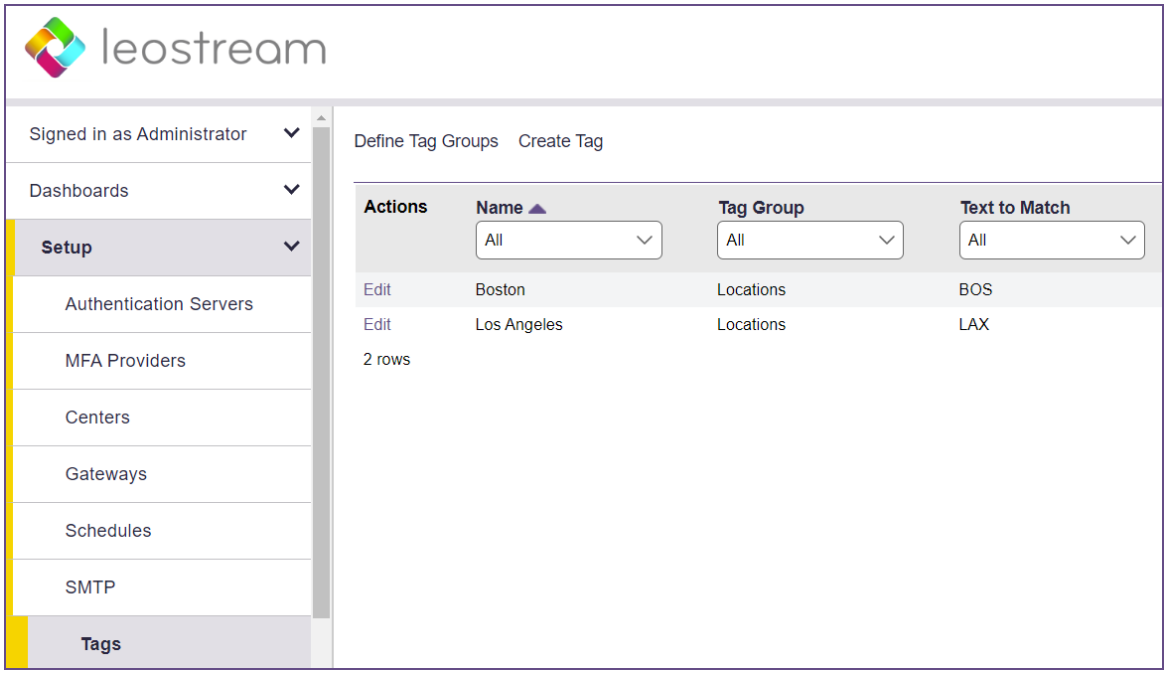
When provisioning new instances in AWS, the Connection Broker automatically tags each instance and its volume in the AWS Management Console with a `Name` tag that contains the instance name. The Connection Broker can create and associate up to four additional AWS tags with any instances provision into or inventoried from an Amazon Web Services center. To tag instances:

1. Select the **Continuously apply any Auto-Tags** option in your AWS center (see Connecting to Your AWS EC2 Regions).

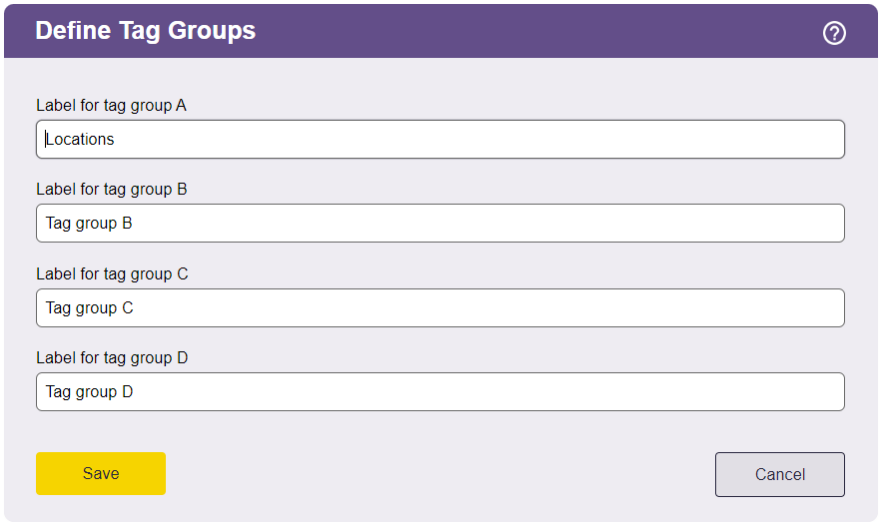
2. Create Leostream tags with auto-tag rules that match your desktop naming scheme, as described in the remainder of this section.

When the Connection Broker provisions or discovers new instances in your AWS center and those instances match any auto-tagging rules, Leostream automatically assigns the Leostream tag to the instance and creates and associates an AWS tag to the instance in the AWS Management Console.

The Leostream tag group name becomes the **Key** name in AWS. The Leostream tag name becomes that key's **Value** in AWS. To define the tag group names and tags, go to the **> Setup > Tags** page, shown in the following figure.



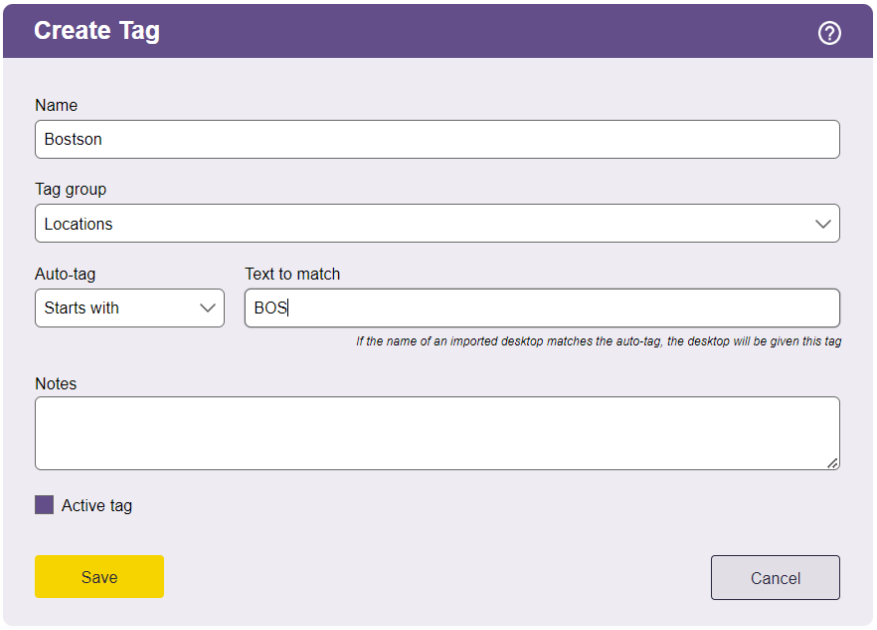
Click the **Define Tag Groups** link at the top of the page to open the **Define Tag Groups** form, shown in the following figure.



In the **Label for tag group** edit fields, enter the string to use for the tag key in AWS. Keys in AWS can have a maximum of 127 characters. For example, the previous figure creates a `Locations` tag key.

Each Leostream tag group must have a label. However, the Connection Broker does not tag the instance in AWS if the Leostream tag group does not contain any tags or if the instance does not match any auto-tagging rules for tags in that group.

After labelling your tag groups, create tags in each of the groups by clicking the **Create Tag** link on the **> Setup > Tags** page. The **Create Tag** form opens, shown in the following figure.



The string entered in the **Name** edit field is the value for the tag key selected in the **Tag group** drop-down menu. The tag is applied to any instance that satisfies the auto-tagging rule defined in the **Auto-tag** drop-down menu.

To decide if an auto-tagging rule applies to a desktop, the Connection Broker matches the value entered in the **Text to match** field against the value shown in the **Name** column on the Connection Broker **> Resources > Desktops** age. For example, in the previous figure, the tag key `Location` is given the value `Boston` for any instance with a name that starts with `BOS`.

Chapter 7: Connecting Users with DCV

After you define your desktops pools, create rules that control how the Connection Broker manages the user's connection to the desktops in those pools, including how long the user retains access to a particular desktop and how they connect to it.

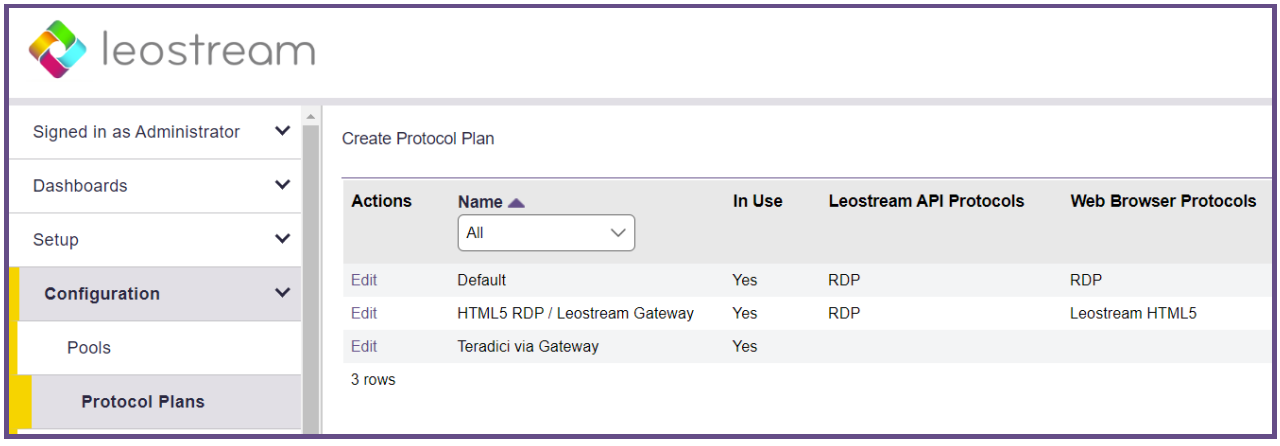
*The Leostream Connection Broker defines a **pool-based plan** as a set of rules that determine how the Connection Broker manages the connection to a desktop in a pool. This step describes three types of pool-based plans. 1) Protocol, 2) Power Control, and 3) Release. The Connection Broker also provides **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.*

Leostream supports a wide range of display protocols and you can mix and match display protocols, to provide the appropriate level of performance for each user based on their tasks at hand. When connecting users to instances in EC2, you can leverage the NICE DCV high performance display protocol to connect users to their EC2 instances at no additional charge. Leostream supports both client-based and in-browser NICE DCV connections, with or without the Leostream Gateway.

The remainder of this chapter focuses on how to use Leostream with NICE DCV. For information on other display protocols, consult the Leostream Display Protocol Guide.

Overview of 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.



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.

Chapter 8: Offering Desktops to Users

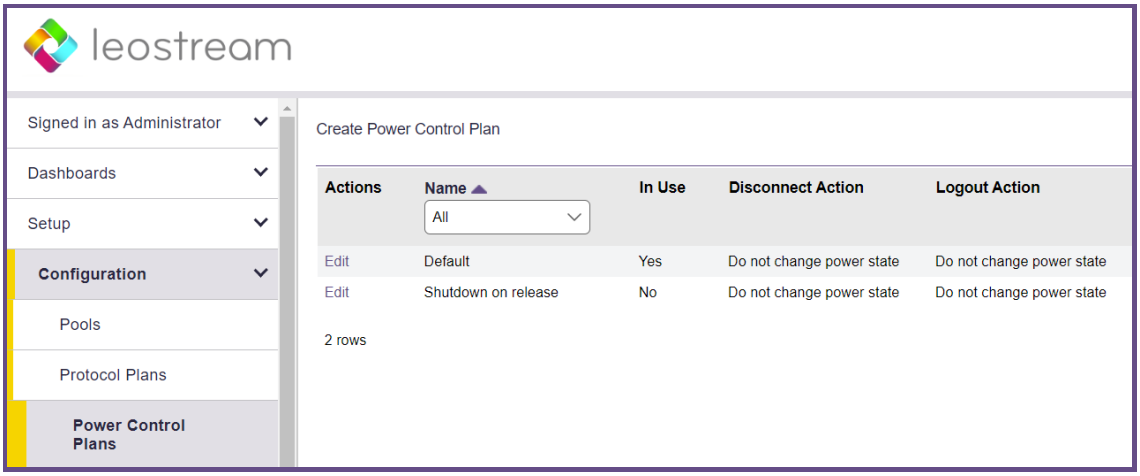
Power Control Plans

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

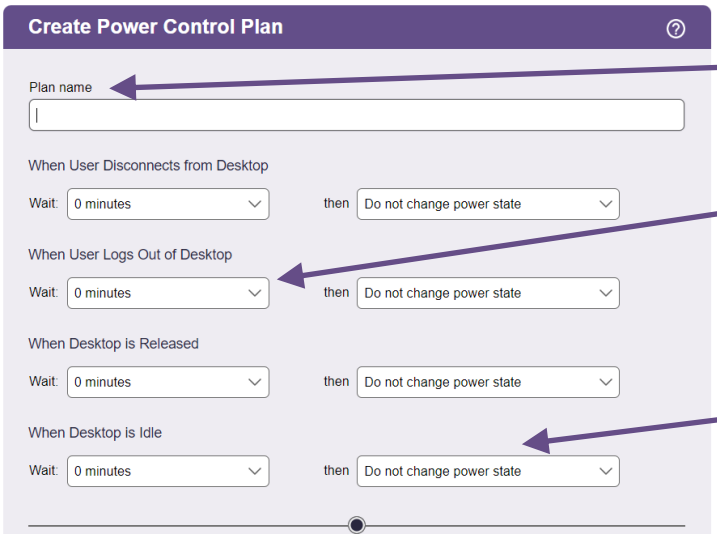
The remote desktop must have an installed and running Leostream Agent to allow the Connection Broker to distinguish between user logout and disconnect and to perform actions based on idle time.

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.

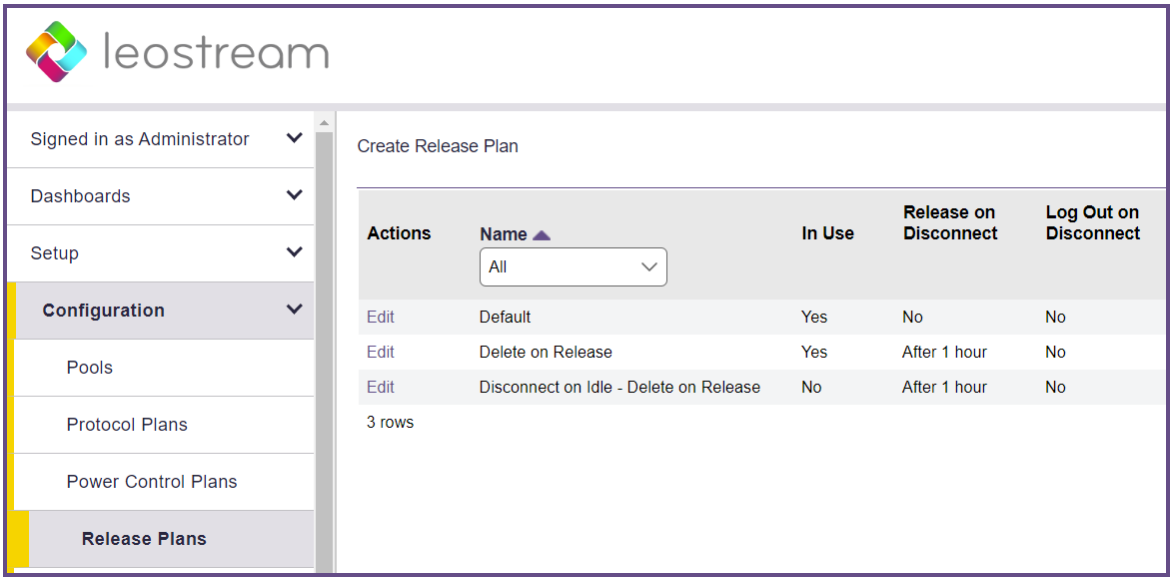
2. Enter a unique name for the plan in the **Plan name** edit field.
3. For each of the remaining sections:
    a. From the **Wait** drop-down menu, select the time to wait before applying the power action.
    b. From the **then** drop-down menu, select the power control action to apply. Selecting **Do not change power state** renders the setting in the **Wait** drop-down menu irrelevant, as no action is ever taken.
4. 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.

---

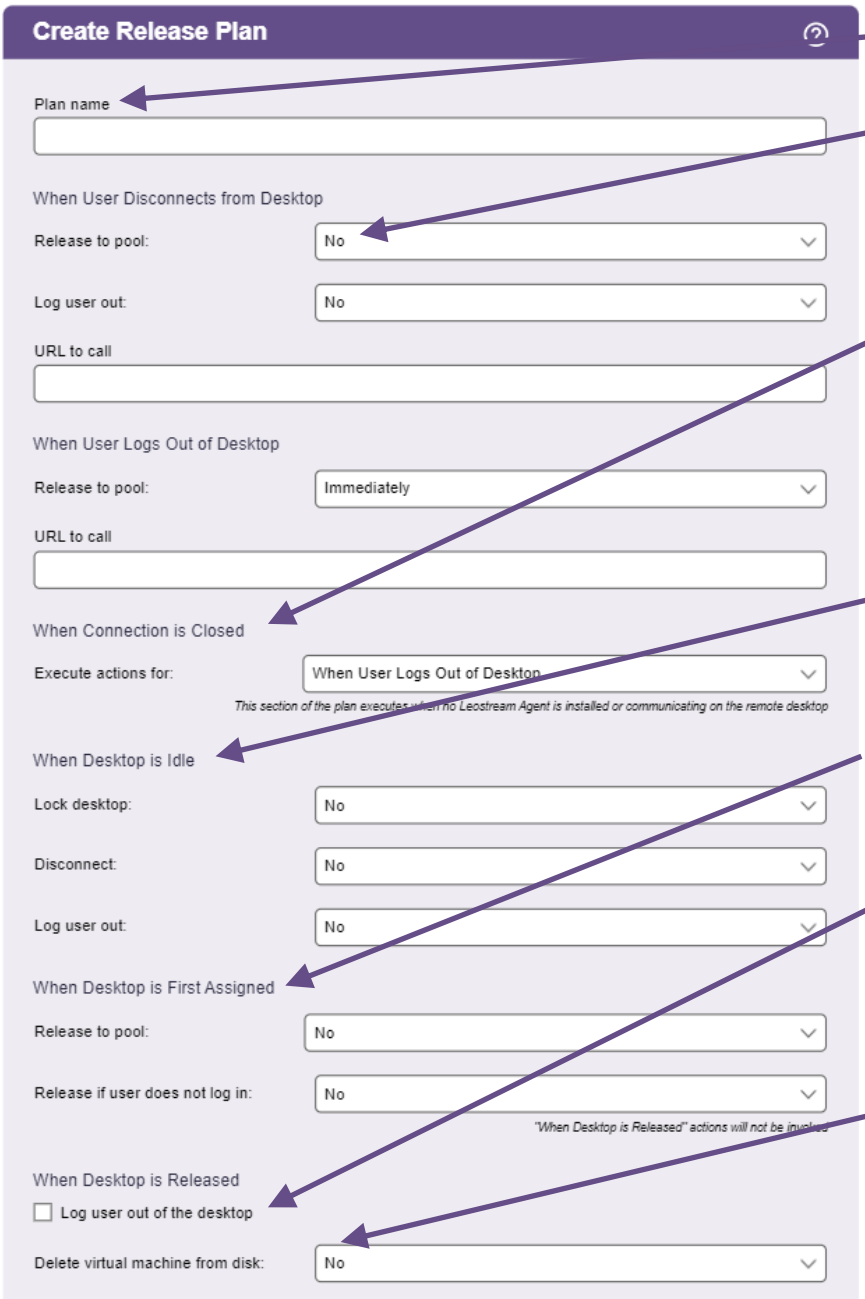
*When a desktop is **assigned** to a user, the Connection Broker always offers that desktop to that user, regardless of where the user logs in, and to no other users. Desktops can be policy-assigned or hard-assigned. For a description of hard-assigned desktops, see the Connection Broker Administrator's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



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.

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

1. Click the **Create Release Plan** link on the **> Configuration > Release Plans** page. The **Create Release Plan** form, shown in the following figure, opens. The figure describes additional use cases you can model using Release Plans.



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. 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.

4. Click **Save**.

When using 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 to its pool and removes the user's desktop assignment.

For more details on creating and using release plans, see the "Release Plans" section in Chapter 10 of the Connection Broker Administrator's Guide.

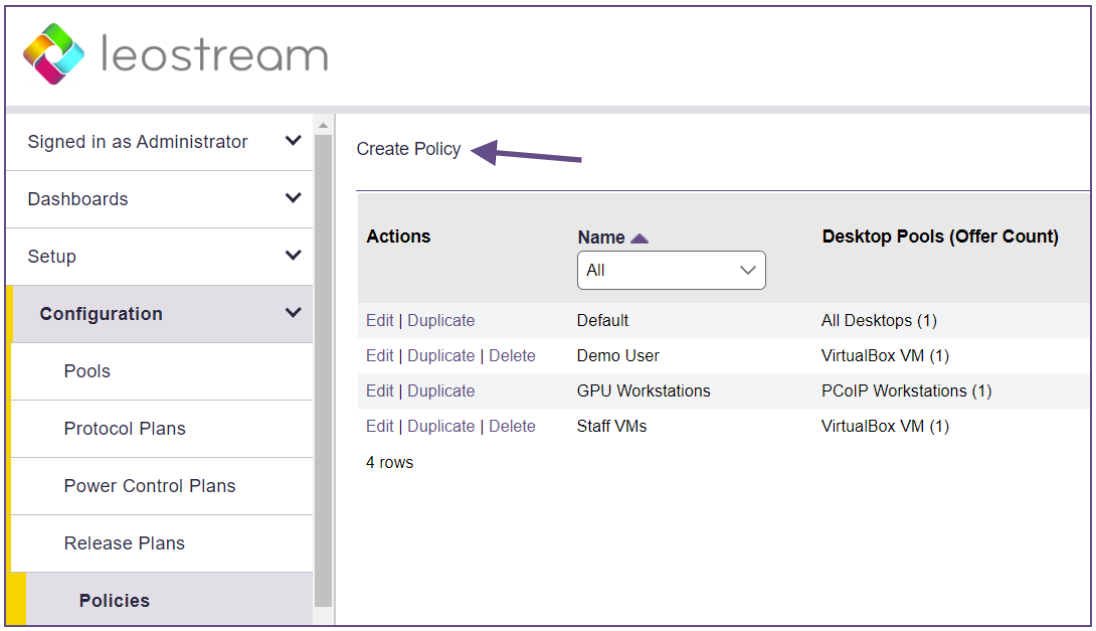
Building User Policies

After you define your pools and plans, build policies.

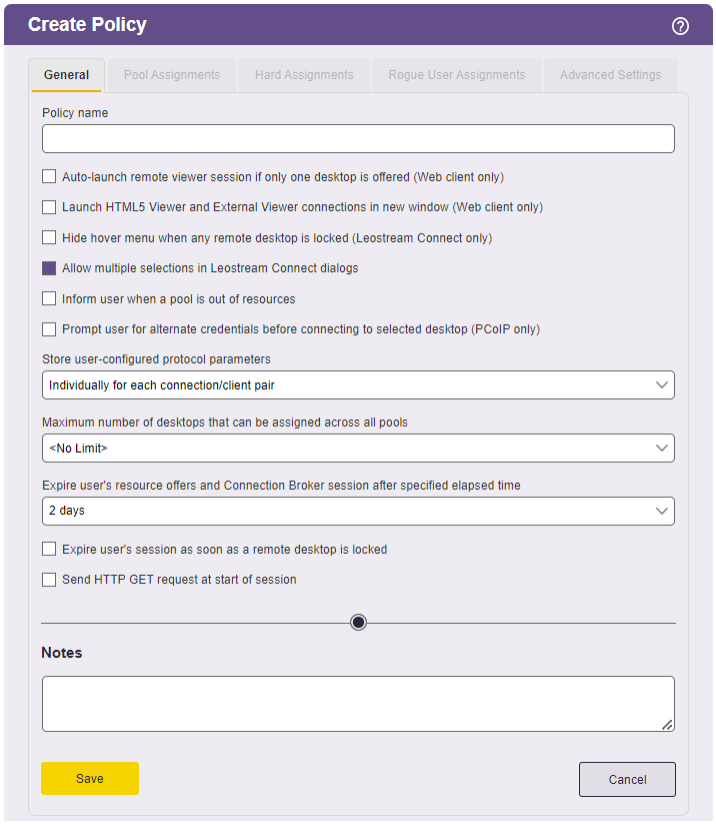
*The Leostream Connection Broker defines a **policy** as a set of rules that determine which pools to offer desktops from, which display protocol to use to connect to those desktops, which power control and release plans to apply to those desktops, which USB devices the user can access in their remote 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 **Create Policy** form, shown in the following figure, opens.



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**.

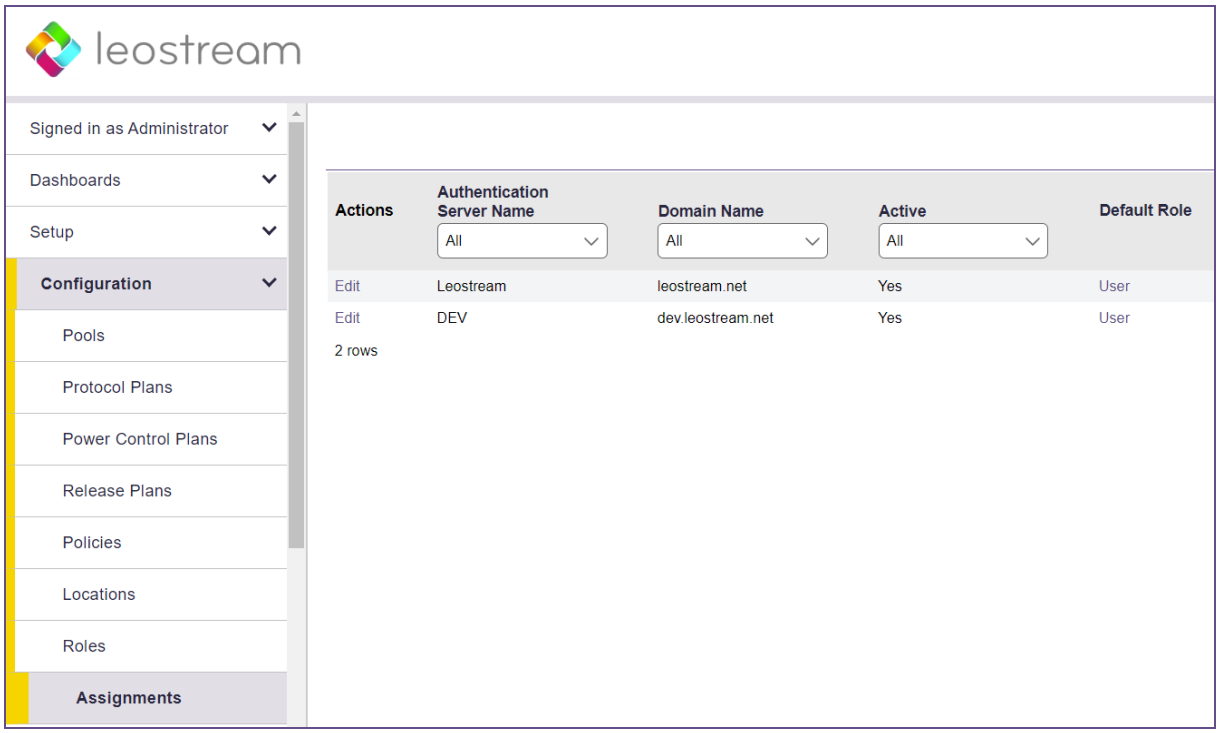
In a simple proof-of-concept environment, many of these settings can be left at their default values. Note that, by default, the Connection Broker does not offer a desktop to the user if the desktop does not have an installed Leostream Agent. If you want to offer desktops that do not have a Leostream 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.

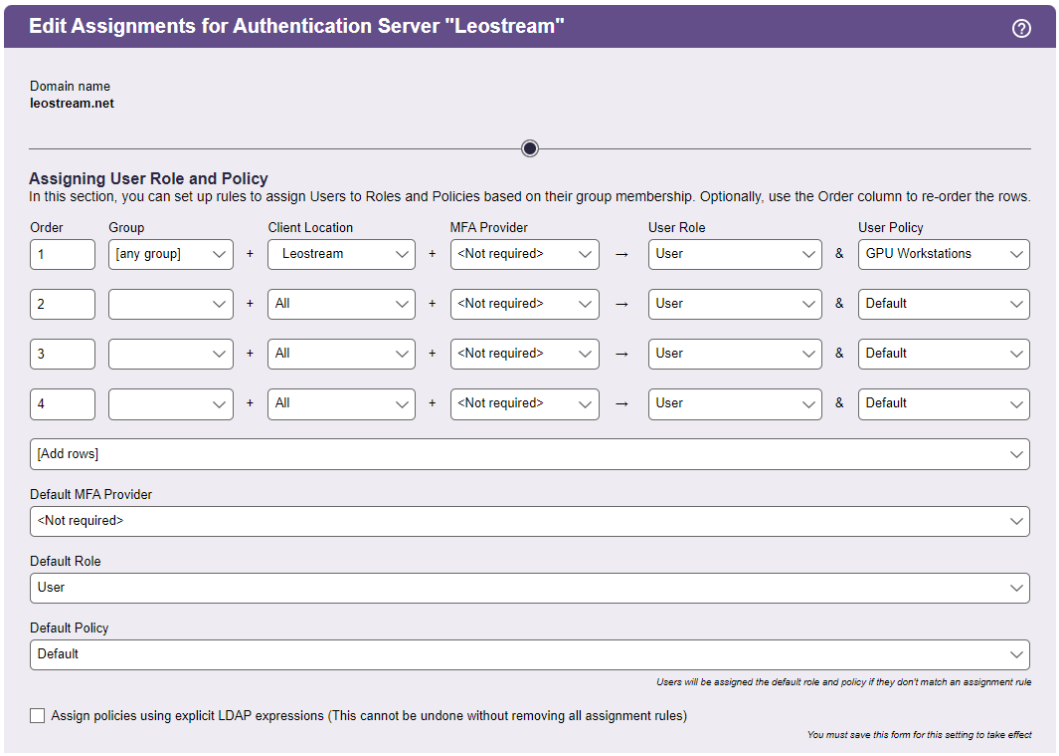
Assigning Policies to Users

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.



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.



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 9 and 12 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.

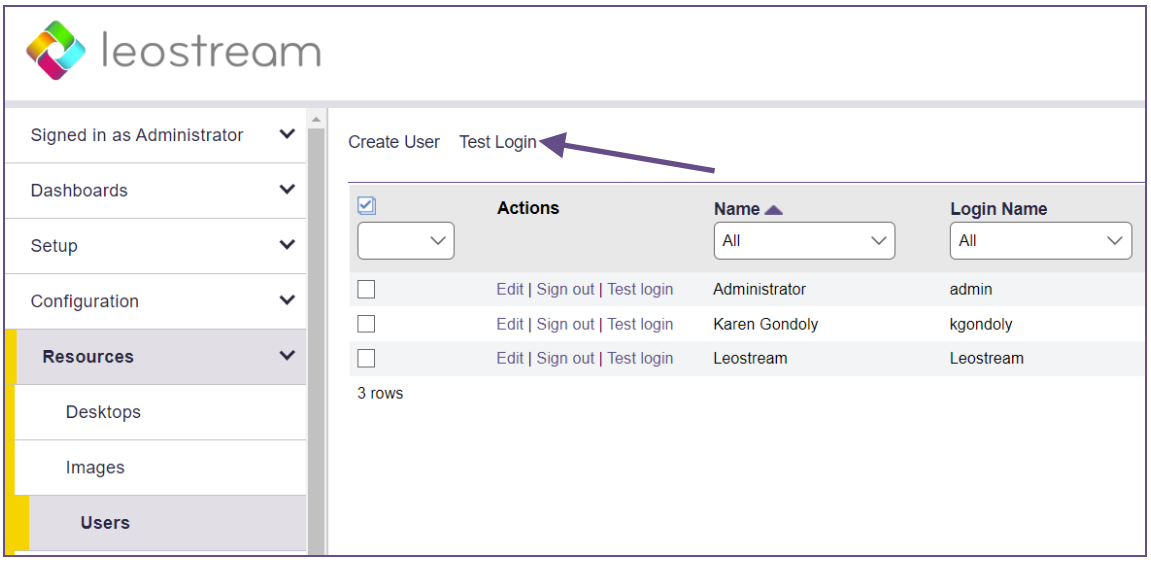
If you need to assign roles and policies based on a different user attributes, see Step 12 under "Adding Microsoft Active Directory Authentication Servers" in Chapter 13 of the Connection Broker Administrator's Guide.

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.