
Deploying Actifio Resiliency Director for AWS from an AMI



Copyright, Trademarks, and other Legal Matter

Copyright © 2021 Google LLC. All rights reserved.

Actifio™, OnVault™, and VDP™ are trademarks of Google LLC.

All other brands, product names, goods and/or services mentioned herein are trademarks or property of their respective owners.

Contents

Preface	v
The ActifioNOW Customer Portal.....	v
Chapter 1 - Introduction	1
Recovery to cloud.....	1
Chapter 2 - Deploying the Actifio Resiliency Director AMI	3
Prerequisites.....	4
CPU and Memory Requirements.....	4
Configuring the Actifio Resiliency Director AMI.....	5
Chapter 3 - Configuring the Resiliency Director Cloud Recovery	13
Chapter 4 - Accessing the Actifio Resiliency Director Cloud Recovery	15
Continue with Resiliency Director Configuration	16

Preface

The information in this guide is intended for users who are configuring Actifio Resiliency Director for AWS.

Once you have finished configuring Actifio Resiliency Director, consult the Resiliency Director online help. It provides detailed instructions on using Actifio Resiliency Director.

The ActifioNOW Customer Portal

From the customer portal you can obtain detailed reports about your appliance, as well as search the portal's knowledge base for answers to specific questions.

To log into the ActifioNOW customer portal:

1. Go to: <https://now.actifio.com>
2. When prompted, enter the user name and password you received after registering for Actifio Resiliency Director for AWS.

1 Introduction

Actifio Resiliency Director (RD) is an orchestration product that is used to automate disaster recovery for environments using Actifio appliances for backup and replication to a disaster recovery (DR) site or Cloud. RD coordinates with the Actifio appliances to automate the tasks of recovering VMs, physical servers, and their data in the event of a site-wide outage or disaster at the production site or cloud region. RD allows users to pre-configure the most manual or tedious aspects of the recovery, allowing for one-step recovery of all the in-scope servers and data in a repeatable, reliable, and predictable fashion.

Resiliency Director (RD) Cloud Recovery is a single instance of Resiliency Director that allows the enterprises to recover their VMs, physical servers, System State applications, filesystems, and database applications in the cloud environment.

To recover VMs and applications on Amazon Web Services (AWS) cloud, you must add an Amazon Machine Image (AMI) instance of Cloud Recovery in your AWS account. An AMI instance is a template that contains data which includes files to deploy Cloud Recovery on AWS along with VMs, databases, and file systems.

Before adding Cloud Recovery AMI instance, you need to subscribe and launch the Resiliency Director on AWS.

Recovery to cloud

- RD runs in a single cloud instance called RD Cloud, that is used for all configuration and recovery tasks.
- RD Cloud communicates with the AGM-managed Actifio appliances in the production environment but does not need to communicate directly with the source-side appliances.
- RD Cloud initiates recoveries on Actifio appliances in the destination cloud. These appliances may be persistent and hold the replicated data that will be used during recovery, or provisioned as-needed, and retrieve data from the cloud-provided object storage.

2 Deploying the Actifio Resiliency Director AMI

This section assumes that you have an AWS account and is familiar with AWS processes and procedures.

It has the following topics:

- [Prerequisites](#) on page 4
- [CPU and Memory Requirements](#) on page 4
- [Configuring the Actifio Resiliency Director AMI](#) on page 5

Prerequisites

Before you begin, you must have the following information available:

- Your AWS Account Number. This must be shared with your Actifio representative, and they will use it to share the Actifio Resiliency Director (RD) AMI
- The AWS region in which the Actifio RD will reside
- The VPC in which the Actifio RD for AWS AMI will be installed
- The VPC must use either a VPN or Public IP for access.
- If you use a Public IP you must use Elastic IP and have defined a gateway for the VPC

Note: If you have multiple VPCs, configure your RD for AWS AMI in the VPC that contains most of the applications to be protected. Applications that reside outside of the specified VPC can be protected if you provide a peering connection between VPCs via AWS.

CPU and Memory Requirements

The following are the CPU and Memory requirements for each Actifio Resiliency Director solution.

- For less than 100 VMs recovery
 - o Core (vCPUs): 2
 - o RAM: 8 GB
 - o Base Partition Size: 49 GB
 - o Instance Type: t2.large
- For 100 and more VMs recovery
 - o Core (vCPUs): 4
 - o RAM: 16 GB
 - o Base Partition Size: 49 GB
 - o Instance Type: t2.xlarge

Configuring the Actifio Resiliency Director AMI

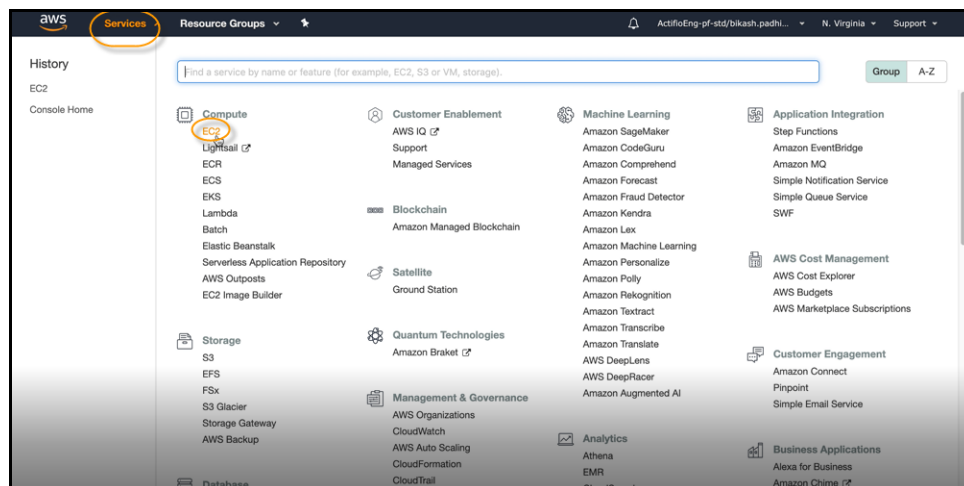
After you provide your Actifio representative with the [Prerequisites](#) on page 4, your Actifio representative will notify you when the Actifio AMI has been shared to your AWS account.

To configure the Actifio Resiliency Director AMI:

1. Log into your AWS account.
2. Ensure you have selected the correct region in which the AMI is to be installed.

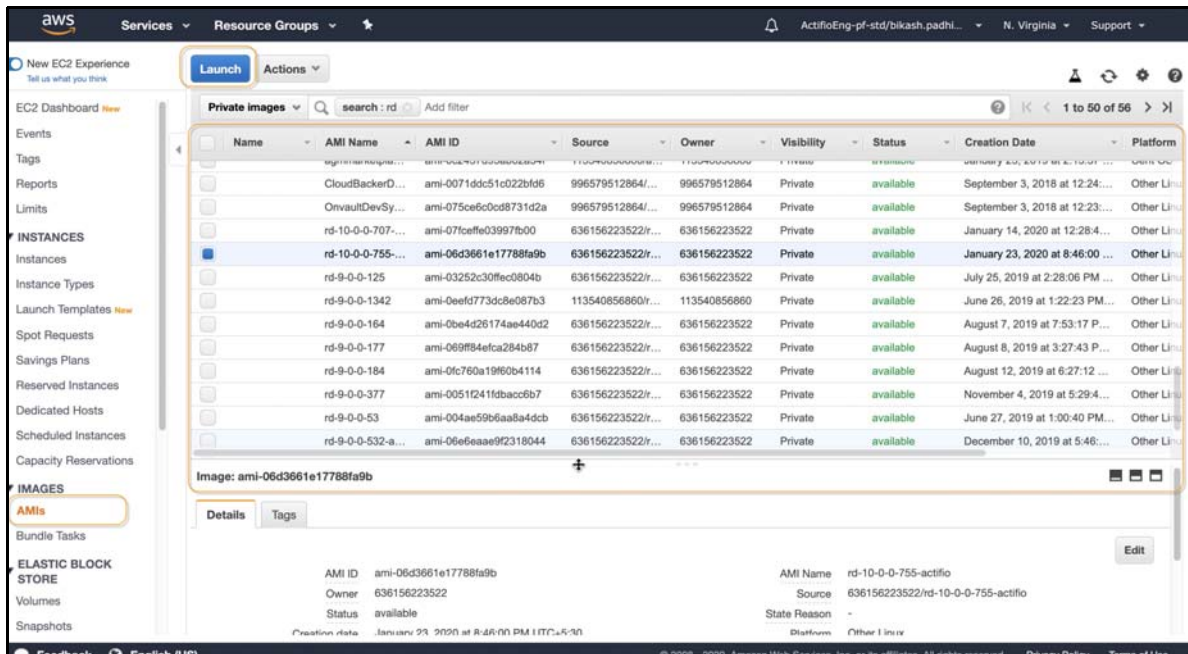


3. From **Services** > **Compute** click **EC2**.

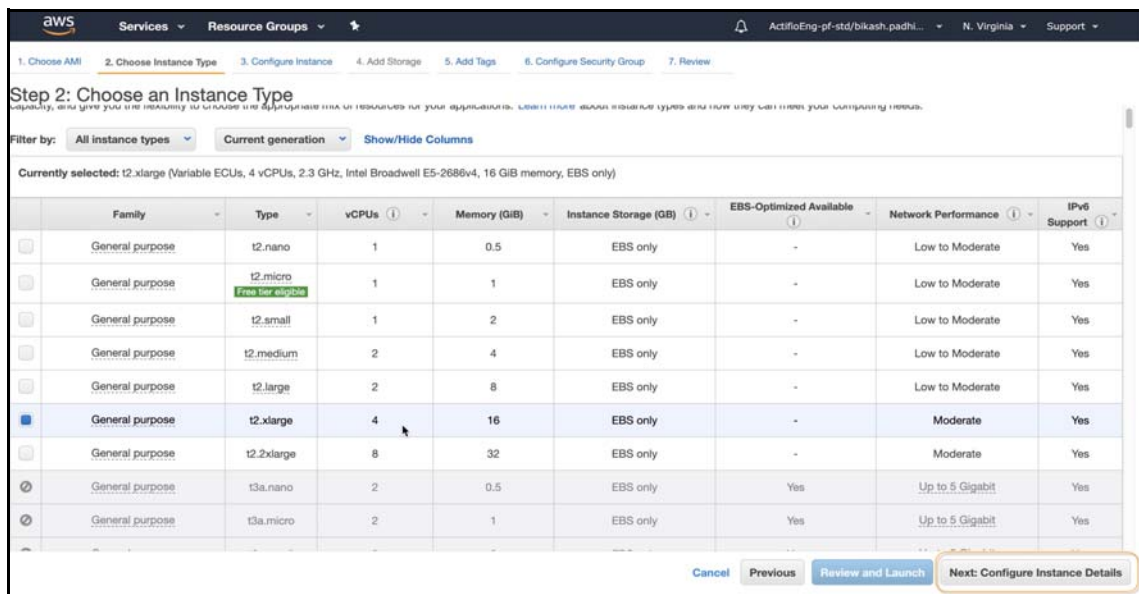


4. From the left navigation menu, under **Images**, click **AMIs** and a list of available AMIs is displayed.

- Select the Actifio Resiliency Director AMI.



- Click **Launch** and the Step 2: Choose an Instance Type page is displayed.



- From **Choose an Instance Type** page, select the required instance type as below:
 - To recover less than 100 VMs, select the instance type of **t2.large** (2 vCPUs, 8 GB RAM)
 - To recover 100 and more VMs, select the instance type of **t2.xlarge** (4 vCPUs, 16 GB RAM)

8. Click **Next: Configure Instance Details** and the Step 3: Configure Instance Details page is displayed.

9. In the **Configure Instance Details** page, configure the following:
 - o Enter one of the number of instances in the provided field.
 - o Select the VPC (network) for the Actifio Resiliency Director instance from the **Network** drop down.
 - o Select a default subnet from **Subnet** drop-down.
 - o **Auto-assign Public IP:** From the drop down list, select **Enable** if this Actifio Resiliency Director instance requires access via the public Internet. This is not required if your IT infrastructure has a VPN.
10. Click **Next: Add Storage** and the Step 4 Add Storage page is displayed.

Note: No more additional storage is required for RD Cloud Recovery.

11. Click **Next: Tag** and the Step 5 Add Tags page is displayed.

aws Services Resource Groups

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.
A copy of a tag can be applied to volumes, instances or both.
Tags will be applied to all instances and volumes. [Learn more](#) about tagging your Amazon EC2 resources.

Key (128 characters maximum) Value (256 characters maximum) Instances Volumes

Add another tag (Up to 50 tags maximum)

Cancel Previous Review and Launch Next: Configure Security Group

12. In the **Add Tags** page, create a tag for the Actifio Resiliency Director instance that is easy to remember and identify.
 - o Enter the key-value pair in the provided fields.
 - o Click **Add another tag**, if you want to add more key-pair values.
13. Click **Next: Configure Security Group** and the Step 6 Configure Security Group page is displayed.

aws Services Resource Groups

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: Create a new security group Select an existing security group

Security group name: launch-wizard-2

Description: launch-wizard-2 created 2020-02-04T17:20:25.850+05:30

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop

Add Rule

Warning
Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Cancel Previous Review and Launch

14. In **Configure Security Group** page, configure the following fields:
 - o From **Assign a security group**, create a new security group or select from an existing group.
 - o Enter the **Security group name**.

- o Ensure the Security Group is set as follows:

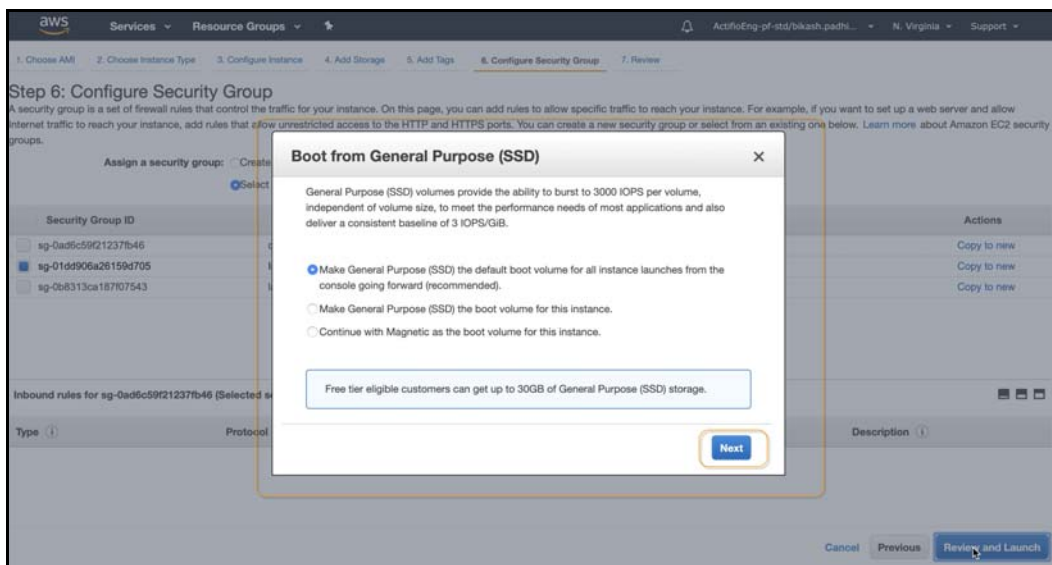
Table 1: Inbound Ports

Type	Protocol	Port Range	Source
SSH	TCP	22	Anywhere
SSH	TCP	26	Anywhere
HTTP	TCP	80	Anywhere
HTTPS	TCP	443	Anywhere

Table 2: Outbound Ports

Type	Protocol	Port Range	Target
SSH	TCP	22	Sky Appliance
SSH	TCP	26	Sky Appliance
HTTPS	TCP	443	Sky Appliance, AWS API Endpoint
Adhd tunnel. TCP	TCP	5103	Sky Appliance

- o Click **Review and Launch** and the Boot from General Purpose (SSD) pop-up opens.



- o Click **Next** in the Boot from General Purpose (SSD) page, The Step 7: Review Instance Launch page is displayed.

15. In the **Review Instance Launch** page, review the instance details. If the selections and settings are correct, click **Launch**.

Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

Warning: Your instance configuration is not eligible for the free usage tier. To launch an instance that's eligible for the free usage tier, check your AMI selection, instance type, configuration options, or storage devices. Learn more about [free usage tier](#) eligibility and usage restrictions.

AMI Details

rd-10-0-0-755-actifio - ami-06d3661e17788fa9b
AWS-VMImport service: Linux - R/C - Cannot determine release - 2.6.32-754.17.1.el6.x86_64
Root Device Type: ebs Virtualization type: hvm

Instance Type

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.xlarge	Variable	4	16	EBS only	-	Moderate

Security Groups

Security Group ID	Name	Description
sg-01dd906a26159d705	InternalOnly	Internal access to Actifio Resources

Buttons: Cancel, Previous, **Launch**

The **Select an existing key pair or create a new key pair** pop-up opens.

Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

Warning: Your instance configuration is not eligible for the free usage tier. To launch an instance that's eligible for the free usage tier, check your AMI selection, instance type, configuration options, or storage devices. Learn more about [free usage tier](#) eligibility and usage restrictions.

AMI Details

rd-10-0-0-755-actifio - ami-06d3661e17788fa9b
AWS-VMImport service: Linux - R/C - Cannot determine release - 2.6.32-754.17.1.el6.x86_64
Root Device Type: ebs Virtualization type: hvm

Instance Type

Instance Type	ECUs	vCPUs
t2.xlarge	Variable	2

Security Groups

Security Group ID	Name	Description
sg-01dd906a26159d705	InternalOnly	Internal access to Actifio Resources

Modal Dialog: Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Choose an existing key pair
Select a key pair
ActifioEngScripts

☒ I acknowledge that I have access to the selected private key file (ActifioEngScripts.pem), and that without this file, I won't be able to log into my instance.

Buttons: Cancel, **Launch Instances**

16. Select either **Choose an existing key pair** or **Create a new key pair** from the drop-down menu.
17. Select the Acknowledgment check-box to indicate that you will access your selected private key file that is required to log into your instance.
18. If the selections and settings are correct, click **Launch Instance** and the RD for AWS instance is deployed. Select **Cancel** if you want to make any changes to the selections or settings.

The created instance is displayed at the Instance page and you can search the instance with the key tags assigned.

The screenshot displays the AWS Management Console interface. On the left-hand side, the navigation menu is visible, with the 'INSTANCES' section highlighted. The main content area shows the 'Private images' page. At the top of this page, there are tabs for 'Launch' and 'Actions'. Below these tabs is a search bar with the text 'search : rd' and a button labeled 'Add filter'. The primary feature is a table listing private images. The table has the following columns: Name, AMI Name, AMI ID, Source, Owner, Visibility, Status, Creation Date, and Platform. There are 12 rows of data, each representing a private image. All images in the table have a status of 'available'. Below the table, there is a prompt that says 'Select an AMI above'.

Name	AMI Name	AMI ID	Source	Owner	Visibility	Status	Creation Date	Platform
903imagetom	903imagetom	ami-045ec132ca628b650	1135408568609...	113540856860	Private	available	October 10, 2019 at 5:10:34 ...	Other Lin
Actifio Target ...	ami-f8d0882	636156223522/...	636156223522/...	636156223522	Private	available	January 18, 2018 at 1:31:58 ...	Other Lin
Actifio Target ...	ami-061746a702de77316	636156223522/...	636156223522/...	636156223522	Private	available	September 6, 2018 at 3:29:0...	Other Lin
Actifio Target ...	ami-0864d6f61a62a1cf7	636156223522/...	636156223522/...	636156223522	Private	available	September 13, 2018 at 2:54:...	Other Lin
Actifio Target ...	ami-050ebbacc43d0224d	636156223522/...	636156223522/...	636156223522	Private	available	September 25, 2018 at 2:40:...	Other Lin
Actifio Target ...	ami-042649295f64d51a1	636156223522/...	636156223522/...	636156223522	Private	available	December 17, 2018 at 6:56:...	Other Lin
Actifio Target ...	ami-0d7d3c95f8ee86413	636156223522/...	636156223522/...	636156223522	Private	available	November 15, 2018 at 3:26:...	Other Lin
Actifio Target ...	ami-0461f3889c24af1d7	636156223522/...	636156223522/...	636156223522	Private	available	December 3, 2018 at 5:23:2...	Other Lin
Actifio Target ...	ami-0adc934222a1ca951	636156223522/...	636156223522/...	636156223522	Private	available	January 22, 2019 at 5:02:30 ...	Other Lin
Actifio Target ...	ami-07a385705300b6464	636156223522/...	636156223522/...	636156223522	Private	available	February 23, 2019 at 4:29:0...	Other Lin
Actifio Target ...	ami-049cd27d20196aa78	636156223522/...	636156223522/...	636156223522	Private	available	April 2, 2019 at 2:03:29 PM ...	Other Lin
Actifio Target ...	ami-00b436c23eb66478f	636156223522/...	636156223522/...	636156223522	Private	available	April 12, 2019 at 1:59:10 AM...	Other Lin
Actifio Target ...	ami-0f18bd90356b050d9	636156223522/...	636156223522/...	636156223522	Private	available	April 11, 2019 at 2:01:04 PM...	Other Lin

3 Configuring the Resiliency Director Cloud Recovery

When the Actifio Resiliency instance is ready, obtain the instance's desired IP. Once you have the IP you are ready to configure the Actifio Resiliency Director in to the instance.

To configure the Actifio Resiliency Director Cloud Recovery:

1. Open a web browser and enter the URL <https://Actifio Resiliency Director IP Address> to launch the Resiliency Director Configuration page.

actifio
Radically Simple

Resiliency Director Configuration

Items marked with * are required.

Appliance IP * 172.27.43.208

Appliance Name * rdsystem01.test.dom

DNS Server 192.168.192.10,192.168.225.2

Subnet Mask * 255.255.252.0

Gateway * 172.27.40.1

NTP Server 172.29.11.179

Admin Password *

TimeZone (US & Canada) Eastern Time ▼

RD Type RD CloudRecovery ▼

Save

© Actifio Inc. All Rights Reserved.

2. Change the network parameters to the following values:
 - o Enter/verify the static IP address of in **Appliance IP**.
 - o Enter the name of Cloud Recovery in **Appliance Name**.
 - o Enter the DNS Server IP address in **DNS Server**.
 - o Enter the **Subnet Mask** and **Gateway**.
 - o Enter the NTP server IP address in **NTP Server**.

- o Set the administrator password in **Admin Password**. Use this password to login to the user interface.

Note: You can change the admin password by using the `resetuserpasswd` command.

- o Select the time zone from **TimeZone**.
- o Select RD CloudRecovery from **RD Type**.

3. Click **Save**. The server reboots after setting the configuration.

Note: To modify the network parameters such as IP address, DNS Server, Gateway, Hostname of the Appliance, use `configsystem` command.

Note: For information on CLI commands, refer the Actifio Resiliency Director CLI guide.

4 Accessing the Actifio Resiliency Director Cloud Recovery

This chapter provides the details to log on to the Actifio Resiliency Director Cloud Recovery graphical user interface. You can login to the Actifio Resiliency Director Cloud Recovery graphical user interface using the Resiliency Director administrator credentials.

To access the Actifio Resiliency Director Cloud Recovery home screen:

1. Open a Web browser and use the URL `https://<Actifio Resiliency Director IP Address>` to access the Actifio Resiliency Director Cloud Recovery **Login** page.

Note: Use the IP address/hostname of the virtual machine where Resiliency Director Cloud Recovery is running.

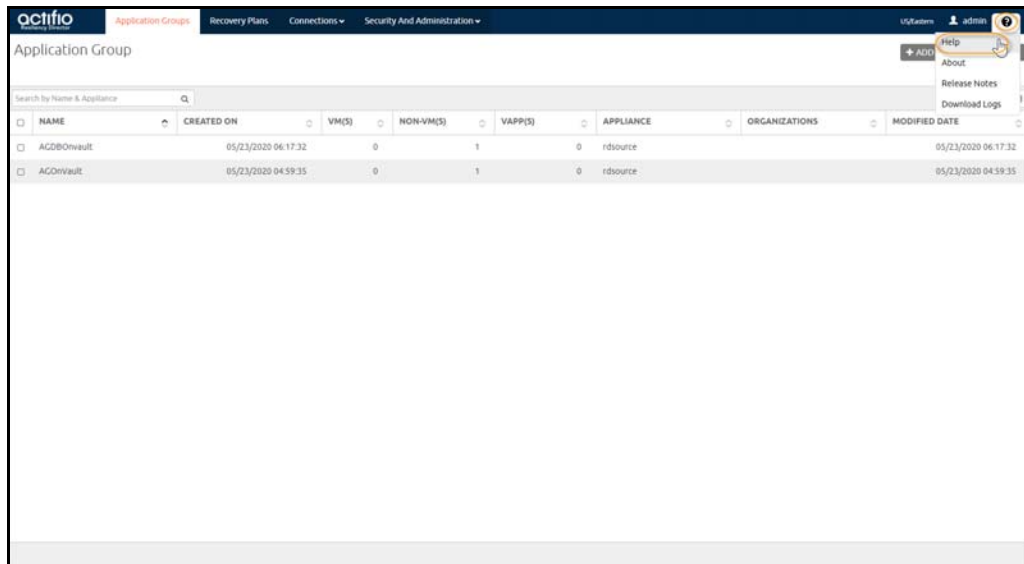


Actifio Resiliency Director Cloud Recovery Login Screen

2. From the Login window, enter the user name as “admin” and the password used during the initial Resiliency Director deployment and installation, then Click **Log In**. The Actifio Resiliency Director Cloud Recovery home screen opens.

Continue with Resiliency Director Configuration

Once successfully logged in, use the Resiliency Directory Online help for guidance on configuring and using Resiliency Director.



Accessing Resiliency Director Online Help