
Actifio Resiliency Director Collector User Guide

Copyright, Trademarks, and other Legal Matter

Copyright © 2009 - 2020 Actifio, Inc. All rights reserved.

Actifio®, AnyIT®, Dedup Async®, OnVault®, Enterprise Data-as-a-Service®, FlashScan®, AppFlash DEVOPS Platform®, Copy Data Cloud®, and VDP® are registered trademarks of Actifio, Inc.

Actifio Sky™, Actifio One™, and Virtual Data Pipeline™ are trademarks of Actifio, Inc.

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

Actifio, Inc., is a provider of data protection and availability products. Actifio's technology is used in products sold by the company and products and services sold and offered by its commercial partners. The current list of Actifio patents is available online at: <http://www.actifio.com/patents/>

Actifio believes the information in this publication is accurate as of its publication date. Actifio reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." ACTIFIO, INC. MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

This software and the associated documentation are proprietary and confidential to Actifio. Use, copying, and distribution of any Actifio software described in this publication requires an applicable software license. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

Actifio strives to produce quality documentation and welcomes your feedback. Please send comments and suggestions to docs@actifio.com.

Contents

Preface	v
Actifio Appliances.....	v
The Actifio Now Customer Portal.....	v
Actifio Support Centers	v
.....	v
Chapter 1 - Introduction to the Actifio Resiliency Director Collector	7
Resiliency Director Collector Overview	7
Chapter 2 - Deploying the Actifio Resiliency Director Collector	9
Deploying the Resiliency Director Collector OVA	9
Configuring the Actifio Resiliency Director Collector	10
Chapter 3 - Accessing the Actifio Resiliency Director Collector	11
Chapter 4 - Adding and Managing Actifio Appliances	15
Adding an Actifio Appliance to the Actifio Resiliency Director Collector.....	16
Listing the Available Actifio Appliances.....	18
Modifying an Actifio Appliance Details	19
Deleting an Actifio Appliance from the Resiliency Director Collector.....	20
Chapter 5 - Adding and Managing Virtual Management Servers	21
Adding a Virtual Management Server	22
Listing the Virtual Management Servers	23
Modifying a Virtual Management Server	24
Deleting a Virtual Management Server.....	25
Chapter 6 - Adding and Managing Application Groups	27
About Application Groups	28
Adding an Application Group.....	29
Setting the recovery order	32
Setting the VM Parameters.....	33
First Sequence script and Last Sequence script.....	38
Failover-script and Reset-script.....	38
Listing Application Groups	39
Modifying an Application Group.....	41

Deleting an Application Group.....	41
Chapter 7 - Creating and Managing Organizations	43
Creating an Organization.....	44
Editing the Organization Details	46
Deleting Organization(s)	47
Chapter 8 - Managing Server Passwords	49
Listing the Server Passwords.....	49
Adding the Server Passwords.....	50
Editing the Server Passwords	50
Deleting the Server Passwords	51
Chapter 9 - Viewing the Actifio Resiliency Director Server Details	53
Viewing the Actifio Resiliency Director Server Details.....	53
Chapter 10 - Adding and Managing User Access Control	55
Creating roles and assigning permissions.....	57
Modifying roles and changing permissions.....	58
Deleting roles	59
Chapter 11 - Downloading Logs	61
Downloading the Logs.....	61
Chapter 12 - Upgrading the Resiliency Director Collector	63
Upgrade using GUI-Based Method.....	63
Upgrade using CLI-Based Method.....	65
Chapter 13 - vCenterPermissions_collector.fm	67
Creating the ActifioReadOnly vCenter Role	68
Creating the ActifioOperations vCenter Role.....	69
The vCenter Permissions List.....	70
Assigning Minimum Permissions.....	71

Preface

This guide provides step-by-step instructions on how to deploy and use the Actifio Resiliency Director Collector. This guide assumes that you are already familiar with Actifio appliances by following ***Getting Started with Actifio Copy Data Management*** guide and have a grasp of the basic concepts associated with an Actifio Appliance.

Your Actifio Appliance's Documentation Library contains detailed, step-by-step, application-specific instructions on how to protect and access your data. Each guide is in PDF format and may be viewed, downloaded, and printed on demand.

Actifio Appliances

Unless otherwise specified, all features and functions described in this document apply to both Actifio CDS and Actifio Sky appliances.

The Actifio Now Customer Portal

During the configuration and initialization of your Actifio appliance your Actifio representative provided you with a user name and password for the Actifio Now customer portal.

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

To log into the Actifio Now customer portal:

1. Go to: <https://now.actifio.com>
2. When prompted, enter the user name and password provided by your Actifio representative.

Actifio Support Centers

To contact an Actifio support representative, you can:

- Send email to: support@actifio.com
- Call:
 - From anywhere:** +1.315.261.7501
 - US Toll-Free:** +1.855.392.6810
 - Australia:** 0011 800-16165656
 - Germany:** 00 800-16165656
 - New Zealand:** 00 800-16165656
 - UK:** 0 800-0155019

1 Introduction to the Actifio Resiliency Director Collector

The Actifio Resiliency Director Collector is a component of the Actifio Resiliency Director, a resiliency solution for non-disruptive automated recovery of virtual machines and database applications.

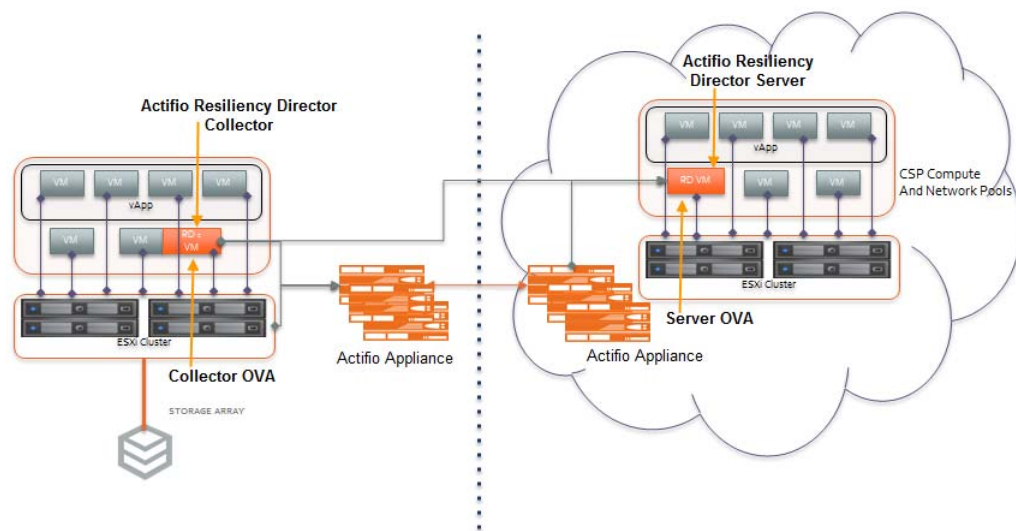
The Actifio Resiliency Director orchestrates the Actifio Appliances, and provides a one-click recovery of all the applications at the enterprise DR site or Cloud Service Provider (CSP) site.

This chapter provides architectural overview of the Actifio Resiliency Director Collector.

Resiliency Director Collector Overview

The Actifio Resiliency Director Collector component discovers applications (VMs, vApps, File Systems, SQL Server Databases) IP address, CPU usage, and tracks changes in parallel to the recovery process. The Actifio Resiliency Director Collector integrates with Actifio Resiliency Director Server and aims to recover the applications in a user specified order or group. In addition to providing a faster recovery process, recoveries are also executed in a repeatable way. This approach reduces the overall recovery time for business critical data.

The Actifio Resiliency Director Collector is deployed at the source data site and allows you to discover applications, create groups of applications, and configured details about how they should be recovered. The following diagram shows how the Resiliency Director Collector fits into an environment.



Actifio Resiliency Director Collector Overview

2 Deploying the Actifio Resiliency Director Collector

This chapter describes how to deploy the Actifio Resiliency Director Collector. Actifio Resiliency Director Collector is available as VMware virtual appliance (.ova). You must configure the Collector after deploying the ova.

This chapter contains the following topics:

- [Deploying the Resiliency Director Collector OVA](#) on page 9
- [Configuring the Actifio Resiliency Director Collector](#) on page 10

Deploying the Resiliency Director Collector OVA

Before deploying Actifio Resiliency Director Collector ova file, ensure that server meets the minimum system requirements of 2 vCPU, 8 GB RAM, and 40 GB storage. You can deploy the Actifio Resiliency Director Collector on the vCenter Server 5.x - 6.x.

To deploy the Actifio Resiliency Director Collector.ova file:

1. Launch the vSphere vCenter client.
2. From **File**, click **Deploy OVF** template.
3. Provide the path to the ActifioRD.ova file and click **Next**.
4. Select the virtual disk type and click **Next**. Provide the details in the VM network properties and select the port group. Confirm the details of the virtual server.
5. Select **Power on after deployment** and click **Finish**. You can see the progress of the OVA deployment.
6. Wait for the VM to show its IP address. You will use this IP address to configure the Actifio Resiliency Director Collector.

To deploy the Actifio Resiliency Director ova file using VMware Web Client:

1. Log on to the vSphere web client <https://<ip-address>/vsphere-client>
2. Select vCenter Server, click on **Actions >>** and choose **Deploy OVF Template** option.
3. Provide the URL or select a local file for the RD virtual appliance and then click **Next**.
URL example: http://192.168.192.179/files/RD-8.0.3.1234.OVA
4. Provide a name for the RD virtual appliance and select a data center or folder and then click **Next**.
5. Select a host or cluster or resource pool or vApp, click **Next**.
6. Review details and click **Next**.
7. Select Storage and click **Next**.
8. Select Networks and click **Next**.
9. Enter the values for the networking properties and click **Next**.
10. Review the configuration data and click **Finish**. Power on the virtual appliance after deployment.
11. Wait for the VM to show its IP address. You will use this IP address to configure the Actifio Resiliency Director.

Configuring the Actifio Resiliency Director Collector

To configure the Actifio Resiliency Director Collector:

1. After the VM is deployed, wait until the VM show its IP address.
2. Open a Web browser and use the URL *https://<Actifio Resiliency Director IP Address>* to launch the **Resiliency Director Configuration** page.
3. Change the network parameters to the following values:
 - o Enter/verify the static IP address of the Actifio Resiliency Director in the **Appliance IP** field.
 - o Enter the name of the Actifio Resiliency Director Collector in the **Appliance Name** field.
 - o Enter the DNS Server IP address in the **DNS Server** field.
 - o Enter the **Subnet Mask** and **Gateway** details in the respective fields.
 - o Enter the NTP server IP address in the **NTP Server** field.
 - o Set the administrator password in the **Admin Password** field that you will use while accessing the Resiliency Director Collector UI. You can change the admin password later using a CLI command.
 - o Select your time zone from the **Timezone** drop-down list.
 - o Select **RD Collector** from the **RD Type** drop-down list.
4. Click **Save** and then click **OK**. The server reboots after setting the configuration.

actifio
Radically Simple

Resiliency Director Configuration

Items marked with * are required.

Appliance IP * 172.29.11.213

Appliance Name * dev.actifio.com

DNS Server 192.169.123.4

Subnet Mask * 255.255.255.0

Gateway * 172.29.11.100

NTP Server 192.168.1.12

Admin Password * *****

Timezone (US & Canada) Eastern Time ▼

RD Type RD Collector ▼

Save

© Actifio Inc. All Rights Reserved.

Actifio Resiliency Director Collector Configuration Parameters

Note: If you wish to modify the network parameters such as IP address, DNS Server, Gateway, Hostname of the RD Appliance, use **rdtask configsystem** command. For more information, see the **configsystem** section in *Actifio Resiliency Director CLI user guide*.

3 Accessing the Actifio Resiliency Director Collector

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

To access the Actifio Resiliency Director Collector home screen:

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

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



Actifio Resiliency Director Collector 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 Collector home screen appears.

Note: The Actifio Resiliency Director always has a single local login named "admin" that has full access. Additionally, it can be configured to leverage the authentication on an Actifio appliance to add support for multiple users, and even pass-through authentication to an LDAP directory. The **User Name** and **Password** fields are case sensitive.

Actifio Components	Description
Actifio Resiliency Director Collector	Allows users to discover applications, create groups of applications, and configure details about how they should be recovered.
Actifio Appliance	Actifio Appliances such as CDS and Sky.
Applications	Recoverable sets of data, including VMs, vApps, File Systems and Databases
Actifio Resiliency Director Server	Performs recovery operations at the DR site, based on the application groups defined on the Resiliency Director Collector.

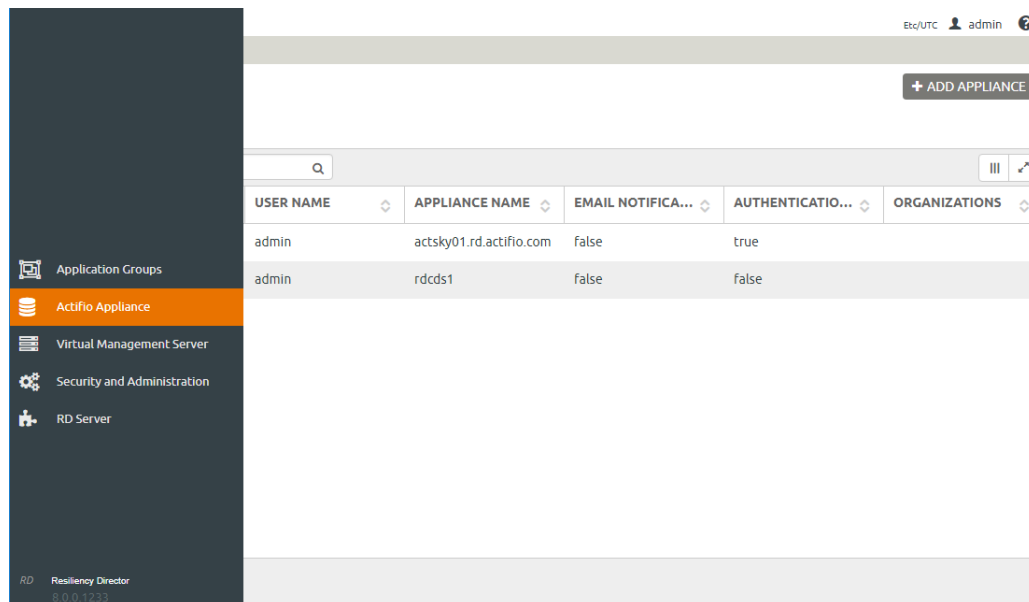
The Actifio Resiliency Director title bar includes:

- **Timezone:** Contains the current time of the Actifio Resiliency Director Server.
- **User name:** Displays the logged in user name and an option to Logout.
- **Help Menu:** The Help menu contains Release Notes, User Guide, and Download logs information.



Actifio Resiliency Director Collector - Title Bar

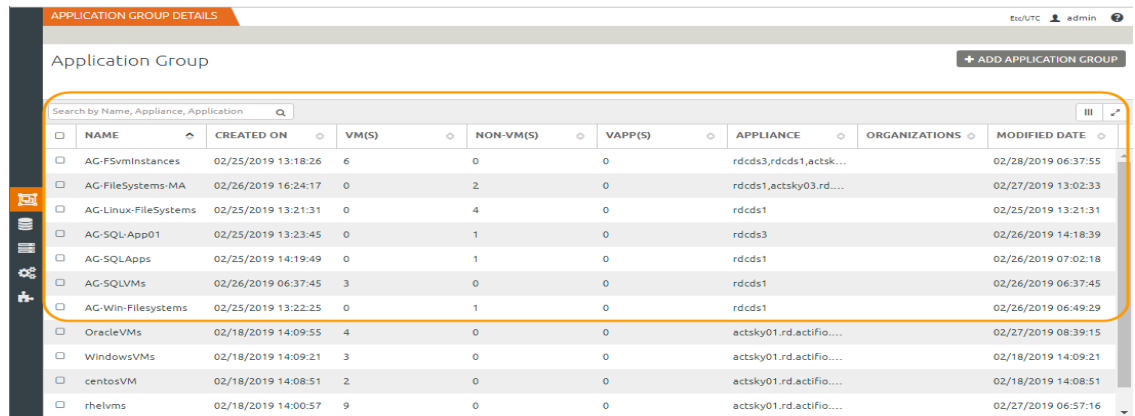
The left pane displays the task icons that are used for navigation. These navigation links on the left pane allows you to perform various tasks. The details of the selected task appears on the information pane, once selected.



Actifio Resiliency Director Collector - Navigation and Information Pane

The Actifio Resiliency Director Collector Home Screen

The Actifio Resiliency Director home screen lists the configured application groups, as seen in figure below. If no Actifio appliances are defined, then instead of displaying the application group listing, the Actifio Appliance screens will be displayed as that is the first step in configuring a newly installed Resiliency Director Collector.



	NAME	CREATED ON	VM(S)	NON-VM(S)	VAPP(S)	APPLIANCE	ORGANIZATIONS	MODIFIED DATE
<input type="checkbox"/>	AG-FSvmInstances	02/25/2019 13:18:26	6	0	0	rdcds3,rdcds1,actsk...		02/28/2019 06:37:55
<input type="checkbox"/>	AG-FileSystems-MA	02/26/2019 16:24:17	0	2	0	rdcds1,actsky03.rd...		02/27/2019 13:02:33
<input type="checkbox"/>	AG-Linux-FileSystems	02/25/2019 13:21:31	0	4	0	rdcds1		02/25/2019 13:21:31
<input type="checkbox"/>	AG-SQL-App01	02/25/2019 13:23:45	0	1	0	rdcds3		02/26/2019 14:18:39
<input type="checkbox"/>	AG-SQLApps	02/25/2019 14:19:49	0	1	0	rdcds1		02/26/2019 07:02:18
<input type="checkbox"/>	AG-SQLVMs	02/26/2019 06:37:45	3	0	0	rdcds1		02/26/2019 06:37:45
<input type="checkbox"/>	AG-Win-Filesystems	02/25/2019 13:22:25	0	1	0	rdcds1		02/26/2019 06:49:29
<input type="checkbox"/>	OracleVMs	02/18/2019 14:09:55	4	0	0	actsky01.rd.actifio....		02/27/2019 08:39:15
<input type="checkbox"/>	WindowsVMs	02/18/2019 14:09:21	3	0	0	actsky01.rd.actifio....		02/18/2019 14:09:21
<input type="checkbox"/>	centosVM	02/18/2019 14:08:51	2	0	0	actsky01.rd.actifio....		02/18/2019 14:08:51
<input type="checkbox"/>	rhelvms	02/18/2019 14:00:57	9	0	0	actsky01.rd.actifio....		02/27/2019 06:57:16

Actifio Resiliency Director Collector Home Screen - Application Groups

The Application Groups home screen allows you to add, edit, and delete the application groups. for more information on adding, editing, and deleting an application groups, see [Adding and Managing Application Groups](#) on page 27.

4 Adding and Managing Actifio Appliances

This chapter provides the details to add, list, edit, and delete the Actifio Appliances used by the Actifio Resiliency Director Collector.

This chapter contains the following topics:

[Adding an Actifio Appliance to the Actifio Resiliency Director Collector](#) on page 16

[Listing the Available Actifio Appliances](#) on page 18

[Modifying an Actifio Appliance Details](#) on page 19

[Deleting an Actifio Appliance from the Resiliency Director Collector](#) on page 20

Adding an Actifio Appliance to the Actifio Resiliency Director Collector

While creating an Application Group, the Resiliency Director Collector displays a list of VMs / File Systems /Databases available to be added to an application group. In order to obtain the list, at least one Appliance must be added.

You must connect Resiliency Director Collector to an Actifio Appliance by providing an IP Address or Host Name and credentials. You can add multiple Actifio Appliances to the Collector. Actifio Appliances should be added with administrator credentials on the Resiliency Director Collector.

To add an Actifio Appliance:

1. In the left navigation pane, click **Actifio Appliance**. The **Appliance** page appears.
2. Click **+ Add Appliance**. The **Add Appliance** page appears.
3. Enter the **IP address** or **Host name** of the Actifio Appliance in the **IP/Host Name** field.
4. Select **Organization** from the drop down list for users of selected organization to have access to this particular Appliance. For more details on organization, see [Chapter 7, Creating and Managing Organizations](#)
5. Enter the respective user credentials in the **User Name** and **Password** fields.

If you want to use the Actifio Appliance authentication mode, then select the check box **Use Actifio Appliance as authentication source for RD**.

The screenshot shows the 'Add Appliance' form within the 'APPLIANCE' section of the Actifio Resiliency Director Collector. The form includes the following fields and options:

- IP/HOST NAME ***: A text input field containing '172.29.xx.11'.
- ORGANIZATIONS**: A dropdown menu.
- USER NAME ***: A text input field containing 'test'.
- PASSWORD ***: A password input field with masked characters.
- USE ACTIFIO APPLIANCE AS AUTHENTICATION SOURCE FOR RD**: A toggle switch that is currently turned on.
- Note**: A text note stating, 'Enabling authentication source for this Actifio Appliance will disable any previously configured authentication source.'
- Buttons**: 'Cancel' and 'Save' buttons at the bottom right.

The interface also features a left navigation pane with icons for various functions and a top header bar showing the user 'admin' and location 'Asia/Calcutta'.

6. Click the **Save** button. A pop-up message appears with the HTTPS certificate for the Actifio appliance.

Accept the certificate to add the appliance

VERSION : V3
SUBJECT : CN=XXX.XXX
SIGNATURE ALGORITHM : SHA256WITHRSA
KEY : SUN RSA PUBLIC KEY, 2048 BITS
VALIDITY : VALIDITY: [FROM: FRI MAR 30 05:30:00 IST 2018,
TO: TUE APR 30 17:30:00 IST 2019]
ISSUER : CN=AMAZON, OU=SERVER CA 1B, O=AMAZON, C=US
TYPE : X.509
IP ADDRESS : AMAZON, OU=SERVER CA 1B, O=AMAZON, C=US
SERIAL NUMBER : 18948441804165503535482938263155198384
MODULUS :
SUN RSA PUBLIC KEY, 2048 BITS
MODULUS:
192190926025019512813496547355169089432707407471270205928054685753114177663
799732671712289890930758872520650611773992417818816386320973003521492988218
943236695163873953036557775062798334685104630560974276792197171029874278830
664154830664902451934441045996724224519679964740475857484001755963592720163
540603020177040615117433147104851724016817866070156276473001708501070406457

Cancel

Accept

7. Click the **Accept** button to add the Actifio appliance.
8. Click **Okay** in the confirmation dialog.

Listing the Available Actifio Appliances

You can see the available Actifio Appliances on the Resiliency Director Collector.

To list the available Actifio Appliances:

1. In the left navigation pane, click **Actifio Appliance**.
2. The **Appliance** page provides the list of available Actifio Appliances.

Actifio Appliance Details Table - Field Elements

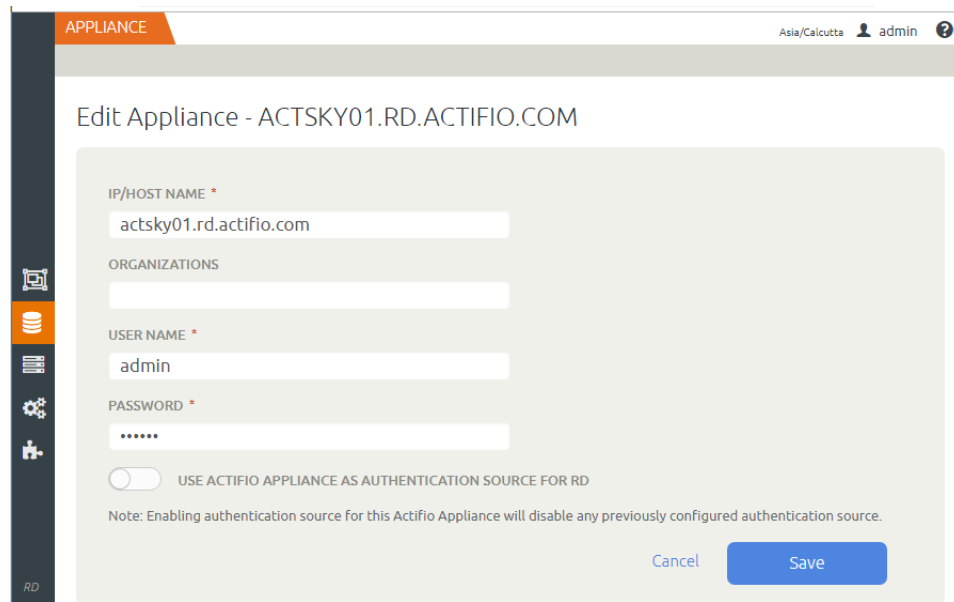
Field/Item	Description
IP/HOST NAME	Displays the hostname or the IP address of the Actifio Appliance.
USER NAME	Displays the user name that is used to communicate with the Actifio Appliance.
APPLIANCE NAME	Displays the name of the Actifio Appliance.
AUTHENTICATION SOURCE	Displays the authentication source.
ORGANIZATIONS	Displays the organization name.

Modifying an Actifio Appliance Details

To edit an Actifio Appliance details:

1. In the left navigation pane, click **Actifio Appliance**. The list of available Actifio Appliances appears.
2. Select the Actifio Appliance you want to modify, then click **Edit**. The **Edit Appliance** page appears.
3. Modify the **IP address** or **Host name** of the Actifio Appliance in the **IP/Host Name** field.
4. Select the organization from the **Organization** drop-down field.
5. Enter the respective user credentials in the **User Name** and **Password** fields.

If you want to use the Actifio Appliance authentication mode, then select the check box **Use Actifio Appliance as authentication source for RD**.



6. Click the **Save** button. A pop-up message appears with the HTTPS certificate for the Actifio appliance.

Accept the certificate to add the appliance

VERSION : V3
SUBJECT : CN=XXXXXXX
SIGNATURE ALGORITHM : SHA256WITHRSA
KEY : SUN RSA PUBLIC KEY, 2048 BITS
VALIDITY : VALIDITY: [FROM: FRI MAR 30 05:30:00 IST 2018, TO: TUE APR 30 17:30:00 IST 2019]
ISSUER : CN=AMAZON, OU=SERVER CA 1B, O=AMAZON, C=US
TYPE : X.509
IP ADDRESS : AMAZON, OU=SERVER CA 1B, O=AMAZON, C=US
SERIAL NUMBER : 18948441804165503535482938263155198384
MODULUS :
SUN RSA PUBLIC KEY, 2048 BITS
MODULUS:
192190926025019512813496547355169089432707407471270205928054685753114177663
799732671712289890930758872520650611773992417818816386320973003521492988218
94323669516387395303655775062798334685104630560974276792197171029874278830
664154830664902451934441045996724224519679964740475857484001755963592720163
5406N30701770A0A615112A331A210A8R5127A016R17866N70156276A27300170R501070A0A457

Cancel

Accept

7. Click the **Accept** button to accept the certificate. Use the **Cancel** button if you do not want to add the Actifio appliance certificate.
8. Click **Okay** in the confirmation dialog.

Deleting an Actifio Appliance from the Resiliency Director Collector

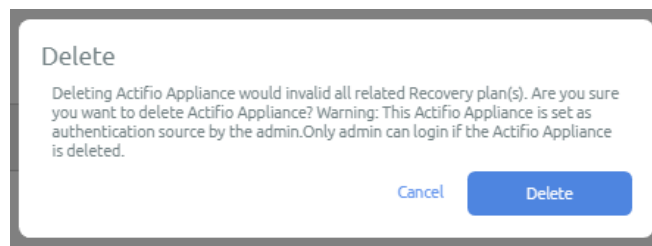
Before you delete, make sure to verify the dependencies, deleting an Actifio Appliance also removes the associated application groups, recovery plans if any.

To delete an Actifio Appliance:

1. In the left navigation pane, click **Actifio Appliance**. The list of available Actifio Appliances appears.
2. Select the Actifio Appliance from the list and click **Delete**. The **Delete** Actifio Appliance dialog box appears asking for the confirmation to delete the selected Actifio Appliance.

Note: You can delete multiple Actifio Appliances at a time. Use the appropriate check-boxes to select multiple Actifio Appliances.

3. Click **Delete** to remove the Actifio Appliance. Deleting an Actifio Appliance record also deletes the associated application groups, if any.



Note: You cannot delete the Actifio Appliance if application groups on the Resiliency Director Collector are part of a recovery plan.

5 Adding and Managing Virtual Management Servers

This chapter provides the details to add, list, edit, and delete the virtual management servers used by the Actifio Resiliency Director Collector.

This chapter contains the following topics:

- [Adding a Virtual Management Server](#) on page 22
- [Listing the Virtual Management Servers](#) on page 23
- [Modifying a Virtual Management Server](#) on page 24
- [Deleting a Virtual Management Server](#) on page 25

Adding a Virtual Management Server

You must provide the credentials and IP address to connect to a virtual management server. The Actifio Resiliency Director Collector can connect to multiple virtual management servers.

Note: You cannot add the same server with different IP addresses.

To add a virtual management server:

1. In the left navigation pane, click **Virtual Management Server**.
2. Click on **+Add Virtual Management Server**. The Add Virtual Management Server page appears.
3. Enter the **IP address** or **Host name** of the virtual management server in the **IP/Host Name** field.
4. Select organization name from **Organizations** drop down list.
5. Enter the user credentials in the **User Name** and **Password** fields.
Optionally, you can use the **Test** button to verify the connection to the Server with provided credentials.
6. Enter the virtual management server port number in the **Port** field. The default port number is 443.

Note: Resiliency Director Collector requires the Alarms, Global, Network, Resource, Schedule task, vApp, and Virtual machine permissions for vCenter Server credentials. For more details, see [vCenterPermissions_collector.fm](#) on page 67.

7. Click **Save** to add the virtual management server.

The screenshot shows the 'Add Virtual Management Server' form within the Actifio Resiliency Director Collector interface. The form is titled 'Add Virtual Management Server' and is located under the 'VIRTUAL MANAGEMENT SERVER' tab. The form fields are as follows:

- IP/Host Name ***: vcenter08.rd.actifio.com
- Organizations**: Organization2 (selected from a dropdown menu)
- User Name ***: admin
- Password ***: [Redacted with asterisks]
- Port**: 443

There are three buttons: a blue 'Test' button next to the User Name field, a blue 'Save' button at the bottom right, and a blue 'Cancel' button next to the 'Save' button. The interface also shows a top navigation bar with 'Esc/UTC', 'admin', and a help icon. A left sidebar contains various icons for navigation.

Note: Configure a DNS server between the source and destination to permit you to add a server using its hostname.

Listing the Virtual Management Servers

To list the virtual management servers:

1. In the left navigation pane, click **Virtual Management Server**.

The list of available virtual management servers appears.

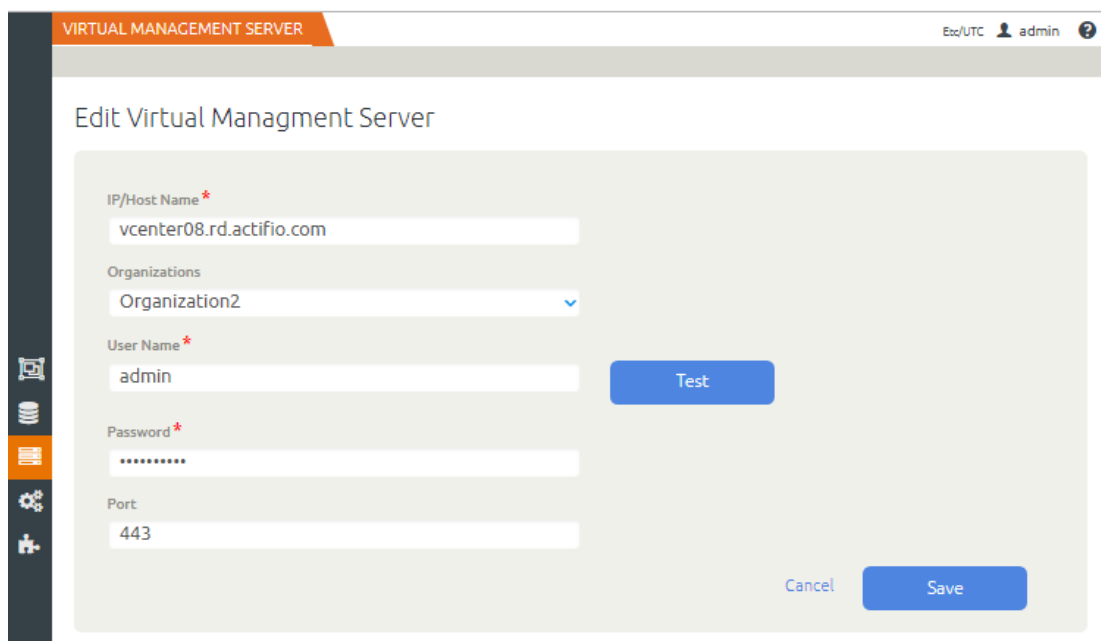
Virtual Management Servers Table - Field Elements

Field/Item	Description
IP/HOST NAME	Displays the hostname or the IP address of the server.
USER NAME	Displays the user name that is used to communicate with the server.
TYPE	Displays the type of the virtual server.
ORGANIZATION	Displays the organization name.
NO. OF RECOVERY PLANS	Displays the number of recovery plans for the server.

Modifying a Virtual Management Server

To edit a virtual management server:

1. In the left navigation pane, click **Virtual Management Server**. The list of available virtual management servers appears.
2. Select the virtual management server that you want to edit and then right-click and **Edit**. The **Edit Virtual Management Server** page appears.
3. Enter the **IP address** or **Host name** of the virtual management server in the **IP/Host Name** field.
4. Select the organization name from the **Organization** field.
5. Enter the user credentials in the **User Name** and **Password** fields.
Optionally, you can use the **Test** button to verify the connection to the Server with provided credentials.
6. Enter the virtual management server port number in the **Port** field. The default port number is 443.



The screenshot shows the 'Edit Virtual Management Server' interface. At the top, there's a header bar with 'VIRTUAL MANAGEMENT SERVER' on the left and 'Est/UTC', 'admin', and a help icon on the right. Below the header, the title 'Edit Virtual Management Server' is displayed. The form contains several fields: 'IP/Host Name' with the value 'vcenter08.rd.actifio.com', 'Organizations' with a dropdown menu showing 'Organization2', 'User Name' with the value 'admin', 'Password' with masked characters, and 'Port' with the value '443'. There is a blue 'Test' button next to the 'User Name' field. At the bottom right of the form, there are 'Cancel' and 'Save' buttons. A vertical navigation pane on the left side of the form contains icons for various system components.

7. Click **Save** to save the changes you have made. The modified details are listed in the available list of virtual management servers.

Deleting a Virtual Management Server

To delete a virtual management server:

1. In the left navigation pane, click **Virtual Management Servers**. The list of available virtual management servers appears.
2. Select the virtual management server(s) that you want to delete and then right-click and **Delete**. The **Delete Virtual Management Server** dialog box appears asking for the confirmation to delete the selected virtual management server.
3. Click **Yes** to delete the virtual management server.
Deleting a virtual management server also deletes the associated application groups and recovery plans.

DELETE VIRTUAL MANAGEMENT SERVER?

Deleting Virtual Management Server would delete all related Application Group(s).

Are you sure you want to delete the Virtual Management Server?

Cancel

Confirm

Note: You can delete multiple virtual management servers at a time. Use the **Ctrl** key (for Windows) or Command key (for Mac) to select multiple virtual management servers.

6 Adding and Managing Application Groups

An application group may consists of virtual machines or file systems or databases (SQL) that represent a logical unit of collectively functioning applications. When creating a recovery plan on the Actifio Resiliency Director Server, all the application groups present on the selected Actifio Resiliency Director Collector are fetched and are used in the recovery plan.

This chapter contains the following topics:

- [About Application Groups](#) on page 28
- [Adding an Application Group](#) on page 29
- [Listing Application Groups](#) on page 39
- [Modifying an Application Group](#) on page 41
- [Deleting an Application Group](#) on page 41

About Application Groups

Application groups can be created for different purposes like recovering VMs, recovering file systems and also recovering databases using different type of filters.

Use the filter type "Recover VM from VMware VM backup" for recovering VMs.

Use the filter type "Create new VM from VMware VM" for cloning VMs.

Use the filter type "Recover SQL Server Database" for recovering SQL server databases.

Use the filter type "Recover File System" for recovering file systems.

The below mentioned table describes the basic requirement for creating application groups:

Table 1: Adding Different Types of Applications in Application Groups

Application Group Type	Application Group Name	Actifio Appliance	Organization	Virtual Management Server	Filter by Type
VM Recovery	Required	Required	Optional	Required	Recover VM from VMware VM backup
VM Clone	Required	Required	Optional	Required	Create new VM from VMware VM
Recover Database (SQL)	Required	Required	Optional	Not Required	Recover SQL Server Database
Recover File System	Required	Required	Optional	Not Required	Recover File System

Note: Make sure that applications (VMs, vApps, File Systems, SQL Databases) are protected by DAR policy.

Adding an Application Group

Before adding an application group, ensure that Actifio Appliance user who wants to add an Application Group must have rights configured on the vCenter, Protected applications (*VMs, vApps, File Systems, SQL Databases*), Profile and template as well as ESX hosts. In order to create an application group, Actifio Appliance and vCenter must be a part of Resiliency Director and Actifio Appliance organization.

To add an application group:

1. In the left navigation pane, click **Application Groups**. The **Application Groups** page appears.
2. Click **+Add Application Group**. The **Application Group and Recovery Order** page appears.

APPLICATION GROUP AND RECOVERY ORDER

Application Group And Recovery Order

SELECTION AND ORDER | NAME AND RESOURCES | CONFIGURATION DETAILS

APPLICATION GROUP NAME *
HybridAG

ORGANIZATION
Organization1

ACTIFIO APPLIANCE(S) *
ACTSKY03.RD.ACTIFIO.COM, RDCDS3

VIRTUAL MANAGEMENT SERVER
172.29.11.174

FILTER BY TYPE *
Recover Filesystem

RECOVER VM FROM VMWARE VM BACKUP
CREATE NEW VM FROM VMWARE VM
RECOVER SQL SERVER DATABASE
RECOVER FILESYSTEM

/mnt/lv22 (rd-r...	File System	actsky03.rd...
/mnt/lv33 (rd-r...	File System	actsky03.rd...
/mnt/lv44 (rd-r...	File System	actsky03.rd...
/oracle/dbhom...	File System	rdcds3
/oradata (myho...	File System	rdcds3
/v1 (fs-rd-rhel75)	File System	rdcds3
/v2 (fs-rd-rhel75)	File System	rdcds3
/v3 (fs-rd-rhel75)	File System	rdcds3
E:\(actsq02.rd...	File System	rdcds3
F:\(actsq02.rd...	File System	rdcds3

ENTER SEQUENCE
5

ADD
REMOVE

SET RECOVERY ORDER

type to search...


SEQUENCE	Appliance
SEQUENCE: 1	
my-rhel75	rdcds3
SEQUENCE: 2	Delay 0 s
my-rhel75_1543571078596	rdcds3
SEQUENCE: 3	Delay 0 s
ACTSQL02 (actsq02.rd.acti...	rdcds3
SEQUENCE: 4	Delay 0 s
/v4 (fs-rd-rhel75)	rdcds3
C:\(actsq02.rd.actifio.com)	rdcds3

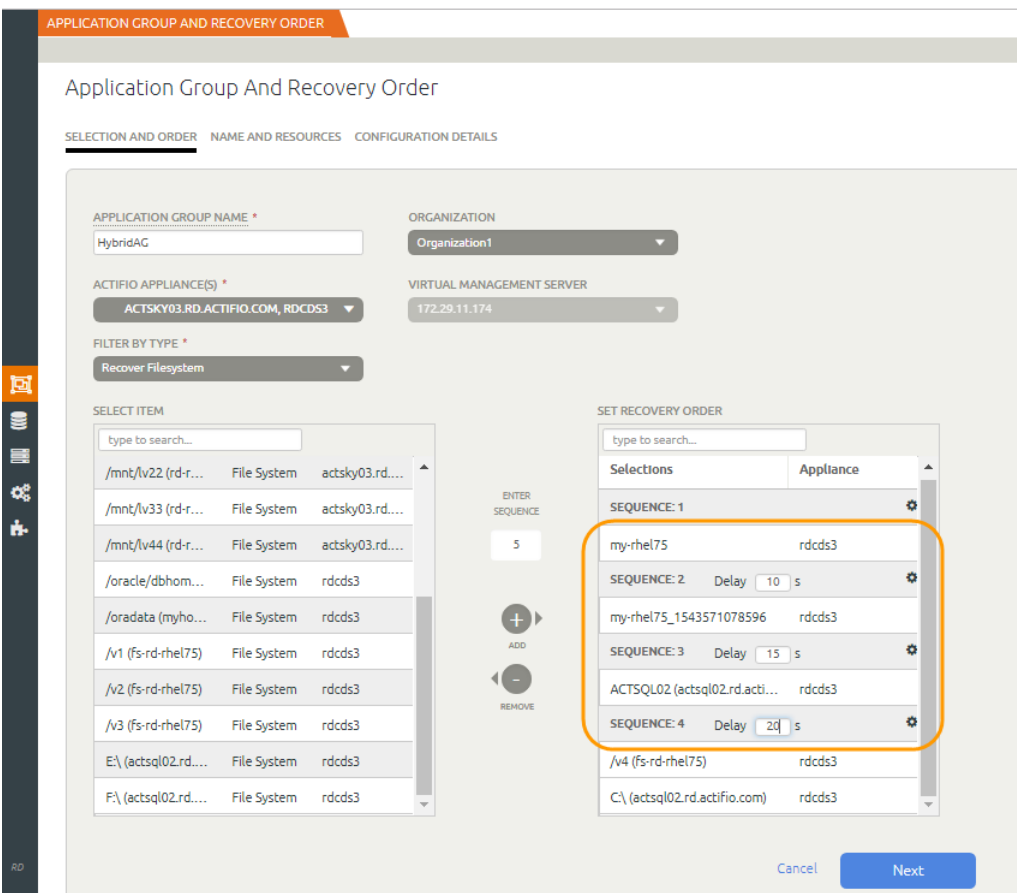
Cancel Next

3. Enter the application group name in the **Application Group Name** field. Only "-" and "_" special characters are supported.
4. Select single or multiple Actifio Appliance from the **Actifio Appliance(s)** drop-down list.
5. For VM recovery and VM cloning, select the virtual management server from the **Virtual Management Server** drop-down list.
6. Select the **Organization** from the Organization drop-down list.
7. Select the filter by type from the **Filter By Type** drop-down list.
 - o Use **'Recover VM from VMware VM backup'** option for recovering VMs.
 - o Use **'Create new VM from VMware VM'** option for cloning VMs.
 - o Use **'Recover SQL Server Database'** option for recovering SQL server databases.
 - o Use **'Recover File System'** option for recovering file systems.

8. Select single or multiple applications (VMs, vApps, File Systems, SQL Databases), and then enter the sequence number (1, 2, 3, and so on) in the Sequence Input Box to define the recovery order.

Note: The sequence number cannot be zero or negative, applications (VMs, vApps, File Systems, SQL Databases), present in the same sequence are recovered in parallel at the time of recovery plan execution.

9. Click the  icon to add the selected applications (VMs, vApps, File Systems, SQL Databases), in the Set Recovery Order pane. The Set Recovery Order pane lists the added applications (VMs, vApps, File Systems, Databases), in an ascending order (Sequence 1, Sequence 2, and so on). You can redefine the recovery order.
10. (Optional) Specify the time delay in seconds. Delay is the specified time interval that is introduced in between two sequences to pause the recovery. By default 0 seconds delay is set. For example, If you configure a delay of 10 seconds to Sequence 3 then at the time of recovery plan execution, after completing the recovery of Sequence 2, Resiliency Director will pause the recovery for 10 seconds before starting the recovery of Sequence 3.



APPLICATION GROUP AND RECOVERY ORDER

Application Group And Recovery Order

SELECTION AND ORDER | NAME AND RESOURCES | CONFIGURATION DETAILS

APPLICATION GROUP NAME *
HybridAG

ORGANIZATION
Organization1

ACTIFIO APPLIANCE(S) *
ACTSKY03.RD.ACTIFIO.COM, RDCDS3

VIRTUAL MANAGEMENT SERVER
172.29.11.174

FILTER BY TYPE *
Recover Filesystem

SELECT ITEM

type to search...		
/mnt/lv22 (rd-r...	File System	actsky03.rd...
/mnt/lv33 (rd-r...	File System	actsky03.rd...
/mnt/lv44 (rd-r...	File System	actsky03.rd...
/oracle/dbhom...	File System	rdcds3
/oradata (myho...	File System	rdcds3
/v1 (fs-rd-rhel75)	File System	rdcds3
/v2 (fs-rd-rhel75)	File System	rdcds3
/v3 (fs-rd-rhel75)	File System	rdcds3
E:\ (actsql02.rd...	File System	rdcds3
F:\ (actsql02.rd...	File System	rdcds3

ENTER SEQUENCE
5

ADD
REMOVE

SET RECOVERY ORDER

type to search...	Appliance
SEQUENCE: 1	
my-rhel75	rdcds3
SEQUENCE: 2	Delay 10 s
my-rhel75_1543571078596	rdcds3
SEQUENCE: 3	Delay 15 s
ACTSQL02 (actsql02.rd.acti...	rdcds3
SEQUENCE: 4	Delay 20 s
/v4 (fs-rd-rhel75)	rdcds3
C:\ (actsql02.rd.actifio.com)	rdcds3

Cancel Next

11. Click **Next**.

If the application group contains VMs, the **Name and Resources** page appears.

APPLICATION GROUP AND RECOVERY ORDER

Enz/UTC admin ?

Application Group And Recovery Order

SELECTION AND ORDER NAME AND RESOURCES CONFIGURATION DETAILS

APPLICATION GROUP : HYBRIDAG

☐ ENABLE APPLICATION GROUP SCRIPTS

CRITICAL	NAME / vAPP(s)	CPU(vCPUs)						MEMORY(MB)	
		Actual Recovery			Test Recovery			ACTUAL RECOVERY	TEST RECOVERY
		SOCKETS	CORES / SOCKETS	TOTAL CORES	SOCKETS	CORES / SOCKETS	TOTAL CORES		
<input type="checkbox"/>	my-rhel75	2	1	2	<input type="text" value="2"/>	<input type="text" value="1"/>	2	2048	<input type="text" value="2048"/>
<input type="checkbox"/>	<input type="text" value="my-rhel75_154"/>	2	1	2	<input type="text" value="2"/>	<input type="text" value="1"/>	2	2048	<input type="text" value="2048"/>

Cancel
Back
Next

12. (Optional) Click the **Enable Application Group Scripts** check box and provide respective details if you want to execute Failover script and Reset script at application group level. For more information on Failover script and reset script, see [Failover-script](#) and [Reset-script](#) on page 38.
13. Provide the details as described in [Setting the VM Parameters](#) section for defining the resource pool.

Note: On the Scripts and VM Settings page, you may see some virtual machines in RED color. These virtual machines are invalid virtual machines. This means these virtual machines cannot be added to an application group. A virtual machine can be invalid if IP Address or Host name is not present for particular virtual machine.

14. Click **Next**.
 15. The Configuration Details page list the Application Name, Type and the Configuration status. By default, the configuration status is set to optional.
- If application group contains VMs and in order to configure a VM, see [Configuring the VM](#) on page 33.

Note: The selected virtual machine cannot get valid IP address or host name if VMware tools are not installed on the same virtual machine.

If application group contains file systems and in order to configure a file system, see [Configuring the file system](#) on page 35.

Note: The file system can be configured while creating Application Group or while creating/editing Recovery Plan.

If application group contains databases (SQL) and in order to configure a file system, see [Configuring the database](#) on page 36.

16. Click **Finish** to add an application group.


Note: You cannot add the same virtual machine to more than one application group.

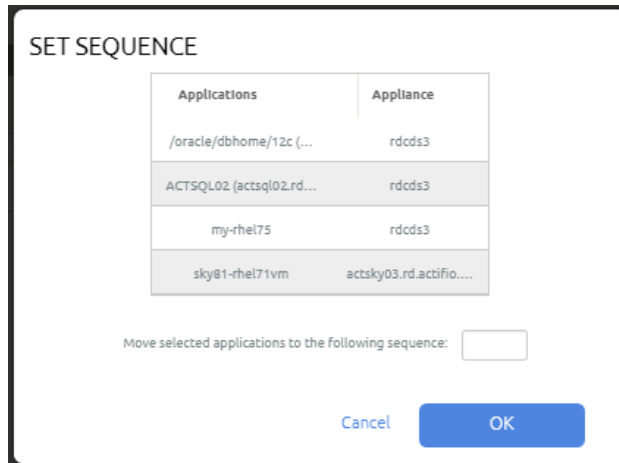
Note: When a virtual application vApp1 has three virtual machines such as vApp1-TVM1, vApp1-TVM2, and vApp1-TVM3, where vApp1-TVM1 is an invalid virtual machine. Then this application group becomes invalid. And if you run a recovery plan for this application group, then corresponding recovery plan will fail. This issue occurs due to vApps having inconsistent virtual machines, that does not recover properly on the Resiliency Director Server site. You must ensure that only valid virtual machines are included in the application group to run the recovery plan successfully.

Setting the recovery order

This section describes how to redefine the recovery order of VMs or vApps.

To set the recovery order:

1. In the **Set Recovery Order** pane, click the  icon for sequence of which you want to redefine the recovery order. The **Set Sequence** dialog box appears.
2. Select single or multiple VMs or vApp and enter the sequence number in **Apply following sequence to all VMs** input box.
3. When you click **OK**, the selected VMs or vApp are then moved under the new sequence. You can view the changes in the Set Recovery Order pane.



The dialog box titled "SET SEQUENCE" contains a table with two columns: "Applications" and "Appliance". The table lists four entries. The second entry, "ACTSQL02 (actsql02.rd...", is highlighted. Below the table is a text input field labeled "Move selected applications to the following sequence:". At the bottom right are "Cancel" and "OK" buttons.

Applications	Appliance
/oracle/dbhome/12c (...)	rdcds3
ACTSQL02 (actsql02.rd...	rdcds3
my-rhel75	rdcds3
sky81-rhel71vm	actsky03.rd.actifio...

Move selected applications to the following sequence:

Cancel OK

Setting the VM Parameters

This section describes the various parameters of a VM or vApp.

On the Scripts and VM Settings page, you may see some virtual machines in RED color. These virtual machines are invalid virtual machines. This means these virtual machines cannot be added to an application group. A virtual machine can be invalid if IP Address or Host name is not present for particular virtual machine.

The following table provides the details of the VM parameters for application groups.

VM SettingsTable - Field Elements

Field/Item	Description
Is Critical	Select the VM to define it as critical. For example, if recovery fails for a VM that is marked as critical, the recovery plan halts and the status of the recovery plan is marked as Failed . If the critical VM recovery passes, then the status of the recovery plan is marked as Success . If the recovery passes for a VM that is marked as critical, but fails for the other VMs, then the recovery plan continues the execution. The status of the recovery plan is marked as Partial Success .
Name/vApp(s)	Click the virtual machine name to configure the VM. The details to configure a VM are described in the section Configuring the VM on page 33.
Actual Recovery	CPU (MHz): Indicates the CPU details that Resiliency Director uses for actual recovery. Memory (MB): Indicates the MB that Resiliency Director uses for actual recovery.
Test Recovery	CPU (MHz): Enter the virtual CPU sockets and cores/socket details that Resiliency Director uses for test recovery. This value cannot be zero or negative, and the value test recovery must be less than or equal to the actual recovery value. Memory (MB): Enter the memory size in MB that Resiliency Director uses for test recovery. This value cannot be zero or negative, and the value test recovery must be less than or equal to the actual recovery value.

Configuring the VM

To configure a VM:

Note: In order to configure a VM, VMware tools must be installed and running on the selected virtual machine.

1. On the **Configuration Details** page, click on **Optional** for the VM you want to configure, the **Configure VM** page appears. By default, configuration status is set to **Optional**. After configuring the VM the status will be changed as Configured.
2. On Configure VM page, select the VM credentials from the **Credentials** drop-down list. if the VM credentials are not available, use **Add New** option and provide the details for Name, User Name and Password fields and click **Save** to add the VM credentials.

3. Select the scripts type (Failover-script and Reset-Script) from the drop-down list and enter the absolute path of the scripts in the **Failover -Script** and **Reset-Script** field respectively. The scripts must be accessible to the VM. The details about the scripts are described in the section [Failover-script and Reset-script](#) on page 38.
4. In Network Settings section:
 - o Select **Keep Current Settings** option if you do not wish to modify the network information. If you want to retrieve the default VM settings, click Retrieve Current Settings.
 - o Select **Change Network Settings** option if you wish to modify the network information.
 - o Enter the IP address of DNS server(s) in the **DNS** field.
 - o If you wish to set the IP address as Static or Dynamic change the allocation type. If you select Static IP address, provide the values for IP address, Subnet and Gateway.
5. Enter the user name and password in the respective fields.

Note: If you want to retrieve the default VM settings, click **Retrieve Current Settings**.

6. Click **Save** to update the changes. The VM is configured.

APPLICATION GROUP AND RECOVERY ORDER

Application Group And Recovery Order

SELECTION AND ORDER NAME AND RESOURCES CONFIGURATION DETAILS

Configure VM: Rh75fs

CREDENTIALS * (Required if any scripts are to be specified, or if network settings are being changed.)

linux [Add New](#)

▼ Scripts

SCRIPT	TYPE	SCRIPTS
FAILOVER SCRIPT	shell	/tmp/failover.sh
RESET SCRIPT	shell	/tmp/reset.sh

▼ New Host Information

HOST NAME*

rh75fs

▼ Network Settings

☐ Keep Current Settings ☒ Change Network Settings

DNS

NETWORK INTERFACE LABEL	ACTION	CURRENT TYPE	IP ADDRESS	SUBNET	GATEWAY
Network adapter 1	Do not change Static Dynamic Change				

Cancel Save

Configuring a VM

Configuring the file system

To configure a file system:

1. On the **Configuration Details** page, click on Required for the **File System** application you want to configure, the **Configure File System** page appears. By default, configuration status is set to Required. After configuring the File System Application, the status will be changed as Configured.
2. On **Configure File System** list or enter target host name in the provided text box.
3. For **Scripts** Section, enter the values for Scripts (PRE-SCRIPT and POST-SCRIPT) and Time Out value in seconds. These values are optional.
4. For **Mount Locations**, you may change the default mount location.

The screenshot shows the 'Configure Filesystem' page for '/Fs1 (Fs-Rd-Rhel74)'. The page is part of the 'APPLICATION GROUP AND RECOVERY ORDER' section. It has three tabs: 'SELECTION AND ORDER', 'NAME AND RESOURCES', and 'CONFIGURATION DETAILS', with the last one being active. The configuration is for a 'File System' application. The 'TARGET' field is set to 'fsrv4.rd.actifio.com'. Under the 'Scripts' section, both 'PRE-SCRIPT' and 'POST-SCRIPT' are set to '/fsapp/pre.sh', and both have a 'TIMEOUT' of 60 seconds. Under the 'Mount Locations' section, there is a table with 'SOURCE' and 'MOUNT LOCATION' columns. The 'SOURCE' is '/fs1' and the 'MOUNT LOCATION' is '/recoveredfs1'. At the bottom right, there are 'Cancel' and 'Save' buttons.

APPLICATION GROUP AND RECOVERY ORDER

Application Group And Recovery Order

SELECTION AND ORDER NAME AND RESOURCES CONFIGURATION DETAILS

Configure Filesystem : /Fs1 (Fs-Rd-Rhel74)

TARGET *
<< TBD >> fsrv4.rd.actifio.com

▼ Scripts

PRE-SCRIPT /fsapp/pre.sh TIMEOUT 60 s
POST-SCRIPT /fsapp/pre.sh TIMEOUT 60 s

▼ Mount Locations

SOURCE	MOUNT LOCATION
/fs1	/recoveredfs1

Cancel Save

Configuring a File System

5. Click **Save** to save the changes. The File System is configured.

Note: The target can be specified while creating Application Group or later while creating the Recovery Plan.

Configuring the database

Note: This release provides the support for Microsoft SQL databases only.

To configure a database:

1. On the **Configuration Details** page, click on Required for the SQL application you want to configure, the **Configure Database** page appears. By default, configuration status is set to Required. After configuring the database, the status will be changed as Configured.
2. On **Configure Database** page, You can select the TARGET host from the TARGET drop-down list or enter a target host name in provided text box.
3. For **Scripts** Section, enter the values for Scripts (PRE-SCRIPT and POST-SCRIPT) and TIMEOUT values in seconds. These values are optional.
4. For **Application Options**:
 - o By default CREATE NEW VIRTUAL DATABASE is selected.
 - o Selected databases will be included for recovery if you choose **Included** option from the drop-down. You may exclude the databases for recovery using **Excluded** option from the drop down.
 - o You can select list of database(s) from the table using the appropriate check-boxes or using the search option.
 - o If you select single/multiple databases, SQL Server Instance name will be populated automatically if the selected target VM / host has SQL instance running. Otherwise you need to provide the name for SQL SERVER INSTANCE NAME. This is required parameter.
 - o When multiple database are selected, UI provides one more option "NAME OF CONSISTENCY GROUP". Provide the name, this is also required parameter when multiple database are selected.
 - o Provide values for following Advanced Options (optional):
 - o PREFIX FOR SQL SERVER DATABASE NAME
 - o SUFFIX FOR SQL SERVER DATABASE NAME
 - o RECOVER DATABASE AFTER RESTORE
 - o RECOVER USER LOGINS
 - o USERNAME
 - o PASSWORD

APPLICATION GROUP AND RECOVERY ORDER

Application Group And Recovery Order

SELECTION AND ORDER NAME AND RESOURCES CONFIGURATION DETAILS

Configure Database(s) : ACTSQL06\ACTSQLSERVER (Actsqli06.Rd.Actifio.Com)

TARGET *
 << TBD >> << Select Target >>

Scripts

Application Options

CREATE NEW VIRTUAL DATABASE ☒

SELECTED DATABASES WILL BE Included

Type to search... 21 SHOW SELECTED (4)

SELECT ITEMS

- ☐ master
- ☐ model
- ☐ msdb
- ☐ ReportServer\$ACTSQLSERVER
- ☐ ReportServer\$ACTSQLSERVERTempDB
- ☒ TestDot1

1 of 1 page

NAME OF CONSISTENCY GROUP * Testdbog

SQL SERVER INSTANCE NAME * sqlym

Advanced Options

PREFIX FOR SQL SERVER DATABASE NAME 30_

SUFFIX FOR SQL SERVER DATABASE NAME _30

RECOVER DATABASE AFTER RESTORE ☒

RECOVER USER LOGINS ☐

USER NAME

PASSWORD

Cancel Save

Configuring a Database

- After providing the required information, click **Save** to save the database configuration.

First Sequence script and Last Sequence script

Resiliency Director supports adding and executing first sequence script and last sequence script. The following section describes the script execution details at the application group and VM level.

Note: Ensure that the added script is present on the selected virtual machine.

Executing Scripts at Application Group Level

Resiliency Director executes first sequence script and last sequence scripts and reset scripts at the application group level. You can add the scripts while creating an application group.

For example, an application group *AG1* has two VMs, *VM1* and *VM2* with the respective startup sequence. The prescript specified with the absolute path should be present at the mentioned location on *VM1*.

The first sequence script executes after *VM1* is up on priority over any other VM specific script. Similarly, the postscript specified with the absolute path should be present at the mentioned location on the last VM that comes in *AG1*, such as *VM2*. The last sequence script executes after *VM2* is powered ON during the recovery plan execution. It executes after any VM specific script is provided.

Failover-script and Reset-script

Resiliency Director supports adding and executing failover scripts and reset scripts. The following section describes the script execution details at the application group and VM level.

Note: Ensure that the added script is present on the selected virtual machine.

Executing Scripts at VM Level

Resiliency Director supports adding failover scripts and reset scripts at the VM level. The scripts execute when the VM is recovered or reset.

Note: You should provide the correct VM User Name and Password for script execution, else the VM recovery fails. You can verify the failure details by viewing the Resiliency Director operation logs.

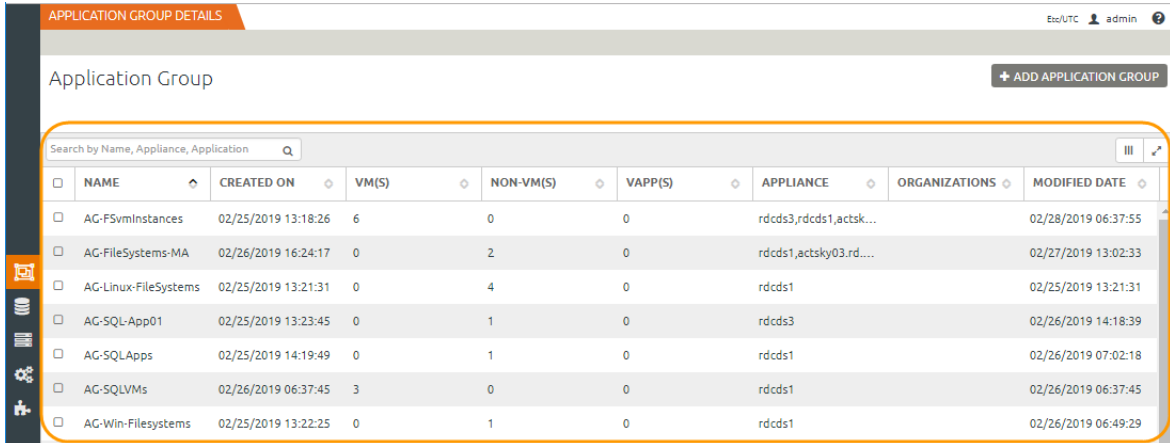
Listing Application Groups

All the created application groups are listed for a Resiliency Director Collector site. The Resiliency Director lists application groups only after they are added to a recovery plan.

To list the application groups:

1. In the left navigation pane, click **Settings > Application Groups**.

The list of available application groups appears as shown below.



<input type="checkbox"/>	NAME	CREATED ON	VM(S)	NON-VM(S)	VAPP(S)	APPLIANCE	ORGANIZATIONS	MODIFIED DATE
<input type="checkbox"/>	AC-F5vmInstances	02/25/2019 13:18:26	6	0	0	rdcds3,rdcds1,actsk...		02/28/2019 06:37:55
<input type="checkbox"/>	AC-FileSystems-MA	02/26/2019 16:24:17	0	2	0	rdcds1,actsky03.rd...		02/27/2019 13:02:33
<input type="checkbox"/>	AC-Linux-FileSystems	02/25/2019 13:21:31	0	4	0	rdcds1		02/25/2019 13:21:31
<input type="checkbox"/>	AC-SQL-App01	02/25/2019 13:23:45	0	1	0	rdcds3		02/26/2019 14:18:39
<input type="checkbox"/>	AC-SQLApps	02/25/2019 14:19:49	0	1	0	rdcds1		02/26/2019 07:02:18
<input type="checkbox"/>	AC-SQLVMs	02/26/2019 06:37:45	3	0	0	rdcds1		02/26/2019 06:37:45
<input type="checkbox"/>	AC-Win-Filesystems	02/25/2019 13:22:25	0	1	0	rdcds1		02/26/2019 06:49:29

2. Click the application group name to view the following details of the selected group.

Application Groups Table - Field Elements

Field/Item	Description
NAME	Displays the application group name.
CREATED ON	Displays the date when the application group was created.
VM(S)	Displays the number of VM(s) in the application group.
NON- VM(S)	Displays the number of NON-VM(s) in the application group
VAPP(S)	Displays the number of vApps in the application group.
APPLIANCE	Displays the name of the appliance configured for the application group.
ORGANIZATIONS	Displays the name of the organization configured for the application group.
MODIFIED DATE	Displays the date when the application group details were last edited.





Details of the Selected Application Group

Field/Item	Description
APPLICATION	Name of the application (VM/SQL Database/File system)
SEQUENCE	Order of the recovery you have set
VCPU	Number of CPUs in the selected application group
MEMORY (MB)	Memory size of the selected application group.
NICS	Number of NICs in the selected application group.
TARGET	Desired name in case of VM recovery, desired host name in case of application recovery.
APPLIANCE	Name of the Actifio Appliance.
Memory (MB)	Displays the memory size of the selected application group.

Modifying an Application Group

Resiliency Director supports modifying the recovery order of an application group. You can modify the properties of the selected VMs under an Application Group such as CPU, memory, and IP address.

To modify an application group:

1. In the left navigation pane, click **Settings > Application Groups**. The list of available application groups appears.
2. Select the application group that you want to modify and click **Edit**. The **Edit Application Group** page appears.
3. Modify the application group name, if required.
4. Modify the recovery order using   or   icon by adding or removing the VMs or vApps in the Set Recovery Order pane.
5. (Optional) Modify the time delay in seconds. Delay is the specified time interval that is introduced in between two sequences to pause the recovery. By default 0 seconds delay is set.
6. Click **Next**. The **Selection and Order** page appears. You may change the Application name if required for the VM instance.
7. (Optional) Click the **Enable Application Group Scripts** check box and provide respective details if you want to execute first sequence script and last sequence script. For more information on scripts, see [Failover-script and Reset-script](#) on page 38.
8. Provide the details as described in [Setting the VM Parameters](#) section for defining the resource pool.
9. (Optional) Configure the VM. To configure a VM, see [Configuring the VM](#) on page 33.
10. (Optional): If the Application Group contains the File System. To configure a file system, see [Configuring the file system](#) on page 35
11. (Optional): If the Application Group contains the SQL Database. To configure a SQL Database, see [Configuring the database](#) on page 36
12. Click **Finish** to save the changes.

Note: You cannot modify an Actifio Appliance and virtual management server fields.

Deleting an Application Group

To delete an application group:

1. In the left navigation pane, click **Settings > Application Groups**. The list of available application groups appears.
2. Select the application group that you want to delete and click **Delete**. The **Delete Application Group** dialog box appears.
3. Click **Yes** to delete the selected application group.
When application group is part of a recover plan, user would not be able to delete the Application Group.

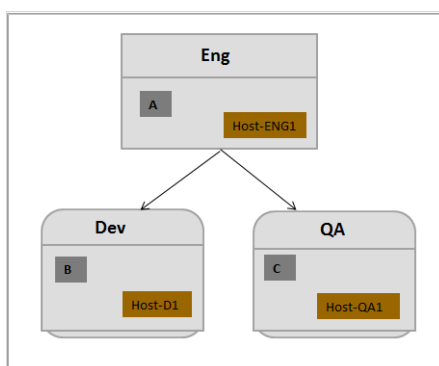
Note: You can delete multiple application groups at a time. Use the **Ctrl** key to select multiple application groups. You cannot delete an application group which is part of a recovery plan.

7 Creating and Managing Organizations

This chapter contains the following topics:

- [Creating an Organization](#) on page 44
- [Editing the Organization Details](#) on page 46
- [Deleting Organization\(s\)](#) on page 47

Organizations and Roles work together to enforce rules set up by Actifio Appliance administrators for users. Organization membership governs which users can access/manage their corresponding resources within an Actifio Appliance. Roles govern what actions users can take on the resources under their control. Organizations can be defined in a hierarchical fashion to match your organizational structure.



Organizations and their access relationships

In this figure, there are three organizations: **Eng**, **Dev**, and **QA**.

- User **A**, **Host-ENG1**, **Dev** and **QA** are the resources of organization **ENG**.
- User **B** and **Host-D1** are the resources of organization **Dev**.
- User **C** and **Host-QA1** are the resources of organization **QA**.
- User **A** can access all the hosts.
- User **B** can access **Host-D1** and cannot access other hosts.
- User **C** can access **Host-QA1** and cannot access other hosts.

An organization can have multiple dependents but only one parent organization. Circular reference of dependent organizations is not allowed.

Actifio Appliance Organizations

An Actifio Appliance provides two predefined organizations: ALL and PUBLIC. You can create other organizations as needed.

ALL: All Actifio Appliance resources of types other than user are resources of this organization. A user added to the organization “ALL” has access to every Actifio Appliance resource (this is usually reserved for administrators).

PUBLIC: Every Actifio Appliance user is a member of this organization. Every Actifio Appliance user has access to an Actifio Appliance resource (of type other than user) added to organization “PUBLIC”.

Creating an Organization

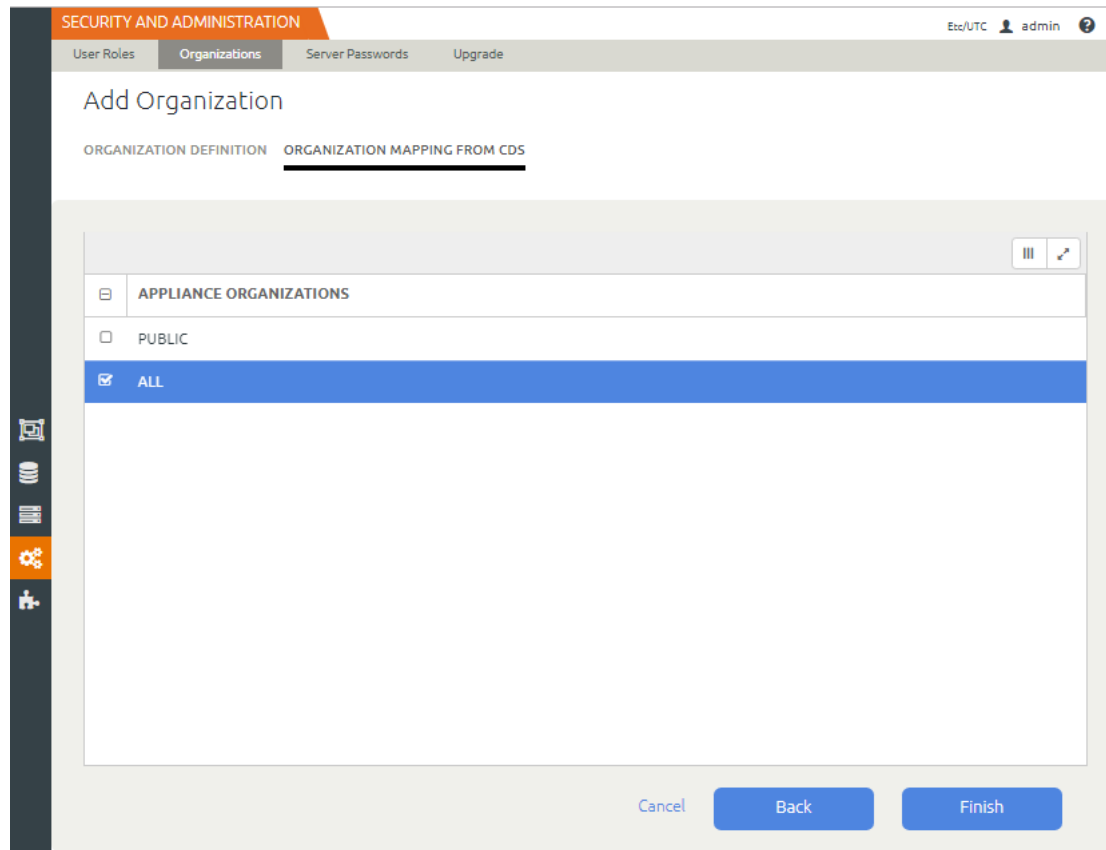
To create an Organization:

1. Click **Settings > Security & Administration > Organizations**. The **Organizations** page displays.
2. Click **+ADD ORGANIZATION** to create a new organization.
3. Enter the **Organization Name**.

The screenshot shows the 'Add Organization' form within the 'SECURITY AND ADMINISTRATION' section. The form has two tabs: 'ORGANIZATION DEFINITION' (selected) and 'ORGANIZATION MAPPING FROM CDS'. The 'NAME' field contains 'ORGFIN' and the 'DESCRIPTION' field contains 'Finance'. The 'CHILD OF' section contains a table with two rows: 'Name' mapped to 'Mapped Appliance Organizations' and 'OrgSales' mapped to 'ALL, PUBLIC, ALL'. The 'OrgSales' row is highlighted in blue. At the bottom right, there are 'Cancel' and 'Next' buttons.

CHILD OF	
<input checked="" type="checkbox"/> Name	Mapped Appliance Organizations
<input checked="" type="checkbox"/> OrgSales	ALL, PUBLIC, ALL

4. Enter the organization **Description**.
5. Select the child-of organizations that should be dependents of the new organization in the **CHILD -OF** section.
6. Click **Next**.



7. Select the check-boxes for existing appliance that should be configured for the new organization, and click **Finish**.

Editing the Organization Details

The Resiliency Director Collector supports modifying the name, description, mapped appliance organizations and of an organization.

To edit the organization details:

1. Click **Settings > Security & Administration > Organizations**. The **Organizations** page displays.
2. Select the organization that you want to edit and click **Edit**. The **Edit Organization** page appears.

SECURITY AND ADMINISTRATION

User Roles Organizations Server Passwords Upgrade

Etc/UTC admin ?

Add Organization

ORGANIZATION DEFINITION ORGANIZATION MAPPING FROM CDS

NAME *

ORGFIN

DESCRIPTION

Finance

CHILD OF

<input checked="" type="checkbox"/>	Name	Mapped Appliance Organizations
<input checked="" type="checkbox"/>	OrgSales	ALL, PUBLIC, ALL

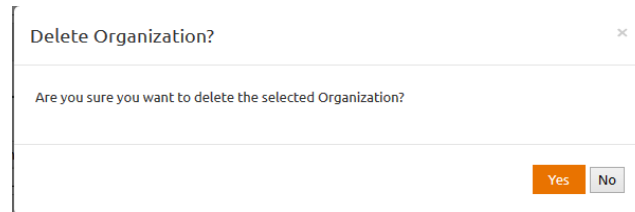
Cancel Next

3. Edit the **Organization Details**:
 - o Name
 - o Description
 - o Mapped Appliance Organizations
4. Select the **Appliance Organizations** name check box.
5. Click **Finish** to save the changes.

Deleting Organization(s)

To delete a organization:

1. Click **Settings > Security & Administration > Organizations**. The **Organizations** page displays.
2. Select the organization that you want to edit and click **Delete**. The **Delete Organization** dialog box appears asking for the confirmation to delete the organization.



3. Click **Yes** to delete the organization.
Deleting an organization also deletes the entities associated with the organization such as, Actifio Resiliency Director Collectors and its associated recovery plans.

Note: You can delete multiple organization at a time. Use the **Ctrl** key to select multiple organization.

8 Managing Server Passwords

This chapter provides information on how to add credentials, which can be used to configure the VM.

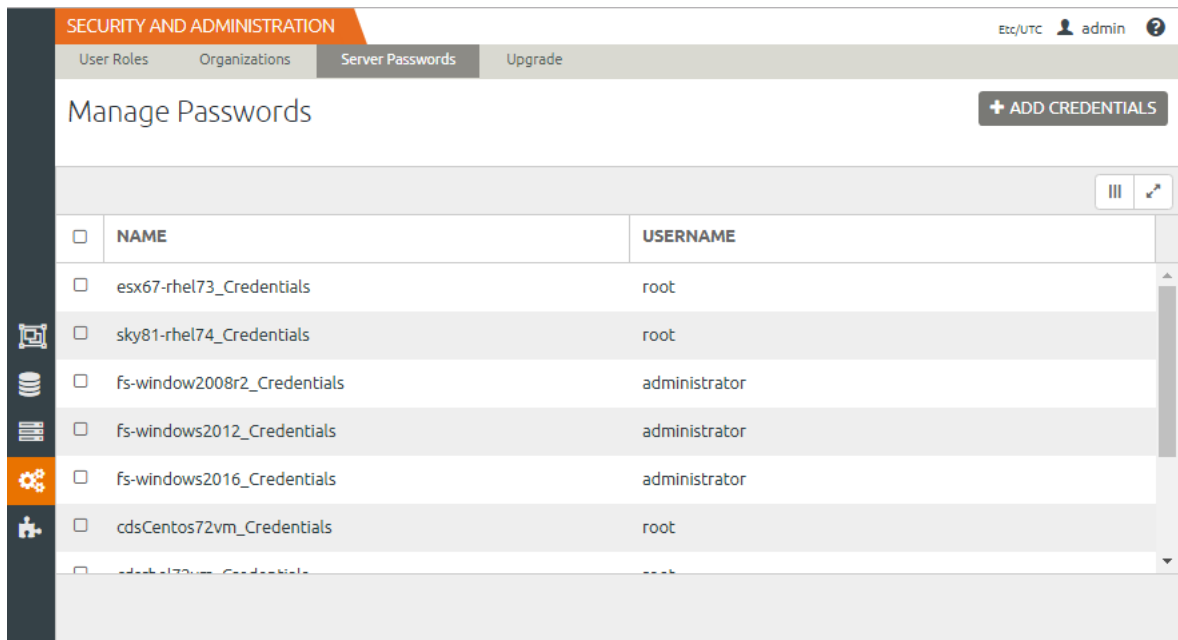
Listing the Server Passwords

To list the Resiliency Director Server details, click **Security & Administration** and then select **Server Passwords**. The list of available credentials appears.

Resiliency Director Manage Passwords Table - Field Elements

Field/Item	Description
Name	Displays the server credentials name.
User Name	Displays the user name being used in the credentials.

List of available server passwords:



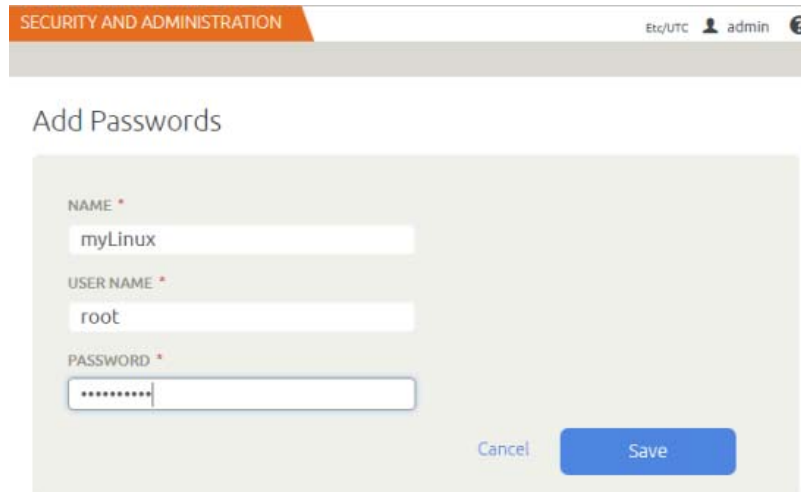
SECURITY AND ADMINISTRATION	
User Roles	Organizations
Server Passwords	Upgrade
Manage Passwords	
+ ADD CREDENTIALS	
NAME	USERNAME
esx67-rhel73_Credentials	root
sky81-rhel74_Credentials	root
fs-window2008r2_Credentials	administrator
fs-windows2012_Credentials	administrator
fs-windows2016_Credentials	administrator
cdsCentos72vm_Credentials	root

Actifio Resiliency Director Collector - Listing Server Passwords

Adding the Server Passwords

To add a server password:

1. Click on **+Add Credentials**. The **Add Passwords** page appears.



The screenshot shows the 'Add Passwords' form within the 'SECURITY AND ADMINISTRATION' section. The form has three input fields: 'NAME *' with the value 'myLinux', 'USER NAME *' with the value 'root', and 'PASSWORD *' with a masked password '*****'. There are 'Cancel' and 'Save' buttons at the bottom right.

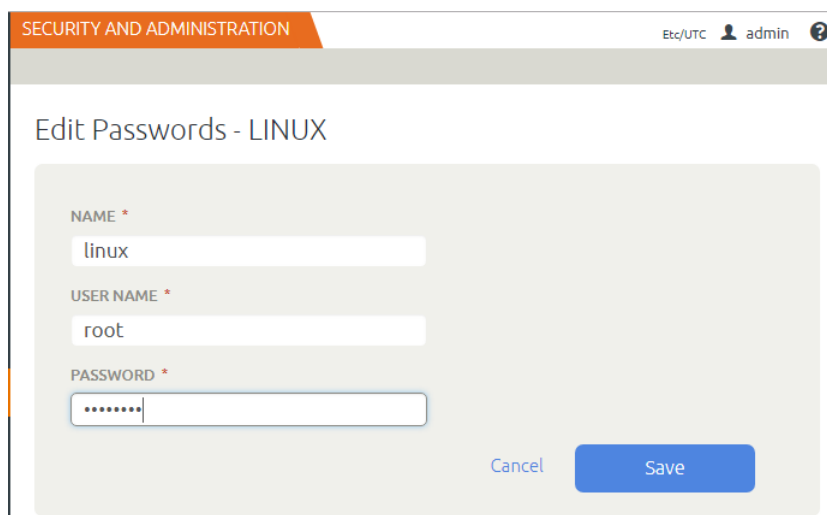
Actifio Resiliency Director Collector - Add Server Passwords

2. Enter the name, user name and password for the credentials in the respective fields.
3. Click **Save** to update the changes.

Editing the Server Passwords

To modify a server password:

1. On Manage Passwords page, right-click on credentials record and select **Edit**. The **Edit Passwords** page appears.



The screenshot shows the 'Edit Passwords - LINUX' form. It has three input fields: 'NAME *' with the value 'linux', 'USER NAME *' with the value 'root', and 'PASSWORD *' with a masked password '*****'. There are 'Cancel' and 'Save' buttons at the bottom right.

Actifio Resiliency Director Collector - Edit Server Passwords

2. Update the name or user name or password for the credentials in the respective fields.
3. Click **Save** to update the changes.

Deleting the Server Passwords

To remove a server password:

1. On Manage Passwords page, right-click on credentials record and select **Delete**. The Delete User Credentials dialog appears.
2. Click **Confirm** to remove the credentials.

9 Viewing the Actifio Resiliency Director Server Details

This chapter describes the Actifio Resiliency Director Server details.

As soon as the CSP administrator adds Resiliency Director Collector on Resiliency Director Server, you can view the paired Resiliency Director Server details on Collector.

Viewing the Actifio Resiliency Director Server Details

To view the Resiliency Director Server details, click **Settings** then **RD Server**. The **RD Servers** details are displayed.



Actifio Resiliency Director - Server Information

10 Adding and Managing User Access Control

An Actifio Resiliency Director allows you to create and manage multiple user access controls. This chapter describes how to create and manage various types of user access controls by assigning rights. Controls correlate with groups of users that share similar responsibilities and have similar requirements when using the Actifio Resiliency Director. Permissions are assigned to roles to grant or deny access to various features.

This chapter contains the following topics:

- [Creating roles and assigning permissions](#) on page 57
- [Modifying roles and changing permissions](#) on page 58
- [Deleting roles](#) on page 59

All user access controls in the Actifio Resiliency Director are managed by the user roles. Following are the roles associated with the user access rights:

Roles	Description	Associated Rights
RD Admin	Administrator role	Appliance Manage, Appliance View, Server View, Application Group View, Application Group Manage, Virtual Management Server Manage, Virtual Management Server View, Upgrade Manage, Upgrade View, Manage Authentication Source, Server Manage, Organization Manage, Organization View
RD Manage	Basic role	Appliance Manage, Server View, Application Group View, Virtual Management Server View, Upgrade View, Server Manage, Organization Manage, Application Group Manage, Virtual Management Server Manage, Manage Authentication Source
RD View	View only	Appliance View, Server View, Application Group View, Virtual Management Server View, Upgrade View, Organization View

Types of User Access Controls:

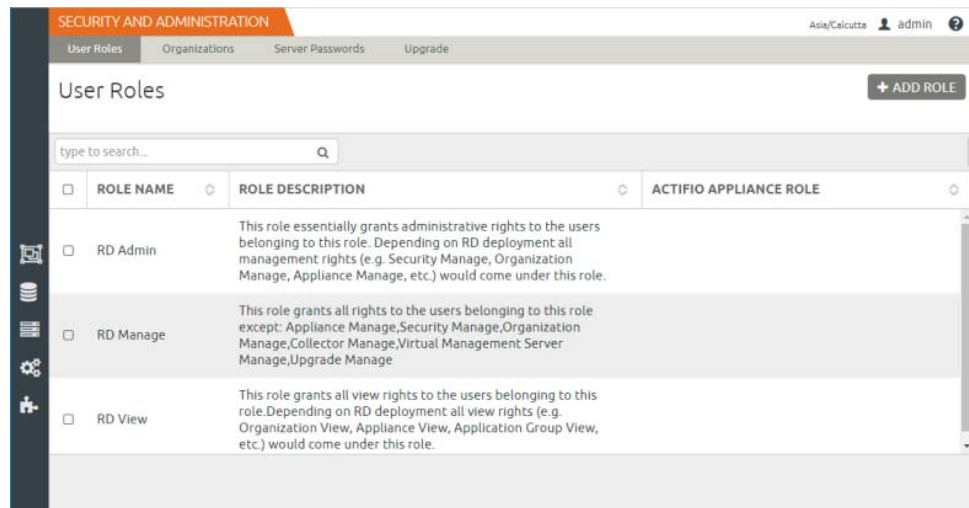
User Access Rights	Description
Appliance Manage	Allows user to perform create, read, update, and delete operations on the Actifio Appliance entity.
Appliance View	Allows user to view the Actifio Appliance entity.
Application Group Manage	Allows user to perform create, read, update, and delete operations on Application Group entity
Application Group View	Allows user to view the operations performed on Application Group entity.
Download RD Logs	Allow user to download RD logs.
Organization Manage	Allows user to perform create, read, update, and delete operation of an organization.
Organization View	Allows user to view the operation performed for an organization.
Security Manage	This user can assign roles to users, and can assign rights to roles. All users on appliance are available to be assigned roles, even if they have never logged-in to RD.
Security View	This user can view roles to users and rights associated to the roles.
Server Manage	Allow RD server to register/unregister on Collector.
Server View	Allows user to view the Actifio Resiliency Director Server entity.
Upgrade Manage	Allows user to perform create, read, update, and delete operations on Upgrade entity.
Upgrade View	Allows user to view operations performed on Upgrade entity.
Virtual Management Server Manage	Allows user to perform create, read, update, delete operations on Virtual Management Server entity.
Virtual Management Server View	Allows user to view operations performed on the Virtual Management Server entity.
Manage Authentication Source	Allows user to enable or disable the authentication source.

Creating roles and assigning permissions

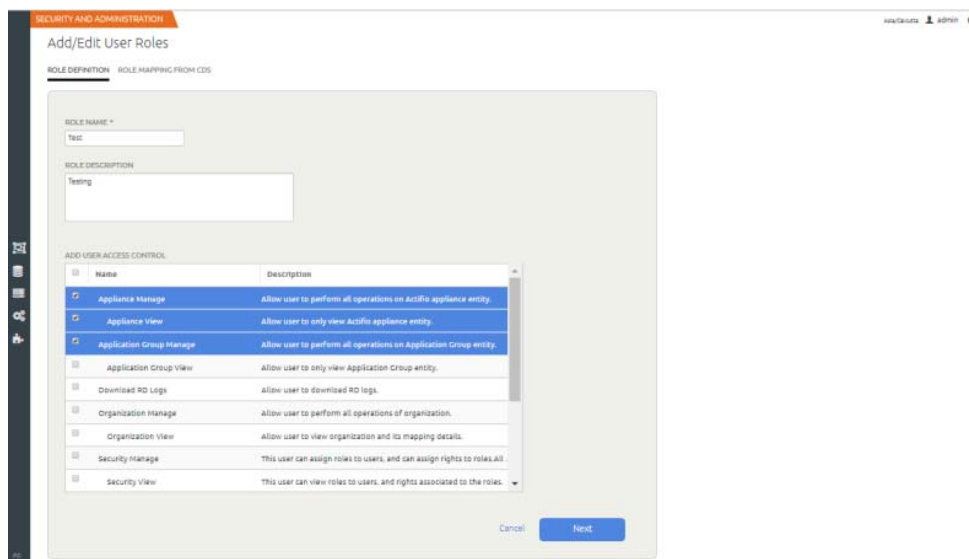
This section describes the steps to create a new role and assign permissions to the role. By default, new roles have no permissions. Therefore, when you create a role, you must assign required access control /permissions for that role.

To create a new role and assign permissions:

1. In the left navigation pane, click **Security and Administration**> **User Roles** to view the **User Roles** page.



2. Click **Add Role**. The Add/Edit User Roles page appears.
3. In **Name**, type a name for the role that makes the role function clear.
4. Enter a brief description of the role in **Description** field.
5. Select the user access that you want to assign for the role from the **User Access Control** section by checking the appropriate box.



6. Click **Next**.
7. Select your desired role(s) from Actifio Appliance to be mapped to this newly created role by checking the appropriate boxes.
8. Click **Finish** to complete the process.

Modifying roles and changing permissions

This section describes the steps to modify existing roles and change permissions to them.

To modify an existing role and permissions:

1. In the left navigation pane, click **Security and Administration**. The **User Roles** page displays all the existing roles.
2. Select the role you want to modify and click **Edit**.

SECURITY AND ADMINISTRATION

Add/Edit User Roles

ROLE DEFINITION ROLE MAPPING FROM CDS

ROLE NAME *

test_role

ROLE DESCRIPTION

Testing edit roles

ADD USER ACCESS CONTROL

Name	Description
<input type="checkbox"/> Appliance Manage	Allow user to perform all operations on Actifio appliance entity.
<input checked="" type="checkbox"/> Appliance View	Allow user to only view Actifio appliance entity.
<input type="checkbox"/> Application Group Manage	Allow user to perform all operations on Application Group entity.
<input checked="" type="checkbox"/> Application Group View	Allow user to only view Application Group entity.
<input type="checkbox"/> Download RD Logs	Allow user to download RD logs.
<input type="checkbox"/> Organization Manage	Allow user to perform all operations of organization.
<input checked="" type="checkbox"/> Organization View	Allow user to view organization and its mapping details.
<input type="checkbox"/> Security Manage	This user can assign roles to users, and can assign rights to roles.
<input checked="" type="checkbox"/> Security View	This user can view roles to users, and rights associated to the roles.

Cancel Next

3. Edit the **Role Name** or **Description** as needed.
4. Modify the user access from the **User Access Control** section by checking the appropriate boxes.
5. Click **Next**.
6. Select and map **Actifio Appliance Role(s)** by checking the appropriate boxes.
7. Click **Finish** to complete the process.

Deleting roles

To delete a user role and its permissions:

1. In the left navigation pane, click **Security and Administration**. The **User Roles** page displays all the existing roles.
2. Select the role you want to remove and click **Delete**. The **Delete User Role** dialog box appears.

Delete User Role?

Are you sure you want to delete user role ?

Warning: Delete operation may affect users linked with this role.

Cancel

Confirm

3. Click **Confirm** to delete the user role.
Deleting user access control may affect the users linked with this role.

Note: You can delete multiple users at a time. Use the appropriate check-boxes to select multiple users.

11 Downloading Logs

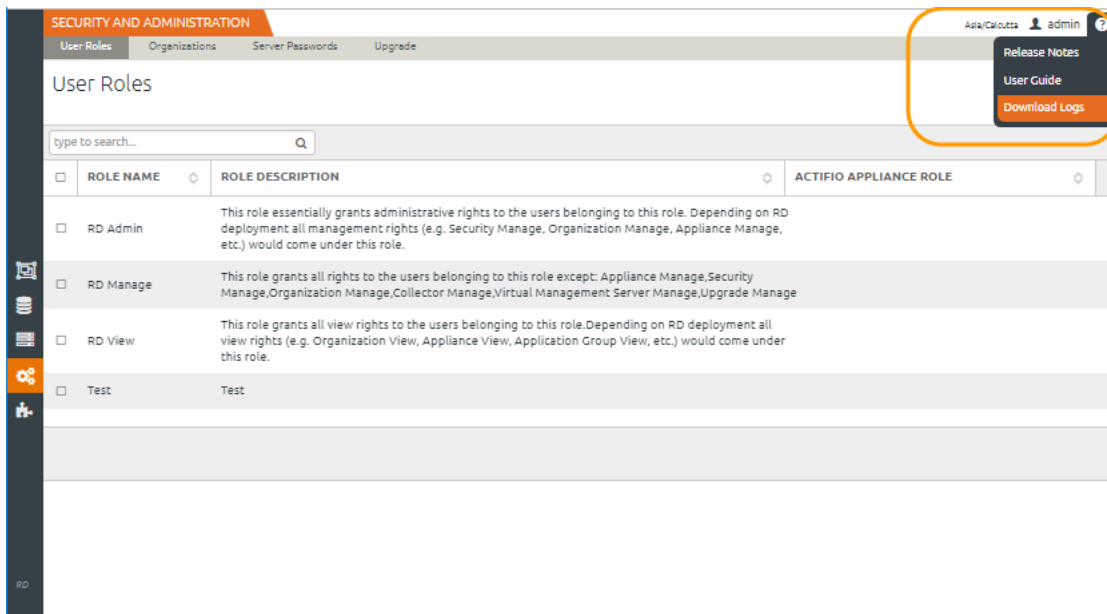
This chapter describes the details to download the Resiliency Director Collector logs.

Downloading the Logs

Logs are generated for each Resiliency Director operation executed in the Collector. The Resiliency Director logs are saved in the rd.log.0 format. The older logs are rotated and renamed to rd.log.0.1 and so on. The log file is saved at the /act/log location.

To download the operation logs:

1. In the right top corner of the page, click **Help (?)**.



Actifio Resiliency Director Collector - Downloading Logs

2. Click **Download** to download the logs.
3. Un-tar the downloaded log file (rd.log.tar.gz) to view the logs.

Note: The maximum download limit (log-file size) is set to 40 Mb and maximum log files to be created (log-file count) is set to 10.

12 Upgrading the Resiliency Director Collector

This chapter provides the details on how to upgrade your Actifio Resiliency Director Collector to a newer version, and explains the upgrade options in detail. You can upgrade the Actifio Resiliency Director Collector in following methods.

This chapter contains the following topics:

- [Upgrade using GUI-Based Method](#) on page 63
- [Upgrade using CLI-Based Method](#) on page 65

Upgrade using GUI-Based Method

The Resiliency Director Collector upgrade process involves the following:

1. Stops all the Resiliency Director related processes.
2. Takes backup of all your current data.
3. Migrates the data.

Note: After upgrading the Resiliency Director Collector, you can find the upgrade logs at: `/var/log/brd-install/` with name `"brd-upgrade.log"`

4. Restart all the Resiliency Director Collector related processes.

Following are the important points you should know while upgrading the Actifio Resiliency Director Server:

- Registered Resiliency Director Collector should be reachable.
- Registered Actifio Appliances should be accessible.
- Registered virtual management servers should be accessible.
- No recovery plan should be in **In Progress** state.

Note: If any one of the above fails, upgrade process fails.

To upgrade the Resiliency Director Collector:

1. Copy **.gpg** file to the Resiliency Director Collector machine.
2. Click **Settings > Security & Administration > Upgrade**. Upgrade screen displays.
Upgrade screen displays current status and upgrade history of the Resiliency Director Collector.

SECURITY AND ADMINISTRATION

Resource Pool Port Group User Roles Organizations Server Passwords **Upgrade**

Etc/UTC admin ?

Current Status

BASE SERVER VERSION: 7.1.0.3197 BINARY VERSION: 8.0.0.830
DB SCHEMA VERSION: 8.0.0.830 MIGRATION STATUS: SUCCESS

Resiliency Director Install/Upgrade History

RD VERSION	BINARY VERSION	DB SCHEMA VER...	UPDATED ON	STATUS
8.0.0.830	8.0.0.830	8.0.0.830	12/11/2018 13:47:38	SUCCESS
7.1.4.4291	7.1.4.4291	7.1.4.4291	07/03/2018 14:48:05	SUCCESS
7.1.2.4218	7.1.2.4218	7.1.2.4218	11/10/2017 06:18:11	SUCCESS
7.1.2.4211	7.1.2.4211	7.1.2.4211	11/08/2017 11:31:55	SUCCESS
7.1.1.4182	7.1.1.4182	7.1.1.4182	08/22/2017 08:26:18	SUCCESS

Uploaded Version

NO FILES UPLOADED. PLEASE UPLOAD.

UPLOAD

Resiliency Director Collector Upgrade

- Click **Upload**. Upload and Upgrade screen displays.
- Click **Browse** to locate the **.gpg** file and select **Yes** against **Installation after upload**. Upgrade confirm field becomes active.

Upload And Upgrade

UPGRADE FILE **BROWSE**

INSTALLATION AFTER UPLOAD ☒ YES ☐ NO

Are you sure you want to upgrade from 8.0.0.830 to 8.0.0.832 ? Please confirm by typing "UPGRADE" in the box.

Note: Resiliency Director UI will not be accessible during upgrade process, approximate upgrade time is upto 15 minutes.

[Cancel](#) **Done**

- Type **UPGRADE** in confirmation field and click **Done**.

Note: After upgrade any existing file is replaced by the new file. During upgrade process, Resiliency Director Collector GUI is not accessible for few minutes. Once upgrade process is completed, you can login and check the latest the latest version of Resiliency Director Collector by clicking the navigation bar.

If upgrade process fails, you must restore the data manually.

To restore data manually,

1. Navigate to the directory `/act/rdbbackup/`
2. Stop all the Resiliency Director related processes.
3. Go to `backup.tar.gz` file on slash('/') and unpack the `backup.tar.gz` file. This will extract the content to a folder structure like `/data/act/`. Ensure that tar file is unpacked correctly.
4. Restart all the Resiliency Director related processes. For more information on Resiliency Director processes, see [Actifio Resiliency Director Collector Configuration Parameters](#) on page 10.

Upgrade using CLI-Based Method

Perform these steps to upgrade the Actifio Resiliency Director Collector to a newer version:

1. Copy the `patch-RD8.0.3.888.gpg` file to the RD virtual appliance.

```
$scp patch-RD8.0.3.888.gpg admin@172.16.201.241:/home/admin
```
2. Prepare the "patch-RDx.x.x.gpg" file to be used during the upgrade.

```
$rdtask uploadupdate /home/admin/patch-RD8.0.3.888.gpg
```

Output: SUCCESS
3. If required, you can list information about the upgrade file that has been uploaded and verified with the following command. This command will also validate applicability of the version uploaded.

```
$ rdinfo lsupdate
```

Output:

Available Update is as follows:

patch-RD8.0.3.888.gpg
4. To validate the uploaded upgrade file, confirm version applicability, and perform the install, use the **installupdate** command.

```
$ rdtask installupdate
```

Output:

Note: Resiliency Director UI is not be accessible during upgrade, approximate upgrade time is up to 15 minutes.

13 vCenterPermissions_collector.fm

VMware sometimes combines, separates, renames, and adds permissions with new releases of vCenter Server. The information here is specific for VMware vCenter Server 5.1 and 5.5. Later versions may have different permissions.

This chapter contains the following topics:

[Creating the ActifioReadOnly vCenter Role](#) on page 68

[Creating the ActifioOperations vCenter Role](#) on page 69

[The vCenter Permissions List](#) on page 70

[Assigning Minimum Permissions](#) on page 71

Before You Begin

In order for Actifio to back up and recover VMware virtual machines, the Actifio appliance must authenticate to the VMware vCenter Server with a user id that has sufficient privileges to perform the required operations. Create a custom Actifio user account assigned custom ActifioReadOnly role and ActifioOperations role with a lesser set of privileges. A custom user also enables traceability within VMware logs to find commands used by the Actifio appliance. In this document, the custom user is referred to as **ActifioUser**.

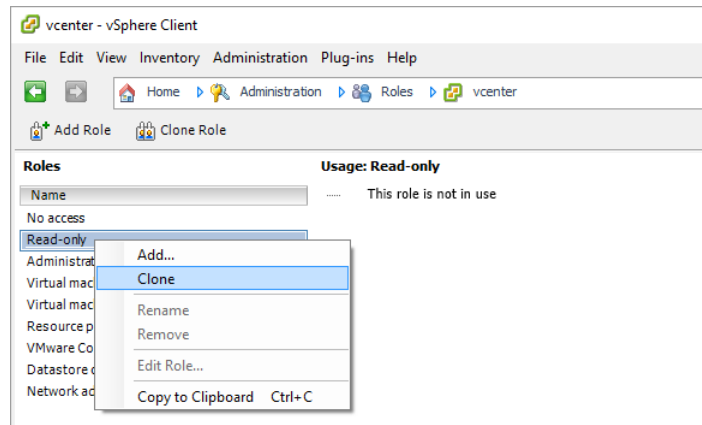
This document provides the minimum set of privileges needed to have the Actifio appliance perform all backup and recovery operations.

Note: Consider setting the password for this user to never expire. If the password expires then your Actifio appliances will be unable to work with vCenter until the password is updated, which would be a manual process.

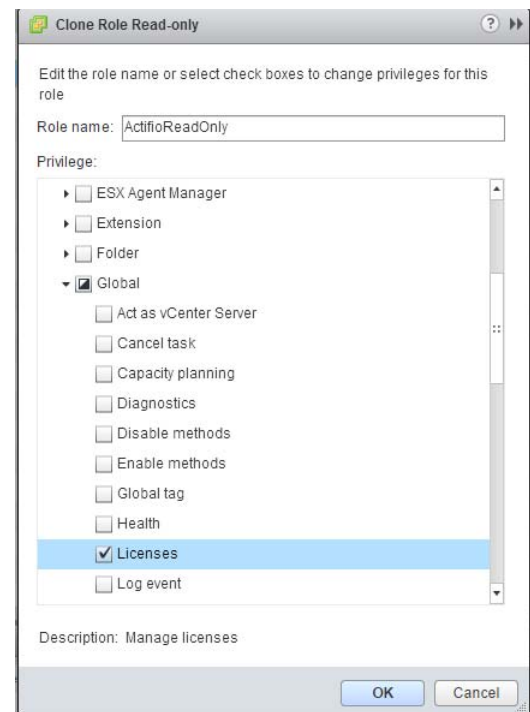
Creating the ActifioReadOnly vCenter Role

You will create two vCenter roles. The first one is an ActifioReadOnly role to assign the licenses permission and no other permissions:

1. Log into vSphere as a user with Administrator privileges.
2. On the vSphere Client Home page, under Administration, click **Roles**.
3. Right-click the **Read-Only** role and click **Clone**. A new *Clone of Read-Only* role appears in the list of roles.



4. Right-click **Clone of Read-Only** and click **Edit**.
5. Rename the new role **ActifioReadOnly**.
6. Under **Global**, check **Licenses**.
7. Assign no other privileges; you will add privileges as needed for the VM, cluster, etc. Click **OK**.

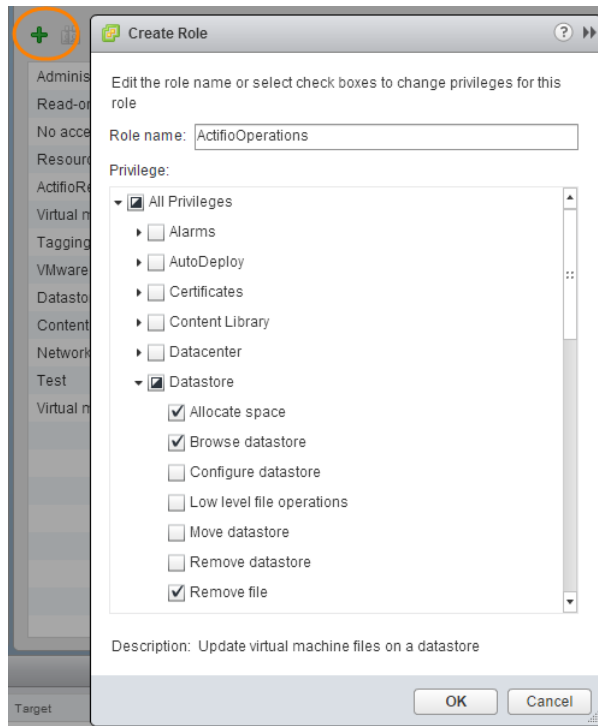


Note: These examples show the vSphere client application running on a Windows host. Your screens will look a little different if you use the VMware web interface.

Creating the ActifioOperations vCenter Role

After the ActifioReadOnly role exists, create a new vCenter role for Actifio operations:

1. Log on to vSphere as a user with Administrator privileges.
2. On the vSphere Client Home page, under Administration, click **Roles**.
3. Create a new role called **ActifioOperations**.
4. Check the check boxes for each of the privileges listed in [The vCenter Permissions List](#) on page 70.
5. Click **OK** to save the role.



Set the Permissions by Checking their Checkboxes

The vCenter Permissions List

The Actifio vCenter user must have the following permissions:

vCenter User	Permission
Network User	Assign Network
Resource User	Assign vApp to resource pool, Assign virtual machine to resource pool, Migrate powered off virtual machine, Migrate powered on virtual machine.
Virtual Machine User	Configuration: Advanced, Change CPU count, Change resource, Configure managedBy, Memory, Modify device settings, Raw device, Rename, Settings Guest Operations Interaction: Device connection, Power Off, Power On Inventory: Move, Register, Unregister
vApp User	Add virtual machine, Add resource pool, Assign vApp, Create, Delete, Power Off, Power On, Rename, View OVF environment, vApp application configuration, vApp instance configuration, vApp managedBy configuration, vApp resource configuration

Assigning Minimum Permissions

To limit access of ActifioUser, assign the ActifioReadOnly role to ActifioUser at the vCenter level and the ActifioOperations role to ActifioUser at the Datacenter level, then set NoAccess at the highest level necessary to restrict ActifioUser from all VMs and ESXi servers that will never be mounted to or backed up by the Actifio appliance.

To assign to ActifioUser the minimum permissions necessary to perform all required functions:

1. Log on to vSphere as a user with Administrator privileges. On the vSphere Client Home page, click **Hosts and Clusters**.
2. Select the vCenter to ensure that permissions are propagated correctly. On the **Permissions** tab or under the Actions dropdown, select **Add Permission**.
3. Select **ActifioReadOnly** from the Assigned Role drop-down menu.
4. Check the **Propagate to Children** check box at the bottom of the window.
5. Click **Add** to open the Select Users or Groups dialog box.
6. Select the domain where **ActifioUser** is located from the Domain drop-down menu and type **ActifioUser** in the Search box. Click **Add**. ActifioUser is added to the Users list. Click **OK**.
7. Select the Datacenter to ensure that permissions are propagated correctly.
8. On the **Permissions** tab or under the Actions drop-down, select **Add Permission**.
9. Select **ActifioOperations** from the Assigned Role drop-down menu.
10. Check the **Propagate to Children** check box at the bottom of the window.
11. Click **Add** to open the Select Users or Groups dialog box.
12. Select the domain where **ActifioUser** is located from the Domain drop-down menu and type **ActifioUser** in the Search box. Click **Add**. ActifioUser is added to the Users list. Click **OK** and then click **OK** again.
13. Go back to Inventory > Hosts and Clusters. Right-click each branch that will have no Actifio jobs, select ActifioUser, and assign the **No Access** role to ActifioUser. Click **OK** to finish.

Index

A

- Actual Recovery 33
- ALL 44
- application group name 29

C

- configure VM 33
- contact information, Actifio Support ii
- copyright ii

D

- default organizations 43
- Deleting User Access Control 59

I

- IP Address Retention 39
- Is Critical 33
 - Failed 33
 - Success 33

L

- legal matter ii
- Login 11

M

- modify an application group 41

P

- postscripts 38
- prescripts 38
- PUBLIC 44

T

- Test Recovery 33
- trademarks ii

U

- Upgrading the Resiliency Director Collector 63

V

- virtual machines 27
- VM parameters 33

W

- warranty ii