Actifio Resiliency Director Server User Guide

Actifio Resiliency Director 8.0.3

Copyright, Trademarks, and other Legal Matter

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**.

Preface

This guide provides step-by-step instructions on how to deploy and use the Actifio Resiliency Director Server. This guide assumes that you are already familiar with Actifio appliances by following ***Getting Started with Actifio Copy Data Management*** 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. The following guides will be of particular interest:

- ***Virtualizing and Protecting Copy Data with the Application Manager***

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 Server

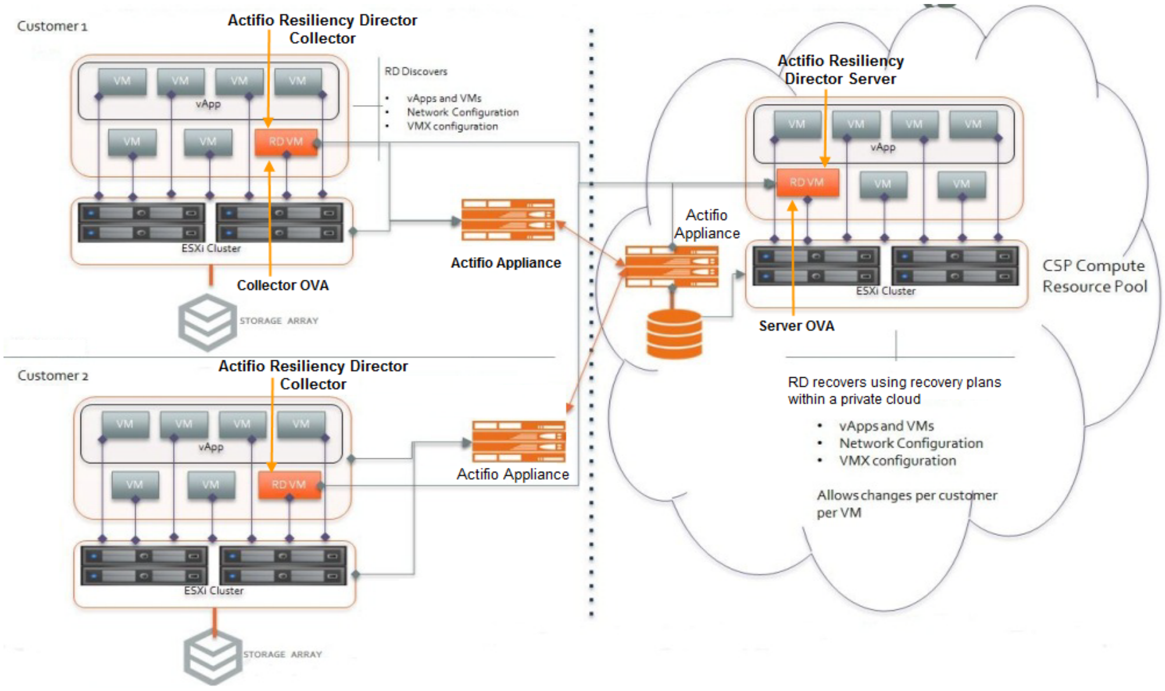
The Actifio Resiliency Director Server is a component of the Actifio Resiliency Director, a resiliency solution for non-disruptive automated recovery of virtual machines and database applications.

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 Server.

Resiliency Director Server Overview

The Actifio Resiliency Director Server is the central manager of resiliency data for multiple Resiliency Director Collectors. Data collected by the Actifio Resiliency Director Collector is sent and saved in the Actifio Resiliency Director Server. This enables Actifio Resiliency Director Server to bring all VMs, vApps, File Systems, SQL Server Databases online in an orchestrated manner in case of failover, or move the VM stacks to cloud for tasks such as data mining, analysis, and optimization.



Actifio Resiliency Director Server Overview

The Resiliency Director Server is deployed in the Cloud Service Provider (CSP) environment and allows you to:

- Add, edit, and delete Actifio Appliance
- Add, edit, and delete virtual management servers
- Add, edit, and delete Resiliency Director Collectors
- Discover, update, and delete the host groups
- Add, edit, and delete organizations
- Add, edit, disable, and delete recovery plans
- Add, edit, and delete user access controls
- View application groups
- Execute recovery plans in test or actual mode
- Execute single/parallel VM or application recovery
- Cancel recovery plan execution
- Download logs

2 Deploying the Actifio Resiliency Director Server

This chapter describes how to deploy the Actifio Resiliency Director Server.

Actifio Resiliency Director Server is available in **.ova** format. You must configure the Actifio Resiliency Director Server after deploying the ova.

Setting up the Actifio Resiliency Director Server requires:

- Deploying the Resiliency Director Server OVA on page 9
- Configuring the Actifio Resiliency Director Server on page 10

Deploying the Resiliency Director Server OVA

Before deploying Actifio Resiliency Director Server OVA file, ensure that server meets the minimum system requirements of 8 v CPU, 16 GB RAM, and 40 GB storage. You can deploy the Actifio Resiliency Director Server on the vSphere 5.x,6.0,6.5 & 6.7.

To deploy the Actifio Resiliency Director Server **ova** file:

1. Launch the vSphere vCenter client.
2. From **File**, click **Deploy OVF** template.
3. Provide the path of 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**. The progress of the OVA deployment appears.
6. Wait for the VM to show its IP address. You will use this IP address to configure the Actifio Resiliency Director.

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

1. Login 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 datacenter or folder, 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**. Select Networks and click **Next**.
8. Enter the values for the networking properties and click **Next**.
9. Review the configuration data and click **Finish**.
10. Power on RD appliance after deployment.
11. Wait for the VM to show its IP address, use will use this to configure the Actifio Resiliency Director.

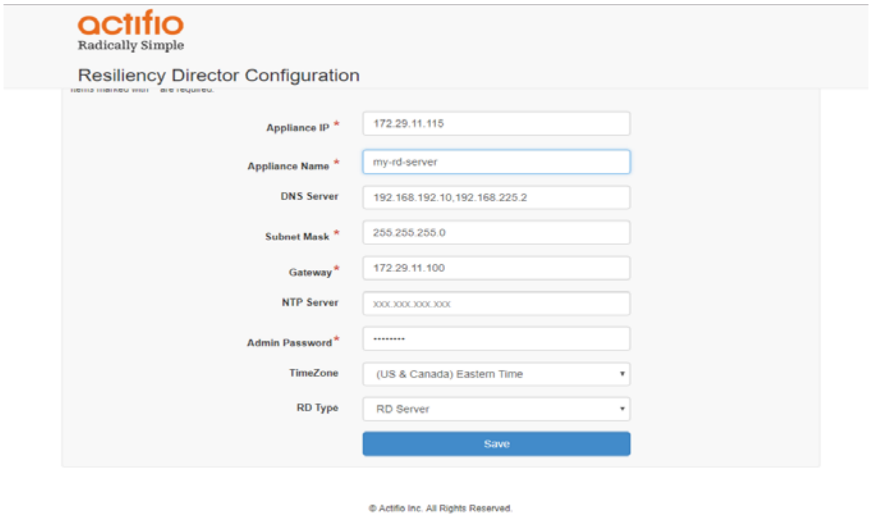
Configuring the Actifio Resiliency Director Server

To configure the Actifio Resiliency Director Server:

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. Use the browser's private, or incognito mode to configure the Actifio Resiliency Director so that the UI is not cached.

   > ***Note:*** *You can also access the Resiliency Director Configuration page using the URL https://<Actifio Resiliency Director IP Address>.*

3. Change the network parameters to the following values:
   - Enter/verify the static IP address of the Actifio Resiliency Director in the **Appliance IP** field.
   - Enter the name of the Actifio Resiliency Director Server in the **Appliance Name** field.
   - Enter the **DNS Server** IP address in the **DNS Server** field.
   - Enter the **Subnet Mask** and **Gateway** details in the respective fields.
   - Enter the NTP server IP address in the **NTP** Server field.
   - 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.
   - Select the your time zone from the **Time Zone** drop-down list.
   - Select **RD Server** from the **RD Type** drop-down list.
4. Click **Save**. The server reboots after setting the configuration.



Resiliency Director Configuration

Appliance IP *	172.29.11.115
Appliance Name *	my-rd-server
DNS Server	192.168.192.10,192.168.225.2
Subnet Mask *	255.255.255.0
Gateway*	172.29.11.100
NTP Server	xxx.xxx.xxx.xxx
Admin Password*	·········
TimeZone	(US & Canada) Eastern Time ▾
RD Type	RD Server ▾

© Actifio Inc. All Rights Reserved.

Actifio Resiliency Director Server 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 Server

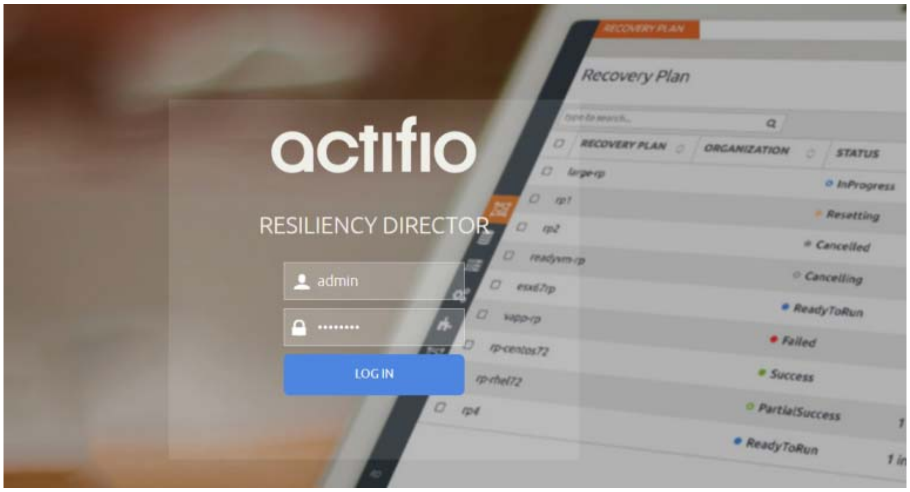
This chapter provides the details to log on to the Actifio Resiliency Director graphical user interface. You can invoke the Actifio Resiliency Director Server GUI using administrator user or the CDS user credentials on the machine that is hosting the Resiliency Director Server.

To access the Actifio Resiliency Director:

Note: *Clear browser cache if you have not used the browser's private or incognito mode while configuring the Actifio Resiliency Director Server to view the login page.*

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

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



□	RECOVERY PLAN	ORGANIZATION	STATUS
□	large-rp		InProgress
□	rp1		Resetting
□	rp2		Cancelled
□	readyvm-rp		Cancelling
□	esxi67rp		ReadyToRun
□	vapp-rp		Failed
□	rp-centos72		Success
	rp-rhel72		PartialSuccess
□	rp4		ReadyToRun

Actifio Resiliency Director Server Login Screen

2. From the login window, enter the user name as "admin" and the password used during the Resiliency Director deployment and installation.

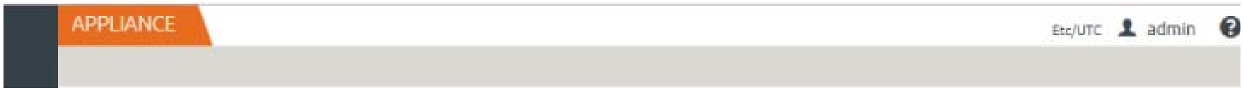
   Note: *The Actifio Resiliency Director always has a single local login named "admin" that has full access. Additionally, it can be configured to leverage the authentication on an Actifio appliance to add support for multiple users, and even pass-through authentication to an LDAP directory.The User Name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

3. Click **Login**. The Actifio Resiliency Director Server home screen appears.

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, Databases.
Actifio Resiliency Director Server	Performs recovery operations at the DR site, based on the application groups defined on the Resiliency Director Collector.

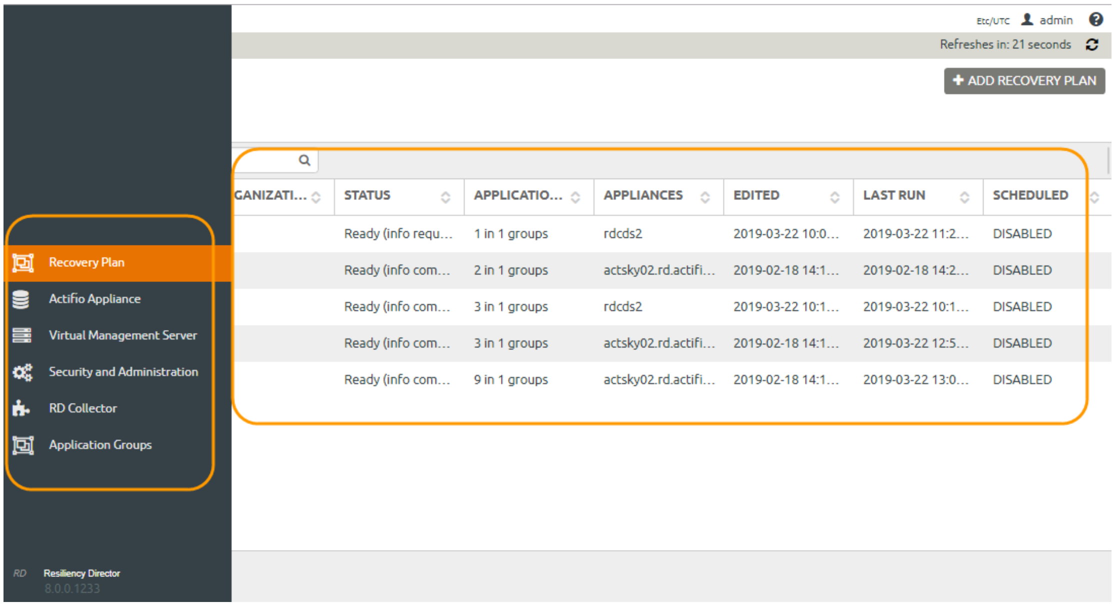
The Actifio Resiliency Director title bar includes:

- **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 User Guide, and Download Logs information.



Actifio Resiliency Director Server 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.

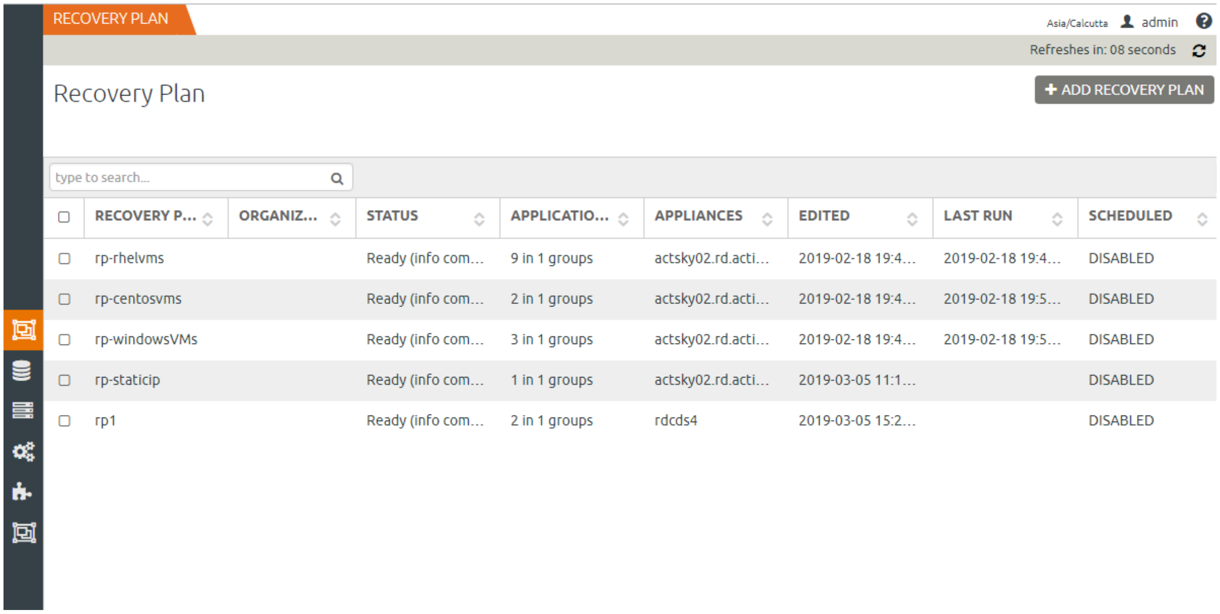


GANIZATI...	STATUS	APPLICATIO...	APPLIANCES	EDITED	LAST RUN	SCHEDULED
	Ready (info requ...	1 in 1 groups	rdcds2	2019-03-22 10:0...	2019-03-22 11:2...	DISABLED
	Ready (info com...	2 in 1 groups	actsky02.rd.actifi...	2019-02-18 14:1...	2019-02-18 14:2...	DISABLED
	Ready (info com...	3 in 1 groups	rdcds2	2019-03-22 10:1...	2019-03-22 10:1...	DISABLED
	Ready (info com...	3 in 1 groups	actsky02.rd.actifi...	2019-02-18 14:1...	2019-03-22 12:5...	DISABLED
	Ready (info com...	9 in 1 groups	actsky02.rd.actifi...	2019-02-18 14:1...	2019-03-22 13:0...	DISABLED

Actifio Resiliency Director Server - Navigation and Information Pane

The Actifio Resiliency Director Server Home Screen

The Actifio Resiliency Director home screen lists the configured recovery plans as seen figure below, If no recovery plans are created, then instead of displaying the recovery plans list, the Actifio Appliance screens will be displayed as that is the first step in configuring a newly installed Resiliency Director Server.The data displayed on the **Home Screen** gets refreshed depending on the configured time interval for which the data is fetched and populated.



Recovery Plan

□	RECOVERY P...	ORGANIZ...	STATUS	APPLICATIO...	APPLIANCES	EDITED	LAST RUN	SCHEDULED
□	rp-rhelvms		Ready (info com...	9 in 1 groups	actsky02.rd.acti...	2019-02-18 19:4...	2019-02-18 19:4...	DISABLED
□	rp-centosvms		Ready (info com...	2 in 1 groups	actsky02.rd.acti...	2019-02-18 19:4...	2019-02-18 19:5...	DISABLED
□	rp-windowsVMs		Ready (info com...	3 in 1 groups	actsky02.rd.acti...	2019-02-18 19:4...	2019-02-18 19:5...	DISABLED
□	rp-staticip		Ready (info com...	1 in 1 groups	actsky02.rd.acti...	2019-03-05 11:1...		DISABLED
□	rp1		Ready (info com...	2 in 1 groups	rdcds4	2019-03-05 15:2...		DISABLED

Actifio Resiliency Director Server Home Screen - Recovery Plan

The Recovery Plan home screen allows you to add, edit, and delete the recovery plans. for more information on adding, editing, and deleting an application groups, see Adding a Recovery Plan on page 50.

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 Server.

This chapter contains the following topics:

Adding an Actifio Appliance to the Actifio Resiliency Director Server

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

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.

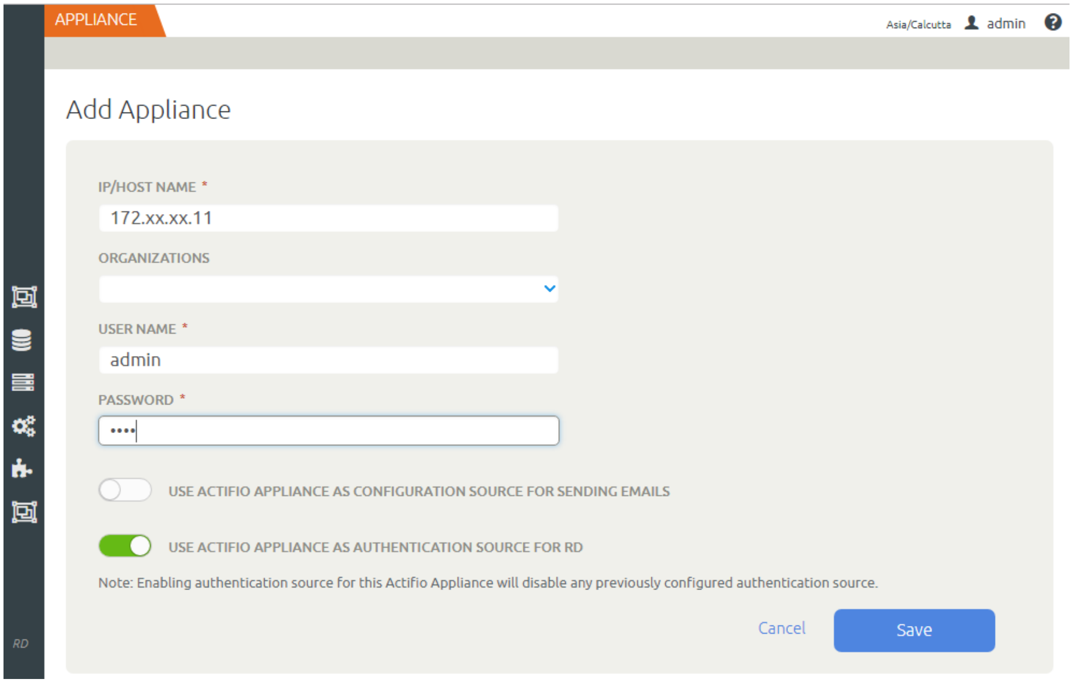
3. Enter the **IP address** or **Host name** of the Actifio Appliance in the **IP/Host Name** field.

4. Select **Organization** from the drop down list for users of selected organization to have access to this particular Appliance.

5. Enter the respective user credentials in the **User Name** and **Password** fields.

   Optionally, you can select **Use Actifio Appliance as Configuration Source for Sending Emails** option.

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



Add Appliance

IP/HOST NAME * 172.xx.xx.11

ORGANIZATIONS

USER NAME * admin

PASSWORD * ••••

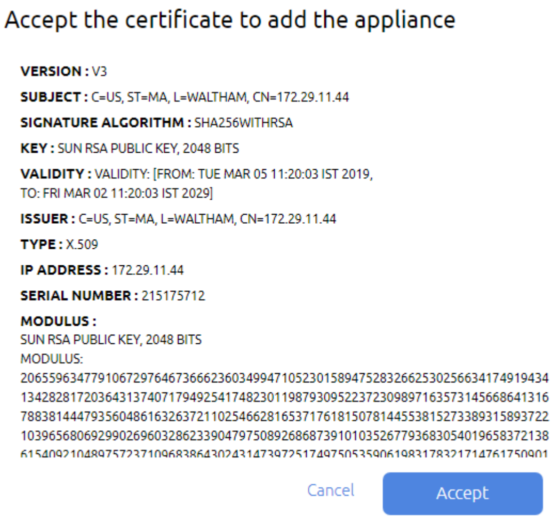
○ USE ACTIFIO APPLIANCE AS CONFIGURATION SOURCE FOR SENDING EMAILS

● USE ACTIFIO APPLIANCE AS AUTHENTICATION SOURCE FOR RD

Note: Enabling authentication source for this Actifio Appliance will disable any previously configured authentication source.

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 : C=US, ST=MA, L=WALTHAM, CN=172.29.11.44

SIGNATURE ALGORITHM : SHA256WITHRSA

KEY : SUN RSA PUBLIC KEY, 2048 BITS

VALIDITY : VALIDITY: [FROM: TUE MAR 05 11:20:03 IST 2019,
TO: FRI MAR 02 11:20:03 IST 2029]

ISSUER : C=US, ST=MA, L=WALTHAM, CN=172.29.11.44

TYPE : X.509

IP ADDRESS : 172.29.11.44

SERIAL NUMBER : 215175712

MODULUS :
SUN RSA PUBLIC KEY, 2048 BITS
MODULUS:
206559634779106729764673666236034994710523015894752832662530256634174919434
134282817203643137407179492541748230119879309522372309897163573145668641316
788381444793560486163263721102546628165371761815078144553815273389315893722
103965680692990269603286233904797508926868739101035267793683054019658372138
615409210489757237109683864302431473972517497505359061983178321714761750901

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

Enabling and Disabling Email Notification

You receive an email notification in the following scenarios:

- When recovery plan execution is completed.
- If you make any changes to an application group which is part of a recovery plan.

Note: *If the email notification setting is not configured on the Actifio Appliance, the Resiliency Director Server displays "Email configuration is not set", after enabling the email notification in Resiliency Director Server and no emails will be sent even if "Enable Email Notification check box is selected.*

Note: *Only one Actifio Appliance email configuration setting is used by Resiliency Director Server at a time. Selecting the Enable Email Notification option for other Actifio Appliance will override any previously selected Actifio Appliance settings.*

To disable email notification:

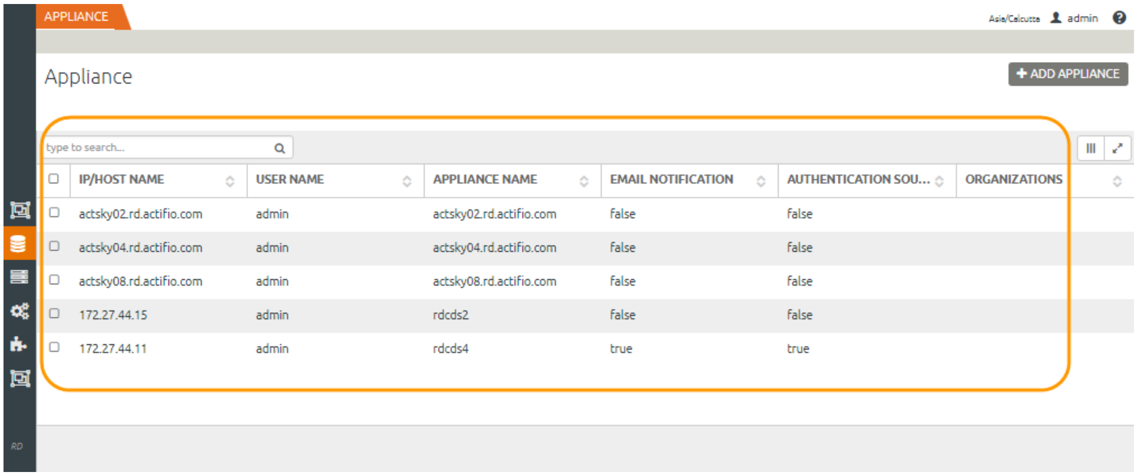
1. In the left navigation pane, click **Actifio Appliance**. The **Actifio Appliance** page appears.
2. Select the Actifio Appliance for which you want to disable the email notification and click **Edit**. The **Edit Appliance** page appears.
3. Clear the **Enable Email Notification** check box to disable the email notification for selected Actifio Appliance.
4. Click **Save** to save the changes.

Listing the Available Actifio Appliances

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

To list the Actifio Appliances:

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



□	IP/HOST NAME	USER NAME	APPLIANCE NAME	EMAIL NOTIFICATION	AUTHENTICATION SOU...	ORGANIZATIONS
□	actsky02.rd.actifio.com	admin	actsky02.rd.actifio.com	false	false	
□	actsky04.rd.actifio.com	admin	actsky04.rd.actifio.com	false	false	
□	actsky08.rd.actifio.com	admin	actsky08.rd.actifio.com	false	false	
□	172.27.44.15	admin	rdcds2	false	false	
□	172.27.44.11	admin	rdcds4	true	true	

Listing 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.
EMAIL NOTIFICATION	True if email notification is enabled.
AUTHENTICATION SOURCE	True if authentication source is enabled.
ORGANIZATIONS	Displays the organization name.

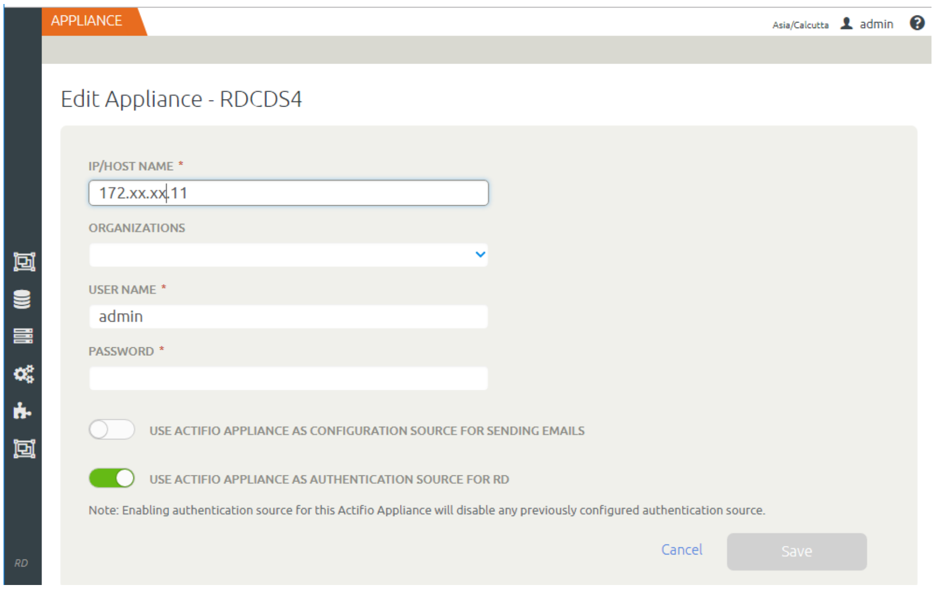
Modifying an Actifio Appliance Details

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**.

   Optionally, you can select **Use Actifio Appliance as Configuration Source for Sending Emails** option.



Edit Appliance - RDCDS4

IP/HOST NAME *
172.xx.xx.11

ORGANIZATIONS

USER NAME *
admin

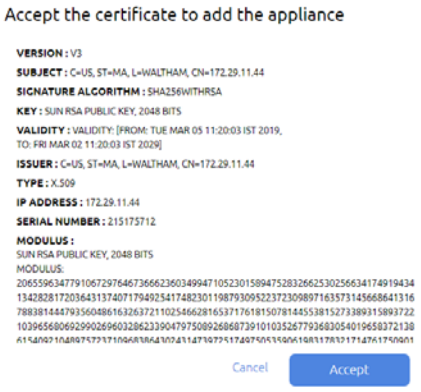
PASSWORD *

○ USE ACTIFIO APPLIANCE AS CONFIGURATION SOURCE FOR SENDING EMAILS

● USE ACTIFIO APPLIANCE AS AUTHENTICATION SOURCE FOR RD

Note: Enabling authentication source for this Actifio Appliance will disable any previously configured authentication source.

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 : C=US, ST=MA, L=WALTHAM, CN=172.29.11.44
SIGNATURE ALGORITHM : SHA256WITHRSA
KEY : SUN RSA PUBLIC KEY, 2048 BITS
VALIDITY : VALIDITY: [FROM: TUE MAR 05 11:20:03 IST 2019,
TO: FRI MAR 02 11:20:03 IST 2029]
ISSUER : C=US, ST=MA, L=WALTHAM, CN=172.29.11.44
TYPE : X.509
IP ADDRESS : 172.29.11.44
SERIAL NUMBER : 215175712
MODULUS :
SUN RSA PUBLIC KEY, 2048 BITS
MODULUS:
206559634779106729764673666236034994710523015894752832662530256634174919434
134282817203643137407179492541748230119879309522372309897163573145668641316
788381444793560486163263721102546628165371761815078144553815273389315893722
103965680692990269603286233904797508926868739101035267793683054019658372138
615409210489757237109683864302431473972517497505359061983178321714761750901

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

Deleting an Actifio Appliance from the Resiliency Director Server

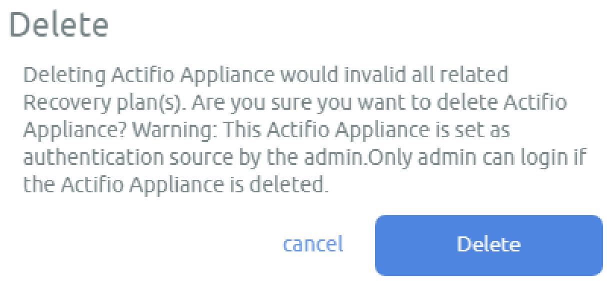
Before you delete, make sure to verify the dependencies, deleting an Actifio Appliance also removes the associated application groups, recovery plans if any.

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 that you want to delete 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 Ctrl key 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.


Delete

Deleting Actifio Appliance would invalid all related Recovery plan(s). Are you sure you want to delete Actifio Appliance? Warning: This Actifio Appliance is set as authentication source by the admin.Only admin can login if the Actifio Appliance is deleted.

Note: *You cannot delete the Actifio Appliance if application groups on the Resiliency Director Collector are part of the 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 Server.

This chapter contains the following topics:

Adding a Virtual Management Server

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

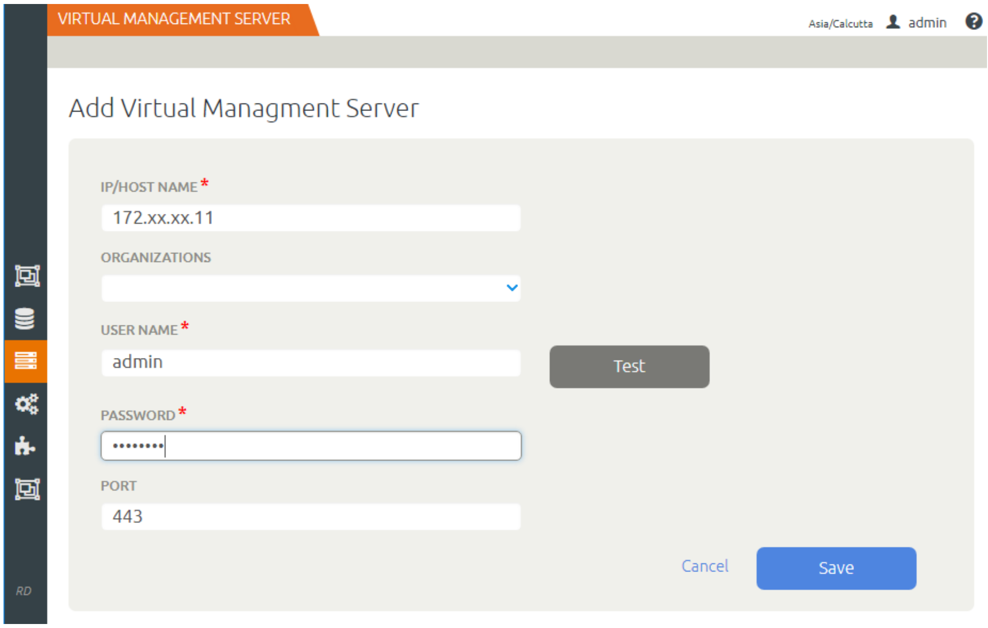
Note: *You cannot add the same server with different IP addresses.*

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 61.*
7. Click **Save** to add the virtual management server.
8. In the confirmation dialogue box, click **Okay**.



Add Virtual Managment Server

IP/HOST NAME *
172.xx.xx.11

ORGANIZATIONS

USER NAME *
admin

PASSWORD *
••••••••

PORT
443

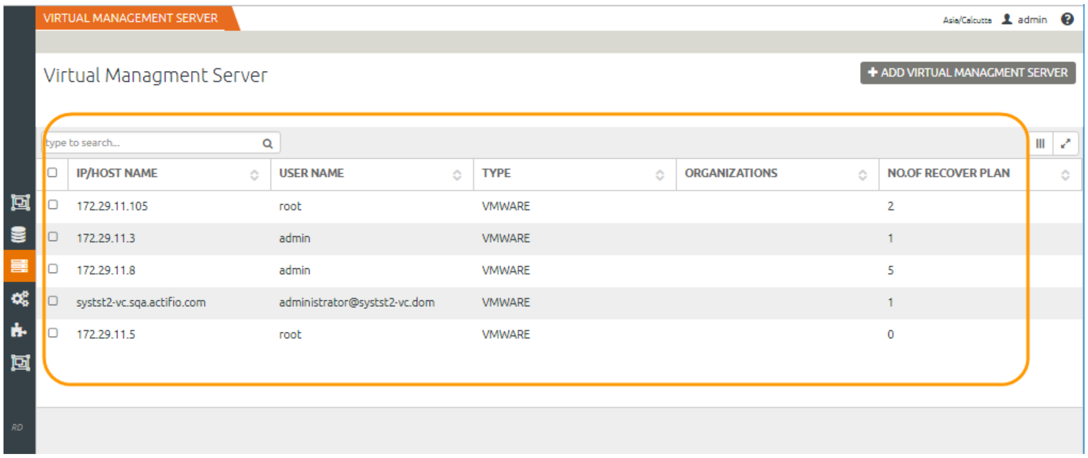
Note: *Configure a DNS server between the source and destination to permit you to add a server using its hostname.*

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.



□	IP/HOST NAME	USER NAME	TYPE	ORGANIZATIONS	NO.OF RECOVER PLAN
□	172.29.11.105	root	VMWARE		2
□	172.29.11.3	admin	VMWARE		1
□	172.29.11.8	admin	VMWARE		5
□	systst2-vc.sqa.actifio.com	administrator@systst2-vc.dom	VMWARE		1
□	172.29.11.5	root	VMWARE		0

Listing Virtual Management Servers

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.
ORGANIZATIONS	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.

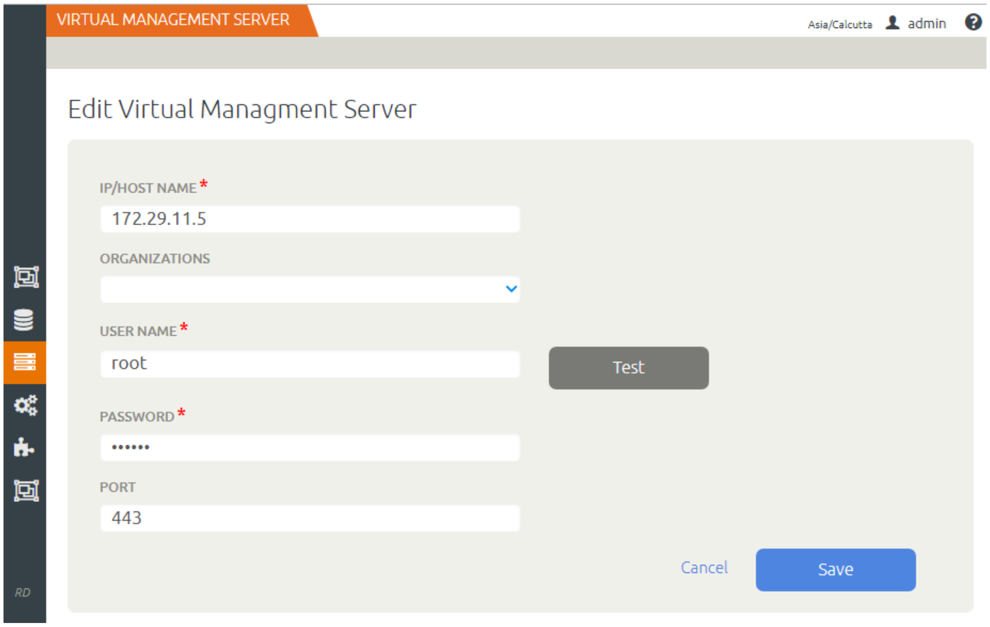
3. Enter the **IP address** or **Host name** of the virtual management server in the **IP/Host Name** field.

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.



Edit Virtual Managment Server

IP/HOST NAME *
172.29.11.5

ORGANIZATIONS

USER NAME *
root

PASSWORD *
••••••

PORT
443

7. Click **Save** to save the changes you have made.

8. In the confirmation dialogue box, click **Okay**.

Deleting a Virtual Management Server

To delete a virtual management server:

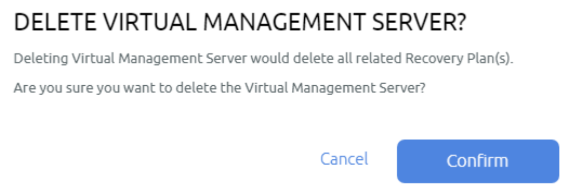
1. In the left navigation pane, click **Virtual Management Servers**.

   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 **Confirm** to delete the virtual management server.
   Deleting a virtual management server also deletes the associated recovery plans.



DELETE VIRTUAL MANAGEMENT SERVER?

Deleting Virtual Management Server would delete all related Recovery Plan(s).

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

Note: *You can delete multiple virtual management servers at a time. Use the appropriate check-boxes to select multiple virtual management servers.*

6 Managing Application Groups

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

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.

This chapter contains the following topics:

- Listing Application Groups on page 27
- Viewing Application Group Details on page 28

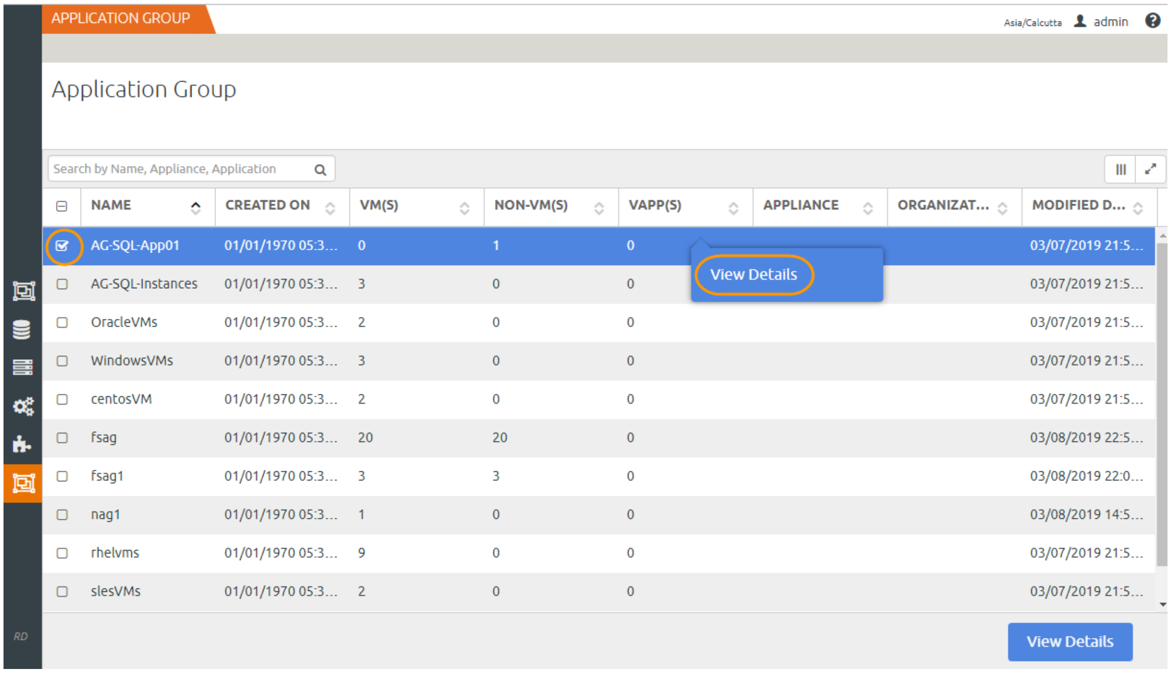
Listing Application Groups

To list the application groups:

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

   The list of available application groups appears.

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



⊟	NAME	CREATED ON	VM(S)	NON-VM(S)	VAPP(S)	APPLIANCE	ORGANIZAT...	MODIFIED D...
☑	AG-SQL-App01	01/01/1970 05:3...	0	1	0			03/07/2019 21:5...
□	AG-SQL-Instances	01/01/1970 05:3...	3	0	0			03/07/2019 21:5...
□	OracleVMs	01/01/1970 05:3...	2	0	0			03/07/2019 21:5...
□	WindowsVMs	01/01/1970 05:3...	3	0	0			03/07/2019 21:5...
□	centosVM	01/01/1970 05:3...	2	0	0			03/07/2019 21:5...
□	fsag	01/01/1970 05:3...	20	20	0			03/08/2019 22:5...
□	fsag1	01/01/1970 05:3...	3	3	0			03/08/2019 22:0...
□	nag1	01/01/1970 05:3...	1	0	0			03/08/2019 14:5...
□	rhelvms	01/01/1970 05:3...	9	0	0			03/07/2019 21:5...
□	slesVMs	01/01/1970 05:3...	2	0	0			03/07/2019 21:5...

Listing Application Groups

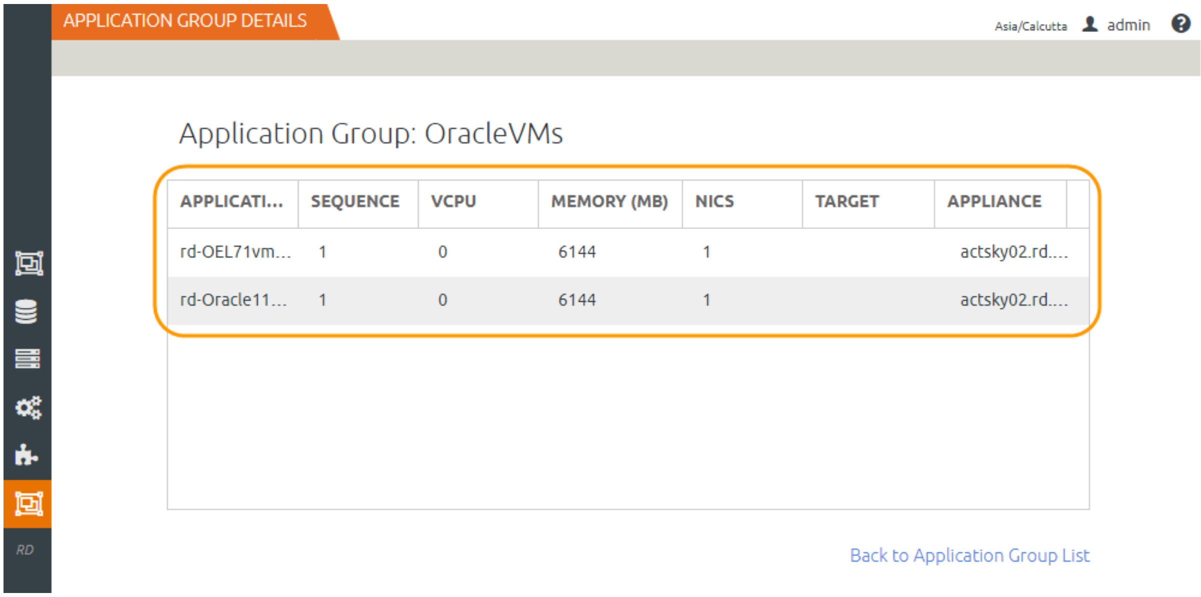
Viewing Application Group Details

To view an application group details:

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

   The list of available application groups appears.

2. Click the required application group name to view the details of the selected group.
3. The Application Group Details page displays the details.



Application Group: OracleVMs

APPLICATI...	SEQUENCE	VCPU	MEMORY (MB)	NICS	TARGET	APPLIANCE
rd-OEL71vm...	1	0	6144	1		actsky02.rd....
rd-Oracle11...	1	0	6144	1		actsky02.rd....

Back to Application Group List

Viewing Application Group Details

Application Groups Table - Field Elements

Field/Item	Description
Name	Displays the application group name.
Created On	Displays the date when the application group is created.
VM(s)	Displays the number of VMs in the application group.
Non VM(s)	Displays the number of non VMs in the application group.
vApp(s)	Displays the number of vApps in the application group.
Appliance	Displays the name of the Actifio 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 last edited.

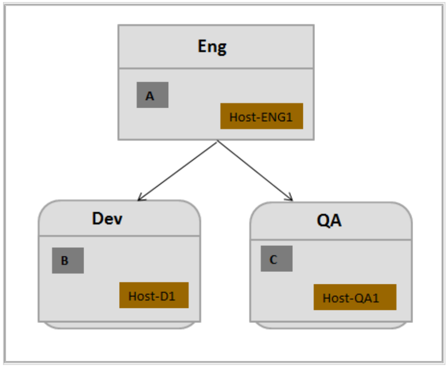
Details of the Selected Application Group

Field/Item	Description
Application	Displays the name of the Application.
Sequence	Displays the order of the recovery you have set.
VCPU	Displays the number of CPUs in the selected application group.
Memory (MB)	Displays the memory size of the selected application group.
NIC(s)	Displays the number of NICs in the selected application group.
Target	Name of the target.
Appliance	Name of the Appliance

7 Creating and Managing Organizations

This chapter introduces features related to managing organizations.

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:

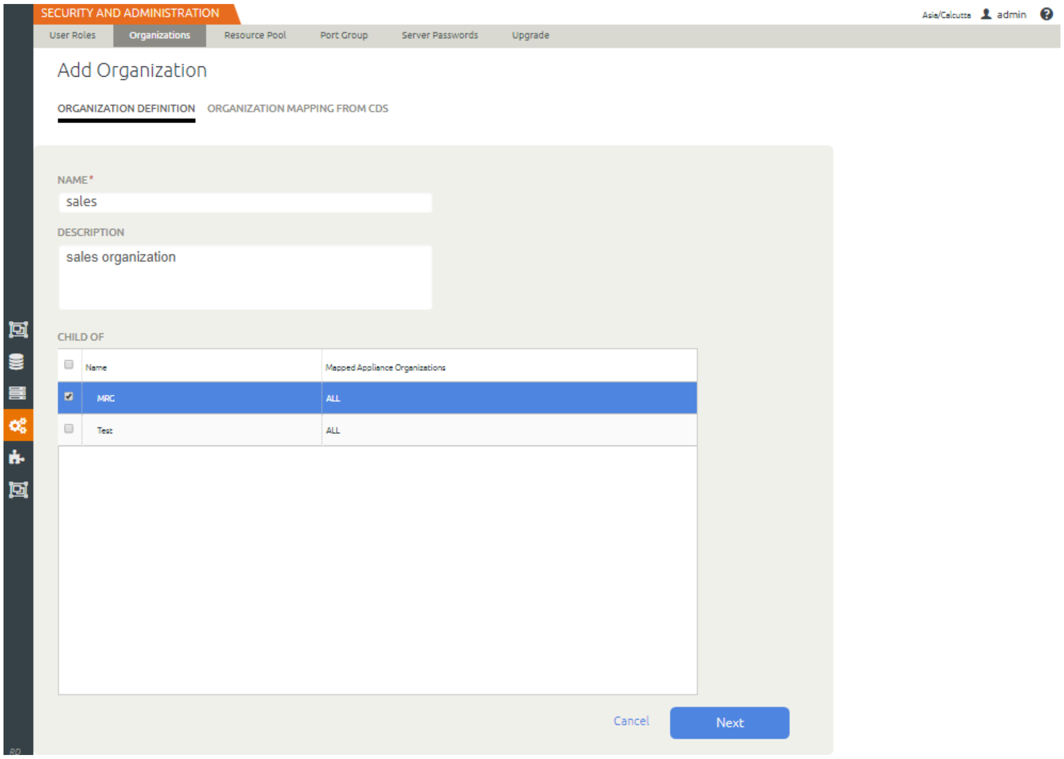
1. In the left navigation pane, click **Settings** > **Security and Administration** > **Organizations**.

   The Organizations page displays.

2. Click **+ADD ORGANIZATION** to create a new organization.

   The **Add Organization** page appears.

3. Enter the Organization Name in the **Name** field.



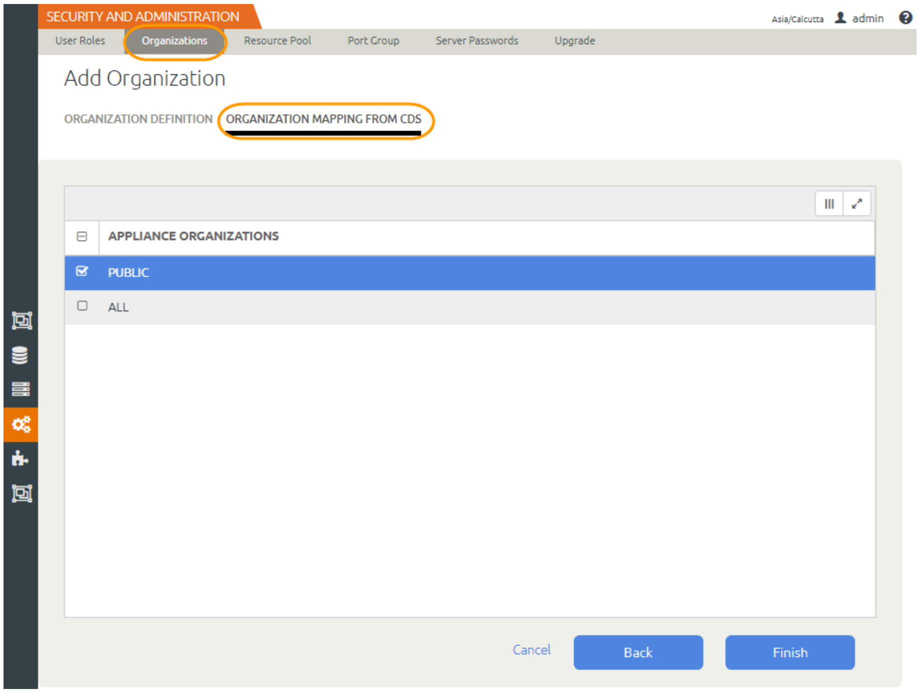
NAME*
sales

DESCRIPTION
sales organization

CHILD OF

□	Name	Mapped Appliance Organizations
☑	MRC	ALL
□	Test	ALL

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



⊟	APPLIANCE ORGANIZATIONS
☑	PUBLIC
□	ALL

7. Select the check-boxes for existing appliance that should be configured for the new organization,
8. Click **Finish** to create the Organization.

Editing an Organization Details

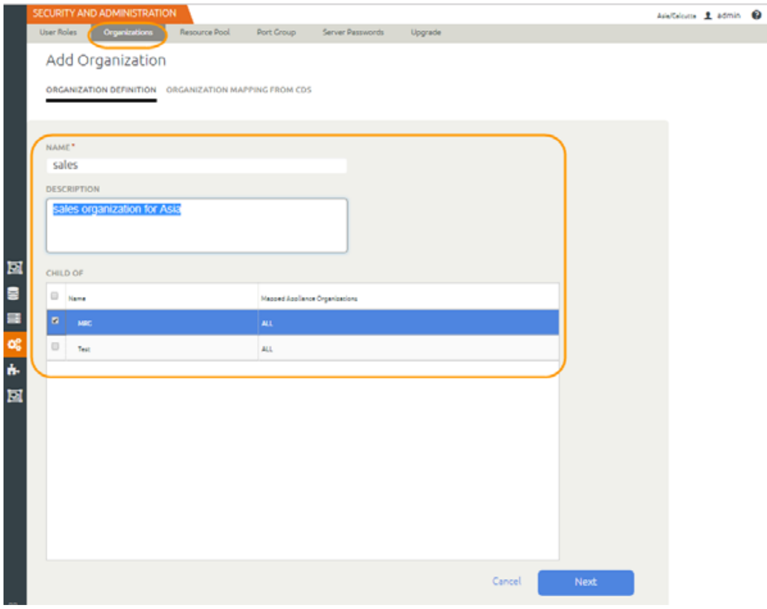
The Resiliency Director Server supports modifying the name, email contact, and address of an organization.

To edit the organization details:

1. In the left navigation pane, 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.



Add Organization

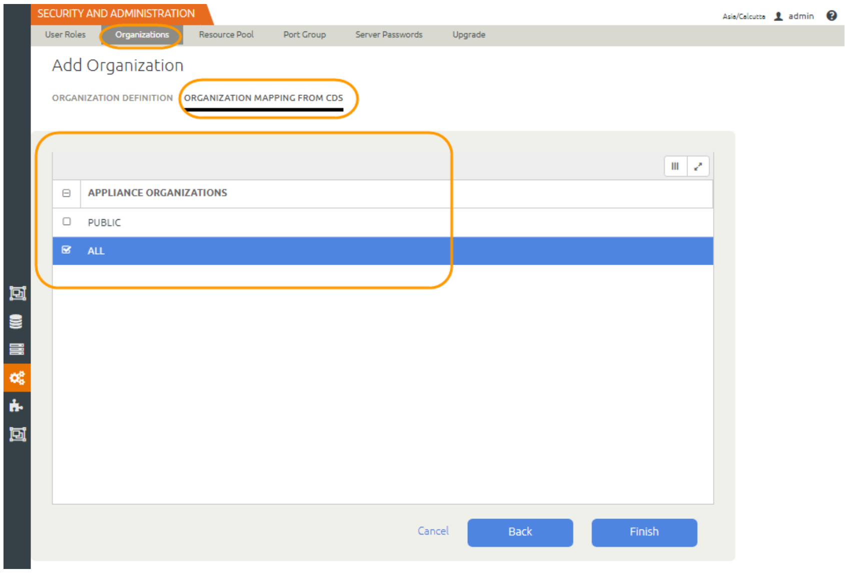
NAME *
sales

DESCRIPTION
sales organization for Asia

CHILD OF

	Name	Mapped Appliance Organizations
☑	MRC	ALL
□	Test	ALL

3. Edit the Organization Name and Description in their respective fields and click **Next**.



Add Organization

⊟	APPLIANCE ORGANIZATIONS
□	PUBLIC
☑	ALL

4. Select the **Appliance Organizations** using the respective name check boxes.

5. Click **Finish** to save the changes made to the organization.

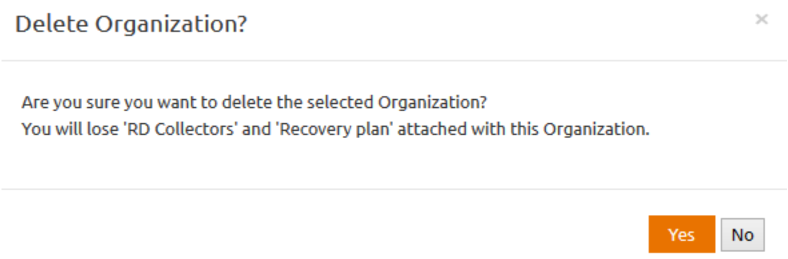
Deleting an Organization

To delete an organization:

1. In the left navigation pane, click Click **Settings** > **Security and Administration** > **Organizations**.

   The **Organizations** page displays.

2. Select the organization that you want to delete and click **Delete**. The **Delete Organization** dialog box appears asking for the confirmation to delete the organization.



Delete Organization?

Are you sure you want to delete the selected Organization?
You will lose 'RD Collectors' and 'Recovery plan' attached with this Organization.

3. Click **Yes** to delete the organization.
   Deleting an organization also deletes the entities associated with the recovery plans.

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

8 Managing the Actifio Resiliency Director Collectors

This chapter provides the details to add, list, edit, and delete the Actifio Resiliency Director Collectors.

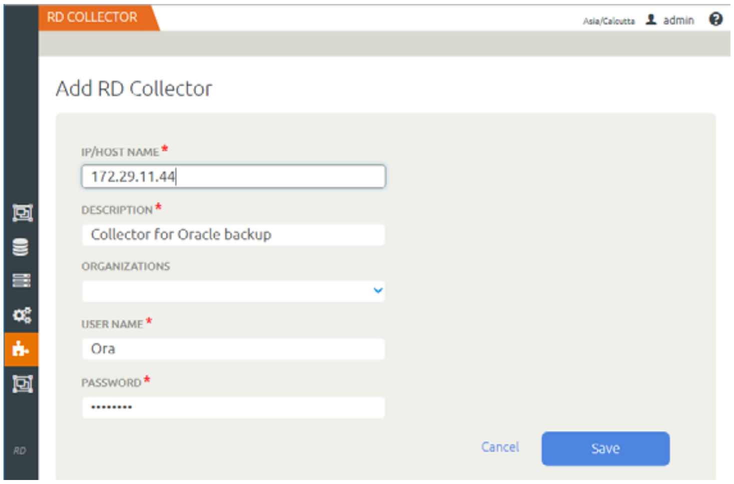
This chapter contains:

Adding an Actifio Resiliency Director Collector

This section provides the details to add an organization Resiliency Director Collector for existing organizations.

To add a Resiliency Director Collector:

1. In the left navigation pane, click **RD Collectors**. The **RD Collectors** page appears.
2. Click +**Add Collector**. The **Add RD Collector** page appears.
3. Enter the following:
   - **IP/Host Name**: Enter the IP address or Host name of the Resiliency Director Collector in the **IP/Host Name** field.
   - **Description**: (Optional) Enter description of the Resiliency Director collector that you want to add in the **Description** field.
   - **Organization**: Select the organization name from the **Organization** drop-down list to register in the Resiliency Director Server.
   - **User Name** and **Password**: Enter the user credentials in the **User Name** and **Password** fields.



Add RD Collector

IP/HOST NAME* 172.29.11.44

DESCRIPTION* Collector for Oracle backup

ORGANIZATIONS

USER NAME* Ora

PASSWORD* ••••••••

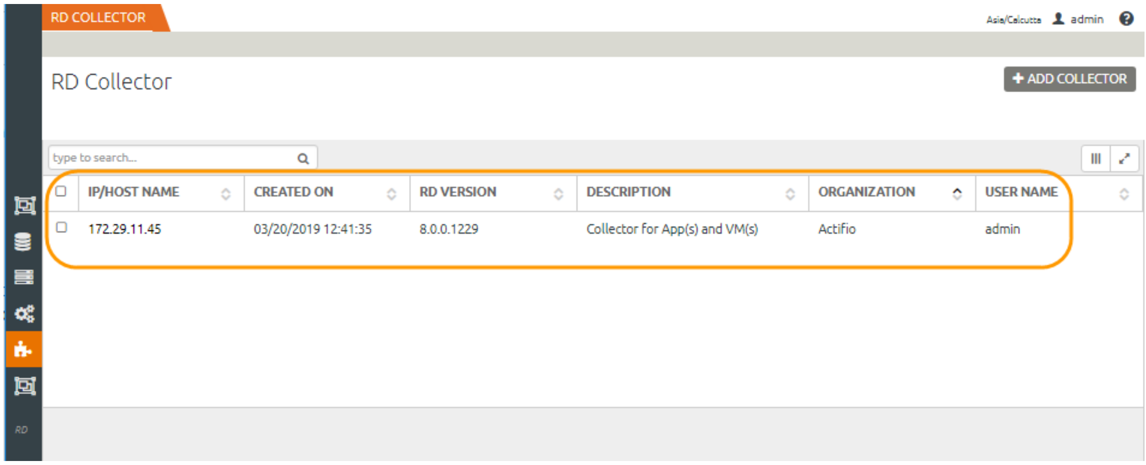
4. Click **Save** to add the Resiliency Director Collector.

Listing the Actifio Resiliency Director Collectors

To list the Resiliency Director Collector,

1. In the left navigation pane, click **RD Collectors**.

   The list of available **RD Collectors** appears.



□	IP/HOST NAME	CREATED ON	RD VERSION	DESCRIPTION	ORGANIZATION	USER NAME
□	172.29.11.45	03/20/2019 12:41:35	8.0.0.1229	Collector for App(s) and VM(s)	Actifio	admin

Resiliency Director CollectorsTable - Field Elements

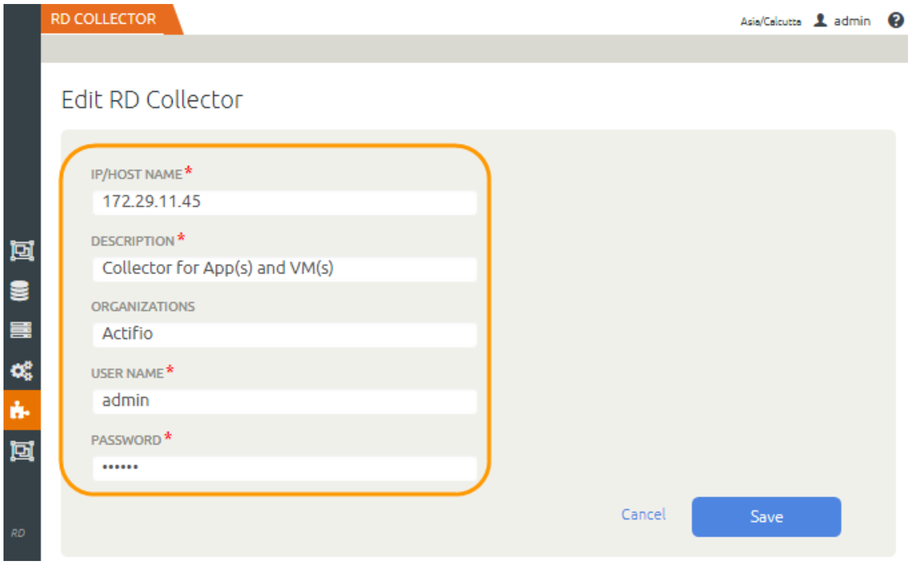
Field/Item	Description
IP/Host Name	Displays the host name or IP address of the Resiliency Director Collector.
Created On	Displays the date when the Resiliency Director Collector was created.
RD Version	Displays the Resiliency Director version.
Description	Displays your notes about the Resiliency Director Collector.
Organization	Displays name of the Resiliency Director organization.
User Name	Displays the logged in user name.

Updating an Actifio Resiliency Director Collector

To edit a Resiliency Director Collector:

1. In the left navigation pane, click **RD Collector**. The **RD Collectors** page appears.
2. Select the Resiliency Director Collector that you want to edit and click **Edit**.

   The **Edit RD Collector** page appears.
3. Edit the following:
   - **IP/Host Name**: Enter the IP address or Host name of the Resiliency Director Collector in the **IP/Host Name** field.
   - **Description**: Enter the description about the Resiliency Director collector that you want to add in the **Description** field.
   - **Organization**: (Optional) Edit the organization name.
   - **User Name** and **Password**: Enter the user credentials in the **User Name** and **Password** fields. The maximum character limit is set to 95.



Edit RD Collector

IP/HOST NAME*: 172.29.11.45

DESCRIPTION*: Collector for App(s) and VM(s)

ORGANIZATIONS: Actifio

USER NAME*: admin

PASSWORD*: ••••••

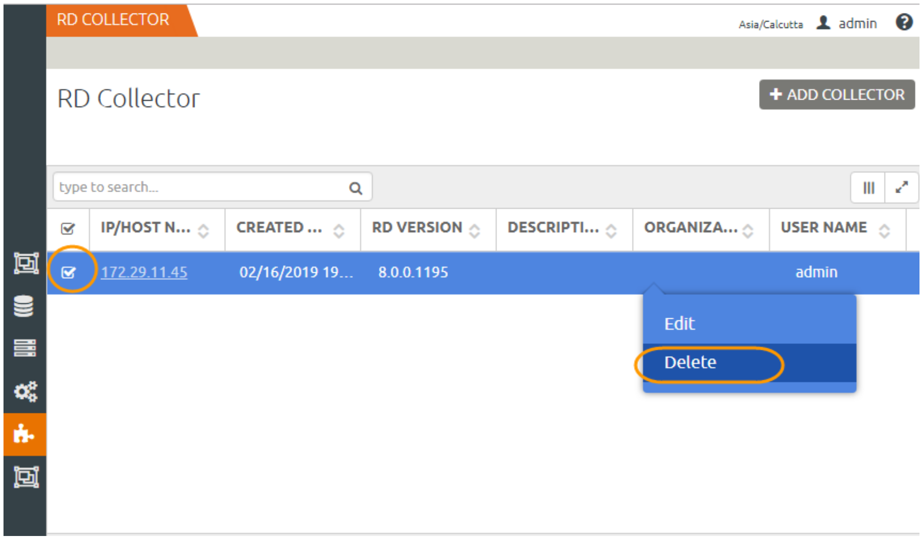
4. Click **Save** to update the changes.

Deleting an Actifio Resiliency Director Collector

The Resiliency Director Server supports deleting an existing Resiliency Director Collectors. You can delete multiple Resiliency Director Collectors at a time.

To delete a Resiliency Director Collector:

1. In the left navigation pane, click **RD Collector**. The list of available **Resiliency Director Collectors** appears.
2. Select the Resiliency Director Collector that you want to delete and click **Delete**.



☑	IP/HOST N...	CREATED ...	RD VERSION	DESCRIPTI...	ORGANIZA...	USER NAME
☑	172.29.11.45	02/16/2019 19...	8.0.0.1195			admin

3. In the Delete RD Collector dialogue, click **Confirm**.

Note: *Deleting an Resiliency Director Collector also deletes associated entities such as recovery plans.*

9 Managing Resource Pool

This chapter provides the details to discover, update, and delete resource pools. You can discover, update and delete child resource pool of any host. The CPU and memory resources for your resource pool are the guaranteed physical resources the host servers for a resource pool.

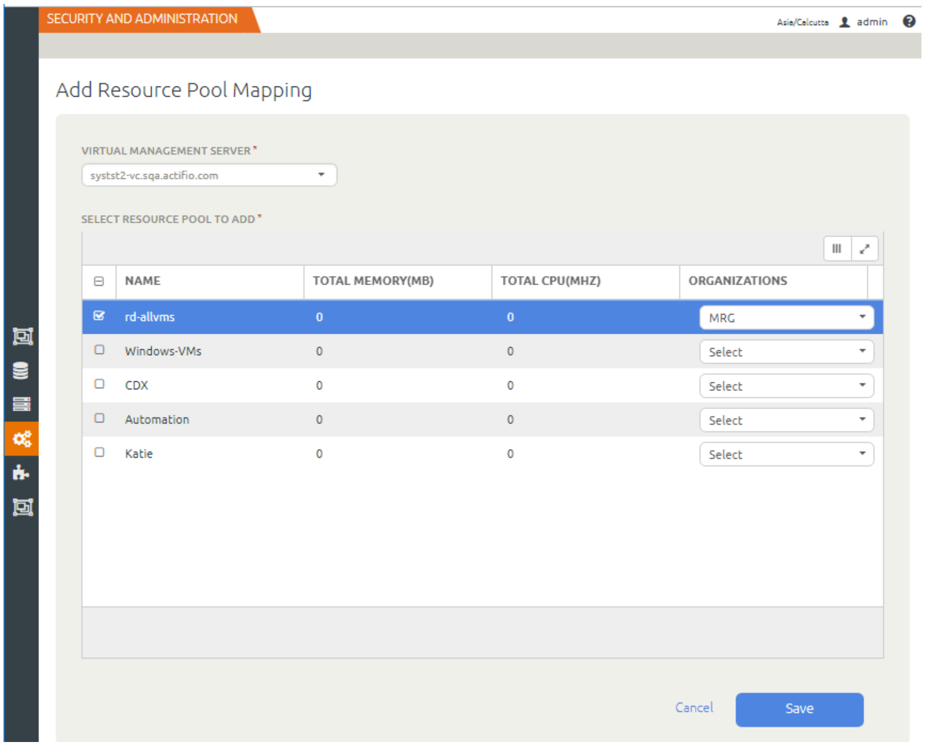
This chapter contains:

Add Resource Pool Mapping

This section provides the details to add a resource pool for any Virtual Management Server and its corresponding Organizations.

To add a resource pool mapping:

1. In the left navigation pane, **Security and Administration** > **Resource Pool**.
2. The **Resource Pool** page displays.
3. Click **+Add Resource Pool**. The **Add Resource Pool** page displays.



Add Resource Pool Mapping

VIRTUAL MANAGEMENT SERVER *
systst2-vc.sqa.actifio.com

SELECT RESOURCE POOL TO ADD *

⊟	NAME	TOTAL MEMORY(MB)	TOTAL CPU(MHZ)	ORGANIZATIONS
☑	rd-allvms	0	0	MRG
☐	Windows-VMs	0	0	Select
☐	CDX	0	0	Select
☐	Automation	0	0	Select
☐	Katie	0	0	Select

4. Select the **Virtual Management Server** for which you want to discover the resource pool and click **Save**.

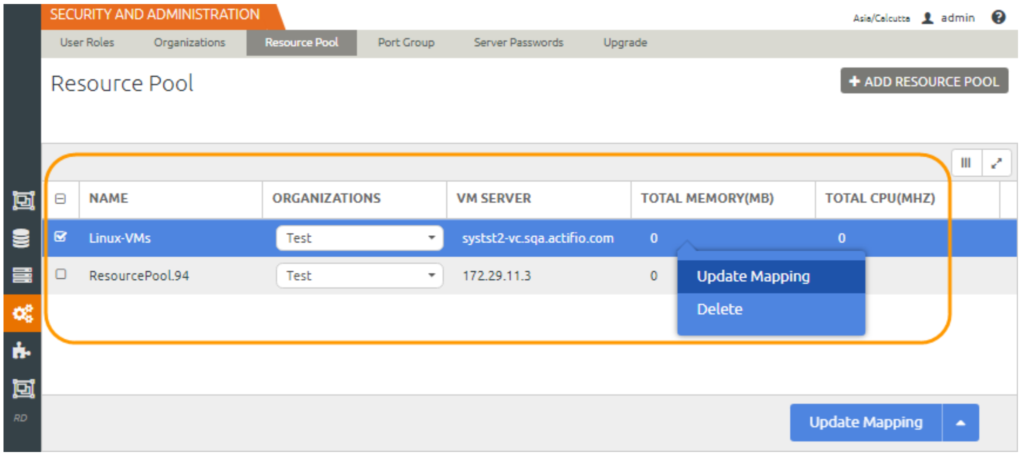
> ***Note:*** *For any resource pool names that are already available and you want to add Resource Pool for any specific organization.Click* ***Save****.*

5. Click name and select the corresponding **Organizations** from the drop down list and click **Save**.

Updating the Resource Pool Mapping

To update the resource pool mapping:

1. In the left navigation pane, click **Security & Administration** > **Resource Pool**. The **Resource Pool** page displays.
2. Select the resource pool name from **Name** column and click **Update Mapping**. The **Update Mapping** page displays.



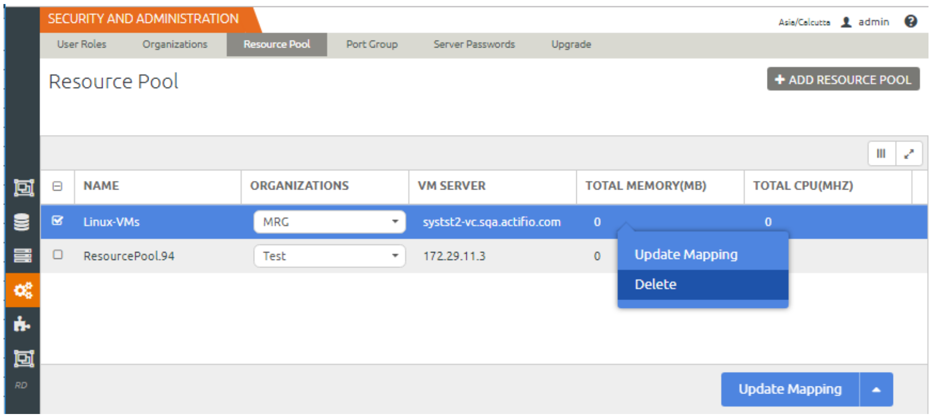
NAME	ORGANIZATIONS	VM SERVER	TOTAL MEMORY(MB)	TOTAL CPU(MHZ)
☑ Linux-VMs	Test	systst2-vc.sqa.actifio.com	0	0
□ ResourcePool.94	Test	172.29.11.3	0	

3. Click on resource pool name to update the mapping.
4. Click on **Organizations** drop down list for the corresponding resource pool name for which you want to update the mapping and click **Save**.

Deleting the Resource Pool Mapping

You can delete any Resource Pool mapping. To delete the resource mapping:

1. In the left navigation pane, click **Security & Administration** > **Resource Pool**. The **Resource Pool** page displays.
2. Select the resource pool name that you want to delete and click **Delete**.



NAME	ORGANIZATIONS	VM SERVER	TOTAL MEMORY(MB)	TOTAL CPU(MHZ)
☑ Linux-VMs	MRG	systst2-vc.sqa.actifio.com	0	0
□ ResourcePool.94	Test	172.29.11.3	0	

3. Click **Delete** in the confirmation dialog box.

Note: *If a resource pool is deleted then all the VMs are reassigned to parent pool.*

10 Managing Port Group Security

Port groups in the Resiliency Director aggregate multiple ports under a common configuration that provides a stable anchor for virtual machines connecting to labeled VMs. The Resiliency Director allows you to map to the VMs or Organizations corresponding to specific VMs.

This chapter provides the details to discover, update and map the port groups. The port groups can mapped for virtual machines or physical machines in the CSP environment.

This chapter contains the following topics:

Discovering and Mapping Port Groups

This section provides the details to discover the port groups for Virtual Management Servers and its corresponding Hosts and Clusters.

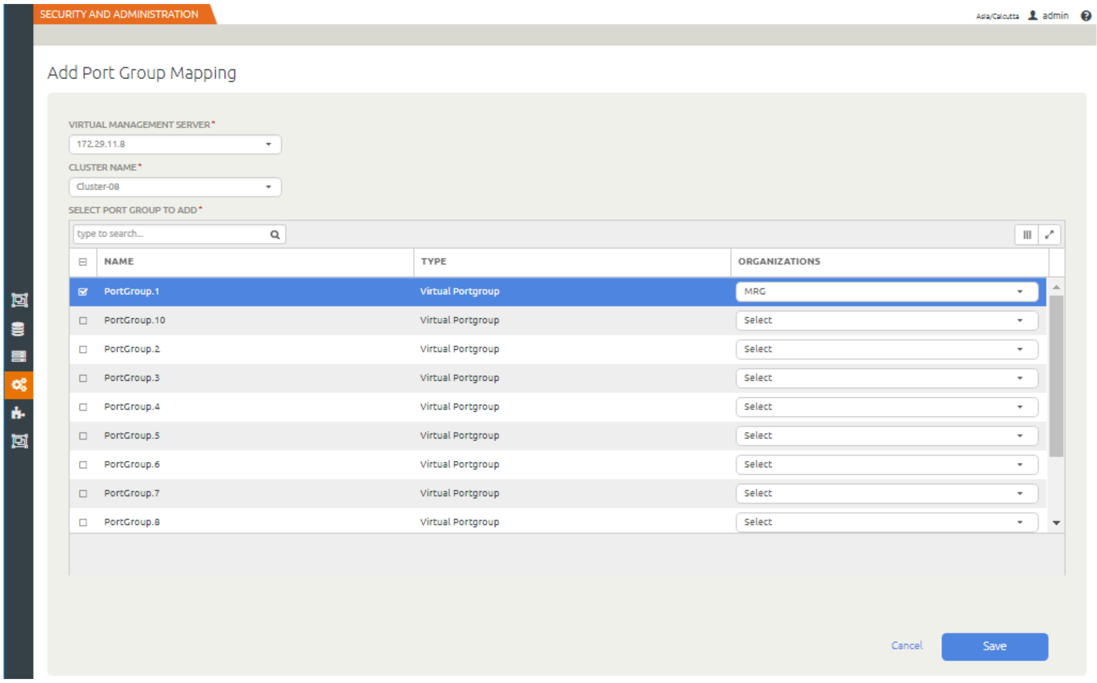
To discover port groups:

1. In the left navigation pane, click **Settings** > **Security and Administration** > **Port Group**.

   The **Port Group** page displays.

2. Click **Add Port Group**.

   The **Add Port Group Mapping** page displays.



Add Port Group Mapping

VIRTUAL MANAGEMENT SERVER*: 172.29.11.8

CLUSTER NAME*: Cluster-08

SELECT PORT GROUP TO ADD*

⊟	NAME	TYPE	ORGANIZATIONS
☑	PortGroup.1	Virtual Portgroup	MRG
□	PortGroup.10	Virtual Portgroup	Select
□	PortGroup.2	Virtual Portgroup	Select
□	PortGroup.3	Virtual Portgroup	Select
□	PortGroup.4	Virtual Portgroup	Select
□	PortGroup.5	Virtual Portgroup	Select
□	PortGroup.6	Virtual Portgroup	Select
□	PortGroup.7	Virtual Portgroup	Select
□	PortGroup.8	Virtual Portgroup	Select

3. Select the virtual management server from **Virtual Management Server** drop down list.

4. Select the desired host or cluster from the **Cluster** drop down list.

5. Select the **Port Group** name from the corresponding port group row and select the Organization using the drop-down list.

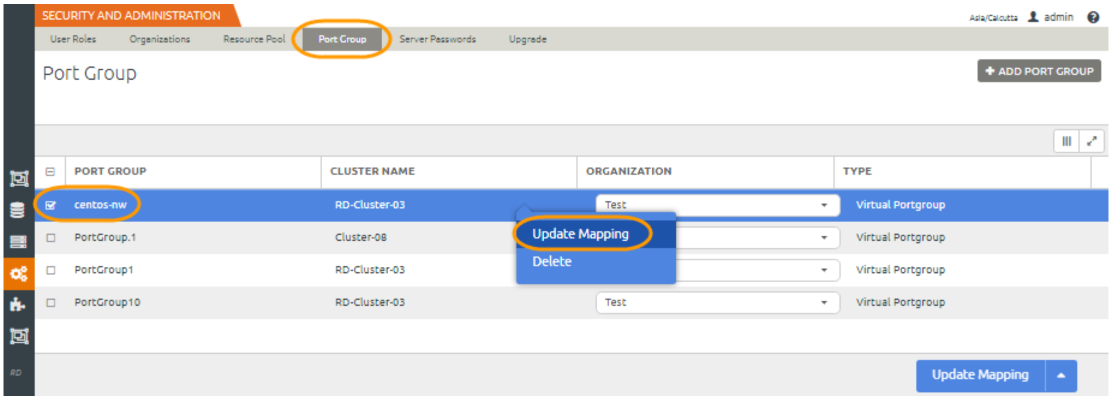
6. Click **Save**.

Updating the Port Group Mapping

To update the port group mapping:

1. In the left navigation pane, click **Settings** > **Security and Administration** > **Port Group**.

   The **Port Group** page displays the available Port Groups.



PORT GROUP	CLUSTER NAME	ORGANIZATION	TYPE
☑ centos-nw	RD-Cluster-03	Test	Virtual Portgroup
□ PortGroup.1	Cluster-08		Virtual Portgroup
□ PortGroup1	RD-Cluster-03		Virtual Portgroup
□ PortGroup10	RD-Cluster-03	Test	Virtual Portgroup

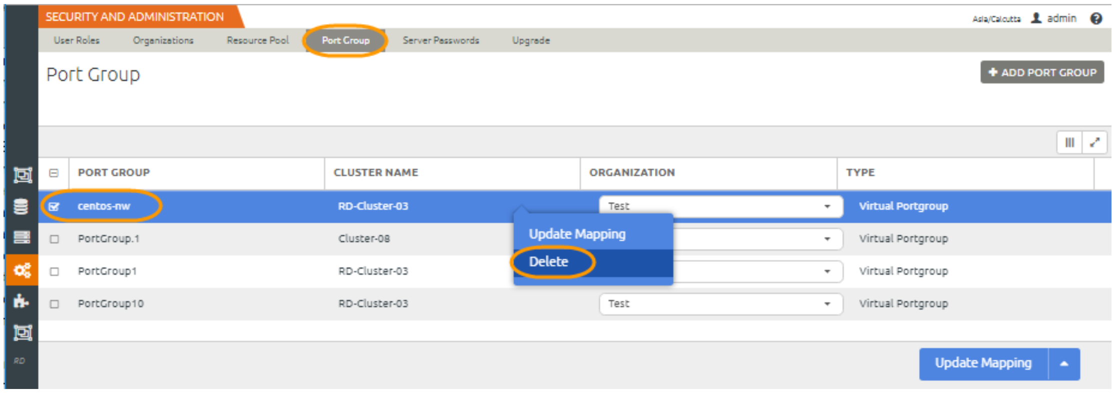
2. Right-click the port group and Click **Update Mapping**. The **Port Group** page displays.
3. Select the **Organizations** name from the corresponding port group you want to discover.

   The **Port Group** page displays.
4. Click **Update Mapping**.

Deleting the Port Groups

This section describes the steps to delete the port groups. To delete the port groups:

1. In the left navigation pane, click **Settings** > **Security and Administration** > **Port Group**. The **Port Group** page displays.
2. Select the port groups from the **Port Group** column and click **Delete**.



PORT GROUP	CLUSTER NAME	ORGANIZATION	TYPE
☑ centos-nw	RD-Cluster-03	Test	Virtual Portgroup
□ PortGroup.1	Cluster-08		Virtual Portgroup
□ PortGroup1	RD-Cluster-03		Virtual Portgroup
□ PortGroup10	RD-Cluster-03	Test	Virtual Portgroup

   A confirmation dialogue appears.

3. Click **Delete** in the confirmation dialogue.

Note: *Before deleting the selected port group(s), ensure that there are no dependencies associated with it, once you delete the port group, once you delete the port group, users edited the recovery plans unable to access them.*

11 Managing the Recovery Plans

This chapter provides the details to add, list, modify, disable, delete, and execute a recovery plan for the registered Resiliency Director organizations.

> ***Note:*** *For a CDS user who wants to run a recovery plan in the Resiliency Director, ensure that the organization for corresponding user has rights configured on the VMware vCenter Server, Protected VMs, Profile and Template with which VM is protected, as well as ESX hosts where we are executing the recovery plan.*

This chapter contains:

Adding a Recovery Plan

Resiliency Director supports creating a recovery plan for an organization and setting the recovery order to recover the application groups. Adding a recovery plan is a wizard based process. The wizard is divided into five steps:

- Application Groups
- Recovery Order
- Network Settings
- Schedule
- Summary

Note: *Port groups are entities present on a standard virtual switch / distributed virtual switch (DVSwtich). Before a CSP creates a recovery plan, you must create a virtual switch with pre-defined port groups on the corresponding virtual management server.*

Preserving the UUID and Ethernet PCI Slot Number

RD Collector collects the UUID and PCI slot numbers of all NIC cards during creation or update of application group. If you do not wish to preserve these values on the recovered VM, you need to set the following properties to false:

- **`preserveuuid`**: This property is set to **true** by default, based on this value, you can preserve the **uuid.bios** of the original VM on to the recovered VM.
- **`preserve-nic-pcislotnumber`**: This property is set to **true** by default, based on this value you can preserve the PCI Slot Numbers of Network Interface Cards that are present in Original VM on to the recovered VM.

If you do not wish to preserve these parameters, you can change them using the following commands:

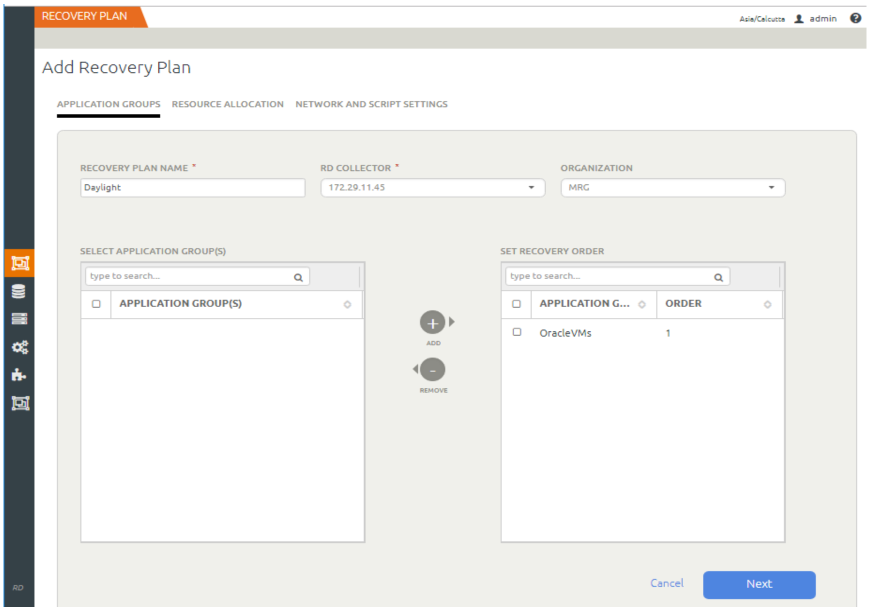
```
rdtask setproperty -property preserve-nic-pcislotnumber -value false

rdtask setproperty -property preserveuuid -value false
```

While creating a recovery plan, you can define:

- Existing application groups for which you can select one or more VMs
- VM resources
- Target resource pool on virtual management server
- Network Settings
- Pre-scripts/post-scripts for individual VM(s) and Application Group(s)

To add a recovery plan:

1. In the left navigation pane, click **Recovery Plans**. The **Recovery Plans** page appears.
2. Click +**Add Recovery Plan**. The **Add Recovery Plan** page appears.
3. Enter the recovery plan name in **Recovery Plan Name** field. You can provide maximum 100 alphanumeric characters. Only "-" and "_" special characters are supported.
4. Select the Resiliency Director Collector from the **RD Collector** drop-down list.
5. You may optionally select an organization from the **Organization** drop-down list, organization membership can be used to limit users to only accessing a subset of recovery plans.
6. Select the application groups from the **Select Application Group(s)** list.



RECOVERY PLAN

Asia/Calcutta admin

Add Recovery Plan

APPLICATION GROUPS RESOURCE ALLOCATION NETWORK AND SCRIPT SETTINGS

RECOVERY PLAN NAME *: Daylight

RD COLLECTOR *: 172.29.11.45

ORGANIZATION: MRG

SELECT APPLICATION GROUP(S)

type to search...

□	APPLICATION GROUP(S)

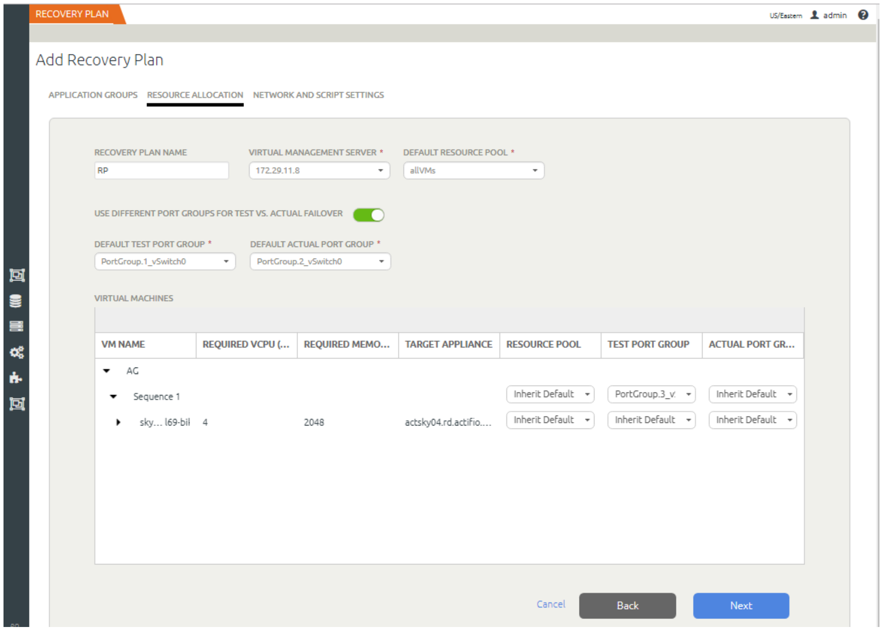
SET RECOVERY ORDER

type to search...

□	APPLICATION G...	ORDER
□	OracleVMs	1

7. To add Application Groups to the recovery plan, select them one at a time and click the "+" add button. Application groups will be executed in the order they are added. To change the order, remove application groups and re-add them using the "-" and "+" buttons. Application groups are always added at the end of the list and click **Next**.

   The **Resource Allocation** page appears.



Add Recovery Plan

RECOVERY PLAN NAME: RP

VIRTUAL MANAGEMENT SERVER *: 172.29.11.8

DEFAULT RESOURCE POOL *: allVMs

USE DIFFERENT PORT GROUPS FOR TEST VS. ACTUAL FAILOVER

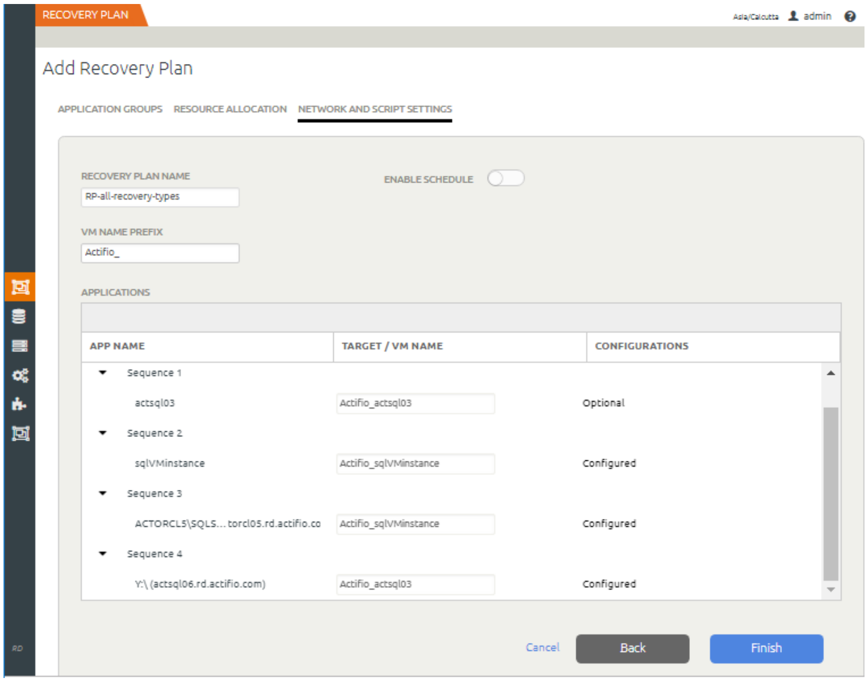
DEFAULT TEST PORT GROUP *: PortGroup.1_vSwitch0

DEFAULT ACTUAL PORT GROUP *: PortGroup.2_vSwitch0

VIRTUAL MACHINES

VM NAME	REQUIRED VCPU (...	REQUIRED MEMO...	TARGET APPLIANCE	RESOURCE POOL	TEST PORT GROUP	ACTUAL PORT GR...
AG						
Sequence 1				Inherit Default	PortGroup.3_v:	Inherit Default
sky... l69-bil	4	2048	actsky04.rd.actifio....	Inherit Default	Inherit Default	Inherit Default

8. Select:
   - The virtual management server from the **Virtual Management Server** drop-down list.
   - The resources from the **Default Resource Pool** drop-down list. For details about resource pool validations, see Resource Pool Validation on page 54.
   - The default resource pool may optionally be overridden for any listed sequence or VM if it is desired to recover VMs into a different resource pool than the default for the recovery plan.
   - The default port group from the **Default Port Group** drop-down list.
   - The default port group may optionally be overridden for any listed sequence, VM, or NIC if it is desired to recover the VMs or NICs into a different port group than the default for the recovery plan.
   - **Use Different Port Groups for Test Vs. Actual Failover** option to choose port groups separately for test and actual recovery.
9. Click **Next**. The **Network and Script Settings** page appears displaying the list of selected VMs or vApps or File Systems or SQL applications.



Add Recovery Plan

RECOVERY PLAN NAME: RP-all-recovery-types

ENABLE SCHEDULE ○

VM NAME PREFIX: Actifio_

APPLICATIONS

APP NAME	TARGET / VM NAME	CONFIGURATIONS
Sequence 1		
actsql03	Actifio_actsql03	Optional
Sequence 2		
sqlVMinstance	Actifio_sqlVMinstance	Configured
Sequence 3		
ACTORCL5\SQLS...torcl05.rd.actifio.co	Actifio_sqlVMinstance	Configured
Sequence 4		
Y:\ (actsql06.rd.actifio.com)	Actifio_actsql03	Configured

10. Use the **Enable Schedule** option to enable a schedule (Monthly, Weekly, Daily).

    Actifio Resiliency Director Server supports creating recovery plan schedules for the following types of intervals:

    - **Daily**: Create a daily schedule as per the defined start time. For example, if you provide the start time 9.00, then the recovery plan executes daily at 9.00 a.m.
    - **Weekly**: Creates a weekly recovery schedule as per the defined day of the week. For example, if you provide the start time as 9.00 and select Monday, then the recovery plan executes every Monday at 9.00.
    - **Monthly**: Creates a monthly recovery schedule as per the defined date of the month. For example, if you provide the start time as 9.00 and select 10 as date, then the recovery plan executes every month on 10th at 9.00.

11. To bulk-change VM names used during recovery with a prefix, modify the value for VM Name Prefix to any value. All VMs that have not had their names manually changed will be updated with the new prefix.

    Note: *for each VM being recovered, you may override the recovery plan's VM Name Prefix, as well as the entire VM name, by modifying the value in the "Target / VM Name" column.*

12. You can proceed without configuring the required applications and recovery plan state becomes Ready (info required). When you run the recovery plan, it will ask you to configure the application(s). For configuring the following applications:

    - For configuring a VM or create a new VM, refer **Configuring the VM** section in Actifio Resiliency Director Collector guide.
    - For configuring a Database Application, refer **Configuring the Database** section in Actifio Resiliency Director Collector guide.
    - For configuring a File System Application, refer **Configuring the File System** section in Actifio Resiliency Director Collector guide.

Note: *Configuration details for each application can be configured in the Application Group, and optionally you can override the configuration details in the Recovery plan.*

13. Click **Finish** to complete the process

Resource Pool Validation

The following conditions are validated while verifying the resource pool:

- Sum up values for required CPU and RAM reservations (if any) for all VMs is assigned to the resource pool.
- Compare the required CPU and RAM to the resource pool LIMIT. Flag condition "ERROR" if the limit is lower than the required CPU or RAM. If pool is set to unlimited, there is no error possible.
- Compare the required CPU and RAM to the resource pool RESERVATION. Flag condition "WARNING" if the reservation is lower than the required CPU or RAM. However, if the limit is set to unlimited, then do not flag as warning status.

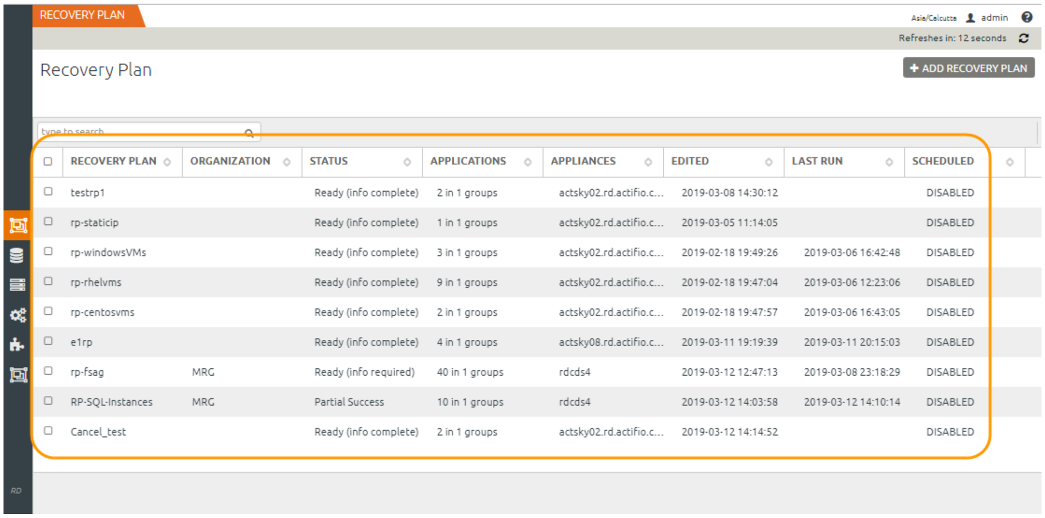
Note: *It is recommended to configure the VM resources (CPU and memory) with finite limits instead of using the unlimited resource configuration.*

If you want to configure a particular VM resource using unlimited settings, then the corresponding resource pool to be used must have unlimited resource consumption setting. The Resiliency Director allows the user to create a recovery plan if the resource pool have “Unlimited” flag enabled for the resource pool limit.

Listing Recovery Plans

The **Recovery Plans** screen includes a list of existing recovery plans in the Resiliency Director Server site. It has the **Add**, **Manage**, **Edit**, **Run**, and **Delete** options.

The details of the Recovery Plans page are described in the following table.



□	RECOVERY PLAN	ORGANIZATION	STATUS	APPLICATIONS	APPLIANCES	EDITED	LAST RUN	SCHEDULED
□	testrp1		Ready (info complete)	2 in 1 groups	actsky02.rd.actifio.c...	2019-03-08 14:30:12		DISABLED
□	rp-staticip		Ready (info complete)	1 in 1 groups	actsky02.rd.actifio.c...	2019-03-05 11:14:05		DISABLED
□	rp-windowsVMs		Ready (info complete)	3 in 1 groups	actsky02.rd.actifio.c...	2019-02-18 19:49:26	2019-03-06 16:42:48	DISABLED
□	rp-rhelvms		Ready (info complete)	9 in 1 groups	actsky02.rd.actifio.c...	2019-02-18 19:47:04	2019-03-06 12:23:06	DISABLED
□	rp-centosvms		Ready (info complete)	2 in 1 groups	actsky02.rd.actifio.c...	2019-02-18 19:47:57	2019-03-06 16:43:05	DISABLED
□	e1rp		Ready (info complete)	4 in 1 groups	actsky08.rd.actifio.c...	2019-03-11 19:19:39	2019-03-11 20:15:03	DISABLED
□	rp-fsag	MRG	Ready (info required)	40 in 1 groups	rdcds4	2019-03-12 12:47:13	2019-03-08 23:18:29	DISABLED
□	RP-SQL-Instances	MRG	Partial Success	10 in 1 groups	rdcds4	2019-03-12 14:03:58	2019-03-12 14:10:14	DISABLED
□	Cancel_test		Ready (info complete)	2 in 1 groups	actsky02.rd.actifio.c...	2019-03-12 14:14:52		DISABLED

Recovery Plans Table - Field Elements

Field/Item	Description
Recovery Plan	Displays the name of the recovery plan.
Organization	Displays the name of the organization configured for the recovery.
Status	Displays the status of the recovery plan.
Applications	Shows the number of applications and application groups in a recovery plan.
Appliances	Name of the Actifio Appliances used
Edited	Last modified date and time of recovery plan.
Last Run	Last run date and time of recovery plan.
Scheduled	Whether schedule is enabled or disabled.

Note: *Any recovery plan that executes at the given schedule time does so in the test recovery mode. You have an option to separately execute a recovery in test recovery mode by clicking the* ***Run Now*** *button present in the recovery plan listing accordion.*

Recovery Plan Execution Status Description

Actifio Resiliency Director Server provides the following recovery plan execution statuses:

Ready (info complete)

When a recovery plan is created and all validations for the recovery plan are successful, the status of a recovery plan becomes `Ready (info complete)`. You can execute a recovery plan whose status is Ready `(info complete)`.

Ready (Info required)

When a recovery plan is created and all validations for the recovery plan are not successful, the status of a recovery plan becomes `Ready (info required)`. You can use **execute once** a recovery plan whose status is Ready `(info required)`.

In Progress

When you execute a recovery plan, the status becomes `In progress`. as the recovery plan execution is in progress.

Failed

When the execution of a recovery plan encounters any error or if recovery of a critical VM fails, the status of a recovery plan becomes `Failed`.

Success

When a recovery plan is executed successfully, the status of a recovery plan becomes `Success`.

Partial Success

When you execute a recovery plan, and recovery of a non critical VM fails; the status of a recovery plan becomes `Partial Success`.

Canceling

When you cancel a recovery plan, the status of a recovery plan becomes `Canceling`.

Canceled

When cancellation of a recovery plan is successful, the status of a recovery plan becomes `Canceled`.

Resetting

When you reset a recovery plan, the status of a recovery plan becomes `Resetting`.

Reset Failed

When resetting a recovery plan fails, the status of a recovery plan becomes `Reset Failed`.

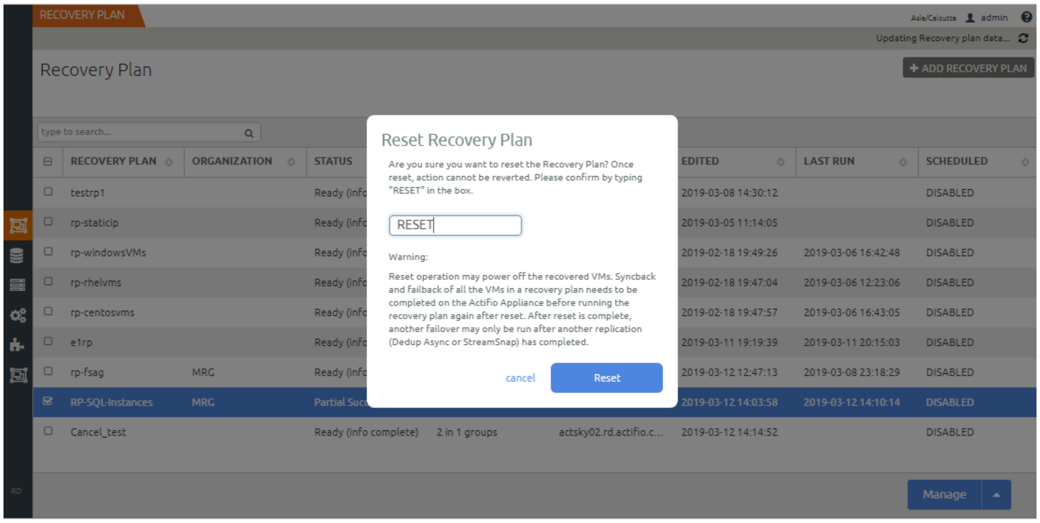
Resetting the Recovery Plan Status

If status of the recovery plan is not **Ready (info required) or Ready (info complete),** you can change it to **Ready (info required) or Ready (info complete)**. However, if status of the recovery plan is in **In progress**, you have to wait until the recovery plan process is complete.

> ***Note:*** *To reset manually from the Actifio Appliance, see* To reset a recovery plan, executed in an actual recovery mode:. *For more information on actual mode, see* Actual mode recovery *on page 61.*

To reset a recovery plan executed in test recovery mode:

1. Select the recovery plan of which you want to change the status and then right-click **Reset**. The **Reset** Recovery Plan dialog appears asking for the confirmation to reset the recovery plan status.



⊟	RECOVERY PLAN	ORGANIZATION	STATUS			EDITED	LAST RUN	SCHEDULED
☐	testrp1		Ready (info			2019-03-08 14:30:12		DISABLED
☐	rp-staticip		Ready (info			2019-03-05 11:14:05		DISABLED
☐	rp-windowsVMs		Ready (info			2019-02-18 19:49:26	2019-03-06 16:42:48	DISABLED
☐	rp-rhelvms		Ready (info			2019-02-18 19:47:04	2019-03-06 12:23:06	DISABLED
☐	rp-centosvms		Ready (info			2019-02-18 19:47:57	2019-03-06 16:43:05	DISABLED
☐	e1rp		Ready (info			2019-03-11 19:19:39	2019-03-11 20:15:03	DISABLED
☐	rp-fsag	MRG	Ready (info			2019-03-12 12:47:13	2019-03-08 23:18:29	DISABLED
☑	RP-SQL-Instances	MRG	Partial Suc			2019-03-12 14:03:58	2019-03-12 14:10:14	DISABLED
☐	Cancel_test		Ready (info complete)	2 in 1 groups	actsky02.rd.actifio.c...	2019-03-12 14:14:52		DISABLED

Reset Recovery Plan

Are you sure you want to reset the Recovery Plan? Once reset, action cannot be reverted. Please confirm by typing "RESET" in the box.

RESET

Warning:

Reset operation may power off the recovered VMs. Syncback and failback of all the VMs in a recovery plan needs to be completed on the Actifio Appliance before running the recovery plan again after reset. After reset is complete, another failover may only be run after another replication (Dedup Async or StreamSnap) has completed.

cancel Reset

2. Type **RESET** in the given field to confirm the operation and click **Reset** to reset the recovery plan status. If you click the Reset button, you cannot cancel the recovery plan that is initiated for the reset operation.

***Note: Reset for Test mode** will unmount-delete the copies which will also delete VMs and remove applications from DR CDS/Sky.*

To reset a recovery plan, executed in an actual recovery mode:

A clean-up is required from Actifio Appliance side to reset a recovery plan executed in an actual mode.

1. Clean-up the failover images from Actifio Appliance.

   ***Note:** For actual recovery of a ready VM, you must rename the VM to its previous name before cleaning-up the failover images from Actifio Appliance.*

   ---

2. From vCenter Server, delete the vApp created by recovery plan.
3. On the Recovery Plans page of Resiliency Director Server UI, click **Reset**. The **Reset** dialog box appears asking for the confirmation to reset the recovery plan status.
4. Type **RESET** in the given field to confirm the operation and click **Reset** to reset the recovery plan status.

   ***Note:** If you click the Reset button, you cannot cancel the recovery plan that is initiated for the reset operation.*

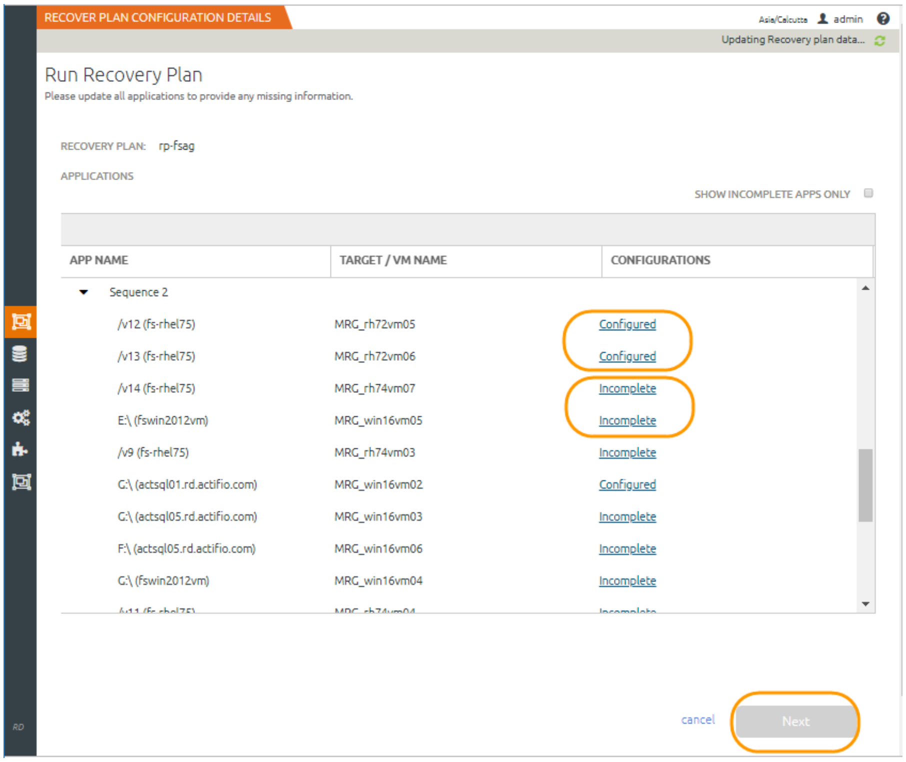
Recovery plan (Run Once):

For any recovery plan that needs more information before it can be run, Actifio uses the status “**Ready (info required)**”.

To Run the recovery plan once:

1. Right-click the recovery plan and select **Run**.

   The **Run Recovery Plan** wizard appears, which shows the configuration status for all the applications, and indicates the applications that need more information. Any plan that has “To be Determined (TBD)” for the target or has a blank required field (like SQL Instance), shows “Incomplete”.


RECOVER PLAN CONFIGURATION DETAILS
Asia/Calcutta
admin
Updating Recovery plan data...
SHOW INCOMPLETE APPS ONLY □
cancel
Next

Run Recovery Plan

Please update all applications to provide any missing information.

RECOVERY PLAN: rp-fsag

APPLICATIONS

APP NAME	TARGET / VM NAME	CONFIGURATIONS
Sequence 2		
/v12 (fs-rhel75)	MRG_rh72vm05	Configured
/v13 (fs-rhel75)	MRG_rh72vm06	Configured
/v14 (fs-rhel75)	MRG_rh74vm07	Incomplete
E:\ (fswin2012vm)	MRG_win16vm05	Incomplete
/v9 (fs-rhel75)	MRG_rh74vm03	Incomplete
G:\ (actsql01.rd.actifio.com)	MRG_win16vm02	Configured
G:\ (actsql05.rd.actifio.com)	MRG_win16vm03	Incomplete
F:\ (actsql05.rd.actifio.com)	MRG_win16vm06	Incomplete
G:\ (fswin2012vm)	MRG_win16vm04	Incomplete
/v11 (fs-rhel75)	MRG_rh74vm04	Incomplete

Run Once Recovery Plan

2. Once you configure the incomplete applications in the recovery plan Run Once wizard, and click **Next**.
3. The **Run** dialogue appears.
4. Type **RECOVER** in the given field, and choose the mode (Test or Actual).
5. Click Run to confirm the operation.

   Once you resets that recovery plan, then it should again go to Ready (info required) status.

Modifying a Recovery Plan

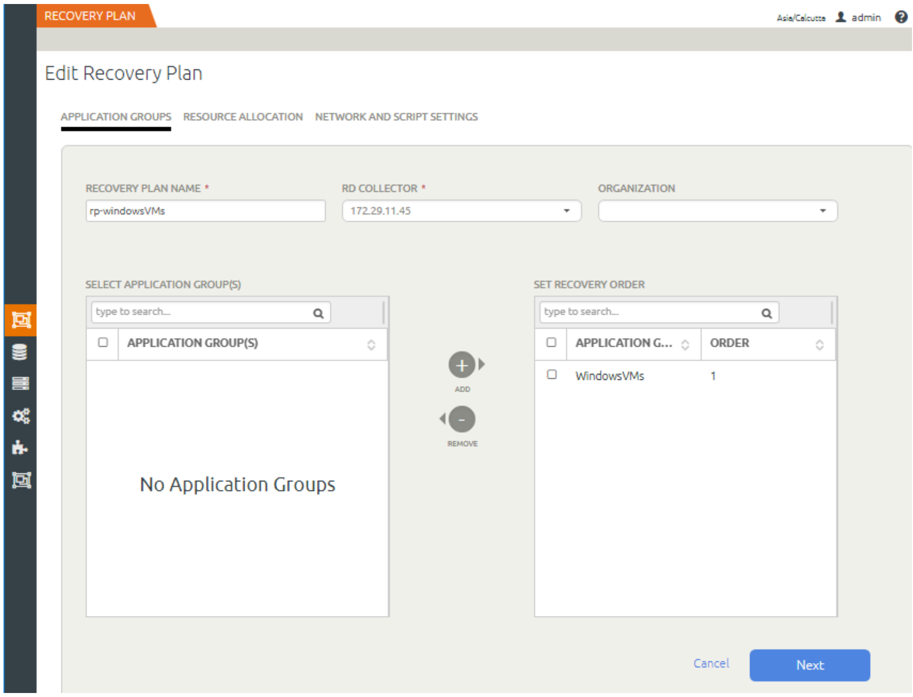
Actifio Resiliency Director Server supports modifying the Actifio Appliance, virtual management server, resource pool, and recovery order of a recovery plan. You can also stop a recovery plan schedule by using the **Edit** option.

If Organization Site Administrator modifies the application groups on Resiliency Director Collector site, the status of corresponding recovery plans having the modified application groups become Invalid on the Resiliency Director Server site. You must edit these recovery plans to validate them and move them back to Ready To Run state.

> ***Note:*** *You can modify the recovery plans with the Ready (info required) or Ready (info complete) status only. Modifying the recovery plans will not remove the VMs from the virtual management server.*

To modify a recovery plan:

1. In the left navigation pane, click **Recovery Plans**. The **Recovery Plans** page appears.
2. Select a recovery plan that you want to edit and then click **Edit**. The **Edit Recovery Plan** page appears.



RECOVERY PLAN NAME * rp-windowsVMs

RD COLLECTOR * 172.29.11.45

ORGANIZATION

□	APPLICATION GROUP(S)
	No Application Groups

□	APPLICATION G...	ORDER
□	WindowsVMs	1

Edit Recovery Plan

3. Modify the recovery plan name in **Recovery Plan Name** field.
4. You can modify select the Resiliency Director, Organization and Application group details using the respective drop-down list.
5. Modify the Application Groups if required, by adding the Application Groups to the **Set Recovery Order** section to define the recovery order. The recovery order appears in the ascending order. You can filter the Application Groups in the Select Application Groups section, if required and click **Next.**

   The **Resource Allocation** page appears.
6. Modify the fields if required for the following:
   - The virtual management server from the **Virtual Management Server** drop-down list.
   - The resources from the **Default Resource Pool** drop-down list. For details about resource pool validations, see Resource Pool Validation on page 54.

- o The default port group from the **Default Port Group** drop-down list.

7. Click **Next**. The **Network and Script Settings** page appears displaying the list of selected VMs or vApps for the recovery plan.
8. Use the **Enable Schedule** option to enable a schedule (Monthly, Weekly, Daily).
9. Click **Finish** to complete the process.

The modified details are listed in the accordion and recovery plan listing grid.

Executing a Recovery Plan

The Actifio Resiliency Director Server supports executing recovery plan in the test and actual mode. If a recovery plan execution is triggered manually, it precedes over the scheduled recovery plan execution.

Test mode recovery

When you execute a recovery plan in test mode, the recovery plan uses less resources if alternate values are entered for CPU and memory of the VMs being recovered. The Reset operation after a test recovery will cleanup all VMs. Also note that the test recovery performs a test-fail over on the associated Actifio Appliance, which does not enable change tracking for reverse incremental replication (Sync-back).

Actual mode recovery

When you execute a recovery plan in actual mode, a recovery plan uses all the resources that are required by the virtual machine. The reset of the recovery plan will not cleanup the recovered VMs, that RD will initiate a "failover" for each VM on the associated Actifio Appliance, and therefore the user has the ability to manually perform reverse incremental replication (sync-back), as well as restores and fail-back using the Actifio Appliance directly.

The following conditions are applicable for the ESXi server having local or shared storages:

- In the Resiliency Director Server, the ESXi server used for a recovery plan (via. a resource pool) should have sufficient single shared storage.
- If the ESXi server has a local storage, after executing the recovery plan, the restored VMs resides in the local storage and the VMs are not available for migration.
- If the ESXi server has a shared storage, after executing the recovery plan, the restored VMs reside in the shared storage. Then the VMs are available for migration.
- If the ESXi server has local storage and shared storage, then by default, Resiliency Director uses the shared storage.

Note: *In the ESXi server, you must first add the shared (SAN) storage. Resiliency Director selects the shared storage (configured local storage is selected last).*

To execute a recovery plan:

1. In the left navigation pane, click **Recovery Plan**. The **Recovery Plan** page appears.
2. Right-click the recovery plan and choose the **Manage** option to see the recovery plan details.
3. To run a recovery plan:

   Note: *Applicable for recovery plans with status '**Ready (Info Complete)**' and '**Ready (Info Required)**'.*

   Note: *For recovery plans with the status: '**Ready (Info Required)**', you need to provide the required information using the **Run Recovery Plan** page.*

   - o Choose a recovery plan, right-click and select the **Run**. The **Run** confirmation dialog appears.
   - o In the **Run** confirmation dialog, type **RECOVER** in the text box.
   - o Select the mode of recovery, Actual or Test from the **Mode** drop-down list.
   - o Click **Run**. The details about test and actual mode are described in the Test mode recovery and Actual mode recovery sections. You cannot modify a recovery plan when recovery is in progress.

4. To reset a recovery plan:

***Note:** Applicable for recovery plans with status '**Success'**, **Failed**' and 'Reset Failed'.*

- o Choose the recovery plan with status, right-click the plan and select the **Reset**. The **Reset Recovery Plan** confirmation dialog appears.
- o In the confirmation dialog, type **RESET** the text box.
- o Click **Reset**.

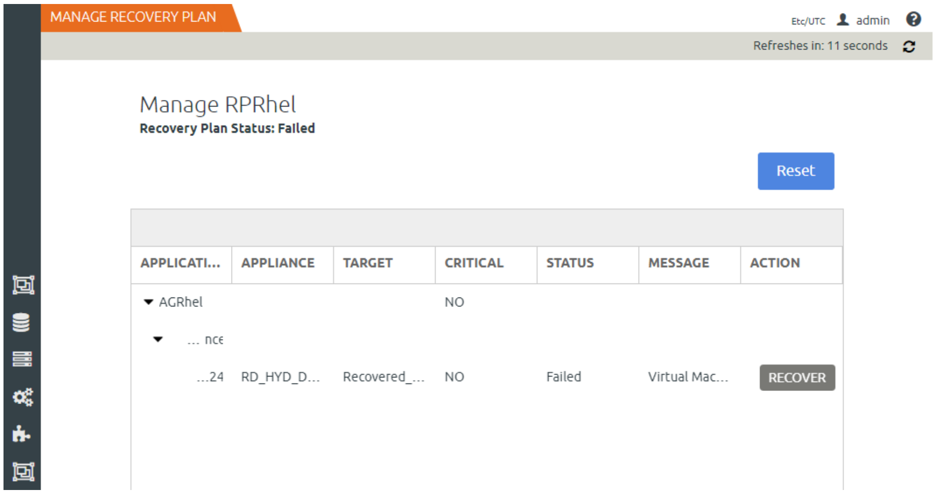
Recovering a Single VM

By using the Single VM Recovery feature, you can recover a single VM in a recovery plan. If a recovery plan is canceled or a single VM is failed during recovery plan execution then you can select that particular VM for recovery without affecting the other VMs.

To recover a single VM:

1. In the left navigation pane, click **Recovery Plans**. The **Recovery Plans** page appears.
2. Select the failed recovery plan of which you want to recover a single VM and right-click and select **Manage** to view the failed VMs.

   The Manage Recovery Plan page appears.

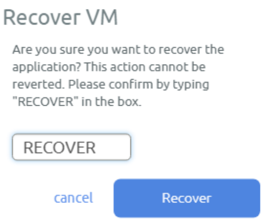


Manage RPRhel

Recovery Plan Status: Failed

APPLICATI...	APPLIANCE	TARGET	CRITICAL	STATUS	MESSAGE	ACTION
AGRhel			NO			
... nce						
...24	RD_HYD_D...	Recovered_...	NO	Failed	Virtual Mac...	RECOVER

3. Click **Recover** with respect to the failed VM. The **Recover VM** dialog box appears asking for the confirmation to recover the selected single VM.



Recover VM

Are you sure you want to recover the application? This action cannot be reverted. Please confirm by typing "RECOVER" in the box.

RECOVER

4. Type **RECOVER** in the text field to confirm the operation and click **OK**. The recovery plan status changes to In progress.

***Note:** You cannot cancel the single VM recovery process that is initiated.*

Recovering parallel VM

For parallel VM recovery feature to work efficiently, you have to tweak the following of properties for vCenter server, Resiliency Director server and ESX host:

vCenter

- **Memory (RAM) / CPU**: Increase RAM/CPU based on the number of VMs to be recovered in the single sequence. Preferably use a multi CPU machine instead of using multi core machine.
- **Java heap size**: Increasing Java heap size for the inventory service and storage profiles usually helps in improving the performance.
- **Database type**: Separate installation of database instead of depending on embedded database would enhance the performance.

ESX host

- Increase the heap size to 256MB.

RD Server

Set the JVM max heap size (xmx) value to 4GB. To change the heap size perform the following steps:

1. Open file `/act/rdprovider/rdstartup.sh`
2. Replace -xmx<value> with the desired heap size value to which you want to increase.

- Example: If you want to increase the heap size t o 4 GB, first the convert the value to MB (4096 MB), and then replace -xmx256 with -xmx4096

IP Address Retention

IP address retention is a feature that allows you to retain the same IP addresses for the virtual machines, present on the Actifio Resiliency Director Server site that were configured on the Actifio Resiliency Director Collector site.

Replicate the DHCP server of the Actifio Resiliency Director site to the Actifio Resiliency Director site to retain the IP address (dynamic or static) for the corresponding VMs. If the DHCP server is not replicated then IP address retention may not work for the DHCP server that is getting used on the Actifio Resiliency Director Server site.

Actifio Resiliency Director clones the MAC addresses of the virtual machines at the time of recovery plan execution to retain the IP addresses. IP addresses are retained irrespective of the IP address type (dynamic or static) allocated to the VMs on the Actifio Resiliency Director Collector site.

***Note:** If the Actifio Resiliency Director Collector user, enforces the IP address type as **static** to a virtual machine while adding or editing an application group under the **VM Settings** page > **VM Configuration**, then for such virtual machines Actifio Resiliency Director will not clone the MAC addresses.*

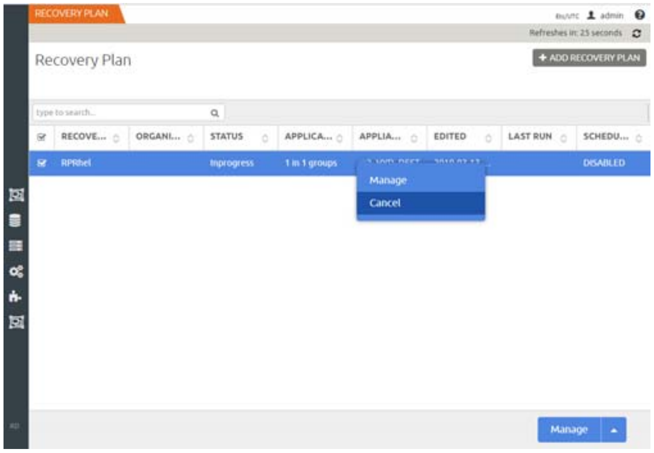
During the recovery plan execution, if a MAC address conflict is detected for a virtual machine, then the recovery status for that virtual machine is marked as failed. Over all recovery plan execution status depends on whether the failed virtual machine is critical or not. For example: If MAC address conflict occurs for a critical virtual machine, then over all recovery plan execution status is **Failed**. And for non critical virtual machine, recovery plan execution status is **Partial Success**.

Canceling a Recovery Plan execution

This section describes how to cancel a recovery plan while it's executing. You can cancel the recovery plan execution in progress at any point-in-time, if that plan is executed by mistake, or most of the virtual machines are failing due to unknown, or resource insufficiency reasons.

To cancel a recovery plan execution:

1. In the left navigation pane, click **Recovery Plans**. The **Recovery Plans** page appears.
2. Select the recovery plan of which you want to cancel the execution and then right-click and select **Cancel**.

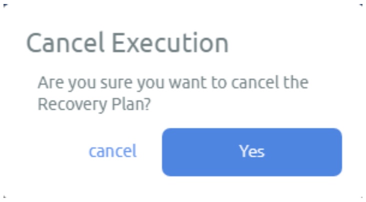


Recovery Plan

☑	RECOVE...	ORGANI...	STATUS	APPLICA...	APPLIA...	EDITED	LAST RUN	SCHEDU...
☑	RPRhel		Inprogress	1 in 1 groups	[illegible]	[illegible]		DISABLED

Canceling a Recovery Plan

The **Cancel Execution** dialog box appears asking for the confirmation to cancel



Cancel Execution

Are you sure you want to cancel the Recovery Plan?

3. Click **Yes** to start the recovery plan execution cancellation.
   If you click the Yes button, you cannot cancel the recovery plan that is initiated for the cancel operation.

Note: *On canceling a recovery plan execution, the Actifio Resiliency Director exits after the next VM processing (recovering) is complete.*

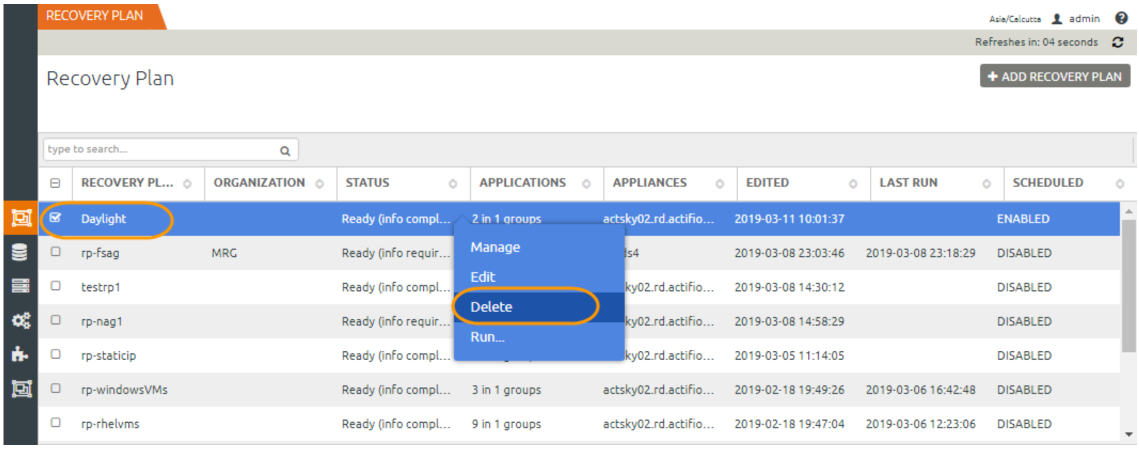
Deleting a Recovery Plan

This section guides you how to delete a recovery plan.

***Note:** You can only delete the recovery plans with status Ready (info required) or Ready (info complete).*

To delete the recovery plan:

1. In the left navigation pane, click **Recovery Plan**. The **Recovery Plan** page appears.
2. Right-click the **Recovery Plan** that you want to delete and click **Delete**. The Delete Recovery Plan dialog box appears asking for the confirmation to delete the selected recovery plan.
3. A confirmation dialogue appears, click **Delete**.



Recovery Plan

⊟	RECOVERY PL...	ORGANIZATION	STATUS	APPLICATIONS	APPLIANCES	EDITED	LAST RUN	SCHEDULED
☑	Daylight		Ready (info compl...	2 in 1 groups	actsky02.rd.actifio...	2019-03-11 10:01:37		ENABLED
□	rp-fsag	MRG	Ready (info requir...		s4	2019-03-08 23:03:46	2019-03-08 23:18:29	DISABLED
□	testrp1		Ready (info compl...		ky02.rd.actifio...	2019-03-08 14:30:12		DISABLED
□	rp-nag1		Ready (info requir...		ky02.rd.actifio...	2019-03-08 14:58:29		DISABLED
□	rp-staticip		Ready (info compl...		ky02.rd.actifio...	2019-03-05 11:14:05		DISABLED
□	rp-windowsVMs		Ready (info compl...	3 in 1 groups	actsky02.rd.actifio...	2019-02-18 19:49:26	2019-03-06 16:42:48	DISABLED
□	rp-rhelvms		Ready (info compl...	9 in 1 groups	actsky02.rd.actifio...	2019-02-18 19:47:04	2019-03-06 12:23:06	DISABLED

Deleting a Recovery Plan

12 Adding and Managing User Access Controls

The 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 69
- Modifying roles and changing permissions on page 71
- Deleting roles on page 72

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

Roles	Description	Associated Rights
RD Admin	This role grants administrative rights to the users. Depending on RD deployment all management rights comes under this role.	Grants the user with all the available rights.
RD Manage	This role grants limited rights to the users to manage RD Server.	Appliance View, Server View, Application Group View, Virtual Management Server View, Upgrade View, Download RD logs, Resource Pool Manage, Resource Pool View, Port Group Manage, Port Group View, Virtual Management Server View
RD View	This role grants view only rights to the users.	Appliance View, Application Group View, Collector View, Server View, Organization View, Recovery Plan View, Security View, Upgrade View, Resource Pool View, Port Group View, Virtual Management Server View
RD Run	This role grants "Recovery Plan Run" rights and all view rights to the users.	Appliance View, Server View, Application Group View, Collector View, Organization View, Recovery Plan Run, Recovery Plan View, Resource Pool View, Port Group View, Virtual Management Server View, Upgrade View, Security View.

Following table describes the user access controls types that are allowed in the Actifio Resiliency Director:

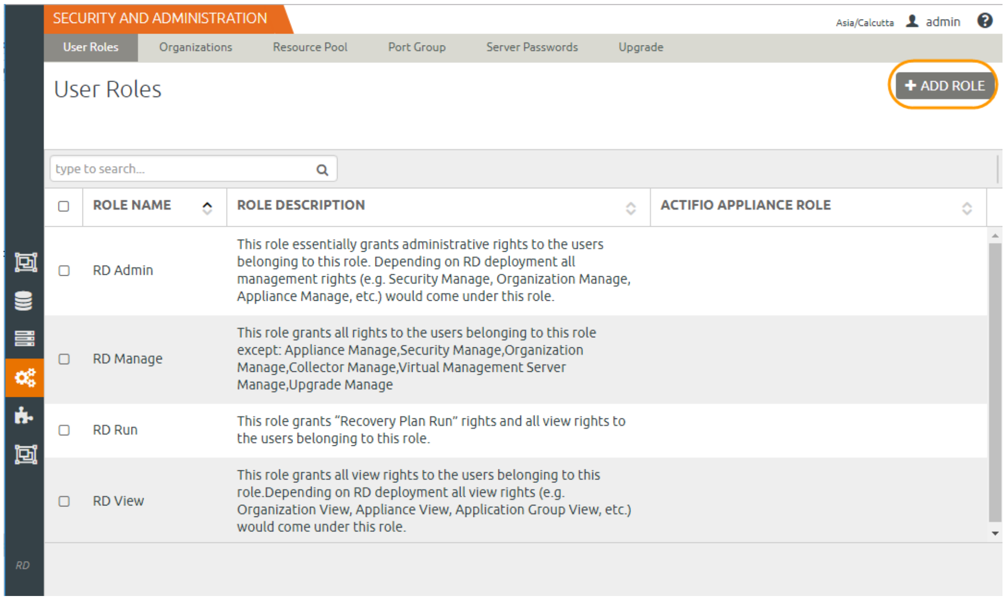
User Access Rights	Description
Appliance Manage	Allows user to perform create, read, update, and delete operations on the Actifio Appliance entity.
Appliance View	Allows user to view the Actifio Appliance entity.
Application Group Manage	Allows user to perform create, read, update, and delete operations on Application Group entity
Application Group View	Allows user to view the operations performed on Application Group entity.
Download RD logs	Allows 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.
Collector Manage	Allows user to perform all operations on Collector entity.
Collector View	Allows user to view Collector 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 them. 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 Access Control** page.



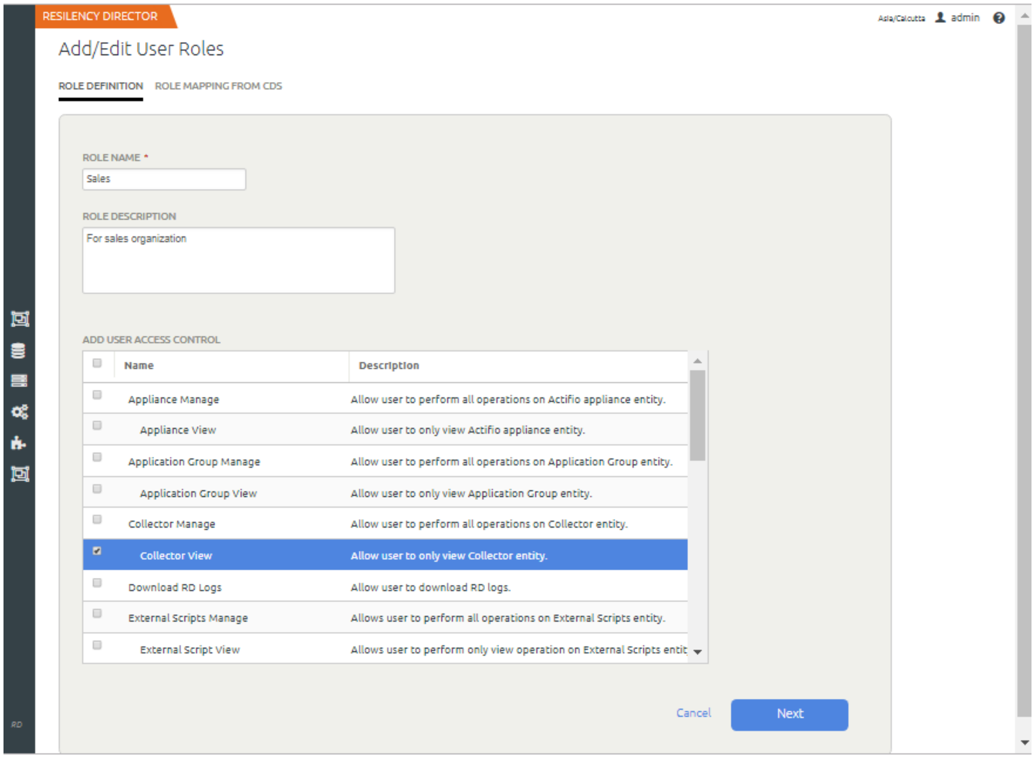
☐	ROLE NAME	ROLE DESCRIPTION	ACTIFIO APPLIANCE ROLE
☐	RD Admin	This role essentially grants administrative rights to the users belonging to this role. Depending on RD deployment all management rights (e.g. Security Manage, Organization Manage, Appliance Manage, etc.) would come under this role.	
☐	RD Manage	This role grants all rights to the users belonging to this role except: Appliance Manage,Security Manage,Organization Manage,Collector Manage,Virtual Management Server Manage,Upgrade Manage	
☐	RD Run	This role grants "Recovery Plan Run" rights and all view rights to the users belonging to this role.	
☐	RD View	This role grants all view rights to the users belonging to this role.Depending on RD deployment all view rights (e.g. Organization View, Appliance View, Application Group View, etc.) would come under this role.	

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** filed.

5. Select the user access that you want to assign for the role from the **User Access Control** section by checking the appropriate box.



Add/Edit User Roles

ROLE NAME *: Sales

ROLE DESCRIPTION: For sales organization

ADD USER ACCESS CONTROL

□	Name	Description
□	Appliance Manage	Allow user to perform all operations on Actifio appliance entity.
□	Appliance View	Allow user to only view Actifio appliance entity.
□	Application Group Manage	Allow user to perform all operations on Application Group entity.
□	Application Group View	Allow user to only view Application Group entity.
□	Collector Manage	Allow user to perform all operations on Collector entity.
☑	Collector View	Allow user to only view Collector entity.
□	Download RD Logs	Allow user to download RD logs.
□	External Scripts Manage	Allows user to perform all operations on External Scripts entity.
□	External Script View	Allows user to perform only view operation on External Scripts entit

6. Click **Next**.

   The Role mapping from CDS page appears.

7. Select your desired role(s) from Actifio Appliance to be mapped to this newly created role by checking the appropriate box.

8. Click **Finish** to complete the process.

Modifying roles and changing permissions

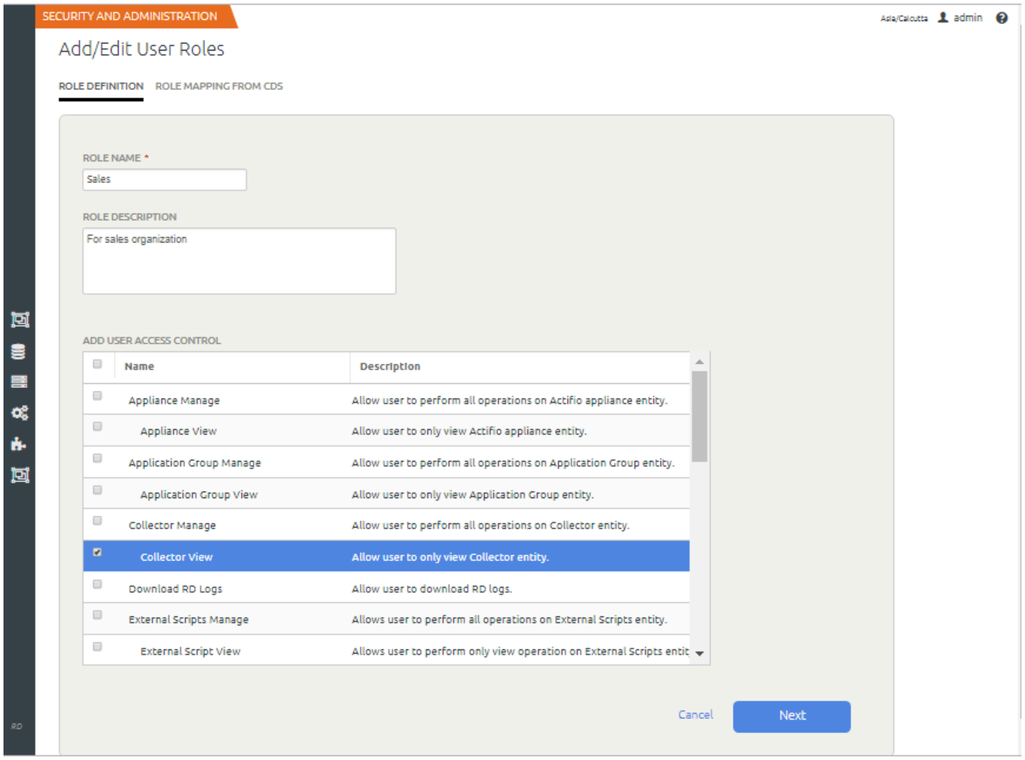
This section describes the steps to modify existing roles and change permissions to them.

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**.



Add/Edit User Roles

ROLE NAME *
Sales

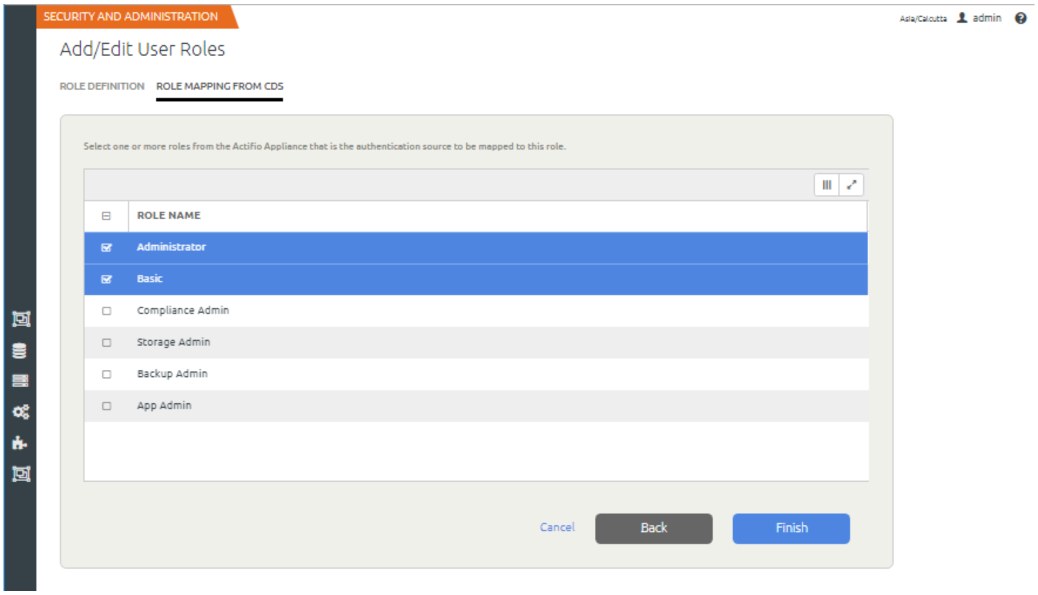
ROLE DESCRIPTION
For sales organization

ADD USER ACCESS CONTROL

□	Name	Description
□	Appliance Manage	Allow user to perform all operations on Actifio appliance entity.
□	Appliance View	Allow user to only view Actifio appliance entity.
□	Application Group Manage	Allow user to perform all operations on Application Group entity.
□	Application Group View	Allow user to only view Application Group entity.
□	Collector Manage	Allow user to perform all operations on Collector entity.
☑	Collector View	Allow user to only view Collector entity.
□	Download RD Logs	Allow user to download RD logs.
□	External Scripts Manage	Allows user to perform all operations on External Scripts entity.
□	External Script View	Allows user to perform only view operation on External Scripts entit

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**.

The Role mapping from CDS page appears.



Add/Edit User Roles

Select one or more roles from the Actifio Appliance that is the authentication source to be mapped to this role.

⊟	ROLE NAME
☑	Administrator
☑	Basic
□	Compliance Admin
□	Storage Admin
□	Backup Admin
□	App Admin

6. Select and map Actifio Appliance Role(s) by checking the appropriate boxes.
7. Click **Finish** to complete the process.

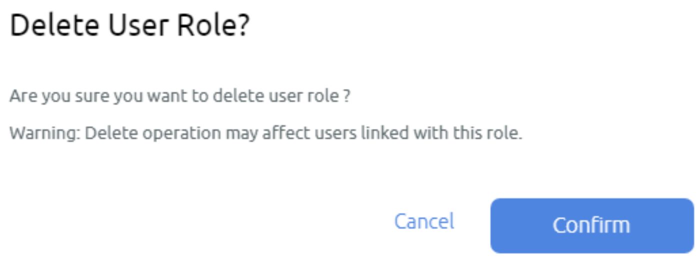
Deleting roles

To delete the user access control:

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 **Delete**.

   The **Delete User Role** dialog appears.



Delete User Role?

Are you sure you want to delete user role ?

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

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

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

13 Viewing Logs

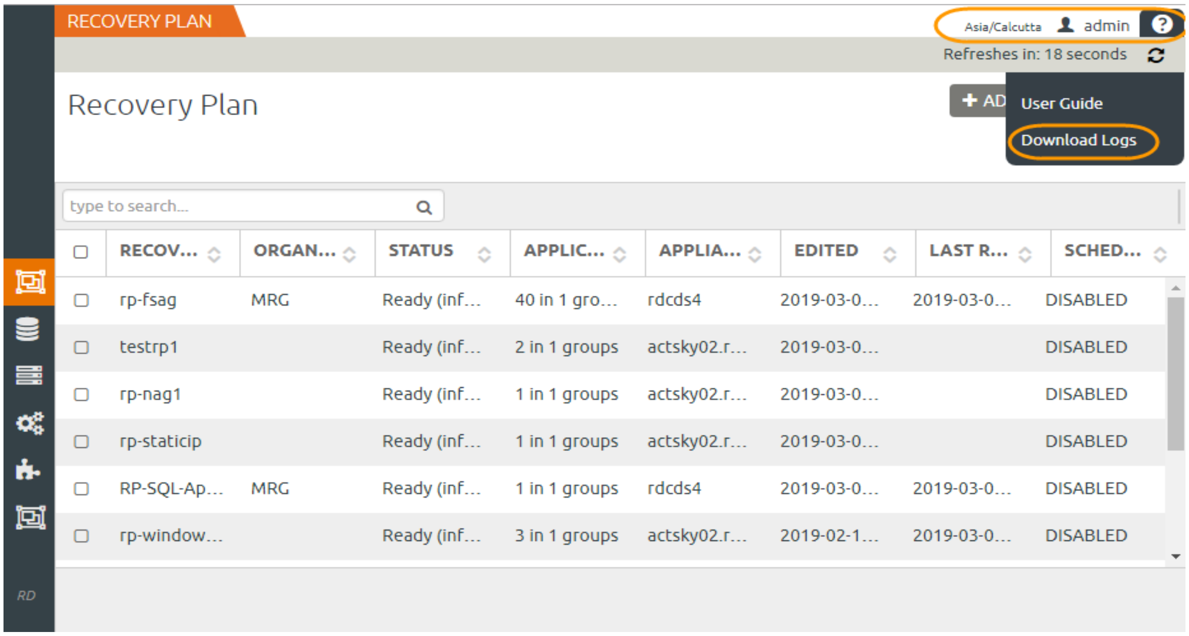
This chapter describes the details to download the Resiliency Director Server logs.

Downloading the Logs

Logs are generated for each Resiliency Director operation executed in the Server. 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 (?)**.



□	RECOV...	ORGAN...	STATUS	APPLIC...	APPLIA...	EDITED	LAST R...	SCHED...
□	rp-fsag	MRG	Ready (inf...	40 in 1 gro...	rdcds4	2019-03-0...	2019-03-0...	DISABLED
□	testrp1		Ready (inf...	2 in 1 groups	actsky02.r...	2019-03-0...		DISABLED
□	rp-nag1		Ready (inf...	1 in 1 groups	actsky02.r...	2019-03-0...		DISABLED
□	rp-staticip		Ready (inf...	1 in 1 groups	actsky02.r...	2019-03-0...		DISABLED
□	RP-SQL-Ap...	MRG	Ready (inf...	1 in 1 groups	rdcds4	2019-03-0...	2019-03-0...	DISABLED
□	rp-window...		Ready (inf...	3 in 1 groups	actsky02.r...	2019-02-1...	2019-03-0...	DISABLED

Actifio Resiliency Director Server - Downloading Logs

2. Click **Download Logs** to download the logs. You can copy the downloaded operation logs.
3. Un-tar the downloaded tar.gz file 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.*

14 Upgrading the Resiliency Director Server

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

This chapter contains the following topics:

Upgrade using GUI-Based Method

The Resiliency Director Server 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, you can find the upgrade logs at:* `/var/log/brd-install/brd-upgrade.log`

4. Restarts all the Resiliency Director Server related processes.

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

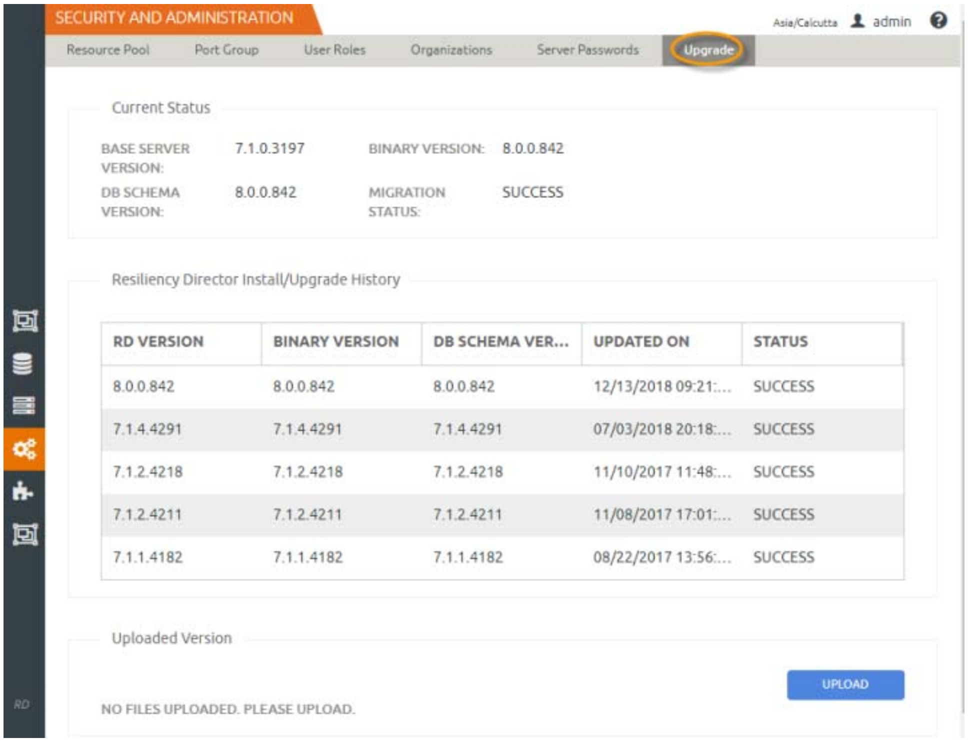
- All the Resiliency Director Collectors registered with the Resiliency Director Server should be accessible, up and running.
- Registered Actifio Appliances should be accessible.
- Registered virtual management servers should be accessible.
- No recovery plan should be in **In Progress** state.

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

To upgrade the Resiliency Director Server:

1. Copy **.gpg** file to the Resiliency Director Server machine.
2. Click **Settings** > **Security & Administration** > **Upgrade**. Upgrade screen displays.

   Upgrade screen displays current status and upgrade history of the Resiliency Director Server.



Current Status

BASE SERVER VERSION:	7.1.0.3197	BINARY VERSION:	8.0.0.842
DB SCHEMA VERSION:	8.0.0.842	MIGRATION STATUS:	SUCCESS

Resiliency Director Install/Upgrade History

RD VERSION	BINARY VERSION	DB SCHEMA VER...	UPDATED ON	STATUS
8.0.0.842	8.0.0.842	8.0.0.842	12/13/2018 09:21:...	SUCCESS
7.1.4.4291	7.1.4.4291	7.1.4.4291	07/03/2018 20:18:...	SUCCESS
7.1.2.4218	7.1.2.4218	7.1.2.4218	11/10/2017 11:48:...	SUCCESS
7.1.2.4211	7.1.2.4211	7.1.2.4211	11/08/2017 17:01:...	SUCCESS
7.1.1.4182	7.1.1.4182	7.1.1.4182	08/22/2017 13:56:...	SUCCESS

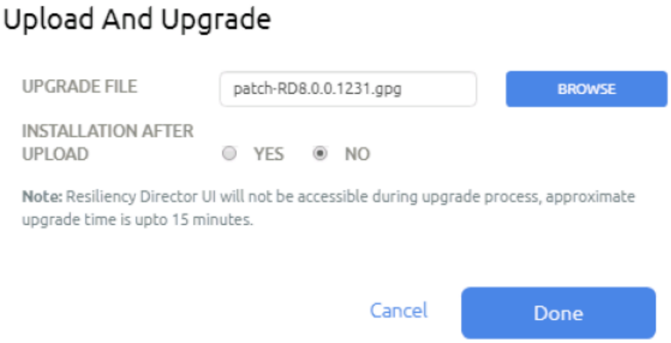
Uploaded Version

NO FILES UPLOADED. PLEASE UPLOAD.

Resiliency Director Server Upgrade

3. Click **Upload**. Upload and Upgrade screen displays.

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


Upload And Upgrade

UPGRADE FILE: patch-RD8.0.0.1231.gpg

INSTALLATION AFTER UPLOAD: ○ YES ● NO

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

5. 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 Server GUI is not accessible for few minutes. Once upgrade process is completed, you can view the latest version in the Current Status field.*

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

To restore data manually,

1. Navigate to the directory `/act/rdbackup/`
2. Stop all the Resiliency Director Server 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 Server related processes. For more information on Resiliency Director Server processes, see Actifio Resiliency Director Server Configuration Parameters on page 10.

Upgrade using CLI-Based Method

Perform these steps to upgrade the Actifio Resiliency Director Server 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.gpg
   ```

   ```
   Output: SUCCESS
   ```

3. If desired, 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 will not be accessible during upgrade process, approximate upgrade time is up to 15 minutes.*

15 Troubleshooting Issues

While using the Actifio Actifio Resiliency Director Server, error messages and warnings may occur for many different reasons.

This chapter contains the issues description along with the possible solution or workaround in the tabular format. It also provides Actifio network port usage information.

Issue Description	Resolution/Workaround
Powershell is unable to provide conclusive results on the remote hosting server and displays result as Failed.	Powershell script is modified to display all results as Success. However, debugging of Powershell script can be done by the user to modify the Powershell script.
Virtual machine recovery failed.	Ensure that an ESX host for the virtual machine has storage port configured.
Not able to log in to Resiliency Director Server/Collector using root credentials.	Ensure that the rdprovider and tomcat is started as a root user.
The Windows machine is detecting IP duplication/conflict.	• Ensure that the DV Switch is connected to the DHCP server. So that, all VMs in Port Groups inside the DV switch will get dynamically configured IP addresses. • Ensure that all the port-Groups are configured with different VLANs. So that, IP address duplication will not occur. ***Note:*** *For virtual machines having non windows OS, the IP address duplication is not detected by the OS.*
Recovery plan execution fails with the error message: "Virtual machine recovery failed due to: Unable to receive any status for the failover job from Actifio Appliance."	Ensure that the VM creation is complete when Actifio Resiliency Director Server starts polling for the failover job status from Actifio Appliance. Increase the retries/retries interval in the act-props.xml property file for the properties "appliance-failover-complete-retries" or "appliance-failover-complete-retries-interval". For more information, refer to the section Viewing the act-props.xml Property File on page 69.

Issue Description	Resolution/Workaround
OVA-VM is unable to acquire the IP address from DHCP.	Ensure that the VM is in correct port group and then enter the following command in VM console: `#/etc/init.d/network restart`
Duplicate IP address at the Actifio Resiliency Director Server site. Description: On the Actifio Resiliency Director Server Collector site, user creates VM1 which gets an IP address from DHCP server (for example: 192.169.10.45), and VM1 is switched off. Later, user creates VM2 and assigns the same static IP (192.169.10.45). Then user create an application group and corresponding Recovery plan. After execution of a recovery plan, on the Actifio Resiliency Director Server side both the VMs (VM1 & VM2) get same IP addresses.(192.168.10.45) and mostly no IP conflict is notified by VMs.	IP conflicts should be handled on the Actifio Resiliency Director Server Collector side.
VMs/vApps in different portgroups on the Actifio Resiliency Director Server Collector site have same portgroup in Actifio Resiliency Director Server Server site. Description: When you create an application group with VMs/vApps having different portgroups and corresponding recovery plan, after recovery plan execution, it is observed that both the application groups are in same portgroup.	You must create two different application groups and their recovery plans and then place them in same resource pool.
Unable to add UNIX based remote host.	Ensure that the ssh server on the remote host has password authentication enabled. This configuration is present in the `sshd_config` file of the system. Typically, you can find the file at the path /etc/ssh/ but it may vary, as in the case of load balancer it is found at /config/ssh/. Change the value PasswordAuthentication no' to 'PasswordAuthentication yes'.
Page 404 error after upgrading the OVA.	Browser must be restarted to clear the cache to avoid this issue. Close and restart the Browser window, once you have upgraded the OVA.

Issue Description	Resolution/Workaround
After upgrade, the new UI is not displayed after restarting the Browser window.	Clear the Browser cache and re-enter the Resiliency Director URL. This issues may not persist always, so restarting the Browser window may also display the new UI.

Actifio Network Ports

Actifio Port Requirements Sorted by TCP Port Number.

Port (TCP)	Protocol	Description
22	SSH	Node IMM Ports CLI access Storage CLI access
26	SSH	Actifio to Actifio SSH Service CLI access
80	HTTP	Node IMM Ports Storage Management Web GUI
443	HTTPS	AGM management of Actifio CDS and Sky appliances Node IMM Ports Storage Management Web GUI VMware vCenter Management Traffic Actifio Appliance to Cloud Data Transfer Actifio Desktop (GUI) Actifio Report Manager (reports & setup/admin) Web browser access to AGM Actifio Report Manager (data collection) RC/RD data collection/recovery orchestration

A Actifio Authentication to VMware vCenter Server

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 section includes:

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**.

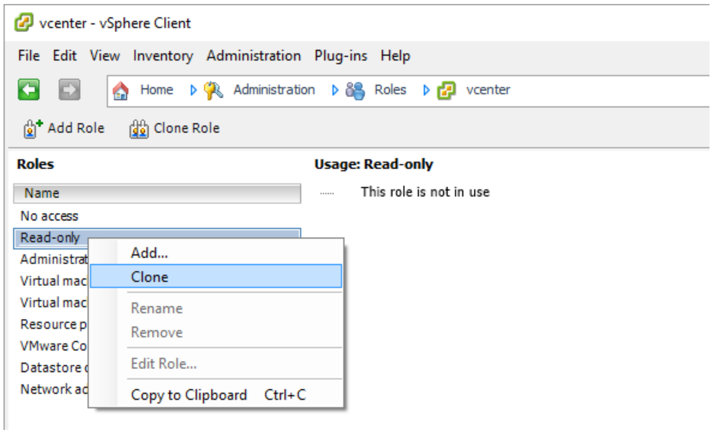
This document provides the minimum set of privileges needed to have the Actifio appliance perform all backup and recovery operations.

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.*

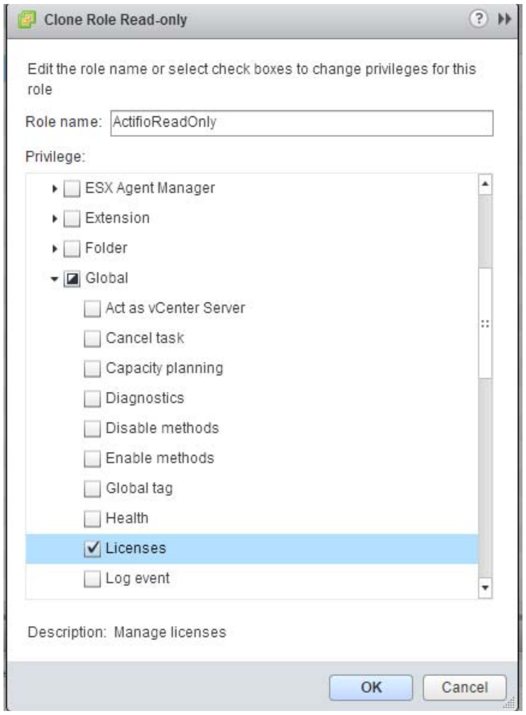
Creating the ActifioReadOnly vCenter Role

You will create two a 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**.



Edit the role name or select check boxes to change privileges for this role

Role name: ActifioReadOnly

Privilege:

- □ ESX Agent Manager
- □ Extension
- □ Folder
- ☒ Global
  - □ Act as vCenter Server
  - □ Cancel task
  - □ Capacity planning
  - □ Diagnostics
  - □ Disable methods
  - □ Enable methods
  - □ Global tag
  - □ Health
  - ☑ Licenses
  - □ Log event

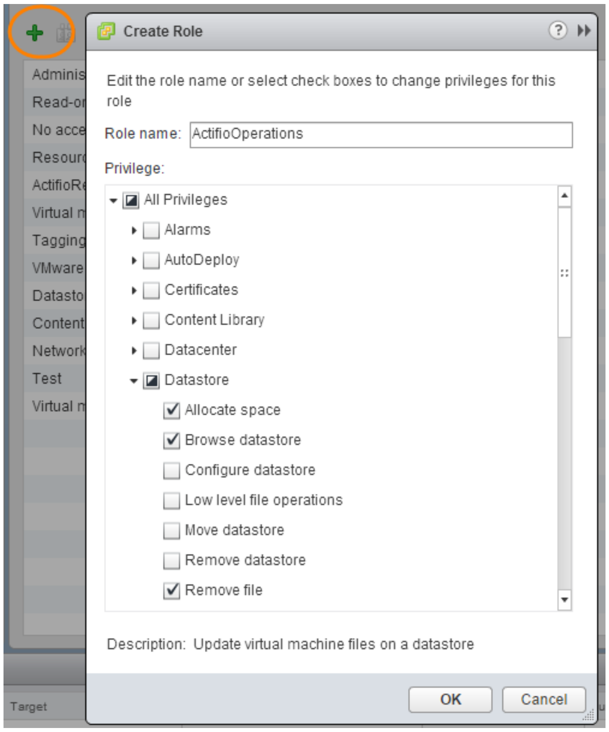
Description: Manage licenses

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 into 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 checkboxes for each of the privileges listed in The vCenter Permissions List on page 86.
5. Click **OK** to save the role.



Create Role

Edit the role name or select check boxes to change privileges for this role

Role name: ActifioOperations

Privilege:

- ▣ All Privileges
  - □ Alarms
  - □ AutoDeploy
  - □ Certificates
  - □ Content Library
  - □ Datacenter
  - ▣ Datastore
    - ☑ Allocate space
    - ☑ Browse datastore
    - □ Configure datastore
    - □ Low level file operations
    - □ Move datastore
    - □ Remove datastore
    - ☑ Remove file

Description: Update virtual machine files on a datastore

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 off 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 into 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 dropdown, 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