
Virtualizing and Protecting Copy Data with the Application Manager

Copyright, Trademarks, and other Legal Matter

Copyright © 2009 - 2019 Actifio, Inc. All rights reserved.

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

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

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

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

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

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

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

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

Contents

Preface	v
Actifio Appliances.....	vi
The Actifio Now Customer Portal.....	vi
Actifio Support Centers	vi
Chapter 1 - Application Manager Protect and Policy Tabs	1
The Application Manager Service Menu	2
Using The Application Manager Protect Tab.....	3
The Application Manager Policies Tab	4
Chapter 2 - Discovering, Creating, and Deleting Applications and VMs	5
Discovering Applications on a Host that Has Been Added to the Actifio System	5
Discovering VMs.....	7
Discovering Applications and Adding the Host to the Actifio System Simultaneously	9
Creating Generic Applications.....	10
Deleting Applications, VMs, and Groups.....	11
Chapter 3 - Virtualizing and Protecting Applications and VMs	13
How Actifio Virtualization and Protection Work.....	14
The Stages in Virtualizing an Application or a VM	15
Basic Procedure for Protecting Applications and VMs.....	16
Validating Projected Resources Prior to Applying Protection	17
Chapter 4 - Marking Applications and Images as Sensitive	19
Marking an Application, VM, or Group as Sensitive.....	19
Marking an Image as Sensitive	20
Chapter 5 - Working with Groups	21
Creating a Group	22
Deleting a Group	22
Chapter 6 - Working with Consistency Groups	23
Creating a Consistency Group	24
Deleting a Consistency Group.....	25

Chapter 7 - Managing Jobs	27
Scheduled Jobs	28
On-Demand Jobs	29
Running an On-Demand Backup.....	30
Running On-Demand Database Log Replication	31
Chapter 8 - Protecting Entire Hyper-V VMs	33
Application Advanced Settings for Hyper-V VMs.....	34
Chapter 9 - Protecting Local File Systems	35
Application Advanced Settings for Local File Systems.....	36
Chapter 10 - Protecting Mapped NFS File Systems	37
Application Advanced Settings for NFS File Systems.....	38
Chapter 11 - Protecting Mapped CIFS File Systems	39
Application Advanced Settings for Mapped CIFS File Systems.....	40
Chapter 12 - Protecting Exchange Databases	41
Protecting a Microsoft Exchange Database	42
Application Advanced Settings for Microsoft Exchange Databases	43
Chapter 13 - Protecting Generic Applications	45
Application Advanced Settings for Generic Applications	45
Chapter 14 - Protecting Groups	47
Chapter 15 - Protecting Consistency Groups	49
Protecting a Consistency Group	50
Application Advanced Settings for Consistency Groups	51
Chapter 16 - Suspending Protection	55
Index	57

Preface

This guide provides general step-by-step instructions on how to virtualize and protect application and VM data with the Actifio Application Manager:

- Use the Application Manager service, see [Chapter 1, Application Manager Protect and Policy Tabs](#)
- Discover applications and VMs, see [Discovering, Creating, and Deleting Applications and VMs](#) on page 5.
- Mark protected data as sensitive, see [Marking Applications and Images as Sensitive](#) on page 19
- Work with Application Groups, see [Working with Groups](#) on page 21
- Work with Consistency Groups, see [Working with Consistency Groups](#) on page 23
- Manage jobs, see [Managing Jobs](#) on page 27

This guide also provides application specific methods of virtualizing and protecting data for:

- Hyper-V VMs, see [Mounting a Hyper-V VM Image](#) on page 35
- File Systems, see [Protecting Local File Systems](#) on page 35, [Protecting Mapped NFS File Systems](#) on page 37, and [Protecting Mapped CIFS File Systems](#) on page 39
- Exchange, see [Protecting Exchange Databases](#) on page 41
- Generic Applications, see [Protecting Generic Applications](#) on page 45
- Application Groups, see [Protecting Groups](#) on page 47
- Consistency Groups, see [Protecting Consistency Groups](#) on page 49
- Suspending protection, see [Suspending Protection](#) on page 55.

It assumes you have read ***Getting Started with Actifio Copy Data Management***, are familiar with the components of the Actifio Desktop, and have a grasp of the basic concepts associated with an Actifio appliance.

Application specific processes and procedures for Microsoft SQL Server, Oracle, and VMware VMs can be found in their respective guides:

- ***An Oracle DBA's Guide to Actifio Copy Data Management***
- ***An SQL Server DBA's Guide to Actifio Copy Data Management***
- ***A VMWare Manager's Guide to Actifio Copy Data Management***

Actifio Appliances

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

The ActifioNOW Customer Portal

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

From the ActifioNOW customer portal you can obtain detailed reports about your Actifio appliance, access the Actifio product documentation, including release notes, and search the knowledge base for answers to specific questions.

To log into the ActifioNOW customer portal:

1. Go to: <https://now.actifio.com>.
2. When prompted, enter the user name and password 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 Application Manager Protect and Policy Tabs

This chapter provides an overview of the components and options of the Application Manager that pertain to protecting applications and VMs:

[The Application Manager Service Menu](#) on page 2

[Using The Application Manager Protect Tab](#) on page 3

[The Application Manager Policies Tab](#) on page 4

It assumes that you have read the **Getting Started with Actifio Copy Data Management** guide and are familiar with the basic concepts and options associated with the Application Manager service.

The Protect and Policies tabs are part of a group of tabs that appears at the top of the Application Manager. Tabs are context sensitive and only appear when they provide a valid action or information for the selected application. For example:



The Application Manager Tabs

When protecting applications and VMs, you will use the Application Manager's:

- **Protect** tab to perform protection operations. Protection operations are described in [Using The Application Manager Protect Tab](#) on page 3.
- **Policies** tab to view the policies assigned to an application and to run an unscheduled job based on one of the assigned policies. The Policy tab is described in [The Application Manager Policies Tab](#) on page 4.

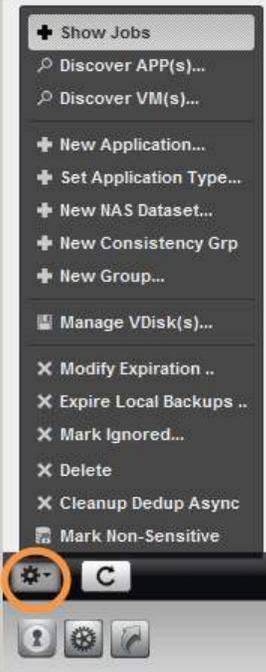
For detailed information on the:

- **Restore** tab, see **Accessing and Recovering Copy Data with the Application Manager** and **Restoring Copy Data with the Application Manager**.
- **Replication** tab see, **Replicating Data Using Actifio Appliances**.
- **Workflow** tab, see **Creating Automated Workflows for SQL Server Databases** and **Creating Automated Workflows for Oracle Databases**.

Note: The **Orgs** tab is used to identify which organizations include an application as a member. Organization membership is described in **Getting Started with Actifio Copy Data Management**.

The Application Manager Service Menu

The gear icon in the lower left corner of the Actifio Desktop displays the Application Manager Service Menu. The Application Manager Service Menu allows you to perform specific protection tasks:

Location of Menu	Menu Item	Task
	Show Jobs	Display jobs associated with the application in context, Switches your view to System Monitor, and applies appropriate filters.
	Discover APP(s)	Find file systems, Oracle databases, and Microsoft Exchange and Microsoft SQL Server applications on a selected host. The host must have an Actifio Connector installed.
	Discover VM(s)	Find virtual machines on an ESX or Hyper-V server.
	New Application	Add an application from a host where the Actifio Connector is not installed and to name a mounted image as a new application.
	Set Application Type	Assign a database type within a consistency group. This is not used for any other application type.
	New NAS Dataset	Create a NAS dataset from an Isilon NAS server. See Configuring Actifio Big Data Director (BDD) for instructions to configure and use Actifio's Big Data Director (BDD).
	New Consistency Grp	Create a group of applications to protect the consistency of data among member applications on the same host.
	New Group	Use an application group if you want to use a single policy to protect several applications. Applications on different hosts can be grouped.
	Manage VDisk(s)	Manage virtual disks.
	Modify Expiration	Change the expiration date for backups for a selected application.
	Expire All Backups	Expire all the backups for the selected application, group, or for a consistency group.
	Mark Ignored	Ignore an application at discovery and for dashboard statistics.
	Unmark Ignored	Reverse the choice you made using the Mark Ignored option.
	Delete	Delete an application, a group, or a consistency group.
	Cleanup Dedup Async	Cleans up artifacts from Dedup-Async operations. This only appears when there are Dedup-Async replication images to be cleaned up.
	Cleanup StreamSnap	Cleans up artifacts from StreamSnap operations. This only appears when there are StreamSnap replication images to be cleaned up.
Mark Sensitive	Mark data as sensitive according to your data-sensitivity policies.	

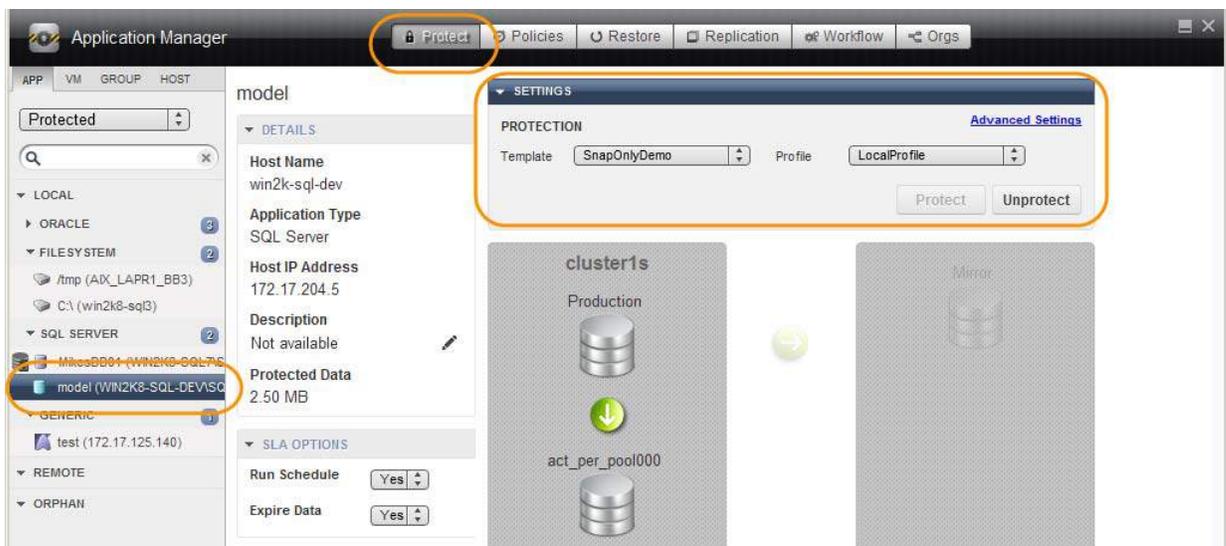
Using The Application Manager Protect Tab

The Protect tab is used to apply a policy template and a resource profile to an application. The Protect tab is detailed in ***Planning and Developing Service Level Agreements*** in the Actifio Documentation Library.

Before you can protect applications, you must:

- Install the Actifio Connector (not required for capturing entire VMware VMs and for Generic Applications). This is described in ***Connecting Hosts to Actifio Appliances*** in your Actifio Documentation Library.
- Have a policy template and a resource profile in a Service Level Agreement (SLA). You develop SLAs with the SLA Architect. This is described in ***Planning and Developing Service Level Agreements*** in your Actifio Documentation Library.
- Discover the applications. This is described in [Chapter 2, Discovering, Creating, and Deleting Applications and VMs](#).

Protection is detailed starting in [Chapter 3, Virtualizing and Protecting Applications and VMs](#). You can review existing policies in [The Application Manager Policies Tab](#) on page 4.

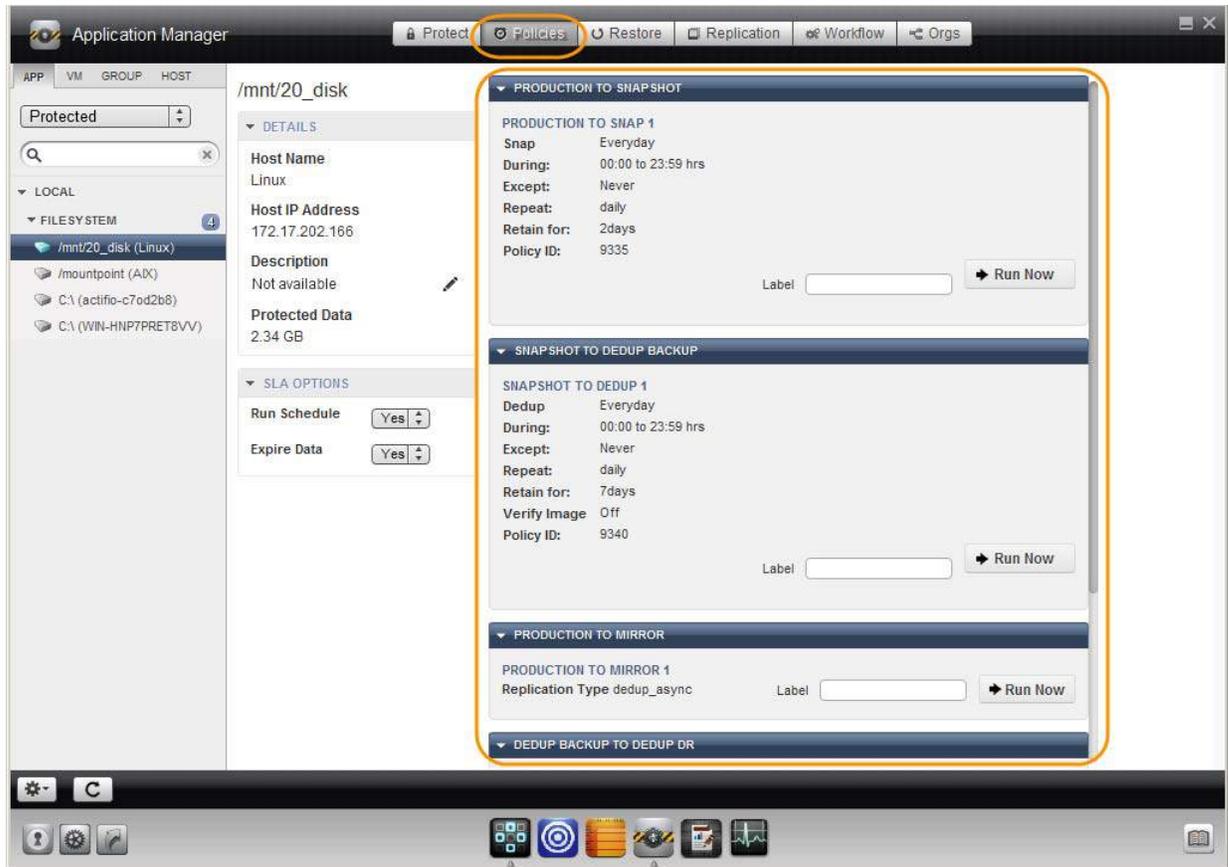


The Protect Tab

The Application Manager Policies Tab

The Policies tab is used to show the protection policies used to protect the selected application. You can review how the policies are configured and run an on-demand backup using any of the available policies.

Policies are detailed in ***Planning and Developing Service Level Agreements***.



The Policies Tab for a File System with Multiple Policies Assigned

Note: The Policies tab is not available to Groups. It is available for Consistency Groups.

2 Discovering, Creating, and Deleting Applications and VMs

Once a host has been added to an Actifio appliance (see **Connecting Hosts to Actifio Appliances**) the applications and VMs on the added hosts can be discovered.

Note: *The Actifio appliance relies on synchronicity between an Actifio appliance and its discovered hosts. Hosts that are not connected to an NTP server can drift, resulting in differences between the host's record and the Actifio appliance's record of the time snapshots taken or other actions performed by the Actifio appliance.*

This chapter details:

[Discovering Applications on a Host that Has Been Added to the Actifio System](#) on page 5

[Discovering VMs](#) on page 7

[Discovering Applications and Adding the Host to the Actifio System Simultaneously](#) on page 9

[Creating Generic Applications](#) on page 10

[Deleting Applications, VMs, and Groups](#) on page 11

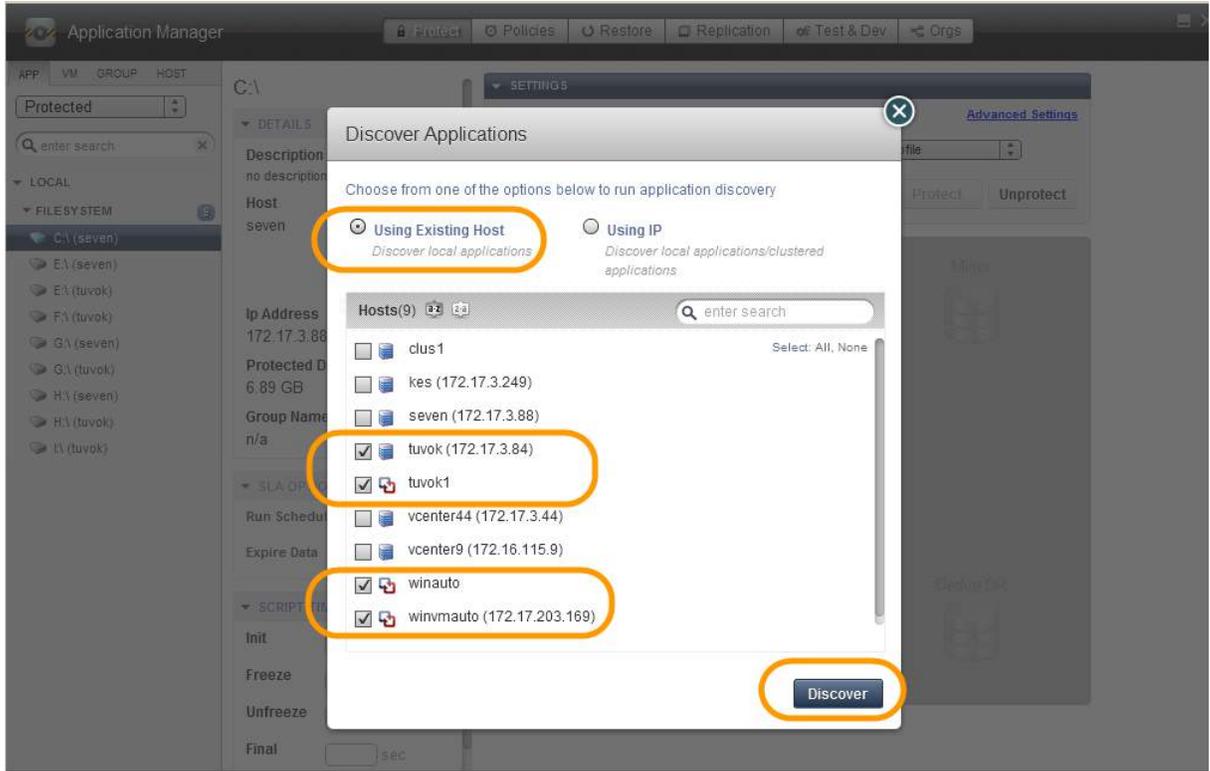
Discovering Applications on a Host that Has Been Added to the Actifio System

You can discover applications on physical hosts and on VMs that are known to the Actifio appliance. You must have the 'Host Manage' or 'Application Manage' rights to discover applications and the Actifio Connector must be installed and configured on the host.

Note: *To discover clustered applications and IBM LPAR virtual machines running on Virtual IO Servers (VIOS) managed by IBM Hardware Management Console, see [Discovering Applications and Adding the Host to the Actifio System Simultaneously](#) on page 9.*

To discover an application:

1. Open the Actifio Desktop to the **Application Manager**.
2. From the service menu, select **Discover App(s)**. The Discover Applications dialog appears.
3. Select **Using Existing Host**.
4. Select the host that includes the application you would like to protect.
5. Click **Discover**. The navigation pane lists all the applications attached to the selected host, including applications residing on out-of-band storage, as soon as they are discovered.



Discovering Applications on a Host

Note: Instructions for installing and configuring the Actifio Connectors are in **Connecting Hosts to Actifio Appliances** in the Actifio Documentation Library.

Discovering VMs

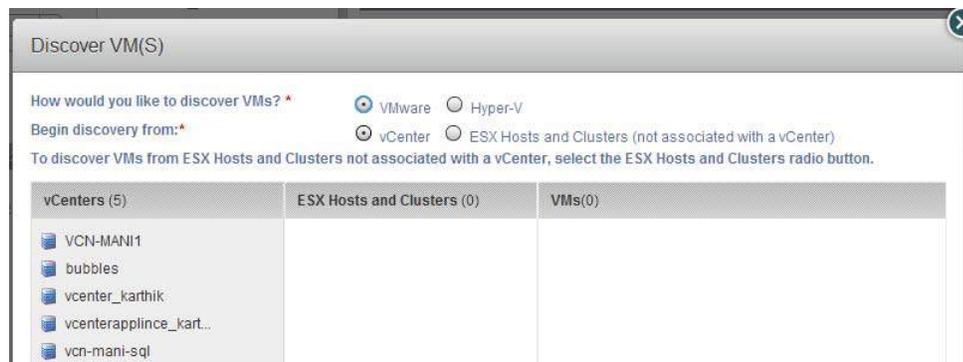
Virtual machines associated with a hypervisor host are discovered through the Application Manager. To discover VMs, you must first add the VM's hypervisor as a host. See **Connecting Hosts to Actifio Appliances** in the Actifio Documentation Library for details on how to add a new host.

Note: When you discover a VMware vCenter, all ESXi hosts are automatically discovered.

Note: Virtual machine discovery on a hypervisor requires an Actifio user with 'Host Manage' Actifio rights.

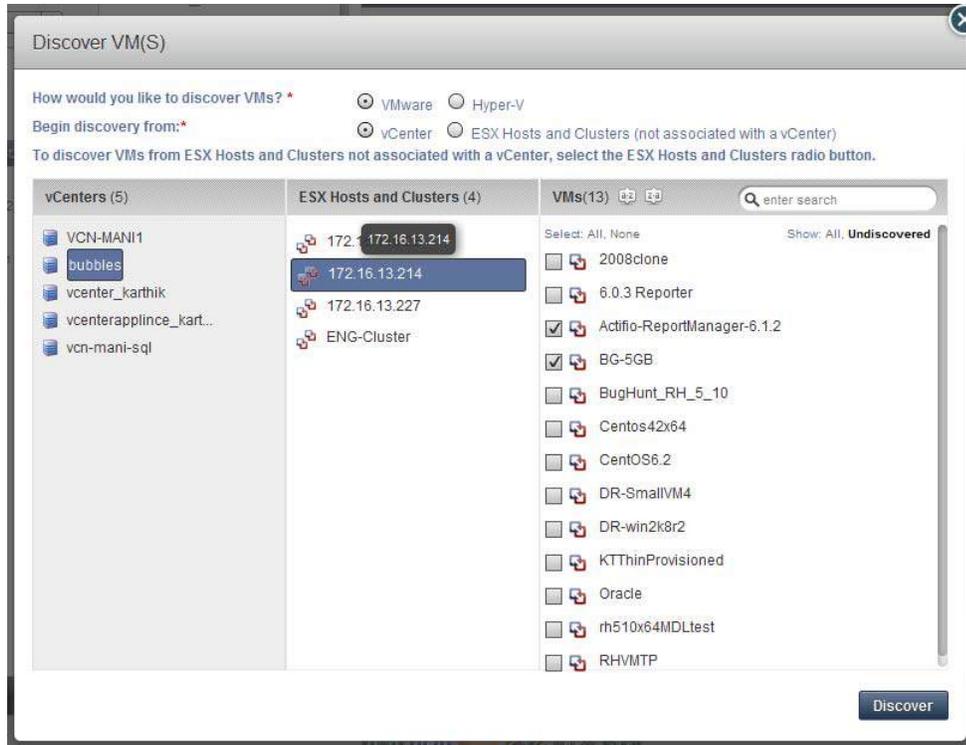
To discover a VM:

1. Open the **Application Manager**.
2. Click **Discover VM(s)**...from the service menu. The Discover VM(s) window appears.



Discovering vCenters on a Host

3. In the Discover VM(s) window, select either **VMware** or **Hyper-V**.
4. Depending on your previous choice select either a vCenter/ESX Host or SCVMM/Hyper-V Server. The Discover VMs window discovers and displays the host/appliances managed by the selected hypervisor.



Discovering VMs on an ESX Host in a vCenter

5. Select the virtual machines to protect.
6. Click **Discover**. The Virtual Machines are added to the list of virtual machines at **Application Manager > Applications by Type > VM**.
7. After discovery, the virtual machines and hypervisors are added as hosts in the Domain Manager.

Note: The Actifio appliance relies on synchronicity between an Actifio appliance and its discovered hosts. Hosts that are not connected to an NTP server can drift, resulting in differences between the host's record and the Actifio appliance's record of the time snapshots taken or other actions performed by the Actifio appliance.

Discovering Applications and Adding the Host to the Actifio System Simultaneously

You can discover local and clustered applications on hosts that are not yet known to the Actifio appliance if you know the IP address. This method registers the host and discovers the applications at the same time. You must have the 'Host Manage' or 'Application Manage' rights to discover applications, and the Actifio Connector must be installed and configured on the host.

Use this method also to discover IBM AIX-based Virtual IO Servers (VIOS) managed by Hardware Management Console.

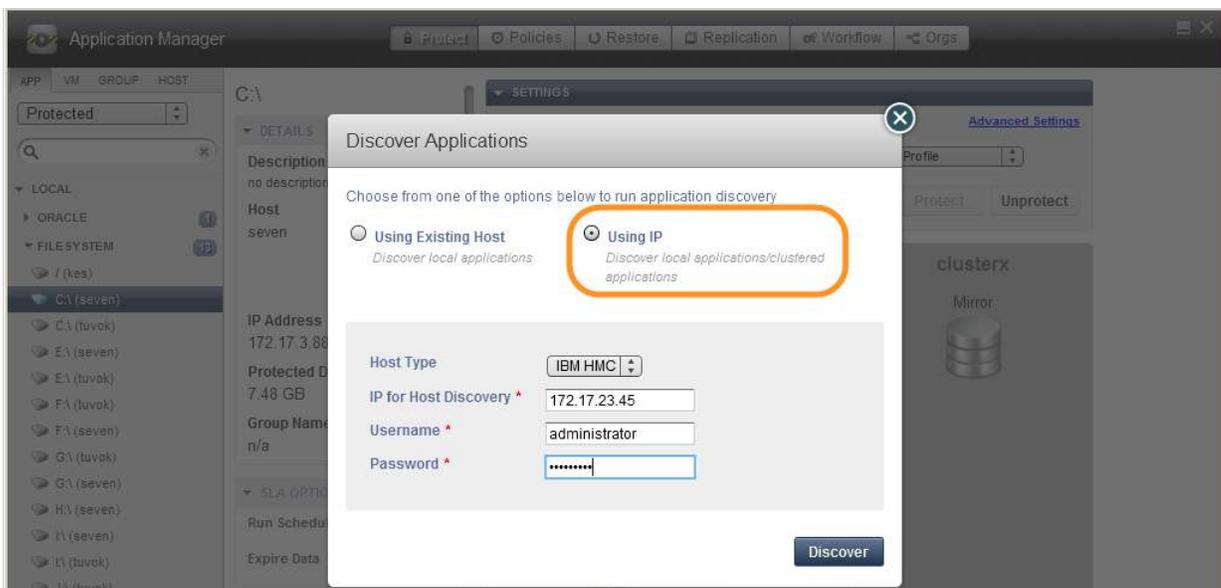
Note: AIX protection is not available for Actifio Sky appliances.

Note: CIFS shares may need user credentials defined for the host before applications can be discovered.

To discover an application over IP, including LPAR virtual machines running on AIX VIOS:

1. Open the Actifio Desktop to the **Application Manager**.
2. From the service menu, select **Discover App(s)**. The Discover Applications dialog appears.
3. Select **Using IP**.
4. Enter the IP address and credentials for the host that includes the applications that you want to discover.
To discover only clustered applications, specify an appliance IP or select an existing appliance host.
To discover both local and clustered applications, specify the IP of an appliance node or select an existing appliance node.
5. Click **Discover**. The navigation pane lists all the applications attached to the selected host, including applications residing on out-of-band storage, as soon as they are discovered.

Note: When clustered applications are discovered, a host for each appliance node is added automatically if one doesn't exist already.



Discovering Applications and IBM LPAR Virtual Machines over IP

Creating Generic Applications

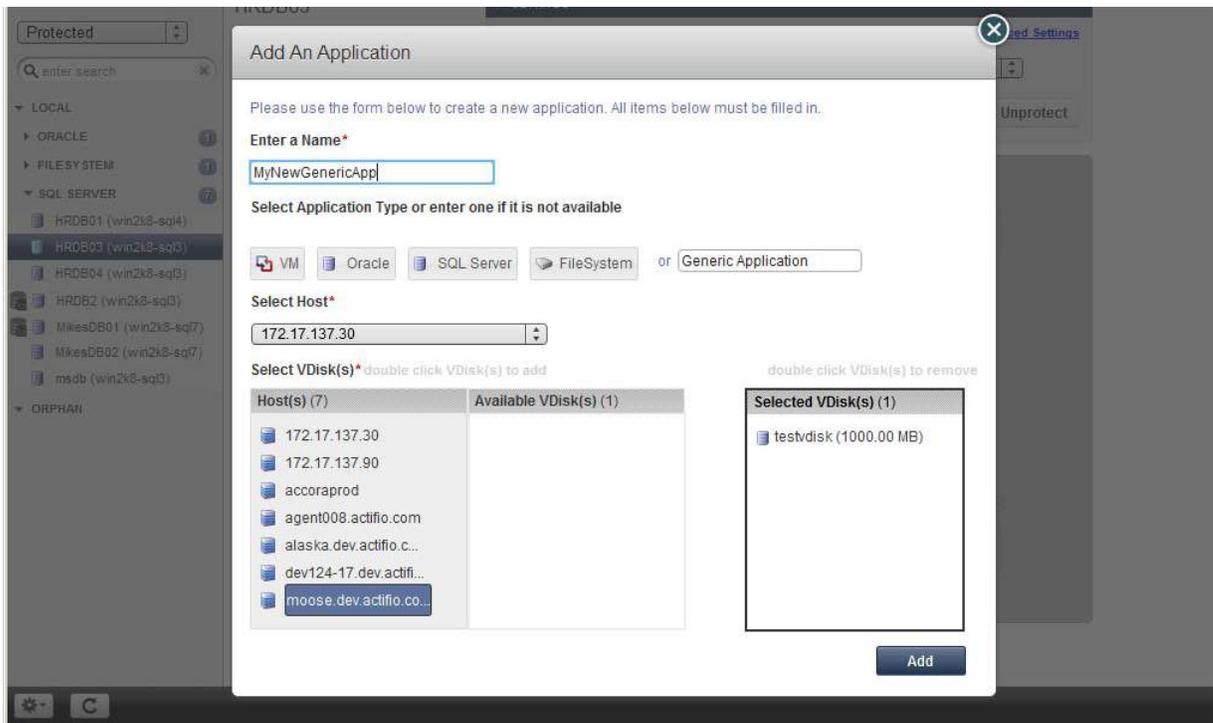
If an application is on a host that cannot be reached by the Actifio Connector or if you need a generic application for Sync or Async replication, you can create a generic application with the New Application feature on the service menu. Generic applications are defined by the LUNs they consist of.

1. Open the Actifio Desktop to the **Application Manager**.
2. From the **Service Menu**, select **New Application**.



Creating a New Application

3. Fill in the Add An Application dialog, including generic application name, application type, and host.
4. Double-click **Hosts and Available VDisks** to add them to the Selected VDisks.
5. Click **Add** to save the new generic application. It appears in the APP list under GENERIC.



Creating a New Generic Application

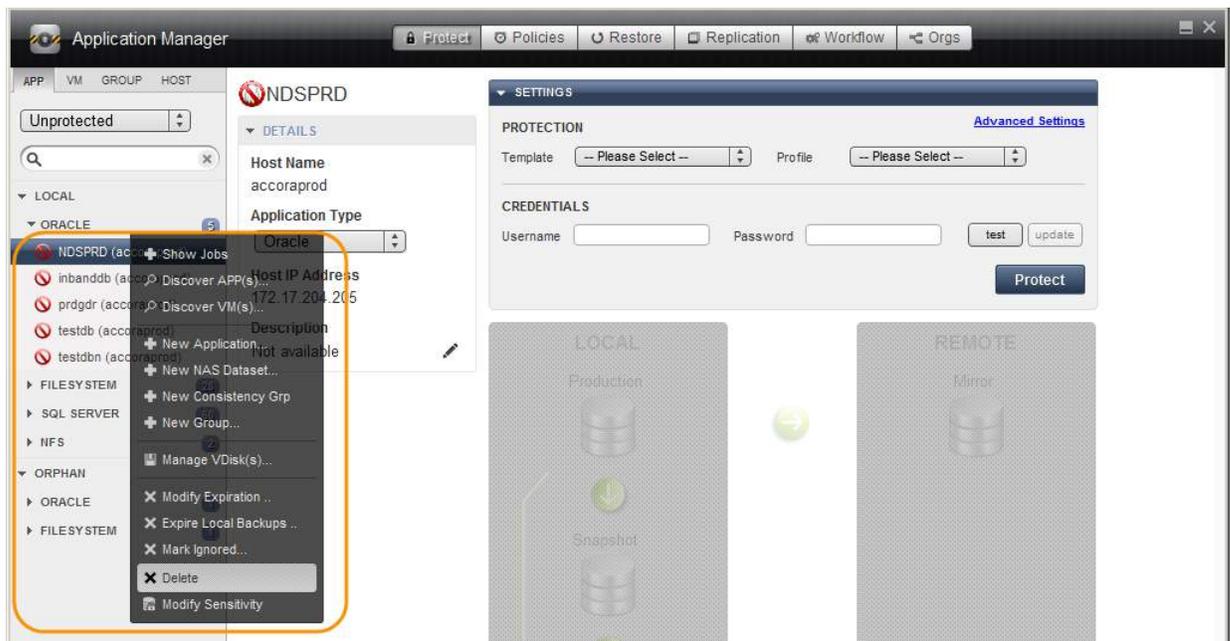
Deleting Applications, VMs, and Groups

You can delete unprotected applications, VMs, groups, and consistency groups. To delete protected applications, VMs, and groups, first unprotect them by disassociating all SLAs.

Note: Remote objects that appear in the Application Manager under the Remote category should be deleted from the remote Actifio appliance.

To delete an application, VM, or group:

1. Open the Application Manager.
2. Click the App, VM, or Group filter tab from the top of the navigation pane.



The Application Manager Navigation Pane List Filter

3. Select the Application/VM/Group to delete.
4. Right-click it to open the service menu, and click **Delete**.
5. Click **Yes** in the confirmation dialog.

Images from a deleted application appear as orphans in the navigation pane under Orphan. You can delete a resource profile or a policy template only when the resource profile or policy template is not used to protect an application. You can see an application in the orphan section only if there are any images of that application.

Note: Deleting an application or removing its protection cleans up all Dedup-Async or StreamSnap related images (if replication is configured for that application). If any stale images are left on an Actifio appliance (usually due to a remote appliance unavailability), in the left bottom menu list you will see an operation called **Cleanup Dedup Async** or **Cleanup StreamSnap**. For more information, see **Replicating Data Using Actifio Appliances**.

3 Virtualizing and Protecting Applications and VMs

You protect VMs and applications by creating Service Level Agreements (SLAs) with the SLA Architect, as described in ***Planning and Developing Service Level Agreements*** in the Actifio Documentation Library. When an SLA is applied to an application, a VM, a group, or a consistency group, the policy and the resource profile that make up the SLA dictate the type of protection to use and where to store the protected image.

This introductory section details [How Actifio Virtualization and Protection Work](#) on page 14, and then [Chapter 7, Managing Jobs](#) discusses what happens when an application is protected.

These introductory sections are followed by specific sections for each type of application and VM:

- [Chapter 8, Protecting Entire Hyper-V VMs](#)
- [Chapter 9, Protecting Local File Systems](#)
- [Chapter 10, Protecting Mapped NFS File Systems](#)
- [Chapter 11, Protecting Mapped CIFS File Systems](#)
- [Chapter 12, Protecting Exchange Databases](#)
- [Chapter 13, Protecting Generic Applications](#)
- [Chapter 14, Protecting Groups](#)
- [Chapter 15, Protecting Consistency Groups](#)

Application specific processes and procedures for Microsoft SQL Server, Oracle, and VMware VMs can be found in their respective guides:

An Oracle DBA's Guide to Actifio Copy Data Management

An SQL Server DBA's Guide to Actifio Copy Data Management

A VMware Manager's Guide to Actifio Copy Data Management

How Actifio Virtualization and Protection Work

This introductory section details the states of an application and then:

[The Stages in Virtualizing an Application or a VM](#) on page 15

[Basic Procedure for Protecting Applications and VMs](#) on page 16

[Validating Projected Resources Prior to Applying Protection](#) on page 17

Maintaining Performance When Adding New Applications

If your system has been performing acceptably and then you add new applications, performance may suffer for a short time. This is because Actifio change block tracking recognizes new data and protects it even when it is only a small part of a large application. This means the system is optimized to process many changed blocks every day.

A new application requires a lot more resources for the initial capture, because it is all new data to the Actifio system.

For best results when adding new applications:

- When you add a new application, protect it for the first time using an on-demand job during a period of light load. This will prevent the resource-intensive initial ingest job from interfering with other jobs.
- When adding multiple new applications or VMs, try to stagger the initial protection jobs for each new application over time, to prevent all of the new data from being ingested simultaneously. Do this by assigning SLAs that run at different times. You can also use the on-ramp job slots feature to minimize disruption; this is described in ***Configuring Resources and Settings With the Domain Manager***.
- Separate the initial protection job in time from the dedup job. Once an application snapshot has been taken, the deduplication job can run some hours later when the system load is lighter.
- When you need to add additional applications, check your MDL. If your managed data is close to or over your licensed capacity, contact your Actifio representative to ensure continued high performance.
- Consistency Groups can be an efficient way to protect multiple applications with similar needs; see [Chapter 6, Working with Consistency Groups](#).
- Be aware of your existing SLAs and try not to schedule snapshot jobs simultaneously with the snapshot jobs for very large or dynamic applications.

States of an Application or VM

After an application has been discovered, then your Actifio appliances consider it to be in one of three states:

Unprotected: An application is unprotected when no SLA is associated with it, or when an SLA is associated with it but the first protection job is yet to complete.

Protected: An application becomes protected when the first replication job completes successfully, or when the application is failed back (see Failed over, below). In this state, there is at least one replicated image to fail over to. An application remains in this state as long as the SLA associated with it is not removed or the application is not failed over. When you remove the SLA, the application becomes unprotected.

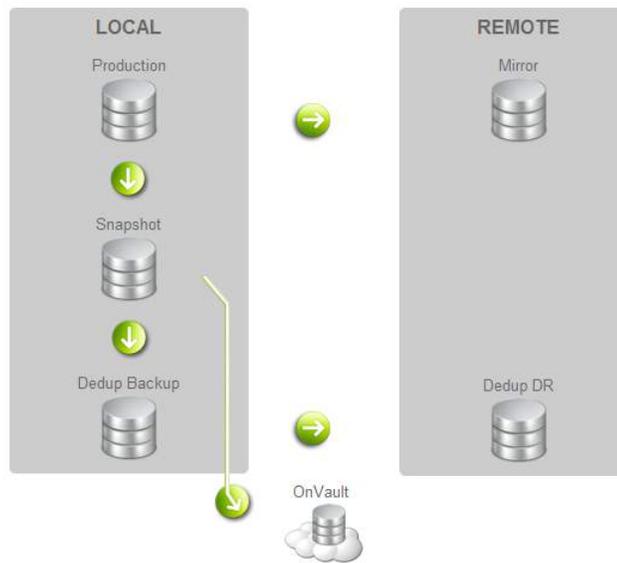
Failed over: If the application fails over to a remote site, its state changes to failed over. In the failed over state, the application, which is also configured on the remote site, accesses the remote image directly (Dedup-Async or StreamSnap image). Consequently, replication to the remote site is paused. When the application is ready to operate from the local site, you can synchronize the data back to the local site (this is called Syncback) and then when the data is back in sync, Failback to the local site.

Syncback and failback are detailed in ***Replicating Data Using Actifio Appliances***. Testing the failover capability does not alter the state of the application.

The Stages in Virtualizing an Application or a VM

When you first virtualize an application or a VM, you assign an SLA, and the SLA runs on schedule. Then:

1. The application or VM is running in local Production.
2. According to the SLA settings, the Actifio appliance takes a snapshot image of the production application. The Actifio appliance immediately stores the snapshot image in the Snapshot Pool.
3. Either immediately or at a later time, the Actifio appliance copies the image from the Snapshot Pool to the Dedup Backup Pool (referred to as simply the Dedup Pool).
4. If the Actifio appliance is joined to other Actifio appliances or to a cloud instance, then the image can be replicated to another Actifio appliance's Remote Dedup DR Pool or to an Actifio OnVault for long-term storage.



Protecting an Application

When Application Protection Takes Effect

Applying an SLA does not immediately protect an application. Protection jobs run on a schedule, according to resource availability. You can also run the job immediately; see [Suspending Protection](#) on page 55.

- The SLA includes a schedule of when to run the protection job for this application, such as daily between 6 PM and 6 AM, every four hours. If you apply protection to an application at 1 PM today, then the first protection operation will be scheduled for 6 PM today.
- At the scheduled time, the job is assigned a **job slot**. Job slots are usually available when the job is scheduled, but some factors can complicate the picture. Job slots are detailed in [Chapter 7, Managing Jobs](#).

Changing Protection

You can change an application's protection at any time. Future backups will occur based on the new template. Existing backups will be retained according to the old template that was in force when they were created.

The Change Tracking Driver

The Actifio Connector with its change tracking driver (sometimes called the filter driver) enables efficient incremental backups by tracking changes from the host side. After the first complete backup of a database, the Actifio appliance performs incremental backups by default. If your backups are still always full backups, then check for the following:

- The change tracking driver service is stopped. In this case, restart the change tracking driver service.
- The change tracking driver is incorrectly configured or not installed. In this case, uninstall and then make a full install of the Actifio Connector.

Basic Procedure for Protecting Applications and VMs

To protect an application:

1. Open the **Application Manager** to the **Protect** tab.
2. From the navigation pane, select **APP** or **VM**.
3. From the filter, select **Unprotected**.
4. On the navigation pane, select the application or VM that you want to protect, then click the blue **Advanced Settings** link in the upper right corner of the Settings section to open the Application Advanced Settings page. Set the Advanced Settings as needed. Details for each application type are provided in each chapter.
5. Select an SLA template from the **Template** drop-down list. This is the template that defines the snapshot/deduplication/replication of the application data.
6. Select a resource profile from **Profile** drop-down list. This defines the resources used to store the data of the application as snapshot/deduplicated/replicated images.
7. Click **Protect**. The application status becomes Protection-Initialization; it is not Protected until the scheduled job runs according to the hours of operations defined in the template. For example, if at 10 AM today you assign a template that has hours of operation from 2 AM to 5 PM, then the first job will not start until there is an available job slot after 2 AM tomorrow.

Note: A Warning screen appears if the selected SLA template policy might impact system resources. See [Validating Projected Resources Prior to Applying Protection](#) on page 17 for additional details.



Protecting an Application

For details on protecting specific application and VM types, see:

- [Chapter 8, Protecting Entire Hyper-V VMs](#)
- [Chapter 9, Protecting Local File Systems](#)
- [Chapter 10, Protecting Mapped NFS File Systems](#)
- [Chapter 11, Protecting Mapped CIFS File Systems](#)
- [Chapter 12, Protecting Exchange Databases](#)
- [Chapter 13, Protecting Generic Applications](#)
- [Chapter 14, Protecting Groups](#)
- [Chapter 15, Protecting Consistency Groups](#)

An Oracle DBA's Guide to Actifio Copy Data Management

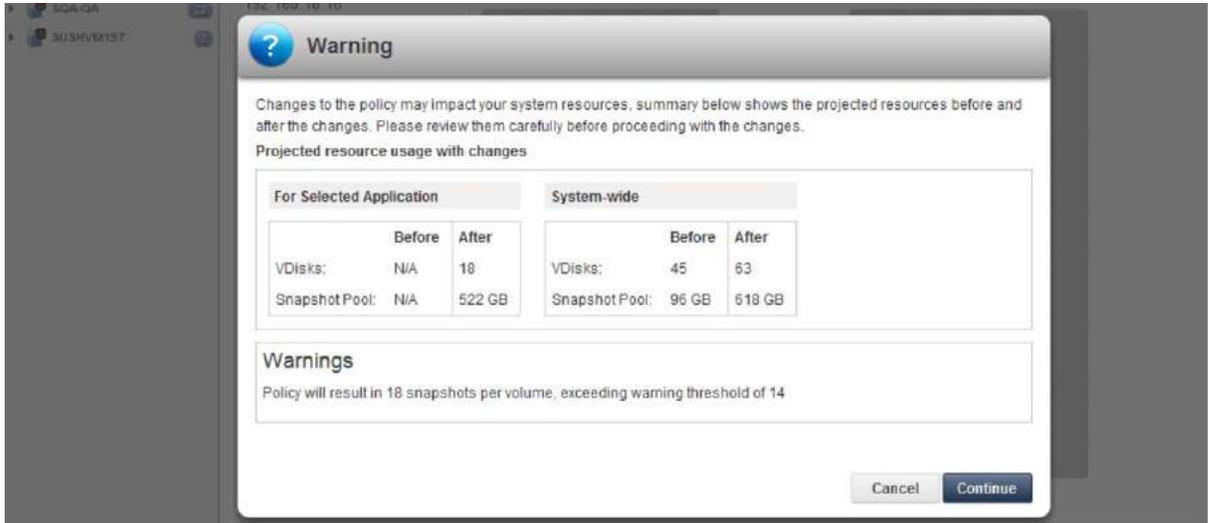
An SQL Server DBA's Guide to Actifio Copy Data Management

A VMware Manager's Guide to Actifio Copy Data Management

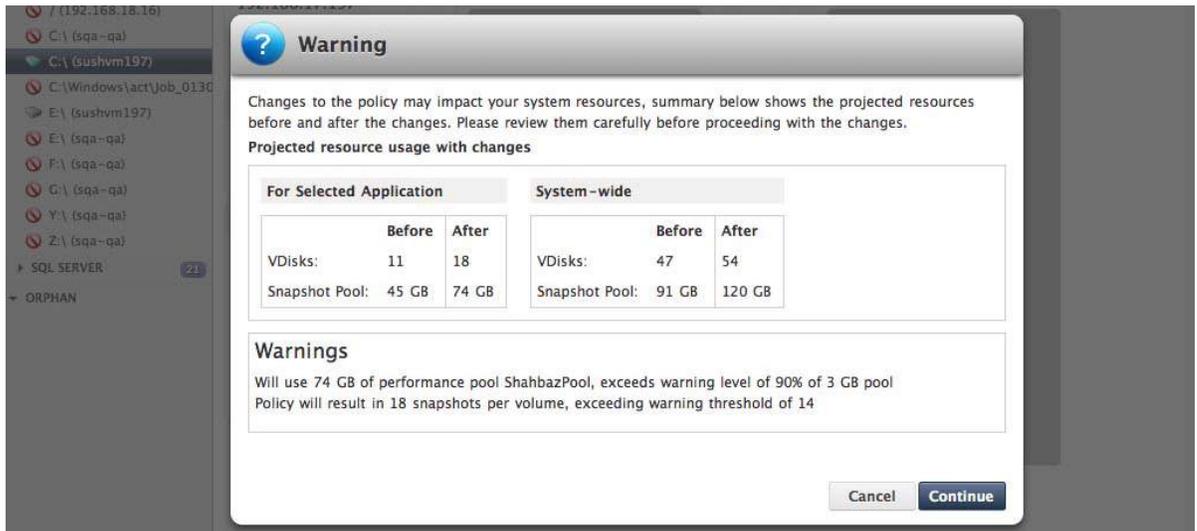
Validating Projected Resources Prior to Applying Protection

To avoid impacting the Actifio appliance's performance when applying an SLA policy template to protect applications and VMs, a warning screen informs you of a potential impact to system resources based on the policy settings.

Note: The calculation of VDisk usage and performance pool usage is directly related to the number of snapshot copies during steady state. The number of snapshot copies during steady state is related to the Recovery Point Objective (RPO) and retention. For example, an RPO of 8 hours and a retention of 3 days means that there will be a total of 9 snapshot copies. This total is subject to the number of days the policy is in effect and the time range defined within the day.



Verifying System Resources for an SLA Policy - Prior to Protecting Applications



Verifying System Resources for an SLA Policy - Changes to SLA After Protection

The Warning screen displays the following information related to applying the configured SLA policy for application protection. It displays projected resource usage with SLA policy changes for the selected applications as well as across the system.

For Selected Applications

VDisks - The expected VDisks usage by the Actifio appliance to protect the selected applications and VMs before **and** after you apply the selected SLA policy. This system resource number is the number of VDisks consumed per volume, including the staging disks.

Snapshot Pools - The expected usage of the performance pools (staging disks and snapshot disks) by the Actifio appliance to protect the selected applications and VMs before **and** after you apply the selected SLA policy. The Snapshot pool holds "golden copies" of application data at the points in time specified by the SLA. This system resource usage is specified as capacity per 1TB based on retention and average change rates.

System-wide

VDisks - The expected VDisks usage across the entire Actifio appliance before **and** after you apply the selected SLA policy for application protection.

Snapshot Pools - The expected performance pool usage across the entries Actifio appliance before **and** after you apply the selected SLA policy for application protection.

The Warning screen can be indicative of the following system resource issues for the specified SLA policy template:

- The SLA policy has more than 14 snapshots.
- VDisk usage with the SLA policy will result in VDisks usage that exceeds the warning level (default of 90%) during steady state.
- Performance pool (staging disks and snapshot disks) usage with the SLA policy will result in a performance pool that exceeds the warning level (default of 90% for the snapshot and primary pools).
- Average dedup pool utilization (7 days) is already at the warning level (75% by default) and there are additional dedup jobs in the queue. This action has the potential of adding more dedup jobs to an already overloaded dedup system.

You can:

- **Cancel** to adjust the SLA policy template in the SLA Architect.
- **Continue** to accept the policy.

If you decide to make changes to the policy in the SLA Architect, evaluate the frequency of the backup operation and lifetime of the backed up data to see where adjustments can be made to resolve the warning. See ***Planning and Developing Service Level Agreements*** in the Actifio Documentation Library.

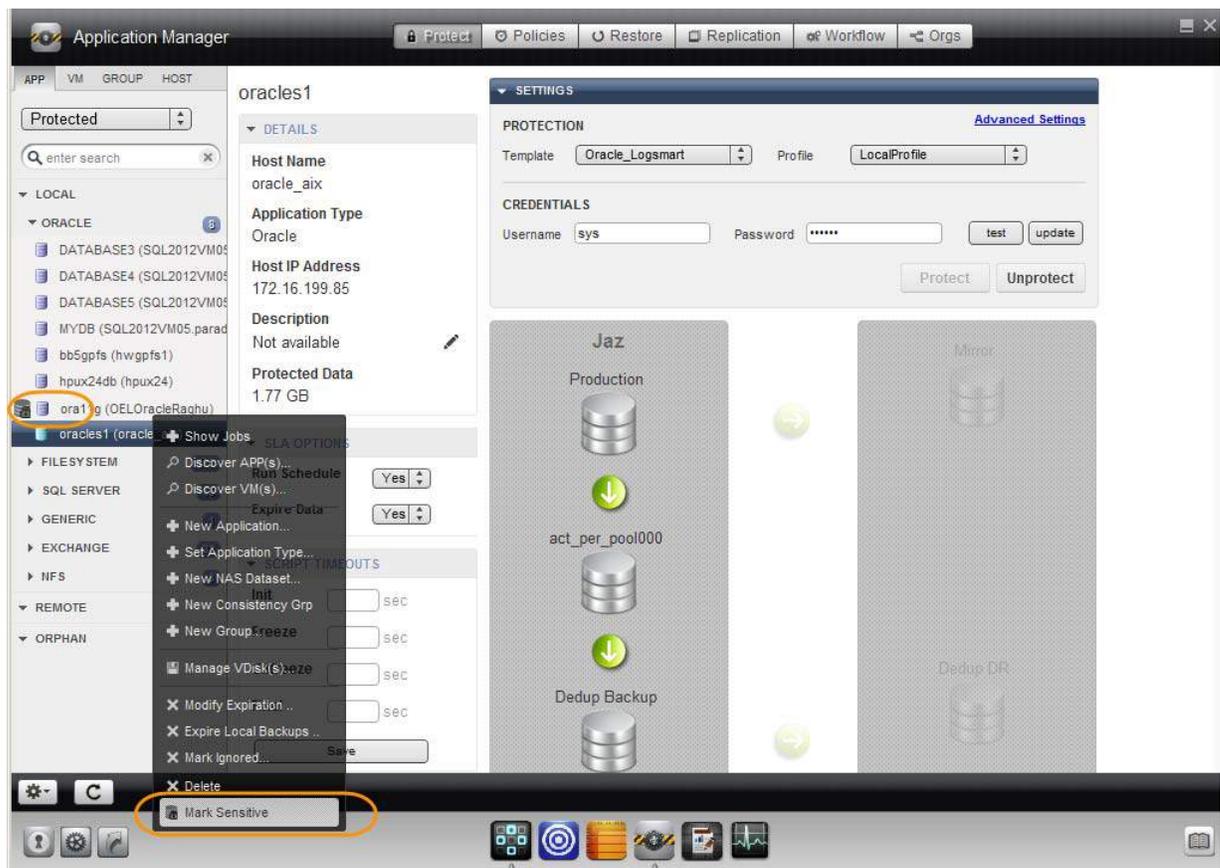
4 Marking Applications and Images as Sensitive

You can mark applications and images as sensitive. Sensitive data can be accessed only by users with access to sensitive data enabled in their LDAP user accounts as detailed in **Setting Up Users and Roles With the Domain Manager** in the Actifio Documentation Library.

- You can mark an application, VM, or group as sensitive, as detailed in [Marking an Application, VM, or Group as Sensitive](#) on page 19. Hosts cannot be marked as sensitive.
- You can mark specific images as sensitive, as described in [Marking an Image as Sensitive](#) on page 20.

Marking an Application, VM, or Group as Sensitive

To mark an application, VM, or group as sensitive, right-click it and select **Mark Sensitive**. The application, VM, or Group is tagged as containing sensitive data. Starting with its next SLA job, images of this application, VM, or group will be marked sensitive as well.



Marking a Database as Sensitive, Another is Already Sensitive

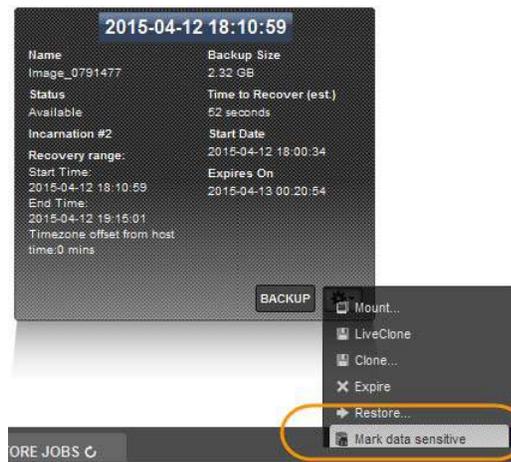
Marking an Image as Sensitive

To mark a specific image as sensitive:

1. Open the Application Manager to the **Restore** tab.
2. Select the image type by clicking on the corresponding Snapshot, Dedup, Syncback, Remote, LiveClone, or OnVault button. You can use the Shift key to select multiple items.
3. Select the image. The image can be a local image or a remote image (from remote Actifio appliances 1 or 2 in a multi-hop appliance configuration).

The color of the box representing the image turns green on selection and the image details are displayed on a tab.

4. Click the image information action pull-down menu at the bottom right.
5. Select **Mark data sensitive**. The image is tagged as containing sensitive data. It can now be accessed only by users with access to sensitive data turned on in their LDAP user accounts.



Marking Data as Sensitive

5 Working with Groups

Use application groups when multiple applications have the same protection needs:

Groups are used for ease of management to apply a common policy to all the group's applications. Mount, clone, and restore operations are performed on the backup images of each application in the group individually.

Consistency Groups are collections of discovered applications from the same host. You create a consistency group to back up application data of all member applications together to preserve consistency of data across the member applications. You apply a common policy to the members of a consistency group. Consistency groups are introduced in [Chapter 6, Working with Consistency Groups](#)

This chapter details:

[Creating a Group](#) on page 22

[Deleting a Group](#) on page 22

To protect groups, see [Chapter 14, Protecting Groups](#).

Creating a Group

To create a group of applications to manage the group using a common policy:

1. Open the Actifio Desktop to the **Application Manager**.
2. From the service menu, select **New Group**.



Creating a Group

3. The Group Properties window opens.
4. Enter a name in **Group Name**.
5. You can use the text field to the right of Apps as a filter. Select an application by clicking the **+** beside it. To add all applications to the group, click **Add All**.
6. When you are finished, click **Save**.

You can also create a group by selecting applications and then right-clicking and selecting **New Group**.

Deleting a Group

To delete a group:

1. Open the Application Manager.
2. Click the **GROUP** tab from the top of the navigation pane.
3. Select the group to delete.
4. From the Service Menu, click **Delete**.
5. Click **Yes** in the confirmation dialog.

The group appears as an orphan in the navigation pane under Orphan if there are any backup images corresponding to that group.

Note: You can also delete a group or a consistency group by right-clicking it and selecting **Delete**.

Note: Deleting an application or removing its protection cleans up all Dedup-Async or StreamSnap related images (if replication is configured for that application). If any stale images are left on an Actifio appliance (usually due to a remote appliance unavailability), in the left bottom menu list you will see an operation called **Cleanup Dedup Async** or **Cleanup StreamSnap**. For more information, see **Replicating Data Using Actifio Appliances**.

6 Working with Consistency Groups

Groups and consistency groups are used when multiple applications have the same protection needs:

Consistency Groups are collections of discovered applications from the same host. You create a consistency group to back up application data of all member applications together to preserve consistency of data across the member applications. A single SLA Policy Template and Resource Profiles is used to capture a consistency group.

Groups are used for ease of management to apply a common policy to all the group's applications. Mount, clone, and restore operations are performed on the backup images of each application in the group individually. Groups are introduced in [Chapter 5, Working with Groups](#).

Consistency groups:

- are protected and restored the same as other applications.
- that contain SQL Server databases or Oracle databases can be mounted together in an application aware mount. An individual SQL Server database and Oracle database in a consistency group cannot be mounted as a virtual application in an application aware mount.
- can be used in Workflows. Individual applications in a consistency group cannot be part of a Workflow.

This chapter details:

[Creating a Consistency Group](#) on page 24

[Deleting a Consistency Group](#) on page 25

To protect consistency groups, see [Chapter 15, Protecting Consistency Groups](#).

Creating a Consistency Group

You can create a consistency group to back up the data of all member applications together to preserve consistency of data across the member applications. In addition, you apply a common policy to the members of a consistency group. Consistency groups are collections of discovered applications from the same host.

The Actifio appliance guarantees a consistent capture that is snapshotted at the same moment in time for:

- Applications on the same host that reside on volumes that are all in-band virtual disks.
- Windows applications on the same host, including SQL Server, Exchange, and SharePoint databases, and local File Systems.

For all other configurations, a consistency group can be defined and backup of its member applications will run as one job on the host but snapshots of each application will be independent and not at the same point in time.

When creating a snapshot of these applications, the Actifio appliance resolves all of the applications into a collection of volumes. If all of these volumes are in-band virtual disks, then the consistency group is snapshotted at the same moment in time. If any one of the volumes is not in-band, then the consistency group is backed up as out-of-band application, and the constituent applications are self-consistent, but not at the same point in time.

Note: *In-Band protection is not applicable to Actifio Sky appliances.*

To create a consistency group:

1. Open the Application Manager.
2. From the service menu, select **New Consistency Grp.**
3. Select an application by clicking the **+** sign displayed against the application. Only unprotected applications are listed. If you cannot find an application, then that application is probably already protected. You can add all applications to the group by clicking **Add All** and then click **Save**.

You can also create a consistency group by right-clicking applications and selecting **New Consistency Group**.



Creating a Consistency Group

Note: *Generic applications and VMs are not allowed in consistency groups. Oracle does not support consistency groups of multiple databases. A consistency group may include a single Oracle database with other applications.*

Deleting a Consistency Group

To delete a consistency group:

1. Open the Application Manager.
2. Click the **GROUP** tab from the top of the navigation pane.
3. Select the consistency group to delete.
4. From the Service Menu, click **Delete**.
5. Click **Yes** in the confirmation dialog.

The consistency group appears as an orphan in the navigation pane under Orphan if there are any backup images corresponding to that consistency group.

Note: You can also delete a consistency group by right-clicking it and selecting **Delete**.

Note: Deleting an application or removing its protection cleans up all Dedup-Async or StreamSnap related images (if replication is configured for that application). If any stale images are left on an Actifio appliance (usually due to a remote appliance unavailability), in the left bottom menu list you will see an operation called **Cleanup Dedup Async** or **Cleanup StreamSnap**. For more information, see **Replicating Data Using Actifio Appliances**.

7 Managing Jobs

All activities run as jobs. Jobs are executed according to the schedules configured when the policies were created. Understanding jobs and how they run will help you to prevent slow performance and missed jobs.

Some jobs take much longer than others. Expiration jobs are fast. Snapshot jobs depend upon variables like the size of the application or VM and how much data has changed since its last snapshot; the initial snapshot of any application or VM is all-new data, so those can take a long time. Deduplication jobs take a varying amount of time depending on how full the Dedup Pool is and if Garbage Collection is running.

This chapter describes:

[Scheduled Jobs](#) on page 28

[On-Demand Jobs](#) on page 29

[Running an On-Demand Backup](#) on page 30

[Running On-Demand Database Log Replication](#) on page 31

Each job type can be scheduled through an SLA Template Policy, and run on-demand as needed. Data-Dependent jobs take longer than jobs that use changed blocks only or jobs that are not data-dependent. Jobs that depend on the Dedup Pool may take longer while GC is running. For more information, see *Managing the Dedup Pool* in **Configuring Resources and Settings With the Domain Manager** in your Actifio Documentation Library.

Scheduled Jobs

Jobs run according to the schedule assigned in their SLA Template Policies. If you try to run many resource-intensive jobs simultaneously, then some will have to wait for the resources to come available. In very bad situation, they may have to wait so long that an SLA Violation occurs.

It is better to stagger the more resource-intensive jobs like initial snapshots and deduplication jobs over time rather than to have them all compete for resources at the same moment. For example, instead of snapping all VMs, file systems, and databases at 6:00pm on weekdays, consider snapping one type of application on the hour, another type at 10 minutes after the hour, another type at 20 minutes after the hour, and so on.

It is not necessary to deduplicate snapshots as soon as they are captured. Once the snapshot is taken, the data is safe in the Snapshot Pool; it can be deduplicated at a slower time such as at night.

The initial snapshot of an application or a VM is the largest and most time-consuming snapshot it will ever get because every bit of data is new. When you add a new application or VM, perform an on-demand snapshot at an off-peak time for the first snapshot and then schedule an SLA Template Policy for all future snaps.

Relaunching Failed Jobs

All scheduled jobs are automatically re-launched if they fail. The number of retries depends on the configuration value that is set in the Actifio appliance.

You can view the relaunched jobs from **System Monitor > Jobs** with the job status as 'retry'. To view the details of a relaunched job, double-click the job. See **Using the System Monitor to Monitor Jobs and Events** for information about the Actifio System Monitor.

The screenshot shows the 'System Monitor' interface with the 'Jobs' tab selected. On the left, the 'FILTER BY STATUS' section has 'RETRIED' selected. The main area displays a table titled 'List of jobs' with the following data:

Job Name	Type	Priority	Status	Host	Application	Policy	Template	Consistency	Start Time	End Time
Job_1454972	snapshot	medium	retry	rhel6.5	newmnt	Production	All-DAR1hr	Sep 26 23:4	Sep 26 23:4	Sep 26 23:4
Job_1454972	snapshot	medium	retry	rhel6.5	newmnt	Production	All-DAR1hr	Sep 26 23:3	Sep 26 23:3	Sep 26 23:3
Job_1453568	snapshot	medium	retry	rhel6.5	newmnt	Production	All-DAR1hr	Sep 26 22:3	Sep 26 22:3	Sep 26 22:3
Job_1453568	snapshot	medium	retry	rhel6.5	newmnt	Production	All-DAR1hr	Sep 26 22:3	Sep 26 22:3	Sep 26 22:3
Job_1451968	snapshot	medium	retry	rhel6.5	newmnt	Production	All-DAR1hr	Sep 26 20:2	Sep 26 20:2	Sep 26 20:2
Job_1451968	snapshot	medium	retry	rhel6.5	newmnt	Production	All-DAR1hr	Sep 26 20:1	Sep 26 20:1	Sep 26 20:1

At the bottom of the interface, it shows 'Updated: 2015-09-27 14:13:21 # Job(s): 6' and 'Page 1 of 1'.

The List of Retried Snapshot Jobs in the System Monitor

On-Demand Jobs

The great majority of jobs run on schedule according to their SLAs, but for upcoming maintenance windows, software upgrades, and for the first snapshot of a new application, you want to ensure that you have a successful copy of the data created before you start your scheduled maintenance task. These cases call for an on-demand job.

To run an on-demand job from the Application Manager, see [Running an On-Demand Backup](#) on page 30.

To run an on-demand log replication job from the Application Manager, see [Running On-Demand Database Log Replication](#) on page 31.

About Job Slots

The Actifio appliance manages jobs by assigning *job slots*. The Actifio appliance reserves a pool of slots for each category of jobs, plus an pool of unreserved slots.

Before starting a job, the Actifio appliance checks whether a slot corresponding to the job's category is available to run the job. When a reserved slot is not available because all the slots of that category are running jobs, the Actifio appliance checks whether an unreserved slot is available. If an unreserved slot is available, the job is started.

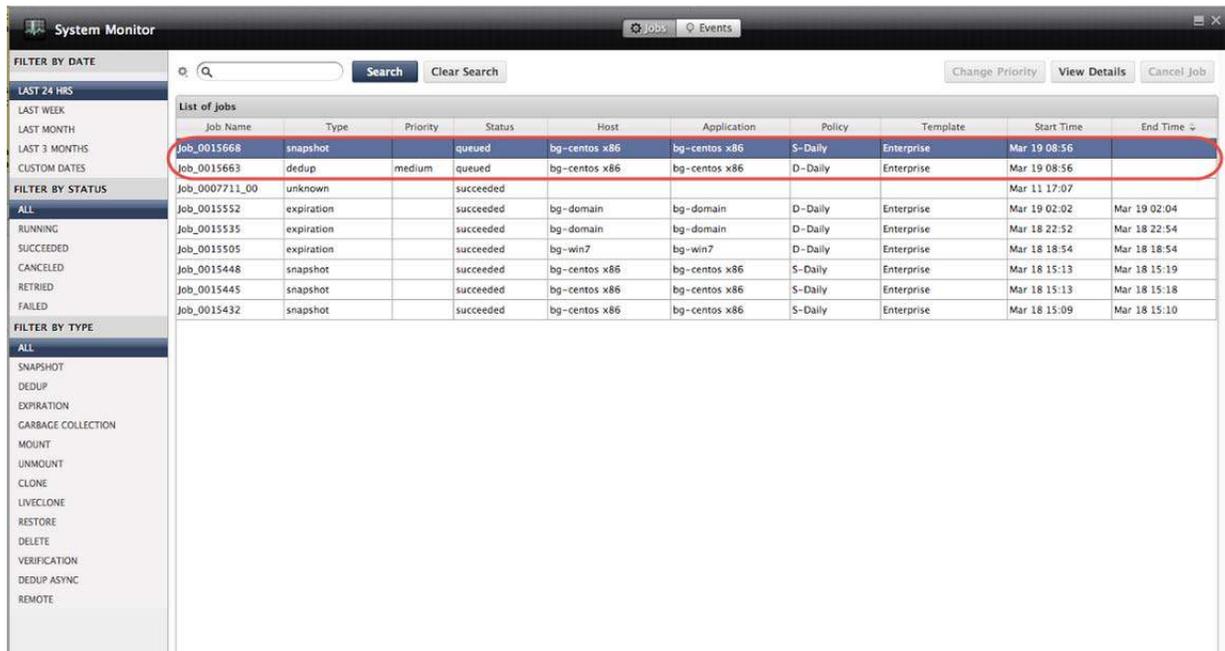
Queuing of On-Demand Backup Jobs

The Actifio appliance supports queuing of on-demand jobs to provide you with the flexibility to create your images without concern for the number of on-demand job slots available to start the job. The queued on-demand job remains in the queued state until an on-demand job slot is available.

When an on-demand slot opens, the job progresses to the running state. This sequence occurs in the order that the job was submitted. If an on-demand job fails, the Actifio appliance will attempt to run the next job in the queue. On-demand jobs use different job slots than scheduled jobs, so scheduled jobs may run before queued jobs.

While an on-demand job is in a queued state you can cancel the job or cancel protection for the application. The on-demand job will then appear in the job history table as a canceled job. The start time of the job and the end time of the job will be the time that the cancel request or the cancellation of application protection was acknowledged.

Using the Actifio Desktop, you can view the queued jobs from **System Monitor > Jobs**.



The screenshot shows the 'System Monitor' window with the 'Jobs' tab selected. The 'List of Jobs' table is displayed with the following data:

Job Name	Type	Priority	Status	Host	Application	Policy	Template	Start Time	End Time
Job_0015668	snapshot		queued	bg-centos x86	bg-centos x86	S-Daily	Enterprise	Mar 19 08:56	
Job_0015663	dedup	medium	queued	bg-centos x86	bg-centos x86	D-Daily	Enterprise	Mar 19 08:56	
Job_0007711_00	unknown		succeeded					Mar 11 17:07	
Job_0015552	expiration		succeeded	bg-domain	bg-domain	D-Daily	Enterprise	Mar 19 02:02	Mar 19 02:04
Job_0015535	expiration		succeeded	bg-domain	bg-domain	D-Daily	Enterprise	Mar 18 22:52	Mar 18 22:54
Job_0015505	expiration		succeeded	bg-win7	bg-win7	D-Daily	Enterprise	Mar 18 18:54	Mar 18 18:54
Job_0015448	snapshot		succeeded	bg-centos x86	bg-centos x86	S-Daily	Enterprise	Mar 18 15:13	Mar 18 15:19
Job_0015445	snapshot		succeeded	bg-centos x86	bg-centos x86	S-Daily	Enterprise	Mar 18 15:13	Mar 18 15:18
Job_0015432	snapshot		succeeded	bg-centos x86	bg-centos x86	S-Daily	Enterprise	Mar 18 15:09	Mar 18 15:10

Queued Job List in the System Monitor

Running an On-Demand Backup

To run an on-demand backup:

1. Open the Application Manager to the **Protect** tab.
2. Select the application that you want to virtualize from the navigation pane.

Note: You cannot run an on-demand backup for an individual member of a consistency group.

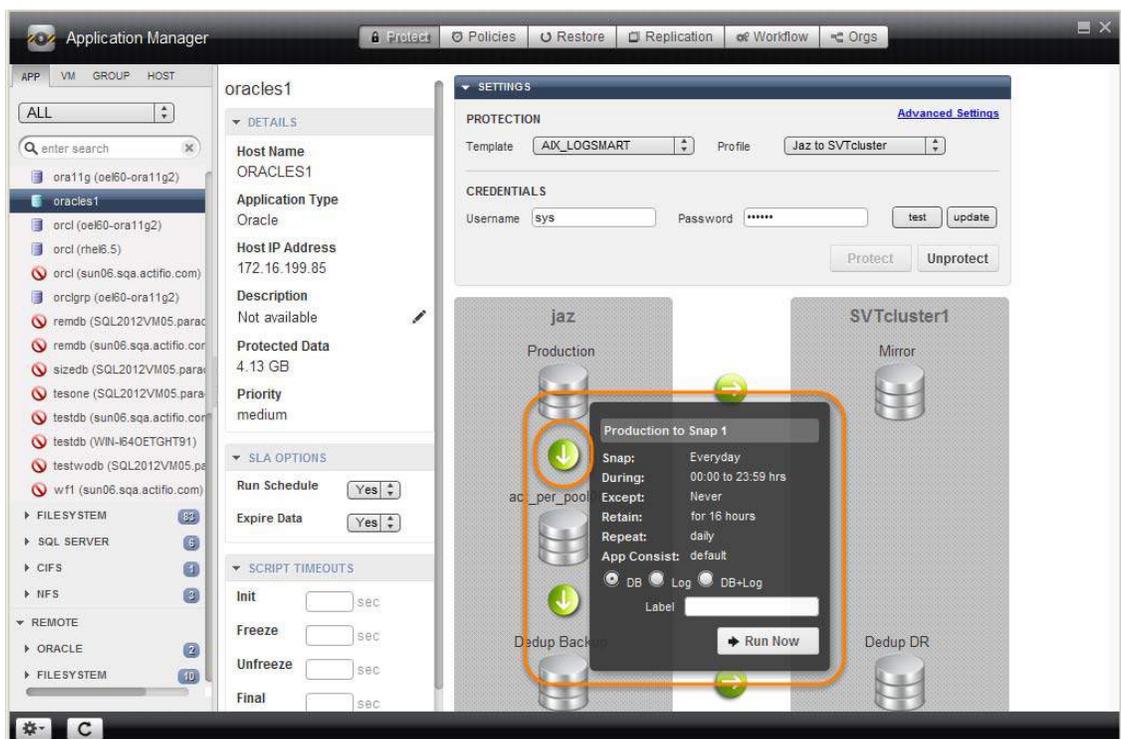
3. Click the arrow that shows the snapshot policies configured to manage the backup.

For Microsoft® SQL Server and Oracle policies with database log backup enabled, you have the option of backing up just the database, just the database log, or the database and its log together.

Note: On-demand StreamSnap jobs can be run for DB and DB+Log types.

To perform on-demand log replication of just the database log to a remote Actifio appliance, use the **Replicate Logs** menu as described in [Running On-Demand Database Log Replication](#) on page 31.

4. In the space provided, enter a label for the backup as needed.
5. Click **Run Now** and a confirmation dialog box appears.
6. Click **Yes** in the confirmation dialog. A backup image will be created and retention as per the policy.



Running an On-Demand Backup Job

Note: If a job corresponding to the policy is already running, then the on-demand job will fail.

Running On-Demand Database Log Replication

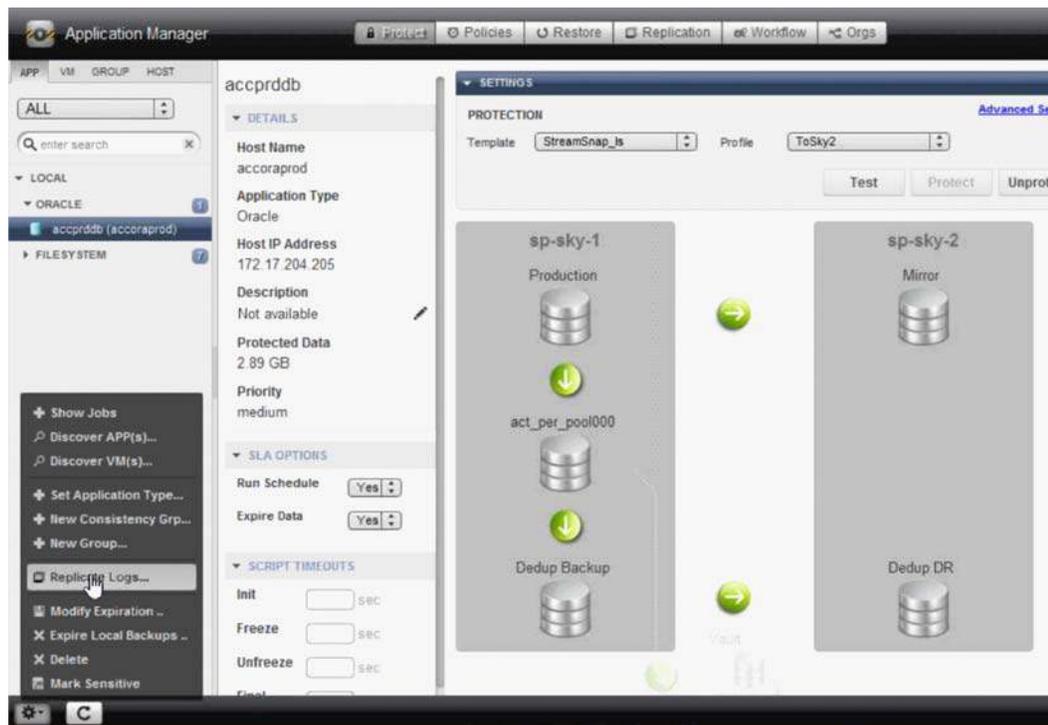
When you enable Oracle or Microsoft® SQL Server database transaction log replication in a snapshot policy and a replication policy is included in the template, database logs will be replicated to the remote Actifio appliance as part of the normally scheduled protection operation. Log replication occurs soon after the log or database and log backup is complete.

In some cases you may need to manually initiate log replication to the remote Actifio appliance for an Oracle or SQL Server database image. For example, you may need to manually perform log replication if the log for a database image did not properly replicate to the Actifio appliance or if there is no log for the database image on the Actifio appliance. You can then use the transaction logs at the remote Actifio appliance to recover a database to a specified point-in-time.

Note: Manually replicated transaction logs will not be visible on the remote Actifio appliance until the Oracle or Microsoft® SQL Server database image is replicated to the remote Actifio appliance. The recover range will only be visible when the replicated database image appears on the remote appliance.

To manually initiate replication for Oracle or SQL Server database logs to the remote Actifio appliance:

1. Open the Application Manager to the **Protect** tab.
2. Select the protected Oracle or SQL Server database application from the navigation pane.
3. Click the gear icon in the lower left corner of the Actifio Desktop and select **Replicate Logs**. A confirmation dialog box appears.
4. Click **Yes** in the confirmation dialog. The database transaction log will be replicated to the remote Actifio appliance as defined per replication policy in the template.



Running On-Demand Log Replication

8 Protecting Entire Hyper-V VMs

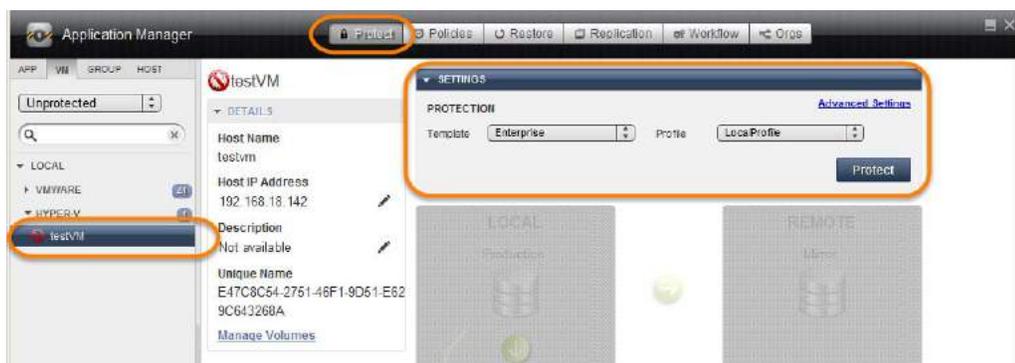
When an Actifio appliance protects an entire VM, it is not aware of VM content so no application-specific actions are possible during backup or restore. Hyper-V VMs are captured through the Actifio Connector on the Hyper-V server.

To protect an entire Hyper-V VM:

1. Open the **Application Manager** to the **Protect** tab.
2. From the navigation pane, select **VM**. From the filter, select **Unprotected**.
3. On the navigation pane, select the Hyper-V VM that you want to protect.
4. Click the blue Advanced Settings link in the upper right corner of the Settings section to open the Application Advanced Settings page. Set the Application Advanced Settings as needed. Application Advanced settings are detailed in [Application Advanced Settings for Hyper-V VMs](#) on page 34.
5. Select an SLA template from the **Template** drop-down list. This is the template that defines the snapshot/deduplication/replication of the application data.
6. Select a resource profile from **Profile** drop-down list. This defines the resources used to store the data of the application as snapshot/deduplicated/replicated images.
7. Click **Protect**. The application status becomes Protection-Initialization; it is not Protected until the scheduled job runs and according to the hours of operations defined in the template. For example, if at 10:00 AM today you assign a template that has hours of operation from 2:00 AM to 5:00 AM, then the first job will not start until the Actifio appliance has an available job slot after 2:00 AM tomorrow.

Note: A Warning screen appears if the selected SLA template policy might impact system resources. See [Validating Projected Resources Prior to Applying Protection](#) on page 17 for additional details.

8. To run a job immediately, see [On-Demand Jobs](#) on page 29.



Protecting a Hyper-V VM

Note: For best results, enable Hyper-V Integration Services.

Application Advanced Settings for Hyper-V VMs

To configure application advanced settings for protecting a Hyper-V VM:

1. Open the Application Manager to the **Protect** tab.
2. Select **VM** and select a Hyper-V VM from the navigation pane.
3. Click the blue **Advanced Settings** link in the upper right corner. The Advanced Settings page appears.
 - o **Application Consistent:** Ignore this setting. If you have Microsoft Hyper-V Integration Services enabled, then backups will be application-consistent. If you do not have Microsoft Hyper-V Integration Services enabled, then backups will be crash-consistent.

Application consistent backups lose no data. It pauses application data I/O, completes in-flight transactions, and flushes memory to disk. On recovery, data is easily accessible.

Crash consistent backups are fast backups of application data in storage as if power were lost at that moment. It does not pause application data I/O. All data on disk are saved, and data in memory is lost. Incomplete transactions may be saved. The recovery of a crash consistent backup may take longer time and introduce exceptions. Typically recovery from crash has to be made manually.

Take crash consistent backup on last try: This option initially takes application consistent backups, but if an application consistent backup fails for any reason, it will then take a crash consistent backup.
 - o **Username/Password:** User credentials for truncating a SQL transaction log. This is required only if log truncation is required.
 - o **Staging Disk Size:** Enter a size for the staging disk to be occupied by the image copy.
 - o Choose **Do Not Unmap** if you want temporary staging disks mapped to the host and used during data movement for backup to remain mapped to the host. LUNs are mapped during the first job and all the subsequent jobs reuse the same mapped LUN. By default, this option is selected.
 - o **Backup Only Boot Volume:** If you want to back up only the boot volume of the VM, then select that option from the dropdown list.
 - o Select whether to truncate the log after every backup from the **Truncate Log After Backup** dropdown list. When this is selected, application-related logs are truncated until the recent or current backup.
 - o If the VM includes an SQL database, then enter an **SQL Database Backup Path** to define a location for a temporary SQL backup. If the Actifio Connector takes a full, native backup of the SQL Server database, the backup will be saved in this directory. Ensure that there is enough free space in the volume hosting this directory to hold a full database backup.
 - o Leave **Connector Options** blank unless you are working with Actifio Support.
4. Click **Save** to update the changes.

9 Protecting Local File Systems

This procedure is for protecting local file systems. To protect mapped NFS file systems, see [Chapter 10, Protecting Mapped NFS File Systems](#) and to protect mapped CIFS file systems, see [Chapter 11, Protecting Mapped CIFS File Systems](#).

To protect a local file system:

1. Open the Actifio Desktop to the **Application Manager**.
2. Select the filesystem application from the navigation pane under **Local > FILESYSTEM**.
3. Select the **Protect** tab.
4. Click the blue **Advanced Settings** link in the upper right corner. The Advanced Settings page appears. Fill in application advanced settings as needed for this file system. Application Advanced settings are detailed in [Application Advanced Settings for Local File Systems](#) on page 36.
5. Select an SLA template from the **Template** drop-down list. This is the template that defines the snapshot/deduplication/ replication of the application data.
6. Select a resource profile from **Profile** drop-down list. This defines the resources used to store the data of the application as snapshot/deduplicated/replicated images.
7. Click **Protect**. The application status becomes Protection-Initialization; it is not Protected until the scheduled job runs according to the hours of operations defined in the template. For example, today at noon you can assign a template that has hours of operation of 2:00 AM to 5:00 AM to an application and the first job will not start before 2:00 AM tomorrow. The first Snapshot or Direct-to-Dedup job should start when the Actifio appliance has its next available slot. Check the System Monitor to find the running job.

Note: A Warning screen appears if the selected SLA template policy will result in a potential impact to system resources based on the policy settings. See [Validating Projected Resources Prior to Applying Protection](#) on page 17 for additional details.



Protecting a Local File System

Application Advanced Settings for Local File Systems

To configure application advanced settings for local file systems:

1. Open the Application Manager to the **Protect** tab.
2. Select **APP**. Under **Local > Filesystem**, select the file system.
3. Click the blue **Advanced Settings** link in the upper right corner. The Advanced Settings page appears:

Staging Disk Size (GB): By default, the Actifio Connector uses 1.2 times the size of the protected file system as the size of the staging disk. This setting allows the administrator to override this value if necessary, for example to allow for growth of the file system.

Staging Disk Granularity: If an application might require multiple staging disks, you can keep a small portion of an application from using a large staging disk. Enter the largest size of staging disks to be used.

Last Staging Disk Minimum Size: If an application might require multiple staging disks, enter the minimum size to be allocated for the staging disk used for the last part of that application.

Enter a **Staging Disk Mount Point** if you need the staging disk mounted to a particular location.

Provide the start path names in the **Start Path** field. Start-path specifies the directory where backup starts. If the start-path field is left blank, backup starts at the root directory of the file system to be backed-up. For example, a value of `\\SERVERNAME\SHARENAME\abc` will back up the `abc` directory on the file share when protecting applications on a Windows host. Click **Add** to define additional start paths.

Provide the prune paths in the **Prune Path(s)** field. Prune-path specifies a point in the file system where directory traversal will stop.

- o When protecting a Windows application, a value of `\\SERVERNAME\SHARENAME\abc` will ensure that nothing below `\\SERVERNAME\SHARENAME\abc` is copied, but all other directories and files in `\\<SERVERNAME\SHARENAME` are copied. If this field is left blank, the directory traversal descends into every subdirectory of the start paths being backed-up.
- o When protecting a Linux application, a value of `/opt/abc` will ensure that nothing below `/opt/abc` is copied, but all other directories and files in `/opt/` are copied. If this field is left blank, the directory traversal descends into every subdirectory of the start paths being backed-up.
- o Click **Add** to define additional prune paths.

Enter the file name pattern to be excluded from backup in the **Exclude Pattern(s)** field. You can exclude certain file types from the backup. Using this option, only the most crucial data is backed-up. Only files are excluded, directories are not excluded. Guidelines for exclude patterns:

- o A pattern can include wild-card characters, for example, an asterisk (*) or a question mark (?). To exclude all the files that contains `.sys` as extension, enter `*.sys` in the Exclude Pattern(s) field.
- o On Windows, `pagefile.sys` and `hiberfil.sys` in the root directory of a drive are automatically ignored.
- o Include one pattern in a field. Click **Add** to create as many fields as you need.

Choose **Do not Unmap** if you want temporary staging disks mapped to the host and used during data movement for backup to remain mapped to the host. LUNs are mapped during the first job and all the subsequent jobs reuse the same mapped LUN. By default, this option is selected.

Map staging disk to all ESX hosts in a cluster: If your ESX servers are in a cluster, you can select this to ensure that the VMs are protected in case of failover during backup.

Enter a **Service Access Point IP Address** to back up from a Windows cluster. Specify the IP address of the cluster node you want the file system to be backed up from. This option is not required for a failover cluster.

Leave **Connector Options** blank unless you are working with Actifio Support.

Check **Force Out of Band Backup** to force in-band backups in to an out-of-band mode.

Fail on Missing Start Path: Check this to force a job to fail if the Start Path entered above is not defined.

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

10 Protecting Mapped NFS File Systems

This procedure is for protecting mapped NFS file systems. To protect mapped CIFS file systems, see [Chapter 11, Protecting Mapped CIFS File Systems](#), and to protect local file systems see [Chapter 9, Protecting Local File Systems](#).

To protect a mapped NFS file system:

1. Open the Actifio Desktop to the **Application Manager**.
2. Select the NFS application from the navigation pane under **Local > NFS**.
3. Select the **Protect** tab.
4. Click the blue **Advanced Settings** link in the upper right corner. The Advanced Settings page appears. Fill in application advanced settings as needed for this file system. Application advanced settings are detailed in [Application Advanced Settings for NFS File Systems](#) on page 38.
5. Select an SLA template from the **Template** drop-down list. This is the template that defines the snapshot/deduplication/ replication of the application data.
6. Select a resource profile from **Profile** drop-down list. This defines the resources used to store the data of the application as snapshot/deduplicated/replicated images.
7. Click **Protect**. The application status becomes Protection-Initialization; it is not Protected until the scheduled job runs according to the hours of operations defined in the template. For example, today at noon you can assign a template that has hours of operation of 2:00am to 5:00am to an application and the first job will not start before 2:00am tomorrow. The first Snapshot or DirectDedup job should start when the Actifio appliance has its next available slot. Check the System Monitor to find the running job.
8. To run a job immediately, see [Running an On-Demand Backup](#) on page 30.

Note: A Warning screen appears if the selected SLA template policy will result in a potential impact to system resources based on the policy settings. See [Validating Projected Resources Prior to Applying Protection](#) on page 17 for additional details.



Protecting an NFS File System

Application Advanced Settings for NFS File Systems

To configure application advanced settings for mapped NFS file systems:

1. Open the Application Manager to the **Protect** tab.
2. Select **APP**. Under **Local > NFS**, select the file system.
3. Click the blue **Advanced Settings** link in the upper right corner. The Advanced Settings page appears.

In **Staging Disk Size**, enter a value in gigabytes. By default, the Actifio Connector uses the size of the protected file system as the size of the staging disk. This setting allows the administrator to override this value to allow for growth of the file system.

Staging Disk Granularity: If an application might require multiple staging disks, you can keep a small portion of an application from using a large staging disk. Enter the largest size of staging disks to be used.

Last Staging Disk Minimum Size: If an application might require multiple staging disks, enter the minimum size to be allocated for the staging disk used for the last part of that application.

Enter a **Staging Disk Mount Point** if you need the staging disk mounted to a particular location.

Provide the start paths in the **Start Path** field. Start-path specifies the point in the file system where backup starts. If the start-path field is left blank, backup starts at the root directory of the file system to be backed-up. For example, a value of `/usr/local` will back up the `/usr/local` directory when protecting applications on a Linux host. Click Add to define additional start paths.

Provide the prune paths in the **Prune Path(s)** field. Use the Add link to add a path. Prune-path specifies a point in the file system where directory traversal will stop. When protecting a Linux application, a value of `/usr/local/lib` will ensure that nothing below `/usr/local/lib` is copied, but all other directories and files in `/usr/local` are copied. If this field is left blank, every subdirectory of the start paths is backed up. Click Add to define additional prune paths

Enter the file name patterns to be excluded from backup in the **Exclude Pattern(s)** field. You can exclude certain file types from the backup. Using this option, only the most crucial data is backed-up leaving aside the non-critical files. Guidelines for exclude patterns:

- o Using this option, only files are excluded, directories are not excluded.
- o A pattern can include wild-card characters, for example, an asterisk (*) or a question mark (?). To exclude all the files that contains .sys as extension, enter *.sys in the Exclude Pattern(s) field.
- o On Windows, pagefile.sys and hiberfil.sys in the root directory of a drive are automatically ignored.
- o Include one pattern in a field. Click **Add** to create as many fields as you need.

Do Not Unmap: This maps temporary staging disks to the host to be used during data movement. LUNs are mapped during the first job, all subsequent jobs reuse the mapped LUN.

Map staging disk to all ESX hosts in a cluster: Select either **Do not map staging disk to all ESX hosts** or **Map staging disk to all ESX hosts**. In the event of an ESX host failure, mapping the staging disk to all ESX hosts in the cluster will protect failover copies of VMware VMs.

Leave **Connector Options** blank unless you are working with Actifio Support.

Fail on Missing Start Path: Check this if you want the job to fail if the Start Path entered above is not found.

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

11 Protecting Mapped CIFS File Systems

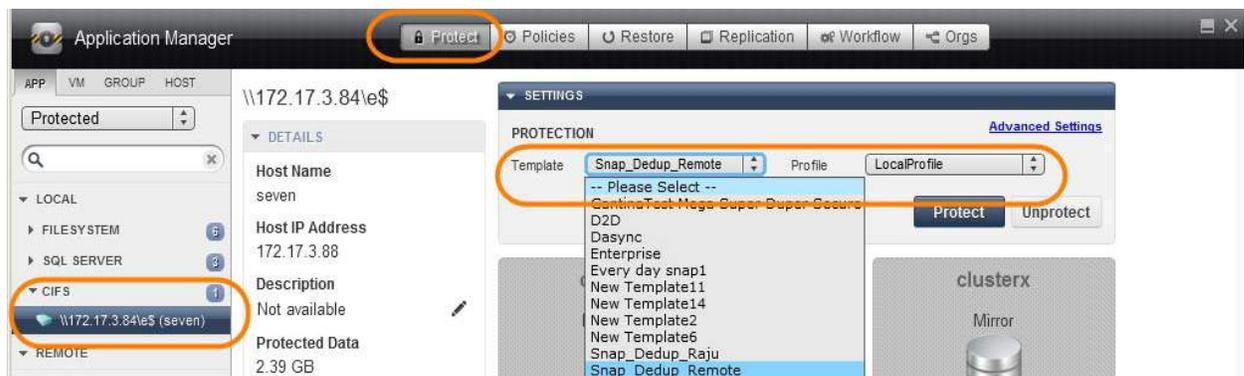
This procedure is for protecting mapped CIFS file systems. To protect mapped NFS file systems, see [Chapter 10, Protecting Mapped NFS File Systems](#), and to protect local file systems see [Chapter 9, Protecting Local File Systems](#).

This section describes how to protect applications on a CIFS host, including [Application Advanced Settings for Mapped CIFS File Systems](#) on page 40.

To protect a mapped CIFS file system:

1. Open the Actifio Desktop to the **Application Manager**.
2. Select the CIFS application from the navigation pane under **Local > CIFS**.
3. Select the **Protect** tab, then click the blue **Advanced Settings** link in the upper right corner. The Advanced Settings page appears. Fill in application advanced settings as needed for this file system. Application advanced settings are detailed in [Application Advanced Settings for Mapped CIFS File Systems](#) on page 40.
4. Select an SLA template from the **Template** drop-down list. This is the template that defines the snapshot/deduplication/replication of the application data.
5. Select a resource profile from **Profile** drop-down list. This defines the resources used to store the data of the application as snapshot/deduplicated/replicated images.
6. Click **Protect**. The application status becomes Protection-Initialization; it is not Protected until the scheduled job runs according to the hours of operations defined in the template. For example, today at noon you can assign a template that has hours of operation of 2:00am to 5:00am to an application and the first job will not start before 2:00am tomorrow. The first Snapshot or DirectDedup job should start when the Actifio appliance has its next available slot. Check the System Monitor to find the running job.
7. To run a job immediately, see [Running an On-Demand Backup](#) on page 30.

Note: A Warning screen appears if the selected SLA template policy will result in a potential impact to system resources based on the policy settings. See [Validating Projected Resources Prior to Applying Protection](#) on page 17 for additional details.



Protecting a CIFS File System

Application Advanced Settings for Mapped CIFS File Systems

There are application advanced settings that may be useful or required. Application advanced settings are reachable from the blue text link in the upper right corner of the Protect page.

To configure advanced protection settings for a CIFS Share:

1. Open the Application Manager to the **Protect** tab.
2. Select **APP**. Under **Local > CIFS**, select the CIFS share from the navigation pane.
3. Click the blue **Advanced Settings** link in the upper right corner. The Advanced Settings page appears.

Username/Password: If alternate credentials were specified when the network drive was mapped to the host, in the spaces provided, enter the CIFS share username/password.

Staging Disk Size (GB): This setting allows you to override the file system size automatically set by the Actifio Connector. Setting the size here allows you to account for file system growth.

Staging Disk Granularity: If an application might require multiple staging disks, you can keep a small portion of an application from using a large staging disk. Enter the largest size of staging disks to be used.

Last Staging Disk Minimum Size: If an application might require multiple staging disks, enter the minimum size to be allocated for the staging disk used for the last part of that application.

Enter a **Staging Disk Mount Point** if you need the staging disk mounted to a particular location.

Start Path: Start-path specifies the point in the CIFS share where backup starts. If the start-path field is left blank, backup starts at the root directory of the file system to be backed-up. For example, a value of `\\SERVERNAME\SHARENAME\abc` will back up the abc directory on the CIFS Share when protecting applications on a Windows host. Click **Add** to define additional start paths.

Prune Path(s): Prune-path specifies a point in the File System where directory traversal will stop. When protecting a Windows application, a value of `\\SERVERNAME\SHARENAME\abc` will ensure that nothing below `\\SERVERNAME\SHARENAME\abc` is copied, but all other directories and files in `\\<SERVERNAME\SHARENAME` are copied. If this field is left blank, the directory traversal descends into every subdirectory of the start paths being backed-up. Click **Add** to define additional prune paths

Exclude Pattern(s): The Actifio appliance allows you to exclude certain file types from a backup. Using this option, only the most crucial data is backed-up. Guidelines for exclude patterns:

- o Using this option, only files are excluded, directories are not excluded.
- o A pattern can include wild-card characters, for example, an asterisk (*) or a question mark (?). To exclude all the files that contains .sys as extension, enter *.sys in the Exclude Pattern(s) field.
- o On Windows, files named pagefile.sys and hiberfil.sys in the root directory of a drive are ignored.
- o Include one pattern in a field. Click **Add** to create as many fields as you need.

Do Not Unmap: When this is selected, temporary staging disks mapped to the host and used during data movement for backup remain mapped to the host. LUNs are mapped during the first job and all the subsequent jobs reuse the mapped LUN. By default, this option is selected.

Map staging disk to all ESX hosts in a cluster: Select either, **Do not map staging disk to all ESX hosts** or **Map staging disk to all ESX hosts**. In the event of an ESX host failure, mapping the staging disk to all ESX hosts in the cluster will protect failover copies of VMware VMs.

Leave **Connector Options** blank unless you are working with Actifio Support.

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

12 Protecting Exchange Databases

Actifio appliances support Microsoft® Exchange with snapshots of individual Exchange databases. You can protect both active and passive mailbox databases. For best results, install the Actifio Connector on all nodes that have data to be protected.

To protect Exchange databases, follow the procedure in [Protecting a Microsoft Exchange Database](#) on page 42.

There are application advanced settings that may be useful or required in some cases. Application advanced settings are reachable from the blue text link in the upper right corner of the Protect page; see [Application Advanced Settings for Microsoft Exchange Databases](#) on page 43.

Note: An Actifio appliance can truncate Exchange logs if the Actifio Connector is installed. Make sure to select "truncate logs" in the SLA template that you bind to the application.

Exchange DAG

In an Exchange DAG configuration, install the Actifio Connector with the change tracking driver (full installation) on all DAG nodes.

The Actifio appliance backs up the passive node unless you specify otherwise in the Advanced Settings; see [Application Advanced Settings for Microsoft Exchange Databases](#) on page 43. In the event of a node failure, the Actifio appliance selects another node to use for backup by comparing the latest production database with what is on the staging disk and only moving changed blocks.

Exchange VMs

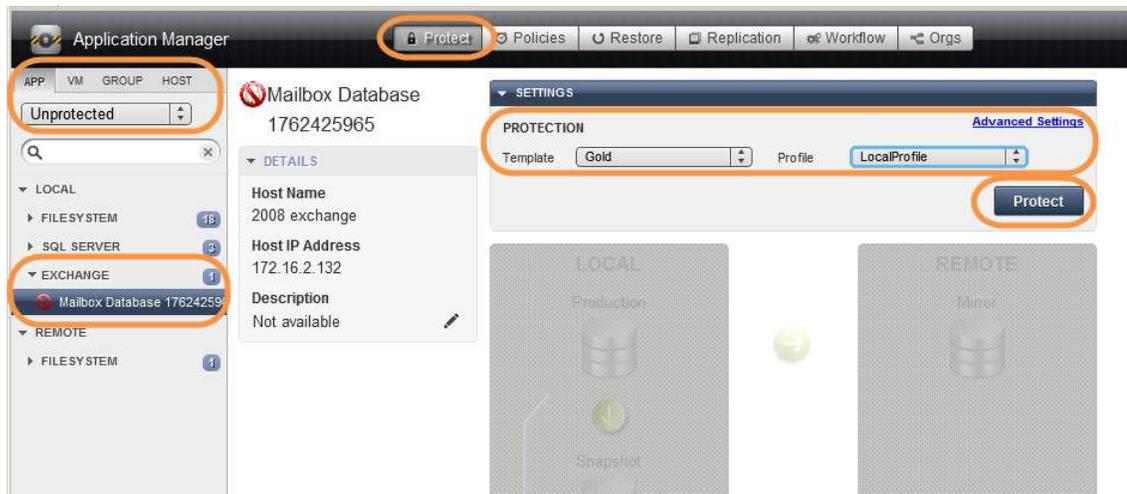
Snapshots of Exchange VMs are not supported by Microsoft, especially in a DAG configuration. VM snapshots can cause performance issues or DAG failovers. Restoring an entire Exchange VM over an existing Exchange VM is not supported by Microsoft. For best results, protect each Exchange database as an application. To do this, install the Actifio Connector on the VM.

Protecting a Microsoft Exchange Database

To protect a Microsoft Exchange database:

1. Open the **Application Manager** to the **Protect** tab.
2. From the navigation pane, select **APP**.
3. From the filter, select **Unprotected**.
4. On the navigation pane, select the Exchange database that you want to protect.
5. Click the blue **Advanced Settings** link in the upper right corner. The Advanced Settings page appears. Fill in advanced settings as needed for this database. Application advanced settings are detailed in [Application Advanced Settings for Microsoft Exchange Databases](#) on page 43.
6. Select an SLA template from the **Template** drop-down list. This is the template that defines the snapshot/deduplication/replication of the application data.
7. Select a resource profile from **Profile** drop-down list. This defines the resources used to store the data of the application as snapshot/deduplicated/replicated images.
8. Click **Protect**. The application status becomes Protection-Initialization; it is not Protected until the scheduled job runs according to the hours of operations defined in the template. For example, if at 10 AM you assign a template that has hours of operation from 2 AM to 5 AM, then the first job will not start until there is an available job slot after 2 AM tomorrow.
9. To run a job immediately, see [Running an On-Demand Backup](#) on page 30.

Note: A Warning screen appears if the selected SLA template policy will result in a potential impact to system resources based on the policy settings. See [Validating Projected Resources Prior to Applying Protection](#) on page 17 for additional details.



Protecting an Exchange Database

Application Advanced Settings for Microsoft Exchange Databases

To configure application advanced settings for an Exchange database:

1. Open the Application Manager to the **Protect** tab.
2. Select the **APP** list. Under **Local > Exchange**, select the Exchange database from the navigation pane.
3. Click the blue **Advanced Settings** link in the upper right corner. The Advanced Settings page appears.
 - o In the **Cluster Nodes** field, click Add and enter the IP addresses of the DAG nodes you want the Actifio appliance to use for backup. The Actifio appliance will try to connect to the nodes in the order they are listed. The first node that can be used for backup will be used by the Actifio appliance. If none of the nodes have a copy of the database that can be backed up, the backup job will fail. By default, one of the passive nodes that hold the database is used for backup.
 - o Select **Do Not Unmap** if you want temporary staging disks mapped to the host and used during data movement to remain mapped to the host. LUNs are mapped during the first job and all the subsequent jobs reuse the mapped LUN. By default, this is selected.
 - o Select whether you want to truncate logs after every backup. When this option is selected, Exchange logs are truncated to the current or most recent backup.
 - o Leave **Connector Options** blank unless you are working with Actifio Support.
4. Click **Save** to update the changes.

13 Protecting Generic Applications

Generic applications rely upon Actifio Optimized Storage and are available only on Actifio CDS appliances.

To protect an application:

1. Open the **Application Manager** to the **Protect** tab.
2. From the navigation pane, select **APP**.
3. From the filter, select **Unprotected**.
4. On the navigation pane, select the generic application that you want to protect.
5. Select an SLA template from the **Template** drop-down list. This is the template that defines the snapshot/deduplication/replication of the application data.
6. Select a resource profile from **Profile** drop-down list. This defines the resources used to store the data of the application as snapshot/deduplicated/replicated images.
7. Click **Protect**. The application status becomes Protection-Initialization; it is not Protected until the scheduled job runs according to the hours of operations defined in the template. For example, if at 10 am you assign a template that has hours of operation from 2 am to 5 am, then the first job will not start until there is an available job slot after 2 am tomorrow.

Note: A Warning screen appears if the selected SLA template policy will result in a potential impact to system resources based on the policy settings. See [Validating Projected Resources Prior to Applying Protection](#) on page 17 for additional details.

Application Advanced Settings for Generic Applications

There is only one advanced protection setting for a generic application: the **unmapping** option. Temporary staging disks are mapped to the host and used during data movement. Select whether you want them to remain mapped to the host. By default, LUNs are mapped during the first job and all the subsequent jobs reuse the same mapped LUN.

14 Protecting Groups

A **Group** is used for ease of management to apply a common policy to all the group's applications. Mount, clone, and restore operations are performed on the backup images of each application in the group individually.

Consistency Groups are collections of discovered applications from the same host. You create a consistency group to back up application data of all member applications together to preserve consistency of data across the member applications. You apply a common policy to the members of a consistency group. To protect a consistency group, see [Chapter 15, Protecting Consistency Groups](#).

Protecting a Group

To protect a group:

1. Open the **Application Manager** to the **Protect** tab.
2. From the navigation pane, select **GROUP**.
3. From the filter, select **Unprotected**.
4. On the navigation pane, select the Group that you want to protect.
5. Select an SLA template from the **Template** drop-down list. This is the template that defines the snapshot/deduplication/replication of the application data.
6. Select a resource profile from **Profile** drop-down list. This defines the resources used to store the data of the application as snapshot/deduplicated/replicated images.
7. Click **Protect**. The application status becomes Protection-Initialization; it is not Protected until the scheduled job runs and according to the hours of operations defined in the template. For example, if today at 10 am you assign a template that has hours of operation from 2 am to 5 am, then the first job will not start until the Actifio appliance has an available job slot after 2 am tomorrow.
8. To run a job immediately, see [Running an On-Demand Backup](#) on page 30.

Note: There are no application advanced settings for groups.



Protecting a Group

15 Protecting Consistency Groups

Consistency Groups are collections of discovered applications from the same host. You create a consistency group to back up application data of all member applications together to preserve consistency of data across the member applications. You apply a common policy to the members of a consistency group.

A **Group** is used for ease of management to apply a common policy to all the group's applications. Mount, clone, and restore operations are performed on the backup images of each application in the group individually. To protect a group, see [Chapter 14, Protecting Groups](#).

This section details:

[Protecting a Consistency Group](#) on page 50

[Application Advanced Settings for Consistency Groups](#) on page 51

Protecting Oracle Databases in a Consistency Group

A consistency group can contain only a single Oracle database and its associated files, so for database recovery, a consistency group offers little benefit for Oracle databases. A consistency group is a very good choice if you plan to access an Oracle database together with its binaries for test/dev and other business agility purposes.

Protecting Microsoft Exchange Databases in a Consistency Group

An entire Consistency Group is captured from a single host. A consistency group can contain multiple Exchange databases, but if they are in a DAG, then there is a possibility that one or more Exchange databases might be configured to failover to different locations. If this happens, then subsequent protection jobs will fail because the Actifio Connector will be unable to find all databases in the Consistency Group on the same host. Only include multiple Exchange DAG databases in a Consistency Group if you can configure them to all be present on a single host.

Protecting a Consistency Group

To protect a consistency group:

1. Open the **Application Manager** to the **Protect** tab.
2. From the filter, select **Unprotected**.
3. From the navigation pane, select **GROUP** and then select the Consistency Group that you want to protect.
4. If the Consistency Group includes databases, then right-click the Consistency Group and select **Set Application Type**. Select either Oracle Group or SQL Server Group and click **Submit**.
5. Click the blue **Advanced Settings** link in the upper right corner. The Advanced Settings page appears. Fill in advanced settings as needed for this database. Advanced settings are detailed in [Application Advanced Settings for Consistency Groups](#) on page 51.
6. Select an SLA template from the **Template** drop-down list. This is the template that defines the snapshot/deduplication/replication of the application data. Select a resource profile from **Profile** drop-down list. This defines the resources used to store the data of the application as snapshot/deduplicated/replicated images.
7. Click **Protect**. The application status becomes Protection-Initialization; it is not Protected until the scheduled job runs and according to the hours of operations defined in the template. For example, if today at 10 AM you assign a template that has hours of operation from 2 AM to 5 AM, then the first job will not start until the Actifio appliance has an available job slot after 2 AM tomorrow.
8. To run a job immediately, see [Running an On-Demand Backup](#) on page 30.



Protecting a Consistency Group

Application Advanced Settings for Consistency Groups

You can set a number of advanced settings for Consistency Groups, to define advanced settings for both a consistency group and for individual members of the group.

The Advanced Settings dialog contains all settings for all application types. For example, only Oracle databases use the advanced settings that refer to RMAN. The text below indicates which application types can use each setting.

To configure advanced protection settings:

1. Open the Application Manager to the **Protect** tab.
2. Click **Group > Consistency**.
3. Select the consistency group from the navigation pane.
4. Click the blue **Advanced Settings** link in the upper right corner. The Advanced Settings page appears.
 - o **Username/Password:** (SQL Server, CIFS)
SQL Server: User credentials for backing up the database transaction log. This account must have backup privileges. Credentials are required only if you select Backup Transaction Log or Truncate Log and if "Local System" does not have permissions to the SQL database.
CIFS: User credentials for authenticating to the CIFS share.
 - o **User Role in the Database:** Select Role sysdba or Role sysbackup. The Sysbackup role is for Oracle 12c only. (Oracle only)
 - o Enter the number of RMAN channels in the **Number of Channels** field. The default is 1, but you can change this; for more see [Chapter 16, Advanced Settings for Oracle Databases](#). (Oracle only) See also [Protecting Oracle Databases in a Consistency Group](#) on page 49.
 - o Enter the staging disk size in the **Staging Disk Size (GB)** field. The Actifio Connector calculates the maximum size of the application as configured. The Staging Disk Size option allows you to allocate a staging disk to hold backup and to allow future growth of the database. (Oracle, local file systems, CIFS, NFS, SQL Server, Exchange)
 - o **Staging Disk Granularity:** If an application might require multiple staging disks, you can keep a small portion of an application from using a large staging disk. Enter the largest size of staging disks to be used. (local file systems, CIFS, NFS, SQL Server, Exchange)
 - o **Last Staging Disk Minimum Size:** If an application might require multiple staging disks, enter the minimum size to be allocated for the staging disk used for the last part of that application. (Local file systems, CIFS, NFS, Oracle databases)
 - o Enter a **Staging Disk Mount Point** if you need the staging disk mounted to a particular location. (Oracle, local file systems, CIFS, NFS)
 - o If you are using an **Oracle named listener**, then enter the listener name in this field. (Oracle only)
 - o If you are using an **Oracle user role**, then enter the listener name in this field. (Oracle only)
 - o Enter the RMAN log path in the **RMAN Log Location** field. This is the custom location (full path along with RMAN filename) where RMAN writes the logs while taking the backup. (Oracle only)
For **Linux**, the default log location is: `/act/log/<sid>_rman.log`. If you change the path, the value must be in the form `/act/log/test/custom_rman.log`
For **Windows**, the default log location is `c:\act_tmp\log\<sid>_rman.log`. If you change the path, be sure there are no spaces in the path.
 - o Choose to validate each backup before restoring it. RMAN provides **Restore Validate** for the backups. When this option is checked the Actifio Connector invokes RMAN restore validate command for each backup. This is a resource-intensive operation. (Oracle only)

- o If you are using a catalog database for RMAN repository, enter these. By default, a control file is used. (Oracle only)
 - The Oracle catalog database SID name if one is used in the **Catalog DB Name** field.
 - The Oracle catalog database user name in the **Catalog User** field.
 - The Oracle catalog database login password in the **Catalog Password** field.
- o By default, Oracle backup skips inaccessible tablespace/datafiles. If you do not want to skip these, then select an option from **RMAN Backup Not Skip** drop-down field. (Oracle only)
- o Enter the Oracle database service name in **Oracle Servicename** field. This is optional for a standalone instance but required for a RAC setup. (Oracle only)
- o **Oracle Data Guard Primary Node Servicename:** This is the servicename configured on the Data Guard node that connects to the primary Actifio node. This is required only when you are protecting data from Oracle Data Guard.
- o **Cluster Nodes:** Specify a failover node choice in format **Failover choice:Node IP:service:role**. This is used for RAC only.
For example: **1:172.16.16.21:svc_orarac2_act:F**
role of member node by default should be **F** (failover). It can also be **M** (maintenance). When an appliance member role is specified as M, then The Actifio appliance uses it as the primary backup node instead of using the original protected node. (Oracle, Exchange)
- o Select a **Do Not Unmap** option depending on whether you want the temporary staging disks mapped to the host and used during data movement to remain mapped to the host. LUNs are mapped during the first job and all the subsequent jobs reuse the same mapped LUN. By default, this option is selected. (Oracle, local file systems, CIFS, NFS, SQL Server, Exchange)
- o Select whether you want to **Truncate Logs** after every backup. When this option is selected, transaction logs are truncated until the recent or current backup. If you truncate logs, you must also back up the transaction log (next step) to enable a roll forward recovery. (SQL Server, Exchange)
- o **Map staging disk to all ESX hosts in an appliance:** If your ESX servers are in an appliance, you can select this to ensure that the VMs are protected in case of failover during backup. (Oracle, local file systems, CIFS, NFS, SQL Server, Exchange)
- o **Backup transaction log:** Choose this if you want the Actifio Connector to back up the transaction log during a snapshot. This option saves transaction logs on the same drive as primary database file. Make sure there is enough space on the drive to accommodate transaction log backup. You use the transaction logs to roll forward the database after a restore. Be sure to back up transaction logs if you opted to truncate logs. (SQL Server only)
- o **Service Access Point IP Address:** Service Access Point is relevant only for SQL server availability groups. Enter a value here to back up from a SQL availability appliance. Specify the IP address of the appliance node you want the database to be backed up from. This option is not required if you want the database to be backed up from the active node and it is not required for a failover appliance. (SQL Server only)
- o Leave **Connector Options** blank unless you are working with Actifio Support.
- o **Force out-of-band backup:** This option is to force the out-of-band backup when database datafiles are in-band. This is used only for databases stored in-band on Actifio Integrated Storage from a CDS appliance.
- o **Enable Database Log Backup:** If this is checked, then log protection is enabled in the SLA.
- o **RPO (minutes):** Set an interval for log backup in minutes. This is used in conjunction with Enable Database Log Backup, above.
- o **Log Purging Retention Period:** In the space provided, enter the number of hours to retain archive logs in the primary log destination. For example, if this is set to 4, then archive logs older than four hours will be purged from the database primary archive destination.

- o **Log Staging Disk Size:** This applies when a log backup policy is set. By default Actifio will use the 30-day high-water mark to determine the staging disk size for archive backup staging disk. Information on determining this value is available in ***An Oracle DBA's Guide to Actifio Copy Data Management***.
- o **Do Not Uncatalog:** To keep RMAN backup cataloged after each backup job. By default, Actifio backup will be cataloged at the start of backup and then be un-cataloged at the end of the backup.
- o **Force New level 0 Backup:** If for any reason a full level 0 backup is required, overwriting the Actifio incremental backup, then select this option for a single backup job. **Be sure to uncheck it** after the full level 0 backup is complete. Not unchecking this option will force each subsequent backup to be a new level 0 Oracle RMAN out-of-band backup.

Performing a level 0 backup will have an impact on snapshot pool storage, with pool consumption likely to rise by the size of the database. For example, if the database is 8TB, then an additional 8TB of snapshot pool space will be consumed until released by snapshot expiration.

- o **Oracle Configuration File Location:** Use this if you are backing up any Oracle configuration files with an Oracle OOB backup such as wallet for encryption support. This requires a full path name. If the folder name is specified then all files under that folder will be backed up. If a file name is specified then only the specified file will be backed up.

For security reasons, keys are not backed up with the wallet.

- o **Oracle TNS_Admin Path:** If tnsnames.ora is in a nonstandard location, then provide the full path of the directory where it is located.
- o **ArchiveLog Backup Servicename:** Provide the dedicated Oracle database service name for the archive log backup.
- o **Use ASM Diskgroup for Backup:** Check this box to protect Oracle databases in an ASM disk group out-of-band configuration.
- o **Auto Discover RAC Members:** Check this checkbox to autodiscover all members of the RAC database databases in an ASM disk group out-of-band configuration. This enables mapping the staging disk to all nodes.
- o **RAC Member Nodes:** If you choose not to autodiscover RAC members, then provide a node list for mapping the staging disk as a shared volume for backup. Use this only for protecting Oracle databases in an ASM disk group.

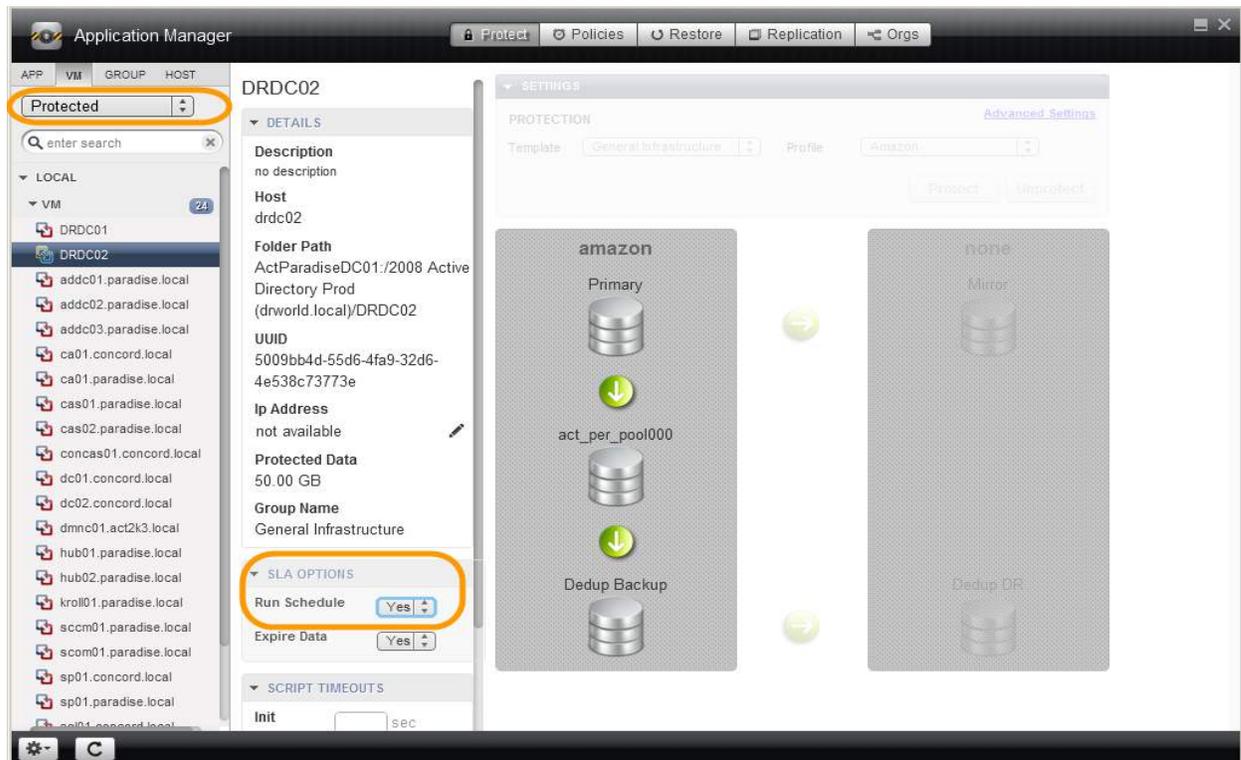
Auto-discovery will not work if the hostname does not have a fully qualified domain name. In that case add the nodes manually.

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

16 Suspending Protection

To temporarily pause the protection applied to an application:

1. Open the Application Manager to the **Protect** tab.
2. Click **Apps, VMs, Groups**, or **Hosts** as required. If the list is long, select **Protected** from the List Filter, or enter a search text to filter by name.
3. Select the application from the navigation pane.
4. Under **SLA Options** > **Run Schedule**, switch Yes to **No**.
5. Click **Yes** in the confirmation dialog.



Suspending Protection

Index

A

- Actifio Connector is not installed 2
- ad hoc backup 30
- application consistent backups 34
- applications
 - deleting 11
 - protecting 45

C

- CIFS Share 40
- clone
 - expiring 20
- consistency group
 - creating 21, 23, 24, 47, 49
 - deleting 11
- contact information, Actifio Support ii
- copyright ii

D

- data sensitivity 2
- Delete service menu item 2
- Discover App(s) service menu item 2
- Discover VM(s) service menu item 2
- discovering
 - applications 5, 9
 - VMs 7

E

- ESX server 7
- exclude certain file types from backup 38
- exclude patterns 36, 38, 40
- Expire All Backups service menu item 2

G

- generic applications
 - creating 10
- group
 - creating 22
 - deleting 11, 22

H

- hiberfil.sys, excluding from a backup 36, 38, 40

L

- legal matter ii
- LiveClone
 - expiring 20
- log replication, on-demand 31
- logs, truncating 34, 43, 52

M

- Manage VDisk(s) service menu item 2
- Mark Ignored service menu item 2
- Modify Expiration service menu item 2
- Modify Sensitivity service menu item 2
- multiple start paths 36, 38, 40

N

- New Application service menu item 2
- New Consistency Grp service menu item 2
- New Group service menu item 2

O

- on-demand
 - backups 30
 - log replication 31
- orphans 11, 22, 25
- out-of-band file systems 38

P

- pagefile.sys, excluding from a backup 36, 38, 40
- pausing protection 55
- protecting several applications with a single policy 2
- protection, suspending 55
- prune paths 36, 38

R

- resource-intensive jobs 28
- RMAN channels 51

S

- SCVMM/Hyper-V Server, discovering 7
- Set Application Type service menu item 2
- Show Jobs service menu item 2
- SLA Violation 28
- snapshot
 - expiring 20

- SQL availability cluster 52
- SQL database backup path 34
- staging disk 36, 38
- stale images 11, 22, 25
- start paths 36, 38
- suspending protection 55
- syncback
 - expiring image 20

T

- trademarks ii
- truncating logs after backup 34, 43, 52

V

- vCenter/ESX Host, discovering 7
- VM
 - deleting 11
 - discovering 7

W

- warranty ii
- wild-card characters in exclusion patterns 36, 40