
Configuring Resources and Settings With the Domain Manager

Copyright, Trademarks, and other Legal Matter

© 2015 Actifio, Inc. All rights reserved.

Actifio® is a registered trademark of Actifio, Inc. AnyIT™, Dedup Async™, Manage Data Simply™, Virtual Data Pipeline™, VDP™, Protection and Availability Storage Platform™, PAS™, Copy Data Storage Platform™, CDS™, Actifio Sky™ and Actifio One™ 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 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.

Rev. Actifio Enterprise 612

Contents

Preface	ix
Actifio Appliances	ix
The Actifio Now Customer Portal	ix
Actifio Support Centers	ix
Chapter 1 - Introduction to the System Functions of the Domain Manager	1
Functions of the Domain Manager System Service	2
The Domain Manager Service Menu	3
Chapter 2 - Monitoring Resource Usage	5
Viewing the Resources Summary	6
Viewing and Managing VDisk Usage	7
Reducing VDisk Consumption	8
Viewing and Managing Snapshot Memory Usage	9
Reducing Snapshot Pool Consumption	10
Viewing and Managing Replication Memory Usage	11
Viewing and Managing the Top 10 SLA Policy Templates	12
Viewing and Managing Mirror Memory Usage	13
Chapter 3 - Understanding In-Band and Out-of-Band Data Storage	15
The Actifio Connector	16
In-Band Data	17
Protecting Physical Hosts In-Band	17
Protecting Entire VMs In-Band	18
Out-of-Band Data	19
Protecting Physical Hosts Out-of-Band	19
Protecting Entire VMware and Hyper-V VMs Out-of-Band	20
Protecting Individual Applications on a VMware or Hyper-V VM Out-of-Band	20
Chapter 4 - Configuring Storage Pools	21
About Storage Pools	22
VDisks and VDisk Consumption	23
How Many VDisks Do I Need?	23
Snapshot Pools	24
Configuring the Alert Levels for Storage Pools and Resource Profiles	25

Creating, Modifying, and Deleting Storage Pools	26
Viewing Storage Pool Information	26
Creating Additional Snapshot Pools	27
Modifying Storage Pools.....	29
Deleting Snapshot Pools	30
Chapter 5 - Understanding Dedup Pools	31
Reducing Dedup Pool Consumption.....	31
Monitoring Dedup Pool Space Consumption	32
Actifio Appliance Reports Related to Dedup Pool Management	32
Chapter 6 - Configuring Dedup Garbage Collection	33
Configuring a GC Schedule	35
Chapter 7 - Managing Appliances	37
Viewing and Removing Certificates.....	38
Viewing Certificates	38
Removing a Certificate	38
Managing Bandwidth Utilization	39
Enabling and Disabling Bandwidth Throttling	40
Overriding Bandwidth Throttling	41
Scheduling Bandwidth Throttling.....	42
Enabling/Disabling Sync/Async Replication	43
Selecting a Storage Pool for Replicated Data	44
Viewing Bandwidth Usage Statistics.....	45
Chapter 8 - Configuring Appliance Settings	47
Managing Security Certificates	48
Viewing Certificates.....	48
Deleting a Certificate	48
Downloading a Certificate.....	49
Uploading a Certificate.....	49
Exchanging Certificates.....	50
Configuring LDAP Settings.....	51
Mapping LDAP Groups to Roles.....	52
Configuring Control Panel Operations	53
Shutting Down the Appliance.....	54
Disabling Expirations and Schedules.....	55
Enabling Remote Problem Resolution	56
Setting Priorities for Ingestion of New Applications	57

Chapter 9 - Sharing Between Actifio Appliances	59
Appliance Topology: Sharing and Peer Relationships.....	59
Sharing Mode.....	60
Non-Sharing Mode	61
Chapter 10 - Configuring Shared Appliances	63
Viewing Details of Joined Appliances	64
Unjoining Appliances	64
Joining in Sharing Mode	65
Joining in Non-Sharing Mode	66
Chapter 11 - Maintaining Connectors on Hosts	67
Using the Connector Manager	68
Chapter 12 - Overview of Configuration Tools	69
Resources	70
Storage Pools.....	71
Dedup Settings	72
Appliance Settings.....	73
Connector Management	74
License Management	75
Notification.....	76
Logs	77
Chapter 13 - Managing Licenses for a Sky Appliance	79
Ordering a License	79
Uploading a License Key.....	80
Copying the System UUID Value.....	83
Chapter 14 - Alerting	85
Monitoring Alerts in the Actifio Desktop System Monitor	86
Chapter 15 - Collecting Alerts from Actifio Storage and Switches	87
Polling Alerts from Actifio Optimized Storage and Switches	88
Forwarding Alerts from Fibre Channel Switches to the Actifio CDS Appliance	89
Chapter 16 - Sending Alerts from the Actifio Appliance	91
Sending Alerts to an SNMP Trap Receiver	92
Setting the Community String for Forwarding Traps to a non-Actifio SNMP Trap Receiver.....	92
Accessing the Actifio MIB.....	93
Sending Alerts via Email	94
Communicating with an SMTP Server	95
Setting Up Automatic Email Notifications	96
Sending Alerts to Actifio Support	97

Chapter 17 - Sending Logs to Actifio Support	99
Chapter 18 - Managing Hosts	101
Details Tab.....	102
Ports Tab.....	103
Storage Tab.....	104
Applications Tab.....	105
Orgs Tab	106
Chapter 19 - Configuring Storage for In-Band Hosts	107
Creating a VDisk	108
Creating an Image Mode VDisk	109
Creating a Mirror Mode VDisk	110
Mapping a VDisk to a Host	111
Unmapping a VDisk from a Host	112
Expanding a Virtual Disk.....	113
Renaming VDisks and MDisks.....	114
Deleting a Virtual Disk.....	115
Chapter 20 - Configuring a BDD Node	117
Viewing and Modifying the Details of a BDD Node Configuration	118
Setting the Port 3 or Port 4 IP Address	119
Joining a BDD Node to a Windows Domain	119
Configuring the Ports of a BDD Node.....	120
Viewing the Storage on a BDD Node	121
Viewing the Organizations to which a BDD Node Belongs	121
Chapter 21 - Adding NAS Servers	123
Adding a NAS Server.....	124
Viewing and Modifying NAS Server Details	126
Viewing Datasets on a NAS Server	127
Viewing the Organizations to which a NAS Server Belongs	128
Chapter 22 - Adding Hosts and Editing Host Information	129
Adding a Generic, HP-UX, TPGS, or OpenVMS Host	130
Adding a Hypervisor Host	134
Adding an IBM HMC Host.....	136
Configuring the Ports of a Host.....	138
Viewing Applications on a Host.....	139
Viewing and Editing Host Information	140

Chapter 23 - Unmounting Active Images141

 Unmounting an Image 142

 Deleting an Unmounted Image 142

 Unmounting and Deleting an Active Image..... 143

 Unmount & Accept Changes or Reject Changes to Prep-Mounted LiveClones 144

Chapter 24 - Using Diagnostics145

 Charts..... 145

 SSD Status Monitoring 146

Index 147

Preface

This guide provides step-by-step instructions on how to configure resources and settings with the Actifio Domain Manager. 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.

Your Actifio appliance's Documentation Library contains detailed, step-by-step, application-specific instructions on how to protect and access your data. Each guide is in PDF format and can be viewed, downloaded, and printed on demand. The following guides will be of particular interest:

- ***Setting Up Users and Roles With the Domain Manager***
- ***Planning and Developing Service Level Agreements***
- ***Virtualizing and Protecting Copy Data with the Application Manager***
- ***Accessing and Recovering Copy Data with the Application Manager***
- ***Restoring Copy Data with the Application Manager***

Actifio Appliances

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

The Actifio Now Customer Portal

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

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

To log into the Actifio Now customer portal:

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

Actifio Support Centers

To contact an Actifio support representative, you can:

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

1 Introduction to the System Functions of the Domain Manager

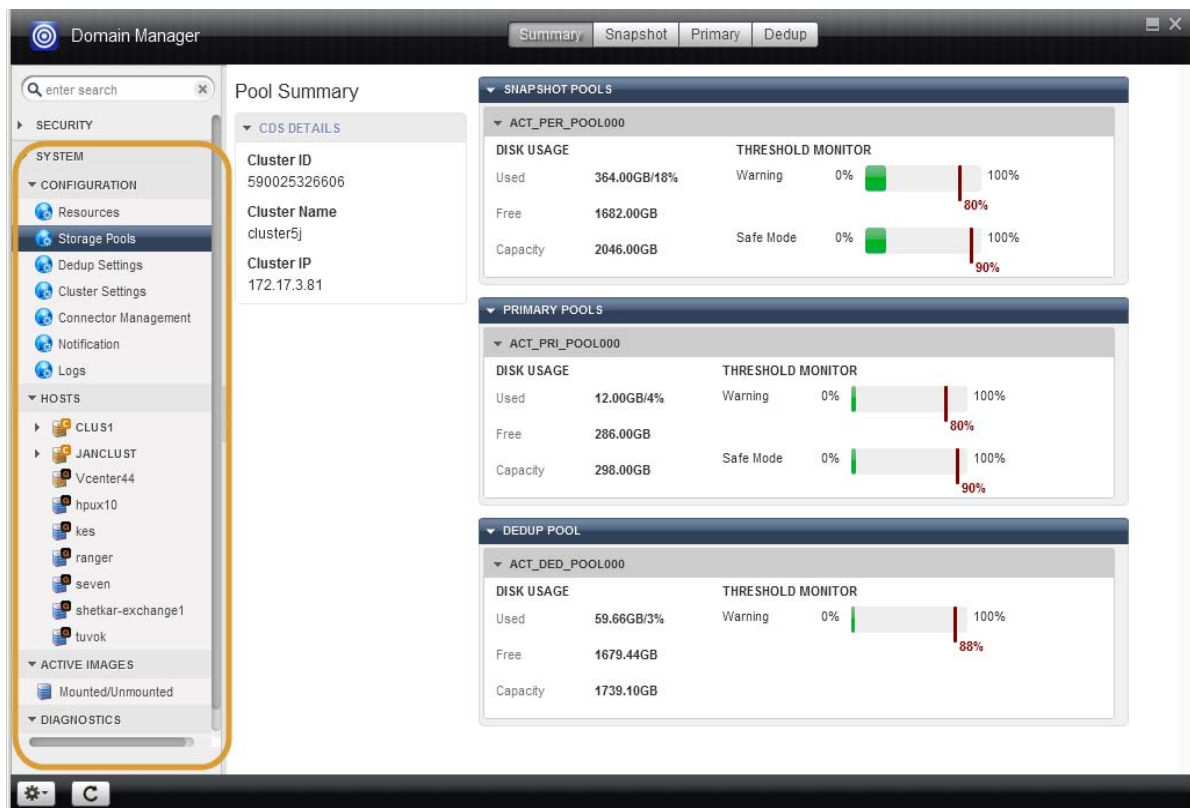
Note: References in this document to the Actifio appliance apply to all Actifio appliance types. Information that pertains only to a specific appliance is clearly called out when the information is presented.

The Actifio Desktop Domain Manager service is your primary tool for configuring and managing relationships among all resources protected by an Actifio appliance. The **System** function is where you configure the hosts and appliances on which copy data resides. These functions are detailed in the following chapters.

This introduction describes:

[Functions of the Domain Manager System Service](#) on page 2

[The Domain Manager Service Menu](#) on page 3



The System Functions of the Actifio Desktop Domain Manager

The Domain Manager also includes a Security section, used for configuring users, roles, and organizations. These functions are detailed in ***Setting Up Users and Roles with the Domain Manager***.

Functions of the Domain Manager System Service

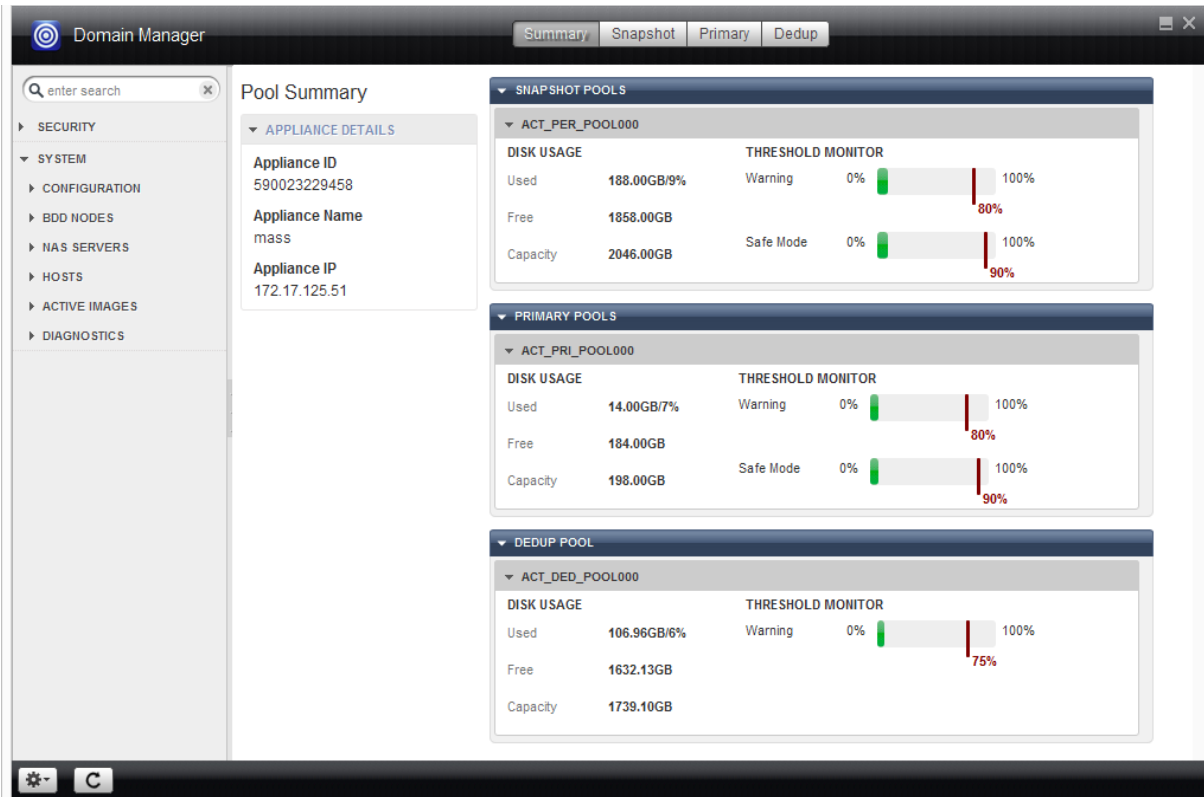
The System function of the Domain Manager provides these tools:

Configuration: a suite of tools for configuring and monitoring your Actifio appliance resources. This suite of tools is introduced in [Chapter 12, Overview of Configuration Tools](#) and detailed in subsequent chapters.

Hosts: for configuring and managing hosts protected by an Actifio appliance. Tools for host management are described in [Chapter 18, Managing Hosts](#).

Active Images: for managing backup images that have been mounted to hosts. The Active Images tools are described in [Chapter 23, Unmounting Active Images](#).

Diagnostics: are described in [Chapter 24, Using Diagnostics](#).



The Four Functions of the Domain Manager's System Section

The Domain Manager Service Menu

The Domain Manager's service menu includes functions for both the Security function and the System function:

Domain Manager Service Menu Items

Command Name	Task
New Organization...	Create a new organization and assign resources. (Security service)
New User...	Create a new user and assign roles to the user. (Security service)
New Role...	Create a new role. (Security service)
New Host...	Configure a new host. (System service)
Add New NAS Server	Add a NAS Server to an Actifio appliance and specify its ports and virtual disks (System service)
Join Appliance	Join the Actifio appliance to another Actifio appliance or where applicable, to the Actifio Business Resiliency Cloud. Once joined, configurations can be shared and data can be replicated between the joined entities. Before joining, a certificate exchange is required. (System service)
Certificate Exchange	Exchange security certificates between two Actifio appliances or where applicable, to the Actifio Business Resiliency Cloud. (System service)
Upload Certificate...	Upload the security certificate from the local appliance to a remote Actifio appliance or where applicable, to the Actifio Business Resiliency Cloud. (System service)
Download Certificate...	Download the security certificate from a remote Actifio appliance or where applicable, from the Actifio Business Resiliency Cloud. (System service)
Archive Job History...	Archive jobs executed using Actifio Desktop. (System service)
Add CLI Access	Add an SSH public key to enable CLI access for a user. (Security service)
Remove CLI Access	Disable CLI access to a user. (Security service)
Upload System Update	Upload patches and hotfixes to Actifio appliance. This is visible only to the admin role. (System service)
Delete	Delete a user, role, org, or host. (System service)

2 Monitoring Resource Usage

Resource usage includes:

[Viewing the Resources Summary on page 6](#)

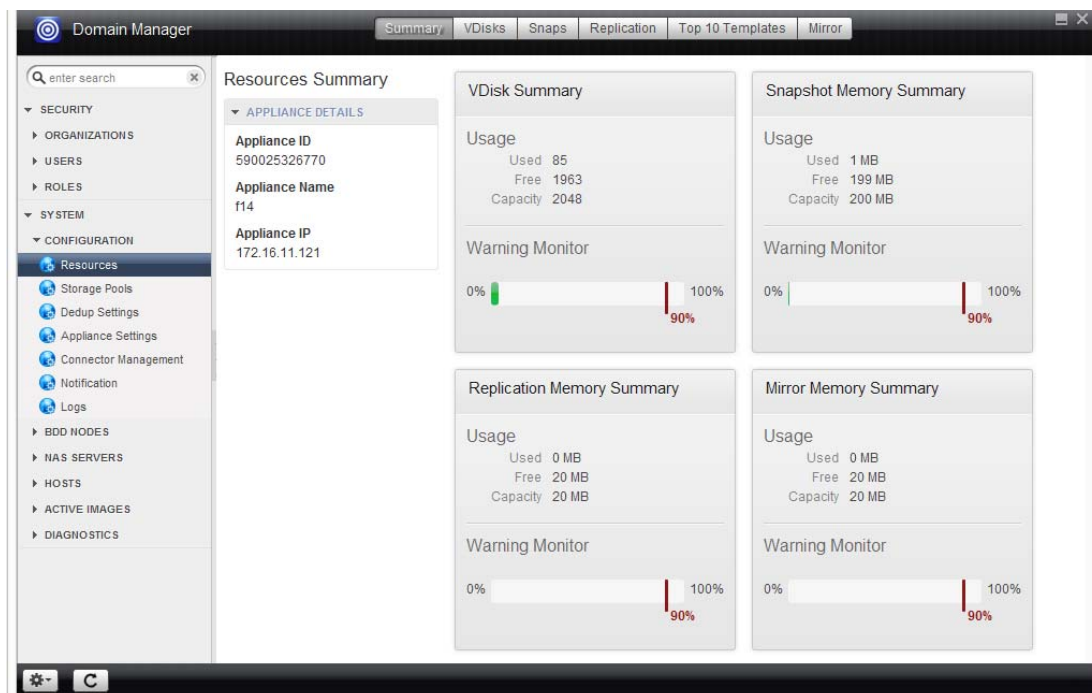
[Viewing and Managing VDisk Usage on page 7](#)

[Viewing and Managing Snapshot Memory Usage on page 9](#)

[Viewing and Managing Replication Memory Usage on page 11](#)

[Viewing and Managing the Top 10 SLA Policy Templates on page 12](#)

[Viewing and Managing Mirror Memory Usage on page 13](#)



The System/Resources Sections of the Domain Manager Service

Viewing the Resources Summary

The Resources Summary provides an at-a-glance view of the status of your Actifio appliance.

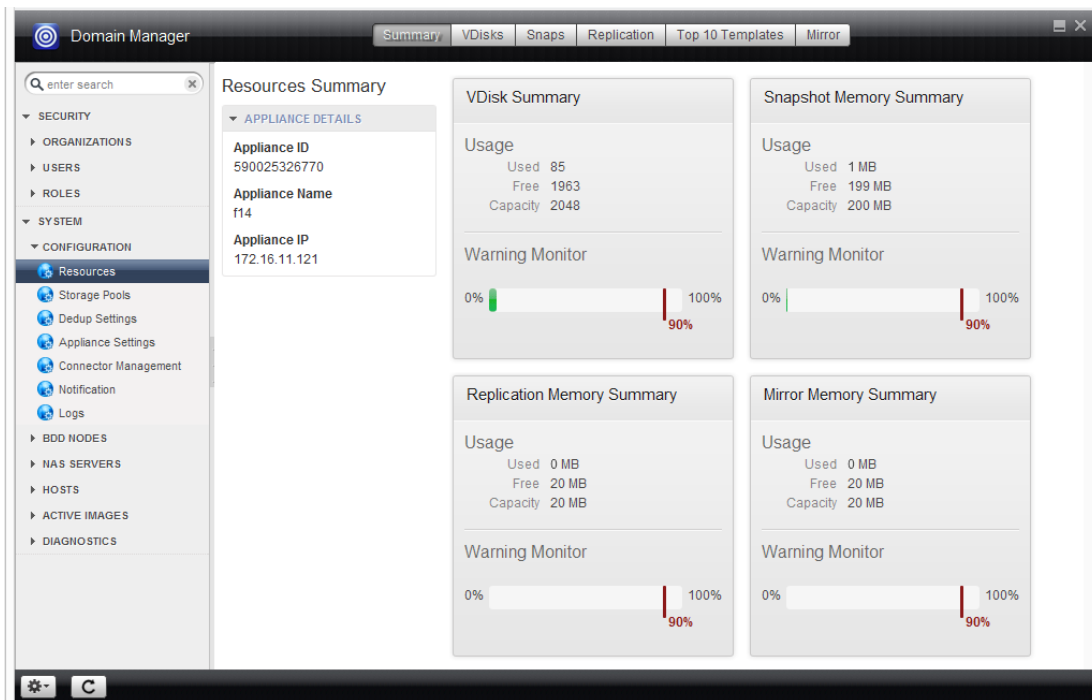
To configure resource limits and warning thresholds, you must access the specific tools:

[Viewing and Managing VDisk Usage](#) on page 7

[Viewing and Managing Snapshot Memory Usage](#) on page 9

[Viewing and Managing Replication Memory Usage](#) on page 11

[Viewing and Managing the Top 10 SLA Policy Templates](#) on page 12



The Domain Manager System Configuration Resources Summary

When usage of any of these resources reaches or exceeds the warning threshold, the Actifio appliance performance can suffer. Call Actifio Support for guidance and solutions.

Viewing and Managing VDisk Usage

For details on VDisks, see: [VDisks and VDisk Consumption](#) on page 23.

A VDisk (volume) is a virtual disk on an Actifio appliance presented to a host as a unit of usable storage capacity. You use VDisks for each LUN, VMDK, VHD, database, or filesystem protected (unless protected direct-to-dedup), each volume comprising a snapshot of an application, and each LUN comprising a mount or clone of an application.

To monitor the number of virtual disks:

1. Open the **Domain Manager** to **System > Configuration > Resources**.
2. Select the **VDisks** tab.

Under VDisk Usage you see the number of VDisks in use and available. You can have a maximum of 2048 VDisks on an Actifio appliance.

Top 10 VDisks List

The Top Ten VDisks list shows the ten applications that have the maximum number of virtual disk copies. These are usually snapshots or mounts/clones.

Changing the Warning Threshold for VDisks

If the number of virtual disks created on an Actifio appliance exceeds the warning threshold, warnings are sent to the email recipients configured in [Sending Alerts via Email](#) on page 94.

The default warning threshold for VDisks usage is 90%. To change the warning value, drag the threshold value to the desired value and click Save.

Note: Do not change the warning threshold simply because your data exceeds the threshold. Change the warning threshold only if your usage requirements justify a different value. Actifio Support can help.

VDISK	APPLICATION	COPIES
vdisk_dnt_delete Host: undefined	undefined	9
vdisk_oobjyothi Host: amanwin10153930	syamala	9
vm-5433C1573C00 Host: linux vm	/	7
vm-5406A4DF0900 Host: undefined	undefined	6
vm-5423E6B60100 Host: undefined	undefined	3
vm-5423E6B61B00 Host: undefined	undefined	3
vm-5423E6B63200 Host: undefined	undefined	3
vm-5423E6B64A00 Host: undefined	undefined	3
vm-5433AA0B5C00 Host: windows vm	C:\	3

Viewing VDisk Usage

Reducing VDisk Consumption

The following changes have an immediate affect on VDisk consumption:

- Move VMware VMs from a snapshot SLA to a Direct-to-Dedup SLA. You will need to expire all snaps to release the VDisks used by the staging disks and last snap. This action only works for VMware VMs, as other application types, including Hyper-V VMs still use some VDisks when protected by a direct-to-dedup policy.
- Change VMware VMDKs that do not need to be protected to Independent mode as these cannot be protected by VMware snapshots.
- Group databases from a single host together into a consistency group. For example, if a single host has 9 SQL databases, create one Consistency Group for that host and include all 9 databases, then protect that group rather than the individual databases. In this example, VDisk consumption is reduced from 9 to 1.
- Reduce the number of snapshots kept for an application by changing the policy template used by an SLA. This action does not necessarily lead to a different RPO, as deduplicated images of each snap can be created before they are expired.
- Delete unneeded mounts, clones, and live-clones

Actifio Appliance Reports Related to VDisks

The Actifio Report Manager includes several useful reports in the Utilization category:

- Application Contribution to Cumulative V-Disk Usage
- Application Contribution to Daily Storage Pool and V-Disk Usage
- Bandwidth Utilization History
- Daily Storage Pool and V-Disk Usage Trend by Appliance

Viewing and Managing Snapshot Memory Usage

A snapshot is the state of a system at a particular point in time. Snapshot memory is memory pre-allocated for tracking differences between on-disk data in snapshots.

To view the usage of the snapshot memory:

1. Open the **Domain Manager** to **System > Configuration > Resources**.
2. Select the **Snaps** tab.

Under Snapshot Memory you see the amount of memory taken by snapshots and how much is still available.

Snapshot Pool Exhaustion

When the safe level has been exceeded, no new snapshots or dedup async jobs can be run. Normal expiration should free up snapshot pool space progressively over time. This process can be accelerated by manually expiring snapshots. Contact Actifio support if the pool has reached 100% as snapshot could have been damaged (since Actifio appliance will have nowhere to destage the changed data to).

If Snapshot Memory Usage is Too High

When Snapshot Memory usage increases to and then exceeds the warning threshold, Actifio appliance performance can suffer. Solutions include:

- Review your SLAs and see if you can reduce the number of snapshots you are taking.
- Increase snapshot memory. It can be increased up to 512MB, if you're not doing any local or remote mirroring.

Changing the Warning Threshold

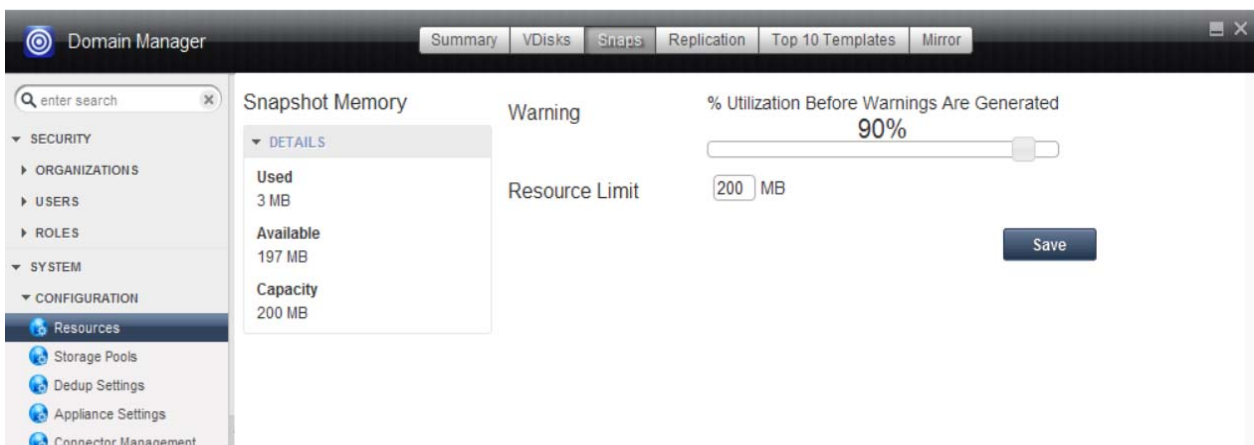
The default threshold for snapshot memory usage is 90%. To change the warning value, move the slider.

Note: Do not use this feature without the direction of Actifio Support.

Changing the Resource Limit

The default snapshot memory capacity is 100 MB. You can change this value if you need more snapshot memory (see [Chapter 4, Configuring Storage Pools](#)).

Each snapshot, mount, or clone uses around a kilobyte of memory per gigabyte size of the target volume. With 100MB snapshot memory you can have about 100TB of snapshots. If you are protecting many large volumes and keeping multiple generations of snapshots, increase your snapshot memory.



Viewing Snapshot Memory Usage

Reducing Snapshot Pool Consumption

To reduce consumption of the snapshot pool:

- Move VMware VMs from a snapshot SLA to a Direct2Dedup SLA. You will need to expire all snapshots to release the space used by the staging disks and last snap. This action only works for VMware VMs as other application types still use some snapshot pool space if protected by a direct2dedup policy.
- Reduce the number of snaps being kept for an application. This reduction is achieved by changing the policy template being used by an SLA. Applications that have high change rates will clearly create larger snaps, so this action will have the highest benefit for high change rate applications. This does not necessarily lead to a different RPO, as deduplicated images of each snap can be created before they are expired.
- Delete mounts, clones, and live-clones if they are not needed
- Change applications from Out-of-Band to In-Band

Actifio Appliance Reports Related to Snapshot Pool Management

The Actifio Report Manager includes several useful reports relating to snapshot pool consumption:

- Application Contribution to Daily Snapshot Pool
- Application Contribution to Daily Storage Pool and V-Disk Usage
- Daily Snapshot Pool Utilization Summary
- Daily Storage Pool and V-Disk Usage Trend by Appliance
- Disk Pool Utilization History
- Snapshot Pool Utilization History by Application
- Storage Pool Usage by Organization
- Storage Resource Usage Summary

Reports are detailed in ***Using the Report Manager*** in the Documentation Library.

Viewing and Managing Replication Memory Usage

Replication memory buffers changes that are being written to a remote appliance using Sync or Async replication.

To view the usage of the replication memory:

1. Open the **Domain Manager** to **System > Configuration > Resources**.
2. Select the **Replication** tab.

Under Replication Memory you see the amount of memory already taken by replication and how much remains available.

If Replication Memory Usage is Too High

When replication memory usage increases to and then exceeds the warning threshold, Actifio appliance performance can suffer. Solutions include:

- See if the latency or bandwidth of your Fibre Channel network is a bottleneck.
- increase memory pre-allocated for replication. The sum of replication + mirror + snapshot memory can be increased to a combined maximum of 512MB.

Changing the Warning Threshold

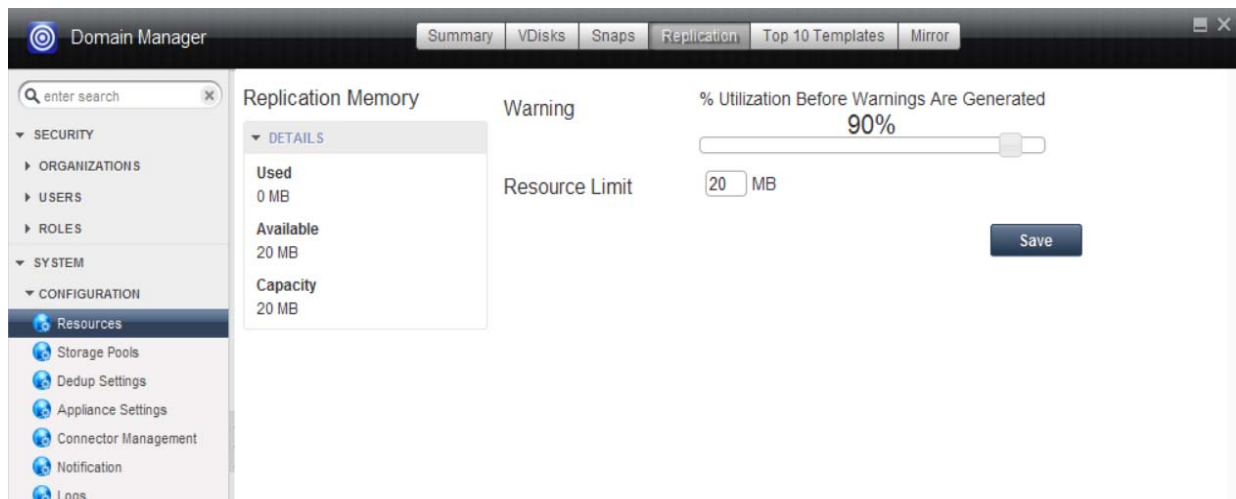
The default threshold for replication memory usage is 90%. To change the warning value, change the default warning threshold value.

Note: Do not change the warning threshold simply because your data exceeds the threshold. Change the warning threshold only if your usage requirements justify a different value. Actifio Support can help.

Changing the Resource Limit

The default replication memory capacity is 70 MB. Change this limit only with the assistance of Actifio Support.

If required, increase or decrease the Resource Limit and click **Save**.



Viewing Replication Memory Usage

Viewing and Managing the Top 10 SLA Policy Templates

For each Service Level Agreement (SLA), the top resources consumed by applications and VMs protected by the SLA policy templates appear in the **System > Configuration > Resources** section of the Domain Manager, in the Top 10 Templates tab. Policy templates are the rules that you create for the Actifio appliance to determine what type of protection to apply to your copy data, when to apply it, and where to store it. Each template policy defines how your applications and VMs are managed by the Actifio appliance. SLA operations have the potential of impacting the performance of the Actifio appliance by running out of critical resources as a result of a template policy.

To view the top 10 SLA policy templates:

1. Open the **Domain Manager** to **System > Configuration > Resources**.
2. Select the **Top 10 Templates** tab.

Resource consumption information includes:

- Top 10 VDisk-consuming applications (with total number of VDIs used)
- Top 10 snapshot pool space usage applications (including total amount of storage used)

If you double-click a row in either the VDisk Usage or Snapshot Pool Usage table, this action brings you to the associated policy template in the SLA Architect.

For details on modifying a policy template to take into consideration how the frequency and retention settings for the various police templates can reduce VDisk and snapshot pool usage, see the **Planning and Developing Service Level Agreements** book in the Actifio Documentation Library.

Domain Manager | Summary | VDIs | Snaps | Replication | **Top 10 Templates** | Mirror

enter search

Top 10 Templates

APPLIANCE DETAILS

Appliance ID
590021132422

Appliance Name
galactica

Appliance IP
172.16.8.11

VDisks Usage

Policy Template	VDisks
ESX10	20
FS9	18
ESX9	18
FS8	16
ESX8	16
FS7	14
ESX7	14
FS6	13
ESX6	12
ESX5	10

*Double click on selected row to see the policy template details.

Snapshot Pool Usage

Policy Template	Snapshot Pool
FS9	75 GB
FS6	74 GB
FS8	63 GB
FS7	56 GB
FS5	36 GB
FS4	23 GB
FS3	22 GB
ESX10	12 GB
ESX9	11 GB

Verifying Resources for SLA Templates

Viewing and Managing Mirror Memory Usage

When an Actifio appliance is protecting an in-band volume, it has the ability to create two identical copies of that volume that it keeps in sync. This function can be used to provide high availability or to facilitate migration of the volume from one storage controller to another. the Actifio appliance uses a memory bitmap to ensure that each copy of the volume is kept in sync.

To view the usage of the mirror memory:

1. Open the **Domain Manager** to **System > Configuration > Resources**.
2. Select the **Mirror** tab. Under Mirror Memory you see the amount of memory already taken by mirroring and how much remains available.

If Mirror Memory Usage is Too High

When Mirror Memory usage increases to and then exceeds the warning threshold, Actifio appliance performance can suffer. Solutions include:

- Removing volume mirrors
- Increasing the size of the memory limit.

Changing the Warning Threshold

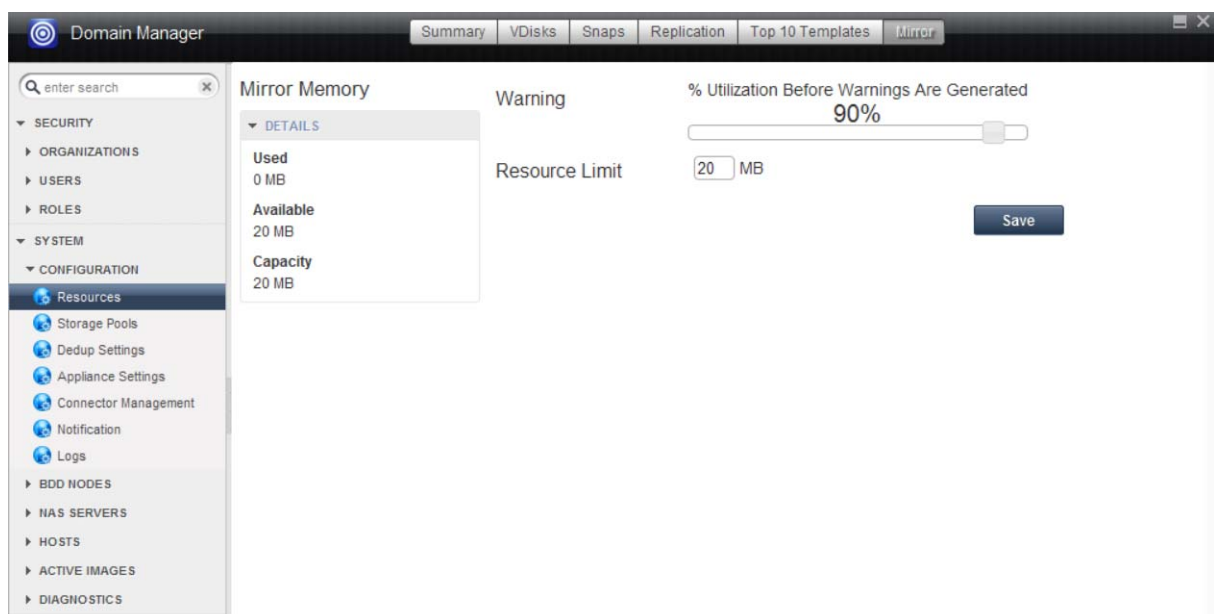
The default threshold for mirror memory usage is 90%. To change the warning value, change the default warning threshold value.

Note: Do not change the warning threshold simply because your data exceeds the threshold. Change the warning threshold only if your usage requirements justify a different value. Actifio Support can help.

Changing the Resource Limit

The default mirror memory capacity is 70 MB, which supports 140TB of mirrored volumes.

Change this setting only with the assistance of Actifio Support. If required, increase or decrease the Resource Limit and click **Save**.



Viewing Mirror Memory Usage

3 Understanding In-Band and Out-of-Band Data Storage

In Actifio terms, production data is the data of your running applications and VMs, and copy data is all the backed-up data. In an Actifio appliance environment, your copy data is virtualized and managed in ways that greatly reduce storage requirements and increase the ease and reliability of recovery.

To store your copy data, an Actifio appliance must first capture it, and the incremental changes that occur to it per the SLAs assigned to each application or VM.

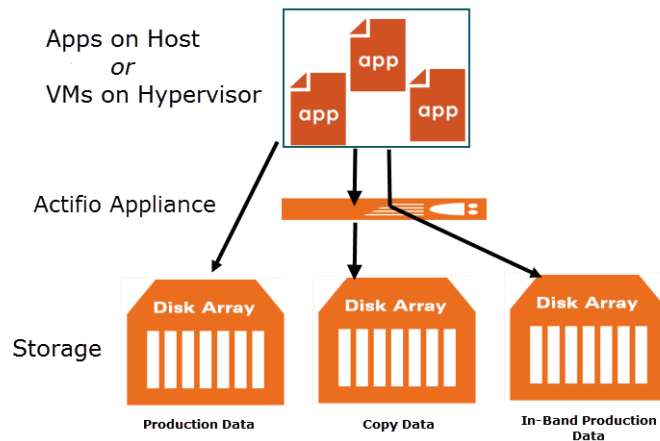
This chapter helps you understand the storage topology choices you can make and how these affect how an Actifio appliance will protect the copy data. The copy data is stored in VDisks in the Actifio appliance storage pools described in [Configuring Storage Pools](#) on page 21.

Production data can be:

In-Band: Production data storage is controlled by an Actifio CDS appliance. Snapshots and changed-block tracking are native to Actifio CDS appliance. In-Band storage is described in [In-Band Data](#) on page 17.

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

Out-of-Band: Production data storage is handled by a non-Actifio volume controller. Snapshots and changed-block tracking are handled by the Actifio Connector on physical hosts and Hyper-V VMs, and through VMware APIs for VMware VMs. Out-of-Band storage uses your existing storage arrays. Out-of-Band storage is described in [Out-of-Band Data](#) on page 19.



A Single Appliance Can Protect Data In-Band and Out-of-Band

The Actifio Connector

The Actifio Connector is a small-footprint lightweight process installed on physical and virtual hosts to provide advanced data protection and restoration capabilities. Under normal conditions, the Actifio Connector requires less than 10 MB of memory and uses less than 0.5% of CPU time.

Note: Protecting an entire VMware VM does not require the use of the Actifio Connector. To protect an entire VMware VM an Actifio appliance makes calls to VMware APIs. To protect an entire Hyper-V VM, you must install the Actifio Connector on the VM's Hyper-V Server.

The Actifio Connector:

- Enables an Actifio appliance to discover supported applications on out-of-band host machines.
- Truncates the logs of an application on application hosts after a backup.
- Quiesces an application on a host machine or in a host VM before backing up the production data. This process ensures an application-consistent backup for applications that support it.

To protect out-of-band applications, install the Actifio Connector on the server(s) that host those applications. After the first full backup, the Actifio appliance performs incremental backups.

If full backups are run instead of incremental backups:

- The Actifio Activity Monitor (change tracking driver) service may have stopped. In this case, check your Windows services and start the Actifio Activity Monitor service.
- The change tracking driver may be incorrectly configured or not installed. In this case, uninstall and then make a full install of the Actifio Connector.

In-Band Data

In addition to the storage pools for copy data, the Actifio CDS appliance can also have additional storage for your applications. Actifio Optimized Storage (AOS) is controlled by the Actifio CDS appliance volume controller.

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

The Actifio CDS appliance can protect a Fibre Channel presented volume using storage virtualization. In-Band means that the Fibre Channel attached back-end storage device presents volumes to the Actifio CDS appliance (using SAN LUN masking) which the Actifio CDS appliance then presents to the host over Fibre Channel or iSCSI. This storage method allows the Actifio CDS appliance to track every block of the volume and determine which blocks change over time.

When the SLA driven scheduler determines a production snapshot is required, the Actifio CDS appliance makes a copy-on-write snapshot. This action allows the Actifio CDS appliance to save space in the snapshot pool by storing only the changed blocks. These snapshots can then be used for:

- **“Instant-Backup”** - Because each snapshot does not in itself move data, copy on first write only occurs when blocks change.
- **“Instant-Restore”** - Because the Actifio CDS appliance is presenting the storage, it can simply present a previous point-in-time to the host. Any data movement needed to complete the restore is done in the background without any further host downtime.

After each snapshot, the Actifio CDS appliance can create a deduplicated and compressed image of the snapshot that is stored in the Actifio dedup pool.

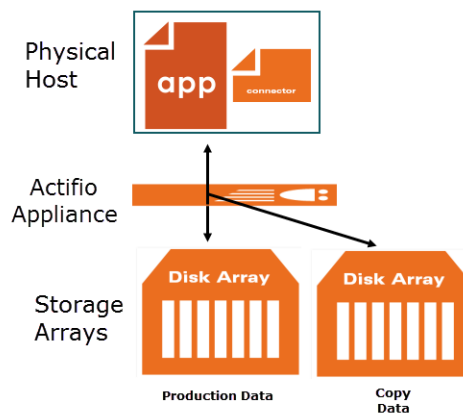
Both physical hosts and hypervisors can be protected in-band:

[Protecting Physical Hosts In-Band](#) on page 17

[Protecting Entire VMs In-Band](#) on page 18

Protecting Physical Hosts In-Band

The Actifio Connector is used to capture applications on physical servers. The Actifio Connector achieves application-consistent backups by enabling Microsoft VSS (Shadow Copy snapshots, and database quiescing).



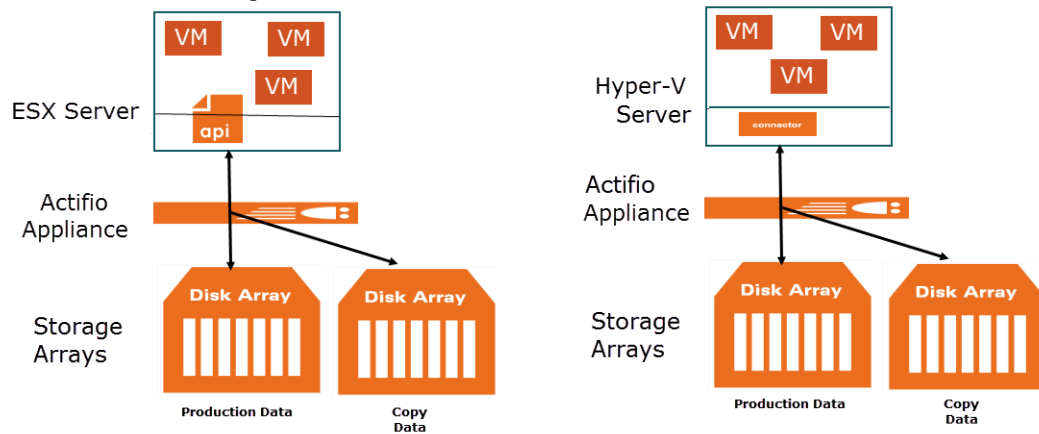
Protecting Physical Server In-Band

Protecting Entire VMs In-Band

An Actifio appliance can protect entire VMware and Hyper-V VMs.

To protect entire VMware VMs, the Actifio appliance takes advantage of VMware APIs to quiesce applications and achieve application-consistent backups.

To protect entire Hyper-V VMs, the Actifio Connector is installed on the Hyper-V server. The Actifio Connector achieves application-consistent backups by enabling Microsoft VSS (Shadow Copy snapshots, and database quiescing).



Protecting Entire VMware and Hyper-V VMs

Out-of-Band Data

When the Actifio appliance is not in the data path, it protects copy data by presenting a staging disk to the host. This staging disk maintains a golden copy of the application data that is protected using Actifio appliance snapshots. On Windows, application-consistent backups are made via VSS. Oracle backups on all platforms are application consistent via RMAN interfaces. Whole VM backups are application-consistent if they are configured with vmtools.

Whenever possible, change block tracking is used to minimize backup data movement. Tracking is accomplished with VSS snapshots, Oracle RMAN, and the Actifio Connector.

This section describes:

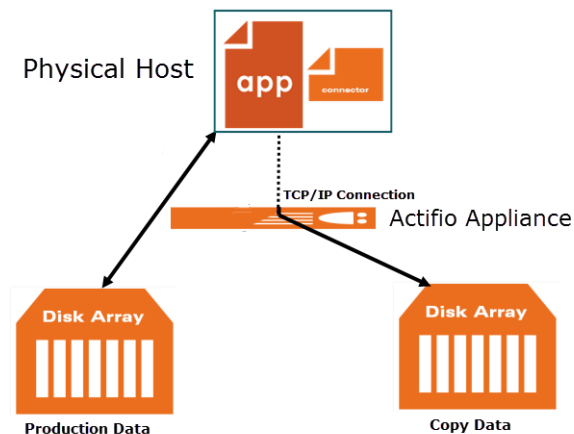
[Protecting Physical Hosts Out-of-Band](#) on page 19

[Protecting Entire VMware and Hyper-V VMs Out-of-Band](#) on page 20

[Protecting Individual Applications on a VMware or Hyper-V VM Out-of-Band](#) on page 20

Protecting Physical Hosts Out-of-Band

Applications on physical hosts are backed up with the Actifio Connector by reading data from the production data and sending this data to the snapshot pool or directly to the dedup pool. Most Windows backups are made in an application-consistent way via VSS, and database backups are application-consistent through database-specific APIs. Change block tracking is typically used to accelerate the process.

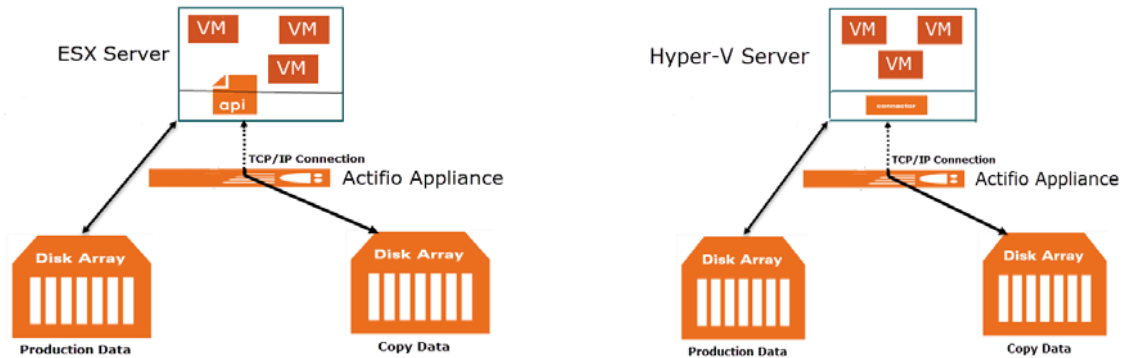


Protecting Applications on Physical Hosts Out-of-Band

Protecting Entire VMware and Hyper-V VMs Out-of-Band

An Actifio appliance can protect entire VMware and Hyper-V VMs Out-of-Band.

To protect entire VMware VMs, the Actifio appliance takes advantage of VMware APIs. To protect entire Hyper-V VMs, the Actifio Connector is installed on the Hyper-V server.

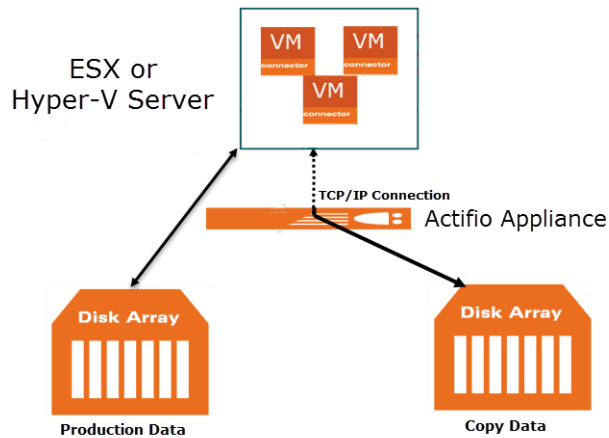


Protecting Entire VMs Out-of-Band

Note: An Actifio Sky appliance is a VMware VM and can be on the same ESX server as VMs it protects.

Protecting Individual Applications on a VMware or Hyper-V VM Out-of-Band

The Actifio Connector is used to protect individual applications on a VM. Once the Actifio Connector is installed on a VM, you can create policies to protect sets of applications on the VM.



Protecting Applications on a VM Out-of-Band

Note: An Actifio Sky appliance is a VMware VM and can be on the same ESX server as VMs it protects.

4 Configuring Storage Pools

Storage management includes:

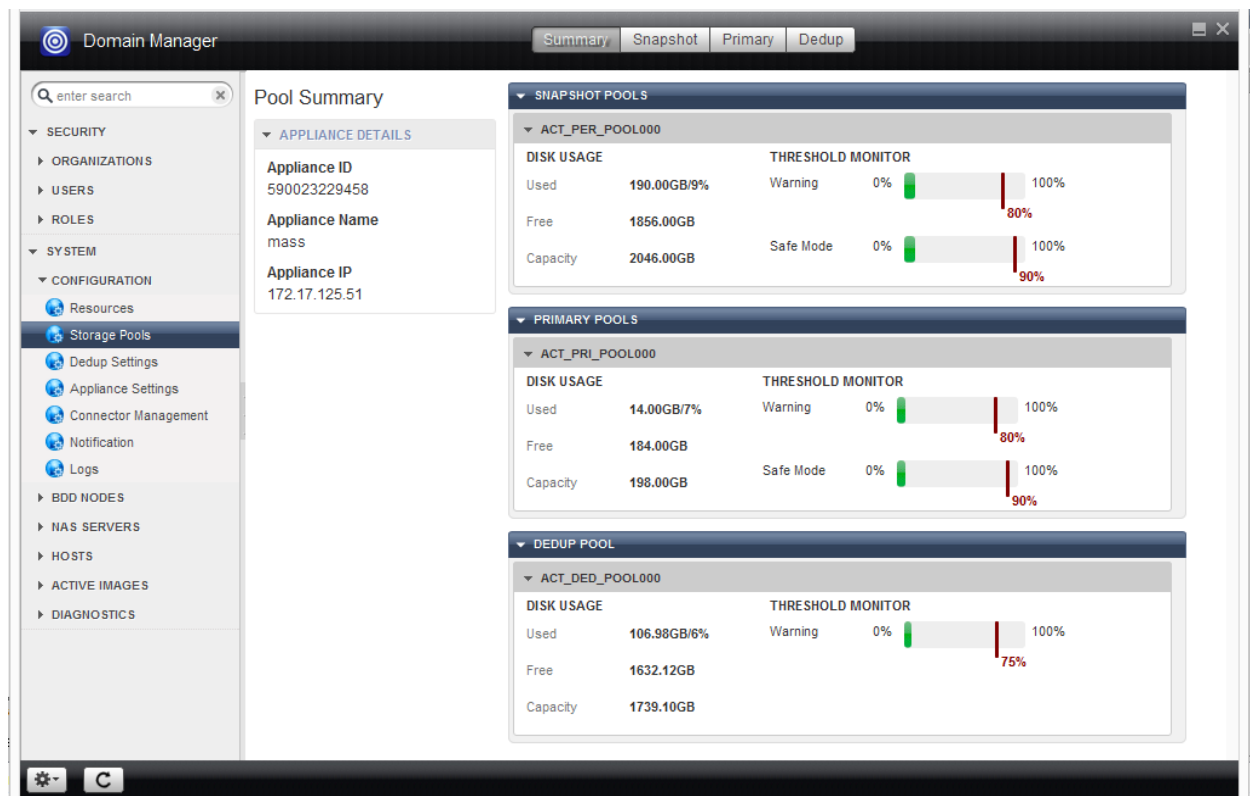
[About Storage Pools](#) on page 22

[VDisks and VDisk Consumption](#) on page 23

[Configuring the Alert Levels for Storage Pools and Resource Profiles](#) on page 25

[Creating, Modifying, and Deleting Storage Pools](#) on page 26

[Deleting Snapshot Pools](#) on page 30



Storage Pools

About Storage Pools

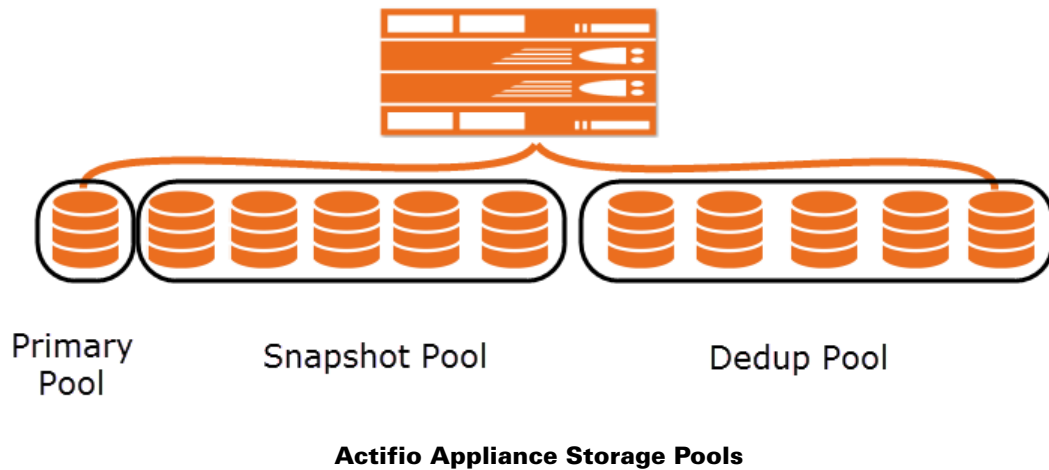
Actifio appliances provide three types of storage pools:

Snapshot storage pool: The Snapshot Pool (also called the Performance pool) is for the instant backup/restore pieces of the process. The snapshot pool often contains hundreds of VDisks. Snapshots are good for instant access. Snapshot pool consumption is detailed in [Viewing and Managing Snapshot Memory Usage](#) on page 9.

Primary pool: The Primary Pool, act_pri_pool000, is for the Actifio appliance use. Do not change the Primary pool or add a second pool unless instructed by Actifio Support.

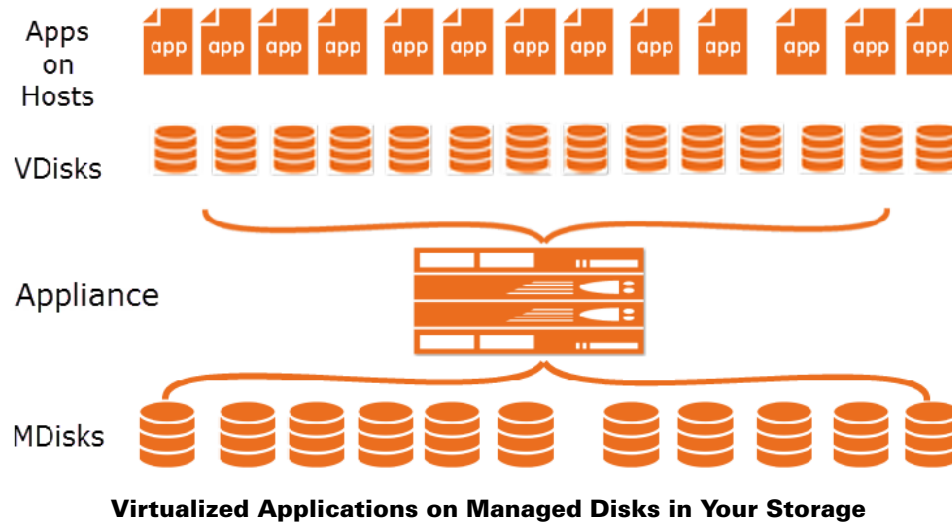
Dedup storage pool: Dedup storage is for compact long-term retention. The Dedup pool consumption is detailed in [Chapter 5, Understanding Dedup Pools](#)

The primary pool provides your fastest storage, while the dedup pool is best for an array that is less performance-critical but requires superior reliability over the long term.



VDisks and VDisk Consumption

VDisks (virtual disks or volumes) are the primary tool of copy data management. Copy data from hosts and VMs is copied to VDisks in the Snapshot Pool. From the VDisks, the data can be deduplicated, cloned, mounted and recovered, presented for test and development work, and manipulated in other tasks.



How Many VDisks Do I Need?

An Actifio appliance creates VDisks as needed from pools of MDisks on the physical disk arrays in the Actifio appliance. The applications and hosts never see the MDisks.

There is a fixed limit of 2048 VDisks per Actifio appliance. If you have enough VDisks for your needs, but they are growing too large for your existing storage, then you must add storage, as described in [Modifying Storage Pools](#) on page 29. If you need more VDisks, then you need another Actifio appliance as described in [Chapter 10, Configuring Shared Appliances](#).

In general, each protected application or VM requires one VDisk for the staging disk plus one VDisk per snapshot.

In addition, note these rules:

- Volumes each consume one VDisk.
- Each protected file system consumes one VDisk.
- Clones of non-VM applications consume VDisks.
- Mounts consume VDisks (they are effectively snapshots).
- LiveClones consume VDisks.
- On Linux and Solaris systems, filesystems and Oracle databases consume one VDisk, plus another for every additional 2TB data is being protected.
- Exchange and SQL databases consume one VDisk for every volume that hosts the database.
- VMs protected by a snapshot SLA consume one VDisk per VMDK/VHD.
- Each Actifio CDS appliance Sideband datastore consumes one VDisk.
- Each snapshot of a VDisk consumes one VDisk per snapshot per protected disk.
- Snapshots show peak usage, as new snapshots are created before old snapshots are expired.
- Each VDisk protected by Dedup-Async consumes one additional VDisk for the DAR snapshot.
- After failover and syncback, the failback operation cleans out all the syncback and failover VDisks.

VDisks are thin-provisioned, and can grow over time, as explained in [Snapshot Pools](#) on page 24.

Snapshot Pools

The Snapshot pool (sometimes referred to as the Performance Pool) holds “golden copies” of application data at the points in time specified by Service Level Agreement (SLA). Snapshot space is also used to rehydrate images from the deduplication pool. The amount of data consumed is determined by whether an existing snapshot can be used.

Snapshot Pool space is consumed by three different kinds of VDisk:

Staging disks: Staging disks are the Actifio golden copy of the application. Staging disks are retained for as long as an application is protected.

Snapshot disks: Snapshots are used to preserve the state of staging disks at specific points in time. Snapshots are retained till their expiry time. However the last snapshot will never expire unless the application is unprotected.

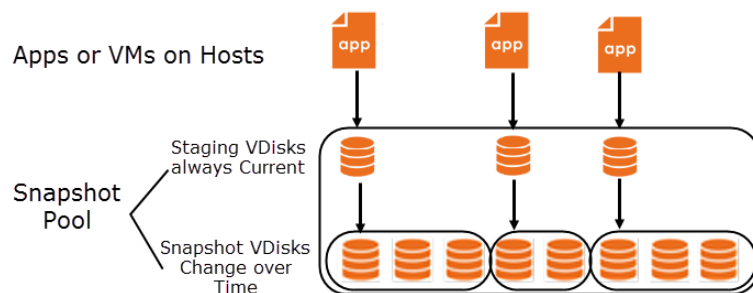
Clone disks: Clone disks are full copies of an application’s production data. Clone disks are not automatically expired.

Staging disks and snapshots are always thin-provisioned.

Staging Disks

A staging disk is a VDisk created when an application is first protected. It is a copy of the production data as of the last backup invoked by the application’s SLA. Each staging disk is associated with a number of snapshots on their own snapshot disks. The number of snapshots for each application or VM is determined by the SLA frequency of snapshot and duration until expiry.

Because a staging disk is a complete copy of the production application or VM, each staging disk requires as much storage space in the Snapshot Pool as the protected application or VM requires in its production storage. Snapshots made from the staging disk reference the data in the staging disk, so they are much smaller, but they can grow over time.



Virtualized Copy Data on Staging VDisks and Snapshot VDisks in the Snapshot Pool

Snapshot Pool Storage Consumption

The Snapshot Pool contains both the staging disks and the snapshot disks for every protected application or VM, plus any clones that you make.

The storage space consumed in the Snapshot Pool depends upon whether the application and VM production data is in-band or out-of-band. For more on in-band and out-of-band storage, see [Chapter 3, Understanding In-Band and Out-of-Band Data Storage](#).

Note: In-Band is not applicable to the Actifio Sky appliance.

- In-band applications have only incremental backups because the Actifio CDS appliance stores the production data.
- Out-of-band applications have one staging disk which is the same size as the object being protected (for instance, a 100GB VM has a 100GB staging disk) then a series of snapshots (based on expiration policy) which can take very little space if they do not change frequently.

Configuring the Alert Levels for Storage Pools and Resource Profiles

You can configure two usage alert levels, Warning and Safe Mode, for the two (snapshot and primary) types of storage pools of the Actifio appliance.

Note: Do not change these settings unless advised by Actifio Support.

The Actifio appliance:

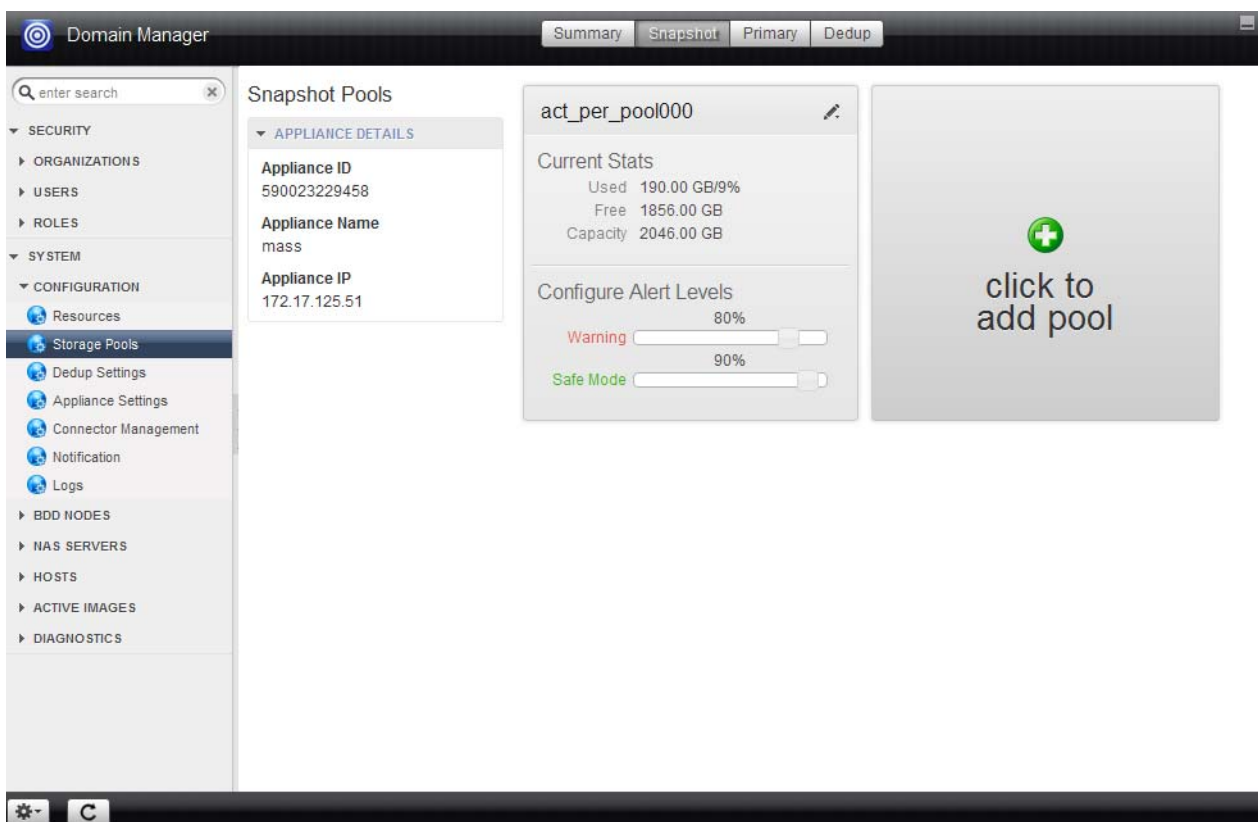
- Issues warnings when the stored data exceeds the configured warning limit.
- Stops the snapshot/primary/deduplication activities and issues alerts when the stored data exceeds the configured safe limit, and all the expiration jobs still continue. If any currently running jobs are taking too much time to complete, they will be canceled automatically.

To configure the usage level:

1. Open the **Domain Manager** to **System > Configuration > Storage Pools**.
2. Select the **Snapshot**, **Primary**, or **Dedup** tab.

The default Warning level is 80% for the snapshot and primary pools and 75% for the deduplication pool. When this level is exceeded, you see warnings.

3. Set Safe Mode to an appropriate level of usage. The default value is 90% for the snapshot and primary pools. When this value is exceeded, the Actifio appliance stops writing to storage. Do not change the default settings unless advised by Actifio Support. The Safe Mode option is not available with deduplication.



Alert Levels

Creating, Modifying, and Deleting Storage Pools

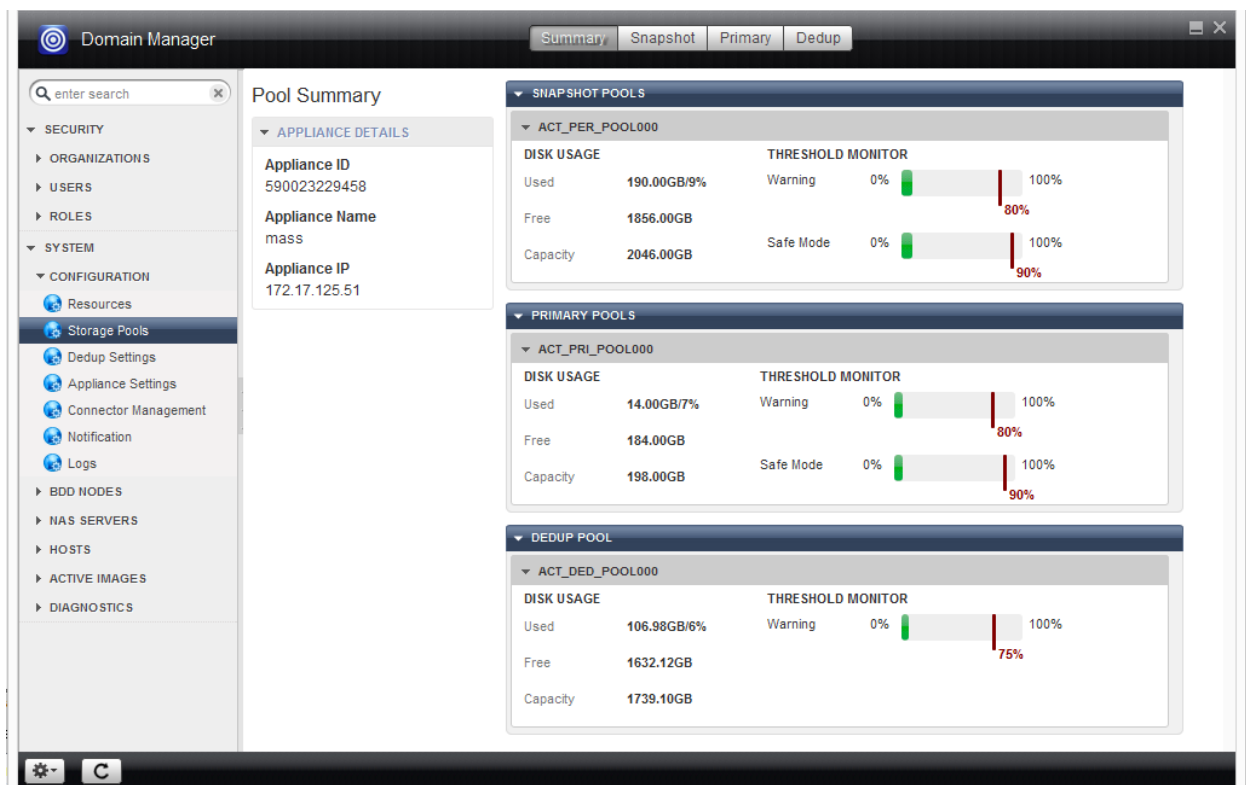
The Actifio appliance provides two types of storage pools that serve different purposes: snapshot storage pools and dedup storage pools.

This section details:

- [Viewing Storage Pool Information](#) on page 26
- [Creating Additional Snapshot Pools](#) on page 27
- [Modifying Storage Pools](#) on page 29
- [Deleting Snapshot Pools](#) on page 30

Viewing Storage Pool Information

To view the existing storage pools information, open the **Domain Manager** to **System > Configuration > Storage Pools**. The pool summary page shows the disk usage (used, free, and total capacity) and alert level (Warning and Safe Mode) settings:



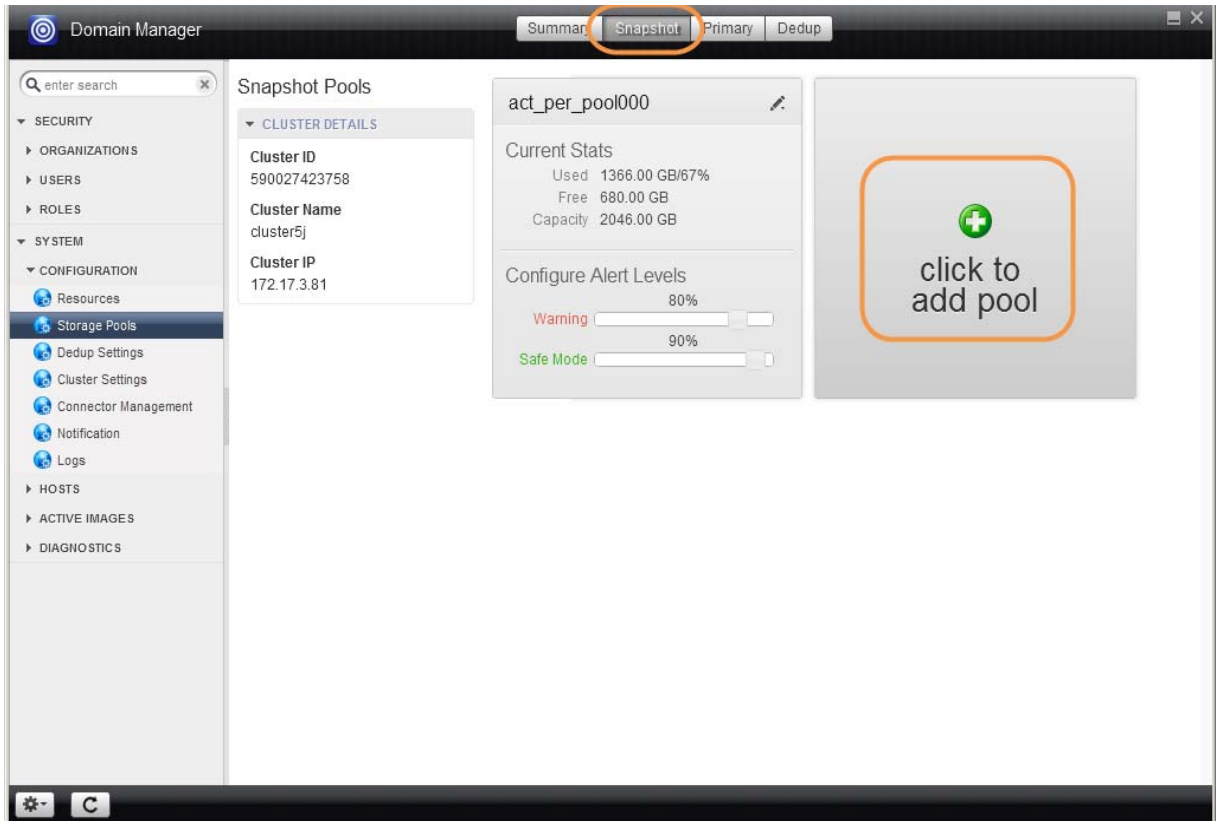
Viewing the Summary of the Three Storage Pools

Creating Additional Snapshot Pools

You can create additional storage pools for snapshot storage. You might do this to keep snapshot data from different groups or systems separate from each other.

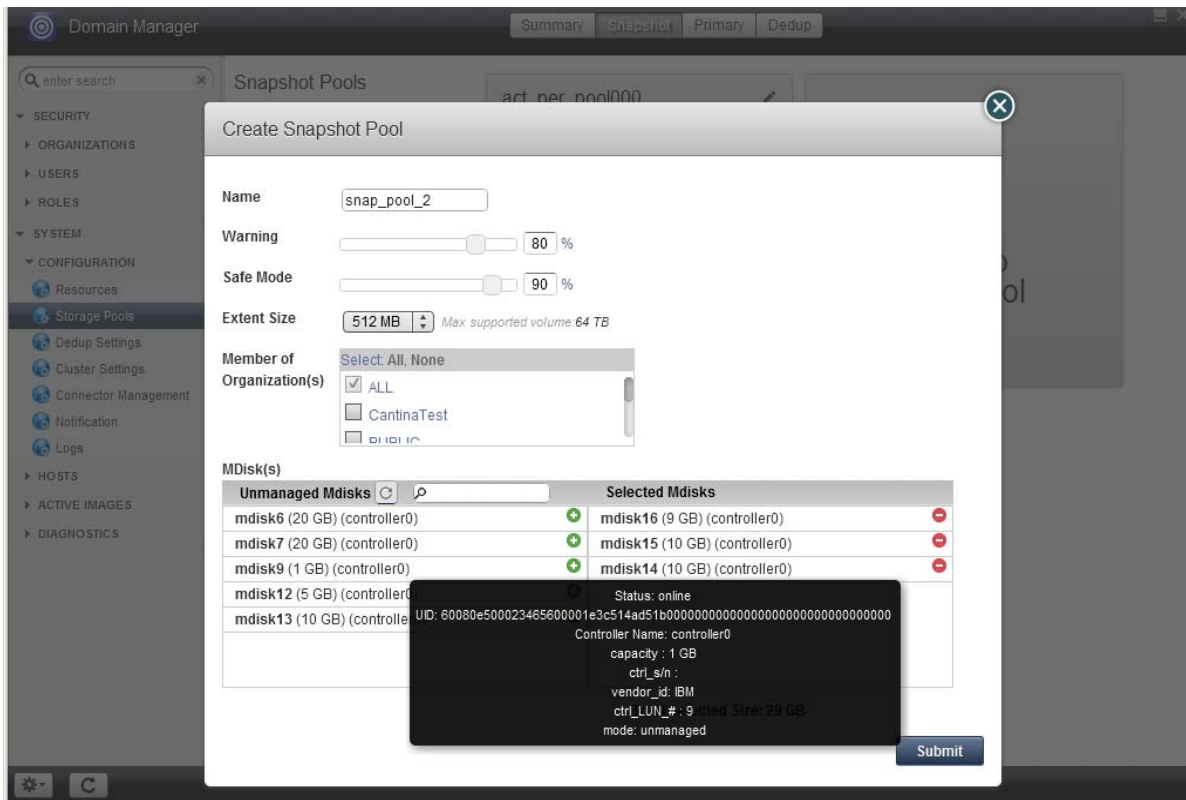
To create an additional snapshot pool:

1. Open the **Domain Manager** to **System > Configuration > Storage Pools**.
2. Select the **Snapshot** tab. The Snapshot Pools page opens.



Adding a Snapshot Pool

3. Click on **click to add pool**. The Create Pool page appears.
4. Enter a **Name** for the storage pool.
5. If required, modify the default **Warning** and **Safe Mode** limits.
6. Choose the required size from the **Extent Size** drop-down list.
7. Select the organizations that will have access to this pool.
8. Select the **MDisk(s)** to include in this pool from the list of unmanaged disks by clicking on the appropriate + symbol. Use the search option to find the required MDisk(s). Selected MDisks appear in the right-hand panel. You can hold the mouse cursor over an MDisk record to see its status, including UID, controller, capacity, etc.
9. Click **Submit**.
10. A warning dialog appears. Type **PROCEED** to confirm.
11. Click **Confirm**. The newly created pool is listed under the snapshot or primary pool page.



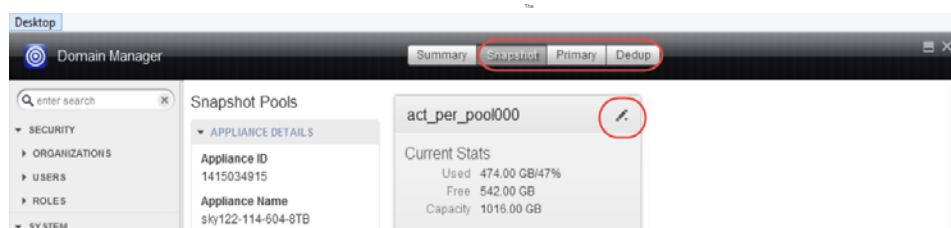
Viewing the Status of an MDisk to be Added to a New Snapshot Pool

Modifying Storage Pools

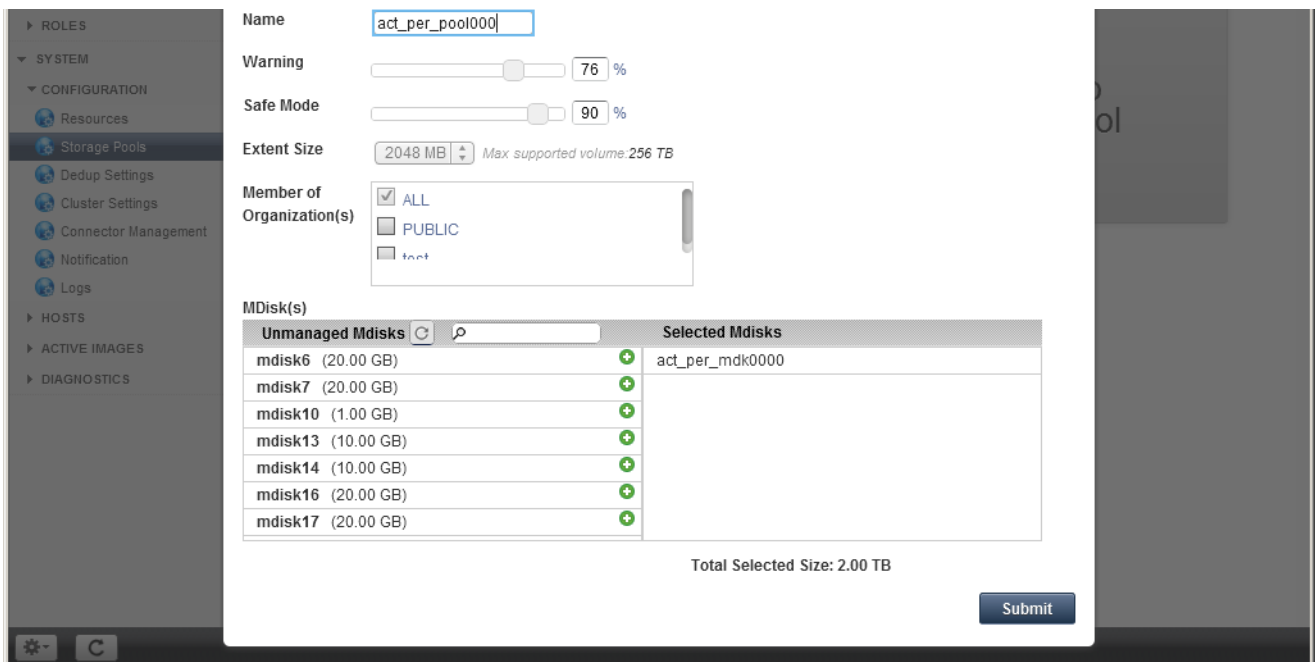
You can extend the size of existing storage pools and also modify the storage pools information.

To modify the existing storage pool information:

1. Open the **Domain Manager** to **System > Configuration > Storage Pools**.
2. Select the **Snapshot** or **Dedup** tab. The Snapshot Pools or Dedup Pool information page opens.
3. Click the pencil edit icon next to the storage pool name. The Manage Pool page appears.
4. Make the required modifications. Add additional unmanaged MDisk(s) to increase the size of the pool. Select one or more MDisk(s) from the list of unmanaged disks by clicking on the appropriate + symbol. Use the search option to find the required MDisk(s). Added MDisk(s) appear in the right-hand panel.
5. Click **Submit**. A warning dialog appears. Enter **PROCEED** in the text box to confirm.
6. You can verify the modified pool details under the corresponding snapshot, primary or dedup pool information page.



Pool Edit Icon



Modifying a Snapshot Pool

Deleting Snapshot Pools

You can delete any of the user-created snapshot pools, but you cannot delete the default storage pools.

Note: Before deleting a storage pool, ensure that the pool is not in use. To remove a pool that is in use, expire all the backup data that exists in the pool. See the *Forcing the Expiry of a Backup Image* section.

To delete an existing storage pool:

1. Open the **Domain Manager** to **System > Configuration > Storage Pools**.
2. Select the **Snapshot** tab. The Snapshot Pools information page opens.
3. Select the desired pool and then click on the delete icon next to the storage pool name. The icon appears only if you have pools that can be deleted.
4. A warning dialog appears. Enter **DELETE** in the text box to confirm.

Click **Confirm**. The selected pool is removed from the Actifio appliance.

5 Understanding Dedup Pools

The dedup pool is used for long term retention of application images on disk. Images are created by deduplication of snapshots, direct to dedup jobs, and dedup async jobs. In addition images can be created by remote replication where remote appliances send data to the local dedup pool.

Space is consumed by deduplicated and compressed images that have fixed expiry dates.

An Actifio 100T appliance can process approximately 3 TB of data per day. This amount of data processing means that if the total daily change rate will exceed 3 TB then an additional Actifio appliance may be required.

This section includes:

[Reducing Dedup Pool Consumption](#) on page 31

[Monitoring Dedup Pool Space Consumption](#) on page 32

When the safe level has been exceeded, no new dedup related jobs can be run. Actifio appliance sends a warning when dedup pool consumption exceeds the warning or safe levels. To configure notifications, see [Alerting](#) on page 85.

Reducing Dedup Pool Consumption

There are three ways that the dedup pool grows:

- Daily changes processed by dedup: MB/s daily changes processed by dedup target for average systems is 3TB a day. Another way to look at this is that for a 100T appliance a 3% change rate is 3TB.
- Daily dedup cores that are busy
- Dedup size

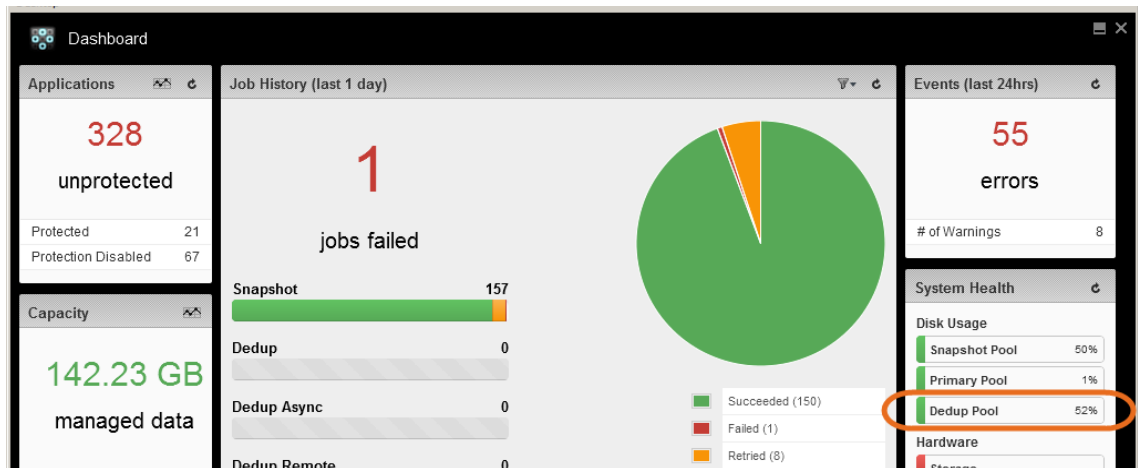
To reduce the amount of dedup pool space consumed:

- Identify applications with high change rates or more importantly, low deduplication rates. Applications with dedup rates below 80% can be major space consumers. Reduce retention for these applications. For example, an application that contributes 30 GB per day to the dedup pool produces after 30 days close to 1 TB of net new data. After 12 months it has required 12 TB of dedup pool space.
- Use a mixed retention policy, retaining daily images for maybe 1 month, weekly images for three months, monthly images for one year, etc.
- Run Garbage Collection (GC) and sweep on a regular basis. Once per month is common.
- If you are using Dedup Async or have dedup jobs with very short retention (one week or less) also schedule Incremental Garbage Collection (IGC) to run weekly.
- Expiring images or reducing retention rates will not have an immediate affect on the dedup pool. You will need to run garbage collection and sweep on a regular basis to remove blocks that are no longer owned by any image.

Note: *Garbage collections is described in [Chapter 6, Configuring Dedup Garbage Collection](#).*

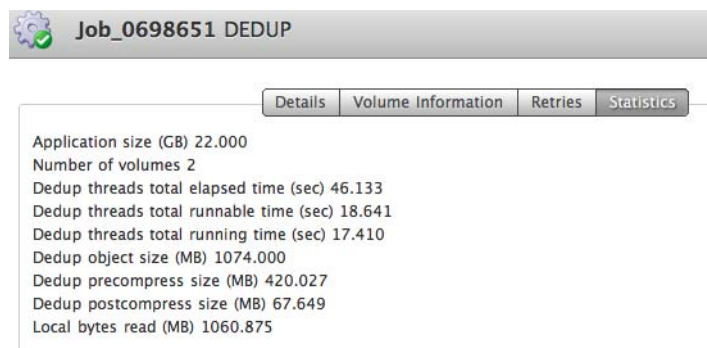
Monitoring Dedup Pool Space Consumption

Dedup pool consumption for the Actifio appliance is shown on the Dashboard panel of the Actifio Desktop.



Dedup pool space consumption is shown in the Domain Manager under System > Configuration > Storage Pools, as described in [Viewing Storage Pool Information](#) on page 26.

The deduplication statistics for each dedup job can be displayed using the Event Monitor in the Actifio Desktop.



Actifio Appliance Reports Related to Dedup Pool Management

In the Actifio Report Manager, there are several reports available from the Utilization category.

The reports relating to dedup consumption are:

- Application Contribution to Daily Dedup Pool
- Application Contribution to Daily Storage Pool and V-Disk Usage
- Dedup Pool Utilization History by Application
- Disk Pool Utilization History
- Storage Pool Usage by Organization
- Storage Resource Usage Summary
- TOP - N Dedup Pool Users

Reports are detailed in **Using the Report Manager** in your Documentation Library.

6 Configuring Dedup Garbage Collection

The amount of storage consumed by the dedup store grows over time, depending on the amount of unique data added with each new image that is ingested. As each image is expired, the space occupied by the unique data that was represented by that image is not immediately reclaimed. The Garbage Collection (GC) process identifies (and later reclaims) space occupied by this no-longer-needed data.

GC consists of two phases:

The **enumeration** uses the current catalog of deduplicated images to decide what data needs to be kept in the system (and, by exclusion, which does not).

The **sweep** phase actually copies the useful data remaining in each region of the dedup store into new regions of the dedup store. The old regions are then freed. In this manner, only the still-relevant data in the dedup store is kept, and the rest has been “swept” away.

Note: *The enumeration phase must complete all at once for a subsequent sweep to happen. The sweep phase can be canceled and restarted without penalty.*

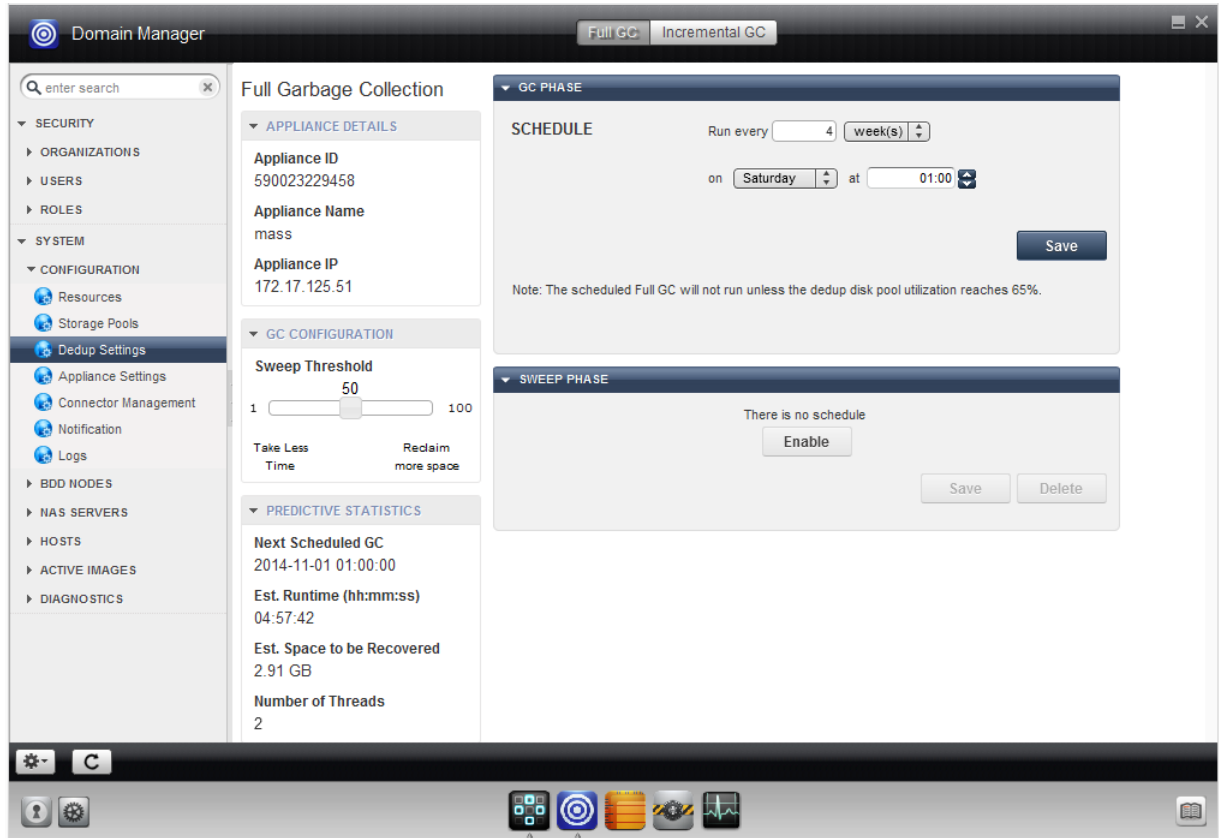
There are two levels of GC:

Full GC: Full GC is very effective, but it is resource-intensive and time-consuming. The first Full GC you run can take days to complete. Check the **Est. Runtime** in the Predictive Statistics section of the GC page. The estimate values are derived from the results of the last run.

Incremental GC: Incremental GC only frees storage space that has been consumed and dereferenced since the last full GC. If you have a high rate of backup and expiration of recent backups, or if you are running dedup async, it is very likely that you need incremental GC to prevent the dedup store growing too fast between full GCs. Incremental GC does not recover all the space that a Full GC does. If the **Enable** button is displayed, then no Incremental GCs are scheduled.

Note: *Incremental GC runs only when at least one dedup-async operation is configured.*

The more often you run GC, the less time subsequent GC operations require. You configure Full and Incremental GC in the same way, described in [Configuring a GC Schedule](#) on page 35.



The Dedup Garbage Collection Section of the Domain Manager's System Section

Configuring a GC Schedule

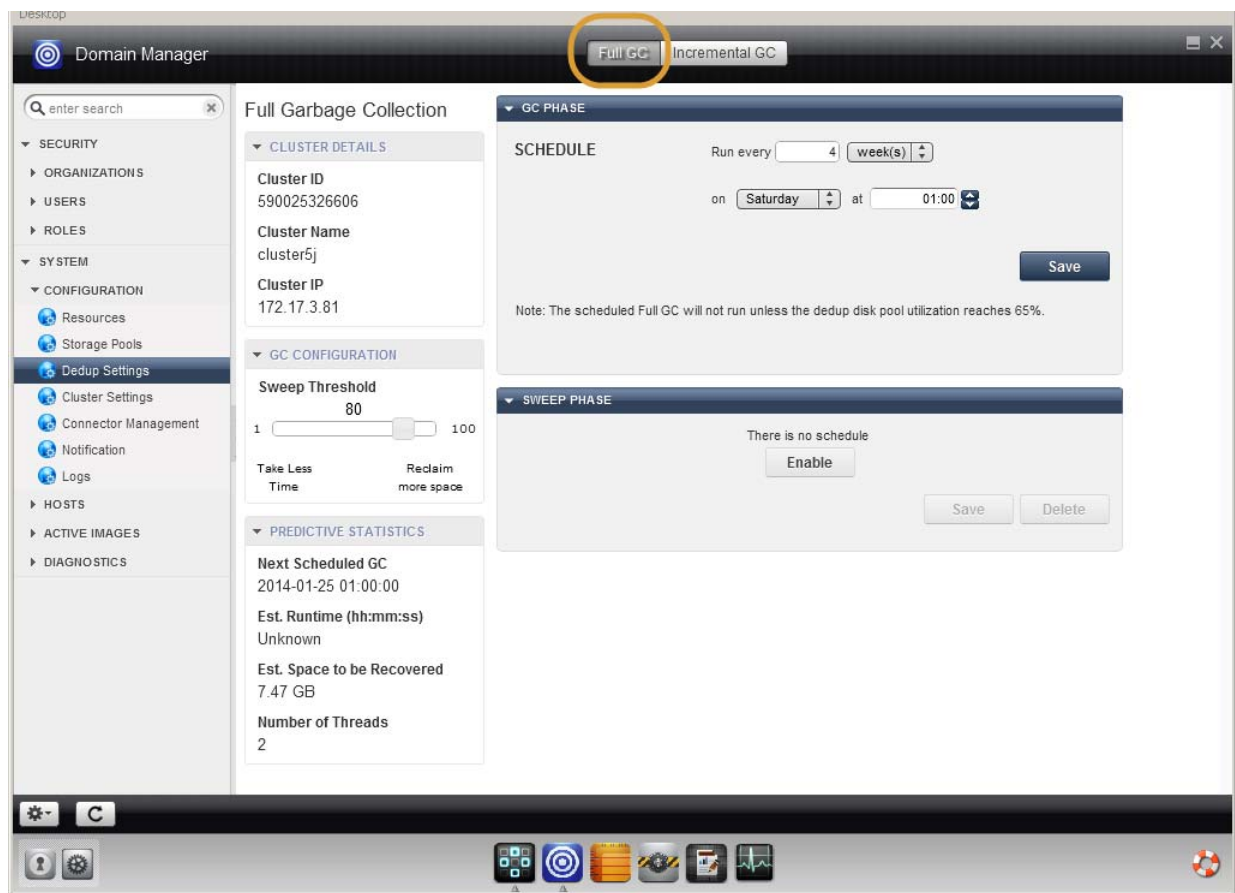
The GC schedule is managed in two phases: [GC Phase](#) and [Sweep Phase](#).

GC Phase

In this phase, all reachable objects are identified and marked.

To configure the GC phase settings:

1. Open the **Domain Manager** to **System > Configuration > Dedup Settings**. This sequence opens the GC configuration page.
2. Select the frequency of garbage collection from **SCHEDULE**. You can set this frequency value to run weekly or monthly.
3. Select the day and time values to perform the garbage collection.
4. Click **Save** to update the changes.



Configuring Garbage Collection (GC)

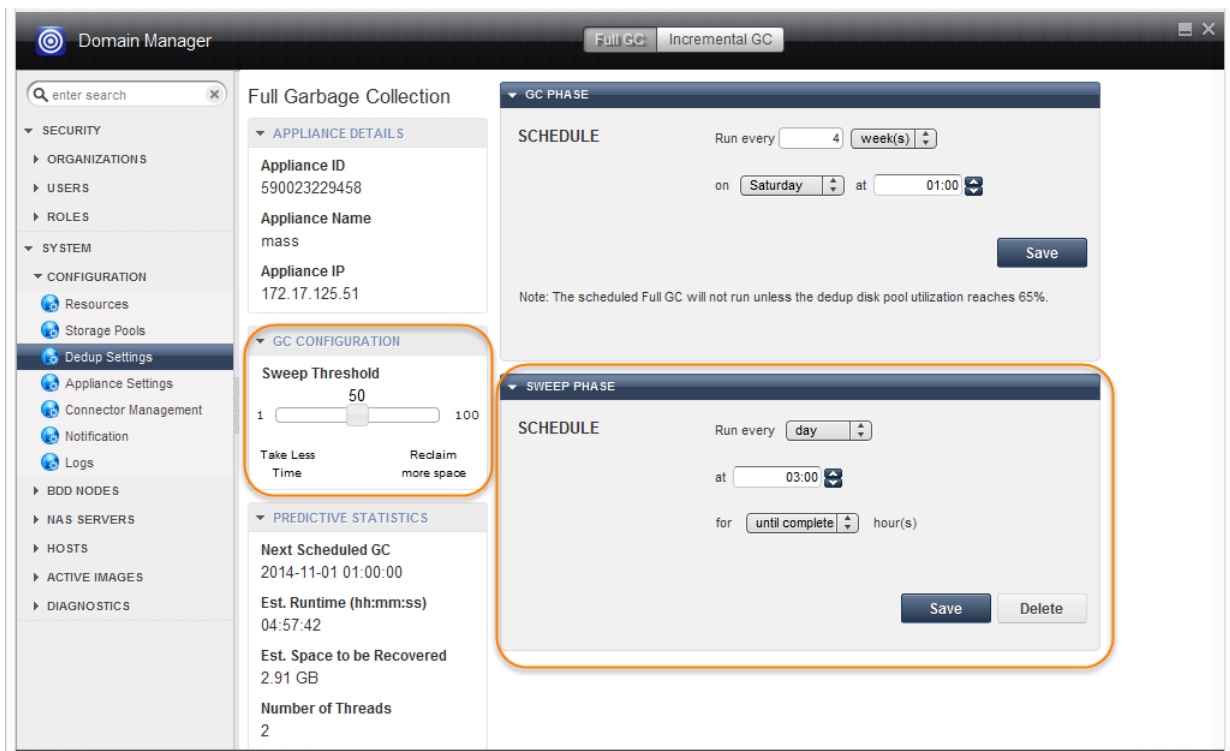
Sweep Phase

The sweep phase examines the marked objects, and frees storage space that has become unused. If no sweep schedule is enabled, then sweep runs after every GC phase. Schedule sweep separately if you want to have a sweep run for several hours every night (for example) until it is complete.

To configure the sweep phase settings:

1. Open the **Domain Manager** to **System > Configuration > Dedup Settings**.
2. In **SWEEP PHASE**, select the frequency of garbage collection: **daily**, **weekly**, or **monthly**.
3. Select the day and time values to perform the sweep.
4. Define how long the schedule should run. You can set this value to until complete or specified hours using the drop-down.
5. In **GC CONFIGURATION**, to the left, set a **Sweep Threshold**. This setting determines how aggressively the sweep process will reclaim space from expired backups. A setting of 100 reclaims all the possible space, but takes longer to run. A lower setting reclaims less space, but it reclaims it at a faster rate. The default value of this variable is 90. The **Est. Runtime** in the Predictive Statistics block in the lower left can help you decide how aggressively to sweep.
6. Click **Save** to update the changes.

The more often you run GC, the less time subsequent GC operations require.

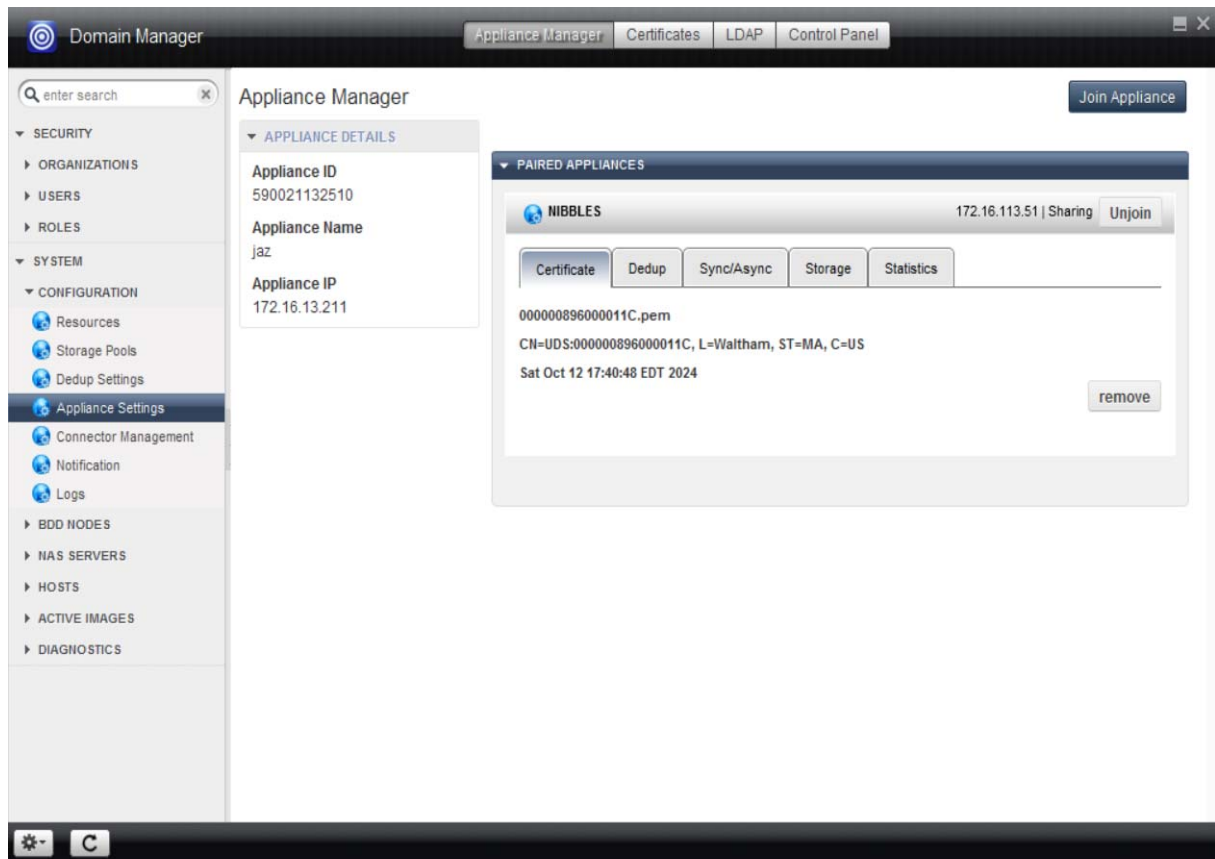


Configuring GC Sweep

7 Managing Appliances

The management of an Actifio appliance from the Appliance Manager includes:

- [Viewing and Removing Certificates](#) on page 38
- [Managing Bandwidth Utilization](#) on page 39
- [Enabling/Disabling Sync/Async Replication](#) on page 43
- [Selecting a Storage Pool for Replicated Data](#) on page 44
- [Viewing Bandwidth Usage Statistics](#) on page 45



The Appliance Manager Section of the Domain Manager

Viewing and Removing Certificates

Digital certificates are used to ensure secure communication between appliances and where applicable, the Actifio Business Resiliency Cloud. All members of a configuration must have matching security certificates in order to establish a secured relationship.

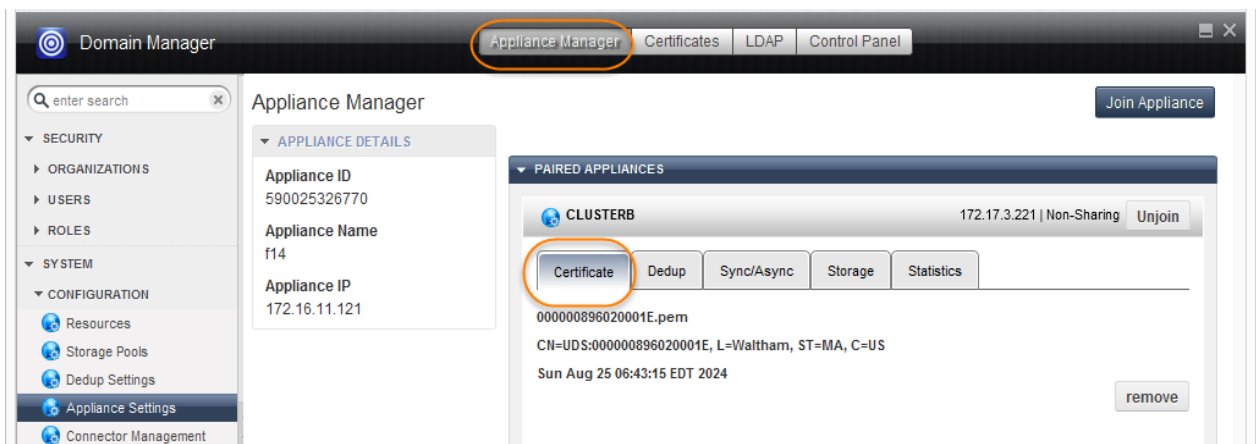
To establish a secured relationship between Actifio appliances or where applicable, between an Actifio appliance and the Actifio Business Resiliency Cloud:

- Exchange certificates as detailed in [Exchanging Certificates](#) on page 50.
- Download and upload certificates one at a time as detailed in [Downloading a Certificate](#) on page 49 and [Uploading a Certificate](#) on page 49.

Viewing Certificates

To view the certificate of all entities connected to the local appliance in the sharing or non-sharing mode:

1. Open the **Domain Manager** to **System > Configuration > Appliance Settings**. This sequence opens the Appliance Manager page.
2. Click the **Appliance Manager** tab and the **Certificate** subtab. A list of all entities connected to the local appliance is displayed along with the corresponding certificates.



Viewing Security Certificates

Removing a Certificate

To remove a certificate, select it as above and click **Remove**.

Managing Bandwidth Utilization

You can configure the bandwidth used to replicate data from one appliance to another so that Actifio appliance data shares the bandwidth available to your organization with the other organizational resources.

When two Actifio appliances are paired for replication, you can set the bandwidth used for this replication. This setting is made from the point-of-view of the originating Actifio appliance, called the “A-side.” When choosing this bandwidth setting, the bandwidth chosen represents the amount of traffic *originating from* this appliance to however many other appliances this Actifio appliance replicates to. If the Actifio appliances replicates to two other appliances, the bandwidth setting chosen will be shared between the two other appliances.

This section contains:

- [Enabling and Disabling Bandwidth Throttling](#) on page 40

- [Overriding Bandwidth Throttling](#) on page 41

- [Scheduling Bandwidth Throttling](#) on page 42

Enabling and Disabling Bandwidth Throttling

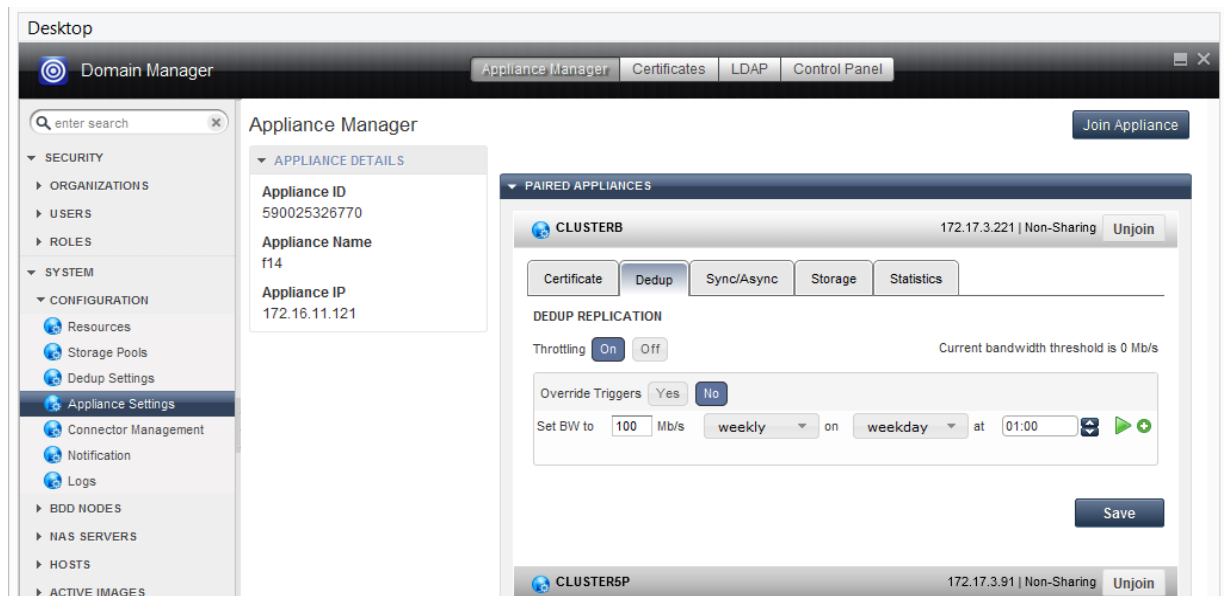
Use the Bandwidth Throttling feature to limit the bandwidth used by the replication process from an Actifio appliance.

Enable Bandwidth Throttling: Choose this option if you plan to choose a fixed amount of bandwidth dedicated for Actifio appliance replication. You can restrict bandwidth usage by enabling bandwidth throttling and limiting the maximum amount of bandwidth that the Actifio appliance should not exceed for all the replication.

Disable Bandwidth Throttling: Choose this option if you do not want to restrict the amount of bandwidth used for Actifio appliance operations. This option allows you to use the maximum available bandwidth.

To enable or disable the bandwidth throttling:

1. Open the **Domain Manager** to **System > Configuration > Appliance Settings**. The Appliance Manager page allows you to enable or disable the settings.
2. In the Appliance Manager, click the **Dedup** subtab.



Accessing the Dedup Subtab

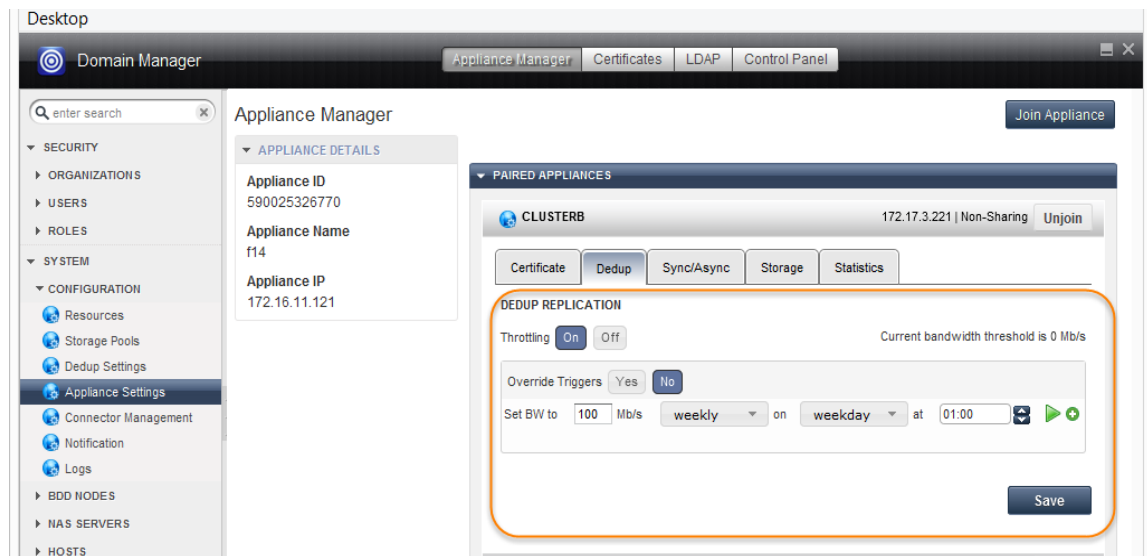
3. To enable throttling, click **On**. Enter the desired bandwidth in **Set BW to**. A value of 0 means unlimited bandwidth. To disable throttling, click the **Off** button.
4. Click **Save** to update the bandwidth configuration settings.

Overriding Bandwidth Throttling

Note: The bandwidth override process works only if you have enabled throttling.

To override the throttling:

1. Open the Domain Manager.
2. Click **System > Configuration > Appliance Settings**. The Appliance Manager page allows you to override throttling.
3. In the Appliance Manager, click the **Dedup** subtab.
4. Enable throttling by clicking the **On** button.
5. Click **Yes** to override existing triggers or to configure a constant bandwidth value.
6. Enter the desired bandwidth in **Set BW value to**. A value of 0 means unlimited bandwidth.
7. Click **Save** to update the changes.



Enabling Throttling in the Dedup Subtab

Scheduling Bandwidth Throttling

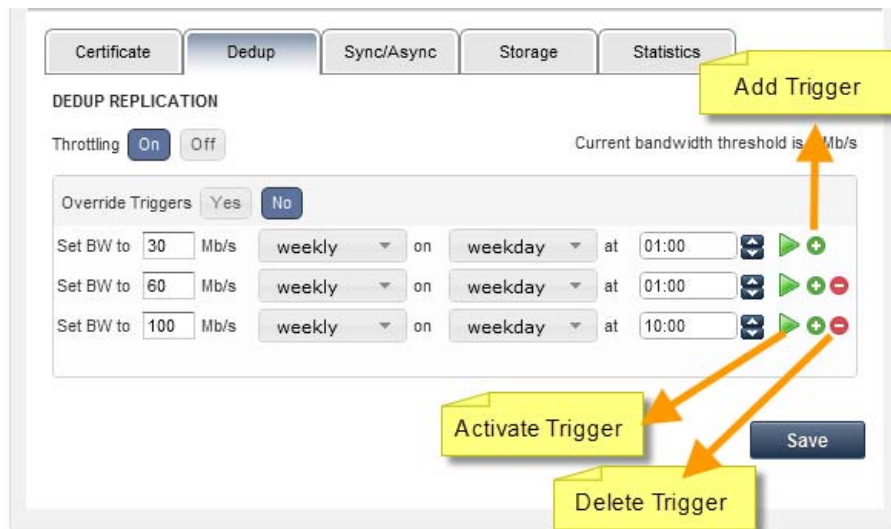
During some parts of the day or week, you may want an Actifio appliance to use less of your bandwidth so that other priority services can use it. You can customize the backup throttle so that it runs automatically based on the pre-defined schedules (triggers). Throttling determines the amount of bandwidth you want to dedicate to an Actifio appliance for your data replication.

This section describes how to create, activate and delete bandwidth triggers. Triggers are part of the scheduling framework. Each trigger allows you to specify the amount of bandwidth that you want to allocate, interval and time of the trigger. You can create separate triggers for weekdays and weekends to use them accordingly based on your needs.

Note: You can create a maximum of 10 different triggers.

To create a bandwidth trigger:

1. Open the Domain Manager.
2. Click **System > Configuration > Appliance Settings**. The Appliance Manager page allows you to override throttling.
3. In the Appliance Manager, click the **Dedup** subtab.



4. Enable throttling by clicking the **On** button next to Throttling.
5. Select **No** to override triggers.
6. Click **Add** new trigger button as showed in the above figure.
7. Provide the values to the trigger settings:
8. Click **Save** to update the changes.

Deleting a Trigger

To delete an existing trigger, select the trigger and click the **Delete Trigger** button.

Activating a Trigger

To activate a trigger, select the trigger and click on the **Activate Trigger** button.

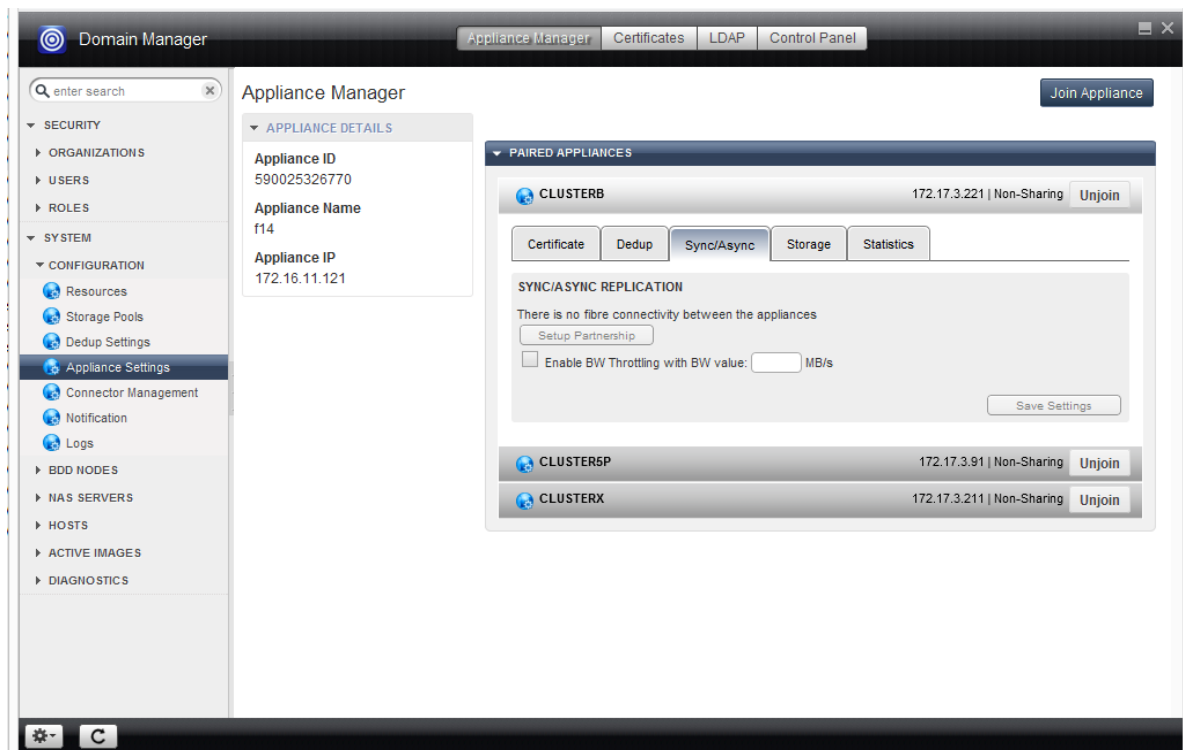
Enabling/Disabling Sync/Async Replication

A pair of joined Actifio CDS appliances requires partnership between the local and the joined appliance. Partnership is a pre-requisite for configuring synchronous or asynchronous replication over fibre-channel. The appliances must be zoned together in the SAN.

Note: Sync/Async Replication is supported only by the Actifio CDS appliance.

To set up partnership between two appliances:

1. Open the **Domain Manager** to **System > Configuration > Appliance Settings**. This sequence opens the Appliance Manager page.
2. Click the **Appliance Manager** tab and the **Sync/Async** subtab. The Sync/Async Replication page appears.
3. Click the **Setup Partnership** button from the Sync/Async tab. If partnership has been enabled, you can disable it from the Disable Partnership button that appears here.
4. (Optional) You can enable bandwidth throttling if you have it configured on the Dedup tab as described in [Managing Bandwidth Utilization](#) on page 39.
5. Click the gray **Save Settings** button.



Setting Up Partnership for Fibre Channel Support

Selecting a Storage Pool for Replicated Data

Incoming replicated Dedup-Async data is stored in a performance pool.

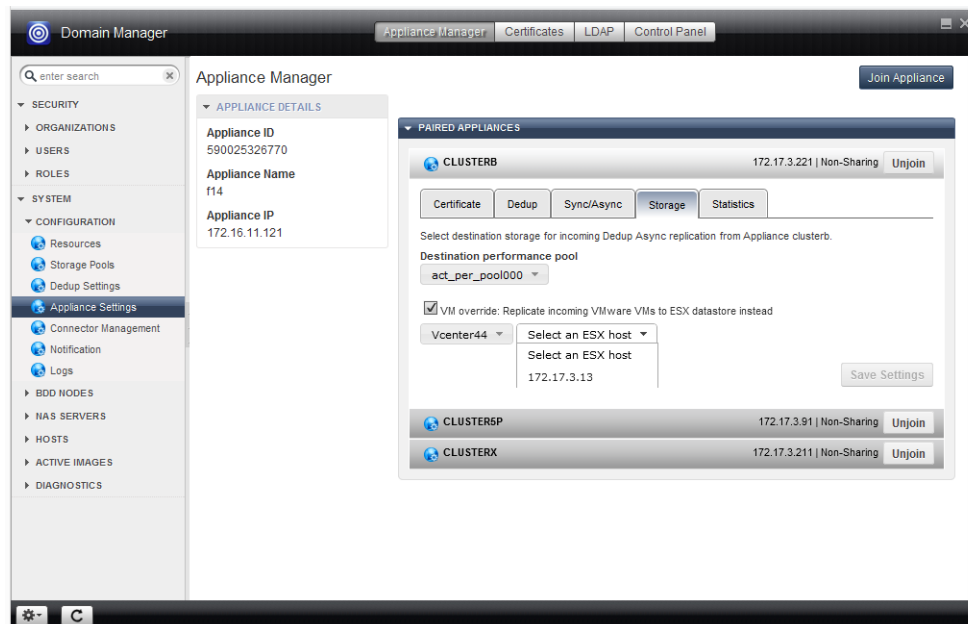
To select the performance pool for incoming DAR data:

1. Open the **Domain Manager** to **System > Configuration > Appliance Settings**. This sequence opens the Appliance Manager page.
2. Click the **Appliance Manager** tab to the **Storage** subtab. A drop down menu appears where you can select the destination performance pool for replicated data that comes to this Actifio appliance.
3. (Optional VMware only) You can override this setting for VMs if you want them to go to an ESX datastore instead. Check the **VMware only** box and make the following selections:
 - o Select a vCenter to manage the operation. This vCenter should ideally be at the DR site.
 - o Select an ESXi host to host the VMware VMs. This ESXi host should also be at the DR site and must be powered on and available at all times. You can only select one ESXi host.
 - o Select the datastores to hold the DR data. The datastores must have space to hold the replicated VMDKs (Virtual Disks). If you select multiple datastores the Actifio appliance will use them in a round-robin fashion.

The Actifio appliance will create new VMs at the DR site using the name DR-*<original VM name>*. For example, if the source VM is called testvm, then the DR copy will be called DR-testvm. If the VM already exists and is powered off, the Actifio appliance will use it as the target for the replicated VMs.

Note: When you configure VMware override, it affects the incoming dedup async to the appliance you are currently logged onto. If you require the DR appliance to create its DR copy in a VMware datastore rather than the DR appliances Snapshot pool, be sure to set the VMware override at the DR appliance site.

4. Click the gray **Save Settings** button.



Viewing Storage

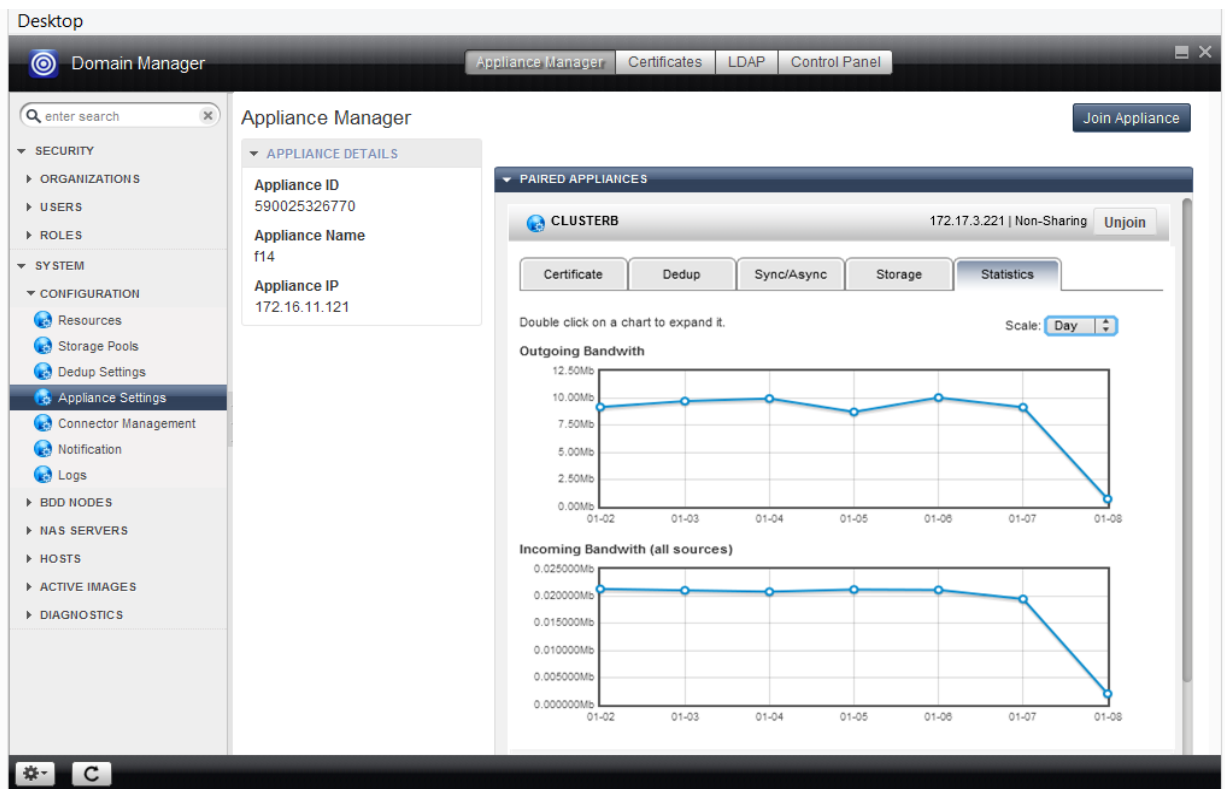
Viewing Bandwidth Usage Statistics

Use the Statistics tab to monitor bandwidth usage.

To view the bandwidth statistics for your Actifio appliances:

1. Open the **Domain Manager** to **System > Configuration > Appliance Settings**. This sequence opens the Appliance Manager page.
2. Select an Actifio appliance from the Navigation pane.
3. Click the **Appliance Manager** tab and then the **Statistics** subtab. A pair of charts appears displaying outgoing and incoming bandwidth consumption statistics for the selected appliance on a time scale that you select.
 - o The **Incoming Bandwidth (All Sources)** graph depicts the incoming traffic reaching the local appliance from all joined appliances.
 - o The **Outgoing Bandwidth** graph depicts the outgoing traffic from the local appliance to the joined appliance.

You can modify the scale by selecting a time unit, such as Day (bandwidth used during the last seven days), Hour (bandwidth used during the last 23 hours), and Minute (bandwidth used in the last 10 minutes). The bandwidth is measured in Mbps.



Viewing Bandwidth Usage Statistics

8 Configuring Appliance Settings

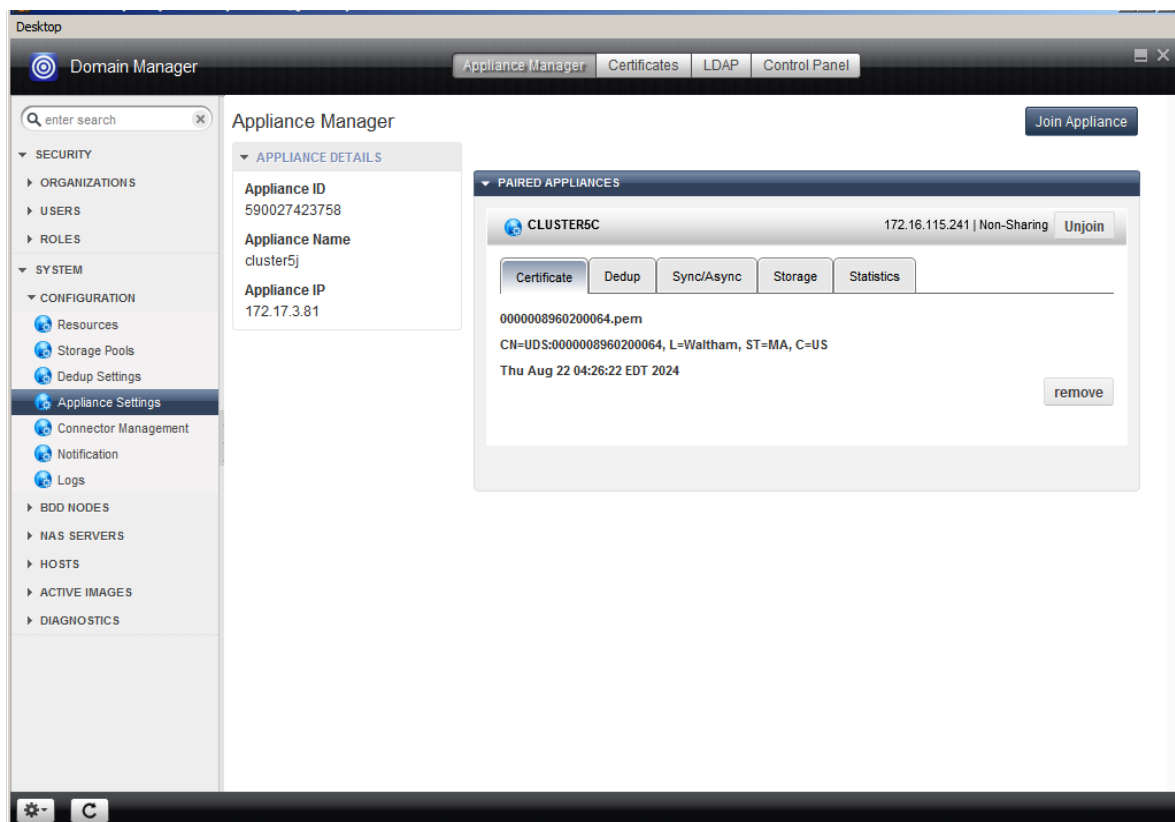
Actifio appliance settings include:

[Managing Security Certificates](#) on page 48

[Configuring LDAP Settings](#) on page 51

[Configuring Control Panel Operations](#) on page 53

Tools for managing multiple appliances by the Appliance Manager are described in [Chapter 7, Managing Appliances](#).



The Appliance Settings of the Domain Manager

Managing Security Certificates

The Actifio appliance uses digital certificates to ensure secure communication between CDS and Sky appliances and where applicable, the Actifio Business Resiliency Cloud. All entities in a configuration must have matching security certificates in order to establish a secured relationship.

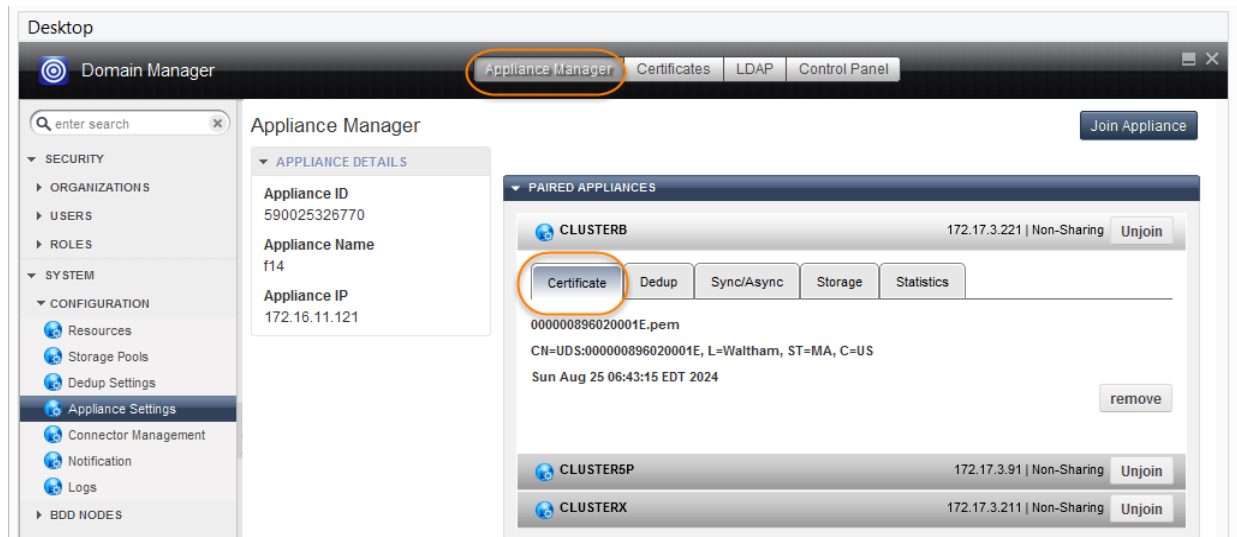
There are two methods to establish a secured relationship between entities:

- Exchange certificates between two entities, as detailed in [Exchanging Certificates](#) on page 50.
- Download a certificate from each appliance and then upload them to the other appliance, as detailed in [Downloading a Certificate](#) on page 49 and [Uploading a Certificate](#) on page 49.

Viewing Certificates

To view the certificate of all entities connected to the local appliance in the sharing or non-sharing mode:

1. Open the **Domain Manager** to **System > Configuration > Appliance Settings**. This sequence opens the Appliance Manager page.
2. Click the **Appliance Manager** tab.
3. Click the **Certificate** subtab. A list of all appliances connected to the local appliance is displayed along with the corresponding certificates.



Viewing Security Certificates

Deleting a Certificate

You may need to delete an existing certificate:

- To disconnect the communication.
- When an existing certificate becomes invalid. In such cases, you may need to remove the old one and upload the new certificate.

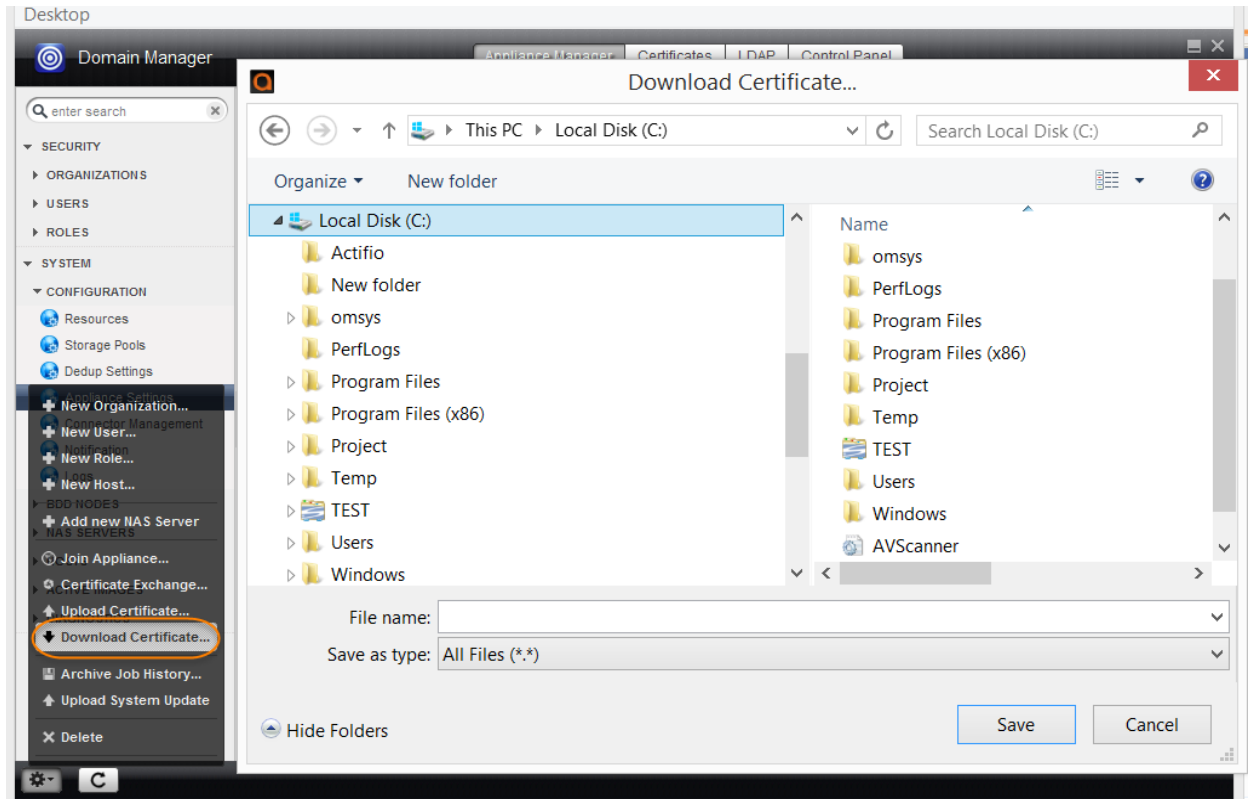
To delete a security certificate:

1. Follow the steps outlined above to view the certificate.
2. Select the certificate and click the **Remove** button.
3. Click **Yes** in the confirmation dialog.

Downloading a Certificate

To download a security certificate:

1. Open the **Domain Manager**.
2. Click **Download Certificates** from the service menu. The Download Certificate window opens:



Downloading a Security Certificate

3. Browse and choose the folder to save the certificate file, and then click **Save**. The certificate is saved in your local system.

Note: To join this appliance to another, you will have to upload this certificate to the other Actifio appliance. Log on to the appliance and perform the steps described in [Uploading a Certificate](#) on page 49.

Uploading a Certificate

To upload a security certificate:

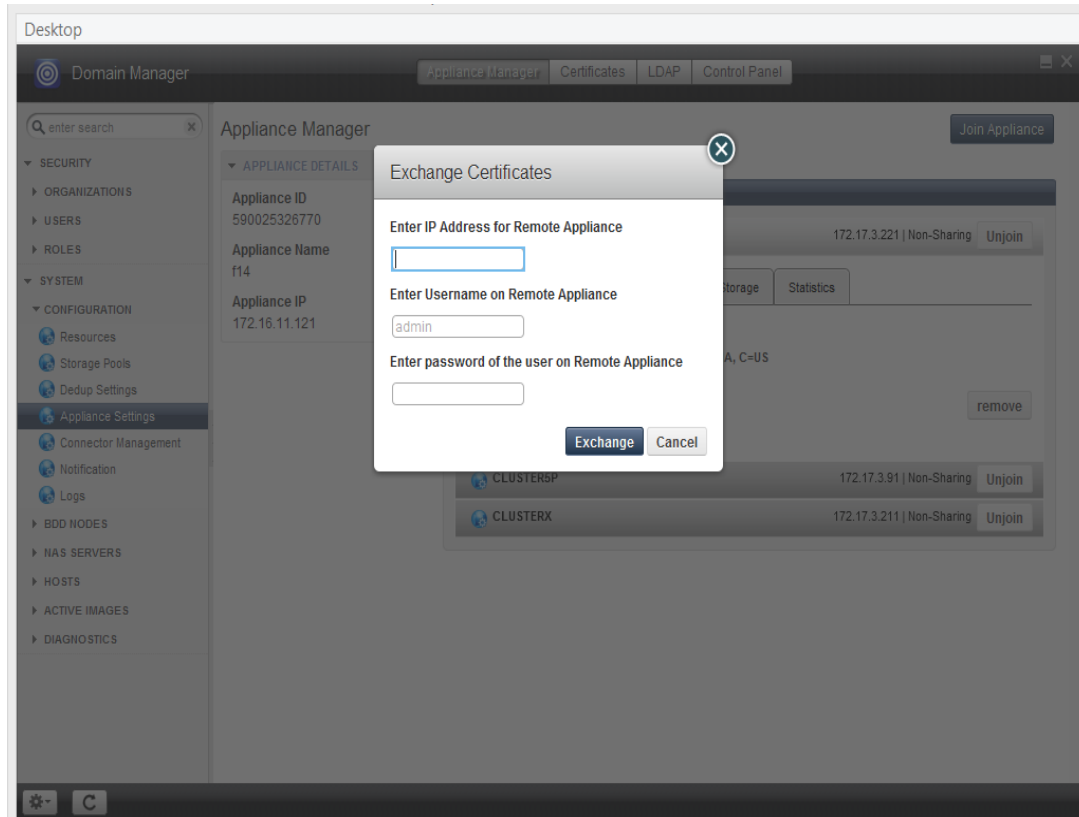
1. Open the **Domain Manager**.
2. Click **Upload Certificates** from the service menu. The **Choose a certificate to import** window opens.
3. Browse and select the certificate file and then click **Open**. The certificate is listed in the certificate store at **Domain Manager > System > Configuration > Appliance Settings > Certificates**.

Exchanging Certificates

Certificate exchange is a quick way to download certificates when you have secure administrative access to both appliances.

To exchange security certificates between two Actifio appliances or where applicable, between an Actifio appliance and the Actifio Business Resiliency Cloud:

1. Open the **Domain Manager**.
2. Click **Certificate Exchange...** from the service menu. The Exchange Certificates dialog opens:



Exchanging a Security Certificate

3. Enter the IP address of the remote appliance, or where applicable, the Actifio Business Resiliency Cloud.
4. In the space provided, enter the Admin password to access the remote appliance or where applicable, the Actifio Business Resiliency Cloud.
5. Click **Exchange**. The security certificates are exchanged between the local appliance and the remote appliance or where applicable, the Actifio Business Resiliency Cloud. Once certificates are exchanged, the local appliance can be joined with the remote appliance or where applicable, the Actifio Business Resiliency Cloud.

Configuring LDAP Settings

You can leverage a single existing LDAP server for Actifio Desktop user authentication and mapping LDAP groups to Actifio appliance roles. To do this, configure the LDAP connection under Domain Manager appliance settings:

1. Open the **Domain Manager** to **System > Configuration > Appliance Settings**.
2. Click the **LDAP** tab. The LDAP Settings panel appears.
3. Check **Use LDAP Authentication** to enable this feature. You can uncheck this at any time without losing the configuration information.
4. Enter **LDAP server IP Address or DNS, Port, Use SSL, BaseDN**, and **Direct Bind** information. Note that the default port value changes if you check or uncheck **Use SSL**.
5. If **Use Direct Bind** is unchecked, you can use the Group Mapping feature described in [Mapping LDAP Groups to Roles](#) on page 52. Enter the **Lookup by Attribute** that the LDAP server uses for login names, and the full **Lookup User DN (Distinguished Name)** and **password** for an LDAP user with rights to do user lookups and mapping.
6. Click **Save**. Optionally you can use the **Test** button to review whether the provided information is accurate.

The screenshot shows the 'Domain Manager' application window. The 'LDAP' tab is selected in the top navigation bar. On the left, a sidebar menu shows 'Appliance Settings' under the 'SYSTEM' section. The main content area is titled 'LDAP Settings' and contains two panels. The 'APPLIANCE DETAILS' panel on the left lists: Appliance ID (590025326770), Appliance Name (f14), and Appliance IP (172.16.11.121). The 'LDAP SETTINGS' panel on the right has the following fields: 'Use LDAP Authentication' (unchecked), 'Server IP / DNS*' (empty text box), 'Port #' (389), 'Use SSL' (unchecked), 'Use cached credentials when directory is unavailable' (unchecked), 'BaseDN*' (empty text box), and 'Use Direct Bind' (checked). At the bottom right of this panel are 'Test' and 'Save' buttons. Below the 'LDAP SETTINGS' panel is a section titled 'LDAP GROUP MAPPING'.

Entering LDAP Connection Information

For more on LDAP authentication, be sure to review *Considerations When Configuring with LDAP* in **Setting Up Users and Roles with the Domain Manager**.

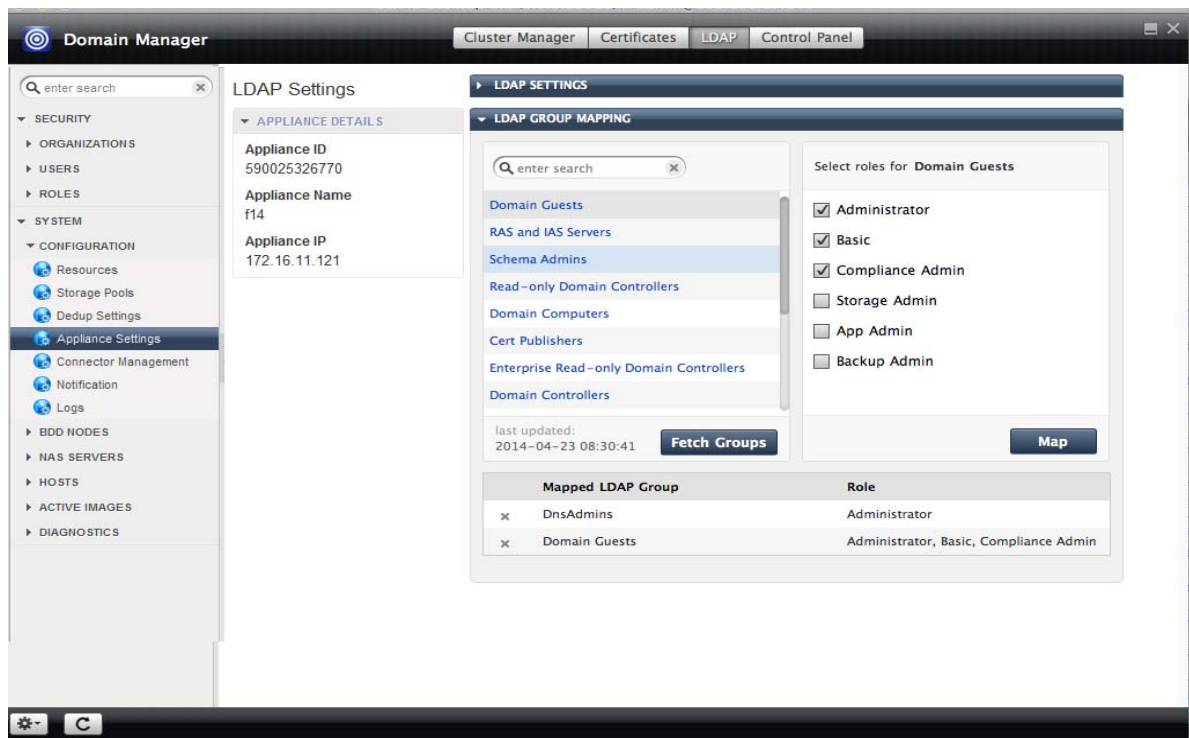
Mapping LDAP Groups to Roles

After your LDAP settings are configured as described in [Configuring LDAP Settings](#) on page 51, you can set up group mapping.

To set up a group mapping:

1. Open the **Domain Manager** to **System > Configuration > Appliance Settings**.
2. Click the **LDAP** tab. The LDAP Settings Panel appears.
3. Click the **LDAP Group Mapping** panel beneath the LDAP Settings panel.
4. The LDAP Group Mapping panel has two lists. Left list contains the LDAP groups, and right list contains Actifio appliance roles. You can use the **Search** field to lookup for a specific group. Click **Fetch Groups** to refresh the LDAP groups list.
5. Select the desired LDAP group from the left list and then select the roles in the right list to map the LDAP group to the role(s), then click **Map**. The mappings appear in a list at the bottom of the LDAP Group Mapping panel.
6. Repeat this process for each group that requires mapping.

Note: Use the “x” icon in the bottom panel to remove mapping.



LDAP Group Mapping

Note: For Active Directory, the Domain Users group is not supported. It will not appear in the list of mappings.

Configuring Control Panel Operations

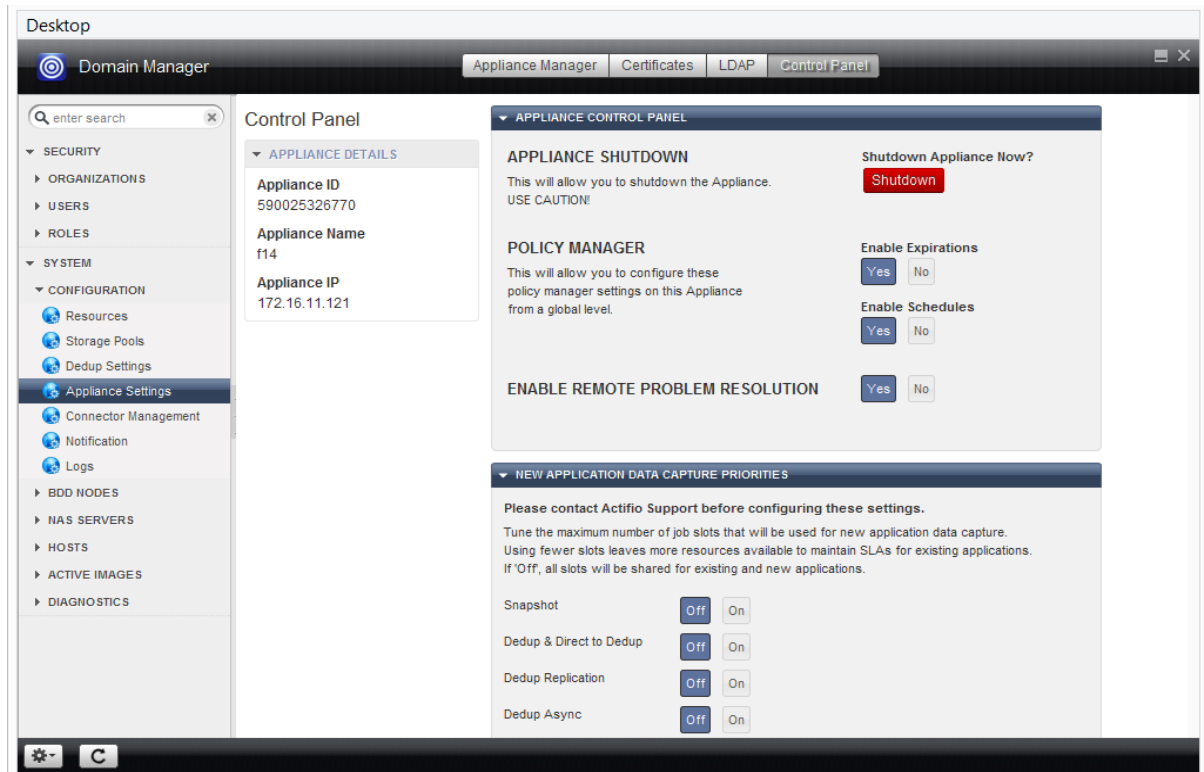
Use the Control Panel for:

[Shutting Down the Appliance](#) on page 54

[Disabling Expirations and Schedules](#) on page 55

[Enabling Remote Problem Resolution](#) on page 56

[Setting Priorities for Ingestion of New Applications](#) on page 57



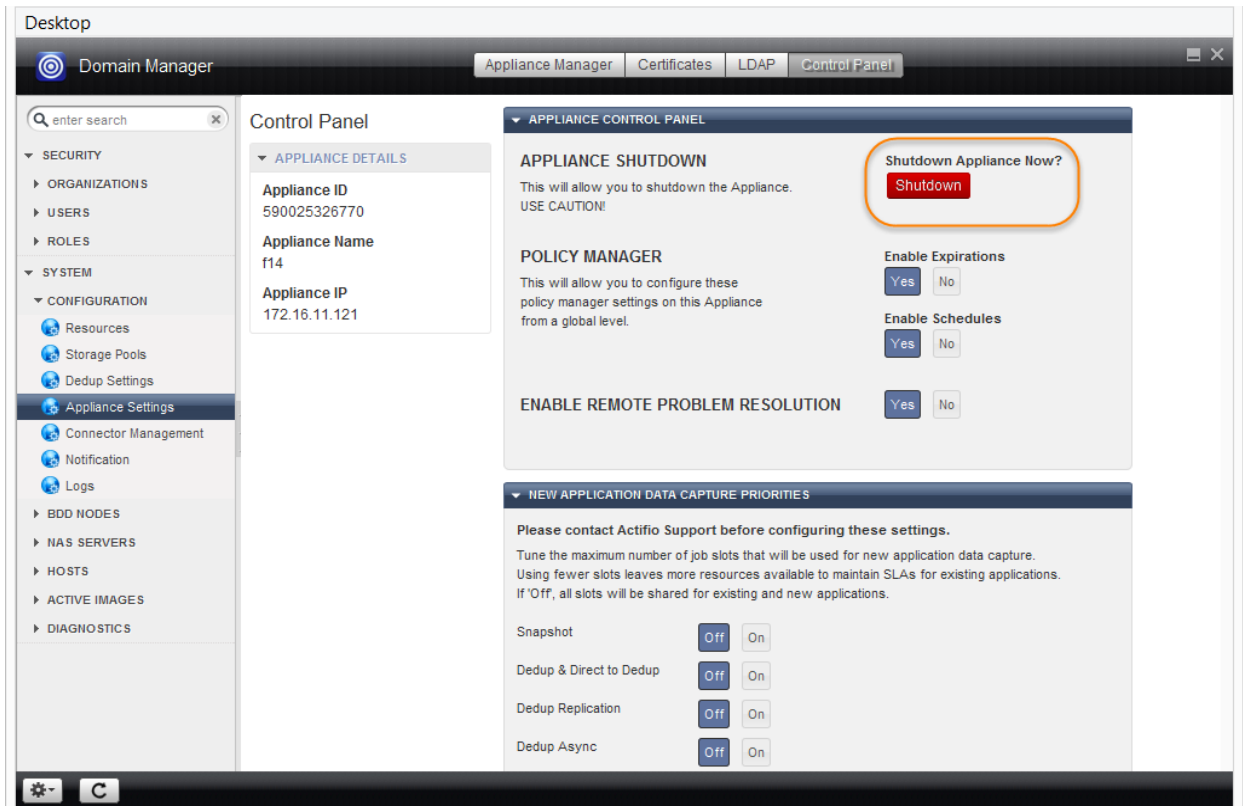
The Control Panel

Shutting Down the Appliance

Note: Shutting down the appliance improperly can result in **data loss**. Shut down the appliance only under the guidance of Actifio Support.

To shutdown the appliance in a controlled manner:

1. Open the **Domain Manager** to **System > Configuration > Appliance Settings**.
2. Click the **Control Panel** tab. The Appliance Control Panel appears.
3. Click **Shutdown**. Complete shutdown takes 10 to 20 minutes.



Appliance Shutdown Procedure

Note: Shutting down the appliance improperly results in **data loss**. Shut down the appliance only from the Control Panel.

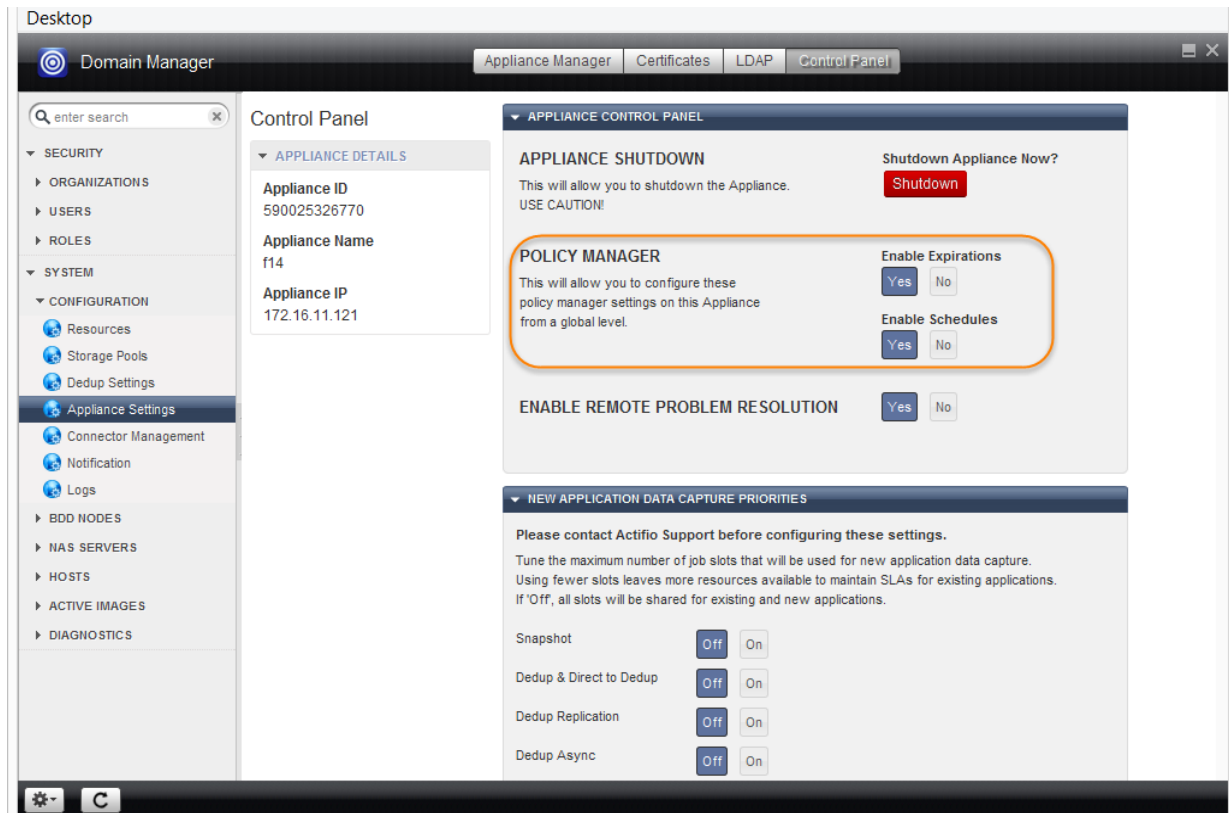
Disabling Expirations and Schedules

Expirations and schedules are not enabled by default. Click **Yes** to enable them. By default, images (backup, dedup, remote-dedup, direct-to-dedup) are expired depending on the policy configuration.

The global configuration set here takes precedence over the individual policy configuration in policy templates. For example, if you configure a policy to expire backup images and then set Enable Expirations to '**No**' using the control panel, the backup images do not expire.

You can save storage by configuring image expiry globally on an Actifio appliance:

1. Open the **Domain Manager** to **System > Configuration > Appliance Settings**.
2. Click the **Control Panel** tab. The Appliance Control Panel appears.



Expirations and Schedules Not Enabled

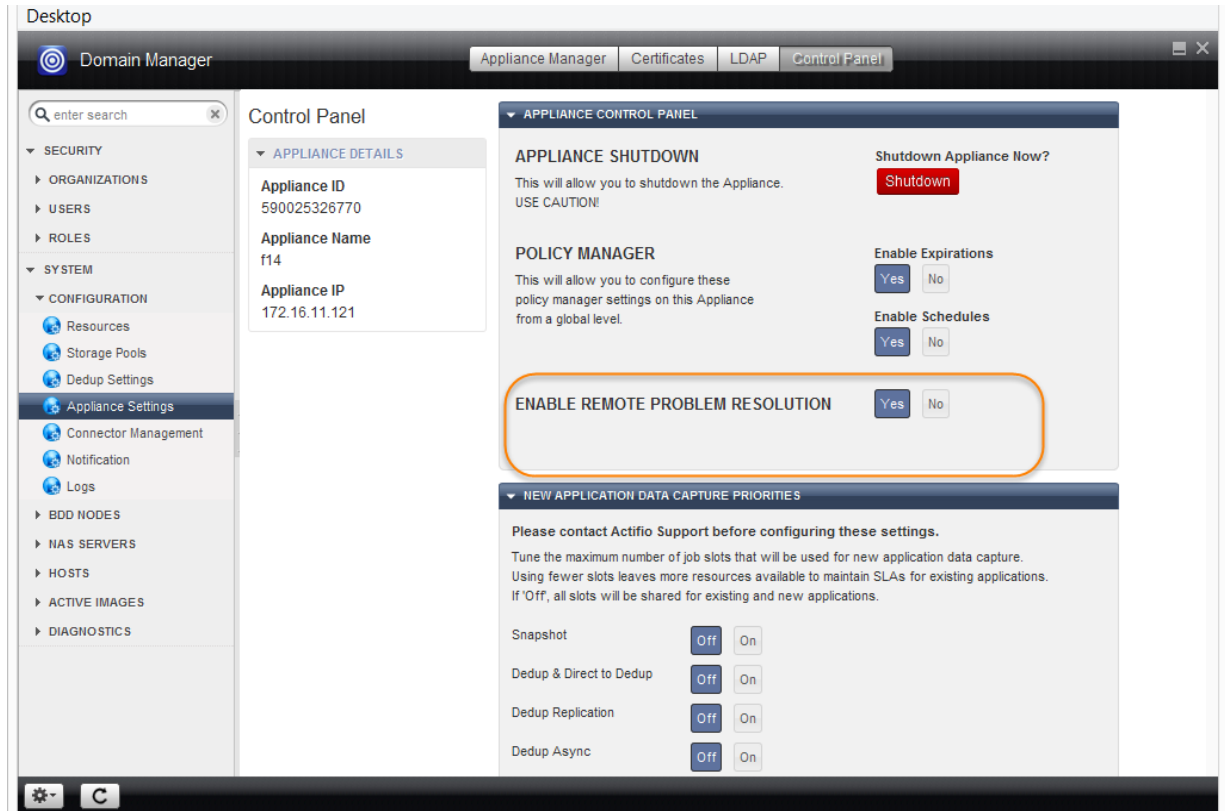
3. Click **Yes** to enable Expirations or Schedules.

Enabling Remote Problem Resolution

Remote Problem Resolution is a feature of Actifio SecureConnect.

To enable Remote Problem Resolution:

1. Make sure **SecureConnect** is enabled under **Software and Settings > System Settings**. You can reach this from the Gear icon in the lower left corner of the Actifio Desktop.
2. Open the **Domain Manager** to **System > Configuration > Appliance Settings**.
3. Click the **Control Panel** tab. The Appliance Control Panel appears.
4. Set **ENABLE REMOTE PROBLEM RESOLUTION** to **Yes**. A dialog opens to confirm the selection.



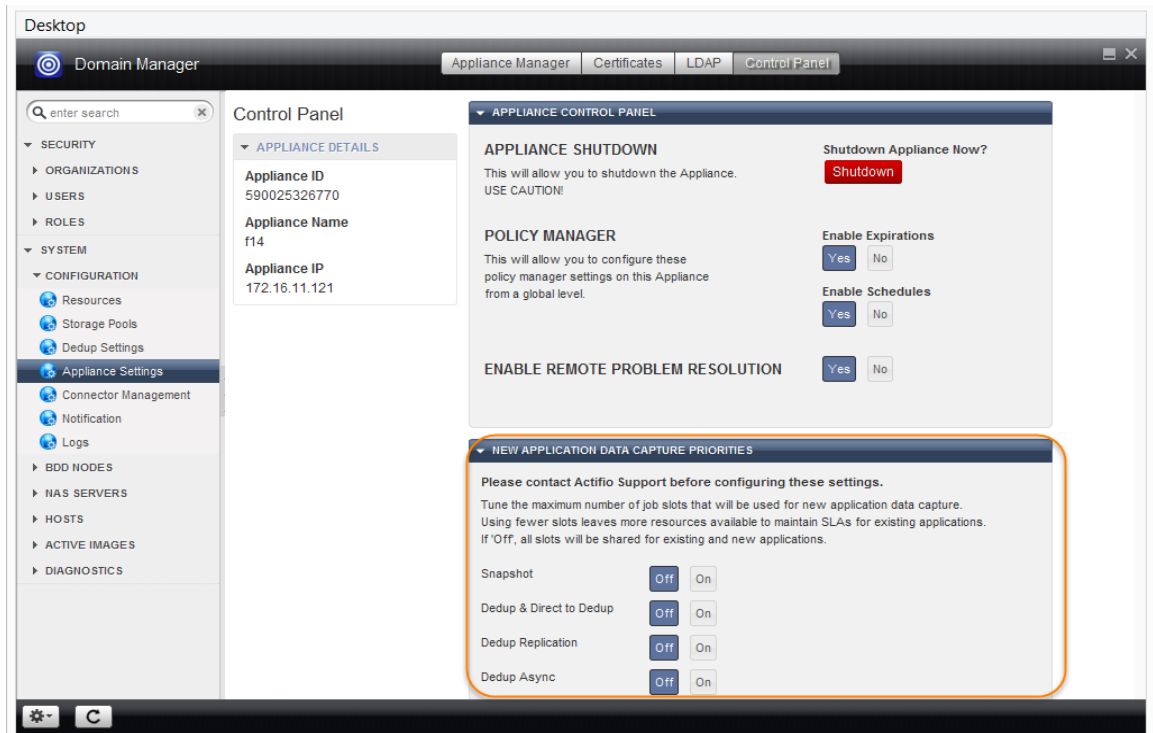
Enabling Remote Problem Resolution

Setting Priorities for Ingestion of New Applications

Use this portion of the Control Panel to optimize your Actifio appliance for capturing new application data. These settings result in a temporary configuration for the Actifio appliance when it must ingest many new applications.

To enable additional job slots for ingestion of new applications:

1. Open the **Domain Manager** to **System > Configuration > Appliance Settings**.
2. Click the **Control Panel** tab. The Appliance Control Panel appears.



Setting Priorities for Capture of New Application Data

3. You can raise, lower, or turn off slots dedicated to capturing new application data. There is a finite number of slots available, so slots assigned here come at the expense of data protection performance.

Note: Do not change the slot assignment values except under the guidance of Actifio Support.

9 Sharing Between Actifio Appliances

The Actifio appliance can support joining any number of appliances at any number of sites, Appliances can be joined in sharing or non-sharing mode.

Note: Before proceeding to [Chapter 10, Configuring Shared Appliances](#), be sure to read [Sharing Mode](#) on page 60 and [Non-Sharing Mode](#) on page 61 in this chapter.

Appliance Topology: Sharing and Peer Relationships

You can join Actifio appliances in two modes:

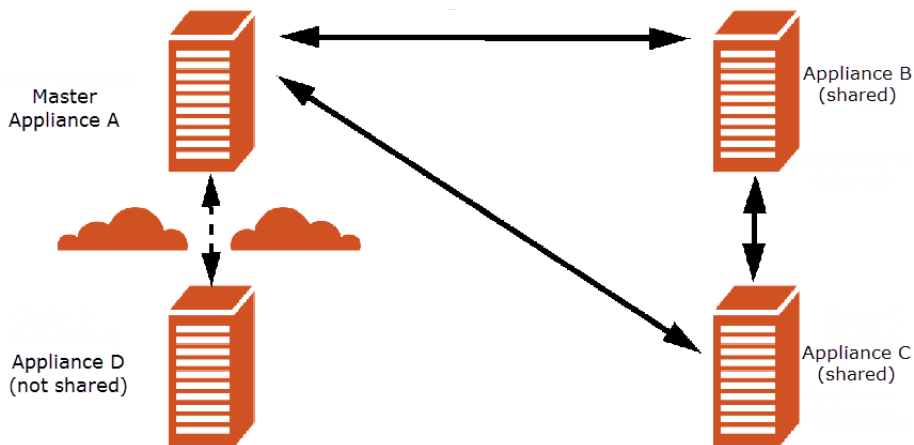
Sharing mode: Use this mode to share:

- o Protected applications
- o Security settings: Organizations, Users, and Roles
- o Policy Templates (but not Resource Profiles)

Sharing mode is described in [Sharing Mode](#) on page 60. The procedure for joining appliances in sharing mode can be found at [Joining in Sharing Mode](#) on page 65.

Non-sharing mode: Use this mode when you want appliances to perform remote backups for each other, for failover, and for dedup-async replication. Non-sharing mode is described in [Non-Sharing Mode](#) on page 61. The procedure for joining appliances in non-sharing mode are in [Joining in Non-Sharing Mode](#) on page 66. This mode is always used for those Actifio appliances that connect to the Actifio Business Resiliency Cloud.

You can use both types of relationships within your enterprise. For example, you might use three joined sharing-mode appliances for day-to-day data protection, and a non-shared appliance for off-site disaster recovery.

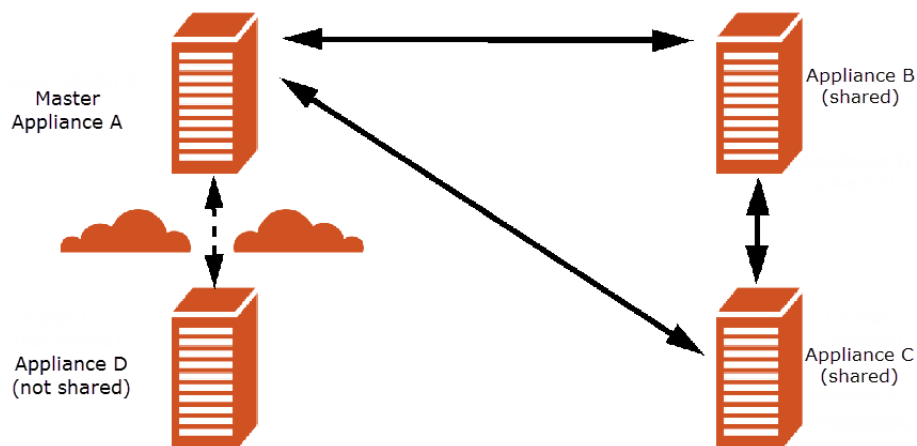


Appliances A, B, and C are Shared for Daily Operations; Remote Appliance D is for Disaster Recovery

Sharing Mode

When B joins A, the latter becomes the master and B, the slave.

- There can be only one master appliance in an Actifio appliance domain. There can be any number of slaves.
- Masters are made, not born. The act of joining in shared mode creates the master-slave relationship. Sharing mode makes a slave of the appliance that joins. In the diagram above appliance B joined appliance A in sharing mode. At that moment appliance B became the slave and appliance A became the master. The slave joins the master.
- A master appliance, which is already in sharing mode (that's why it's a master) cannot join any other appliance, because it would become a slave; once the master, always the master.
- All slave appliances are peers to each other.
- An Actifio appliance can join any appliance in non-sharing mode. Non-shared appliances are peers to all appliances.
- An Actifio appliance cannot join a slave appliance. In the diagram above appliance D cannot join appliance C or appliance B. Appliance D can join appliance A in the sharing or non-sharing mode.



Master Appliance A Shares Rules with Slave Appliances B & C, but Not Remote Appliance D

When Appliance B is joined to Appliance A:

- If Appliance B has no protected applications, and no users, roles, organizations, and policy templates defined, then Appliance B gets users, roles, organizations, and policy templates shared from A, but no applications.
- If Appliance B has users, roles, policy templates, and organizations defined, they are deleted and replaced by those shared from Appliance A.
- If Appliance B has protected applications, they are preserved, but they are protected by the policy templates shared from Appliance A.
- If Appliances A and B both do not contain protected applications, users, roles, policy templates, and organizations, then when Appliance B is joined to Appliance A, no obvious changes occur. However, once you create users, roles, organizations, and policy templates on Appliance A, they are shared with Appliance B.

Non-Sharing Mode

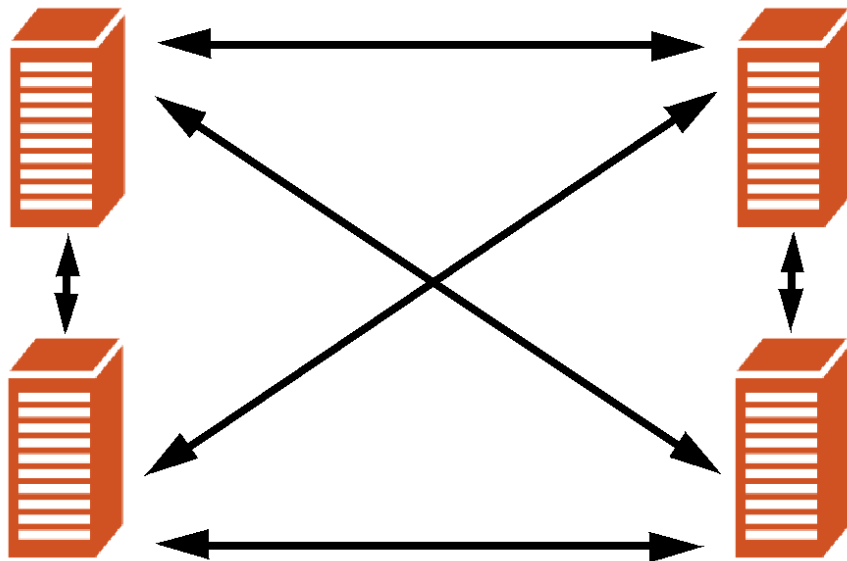
Two appliances that belong to different Actifio appliance domains can be joined in non-sharing mode. You can join:

- One appliance with another appliance to enable replication from the former to the later.
- One appliance with two appliances to enable different applications to replicate to separate appliances.
- Two appliances with one appliance to let the later act as a target for replication.

Note: Non-sharing mode is always used for those Actifio appliances that connect to the Actifio Business Resiliency Cloud.

Non-sharing mode makes peers of the appliances that are joined. When two appliances join in the non-sharing mode, each appliance can be the destination for remote replication of data from the other appliance.

In the non-sharing mode, each appliance uses its own users, policies, templates, and organizations and protects only the applications assigned to it; peer appliances do not share users, policies, templates, and organizations.



The Master Appliance Shares Users and Policy Templates with Slave Appliances

The types of replications supported by Actifio appliance are given below. All of these replications can use the appliance setup described above.

- Synchronous replication from the primary appliance to a remote appliance.
- Asynchronous replication from the primary appliance to a remote appliance.
- Asynchronous replication of deduped data from the primary appliance to a remote appliance.
- Remote deduplication replication from the dedup pool of the primary appliance to a remote appliance.

10 Configuring Shared Appliances

Actifio appliances can stand alone or be joined to additional appliances for disaster recovery and business continuity purposes at the same site or at different sites. Actifio appliances can be joined in Sharing Mode and in Non-Sharing Mode.

Note: Before performing the joined and shared appliance procedures outlined in this chapter, be sure to read [Sharing Mode](#) on page 60 and [Non-Sharing Mode](#) on page 61 in Chapter 9, [Sharing Between Actifio Appliances](#).

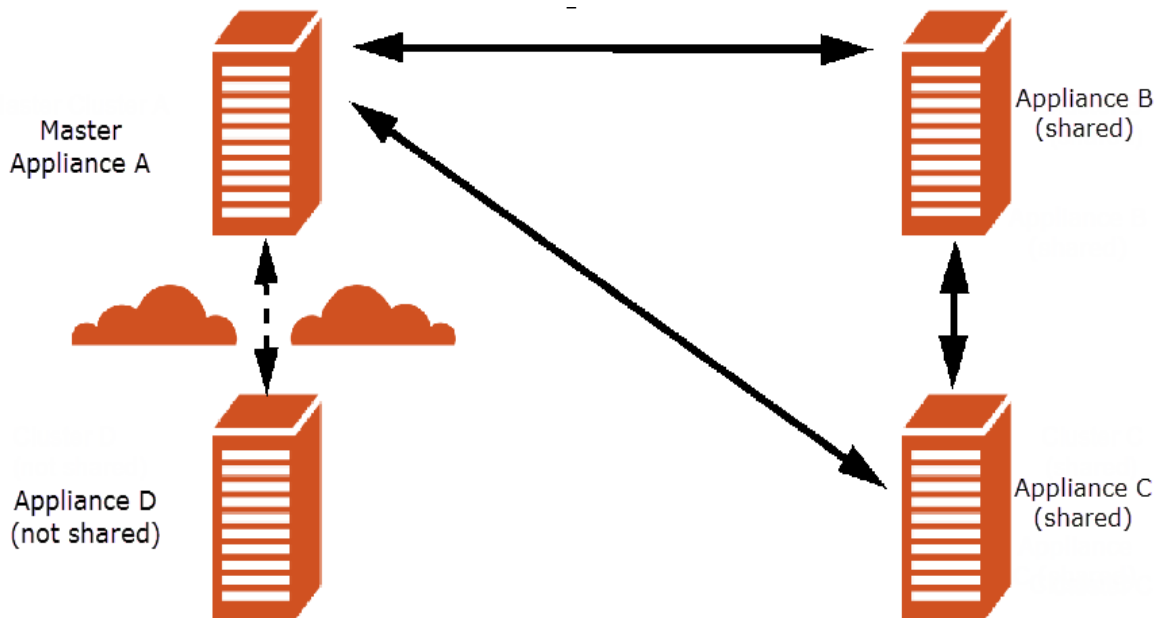
This section describes:

[Viewing Details of Joined Appliances](#) on page 64

[Unjoining Appliances](#) on page 64

[Joining in Sharing Mode](#) on page 65

[Joining in Non-Sharing Mode](#) on page 66

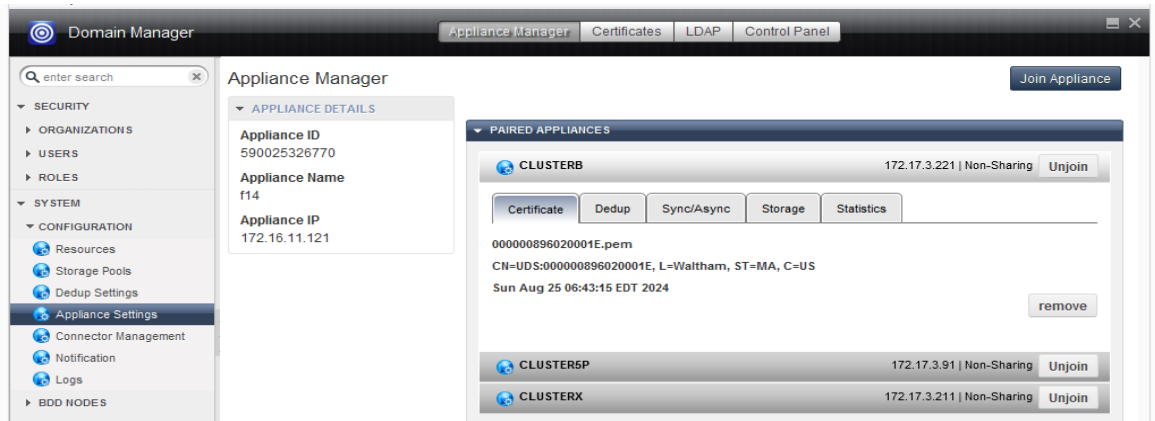


Example Appliance Topology

Viewing Details of Joined Appliances

To view the list of Actifio appliances and their details:

1. Open the **Domain Manager** to **System > Configuration > Appliance Settings**. A list of Actifio appliances joined to the local appliance and their certificates is displayed. A master appliance has all the other appliances in the sharing mode.



Viewing Details of Joined Appliances

2. If an Actifio appliance is the master of a domain, it is listed as Sharing.

Unjoining Appliances

Note: Prior to deleting a joined appliance, ensure that running jobs are not using the remote appliance.

When you delete a joined appliance:

- The certificates that were exchanged when joining the appliances are deleted.
- Jobs in progress change to Stalled status and the jobs are displayed as **Stalled** by the System Monitor.

To delete a joined appliance:

1. Open the **Domain Manager** to **System > Configuration > Appliance Settings**. A list of joined appliances is displayed.
2. Click **Unjoin** against the appropriate appliance.

Note: If an Actifio appliance is in use in any Resource Profile, then the unjoin process will fail.

Joining in Sharing Mode

The following are step-by-step instructions for joining appliances in sharing mode. For details on Sharing Mode see [Sharing Mode](#) on page 60.

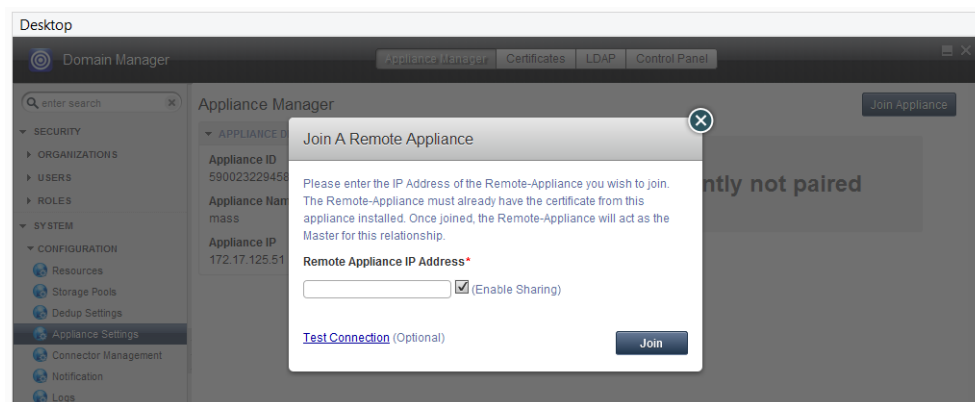
To join in Non-Sharing Mode, see [Joining in Non-Sharing Mode](#) on page 66.

Note: The local appliance shares the rules with the joined remote appliance.

To join local appliance A to remote appliance B:

Note: Before joining, ensure certificates have been exchanged between appliances. See [Exchanging Certificates](#) on page 50 for details.

1. Open the **Actifio Desktop** on **Appliance B**.
2. Open the **Domain Manager**.
3. On Appliance B, click **Domain Manager > Appliance Settings** and click the **Join Appliance** button. The **Join a Remote Appliance** window appears.
4. Enter the IP address of Actifio appliance A in **Remote Appliance IP Address**.
5. Select **Enable Sharing** to use the remote Appliance A as the master appliance. When you select this option, the remote appliance's users, roles, templates, and organizations replace those on Appliance B.
6. Click **Join**. On successful configuration Appliance B appears connected to the Appliance A.



Sharing Mode

7. If you have joined Actifio CDS appliances, set up partnerships between the local and the remote appliances as explained in [Enabling/Disabling Sync/Async Replication](#) on page 43.

Joining in Non-Sharing Mode

The following are step-by-step instructions for joining appliances. and where applicable the Actifio Business Resiliency Cloud in non- sharing mode. For details on Non-Sharing Mode, see [Joining in Non-Sharing Mode](#) on page 66.

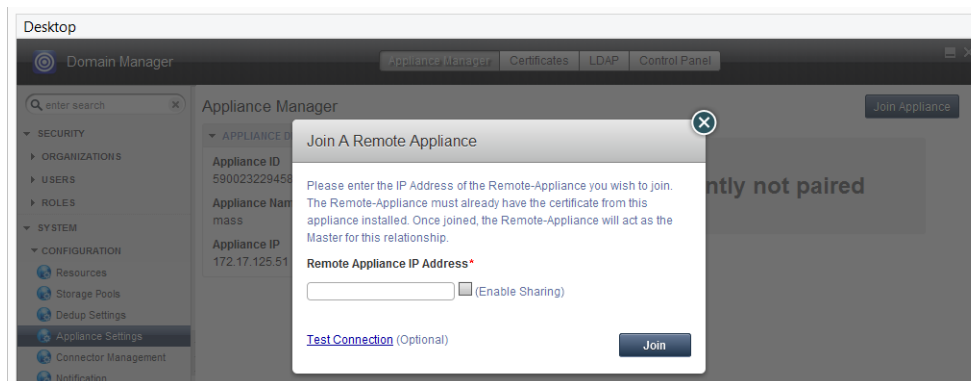
To join in Sharing Mode, see [Joining in Sharing Mode](#) on page 65.

Note: Non-sharing mode is always used for those Actifio appliances that connect to the Actifio Business Resiliency Cloud.

To join the local appliance A and the remote appliance B or where applicable, the local appliance A with the Actifio Business Resiliency Cloud:

Note: Before joining, ensure certificates have been exchanged. See [Exchanging Certificates](#) on page 50 for details.

1. Open the **Actifio Desktop** on **appliance A**.
2. Open the **Domain Manager**.
3. Exchange certificates as described in [Exchanging Certificates](#) on page 50.
4. Click **Domain Manager > Appliance Settings > Join Appliance**. The **Join a Remote Appliance** window appears.
5. In the space provided, enter the IP address of the remote Actifio appliance B, or where applicable, the IP address of the Actifio Business Resiliency Cloud.
6. Do **NOT** check Enable Sharing. The appliances will be joined for purposes of sharing protected applications, but each will use its own users, roles, and organizations and its own policy templates and resource profiles.
7. Click **Join**. On successful configuration appliance B appears connected to the appliance A.



Non-Sharing Mode

8. If you have joined Actifio CDS appliances, set up partnerships between the local and the remote appliances as explained in [Enabling/Disabling Sync/Async Replication](#) on page 43.

11 Maintaining Connectors on Hosts

The Actifio Connector is a small-footprint lightweight process installed on hosts to provide advanced data protection and restoration capabilities using the Actifio appliance. The Actifio Connector enables the appliance to discover supported applications on host machines.

Note: *To protect an entire VMware VM an Actifio appliance makes calls to VMware APIs. To protect an entire Hyper-V VM, you must install the Actifio Connector on the VM's Hyper-V Server.*

The Actifio Connector:

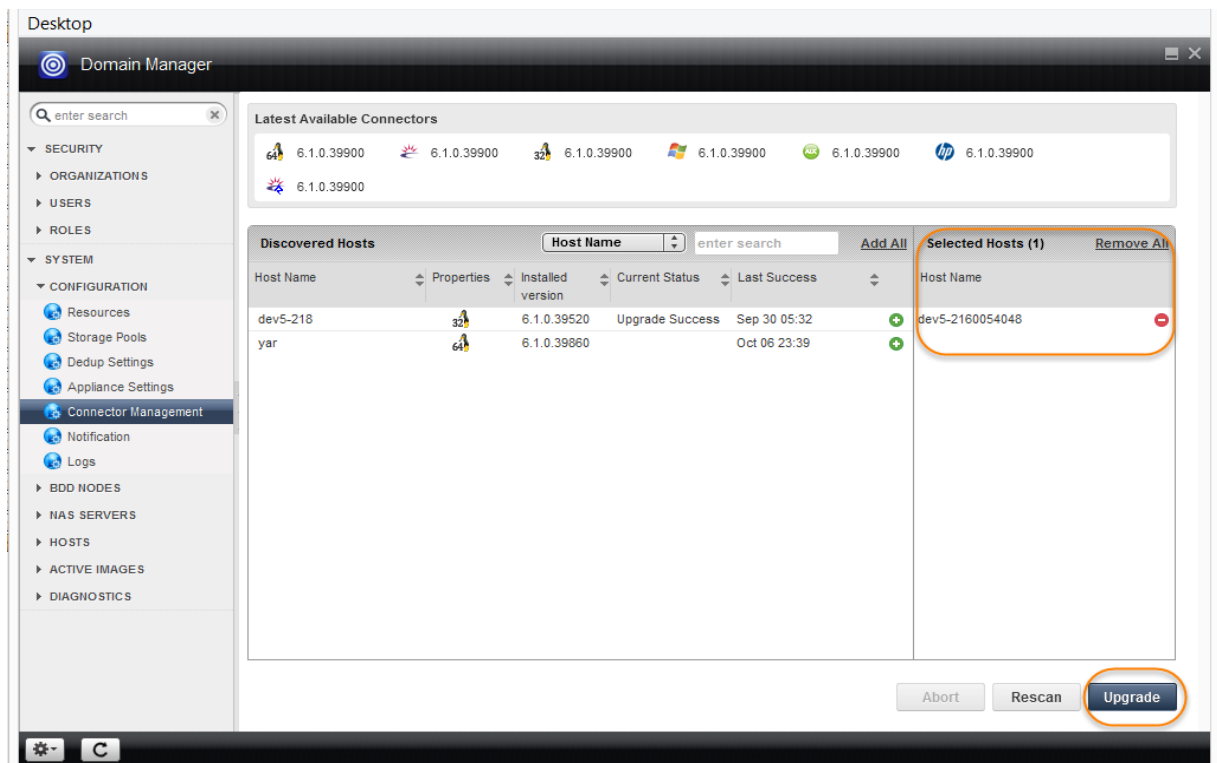
- Enables the Actifio appliance to discover supported applications on host machines.
- Quiesces an application on a host machine before backing up to ensure an application-consistent backup.
- Truncates the logs of an application on application hosts after a backup.
- Rescans storage buses, brings new devices on-line, assigns drive letters, imports volume groups, and mounts file systems, based on the operating system of the application host.
- Prepares application volumes for a restore operation.
- Enables directory and file browsing, and packages the selected files into a ZIP archive when restoring one or more files from a mounted backup.

These functions are detailed in **The Actifio Connector** in your Actifio Documentation Library.

Using the Connector Manager

Use the Connector Manager to update the Actifio Connectors on your discovered hosts:

1. Open the **Domain Manager** to **System > Configuration > Connector Management**. This sequence opens the Connector Manager. Here you can see each of your hosts and the Actifio Connector installed on each.
2. From the Discovered Hosts pane on the left, select which hosts are to get upgraded connectors by clicking on their green + icons. This action moves them to the Selected Hosts pane on the right. Once there, a red - icon allows you to remove them back to the Discovered Hosts list. Grayed-out hosts are those with the Actifio PAS 5.x Connectors; these are not supported by the Connector Manager.
3. Click **Upgrade** to upgrade the Connector on the selected hosts.
4. Select an upgrade option:
Start Upgrade: Starts the upgrade. The upgrade will fail if there are jobs running on the selected host.
Force Upgrade: Attempts to cancel running jobs and upgrades immediately.
5. Click **Submit**.

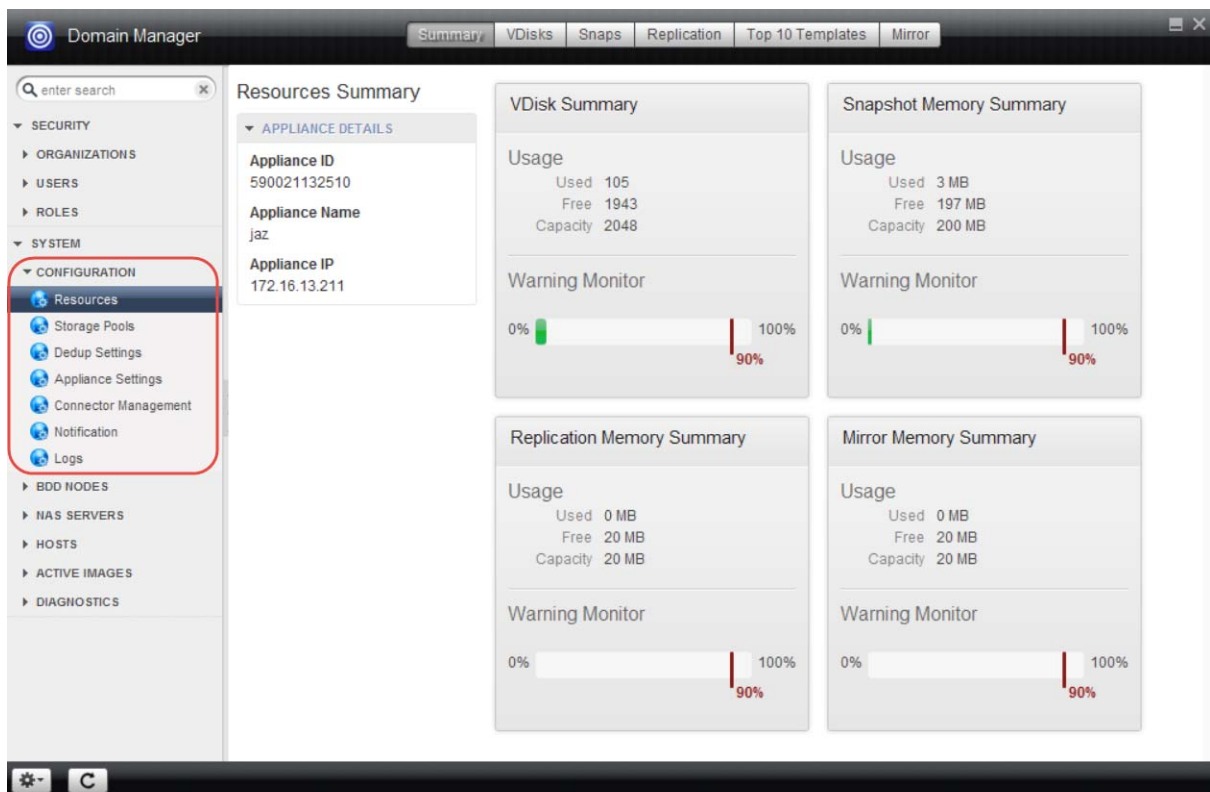


The Connector Manager Showing Two Hosts to Receive Connector Upgrades

12 Overview of Configuration Tools

Configuration tools in the System function of the Domain Manager include:

- [Resources](#) on page 70
- [Storage Pools](#) on page 71
- [Dedup Settings](#) on page 72
- [Appliance Settings](#) on page 73
- [Connector Management](#) on page 74
- [License Management](#) on page 75
- [Notification](#) on page 76
- [Logs](#) on page 77

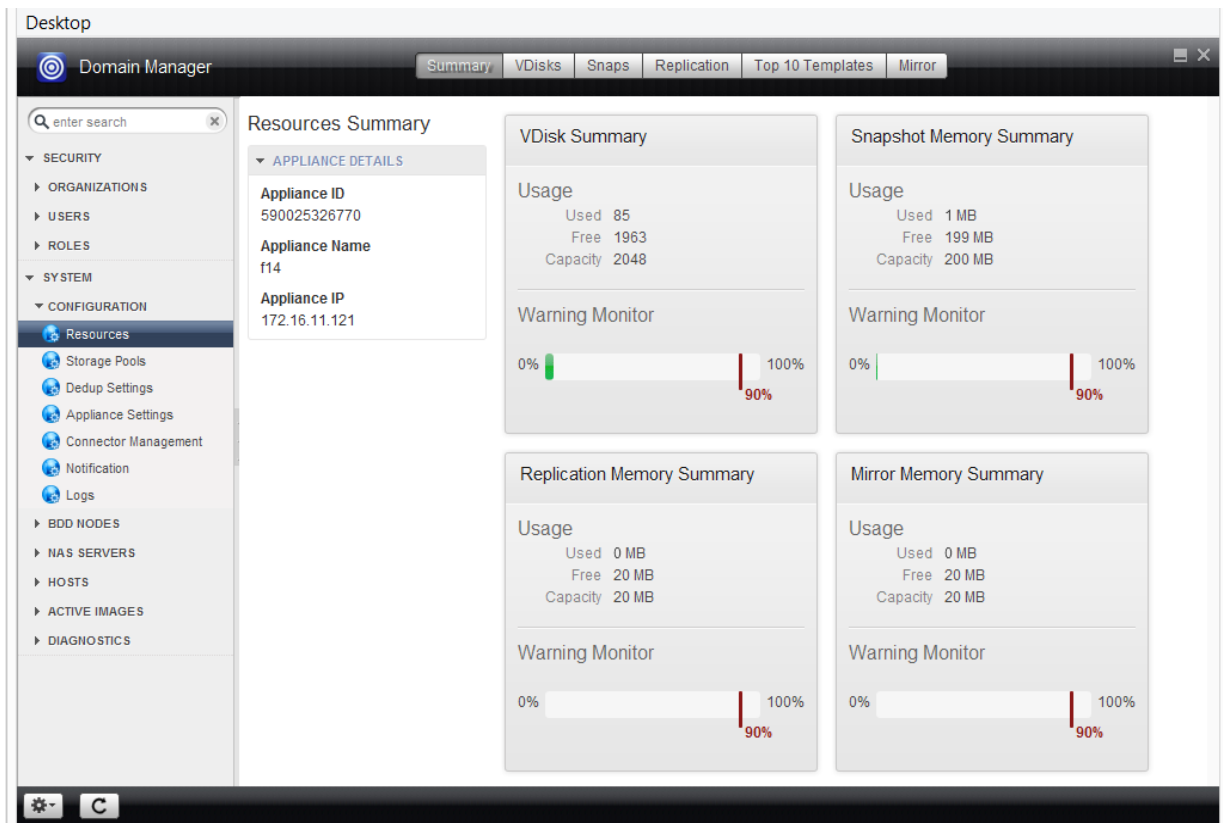


The Configuration Section of the Domain Manager's System Section

Resources

Use the Resources tool to view storage resources, and to set resource limits, and warning thresholds.

Resources tools are detailed in [Chapter 2, Monitoring Resource Usage](#).



The Resources Summary of the Domain Manager

Storage Pools

Use the Storage Pools tool to view the storage pools, and to set resource limits, and warning thresholds.

Storage pools are detailed in [Chapter 4, Configuring Storage Pools](#).

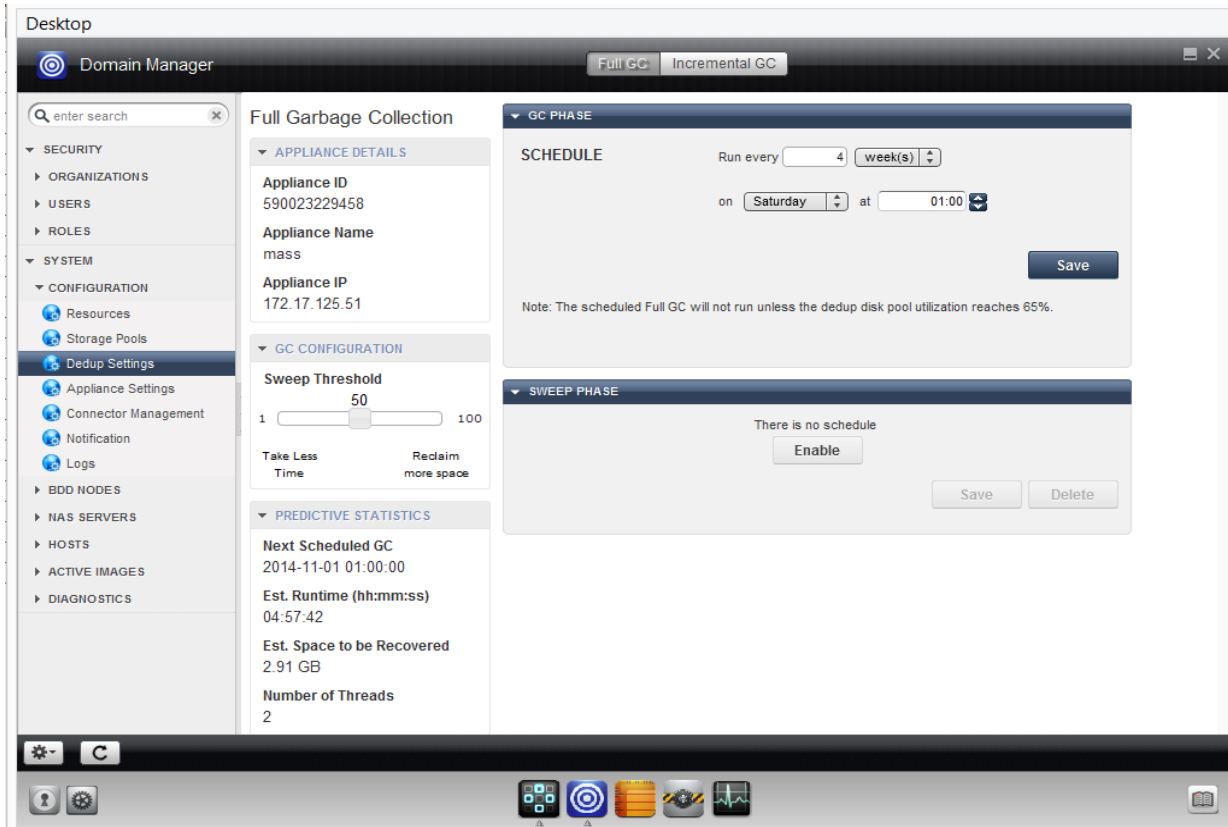


The Storage Pools Summary of the Domain Manager

Dedup Settings

The amount of storage consumed by the dedup store grows over time, depending on the amount of unique data added with each new image that is ingested. As each image is expired, the space occupied by the unique data that was represented by that image is not immediately reclaimed. The garbage collection process identifies (and later reclaims) space occupied by this no-longer-needed data. The Dedup Settings page is where you configure Garbage Collection.

The Dedup pool is introduced in [Chapter 5, Understanding Dedup Pools](#), and dedup garbage collection is detailed in [Chapter 6, Configuring Dedup Garbage Collection](#).

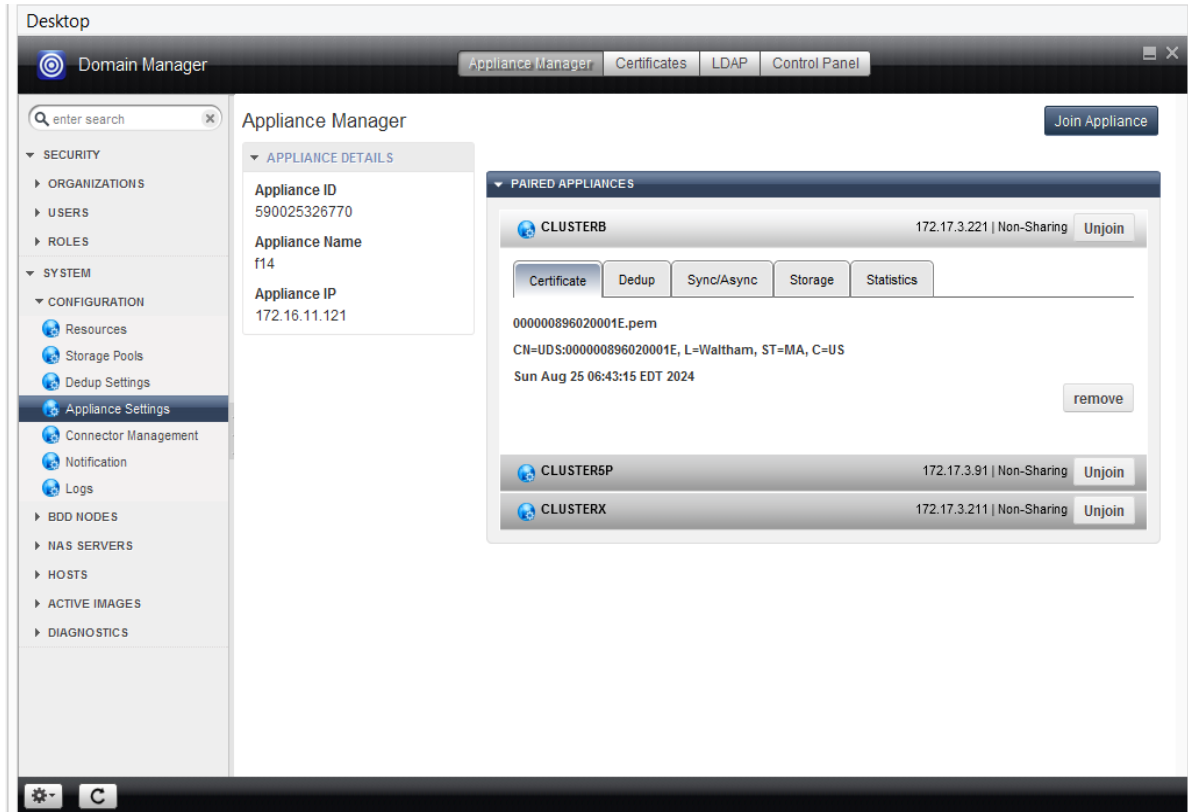


The Dedup Storage Summary of the Domain Manager

Appliance Settings

Use the Appliance Settings tools to add appliances, join them together, and perform other configuration and maintenance tasks on your Actifio appliances.

Appliance settings are detailed in [Chapter 8, Configuring Appliance Settings](#), and the tools for managing multiple appliances are described in [Chapter 7, Managing Appliances](#).

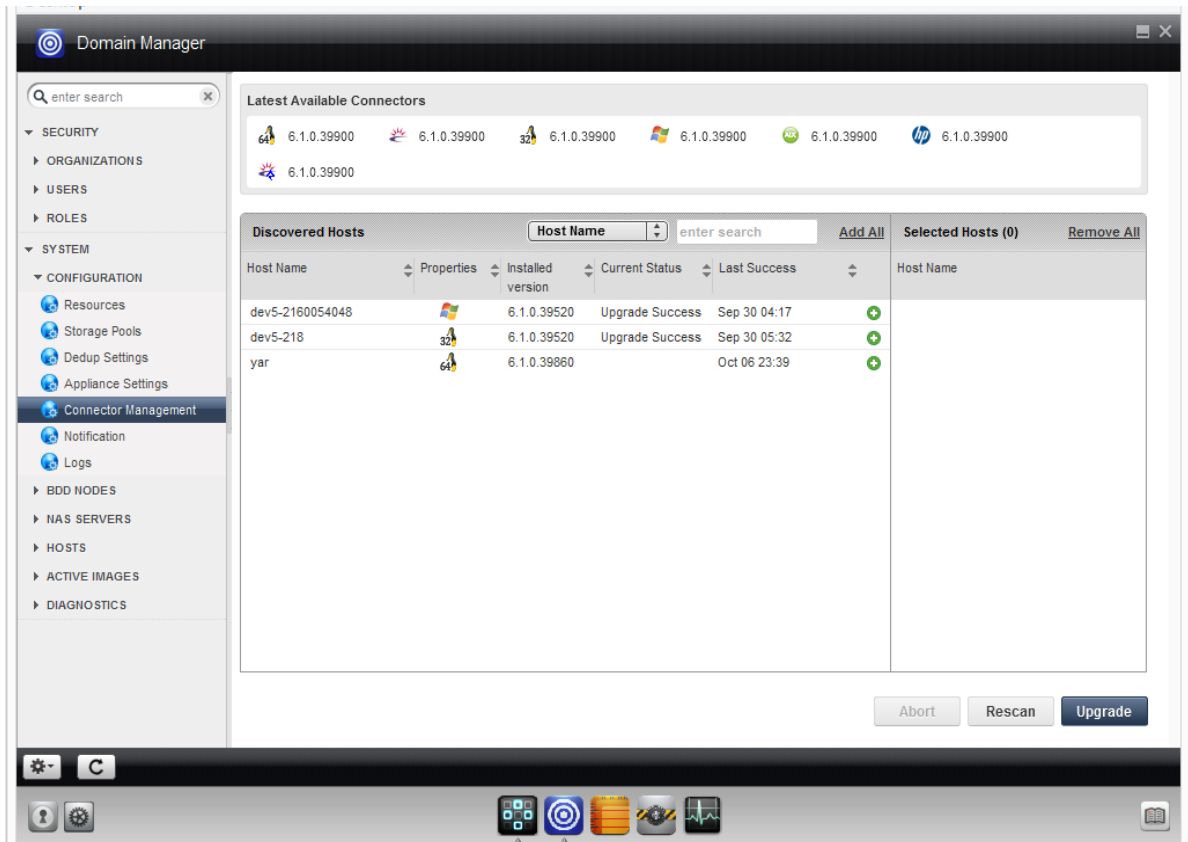


The Appliance Settings Summary of the Domain Manager

Connector Management

Use this tool to upgrade the Actifio Connector on your hosts.

Connector management is detailed in [Chapter 11, Maintaining Connectors on Hosts](#).



The Actifio Connector Manager

License Management

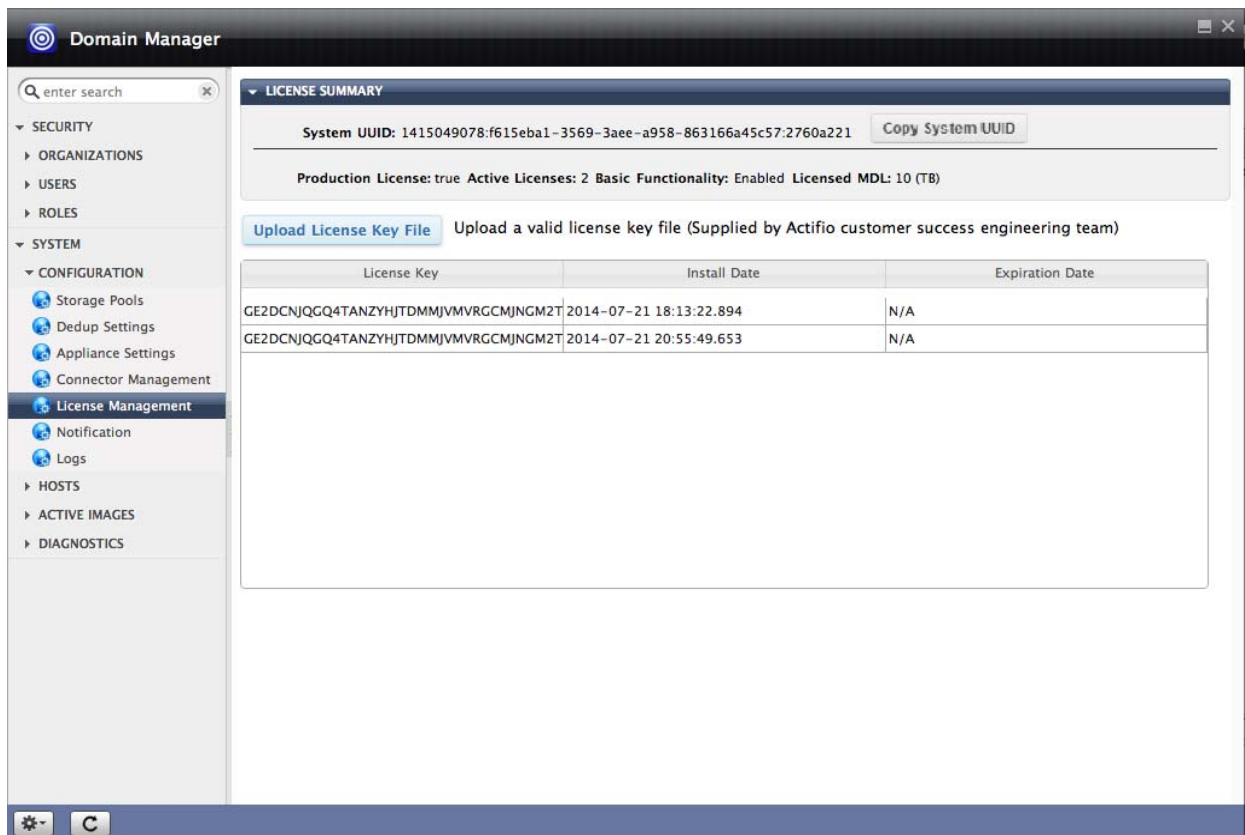
Use this tool to manage your Actifio Sky appliance licenses.

Note: Licensing is not applicable to Actifio CDS appliances

Use the License Manager to upload:

- An evaluation-to-production license key if you intend to upgrade from the 30-day full-feature evaluation version of the base Actifio appliance software to the production version.
- An add-on functionality license key (for example, to add support for protecting Oracle databases).

Actifio Sky appliance license management is detailed in [Chapter 13, Managing Licenses for a Sky Appliance](#).



The License Manager

Notification

You can configure an SNMP (Simple Network Management Protocol) trap receiver as the target of SNMP traps generated by the Actifio CDS or Sky appliance. You can also configure email notification to inform administrators when events of selected severity occur.

Notifications are detailed in:

[Chapter 14, Alerting](#)

[Chapter 15, Collecting Alerts from Actifio Storage and Switches](#)

[Chapter 16, Sending Alerts from the Actifio Appliance](#)

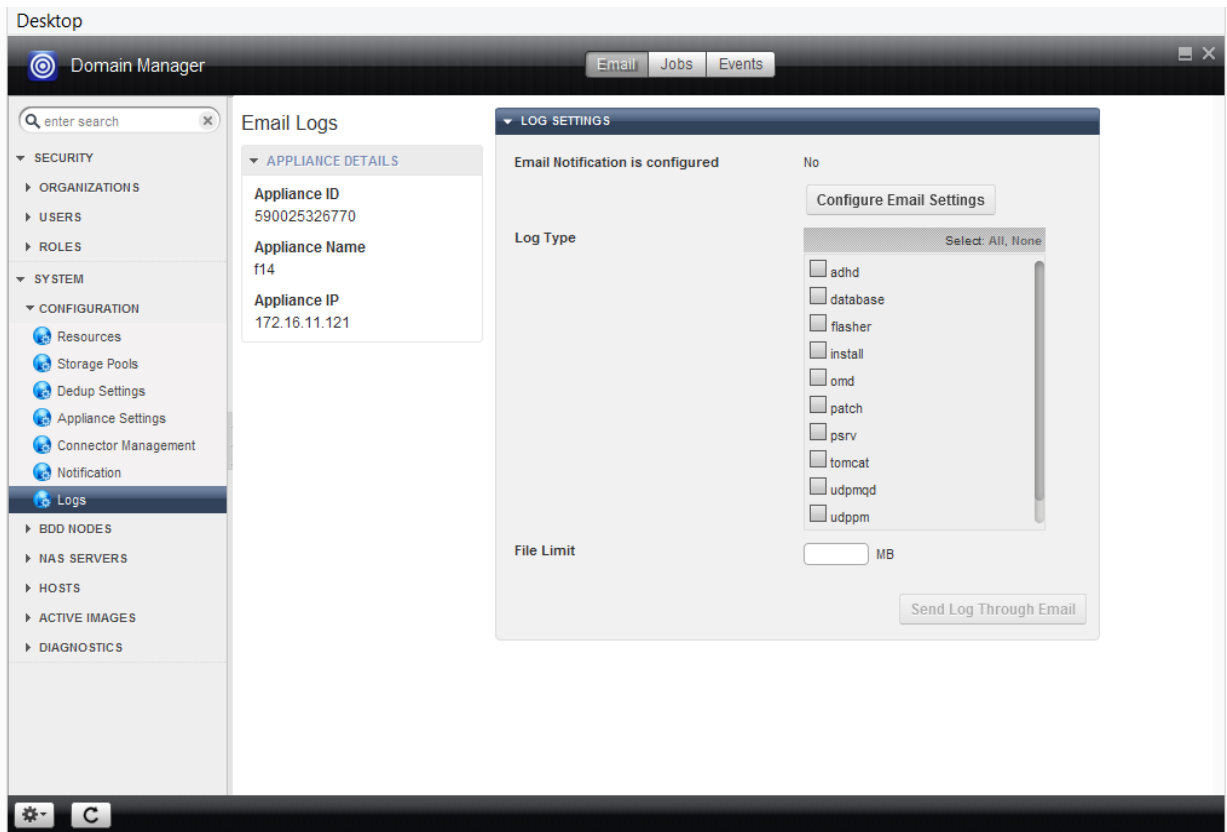
The screenshot displays the 'Domain Manager' web interface. The top navigation bar includes 'EMAIL' and 'SNMP' tabs. The left sidebar contains a search bar and a tree view with categories: SECURITY (ORGANIZATIONS, USERS, ROLES), SYSTEM (CONFIGURATION: Resources, Storage Pools, Dedup Settings, Appliance Settings, Connector Management, Notification, Logs; BDD NODES; NAS SERVERS; HOSTS; ACTIVE IMAGES; DIAGNOSTICS). The 'Email Configuration' page is active, showing 'APPLIANCE DETAILS' for Appliance ID 590025326770, Appliance Name f14, and Appliance IP 172.16.11.121. The main form has tabs for SMTP Server, Event Notification, Call Home, and Switches & Storage. The SMTP Server tab is selected, showing fields for Server Name/IP*, Port* (with a 'Use SSL' checkbox), Host Name, Email*, Password*, and Message Limit (with a 'MB' dropdown). 'Test Email' and 'Save' buttons are at the bottom right.

Domain Manager Notifications

Logs

Use the Logs tool to send Actifio appliance statistics and logs to the Actifio support team.

Logs are detailed in [Chapter 17, Sending Logs to Actifio Support](#).



The Domain Manager Logs Section

13 Managing Licenses for a Sky Appliance

The Actifio License Manager is unique to Actifio Sky appliances. During your initial software installation, a license is installed to register the Actifio Sky software. The registration of your Actifio Sky software is based on a unique 128-bit system UUID. After installation, you then use the License Manager when you need to upload:

- An evaluation-to-production license key if you intend to upgrade from the 30-day full-feature evaluation version of the base Actifio Sky software to the production version.
- An add-on functionality license key (for example, to add support for protecting Oracle databases).

This chapter describes:

[Ordering a License](#) on page 79

[Uploading a License Key](#) on page 80

[Copying the System UUID Value](#) on page 83

Ordering a License

To order a Actifio Sky license from an Actifio representative:

1. Contact your Actifio representative to order a Actifio Sky license.

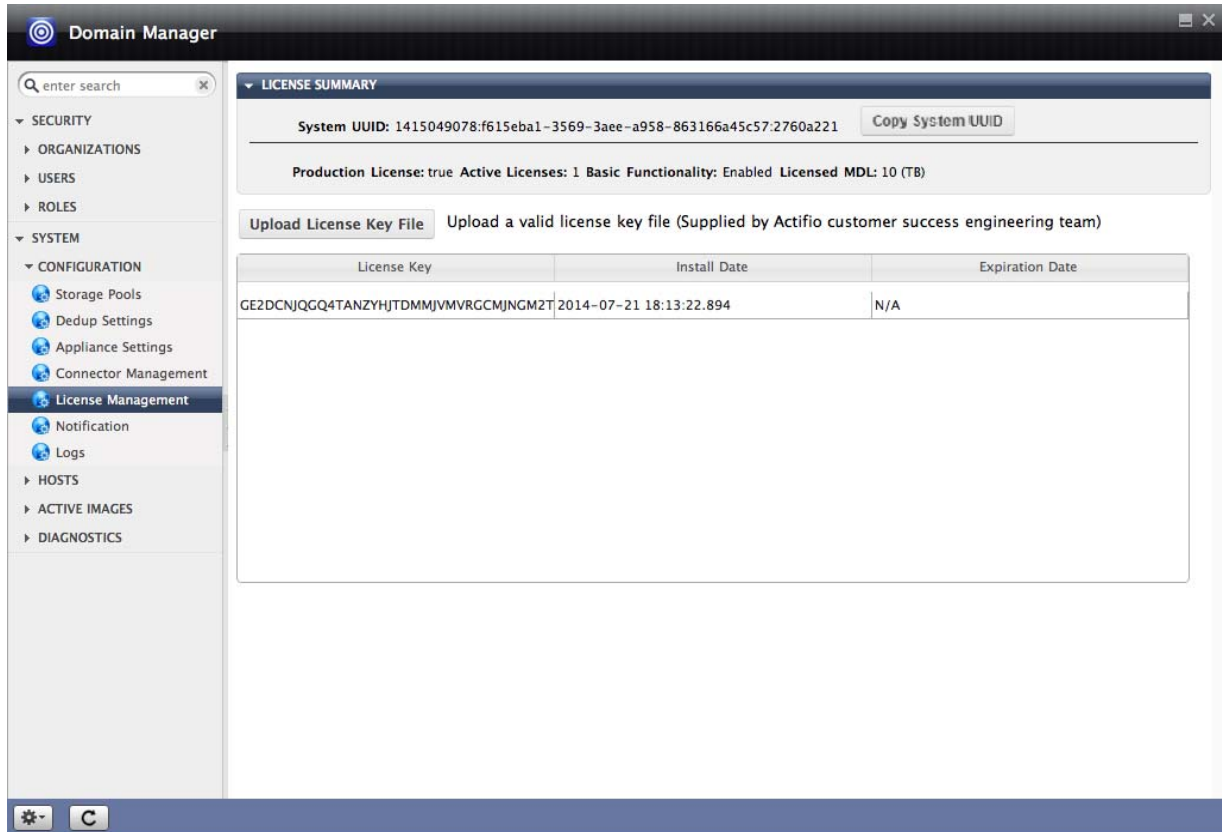
Note: As part of the initial installation of Actifio Sky appliance, a unique 128-bit system UUID is generated for the host running Sky. This unique UUID will be required when you order a Actifio Sky license, and can be found on the License Manager (see [Uploading a License Key](#) on page 80).

2. You will receive a license key email with an attached license file. Save the license key file in a location where it will be easy to locate and retrieve when uploading it to the Actifio Sky appliance. We also recommend that you save the original e-mail in a safe place in case you need it in the future.
3. Upload the license key as described in [Uploading a License Key](#) on page 80.

Uploading a License Key

After you receive the license key from your Actifio representative, upload it in the Domain Manager License Manager as described in this section.

1. Open the **Domain Manager** to **System > Configuration > License Management**. This sequence opens the License Manager.



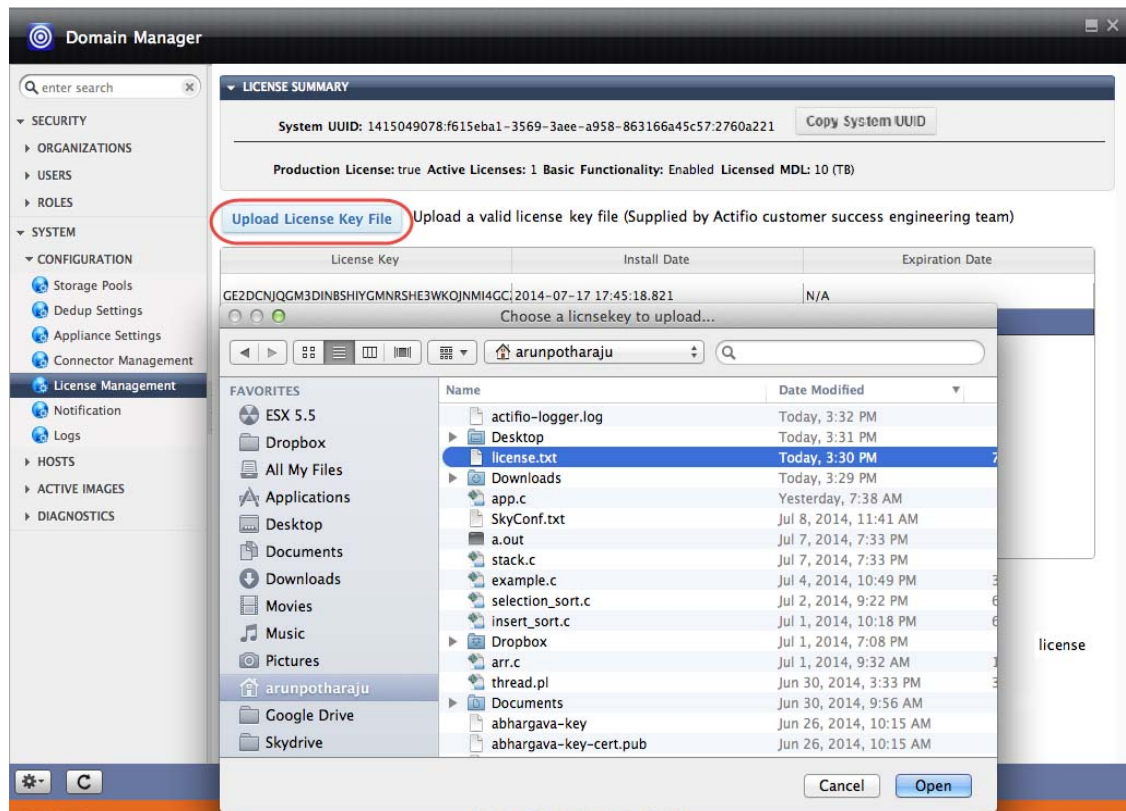
The screenshot shows the Domain Manager web interface. On the left is a navigation sidebar with categories: SECURITY (ORGANIZATIONS, USERS, ROLES), SYSTEM (CONFIGURATION, HOSTS, ACTIVE IMAGES, DIAGNOSTICS). Under CONFIGURATION, 'License Management' is selected. The main content area is titled 'LICENSE SUMMARY' and displays the following information:

- System UUID:** 1415049078:f615eba1-3569-3aee-a958-863166a45c57:2760a221 (with a 'Copy System UUID' button)
- Production License:** true **Active Licenses:** 1 **Basic Functionality:** Enabled **Licensed MDL:** 10 (TB)
- Upload License Key File** button with text: 'Upload a valid license key file (Supplied by Actifio customer success engineering team)'
- A table with the following data:

License Key	Install Date	Expiration Date
GE2DCNJQGQ4TANZYHJTDMMJVMVRGCMJNGM2T	2014-07-21 18:13:22.894	N/A

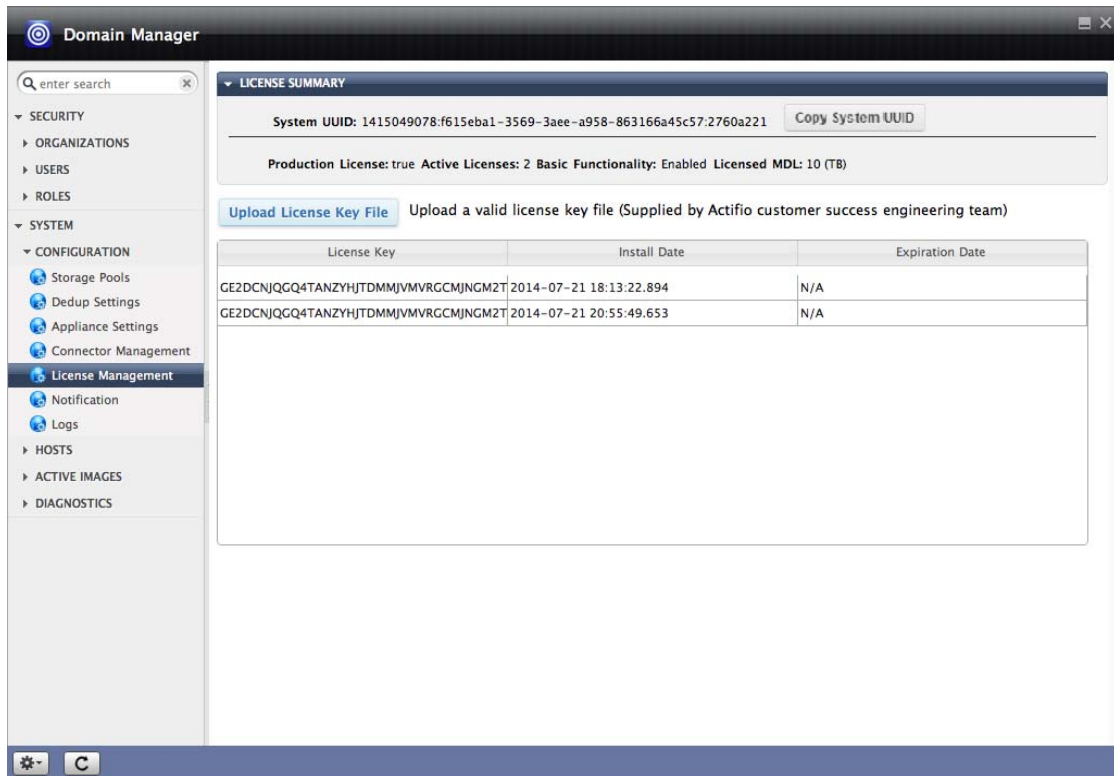
Accessing the License Manager

2. Click **Upload License Key File** to install the license key file. Navigate to the stored location of the license key, then click **Open**.



Navigating to the License Key File

3. The license key uploads into the Actifio Sky appliance, and the License Manager updates with information about the newly installed license key (License Key, Install Date, and Expiration Date).



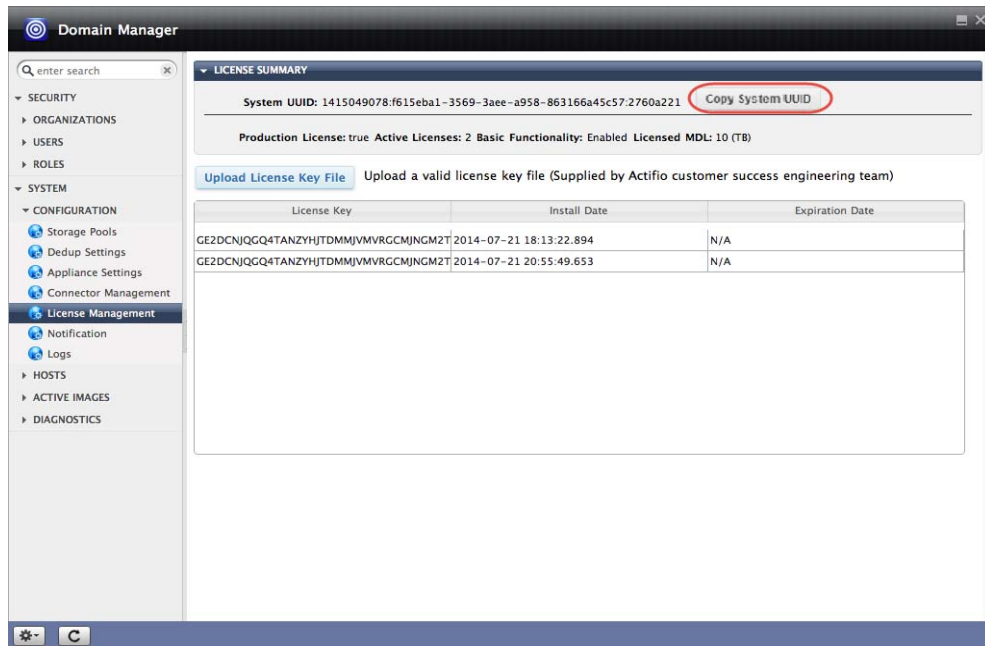
License Manager with Uploaded License Key

4. Once the license key upload process is complete you can use your add-on functionality (such as to protect Oracle databases).

Copying the System UUID Value

If you wish to save the Actifio Sky system UUID value to reference for future service requests, you can use the Copy System UUID button as follows:

1. Open the **Domain Manager** to **System > Configuration > License Management**. This sequence opens the License Manager.
2. Click **Copy System UUID**.



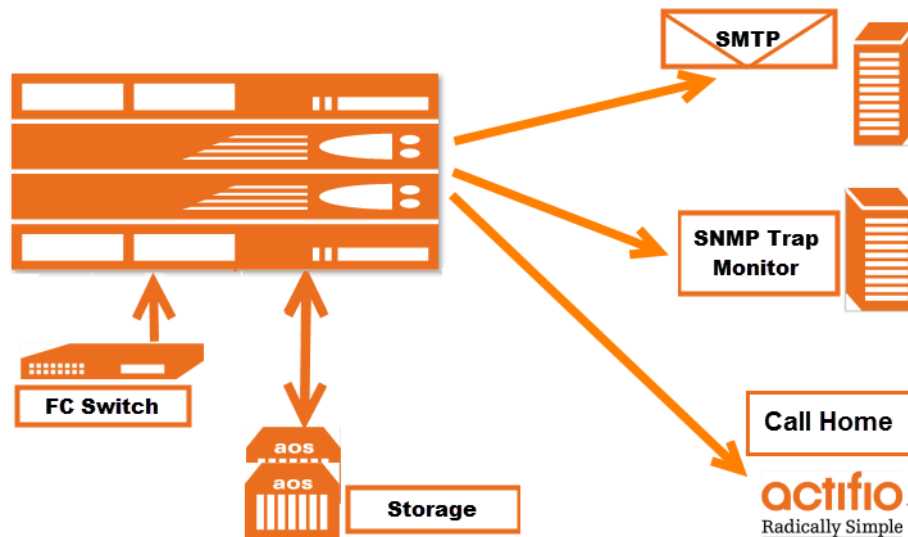
License Manager with Uploaded License Key

3. Use the **CTRL+V** sequence to save the system UUID value to a text file or a document for future reference.
4. Save the file.

14 Alerting

An Actifio appliance actively monitors event notifications. Specifically:

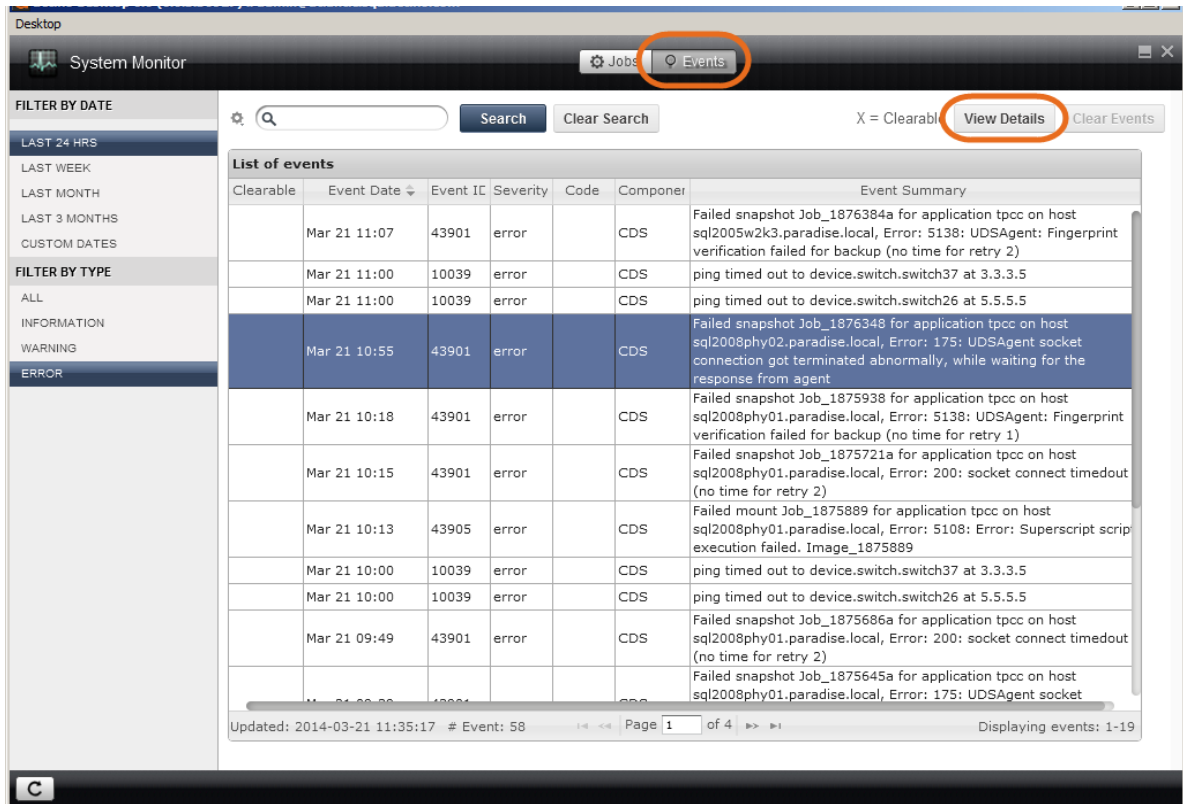
- You can configure your Actifio CDS appliances to collect event notifications from your AOS storage arrays and Fibre Channel switches. These procedures are outlined in [Chapter 15, Collecting Alerts from Actifio Storage and Switches](#). Actifio Sky appliances do not monitor switches and storage.
- You can also send event notifications from Actifio CDS and Sky appliances using email, by generating SNMP traps, and using the secure Actifio Call Home health check feature as detailed in [Chapter 16, Sending Alerts from the Actifio Appliance](#).



Overview of Alert Options

Monitoring Alerts in the Actifio Desktop System Monitor

You can learn about the context of an event in the Actifio Desktop System Monitor.



Viewing All Events of the Past 24 Hours

Click **View Details** to show the details of a selected event. The fields reported vary with the event type.



Viewing Event Details

15 Collecting Alerts from Actifio Storage and Switches

Note: *The Actifio Sky appliance does not generate hardware-related alerts.*

You can configure your Actifio CDS appliance to collect event notifications from your Actifio Optimized Storage (AOS) storage arrays and Fibre Channel switches. These procedures are detailed in:

[Polling Alerts from Actifio Optimized Storage and Switches](#) on page 88

[Forwarding Alerts from Fibre Channel Switches to the Actifio CDS Appliance](#) on page 89

Note: *For an overview on alerts and monitoring alerts in the Actifio Desktop system monitor, see [Chapter 14, Alerting](#).*

Polling and Forwarding

The Actifio CDS appliance can collect alerts in two ways:

Receiving Forwarded Alerts: You can configure storage and switches to forward alerts to the Actifio CDS appliance. Fibre Channel switches and non-AOS storage array must forward alerts.

Polling: Actifio CDS appliance can actively poll AOS storage arrays. Polling is the better option. All AOS arrays can be polled. The Fibre Channel switches cannot be polled; they must forward alerts to the Actifio CDS appliance.

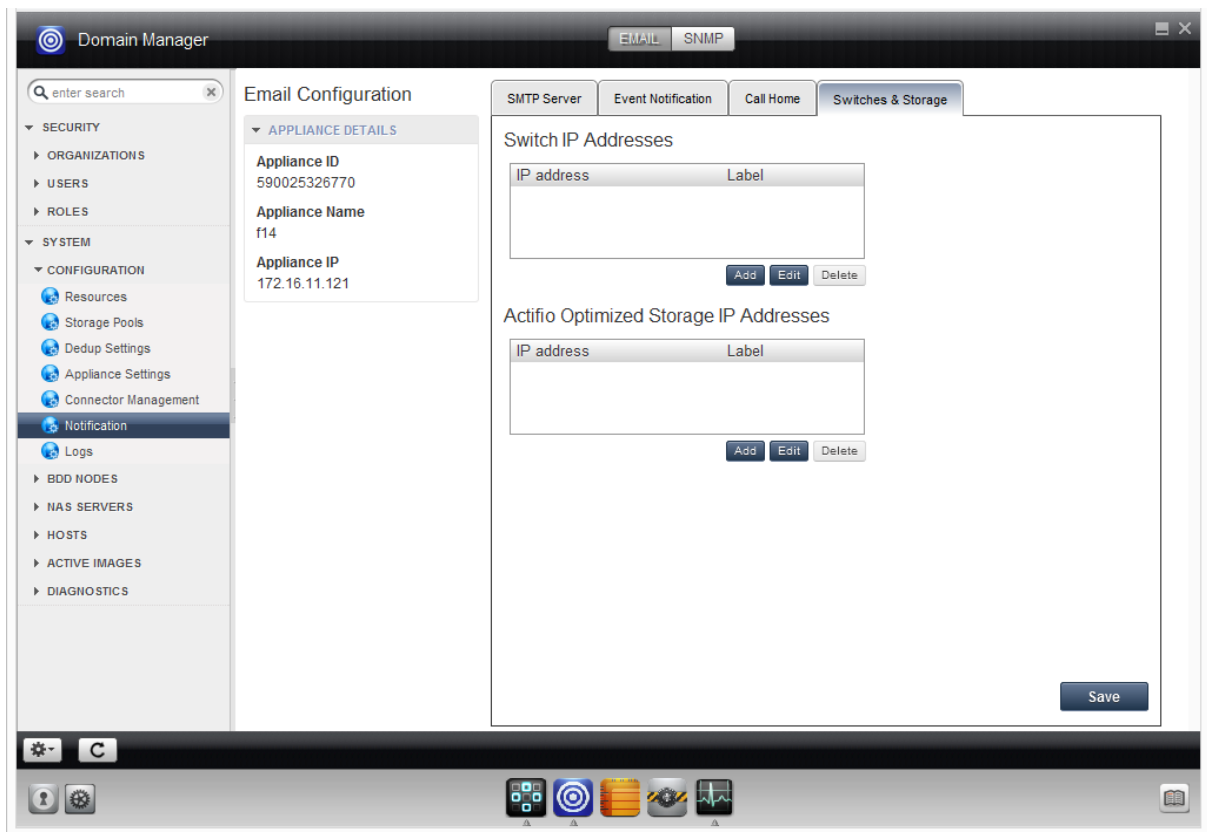
Note: *Alerts from non-Actifio storage can be configured using their native interfaces to forward traps to Actifio CDS appliance where they are logged and passed through to the customer SNMP trap receiver.*

Polling Alerts from Actifio Optimized Storage and Switches

To monitor the SNMP notifications generated by attached Actifio Optimized Storage (AOS) systems and switches, you must configure them in the Switches & Storage subtab. Notifications (traps and informs) are system alerts generated when certain events occur.

To configure the storage and switches:

1. Open the **Domain Manager** to **System > Configuration > Notification**.
2. Click the **Email** tab.
3. Click the **Switches & Storage** subtab.
4. Provide the IP address details in the two panes:
 - o In the **Switch IP Addresses** box, click **Add** to open the IP Addresses dialog.
 - o Enter a label and a switch IP address, then click **Save**. Repeat to add the second switch.
5. Repeat the process in the **Actifio Optimized Storage IP Addresses** box, adding two storage arrays and another ping address. You can use **Edit** to modify and **Delete** to remove an existing IP address.
6. Click **Save**.



Configuring Automatic Notification of Storage and Switch System Events

Forwarding Alerts from Fibre Channel Switches to the Actifio CDS Appliance

To access the SNMP configuration on the Fibre Channel switches:

1. Open Internet Explorer (only) to the IP address of the Fibre Channel switch.
2. Select **Switch Admin** from the upper left hand menu list.
3. In the upper right hand corner of the window, click **Show Advanced**.
4. Select the **SNMP** tab.
5. In the SNMPv3 Inform / Trap Recipient:
 - o Select the username of the switch administrator account.
 - o Enter the IP address of the Actifio CDS appliance to receive the traps.
 - o Ignore Port Number (leave it at 162).
 - o Select the level of traps to send to the appliance.
6. Click **Apply** and **Close**.
7. Repeat for each switch.

IBM_SAN80B_217 - Switch Administration

SwitchName: IBM_SAN80B_217 DomainID: 2(0x2) VVWN: 10:00:00:05:1e:09:97:01 Mon Jul 20 2009 18:52:25 GMT+00:00

SNMP Configure Routing Extended Fabric AAA Service Trace FICON CUP Security Policies

SNMP Information

Contact Name: Field Support.

Description: Fibre Channel Switch.

Location: End User Premise.

Enable/Disable Authentication Trap

☐ Enable Authentication Trap

SNMPv3 Inform / Trap Recipient

User Name	Recipient IP	Port Number	Trap Level
admin - RO	10.64.210.104	162	4 - Informational
snmpadmin2 - RW	0.0.0.0	162	0 - None
snmpadmin3 - RW	0.0.0.0	162	0 - None

SNMPv1 Community/Trap Recipient

Community String	Recipient	Port Number	Access Control	Trap Level
Secret C0de	10.64.210.74	162	Read Write	4 - Informational
OrigEquipMfr	dell-storage-074	162	Read Write	4 - Informational
private	127.0.0.1	162	Read Write	0 - None
public	10.64.210.72	162	Read Only	4 - Informational

Access Control List

Access Host	Access Control List
0.0.0.0	Read Write
0.0.0.0	Read Write
0.0.0.0	Read Write
0.0.0.0	Read Write

Apply Close Refresh

Configure SNMP parameters Mode: Advanced Free Professional Management Tool 10.64.210.217 AD0 User: admin Role: admin

Setting SNMP Trap Destinations in the Fibre Channel Switch

16 Sending Alerts from the Actifio Appliance

You can send alerts by the following methods:

[Sending Alerts to an SNMP Trap Receiver](#) on page 92

[Sending Alerts via Email](#) on page 94

[Sending Alerts to Actifio Support](#) on page 97

Note: For an overview on Actifio alerts and monitoring alerts using the Actifio Desktop system monitor, see [Chapter 14, Alerting](#).

Sending Alerts to an SNMP Trap Receiver

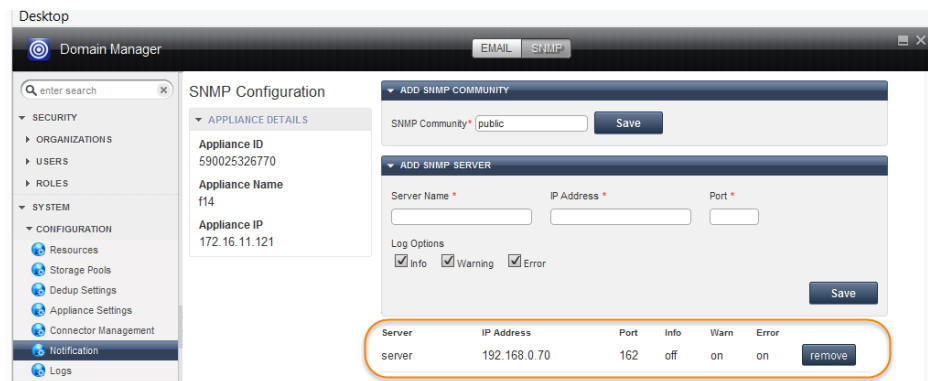
The Actifio appliance supports the sending of SNMP traps to a defined SNMP trap receiver. The Actifio MIB is available from the Actifio Resource Center to help analyze these traps. See [Accessing the Actifio MIB](#) on page 93

To configure an SNMP trap receiver:

1. Open the **Domain Manager** to **System > Configuration > Notification**.
2. Click the **SNMP** tab to see the SNMP Configuration.
3. Enter the SNMP trap receiver name in **Server Name**.
4. Enter the IP address of the SNMP trap receiver in **IP Address**. The IP address should be an IPv4 address.
5. Enter the remote port number in **Port**. Normally the port is 162, but check to be sure. The port number must be between 1 and 65535.

Note: Traps are sent by Actifio appliance to the SNMP Trap receiver over UDP and not by TCP/IP.

6. Select the type of traps to forward: Info, Warning, and Error. The Actifio appliance MIB will send notifications about these traps to the SNMP trap receiver.
7. Click **Save**.



Configuring Report Events to an SNMP Trap Receiver

You can add multiple SNMP trap receivers and you can specify different types of events to be sent to each.

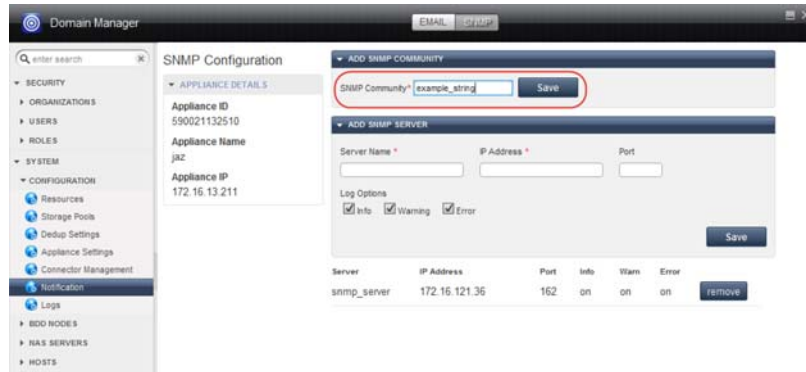
Note: As a reminder to administrators, clearable events that have not been acted upon will trigger repeated event notifications once every 25 hours until cleared.

Setting the Community String for Forwarding Traps to a non-Actifio SNMP Trap Receiver

If you want to send the traps to another SNMP trap receiver, and that server requires a different community string, you can set the string from the SNMP Configuration window.

To set the community string:

1. Open the **Domain Manager** to **System > Configuration > Notification**.
2. Click the **SNMP** tab to see the SNMP Configuration.
3. Enter the SNMP community string in **SNMP Community**.
4. Click **Save**.



Configuring SNMP Community String

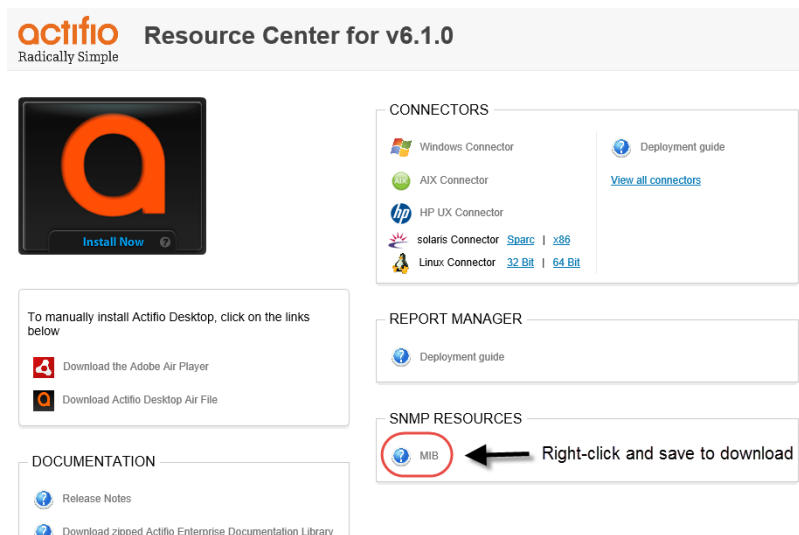
Accessing the Actifio MIB

To receive alerts from the Actifio appliance for purposes of translating the object identifiers (OIDs) used by the Actifio appliance, you can import the Actifio MIB file (Actifio_UDS_1.0.MIB) to your SNMP trap receiver. An SNMP trap receiver can listen to the SNMP traps that are being sent by an Actifio appliance in the network. The Actifio MIB file includes all of object identifiers, notification types, object types, and notification groups used by the Actifio appliance.

Note: If you are using an SNMP-based monitoring and management systems to pull data on-demand, you can extend SNMPv2 support for the SNMP GET request process to the Actifio appliance through the activation of an SNMP agent in the appliance. By using the Actifio MIB file, SNMP GET requests pull specific objects to monitor and Actifio appliance configurations, system statistics and performance, and so on. For details, see the **Configuring the SNMP Agent to Support SNMP GET Operations** Tech Brief.

You can access the Actifio MIB file from the Actifio Resource Center:

1. Open a web browser to your Actifio appliance IP address (http://<Actifio_appliance_IP_address>). The Actifio Resource Center page opens.



2. Right-click the MIB link under SNMP Resources and save the Actifio_UDS_1.0 file to a convenient location.

Sending Alerts via Email

You can configure email notifications to be sent when an event of severity *warning* or *error* is raised by Actifio appliance. The first step is to configure an email server in the Actifio Desktop.

There are two parts to this configuration, all managed from the Actifio Desktop Domain Manager Notifications section:

[Communicating with an SMTP Server](#) on page 95

[Setting Up Automatic Email Notifications](#) on page 96

a-bot@mail.com

6:13 AM (1 hour ago) ☆ ↩

to me ▾

Customer: Actigsoluter

Cluster Id: 590021132632

Cluster Name: sepascl7

Hostname: sepn13

CDS IP Address: 172.16.215.161

date	component	type	eventid	message
2013-12-16 05:59:26	CDS	error	10036	FC map copies 256 reaching limit for vdisk vm-52A8E1482C00
2013-12-16 06:01:58	CDS	error	43901	Failed snapshot Job_0010646a for application RHEL5.8_vm41_01 on host rhel5.8_vm41_01, Error: 90: object manager: prepare snapshot failed (no time for retry 2)
2013-12-16 06:04:26	CDS	error	10036	FC map copies 256 reaching limit for vdisk vm-52A8E1482C00
2013-12-16 06:09:26	CDS	error	10036	FC map copies 256 reaching limit for vdisk vm-52A8E1482C00
2013-12-16 06:14:26	CDS	error	10036	FC map copies 256 reaching limit for vdisk vm-52A8E1482C00
2013-12-16 06:17:01	CDS	error	43901	Failed snapshot Job_0010663a for application RHEL5.8_vm41_01 on host rhel5.8_vm41_01, Error: 90: object manager: prepare snapshot failed (no time for retry 2)

Example Email Notification

Communicating with an SMTP Server

To configure the Actifio appliance to communicate with an email server:

1. Open the **Domain Manager** to **System > Configuration > Notification**.
2. Click the **EMAIL** tab.
3. Click the **SMTP Server** subtab.
4. Enter the SMTP server name or IP address (IPv4) in **Server Name/IP**.
5. Enter the SMTP or SMTPS port number in **Port**. Select **Use SSL** to send emails securely using SSL.
6. (Optional) Enter a Host Name. This entry is the address that will appear in the From field of each email.
7. Enter a mail server user name and password.
8. Enter the maximum size of the email to be sent in **Message Limit**. When an email exceeds this size, the email is split into two or more emails. For example, if the limit is 1MB and the email is 2MB in size, Actifio Desktop splits the attachments into two 1 MB attachments and sends two separate emails.
9. Click **Test Email** to send a test mail to an address that you will enter in a pop- up window.
10. Click **Save**.

The screenshot shows the 'Domain Manager' web interface. On the left is a sidebar with a search bar and a navigation tree. The tree has categories: SECURITY (ORGANIZATIONS, USERS, ROLES), SYSTEM (CONFIGURATION, Resources, Storage Pools, Dedup Settings, Appliance Settings, Connector Management, Notification, Logs), BDD NODES, NAS SERVERS, HOSTS, ACTIVE IMAGES, and DIAGNOSTICS. 'Notification' is selected. The main area is titled 'Email Configuration' and has tabs for 'SMTP Server', 'Event Notification', 'Call Home', and 'Switches & Storage'. The 'SMTP Server' tab is active. It contains the following fields: 'Server Name/IP*' with value '192.168.255.2', 'Port*' with value '25' and a 'Use SSL' checkbox, 'Host Name' (empty), 'Email*' with value 'user@user.com', 'Password*' (masked with dots), and 'Message Limit' with a value of '10' and a unit dropdown set to 'MB'. At the bottom right are 'Test Email' and 'Save' buttons. A 'Domain Manager' header bar at the top shows 'EMAIL' and 'SNMP' tabs.

Configuring Event Notifications

Configure the email server to either:

- Use a set of user credentials that you enter
- Allow anonymous relaying to email addresses outside the domain (so userid becomes the “from” address and the password field can be left blank)

Note: For useful information about setting up anonymous email in Exchange, see:
<http://www.petri.co.il/authenticated-or-anonymous-smtp-relay-with-exchange-2007.htm#>

After the email server has been properly configured, you can configure automated emails for events as described in [Setting Up Automatic Email Notifications](#) on page 96.

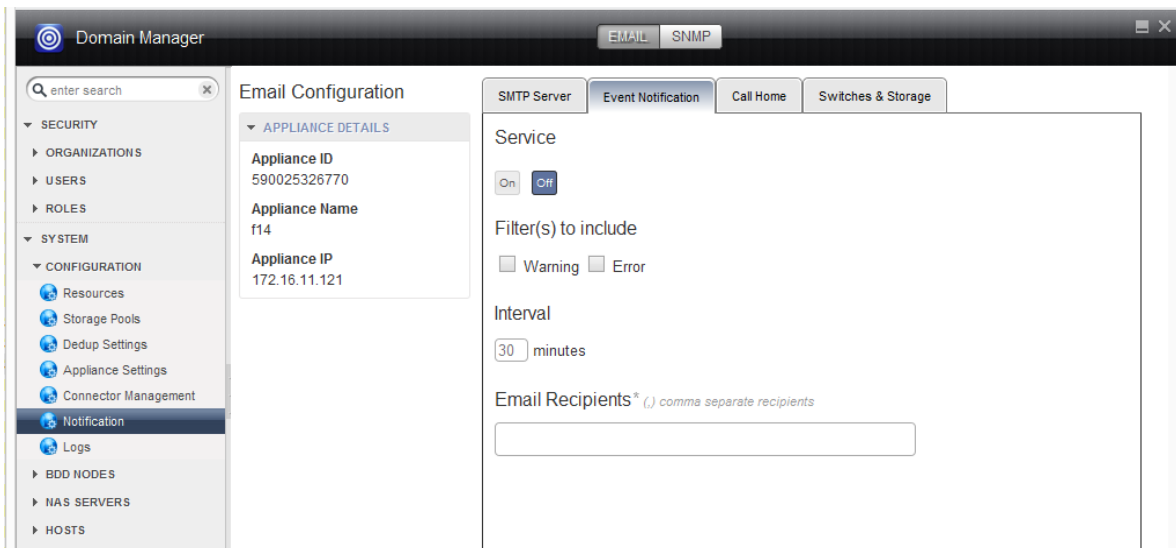
Setting Up Automatic Email Notifications

Before configuring the levels of events that trigger emails or the addresses to receive the emails, you must configure an email server as described in [Sending Alerts via Email](#) on page 94.

The Actifio appliance can send an email notification when an event of the severity *Warning* or *Error* is raised. Emails about critical events are sent immediately.

To configure email notification:

1. In the Actifio Desktop, open the **Domain Manager** to **System > Configuration > Notification**.
2. Click the **EMAIL** tab.
3. Click the **Event Notification** subtab.
4. Under **Service**, select **On** and confirm the selection.
5. Check **Warning**, **Error**, or both checkboxes from **Filter(s) to Include** to send those events to the email recipients listed in Email Recipients (below). In most cases you should check both **Warning** and **Error**.
6. Enter the desired time interval in **Interval**. Emails about critical events are sent immediately. This value is the minimum time between when emails for all other events are sent, so it may be almost 30 minutes from the time that an event occurs until the time the next email is sent. The default value of 30 minutes is appropriate for most sites.
7. In **Email Recipients**, enter a comma separated list of email addresses of persons who are to receive email notifications.
8. Click **Save**.



Configuring Event Notifications

Sending Alerts to Actifio Support

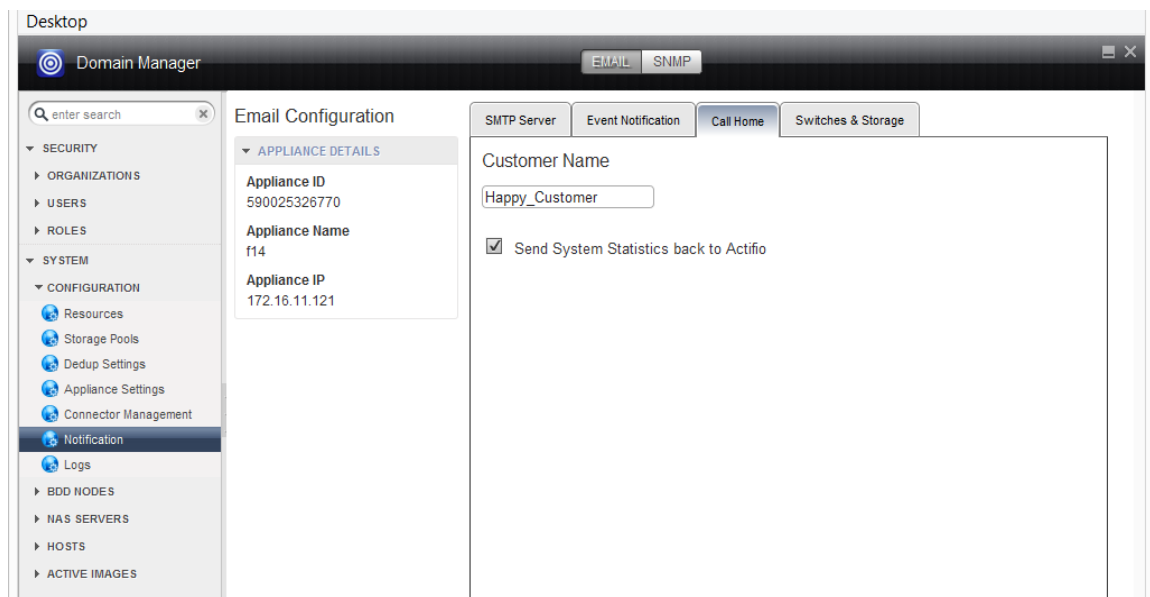
Note: Sending Actifio appliance statistics to the support team at Actifio requires an SMTP server.

The Call Home feature sends an email to Actifio Support every six hours. In the event of a problem, Actifio Support can refer to this information to minimize time to recovery. The email includes these statistics:

- Actifio appliance version information
- Uptime of the Actifio appliance
- Status check of services
- Process summary
- Logs of various processes
- Failed jobs and total jobs
- Storage pool and deduplication statistics

To send Actifio appliance statistics to Actifio Customer Support every 6 hours:

1. Open the **Domain Manager** to **System > Configuration > Notification**.
2. Click the **Email** tab.
3. Click the **Call Home** tab.
4. Enter your organization name in **Customer Name** and select **Send System Statistics back to Actifio**.
5. Click **Save**.



Configuring the Call Home Health Check Feature

17 Sending Logs to Actifio Support

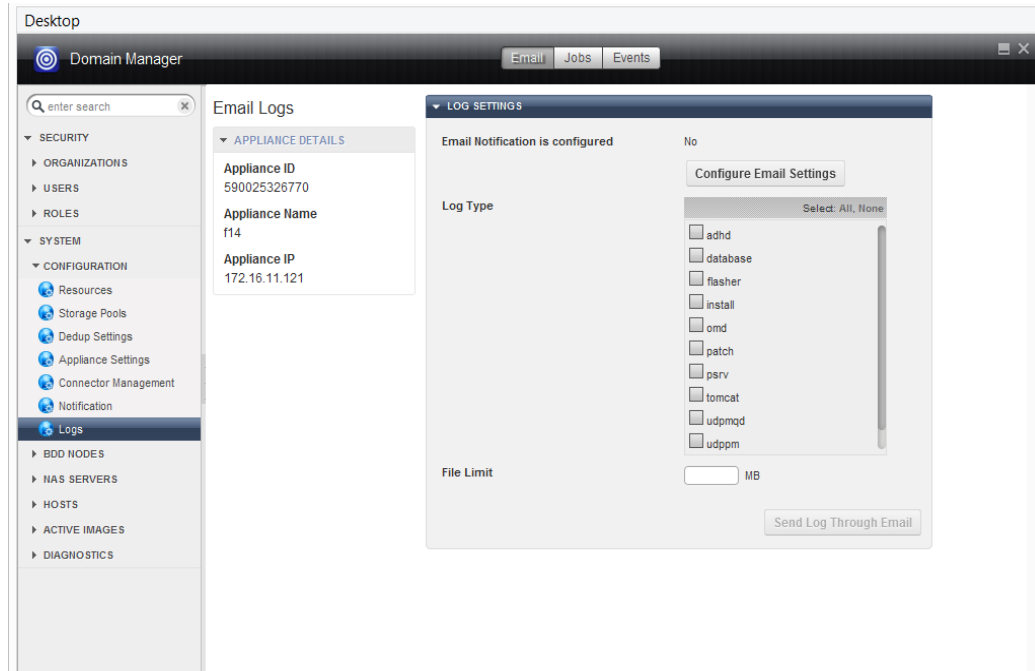
Use the Logs section of the Domain Manager to identify one or more Actifio appliance logs to send to Actifio Support to help if you encounter issues with your Actifio appliance. The Actifio appliance creates log files for each type of log in the /act/logs folder.

To send Actifio appliance logs to Actifio Support:

1. Open the **Domain Manager** to **System > Configuration > Logs**.
2. Click the **Email** tab to access the Log Settings. If Email Notification is not configured, configure the setting before proceeding. See the procedure in [Sending Alerts via Email](#) on page 94.
3. Select the types of logs to send from **Log Type**. To select all categories of logs, click **All**.

Optionally, you can specify the number of log files to be sent to the Actifio Support team in **File Limit**. the Actifio appliance creates one log file for each type of log every day in the /act/logs folder. To email the log files of the past ten days for the selected type, specify **10** in File Limit. If you do not specify the file limit, all logs files from the /act/logs folders are sent. Set the value to **1** to receive the latest log file of the selected type.

4. Click **Send Log Through Email** to save the configuration.



Selecting Logs to Send to Actifio Support

18 Managing Hosts

Hosts contain VMs and applications to be protected by an Actifio appliance. You use the Host section of the Domain Manager for a variety of host management functions, such as adding hosts, editing information about a host, configuring ports used to access a host, viewing applications on a host, and viewing the associated organizations that have access to a host.

This section introduces.

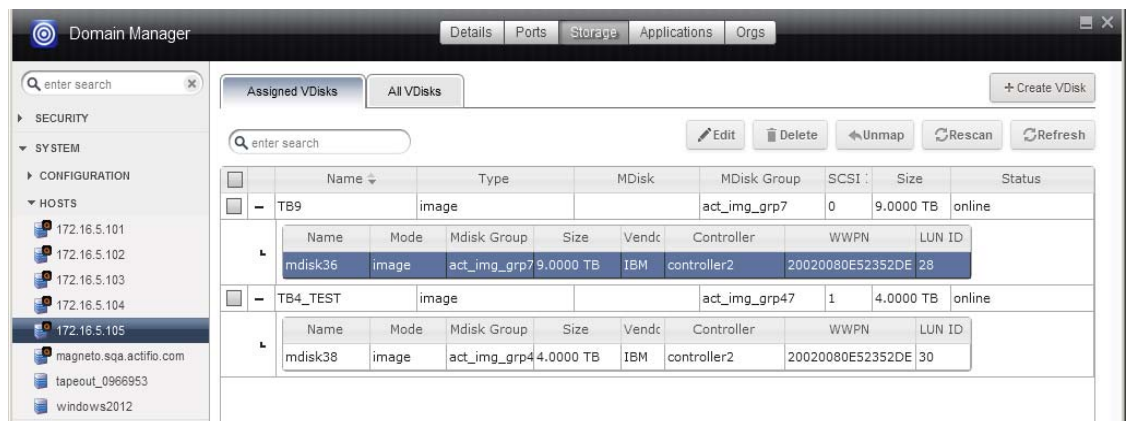
[Details Tab](#) on page 102

[Ports Tab](#) on page 103

[Storage Tab](#) on page 104

[Applications Tab](#) on page 105

[Orgs Tab](#) on page 106



A Host with In-Band Protection Assigned to Two Image VDisks Mapped to MDisks

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

Details Tab

Use the Details tab to view and edit information about a configured host.

To configure a new host, see [Adding Hosts and Editing Host Information](#) on page 129. To review the parameters related to a configured host, see [Viewing and Editing Host Information](#) on page 140.

The screenshot displays the 'Domain Manager' application window. The 'Details' tab is selected, showing configuration for host 'dev5-2160054048'. The left sidebar contains a tree view with categories: SECURITY (ORGANIZATIONS, USERS, ROLES), SYSTEM (CONFIGURATION, BDD NODES, IAS SERVERS, HOSTS). Under 'HOSTS', several hosts are listed, with 'dev5-2160054048' highlighted. The main panel shows the host's details in a form. The 'Host' section includes 'Name*' (dev5-2160054048) and 'Friendly Name'. The 'Type of Host' is set to 'Generic'. The 'Network' section shows 'IP Address' (172.17.5.216) with 'Add' and 'Clear' buttons. The 'Description' field is empty. The 'Connector Port' is set to 5106. The 'Login Credentials for connector' section has 'Username' and 'Password' fields. A 'Save' button is at the bottom right.

Host	Name*	Friendly Name
dev5-2160054048	dev5-2160054048	

Type of Host
Generic

Network
IP Address: 172.17.5.216

Description

Connector Port
5106

Login Credentials for connector
Username: Password:

Save

The Details Tab for An Out-of-Band ESX Host

Ports Tab

Hosts that have any applications protected in-band include a Ports tab. Use the Ports tab to record the WWPN or iSCSI ports that Actifio CDS appliance will use to connect to a host.

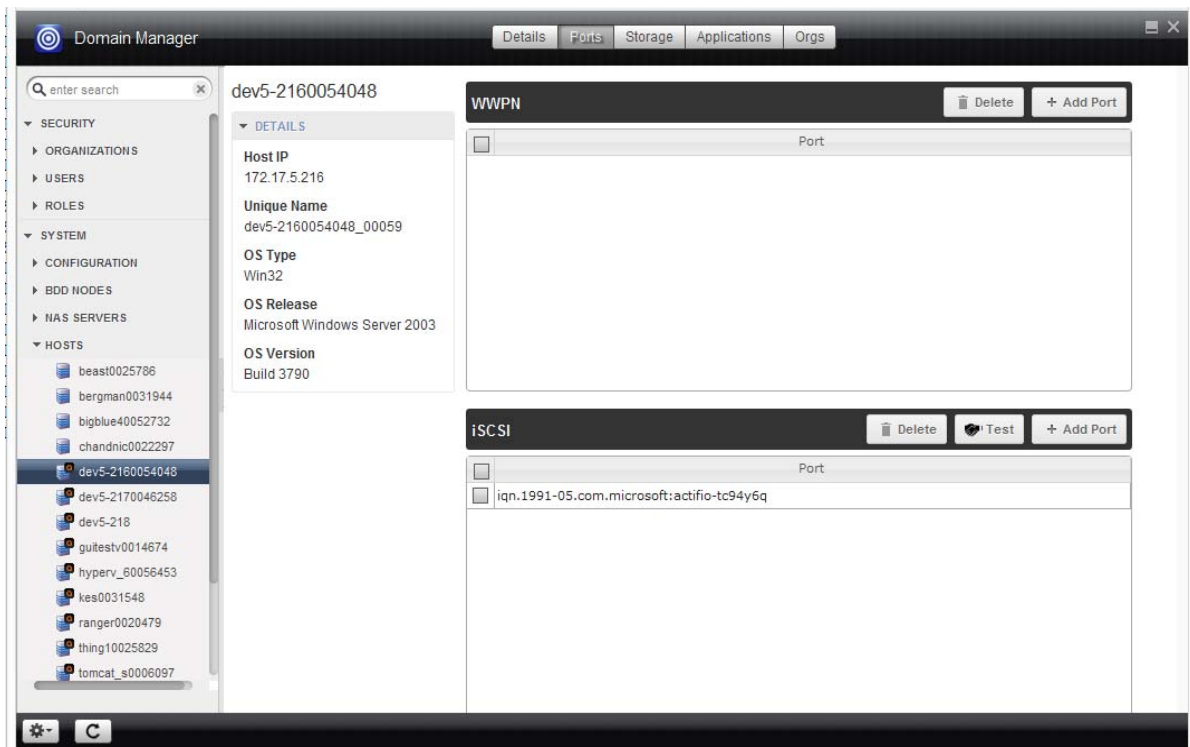
Note: *In-band and WWPN is not applicable to Actifio Sky appliances.*

Ports can be:

WWPN (World Wide Port Name): The unique address assigned to a port in your fibre channel fabric. Use this address for in-band hosts that present VDisks from the Actifio appliance.

iSCSI (Internet Small Computer System Interface): The IQN (iSCSI Qualified Name) from the host.

To configure ports for a new host, see [Configuring the Ports of a Host](#) on page 138.

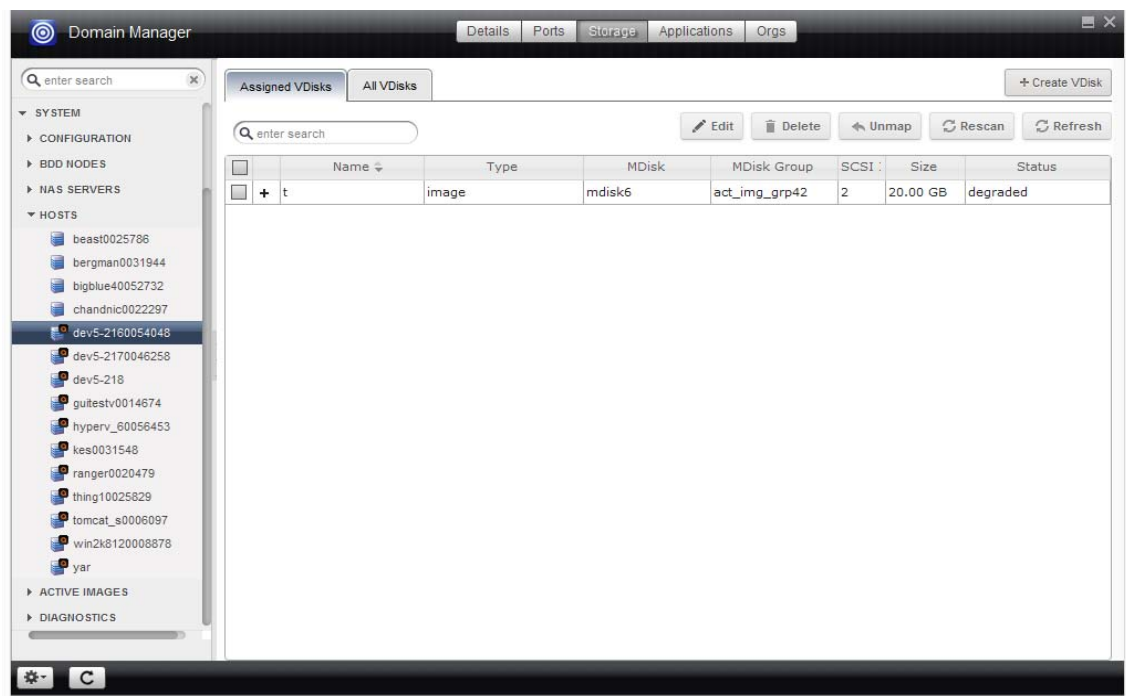


The Ports Tab for an In-Band Host Reached via Fibre Channel

Storage Tab

Note: In-band storage is not applicable to the Actifio Sky appliance.

Hosts that have any applications protected in-band show the Storage tab. Use the Storage tab to create and map VDIs and MDIs for the selected host. VDIs and MDIs are detailed in [Chapter 19, Configuring Storage for In-Band Hosts](#).



The Storage Tab for an In-Band Host Assigned to Two VDIs, Showing One MDisk

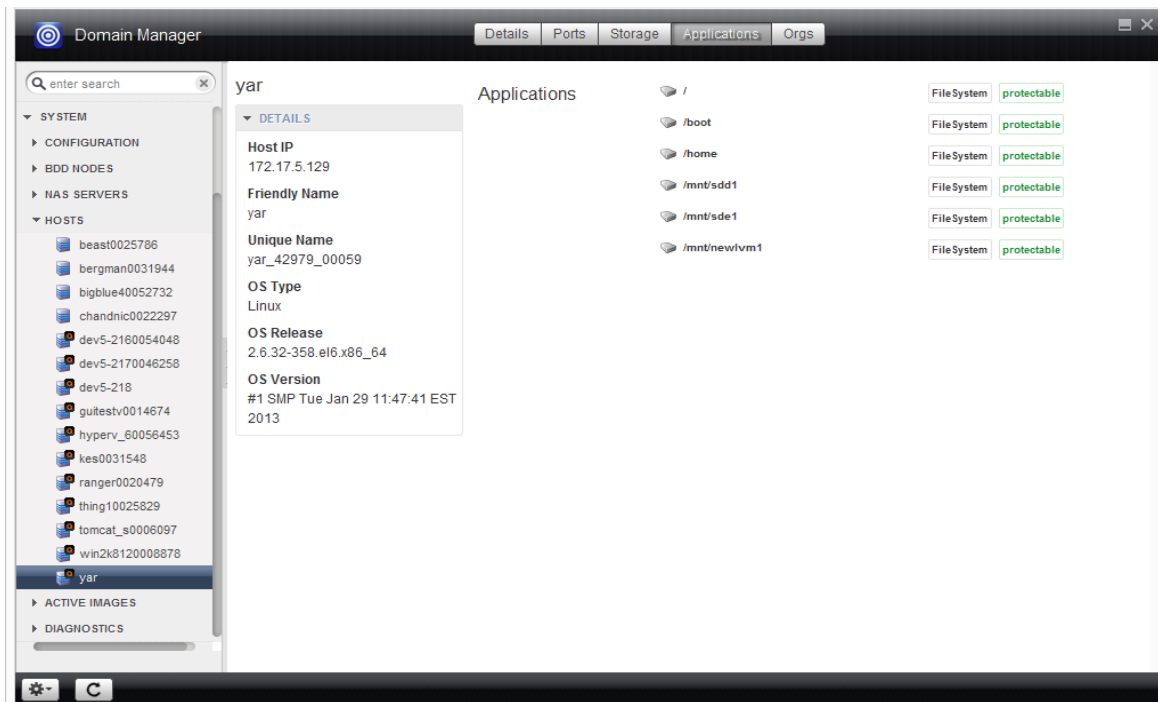
Hosts can use in-band or out-of-band storage; please review [Chapter 3, Understanding In-Band and Out-of-Band Data Storage](#).

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

Applications Tab

Use the Applications tab to view information about the applications protected from each host.

To view protected applications on a host, see [Viewing Applications on a Host](#) on page 139.

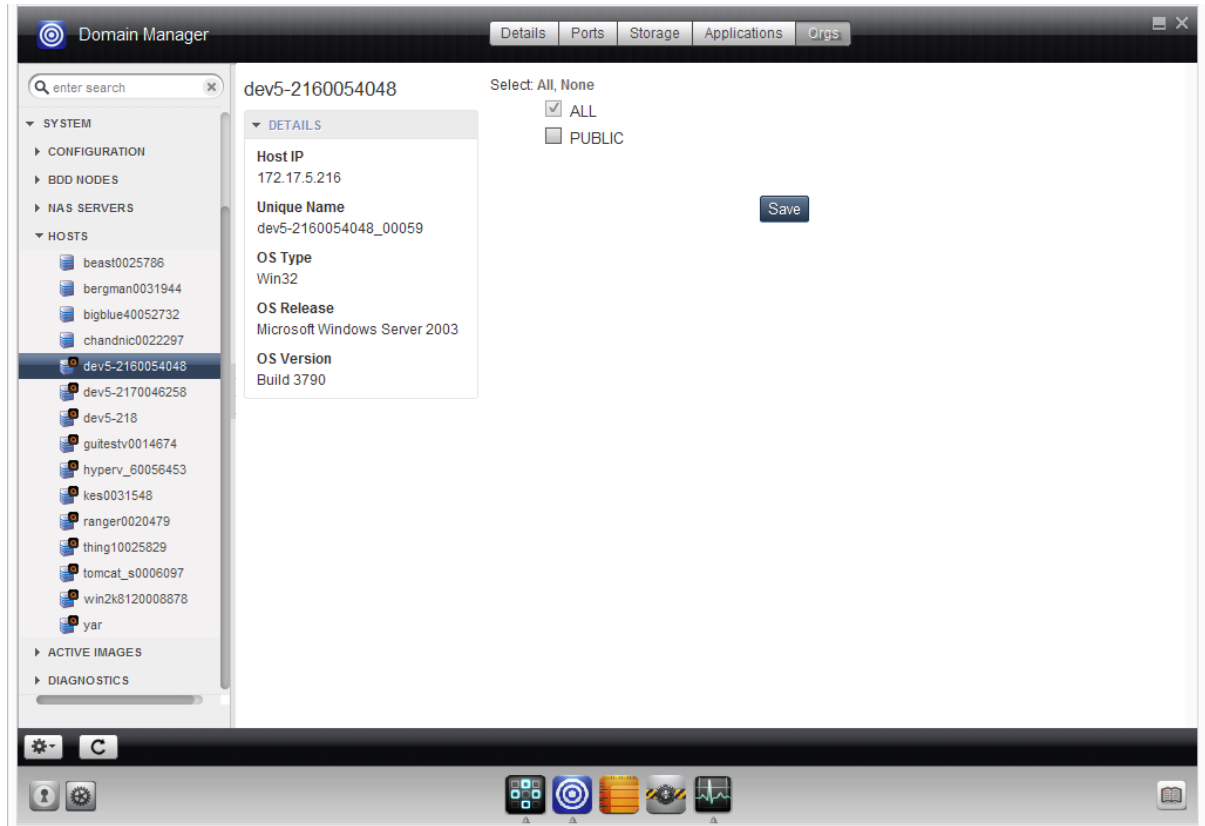


The Applications Tab for Applications Discovered and Protected on a Host

Orgs Tab

Orgs are the organizations configured in the Domain Manager Security section that have access to this host. Organization membership govern which users can access or manage which resources within an Actifio appliance.

Organizations are detailed in ***Setting Up Users and Roles in the Domain Manager***.



The Orgs Tab for a Host That Has Not Yet Been Assigned to a Specific Organization

19 Configuring Storage for In-Band Hosts

Note: *In-band storage is not applicable to the Actifio Sky appliance.*

The Actifio CDS appliance uses VDisks (virtual disks) to virtualize copy data from hosts. VDisks are logical disks taken from a pool of MDisks presented to the Actifio CDS appliance from one or more internal and external arrays. VDisks are explained in [VDisks and VDisk Consumption](#) on page 23.

In-band storage is discussed in [In-Band Data](#) on page 17.

VDisks are explained in [VDisks and VDisk Consumption](#) on page 23.

VDisk management includes:

[Creating a VDisk](#) on page 108

[Mapping a VDisk to a Host](#) on page 111

[Unmapping a VDisk from a Host](#) on page 112

[Expanding a Virtual Disk](#) on page 113

[Renaming VDisks and MDisks](#) on page 114

[Deleting a Virtual Disk](#) on page 115

You use Create VDisk in the Hosts section of the Domain Manager to create different types of virtual disks and assign them to hosts. VDisks are then visible to the host systems that use them.

VDisks are typically used to allow for in-band Fibre Channel snapshots to be taken as part of the overall copy data management solution. VDisks allow new volumes and volumes with existing customer data to be presented to the host through the Actifio CDS appliance. For existing volumes, this capability allows the appliance to move in band between the existing storage and the host and, essentially, to pass the disks through with the existing data intact.

Creating a VDisk

This section details:

[Creating an Image Mode VDisk on page 109](#)

[Creating a Mirror Mode VDisk on page 110](#)

VDisks are created from a set of extents in an MDisk group. VDisks can be created as:

Image Mode: An image mode VDisk provides a direct block-for-block translation from the managed disk (MDisk) to the VDisk. Image mode VDisks have a direct relationship with one MDisk. When you create an image mode VDisk, a direct mapping is made between extents that are on the MDisk and extents that are on the VDisk. This mode allows you to insert Actifio CDS into the data path of an existing storage volume or LUN with minimal downtime.

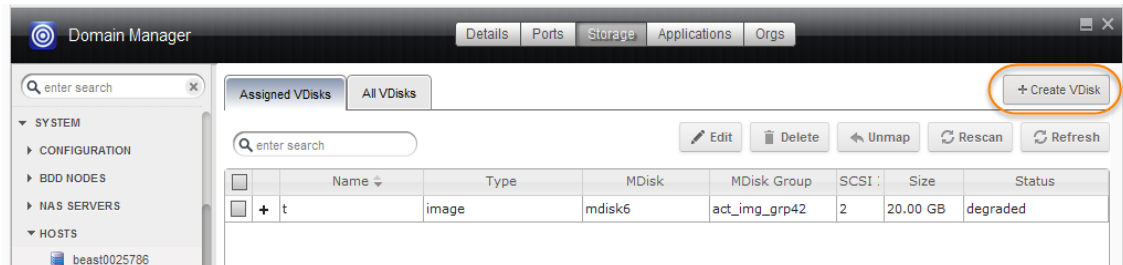
Mirror Mode: Mirroring adds a second identical disk to back up the first image. A mirrored virtual disk can remain operational if one VDisk fails or corrupted. The first disk is always an image disk, as described above. The second disk might be another image disk or it could be a striped disk:

- o **Mirror Mode: Image-Image:** In Image-Image mode, the secondary disk is of Image type.
- o **Mirror Mode: Image-Striped:** In Image-Striped mode, the secondary disk is of Striped type. A striped virtual disk is one in which the data is broken into chunks and distributed on the disks comprising the MDisk group on which the virtual disk is created. Striped mode indicates that the VDisk is created from multiple MDisks in the MDisk group. Striped-mode VDisks can be expanded as described in [Expanding a Virtual Disk on page 113](#).

Creating an Image Mode VDisk

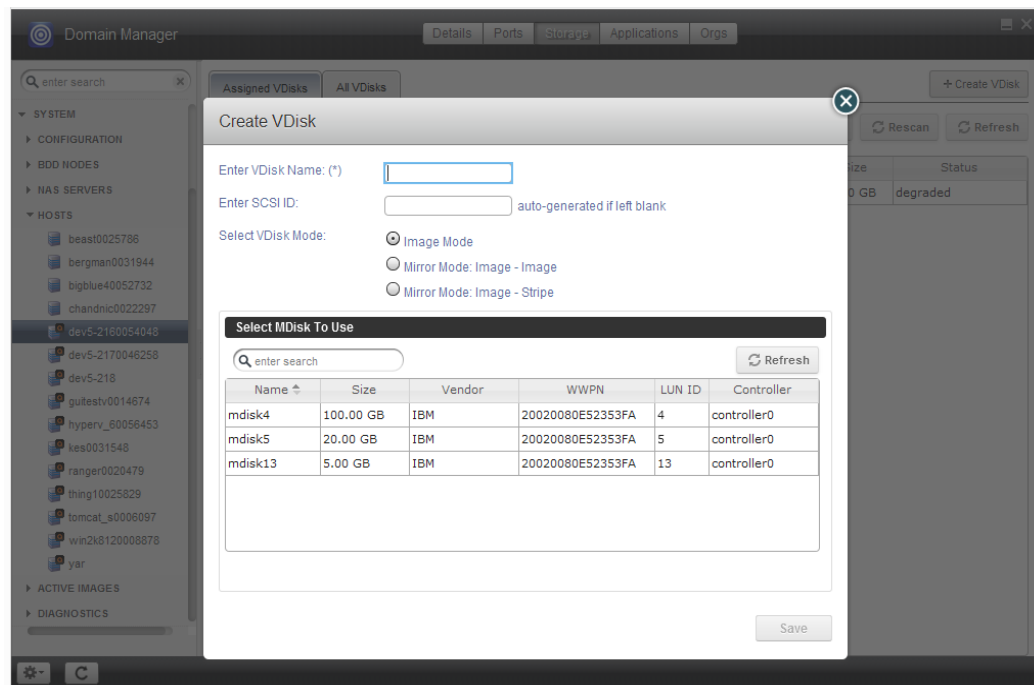
Perform the following steps to create an image mode VDisk:

1. Open the **Domain Manager** to **System > Configuration > Hosts** and select a host.
2. Click the **Storage** tab.



Creating a VDisk

3. Click **Create VDisk**. The Create VDisk window opens. All the unmanaged MDisks are listed. You can move the mouse pointer on the disk row to see the UUID of the MDisk.



Creating a VDisk

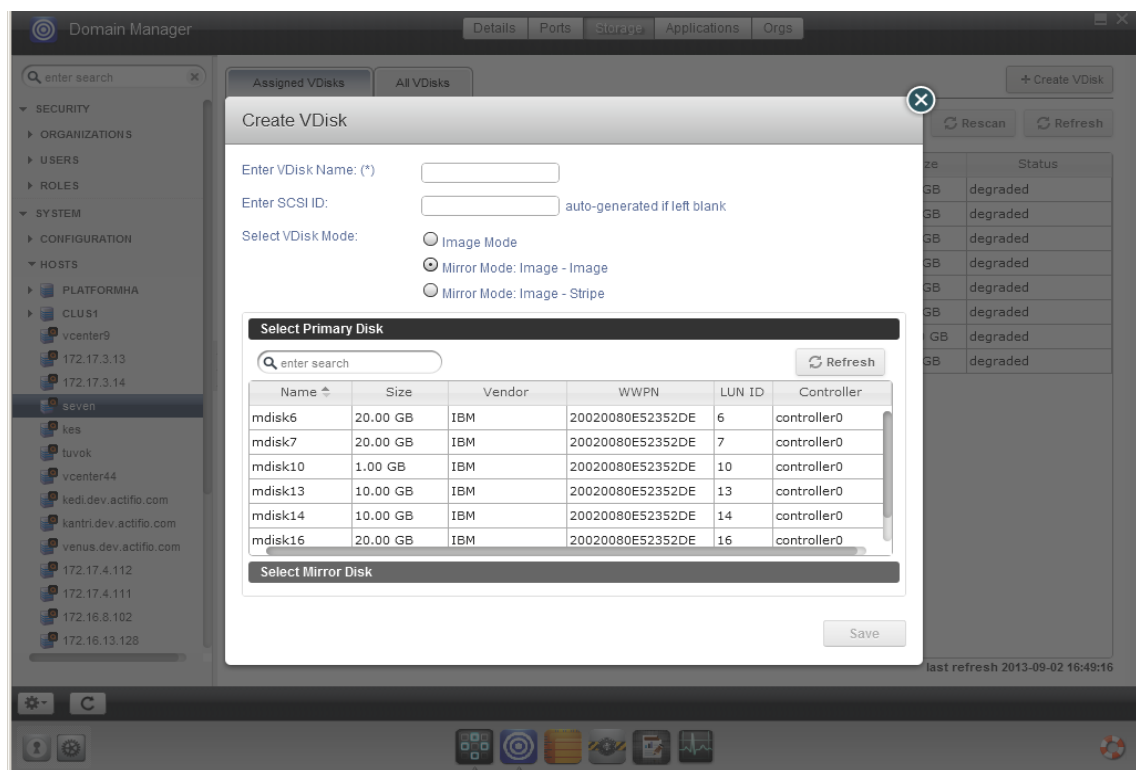
4. Enter the name of the virtual disk you would like to create in **Enter VDisk Name**. This name will be presented in the list of disks that you can present to a host. It's a good idea to use a descriptive name, including the host name, to make identification and troubleshooting easier.
5. Enter the SCSI ID in **Enter SCSI ID**. The SCSI ID is auto generated if the field is left blank.
6. Select Image Mode from the **Select VDisk Mode** options.
7. From the list of available MDisks, select the desired MDisk by clicking on any field of the **MDisk** row.
8. Click **Save**.

Creating a Mirror Mode VDisk

Select Mirror Mode when you want to create an image for your VDisk.

Perform the following steps to create a VDisk in mirror mode:

1. Open the **Domain Manager** to **System > Configuration > Hosts** and select a host.
2. Click the **Storage** tab.
3. Click **Create VDisk**. The Create VDisk window opens.
4. Enter the name of the virtual disk you would like to create in **Enter VDisk Name**.
5. Enter the SCSI ID in **Enter SCSI ID**. The SCSI ID is auto generated if the field is left blank.
6. Select **Mirror Mode: Image-Image** or **Mirror Mode: Image-Striped** from Select VDisk Mode.
7. Under **Select Primary Disk**, select an MDisk from the list of available MDisks.
8. The Select Primary Disk area collapses and a new **Select Mirror Disk** row appears beneath Select Primary Disk. From the list of remaining MDisks, select a **Mirror Disk** by clicking its row.

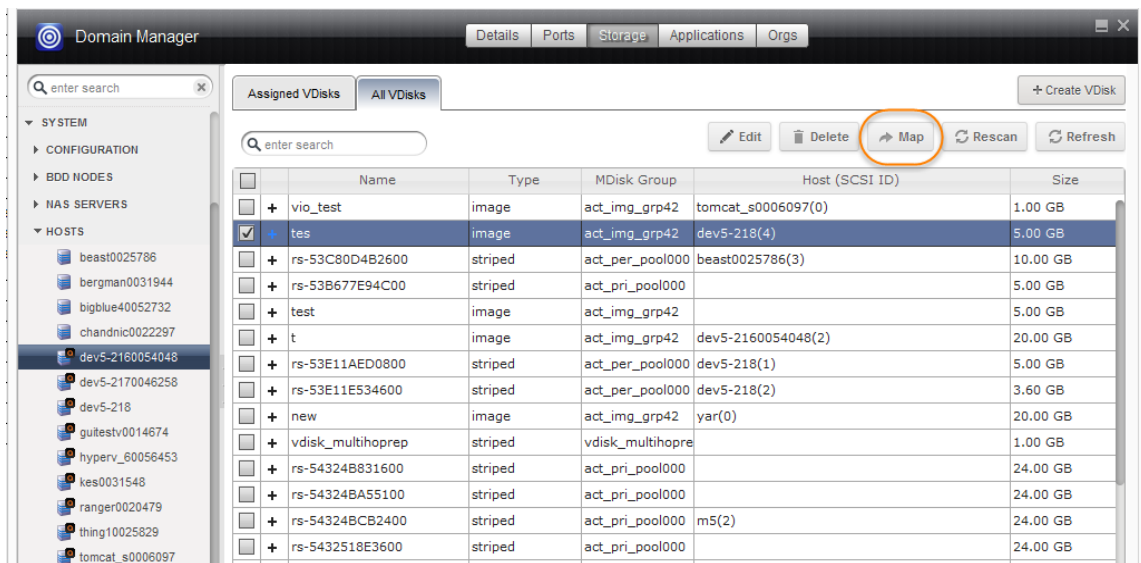


9. The selected Primary and Mirror disks are listed at the bottom of the Create VDisk window. Verify the selection, then click **Save**.

Mapping a VDisk to a Host

To assign a virtual disk to a host:

1. Open the Actifio Desktop to the **Domain Manager**.
2. Select the **Host** from the navigation pane.
3. Select **Storage** tab and the **All VDisks** subtab.
4. Select one or more virtual disks.
5. Click **Map**. A confirmation dialog appears.
6. Enter the **SCSI ID** for the vDisk. The SCSI ID is auto-generated if it is left blank.
7. Click **Map VDisk**.

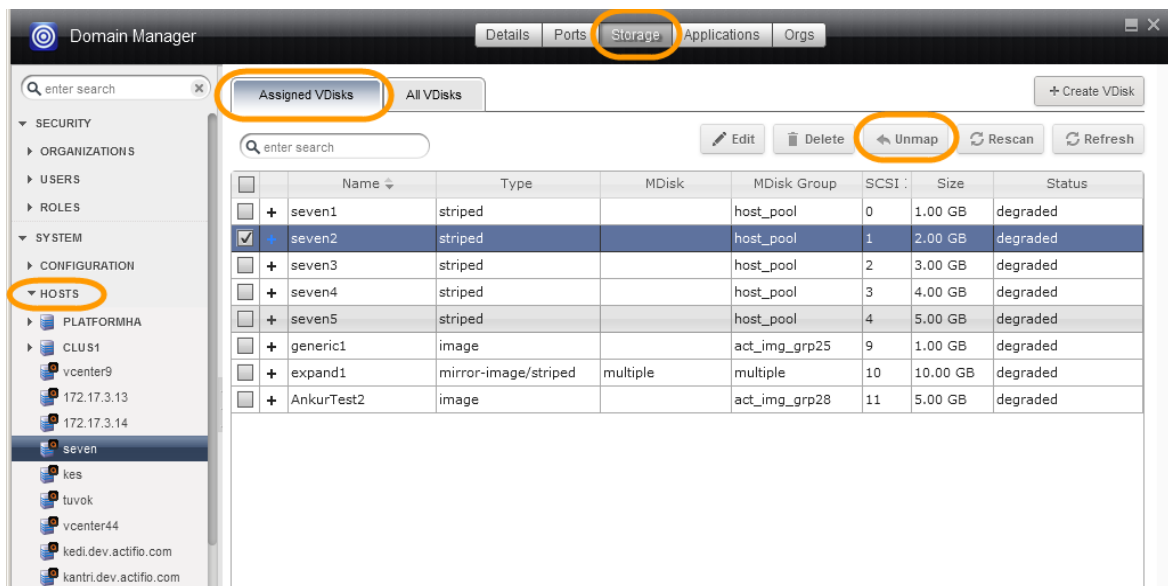


Unmapping a VDisk from a Host

You can remove the mapping between a virtual disk and a host by using the Unmap functionality. The VDisk unmapping process makes the unmapped virtual disks available to other hosts.

To unmap a VDisk from a host:

1. Open the Actifio Desktop to the **Domain Manager**.
2. Select the **Host** from the navigation pane.
3. Select **Storage** tab and the **Assigned VDisks** subtab. The VDisks mapped to the host are listed.
4. Select one or more VDisk(s) from the list.
5. Click **Unmap**. A confirmation dialog appears.
6. Click **OK**. The selected virtual disk is unmapped from the host.



Expanding a Virtual Disk

The Expand Virtual Disk functionality is used to increase the size of an existing VDisk. The VDisk Expansion Wizard allows you to perform this function.

Note: Expansion is supported only on disks that are created in Mirror Mode (Image-Striped).

Note: A VDisk can be expanded only if it has no snapshots.

To expand a VDisk:

1. Open the Actifio Desktop to the **Domain Manager**.
2. Select the **Host** from the navigation pane.
3. Select **Storage** tab and the **Assigned VDIs** subtab. The VDIs mapped to the host are listed.
4. Select the VDisk that you want to extend and then click **Extend**.

Note: The Extend option is available only after selecting a single VDisk, and is supported only for Mirror Mode (Image-Striped) VDIs. The Extend option is not available if you select multiple VDIs.

The VDisk Expansion Wizard opens to allow you to extend the size of a VDisk in an existing mirror configuration.

Note: Clicking **Next** disrupts the mirroring operations. Make sure to extend the Image Mode MDisk before proceeding.

5. Click **Next**. The Wizard displays the old and new size of the Image Mode MDisk.
6. Review and confirm the MDisk expansion results. This new size is the reflection of changes manually made to the storage array. Use the Refresh function if the new size value is not reflected.

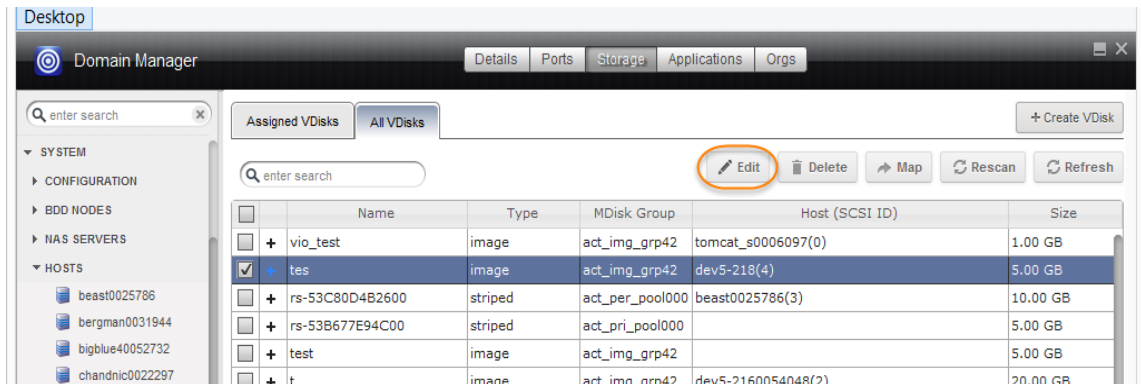
Note: If required, you can change the sync-rate by using the Select Sync Rate drop-down. Sync-rate specifies the rate for synchronization for mirrored copies. The default sync-rate is 64 MB per second.

7. Click **Next**. The Wizard displays the available MDIs to add to the striped set. S
8. Select the MDisk(s) you wish to add, then click **Use Selected MDisk(s)** to proceed with re-establishing the mirror. This wizard gives you additional MDisk storage that is required to be added on Striped Mode MDisk for establishing the mirror. The wizard screen displays the percentage of mirroring progress.
9. Click **Close** to complete the process. You can see the mirroring status in the Assigned VDisk grid.

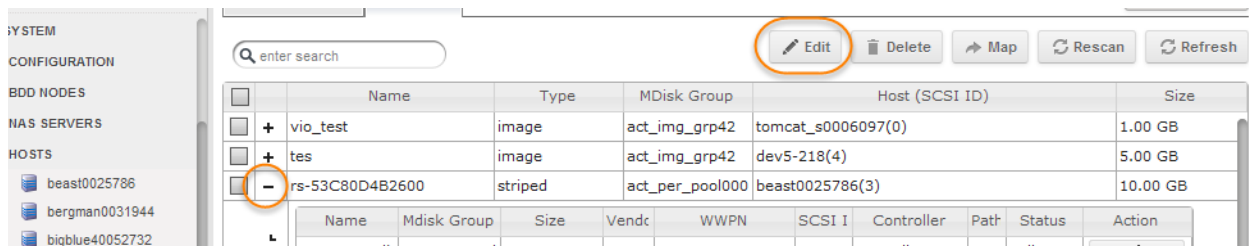
Renaming VDisks and MDisks

To rename a VDisk or an MDisk:

1. Open the **Domain Manager** to **System > Configuration > Hosts** and select a host.
2. Click the **Storage** tab.
3. Select the **All VDisks** subtab. All VDisks (mapped and unmapped) are listed.



4. Select the VDisk you wish to rename. To rename an MDisk, select the VDisk and expand it by clicking the [+] symbol. The managed disks associated with the selected VDisk are displayed.



5. Click the **Edit** button.
6. The **Edit VDisk** dialog appears. Enter a new name for the VDisk, then click **Update Name**.

Deleting a Virtual Disk

This task allows you to delete mapped and unmapped virtual disks. When you delete a mapped virtual disk under the Assigned Virtual Disks tab, the virtual disk is first un-mapped and then deleted.

To delete a VDisk from an Actifio CDS appliance:

1. Open the **Domain Manager** to **System > Configuration > Hosts** and select a host.
2. Click the **All VDisks** or the **Assigned VDisks** tab.
3. Select the **All VDisks** tab. All the VDisks (mapped and unmapped) are listed.
4. Select VDisk(s) from the list. A warning dialog appears.
5. Enter **DATA LOSS** in the DATA LOSS field.
6. Click **Delete VDisk(s)**. The selected VDisk is removed from the Actifio CDS appliance.

20 Configuring a BDD Node

This section describes the configuration of the BDD Node. Once a BDD node has been installed and the software installation step completed, the BDD Nodes selection appears in the left pane of the Domain Manager, above a selection for the NAS Servers that host the data. The NAS Servers are detailed in [Chapter 21, Adding NAS Servers](#). There are additional controls relating to protecting and recovering data in the Application Manager.

Note: BDD Nodes and NAS servers are not applicable to Sky appliances.

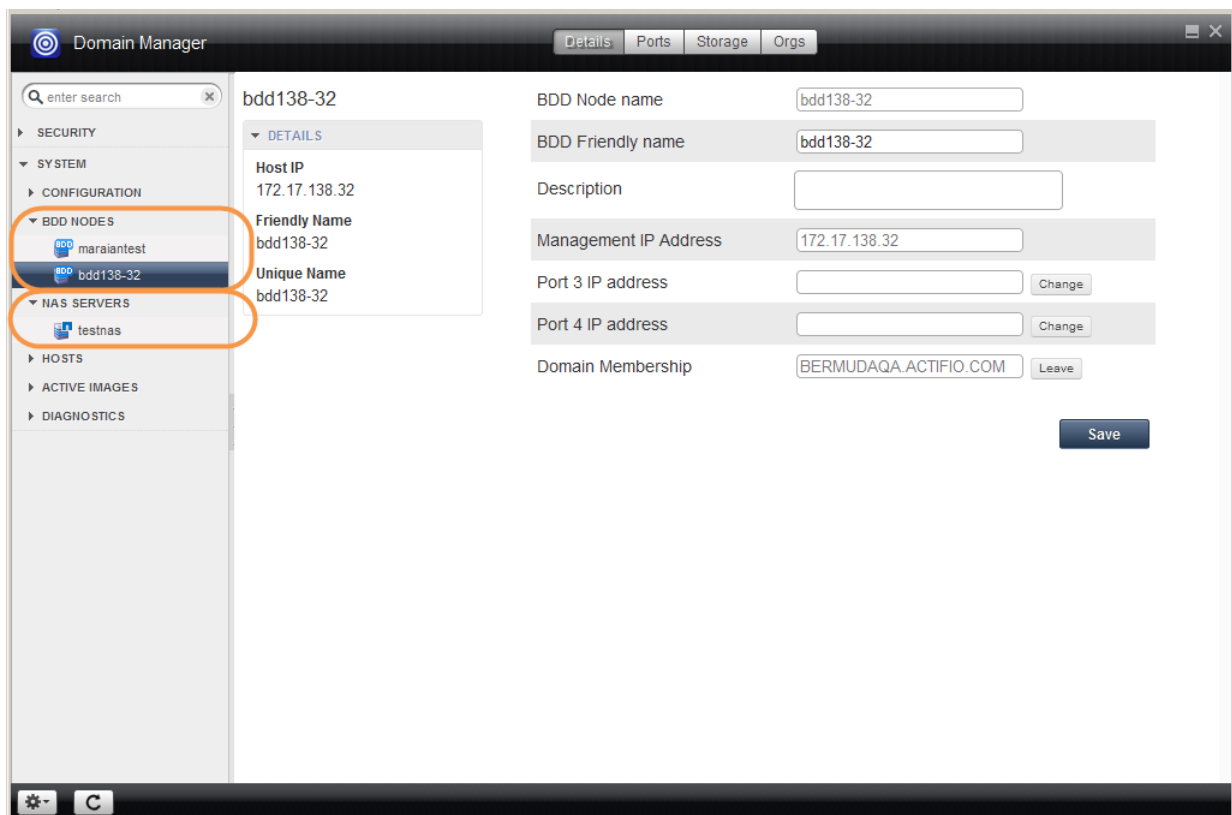
This section describes:

[Viewing and Modifying the Details of a BDD Node Configuration](#) on page 118

[Configuring the Ports of a BDD Node](#) on page 120

[Viewing the Storage on a BDD Node](#) on page 121

[Viewing the Organizations to which a BDD Node Belongs](#) on page 121



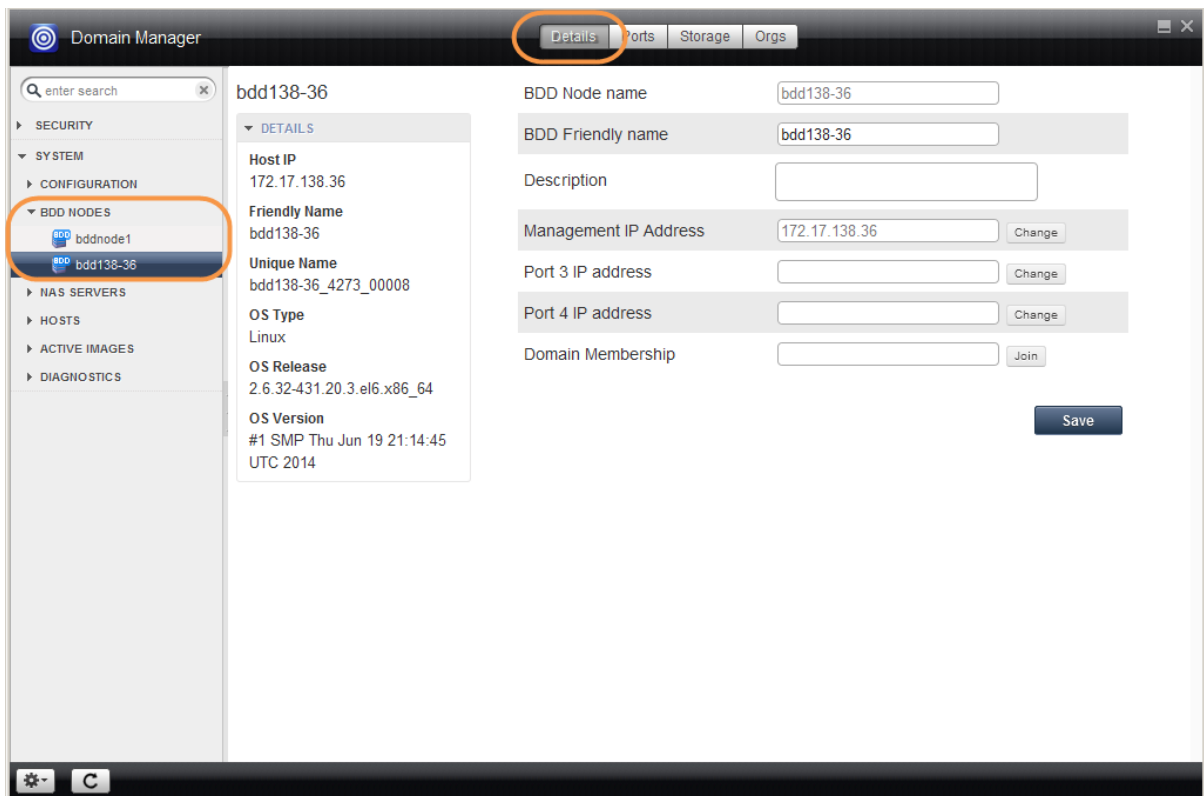
An Actifio Enterprise System that Includes BDD Shows BDD Nodes and NAS Servers

Viewing and Modifying the Details of a BDD Node Configuration

Click on a BDD Node to display the current properties of the BDD Node and to change some of the properties.

The properties shown on the Details tab are:

- BDD Name
- BDD Friendly name
- Description
- Management IP address
- Port 3 IP address
- Port 4 IP address
- Domain Membership



The Details for a BDD Node

Setting the Port 3 or Port 4 IP Address

Setting the IP addresses of Port 3 or Port 4 is straightforward. If a valid set of inputs is provided, the change of address will be completed. There is no guarantee that the port will be able to reach the customer network, and no test to prove that this is the case.

Changing any of the IP addresses brings up a dialog box that shows:

- IP Address
- Gateway
- Net Mask

A dialog box titled "Change Port 3 IP Address" with a close button in the top right corner. It contains three input fields: "IP Address*", "Gateway*", and "Net Mask*", each with a corresponding text box. At the bottom right, there are two buttons: "Apply" and "Cancel".

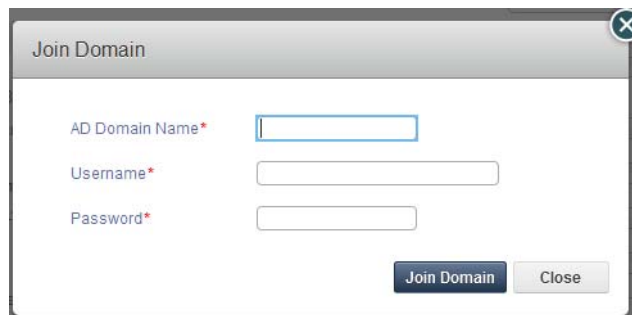
Changing the Port 3 or Port 4 IP Address of a BDD

Joining a BDD Node to a Windows Domain

If the BDD Node is not currently a member of a Windows domain, the Join button is displayed in the Details pane. Pressing the Join button displays a dialog that has the following fields:

- Domain Name (DNS resolvable name of the Domain Controller)
- Administrative User name
- Password

Fill out these fields and press **OK** to join the BDD to the domain.

A dialog box titled "Join Domain" with a close button in the top right corner. It contains three input fields: "AD Domain Name*", "Username*", and "Password*", each with a corresponding text box. At the bottom right, there are two buttons: "Join Domain" and "Close".

Joining a BDD to a Windows Domain

Leaving a Domain

If the BDD Node is joined to a domain, a Leave Domain button is shown in the details pane. Pressing this button displays a dialog with the following fields:

- Administrative User name
- Password

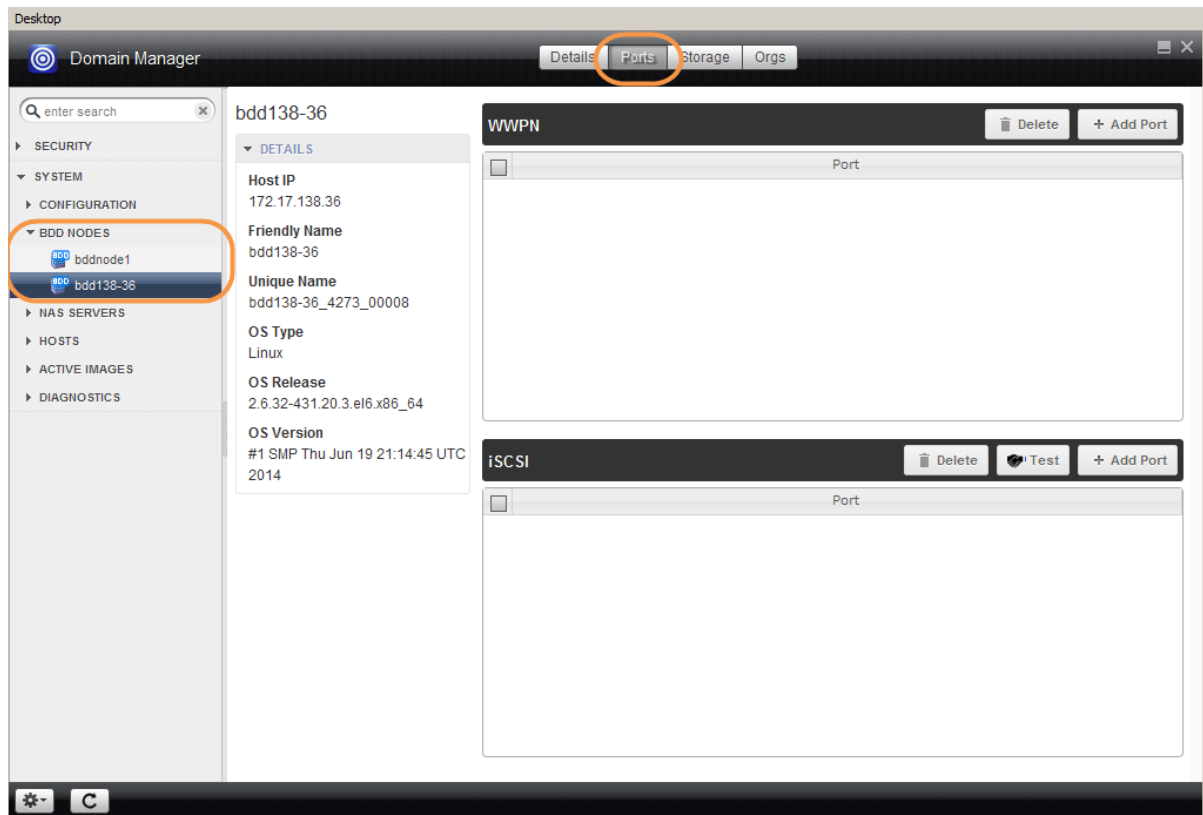
Press **OK** to attempt to leave the domain. If the action fails, the BDD Node remains a member of the domain.

Configuring the Ports of a BDD Node

The ports pane shows Fibre Channel ports configured for the BDD. You can configure one or more ports of a host.

To configure the ports of a host:

1. Open the **Domain Manager** to **System > Configuration > Hosts** and click the **Ports** tab.
2. Add the World Wide Port Name (WWPN) of the Host. To add or choose the WWPN, click **+Add Port** in upper-right corner of the WWPN panel. The Add Port dialog appears. Choose the corresponding WWPN of the host or enter the WWPN using the Custom... option, then click **Add Port**.

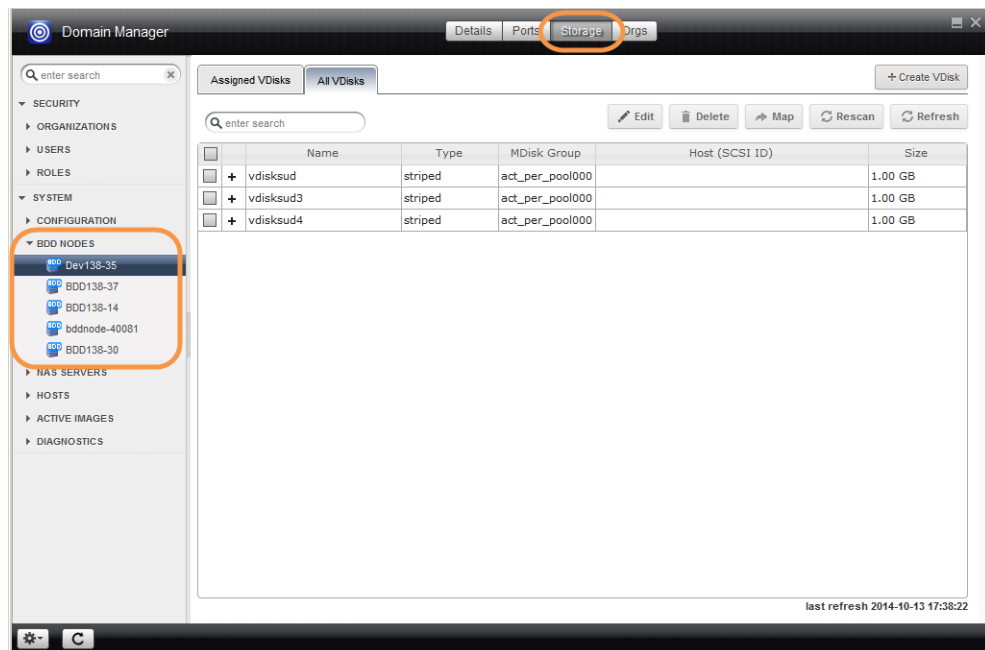


Adding Fibre Channel Ports for the BDD

Note: Ignore the lower iSCSI section.

Viewing the Storage on a BDD Node

The storage pane shows indexing volumes and staging volumes (if any) that might be currently exported to the BDD.



The Storage Tab for a BDD Node

Viewing the Organizations to which a BDD Node Belongs

The **Organizations** pane shows the Organizations of which the BDD Node is a member.



The Orgs Tab Shows the Organizations to which a BDD Node Belongs

21 Adding NAS Servers

Before you can protect an application's data, you must first add its NAS Server to an Actifio appliance and specify its ports and virtual disks. NAS server details can be modified via the Details tab. Datasets currently protected from a NAS server can be viewed via the Applications tab.

Note: *BDD Nodes and NAS servers are not applicable to Sky appliances.*

This section describes:

- [Adding a NAS Server](#) on page 124

- [Viewing and Modifying NAS Server Details](#) on page 126

- [Viewing Datasets on a NAS Server](#) on page 127

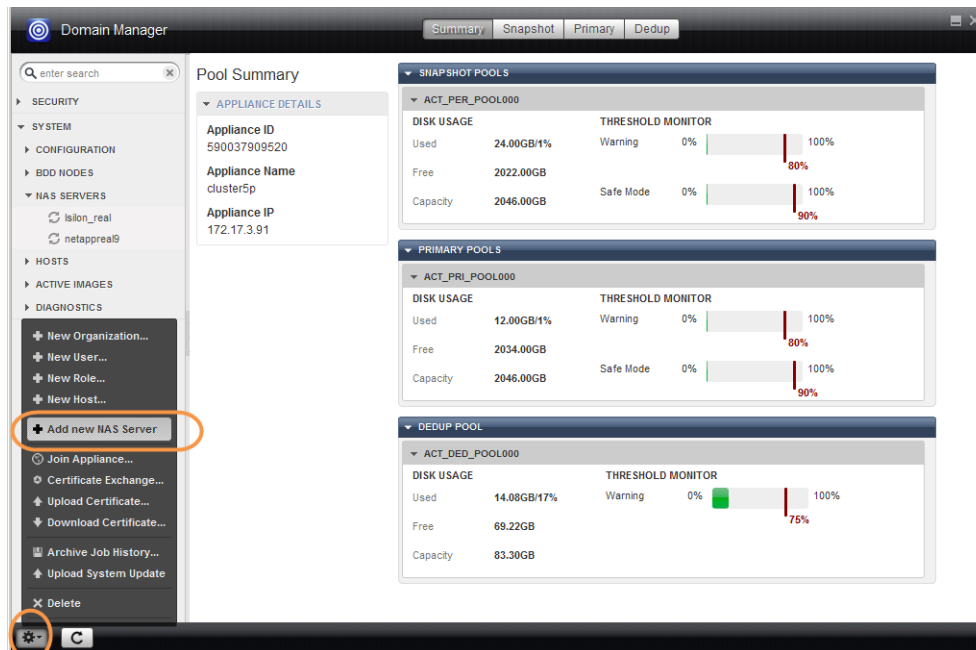
- [Viewing the Organizations to which a NAS Server Belongs](#) on page 128

Adding a NAS Server

You can add a NAS server and discover the datasets running on it to protect them.

To add a new NAS server:

1. Open the **Domain Manager**.
2. From the service menu, select **Add New NAS Server**.



Adding a NAS Server

3. The Add New NAS Server dialog appears.

The 'Add New NAS Server' dialog box is shown. It contains the following fields:

- NAS Server Name*: netappreal8
- IP Address*: 172.17.130.8
- Type*: NetApp (dropdown menu)
- Management port number: 443
- Management Username*: admin
- Management User's password*: (masked with dots)

At the bottom are two buttons: 'Add new NAS Server' and 'Close'.

Adding a NAS Server: Details

4. Enter a **NAS Server Name** that is unique within this CDS appliance.
5. Enter an **IP Address**.

6. For **Type** select either Isilon or NetApp.
7. The **Management port number** is filled in automatically based on your selection of Isilon or NetApp.
8. **Management Username** and a valid **Management User's password**.
9. Click **Add new NAS Server**.

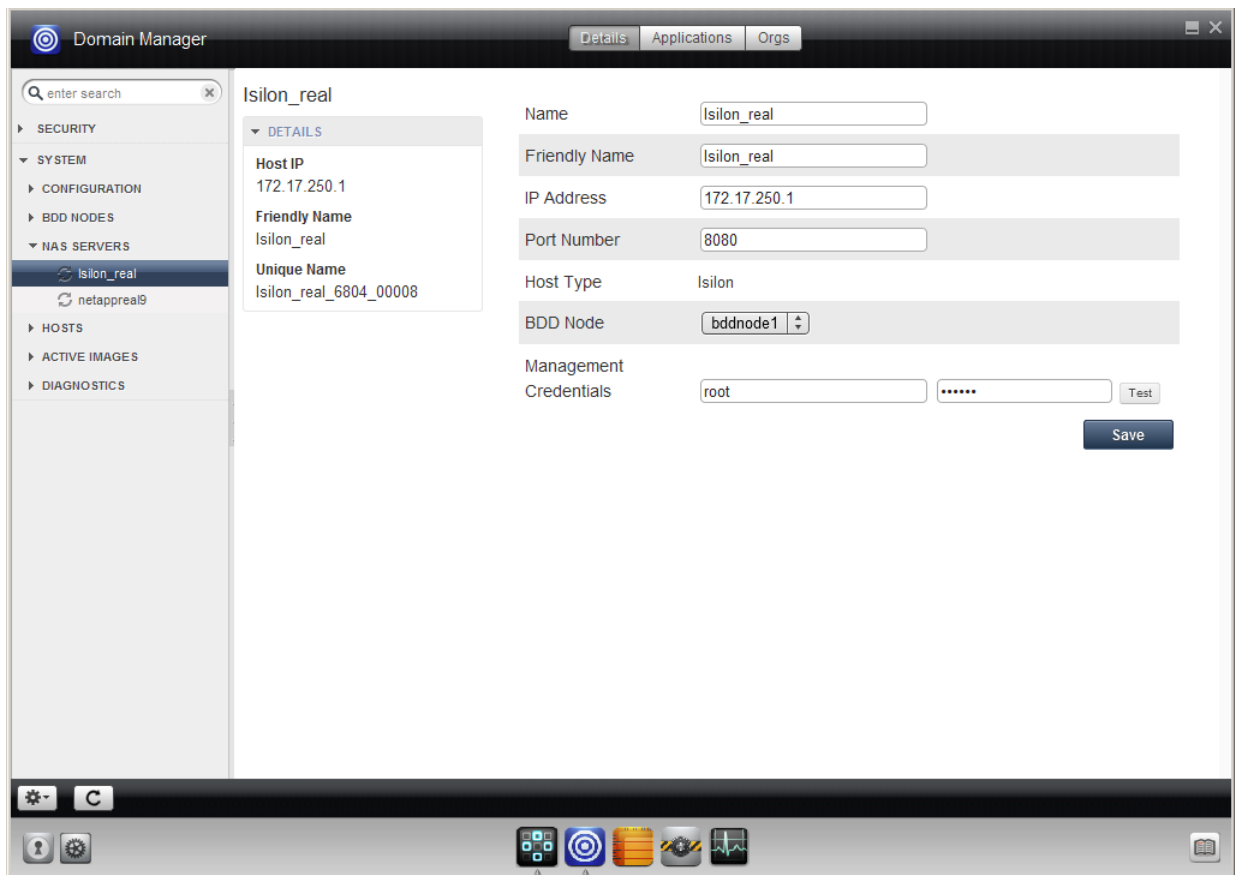
The IP address, port and user authentication parameters are used to connect to the server, and if it all checks out, the NAS server is added, and shows up in the left pane under NAS Servers.

Viewing and Modifying NAS Server Details

You can modify the NAS server details, datasets, and organizations.

To view or modify a NAS server's details:

1. Open the **Domain Manager** to **System > NAS Servers** and click the **Details** tab.
2. Selecting a NAS server in the left pane brings up the details of the server in the right pane.
3. There are tabs for Details, Applications and Organizations. The Details pane of the NAS server allows you to view or modify the NAS Server definition.
4. The Type field cannot be changed after the server has been created. Some of the fields can be modified:
 - o Name
 - o IP Address
 - o Port
 - o Username
 - o Password
5. A test button allows the IP address, port and authentication parameters to be verified.



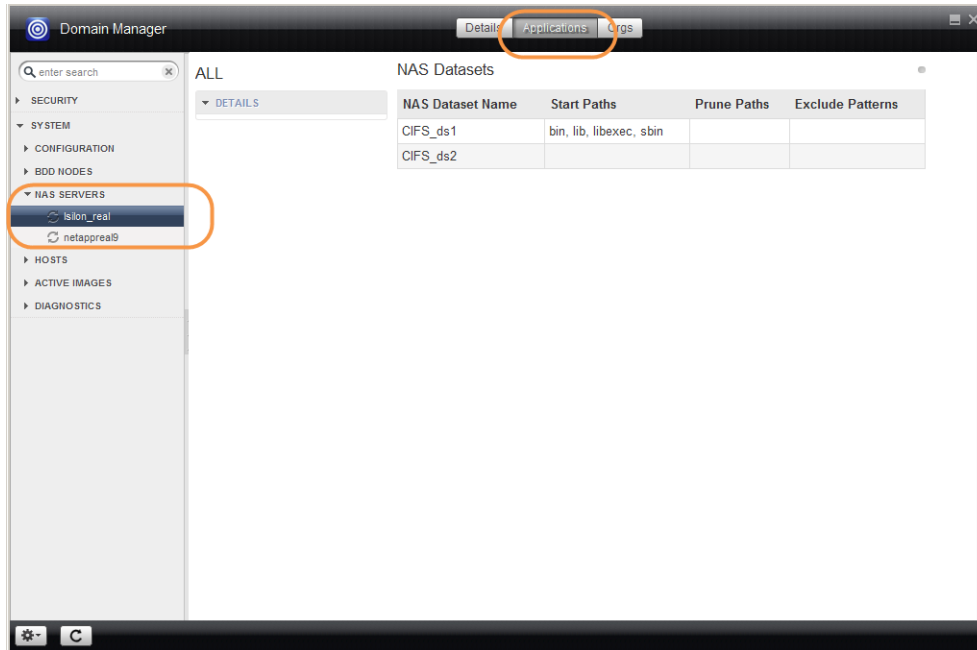
Editing NAS Server Configuration Details

Viewing Datasets on a NAS Server

The NAS server's **Applications** tab shows the datasets that have been defined for the particular NAS Server. The details for each dataset should show the number of unexpired images, and the capacity protected.

To view all protected applications on a NAS server:

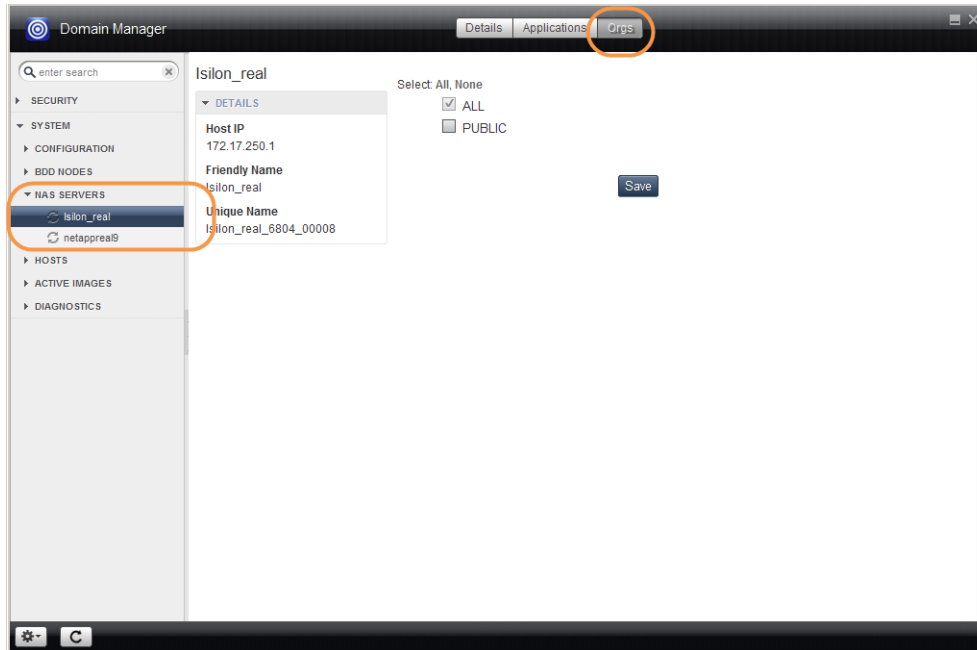
1. Open the **Domain Manager** to **System > NAS Servers**.
2. Select from the list of previously created NAS servers.
3. Click the **Applications** tab. You will see a complete list of datasets for the selected NAS server, and details about them.



The Applications Tab Shows Datasets on a NAS Server

Viewing the Organizations to which a NAS Server Belongs

The NAS Server's **Organizations** tab shows the Organizations of which the NAS server is a member.



The Orgs Tab Shows Organizational Membership

22 Adding Hosts and Editing Host Information

Before you can protect an application's data, you must first add its host to an Actifio appliance. Once the host is added, you must specify its ports and virtual disks.

Applications and VMs that reside on hosts are discovered in the Application Manager Service.

Note: *The Actifio appliance supports multiple hosts with the same Host Name.*

This section describes:

- [Adding a Generic, HP-UX, TPGS, or OpenVMS Host](#) on page 130

- [Adding a Hypervisor Host](#) on page 134

- [Adding an IBM HMC Host](#) on page 136

- [Configuring the Ports of a Host](#) on page 138

- [Viewing Applications on a Host](#) on page 139

- [Viewing and Editing Host Information](#) on page 140

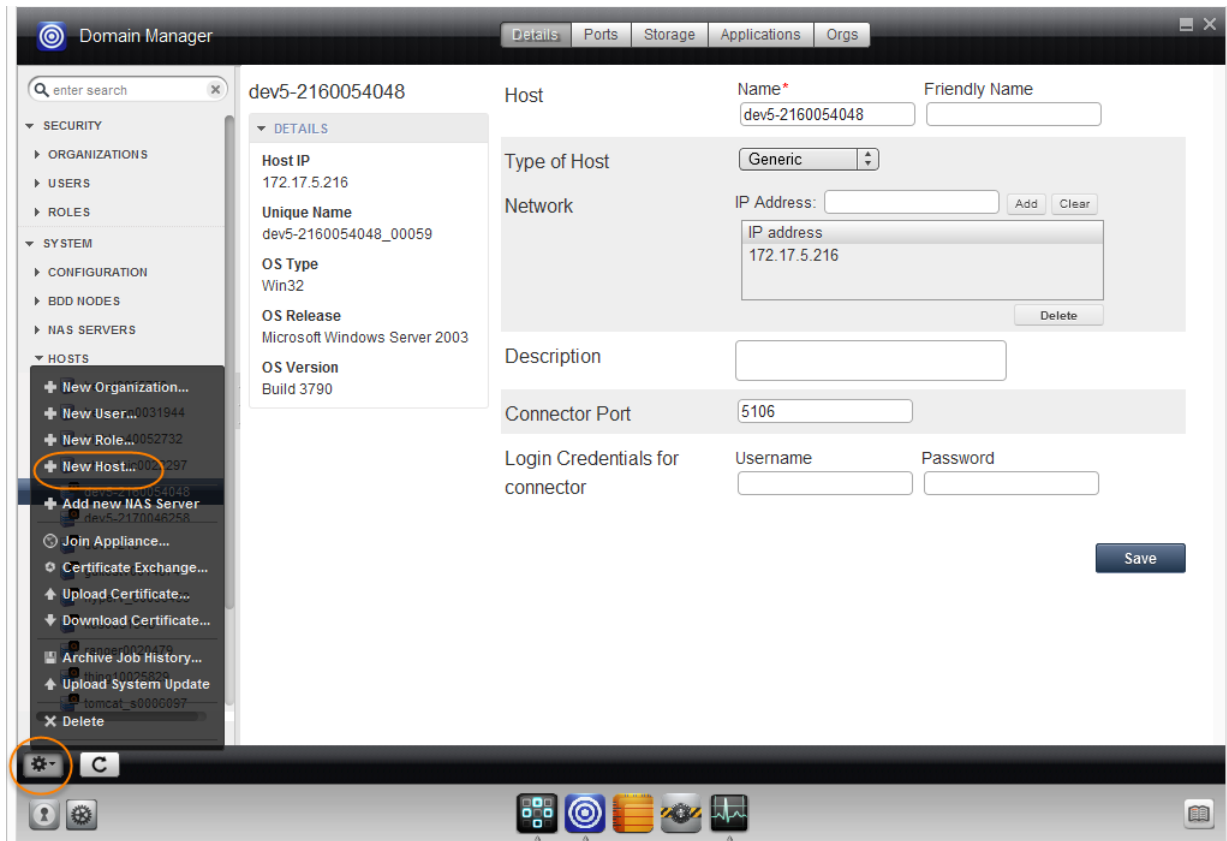
Background information on managing hosts from the Host section of the Domain Manager is provided in [Chapter 18, Managing Hosts](#).

You also need to understand VDisks. VDisks are detailed in [Chapter 19, Configuring Storage for In-Band Hosts](#).

Adding a Generic, HP-UX, TPGS, or OpenVMS Host

To add a new host:

1. Open the **Domain Manager**.
2. From the service menu, select **New Host....**

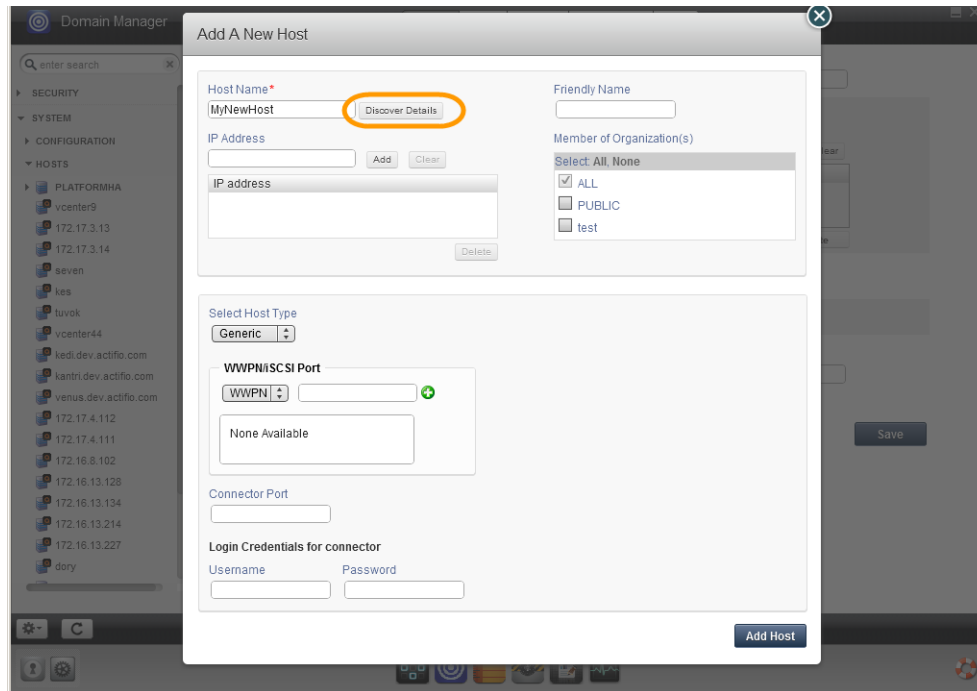


Adding a Host

Types of Hosts

Parameter	Description
Host Name	The name, fully qualified domain name, or the IP address of the host. The name of a host should start with a letter, and can contain letters, digits (0-9), and an underscore ('_').
Friendly Name	The friendly name for the host to complement the specified Host Name and provide an easier to understand name (for example, Finance_Dept_Host).
Network IP Address	To add additional IP addresses for the host, click Add and enter each IP address. To remove the previously set IP address, highlight the IP address, click Delete , and then enter the new IP address. You can enter additional IP addresses by using the Add button.
Type of Host	If a host type has not yet been specified for the host, this field will display None. You can then choose from the following host types: • ESX Host • Generic • HP-UX • Hyper-V Server • IBM HMC • OpenVMS • SCVMM • TPGS • vCenter
Description	Specifies additional information related to the host or related to modifications made to the host.
Connector Port	Identifier of the Actifio Connector port.
Login Credentials for Connector: Username and Password	User name and password of the host or the Actifio Connector on the host. You need to provide the login credentials to run the pre- and post-scripts successfully on the host.

3. In the Add a New Host form, enter the name, fully qualified domain name, or the IP address of the host in **Host Name**. The name of a host should start with a letter, and can contain letters, digits (0-9), and an underscore ('_').



Adding a New Host Form -- Generic Host

4. Enter the friendly name for the host to complement the specified Host Name and provide an easier to understand name (for example, Finance_Dept_Host).
5. Click **Discover Details**. Actifio Desktop lists all IP addresses used by the host.
6. Select the type of host in **Select Host Type**.
7. Enter the IP address of the host in **IP Address**. Click **Add** to add multiple IP addresses for a host.
8. Depending on how the host is accessed, specify one of the following for **WWPN/iSCSI Port**:
 - o If the host can be reached using a Fibre Channel port, select **WWPN (World Wide Port Name)**.
 - o If the host can be reached using an IP network, select **iSCSI** (Internet Small Computer System Interface).

Note: Fibre Channel and WWPN is not applicable to Sky appliances.

You can add multiple port types for a single host.

Note: For HP-UX hosts, if the WWPN is not shown in the selection box, enter the 16-digit WWPN in the space provided and click **Add**. As soon as the host has been added in [Step 11](#) below, map a VDisk to it as detailed in [Mapping a VDisk to a Host](#) on page 111. This is necessary only for HP-UX hosts.

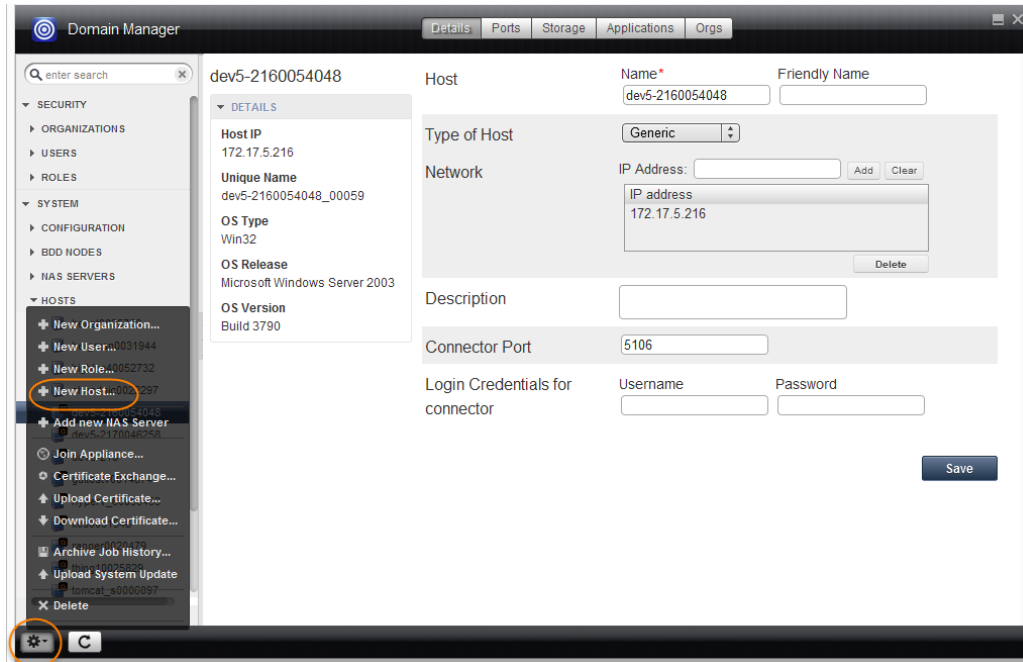
9. To reach the host via an IP network, select **iSCSI**. To add the iSCSI port, click **+Add Port** in upper-right corner of the iSCSI panel. The Add Port dialog appears. Enter the iSCSI host IQN, then click **Add Port**.
10. Enter the user name and password of the Actifio Connector on the host if you intend to:
 - o Run pre- and post-scripts on the host
 - o Protect a CIFS share (the login credentials of the local/domain user on Windows who mapped the share).
11. Click **Add Host**.

Adding a Hypervisor Host

Note: Actifio Desktop and the command line interface do not allow creation of mapped disks to protect Hypervisor hosts. If your deployment requires MDisk allocation to a hypervisor host, define the host type as 'generic'.

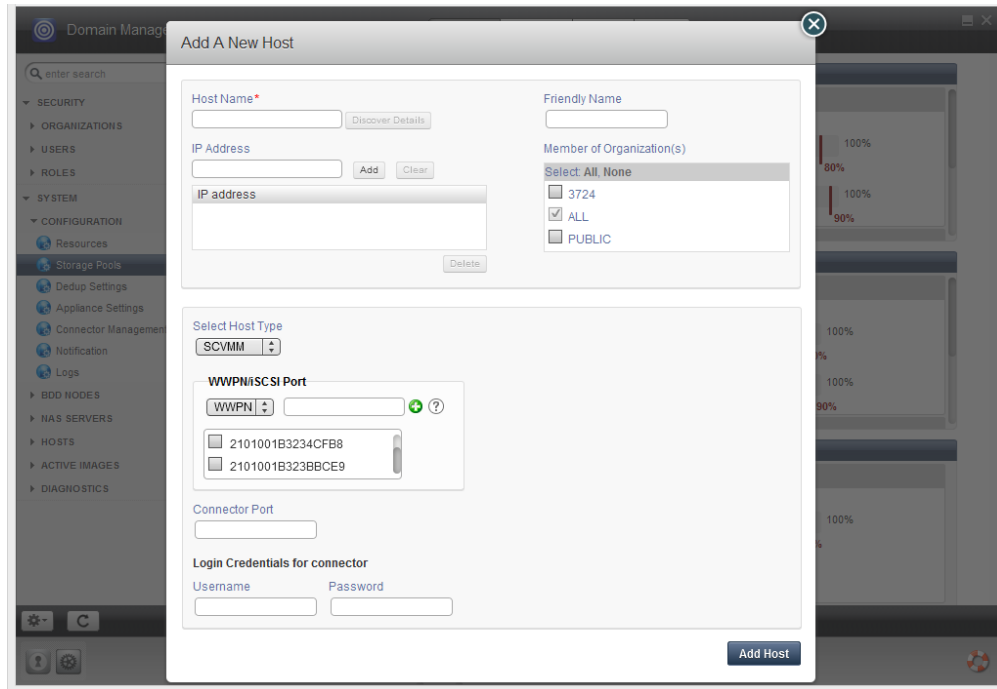
To add a new hypervisor host:

1. Open the **Domain Manager**.
2. From the service menu, select **New Host....**



Adding a New Host

3. In the Add a New Host form, enter the name, fully qualified domain name, or the IP address of the host in **Host Name**. The name of a host should start with a letter, and can contain letters, digits (0-9), and an underscore ('_').
4. Enter the friendly name for the host to complement the specified Host Name and provide an easier to understand name (for example, Finance_Dept_Host).
5. Click **Discover Details**. Actifio Desktop lists all IP addresses used by the host.
6. Enter the IP address of the host in **IP Address**. Click Add to add multiple IP addresses for a host.
7. In **Select Host Type**, select the hypervisor host.



8. Depending on how the host is accessed, specify one of the following for **WWPN/iSCSI Port**:
 - o If the host can be reached using a Fibre Channel port, select **WWPN**.
 - o If the host can be reached using an IP network, select **iSCSI**.

Note: Sky appliances do not connect to Fibre Channel and do not use WWPN.

You can add multiple port types for a single host.

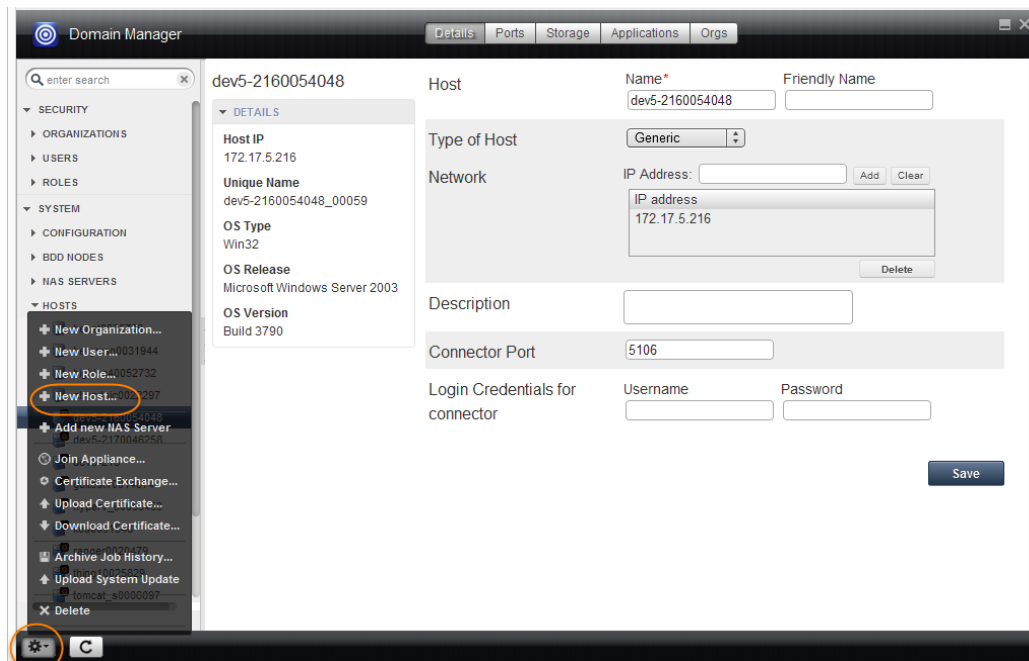
9. To reach the host via an IP network, select **iSCSI**. To add the iSCSI port, click **+Add Port** in upper-right corner of the iSCSI panel. The Add Port dialog appears. Enter the iSCSI host IQN, then click **Add Port**.
10. In the spaces provided, enter the user name and password of the host. This required for the connector to run pre- and post-scripts on the host.
11. Click **Add Host**.

Adding an IBM HMC Host

The Actifio appliance discovers all VIOs and LPARs on the IBM HMC host.

To add a new host:

1. Open the **Domain Manager**.
2. From the service menu, select **New Host...**



Adding a Host -- IBM HMC

3. The Add a New Host form appears.

Adding a New IBM HMC Host

4. Enter the name, fully qualified domain name, or the IP address of the host in **Host Name**. The name of a host should start with a letter, and can contain letters, digits (0-9), and an underscore ('_').
5. Enter the friendly name for the host to complement the specified Host Name and provide an easier to understand name (for example, Finance_Dept_Host).
6. Click **Discover Details**. Actifio Desktop lists all IP addresses used by the host.
7. In **Type of Host**, select IBM HMC.
8. Enter the IP address of the host in **IP Address**. Click **Add** to add multiple IP addresses for a host.
9. In the spaces provided, add the login credentials for the IBM HMC host as needed.
10. Click **Test** to ensure the credentials have been properly entered.

Note: When an IBM HMC host type is added, the LPAR hosts available on that HMC are also discovered. If an LPAR host is created or deleted after the IBM HMC was discovered, use the re-discover option to update the known LPARs.

11. Click **Add Host**.

Configuring the Ports of a Host

You can configure one or more ports of a host.

Note: When you add a vCenter as a host, you cannot define the ports and virtual disks.

To configure the ports of a host:

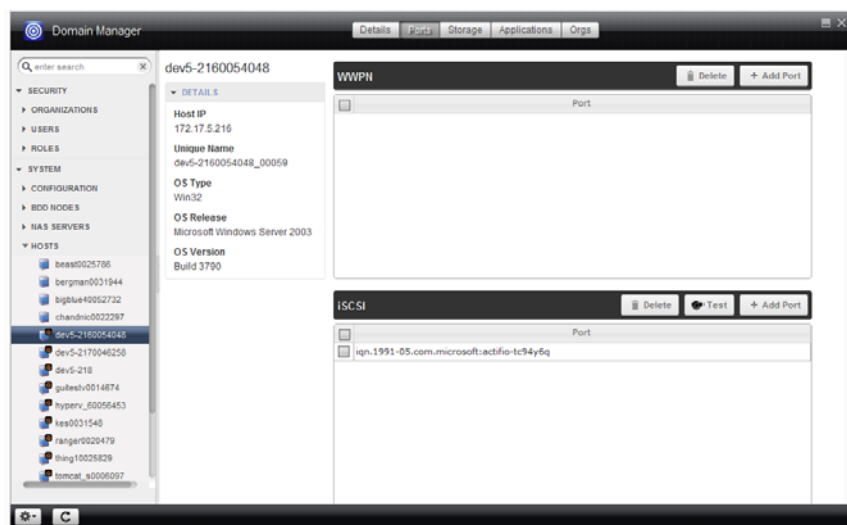
1. Open the **Domain Manager** to **System > Configuration > Hosts** and click the **Ports** tab.
 - o If the host is reached via a Fibre Channel port, add the World Wide Port Name (WWPN) of the Host. To add or choose the WWPN, click **+Add Port** in upper-right corner of the WWPN panel. The Add Port dialog appears. Choose the corresponding WWPN of the host or enter the WWPN using the Custom... option, then click **Add Port**.
 - o If the host is reached over an IP network, add its Internet Small Computer System Interface (iSCSI) port. To add the iSCSI port, click **+Add Port** in upper-right corner of the iSCSI panel. The Add Port dialog appears. Enter the iSCSI host IQN, then click **Add Port**.

Note: Fibre Channel and WWPN is not applicable to Sky appliances.

To reach the host via an IP network, add its iSCSI port. To add the iSCSI port, click **+Add Port** in upper-right corner of the iSCSI panel. The Add Port dialog appears. Enter the iSCSI host IQN, then click **Add Port**.

2. Test the iSCSI Host configuration to verify communication between the Actifio appliance and the Host as follows:
 - o Select single or multiple iSCSI ports, then click **Test**.
 - o Click **OK** in the information dialog.
 - o Click the iSCSI test results link at the top right corner to view the test result. If the test fails, the iSCSI Test Results dialog gives you the reason for failing.

Note: To perform the iSCSI test on a Host system, the Actifio Connector must be installed on the host unless the host is an ESX server.



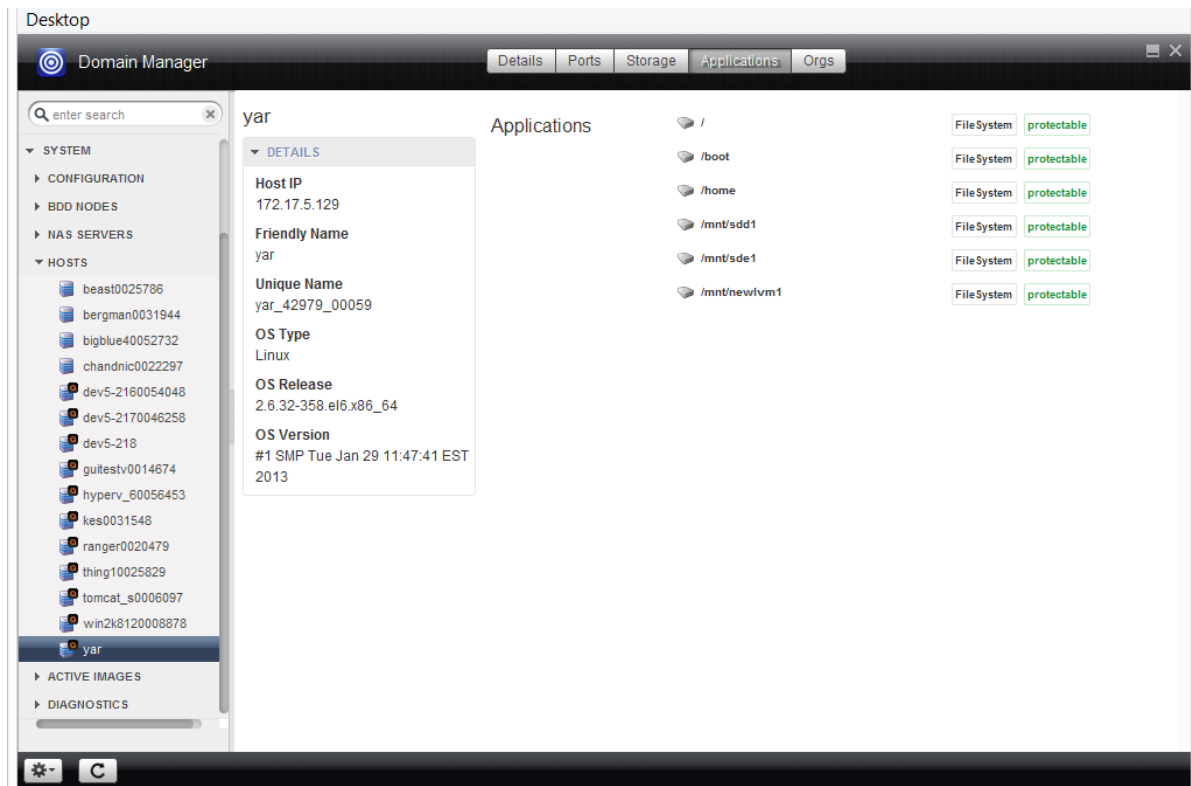
Adding Ports

Viewing Applications on a Host

After you add a host to the Actifio appliance and discover the applications running on that host, you can access the Applications tab to view information about the applications protected on each host.

To view all protected applications on a host:

1. Open the **Domain Manager** to **System > Configuration > Hosts**.
2. Select from the list of previously created hosts in the Hosts section of the Domain Manager.
3. Click the **Applications** tab. You will see a complete list of applications for the selected host, and an identification as to whether those applications are protected by the Actifio appliance.



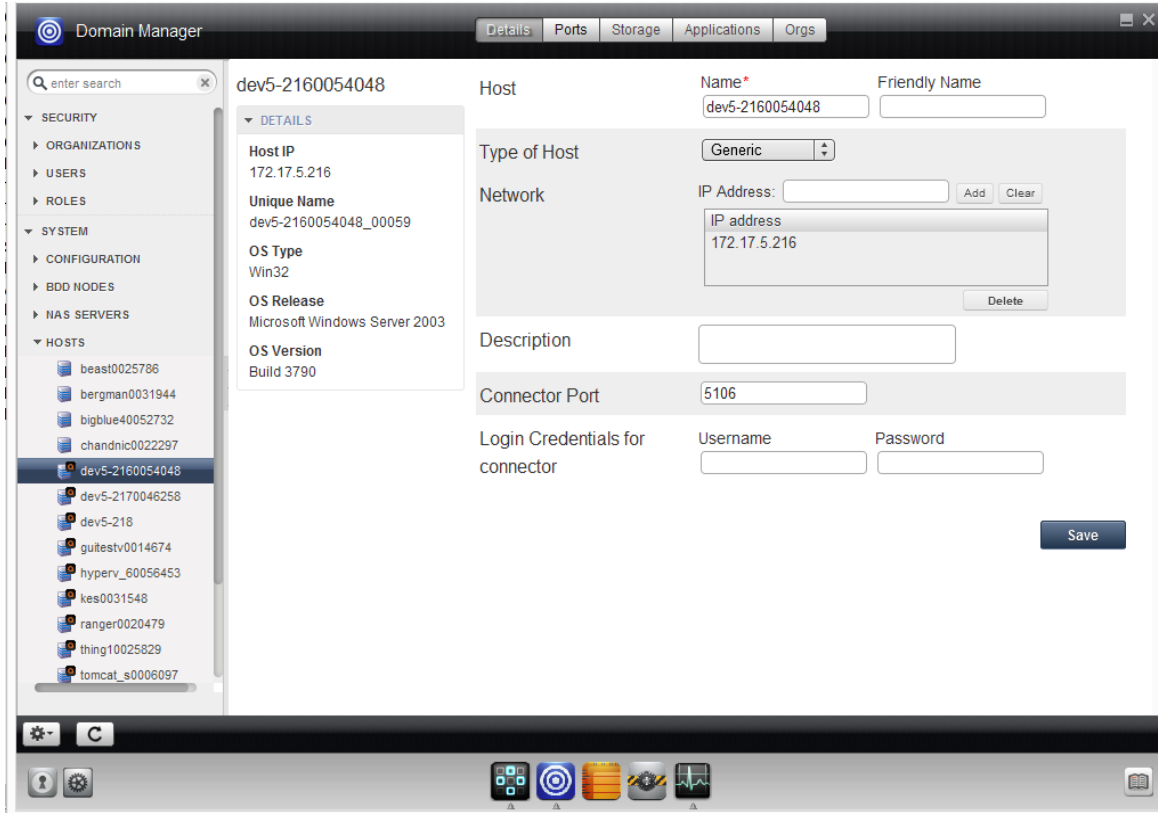
The Applications Tab for Applications Discovered and Protected on a Host

Viewing and Editing Host Information

After you add and configure a host to the Actifio appliance, you can use the Details tab to view and edit information about this host.

To view and edit information related to a configured host:

1. Open the **Domain Manager** to **System > Configuration > Hosts**.
2. Select from the list of previously created hosts in the Hosts section of the Domain Manager.
3. Click the **Details** tab. You will see a summary of configuration information related to the selected host. If required, you can make updates to the following editable parameters for this host.



The Details Tab for An Out-of-Band ESX Host

23 Unmounting Active Images

Active images are mounted copies of backup images. Mounting a backup image presents a copy of the image to a host. You can access the mounted and unmounted images under the Active Images section of the Domain Manager. When you are finished with the Active Image, you can unmount the image, or you can unmount and delete the image.

This section details:

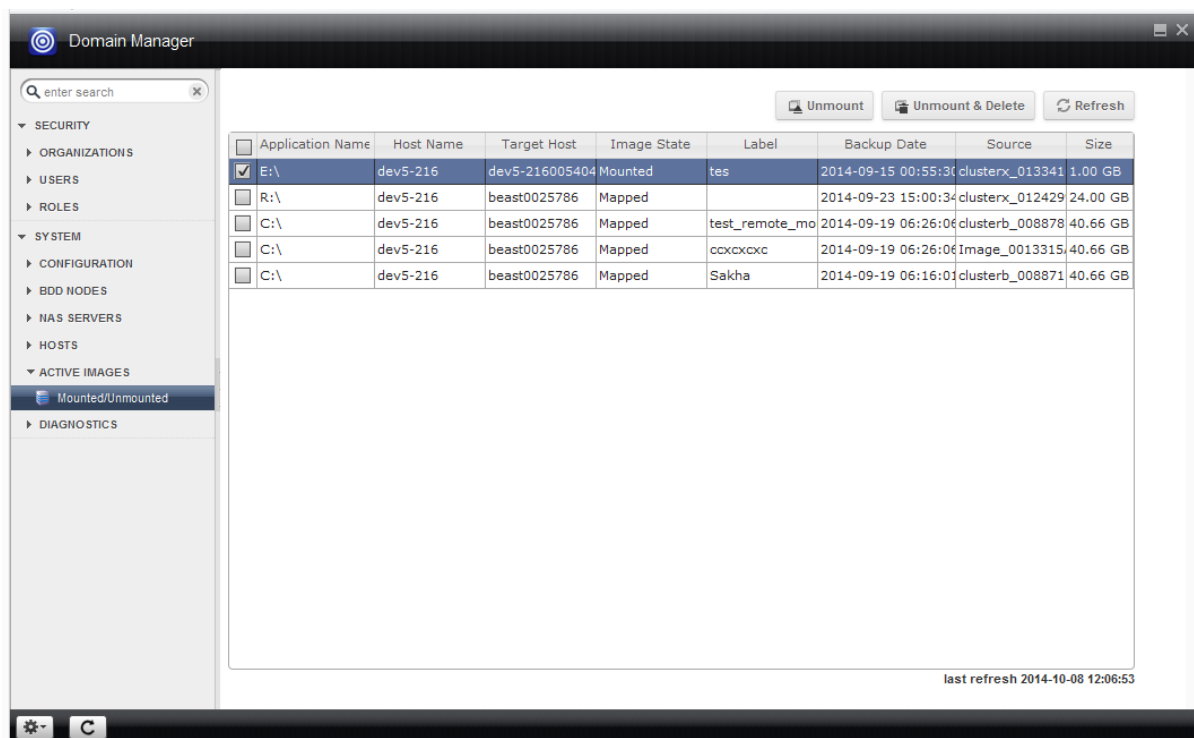
[Unmounting an Image](#) on page 142

[Deleting an Unmounted Image](#) on page 142

[Unmounting and Deleting an Active Image](#) on page 143

[Unmount & Accept Changes or Reject Changes to Prep-Mounted LiveClones](#) on page 144

Note: Images are not mounted in the Active Images section of the Domain Manager; you mount images from the Application Manager Restore tab.



☐	Application Name	Host Name	Target Host	Image State	Label	Backup Date	Source	Size
☒	E:\	dev5-216	dev5-216005404	Mounted	tes	2014-09-15 00:55:30	clusterx_013341	1.00 GB
☐	R:\	dev5-216	beast0025786	Mapped		2014-09-23 15:00:34	clusterx_012429	24.00 GB
☐	C:\	dev5-216	beast0025786	Mapped	test_remote_mo	2014-09-19 06:26:06	clusterb_008878	40.66 GB
☐	C:\	dev5-216	beast0025786	Mapped	ccxcxcxc	2014-09-19 06:26:06	image_0013315	40.66 GB
☐	C:\	dev5-216	beast0025786	Mapped	Sakha	2014-09-19 06:16:01	clusterb_008871	40.66 GB

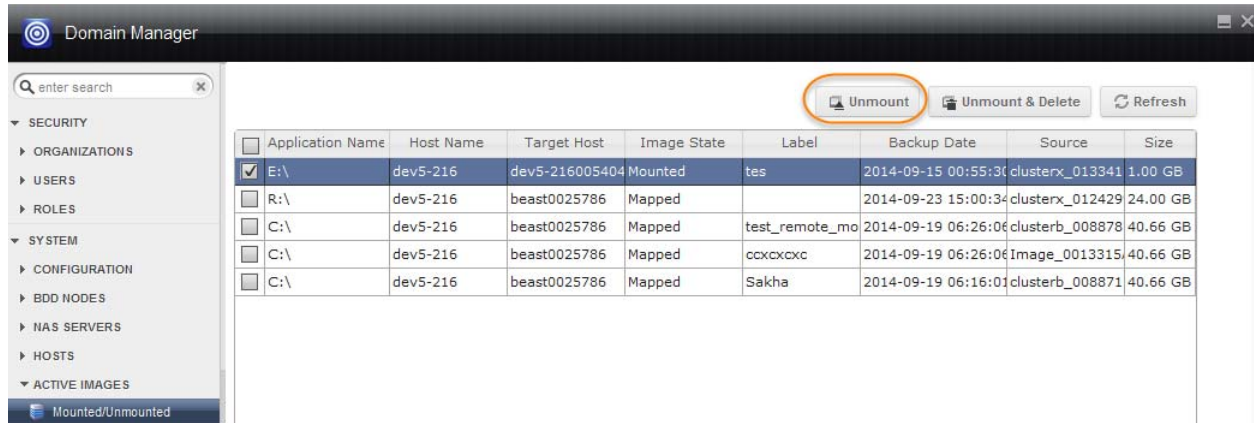
last refresh 2014-10-08 12:06:53

The Global List of Currently Mounted, Unmounted, and Mapped Images

Unmounting an Image

To unmount an image from a host:

1. Open the **Domain Manager** to **Active Images > Mounted/Unmounted** (in the navigation pane). All mounted and unmounted images are listed.
2. Select a single image or multiple images using the appropriate check boxes.
3. Click **Unmount**.
4. Click **Yes** in the confirmation dialog.
5. Click **Refresh** to refresh the images list.

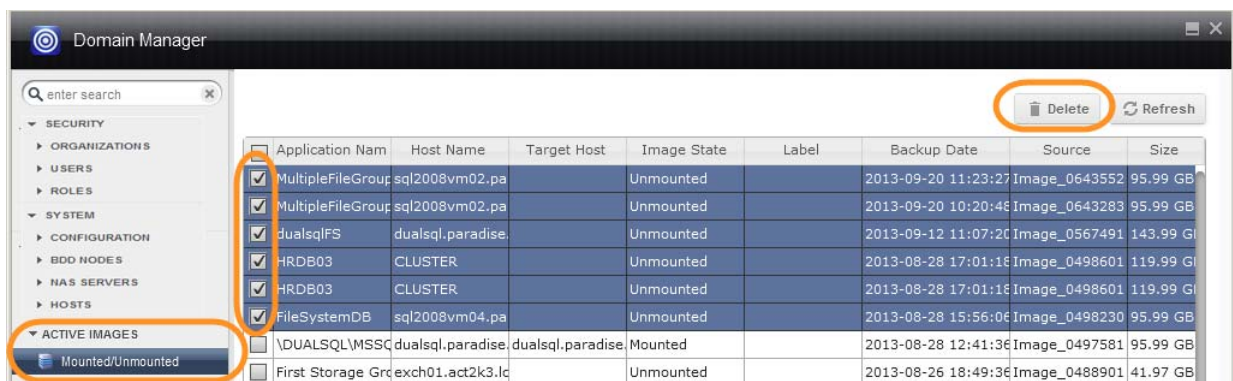


Unmounting an Active Image

Deleting an Unmounted Image

Images take up storage space, so it is a good idea to delete unneeded images. To remove an unmounted image:

1. Open Actifio Desktop to the **Domain Manager**.
2. Click **Active Images > Mounted/Unmounted** from the navigation pane. All mounted and unmounted images are listed in the right panel.
3. Select a single or multiple images using the appropriate check boxes.
4. Click **Delete**.
5. Click **Yes** in the confirmation dialog.
6. Click **Refresh** to refresh the images list.

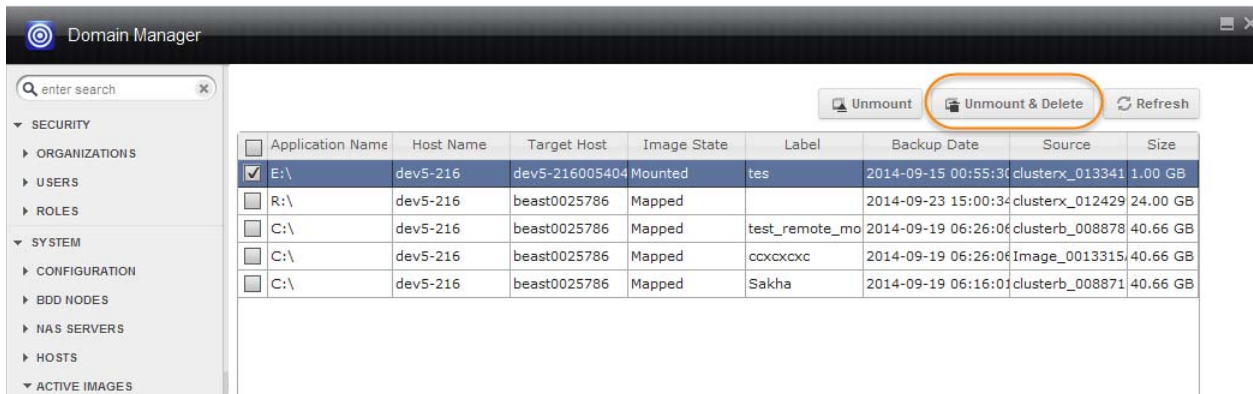


Deleting Unmounted Images

Unmounting and Deleting an Active Image

To unmount and delete a mounted image:

1. Open Actifio Desktop to the **Domain Manager**.
2. Click **Active Images > Mounted/Unmounted** from the navigation pane. All the Mounted and Unmounted images are listed in the right panel:
3. Select a single or multiple images using appropriate check boxes.
4. Click **Unmount & Delete**.
5. Click **Yes** in the confirmation dialog.
6. Click **Refresh** to refresh the images list.



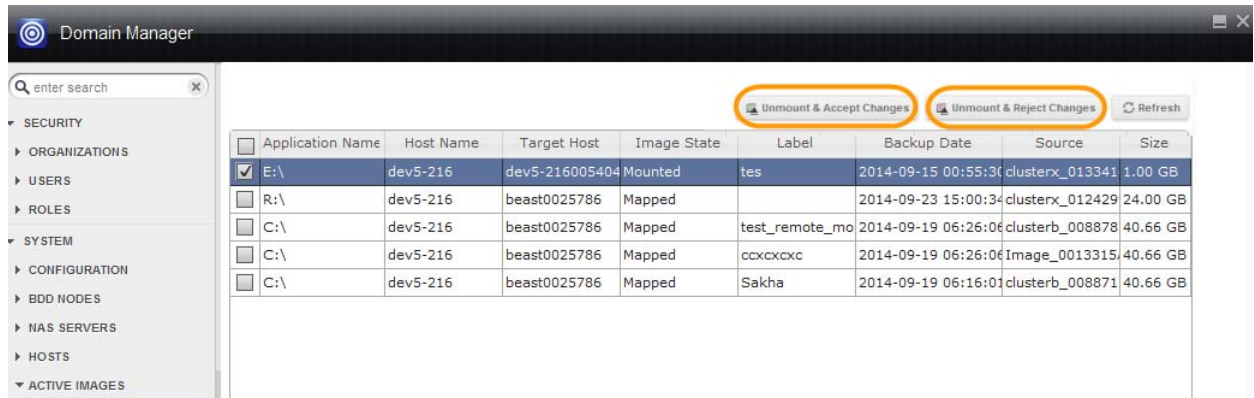
Unmounting and Deleting an Active Image in a Single Operation

Unmount & Accept Changes or Reject Changes to Prep-Mounted LiveClones

LiveClone images permit prep-mounting images for additional preparation work before presenting the prepped LiveClone image to a host.

When you are finished working on a prep-mounted LiveClone image, you can:

- Unmount & Accept Changes
- Unmount & Reject Changes



Unmount and Accept Changes or Reject Changes

24 Using Diagnostics

The Actifio appliance provides two sets of diagnostic tools in the Diagnostics section of the Domain Manager:

[Charts](#) on page 145

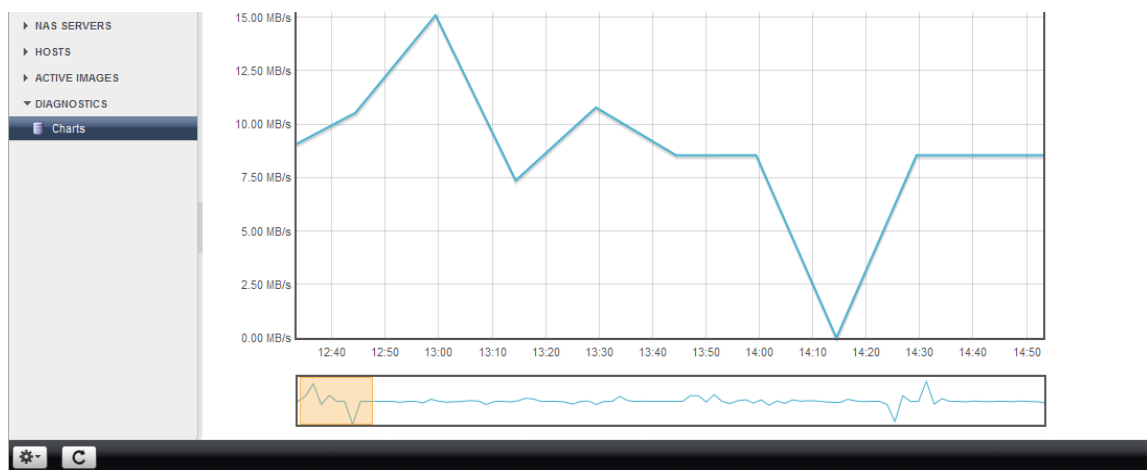
[SSD Status Monitoring](#) on page 146

Charts

The Actifio appliance includes a suite of diagnostic charts to help you keep your system running efficiently. Information from the diagnostic charts can help you to plan changes to your Actifio system and to identify problems and potential problems with your Actifio system.

To display diagnostic charts:

1. Open the **Domain Manager** to **Diagnostics > Charts**.
2. You can select the past day, week, or month to display the following diagnostic information:
 - Dedup - Data Deduped**: The actual amount of data processed by dedup, in MB/sec.
 - Dedup - Disk IOPS**: The disk I/O per second required by dedup.
 - Dedup - Disk I/O**: The logical amount of data replicated by dedup, in KB/sec.
 - Dedup - Jobs**: The jobs/sec relative to capacity measured by the number of cores assigned.
 - Dedup - Replication**: The amount of data replicated by dedup in MB/sec.
 - Snapshot - Disk IOPS**: The disk I/O per second required by snapshots.
 - Snapshot - Disk I/O**: The logical amount of data required for snapshots, in KB/sec.
 - VDisk Count**: A count of SVC VDIs every 15 minutes.
3. Use the zoom display below the selected chart to expand on a particular period of time. To zoom:
 - o Click-drag within a desired time period in the zoom display to select the view area. You can repeat this process for different time intervals in the display.
 - o To revert back to the normal chart display, click anywhere within the zoom display.



Selecting the View Area on a Diagnostics Chart

SSD Status Monitoring

The solid-state drive (SSD) memory in your Actifio CDS appliance improves dedup performance. SSD devices can degrade over time. Use the SSD item that appears beneath Charts in the Diagnostics section of the System list to review the status and expected remaining life of your SSD drives.

Note: SSD Device Status is not applicable for the Actifio Sky appliance.

The status of the drives is color-coded:

Green: The SSD drive is in use.

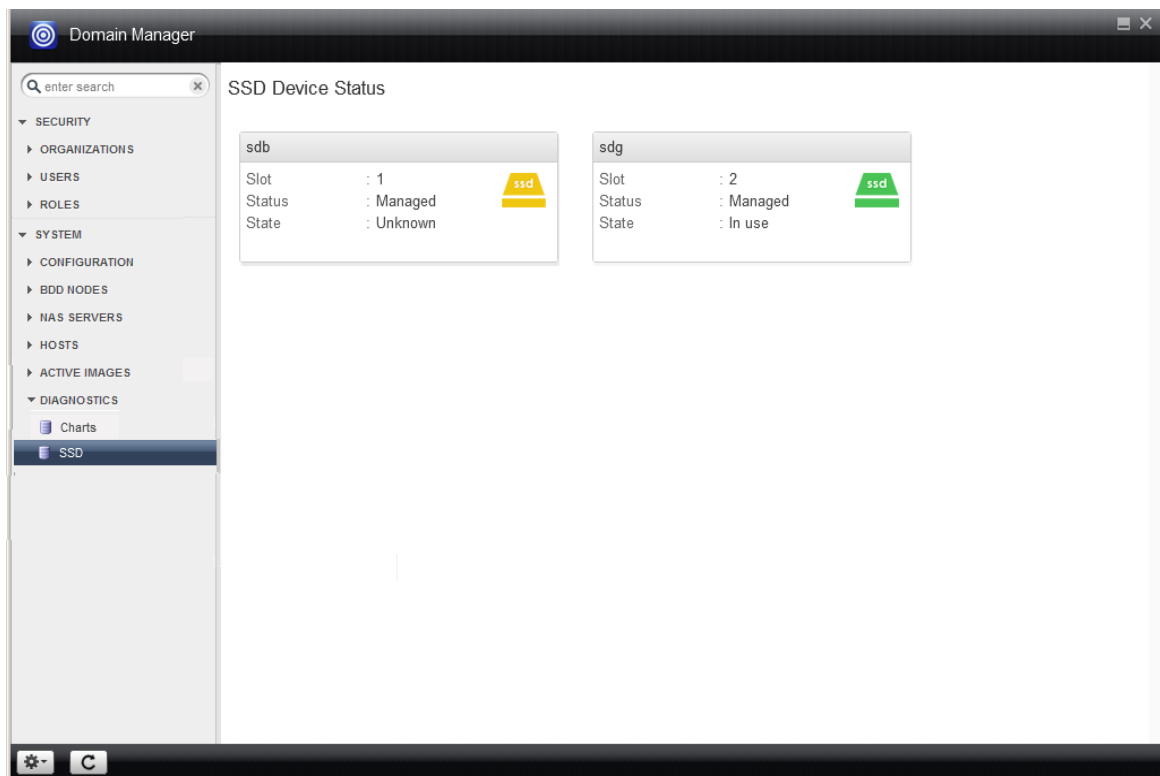
Yellow: The SSD drive is installed and pending activation by Actifio Support.

Blue: The SSD drive is not in use. The drive may be full.

Red: The SSD drive is installed, but errors exist.

Gray: The SSD drive is installed, but not managed by Actifio CDS appliance

Note: If any SSD icon is not green, or if any SSD device has less than 50% remaining life, Contact Actifio Support.



SSD Device Status

Index

A

- Actifio Activity Monitor 16
- Actifio Change Tracking Driver 19
- Actifio Connector
 - about 16
 - Connector Manager, using 68
 - keeping updated 68
- Actifio MIB, accessing 93
- Active Images, about 141
- act_pri_pool000 (primary pool) 22
- additional storage pools 27
- alerts, see notifications
- appliance
 - joining to another 63
 - non-sharing mode 61
 - partnership for fibre channel support 43
 - sharing mode 60
 - shutting down 54
 - unjoining 64
- applications, viewing 127, 139
- assigning VDisks to a host 111
- async-dedup replication 61
- asynchronous replication 61
- authentication via LDAP 51

B

- bandwidth throttling 40
- bandwidth utilization, monitoring 39
- BDD Nodes, selection in Domain Manager 117

C

- Call Home feature 97
- cannot define the ports and virtual disks of vCenter host 138
- certificates
 - exchanging 50
 - managing 48
 - viewing 38
- community string for forwarding traps 92
- Configuration tools 69
- Connector Manager, using 68
- Connector, see Actifio Connector
- contact information, Actifio Support ii

- copyright ii
- creating additional storage pools 27

D

- dedup async 33
- dedup settings
 - about 72
- Dedup storage pools 22
- deduplication, see dedup
- deleting user created storage pools 30
- Diagnostics
 - charts 145
 - information, displaying 145
 - SSD Device Status 146
 - tools 145
- disaster recovery 59
- Domain Manager
 - Service Menu commands 3

E

- event notifications, see notifications
- expirations and schedules 55
- expired objects, elimination of 33

F

- fastest storage, assigning to the primary storage pool 22
- Fibre Channel
 - as a bottleneck to replication memory 11
 - support 43
 - switches, forwarding alerts from 89
- Full GC 33

G

- garbage collection (GC) 33, 35
- generic host, adding 130

H

- HMC host, see IBM HMC host
- hosts
 - about 123, 129
 - adding HP-UX 130
 - adding IBM HMC 136
 - adding OpenVMS 130

- adding TGPS 130
- applications, viewing 127, 139
- configuring BDD ports 120
- configuring ports 138
- editing 140
- viewing 140
- HP-UX, adding host 130

I

- IBM HMC host, adding 136
- image mode VDisk 108
- in-band hosts 103
- in-band storage 24
- incremental backups 16
- Incremental GC 33
- IQN, for iSCSI port on a host 133, 135, 138
- iSCSI ports 103

J

- joining
 - sharing mode 65

L

- LDAP
 - group mapping 52
 - groups 52
 - server, connecting 51
- legal matter ii
- licensing
 - license key email 79
 - license key, locating 81
 - ordering a license 79
 - system UUID 79
 - uploading license keys 80
- limit of VDIsks per Actifio appliance 23
- LiveClones
 - unmounting 144
 - VDisk consumption 23
- logs
 - about 77
 - sending to Actifio Support 99
 - truncation 16
- LPARs, discovering 136

M

- mapping LDAP groups to roles 52
- master and slave relationship 60
- MDisk 29
- MIB, accessing 93
- Mirror Memory
 - about 13
 - usage 13
- mirror mode VDisk 108

N

- NAS server
 - about 123
 - adding to Actifio appliance 124
 - modifying configuration details 126
 - viewing datasets on 127
 - viewing organization membership 128
- notifications
 - about 76
 - email notifications of events 94
 - event context information displayed in the Actifio Desktop 86
 - polling from Actifio Optimized Storage 88
 - sending logs to Actifio Support 99
 - sending statistics to Actifio support team 97
 - UDP trap protocol 92

O

- OpenVMS host, adding 130
- Oracle RMAN 19
- organizations 106
- out-of-band storage 24

P

- partnership between two appliances 43, 65, 66
- Performance pools 22
- performance, reduced 6
- Predictive Statistics block 33
- Primary storage pools 22

R

- Remote Problem Resolution, enabling 56
- Replication Memory
 - usage 11
- Resources
 - Summary 6
 - top 10 SLA policy templates 12
- resources
 - about 70
- resources consumed by applications and VMs 12

S

- Safe Mode, setting for storage pools 25
- SecureConnect, enabling 56
- service menu commands 3
- Shadow Copy, see VSS
- shared mode, joined appliances 65
- sharing users, roles, policy templates, and organizations between appliances 60
- shutdown an appliance, correct procedure 54
- snapshot memory
 - about 9
 - usage 9
- snapshot pools

- consumption 10
- deleting 30
- reports relating to 10
- Snapshot storage pools 22
- SNMP
 - community string, setting 92
 - configuration on Fibre Channel switches 89
 - notifications 88
 - trap receiver 92
- SNMP traps 85, 89
- solid-state drive (SSD) memory 146
- SSD device status 146
- storage management 21
- storage pools, about 71
- storage pools, creating more 27
- striped VDisks 108
- sweep phase 36
- synchronous replication to a remote appliance 61
- system UUID
 - copying 83
 - licensing 79
 - locating 80

T

- TGPS host, adding 130
- threshold value, for warnings 7
- throttling bandwidth usage 40
- top 10 SLA policy templates
 - managing 12
 - over 12
 - viewing 12
- Top Ten VDisks list 7
- trademarks ii
- trap receiver, sending traps to 92
- traps and informs, see notifications

U

- unjoining joined appliances 64
- unmounting
 - image 142
 - unmounting and deleting a mounted image 143
- unused storage space, reclaiming 33
- user authentication via LDAP 51

V

- vCenter host, adding 134
- VDisk
 - consumption, reducing 8
 - created from multiple MDisks 108
 - defined 7
 - deleting 115
 - expanding 113
 - image mode, creating 109

- limit 23
- management 107
- mapping to a host 111
- mirror mode 108
- mirror mode, creating 110
- renaming 114
- reports relating to consumption 8
- unmapping from a host 112
- usage 7
- VIOs, discovering 136
- virtual disks, see VDisk
- VMDK and VDisk consumption 23
- volume, see VDisk
- VSS
 - enabled by in-band Actifio Connector use 17, 18

W

- Warning Threshold setting
 - VDisks 7
- warning thresholds 6
- warranty ii
- WWPN ports 103
- WWPN, for Fibre Channel port on a BDD host 120
- WWPN, for Fibre Channel port on a host 138

