
Network Administrator's Guide to Actifio VDP

Copyright, Trademarks, and other Legal Matter

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

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

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

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

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

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

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

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

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

Contents

Preface	vii
Actifio Appliances	vii
The ActifioNOW Customer Portal	vii
Actifio Support Centers	vii
Chapter 1 – Modifying Your Network Configuration Settings	1
DNS and NTP	2
IPs and Interfaces	3
NIC Usage for Each Actifio Appliance Type	4
Outbound Policies	6
Outbound Policies and Custom Configurations	7
Network Troubleshooting	8
Host Resolution	9
Configure Self Service Network for Actifio Sky Appliances in the Cloud	10
Chapter 2 – Reference Architectures for Actifio Appliances	11
Actifio Sky Appliances	11
Actifio CDX Appliances	11
Actifio CDS Appliance: Generation-3	12
Actifio CDS Appliance: Generation-4	13
Actifio CDS Appliance: Generation-5	14
Chapter 3 – Firewall Rules	15
Internet Protocol (IP) Network Security in an Actifio Environment	15
Chapter 4 – About the Actifio Connector	23
What Does the Connector Do?	23
The Connector and the Network Environment	24
Host-Side Scripting	24
Obtaining the Right Actifio Connector for Your Host	25
Maintaining Connectors on Hosts	26
Chapter 5 – Supporting VMware with Actifio VDP	27
Actifio Sky Appliance Networking Requirements	27

Ensuring iSCSI Connectivity from ESX to Storage.....	28
Ensuring iSCSI Connectivity with an ESX Server.....	28
Adding the iSCSI Actifio Definition to the ESX server	29
Configuring AGM to See the ESX Host.....	29
Ensuring NFS Connectivity from ESX to Storage.....	30
Setting NFS Data Transport Mode to a Host in VMware.....	31
Specifying the NIC for NFS Mounts.....	32
Renaming a vCenter	32
Chapter 6 – Supporting Microsoft Windows Server with Actifio VDP	33
Ensuring iSCSI Connectivity on a Windows Physical Host.....	34
Ensuring Fibre Channel Connectivity on a Windows Physical Host	35
Installing the Actifio Connector on Microsoft Windows Hosts.....	36
Restricting Windows Connector Communication to Specific Appliances.....	37
To Unrestrict a Restricted Windows Connector	38
Notes on Discovering Specific Microsoft Application Types.....	39
Chapter 7 – Supporting Microsoft Hyper-V with Actifio VDP	41
Chapter 8 – Supporting Linux with Actifio VDP	43
Ensuring iSCSI Connectivity on a Linux Host.....	43
Ensuring Fibre Channel Connectivity to a Linux Host	45
Ensuring NFS Connectivity on a Linux Host Connected to a Sky Appliance.....	49
Installing the Actifio Connector on a Linux Host.....	50
Upgrading or Uninstalling the Actifio Connector from a Host Using AGM.....	51
Chapter 9 – Supporting IBM AIX with Actifio VDP	53
Supported IBM AIX Configurations.....	53
Ensuring NFS Connectivity on an IBM AIX Host Connected to a Sky Appliance	55
Installing the Actifio Connector on IBM AIX Hosts.....	56
Chapter 10 – Supporting IBM HMC with Actifio VDP	57
Ensuring vSCSI Connectivity on an IBM HMC Host	58
Installing, Upgrading, or Uninstalling the Actifio Connector on an IBM HMC Host.....	58
Chapter 11 – Supporting Oracle Solaris with Actifio VDP	59
Installing the Actifio Connector on Solaris Hosts.....	60
Ensuring iSCSI Connectivity on an Oracle Sun Solaris Host.....	61
Ensuring Connectivity on a Solaris Host over Fibre Channel SAN.....	61
Ensuring NFS Connectivity on a Solaris Host.....	62
Chapter 12 – Supporting HP-UX with Actifio VDP	63
Ensuring iSCSI Connectivity on an HP-UX Host (Actifio Sky only)	63

Ensuring Fibre Channel Connectivity on an HP-UX Host.....	63
Ensuring NFS Connectivity on an HP-UX Host Connected to a Sky Appliance.....	64
Installing the Actifio Connector on HP-UX Hosts.....	65
Chapter 13 - Adding Your Hosts to an Actifio Appliance	67
Assigning VDisks for the Host Copy Data (In-Band CDS Appliance only).....	68
Configuring Hosts to Auto-Discover their Applications.....	69
Reconciling Inconsistent Host Information across Multiple Appliances	70
Security Software on Hosts.....	70
Deleting Hosts Using the AGM.....	70
Chapter 14 - Adding Unix Hosts to AGM	71
Notes for HMC Hosts.....	72
Chapter 15 - Adding Windows Server and Hyper-V Hosts to AGM	73
Chapter 16 - Configuring External Snapshot Pools on IBM Storewize and Pure Storage FlashArray	75
Prerequisites for an External Snapshot Pool Deployment	76
Adding an External Storage Array.....	77
Adding an External Snapshot Pool.....	78
Chapter 17 - Configuring LDAP and Role-Based Access	79
LDAP Authentication.....	79
Things to Consider when AGM Is Configured for LDAP Authentication.....	79
Configuring LDAP Settings	80
Mapping LDAP Groups to Roles and Organizations.....	81
Viewing LDAP Groups.....	83
Deleting an LDAP Group.....	84
SAML Authentication.....	85
Configuring SAML Settings.....	85
Downloading SP Metadata.....	85
Managing Web Certificates.....	86
Upload PKCS12 File	86
Reset and Generate New Web Certificate.....	87
Chapter 18 - APPID Pre- and Post-Scripts for Scheduled Data Protection Jobs	89
Chapter 19 - Super Scripts for Workflows and On-Demand Data Access Jobs	91
Super Script Phases.....	92
Super Script Arguments.....	92
Super Script Timeouts.....	92
Super Script Environment Variables.....	93
CLI Commands Supported in Super Scripts.....	94

Sample Super Scripts	95
Chapter 20 – Actifio Event Notifications	97
Types of Actifio Events	98
Example of Automating Corrective Action Based Upon an Event Notification	98
Events that Go from Information or Warning to Error	99
Alert Methods Supported by Actifio Appliances	100
Chapter 21 – Monitoring Alerts in the AGM Events Monitor	101
Interpreting Event Details in the Events Monitor	102
Chapter 22 – Configuring the Call Home Feature	103
Sending Alerts from an Actifio Appliance by HTTPS	103
Sending Alerts from an Actifio Appliance by Email	105
Configuring an Actifio Appliance to Communicate with an SMTP Server	105
Setting Up Automatic Emails of Events	106
Interpreting Notifications	108
Chapter 23 – Sending Traps from the Actifio Appliance to a Trap Receiver	109
Configuring an Actifio Appliance to Forward Traps to a Trap Receiver	109
Setting the Community String for Forwarding Traps to a non-Actifio SNMP Trap Receiver	110
Configuring the SNMP Agent to Support SNMP GET Operations	111
Activating the SNMP Agent in an Actifio Appliance	111
Accessing the Actifio MIB	112
Using the Actifio MIB	113
Interpreting Traps	115
Chapter 24 – Collecting Alerts from Storage and Switches (CDS only)	117
Polling Alerts from IBM V3700, IBM DS 3512, and NetApp E2700 Storage Arrays	117
Forwarding Alerts from an IBM System Storage SAN24B-4 Express Switch to an Actifio CDS Appliance	118
Checking Fibre Channel Connectivity from a CDS Appliance to Storage	119
Chapter 25 – Actifio Remote Support	121
Actifio Call Home Remote Event Notification	122
Actifio SecureConnect	123
Index	125

Preface

This guide is for network administrators and system administrators who have to support Actifio systems. It provides information and procedures necessary to ensure connectivity and performance between the Actifio system, your production data, and your data storage.

Actifio Appliances

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

The ActifioNOW Customer Portal

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

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

To log into the ActifioNOW customer portal:

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

Actifio Support Centers

To contact an Actifio support representative, you can:

- Send email to: support@actifio.com
- Call:

From anywhere: +1.315.261.7501

US Toll-Free: +1.855.392.6810

Australia: 0011 800-16165656

Germany: 00 800-16165656

New Zealand: 00 800-16165656

UK: 0 800-0155019

1 Modifying Your Network Configuration Settings

Your Actifio Appliance includes a self-service network configuration feature. This chapter describes how to use it to:

- Modify [DNS and NTP](#) on page 2
- Modify [IPs and Interfaces](#) on page 3
- Create and modify [Outbound Policies](#) on page 6
- Perform [Network Troubleshooting](#) on page 8
- Create and modify [Host Resolution](#) on page 9
- [Configure Self Service Network for Actifio Sky Appliances in the Cloud](#) on page 10

Accessing the Appliance System Management Tools

1. Open a browser to the Resource Center **HTTP://<appliance IP address>/**.
2. Click System & Network Management Login Page.
3. Log in using the appliance credentials. The Network Settings page opens. If your Sky Appliance is in a public cloud platform, such as AWS, GCP, or Azure, see [Configure Self Service Network for Actifio Sky Appliances in the Cloud](#) on page 10.



Accessing the System & Network Management Tools

DNS and NTP

Enter this information:

DNS Domain: Enter the domain of the hosts connected to this appliance.

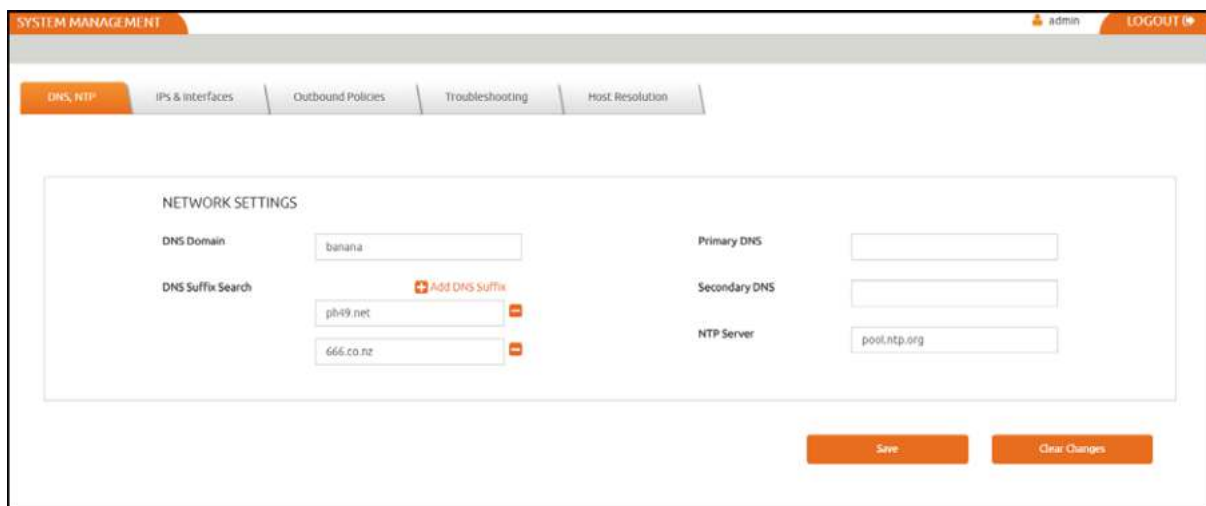
If you have additional hosts on other domains, you can set up a **DNS Suffix Search** to ensure the Actifio Appliance can find them by their short names.

Note: If you set any entries in DNS Suffix Search, then the DNS Domain will NOT be searched. To search both the manual entries AND the DNS domain, include the DNS domain in the DNS Suffix Search.

Primary DNS: Enter the IP address of your primary DNS server.

Secondary DNS: Enter the IP address of your secondary DNS server (optional).

NTP Server: Enter the IP address or hostname of your NTP server.



The screenshot displays the 'SYSTEM MANAGEMENT' interface for 'DNS, NTP' settings. The page has a top navigation bar with 'admin' and 'LOGOUT' options. Below the navigation bar, there are tabs for 'DNS, NTP', 'IPs & Interfaces', 'Outbound Policies', 'Troubleshooting', and 'Host Resolution'. The main content area is titled 'NETWORK SETTINGS' and contains several input fields:

- DNS Domain:** A text box containing 'banana'.
- DNS Suffix Search:** A list of text boxes. The first contains 'pb49.net' and the second contains '666.co.nz'. There is a red '+ Add DNS Suffix' button above the list.
- Primary DNS:** An empty text box.
- Secondary DNS:** An empty text box.
- NTP Server:** A text box containing 'pool.ntp.org'.

At the bottom right of the settings area, there are two orange buttons: 'Save' and 'Clear Changes'.

DNS and NTP

IPs and Interfaces

The IPs & Interfaces tab shows a list of configured IP addresses. You can modify these if necessary, and configure new interfaces added to the Sky Appliance in vCenter. The list is sorted by node first, then by interface, then by type in order (Node, iSCSI). appliance IPs are listed at the end since they are not associated with a single node. DHCP is not supported.

	Type	Node	Interface	IP Address	Network Mask	Gateway	MTU
<input type="checkbox"/>	node	node0	eth0	172.17.134.50	255.255.0.0	172.17.1.1	1500
<input type="checkbox"/>	iscsi	node0	eth0	172.17.134.52	255.255.0.0	172.17.1.1	1500
<input type="checkbox"/>	node	node0	eth1	172.17.134.56	255.255.0.0	172.17.1.1	1500
<input type="checkbox"/>	node	node1	eth0	172.17.134.60	255.255.0.0	172.17.1.1	1500
<input type="checkbox"/>	node	node1	eth1	172.17.134.66	255.255.0.0	172.17.1.1	1500
<input type="checkbox"/>	cluster	cluster	eth0	172.17.134.51	255.255.0.0	172.17.1.1	1500

IPs and Interfaces

Configuring a Default Interface

The **Default Interface** specifies which interface is used to reach arbitrary remote hosts:

- If you specify a Default Interface on a CDS Appliance, then that interface's Node IP address is used.
- If none is specified for a CDS Appliance, then the eth0 cluster IP address is used.
- Sky Appliances have no cluster IP address. Sky Appliances always use a Node IP address.
- If no Default Interface is specified for a Sky Appliance, then the first valid Node IP address is used.

Modifying IP Address Settings

To modify a setting:

1. Check its box and click **Modify**.
2. Make your changes and click **Update**. Changes take effect immediately.

Type	Node	Interface	IP Address	Network Mask	Gateway	MTU
node	node0	eth0	172.17.134.50	255.255.0.0	172.17.1.1	1500
iscsi	node0	eth0	172.17.134.52	255.255.0.0	172.17.1.1	1500
node	node0	eth1	172.17.134.56	255.255.0.0	172.17.1.1	1500
node	node1	eth0	172.17.134.60	255.255.0.0	172.17.1.1	1500
node	node1	eth1	172.17.134.66	255.255.0.0	172.17.1.1	1500
cluster	cluster	eth0	172.17.134.51	255.255.0.0	172.17.1.1	1500

Modifying the MTU for eth0 of Node1

NIC Usage for Each Actifio Appliance Type

Actifio Appliances can be configured for different levels of security and availability depending on network resources. For best results, configure appliances according to the following tables:

[Table 1: Actifio Sky Appliance NIC Usage on page 4](#)

[Table 2: Actifio CDS Appliance Generation-3 NIC Usage on page 4](#)

[Table 3: Actifio CDS Appliance Generation-4 and Generation 5 NIC Usage on page 5](#)

[Table 4: Actifio CDX Appliance NIC Usage on page 5](#)

Table 1: Actifio Sky Appliance NIC Usage

Network	Security Requirement	Use
1G only virtual network	Low	Eth0 (1G) for all traffic
1/10G mixed virtual network	Medium	Eth0 (1G) for management Eth1 (1/10G) for backup/restore/replication
1/10G mixed virtual network	High	Eth0 (1G) for management Eth1 (10G) for backup Eth2 (1/10G) for replication More Eth* for backups only if required.

Each Sky appliance can support up to 100 iSCSI sessions. You can support an additional 100 sessions by adding a NIC card to the Sky appliance.

Table 2: Actifio CDS Appliance Generation-3 NIC Usage

Network	Security Requirement	Use
1G only	Low	Eth0 (1G) for all traffic
1G only	Medium	Eth0 (1G) for management Eth1 (1G) for backup/restore/replication
1/10G mixed	Medium	Eth0 (1G) for management Eth2 (10G) for backup/restore/replication
1/10G mixed	High	Eth0 (1G) for management Eth2 (10G) for backup Eth3 (10G) replication
1/10G mixed	High, with improved availability	Eth0 (1G) for management Eth1 (1G) for replication Eth2/3 (10G & HA) for backup

Table 3: Actifio CDS Appliance Generation-4 and Generation 5 NIC Usage

Network	Security Requirement	Use
1G only	Low	Eth0 (1G) for all traffic
1G only	Medium	Eth0 (1G) for management Eth1 (1G) for backup/restore/replication
1G only	Medium	Eth0 (1G) for management Eth1 (1G) for backup/restore Eth2 (1G) for replication
1/10G mixed	Medium	Eth0 (1G) for management Eth2 (10G) for backup/restore/replication
1/10G mixed	High	Eth0 (1G) for management Eth3 (10G) for backup Eth5 (10G) replication
1/10G mixed	High, with improved availability	Eth0 (1G) for management Eth1 (1G) for replication Eth3/4 (10G & HA) for backup
1/10G mixed	High, with improved availability	Eth0 (1G) for management Eth3/4 (10G & HA) for backup Eth5 (10G) for replication
1/10G mixed	High, with improved availability	Eth0 (1G) for management Eth3/4 (10G & HA) for backup Eth5/6 (10G & HA) for replication

Table 4: Actifio CDX Appliance NIC Usage

Ethernet NIC	Number of Ports	Comments
10Gb DA/SFP+ Ethernet	4	Quad port adapter. General use
10Gb DA/SFP+ Ethernet	2	Dual port adapter. Dedicated interconnect
1GbE Ethernet	4	DO NOT USE - Quad port adapter. Reserved.
1GbE Ethernet	1	Dedicated BMC management port

Outbound Policies

Outbound policies define how the Actifio Appliance will reach specific remote networks for outbound connections. Any remote network not addressed by an outbound policy will be governed by the Default Interface configured in [IPs and Interfaces](#) on page 3.

You can also use this page to set a static route. An outbound policy is essentially a group of static routes that are automatically tailored to each of your specific interfaces.



Outbound Policies

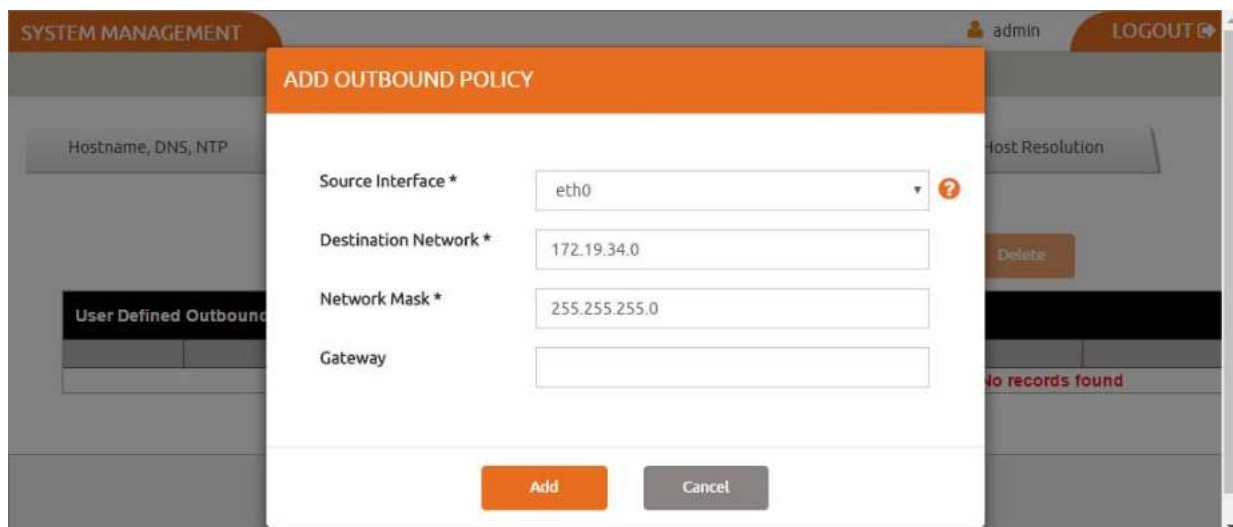
To modify an outbound policy:

1. Check its box and click **Modify**.
2. Make your changes and click **Update**. Changes take effect immediately.

To add a new outbound policy:

1. Click **Add**.
2. Enter your information and click **Add**. Changes take effect immediately.

A Gateway setting is optional. If you do not assign a gateway, then the default gateway for the interface is used. If your traffic must traverse a non-default gateway, then assign that gateway here. This gateway will be installed on every interface where it fits the netmask.



Adding an Outbound Policy

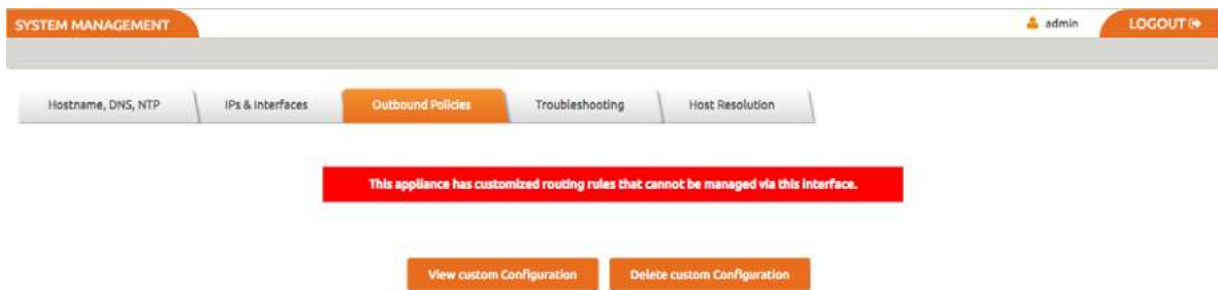
Outbound Policies and Custom Configurations

If this system has some custom networking configured by Actifio Support, then the View and Delete Custom Configuration buttons appear on this page. You can view the text of the custom networking configuration file here.

Note: These buttons are not visible if your appliance has never had a custom configuration. A custom configuration can be created/modified only by Actifio Support. If you cannot make modifications to this page, it means that this system has some custom networking configured by Actifio Support. Contact Actifio Support for guidance.

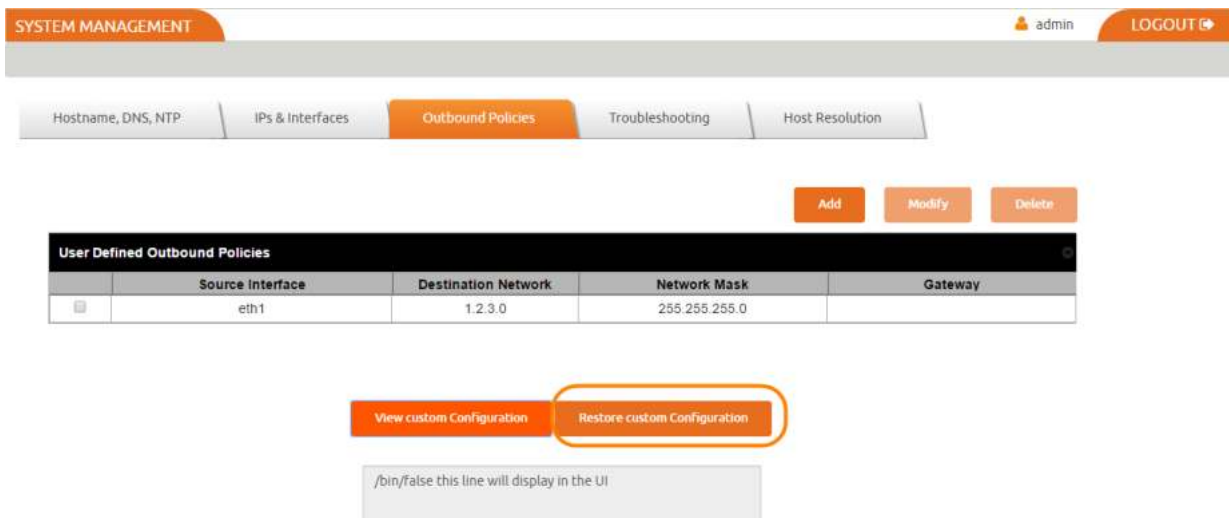
If the appliance has an active custom configuration, then you see a Delete option. This disables the custom part of the configuration, allowing you to proceed with the formerly disabled management functions.

Note: Disabling a custom configuration may make the appliance unreachable.



This Appliance has a Custom Configuration

If you want to reactivate your custom configuration, use the **Restore Custom Configuration** button.



Restoring a Custom Configuration

Network Troubleshooting

Use this page to troubleshoot problematic network connections. Under **Utility**, select the troubleshooting tool to use, enter the necessary parameters, and then click **Run Test**. The results appear in the Test Results box.

Ping: Runs a ping to determine reachability of a target host, returning the output as a plain text stream. This command sends 3 ICMP echo packets.

Enter:

- o **Source IP:** Select the IP address of the appliance to test. This tests the behavior of a reply packet. If you do not enter a value here, then the Outbound Policy rules are used. This tests the behavior of outbound connections.
- o **Destination IP:** A valid IPv4 or IPv6 address.

Example Ping result:

```
PING 1.2.3.4 (1.2.3.4) 56(84) bytes of data.  
--- 1.2.3.4 ping statistics ---  
3 packets transmitted, 0 received, 100% packet loss, time 3001ms
```

IP route get: Queries the routing tables for the selected Destination IP address without sending any packets. Enter:

- o **Source IP:** Select the IP address of the appliance to test. This tests the behavior of a reply packet. If enter no value, then Outbound Policy rules are used to test the behavior of outbound connections.
- o **Destination IP:** The IP address of a target host.

Example IP route get result:

```
test/routeget 1.2.3.4  
1.2.3.4 via 172.17.1.2 dev eth0 src 172.17.134.80  
cache mtu 1500 advmss 1460 hoplimit 64
```

Traceroute: Runs a traceroute to the given IP address by sending a series of UDP probes, returning the output as a plain text stream. This can take 30 or more seconds to run. Use Traceroute to identify intervening networks on the path. Traceroute cannot accept a source IP parameter, so it is not useful for testing the behavior of reply packets. Only outgoing connections can be diagnosed with this tool.

- o **Destination IP:** The IP address of a target host.
- o **UDP Port:** See [Chapter 3, Firewall Rules](#)

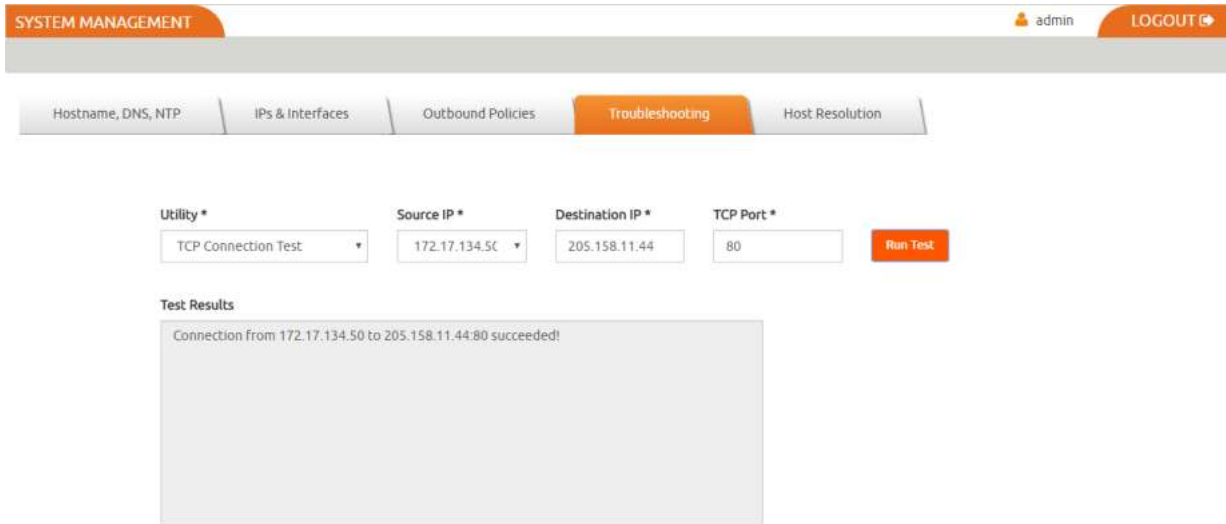
Example Traceroute result:

```
test/traceroute 8.8.8.8  
1: dev134-86.dev.acme.com (172.17.134.86) 0.092ms pmtu 1500  
1: devgw-waln5k02.dev.acme.com (172.17.0.3) 4.287ms  
1: devgw-waln5k02.dev.acme.com (172.17.0.3) 1.287ms  
2: e-1-20-walpalo.core.acme.com (192.168.255.21) 2.805ms  
3: ge-0-0-1-walasr.edge.acme.com (192.43.242.209) 2.769ms  
4: 205.158.44.81.ptr.us.xo.net (205.158.44.81) 9.247ms asymm 14  
5: vb1020.rar3.nyc-ny.us.xo.net (216.156.0.25) 10.080ms asymm 12  
6: 207.88.12.104.ptr.us.xo.net (207.88.12.104) 8.537ms asymm 12  
7: 207.88.13.35.ptr.us.xo.net (207.88.13.35) 8.175ms asymm 11  
8: no reply  
9: no reply  
.br/>.br/>.br/>31: no reply  
Too many hops: pmtu 1500  
Resume: pmtu 1500
```


TCP Connection Test: Attempts a TCP connection to the target IP and port. If successful, the connection is closed immediately without transferring any data. If not successful it returns a failure message.

- o **Source IP:** Select the IP address of the appliance to test. This tests the behavior of a reply packet. If you do not enter a value here, then the Outbound Policy rules are used. This tests the behavior of outbound connections.
- o **Destination IP:** The IP address of a target host.
- o **TCP Port:** See [Chapter 3, Firewall Rules](#).

Example TCP Connection Test result:



Troubleshooting: TCP Connection Test

Host Resolution

A host that has both management and production IP addresses may be configured with only the IP address for the management NIC in DNS. Use this page to add the NIC used for production communications. The information that you enter here becomes the contents of `/etc/hosts`.

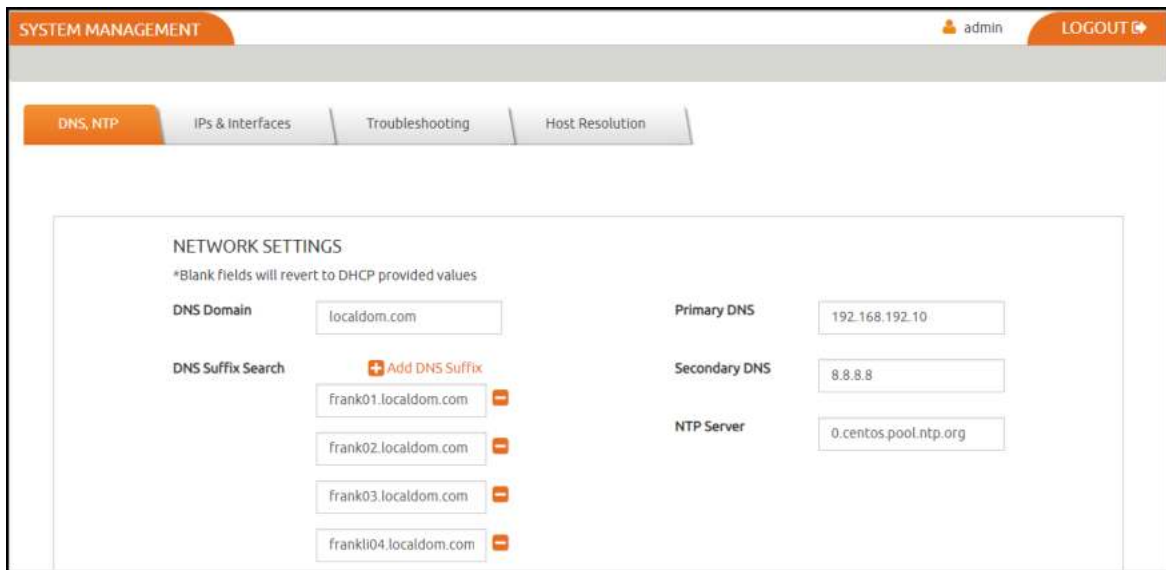
Note you cannot define a single hostname with multiple IP addresses, as the Management Panel will not allow you to do this. Even if it allowed more than one IP address to be added for the same hostname, only the first IP address would ever be used as this how name resolution with the `/etc/hosts` file works (which is the reason the panel blocks attempts to add the same hostname). For the scenario where a single hostname needs to resolve to more than IP, you must rely on an external DNS to do this resolution.



Host Resolution

Configure Self Service Network for Actifio Sky Appliances in the Cloud

For Actifio Appliances on the Cloud, once you login to the System Management you will see the **DNS, NTP** tab.



System Management Tool for Actifio Appliance on Cloud

3. Enter or modify the network settings using information in [DNS and NTP](#) on page 2. Any field you leave empty will revert to DHCP provided values.
4. Click the **IP & Interfaces** tab to view the a list of configured IP addresses. You cannot edit any information, it is view only. For more information, see [IPs and Interfaces](#) on page 3.
5. Click the **Troubleshooting** tab and troubleshoot problematic network connections using information in [Network Troubleshooting](#) on page 8.



Network Troubleshooting

6. Click the **Host Resolution** tab to override DNS resolution for specific hosts. For more information, see [Host Resolution](#) on page 9.

Note: For appliances on the Cloud, you will not see the **Outbound Policies** tab.

2 Reference Architectures for Actifio Appliances

Actifio Appliances can be configured for different levels of security and high availability depending on network resources. For best results, appliances should be configured according to the following tables:

[Table 1: Actifio Sky Appliance Reference Architectures on page 11](#)

[Table 2: Actifio CDX Appliance Reference Architecture on page 11](#)

[Table 3: Actifio CDS Appliance Generation-3 Reference Architectures on page 12](#)

[Table 4: Actifio CDS Appliance Generation-4 Reference Architectures on page 13](#)

[Table 5: Actifio CDS Appliance Generation-5 Reference Architectures on page 14](#)

Actifio Sky Appliances

Table 1: Actifio Sky Appliance Reference Architectures

Sky	Using	Network	Security	High Availability
Sky-1	Eth0 (1G) for all traffic	1G only virtual network	Low	The Sky Appliance uses the hypervisor's High Availability features.
Sky-2	Eth0 (1G) for management Eth1 (1/10G) for backup/restore/replication	1/10G mixed virtual network	Medium	
Sky-4	Eth0 (1G) for management Eth1 (10G) for backup Eth2 (1/10G) for replication More Eth* for backups only if required.	1/10G mixed virtual network	High	

Actifio CDX Appliances

Table 2: Actifio CDX Appliance Reference Architecture

CDX	Using	Network	Security	High Availability
CDX-1	eth0, eth1 for management eth2, eth3 for backup	10G only 10G only	High	Ports bonded for HA

Actifio CDS Appliance: Generation-3

The Actifio CDS Appliance Generation-3 includes the two nodes in the middle and the batteries above and below.



An Actifio CDS Appliance Generation-3

These are the most reliable network architectures for a CDS Appliance Generation-3:

Table 3: Actifio CDS Appliance Generation-3 Reference Architectures

Type	Using	Network	Security	High Availability
3CDS-1	Eth0 (1G) for all traffic	1G only	Low	No
3CDS-2	Eth0 (1G) for management Eth1 (1G) for backup/restore/replication	1G only	Medium	No
3CDS-3	Eth0 (1G) for management Eth2 (10G) for backup/restore/replication	1/10G mixed	Medium	No
3CDS-4	Eth0 (1G) for management Eth2 (10G) for backup Eth3 (10G) replication	1/10G mixed	High	No
3CDS-5	Eth0 (1G) for management Eth1 (1G) for replication Eth2/3 (10G & HA) for backup	1/10G mixed	High	Yes

Actifio CDS Appliance: Generation-4

The Actifio CDS Appliance Generation-4 looks like this:



These are the most reliable network architectures for a CDS Appliance Generation-4:

Table 4: Actifio CDS Appliance Generation-4 Reference Architectures

Type	Using	Network	Security	High Availability
4CDS-1	Eth0 (1G) for all traffic	1G only	Low	No
4CDS-2	Eth0 (1G) for management Eth1 (1G) for backup/restore/replication	1G only	Medium	No
4CDS-3	Eth0 (1G) for management Eth1 (1G) for backup/restore Eth2 (1G) for replication	1G only	Medium	No
4CDS-4	Eth0 (1G) for management Eth2 (10G) for backup/restore/ replication	1/10G mixed	Medium	No
4CDS-5	Eth0 (1G) for management Eth3 (10G) for backup Eth5 (10G) replication	1/10G mixed	High	No
4CDS-6	Eth0 (1G) for management Eth1 (1G) for replication Eth3/4 (10G & HA) for backup	1/10G mixed	High	Yes
4CDS-7	Eth0 (1G) for management Eth3/4 (10G & HA) for backup Eth5 (10G) for replication	1/10G mixed	High	Yes
4CDS-8	Eth0 (1G) for management Eth3/4 (10G & HA) for backup Eth5/6 (10G & HA) for replication	1/10G mixed	High	Yes

Actifio CDS Appliance: Generation-5

The Actifio CDS Appliance Generation-5 looks like this:



These are the most reliable network architectures for a CDS Appliance Generation-5:

Table 5: Actifio CDS Appliance Generation-5 Reference Architectures

Type	Using	Network	Security	High Availability
5CDS-1	Eth0 (1G) for all traffic	1G only	Low	No
5CDS-2	Eth0 (1G) for management Eth1 (1G) for backup/restore/replication	1G only	Medium	No
5CDS-3	Eth0 (1G) for management Eth1 (1G) for backup/restore Eth2 (1G) for replication	1G only	Medium	No
5CDS-4	Eth0 (1G) for management Eth2 (10G) for backup/restore/ replication	1/10G mixed	Medium	No
5CDS-5	Eth0 (1G) for management Eth3 (10G) for backup Eth5 (10G) replication	1/10G mixed	High	No
5CDS-6	Eth0 (1G) for management Eth1 (1G) for replication Eth3/4 (10G & HA) for backup	1/10G mixed	High	Yes
5CDS-7	Eth0 (1G) for management Eth3/4 (10G & HA) for backup Eth5 (10G) for replication	1/10G mixed	High	Yes
5CDS-8	Eth0 (1G) for management Eth3/4 (10G & HA) for backup Eth5/6 (10G & HA) for replication	1/10G mixed	High	Yes

3 Firewall Rules

This section opens with an overview of [Internet Protocol \(IP\) Network Security in an Actifio Environment](#). Then it details the network ports used within a fully functional Actifio VDP environment:

[Actifio Local Management from Administrator Workstation](#) on page 16

[Actifio Appliance Local Services](#) on page 16

[Traffic to and from the Actifio Appliance](#) on page 17

[Backup Traffic from the Actifio Appliance, Replication Traffic Between Appliances](#) on page 18

[Actifio Remote Support](#) on page 18

[Local Storage Management](#) on page 19

[Actifio Report Manager](#) on page 20

[Actifio Global Manager \(AGM\)](#) on page 20

[Resiliency Director](#) on page 21

Internet Protocol (IP) Network Security in an Actifio Environment

All components of Actifio Virtual Data Pipeline have been designed with security in mind and the IP interfaces as traditional attack vectors have been given particular focus in hardening efforts.

Appliance Outbound Connections

The appliance may make outbound connections to some services, but does not listen on or run a service for these ports unless listed in [Actifio Local Management from Administrator Workstation](#) on page 16.

SNMP

For the most part SNMP code on an Actifio Appliance is outgoing only, sending traps to a configured receiver to notify of events and failures. The exception is when integrated with Actifio Optimized Storage or SAN Fabric, a CDS Appliance will listen on UDP 162 for SNMP traps from specified IPs that are whitelisted for Actifio CDS Integrated Storage components.

To see a list of whitelisted IP addresses, use `udsinfo lsmonitoreddevice`. SNMP v1 and v2 are supported.

No Actifio configuration can accept any SNMP walk or write (e.g. GetRequest, SetRequest, GetNextRequest, GetBulkRequest) and this configuration of community names is not required or supported.

Cross Appliance Communication and Replication

All Actifio Appliances utilize strong mutual authentication of the partner appliance with verification of 2048-bit RSA public keys.

Once authenticated, data in flight between appliances is encrypted using 256-bit AES encryption with session keys protected by Diffie-Hellman algorithms affording Perfect Forward Secrecy (PFS) over a TLS v1.2 channel.

Actifio Appliance IP

Actifio Appliance IP Address depends on the type of appliance:

Actifio Sky Appliance: Actifio Appliance IP is the IP address of the Sky Appliance.

Actifio CDX Appliance: Actifio Appliance IP addresses must include Node 0, Node 1, and cluster.

Actifio CDS Appliance: Actifio Appliance IP addresses must include Node 0, Node 1, and cluster.

Actifio Local Management from Administrator Workstation

Destination Port	Protocol	Source	Destination	Description
22 (TCP)	SSH	Admin workstation	Actifio IMM addresses	CLI access for management and backup commands. Hosts may also need to connect to Actifio. Node IMM Ports for installation and service
26 (TCP)	SSH	Admin workstation	Actifio Appliance IP	Service CLI access.
80 (TCP) or 443 (TCP)	HTTP HTTPS	Admin workstation	Actifio IMM addresses	Node IMM Ports for installation and service. Enables local download of Actifio Connector. No appliance control or data access possible on this port.
443 (TCP)	HTTPS	Admin workstation	Actifio Appliance IP	TLS-encrypted communication between Actifio Desktop and the appliance, and some appliance-to-appliance communication. SSL certificates may be replaced.
3900 (TCP)	HTTP	Admin workstation	Actifio IMM	Node IMM for remote access
ICMP		Admin workstation	Target Host	System & Network Mgmt ping

Actifio Appliance Local Services

Destination Port	Protocol	Source	Destination	Description
25 (TCP) or 465 (TCP)	SMTP SMTPS	Actifio Appliance IP	Client email server	Event notification via your SMTP email relay server.
53 (UDP)	DNS	Actifio Appliance IP	Client DNS server	DNS
123 (UDP)	NTP	Actifio Appliance IP	Client NTP server	NTP
162 (UDP)	SNMP	Actifio Appliance IP	Client SNMP server	SNMP trap notification

Actifio Appliance Local Services

Destination Port	Protocol	Source	Destination	Description
389 (TCP) or 636 (TCP)	LDAP LDAPS	Actifio Appliance IP	Client AD server and LDAP	Authentication of user accounts against Microsoft AD/LDAP directory, if configured.

Traffic to and from the Actifio Appliance

Destination Port	Protocol	Source	Destination	Description
26 (TCP)	SSH	Actifio Appliance IP	Actifio Appliance IP	Appliance to appliance cross- node management. Node addresses should also be allowed.
111	tcp/udp	Actifio Appliance IP	Host IP addresses	An RPC service used to map other RPC services
756	tcp/udp			Network status monitor daemon
4045	tcp/udp			Network lock daemon
427 (TCP)	SLP	Actifio Appliance IP	“any”	Service location for WBEM (CDS only)
443 (TCP)	HTTPS	Actifio Appliance IP	vCenter Server IP	Required to communicate with vCenter servers and ESX hosts for snapshot and image management during backup and mounts over an encrypted link. Used for joining Actifio Appliances and sharing certificates.
623	UDP	Actifio Appliance IP	idrac	CDX appliance (only) installation Used for STONITH.
5106 (TCP)	Actifio API	Actifio Appliance IP	Host Servers, including Hyper-V Host Servers	Encrypted control channel between Actifio Appliance and hosts running the Actifio Connector.
5989 (TCP)	CIMOM	VMware SRM server	Actifio Appliance IP	SSL encrypted WBEM (CDS only, used for VMware SRM integration).

Backup Traffic from the Actifio Appliance, Replication Traffic Between Appliances

Destination Port	Protocol	Source	Destination	Description
443 (TCP)	HTTPS	Actifio Appliance IP	Other Actifio Appliance, Amazon S3 endpoint or other OnVault cloud.	Appliance-to-appliance traffic, appliance-to-Actifio OnVault cloud data transfer, StreamSnap traffic
902 (TCP)	VMware	Actifio Appliance IP	ESX Server VMKernel IPs	Encrypted connectivity to VMware ESXi hosts for data movement operations.
2049 4001	tcp/udp tcp/udp	Host IP addresses	Actifio Appliance IP	NFS server process NFS mount daemon
3205 and 3260 (TCP)	iSCSI	Host servers	Actifio iSCSI addresses	iSCSI target
5103 (TCP)	Actifio API	Actifio Appliance IP	Actifio Appliance IP	Encrypted bidirectional appliance-to-appliance data replication traffic. Both sides use strong mutual authentication of the partner appliance.
5107 (TCP)	Actifio API	Actifio Appliance IP	Actifio Appliance IP	Actifio Appliance to appliance bidirectional data transfer for cross-site mirroring and Actifio StreamSnap data replication.

Actifio Remote Support

Destination Port	Protocol	Source	Destination	Description
443 (TCP)	HTTPS	Actifio Appliance IP	callhome.actifio.net	Call Home Alerting
25 (TCP)	SMTP	Actifio Appliance IP	callhome.actifio.net	Call Home Alerting (legacy)
443 (TCP)	OpenVPN/ HTTPS	Actifio Appliance IP	secureconnect2.actifio.com	SecureConnect proxy mode (optional)

Actifio Remote Support

Destination Port	Protocol	Source	Destination	Description
1194 (UDP)	OpenVPN	Sky Appliance: Sky Appliance IP CDX Appliance: node 0 CDS Appliance: CDS node	secureconnect2.actifio.com	SecureConnect encrypted remote support access to Actifio data centers. As the connection is mutually authenticated with strong cryptography, the destination should not be limited by a firewall.

Local Storage Management

Destination Port	Protocol	Source	Destination	Description
------------------	----------	--------	-------------	-------------

Actifio SAN Switch

TCP-22, 23	SSH	Admin workstation	Actifio SAN switch	CLI access for installation and service
TCP-80 TCP-443	HTTP HTTPS	Admin workstation	Actifio SAN switch	Management web GUI for installation and service
UDP-162	SNMP	SAN Switch Management IP	Actifio Appliance IP	Optional delivery of events in the form of SNMP traps to a trap receiver
UDP-123	NTP	SAN Switch Management IP	Client NTP server	NTP

Actifio Storage V3700

TCP-22	SSH	Actifio Appliance IP	Actifio Storage V3700 (Node1/2)	CLI access for installation and service
UDP-162	SNMP	Actifio Storage V3700 (Node1/2)	Actifio Appliance IP	Internal SNMP Notification
UDP-123	NTP	Actifio Storage V3700 (Node1/2)	Client NTP server	NTP
TCP-25	SMTP	Actifio Storage V3700 (Node1/2)	Client Email Server	SMTP Email Notification
TCP-22	SSH	Admin workstation	Actifio Storage V3700 (Node1/2)	CLI access for installation and service

Local Storage Management

Destination Port	Protocol	Source	Destination	Description
Actifio Storage DS3512				
TCP-2463	Management	Admin workstation	Actifio Storage DS3512 (Ctrl A/B)	DS Storage Manager installation and service

Actifio Report Manager

Destination Port	Protocol	Source	Destination	Description
443 (TCP)	HTTPS	Administrator workstation	Report Manager server	Actifio Report Manager (reports & setup/admin)
5103 (TCP)	SSH	Report Manager server	Actifio Appliance IP	Actifio Report Manager (data collection)

Actifio Global Manager (AGM)

Destination Port	Protocol	Source	Destination	Description
5103 (TCP)	SSH	AGM server	Actifio Appliance IP	Outbound connection from AGM to all Actifio Appliances. Once the connection is established, data flow is bidirectional.
443 (TCP)	SSH	AGM server	Actifio Appliance IP	Outbound connection from AGM to Sky Appliances. Once the connection is established, data flow is bidirectional.
443 (TCP)	HTTPS	Workstation or laptop	AGM server	Web browser access to AGM for inbound connection to AGM server.
TCP-389 (TCP) or TCP-636 (TCP)	LDAP LDAPS	AGM server	Client AD server	Microsoft AD/LDAP Active Directory Authentication

Resiliency Director

Destination Port	Protocol	Source	Destination	Description
TCP-443	HTTPS	Resiliency Director Collector	Source appliances	Data collection
		Resiliency Director Collector	Source vCenter	Data collection
		Resiliency Director Collector	RD Server	Replication of configuration data
		Resiliency Director Server	DR appliances	Recovery orchestration
		Resiliency Director Server	DR vCenter	Recovery orchestration
		Resiliency Director Server	RD Collector	Partnership setup
		Resiliency Director Cloud	AGM	Data collection
		Resiliency Director Cloud	DR appliances	Recovery orchestration
		Resiliency Director Cloud	Cloud REST API endpoint	Security verification
TCP-5103	HTTPS	Resiliency Director Collector	Source appliances	Used to establish secure session ID
		Resiliency Director Server	DR appliances	
		Resiliency Director Cloud	DR appliances	
ICMP		Resiliency Director Collector	RD Server	ping used to validate connectivity between collector and server
		Resiliency Director Server	RD Collector	

4 About the Actifio Connector

This chapter describes the Actifio Connector, including [Obtaining the Right Actifio Connector for Your Host](#) on page 25 and [Maintaining Connectors on Hosts](#) on page 26. The Actifio Connector is a small-footprint process that you install on your hosts.

This section includes:

- [What Does the Connector Do?](#) on page 23
- [The Connector and the Network Environment](#) on page 24
- [Host-Side Scripting](#) on page 24
- [Obtaining the Right Actifio Connector for Your Host](#) on page 25
- [Maintaining Connectors on Hosts](#) on page 26

What Does the Connector Do?

Actifio Connectors:

- Discover and capture individual and groups of applications, including applications that cannot be snapped by VMware, Microsoft SQL Server clusters, and Microsoft Exchange Database Availability Groups (DAGs).
- Quiesce applications for application consistency during capture
- Enable change block tracking on Windows hosts and low-splash on non-Windows hosts for incremental-forever capture
- Capture and manage transaction logs, including truncating database transaction logs and rolling database transaction logs forward for point-in-time recovery.
- Rescan 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.
- Prepare application volumes for restore operations
- Enable directory and file browsing, and packages selected files into a ZIP archive when restoring one or more files from a mounted backup.
- For Hyper-V servers, the Actifio Connector enables the capture of entire Hyper-V VMs and incremental backup of Hyper-V VMs stored on Clustered Shared Volume (CSV) disks.
- Enable applications on pRDMs and vRDMs on VMware VMs to avoid virtual server “stun” issues.
- When the Actifio Connector manages data movement, the Actifio Appliance uses a staging disk to create a copy of application data during each Snapshot or Dedup Async job.

Each new version of Actifio VDP is compatible with older versions of the Actifio Connectors up to two minor releases back (VDP software version 9.0 supports VDP 8.0.x and VDP 8.1.x Actifio Connectors), but it is always best to use the most recent versions available.

The Connector and the Network Environment

The Actifio Connector runs as the UDSAgent process, either UDSAgent.exe (Windows) or udsagent (unix). For best results with the Actifio Connector, pay attention to network traffic and possible interference from antivirus software.

Network Traffic

Traffic between the Actifio Appliances and the connector on your hosts is encrypted and communicated via SSL. The Actifio Connector uses port 5106 by default for bidirectional communication from the Actifio Appliance. You may see the legacy port 56789 in use for the same purposes. Make sure your firewall permits bidirectional communication through this port. If you have existing services using both ports, contact Actifio Support for assistance. For much more on network best practices, including iSCSI and Fibre Channel configuration, see the chapter for the OS of the host.

Antivirus Software

Here are some high-level recommendations. Specific anti-virus/security products may call things by different names, not support some features (process exclusion is commonly not supported), and are configured by different means.

Exclude the udsagent process from Anti-Virus Monitoring: This is typically called "Process exclusion" or "Process Threat Level". Excluding anything that UDSAgent.exe (Windows) or udsagent (unix) does from scanning provides the best performance for the backup and the least chance that the antivirus software will block anything.

Exclude scanning of mounted staging disks: Prevent the antivirus software from scanning everything that VDP writes to the staging disk. This is typically slower than reading files on the protected volume already.

- o On Windows, exclude C:\Windows\act
- o On Unix, exclude /act/mnt

Note: You might still have failures if the antivirus software blocks the Connector from opening or reading a file on the protected volume.

Disable antivirus heuristics: This is not required, but may help in some cases. Anti-virus heuristics typically block operations that look suspicious. When the connector is running a backup of a system volume, it looks suspicious since it is reading the contents of the Windows directory and re-creating it on the staging disk.

In some cases, disabling the antivirus software failed to prevent backup failures, but disabling the antivirus software heuristics allowed backups to succeed.

Host-Side Scripting

The Actifio Connector enables scripting on the hosts on which it is installed. Scripts can be invoked for:

- On-demand jobs triggered by the Actifio CLI with the **-scripts** argument.
- Pre and Post phases of a VDP Workflow job.

For detailed instructions on how use VDP scripting, see:

- [Chapter 18, APPID Pre- and Post-Scripts for Scheduled Data Protection Jobs](#)
- [Chapter 19, Super Scripts for Workflows and On-Demand Data Access Jobs](#)

Obtaining the Right Actifio Connector for Your Host

The Actifio Appliance comes with different connector installer files. Each is of a file type appropriate to its intended host type. You can download these with a web browser from the Actifio Resource Center; just open a browser to the IP address of the appliance.

- connector-AIX-<version>.bff
- connector-HPUX-<version>.depot
- connector--Linux_x86-<version>.depot
- connector--Linux-<version>.depot
- connector-Linux_Ubuntu_amd64-latestversion.deb
- connector-Solaris_SPARC-<version>.depot
- connector-Solaris_x86-<version>.depot
- connector-win32-<version>.depot

Each section of this book details which connector installer you need for each type of host.

actifio Resource Center for VDP 10.0

SYSTEM & NETWORK MANAGEMENT

- System & Network Management Login Page

DOCUMENTATION

- Release Notes and Product Documentation via the Actifio NOW Website (Login Required)
- Download zipped Actifio Documentation Library

CONNECTORS

- Windows Connector
- AIX Connector
- HP-UX Connector
- Ubuntu Connector
- Solaris Connector [SPARC](#) | [x86](#)
- Linux Connector [32 Bit](#) | [64 Bit](#) | [PPC](#)

[Deployment guide](#)

[View all connectors](#)

SNMP RESOURCES

- MIB

LICENSES

- Additional Software Licenses

All of the Actifio Connectors are Available from the Actifio Resource Center

Maintaining Connectors on Hosts

From the AGM **Manage > Appliance** page, right-click the appliance that supports the host and select **Configure Appliance**. Then use the Connector Management tool to uninstall or upgrade the Actifio Connector on your hosts when new versions are available. For details, refer to the AGM online help.

The screenshot shows the 'Appliance Configuration' interface. On the left sidebar, the 'Connector Management' option is highlighted with an orange circle. The main content area is divided into two sections: 'Latest Available Connectors' and 'Discovered Hosts'.

Latest Available Connectors:

- 10.0.0.2933 (Green status)
- 10.0.0.2933 (Yellow status)
- 10.0.0.2933 (Green status)
- 10.0.0.2933 (Green status)
- 10.0.0.2933 (Blue status)
- 10.0.0.2933 (Blue status)
- 10.0.0.2933 (Green status)
- 10.0.0.2933 (Green status)

Discovered Hosts Table:

Host Name	Properties	Installed version	Current Status	Last Success	
BB1_box1		10.0.0.2653	Upgrade Success	Feb 01 14:28	Green
BB1_box2		10.0.0.2653	Upgrade Success	Feb 01 14:25	Green
activedgnode1		10.0.0.2623	Upgrade Success	Jan 29 12:07	Green
activedgnode2		10.0.0.2623	Upgrade Success	Jan 29 12:07	Green
asndev01		8.1.2.545 HotFix 1861		Feb 16 16:43	Green
asndev02		10.0.0.2623	Upgrade Success	Jan 29 12:11	Green
atlas		9.0.3.6	Upgrade Success	Dec 05 14:50	Green
epimetheus		10.0.0.2653	Upgrade Success	Feb 04 16:25	Green
trora21		10.0.0.2653	Upgrade Success	Feb 01 13:30	Green
trora23		10.0.0.2653	Upgrade Success	Feb 05 08:34	Green
janus		9.0.3.741	Upgrade Success	Aug 14 07:44	Green
mimas		10.0.0.2653	Upgrade Success	Feb 04 16:25	Green
ndmpar5.sqa.actifio.com		10.0.0.2653	Upgrade Success	Feb 01 13:29	Green
orarachw1		10.0.0.2653	Upgrade Success	Feb 05 22:50	Green

At the bottom of the interface, there are buttons for 'About', 'Retain', 'Upgrade', 'Remove', and 'Uninstall'.

5 Supporting VMware with Actifio VDP

This includes:

- [Actifio Sky Appliance Networking Requirements](#) on page 27
- [Ensuring iSCSI Connectivity from ESX to Storage](#) on page 28
- [Ensuring iSCSI Connectivity with an ESX Server](#) on page 28
- [Ensuring NFS Connectivity from ESX to Storage](#) on page 30
- [Setting NFS Data Transport Mode to a Host in VMware](#) on page 31

Actifio Sky Appliance Networking Requirements

Sky Appliances installed in a vCenter require the following network settings:

- **Static IPs:** You must provide static IPs for all NICs on Sky Appliances.
- **VMXNET3:** Sky Appliance models 30, 50, 120, and 200 must use the VMXNET3 Ethernet adapter. These adapters enable 10GB performance.
- **Adding NICs:** By default, the Sky Appliance comes with a single NIC. To add additional NICs, see [Adding and Configuring Additional Network Interfaces](#) on page 29.

Actifio Sky Network Protocol support

Actifio Sky installed in a VMware environment supports storage presentation (as part of backup/recovery and mount operations) over iSCSI or NFS. The configuration requirements for each of these protocols are:

- **NFS:** As long as you have a network connection from both the Sky Appliance and the vSphere host that the VM resides on, all backups and mounts using NFS will proceed normally. You can use NFS over your network without configuring iSCSI.
- **iSCSI:** The Sky Appliance uses iSCSI to mount data. Ensure that iSCSI is on for the Sky Appliance's vSphere host, and for the servers that host the data the Sky Appliance will capture and manage.

When capturing an entire vSphere VM, iSCSI does not need to be configured on the vSphere host that hosts the VM to be captured. Once the VM has been captured, to present the VM to another vSphere host, including the vSphere host from which it was captured, the vSphere host must have iSCSI configured.

When capturing individual applications on a VM, rather than capturing the entire VM, iSCSI must be configured on the VM's vSphere host.

The Snapshot pool and the Dedup pool each need their own SCSI controller set to VMware Paravirtual.

Note: For best iSCSI network traffic results, see [NIC Usage for Each Actifio Appliance Type](#) on page 4.

Each Sky Appliance and CDX Appliance can support up to 100 iSCSI sessions. A CDS Appliance can support 275 sessions. You can support an additional 100 sessions by adding a NIC card to a Sky Appliance.

Ensuring iSCSI Connectivity from ESX to Storage

To test the iSCSI connection from an ESXi server to a V3700 or V7000 storage array or to an Actifio CDS Appliance:

1. Enable ESXi Shell and connect to ESXi as root.
2. Use netcat (nc) command to confirm connectivity:

```
~ # nc -z 123.45.67.89 3260  
Connection to 123.45.67.89 3260 port [tcp/*] succeeded!  
This example confirms that the device is listening on that port. If a port is unreachable then you return to the prompt with no output.
```

Note: ESXi does not have telnet, so issuing a ping does not prove that connectivity for iSCSI is available.

Ensuring SAN transport of data to an external storage pool

A newly created vCenter will default to Transport Type NFS. This is incompatible with ESP, and should be changed to SAN. This setting is visible in AGM and from the Command Line, but is not displayed in the Actifio Desktop.

You can also do this from the CLI:

```
[root@sky812-900-RC2 ~]# udsinfo lshost 207823  
udstask chhost -transport san <id>'\
```

The -transport parameter is detailed in the **Actifio CLI Reference**.

Ensuring iSCSI Connectivity with an ESX Server

This has two parts:

1. [Adding the iSCSI Actifio Definition to the ESX server on page 29](#)
2. [Configuring AGM to See the ESX Host on page 29](#)

Before You Begin

In order to ensure connectivity to ESX servers reached via iSCSI:

- Check that the NICs are as described in [NIC Usage for Each Actifio Appliance Type on page 4](#).
- Check that the network ports are as described in **<Title of this Document>**.
- Check each ESX server to be sure that these are set to the following recommended values:

Setting	Recom. Value	Description
LoginTimeout	60	When iSCSI establishes a session between initiator and target, it must log into the target. It will try to log in for a period of LoginTimeout. If the login attempt exceeds LoginTimeout, then the login fails.
Noopinterval	30	iSCSI uses the noop timeout to passively discover if this path is dead when it is not the active path.
Nooptimeout	30	This is tested on non-active paths every NoopInterval. If no response is received by NoopTimeout, the path is marked dead.

This procedure is for a single Actifio Ethernet iSCSI connection to a single iSCSI Ethernet connection on the ESX server. Actifio Professional Services can help you with any other configuration.

For CDX Appliance cluster (which is high availability), these parameters are different to ensure the iSCSI connection survives a failover event.

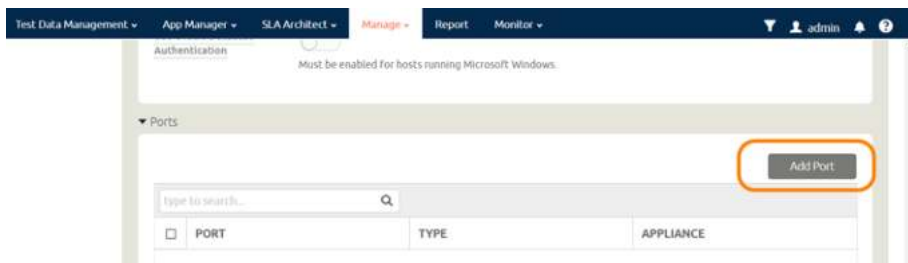
Adding the iSCSI Actifio Definition to the ESX server

1. Highlight the ESX server in vCenter and select the **Configuration** tab.
2. Select the iSCSI Software Adapter and then **Properties**. A pop up window appears to discover the Actifio iSCSI connection.
3. Select Dynamic Discovery tab and click **Add** to add the iSCSI IP of the Actifio Appliance.
4. Enter the IP address of the Actifio iSCSI port and click **OK**. It is added to the target listing.
5. Right click on the iSCSI software adapter and click **Rescan**.

Continue to [Configuring AGM to See the ESX Host](#) on page 29.

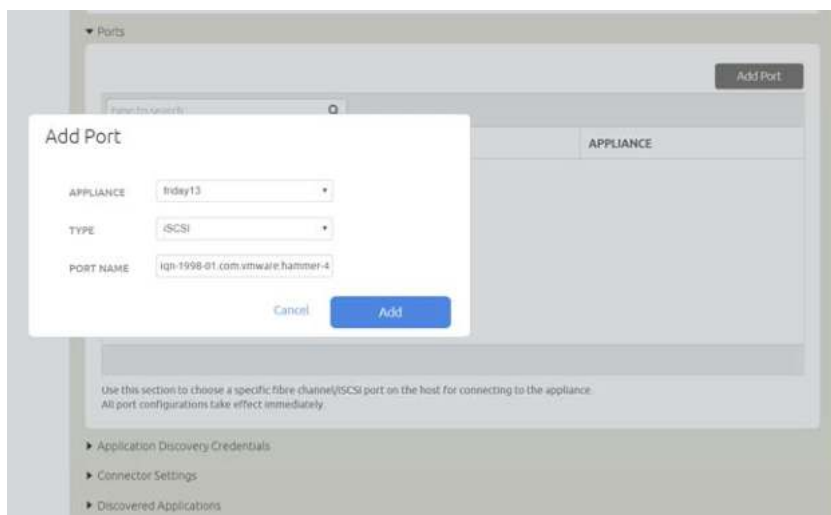
Configuring AGM to See the ESX Host

1. Open AGM to **Manage > Hosts**.
2. Right-click the ESX server and select **Edit**.
3. Scroll down the right side to the Ports section and click **Add Port**.



Configuring AGM to Recognize an ESX Server

4. From the Type menu, select **iSCSI**.
5. At Port Name, enter the iSCSI iqn name, and click **Add**. This will configure the iSCSI relationship on Actifio to the ESX server.



Adding the Port

Ensuring NFS Connectivity from ESX to Storage

Minimum ESX versions

ESXi hosts must be running these minimum levels to support NFS client.

- ESXi Version 5.5 Patch 5 (Build 2718055) OR
- ESXi Version 6.0 U1a (Build 3073146)

Increasing the NFS datastore limit in ESX

The vSphere ESXi/ESX default configuration allows for only eight NFS mounts per ESXi/ESX host. There are three advanced configuration options which control the maximum number of NFS mounts. These settings enable the maximum number of NFS mounts for vSphere ESXi/ESX, listed in [Table 1: ESX Advanced Configuration Options, Limits per ESX Version](#) on page 30.

To edit advanced configuration options, select the ESXi/ESX host in the Inventory Panel, then navigate to Configuration > Software > Advanced Settings to launch the Settings window.

Set the following values:

1. The number of NFS datastores which can be mounted by the vSphere ESXi/ESX host concurrently is limited. The default value is 8.
Under NFS, Select **NFS.MaxVolumes**: Limits the number of NFS datastores which can be mounted by the vSphere ESXi/ESX host concurrently.
2. When increasing the number of NFS datastores, increase the *maximum* amount of heap memory as well.
Under Net, Select **Net.TcpipHeapMax**: The maximum amount of heap memory, measured in megabytes, which can be allocated for managing VMkernel TCP/IP network connectivity.
3. When increasing the number of NFS datastores, increase the *default* amount of heap memory.
Under Net, Select **Net.TcpipHeapSize**: The amount of heap memory, measured in megabytes, which is allocated for managing VMkernel TCP/IP network connectivity.

Table 1: ESX Advanced Configuration Options, Limits per ESX Version

Version	NFS.MaxVolumes	Net.TcpipHeapMax	Net.TcpipHeapSize
ESXi/ESX 3.x	32	120	30
ESXi/ESX 4.x	64	128	32
ESXi 5.0/5.1	256	128	32
ESXi 5.5	256	512	32
ESXi 6.0	256	1536	32

Note: Changing *Net.TcpipHeapSize* and/or *Net.TcpipHeapMax* requires a host reboot.

Setting NFS Data Transport Mode to a Host in VMware

NFS Datastore Transport Mode with VMware is an alternative to iSCSI. NFS datastore enables simpler initial setup and fast onboarding of VMs into Actifio VDP. It is enabled by default for new deployments. You can set the NFS transport mode to a VM host to avoid HBA scans that may cause the VM host to crash.

Before You Begin

To set NFS datastore support on VM:

- The ESX hosts involved in the restore must have the NFS protocol enabled in the Security Profile settings.
- The TCP ports for NFS between the Sky and ESX must be open.

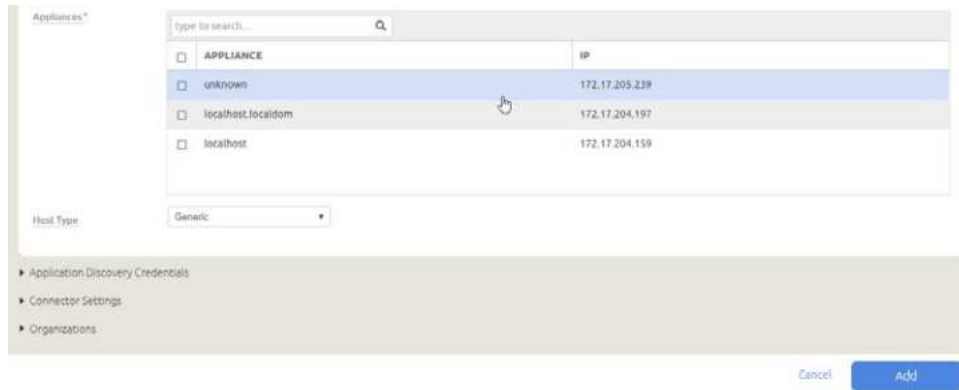
To convert the data transport for mounting staging disks to a Connector-based Windows or Linux host from iSCSI to NFS:

Note: Once the NFS datastore is mounted, you cannot unmount if any images exist.

1. In AGM, click the **Manage** tab and select **Hosts** from the drop-down menu. The Hosts page opens.
2. Select **Add Host**. The upper portion is for network and other identification information. Below that are dynamic sections for host connections and for organizations that the host belongs to.

Appliance	IP
<input type="checkbox"/> APPLIANCE	IP
<input type="checkbox"/> unknown	
<input type="checkbox"/> localhost.localdom	
<input type="checkbox"/> localhost	

3. Enter the host name and a friendly path for the host. The name of a host should start with a letter, and can contain letters, digits (0-9), and an underscore ('_').
4. Enter the IP address of the host, then click +. You can enter an additional IP address in IP Address. Click + to add each additional IP address for the host.
5. Optionally, add a description of this host.
6. In the Appliances section, select the AGM managed appliances that will serve this host. If the list is long, you can use the Search box to find a specific appliance or group of appliances.



7. Select the **Host Type**: vCenter, ESX Server, or Generic. Select Generic for hosts that are not one of the four VM types. This includes Windows and Linux hosts and all physical hosts. Generic hosts require an Actifio Connector of the type that matches their OS.

For vCenter or ESX Server selections, you also get the option to select a Transport Mode. You see the Transport Mode option only during adding a host. This option can be edited after the host has been added:

- o **NFS** (default): Select NFS if you are in an NFS network. Transport will be Network Based in the Application Manager image details and in the System Monitor Transport column.
- o **SAN** (block storage): Select SAN if you are using Fibre Channel or iSCSI networking. Transport will be SAN Based in the Application Manager image details and in the System Monitor Transport column.

Note: As of v9.0, vCenter hosts on appliances default to the transport type NFS. This may be incompatible with External Storage Pools (ESP) under certain circumstances. If you plan to use ESP, change the transport type to SAN. For more information, see *Transport Setting for External Snapshot Pools in the AGM Online help*.

8. If you must override the connection settings from the appliance, then click **Connector Settings**, **vCenter Settings**, or **ESX Settings** as appropriate. For more information, refer to Connector Settings Overrides in the AGM Online help.
9. Click **Organizations**. Select one or more organizations for the host to join. For details on Organizations, see Viewing Organizations in the AGM Online help.
10. Click **Submit** to save the host information.

The Edit Host page opens where additional steps are required if you are adding a host that will use NFS storage or Oracle database authentication. If the new host is defined on multiple appliances and if the information is not identical for them all, then you will see the Host Reconciliation page first. Refer to the AGM Online help for more information.

Specifying the NIC for NFS Mounts

Specify the NIC for an NFS mount at the ESX level:

```
udstask chost -nfsoption server:serverip=1.1.1.1 <hostid>
```

The -nfsoption parameter is detailed in the **Actifio CLI Reference**.

Renaming a vCenter

If you change the name of a vCenter, then remember to rename the vCenter within AGM.

If the UUID of a captured VM changes, then a new full copy will occur on the next backup job.

6 Supporting Microsoft Windows Server with Actifio VDP

Windows Server hosts include Microsoft SQL Server, SharePoint, and Exchange hosts, as well as Active Directory, CIFS, and other file systems.

This chapter includes:

[Ensuring iSCSI Connectivity on a Windows Physical Host on page 34](#)

[Ensuring Fibre Channel Connectivity on a Windows Physical Host on page 35](#)

[Installing the Actifio Connector on Microsoft Windows Hosts on page 36](#)

[Restricting Windows Connector Communication to Specific Appliances on page 37](#)

[Notes on Discovering Specific Microsoft Application Types on page 39](#)

Location of UDSAgent.log on Windows Server Hosts

On a Microsoft Windows Server host, logs are stored in C:\Program Files\Actifio\log.

Location of Scripts on Windows Hosts

You can create scripts to perform pre- and post- actions on applications on your Windows hosts. Create a new folder in which to store all scripts: C:\Program Files\Actifio\scripts. For detailed instructions on how use VDP scripting, see [Chapter 18, APPID Pre- and Post-Scripts for Scheduled Data Protection Jobs](#) and [Chapter 19, Super Scripts for Workflows and On-Demand Data Access Jobs](#).

Note: *The Actifio Connector can be “firewalled” out if the host joins a domain after the Connector has been installed. If this happens, uninstall and then re-install the Actifio Connector.*

Ensuring iSCSI Connectivity on a Windows Physical Host

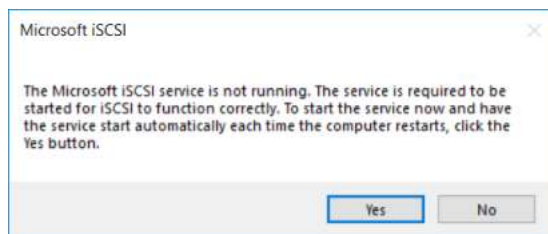
Windows Server hosts include Microsoft SQL Server, SharePoint, and Exchange hosts, as well as Active Directory, CIFS, and other file systems.

When the Actifio Connector manages data movement over iSCSI, VDP uses a staging disk to create a copy of application data during each Snapshot or Dedup Async job.

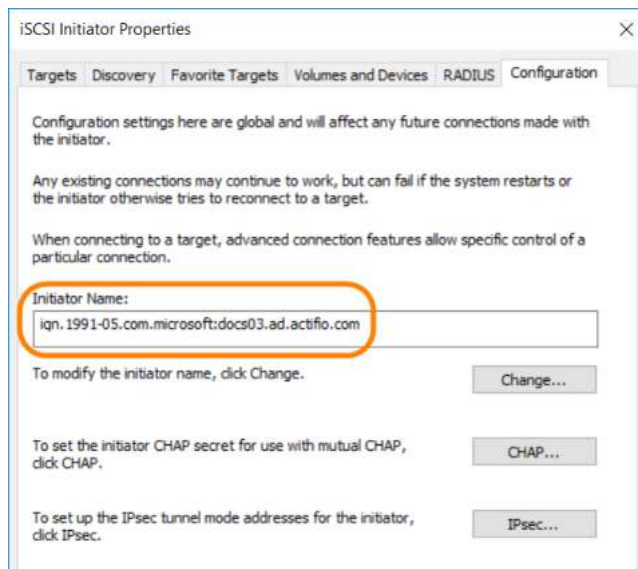
An Actifio-approved iSCSI initiator must be installed on the host. While it is possible to also present the staging disk to a VM using an iSCSI initiator running in the VM, this is normally not necessary.

Learn the iSCSI Initiator Name from a Physical Windows Host via Server Manager

1. On Windows Server 2012, 2012 R2, or 2016, open up Server Manager.
2. Click Tools and select iSCSI Initiator to start the MSiSCSI Initiator Service.
3. The Microsoft iSCSI dialog will open indicating that the service is not running. Click Yes to start the service and to set it to start automatically when the server reboots.



4. After the MSiSCSI Initiator Service has started the Properties dialog will be opened. Click the Configuration tab to retrieve the iSCSI Qualified Name (IQN).
5. Write down or copy the Initiator Name.



Learn the iSCSI Initiator Name from a Physical Windows Host via the CLI

To learn the iSCSI initiator name from a physical Windows host, use the `iscsicli` command:

```
C:\Users\Administrator>iscsicli
Microsoft iSCSI Initiator Version 6.0 Build 6000
[iqn.1991-05.com.microsoft:winsql2016-1.sqa.actifio.com] Enter command or ^C to exit
```

You will need this value when you add the host to the Actifio Appliance.

Ensuring Fibre Channel Connectivity on a Windows Physical Host

When adding a new host that is accessed via Fibre Channel SAN, the new host must be zoned to the Actifio Appliance using an Actifio-approved multipath driver by your storage administrator. The storage administrator will need to know the host WWN; procedures to find WWN on three common Windows servers are below.

Zoning for CDX Appliances

For best results, use single-initiator, single-target zoning for CDX appliances, their hosts, and their storage.

Multipathing

Define a total of four paths (this is both the recommended minimum and maximum) or at most eight paths (absolute maximum) between the CDS Appliance and the Windows host.

Note: Proper multipathing is especially important for maintaining application-aware mounts over a system restart. Multiple different multipathing systems on a single HBA can result in hard-to-identify conflicts.

If the Windows host has two HBA ports (two WWPNs) and each is zoned to one port on Actifio Node 1 and one port on Actifio Node 2, then that host has four paths; this is the recommended configuration. Do not use more than eight paths. When you discover the WWPN, make a note of it. You will use it when you add the host.

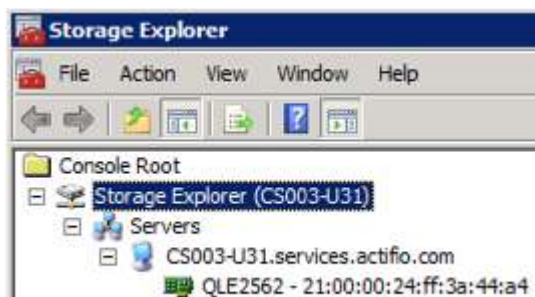
Connecting to a Windows Server 2003 Host over Fibre Channel SAN

To find the WWN of a Windows Server 2003 host, use Microsoft fcinfo (Fibre Channel Information Tool):

<http://www.microsoft.com/en-us/download/details.aspx?id=17530>

Connecting to a Windows Server 2008 Host over Fibre Channel SAN

To find the WWN of a Windows Server 2008 host on a Fibre Channel SAN, use Windows Storage Explorer:



Using Windows Storage Explorer

Connecting to a Windows Server 2012 Host over Fibre Channel SAN

To find the WWN of a Windows Server 2012 host, use PowerShell to perform Get-InitiatorPort.

Installing IBM SDDDSM for In-Band Storage

If you are using in-band storage, then multipathing requires IBM SDDDSM. To install SDDDSM:

1. Get SDDDSM from <http://www-01.ibm.com/support/docview.wss?uid=ssg1S4000350>.
2. From a command prompt with Administrative privileges, run setup.exe.
3. Restart the machine.
4. Verify SDDDSM is installed successfully by running `datapath query version`.

Installing the Actifio Connector on Microsoft Windows Hosts

The Actifio Connector for Microsoft Windows runs as a Windows service under the Local System account. The Actifio Connector writes logs to a log file in its installation directory. On Microsoft Windows systems, the installer comes as: `connector-Win32-<version>.exe`.

If you are managing multiple clustered Windows hosts, then install an Actifio Connector on each host.

The Actifio Connector for Windows is also used for Hyper-V data protection. It should be installed on each Hyper-V server. If an SCVMM Server is in use, then it should also be installed on that server as well. The Actifio Connector only needs to be installed into a VM (VMware, Hyper-V VM, or Hyper-V VM stored on CSV disks) if you want to protect individual applications inside the VM rather than simply protect the entire VM.

VDP Change Tracking Driver Options for Windows Physical Hosts

When installing the Windows Actifio Connector you have the option of installing the VDP Change Tracking Driver. If you intend to protect file systems and applications (SQL Server, Exchange, Sharepoint), install the Actifio Connector with the Change Tracking Driver to enable efficient incremental backups.

Microsoft SQL Server, Microsoft Exchange, and Hyper-V VMs are supported on NTFS and ReFS volumes. Hyper-V VMs are also supported on CSV disks. The Change Tracking Driver does not support CIFS volumes.

Installing the Actifio Connector on a Windows Host

To install the Actifio Connector on a Windows host:

1. Log on to the host as administrator and open a web browser to `https://<Actifio Appliance IP>` to access the Actifio Resource Center.
2. Click the **Windows Connector** icon to download `connector-win32-<version>.exe`.
3. Launch `connector-win32-<version>.exe`.
4. Click **Run** and follow the setup wizard instructions. If you intend to protect SQL or Exchange databases, perform a Full Installation to include the VDP Change Tracking Driver.
5. Click **Finish**. To verify that the Actifio Connector is running, run `services.msc` on the host.

Installing the Actifio Connector from the Windows Command Line

Windows 2012 Core doesn't have a UI, so you need to install it manually on the host command line:

```
> connector-Win32-<version>.exe /SUPPRESSMSGBOXES /NORESTART /VERYSILENT /TYPE=FULL
```

Restarting the Actifio Connector on a Windows Host

To restart the Actifio Connector on a Windows host:

1. Open **services.msc** on the host.
2. Select **Actifio UDS Host Agent** and click **Restart**.

Uninstalling the Actifio Connector from a Windows Host

To uninstall the Actifio Connector from a Windows host:

1. Go to the `c:\program files\Actifio` folder created during the installation.
2. Select and double-click the uninstaller executable: `unins000.exe`.
3. Click **Yes** to confirm and then click **OK** to finish.

To uninstall via script:

```
C:\Program Files\Actifio\unins000.exe" /VERYSILENT /NORESTART /SUPPRESSMSGBOXES
```

Upgrading the Actifio Connector on a Windows Host

Use the Connector Management tool in the Actifio Desktop to auto upgrade the Actifio Connector on your hosts when new versions are available. Refer to [Maintaining Connectors on Hosts](#) on page 26.

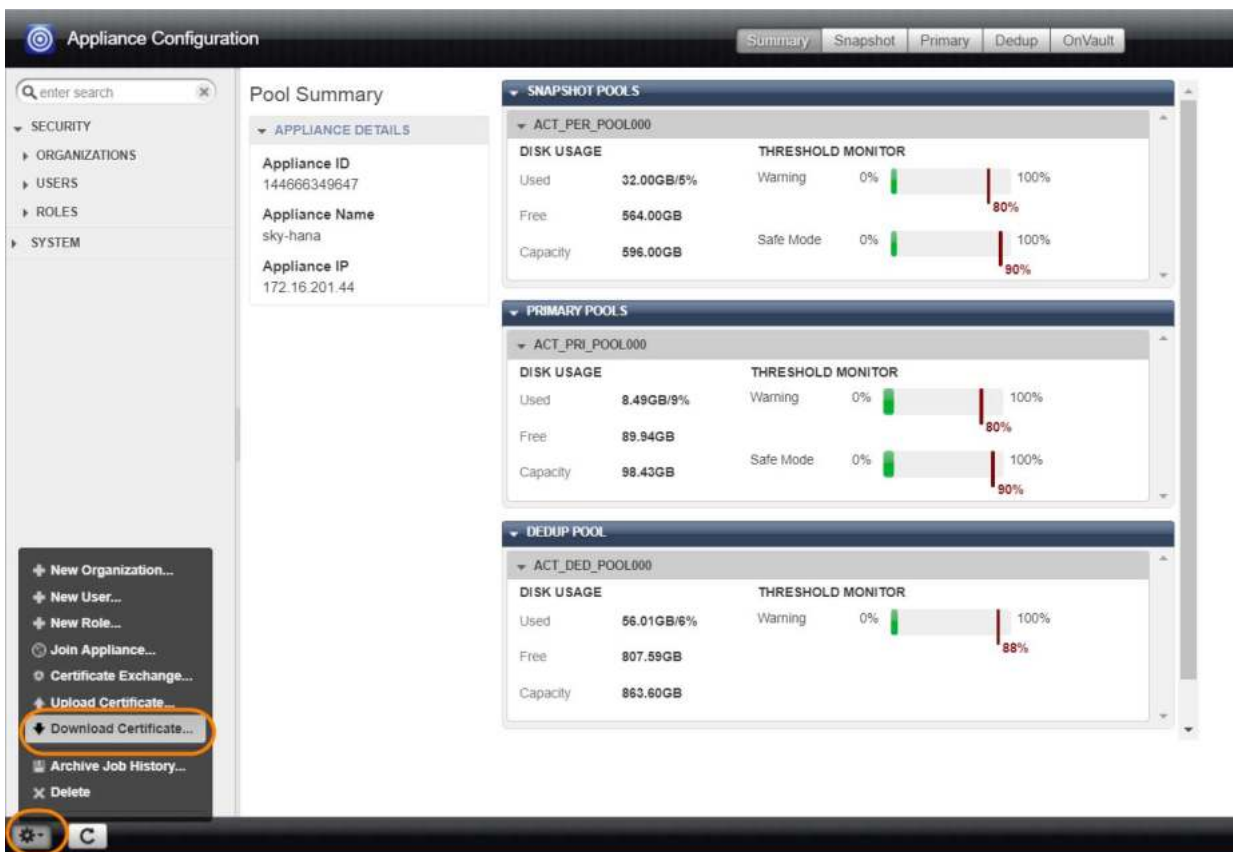
Restricting Windows Connector Communication to Specific Appliances

If you have multiple Actifio Appliances and you want to restrict which appliance can communicate to the connector of a specific host, copy the certificate file from the desired appliance to a specific location on the host. The Actifio Connector on the host will only be able to communicate with the appliance that has the matching certificate. This ensures that an unauthorized appliance cannot be used to create images of application data on the host. In addition to restricting the connector to authorized appliances, this procedure enables certificate verification in the connector, protecting it from man-in-the-middle attacks from a device between the appliance and the connector host.

A single host connector can be restricted to any number of appliances using this method.

For this procedure, assume a host and two appliances: **Host**, **AuthorizedAppliance**, and **UnauthorizedAppliance**.

1. On **AuthorizedAppliance**, open AGM to the Domain Manager, Appliance page.
2. Select the appliance and right click it. Select **Configure Appliance**.
3. The Appliance Configuration window opens. Click the gear icon in the lower left corner, then select **Download Certificate**.



Downloading an Appliance Certificate

4. Save the file with meaningful unique name and with the extension .crt, such as AuthorizedAppliance1.crt. The file name is not important.
5. Copy the certificate file to the host at **C:\Program Files\Actifio\certs\trusted**.
6. Stop and start the connector (UDSAgent) using services.msc.
7. Attempt application discovery from the **AuthorizedAppliance** in AGM. Discovery will succeed.

- Attempt application discovery from the **UnauthorizedAppliance** in AGM. Discovery fails:



To Unrestrict a Restricted Windows Connector

- Delete the certificate file from the host at
C:\Program Files\Actifio\certs\trusted\AuthorizedAppliance.crt
- Stop and start the connector (UDSAgent) using services.msc.
- Repeat the test in [Restricting Windows Connector Communication to Specific Appliances](#) on page 37.

Notes on Discovering Specific Microsoft Application Types

The following information will be of use when discovering applications:

Discovering SQL Databases

- Actifio Appliances support Microsoft SQL Server on Windows Server 2003+.
- Discovery relies on SQL VSS Writer. For the discovery to work correctly, SQL VSS writer must be installed and running on the host.
- Actifio Appliances can protect Microsoft SQL Servers and SQL availability groups. You can snap VMs or applications.
- For a SQL Failover appliance, the discovery needs to be run on either the active node (or node IP) or appliance node (or appliance IP). Otherwise, clustered databases will not be discovered.
- For SQL AlwaysOn Availability Groups:
 - Install the Actifio Connector on each AAG member node. Make sure the Connector installation includes the Connector and the AAM services.
 - To discover AAG groups from the Listener IP, you need firewall rules to open port 5106 (TCP) from AAG member nodes and/or AAG Listener IP to Actifio appliance Cluster IP and Node IP.

Discovering SharePoint Servers

- Only single tier SharePoint deployments can be discovered using Actifio Connector. If you have a multi-tier deployment, discover and protect content databases separately.
- For the discovery to work correctly, SharePoint VSS writer must be installed and running on the host.

Discovering Exchange Mailbox Databases

- All databases in a Microsoft Exchange Database Availability Group (DAG) can be discovered from a single DAG node. Run discovery on a single node to discover all Exchange databases in DAG.
- For the discovery to work correctly, Exchange VSS writer must be installed and running on the host.
- No special permissions are required for backup or restore of Exchange databases, including DAG databases. Local admin has sufficient privileges.

Discovering Mapped File Systems

Before you begin:

1. Log onto the target server as a user.
2. For all existing and new CIFS shares, use Windows Explorer to map the target CIFS share to a local drive letter. Do not specify additional credentials when mapping the drive. Specify **Reconnect at logon**.

When complete, ensure that the application has been added as a host in the AGM. In the Domain page, enter the username and password for the host that you used in Step 1.

Note: In order to find the share, the username and password for the host server must be set to the user that mapped the server. You can only find mapped shares for a user if an Actifio Appliance can impersonate that user.

7 Supporting Microsoft Hyper-V with Actifio VDP

Location of UDSAgent.log on Hyper-V Hosts

On a Hyper-V host, logs are stored in C:\Program Files\Actifio\log.

Location of Scripts on Hyper-V Hosts

You can create scripts to perform pre- and post- actions on applications on the host. Create a folder at C:\Program Files\Actifio\scripts and store scripts there. Details on VDP scripting are in [Chapter 18, APPID Pre- and Post-Scripts for Scheduled Data Protection Jobs](#) and [Chapter 19, Super Scripts for Workflows and On-Demand Data Access Jobs](#).

Installing the Actifio Connector on Hyper-V Hosts

On Hyper-V systems the Actifio Connector runs as a daemon process under the username root. It listens on a TCP port 5106 and 56789 (legacy port) for communication from the Actifio Appliance.

The Actifio Connector writes to a log file in the installation directory (C:\Program Files\Actifio\log).

To install the Actifio Connector on a Hyper-V host:

1. Log on to the host as administrator and open a web browser to `https://<any Actifio Appliance IP>` to access the Actifio Resource Center.
2. Click the **Windows Connector** icon to download `connector-win32-latestversion.exe`. Save the file.
3. Launch `connector-win32-latestversion.exe`.
4. Click **Run** and follow the setup wizard instructions. If you intend to protect SQL or Exchange databases, it is good practice to always perform a Full Installation to include the VDP Change Tracking Driver.
5. Click **Finish**, then verify that the Actifio Connector is running correctly by running `services.msc` on the host.

Restarting the Actifio Connector on a Hyper-V Host

To restart the Actifio Connector on a Windows host:

1. Open **services.msc** on the host.
2. Select **Actifio UDS Host Agent**.
3. Click **Restart**.

Upgrading the Actifio Connector on a Hyper-V Host

Use the Connector Management tool in AGM to upgrade the Actifio Connector on your hosts when new versions are available. Refer to [Maintaining Connectors on Hosts](#) on page 26.

Uninstalling the Actifio Connector from a Windows Host

To uninstall the Actifio Connector from a Windows host:

1. Go to the `c:\program files\Actifio` folder created during the installation.
2. Select and double-click the uninstaller executable: `unins000.exe`.
3. Click **Yes** to confirm and then click **OK** to finish.

8 Supporting Linux with Actifio VDP

This chapter includes:

- Ensuring iSCSI Connectivity on a Linux Host on page 43
- Ensuring Fibre Channel Connectivity to a Linux Host on page 45
- Ensuring NFS Connectivity on a Linux Host Connected to a Sky Appliance on page 49
- Installing the Actifio Connector on a Linux Host on page 50
- Upgrading or Uninstalling the Actifio Connector from a Host Using AGM on page 51

Location of UDSAgent.log on Linux Hosts

On a Linux host, logs are stored in `/var/act/log`.

Location of Scripts on Linux Hosts

You can create scripts to perform pre- and post- actions on applications on the Linux host. To use scripts, create a folder called `/act/scripts` and store all scripts there. For detailed instructions on how use VDP scripting, see [Chapter 18, APPID Pre- and Post-Scripts for Scheduled Data Protection Jobs](#) and [Chapter 19, Super Scripts for Workflows and On-Demand Data Access Jobs](#).

Ensuring iSCSI Connectivity on a Linux Host

When the Actifio Connector manages data movement over iSCSI, VDP uses a staging disk to create a copy of application data during each Snapshot or Dedup Async job.

Learning iSCSI information from a Linux Host

An Actifio-approved iSCSI initiator must be installed on the host. To learn if the initiator is installed, use this command:

```
[root@psa-611 ~]# grep -v ^# /etc/iscsi/initiatorname.iscsi | cut -d "=" -f 2
iqn.1994-05.com.redhat:6d11e98139fb
[root@psa-611 ~]# iscsiadm -m discovery
172.25.128.200:3260 via sendtargets
```

Installing the iSCSI Initiator on a Red Hat RHEL 6 or CentOS Linux Host

To install the iSCSI initiator on a Linux host:

- Make sure you have the `iscsiadm` package installed.
- Run: `# rpm -qa | grep iscsi`
- This should show something similar to: `iscsi-initiator-utils-6.2.0.865-6.el5.x86_64.rpm`
- If you see nothing, then you must install the package: `# yum install iscsi-initiator-utils`

Installing the iSCSI Initiator on a SLES Linux Host

Use YaST to install the iSCSI initiator package.

Make sure you have the `open-iscsi` package installed.

Run: `# rpm -qa | grep iscsi`

This should show something similar to:

```
open-iscsi-x.x.x.x
```

```
yast2-iscsi-client-x.x.x.x
```

If you do not see both of these packages, then you must install `open-iscsi`:

1. `# yast2 sw_single`
2. In the search, enter `iscsi`
3. Select `open-iscsi` and click **Accept**.

Note: If Linux is running on a PowerPC system, then `largesend` must be enabled.

Table 1: Linux iSCSI Multipathing Requirements on Actifio CDX Appliances

CentOS 6.x

```
devices {
    device {
        vendor "ACTIFIO"
        product "LUN0|CDX"
        path_selector "round-robin 0"
        path_grouping_policy failover
        path_checker tur
        rr_min_io 100
        failback immediate
        no_path_retry "5"
        dev_loss_tmo 180
    }
}
```

Ensuring Fibre Channel Connectivity to a Linux Host

If an application is running on a physical server where Fibre Channel is used, then zoning must exist between the appliance and the host, and an Actifio-approved multipath driver must be in use.

Zoning for CDX Appliances

For best results, use single-initiator, single-target zoning for all CDX appliances, their hosts, and their storage.

Host Zoning

When adding a new host that is accessed via Fibre Channel SAN, the new host must be zoned to the Actifio Appliance by your storage administrator. The storage administrator will need to know the host WWN.

To find the WWN of a Linux host on a Fibre Channel SAN:

```
[root@cs003-u34 ~]# cat /sys/class/scsi_host/host*/device/fc_host/host*/node_name
0x200000e08b127a8e
0x200100e08b327a8e
```

Multipathing

Proper multipathing is especially important for maintaining application-aware mounts over a system restart. These are the currently supported multipathing options:

- IBM System Storage Multipath Subsystem Device Driver (SDD)
- Symantec/Veritas Volume Manager 5.1, 6.0, 6.0.1, 6.1
- PVLinks for HP-UX (pre 11.31 v1), HP-UX native
- MPIO for Windows and IBM AIX
- MPxIO for Solaris
- Native VMware multipathing driver for VMware ESX 4.X and later
- Native multipathing drivers for OpenVMS and Linux(DM-MPIO)

If the Linux host has two HBA ports (two WWPNs) and each is zoned to one port on Actifio Node 1 and one port on Actifio Node 2, then that host will have four paths; the recommended configuration. Don't use more than eight paths.

Linux systems employ a multipath.conf file at /etc/multipath.conf. For each Linux distribution and releases within a distribution, refer to the default settings:

- Red Hat Linux: /usr/share/doc/device-mapper-multipath.*
- Novell SuSE Linux: /usr/share/doc/packages/multipath-tools

Include in /etc/multipath.conf the information in the tables below that corresponds to the Linux version on the host that you are configuring. Ensure that the entries added to multipath.conf match the format and syntax for the required Linux distribution. Use the multipath.conf only from your related distribution and release. Do not copy the multipath.conf file from one distribution or release to another.

[Table 2: Linux Multipathing Requirements on Actifio CDS Firmware 7.3.0](#) on page 46

[Table 3: Linux Multipathing Requirements on Actifio CDS Firmware 7.8.1](#) on page 46

[Table 4: Linux Multipathing Requirements for an Actifio CDX Appliance](#) on page 48

Table 2: Linux Multipathing Requirements on Actifio CDS Firmware 7.3.0

Red Hat Linux	SuSE Linux
<p>RHEL Versions 5.x, 6.0 and 6.1</p> <pre> vendor "IBM" product "2145" path_grouping_policy "group_by_prio" path_selector "round-robin 0" prio "alua" path_checker "tur" failback "immediate" no_path_retry 5 rr_weight uniform rr_min_io 1000 dev_loss_tmo 120 </pre>	<p>SUSE Linux Versions 10.x, 11.0, and 11SP1</p> <pre> vendor "IBM" product "2145" path_grouping_policy "group_by_prio" path_selector "round-robin 0" prio "alua" path_checker "tur" failback "immediate" no_path_retry 5 rr_weight uniform rr_min_io 1000 dev_loss_tmo 120 </pre>
<p>RHEL Versions 6.2 and higher and 7.x</p> <pre> vendor "IBM" product "2145" path_grouping_policy "group_by_prio" path_selector "round-robin 0" # path_selector "service-time 0" # Used by RedHat 7.x prio "alua" path_checker "tur" failback "immediate" no_path_retry 5 rr_weight uniform rr_min_io_rq "1" dev_loss_tmo 120 </pre>	<p>SUSE Linux versions 11SP.2 and higher</p> <pre> vendor "IBM" product "2145" path_grouping_policy "group_by_prio" path_selector "round-robin 0" # Used by SLES 11 SP2 # path_selector "service-time 0" # Used by SLES 11 SP3+ prio "alua" path_checker "tur" failback "immediate" no_path_retry 5 rr_weight uniform rr_min_io_rq "1" dev_loss_tmo 120 </pre>

Table 3: Linux Multipathing Requirements on Actifio CDS Firmware 7.8.1

Red Hat Linux	SuSE Linux
<p>RHEL Versions 5.x, 6.0 and 6.1</p> <pre> vendor "IBM" product "2145" path_grouping_policy "group_by_prio" path_selector "round-robin 0" prio_callout "/sbin/mpath_prio_alua /dev/ %n" #Used by Red Hat 5.x prio "alua" path_checker "tur" failback "immediate" no_path_retry 5 rr_weight uniform rr_min_io 1000 dev_loss_tmo 120 </pre>	<p>SUSE Linux Versions 10.x, 11.0, and 11SP1</p> <pre> vendor "IBM" product "2145" path_grouping_policy "group_by_prio" path_selector "round-robin 0" prio "alua" path_checker "tur" failback "immediate" no_path_retry 5 rr_weight uniform rr_min_io 1000 dev_loss_tmo 120 </pre>
<p>RHEL Versions 6.2 and higher</p>	<p>SUSE Linux versions 11SP.2</p>

Table 3: Linux Multipathing Requirements on Actifio CDS Firmware 7.8.1

Red Hat Linux	SuSE Linux
<pre> vendor "IBM" product "2145" path_grouping_policy "group_by_prio" path_selector "round-robin 0" # Used by Red Hat 6.2 prio "alua" path_checker "tur" failback "immediate" no_path_retry 5 rr_weight uniform rr_min_io_rq "1" dev_loss_tmo 120 </pre>	<pre> vendor "IBM" product "2145" path_grouping_policy "group_by_prio" path_selector "round-robin 0" # Used by SLES 11 SP2 prio "alua" path_checker "tur" failback "immediate" no_path_retry 5 rr_weight uniform rr_min_io_rq "1" dev_loss_tmo 120 </pre>
<p>RHEL Versions 7.x</p> <pre> vendor "IBM" product "2145" path_grouping_policy "group_by_prio" path_selector "round-robin 0" prio "alua" path_checker "tur" failback "immediate" no_path_retry 5 rr_weight uniform rr_min_io 1000 dev_loss_tmo 120 </pre>	<p>SUSE Linux Versions 11SP3+</p> <pre> vendor "IBM" product "2145" path_grouping_policy "group_by_prio" path_selector "service-time 0" # Used by SLES 11 SP3+ prio "alua" path_checker "tur" failback "immediate" no_path_retry 5 rr_weight uniform rr_min_io_rq "1" dev_loss_tmo 120 </pre>

Table 4: Linux Multipathing Requirements for an Actifio CDX Appliance

Red Hat Linux

CentOS 6.x

```
devices {
    device {
        vendor "ACTIFIO"
        product "LUN0"
        path_grouping_policy group_by_prio
        detect_prio yes
        path_checker tur
        failback immediate
        no_path_retry "5"
        dev_loss_tmo 180
    }
    device {
        vendor "ACTIFIO"
        product "CDX"
        path_grouping_policy group_by_prio
        features "1 queue_if_no_path"
        detect_prio yes
        hardware_handler "1 alua"
        path_checker tur
        failback immediate
        dev_loss_tmo 180
    }
}
```

CentOS 7.x

```
devices {
    device {
        vendor "ACTIFIO"
        product "LUN0"
        path_grouping_policy group_by_prio
        detect_prio yes
        path_checker tur
        failback immediate
        no_path_retry "5"
        dev_loss_tmo 180
    }
    device {
        vendor "ACTIFIO"
        product "CDX"
        path_grouping_policy group_by_prio
        features "1 queue_if_no_path"
        detect_prio yes
        hardware_handler "1 alua"
        path_checker tur
        failback immediate
        dev_loss_tmo 180
    }
}
```


Ensuring NFS Connectivity on a Linux Host Connected to a Sky Appliance

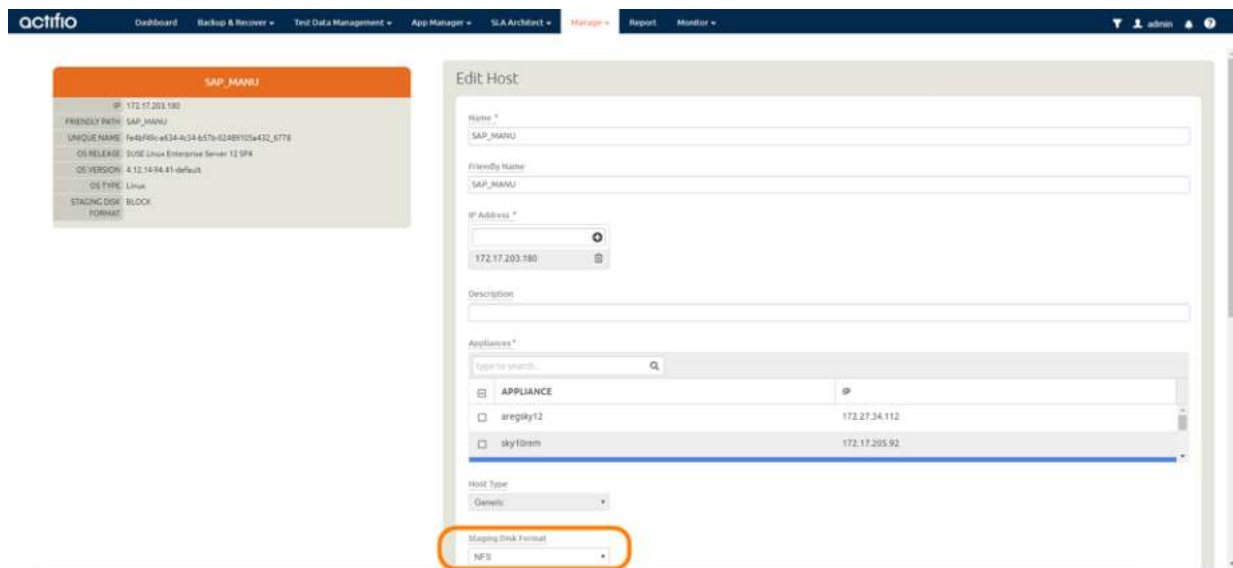
When VDP manages data movement over NFS, during each Snapshot, Dedup Async, or StreamSnap job, VDP uses an NFS share created on the appliance and exports to the Linux host a copy of application data.

Using NFS protocol for Linux Hosts

To use NFS protocol for Linux physical hosts, in order to backup from or mount to a host over NFS, the **nfs-utils** and **nfs-utils-lib** libraries must be installed on the hosts.

```
$ rpm -qa | grep -i nfs
libnfsidmap-0.25-19.el7.x86_64
nfs-utils-1.3.0-0.54.el7.x86_64
```

Use the AGM Manage > Hosts Edit section to set the Staging Disk Format to NFS. Setting this ensures that the staging disk will be presented as an NFS share and the Actifio Connector will consume this share. When mounting an image captured this way, you have the option to mount them as an NFS share.



Setting Staging Disk Format to NFS for a Linux VM

Setting the Staging Disk I/O Path

Linux VMs must also select a staging disk I/O path. You can assign either NFS or SAN (iSCSI) transport for the data from the host to the staging disk. To configure staging disk I/O path:

1. From the AGM Manage > Hosts section, right-click the host to configure and select Edit.
2. In the Edit Host page, scroll down to the Staging Disk I/O Path section.
3. Select one of the following options:

Transport	Actifio volumes are presented	to the	attached to VM as
NFS to Guest	as NFS shares	ESX server	vmdk
NFS Transport	over NFS data store	ESX server	raw device mapping
SAN to Guest	to the iSCSI initiator	Guest VM	ESX is bypassed
SAN Transport	to the iSCSI initiator or to Fibre Channel	Guest VM	ESX is bypassed

Installing the Actifio Connector on a Linux Host

The Actifio Connector for Linux runs as a daemon process under the username **root**. It listens on a TCP port 5106 for communication from the Actifio Appliance. The Actifio Connector writes to a log file in the installation directory (`/var/act/log/UDSAgent.log`) and posts significant events to the `/var/log/` messages repository.

Use the `rpm` utility to install the Actifio Connector. The installer creates Init RC scripts to start and stop the Actifio Connector that runs as a daemon. After the installation completes, use the RC script to start the Actifio Connector for the first time.

To install the Actifio Connector on a Linux host:

1. Log on to the host as root.
2. Open a browser to `https://<Actifio Appliance IP>` to access the Actifio Resource Center.
3. Click the **Linux Connector** icon to download the Actifio Connector.
4. Click **OK** in the information dialog.
5. To check the RPM package before proceeding with installation, run `rpm --checksig <connector_filename>.rpm`
6. To install the Actifio Connector, run:

```
rpm -ivh connector-Linux-<version>.rpm (for the 64-bit installation)
```

```
rpm -ivh connector-Linux_x86-<version>.rpm (for the 32-bit installation)
```

```
dpkg -i connector-linux_ubuntu_amd64-latestversion.deb (for the Ubuntu installation)
```

The Actifio Connector is always installed at `'/opt/act'`.

7. Verify that the Actifio Connector is running:

On non-systemd targets (SUSE Linux before 12.0 and RHEL before 7.0), run `service udsagent status`.

In the output, look for the line `udsagent daemon is running`:

```
root@centos65-mac /home/bomarc01/src/actifio/uds (trunk $%=)
# service udsagent status
udsagent daemon is running
```

On systemd targets (SUSE Linux 12.0+ and for RHEL 7.0+), run `systemctl status udsagent`.

In the output, look for the line `Active: active`:

```
[root@myrhel172 ~]# systemctl status udsagent
? udsagent.service - Actifio UDSAgent Service
Loaded: loaded (/usr/lib/systemd/system/udsagent.service; enabled; vendor preset: disabled)
Active: active (exited) since Wed 2017-04-05 02:10:07 IST; 22h ago
Process: 29460 ExecStop=/act/initscripts/udsagent.init stop (code=exited, status=0/SUCCESS)
Process: 29568 ExecStart=/act/initscripts/udsagent.init start (code=exited, status=0/SUCCESS)
Main PID: 29568 (code=exited, status=0/SUCCESS)
   CGroup: /system.slice/udsagent.service
           +-29587 /opt/act/bin/udsagent start
           +-29588 /opt/act/bin/udsagent start
Apr 05 02:10:07 myrhel172 udsagent.init[29568]: Starting /opt/act/bin/udsag...n
Apr 05 02:10:07 myrhel172 udsagent.init[29568]: Starting /opt/act/bin/udsag...n
```

On Ubuntu targets run `cat /act/etc/key.txt`

Restarting the Actifio Connector on a Linux Host

To restart the Actifio Connector on a Linux host, execute this command on the host:

Non-systemd (SUSE Linux before 12.0 and RHEL before 7.0): `/etc/init.d/udsagent restart`

Systemd (SUSE Linux 12.0+ and for RHEL 7.0+): `systemctl restart udsagent`

Uninstalling the Actifio Connector from a Linux Host using the Command Line

To uninstall the Actifio Connector from a Linux host:

1. Stop the Actifio Connector by running `/etc/init.d/udsagent stop`.
2. Learn the currently installed Linux Connector RPM name:

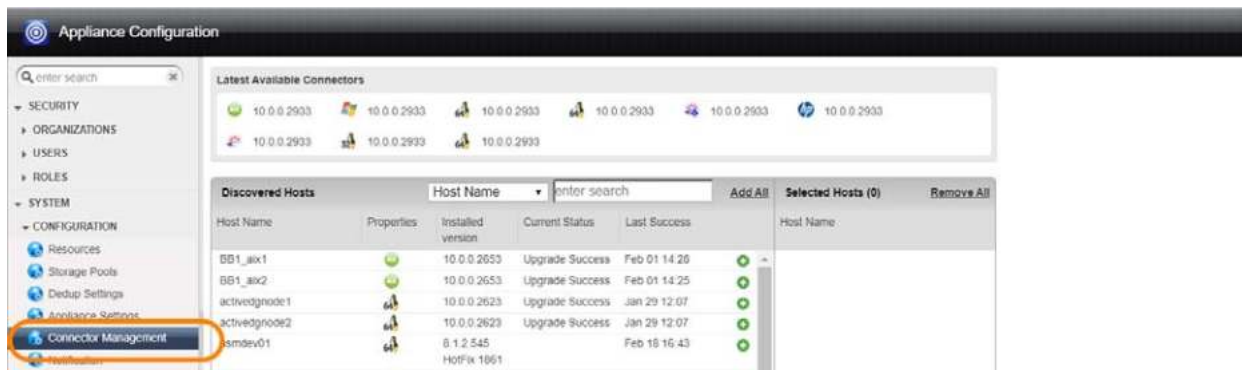
```
[oregon@vq-oregon ~]$ rpm -qa udsagent
```

This returns the package name and version, such as: `udsagent-7.1.0-62339.x86_64`
3. Uninstall the package using `rpm -e udsagent` with the package name you obtained from the query. For example:

```
rpm -e udsagent-7.1.0-62339.x86_64
```

Upgrading or Uninstalling the Actifio Connector from a Host Using AGM

From the AGM Manage > Appliance page, right-click the appliance that supports the host and select Configure Appliance. A new Appliance Configuration screen opens for that appliance. Use the Connector Management tool to uninstall or upgrade the Actifio Connector on your hosts.



Connector Management

9 Supporting IBM AIX with Actifio VDP

This chapter includes:

[Supported IBM AIX Configurations](#) on page 53

[Ensuring NFS Connectivity on an IBM AIX Host Connected to a Sky Appliance](#) on page 55

[Installing the Actifio Connector on IBM AIX Hosts](#) on page 56

Location of UDSAgent.log on AIX Hosts

On an IBM AIX host, logs are stored in `/var/act/log`.

Location of Scripts on AIX Hosts

You can create scripts to perform pre- and post- actions on applications on the AIX host. To use scripts, create a folder called `/act/scripts` and store all scripts there. For detailed instructions on how use VDP scripting, see [Chapter 18, APPID Pre- and Post-Scripts for Scheduled Data Protection Jobs](#) and [Chapter 19, Super Scripts for Workflows and On-Demand Data Access Jobs](#).

Supported IBM AIX Configurations

These common AIX configurations can be protected by an Actifio Appliance.

Physical Machine: All hardware on the server is dedicated to a single LPAR and no virtualization is involved. LUN presentation to this environment is directly to the HBAs in the physical machine (assuming storage is presented via Fibre Channel).

VDP can protect and recover in-band physical machine configurations via Fibre Channel, iSCSI or NFS including the rootvg of the host in a bootable state. This can be accomplished in both a crash-consistent or application-consistent state.

LPAR with Dedicated FC HBAs: A physical server has multiple LPARs, each with dedicated access to one or more physical HBAs while sharing other resources like CPU and memory with other LPARs. This provides better use of your environment than physical machines with some virtualization. LUN presentation within this environment is typically directly through a dedicated HBA (assuming storage is presented via Fibre Channel).

VDP can manage in-band dedicated LPAR configurations via Fibre Channel, iSCSI or NFS in crash-consistent or application-consistent state. VDP can protect rootvg in a bootable state.

LPAR with NPIV mapping: The LPAR has one or more dedicated virtual HBAs assigned to it through a VIO server. The virtual HBAs have unique WWPNs through the mechanism of NPIV. With this methodology, all resources are managed by the HMC, by the VIO server, or by both. Each LPAR has a representation of WWPNs as if the host had physical HBAs.

VDP can protect and recover in-band NPIV environments including rootvg of an LPAR in a bootable state. These hosts can be added as physical hosts, as detailed in [Chapter 9, Supporting IBM AIX with Actifio VDP](#). Storage ports must be configured for them.

LPAR with vSCSI mapping: You can also add LPARs with vSCSI mapping on VIO servers. These are described in [Ensuring vSCSI Connectivity on an IBM HMC Host](#) on page 58.

Ensuring NFS Connectivity on an IBM AIX Host Connected to a Sky Appliance

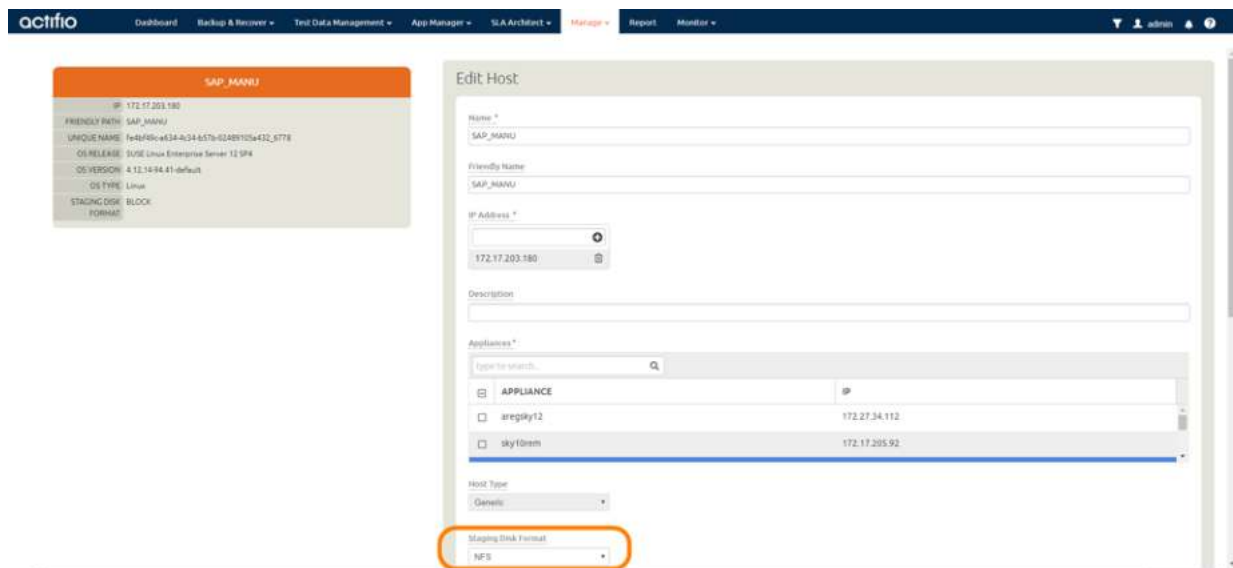
When Actifio VDP manages data movement over NFS, during each Snapshot or Dedup Async or StreamSnap job, VDP uses an NFS share created on the appliance and exports to the Linux host a copy of application data.

Using NFS protocol for AIX Hosts

In order to backup from or mount to a host over NFS, the NFS client must be installed on the hosts.

```
root@nstlpar19: /> ls -l | grep -i nfs
bos.net.nfs.client      7.2.3.15  COMMITTED  Network File System Client
bos.net.nfs.client      7.2.3.15  COMMITTED  Network File System Client
```

Use the AGM Manage > Hosts Edit section to set the Staging Disk Format to NFS. When mounting an image captured this way, you have the option to mount them as an NFS share.



Setting Staging Disk Format to NFS for a Linux VM

Setting the Staging Disk I/O Path

Linux VMs must also select a staging disk I/O path. You can assign either NFS or SAN (iSCSI) transport for the data from the host to the staging disk. To configure staging disk I/O path:

1. From the AGM Manage > Hosts section, right-click the host to configure and select Edit.
2. In the Edit Host page, scroll down to the Staging Disk I/O Path section.
3. Select one of the following options:

Transport	Actifio volumes are presented	to the	attached to VM as
NFS to Guest	as NFS shares	ESX server	vmdk
NFS Transport	over NFS data store	ESX server	raw device mapping
SAN to Guest	to the iSCSI initiator	Guest VM	ESX is bypassed
SAN Transport	to the iSCSI initiator or to Fibre Channel	Guest VM	ESX is bypassed

Installing the Actifio Connector on IBM AIX Hosts

On AIX systems, including those using the NPIV protocol, the Actifio Connector runs as a daemon process under the username root. It listens on TCP port 5106 and 56789 (legacy port) for communication from the Actifio Appliance. The Actifio Connector writes to a log file in the installation directory (`/var/act/log/UDSAgent.log`).

Note: IBM AIX 6.1 pSeries platform introduced a bug that may cause backups to fail. TL7 fixed the bug.

Installing the Actifio Connector on an AIX Host

On AIX systems, the installer is a .bff package: `connector-AIX-<version>.bff`. To install the Actifio Connector:

1. Open a browser to `https://<Actifio Appliance IP>` to access the Actifio Resource Center and click the **AIX Connector** icon to download the AIX install package.
2. Install the Actifio Connector by running `installp -aXgd connector-AIX-<version>.bff all`.

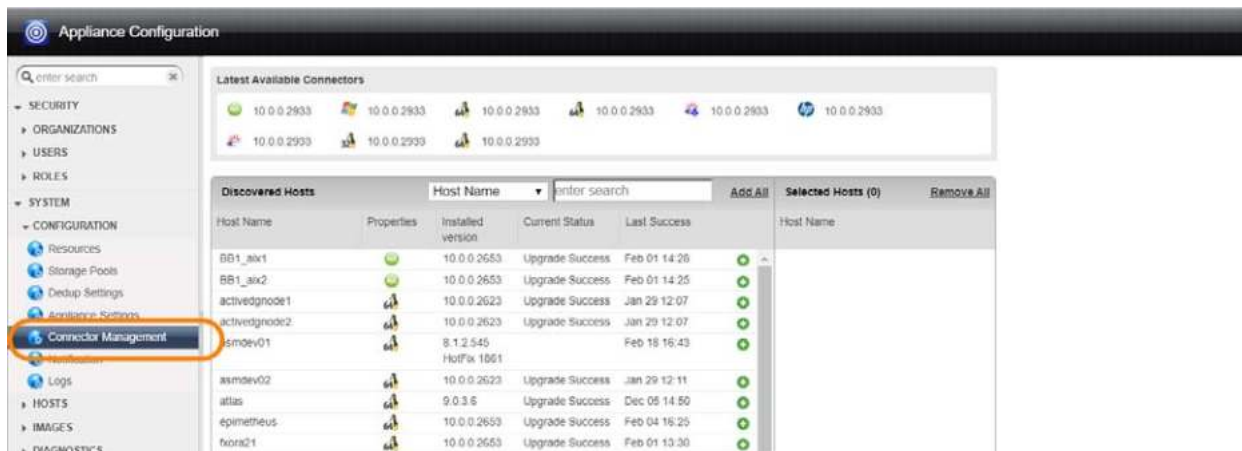
Task	Command option
Verify the successful installation of the Actifio Connector	<code>lslpp -L grep udsagent</code>
Verify the status of the Connector	<code>/etc/udsagent status</code>
Manually stop the Connector service	<code>/etc/udsagent stop</code>
Manually start the Connector service	<code>/etc/udsagent start</code>
View the Connector log	<code>/var/act/log/UDSAgent.log</code>

Manually Uninstalling the Actifio Connector from an AIX Host

To uninstall the Actifio Connector from a AIX host, run: `installp -u udsagent`. You can also use the AGM to uninstall many connectors simultaneously; see [Upgrading or Uninstalling the Actifio Connector on an AIX Host](#) on page 56.

Upgrading or Uninstalling the Actifio Connector on an AIX Host

From the AGM **Manage > Appliance** page, right-click the appliance that supports the host and select **Configure Appliance**. Then use the Connector Management tool to uninstall or upgrade the Actifio Connector on your hosts when new versions are available. For details, refer to the AGM online help.



10 Supporting IBM HMC with Actifio VDP

This chapter includes:

[Ensuring vSCSI Connectivity on an IBM HMC Host on page 58](#)

[Installing, Upgrading, or Uninstalling the Actifio Connector on an IBM HMC Host on page 58](#)

Physical Machines, Dedicated LPARs, and LPARs with NPIV Mapping

Typically these hosts have Fibre Channel connectivity configured for the best performance. iSCSI connectivity is an option for these hosts, but vSCSI is not. These configurations are detailed in [Chapter 9, Supporting IBM AIX with Actifio VDP](#).

Location of UDSAgent.log on IBM HMC Hosts

On an IBM HMC host, logs are stored in `/var/act/log`.

Location of Scripts on IBM HMC Hosts

You can create scripts to perform pre- and post- actions on applications on the HMC host. To use scripts, create a folder called `/act/scripts` and store all scripts there.

Opening Network Ports

Make sure port TCP-5106 is open for Actifio Connector traffic.

Limitations

IBM HMC hosts can be added to a Sky Appliance for LPAR discovery, but Sky Appliances do not support Fibre Channel connectivity, so the LPARs must be presented to their staging disks over an iSCSI connection.

Ensuring vSCSI Connectivity on an IBM HMC Host

Limitations

IBM HMC hosts can be added to an Actifio Sky Appliance for LPAR discovery, but Sky Appliances do not support Fibre Channel connectivity, so the LPARs must be presented to their staging disks over an iSCSI connection.

Ensuring Connectivity

LPAR hosts with vSCSI mapping are virtual hosts that rely on VIO servers for vSCSI connectivity. They do not have direct FC connectivity and FC is not an option for them. If they are discovered as regular physical hosts, then the only option to back them up is using iSCSI, which is inferior to vSCSI. For enabling vSCSI connectivity with this class of LPARs:

- They must be discovered indirectly through HMC discovery, not directly as regular physical hosts.
- The Actifio Appliance should have Fibre Channel connectivity to VIO servers catering storage to these LPARs.

If either of these two conditions are not met, the appliance will use iSCSI connectivity.

Resources such as RAM and CPU are still managed by the HMC but I/O such as network and fibre are managed through the VIO server. This is more scalable than earlier technologies. LUN presentation is done through the HBA cards on the VIO server(s). The VIO server presents the LUNs in a virtual SCSI mapping manner to the LPAR or vhost.

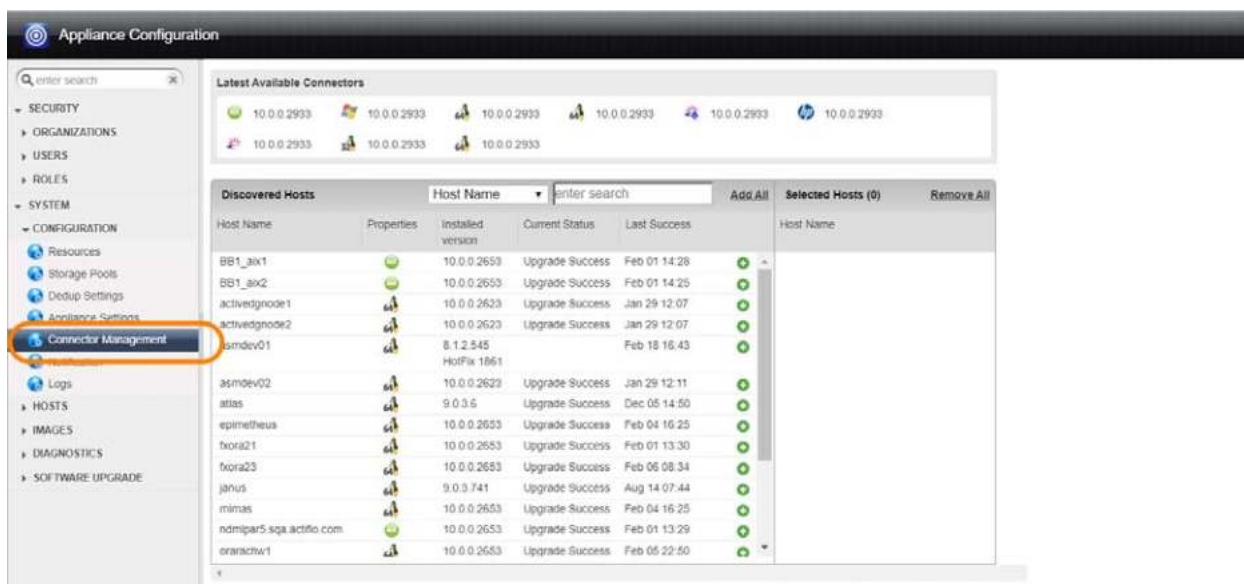
Because the Actifio Connector has direct ties with the HMC of the environment, VDP can protect and recover vSCSI VIO mapped LPARS from an environment including the rootvg in a bootable state.

When the Actifio Connector manages data movement over vSCSI, VDP uses a staging disk to create a copy of application data during each Snapshot or Dedup Async job.

To discover a vSCSI LPAR host, see [Notes for HMC Hosts](#) on page 72.

Installing, Upgrading, or Uninstalling the Actifio Connector on an IBM HMC Host

From the AGM Manage > Appliances page, right-click the appliance that supports the host and select Edit. A new Appliance Configuration screen opens for that appliance. Use the Connector Management tool to uninstall or upgrade the Actifio Connector on your hosts when new versions are available. For details, refer to the AGM online help.



11 Supporting Oracle Solaris with Actifio VDP

This chapter includes:

- Installing the Actifio Connector on Solaris Hosts on page 60
- Ensuring iSCSI Connectivity on an Oracle Sun Solaris Host on page 61
- Ensuring Connectivity on a Solaris Host over Fibre Channel SAN on page 61
- Ensuring NFS Connectivity on a Solaris Host on page 62

Location of UDSAgent.log on Solaris Hosts

On a Solaris host, logs are stored in `/var/act/log`.

Location of Scripts on Solaris Hosts

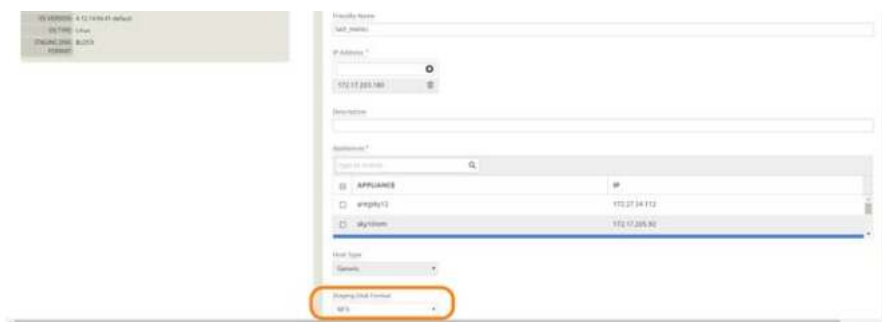
You can create scripts to perform pre- and post- actions on applications on the host. To use scripts, create a folder called `/act/scripts` and store all scripts there. For more on VDP scripting, see [Chapter 18, APPID Pre- and Post-Scripts for Scheduled Data Protection Jobs](#) and [Chapter 19, Super Scripts for Workflows and On-Demand Data Access Jobs](#).

Limitations

The Sky Appliance does support iSCSI on Solaris V71 systems after applying Solaris patch 11.3.21.5.0. The CDS Appliance does not support iSCSI for Solaris SPARC hosts. The CDX Appliance does not support Solaris hosts.

Using NFS protocol for Solaris LDOM and Solaris Zones hosts in AGM

To use NFS protocol for Solaris LDOM and Zones hosts, use the AGM Manager Hosts Edit section to set the Staging Disk Format to NFS. The staging disk will be presented as an NFS share and Actifio Connector will consume it. When mounting an image captured this way, you can mount them as NFS shares.



Setting Staging Disk Format to NFS

Installing the Actifio Connector on Solaris Hosts

On Sun Solaris systems, the installer takes the form of a package file. On Solaris systems, the Actifio Connector runs as a daemon process under the user name **root**. It listens on TCP port 5106 and 56789 (legacy port) for communication from the Actifio Appliance. The Actifio Connector writes to a log file in the installation directory (`/var/act/log/UDSAgent.log`).

To install the Actifio Connector on a Solaris host:

1. Open a browser to `https://<Actifio Appliance IP>` to access the Actifio Resource Center.
2. Click the appropriate **Solaris Connector** install package icon to download the Actifio Connector.
3. To install the Actifio Connector, run:
 - o SPARC: `pkgadd -d /tmp/connector-Solaris_SPARC-<version>.pkg all`
 - o Solaris x86: `pkgadd -d /tmp/connector-Solaris_x86-<version>.pkg all`

Tasks and Available Command Options

Task	Command option
Verify the successful installation of the Actifio Connector	<code>pkginfo -l udsagent</code>
Verify the status of Connector	<code>/etc/udsagent status</code>
Manually stop the Connector service	<code>/etc/udsagent stop</code>
Manually start the Connector service	<code>/etc/udsagent start</code>
See the Connector logs	<code>/var/act/log/UDSAgent.log</code>

Manually Uninstalling the Actifio Connector from a Solaris Host

To uninstall the Actifio Connector from a Solaris host, run: `pkgrm udsagent`.

Note: You can also uninstall the Actifio Connector on many hosts simultaneously; see [Maintaining Connectors on Hosts on page 26](#)

Using the Connector Management Tool to Upgrade or Uninstall the Actifio Connector on a Solaris Host

Use the Connector Management tool in the AGM Domain Manager service to upgrade or uninstall the Actifio Connector on your hosts when new versions are available. Refer to [Maintaining Connectors on Hosts on page 26](#).

Ensuring iSCSI Connectivity on an Oracle Sun Solaris Host

The Actifio Appliance must be able to communicate with the Actifio Connector running on the new host over a Fibre Channel or iSCSI network.

Note: *The Actifio CDS Appliance does not support iSCSI for Solaris SPARC hosts but the Actifio Sky Appliance does support it.*

When the Actifio Connector manages data movement over iSCSI, VDP uses a staging disk to create a copy of application data during each Snapshot or Dedup Async job.

Connecting to Solaris x86 Hosts over iSCSI

To learn the iSCSI initiator Name from a Solaris x86 Host, use this command:

```
root@solaris5531:~# iscsiadm list initiator-node | grep -i "Initiator node name" | cut -d ":" -f 2,3
iqn.2015-02.com.actifio:solaris5531
```

Make sure you have the iSCSI package installed:

```
# pkginfo |grep SUNWiscsi
system      SUNWiscsir      Sun iSCSI Device Driver (root)
system      SUNWiscsiu      Sun iSCSI Management Utilities (usr)
```

Installing the pkg File

To install the iSCSI Initiator package on a Solaris Host:

```
# pkgadd -d <path_to_pkg_file> all
```

Solaris iSCSI Initiator Limitations

Here are the current limitations or restrictions of using the Solaris iSCSI initiator software:

- Support for iSCSI devices that use SLP is not currently available.
- Boot support for iSCSI devices is not currently available.
- iSCSI targets cannot be configured as dump devices.
- iSCSI supports multiple connections per session, but the current Solaris implementation only supports a single connection per session. For more information, see RFC 3720.
- Transferring large amounts of data over your existing network can impact performance.

Ensuring Connectivity on a Solaris Host over Fibre Channel SAN

Define a total of four paths (this is both the recommended minimum and maximum) or at most eight paths (absolute maximum) between the CDS Appliance and the Solaris host. If the Solaris host has two HBA ports (two WWNs) each zoned to one port on Actifio Node 1 and one port on Actifio Node 2, then that host will have four paths; this is the recommended configuration. Do not use more than eight paths.

When adding a new host that is accessed via Fibre Channel SAN, the new host must be zoned to the Actifio Appliance by your storage administrator. The storage administrator will need to know the host WWN.

To find the WWN of a Solaris host on a Fibre Channel SAN:

```
-bash-4.1# fcinfo hba-port | grep HBA
HBA Port WWN: 2100001b328179fe
HBA Port WWN: 2101001b32a179fe
```

Note: *Proper multipathing is critical for maintaining application-aware mounts over a system restart.*

Ensuring NFS Connectivity on a Solaris Host

This section includes:

[Limitations](#) on page 59

[Using NFS protocol for Solaris LDOM and Solaris Zones hosts in AGM](#) on page 59

When the Actifio Connector manages data movement over NFS, the Actifio sky appliance uses an NFS share created on it and exports to the Solaris host to create a copy of application data during each Snapshot or Dedup Async or StreamSnap job.

Limitations

- Only NFSv3 is supported.
- System state captured with staging disk format NFS are ineligible for Actifio Cloud Mobility.
- Cross platform presentation of Oracle images captured over NFS is not supported. For example, Oracle data captured from a Solaris system cannot be presented on a Linux system.
- Oracle databases captured as ASM Disk over NFS cannot be mounted as Standalone ASM or as ASM RAC.

Before You Begin

Actifio supports NFS protocol to present a staging disk as a NFS share to a Linux or Solaris host. The staging disk is presented directly to the production host. These firewall ports must be open on the client:

Required Ports for NFS

Port	Used For
111	Portmapper/rpcbind
2049	nfsd
4001	Mountd
4045	lockd
756	statd

Ensuring NFS Connectivity in an Oracle Sun Solaris Environment

The Actifio Appliance must be able to communicate with the Actifio Connector on the host over an IP network.

These two packages must be installed on each host:

- nfs-utils
- nfs-utils-lib

For Oracle Databases in a Solaris Environment, Local Zones, the Actifio Connector and an NFS client must be running in the Local Zones, and the local zone IP must be added as a physical host (Generic) to the appliance in the AGM Manager.

Use the staging disk format NFS from AGM, or set this using `udstask chost -diskpref "NFS" <hostid>` from the CLI. NFS staging disks get mounted on the appliance and exported as an NFS share to the Host/Zones.

For more information, refer to the **Oracle DBA's Guide to Actifio Copy Data Management**.

12 Supporting HP-UX with Actifio VDP

This chapter includes:

- Ensuring iSCSI Connectivity on an HP-UX Host (Actifio Sky only) on page 63
- Ensuring Fibre Channel Connectivity on an HP-UX Host on page 63
- Ensuring NFS Connectivity on an HP-UX Host Connected to a Sky Appliance on page 64
- Installing the Actifio Connector on HP-UX Hosts on page 65

Location of UDSAgent.log on HP-UX Hosts

On an HP-UX host, logs are stored in `/var/act/log`.

Location of Scripts on HP-UX Hosts

You can create scripts to perform pre- and post- actions on applications on the HP-UX host. To use scripts, create a folder called `/act/scripts` and store all scripts there. For detailed instructions on how use VDP scripting, see [Chapter 18, APPID Pre- and Post-Scripts for Scheduled Data Protection Jobs](#) and [Chapter 19, Super Scripts for Workflows and On-Demand Data Access Jobs](#).

Note: Only Fibre Channel connectivity to CDS Appliances is supported. For Sky Appliances, iSCSI connectivity is supported. CDX Appliances do not support HP-UX.

Ensuring iSCSI Connectivity on an HP-UX Host (Actifio Sky only)

When the Actifio Connector manages data movement over iSCSI, VDP uses a staging disk to create a copy of application data during each Snapshot or Dedup Async job.

If iSCSI is used, then an Actifio-approved iSCSI initiator must be installed on the host; a reboot is required after this. It is also possible to present the staging disk to a VM using an iSCSI initiator running in the VM; this is normally not necessary.

Note: After the iSCSI initiator is configured, the HP-UX native multipathing is statically linked with the kernel, so no setup is required to use the multipathing support.

Ensuring Fibre Channel Connectivity on an HP-UX Host

When adding a host that is accessed via Fibre Channel SAN, the new host must be zoned to the Actifio Appliance by your storage administrator. The storage administrator will need to know the host WWPN.

Define a total of four paths (this is both the minimum and recommended number) or at most eight paths (absolute maximum) between the CDS Appliance and the AIX host.

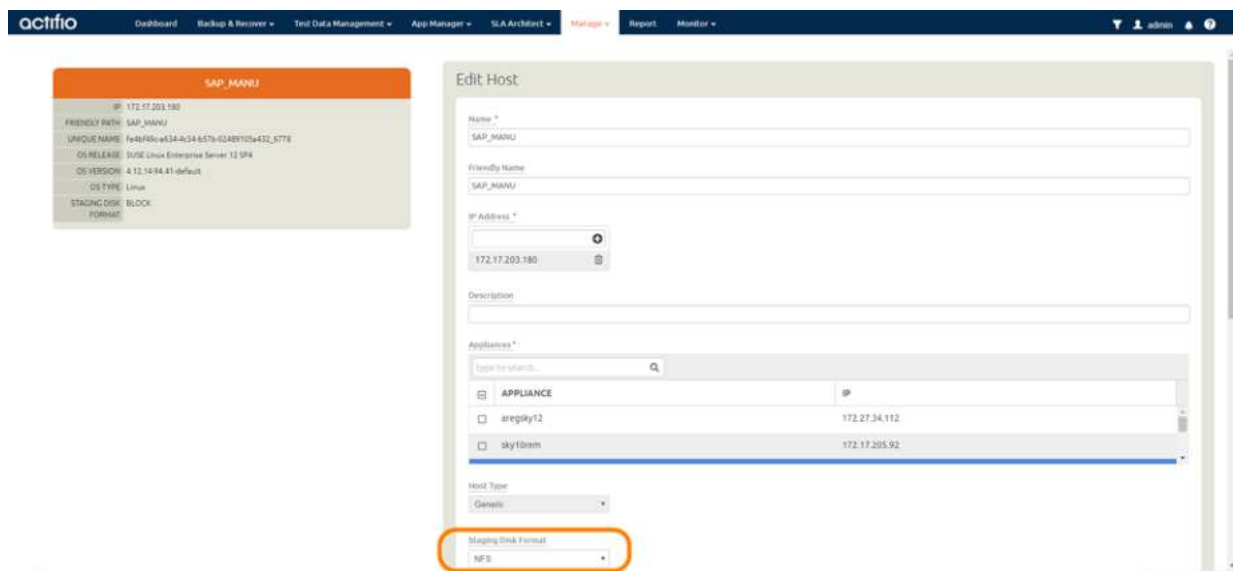
If the HP-UX host has two HBA ports (two WWPNs) and each is zoned to one port on Actifio Node 1 and one port on Actifio Node 2, then the host will have four paths; this is the recommended configuration.

Ensuring NFS Connectivity on an HP-UX Host Connected to a Sky Appliance

When Actifio VDP manages data movement over NFS, during each Snapshot or Dedup Async or StreamSnap job, VDP uses an NFS share created on the appliance and exports to the Linux host a copy of application data.

Using NFS protocol for HP-UX Hosts

Use the AGM Manage > Hosts Edit section to set the Staging Disk Format to NFS. When mounting an image captured this way, you have the option to mount them as an NFS share.



Setting Staging Disk Format to NFS for an HP-UX Host

Setting the Staging Disk I/O Path

HP-UX VMs must also select a staging disk I/O path. You can assign either NFS or SAN (iSCSI) transport for the data from the host to the staging disk. To configure staging disk I/O path:

1. From the AGM Manage > Hosts section, right-click the host to configure and select Edit.
2. In the Edit Host page, scroll down to the Staging Disk I/O Path section.
3. Select one of the following options:

Transport	Actifio volumes are presented	to the	attached to VM as
NFS to Guest	as NFS shares	ESX server	vmdk
NFS Transport	over NFS data store	ESX server	raw device mapping
SAN to Guest	to the iSCSI initiator	Guest VM	ESX is bypassed
SAN Transport	to the iSCSI initiator or to Fibre Channel	Guest VM	ESX is bypassed

Installing the Actifio Connector on HP-UX Hosts

For HP-UX, the installer comes as the file: **connector-HPUX-*<version>*.depot**. It runs as a daemon process under the user name root. The connector writes to a log file in the installation directory (`/var/act/log/UDSAgent.log`).

To install the Actifio Connector on a HP-UX host:

1. Open a browser to `https://<Actifio Appliance IP>` to access the Actifio Resource Center.
2. Click the **HP UX Connector** icon to download the HP-UX install package.
3. Install the Actifio Connector by running `swinstall -s /<connector_filename>.depot *`

Note: Enter the `*` included at the end of the **swinstall** command as shown above. It instructs **swinstall** to install only the software it finds in the depot (the Actifio Connector). If you accidentally enter `/*` you will receive a number of spurious error messages regarding software packages that could not be found.

Manually Uninstalling the Actifio Connector from an HP-UX Host

To uninstall the Actifio Connector from an HP-UX host, run: `swremove udsagent`.

You can also remove connectors from many hosts simultaneously from AGM; see [Maintaining Connectors on Hosts](#) on page 26.

Upgrading the Actifio Connector on an HP-UX Host

Use the Connector Management tool in AGM to upgrade the Actifio Connector on your hosts. Refer to [Maintaining Connectors on Hosts](#) on page 26.

Table 1: HP-UX Connector Commands

Task	Command option
Verify the successful installation of the Actifio Connector	<code>swlist grep udsagent</code>
Verify the status of the Connector	<code>/etc/udsagent status</code>
Manually stop the Connector service	<code>/etc/udsagent stop</code>
Manually start the Connector service	<code>/etc/udsagent start</code>
See the Connector logs	<code>/var/act/log/UDSAgent.log</code>

13 Adding Your Hosts to an Actifio Appliance

These are the steps to connecting a non-VMware host to your VDP system. The first two are operating system-specific, the third applies only to hosts that will use VDP in-band storage (CDS Appliance only).

Table 1: The Two OS-Specific Steps for Connecting Non-VMware Hosts

Host	Install the Connector	Add the Host
Windows Server, or Hyper-V or SCVMM	Installing the Actifio Connector on Microsoft Windows Hosts on page 36	Chapter 15, Adding Windows Server and Hyper-V Hosts to AGM Adding Unix Hosts to AGM on page 71
Linux	Installing the Actifio Connector on a Linux Host on page 50	
IBM AIX	Installing the Actifio Connector on IBM AIX Hosts on page 56	
IBM HMC	The Connector is not required for IBM HMC hosts.	
Sun Solaris	Installing the Actifio Connector on Solaris Hosts on page 60	
HP-UX	Installing the Actifio Connector on HP-UX Hosts on page 65	
VMware VMs	<i>A VMware Administrator's Guide to Actifio Copy Data Management</i>	

After performing the OS-specific steps in the table above, the next steps are the same for all host types:

1. [Assigning VDisks for the Host Copy Data \(In-Band CDS Appliance only\) on page 68.](#)
2. [Configuring Hosts to Auto-Discover their Applications on page 69.](#)
3. [Reconciling Inconsistent Host Information across Multiple Appliances on page 70](#)

If you no longer want to protect the applications or VMs on a host, you can delete it from VDP management; see [Deleting Hosts Using the AGM on page 70.](#)

You can have pre- and post-scripts run on your applications and VMs when they are triggered by a VDP job. Scripting is detailed in [Chapter 18, APPID Pre- and Post-Scripts for Scheduled Data Protection Jobs](#) and in [Chapter 19, Super Scripts for Workflows and On-Demand Data Access Jobs.](#)

Note: You don't add a vCenter or an ESXi Cluster, you discover it; see ***A VMware Administrator's Guide to Actifio Copy Data Management.***

Assigning VDisks for the Host Copy Data (In-Band CDS Appliance only)

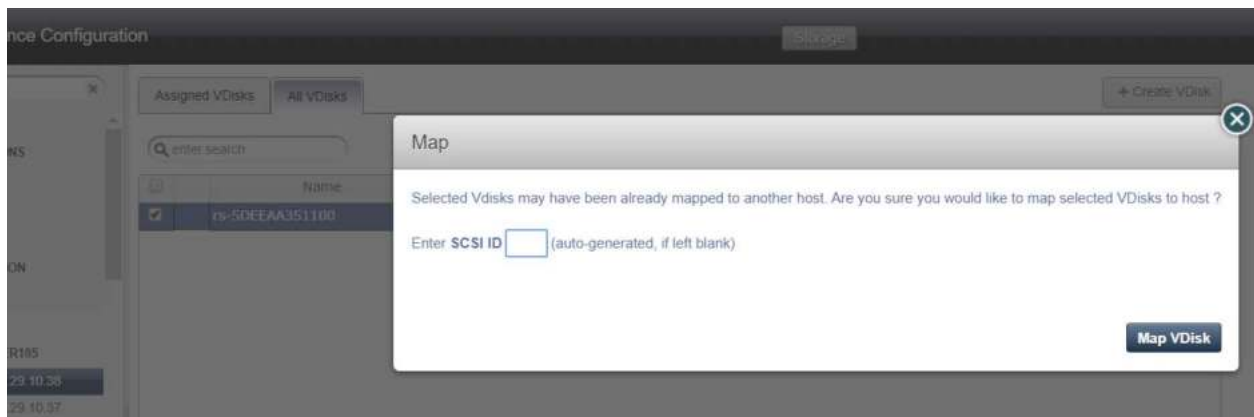
Hosts that use Actifio-provided in-band storage must have VDisks assigned (mapped) to them.

To assign a virtual disk to a host:

1. Open AGM to **Manage > Appliances**.
2. Right-click the and select **Configure Appliance**.
3. In the navigation pane under Hosts, select the host and the **All VDisks** tab.
4. Select one or more virtual disks and click **Map**. A confirmation dialog appears.
5. Enter the **SCSI ID** for the VDisk. The SCSI ID is auto-generated if it is left blank.
6. Click **Map VDisk**.



Mapping a VDisk to an In-Band Host



Confirmation of VDisk Mapping

Configuring Hosts to Auto-Discover their Applications

You can enable your appliances to auto-discover new applications on a configured host. This does not protect the new applications, it only discovers them. You can only enable this feature after the host has been added.

1. Open the **AGM** to the **Manage > Hosts** page.
2. Right-click the host to enable auto-discovery on, and select **Edit**.
3. Slide the **Enable Auto Discovery** button to the right and click **Save** in the lower right corner.

The screenshot shows the Actifio AGM interface. On the left, a host card for 'agm-rh5.8-orcl' displays details: IP (172.17.139.206), Friendly Path (agm-rh5.8-orcl), Unique Name (agm-rh5.8-orcl_2463090_000df), OS Release (Red Hat Enterprise Linux Server release 5.11), OS Version (2.6.18-417.el5), OS Type (Linux), and Staging Disk Format (BLOCK). On the right, the 'Edit Host' form is open. Fields include Name (agm-rh5.8-orcl), Friendly Name (agm-rh5.8-orcl), IP Address (172.17.139.206), and Description. The 'Appliances' section shows a search bar and a table of available appliances:

APPLIANCE	IP
<input type="checkbox"/> rdsrsc	172.29.11.220
<input type="checkbox"/> dev134-251.dev.actifio.com	172.17.134.251
<input type="checkbox"/> glamour	172.17.134.234
<input type="checkbox"/> SKY8.0-226	172.16.122.226

Below the appliances list, the 'Host Type' is set to 'Generic' and 'Staging Disk Format' is set to 'Block'. At the bottom, the 'Enable Auto Discovery' toggle is turned on and highlighted with an orange circle.

Enabling Application Auto Discovery for a vCenter Host

Reconciling Inconsistent Host Information across Multiple Appliances

A host can be defined on multiple appliances, either intentionally or unintentionally. This is common with VMware VMs. If the host is managed by two VDP appliances, then the name is preceded by a multiple-appliances icon and the entry in the Appliance column shows a link to the other appliance.

When records of the same host reside on multiple VDP appliances, the host information can be slightly different from one appliance to another. In that case, when you edit the host record, you will see a Host Reconciliation section at the top of the host record. Review the information in the table, and select the host record that has the most up-to-date information. Then click Submit. All other host records in the table will be reset to match the selected host record. After this, you see the Edit Host page detailed in Editing Host Properties.

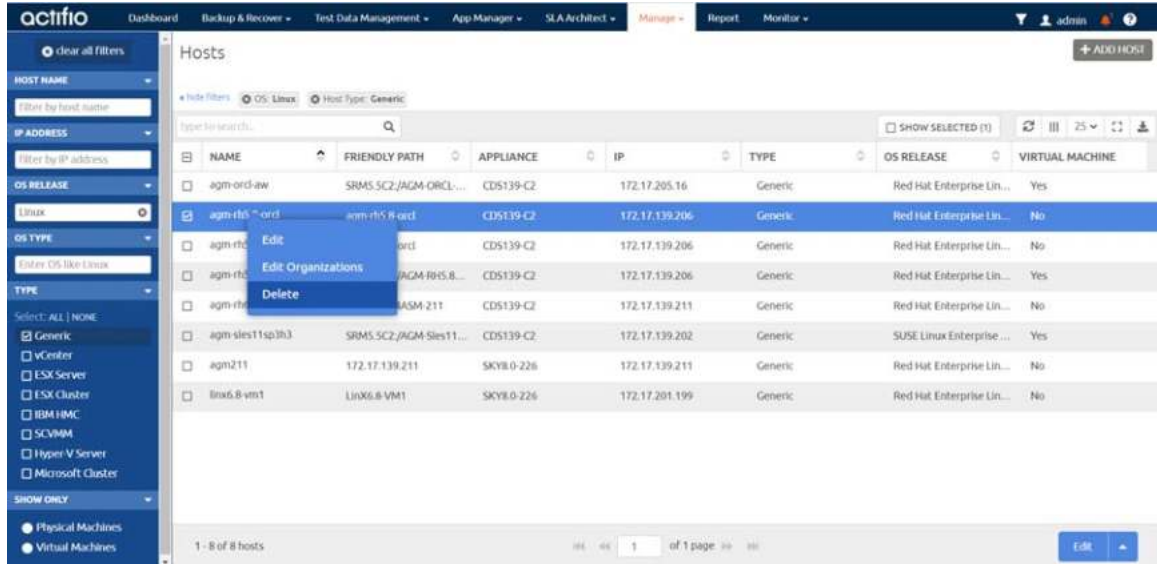
Security Software on Hosts

Security software, including antivirus and other disk monitoring software, can interfere with mounting, cloning, LiveCloning, or restoring any non-VM application to a host. Consider exempting the target disk from the interfering software for the duration of the operation. For more information, see [The Connector and the Network Environment](#) on page 24.

Deleting Hosts Using the AGM

You can delete Hosts. To delete a host:

1. Open the **AGM** to the **Manage > Hosts** page.
2. Right-click the host to enable auto-discovery on, and select **Delete**.
3. In the Delete Host window, click **OK**.



Deleting a Host from AGM

14 Adding Unix Hosts to AGM

Unix hosts include Linux, AIX, IBM HMC, Solaris, and HP-UX hosts. To add a Unix host to your VDP system:

1. Open the AGM to **Manage > Hosts**.
2. In the upper right corner, select **+ Add Host**.
3. In the Add Host form, enter the name and an optional friendly name. The name of a host should start with a letter, and can contain letters and digits (0-9).

Note: Underscore ('_') characters are not valid in host names.

4. Enter the IP address of the host in **IP Address**. Click **+** to add multiple IP addresses.
5. In the Appliances section, select the AGM managed appliances that will serve this host. If the list is long, you can use the Search box to find a specific appliance or group of appliances.
6. In Host Type, select **Generic**.

The screenshot shows the 'Add Host' form in the Ocular interface. The form includes the following fields and sections:

- Name ***: Text input field.
- Friendly Name**: Text input field.
- IP Address ***: Text input field with a dropdown arrow, containing the IP address 172.16.199.85 and a trash icon.
- Description**: Text input field.
- Appliances ***: A searchable list of appliances. The search bar contains 'type to search...'. The list has columns for 'APPLIANCE' and 'IP'. The selected appliance is 'dev134-251.dev.ocular.com' with IP '172.17.134.251'. Other appliances include 'rdsr' (172.29.11.220), 'glamour' (172.17.134.234), and 'SKY8.0-226' (172.16.122.226). A 'SHOW SELECTED (1)' button is visible.
- Host Type**: A dropdown menu set to 'Generic'.
- Footer**: 'Application Discovery Credentials', 'Connector Settings', and 'Organizations' sections.
- Buttons**: 'Cancel' and 'Add' buttons at the bottom right.

Adding a New Host

7. Enter **Application Discovery Credentials** as needed to discover and protect the applications on the host.
8. In **Connector Settings**, use **5106** for Connector Port unless you have changed from the default value. You can also use 56789. Do not use any other port unless instructed by Actifio Support. Enter the user name and password of the Actifio Connector on the host if you intend to run pre- and post-scripts on the host.
9. In **Organizations**, select one or more Actifio organizations for the host to be a member of. Organizations are explained in the AGM online help.
10. Click **Add**.

The next step is [Assigning VDisks for the Host Copy Data \(In-Band CDS Appliance only\)](#) on page 68.

Notes for HMC Hosts

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

When an IBM HMC host is added, LPARs in an active state (rmc_state is ACTIVE) on that HMC are also discovered. If an LPAR host is created or deleted after the IBM HMC was discovered, use re-discover to update the known LPARs.

To activate the rmc state of an LPAR, run:

```
/usr/sbin/rsct/install/bin/recfgct  
/usr/sbin/rsct/bin/rmcctrl -p
```

(CDS Appliance only) If any VIO servers were discovered after adding the HMC host, then manually define any FC HBAs in use on those VIO Servers that are also zoned to the Actifio Appliance. To do this go to the Ports tab of each VIO Server and use the 'Add Port' Button. If the VIO Server WWPNs do not appear, use the Custom option to add them manually. Failure to do this may result in LPARs that use vSCSI automatically configuring the iSCSI initiator in the LPAR, rather than use FC staging disks presented to and then passed through the VIO server to the LPAR using vSCSI.

15 Adding Windows Server and Hyper-V Hosts to AGM

To add a new Windows Server or Hyper-V host to AGM:

1. Open the AGM to **Manage > Hosts**.
2. In the upper right corner, select **+ Add Host**.
3. In the Add Host form, enter the name and an optional friendly name. The name of a host should start with a letter, and can contain letters and digits (0-9). Underscore ('_') characters are not valid in host names.
4. Enter the IP address of the host in **IP Address**. Click **+** to add multiple IP addresses.
5. In the Appliances section, select the AGM managed appliances that will serve this host. If the list is long, you can use the Search box to find a specific appliance or group of appliances.
6. In Host Type, the type you pick depends on what you're using the Windows host for. These are detailed in [Table 1: Host Types and Connector Settings Overrides](#) on page 73.

If you select vCenter or ESX Server, then you must also select the data transport mode, NFS or SAN. NFS is the default setting.

If you select vCenter or ESX Server, you will also see a new section appear for vCenter Settings or ESX Settings. Enter and test the port, username, and password to connect to the host.

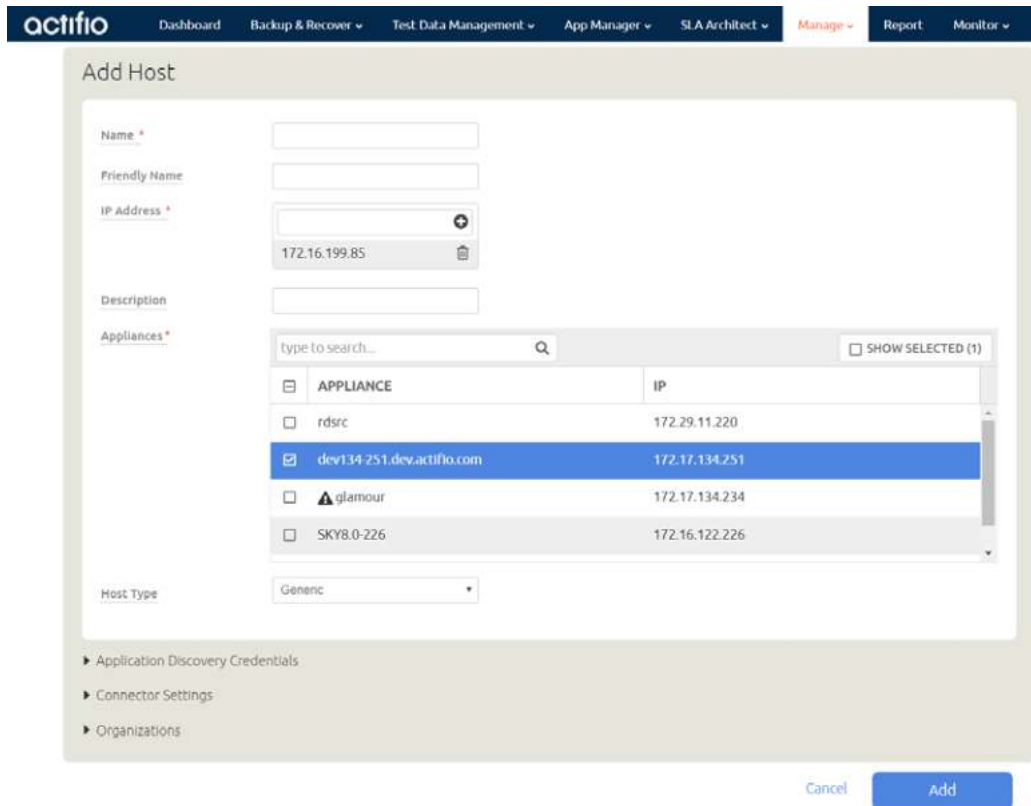
Table 1: Host Types and Connector Settings Overrides

To Protect	Select Host Type	Connection Type
CIFS file systems, SQL Server, SharePoint, Exchange	Generic	The default connector port for Generic hosts, SCVMM and Hyper-V VMs is 5106. If you use a different port, then enter it here.
Hyper-V managed by Microsoft SCVMM	SCVMM	If the Connector username and password have changed, then change them here.
Standalone Hyper-V on Windows server	Hyper-V Server	If you do not need to override the default settings, then enter nothing here.
ESXi standalone	ESX Server	The default ESX Server management port is 902. If you use a different port, then enter it here. If the ESX server username and password have changed, then change them here. If you do not need to override the default settings, then enter nothing here.

Table 1: Host Types and Connector Settings Overrides

To Protect	Select Host Type	Connection Type
vCenter with ESXi VMs	vCenter	<p>A vCenter can have both vCenter Settings and Connector Settings, because a vCenter might also have the Actifio Connector installed on it.</p> <p>The default vCenter management port is 443. If you use a different port, then enter it here.</p> <p>If the vCenter username and password have changed, then change them here.</p> <p>If you do not need to override the default settings, then enter nothing here.</p>

7. Enter **Application Discovery Credentials** to discover and protect the applications on the host.
8. In **Connector Settings**, use **5106** for Connector Port unless you have changed from the default value. You can also use 56789. Enter the user name and password of the Actifio Connector on the host if you intend to run pre- and post-scripts on the host.
9. In **Organizations**, select one or more Actifio organizations for the host to be a member of. Organizations are explained in the AGM online help.
10. Click **Add**.



Adding a New Host

16 Configuring External Snapshot Pools on IBM Storwize and Pure Storage FlashArray

This chapter details:

[Prerequisites for an External Snapshot Pool Deployment](#) on page 76

[Adding an External Storage Array](#) on page 77

[Adding an External Snapshot Pool](#) on page 78

[Adding New Hosts](#) on page 78

About External Snapshot Pools

Actifio Sky appliances can use storage pools on IBM Storwize and Pure Storage FlashArray storage arrays, to store Snapshot images instead of within a Sky appliance's Snapshot pool. External Snapshot Pools (ESP) enable the Sky appliance to implement very high speed backup since ESPs leverage snapshot capabilities of modern arrays, especially flash-based arrays, which can handle a very large number of snapshots with high performance and very low operational overhead. VDP can work with any host that can connect to a supported Fibre Channel and iSCSI connected external storage array. This enables the hosts to have Fibre Channel connectivity to the storage array with Sky support, which then presents a number of options for storing the backups. The Sky appliance itself connects to the external storage array using an iSCSI connection.

Backed up data can be stored in the Dedup pool of the Sky appliance or in a remote Actifio appliance where data is sent using StreamSnap or Dedup-Async replication policies and stored in a regular or external snapshot pool. You can also send the data to an OnVault pool for object storage either on premise or in a Cloud.

When the production data is not on the same array as the ESP, use the Actifio Connector to perform a full copy, and subsequently, incremental forever copies of the changed production data. The copied data is sent to the storage array and the array manages snapshots of the copied data. The Actifio Connector on the host reads data from the production array and writes changed blocks to the ESP.

There is substantial savings in storage footprint if the production data can be in the same array as the ESP (Actifio recommends you keep a separate full copy backup). This configuration enables the fastest backup of data; the storage array takes only incremental snapshots and the snapshots are faster since no unchanged blocks are copied.

The backed up data can be recovered either locally or remotely. You can, for example, instantly mount images from storage array snapshots. You can also mount local and remote dedup images via the storage array, clone OnVault images to the storage array and then mount them, and mount OnVault images directly from the Sky appliance.

In addition, data can be available to Test and Dev environments with high performance and availability of mounted images, and SmartCopy backups perform better.

Prerequisites for an External Snapshot Pool Deployment

External Snapshot pools are used to store snapshot images in IBM Storwize and Pure Storage FlashArray storage arrays instead of within a Sky appliance's Snapshot pool.

Note: External Snapshot pools may not contain spaces in the underlying disk group name or some backups may not run in the desired in-place snapshot mode. Rename the disk pool on the source storage array to remove spaces.

For IBM Storwize and Dell Unity Storage Arrays

Here are the pre-requisites for a successful External Snapshot Pool deployment on a IBM Storwize or a Dell Unity storage array:

- An iSCSI port configured on the SVC that can be reachable from the Sky VM.
- A dedicated empty mdiskgrp. This can be a child mdiskgrp, but it must have no VDisks in it at the time you start using it.
- A Flashcopy license on the array/SVC.
- A log-in as a privileged (admin) user with a password.
- All hosts must be Fibre Channel enabled and able to connect to Storwize. The connectivity can actually be either FC or iSCSI. For FC, this means all host (source and target) must be able to be FC zoned to Storwize.
- Actifio VDP needs to connect to both Storwize cluster IP and iSCSI IP. The VDP to Storwize connection requires iSCSI because VDP is on VMware.
- The VDP connector must be installed in all host source and target.
- Hosts you intend to protect should be defined and connected as Hosts to the Storage Array.

Note: Hostnames must not include spaces or the connection will fail.

For Pure Storage FlashArray Storage Arrays

The External Snapshot Pool for Pure Storage is created automatically when you add the Pure Storage array. Here are the pre-requisites for a successful Pure External Snapshot Pool deployment:

- An iSCSI port configured on the SVC that can be reachable from the Sky VM.
- A log-in as a privileged (admin) user with a password.
- System clocks on the Pure storage array and the Sky appliance should be in sync. If there is more than twenty five (25) minutes discrepancy between the two, connections from the Sky appliance to the Pure storage array may fail. For existing connections, jobs may fail with errors.
- The VDP connector must be installed in all host source and target.

Adding an External Storage Array

Before you add an external storage array:

- AGM must be managing at least one Sky appliance. CDS appliances do not support ESPs.
- You need administrator credentials for the storage array and the IP Address or FQDN (fully qualified domain name) of the storage array.
- For an IBM Storwize (v3700, v5000, v7000, SVC) storage array:
 - The storage array administrator has provisioned an empty mdiskpool for use by the Sky appliance.
 - VDP needs to connect to both Storwize cluster IP and iSCSI IP

To add an external storage array:

1. In the AGM Manager, click **Storage Arrays**. The Storage Array page opens.
2. Click **Add Storage Array**.
3. In **Name**, add a descriptive name for the external storage array. This name will be used on both the AGM and the Sky appliances. It does not need to match any name on the storage array.
4. In **IP/FQDN**, add the IP address or the fully qualified domain name (array.thiscompany.com) of the external storage array.
5. From the **Storage Array Type** drop-down, select either Pure Storage FlashArray or IBM Storwize.
6. In **Username** and **Password**, enter login credentials of the administrator account on the storage array.

Note: The Pound Sterling character (£) is not supported for passwords.

7. In the **Select Appliance** section, select one or more Sky appliances.
8. Click **Test Connectivity** to check connection to the appliance(s). If the test succeeds but the pool is not created, see [If Test Connectivity succeeds but no pool is created](#) below.
9. Expand the Organizations menu and select the Users/Groups/Organizations to associate with this array. The Users/Groups/Organizations that you do not select cannot use the array.

If you do not select any specific Users/Groups/Organizations, the storage array and its associated pools will be available to all AGM users.
10. Click **Save** to create the array.

The newly created array will be listed in the Storage Array page with the array name and other properties.

Note: Future pool expansion on a Storwize ESP pool must be done on the Storwize array. VDP will detect this expansion automatically.

Note: For an IBM Storwize storage array you will see a newly created username for each Sky appliance to use with the array. These have the pattern 'act' followed by a 10-digit number (for example: act1415066080). Manipulations of snapshots and images on the array by Sky will appear in the Storwize Audit Log using this act-<number> username.

If Test Connectivity succeeds but no pool is created

If Test Connectivity succeeds, but fails to create the storage pool for Pure Storage FlashArray, or fails to create either the storage array or the external snapshot pools for IBM Storwize, then check the iSCSI network connection between the Sky appliance and the storage array. Test Connectivity checks only the connectivity with the management IPs of the array and not the iSCSI network, which may be on a separate network.

Adding an External Snapshot Pool

Once you have created an external storage array, it is necessary to specify which pool on that array will be used as an External Snapshot Pool for an Sky appliance.

Adding an External Snapshot Pool to an IBM Storwize array

The pool on the IBM Storwize array must be empty. Each pool should be used with only one appliance. If you have more than one appliance using an IBM Storwize array, each appliance should have its own pool.

To add an External Snapshot pool to an IBM Storwize array:

1. In the AGM Manager > Appliances, right-click the selected appliance to open the Appliance Configuration page, then click **Storage Pools**. The Storage Pool page opens listing all storage pools on different appliances managed by AGM.
2. Click **Add External Snapshot Pool**. The Add External Pool page opens. This is visible only after you have created at least one IBM Storwize array.
3. From the **Choose Storage Array** drop-down, select an array. Only IBM Storwize arrays are listed in this drop-down.
4. In **Pool Name**, add a descriptive name for the External Snapshot Pool.
5. From the **Choose Appliance** drop-down, select the appliances that should use the External Snapshot Pool.
6. In the **Choose IBM Storwize Pool** section, select a pool. You can use the search box to look for a specific pool by name. (The pools listed in this section are empty pools.)
7. In the **Threshold Monitor** section:
 - o Use the slider to set the Warning level. The default Warning level is 80%. When this level is exceeded, you see warnings.
 - o Use the slider to set Safe Mode to an appropriate level of usage. The default value is 90%. When this value is exceeded, the Sky appliance stops writing to storage and jobs fail.
8. Expand the Organizations menu and select the Users/Groups/Organizations to associate with this pool. If you do not select any Users/Groups/Organizations, the pool will be available to all AGM users.
9. Click **Save** to create the External Snapshot Pool. The newly created pool will be listed in the Storage Pools page with Type *Ext Snapshot*.

Configuring an External Snapshot Pool on a Pure Storage FlashArray

The Pure Storage FlashArray doesn't have a Pool virtualization concept. Sky supports this by displaying the used and available space on the entire PureStorage Flasharray as it is presented to the Storage Administrator on the array itself. There is no need to provision a distinct pool within the array for use.

In the Threshold Monitor section:

- o Use the slider to set the Warning level. The default Warning level is 80%. When this level is exceeded, you see warnings.
- o Use the slider to set Safe Mode to an appropriate level of usage. The default value is 90%. When this value is exceeded, the Sky appliance stops writing to storage.

Adding New Hosts

If you create a host on the storage array after configuring the storage array as an ESP, the new hosts cannot complete snapshots until the next scan for new host data is complete.

Scanning the array for the host data is triggered:

- When the array is added to the appliance
- When a host is created on the appliance
- Daily, at midnight.

17 Configuring LDAP and Role-Based Access

This chapter details:

[LDAP Authentication](#) on page 79

[SAML Authentication](#) on page 85

[Managing Web Certificates](#) on page 86

LDAP Authentication

You can use a single existing LDAP (Lightweight Directory Access Protocol) server for AGM user authentication and to map LDAP groups to AGM roles. Active Directory provides authentication, directory, policy, and other services in a Windows environment, and LDAP is an application protocol for querying and modifying items in directory service providers such as Active Directory.

This section includes:

[Things to Consider when AGM Is Configured for LDAP Authentication](#) on page 79

[Configuring LDAP Settings](#) on page 80

[Mapping LDAP Groups to Roles and Organizations](#) on page 81

[Viewing LDAP Groups](#) on page 83

[Deleting an LDAP Group](#) on page 84

Things to Consider when AGM Is Configured for LDAP Authentication

When AGM connects to the LDAP server for authentication it updates users with credentials cached from the LDAP server. When AGM is configured for LDAP to authenticate users:

- LDAP users who need to access AGM can have a user created the first time they successfully log into AGM if the Auto Create User parameter is enabled (see [Configuring LDAP Settings](#)).
- LDAP users can also be created in AGM by administrators. These new users can have their passwords left blank. User accounts with empty passwords will be “locked” until the user logs in with LDAP once to set their cached credential.
- The login process is transparent to users; username and password are the same as their LDAP credentials. Users receive no feedback on the reason for a failed login attempt. The reason is logged for administrative use but for security purposes the user is only informed that login failed. Users receive no information about which authentication method is in use.
- The hash value of each user credential is cached in the AGM database.
- If AGM is not able to reach the LDAP server and if AGM is configured to use database fallback (not selected by default), then each user will be authenticated against their cached credential hash value stored in the AGM database.
- Cached credential hash values are refreshed upon establishing connection with configured LDAP servers.

- The default “admin” account will always be authenticated against internal credentials stored in the AGM database.
- LDAP configuration is not shared between AGM and managed Actifio appliances.

Configuring LDAP Settings

You can use a single existing LDAP (Lightweight Directory Access Protocol) server for AGM user authentication and to map LDAP groups to AGM roles. Active Directory is a database-based system that provides authentication, directory, policy, and other services in a Windows environment, and LDAP is an application protocol for querying and modifying items in directory service providers such as Active Directory.

To configure LDAP server authentication:

1. Click the Manage tab and select Authentication from the drop-down menu. The Authentication page opens.
2. Click LDAP from the drop-down menu to open the Configure LAP page.

Click image to expand.

3. In the LDAP Settings page, (default option), enter the following information:
 - o Server IP/DNS: The server IP address or host name of the server where LDAP is hosted to authenticate AGM users. If you specify a host name, make sure that it can be resolved.
 - o Port #: TCP/IP port number on which the server is processing LDAP requests. We recommend that you leave this setting at the default of port 389. If you plan to use SSL for the connection, specify port 636.
 - o Use TLS: Specifies that the connection uses TLS to connect with the LDAP server.

Note: In the case of Microsoft Active Directory, for the SSL/TLS connection to properly connect to the LDAP server, the server must have Certificate services installed on it so that it can answer on port 636. You can confirm that the connection is working properly by looking in the event viewer of the LDAPSERVER under Windows Logs -> System. Look for event 36886 by source Schannel. If your output shows a connection and no disconnect, then that means that was a successful connection and LDAP is communicating properly.

- o Privileged User DN: The full DN (distinguished name) of the user that is to perform user lookups in the LDAP server. This field creates the user within AGM that matches the LDAP server account properties.
 - o Password: Password for the lookup user.
 - o Search by Base DN: The base distinguished name (DN) subtree that is used by AGM to search for user and group entries.
 - o Search by Username Attribute: The LDAP attribute to use to match against the supplied login name.
 - o Use Cached Credentials When Directory is Unavailable: Specifies to use the cached credentials in the AGM database for verification when the LDAP server is offline or unavailable. When enabled, all previously cached LDAP users can login using their credentials.
 - o Auto Create User: Specifies to store the username and the hash value of the user credentials in the AGM database when that user logs in through the LDAP server.
4. Optionally, you can use the Test button to confirm that the LDAP server access information is accurate and that authentication has been accepted by the LDAP server. The Test Credentials dialog opens.
Enter your login credentials, then press Test. You should receive a Success message. Click OK to return to the LDAP Settings page.

Note: If you receive an *Error While Testing* message, double-check that you entered the login credentials correctly. If the login credentials are correct, confirm that the LDAP server settings are correct as described in step 5.

5. Click Save.
6. You can now set up group mapping by choosing an LDAP Group and associating it with a role.

Mapping LDAP Groups to Roles and Organizations

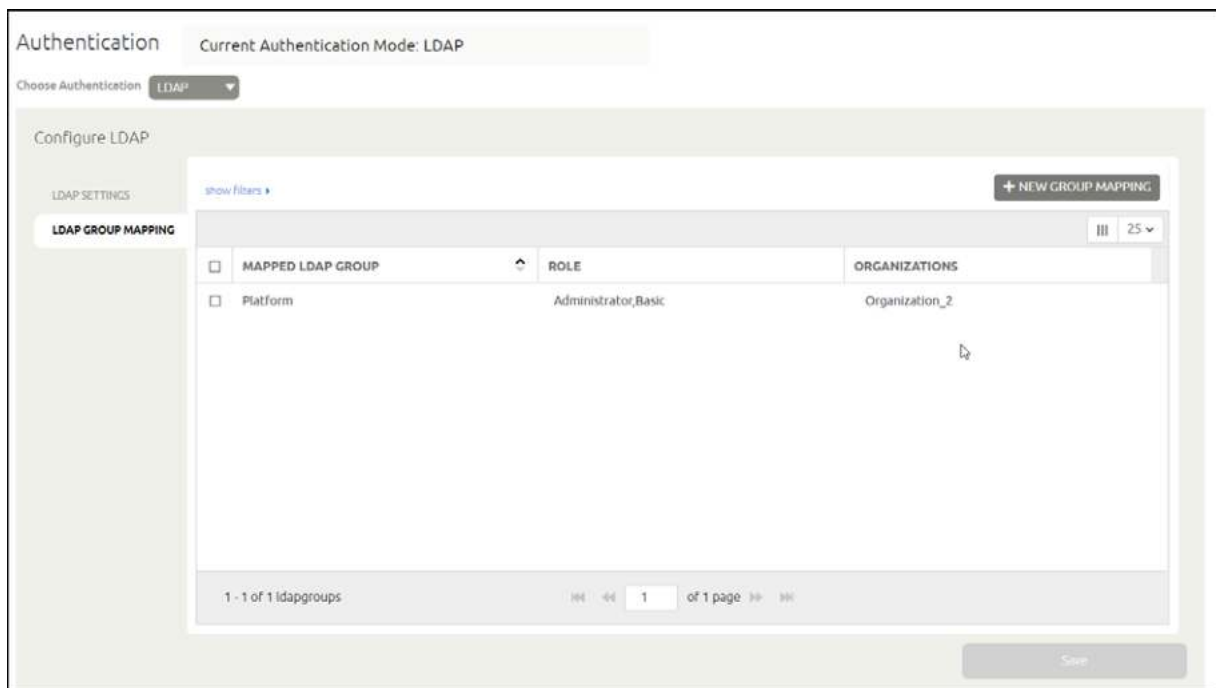
After you have configured your LDAP settings, you can set up group mapping. You can create a mapping by associating an LDAP Group with a role.

Before you begin:

- You must have the Administrative role to perform LDAP group mapping. If you are not an Administrator, you will see this error: *User does not have sufficient rights to perform this Action.*
- During LDAP user authentication, if the group mapping information is not found then the user is assigned with the previously assigned roles/organizations.
- For the LDAP server, the Domain Users group is not supported and will not appear in the list of mappings.

To set up a group mapping:

1. Click the Manage tab and select Authentication from the drop-down menu. The Authentication page opens.
2. Click LDAP to open the Configure LDAP page.
3. Click LDAP Group Mapping to open the LDAP Groups Mapping table.



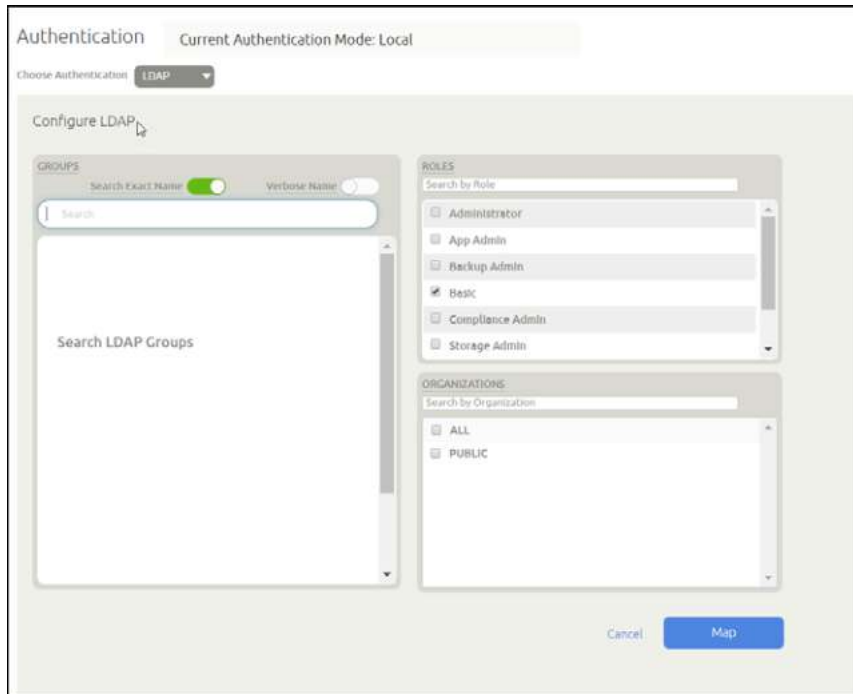
4. Depending on whether you want to edit an existing LDAP group or create a new LDAP group:
 - o To modify an existing LDAP group, select the LDAP group from the list and then select Edit (bottom right-hand corner of the window).
 - o To create a new LDAP group, click New Group Mapping.

The LDAP Group Mapping page appears. The LDAP Group Mapping page has three panels:

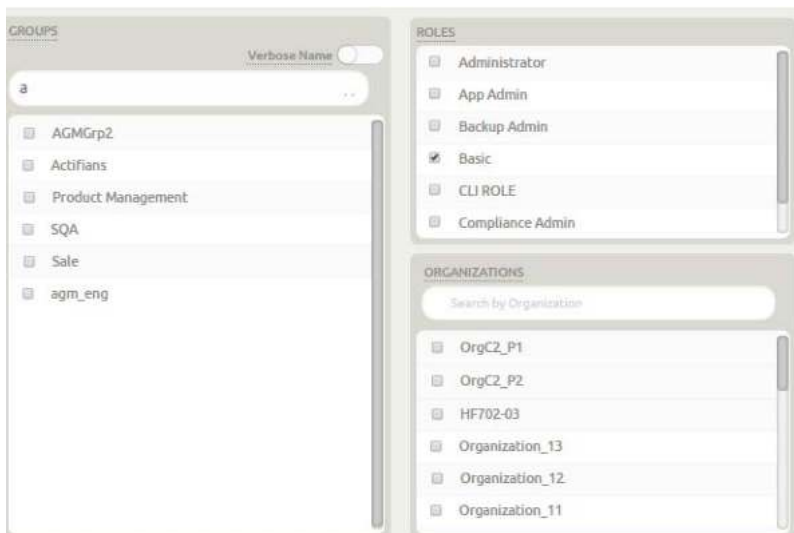
- o Mapped LDAP Group
- o Role
- o Organizations

LDAP groups that appear after a query is performed

- o AGM roles
- o AGM organizations



5. Use the Groups search field to perform a lookup for a specific group from the LDAP server. You can view the full path of each LDAP group found in a search query through the use of the Verbose Name slider. Verbose Name toggles the display of all found LDAP groups by their full distinguished name (DN).



6. Select the desired LDAP group from the left list and then select:
 - o The roles in the Roles list to map the LDAP group to the specific role(s).
 - o The organizations in the Organizations list that will use this resource. This action creates a relationship between the resource (an LDAP group in this case) and one or more organizations.

Note: For details on roles and organizations see [Organizations, Users, Roles and Rights](#), below.

7. Click the following when you are done:
 - o Update, if modifying an existing LDAP group
 - o Map, if creating a new LDAP group
8. Repeat this process for each group that requires mapping.

Organizations, Users, Roles and Rights

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

After you add an Actifio appliance to AGM, all of the imported organizations, users, and roles associated with each appliance are replicated into the AGM as part of the import process. These objects become AGM-level objects and are added to the AGM database. Imported organizations, users, and roles become available for use in AGM (within organization limits). You can modify the imported organizations, users, and roles from AGM.

Note: Modifications to imported organizations, users, and roles are not synchronized back to the appliance from which they were originally imported. Once imported, you cannot make changes to these objects on the appliance; all changes must be made in AGM. This includes subsequent resource assignments (or reassignments) to existing organizations.

Organizations, Users, Roles and Rights are detailed in the AGM Online Help.

Viewing LDAP Groups

The LDAP Group Mapping window lists all of the LDAP groups created in AGM. You can see information such as mapped LDAP group name, assigned role(s), and assigned organization(s).

1. Click the Manage tab and select Authentication from the drop-down menu. The Authentication page opens.
2. Click LDAP to open the Configure LDAP page.
3. Click LDAP Group Mapping to access the mapped LDAP groups list.
4. To modify the display, you can:

Note: Filters of type text, list, and date, persist across different AGM sessions for the same user.

- o Adjust Fields: To modify the fields that appear in the table, right-click within the table header row and click the check boxes for the fields you want displayed (or those fields you do not want to view).
- o Sort Content: To sort the content listed in a table column by alphanumeric order, select a column header and then click the Up or Down arrow to change the order.

- o Adjust Column Width: To adjust the width of a table column to show more content in the table, drag the column divider in a column header to the left or right to resize the column width. Column dividers are marked by a pair of thin gray lines.
- o Filter By: To filter the list, enter one or more filter criteria. (If you do not see the Filter By area, click Show Filter). To clear a filter, click the x to the right of the applied filter.

Note: Filters of type text, list, and date, persist across different AGM sessions for the same user.

5. To export the LDAP groups list click the export icon. You can export in CVS or PDF format.

Deleting an LDAP Group

You can delete an LDAP group that is no longer needed.

To remove an LDAP group:

1. Click the Manage tab and select Authentication from the drop-down menu. The Authentication page opens.
2. Click LDAP to open the Configure LDAP page.
3. Click LDAP Group Mapping to access the mapped LDAP groups list
4. Select the LDAP group from the list and then select Delete (bottom right-hand corner of the window).

Note: You can also right-click on the LDAP group in the list and select Delete from the menu.

5. Click Confirm in the confirmation dialog.

SAML Authentication

You can use Security Assertion Markup Language (SAML) for AGM user authentication. SAML is an open standard for exchanging authentication and authorization data, in particular between an identity provider and a service provider. To configure SAML authentication, you need the IDP metadata. The IDP metadata defines the attributes/behavior of SAML IDP. This metadata must be registered with AGM SAML SP before SAML single sign on (SSO) can work.

Terms:

- AGM SAML SP (Service Provider): Part of AGM, it serves SAML SSO/SLO requests and responses.
- SAML IDP (Identity Provider): Is the enterprise authentication and authorization server that AGM SAML SP relies on for login decisions.

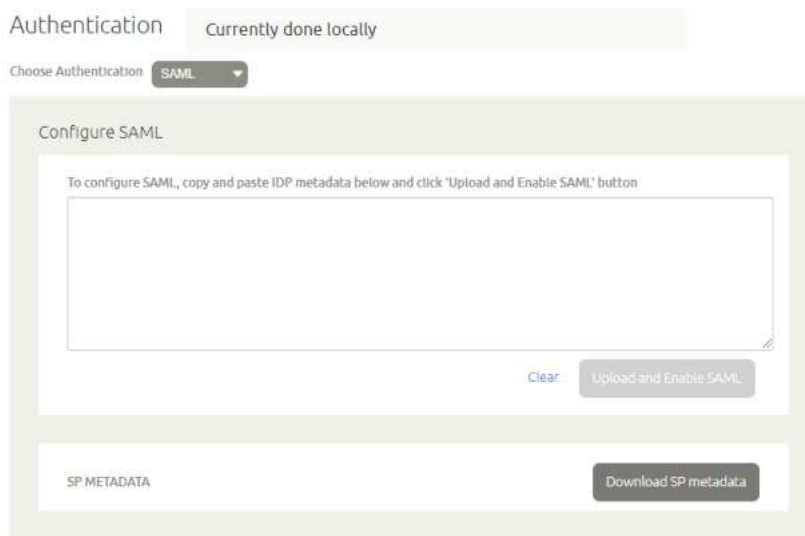
Login and Logout User Experience when using SAML Authentication

During AGM login, the SAML user is redirected to the SAML SSO login page instead of the AGM login page. During logout, the SAML user is logged out of AGM and any other websites they were logged in using SSO.

Configuring SAML Settings

To configure SAML authentication:

1. From the AGM top navigation, click Manage > Authentication. The Authentication page opens.
2. Click Choose Authentication drop-down and select SAML. The Configure SAML page opens.



The screenshot shows the 'Authentication' page in AGM. At the top, it says 'Currently done locally'. Below that, there is a 'Choose Authentication' dropdown menu with 'SAML' selected. The main content area is titled 'Configure SAML' and contains a text box for pasting IDP metadata. Below the text box are 'Clear' and 'Upload and Enable SAML' buttons. At the bottom, there is a section for 'SP METADATA' with a 'Download SP metadata' button.

3. In the text box, copy and paste the IDP metadata. If you need to make modifications and begin again, click Clear.
4. Click Upload and Enable SAML when you are ready to upload the file. AGM will not force you to log out of your off current session. The next time you log into AGM, you will be directed to the to SAML SSO login page.

Downloading SP Metadata

If AGM is configured to use SAML authentication, you can download and review the IDP metadata.

To download IDP metadata:

1. Click the Manage tab and select Authentication from the drop-down menu. The Authentication page opens. The Current Authentication Mode should be SAML.
2. Click the Download SP metadata option.
3. Browse to the Downloads folder and open the IDP file to view it.

Managing Web Certificates

Out of the box, AGM uses self-signed TLS web service certificate. Some companies may require replacing the TLS certificates with those that are in compliance with their security model. AGM users with administrator rights can:

- [Upload PKCS12 File](#) on page 86
- [Reset and Generate New Web Certificate](#) on page 87



Note: Non-administrator AGM users cannot see the Web Certificate drop-down menu option from the Manage tab and cannot upload a PKCS file or replace a self signed TLS certificate.

Upload PKCS12 File

Companies can require replacing the out of the box TLS Certificate to comply with their security model. You can upload a PKCS file to replace a TLS certificate using the instructions below.

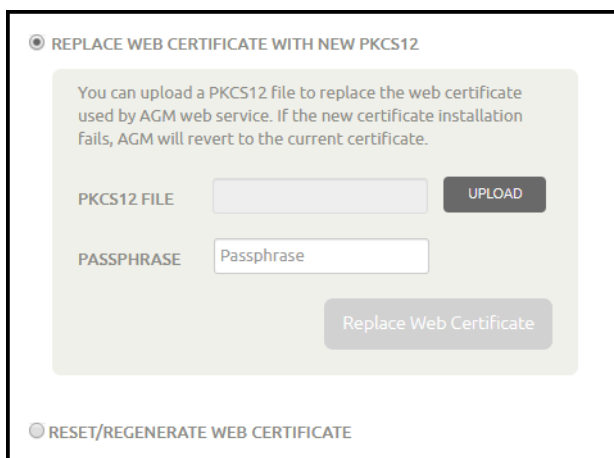
Requirements:

- A valid PKCS file generated for use
- Valid passphrase to use when uploading the PKCS file

Uploading the PKCS File

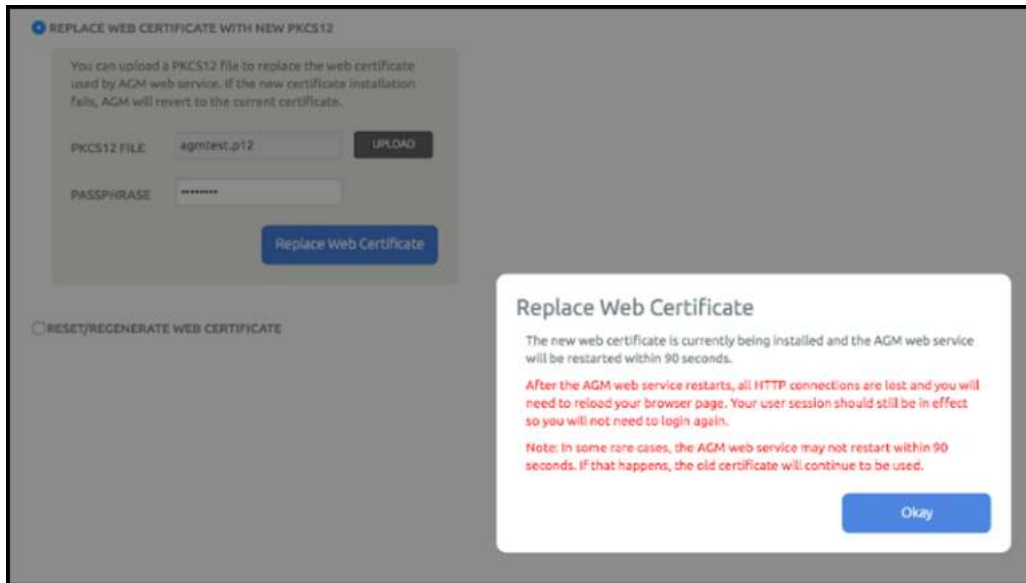
To upload a PKCS file to replace a TLS certificate:

1. Click the Manage tab and select Web Certificate from the drop-down menu. The Web Certificates management page opens listing options to upload a PKCS file (default) or generate and replace a self-signed certificate.



2. Verify the Replace Web Certificate with New PKCS12 option is selected and click Upload. Browse to the location where you have saved the PKCS file and select it.
3. In Passphrase, enter the password for the PKCS file.

4. Click Replace Web Certificate. You will see the following message containing useful information.

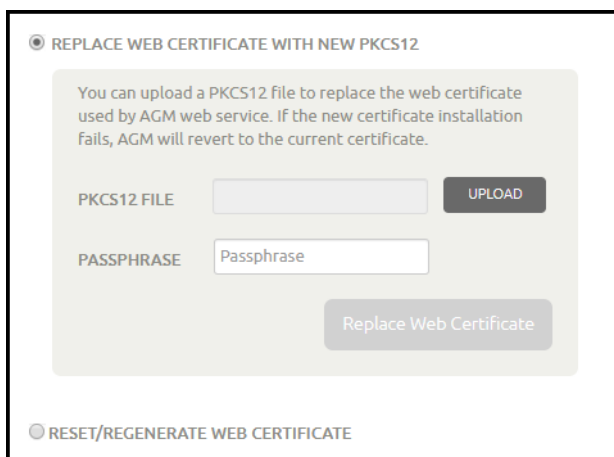


5. Click Okay to begin uploading the file. In case the PKCS file is invalid or the passphrase is incorrect, you will see the message: *Error 10040 Web certificate installation fails due to invalid PKCS12.*
6. Upload a valid PKCS file using instructions in steps 3 to 6. The certificate is replaced and the web service restarts within one hundred and twenty (120) seconds.
7. Refresh your browser and continue using AGM. You will not need to login to a new session.

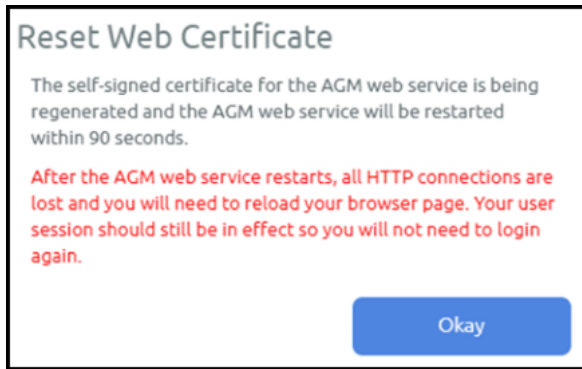
Reset and Generate New Web Certificate

You can generate a new TLS certificate and replace the existing certificate. To generate and replace a self signed TLS certificate:

1. Click the Manage tab and select Web Certificate from the drop-down menu. The Web Certificates management page opens listing options to upload a PKCS file (default) or generate and replace a self-signed certificate.



2. Select the Reset/Regenerate Web Certificate option and click Reset Web Certificate. You will see this message.



3. Click Okay to begin regenerate the new certificate and replace the existing certificate file. If you try to generate a new certificate before the generation and replacement of the in process finishes, you see the message: *Error 10040 Another web certificate management operation is in progress.*

The certificate is replaced and the web service restarts within one hundred and twenty (120) seconds.
4. Refresh your browser and continue using AGM. You will not need to login to a new session.

18 APPID Pre- and Post-Scripts for Scheduled Data Protection Jobs

You can create application-specific pre-scripts and post-scripts to perform operations on a host before and after a VDP capture operation. APPID scripts must follow these guidelines:

- The script name must begin with `appid.<appid>`. To learn the `appid` for an application, hold the mouse cursor over the application name in the Actifio Desktop.
- On a Windows host, the script location must be: `C:\Program Files\Actifio\scripts`. Scripts run on Windows hosts must be `.bat` or `.vbs` files.
- On a non-Windows host, the script location must be: `/act/scripts`. Scripts run on non-Windows hosts must have execute permissions.

Note: You can use root credentials or a local username/password. Without valid stored credentials, the scripts will fail to execute. The scripts run as root unless the script itself calls something like 'sudo'.

Setting	Description	Default Timeout	Range
Init	The init script is invoked with an <code>init</code> parameter when the backup is about to start.	60 seconds	N/A
Freeze	The freeze script is invoked with a <code>freeze</code> parameter when the backup operation is just about to freeze the application.	60 seconds	1- 86400 seconds
Unfreeze	The thaw script is invoked with a <code>thaw</code> parameter when the backup operation is just finished unreeling the application.	60 seconds	1- 86400 seconds
Finish	The fini script is invoked with a <code>fini</code> parameter when the backup operation is about to complete. This phase is applicable only for the Actifio Connector.	60 seconds	1- 86400 seconds
Abort	The abort script is invoked with an <code>abort</code> parameter if the backup is aborted for any reason.	N/A	N/A

Troubleshooting APPID Scripts

A successfully executed script includes two lines in the UDSAgent.log file:

PrepareForSnapshot: Executing init script

Launched script with arguments [0]=/act/scripts/appid.22448 [1]=init pid 6914

If you only see the first line, that means the script did not execute. The most common reasons are:

- Invalid credentials or no credentials. Validate them by logging in over RDP or using "run-as" from the shell.
- The script may not be readable or executable. Ensure that you can execute the script manually.

Sample APPID Script for Windows

```
@echo off
if /i %1 equ init goto :handle_init
if /i %1 equ fini goto :handle_fini
if /i %1 equ freeze goto :handle_freeze
if /i %1 equ thaw goto :handle_thaw
if /i %1 equ abort goto :handle_abort
echo Unknown command %1
goto :eof
:handle_init
    echo Got an init command
    ping -n 5 google.com
    echo %time% >C:\inittime.txt
    whoami >> C:\inittime.txt
    goto :end
:handle_fini
    echo Got a fini command
    ping -n 5 google.com
    echo %time% >C:\Finishtime.txt
    whoami >> C:\Finishtime.txt
    goto :end
:handle_freeze
    echo Got a freeze command
    ping -n 10 google.com
    echo %time% >C:\pretime.txt
    whoami >> C:\pretime.txt
    goto :end
:handle_thaw
    echo Got a thaw command
    ping -n 5 google.com
    echo %time% >C:\posttime.txt
    whoami >> C:\posttime.txt
    goto :end
:handle_abort
    echo Got an abort command
    ping -n 5 google.com
    echo %time% >C:\aborttime.txt
    whoami >> C:\aborttime.txt
    goto :end
:end
echo Done processing commands
```

Sample APPID Script for Linux

```
#!/bin/sh
if [ $1 = "freeze" ]; then
    echo freeze > /tmp/pretime.txt
    echo $1 >> /tmp/pretime.txt
    sleep 10
    echo date >>/tmp/pretime.txt
    exit 0
fi

if [ $1 = "thaw" ]; then
    echo thaw > /tmp/posttime.txt
    echo $1 >> /tmp/posttime.txt
    sleep 5
    echo date >>/tmp/posttime.txt
    exit 0
fi

if [ $1 = "abort" ]; then
    echo abort > /tmp/aborttime.txt
    echo $1 >> /tmp/aborttime.txt
    sleep 5
    echo date >> /tmp/aborttime.txt
    exit 0
fi

if [ $1 = "init" ]; then
    echo init > /tmp/inittime.txt
    echo $1 >> /tmp/inittime.txt
    sleep 5
    echo date >>/tmp/inittime.txt
    exit 0
fi

if [ $1 = "fini" ]; then
    echo fini > /tmp/finishtime.txt
    echo $1 >> /tmp/finishtime.txt
    sleep 5
    echo date >> /tmp/finishtime.txt
    exit 0
fi
```

19 Super Scripts for Workflows and On-Demand Data Access Jobs

You can develop scripts to be called by the scripting engine during initialization, pre, post, and final phases of backup or restore jobs. Scripts are executed only on hosts on which the Actifio Connector is installed. Individual script names and arguments for each phase can be specified separately. The scripting engine uses environment variables to provide job information to the scripts.

The VDP host-side super scripts are invoked for on-demand jobs that are triggered by the CLI with the **-scripts** argument. Supported CLI jobs are listed in the [CLI Commands Supported in Super Scripts](#) on page 94.

Scripts can be defined and executed for all on demand backup and restore jobs that invoke the host connector.

Note: *Super scripts are not supported for Dedup Async jobs on in-band applications.*

This chapter contains the following topics:

- [Super Script Phases](#) on page 92
- [Super Script Arguments](#) on page 92
- [Super Script Timeouts](#) on page 92
- [Super Script Environment Variables](#) on page 93
- [CLI Commands Supported in Super Scripts](#) on page 94
- [Sample Super Scripts](#) on page 95

Super Script Naming Conventions and Location

A super script can have any valid filename for the OS.

- For Microsoft Windows platforms: Supported interpreters are batch files (cmd.exe) and visual basic scripts. Scripts must be located in the scripts directory under C:\Program Files\Actifio\scripts
- For Linux, AIX, HP-UX, and Solaris platforms: Any installed interpreters must be visible to /bin/sh shell. The script should declare the interpreter by shebang line (e.g. #!/bin/bash). Scripts must be located in the scripts directory under /act/scripts

Super Script Phases

INIT: The early initialization phase. It starts when the Actifio Appliance connects to the Connector, the job is initialized, and the credentials are verified.

PRE: This phase starts just before the major operation of the job. For snapshots and direct-to-Dedup, this starts before the application is frozen. For mount type jobs, this is after devices are mapped to the host but before connector based operations like rescan, import and mounting of file systems is started.

POST: This phase starts immediately after the major operation of the job is completed. For backup type jobs, this is after the application is unfrozen. For mount type jobs, this is after all import/mounting/bringing applications on-line is completed.

FINAL: This phase is end of the job. The operation is essentially complete, however, this script still has the opportunity to return a non-zero code and fail the job.

ABORT: This phase is the abort handling part of the job, when it has failed due to some reason. Any of the script failures are also considered as job failure, hence this phase will be triggered.

Super Script Arguments

A user or administrator can define per-script arguments that are passed to script during invocation. The first argument to the script is always the current phase followed by user-defined arguments.

Example

This example demonstrates a database handler on a Unix platform:

(script: /act/scripts/init.sh with args arg1 & arg2)

```
#!/bin/bash
if [[ $1 != "init" ]];
then
echo "Called outside connector. Exiting..." >>/act/log/scripts.log
exit -1
fi
DB_DIR=$2          # arg1 in this example
if [[ ! -d $DB_DIR ]];
then
echo "Error: DB Directory empty." >>/act/log/scripts.log
echo "Aborting the job..." >>/act/log/scripts.log
fi
# Put the database in read-only mode...
```

Script Returns and Failures

A job-in-progress will be terminated if the script:

- Cannot be executed (e.g. no execute permission or file not found)
- Failed (e.g. interpreter finds a script error and aborts)
- Returns an error code (a non zero value)

If specified, the abort script will be called in the above mentioned scenarios. The failure of an abort script is ignored.

Super Script Timeouts

Each super script may be specified with individual timeout values in seconds. If a script for a given phase runs beyond the timeout, the script is marked as failed and the job-in progress is aborted. The default value is 60 seconds: Example: (script: /act/scripts/init.sh <appid> <argument> timeout = 120)

Refer to the [CLI Commands Supported in Super Scripts](#) on page 94 for CLI usage examples.

Super Script Environment Variables

The Connector portion of an on-demand script is invoked with environment variables set to job-specific values. Not all environment variables are applicable to all jobs. Only the variables applicable to the current jobs are exported to scripts. All environment variables exported by the Connector to the scripts are prefixed with "ACT_".

For example:

Current phase (PHASE) is exported as ACT_PHASE

Current VDP job name (JOBNAME) is exported as ACT_JOBNAME

The following is a list of environment variables with sample values in parentheses.

- ACT_APPID: The database ID of the application (e.g. 4186)
- ACT_APPNAME: Name of the application (e.g. My-DB)
- ACT_HOSTNAME: The name of the host which is the target of this job (e.g. Jupiter)
- ACT_JOBNAME: The name of the job (e.g. Job_0123456)
- ACT_JOBTYPE: a text version of the job class (e.g. mount)
- ACT_LOGSMART_TYPE: db is the only valid value. This must be present for database logs to be captured.
- ACT_MULTI_END: After mount, if True, recover database into open state (default). If False, the database is left in the mounted (Oracle) or restoring (SQL Server) state.
- ACT_MULTI_OPNAME: the name of the operation currently running for a job that consists of multiple operations. Reprovision and Restore jobs involve an unmount operation followed by a mount operation. Operations include:
 - o mount
 - o unmount
 - o refresh
 - o restore
 - o reprovision
 - o scrub-mount
 - o scrub-unmount
 - o migrate
 - o clone
- ACT_OPTIONS: Policy options that apply to this job
- ACT_PHASE: A text string that describes the job phase (e.g. init)
- ACT_POLICY: Name of the policy related to this job (e.g. Daily4Hr)
- ACT_PROFILE: The name of the profile (e.g. Standard)
- ACT_SCRIPT_TMOUT: Superscripting timeout. If response is not received within timeout value (default 60 seconds), then the script will fail.
- ACT_SOURCEHOST: The name of the host that was the source for this application (e.g. Saturn)
- ACT_TEMPLATE: Name of the template related to the job (e.g. Standard)
- ACT_TIMEOUT: Define the duration of the script, how long the script is allowed to run
- ACT_VOLUMES: For generic applications, list of volumes that are configured for backup

CLI Commands Supported in Super Scripts

The following CLI commands are supported for on-demand super scripting:

- `udtask backup`
- `udtask restoreimage`
- `udtask cloneimage`
- `udtask mountimage`
- `udtask mountimage`
- `udtask testfailover`
- `udtask failover`
- `udtask deletetailover`
- `udtask createliveclone`
- `udtask refreshliveclone`
- `udtask prepmount`
- `udtask prepunmount`

With all of these commands, there will be an option to specify scripts to run at four phases of the job:

init: when the job is just started

pre: just before “the main operation” of the job

post: just after “the main operation” of the job

final: towards the very end of the job, but not after it is finished

The script, script parameters, and settings are specified using this CLI syntax:

```
-script  
name=<scriptname>:phase={INIT|PRE|POST|FINAL}[ :timeout=value][ :args=<arg1,arg2>];[ :name=<scrip  
tname>:phase={INIT|PRE|POST|FINAL}...]
```

Note: *The phase names are case-insensitive.*

The script name and phase are required. Timeout and arguments are optional. There are name value pairs, separated by colons. The arguments are a set of values separated by commas. Special characters like colons, spaces and commas are not supported.

A command invocation with a pre script might look like this:

```
udtask backup -app $MYAPP -policy $MYPOLICY \  
-script "name=MYSCRIPT.sh:phase=PRE:timeout=60:args=ARG1,ARG2"
```

Sample Super Scripts

Here are two sample super scripts to illustrate VDP super scripting.

Sample Super Script for Windows

At: \<InstallDir>\scripts

Example: C:\Program Files\Actifio\scripts\wrapper_script.bat

```
echo ..... Running %ACT_PHASE% hook ..... >> c:\act_script.log
echo %time% >> c:\act_script.log
echo Args: %0 %1 %2 >> c:\act_script.log
echo Current phase is %1 >> c:\act_script.log
set >> c:\act_script.log
echo ..... End %ACT_PHASE% hook ..... >> c:\act_script.log
```

Sample Super Script for Linux and other Unix Platforms

For Linux: /act/scripts

Example: /act/scripts/wrapper_script.sh

```
#!/bin/bash

LOG_FILE="/tmp/act_script.log"

# Redirect STDOUT & STDERR to $LOG_FILE file
exec 1<&-
exec 2<&-
exec 1>>$LOG_FILE
exec 2>&1

echo
echo "..... Running $ACT_PHASE hook ....."
printenv | grep "ACT_" |sort
echo "Current time is: `date`"
echo "Running script as `whoami`"
echo "CLI Args are: $0 $*"
echo "..... End $ACT_PHASE hook ....."
echo
```

20 Actifio Event Notifications

An Actifio Appliance generates notifications for hundreds of system events ranging from critical hardware failures to informational network messages. This chapter describes Actifio event notifications, and then the following two chapters list all known event notifications for the CDS, AOS, and Platform components.

Event notifications can be sent as emails and they can also be routed to a trap receiver.

This section describes:

[Types of Actifio Events](#) on page 98

[Example of Automating Corrective Action Based Upon an Event Notification](#) on page 98

[Events that Go from Information or Warning to Error](#) on page 99

[Alert Methods Supported by Actifio Appliances](#) on page 100

Glossary of Event-Related Terms

These terms have specific meanings with regard to event notifications:

Component: Actifio appliance, Actifio Optimized Storage (AOS), and some IBM storage (Platform).

Error: The most serious level of Event Notification, more serious than both Information and Warning.

Error Message: The human-readable explanatory component of an Event Notification.

Event: Any change reported by the system or by some of the resources it relies on, including network and storage.

Event ID: The unique identifier for an Event Notification.

Event Notification: A set of information about a job or other system event that can be communicated via SMTP, SNMP, and in the AGM Events Monitor.

Information: The least serious level of Event Notification severity, less serious than Warning and Error.

MIB: The Management Information Base, a collection of event notification information consumable by a trap receiver via SNMP.

Trap: An event notification received by a trap server over SNMP.

Trap Receiver: A device that receives event notifications via SNMP and responds according to user-configured rules.

Warning: The middle level of Event Notification severity, more serious than Information but not as serious as an Error.

Types of Actifio Events

The Actifio appliance sends notifications for these components of your Actifio System:

CDS system events

CDS system events come from the execution of Actifio copy data management jobs. This includes job failures or delays, missed SLAs, and other events not related to storage or underlying hardware.

CDS system events often include additional detailed information about job IDs, affected hosts or appliances, and more in the Error Message part of the event notification. In addition, if there is more information available from a subsystem, then that is concatenated to the error message.

Some job failure CDS events are initially reported as warnings, and later become errors. If a job fails during a period in which it can be retried, the event is a warning. If the retry attempts fail, the event finally becomes an error.

CDS events are listed in **Actifio Event IDs and Error Codes**, available on ActifioNOW.

AOS Events, Main System Chassis Events, and Platform Events

AOS events are from Actifio Optimized Storage (storage that the Actifio appliance integrates with via IBM APIs). You get these from IBM Storwize V3700, IBM System Storage DS3512, and NetApp E2700 storage arrays. These are documented by IBM in the IBM Knowledge Center at: <https://www.ibm.com/support/knowledgecenter/>.

Main System Chassis events are from the Actifio CDX appliance hardware.

Platform events relate to the physical hardware and network connections on which an Actifio CDS appliance is installed. Platform events come from Actifio CDS appliances only; Sky appliances do not send platform events.

Clearable Events

Some platform and AOS events are clearable. Clearable events that are not cleared trigger repeated event notifications every 25 hours until cleared.

Example of Automating Corrective Action Based Upon an Event Notification

Suppose a snapshot job fails while a datastore is pending consolidation. You see in the System Monitor:

```
Event ID      43901
Error Code    937
Error Message Failing the job since disk consolidation is pending on VM
```

You want to perform the consolidation and resubmit the job right away, unless the datastore is so large that consolidation might impact production hosts. If you are using monitoring software like SolarWinds or Control M, then:

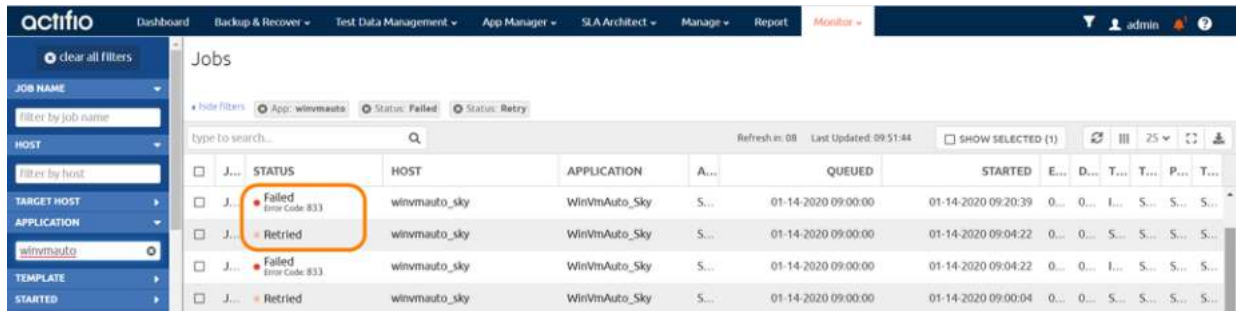
1. The job failure is reported by the Actifio appliance.
2. The monitoring software catches the failure, noting the error code for consolidation required.
3. Then the software makes a vSphere API call `reportsnaps` to query the size of the datastore.
 - o If the datastore is small enough to consolidate without impacting production hosts, the monitoring software sends an Actifio CLI or API call to enable consolidation for that policy and application, then runs the job from the CLI using `udstask mkipolicyoption` and `udstask backup`. The appliance responds with `Success Job_<Job number>`. The job number is captured and tracked. Upon completion of the job the auto consolidate feature is disabled via `udstask rmpolicyoption`.
 - o If the datastore is so large that consolidation might impact production hosts, the monitoring software crafts a ticket for the VMware team to manually consolidate that datastore at a more appropriate time.

Events that Go from Information or Warning to Error

Actifio VDP employs three notification types: **info**, **warning**, and **error**. Some UDP events experience all three error notification types. This is because some jobs may not succeed on their first execution due to an event that is later resolved. For example, a snapshot job may encounter a timeout event of type Warning due to network traffic. If there is still time within the SLA job window, the job may be retried several times; that job gets **Retried** status in the Jobs Monitor.

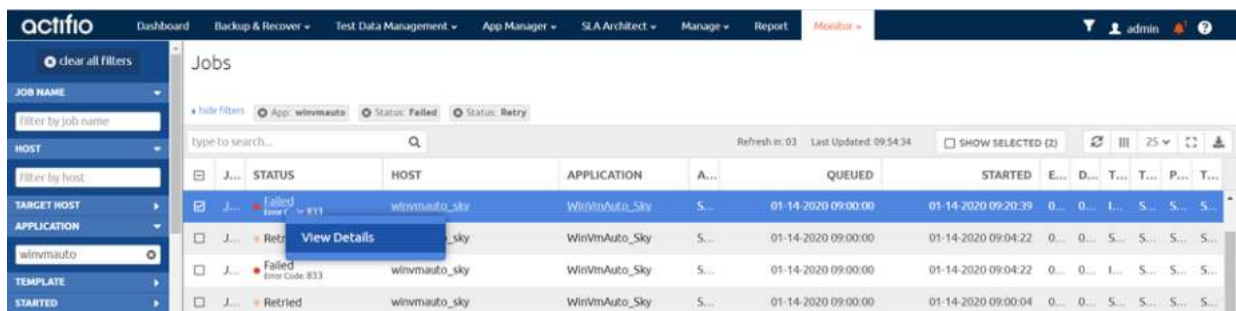
If the job ultimately fails (the SLA time window elapses before success) then that job gets **Failed** status in the System Monitor. At this time, a timeout event of type Error is posted.

For complete information on job statuses, see the AGM online help.



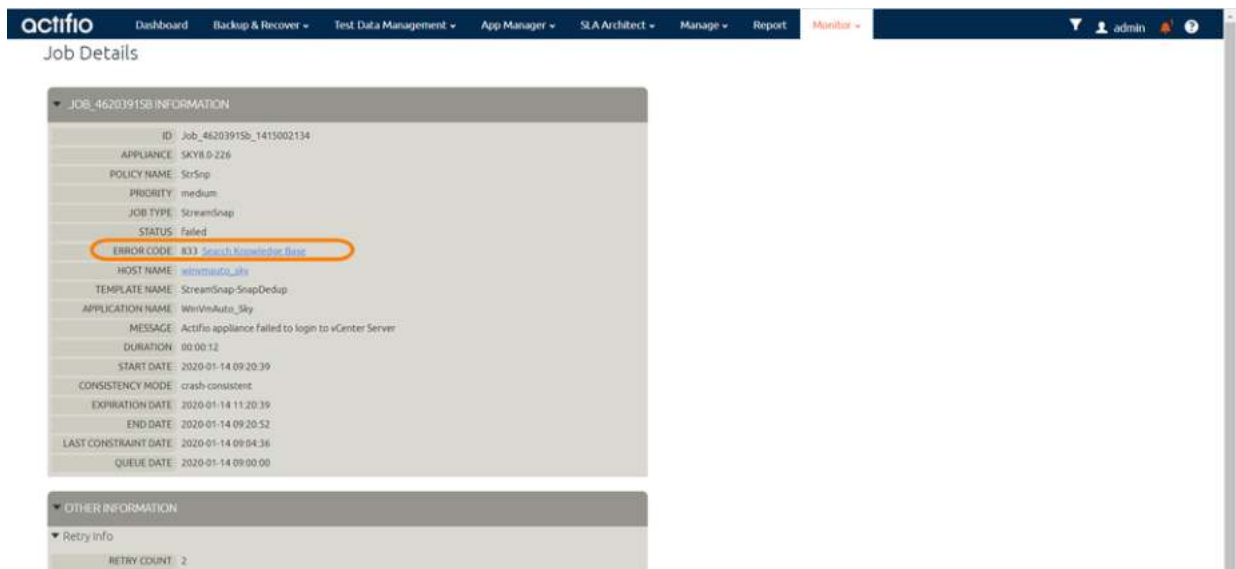
J...	STATUS	HOST	APPLICATION	A...	QUEUED	STARTED	E...	D...	T...	T...	P...	T...
J...	Failed Error Code 833	winvmauto_sky	WinVmAuto_Sky	S...	01-14-2020 09:00:00	01-14-2020 09:20:39	0...	0...	I...	S...	S...	S...
J...	Retried	winvmauto_sky	WinVmAuto_Sky	S...	01-14-2020 09:00:00	01-14-2020 09:04:22	0...	0...	S...	S...	S...	S...
J...	Failed Error Code 833	winvmauto_sky	WinVmAuto_Sky	S...	01-14-2020 09:00:00	01-14-2020 09:04:22	0...	0...	I...	S...	S...	S...
J...	Retried	winvmauto_sky	WinVmAuto_Sky	S...	01-14-2020 09:00:00	01-14-2020 09:00:04	0...	0...	S...	S...	S...	S...

This Job was Retried Until it Failed



J...	STATUS	HOST	APPLICATION	A...	QUEUED	STARTED	E...	D...	T...	T...	P...	T...
J...	Failed Error Code 833	winvmauto_sky	WinVmAuto_Sky	S...	01-14-2020 09:00:00	01-14-2020 09:20:39	0...	0...	I...	S...	S...	S...
J...	Retried	winvmauto_sky	WinVmAuto_Sky	S...	01-14-2020 09:00:00	01-14-2020 09:04:22	0...	0...	S...	S...	S...	S...
J...	Failed Error Code 833	winvmauto_sky	WinVmAuto_Sky	S...	01-14-2020 09:00:00	01-14-2020 09:04:22	0...	0...	I...	S...	S...	S...
J...	Retried	winvmauto_sky	WinVmAuto_Sky	S...	01-14-2020 09:00:00	01-14-2020 09:00:04	0...	0...	S...	S...	S...	S...

Right-Click to View Job Details



Job Details

JOB_46203915b INFORMATION

- ID: Job_46203915b_1415002134
- APPLIANCE: SKY18-D-226
- POLICY NAME: StrSnap
- PRIORITY: medium
- JOB TYPE: StreamSnap
- STATUS: Failed
- ERROR CODE: 833 [Search Knowledge Base](#)
- HOST NAME: winvmauto_sky
- TEMPLATE NAME: StreamSnap-SnapDedup
- APPLICATION NAME: WinVmAuto_Sky
- MESSAGE: Actifio appliance failed to login to vCenter Server
- DURATION: 00:00:12
- START DATE: 2020-01-14 09:20:39
- CONSISTENCY MODE: crash-consistent
- EXPIRATION DATE: 2020-01-14 11:20:39
- END DATE: 2020-01-14 09:20:52
- LAST CONSTRAINT DATE: 2020-01-14 09:04:36
- QUEUE DATE: 2020-01-14 09:00:00

OTHER INFORMATION

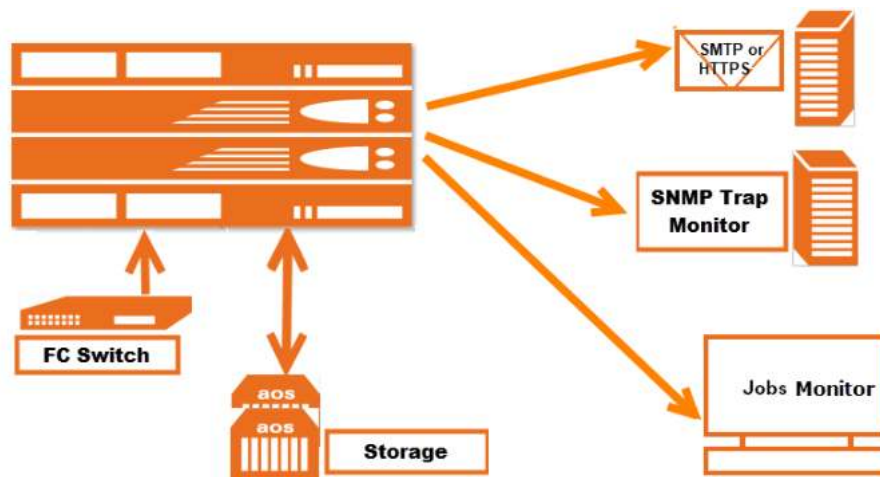
- Retry info
- RETRY COUNT: 2

Job Details, with a Link to the Actifio Knowledge Base

Alert Methods Supported by Actifio Appliances

The Actifio appliance actively monitors event notifications. Specifically:

- You can monitor job successes and failures directly in the System Monitor as described in [Chapter 21, Monitoring Alerts in the AGM Events Monitor](#).
- You can send event notifications from Actifio appliances by email or HTTPS as described in [Chapter 22, Sending Alerts from an Actifio Appliance by Email](#).
- You can send event notifications as SNMP traps from Actifio appliances to a trap receiver. This is detailed in [Chapter 23, Sending Traps from the Actifio Appliance to a Trap Receiver](#).
- You can collect alerts from some storage and switches onto the Actifio appliance, as detailed in [Chapter 24, Collecting Alerts from Storage and Switches \(CDS only\)](#)



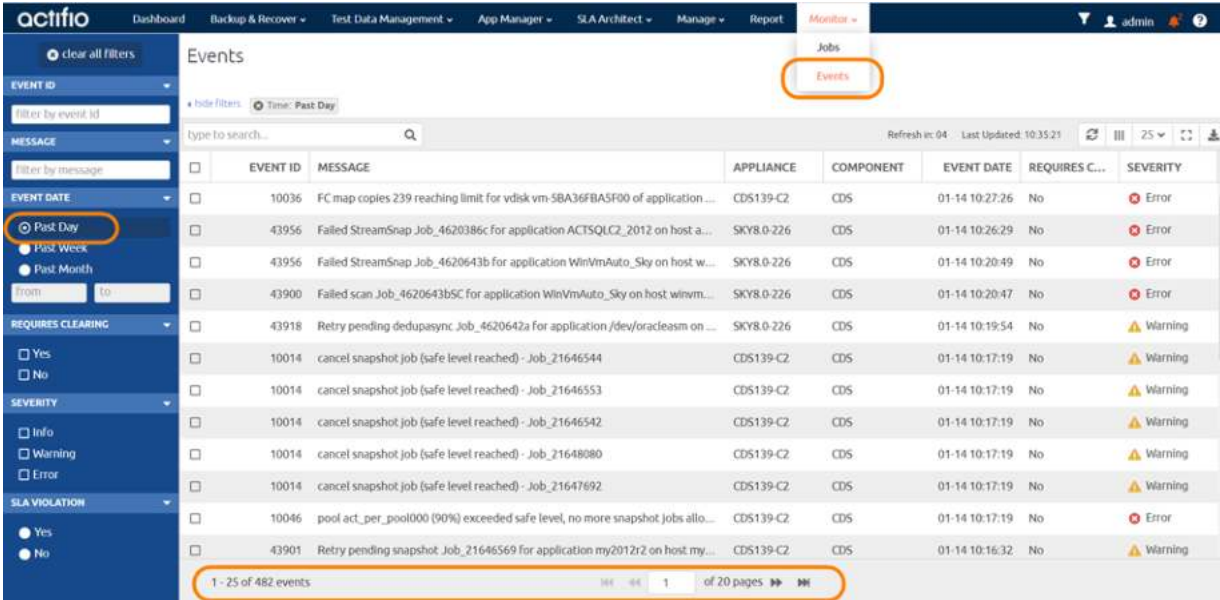
Overview of Alert Options

21 Monitoring Alerts in the AGM Events Monitor

You can learn about the context of an event in the Events Monitor. Events are information/warning/error notifications raised by an Actifio appliance. You can view events in the Events Monitor by:

- Viewing events based on date or severity
- Filtering events based on columns displayed in the Events window

See the AGM online help for details.



The screenshot shows the Actifio Events Monitor interface. The top navigation bar includes 'actifio', 'Dashboard', 'Backup & Recover', 'Test Data Management', 'App Manager', 'SLA Architect', 'Manage', 'Report', and 'Monitor'. The 'Monitor' tab is active, and the 'Events' sub-tab is selected. The left sidebar contains filter options for 'EVENT ID', 'MESSAGE', 'EVENT DATE', 'REQUIRES CLEARING', 'SEVERITY', and 'SLA VIOLATION'. The 'EVENT DATE' filter is set to 'Past Day'. The main area displays a table of events with columns: EVENT ID, MESSAGE, APPLIANCE, COMPONENT, EVENT DATE, REQUIRES C..., and SEVERITY. The table shows 25 events, with the first row highlighted. The bottom of the table indicates '1 - 25 of 482 events' and '1 of 20 pages'.

EVENT ID	MESSAGE	APPLIANCE	COMPONENT	EVENT DATE	REQUIRES C...	SEVERITY
10036	FC map copies 239 reaching limit for vdisk vm-5BA36F8A5F00 of application ...	CDS139-C2	CDS	01-14 10:27:26	No	Error
43956	Failed StreamSnap_Job_4620386c for application ACTSQLC2_2012 on host a...	SKY8.0-226	CDS	01-14 10:26:29	No	Error
43956	Failed StreamSnap_Job_4620643b for application WinVmAuto_Sky on host w...	SKY8.0-226	CDS	01-14 10:20:49	No	Error
43900	Failed scan_Job_4620643b5C for application WinVmAuto_Sky on host winvm...	SKY8.0-226	CDS	01-14 10:20:47	No	Error
43918	Retry pending dedupasync_Job_4620642a for application /dev/oracleasm on ...	SKY8.0-226	CDS	01-14 10:19:54	No	Warning
10014	cancel snapshot job (safe level reached) - Job_21646544	CDS139-C2	CDS	01-14 10:17:19	No	Warning
10014	cancel snapshot job (safe level reached) - Job_21646553	CDS139-C2	CDS	01-14 10:17:19	No	Warning
10014	cancel snapshot job (safe level reached) - Job_21646542	CDS139-C2	CDS	01-14 10:17:19	No	Warning
10014	cancel snapshot job (safe level reached) - Job_21648080	CDS139-C2	CDS	01-14 10:17:19	No	Warning
10014	cancel snapshot job (safe level reached) - Job_21647692	CDS139-C2	CDS	01-14 10:17:19	No	Warning
10046	pool act_per_pool000 (90%) exceeded safe level, no more snapshot jobs allo...	CDS139-C2	CDS	01-14 10:17:19	No	Error
43901	Retry pending snapshot_Job_21646569 for application my2012r2 on host my...	CDS139-C2	CDS	01-14 10:16:32	No	Warning

Viewing All Events of the Past 24 Hours

Right-click the event to select **View Details** of a selected event. To interpret the information in the event, see [Interpreting Event Details in the Events Monitor](#) on page 102.

Interpreting Event Details in the Events Monitor

Item	Meaning
ID	Error sequence number.
Event ID	Event identifier. CDS events are listed in Actifio Event IDs and Error Codes .
Appliance Name	The name of the Actifio appliance that processed the job.
Component	CDS, AOS, or Platform, described in Types of Actifio Events on page 98.
Application Name	The name of the application as it appears in the App Manager.
Application Type	The type of application in the App Manager.
Job Name	The job name as it appears in the System Monitor Jobs tab.
Error Code	Event identifier. Error codes are listed in Actifio Event IDs and Error Codes .
Error Message	Descriptive text, often with an additional error message appended to it.
Requires Clearing	Some events are clearable. Clearable events that are not cleared trigger repeated event notifications every 25 hours until cleared.
Event Date	A timestamp for the event.
Object Type and Object ID	The CDS/Sky component that encountered the event: 1. PSRV 2. UDP 3. OMD 4. Dedup
Notification Type	Severity: information, warning, or error.

Note: Not all fields are shown for all events. A field is shown only if it is relevant to the event.

An Event in the Events Monitor: ERROR MESSAGE includes both the Event 43918 “Failed dedupasync <job> for <app> on <host>” and specific Error Code 15 “Could not connect to backup host”

22 Configuring the Call Home Feature

You can configure notifications to be sent to Actifio Support via email or HTTPS when an event of severity *warning* or *error* is raised by the Actifio appliance. Call Home is disabled by default on all Actifio Appliances. You enable Call Home on individual appliances.

This chapter details:

[Sending Alerts from an Actifio Appliance by HTTPS](#) on page 103

[Sending Alerts from an Actifio Appliance by Email](#) on page 105

[Interpreting Notifications](#) on page 108

```
Cluster Id: 590029521144
Cluster Name: BedewadaCDS
CDS IP Address: 198.188.16.81
Customer: UNKNOWN
Hostname: Bedewada
```

```
date      component type eventid appname  apptype  jobname message
-----
2017-03-21 02:54:12 CDS error 43901 check Oracle Job_0111009 Failed snapshot Job_0111009 for application check on host linux_raju_ora, Error: 15: 15:
Could not connect to backup host. Make sure Connector is running on linux_raju_ora(192.168.18.155:5106) and network port 5106 is open.
```

Example Notification

Sending Alerts from an Actifio Appliance by HTTPS

To enable Call Home via HTTPS on an Actifio Appliance:

1. Open the AGM to the Manage, Appliances list. Right-click the appliance to configure and select **Configure Appliance**.

NAME	APPLIANCE ID	CONNECTIVITY STATUS	IP	LAST SYNCHRONIZED	VERSION	CALL HOME STATUS
arepsky9	1415719549	●	172.27.34.96	2020-04-06 10:48:11	9.0 (9.0.6.15R2)	MAIL
caf-source	145866	●	172.17.206.77	2020-04-03 18:33:51	10.0 (10.0.0.696)	Disabled
sky10sp1	145507	●	172.17.205.90	2020-04-06 10:48:12	10.0 (10.0.1.3027)	Disabled
sky905	144923	●	172.17.202.11	2020-04-03 18:35:31	9.0 (9.0.5.72)	Disabled

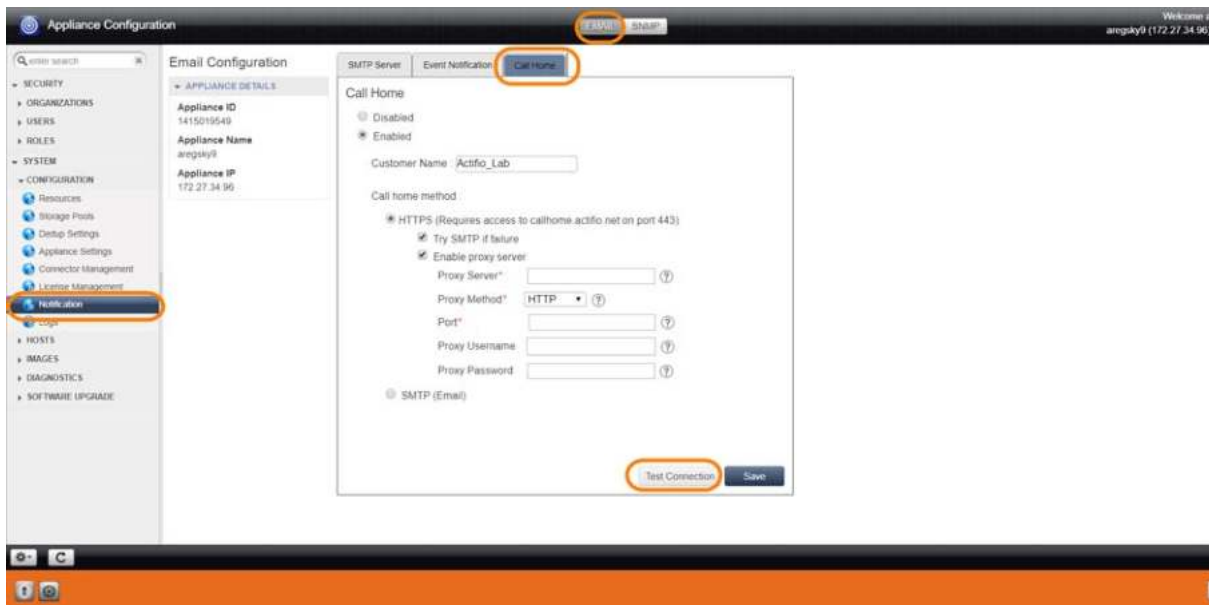
Configuring the Appliance for Call Home

2. Log into the Appliance Configuration page, to **System > Configuration > Notification**. Select the **Email** tab and the **Call Home** subtab. Call Home is disabled by default.



Enabling Call Home

3. Select **Enabled**, and under Call Home Method select **HTTPS**.



Configuring Call Home to Use HTTPS

Options:

- o **Try SMTP if failure:** If this is set, then if the HTTPS communication fails, the appliance will try to send an email notification instead. This must be configured; see [Sending Alerts from an Actifio Appliance by Email](#) on page 105
 - o **Enable proxy server:** Fill in the necessary HTTP or SOCKS5 proxy server information, including credentials if your proxy server requires them.
4. Click **Test Connection** to verify the connection.
 5. Click **Save**.
 6. Repeat for any other Actifio Appliances that you want to send notifications.

Sending Alerts from an Actifio Appliance by Email

You can configure notifications to be sent to Actifio Support or to anyone via email when an event of severity *warning* or *error* is raised by the Actifio appliance. This involves:

[Configuring an Actifio Appliance to Communicate with an SMTP Server](#) on page 105

[Setting Up Automatic Emails of Events](#) on page 106

```
Cluster Id: 590029521144
Cluster Name: BedewadaCDS
CDS IP Address: 198.188.16.81
Customer: UNKNOWN
Hostname: Bedewada
```

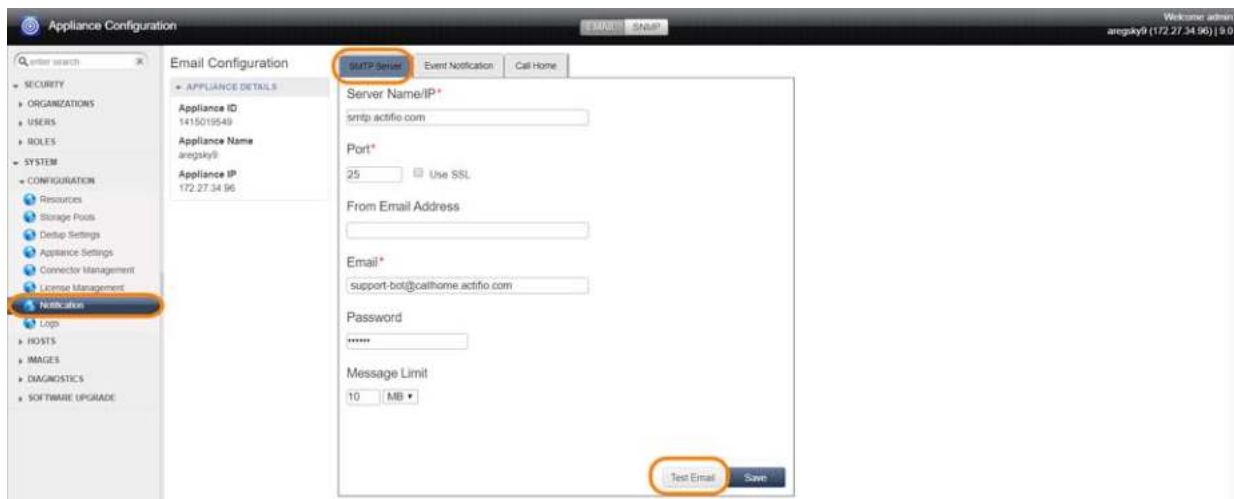
```
date      component type eventid appname  apptype  jobname message
=====
2017-03-21 02:54:12 CDS error 43901 check Oracle Job_0111009 Failed snapshot Job_0111009 for application check on host linux_raj_u_ora, Error: 15: 15:
Could not connect to backup host. Make sure Connector is running on linux_raj_u_ora(192.168.18.155:5106) and network port 5106 is open.
```

Example Emailed Notification

Configuring an Actifio Appliance to Communicate with an SMTP Server

To configure an Actifio Appliance to communicate with an email server:

1. In AGM, under Manage, Appliances, right-click the appliance and select **Configure Appliance**.
2. Under System > Configuration > Notification, select the **EMAIL** tab and the **SMTP Server** subtab.
3. Enter the SMTP server name or IP address (IPv4) in **Server Name/IP**.
4. Enter the SMTP or SMTPS port number in **Port**. Select **Use SSL** to send emails securely using SSL.
5. (Optional) Enter a **From Email Address**. This entry is the address that will appear in the From field of each email. Use your company name for better support from Actifio Call Home.
6. At **Email**, enter **support-bot@callhome.actifio.com** for support from Actifio Call Home.
7. Enter a mail server password.
8. Enter the maximum size of the email to be sent in **Message Limit**. When an email exceeds this size, the attachment is split into two or more 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**.



SMTP Server Settings

After the email server has been configured, you can configure automated emails for events as described in [Setting Up Automatic Emails of Events](#) on page 106.

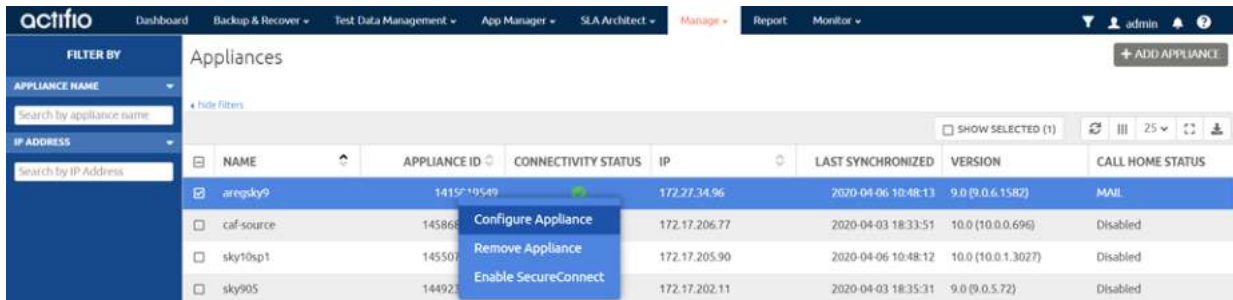
Setting Up Automatic Emails of Events

Before configuring the levels of events that trigger email notifications or the addresses to receive the emails, you must configure an email server as described in [Configuring an Actifio Appliance to Communicate with an SMTP Server](#) on page 105.

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.

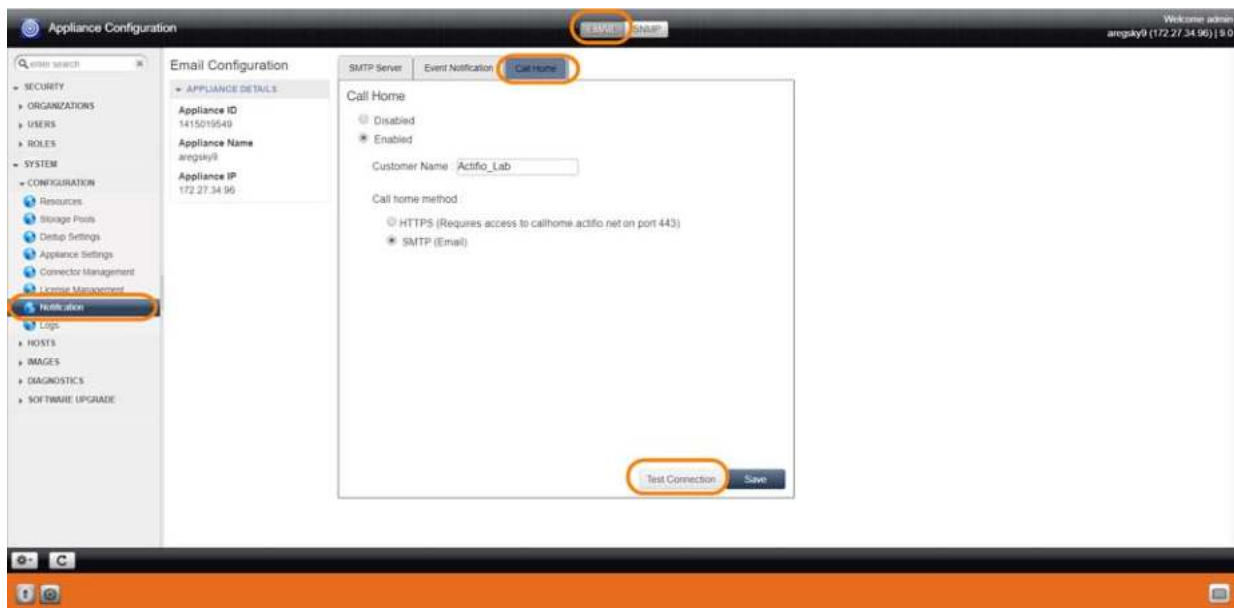
To enable Call Home on an Actifio Appliance:

1. Open the AGM to the Manage, Appliances list. Right-click the appliance to configure and select **Configure Appliance**.



Configuring the Appliance for Call Home

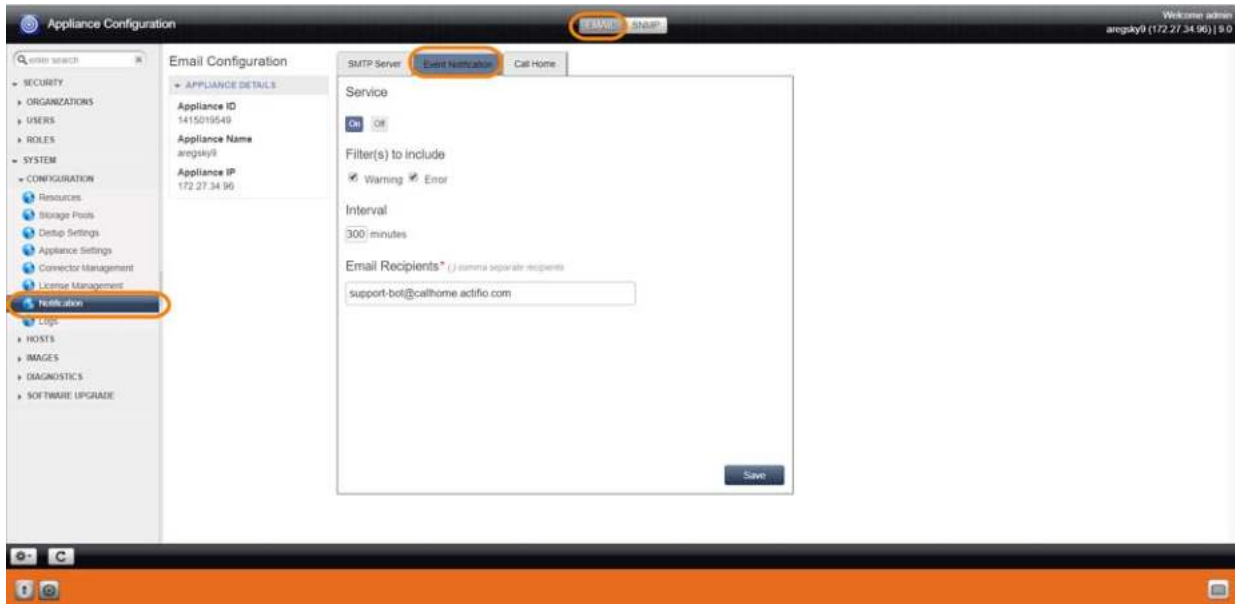
2. Log into the Appliance Configuration page, to **System > Configuration > Notification**. Select the **Email** tab and the **Call Home** subtab. Call Home is disabled by default.



Configuring Event Notifications via Email

3. Select **Enabled** and under Call Home Method, select **SMTP**.
4. Click **Test Connection** to verify the connection.
5. Click **Save**.
6. Next, select the severity level of notifications to send. Select the **Event Notification** subtab.

7. 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**.
8. 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.
9. In **Email Recipients**, enter a comma separated list of email addresses of persons who are to receive email notifications. If Call Home is enabled, then support-bot@callhome.actifio.com is included by default.



Configuring Event Severity for Notifications via Email

10. Click **Save**.
11. Repeat for any other Actifio Appliances that you want to send notifications.

Interpreting Notifications

Table 1: Elements of an Event Notification

Item	Meaning
Cluster Id	A unique identifier of the Actifio appliance that processed the job.
Cluster Name	The name of the Actifio appliance that processed the job.
CDS IP Address	The IP address of a Sky appliance, or the cluster IP address of a CDS appliance.
Customer	The name of the customer site where the event occurred, used by service providers.
Hostname	The host name of the host where the event originated.
date	A timestamp for the event.
component	CDS, AOS, or Platform, described in Types of Actifio Events on page 98.
type	Notification severity: error, warning, or information
eventid	Event identifier. Events are listed in Actifio Event IDs and Error Codes , available on ActifioNOW.
appname	The name of the application as it appears in the Application Manager.
apptype	The type of application in the Application Manager.
jobname	The job name as it appears in the System Monitor Jobs tab.
message	Error Message text, sometimes with an additional error message appended to it.

Cluster Id: 590029521144
 Cluster Name: BedewadaCDS
 CDS IP Address: 198.188.16.81
 Customer: UNKNOWN
 Hostname: Bedewada

```

date      component type eventid appname  apptype  jobname message
=====
2017-03-21 02:54:12  CDS  error  43901      check  Oracle Job_0111009 Failed snapshot Job_0111009 for application check on host linux_raju_oracle, Error
Could not connect to backup host. Make sure Connector is running on linux_raju_oracle(192.168.18.155:5106) and network port 5106 is open.
  
```

A Sample Emailed Event

23 Sending Traps from the Actifio Appliance to a Trap Receiver

This section includes:

[Configuring an Actifio Appliance to Forward Traps to a Trap Receiver](#) on page 109

[Configuring the SNMP Agent to Support SNMP GET Operations](#) on page 111

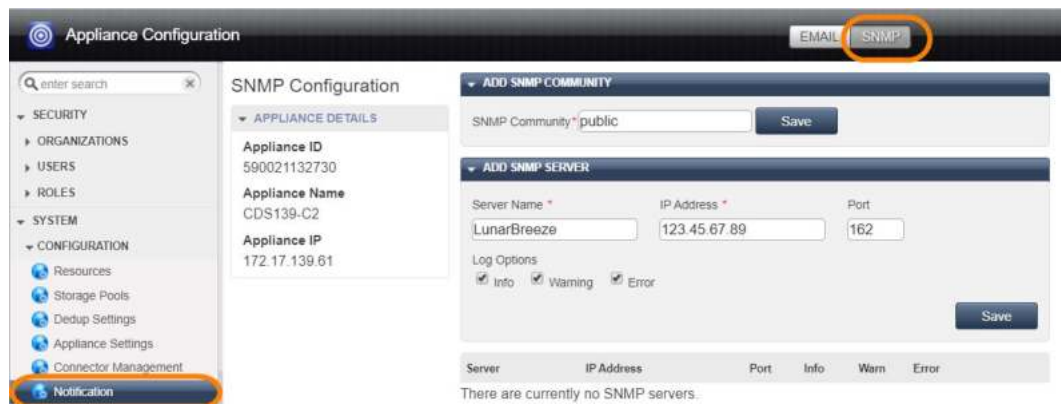
[Using the Actifio MIB](#) on page 113

[Interpreting Traps](#) on page 115

Configuring an Actifio Appliance to Forward Traps to a Trap Receiver

The Actifio appliance supports sending SNMP traps to a SNMP trap receiver. The Actifio trap handler (receiver and forwarder) uses SNMP4J. It runs within the Actifio "psrv" process, the status of which can be displayed by running "Monit Summary" at the command line of the primary node. It supports SNMPv1 and SNMPv2. To add an SNMP trap receiver:

1. In AGM, at Manage, select Appliances. Right-click an appliance and select **Configure Appliance**.
2. Under System > Configuration > Notification, select the **SNMP** tab to see the SNMP Configuration.
3. Enter the SNMP trap receiver name in **Server Name**. To send the traps to an SNMP trap receiver that server requires a different community string, you can set the string as shown in [Setting the Community String for Forwarding Traps to a non-Actifio SNMP Trap Receiver](#) on page 110.
4. Enter the IP address of the 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. Traps are sent over UDP and not by TCP/IP.
6. Select the type of traps to forward: Info, Warning, and Error. Error is the most serious level of event. The Actifio appliance MIB will send these traps to the SNMP trap receiver. Click **Save**.



Adding an SNMP Trap Receiver

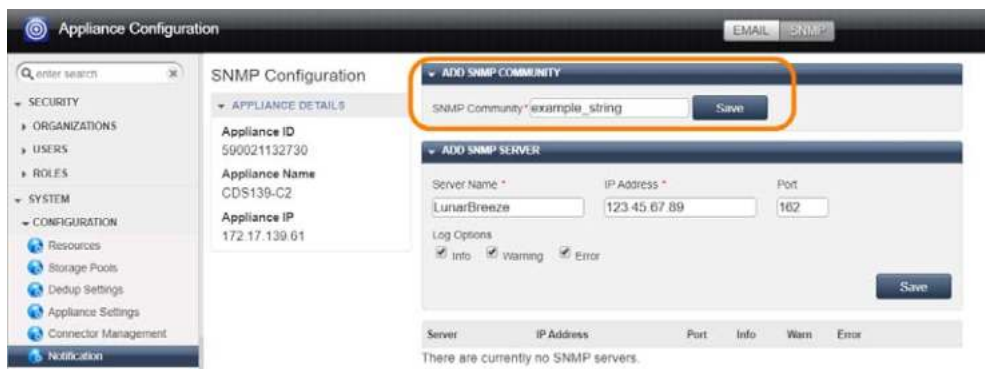
You can add multiple trap receivers and you can specify different types of events to be sent to each. The Actifio MIB is available from the Actifio Resource Center to help analyze these traps. See [Accessing the Actifio MIB](#) on page 112.

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. In AGM, at Manage, select Appliances. Right-click an appliance and select **Configure Appliance**.
2. Under System > Configuration > Notification, select the **SNMP** tab to see the SNMP Configuration.
3. Enter the SNMP community string in **SNMP Community**.
4. Click **Save**.



Configuring SNMP Community String

Configuring the SNMP Agent to Support SNMP GET Operations

If you are using an SNMP-based monitoring and management system 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.

Introduction to SNMP GET Operations

Note: Actifio appliances do not support SNMP SET operations.

The Actifio SNMP Agent

Actifio appliances extend SNMPv2 support to the SNMP GET request process through the activation of an SNMP agent (a wrapper over the SNMP4j Agent) in the Actifio appliance to register all corresponding Actifio MIB classes to support the PULL/GET mechanism. The management system (the client) “pulls” data from the SNMP agent in the Actifio appliance.

The Actifio SNMP agent runs on an Actifio appliance as part of the PSRV service on port UDP-161. It serves all requests sent by any SNMP client or management system to monitor and manage Actifio appliance configurations, system statistics and performance, and so on. The SNMP agent integrates monitoring and management extensions into the Actifio appliance, and uses SNMPv2 GET requests to allow data to be pulled on-demand. You can integrate the SNMP GET operations with your existing management system.

Actifio SNMP GET Request

An SNMP GET request reads the value of SNMP objects and performs network monitoring through a set of predefined Object Identifiers (OIDs). OIDs uniquely identify managed objects in the MIB hierarchy. By using the Actifio MIB, SNMP GET pulls information to monitor Actifio appliance configurations, system statistics, and performance.

To activate the SNMP agent in an Actifio appliance to support SNMP GET requests from an external management system, see [Activating the SNMP Agent in an Actifio Appliance](#) on page 111.

The Actifio MIB

The Actifio MIB file includes all of the object identifiers, notification types, object types, and notification groups used by the Actifio appliance. The Actifio MIB is available for download from the Actifio Resource Center. For more, see [Accessing the Actifio MIB](#) on page 112.

This section includes:

[Activating the SNMP Agent in an Actifio Appliance](#) on page 111

[Supported CLI Commands and their Mapped OIDs for SNMP GET Requests](#) on page 113

[System MIB Variables](#) on page 114

Activating the SNMP Agent in an Actifio Appliance

Use the **udstask configsnmpagent** CLI command to enable the SNMP agent in an Actifio appliance and, optionally to specify a community string for SNMP authentication by the SNMP agent and the management system.

Here is the syntax for the **udstask configsnmpagent** command.

```
>>- udstask -- -- configsnmpagent -- ----->
>--+-----+-----+--+-----+-----+><
  '- -communitystring -- key -'      '- -enable --+ true --+-- -'
                                     +- false -+
```

Table 1: configsnmpagent Parameters

Parameter	Description
<code>-enable true false</code>	Optional. This value enables or disables the SNMP agent. Supported settings are: <ul style="list-style-type: none"> true: Enables the SNMP agent in the Actifio appliance false: Disables the SNMP agent in the Actifio appliance
<code>-communitystring key</code>	Optional. Sets the SNMPV2 community string for performing SNMP GET requests by the Actifio appliance. Enter an authentication pass phrase for connecting to the SNMP agent as the <i>key</i> .

To enable the SNMP agent and specify `Test_password_1` as the community string to connect to the SNMP agent:

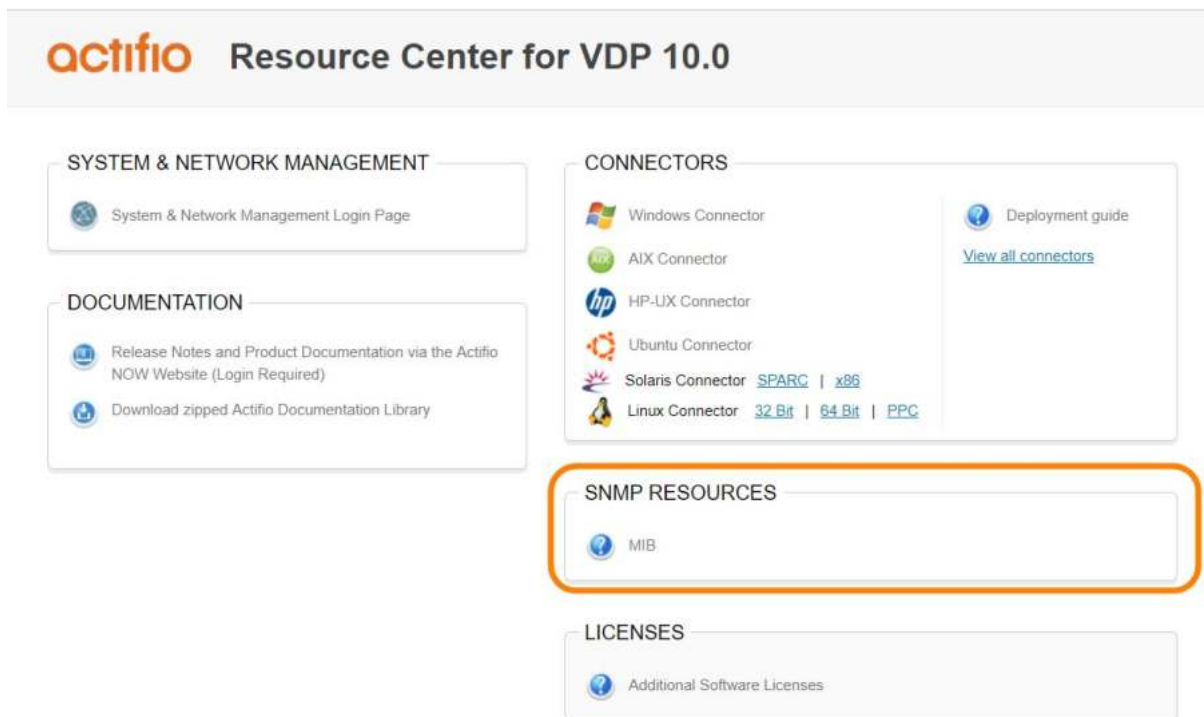
```
$ udstask configsnmpagent -communitystring Test_password_1 -enable true
```

Accessing the Actifio MIB

An SNMP trap receiver can listen to the SNMP traps that are being sent by an Actifio appliance in the network. 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 to your SNMP trap receiver. The Actifio MIB file includes all object identifiers, notification types, object types, and notification groups used by the Actifio appliance.

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

1. Open a web browser to **`http://<Actifio_appliance_IP_address>`**.
2. The Actifio Resource Center page opens. Right-click the MIB link under SNMP Resources and save the MIB file to a convenient location.



The Actifio Resource Center at `http://<Appliance IP Address>`

Using the Actifio MIB

Supported CLI Commands and their Mapped OIDs for SNMP GET Requests

This table lists the mapped OID assignments for each of the supported udsinfo and usvcinfo CLI commands:

This section lists the **udsinfo** and **usvcinfo** CLI commands supported for SNMP GET requests:

Table 2: Mapped OIDs

Actifio Base OID	1.3.6.1.4.1.35795	
Traps OID	1.3.6.1.4.1.35795	.1
CDS OID	1.3.6.1.4.1.35795	.2
USVCINFO commands	1.3.6.1.4.1.35795	.2.1
UDSINFO commands	1.3.6.1.4.1.35795	.2.2

Table 3: udsinfo and usvcinfo CLI Commands and their Mapped OIDs

Command	OID Assignment
usvcinfo lssystemstats	1.3.6.1.4.1.35795.2.1.1
udsinfo lsversion	1.3.6.1.4.1.35795.2.2.2
udsinfo lscluster	1.3.6.1.4.1.35795.2.2.3
udsinfo lssnmpevent	1.3.6.1.4.1.35795.2.2.4
udsinfo lssnmconfig	1.3.6.1.4.1.35795.2.2.5
udsinfo lsdiskpoolstat	1.3.6.1.4.1.35795.2.2.6
udsinfo lspolicy	1.3.6.1.4.1.35795.2.2.7
udsinfo lsavailableconnector	1.3.6.1.4.1.35795.2.2.8
udsinfo lsuser	1.3.6.1.4.1.35795.2.2.9
udsinfo lsjob	1.3.6.1.4.1.35795.2.2.10
udsinfo getsysteminfo	1.3.6.1.4.1.35795.2.2.11
udsinfo lsdiskpool	1.3.6.1.4.1.35795.2.2.12

System MIB Variables

This section lists the System MIB variables and their mapped OIDs:

Table 4: System MIB variables and Their Mapped OIDs

System MIB variable	Set By	mapped OIDs
sysDescr	SNMP Agent	1.3.6.1.2.1.1.1
sysObjectID	SNMP Agent	1.3.6.1.2.1.1.2
sysUpTime	SNMP Agent	1.3.6.1.2.1.1.3
sysContact	User, via setparameter	1.3.6.1.2.1.1.4
sysName	SNMP Agent	1.3.6.1.2.1.1.5
sysLocation	User, via setparameter	1.3.6.1.2.1.1.6
sysServices	SNMP Agent	1.3.6.1.2.1.1.7
sysORLastChange	SNMP Agent	1.3.6.1.2.1.1.8

Note: The SysUptime value is the time since the SNMP agent was started.

Setting System Variables with setparameter

Values for sysDescr, sysName, sysObjectID and sysUptime system OIDs are defined by the SNMP agent. You define the system parameter values for the sysContact and sysLocation OIDs in the SNMP agent using the **setparameter** command.

- Set the sysContact OID value using the **systemcontact** parameter.
- Set the sysLocation OID value using the **systemlocation** parameter.

For example:

```
$ udstask setparameter -param systemcontact -value admin
$ udstask setparameter -param systemlocation -value Boston
```

Limiting the Number of Records Sent by the SNMP Agent with setparameter

You can use the **setparameter** CLI command to limit the number of records sent by the SNMP agent in the Actifio appliance to the management system (the client). When you set the **snmptablesizesize** parameter, the SNMP agent retrieves only the specified number of records and send those records to the respective SNMP clients. The range is 100 to 5000 records (default of 500).

To configure the SNMP agent to retrieve only 400 records and send those records to the SNMP client:

```
$ udstask setparameter -param snmptablesizesize -value 400
```

See the **Actifio CLI Reference** in the Actifio Documentation Library for details on CLI commands and parameters.

Interpreting Traps

Table 5: Contents of a CDS Trap Event

Term	OID 1.3.6.1.4.1.35795.x	Description
Error ID	1.4.1.0	Event identifier. CDS events are listed in Actifio Event IDs and Error Codes , available on ActifioNOW.
Error Code	1.4.2.0	Error code. Error codes are listed in Actifio Event IDs and Error Codes , available on ActifioNOW.
Cluster Name	1.4.3.0	The Actifio appliance that processed the job.
Error Sequence Number	1.4.4.0	Error sequence number.
Timestamp	1.4.5.0	Timestamp for the event: Day Mon dd hh:mm:ss yyyy
Object Type	1.4.6.0	The object type that encountered the event:
Object Id	1.4.7.0	1. PSRV 2. UDP 3. OMD 4. Dedup 5. NetApp 6. NetApp Connector 7.
Application name	1.4.8.0	The name of the application in the Application Manager.
Application Type	1.4.9.0	The type of application in the Application Manager.
Job name	1.4.10.0	The job name in the System Monitor Jobs tab.

Trap Details

Community: public

Ip Address: 192.168.16.40

Request ID: 947349539

Error Index: 0

Error Status: 0

Trap Type: SNMPv2c

Variable Bindings

OID	Type	Value
1.3.6.1.2.1.1.3.0	TimeTick	0 days 00h:00m:00.00s
1.3.6.1.6.3.1.1.4.1.0	OID	1.3.6.1.4.1.35795.1.1
1.3.6.1.4.1.35795.1.4.1.0	String	Error ID = 43901 : Failed snapshot Job_0123209 for ap...
1.3.6.1.4.1.35795.1.4.2.0	String	Error Code = 15
1.3.6.1.4.1.35795.1.4.3.0	String	Cluster Name = BezawadaCDS
1.3.6.1.4.1.35795.1.4.4.0	String	Error Sequence Number = 0
1.3.6.1.4.1.35795.1.4.5.0	String	Timestamp = Wed Apr 05 02:28:50 2017
1.3.6.1.4.1.35795.1.4.6.0	String	Object Type = udp
1.3.6.1.4.1.35795.1.4.7.0	String	Object Id = 4

Close Show Raw << prev next >>

A Sample Event in the Events Monitor

24 Collecting Alerts from Storage and Switches (CDS only)

You can configure your Actifio CDS appliance to collect AOS event notifications from storage arrays and platform events from Fibre Channel switches. The Actifio CDS appliance can collect alerts in two ways:

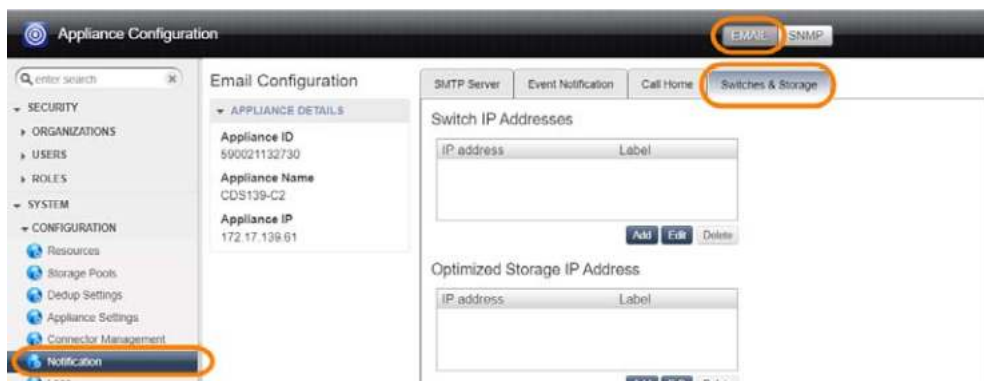
Polling Storage Arrays: Actifio CDS appliances can actively poll some storage arrays. See [Polling Alerts from IBM V3700, IBM DS 3512, and NetApp E2700 Storage Arrays](#) on page 117.

Receiving Forwarded Alerts from Switches: You can configure an IBM System Storage SAN24B-4 Express Fibre Channel Switch to forward alerts to the Actifio CDS appliance. See [Forwarding Alerts from an IBM System Storage SAN24B-4 Express Switch to an Actifio CDS Appliance](#) on page 118.

Polling Alerts from IBM V3700, IBM DS 3512, and NetApp E2700 Storage Arrays

To monitor SNMP notifications generated by attached storage systems and switches known to the Actifio appliance, configure them in the Switches & Storage subtab. To configure the storage and switches:

1. In AGM, at Manage, select Appliances. Right-click an appliance and select **Configure Appliance**.
2. Under System > Configuration > Notification, select the **EMAIL** tab and the **Switches & Storage** subtab. This subtab is absent on Sky appliances.
3. Provide the IP address details in the **Switch IP Addresses** box:
 - o Click **Add** to open the IP Address dialog. Enter a label and switch address and click **Save**.
 - o Repeat to add the second Fibre Channel switch.
4. Repeat the process in the **Optimized Storage IP Address** box, adding two storage arrays and another ping address. You can use **Edit** to modify and **Delete** to remove an existing IP address.
5. Click **Save**.

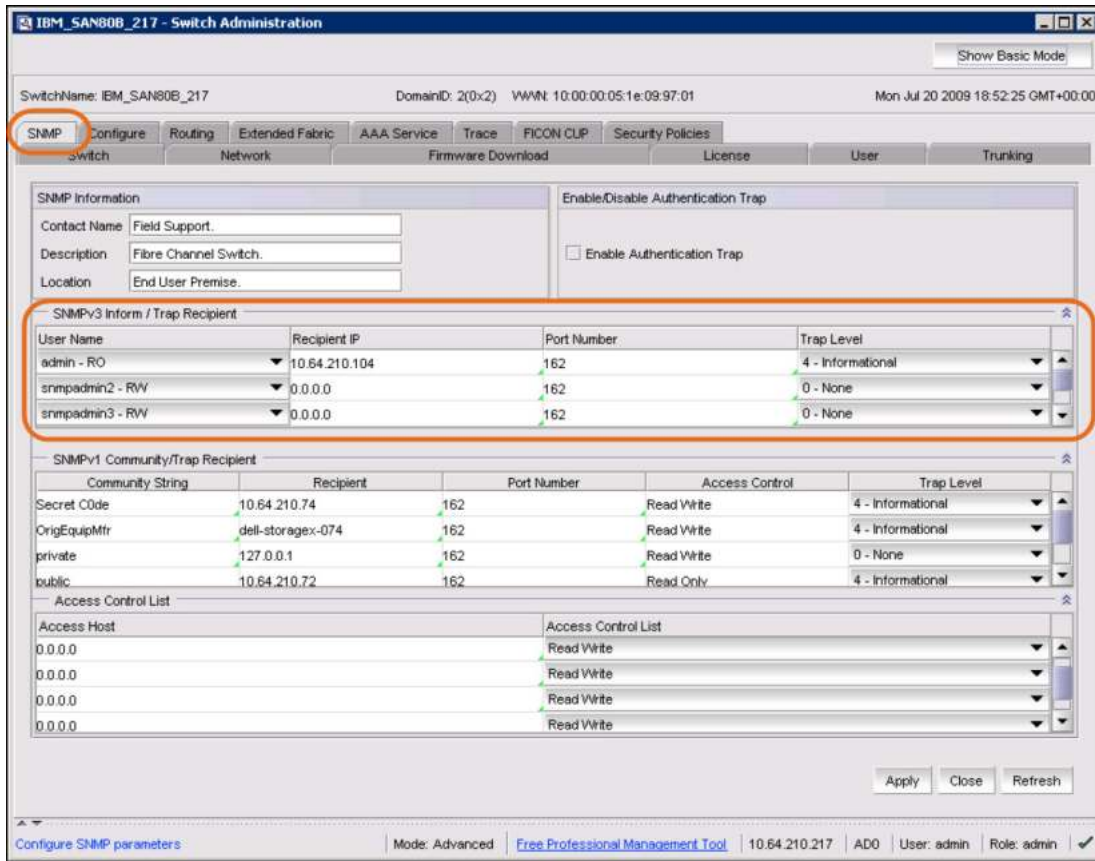


Configuring Automatic Notification of Storage and Switch System Events

Forwarding Alerts from an IBM System Storage SAN24B-4 Express Switch to an Actifio CDS Appliance

To access the SNMP configuration on an IBM System Storage SAN24B-4 Express Fibre Channel switch:

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 section:
 - 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 Fibre Channel switch.



Setting SNMP Trap Destinations in the Fibre Channel Switch

Checking Fibre Channel Connectivity from a CDS Appliance to Storage

To check the Fibre Channel connectivity to storage:

1. Use the Actifio SARG `reportfabric` command to ensure the appliance sees switches and target ports.
2. Use the Actifio SARG `reportmdiskspace` command to check that the appliance sees LUNs.

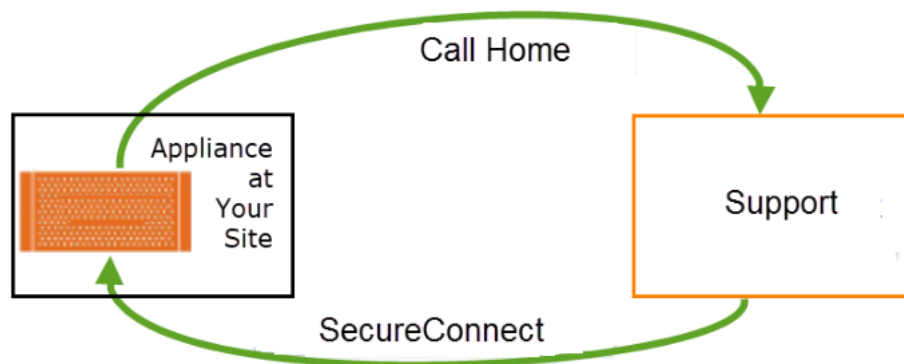
Note: The **SARG User Guide** is in your Actifio Documentation Library and online at ActifioNOW.

25 Actifio Remote Support

Actifio offers two optional remote support features:

Call Home remote event notification: When you enable the Call Home feature, your Actifio Appliance sends alerts and other diagnostic data to Actifio. Actifio Customer Support engineers monitor system alerts and conduct impact assessments. Based upon the alert level, the system may even initiate a problem resolution case and an associated escalation plan for you. Actifio Call Home is detailed in [Actifio Call Home Remote Event Notification](#).

SecureConnect remote service access: When you enable SecureConnect, Actifio Customer Support engineers can access your system remotely on an as-needed basis. As a situation requires, they can manage major upgrades and service pack updates and hotfixes, phase out failing hardware, collect log data on history of failures, restart data and I/O modules, change the configuration of ports, and more. All actions are documented in the VDP audit log and in the Actifio installation/problem reporting databases for further review. Actifio SecureConnect is detailed in [Actifio SecureConnect](#) on page 123.



Call Home and SecureConnect

Actifio Call Home Remote Event Notification

Actifio Call Home sends a notification (email or HTTPS) to Actifio Customer Support every six hours. In the event of a problem, Actifio Support can refer to this information to minimize time to recovery. The notification includes these statistics:

- VDP 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

Actifio Customer Support engineers monitor system alerts and conduct impact assessments. Based upon the alert level, the system may even initiate a problem resolution case and an associated escalation plan for you.

Can I Enable Call Home Without Enabling SecureConnect?

Yes. Call Home provides data, and SecureConnect provides access. Enabling Call Home without enabling SecureConnect ensures that Actifio Customer Support has excellent monitoring, alerting, and analytics data, without the access that might be needed to perform further diagnostics or remediation. The data lets Actifio Customer Support know when a problem has occurred and prepare a response if needed, but investigation and troubleshooting has to be performed via WebEx or conference call.

Most investigations require additional data to be gathered from the appliance, and without SecureConnect, the cycle of gather-analyze-followup-analyze can become cumbersome.

Call-Home Network Requirements

Actifio Call Home uses HTTPS or SMTP. The port numbers for these configurations will depend on your own network setup. The default port numbers are: 25 for SMTP, 443 for HTTPS.

Note: Access to the Call Home web site <https://callhome.actifio.net> should never be blocked by your firewall.

An Actifio Administrator must configure the Actifio Appliance to communicate with an SMTP/HTTPS/proxy server as detailed in [Chapter 20, Actifio Event Notifications](#).

Configuring Actifio Call Home

To send Actifio Appliance statistics to Actifio Support every 6 hours, refer to [Chapter 20, Actifio Event Notifications](#).

Actifio SecureConnect

Actifio SecureConnect is a secure method for remote support that employs dedicated ports and encrypted data. These built-in security features greatly reduce the risks associated with a connection to an external network. The SecureConnect protocol allows Actifio Customer Support engineers to access your system on an as-needed basis to manage cases and updates while meeting your SLA requirements.

Your Actifio account team is kept up to date on a repair status as the case progresses. If hardware replacement is required, parts & local support are shipped to the site and an Actifio Services engineer is dispatched to handle the installation. When the incident is resolved to your satisfaction, the Actifio Customer Support engineer logs out of your Actifio Appliance, disconnects from the remote access line, and creates a summary report of problem root cause and repair actions that is delivered to your account team and to you.

Advantages to using Actifio SecureConnect include:

- **Accelerated problem solving:** By leveraging Actifio follow-the-sun support, you can resolve problems without extending the wait time that invariably gets generated by relying on log files, dumps, and traces being transmitted across the globe.
- **Fine-grained monitoring and collaboration:** You can monitor remote support activities and join in conference calls with Actifio Customer Support engineers as the problem determination process proceeds.
- **Real-time learning:** Remote Actifio Customer Support engineers provide you with ongoing assistance in the setup, configuration, and management of your Actifio Appliances.

Without SecureConnect enabled, you can still contact Actifio Customer Support. Actifio support engineers can work with you via WebEx and other remote support tools for log file gathering and other forensics to help resolve the issue.

Can I Enable SecureConnect Without Enabling Call Home?

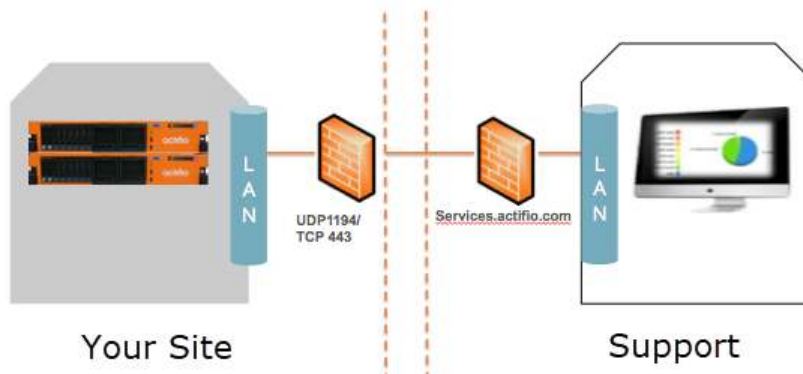
Yes. Call Home provides data, and SecureConnect provides access. Enabling SecureConnect without enabling Call Home allows Actifio Customer Support engineers to respond and investigate issues after you tell us a problem exists. Without Call Home, Actifio Customer Support has no way to know of problems with your system. There is no proactive data collection associated with activating SecureConnect.

How SecureConnect Works

SecureConnect uses client/server architecture. The SecureConnect client comes built into your Actifio Appliances, to be enabled and disabled by you.

After you enable the connection through the Actifio Appliance, your Actifio Appliance establishes a secure point-to-point connection to a secure server at the Actifio Global Support Center, enabling remote access from the Actifio Global Support Center to your Actifio Appliance. You must configure a firewall rule to allow the Actifio Appliance to connect over UDP on port 1194.

As a client connection, SecureConnect does not bridge networks or perform any form of routing. Connections initiated at the Actifio Global Support Center communicate with your Actifio Appliance and no other systems on your network.



How Secure Is Actifio SecureConnect?

SecureConnect utilizes 2048-bit RSA cryptography for strong mutual authentication and encryption, 256-bit AES for encryption of data in flight, and Diffie-Hellman for Perfect Forward Secrecy (PFS) key exchange. Each connection is a point-to-point link and none of your equipment can access another endpoint. Intrusion detection software continually monitors the connection for any anomalous activity. Authentication records are replicated in real-time to off-site locations. The SecureConnect servers are routinely monitored for emerging threats and vulnerabilities.

Only select users within the support and engineering organizations are authorized with this level of access. Actifio employees who have a business need to access your systems must pass a third-party background check and sign a security, compliance, and confidentiality agreement. Access is reviewed annually and terminated immediately in the event of separation or role change. Authorized employees authenticate to SecureConnect with a 2048-bit X.509 certificate stamped with the identity of the user. A two-factor challenge is required after cryptographic authentication in the form of a smart phone push or code-generating token. The certificate must be renewed annually. Issuance is logged to an audit log, and all activities on a system while logged in using the certificate are logged along with the identity of the user. The VPN connection is protected using NIST-approved strong cryptography including AES-256 data encryption.

No Access to Your Business Data

Appliance service credentials are completely independent from SecureConnect and are generated on entirely separate systems. To gain access to a customer system, an Actifio Support staff member generates a time-limited, passphrase-protected authentication token which is locked specifically to the machine they have been granted access to log into. The system generating these tokens is on a secure network separate from the SecureConnect network and itself authenticates against a robust corporate directory. The ability to generate authentication tokens is limited to Actifio Support staff members who have been approved by a rigorous screening process.

Actifio SecureConnect Network Requirements

Actifio SecureConnect is a strong 2048-bit RSA mutually authenticated service not subject to redirection or man-in-the-middle attacks. SecureConnect requires a UDP connection over port 1194 **from** the Actifio Appliance IP address **to** secureconnect2.actifio.com and a setting of "any" IP address. If you cannot use 'any', then contact Actifio Support.

Actifio Appliance IP Address depends on the type of appliance:

Actifio Sky Appliance: the Actifio Appliance IP is the IP address of the Sky Appliance.

Actifio CDX Appliance: the Actifio Appliance IP must include the IP addresses for Node 0 and Node 1.

Actifio CDS Appliance: the Actifio Appliance IP must include the IP addresses for the CDS node.

Enabling Actifio SecureConnect

To enable SecureConnect mode, refer to the AGM online help, reachable from the ? icon in the top right corner of the AGM.

Index

Symbols

_ 71, 73
£ 77

A

Actifio Change Tracking Driver 36
Actifio MIB
 accessing 112
 mapped OID assignments 113
 SNMP GET requests 111
 System MIB variables 114
Actifio Optimized Storage, defined 98
Actifio Remote Support 121
Actifio Resiliency Director, network ports used 21
Actifio SNMP agent 111
AIX connector
 installing 56
 uninstalling 56
AIX host
 installing/modifying Actifio Connector 41, 56
 supported configurations 53
alerts 117
 collecting 117
 forwarding from Fibre Channel switches 118
 methods support by an Actifio appliance 100
 monitoring by System Monitor 101
 polling 117
 polling from Actifio Optimized Storage and Switches 117
 receiving forwarded alerts 117
 sending by email 103, 105
 sending by HTTPS 103
 sending to SNMP trap receiver 109
AOS events 98
assigning VDisks to a host 68
autodiscover applications on a host 69

B

backup and restore jobs 91
batch files 91

C

Call Home remote event notification
 configuring 103, 122
 contrasted with SecureConnect 122
 overview 121

CentOS Linux 43
CIFS file systems 73
clearable events 98, 102
CLI commands 113
community string
 for forwarding traps 110
 SNMPv2 community string 112
connecting a host, overview 67
Connector installer file, downloading 25
Connector, and encrypted network traffic 24
contact information, Actifio Support ii
copyright ii
custom configuration (legacy mode) 7
custom route, see static route

D

data transport mode, NFS or SAN 73
deleting hosts 70
Dell Unity storage arrays 76
Diffie-Hellman
 (PFS) key exchange 124
 data in flight encryption 15
DNS domain, configuring 2
downloading the Actifio Connector installer file 25

E

email for Call Home
 support-bot@callhome.actifio.com 107
email notification of events, automatic 106
email server, configuring appliance communications to 105
ESXi cluster 73
etc/hosts editor 9
event notifications, see notifications
Exchange 73
External Snapshot Pools (ESP) 75

F

Fibre Channel
 HP-UX host 63
 Linux host 45
 Solaris host 61
 Windows Server host 35
Fibre Channel switches, forwarding alerts from 118
Filter Driver, see Actifio Change Tracking Driver
firewall ports 15

G

GetRequest, SNMP 15

H

HBA ports 64

HMC host, see IBM HMC host

host names, invalid characters in 71, 73

Host Resolution 9

host type

Windows Server 73

hosts

adding IBM HMC 72

adding Linux, AIX, HMC, Solaris, HP-UX 71, 73

adding Windows Server 73

HP-UX host

Fibre Channel connectivity 63

installing/modifying Actifio Connector 65

iSCSI connectivity (Sky only) 63

multipathing 63

HTTPS communication of events 104

Hyper-V VMs 73

I

IBM HMC host

adding 72

vSCSI connectivity 58

IBM Storwize storage arrays 75, 76

in-band storage 68

installer files, Connector, downloading 25

invalid PKCS12 87

IP addresses, configuring 3

IP route get, troubleshooting via 8

iSCSI initiator

HP-UX hosts 63

Linux host 43

Solaris x86 host 61

Windows Server host 34

iSCSI sessions

increasing number of on Sky appliance 4

supported number of 27

L

LDAP 79

legal matter ii

limiting number of records sent 114

limiting the number of records sent by the SNMP agent 114

Linux connector

installing 50

uninstalling 50

Linux host

Fibre Channel connectivity 45

finding WWN 45

installing/modifying the Actifio Connector 50

iSCSI connectivity 43

local management and service and backup traffic 16

local storage management, ports required for 19

logs

on a Linux host 43

on a Solaris host 59

on a Windows Server host 33

on an HP-UX host 63

on an IBM AIX host 41, 53

on an IBM HMC host 57

LPAR hosts, see IBM HMC hosts

LPAR with NPIV mapping 53

LPARs, discovering 72

M

MIB

about 111

accessing 112

mapped OID assignments 113

SNMP GET requests 111

System MIB variables 114

Microsoft SCVMM 73

multipathing 35, 45

N

network ports 15

new applications, auto-discovering on host 69

NFS protocol 49, 55, 59

NFSv3 62

notifications

automatic email, setting up 106

email notifications of events 103, 105

event context information displayed in the Events Monitor 101

HTTPS notifications of events 103

polling from Actifio Optimized Storage 117

SMTP server, communicating with 105

UDP trap protocol 109

NTP server, configuring Actifio appliance connection to 2

number of records sent by the SNMP agent, limiting 114

O

OID assignments 113

operations on a host before and after capture 89

Oracle Databases in a Solaris Environment, with NFS 62

Outbound Policies 6

P

Perfect Forward Secrecy (PFS) 15

ping, troubleshooting via 8

PKCS12 86

platform events 98

polling alerts from Actifio Optimized Storage and Switches 117

ports, firewall 15

Pound Sterling character (£) 77

PowerPC 44

pre- and post- actions on applications 89

pre-scripts and post-scripts 89

Pure Storage FlashArray storage arrays 75, 76

R

- Red Hat RHEL 6 43
- reference architectures 11
- remote network, rules for reaching over network 6
- Report Manager 20
- restore jobs 91
- role-based access (RBAC) 79
- rootvg, bootable, AIX non-HMC 53
- rootvg, bootable, for vSCSI-mapped LPARs 58
- RSA public keys 15

S

- SAML authentication 85
- SAN switch, network ports used 19
- scripts
 - on a Linux host 43
 - on a Solaris host 59
 - on a Windows Server host 33
 - on an HP-UX host 63
 - on an IBM AIX host 41, 53
 - on an IBM HMC host 57
- SCVMM 73
- SecureConnect remote service access
 - enabling 124
 - how it works 123
 - overview 121
 - security features 124
- security, network 15
- self-service network configuration 1
- SetRequest, SNMP 15
- SharePoint 73
- SMTP server, communicating with 105
- SNMP 15
 - Actifio SNMP agent 111, 114
 - CLI commands supported for SNMP GET requests 113
 - community string, setting 110
 - configuration on Fibre Channel switches 118
 - notifications 117
 - SNMP agent, activating from CLI 111
 - SNMP GET request 111
 - SNMPv2 community string 112
 - SNMPv2 support 111
 - Trap receiver 111
 - trap receiver 109
 - traps 100, 111, 118
- SNMP agent
 - about 111
 - enabling 111
- SNMP v1 and v2 15
- SOCKS5 104
- Solaris host
 - Fibre Channel connectivity 61
 - finding WWN 61
 - installing/modifying the Actifio Connector 60
 - iSCSI connectivity 61
- SQL Server 73
- SQL VSS Writer 39
- SSN for cloud 10

- static route, setting 6
- STONITH 17
- storage, assigning to in-band hosts 68
- System Monitor, monitoring alerts 101

T

- TCP Connection Test, troubleshooting via 9
- TLS web service certificate 86
- tracpath, see traceroute
- Traceroute, troubleshooting via 8
- trademarks ii
- trap receiver, sending traps to 109
- traps and informs, see notifications

U

- Ubuntu connector installation 50
- UDSAgent 24
- Unix hosts 71

V

- vCenter server 74
- VDisk, mapping to a host 68
- VIOS, discovering 72
- VMware SRM integration 17
- vSCSI connectivity for IBM HMC hosts 58
- vSCSI VIO mapped LPARS 58

W

- warranty ii
- WBEM 17
- web service certificate 86
- whitelisted IP addresses 15
- Windows host
 - adding to appliance 73
 - Fibre Channel connectivity 35
 - finding WWN 35
 - installing/modifying Actifio Connector 36
 - iSCSI connectivity 34
 - logs and scripts 33

Y

- YaST, to install the iSCSI initiator 44

