Network Administrator's Guide to Actifio Copy Data Management

actifio

Actifio 9.0

Copyright, Trademarks, and other Legal Matter

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

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

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

Contents

Preface

This guide provides step-by-step instructions on how to configure your Actifio appliance into your network. It assumes you have read ***Introducing Actifio Copy Data Management***, are familiar with the components of the Actifio Desktop, and have a grasp of the basic concepts associated with an Actifio appliance.

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

- ***Configuring Resources and Settings With the Domain Manager***
- ***Connecting Hosts to Actifio Appliances***

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

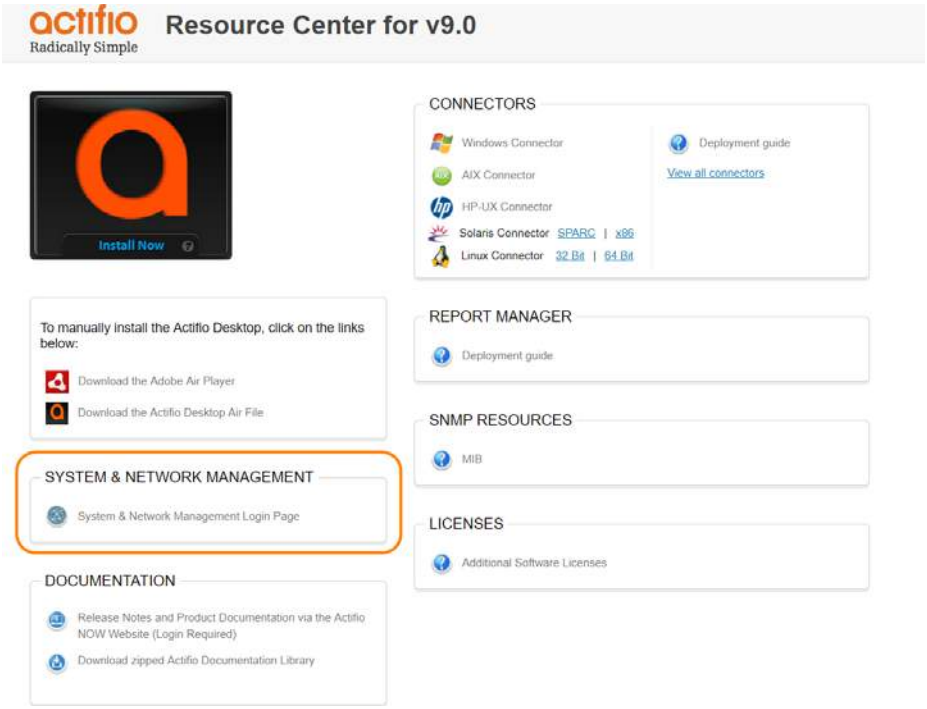
1 Modifying Your Network Configuration Settings

Your Actifio appliance includes a self-service network configuration feature. This document 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
- Perform Host Resolution on page 10
- Configure Self Service Network for Actifio Sky Appliances in the Cloud on page 11

Accessing the Appliance System Management Tools

1. Open a browser to the Actifio 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 11.



Accessing the System & Network Management Tools

DNS, and NTP

Enter this information:

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

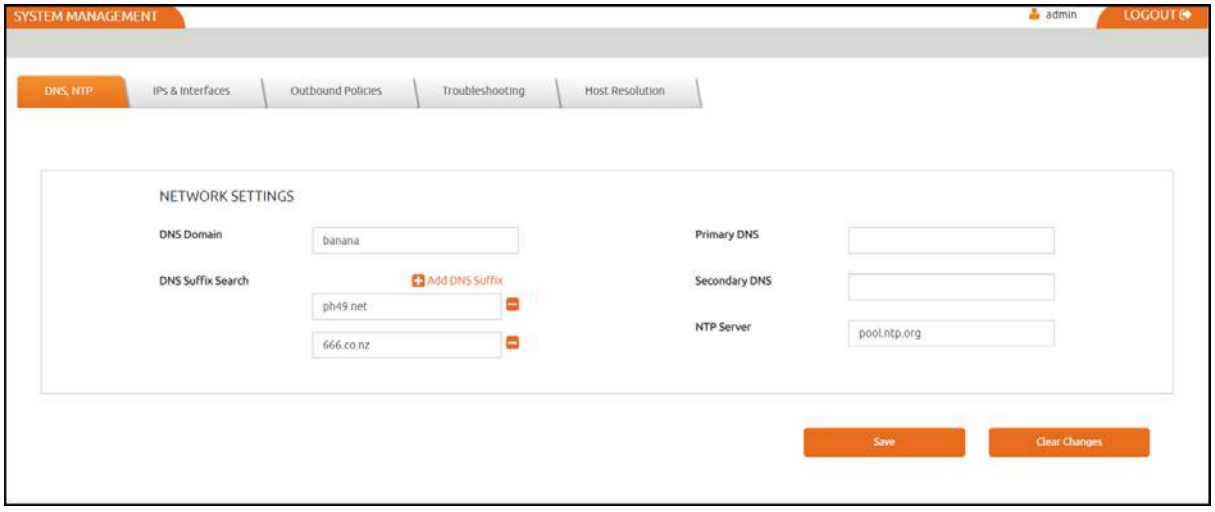
If you have additional hosts on other domains, you can set up a **DNS Suffix Search** to ensure the Actifio appliance can find them by their short names.

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).

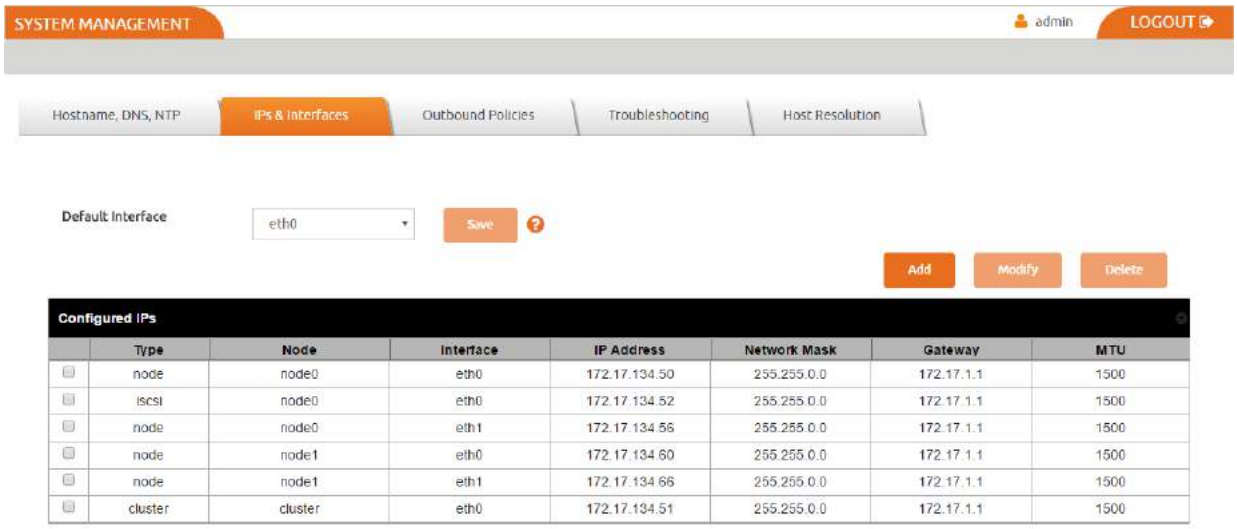
NTP Server: Enter the IP address or hostname of your NTP server.



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 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.



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.

Modifying the MTU for Node1

Note: *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.*

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:

Actifio Sky NIC Usage on page 4

Actifio CDS Generation-3 Appliance NIC Usage on page 4

Actifio CDS Generation-4 and Generation 5 Appliance NIC Usage on page 5

Actifio Sky 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.

Actifio CDS Generation-3 Appliance 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

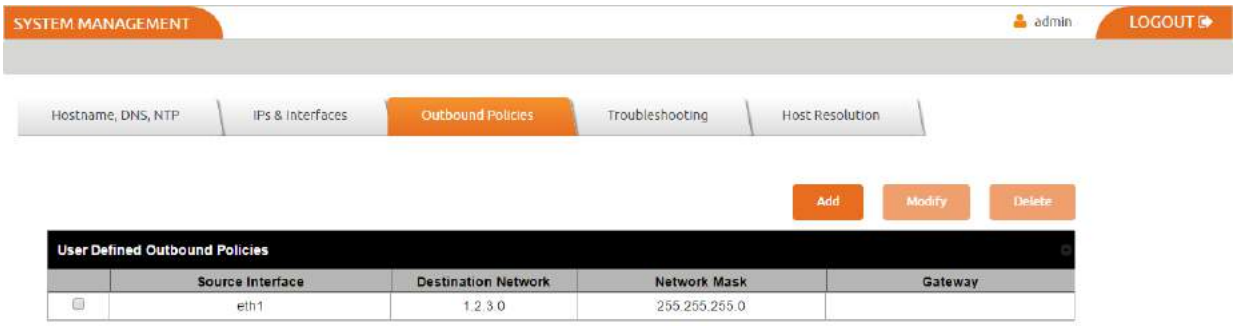
Actifio CDS Generation-4 and Generation 5 Appliance NIC Usage

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

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

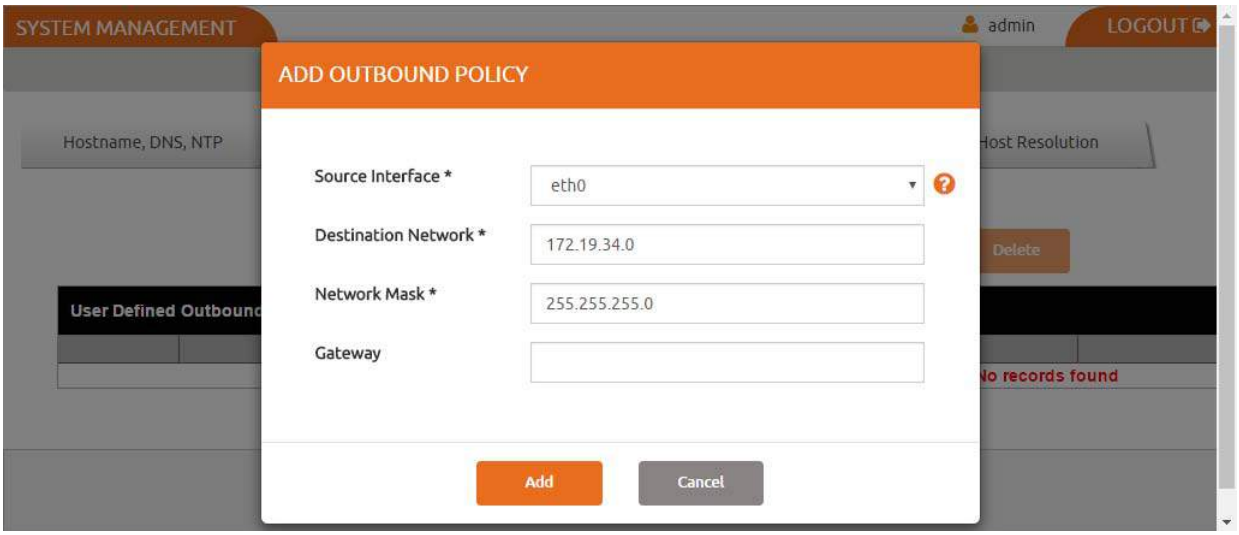
To modify an outbound policy:

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

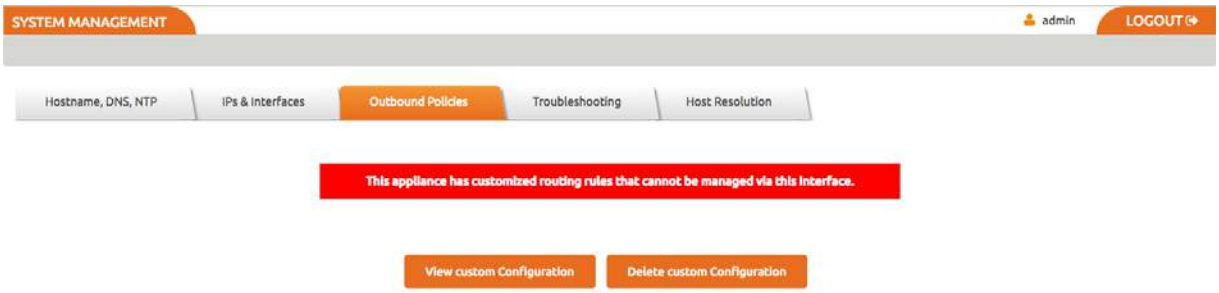
Outbound Policies and Custom Configurations

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.*

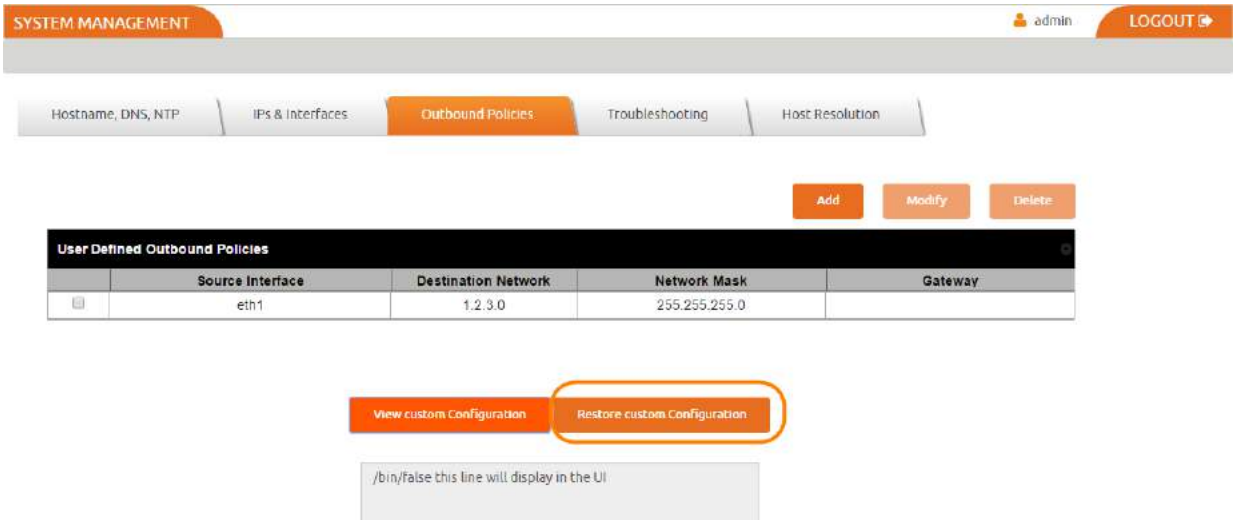
If the appliance has an active custom configuration, then you see a Delete option. This disables the custom part of the configuration, allowing you to proceed with the formerly disabled management functions.

> ***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:

- **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.
- **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:

- **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.
- **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.

- **Destination IP**: The IP address of a target host.
- **UDP Port**: See Chapter 3, Firewall Rules

Example Traceroute result:

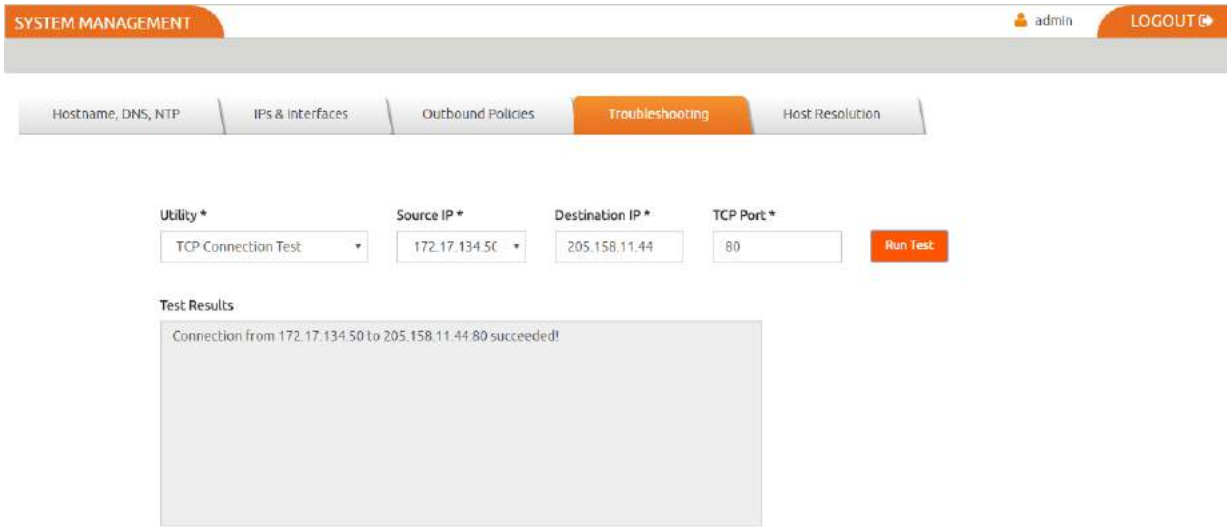
```
test/traceroute 8.8.8.8
1: dev134-86.dev.actifio.com (172.17.134.86) 0.092ms pmtu 1500
1: devgw-waln5k02.dev.actifio.com (172.17.0.3) 4.287ms
1: devgw-waln5k02.dev.actifio.com (172.17.0.3) 1.287ms
2: e-1-20-walpalo.core.actifio.com (192.168.255.21) 2.805ms
3: ge-0-0-1-walasr.edge.actifio.com (192.43.242.209) 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
10: no reply
11: no reply
12: no reply
```

```
13: no reply
14: no reply
15: no reply
16: no reply
17: no reply
18: no reply
19: no reply
20: no reply
21: no reply
22: no reply
23: no reply
24: no reply
25: no reply
26: no reply
27: no reply
28: no reply
29: no reply
30: no reply
31: no reply
Too many hops: pmtu 1500
Resume: pmtu 1500
```

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

- **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.
- **Destination IP**: The IP address of a target host.
- **TCP Port**: See Chapter 3, Firewall Rules.

Example TCP Connection Test result:



Troubleshooting: TCP Connection Test

Host Resolution

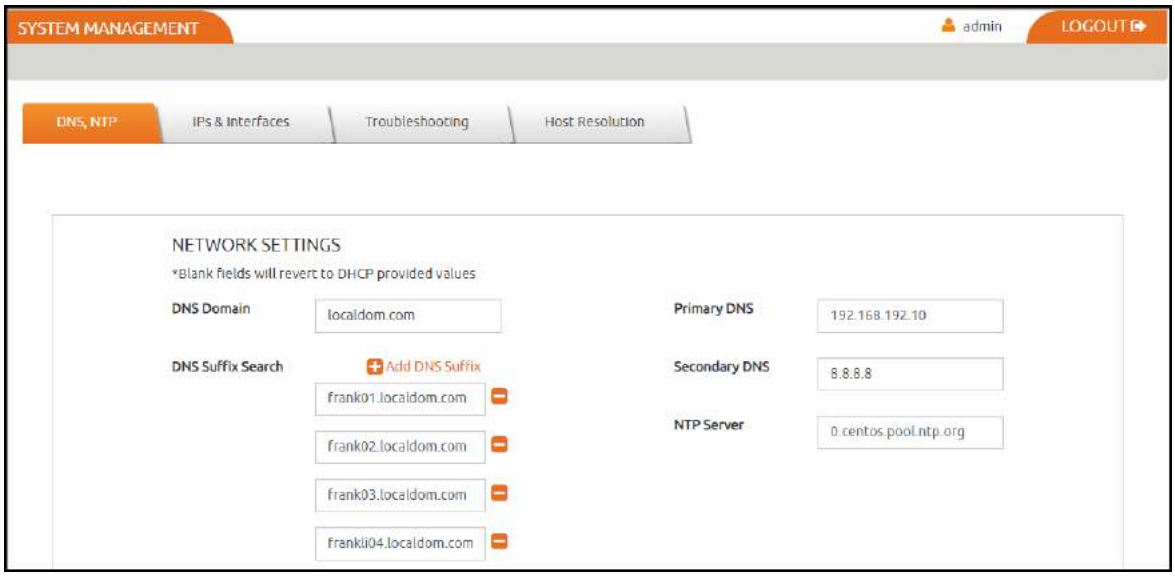
A host that has both management and production IP addresses may be configured with only the IP address for the management NIC in DNS. Use this page to add the NIC used for production communications. The information that you enter here becomes the contents of /etc/hosts.

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

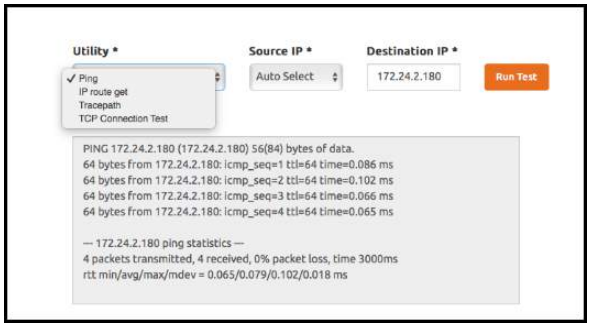
Configure Self Service Network for Actifio Sky Appliances in the Cloud

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 10.

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 available network resources. For best results, appliances should be configured according to the following tables:

Actifio Sky Appliances

Actifio Sky 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

Actifio CDX Reference Architecture

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

Actifio CDS Generation-3 Appliances

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

An Actifio CDS Generation-3 Appliance

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

Actifio CDS 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 Generation-4 Appliances

The Actifio CDS Generation-4 appliance looks like this:

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

Actifio CDS 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 Generation-5 Appliances

The Actifio CDS Generation-5 appliance looks like this:

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

Actifio CDS 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 employed within a fully functional Actifio copy data management environment:

Internet Protocol (IP) Network Security in an Actifio Environment

All components of Actifio Copy Data Virtualization have been designed from the ground up 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 the following services, but not does not listen on or run a service for these ports unless listed in Actifio Local Management from Administrator Workstation on page 18.

SNMP

For the most part SNMP code on Actifio CDS 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, Actifio CDS will listen on UDP 162 for SNMP traps from specified IPs that are whitelisted for Actifio CDS Integrated Storage components.

A list of whitelisted IPs can be viewed with the commands `udsinfo` and `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 Local Management from Administrator Workstation

Destination Port	Protocol(s)	Source IP Address	Destination IP Address	Description
22 (TCP)	SSH	Admin workstation	Actifio Appliance IP 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 the Actifio Desktop and Connector software. No appliance control or data access is possible on this port.
443 (TCP)	HTTPS	Admin workstation	Actifio Appliance IP	Provides TLS-encrypted communication between Actifio Desktop clients and the appliance, as well as some appliance-to-appliance communication. SSL certificates may be customer replaced.
3900 (TCP)	HTTP	Admin workstation	Actifio IMM Addresses	Node IMM ports for remote access

Actifio Appliance Local Services

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

Management Traffic to and from the Actifio Appliance

Destination Port	Protocol(s)	Source IP Address	Destination IP Address	Description
26 (TCP)	SSH	Actifio Appliance IP	Actifio Appliance IP	Actifio to Actifio cross node management. Node addresses should also be allowed.
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.
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 and Replication Traffic Between Appliances

Destination Port	Protocol(s)	Source IP Address	Destination IP Address	Description
443 (TCP)	HTTPS	Actifio Appliance IP	Amazon S3 Endpoint Other Appliance	Actifio OnVault cloud data transfer Actifio appliance - appliance traffic
902 (TCP)	VMware	Actifio Appliance IP	ESX Server VMKernel IPs	Encrypted connectivity to VMware ESXi hosts for data movement operations.
3205 and 3260 (TCP)	iSCSI	Host servers	Actifio iSCSI Addresses	iSCSI target

Backup Traffic from the Actifio Appliance and Replication Traffic Between Appliances

Destination Port	Protocol(s)	Source IP Address	Destination IP Address	Description
111 756 2049 4001 4045	tcp/udp tcp/udp tcp/udp tcp/udp tcp/udp	Host servers	Actifio NFS Addresses	Portmapper/rpcbind statd nfsd mountd lockd
5103	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 data transfer for cross-site mirroring and for Actifio StreamSnap data replication. Bidirectional rules are needed.
5108 (TCP)	Actifio API	Actifio Appliance IP	Actifio Appliance IP	Please keep this port open for a planned StreamSnap feature.

Actifio Remote Support

Destination Port	Protocol	Source IP Address	Destination IP Address	Description
443 (TCP)	HTTPS	Actifio Appliance IP	callhome.actifio.net	Actifio Call Home Alerting
25 (TCP)	SMTP	Actifio Appliance IP	callhome.actifio.net	Actifio Call Home Alerting (legacy)
443 (TCP)	OpenVPN/ HTTPS	Actifio Appliance IP	secureconnect2.actifio.com	SecureConnect proxy mode (optional)
1194 (UDP)	OpenVPN	Actifio Appliance IP	secureconnect2.actifio.com	Actifio SecureConnect. Encrypted remote support access to Actifio data centers. As the connection is mutually authenticated with strong cryptography, it is recommended that the destination not be limited by a firewall.

Local Storage Management

Destination Port	Protocol(s)	Source IP Address	Destination IP Address	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
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 IP Address	Destination IP Address	Description
443 (TCP)	HTTPS	Administrator workstation	Report Manager server	Actifio Report Manager (reports & setup/admin)
5103 (TCP) Use 443 if the firewall blocks outbound traffic	SSH	Report Manager server	Actifio Appliance IP	Actifio Report Manager (data collection)

Actifio Global Manager (AGM)

Destination Port	Protocol(s)	Source IP Address	Destination IP Address	Description
5103 (TCP) Use 443 if the firewall blocks outbound traffic	SSH	AGM server	Actifio Appliance IP	Outbound connection from AGM to all managed Actifio 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 IP Address	Destination IP Address	Description
TCP-443	HTTPS	Resiliency Director Collector	Actifio Appliance IP	Data Collection/Recovery Orchestration at source site
		Resiliency Director Collector	vCenter Server IP	Data Collection/Recovery Orchestration at source site
		Resiliency Director Server	Actifio Appliance IP	Data Collection/Recovery Orchestration at DR site
		Resiliency Director Server	vCenter Server IP	Data Collection/Recovery Orchestration at DR site
		Resiliency Director Server	Resiliency Director Collector	Partnership setup
		Resiliency Director Collector	Resiliency Director Server	Replication of configuration data
		Administrator workstation	Resiliency Director Collector	Resiliency Director Collector configuration/administration
		Administrator workstation	Resiliency Director Server	Resiliency Director Server configuration/administration
TCP-5103	HTTPS	Resiliency Director Collector	Actifio Appliance IP	Used to establish secure session ID
		Resiliency Director Server	Actifio Appliance IP	Used to establish secure session ID

Actifio Appliance IP

Actifio Appliance IP Address depends on if you are using a Sky appliance or a CDS appliance:

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

Actifio CDS Appliance: the Actifio Appliance IP must include the IP addresses for Node 1, Node 2, and for the cluster.

4 iSCSI Connectivity

This includes:

Note: *For best iSCSI network traffic results, see* NIC Usage for Each Actifio Appliance Type *on page 4.*

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.
   If the iSCSI IP address is 123.45.67.89 then issue a command like this:
   (Shown is the response if the device is listening on that port. This is a good result.)

   ```
   ~ # nc -z 123.45.67.89 3260
   Connection to 123.45.67.89 3260 port [tcp/*] succeeded!
   ```

   If a port is unreachable then you will simply return to the prompt with no output.

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

Ensuring iSCSI Connectivity with an ESX Server

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 Chapter 3, Firewall Rules.
- 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.

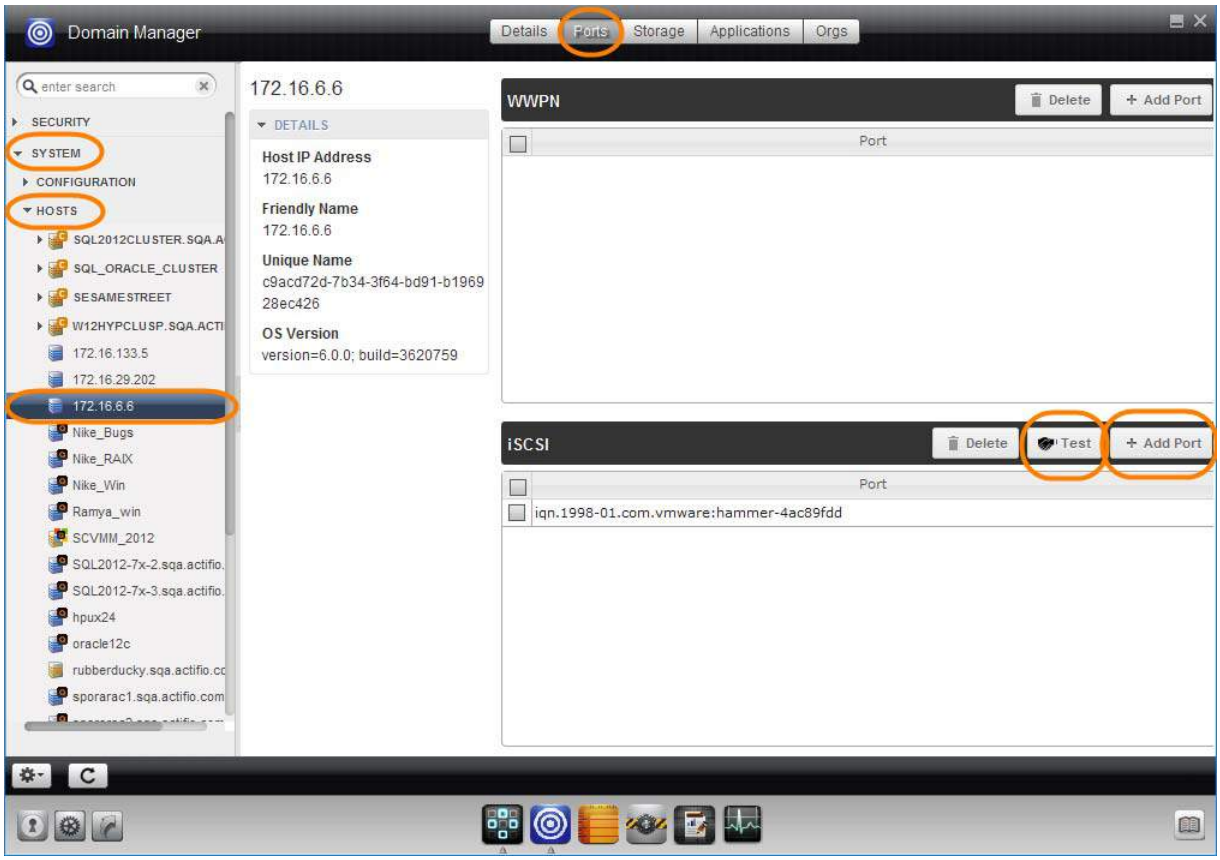
This procedure is designed around a single Actifio Ethernet iSCSI connection to a single iSCSI Ethernet connection on the ESX server. Actifio Professional Services can help you with any other configuration.

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**.

Configuring the ESX Host within the Actifio Desktop

1. Open the Actifio Desktop to the **Domain Manager**.
2. From **System** > **Hosts**, select the ESX server.
3. On the **Ports** tab, under iSCSI, click **+ Add Port**.
4. Enter the iSCSI iqn name in the Enter iSCSI field, and click **Add Port**. This will configure the iSCSI relationship on Actifio to the ESX server.
5. Use the **Test** button to test the connection.



Configuring the Actifio Appliance to Recognize an ESX Server

Ensuring iSCSI Connectivity on a Linux Host

This section includes:

When the Actifio Connector manages data movement over iSCSI, the Actifio appliance 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_sky-611 ~]# grep -v ^# /etc/iscsi/initiatorname.iscsi | cut -d "=" -f 2
iqn.1994-05.com.redhat:6d11e98139fb
[root@psa_sky-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**.

Ensuring iSCSI Connectivity on an IBM AIX 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. This section includes:

Supported AIX iSCSI 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).

Note: *Actifio can protect and recover in-band physical machine configurations via Fibre Channel or iSCSI 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 LPAR has dedicated access to one or more physical HBAs while sharing other resources like CPU and memory with other LPARs. This provides better total 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).

Note: *Actifio can protect and recover in-band dedicated LPAR configurations both via Fibre Channel and iSCSI in a crash-consistent or application-consistent state. Actifio can also protect the 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.

Note: *Actifio can protect and recover in-band NPIV environments including the rootvg of an LPAR in a bootable state.*

These hosts can be added as physical hosts, but storage ports need to be configured for them; see Ensuring Fibre Channel Connectivity on an IBM AIX Host on page 37.

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 32.

Connecting to AIX Hosts over iSCSI

When Fibre Channel is not available, you can use iSCSI. If iSCSI is used, then 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.

To Learn the iSCSI Initiator Name from an AIX Host

To learn the name of the iSCSI initiator already installed on a host:

```
bash-4.2# lsattr -El iscsi0| grep -i "initiator_name" | awk '{print $2;}'
iqn.localhost.hostid.7f000001
```

Validating that the iSCSI Initiator is Installed on an IBM AIX Host

To determine if the iSCSI initiator is installed on an AIX host:

```
[bigblue4:root] / > lslpp -l | grep iscsi
  devices.common.IBM.iscsi.rte
  devices.iscsi.disk.rte    7.1.0.15  COMMITTED  iSCSI Disk Software
  devices.iscsi.tape.rte    7.1.0.0  COMMITTED  iSCSI Tape Software
  devices.iscsi_sw.rte      7.1.1.15  COMMITTED  iSCSI Software Device Driver
  devices.common.IBM.iscsi.rte
  devices.iscsi_sw.rte      7.1.1.15  COMMITTED  iSCSI Software Device Driver
[bigblue4:root] / >
```

> ***Note:*** *Inband devices (VDisks) presented to the AIX host via iSCSI must have the* `rw_timeout` *attribute to 120 seconds.*

Ensuring iSCSI Connectivity on a 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, the Actifio appliance 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 have an impact on performance.

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

When the Actifio Connector manages data movement over iSCSI, the Actifio appliance 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. 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.

> ***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 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.
- Actifio 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, Actifio 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, the Actifio appliance uses a staging disk to create a copy of application data during each Snapshot or Dedup Async job.

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, the Actifio appliance 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

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

[w2k8r2-4104] Enter command or ^C to exit
```

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

5 Fibre Channel Connectivity

This includes:

Ensuring Fibre Channel Connectivity to Storage (CDS only)

To check the Fibre Channel connectivity to storage:

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

Note: *The* ***SARG User Guide*** *is in your Actifio Documentation Library.*

Fibre Channel Zoning between ESX Servers and CDS Appliances

When performing a mount to a VM, the Actifio appliance can present the disks for the mount either over iSCSI to the VMkernel port of the ESX Server, or over Fibre Channel to the Fibre Channel ports of an ESX Server(s). If your ESX Servers have FC adapters it makes sense to allow mount traffic to travel over the FC SAN.

To achieve this you must pre-zone your ESX HBA ports to the Actifio CDS HBA ports:

1. Zone every ESX FC port to every Actifio FC port.
2. Define the vCenter server to Actifio and perform discovery. Actifio will match the ESX ports zoned over FC to the ESX Servers learned through VMware discovery.

   If you zone the ESX servers to Actifio *after* VMware discovery has been performed, you may need to manually add the WWPNs to each ESX host listed in the Hosts section of Domain Manager. Find the HBA ports for each server from the WWPN dropdown and select the correct WWPNs for that server.

When Actifio performs a VMware snapshot, traffic will either flow over the LAN (from the ESX Server VMKernel port to Actifio) or over the SAN (from the backend storage hosting the datastores to the CDS Appliances). This means that snapshots will run even if no zoning exists between Actifio CDS and the ESX Servers.

VMware Multipathing

Actifio FC ports are automatically assigned the correct VMware multipathing options (known as a Storage Array Type Plugin or SATP). No manual configuration is required.

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 Actifio CDS appliance and the host, and an Actifio-approved multipath driver must be in use.

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.

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.

Linux Multipathing Requirements on Actifio Firmware SVC 7.3.0 on page 35

Linux Multipathing Requirements on Actifio Firmware SVC 7.8.1 on page 36

Linux Multipathing Requirements on Actifio Firmware SVC 7.3.0

Red Hat Linux	SuSE Linux
RHEL Versions 5.x, 6.0 and 6.1	**SuSE Linux Versions 10.x, 11.0, and 11SP1**
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	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
RHEL Versions 6.2 and higher and 7.x	**SUSE Linux versions 11SP2 and higher**
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	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

Linux Multipathing Requirements on Actifio Firmware SVC 7.8.1

Red Hat Linux	SuSE Linux
RHEL Versions 5.x, 6.0 and 6.1	**SUSE Linux Versions 10.x, 11.0, and 11SP1**
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	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
RHEL Versions 6.2 and higher	**SUSE Linux versions 11SP2**
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	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
RHEL Versions 7.x	**SUSE Linux Versions 11SP3+**
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	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

Ensuring Fibre Channel Connectivity on an IBM AIX Host

The Actifio appliance must be able to communicate with the Actifio Connector running on the host. This section includes:

Supported AIX Fibre Channel 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).

Note: *Actifio can protect and recover in-band physical machine configurations via Fibre Channel or iSCSI 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 LPAR has dedicated access to one or more physical HBAs while sharing other resources like CPU and memory with other LPARs. This provides better total 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).

Note: *Actifio can protect and recover in-band dedicated LPAR configurations both via Fibre Channel and iSCSI in a crash-consistent or application-consistent state. Actifio can also protect the 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.

Note: *Actifio can protect and recover in-band NPIV environments including the rootvg of an LPAR in a bootable state.*

These hosts can be added as physical hosts, but storage ports need to be configured for them; see Configuring Storage over Fibre Channel for AIX Hosts on page 39.

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 32.

Connecting to an AIX Host over Fibre Channel SAN

Fibre Channel connectivity provides the best performance. It can be used by physical hosts, dedicated LPAR hosts, and LPAR hosts with NPIV mapping. Fibre channel is not available for LPAR hosts with vSCSI mapping.

AutoconfigSanports option would make the best possible attempts to automatically configure storage ports.

> ***Note:*** *It is also possible to also present the staging disk to a VM using NPIV with Fibre Channel, but this is normally not necessary.*

Host Zoning and MPIO

A physical host connected via Fibre Channel requires zoning must between the Actifio CDS appliance and the host, and the path control module (PCM) in use must be AIXPCM (preferred) or IBM SDDPCM.

> ***Note:*** *IBM SDD is not supported. For best results, use a native host MPIO.*

Set the MPIO path health checker to `hcheck_mode = nonactive`.

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

If the AIX host has two HBA ports (two WWNs) 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; 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 an AIX host on a Fibre Channel SAN:

```
bash-4.2# lsdev -Cc adapter | grep -i Fibre|cut -d " " -f 1| while read fc;do lscfg -vspl $fc
|grep Z8;done
Device Specific.(Z8)........C050760782FD002E
Device Specific.(Z8)........C050760782FD0030
```

If you are using SDDPCM then you can validate:

- adapter status using `pcmpath query adapter`
- device status using `pcmpath query device`
- path count using `pcmpath query device` or the AIX MPIO command `lspath`

Time out policy

Recent technology levels of AIX include a `timeout_policy` attribute for some devices. This attribute indicates the action that the path control module should take when a command timeout occurs (when an I/O operation fails to complete within the rw_timeout value on the disk). There are three possible values for `timeout_policy`.

> **`timeout_policy = retry_path`**: This represents the legacy behavior, where a command may be retried on the same path that just experienced a command timeout. This is likely to lead to delays in the I/O recovery, as it is likely that the command will continue to fail on this path. Only after several consecutive failures, will AIX fail the path and try the I/O on an alternate path.
>
> **`timeout_policy = fail_path`**: This setting causes AIX to fail the path after a single command timeout, assuming that the device has at least one other path that is not in the failed state. Failing the path forces the I/O to be retried on a different path. This can lead to much quicker recovery from a command time out and also much quicker detection of situations where all paths to a device have failed. A path that is failed due to timeout policy can later be recovered by the AIX health check commands. However, AIX avoids using the path for user I/O for a period of time after it recovers to help ensure that the path is not experiencing repeated failures. (Other PCMs might not implement this grace period.) This is the recommended setting.

`timeout_policy = disable_path`: This setting causes the path to be disabled. A disabled path is only recovered by manual user intervention using the chpath command to re-enable the path.

Configuring Storage over Fibre Channel for AIX Hosts

To configure storage for AIX hosts accessed over Fibre Channel, see Assigning VDisks for the Host Copy Data (In-Band only) on page 2 of ***Connecting Hosts to Actifio Appliances***.

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 Actifio 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 especially important for maintaining application-aware mounts over a system restart.*

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 Actifio 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 Fibre Channel 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 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.

Multipathing

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

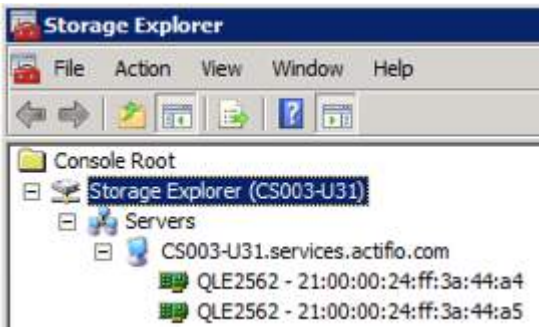
Connecting to a Windows Server 2003 Host over Fibre Channel SAN

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

`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:

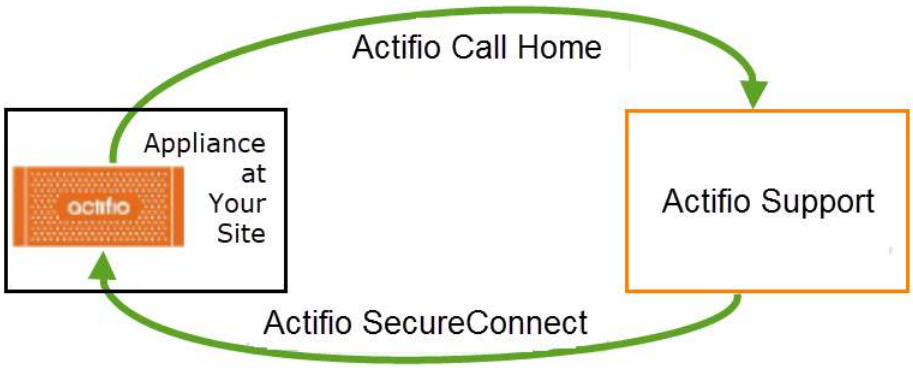
1. Download SDDDSM from http://www-01.ibm.com/support/docview.wss?uid=ssg1S4000350 and unzip it.
2. From a command prompt with Administrative privileges, run setup.exe.
3. Restart the machine.
4. Verify SDDDSM is installed successfully by running `datapath query version`.

6 Actifio Remote Support

Actifio offers two optional remote support features:

Call Home remote event notification: When you enable the Actifio 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 Actifio 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 Actifio appliance audit log and in the Actifio installation/problem reporting databases for further review.
Actifio SecureConnect is detailed in Actifio SecureConnect on page 45.



Actifio Call Home and Actifio SecureConnect

Actifio Call Home Remote Event Notification

Actifio Call Home sends an email 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 email includes these statistics:

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

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. Due to the redundant design of an Actifio appliance, most alerts do not require immediate service attention.

As of v9.0 release, Actifio is offering customers an optional HTTPS Call Home capability that enables the Customer Success team to proactively identify and remediate potential issues. It can also be used to generate the Insight reports available through Actifio Now. In prior releases, the Actifio Call Home data could only be sent using email over SMTP. The HTTPS transport is often more reliable and simpler to configure than SMTP.

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 get blocked.*

An Actifio Administrator must configure the Actifio Appliance to communicate with an SMTP/HTTPS/proxy server as detailed in ***Configuring Actifio Event Alerting***.

Configuring Actifio Call Home

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

1. Open the **Domain Manager** to **System** > **Configuration** > **Notification**.
2. On the **Email** tab, click the **Call Home** tab. Call Home is disabled by default.
3. Click the **Enabled** option to enable Call Home.
4. In the Customer Name, enter the name of the Actifio customer.
5. In the Call Home method section:
    - Select **SMTP** to enable Call Home using SMTP. Go to step 8.
    - Otherwise select **HTTPS** to enable Call Home using HTTPS.

6. You can optionally select **Try SMTP if failure** if you want to send email via SMTP when connection to HTTPS server fails for any reason (due to firewall or network failure for example).

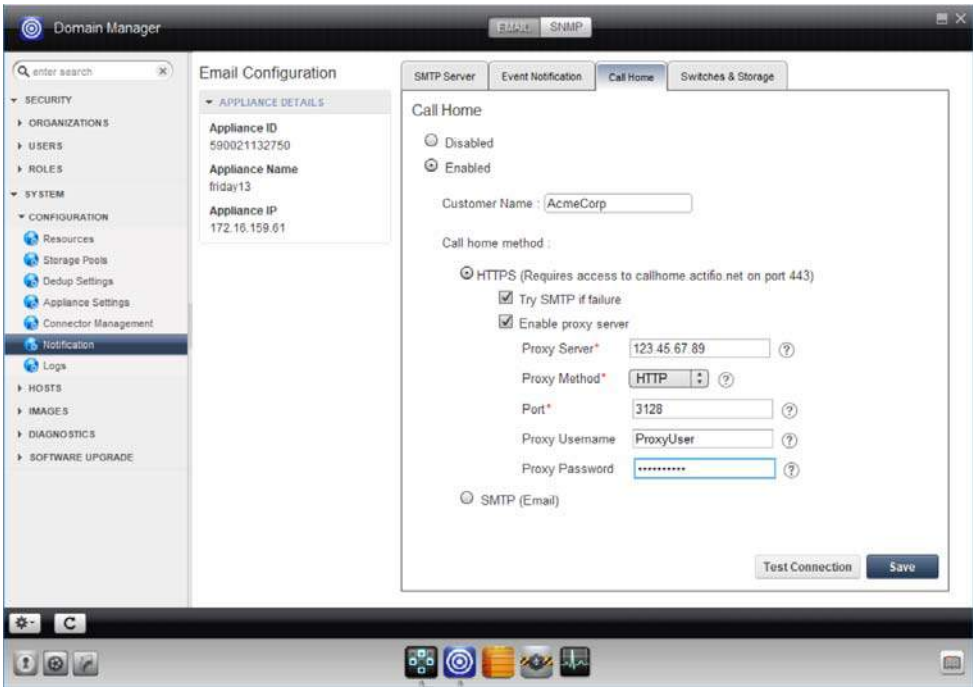
7. To specify a proxy server, check **Enable proxy server**. If you do not need to specify a proxy server, go to step 8.

    a. In **Proxy Server**, enter the IP address of the proxy server.

    b. For **Proxy Method**, choose from SOCKS5 or HTTP.

    c. For **Port**, enter the port to use when sending data to the proxy server.

    d. For **Proxy Username** and **Proxy Password**, enter the username and password to use for proxy authentication, if the proxy server requires such authentication.



Configuring the Call Home Health Check Feature

8. Click **Save** to save the configuration.

    Optionally, click on **Test Connection** and enter your email address. If the connection is configured correctly, after a brief wait you will get a pop-up message. If you entered your email address, you should receive a message within an hour from the Actifio Call Home system confirming that the test succeeded. If the test is successful, you will see the message: *Test Connection Successful!*

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?

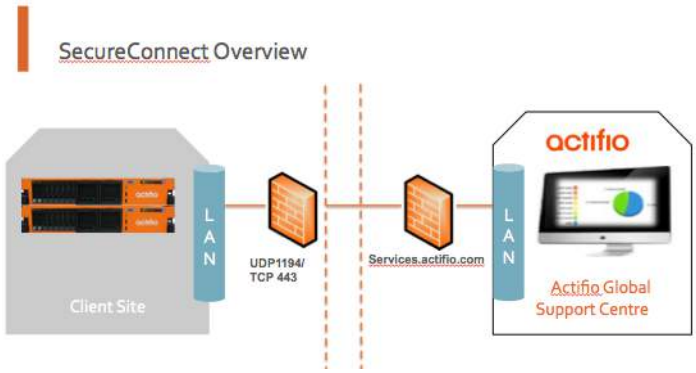
Yes. Call Home provides data, and SecureConnect provides access. Enabling SecureConnect without enabling Call Home allows Actifio Customer Support engineers to respond and investigate issues after you tell us a problem exists. Without Call Home, Actifio Customer Support has no way to know of problems 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 Desktop, 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

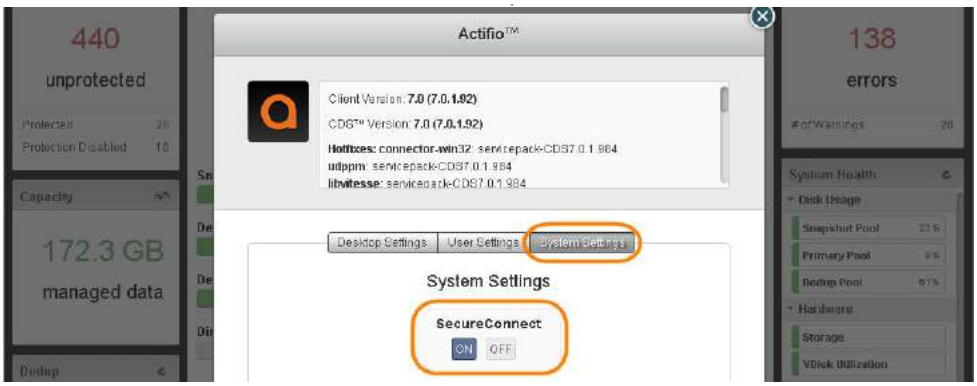
Actifio SecureConnect requires a UDP connection over port 1194 **from** CDS (Node 1) or the Sky IP address **to** secureconnect2.actifio.com and a setting of "any" IP address. SecureConnect is a strong 2048-bit RSA mutually authenticated service not subject to redirection or man-in-the-middle attacks. If you cannot use 'any', then contact Actifio Support.

Enabling Actifio SecureConnect

To enable SecureConnect mode:

1. Click the Software & Settings gear icon at the bottom of the Actifio Desktop.

2. The Desktop Settings window opens. Click the **System Settings** tab.
3. Set SecureConnect to **ON**.



Index

R

S

T

V

W

Y

Z