Network Administrator's Guide to Actifio GO

Updated August 24, 2023

Actifio GO

Actifio VDP 10.0

Copyright, Trademarks, and other Legal Matter

Copyright © 2022 Google LLC. All rights reserved.

Actifio™, OnVault™, and VDP™ are trademarks of Google LLC.

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

Contents

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: ActifioGO-CS@google.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

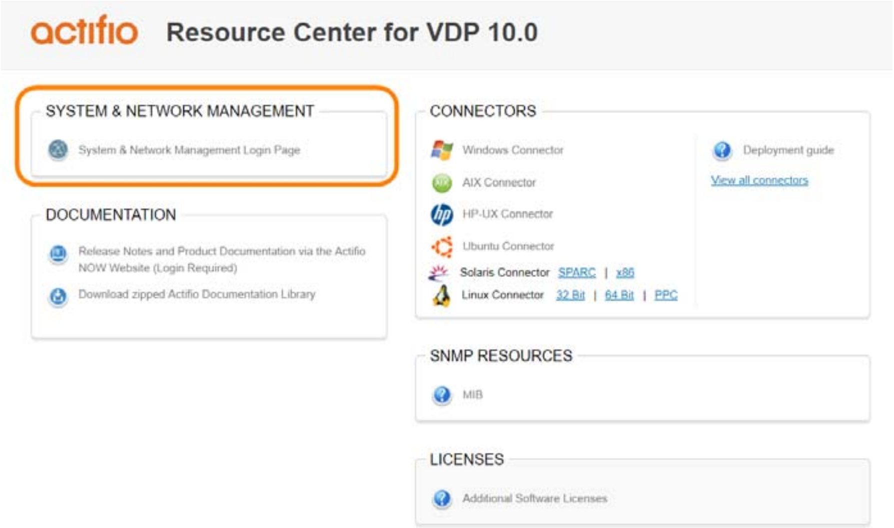
1 Modifying Your Network Configuration Settings

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 4
- Perform Network Troubleshooting on page 6
- Create and modify Host Resolution on page 7
- Configure Self Service Network for Actifio Sky Appliances in the Cloud on page 8

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 Google Cloud, see Configure Self Service Network for Actifio Sky Appliances in the Cloud on page 8.


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

Accessing the System & Network Management Tools

DNS and NTP

Enter this information:

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

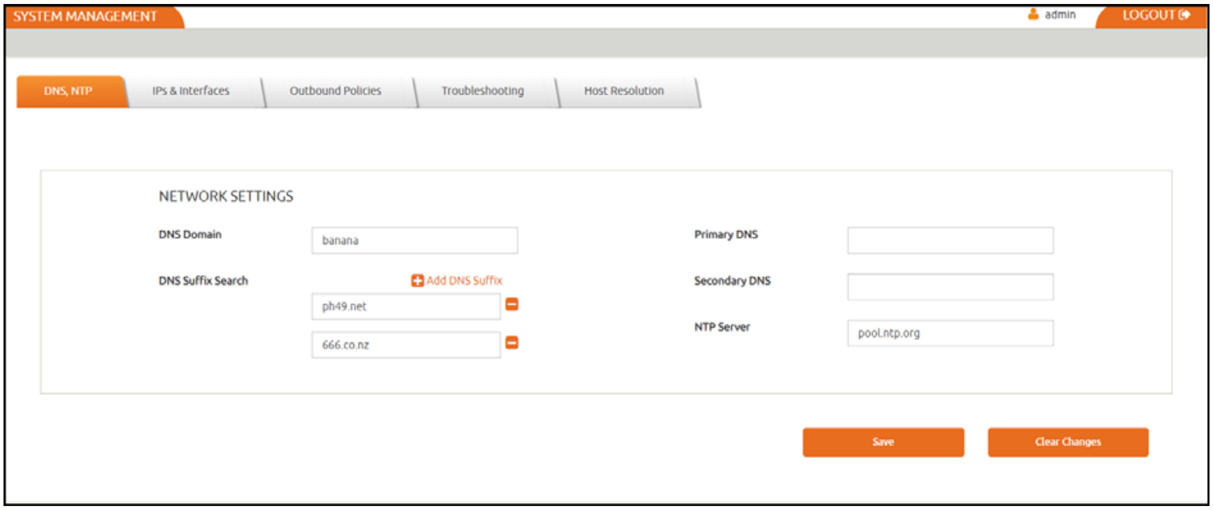
If you have additional hosts on other domains, you can set up a **DNS Suffix Search** to ensure the Actifio Appliance can find them by their short names.

> ***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.

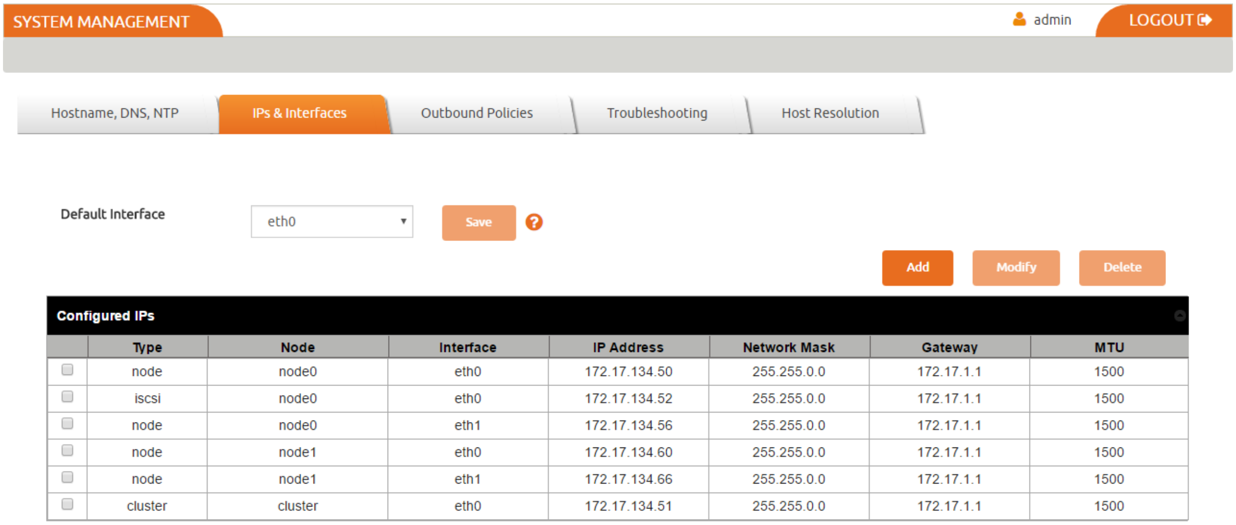


DNS Domain	banana
DNS Suffix Search	ph49.net 666.co.nz
Primary DNS	
Secondary DNS	
NTP Server	pool.ntp.org

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.



Default Interface: eth0

Configured IPs

	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

IPs and Interfaces

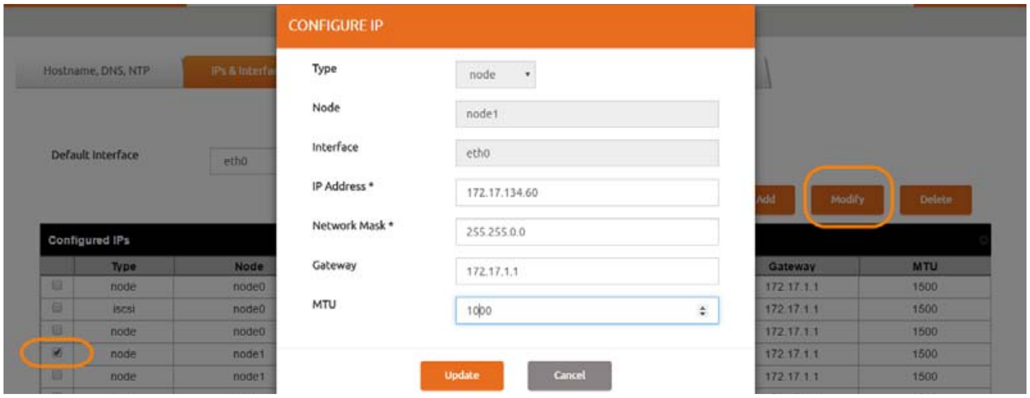
Configuring a Default Interface

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



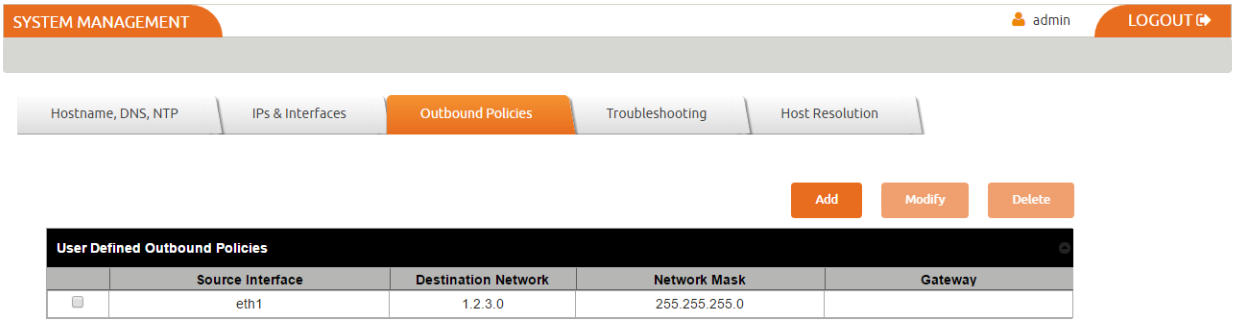
Type: node
Node: node1
Interface: eth0
IP Address *: 172.17.134.60
Network Mask *: 255.255.0.0
Gateway: 172.17.1.1
MTU: 1000

Modifying the MTU for eth0 of Node1

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.



User Defined Outbound Policies

	Source Interface	Destination Network	Network Mask	Gateway
□	eth1	1.2.3.0	255.255.255.0	

Outbound Policies

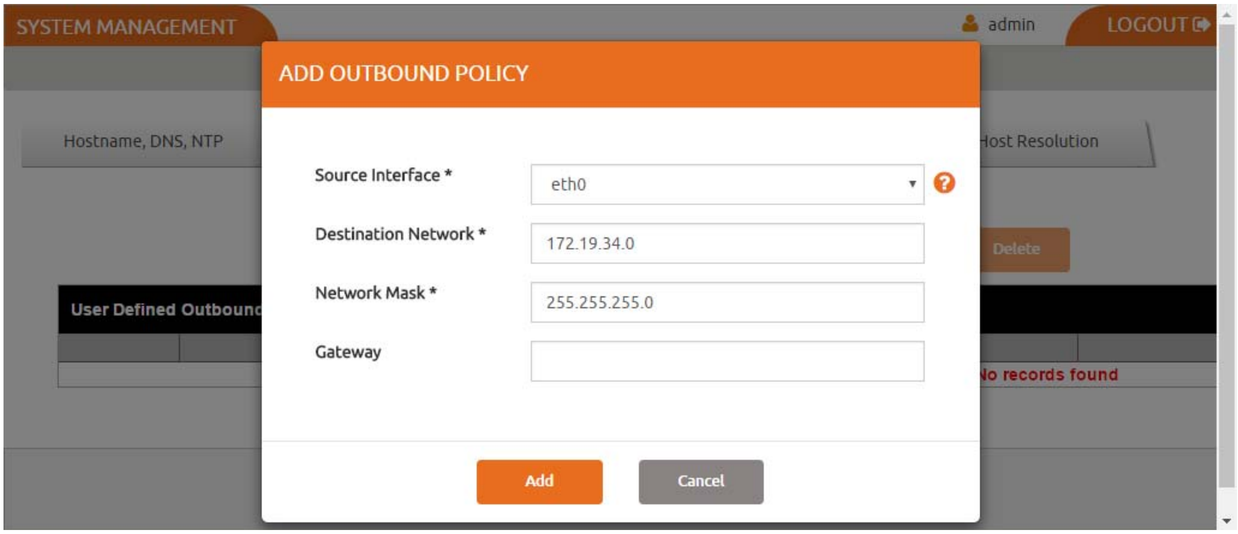
To modify an outbound policy:

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.



Source Interface * eth0

Destination Network * 172.19.34.0

Network Mask * 255.255.255.0

Gateway

Adding an Outbound Policy

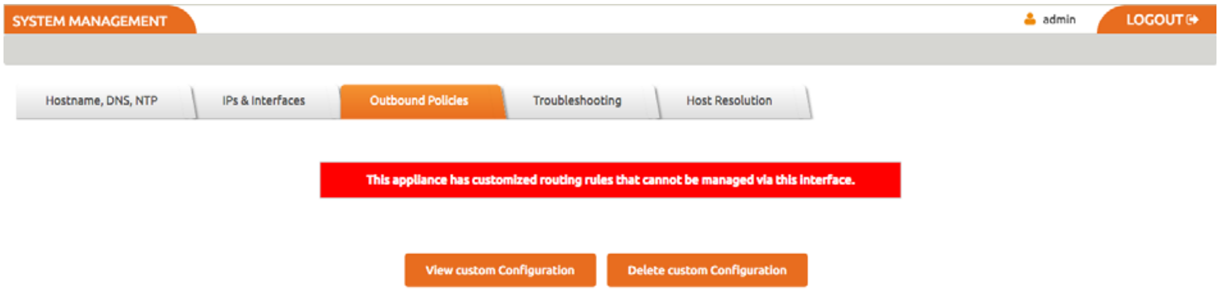
Outbound Policies and Custom Configurations

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.

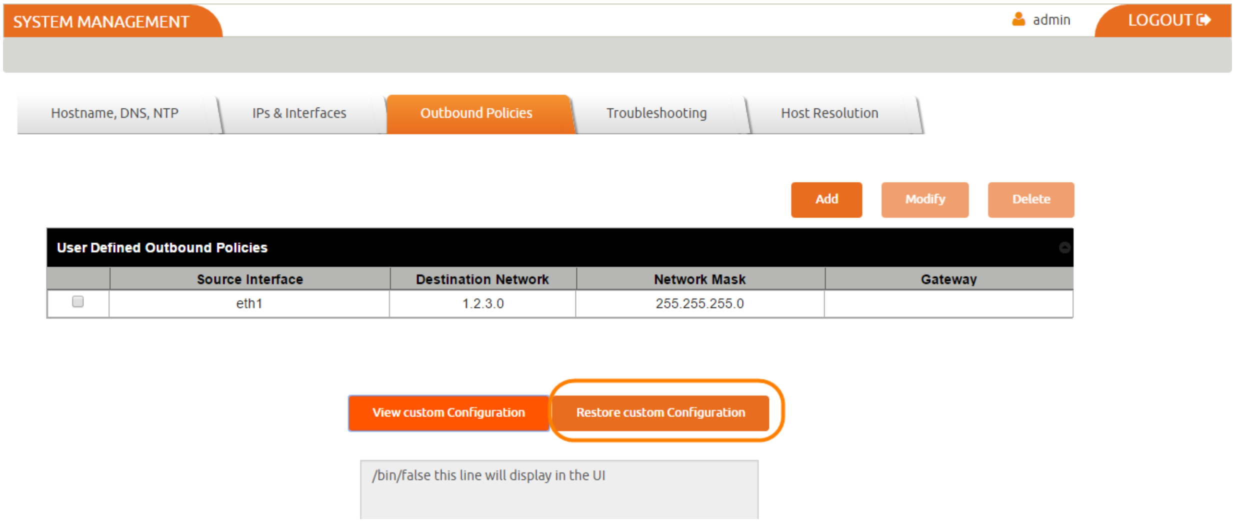
> ***Note:*** *Disabling a custom configuration may make the appliance unreachable.*



This appliance has customized routing rules that cannot be managed via this interface.

This Appliance has a Custom Configuration

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



User Defined Outbound Policies

	Source Interface	Destination Network	Network Mask	Gateway
□	eth1	1.2.3.0	255.255.255.0	

```
/bin/false this line will display in the UI
```

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 enter no value, then Outbound Policy rules are used to test 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

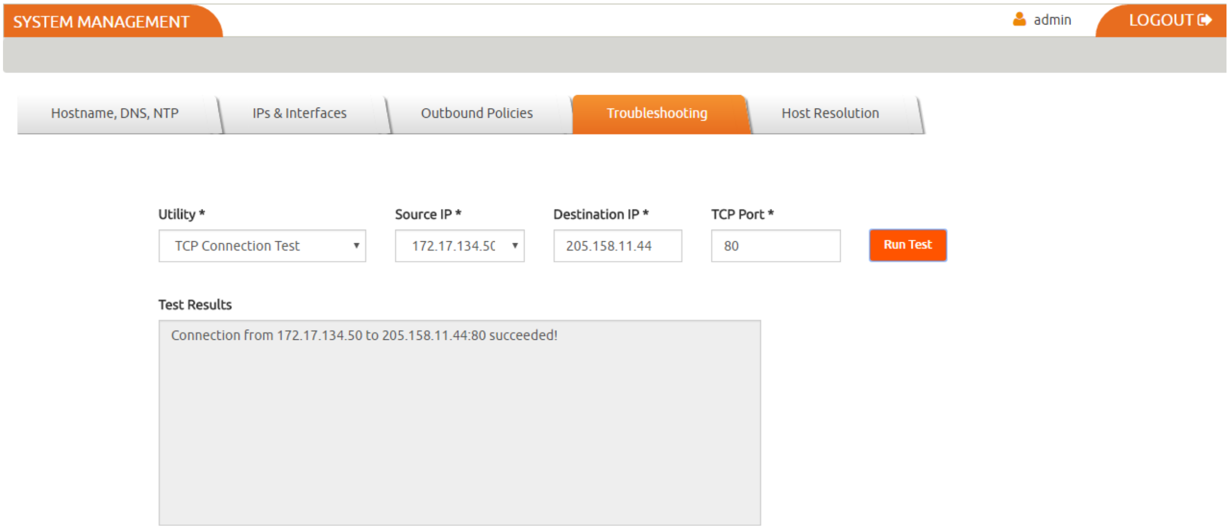
Example Traceroute result:

```
test/traceroute 8.8.8.8
1: dev134-86.dev.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
.
.
.
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.

- **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:



Utility *: TCP Connection Test
Source IP *: 172.17.134.5(
Destination IP *: 205.158.11.44
TCP Port *: 80

Test Results

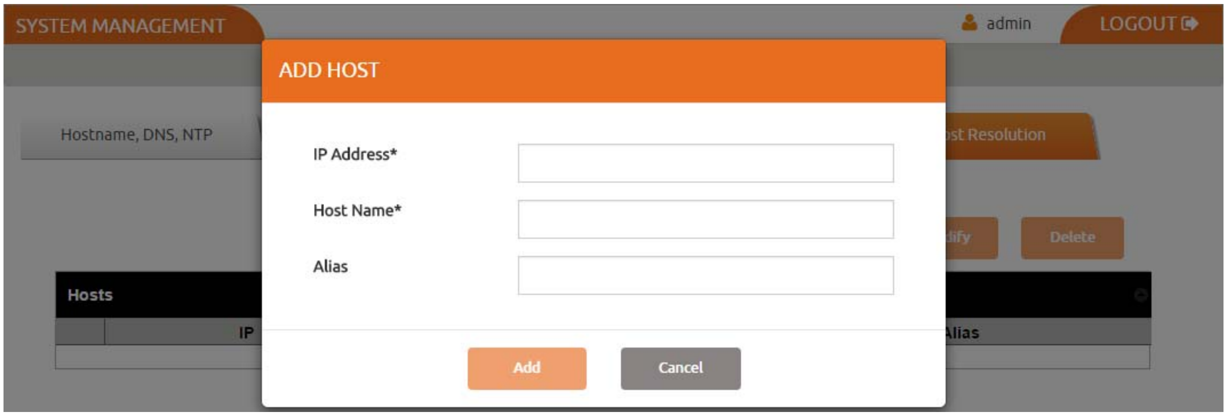
```
Connection from 172.17.134.50 to 205.158.11.44:80 succeeded!
```

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.

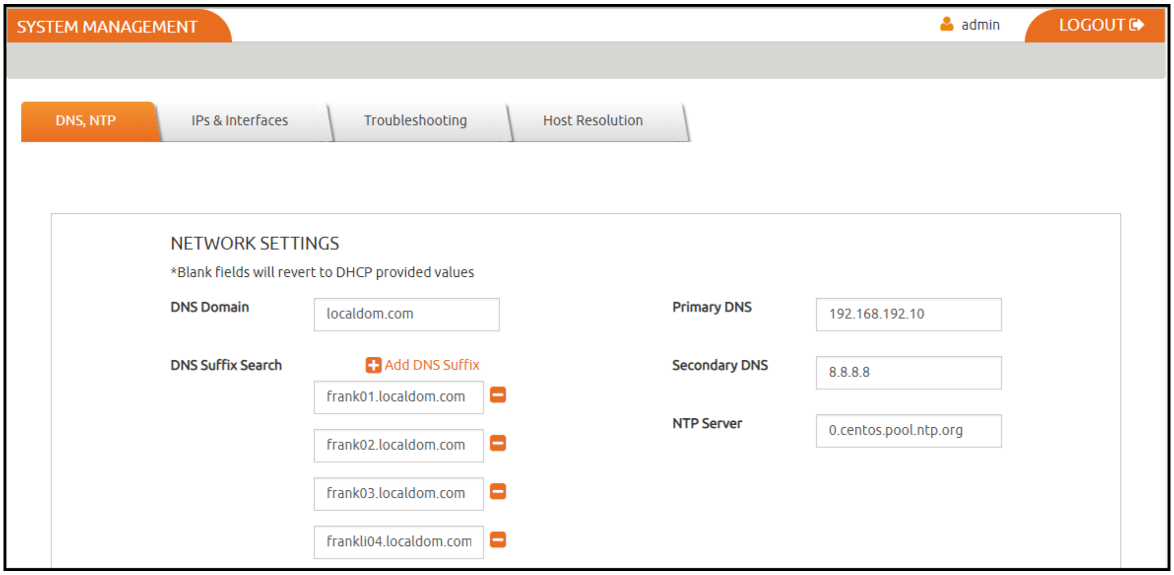
Note you cannot define a single hostname with multiple IP addresses, as the Management Panel will not allow you to do this. Even if it allowed more than one IP address to be added for the same hostname, only the first IP address would ever be used as this how name resolution with the /etc/hosts file 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.



NETWORK SETTINGS

*Blank fields will revert to DHCP provided values

DNS Domain: localdom.com

DNS Suffix Search: frank01.localdom.com, frank02.localdom.com, frank03.localdom.com, frankli04.localdom.com

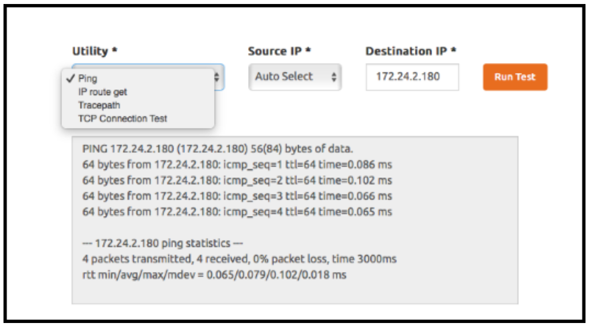
Primary DNS: 192.168.192.10

Secondary DNS: 8.8.8.8

NTP Server: 0.centos.pool.ntp.org

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 6.



Destination IP: 172.24.2.180

```
PING 172.24.2.180 (172.24.2.180) 56(84) bytes of data.
64 bytes from 172.24.2.180: icmp_seq=1 ttl=64 time=0.086 ms
64 bytes from 172.24.2.180: icmp_seq=2 ttl=64 time=0.102 ms
64 bytes from 172.24.2.180: icmp_seq=3 ttl=64 time=0.066 ms
64 bytes from 172.24.2.180: icmp_seq=4 ttl=64 time=0.065 ms

--- 172.24.2.180 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3000ms
rtt min/avg/max/mdev = 0.065/0.079/0.102/0.018 ms
```

Network Troubleshooting

6. Click the **Host Resolution tab** to override DNS resolution for specific hosts. For more information, see Host Resolution on page 7.

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

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 14
Actifio Appliance Local Services on page 14
Traffic to and from the Actifio Appliance on page 14
Backup Traffic from the Actifio Appliance, Replication Traffic Between Appliances on page 15
Actifio Remote Support on page 16
Actifio Report Manager on page 16
Actifio Global Manager (AGM) on page 16
Resiliency Director on page 17

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 14.

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.

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 is the IP address of the Sky Appliance.

26 (TCP)	SSH	Admin workstation	Actifio Appliance IP	Service CLI access.
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.
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
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.

4045	tcp/udp			Network lock daemon
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	Encrypted control channel between Actifio Appliance and hosts running the Actifio Connector.

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 or OnVault.	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.

				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)
1194 (UDP)	OpenVPN	Sky Appliance IP	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.

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 Cloud	AGM	Data collection
		Resiliency Director Cloud	DR appliances	Recovery orchestration
		Resiliency Director Cloud	Cloud REST API endpoint	Security verification
TCP-5103	HTTPS			Used to establish secure session ID
		Resiliency Director Cloud	DR appliances	

4 About the Actifio Connector

This chapter describes the Actifio Connector, including Obtaining the Right Actifio Connector for Your Host on page 21 and Maintaining Connectors on Hosts on page 21. The Actifio Connector is a small-footprint process that you install on your hosts.

This section includes:

What Does the Connector Do?

Actifio Connectors:

- Discover and capture individual and groups of applications, including applications that cannot be snapped by VMware, such as Microsoft SQL Server clusters.
- 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.
- 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 job.

The Connector and the Network Environment

The Actifio Connector runs as the UDSAgent process, either UDSAgent.exe (Windows) or udsagent (Linux). 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 (Linux) 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.

- On Windows, exclude `C:\Windows\act`
- On Linux, 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 13, APPID Pre- and Post-Scripts for Scheduled Data Protection Jobs
- Chapter 14, Super Scripts for Workflows and On-Demand Data Access Jobs

Obtaining the Right Actifio Connector for Your Host

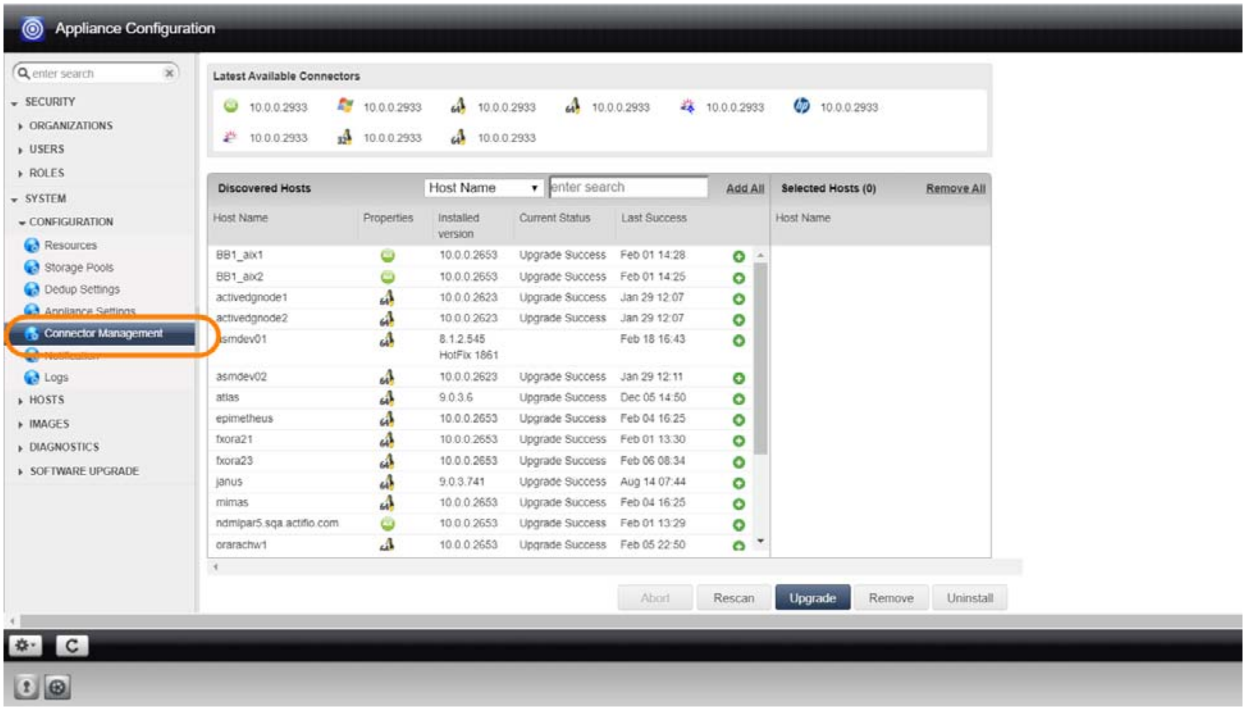
The Actifio Appliance comes with different connector installer files. Each is of a file type appropriate to its intended host type. You can download these with a web browser from the Actifio Resource Center; just open a browser to the IP address of the appliance.

- connector--Linux_x86-<version>.depot
- connector--Linux-<version>.depot
- connector-Linux_Ubuntu_amd64-latestversion.deb
- connector-win32-<version>.depot

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

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.



Host Name	Properties	Installed version	Current Status	Last Success
BB1_aix1		10.0.0.2653	Upgrade Success	Feb 01 14:28
BB1_aix2		10.0.0.2653	Upgrade Success	Feb 01 14:25
activedgnode1		10.0.0.2623	Upgrade Success	Jan 29 12:07
activedgnode2		10.0.0.2623	Upgrade Success	Jan 29 12:07
asmdev01		8.1.2.545 HotFix 1861		Feb 18 16:43
asmdev02		10.0.0.2623	Upgrade Success	Jan 29 12:11
atlas		9.0.3.6	Upgrade Success	Dec 05 14:50
epimetheus		10.0.0.2653	Upgrade Success	Feb 04 16:25
fxora21		10.0.0.2653	Upgrade Success	Feb 01 13:30
fxora23		10.0.0.2653	Upgrade Success	Feb 06 08:34
janus		9.0.3.741	Upgrade Success	Aug 14 07:44
mimas		10.0.0.2653	Upgrade Success	Feb 04 16:25
ndmipar5.sqa.actifio.com		10.0.0.2653	Upgrade Success	Feb 01 13:29
orarachw1		10.0.0.2653	Upgrade Success	Feb 05 22:50

2 Supporting VMware with Actifio VDP

This includes:

Actifio Sky Appliance Networking Requirements

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

- **Static IPs**: You must provide static IPs for the NIC on the Sky Appliance.
- **VMXNET3**: Sky Appliance must use the VMXNET3 Ethernet adapter. These adapters enable 10GB performance.

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.

Note: *For best iSCSI network traffic results, see* Ensuring iSCSI Connectivity on a Linux Host *on page 35.*

Each Sky Appliance can support up to 100 iSCSI sessions.

Ensuring iSCSI Connectivity from ESX to Storage

To test the iSCSI connection from an ESXi server to a Sky 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 iSCSI Connectivity with an ESX Server

This has two parts:

1. Adding the iSCSI Actifio Definition to the ESX server on page 12
2. Configuring AGM to See the ESXi Host on page 13

Before You Begin

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

- Check that the network ports are as described in ***Network Administrator's Guide to Actifio GO***.
- 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.

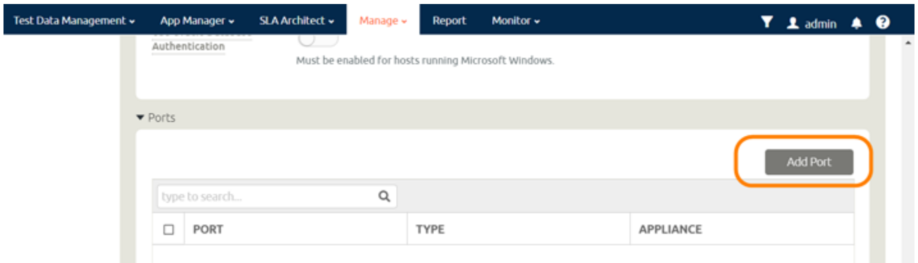
Adding the iSCSI Actifio Definition to the ESX server

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 ESXi Host on page 13.

Configuring AGM to See the ESXi Host

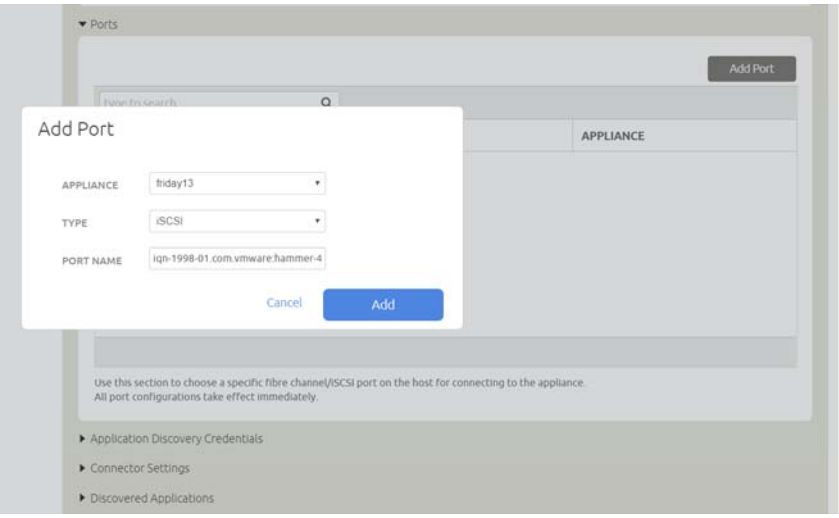
1. Open AGM to **Manage** > **Hosts**.
2. Right-click the ESXi server and select **Edit**.
3. Scroll down the right side to the Ports section and click **Add Port**.



Must be enabled for hosts running Microsoft Windows.

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.



APPLIANCE: friday13

TYPE: iSCSI

PORT NAME: iqn-1998-01.com.vmware:hammer-4

Use this section to choose a specific fibre channel/iSCSI port on the host for connecting to the appliance.
All port configurations take effect immediately.

Adding the Port

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

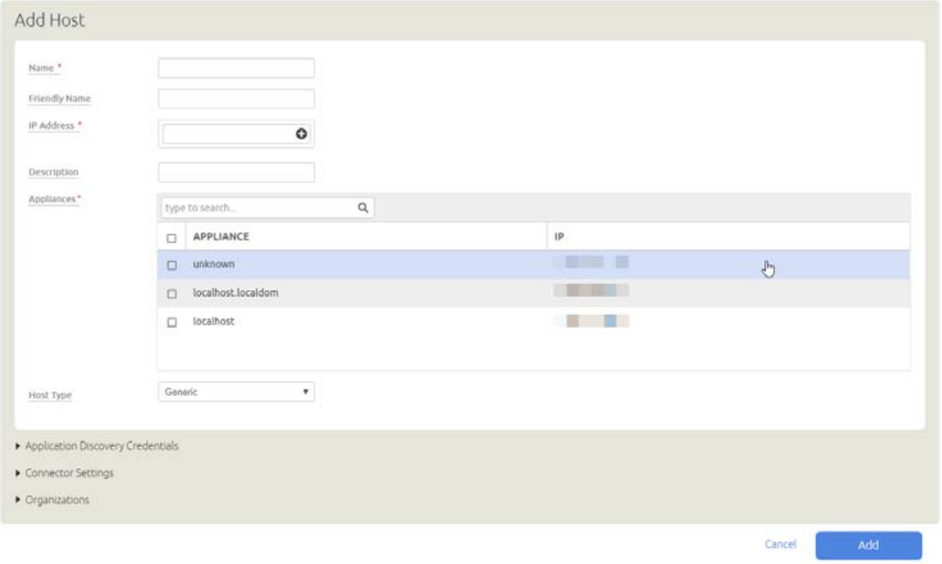
To set NFS datastore support on VM:

- 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.



Add Host

Name *

Friendly Name

IP Address *

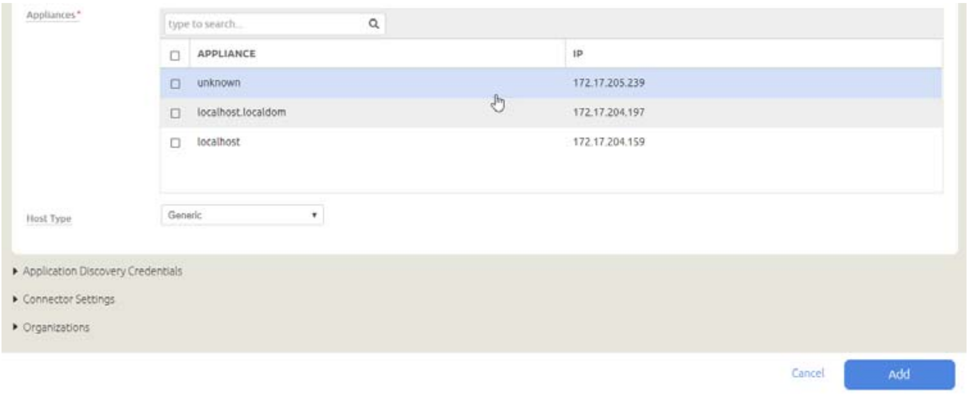
Description

Appliances *

□	APPLIANCE	IP
□	unknown	[redacted]
□	localhost.localdom	[redacted]
□	localhost	[redacted]

Host Type: Generic

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.



Appliances*

type to search...

□	APPLIANCE	IP
□	unknown	172.17.205.239
□	localhost.localdom	172.17.204.197
□	localhost	172.17.204.159

Host Type: Generic

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:

   - **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.
   - **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:** 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.

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 Servers with Actifio VDP

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

This chapter includes:

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 13, APPID Pre- and Post-Scripts for Scheduled Data Protection Jobs and Chapter 14, 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.*

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.

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 SQL Server applications and data, install the Actifio Connector with the Change Tracking Driver to enable efficient incremental backups.

Microsoft SQL Server VMs are supported on NTFS and ReFS volumes. 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 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 to auto upgrade the Actifio Connector on your hosts when new versions are available. Refer to Maintaining Connectors on Hosts on page 21.

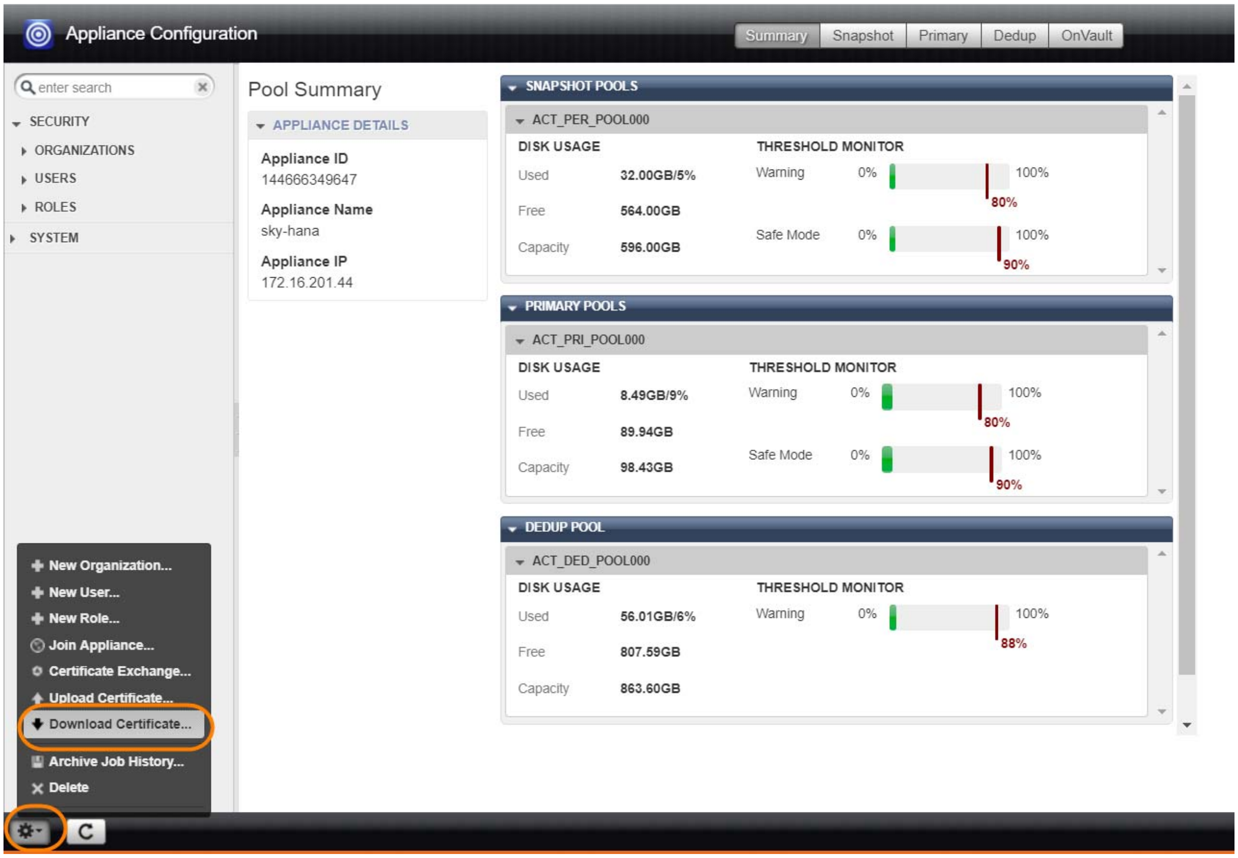
Restricting Windows Connector Communication to Specific Appliances

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 form 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**.



Pool Summary

APPLIANCE DETAILS

Appliance ID
144666349647

Appliance Name
sky-hana

Appliance IP
172.16.201.44

SNAPSHOT POOLS

ACT_PER_POOL000

DISK USAGE		THRESHOLD MONITOR			
Used	32.00GB/5%	Warning	0%	100%	80%
Free	564.00GB				
Capacity	596.00GB	Safe Mode	0%	100%	90%

PRIMARY POOLS

ACT_PRI_POOL000

DISK USAGE		THRESHOLD MONITOR			
Used	8.49GB/9%	Warning	0%	100%	80%
Free	89.94GB				
Capacity	98.43GB	Safe Mode	0%	100%	90%

DEDUP POOL

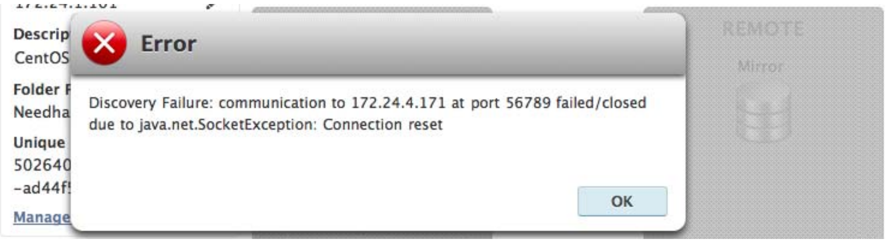
ACT_DED_POOL000

DISK USAGE		THRESHOLD MONITOR			
Used	56.01GB/6%	Warning	0%	100%	88%
Free	807.59GB				
Capacity	863.60GB				

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.

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



Error

Discovery Failure: communication to 172.24.4.171 at port 56789 failed/closed due to java.net.SocketException: Connection reset

To Unrestrict a Restricted Windows Connector

1. Delete the certificate file from the host at `C:\Program Files\Actifio\certs\trusted\AuthorizedAppliance.crt`
2. Stop and start the connector (UDSAgent) using `services.msc`.
3. Repeat the test in Restricting Windows Connector Communication to Specific Appliances on page 31.

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 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 Linux with Actifio VDP

This chapter includes:

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 13, APPID Pre- and Post-Scripts for Scheduled Data Protection Jobs and Chapter 14, 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.*

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

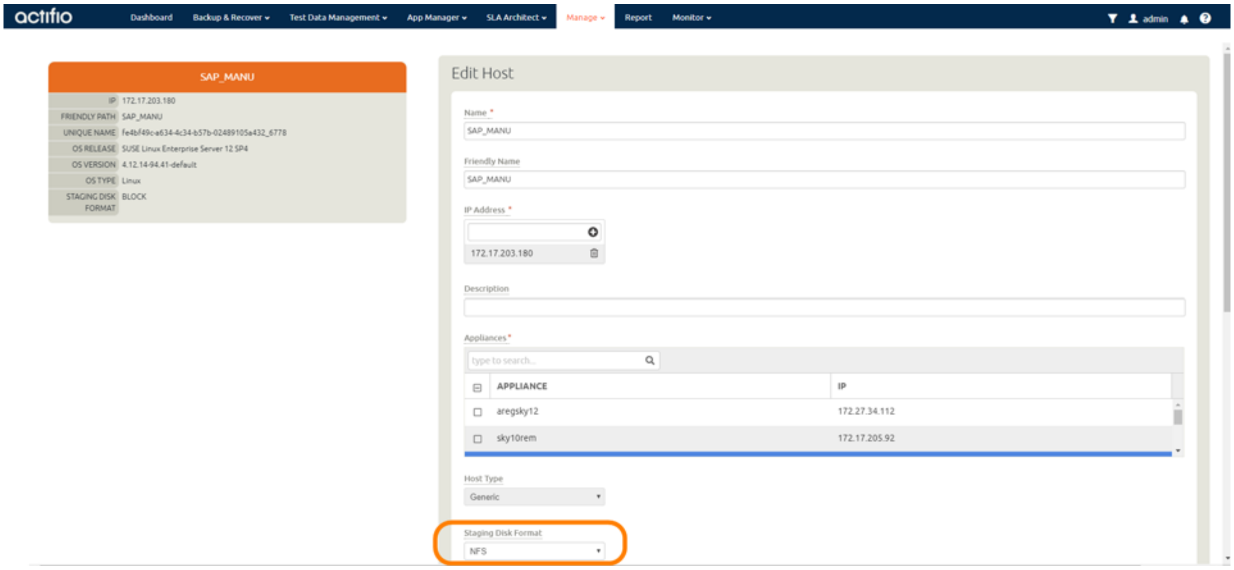
When VDP manages data movement over NFS, during each Snapshot, Dedup Async, or StreamSnap job, VDP uses an NFS share created on the appliance and exports to the Linux host a copy of application data.

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.



SAP_MANU

IP	172.17.203.180
FRIENDLY PATH	SAP_MANU
UNIQUE NAME	fe4bf49c-a634-4c34-b57b-02489105a432_6778
OS RELEASE	SUSE Linux Enterprise Server 12 SP4
OS VERSION	4.12.14-94.41-default
OS TYPE	Linux
STAGING DISK FORMAT	BLOCK

Edit Host

Name *: SAP_MANU

Friendly Name: SAP_MANU

IP Address *: 172.17.203.180

Description:

Appliances *

	APPLIANCE	IP
□	aregsky12	172.27.34.112
□	sky10rem	172.17.205.92

Host Type: Generic

Staging Disk Format: NFS

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 Transport	over NFS data store	ESX server	vmdk
SAN Transport	to the iSCSI initiator or to Fibre Channel	ESX server	raw device mapping
SAN to Guest	to the iSCSI initiator	Guest VM	ESX is bypassed
NFS to Guest	as NFS shares	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@myrhel72 ~]# 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 myrhel72 udsagent.init[29568]: Starting /opt/act/bin/udsag...n
Apr 05 02:10:07 myrhel72 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:

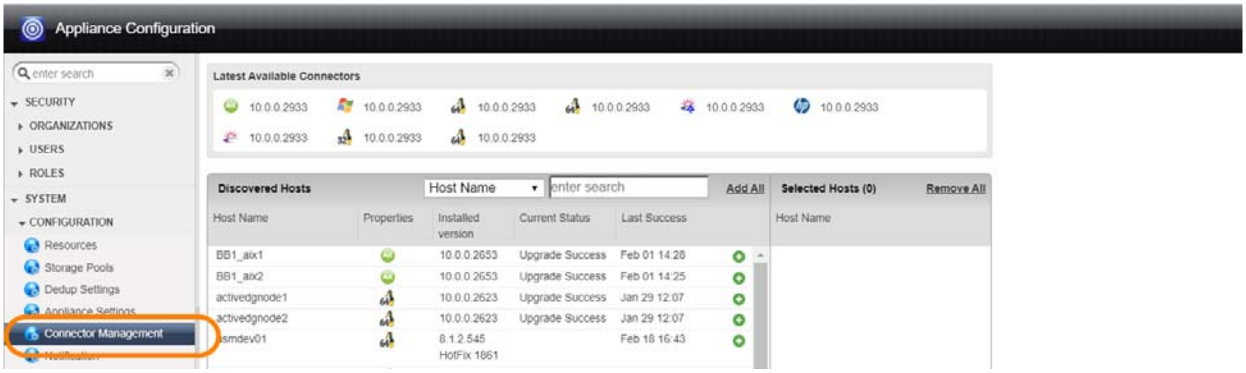
   ```
   [oregon@vq-oregon ~]$ rpm -qa udsagent
   ```

   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 .



Host Name	Properties	Installed version	Current Status	Last Success
BB1_aix1		10.0.0.2653	Upgrade Success	Feb 01 14:28
BB1_aix2		10.0.0.2653	Upgrade Success	Feb 01 14:25
activedgnode1		10.0.0.2623	Upgrade Success	Jan 29 12:07
activedgnode2		10.0.0.2623	Upgrade Success	Jan 29 12:07
smdev01		8.1.2.545 HotFix 1861		Feb 18 16:43

Connector Management

8 Adding Your Hosts to an Actifio Appliance

These are the steps to connecting a host to your VDP system.

Table 1: Connecting Hosts

Host	Install the Connector	Add the Host
Windows Server,	Installing the Actifio Connector on Microsoft Windows Hosts on page 30	Chapter 10, Adding Windows Server Hosts to AGM
Linux	Installing the Actifio Connector on a Linux Host on page 38	Chapter 9, Adding Linux Hosts to AGM
VMware VMs	***A VMware Administrator's Guide to Actifio Copy Data Management***	

The next steps are:

1. Configuring Hosts to Auto-Discover their Applications on page 42.
2. Reconciling Inconsistent Host Information across Multiple Appliances on page 43

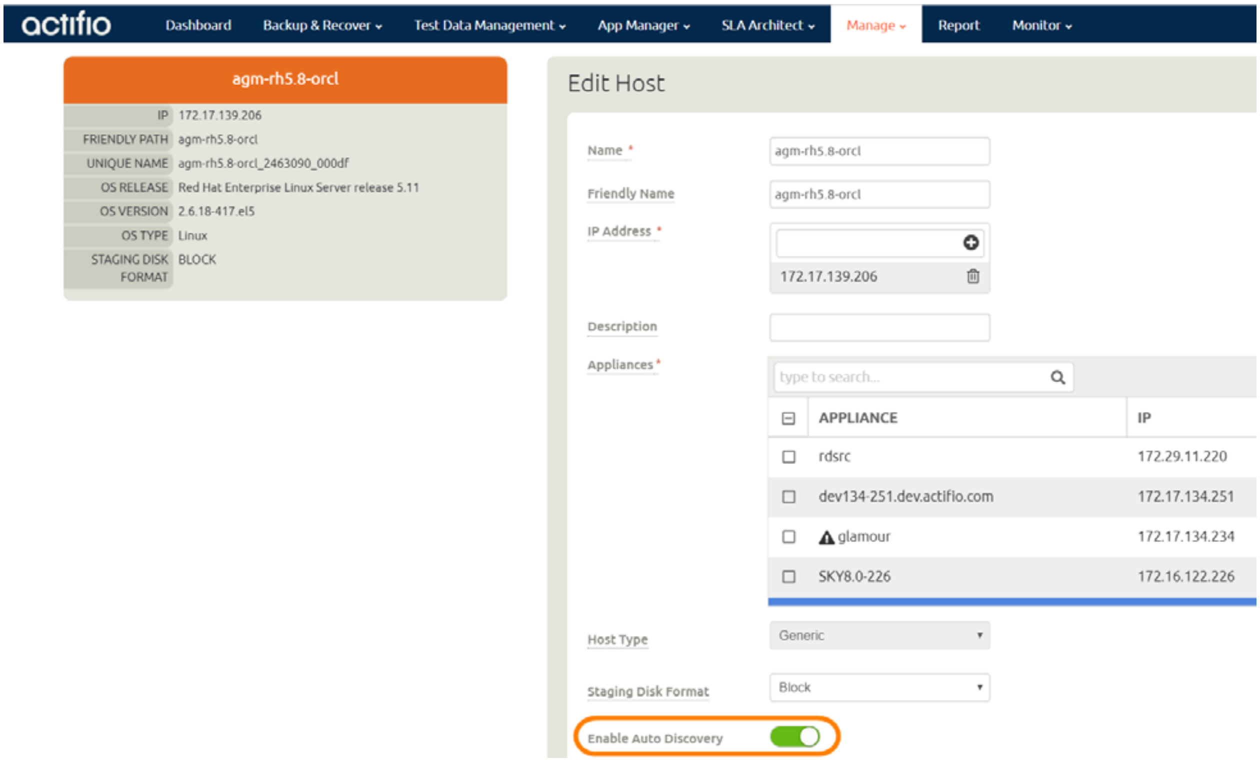
If you no longer want to protect the applications or VMs on a host, you can delete it from VDP management; see Deleting Hosts Using the AGM on page 43.
You can have pre- and post-scripts run on your applications and VMs when they are triggered by a VDP job. Scripting is detailed in Chapter 13, APPID Pre- and Post-Scripts for Scheduled Data Protection Jobs and in Chapter 14, 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****.*

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. Side the **Enable Auto Discovery** button to the right and click **Save** in the lower right corner.



agm-rh5.8-orcl

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
STAGING DISK FORMAT	BLOCK

Edit Host

Name * agm-rh5.8-orcl

Friendly Name agm-rh5.8-orcl

IP Address * 172.17.139.206

Description

Appliances * type to search...

⊟	APPLIANCE	IP
□	rdsrc	172.29.11.220
□	dev134-251.dev.actifio.com	172.17.134.251
□	⚠ glamour	172.17.134.234
□	SKY8.0-226	172.16.122.226

Host Type Generic

Staging Disk Format Block

Enable Auto Discovery

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.

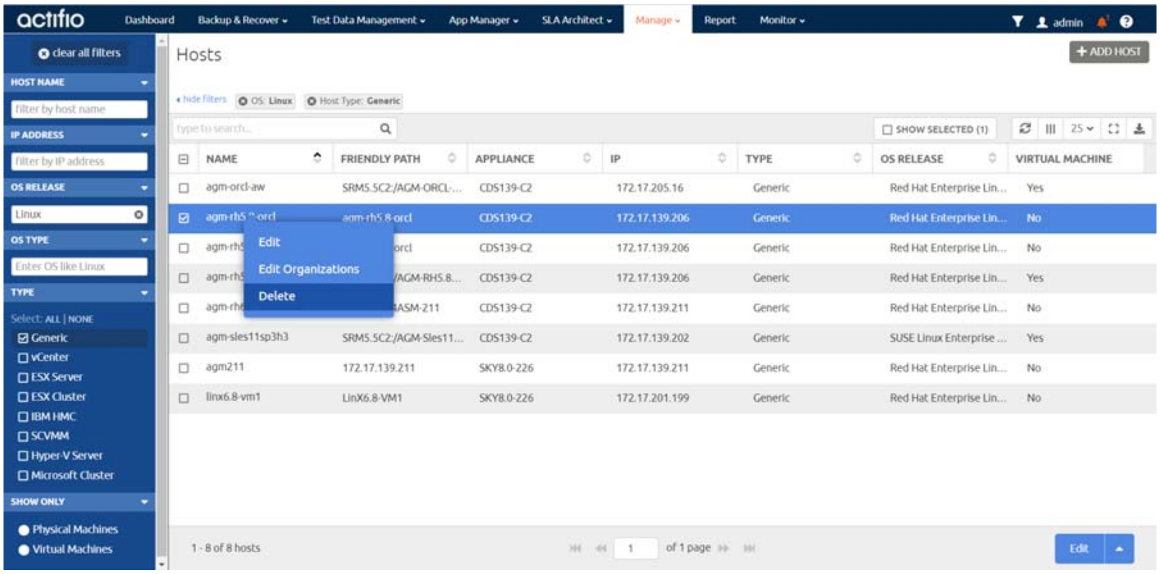
Security Software on Hosts

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 20.

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**.



☐	NAME	FRIENDLY PATH	APPLIANCE	IP	TYPE	OS RELEASE	VIRTUAL MACHINE
☐	agm-orcl-aw	SRM5.5C2:/AGM-ORCL-...	CDS139-C2	172.17.205.16	Generic	Red Hat Enterprise Lin...	Yes
☑	agm-rh5 "-orcl	agm-rh5.8-orcl	CDS139-C2	172.17.139.206	Generic	Red Hat Enterprise Lin...	No
☐	agm-rh5	orcl	CDS139-C2	172.17.139.206	Generic	Red Hat Enterprise Lin...	No
☐	agm-rh5	/AGM-RH5.8...	CDS139-C2	172.17.139.206	Generic	Red Hat Enterprise Lin...	Yes
☐	agm-rh6	ASM-211	CDS139-C2	172.17.139.211	Generic	Red Hat Enterprise Lin...	No
☐	agm-sles11sp3h3	SRM5.5C2:/AGM-Sles11...	CDS139-C2	172.17.139.202	Generic	SUSE Linux Enterprise ...	Yes
☐	agm211	172.17.139.211	SKY8.0-226	172.17.139.211	Generic	Red Hat Enterprise Lin...	No
☐	linx6.8-vm1	LinX6.8-VM1	SKY8.0-226	172.17.201.199	Generic	Red Hat Enterprise Lin...	No

Deleting a Host from AGM

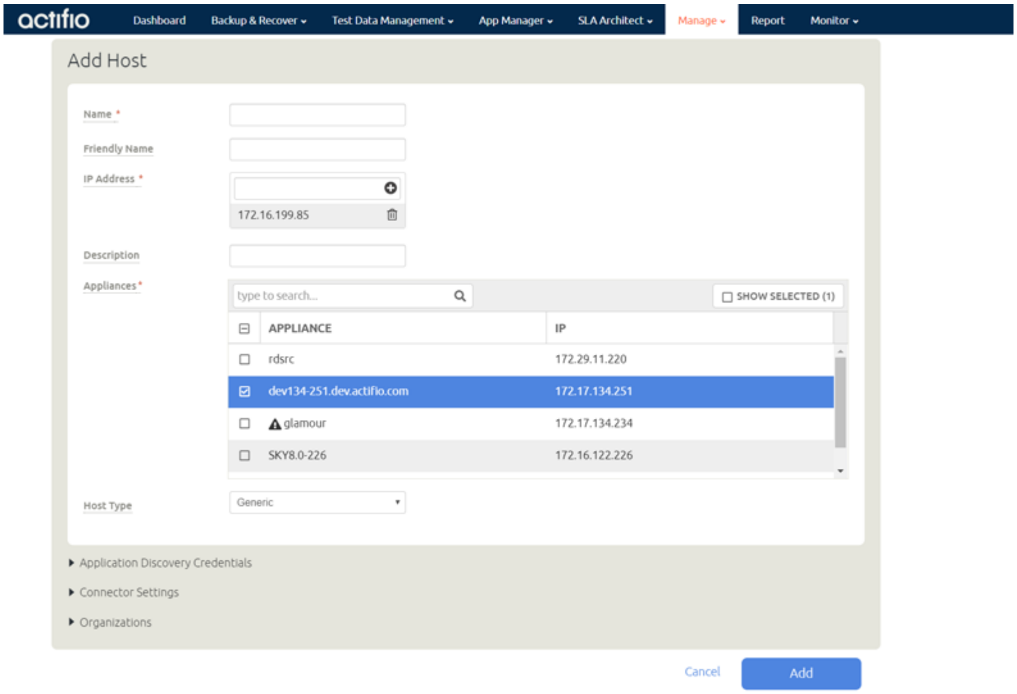
9 Adding Linux Hosts to AGM

To add a Linux 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**.



Name *

Friendly Name

IP Address * 172.16.199.85

Description

Appliances *

	APPLIANCE	IP
□	rdsrc	172.29.11.220
☑	dev134-251.dev.actifio.com	172.17.134.251
□	glamour	172.17.134.234
□	SKY8.0-226	172.16.122.226

Host Type: Generic

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**.

10 Adding Windows Server Hosts to AGM

To add a new Windows Server 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 47.

   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	Generic	The default connector port for Generic hosts and SCVMM is 5106. If you use a different port, enter it here. If the Connector username and password have changed, then change them here. 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

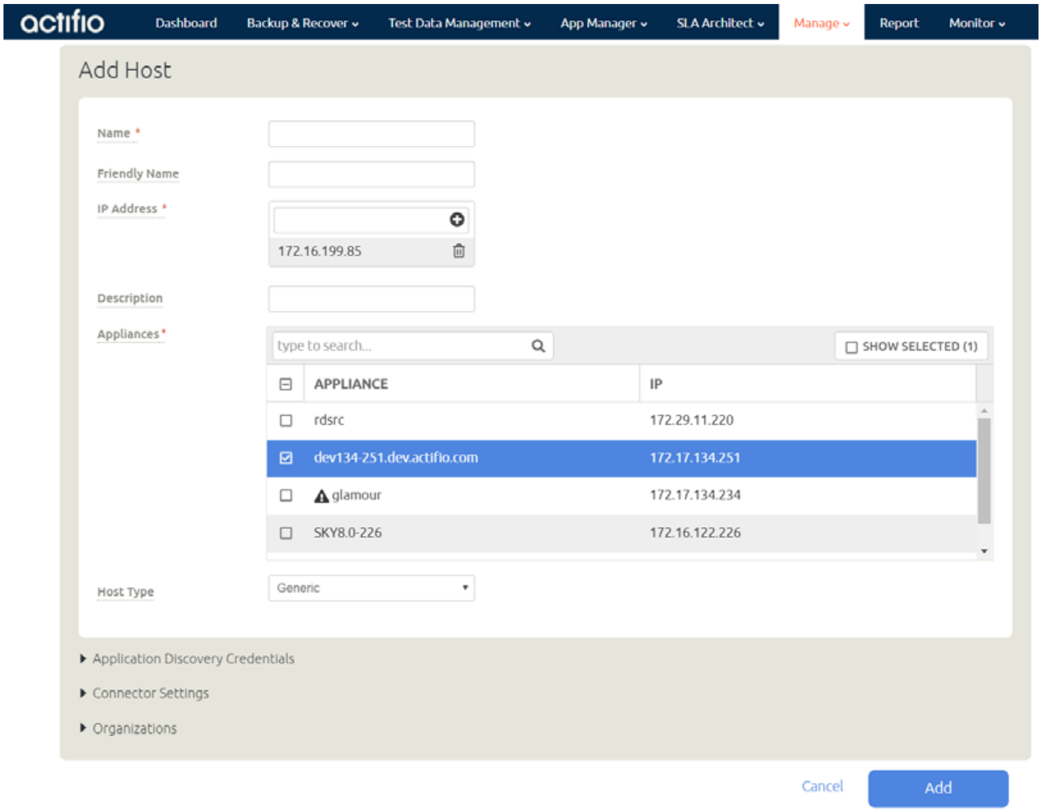
To Protect	Select Host Type	Connection Type
vCenter with ESXi VMs	vCenter	A vCenter can have both vCenter Settings and Connector Settings, because a vCenter might also have the Actifio Connector installed on it. The default vCenter management port is 443. If you use a different port, then enter it here.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

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**.



Add Host

Name *

Friendly Name

IP Address *

172.16.199.85

Description

Appliances *

type to search...

□ SHOW SELECTED (1)

⊟	APPLIANCE	IP
□	rdsrc	172.29.11.220
☑	dev134-251.dev.actifio.com	172.17.134.251
□	⚠ glamour	172.17.134.234
□	SKY8.0-226	172.16.122.226

Host Type: Generic

▸ Application Discovery Credentials

▸ Connector Settings

▸ Organizations

Cancel Add

Adding a New Host

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

This chapter details:

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 an OnVault pool or in a remote Actifio appliance where data is sent using StreamSnap replication and stored in a regular or external snapshot pool.

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.
- 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:
  - o The storage array administrator has provisioned an empty mdiskpool for use by the Sky appliance.
  - o 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:
   - Use the slider to set the Warning level. The default Warning level is 80%. When this level is exceeded, you see warnings.
   - 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:

- Use the slider to set the Warning level. The default Warning level is 80%. When this level is exceeded, you see warnings.
- 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.

12 Configuring LDAP and Role-Based Access

This chapter details:

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

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:
    - 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.
    - 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.
    - 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.*

    - 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.
    - Password: Password for the lookup user.
    - Search by Base DN: The base distinguished name (DN) subtree that is used by AGM to search for user and group entries.
    - Search by Username Attribute: The LDAP attribute to use to match against the supplied login name.
    - 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.
    - 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

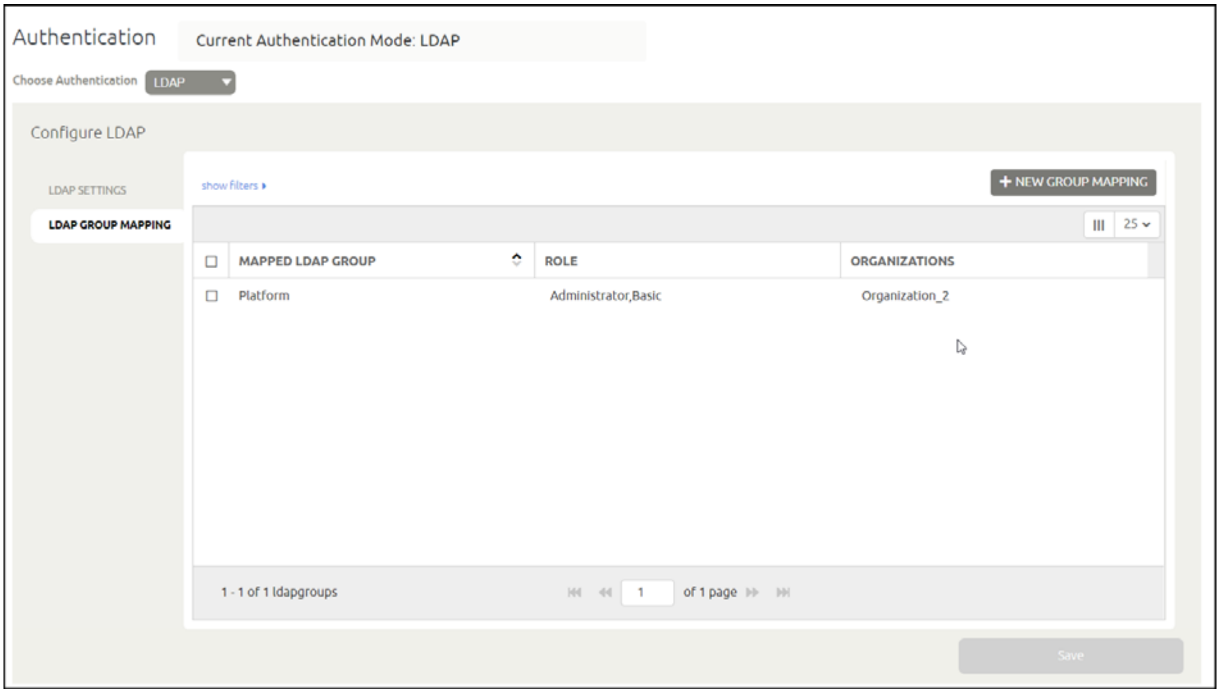
After your have configured your LDAP settings, you can set up group mapping. You can create a mapping by associating an LDAP Group with a role.

Before you begin:

- You must have the Administrative role to perform LDAP group mapping. If 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.



□	MAPPED LDAP GROUP	ROLE	ORGANIZATIONS
□	Platform	Administrator,Basic	Organization_2

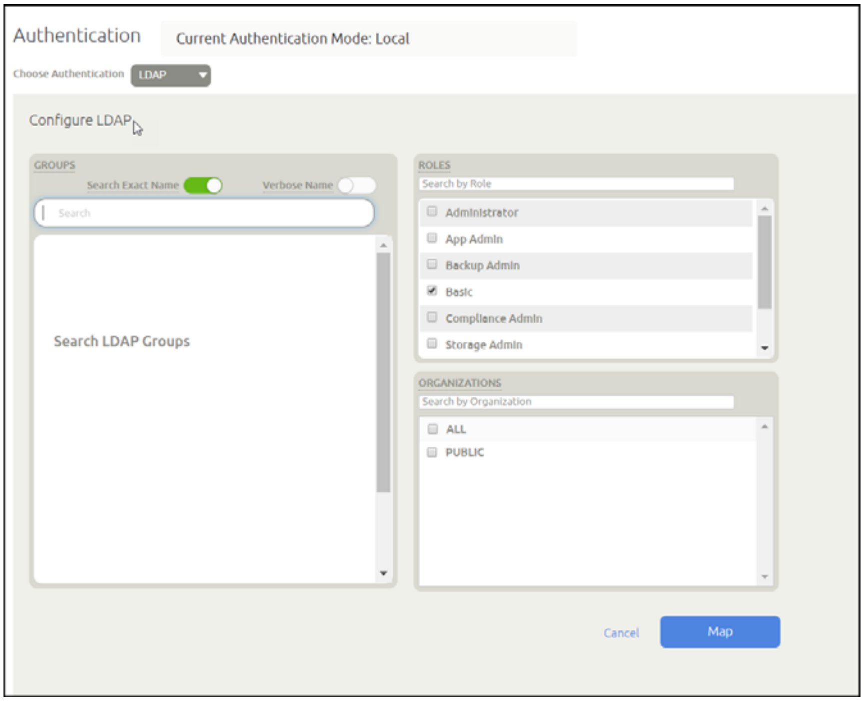
4. Depending on whether you want to edit an existing LDAP group or create a new LDAP group:
   - To modify an existing LDAP group, select the LDAP group from the list and then select Edit (bottom right-hand corner of the window).
   - To create a new LDAP group, click New Group Mapping.

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

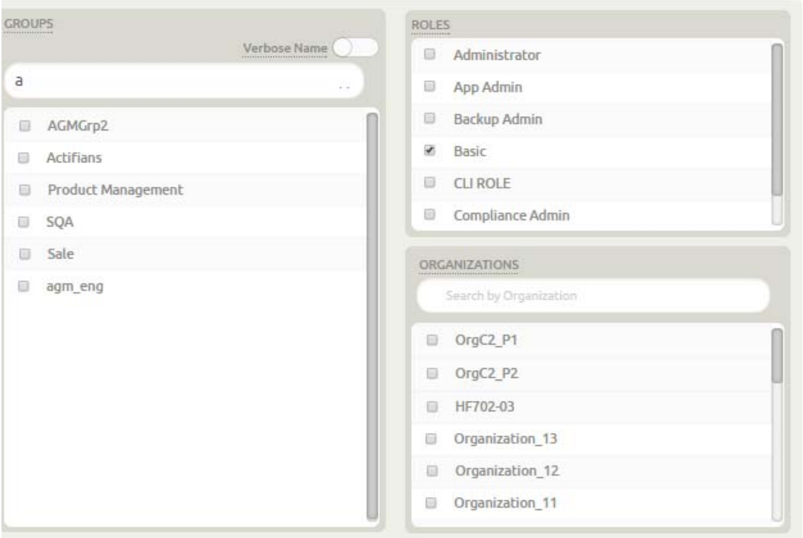
- o Mapped LDAP Group
- o Role
- o Organizations

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:
    - The roles in the Roles list to map the LDAP group to the specific role(s).
    - 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:
    - Update, if modifying an existing LDAP group
    - 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.*

- 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).
- 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).

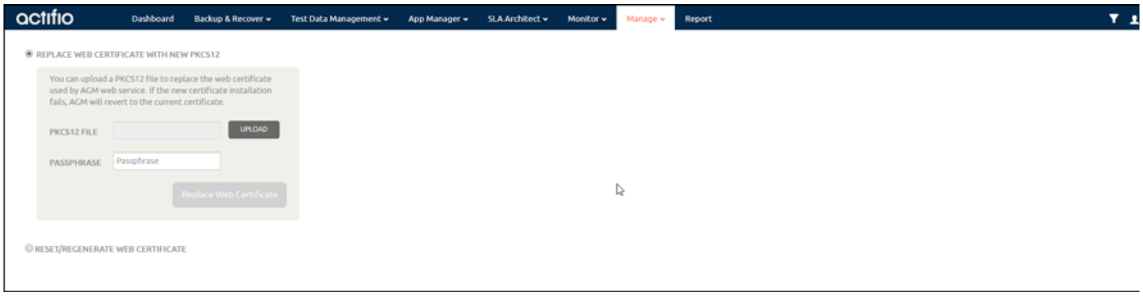
Note: *You can also right-click on the LDAP group in the list and select Delete from the menu.*

5. Click Confirm in the confirmation dialog.

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 59
- Reset and Generate New Web Certificate on page 60



You can upload a PKCS12 file to replace the web certificate used by AGM web service. If the new certificate installation fails, AGM will revert to the current certificate.

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.

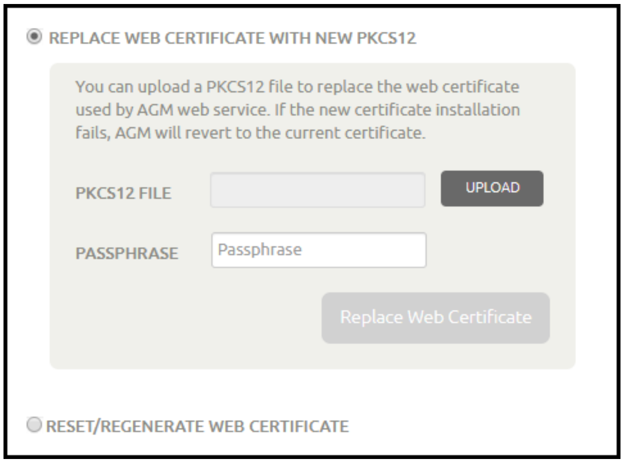
Requirements:

- 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:

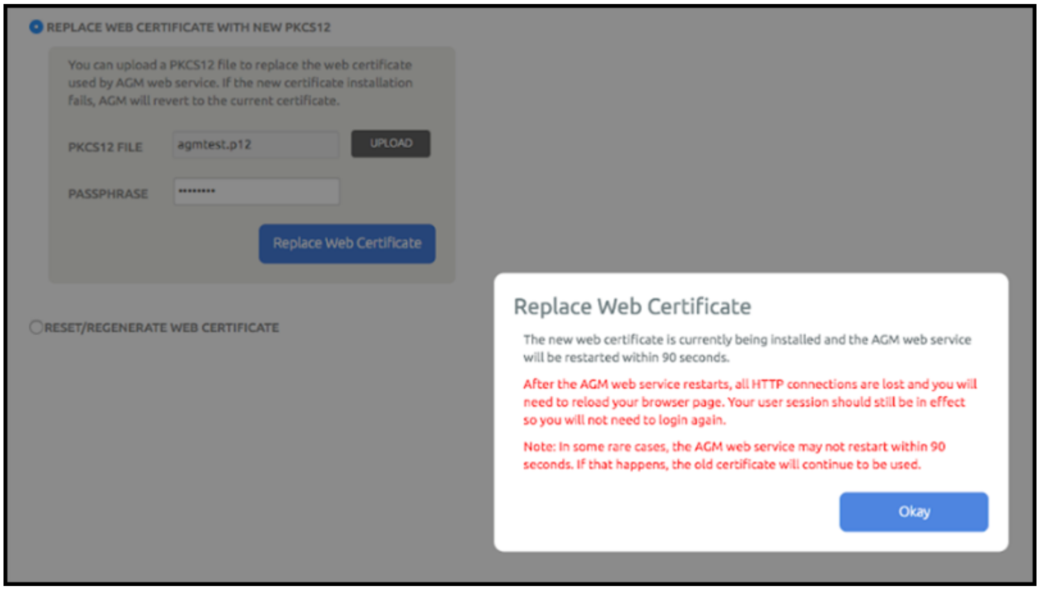
1. Click the Manage tab and select Web Certificate from the drop-down menu. The Web Certificates management page opens listing options to upload a PKCS file (default) or generate and replace a self-signed certificate.


● REPLACE WEB CERTIFICATE WITH NEW PKCS12
PKCS12 FILE
UPLOAD
PASSPHRASE
Passphrase
Replace Web Certificate
○ RESET/REGENERATE WEB CERTIFICATE

You can upload a PKCS12 file to replace the web certificate used by AGM web service. If the new certificate installation fails, AGM will revert to the current 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.



● REPLACE WEB CERTIFICATE WITH NEW PKCS12

You can upload a PKCS12 file to replace the web certificate used by AGM web service. If the new certificate installation fails, AGM will revert to the current certificate.

PKCS12 FILE: agmtest.p12 UPLOAD

PASSPHRASE: ••••••••

Replace Web Certificate

○ RESET/REGENERATE WEB CERTIFICATE

Replace Web Certificate

The new web certificate is currently being installed and the AGM web service will be restarted within 90 seconds.

After the AGM web service restarts, all HTTP connections are lost and you will need to reload your browser page. Your user session should still be in effect so you will not need to login again.

Note: In some rare cases, the AGM web service may not restart within 90 seconds. If that happens, the old certificate will continue to be used.

Okay

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.*

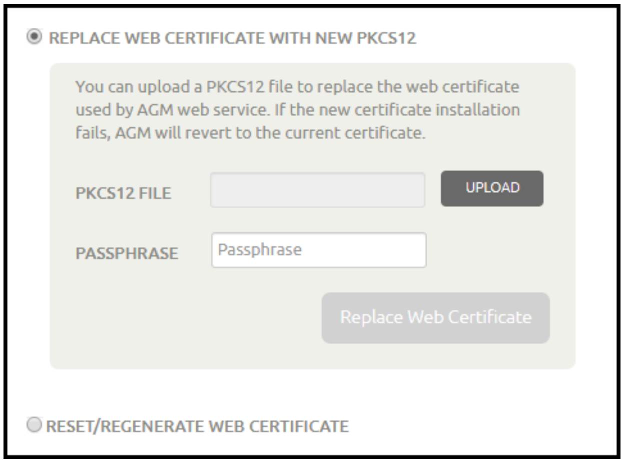
6. Upload a valid PKCS file using instructions in steps 3 to 6. The certificate is replaced and the web service restarts within one hundred and twenty (120) seconds.

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.



● REPLACE WEB CERTIFICATE WITH NEW PKCS12

You can upload a PKCS12 file to replace the web certificate used by AGM web service. If the new certificate installation fails, AGM will revert to the current certificate.

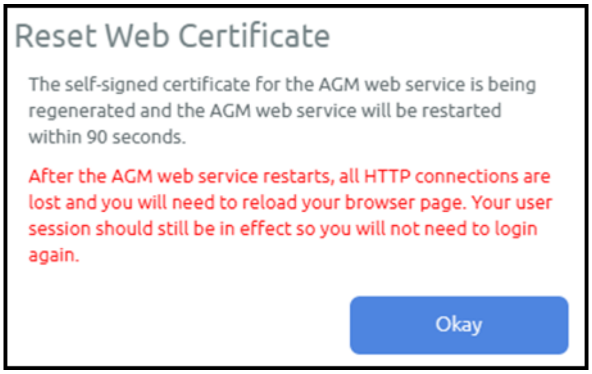
PKCS12 FILE: UPLOAD

PASSPHRASE: Passphrase

Replace Web Certificate

○ RESET/REGENERATE WEB CERTIFICATE

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



Reset Web Certificate

The self-signed certificate for the AGM web service is being regenerated and the AGM web service will be restarted within 90 seconds.

After the AGM web service restarts, all HTTP connections are lost and you will need to reload your browser page. Your user session should still be in effect so you will not need to login again.

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.

15 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.

Event notifications can be routed to a trap receiver.

This section describes:

Glossary of Event-Related Terms

These terms have specific meanings with regard to event notifications:

Component: Actifio appliance.

Error: 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: Least serious level of Event Notification severity, less serious than Warning or 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.

Clearable Events

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

Monitoring System Alerts

You can monitor job successes and failures directly in the System Monitor as described in Chapter 16, Monitoring Alerts in the AGM Events Monitor.

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:

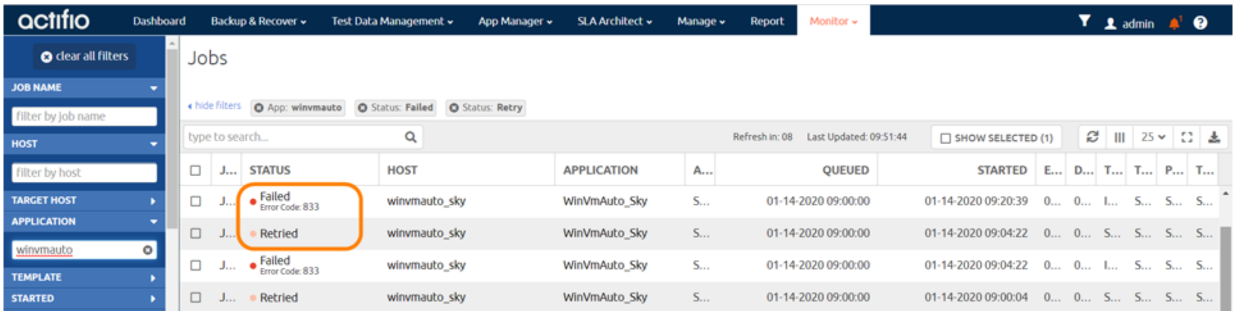
1. The job failure is reported by the Actifio appliance.
2. The monitoring software catches the failure, noting the error code for consolidation required.
3. Then the software makes a vSphere API call `reportsnaps` to query the size of the datastore.
    - If the datastore is small enough to consolidate 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 mkpolicyoption` 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`.
    - 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.

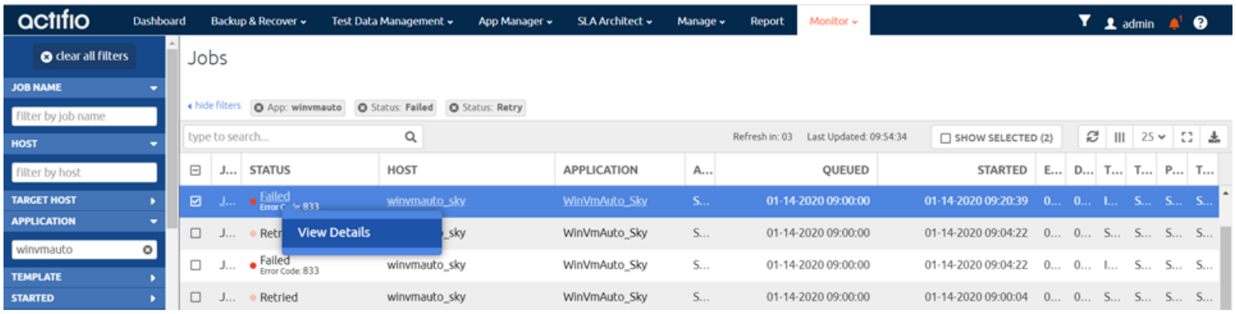
If the job ultimately fails (the SLA time window elapses before success) then that job gets **Failed** status in the System Monitor. At this time, a timeout event of type Error is posted.

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



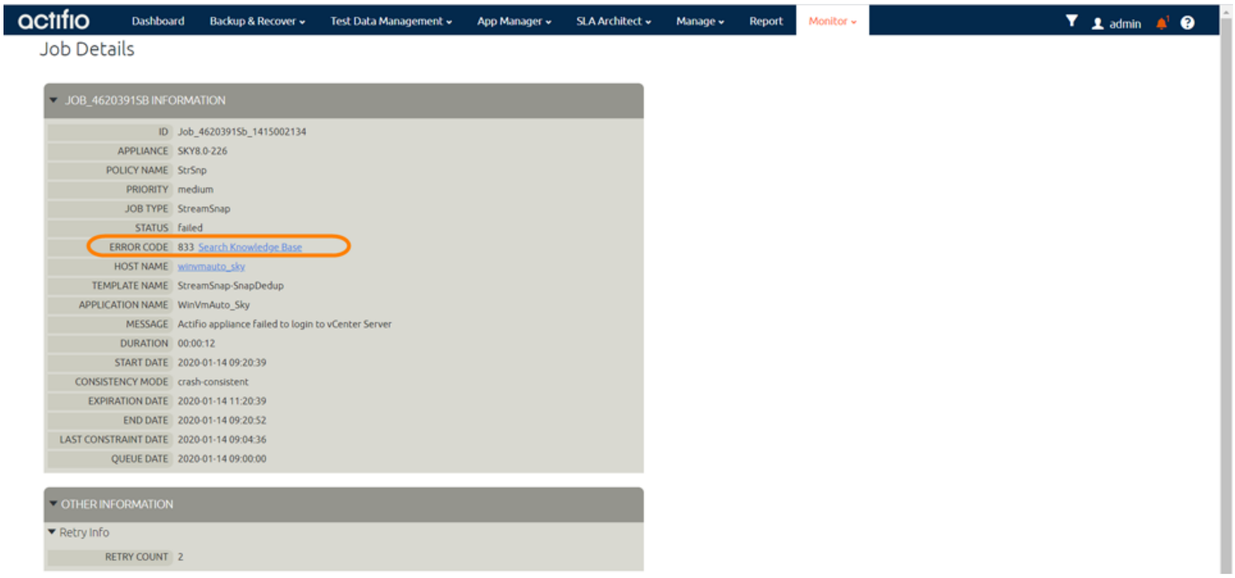
□	J...	STATUS	HOST	APPLICATION	A...	QUEUED	STARTED	E...	D...	T...	T...	P...	T...
□	J...	● Failed Error Code: 833	winvmauto_sky	WinVmAuto_Sky	S...	01-14-2020 09:00:00	01-14-2020 09:20:39	0...	0...	I...	S...	S...	S...
□	J...	● Retried	winvmauto_sky	WinVmAuto_Sky	S...	01-14-2020 09:00:00	01-14-2020 09:04:22	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 C ·e 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...	● Retr	_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_4620391SB INFORMATION

ID	Job_4620391Sb_1415002134
APPLIANCE	SKY8.0-226
POLICY NAME	StrSnp
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

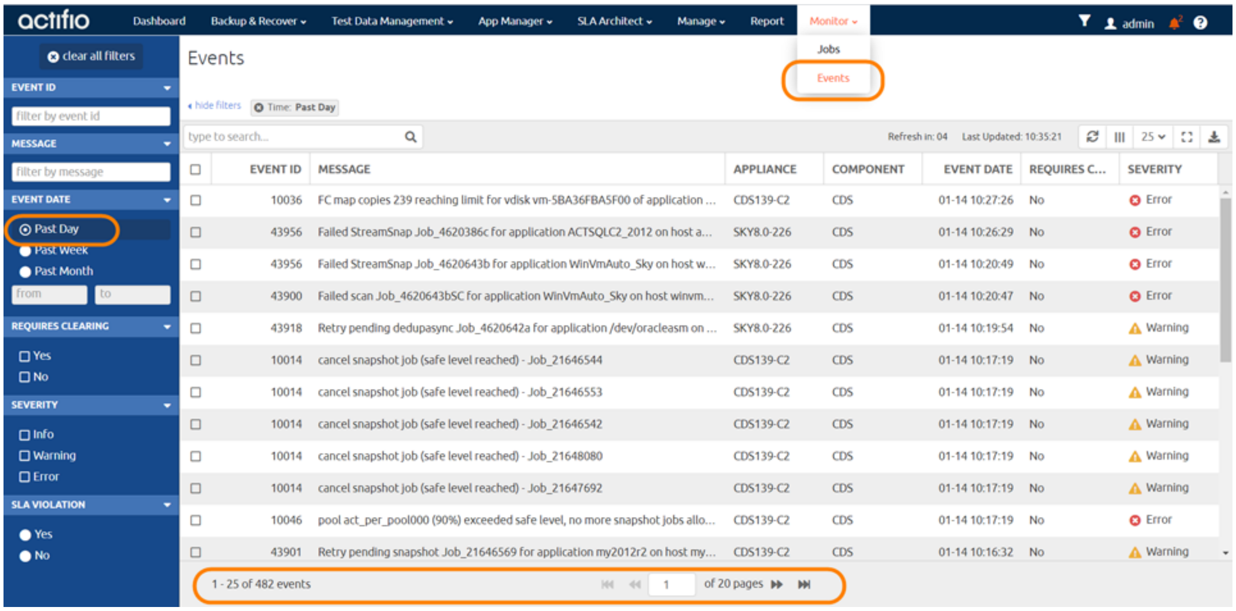
Job Details, with a Link to the Actifio Knowledge Base

16 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.



Events

Time: Past Day

Refresh in: 04 Last Updated: 10:35:21

□	EVENT ID	MESSAGE	APPLIANCE	COMPONENT	EVENT DATE	REQUIRES C...	SEVERITY
□	10036	FC map copies 239 reaching limit for vdisk vm-5BA36FBA5F00 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_4620643bSC for application WinVmAuto_Sky on host winwm...	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

1 - 25 of 482 events 1 of 20 pages

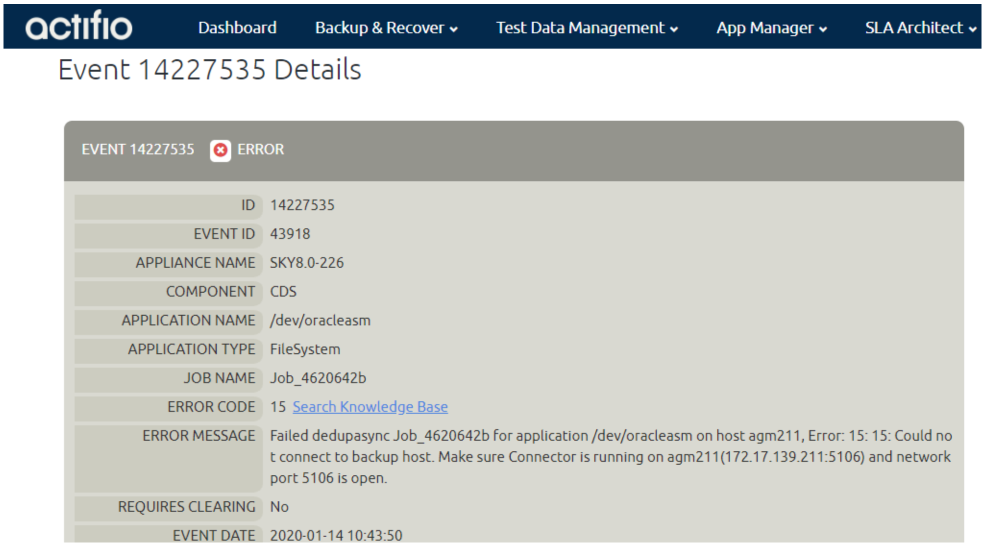
Viewing All Events of the Past 24 Hours

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 76.

Interpreting Event Details in the Events Monitor

Item	Meaning
ID	Error sequence number.
Event ID	Event identifier. Events are listed in ***Actifio Event IDs and Error Codes***.
Appliance Name	The name of the Actifio appliance that processed the job.
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 Sky component that encountered the event: 1. PSRV 2. UDP 3. OMD 4. Dedup (deprecated)
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.*



Event 14227535 Details

EVENT 14227535 ERROR

ID	14227535
EVENT ID	43918
APPLIANCE NAME	SKY8.0-226
COMPONENT	CDS
APPLICATION NAME	/dev/oracleasm
APPLICATION TYPE	FileSystem
JOB NAME	Job_4620642b
ERROR CODE	15 Search Knowledge Base
ERROR MESSAGE	Failed dedupasync Job_4620642b for application /dev/oracleasm on host agm211, Error: 15: 15: Could not connect to backup host. Make sure Connector is running on agm211(172.17.139.211:5106) and network port 5106 is open.
REQUIRES CLEARING	No
EVENT DATE	2020-01-14 10:43:50

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"

Index