
Connecting Hosts to Actifio Appliances

Copyright, Trademarks, and other Legal Matter

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

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

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

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

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

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

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

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

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

Contents

Preface	vii
Actifio Appliances	vii
The ActifioNOW Customer Portal	vii
Actifio Support Centers	vii
Chapter 1 - Adding Your Hosts to the Actifio Appliance	1
Assigning VDisks for the Host Copy Data (In-Band CDS Appliance only)	2
Configuring Hosts to Auto-Discover their Applications	3
Reconciling Inconsistent Host Information across Multiple Appliances.....	3
Security Software on Hosts	3
Deleting Hosts Using the AGM.....	4
Chapter 2 - About the Actifio Connector	5
What Does the Connector Do?	5
The Connector and the Network Environment	6
Host-Side Scripting	6
Obtaining the Right Actifio Connector for Your Host.....	7
Maintaining Connectors on Hosts	8
Chapter 3 - Adding a Windows Server Host	9
Installing the Actifio Connector on Microsoft Windows Hosts	10
Restricting Windows Connector Communication to Specific Appliances	11
To Unrestrict a Restricted Windows Connector	12
Adding a Windows Server Host to the Actifio Appliance from AGM	13
Notes on Discovering Specific Microsoft Application Types.....	15
Chapter 4 - Adding a Hyper-V Host	17
Installing the Actifio Connector on Hyper-V Hosts	17
Adding a Hyper-V Host to the Actifio Appliance from AGM	18
Chapter 5 - Adding a Linux Host	21
Installing the Actifio Connector on a Linux Host	22
Adding a Linux Host to the Actifio Appliance from AGM	23
Upgrading or Uninstalling the Actifio Connector on a Linux Host	24
Ensuring NFS Connectivity on a Linux Host.....	25
Ensuring iSCSI Connectivity on a Linux Host.....	26

Chapter 6 - Adding an AIX Host	27
Supported AIX Configurations	27
Installing the Actifio Connector on IBM AIX Hosts	28
Adding an AIX Host through the Actifio Desktop	29
Chapter 7 - Discovering LPARs from an IBM HMC Host	31
Ensuring vSCSI Connectivity on an IBM HMC Host	31
Adding an IBM HMC Host and its LPARs through the Actifio Desktop	32
Chapter 8 - Adding a Solaris Host	35
Installing the Actifio Connector on Sun Solaris Hosts	36
Adding a Solaris Host through the Actifio Desktop	37
Ensuring NFS Connectivity on a Solaris Host	39
Chapter 9 - Adding an HP-UX Host	41
Installing the Actifio Connector on HP-UX Hosts	42
Adding an HP-UX Host through the Actifio Desktop	43
Chapter 10 - APPID Pre- and Post-Scripts for Scheduled Data Protection Jobs	45
Sample APPID Script for Windows	46
Sample APPID Script for Linux	46
Chapter 11 - Super Scripts for Workflows and On-Demand Data Access Jobs	47
Super Script Phases	48
Super Script Arguments	48
Super Script Timeouts	49
Super Script Environment Variables	49
CLI Commands Supported in Super Scripts	50
Sample Super Scripts	51
Index	53

Preface

This guide provides step-by-step instructions on how to connect the Actifio Appliance to your hosts. It assumes you have read **Getting Started with Actifio Copy Data Management**, are familiar with the components of the Actifio Desktop, and have a grasp of the basic concepts associated with an Actifio Appliance.

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

- ***Configuring Resources and Settings With the Domain Manager***
- ***Setting Up Users and Roles With the Domain Manager***
- ***Network Administrator's Guide to Actifio Copy Data Management***

Actifio Appliances

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

The ActifioNOW Customer Portal

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

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

To log into the ActifioNOW customer portal:

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

Actifio Support Centers

To contact an Actifio support representative, you can:

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

1 Adding Your Hosts to the Actifio Appliance

These are the steps to connecting a non-VMware host to your VDP system. The first two are operating system-specific, the third applies only to hosts that will use VDP in-band storage (CDS Appliance only). To add VMs, see **A VMware Administrator's Guide to Actifio Copy Data Management**.

The Two OS-Specific Steps for Connecting Non-VMware Hosts

Host	1 Install the Connector	2 Add the Host
Windows Server, or Hyper-V or SCVMM	Installing the Actifio Connector on Microsoft Windows Hosts on page 10	Adding a Windows Server Host to the Actifio Appliance from AGM on page 13
Linux	Installing the Actifio Connector on a Linux Host on page 22	Adding a Linux Host to the Actifio Appliance from AGM on page 23
IBM AIX	Installing the Actifio Connector on IBM AIX Hosts on page 28	Adding an AIX Host through the Actifio Desktop on page 29
IBM HMC	The Connector is not required for IBM HMC hosts.	Adding an IBM HMC Host and its LPARs through the Actifio Desktop on page 32
Sun Solaris	Installing the Actifio Connector on Sun Solaris Hosts on page 36	Adding a Solaris Host through the Actifio Desktop on page 37
HP-UX	Installing the Actifio Connector on HP-UX Hosts on page 42	Adding an HP-UX Host through the Actifio Desktop on page 43

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

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

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 4.](#)

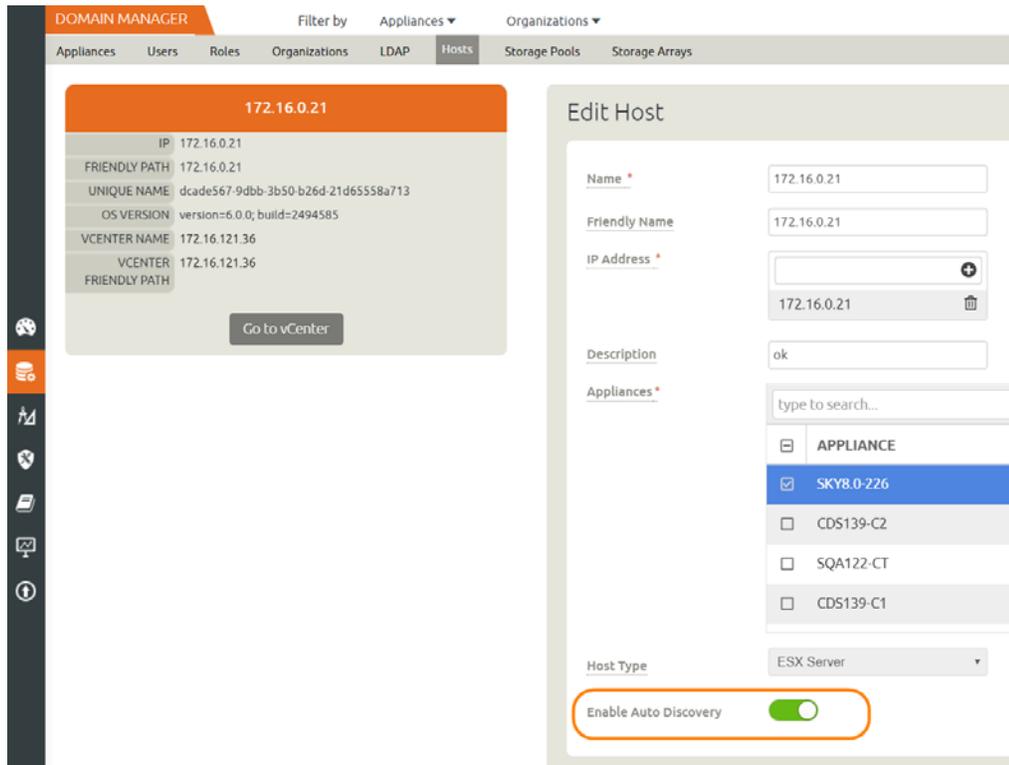
You can have pre- and post-scripts run on your applications and VMs when they are triggered by a VDP job. Scripting is detailed in [Chapter 10, APPID Pre- and Post-Scripts for Scheduled Data Protection Jobs](#) and in [Chapter 11, Super Scripts for Workflows and On-Demand Data Access Jobs.](#)

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 Domain Manager, Hosts tab.
2. Right-click the host to enable auto-discovery on, and select Edit.
3. Slide the Enable Auto Discovery button to the right and click Save in the lower right corner.



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.

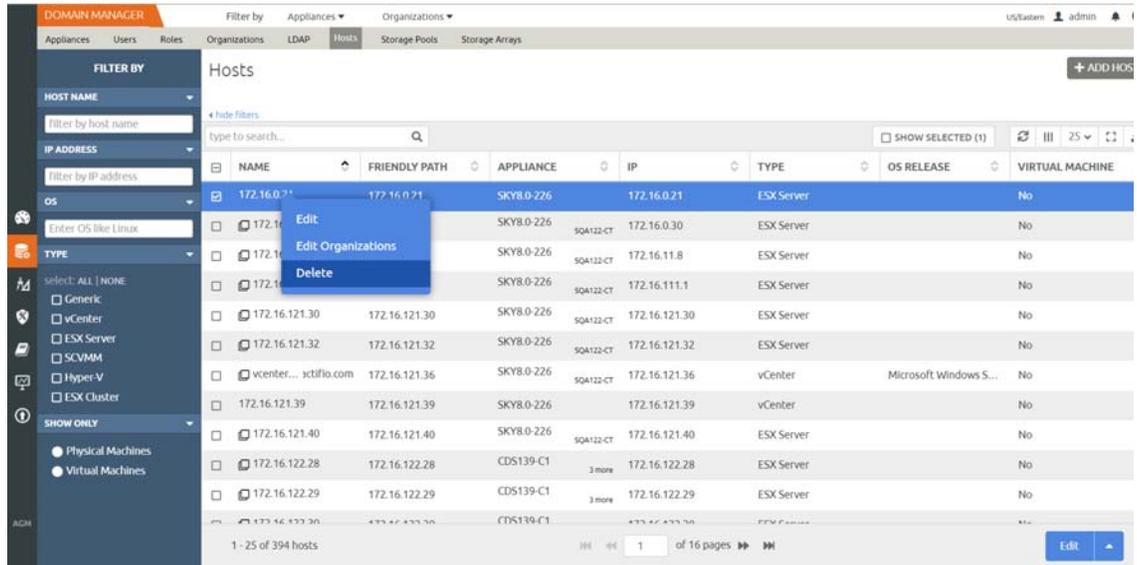
Security Software on Hosts

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 6.

Deleting Hosts Using the AGM

You can delete Hosts. To delete a host:

1. Open the AGM to the Domain Manager, Hosts tab.
2. Right-click the host to delete, and select Delete.
3. In the Delete Host window, click OK.



Deleting a Host in the Domain Manager

2 About the Actifio Connector

This chapter describes the Actifio Connector, including [Obtaining the Right Actifio Connector for Your Host](#) on page 7 and [Maintaining Connectors on Hosts](#) on page 8. The Actifio Connector is a small-footprint process that you install on your hosts.

This section includes:

- [What Does the Connector Do?](#) on page 5
- [The Connector and the Network Environment](#) on page 6
- [Host-Side Scripting](#) on page 6
- [Obtaining the Right Actifio Connector for Your Host](#) on page 7
- [Maintaining Connectors on Hosts](#) on page 8

What Does the Connector Do?

Actifio Connectors:

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

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

The Connector and the Network Environment

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

Network Traffic

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

Antivirus Software

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

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

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

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

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

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

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

Host-Side Scripting

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

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

For detailed instructions on how use VDP scripting, see:

- [Chapter 10, APPID Pre- and Post-Scripts for Scheduled Data Protection Jobs](#)
- [Chapter 11, Super Scripts for Workflows and On-Demand Data Access Jobs](#)

Obtaining the Right Actifio Connector for Your Host

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

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

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

actifio Resource Center for v9.0
Radically Simple



CONNECTORS

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

[Deployment guide](#)
[View all connectors](#)

To manually install the Actifio Desktop, click on the links below:

-  [Download the Adobe Air Player](#)
-  [Download the Actifio Desktop Air File](#)

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](#)

REPORT MANAGER

-  [Deployment guide](#)

SNMP RESOURCES

-  [MIB](#)

LICENSES

-  [Additional Software Licenses](#)

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

actifio | actifio.com | Connecting Hosts to Actifio Appliances

7

Maintaining Connectors on Hosts

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

The screenshot shows the 'Appliance Configuration' interface. On the left sidebar, 'Connector Management' is highlighted. The main area displays 'Latest Available Connectors' and a table of 'Discovered Hosts'.

Host Name	Properties	Installed version	Current Status	Last Success	
SCVM42016		8.0.9.1344	Upgrade Success	Oct 22 11:12	+
V2k8E10.211		9.0.1.90	Upgrade Success	Mar 05 16:57	+
ermie.sqa.actifio.com		7.1.4.272	Upgrade Success	Jul 26 04:15	+
gonzo.sqa.actifio.com		8.1.4.791	Upgrade Success	Mar 11 02:44	+
linux.8-vm1		8.1.0.1615	Upgrade Success	Jul 13 10:25	+
r3hyper4.sqa.actifio.com		9.0.0.1331	Upgrade Success	Jan 31 02:13	+
r3hyperv5.sqa.actifio.com		9.0.0.1331	Upgrade Success	Jan 31 02:12	+
snuffles.sqa.actifio.com		8.1.3.587	Upgrade Success	Jan 23 00:19	+
vcenter36.sqa.actifio.com		7.1.0.547	Upgrade Success	Oct 17 15:06	+
w2k8r2-sasqj		8.0.0.1401	Upgrade Success	Sep 21 11:04	+
windows 2012 r2		8.1.2.507 HotFix 1714	Upgrade Success	Mar 21 13:40	+
windows2012_lov_sql		8.1.1.201	Upgrade Success	Sep 30 03:55	+
winvmaulo_sky		8.1.0.1646	Upgrade Success	Jun 25 08:21	+
aqm211		7.1.5.427			+

Buttons at the bottom: Abort, Rescan, Upgrade, Remove.

3 Adding a Windows Server Host

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

This chapter includes:

[Installing the Actifio Connector on Microsoft Windows Hosts](#) on page 10

[Restricting Windows Connector Communication to Specific Appliances](#) on page 11

[Notes on Discovering Specific Microsoft Application Types](#) on page 15

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 10, APPID Pre- and Post-Scripts for Scheduled Data Protection Jobs](#) and [Chapter 11, 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.

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

VDP Change Tracking Driver Options for Windows Physical Hosts

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

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

Installing the Actifio Connector on a Windows Host

To install the Actifio Connector on a Windows host:

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

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**.
3. 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.

Upgrading the Actifio Connector on a Windows Host

Use the Connector Management tool in the Actifio Desktop to auto upgrade the Actifio Connector on your hosts when new versions are available. Refer to [Maintaining Connectors on Hosts](#) on page 8.

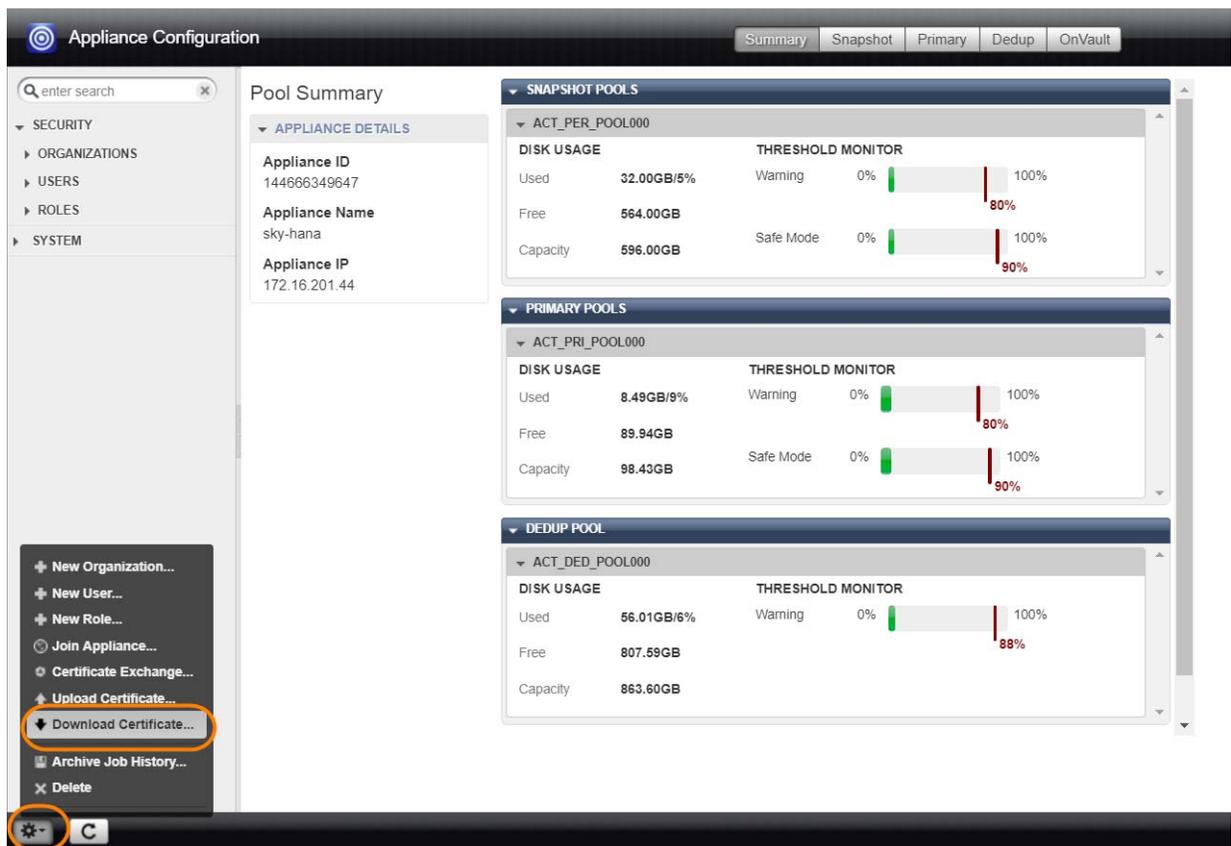
Restricting Windows Connector Communication to Specific Appliances

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

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

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

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



Downloading an Appliance Certificate

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

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



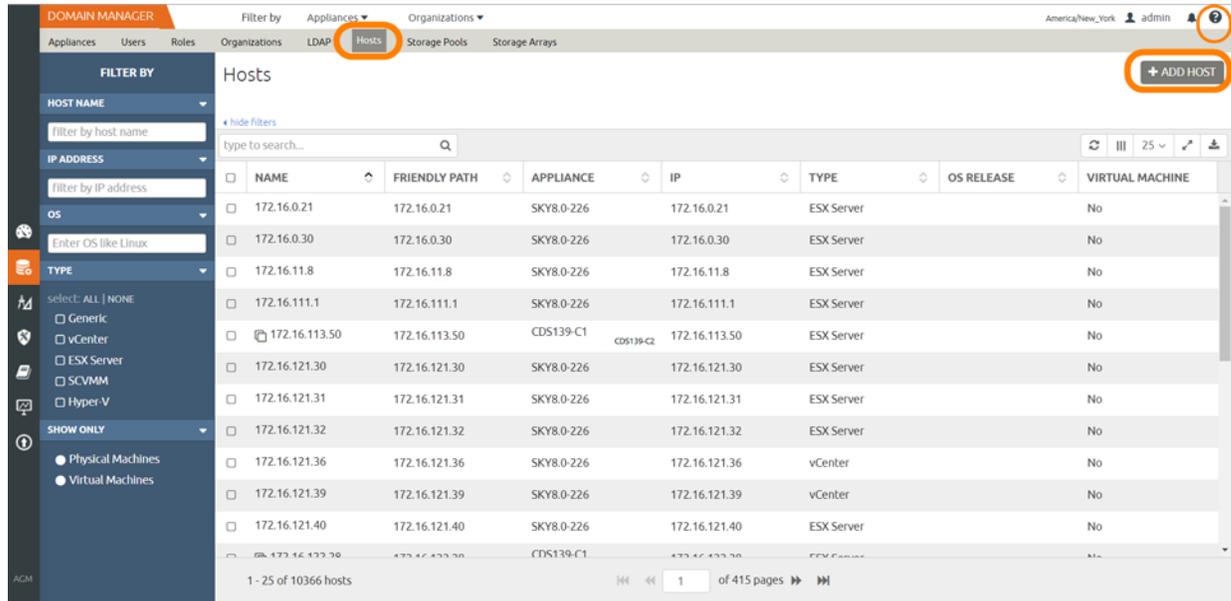
To Unrestrict a Restricted Windows Connector

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 11.

Adding a Windows Server Host to the Actifio Appliance from AGM

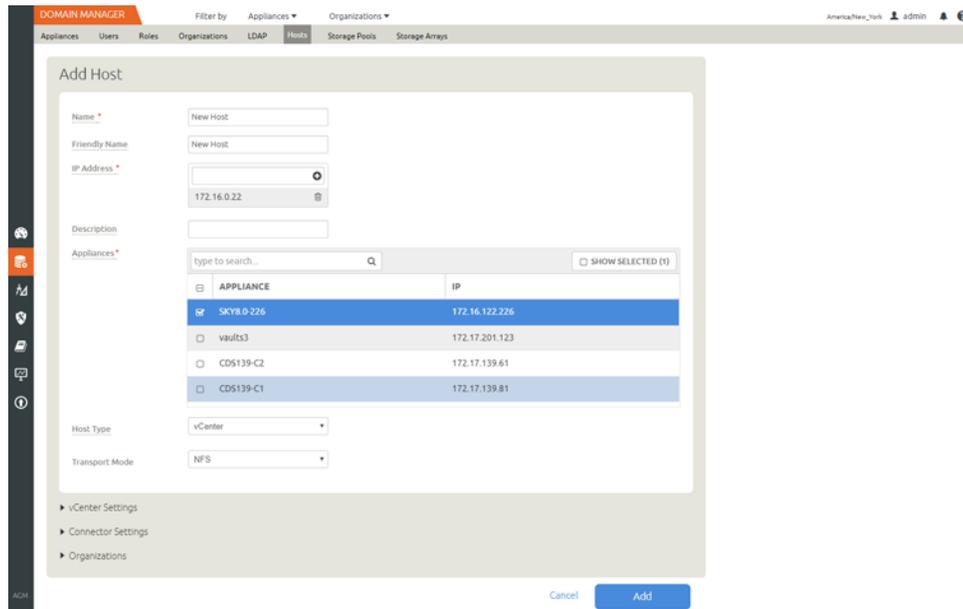
To add a new Windows host from AGM:

1. Open the AGM to the **Domain Manager**.
2. From the Hosts tab, select **+ Add Host**.



Adding a New Windows Host in AGM

3. In the Add Host form, enter the name, optional friendly name, and the IP address of the host. The name of a host can contain letters, digits (0-9), and an underscore ('_').



Adding a Host Details in AGM

4. You can enter an additional IP address in **IP Address**. Click **+** to add multiple IP addresses for a host.
5. (Optional) Add a description.
6. Select the Actifio Appliance that will manage the host's data.
7. In Host Type, the type you pick depends on what you're using the Windows host for. These are detailed in [Host Types and Connector Settings Overrides](#) on page 14.
8. If you select vCenter or ESX Server, then you must also select the data transport mode, NFS or SAN. NFS is the default setting.
9. If you select vCenter or ESX Server, then you will also see a new section appear for vCenter Settings or ESX Settings. This is where you enter and test the port, username, and password to connect to the host.
10. Whatever type you select, enter **Connector Settings**. Enter **5106** in port unless you have changed from the default setting. Then enter a username and password for the Connector to use.
11. In **Organizations**, select one or more organizations for the host to be a member of. Organizations are explained in the AGM Online Help.

Host Types and Connector Settings Overrides

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

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.

Discovering SharePoint Servers

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

Discovering Exchange Mailbox Databases

- All databases in a Microsoft Exchange Database Availability Group (DAG) can be discovered from a single DAG node. Run discovery on a single node to discover all Exchange databases in DAG.
- For the discovery to work correctly, Exchange VSS writer must be installed and running on the host.

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 Actifio Desktop. 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.*

4 Adding a Hyper-V Host

This chapter includes:

[Installing the Actifio Connector on Hyper-V Hosts](#) on page 17

[Adding a Hyper-V Host to the Actifio Appliance from AGM](#) on page 18

Location of UDSAgent.log on Hyper-V Hosts

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

Location of Scripts on Hyper-V Hosts

You can create scripts to perform pre- and post- actions on applications on the host. Create a folder at C:\Program Files\Actifio\scripts and store scripts there. Details on VDP scripting are in [Chapter 10, APPID Pre- and Post-Scripts for Scheduled Data Protection Jobs](#) and [Chapter 11, Super Scripts for Workflows and On-Demand Data Access Jobs](#).

Installing the Actifio Connector on Hyper-V Hosts

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

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

Installing the Actifio Connector on a Hyper-V Host

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

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

Restarting the Actifio Connector on a Hyper-V Host

To restart the Actifio Connector on a Windows host:

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

Upgrading the Actifio Connector on a Hyper-V Host

Use the Connector Management tool in AGM or in the Actifio Desktop Domain Manager service to upgrade the Actifio Connector on your hosts when new versions are available. Refer to [Maintaining Connectors on Hosts](#) on page 8.

Uninstalling the Actifio Connector from a Windows Host

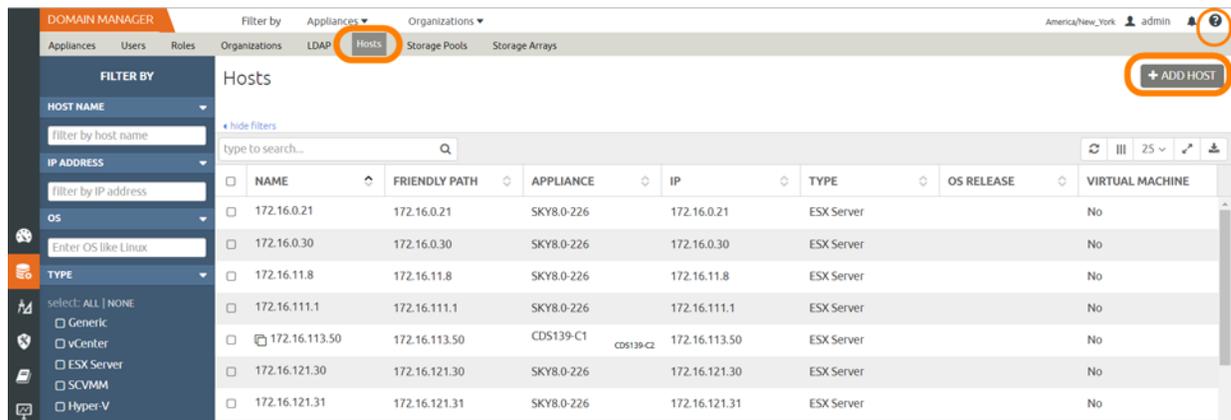
To uninstall the Actifio Connector from a Windows host:

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.

Adding a Hyper-V Host to the Actifio Appliance from AGM

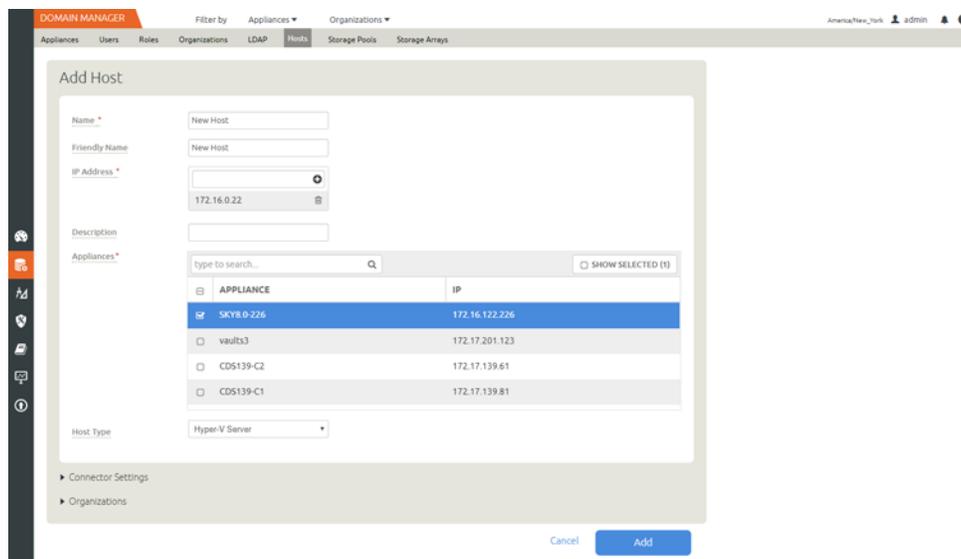
To add a new Hyper-V host from AGM:

1. Open the AGM to the **Domain Manager**.
2. From the Hosts tab, select **+ Add Host**.



Adding a New Hyper-V Host in AGM

3. In the Add Host form, enter the name, optional friendly name, and the IP address of the host. The name of a host can contain letters, digits (0-9), and an underscore ('_').



Adding Host Details in AGM

4. You can enter an additional IP address in **IP Address**. Click **+** to add multiple IP addresses for a host.
5. (Optional) Add a description.
6. Select the Actifio Appliance that will manage the host's data.
7. In Host Type, select **Hyper-V Server** or **SCVMM**.
8. Enter **Connector Settings**. Enter **5106** in port unless you have changed from the default setting. Then enter a username and password for the Connector to use.
9. In **Organizations**, select one or more organizations for the host to be a member of. Organizations are explained in the AGM Online Help.

5 Adding a Linux Host

This chapter includes:

- [Installing the Actifio Connector on a Linux Host on page 22](#)
- [Adding a Linux Host to the Actifio Appliance from AGM on page 23](#)
- [Upgrading or Uninstalling the Actifio Connector on a Linux Host on page 24](#)
- [Ensuring NFS Connectivity on a Linux Host on page 25](#)

Location of UDSAgent.log on Linux Hosts

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

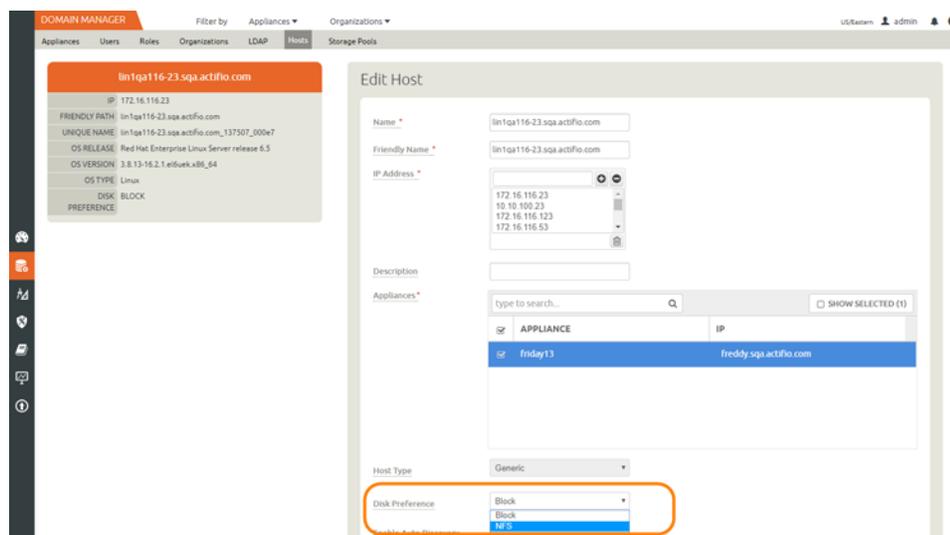
Location of Scripts on Linux Hosts

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 10, APPID Pre- and Post-Scripts for Scheduled Data Protection Jobs](#) and [Chapter 11, Super Scripts for Workflows and On-Demand Data Access Jobs](#).

Using NFS protocol for Linux hosts in the AGM

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.

Use the AGM Domain Manager Hosts Edit section to set the Disk Preference 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, the mount screens will automatically show you the option to mount them as an NFS share.



Setting Disk Preference to NFS

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`

Manually Uninstalling the Actifio Connector from a Linux Host

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:

```
[oracle@vq-oracle ~]$ 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
```

Adding a Linux Host to the Actifio Appliance from AGM

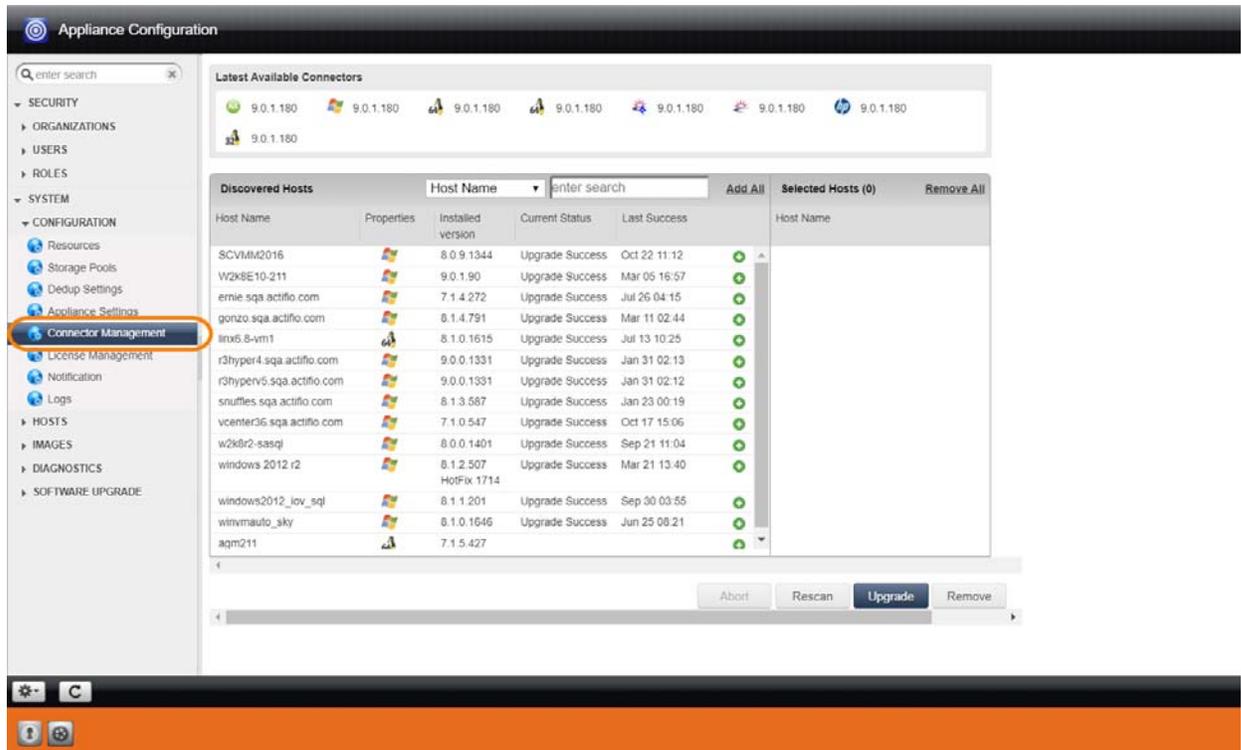
To add a new Linux host from AGM, open AGM to the **Domain Manager** and from the Hosts tab, select **+ Add Host**. Refer to the AGM online help for details.

The screenshot shows the Actifio Domain Manager interface. The 'Hosts' tab is selected in the top navigation bar. The sidebar on the left contains filter options for Host Name, IP Address, OS, and Type. The main area displays a table of hosts with the following columns: NAME, FRIENDLY PATH, APPLIANCE, IP, TYPE, OS RELEASE, and VIRTUAL MACHINE. The table contains 10 rows of host data. A '+ ADD HOST' button is highlighted in the top right corner of the interface.

NAME	FRIENDLY PATH	APPLIANCE	IP	TYPE	OS RELEASE	VIRTUAL MACHINE
172.16.0.21	172.16.0.21	SKY8.0-226	172.16.0.21	ESX Server		No
172.16.0.30	172.16.0.30	SKY8.0-226	172.16.0.30	ESX Server		No
172.16.11.8	172.16.11.8	SKY8.0-226	172.16.11.8	ESX Server		No
172.16.111.1	172.16.111.1	SKY8.0-226	172.16.111.1	ESX Server		No
172.16.113.50	172.16.113.50	CDS139-C1	172.16.113.50	ESX Server	CD6139-C2	No
172.16.121.30	172.16.121.30	SKY8.0-226	172.16.121.30	ESX Server		No
172.16.121.31	172.16.121.31	SKY8.0-226	172.16.121.31	ESX Server		No
172.16.121.32	172.16.121.32	SKY8.0-226	172.16.121.32	ESX Server		No
172.16.121.36	172.16.121.36	SKY8.0-226	172.16.121.36	vCenter		No
172.16.121.39	172.16.121.39	SKY8.0-226	172.16.121.39	vCenter		No

Upgrading or Uninstalling the Actifio Connector on a Linux Host

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



The screenshot shows the 'Appliance Configuration' interface. On the left sidebar, 'Connector Management' is highlighted. The main area displays 'Latest Available Connectors' at the top, followed by a table of 'Discovered Hosts'. The table has columns for Host Name, Properties, Installed version, Current Status, and Last Success. Below the table are buttons for 'Abort', 'Rescan', 'Upgrade', and 'Remove'.

Host Name	Properties	Installed version	Current Status	Last Success
SCVMM2016		8.0.9.1344	Upgrade Success	Oct 22 11:12
W2K8E10-211		9.0.1.90	Upgrade Success	Mar 05 16:57
ernie.sqa.actifio.com		7.1.4.272	Upgrade Success	Jul 26 04:15
gonzo.sqa.actifio.com		8.1.4.791	Upgrade Success	Mar 11 02:44
linux.8-vm1		8.1.0.1615	Upgrade Success	Jul 13 10:25
r3hyper4.sqa.actifio.com		9.0.0.1331	Upgrade Success	Jan 31 02:13
r3hyperv5.sqa.actifio.com		9.0.0.1331	Upgrade Success	Jan 31 02:12
snuffles.sqa.actifio.com		8.1.3.587	Upgrade Success	Jan 23 00:19
vcenter36.sqa.actifio.com		7.1.0.547	Upgrade Success	Oct 17 15:06
w2k8r2-sasqj		8.0.0.1401	Upgrade Success	Sep 21 11:04
windows 2012 r2		8.1.2.507 HotFix 1714	Upgrade Success	Mar 21 13:40
windows2012_jov_sqj		8.1.1.201	Upgrade Success	Sep 30 03:55
winvmauto_sky		8.1.0.1646	Upgrade Success	Jun 25 08:21
aqm211		7.1.5.427		

Connector Management

Ensuring NFS Connectivity on a Linux Host

This section includes:

[Installing the NFS client on a Red Hat RHEL 6 or CentOS Linux Host on page 25](#)

[Installing the NFS client on a SLES Linux Host on page 25](#)

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

Installing the NFS client on a Red Hat RHEL 6 or CentOS Linux Host

To see if the client is installed, run:

```
# rpm -qa | grep nfs
```

This should return something like:

```
nfs-utils-lib-1.1.5-9.el6.x86_64
nfs-utils-1.2.3-54.el6.x86_64
```

If you see nothing, then use yum to install the NFS client packages. Run:

```
# yum install nfs-utils nfs-utils-lib
```

Make sure rpcbind /portmapper package is installed on the Linux host. Run:

```
# rpm -qa | grep rpcbind
```

This should return something like:

```
rpcbind-0.2.0-11.el6.x86_64
```

If you see nothing, then use yum to install the rpcbind. Run:

```
# yum install rpcbind
```

Installing the NFS client on a SLES Linux Host

To see if the client is installed, run:

```
# rpm -qa | grep nfs
```

This should return something similar to:

```
nfs-client-1.2.1-2.6.6
yast2-nfs-common-2.17.7-1.1.2
yast2-nfs-client-2.17.12-0.1.81
```

If you do not see either nfs-client or yast2-nfs-xxxx packages, then use either YaST or zypper to install the NFS client packages.

Using YaST:

```
# yast2 --install yast2-nfs-client
# yast2 --install yast2-nfs-common
```

Using Zypper:

```
# zypper install nfs-client
```

Make sure rpcbind / portmapper package is installed on the Linux host. Run:

```
# rpm -qa | grep rpcbind
```

This should return something like:

```
rpcbind-0.1.6+git20080930-6.15
```

If you see nothing, then you must install the packages using either YaST or zypper.

Using YaST:

```
# yast2 --install rpcbind
```

Using Zypper:

```
# zypper install rpcbind
```

Learning NFS client information from a Linux Host

An Actifio-approved NFS client packages and version must be installed on the host.

Check if the portmapper/rpcbind service is running. Run:

```
# service rpcbind status
```

On a Red Hat RHEL 6 or CentOS Linux host, this should return something like:

```
rpcbind (pid 1591) is running...
```

On a SLES Linux host, this should return something like:

```
Checking for service rpcbind      running
```

If rpcbind service is not running on Linux host, start it with:

```
# service rpcbind start
```

Use rpcinfo to list the registered RPC programs / services. Portmapper should be registered and running. Run:

```
# rpcinfo -p
program vers proto  port  service
100000   4   tcp    111  portmapper
100000   3   tcp    111  portmapper
100000   2   tcp    111  portmapper
100000   4   udp    111  portmapper
100000   3   udp    111  portmapper
100000   2   udp    111  portmapper
```

Check if the Linux host can make an RPC call to rpcbind & nfs programs on the Actifio Sky Appliance using following.

```
# rpcinfo -T tcp <#appliance IP> rpcbind
program 100000 version 2 ready and waiting
program 100000 version 3 ready and waiting
program 100000 version 4 ready and waiting
```

```
# rpcinfo -T tcp <#appliance IP> nfs
program 100003 version 2 ready and waiting
program 100003 version 3 ready and waiting
```

If the above commands return the output shown above, then NFS connectivity from Linux host to the Actifio sky appliance is fine.

Ensuring iSCSI Connectivity on a Linux Host

Network connectivity is detailed in **Network Administrator's Guide to Actifio VDP**.

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

6 Adding an AIX Host

This chapter includes:

[Supported AIX Configurations](#) on page 27

[Installing the Actifio Connector on IBM AIX Hosts](#) on page 28

[Adding an AIX Host through the Actifio Desktop](#) on page 29

Location of UDSAgent.log on AIX Hosts

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

Location of Scripts on AIX Hosts

You can create scripts to perform pre- and post- actions on applications on the AIX host. To use scripts, create a folder called `/act/scripts` and store all scripts there. For detailed instructions on how use VDP scripting, see [Chapter 10, APPID Pre- and Post-Scripts for Scheduled Data Protection Jobs](#) and [Chapter 11, Super Scripts for Workflows and On-Demand Data Access Jobs](#).

Supported AIX Configurations

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

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

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

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

VDP can protect and recover in-band dedicated LPAR configurations both via Fibre Channel and iSCSI in a crash-consistent or application-consistent state. VDP can also protect the rootvg in a bootable state.

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

VDP can protect and recover in-band NPIV environments including rootvg of an LPAR in a bootable state.

These hosts can be added as physical hosts, as detailed in [Adding an AIX Host through the Actifio Desktop](#) on page 29. Storage ports need to be configured for them.

LPAR with vSCSI mapping: You can also add LPARs with vSCSI mapping on VIO servers. These are described in [Discovering LPARs from an IBM HMC Host](#) on page 31.

Installing the Actifio Connector on IBM AIX Hosts

On AIX systems, including those using the NPIV protocol, the Actifio Connector runs as a daemon process under the username root. It listens on a TCP port 5106 and 56789 (legacy port) for communication from the Actifio Appliance.

The Actifio Connector writes to a log file in the installation directory (*/var/act/log/UDSAgent.log*).

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

Installing the Actifio Connector on an AIX Host

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

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

Tasks and Available Command Options

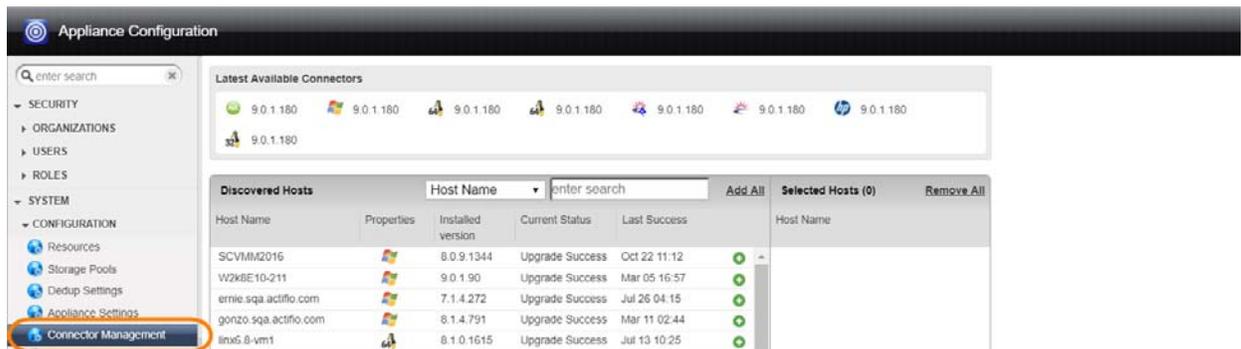
Task	Command option
Verify the successful installation of the Actifio Connector	<code>lslpp -L grep udsagent</code>
Verify the status of the Connector	<code>/etc/udsagent status</code>
Manually stop the Connector service	<code>/etc/udsagent stop</code>
Manually start the Connector service	<code>/etc/udsagent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

Manually Uninstalling the Actifio Connector from an AIX Host

To uninstall the Actifio Connector from a AIX host, run: `installp -u udsagent`. You can also use the AGM Domain Manager to uninstall many connectors simultaneously; see [Upgrading or Uninstalling the Actifio Connector on an AIX Host](#) on page 28.

Upgrading or Uninstalling the Actifio Connector on an AIX Host

From the AGM Domain Manager Appliance page, right-click the appliance that supports the host and 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.



Adding an AIX Host through the Actifio Desktop

Note: AGM does not support adding AIX hosts.

To add a new physical AIX host, dedicated LPAR host, or LPAR host with NPIV mapping:

1. Open the Actifio Desktop to the **Domain Manager**.
2. From the service menu, select **New Host...**
3. In the Add a New Host form, enter the name, fully qualified domain name, or the IP address of the host in **Host Name**. The name of a host should start with a letter, and can contain letters, digits (0-9), and an underscore ('_').
4. Click **Discover Details**. Actifio Desktop lists all IP addresses used by the host.
5. Enter the IP address of the host in **IP Address**. Click **Add** to add multiple IP addresses for a host.
6. (Optional) Add a **Friendly Name**.
7. In **Member of Organization(s)**, select one or more Actifio Desktop organizations for the host to be a member of. Organizations are explained in **Setting Up Users and Roles With the Domain Manager**.
8. In Select Host Type, select **Generic** or **None**. The Actifio Connector natively supports AIX servers, so you do not have to select a host type.

Add A New Host

Host Name*
172.16.199.85 Discover Details

Friendly Name

IP Address
Add Clear

IP address
172.16.199.85 Delete

Member of Organization(s)
Select All, None
 ALL
 Actifioorg
 Bharath_ORG

Select Host Type
Generic

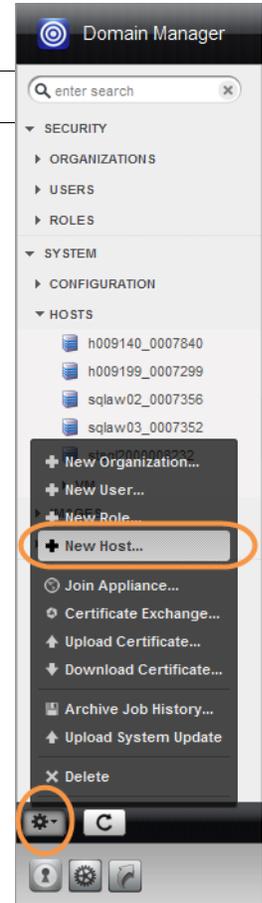
WWPN/iSCSI Port
WWPN
2100001B328626E4
2100001B328AFDCE

Connector Port

Use Oracle Database Authentication
Note: Windows host requires DB Authentication

Login Credentials for connector
Username Password

Adding a New AIX Host



9. Depending on how the host is accessed, specify one of the following for **WWPN/iSCSI Port**:
 - o If the host can be reached using a Fibre Channel port, select **WWPN (World Wide Port Name)**.
 - o If the host can be reached using an IP network, select **iSCSI** (Internet Small Computer System Interface).

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

10. In Connector Port enter **5106** unless you have changed from the default value. You can also use 56789. Do not use any other port unless instructed by Actifio Support.
11. 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.
12. Click **Add Host**.
13. The next step is [Assigning VDisks for the Host Copy Data \(In-Band CDS Appliance only\)](#) on page 2.

7 Discovering LPARs from an IBM HMC Host

This chapter includes:

[Ensuring vSCSI Connectivity on an IBM HMC Host](#) on page 31

[Adding an IBM HMC Host and its LPARs through the Actifio Desktop](#) on page 32

Physical Machines, Dedicated LPARs, and LPARs with NPIV Mapping

Typically these hosts have Fibre Channel connectivity configured for the best performance. iSCSI connectivity is an option for these hosts, but vSCSI is not. These configurations are detailed in [Chapter 6, Adding an AIX Host](#).

Location of UDSAgent.log on IBM HMC Hosts

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

Location of Scripts on IBM HMC Hosts

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

Opening Network Ports

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

Limitations

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

Ensuring vSCSI Connectivity on an IBM HMC Host

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

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

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

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

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

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

To discover a vSCSI LPAR host, see [Adding an IBM HMC Host and its LPARs through the Actifio Desktop](#) on page 32.

Adding an IBM HMC Host and its LPARs through the Actifio Desktop

Note: AGM does not support adding HMC hosts.

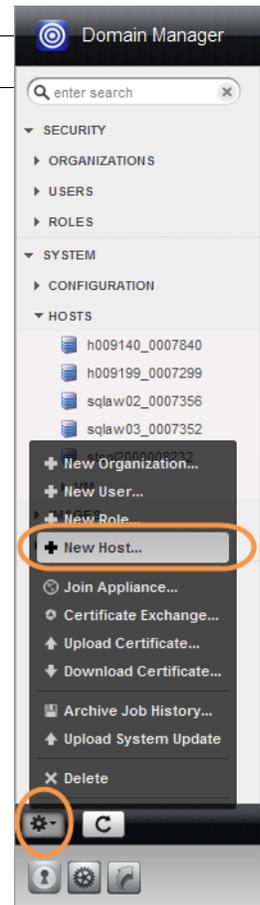
The Actifio Appliance discovers all VIOs and LPARs on the IBM HMC host. To add a host:

1. Open the Actifio Desktop to the **Domain Manager**.
2. From the service menu, select **New Host....**
3. The Add a New Host form appears.
4. Enter the name, fully qualified domain name, or the IP address of the host in **Host Name**. A host name should start with a letter, and can contain letters, digits (0-9), and an underscore ('_').
5. Click **Discover Details**. Actifio Desktop lists all IP addresses used by the host.
6. Enter the IP address of the host in **IP Address**. Click **Add** to add multiple IP addresses for a host. Optionally, you can add a **Friendly Name**.
7. In **Member of Organization(s)**, select one or more Actifio Desktop organizations for the host to be a member of. Organizations are explained in **Setting Up Users and Roles With the Domain Manager**.
8. In Select Host Type, select **IBM HMC**.
9. In the spaces provided, add the login credentials for the IBM HMC host as needed. Click **Test** to ensure the credentials have been properly entered.

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

To activate the rmc state of an LPAR, run:
/usr/sbin/rsct/install/bin/recfgct
/usr/sbin/rsct/bin/rmcctrl -p

10. Click **Add Host**.

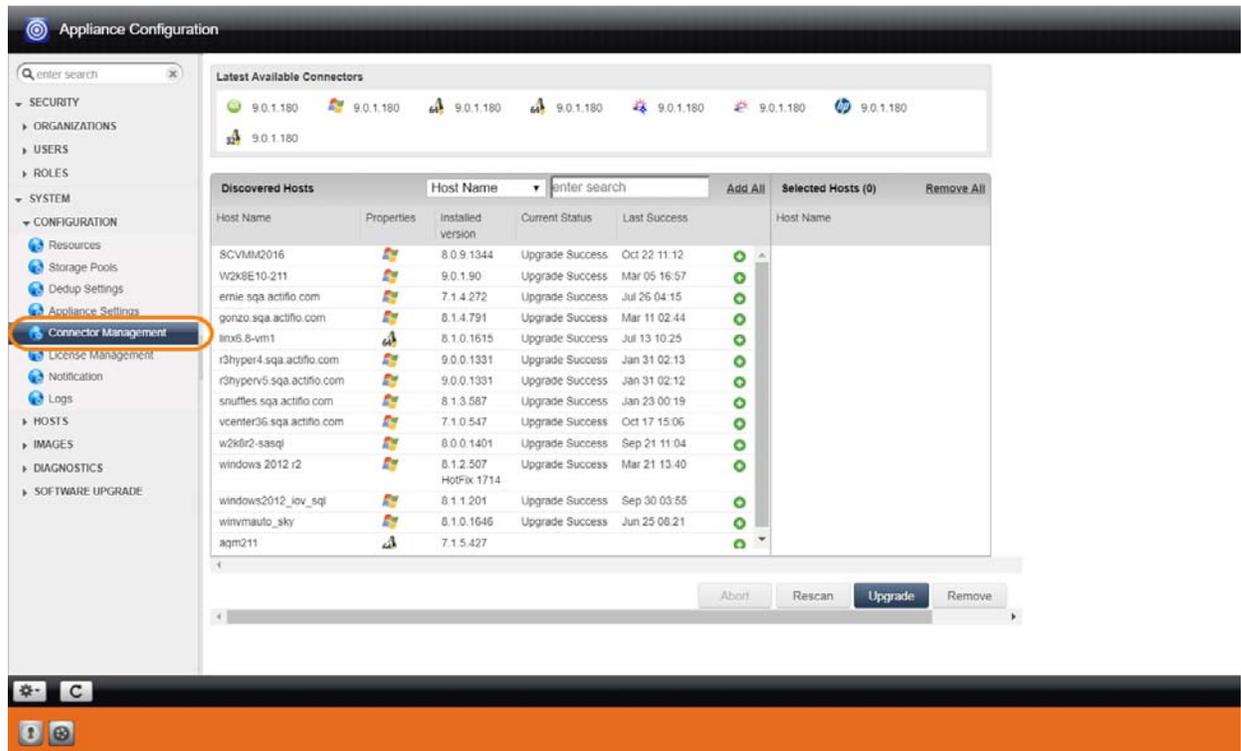


Adding a New IBM HMC Host

11. (CDS Appliance only) If any VIOS servers were discovered after adding the HMC host, then manually define any FC HBAs in use on those VIO Servers that are also zoned to the Actifio Appliance. To do this go to the Ports tab of each VIO Server and use the 'Add Port' Button. If the VIO Server WWPNs do not appear, use the Custom option to add them manually. Failure to do this may result in LPARs that use vSCSI automatically configuring the iSCSI initiator in the LPAR, rather than use FC staging disks presented to and then passed through the VIO server to the LPAR using vSCSI.
12. The next step is [Assigning VDisks for the Host Copy Data \(In-Band CDS Appliance only\)](#) on page 2.

Upgrading or Uninstalling the Actifio Connector on an IBM HMC Host

From the AGM Domain Manager Appliance page, right-click the appliance that supports the host and 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.



8 Adding a Solaris Host

This chapter includes:

[Installing the Actifio Connector on Sun Solaris Hosts](#) on page 36

[Adding a Solaris Host through the Actifio Desktop](#) on page 37

[Ensuring NFS Connectivity on a Solaris Host](#) on page 39

Location of UDSAgent.log on Solaris Hosts

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

Location of Scripts on Solaris Hosts

You can create scripts to perform pre- and post- actions on applications on the host. To use scripts, create a folder called `/act/scripts` and store all scripts there. For more on VDP scripting, see [Chapter 10, APPID Pre- and Post-Scripts for Scheduled Data Protection Jobs](#) and [Chapter 11, Super Scripts for Workflows and On-Demand Data Access Jobs](#).

Limitations

AGM does not support adding Solaris hosts. They must be added directly from the Actifio Desktop on the appliance. See [Adding a Solaris Host through the Actifio Desktop](#) on page 37.

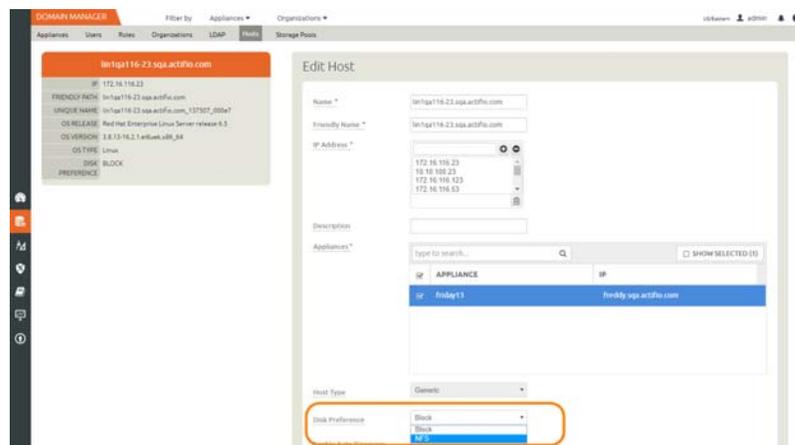
The Sky Appliance does support iSCSI on Solaris V11 systems after applying Solaris patch 11.3.21.5.0.

The CDS Appliance does not support iSCSI for Solaris SPARC hosts.

The CDX Appliance does not support Solaris hosts.

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

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



Setting Disk Preference to NFS

Installing the Actifio Connector on Sun Solaris Hosts

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

Installing the Actifio Connector on a Solaris Host

To install the Actifio Connector on a Solaris host:

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

Tasks and Available Command Options

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

Manually Uninstalling the Actifio Connector from a Solaris Host

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

Note: You can also uninstall the Actifio Connector on many hosts simultaneously; see [Maintaining Connectors on Hosts](#) on page 8

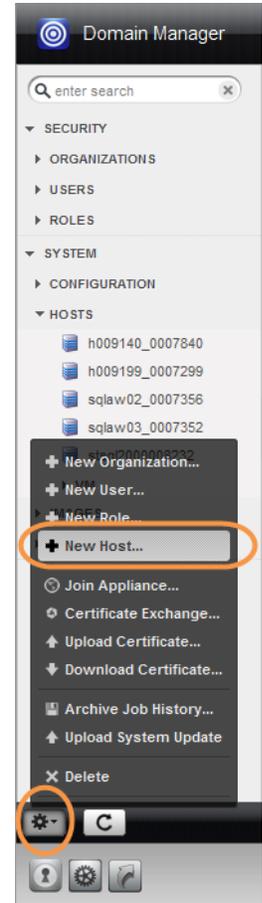
Using the Connector Management Tool to Upgrade or Uninstall the Actifio Connector on a Solaris Host

Use the Connector Management tool in the AGM Domain Manager service to upgrade or uninstall the Actifio Connector on your hosts when new versions are available. Refer to [Maintaining Connectors on Hosts](#) on page 8.

Adding a Solaris Host through the Actifio Desktop

To add a new host:

1. Open the **Domain Manager**.
2. From the service menu, select **New Host...**
3. In the Add a New Host form, enter the name, fully qualified domain name, or the IP address of the host in **Host Name**. The name of a host should start with a letter, and can contain letters, digits (0-9), and an underscore ('_').
4. Click **Discover Details**. Actifio Desktop lists all IP addresses used by the host.
5. Enter the IP address of the host in **IP Address**. Click **Add** to add multiple IP addresses for a host.
6. (Optional) Add a **Friendly Name**.
7. In **Member of Organization(s)**, select one or more Actifio Desktop organizations for the host to be a member of. Organizations are explained in **Setting Up Users and Roles With the Domain Manager**.
8. In Select Host Type, select **TPGS**.

A screenshot of the 'Add A New Host' form. The form is divided into several sections. The top section contains 'Host Name*' (with 'sun06.sqa.actifio.com' entered and 'Discover Details' button), 'Friendly Name', 'IP Address' (with 'Add' and 'Clear' buttons), and 'Member of Organization(s)' (with a list including 'ALL', 'Actifioorg', and 'Bharath_ORG'). The bottom section contains 'Select Host Type' (with 'TPGS' selected and highlighted by an orange circle), 'WWPN/iSCSI Port' (with a list of WWPNs), 'Connector Port' (with '5106' entered), 'Use Oracle Database Authentication' (checked), and 'Login Credentials for connector' (with 'dba' as the username and a masked password).

Adding a New Solaris Host

9. The Discover Details step populated the next section with known ports. You can add more. Depending on how the host is accessed, specify one of the following for **WWPN/iSCSI Port**:
 - o If the host can be reached using a Fibre Channel port, select **WWPN**.
 - o If the host can be reached using an IP network, select **iSCSI**. Enter the iSCSI host IQN.

You can add multiple port types for a single host.

10. In Connector Port enter **5106** unless you have changed from the default value. You can also use 56789. Do not use any other port unless instructed by Actifio Support.
11. 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.
12. Click **Add Host**.
13. The next step is [Assigning VDisks for the Host Copy Data \(In-Band CDS Appliance only\)](#) on page 2.

Ensuring NFS Connectivity on a Solaris Host

This section includes:

[Installing the NFS client on a Solaris 10 Host](#) on page 39

[Learning NFS client information from a Solaris 10 Host](#) on page 39

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

Installing the NFS client on a Solaris 10 Host

NFS client and server packages come default on a Solaris host.

To check if the NFS client packages are installed, run:

```
# pkginfo | grep nfs
```

This should return something like:

```
system      SUNWnfsckr      Network File System (NFS) client kernel support (Root)
system      SUNWnfsclr      Network File System (NFS) client support (Root)
system      SUNWnfscl       Network File System (NFS) client support (Usr)
```

If you see nothing, then you must install the packages. To install the NFS client packages on a Solaris host, run:

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

Learning NFS client information from a Solaris 10 Host

An Actifio-approved NFS client package and version must be installed on the host.

Check if portmapper/rpcbind service is running. Run:

```
# ps -ef | grep rpcbind
root 115 1 0 May 31 ?      0:14 /usr/sbin/rpcbind
```

If rpcbind process doesn't show up in the above output, start it by running:

```
# svcadm enable svc:/network/rpc/bind
```

Use rpcinfo to list the registered RPC programs / services. rpcbind service should be registered. Run:

```
# rpcinfo -p
program vers proto  port  service
100000   4   tcp    111  rpcbind
100000   3   tcp    111  rpcbind
100000   2   tcp    111  rpcbind
100000   4   udp    111  rpcbind
100000   3   udp    111  rpcbind
100000   2   udp    111  rpcbind
```

Check if the Solaris host can make an RPC call to rpcbind & nfs programs on the Actifio Sky appliance by running:

```
# rpcinfo -T tcp <#appliance IP> rpcbind
program 100000 version 2 ready and waiting
program 100000 version 3 ready and waiting
program 100000 version 4 ready and waiting
```

```
# rpcinfo -T tcp <#appliance IP> nfs
program 100003 version 2 ready and waiting
program 100003 version 3 ready and waiting
```

If the above commands return the output shown above, then NFS connectivity from Solaris host to the Actifio sky appliance is good.

9 Adding an HP-UX Host

This chapter includes:

[Installing the Actifio Connector on HP-UX Hosts](#) on page 42

[Adding an HP-UX Host through the Actifio Desktop](#) on page 43

Location of UDSAgent.log on HP-UX Hosts

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

Location of Scripts on HP-UX Hosts

You can create scripts to perform pre- and post- actions on applications on the HP-UX host. To use scripts, create a folder called `/act/scripts` and store all scripts there. For detailed instructions on how use VDP scripting, see [Chapter 10, APPID Pre- and Post-Scripts for Scheduled Data Protection Jobs](#) and [Chapter 11, Super Scripts for Workflows and On-Demand Data Access Jobs](#).

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

Installing the Actifio Connector on HP-UX Hosts

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

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

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

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

Manually Uninstalling the Actifio Connector from an HP-UX Host

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

You can also remove connectors from many hosts simultaneously from AGM; see [Maintaining Connectors on Hosts](#) on page 8.

Upgrading the Actifio Connector on an HP-UX Host

Use the Connector Management tool in AGM to upgrade the Actifio Connector on your hosts. Refer to [Maintaining Connectors on Hosts](#) on page 8.

HP-UX Connector Commands

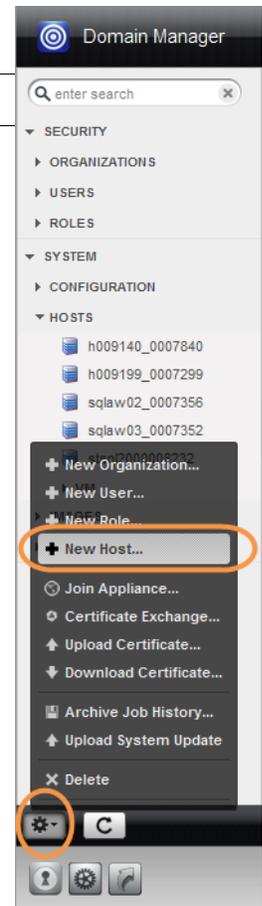
Task	Command option
Verify the successful installation of the Actifio Connector	<code>swlist grep udsagent</code>
Verify the status of the Connector	<code>/etc/udsagent status</code>
Manually stop the Connector service	<code>/etc/udsagent stop</code>
Manually start the Connector service	<code>/etc/udsagent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

Adding an HP-UX Host through the Actifio Desktop

Note: AGM does not support adding HP-UX hosts.

To add a new HP-UX host to a CDS Appliance:

1. Open the **Domain Manager**.
2. From the service menu, select **New Host...**
3. In the Add a New Host form, enter the name, fully qualified domain name, or the IP address of the host in **Host Name**. The name of a host should start with a letter, and can contain letters, digits (0-9), and an underscore ('_').
4. Click **Discover Details**. Actifio Desktop lists all IP addresses used by the host.
5. Enter the IP address of the host in **IP Address**. Click **Add** to add multiple host addresses.
6. (Optional) Add a **Friendly Name**.
7. In **Member of Organization(s)**, select one or more Actifio Desktop organizations for the host to be a member of. Organizations are explained in **Setting Up Users and Roles With the Domain Manager**.
8. In **Select Host Type**, select HP-UX.
9. The Discover Details step populated the next section with known ports. You can add more. Depending on how the host is accessed, specify one of the following for **WWPN/iSCSI Port**:
 - o If the host can be reached using a Fibre Channel port, select **WWPN**.
 - o If the host can be reached using an IP network, select **iSCSI**.

A screenshot of the 'Add A New Host' form in the Actifio Desktop. The form is divided into several sections. The top section has 'Host Name*' (with 'NewHP-UXhost' entered and a 'Discover Details' button) and 'Friendly Name' (with 'HP-UX001' entered). Below this is the 'IP Address' section, which includes a text input field (containing '172.16.202.73'), an 'Add' button, a 'Clear' button, and a 'Delete' button. The 'Member of Organization(s)' section has a dropdown menu set to 'Select: All, None' and three checkboxes: 'ALL' (checked), 'Bharath_Org', and 'Org_4'. The 'Select Host Type' section has a dropdown menu set to 'HP-UX'. Below this is the 'WWPN/iSCSI Port' section, which has a dropdown menu set to 'WWPN', a text input field, and two checkboxes: '2100001B328626E4' and '2100001B328EC7D7'. The bottom section is for 'Login Credentials for connector', with fields for 'Username' and 'Password'. An 'Add Host' button is located at the bottom right of the form. Several fields and buttons are highlighted with orange circles: 'Host Name*', 'Discover Details', 'Add', 'Clear', 'Delete', 'Select Host Type', 'WWPN/iSCSI Port', and the 'Add Host' button.

Adding a New Host

You can add multiple port types for a single host.

Note: If the WWPN is not shown in the selection box, enter the 16-digit WWPN in the space provided and click **Add**. As soon as the host has been added in [Step 12](#) below, map a VDisk to it as detailed in **Configuring Resources and Settings With the Domain Manager**. This is necessary only for HP-UX hosts.

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

10. In Connector Port enter **5106** unless you have changed from the default value. You can also use 56789. Do not use any other port unless instructed by Actifio Support.
11. 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.
12. Click **Add Host**.
13. The next step is [Assigning VDisks for the Host Copy Data \(In-Band CDS Appliance only\)](#) on page 2.

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

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

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

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

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

Troubleshooting APPID Scripts

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

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

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

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

Sample APPID Script for Windows

```
@echo OFF

if /i %1 equ init goto :handle_init
if /i %1 equ fini goto :handle_fini
if /i %1 equ freeze goto :handle_freeze
if /i %1 equ thaw goto :handle_thaw
if /i %1 equ abort goto :handle_abort
echo Unknown command %1

goto :eof
:handle_init
    echo Got an init command
    ping -n 5 google.com
    echo %time% >C:\inittime.txt
    whoami >> C:\inittime.txt
    goto :end

:handle_fini
    echo Got a fini command
    ping -n 5 google.com
    echo %time% >C:\Finishtime.txt
    whoami >> C:\Finishtime.txt
    goto :end

:handle_freeze
    echo Got a freeze command
    ping -n 10 google.com
    echo %time% >C:\pretime.txt
    whoami >> C:\pretime.txt
    goto :end

:handle_thaw
    echo Got a thaw command
    ping -n 5 google.com
    echo %time% >C:\posttime.txt
    whoami >> C:\posttime.txt
    goto :end

:handle_abort
    echo Got an abort command
    ping -n 5 google.com
    echo %time% >C:\aborttime.txt
    whoami >> C:\aborttime.txt
    goto :end

:end
echo Done processing commands
```

Sample APPID Script for Linux

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

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

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

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

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

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

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

The VDP host-side super scripts are invoked for on-demand jobs that are triggered by the CLI with the **-scripts** argument. Supported CLI jobs are listed in the [CLI Commands Supported in Super Scripts](#) on page 50.

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

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

This chapter contains the following topics:

- [Super Script Phases](#) on page 48
- [Super Script Arguments](#) on page 48
- [Super Script Timeouts](#) on page 49
- [Super Script Environment Variables](#) on page 49
- [CLI Commands Supported in Super Scripts](#) on page 50
- [Sample Super Scripts](#) on page 51

Super Script Naming Conventions and Location

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

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

Super Script Phases

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

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

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

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

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

Super Script Arguments

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

Example

This example demonstrates a database handler on a Unix platform:

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

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

Script Returns and Failures

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

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

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

Super Script Timeouts

Each super script may be specified with individual timeout values in seconds. If a script for a given phase runs beyond the timeout, the script is marked as failed and the job-in progress is aborted. The default value is 60 seconds:

Example: (script: /act/scripts/init.sh <appid> <argument> timeout = 120)

Refer to the [CLI Commands Supported in Super Scripts](#) on page 50 for CLI usage examples.

Super Script Environment Variables

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

For example:

Current phase (PHASE) is exported as ACT_PHASE

Current VDP job name (JOBNAME) is exported as ACT_JOBNAME

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

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

CLI Commands Supported in Super Scripts

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

- `udstask backup`
- `udstask restoreimage`
- `udstask cloneimage`
- `udstask mountimage`
- `udstask mountimage`
- `udstask testfailover`
- `udstask failover`
- `udstask deletefailover`
- `udstask createliveclone`
- `udstask refreshliveclone`
- `udstask prepmount`
- `udstask prepunmount`

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

init: when the job is just started

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

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

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

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

`-script`

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

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

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

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

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

Sample Super Scripts

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

Sample Super Script for Windows

At: \<InstallDir>\scripts

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

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

Sample Super Script for Linux and other Unix Platforms

For Linux: /act/scripts

Example: /act/scripts/wrapper_script.sh

```
#!/bin/bash

LOG_FILE="/tmp/act_script.log"

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

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


Index

A

- Actifio Change Tracking Driver 10
- Actifio Connector
 - encrypted network traffic 6
- Actifio Connector installer file, downloading 7
- AIX connector
 - installing 28
 - uninstalling 28
- AIX host
 - adding to appliance 29
 - installing/modifying Actifio Connector 17, 28
 - supported configurations 27
- assigning VDisks to a host 2
- autodiscover applications on a host 3

B

- backup and restore jobs 47
- batch files 47

C

- CIFS file systems 14
- connecting a host, overview 1
- contact information, Actifio Support ii
- copyright ii

D

- data transport mode, NFS or SAN 14
- deleting hosts 4
- downloading the Actifio Connector installer file 7

E

- ESXi cluster 14
- Exchange 14

F

- Filter Driver, see Actifio Change Tracking Driver

H

- HMC host, see IBM HMC host
- host type
 - AIX 29
 - HP-UX 43
 - IBM HMC 32
 - Solaris 37

- TPGS 37
- Windows Server 14

hosts

- adding AIX 29
- adding HP-UX 43
- adding IBM HMC 32
- adding Linux 23
- adding Solaris 37
- adding Windows Server 13, 18

HP-UX host

- adding to appliance 43
- installing/modifying Actifio Connector 42

Hyper-V VMs 14

- Hyper-V, adding a Hyper-V host 18

I

- IBM HMC host
 - adding 32
 - vSCSI connectivity 31
- in-band storage 2
- installer files, Connector, downloading 7
- IQN, for iSCSI port on a host 30, 38, 44

L

- legal matter ii
- Linux connector
 - installing 22
 - uninstalling 22
- Linux host
 - installing/modifying the Actifio Connector 22
- logs
 - on a Linux host 21
 - on a Solaris host 35
 - on a Windows Server host 9
 - on an HP-UX host 41
 - on an IBM AIX host 17, 27
 - on an IBM HMC host 31
- LPAR hosts, see IBM HMC hosts
- LPAR with NPIV mapping 27
- LPARs, discovering 32

M

- Microsoft SCVMM 14

N

new applications, auto-discovering on host 3
NFS protocol 21, 35

O

operations on a host before and after capture 45

P

PowerPC 26
pre- and post- actions on applications 45
pre-scripts and post-scripts 45

R

restore jobs 47
rootvg, bootable, AIX non-HMC 27
rootvg, bootable, for vSCSI-mapped LPARs 31

S

scripts
 on a Linux host 21
 on a Solaris host 35
 on a Windows Server host 9
 on an HP-UX host 41
 on an IBM AIX host 17, 27
 on an IBM HMC host 31
SCVMM 14
SharePoint 14
Solaris host
 adding to the Actifio appliance 37
 installing/modifying the Actifio Connector 36
SQL Server 14
SQL VSS Writer 15
storage, assigning to in-band hosts 2

T

TPGS host type, for Solaris hosts 37
trademarks ii

U

Ubuntu connector installation 22
UDSAgent 6

V

vCenter server 14
VDisk
 mapping to a host 2
VIOs, discovering 32
vSCSI connectivity
 for IBM HMC hosts 31
vSCSI VIO mapped LPARS 31

W

warranty ii
Windows host
 adding to appliance 13

installing/modifying Actifio Connector 10
logs and scripts 9