Connecting Hosts to Actifio Appliances
Contents

Preface ................................................................................................................................................................. v

Actifio Appliances .................................................................................................................................................. v
The ActifioNOW Customer Portal ............................................................................................................................ v
Actifio Support Centers .......................................................................................................................................... v

Chapter 1 - Adding Your Hosts to the Actifio Appliance ......................................................................................... 1

Assigning VDisks for the Host Copy Data (In-Band CDS only) ............................................................................ 2
Discovering VMs .................................................................................................................................................. 3
Discovering VMs from the AGM ............................................................................................................................. 3
Discovering VMs from the Actifio Desktop .............................................................................................................. 5
Discovering Local Applications on a Physical Host Using the AGM ..................................................................... 7
Discovering Applications Over IP with the AGM ..................................................................................................... 8
Discovering Applications on a Physical Host Using the Actifio Desktop ............................................................ 9
Configuring Hosts to Auto-Discover their Applications ....................................................................................... 10
Reconciling Inconsistent Host Information across Multiple Appliances ............................................................. 10
Deleting Hosts Using the Actifio Desktop .............................................................................................................. 11
Restricting a Unix Connector to Communicate with Specific Appliances ......................................................... 12
To Unrestrict a Restricted Unix Connector ........................................................................................................... 13

Chapter 2 - About the Actifio Connector ............................................................................................................... 15
What Does the Connector Do? ................................................................................................................................ 15
The Connector and the Network Environment ........................................................................................................ 16
Host-Side Scripting ............................................................................................................................................... 16
Obtaining the Right Actifio Connector for Your Host ............................................................................................ 17
Maintaining Connectors on Hosts ........................................................................................................................... 18

Chapter 3 - Adding a Windows Server Host ........................................................................................................... 19
Installing the Actifio Connector on Microsoft Windows Hosts ........................................................................... 20
Restricting Windows Connector Communication to Specific Appliances ............................................................ 21
To Unrestrict a Restricted Windows Connector ...................................................................................................... 22
Adding a Windows Server Host to the Actifio Appliance from the Actifio Desktop ............................................. 23
Adding a Windows Server Host to the Actifio Appliance from the AGM ........................................................... 25
Notes on Discovering Specific Microsoft Application Types ................................................................................ 27
<table>
<thead>
<tr>
<th>Chapter 4 - Adding a Hyper-V Host</th>
<th>29</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installing the Actifio Connector on Hyper-V Hosts</td>
<td>29</td>
</tr>
<tr>
<td>Adding a Hyper-V Host through the Actifio Desktop</td>
<td>31</td>
</tr>
<tr>
<td>Adding a Hyper-V Host to the Actifio Appliance from AGM</td>
<td>33</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 5 - Adding a Linux Host</th>
<th>35</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installing the Actifio Connector on a Linux Host</td>
<td>36</td>
</tr>
<tr>
<td>Adding a Linux Host through the Actifio Desktop</td>
<td>38</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 6 - Adding an AIX Host</th>
<th>41</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported AIX Configurations</td>
<td>42</td>
</tr>
<tr>
<td>Installing the Actifio Connector on IBM AIX Hosts</td>
<td>43</td>
</tr>
<tr>
<td>Adding an AIX Host through the Actifio Desktop</td>
<td>44</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 7 - Discovering LPARs from an IBM HMC Host</th>
<th>47</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensuring vSCSI Connectivity on an IBM HMC Host</td>
<td>47</td>
</tr>
<tr>
<td>Adding an IBM HMC Host and its LPARs through the Actifio Desktop</td>
<td>48</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 8 - Adding a Solaris Host</th>
<th>51</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installing the Actifio Connector on Sun Solaris Hosts</td>
<td>52</td>
</tr>
<tr>
<td>Adding a Solaris Host through the Actifio Desktop</td>
<td>53</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 9 - Adding an HP-UX Host (Actifio CDS Only)</th>
<th>55</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installing the Actifio Connector on HP-UX Hosts</td>
<td>56</td>
</tr>
<tr>
<td>Adding an HP-UX Host through the Actifio Desktop</td>
<td>57</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 10 - APPID Pre- and Post-Scripts for Scheduled Data Protection Jobs</th>
<th>59</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sample APPID Script for Windows</td>
<td>60</td>
</tr>
<tr>
<td>Sample APPID Script for Linux</td>
<td>60</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 11 - Super Scripts for Workflows and On-Demand Data Access Jobs</th>
<th>61</th>
</tr>
</thead>
<tbody>
<tr>
<td>Super Script Phases</td>
<td>62</td>
</tr>
<tr>
<td>Super Script Arguments</td>
<td>62</td>
</tr>
<tr>
<td>Super Script Timeouts</td>
<td>63</td>
</tr>
<tr>
<td>Super Script Environment Variables</td>
<td>63</td>
</tr>
<tr>
<td>CLI Commands Supported in Super Scripts</td>
<td>64</td>
</tr>
<tr>
<td>Sample Super Scripts</td>
<td>65</td>
</tr>
</tbody>
</table>

| Index | 67 |
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](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

There are four steps to connecting a non-VMware host to your Actifio system. The first two are operating system-specific, the third applies only to hosts that will use Actifio in-band storage (CDS only). The last is common to all hosts. To add VMs, see *A VMware Manager’s Guide to Actifio Copy Data Management*.

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

<table>
<thead>
<tr>
<th>Host</th>
<th>1 Install the Connector</th>
<th>2 Add the Host</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Server, or</td>
<td>Installing the Actifio Connector on Microsoft Windows Hosts on page 2</td>
<td>Adding a Windows Server Host to the Actifio Appliance from the Actifio Desktop on page 23</td>
</tr>
<tr>
<td>Hyper-V or SCVMM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Linux</td>
<td>Installing the Actifio Connector on a Linux Host on page 36</td>
<td>Adding a Linux Host through the Actifio Desktop on page 38</td>
</tr>
<tr>
<td>IBM AIX</td>
<td>Installing the Actifio Connector on IBM AIX Hosts on page 43</td>
<td>Adding an AIX Host through the Actifio Desktop on page 44</td>
</tr>
<tr>
<td>IBM HMC</td>
<td>The Actifio Connector is not required for IBM HMC hosts.</td>
<td>Adding an IBM HMC Host and its LPARs through the Actifio Desktop on page 48</td>
</tr>
<tr>
<td>Sun Solaris</td>
<td>Installing the Actifio Connector on Sun Solaris Hosts on page 52</td>
<td>Adding a Solaris Host through the Actifio Desktop on page 53</td>
</tr>
<tr>
<td>HP-UX</td>
<td>Installing the Actifio Connector on HP-UX Hosts on page 56</td>
<td>Adding an HP-UX Host through the Actifio Desktop on page 57</td>
</tr>
</tbody>
</table>

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

1. Assigning VDisks for the Host Copy Data (In-Band CDS only) on page 2.
2. Discovering Applications on a Physical Host Using the Actifio Desktop on page 9. You can also configure already-added hosts to auto-discover new applications: Configuring Hosts to Auto-Discover their Applications on page 10.

If you no longer want to protect the applications or VMs on a host, you can delete it from Actifio management; see Deleting Hosts Using the Actifio Desktop on page 11.

You can have pre- and post-scripts run on your applications and VMs when they are triggered by an Actifio 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 as described in Discovering VMs on page 3.*
Assigning VDisks for the Host Copy Data (In-Band CDS only)

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

To assign a virtual disk to a host:

1. Open the Actifio Desktop to the **Domain Manager**.
2. Select the **Host** from the navigation pane.
3. Select **Storage** tab and the **All VDisks** subtab.
4. Select one or more virtual disks.
5. Click **Map**. A confirmation dialog appears.
6. Enter the **SCSI ID** for the VDisk. The SCSI ID is auto-generated if it is left blank.
7. Click **Map VDisk**.
8. If the host is a Windows Server, Linux, or HMC host, then the next step is **Discovering Applications on a Physical Host Using the Actifio Desktop** on page 9.

![Mapping a VDisk to an In-Band Host](image)
Discovering VMs

You can discover VMs in three ways:

Discovering VMs from the AGM
Discovering VMs from the Actifio Desktop on page 5
Discovering VMs from the Actifio Sky/CDS CLI using the vmdiscovery command detailed in the Actifio CLI Reference

Discovering VMs from the AGM

Virtual machines associated with a hypervisor host are discovered through the Application Manager on the AGM. VMs are managed using either VMware snapshots or the Actifio Connector. The datastores on which VMware VMDKs reside may be in-band or out-of-band.

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

To discover VMs, you must first add the VM’s hypervisor as a host on the Actifio appliance. When an ESX host has virtual machines already created, add a vCenter or ESX server/cluster as hosts separately. You can discover and manage the virtual machines associated with a vCenter using an ESX host or cluster from AGM.

**Note:** You can also discover local applications on VMs. In this case, the Actifio Connector must be installed and configured on the VM, and you discover the applications at the individual Actifio CDS or Sky appliance using the Actifio Desktop. See Application Discovery Overview for details.

To discover a VM:

1. Open the Application Manager service in AGM.
2. Click Applications to access the Applications window, then click the Add Virtual Machine button. The Add Virtual Machines window appears.
3. Click vCenter or ESX Hosts and Clusters to instruct AGM where to begin VM discovery.

Use the Application Manager Service Menu to Discover VMs in the AGM
4. Select a vCenter/ESX Host from which you want to discover VMs. The Add Virtual Machines window discovers and displays the ESX host/clusters managed by the vCenter.

**Note:** Use the **ESX Hosts and Clusters** option to view ESX Hosts not associated with a vCenter.

5. Select the virtual machines, then click **Discover VMs**.

6. Select the virtual machines that you would like to add to the AGM, then click **Add Using Round-Robin**. This selection randomly and evenly distributes the discovered VMs from among all Actifio appliances which have the vCenter host discovered.

The right pane shows the recommended placement. You can also specify the appliance from which you want to add the virtual machines from the drop-down list under **Appliance**.
7. Click **Add Selected to Appliance**.

8. Verify the VM discovery status. You can choose to manage additional VMs or proceed to the application list in the Application Manager.

   The virtual machines are added to the list of applications in the Application window of the Application Manager. This list also includes the ESXs that can be seen from that vCenter and the discovered VMs are added as hosts.

   **Note:** If you must delete VMs, see Deleting Applications and VMs Using AGM.

---

**Discovering VMs from the Actifio Desktop**

Virtual machines associated with a hypervisor host are discovered through the Application Manager. To discover VMs, you must first add the VM’s hypervisor as a host.

**Note:** When you discover a VMware vCenter, all ESXi hosts are automatically discovered.

**Note:** Virtual machine discovery on a hypervisor requires an Actifio user with ‘Host Manage’ Actifio rights.

To discover a VM:

1. Open the Actifio Desktop to the **Application Manager**. By default the VM tab is selected.
2. Click **Discover VM(s)**... from the service menu.

   ![Use the Application Manager Service Menu to Discover VMs in the Desktop](image)

   **Use the Application Manager Service Menu to Discover VMs in the Desktop**

3. The Discover VM(s) window appears.
Discovering vCenters on a Host

4. In the Discover VM(s) window, select either VMware or Hyper-V.
5. Depending on your previous choice select either a vCenter/ESX Host or SCVMM/Hyper-V Server. The Discover VMs window discovers and displays the host/appliances managed by the selected hypervisor.

Discovering VMs on an ESX Host in a vCenter

6. Select the virtual machines to protect.
7. Click Discover. The Virtual Machines are added to the list of virtual machines at Application Manager > Applications by Type > VM.
8. After discovery, the virtual machines and hypervisors are added as hosts in the Domain Manager.

Note: The Actifio appliance relies on synchronicity between an Actifio appliance and its discovered hosts. Hosts that are not connected to an NTP server can drift, resulting in differences between the host’s record and the Actifio appliance’s record of the time snapshots taken or other actions performed by the Actifio appliance.
Discovering Local Applications on a Physical Host Using the AGM

You can discover local applications on physical hosts and on VMs. You must have the Actifio Connector installed and configured.

**Note:** To discover clustered applications and IBM LPAR virtual machines running on Virtual I/O Servers (VIOS) managed by IBM Hardware Management Console, see Discovering Applications Over IP.

To discover a local application:

1. Open the Application Manager service in AGM.
2. Click Applications to access the Applications window, then click the Add Application button. The Add Applications window appears.
3. Select Using Existing Host.
4. From the Appliance drop-down list, select the Actifio appliance that connects to the host(s) that includes the applications you would want AGM to discover. You can choose All for multiple Actifio appliances or select a specific appliance.
5. To modify the appearance of the fields that appear in the table, you can:
   - Adjust Fields—To modify the fields that appear in the table, right-click within the table header row and click the check boxes for the fields you want displayed (or those fields you do not want to view).
   - Sort Content—To sort the content listed in a table column by alphanumeric order, select a column header and then click the Up or Down arrow to change the order.
   - Adjust Column Width—To adjust the width of a table column to show more content in the table, drag the column divider in a column header to the left or right to resize the column width. Column dividers are marked by a pair of thin gray lines.
6. To filter the list of hosts and view only a subset, select from the choices listed under Available Hosts (Host, IP, Friendly Path), then enter a filter string in text box. Hosts are then automatically filtered in the table based on your selections.

**Note:** To clear a single filter without clearing all filters, click the x to the right of the applied filter. To clear all filtering, click Clear Filters.

7. Select one or more hosts from the Available Hosts table, then click Add Applications.

**Note:** The application discovery process can sometimes take a period of time (minutes) depending on the number of applications associated with the selected hosts.

8. Verify the application discovery status in the Notification Center.
9. Add additional applications or proceed to the application list in the Application Manager. The discovered applications are added to the list of applications in the Application List window of the Application Manager.
Discovering Applications Over IP with the AGM

You can discover local and clustered applications on hosts that are not yet known to AGM and the Actifio appliances. Use this method also to discover IBM AIX-based Virtual IO Servers (VIOS) managed by Hardware Management Console. You must have the Actifio Connector installed and configured (see Connecting Hosts to Actifio Appliances in the Actifio Documentation Library located on each Actifio appliance and also on the ActifioNOW customer portal.

To discover an application over IP, including LPAR virtual machines running on AIX VIOS:

1. Open the Application Manager service in AGM.
2. Click Applications to access the Applications window, then click the Add Application button. The Add Applications window appears.

**Note:** Once you fill in all of the fields in the Add Applications window the Add Applications button will be enabled.

4. From the Target Appliance drop-down list, select the Actifio appliance that connects to the host(s) that includes the applications you would want AGM to discover.
5. Select the host type. Choose from the following host types:
   - Standard (ESX Host, Generic Hyper-V, HP-UX, OpenVMS, SCVMM, TPGS, vCenter)
   - IBM HMC
6. If necessary, enter login credentials (username and password) for the host that includes the applications that you want to discover. Login credentials may be required if you are trying to connect to a management server such as an ESX host or vCenter server.
7. To discover local and/or cluster applications, specify the following:
   - To discover only clustered applications, specify an appliance IP or select an existing appliance host.
   - To discover both local and clustered applications, specify the IP of an appliance node or select an existing appliance node.
8. Click Add Applications.

**Note:** The application discovery process can sometimes take a period of time (minutes) depending on the number of applications associated with the selected host.

**Note:** When clustered applications are discovered, a host for each appliance node is added automatically if one does not exist already.

9. Verify the application discovery status in the Notification Center.
10. Add additional applications or proceed to the application list in the Application Manager. The discovered applications are added to the list of applications in the Applications window of the Application Manager.
Discovering Applications on a Physical Host Using the Actifio Desktop

**Note:** This details how to discover applications on physical hosts. To discover VMs, see Discovering VMs from the AGM on page 3 and Discovering VMs from the Actifio Desktop on page 5.

You can discover applications on physical hosts and on VMs that are known to the Actifio appliance. To discover applications, a user must be assigned a role with the 'Application Manage' right.

To discover an application:

1. Open the Actifio Desktop to the **Application Manager**.
2. From the service menu, select **Discover App(s)**. The Discover Applications dialog appears.
3. Select **Using Existing Host** and select the host that includes the application you would like to protect.
4. Click **Discover**. The navigation pane lists all the applications attached to the selected host as soon as they are discovered.

If you are discovering applications on a Windows Server host, be sure to see **Notes on Discovering Specific Microsoft Application Types** on page 27.

After you have discovered applications and VMs, assign SLAs as detailed in **Planning and Developing Service Level Agreements**.

The first time an application or file system is protected, it can consume a lot of resources relative to the later incremental snapshot jobs. If you are adding many applications in a short time, think carefully about how you will develop your SLAs. It is usually a good idea to run a few on-demand jobs at selected low-demand times to ensure that the system continues to run smoothly as all the new initial-ingest jobs come in.
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 Domain Manager to System > Configuration > Hosts.
2. Select from the list of previously created hosts in the Hosts section of the Domain Manager.
3. Click the Details tab. You will see a summary of configuration information related to the selected host.
4. Check the Enable Auto Discovery check box and click Save.

Enabling Application Auto Discovery for a vCenter Host

Note: This feature is not supported for VMware ESX hosts because discovery is done via the vCenter host. You can enable auto-discovery for vCenter hosts.

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 Actifio 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 Actifio 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.
Deleting Hosts Using the Actifio Desktop

You can delete Hosts after un-mapping any VDisks associated with them. To delete a host:

1. Open the Domain Manager.
2. Under System > Hosts, select the host to delete.

Deleting a Host in the Domain Manager

3. Right-click it to open the service menu, and click Delete.
4. Click Yes in the confirmation dialog.
Restricting a Unix Connector to Communicate with Specific Appliances

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

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

**Note:** The procedure for a Windows host is the same, except that you copy the appliance certificate to `C:\Program Files\Actifio\certs\trusted`. See Restricting Windows Connector Communication to Specific Appliances on page 21.

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

1. On **AuthorizedAppliance**, open the Actifio Desktop to the Domain Manager and download the certificate.

   ![Domain Manager](image)

   **Downloading an Appliance Certificate**

   2. Save the file with meaningful and unique name and with the extension `.crt` like AuthorizedAppliance1.crt. The file name is not important.

   3. Copy the certificate file to the host and set permissions and ownership:


   ```
   /act/certs/trusted/CDSA.crt
   chmod 600 /act/certs/trusted/CDSA.crt
   chown root:root /act/certs/trusted/CDSA.crt
   ```
4. Restart the connector (UDSAgent):
   a. Get the PID of the connector: `pgrep udsagent` (or `ps -ef | grep udsagent`)
   b. Restart the connector: `/etc/rc.d/init.d/udsagent restart`
   c. Validate that the connector has restarted by the new PID:
      `pgrep udsagent` (or `ps -ef | grep udsagent`)


5. Attempt application discovery from **AuthorizedAppliance**. You should see something like this. Discovery will succeed.

```
2017-06-08 13:06:13.165 GEN-INFO  [19415] SSL Sock: certificate details:
```

6. Attempt application discovery from **UnauthorizedAppliance**. You should see something like this. Discovery will fail.

```
2017-06-08 13:07:06.883 GEN-INFO  [19577] SSL Sock: certificate details:
```

If you attempt application discovery from the **UnauthorizedAppliance** Actifio Desktop, you will get this message:

![Discovery Failure Error Message](image)

**To Unrestrict a Restricted Unix Connector**

1. Delete the certificate file on host side: `rm /act/certs/trusted/CDSA.crt`
2. Confirm PID: `pgrep udsagent` (or `ps -ef | grep udsagent`)
3. Restart the connector: `/etc/rc.d/init.d/udsagent restart`
4. Validate new PIDs: `pgrep udsagent` (or `ps -ef | grep udsagent`)
2  About the Actifio Connector

This chapter describes the Actifio Connectors, including Obtaining the Right Actifio Connector for Your Host on page 17 and Maintaining Connectors on Hosts on page 18. The Actifio Connector is a small-footprint process that you install on your hosts.

This section includes:

- What Does the Connector Do? on page 15
- The Connector and the Network Environment on page 16
- Host-Side Scripting on page 16
- Obtaining the Right Actifio Connector for Your Host on page 17
- Maintaining Connectors on Hosts on page 18

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 is compatible with older versions of the Actifio Connectors up to two minor releases back (Actifio software version 9.0 supports Actifio 8.0.x and Actifio 8.1.x 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 Actifio writes to the staging disk. This is typically slower than reading files on the protected volume already.

- On Windows, exclude C:\Windows\act
- 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 an Actifio Workflow job.

For detailed instructions on how use Actifio 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.
Maintaining Connectors on Hosts

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

1. Open the **Domain Manager** to **System > Configuration > Connector Management**. This sequence opens the Connector Manager. You can see each of your hosts and the Actifio Connector installed on each host.

2. From the Discovered Hosts pane on the left, select which hosts are to get upgraded connectors by clicking on their green + icons. This action moves them to the Selected Hosts pane on the right. Once there, a red - icon allows you to remove them back to the Discovered Hosts list.

3. Click **Upgrade** to upgrade the Actifio Connector on the selected hosts.

4. Select an upgrade option:
   - **Start Upgrade**: Starts the upgrade. The upgrade will fail if there are jobs running on the selected host.
   - **Force Upgrade**: Attempts to cancel running jobs and then performs the upgrade immediately.

5. Click **Submit**.

![The Connector Manager Showing a Host to Receive a Connector Upgrade](image-url)
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 20
- Restricting Windows Connector Communication to Specific Appliances on page 21
- Adding a Windows Server Host to the Actifio Appliance from the Actifio Desktop on page 23
- Notes on Discovering Specific Microsoft Application Types on page 27

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 Actifio 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.

Actifio Change Tracking Driver Options for Windows Physical Hosts

When installing the Windows Actifio Connector you have the option of installing the Actifio 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.
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 Actifio 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 18.
Restricting Windows Connector Communication to Specific Appliances

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

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

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

1. On AuthorizedAppliance, open the Actifio Desktop to the Domain Manager and download the certificate.

![Downloading an Appliance Certificate](image)

2. Save the file with meaningful unique name and with the extension .crt like AuthorizedAppliance1.crt. The file name is not important.
3. Copy the certificate file to the host at C:\Program Files\Actifio\certs\trusted.
4. Stop and start the connector (UDSAgent) using services.msc.
5. Attempt application discovery from the AuthorizedAppliance Actifio Desktop. Discovery will succeed.
6. Attempt application discovery from the UnauthorizedAppliance Actifio Desktop. 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 21.
Adding a Windows Server Host to the Actifio Appliance from the Actifio Desktop

**Note**: This is the procedure to add a Windows server host using the Actifio Desktop. To add a host using the AGM, refer to the AGM online help.

To add a new Windows host from the Actifio Desktop:

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. You can enter an additional IP address in **IP Address**. Click **Add** to add multiple IP addresses for a host.
6. In **Member of Organization(s)**, select one or more Actifio organizations for the host to be a member of. Actifio Desktop Organizations are explained in Setting Up Users and Roles With the Domain Manager.
7. In **Select Host Type**, the type you pick depends on what you’re using the Windows host for. These are detailed in Windows Host Types on page 24.
8. Depending on how the host is accessed, specify one of the following for **WWPN/iSCSI Port**:
   - If the host can be reached using a Fibre Channel port, select **WWPN (World Wide Port Name)**.
   - If the host can be reached using an IP network, select **iSCSI** (Internet Small Computer System Interface). 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**.

9. 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.

10. Enter the username and password of the Actifio Connector on the host if you intend to:
   - Run pre- and post-scripts on the host
   - Protect a CIFS share (the login credentials of the local/domain user on Windows who mapped the share).

11. Click **Add Host**.

12. The next steps are:
   - Assigning VDisks for the Host Copy Data (In-Band CDS only) on page 2.
   - See Notes on Discovering Specific Microsoft Application Types on page 27, then go to Discovering Applications on a Physical Host Using the Actifio Desktop on page 9.
Adding a Windows Server Host to the Actifio Appliance from the 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 ('_').
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 **Windows Host Types** on page 24.

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 Actifio organizations for the host to be a member of. Organizations are explained in the AGM Online Help.
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**

To protect file systems, follow the common procedure in Discovering Applications on a Physical Host Using the Actifio Desktop on page 9.

**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 29
- Adding a Hyper-V Host through the Actifio Desktop on page 31
- Adding a Hyper-V Host to the Actifio Appliance from AGM on page 33

**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. To use scripts, create a folder called /act/scripts and store all scripts there. Details on Actifio 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.
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 Actifio 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**.

**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 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 18.
Adding a Hyper-V Host through the Actifio Desktop

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 Hyper-V Server. The Actifio Connector natively supports AIX servers, so you do not have to select a host type.

Adding a New AIX Host

9. Depending on how the host is accessed, specify one of the following for WWPN/iSCSI Port:
   - If the host can be reached using a Fibre Channel port, select WWPN (World Wide Port Name).
   - 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 steps are:
   - Assigning VDisks for the Host Copy Data (In-Band CDS only) on page 2.
   - Discovering Applications on a Physical Host Using the Actifio Desktop on page 9.
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 Actifio organizations for the host to be a member of. Organizations are explained in the AGM Online Help.
This chapter includes:

- Installing the Actifio Connector on a Linux Host on page 36
- Adding a Linux Host through the Actifio Desktop on page 38

**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 Actifio 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, 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 a NFS share.

![Setting Disk Preference to NFS](image-url)
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:

```
/etc/init.d/udsagent restart
```
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:
   ```bash
   [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:
      ```bash
      rpm -e udsagent-7.1.0-62339.x86_64
      ```

Upgrading the Actifio Connector on a Linux Host

Use the Connector Management tool 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 18.
Adding a Linux Host through the Actifio Desktop

Note: AGM does not support adding Linux hosts.

To add a new Linux 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 and click Add. You can 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. Actifio Desktop 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 Linux hosts, so you do not have to select a host type.

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**:
   - If the host can be reached using a Fibre Channel port, select **WWPN (World Wide Port Name)**.
   - 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 steps are:
   - **Assigning VDisks for the Host Copy Data (In-Band CDS only)** on page 2.
   - **Discovering Applications on a Physical Host Using the Actifio Desktop** on page 9.
6  Adding an AIX Host

This chapter includes:

- Supported AIX Configurations on page 42
- Installing the Actifio Connector on IBM AIX Hosts on page 43
- Adding an AIX Host through the Actifio Desktop on page 44

**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 Actifio 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).

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

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

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

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

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

These hosts can be added as physical hosts, as detailed in Adding an AIX Host through the Actifio Desktop on page 44. 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 47.
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 -aXgd connector-AIX-<version>.bff all`.

**Tasks and Available Command Options**

<table>
<thead>
<tr>
<th>Task</th>
<th>Command option</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify the successful installation of the Actifio Connector</td>
<td>`lslpp -L</td>
</tr>
<tr>
<td>Verify the status of the Connector</td>
<td><code>/etc/udsagent status</code></td>
</tr>
<tr>
<td>Manually stop the Connector service</td>
<td><code>/etc/udsagent stop</code></td>
</tr>
<tr>
<td>Manually start the Connector service</td>
<td><code>/etc/udsagent start</code></td>
</tr>
<tr>
<td>View the Connector log</td>
<td><code>/var/act/log/UDSAgent.log</code></td>
</tr>
</tbody>
</table>

Uninstalling the Actifio Connector from a AIX Host

To uninstall the Actifio Connector from a AIX host, run: `installp -u udsagent`

Upgrading the Actifio Connector on an AIX Host

Use the Connector Management tool 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 18.
Adding an AIX Host through the Actifio Desktop

Note: The 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.
9. Depending on how the host is accessed, specify one of the following for WWPN/iSCSI Port:
   
   - If the host can be reached using a Fibre Channel port, select WWPN (World Wide Port Name).
   - 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 steps are:

   - Assigning VDisks for the Host Copy Data (In-Band CDS only) on page 2.
   - Discovering Applications on a Physical Host Using the Actifio Desktop on page 9.
This chapter includes:

Ensuring vSCSI Connectivity on an IBM HMC Host on page 47
Adding an IBM HMC Host and its LPARs through the Actifio Desktop on page 48

**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 an Actifio Sky appliance for LPAR discovery, but Sky appliances do not support Fibre Channel connectivity, so the LPARs must be presented to their staging disks over an iSCSI connection.

**Ensuring 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.
- Actifio should have Fibre Channel connectivity to VIO servers catering storage to these LPARs.

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

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

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

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

To discover a vSCSI LPAR host, see Adding an IBM HMC Host and its LPARs through the Actifio Desktop on page 48.
Adding an IBM HMC Host and its LPARs through the Actifio Desktop

**Note:** The AGM does not support adding HMC hosts.

The Actifio appliance discovers all VIOs and LPARs on the IBM HMC host. To add a new 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**.
11. (CDS 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 steps are Assigning VDisks for the Host Copy Data (In-Band CDS only) on page 2 and then Discovering Applications on a Physical Host Using the Actifio Desktop on page 9.
8 Adding a Solaris Host

This chapter includes:

- Installing the Actifio Connector on Sun Solaris Hosts on page 52
- Adding a Solaris Host through the Actifio Desktop on page 53

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 Solaris host. To use scripts, create a folder called /act/scripts and store all scripts there. For detailed instructions on how use Actifio 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

The AGM does not support adding Solaris hosts. They must be added directly from the appliance. The Actifio CDS appliance does not support iSCSI for Solaris SPARC hosts but the Actifio Sky appliance does support it.

Using NFS protocol for Solaris LDOM and Solaris Zones hosts in the 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.
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:
   - `SPARC: pkgadd -d /tmp/connector-Solaris_SPARC-<version>.pkg all`
   - `Solaris x86: pkgadd -d /tmp/connector-Solaris_x86-<version>.pkg all`

### Tasks and Available Command Options

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

Uninstalling the Actifio Connector from a Solaris Host

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

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

Use the Connector Management tool 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 18.

Manually Upgrading the Actifio Connector from a Solaris Host

To upgrade the connector manually:

1. Back-up the logs found in `/var/act/log/`
2. Uninstall the connector.
3. Install the new connector.
4. Restore the backed up logs to `/var/act/log`. 
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**.

![Adding a New Solaris Host](image_url)
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:
    If the host can be reached using a Fibre Channel port, select WWPN.
    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 steps are:
    Assigning VDisks for the Host Copy Data (In-Band CDS only) on page 2.
    Discovering Applications on a Physical Host Using the Actifio Desktop on page 9.
This chapter includes:

- Installing the Actifio Connector on HP-UX Hosts on page 56
- Adding an HP-UX Host through the Actifio Desktop on page 57

**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 Actifio 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.
Installing the Actifio Connector on HP-UX Hosts

For HP-UX, the installer comes as the file: `connector-HPUX-&lt;version&gt;.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://&lt;ACTIFIO_APPLIANCE_IP&gt;` 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 /&lt;connector_filename&gt;.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.

Uninstalling the Actifio Connector from an HP-UX Host

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

Upgrading the Actifio Connector on an HP-UX Host

Use the Connector Management tool in the Actifio Desktop Domain Manager service to upgrade the Actifio Connector on your hosts. Refer to the section **Maintaining Connectors on Hosts** on page 18.

### HP-UX Connector Commands

<table>
<thead>
<tr>
<th>Task</th>
<th>Command option</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify the successful installation of the Actifio Connector</td>
<td>`swlist</td>
</tr>
<tr>
<td>Verify the status of the Connector</td>
<td><code>/etc/udsagent status</code></td>
</tr>
<tr>
<td>Manually stop the Connector service</td>
<td><code>/etc/udsagent stop</code></td>
</tr>
<tr>
<td>Manually start the Connector service</td>
<td><code>/etc/udsagent start</code></td>
</tr>
<tr>
<td>See the Connector logs</td>
<td><code>/var/act/log/UDSAgent.log</code></td>
</tr>
</tbody>
</table>
Adding an HP-UX Host through the Actifio Desktop

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

To add a new HP-UX host to an Actifio 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**:
   - If the host can be reached using a Fibre Channel port, select **WWPN**.
   - If the host can be reached using an IP network, select **iSCSI**.

![Adding a New Host](image-url)
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 steps are:
   - Assigning VDisks for the Host Copy Data (In-Band CDS only) on page 2.
   - Discovering Applications on a Physical Host Using the Actifio Desktop on page 9.
You can create application-specific pre-scripts and post-scripts to perform operations on a host before and after an Actifio 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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Default Timeout</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Init</td>
<td>The init script is invoked with a <code>init</code> parameter when the backup is about to start.</td>
<td>120 seconds</td>
<td>N/A</td>
</tr>
<tr>
<td>Freeze</td>
<td>The freeze script is invoked with a <code>freeze</code> parameter when the backup operation is just about to freeze the application.</td>
<td>60 seconds</td>
<td>1 - 120 seconds</td>
</tr>
<tr>
<td>Unfreeze</td>
<td>The thaw script is invoked with a <code>thaw</code> parameter when the backup operation is just finished unreeing the application.</td>
<td>60 seconds</td>
<td>1 - 120 seconds</td>
</tr>
<tr>
<td>Finish</td>
<td>The fini script is invoked with a <code>fini</code> parameter when the backup operation is about to complete. This phase is applicable only for the Actifio Connector.</td>
<td>60 seconds</td>
<td>1 - 86400 seconds</td>
</tr>
<tr>
<td>Abort</td>
<td>The abort script is invoked with an <code>abort</code> parameter if the backup is aborted for any reason.</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

### Troubleshooting APPID Scripts

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

```
PrepareForVdpSnapshot: 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 Actifio 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 64.

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 62
- Super Script Arguments on page 62
- Super Script Timeouts on page 63
- Super Script Environment Variables on page 63
- CLI Commands Supported in Super Scripts on page 64
- Sample Super Scripts on page 65

**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 600 seconds:

Example: (script:/act/scripts/init.sh <appid> <argument> timeout = 60)

Refer to the CLI Commands Supported in Super Scripts on page 64 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 Actifio 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 600 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=<scriptname>: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=MYSCRIPT.sh:phase=PRE:timeout=60:args=ARG1,ARG2"
```
Sample Super Scripts

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

Sample Super Script for Windows
At: \<InstallDir>\scripts
Example: C:\Program Files\Actifio\scripts\wrapper_script.bat

```bash
echo ........ Running %ACT_PHASE% hook ........ >> c:\act_script.log
echo %time% >> c:\act_script.log
echo Args: %0 %1 %2 >> 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

```bash
#!/bin/bash
LOG_FILE="/tmp/act_script.log"

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 "........ 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 ........"
```
Index

A
Actifio Change Tracking Driver 20
Actifio Connector
downloading from ARC 17
encrypted network traffic 16
keeping updated 18
Actifio Connector installer file, downloading 17
AIX connector
installing 43
uninstalling 43
AIX host
adding to appliance 31, 44
installing/modifying Actifio Connector 29, 43
supported configurations 42
applications, discovering on host 9
assigning VDisks to a host 2
autodiscover applications on a host 10
B
backup and restore jobs 61
batch files 61
C
CIFS file systems 24
connecting a host, overview 1
Connector, see Actifio Connector
contact information, Actifio Support ii
copyright ii
D
data transport mode, NFS or SAN 26
deleting hosts 11
discovering
VMs 5
discovering applications 9
downloading the Actifio Connector installer file 17
E
ESX server 5
ESXi cluster 24
Exchange 24
F
Filter Driver, see Actifio Change Tracking Driver
H
HMC host, see IBM HMC host
host type
AIX 31, 44
HP-UX 57
IBM HMC 48
Linux 39
Solaris 53
TPGS 53
Windows Server 24
hosts
adding AIX 31, 44
adding HP-UX 57
adding IBM HMC 48
adding Linux 38
adding Solaris 53
adding Windows Server 23, 25, 33
HP-UX host
adding to appliance 57
installing/modifying Actifio Connector 56
Hyper-V hosts not in SCVMM, discovering 6
Hyper-V SCVMM, discovering 6
Hyper-V VMs 24
Hyper-V, adding a Hyper-V host 33
I
IBM HMC host
adding 48
vSCSI connectivity 47
in-band storage 2
installer files, Connector, downloading 17
IQN, for iSCSI port on a host 24, 32, 39, 45, 54, 58
L
legal matter ii
Linux connector
installing 36
uninstalling 36
Linux host
adding to Actifio appliance 38
installing/modifying the Actifio Connector 36
logs
on a Linux host 35
on a Solaris host 51
on a Windows Server host 19
on an HP-UX host 55
on an IBM AIX host 29, 41
on an IBM HMC host 47

LPAR hosts, see IBM HMC hosts
LPAR with NPIV mapping 42
LPARs, discovering 48

M
Microsoft SCVMM 24

N
new applications, auto-discovering on host 10
NFS protocol 35, 51

O
operations on a host before and after capture 59

P
pre- and post-actions on applications 59
pre-scripts and post-scripts 59

R
restore jobs 61
rootvg, bootable, AIX non-HMC 42
rootvg, bootable, for vSCSI-mapped LPARs 47

S
scripts
  on a Linux host 35
  on a Solaris host 51
  on a Windows Server host 19
  on an HP-UX host 55
  on an IBM AIX host 29, 41
  on an IBM HMC host 47
SCVMM 24
SCVMM/Hyper-V Server, discovering 6
Service Menu 3, 4, 5
SharePoint 24
Solaris host
  adding to the Actifio appliance 53
  installing/modifying the Actifio Connector 52
SQL Server 24
SQL VSS Writer 27
storage, assigning to in-band hosts 2

T
TPGS host type, for Solaris hosts 53
trademarks ii

U
UDSAgent 16

V
vCenter server 24
vCenter/ESX Host, discovering 6
VDisk
  mapping to a host 2
VIOs, discovering 48
VM
  discovering 5
VMware ESX Server, discovering 6
VMware vCenter, discovering 6
vSCSI connectivity
  for IBM HMC hosts 47
vSCSI VIO mapped LPARS 47

W
warranty ii
Windows host
  adding to appliance 23, 25
  installing/modifying Actifio Connector 20
  logs and scripts 19