Connecting Hosts to IBM InfoSphere VDP Appliances

InfoSphere VDP 9.0

Contents

1 Adding Your Hosts to the InfoSphere VDP Appliance

These are the steps to connecting a non-VMware host to your VDP system. To add VMs, see ***A VMware Administrator's Guide to Copy Data Management***.

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

Host	1 Install the Connector	2 Add the Host
Windows Server, or Hyper-V or SCVMM	Installing the VDP Connector on Microsoft Windows Hosts on page 10	Adding a Windows Server Host to the InfoSphere VDP Appliance from IVGM on page 13
Linux	Installing the VDP Connector on a Linux Host on page 22	Adding a Linux Host to the InfoSphere VDP Appliance from IVGM on page 23
IBM AIX	Installing the VDP Connector on IBM AIX Hosts on page 22	Adding an AIX Host through the VDP Desktop on page 23
IBM HMC	The Connector is not required for IBM HMC hosts.	Adding an IBM HMC Host and its LPARs through the VDP Desktop on page 26
Sun Solaris	Installing the VDP Connector on Sun Solaris Hosts on page 30	Adding a Solaris Host through the VDP Desktop on page 31
HP-UX	Installing the VDP Connector on HP-UX Hosts on page 34	Adding an HP-UX Host through the VDP Desktop on page 35

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

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

If you no longer want to protect the applications or VMs on a host, you can delete it from VDP management; see Deleting Hosts Using the IVGM on page 3.

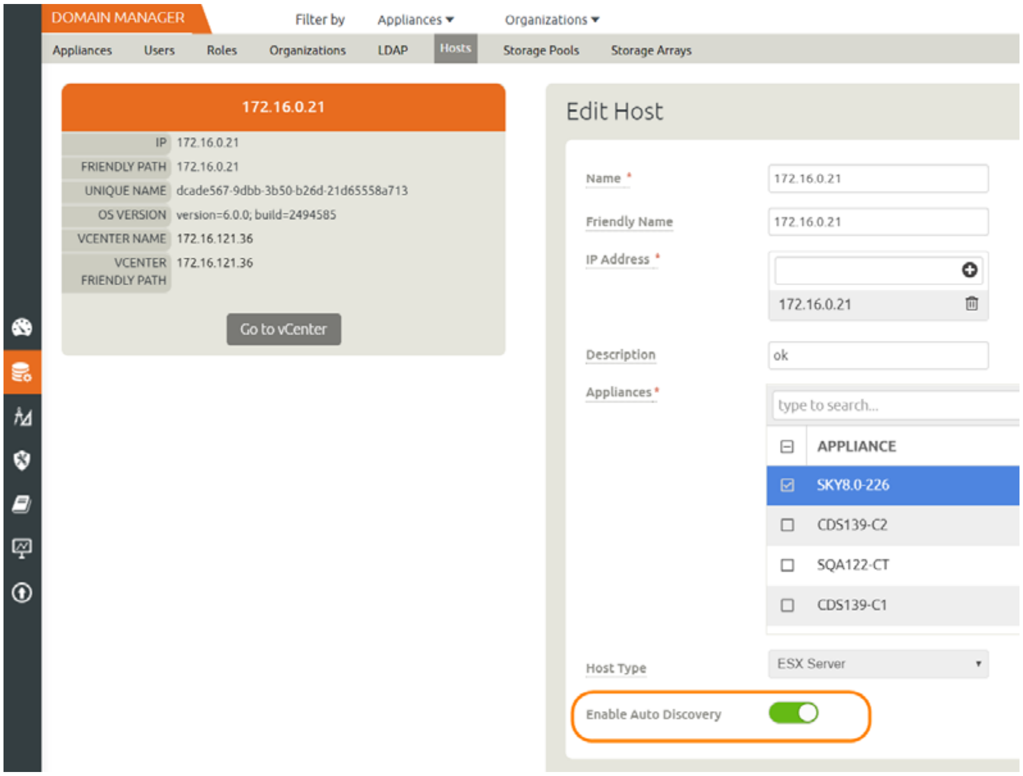
You can have pre- and post-scripts run on your applications and VMs when they are triggered by a VDP job. Scripting is detailed in Chapter 6, APPID Pre- and Post-Scripts for Scheduled Data Protection Jobs and in Chapter 7, Super Scripts for Workflows and On-Demand Data Access Jobs.

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

Configuring Hosts to Auto-Discover their Applications

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

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



172.16.0.21

IP	172.16.0.21
FRIENDLY PATH	172.16.0.21
UNIQUE NAME	dcade567-9dbb-3b50-b26d-21d65558a713
OS VERSION	version=6.0.0; build=2494585
VCENTER NAME	172.16.121.36
VCENTER FRIENDLY PATH	172.16.121.36

Edit Host

Name * 172.16.0.21

Friendly Name 172.16.0.21

IP Address * 172.16.0.21

Description ok

Appliances *

⊟	APPLIANCE
☑	SKY8.0-226
□	CDS139-C2
□	SQA122-CT
□	CDS139-C1

Host Type ESX Server

Enable Auto Discovery ●

Enabling Application Auto Discovery for a vCenter Host

Reconciling Inconsistent Host Information across Multiple Appliances

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

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

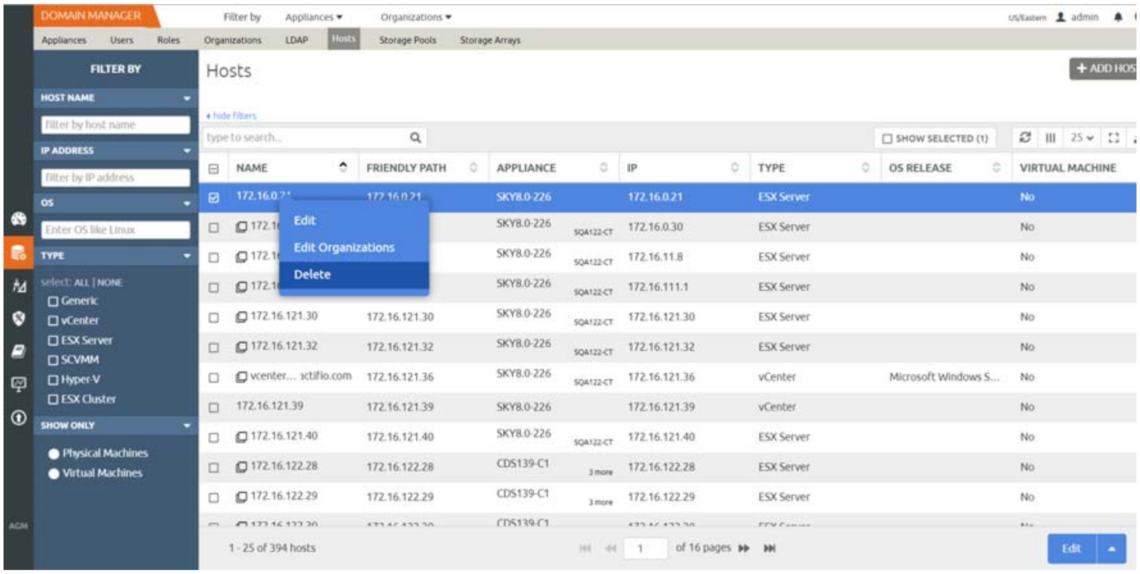
Security Software on Hosts

Security software, including antivirus and other disk monitoring software, can interfere with mounting, cloning, LiveCloning, or restoring any non-VM application to a host. Consider exempting the target disk from the interfering software for the duration of the operation. For more information, see The Connector and the Network Environment on page 6.

Deleting Hosts Using the IVGM

You can delete Hosts. To delete a host:

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



☑	NAME	FRIENDLY PATH	APPLIANCE		IP	TYPE	OS RELEASE	VIRTUAL MACHINE
☑	172.16.0.2'	172.16.0.21	SKY8.0-226		172.16.0.21	ESX Server		No
□	172.1		SKY8.0-226	SQA122-CT	172.16.0.30	ESX Server		No
□	172.1		SKY8.0-226	SQA122-CT	172.16.11.8	ESX Server		No
□	172.1		SKY8.0-226	SQA122-CT	172.16.111.1	ESX Server		No
□	172.16.121.30	172.16.121.30	SKY8.0-226	SQA122-CT	172.16.121.30	ESX Server		No
□	172.16.121.32	172.16.121.32	SKY8.0-226	SQA122-CT	172.16.121.32	ESX Server		No
□	vcenter... ıctifio.com	172.16.121.36	SKY8.0-226	SQA122-CT	172.16.121.36	vCenter	Microsoft Windows S...	No
□	172.16.121.39	172.16.121.39	SKY8.0-226		172.16.121.39	vCenter		No
□	172.16.121.40	172.16.121.40	SKY8.0-226	SQA122-CT	172.16.121.40	ESX Server		No
□	172.16.122.28	172.16.122.28	CDS139-C1	3 more	172.16.122.28	ESX Server		No
□	172.16.122.29	172.16.122.29	CDS139-C1	3 more	172.16.122.29	ESX Server		No
□	172.16.122.30	172.16.122.30	CDS139-C1		172.16.122.30	ESX Server		No

1 - 25 of 394 hosts

1 of 16 pages

Deleting a Host in the Domain Manager

2 About the VDP Connector

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

This section includes:

What Does the Connector Do?

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

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

The Connector and the Network Environment

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

Network Traffic

Traffic between the InfoSphere VDP Appliances and the connector on your hosts is encrypted and communicated via SSL. The VDP Connector uses port 5106 by default for bidirectional communication from the InfoSphere VDP 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 IBM InfoSphere Support for assistance. For much more on network best practices, including iSCSI and Fibre Channel configuration, see ***Network Administrator's Guide to IBM InfoSphere VDP***.

Antivirus Software

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

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

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

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

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

For detailed instructions on how use VDP scripting, see:

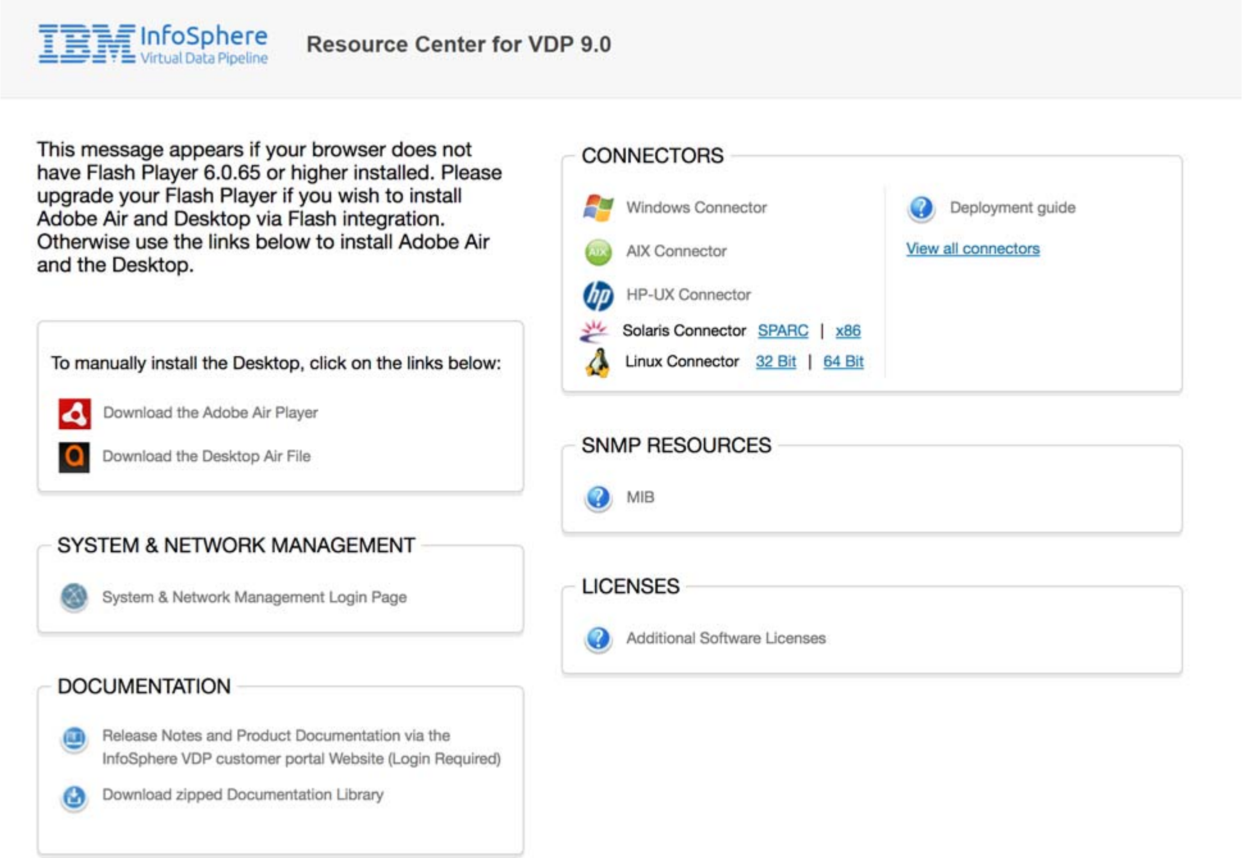
- Chapter 6, APPID Pre- and Post-Scripts for Scheduled Data Protection Jobs
- Chapter 7, Super Scripts for Workflows and On-Demand Data Access Jobs

Obtaining the Right VDP Connector for Your Host

The InfoSphere VDP 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 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.



IBM InfoSphere Virtual Data Pipeline

Resource Center for VDP 9.0

This message appears if your browser does not have Flash Player 6.0.65 or higher installed. Please upgrade your Flash Player if you wish to install Adobe Air and Desktop via Flash integration. Otherwise use the links below to install Adobe Air and the Desktop.

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

Download the Adobe Air Player

Download the Desktop Air File

SYSTEM & NETWORK MANAGEMENT

System & Network Management Login Page

DOCUMENTATION

Release Notes and Product Documentation via the InfoSphere VDP customer portal Website (Login Required)

Download zipped Documentation Library

CONNECTORS

Windows Connector

AIX Connector

HP-UX Connector

Solaris Connector SPARC | x86

Linux Connector 32 Bit | 64 Bit

Deployment guide

View all connectors

SNMP RESOURCES

MIB

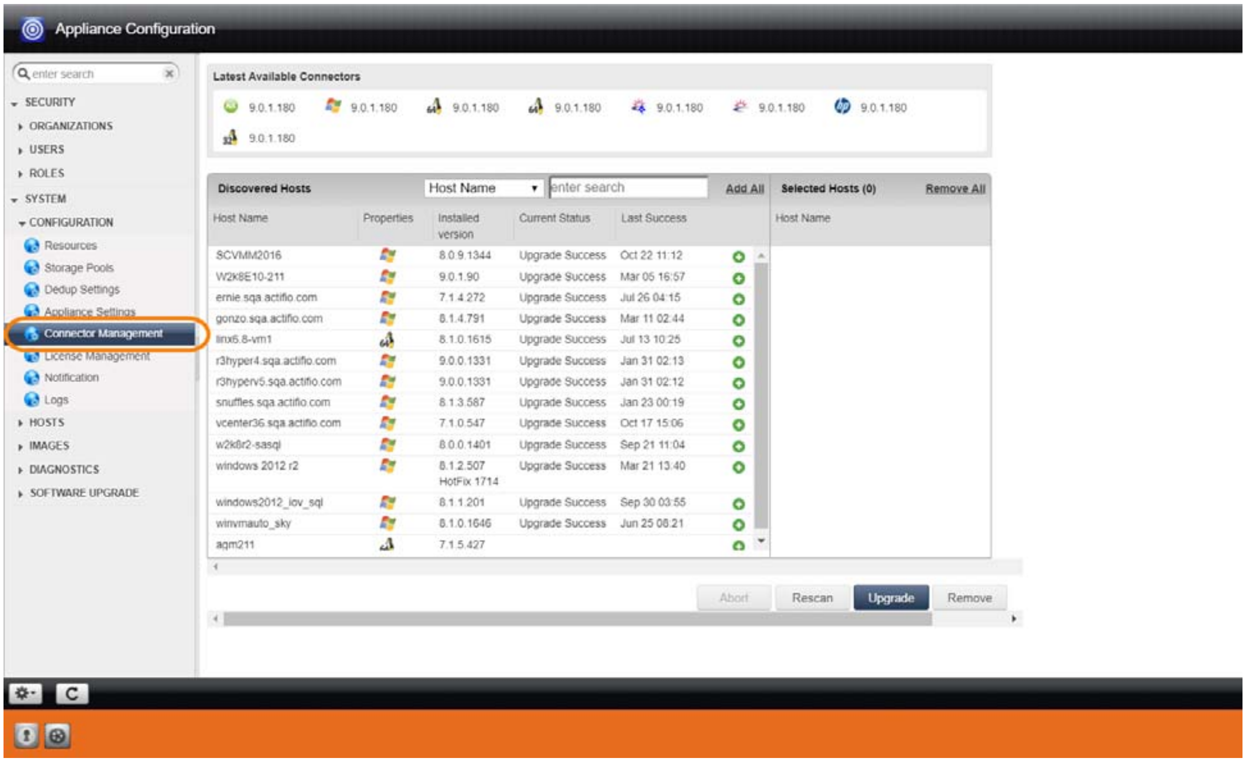
LICENSES

Additional Software Licenses

All of the VDP Connectors are Available from the Resource Center

Maintaining Connectors on Hosts

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



Host Name	Properties	Installed version	Current Status	Last Success
SCVMM2016		8.0.9.1344	Upgrade Success	Oct 22 11:12
W2K8E10-211		9.0.1.90	Upgrade Success	Mar 05 16:57
ernie.sqa.actifio.com		7.1.4.272	Upgrade Success	Jul 26 04:15
gonzo.sqa.actifio.com		8.1.4.791	Upgrade Success	Mar 11 02:44
linx6.8-vm1		8.1.0.1615	Upgrade Success	Jul 13 10:25
r3hyper4.sqa.actifio.com		9.0.0.1331	Upgrade Success	Jan 31 02:13
r3hyperv5.sqa.actifio.com		9.0.0.1331	Upgrade Success	Jan 31 02:12
snuffles.sqa.actifio.com		8.1.3.587	Upgrade Success	Jan 23 00:19
vcenter36.sqa.actifio.com		7.1.0.547	Upgrade Success	Oct 17 15:06
w2k8r2-sasql		8.0.0.1401	Upgrade Success	Sep 21 11:04
windows 2012 r2		8.1.2.507 HotFix 1714	Upgrade Success	Mar 21 13:40
windows2012_iov_sql		8.1.1.201	Upgrade Success	Sep 30 03:55
winvmauto_sky		8.1.0.1646	Upgrade Success	Jun 25 08:21
aqm211		7.1.5.427		

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:

Location of UDSAgent.log on Windows Server Hosts

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

Location of Scripts on Windows Hosts

You can create scripts to perform pre- and post- actions on applications on your Windows hosts. Create a new folder in which to store all scripts: C:\Program Files\Actifio\scripts. For detailed instructions on how use VDP scripting, see Chapter 6, APPID Pre- and Post-Scripts for Scheduled Data Protection Jobs and Chapter 7, Super Scripts for Workflows and On-Demand Data Access Jobs.

Note: *The VDP 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 VDP Connector.*

Installing the VDP Connector on Microsoft Windows Hosts

The VDP Connector for Microsoft Windows runs as a Windows service under the Local System account. The VDP 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 VDP Connector on each host.

The VDP 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 VDP Connector only needs to be installed into a VM (VMware, Hyper-V VM, or Hyper-V VM stored on CSV disks) if you want to protect individual applications inside the VM instead of simply protecting the entire VM.

VDP Change Tracking Driver Options for Windows Physical Hosts

When installing the Windows VDP Connector you have the option of installing the VDP Change Tracking Driver. If you intend to protect file systems and applications (SQL Server, Exchange, Sharepoint), install the VDP 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 VDP Connector on a Windows Host

To install the VDP Connector on a Windows host:

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

Installing the VDP 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 VDP Connector on a Windows Host

To restart the VDP Connector on a Windows host:

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

Uninstalling the VDP Connector from a Windows Host

To uninstall the VDP 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 VDP Connector on a Windows Host

Use the Connector Management tool in the VDP Desktop to auto upgrade the VDP Connector on your hosts when new versions are available. Refer to Maintaining Connectors on Hosts on page 8.

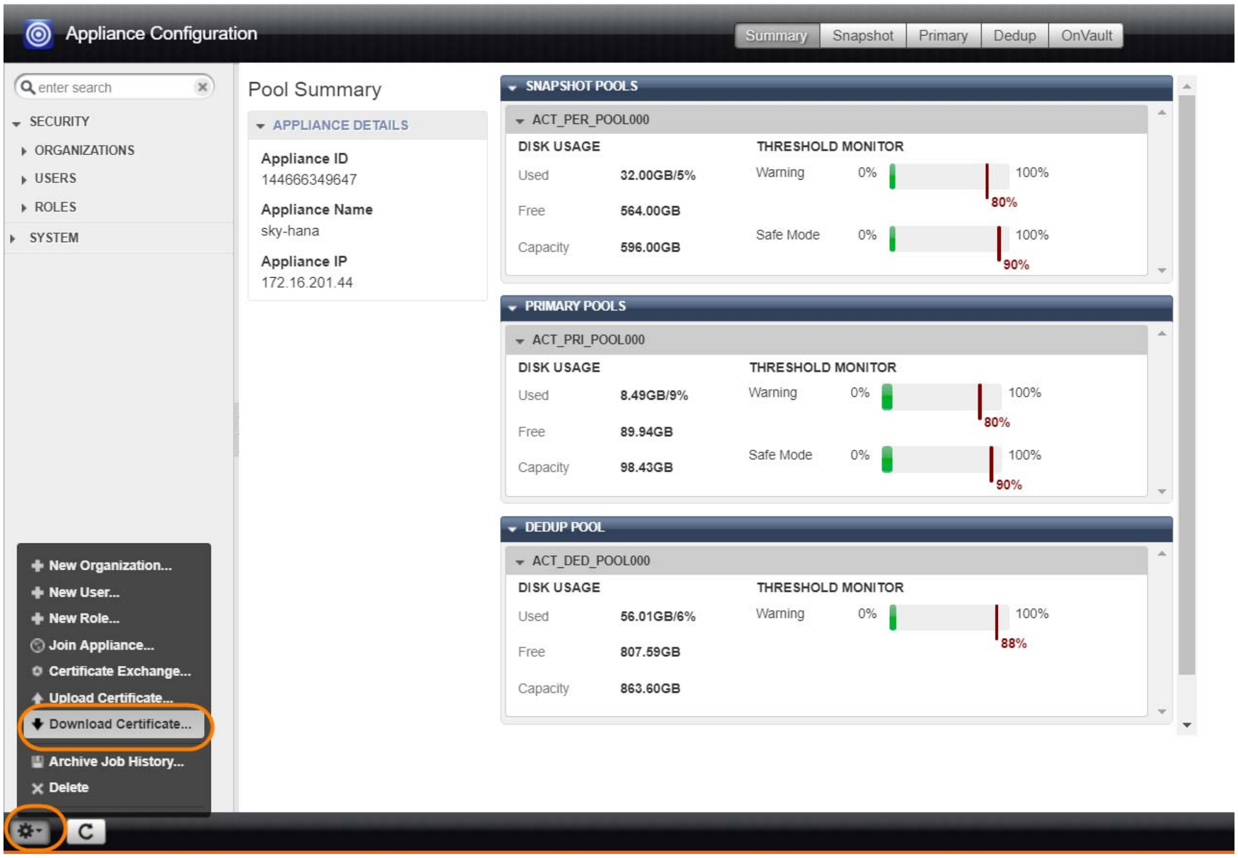
Restricting Windows Connector Communication to Specific Appliances

If you have multiple InfoSphere VDP 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 VDP 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 IVGM to the Domain Manager, Appliance page.
2. Select the appliance and right click it. Select **Configure Appliance**.
3. The Appliance Configuration window opens. Click the gear icon in the lower left corner, then select **Download Certificate**.



Pool Summary

APPLIANCE DETAILS

Appliance ID
144666349647

Appliance Name
sky-hana

Appliance IP
172.16.201.44

SNAPSHOT POOLS

ACT_PER_POOL000

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

PRIMARY POOLS

ACT_PRI_POOL000

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

DEDUP POOL

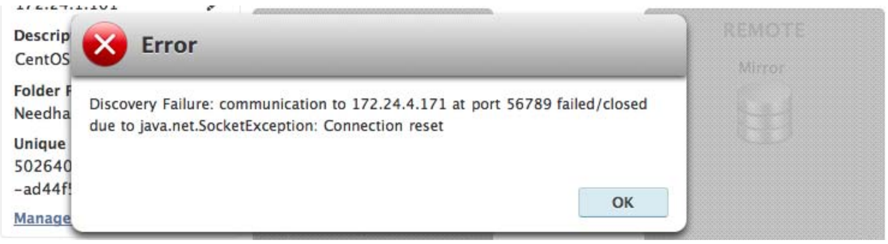
ACT_DED_POOL000

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

Downloading an Appliance Certificate

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

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



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

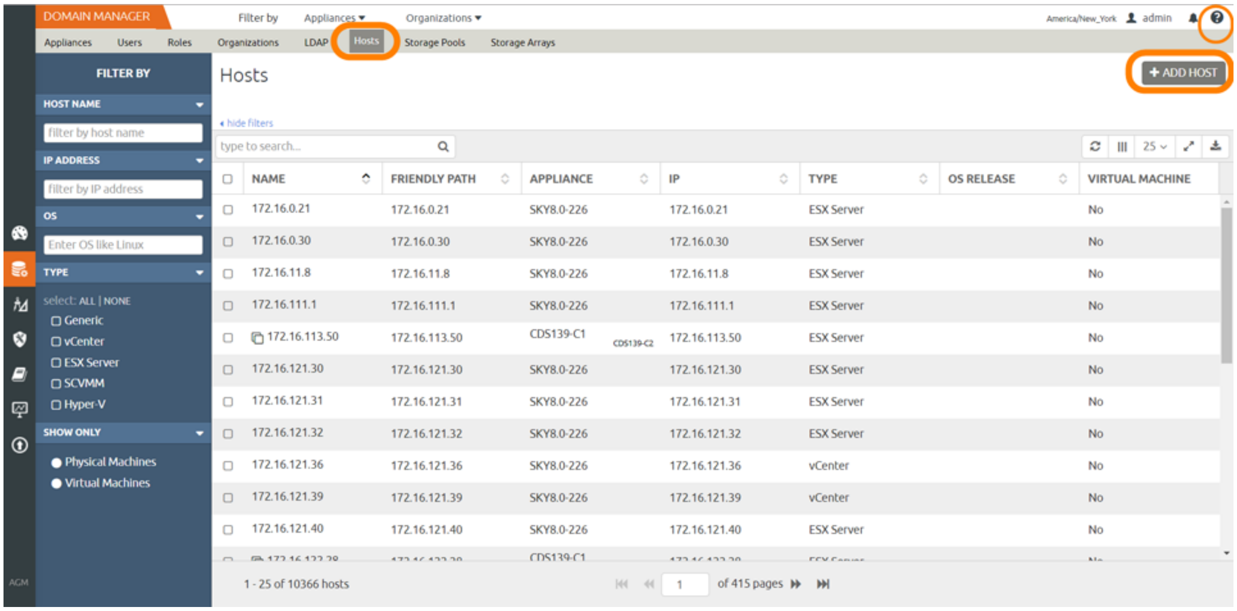
To Unrestrict a Restricted Windows Connector

1. Delete the certificate file from the host at `C:\Program Files\Actifio\certs\trusted\AuthorizedAppliance.crt`
2. Stop and start the connector (UDSAgent) using `services.msc`.
3. Repeat the test in Restricting Windows Connector Communication to Specific Appliances on page 11.

Adding a Windows Server Host to the InfoSphere VDP Appliance from IVGM

To add a new Windows host from IVGM:

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

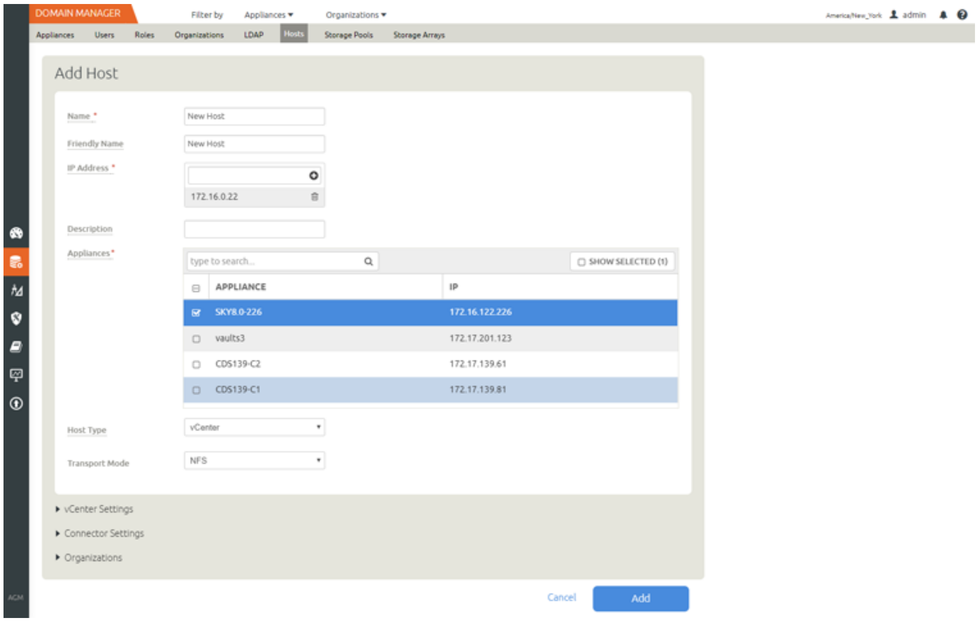


□	NAME	FRIENDLY PATH	APPLIANCE	IP	TYPE	OS RELEASE	VIRTUAL MACHINE
□	172.16.0.21	172.16.0.21	SKY8.0-226	172.16.0.21	ESX Server		No
□	172.16.0.30	172.16.0.30	SKY8.0-226	172.16.0.30	ESX Server		No
□	172.16.11.8	172.16.11.8	SKY8.0-226	172.16.11.8	ESX Server		No
□	172.16.111.1	172.16.111.1	SKY8.0-226	172.16.111.1	ESX Server		No
□	172.16.113.50	172.16.113.50	CDS139-C1 CDS139-C2	172.16.113.50	ESX Server		No
□	172.16.121.30	172.16.121.30	SKY8.0-226	172.16.121.30	ESX Server		No
□	172.16.121.31	172.16.121.31	SKY8.0-226	172.16.121.31	ESX Server		No
□	172.16.121.32	172.16.121.32	SKY8.0-226	172.16.121.32	ESX Server		No
□	172.16.121.36	172.16.121.36	SKY8.0-226	172.16.121.36	vCenter		No
□	172.16.121.39	172.16.121.39	SKY8.0-226	172.16.121.39	vCenter		No
□	172.16.121.40	172.16.121.40	SKY8.0-226	172.16.121.40	ESX Server		No

1 - 25 of 10366 hosts   1 of 415 pages

Adding a New Windows Host in IVGM

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 ('_').



Add Host

Name *	New Host
Friendly Name	New Host
IP Address *	172.16.0.22
Description	
Appliances*	

⊟	APPLIANCE	IP
☑	SKY8.0-226	172.16.122.226
□	vaults3	172.17.201.123
□	CDS139-C2	172.17.139.61
□	CDS139-C1	172.17.139.81

Host Type	vCenter
Transport Mode	NFS

Adding a Host Details in IVGM

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 InfoSphere VDP Appliance that will manage the host's data.
7. In Host Type, the type you pick depends on what you're using the Windows host for. These are detailed in Host Types and Connector Settings Overrides on page 14.
8. If you select vCenter or ESX Server, then you must also select the data transport mode, NFS or SAN. NFS is the default setting.
9. If you select vCenter or ESX Server, then you will also see a new section appear for vCenter Settings or ESX Settings. This is where you enter and test the port, username, and password to connect to the host.
10. Whatever type you select, enter **Connector Settings**. Enter **5106** in port unless you have changed from the default setting. Then enter a username and password for the Connector to use.
11. In **Organizations**, select one or more organizations for the host to be a member of. Organizations are explained in the IVGM Online Help.

Host Types and Connector Settings Overrides

To Protect	Select Host Type	Connection Type
CIFS file systems, SQL Server, SharePoint, Exchange	Generic	The default connector port for Generic hosts, SCVMM and Hyper-V VMs is 5106. If you use a different port, then enter it here. If the Connector username and password have changed, then change them here. If you do not need to override the default settings, then enter nothing here.
Hyper-V managed by Microsoft SCVMM	SCVMM	
Standalone Hyper-V on Windows server	Hyper-V Server	
vCenter with ESXi VMs	vCenter	A vCenter can have both vCenter Settings and Connector Settings, because a vCenter might also have the VDP Connector installed on it. The default vCenter management port is 443. If you use a different port, then enter it here. If the vCenter username and password have changed, then change them here. If you do not need to override the default settings, then enter nothing here.
ESXi standalone	ESX Server	The default ESX Server management port is 902. If you use a different port, then enter it here. If the ESX server username and password have changed, then change them here. If you do not need to override the default settings, then enter nothing here.

Notes on Discovering Specific Microsoft Application Types

The following information will be of use when discovering applications:

Discovering SQL Databases

- InfoSphere VDP 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.
- InfoSphere VDP 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 VDP Connector. If you have a multi-tier deployment, discover and protect content databases separately.
- For the discovery to work correctly, SharePoint VSS writer must be installed and running on the host.

Discovering Exchange Mailbox Databases

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

Discovering Mapped File Systems

Before you begin:

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

When complete, ensure that the application has been added as a host in the VDP 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 InfoSphere VDP Appliance can impersonate that user.*

4 Adding a Hyper-V Host

This chapter includes:

Location of UDSAgent.log on Hyper-V Hosts

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

Location of Scripts on Hyper-V Hosts

You can create scripts to perform pre- and post- actions on applications on the host. Create a folder at C:\Program Files\Actifio\scripts and store scripts there. Details on VDP scripting are in Chapter 6, APPID Pre- and Post-Scripts for Scheduled Data Protection Jobs and Chapter 7, Super Scripts for Workflows and On-Demand Data Access Jobs.

Installing the VDP Connector on Hyper-V Hosts

On Hyper-V systems the VDP 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 InfoSphere VDP Appliance.

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

Installing the VDP Connector on a Hyper-V Host

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

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

Restarting the VDP Connector on a Hyper-V Host

To restart the VDP Connector on a Windows host:

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

Upgrading the VDP Connector on a Hyper-V Host

Use the Connector Management tool in IVGM or in the VDP Desktop Domain Manager service to upgrade the VDP Connector on your hosts when new versions are available. Refer to Maintaining Connectors on Hosts on page 8.

Uninstalling the VDP Connector from a Windows Host

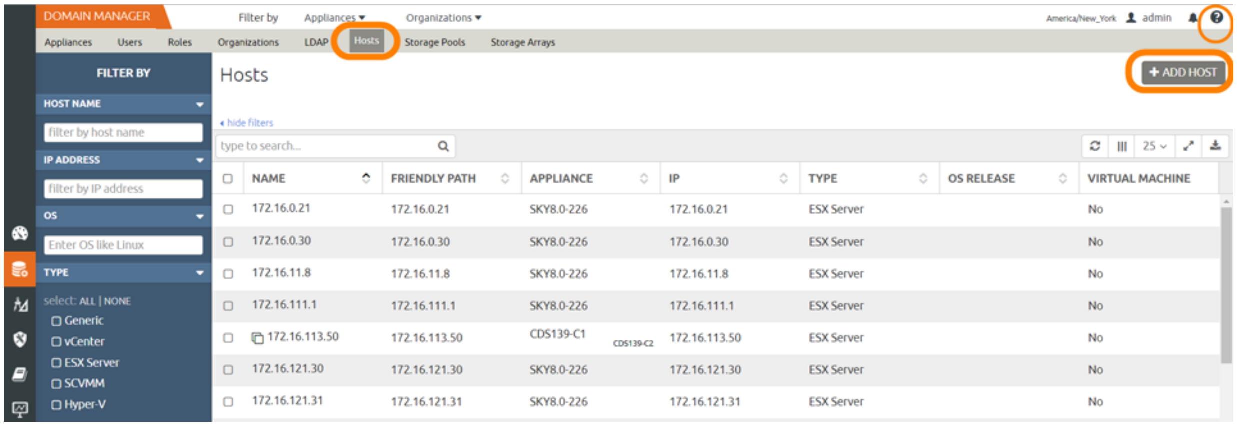
To uninstall the VDP Connector from a Windows host:

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

Adding a Hyper-V Host to the InfoSphere VDP Appliance from IVGM

To add a new Hyper-V host from IVGM:

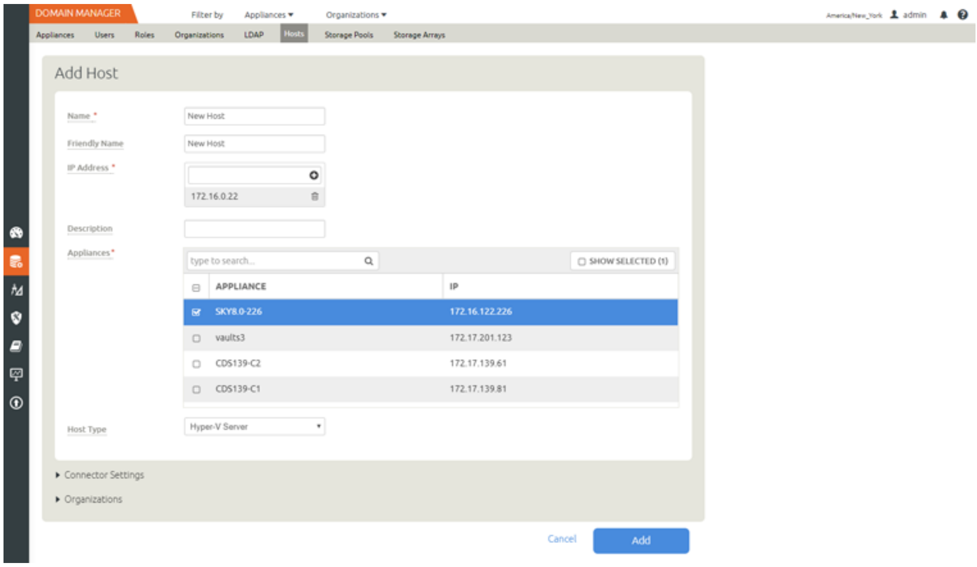
1. Open the IVGM to the **Domain Manager**.
2. From the Hosts tab, select **+ Add Host**.



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

Adding a New Hyper-V Host in IVGM

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 ('_').



Name *	New Host
Friendly Name	New Host
IP Address *	172.16.0.22
Description	
Host Type	Hyper-V Server

Appliances *

	APPLIANCE	IP
☑	SKY8.0-226	172.16.122.226
□	vaults3	172.17.201.123
□	CDS139-C2	172.17.139.61
□	CDS139-C1	172.17.139.81

Adding Host Details in IVGM

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 InfoSphere VDP Appliance that will manage the host’s data.
7. In Host Type, select **Hyper-V Server** or **SCVMM**.
8. Enter **Connector Settings**. Enter **5106** in port unless you have changed from the default setting. Then enter a username and password for the Connector to use.
9. In **Organizations**, select one or more organizations for the host to be a member of. Organizations are explained in the IVGM Online Help.

5 Adding a Linux Host

This chapter includes:

Location of UDSAgent.log on Linux Hosts

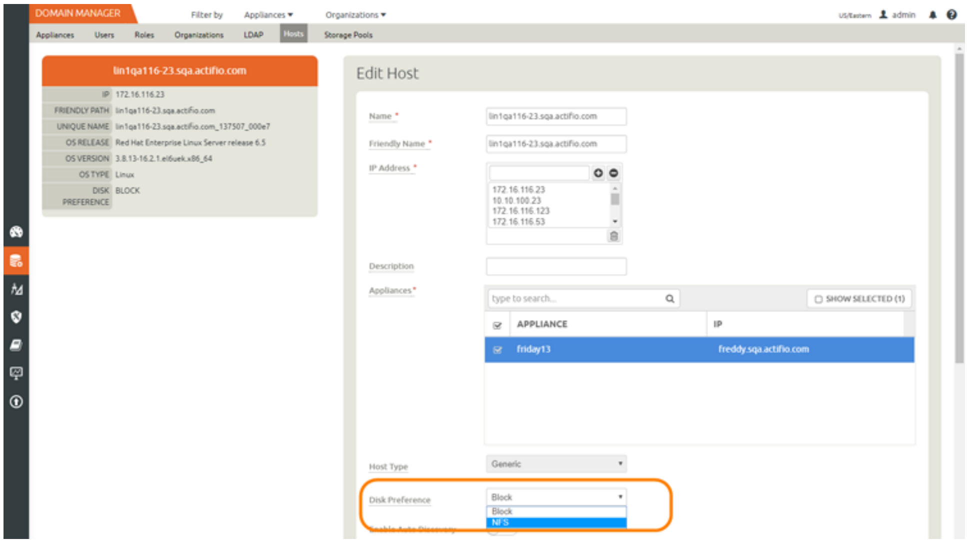
On a Linux host, logs are stored in /var/act/log.

Location of Scripts on Linux Hosts

You can create scripts to perform pre- and post- actions on applications on the Linux host. To use scripts, create a folder called /act/scripts and store all scripts there. For detailed instructions on how use VDP scripting, see Chapter 6, APPID Pre- and Post-Scripts for Scheduled Data Protection Jobs and Chapter 7, Super Scripts for Workflows and On-Demand Data Access Jobs.

Using NFS protocol for Linux hosts in the IVGM

To use NFS protocol for Linux physical hosts, use the IVGM 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 VDP Connector will consume this share. When mounting an image captured this way, the mount screens will automatically show you the option to mount them as an NFS share.



lin1qa116-23.sqa.actifio.com

IP	172.16.116.23
FRIENDLY PATH	lin1qa116-23.sqa.actifio.com
UNIQUE NAME	lin1qa116-23.sqa.actifio.com_137507_000e7
OS RELEASE	Red Hat Enterprise Linux Server release 6.5
OS VERSION	3.8.13-16.2.1.el6uek.x86_64
OS TYPE	Linux
DISK PREFERENCE	BLOCK

Edit Host

Name * lin1qa116-23.sqa.actifio.com

Friendly Name * lin1qa116-23.sqa.actifio.com

IP Address *
172.16.116.23
10.10.100.23
172.16.116.123
172.16.116.53

Description

Appliances* type to search... □ SHOW SELECTED (1)

☑	APPLIANCE	IP
☑	friday13	freddy.sqa.actifio.com

Host Type Generic ▾

Disk Preference Block ▾
Block
NFS

Enable Auto Discovery

Setting Disk Preference to NFS

Installing the VDP Connector on a Linux Host

The VDP Connector for Linux runs as a daemon process under the username **root**. It listens on a TCP port 5106 for communication from the InfoSphere VDP Appliance. The VDP 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 VDP Connector. The installer creates `Init` RC scripts to start and stop the VDP Connector that runs as a daemon. After the installation completes, use the RC script to start the VDP Connector for the first time.

To install the VDP Connector on a Linux host:

1. Log on to the host as root.
2. Open a browser to `https://<InfoSphere VDP Appliance IP>` to access the Resource Center.
3. Click the **Linux Connector** icon to download the VDP 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 VDP 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 VDP Connector is always installed at `'/opt/act'`.
7. Verify that the VDP 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 VDP Connector on a Linux Host

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

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

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

Manually Uninstalling the VDP Connector from a Linux Host

To uninstall the VDP Connector from a Linux host:

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

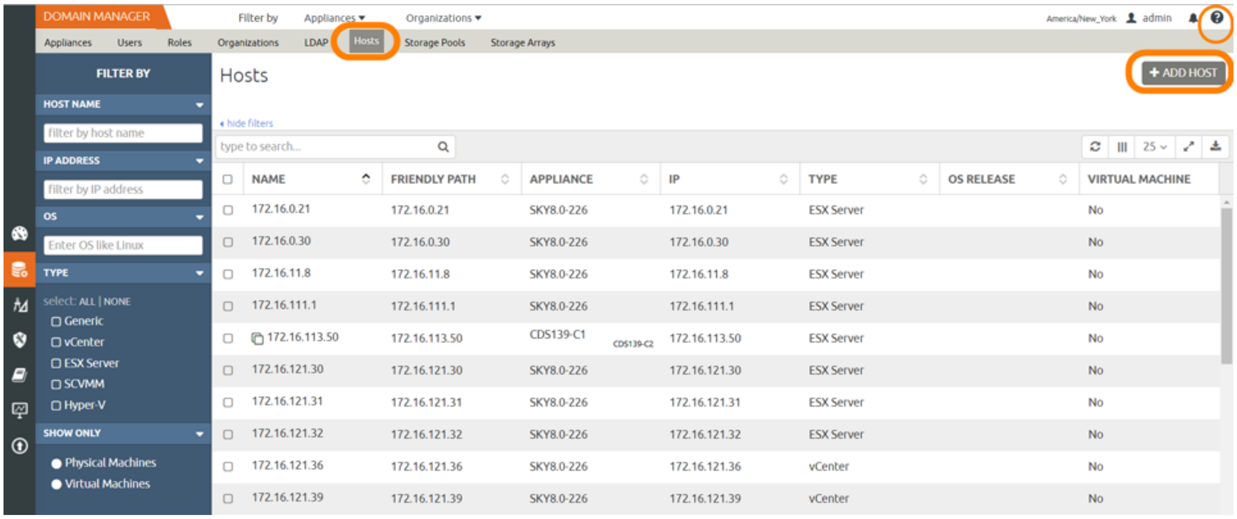
   ```
   [oracle@vq-oracle ~]$ rpm -qa udsagent
   ```

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

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

Adding a Linux Host to the InfoSphere VDP Appliance from IVGM

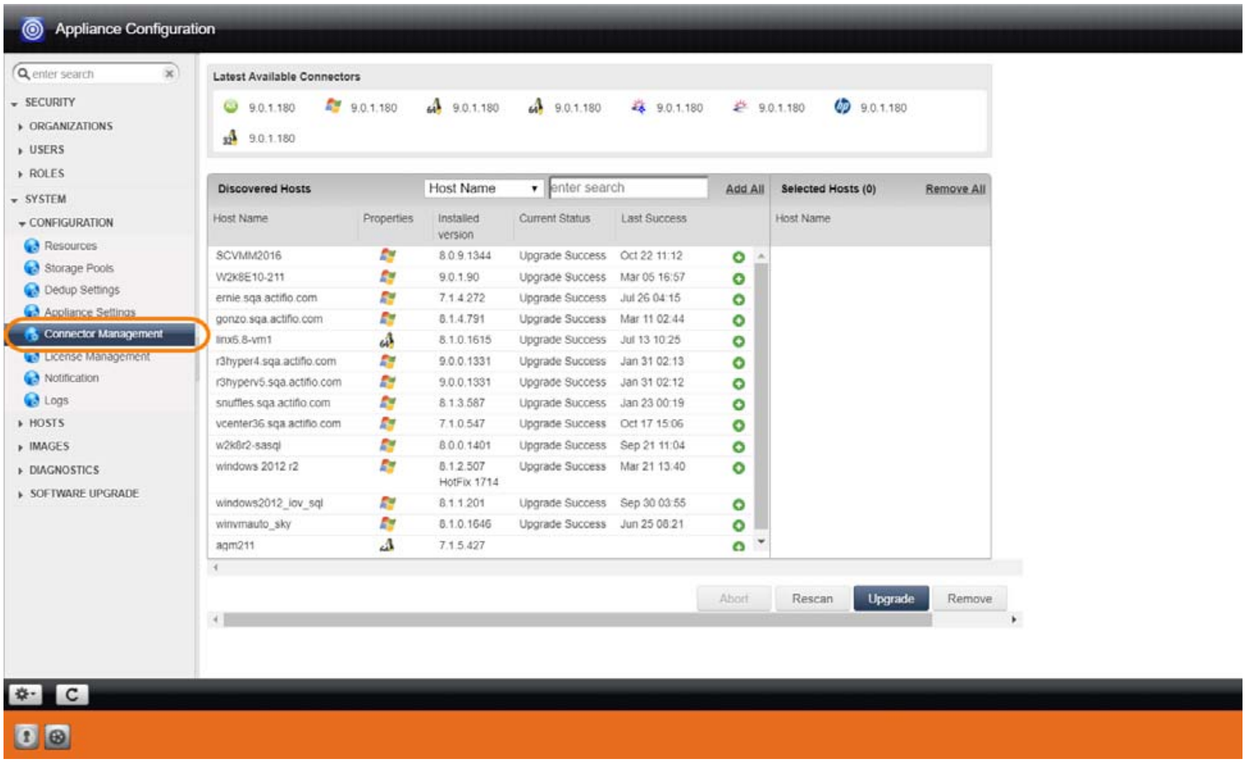
To add a new Linux host from IVGM, open IVGM to the **Domain Manager** and from the Hosts tab, select **+ Add Host**. Refer to the IVGM online help for details.



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

Upgrading or Uninstalling the VDP Connector on a Linux Host

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



Host Name	Properties	Installed version	Current Status	Last Success
SCVMM2016		8.0.9.1344	Upgrade Success	Oct 22 11:12
W2K8E10-211		9.0.1.90	Upgrade Success	Mar 05 16:57
ernie.sqa.actifio.com		7.1.4.272	Upgrade Success	Jul 26 04:15
gonzo.sqa.actifio.com		8.1.4.791	Upgrade Success	Mar 11 02:44
linx6.8-vm1		8.1.0.1615	Upgrade Success	Jul 13 10:25
r3hyper4.sqa.actifio.com		9.0.0.1331	Upgrade Success	Jan 31 02:13
r3hyperv5.sqa.actifio.com		9.0.0.1331	Upgrade Success	Jan 31 02:12
snuffles.sqa.actifio.com		8.1.3.587	Upgrade Success	Jan 23 00:19
vcenter36.sqa.actifio.com		7.1.0.547	Upgrade Success	Oct 17 15:06
w2k8r2-sasql		8.0.0.1401	Upgrade Success	Sep 21 11:04
windows 2012 r2		8.1.2.507 HotFix 1714	Upgrade Success	Mar 21 13:40
windows2012_iov_sql		8.1.1.201	Upgrade Success	Sep 30 03:55
winvmauto_sky		8.1.0.1646	Upgrade Success	Jun 25 08:21
aqm211		7.1.5.427		

Connector Management

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

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

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

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

Setting	Description	Default Timeout	Range
`Init`	The init script is invoked with an **`init`** parameter when the backup is about to start.	120 seconds	N/A
`Freeze`	The freeze script is invoked with a **`freeze`** parameter when the backup operation is just about to freeze the application.	60 seconds	1 - 120 seconds
`Unfreeze`	The thaw script is invoked with a **`thaw`** parameter when the backup operation is just finished unreeling the application.	60 seconds	1 - 120 seconds
`Finish`	The fini script is invoked with a **`fini`** parameter when the backup operation is about to complete. This phase is applicable only for the VDP Connector.	60 seconds	1 - 86400 seconds
`Abort`	The abort script is invoked with an `abort` parameter if the backup is aborted for any reason.	N/A	N/A

Troubleshooting APPID Scripts

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

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

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

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

Sample APPID Script for Windows

```
@echo oFF

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

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

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

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

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

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

:end
echo Done processing commands
```

Sample APPID Script for Linux

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

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

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

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

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

7 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 VDP Connector is installed. Individual script names and arguments for each phase can be specified separately. The scripting engine uses environment variables to provide job information to the scripts.

The VDP host-side super scripts are invoked for on-demand jobs that are triggered by the CLI with the **-scripts** argument. Supported CLI jobs are listed in the CLI Commands Supported in Super Scripts on page 30.

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

This chapter contains the following topics:

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 InfoSphere VDP 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 30 for CLI usage examples.

Super Script Environment Variables

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

For example:

Current phase (PHASE) is exported as ACT_PHASE

Current VDP job name (JOBNAME) is exported as ACT_JOBNAME

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

- ACT_APPID: The database ID of the application (e.g. 4186)
- ACT_APPNAME: Name of the application (e.g. My-DB)
- ACT_HOSTNAME: The name of the host which is the target of this job (e.g. Jupiter)
- ACT_JOBNAME: The name of the job (e.g. Job_0123456)
- ACT_JOBTYPE: a text version of the job class (e.g. mount
- ACT_LOGSMART_TYPE: db is the only valid value. This must be present for database logs to be captured.
- ACT_MULTI_END: After mount, if True, recover database into open state (default). If False, the database is left in the mounted (Oracle) or restoring (SQL Server) state.
- ACT_MULTI_OPNAME: the name of the operation currently running for a job that consists of multiple operations. Reprovision and Restore jobs involve an unmount operation followed by a mount operation. Operations include:
  - MOUNT
  - UNMOUNT
  - REFRESH
  - RESTORE
  - REPROVISION
  - SCRUB-MOUNT
  - SCRUB-UNMOUNT
  - MIGRATE
  - CLONE
- ACT_OPTIONS: Policy options that apply to this job
- ACT_PHASE: A text string that describes the job phase (e.g. init)
- ACT_POLICY: Name of the policy related to this job (e.g. Daily4Hr)
- ACT_PROFILE: The name of the profile (e.g. Standard)
- ACT_SCRIPT_TMOUT: Superscripting timeout. If response is not received within timeout value (default 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=<scrip
tname>:phase={INIT|PRE|POST|FINAL}...]
```

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

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

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

```
udstask backup -app $MYAPP -policy $MYPOLICY \

-script “name=MYSCRIPT.sh:phase=PRE:timeout=60:args=ARG1,ARG2”
```

Sample Super Scripts

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

Sample Super Script for Windows

At: `\<InstallDir>\scripts`

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

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

Sample Super Script for Linux and other Unix Platforms

For Linux: /act/scripts

Example: /act/scripts/wrapper_script.sh

```
    #!/bin/bash

    LOG_FILE="/tmp/act_script.log"

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

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