Technical white paper

HP CloudSystem Enterprise

HP Cloud Service Automation Design for Microsoft Windows VM with HP Data Protector

Table of contents

Executive summary

HP CloudSystem Enterprise provides automation to rapidly deliver compute resources to cloud consumers. The ability to provide data protection through backup services is critical to the success of these compute resources. This document describes how to configure an HP Cloud Service Automation Service Design leveraging HP Operations Orchestration, Server Automation, and VMware vSphere to deploy an HP Data Protector 8 client and dynamically create a Data Protector backup specification for a Microsoft® Windows® Server 2008 virtual machine. This allows organizations to offer a backup service to cloud consumers and incorporate those backup services into their cloud service offerings.

Target audience: The intended audience of this white paper is system integrators, installers, and administrators of HP CloudSystem Enterprise. The reader should be familiar with CloudSystem Enterprise and HP CloudSystem Matrix.
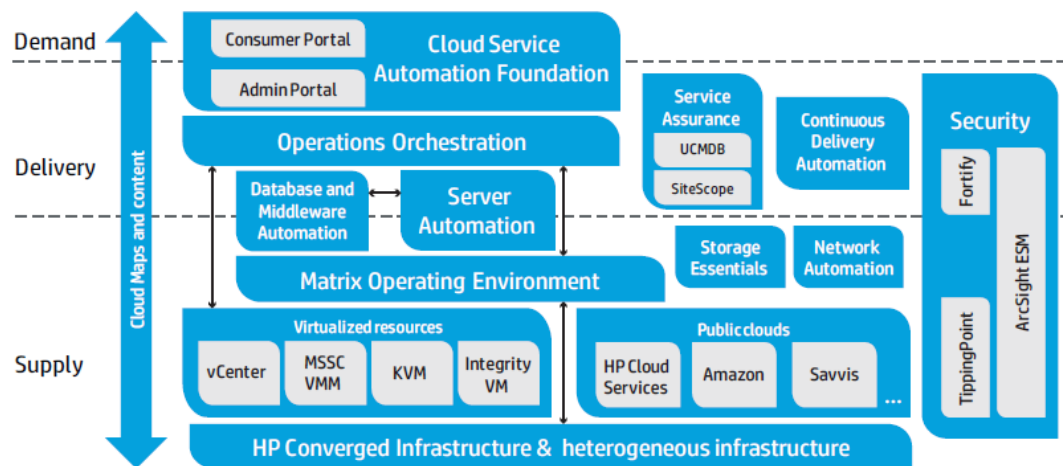
HP CloudSystem Enterprise overview

With HP CloudSystem Enterprise, an organization can deliver not only infrastructure as a service (IaaS), but also anything as a Service (XaaS) directly to line-of-business teams. That is, in addition to delivering virtual servers and storage as services, CloudSystem Enterprise can manage and provision enterprise-grade applications such as Microsoft Exchange Server, or even custom developed applications, such as cloud-based services. Figure 1 illustrates the HP CloudSystem Enterprise architecture. HP CloudSystem Enterprise extends the foundation of HP CloudSystem Matrix with the seamless integration of HP Cloud Service Automation (CSA). HP CloudSystem Enterprise manages the entire application-to-infrastructure lifecycle—from provisioning, to managing and monitoring, to releasing resources back to the cloud. The diagram shows how Cloud Service Automation, with its cloud management platform for brokering and managing enterprise grade application and infrastructure cloud services, and HP Matrix Operating Environment are engineered to work together, as well as with additional HP CloudSystem extensions and third-party assets.

HP CloudSystem Enterprise supply layer

Like the HP CloudSystem Matrix offering, the supply layer in HP CloudSystem Enterprise calls on the Matrix Operating Environment for service delivery of infrastructure elements such as compute, network, storage, and other resources, both physical and virtual. HP CloudSystem Enterprise can also leverage VMware vCenter for infrastructure services. Supported infrastructure includes HP BladeSystem servers, HP storage, and HP networking, as well as servers, storage, and networking from third parties.

Figure 1. CloudSystem Enterprise Functional Architecture

HP CloudSystem Enterprise demand and delivery: HP Cloud Service Automation

HP Cloud Service Automation software enables and manages the delivery of application services. It includes user interfaces that allow infrastructure design, specifying what assets will be available, and service design, in which a service designer can add to and manage service catalogs. Cloud Service Automation orchestrates the deployment of compute resources and complex multi-tier application architectures. It integrates and leverages the strengths of several mature HP management and automation products. And it adds workload management, service design, and a customer portal to create a comprehensive service automation solution. Cloud Service Automation (CSA) can leverage CloudSystem Matrix infrastructure services, and adds applications to the supply layer. It also expands the system's infrastructure capabilities: for example, with CSA, HP CloudSystem Enterprise can support multiple hypervisors—such as those from VMware, Microsoft,

Kernel Virtual Machine (KVM), and Xen—within the supply layer. Cloud Service Automation also provides portal services for the demand layer, where consumers or business users can request services. The software delivers IaaS and platform as a service (PaaS) in a heterogeneous environment, as well as virtual desktop infrastructure (VDI or "Desktop as a Service") and XaaS. Cloud Service Automation manages the entire cloud service lifecycle, including provisioning the infrastructure, whether by extension to one—or several—Matrix Operating Environment resource pools, or from non-Matrix infrastructure pools. It also handles provisioning, patching, and ensuring compliance of business and custom applications; managing and monitoring the cloud; and releasing resources back to the cloud. Extensions allow adding further service assurance, enhanced security, storage management, and network management.

HP CloudSystem Enterprise users can:

- Broker and manage on-demand application and infrastructure services
- Enforce compliance
- Meet service-level agreements (SLAs) with performance and availability management
- Secure data with multi-tenancy and role-based access
- Deliver comprehensive, unified service lifecycle management

HP CloudSystem Enterprise components

Besides Cloud Service Automation, components of CloudSystem Enterprise that enable its capabilities include:

HP Operations Orchestration (OO)
OO coordinates communication between integrated products and managed devices.

HP Server Automation (SA)
SA deploys operating systems and policies to managed devices. It provides lifecycle server management and automated application deployment, and automates tasks such as provisioning, patching, configuration management, and compliance management.

HP Database and Middleware Automation (DMA)
DMA provides a content library for database and middleware management. It provisions application architectures onto existing infrastructure, and can also manage those applications, providing pre-packaged workflows for application patching, compliance, and code release. DMA eliminates the need for manual customization.

HP SiteScope
SiteScope provides agentless monitoring of infrastructure platforms and the key performance indicators (KPIs) of applications. KPIs include CPU, disk, memory usage, etc.

HP Universal Configuration Management Database (UCMDB)
UCMDB maintains accurate, up-to-date information regarding the relationships between infrastructure, applications, and cloud services.

HP Matrix Operating Environment
Matrix Operating Environment supplies infrastructure services. Cloud Service Automation is thoroughly integrated with the infrastructure services created by the Matrix Operating Environment and through this layer can burst to public cloud services.

HP Data Protector 8 overview

HP Data Protector is a backup solution that provides reliable data protection and high accessibility for your fast growing business data. Data Protector offers comprehensive backup and restore functionality specifically tailored for enterprise-wide and distributed environments. The following is a list of major Data Protector features:

- Scalable and highly flexible architecture
- Easy central administration
- High-performance backup
- Data security
- Supporting mixed environments
- Easy installation for mixed environments
- High-availability support

- Backup object operations
- Easy restore
- Automated or unattended operation
- Monitoring, reporting, and notifications
- Integration with online applications
- Integration with other products

Background assumptions

This reference implementation requires that the HP CloudSystem Enterprise environment is already installed, configured, and functioning correctly. Each component must be verified to work individually, and as a complete HP CloudSystem Enterprise environment. The major components include the following:

- HP CloudSystem
- HP Cloud Service Automation (CSA)
- HP Matrix Operating Environment (Matrix OE)
- HP Operations Orchestration (OO)
- HP Data Protector 8 Cell Manager and Installation Server

Pointers to the documentation for installing, configuring, and verifying these components and their interoperability may be found in the For more information section.

Overview

This document describes how to add the HP Data Protector client to a deployed VMware virtual machine running Windows Server 2008 and create the associated backup specification using Cloud Service Automation with VMware vSphere. The service design will perform the following operations:

- Deploy a VMware virtual machine running Windows Server 2008 using a CSA Service Design.
- Add an option to the Service Design that allows the Cloud Consumer to add a backup client to the virtual machine and register the virtual machine with the Data Protector Cell Manager.
- Create the associated Data Protector backup specification on the Data Protector Cell Manager.

HP Cloud Service Automation and VMware vSphere

Deployment of a Windows Server 2008 (Windows 2008) virtual machine service using VMware vSphere as a compute provider in HP Cloud Service Automation is described in the steps below:

1. The User requests a service through the HP Cloud Service Automation Consumer Portal.
2. HP Cloud Service Automation uses an HP Operations Orchestration workflow to make a request to deploy a virtual machine template to VMware vCenter.
3. VMware vCenter deploys virtual machines from pre-created virtual machine templates.
4. The virtual machines are deployed on VMware vSphere.
5. The virtual machine subscription will have an option titled `Add the Data Protector Client.`

Figure 2. CSA Service Design sample deployment
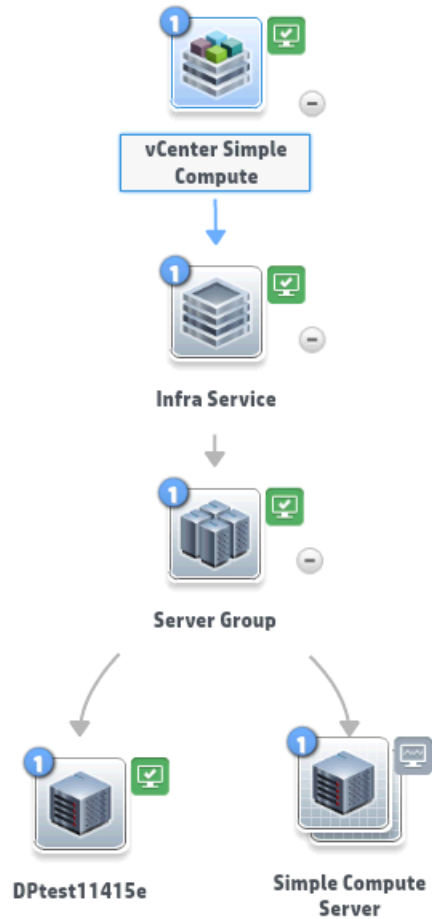
Configuration process steps

This reference implementation details the major steps required to install and configure the HP Data Protector Client for Windows Service. They include the following:

1. Retrieving and unpacking the scripts and content provided with this reference implementation.
2. Creating the base virtual machine image required for the Windows 2008 virtual machine deployment.
3. Configuring Data Protector Cell Manager.
4. Importing the Operations Orchestration Workflows.
5. Importing Service Designs and publishing Service Offerings in CSA.
6. Creating and using the application service.

After these steps are complete, the application will be available for business users to automatically deploy using the CSA Consumer portal.

A final step is also included that will decommission the service and return the resources to the HP CloudSystem Enterprise environment.

Storage and server requirements

The information below defines the requirements. If you plan to use a different operating system version for your virtual machine, refer to the Administrators Guide or Release Notes for the supported OS types and system configurations for the version of HP Data Protector Client you need to deploy.

Supported operating systems used in this design:

- Windows Server 2008 R2
- VM Windows Instances

    Memory: 512 MB (Minimum)

    Free Disk Space for Data Protector Client and Disk Agent: 180 MB

Configuring HP CloudSystem Enterprise

This reference implementation is supplied with a zip file (HP-Data-Protector-SD-v1.zip) that contains a Cloud Service Automation service design, Operations Orchestration workflows, and scripts required to complete the configuration. The zip file should be unpacked into a location that is accessible to the Cloud Service Automation server (CSA), Data Protector Cell Manager, and the Operations Orchestration server along with other servers in the CloudSystem Enterprise environment. The contents of the zip include the files listed in the following table.

Table 1. Downloaded zip file (HP-Data-Protector-SD-v1.zip) contents

Folder	File names	Description
HP Cloud Service Automation Service Design	SERVICE_DESIGN_VCENTER_COMPUTE_Data_Protector_3.20.zip	VMware and Data Protector Service Design archive
HP Data Protector Scripts	backup-policy.template, build-backup-policy.ps1	Data Protector PowerShell script and Data Protector Template
HP Operations Orchestration Workflows	vCenter_Data_Protector_3.20_Flows-ContentInstaller.jar	HP Operations Orchestration workflow

Note: The zip file can be found at http://h71028.www7.hp.com/enterprise/downloads/HP-Data-Protector-SD-v1.zip

Creating the virtual machine image required for HP Data Protector Client

The instructions below describe how to create the virtual machine image used for the Data Protector Client deployment. A virtual machine template will be used as a base image. The image can be created using the VMware vSphere client. The virtual machine image must include the Server Automation agent in order for the server to be managed by Server Automation.

1. Create a Windows 2008 R2 virtual machine, from the VMware vSphere client on your VMware vCenter host. Include the management network connected to your SA server.
2. After the Windows installation completes and the VM boots, obtain the IP address of your virtual machine.

Create Data Protector user account
1. Create a Data Protector user account DPUser and add this user to the local Administrators group. This user account will be specified in the Operations Orchestration System Variable "DPUser"
2. Turn off Windows User Account Control on the virtual machine.

Notes:

- The "DPUser" account must be defined as an operator in the Data Protector Cell Manager if this user is going to execute the backup operation.
- Ensure the "DPUser" account has permissions to access the OmniBack share on the Data Protector Installation server.

Copy the agent installation file
1. Log in to the HP Server Automation Java client as an administrative user.
2. You can download the Server Automation Java client from the Server Automation web client from `https://<SA Core IP address>`. The link to download the Java client is on the login page. Click **Download Hewlett-Packard Launcher** to install the application. The installer has an option to create a shortcut on your desktop. You don't need to log in to the web client.
3. Select **Devices** from the button on the bottom left.
4. Select **Servers** and then **Unmanaged Servers**.
5. In the **from** and **to** fields, enter the IP addresses of your virtual machines and click on the **Scan** button.

6. In the Manage Servers pop-up window, enter the **Username** and **Password** for your virtual machine. Under Actions, select **Verify prerequisites and copy agent installer to servers**. This will copy the agent to the c:\Windows folder on your virtual machine.

7. Login to each of your virtual machines and move the opsware-agent-*.exe file from c:\Windows to c:\tmp. Make a note of the exact filename of the opsware-agent executable file. It will be used in the next section.

Edit the Windows Registry

1. After copying the agent installation file to the `c:\tmp` folder on both of your virtual machines, complete the following steps on each virtual machine to enable automatic agent installation during server deployment.

2. From the Start menu, click on **Run** and type `regedit` to open the Windows Registry Editor.

3. Expand **HKEY_LOCAL_MACHINE → SOFTWARE → Microsoft → Windows → Current Version** and click on **RunOnce**.

4. Double click on **Default**. Enter the following string in the Value data field:

```
c:\tmp\opsware-agent-<enter exact file name>.exe --opsw_gw_addr <SA
ipaddr>:3001 --force_full_hw_reg --logfile c:\tmp\opsw.log
```

As an example, the registry entry may look like this:

```
c:\tmp\opsware-agent-45.0.31322.0-win32-6.1-X64.exe --opsw_gw_addr
10.116.83.23:3001 --force_full_hw_reg --logfile c:\tmp\opsw.log
```

5. Note that the options specified in the preceding step (4) for the opsware-agent installation, opsw_gw_addr, force_full_hw_reg and loglevel switches, are preceded by two dashes. Replace **<SA ipaddr>** with the address of your Server Automation server.

6. In addition to adding the Server Automation agent to the registry, the following two entries must be modified to allow sysprep to complete successfully:

   • Set **HKEY_LOCAL_MACHINE\SYSTEM\Setup\Status\SysprepStatus\GeneralizationState** to **7**

   • Set **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\SkipRearm** to **1**

7. Close the Windows Registry Editor.

8. Power off the virtual machine.

9. Convert the image to a VMware VM template. In the vSphere Client, right-click the VM and from the **Template** dropdown select **Convert to Template**.

Required software packages and files

There are no Server Automation based software packages required for the Data Protector client installation. The Windows virtual machine that will have the Data Protector client installed must have network access to the Data Protector Cell Manager and Data Protector Installation Server. In our example both the Data Protector Cell Manager and Installation Server are installed on the same host and identified by the Operations Orchestration System Properties variables DPCellManager and DPCellManagerIP.

Configure the Data Protector Cell Manager

This service design contains two files, a Windows PowerShell script and a Data Protector backup specification template file that must be copied to the Data Protector Cell Manager. The Operations Orchestration workflows require that these files be located in c:\dataprotector on the Data Protector Cell Manager.

1. On the Data Protector Cell Manager create a directory C:\dataprotector.

2. Copy backup-policy.template and build-backup-policy.ps1 to C:\dataprotector on the Data Protector Cell Manager.

3. Modify the build-backup-policy.ps1 to specify your backup device `'XXXDEVICE' = "<Backup Device Name>"`.

Notes:

• The backup device must reflect a backup device that is available to your Data Protector Cell Manager. The backup device used in this example is `'XXXDEVICE' = "DPStore_Writer0"`.

• To execute the PowerShell script on your Data Protector Cell Manager server the PowerShell Script Execution Policy must be set to RemoteSigned on the Data Protector Cell Manager.

Importing the Operations Orchestration workflows

Import the Operations Orchestration workflows into Operations Orchestration. Below is an overview of the steps required for importing the Operations Orchestration workflows and configuring the Operations Orchestration system variables.

1. Import the workflows.
2. Modify the DPAdmin System Account username and password in Operations Orchestration Studio.
3. Modify the DPUser System Account username and password in Operations Orchestration Studio.
4. Modify the DPCellManager and DPCellManagerIP system properties in Operations Orchestration Studio.
5. Run the Cloud Service Automation process definition tool.

Import the HP Operations Orchestration workflows

The Operations Orchestration workflow jar file is found in the HP Operations Orchestration Workflows folder where you downloaded HP-Data-Protector-SD-v1.zip. Create a temporary folder on your Operations Orchestration server and copy the vCenter_Data_Protector_3.20_Flows-ContentInstaller.jar file to your temporary folder on your Operations Orchestration server.

To import the workflows, complete the following steps:

1. Open a command line window on your Operations Orchestration server.
2. Change folders to the location where you copied the jar file.
3. Enter the following command:

```
java –Xmx1024m –jar vCenter_Data_Protector_3.20_Flows-ContentInstaller.jar -
centralUsername <admin user> -centralPassword <password>
```

4. Upon completion, the workflows are automatically imported into Operations Orchestration in the /Library/CSL/Contrib/CSA3.2/DataProtector directory.

Modify the DPAdmin Account in Operations Orchestration Studio

The Data Protector System Account, DPAdmin, is the Administrator account and password for your Data Protector Cell Manager or an account that has privileges to run a PowerShell command and create a Data Protector backup specification.

1. Open Operations Orchestration Studio on your Operations Orchestration server and login as the admin user.
2. Expand the Configuration folder and System Accounts folder.
3. Open the DPAdmin system account.
4. Click on ![lock icon] to check it out.
5. Enter the user name for the DPAdmin System Account in the User Name field.
6. Click on the **Assign Password** button.
7. Enter the DPAdmin user password and click on OK.
8. Click on ![unlock icon] to check in your changes and click on OK.

Note:

The DPAdmin account must have permission to create backup specifications and execute PowerShell scripts on the Data Protector Cell Manager.

Modify the DPUser Account in Operations Orchestration Studio

The Data Protector User Account, DPUser, is the user account created in the virtual machine template.

1. Open Operations Orchestration Studio on your Operations Orchestration server and login as the admin user.
2. Expand the Configuration folder and System Accounts folder.
3. Open the DPUser system account.
4. Click on ![lock icon] to check it out.
5. Enter the user name for the DPUser System Account in the User Name field.
6. Click on the **Assign Password** button.
7. Enter the DPUser user password and click on OK.
8. Click on ![unlock icon] to check in your changes and click on OK.

Create the DPCellManager and the DPCellManagerIP System Properties in Operations Orchestration Studio

The Data Protector Cell Manager IP Address and Host name are defined as variables in the System Properties folder in Operations Orchestration.

Open Operations Orchestration Studio on your Operations Orchestration server and login as the admin user.

1. Expand the Configuration folder and System Properties folder.
2. Right click on **System Properties** and select New.
3. Enter DPCellManager as the name of the System Property.
4. In the **Property Value** section enter the host name of the Data Protector Cell Manager.
5. Click on ![lock icon] to check in your changes and click on OK.

6. Right click on **System Properties** and select New.
7. Enter DPCellManagerIP as the name of the System Property.
8. In the **Property Value** section enter the IP Address of the Data Protector Cell Manager.
9. Click on ![lock icon] to check in your changes and click on OK.

**Running the process definition tool**

A process definition tool is created when you install and configure HP Cloud Service Automation. This tool ensures that HP Cloud Service Automation can correctly locate the HP Operations Orchestration workflows that you imported.

To run the process definition tool on the Cloud Service Automation server, complete the following steps:

1. Open the following file in a text editor:
   ```
   C:\Program Files\Hewlett-
   Packard\CSA\Tools\ProcessDefinitionTool\HPOOInfoInput.xml
   ```
2. Add the following line at the end of the file:
   ```
   <folder path="/Library/CSL/Contrib/CSA3.2/HP Data Protector" update="true"
   recursive="true"/>
   ```
3. Run the following command from the ProcessDefinitionTool folder:

   If you are using Oracle database for CSA:
   ```
   java –Done-jar.class.path=ojdbc6.jar –jar process-defn-tool.jar –d
   db.properties –i HPOOInfoInput.xml
   ```

   If you are using Microsoft SQL Server:
   ```
   java –jar process-defn-tool.jar –d db.properties –i HPOOInfoInput.xml
   ```

The Operations Orchestration HP Data Protector workflow is shown below in Figure 3. This is a graphical representation of the Operations Orchestration workflow that installs the Data Protector client, registers the client with the Data Protector Cell Manager and creates a full system back specification on the Data Protector Cell Manager.

Figure 3. HP Data Protector OO Flows
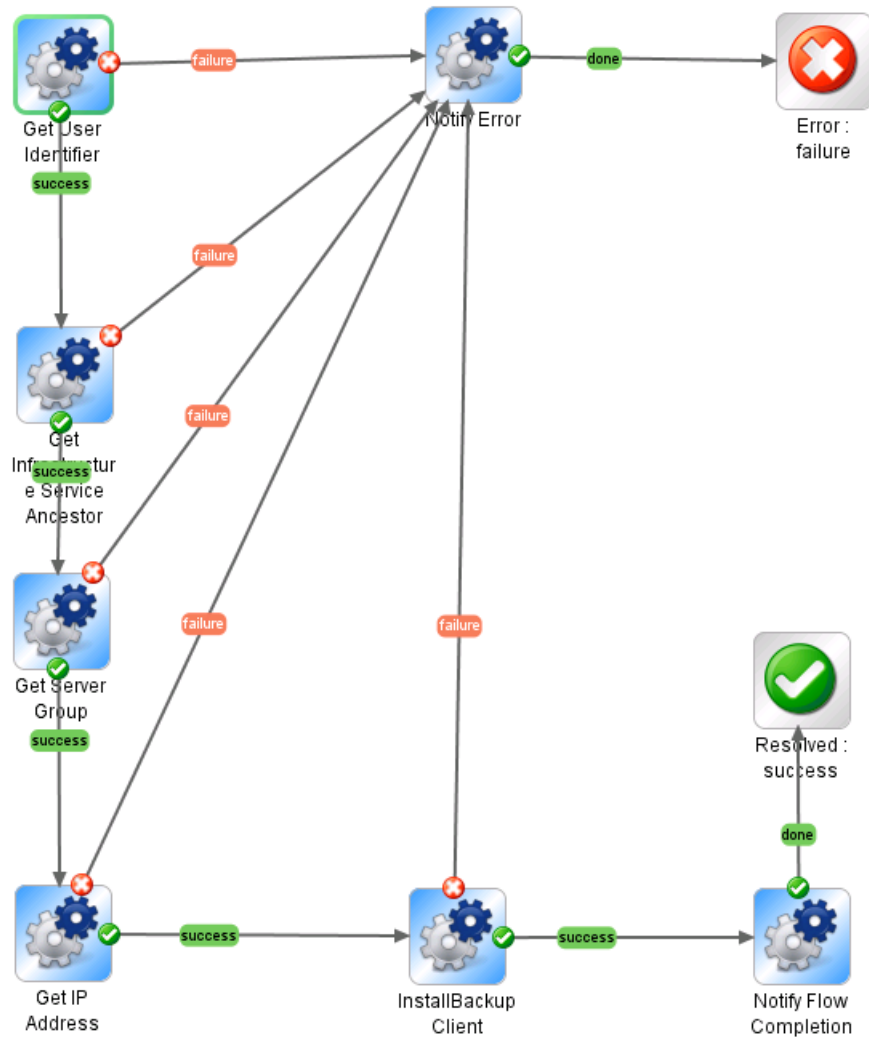
The HP Data Protector workflows are shown below in Figure 4. The Add Data Protector Windows Client workflow is called by the Cloud Service Automation Service design and will install the Windows Data Protector Client when requested from the Cloud Service Automation consumer subscription.

Figure 4. Data Protector OO Action and Subflows

Importing and configuring the HP Data Protector Service Design

Import the VCENTER_COMPUTE_Data_Protector_3.20 Service Design into HP Cloud Service Automation. The service design archive is in the form of a zip file format named SERVICE_DESIGN_VCENTER_COMPUTE_Data_Protector_3.20.zip.

To import the service design archive, complete the following steps:

1. Log on to the HP Cloud Service Automation Administrator portal using an account with administrator privileges.
2. Select the **Designs** tile.

3. Click **Import Service Design Archive** ⬆️.

4. Browse to select `SERVICE_DESIGN_VCENTER_COMPUTE_Data_Protector_3.20.zip` from the distribution files.

5. Click **Import** to import the Service Design archive.

6. You will need to change the pre-defined values to match your environment. Open the `VCENTER_COMPUTE_Data_Protector_3.20` Service Design and select the **Designer** tab.

7. Select the **Simple Compute Server** component, and select **Properties** from the right side. See Table 2 for information about the Properties.

Table 2. Virtual Machine Properties

Property	Value	Description
customSpec	String	VM Template Customization Specification. Customization Specifications are defined in VMware vCenter in Home → Custom Specifications Manager.
datacenterName	String	Name of the Datacenter to deploy the Windows 2008 VM into in VMware vCenter
memory	Integer	Amount of Memory in MB for the VM
nCPU	Integer	Number of CPUs for the VM
osType	Sting	Indicate the OS type being deployed. Value Windows is pre-filled in and is required.
templateReference	String	Name of the OS Template in VMware vCenter to use for the Windows 2008 R2 Virtual Machine.

Figure 5. CSA Service Design
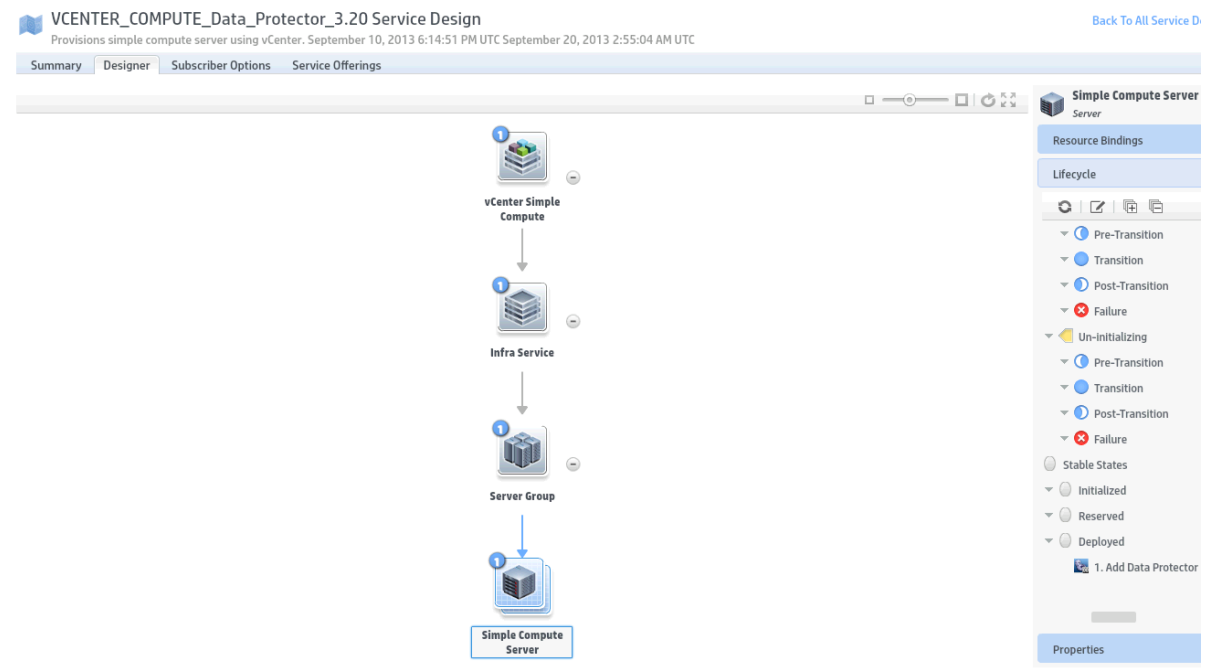
Create and publish the service offering

A service offering must be created in HP Cloud Service Automation before subscribers can request services based on this service design.

To create a service offering, complete the following steps:

1. Log on to the HP Cloud Service Automation Administrator portal using an account with administrator privileges.

2. Select the **Offerings** tile to display all available service offerings.

3. Click **Create Offering** in the left panel. The Create New Service Offering dialog will open.

4. Enter a name for the new Windows VM with HP Data Protector service offering, for example Windows VM with HP Data Protector. This is the name of the offering that will be visible to the subscribers of this service.

5. Select the **VCENTER_ COMPUTE_Data_Protector_3.20** Service Design and click **Create**.

6. After the offering is created, you can modify the pricing information, associate documents, or modify the subscriber options for this subscription and save the changes.

HP Cloud Service Automation is installed with a default global catalog named **Global Shared Catalog**. When you publish a service offering in this global catalog, that service offering will be visible in every organization's Cloud Subscriber Portal.

To publish a service offering in the default catalog, complete the following steps:

1. Log on to the HP Cloud Service Automation Administrator portal using an account with administrator privileges.

2. Select the **Catalogs** tile.

3. Select **Global Shared Catalog** in the panel on the left.

4. Select **Published Offerings** in the central panel.

5. Click **Add Offering**.

6. Select the service offering you created for the Windows VM with HP Data Protector service and click **Select**.

7. For **Select Category**, select the category under which this service offering should appear in the consumer portal. Suggestion is to put the Windows VM with HP Data Protector service offering under Application Services.

8. Click **Add**.

9. Click **OK** on the Success message box.

Adding the Data Protector Client

This section gives examples of how a subscriber can add the Data Protector Client to the virtual machine via the subscription portal. It does not give a complete list of what the subscriber can do.

Creating a subscription in HP Cloud Service Automation

You can order the HP Data Protector service from the HP Cloud Service Automation Consumer Portal Catalog.

1. Enter the URL for the HP Cloud Service Automation Consumer Portal in a web browser. The default URL is `https://<HP CSA Server>:8444/csp`.

   A. The URL will be unique to your installation. Contact your administrator if you are not using the default HP CSA Consumer portal.

2. Enter the following information:

   A. **User Name**: Your HP Cloud Service Automation Consumer Portal user name.

   B. **Password**: Your HP Cloud Service Automation Consumer Portal password.

3. Click **Log In**.

4. Select the **Catalog** tab. In the previous section we suggested that you publish your offerings in the Global Shared Catalog. Select a catalog in the panel on the left. Select the Category (we suggested Application Services in the previous step). The offerings available in this catalog will be displayed.

5. Select the **Windows VM HP Data Protector** service and click on **Select**.

6. Enter a name and description for the subscription.

7. Select a start and end date for the subscription (if required).

8. Click **Request Now**.

The status of your subscription can be monitored on the subscriptions panel, by clicking **Subscriptions** on the tab.

Note

This reference implementation uses the default HP CSA Consumer portal. If your environment is set up for a different consumer organization, please contact your administrator for the URL.

If you wish to follow the service deployment process more closely, you can do so through the various provider interfaces. The first part of the service deployment process is the creation of the virtual machine through VMware vCenter. Login to VMware vCenter and navigate to Home → Inventory → VMs and Templates and you can see the virtual machine being

created. You can view the progress by viewing the Recent Tasks section of the interface or going to Home → Management → Events and you can track the progress of the deployment request in progress.

Adding the Data Protector Client

The HP Data Protector Client is added to the virtual machine by requesting an action through the subscription portal. The user can add the HP Data Protector Client by completing the following steps:

1. Log in to the CSA Consumer Portal at `https://<HP CSA Server>:8444/csp`
2. Click on the Subscriptions tab and the **View Details** button for your newly deployed service.
3. Scroll down to the "`Server`" section and find the deployed Windows virtual machine.
4. Select the drop down to the right of the Windows virtual machine host name and select **Add Data Protector Client** (highlighted in yellow in Figure 6).
5. Select **Request Action**.

Figure 6. Adding HP Data Protector Client

Returning the resource

To conclude the subscription, we will cancel the subscription to return the resources to our pool. To cancel a subscription, complete the following steps:

1. Log in to the CSA Consumer Portal by entering the following address in a browser:
   `https://<HP CSA Server>:8444/csp`
2. Select the **Subscriptions** tab.
3. Locate your subscription and click the **View Details** button.
4. Click on the red **Cancel Subscription** button.
5. Click **Yes** on the message box pop-up and then click on **OK**.
6. The Subscription Status is updated to Cancelled and Service Instance Status to Offline.

Note: Your cancellation time may vary depending on the hardware in your environment.

You will be notified by email that the service has been cancelled.

Submitting a Backup Request to the HP Data Protector Cell Manager

Once the HP Data Protector Manager Windows Client has been installed on the Windows virtual machine, the backup job can be run using the HP Data Protector Manager client. This can be performed from the Windows virtual machine or from the HP Data Protector Cell Manager. If this operation is performed from the Windows virtual machine the user account that is logged into the Windows virtual machine must be specified as a Backup Operator in the HP Data Protector Cell Manager. The following section demonstrates how to launch a full system backup using the HP Data Protector Manager Client from the Windows virtual machine.

HP Data Protector Manager

Log into the Windows virtual machine with a user account that has been specified as a Backup Operator on the HP Data Protector Cell Manager server. From the Start Menu on the Windows virtual machine, launch the HP Data Protector Manager. From the drop down menu, select **Backup.** Expand the **Backup Specification → File System** and select the backup specification for the newly deployed Windows virtual machine. Right-click on the backup specification and select **Start Backup…** This will initiate a full system backup of the Windows virtual machine. You can also perform a preview of the backup by selecting **Preview Backup…** This will test the Backup Specification and provide a report without actually executing the Backup operation. The Preview Backup operation is shown in Figure 7.

Figure 7. HP Data Protector Manager
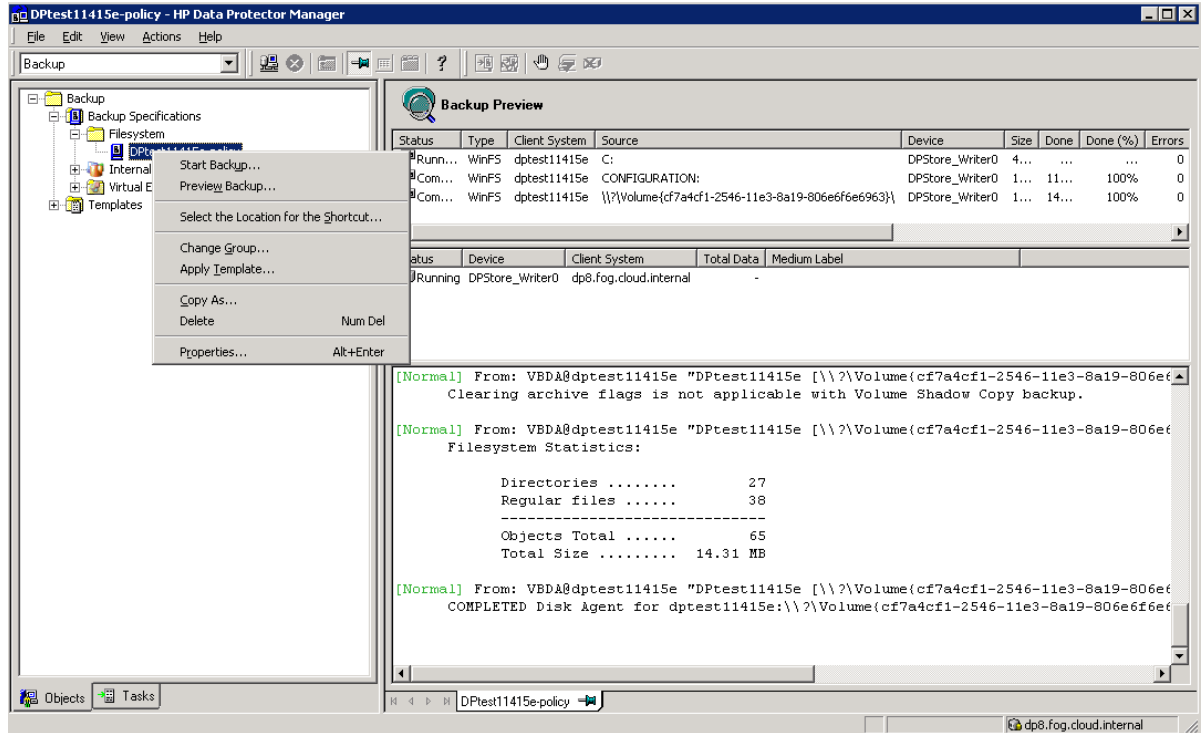
System component details

The table below lists the major component versions of CloudSystem Enterprise and the associated products used in this service design.

Table 3. HP CloudSystem Enterprise components

Component	Version
Servers	HP ProLiant BL460c Gen8
Storage	HP 3PAR StoreServ Storage, HP StoreFabric Switches
Networking	HP 5820 Switch Series
Testing Environment	Physical and virtual servers
HP Onboard Administrator	3.71
HP Virtual Connect Manager	3.75
HP Integrated Lights-Out	1.20 (iLO 4)
HP Matrix Operating Environment	7.2
HP Server Automation	9.14

Component	Version
HP Cloud Service Automation	3.20
HP Operations Orchestration	9.07
HP Data Protector	A.08.00
VMware vCenter Server	5.0.0
VMware vSphere	5.0.0

For more information

Learn more at
hp.com/go/dataprotector

To read more about CloudSystem Enterprise go to
hp.com/go/cloudsystementerprise

Understanding the HP CloudSystem reference architecture
http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA3-4548ENW

HP software product manuals and documentation for the following products can be found at:
http://h20230.www2.hp.com/selfsolve/manuals. You will need an HP Passport to sign in and gain access.

• HP Cloud Service Automation
• HP Server Automation
• HP Operations Orchestration
• HP Data Protector

To help us improve our documents, please provide feedback at hp.com/solutions/feedback.

Sign up for updates
hp.com/go/getupdated

4AA5-0561ENW, January 2014