Abstract
This guide describes the administration functionality of Enterprise Hybrid Cloud 4.1.1. Enterprise Hybrid Cloud enables IT organizations to deliver infrastructure, storage, backup, continuous availability, and disaster recovery as cloud services.

H15830.1R

This document is not intended for audiences in China, Hong Kong, and Taiwan.
# Contents

## Chapter 1 Executive Summary

- Document purpose .......................................................... 6
- Audience ........................................................................ 6
- Essential reading ............................................................ 6
- Business challenge .......................................................... 6
- Solution purpose ............................................................. 7
- Technology solution ......................................................... 7
- We value your feedback ................................................... 8

## Chapter 2 Getting Started

- Terminology ..................................................................... 10
- Important prerequisites .................................................... 11
- Administration scenarios .................................................. 11
- Special character restrictions ........................................... 11

## Chapter 3 Environment Configuration

- Managing features and environmental defaults .................. 13
- Managing environment connections ................................ 15
- Managing sites ................................................................ 17
- Managing vCenters .......................................................... 19
- Managing vCenter relationships ....................................... 22
- Managing hardware islands ............................................. 29
- Managing EMC RecoverPoint for Virtual Machines vRPA clusters ...... 33
- Managing vSphere clusters ............................................... 35
- Remove a VMware ESXi host from a cluster ....................... 43
- Managing datastores ....................................................... 49

## Chapter 4 Storage Services

- Overview ......................................................................... 52
- Storage provisioning services .......................................... 52
- Creating resource reservations ........................................ 53
- Storage as a Service ......................................................... 55
- Assigning storage to business group reservations ............... 63

## Chapter 5 Virtual Machine Lifecycle

- Virtual machine lifecycle .................................................. 66
- Continuous availability .................................................... 71
VMware Site Recovery Manager disaster recovery .......................................................... 72
EMC RecoverPoint for Virtual Machines ...................................................................... 76
Virtual machine encryption ....................................................................................... 83
Public cloud services ............................................................................................... 95
Onboarding a VxRail endpoint ................................................................................ 104

Chapter 6    Data Protection    105
Overview .................................................................................................................. 106
Managing Avamar ..................................................................................................... 106
Managing Avamar Site Relationships .................................................................... 109
Managing Avamar Replication Relationships ....................................................... 112
Managing Avamar proxies ....................................................................................... 116
Managing Backup service levels ............................................................................. 124
Virtual machine backup lifecycle ........................................................................... 130
Ensuring continuity of backup in CA failure scenarios ......................................... 136
Data protection reporting ....................................................................................... 142

Chapter 7    Administration Scenarios    146
Overview .................................................................................................................. 147
Scenario 1: Single site with backup ....................................................................... 147
Scenario 2: Dual site CA with replicated backup ................................................ 150
Scenario 3: Dual-site SRM DR with replicated backup ......................................... 153

Chapter 8    Conclusion    157
Summary .................................................................................................................. 158

Chapter 9    References    159
Documentation ........................................................................................................ 160
This chapter presents the following topics:

Document purpose ............................................................................................. 6
Audience .............................................................................................................. 6
Essential reading ................................................................................................ 6
Business challenge ............................................................................................. 6
Solution purpose ............................................................................................... 7
Technology solution .......................................................................................... 7
We value your feedback ..................................................................................... 8
Chapter 1: Executive Summary

Document purpose

This guide describes the use cases and functionality of Enterprise Hybrid Cloud. It explains how IT organizations can use Enterprise Hybrid Cloud to deliver infrastructure, storage, backup, continuous availability (CA), and disaster recovery (DR), among other functions, as services.

Audience

This document is intended for architects, cloud administrators, and technical administrators of IT environments who want to implement or use Enterprise Hybrid Cloud. Readers should be familiar with the VMware vRealize Suite, storage technologies, and general IT functions and requirements, and how they fit into a hybrid cloud architecture.

Essential reading

The following guides provide further information about various aspects of Enterprise Hybrid Cloud:

- Enterprise Hybrid Cloud 4.1.1: Concepts and Architecture
- Enterprise Hybrid Cloud 4.1.1: Reference Architecture
- Enterprise Hybrid Cloud 4.1.1: Infrastructure and Operations Management

Business challenge

While many organizations have successfully introduced virtualization as a core technology within their data centers, the benefits of virtualization have largely been restricted to the IT infrastructure owners. End users and business units within customer organizations have not experienced many of the benefits of virtualization, such as increased agility, mobility, and control.

Transforming from the traditional IT model to a cloud-operating model involves overcoming the challenges of legacy infrastructure and processes, such as:

- Inefficiency and inflexibility
- Slow, reactive responses to customer requests
- Inadequate visibility into the cost of the requested infrastructure
- Limited choice of availability and protection services

To meet these challenges, public cloud providers have built technology and business models that cater to the requirements of end-user agility and control. Many organizations are under pressure to provide these same service levels within the secure and compliant confines of the on-premises data center. As a result, IT departments must create alternative cloud solutions that are cost-effective and that do not compromise enterprise requirements such as data protection, DR, and guaranteed service levels.
Solution purpose

Enterprise Hybrid Cloud is a completely virtualized data center, fully automated by software. It starts with a foundation that delivers infrastructure as a service. When Enterprise Hybrid Cloud is live, you can customize it with add-on modules, including database as a service, platform as a service, and cloud brokering. In addition, you can optionally implement high availability and data recovery, as well as backup and recovery services.

Enterprise Hybrid Cloud enables:
- Complete management of the infrastructure service lifecycle
- On-demand management of network bandwidth, servers, storage, and security
- Provisioning, monitoring, protection, and management of the infrastructure services by line-of-business users (without IT administrator involvement)
- Provisioning of application blueprints with associated infrastructure resources by line-of-business application owners (without IT administrator involvement)
- Provisioning of backup, CA, and DR services as part of the cloud service provisioning process
- Maximum asset utilization

Technology solution

Enterprise Hybrid Cloud integrates automated workflows and application blueprints with converged and hyper-converged infrastructures with Dell EMC, VMware, professional services, and single contact support into an easy-to-consume hybrid cloud converged platform.

Enterprise Hybrid Cloud integrates the best of Dell EMC and VMware products and services with converged and hyper-converged infrastructures. This integration empowers IT organizations to accelerate implementation and adoption of a hybrid cloud infrastructure, while still enabling customer choice for the compute and networking infrastructure within the data center. Enterprise Hybrid Cloud caters to customers who want to preserve their investment and make better use of their existing infrastructure and to those who want to build out new infrastructures that are dedicated to a hybrid cloud.

Enterprise Hybrid Cloud takes advantage of the strong integration between Dell EMC technologies and the VMware vRealize Suite. Enterprise Hybrid Cloud, developed by Dell EMC, includes Dell EMC scalable storage arrays, integrated Dell EMC and VMware monitoring, and data protection suites to provide the foundation for enabling cloud services within the customer environment.

Enterprise Hybrid Cloud offers several key benefits to customers:
- **Rapid implementation**—Enterprise Hybrid Cloud provides the foundation for infrastructure as a service (IaaS) and can be designed and implemented in a validated, tested, and repeatable way that is based on Dell EMC converged infrastructure. This increases the time-to-value for the customer while simultaneously reducing risk. You will be able to deliver IT as a service (ITaaS) with add-on modules for backup, DR, CA, virtual machine encryption,
applications, application lifecycle automation for continuous delivery, ecosystem extensions, and more.

- **Defined upgrade path**—Customers implementing Enterprise Hybrid Cloud receive upgrade guidance based on the testing and validation completed by the engineering teams. This upgrade guidance enables customers, partners, and Dell EMC services teams to perform upgrades faster and with much less risk.

- **Validated and tested integration**—Extensive integration testing by Dell EMC has made Enterprise Hybrid Cloud simpler to use and manage, and more efficient to operate.

## We value your feedback

Dell EMC and the authors of this document welcome your feedback on the solution and the solution documentation. Contact [EMC.Solution.Feedback@emc.com](mailto:EMC.Solution.Feedback@emc.com) with your comments.

**Authors**: Brian O’Connell, Penelope Howe-Mailly
This chapter presents the following topics:

- **Terminology** ................................................................. 10
- **Important prerequisites** ............................................... 11
- **Administration scenarios** ........................................... 11
- **Special character restrictions** ................................. 11
## Terminology

Table 1 defines some of the terms used in this guide when describing Enterprise Hybrid Cloud.

<table>
<thead>
<tr>
<th>Terminology</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object model</td>
<td>Enterprise Hybrid Cloud uses an object model that provides the framework for storing and referencing metadata related to infrastructure and compute resources. It also acts as the rules engine for provisioning storage, backup service levels, and inter-site or intra-site protection services.</td>
</tr>
<tr>
<td>Hardware island</td>
<td>An Enterprise Hybrid Cloud hardware island of compute, storage, and networking resources. The hardware island concept is the key determining factor in configuring VMware vSphere clusters that offer inter-site or intra-site resilience.</td>
</tr>
<tr>
<td>Avamar Site Relationship (ASR)</td>
<td>A relationship between sites for backup purposes. An ASR is required even if there is only one physical site.</td>
</tr>
<tr>
<td>Avamar Replication Relationship (ARR)</td>
<td>A relationship between as many as three Avamar grids. The ARR determines the specific Avamar grids that are responsible for backup operations on an individual Enterprise Hybrid Cloud workload. An ARR is required even if there is only one physical site.</td>
</tr>
<tr>
<td>Storage as a service (STaaS)</td>
<td>Storage provisioning services provided by EMC ViPR™ Controller.</td>
</tr>
<tr>
<td>Backup as a service (BaaS)</td>
<td>Virtual machine backup services provided by EMC Avamar™.</td>
</tr>
</tbody>
</table>
Important prerequisites

When configuring your Enterprise Hybrid Cloud, you must meet certain requirements for the operations that you want to run.

The flowchart in Figure 1 shows the steps that you must complete before you can create an Avamar backup service level, for example. Each of these steps represents a VMware vRealize Automation catalog item. Where environmental prerequisites exist, they are described in each section and represented in each flow diagram by the initial green step.

Administration scenarios

This guide outlines all Day 2 operations that are possible with Enterprise Hybrid Cloud. Chapter 7 contains common end-to-end administration scenarios that you can use as a reference when configuring Enterprise Hybrid Cloud.

Special character restrictions

Due to delimiter requirements in the backend database, do not use the pipe character ‘|’ or the underscore character ‘_’ in a property name or property value (for example, Site Names) in the object model.
Chapter 3: Environment Configuration

This chapter presents the following topics:

- Managing features and environmental defaults .............................................. 13
- Managing environment connections ............................................................... 15
- Managing sites .............................................................................................. 17
- Managing vCenters ...................................................................................... 19
- Managing vCenter relationships ................................................................. 22
- Managing hardware islands ......................................................................... 29
- Managing EMC RecoverPoint for Virtual Machines vRPA clusters ............ 33
- Managing vSphere clusters .......................................................................... 35
- Remove a VMware ESXi host from a cluster ............................................... 43
- Managing datastores .................................................................................. 49
Managing features and environmental defaults

Overview
The Enterprise Hybrid Cloud object model contains options that you can use to control system behavior across all sites and infrastructure. Some options are internal controls that are visible but cannot be manipulated directly by an Enterprise Hybrid Cloud administrator. EHC Global Options Maintenance enables you to edit the values of the Enterprise Hybrid Cloud global options, to enable features, and to set environmental defaults.

Enable CA
To enable the Enterprise Hybrid Cloud CA protection service:
1. Log in to the Enterprise Hybrid Cloud tenant portal as the system administrator with entitlements to the EHC Global Options Maintenance catalog item (for example, ehc_config_admin@domain.local).
2. Go to Catalog > EHC Configuration and select EHC Global Options Maintenance.
3. Choose ca_enabled from the list box and select Yes.

Modify Avamar replication port
To modify the default Avamar replication port, which is 27000:
1. Log in to the Enterprise Hybrid Cloud tenant portal as the system administrator with entitlements to the EHC Global Options Maintenance catalog item (for example, ehc_config_admin@domain.local).
2. Go to Catalog > EHC Configuration and select EHC Global Options Maintenance.
3. Select avamar_replication_port.
4. Set the value to a different port.

Enable Data Domain
If EMC Data Domain™ has been added to the environment, enable Data Domain to ensure backup settings are optimized:
1. Log in to the Enterprise Hybrid Cloud tenant portal as the system administrator with entitlements to the EHC Global Options Maintenance catalog item (for example, ehc_config_admin@domain.local).
2. Go to Catalog > EHC Configuration and select EHC Global Options Maintenance.
3. Select the data_domain_available option and set the value to Yes.

Modify the default ViPR project
If you change your ViPR project name, update the object model with the new name:
1. Log in to the Enterprise Hybrid Cloud tenant portal as the system administrator with entitlements to the EHC Global Options Maintenance catalog item (for example, ehc_config_admin@domain.local).
2. Go to Catalog > EHC Configuration and select EHC Global Options Maintenance.
3. Select the default_vipr_project option and click Next.
4. Select the new ViPR project name from the list box.
Chapter 3: Environment Configuration

5. Click Next, and then click Submit.

*Note:* The project must exist in ViPR.

### Modify data protection task wait times

If data protection tasks time out due to latency or high wait times, increase the default timeout:

1. Log in to the Enterprise Hybrid Cloud tenant portal as the system administrator with entitlements to the EHC Global Options Maintenance catalog item (for example, ehc_config_admin@domain.local).
2. Go to Catalog > EHC Configuration and select EHC Global Options Maintenance.
3. Select `dp_task_completion_max_wait_time` and type the updated value in seconds.

### Modify the data protection polling time

To set the polling interval for data protection tasks:

1. Log in to the Enterprise Hybrid Cloud tenant portal as the system administrator with entitlements to the EHC Global Options Maintenance catalog item (for example, ehc_config_admin@domain.local).
2. Go to Catalog > EHC Configuration and select EHC Global Options Maintenance.
3. Select `dp_task_polling_time` and type the updated value.

### Modify the virtual pool collapser function

If multiple physical arrays provide physical storage pools of the same service level to EMC VPLEX™ through different ViPR virtual pools, use the virtual pool collapser (VPC) function to ensure that all LUNs provisioned across those physical pools are collapsed into the same storage reservation policy (SRP).

1. Log in to the Enterprise Hybrid Cloud tenant portal as the system administrator with entitlements to the EHC Global Options Maintenance catalog item (for example, ehc_config_admin@domain.local).
2. Go to Catalog > EHC Configuration and select EHC Global Options Maintenance.
3. Select `ehc_vpc_disabled` and select Yes or No.
Enable the hardware island name in the storage reservation name

Enable the policy to present hardware island names in the SRP names in vRealize Automation. This functionality is useful if you have multiple hardware islands per site and want to have control of the destination of a virtual machine.

1. Log in to the Enterprise Hybrid Cloud tenant portal as the system administrator with entitlements to the EHC Global Options Maintenance catalog item (for example, ehc_config_admin@domain.local).
2. Go to Catalog > EHC Configuration and select EHC Global Options Maintenance.
3. Select hwi_srp_policy_enabled and select Yes or No.

Modify the environment logging level

To choose the log level for VMware vRealize Orchestrator logging or change the log level if debugging issues (the default is Info.):

1. Log in to the Enterprise Hybrid Cloud tenant portal as the system administrator with entitlements to the EHC Global Options Maintenance catalog item (for example, ehc_config_admin@domain.local).
2. Go to Catalog > EHC Configuration and select EHC Global Options Maintenance.
3. Select log_level and select the required level.

Reserve HLUs for SAN boot

Create a list of Host LUN Units (HLUs) to exclude from use by ViPR. This functionality is useful when certain HLUs are used for SAN boot.

1. Log in to the Enterprise Hybrid Cloud tenant portal as the system administrator with entitlements to the EHC Global Options Maintenance catalog item (for example, ehc_config_admin@domain.local).
2. Go to Catalog > EHC Configuration and select EHC Global Options Maintenance.
4. Enter the HLU value that you want to reserve and click the green plus sign.
5. Click Submit.

Managing environment connections

Use the Connection Maintenance catalog item to update Enterprise Hybrid Cloud connections, in the Enterprise Hybrid Cloud object model, that were created when the environment was first initialized. This functionality is useful for managing the password lifecycle.

Note: Passwords are updated in the object model only. Update them in other locations manually (for example, Active Directory, service accounts, and so on).

Modify Active Directory details

1. Log in to the Enterprise Hybrid Cloud tenant portal as the system administrator with entitlements to the EHC Connection Maintenance catalog item (for example, ehc_config_admin@domain.local).
2. Go to Catalog > EHC Configuration and select Connection Maintenance.
3. Select **ActiveDirectoryConnection** and modify the details.

**Modify Data Protection Advisor details**

1. Log in to the Enterprise Hybrid Cloud tenant portal as the system administrator with entitlements to the EHC Connection Maintenance catalog item (for example, ehc_config_admin@domain.local).
2. Go to **Catalog > EHC Configuration** and select **Connection Maintenance**.
3. Select **DPAClone** and modify the details.

**Modify vRealize Automation IaaS Web VIP details**

1. Log in to the Enterprise Hybrid Cloud tenant portal as the system administrator with entitlements to the EHC Connection Maintenance catalog item (for example, ehc_config_admin@domain.local).
2. Go to **Catalog > EHC Configuration** and select **Connection Maintenance**.
3. Select **IAASConnection** and modify the details.

**Modify NSX details**

1. Log in to the Enterprise Hybrid Cloud tenant portal as the system administrator with entitlements to the EHC Connection Maintenance catalog item (for example, ehc_config_admin@domain.local).
2. Go to **Catalog > EHC Configuration** and select **Connection Maintenance**.
3. Select **NSXConnection** and modify the details.

**Modify SMTP server details**

1. Log in to the Enterprise Hybrid Cloud tenant portal as the system administrator with entitlements to the EHC Connection Maintenance catalog item (for example, ehc_config_admin@domain.local).
2. Go to **Catalog > EHC Configuration** and select **Connection Maintenance**.
3. Select **SMTPConnection** and modify the details.

**Modify SOAP server details**

1. Log in to the Enterprise Hybrid Cloud tenant portal as the system administrator with entitlements to the EHC Connection Maintenance catalog item (for example, ehc_config_admin@domain.local).
2. Go to **Catalog > EHC Configuration** and select **Connection Maintenance**.
3. Select **SOAPConnection** and modify the details.

**Modify SQL server details**

1. Log in to the Enterprise Hybrid Cloud tenant portal as the system administrator with entitlements to the EHC Connection Maintenance catalog item (for example, ehc_config_admin@domain.local).
2. Go to **Catalog > EHC Configuration** and select **Connection Maintenance**.
3. Select **SQLConnection** and modify the details.

**Modify ViPR details**

1. Log in to the Enterprise Hybrid Cloud tenant portal as the system administrator with entitlements to the EHC Connection Maintenance catalog item (for example, ehc_config_admin@domain.local).
2. Go to **Catalog > EHC Configuration** and select **Connection Maintenance**.
3. Select **ViPRConnection** and modify the details.
1. Log in to the Enterprise Hybrid Cloud tenant portal as the system administrator with entitlements to the EHC Connection Maintenance catalog item (for example, ehc_config_admin@domain.local).

2. Go to Catalog > EHC Configuration and select Connection Maintenance.

3. Select vRAConnection and modify the details.

Modify vRealize Automation details

1. Log in to the Enterprise Hybrid Cloud tenant portal as the system administrator with entitlements to the EHC Connection Maintenance catalog item (for example, ehc_config_admin@domain.local).

2. Go to Catalog > EHC Configuration and select Connection Maintenance.

3. Select vROConnection and modify the details.

Modify vRealize Orchestrator details

Managing sites

In the Enterprise Hybrid Cloud object model, sites are the first item to be created and all other items ultimately depend on one or more sites. A site is a label that is given to a physical site. The site maintenance catalog item enables the administrator to manipulate site objects.

Note: For information about the maximum number of sites, refer to the Enterprise Hybrid Cloud 4.1.1 Concepts and Architecture Guide.

To perform site maintenance:

1. Log in to the Enterprise Hybrid Cloud tenant portal as the system administrator with entitlements to the EHC Maintenance catalog items (for example, ehc_config_admin@domain.local).

2. Go to Catalog > EHC Configuration and select Site Maintenance, as shown in Figure 2.

Service Catalog

Browse the catalog for services you need.

![Service Catalog Image]

Figure 2. Site Maintenance catalog item
Chapter 3: Environment Configuration

3. Under **Request Information**, type a description, optionally type a reason, and click **Next**, as shown in Figure 3.

![Figure 3. Site Maintenance: Request Information](image)

4. Select an action from the list, as shown in Figure 4.

![Figure 4. Site Maintenance: Action Choice](image)

**Prerequisites**

While there are no physical prerequisites for adding a site to the object model, it is assumed that the corresponding physical site exists.

Figure 5 shows the required steps to add a site.

![Figure 5. Add a site flowchart](image)
Catalog Item description

Table 2 describes the Add Site catalog item requirements.

Table 2. Add Site Options

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site Name</td>
<td>A free-text field that is verified to ensure no duplication occurs of an existing site name.</td>
</tr>
</tbody>
</table>

Update a site

Catalog Item description

Table 3 describes the Update Site catalog item requirements.

Table 3. Update site options

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site</td>
<td>Select an existing site from the list.</td>
</tr>
<tr>
<td>New Site Name</td>
<td>Editing a site name is only permitted if the site is not referenced elsewhere in the Enterprise Hybrid Cloud object model. Otherwise, a list of references that need to be updated or deleted before editing is presented to the administrator.</td>
</tr>
</tbody>
</table>

Delete a site

Catalog Item description

Table 4 describes the Delete Site catalog item requirements.

Table 4. Delete site options

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site</td>
<td>Select an existing site from the list.</td>
</tr>
<tr>
<td>Confirm</td>
<td>Select Confirm or Deny, as required. Deleting a site name is only permitted if that name is not referenced elsewhere in the Enterprise Hybrid Cloud object model. Otherwise, a list of references that need to be updated or deleted first is presented to the administrator.</td>
</tr>
</tbody>
</table>

Managing vCenters

Enterprise Hybrid Cloud supports up to four VMware vCenter endpoints, which are managed by Enterprise Hybrid Cloud. Each managed vCenter can be configured as a vRealize Automation vCenter endpoint to provide Enterprise Hybrid Cloud services. An additional six IaaS-only vCenter endpoints may be added for a maximum of 10 vCenters. The vCenter maintenance catalog item enables the administrator to manipulate vCenter objects.

To perform vCenter endpoint maintenance:

1. Log in to the Enterprise Hybrid Cloud tenant portal as the system administrator with entitlements to the EHC Maintenance catalog items (for example, ehc_config_admin@domain.local).
2. Go to Catalog > EHC Configuration and select vCenter Endpoint Maintenance, as shown in Figure 6.

Service Catalog
Browse the catalog for services you need.

All Services

Cloud Storage

Data Protection Services

EHC Configuration

All Services (1)

vCenter Endpoint Maintenance
Create, edit and delete vCenter objects in the EHC data model.

Request

Figure 6. vCenter Endpoint Maintenance catalog item

3. Under Request Information, type a description, optionally a reason, and click Next, as shown in Figure 7.

New Request

vCenter Endpoint Maintenance
Create, edit and delete vCenter objects in the EHC data model.

Request Information  Action Choice

* Description: Add vCenter

* Reasons: 

Figure 7. vCenter Endpoint Maintenance: Request Information

4. Select the operation you want to perform from the list, as shown in Figure 8.

New Request

vCenter Endpoint Maintenance
Create, edit and delete vCenter objects in the EHC data model.

Request Information  Action Choice

Action:
Add vCenter
Update vCenter
Delete vCenter

Figure 8. vCenter Endpoint Maintenance: Action Choice
Prerequisites

- The vCenter must exist.
- The vCenter must be added to the vRealize Orchestrator vCenter plug-in.

Figure 9 shows the required steps to add a vCenter.

![Add a vCenter flowchart](image)

**Catalog Item description**

Table 5 describes the Add vCenter catalog item requirements.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name for vCenter endpoint</td>
<td>Add a user-friendly name for the vCenter.</td>
</tr>
<tr>
<td>Select VC FQDN to add</td>
<td>Select a Fully Qualified Domain Name (FQDN) with values from the vRealize Orchestrator vCenter plug-in. vCenters that are already added to the object model are not shown.</td>
</tr>
<tr>
<td>New vCenter Associated Sites</td>
<td>Select up to two sites from a list of on-boarded sites.</td>
</tr>
<tr>
<td>Select Datacenter to Add</td>
<td>Select a single datacenter from list of datacenters discovered in the chosen vCenter.</td>
</tr>
</tbody>
</table>
Chapter 3: Environment Configuration

Update a vCenter

Table 6 describes the Updated vCenter catalog item requirements.

Table 6. Update vCenter Options

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter</td>
<td>Select a vCenter from the list box of previously-added vCenters.</td>
</tr>
<tr>
<td>New vCenter name</td>
<td>Edit this parameter only if it is not referenced by any cluster or hardware island. If it is part of a DR pair relationship, you must also update its partner’s dr_partner_name.</td>
</tr>
<tr>
<td>FQDN</td>
<td>Select an alternate vCenter FQDN from the list of vCenters presented by the vRealize Orchestrator plug-in. vCenters that are already added are not shown. Edit this parameter only if the vCenter is not referenced by any hardware islands or clusters.</td>
</tr>
<tr>
<td>Datacenter</td>
<td>Edit this parameter only if the vCenter is not referenced by any hardware islands or clusters associated with the same vCenter.</td>
</tr>
<tr>
<td>Site(s)</td>
<td>Edit this parameter only if it is not referenced by any hardware islands or clusters associated with the same vCenter.</td>
</tr>
</tbody>
</table>

Note: A vCenter object may only be deleted if not referenced by any other objects (clusters, hardware islands, or other vCenters).

Delete a vCenter

Table 7 describes the Delete vCenter parameters.

Table 7. Delete vCenter options

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter</td>
<td>Select a vCenter from the list of previously-added vCenters.</td>
</tr>
<tr>
<td>Confirm</td>
<td>Select Confirm or Deny, as required.</td>
</tr>
</tbody>
</table>

Managing vCenter relationships

The vCenter Relationship Maintenance catalog item allows you to manipulate the relationships between vCenters in the Enterprise Hybrid Cloud object model. vCenters that participate in DR relationships require a relationship in the object model to enable and control the availability of DR services.

To perform vCenter relationship maintenance:

1. Log in to the Enterprise Hybrid Cloud tenant portal as the system administrator with entitlements to the EHC Maintenance catalog items (for example, ehc_config_admin@domain.local).
2. Go to Catalog > EHC Configuration and select vCenter Relationship Maintenance, as shown in Figure 10.

Service Catalog
Browse the catalog for services you need.

![Service Catalog Image]

Figure 10. vCenter Relationship Maintenance catalog item

3. Under Request Information, type a description, optionally type a reason, and click Next.

4. Under Action Choice, select the operation you want to perform, as shown in Figure 11.

![New Request Image]

Figure 11. vCenter Relationship Maintenance: Action Choice
Add an EMC RecoverPoint for Virtual Machines vCenter relationship

Prerequisites

- Both vCenters must exist.
- Both vCenters must be added to the vRealize Orchestrator vCenter plug-in.
- Cross vCenter NSX must be configured.
- EMC RecoverPoint for Virtual Machines must be configured.

Figure 12 shows the required steps to add a vCenter relationship.

![Add a vCenter Relationship flowchart](image)

**Catalog item description**

To add an EMC RecoverPoint for Virtual Machines vCenter relationship, supply information about each vCenter and its associated components.

Table 8 describes the available vCenter parameters.

**Table 8. Add EMC RecoverPoint for Virtual Machines vCenter relationship: vCenter Information**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protected vCenter</td>
<td>Select the protected vCenter from the list. Only vCenters already added in the object model are shown.</td>
</tr>
<tr>
<td>Protected vCenter Username</td>
<td>Enter a vCenter username (for example, <a href="mailto:app_vro_vcenter@domain.local">app_vro_vcenter@domain.local</a>).</td>
</tr>
<tr>
<td>Protected vCenter Password</td>
<td>Enter a vCenter password.</td>
</tr>
<tr>
<td>Recovery vCenter</td>
<td>Select the recovery vCenter. Only vCenters already added in the object model are shown.</td>
</tr>
<tr>
<td>Recovery vCenter Username</td>
<td>Enter a vCenter username (for example, <a href="mailto:app_vro_vcenter@domain.local">app_vro_vcenter@domain.local</a>).</td>
</tr>
<tr>
<td>Recovery vCenter Password</td>
<td>Enter a vCenter password.</td>
</tr>
</tbody>
</table>

**Note:** The recovery vCenter must be on a different site from the protected vCenter.
Table 9 describes the parameters that are available for NSX Manager host configurations.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSX Available</td>
<td>Select if NSX is being used.</td>
</tr>
<tr>
<td>Protected site NSX endpoint Name</td>
<td>Enter a friendly name for the protected site NSX endpoint.</td>
</tr>
<tr>
<td>Enter Protected site NSX manager URL</td>
<td>Enter the protected site NSX manager URL.</td>
</tr>
<tr>
<td>Protected site NSX manager username</td>
<td>Enter a username for the protected site NSX manager (for example, <a href="mailto:app_vro_nsx@domain.local">app_vro_nsx@domain.local</a>).</td>
</tr>
<tr>
<td>Protected site NSX manager password</td>
<td>Enter an NSX manager password.</td>
</tr>
<tr>
<td>Recovery site NSX endpoint Name</td>
<td>Enter a friendly name for the recovery site NSX manager.</td>
</tr>
<tr>
<td>Enter Recovery site NSX manager URL</td>
<td>Enter the URL of the recovery site NSX manager.</td>
</tr>
<tr>
<td>Recovery site NSX manager username</td>
<td>Enter the recovery site NSX manager username (for example, <a href="mailto:app_vro_nsx@domain.local">app_vro_nsx@domain.local</a>).</td>
</tr>
<tr>
<td>Recovery site NSX manager password</td>
<td>Enter the password for the recovery site NSX manager.</td>
</tr>
</tbody>
</table>

Prerequisites

- Both vCenters must exist.
- Both vCenters must be added to the vRealize Orchestrator vCenter plug-in.
- When vCenters are added to the object model, they must be associated with different sites.
- NSX must be configured (if being used).
- VMware Site Recovery Manager must be configured.

Figure 13 shows the required steps to add a vCenter Relationship.
Catalog item description

To add a VMware Site Recovery Manager DR vCenter relationship, provide information about each vCenter and associated components.

Table 10 describes the parameters that are available for vCenter Information.

Table 10. Add SRMDR vCenter relationship: vCenter Information

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protected vCenter</td>
<td>Select the protected vCenter. Only vCenters already added are shown.</td>
</tr>
<tr>
<td>Protected vCenter Username</td>
<td>Type a vCenter username (for example, <a href="mailto:app_vro_vcenter@domain.local">app_vro_vcenter@domain.local</a>).</td>
</tr>
<tr>
<td>Protected vCenter Password</td>
<td>Type a vCenter password.</td>
</tr>
<tr>
<td>Recovery vCenter</td>
<td>Select the recovery vCenter. Only vCenters already added in the object model are shown.</td>
</tr>
<tr>
<td>Recovery vCenter Username</td>
<td>Type a vCenter username (for example, <a href="mailto:app_vro_vcenter@domain.local">app_vro_vcenter@domain.local</a>).</td>
</tr>
<tr>
<td>Recovery vCenter Password</td>
<td>Type a vCenter password.</td>
</tr>
</tbody>
</table>

Table 11 describes the parameters that are available for NSX Manager host configurations.

Table 11. Add SRMDR vCenter relationship: NSX Manager host configurations

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSX Available</td>
<td>Select if NSX is being used.</td>
</tr>
<tr>
<td>Protected site NSX endpoint Name</td>
<td>Type a friendly name for the protected site NSX endpoint.</td>
</tr>
<tr>
<td>Enter Protected site NSX manager URL</td>
<td>Type the protected-site NSX manager URL.</td>
</tr>
<tr>
<td>Protected site NSX manager username</td>
<td>Type a username for the protected-site NSX manager (for example, <a href="mailto:app_vro_nsx@domain.local">app_vro_nsx@domain.local</a>).</td>
</tr>
<tr>
<td>Protected site NSX manager password</td>
<td>Type the password for the account defined above (for example, <a href="mailto:app_vro_nsx@domain.local">app_vro_nsx@domain.local</a>).</td>
</tr>
<tr>
<td>Recovery site NSX endpoint Name</td>
<td>Type a friendly name for the recovery-site NSX manager.</td>
</tr>
<tr>
<td>Enter Recovery site NSX manager URL</td>
<td>Type the recovery-site NSX manager URL.</td>
</tr>
<tr>
<td>Recovery site NSX manager username</td>
<td>Type the recovery-site NSX manager username (for example, <a href="mailto:app_vro_nsx@domain.local">app_vro_nsx@domain.local</a>).</td>
</tr>
<tr>
<td>Recovery site NSX manager password</td>
<td>Type the password for the account defined above (for example, <a href="mailto:app_vro_nsx@domain.local">app_vro_nsx@domain.local</a>).</td>
</tr>
</tbody>
</table>
Table 12 describes the parameters that are available for Site Recovery Manager plug-in information.

**Table 12. Add SRMDR vCenter relationship: SRM plug-in information**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Protected SRM Site</td>
<td>Select the protected SRM site.</td>
</tr>
<tr>
<td>Username</td>
<td>Type a username for the protected-site SRM server (for example, <a href="mailto:app_vro_srm@domain.local">app_vro_srm@domain.local</a>).</td>
</tr>
<tr>
<td>Password</td>
<td>Type the password for the account defined above (for example, <a href="mailto:app_vro_srm@domain.local">app_vro_srm@domain.local</a>)</td>
</tr>
<tr>
<td>Select Recovery SRM Site</td>
<td>Select the recovery SRM site.</td>
</tr>
<tr>
<td>Username</td>
<td>Type a username for the recovery-site SRM server (for example, <a href="mailto:app_vro_srm@domain.local">app_vro_srm@domain.local</a>).</td>
</tr>
<tr>
<td>Password</td>
<td>Type the password for the account defined above (for example, <a href="mailto:app_vro_srm@domain.local">app_vro_srm@domain.local</a>)</td>
</tr>
</tbody>
</table>

Table 13 describes the parameters that are available for SRM SQL Site Information.

**Table 13. Add SRMDR vCenter relationship: SRM SQL site information**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protected SRM SQL host Name</td>
<td>Type a friendly name for the protected-site SRM SQL Server.</td>
</tr>
<tr>
<td>SRM Protected Site SQL Database Host</td>
<td>Type the protected-site SRM SQL Server FQDN (for example, sql01.domain.local).</td>
</tr>
<tr>
<td>Protected Site SQL Database Port</td>
<td>Type the protected-site SRM SQL Server port (for example, 1433).</td>
</tr>
<tr>
<td>Select Authentication Type (Local SQL or Domain)</td>
<td>Select windows domain authentication.</td>
</tr>
<tr>
<td>Protected Site SQL Username</td>
<td>Type the username for the protected-site SRM SQL Server for example, app_vro_sql).</td>
</tr>
<tr>
<td>Protected Site SQL Password</td>
<td>Type a name for the protected-site SRM SQL Server password.</td>
</tr>
<tr>
<td>Protected Site SQL User Domain</td>
<td>Type the protected-site SRM SQL Server domain (for example, domain.local).</td>
</tr>
<tr>
<td>Protected Site SQL Database Name</td>
<td>Type the protected-site SRM SQL Server database name (for example, srm01).</td>
</tr>
<tr>
<td>Recovery SRM SQL host Name</td>
<td>Type a friendly name for the recovery-site SRM SQL Server.</td>
</tr>
<tr>
<td>SRM Recovery Site SQL Database Host</td>
<td>Type the protected-site SRM SQL Server FQDN (for example, sql02.domain.local).</td>
</tr>
<tr>
<td>Recovery Site SQL Database Port</td>
<td>Type the recovery-site SRM SQL Server port (for example, 1433).</td>
</tr>
<tr>
<td>Select Authentication Type (Local SQL or Domain)</td>
<td>Select windows domain authentication.</td>
</tr>
</tbody>
</table>
## Chapter 3: Environment Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recovery Site SQL Username</td>
<td>Type the username for the recovery-site SRM SQL Server (for example, app_vro_sql).</td>
</tr>
<tr>
<td>Recovery Site SQL Password</td>
<td>Type the password for the recovery site SRM SQL Server.</td>
</tr>
<tr>
<td>Recovery Site SQL User Domain</td>
<td>Enter the recovery site SRM SQL Server domain (for example, domain.local).</td>
</tr>
<tr>
<td>Protected Site SQL Database Name</td>
<td>Type the protected site SRM SQL Server database name (for example, srm02).</td>
</tr>
</tbody>
</table>

Table 14 describes the parameters that are available for SRM Plug-in Information.

### Table 14. Add SRMDR vCenter relationship: SRM SOAP information

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protected SRM SOAP host Name</td>
<td>Type a friendly name for the protected site SRM SOAP host</td>
</tr>
<tr>
<td>Protected SRM SOAP Host FQDN</td>
<td>Type the FQDN for the protected site SRM server (for example, sm01.domain.local). This parameter is used for creating a SOAP host in vRealize Orchestrator for execution of SOAP calls.</td>
</tr>
<tr>
<td>Username</td>
<td>Username for the protected site SRM SOAP host (for example, <a href="mailto:app_vro_srm@domain.local">app_vro_srm@domain.local</a>).</td>
</tr>
<tr>
<td>Password</td>
<td>Password for the protected site SRM SOAP host</td>
</tr>
<tr>
<td>Recovery SRM SOAP host Name</td>
<td>Type a friendly name for the recovery site SRM SOAP host</td>
</tr>
<tr>
<td>Recovery SRM SOAP Host FQDN</td>
<td>Type the FQDN for the recovery site SRM server. This parameter is used for creating a SOAP host in vRealize Orchestrator for execution of SOAP calls.</td>
</tr>
<tr>
<td>Username</td>
<td>Username for the recovery site SRM SOAP host (for example, <a href="mailto:app_vro_srm@domain.local">app_vro_srm@domain.local</a>).</td>
</tr>
<tr>
<td>Password</td>
<td>Password for the recovery site SRM SOAP host</td>
</tr>
</tbody>
</table>

Delete a vCenter relationship

A vCenter relationship can only be deleted if it has no associated clusters of type DR2S.

**Catalog item description**

Table 15 describes the delete parameters that are available.

### Table 15. Delete vCenter options

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protected vCenter Name</td>
<td>Select a vCenter from the list.</td>
</tr>
<tr>
<td>Recovery vCenter Name</td>
<td>Select a vCenter from the list.</td>
</tr>
</tbody>
</table>
Add SRM DR to an environment with EMC RecoverPoint for Virtual Machines

An EMC RecoverPoint for Virtual Machines vCenter relationship can be extended with SRM DR protection to allow both protection services to co-exist. This catalog item action allows you to type SRM DR information, as described in Add a VMware Site Recovery Manager DR vCenter relationship, to extend the protection services.

Managing hardware islands

A hardware island is a concept within Enterprise Hybrid Cloud that describes an island of compute, storage, and networking resources. The hardware island concept is the key determining factor for configuring vSphere clusters that offer inter- or intra-site resilience. The hardware island maintenance catalog item lets you manipulate hardware island objects.

To perform hardware island maintenance:

1. Log in to the Enterprise Hybrid Cloud tenant portal as the system administrator with entitlements to the EHC Maintenance catalog items (for example, ehc_config_admin@domain.local).
2. Go to Catalog > EHC Configuration and select Hardware Island Maintenance, as shown in Figure 14.
3. Under Request Information, type a description, optionally type a reason, and click Next.
4. Under **Action Choice**, select the action you want to perform, as shown in Figure 15.

**New Request**

*Hardware Island Maintenance*
Create, edit, and delete a Hardware Island object in the EHC data model.

<table>
<thead>
<tr>
<th>Action Choice</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>[choose action]</td>
<td>Add VoRail based Hardware Island</td>
</tr>
<tr>
<td>[choose action]</td>
<td>Add VoRack</td>
</tr>
<tr>
<td>[choose action]</td>
<td>Edit VoRail based Hardware Island</td>
</tr>
<tr>
<td>[choose action]</td>
<td>Edit VoRack</td>
</tr>
<tr>
<td>[choose action]</td>
<td>Delete Hardware Island</td>
</tr>
</tbody>
</table>

**Figure 15. Hardware Island Maintenance: Action Choice**

**Add a hardware island**

**Prerequisites**
- The vCenters must exist.
- The vCenters must be added to the vRealize Orchestrator vCenter plug-in.
- ViPR must be configured with virtual arrays (applicable to hardware islands with clusters that require ViPR based storage provisioning services).

Figure 16 shows the required steps to a hardware island.

**Figure 16. Add a hardware island flowchart**
Catalog item description
Table 16 describes the add hardware island parameters that are available for Dell EMC VxRail™ Appliances.

Table 16. Add hardware island options for VxRail Appliances

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A free-text field that is verified to ensure no duplication occurs of an existing hardware island name. Type a name.</td>
</tr>
<tr>
<td>vCenter</td>
<td>A list that presents vCenter endpoints configured within the vCenters object. Choose one.</td>
</tr>
<tr>
<td>Site</td>
<td>A list of sites associated with the chosen vCenter object. Choose one.</td>
</tr>
</tbody>
</table>

Table 17 describes the add hardware island parameters that are available for Dell EMC VxRack™ System FLEX and Dell EMC VxBlock™ Systems.

Table 17. Add hardware island options for VxRack FLEX and VxBlock Systems

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A free-text field that is verified to ensure no duplication occurs of an existing hardware island name. Type a name.</td>
</tr>
<tr>
<td>vCenter</td>
<td>A list that presents vCenter endpoints configured within the vCenters object. Choose one.</td>
</tr>
<tr>
<td>Site</td>
<td>A list of sites associated with the chosen vCenter object. Choose one.</td>
</tr>
<tr>
<td>ViPR Instance</td>
<td>Pre-populated with the ViPR information of the ViPR instance used in Enterprise Hybrid Cloud.</td>
</tr>
<tr>
<td>ViPR Virtual Arrays</td>
<td>A list of ViPR virtual arrays, filtered to exclude virtual arrays already associated with a Hardware Island. Choose vArray(s) to be associated with the new hardware island.</td>
</tr>
</tbody>
</table>

Catalog item description
Table 18 describes the update hardware island parameters that are available for VxRail Appliances.

Table 18. Update VxRail-based hardware island options for VxRail Appliances

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Island</td>
<td>A list of hardware islands. Choose one.</td>
</tr>
<tr>
<td>New Name</td>
<td>This parameter can be edited only if the hardware island is not referenced by a cluster or datastore.</td>
</tr>
<tr>
<td>vCenter</td>
<td>This parameter can be edited only if there are no clusters mapped to the hardware island.</td>
</tr>
<tr>
<td>Site(s)</td>
<td>This parameter can be edited only if the hardware island is not used by any cluster or datastore.</td>
</tr>
</tbody>
</table>
Table 19 describes the update hardware island parameters that are available for VxRack System FLEX and VxBlock Systems.

**Table 19. Update hardware island options for VxRack FLEX and VxBlock Systems**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Island</td>
<td>This is a list of hardware islands. Choose one.</td>
</tr>
<tr>
<td>New Name</td>
<td>This parameter can be edited only if the hardware island is not referenced by a cluster or datastore.</td>
</tr>
<tr>
<td>vCenter</td>
<td>This parameter can be edited only if there are no clusters mapped to the hardware island.</td>
</tr>
<tr>
<td>Site(s)</td>
<td>This parameter can be edited only if the hardware island is not used by any cluster or datastore.</td>
</tr>
<tr>
<td>ViPR Instance</td>
<td>This parameter can be edited only if there are no datastores associated with the hardware island.</td>
</tr>
<tr>
<td>ViPR Virtual Arrays</td>
<td>This parameter can be appended with additional vArrays. A vArray can be removed only if there are no datastores associated with it.</td>
</tr>
</tbody>
</table>

**Note:** If CA clusters exist, their affinity groups might need to be updated if `hwi_srp_policy_enabled` is true. See [Enable the hardware island name in the storage reservation name](#) for more information.

Delete Hardware Island

**Catalog item description**

Table 20 describes the delete hardware island parameters that are available.

**Table 20. Delete hardware island options**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Island</td>
<td>Select one from the list of hardware islands. A hardware island can only be deleted if there are no associated clusters or datastores.</td>
</tr>
<tr>
<td>Confirm</td>
<td>Select Confirm or Deny, as required.</td>
</tr>
</tbody>
</table>
Managing EMC RecoverPoint for Virtual Machines vRPA clusters

To enable RecoverPoint for Virtual Machines protection services in the Enterprise Hybrid Cloud, the system administrator must onboard the virtual RecoverPoint appliances (vRPAs) to the Enterprise Hybrid Cloud object model.

To onboard vRPAs:

1. Log in to the Enterprise Hybrid Cloud tenant portal as the system administrator with entitlements to the EHC Maintenance catalog items (for example, ehc_config_admin@domain.local).

2. Go to Catalog > EHC Configuration and select RP4VM vRPA Cluster Maintenance, as shown in Figure 17.
3. Under **Request Information**, type a description, optionally type a reason, and click **Next**, as shown in Figure 18.

![Figure 18. Cluster Maintenance: Request Information](image)

4. Under **Action Choice**, select the action you want to perform, as shown in Figure 19.

![Figure 19. Cluster Maintenance: Action Choice](image)

### Add a vRPA cluster pair

#### Prerequisites
- Two vCenters must exist.
- Both vCenters must be added to the vRealize Orchestrator vCenter plug-in.
- A vRPA cluster must be deployed and configured at each physical site.
- Each vRPA cluster must be associated with a vCenter cluster.
- The vRPA clusters must not be present in the object model.
Figure 20 shows the required steps to onboard a vRPA cluster pair.

![Onboard a vRPA cluster pair flowchart](image)

**Catalog item description**

1. To onboard a vRPA cluster pair, select **Add Cluster Pair** and click **Next**.

Table 21 describes the local cluster on-boarding parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary Cluster Management IP</td>
<td>Type the IP address of the primary vRPA cluster.</td>
</tr>
<tr>
<td>Primary Cluster Admin Username</td>
<td>Type the primary vRPA cluster admin username (for example, ehc_rp4vm_admin).</td>
</tr>
<tr>
<td>Primary Cluster Password</td>
<td>Type the password for the vRPA cluster admin user defined above (for example, ehc_rp4vm_admin).</td>
</tr>
<tr>
<td>Secondary Cluster Management IP</td>
<td>Type the IP address of the secondary vRPA cluster.</td>
</tr>
<tr>
<td>Secondary Cluster Admin Username</td>
<td>Type the secondary vRPA cluster admin username (for example, ehc_rp4vm_admin).</td>
</tr>
<tr>
<td>Secondary Cluster Password</td>
<td>Type the password for the vRPA cluster admin user defined above (for example, ehc_rp4vm_admin).</td>
</tr>
</tbody>
</table>

2. Click **Next** to review and then click **Submit**.

**Managing vSphere clusters**

A cluster object is created in the Enterprise Hybrid Cloud object model as soon as a vSphere cluster is onboarded through the vRealize Automation catalog. When onboarding clusters, each cluster must be given a type, which then dictates the type of storage that can be provisioned to the cluster. The cluster maintenance catalog item allows the administrator to manipulate cluster objects.
Chapter 3: Environment Configuration

Table 22 shows the cluster types available in the model.

Table 22. Cluster types

<table>
<thead>
<tr>
<th>Datastore type</th>
<th>Storage description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LC1S</td>
<td>Local Copy on One Site</td>
</tr>
<tr>
<td>VS1S</td>
<td>VSAN Storage on One Site (not used by STaaS)</td>
</tr>
<tr>
<td>CA1S</td>
<td>CA VPPLEX Metro Storage on One Site</td>
</tr>
<tr>
<td>CA2S</td>
<td>CA VPPLEX Metro Storage across Two Sites</td>
</tr>
<tr>
<td>DR2S</td>
<td>DR RecoverPoint Storage across Two Sites</td>
</tr>
</tbody>
</table>

To perform cluster maintenance:

1. Log in to the Enterprise Hybrid Cloud tenant portal as the system administrator with entitlements to the EHC Maintenance catalog items (for example, ehc_config_admin@domain.local).

2. Go to Catalog > EHC Configuration and select Cluster Maintenance, as shown in Figure 21.

Figure 21. Cluster Maintenance catalog item
4. Under **Request Information**, type a description, optionally type a reason, and click **Next**, as shown in Figure 22.

![Figure 22. Cluster Maintenance: Request Information](image)

5. Under **Action Choice**, select the action you want to perform, as shown in Figure 23.

![Figure 23. Cluster Maintenance: Action Choice](image)

### Prerequisites

- The vCenter must exist
- The vCenter must be added to the vRealize Orchestrator vCenter plug-in.
- The cluster must exist.
- The cluster must not be present in the object model.
Chapter 3: Environment Configuration

Figure 24 shows the required steps to onboard a local cluster.

![Onboard a local cluster flowchart](image)

**Catalog item description**

1. To onboard a local cluster, select **Onboard Local Cluster** and click **Next**.
   
   Table 23 describes the local cluster onboarding parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select a hardware island</td>
<td>Select the relevant island.</td>
</tr>
<tr>
<td>Select unprepared cluster</td>
<td>Select a cluster.</td>
</tr>
</tbody>
</table>

2. Click **Next** to review and then click **Submit**.

**Onboard a vSAN cluster**

**Prerequisites**

- The vCenter must exist.
- The vCenter must be added to the vRealize Orchestrator vCenter plug-in.
- The cluster must exist.
- The cluster must not be present in the object model.

Figure 25 shows the required steps to onboard a local cluster.

![Onboard a local cluster flowchart](image)
Catalog item description

1. To onboard a vSAN cluster, select **Onboard vSAN Cluster** and click **Next**.
   
   Table 24 describes the local cluster on-boarding parameters.
   
   **Table 24. vSAN cluster on-boarding parameters**
   
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select a Hardware Island</td>
<td>Select a Hardware Island from the list box.</td>
</tr>
<tr>
<td>Select unprepared cluster</td>
<td>Select a cluster from the list box.</td>
</tr>
</tbody>
</table>

2. Click **Next** to review and then click **Submit**.

Onboard a CA cluster

Prerequisites

- The vCenter must exist.
- The vCenter must be added to the vRealize Orchestrator vCenter plug-in.
- During onboarding, the vCenter can be associated with one or two sites in the object model, depending on the CA configuration (single-site or dual-site).
- Two hardware islands must exist.
- The cluster must exist.
- The cluster must not be present in the object model.

Figure 26 shows the required steps to onboard a CA cluster.

![Prerequisites flowchart](image)

**Figure 26. Onboard a CA cluster flowchart**
Chapter 3: Environment Configuration

Catalog item description

1. To onboard a CA cluster, select **Onboard CA Cluster** and click **Next**. Table 25 describes the CA cluster on-boarding parameters.

Table 25. CA cluster on-boarding parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Island 1</td>
<td>Select a hardware island.</td>
</tr>
<tr>
<td>Cluster</td>
<td>Select a cluster.</td>
</tr>
<tr>
<td>Inter-site vs. Intra-site</td>
<td>Choose whether the CA configuration is inter-site (dual site) or intra-site (single site).</td>
</tr>
<tr>
<td>Hardware Island 2</td>
<td>Select a hardware island.</td>
</tr>
<tr>
<td>Hosts for Hardware Island 1</td>
<td>Select hosts to be assigned to distributed resource scheduler (DRS) groups for hardware island 1.</td>
</tr>
<tr>
<td>Hosts for Hardware Island 2</td>
<td>Select hosts to be assigned to DRS groups for hardware island 2.</td>
</tr>
</tbody>
</table>

2. Click **Next** to review and then click **Submit**.

Onboard an EMC RecoverPoint for VMs cluster

Prerequisites

- Two vCenters must exist.
- Both vCenters must be added to the vRealize Orchestrator vCenter plug-in.
- When vCenters are added to the object model, they must be associated with different sites.
- Two hardware islands must exist.
- The cluster must exist in each vCenter.
- Cluster names must be unique.
- The clusters must not be present in the object model.

Figure 27 shows the required steps to onboard an EMC RecoverPoint for VMs cluster.

Figure 27. Onboard RP4VM cluster flowchart
Catalog item description

To onboard an EMC RecoverPoint for VMs cluster:

1. Select **Onboard Local Cluster** and click **Next**.

   **Note:** Enterprise Hybrid Cloud EMC RecoverPoint for VMs protection service is enabled on virtual machines that reside on local clusters at each physical site

Table 26 describes the EMC RecoverPoint for VMs cluster on-boarding parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Island</td>
<td>Select the primary hardware island.</td>
</tr>
<tr>
<td>Cluster</td>
<td>Select the primary local cluster.</td>
</tr>
<tr>
<td>Partner Hardware Island</td>
<td>Select the partner hardware island.</td>
</tr>
<tr>
<td>Partner cluster</td>
<td>Select the partner cluster.</td>
</tr>
</tbody>
</table>

1. Click **Next** to review and then click **Submit**.

Onboard a VMware SRM DR cluster

**Prerequisites**

- Two vCenters must exist.
- Both vCenters must be added to the vRealize Orchestrator vCenter plug-in.
- When vCenters are added to the object model, they must be associated with different sites.
- Two hardware islands must exist.
- The cluster must exist in each vCenter.
- Cluster names must be unique.
- The cluster must not be present in the object model.
Figure 28 shows the required steps to onboard a VMware SRM DR cluster.

Figure 28. Onboard a VMware SRM DR cluster flowchart

**Catalog item description**

To onboard a VMware SRM DR cluster:

1. Select **Onboard DR Cluster** and then click **Next**.
   
   Table 27 describes the DR cluster on-boarding parameters.
   
   **Table 27. DR cluster on-boarding parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protected Hardware Island</td>
<td>Select the protected hardware island.</td>
</tr>
<tr>
<td>Protected cluster</td>
<td>Select the protected cluster.</td>
</tr>
<tr>
<td>Recovery Hardware Island</td>
<td>Select the recovery hardware island.</td>
</tr>
<tr>
<td>Recovery cluster</td>
<td>Select the recovery cluster.</td>
</tr>
</tbody>
</table>

2. Click **Next** to review and then click **Submit**.

**Edit a cluster**

Table 28 describes the edit cluster parameters that are available for edit.

**Table 28. Edit cluster parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select cluster</td>
<td>Select the cluster to edit.</td>
</tr>
<tr>
<td>Select new site</td>
<td>Edit this parameter only if there are no virtual machines or datastores associated with the cluster. Changing a site implies a change of hardware island in the same vCenter, but a different site. Site affinity groups might need manual remediation.</td>
</tr>
<tr>
<td>Select new hardware island</td>
<td>Edit this parameter only if there are no virtual machines or datastores associated with the cluster. Changing hardware island implies a change to a hardware island in the same vCenter and the same site. Site affinity groups may need manual remediation.</td>
</tr>
</tbody>
</table>
Delete a cluster

Delete clusters from the Enterprise Hybrid Cloud object model only if there are no dependent datastores associated with that cluster.

**Note:** This action is irrevocable and must not be performed unless all virtual machines and datastores have been removed from the cluster.

Table 29 describes the available parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Cluster Name</td>
<td>Select a vSphere cluster.</td>
</tr>
<tr>
<td>Confirm</td>
<td>Select Confirm or Deny, as required.</td>
</tr>
</tbody>
</table>

Remove a VMware ESXi host from a cluster

Before removing a VMware ESXi host from an Enterprise Hybrid Cloud tenant cluster, be aware of the impact in ViPR. Also, remove the host from the ViPR export group to ensure that the correct datastores are mounted.

**SMI-S Version**

Ensure that the version of SMI-S complies with the version stated in the Enterprise Hybrid Cloud ESSM.

**Remove a host from a ViPR Export Group**

The following steps show the procedure for removing a host from a vSphere ESXi cluster in vCenter and using the ViPR command line interface (CLI) to remove the same host from the cluster Export Group.

Ensure that **Auto-Exports** is disabled for all clusters in ViPR; otherwise the host removal and add process shown below will fail:

1. Log in to the ViPR user interface (UI) as a user with administrative permissions (for example, ehc_vipr_admin).
2. Navigate to **Physical > Clusters**, click the cluster name, and then deselect **Auto-Exports**, as shown in Figure 29.

![Edit Cluster](image)

**Figure 29. Disable Auto-Exports**
Remove ESXi host from a vCenter cluster

1. Log in to vCenter as a user with vCenter administrator permissions (for example, ehc_vc_admin).

2. Right click the ESXi host that you plan to remove from the cluster and select **Enter Maintenance Mode**, as shown in Figure 30.

![Figure 30. Enter maintenance mode](image)

3. Move the host out of the source cluster and into the target cluster, as shown in Figure 31.

![Figure 31. Move ESXi host](image)

4. Right-click the ViPR-provisioned datastores associated with the host that you moved (drm-esxi084.infra.lab.local in this example). To remove the datastores, select **Unmount**, as shown in Figure 32, and then **Detach**, as shown in Figure 33.

![Figure 32. Unmount ViPR-provisioned datastores](image)
Chapter 3: Environment Configuration

Figure 33. Detach datastores

Rediscover vCenter server from the ViPR interface

1. Log in to the ViPR UI as a user with administrative permissions (for example, ehc_vipr_admin).
2. Navigate to Physical > vCenters. Select the relevant vCenter and click Rediscover, as shown in Figure 34.

Figure 34. Rediscover vCenter

Edit the ViPR profile to enable CLI functionality

1. Connect to ViPR using Secure Shell (SSH) and log in as root.
2. Navigate to /opt/storageos/cli/ and run the following command to edit the profile:
   vi viprcli.profile
3. Set `VIPR_HOSTNAME` to the ViPR FQDN and ensure `VIPR_PORT` is set to 4443, as shown in Figure 35.

```
# Set ViPR_HOSTNAME to the FQDN
VIPR_HOSTNAME=vipr1.ppssilver.lab.local

# Set VIPR_PORT to 4443
VIPR_PORT=4443
```

Figure 35. Edit ViPR.Profile

4. Save the changes and exit vi.

**Authenticate with ViPR to use CLI mode**

1. Change directory to `/opt/storageos/cli/bin/` and run the `. /viprcli authenticate –u root –d /tmp` authentication command, as shown in Figure 36.

```
viprcli: /opt/storageos/cli/bin/
VIPR_CLI_INSTALL_DIR=/opt/storageos/cli
VIPR_PORT=4443
```

Figure 36. Authenticate command

2. Run the `. /viprcli exportgroup remove_host -n OldExportGroupName -h1 ESXi-Hostname -pr Project host removal` command, as shown in Figure 37:

```
viprcli: /opt/storageos/cli/bin/ 
viprcli: /opt/storageos/cli/bin # ./viprcli exportgroup remove_host -n EMCWorkload01 -h1 dsm-esx1084.infra.lab.local -pr ehc
```

Figure 37. Remove host command
3. Navigate to Resources > Tasks to monitor the task’s progress from the ViPR UI, as shown in Figure 38.

![Figure 38. Task status](image)

**Update vRealize Automation compute resources**

1. Log in into the vRealize Automation Enterprise Hybrid Cloud tenant as a user with fabric admin privileges (for example, ehc_fabric_admin).
2. Navigate to Infrastructure > Compute Resources > Compute Resources.
3. Move the mouse over the relevant Compute Resource (EHCWorkload01 in this example) and select Data Collection, as shown in Figure 39.
4. Click Request now under Inventory.

![Figure 39. Data Collection](image)
Chapter 3: Environment Configuration

Add ESXi Host to a ViPR Export Group

Perform a rediscovery of vCenter server from the ViPR interface.

1. Log in to the ViPR UI as a user with administrative permissions (for example, ehc_vipr_admin).
2. Navigate to Physical > vCenters, select the relevant vCenter, and click Rediscover, as shown in Figure 40.

![Figure 40. Rediscover vCenter](image)

3. Connect to ViPR using SSH and log in as root.
4. Navigate to /opt/storageos/cli/bin and run the ./viprcli exportgroup add_host -n NewExportGroupName -hl ESXi-Hostname -pr Project command, as shown in Figure 41:

```bash
./viprcli exportgroup add_host -n "EHC Management" -hl ovrl-esxi1084.infra.lab.local -pr ch
```

![Figure 41. Add Host](image)

**Note:** This step adds the ESXi host to the new target Export Group in ViPR, with associated zoning, masking, and LUN provisioning tasks being executed.

5. Navigate to Resources > Tasks to monitor the task’s progress from the ViPR UI, as shown in Figure 42.

![Figure 42. Task Status](image)
Update vRealize Automation compute resources

1. Log in into the vRealize Automation Enterprise Hybrid Cloud tenant as a user with fabric admin privileges (for example, ehc_fabric_admin).

2. Navigate to Infrastructure > Compute Resources > Compute Resources.

3. Move the mouse over the relevant Compute Resource (EHCWorkload01 in this example) and select Data Collection, as shown in Figure 43.

![Image](image.png)

Figure 43. Data Collection

4. Click Request now under Inventory.

Managing datastores

Datastore objects are created in the Enterprise Hybrid Cloud object model when STaaS workflows perform a storage provisioning operation against an on-boarded Enterprise Hybrid Cloud cluster. The cluster type guides you to provision only suitable storage to that cluster.

**Add a datastore**

Run the Provision Cloud Storage catalog item to add new datastores. See Storage provisioning services for more information.

**Edit a datastore**

Editing datastores is not supported.

**Delete a datastore**

This catalog item deletes a datastore object from the Enterprise Hybrid Cloud object model. Table 30 describes the parameter that is available.

**Prerequisites**

The datastore must be empty.
Catalog item description

**Note:** Deletion of the physical datastore is a manual task.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Datastore</td>
<td>Select the datastore to be deleted from the object model.</td>
</tr>
</tbody>
</table>
This chapter presents the following topics:

- **Overview** ............................................................................................................ 52
- **Storage provisioning services** ......................................................................... 52
- **Creating resource reservations** ....................................................................... 53
- **Storage as a Service** ......................................................................................... 55
- **Assigning storage to business group reservations** ........................................ 63
Overview

This chapter describes the storage services and the virtual machine lifecycle and networking services available with Enterprise Hybrid Cloud. These services and the associated use cases fall into the following categories:

- Storage provisioning services
- Virtual machine services
- Advanced networking services
- Public cloud services

This chapter focuses on the configuration and provisioning of storage and virtual machine blueprints, as well as the provisioning of virtual machines with data protection services.

Storage provisioning services

Overview

Storage is provisioned, allocated, and consumed by different cloud users in Enterprise Hybrid Cloud:

- **Storage administrators** provision storage resources for consumption by other cloud users, using the storage services that are provided in the vRealize Automation service catalog.

  The storage administrator selects **Provision Cloud Storage** under **Storage Services** in the vRealize Automation service catalog. This catalog item works dynamically with ViPR software-defined storage to discover the available storage, based on the administrator’s selections through the deployment wizard, and provides the ability to provision the following storage:
  - Block (EMC VNX™, EMC VMAX™, EMC XtremIO™, EMC ScaleIO™)
  - File (VNX)
  - Highly available (with EMC VPLEX™)
  - Replicated (with EMC RecoverPoint)

- **vRealize Automation fabric group administrators** assign the provisioned storage resources to business groups.

- **Business group managers** define virtual machine storage when they create virtual machine blueprints with storage reservation policies.

- **End users** can, depending on their entitlements, choose the storage service level when they provision their virtual machines.

Note: Storage provisioning services are not available on a VxRail Appliance because it is based on fully pre-provisioned vSAN storage.

Cloud roles and personas

For the purposes of this guide, a storage administrator executes the storage services in the vRealize Automation service catalog. In production environments, use vRealize Automation entitlements to assign these services to other cloud administrators or users as required.
Creating resource reservations

Resource reservations are created to allocate provisioning resources in the fabric group to a specific business group. Resource reservations allow sharing of compute resources.

To create a resource reservation, as shown in Figure 44:

1. Log in as a user with vRealize Automation infrastructure administrator privileges (for example, ehc_fabric_admin).
2. Select Infrastructure > Reservations > Reservations.
3. Select New > vSphere.
4. Enter a descriptive Name.
5. Select the appropriate vRA Tenant.
6. Select the appropriate Business Group.
7. Set the Priority.
8. Click Resources.
9. Select the relevant compute resource.
10. Allocate the required amount of memory and storage, as shown in Figure 45.
Chapter 4: Storage Services

New Reservation - vSphere
Create a reservation to allocate provisioning resources to a business group in a tenant. You also can copy an existing reservation as a starting point.

Figure 45. New Reservation: Resources

11. Click Network, select the relevant network path and, if applicable, network profile, as shown in Figure 46. If NSX is part of the solution, you can also select advanced settings such as Transport Zones and Security groups.

Figure 46. New Reservation: Network

12. Click OK.

When the request succeeds, the new reservation is created and associated with the business group. View the properties in vRealize Automation under Infrastructure > Resources.
Storage as a Service

Set boot LUN HLU (SAN boot only)

Enterprise Hybrid Cloud can reserve LUN IDs for use by SAN boot hosts. By default no LUN IDs are reserved, but this is configurable and allows for multiple exclusions by setting the global option. See Reserve HLUs for SAN boot for more details.

Note: When enabled, all LUN IDs specified are excluded from use by ViPR when you are provisioning to system-wide tenant resource pods.

Provision local storage

Prerequisites

- The vCenter must exist.
- The vCenter must be added to the vRealize Orchestrator vCenter plug-in.
- The cluster must exist.
- The cluster must be present in the object mode.

Figure 47 shows the required steps to provision local storage.

![Provision local storage flowchart](image)

Catalog item description

An Enterprise Hybrid Cloud storage administrator can provision ViPR software-defined storage from the vRealize Automation self-service portal by selecting the Provision Cloud Storage item from the service catalog, as shown in Figure 48.
Chapter 4: Storage Services

Figure 48. Provision Cloud Storage catalog item

The request to provision cloud storage requires the following inputs:

- Request information
- User authentication
- vCenter cluster
- Hardware island
- Storage type: VMFS or NFS
- Storage tier
- Datastore size

The storage administrator selects most of these inputs from lists of items that are determined by the cluster resources available through vCenter and the virtual pools available in ViPR.

User authentication

Under Authentication, the requestor of this service provides their vRealize Automation password, which is required to authenticate the request into ViPR during the storage provisioning process. The user may optionally include a reason for the request, which might be required if the request is subject to an approval. To provision storage using this workflow requires the ViPR System Monitor role in ViPR.
**vCenter Cluster**

The **vCenter Cluster** tab displays the **Choose vCenter cluster** option, as shown in Figure 49.

<table>
<thead>
<tr>
<th>New Request</th>
<th>Request Information</th>
<th>Authentication</th>
<th>vCenter Cluster</th>
<th>Hardware Island</th>
<th>Storage Type</th>
<th>Storage Tier</th>
<th>Datastore Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provision Cloud Storage</td>
<td>Allow users to create a datastore</td>
<td>Choose vCenter cluster to which the storage tier will be made available.</td>
<td>VMware vCenter Server might be managing multiple tenant pod clusters; therefore, the storage administrator must select the correct vCenter cluster to instruct the provisioning operation where to assign the storage device.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Hardware Island**

Under **Hardware Island**, the storage administrator selects the relevant hardware island.

**Storage Type**

Under **Storage Type**, the storage administrator selects which type of datastore is required, based on the storage types detected in the underlying ViPR pools, as shown in Figure 50.

<table>
<thead>
<tr>
<th>New Request</th>
<th>Request Information</th>
<th>Authentication</th>
<th>vCenter Cluster</th>
<th>Hardware Island</th>
<th>Storage Type</th>
<th>Storage Tier</th>
<th>Datastore Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provision Cloud Storage</td>
<td>Allow users to create a datastore</td>
<td>Choose datastore type</td>
<td>A VMFS datastore type requires block storage, while NFS requires file storage. Other data services, such as DR and CA, are displayed only if they are detected in the underlying infrastructure.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Storage Tier**

Under **Storage Tier**, the storage administrator selects the storage tier from which the new storage device should be provisioned. The list of available tiers reflects the virtual pools available from the ViPR virtual array. Virtual pools can consist of XtremIO, ScaleIO, VNX, VMAX, or VPLEX storage types.
The available capacity of the virtual pool is also displayed, as shown in Figure 51.

Figure 51. Provision Cloud Storage request: Selecting the ViPR storage pool

**Datastore size**
Under **Datastore Size**, the storage administrator enters the required storage size, in GB, as shown in Figure 52.

Figure 52. Provision Cloud Storage request: Specifying the storage size

**Additional automated tasks**
The storage provisioning task includes values that are dynamically assigned by the workflows, such as the LUN and datastore name. Therefore, fields are not provided to capture those values. The orchestration logic manages these values to ensure consistency.

The workflow automates the vRealize Automation rediscovery of resources under the vCenter endpoint, in addition to assigning a storage reservation policy to the new datastore. If a matching storage reservation policy does not exist, it is created as part of the process. An email notifies the fabric group administrator that the storage is ready and available in vRealize Automation. The vRealize Automation fabric group administrator must manually reserve the new storage for use by a business group, as shown in Figure 53. See Assigning storage to business group reservations for more information.

Figure 53. Storage reservation for vRealize Automation business group
### Prerequisites

- The vCenter must exist.
- The vCenter must be added to the vRealize Orchestrator vCenter plug-in.
- VPLEX must be configured.
- The cluster must exist.
- The cluster must be present in the object model.
- The ViPR virtual array must exist.

Figure 54 shows the required steps to provision CA protected storage.

**Figure 54. Provision CA storage flowchart**

### Catalog item description

The storage provisioning process for CA environments differs slightly from the process for a single site. The selection of the hardware island, as shown in Figure 55, determines which hardware island will be the winning site in the event of a site failure. It also determines the site affinity of the virtual machines deployed onto the storage.

After selecting the hardware island, you are presented with the **Choose vCenter cluster** option, as shown in Figure 56. Select the correct CA-enabled vCenter cluster to instruct the provisioning operation where to assign the storage device.
Chapter 4: Storage Services

In this example, the vCenter cluster was configured with descriptive tags during implementation, making it easy to identify the CA-enabled vCenter cluster. The selected cluster is a single site CA cluster in New York.

**Storage type**

When you choose a CA-enabled vCenter cluster, **Storage Type** is filtered to CA-enabled storage. In this case, only **VMFS CA-Enabled** is applicable, as shown in Figure 57.

In this example, a single ViPR virtual pool, based on VPLEX Metro™, from which to provision storage is available. That pool, along with its available capacity, is displayed under **Storage Tier**, as shown in Figure 58.

You can then enter the required datastore size and, when provisioning is complete, continue to configure the appropriate business group reservations. See **Assigning storage to business group reservations** for more information.

### Prerequisites

- Two vCenters must exist.
- Both vCenters must be added to the vRealize Orchestrator vCenter plug-in.
- When vCenters are added to the object model, they must be associated with different sites.
Chapter 4: Storage Services

- Two hardware islands must exist (one per site).
- The clusters must exist in vCenter.
- The clusters must be present in the object model.
- The ViPR virtual array must exist for each site.
- The VMware SRM recovery group is created and contains both clusters.

Figure 59 shows the required steps to provision DR-protected storage.

![Provision DR-protected storage flowchart](image)

Figure 59. Provision DR-protected storage flowchart

**Catalog item description**

The storage provisioning process for DR environments is slightly different from the process for a single site.

After selecting a provisioning site, the storage administrator is presented with the **Choose vCenter Cluster** option, as shown in Figure 60, which displays only clusters on the selected provisioning site. The storage administrator must select a DR-enabled cluster as the target to provision the DR-protected storage.

![Selecting the DR-protected Tenant Pod (vCenter cluster)](image)

Figure 60. Selecting the DR-protected Tenant Pod (vCenter cluster)

The **Storage Type** option lists the types of datastores that are available for provisioning, based on the type of storage in the underlying infrastructure. If the selected Tenant Pod is
configured for DR services, then only DR-enabled VMFS storage is presented as an available option, as shown in Figure 61.

![Figure 61. Provision Cloud Storage request: Selecting the required storage type](image)

The storage administrator then selects the storage tier offering from which the new datastore is to be provisioned. To expose the underlying recovery point objective (RPO) to the storage administrator, make sure the ViPR pool includes the RPO in its name, as shown in Figure 62.

Each tier of DR-enabled storage has a predetermined RPO. The storage administrator selects a tier that supports the RPO required for the storage that is being provisioned.

![Figure 62. Provision Cloud Storage request: Selecting the storage tier and RPO](image)

The storage administrator can then enter the required datastore size. The newly provisioned storage is then automatically associated with the corresponding SRP, as shown in Figure 63.

![Figure 63. ViPR storage tiers and corresponding vRealize Automation reservation policies](image)
**Automatic addition of the new datastore to a protection group**

When the new datastore is provisioned, the workflow creates a corresponding protection group and adds the newly created datastore to that protection group. The workflow then adds the protection group to the recovery plan that corresponds to the compute cluster where the storage is provisioned, as shown in Figure 64. These steps ensure that any virtual machines provisioned on the storage are replicated to the recovery site and are protected.

**Rescan arrays to detect configuration changes**

By default, Site Recovery Manager checks arrays for changes to device configurations by rescanning arrays every 24 hours. However, you can force an array rescan at any time.

You can reconfigure the frequency with which Site Recovery Manager performs regular array scans by changing the `storage.minDsGroupComputationInterval` option in Advanced Settings. See Site Recovery Manager Administration for more information.

---

Before adding a newly provisioned datastore to a vRealize Automation reservation, ensure that the datastore has been discovered by VMware Site Recovery Manager.

**Note:** if provisioning multiple DS, it is recommended to wait until the last datastore has completed deploying before performing the SRA rediscovery.

---

**Assigning storage to business group reservations**

After the newly provisioned storage is protected, the vRealize Automation fabric administrator can configure reservations on the storage for the appropriate business group.

**Set the virtual machine storage policy**

Business group managers can set the storage policy for a virtual machine and, if appropriate, allow end users to view and change the policy.

Business group managers set the storage type for the virtual machine disks when they create a virtual machine blueprint by applying the appropriate storage reservation policy to each of the virtual disks, as shown in Figure 65.
When the storage reservation policy is set, the blueprint always deploys the virtual machine and its virtual disks to the specified storage type.

To enable more user control at deployment time, the business group manager can select the **Allow users to see and change storage reservation policies** option, which permits business group users to reconfigure the storage reservation policies at deployment time.
Chapter 5 Virtual Machine Lifecycle

This chapter presents the following topics:

Virtual machine lifecycle .............................................................................................. 66
Continuous availability .................................................................................................. 71
VMware Site Recovery Manager disaster recovery ..................................................... 72
EMC RecoverPoint for Virtual Machines ..................................................................... 76
Virtual machine encryption ......................................................................................... 83
Public cloud services .................................................................................................. 95
Onboarding a VxRail endpoint .....................................................................................104
Virtual machine lifecycle

This section provides an overview of some of the more common tasks in the lifecycle of virtual machines in Enterprise Hybrid Cloud.

Virtual machine blueprints

A blueprint must be created for a virtual machine before the machine can be provisioned from the vRealize Automation service catalog. A blueprint contains the complete specification for a virtual machine, defining the machine’s attributes, policy, and management settings—including any approvals required, expiration date, and owner operations—and the manner in which the machine is provisioned.

When users provision a machine using the self-service portal, the machine is provisioned according to the specifications of the associated blueprint.

Blueprints can be single-machine or multi-machine and can include multitier enterprise applications that require multiple components (application, database, and web). A multi-machine blueprint contains multiple individual machine blueprints.

Provision a virtual machine

When a virtual machine is provisioned, it is deployed from a vSphere virtual machine template and customized within a vRealize Automation virtual machine blueprint.

Tenant administrators can create a global blueprint, which can be made available to all business groups, or a local blueprint, which is available only to a single business group. Business group managers can create blueprints for only the business groups for which they are responsible.

Prerequisites

- The vCenter must exist.
- The vCenter must be added to the vRealize Orchestrator vCenter plug-in.
- The virtual machine template must exist in vCenter.

Figure 66 shows the required steps to provision a virtual machine.
Creating a local blueprint

To create a virtual machine blueprint in the vRealize Automation console:

1. Log in as a user with vRealize Automation tenant administrator or business group manager privileges.
2. Select Design > Blueprints.
4. In the New Blueprint window, provide the required information under the following tabs:
   - General
   - NSX Settings
   - Properties

   Each tab contains input fields that combine to define the final blueprint.

5. Click OK.

Design Canvas

The design canvas enables you to define and customize the new blueprint properties:

1. Under Categories, click Machine Types.
2. Select vSphere Machine and then drag it to the design canvas to customize it, as shown in Figure 67.
Figure 67. Creating a virtual machine blueprint

**Build Information**

Under **Build Information**, the blueprint type is **Server** and the action is **Clone**, which means that virtual machines deployed from this blueprint leverage an existing template in vSphere. You can select the required template from the **Clone from** list, as shown in Figure 68.
The virtual machine inherits the minimum required resources that are defined within the virtual machine template. You can set the blueprint to allow these values to be increased to the maximum value at a later time. Figure 69 shows how to set the maximum values for the machine resources and specify the storage service level (Storage Reservation Policy) to be used.

Properties

The Properties tab can contain build profiles that consist of a set of properties that you can apply to a machine when it is provisioned.

You can publish the virtual machine blueprint and, using vRealize Automation service entitlements, make it available to end users as a catalog item in their self-service portal, as shown in Figure 70.
Chapter 5: Virtual Machine Lifecycle

Figure 70. Deploying a new virtual machine blueprint from the self-service portal

To provision the virtual machine, you can request the virtual machine from the service catalog, as shown in Figure 71.

Figure 71. Specifying request information for a virtual machine

The request process can require user input to confirm the number of virtual machines to be provisioned and any increases in CPU, memory, and storage. The blueprint controls these settings, which can be configured as required.

Figure 72 shows how to select the storage service level for the virtual machine by selecting the corresponding vRealize Automation storage reservation policy.

Figure 72. Selecting the storage reservation policy for a virtual machine

Click Submit after the virtual machine is configured to initiate the provisioning process, which can be viewed under the Requests tab.

You can configure the provisioning process to include approval operations, either with vRealize Automation or with integrated third-party approval or ticketing systems.
Chapter 5: Virtual Machine Lifecycle

When the provisioning process is complete, you can access the virtual machine from the Items menu in the vRealize Automation console.

Continuous availability

Provision a CA protected virtual machine

**Prerequisites**
- The vCenter must exist.
- The vCenter must be added to the vRealize Orchestrator vCenter plug-in.
- VPLEX must be configured.
- The cluster must exist.
- The cluster must be present in the object model.
- The ViPR virtual array must exist.
- The virtual machine template must exist.

Figure 73 shows the required steps to provision a CA-protected virtual machine.

![Figure 73. Provision CA-protected virtual machine flowchart](image)

**Single site CA**

In a CA configuration, the preferred hardware island is selected during storage provisioning. See Provision CA protected storage for more information.

**Note:** In the case of single-site CA, both hardware islands reside on the same geographical site.

Users can also set the preferred hardware island during virtual machine deployment, if the option to do so has been enabled by the administrator, by choosing a storage reservation policy in vRealize Automation during virtual machine deployment.
Chapter 5: Virtual Machine Lifecycle

Setting a preferred hardware island during virtual machine deployment

**Note:** The following example is applicable when a user is permitted to select the storage reservation policy for the virtual machine at deployment time. The virtual machine storage reservation policy can also be set and locked in the virtual machine blueprint, in which case the virtual machine always has its preferred hardware island set to the hardware island specified in the policy.

Figure 74 shows how a user sets site affinity by selecting a storage reservation policy when deploying a virtual machine.

![Figure 74. Selecting a storage reservation policy and determining site affinity while deploying a virtual machine](image)

As part of the deployment process, the virtual machine is added to the vSphere host affinity group for the selected site.

VMware Site Recovery Manager disaster recovery

**Site mappings**

To support SRM-based DR protection, the SRM configuration must include resource mappings for resource pools, folders and network objects between the vCenter Server instance on the protected site and the vCenter Server instance on the recovery site.

These mappings enable you to define automated recovery plans to fail over application workloads between the sites according to defined recovery time objectives (RTOs) and recovery point objectives (RPOs). Configure the settings on both the protected and recovery sites to support application workload recovery between the two sites.

**Note:** When failover occurs with the SRM-based DR protection service, all Layer 3 networks associated with the protected cluster fail over entirely. Active machines in a specified Layer 3 network must reside only in the site with the "permit" route redistribution policy.

**Placeholder datastore**

A placeholder datastore must be accessible to the compute clusters that support the DR services. The placeholder datastore must be configured in SRM and must be associated with the compute clusters.

**Protection groups**

A protection group is the unit of failover in SRM. Enterprise Hybrid Cloud supports failover at a Workload Pod level.

In the context of the SRM-based DR protection, two Workload Pods are assigned to a DR cluster pair. One pod is at the primary site and is the protected cluster. The second pod is
at the alternate site and is the recovery cluster. All protection groups associated with a DR cluster pair and all the virtual machines running on a particular pod must fail over together.

With SRM-based DR protection, there is a 1:1 mapping between a DR cluster pair and a recovery plan. Each recovery plan contains one or more protection groups.

Each protection group contains a single replicated vSphere datastore, and all the virtual machines that are running on that datastore. When you deploy new virtual machines to a Workload Pod using vRealize Automation, Enterprise Hybrid Cloud lifecycle customizations automatically add them to the corresponding protection group so that they fail over successfully.

**Recovery plans**

Recovery plans enable administrators to automate the steps required for recovery between the primary and recovery sites. A recovery plan may include one or more protection groups.

You can test recovery plans to ensure that protected virtual machines recover correctly to the recovery site.

**Tenant Pod recovery plans**

The automated network reconvergence capabilities of SRM-based DR protection for Enterprise Hybrid Cloud eliminate the need to change the IP addresses of workload virtual machines when they fail over from one site to the other. Instead, the tenant networks move with the virtual machines and support virtual machine communication outside the network when on the recovery site.

When using VMware NSX, Enterprise Hybrid Cloud can automate network reconvergence of the tenant pods and, through a custom SRM step in the SRM recovery plan, ensure security policy compliance on the recovery site during a failover. However, running a test SRM recovery plan with NSX does not affect the production virtual machines. Because the network convergence automation step has the required built-in intelligence, it does not reconverge the networks in that scenario.

If non-NSX alternatives are used, then network reconvergence is not automated. The reconvergence must be performed manually during a pause in the SRM recovery plan or by an automated SRM task created as part of a professional services engagement.

---

**Note:** Create a recovery plan manually for each DR-enabled workload cluster before you execute any STaaS operations. There must be two recovery plans for a cluster pair to enable failover and failback.

**Automation pod recovery plans**

Network reconvergence of the network that supports the Enterprise Hybrid Cloud Automation Pod is a manual task regardless of the presence of VMware NSX.

---

**Note:** This behavior is the solution default. A professional services engagement provides automated network reconvergence for the Automation Pod.
Chapter 5: Virtual Machine Lifecycle

Provision an SRM DR-protected virtual machine

The vRealize Automation self-service portal supports the provisioning of virtual machines on storage that has SRM DR protection.

Prerequisites

- Two vCenters must exist.
- Both vCenters must be added to the vRealize Orchestrator vCenter plug-in.
- When vCenters are added to the object model, they must be associated with different sites.
- Two hardware islands must exist (one per site).
- The clusters must exist in vCenter.
- The clusters must be present in the object model.
- The ViPR virtual array must exist for each site.
- VMware SRM must be fully configured.

Figure 75 shows the required steps to provision a DR-protected virtual machine.

![DR-protected VM flowchart image]

Figure 75. Provision DR-protected VM flowchart

Users can protect their virtual machines at deployment time by selecting a storage reservation policy that includes SRM DR protection, as shown in Figure 76, which can be set and locked in the blueprint. A storage reservation policy can also be configured to allow users to modify it for DR protection as required.

![Assigning a storage reservation policy image]

Figure 76. Assigning a storage reservation policy

Selecting a storage reservation policy that has DR protection ensures that the virtual machine is deployed on storage that is being replicated to the recovery site with the
required RPO. To restrict provisioning of machines to a subset of available reservations such as a DR protected cluster, you can also apply a reservation policy to the blueprint.

**Protecting virtual machines with VMware vCenter SRM**

As shown in Figure 77, the new virtual machine is deployed on the protected vSphere cluster and datastore that provide DR protection. The virtual machine is automatically added to the SRM protection group associated with the datastore and included in any recovery plans that include the protection group.

![Figure 77. Virtual machine summary displaying the protected site](image)

**Placeholder virtual machine on the recovery site**

As part of the protection process, a placeholder virtual machine that corresponds to the deployed source virtual machine is provisioned on the recovery site, as shown in Figure 78. The placeholder virtual machine maintains the configuration properties of the source virtual machine—for example, compute resources, folder, network, and security group.

![Figure 78. Placeholder virtual machine summary on the recovery site](image)

When a recovery plan is executed, meaning that the source virtual machine is recovered on the DR site, the source virtual machine properties are retained on the recovered virtual machine.

**Enabling virtual machine restart priority for recovery**

The creator of the virtual machine blueprint can set the order, or priority, in which SRM restarts virtual machines on the recovery site.
To enable this option, select the **SRM Power On Priority Option** build profile on the **Properties** tab of the virtual machine blueprint.

**EMC RecoverPoint for Virtual Machines**

**Provision an EMC RecoverPoint for Virtual Machines protected virtual machine**

In a dual-site/dual vCenter environment, EMC RecoverPoint for Virtual Machines provides DR for the virtual machines hosted on a vSphere environment. This section describes how to set up a replication policy, subscribe to the replication policy, and make changes to replication policy of virtual machines.

**Create a replication policy**

The EMC RecoverPoint for Virtual Machines administrator creates various replication policies based on the RPO. Users can subscribe to policies based on their RPO need.

1. Log in to the EHC Portal with the entitled user for Create an RP4VM Policy advanced service blueprint (for example, ehc_config_admin@domain.local).

2. Under Create an RP4VM Policy, click **Request** as shown in Figure 79.

   ![Figure 79. Create an RP4VM Policy catalog item](image)

3. Provide a description for the request and click **Next**, as shown in Figure 80.

   ![Figure 80. Create an RP4VM request information](image)
4. Select the replication type. For asynchronous replication, provide a policy name, journal size, and RPO information, as shown in Figure 81.

![Figure 81. Create an RP4VM policy replication information](image)

5. For synchronous replication, provide a policy name and journal size, as shown in Figure 82.

![Figure 82. Create an RP4VM policy name](image)

6. Click Submit.

**Replication policy subscription**

This section describes how to subscribe to an EMC RecoverPoint for Virtual Machines replication policy during the virtual machine provisioning as well as Day 2 operation for any existing machines.

The vRealize Automation blueprint administrator must apply the EMC RecoverPoint for Virtual Machines build profile to a blueprint to enable EMC RecoverPoint for Virtual Machines protection of virtual machines at provisioning time. Figure 83 shows the build profile.
When users request a virtual machine from an EMC RecoverPoint for Virtual Machines enabled blueprint, they are prompted for the following additional information, as shown in Figure 84:

- Power-on priority of the virtual machine
- Whether to create a new consistency group (CG) for the virtual machine or reuse an existing CG
- Replication policy, which lists the policies created by the administrator
Note: When a VM fails over, the source blueprint cannot be modified and VM resources cannot be changed outside the original parameters of the blueprint.

Protect an existing virtual machine with EMC RecoverPoint for Virtual Machines

To protect an existing virtual machine with EMC RecoverPoint for Virtual Machines, navigate to the Items tab in vRealize Automation. Select the virtual machine you want to protect and then select RP4VM Protect VM from the Actions list box, as shown in Figure 85.

You are presented with the option to create a new CG or to use an existing CG. When you create a new CG, the group name is auto populated with the virtual machine name and provides a list from which to select the replication policy for the CG, as shown in Figure 86.

If you choose to use an existing CG, the form refreshes and provides an option to select an existing CG, as shown in Figure 87.
If there are multiple virtual machines in the CG, the boot sequence defines the order of power-on. For example, 1 is first to power on and 5 is the last to power on. The default is 3. Refer to the EMC RecoverPoint for Virtual Machines Product Guide for more information.

**Change a consistency group**

A consistency group (CG) allows a set of virtual machines to recover in a consistent state and is the unit of failover with EMC RecoverPoint for Virtual Machines.

To move a virtual machine from one CG to another:

1. Log in to the vRealize Automation portal with a username that has an entitlement to the **RP4VM Change CG** resource action.
2. Under **Items**, select the virtual machine for which you would like to change the CG. Then click the **Actions** menu and select **RP4VM Change CG**, as shown in Figure 88.
3. Select an existing CG or select the option to create a new one, as shown in Figure 89. Enter the details and click **Submit**.

**Figure 89. Consistency group selection**

**Change Power-On Priority**

Power-On Priority of a CG specifies the power-on order of virtual machines in the CG. Power-on priority is by ascending order. Virtual machines with priority 1 power on first.

To modify power-on priority of a virtual machine:

1. Select the virtual machine from the **Items** tab. Select the **RP4VM Change Boot Sequence Option** from the **Actions** menu, as shown in Figure 90.

**Figure 90. RP4Vm Change Boot Sequence Action**

2. Select a new boot sequence from the list box, as shown in Figure 91.
Delete a replication policy

When a replication policy is no longer required, it can be removed. Removing the replication policy does not affect existing consistency groups that use the policy. You remove the replication policy from the vRealize Orchestrator inventory and also from the property dictionary.

To delete a replication policy:

1. Log in to the vRealize Automation portal as a user that has an entitlement to the Delete an RP4VM Policy catalog item.
2. Click Request and select the policy to delete, as shown in Figure 92.
3. Click Submit.

Remove EMC RecoverPoint for Virtual Machines protection

When a virtual machine no longer requires replication, it can be unprotected to remove it from a CG. If it is the last virtual machine on the CG, the group also is removed.

1. Log in to the vRealize Automation portal as a user that has an entitlement to the RP4VM Unprotect VM resource action.
2. Under **Items**, select the virtual machine that you want to unprotect. From the **Actions** menu, select **RP4VM UnProtect VM**, as shown in Figure 93.

![Machines](image)

**Figure 93. RP4VM UnProtect VM**

*Note: This operation is irreversible and all the journal data will be lost.*

---

**Virtual machine encryption**

**Overview**

The Enterprise Hybrid Cloud Encryption module and EMC CloudLink™ SecureVM provide encryption for virtual machines. CloudLink SecureVM uses an agent that is installed in the virtual machine to control the native operating system’s encryption technologies. The encryption keys are stored within CloudLink Center. If the key release policies are met, the keys are returned to the virtual machine when requested. If the policies are not met, the key request is placed in a pending state and the request must be manually accepted or rejected.

**Add a CloudLink Center cluster**

Before a virtual machine can be encrypted, add a CloudLink Center cluster to Enterprise Hybrid Cloud. CloudLink Center might have been deployed when the initial Enterprise Hybrid Cloud deployment was built or deployed at a later time. If CloudLink Center was deployed at a later time, add it as follows:

1. Log in to vRealize Orchestrator client as the vRealize Orchestrator administrator.
2. Select the **Workflows** tab on the left navigation pane.
3. Select **Library > CloudLink SecureVM > Cluster Configuration > Add cluster**.
4. Click the **Start Workflow** icon.
5. Enter a unique name in the **Cluster unique name** field.
6. Enter the hostname or the IP address of one server in the CloudLink Center cluster in the **Cluster known server address** field. Only a single value is needed. Additional servers in the cluster are discovered automatically.
7. Enter the username and password of a client user in CloudLink Center in the **CloudLink Center user name** and **CloudLink Center password** fields. Client users in CloudLink Center are special users that represent a client application and are only allowed to use the CloudLink Center REST APIs.
When a CloudLink Center cluster is added, all existing SecureVM machine groups appear as encryption groups in Enterprise Hybrid Cloud. These groups can be restricted by configuring the encryption groups.

**Configure encryption groups**

When you encrypt a virtual machine, it is automatically registered in the SecureVM machine group associated with the encryption group. You can restrict the encryption groups to which a business group has access. For example, a specified business group might want all encrypted virtual machines to be associated with a specific SecureVM machine group.

To configure encryption groups:

1. Log in to the Enterprise Hybrid Cloud tenant portal as the system administrator with entitlements to the EHC Encryption catalog items (for example, ehc_encryption_admin@domain.local).
2. Go to Catalog > EHC Configuration and select Configure Encryption Groups.
3. Under Request Information, type a description, optionally type a reason, and click Next.
4. On the Configure Encryption Groups tab, select the business group in which to configure the encryption groups.
5. Select each encryption group that members of the business group can select when encrypting a virtual machine. The No Encryption group option lets the user provisioning a virtual machine to decide not to encrypt a virtual machine, even if the blueprint is enabled for encryption.
6. Click Next to review the request.
7. On the Review and Submit tab, ensure the selections are correct and click Submit.

**Bulk encryption status**

The Bulk Encryption Status catalog item generates and sends an email report of all virtual machines owned by a business group. The report lists if the SecureVM agent is installed and the encryption status for each volume in the virtual machine. You do not have to start the virtual machine. The report contains the encryption status of the volumes when the virtual machine was last running.

To generate the bulk encryption status report:

1. Log in to the Enterprise Hybrid Cloud tenant portal as the system administrator with entitlements to the EHC Encryption catalog items (for example, ehc_encryption_admin@domain.local).
2. Go to Catalog > EHC Configuration and select Bulk Encryption Status.
3. Under Request Information, type a description, optionally type a reason, and click Next.
4. On the Bulk Encryption Status tab, select the business group for which to generate the report.
5. The Encryption Report field shows the entire report.

**Note:** If this report does not provide enough information, click Cancel to dismiss the request without sending the email report.
Chapter 5: Virtual Machine Lifecycle

Add user entitlements to Enterprise Hybrid Cloud encryption resource actions

You can perform encryption on existing virtual machines when the correct entitlements are granted.

To update an entitlement:

1. Log in to the vRealize Automation tenant portal as the tenant administrator, for example, ehc_tenant_admin@domain.local.
2. From Administration, click Catalog Management and then select Entitlements.
3. Select the entitlement and click Edit.
4. From Items & Approvals, click Add for Entitled Actions.
5. Select the resource action you want and then click OK.
6. Click Update to save changes.

Show the encryption status of a virtual machine

To show the encryption status of a virtual machine:

1. Log in to the Enterprise Hybrid Cloud tenant portal as the system administrator with entitlements to the EHC Encryption resource actions (for example, ehc_encryption_admin@domain.local).
2. Select Items.
3. Select the virtual machine.
4. Select Encryption Status from Actions.
5. Under Request Information, type a description, optionally type a reason, and click Next.

The SecureVM Summary field shows the current encryption status of the virtual machine.

**Note**: If this is enough information, click Cancel to dismiss the request without sending the report by email.

6. Enter a valid SMTP email address in the Target Email field and click Next.
7. On the Review and Submit tab, review the Action and Target Email fields and click Submit to send the encryption status report by email.

Encrypt or decrypt a virtual machine’s volumes

To encrypt or decrypt a virtual machine’s volumes:

1. Log in to the Enterprise Hybrid Cloud tenant portal as the system administrator with entitlements to the EHC Encryption resource actions (for example, ehc_encryption_admin@domain.local).
2. Select Items.
3. Select the virtual machine.
4. Select Encrypt or Decrypt from Actions.
5. Under Request Information, type a description, optionally type a reason, and click Next.
6. Under Action Choice, select either Encrypt or Decrypt action and click Next.
7. On the Encrypt tab or Decrypt tab (depending on the action selected on the previous tab), check the Volumes To Encrypt field if encrypting an unencrypted volume or check the Volumes To Decrypt field if decrypting a volume.
8. Click Next to review the request.
9. On the Review and Submit tab, review the information and click Submit to implement the encryption.

Install or Uninstall SecureVM agent

To install or uninstall SecureVM agent to or from an existing virtual machine:

1. Log in to the Enterprise Hybrid Cloud tenant portal as the system administrator with entitlements to the EHC Encryption resource actions (for example, ehc_encryption_admin@domain.local).
2. Select Items.
3. Select the virtual machine.
4. Select Encrypt or Decrypt from Actions.
5. Under Request Information, type a description, optionally enter a reason and click Next.
6. Under Action Choice, select either Install SecureVM agent or Uninstall SecureVM and click Next.

   Note: If the SecureVM agent is not installed on the virtual machine, you can only select the Install SecureVM agent action. If the SecureVM agent is installed on the virtual machine, you can select one of three available actions: Encrypt, Decrypt, or Uninstall SecureVM.

7. On the Credentials tab, enter a username and password of the VM administrator account and click Next. The username and password are required to deploy the SecureVM agent into the virtual machine or to uninstall it.
8. If you are installing the SecureVM agent, on the Install SecureVM options tab select the encryption group and click Next.
9. On the Review and Submit tab, review the Action field and click Submit.

Accept or reject pending key releases

When the key release policies are not met, a key request is placed in a pending state.

To accept or reject a pending key release:

1. Log in to the Enterprise Hybrid Cloud tenant portal as the system administrator with entitlements to the EHC Encryption resource actions (for example, ehc_encryption_admin@domain.local).
2. Select **Items**.
3. Select the virtual machine.
4. Select **Accept or Reject Pending Key Release** from **Actions**.
5. Under **Request Information**, type a description, optionally enter a reason, and click **Next**.
6. Under **Action Choice**, choose **Accept** or **Reject** for the **Action** field, and click **Next**.

   **Note:** The virtual machine must be in a pending state.

7. On the **Review and Submit** tab, select **Submit**.

### Block or unblock a virtual machine

You can block a virtual machine when you do not want to release encryption keys for the virtual machine’s volumes.

To block or unblock a virtual machine:

1. Log in to the Enterprise Hybrid Cloud tenant portal as the system administrator with entitlements to the EHC Encryption resource actions (for example, ehc_encryption_admin@domain.local).
2. Select **Items**.
3. Select the virtual machine.
4. Select **Block or Unblock VM** from **Actions**.
5. Under **Request Information**, type a description, optionally type a reason, and click **Next**.
6. Under **Action Choice** tab, choose **Block** or **Unblock** for the **Action** field, and click **Next**.
7. On the **Review and Submit** tab, select **Submit**.

### Release the encryption license

When a virtual machine is encrypted, it uses a CloudLink SecureVM license. The license is automatically released when the virtual machine is decrypted. However, the license can be manually released if the virtual machine is powered off. When the virtual machine is powered on, it uses a CloudLink SecureVM license automatically.

To release the encryption license:

1. Log in to the Enterprise Hybrid Cloud tenant portal as the system administrator with entitlements to the EHC Encryption resource actions (for example, ehc_encryption_admin@domain.local).
2. Select **Items**.
3. Select the virtual machine.
4. Select **Release Encryption License** from **Actions**.
5. Under **Request Information**, type a description, optionally type a reason, and click **Next**.
6. On the **Release Encryption License** tab, review an **Action** field and click **Submit**.
Provision an encrypted virtual machine

Update a blueprint

A blueprint can specify that a virtual machine have encrypted volumes after provisioning. To encrypt a virtual machine, the Enterprise Hybrid Cloud encryption module is required and a CloudLink Center cluster must be added to the environment. See Add a CloudLink Center cluster for more information.

To update a virtual machine blueprint in the vRealize Automation console:

1. Log in as a user with vRealize Automation tenant administrator or business group manager privileges.
2. Select Design > Blueprints.
3. Select the blueprint to edit.
4. Select the vSphere machine to edit.
5. Select the Properties tab.
6. Click Add and then select CloudLink SecureVM Encryption in the Add Property Groups list.

Customize encryption properties in the blueprint

The CloudLink SecureVM Encryption property group contains four properties that control the encryption process. Some of these properties can be customized directly in the blueprint to lock down what you see during provisioning.

To force the use of a specific encryption group, set the blueprint properties as shown in Table 31.

Table 31. CloudLink SecureVM Encryption property group properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>com.emc.ehc.encryption.businessgroup</td>
<td>Clear Show in Request and type the name of the business group for the Value.</td>
</tr>
<tr>
<td>com.emc.ehc.encryption.group</td>
<td>Clear Show in Request and type the name of the encryption group for the Value.</td>
</tr>
</tbody>
</table>

To deploy the SecureVM agent in the virtual machine without prompting the user for a username and password, set the blueprint properties as shown in Table 32.

Table 32. CloudLink SecureVM Encryption build profile credential properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>com.emc.ehc.encryption.username</td>
<td>Clear Show in Request and type the username of the administrator account in the virtual machine for the Value.</td>
</tr>
<tr>
<td>com.emc.ehc.encryption.password</td>
<td>Clear Show in Request and type the password of the administrator account in the virtual machine for the Value. Encrypted must be cleared, otherwise the provisioning workflows have no access to the required clear password.</td>
</tr>
</tbody>
</table>
Select encryption options during provisioning

When requesting a virtual machine from an encryption-enabled blueprint, the user is prompted to supply the information described in Table 33.

Table 33. Encryption options during provisioning

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business group</td>
<td>List box with available business groups.</td>
</tr>
<tr>
<td>Encryption group</td>
<td>List box with available encryption groups based on the selected business group. Selecting the value <strong>No Encryption</strong> deploys the virtual machine without encrypting it.</td>
</tr>
<tr>
<td>VM administrator username</td>
<td>The username of the VM administrator account. The username is required to deploy the SecureVM agent into the virtual machine.</td>
</tr>
<tr>
<td>VM administrator password</td>
<td>The password of the VM administrator account. This is required to deploy the SecureVM agent into the virtual machine.</td>
</tr>
</tbody>
</table>

For environments that require existing virtual machines to be imported into the Enterprise Hybrid Cloud, the vRealize Automation bulk import feature enables the import of one or more virtual machines.

This functionality is available only to vRealize Automation users who have Fabric Administrator and Business Group Manager Privileges. The Bulk Import feature imports virtual machines complete with defining data such as reservation, storage path, blueprint, owner, and any custom properties.

The Enterprise Hybrid Cloud offers the ability to layer Enterprise Hybrid Cloud services onto pre-existing virtual machines by using the bulk import process. Before beginning the bulk import process, the following must be true:

- Target virtual machines are located in an Enterprise Hybrid Cloud vCenter endpoint.
  
  **Note:** This is not an additional IaaS-only vCenter endpoint if they are also present.
  
- Target virtual machines are on the correct vRealize Automation-managed compute resource cluster and that cluster is already onboarded as an Enterprise Hybrid Cloud cluster:
  - In cases where DR services are required for the target virtual machines, the machines are on a DR-enabled cluster.
  - In cases where data protection services are required for the target virtual machines, the machines are on a cluster that is associated with an Avamar pair.

- Target virtual machines are on the correct vRealize Automation-managed datastore:
  - In cases where DR services are required for the target virtual machines, they are on a datastore protected by EMC RecoverPoint.
  - In cases where data protection services are required for the target virtual machines, they are on a datastore that is registered with an Avamar grid.
Applying data protection backup services to imported virtual machines

To apply data protection backup services to newly imported virtual machines, first create a new blueprint with the **BackupAndRestoreForBulkImport** build profile.

This build profile is available after import of either of these Enterprise Hybrid Cloud modules:

- Data protection
- Disaster recovery

To import existing virtual machines, first generate a CSV file containing the virtual machines to be imported, and then edit the CSV file to specify the virtual machine reservation details.

**Virtual machine import procedure**

1. In the vRealize Automation portal, select **Infrastructure > Infrastructure Organizer > Bulk Imports**.

2. Under **Generate CSV File**, make the following selections, as shown in Figure 94:
   a. For virtual machines currently outside of vRealize Automation management, set **Machines** to **Unmanaged**.
   b. Select the relevant vRealize Automation **Business group**, and **Owner**, and the **Blueprint** created earlier.
      The associated virtual machine blueprint can be created specifically for the import or it can be an existing blueprint.

   **Note**: Ensure that virtual machine blueprint parameters are appropriate to incoming virtual machines and do not cause conflict. The parameters specified in the blueprint are assigned to virtual machines that are attached to the blueprint. Pay particular attention to lease and archive periods.

   c. At **Resource**, select either **EndPoint** (for example, vCenter) or **Compute Resource** (for example, vSphere cluster) to locate the virtual machines to be imported.

   d. At **Name**, depending on the resource type you have chosen, select an endpoint or vSphere cluster.
3. Click OK.

4. Edit the CSV file to specify the virtual machine reservation details, as shown in Figure 95.

![Generate CSV File](image)

**Figure 94. Generating the CSV file containing virtual machines to be imported**

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
<th>I</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Import–Yes or No</td>
<td>Virtual Machine Name</td>
<td>Virtual Machine ID</td>
<td>Host Reservation (Name or ID)</td>
<td>Host To Storage (Name or ID)</td>
<td>Blueprint (Name or ID)</td>
<td>Owner Name</td>
<td>Property Name</td>
</tr>
<tr>
<td>2</td>
<td>Yes</td>
<td>EXT-VAVS</td>
<td>bd52566fca-91-6b-36-01</td>
<td>vpx-01.5x-0.3.25</td>
<td>storage-02</td>
<td>storage-01</td>
<td><a href="mailto:devops_bg_admin@ppsliver.lab.local">devops_bg_admin@ppsliver.lab.local</a></td>
<td>epc.backup.servicelevels</td>
</tr>
</tbody>
</table>

**Figure 95. Editing the CSV file to match virtual machines and storage reservation policies**

All of the values for each machine must be present in the target vRealize Automation deployment for the import to succeed. To change the values for reservation, storage location, blueprint, and owner for each machine that you want to import, edit the CSV file.

**Note:** The storage location (which is listed in the Host To Storage column of the CSV file) is the name of the storage device/path, not the storage reservation policy or the name of the storage reservation for the business group. To apply DR services to newly imported virtual machines, the storage device entered must be a DR protected datastore.

If any virtual machines are discovered and present in the CSV file that do not need to be imported, manually set their value for **Import–Yes or No** to **No** in the first column of the CSV file.

To apply Data Protection services to newly imported virtual machines, type **epc.backup.servicelevels** in the Property Name column and the backup Service Level name in the Property Value column.

To import existing virtual machines, select the CSV file containing the virtual machines to be imported and then begin the import, as follows:

1. In the vRealize Automation portal, navigate to **Infrastructure > Infrastructure Organizer > Bulk Imports**.
2. Select **New Bulk Import**, and provide the following details:
   a. Type a **Name** for the import and select the **CSV file**, as shown in Figure 96.
   
   ![](image)
   
   **Figure 96. Executing the Bulk Import operation**
   
   b. At **Start time**, select **Now** or specify a date and time.
   c. At **Batch size**, select **Batch** to define the total number of machines being registered at a specified time.
   d. Select **Ignore managed machines** to omit managed machines during the import process.
   e. Select **Skip user validation** to omit validating users during the import process.
   f. Complete other options as appropriate to the import.

3. Click **OK**.

When the import operation is complete, the requestor receives an email notification for each virtual machine that is successfully imported, as shown in Figure 97.
As shown in Figure 98, the newly imported virtual machines are immediately available in the vRealize Automation portal to the virtual machine owner specified in the import CSV file.

Cloud users can reconfigure the resources already assigned to their virtual machines as defined by the virtual machine blueprint. When business group managers create a virtual machine blueprint, they can restrict the scope of possible reconfiguration by a business group user.

As a machine owner, the cloud user can make any of the following changes to a provisioned machine:

- Increase or decrease memory or number of CPUs
- Modify storage by adding, removing, or increasing the size of volumes
- Modify networks by adding, removing, or updating network adapters

**Reconfiguring an existing virtual machine**
As shown in the example in Figure 99, changes to each of these parameters are subject to the upper limits defined in the blueprint used to provision the machine.

![Figure 99. Reconfiguring virtual machine resources](image)

The execution of the reconfiguration task can be immediate, scheduled, or queued for the virtual machine user, as shown in Figure 100.

![Figure 100. Scheduling reconfiguration of virtual machine resources](image)

**Note:** A deployed VM’s upper limit cannot be increased beyond the original maximum set on the source blueprint, even after increasing the limit on the blueprint. Any subsequent VMs deployed from the increased blueprint inherit the new limits.

### Decommissioning a virtual machine

When the lease on a virtual machine expires, or the machine is manually expired, the machine is either archived or destroyed, depending on whether its blueprint specifies an archive period.
When the end of the archive period is reached, or if no archive period exists, the virtual machine is decommissioned. The business group user can also manually destroy the virtual machine, as shown in Figure 101.

![Machines](image)

**Figure 101. Destroying a virtual machine**

When a virtual machine is destroyed, all charges relating to it are removed from vRealize Business. Its resources are recycled and made available to provision new machines in vRealize Automation.

---

**Note**: DR-protected virtual machines that have expired but have not yet been decommissioned are recovered by SRM during a recovery operation. After a recovery, these virtual machines cannot be managed until they have been failed back to their original vSphere cluster. The recommendation, where possible, is to destroy or reactivate the protected virtual machine prior to a recovery.

---

### Public cloud services

#### Automated provisioning of public cloud resources

The examples in this section demonstrate the public cloud side of Enterprise Hybrid Cloud and show how an end user, using VMware vCloud Air, can create workloads in a public cloud using the same self-service catalog that is used within the on-premises private cloud.

vCloud Air is a secure, hybrid cloud service operated by VMware, built on a foundation of vSphere and Dell EMC-powered technologies. The service supports existing workloads and third-party applications as well as new application development, giving IT organizations a common platform to seamlessly extend their data center into the public cloud and maintain control.
Enterprise Hybrid Cloud takes advantage of the underlying features of vRealize Automation to present a service catalog with items that exist both on and off premises. The examples in this section include details about how to create a catalog item with a workload deployed into vCloud Air, as shown in Figure 102.

![Figure 102. Enterprise Hybrid Cloud resources—private and public](image)

A vCloud Air catalog item that is called from the service catalog is a virtual machine blueprint on a public cloud endpoint.

The following steps provide general guidance for creating a vCloud Air endpoint.

**Note:** Refer to [https://www.vmware.com/support/pubs/vcac-pubs.html](https://www.vmware.com/support/pubs/vcac-pubs.html) for vRealize Automation documentation. The *vRealize Automation Installation and Configuration* document provides details on configuring endpoints and blueprints.

1. Ensure that the following vCloud Air subscription details and information are available:
   - **vCloud Air username and password**—Used to log in to the vCloud Air dashboard, where resource snapshots and virtual data centers can be viewed. These vCloud Air account credentials are entered once in vRealize Automation in the **Credentials** field when an endpoint is created. The same credentials can be used to define multiple vCloud Air endpoints. VMware supplies these credentials and the vCloud Air dashboard URL when the vCloud Air subscription is purchased.
   - **vCloud Provider Address**—Obtained from the specific virtual data center shown on the main dashboard under the **Virtual Data Centers** tab at the bottom of the screen. If more than one virtual data center exists, click the virtual data center for this endpoint. On the right-most side of the virtual data center details page, as shown in Figure 103, click **Cloud Provider Address**, and then copy the URL and organization name to a text file.
2. From the vRealize Automation administration console, select **Infrastructure > Endpoints-Create New Endpoint**, and then select **vApp (vCloud Director)**. Under **Endpoint**, as shown in Figure 104, enter the information that was collected previously from the vCloud Air Cloud Provider Address.

3. Click **OK** to save the new vCloud Air endpoint to the list of endpoints and start the initial endpoint discovery process.

   The process discovers only the virtual data center and should take only a few seconds. To gather everything available within the endpoint, perform a data collection.

4. To run a data collection from the list of endpoints, as shown in Figure 105, select **vCloud Air > Data Collection**. In the window that opens, click **Start**.

   The list of endpoints is displayed while the discovery process runs in the background.

**Note**: You can view the data status by returning to the **Data Collection** option for that endpoint and clicking **Refresh**. When the process is complete, **Endpoint Data collection successful** is displayed. Click **Cancel** to return to the endpoint list.
Assign the resources to an existing fabric group, which places the resources under vRealize Automation control, by navigating to **Infrastructure > Groups > Fabric Groups**.

6. Apply the vCloud Air endpoint to one or more fabric groups:
   a. Select the required fabric group and click **Edit**.
   b. As shown in Figure 106, add the vCloud Air virtual data center resources to the selected fabric group by selecting the **Compute resources** checkbox associated with vCloud Air.
   c. Click **OK**.

The list of fabric groups, which shows that the resource has been assigned to the selected group, is displayed.
7. Assign a portion of the resources to an existing business group:
   a. Select **Infrastructure > Resources > Reservations**.
   b. Select **New Reservation – vAPP (vCloud Director)**, and provide the reservation information, as shown in Figure 107, by selecting the required options.

![New Reservation - vApp (vCloud Director)](image)

Figure 107. Reservation information

8. Click the **Resources** tab to see the storage profiles that are selected for this reservation policy, as shown in Figure 108.

![New Reservation - vApp (vCloud Director)](image)

Figure 108. Reservation resources

9. Click the **Network** tab and select the network path and, optionally, a network profile.

Refer to the **VMware vRealize Automation User Guide** for more information about reservation profiles.
This use case provides instructions for creating a blueprint that can use the previously defined configuration to provision to vCloud Air. In this example, first create the vApp component blueprint on which the vApp is based.

1. From the Infrastructure tab, navigate to Blueprints > Blueprints, select Create New Blueprint, and then select Cloud > vApp Component (vCloud Director).

2. Name the blueprint component to be used in the blueprint vApp template, as shown in Figure 109.

![New Blueprint - vApp Component (vCloud Director)](image)

Figure 109. Creating a blueprint: Blueprint Information

3. On the Build Information tab:
   a. Define the blueprint type and action.
   b. In the Clone from field, select the vApp component template from which to make the clone.

   The vApp component template is taken from the vCloud endpoint and can be a published public vCloud Director host template available as part of the vCloud Air service.

   c. Set the machine resources that this cloned machine will consume, as shown in the example in Figure 110.
4. Select additional options, if required, as shown in Figure 111.

5. Review the information on all the tabs and, when you are satisfied that all relevant options are correct, click **OK** to save the template.

6. Create a new vApp blueprint that uses the new vApp component template to deploy the vApp:
   a. From the **Infrastructure** tab, navigate to **Blueprints > Blueprints**, select **Create New Blueprint**, and then select **Cloud > vApp (vCloud Director)**.
b. On the **Build Information** tab, in the **Clone from** field select the vApp template from which you are cloning.

You previously created the vApp template in vCloud Air as part of the subscription process. This vApp template is paired with the vApp component template that you created in this procedure, as shown in Figure 112. The vApp template is then deployed to vCloud Air as the endpoint.

![Figure 112. vApp blueprint: Build Information](image)

7. After entering all remaining required information, publish the blueprint to the service catalog so that users can provision this vApp into the vCloud Air public cloud.

For more information, refer to *VMware vCloud Air User’s Guide* and *vRealize Automation Installation and Configuration*.

### Deploying a virtual machine to a public cloud

After the public cloud virtual machine blueprint has been created and added to the vRealize Automation service catalog, users with the appropriate entitlement can execute this catalog item and deploy a virtual machine to the vCloud Air endpoint as follows:

1. Select the virtual machine from the vRealize Automation service catalog, as shown in Figure 113.

![Figure 113. Requesting a Public Cloud virtual machine](image)
2. Under **Request Information**, specify any options, such as the number of virtual machines and provisioning details, as shown in Figure 114.

![Figure 114. Specifying request information when deploying a public cloud virtual machine](image)

3. Click **Submit**.

   When the provisioning process has completed, the new virtual machine is available to access under **Home > Items > Machines**.

You can view the new virtual machine in the vCloud Air portal, as shown in Figure 115.

![Figure 115. vCloud Air display of a virtual machine](image)
Onboarding a VxRail endpoint

To onboard a VxRail Appliance as an endpoint:

1. Log in to the Enterprise Hybrid Cloud tenant portal with an account that has infrastructure administrator privileges.

2. Click the Infrastructure tab and then click Endpoints.

3. Click the New Endpoint link on the right, navigate to Virtual, and then click vSphere (vCenter). See Figure 116.

4. Enter the name for the endpoint, which must match the endpoint name that was entered during the IaaS agent installation.

   **Note:** The vCenter endpoint must be configured with the same vSphere agent endpoint name that was used during the initial installation of the IaaS Proxy Agent roles. Otherwise, discovery fails.

5. In the Address field, type the URL of the vCenter SDK: https://vxrail01-vc01.domain.local/sdk.

6. To select the credentials, click the ellipsis and select the vCenter Server credentials, and then click OK.

7. If NSX is present, enable Specify manager for network and security platform and in the resulting address field, type the URL of the NSX manager: https://nsx-mgr.domain.local.

8. To select the credentials, click the ellipsis and select the NSX manager credentials. Click OK and then click OK again.

9. Click OK.

![Figure 116. Create VxRail vCenter endpoint for vRealize Automation](image)
This chapter presents the following topics:

Overview .......................................................................................................... 106
Managing Avamar ........................................................................................... 106
Managing Avamar Site Relationships ............................................................ 109
Managing Avamar Replication Relationships ............................................... 112
Managing Avamar proxies .............................................................................. 116
Managing Backup service levels ................................................................... 124
Virtual machine backup lifecycle ................................................................. 130
Ensuring continuity of backup in CA failure scenarios ............................... 136
Data protection reporting ............................................................................... 142
Overview

This chapter provides information about the data protection services available with Enterprise Hybrid Cloud. It focuses on the services available to cloud users responsible for the administration and management of data protection services, as follows:

- Data protection backup
- Data protection CA
- Data protection DR

Cloud infrastructure or backup administrators, as well as cloud end users, consume the backup and recovery services available with Enterprise Hybrid Cloud.

vRealize Automation cloud administrators use their service catalog to create backup service levels. At virtual machine deployment time, cloud users, in the vRealize Automation self-service portal, can choose to protect their machines with a predefined backup service level, and initiate on-demand, point-in-time backups and restores of their virtual machines.

The following section describes the catalog services and provides an overview of some of the infrastructural and operational tasks involved in the protection of virtual machines in Enterprise Hybrid Cloud. Before you can take advantage of Enterprise Hybrid Cloud Data Protection Backup, set up your environment using the Avamar maintenance catalog items in the vRealize Automation Service Catalog.

Managing Avamar

When the data protection packages have been installed and initialized, Avamar grids are introduced into the Enterprise Hybrid Cloud object model. The Avamar Grid Maintenance catalog item allows the administrator to manipulate Avamar grid objects.

To perform Avamar grid maintenance:

1. Log in to the Enterprise Hybrid Cloud tenant portal as the system administrator with entitlements to the EHC Data Protection Services catalog items (for example, ehc_backup_admin@domain.local).

2. Go to Catalog > Data Protection Services and select Avamar Grid Maintenance, as shown in Figure 117.
Service Catalog

Browse the catalog for services you need.

Figure 117. Avamar Grid Maintenance catalog item

3. Under Request Information, type a description, optionally type a reason, and click Next, as shown in Figure 118.

Figure 118. Avamar Grid Maintenance Request Information tab

4. Select the action you want to perform from the Select Operation Type list box, as shown in Figure 119.
Add Avamar Grid  Prerequisites

- The Avamar grid must be deployed and configured for authentication.
- A minimum of one Avamar proxy must be deployed and registered to Avamar.
- A nonreplicated datastore must exist for proxy placement.

Figure 75 shows the required steps to add an Avamar grid.

Figure 120. Add Avamar Grid flowchart

Catalog item description

Table 34 describes Add Avamar Grid parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avamar Grid Name</td>
<td>User-friendly name for the Avamar Grid.</td>
</tr>
<tr>
<td>Avamar Grid FQDN</td>
<td>FQDN of the Avamar Grid.</td>
</tr>
<tr>
<td>Avamar Grid Admin User</td>
<td>Username of the admin user of the Avamar Grid (for example, admin).</td>
</tr>
<tr>
<td>Avamar Grid Admin Password</td>
<td>Password of the admin user of the Avamar Grid.</td>
</tr>
<tr>
<td>Registered Proxies</td>
<td>List of proxies registered with the Avamar Grid.</td>
</tr>
<tr>
<td>Choose Site</td>
<td>List of available sites to associate with the Avamar Grid.</td>
</tr>
<tr>
<td>Avamar SOAP Username</td>
<td>Username of the SOAP user of the Avamar Grid (for example, <a href="mailto:app_avamar_soap@domain.local">app_avamar_soap@domain.local</a>).</td>
</tr>
<tr>
<td>Avamar SOAP Password</td>
<td>Password of the SOAP user of the Avamar Grid.</td>
</tr>
</tbody>
</table>
Edit Avamar Grid  
Table 35 describes the Edit Avamar Grid parameters.

Table 35. Edit Avamar Grid parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modify Avamar Grid details</td>
<td>Allows the administrator to edit all values entered during the Add Avamar Grid catalog item.</td>
</tr>
<tr>
<td>Associate manually deployed Avamar proxies with Avamar Grid</td>
<td>Allows the administrator to select an Avamar Grid and then associate manually deployed proxies with that grid.</td>
</tr>
<tr>
<td>Set Avamar Grid to Admin Full</td>
<td>Allows the administrator to set an Avamar grid to Admin Full when a grid is full or when maintenance operations are required. All backup operations to that grid are suspended.</td>
</tr>
</tbody>
</table>

Delete Avamar Grid  
An Avamar grid object can be deleted only if it is not referenced by any other objects (clusters, hardware islands, or other vCenters).

Table 36 describes the Delete Avamar Grid parameters.

Table 36. Delete Avamar Grid parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avamar Grid</td>
<td>Select an Avamar Grid from the list.</td>
</tr>
<tr>
<td>Confirm</td>
<td>Select <strong>Confirm</strong> or <strong>Deny</strong>, as required.</td>
</tr>
</tbody>
</table>

Managing Avamar Site Relationships  
An ASR is a relationship between sites for backup purposes. The Avamar Site Relationship (ASR) Maintenance catalog item allows the administrator to manipulate ASR objects.

To perform ASR maintenance:

1. Log in to the Enterprise Hybrid Cloud tenant portal as the system administrator with entitlements to the EHC Data Protection Services catalog items (for example, ehc_backup_admin@domain.local).
2. Go to **Catalog > Data Protection Services** and select **Avamar Site Relationship (ASR) Maintenance**, as shown in Figure 121.
3. Under Request Information, type a description, optionally type a reason, and click Next, as shown in Figure 122.

4. Select an action to perform, as shown in Figure 123.
### Add an ASR

#### Prerequisites

- The Avamar grid must be deployed and configured for authentication.
- A minimum of one Avamar proxy must be deployed and registered to Avamar.
- A nonreplicated datastore must exist for proxy placement.

Figure 124 shows the required steps to add an ASR.

![Add an ASR flowchart](image)

**Figure 124. Add an ASR flowchart**

### Catalog item description

Table 37 describes the ASR backup types.

#### Table 37. Add ASR parameters

<table>
<thead>
<tr>
<th>Backup type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1C1VC</td>
<td>One backup copy. One vCenter. Applicable to local virtual machines only.</td>
</tr>
<tr>
<td>MC2VC</td>
<td>Mixed copy. Two vCenters. Applicable to environments with EMC RecoverPoint for Virtual Machines enabled. Because EMC RecoverPoint for Virtual Machines protection can be enabled for any local VM, the ASR for all local clusters must be assigned as MC2VC. This assignment is required because a local cluster can contain both local-only virtual machines and virtual machines protected by EMC RecoverPoint for Virtual Machines.</td>
</tr>
<tr>
<td>2C1VC</td>
<td>Two backup copies. One vCenter. Applicable to CA-protected virtual machines and only available when global option <code>ca_enabled = true</code>. See <a href="#">Enable the hardware island name in the storage reservation name</a> for more information.</td>
</tr>
<tr>
<td>2C2VC</td>
<td>Two backup copies. Two vCenters. Applicable to SRM DR protected virtual machines and only available when global option <code>dr_enabled = true</code>. See <a href="#">Managing features and environmental defaults</a> for more information.</td>
</tr>
</tbody>
</table>

The administrator must also specify the site or sites to be associated with the ASR.
### Edit an ASR

You can edit an ASR object only if it is not associated with an ARR. Table 38 describes the Edit ASR parameters.

**Table 38. Edit ASR parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select ASR</td>
<td>Select an ASR to edit.</td>
</tr>
<tr>
<td>Select First Site</td>
<td>Select the first site you want to associate.</td>
</tr>
<tr>
<td>Select Second Site</td>
<td>Select the second site you want to associate.</td>
</tr>
</tbody>
</table>

### Delete an ASR

You can delete an ASR object only if it is not referenced by any other objects (ARRs or vCenter Clusters). Table 39 describes the Delete ASR parameter.

**Table 39. Delete ASR parameter**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select ASR</td>
<td>Select an ASR to delete.</td>
</tr>
</tbody>
</table>

### Managing Avamar Replication Relationships

An ARR is a relationship between as many as three Avamar grids. The ARR determines the specific Avamar grids that are responsible for backup operations on an individual Enterprise Hybrid Cloud workload. The Avamar Replication Relationship (ARR) Maintenance catalog item allows the administrator to manipulate ARR objects.

To perform ARR maintenance:

1. Log in to the Enterprise Hybrid Cloud tenant portal as the system administrator with entitlements to the EHC Data Protection Services catalog items (for example, ehc_backup_admin@domain.local).

2. Go to Catalog > Data Protection Services and select Avamar Replication Relationship (ARR) Maintenance, as shown in Figure 125.
3. Under Request Information, type a description, optionally type a reason, and click Next, as shown in Figure 126.

4. Select the action you want to perform, as shown in Figure 127.
Add an ARR

**Prerequisites**
- The Avamar grid must be deployed and configured for authentication.
- A minimum of one Avamar proxy must be deployed and registered to Avamar.
- A nonreplicated datastore must exist for proxy placement.

Figure 128 shows the required steps to add an ARR.

![Add an ARR flowchart](Figure)

**Catalog item description**

Table 40 describes the Add ARR parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASR</td>
<td>Select the relevant ASR.</td>
</tr>
<tr>
<td>First Avamar Grid</td>
<td>Select the first Avamar Grid for the ARR.</td>
</tr>
<tr>
<td>Second Avamar Grid</td>
<td>Select the second Avamar Grid for the ARR.</td>
</tr>
</tbody>
</table>

Edit an ARR

Table 41 describes the edit ARR parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select ARR</td>
<td>Select an ARR to edit.</td>
</tr>
<tr>
<td>Admin Full</td>
<td>Allows the administrator to set an Avamar grid to Admin Full when a grid is full or when maintenance operations are required. All backup operations to that grid are suspended.</td>
</tr>
</tbody>
</table>
Delete an ARR

An ARR object may only be deleted if not referenced by any other objects (ARRs or vCenter Clusters). Table 42 describes the parameter that is available.

Table 42. Delete ARR parameter

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select ARR</td>
<td>Select an ARR to delete from the list.</td>
</tr>
</tbody>
</table>

Associate a cluster to an ASR

This catalog item associates a cluster with an ASR. This association dictates the backup type that is available to virtual machines deployed on the cluster.

Prerequisites

- The Avamar grid must be deployed and configured for authentication.
- A minimum of one Avamar proxy must be deployed and registered to Avamar.
- A non-replicated datastore must exist for proxy placement.

Figure 129 shows the required steps to associate a cluster to ASR.

![Figure 129. Associate a cluster to an ASR flowchart](image)

Catalog item description

Table 43 describes the parameters that are available.

Table 43. Associate Cluster to ASR parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Cluster Name</td>
<td>Select a vSphere cluster.</td>
</tr>
<tr>
<td>Select ASR Name</td>
<td>Select the ASR to associate with the chosen vSphere cluster.</td>
</tr>
</tbody>
</table>
Managing Avamar proxies

Deploy Avamar proxy virtual machines to each Enterprise Hybrid Cloud-enabled cluster to mount VMDKs directly from the datastores on that cluster. Each cluster type has its own proxy requirements.

To determine the required number of Avamar proxy virtual machines for an LC1S cluster, use the following logic:

1. Identify the 1C1VC ASR to which the cluster is mapped.
2. Determine the number of ARRs associated with the cluster’s ASR.
3. For each ARR that is discovered, deploy a minimum of one proxy virtual machine, registered to the Avamar grid that is a member of the 1C1VC ARR.

If there is scope within the overall number of proxies that can be deployed to the environment, two proxies are recommended for high availability, as shown in Figure 130. This number can be approximately 60 to 80 proxies per vCenter.

Figure 130. LC1S without EMC RecoverPoint for Virtual Machines proxy example
To determine the required number of Avamar proxy virtual machines for an LC1S cluster, use the following logic:

1. Identify the MC2VC ASR to which the cluster is mapped.
2. Determine the number of ARRs associated with the cluster’s ASR.
3. For each ARR discovered, deploy a minimum of two proxy virtual machines:
   - One proxy must be on the LC1S cluster on the first site and registered to the Avamar grid member of the MC2VC ARR that is on the same site.
   - The second proxy must be on the LC1S cluster’s partner cluster on the second site and registered to the Avamar grid member of the MC2VC ARR that is on the same site as the partner cluster.

If there is scope within the overall number of proxies that can be deployed to the environment, four proxies are recommended for high availability, as shown in Figure 131. This number can be approximately 60 to 80 proxies per vCenter.

![Figure 131. LC1S with EMC RecoverPoint for Virtual Machines proxy example](image)

**Note:** In this configuration, if a single Avamar instance fails without a vCenter infrastructure failure on the same site, the second member of the ARR does not automatically back up virtual machines. For additional resilience on each site, use an Avamar Redundant Array of Independent Nodes (RAIN) grid. Alternatively, move workloads to the site that is fully operational to continue using backup services.
CA1S clusters

To determine the required number of Avamar proxy virtual machines for a CA1S cluster, use the following logic:

1. Identify the 1C1VC ASR to which the cluster is mapped.
2. Determine the number of ARRs associated with the cluster’s ASR.
3. For each ARR discovered, deploy a minimum of one proxy virtual machine, registered to the Avamar grid that is a member of the 1C1VC ARR.

If there is scope within the overall number of proxies that can be deployed to the environment, two proxies are recommended for high availability, as shown in Figure 132. This number can be approximately 60 to 80 proxies per vCenter.

Note: The hardware island on which these proxies normally reside on the CA1S cluster is of no importance to the backup solution. It is assumed that latency from either side of the half of the CA1S cluster to the Avamar infrastructure is the same because both hardware islands are on the same site.

Figure 132. CA1S proxy example
CA2S clusters

To determine the required number of Avamar proxy virtual machines for a CA2S cluster, use the following logic:

1. Identify the 2C1VC ASR to which the cluster is mapped.
2. Determine the number of ARRs associated with the cluster’s ASR.
3. For each ARR discovered, deploy a minimum of two proxy virtual machines. One proxy should be registered to each Avamar grid that is a member of the 2C1VC ARR.

If there is scope within the overall number of proxies that can be deployed to the environment, four proxies are recommended for high availability, as shown in Figure 133. This number can be approximately 60 to 80 proxies per vCenter.

Proxies must be bound to hosts in the cluster that are physically on the same site as the Avamar grid to which they are registered by:

- Adding the proxy virtual machines to DRS virtual machine affinity groups created on a per site basis.
- Adding a DRS virtual machine to host rule that sets those virtual machines to *must run* on the DRS host group created by the CA2S onboarding process.

No unnecessary cross-WAN backups occur because Avamar can use vStorage APIs for data protection to add VMDKs (from the local leg of the VPLEX volume) to proxy virtual machines bound to physical hosts on the same site as the Avamar grid.

![Figure 133. CA2S proxy example](image-url)
To determine the required number of Avamar proxy virtual machines for a DR2S cluster, use the following logic:

1. Identify the 2C2VC ASR to which the cluster is mapped.
2. Determine the number of ARRIs associated with the cluster’s ASR.
3. For each ARR discovered, deploy a minimum of two proxy virtual machines:
   - One proxy must be on the DR2S cluster on the first site and registered to the Avamar grid member of the 2C2VC ARR that is on the same site.
   - The second proxy must be on the DR2S cluster’s partner cluster on the second site and registered to the Avamar grid member of the 2C2VC ARR that is on the same site as the partner cluster.

If there is scope within the overall number of proxies that can be deployed to the environment, four proxies are recommended for high availability, as shown in Figure 134. This number can be approximately 60 to 80 proxies per vCenter.

---

**Note**: In this configuration, if a single Avamar instance fails without a vCenter infrastructure failure on the same site, the second member of the ARR does not automatically back up virtual machines. For additional resilience on each site, use an Avamar RAIN grid. Alternatively, move workloads to the site that is fully operational to continue using backup services.
A user who is assigned the data protection backup service entitlement can deploy additional Avamar proxies.

**Prerequisites**

- The Avamar grid must be deployed and configured for authentication.
- A minimum of one Avamar proxy must be deployed and registered to Avamar.
- Avamar proxies must be added to DNS.
- A nonreplicated datastore must exist for proxy placement.

Figure 135 shows the required steps to deploy Avamar proxies.

**Catalog item description**

To deploy Avamar proxies:

1. In the vRealize Automation service catalog, click **Request** on **Deploy Avamar Proxy**.
2. Under **Request Information**, type a description of the request and click **Next**, as shown in Figure 136.
3. Select the required action:
   - Select **Add Proxy** to add an Avamar proxy.
   - Select **Delete Proxy** to delete an Avamar proxy.

4. Under **vCenter Information**, enter the information described in Table 44:

   **Table 44. Deploy Avamar proxy vCenter information parameters**
   
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster Name</td>
<td>The vSphere cluster on which to deploy the proxy</td>
</tr>
<tr>
<td>Datastore Name</td>
<td>The vSphere datastore on which to deploy the proxy</td>
</tr>
<tr>
<td>Network Name</td>
<td>The vSphere network on which the proxy must be</td>
</tr>
<tr>
<td></td>
<td>connected</td>
</tr>
</tbody>
</table>

5. 

6. Under **Proxy Information**, enter the information described in Table 45:

   **Table 45. Deploy Avamar proxy information parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the proxy virtual machine in vCenter.</td>
</tr>
<tr>
<td>Avamar Proxy Path</td>
<td>The Avamar path to the proxy using FQDN (for example, /clients/ny-av1-p0.domain.local)</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of the proxy</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>The subnet mask of the proxy</td>
</tr>
<tr>
<td>Gateway</td>
<td>The gateway of the proxy</td>
</tr>
<tr>
<td>DNS</td>
<td>The DNS server of the proxy</td>
</tr>
<tr>
<td>Username</td>
<td>The username of the proxy (the default is root)</td>
</tr>
<tr>
<td>Password</td>
<td>The password for the user</td>
</tr>
</tbody>
</table>

7. Under **Avamar Information**, enter the information described in Table 46:

   **Table 46. Deploy Avamar proxy Avamar information parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avamar Grid Name</td>
<td>Select an Avamar grid with which to associate the proxy.</td>
</tr>
<tr>
<td>Avamar Domain</td>
<td>The Avamar domain with which to associate the proxy.</td>
</tr>
<tr>
<td>OVA Location</td>
<td>The proxy OVA location on the Avamar appliance. Update the default value as required.</td>
</tr>
</tbody>
</table>
8. Under **Deployment Server Information**, enter the information described in Table 47:

Table 47. Deploy Avamar proxy deployment server information parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deployment Server</td>
<td>The FQDN of the deployment server.</td>
</tr>
<tr>
<td>Username</td>
<td>The username for the Deployment Server.</td>
</tr>
<tr>
<td>Password</td>
<td>The password for the user.</td>
</tr>
<tr>
<td>Disable Verification</td>
<td>Optionally, skips SSL verification. The recommended setting is No.</td>
</tr>
</tbody>
</table>

9. Click **Next** and click **Submit**.

When all details are submitted, a new Avamar proxy is deployed to the specified location and is automatically registered with Avamar.

This catalog item associates a cluster with manually deployed Avamar proxies.

**Prerequisites**
- The Avamar grid must be deployed & configured for authentication.
- A minimum of one Avamar proxy must be deployed and registered to Avamar.
- A nonreplicated datastore must exist for proxy placement.

Figure 137 shows the required steps to associate Avamar proxies with a cluster.
Catalog item description

Table 48 describes the parameters that are available.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Cluster Name</td>
<td>Select a vSphere cluster.</td>
</tr>
<tr>
<td>Registered Proxy List</td>
<td>Select Avamar proxies to associate with the chosen vSphere cluster.</td>
</tr>
</tbody>
</table>

Managing Backup service levels

Backup service levels are created using the vRealize Automation catalog item Create Backup Service Level. An IaaS user can select a backup service level when deploying a workload or apply BaaS policies to a workload as a Day 2 operation. The Backup Service Level Maintenance catalog item lets the administrator manipulate backup service levels.

To perform backup service level maintenance:

1. Log in to the Enterprise Hybrid Cloud tenant portal as the system administrator with entitlements to the EHC Data Protection Services catalog items (for example, ehc_backup_admin@domain.local).

2. Go to Catalog > Data Protection Services and select Backup Service Level Maintenance, as shown in Figure 138.

Service Catalog

Browse the catalog for services you need.
3. Under **Request Information** type a description, optionally type a reason, and click **Next**, as shown in Figure 139.

![Backup Service Level Maintenance Request Information tab](image)

**Figure 139. Backup Service Level Maintenance Request Information tab**

4. Select the action you want to perform, as shown in Figure 140.

![Backup Service Level Maintenance: Choose Action](image)

**Figure 140. Backup Service Level Maintenance: Choose Action**

**Prerequisites**

- vCenter Endpoint Cloud-VC01 is added to the vRealize Orchestrator vCenter plug-in.
- The ViPR virtual array has been created.
- Local cluster **NY-HWI-1-C1** has been created in Cloud-VC01.
- The Avamar grid is online.
- Avamar proxies deployed.
Chapter 6: Data Protection

Figure 141 shows the required steps to add a backup service level.

1. Select Add Backup Service Level from the Backup Service Level catalog item actions list.
2. Under Backup Service Level, type a name for the new backup service level, as shown in Figure 142.
3. Select a backup schedule. The options are Daily, Weekly, and Monthly, as shown in Figure 143.

When selecting a daily schedule, specify one or more time intervals (for example, 03:00 and 03:30).
When selecting a monthly schedule, specify the week in which the backup will take place. The backup time follows the default backup window.

4. On the **Retention Policy** tab, specify or create a retention policy appropriate for this backup service level.

You can specify or create one of several types of retention policies:

- Retain the backups forever.
- Retain the backups for a certain number of days/weeks/months/years.
- Retain the backups until a certain date.
- Define a custom retention period.

To keep the backups for a certain number of days, weeks, months, or years, select the **for** option, type a number, and select **days, weeks, months, or years** from the menu, as shown in Figure 144.

To define a backup retention period of forever, select **forever**. To keep the backup until a certain date, select **Until**, which enables you to choose any future date.

You can apply a custom retention schedule based on each of the backup types by making selections from all of the possible parameters available.

![Figure 144. Create Backup Service Level request: Specifying retention policy details](image)

5. Under **Replication Schedule**, select a schedule from the list.

6. Click **Next** and **Submit**.

After you create the required Avamar objects, the vRealize Orchestrator workflows create or update the service-level property in the Enterprise Hybrid Cloud Object Model and the vRealize Automation custom dictionary with the new backup-service-level name. The requester is notified by email when the workflow completes.
A backup service level may only be deleted if the associated vCenter folder does not contain any virtual machines.

The following parameters are available:

- **Select Backup Service Level**—Select the backup service level to be deleted.
- **Confirm**—Select **Yes** or **No**.

Before the backup service level is deleted, the operation checks for any virtual machines that are actively using that backup service level. If any exist, then the operation stops and instructs the user to remove the virtual machine from that backup service level before attempting to delete the backup service level again.

To remove the virtual machine from the backup service level, the user in vRealize Automation can retire the virtual machine or a vCenter administrator can manually move the virtual machine from the backup service level folder to the VRM folder in vCenter.

**Note:** When a virtual machine is retired, a long-term backup is created before the machine is destroyed. Moving the virtual machine to another vCenter folder keeps the virtual machine active, but no further backups are performed.

When adding additional vCenters to the Enterprise Hybrid Cloud, you can add existing backup service levels to the new vCenter. The Remediate Backup Service Level for new vCenter Endpoint catalog item performs all of the actions necessary to remediate the data protection components when adding a new vCenter.

To remediate backup service levels for a new vCenter endpoint:

1. Log in to the Enterprise Hybrid Cloud tenant portal as the system administrator with entitlements to the EHC Data Protection Services catalog items (for example, ehc_backup_admin@domain.local).
2. Go to **Catalog > Data Protection Services** and select **Remediate Backup Service Level for new vCenter Endpoint**, as shown in Figure 145.
Figure 145. Remediate Backup Service Level for new vCenter Endpoint catalog item

3. Under **Request Information**, type a description, optionally type a reason, and click **Next**, as shown in Figure 146.

Figure 146. Remediate Backup Service Level for new vCenter Endpoint Request Information tab

4. Select the vCenter you want to remediate from the **Select vCenter to remediate** list box and click **Submit**.

**Remediate a single failed Avamar grid**

Use the Remediate Single Failed Avamar service when an Avamar grid has been replaced or brought back online.

Unless all the backup and replication policies on the failed unit are disabled when the unit comes back online, both the primary and secondary Avamar instances attempt to execute parallel scheduled backups of the virtual machines.
As shown in Figure 147, the Remediate Single Failed Avamar service requires the selection of the Avamar grid for remediation.

![Figure 147. Remediate Single Failed Avamar request: Selecting the Avamar grid](image)

The service interrogates the Avamar grid and remediates any missing information.

### Virtual machine backup lifecycle

**Enable backup and restore for a blueprint**

To enable backup and restore functionality for a vRealize Automation blueprint, enable the `BackupAndRestoreFunctions` build profile on the blueprint, as shown in Figure 148.

![Figure 148. Enabling a build profile for backup and restore functions in the blueprint](image)

**Prerequisites**

- The Avamar grid is online.
- Avamar proxies deployed.
- The blueprint with `BackupAndRestoreFunctions` is created and available to the business group.
Figure 149 shows the required steps to deploy a virtual machine with backup protection.

1. In the vRealize Automation self-service portal, log in to your account, click Catalog, and select a blueprint from the list of available blueprints, as shown in Figure 150.
2. Within the virtual machine blueprint, select the required backup service level, as shown in Figure 151.

![Figure 151. Selecting a backup service level for the virtual machine](image)

You can also select the number of virtual machines to deploy, and increase or decrease virtual machine resources, depending on your entitlements.

3. Review and edit the storage options for the virtual machine, click **Next** to view the **Cost Summary**, and then click **Submit**.

The virtual machine is provisioned into the relevant folder defined in vCenter for that service level, and it inherits the backup schedules defined for that service level.

Cloud users receive the name of the virtual machine in an email notification from the administrator after the provisioning process successfully completes. The email notification advises the user to wait a period of time before attempting to access the newly deployed virtual machine. The customization operations, which are required to automatically protect the virtual machine, are run during that time.

**On demand backup**

This use case describes how a cloud user can request an on-demand backup of a virtual machine from the vRealize Automation self-service portal. The user does not have to wait for the completion of the backup task. An email notification of the backup status is automatically generated when the task is complete, whether the task succeeded or failed.

After logging in to the vRealize Automation self-service portal, a cloud user can select **On Demand Backup** from the **Actions** menu for a virtual machine, as shown in Figure 152.
Chapter 6: Data Protection

Figure 152. Selecting an on demand backup for a virtual machine

The on-demand backup request initiates the relevant vRealize Orchestrator workflow, which performs the backup using the dataset and retention policy defined by the backup service level.

When the task is complete, the user receives an automated email notification with the status of the task. The email status workflow runs asynchronously and, therefore, the user does not have to wait for the completion status of the backup.

This use case describes the on-demand restore of a virtual machine from the vRealize Automation self-service portal, where the user can choose to restore from a list of the available backups.

The cloud user follows these steps to restore a virtual machine with an available backup:

1. Power off the virtual machine.
2. Log in to the vRealize Automation self-service portal and browse to Items.
3. Select the virtual machine to be restored and click On Demand Restore under Actions, which opens the On Demand Restore request wizard.
4. Under **Request Information**, type a description of the request in the **Description** field, as shown in Figure 153.

![New Request](image)

**Figure 153.** On Demand Restore request: Specifying request information

5. Under **Choose Backup Point**, select required, as shown in Figure 154.

![New Request](image)

**Figure 154.** On Demand Restore request: Selecting a backup point-in-time to restore

After requesting the on-demand restore, the cloud user receives an email notification that indicates the success or failure status of the job, including the reason for a failure if applicable, and how long it took to restore the backup.

If, for example, a virtual machine is powered on, then the restore operation fails and an email is sent to the user that identifies the power state as the reason for the failure.

Selecting a restore point during an on-demand restore (multisite, single vCenter)

Restore points of a virtual machine fall into one of two categories:

- Backups performed locally to the primary Avamar system
- Replicated backups from the secondary Avamar system where the backups were previously performed on the secondary instance and later replicated to the primary

During an on-demand restore operation, Enterprise Hybrid Cloud workflows dynamically interrogate the primary Avamar instance for relevant backups of both types and present a consolidated list of available backups from which to choose, as shown in Figure 155.
Chapter 6: Data Protection

Figure 155. On Demand Restore request: Selecting a backup point

Restore points that are taken to the other Avamar instance and replicated to the system currently designated as primary have **REPLICATED** appended to the end of the backup details.

Based on the choice you make, the Enterprise Hybrid Cloud workflows execute the relevant restore tasks to return the virtual machine to the correct point in time. Regardless of where the backup is taken (that is, to which Avamar instance) the data is always restored from the Avamar system currently configured as the primary.

This use case describes how a cloud user can request the decommissioning of a virtual machine that has data protection backup. From the vRealize Automation self-service portal, the user can request that a virtual machine be destroyed (or retired), as shown in Figure 156.

Figure 156. Destroying a virtual machine

The request initiates a number of tasks. Based on the service level of the virtual machine, a final backup is taken and the virtual machine is retired in the Avamar system, meaning that the virtual machine is permanently deleted from the service-level folder. A retired virtual machine can be restored from Avamar at any time prior to the backup expiration date. Retired virtual machine backups expire according to the retention policy of the service level, but the last backup expires according to the long-term retention policy applied at the time of retirement. Retired virtual machines do not participate in any further backup schedules after they have been retired.
RetireVM is the vRealize Orchestrator workflow that orchestrates the various tasks required to decommission a virtual machine. The steps in the RetireVM workflow are as follows:

1. **Create Retire VM folder**—A temporary virtual machine folder is created with a unique string. The name of the folder also contains the long retention name and the virtual machine name. This is achieved using a VMware vCenter API call.

2. **Move VM to Retire folder**—The virtual machine is moved to the Retire folder from its service-level folder.

3. **Perform on-demand backup**—Because this virtual machine is retired permanently and no further backups of the machine are possible, a final backup is taken with a long-term retention policy based on the service level.

4. **Retire Client**—After the backup is complete, the client is retired in the Avamar system. This de-lists the virtual machine from the regular Avamar backups, and no further backups are performed on this virtual machine. The virtual machine is also removed from the active view of the Avamar client folder.

5. **Move VM back to Service Level folder**—The virtual machine is moved to its original service level and the vRealize Automation destroy process deletes it permanently from vCenter.

6. **Delete the temporary SL folder**—As a cleanup process, the temporary virtual machine folder is deleted from vCenter.

### Ensuring continuity of backup in CA failure scenarios

**Failover Avamar policies for an offline Avamar grid**

If a grid goes offline, the Failover Avamar policies for Offline Avamar Grid service enable the administrator to fail over all backup policies to the secondary grid, and all backup operations to continue.

To fail over Avamar policies:

1. Log in to the Enterprise Hybrid Cloud tenant portal as the system administrator with entitlements to the EHC Data Protection Services catalog items (for example, ehc_backup_admin@domain.local).

2. Go to **Catalog > Data Protection Services** and select **Failover Avamar policies for offline Avamar grid**, as shown in Figure 157.
Service Catalog

Browse the catalog for services you need.

![Failover Avamar Policies catalog item](image)

**Figure 157. Failover Avamar Policies catalog item**

3. Under Request Information, type a description, optionally type a reason, and click Next, as shown in Figure 158.

![Failover Avamar Policies Request Information tab](image)

**Figure 158. Failover Avamar Policies Request Information tab**

4. Select the failed Avamar grid and click Submit, as shown in Figure 159.

![Failover Avamar Policies: Select the failed Avamar Grid](image)

**Figure 159. Failover Avamar Policies: Select the failed Avamar Grid**

If the original primary Avamar grid is offline because of unit or site failure, the Failover Avamar Policies for offline Avamar Grid service enables the policies on the surviving Avamar instance.
The Failback Avamar policies after restoring an Avamar grid service enables the administrator to fail back all backup policies to the original Avamar grid when the original Avamar grid is brought back online.

To fail back Avamar policies:

1. Log in to the Enterprise Hybrid Cloud tenant portal as the system administrator with entitlements to the EHC Data Protection Services catalog items (for example, ehc_backup_admin@domain.local).
2. Go to Catalog > Data Protection Services and select Failback Avamar policies after Restoring Avamar grid, as shown in Figure 160.

3. Under Request Information, type a description, optionally type a reason, and click Next as shown in Figure 161.
4. Select the Avamar grid that has been restored and click **Submit**, as shown in Figure 162.

![New Request](image)

**Figure 162. Failback Avamar Policies: Select restored Avamar grid**

**Failover Avamar grids after a site failure**

The Failover Avamar Grids after Site Failure service enables the administrator to fail over all backup policies to the secondary site if a site goes offline. This allows all backup operations to continue.

**To fail over Avamar policies:**

1. Log in to the Enterprise Hybrid Cloud tenant portal as the system administrator with entitlements to the EHC Data Protection Services catalog items (for example, `ehc_backup_admin@domain.local`).

2. Go to **Catalog > Data Protection Services** and select **Failover Avamar Grids after Site Failure**, as shown in Figure 163.

![Service Catalog](image)

**Figure 163. Failover Avamar Grids after Site Failure catalog item**
3. Under **Request Information**, type a description, optionally type a reason, and click **Next**, as shown in Figure 164.

4. Select the failed site and click **Submit**, as shown in Figure 165.

---

**Failback Avamar policies after site restoration**

The Failback Avamar Policies after Site Restoration service allows the administrator to fail back all backup policies to the original site when the original site is restored. All backup policies revert to their original Avamar grid.

To fail over Avamar policies:

1. Log in to the Enterprise Hybrid Cloud tenant portal as the system administrator with entitlements to the EHC Data Protection Services catalog items (for example, ehc_backup_admin@domain.local).

2. Go to **Catalog > Data Protection Services** and select **Failback Avamar Policies after Site Restoration**, as shown in Figure 166.
Chapter 6: Data Protection

Figure 166. Failback Avamar Policies after Site Restoration catalog item

3. Under Request Information, type a description, optionally type a reason, and click Next as shown in Figure 167.

Figure 167. Failback Avamar policies after Site Restoration Request Information tab

4. Select the failed site and click Submit, as shown in Figure 168.

Figure 168. Failback Avamar Policies after Site Restoration: Site selection
Data protection reporting

Initialize Data Protection Advisor

Data Protection Advisor (DPA) is required for data protection reporting workflows. If DPA was not initialized during the initial Enterprise Hybrid Cloud data protection setup, use the Initialize DPA catalog item to add DPA to the environment.

To initialize DPA:

1. Log in to the Enterprise Hybrid Cloud tenant portal as the system administrator with entitlements to the EHC Data Protection Services catalog items (for example, ehc_backup_admin@domain.local).

2. Go to Catalog > Data Protection Services and select Initialize DPA, as shown in Figure 169.

3. Under Request Information, type a description, optionally type a reason, and click Next, as shown in Figure 170.
4. Under **Initialize DPA**, type the DPA server FQDN and credentials of a user with DPA User role, as shown in Figure 171.

![Figure 171. Initialize DPA server details](image)

**New Request**

<table>
<thead>
<tr>
<th>Request Information</th>
<th>Initialize DPA Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>DPA FQDN:</td>
<td>dps.domain.local</td>
</tr>
<tr>
<td>Username:</td>
<td><a href="mailto:app_vro_dpa@domain.local">app_vro_dpa@domain.local</a></td>
</tr>
<tr>
<td>Password:</td>
<td>*****************</td>
</tr>
</tbody>
</table>

**Initialize DPA**

Initialize a connection to the Data Protection Advisor (DPA) to enable detailed Avamar (backup) reports. If DPA Available was chosen during the Data Protection module initialization, the DPA connection has already been established.

From the vRealize Automation self-service portal, a cloud user can run an on-demand status report of available virtual machine backups.

1. After logging in to the vRealize Automation self-service portal, request the available backups by navigating to the virtual machine under **Items**, and then clicking **Get Backup Status** under **Actions**.

2. Provide the required information in the **New Request** dialog box, as shown in Figure 172.

![Figure 172. Requesting a list of all available backups of a virtual machine](image)

The vRealize Orchestrator workflow that supports this operation runs an Avamar MCCLI command requesting that all the available backups for a virtual machine be emailed to the cloud user.
When the workflow is complete, you receive an email notification that lists all the backups available for the virtual machine, as displayed in Figure 173.

Cloud users can request cost and usage information about any of their virtual machines from the vRealize Automation self-service portal by selecting Get Backup Summary from the virtual machine’s Actions menu.

You receive an email notification containing the relevant backup usage information, as shown in Figure 174.

Cloud users can request a report containing comprehensive backup details specific to any of their virtual machines. A user can run this operation from the self-service portal by selecting the virtual machine and selecting Get Backup Detailed Report from the Actions menu.

This backup report contains the following information categories:

- Job Summary
- Failed Jobs
- Backup Jobs with Last Resolution
Chapter 6: Data Protection

- Estimated Protected Backup Capacity Details
- Backup Client De-Dupe Ratios
- Chargeback Summary
- Client Configuration

You receive an email message containing a report with backup information specific to the virtual machine, as shown in Figure 175.

![Backup Report](image)

**Figure 175.** Backup status report emailed to cloud user on request

**Note:** DPA is required for the backup report.
Chapter 7 Administration Scenarios

This chapter presents the following topics:

Overview ................................................................................................................. 147
Scenario 1: Single site with backup ........................................................................ 147
Scenario 2: Dual site CA with replicated backup .................................................... 150
Scenario 3: Dual-site SRM DR with replicated backup ........................................... 153
Overview

This chapter presents some common scenarios that an Enterprise Hybrid Cloud administrator might need to perform. The scenarios are presented as high level steps and explain the sequence of events required to initialize and update sample Enterprise Hybrid Cloud configurations.

Setup and integration of the cloud components in the Enterprise Hybrid Cloud Object Model are performed on Day 2 and after. vRealize Automation cloud administrators use their service catalog, when it has been populated, to initialize and update their environment.

Scenario 1: Single site with backup

Overview

The Enterprise Hybrid Cloud administrator wants to set up a single site with backup services, where the following are present:

- Single site
- Single vCenter
- Single hardware island
- Local-only cluster
- Single Avamar grid with proxies

Prerequisites

The following requirements must be met for this scenario:

- vCenter Endpoint Cloud-VC01 is added to the vRealize Orchestrator vCenter plug-in.
- ViPR virtual array NY-HWI-1-vArray1 has been created.
- Local cluster NY-HWI-1-C1 has been created in Cloud-VC01.
- Avamar grid NY-AV1 is online.
- Avamar proxies are deployed.
Figure 176 shows the required steps to set up a single site with backup.

The following scenario outlines the steps required to set up an environment with the elements shown in Figure 177.
Follow these steps to complete scenario 1:

1. Add the site:
   a. Run the Site Maintenance catalog item.
   b. Select Add Site—**NewYork**.

2. Add a vCenter endpoint:
   a. Run the vCenter Endpoint Maintenance catalog item.
   b. Select **Add vCenter**:
      i. Enter the vCenter name—**Cloud-VC01**.
      ii. Select the vCenter FQDN (populated from the vRealize Orchestrator vCenter plug-in).
      iii. Select Associated site—**NewYork** (populated by the Site Maintenance workflow).
      iv. Select vCenter Datacenter (populated from the vRealize Orchestrator vCenter plug-in).

3. Add a hardware island:
   a. Run the Hardware Island Maintenance catalog item.
   b. Select **Add Hardware Island**:
      i. Enter the hardware island name—**NewYork-HWI-1**.
      ii. Select the associated vCenter—**Cloud-VC01** (populated from the vRealize Orchestrator vCenter plug-in).
      iii. Select the associated site—**NewYork** (populated by the Site Maintenance workflow).
      iv. Select the ViPR instance (populated from the Enterprise Hybrid Cloud Object Model).
      v. Select the associated ViPR virtual array(s) —**NY-HWI-1-vArray1** (populated from the vRealize Orchestrator ViPR plug-in).

4. Onboard the local cluster:
   a. Run the Cluster Maintenance catalog item.
   b. Select **Onboard Local Cluster**.
   c. Select Hardware Island—**NewYork-HWI-1**.
   d. Select unprepared local cluster—**NY-HWI-1-C1**.

5. Add the New York Avamar grid:
   a. Run the Avamar Grid Maintenance catalog item.
   b. Select **Add Avamar Grid**.
   c. Enter the Avamar grid name—**NY-AV1**.
   d. Enter the grid FQDN.
   e. Enter the admin credentials.
   f. Select proxies.
   g. Select the associated site—**NewYork** (populated by the Site Maintenance workflow).
h. Enter Avamar Simple Object Access Protocol (SOAP) credentials.

6. Add the ASR:
   a. Run the Avamar Site Relationship (ASR) Maintenance catalog item.
   b. Select Add an ASR.
   c. Select 1C1VC (One backup copy. Virtual machines on one site only).
   d. Select ASR site—NewYork.

7. Add the ARR:
   a. Run the Avamar Replication Relationship (ARR) Maintenance catalog item.
   b. Select Add an ARR.
   c. Select the 1C1VC ASR created in step 6.

8. Select the Avamar grid that was added in step 5.

9. Associate the local cluster with ASR:
   a. Run the Cluster Maintenance catalog item.
   b. Select Associate Cluster to ASR.
   c. Select local cluster—NY-HWI-1-C1.
   d. Select the relevant ASR (only ASRs matching the cluster type are shown).

10. Deploy Avamar proxies to the cluster using the Deploy Avamar proxy catalog item (or associate existing proxies to the cluster using the Cluster Maintenance catalog item).

11. Provision local datastore using the Provision Cloud Storage catalog item.

Scenario 2: Dual site CA with replicated backup

Overview

The Enterprise Hybrid Cloud administrator wants to set up a dual-site CA environment with data protection backup services, as shown in Figure 178. The following scenario outlines the steps required to set up an environment with the following (additional to Scenario 1):

- Two sites
- One vCenter
- Two hardware islands
- Local-only cluster on one site
- CA cluster across sites
- A single Avamar grid at each site
The following prerequisites are required for scenario 2:

- Scenario 1 has been completed.
- vCenter Endpoint Cloud-VC01 is added to the vRealize Orchestrator vCenter plug-in.
- ViPR virtual arrays NY-HWI-1-vArray1 and BOS-HWI-1-vArray1 have been created.
- CA cluster NY-BOS-CA-C1 has been created in Cloud-VC01.
- Avamar grids NY-AV1 and BOS-AV1 are online.

Figure 179 shows the required steps to set up a dual site CA environment with replicated backup.
Setup steps

Follow the steps below to complete scenario 2:

1. Add the second site:
   a. Run the Site Maintenance catalog item.
   b. Select Add Site—Boston.

2. Update vCenter endpoint:
   a. Run the vCenter Endpoint Maintenance catalog item.
   b. Select Update vCenter:
      i. Select vCenter to update—Cloud-VC01.
      ii. Select vCenter FQDN (populated from the vRealize Orchestrator vCenter plug-in).
      iii. Select vCenter Datacenter (populated from the vRO vCenter plug-in).
      iv. Select site to add—Boston (populated by the Site Maintenance workflow).

3. Add a hardware island:
   a. Run the Hardware Island Maintenance catalog item.
   b. Select Add Hardware Island.
      i. Enter the hardware island name—Boston-HWI-1.
      ii. Select the associated vCenter—Cloud-VC01 (populated from the vRealize Orchestrator vCenter plug-in).
      iii. Select the associated site—Boston (populated by the Site Maintenance workflow).
      iv. Select the ViPR instance (populated from the Enterprise Hybrid Cloud Object Model).
      v. Select the associated ViPR virtual array(s)—BOS-HWI-1-vArray1 (populated from the vRealize Orchestrator ViPR plug-in).

4. Onboard the CA cluster:
   a. Run the Cluster Maintenance catalog item.
   b. Select Onboard CA Cluster.
   c. Select Hardware Island 1—NewYork-HWI-1.
   d. Select unprepared CA cluster—NY-BOS-CA-C1.
   e. Select Inter-site (Intra-site would be selected for single site CA).
   f. Select Hardware Island 2—Boston-HWI-1.
   g. Select the hosts from hardware island 1—Hosts from NewYork-HWI-1.
   h. Select the hosts from hardware island 2—Hosts from Boston-HWI-1.

5. Add the Boston Avamar grid:
   a. Run the Avamar Grid Maintenance catalog item.
   b. Select Add Avamar Grid.
   c. Enter the Avamar grid name—BOS-AV1.
   d. Enter the grid FQDN.
e. Enter admin credentials.
f. Select proxies.
g. Select the associated site—**Boston** (populated by the Site Maintenance workflow).
h. Enter Avamar SOAP credentials.

6. Add the ASR:
   a. Run the Avamar Site Relationship (ASR) Maintenance catalog item.
   b. Select **Add an ASR**.
   c. Select 2C1VC (Two backup copies. Virtual machines move between two sites).
   d. Select first ASR site—**New York**.
   e. Select second ASR site—**Boston**.

7. Add the ARR.
   a. Run the Avamar Replication Relationship (ARR) Maintenance catalog item.
   b. Select **Add an ARR**.
   c. Select the 2C1VC ASR created in step 6.
   d. Select site 1 Avamar grid—**NY-AV1**.
   e. Select site 2 Avamar grid—**BOS-AV1**.

8. Associate the CA cluster with ASR:
   a. Run the Cluster Maintenance catalog item.
   b. Select **Associate Cluster to ASR**.
   c. Select CA cluster—**NY-BOS-CA-C1**.
   d. Select the 2C1VC ASR created in step 6 (Only ASRs matching the cluster type are shown).

9. Deploy Avamar proxies to the cluster using the Deploy Avamar proxy catalog item (or associate existing proxies to the cluster using the cluster maintenance catalog item).


When complete, you can create a backup service level with Avamar replication and deploy CA protected virtual machines with data protection.

---

**Scenario 3: Dual-site SRM DR with replicated backup**

**Overview**

The Enterprise Hybrid Cloud administrator wants to set up a dual site VMware vCenter SRM DR environment with data protection backup services, as shown in Figure 180. The following scenario outlines the steps required to set up an environment with the following (additional to scenario 1):

- Two sites
- Two vCenters
- Two hardware islands
Chapter 7: Administration Scenarios

- Local-only cluster on one site
- DR-protected cluster at each site
- A single Avamar grid at each site

![Figure 180. Dual Site SRM DR with backup](image)

**Prerequisites**

The following are required for scenario 3:

- Scenario 1 has been completed.
- vCenter Endpoint Cloud-VC02 is added to the vRealize Orchestrator vCenter plug-in.
- ViPR virtual arrays NY-HWI-1-vArray1 and BOS-HWI-1-vArray1 have been created.
- DR clusters NY-SEA-DR-C1 and SEA-NY-DR-C1 have been created in Cloud-VC01 and Cloud-VC02 respectively.
- Avamar grids NY-AV1 and SEA-AV1 are online.

**Setup steps**

*Note:* Scenario 3 is independent of scenario 2 as CA and SRM DR in the same environment is not a supported Enterprise Hybrid Cloud topology.

Follow the steps below to complete scenario 3:

1. Add the second site:
   a. Run the Site Maintenance catalog item.
   b. Select Add Site—Seattle.

2. Add the vCenter endpoint:
   a. Run the vCenter Endpoint Maintenance catalog item.
   b. Select Add vCenter:
      i. Enter the vCenter name—Cloud-VC02.
      ii. Select vCenter FQDN (populated from the vRealize Orchestrator vCenter plug-in).
iii. Select vCenter Datacenter (populated from the vRealize Orchestrator vCenter plug-in).

iv. Select site to associate—Seattle (populated by the Site Maintenance workflow).

3. Add the vCenter relationship:
   a. Run the vCenter Relationship Maintenance catalog item.
   b. Select Add SRMDR vCenter Relationship:
      i. Enter the vCenter protected and recovery vCenters.
      ii. Enter NSX manager details (if present).
      iii. Enter SRM details.
      iv. Enter SRM SQL details.
      v. Enter SRM SOAP details.

4. Add a hardware island:
   a. Run the Hardware Island Maintenance catalog item.
   b. Select Add Hardware Island:
      i. Enter the hardware island name—Seattle-HWI-1.
      ii. Select the associated vCenter—Cloud-VC02 (populated from the vRealize Orchestrator vCenter plug-in).
      iii. Select the associated site—Seattle (populated by the Site Maintenance workflow).
      iv. Select a ViPR instance (populated from the Enterprise Hybrid Cloud Object Model).
      v. Select associated ViPR virtual array(s)—SEA-HWI-1-vArray1 (populated from the vRealize Orchestrator ViPR plug-in).

5. Onboard DR clusters:
   a. Run the Cluster Maintenance catalog item.
   b. Select Onboard DR Cluster.
   c. Select protected cluster hardware island—NewYork-HWI-1.
   d. Select unprepared DR cluster—NY-SEA-DR-C1.
   e. Select recovery cluster hardware island—Seattle-HWI-1.
   f. Select unprepared DR cluster—SEA-NY-DR-C1.

6. Add the Seattle Avamar grid:
   a. Run the Avamar Grid Maintenance catalog item.
   b. Select Add Avamar Grid.
   c. Enter the Avamar grid name—SEA-AV1.
   d. Enter the grid FQDN.
   e. Enter the admin credentials.
   f. Select proxies.
   g. Select associated site—Seattle (populated by the Site Maintenance workflow).
Chapter 7: Administration Scenarios

7. Add the ASR:
   a. Run the Avamar Site Relationship (ASR) Maintenance catalog item.
   b. Select **Add an ASR**.
   c. Select 2C2VC (Two backup copies. Virtual machines move between two sites/vCenters).
   d. Select first ASR site — **New York**.
   e. Select second ASR site— **Seattle**.

8. Add the ARR:
   a. Run the Avamar Replication Relationship (ARR) Maintenance catalog item.
   b. Select **Add an ARR**.
   c. Select the 2C2VC ASR created in step 6.
   d. Select site 1 Avamar grid— **NY-AV1**.
   e. Select site 2 Avamar grid— **SEA-AV1**.

9. Associate the DR cluster with ASR:
   a. Run the Cluster Maintenance catalog item.
   b. Select **Associate Cluster to ASR**.
   c. Select CA cluster— **NY-BOS-CA-C1**.
   d. Select the 2C1VC ASR created in step 6 (Only ASRs matching the cluster type are shown).

10. Deploy Avamar proxies to the clusters using the Deploy Avamar proxy catalog item (or associate existing proxies to the cluster using the cluster maintenance catalog item).

11. Provision a DR protected datastore using the Provision Cloud Storage catalog item.

When complete, you can create a backup service level with Avamar replication and deploy VMware SRM DR protected virtual machines with data protection.
This chapter presents the following topics:

Summary ............................................................................................................... 158
Summary

Enterprise Hybrid Cloud is the bridge between the applications of today (Platform 2) and the social, mobile, analytics, and cloud applications of the future (Platform 3). It empowers IT to be a broker of cloud services, providing the control and visibility that IT organizations need and the on-demand self-service that developers and application users expect.

The data protection and recovery plans chapters in this guide discussed some of the data protection services available with Enterprise Hybrid Cloud. The use cases presented data protection scenarios addressing requirements for backup, CA, and DR. These services are available to various cloud users, from those responsible for the administration and management of data protection services to end users who consume the data protection services for their virtual machines and applications. These data protection solutions are optional for Enterprise Hybrid Cloud and require additional resources on top of the foundation solution.

Enterprise Hybrid Cloud users can easily provision standardized services directly from an application marketplace portal, with upfront pricing. Delivery of these resources from private and public clouds, whatever the workload calls for, is built on policies set by IT, which ensures application workloads are placed in the right cloud, with the right cost, security, and performance.
This chapter presents the following topic:

Documentation

160
Chapter 9: References

Documentation

The following documents, available on EMC Online Support or EMC.com, provide additional, relevant information. If you do not have access to a document, contact your Dell EMC representative.

- Enterprise Hybrid Cloud 4.1.1: Concepts and Architecture Guide
- Enterprise Hybrid Cloud 4.1.1: Reference Architecture Guide
- Enterprise Hybrid Cloud 4.1.1: Infrastructure and Operations Management Guide

For additional information, see the following document on the VMware documentation website:

- vRealize Automation Installation and Configuration