## CONTENTS

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 1</td>
<td>ViPR Controller VDC Requirements and Information Overview</td>
<td>7</td>
</tr>
<tr>
<td>Chapter 2</td>
<td>ViPR Controller user role requirements</td>
<td>9</td>
</tr>
<tr>
<td>Chapter 3</td>
<td>Physical Asset Requirements and Information</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>Storage systems</td>
<td>14</td>
</tr>
<tr>
<td></td>
<td>EMC VMAX</td>
<td>14</td>
</tr>
<tr>
<td></td>
<td>EMC VNX for Block</td>
<td>14</td>
</tr>
<tr>
<td></td>
<td>EMC Unity</td>
<td>14</td>
</tr>
<tr>
<td></td>
<td>VPXES</td>
<td>15</td>
</tr>
<tr>
<td></td>
<td>Hitachi Data Systems</td>
<td>15</td>
</tr>
<tr>
<td></td>
<td>Known issues with provisioning</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td>Enable performance data logging of HDS storage arrays in Storage</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td>Navigator</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td>Create a new user using the Storage navigator on HDS</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td>Host mode and host mode options</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td>Third-party block storage (OpenStack)</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>Third-party block storage provider installation requirements</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>Third-party block storage system support</td>
<td>21</td>
</tr>
<tr>
<td></td>
<td>Supported ViPR Controller operations</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>OpenStack configuration</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>Cinder service configuration requirements</td>
<td>23</td>
</tr>
<tr>
<td></td>
<td>VM sizing guidelines for arrays accessed by ViPR Controller through</td>
<td>23</td>
</tr>
<tr>
<td></td>
<td>Cinder</td>
<td>23</td>
</tr>
<tr>
<td></td>
<td>Storage system (backend) configuration settings</td>
<td>23</td>
</tr>
<tr>
<td></td>
<td>Volume setup requirements for OpenStack</td>
<td>24</td>
</tr>
<tr>
<td></td>
<td>ViPR Controller configuration for third-party block storage ports</td>
<td>25</td>
</tr>
<tr>
<td></td>
<td>Stand-alone EMC ScaleiO</td>
<td>26</td>
</tr>
<tr>
<td></td>
<td>EMC XtremiO</td>
<td>26</td>
</tr>
<tr>
<td></td>
<td>Support for IBM XIV</td>
<td>26</td>
</tr>
<tr>
<td></td>
<td>Dell SC Series</td>
<td>27</td>
</tr>
<tr>
<td></td>
<td>EMC VNxE</td>
<td>29</td>
</tr>
<tr>
<td></td>
<td>General file storage system requirements</td>
<td>29</td>
</tr>
<tr>
<td></td>
<td>EMC® Data Domain®</td>
<td>29</td>
</tr>
<tr>
<td></td>
<td>EMC Isilon</td>
<td>30</td>
</tr>
<tr>
<td></td>
<td>NetApp 7-mode</td>
<td>33</td>
</tr>
<tr>
<td></td>
<td>NetApp Cluster-mode</td>
<td>33</td>
</tr>
<tr>
<td></td>
<td>EMC VNX for File</td>
<td>33</td>
</tr>
<tr>
<td></td>
<td>vNAS discovery and project assignment</td>
<td>33</td>
</tr>
<tr>
<td></td>
<td>EMC Elastic Cloud Storage</td>
<td>34</td>
</tr>
<tr>
<td></td>
<td>RecoverPoint systems</td>
<td>35</td>
</tr>
<tr>
<td></td>
<td>Fabric Managers (switches)</td>
<td>36</td>
</tr>
<tr>
<td></td>
<td>ViPR Controller switch and network terminology</td>
<td>36</td>
</tr>
<tr>
<td></td>
<td>Brocade</td>
<td>36</td>
</tr>
<tr>
<td></td>
<td>Cisco</td>
<td>40</td>
</tr>
<tr>
<td></td>
<td>Vblock system requirements</td>
<td>44</td>
</tr>
<tr>
<td></td>
<td>Compute image server requirements</td>
<td>45</td>
</tr>
<tr>
<td></td>
<td>Compute image server network requirements</td>
<td>46</td>
</tr>
<tr>
<td></td>
<td>Compute images</td>
<td>46</td>
</tr>
</tbody>
</table>
Vblock compute systems................................................................. 47
Hosts and clusters.........................................................................................48
Support for Host/Array Affinity for VMAX, VNX for Block, Unity, and
XtremIO storage systems..................................................................48
AIX hosts and AIX VIO Servers.......................................................... 48
HP-UX .............................................................................................. 48
Linux ................................................................................................... 49
Windows ..........................................................................................49
SUN-VCS .......................................................................................... 51
VMware® vCenter..................................................................................51
Required VMware® VirtualCenter role privileges...............................52
FAQs for vCenters discovered and managed in ViPR Controller....... 52
Host/array affinity discovery for unmanaged volumes................................... 53
Virtual Asset Requirements and Information 57
Overview....................................................................................................... 58
Plan to build your virtual array............................................................... 58
SAN zoning requirements.......................................................................... 58
Plan how to add the physical assets to the virtual array.............................58
Virtual array configuration considerations for ECS systems................ 60
Virtual Array requirements for Vblock system services...................... 60
Block storage configuration considerations................................................. 61
Block storage systems under ViPR Controller management................. 62
Hitachi Data Systems ........................................................................... 62
EMC VPLEX ...................................................................................... 63
XtremIO .............................................................................................. 63
Third-party block (OpenStack) storage systems................................. 64
File storage configuration considerations.................................................. 64
EMC® Data Domain® ........................................................................... 64
EMC VNX for File .............................................................................. 65
Object storage configuration considerations.............................................. 65
ECS .................................................................................................. 65
ViPR requirements for service profile templates........................................ 65
Selecting Storage Pools for Provisioning 67
Overview....................................................................................................... 68
Understanding pool utilization and subscription...................................... 68
Block storage resource placement options.............................................. 69
Default selection process for block storage............................................ 69
Host/array affinity resource placement.................................................. 71
Selection process for file storage............................................................... 73
Administering Vblock Systems with ViPR Controller 75
Administering Vblock systems in your ViPR Controller virtual data center...... 76
How Vblock systems are discovered by ViPR Controller........................ 76
Add Vblock system components to ViPR Controller physical assets........ 77
ViPR Controller discovery of Vblock system components.................... 78
ViPR Controller registration of added and discovered physical assets....... 79
Additional resources required by ViPR Controller for OS installation on
Vblock systems...................................................................................... 79
How Vblock system components are virtualized in ViPR Controller........ 79
Chapter 4
Virtual Asset Requirements and Information

Chapter 5
Selecting Storage Pools for Provisioning

Appendix A
Administering Vblock Systems with ViPR Controller
CHAPTER 1

ViPR Controller VDC Requirements and Information Overview

This guide is for ViPR Controller System Administrators and Tenant Administrators to understand the information needed to configure the physical assets that are added to the ViPR Controller Virtual Data Center (VDC), as well as the requirements and information to convert the ViPR Controller physical assets, discovered by the ViPR Controller, into the ViPR Controller networks, virtual arrays, and virtual pools of the ViPR Controller VDC.

Related documents
Refer to the following guides for UI steps, CLI commands, and REST API calls to configure your virtual data center:

- *ViPR Controller User Interface Virtual Data Center Configuration Guide*
- *ViPR Controller CLI Reference Guide*
- *EMC ViPR Controller REST API Reference*

The provides the version requirements for the physical assets.

All of these documents are accessible from the ViPR Controller Product Documentation Index.
CHAPTER 2

ViPR Controller user role requirements

ViPR Controller roles fall into two groups: roles that exist at the ViPR Controller virtual data center level, and roles that exist at the tenant level.

Note
Access to different areas of the ViPR Controller UI is governed by the actions permitted to the role assigned to the user. The actions authorized when you access ViPR Controller from the UI can differ (be more constrained) from those available when you use the REST API or CLI.

Virtual data center-level roles
VDC roles are used to set up the ViPR Controller environment which is shared by all tenants. The following table lists the authorized actions for each user role at the virtual data center level.

Table 1 VDC roles

<table>
<thead>
<tr>
<th>VDC Role</th>
<th>Authorized Actions</th>
</tr>
</thead>
</table>
| Security Administrator | • Manages the authentication provider configuration for the ViPR Controller virtual data center to identify and authenticate users. Authentication providers are configured to:  
  ▪ Use Active Directory/Lightweight Directory Access Protocol (AD/LDAP) user accounts/domains to add specified users into ViPR Controller.  
  ▪ Register ViPR Controller as block storage service in Openstack (Keystone).  
    Note  
    Security Administrator role is required to add Keystone, but Keystone users cannot be added into ViPR Controller.  
  • Creates ViPR Controller User Groups.  
  • Assigns VDC and Tenant roles.  
  • Sets ACL assignments for Projects, and Service Catalog.  
  • Sets ACL assignments for virtual arrays, and virtual pools, from the ViPR Controller API and CLI.  
  • Update vCenter Tenants (ACLs) and Datacenter Tenant from ViPR Controller REST API and CLI (Only System Administrators can perform any of these functions from the ViPR Controller UI).  
  • Creates, modifies, and deletes sub-tenants.  
  • Assigns the tenant quotas, and user mappings.  
  • Manages ViPR Controller virtual data center software and license updates. |
### Table 1 VDC roles (continued)

<table>
<thead>
<tr>
<th>VDC Role</th>
<th>Authorized Actions</th>
</tr>
</thead>
</table>
|                               | • Configures the repository from which ViPR Controller upgrade files will be downloaded and installed.  
• Manages SSL, and trusted certificates.  
• Can change IPs for ViPR Controller nodes deployed on VMware without a vApp, and Hyper-V.  
• Schedule backups of ViPR Controller instances.  
• Reset local user passwords.  
• Configures ACLs.  
• Restores access to tenants and projects, if needed. (For example, if the Tenant Administrator locks himself/herself out, the Security Administrator can reset user roles to restore access.)  
• Can add or change ViPR Controller node names.  
• Initiate a minority node recovery from the ViPR Controller REST API, and CLI.  
• View the minority node recovery status from the ViPR Controller CLI.  
• Make changes to the ViPR Controller, General Configuration, Security settings.  
• Shuts down, reboots, and restarts ViPR Controller services from the ViPR Controller REST API/CLI.  
• Manages IPsec actions, such as rotate IPsec key, check IPsec status.  
• The Security Administrator must also be assigned a System Administrator role to perform the following operations from the ViPR Controller UI:  
  • Shut down, reboot, and restart ViPR Controller nodes or services.  
  • Set ACL assignments for virtual arrays, and virtual pools.  
  • Initiate a minority node recovery.  
• In Geo-federated Environment:  
  • Has Security Administrator privileges on authentication providers, which are global resources.  
• System Administrator  
  • Performs system upgrades.  
  • Creates system backups  
  • Add ViPR Controller licenses.  
  • Send support requests.  
  • Add, edit, delete, disconnect, and reconnect virtual data centers (VDCs).  
  • Sets up the physical storage infrastructure of the ViPR Controller virtual data center and configures the physical storage into two types of virtual resources: virtual arrays and virtual pools. Authorized actions include:  
    • Adding, modifying, and deleting the following physical storage resources into ViPR Controller such as storage systems, storage ports, and storage pools, data protections systems, fabric managers, networks, compute images, Vblock compute systems, and vCenters.
Table 1 VDC roles (continued)

<table>
<thead>
<tr>
<th>VDC Role</th>
<th>Authorized Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note</strong></td>
<td>System Administrators cannot add, delete, or modify hosts or clusters.</td>
</tr>
<tr>
<td></td>
<td>- Updating vCenter cascade tenancy and vCenter tenants (ACLs) and Datacenter Tenant from the ViPR Controller REST API, UI and CLI.</td>
</tr>
<tr>
<td></td>
<td>- Associate a vNAS server to one or more projects (Requires both the System and Tenant Administrator roles).</td>
</tr>
<tr>
<td></td>
<td>- Creating virtual pools.</td>
</tr>
<tr>
<td></td>
<td>- Creating virtual arrays.</td>
</tr>
<tr>
<td></td>
<td>- Creating mobility groups.</td>
</tr>
<tr>
<td></td>
<td>- Manages the ViPR Controller virtual data center resources that tenants do not manage.</td>
</tr>
<tr>
<td></td>
<td>- Retrieves ViPR Controller virtual data center status and health information.</td>
</tr>
<tr>
<td></td>
<td>- Retrieves bulk event and statistical records for the ViPR Controller virtual data center.</td>
</tr>
<tr>
<td></td>
<td>- View the Database Housekeeping Status.</td>
</tr>
<tr>
<td></td>
<td>- View the minority node recovery status from the ViPR Controller CLI.</td>
</tr>
<tr>
<td></td>
<td>In Geo-federated Environment:</td>
</tr>
<tr>
<td></td>
<td>- Adds a VDC to create Geo-federated environment</td>
</tr>
<tr>
<td></td>
<td>- Add, disconnect, reconnect, or delete a VDC</td>
</tr>
<tr>
<td></td>
<td>- Has System Administrator privileges on global virtual pools, which are global resources.</td>
</tr>
<tr>
<td></td>
<td>- Sets ACL assignments for virtual arrays, and virtual pools, from the ViPR Controller API</td>
</tr>
<tr>
<td>System Monitor</td>
<td>- Has read-only access to all resources in the ViPR Controller virtual data center. Has no visibility into security-related resources, such as authentication providers, ACLs, and role assignments.</td>
</tr>
<tr>
<td></td>
<td>- Retrieves bulk event and statistical records for the ViPR Controller virtual data center.</td>
</tr>
<tr>
<td></td>
<td>- Retrieves ViPR Controller virtual data center status and health information.</td>
</tr>
<tr>
<td></td>
<td>- (API only) Can create an alert event, with error logs attached, as an aid to troubleshooting. The alert event is sent to ConnectEMC.</td>
</tr>
<tr>
<td></td>
<td>- View the Database Housekeeping Status.</td>
</tr>
<tr>
<td></td>
<td>- View the minority node recovery status from the ViPR Controller UI, and CLI.</td>
</tr>
<tr>
<td></td>
<td>- List backups from external server.</td>
</tr>
<tr>
<td></td>
<td>- Check upload status of a backup.</td>
</tr>
<tr>
<td></td>
<td>- Check restore status.</td>
</tr>
<tr>
<td>System Auditor</td>
<td>Has read-only access to the ViPR Controller virtual data center audit logs.</td>
</tr>
</tbody>
</table>

11
Tenant-level roles

Tenant roles are used to administrate the tenant-specific settings, such as the service catalog and projects, and to assign additional users to tenant roles. The following table lists the authorized actions for each user role at the tenant level.

Table 2 Tenant roles

<table>
<thead>
<tr>
<th>Tenant-Level Role</th>
<th>Authorized Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tenant Administrator</td>
<td>• Becomes Tenant Administrator of created tenant.</td>
</tr>
<tr>
<td></td>
<td>• A single-tenant enterprise private cloud environment has only one tenant, the Provider Tenant, and Tenant Administrators have access to all projects.</td>
</tr>
<tr>
<td></td>
<td>• Modifies the name and description of the tenants.</td>
</tr>
<tr>
<td></td>
<td>• Add vCenters to ViPR Controller physical assets in their own tenant.</td>
</tr>
<tr>
<td></td>
<td>• Manages tenant resources, such as Hosts, Clusters vCenters, and Projects.</td>
</tr>
<tr>
<td></td>
<td>• Configures ACLs for projects and the Service Catalog in their tenant.</td>
</tr>
<tr>
<td></td>
<td>• Assigns roles to tenant users. (Can assign Tenant Administrator or Project Administrator roles to other users.)</td>
</tr>
<tr>
<td></td>
<td>• Create Schedule Policies.</td>
</tr>
<tr>
<td></td>
<td>• Associate a vNAS server to one or more projects (Requires both the System and Tenant Administrator roles).</td>
</tr>
<tr>
<td></td>
<td>• Manage application services.</td>
</tr>
<tr>
<td></td>
<td>• Accept or decline actionable events</td>
</tr>
<tr>
<td></td>
<td>• Edit service order schedules.</td>
</tr>
</tbody>
</table>

Note

A user or group of users can be configured to have a Tenant Administrator role for Multiple Tenants. This user/group of users must belong to the Provider Tenant. However, they do not have to have the Tenant Administrator role in the provider tenant. This functionality can be used in multi-tenant environments in cases where a group of users needs to perform provisioning operations for multiple tenants and they do not want to use root user for these operations.

In Geo-federated Environment:

• Has Tenant Administrator privileges on tenants, which are global resources.

Tenant Approver

• Approves or rejects Service Catalog orders in their tenant.
• Views all approval requests in their tenant.

Project Administrator

• Creates projects in their tenant and obtains an OWN ACL on the created project.
CHAPTER 3
Physical Asset Requirements and Information

This chapter contains the following topics:

- Storage systems ................................................................. 14
- EMC VMAX ........................................................................ 14
- EMC VNX for Block ............................................................ 14
- EMC Unity .......................................................................... 14
- VPLEX ................................................................................ 15
- Hitachi Data Systems ........................................................... 15
- Third-party block storage (OpenStack) ................................. 20
- ViPR Controller configuration for third-party block storage ports........................................................................... 25
- Stand-alone EMC ScaleIO .................................................... 26
- EMC XtremIO ...................................................................... 26
- Support for IBM XIV ............................................................ 26
- Dell SC Series ...................................................................... 27
- EMC VNXe ......................................................................... 29
- General file storage system requirements ............................. 29
- EMC Elastic Cloud Storage ................................................. 34
- RecoverPoint systems ........................................................... 35
- Fabric Managers (switches) .................................................. 36
- Vblock system requirements ............................................... 44
- Hosts and clusters ............................................................... 48
- VMware® vCenter .............................................................. 51
- Host/array affinity discovery for unmanaged volumes ............. 53
Storage systems

You can review the ViPR Controller requirements and information necessary for entering user credentials and setting up port-based metrics for storage systems, and review the information needed for adding and configuring a storage system in ViPR Controller.

Storage system user credentials

When adding storage systems to ViPR Controller, you specify the credentials of the user who will access the storage system from ViPR Controller. These credentials are independent of the user who is currently logged into ViPR Controller. All ViPR Controller operations performed on a storage system are executed as the user who was given access to the storage system.

ViPR Controller operations require that the ViPR Controller user has administrative privileges. If there are additional credential requirements for a specific type of storage system, it is explained in more detail in the following storage-specific sections of this guide.

EMC VMAX

For the configuration requirements and information necessary to configure VMAX storage systems in the ViPR Controller physical and virtual assets, refer to the ViPR Controller Integration with VMAX and VNX Storage Systems Guide, which is available from the ViPR Controller Product Documentation Index.

EMC VNX for Block

For the configuration requirements and information necessary to configure VNX for Block storage systems in the ViPR Controller physical and virtual assets, refer to the ViPR Controller Integration with VMAX and VNX Storage Systems Guide, which is available from the ViPR Controller Product Documentation Index.

EMC Unity

Be aware of the following when using ViPR Controller to manage Unity storage systems.

RecoverPoint with Unity backed volumes

Limitations to the ViPR Controller support of RecoverPoint with Unity backed volumes:

- You can have one or more Unity storage system connected to 1 RecoverPoint system, however you cannot connect one Unity system to multiple RecoverPoint systems. If you attempt to connect a Unity storage system to multiple RecoverPoint systems, EMC Unity adds all the initiators from different RecoverPoint systems to the same host on Unity.
- RecoverPoint with Unity backed volumes is not supported with XtremelIO. You cannot create a source copy on Unity, and have the target copy on XtremelIO, and vice versa.

ViPR Controller Application support for Unity volumes

Limitations of support for Unity volumes in ViPR Controller applications:

- Unity volumes, which are included in subgroups, which have snapshots, cannot be removed or deleted from the subgroup. This is a Unity limitation, which ViPR Controller enforces. To work around this issue, first remove the snapshots and then proceed to remove the volumes from the subgroup.
• Application full copies are not supported by ViPR Controller for Unity volumes.

**VPLEX**

Before adding VPLEX storage systems to ViPR Controller, validate that the VPLEX environment is configured as follows:

• ViPR supports VPLEX in a Local or Metro configuration. VPLEX Geo configurations are not supported.

• Configure VPLEX metadata back-end storage.

• Create VPLEX logging back-end storage.

• Verify that the:
  - Storage systems to be used are connected to the networks containing the VPLEX back-end ports.
  - Hosts to be used have initiators in the networks containing the VPLEX front-end ports.

• Verify that logging volumes are configured to support distributed volumes in a VPLEX Metro configuration.

• It is not necessary to preconfigure zones between the VPLEX and storage systems, or between hosts and the VPLEX, except for those necessary to make the metadata backing storage and logging backing storage available.

• Use the SUN-VCS operating system type, when adding a SUN-VCS host to ViPR Controller, which will be provisioned with a VPLEX storage system. The host initiators for the SUN-VCS cluster must then be manually added to ViPR Controller.

**Hitachi Data Systems**

Before you add Hitachi Data Systems (HDS) storage to ViPR Controller, configure the storage as follows.

**Gather the required information**

Hitachi HiCommand Device Manager (HiCommand) is required to use HDS storage with ViPR Controller. You need to obtain the following information to configure and add the HiCommand manager to ViPR Controller.

**Table 3 Hitachi required information**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>A host or virtual machine for HiCommand</td>
<td></td>
</tr>
<tr>
<td>Device Manager setup</td>
<td></td>
</tr>
<tr>
<td>HiCommand Device Manager license</td>
<td></td>
</tr>
<tr>
<td>HiCommand Device Manager host address</td>
<td></td>
</tr>
<tr>
<td>HiCommand Device Manager user credentials</td>
<td></td>
</tr>
<tr>
<td>HiCommand Device Manager host port (default</td>
<td></td>
</tr>
<tr>
<td>is 2001)</td>
<td></td>
</tr>
</tbody>
</table>
General configuration requirements

- HiCommand Device Manager software must be installed and licensed.
- Create a HiCommand Device Manager user for ViPR Controller to access the HDS storage. This user must have administrator privileges to the storage system to perform all ViPR Controller operations.
- HiCommand Device Manager must discover all Hitachi storage systems (that ViPR Controller will discover) before you can add them to ViPR Controller.
- When you add the HiCommand Device Manager as a ViPR Controller storage provider, all the storage systems that the storage provider manages will be added to ViPR Controller. If you do not want ViPR Controller to manage all the storage systems, before you add the HiCommand Device Manager, configure the HiCommand Device Manager to manage only the storage systems that will be added to ViPR Controller.

**Note**
After you add the storage provider to ViPR Controller, you can deregister or delete storage systems that you will not use in ViPR Controller.

Configuration requirements for auto-tiering

ViPR Controller provides auto-tiering for the six standard HDS auto-tiering policies for Hitachi Dynamic Tiering (HDT) storage pools.

HDS auto-tiering requires the Hitachi Tiered Storage Manager license on the HDS storage system.

Configuration requirements for data protection features

HDS protection requires:

- Hitachi Thin Image Snapshot software for snapshot protection
- Hitachi Shadow Image Replication software for clone and mirror protection.

ViPR Controller requires the following is configured to use the Thin Image, and ShadowImage features:

- Requires Hitachi Replication Manager is installed on a separate server.
- The HiCommand Device Manager agent must be installed and running on a pair management server.
- To enable ViPR Controller to use the Shadow Image pair operations, create a ReplicationGroup on the HDS, named `ViPR-Replication-Group` using either the HiCommand Device Manager or Hitachi Storage Navigator.
- To enable ViPR Controller to use the Thin Image pair operations, create a SnapshotGroup on the HDS, named `ViPR-Snapshot-Group` using either the HiCommand Device Manager or Hitachi Storage Navigator.

Configuration requirements for ViPR Controller to collect HDS port metrics

Before ViPR Controller can collect statistical information for HDS storage ports, you must perform the following operations in the HDS Storage Navigator to enable performance logging on the storage system:

- Enable performance data logging of HDS storage on page 17
- Create a new user using Storage Navigator on HDS on page 18
- Enable the certificate on the HDS to access SMI-S in secure mode. For details, refer to the Using the SMI-S function section of the *Hitachi Command Suite Administrator Guide*. 
Known issues with provisioning

When provisioning storage from an HDS array using ViPR Controller, you may experience some issues. This section explains when these issues may occur and how to resolve them.

Placing multiple provisioning orders in the Service Catalog

If multiple orders are placed quickly in ViPR Controller or a user with modify permissions is active on the HiCommand Suite at the same time as the ViPR Controller provisioning orders, the following exception is generated:

```
Error 25005: Error occurred running HiCommand Device Manager command. An error occurred executing operation deleteSingleVolumeSnapshot. Caused by: Error response received with error code 6,400 and message "An error occurred during storage system processing. (error code 1 = "1", error code 2 = "5132", meaning = "The specified user ID is already logged on, or the previous logon was not properly terminated. Please try again later. (By default, the session/RMI time-out is one minute.)") If the configuration was changed, refresh the storage system information. If you do not have the permissions required to refresh the information, ask the storage system administrator to do it for you.
```

HDS automatic refresh

When the Hitachi device manager automatically refreshes its information from the array, it can interrupt ViPR Controller provisioning orders and generate this error message:

```
Operation failed due to the following error: Error response received with error code 7,473 and message "The storage system information ("VSP@10.247.55.244") is being updated."
```

In the HiCommand suite, you can turn off this automatic refresh option.

What to do

If you experience either of these two errors, rerun the order after a short period of time. If you continually experience these issues, review the HDS user accounts setup. By separating the HDS user accounts without modify permissions, you may resolve these issues.

Enable performance data logging of HDS storage arrays in Storage Navigator

Before you can set up the metrics-based port selection for HDS, you must enable performance data logging for the HDS storage arrays in Storage Navigator in order for ViPR Controller to collect statistical information about the storage ports.

Procedure

1. Log into the Storage Navigator.
2. Select Performance Monitor.
3. Click Edit Monitor Switch.
4. Enable Monitor Switch.
5. Set the Sample Interval.
Create a new user using the Storage navigator on HDS

To collect statistics using the embedded SMI-S provider, you must create a new user using the Storage Navigator on the Hitachi storage array.

**Procedure**

1. Log into the Storage Navigator.
2. Select Administrator.
3. Click User Groups.
5. Click Create User.

**Note**

The username and password must be the same as the HiCommand Device Manager credentials that ViPR Controller uses to discover the storage provider.

6. Type a User Name.
7. Type a Password.
8. Type the Account status.
9. Type the Authentication details.

**Host mode and host mode options**

ViPR Controller System Administrators can learn about the Hitachi Data Systems Host Mode and Host Mode Option, how ViPR Controller sets the Host Mode and Host Mode Option, the ViPR Controller configuration requirements for ViPR Controller to apply the settings, and the steps to customize the Host Mode Option using the ViPR Controller UI.

**Host Mode and Host Mode Options**

Host Modes are HDS flags which are set on HDS host groups when an HDS storage volume is exported to the host group. The Host Mode is used to optimize the connection and communication between HDS storage and the host to which the HDS volume has been exported.

The Host Mode Options are a set of flags which can be enabled or disabled to further optimize the Host Mode set on the HDS host groups.

Refer to the Hitachi Data Systems documentation for details about the HDS Host Mode, and Host Mode Options.

**How ViPR Controller sets the Host Mode**

By default, when ViPR Controller is used to export an HDS volume to an AIX, ESX, HP-UX, Linux, or Windows host, ViPR Controller sets the following Host Mode on the host group by determining the host operating system details.

**Table 4 ViPR Controller default settings for Host Modes**

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Default Host Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIX</td>
<td>0F AIX</td>
</tr>
<tr>
<td>ESX</td>
<td>21 VMware</td>
</tr>
</tbody>
</table>
Table 4 ViPR Controller default settings for Host Modes (continued)

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Default Host Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP-UX</td>
<td>03 HP</td>
</tr>
<tr>
<td>Linux</td>
<td>00 Standard</td>
</tr>
<tr>
<td>Windows</td>
<td>2C Windows Extension</td>
</tr>
</tbody>
</table>

Host Mode settings for "Other" hosts

When ViPR Controller is used to export an HDS volume to a host that was added to ViPR Controller as "Other," or to a host of which ViPR Controller cannot determine the type, the 00 Standard Host Mode is set on the host by the Hitachi HiCommand DM. 00 Standard is the HiCommand DM default Host Mode.

Changing the Host Mode

The ViPR Controller Host Mode settings are automatically set by ViPR Controller during an export operation, and you cannot change the ViPR Controller Host Mode settings. Once ViPR Controller has set the Host Mode on a host, you can use Hitachi Storage Navigator to change the Host Mode on the host.

Prior to ViPR Controller 2.2

ViPR Controller did not set the Host Mode for hosts prior to ViPR Controller 2.2. However, HiCommand Device Manager sets the 00 Standard Host Mode as the default on all HDS host groups.

If a host to which an HDS volume was exported by ViPR Controller, prior to ViPR Controller 2.2, is re-used by ViPR 2.2 or higher to export another HDS volume, the Host Mode will not be set by ViPR Controller on the host.

How ViPR Controller sets the Host Mode Option

By default, when ViPR Controller is used to export an HDS volume to an AIX, ESX, HP-UX, Linux, or Windows host, ViPR Controller sets the following Host Mode Options on the host group.

Table 5 ViPR Controller default settings for Host Mode Options

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Default Host Mode</th>
</tr>
</thead>
</table>
| AIX, Linux, Windows | 2 => VERITAS Database Edition/Advanced Cluster  
  22 => Veritas Cluster Server |
| ESX              | 54 => Support option for the EXTENDED COPY command  
  63 => Support option for the vStorage APIs based on T10 standards |
| HP-UX            | 12 => No display for ghost LUN                                                    |

Note

Refer to Hitachi storage system provisioning documentation for details about the Host Mode Options.
Host Mode Option settings for "Other," hosts
ViPR Controller does not set the Host Mode Option when ViPR Controller is used to export an HDS volume to a host that was added to ViPR Controller as "Other," or to a host of which ViPR Controller cannot determine the type.

Changing the Host Mode Option
The Host Mode Option is set on the host group the first time you export an HDS volume to the host. Once ViPR Controller has set the Host Mode Option on the host group, the Host Mode Option cannot be changed by ViPR Controller for example:

- If an HDS volume was exported to a host that was added to ViPR Controller as "Other," the Host Mode Option configured in ViPR Controller is not set on the host. If the type of host is changed in ViPR Controller from Other, to AIX, ESX, HP-UX, Linux, or Windows, and ViPR Controller is used to export another HDS volume to the same host, the Host Mode Options which are configured in ViPR Controller will not be set on the host by ViPR Controller, since it was not set on the host group the first time the volume was exported from ViPR Controller to that same host.

- If an HDS volume was exported to an AIX, ESX, HP-UX, Linux, or host, the Host Mode Options currently configured in ViPR Controller are set on the host. If the Host Mode Options are changed in ViPR Controller after the export, and ViPR Controller is used to export another HDS volume to the same host, the original Host Mode Options remain on the host, and are not configured with the new Host Mode Options.

Once the HDS volume has been exported to a host from ViPR Controller, you can change the Host Mode Setting from Hitachi Storage Navigator. If ViPR Controller is used to export another HDS volume to the same host after the Host Mode Option has been changed from Storage Navigator, ViPR Controller will reuse the Storage Navigator settings in the export.

Prior to ViPR 2.2
- The Host Mode options are only set to new host groups created using ViPR Controller 2.2 and higher.
- Prior to ViPR Controller 2.2, ViPR Controller did not set any Host Mode Options on HDS host groups.
- If a host group, that was created prior to ViPR Controller 2.2, is re-used by ViPR Controller, the ViPR Controller Host Mode Options are not set by ViPR Controller on the host group created prior to ViPR Controller 2.2.

Third-party block storage (OpenStack)
ViPR Controller uses the OpenStack Block Storage (Cinder) service to manage OpenStack supported block storage systems. Your OpenStack block storage systems must meet the following installation and configuration requirements before the storage systems in OpenStack, and the storage system's resources can be managed by ViPR Controller.

Third-party block storage provider installation requirements
Use the OpenStack Block Storage (Cinder) Service to add third-party block storage systems into ViPR Controller.

Supported Openstack installation platforms
Openstack installation is supported on the following platforms:
- Red Hat Enterprise Linux
- SUSE Enterprise Linux
• Ubuntu Linux

For a list of the supported platform versions, see Openstack documentation at: http://docs.openstack.org.

**OpenStack installation requirements**
You must install the following two components on either the same server or separate servers:

- OpenStack Identity Service (Keystone): Required for authentication
- OpenStack Block Storage (Cinder): The core service that provides all storage information.

For complete installation and configuration details, refer to the OpenStack documentation at: http://docs.openstack.org.

**ViPR Controller user requirements for OpenStack**
When using Openstack Liberty as the third-party provider in ViPR Controller the default Cinder user, which is entered while adding the Openstack storage provider to ViPR Controller, must have “admin” privileges. Refer to the Openstack documentation for steps to assign the default Cinder user with admin privileges.

**Third-party block storage system support**

You configure third-party storage systems on the OpenStack Block Storage Controller node (Cinder service).

**Supported third-party block storage systems**

ViPR Controller operations are supported on any third-party block storage systems tested by OpenStack that use Fibre Channel or iSCSI protocols.

**Non-supported storage systems**

ViPR Controller does not support third-party storage systems using:

- Proprietary protocols, such as Ceph.
- Drivers for block over NFS.
- Local drivers such as LVM.

ViPR Controller does not support these OpenStack supported storage systems and drivers:

- LVM
- NetAppNFS
- NexentaNFS
- RBD (Ceph)
- RemoteFS
- Scality
- Sheepdog
- XenAPINFS

Refer to www.openstack.org for information about OpenStack third-party storage systems.

**ViPR Controller native driver support and recommendations**

ViPR Controller provides limited support for third-party block storage. For full support of all ViPR Controller operations, it is recommended that you add and manage the following storage systems with ViPR Controller native drivers, and not use the OpenStack third-party block storage provider to add these storage systems to ViPR Controller:
EMC VMAX
EMC VNX for Block
EMC VPLEX
Hitachi Data Systems (with Fibre Channel only)

Add these storage systems directly in ViPR Controller using the storage system host address or the host address of the proprietary storage provider.

**Supported ViPR Controller operations**

You can perform ViPR Controller discovery and various service operations on third-party block storage systems.

You can perform these service operations on third-party block storage systems:

- Create Block Volume
- Export Volume to Host
- Create a Block Volume for a Host
- Expand block volume
- Remove Volume by Host
- Remove Block Volume
- Create Full Copy
- Create Block Snapshot
- Create volume from snapshot
- Remove Block Snapshot

**Note**

You cannot use the ViPR Controller **Create VMware Datastore** service to create a datastore from a block volume created by a third-party storage system. However, you can manually create datastores from third-party block volumes through the VMware vCenter.

**OpenStack configuration**

After installing the Keystone and Cinder services, you must modify the Cinder configuration file to include the storage systems to be managed by ViPR Controller. After modifying the configuration file, you must create the volume types to map to the backend drivers. These volume types are discovered as storage pools of a certain storage system in ViPR Controller.

**OpenStack third-party storage configuration recommendations**

Before adding the storage provider to ViPR Controller, configure the storage provider with only the storage systems to be managed by ViPR Controller through a third-party block storage provider. When the third-party block storage provider is added to the ViPR Controller Physical Assets, all storage systems managed by the OpenStack block storage service and supported by ViPR Controller are added to ViPR Controller.

If you included storage systems in the storage provider that will not be managed by ViPR Controller, you can deregister or delete those storage systems from ViPR Controller. However, it is a better practice to configure the storage provider for ViPR Controller integration before adding the storage provider to ViPR Controller.
Access to OpenStack UI
When ViPR Controller is added as block storage to Openstack, you cannot access the
Openstack UI until the ViPR Controller service are brought back up.

Cinder service configuration requirements
You must add an entry in the Cinder configuration file for each storage system to be
managed by ViPR Controller. This file is located in /etc/cinder/cinder.conf.

Cinder does not have any specific standards on backend driver attribute definitions. See
the vendor-specific recommendations on how to configure the cinder driver, which may
involve installing a vendor specific plugin or command line interface.

VM sizing guidelines for arrays accessed by ViPR Controller through Cinder
The following sizing guidelines apply when ViPR Controller accesses storage arrays
through Cinder.

These guidelines assume:
- The Cinder node is deployed as a separate Virtual Machine (VM).
- The Cinder node is available exclusively to ViPR Controller.

<table>
<thead>
<tr>
<th>Volumes</th>
<th>Number of Cores</th>
<th>Memory (in GB)</th>
<th>Disk space (in GB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000</td>
<td>1</td>
<td>1</td>
<td>15</td>
</tr>
<tr>
<td>10000</td>
<td>2</td>
<td>2</td>
<td>15</td>
</tr>
<tr>
<td>100000</td>
<td>3</td>
<td>3</td>
<td>15</td>
</tr>
</tbody>
</table>

The number of storage arrays and volume size does not impact the Cinder VM resource
configuration.

Storage system (backend) configuration settings
Cinder defines backend configurations in individual sections of the cinder.conf file to
manage the storage systems. Each section is specific to a storage system type.

Edit the cinder.conf file:

Procedure
1. Uncomment enabled_backends, which is commented by default, and add the
multiple backend names. In the following example, NetApp and IBM SVC are added as
backend configurations.

   enabled_backends=netapp-iscsi,ibm-svc-fc

2. Near the end of the file, add these storage system specific entries.

   [netapp-iscsi]
   #NetApp array configuration goes here
   [ibm-svc-fc]
   #IBM SVC array configuration goes here
3. Restart the Cinder service.

```
#service openstack-cinder-volume restart
```

**Volume setup requirements for OpenStack**

ViPR Controller has specific setup requirements for volumes created in OpenStack.

ViPR Controller requires that you do the following for each volume in OpenStack:

- Map the volume to the backend driver.
- Indicate if the volume is set for thin or thick provisioning.

**ViPR Controller-specific properties**

You can create volume types through Cinder CLI commands or the Dashboard (OpenStack UI). The properties required by ViPR Controller in the Cinder CLI for the volume type are:

- `volume_backend_name`
- `vipr:is_thick_pool=true`

**volume_backend_name**

The following example demonstrates the Cinder CLI commands to create volume types (NetApp, IBM SVC) and map them to the backend driver.

```
cinder --os-username admin --os-password <password> --os-tenant-name admin type-create "NetAPP-iSCSI"
cinder --os-username admin --os-password <password> --os-tenant-name admin type-key "NetAPP-iSCSI" set volume_backend_name=NetAppISCSI

cinder --os-username admin --os-password <password> --os-tenant-name admin type-create "IBM-SVC-FC"
cinder --os-username admin --os-password <password> --os-tenant-name admin type-key "IBM-SVC-FC" set volume_backend_name=IBMSVC-FC

cinder --os-username admin --os-password <password> --os-tenant-name admin extra-specs-list
```

**vipr:is_thick_pool=true**

By default, ViPR Controller sets the provisioning type of OpenStack volumes to thin during discovery. If the provisioning type is thick, you must set the ViPR Controller-specific property for thick provisioning to `true` for the volume type. If the provisioning type of the volume is thin, you do not need to set the provisioning type for the volume in OpenStack.

The following example demonstrates the Cinder CLI commands to create a volume type (NetApp), and define the provisioning type of the volume as thick.

```
cinder --os-username admin --os-password <password> --os-tenant-name admin --os-auth-url=http://<hostname>:35357/v2.0 type-create "NetAPP-iSCSI"
cinder --os-username admin --os-password <password> --os-tenant-name admin --os-auth-url=http://<hostname>:35357/v2.0 type-key "NetAPP-iSCSI" set volume_backend_name=NetAppISCSI

cinder --os-username admin --os-password <password> --os-tenant-name admin --os-auth-url=http://<hostname>:35357/v2.0 type-key "NetAPP-iSCSI" set vipr:is_thick_pool=true

cinder --os-username admin --os-password <password> --os-tenant-name admin --os-auth-url=http://<hostname>:35357/v2.0 extra-specs-list
```
Validate setup
Validate that OpenStack was configured correctly to create volumes for each of the added storage systems.

1. Create volumes for each type of volume created in OpenStack.
   You can create volumes in the OpenStack UI or the Cinder CLI. The Cinder CLI command to create a volume is:
   ```
cinder --os-username admin --os-tenant-name admin  --display-name <volume-name> --volume-type <volume-type-id> <size>
```

2. Check that the volumes are getting created on the associated storage system. For example, NetApp-iSCSI type volumes should be created only on the NetApp storage system.

**ViPR Controller configuration for third-party block storage ports**

The OpenStack API does not provide the storage port World Wide Port Name (WWPN) for Fibre Channel connected storage systems and the IQN for iSCSI connected storage systems. As a result, ViPR Controller cannot retrieve the storage port WWPNs or IQNs during discovery.

After ViPR Controller discovers a third-party block storage array, a default storage port is created for the storage system, and appears in the **Storage Port** page with the name **Default** and the storage port identifier of **Openstack+<storagesystemserialnumber>+Port+Default**.

**Fibre Channel configured storage ports**
ViPR Controller export operations cannot be performed on an FC connected storage system, which was added to ViPR Controller without any WWPNs assigned to the storage port. Therefore, ViPR Controller system administrators must manually add at least one WWPN to the default storage port before performing any export operations on the storage system. WWPNs can be added to ViPR Controller through the ViPR Controller CLI and UI.

After the WWPN is added to the storage port, you can perform export operations on the storage system from ViPR Controller. At the time of the export, ViPR Controller reads the export response from the Cinder service. The export response will include the WWPN, which was manually added by the system administrator from the ViPR Controller CLI, and any additional WWPNs listed in the export response. ViPR Controller then creates a storage port for each of the WWPNs listed in the export response during the export operation.

After a successful export operation is performed, the **Storage Port** page displays any newly created ports and the Default storage port.

Each time another export operation is performed on the same storage system, ViPR Controller reads the Cinder export response. If the export response presents WWPNs, which are not present in ViPR Controller, then ViPR Controller creates new storage ports for every new WWPN.

For steps to add WWPNs to FC connected third-party block storage ports, see the **ViPR Controller CLI Reference Guide**, which is available from the ViPR Controller Product Documentation Index.

**iSCSI configured storage ports**
The default storage port is used to support the storage system configuration until an export is performed on the storage system. At the time of the export, ViPR Controller reads the export response from the Cinder service, which includes the iSCSI IQN. ViPR Controller then modifies the default storage port’s identifier with the IQN received from the Cinder export response.
Each time another export operation is performed on the same storage system, ViPR Controller reads the Cinder export response. If the export response presents an IQN, which is not present in ViPR Controller, then ViPR Controller creates a new storage port.

Stand-alone EMC ScaleIO

Your stand-alone ScaleIO should meet the following system requirements and be configured as follows before adding the storage to ViPR Controller.

- Protection domains are defined.
- All storage pools are defined.

In addition, you must have the following:

- The IP address of the ScaleIO Gateway host.
- The port used to communicate with the ScaleIO REST API service.
- The username and password of a user who can access the Primary MDM.

EMC XtremIO

Before adding XtremIO storage to ViPR, ensure that there is physical connectivity between hosts, fabrics and the array.

If you are using ViPR Controller to manage RecoverPoint with XtremIO, be sure your configuration is set up as described in the RecoverPoint XtremIO Technical Notes which are provided from EMC Online Support.

Best practices

- When XtremIO is configured with vSphere native multipathing, configure vSphere NMP Round Robin as the default pathing policy for all XtremIO volumes, using the ESX command line. For details see the EMC XtremIO Storage Array Host Configuration Guide, which is available on EMC Online Support.
- If credentials are changed following the XtremIO upgrade, ensure that the username for the XtremIO storage provider in ViPR Controller matches the username in XtremIO. Usernames with capital letters are automatically converted to lowercase following the XtremIO upgrade. If necessary, change the username for the XtremIO storage provider in ViPR Controller to match the username in XtremIO. You must make this change in ViPR Controller. Changing the name in XtremIO will not solve this issue in ViPR Controller.

Support for IBM XIV

ViPR Controller manages XIV arrays using an SMI-S provider and (optionally) Hyper Scale Manager.

**VPLEX with IBM XIV backing volumes**

In earlier releases, IBM XIV could be used as a VPLEX backend storage system only if configured using OpenStack Cinder. Cinder is no longer a requirement. All VPLEX operations supported by ViPR Controller can be used when VPLEX is configured natively with IBM XIV backing volumes.

ViPR Controller supports the following configurations for VPLEX with IBM XIV backing volumes

- VPLEX Local volumes
- VPLEX Distributed volumes
- Consistency groups — volumes within a consistency group, or stand-alone volumes.

**Discovery, provisioning, and export**

Use either of these pages to configure the XIV storage system from the ViPR Controller user interface:

- **Physical > Storage Systems > Add**
- **Physical > Storage Providers > Add**

When configuring the storage system provider, choose one of two methods:

1. **SMI-S only**
   - SMI-S is required for storage provider or storage system discovery. If ViPR Controller is using only SMI-S to provision host clusters, then ViPR Controller creates stand-alone host objects for each cluster member on the IBM XIV storage system. ViPR Controller ensures a consistent HLU is used for cluster export.

2. **SMI-S plus Hyper Scale Manager**
   - When ViPR Controller is using SMI-S plus Hyper Scale Manager, ViPR Controller can create cluster objects on IBM XIV. This ensures a consistent HLU is used for cluster export.

When you configure the storage system in ViPR Controller to use IBM Hyper Scale Manager, the REST API is used, allowing volumes to be exported to an IBM XIV cluster host. Use of IBM Hyper Scale Manager is optional; however, you cannot delete Hyper Scale Manager from the storage system configuration after adding it.

---

**Note**

SMI-S does not identify clusters. If only SMI-S is used to export volumes to a cluster, then standalone hosts are created for each member of the cluster on IBM XIV.

---

**ViPR Controller CLI updates**

`viprcli storage provider create` and `viprcli storage provider update` have new options to support the Hyper Scale Manager. For example:

```bash
viprcli storageprovider create -name xiv -provip <IP address or FQDN> -provport 5989 -user admin -if ibmxiv -hyperScaleHost <IP address or FQDN> -hyperScalePort 8443 -secondary_username admin
Enter password of the storage provider:
Retype password:
Enter password of the secondary password:
Retype password:
```

```bash
viprcli storageprovider update -n xiv -provip <IP address or FQDN> -provport 5989 -user admin -if ibmxiv -hyperScaleHost <IP address or FQDN> -hyperScalePort 8443 -secondary_username admin -newname xiv
Enter password of the storage provider:
Retype password:
Enter password of the secondary password:
Retype password:
```

---

**Dell SC Series**

Dell SC Series (formerly Compellent) arrays may be discovered using ViPR Controller UI or CLI commands. Discover the Dell SC arrays by connecting to a Dell Storage Manager (DSM, formerly known as Dell Enterprise Manager). DSM manages one or more Dell SC arrays and can be configured to allow access per array based on the credentials that are
used. The DSM IP address and credentials are obtained from the System Administrator at the time of discovery.

Use these ViPR Controller services to manage Dell SC Series arrays:

- Provisioning
- Exports
- Snaps and clones
- Support for Consistency Groups
- Ingestion
- Discovery of ports and pools
- Detection of volume WWN
- Ability to specify ports for volume exports

**Discovery**

- Discover the Dell SC arrays by connecting to a Dell Storage Manager (DSM, formerly known as Dell Enterprise Manager). DSM manages one or more SC arrays and can be configured to allow access per array based on credentials used.
- Discover array serial number, pools, and ports.
- Discover number of ports, port type (FC/iSCSI), port speed and port metrics (load on port). Only the ports marked as "front-end" ports will be discovered and registered in CoprHD (target ports meant for accessing backend storage will be filtered out).
- Discover number of storage pools, capacity metrics for each pool (total and used capacity), type of storage profiles (RAID types and disk speeds/SSD).

**Provisioning and export**

- Create and delete volume, expand volume.
- Create thin or thick volumes.
- Export and unexport volumes. Export volumes to hosts/clusters/host initiators.
- Support various multi-path configurations (combinations of min path, max path and paths per initiator).
- Export and un-export snapshot through the creation of view volumes of the snapshot.

**Snapshot and clone operations**

- Create and delete snapshot.
- Create volume ("view volume") from snapshot (snapshot clone).
- Create and delete volume clones - full copy of volume to new volume.

**Ingestion**

- Ingest stand-alone volumes.
- Ingest exported volume along with their exports information.
- Ingest all the snapshots of the volume (if they exist).

**ViPR Controller UI and CLI updates**

The Dell SC option has been added to the ViPR Controller UI, and the array type, `dellsc`, has been added to the ViPR Controller CLI. Use these options for selecting Dell SC storage to add, virtualize or manage such as when adding Dell SC storage systems to ViPR Controller.
Communication with the array
The ViPR Controller Dell SC driver uses the REST API available with Dell Storage Manager 2015 R3 or above. All API communication uses HTTPS over port 3033.

Exclusions and limitations
These features are not supported using ViPR Controller at this time. The storage administrator may still enable them using Dell SC management tools if desired.

- Remote replication
- QoS (Quality of Service)
- File storage on Dell Storage FluidFS
- Deduplication
- Compression
- Live volume auto-failover

EMC VNXe

Before you add VNXe storage systems to ViPR Controller review the following information.

Table 6 Gather the EMC Unisphere required information

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unisphere host IP address</td>
<td></td>
</tr>
<tr>
<td>Unisphere user credentials</td>
<td></td>
</tr>
<tr>
<td>Unisphere host port (default is 443)</td>
<td></td>
</tr>
</tbody>
</table>

Create a sufficient amount of storage pools for storage provisioning with ViPR Controller.

General file storage system requirements

When configuring a file storage system for ViPR Controller, verify the system meets these requirements.

- NFS server must be configured in the storage system for ViPR Controller to create the NFS exports.
- CIFS share must be configured in the storage system for ViPR Controller to create the CIFS shares.
- NETBIOS configuration needs to be done to access the share with the NETBIOS name. If NETBIOS is present, the mount point is constructed with the NETBIOS name instead of IP.

For EMC Isilon, NetApp 7-Mode, and NetApp Cluster-Mode
To add domain users to a share, you must configure the AD server on the storage system (CIFS server).

EMC® Data Domain®

Before adding Data Domain storage to ViPR Controller, configure the storage as follows.

- The Data Domain file system (DDFS) is configured on the Data Domain system.
- Data Domain Management Center (DDMC) is installed and configured.
Network connectivity is configured between the Data Domain system and DDMC. While adding Data Domain storage to ViPR Controller, it is helpful to know that:

- A Data Domain Mtree is represented as a file system in ViPR Controller.
- Storage pools are not a feature of Data Domain. However, ViPR Controller uses storage pools to model storage system capacity. Therefore, ViPR Controller creates one storage pool for each Data Domain storage system registered to ViPR Controller, for example, if three Data Domain storage systems were registered to ViPR Controller, there would be three separate Data Domain storage pools. One storage pool for each registered Data Domain storage system.

EMC Isilon

Before adding EMC Isilon storage to ViPR Controller, configure the storage as follows.

Gather the required information
The following information is needed to configure the storage and add it to ViPR Controller.

Table 7 Isilon required information

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 or IPv6 address</td>
<td></td>
</tr>
<tr>
<td>Port (default is 8080)</td>
<td></td>
</tr>
<tr>
<td>Credentials for the user to add Isilon storage</td>
<td></td>
</tr>
<tr>
<td>systems to ViPR Controller, and to own all of the</td>
<td></td>
</tr>
<tr>
<td>file systems created on the Isilon through ViPR</td>
<td></td>
</tr>
<tr>
<td>Controller. This user must have root or administrator privileges to Isilon.</td>
<td></td>
</tr>
</tbody>
</table>

General requirements and information to manage Isilon storage systems

- SmartConnect is licensed and configured as described in Isilon documentation. Be sure to verify that:
  - The names for SmartConnect zones are set to the appropriate delegated domain.
  - DNS is in use for ViPR Controller and provisioned hosts are delegating requests for SmartConnect zones to SmartConnect IP.
- SmartQuota must be licensed and enabled.
- There is a minimum of 3 nodes in the Isilon cluster configured.
- Isilon clusters and zones will be reachable from ViPR Controller Controller VMs.
- When adding an Isilon storage system to ViPR Controller, you will need to use either the root user credentials, or create an account for ViPR Controller users, that has administrative privileges to the Isilon storage system.
- The Isilon user is independent of the currently logged in ViPR Controller user. All ViPR Controller operations performed on the Isilon storage system, are executed as the Isilon user that is entered when the Isilon storage system is added to ViPR Controller.

Requirements and information to enable continuous copies of Isilon file systems
Be aware of the following before enabling replication on Isilon file systems:

- Isilon storage systems, must be licensed, and enabled with SyncIQ.
- Only asynchronous replication is supported.
• Replication can be performed on local or remote file systems.
• Replication is supported on the same types of storage devices.
• Full copy or Clone of Isilon storage systems is not supported.
• Synchronizing from an older version of Isilon file systems to a new version of Isilon storage systems is supported, however synchronizing from a higher version of Isilon file systems to lower version of Isilon file systems is not supported.
• ViPR Controller can only be used to create one target copy of a source file system. Creating multiple targets for one source file system, and cascading replication is not supported.

To use ViPR Controller to create continuous copies of Isilon file systems, and failover to target devices, you will need to perform the following operations:

1. Discover the Isilon storage systems in ViPR Controller.
2. Create a file virtual pool, and set the Data Protection, Replication attributes.
3. Use the file provisioning services to create the source and target file systems from the replication enabled virtual pool.
4. Use the file protection catalog services to create continuous copies.

All of these steps can be performed from the ViPR Controller UI, CLI, and REST API.

Information and requirements to enable replication copies of Isilon file systems
ViPR Controller supports Disaster Recovery Failover and Failback operations for Isilon file systems. From the ViPR Controller UI, select Catalog > View Catalog > File Protection Services to access Failover File System or Failback File System.

Be aware of the following before enabling replication on Isilon file systems:
• Isilon storage systems, must be licensed, and enabled with SyncIQ.
• Only asynchronous replication is supported.
• Local or remote replication is supported for file systems.
• Replication is supported on the same types of storage devices.
• Full copy or Clone of Isilon storage systems is not supported.
• Synchronizing from an older version of Isilon file systems to a new version of Isilon storage systems is supported, however synchronizing from a higher version of Isilon file systems to lower version of Isilon file systems is not supported.
• ViPR Controller can only be used to create one target copy of a source file system. Creating multiple targets for one source file system, and cascading replication is not supported.
• You can only move file systems from an unprotected virtual pool to a protected virtual pool. All other options must be configured the same in both the virtual pool from which the file system is being moved and the virtual pool in which the file system is being moved.
• When the target file system is created in ViPR Controller, it is write enabled until the file replication copy operation is run using it as a target file system (Catalog > View Catalog > File Protection Services > Create Replication Copy). Once it is established as a target file system by the file replication copy order, any data that was previously written to the target file system will be lost.

To use ViPR Controller to create replication copies of Isilon file systems, and failover to target devices, you will need to perform the following operations:

1. Discover the Isilon storage systems in ViPR Controller.
2. Create a file virtual pool, and set the Data Protection, Replication attributes.

3. Use the file provisioning services to create the source and target file systems from the replication enabled virtual pool.

4. Start replication by going to Resources > File Systems. Select the file system that was created, click File Mirrors, and then click Start.

**Information and requirements to schedule snapshots of Isilon file systems**

Be aware of the following before scheduling snapshots on Isilon file systems:

- Only Tenant Administrators can configure schedule policies.
- Schedule policies are only supported for local snapshots on Isilon storage systems with SnapshotIQ enabled.
- Snapshot scheduling must be enabled on the virtual pool.
- Schedule policies cannot be created on ingested file systems, or file systems created in ViPR Controller prior to this release.
- The snapshot policy can be reused for different file systems.
- One file system can be assigned one or more schedule policies.

The steps to create and assign schedule policies are:

1. Discover storage systems.
2. Create a file virtual pool with the schedule snapshot option enabled.
3. Create one or more snapshot schedule policies in ViPR Controller.
4. Create file systems from file virtual pools with snapshot scheduling enabled.
5. Assign one or more snapshot policies to the file system.

**Information and requirements to set smart quota limits**

- Smart Quota limits can only be set on Isilon storage systems which are configured with a SmartQuota license.
- ViPR Controller detects whether the storage system is configured with a SmartQuota license at the time of provisioning, and provisioning will fail if you have entered smart quota values on a service for:
  - Isilon storage systems which are not enabled with a SmartQuota license.
  - All storage systems, other than Isilon storage enabled with a SmartQuota license.
- When SmartQuota limits are set on the file system, the QuotaDirectories under the file system will inherit the same limits that were set on the file system, unless the different SmartQuota limits are set on the QuotaDirectories, while the QuotaDirectories are being created.
- Once you have set the SmartQuota limits from ViPR Controller, you cannot change the SmartQuota values on the file system, or QuotaDirectories from the ViPR Controller UI. You must use the ViPR Controller CLI or ViPR Controller REST API to change the SmartQuota limits.
- ViPR Controller will only enforce smart quota limits set on the file system by ViPR Controller.
- For troubleshooting, refer to the apisvc.log, and the controllersvc.log log files.
NetApp 7-mode

Before adding NetApp 7-mode storage to ViPR Controller, configure the storage as follows.

- ONTAP is in 7-mode configuration.
- ViPR Controller supports NetApp 7-mode with and without multi-store enabled.
- Aggregates are created.
- NetApp licenses for NFS, CIFS, and snapshots are installed and configured.
- vFilers are created and necessary interfaces/ports associated with them
- Setup NFS/CIFS on the vFilers

NetApp Cluster-mode

Before adding NetApp Cluster-mode storage to ViPR Controller, configure the storage as follows.

- ONTAP is in Cluster-mode configuration
- Aggregates are created.
- NetApp licenses for NFS, CIFS and snapshots are installed and configured.
- Storage Virtual Machines (SVMs) are created and the necessary interfaces and ports are associated with them.
- Setup NFS, and CIFS on SVMs.
- When discovering NetApp Cluster-mode storage systems with ViPR Controller, you must use the management IP. You cannot discover NetApp Cluster-mode storage systems using LIF IP.

EMC VNX for File

Before adding VNX for File storage to ViPR Controller, you must verify that VNX for File meets specific requirements.

These are the requirements for adding VNX for File storage to ViPR Controller:

- Storage pools for VNX for File are created.
- Control Stations are operational and reachable from ViPR Controller Controller VMs.
- VNX SnapSure is installed, configured, and licensed.

vNAS discovery and project assignment

You can group file systems to different projects by associating a vNAS (virtual NAS) to one or more projects. Users of the projects can then use the vNAS for storage provisioning. This enables environments without multi-tenancy enabled at the organization level to group file systems to different projects.

EMC Isilon access zones

ViPR Controller can discover access zones and ingest them as a vNAS, and ingest their smart connect zones as storage ports. You can assign these vNAS to a single project, or to multiple projects. Users of that project can then provision file systems using these assigned vNAS.

Prior to running discover on Isilon storage, verify the following:
Authentication providers are configured.

Valid smart connect zones are associated with access zones.

**VNX for File virtual data movers**

A virtual data mover is an EMC VNX feature that groups CIFS and/or NFS servers into virtual containers. Each virtual container stores the necessary data to support one or more CIFS and/or NFS servers and their file systems. Each virtual data mover only has access to the file systems mounted to it, which provides logical isolation between multiple virtual data movers. A virtual data has a root file system that stores the CIFS or NFS identity information, such as local groups, shares, security credentials and audit logs.

ViPR Controller discovers the virtual data movers and ingests them as vNAS server objects. You can assign these vNAS servers to a project. Users of that project can then provision file systems using these assigned vNAS servers.

**Configuration requirements to discover, and provision vNAS servers**

You can assign these vNAS servers to a single project, or to multiple projects. Users of that project can then provision file systems using these assigned vNAS servers.

Before associating a vNAS server to a project, verify the following:

- The vNAS server and project are in the same domain.
- The vNAS server is not tagged or associated with another project.
- The vNAS server does not have file systems that belong to a different project.
- The **Enable Associate of Virtual NAS to Multiple Projects** option must be enabled to allow users to share a vNAS across multiple projects. In the ViPR Controller UI, this feature is enabled in the **Physical » Controller Config » NAS** tab.

If a vNAS server is in an invalid state, such as the unloaded state, or was deleted from its storage system, ViPR Controller is unable to detect this until the next array discovery. ViPR Controller still selects these vNAS servers for provisioning, resulting in an error. You can run a provisioning operation again after the vNAS server have been rediscovered.

**Steps to assign a vNAS server to one or more projects**

Steps to configure ViPR Controller to share a vNAS with multiple projects are:

1. Discover the storage system.
2. Set the Controller Configuration to allow a vNAS to be shared with multiple projects.
3. Map a vNAS to multiple projects.

---

**EMC Elastic Cloud Storage**

Before you add EMC Elastic Cloud Storage (ECS) to ViPR Controller, configure the ECS storage as follows:

- You can use any of the ECS IP addresses when adding the ECS to ViPR Controller.
- When adding the ECS, you need to enter the user credential. The user credentials:
  - Must have been created in the ECS with ECS System Admin privileges.
  - The ECS user can be an ECS local or domain user. If domain user then the ECS user must share the same Ldap or AD as the user logged in ViPR Controller.

**Note**

The user logged into the ViPR Controller must be a domain user.
Will be used by ViPR Controller to log into the ECS, and to perform operations on the ECS such as discover the ECS, create a bucket, and assign a bucket owner.

- Replication Groups must be configured on the ECS prior to running discovery or rediscovery from the ViPR Controller.
- ViPR Controller only supports management of ECS local Replication Groups when ECS is configured in a GEO (multi-site) environment.

**Note**

Discovery of ECS buckets (i.e. ViPR Controller ingestion of buckets) is not supported.

- You must map an ECS Namespace to a ViPR Controller Tenant.
  - The ECS namespace must have been created on the ECS prior to mapping it to a ViPR Controller tenant.
  - A ViPR Controller Tenant can only be configured with one ECS namespace.
  - An ECS namespace can only be mapped to one ViPR Controller tenant. The same namespace cannot be shared with different ViPR Controller tenants.
- If you will be assigning user access control to buckets, the user, group, or custom group must have been configured for the ECS prior to assigning the user access control to the bucket from ViPR Controller.

You can use ViPR Controller to generate ECS user secret keys using the ViPR Controller REST API, or CLI. This option is not available in the ViPR Controller UI.

- For ViPR Controller CLI details refer to the ViPR Controller CLI Reference, which is available from the .ViPR Controller Product Documentation Index.
- For ViPR Controller REST API details, see the ViPR Controller REST API Reference.

## RecoverPoint systems

Review the ViPR Controller requirements and the information necessary to add and configure an EMC RecoverPoint system to ViPR Controller.

**RecoverPoint site information**

This information is required to add a RecoverPoint system to ViPR Controller:

- RecoverPoint site management IPv4 or IPv6 address or hostname
- Port
- Credentials for an account that has the RecoverPoint administrator role to access the RecoverPoint site

**Configuration requirements**

To add a RecoverPoint system toViPR Controller, do the following:

- Install and license the RecoverPoint systems.
- If ViPR Controller is not managing the SAN network, zone the RecoverPoint systems to the storage arrays and attach the RecoverPoint splitters.
- Establish IP connectivity between RecoverPoint and the ViPR Controller virtual appliance.

If you are using ViPR Controller to manage RecoverPoint with XtremIO, be sure you configuration is set up as described in the RecoverPoint XtremIO Technical Notes which are provided from EMC Online Support.
Fabric Managers (switches)

ViPR Controller supports Brocade and Cisco switches. System Administrators can review the ViPR Controller requirements and information necessary to add and configure Fabric Managers (switches) to ViPR Controller.

DNS Server requirements
The DNS server configured for ViPR Controller deployment must be able to perform both forward and reverse lookup for all devices, including Brocade fabrics, and Cisco switches, managed by ViPR Controller.

ViPR Controller switch and network terminology

ViPR Controller has three external interfaces - a REST API, a Command Line Interface (CLI), and a User Interface. The scripting and programming interfaces (API and CLI) use slightly different terminology to refer to the network elements of your Storage Area Network (SAN).

The terminology used in each ViPR Controller Interface is as follows:

- Cisco® switches and Brocade CMCNE management stations are called fabric managers in the user interface.
- In the ViPR REST API and the ViPR CLI, Brocade CMCNE management stations and Cisco switches are called network-systems. Cisco VSANs and Brocade fabrics are called networks.

Brocade

Your Brocade switch should meet the following system requirements and be configured as follows before adding the switch to ViPR Controller.

Software requirements
ViPR Controller requires that EMC Connectrix Manager Converged Network Edition (CMCNE) is installed. For supported versions, see the on the EMC Community Network (community.emc.com).

CMCNE can be downloaded from EMC Support Zone (https://support.emc.com).

CMCNE installation and configuration requirements

- CMCNE must be installed on a different host than the storage system SMI-S provider. CMCNE uses the same port as the SMI-S provider, and therefore causes a port conflict if CMCNE and the SMI-S provider are installed on the same machine.
- The SMI Agent (SMIA) must be installed and started as part of the CMCNE installation. Validating CMCNE SMI Agent Installation on page 37 provides instructions to validate that the SMI Agent was installed correctly with CMCNE.
- CMCNE must have access to the switches with administrator privileges and the account must be configured with privileges to discover SAN topology, and to activate, create, and delete zones and zonesets.
- Use the CMCNE UI to prediscover the fabrics.
- You must have created the necessary fabrics that will be used by ViPR, assigned the ports to the fabrics, and configured any ISL links needed to connect a fabric between multiple switches.
- It is highly recommended that you implement redundant connections among ISL connections, so that the failure of a single ISL link does not partition fabrics.
- ViPR Controller has no restrictions on the number of fabrics.
- You do not need to create zones.

Validating CMCNE SMI Agent installation

The SMI Agent (SMIA) must have been installed and started as part of the CMCNE installation.

To validate that the SMI Agent was installed with the CMCNE installation, enter the CMCNE IP address in a browser to go to the EMC Connectrix Manager Converged Network Edition start page.

- If the SMIA provider was installed with CMCNE, a link to start the CMCNE SMIA configuration tool appears in the start page as shown below.

![CMCNE Start Page](image)

**CMCNE** - [Web Start the CMCNE Client](#)

**CMCNE SMIA** - [Web Start the CMCNE SMIA Configuration Tool](#)

Download Java Runtime Environments (version 1.6.0_26)

- [Windows](#)

Download SNMP MIB Files

- If a link to start the CMCNE SMIA configuration tool does not appear in the start page, it was not installed with CMCNE as shown below.
If the SMIA is installed, and not functioning as expected, check the C:\<installation path>\cimom\server\logs\smia-provider.log file for any errors.

ViPR Controller support for fibre channel routing with Brocade switches

ViPR Controller includes support for Fibre Channel routing configurations using Brocade switches. Fibre Channel Routing (FCR) is designed to allow devices from separate fabrics to communicate without merging the fabrics.

Fibre Channel Routing allows separate autonomous fabrics to maintain their own fabric-wide services and provide the following benefits:

- Faults in fabric services, fabric reconfigurations, zoning errors, and misbehaving devices do not propagate between fabrics.
- Devices that cause performance issues in a fabric do not propagate those issues to other fabrics.

This support expands ViPR Controller network and switch support to include configurations that use a Brocade router to move traffic from one physical data center to another. The following figure shows an example of a ViPR Controller-supported datacenter configuration that uses Fibre Channel routing. The DCX switch acts as the router between the devices in Fabric 15 and the devices in Fabric 10. In this simple example, Host 5 in Fabric 10 can consume storage on VNX 1 in Fabric 15.
Brocade Fibre Channel routing configuration requirements

The following guidelines apply to Brocade fibre channel routing configurations.

- As a part of the routing setup, at least one LSAN zone must be created between each pair of fabrics you expect ViPR Controller to consider. When ViPR Controller discovers the topology, it assumes that if an LSAN zone exists between two fabrics, then routing between the fabrics is allowed. If there is no LSAN zone between the fabrics, ViPR Controller assumes that routing is not allowed between the fabrics.

- CMCNE must discover the router and a seed switch in each participating fabric. In this example, CMCNE running on Host 1 would have to discover Brocade_Switch1, the DCX Switch, and Brocade Switch 2.

- ViPR Controller must successfully discover CMCNE. Choose Physical Assets > Fabric Managers to add and discover CMCNE.

For more information, refer to the following documents:

- *EMC Connectrix Manager Converged Network Edition User Guide* for more information on installing and configuring CMCNE

- *CMCNE Release Notes* for a list of supported switch platforms and the minimum firmware revisions.

Brocade failover in ViPR Controller

Refer to the following information when performing a failover on a Brocade fabric.

**Configuration requirements**

Before you perform the failover, make sure that...
The fabric name to which you are failing over, is exactly the same as the original fabric name.

- The logical and physical fibre channel switches are configured exactly the same on both the original fabric, and the fabric to which you are failing over.

**Procedure**

1. In ViPR Controller discover, and register the original Fabric.
2. Export the volumes to hosts which are using the ports that are managed by this Fabric.
3. Setup and configure another Fabric (failover Fabric) the same as you configured the original Fabric outside of ViPR Controller.
4. In ViPR Controller discover, and register the failover Fabric.
5. Power down the original Fabric.
6. In ViPR Controller re-discover, and register the failover Fabric.
7. Validate that the networks are associated to the failover Fabric.
8. Unexport the volumes, and zones which were removed.

**Cisco**

You will need the following information and your Cisco switches must be configured as follows before the switch can be added and used in ViPR Controller.

**Cisco switch login credentials**

Obtain the login credentials to use when adding the Cisco switch to ViPR Controller. The account must have privileges to provision (configure the mode of zone, zonesets, and VSAN) and to show the FCNS database.

**Configuration requirements**

Configure the switch as follows before adding it to ViPR Controller:

- Enable SSH.
- Create the VSANs that will be used by ViPR Controller on the Cisco switch.
- Assign the appropriate interfaces to the VSAN database.
- Configure any ISL links, and port channels, for multiple switch networks, and validate that the ISL links are operational. Doing so ensures that the FCNS database is correctly distributed and current on any switches that you add to ViPR Controller.

**Configuration recommendations**

It is highly recommended, but not required that you:

- Implement redundant connections between all ISL connections, so that the failure of a single ISL link does not partition VSANs.
- Enable Enhanced Zoning to avoid simultaneous modifications of the zoning database by ViPR Controller and other applications from overwriting each other’s changes. If Enhanced Zoning cannot be enabled (not a recommended configuration), it is advisable to limit the number of fabric managers in ViPR Controller to one fabric manager per VSAN.

**Cisco Smart Zones and ViPR Controller**

Smart Zones may be reused as long as they are in the active zoneset and device aliases are not used.

With SAN Zoning configured to "Automatic" in the Virtual Array, ViPR Controller will create new zones. These new zones may overlap the existing Smart Zones. It is also possible
that these new zones may not overlap the existing Smart Zones. This can result in additional paths exposed to the host or cluster.

With SAN Zoning configured to “Manual” in the Virtual Array, ViPR Controller will not create new zones. During the port selection process, ViPR Controller may select different array ports for the array-level export (e.g. Masking View). This can result in insufficient paths because target ports in the zone don’t match the target ports selected by ViPR Controller for the array-level export.

With SAN Zoning configured to “Manual” in the Virtual Array and “Zoned Ports Used for Backend Exports” and “Zoned Ports Favored for Host Exports” set to “True,” ViPR Controller will not create new zones and it will ignore the target ports in the Smart Zones during the port selection process.

With SAN Zoning configured to “Automatic” in the Virtual Array and “Zoned Ports Used for Backend Exports” and “Zoned Ports Favored for Host Exports” set to “True,” ViPR Controller will create new zones and it will ignore the target ports in the Smart Zones during the port selection process.

Automate cloning of Cisco zonesets

Cisco zonesets are created, modified, or deleted when ViPR Controller operations, which include exporting, and unexporting, block volumes to and from hosts are performed.

When using ViPR Controller to perform operations on Cisco zonesets, you can enable ViPR Controller to automatically create a clone of the zoneset prior to committing the change on the zoneset. The clone can then be used as a backup of the zoneset prior to the change.

Additionally, you can control whether a ViPR Controller operation can continue in the event that the creation of a zoneset failed.

Automation of cloning Cisco zonesets can be performed from the ViPR Controller UI, CLI or REST API.

Configuration requirements

When defining automation of Cisco zonesets through ViPR Controller note the following

- Automation of zonesets can only be enabled in ViPR Controller for Cisco switches.
- Zoneset clones are stored on the MDS switch.
- ViPR Controller only maintains the most recent successfully created zoneset clone, per day, per zoneset, per VSAN. In other words, for a given day, ViPR Controller maintains only one zoneset clone for that VSAN and that is the most recent successfully created clone.
- Cloning zonesets increases the size of the zone database (zoneDB) on the Cisco switch. Therefore, you may need to manually cleanup old zonesets as the zoneDB nears its limit size.
- The cloned zoneset will be named as follows: ViPR-<zoneset name>-<MM_dd_yy-HH_mm>, where:
  - `<zoneset name>` is the name of the zoneset being cloned.
  - `<MM_dd_yy-HH_mm>` is the timestamp of when the clone was taken.
- Creation of Cisco zoneset clones by ViPR Controller, is disabled by default.

ViPR Controller UI

The following options in the ViPR Controller UI General Configuration > Controllers tab are provided for this feature:
### Option Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clone Cisco Zoneset</td>
<td>Set to:</td>
</tr>
<tr>
<td></td>
<td>• True, to enable automatic creation of zoneset clones.</td>
</tr>
<tr>
<td></td>
<td>• False, to disable automatic creation of zoneset clones.</td>
</tr>
<tr>
<td></td>
<td>This option is set to False by default.</td>
</tr>
<tr>
<td>Allow Cisco Zoneset Commit</td>
<td>Set to:</td>
</tr>
<tr>
<td></td>
<td>• True, to allow the operation to continue even when creation of the</td>
</tr>
<tr>
<td></td>
<td>zoneset backup failed.</td>
</tr>
<tr>
<td></td>
<td>• False, to pause the operation when the creation of the zoneset</td>
</tr>
<tr>
<td></td>
<td>fails.</td>
</tr>
<tr>
<td></td>
<td>This option is set to False by default.</td>
</tr>
</tbody>
</table>

**ViPR Controller CLI**

The following options in the ViPR Controller CLI `viprcli system set-properties -pn` command are provided for this feature.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>controller_mds_clone_zoneset -pvf property_value.txt</code></td>
<td>Sets the value to true, to enable automatic creation of zoneset clones. When this value is not added to the <code>viprcli system set-properties -pn</code> option, automatic creation of zoneset clones is disabled by default.</td>
</tr>
<tr>
<td><code>controller_mds_allow_zoneset_commit -pvf property_value.txt</code></td>
<td>Sets the value to true, to allow the operation to continue even when creation of the zoneset backup failed. When this value is not added to the <code>viprcli system set-properties -pn</code> option, the ViPR Controller operation will not proceed if the creation of the clone failed.</td>
</tr>
</tbody>
</table>

**ViPR Controller support for Inter-VSAN Routing with Cisco switches**

ViPR Controller includes support for Inter-VSAN Routing (IVR) configurations using Cisco switches. IVR is designed to allow hosts, storage arrays and other devices residing in separate VSANs to communicate without merging the VSANs.

IVR allows separate autonomous VSANs to maintain their own VSAN-wide services and provide the following benefits:

- Accesses resources across VSANs without compromising other VSAN benefits.
- Transports data traffic between specific initiators and targets on different VSANs without merging VSANs into a single logical fabric.
Establishes proper interconnected routes that traverse one or more VSANs across multiple switches. IVR is not limited to VSANs present on a common switch.

Shares valuable resources across VSANs without compromise. Fibre Channel traffic does not flow between VSANs, nor can initiators access resources across VSANs other than the designated VSAN.

Provides efficient business continuity or disaster recovery solutions when used in conjunction with FCIP.

IVR Is in compliance with Fibre Channel standards.

The following figure shows an example of a ViPR Controller-supported datacenter configuration that uses Inter-VSAN routing. In this example, the IVR switch acts as the router between the devices in VSAN 15 and the devices in VSAN 10. Host 5 in VSAN 10 can consume storage on VNX 1 in VSAN 15.

Isolated VSANS
ViPR Controller can recognize and create IVR zones between isolated VSANs, whether they exist on a single switch or span multiple physical switches.

In order to accomplish and complete IVR zoning, ViPR Controller requires that the proper transit VSANs exist between the IVR routed VSANs. Additionally, ViPR Controller requires at least one IVR zone be created between each of the IVR routed VSANs. This allows ViPR Controller to associate and consider the IVR path as available and as an active provisioning path across VSANs.

When ViPR Controller discovers the topology, it assumes that when an IVR zone exists between the two VSANs, then routing between the VSANs is allowed and configured properly to allow host to storage access.
If there is not a pre-instantiated IVR zone between the IVR routed VSANs, ViPR Controller assumes routing is not allowed between the VSANs and does not create IVR zones.

For example, ViPR Controller can support this configuration.

**Figure 1** VSAN configuration supported in ViPR Controller

---

### Cisco Inter-VSAN routing configuration requirements

The following guidelines apply to all Fibre Channel routing configurations.

- For each VSAN, ViPR Controller must successfully discover the Fabric Manager (Cisco switch).
- As a part of the routing setup, at least one IVR zone must be created between each pair of VSANs you expect ViPR Controller to consider. When ViPR Controller discovers the topology, it assumes that if an IVR zone exists between two VSANs, then routing between the VSANs is allowed. If there is no IVR zone between the VSANs, ViPR Controller assumes that routing is not allowed between the VSANs.
- ViPR Controller must also discover the IVR-enabled switches that enable routing between ViPR Controller managed VSANs in your data center.


---

### Vblock system requirements

Review the information and requirements necessary to configure ViPR Controller to manage your Vblock system.

**Vblock system components that must be added to ViPR Controller**

At a minimum, Vblock system UCS, storage systems, and Cisco MDS switches must be added to the ViPR Controller physical assets for ViPR Controller to perform bare metal provisioning operations on a Vblock system. Review the following configuration requirements and information prior to adding the component to ViPR Controller:
• **Vblock compute systems on page 47** for UCS requirements.

  The section of this guide which provides the requirements for the type of storage system configured in your Vblock system.

• **Fabric Managers on page 36** for Cisco MDS switch requirements.

After the Vblock system components are added to ViPR Controller, they are automatically discovered and registered in ViPR Controller. For details about how Vblock system components are discovered and registered in ViPR Controller refer to Administering Vblock Systems with ViPR Controller on page 76.

**Requirements to perform OS installation during provisioning**

If you are planning to use ViPR Controller to perform OS installation on Vblock compute systems during ViPR Controller, Vblock service operations, you will need to configure your compute image server, compute images, and Vblock compute systems in the ViPR Controller environment as described below, prior to running the service operation.

1. Load your compute images, which contain the OS installation files, onto an FTP site.
2. Deploy each compute image server you wish to use.
3. Configure the compute image server networks for each compute image server you are deploying.
4. Add the compute image server to the ViPR Controller physical assets, and repeat this step for each compute image server you deployed in step 2.
5. Add the compute image to the ViPR Controller physical assets, and repeat this step for each compute image you are using.
6. Associate each Vblock compute systems with a compute image server.

Prior to performing any of these operations, review the requirements and information described in the following sections:

• **Compute image server on page 45**
• **Compute image server networks on page 46**
• **Compute images on page 46**
• **Vblock compute systems on page 47**

**Compute image server requirements**

A compute image server is required by ViPR Controller to deploy the compute images when you run a ViPR Controller, Vblock System provisioning service, which performs operating system installation on the Vblock compute systems.

You can add a single or multiple compute image servers to ViPR Controller.

While deploying a compute image server:

• You can use either the compute image server OVF file provided with ViPR Controller, or build a custom compute image server. Steps to deploy the OVF file, or the requirements to build a custom compute image server are both described in the *ViPR Controller Installation, Upgrade, and Maintenance Guide*.

• The management and OS installation networks must be configured for the compute image server. For details see: **Compute image server networks on page 46**.

You will need the following information to add the compute image server to ViPR Controller:

• FQDN or IP address of the compute image server.
• IP address of the OS Installation network.
- User credentials for ViPR Controller to access the compute image server.
- Path to TFTPBOOT directory on the compute image server. Default is `/opt/tftpboot/`.
- Timeout value for OS installation (in seconds). Default value is 3600.

After adding the compute image server to ViPR Controller:
- Provisioning with OS Installation requires that one compute image server is associated with each compute system.
- A compute image server can be associated to multiple compute systems, however a compute system can only be associated with one compute image server.
- For any Vblock compute systems added to ViPR Controller version 2.4 or higher, you will need to associate a compute image server prior to using the compute system for provisioning with OS installation.
- If you are upgrading to ViPR Controller from a version prior to 2.4, and had previously configured ViPR Controller for provisioning with OS Installation, the association between the compute image server, and the compute system will remain after you upgrade ViPR Controller.

### Compute image server network requirements

A network administrator must configure two networks for each compute image server your are deploying.

**Management network**
The management network is required for communication between ViPR Controller, and the compute image server.

**Private OS Installation Network**
The OS Installation Network is a private network for operating system (OS) installation. The OS installation Network is used by ViPR Controller during provisioning, for communication between the hosts, and the ViPR Controller compute image server. Once the hosts, and ViPR Controller compute image server are connected over the OS Install Network, the operating system installation is then performed over the OS Installation Network. Once installation is complete, the OS Installation Network is removed from the hosts.

The Private OS Installation Network must be:
- Configured with its own private DHCP server. No other DHCP server can be configured on the OS Installation Network.

**Note**
The OS Image Server, which is provided with ViPR Controller, contains a dedicated DHCP server.

- Isolated from other networks to avoid conflicts with other VLANs.

### Compute images

Compute images are the operating system (OS) installation files that can be installed by the ViPR Controller onto Vblock compute systems.

The compute image is not packaged with ViPR Controller, however ViPR Controller can be used to install the operating system on Vblock compute systems during ViPR Controller, Vblock system provisioning operations. To support this functionality:
You must have access to OS installation files that are supported by ViPR Controller. For supported versions see the ..

The OS Installation files must be placed on an HTTP, or an FTP site.

The compute image server, and the required networks, must have been deployed and added to ViPR Controller, before the compute images can be added to ViPR Controller. For details see: Compute image server on page 45

When adding the compute image to ViPR Controller, you will need the HTTP, or FTP address where the compute image resides. If a user name and password are required to access the site, specify them in the URL for example: ftp:// username:password@hostname/ESX/VMware-Installer-5.0-20.x86_64.iso.

You can add the compute images to ViPR Controller using the ViPR Controller UI, REST API, or CLI.

Once a compute image is added to ViPR Controller, the compute image is automatically loaded onto each compute image server that has been added to ViPR Controller, and the compute image name is stored in the ViPR Controller database.

If a compute image is removed from ViPR Controller it is removed from all of the compute image servers.

For specific steps to perform the operations described above see one of the following documents depending on which interface you are using, which are available from the ViPR Controller Product Documentation Index :

- ViPR Controller User Interface Virtual Data Center Configuration Guide
- EMC ViPR Controller REST API Reference
- ViPR Controller CLI Reference Guide

Vblock compute systems

Review the ViPR Controller requirements, and information necessary to add, and configure Vblock compute systems to ViPR Controller.

To prepare the Vblock compute systems for ViPR Controller discovery:

- Service Profile Templates must be configured in UCSM for ViPR Controller to apply to the compute virtual pools when a cluster is created by ViPR Controller. Discuss which service profile templates should be used to provision with your UCS administrator. For the ViPR Controller configuration requirements for UCS service profile templates, see ViPR Controller requirements for Service Profile Templates on page 65.
- While adding the compute system to ViPR Controller you will need the IP address, and user credentials with administrator privileges to the UCSM being used to manage the UCS.

To prepare the compute system for provisioning with OS Installation:

- If you have added the compute system to a ViPR Controller 2.4 or higher, you will need to associate one compute image server with each compute system.
- If you are upgrading to ViPR Controller version 2.4 or higher, and had previously configured ViPR Controller for provisioning with OS Installation, the association between the compute image server, and the compute system will remain after you upgrade ViPR Controller.
- You will need the VLAN ID for the OS Install Network.

For specific steps to perform the operations described above see one of the following documents depending on which interface you are using, which are available from the ViPR Controller Product Documentation Index :
Hosts and clusters

ViPR Controller Tenant Administrators can review the ViPR Controller requirements, and information necessary to add and configure hosts and clusters in ViPR Controller.

There are two ways to add hosts to ViPR Controller:

- Discoverable - once you have added the host, the ViPR Controller automatically discovers the host, and host initiators, and Windows clusters, and registers them to ViPR Controller. Only AIX®, AIX VIO, HP-UX®, Linux®, and Windows hosts can be added as discoverable. Only Windows clusters can be automatically discovered in ViPR Controller.

- Undiscoverable - ViPR Controller does not discover, or register the host or host initiators. Any host that is not an AIX, AIX VIO, HP-UX®, Linux, and Windows is added to ViPR Controller as undiscoverable. Optionally, AIX, AIX VIO, HP-UX®, Linux, and Windows can be added as undiscoverable as well. When an undiscoverable host has been added to ViPR Controller, you must manually add, and register the host initiators before using the host in a service operation.

Support for Host/Array Affinity for VMAX, VNX for Block, Unity, and XtremIO storage systems

Support for host/array affinity allows you to do the following:

- Host/array affinity discovery on page 53
- Host/array affinity resource placement on page 71

AIX hosts and AIX VIO Servers

AIX hosts must be configured as follows to be discovered by ViPR Controller, and for ViPR Controller provisioning.

- Either EMC PowerPath, or AIX default MPIO (not both) must be enabled.
- EMC Inquiry (INO) utility is required to be installed to match the volume World Wide Names (WWNs) to the host disks (hdisks).
- SSH must be installed and configured on the AIX hosts.

HP-UX

After adding HP-UX hosts to ViPR Controller, physical assets, ViPR Controller automatically discovers, and registers the hosts, and hosts initiators. In addition to discovering the host, the HP-UX® option also:

- Sets the Volume Set Addressing (VSA) flag, which is required for exporting EMC VMAX, and VPLEX volumes to HP-UX hosts.
- Is required to use the Host Mode Option when provisioning with HDS storage systems.
**Linux**

Linux hosts must be configured as follows to be discovered by ViPR Controller, and used for ViPR Controller provisioning.

- SSH and LVM are enabled. ViPR Controller uses SSH for Linux hosts.
- EMC PowerPath or native Linux multipathing software is installed. Refer to the *EMC PowerPath for Linux Installation and Configuration Guide* and the *SuSE Linux Enterprise Server (SLES): Storage Administration Guide*, under "Configuring the System for Multipathing."
- Time synchronization is configured.
- In some cases, it may be necessary to install lsb_release. If host discovery fails due to compatibility, and logs indicate that the lsb_release command is not found, the package that includes that command must be installed.

**Linux user requirements**

When ViPR Controller storage is attached to a Linux host it needs to run commands on the host. To access the host, ViPR Controller uses the credentials entered at the time the host is added to ViPR Controller. These are usually the credentials for the root account. If you do not wish to give ViPR Controller root access to a Linux host, it is recommended to give the sudo user `ALL` privileges to run the commands ViPR Controller requires.

**Using sudo for Linux host discovery**

When using a sudo user for host discovery, do the following:

1. Make sure tty is disabled for this user in `/etc/sudoers`.
2. Modify `/etc/sudoers` by adding the line `Defaults:<user1> !requiretty` under `Defaults requiretty`. For example:

   ```
   Defaults requiretty
   Defaults:smith !requiretty
   ```

**ViPR Controller requirement for SUSE Linux Enterprise Server (SLES) 12**

If you plan to use ViPR Controller UI to export or mount a volume to a Linux host running SLES 12, you must first manually create and mount one `ext3` or `ext4` filesystem on the host, prior to exporting or mounting a volume using the ViPR Controller UI.

Note

Manually creating an `ext3` or `ext4` filesystem is only required if you are using the ViPR Controller UI to export or mount a volume. You do not need to create the filesystem prior to exporting or mounting a volume, if you are using the ViPR Controller REST API.

**Windows**

Windows hosts must be configured as follows to be discovered by ViPR Controller, and used for ViPR Controller provisioning.

**Windows Remote Management (WinRM) must be enabled.**

Refer to *Configuring WinRM on a Windows Host for ViPR* on page 50.

**Either EMC PowerPath, or Microsoft MPIO (not both) must be enabled.**

For details see either the *EMC PowerPath and PowerPath/VE for Microsoft Windows Installation and Administration Guide* or the *Windows: Microsoft Multipath I/O Step-by-Step Guide*. 
Time synchronization is configured.
For host discovery, if using LDAP or Active Directory domain account credentials, the
domain user credentials can be in the same domain or in a different domain (but within
the same forest) from where the Windows host is located. For example, if a Windows host
is in the child1.example.com domain and the user account is in the parent domain
(example.com), ViPR Controller can discover the Windows host in the
child1.example.com domain using the user account from the parent domain
(example.com).

Configuring WinRM on a Windows host for ViPR Controller
Configures a Windows host to allow ViPR Controller to run commands on it.

Before you begin
- The account used to configure WinRM services has to be part of the Windows local
  administrators group or the Windows domain administrators group.
- For the ViPR Controller server to connect to Windows remote hosts, the host must
  accept remote Windows PowerShell commands. You can do this by enabling
  Windows remote access over HTTP.
- The Windows Firewall must be running to configure WinRM.
- WinRM can be configured over HTTP or HTTPs.
  - For HTTP — port 5985 is used by default.
  - For HTTPS — 5986 is used by default. You are required to have a valid CA signed
certificate installed on the Windows host.
    Contact your Windows administrator to determine if CA certificates were properly
    installed.

The commands in the following procedure are executed in the Windows command
prompt. If you are using Windows PowerShell to perform these commands, surround
the values in single quotes. For example: \texttt{winrm set winrm/config/service/auth
'@{Basic="true"}'}

Procedure
1. At an administrator command, or powershell prompt on the Windows host, issue
either of the following commands:
   - For HTTP use: \texttt{winrm quickconfig}
   - For HTTPS use: \texttt{winrm quickconfig -transport.https}

   This starts up a listener on the port. The port on which you start the listener must be
consistent with the port that you configure for the host in the host asset page.
2. You may need to make some configuration changes depending on how you want ViPR
Controller to connect to the host.
   - If you want ViPR Controller to connect to the host as a local user, you need to:
     a. To see the current WinRM service configuration run:
        \texttt{winrm get winrm/config/service}
        Basic Authentication and AllowUnencrypted must be set to true.
     b. If basic authentication is not set to true, run:
        \texttt{winrm set winrm/config/service/auth @{Basic="true"}}
     c. If AllowUnencrypted is not set to true, run:
        \texttt{winrm set winrm/config/service @{AllowUnencrypted="true"}}
d. You can now add the Windows host to ViPR Controller. The port on which you started the listener in step 1, must be consistent with the port that you enter when adding the host to ViPR Controller.

- If you want ViPR Controller to connect to the host as a domain user, you need to:
  a. Ensure Kerberos is enabled. You can check using:
     ```
     winrm get winrm/config/service
     ```
  b. If you need to enable Kerberos, run:
     ```
     winrm set winrm/config/service/auth @{Kerberos="true"}
     ```
  c. A System Administrator must ensure that the domain has been configured as an authentication provider in ViPR Controller (Security > Authentication Providers).
  d. A Tenant Administrator adds the host to ViPR Controller (Physical Assets > Hosts) page.

Use one of the following formats when entering the AD account names:
- username@domain.suffix for example: user1@domain1.company1.com
- domain.suffix\username for example: domain1.company1.com\user

3. Check that the host is displayed as valid in the table.

**After you finish**

After ViPR Controller is deployed, you can check that the host is displayed as valid in the Physical Assets > Hosts page. If you receive the following message WinRM may not be enabled or configured properly, or there may be a network problem.

Failed to connect to host. Please ensure the connection details are correct. [Error connecting: Connection refused]

### SUN-VCS

SUN-VCS clusters are added to ViPR Controller, physical assets, but are not discovered, or registered by ViPR Controller.

- Adding a host to ViPR Controller as SUN-VCS labels the cluster as SUN-VCS in the ViPR Controller repository.
- After adding SUN-VCS clusters to ViPR Controller, you will need manually add, and register the host initiators to ViPR Controller.
- The SUN-VCS operating system type is required to provision SUN-VCS clusters with VPLEX storage systems.

### VMware® vCenter

Review the ViPR Controller requirements, and information necessary to add, and configure vCenter to ViPR Controller.

For the ViPR Controller user roles required to perform this operation see ViPR Controller user role requirements on page 9.

**vCenter role requirements**

The role, which will be used by ViPR Controller to access vCenter, must have at least the following privileges enabled:

Datastore privileges:
- Allocate space
Required VMware® VirtualCenter role privileges

ViPR Controller requires that you have certain role privileges in VMware VirtualCenter to perform vCenter discovery and to create datastores.

**Required datastore privileges**
- Datastore
  - Allocate space
  - Browse datastore
  - Configure datastore
  - Remove datastore

**Required host privileges**
- Host
  - CIM
  - Configuration
    - Storage Partition Configuration

**FAQs for vCenters discovered and managed in ViPR Controller**

**vCenter migration: server UUID**
Q: The UUID of the vCenter server itself will obviously change. Does this pose a problem in ViPR?
A: This is not a problem. During discovery, ViPR will update the new vCenter UUID.

**vCenter migration: VMware entity identifiers**
Q: All VMware entities in vCenter (datastores, hosts, VMs, etc.) have unique identifiers in the vCenter database. I assume these will change, since we are not doing a backup/restore of the old vCenter. Does this pose a problem, or is ViPR only concerned with the naming structures?
A: During discovery of datacenters, clusters, and hosts, ViPR first searches the database by UUID. If it can't find a match, then it searches by name. In this case, ViPR won't be able to find the entities by UUID because that will change -- but it will find them by name.

**vCenter migration to a new vCenter server instance**
Q: For a vCenter migration to a new vCenter server instance, would there be a problem, assuming the following conditions:
- the host's ESXis are moved
• different IP
• different vCenter UUID
• different hostname

A: This would cause a problem if the same structure isn’t discovered (for example, different ESXi host name, different cluster names, etc.). If the structure remains the same underneath the vCenter, then no unmasking is triggered.

vCenter server appliance upgrade from 5.5 to 6.0
Q: For a vCenter server appliance upgrade from 5.5 to 6.0, would there be a problem, assuming the following conditions:
• the host’s ESXis are not moved
• same IP
• different vCenter UUID
• same hostname

A: This would not cause a problem. No unmasking will be performed.

VCenter migration: host renamed
Q: For a vCenter host rename, would there be a problem, assuming the following conditions:
• the hosts ESXs are not moved
• same IP
• same vCenter UUID
• different hostname

A: A vCenter with a different hostname is not a problem. No unmasking is triggered due to a vCenter rename.

Host/array affinity discovery for unmanaged volumes

Host/array affinity discovery allows ViPR Controller to discover when VMAX, VNX for Block, Unity, or XtremIO storage is provisioned to a given host, when the storage volumes are not under ViPR Controller management (unmanaged volumes).

Host/array affinity discovery identifies the storage and host connectivity through the host initiator. Once the host initiator is added to ViPR Controller, enabling discovery of host/array affinity includes discovery of the storage volumes, and the masking views used by the host initiator to connect the storage and the host.

When an unmanaged volume, or unmanaged masking view is discovered by host/array affinity for a storage system, and a host that have been discovered by ViPR Controller, the storage system is identified as the preferred storage system. When an unmanaged volume, or unmanaged masking view is discovered by host/array affinity for a storage system, and a cluster discovered by ViPR Controller, the storage systems associated with the cluster, as well as storage systems that are associated with individual hosts in the clusters are identified as the preferred storage system.

When a storage system is identified as the preferred storage system, and there are no managed volumes provisioned to the host, ViPR Controller will provision from the preferred storage system to the same host, or cluster when host/array affinity resource placement is enabled. For details see Host/array affinity resource placement on page 71.
Discovery of host/array affinity is disabled by default. ViPR Controller allows you to perform host/array affinity discovery on demand, or at scheduled intervals. Once host/array affinity discovery is scheduled:

- For the hosts already discovered in ViPR Controller host/array affinity discovery will occur 90 seconds after the ViPR Controller nodes are restarted.
- When a new host is added to ViPR Controller, host/array affinity discovery will occur for the newly added host at the next scheduled interval.
- When a vCenter is added to ViPR Controller, host/array affinity discovery is performed on the hosts brought in with the vCenter. When a new vCenter is added to ViPR Controller, host/array affinity discovery will occur for the hosts brought in with the vCenter, at the next scheduled interval.

**Configuration requirements**
When using ViPR Controller to discover host/array affinity be aware of the following:

- This feature is supported with VMAX, VNX for Block, Unity, or XtremIO storage systems.
- The host initiator, for which you want to discover host/array affinity, must have been added to ViPR Controller.
- While discovery of host/array affinity makes ViPR Controller aware of unmanaged VMAX, VNX for Block, Unity, or XtremIO storage volumes provisioned to a host, it does not discover and ingest the unmanaged storage volumes. You must perform the ingest operation to bring the unmanaged volumes under ViPR Controller management.
- You must rediscover host/array affinity after an unmanaged volume, has been exported, or unexported to a host, or if the unmanaged volume has been ingested. You can perform host/array affinity on demand or at a scheduled interval. If you use scheduled host/array affinity will not identify the unmanaged volume as managed, until the next successful discovery.
- On demand host/array affinity discovery can be initiated from the host from the ViPR Controller UI, CLI or REST API.
- You can perform host/array affinity discovery on the storage system using the ViPR Controller CLI or REST API. If you perform host/array affinity discovery on a storage system managed by a storage provider, host/array affinity discovery will occur on all the storage systems managed by the storage provider.
- Host/array affinity discovery can be scheduled from the ViPR Controller UI.

**ViPR Controller UI**
The following options on the ViPR Controller UI provide the functionality to use the feature:

<table>
<thead>
<tr>
<th>ViPR Controller UI Pages and Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Physical &gt; Hosts &gt; Discover Array Affinity</strong></td>
<td>Select the hosts for which you want to run host/array affinity discovery, and click Discover Array Affinity to run discovery, or rediscovery of the host/array affinity for the selected hosts immediately.</td>
</tr>
<tr>
<td><strong>System &gt; General Configuration &gt; Discovery</strong></td>
<td>The following options are used to schedule ViPR Controller to automatically perform host/array affinity discovery:</td>
</tr>
<tr>
<td></td>
<td>- Enable Array Affinity Discovery — Set to true to enable ViPR Controller for scheduled host/array affinity discovery.</td>
</tr>
</tbody>
</table>
ViPR Controller UI Pages and Options

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>set to false, host/array affinity discovery must be performed on demand.</td>
</tr>
<tr>
<td><strong>Array Affinity Discovery</strong> — When Array Affinity Discovery is enabled, this is the number of seconds between the time that ViPR Controller will rediscover for host/array affinity.</td>
</tr>
<tr>
<td><strong>Array Affinity Refresh Interval</strong> — When Array Affinity Discovery is enabled, this is the number of seconds before a new discovery operation is allowed since the last time host/array affinity was discovered.</td>
</tr>
</tbody>
</table>

ViPR Controller CLI
The following commands are used to perform on demand host/array affinity discovery from the ViPR Controller CLI.

<table>
<thead>
<tr>
<th>ViPR Controller CLI Commands and Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>viprcli storagesystem discover_arrayaffinity</td>
<td>Performs host/array affinity discovery for the given storage system.</td>
</tr>
<tr>
<td>viprcli host discover-array-affinity</td>
<td>Performs host/array affinity discovery for the given hosts.</td>
</tr>
</tbody>
</table>
Physical Asset Requirements and Information
CHAPTER 4

Virtual Asset Requirements and Information

This chapter contains the following topics:

- Overview .......................................................................................................................... 58
- Plan to build your virtual array .................................................................................... 58
- Block storage configuration considerations ............................................................... 61
- File storage configuration considerations ..................................................................... 64
- Object storage configuration considerations ............................................................... 65
- ViPR requirements for service profile templates ......................................................... 65
Overview

ViPR Controller System Administrators can review required storage information before configuring the various storage systems in ViPR Controller virtual arrays and virtual pools, as well understand how ViPR Controller works with the storage system element managers after the volumes or file systems are under ViPR Controller management.

Plan to build your virtual array

Review the following before you configure a virtual array.

- To decide the type of SAN zoning to set on your virtual array, see SAN zoning requirements on page 58.
- To decide which is the best method to set up the virtual array, see Plan how to add the physical assets to the virtual array on page 58.
- If adding a Vblock system to ViPR Controller, see Virtual array requirements for Vblock system services on page 60.

SAN zoning requirements

In the virtual array, you define whether ViPR Controller automates SAN zoning at the time the storage is exported to the host from ViPR Controller, or if the SAN zoning is handled manually outside of ViPR Controller operations. This discussion explains what to do when you chose manual SAN zoning.

If you chose manual SAN zoning:

- If there is an existing zone for the Host and Array:
  After the ViPR provisioning operation completes, check the Port Group within the Masking View to identify the FA ports that ViPR selected for the provisioning request. Compare the FA ports in the zone to the FA ports in the Port Group. If they match, no further action is required. If they do not match, reconfigure the zone to use the same FA ports. Alternatively, a new zone can be created.

- If there is no existing zoning for the Host and Array:
  After the ViPR provisioning operation completes, check the Port Group within the Masking View to identify the FA ports that ViPR selected for the provisioning request. Create a zone with the appropriate initiator and target ports.

Plan how to add the physical assets to the virtual array

At a minimum, a virtual array must include one network, and one storage system connected to the network.

When configuring the virtual array, you have the option to create a virtual array either by adding:

- Storage systems to the virtual array
- Storage ports to the virtual array

For instructions on creating a virtual array, see the EMC ViPR Controller User Interface Virtual Data Center Configuration Guide.

Add storage systems to the virtual array

You may want to add an entire storage system to the virtual array if you are planning to manage an entire storage system, or multiple storage systems in a single virtual array.
When you add an entire storage system to the virtual array, ViPR Controller automatically adds all of the registered networks, and storage ports associated with the storage system, to the virtual array. In the following example, when Storage System XYZ was added to the virtual array, all the storage ports, Networks A, Network B, VSAN 1, VSAN 2, VSAN 3, and VSAN 4 are all added to the virtual array.

**Figure 2**  Virtual array created by adding storage systems

![Virtual array created by adding storage systems](image)

When you add an entire storage system to a virtual array, you will need to go back into the virtual array and remove any resources you don’t want ViPR Controller to use.

**Add storage ports to the virtual array**

If you want to partition a single storage system into multiple virtual arrays for example, allocate some of the storage system resources for testing and some for production, it maybe more useful to add the storage ports first to create the virtual array. If you choose to create the virtual array by first adding the storage ports, ViPR Controller will add only the networks, and storage systems associated to the storage ports, and you will start out with a more defined inventory in your virtual array. The following figure demonstrates how two virtual arrays were created from a single storage system by adding the ports first when creating the Production and Test virtual arrays.
The Production virtual array was created by adding SP2, and SP3, which automatically adds Storage System XYZ, VSAN 2, VSAN 3, Network A, and Network B to the virtual array. While VSAN 1 is part of Network A, it is not added to the virtual array, because no storage ports, associated with VSAN 1 were selected to add to the virtual array.

The Test virtual array was created by adding SP4, and SP5, which automatically adds Storage System XYZ, VSAN 4, VSAN 5, Network B, and Network C to the virtual array. While VSAN 6 is part of Network C, it is not added to the virtual array, because no storage ports, associated with VSAN 6, were selected to add to the virtual array.

Furthermore, this image demonstrates how a network can be shared across two different virtual arrays. Since a storage port associated with Network B was added to each of the virtual arrays, Network B was added to both virtual arrays.

**Virtual Array requirements for Vblock system services**

For Vblock systems, storage must be accessible to compute systems through the virtual array. Vblock systems configured using the VCE logical build guide will have networks...
configured that connect the Cisco Unified Computing System™ (UCS) compute system to the storage via the SAN switches.

In ViPR Controller, virtual arrays should be created just as you would for any non-Vblock system. The networks that are defined in the virtual arrays will then determine whether the UCS systems have visibility to ViPR Controller storage.

The most effective thing to do is discover all the Vblock system physical assets before defining virtual arrays. After discovering all components, consult with the UCS administrator to determine which networks (VSANs) will be used on a given Vblock system. Use those networks to define the ViPR Controller virtual arrays. On less complicated Vblock system configurations, for example, a single Vblock system, simply adding the storage system to the virtual array may be enough. Once the virtual arrays are defined, they will be used by ViPR Controller for the following:

- ViPR Controller will automatically determine which UCS compute systems are available to compute virtual pools based on the selection of virtual arrays.
- ViPR Controller will automatically determine which blades to use to provision hosts based on the virtual arrays and compute virtual pools.

ViPR Controller makes these determinations by calculating which UCS compute systems have visibility to storage through the networks in the virtual arrays.

If working with updating service profile templates

When using updating service profile templates, it is recommended to create a dedicated virtual array that:

- Includes only the specific storage arrays that are intended to be used with the updating service profile template.
- Includes only the specific storage ports that are intended to be used with the updating service profile template.

**Block storage configuration considerations**

Review the following information before you create virtual arrays and virtual pools for block storage in ViPR Controller.

**General block storage configuration considerations**

It is recommended that you deregister any initiators that you do not want provisioned. If you do not, ViPR Controller provisions all your initiators if the Maximum Paths value, which is set on the virtual pool, is high enough. If one of the initiators is in a network with unallocatable ports, the following error message is generated:

```
There are no storage ports in the requested network. There are no available storage ports in the Network <FABRIC_BJ_Vsan3> requested to be used for export. This may be because they are all over an allocation ceiling.
```

**Storage system-specific configuration considerations**

Review the storage system-specific information in the following sections:

- **Hitachi Data System (HDS) on page 62**
- **EMC VPLEX on page 63**
- **XtremIO on page 63**
- **Third-party block (OpenStack) storage systems on page 64**

For the configuration requirements and information necessary to configure VMAX, and VNX for Block storage systems in the ViPR Controller virtual assets, refer to the **ViPR**
Block storage systems under ViPR Controller management

Using only ViPR Controller to manage the volume prevents conflicts between the storage system database and the ViPR Controller database, and avoids concurrent lock operations being sent to the storage system.

After a volume is placed under ViPR Controller management and is provisioned or exported to a host through a ViPR Controller service, do not use the storage system element manager to provision or export the volume to hosts. Here are some examples of failures that could occur when the element manager and the ViPR Controller database are not synchronized:

- If you use the element manager to create a volume, and at the same time another user tries to run the "Create a Volume" service from ViPR Controller on the same storage system, the storage system may be locked by the operation run from the element manager, causing the ViPR Controller “Create a Volume” operation to fail.

- After a volume is exported to a host through ViPR Controller, the same masking view, which was used by ViPR Controller during the export, was changed on the storage system through the element manager. When ViPR Controller attempts to use the masking view again, the operation fails because what ViPR Controller has in the database for the masking view is not the same as the actual masking view reconfigured on the storage system.

However, you can continue to use the storage system element manager to manage storage pools, add capacity, and troubleshoot ViPR Controller issues.

Hitachi Data Systems

Review the following configuration requirements and recommendations before virtualizing your Hitachi Data Systems (HDS) in ViPR Controller.

Virtual pool considerations
ViPR Controller provides auto-tiering for the six standard HDS auto-tiering policies for Hitachi Dynamic Tiering (HDT) storage pools.

The HDS auto-tiering policy options in ViPR Controller are:

<table>
<thead>
<tr>
<th>Policy name in ViPR Controller</th>
<th>Policy number</th>
<th>HDS level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>0</td>
<td>All</td>
<td>Places the data on all tiers.</td>
</tr>
<tr>
<td>T1</td>
<td>1</td>
<td>Level 1</td>
<td>Places the data preferentially in Tier 1.</td>
</tr>
<tr>
<td>T1/T2</td>
<td>2</td>
<td>Level 2</td>
<td>Places the data in both tiers when there are two tiers, and preferentially in Tiers 1 and 2 when there are three tiers.</td>
</tr>
<tr>
<td>T2</td>
<td>3</td>
<td>Level 3</td>
<td>Places the data in both tiers when there are two tiers, and preferentially in Tier 2 when there are three tiers.</td>
</tr>
<tr>
<td>T2/T3</td>
<td>4</td>
<td>Level 4</td>
<td>Places the data in both tiers when there are two tiers, and preferentially in Tiers 2 and 3 when there are three tiers.</td>
</tr>
<tr>
<td>Policy name in ViPR Controller</td>
<td>Policy number</td>
<td>HDS level</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------</td>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>T3</td>
<td>5</td>
<td>Level 5</td>
<td>Places the data preferentially in Tier 2 when there are two tiers, and preferentially in Tier 3 when there are three tiers.</td>
</tr>
</tbody>
</table>

**EMC VPLEX**

Review the following configuration requirements and recommendations before virtualizing third-party block storage in VPLEX.

**Virtual array configuration requirements and recommendations**
While creating virtual arrays, manually assign the VPLEX front-end and back-end ports of the cluster (1 or 2) to a virtual array, so that each VPLEX cluster is in its own ViPR Controller virtual array.

**Virtual pool configuration requirements and recommendations**
When running VPLEX with VMAX, the Storage Tier and FAST Policy names must be consistent across all VMAX storage systems.

**Thin virtual volume provisioning on VPLEX with XtremIO backing volumes**
ViPR Controller will perform thin provisioning on VPLEX virtual volumes with XtremIO backing volumes.
When creating virtual pools, you can select the thin provisioning type to have the thin-capable volumes added to the virtual pool. At the time of provisioning ViPR Controller will perform thin provisioning when the volumes are created from the virtual pool.
You can move the VPLEX volume from a non-thin virtual pool to a thin enabled virtual pool to change the virtual volume to be thin-enabled.
If you run the **Move into VPLEX** service order on a thin-capable non-VPLEX volume the virtual volume (local or distributed) becomes thin-enabled.
Ingestion of VPLEX thin-enabled virtual volumes with XtremIO backing volumes is also supported.

**Configuration requirements**
- ViPR Controller only supports this feature for VPLEX with XtremIO backing volumes.
- The VPLEX version must support thin provisioning. Refer to the ViPR Controller Support Matrix to determine which versions of VPLEX support this functionality.

**XtremIO**

Review the following configuration information before virtualizing your XtremIO storage system in ViPR Controller.

**Virtual pool considerations**
Metering collection is supported for XtremIO 4.2 and higher storage systems, and ViPR Controller uses the collected system’s average port usage metrics in storage pool selection for the ViPR Controller virtual pool.
Metering collection is not supported for earlier XtremIO storage systems. Therefore ViPR Controller uses the system’s average port usage metrics as 50% during XtremIO storage pool selection for a ViPR Controller virtual pool.
Third-party block (OpenStack) storage systems

Review the following configuration requirements and recommendations before virtualizing third-party block storage in ViPR Controller.

Virtual pool recommendations and requirements
If the discovered storage system is configured for multipathing, you can increase the values set in the virtual pool after the target ports are detected by ViPR Controller.

File storage configuration considerations

Review the following information before you add file storage systems to ViPR Controller virtual arrays and virtual pools, and before you use the file systems in a ViPR Controller service.

Virtual pool for configuration settings for all file storage systems
File systems are only thinly provisioned. You must set the virtual pool to Thin, when adding file storage to the virtual pool.

File storage systems under ViPR Controller management
Once a filesystem is under ViPR Controller management, and has been provisioned or exported to a host through a ViPR Controller service, you should no longer use the storage system element manager to provision or export the filesystem to hosts. Using only ViPR Controller to manage the volume will prevent conflicts between the storage system database and the ViPR Controller database, as well as avoid concurrent lock operations being sent to the storage system. You can however continue to use the storage system element manager to manage storage pools, add capacity, and troubleshoot ViPR Controller issues.

Specific storage system configuration requirements
Before you create virtual arrays and virtual pools for File storage in ViPR Controller, review the following sections for storage system specific configuration requirements and recommendations:

- EMC Data Domain on page 64
- EMC VNX for File on page 65

EMC® Data Domain®

Review the following information before virtualizing the Data Domain storage in the ViPR Controller virtual arrays and virtual pools.

Virtual pool configuration requirement and considerations
When creating the file virtual pool for Data Domain storage, the Long Term Retention attribute must be enabled.

While configuring the file virtual pools for Data Domain storage systems it is helpful to know that:

- A Data Domain Mtree is represented as a file system in ViPR Controller.
- Storage pools are not a feature of Data Domain. However, ViPR Controller uses storage pools to model storage system capacity. Therefore, ViPR Controller creates one storage pool for each Data Domain storage system registered to ViPR Controller, for example, if three Data Domain storage systems were registered to ViPR Controller, there would be three separate Data Domain storage pools. One storage pool for each registered Data Domain storage system.
EMC VNX for File

When configuring a VNX file virtual pool that uses CIFS protocol, there must be at least one CIFS server on any one of the physical data movers.

Object storage configuration considerations

Review the following information before you add file storage systems to ViPR Controller virtual arrays and virtual pools, and before you use the object storage systems in a ViPR Controller service.

ECS

While creating Object Virtual Pools for ECS systems:

- You must assign the pool to one or more virtual arrays which contain one or more ECS systems.
- The maximum Retention Period, sets the maximum retention that the buckets created with this virtual pool can not exceed.
- If you assign the virtual pool to a tenant, the ViPR Controller tenant must have been configured with an ECS namespace.

ViPR requirements for service profile templates

The following sections explain the requirements to configure a service profile template for ViPR Controller provisioning operations.

Note

If existing service profile templates do not match the following requirements, clone one of the service profile template to create a new service profile template and alter the settings as required by ViPR Controller.

General properties

- The service profile template must not be associated to a server pool. Blade selection is performed by the ViPR Controller Compute Virtual Pools.
- UUID assignment must be from a valid UUID Suffix Pool set up in the UCS with available addresses.

Storage

ViPR Controller currently supports Fibre Channel boot for UCS servers. The following lists the Fibre Channel requirements:

- World Wide Node Name (WWNN) assignment must be from a valid UUID Suffix Pool set up in the UCS with available addresses.
- The Local Disk Configuration Policy must be set to a local disk configuration policy where the Mode is set to No Local Storage.
- There must be at least one vHBA interface.
- For each vHBA, the World Wide Port Name (WWPN) assignment must be from a valid WWPN pool set up in the UCS with available addresses.
The VSAN set on each vHBA must be a valid network discovered by ViPR Controller. The VSAN must match one of the networks in a ViPR Controller virtual array.

Policy settings on the vHBAs are not set by ViPR Controller provisioning and are at the administrator's discretion.

**Network**

- Policy settings on the vNICs are not set by ViPR Controller provisioning and are at the administrator's discretion.
- There must be at least one vNIC interface.
- For each vNIC, the MAC Address Assignment must be from a valid MAC pool that was set up in the UCS with available addresses.
- Each vNIC must have at least one VLAN.

**Boot Policy and Boot Order**

There are no Boot Policy requirements. ViPR Controller ignores all Boot Policy settings in the service profile template and overwrites any existing parameters when it creates service profiles.

**Policies**

ViPR Controller does not set any policies. The UCS administrator is responsible for setting the policies.

**Updating service profile templates**

If provisioning with updating service profile templates,

- The boot policy of the updating service profile template must specify SAN as the first boot device.
- If the boot policy of the updating service profile template enforces vNIC and vHBA names, the names of the vNICs and vHBAs in the service profile template must match those in its boot policy.
- The compute virtual pool with which the updating service profile template is being associated, must be associated to a virtual array that has storage ports on the VSANs that the vHBAs of the template use.
- If the boot policy of the updating service profile template specifies SAN boot target WWPNs, then compute virtual pool that the template is associated with must be associated with a virtual array that includes those storage ports on the appropriate VSANs.
CHAPTER 5

Selecting Storage Pools for Provisioning

This chapter contains the following topics:

- Overview ........................................................................................................... 68
- Understanding pool utilization and subscription .............................................. 68
- Block storage resource placement options .................................................... 69
- Selection process for file storage ................................................................. 73
Overview

Learn how ViPR Controller automatically selects block and file physical storage pools for provisioning.

ViPR Controller runs filters against a set of storage pools that cover the physical storage systems associated with the virtual pools in the virtual arrays. If the storage pool meets all the filter criteria, it becomes a candidate for provisioning.

Understanding pool utilization and subscription

ViPR Controller uses pool utilization and subscription when evaluating storage pools for provisioning.

The storage pool’s capacity and subscription parameters are evaluated for pool utilization. Pool utilization is a calculation of the space that is currently being used compared to what is available as a percentage value. If the storage pool is below the utilization threshold, it is considered a match for provisioning.

Thick pool allocations are straight percentage values from 0 to 100%. Thin pools are allocated on-demand, and you can create volumes in excess of the pool size. A subscription percentage can be over 100%, implying that the aggregate size of the volumes provisioned pool is over the capacity. This over-subscription is limited to a certain percentage of the pool.

In the ViPR Controller user interface, you set the pool utilization and thin pool subscription on the Configuration Properties panel, shown below. To access this panel, select the Settings icon and then Configuration > Controller.

If you use the default Pool Utilization of 75% and the default Thin Pool Subscription of 300% on the Configuration Properties panel, the following occurs:

- Thick and thin storage pools: If the space used is 75% or more of the available capacity, the physical storage pool is not a match for provisioning. If the thin storage pool is utilized more than the utilization limit, it is not a match for provisioning.
- Thin storage pool: If the space subscribed is more than 300%, the physical thin storage pool is not a match for provisioning.
Block storage resource placement options

You can define how ViPR Controller selects the block storage volumes to use for provisioning. Options include to use:

- The Default selection process for block storage on page 69
- Host/array affinity resource placement on page 71

Default selection process for block storage

ViPR Controller runs filters at volume creation and volume provisioning time. If the storage pool meets all the filter criteria, it becomes a candidate for block volume placement.

Filtering process
The following table explains the filters involved in the selection process.

Table 8 Filters for creating block volumes

<table>
<thead>
<tr>
<th>Filter</th>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>activePoolMatcher</td>
<td>Active StoragePools</td>
<td>Filters out all inactive pools, such as storage arrays that are unreachable.</td>
</tr>
<tr>
<td>neighborhoodsMatcher</td>
<td>VirtualArray</td>
<td>Filters out all storage pools that are not part of the virtual array.</td>
</tr>
<tr>
<td>protectionMatcher</td>
<td>Volume Protection</td>
<td>RecoverPoint and High Availability:</td>
</tr>
</tbody>
</table>
### Table 8 Filters for creating block volumes (continued)

<table>
<thead>
<tr>
<th>Filter</th>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If the Metro point is enabled, looks for the High_availability_RP parameter value set on the pool.</td>
<td>• If the Metro point is enabled, looks for the High_availability_RP parameter value set on the pool.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If not a Metro point and has a mirror attribute and the pool does not support mirror capabilities, the pool is filtered out.</td>
</tr>
<tr>
<td>maxResourcesMatcher</td>
<td>VirtualPool Allocation</td>
<td>Checks the setting for the number of resources that can be created in the virtual pool, and filters out all storage pools exceeding this number.</td>
</tr>
<tr>
<td>capacityMatcher</td>
<td>StoragePool Capacity</td>
<td>Filters out the pools that do not have enough storage capacity.</td>
</tr>
<tr>
<td>vmaxBlockFastPolicyMatcher</td>
<td>VNX Array Tiering Policy</td>
<td>(VNX block volumes only) Verifies the FAST policy.</td>
</tr>
<tr>
<td>storageSystemMatcher</td>
<td>StorageSystem Affinity</td>
<td>(Multi-volume consistency only) Checks if the pools in the virtual pool are in the virtual array. If not, filters them out. Returns the highest capacity storage pool for the consistency pool.</td>
</tr>
<tr>
<td>vmaxFASTInitialTierSelectionMatcher</td>
<td>VMAX Array Tiering Policy</td>
<td>(VMAX only) Determines the storage pool on which to initially place the volume (initial placement tier). This initial placement tier is based on the drive type and RAID level settings in the virtual pool. If these parameters were set, retrieves the storage pool with the same drive type and RAID level. This filter runs at volume provisioning time.</td>
</tr>
<tr>
<td>poolPreferenceBasedOnDriveMatcher</td>
<td>StoragePool Drive Type</td>
<td>(VMAX only) Matches the drive type of the storage pool against the virtual pool drive type setting. If the drive type is not set in the virtual pool, uses the FC pool by default for volume provisioning. If unable to find the FC pool, uses the SAS, NL_SAS, SATA, SSD pools (in that order). This filter runs at volume provisioning time.</td>
</tr>
</tbody>
</table>
Candidate storage pools

After the filters are run, a listing of candidate storage pools is created for volume placement. They are ordered according to these rules:

- Least busy arrays and highest capacity pools
- Ascending order of its storage system's average port usage metrics (first order)
- Descending order by free capacity (second order)
- Ascending order by ratio of pool's subscribed capacity to total capacity (suborder).

ViPR Controller uses this ordered list of storage pools to place the volumes. If the number of volumes is more than one, the volumes may be spread across the storage pools, depending on the sizes and the available storage pool capacity.

As the ViPR Controller places the volumes, it marks the volume capacity as reserved against the storage pool. This ensures that other provisions that happen subsequent to or during a volume creation are correctly distributed based on capacity. After the volume is created, or if there is an error in creating the volume, the reserved space is removed from the storage pool and the actual allocated space takes its place.

Host/array affinity resource placement

ViPR Controller host/array affinity resource placement allows you to use the preferred storage during provisioning for a given host. You can further define that if the preferred storage becomes unavailable, whether or not ViPR Controller can continue to provision to that host from non-preferred storage.

Discovery of preferred storage

When host/array affinity resource placement is enabled, ViPR Controller identifies the preferred storage for

- Unmanaged volumes through host/array affinity discovery. For details see Host/array affinity discovery for unmanaged volumes on page 53.
- Managed volumes as the storage, and masking views which have already been provisioned to the hosts or cluster using ViPR Controller.

Configuration requirements

Be aware of the following when using this feature:

- This feature is supported with VMAX, VNX for Block, Unity, or XtremIO storage systems.
- Host/array affinity is identified by the connectivity through the host initiator. Therefore, the host initiator, for which you want to manage host/array affinity, must have been added to ViPR Controller.
- Host/array affinity provisioning is only applied when you use the following block storage services: Create a Block Volume for a Host, or Create and Mount Block Volume from anyone of the host-specific block storage services. If you only use the Create Block Volume service to first create the volume, and then later export the volume to a host, host/array affinity will not be applied.

ViPR Controller UI

The following ViPR Controller UI pages, and options provide the functionality to use the feature:
### Selecting Storage Pools for Provisioning

<table>
<thead>
<tr>
<th>ViPR Controller UI Pages</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual &gt; Block Virtual Pools &gt; Create or Edit Block Virtual Pools &gt; Resource Placement Policy</td>
<td>Options are:</td>
</tr>
<tr>
<td></td>
<td>• Default - Storage Array selection based on performance metrics and capacity — allows ViPR Controller to use the default method of storage selection during provisioning.</td>
</tr>
<tr>
<td></td>
<td>• Host/Array Affinity - Storage Arrays/Pools selection based on Host/Cluster array affinity first, then performance metrics and capacity — enables the virtual pool to be used for host/array affinity provisioning. During provisioning ViPR Controller will only provision from the preferred storage. If there are no preferred storage pools in the virtual pool or if preferred storage is unavailable, then ViPR Controller will continue to provision from non-preferred storage only if the value set in the Physical &gt; Controller Config &gt; Host/Array Affinity Resource Placement tab is greater than the number of preferred storage systems.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>You can define the Host/Array Affinity Resource Placement value. The default value is 4096. Decrease the value to enforce stricter host/array affinity resource placement.</td>
</tr>
</tbody>
</table>

| Physical > Controller Config > Host/Array Affinity Resource Placement tab | When the virtual pool from which the storage is being provisioned is enabled for host/array affinity, use this to set the maximum number of storage from which storage can be provisioned to a host. |
| | • **Scope Type: Global** — this setting is applied to all hosts, when host/array affinity resource placement is enabled. |
| | • **Scope Value** — is not applicable at the time of this release. |
| | • **Value** — the maximum number of storage systems from which ViPR Controller can provision. By default, the value is set to 4096. To use non preferred systems, the value must be equal to or greater than the number of preferred storage systems. If the value is: |
| | ▪ Less than or equal to the number of preferred storage systems, then the provisioning order will fail when the preferred storage becomes unavailable. |
| | ▪ Greater than the number of preferred storage systems, then ViPR Controller will attempt the provisioning order on the non-preferred storage systems if the preferred storage becomes unavailable. Once the storage from a non-preferred storage system is provisioned to the host, the storage becomes preferred storage for that host, and the number of preferred storage system is increased by one. |

### ViPR Controller CLI

The `viprcli vpool create` and `viprcli vpool update` commands includes the `[-placementpolicy | pp]` option to set the resource placement type from the CLI. Enter either of the following:
• **default_policy** — to have ViPR Controller to use the default method of storage selection during provisioning.

• **array_affinity** — to enable the virtual pool to be used for host/array affinity provisioning.

**Selection process for file storage**

ViPR Controller runs filters at file creation. If the storage pool meets all the filter criteria, it becomes a candidate for file placement.

The following explains the selection process for file storage.

• **activePoolMatcher**: Filters out all inactive storage pools, such as storage arrays that are unreachable.

• **neighborhoodsMatcher**: eliminates all pools that are not part of the virtual array.

• Retrieves all storage pools that match the passed virtual pool parameters and protocols. In addition, the storage pool must have enough capacity to hold at least one resource of the requested size.

• **maxResourcesMatcher**: Checks the setting for the number of resources that can be created in the virtual pool, and filters out all storage pools exceeding this number.

• **capacityMatcher**: Filters out the storage pools that do not have enough storage capacity.

• After the filters are run, a list of candidate storage pools is created for file placement. They are ordered according to these rules:
  - Least busy arrays and highest capacity pools
  - Ascending order of its storage system’s average port usage metrics (first order)
  - Descending order by free capacity (second order)
  - Ascending order by ratio of pool’s subscribed capacity to total capacity (suborder)

**File system placement for vNAS servers**

ViPR Controller uses performance metrics and calculations when evaluating vNAS servers for file system placement. For access zones, this pertains to vNAS servers with static work loads. ViPR Controller collects the number of storage objects, such as file systems and snapshots, and their capacity. The performance statistics of a vNAS server is then calculated as the aggregate performance of its network interfaces as follows:

1. Uses FileShareScheduler>getRecommendationForPools to retrieve a list of storage pools from the virtual pool recommendation. If there are no recommended storage pools, a placement error occurs.

2. If a project in the file system placement request has associated vNAS servers, retrieves all vNAS servers for that project in the virtual array.

3. Filters out the vNAS servers that have reached maximum resources or capacity.

4. If step 3 results in an empty vNAS list or the project in the request does not have any assigned vNAS servers, retrieves the virtual and System access zone that are unassigned.

5. Filters out the vNAS servers that have reached maximum resources or capacity. If an empty list is created, generates an error stating that vNAS and System access zone have reached the maximum limits.

6. Chooses the overlapping vNAS servers with storage pools that were recommended in step 1. If no vNAS servers exist, fails with a placement error.
7. Based on least load and performance factors, places the file system on a qualified vNAS server.
APPENDIX A

Administering Vblock Systems with ViPR Controller

This appendix contains the following information.

- Administering Vblock systems in your ViPR Controller virtual data center ............76
- How Vblock systems are discovered by ViPR Controller ........................................76
- How Vblock system components are virtualized in ViPR Controller ..........................79
- Examples of virtual arrays for Vblock systems .........................................................80
Administering Vblock systems in your ViPR Controller virtual data center

This appendix provides an overview of how Vblock systems, and the Vblock system components are administered in the ViPR Controller virtual data center (VDC).

To see how the Vblock compute and storage systems are provisioned using ViPR Controller refer to the ViPR Controller Service Catalog Reference Guide which is available from the ViPR Controller Product Documentation Index.

How Vblock systems are discovered by ViPR Controller

A Vblock system is a converged hardware system from VCE (VMware®, Cisco®, and EMC®) that is sold as a single unit consisting of the following components:

- Compute: Cisco Unified Computing System™ (UCS)
- Storage: EMC Storage System
- Network:
  - Pair of Cisco SAN switches
  - A Pair of LAN switches when the UCS will not be plugged directly into a customer network
- Virtualization: VMware vSphere®
Add Vblock system components to ViPR Controller physical assets

For ViPR Controller to discover the Vblock system, ViPR Controller requires that you add each Vblock system component to the ViPR Controller physical assets as follows:

Table 9 Vblock system components in ViPR Controller

<table>
<thead>
<tr>
<th>Add Vblock components</th>
<th>Into ViPR Controller Physical Assets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compute</td>
<td></td>
</tr>
<tr>
<td>Cisco Unified Computing System Manager</td>
<td>Vblock Compute System</td>
</tr>
<tr>
<td>VMware vSphere vCenter systems</td>
<td>vCenters</td>
</tr>
<tr>
<td>Network (SAN)</td>
<td>Fabric Managers (Cisco MDS switch)</td>
</tr>
<tr>
<td>Network (IP)</td>
<td>Networks</td>
</tr>
</tbody>
</table>
Table 9 Vblock system components in ViPR Controller (continued)

<table>
<thead>
<tr>
<th>Add Vblock components</th>
<th>Into ViPR Controller Physical Assets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage</td>
<td>Storage systems or Storage Providers</td>
</tr>
</tbody>
</table>

ViPR Controller discovery of Vblock system components

Once the Vblock system components are added to ViPR Controller, ViPR Controller automatically discovers the components and the component resources as follows:

Table 10 ViPR Controller discovery of Vblock system components

<table>
<thead>
<tr>
<th>When you add the physical asset to ViPR</th>
<th>ViPR discovers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vblock Compute System</td>
<td>Cisco Unified Computing System Manager Blades (referred to as Compute Elements in ViPR Controller).</td>
</tr>
<tr>
<td></td>
<td>Service Profile Templates</td>
</tr>
<tr>
<td></td>
<td>Updating Service Profile Templates (uSPT)</td>
</tr>
<tr>
<td>Fabric Managers (Cisco MDS and Nexus 5000 series switches)</td>
<td>Cisco MDS switch VSANs</td>
</tr>
<tr>
<td></td>
<td>Fibre Channel Ports</td>
</tr>
<tr>
<td>VMware vSphere vCenter</td>
<td>Discovering vCenter will discover existing hosts &amp; clusters as well as provide a target for new hosts &amp; clusters that are provisioned by ViPR Controller to be loaded into. (ESX hosts not managed by a vCenter instance can be discovered individually as part of standalone host discovery.)</td>
</tr>
<tr>
<td>Network IP</td>
<td>For file storage, ViPR Controller can discover the ports of IP connected storage systems and hosts, but it cannot discover the paths between them, so it is necessary to create IP networks in ViPR Controller, and manually add the host, and storage system ports, which will be provisioned together, to the same IP network.</td>
</tr>
<tr>
<td>Storage</td>
<td>Storage system</td>
</tr>
<tr>
<td></td>
<td>Storage pools</td>
</tr>
<tr>
<td></td>
<td>Storage ports</td>
</tr>
</tbody>
</table>

ViPR Controller discovers each Vblock system component as an individual ViPR Controller physical asset. The connectivity between the Vblock system components is determined within the context of the ViPR Controller virtual array. When virtual arrays are created, ViPR Controller determines which compute systems have storage connectivity through the virtual array definition. The virtual arrays are used when defining compute virtual pools and during provisioning to understand connectivity of the Vblock system components.

For more information refer to How Vblock system components are virtualized in ViPR on page 79.
Ingestion of compute elements

Upon discovery of an ESX host or cluster, ViPR Controller discovers the compute element UUID, which allows ViPR Controller to identify the linkage between the host, or cluster and the compute elements (blades). When a host, or cluster is then decommissioned through the ViPR Controller, the ViPR Controller identifies the compute element as available, and makes it available to be used in other service operations.

ViPR Controller registration of added and discovered physical assets

After a physical asset is successfully added and discovered in ViPR Controller, ViPR Controller automatically registers all of the physical assets, which are not in use, and its resources to ViPR Controller. Physical assets that are registered in ViPR Controller are available to use as ViPR Controller resources for ViPR Controller service operations.

Compute elements, or blades, which are found to be in use, are automatically set to unregistered to prevent ViPR Controller from disturbing it.

Optionally, you can deregister physical assets that you would like to see in ViPR Controller, but do not want ViPR Controller to use as a resource, or some resources can be deleted from ViPR Controller entirely.

Additional resources required by ViPR Controller for OS installation on Vblock systems

In addition to the Vblock system components, ViPR Controller requires a compute image server, a compute image, and networks for the compute image server are configured, and added to the ViPR Controller physical assets for ViPR Controller to install operating systems on the UCS blades during ViPR Controller, Vblock system provisioning operations.

While the compute image server, and compute image are added to the ViPR Controller physical assets, neither are discovered, or registered in the ViPR Controller.

The compute images are operating installation files that are added to ViPR Controller from and FTP site. The compute image server is used to server the os installation files, over the compute image server networks during a ViPR Controller Vblock system provisioning operation that is used to install an operating system on the Vblock compute systems.

How Vblock system components are virtualized in ViPR Controller

Once the Vblock system components have been added to the ViPR Controller physical assets, the user can begin to virtualize the components into the virtual arrays, and virtual pools.

Vblock compute systems

The Vblock compute system is virtualized in ViPR Controller in both the compute virtual pools and the virtual array networks.

Compute virtual pools

Compute virtual pools are a group of compute elements (UCS blades). ViPR Controller system administrators can manually assign specific blades to a pool, or define qualifiers, which allow ViPR Controller to automatically assign the blades to a pool based on the criteria of the qualifier.

Service profile templates are also assigned to a compute virtual pool. Service profiles are associated to blades to assign the required settings. Additionally, the UCS has the
concept of, "service profile templates, (SPTs)," and "updating Service Profile Templates (uSPTs)," that must be set up by UCS administrators. These service profile templates can be used by non-admin users to create the service profiles that turn a blade into a host.

ViPR Controller does not perform the functions of the UCS administrator, rather ViPR Controller utilizes service profile templates to assign the required properties to blades. A UCS administrator will need to create service profile templates that ViPR Controller can use to provision servers and hosts.

When a Vblock system provisioning service is run, ViPR Controller pulls the resources from the compute virtual pool selected in the service, and creates a cluster from the blades in the virtual pool, and applies the same service profile template settings to each of the blades in the virtual pool.

Vblock storage systems

Vblock storage systems are virtualized in the ViPR Controller block or file virtual pools, and in the virtual array.

Block or File virtual pools

Block and file virtual pools are storage pools grouped together according to the criteria defined by the ViPR Controller system administrator. Block and file virtual pools can consist of storage pools from a single storage system, or storage pools from different storage systems as long as the storage pool meets the criteria defined for the virtual pool. The block or file virtual pool can also be shared across different virtual arrays.

Vblock systems require the storage from block virtual pools for the boot LUN when ViPR Controller will be used to install an operating system on a Vblock compute system. Once the hosts are operational, ViPR Controller can use storage from any connected Vblock storage pools and export storage to those hosts.

Vblock networks in the virtual array

Connectivity between the Vblock storage system, and Vblock compute system is defined in the networks in the virtual array. The storage system, and Vblock compute systems that will be managed together must be on the same VSAN in the ViPR Controller virtual array.

Examples of virtual arrays for Vblock systems

ViPR Controller provides flexibility for how you can manage Vblock system resources in ViPR Controller, by how you configure the Vblock systems in ViPR Controller virtual arrays, or create virtual pools with Vblock system resources:

- Traditional Vblock system on page 81
- Multiple Vblock systems configured in a single virtual array for:
  - Automatic resource placement managed by ViPR on page 81
  - Manual resource placement managed through compute virtual pools or storage virtual pools on page 82
- Tenant isolation in virtual array through
  - Virtual array networks on page 83
  - Compute virtual pools on page 84
Traditional Vblock system

In this example, two Vblock systems are defined in two different virtual arrays.

Figure 6 Two Vblock systems configured in two virtual arrays

The two virtual arrays are isolated from each other by the physical connectivity.

- Virtual Array A is defined by VSAN 20, from SAN Switch A and VSAN 21 from SAN Switch B.
- Virtual Array B is defined by VSAN 20, from SAN Switch X and VSAN 21 from SAN Switch Y.

**Note**

While the UCS is not included in the virtual array, the networks that are defined in the virtual array will determine the UCS visibility to the ViPR Controller storage.

Multiple Vblock systems configured in a single ViPR Controller virtual array

In this example, two Vblock systems are configured in a single virtual array, and all the compute systems, and storage systems are communicating across the same VSANs: VSAN 20, and VSAN 21.

With this architecture, you could allow ViPR Controller to automate resource placement during provisioning using:

- A single compute virtual pool to allow ViPR Controller to determine compute placement.
- A single block virtual pool to allow ViPR Controller to determine storage placement.
Manual resource management with ViPR Controller virtual pools

You can also more granularly manage resource placement during provisioning by:

- Creating multiple compute virtual pools, and manually assigning compute elements to each compute virtual pool.
- Creating multiple storage virtual pools, and manually assigning storage groups to each storage virtual pool.

During provisioning the desired targets can be specified to ensure only the resources you need are used for your provisioning operation.
Tenant isolation through virtual array networks

You can allocate Vblock system resources by assigning the virtual array VSANs to different tenants. In the following example:

- Tenant A will only have visibility to the resources on VSANs 20, and 21.
- Tenant B will only have visibility to the resources on VSANs 30, and 31.

When using tenant isolation of networks, separate service profile templates would need to be defined for the compute pools used for each network.
For details about ViPR Controller tenant functionality, see *ViPR Controller User Interface Tenants, Projects, Security, Users and Multisite Configuration Guide*, which is available from the *ViPR Controller Product Documentation Index*.

**Tenant isolation through compute virtual pools**

Tenant isolation using compute pools is achieved by creating compute virtual pools with the compute resources (blades) dedicated to a specific tenant such as HR or Finance.

Tenant ACLs allow ViPR Controller to restrict access and visibility to the compute virtual pools outside of a user tenancy.

When defining tenant isolation through compute virtual pools, the service profile templates can still be shared since network isolation is not an issue.
Figure 10  Resource management through tenant isolation of compute virtual pools

Tenant isolation through compute virtual pools
APPENDIX B

ViPR Controller Support for EMC Elastic Cloud Storage (ECS)

This appendix contains the following sections.

- ViPR Controller support for EMC Elastic Cloud Storage overview ...........................................88
- Discovery of ECS systems in ViPR Controller ........................................................................... 88
- Mapping an ECS Namespace to a ViPR Controller Tenant ............................................................88
- Virtualizing ECS storage in ViPR Controller ..............................................................................89
ViPR Controller support for EMC Elastic Cloud Storage overview

ViPR Controller support for EMC Elastic Cloud Storage (ECS) includes the following:

**ViPR Controller administration of ECS systems**
ViPR Controller administrators can:
- Discover of ECS systems
- Map ECS Namespace to a ViPR Controller Tenant
- Create virtual arrays which include ECS systems, ports, and networks
- Group ECS Replication Groups into ViPR Controller Object Virtual Pools

Refer to the relevant sections of this guide to review the requirements, and information necessary to prepare to administer the ECS for ViPR Controller.

For the specific steps to configure the ECS in the ViPR Controller virtual data center see the [ViPR Controller User Interface Virtual Data Center Configuration Guide](#) which is available from the [ViPR Controller Product Documentation Index](#).

**ViPR Controller object storage services to:**
ViPR Controller users can:
- Create a bucket
- Edit a bucket
- Delete a bucket

For information about ViPR Controller services refer to the [ViPR Controller Service Catalog Reference Guide](#) which is available from the [ViPR Controller Product Documentation Index](#).

Discovery of ECS systems in ViPR Controller

ViPR Controller System Administrators add EMC Elastic Cloud Storage (ECS) systems to the ViPR Controller, Physical Assets, Storage Systems.

Once added, ViPR Controller:
- Discovers, and registers the ECS storage system
- Discovers, and registers the ECS Replication Groups, and adds the Replication Groups to the ViPR Controller storage pools.
- Discovers ECS namespaces.
- Uses the ECS IP address to create the management storage port which will be used for communication between ViPR Controller and the ECS.

**Note**
Discovery of ECS buckets (i.e. ViPR Controller ingestion of buckets) is not supported.

Mapping an ECS Namespace to a ViPR Controller Tenant

To use ViPR Controller to manage object storage in an ECS system, you must map a ViPR Controller Tenant to an ECS Namespace. When a bucket is created from the ViPR
Virtualizing ECS storage in ViPR Controller

When creating a virtual array for ECS object storage, you will need to configure an IP network and add the ECS ports to the network.

Once the network is added to the virtual array, the storage pools (ECS Replication Groups), and object storage system (ECS) will automatically be added to the virtual array.

Grouping of ECS Replication Groups into ViPR Controller virtual pools
ViPR Controller Object Virtual Pools are used to group ECS Replication Groups based on user-defined criteria. Once the criteria for creating the pool is defined by the user, ViPR Controller filters through the ECS Replication Groups, which were discovered by ViPR Controller, and only includes the Replication Groups, matching the criteria in the Object Virtual Pool.

Once the Replication Groups are put into the Object Virtual Pool, you can manually select, or allow ViPR Controller to automatically select which Replication Group, from the VIPR Controller virtual pool, to use to create buckets when the ViPR Controller, Create Bucket service is run.

If the Object Virtual Pool only contains one Replication Group, then all buckets created from that ViPR Controller Object Virtual Pool will be created from that Replication Group.