



EMC ViPR Controller

Version 2.3

Service Catalog Reference Guide

302-002-072

REV 02

Copyright © 2013-2015 EMC Corporation. All rights reserved. Published in USA.

Published July, 2015

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

The information in this publication is provided as is. EMC Corporation makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose. Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

EMC², EMC, and the EMC logo are registered trademarks or trademarks of EMC Corporation in the United States and other countries. All other trademarks used herein are the property of their respective owners.

For the most up-to-date regulatory document for your product line, go to EMC Online Support (<https://support.emc.com>).

EMC Corporation
Hopkinton, Massachusetts 01748-9103
1-508-435-1000 In North America 1-866-464-7381
www.EMC.com

CONTENTS

Tables		5
Chapter 1	Service Catalog Overview	7
Chapter 2	ViPR Controller Block Storage Services	9
	Overview of Block Storage Services.....	10
	Block storage provisioning services.....	10
	Block storage services for unmanaged volumes.....	12
	Block storage services to change a volume, virtual pool, or virtual array.....	13
	Block storage protection services.....	14
Chapter 3	ViPR Controller File Storage Services	17
	File storage services.....	18
	File Provisioning Support.....	18
	Create and manage file systems.....	18
	Create and manage CIFS shares.....	19
	Create and manage NFS exports.....	21
	Create and remove file system quotas.....	23
	File storage services for unmanaged file systems.....	24
	File System Protection Support.....	26
	File system snapshots.....	26
	Export NFS snapshots.....	27
	Export CIFS snapshots.....	27
	File Provisioning for VMware Support.....	28
Chapter 4	ViPR Controller Vblock System Services	29
	Vblock System Services.....	30
	Use the VCE Vblock System Services to create clusters on the Vblock compute system.....	30
	Create a new block volume and attach it to the ESX cluster as a datastore.....	32
Chapter 5	Monitor, and Troubleshoot ViPR Controller Services	35
	Monitoring and troubleshooting a service order.....	36
Chapter 6	Work with Service Resources	37
	Working with service resources.....	38
	How ViPR Controller deletes Masking Views for VMAX and VNX for Block storage.....	38
	File System Resources.....	39
	File System Snapshot Resources.....	41
	Block storage systems under ViPR Controller management.....	42
	File storage systems under ViPR Controller management.....	42

CONTENTS

TABLES

1	General block storage provisioning services.....	10
2	Block provisioning services for AIX, AIX VIO, Linux or Windows.....	10
3	Block provisioning services for vCenter.....	11
4	Block storage services for unmanaged volumes.....	13
5	Protection services for block storage.....	14
6	Services to create and manage file systems.....	19
7	File storage services for unmanaged File Systems.....	24
8	ViPR Controller Service Catalog, VCE Vblock System Services.....	30

CHAPTER 1

Service Catalog Overview

The ViPR Controller Service Catalog provides a selection of services to automate provisioning, and protection of block, and file storage, as well as host provisioning services for Vblock compute systems.

ViPR Controller Storage system support

The storage systems, and hosts that are supported are listed in the *ViPR Controller Support Matrix* which is available on the EMC Community Network (community.emc.com).

ViPR Controller service interfaces

The services in the Service Catalog can be managed from anyone of the following ViPR Controller interfaces:

- Using the services from the Service Catalog at the ViPR Controller UI or from the Catalog API
- Using the ViPR Controller API
- Using the ViPR Controller CLI

This guide focuses on the capabilities provided by the Service Catalog to demonstrate the support provided by ViPR Controller. However, you can perform the same operations using the API or CLI.

User requirements

Service operations can be run by ViPR Controller administrators, and users, however when logged into ViPR Controller with a user role you can only create resources and perform operations on resources belonging to project that you are assigned to (or are the owner of). If you are a Tenant Administrator you can run all services and choose any project to be the owner of the resource.

ViPR Controller and Virtual Data Center configuration requirements

Services can only be run after the ViPR Controller System Administrator has:

- Installed the ViPR Controller.
- Configured users, and projects.
- Configured the ViPR Controller virtual data center.
For more details see the *ViPR Controller Installation and Configuration Roadmap*, which is available from the [ViPR Controller Product Documentation Index](#).

Virtual pool requirements

Service provisioning, and protection capabilities depend on the use of one or more virtual pool from which block volumes, file systems, and compute systems can be created.

Information on adding storage systems and on creating virtual pools is provided in *ViPR Controller User Interface Virtual Data Center Configuration Guide*, and the *ViPR Controller REST API Virtual Data Center Configuration Guide* which are available from the [ViPR Controller Product Documentation Index](#).

CHAPTER 2

ViPR Controller Block Storage Services

This chapter includes the following topics:

- [Overview of Block Storage Services](#) 10

Overview of Block Storage Services

ViPR Controller Service Catalog provides the following types of services for block storage.

- Block Storage Services which include:
 - [Block storage provisioning services on page 10](#)
 - [Block storage services for unmanaged volumes on page 12](#)
 - [Block storage services to change a volume, virtual pool, or virtual array on page 13](#)
 - [Block Protection Services on page 14](#)

Block storage provisioning services

The ViPR Controller Service Catalog provides access to a set of predefined services, which includes high-level operations that carry out common provisioning activities, such as creating a block storage volume and exporting it to a host or cluster, and "building block" services that perform more granular operations, such as creating a ViPR Controller volume or exporting storage to a host.

General block storage provisioning services

ViPR Controller services are organized in categories. There is a general Block Storage Services category used to create block storage volumes and export them to any type of host.

Table 1 General block storage provisioning services

Service name	Description
Create Block Volume for a Host	Creates the volume from the selected virtual array, and virtual pool, and the exports for the host or cluster.
Expand Block Volume	Increases the amount of provisioned storage to the host or cluster.
Create Block Volume	Creates a block volume from the selected virtual array, and virtual pool.
Export Volume to Host	Creates the exports from the volume to the host or cluster.

Block provisioning services for hosts and vCenter

ViPR Controller also provides a set of predefined block storage services for AIX[®], AIX VIO, Linux[®], Windows[®], and vCenters. In addition to provisioning the storage to the hosts, these services perform operations on the host, cluster, or vCenter after the storage is provisioned.

Table 2 Block provisioning services for AIX, AIX VIO, Linux or Windows

Service name	Description
Create and Mount Block Volume	<ol style="list-style-type: none"> 1. Creates the volume from the selected virtual array and virtual pool, and exports to a host or a cluster. 2. Mounts and formats the volume on a host or cluster.

Table 2 Block provisioning services for AIX, AIX VIO, Linux or Windows (continued)

Service name	Description
Mount Existing Volume	Mounts and formats an existing volume that was already exported to a host or a cluster.

Table 3 Block provisioning services for vCenter

Service name	Description
Create a new block volume for VMware	Creates the volume from the selected virtual array and virtual pool, and then exports it to the ESX/ESXi host or cluster.
Create block volume and VMware Datastore	Creates a volume from one or multiple volumes from the selected virtual array and virtual pool, creates a VMware datastore for each volume created, and then associates the datastore to the ESX/ESXi host or cluster.
Create VMware Datastore	Creates a VMWare datastore from an existing volume.
Export Volume for VMware	Exports a volume to a vCenter host or cluster, and then rescans the HBAs on the vCenter host or cluster.
Unexport Volume for VMware	Unexports a volume from a vCenter host or cluster, and then rescans the HBAs on the vCenter host or cluster.
Extend Datastore with New Volume	Creates a new volume to increase the amount of storage allocated to the datastore.
Extend Datastore with Existing Volume	Uses an existing volume to increase the amount of storage allocated to the datastore.

Block storage services for hosts and vCenters unsupported for Openstack Third-party storage systems

The OpenStack Cinder API does not provide the storage volume world wide name (WWN) that is required to perform some of the operations for Block Storage services for hosts and vCenters. Due to this issue, you cannot use the following services for third-party block storage systems:

- **Block Services for AIX › Create and Mount Volume**
- **Block Services for AIX › Mount Volume on AIX**
- **Block Services for Linux › Create and Mount Volume**
- **Block Services for Linux › Mount Volume on Linux**
- **Block Services for Windows › Create and Mount Volume**
- **Block Services for Windows › Mount Volume on Windows**
- **Block Services for VMware vCenter › Create Volume and VMware Datastore**
- **Block Services for VMware vCenter › Create VMware Datastore**

Create, mount, and format a block volume on a Windows cluster

The following procedure is an example of how a self-service, provisioning, user could use ViPR Controller user interface to create, mount, and format a block volume on a Windows cluster.

Before you begin

All of the hosts must be powered on to successfully provision volumes.

Procedure

1. Go to the **Service Catalog > Block Services for Windows > Create and Mount Volume** service.
2. Select **Shared** for the **Storage Type**.
 Shared is to provision the storage across the cluster.
 Exclusive is to provision the storage to a single host.
3. Select the cluster for which the storage will be provisioned.
4. Select the virtual array from which the storage will be allocated.

Note

Available virtual arrays are based on ViPR Controller's visibility to the host initiator. If the virtual array you are wanting to select is not available in the selection list, it may be that the host is powered down.

5. Select the virtual pool from which the storage will be allocated.
6. Select the project to which the resources will be assigned once the storage is provisioned.
7. Provide a name for the volume.
8. If required, select the volume consistency group.
9. Enter the size the volume will be after provisioned.
10. In the **File System Type** field, select the volume format.
11. Enter the drive letter for the mount point.
 If left blank, the next available letter will be used.
12. Enter a drive label.
 If left blank, ViPR Controller assigns the volume name as the drive label..
13. Click **Order**.
 The Orders page is displayed with the progress of the order.

Block storage services for unmanaged volumes

Unmanaged volumes, are volumes that exist on a storage system discovered by ViPR Controller, but were not created or discovered by ViPR Controller. The discover, and ingest services are used by ViPR Controller to get the unmanaged volumes under ViPR Controller management.

When working with services for unmanaged volumes:

- The services for unmanaged volumes can only be performed by ViPR Controller system administrators.

- You can perform the ingest operations from the ViPR Controller UI, API and CLI.
- You must run the Discover Unmanaged Volumes service on the storage system before running an ingest service.

Table 4 Block storage services for unmanaged volumes

Service category	Service name	Description
Block storage services	Discover unmanaged volumes	Finds block volumes that are not under ViPR Controller management and matches them to a ViPR Controller virtual pool. When performing discovery it is important to note: <ul style="list-style-type: none"> • The virtual array and virtual pool into which you want to ingest the storage pools must exist when the discovery is performed. • There must be at least one virtual pool in ViPR Controller that matches the physical storage pool that contains the volume.
	Ingest unexported unmanaged volumes	Ingests volumes that were created on a storage system but were not exported to hosts. After the unmanaged volumes are ingested into ViPR Controller, you can export them to a host and mount them, or use them for other functions such as SRDF mirror volumes.
	Ingest exported volumes	Brings previously discovered unmanaged block volumes that were already exported to hosts under ViPR Controller management.

Review the following before using the ingest services:

- Ingested volumes are assigned to a project. You must belong to the selected project and have write permissions on that project.
- If the virtual array or virtual pool was modified since the last time the unmanaged volumes were discovered, rerun Discover Unmanaged Volumes prior to running the ingest operation to ensure volumes are assigned to the correct virtual array and virtual pool.
- For specific details on working with unmanaged volumes, refer to the *ViPR Controller Ingest Services for Existing Environments*, which is available from the [ViPR Controller Product Documentation Index](#).

Block storage services to change a volume, virtual pool, or virtual array

You can change the virtual array or virtual pool of volumes.

When working with services for changing the virtual array or virtual pool of volumes:

- The services for changing the virtual array or virtual pool can only be performed by ViPR Controller system administrators.
- The operations can be performed from the ViPR Controller UI, API and CLI.

Service category	Service name	Description
Block Storage Services	Change Volume Virtual Pool	<p>Moves a volume from one virtual pool to another. The target virtual pool can be used to:</p> <ul style="list-style-type: none"> • Add data protection to the volume • Change VPLEX local to VPLEX distributed • Change export path parameters • Change auto-tiering policy or host limits <p>You can also change the protection of all volumes in a consistency group from RecoverPoint +VPLEX CRR to MetroPoint CRR with no disruption in service. The target virtual array and virtual pool for the RecoverPoint copy are defined in Data Protection > RecoverPoint Copies > Add Copy. It is important to note that the target virtual pool must have:</p> <ul style="list-style-type: none"> • Data Protection setting of VPLEX Distributed. • Protect Source Site selected in Data Protection > RecoverPoint Advanced settings. • Protect HA Site selected in Data Protection > RecoverPoint Advanced settings
	Change Virtual Pool	<p>Move volumes from one virtual pool to another. The target virtual pool can be used to:</p> <ul style="list-style-type: none"> • Add data protection to the volumes • Change VPLEX local to VPLEX distributed • Change export path parameters • Change auto-tiering policy or host limits • Non-disruptively change the protection of all volumes in a consistency group from RecoverPoint +VPLEX CRR to MetroPoint CRR.
	Change Virtual Array	<p>Move a volume from one virtual array to another.</p>

Block storage protection services

The ViPR Controller block protection services use various technologies, such as SRDF and TimeFinder, to replicate and secure data on storage systems.

Before you run any of these protection services on a volume, export the volume to a host.

Table 5 Protection services for block storage

Service name	Description
Failover Block Volume	Uses RecoverPoint or SRDF to fail over the source volume to a target volume during disaster recovery.

Table 5 Protection services for block storage (continued)

Service name	Description
Swap Continuous Copies	Uses RecoverPoint or SRDF to swap the failover copy to a target volume.
Create Block Snapshot for a Volume	Creates a point-in-time copy of a volume.
Restore Block Snapshot	Restores the snapshot's point-in-time data back to the source volume.
Remove Block Snapshot	Removes a snapshot from a volume.
Create Full Copy	Creates full copies of the source volume. Note Full copy is not supported on a VMAX, VPLEX and HDS snapshot.
Remove Full Copies	Removes full copies from a volume. To remove snapshot full copies, you must use the Remove Volume service.
Restore From Full Copies	Restores a source volume with the latest data from a full copy.
Resynchronize Full Copies	Copies the latest data from a source volume to a full copy.
Detach Full Copies	Removes the source and target relationship of a copy session.
Create Snapshot Full Copy	Creates full copies of a snapshot.
Create Continuous Copy	Creates ongoing mirroring of data from the source volume to the target volume.
Remove Continuous Copy	Stops ongoing mirroring of data from the source volume to the target volume.
Export Snapshot to a Host	Exports a snapshot of a volume to a host. You can specify the volume's LUN or have ViPR Controller automatically assign this number.
Unexport Snapshot	Removes a snapshot from an export. You can use another export to access the volume.

Note

When remounting a source or target volume using one of the mounting existing volume services, make sure you deselect the Format Volume checkbox to ensure that ViPR Controller does not remove data from these volumes.

CHAPTER 3

ViPR Controller File Storage Services

This chapter includes the following topics:

- [File storage services](#)..... 18
- [File Provisioning Support](#)..... 18
- [File storage services for unmanaged file systems](#)..... 24
- [File System Protection Support](#)..... 26
- [File Provisioning for VMware Support](#)..... 28

File storage services

ViPR Controller supports the provisioning of file systems and the protection of file storage, using snapshots.

The Service Catalog provides the following areas for file storage:

- File Storage Services for [File Provisioning Support on page 18](#)
- [File System Protection Support on page 26](#)
- [File Provisioning for VMware Support on page 28](#)

File Provisioning Support

ViPR enables file systems to be created and made available as CIFS shares or NFS exports, or both.

The services provided in the Service Catalog enable a file system to be created first and subsequently shared using CIFS or NFS protocols, alternatively, file systems can be created and shared in a single operation.

The table below lists the services that are provided in the ViPR Service Catalog to support file system provisioning.

Category	Service function	Services
File Storage Services	Create and manage file systems on page 18	Create File System
		Expand File System
		Remove File System
	Create and manage CIFS shares on page 19	Create File System and CIFS Share
		Create CIFS Share for File System
		Remove CIFS Share for File System
	Create and manage NFS exports on page 21	Create File System and NFS Export
		Create NFS Export for File System
		Remove NFS Export for File System
	Create and remove file system quotas on page 23	Create File System Quota Directory
		Remove File System Quota Directory

Create and manage file systems

ViPR provides the ability to create file systems and to make them available as CIFS shares and NFS exports, or both.

The following services are provided to enable the creation and management of file systems.

Table 6 Services to create and manage file systems

Service	Description
Create a File System	Enables you to create a new file system from a specified file virtual pool. The file system can be made available as a CIFS share or NFS export, or both.
Expand File System	Enables you to expand an existing file system.
Remove File System	Enables you to remove a file system.

If you run the Create a File System service, the file system will create either CIFS shares, or NFS exports, or both depending on the settings in your virtual pool. If the virtual pool is set to both CIFS, and NFS, but the storage system is not enabled for NFS, then at the time the service is run the CIFS share is created, no NFS export is created, and the following error is returned:

```
com.emc.vipr.client.exceptions.ServiceErrorException: Error 1034
(http: 400): An error occurred while finding a suitable placement to
handle the request. No Storage Port was assigned to virtual array...
```

The **Resources > File Systems** area enables you to view information about a file share and how it has been made available as a CIFS share or NFS export.

Expanding File Systems on EMC Isilon

When expanding a file system that resides on an EMC Isilon array, you can specify a file system size that is larger than the available capacity.

All Isilon file systems are thinly provisioned and do not consume any capacity when created. Hence, when extending a file system, a client may violate the limit, but the array will always alert when the array is near full utilization.

Create and manage CIFS shares

You can expose a previously created file system as a CIFS share, or you can create a file system and a CIFS share in a single operation. The service catalog also allows you to delete a CIFS share.

The following services support the creation and management of CIFS shares.

Service	Description
Create File System and CIFS Share	Enables you to create a new file system from a file virtual pool and to share the file system as a CIFS share.
Create CIFS Share for File System	Enables you to share an existing file system as a CIFS share.
Remove CIFS Share for File System	Enables the sharing of a file system using CIFS to be removed. The Resources > File Systems page also enables the CIFS shares associated with a file system to be listed and individual shares to be deleted.

Notes on creating CIFS shares are provided in [CIFS Share Notes on page 20](#).

The **Resources > File Systems > <File System Name> > Shares** area enables you to view the shares that have been created for a selected file system.

Projects

In ViPR, each file system is associated with a project and any CIFS shares created for a file system can be considered to belong to the same project as the file system. Hence, when selecting a file system you need to select the project that it belongs to.

CIFS Share Notes

The following notes apply to the creation of CIFS shares from file systems and file system snapshots.

Share Names

Valid characters that can be used for CIFS share names are alphanumeric characters, and "_" (underscore).

CIFS Shares and Permissions

The permissions that can be set for an CIFS shares are detailed in the table below:

Array	File System Export	Snapshot Export
Isilon	Read,Change,FullControl	Not supported
VNX	Read,Change,FullControl	Read
NetApp 7-mode	Read,Change,FullControl	Read
NetApp Cluster-mode	Read,Change,FullControl	Read
VNXe	Read,Change,FullControl	Read
Data Domain	Read,Change,FullControl	Not supported

Access Permissions

For EMC Isilon, NetApp 7-mode, and NetApp Cluster-mode file storage systems the following Access Control List (ACL) functionality is supported:

- Use ViPR Controller to add, modify, and delete permissions for a user or group on CIFS share.
- ACLs are discovered, and ingested with discovery, and ingestion of unmanaged filesystems.

For Data Domain, VNX for File, and VNXe:

- Default access permissions are enforced when creating CIFS shares from the ViPR Controller.
- Access permissions for CIFS shares must be configured using Access Control Lists on the storage system that provides the file system.
- ACLs are not discovered and ingested with discovery of unmanaged filesystems.

Mapping a CIFS Share

To map the Windows share as a network drive, you can look at the order or at the **Resources > File Systems** page to find its location.

The share location is shown in the format:

```
\\ComputerNameFQDNorIP\SharedFolder
```

or

```
\\netbios name\SharedFolder
```

For example:

```
\\vipr-isi6132.lss.emc.com\tcshare01
```

is the FQDN location, where

```
\\LGLW6204\etapp7thickjune18shr1
```

is the netbios name configured on the array. The netbios name is only used if it is configured on the storage system. If it is not configured on the storage system, then the FQDN or CS IP will be shown as mount path.

Create and manage NFS exports

You can expose a previously created file system as an NFS export or you can create a file system and NFS export in a single operation.

The following services are provided to enable you to create and manage NFS exports.

Service	Description
Create NFS Export for a File System	Enables you to create an NFS export for an existing file system.
Create File System and NFS Export	Enables you to create a new file system from a file virtual pool and to make the file system available as an NFS export.
Remove NFS Export for a File System	Enables you to remove an NFS export for a file system.

In addition the following operations can be performed from the **Resources > File Systems** page.

Service	Description
Add an Export Rule	Enables you to add additional export rules to those that already exist.
Modify (an Export Rule)	Enables you to change an existing export rule.
Delete (an Export Rule)	Enables you to delete an export rule.

General notes on creating NFS exports are provided in [NFS Export Notes on page 22](#) and any constraints on creating exports for each file storage system supported by ViPR are described in [NFS Export Rules and Permissions on page 22](#).

Projects

In ViPR, each file system is associated with a project and any NFS exports created for a file system can similarly be considered to belong to the same project as the file system. Hence, when creating a file system you need to assign it to a project and when selecting a file system you need to select the project that it belongs to.

NFS Export Notes

The following notes apply to the creation of NFS exports from file systems (and file system sub-directories) and file system snapshots.

Sub-directory Exports

You can export sub-directories of a file system. The sub-directory must already exist and cannot be created from within ViPR.

Snapshots of file system sub-directories are not supported.

Adding and Modifying an Export Rule

In general, you can add an export rule for each file system or file system snapshot for each security type. The export rules that can be created for an export depend on the storage system. See [NFS Export Rules and Permissions on page 22](#) for details.

To add an export rule you need to:

1. Specify the hosts that can access the export. To specify more than one Export Host for a rule, the IP addresses or FQDNs of the hosts can be entered as a comma separated list.
2. Specify the Security Type for the export rule.
3. Set permissions to specify access that clients will have to the export: Read/Write (rw), Read Only (ro), or Root (root).

Modifying an export rule allows you to:

- Add additional endpoints that can access the share
- Specify the effective user id of anonymous users
- Specify the permissions for each export. This allows more granular setting of permissions than those configured when the NFS export is created.

Mounting an NFS Export

To mount the NFS export, you can look at the order or at the **Resources > File Systems** page or, for a snapshot, at the **Resources > File Snapshots** page, to find its mount point.

For example:

```
vipr-isi6132.lss.emc.com:/ifs/vipr/Isilon_Pool/Provider_Tenant/ProjectA/myNFSExport
```

If you have created a mount-point directory on you system (for example, /mnt/mynfs) the export can then be mounted using:

```
mount -t nfs vipr-isi6132.lss.emc.com:/ifs/vipr/Isilon_Pool/Provider_Tenant/ProjectA/myNFSExport /mnt/mynfs
```

NFS Export Rules and Permissions

File systems, file system sub-directories, and file system snapshots can be exported as NFS exports and access to an exported file systems depends on the security type and the permissions assigned.

The security types supported and the rules that can be created on each supported array are detailed below.

Isilon

Supports sys, krb5, krb5p, krb5i security types, but allows only one rule to be set. If you have set a rule for sys, for example, you cannot set a further rule for another security type.

VNX

Supports sys, krb5, krb5p, krb5i security types and allows one rule per security type.

NetApp

Supports sys, krb5, krb5p, krb5i security types and allows one rule per security type.

VNXe

Supports sys security type, with one rule.

Data Domain

Supports sys and krb5 security type, with one rule per security type.

The permissions that can be set for an export are detailed in the table below:

Array	File System Export	Snapshot Export
Isilon	rw, ro, root	Not supported
VNX	rw, ro, root	ro
NetApp 7-mode	rw, ro, root	ro
NetApp Cluster-mode	rw, ro, root	Not supported
VNXe	rw, root (See Note)	ro
Data Domain	rw, ro, root	Not supported

Note

For VNXe, a file system or sub-directory export must have root permission in order to mount it on a host and write data to it. If an export has read-write permissions, you can mount it but cannot write data to it.

Create and remove file system quotas

You can create a quota directory at the root of a file system.

In NetApp this is a QTree, for VNX File this is a Quota Tree, and for Isilon this is a Sub-directory with Quota. The size of the directory is a Group Quota Hard limit.

In NetApp Cluster-mode Data ONTAP, for an NFS client to mount a qtree, the NFS client must have read-only permissions at all the parent junction paths up to the Storage Virtual Machines (SVMs) root file system junction path (that is, /). For NFS clients to mount qtrees, the qtrees must belong to a file system that has read-only permissions. Without the read-only permissions at the file system, the NFS clients cannot mount the qtree.

The Service Catalog provides the following services to enable the creation and deletion of file system quotas:

Service	Description
Create File System Quota Directory	Enables you to create a quota directory at the root of the file system.
Remove File System Quota Directory	Enables you to remove a quota directory.

In addition, the **Resources > File Systems** page enables the quota directories associated with a file system to be displayed and for the following operations to be performed.

Operation	Description
Modify (Quota Directory)	Enables you to modify the setting for a quota directory: set the security style and change the size.
Delete (Quota Directory)	Enables you to remove a quota directory.

Modifying a quota directory enables the size to be changed and, for NetApp, enables the Security Style and Read/Write Cache (oplock) to be enabled.

File storage services for unmanaged file systems

Unmanaged file systems, are file systems that exist on a storage system discovered by ViPR Controller, but were not created or discovered by ViPR Controller. The discover, and ingest services are used by ViPR Controller to get the unmanaged file systems under ViPR Controller management.

Table 7 File storage services for unmanaged File Systems

Service category	Service name	Description
File storage services	Discover unmanaged file systems	Finds file systems which are not under ViPR Controller management and matches them to a ViPR Controller virtual pool. When performing discovery it is important to note: <ul style="list-style-type: none"> The virtual array and virtual pool into which you want to ingest the storage pools must exist when the discovery is performed. There must be at least one virtual pool in ViPR Controller that matches the physical storage pool that contains the volume.
	Ingest file systems	Used to ingest the file systems, which have been created on the storage system, but have not yet been exported to hosts. Refer to the Ingest File System Support table below.

When working with services for unmanaged file systems:

- The services for unmanaged file systems can only be performed by ViPR Controller system administrators.
- The operations can be performed from the ViPR Controller UI, API and CLI.
- You must run the Discover Unmanaged File Systems service on the storage system before running an ingest service.
- The virtual array and virtual pool into which you want to ingest the storage pools must exist when the discovery is performed.
The discovery process finds storage pools on a selected storage system and identifies the virtual array and virtual pool that each discovered file system matches.
- To be ingested, the unmanaged file systems must be in physical pools which are already associated with a ViPR Controller virtual storage pool.

- Rerun the Discover Unmanaged File Systems service if the virtual array or virtual pools have been modified since the last time the Discover Unmanaged File Systems service was run.
- Ingested file systems will be assigned to a project. You must belong to the selected project and have write-permission on the project.
- To ingest an Isilon unmanaged file systems:
 - The virtual pool must have been configured with the Provisioning Type set to Thin. Isilon file systems are thinly provisioned. Thin resources can only be created in "thin" v pools.
 - The Isilon file system exports must be in either /ifs/sos or /ifs/vipr. File systems exported to other locations will not be ingested by ViPR Controller.
- ACLs are discovered, and ingested with discovery, and ingestion of unmanaged filesystems for EMC Isilon, NetApp 7-mode, and NetApp Cluster-mode file storage systems.

Ingest File System support

The following table lists the resources that are ingested for a file system for each type of file storage system.

Resource	Isilon	VNX File	NetApp 7-Mode	NetApp Cluster-Mode	Data Domain	VNXe
FileSystem without Exports	Yes	Yes	Yes	Yes	Yes	Yes
FileSystem with Exports	Yes	Yes	Yes	Yes	Yes	Yes
NFS Exports and rules	Yes	Yes	Yes	Yes	Yes	Yes
CIFS Shares	Yes	Yes	Yes	Yes	Yes	Yes
CIFS Share ACL	Yes	No	Yes	Yes	No	No
Sub Directory/QD Exports	Yes	Yes	Yes	No	Yes	Yes
Sub Directory/QD Shares	Yes	Yes	Yes	No	Yes	Yes
Quota Directory	No	No	No	No	No	No
Snapshots	No	No	No	No	No	No
Snapshot NFS Exports	No	No	No	No	No	No
Snapshot CIFS Shares	No	No	No	No	No	No

Note

Filesystems with more than one export rule of same security type for an export, and exports other than supported security types (sys, krb5, krb5p, krb5i) will not be ingested.

File System Protection Support

ViPR supports the creation of file system snapshots and enables previously created file system snapshots to be made available as CIFS shares or NFS exports.

The following services are provided in the ViPR Services Catalog.

Category	Service Function	Service
File Protection Services	File system snapshots on page 26	Create File System Snapshot
		Restore File System Snapshot
		Remove File System Snapshot
	Export CIFS snapshots on page 27	Create CIFS Share for Snapshot
		Remove CIFS Share for Snapshot
	Export NFS snapshots on page 27	Create NFS Share for Snapshot
Remove NFS Share for Snapshot		

File system snapshots

You can create snapshots of file systems that you have created and restore the snapshot.

The following services are provided:

Service	Description
Create File System Snapshot	<p>Enables you to create a snapshot of an existing file system.</p> <p>The following prerequisites apply:</p> <ul style="list-style-type: none"> You must have access to the project to which the file system you want to snapshot belongs. The snapshot that you create will also belong to this project. A file system must exist and the file virtual pool from which it was created must be enabled for snapshots. A System Administrator can access the file virtual pool at Virtual Assets > File Virtual Pools, and the number of snapshots allowed for a selected file virtual pool can be set at the Data Protection > Maximum Snapshots field.
Restore File System Snapshot	<p>Enables you to restore a previously created file system snapshot. You must have access to the project to which the file system and its snapshots belong.</p>
Remove File System Snapshot	<p>Enables you to remove a previously created snapshot. You must have access to the project to which the file system and its snapshots belong.</p>

Virtual Pool Maximum Snapshots

To be allowed to create a snapshot of a file system, the file virtual pool that the file system is assigned to must be enabled for snapshot. At the UI, you can access the file virtual pool at **Virtual Assets > File Virtual Pools**, and the number of snapshots allowed for a selected file virtual pool can be set at the **Data Protection > Maximum Snapshots** field.

Snapshot names

Valid characters for the snapshot name are numbers, the English alphabet, and the underscore (_).

Export NFS snapshots

You can make snapshots available as NFS exports.

The following services support the management of NFS mounted snapshots:

Note

Create, modify, and removal NFS exports is not supported for NetApp Cluster-Mode.

Service	Description
Create NFS Export for Snapshot	Enables you to select a previously created snapshot and make it available as an NFS export.
Remove NFS Export for Snapshot	Enables you to remove an NFS export for a snapshot.

In addition the following operations can be performed from the **Resources > File Snapshots** page.

Service	Description
Add an Export Rule	Enables you to add additional export rules to those that already exist.
Modify (an Export Rule)	Enables you to change an existing export rule.
Delete (an Export Rule)	Enables you to delete an export rule.

Note

For VNXe, it is not possible to delete an export for a snapshot; the delete operation causes the export to be deleted from ViPR, however, the VNXe has not deleted it. Subsequent attempts to add an export will fail.

General notes on creating NFS exports are provided in [NFS Export Notes on page 22](#) and the support for creating exports for each file storage system supported by ViPR Controller is described in [NFS Export Rules and Permissions on page 22](#).

Export CIFS snapshots

You can make a file system snapshot available as a CIFS share.

The following services support the creation and management of CIFS shares.

Service	Description
Create CIFS Share for File System	Enables you to select a previously created snapshot and make it available as a CIFS share. ViPR Controller does not support creating CIFS share for File System for Isilon storage systems.
Remove CIFS Share for Snapshot	Enables you to remove a CIFS share for a snapshot.

Notes on creating CIFS shares are provided in [CIFS Share Notes on page 20](#).

File Provisioning for VMware Support

The file systems for VMware enable the creation of file systems and attaching the created file systems, or existing file systems, as a datastore on an ESX host.

Service	Description
Create File System and NFS Datastore	Enables you to create an NFS export and mounts it to an ESX host as a datastore.
Create VMware NFS Datastore	Enables you to create a datastore from an existing NFS export.
Delete NFS Datastore and File System	Enables you to delete a datastore, its underlying file system, and the associated NFS export.
Delete VMware NFS Datastore	Enables you to delete a VMware datastore leaving the NFS export intact.

CHAPTER 4

ViPR Controller Vblock System Services

This chapter includes the following topics:

- [Vblock System Services](#).....30
- [Use the VCE Vblock System Services to create clusters on the Vblock compute system](#)..... 30
- [Create a new block volume and attach it to the ESX cluster as a datastore](#).....32

Vblock System Services

The **VCE Vblock System Services** is a category of services in the ViPR Controller Service Catalog that are used to manage the compute resources in a Vblock system.

Table 8 ViPR Controller Service Catalog, VCE Vblock System Services

Service	Description
Provision Clusters	Provisions clusters of hosts on the compute system (Cisco Unified Computing System™ (UCS)), installs the operating system (ESX) on the hosts, and adds the cluster to a vCenter data center.
Add Host(s) to Cluster	Creates new hosts on the compute systems, installs the operating system on the hosts, adds the host to a cluster previously created in ViPR Controller, and adds the host to the vCenter datacenter if the vCenter was previously added to ViPR Controller.
Provision Bare Metal Cluster	Provisions clusters on the compute system, without installing an operating system.
Add Bare Metal Hosts to Cluster	Adds a new host to a cluster without installing an operating system on the host.
Update vCenter Cluster	Updates the vCenter with new cluster or host. If creating a new cluster, the cluster is added to the vCenter. If a new host was added to the cluster, and the cluster is already in the vCenter, only the new host is added to the cluster in vCenter.
Decommission Host(s) from Cluster	Decommissions one or more hosts from a cluster that was provisioned by ViPR Controller.
Decommission Cluster	Decommissions an entire cluster that was provisioned by ViPR Controller.

For details about ViPR Controller support for Vblock systems, see *ViPR Controller Support for Vblock Systems*, which is available from the [ViPR Controller Product Documentation Index](#).

Use the VCE Vblock System Services to create clusters on the Vblock compute system

Before you begin

Before you can successfully provision a cluster, ViPR Controller system administrators, and tenant administrators must have configured the necessary projects, physical assets, and virtual assets in ViPR Controller as described in: [Work with service resources](#).

The **Provision Cluster** service performs the following tasks in a single ViPR operation:

- Creates a cluster in ViPR Controller, provisions hosts on the compute system (UCS).
- Creates boot volumes and zones them to their respective hosts.
- Installs the operating system (ESX) on the hosts.
- Adds the cluster to a vCenter data center.

Procedure

1. Go to the **Service Catalog > VCE Vblock System Services > Provision Cluster** service.
2. Complete the order form as follows:

Option	Description
Project	The project in which the cluster will be added after it is created.
Name	The name of the cluster that will be created on the Vblock system and vCenter.
Virtual Array	The virtual array in which the Vblock networks, and boot LUN storage are included.
Compute Virtual Pool	The compute pool containing available compute elements to use in provisioning.
VCE Vblock Compute Image (OS)	The operating system that will be installed on the cluster hosts. A ViPR Controller System Administrator must add the compute image to the ViPR Controller Physical Assets, before the service can be ordered.
Hosts	The host information for each host created in the cluster. Click Add for each additional host to add to the cluster.
Host Name (FQDN)	The fully qualified domain name that will be assigned to each host created in the cluster.
IP Address	The IP Address that will be assigned to each host created in the cluster.
Netmask	Netmask that will be used by all of the hosts in the cluster.
Gateway	Gateway that will be used by the hosts.
Management Network	The Management VLAN over which ViPR Controller will use to communicate with the hosts for management purposes. The management network is required to add the ESX hosts to a vCenter and for any communication between ViPR Controller and the ESX hosts.
NTP Server	NTP Server that will be used by all of the hosts in the cluster.
DNS Servers	Comma separated list of DNS Servers that will be used by the hosts.
Host Root Password	The password that will be assigned to the root user for all the hosts in the cluster.
Block Virtual Pool	The block virtual pool from which the boot LUN will be created.
Size of Boot Volume	The size of the volumes that will be used to boot the hosts.
vCenter	The vCenter in which the datacenter, to which the cluster will be added, resides. A ViPR Controller Tenant Administrator must add the vCenter to ViPR Controller before the service can be ordered.

Option	Description
Datacenter	The vCenter Datacenter to which the cluster will be added. A ViPR Controller Tenant Administrator must add the vCenter to ViPR Controller before the service can be ordered.

3. Click **Order**.

The Orders page is displayed with the progress of the order.

Create a new block volume and attach it to the ESX cluster as a datastore

Once the ESX cluster has been created and added to a vCenter by ViPR Controller you can use the ViPR Controller, Block Storage Services to create a new block volume from the Vblock storage system to allocate to the ESX cluster.

For VNX, an initiator cannot be part of more than one storage group. If there is one storage group for an ESX cluster, ViPR Controller adds the volume to the existing ESX storage group, regardless of the specified storage type.

Procedure

1. Go to the **Service Catalog > Block Services for VMware > Create Volume and Datastore**.
2. Complete the order form:

Option	Description
Datastore name	The datastore name.
VMware vCenter	The vCenter in which the datastore will be created.
VMwarevCenter Datacenter	The vCenter datacenter in which the datastore will be created.
Storage Type	Either, Shared to manage the storage for the entire cluster, or Exclusive to manage the storage for an individual host.
ESX Host/Cluster	The ESX host or cluster to which the storage will be allocated.
Virtual Array	The virtual array from which the storage will be allocated.
Virtual Pool	The virtual pool from which the storage will be allocated.
Project	The project to which the resources will be added. If the Project option is not displayed the service has been locked to a project and is for use only by members of that project.
Name	The volume name.
Consistency Group	Provides protection for the provisioned resource. The selection list contains the consistency groups previously associated with the project. Consistency groups are only required if the virtual pool configuration requires it, otherwise it is optional to choose consistency groups.
Size	The size of the volume.

Option	Description
Multipath Policy	<p>VMware multipath policy to use with ESX hosts or clusters. Options are:</p> <ul style="list-style-type: none"> • Default — To allow ViPR to define the policy. • Fixed — Uses the designated preferred path flag, if it has been configured. Otherwise, it uses the first working path discovered at system boot time. If the ESX host cannot use the preferred path or it becomes unavailable, the ESX host selects an alternative available path. The host automatically returns to the previously defined preferred path as soon as it becomes available again. • Most Recently Used – Selects the first working path. If the path becomes unavailable, the ESX host switches to an alternative path. • Round Robin — Uses an automatic path selection rotating through all available paths. <p>Refer to VMware documentation for further details.</p>
HLU	The Host Logical Unit (HLU). Use -1 to have ViPR Controller automatically assign the HLU.

3. Click **Order**.

The **Orders** page is displayed with the progress of the order.

CHAPTER 5

Monitor, and Troubleshoot ViPR Controller Services

This chapter includes the following topics:

- [Monitoring and troubleshooting a service order](#).....36

Monitoring and troubleshooting a service order

Once a service is ordered, you can watch the progress of the service, and troubleshoot issues with the service from the ViPR Controller user interface, **Orders** page, or the **My Orders** page.

After ordering a service, the order page opens displaying the progress of the order.

Procedure

1. Keep the order page open to continue to watch the progress of the service operation.
If you have left the orders page, go to the **Service Catalog** > **My Orders** page, and you will see the order in the list.
2. Click the order to view the details of the order.
3. Expand the **Logs** section to view the logs entered for the service.
Red text indicates that an error occurred while the service was running, and provides details of the error.
4. Expand **Precheck Steps** to view the steps ViPR performs before executing the service.
The order will not proceed if any of the precheck steps fail.
5. Expand **Execution Steps** to view the steps ViPR performs to complete the service order.
Red text indicates an error occurred during the service execution and the point in the execution steps where an error occurred.
6. Expand **Tasks** to view the details of each specific task run to complete the order. If an order failed, the Tasks will show the specific task where the order to fail.

CHAPTER 6

Work with Service Resources

This chapter includes the following topics:

- [Working with service resources](#) 38
- [Block storage systems under ViPR Controller management](#) 42
- [File storage systems under ViPR Controller management](#) 42

Working with service resources

Once a service operation has completed successfully, the resources are put into the project that was assigned in the service order. The resources can then be viewed, and deleted through the ViPR Controller user interface **Resources** pages.

Before you begin

Provisioning users can only select the projects to which they have been assigned, and can only see the resources in those projects.

Tenant administrators can see all projects and all project resources.

Procedure

1. Open the Resources menu, and select the type of resource to view:

- Volumes
- Block Snapshots
- Consistency Groups
- Export Groups
- File System
- File Snapshots

2. Select the project in which the resource belongs.

A list of the resources, of the selected type, appear in the table. For example, if you selected **File System**, a list of file systems that were provisioned in the selected project appears in the **File System** table.

If you selected **Volumes**, a list of block volumes that were provisioned in the selected project appears in the **Volumes** table.

3. Select the box for the row, and click **Delete** to delete the resource.

4. Click anywhere in the row, to see more details for the resource.

How ViPR Controller deletes Masking Views for VMAX and VNX for Block storage

ViPR Controller sets the Solutions Enabler `DeleteWhenBecomcesUnassociated` flag to true when it is used to provision VMAX, or VNX for Block storage.

Note

Non-ViPR Controller created groups will have this flag set to FALSE, this an SMI-S API exposed parameter.

When ViPR Controller is then used to delete or decommission the storage previously created and provisioned by ViPR Controller, the masking views will be deleted or decommissioned as follows:

Example 1 Example 1

Deleting a Masking View with the `DeleteWhenBecomcesUnassociated` group flag set to `TRUE` at the parent groups will only delete the parent, since the children do not have the flag set to `TRUE` also.

Example 1 Example 1 (continued)

Deleting a Masking View with the `DeleteWhenBecomcesUnassociated` group flags set at only the parent groups, will only delete the groups if they are not part of any other masking view.

Example 2 Example 2

Deleting a masking view with the `DeleteWhenBecomcesUnassociated` group flag set to `TRUE` at both parent and child group levels will delete all groups at all levels.

Deleting a Masking View with the `DeleteWhenBecomcesUnassociated` group flags set to `TRUE` at both parent and child group levels will **ONLY** delete these groups if they are **NOT** part of any other masking view.

Example 3 Example 3

Deleting a masking view with the `DeleteWhenBecomcesUnassociated` group flags set to `TRUE` at the child group, will only delete the child group leaving the parent intact.

Deleting a Masking View with the `DeleteWhenBecomcesUnassociated` group flags set to `TRUE` at the child group, will only delete the child group if they are not part of any other masking view.

Note

However, if the storage group is FAST managed, it will not get deleted.

File System Resources

The File System Resources view enables the file systems that have been created in ViPR, and are under ViPR management, to be displayed and enables individual file systems to be viewed and managed.

The File Systems table enables you to view the file systems that have been created, their size, the virtual array and virtual pool to which each belongs, and the protocols they support.

The File System page for each resource comprises the areas detailed in the table below.

Area	Description
File System Summary	Provide summary information for the file system: Its size, supported protocols (NFS and/or CIFS), mount path and the ViPR virtual array and virtual pool that it belongs to.
File System Details	Provides additional details about the file system.
Export Rules	Lists the NFS exports that have been created for the file system and the security associated with each rule. The mount point displayed can be used to mount the NFS export on a host to which it has been exported. Provides operations that enable:

Area	Description
	<ul style="list-style-type: none"> • Modify the rule by adding or removing allowed hosts and changing the permissions associated with a host. • Delete a rule. • Add a Rule <hr/> <p>Note</p> <p>Adding an export rule is not supported for Isilon storage systems</p>
Shares	<p>Lists the CIFS shares associated with a file system. A file system can be shared with a number of names. The Shares area provides options to perform the following tasks:</p> <ul style="list-style-type: none"> • Delete — to delete the CIFS share • Share — to add a CIFS share at the subdirectory level. The subdirectory must already exist on the file system. • Access Control — access control can be added, modified, or deleted from the share for Isilon, and NetApp 7-mode, and NetApp Cluster-mode storage systems. Two types of users, or groups can be used for ACLs <ul style="list-style-type: none"> ▪ Domain users or groups — must be registered on the domain controller and the storage system's data mover has to be added to the domain. ▪ Local users or groups — can be a local user or group, or part of the Authentication Provider (For example, AD, LDAP), which is configured on the storage system.
Snapshots	Lists the snapshots that have been created for the file system.
Quota Directory	Lists any quota directories that have been created and allows them to be deleted or modified. The modify action allows you to change the size of the quota directory and set its security style.
Tasks	Lists the tasks associated with the file system that have been performed. The task details can be displayed, which in turn, can be used to link back to the original order.

Deleting a file system

You can delete a file system from the **Resources > File Systems** page if you have removed all of its associated exports, shares, snapshots, and quota directories. However, even if you have removed all of the Export Rules, you must also ensure that any NFS exports have been removed using the **Service Catalog > View Catalog > File Storage Services > Remove NFS Export for File System** service.

File System Snapshot Resources

The File System Snapshots page enables the file system snapshots that have been created in ViPR and are under ViPR management to be displayed, and enables individual snapshots to be viewed and managed.

The File Snapshots table enables you to view the snapshots that have been created and select a snapshot in order to view its details.

The Snapshots page for each resource comprises the areas detailed in the table below.

Area	Description
Snapshot Summary	Provide summary information for the file system: Its size, supported protocols (NFS and/or CIFS), mount path and the ViPR virtual array and virtual pool that it belongs to.
Snapshot Details	Provides additional details about the snapshot.
Export Rules	<p>Lists the NFS exports that have been created for the file snapshot and the security associated with each rule.</p> <p>The mount point displayed can be used to mount the NFS export on a host to which it has been exported.</p> <p>Provides operations that enable:</p> <ul style="list-style-type: none"> • Modify the rule by adding or removing allowed hosts and changing the permissions associated with a host. • Delete a rule. • Add an Export Rule. <hr/> <p>Note</p> <p>Adding an export rule is not supported for Isilon storage systems</p>
Shares	<p>Lists the CIFS shares associated with a snapshot.</p> <p>The Shares area provides options to perform the following tasks:</p> <ul style="list-style-type: none"> • Delete — to delete the CIFS share snapshot • Add Share — to add a CIFS share to the snapshot at the subdirectory level. The subdirectory must already exist on the file system. • Access Control — access control can be added, modified, or deleted from the snapshot for Isilon, NetApp 7-mode, and NetApp Cluster-mode storage systems. Two types of users, or groups can be used for ACLs <ul style="list-style-type: none"> ▪ Domain users or groups — must be registered on the domain controller and

Area	Description
	<p>the storage system's data mover has to be added to the domain.</p> <ul style="list-style-type: none"> ▪ Local users or groups — can be a local user or group, or part of the Authentication Provider (For example, AD, LDAP), which is configured on the storage system.
Tasks	Lists the tasks associated with the snapshot that have been performed. The task details can be displayed, which in turn, can be used to link back to the original order.

Deleting a file snapshot

You can delete a file snapshot from the **Resources > File Snapshots** page if you have removed all of its associated exports and shares. However, even if you have removed all of the Export Rules, you must also ensure that any NFS exports have been removed using the **Service Catalog > View Catalog > File Protection Services > Remove NFS Export for Snapshot** service.

Block storage systems under ViPR Controller management

Once a volume 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 volume 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. Some examples of failures that could occur when the element manager and ViPR database are not synchronized are:

- 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 on the same storage system, the storage system may be locked by the operation run from the element manager, causing the ViPR "Create a Volume" operation to fail.
- After a volume was exported to a host through ViPR, the same masking view, which was used by ViPR during the export, was changed on the storage system through the element manager. When ViPR attempts to use the masking view again, the operation will fail because what ViPR has in the database for the masking view is not the same as the actual masking view reconfigured on 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.

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.

