EMC ViPR Controller

Version 3.6

User Interface Virtual Data Center Configuration Guide

302-003-712

REV 01

EMC²

Published May 2017

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

CONTENTS

FIGURES

TABLES

CHAPTER 1

Virtual Data Center Configuration Overview

This chapter contains the following topics:

Overview of ViPR Controller Virtual Data Center Deployment Options

After EMC ViPR Controller installation, ViPR Controller System Administrators and Tenant Administrators can use the ViPR Controller UI, REST API, or CLI to configure the ViPR Controller Virtual Data Center (VDC). This document provides the steps to configure the ViPR Controller VDC using the ViPR Controller UI.

Related documents

Before you begin the VDC configuration, review the *ViPR Controller Virtual Data Center Requirements and Information Guide*.

To configure a VDC using the ViPR Controller REST API, see the *EMC ViPR Controller REST API Reference*.

To configure a VDC using the ViPR Controller CLI, see the *ViPR Controller CLI Reference Guide*.

All documents are available from the ViPR Controller Product Documentation Index .

Guided versus Manual VDC deployment

TheViPR Controller UI provides two ways to configure your virtual data center:

- Guided — The **Getting Started Guide**, which walks you through the VDC configuration process, is provided in the ViPR Controller UI for VMAX All Flash, Unity All Flash, and XtremIO storage systems. For details see: Guided Licensing, Initial Setup, and Deployment of your Virtual Data Center.
- Manual — You must manually create the VDC for all storage systems other than VMAX All Flash, Unity All Flash, and XtremIO storage systems. You also have the option of manually creating a VDC for your VMAX All Flash, Unity All Flash, and XtremIO storage systems. You are not required to use the guided option for any storage system. For details see: Step-by-step overview: to manually configure a ViPR Controller VDC on page 12.

Step-by-step overview: to manually configure a ViPR Controller VDC

After you install and configure ViPR Controller, set up the virtual data center in ViPR Controller. You must manually create the VDC for all storage systems other than VMAX All Flash, Unity All Flash, and XtremIO storage systems. You also have the option to manually configure a VDC for your VMAX All Flash, Unity All Flash, and XtremIO storage systems.

The following steps are required to build your VDC from the ViPR Controller UI. .

1. Review the physical asset version requirements in the ViPR Controller Support Matrix, which is available from the EMC Community Network.
2. Review the configuration requirements, and information for the ViPR Controller physical and virtual assets in the *ViPR Controller Virtual Data Center Requirements and Information Guide*, which is available from the ViPR Controller Product Documentation Index .
3. Add physical assets to ViPR Controller.
   - Add storage systems (**Physical** > **Storage Systems**).

- Add data protection systems (**Physical** > **Data Protection Systems**).
- Add fabric managers and SAN networks (**Physical** > **Fabric Managers**).
- Add hosts and clusters (**Physical** > **Hosts, Clusters**).
- Add vCenters and ESX/ESXi clusters (**Physical** > **vCenters**).
- For VCE Vblock systems, Add a Vblock compute system (**Physical** > **Vblock Compute Systems**) and compute images (**Physical** > **Compute Images**).

4. Create ViPR Controller virtual assets.
   - Create and configure a virtual array. (**Virtual** > **Virtual Arrays**).
   - Create virtual pools.
     a. Create Block virtual pools (**Virtual** > **Block Virtual Pools**).
     b. Create File virtual pools (**Virtual** > **File Virtual Pools**).
     c. Create Compute virtual pools (**Virtual** > **Compute Virtual Pools**) .

Guided Licensing, Initial Setup, and Deployment of your Virtual Data Center

The ViPR Controller UI Getting Started Guide is used to quickly and easily navigate you through:

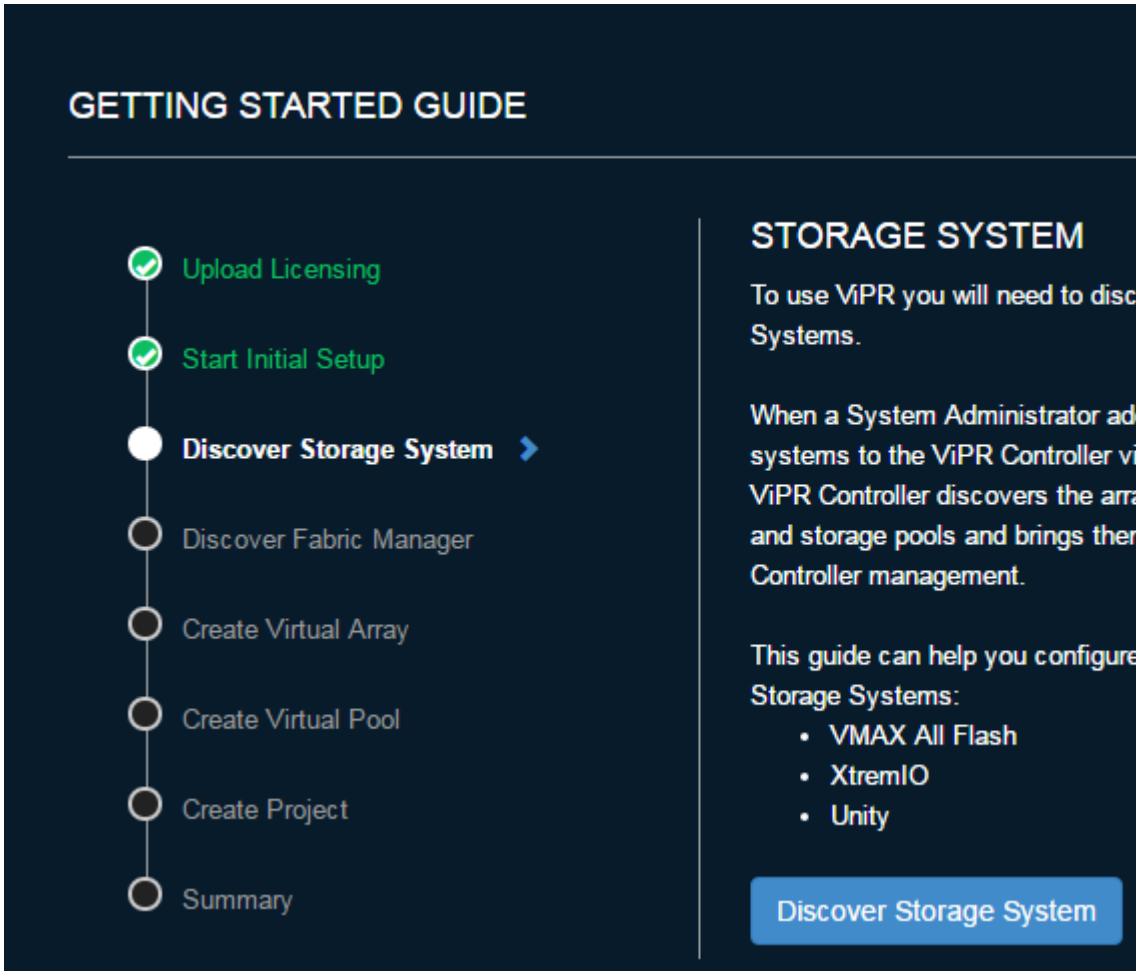
- The licensing and set up process when setting up your ViPR Controller instance.
- Setting up your virtual data center, and provisioning storage when using ViPR Controller to manage VMAX All Flash, Unity All Flash, or XtremIO storage systems.

Configuration requirements
Review the following before using the Getting Started Guide to configure your VDC:

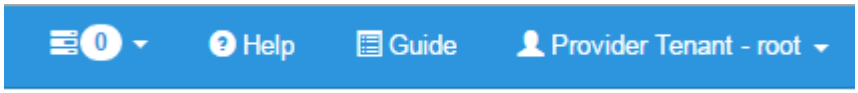
- The **Getting Started Guide** can only be used for VMAX All Flash, Unity All Flash, or XtremIO storage systems.
- You must be assigned both System Administrator and Tenant Administrator roles in ViPR Controller to complete all the steps in the **Getting Started Guide**.
- While in the guide, ViPR Controller will allow you to add non-flash VMAX, and Unity storage systems, however an error will occur when you attempt to create the virtual array through the Getting Started Guide.
- The **Getting Started Guide** is only for basic configurations. You will not be able to use the guide to configure complex configurations such as configurations which include EMC data protection systems.

ViPR Controller UI
The **Getting Started Guide** opens the first time you log into the ViPR Controller UI and automatically walks you through the licensing and initial set up steps.

If you are provisioning with VMAX All Flash, Unity All Flash, or XtremIO storage systems, the **Getting Started Guide** takes you through the necessary steps to build your VDC, and provision storage.



Additionally, you have the option to close out of the ViPR Controller **Getting Started Guide** at any time. ViPR Controller checks off each step that you have completed, allowing you to go back to the guide, and begin where you left off. Simply, click the **Guide** option in the upper, right menu of the ViPR Controller UI to re-enter the guide at the same point from which you exited the guide



CHAPTER 2

Adding and Configuring Physical Assets

This chapter contains the following topics:

Add storage to ViPR Controller

When you add a storage system to ViPR Controller, ViPR Controller discovers, and registers the storage system and the storage system resources. Once the storage system is discovered by ViPR Controller, there are optional configuration steps that can be performed on the storage system resources.

Before you begin

To see the configuration requirements for the type of storage system you are adding to ViPR Controller, see the *ViPR Controller Virtual Data Center Requirements and Information Guide*, which is available from the ViPR Controller Product Documentation Index .

Procedure

1. Log into the ViPR Controller UI with System Administrator privileges.
2. Select **Physical** > **Storage Systems**

   Block storage systems can also be added to ViPR Controller from the **Physical** > **Storage Providers** page.
3. Click **Add**.
4. Select the storage system or storage provider type.

   Choose one of two ways to add the IBM XIV storage system:

   a. SMI-S only (this is the same as in previous ViPR Controller releases)

   b. SMI-S plus Hyper Scale Manager

   The SMI-S Provider for IBM XIV can have up to three redundant storage providers. You specify each one separately on the **Add Storage System** screen. If more than one SMI-S Provider for IBM XIV exists, ViPR Controller randomly selects one of them as the active one and adds any remaining ones to the passive list.
   IBM Hyper Scale Manager is optional; however, you cannot delete HSM after adding it. (HSM is used for making the REST API call to IBM XIV.)

   If you want to discover eNAS file systems on VMAX3 storage systems, select **EMC VNX File** to add the VMAX3 storage system, and eNAS file systems.
5. Type the storage system name.
6. Type the host IP address.
   - For ScaleIO Gateway, type the FQDN or IP Address of the ScaleIO Gateway host.
   - For VPLEX , type the FQDN or IP Address for the VPLEX management server.
   - You must use the management IP when discovering NetApp Cluster-mode storage systems with ViPR Controller. You cannot discover NetApp Cluster-mode storage systems using LIF IP.
   - For EMC XtremIO, type the IP address for the XtremIO Management Server.
7. If adding block storage, enable if SSL will be used.
8. Leave the default or enter the port.

- ForScaleIO Gateway, enter the port used to communicate with the ScaleIO REST API service.
- For EMC XtremIO, enter the port used to communicate with the XtremIO Management Server

9. Type the user credentials with storage system administrator privileges.
   - The credentials entered when you add a storage system to ViPR Controller are independent of the currently logged in ViPR Controller user. All ViPR Controller operations, which you perform on a storage system, are executed as the user that is entered when the storage system is added to ViPR Controller. .
   - ViPR Controller operations require that the ViPR Controller user has administrative privileges.
   - If the OpenStack Block Storage System nodes are installed on separate servers, enter the OpenStack Block Storage (Cinder) Controller node credentials.
   - If adding EMC XtremIO, type the username and password of a user that has administrative access to the XtremIO Management Server
10. If adding VNX for File:
    a. Type the Onboard storage provider host.
    b. Enable or disable SSL access to the storage provider.
    c. Leave the default or type the port to access the storage provider.
    d. Enter the user credentials to access the Onboard Storage Provider.
11. If adding ScaleIO Gateway,
    a. Type the **MDM User** and **MDM Password** with a user that can access the Primary MDM.
12. Click **Save**

Results

- All added storage systems are displayed on the **Storage Systems** page.
- If adding block storage, the storage provider is displayed on the **Storage Provider** page.
- A green check in the **Status** column indicates that ViPR Controller has successfully discovered, and registered the storage system.
- For EMC XtremIO, each cluster is discovered and registered as a storage system.
- For ScaleIO, ViPR Controller automatically creates storage ports, hosts and host initiators. ViPR Controller automatically creates a network for the ScaleIO using the SDCs, and the storage ports that were created from all of the discovered SDSs. These can not be edited.

Table 1 Mapping of ScaleIO components to ViPR Controller components

ScaleIO component	ViPR Controller component
Protection Domain	Storage System
Storage Pool	Storage Pool

Table 1 Mapping of ScaleIO components to ViPR Controller components (continued)

ScaleIO component	ViPR Controller component
SDS	Storage Port **Note** The name of the storage port maps to the name of the SDS ID.
SDC	Host

Configuring storage systems added to ViPR Controller

After a storage system is added to ViPR Controller, the associated networks must be added or configured, if required the data protection system must be added to the physical assets. Additionally, the storage system resources can be configured to support your environment.

Network configuration for storage systems

After the storage system is added to ViPR Controller, you can configure the storage system networks in the **Physical**, **Fabric Manager**, and **Networks**.

Fibre Channel
Add the corresponding SAN Switch from the ViPR Controller UI **Physical** , **Fabric Manager** page. For specific steps see: Add Fabric Managers (SAN switches) to ViPR Controller

When a SAN switch is added to ViPR Controller, the SAN networks (Brocade Fabrics or Cisco VSANs), are automatically discovered and registered in ViPR Controller. Through discovery of the SAN switch topology, ViPR Controller discovers, and identifies which storage systems that are associated with the SAN switch. During provisioning ViPR Controller automatically selects the storage and host ports that will be used to connect the hosts and storage.

Optionally, ViPR Controller allows you to customize the paths in the SAN networks to use during provisioning.

IP Networks
If your storage is connected through IP networks , you will need to create the IP networks in the ViPR Controller Physical Assets, or virtual array. While creating the IP networks, be sure to add the necessary storage and host ports to use to provision the storage to the hosts.

iSCSI
For Storage Systems that use ViPR Controller services with the iSCSI protocol, the iSCSI host ports must be logged into the correct target array ports before they can be used in the service.

For network configuration details see: Configuring Networks in the ViPR Controller.

Deregister or delete a storage system from ViPR Controller

Deregister a storage system to keep the storage system in ViPR Controller but not allow ViPR Controller to use any of the available storage resources. Delete a storage system to remove it completely from ViPR Controller.

Block storage systems

Block storage systems are added to ViPR Controller by adding the storage provider. When you add a storage provider to ViPR Controller, you add all the storage systems managed by the provider to ViPR Controller. If you want ViPR Controller to manage only some of the storage systems discovered with the storage provider, you can deregister or delete the storage system from ViPR Controller.

Deregister or delete a storage system

Before you begin

- You cannot delete a storage system that has resources currently under ViPR Controller management.
- You can deregister a storage system that has resources currently under ViPR Controller management. Once deregistered, the resources under ViPR Controller management remain under ViPR Controller management, but no more of the storage system resources are used by ViPR Controller.

Procedure

1. Navigate to **Physical** > **Storage Systems**.
2. Select the box in the storage system row.
3. Do one of the following:
   - Click **Deregister** to keep the storage system in ViPR Controller and make it unavailable to use as a ViPR Controller resource.
   - Click **Delete** to remove the storage system from ViPR Controller.

Define the storage system resource allocation limit

By default, storage systems are configured with unlimited resources that ViPR Controller can use. You can set resource limits that define the amount of storage in the system available for use by ViPR Controller.

Procedure

1. Select **Physical** > **Storage Systems**.
2. Click the storage system name in the **Storage System** table.
3. In the **Edit Storage System** page, disable **Unlimited Resource Allocation** setting.
4. For block storage, specify the maximum number of volumes, for file storage specify the maximum number of file systems to allocate to ViPR Controllerfor provisioning on this storage system. The amount must be 0 or higher.

   The Resource Limit value is a count of the number of volumes, or file systems allowed to be provisioned on the storage system.
5. Click **Save.**

Deregister storage pools

By default, all discovered storage pools are available for provisioning in ViPR Controller. To make storage pools unavailable to ViPR Controller for provisioning, deregister them.

If a storage pool becomes unavailable on the storage system, the storage pool remains in the list of available ViPR Controller storage pools. You must deregister the storage pool manually in ViPR Controller to ensure ViPR Controller does not use it as a resource when a service operation is executed.

Note

This operation does not apply to VPLEX storage systems.

Procedure

1. Select **Physical** > **Storage Systems**.
2. Locate the row for the storage system in which the pools reside.
3. In the **Edit** row, click **Pools**.
4. Check the row for each pool that you want to make unavailable to ViPR Controller for provisioning.
5. Click **Deregister**.

Set the storage pool utilization limits

Storage pool utilization limits enable you to define the maximum amount of storage that ViPR Controller can use from a storage pool, the maximum number of block volumes, or file systems that ViPR Controller can provision from a storage group, and the maximum subscription percentage for thin pool provisioning.

Note

This operation does not apply to VPLEX storage systems.

Procedure

1. Select **Physical** > **Storage Systems**.
2. Locate the row for the storage system where the pools reside.
3. In the **Edit** row, click **Pools**.
4. Click the pool name.
5. Change the maximum utilization percentage.

   The default is 75%.
6. For block storage, thin pool provisioning, set a maximum snapshot percentage.

   The default is 300%.
7. Enter a numeric value for the block volume, or file system limit available to ViPR Controller to provision from this storage pool.

   By default, there is no limit on the amount of storage from a storage pool that can be used by ViPR Controller.

   The Resource Limit value is a count of the number of block volumes, or file systems allowed to be provisioned using the selected storage pool.

8. Click **Save**.

Storage ports

The **Physical** > **Storage Systems**, **Storage Ports** page is used to view the storage ports, and storage port attributes for the selected storage system, and to register and deregister the ViPR Controller storage ports.

Table 2 Storage port attributes and options

Column name	Description
Name	Storage port name.
Registered	Check ✔ indicates the storage port is registered. ✖ indicates the storage port is not registered with ViPR Controller.
Group	The storage group to which the storage port belongs.
Identifier	The Storage Port World Wide Name.
IQN	
Alias	Storage port alias if configured on the switch. If the column is empty, ViPR Controller did not discover an alias for the storage port with the switch.
Type	Protocol type: FC, iSCSI, or IP
Allocatable	A "thumbs up" icon indicates that the port is allocatable.
DR Port	For Isilon systems, a checkmark indicates that the port is designated as a Disaster Recovery port.
Status	Displays the storage port registration and operational status. See the following Storage port registration and operational status table.

Table 3 Storage port registration and operational status

Icon	Meaning
✔	Storage port operation and registration was successful.
✖	Error occurred either during the storage port operation, or while registering the storage port.
?	Storage port registration, or operational status unknown. ViPR Controller is unable to detect the storage port status for Isilon, VPLEX, VNX File, and NetApp storage systems. The unknown status will always appear for these storage ports.

Storage port registration

By default ports are automatically registered with ViPR Controller when the storage system is discovered. Optionally, ports can be deregistered to make them unavailable to be used by ViPR Controller. Deregistered ports can always be registered again at a later date.

To register or deregister a storage port:

1. Select **Physical** > **Storage Systems**.
2. Locate the row for the storage system in which the ports reside.
3. Click **Ports** in the **Edit** column.
4. Select the box in the first column of the port row.
5. Click **Register** to register the port for use in ViPR Controller, or **Deregister** to make the port unavailable for use in ViPR Controller.

Storage port registration as a Disaster Recovery port
For Isilon systems, it is recommended that there be a dedicated SmartConnect Zone for data access, per SyncIQ Policy, rather than sharing the SmartConnect Zone between policies. After a port is registered as a Disaster Recovery port, the dedicated port is picked up for SyncIQ activities.

To register a storage port as a Disaster Recovery port:

1. Select **Physical** > **Storage Systems**.
2. Locate the row for the storage system in which the ports reside.
3. Click **Ports** in the **Edit** column.
4. Select the box in the first column of the port row.
5. Click **Set as DR Port** to register the storage port as a Disaster Recovery port, or **Unset as DR Port** to de-register the storage port as a Disaster Recovery port.

Deregister storage ports

By default, all storage ports are available for provisioning in ViPR Controller after ViPR Controller discovers, and registers the storage system. To make storage ports unavailable to ViPR Controller for provisioning, deregister them.

Note

This operation does not apply to third-party storage systems added through OpenStack.

Procedure

1. Select **Physical** > **Storage Systems**.
2. Locate the row for the storage system where the port resides.
3. In the **Edit** row, click **Ports**.
4. Check the row for each port that you want to make unavailable to ViPR Controller for provisioning.
5. Click **Deregister**.

Hitachi Data Systems Host Mode options

Host Modes are Hitachi Data Systems (HDS) flags set on HDS host groups when an HDS storage volume is exported to a host group. The Host Mode optimizes the connection and communication between HDS storage and the host to which the HDS volume is exported.

The Host Mode options are a set of flags that you enable 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 its options.

Customize the Host Mode Option

The Host Mode Option is customized from the **Controller Configurations** page.

Before you begin

Only ViPR Controller System Administrators can customize the Host Mode Option.

Procedure

1. Go to the **Physical** > **Controller Config** > **HDS** tab.
2. Select the Host Mode Option, from the drop-down box.
3. Click **Add**.
4. Select **Host Type** in the Scope Type column.
5. Select the type of operating system in the Scope Value column.
6. Leave the defaults, or enter the numeric value for the Host Mode Option in the Values column.
7. Click Save.

Note

Even though the UI shows multiple entries for the same Host Type, only the last one is actually used by ViPR Controller.

Configuring multipathing for Third-Party Block (OpenStack) storage systems

ViPR Controller System Administrators can learn the necessary information to configure multipathing for third-party block storage.

ViPR Controller uses the OpenStack Block Storage (Cinder) service to support third-party block storage systems that are not supported natively. Throughout this document, wherever third-party block storage is mentioned, it refers to OpenStack Block Storage (Cinder), unless otherwise noted.

ViPR Controller supports multipathing on third-party block storage only for Fibre Channel.

Configuration requirements

Before configuring multipathing for third-party block storage, validate that the environment meets the following requirements.

To configure multipathing for third-party block storage, you must have at least two paths from the host to the storage system and at least two storage ports on the storage system.

OpenStack Cinder requirements

- At least one Cinder storage backend must be configured.
- The volume types must be created and mapped for each configured backend driver.

ViPR Controller requirements

- The Cinder storage backends must be discovered as storage systems in ViPR Controller.
- The volume type on the Cinder storage backend must be discovered as a storage pool of a specific storage system in ViPR Controller.
- The Fabric Manager in which the storage system and participating hosts are connected must be discovered.
- The host to which volumes need to be attached must be added and its Fibre Channel initiators discovered. When adding the host, select the `discoverable` attribute so that host initiators will be discovered automatically. If you are using a VMware ESX host, discover it by adding the vCenter in which the host is present.
- Verify that all discovered initiators are automatically assigned to a virtual network based on the connectivity.

Create a storage port using the ViPR Controller UI

Create a third-party block storage system port.

Before you begin

Only System Administrators can create storage ports.

Ensure that you have the correct port WWN.

The following procedure describes how to create the storage port using the ViPR Controller UI.

Procedure

1. Select **Physical** > **Storage Systems**.
2. From the list of storage systems, select the third-party block storage system to which to add storage ports.
3. In **Edit**, click **Ports** to see the list of ports that are available. If no ports were created, a single dummy or unusable port displays.
4. Click **Add** to enter the new port information.
5. Click **Save**.

Results

The newly added port displays in the list of ports.

Create a storage port using the ViPR Controller CLI

Create a third-party block storage system port.

Before you begin

Only System Administrators can create storage ports.

Ensure that you have the correct port WWN.

The following procedure describes how to create the storage port using the ViPR Controller CLI. For more information see the *EMC ViPR Controller CLI Reference* Guide, which is available from the ViPR Controller Product Documentation Index .

Procedure

1. List the storage systems.

```
viprcli storagesystem list
```

Note the last three digits of the serial number of the storage system to which the storage port needs to be added.

2. Create the storage ports.

   ```
   viprcli storageport create -portname|pn portname -pid
   wwn_of_the_port -transporttype|tt transport_type -
   systemtype|st storage_type -serialnumber|sn serialnumber
   ```

3. List the storage ports for the storage system to ensure that the new storage port created successfully.

   ```
   viprcli storageport list -sn serialnumber -t storage_type
   ```

Discover storage ports dynamically

The alternative to creating storage ports manually is to discover multiple storage ports dynamically by performing an export or attach volume operation to a host.

While discovering multiple storage ports dynamically is supported, create storage ports manually when possible.

Procedure

1. Create a new single storage port or modify the existing dummy storage port by modifying its WWN to the correct and valid WWN of a storage port of the storage system.
2. Create a virtual array and then select the Automatic type of SAN Zoning.

   Automatic allows ViPR Controller to automatically create the required zones in the SAN fabric when a provisioning request is made in this virtual array.

3. Add a network for the virtual array in which the storage system port displays.

   The storage system displays as an associated entity in virtual array.

4. Create the virtual pool by associating it with the created virtual array.
   a. Select **FC** as the protocol type.
   b. In **SAN Multi Path**, set the minimum and maximum paths and the paths per initiator to **1**.

      All matching pools of storage system display.

   c. Save the virtual pool.
5. Create a project in which you want to assign the new resources.
6. Create a volume resource using the Service Catalog or CLI.
7. Export the newly created volume to the host.
8. Verify that the volume export is successful in **Resources** > **Volumes** > **Volume**.

   Because the host to which the volume is exported has multiple paths to the storage system, the initiator to target mapping data from the export response should contain one initiator to multiple storage ports mapping. Any new storage ports apart from the one that was discovered in the initial discovery will get added to the virtual array.

Data protection configuration for storage systems

ViPR Controller supports EMC RecoverPoint and SRDF protection.

EMC RecoverPoint
ViPR Controller supports RecoverPoint protection for VMAX, and VNX for Block storage.

RecoverPoint is added to ViPR Controller from the ViPR Controller UI **Physical** > **Data Protection Systems** page.

For further information:

- To add RecoverPoint to ViPR Controller see: Add data protection systems to ViPR Controller.
- About the RecoverPoint configurations supported by ViPR Controller see: *ViPR Controller Support for VPLEX and VPLEX with EMC Data Protection User and Administration Guide*, which is available from the ViPR Controller Product Documentation Index .

EMC SRDF
ViPR Controller supports SRDF protection for VMAX storage.

ViPR Controller discovers the SRDF protection with the storage system. If the storage system has been configured with SRDF, you configure the ViPR Controller virtual arrays, and virtual pools for SRDF protection as required.

For further information:

- To create and configure virtual arrays, and virtual pools see: Creating, and Configuring the Virtual Data Center, Virutal Assets
- About ViPR Controller support for SRDF see: *ViPR Controller Integration with VMAX and VNX Storage Systems Guide*, which is available from the ViPR Controller Product Documentation Index .

Add data protection systems to ViPR Controller

The following steps describe how to add a data protection system to ViPR Controller using the ViPR Controller UI.

Procedure

1. Select **Physical** > **Data Protection Systems**.
2. Click **Add**.
3. Type the data protection system **Name**.
4. Select the data protection system **Type**.
5. Type the fully qualified domain name or IP address of the **Host**.
6. Leave the default or type the **Port**.
7. Type user credentials that have system administrator privileges.
8. Click **Save**.

Add Fabric Managers (SAN switches) to ViPR Controller overview

ViPR Controller System Administrators can learn the steps to add Fabric Managers (SAN switches) to the ViPR Controller physical assets.

ViPR Controller provides support for Brocade, and Cisco switches.

When you add a switch to ViPR Controller, ViPR Controller discovers and registers the Brocade fabrics, and Cisco VSANs with the switch. Through discovery of the switch topology, ViPR Controller can identify the hosts and storage systems connected through the same switch. This allows ViPR Controller to automatically build the connectivity between the hosts and storage systems when you run a provisioning service, such as "Creating a block volume for a host."

Adding a switch to ViPR Controller

Add a Brocade or Cisco switch to ViPR Controller.

Before you begin

When adding a Brocade switch:

- You must use the log in credentials for the EMC Connectrix Manager Converged Network Edition (CMCNE) currently being used to manage the switch. The CMCNE log in credentials must have administrator privileges to the switch, and the account must have been configured with privileges to discover SAN topology, and to activate, create, and delete zones and zonesets.
- The CMCNE log in credentials, which will be used to add the Brocade switch to ViPR Controller, must have administrator privileges to the switch, and the account must have been configured with privileges to discover SAN topology, and to activate, create, and delete zones and zonesets.

Procedure

1. Go to the **Physical** > **Fabric Managers** page.
2. Click **Add**.
3. Select the type of switch.
4. Type the SMI-S host address for the Brocade switch, or the host address for the Cisco switch.
5. Enable or disable **SSL**.
6. Leave the default, or type the port (SMI-S port for Brocade).
7. Type the credentials for an account that has administrator privileges to the Brocade SMI-S provider, or the Cisco switch..
8. Click **Save**.

   ViPR Controller discovers, and registers the switch and associated fabrics. The **Physical**> **Fabric Managers** page displays the switch and the **Physical**> **Networks** page displays the Fabrics and VSANs.

After you finish

For Cisco switches, each VSAN you configured to work with ViPR Controller should be visible from at least one registered switch in ViPR Controller. If multiple registered switches have access to the same VSAN, ViPR Controller will take the switches

directly connected to the storage port being zoned as the control point to add or remove zones.

Add Vblock system components

You must add each Vblock system component to ViPR Controller as an individual physical asset. Once all of the physical assets of the Vblock system have been added to ViPR Controller, you can set up storage visibility using the ViPR Controller virtual arrays. After configuring virtual arrays, you can configure ViPR Controller compute virtual pools.

Before adding the Vblock system components to ViPR Controller, review the Vblock system requirements and information described in the *ViPR Controller Virtual Data Center Requirements and Information Guide* which is available from ViPR Controller Product Documentation Index .

Vblock system components that must be added to ViPR Controller

At a minimum, the following Vblock components must be added to the ViPR Controller physical assets, to use ViPR Controller to perform bare metal provisioning on the Vblock compute systems during a provisioning operation.

- Vblock storage system
  See the section of this guide which provides the steps to add the type of storage system which is configured in your Vblock system.
- Vblock Fabric managers (Cisco MDS)
  See: Adding a switch to ViPR Controller
- Vblock compute system (UCS)
  See: Add a Vblock compute system to ViPR Controller

Add and configure components for OS Installation

In addition to the components listed above, if you plan to install an operating system on the Vblock compute systems during a Vblock system provisioning service operation, you will need to perform the following steps:

1. Add at least one compute image server as described in: Add a compute image server to ViPR Controller.
2. Add at lease one compute image as described in: Add compute images to ViPR Controller
3. Add at least one Vblock compute system as described in: Add Vblock compute system to ViPR Controller.
4. Associate each compute system with a compute image server as described in: Add Vblock compute system to ViPR Controller.

Add a compute image server to ViPR Controller

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

Before you begin

- For the ViPR Controller user roles required to perform this operation see the *ViPR Controller Virtual Data Center Requirements and Information Guide*, which is available from the ViPR Controller Product Documentation Index .
- Changes that you make to these properties will initiate a reboot of ViPR Controller nodes when you click **Save**.

Note

Rebooting the ViPR Controller nodes may disrupt ViPR Controller processes currently running.

Procedure

1. Go to the **Physical** > **Compute Image Servers** page.
2. If you are adding a new compute image server, click **Add**.

   If you are editing the properties of a compute image server, click the server name.
3. Enter values for the properties.

Option	Description
Name	Enter a name for the compute image server.
Image Server IP Address	FQDN or IP address of the compute image server.
OS Install Network IP Address	IP address of the OS Install Network. The OS Install Network is the second network configured when the compute image server was deployed.
Username	Leave the default username, Root, or enter a new user name ViPR Controller will use to access the compute image server.
Password	Password for the compute image server user name.
Confirm Password	Confirm the password for the compute image server name.
TFTPBOOT Directory	Path to TFTPBOOT directory on the compute image server. Original value is /opt/tftpboot/.
OS Install Timeout in seconds	Timeout value for OS installation (in seconds). Original value is 3600.
Timeout in seconds for SSH commands sent to Image Server	
Image Import Timeout in seconds	

4. **Save**.

Add compute images to ViPR Controller

Compute Images are operating system (OS) installation files (ISO images) that ViPR Controller uses to deploy operating systems on Vblock compute elements that were registered to ViPR Controller. If ViPR Controller is used to provision ESX clusters, it can also be used to add the cluster to a vCenter datacenter that was registered to ViPR Controller.

Before you begin

Procedure

1. Go to the **Physical** > **Compute Images** page.
2. Click **Add**.
3. Complete the following fields.

Option	Description
Name	The installation file name that will be seen by ViPR Controller users when selecting the OS installation file to use for a service operation.
Image URL	The URL location where the image file was added. If a user name and password are required to access the site, specify them in the URL.

Add a Vblock compute system to ViPR Controller

Review the steps to addVblock compute system (UCS) to the ViPR Controller physical assets.

Before you begin

- For the ViPR Controller user roles required to perform this operation see the *ViPR Controller Virtual Data Center Requirements and Information Guide*, which is available from the ViPR Controller Product Documentation Index .
- To see the planning and configuration details required before the Vblock compute system is added to ViPR Controller, review the *ViPR Controller Virtual Data Center Requirements and Information Guide*, which is available from the ViPR Controller Product Documentation Index .

Procedure

1. Go to the **Physical** > **Vblock Compute Systems** page.
2. Click **Add**.
3. Complete the following fields.

Option	Description
Name	The name to identify the compute system in ViPR Controller.
Type	The type of compute system.
IP Address	IP address of the compute system.
Use SSL	Enable to use SSL.
Port	Leave the default, or enter the port for ViPR Controller to connect with the compute system .
OS Install Network	The OS Install Network is a private VLAN for operating system (OS) installation. The OS Install Network is used by ViPR Controller during provisioning for communication between the hosts and the ViPR Controller compute image server. Since ViPR Controller utilizes a PXE boot process, a DHCP server is used and must be isolated from the customer network. During provisioning, the compute blades communicate with the image server and the operating system

Option	Description
	installation is performed over the OS Install Network. Once the OS installation is complete for a given host, the OS Install Network is no longer used to communicate to that host.
User name	The credentials ViPR Controller will use to access the compute system element manager, for example UCS Manager for UCS. The user must have administrator privileges.
User Password	The password ViPR Controller will use to access the compute system element manager.
Confirm Password	Confirm the password used to access the compute system.
Compute Image Server	Select which compute image server to associate with this compute system when multiple compute image servers have been added to ViPR Controller.

4. Click **Save**.

   The Vblock compute system is added to the Vblock Compute Systems page.

After you finish

Once you have added the Vblock compute system to ViPR Controller, you will need to associate a compute image server with the Vblock compute system, which can only be done using the ViPR Controller REST API, or CLI. For details refer to the ViPR Controller REST API Reference or *ViPR Controller CLI Reference Guide* which can be accessed from ViPR Controller Product Documentation Index .

Deregister UCS blades

After the Vblock compute system is successfully added, and discovered by ViPR Controller, you can deregister available blades that you do not want managed by ViPR Controller.

Before you begin

- You cannot delete blades from ViPR Controller, you can only deregister them.
- Blades that have been provisioned outside of ViPR Controller will not be available for selection. If you want to use those blades, they will have to be released by the compute system and rediscovered. At that point, you can register the blades for provisioning.

Procedure

1. Go to the **Physical** > **Vblock Compute System** page.
2. Locate the compute system for which you will deregister blades.
3. In the row of the compute system, click **Blades** in the **Edit** column.
4. Select the blades to deregister.
5. Click **Deregister**.

Adding and configuring hosts overview

ViPR Controller Tenant Administrators can add, and configure hosts in ViPR Controller.

There are two ways to add hosts to ViPR Controller:

- Discoverable - to allow the ViPR Controller to automatically discover an AIX®, AIX VIO, Linux®, or Windows® host, and host initiators, and Windows clusters, and register them to ViPR Controller.
- Undiscoverable - to manually register the host or host initiators in ViPR Controller. Any host that is not an AIX, AIX VIO, Linux, and Windows is added to ViPR Controller as undiscoverable. Optionally, AIX, AIX VIO, Linux, and Windows can also 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.

Add undiscoverable hosts to ViPR Controller

When a host is added as undiscoverable, ViPR Controller does not discover, or register the host or host initiators. Any host that is not an AIX, AIX VIO, Linux, and Windows is added to ViPR Controller as undiscoverable. Optionally, AIX, AIX VIO, Linux, and Windows can also 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.

Before you begin

Hosts can only be added to ViPR Controller by ViPR Controller Tenant Administrators.

Procedure

1. Select **Physical** > **Hosts**.
2. If working in a multi-tenancy environment, select the tenant.
3. Click **Add**.
4. Select **Other**, or **HPUX** as the operating system type.
5. Enter a name to identify the host in ViPR Controller.
6. Enter the host fully qualified domain name or IP address.
7. Click **Save**.

After you finish

The Host Initiators must be manually registered in ViPR Controller before the host can be used in a provisioning operation. Adding host initiators for the steps to add the host initiators.

Add discoverable hosts to ViPR Controller

When you add a host to ViPR Controller as discoverable, ViPR Controller automatically discovers, and registers the host, and host initiators, and Windows clusters in ViPR Controller.

Before you begin

- Hosts can only be added to ViPR Controller by ViPR Controller Tenant Administrators.

- ViPR Controller supports automatic discovery of AIX, AIX VIO, Linux, and Windows hosts and host initiators.
- ViPR Controller only support automatic discovery of Windows clusters.

Procedure

1. Select **Physical** > **Hosts**.
2. If working in a multi-tenancy environment, select the tenant.
3. Click **Add**.
4. Select the type of operating system.
5. Enter a name to identify the host in ViPR Controller.
6. Enter the host fully qualified domain name or IP address.
7. For Linux, or Windows, select the protocol: **HTTP** or **HTTPs**
8. Leave the default, or enter the port that ViPR Controller will use to communicate with the host.
9. Leave **Discoverable** enabled, to allow ViPR Controller to automatically discover the host initiators, and Windows clusters, or disable the option to manually manage the initiators associated with the host, and not discover the Windows clusters.

   If **Discoverable** is disabled, the host initiators must be manually registered in ViPR Controller.
10. Enter the host login credentials.

    When ViPR Controller storage is attached to a Linux host it needs to run commands to the host. To access the host, ViPR Controller uses the credentials entered here. These are usually the root account credentials. 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 required by the ViPR Controller.
11. Enable **Validation on Save** to enable ViPR Controller to check connectivity to the host before saving the host details.
12. **Save**.

Host initiator and host port configuration

Once the host has been added to ViPR Controller, Tenant Administrators can configure the host initiators, or host ports as required.

- Deregister host initiators to make the host initiators unavailable for use in a ViPR Controller service. Refer to Deregister host initiators.
- Add host initiators to hosts that were manually added to ViPR Controller without automatic discovery. Refer to Add host initiators.
- Register the host initiators that were manually added to ViPR Controller. Refer to Register host initiators.

Deregister host initiators

Deregistering a host initiator leaves the host initiator in the ViPR Controller assets but makes it unavailable to use in any ViPR Controller service operations.

Before you begin

Only host initiators that are currently not in use in a ViPR Controller export can be deregistered.

Procedure

1. Open the **Host Initiators** page.
   a. Select **Physical** > **Hosts**.
   b. Locate the row for the host, and click **Initiators** in the **Edit** column.
2. Check the box in first column of the row with the host initiator to deregister.
3. Click **Deregister**.

Adding host initiators

You must manually add host initiators for hosts that are not automatically discovered by ViPR Controller.

Procedure

1. Open the **Host Initiators** page
   a. Select **Physical** > **Hosts**.
   b. Locate the row for the host, and click the **Initiators** button in the **Edit** column.
2. Click **Add**.
3. If Fibre Channel, enter the host initiator **Node** (World Wide Name) name.
4. Enter the **Port** information:
   - World Wide Port Name (WWPN) for Fibre Channel.
   - iSCSI Qualified Name (IQN) for iSCSI .
5. Click **Add**.

After you finish

After adding the host initiators, you must then register them for use by ViPR Controller service operations.

Registering host initiators

All host initiators manually added to ViPR Controller or that were previously unregistered in ViPR Controller, must be registered to use in a service.

Procedure

1. Open the **Host Initiators** page.
   a. Select **Physical** > **Hosts**.
   b. Locate the row for the host, and click **Initiators** in the **Edit** column.
2. Check the box in first column of the row or rows with the host initiators to register.
3. Click **Register**.

Add a host to a cluster

Optionally, hosts can be added to ViPR Controller clusters. Adding hosts to clusters allows service operations to be performed exclusively on a single host, or shared across all the hosts in a cluster.

- A host can only be used in one cluster.

- Hosts that are not currently in use in a ViPR Controller service, can be moved to different clusters by adding it to the new cluster. The host does not have to be removed from the previous cluster, to move it to a new cluster. ViPR Controller will recognize the last assigned cluster as the cluster to which the host belongs.
- Clusters can only contain the same type of hosts.

Note

Do not manually add Windows or VMware ESX hosts to a cluster in ViPR Controller. During Windows discovery, ViPR Controller detects when a host is in a cluster. If you manually add a discoverable Windows host into a cluster, the next discovery of this host identifies it as not belonging in the cluster and removes it.

For Windows hosts:

- When a Windows host is added to ViPR Controller with discovery enabled, ViPR Controller identifies it if the Windows host is part of a cluster, and adds the cluster to the ViPR Controller physical assets. Once it is added to ViPR Controller, the cluster is managed as a ViPR Controller cluster. Any changes made to the Windows cluster from ViPR Controller are only made in the ViPR Controller environment and are not applied to the Windows configuration.
- ViPR Controller imports the Windows cluster information with the host, but does not discover the other hosts that are in the Windows cluster until the hosts are manually added to the ViPR Controller physical assets.

Procedure

1. Select **Physical** > **Clusters**.
2. If in a multi-tenancy environment, select the **Tenant**.
3. If the cluster is not listed, create it:
   a. Click **Add**.
   b. Provide the name, and click **Save**.
4. Locate the cluster that will be edited in the list of clusters.
5. Click **Edit Hosts** in the right column in the same row as the cluster.
6. Click **Add**.
7. Check the box next to the host to add to the cluster, and click **Add** again.

Auto-Export examples

Review these examples to understand how Auto-Export works with different clusters. The Auto-Export option has been removed from the Add Clusters page. Export group updates are managed in the **Resources** > **Actionable Events** page or with `viprcli event` CLI commands.

Actionable events on page 42 provides additional information.

Windows clusters

Cluster1 has host1 and host2. Export groups are already created since you already provisioned storage against this cluster. In the ViPR Controller UI, you remove H1 from the cluster.

- For Windows clusters, if an actionable event occurs, the export groups are not updated automatically. Instead, you can check the **Resources** > **Actionable Events** page and accept or decline the export group update.

ViPR Controller discovery does not have to run for this scenario.

Cluster2 has host1 and host2. Externally on host1, you decouple host2 from the cluster. ViPR Controller discovery runs.

- An actionable event is generated when the host2 removal is found. You can choose to accept or decline the export update action.

Note

You must address any pending or failed actionable events before you can successfully process orders for the affected hosts or clusters.

Linux clusters

Cluster1 has host1 and host2. Export groups are already created since you have already provisioned storage against this cluster. In the ViPR Controller UI, you remove H1 from the cluster.

- By default, the Auto-Export setting is on, and the export groups are updated.

Cluster2 has host1 and host2. Externally on host1, the HBAs are changed. ViPR Controller discovery runs.

- By default, the host2 removal is found and exports are updated.

For Linux clusters, the Auto-Export setting is on by default. You cannot change this default setting in the user interface. If you want changes, use the `viprcli` commands to manage the export group updates.

ESX clusters

Discovery must always run before ViPR Controller can detect any changes made to ESX clusters. You cannot remove ESX hosts from a cluster in the ViPR Controller UI.

If you move host1 (H1) between cluster1 (C1) and cluster 2 (C2), actionable events will be generated and you can accept or decline the action in the **Resources** > **Actionable Events** page or by using the `viprcli event` commands. See Responding to actionable events on page 44 for examples.

Host network configuration

After a host is added to ViPR Controller, System Administrators can configure the networks, if required, before using the host in a service.

Fibre Channel

If the host was discovered by ViPR Controller, no action is required.

The host initiators, for discoverable hosts, which are configured on a Fibre Channel networks, are automatically discovered and registered in ViPR Controller when the switch is added to the ViPR Controller Fabric Manager.

If the host was added, as undiscoverable by ViPR Controller, or you want to customize the path between the storage and the hosts for ViPR Controller to use when a block storage provisioning operation is perform, you must manually assign the host ports to the SAN networks as described in: Assigning storage ports and host ports in the ViPR Controller SAN networks.

IP

If the host will have IP connectivity to the storage, add the host ports to the IP network.

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, and then add the host, and storage system ports, which will be provisioned together, to the same IP network.

For steps to configure the IP networks see: Configuring IP networks.

iSCSI

If the hosts will have iSCSI connectivity to the storage, the hosts must have their iSCSI ports logged into the correct target array ports before they can be used in the service.

For steps to configure iSCSI networks see: Configuring IP and iSCSI networks on page 79.

Replace host initiators after a storage volume is exported to a host

Once you have used ViPR Controller to export a volume to a host, you can add a host initiator to the export, remove a host initiator from the export, or perform both actions to swap out one host initiator for another in the export group.

Update ViPR Controller after a host initiator is replaced outside of ViPR Controller

After you use ViPR Controller to export a volume to an AIX, ESX, Linux, or Windows host or cluster, which was added to ViPR Controller as discoverable, you can add, remove, or replace a host initiator used by ViPR Controller using an application other than ViPR Controller.

Procedure

1. Outside of ViPR Controller, power off the host or cluster and replace the host initiators.
2. Power the hosts on and rediscover the hosts in ViPR Controller.

   During discovery, four Actionable Events are created for host initiator removal and four for host initiator addition.
3. If replacing four host initiators:

   a. If the path parameters which were set on the virtual pool are not exceeded, go to the **Resources** > **Actionable Events** page and approve the **Add initiators** event first. Then approve the **Remove Initiator** events.

   b. If the parameters which were set on the virtual pool are exceeded, go to the **Resources** > **Actionable Events** page and approve the **Remove Initiator** events first. You must keep at least one initiator associated with the host at all times to prevent data unavailability.

   If replacing the only host initiator:

   a. If the max paths parameter in the virtual pool is greater than 1, the **Add Initiator** event can be approved first and then the **Remove Initiator** event can be approved.

   b. If the max paths parameter equals 1, you must use the ViPR Controller CLI to update the host initiators in ViPR Controller:

      a. Remove the old initiator from it's export groups.

      b. Add the new initiator to the same export groups.
      The initiator is no longer associated with the host export groups, so the initiator can be deleted.

   c. Go to the **Resources** > **Actionable Events** page, and approve the **Remove Initiator** event.

Replace a host initiator of an undiscovered host after a ViPR Controller export operation

If ViPR Controller was used to export a volume to a host, which was added to ViPR Controller as "Other," or if the host was added as undiscoverable, use the following procedures to replace a host initiator with a different host initiator after the export operation:

Procedure

1. In ViPR Controller, add the host port on which the host initiator resides to the same network from which the host initiator is being replaced. This enables ViPR Controller to see the connectivity between the host and the storage after the swap is complete.

   This should be the host initiator that will replace the initiator in the export.

   a. Go to the **Physical** > **Networks** page.

   b. Locate the network to which you are adding the host port.

   c. Click the network name.

   d. Click **Add** > **Add Ports** at the bottom of the Fibre Channel Ports table.

   e. Add the host port on which the host initiator you are adding resides.

2. Add the host initiator to the host in ViPR Controller
3. Register the host initiator in ViPR Controller.
4. Remove the host initiator, which will be replaced by the host initiator added in the previous steps, from ViPR Controller.

   a. Locate the row for the host on which the host initiator is being removed.

   b. Click **Remove** to remove the initiator in the export group initiators column list.

   c. Locate the row for the export group on which the host initiator is being removed.

   d. Click **Initiator** in the **Edit** column of the host row.

   e. Select the row for the host initiator being removed, and click **Deregister**.

   f. Click **Delete** to delete the host initiator from ViPR Controller.

   ViPR Controller automatically updates the host initiators in the export group after detecting the add and remove operations.

Add and configure vCenters in ViPR Controller

Use the **Physical** > **vCenters** > **Add vCenters** page to add a vCenter to ViPR Controller.

Before you begin

ViPR Controller allows a vCenter to be added twice if the IP address is used once, and then the hostname is used to add it again.

For the ViPR Controller user roles required to perform this operation see the *ViPR Controller Virtual Data Center Requirements and Information Guide*, which is available from the ViPR Controller Product Documentation Index .

Procedure

1. Select **Physical** > **vCenters**.
2. Click **Add**.
3. Enter a **Name** for the vCenter Server.
4. Enter the vCenter **Host** Fully Qualified Domain Name (FQDN) or IP address.
5. Enter the **Port** used for communication between the ViPR Controller and the vCenter Server.
6. Enter the vCenter administrator credentials (**Username** and **Password**)..

   Note

   vCenter user entered here must have administrator privileges.

7. Optionally, a System Administrator can select the **Tenant Access** to control which tenants will have access to the vCenter.
   - Enable **Cascade Tenancy** to assign the vCenter, and all its current resources, (datacenters, clusters, and hosts), and any resources added to the vCenter after Cascade Tenancy is enabled on the vCenter, to the same tenant. If you choose to cascade tenancy, then you can only assign the vCenter to one tenant.
   - Disable **Cascade Tenancy**, to assign the vCenter to be shared across different tenants. If you did not enable Cascade Tenancy select the tenants with which the vCenter will be shared.
8. Check the status of the **Validate Connection on Save** checkbox.

   If you leave this box checked, ViPR Controller will check that it can connect to the host before saving the host details. If validation fails you will not be allowed to save the host details.

   If some of the information, such as the user credentials, are incorrect, but you still want to save the information you have entered, uncheck the box. The host will fail discovery, however, you can edit the host details later and, once corrected, it will be successfully discovered.
9. Click **Save**.

After you finish

- If a vCenter is not assigned to any tenant, then you cannot assign its resources (Datacenter, Hosts, or Clusters) to any tenants.
- If you assigned the vCenter to multiple tenants, in step 7, you will need to assign its datacenters to one of the tenants that shares the vCenter. Assigning the tenant to the Datacenter will intern assign its Clusters and Hosts to the same tenant. The Hosts and Clusters in a Datacenter will not be visible in the ViPR Controller UI until the unassigned Datacenter is assigned to a tenant.To assign a Datacenter to a tenant:
  1. Go to the **Physical** > **vCenters** page.

     Note

     Both Datacenters and vCenters are filtered based on the Tenant Selector. To view all the Datacenters of the vCenter, select [No-Filter] from the Tenant Selector.

2. Expand the vCenter to list its datacenters.
3. Click the datacenter to assign to a tenant.
4. Select the tenant in the popup dialog box.

   Note

   The popup dialog box lists only the tenants that share the vCenter. If the vCenter is not assigned to any tenant, this popup dialog box will not have any options.

5. Repeat steps 1 - 4 for each datacenter in the vCenter.

- If you disable Cascade Tenancy, after the tenants were previously set as part of the cascade setting, the vCenters, and its resources will remain in the same tenant, until they are manually reassigned to a different tenant.
- If you did not choose Cascade Tenancy and you add more datacenters to a vCenter after the vCenter that has been assigned to a ViPR Controller Tenant, you will need to rediscover the vCenter in ViPR Controller, and assign the datacenter to a tenant in the ViPR Controller. The datacenter will not automatically be assigned to the tenant defined in the original tenant to which vCenter was assigned.
- You can remove a tenant from a vCenter, even if the vCenter contains datacenters, clusters, and hosts, still assigned to the same tenant, when no storage volumes were provisioned byViPR Controller from that tenant to any of the clusters and hosts in the datacenter. You cannot however remove a tenant from a vCenter if the vCenter contains datacenters, clusters, and hosts assigned to the same tenant when storage volumes have been provisioned by ViPR Controller from the same tenant to any of the hosts and clusters in the datacenter.

ESX/ESXi initiator and port configuration

After vCenter is added to ViPR Controller, configure the ESX/ESXi host initiators or the ports.

- Deregister host initiators to make the host initiators unavailable for use in a ViPR Controller service. See Deregister host initiators.
- For IP connected hosts, see Add the ESX/ESXi ports to the IP Network.

Deregister host initiators

Deregistering a host initiator leaves the host initiator in the ViPR Controller assets but makes it unavailable to use in any ViPR Controller service operations.

Before you begin

Only host initiators that are currently not in use in a ViPR Controller export can be deregistered.

Procedure

1. Open the **Host Initiators** page.
   a. Select **Physical** > **Hosts**.
   b. Locate the row for the host, and click **Initiators** in the **Edit** column.
2. Check the box in first column of the row with the host initiator to deregister.
3. Click **Deregister**.

Add ESX/ESXi ports to an IP network

If adding ESX/ESXi hosts to provision over an IP network, you must add ports to the IP network.

Before you begin

- IP Networks are created by System Administrators. Tenant Administrators cannot configure IP networks or add host ports to the network.
- Add all ESX/ESXi server IP interface addresses (Management IP, vMotion IPs, and any other IP VMNIC visible in vCenter) per cluster when creating a network for a virtual array to use for file system exports to an ESX/ESXi cluster.

Procedure

1. Select the **Physical** > **Networks** page.
2. If the network is already created, click the name from the list of networks.

   If the network is not created, create it by doing the following:

   a. Click **Add IP Network**.

   b. Enter the network **Name**.

   c. Select the storage systems to include in the network.
3. Under the IP Ports table, click the **Add** to manually add the host ports, or click the **Add arrow**, and select **Add Host Ports** to select from discovered ports.
4. Enter or select the host ports to use in the IP network.
5. Click **Save**.

View ESX/ESXi clusters

You can view ESX/ESXi clusters on the **Physical** > **Clusters** page in ViPR Controller.

Before you begin

ESX/ESXi clusters are automatically discovered with vCenter. You cannot remove hosts from ESX/ESXi clusters in ViPR Controller.

Procedure

1. Select **Physical** > **Clusters**.
2. If in a multi-tenancy environment, select the **Tenant**.
3. Locate the cluster to be edited in the list of clusters.
4. Click **Edit Hosts** in the right column in the same row as the cluster to view the list of ESX/ESXi hosts in the cluster.

Updating a vCenter or datacenter reference when moving clusters

When moving an entire cluster from one vCenter or datacenter to another vCenter or datacenter, you must use ViPR Controller API or CLI commands to update the cluster's vCenter or DataCenter reference.

Prior to release 3.5, ViPR Controller would delete manually created clusters that were discovered in vCenter and automatically unexport the volumes. Beginning with release 3.5, you can check **Resources** > **Actionable Events** and decline the unexport action. You can then use ViPR Controller API or CLI commands to manually bring the created cluster under control of the vCenter.

Use the API or CLI commands to update the ViPR Controller database for these situations:

- Cluster moves from one vCenter or datacenter to another.
- Manually created clusters and hosts are merged into a vCenter cluster.

Note

If a volume is removed from inventory, you can delete the Export Group from inventory using the **Resources** > **Export Groups** > **Delete** .

For examples and additional information about Actionable Events and `viprcli cluster update` commands used to update vCenter or datacenter references, see Responding to actionable events on page 44.

ViPR Controller network configuration for vCenter

After a host is added to ViPR Controller, System Administrators can configure the networks, if required, before using the host in a service.

Fibre Channel
No action is required when a vCenter is added on a Fibre Channel network.

The host initiators for ESX/ESXi hosts on Fibre Channel networks are automatically discovered and registered in ViPR Controller when vCenter is added to ViPR Controller. At the time the switch is added to the ViPR Controller physical assets, ViPR Controller also discovers the storage systems on the same network. During provisioning ViPR Controller automatically selects the storage and host ports that will be used to connect the hosts and storage.

IP
Add the ESX/ESXi ports to an IP network.

ViPR 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, and then add the host, and storage system ports, which will be provisioned together, to the same IP network.

If creating a network for a virtual array that will be used for file system exports to an ESXi cluster, add all ESXi server IP interface addresses (Management IP, vMotion IPs, and any other IP VMNIC visible in vCenter) per cluster.

For steps to configure the IP networks, see Configuring IP and iSCSI networks on page 79.

iSCSI
Hosts that use ViPR Controller services with the iSCSI protocol must have their iSCSI ports logged into the correct target array ports before they can be used in the service.

For steps to configure iSCSI networks, see Configuring IP and iSCSI networks on page 79.

Actionable events

If changes occur during vCenter or Host discovery, ViPR Controller may need to update export groups in order to maintain the correct state among hosts, clusters, and their export groups. Instead of performing these updates automatically, a list of

actionable events is generated. Only the Tenant Administrator can approve or decline the event.

In many cases changes in vCenter discovery are temporary and are due to maintenance activities. Usually, the environment returns to the previous state after maintenance. ViPR Controller no longer performs updates automatically when it detects post-discovery changes. Instead, the tenant administrator is given a chance to approve or decline the update based upon knowledge of the data center activities.

Use the **Resources** > **Actionable Events** page to review the list of Pending, Approved, Failed, or Declined actionable events. (There is also a loud speaker icon at the top of the screen showing the number of events that need to be reviewed. Click the icon to open the actionable events page.) In addition to viewing actionable events, you can click the event and delete associated tasks.

Note

The Auto-Export option has been removed from the **Physical** > **Clusters** > **Add Cluster** page. Default behavior for automatic exports varies depending upon the type of host or cluster:

- For vCenter, Windows, Linux, AIX, or HP-UX-discovered hosts, you must use the **Resources** > **Actionable Events** page to manage export group updates. Automatic export is turned off.
- Automatic export is on by default for manual or user-created clusters when moving hosts between clusters in the UI.
- Automatic export is off by default when using the CLI commands.
- There is no automatic export for NFS exports. Actionable events are created only if the host is in a shared block export group and is being removed/added to a cluster. An actionable event is created if the host moved to a different datacenter or if it was added/removed from vCenter.
- If a host is removed from vCenter (not discoverable at all through vCenter), then an actionable event is created even if it doesn't have any block exports. Approving the event will unassign the host from vCenter but not perform any block export updates.

ViPR Controller UI	ViPR Controller CLI command	Description

Resources > **Actionable Events**	`viprcli event {list,show,delete,approve,decline,details} ...`
	
	with the following options:
	
	`[-h][-hostname <hostname>][-portui <ui_port_number>] [-cf <cookiefile>]`
		If changes occur during vCenter or Host discovery, ViPR Controller may need to update export group in order to maintain the correct state among hosts, clusters, and their export groups. Actionable events on page

ViPR Controller UI	ViPR Controller CLI command	Description
		42 provides more information.

Improved maintenance of export group inventory

In a continuing effort to provide more self-healing capabilities natively within ViPR Controller, stale export group inventory data is updated so that volumes, initiators, hosts, or cluster fields in the database are reset to "null."

Prior to the 3.6 version of ViPR Controller, users were allowed to create or leave behind empty export groups or export groups with compute resources and initiators tied to them. This is still allowed up to the point of removing Host(s) or initiators. After that, however, the ViPR Controller database is updated with current export group information.

Stale data could result from

- failure to follow through on an API execution path
- removal of devices without removing the export group itself
- prior failures, including failures of rollback

Responding to actionable events

Here is a list of actions that can generate events during the ViPR Controller discovery process. Some actions create events, and some do not. Some actions prevent data from moving between vCenters.

Actionable events triggered during host discovery

Note

For all of these actions, the exclusive exports remain unchanged.

Action	Approve event	Decline event
Host moves between clusters in same vCenter (Review the examples in this topic for moving clusters across vCenters.)	Approving the actionable events unexports old cluster datastores and adds new cluster datatores to this host.	Do not decline actionable events because host will still have old stores that don't belong in new cluster.
Host returns subset of initiators or new initiators	Approving will update exclusive exports and will update shared exports with old/new initiator path.	Do not decline the actionable event if initiators are really changed on the host. Declining will not change the export path.
Unable to discover a host	Approving will unexport shared exports and unassign host from vCenter. You can also use the Service Catalog to	Decline this actionable event if the host exists but was not discovered. Investigate the problem and rediscover.

Action	Approve event	Decline event
	unexport and decommission if needed.	
vCenter A is dead. All content is seen in vCenter B.	Do not approve the actionable event.	Decline the actionable event. Use the `viprcli cluster update` commands to update cluster from A to B. That causes the ViPR Controller database to synchronize with the new vCenter. Exports will not be affected.
Actionable events are marked as failed if they have failed tasks.	Do not approve the actionable event.	Decline the actionable event. Click **>** icon and look at the Event Tasks and Event ID. Click the Update Host task or the Event ID URL to learn more about errors associated with the failed task. Correct the problem and then Approve or Decline the actionable event again.

Actionable events that are not triggered during host discovery

Changes resulting from discovery	Impact	Remediation
Host returns 0 initiators	Host discovery failed. No actionable event.	vCenter reported incorrect data. Fix issues in vCenter and rediscover.
Unable to rediscover all hosts in a cluster	Host discovery failed. No actionable event	vCenter reported incorrect data. Fix issues in vCenter and rediscover.
Rename host	No actionable event.	No action required.
Rename cluster	No actionable event	No action required.
Rename datacenter	No actionable event	No action required. After rediscovery, the ViPR Controller database is updated to reflect the new datacenter name.
Rename vCenter	No actionable event	No action required.
User creates host with type, "other" in ViPR Controller and adds it to a cluster.	No actionable event. **Note** Auto-export updates occur when moving hosts between clusters in the UI.	Use `viprcli` command if you do NOT want auto-export to occur. (When using CLI commands, the default is to NOT perform auto-export updates.)
Changes in vCenter credentials prevent ViPR Controller from discovering all hosts and clusters. When you log into the vCenter using the ViPR Controller credentials, the number of hosts or clusters that are listed is reduced.	Host discovery failed. No actionable event.	Update the permissions on the vCenter to allow ViPR Controller to access all hosts and clusters. Host discovery fails because ViPR Controller can't rediscover the hosts.

Changes resulting from discovery	Impact	Remediation
(User sees a limited set of clusters and hosts on a vCenter where everything was previously discovered. There are no actionable events. No clusters or exports change.)		

Service catalog behavior associated with pending events

The "horn" icon in the UI banner displays the number of pending and failed events. This number is refreshed every 10 seconds. You must Approve or Decline these events before you can successfully process orders for the affected hosts or clusters. If the event fails, you must correct the underlying problem and Approve or Decline the event before submitting new orders.

Click the **>** button to open the details panel for the actionable event. The "If Approved" and "If Declined" text explains what will happen if you choose "Approve" or "Decline." If a link is available in the Event Tasks row, click it to get more information or to confirm your action. When you Approve or Decline an event, you must type **`confirm`** in the dialog in order for the action to take place. If the action fails, there will not be a link associated with Event Task. Use the Event ID URL to obtain more information or to report the problem for troubleshooting.

Examples of vCenter changes that require ViPR Controller

When using CLI to manage cluster or host changes, use the `viprcli cluster update` and `viprcli host update`commands. Examples are provided in this section.

```
./viprcli cluster update
usage: viprcli cluster update [-h] [-hostname <hostname>]
                              [-port <port_number>] [-portui
<ui_port_number>]
                              [-cf <cookiefile>] -name <name>
                              [-tenant <tenantname>]
                              [-datacenter <datacentername>]
                              [-newdatacenter <newdatacentername>]
                              [-label <label>] [-vcenter
<vcentername>]
                              [-newvcenter <newvcentername>]
                              [-autoExportsEnabled {true,false}]
                              [-updateExports {true,false}]
```

```
./viprcli host update
usage: viprcli host update [-h] [-hostname <hostname>] [-port
<port_number>]
                           [-portui <ui_port_number>] [-cf
<cookiefile>]
                           [-nhn <newviprhostname>]
                           [-nt
{Windows,HPUX,Linux,Esx,Other,AIXVIO,AIX,No_OS,SUNVCS}]
                           -hl <hostlabel> [-nl <newlabel>]
                           [-nhp <newhostport>] [-nun
<newhostusername>]
                           [-tn <tenant>] [-hostssl {true,false}]
```

```
                                [-ov <osversion>] [-nc <cluster>]
                                [-ndc <newdatacenter>] [-vc
<vcentername>]
                                [-autodiscovery {true,false}]
                                [-bootvolume <bootvolume>] [-project
<project>]
                                [-updateExports {true,false}]
```

Example 1 Moving a vCenter cluster from vCenter1 to vCenter2

When you have two different discovered instances within ViPR Controller and the cluster needs to be moved from one vCenter instance to the other vCenter instance, use these steps:

1. Update vCenter 5.x in ViPR with incorrect credentials. This prevents discovery during the migration.
2. In vCenter 5.x, remove hosts and add them to vCenter 6.x. Make sure the same structure is used in vCenter 6.x that was in 5.x (same host labels, cluster names, datacenter names, HBAs).
3. Update vCenter in ViPR with credentials and hostname to point to vCenter 6.x. (This triggers discovery of vCenter 6.x and the same structure will be kept.)
4. DECLINE the events that are generated and use viprcli commands to rename the Datacenter to the new vCenter. SkipExports = try. No export changes are made. For example, `viprcli cluster update -name "Cluster1" -datacenter dc -vcenter old_vc -newdatacenter dc -newvcenter new_vc` (Only the vCenter changes. Note that `-updateExports` is false if the field is not mentioned in the CLI command.)

   Note

   Ensure you do not approve any events generated by these actions.

5. Update vCenter 5.x in ViPR Controller with the correct credentials.

Example 2 Migration of vCenter from 5.5 to 6.0

When migrating the vCenter from 5.5 to 6.0 where only one vCenter is discovered in ViPR Controller at any point in time, use these steps:

1. Update vCenter 5.x in ViPR with incorrect credentials. This prevents discovery during the migration.
2. In vCenter 5.x, remove hosts and add them to vCenter 6.x. Make sure the same structure is used in vCenter 6.x that was in 5.x (same host labels, cluster names, datacenter names, HBAs).
3. Update vCenter in ViPR with credentials and hostname to point to vCenter 6.x. (This triggers discovery of vCenter 6.x and the same structure will be kept.)
4. Update vCenter 5.x in ViPR Controller with the correct credentials.

Note

In this use case, there are no actionble events.

Example 3 Ensuring data availability when discovering manually created hosts and clusters from vCenter

If you created hosts and clusters manually in ViPR Controller and now want to automatically discover them from vCenter, follow this procedure. The cluster and hosts will be re-assigned to the vCenter. For example:

1. In ViPR Controller, manually create cluster C1 and manually add hosts H1 and H2 to this cluster.
2. Export volumes to cluster C1.
3. Add the vCenter into ViPR Controller. This triggers discovery and actionable events are generated. (Actionable events are created as a result of trying to bring manual hosts H1 and H2 under vCenter control.)
4. Use the CLI or API to update the manual cluster C1's datacenter reference to the one created by vCenter discovery. For example, `viprcli cluster update -name C1 -vc "" -nvc newVC -ndc NDC`
5. On rediscovery, Cluster C1 and hosts H1 and H2 are now under vCenter's discovery. No actionable event occurs. Hosts H1 and H2 are now assigned type, ESX, in the UI.

Example 4 Move one host into, out of, or between clusters, but do not modify exports

Use the ViPR Controller user interface to make the changes in vCenter. Then rediscover in ViPR Controller. Decline any actionable events that are generated.

Use viprcli commands. For example:

```
viprcli host update -hl foobar.xyz.com -vc vcenterXX -newcluster
NEW_Cluster -newdatacenter NEW_DC
```

Note

`-updateExports false` is the default behavior. This ensures that exports are not modified.

Example 5 Move one host into, out of, or between clusters and modify exports

Use either the ViPR Controller user interface to make the changes in vCenter or viprcli commands. Then rediscover in ViPR Controller. If using the UI, accept the actionable events. If using the CLI, decline any actionable events that are generated and issue this command.

For example:

```
viprcli host update -hl foobar.xyz.com -vc vcenterXX -newcluster
NEW_Cluster -newdatacenter NEW_DC -updateExports true
```

Note

`-updateExports true` ensures that exports are modified.

Example 5 Move one host into, out of, or between clusters and modify exports (continued)

Tips and limitations associated with actionable events

Here is a list of tips and limitations to be aware of when managing actionable events.

- Events are restricted to actions against vCenter and Host discovery. For example, Host cluster change, Host initiator change, Host removed from vCenter, Host added to vCenter.
- Ensure there are no pending or failed actionable events. If these exist, then new orders for hosts and clusters will fail to execute. You can view messages associated with an actionable event by clicking **>** on the **Resources** > **Actionable Events** page.
- When you need to perform an inventory delete action and the order fails with a validation error, follow these steps to correct the problem:
  1. Perform a rediscovery. (This creates an actionable event with status of Pending on the **Resources** > **Events** page. Both the inventory delete and the new order fail due to the event status being set to Pending.)
  2. Decline the actionable event. (This removes the Pending or Failed states.)
  3. Delete the export group manually using the viprcli remove tag if the inventory delete action failed due to problems with a mounted volume.
- If a datastore has been removed in vCenter and ViPR Controller does not know about it, you can use CLI or API commands to remove the datastore tag from the volume. Then you can unexport or delete the volume if needed. For example, `./viprcli volume tag -remove "vipr:vmfsDatastore-urn:storageos:Cluster:0345d31c-1e2f-4af6-9def-ebb5301f7c1c:vdc1=ww610" -name ww600 -pr VM1`
- When initiators are added, they are assigned to the Host during discovery. Actionable events are then created to update exports with the new initiator. Host discovery fails if a Host is stealing an initiator from another Host. But if a new initiator is found, it is assigned to the Host during discovery.
  Here is an example of the Add Initiator action and an actionable event:
  1. An initiator is added to a Host.
  2. Discovery assigns the initiator to the Host and creates an event.
  3. When the event is approved, the export groups are updated.

  Note

  During the Add Initiator action, the Host is first updated with the new initiator. The export group is modified when the event is approved.

  Here is an example of the Remove Initiator action and an actionable event:
  1. An initiator is removed from a Host.
  2. Discovery creates an event for the removed initiator.
  3. When the event is approved, the initiator is removed from export groups and deleted.

Note

During the Remove Initiator action, the export group is modified when event is approved. Then the initiator is removed from the Host.

- When removing the last initiator from a Host, the Host reference will no longer exist in any export group. Adding an initiator to this Host will require manual creation or updating of export groups.
- After 30 days, the approved and declined events are deleted from the database. Pending and failed events are not deleted because you need to take action on them.
- Linux/HP-UX/AIX clusters are manually created in ViPR Controller. You must add/remove hosts to these clusters as needed. Automatic exports are triggered for these manual cluster operations in the UI. If you use CLI commands, automatic exports are disabled by default.
- The Windows cluster rename action and add/remove cluster members action cause the same types of events as VMware handling. (Cluster rename will NOT create an event, similar to Vmware cluster rename that does not create events.) HBA swaps with initiator add/remove cause actionable events.
- Only a Tenant Administrator may approve actionable events.
- If you want to assign a datacenter to another tenant, you can navigate to the UI page and select "No Filter" or "Not Assigned" from the drop-down. From there you can view vCenters and click on the Datacenters. This action pops up a new window where you can assign the datacenter to another tenant.

Note

Moving an ESX Host into another vCenter or datacenter that belongs to another tenant is not supported. You should only move Hosts between vCenters and datacenters that are owned by the same tenant as the Host.

- These viprcli commands may be used to manage actionable events:
  - `viprcli event list`
  - `viprcli event details`
  - `viprcli event show`
  - `viprcli event approve`
  - `viprcli event delete`

Setting discovery properties

You can change the properties for auto-discovery of storage systems, switches, and SMI-S providers.

Before you begin

For the ViPR Controller user roles required to perform this operation see the *ViPR Controller Virtual Data Center Requirements and Information Guide*, which is available from the ViPR Controller Product Documentation Index .

Changes that you make to any of these values will initiate a reboot when you click Save.

Procedure

1. Select **Settings** > **General Configuration** > **Discovery**.
2. Enter values for the properties.

Option	Description
Enable auto-Discovery	Indicates whether auto-discovery is enabled. It is not recommended to change this value unless advised by your EMC customer service representative. Reboot required. Default is true.
Storage Systems	Number of seconds between discovery operations of storage systems. Reboot required. Default is 3600. **Note** Whenever there are manual edits made to the `Storage Systems` and `Scan Interval` properties, set the `Storage Systems Refresh Interval` and `Scan Refresh Interval` to 50% of the settings in `Storage Systems` and `Scan interval` fields.
Network Systems	Number of seconds between discovery operations of switches (fabric managers). Reboot required. Default is 3600.
Hosts and VMware vCenters	Number of seconds between discovery operations of Hosts and VMware vCenters (hosts/vcenters). Default is 86400.
Vblock Compute Systems	Number of seconds between discovery operations of Vblock Compute Systems. Reboot required. Default is 3600.
Enable Auto-Scan	Indicates whether auto-scan of storage providers is enabled. Reboot required. Default is true.
Scan Interval	Number of seconds between scan operations of storage providers. Reboot required. By default the Scan Interval time is set to 600 seconds (10 minutes). However, it is recommended that you increase the scan time when you are running multiple storage providers as follows: • If there are 10 or more storage providers, set the Scan Interval to 1800 seconds (30 minutes). • If there are 20 or more storage providers, set the Scan Interval to 3600 seconds (60 minutes).

Option	Description
	Note Whenever there are manual edits made to `Storage Systems` and `Scan Interval` properties, set the `Storage Systems Refresh Interval` and `Scan Refresh Interval` to 50% of the settings in `Storage Systems` and `Scan interval` fields.
Enable Array Affinity Discovery	Default is false. Set to true to enable ViPR Controller for scheduled host/array affinity discovery. When set to false, host/array affinity discovery must be performed on demand. Host/array affinity discovery is used by ViPR Controller to identify the storage provisioned to a given host. Host/array affinity can be discovered on demand from the **Physical** > **Hosts** page.
Array Affinity Discovery	When array affinity discovery is enabled, this is the number of seconds between the time that ViPR Controller will rediscover for host/array affinity. Default is 3600.
CIM Connection TTL	Maximum number of seconds before an inactive SMI-S is reaped. Should be less than the Discovery Scan interval. If set to 0, reaping is disabled. Reboot required. Default is 480.
Discovery Threads	Number of threads each node uses for discovery of storage system. Set this value to 1 on configurations with less than 12 GB RAM. Reboot required. Default is 3.
Storage Systems Refresh Interval	Number of seconds allowed before a new discovery of the storage systems can run since the last discovery operation. Reboot required. Default is 600. **Note** Whenever there are manual edits made to `Storage Systems` and `Scan Interval` properties, set the `Storage Systems Refresh Interval` and `Scan Refresh Interval` to 50% of the settings in `Storage Systems` and `Scan interval` fields.
Network Systems Refresh Interval	Number of seconds allowed before a new discovery of the switches (fabric managers) can run since the last discovery operation. Reboot required. Default is 60.
Hosts and VMware	Number of seconds before a new discovery of Hosts and VMware vCenters (host/vcenters) is allowed since the last discovery operation. Reboot required.

Option	Description
vCenters Refresh Interval	Default is 60.
Vblock Compute Systems Refresh Interval	Number of seconds allowed before a new discovery of Vblock Compute Systems can run since the last discovery operation. Reboot Required. Default is 60.
Scan Refresh Interval	Number of seconds allowed before a new storage provider scan operation can run since the last scan of the SMI-S provider was performed. Reboot required. Default is 60. **Note** Whenever there are manual edits made to `Storage Systems` and `Scan Interval` properties, set the `Storage Systems Refresh Interval` and `Scan Refresh Interval` to 50% of the settings in `Storage Systems` and `Scan interval` fields.
Array Affinity Refresh Interval	This is the number of seconds before a new array affinity discovery operation is allowed since the last time the host to storage relationship was discovered. Default is 600.

3. **Save**.

vNAS server discovery and management

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

Prior to performing operations to discover and manage vNAS servers, be sure to review the information in the *ViPR Controller Virtual Data Center Requirements and Information Guide* which is available from the ViPR Controller Product Documentation Index .

Discovering vNAS servers

When you add a VNX for File, or Isilon storage system ViPR Controller discovers and registers its vNAS servers and attributes, such as logical interfaces and base directory.

Before you begin

Procedure

1. Go to **Physical** > **Storage Systems**.
2. Click **Add**.

   The **Add Storage System** page appears.
3. Select EMC VNX File, or EMC Isilon for the type of storage system.

4. Type the name of the storage system.
5. Type the IP address of the Control Station that manages the vNAS servers to discover.
6. Leave the default port or type the port to access the Control Station.
7. Type the user credential to access the Control Station.
8. Enter the Onboard Storage Provider information:
   a. Type the Onboard Storage Provider host.
   b. Enable or disable SSL access to the Onboard Storage Provider.
   c. Leave the default port or type the port to access the Onboard Storage Provider.
   d. Type the user credentials to access the Onboard Storage Provider.
9. Click **Save**.

Set the Controller Configuration to allow a vNAS to be shared with multiple projects

If you want to associate a vNAS server with multiple projects, you must set the Controller Configuration to allow a vNAS to be shared with multiple projects.

Procedure

1. Go to **Physical** > **Controller Config**.
2. Click **NAS**.
3. From the drop-down list, select **Enable Associate of Virtual NAS to Multiple Projects**.
4. Click **Save**.

Associating vNAS servers to a project

You can associate vNAS servers to one or more projects.

Before you begin

Procedure

1. Go to **Physical** > **Storage System** page, select the storage system, and click **vNAS**.

   A list of vNAS servers appears.
2. Select the vNAS server.
3. Click **Associate Project** and select a tenant (if applicable) and one or more projects.
4. Click **Save**.

Viewing vNAS servers

You can view the vNAS servers by project.

Procedure

1. Go to **Resources** > **vNAS Servers**.
2. Select the project.

Each vNAS server appears with its registered check mark, name, protocol, parent NAS server, domain, and state.

Enabling performance metrics for dynamic loads

You must enable performance metrics to place file systems with dynamic loads on qualified vNAS servers. After enabled, ViPR Controller collects performance metrics, such as input and output IOPS of the network interfaces of vNAS servers. The performance statistics of a vNAS server is then calculated as the aggregate performance of its network interfaces.

Procedure

1. Go to **Physical** > **Controller Config**.
2. Click **NAS**.

   The first two entries show the default values, which are greyed out.
3. From the drop-down list, select Dynamic Performance Placement Enabled.
4. Click **Add**.
5. If enabling performance metrics for the first time, set the global default value to true.
6. Set the system value to true.
7. Click **Save**.

After you finish

To view the performance statistics of a vNAS server, click the **vNAS** button next to a VNX for File, or EMC Isilon array on the **Physical** > **Storage Systems** page.

Customizing resource names created on physical systems

As you add physical assets, ViPR Controller automatically creates a number of resources on the physical system, such as masking views and zones, using a single global hard-coded naming convention for each type of resource. You can override these default names and provide your own naming convention for several types of resources.

If you define your own naming convention for a resource, ViPR Controller uses your convention. Otherwise, the default naming convention is used to name the resource. Your custom naming convention applies to all new instances of that resource. It does not rename existing instances.

Note

ViPR Controller does not enforce uniqueness for custom names. To avoid any naming conflicts, make sure your naming conventions are unique.

You can configure custom naming conventions globally or per system type scope.

The name that is generated from your custom naming convention must adhere to the following restrictions imposed by the storage or network system to which it applies:

- The name can not exceed the maximum length for the resource.
- The name must only include characters that are part of the valid characters set for the resource.

Note

For a clone set with the BCV attribute, ViPR Controller does not support VMAX Masking for Host Masking View Name, Cluster Masking View Name, Host Storage Group Name, Cluster Storage Group Name, Host Port Group Name and Cluster Port Group Name.

You can modify the default names of these ViPR Controller resources.

- San Zoning
  - Zoning - scope can be set globally or by system type
- VMAX Masking
  - Host Masking View Name
  - Cluster Masking View Name
  - Host Storage Group Name
  - Cluster Storage Group Name
  - Host Cascaded IG Name
  - Cluster Cascaded IG Name
  - Host Cascaded SG Name
  - Cluster Cascaded SG Name
  - Host Initiator Group Name
  - Cluster Initiator Group Name
  - Host Port Group Name
  - Cluster Port Group Name
- VNX Storage Groups
  - Host Storage Group Name
- VPLEX
  - Storage View Name
- XtremIO
  - Volume Folder Name
  - Initiator Group Name
  - Host Initiator Group Folder Name
  - Cluster Initiator Group Folder Name
- HDS
  - Host Storage Domain Name
  - Host Storage Domain Nick Name
- Isilon
  - File System Directory Path
  - System Access Zone Directory
  - Unmanaged File System Locations
- Volume Naming
  - Custom Volume Naming Enabled

- Volume Custom Name
- Export Volume Custom Name

Naming policy syntax

When you create a custom naming convention for a resource, it must follow a specific syntax.

For each of the resources for which you can provide a custom naming convention, there are a set of variables and functions that you can use to create the name. The functions are the same for all of the resources, but the variables will differ by resource.

A custom naming convention can include the following:

- Literal strings.
- Special characters, such as underscores (_), that are part of the valid character set for the resource. When using a dot (.) you must preface it with a backslash (\), such as emc\.com.
- Variable name surrounded by curly brackets.
- Function,
  - Applied to an individual variable string to select certain parts of the string value for the name, using the syntax *<variable_name>.<function_name>*(*<function values>*)
  - Applied to the entire custom naming mask, using the syntax, (*<entire_name_mask>*).*<function_name>*(*<function_values>*)

Refer to the documentation for the physical system for the list of valid characters for the literal strings and special characters for each resource.

In this example, *host_name* and *array_serial_number* are variables , and FIRST and LAST are functions that are applied to those variables to select the part of the string that is to become part of the custom name. The name of the resource will be comprised of the first 12 characters of the host name, followed by an underscore (_) and the last 3 characters of the array serial number, followed by _CSG.

```
{host_name.FIRST(12)}_{array_serial_number.LAST(3)}_CSG
```

Note

Any function being applied to a variable is within the curly brackets for that variable.

If any variables contain invalid characters for the resource name, by default ViPR Controller removes those invalid characters. For example, if the zone name variable, {host_name}, contains ".", ViPR Controller removes them after all the string functions are applied.

Available functions

For each of the resources for which you can provide a custom naming convention, there are a set of variables and functions that you can use to create the naming policy.

The functions are the same for all of the resources, but the variables will differ by resource.

The functions that are available are described in the table. The general format for using a function is:
`{<variable_name>.<function_name>(<function_values>)}`

Note

These examples refer to the variable *host_name* which corresponds to the **Host** field when you added the host to ViPR Controller. The *host_name* variable is the host FQDN or IP address. There is also a *host_assigned_name* variable that you can use in some of your custom names that corresponds to the **Name** field when you added the host. The *host_assigned_name* variable is just a label that you can assign to the host.

Function	Description
FIRST	Use the first n characters of the string value of a variable. For example, `{host_name.FIRST(60)}`
LAST	Use the last n characters of the string value of a variable. For example, `{array_serial_number.LAST(3)}`
REPLACE	Replace a character with another character. In this example, all of the dashes in the string value of the variable, *hba_port_wwn*, are replaced with a null string, essentially deleting all of the dashes. `{hba_port_wwn.REPLACE("-","")}`
SUBSTRING	Use part of a string. You specify the beginning and ending character of the string that defines the substring. In this example, only the characters 3-9 are selected from the *host_name* variable to be part of the custom name. `{host_name.SUBSTRING(3,9)}`
TOLOWER	Change all characters in the specified string to lower case. `{host_name.TOLOWER()}`
TOUPPER	Change all characters in the specified string to upper case. `{host_name.TOUPPER()}`

Function	Description

TRIM	Remove leading and trailing characters from a string. The TRIM function can be used on the final generated name or on the individual variable strings.
	To apply the function to the entire generated name, the syntax is as shown. Note that the entire custom name mask is contained within parentheses.
	`({cluster_name.FIRST(19)}_{host_name.FIRST(2)}).TRIM("_")`
	To apply the function to an individual variable, the syntax is as shown.
	`({cluster_name.FIRST(19)}).TRIM(";")`

You can also concantenate functions on an individual variable, with the functions being evaluated from left to right. In this example, the name would use the first 15 characters of the value of the variable *host_name* and change those characters to all lowercase.

```
{host_name.FIRST(15).TOLOWER()}
```

Add custom naming conventions

You can add custom naming conventions in the ViPR Controller UI.

Before you begin

- System Administrators can only add custom naming conventions.
- Review the maximum name length and the list of valid characters for the resource name on the physical system for which you are adding a custom naming convention.
- ViPR Controller does not enforce uniqueness for your custom name. To avoid any naming conflicts, make sure your naming conventions are unique.

Procedure

1. Navigate to **Physical** > **Controller Config**.
2. Select the tab that corresponds to the physical system for which you are creating a new custom naming convention. Your choices are: `SAN Zoning`, `VMAX Masking`, `VNX Storage Groups`, `VPLEX`, `XtremIO`, `HDS.`, `Isilon`, and `Volume Naming`.
3. Select the type of name you are creating. For example, if you selected VMAX Masking, you can select `Cluster Storage Group Name` from the name list.

   The default ViPR Controller naming convention with the **Scope Type** and **Scope Value** in light grey text appears. You cannot select and change the default convention until you add a new naming convention.
4. Click **Add.**
5. Select the **Scope Type**.
6. Select the **Scope Value**.

7. Type the **Value** of your custom naming convention.

   Following the naming convention syntax, use the available functions and the variables for the selected name. The variables for the name you selected are listed on the bottom of the screen. In addition, the variables that are recommended to ensure a unique name are marked with an asterisk (*).

8. Click **Save.**

Custom volume naming

You can set up a custom volume naming convention so the volume names will match between VPLEX and ViPR Controller. You can also customize the volume name to include other identifiers, such as the project name, host name, and so forth.

In a ViPR Controller configuration, there is a **Volume Naming** feature with three options available for use in customizing volume names:

Custom Volume Naming Enabled

This option is disabled by default. When set to `Yes`, the values in the next two choices in the drop-down list are used to name the volumes.

Volume Custom Name

When provisioning volumes using **Catalog** > **Block Storage Services**, the custom configuration settings specified in the `Volume Custom Name` values are used to name the volumes. This allows the user-supplied volume label to display in both VPLEX and ViPR Controller. You can customize any of these variables:

- volume_label
- volume_wwn
- project_name
- tenant_name

Export Custom Volume Name

When you want the volume name to include the name of the compute resource that the volume will be exported to, edit the `Export Custom Volume Name` values. For example, when you use **Catalog** > **Block Storage Services** > **Create Block Volume for Host**, you specify a Host in the service, If you have enabled the `Export Custom Volume Name` option, ViPR Controller will name the volume with the user-supplied label plus the export_name of the Host. For example, Demo1_lglw1024 where lgl21024 is the Host name. You can customize any of these variables:

- volume_label
- volume_wwn
- project_name
- tenant_name
- export_name

You may provision volumes using other host catalogs too, such as Block Services for Windows, Linux, and VMware.

Note

The user-supplied volume label cannot start with a numeric character. The label can only begin with the underscore character (_) or an alpha character.

Other services that use the custom volume naming conventions include:

- VPLEX volume clones
- VPLEX volume snapshots exposed as VPLEX volumes
- A vPool change to import a non-VPLEX volume
- VPLEX volume with mirror where the mirror is detached and promoted to become a new VPLEX volume
- Change virtual array
- VPLEX data migration

Note

There are some limitations in renaming volumes:

- You cannot rename a volume when you unexport and export to a different host.
- When moving a VPLEX volume from local to distributed, renaming of the VPLEX volume does not take place. The name at creation is retained throughout the life of the VPLEX volume.
- During change virtual array or VPLEX data migration operations, there is no dynamic renaming of VPLEX volumes when custom naming is enabled.

Procedure

1. Navigate to **Physical** > **Controller Config** > **Volume Naming**.
2. Select **Custom Volume Naming Enabled**.
3. Click **Add.**
4. Select the **Scope Type**.

   Click **System Type**.
5. Select the **Scope Value**.

   Click VPLEX .
6. Select or type the **Value** of your custom naming convention.

   Choose **Yes** to enable the Custom Volume Naming feature. Then select the Custom Volume Name and/or Export Custom Volume Name options and set up the naming conventions for each.

   Follow the syntax recommendations for creating custom names. The variables for the name you selected are listed on the bottom of the screen. In addition, the variables that are recommended to ensure a unique name are marked with an asterisk (*).
7. Click **Save.**

CHAPTER 3

Understanding and Setting Up Port Selection Rules

This chapter contains the following topics:

Summary of port allocation rules

ViPR Controller allocates storage ports for exported volumes from hosts and clusters using rules that consider the type of host initiator and various user-defined settings.

Port allocation evaluates available ports using the following rules, in the order listed. Rules 1 through 5 do not apply to the first port in a request, but are applied to the subsequent (redundant) storage port allocations in the same export.

Table 4 Summary of port allocation rules

Number	Rule	Explanation
1	DirectorRule17	Skipped for first port. Applies to VMAX only. Disabled for VMAX3. Select additional storage ports so that the director index, when added to the index of the first selected storage port, adds up to 17.
2	Different director type	Skipped for first port. Applies to VPLEX only. Select additional storage ports with a director type (A or B) different from the type used by the first selected storage port.
3	Different engine	Skipped for first port. Applies to VMAX, VPLEX, XtremIO, and HDS. From the available storage ports after the second rule, select storage ports whose engine is different from the previously selected storage port.
4	Different director	Skipped for first port. Applies to all array types, except XtremIO. From the available storage ports after the third rule, select storage ports using a different director from the previously selected storage port director.
5	Different CPU	Skipped for first port. Applies to VMAX only. From the available storage ports after the fourth rule, select storage ports using a different CPU from the previously selected storage port CPU.
6	Switch affinity (if set to true)	Applies to the first port and subsequent selections, if switch affinity is enabled. Applies to all supported host initiators and VPLEX. From the available storage ports after the fifth rule, select storage ports that connect to the same switch as the initiator.
7	Different switch	Applies to VMAX, VNX, XtremIO, Unity, and VPLEX. When exporting from clusters, there might be multiple initiators connected to different switches. From the available storage ports after the sixth rule, select storage ports that connect to a different switch from the previously selected storage port. If the sixth rule does not find any ports, use the results of the fifth rule, and select storage ports that connect to a different switch from the previously selected storage port.
8	Metrics-based port selection	Algorithms determine ports to avoid based on collected metrics.

Set up switch affinity

Switch affinity considers the location of the initiator port and gives preference to storage ports that are local on the same physical switch as the initiator port. By allocating local ports whenever possible, inter-switch link (ISL) traffic is reduced.

When the **Switch Affinity Enabled** parameter value is **True**, the switch affinity logic is considered in the list of rules for port allocations. The default state is **True**.

Note that the switch affinity logic is preceded by other rules for port allocation. Even when **True**, switch affinity might be overridden by other rules.

Switch affinity is supported for:

- VMAX
- VNX
- XtremIO
- Unity
- VPLEX
- VPLEX Backend—(export backend volumes to VPLEX), the VPLEX backend ports are considered the initiators.

To set the value of the **Switch Affinity Enabled** parameter:

Procedure

1. Select **Physical** > **Controller Configs** > **Port Allocation**.
2. Select **Switch Affinity Enabled** from the drop-down list.
3. Click **Add**.
4. For **Scope Type**, select **Global**.
5. For **Scope Value**, select **Default**.
6. For **Value**, select **True** to enable switch affinity logic or **False** to disable it.

Results

After a volume export, messages in the `controllersvc.log` file show the switch affinity results, as follows:

- initiators with switch affinity
- initiators with partial switch affinity—Some of the allocated storage ports are connected to the same switch as the initiators for the compute resources, and others are not.
- initiators without switch affinity

Overview of metrics-based port selection

Learn how to define the maximum performance-based limits for ports and how those limits are used by ViPR Controller for allocating new ports. Allocating new ports based on performance metrics, computed metrics, and user-defined maximum limits is supported on VMAX, VPLEX , VNX for Block, and Hitachi Data Systems (HDS).

Several performance-based metrics are collected from VMAX, VPLEX, VNX for Block, and HDS and are used to determine:

- Port percent busy.
- CPU percent busy.

Two additional metrics are also computed:

- Number of initiators using a storage port.
- Number of volumes using a storage port.

These metrics are then used to allocate new ports to avoid:

- Ports that are overloaded with too many volumes or too high of an I/O load.
- Ports that reside on CPUs where the CPU percent busy is too high or the CPU is servicing too many volumes.
- Allocating more storage on arrays that are overloaded.

For information on how ViPR Controller allocates new ports, based on these metrics, see How does ViPR Controller select a port when using performance metrics on page 66.

Before ViPR Controller can allocate new ports based on performance metrics, there are configuration requirements you must set up on HDS, and VNX for Block storage systems. For configuration requirements refer to the: *ViPR Controller Virtual Data Center Requirements and Information Guide* on the ViPR Controller Product Documentation Index .

You must also enable ViPR Controller for the collection of metrics from the storage arrays, as described in Set up metering prerequisites in ViPR Controller on page 70.

How does ViPR Controller select a port when using performance metrics

ViPR Controller takes averages of the performance-based metrics collected from the storage arrays and the number of initiators and volumes that it has already allocated to ports, and then compares these metrics to maximum limits (ceilings) that you configure fo determine which ports to select.

Metric calculations and averages

Several performance-based metrics are collected from VMAX, VPLEX , VNX for Block, and HDS and are used to determine:

- Port percent busy
- CPU percent busy

In addition, two additional metrics are computed byViPR Controller :

- Number of initiators ViPR Controller has already assigned to a storage port
- Number of volumes ViPR Controller has already assigned to a storage port

Note

On VMAX2, the number of volumes is computed across both ports on a director.

These numbers may not reflect all exports done outside of ViPR Controller.

Averaging the metrics values

The metrics collected for CPU Percent Busy and Port Percent Busy are averaged over time so that they reflect a relatively long term view of whether the port is overloaded. The system administrator can control this averaging process. There are three important time periods:

- The `Metering Interval` controls how often metering records will be read from the storage arrays. The default time period for this is one hour. This can be reduced to 30 minutes, or increased to multiple hours. To get accurate metrics on heavily loaded ports, it may be necessary to decrease the metering interval to 30 minutes, although this will cause increased ViPR Controller load for systems with many arrays. Increasing the metering interval will reduce the load. It is not recommended to have a metering interval greater than four hours. For information on how to set `Metering Interval`, see Set up metering prerequisites in ViPR Controller on page 70.
- The `Days to Average Utilization`, one of the ViPR Controller Port Allocation parameters, controls how long various samples are averaged together using a modified moving average. The default averaging period is 1 day, but you can configure the period from 1 to 30 days. The longer the averaging period, the less an instantaneous change in load is reflected in the average, and the less affect a current sample will have on the average. After the averaging period has been completed, a new average starts and will be computed. For information on how to set `Days to Average Utilization`, see *EMC ViPR Controller REST API Reference*.
- At the end of each averaging period, the modified moving average is added into a longer term Exponential Moving Average (EMA) that is calculated for each metric. The purpose of the EMA is to retain history about the port's utilization over time. An EMA is used because it weights recent values higher, and past values with exponentially decreasing weights as the sample's age increases. In that way recent port utilization is more important than past utilization. The `Weight for Exponential Moving Average` controls the weight of the current modified moving average versus past averages. For information on how to set `Weight for Exponential Moving Average`, see *EMC ViPR Controller REST API Reference*.

The default weight of the EMA is set at 0.6, but you can configure the weight from greater than 0 to less than or equal to 1. The higher the EMA weighting factor the more weight that the current modified moving average has on the EMA. A value of 1.0 uses only the current averaging period. For example, if the EMA weight is 0.6, the current modified moving average is multiplied by 0.6 and added to the previous EMA multiplied by 0.4 (1 - 0.4).

User-configurable parameters

There are several maximum limits (ceilings) that you can set, in addition to sampling times and the weight to use for the exponential moving average (EMA).

When a port reaches or exceeds one of the ceiling values, it is no longer available for new allocations, even if that causes provisioning to fail. You can change the settings. See the *EMC ViPR Controller REST API Reference* .

You can change the following settings:

- Maximum number of initiators that can use the port before new allocations are not allowed.
- Maximum number of volumes that can use the port before new allocations are not allowed.

Note

Volumes may be added to existing exports, such as masking views, storage groups, and storage views, with allocating new ports. These will put additional port load on the ports in that existing export. Therefore, you should set your ceilings lower than the maximum limit you require.

- Maximum average port percent busy value (from 0 - 100%) before new allocations are not allowed.
- Maximum average CPU percent busy value (from 0 - 100%) before new allocations are not allowed.
- The sample averaging time in days (1 -30 days)
- The weight for the EMA (the EMA factor).
- Metrics enabled
  - true = use collected metrics and calculate the port percent busy and the CPU percent busy.
  - false = only use the number of initiators and the number of volumes to allocate ports; ignore the collected metrics and do not calculate port percent busy and CPU percent busy.

Note

You should take care in setting ceilings. These are absolute limits. Ports which have one or more metrics over a ceiling will not be used for any allocations until such time as all metrics return to a value under the ceilings (or the ceiling limits are increased).

Allocating a port

The EMA Factor and (1- EMA Factor) values that you configured are used when ViPR Controller allocates a port. ViPR Controller takes the (modified moving average x EMAfactor) and the (EMA x 1 - EMAfactor) and does an instantaneous check of these values against the ceilings that you configured. For example, if you have the EMA factor set at 0.6, then ViPR Controller takes the (modified moving average x 0.6) and the (EMA x 0.4) for the instantaneous check against your configured ceiling values.

The port with the lowest metric, which has not reached or exceeded a ceiling is selected. When you require more than one port allocated, ViPR Controller tries to choose two ports that are on different hardware units. For example, you need two ports on a VMAX and there are 3 ports available:

- 7E0 has a port metric of 10
- 7F0 has a port metric of 20
- 8E0 has a port metric of 30

ViPR Controller chooses 7E0 as the first port since it has the lowest port metric, but 8E0 is chosen as the second port. Port 8E0 has a higher port metric than 7F0, but 8E0 is on a different director and, therefore, on different hardware units. This provides redundancy against hardware failures.

Note

If you have already allocated ports to a host or cluster, and you are just adding volumes to the same host, then ViPR Controller does not reallocate ports, it just adds the volumes to the export structure.

Global default port selection

ViPR Controller has a default port selection algorithm that can be used globally across all arrays.

The global default port selection algorithm is used:

- When performance-metrics collection is disabled for VMAX, VPLEX , VNX for Block, or Hitachi Data Systems (HDS).
- For storage arrays other than VMAX, VPLEX , VNX for Block, and HDS.

Calculated values
ViPR Controller automatically calculates two values from its database:

- Number of initiators ViPR Controller has already assigned to a storage port.
- Number of volumes ViPR Controller has already assigned to a storage port.

Note

On VMAX2, the number of volumes is computed across both ports on a director.

These numbers may not reflect all exports done outside of ViPR Controller.

User-configurable parameters
You can set a maximum limit for the number of initiators and volumes that use the port before new allocations are not allowed.

Volumes may be added to existing exports, such as masking views, storage groups, and storage views, with allocating new ports. These will put additional port load on the ports in that existing export. Therefore, you should set your ceilings lower than the maximum limit you require.

When a port exceeds one of the ceiling values, it is no longer available for new allocations, even if that causes provisioning to fail. You can change the settings in the ViPR Controller UI, as explained Change the port allocation parameters using the UI.

Note

You should take care in setting ceilings. These are absolute limits. Ports which have one or more of the number of initiators or volumes over their ceiling will not be used for any allocations until such time as both the number of initiators and the number of volumes return to a value under the ceilings (or the ceiling limits are increased).

Allocating a port
The port is determined as follows:

1. Ports are checked against the ceilings for the number of initiators and volumes.
2. The ports below their ceilings are checked for redundancy. When you require more than one port allocated, ViPR Controller tries to choose two ports that are on different hardware units.
3. From the set of ports with the most redundancy, the ports with the fewest number of volumes are selected.

Note

If you have already allocated ports to a host or cluster, and you are just adding volumes to the same host, then ViPR Controller does not reallocate ports, it just adds the volumes to the export structure.

Set up metering prerequisites in ViPR Controller

There are two configuration properties that you must ensure are set in ViPR Controller to enable the collection of metrics from VMAX, VPLEX , VNX for Block, and HDS.

You can set these configuration properties using both the ViPR Controller UI and the ViPR Controller UI REST API.

Use the ViPR Controller UI

After logging into the ViPR Controller UI as a system administrator, check whether metering is enabled, and to what value the metering interval is set.

Selecting **System** > **General Configuration** > **Controller** displays:

- The value of **Enable Metering** that must be set to **true** to collect metrics from the arrays.
- The value of **Metering Interval** that defines how often ViPR Controller collects data from the arrays. The metering interval can be set from 1800 seconds (30 minutes) up to 4 hours. The lower the number of seconds, the more accurate are the results. However, the higher the metering interval, the less overhead there is on ViPR Controller and the array.

Prerequisites for VNX and HDS metrics-based port selection

There are configuration settings on the VNX and HDS that are required for metrics-based port selection.

For prerequisite configuration settings for both VNX and HDS, see the *ViPR Controller Virtual Data Center Requirements and Information Guide* on the ViPR Controller Product Documentation Index .

Change the default port allocation parameters

System administrators can change the default values of the port allocation parameters.

You can use ViPR Controller UI or the REST API to change the port allocation parameters.

Change the port allocation parameters using the UI

You change the default values of the port allocation parameters by adding a new parameter setting. When you add a new parameter setting, ViPR Controller uses your setting value instead of the default value.

Before you begin

- You must set how often ViPR Controller will collect data from the array.
- Only system administrators can change port allocation parameters.

You can change these parameters:

- Initiator Ceiling = Maximum number of initiators that can use the port before new allocations are not allowed.

- Volume Ceiling = Maximum number of volumes that can use the port before new allocations are not allowed.
- Port Utilization Ceiling = Maximum average port percent busy value (from 0 - 100%) before new allocations are not allowed.
- CPU Utilization Ceiling = Maximum average CPU percent busy value (from 0 - 100%) before new allocations are not allowed.
- Days To Average Utilization = The sample averaging time in days (1 -30 days) . Default is one day.
- Weight For Exponential Moving Average = The EMA weight for the current sample. The EMA weight is greater than zero and less than or equal to 1.0. A value of 1.0 uses only the current averaging period.
- Metrics Enabled

  Note

  CPU percent busy is not calculated for HDS

  - true = use collected metrics and calculate Port percent busy and CPU percent busy.
  - false = only use the number of initiators and the number of volumes to allocate ports; ignore the collected metrics and do not calculate Port percent busy and CPU percent busy.

Procedure

1. Log into the ViPR Controller UI with System Administrator privileges.
2. Select **Physical** > **Controller Config**
3. Select **Port Allocation**.
4. Select the port allocation parameter that you want to change.
5. Click **Add.**
6. Select the **Scope Type**.
7. Select the **Scope Value**.
8. Type the value of the parameter.
9. Click **Save.**

VMAX performance metrics

The VMAX metrics collection is contingent on having metering turned on and configured.

The table describes the metrics collected from VMAX that ViPR Controller uses to allocate ports.

Table 5 Performance metrics collected on VMAX

Metric	Variable	Description
FEPort, FEAdapt: StatisticTime	sampleTime	A string representing the current time with the format, *yyyyMMddHHmmss.SSSSSS sutc*, where:

Table 5 Performance metrics collected on VMAX (continued)

Metric	Variable	Description
		• yyyy - is a 4 digit year • MM - is the month • dd - is the day of the month • HH - is the hour (24 hour clock) • mm - is the minut;e ss - is the second • mmmmmm - is the number of microseconds • sutc gives the sign and offset from GMT
FEAdapt: TotalIOs	iops	The cumulative number of I/O operations for the CPU (read and write).
FEAdapt: EMCIdleTimeDir	idle	The cumulative number of idle ticks.
FEPort: TotalIOs	iops	The cumulative number of IO requests for a port (read and write).
FEPort: KbytesTransferred	kbytesTransferred	The cumulative number of kilobytes transferred for read or write.
FEAdapt: EMCCollectionTimeDir	ticks	The cumulative number of ticks.

These metrics are used to calculate two values:

- Percent busy for the port (FEPort) which is computed from kbytesTransferred over the time period since the last valid sample.
- Percent busy for the CPU (FEAdapt) which is computed from the non IdleTime over the time period since the last valid sample.

VPLEX performance metrics

The VPLEX metrics collection is contingent on having metering turned on and configured. Set **Enable Metering** to `true` in **System** > **General Configuration** > **Controller** .

Each management server in a VPLEX MetroPoint configuration is a storage provider for VPLEX . Add the provider details for each of the VPLEX management servers using the **Physical** > **Storage Providers** > **Add** page in the ViPR Controller UI. This adds both cluster manager IP addresses to ViPR Controller and enables VPLEX port performance on both front-end ports.

The table describes the metrics collected from VPLEX that ViPR Controller uses to allocate ports.

Table 6 Performance metrics collected on VPLEX

Metric	Variable	Description
Timestamp	Time	The sample time in format: yyyy-mm-dd hh:mm:ss in UTC.
Director percent busy	director.busy	The percent time the director is busy performing I/O operations.
Director IOPs/sec	director.fe-ops	The number of I/O operations executed per second by the director.
Port IOPs/sec	fe-prt.ops	The number ofI/O operations executed per second by the port.
Port KB read/sec	fe-prt.read	The number of Kilobytes read per second by the port
Port KB write/sec	fe-prt.write	The number of Kilobytes written per second by the port

These metrics are used to calculate:

- Percent busy for the port (FEPort) which is computed from kbytesTransferred over the time period since the last valid sample.

VNX for Block performance metrics

The table describes the metrics that are collected onVNX for Block which ViPR Controller uses to allocate ports.

Note

VNX for Block metrics collection is contingent on having metering turned on and configured. See Prerequisites for VNX and HDS metrics-based port selection for more information.

Table 7 Performance metrics collected on VNX for Block

Metric	Variable	Description
FEPort: Total IOPs	iops	The cumulative number of IO requests for a port (read and write).
FEPort: KbytesTransferred	kbytesTransferred	The cumulative number of kilobytes transferred for read or write.

Table 7 Performance metrics collected on VNX for Block (continued)

Metric	Variable	Description
FEAdapt: IdleTimeCounter	idle	The cumulative ticks of idle time (idleTicksValue)
FEAdapt: IOTimeCounter	ioTime	The cumulative ticks of I/O busy time.
FEAdapt: TotalIOs	iops	he cumulative number of I/O operations for the CPU (read and write).
FEPort, FEAdapt: StatisticTime	sampleTime	A string representing the current time, of the format *yyyyMMddHHmmss.SSSSSS sutc* where: • yyyy - is a 4 digit year • MM - is the month • dd - is the day of the month • HH - is the hour (24 hour clock) • mm - is the minutes • ss - is the seconds • mmmmmm - is the number of microseconds • sutc gives the sign and offset from GMT

These metrics are used to calculate two values:

- Percent busy for the port (FEPort) which is computed from kbytesTransferred over the time period since the last valid sample.
- Percent busy for the CPU (FEAdapt) which is computed from the non idle time over the time period since the last valid sample.

HDS performance metrics

The table describes the metrics collected from HDS that ViPR Controller uses to allocate ports.

Table 8 Performance metrics collected on HDS

Metric	Variable	Description
FEPort: Total IOPs	iops	The cumulative number of IO requests for a port (read and write).

Table 8 Performance metrics collected on HDS (continued)

Metric	Variable	Description
FEPort: KbytesTransferred	kbytesTransferred	The cumulative number of kilobytes transferred for read or write.
FEPort, FEAdapt: StatisticTime	sampleTime	A string representing the current time, of the format *yyyyMMddHHmmss.SSSSSS sutc* where: • yyyy - is a 4 digit year • MM - is the month • dd - is the day of the month • HH - is the hour (24 hour clock) • mm - is the minutes • ss - is the seconds • mmmmmm - is the number of microseconds • sutc gives the sign and offset from GMT

These metrics are used to calculate:

- Percent busy for the port (FEPort) which is computed from kbytesTransferred over the time period since the last valid sample.

CHAPTER 4

Configuring Networks

This chapter contains the following topics:

Overview

ViPR Controller System Administrators can create and configure the networks in the ViPR Controller before creating virtual arrays or create and set up the networks while configuring a virtual array.

For information to create and configure networks in the virtual array see: Adding Fibre Channel networks in the virtual array, or Adding the IP networks in a virtual array.

Fibre Channel, iSCSI, and IP network configurations are supported by the ViPR Controller.

Fibre Channel

ViPR Controller supports discovery and use of Brocade and Cisco switches. When a SAN switch is added to ViPR Controller, the SAN networks (Brocade Fabrics or Cisco VSANs), are automatically discovered and registered in ViPR Controller, and displayed in the **Physical**, **Networks** page. Through discovery of the SAN switch topology, ViPR Controller discovers, and registers the host initiators for discovered hosts on the network, and identifies which storage systems are associated with the SAN switch. During a block storage provisioning operation, ViPR Controller will automatically assigns the host initiators, and storage ports, to use when the storage is provisioned to a host.

You can customize the path ViPR Controller will use during provisioning by:

- Deregistering fabrics, or VSANs from ViPR Controller networks.
  To exclude the network from being used as a resource n a ViPR Controller service.
- Assigning storage ports and host ports to the ViPR Controller networks.
  To specify the storage and host ports that ViPR Controller will use for connectivity during provisioning. By default, ViPR Controller selects the ports to use for connectivity between the storage and hosts during provisioning. However, if you specify the ports, ViPR Controller uses those ports for connectivity during provisioning.

ViPR Controller does not automatically create new zoning after you swap the storage ports and host initiators to a new fibre channel switch and create a new export for the host.

IP networks

You create the IP networks in the **PhysicalNetworks** page. While creating the IP networks, be sure to add the necessary storage and host ports to use to provision the storage to the hosts.

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, and then add the host, and storage system ports, which will be provisioned together, to the same IP network.

For steps to configure the IP networks see: Configuring IP, and iSCSI networks.

iSCSI

The iSCSI host ports must be logged into the correct target storage system ports before they can be used in the service.

For steps to configure iSCSI networks see: Configuring IP, and iSCSI networks.

Configuring IP and iSCSI networks

ViPR Controller can discover the ports of IP connected storage systems and hosts but it cannot discover the paths between them. It is necessary to create IP networks, and then add the host and storage system ports, which are provisioned together through the same IP network.

Before you begin

- IP Networks are created by System Administrators. Tenant Administrators cannot configure IP networks or add host ports to the network.
- If creating a network for a virtual array that will be used for file system exports to an ESXi cluster, add all ESXi server IP interface addresses (Management IP, vMotion IPs, and any other IP VMNIC visible in vCenter) per cluster.
- When configuring iSCSI networks for a provisioning service, the host initiators and storage ports which will be provisioned together, must be configured on the same network.
- Fibre channel ports may be added to an export group even if the virtual pool is configured for iSCSI only. XtremIO and VNX arrays perform their own storage port assignment, not ViPR Controller. As a result, there are still iSCSI and IP ports available regardless of the protocol type selected for the virtual pool.

Procedure

1. Go to the **Physical** > **Networks** page.
2. Click **Add IP Network**.
3. Enter the network **Name**.
4. Select the virtual arrays for which the IP network is being created.
5. In the IP Ports table, to select from discovered ports click:
   - **Add** > **Add Array Ports** to select from the list of discovered storage system ports.
   - **Add** > **Add Host Ports** to select from a list of added host ports.

   To manually add ports, click **Add** > **Add Ports**.
6. Click **Save**.

Configuring ViPR Controller to use existing SAN zones

When a block volume is exported to a host via a SAN network, SAN zones are created between the host initiators and the storage array ports allocated to the export. By default, ViPR Controller ignores existing SAN zones and uses its own intelligence to select ports to assign to a host or a cluster export. You have the option to configure ViPR Controller to consider using existing zoned ports when assigning ports to a host or cluster export. For example, you can use existing alias-based zones instead of zones created by ViPR Controller.

When reusing existing SAN zones, you can set one or both of these port allocation modes:

- Set the port allocation mode for host exports.
- Set the port allocation mode for back-end exports.

Limitations

- ViPR Controller can only discover alias-based and WWN-based zones in regular and smart zones.
- ViPR Controller does not discover port-based zones.
- You must manage these SAN zones outside of ViPR Controller. These zones are not removed when the export is removed.
- ViPR Controller does not recheck the paths for an existing export when a new volume is added with a different paths requirement.
- For co-existing exports, ViPR Controller assumes that zoning is done by the user and does not check or enforce any paths requirements.ViPR Controller tries to find existing zones and displays these zones in the UI. The only exception is when new initiators are added to an existing export. In this case, ViPR Controller tries to allocate additional ports for the new initiators and follows the same rules as newly ViPR Controller-created exports. ViPR Controller does not enforce any path requirement for co-existing exports.

Automatic and manual zoning

ViPR Controller provides two options for SAN zoning: automatic and manual that are set on the block virtual array. If no network systems are discovered in ViPR Controller, zoning is treated as manual for all virtual arrays regardless of this SAN zoning setting.

Note

Fiber channel (FC) alias zones are supported.

When automatic zoning is on, ViPR Controller does the following when using existing zoned ports:

- Gives zoned ports a higher priority for assignment than non-zoned ports.
- If more ports are zoned than needed,ViPR Controller applies the port selection criteria and selects a subset of ports for the export.
- If fewer ports are zoned than needed, ViPR Controller assigns additional ports and zones accordingly.

When automatic zoning is off, ViPR Controller does the following when using existing zoned ports:

- If more ports are zoned than needed, ViPR Controller applies the port selection criteria and selects a subset of ports for the export.
- If fewer ports are zoned than needed, ViPR Controller fails the operation because it cannot ensure that a sufficient number of paths exist.

Note

Do not mix SAN zoning settings. That is, if you set SAN zoning to manual for one virtual array and to automatic for another, it is possible that a zone could be deleted even it is in use by another export group.

Zones outside of ViPR Controller

In a SAN environment, there may be existing zones created outside of ViPR Controller that are not activated. Even if these zones have valid initiator and port configurations, ViPR Controller does not reuse them. ViPR Controller only uses activated SAN zones for provisioning. It never assumes deactivated SAN zones are available for provisioning.

Existing zoned ports: set port allocation mode for host exports

When using existing zoned ports, you can specify the port allocation mode for host exports or front-ends.

Before you begin

For the ViPR Controller user roles required to perform this operation see the *ViPR Controller Virtual Data Center Requirements and Information Guide*, which is available from the ViPR Controller Product Documentation Index .

Procedure

1. Go to **Physical** > **Controller Config**.
2. Click **Port Allocation**.
3. In the drop-down list, select Zoned Ports Favored for Host Exports.

Existing zoned ports: set port allocation mode for back-end exports

When using existing zoned ports, you can specify the port allocation mode for back-end exports for each back-end system type. Use this when creating exports between storage systems such as VMAX, VNX, VPLEX, and RecoverPoint.

Before you begin

For the ViPR Controller user roles required to perform this operation see the *ViPR Controller Virtual Data Center Requirements and Information Guide*, which is available from the ViPR Controller Product Documentation Index .

Procedure

1. Go to **Physical** > **Controller Config**.
2. Click **Port Allocation**.
3. In the drop-down list, select Zoned Ports Used for Backend Exports.

   If the number of zoned ports is insufficient for VPLEX and RecoverPoint back-end exports, this option does not appear.

Assigning storage ports and host ports in the ViPR Controller SAN networks

You can optionally add storage ports and host ports to a Brocade fabric or a Cisco VSAN to define the Fibre Channel connectivity that ViPR Controller uses when provisioning storage to hosts.

Before you begin

Procedure

1. Go to the **Physical**, **Networks** page.
2. Click the network name to open the **Edit Network** page.

3. Add storage ports to the network. Click:
   - **Add** > **Add Array Ports** to select from the list of discovered array ports.
   - **Add** > **Add Ports** to enter the storage ports manually.
4. Add host ports to the network. Click:
   - **Add** > **Add Host Ports** to select from the list of discovered host ports.
   - **Add** > **Add Ports** to enter the host ports manually.
5. Click **Save**.

Disabling SAN zoning when adding a volume into an export group

ViPR Controller performs a network check for each add volume request, which can degrade system performance. This check ensures that all zones created by ViPR Controller for an export continue to exist and any removed zone are re-created. You have the option to disable or enable this network check.

Before you begin

For the ViPR Controller user roles required to perform this operation see the *ViPR Controller Virtual Data Center Requirements and Information Guide*, which is available from the ViPR Controller Product Documentation Index .

Procedure

1. Go to **Physical** > **Controller Config**.
2. Click **SAN Zoning**.
3. In the drop-down list, select either Enable Zoning On Export Add Volume (the default) or Disable Zoning On Export Add Volume.

Deregistering fabrics or VSANs from ViPR Controller networks

Deregister the fabrics, or VSANs to exclude as a ViPR Controller resource.

You can deregiser but not delete networks from ViPR Controller.

Procedure

1. Select **Physical** > **Networks**.
2. Select the fabric or VSAN from the list.
3. Click **Deregister**.

CHAPTER 5

Creating and Configuring Virtual Assets

This chapter contains the following topics:

Creating a virtual array using storage systems

Add storage systems to create a virtual array when you want to add all of the storage system resources, and associated physical assets to the virtual array.

Before you begin

Procedure

1. Select **Virtual** > **Virtual Arrays**..
2. Click **Add** and enter the virtual array name.

   The **Edit Virtual Array** page opens.
3. Select the type of SAN zoning:
   - **Automatic** to allow ViPR Controller to automatically create the required zones in the SAN fabric when a provisioning request is made in this virtual array.
   - Select **Manual** to configure the zones outside of ViPR Controller.
4. If working in a multi-tenant environment, click **Grant Access to Tenant**, and select the tenants that will have access to the virtual array.
5. Click **Storage Systems** to add a storage system to ViPR.
6. Add the networks according to the type of storage that was added. Refer to either of the following sections for more information:
   - Add and configure the networks for block storage in the virtual array.
   - Add and configure the networks for file storage in a virtual array.
7. Optionally, click **Storage Ports** to add, or remove the physical storage ports associated with the virtual array.
8. Optionally, click **Storage Pools** to view the physical storage pools associated with the virtual array.

   You can also add or remove the storage pools from the list of storage pools that are displayed in the virtual array. This only removes the storage pools from the list. It does not remove the storage pool from the ViPR Controller resources.
9. Click **Save**.

Creating a virtual array using storage ports

Add storage ports to create a virtual array, when you want to partition portions of the storage system, and use only the storage system resources, associated with the storage ports in the virtual array.

Before you begin

Procedure

1. Select **Virtual** > **Virtual Arrays**..
2. Click **Add** and enter the virtual array name.

   The **Edit Virtual Array** page opens.
3. Select the type of SAN zoning:

- **Automatic** to allow ViPR Controller to automatically create the required zones in the SAN fabric when a provisioning request is made in this virtual array.
- Select **Manual** to configure the zones outside of ViPR Controller.

4. Click **Storage Ports**.
5. Click **Add** in the **Storage Ports** page.
6. Select only the storage ports you want to add to the virtual array.

   You can search for a storage port by entering characters of any one of the storage port attributes in the **Search** field.
7. Click **Add** once you have selected all the storage ports for the virtual array.
8. Go back to the **Edit Virtual Array** page to review the contents of the array.

   You will see only the selected storage ports, networks, and storage systems associated with the storage ports are added to the virtual array.

Adding Fibre Channel networks in the virtual array

Fibre Channel networks are automatically added, discovered, and registered in ViPR Controller when the fabric switch is added to the ViPR Controller physical assets.

Before you begin

- When selecting the Fibre Channel networks to add to the virtual array the storage systems and hosts to which the storage will be provisioned must be configured on the same network.
- If the hosts were added to ViPR Controller, and not discovered, the host ports must be manually added to the networks.
- Optionally, storage ports can be added to the network to control which ports will be used when the storage is provisioned on the host.

Procedure

1. Click the virtual array name.
2. Click **Networks** in the **Edit Virtual Array** page.
3. Click **Add**.
4. Leave the selected virtual array, and select any other virtual array in which to add the network.

   If the Fibre Channel network has already been created, and configured you can stop here. Otherwise, continue to configure the network ports.
5. If required: add host ports to the network. Click
   - **Add** > **Add Host Ports** to select from the list of discovered host ports.
   - **Add** > **Add Ports** to enter the host ports manually.
6. Optionally, add storage ports to the network. Click
   - **Add** > **Add Array Ports** to select from the list of discovered array ports.
   - **Add** > **Add Ports** to enter the storage ports manually.
7. Click **Save**

Adding IP networks in a virtual array

ViPR Controller can discover the ports of IP connected storage systems and hosts but it cannot discover the paths between them. It is necessary to create IP networks, and then add the host and storage system ports, which will be provisioned together to the same IP network.

Procedure

1. Go to **Virtual** > **Virtual Array**.
2. Click the virtual array name.
3. Click **Networks** in the **Edit Virtual Array** page.
4. Click **Create IP Network**.
5. Leave the selected virtual array, and select any other virtual array in which to add the network.

   If the IP network has already been created, and configured you can stop here. Otherwise, continue to configure the network ports.
6. Add host ports to the network. Click
   - **Add** > **Add Host Ports** to select from the list of discovered host ports.
   - **Add** > **Add Ports** to enter the host ports manually.

   If creating a network for a virtual array that will be used for file system exports to an ESXi cluster, add all ESXi server IP interface addresses (Management IP, vMotion IPs, and any other IP VMNIC visible in vCenter) per cluster.
7. Add storage ports to the network. Click
   - **Add** > **Add Array Ports** to select from the list of discovered array ports.
   - **Add** > **Add Ports** to enter the storage ports manually.
8. Click **Save**.

Creating block virtual pools

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. You specify this criteria when creating block virtual pools.

Before you begin

For information on how ViPR Controller performs the selection process for provisioning, see the *ViPR Controller Virtual Data Center Requirements and Information Guide*, *How Storage Pools are Selected for Provisioning*, section which is available on the ViPR Controller Product Documentation Index .

When creating virtual pools for source and target configurations, it is recommended to create the target virtual pool before creating the source virtual pool, since the source virtual pool requires the target virtual pool to be created.

After ViPR Controller uses a virtual pool, you may not be able to change some of its attributes. These attributes appear as disabled fields or may generate an error message when selected.

Procedure

1. Go to the **Virtual** > **Block Virtual Pools** page.
2. Click **Add** to create a block virtual pool.
3. Type the name and description for the virtual pool.

   Since the virtual pool performs provisioning operations, it is recommended that the name .

   - Conveys information about the type of storage that it provides, its performance and protection level, or how to use it, such as gold, tier1, backup.
   - Be created with a limited number of characters. When creating volumes, ViPR Controller truncates the volume name after 64 characters. Volume names can get lengthy, for example. when an R2 device is created, ViPR Controller names it with the label+virtual pool name+volume name, therefore it is important to be aware of the number of characters you are using in the virtual pool name.

4. Select the virtual arrays on which the virtual pool is created.
5. To limit the total amount of capacity provisioned from this virtual pool, check **Enable Quota** and specify a maximum value in GB.
6. Expand **Hardware**.

   The options that appear depend on the selected system type. For example, Thin Volume Preallocation is only available for the EMC VMAX system type.

Option	Description
Provisioning Type	Thick provisioning allocates all the physical storage space for the entire size of a LUN at creation time. Thin provisioning causes storage space to be allocated to a LUN as data is written to the LUN. For thin provisioning, you may pre-allocate a percentage of a LUN's physical storage space by specifying a percentage value in the **Thin Volume Preallocation** field. **Note** If you are creating a virtual pool for RecoverPoint journal volumes on VMAX, set the provisioning type to `Thick`, as ViPR Controller does not pre-allocate the volumes.
Protocols	The block protocols, such as FC and iSCSI, supported by the physical storage pools that comprise the virtual pool. This field lists only the protocols supported by the virtual array networks.
Drive Type	The drive type supported by the physical storage pools. The value of NONE allows any drive type.
System Type	The storage system type, such as VMAX and VNX block, to provide the storage pools. This field lists only the storage systems supported by the networks that were configured for the virtual array. The value of NONE allows any storage system to provide the pools.

Option	Description
Thin Volume Preallocation	If you selected thin provisioning, specify the percentage of the physical storage to initially allocate to a volume. **Note** Preallocation for storage on a VMAX 2 system requires the following configuration setting. The line `SYMAPI_ALLOW_PARTIAL_ALLOC_PRE_V3=TRUE` must exist in the SMI-S Provider's `options` file. See the *ViPR Controller Integration with VMAX and VNX Storage Systems Guide* for more information.
Multi-Volume Consistency	When enabled, resources provisioned from the pool support the use of consistency groups. If disabled, a resource cannot be assigned to a consistency group when running ViPR Controller block provisioning services. This option is • required for RecoverPoint, and VPLEX Metro • Optional for SRDF, Snaps or Clones When used with VPLEX, this option must be set for both the source and target VPLEX pools.
Expandable	When enabled: • Volumes are expanded non-disruptively. **Note** This can cause a decrease in performance. • Native continuous copies are not supported. When disabled, storage is selected based on performance over expandability.

These additional options only appear for EMC VMAX storage systems:

Option	Description
RAID level	Select the RAID levels for the volumes in the virtual pool.
Unique Auto-tiering Policy Names	When you create auto-tiering policies on a VMAX storage system through Unisphere, you can assign names to the policies you build. These names are visible when you enable Unique Auto-tiering Policy Names.
Auto-tiering Policy	The Fully Automated Storage Tiering (FAST) policy for the virtual pool.
Enable Compression	When enabled, only the VMAX3 All Flash storage groups, which support compression will be available to add to the virtual pool. It is not required that compression is enabled on the VMAX3 storage groups, it is only required that compression is supported on the storage groups. When storage from this virtual pool is provisioned to the host, it

Option	Description
	will apply the compression settings defined on the storage system.
Fast Expansion	When enabled, ViPR Controller creates concatenated meta volumes in the virtual array. If disabled, ViPR Controller creates striped meta volumes
Host Front End Bandwidth Limit	Controls VMAX resource consumption at the storage group level by limiting the amount of front-end bandwidth that are consumed by the VMAX devices provisioned from this virtual pool. This value is measured in MB/s. To allow unlimited front-end bandwidth consumption, set this value to zero.
Host Front End I/O Limit	Controls VMAX resource consumption at the storage group level by limiting the amount of I/Os per second (IOPS) that are consumed by the VMAX devices provisioned from this virtual pool. This value is measured in IOPS. To allow unlimited front-end I/O consumption, set this value to zero.

7. For VMAX, VNX Block, Unity, or XtremIO storage systems, expand Resource Placement Policy to set these options:

Option	Description
Default - Storage Arrays/Pools selection based on performance metrics and capacity	Allow ViPR Controller to use the default method of storage pool selection when provisioning from this virtual pool.
Host/Array Affinity - Storage Arrays/Pools selection based on Host/Cluster array affinity first, then performance metrics and capacity	**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** > **Controller Config** > **Host/Array Affinity Resource Placement** tab is greater than the amount of available preferred storage systems. **Note** 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.

8. Expand **SAN Multi Path** to set these options:

Option	Description
Minimum Paths	The minimum number of paths that ViPR Controller can create from the host to the storage array. If ViPR Controller is unable to establish the specified minimum number of paths, the provisioning operation fails.
Maximum Paths	The maximum number of paths that ViPR Controller can attempt to configure per host. ViPR Controller initially attempts to create the number of paths specified in this option. If ViPR Controller is unable to create the number of paths specified in this option, it attempts to create a decreasingly fewer number of paths down to the value specified in Minimum Paths. If you set the Maximum Path too low, it can result in unused initiators that are not zoned to ports.
Paths per Initiator	The number of ports to allocate to each used initiator.

- If the number of initiators is less than max_paths and paths_per_initiator = 1, then some paths are unused and each initiator gets one port.
- If the number of initiators is less than max_paths and paths_per_initiator > 1, then some initiators are assigned multiple ports until max_paths is reached. The ports are balanced across networks, if possible.
- If the number of initiators is equal to max_paths, each initiator is masked and zoned to exactly one path if paths_per_initiator=1. If paths_per_initiator is > 1, then some initiators are unused, and each ports that used is assigned paths_per_initiator number of ports.
- If the number of initiators is greater than max_paths, max_path number of ports is assigned to initiators and the remaining initiators are unassigned. The ports are balanced across networks, if possible.

9. For VPLEX environments, expand **High Availability** to set these options:

Option	Description
None	No High Availability. Only the VPLEX Local / VPLEX Distributed option supports High Availability.
VPLEX Local	Uses only the VPLEX local volumes in the virtual pool. When enabled, the **Automatic Cross-Connect** option allows exports to automatically occur from both VPLEX clusters when possible.
VPLEX Distributed	Uses only VPLEX distributed volumes in the virtual pool that match other virtual pool settings in the virtual pool. Specify the following values: • **High Availability Virtual Array** as the destination array for the distributed volume. • **High Availability Virtual Pool** as the pool for the distributed volume. • **Automatic Cross-Connect**

10. To protect the volumes in the virtual pool, expand **Data Protection** to set these options:

Option	Description
Maximum Snapshots	The maximum number of local snapshots allowed for resources from this virtual pool. To be able to use the ViPR Controller Create Block Snapshot for a Volume catalog service, specify a minimum value of 1
Maximum Continuous Copies	The maximum number of native continuous copies allowed for resources from this virtual pool. To be able to use the ViPR Controller Create Continuous Copy catalog service, specify a minimum value of 1.
Continuous Copies Virtual Pool	Allows a different virtual pool to be used for native continuous copies. Native continuous copies are not supported for virtual pools with the expandable attribute enabled.
Protection System	Provides protection for volumes created in the virtual pool. The possible values are: • **None** • **EMC Recoverpoint** ▪ RecoverPoint protection requires a virtual array to act as the RecoverPoint target and optionally an existing target virtual pool. ▪ Set the source journal size as needed. The RecoverPoint default is 0.25 times protected storage. A fixed value (in MB, GB or TB). A multiplier of the protected storage. Minimum allowable by RecoverPoint (10 GB). ▪ Select **Add Copy** to add one or two RecoverPoint copies, specifying the destination **Virtual Array**, and optionally, A **Virtual Pool** to specify the characteristics of the RecoverPoint target. The default is to the same virtual pool as the source volume. A **Journal Virtual Array** for the journal volume of this RecoverPoint copy. The default is the same virtual array as the RecoverPoint copy. A **Journal Virtual Pool** for the journal volume of this RecoverPoint copy. The default is the same virtual pool as the RecoverPoint copy. The RecoverPoint target **Journal Size**. The RecoverPoint default is 0.25 times protected storage. **Note** The virtual array chosen for the journal volume must provide storage on the same site as the corresponding RecoverPoint copy volume. ▪ If you selected **VPLEX Distributed** for **High Availability**, select **RecoverPoint Advanced Settings**, and optionally,

Option	Description
	Select entries for **Journal Settings** to specify a virtual array and virtual pool for the journal volume of this RecoverPoint copy. The default is to the same virtual array and virtual pool as the RecoverPoint copy. Select **Protect HA Site** to specify RecoverPoint protection from the High Availability VPLEX site for the source volume to the target virtual array.. Select an **Active Site** to specify the VPLEX site for active protection with RecoverPoint . • **VMAX SRDF** ▪ VMAX SRDF protection requires a virtual array to act as the SRDF target, and optionally an existing target virtual pool. ▪ Select the **SRDF Copy Mode**: Synchronous, Asynchronous, or Active (Active is for SRDF Metro on VMAX3 systems only). ▪ Select **Add Copy** to add an SRDF copy, specifying the destination virtual array, and optionally a virtual pool. • **VPLEX Local** • **VPLEX Distributed** ▪ Select the ViPR Controller virtual array to use as the destination for the distributed volume. ▪ Select the ViPR Controller virtual pool to use when creating the distributed volume.

11. To restrict access in a multiple tenant environment, expand **Access Control** to set these options:
    a. Enable **Grant Access to Tenants**.
    b. Select which **Tenants** can access this virtual pool.
12. To view the discovered storage pools and to choose how to perform **Pool Assignment**, expand **Storage Pools**:
    - Automatic — the storage pools of the virtual pool are automatically updated as the pools meeting the criteria are added or removed from the virtual array, or when their registration or discovery status changes.
    - Manual — provides a checkbox against each pool to include in the virtual pool.
13. Click **Save**.

Creating file virtual pools

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. You specify this criteria when creating file virtual pools.

Before you begin

- Before creating virtual pools in ViPR Controller, review the storage system-specific field descriptions, configuration requirements, and recommendations in the *ViPR Controller Virtual Data Center Requirements and Information Guide* which is available from the ViPR Controller Product Documentation Index .
- For the ViPR Controller user roles required to perform this operation see the *ViPR Controller Virtual Data Center Requirements and Information Guide*, which is available from the ViPR Controller Product Documentation Index .
- Once resources in the virtual pool have been used, only some of the attributes can be changed. Fields that cannot be changed are disabled, or an error message is generated when it is selected.

Procedure

1. Go to the **Virtual** > **File Virtual Pools** page.
2. Click **Add** or select an existing virtual pool name to edit.
3. Enter a **Name** and a **Description** for the virtual pool.
4. Select the **Virtual Arrays** for which the virtual pool will be created.
5. Check or uncheck **Enable Quota**. If enabled enter the maximum amount of storage, in GB, that can be allocated to this virtual pool.
6. While defining the virtual pool criteria, it is recommended to change the criteria one at a time and expand Storage Pools to check which storage pools matching the criteria are available.

   The pool matching algorithm runs shortly after a criteria has been selected and the matching pools will be from all systems that can provide pools that support the selected protocol.
7. Expand **Hardware** to define the following criteria:

Option	Description
Provisioning Type	Must be set to **Thin**. File systems are only thinly provisioned. When adding file storage to the virtual pool, set the pool to Thin provisioning.
Protocols	The file protocols supported by the physical storage pools that will comprise the virtual pool. Possible protocols are CIFs, or NFS for all file storage systems, and NFSv4 for Isilon storage systems.
Drive Type	The drive type that any storage pools in the virtual pool must support. NONE will allow storage pools to be contributed by any storage pool that support the rest of the defined criteria
System Type	The system type that you want the storage pools to be provided by. NONE will allow storage pools to be contributed by any array that supports the rest of the defined criteria. Only the systems supported by the networks configured in the virtual array are selectable.

8. Expand **Data Protection** to define the following:

Option	Description
Maximum Snapshots	The maximum number of local snapshots allowed for resources from this virtual pool. To use the ViPR Controller Create Snapshot services, a value of at least 1 must be specified.
Schedule Snapshots	When enabled, we filter storage pools that have snapshot scheduling capabilities.
Replication	When enabled, storage pools that support replication are displayed.
Allow Policies at Project	When enabled by the System Administrator, policies can be applied at the Project level during vPool configurations.
Allow Policies at File System	When enabled by the System Administrator, policies can be applied at the file system level for file systems from this vPool.

9. Expand Archive to enable the Long Term Retention period.
10. Expand **Access Control** to restrict access in a multiple tenant environment.
    a. Enable **Restrict Tenant Access**.
    b. Select the **Tenants** that will have access to this Virtual Pool.
11. Expand **Storage Pools** to view the discovered storage pools, and to choose how the **Pool Assignment** will be performed:
    - Automatic — the storage pools that make up the virtual pool will be updated as pools that meet the criteria are added or removed from the virtual array. This can occur when new pools that meet the criteria are added or removed from the system, or their registration or discovery status changes.
    - Manual — provides a checkbox against each pool to enable it to be selected. Only the selected storage pools will be included in the virtual pool.

    The pool matching algorithm runs shortly after a criteria has been selected and the matching pools will be from all systems that can provide pools that support the selected protocol.
12. Select **Save**.

Creating object virtual pools

The **Assets** > **Object Virtual Pools** > **Create or Edit Object Virtual Pool** pages to view, create, edit, and delete object virtual pools.

Before you begin

Prior to creating or editing object virtual pools, review the requirements, and information provided in the *ViPR Controller Virtual Data Center Requirements and Information Guide* provided in the ViPR Controller Product Documentation Index .

After ViPR Controller uses a virtual pool, you may not be able to change some of its attributes. These attributes appear as disabled fields or may generate an error message when selected.

Procedure

1. Go to **Virtual** > **Object Virtual Pools** > page.
2. Click **Add**, or if editing an existing Object Virtual Pool, click the Object Virtual Pool name.
3. Enter a **Description**.
4. Select the virtual arrays on which the virtual pool is created.

   You must select at least one virtual array that has been configured with an object storage system.

   - Select **All** to associate the virtual pool with all the virtual arrays.
   - Select **None** to unselect all the virtual arrays previously selected.
5. Expand **Hardware**, select.
   - The **Protocol** on which to filter the list of available Replication Groups to add to the Object Virtual Pool.
   - Select the **System Type** storage system.
6. Expand Data Protection to set the:

Option	Description
Maximum Retention (Days)	Sets the maximum number of retention time in days, on the virtual pool. If a retention value is set greater than zero, then all the buckets created with this virtual pool can be created with a retention period up to the maximum retention value set here. If this field is left empty, or set to zero, then there is no maximum retention is defined on the virtual pool.
Minimum Data Centers	The minimum number of data centers that the storage group is spanning accross to be included in this virtual pool. The minimum value must be one.

7. Expand **Access Control** to only include storage pools from a specific ViPR Controller tenant.
8. Expand **Storage Pools** to see the list of available storage pools that meet the criteria you have defined, and define the way ViPR Controller will select the storage pools that will be used to create the buckets:
   - When **Automatic** is selected the storage pools that comprise the virtual pools are automatically updated during the virtual pool's lifetime based on the availability of storage pools in the virtual array.
   - When **Manual** is selected, you must select which storage pools to add to the virtual pool and the storage pools included in the virtual pool will be fixed unless manually edited.
9. Click **Save**.

Creating a compute virtual pool

Compute virtual pools are a pool of compute system elements (blades for UCS). When a Vblock System Service is run, ViPR Controller pulls the required compute resources from the selected compute virtual pool.

Before you begin

- After a virtual pool is used by ViPR Controller, you can only change some of its attributes. Fields that you cannot change are disabled or an error message appears when selected.
- For ViPR Controller to use a compute virtual pool, which is made up of UCS blades, for provisioning, at least one service profile template must be selected in the compute virtual pool.
- Contact your UCS administrator about which service profile template to use with ViPR Controller to provision the Vblock system, and review the ViPR Controller requirements for service profile templates in the *ViPR Controller Virtual Data Center Requirements and Information Guide*, which is available from the ViPR Controller Product Documentation Index .

Procedure

1. Go to the **Virtual** > **Compute Virtual Pools** page.
2. Click **Add**.
3. Complete the following fields.

Option	Description
Name	Enter the name of the virtual pool.
Description	Optionally, enter a virtual pool description.
System Type	The type of compute system for example, Cisco UCS.
Virtual Arrays	Select one or more virtual array. The compute system, from which you will be assigning compute elements to the compute virtual pool, must have connectivity to the selected virtual array. ViPR Controller identifies which compute systems are part of a virtual array by the networks (VSANs) that were added to the virtual array. When a network (VSAN), to which a compute system is connected, is added to a virtual array, ViPR Controller includes the compute system in the virtual array topology, and determines which compute elements (blades) are available in the selected virtual arrays.
Access Control	Optionally, assign the tenants who will have access to the compute virtual pool.
Qualifiers	Optionally, enter minimum and maximum values to eliminate blades, which do not match the criteria, from the list of available blades that will appear in the **Compute Element** list. When no minimum is set, ViPR Controller defaults to zero. There is no default maximum value. The maximum is unlimited when it is not set. For example:

Option	Description
	• If processors are set with a minimum of 6 and no maximum, then only blades with 6 or more processors will be available to use in the compute virtual pool. • If processors are set with no minimum, and a maximum of 16, then any blade with 16 or less processors will be available to use in the compute virtual pool. • If no minimum or maximum value is set for processors ViPR Controller will include available blades with any number of processors in the virtual pool.
Compute Elements	Choose whether to manually assign the compute elements to the virtual pool, or to allow ViPR Controller to automatically assign the compute elements to the pool based on the criteria defined in the **Qualifiers**. If **Manual** was selected, chose the compute elements to include in the virtual pool. The compute elements are populated from any compute systems determined to be in the selected virtual arrays. The compute elements must be registered and available. If qualifiers were defined, only the compute elements within the constraints of the qualifiers will be presented. If no qualifiers were assigned, all the available compute elements from the compute system are presented. Compute elements that are not available in the Compute Virtual Pools have been used by ViPR Controller for a ViPR Controller operation, or by an external process.
System Type Configuration	For UCS, select the service profile template, or updating service profile template that contains the configuration definitions to apply to the blades in the virtual pool. Invalid updating service profile templates are omitted, or greyed out, and cannot be selected.

4. Click **Save**.

Set up VDC for a tenant

You can add access control to virtual arrays and virtual pools to make them available to specific tenants.

A virtual array comprises array endpoints and host endpoints interconnected by a SAN fabric or an IP network. The virtual array can comprise both fibre channel and IP networks. In this way different array ports can be configured into different virtual arrays, allowing a physical array to contribute to more than one virtual array.

This partitioning of physical arrays into virtual arrays, coupled with the ability to assign access to specific tenants, provides control over the storage provisioning environment made available to a tenant.

Even finer grained control can be obtained by assigning specific virtual pools to tenants. For storage provisioning purposes, the physical storage pools of a virtual array are offered as virtual pools based on their performance and protection characteristics. Restricting access to a virtual pool to specific tenants could mean that

if a virtual pool is configured to use a particular array type, restricting access to the virtual pool can prevent a particular tenants from accessing the array. Similarly, you could restrict access to a pool that provides a particular performance characteristic, such as SSD.

Set up tenant access to virtual arrays and virtual pools

When configuring a tenant, you define which virtual arrays and virtual pools a tenant can access using an access control list. This lists controls which tenants are authorized to access VDC-level resources and which users or groups are authorized to access tenant-level resources.

Before you begin

- You must be a System Administrator in ViPR Controller.

Procedure

1. To make a virtual array available to specific tenants:
   a. Navigate to **Virtual** > **Virtual Arrays**.
   b. Select the virtual array to assign tenant access.
      The **Edit Virtual Array** page appears.
   c. Expand **Access Control**.
   d. Click the **Grant Access to Tenants** box and select the tenants to access this virtual array.
   e. Click **Save**.
      Users belonging to the selected tenants can access the virtual array.
2. To make a virtual pool available to specific tenants:
   a. Navigate to **Virtual** > **Block Virtual Pools** or **Virtual** > **File Virtual Pools**.
   b. Select the virtual pool to assign tenant access.
      The **Edit Virtual Pool** page appears.
   c. Expand **Access Control**.
   d. Click the **Grant Access to Tenants** box and select the tenants to access this virtual pool.
   e. Click **Save**.
      Users belonging to the selected tenants can access the virtual pool.

File Protection Policy Templates

Use the **Virtual** > **File Protection Policy Templates** page to view, create, edit, and delete file protection policies for Isilon. You can create file snapshot policies and file replication policies and apply them at the Virtual Pool, Project, or File System level. Policies are multi-tenant aware and have controlled access.

The ViPR Controller roles required for file protection policy management are as follows:

Table 9 File Protection Policy role requirements

Function	Role requirements
Create/edit policy template	System Administrator, System Monitor
Create vPool	System Administrator, System Monitor
Policy assignment at vPool level	System Administrator
Policy assignment at Project level	System Administrator AND System Monitor
Policy assignment at File System level	System Administrator AND System Monitor

The **File Protection Policy Templates** page lists the file protection policies and the following attributes:

Table 10 File Protection Policy attributes

Column name	Description
Selection column	Select one or more rows and click **Delete** to delete the file protection policies. Select one or more rows and click **Assign Policy** to assign the policies to one or more virtual pools, projects, or file systems. Select one or more rows and click **Unassign Policy** to unassign the policies.
Name	The name of the file protection policy.
Type	The file protection policy type: File Snapshot Policy, File Replication Policy.
Applied At	The level at which the policy is applied: Virtual Pool, Project, File System.
vPool(s)	The Virtual Pools to which the policy is assigned.
Project(s)	The projects to which the policy is assigned.
Priority	The policy priority: High, Normal.
Description	A description of the policy.

Note

Scheduled policies from earlier ViPR Controller versions are migrated to File Protection Policy Templates during an upgrade. They can be found under **Virtual** > **File Protection Policy Templates** and have the following **Description**: "Policy created from virtual pool <name> replication while system upgrade."

Creating a file protection policy template

Click **Add** on the **Virtual** > **File Protection Policy Templates** page to open the **Create File Protection Policy Template** page and create a file protection policy. You can

create a file snapshot policy or a file replication policy and apply it at the Virtual Pool, Project, or File System level.

The ViPR Controller roles required for file protection policy management are as follows:

Table 11 File Protection Policy role requirements

Function	Role requirements
Create/edit policy template	System Administrator, System Monitor
Create vPool	System Administrator, System Monitor
Policy assignment at vPool level	System Administrator
Policy assignment at Project level	System Administrator AND System Monitor
Policy assignment at File System level	System Administrator AND System Monitor

Procedure

1. Specify information for the following options:

Option	Description
Type	Select: File Snapshot Policy, File Replication Policy.
Name	Specify a name for the file protection policy.
Description	Specify a description for the file protection policy.
Snapshot Name Pattern	File Snapshot Policy only. The default pattern is: `{Cluster}_{vNas}_{VPool}_{Policy_TemplateName}_%Y-%m-%d-_%H-%M`, and is not editable.
Replication Type	File Replication Policy only. Select: Remote, Local.
Copy Type	File Replication Policy only. The default is Asynchronous.
Priority	File Replication Policy only. Select High, Normal. When a policy needs precedence over other policies, select High.
Worker Threads	File Replication Policy only. Select a value from 3 to 10. The default is 3. Increase the number of worker threads if there is a large amount of data to be replicated.
Run every	Specify a Frequency and a value. For Frequency, select Minutes, Hours, Days, Weeks, Months. For Weeks, specify Day of Week. For Months, specify Day of Month.
Run/Start at	Specify the time to start the run in `HH:MM` format.

Option	Description
Snapshot Expiration	File Snapshot Policy only. Select Never expires, Snapshot expires. For Snapshot expires, specify Hours, Days, Weeks, Months, and a value.
Apply Policies at	Select Virtual Pool, Project, File System.

2. Click **Save** to create the new file protection policy.

Assigning a file protection policy template

Click **Assign Policy** on the **Virtual** > **File Protection Policy Templates** page to open the **Assign Policy** page for the selected policy. You can assign the policy at the Virtual Pool or Project level.

The ViPR Controller roles required for file protection policy management are as follows:

Table 12 File Protection Policy role requirements

Function	Role requirements
Create/edit policy template	System Administrator, System Monitor
Create vPool	System Administrator, System Monitor
Policy assignment at vPool level	System Administrator
Policy assignment at Project level	System Administrator AND System Monitor
Policy assignment at File System level	System Administrator AND System Monitor

Procedure

1. Specify information for the following options:

Option	Description
Policy	The name of the policy selected in the **File Protection Policy Templates** page.
Apply Policies at	The policy level specified in the **File Protection Policy Templates** page: Virtual Pool, Project, File System. Not editable.
Virtual Pool	Specify a virtual pool for the Project or Virtual Pool policy. A file snapshot policy can be applied to multiple vPools; a file replication policy can be applied to one vPool.
Projects	For Project policy only. Specify one or more projects for the Project policy.
Source Virtual Array	For Replication policy only. Specify the source virtual array for the Replication policy.

Option	Description
Target Virtual Array	For Replication policy only. Specify the target virtual array for the Replication policy.

2. Click **Save** to assign the file protection policy.

CHAPTER 6

Tracking Asynchronous Operations

This chapter contains the following topics:

Overview

A number of ViPR Controller operations and services are processed asynchronously. Asynchronous operations return a `task` (or list of `tasks`).

Each operation has a unique operation ID. All tasks related to an operation have that same operation ID.

Each `task` represents a block of work performed by the controller engine. You can check these `tasks` to see if the operation succeeded, failed or is still in progress. You can use the UI and the ViPR Controller REST API to view the progress of these `tasks`.

There are two types of `tasks`:

- Tenant `tasks`, such as adding a host.
  - Any user that is a member of the tenant can view the `tasks` that are related to that tenant.
  - Any user that is a member of the tenant can view the details of the `tasks` related to that tenant.
- System `tasks` that are not associated with any tenant, such as adding a storage array.
  - Only a system administrator can view system `tasks`.
  - Only system administrators and security administrators can view the details of a system `task`.

By default, `tasks` last for seven days from the date of completion. But this value can be changed in `task` configuration options. In addition, when you delete a resource the `tasks` that are associated with the resource are still available for viewing.

Viewing of tasks

You can view tenant and system tasks but only system administrators and security administrators can view the details of these tasks.

There are two different means to view tasks:

- A Task popup
- The **Tasks** screen in **Resources** > **Tasks**

Task popup

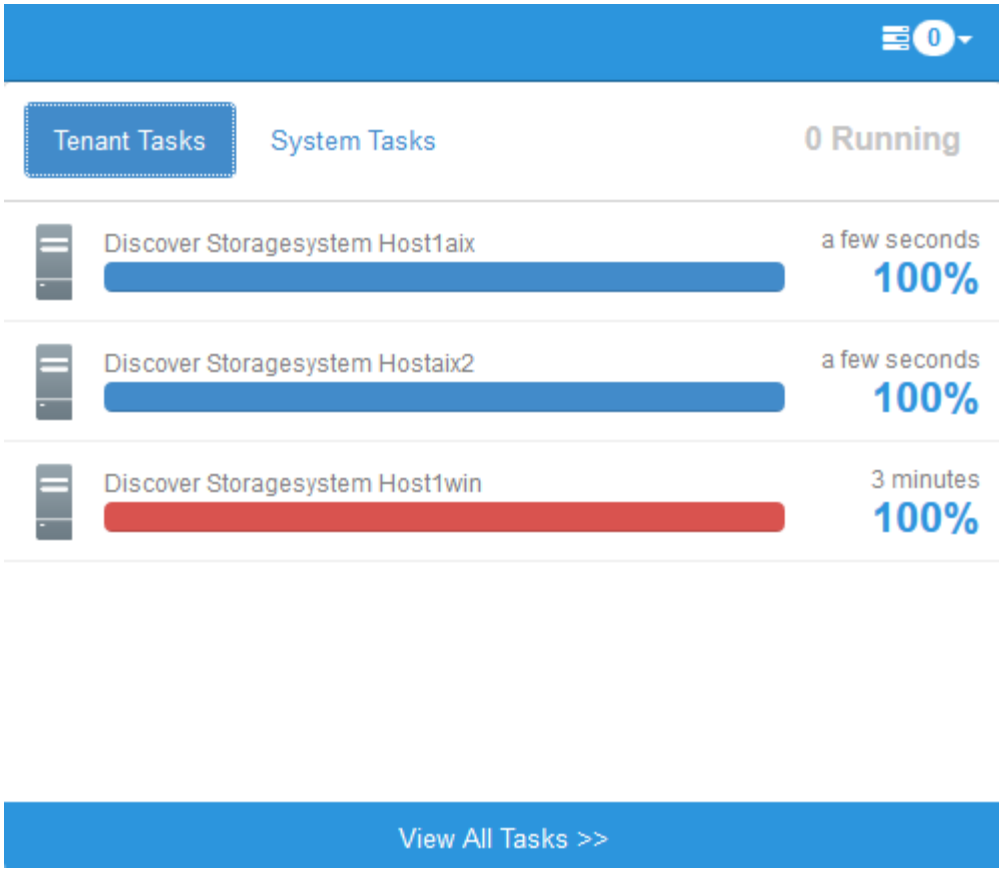
The Task popup is available on all ViPR Controller UI screens and displays the last five tasks for your tenant or system (if you are a system administrator) that ran during the last twelve hours.

You display the Task popup by clicking the icon that shows the count of running tasks in the top bar of the UI. In the figure below, the icon shows 0 running tasks, as all tasks have completed.

Note

If you see a double dash (--) as the number of tasks when performing a screen refresh or navigating to another screen, it indicates that ViPR Controller is recalculating the number of running tasks.

Figure 1 Task popup example



The Task popup has two tabs that can be displayed; one for tenant-level tasks and one for system tasks. The **Tenant Tasks** tab is displayed for all users. However, the **System Tasks** tab is only displayed for system administrators and security administrators.

The elasped time to complete the task appears for each task. A status bar also displays for each task that shows the percentage complete for the task:

- Blue = `task` completed successfully or is still in progress if percentage complete is less than 100%.
- Red = `task` completed with errors

Selecting **View All Tasks** displays the `Tasks` screen that provides access to the last 1000 tasks.

If you are a system administrator or security administrator, you can view the details of the `task` by selecting the `task` in the list.

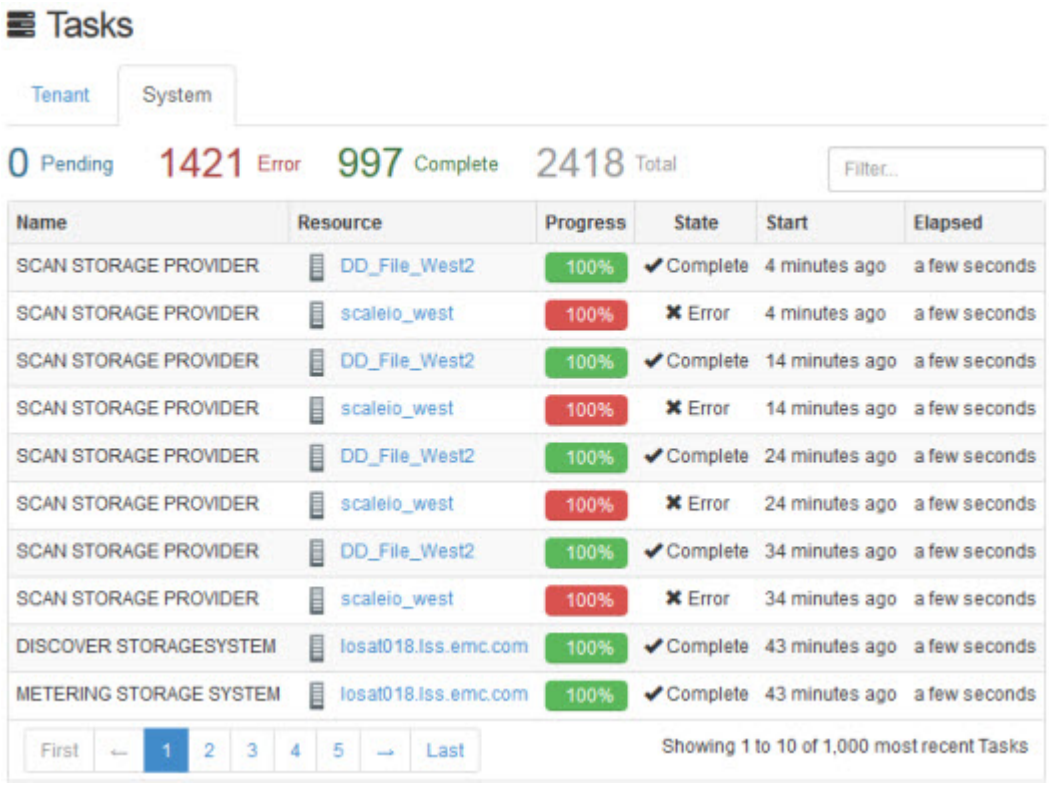
Tasks screen

Selecting **Resources** > **Tasks** opens the **Tasks** screen. The last 1000 tenant and system `tasks` are displayed.

The **Tasks** screen has two tabs, **Tenant** and **System** to display the corresponding types of `tasks`. Each tab includes the total number of `tasks` in ViPR Controller for that `task` type, as well as a count of the number of `tasks` that are pending, that completed but with an error, and that successfully completed.

There may be more than 1000 tenant or system tasks in ViPR Controller, but the UI shows only the last 1000 tasks for each type, which means you may not see all of the tasks you are searching for. For example, you search for tenant tasks in the pending state and while the count of pending tasks shows 14, you only see 6 because the other 8 tasks are older than the 1000 tenant tasks shown in the **Tasks** screen. However, you can use the ViPR Controller REST API to retrieve all tasks.

Figure 2 Resources > **Tasks** Screen



For each task, the following information displays:

- The name of the operation which created the task.
- The name of the resource for which the task was created. Clicking the resource name displays the screen to edit the resource.
- A progress bar that shows the percentage complete, and is color coded:
  - Green = task completed successfully
  - Red = task encountered an error
- The state of the task
- How long ago the task was started
- The elapsed time to complete the task.

If you are a system administrator or security administrator, you can view the details of the task by selecting the task in the list.

Task details

Selecting one of the tasks in the **Tasks** screen or the Task popup displays a screen showing the details of the selected task. Only system administrators and security

administrators can view the details of a system `task`. But any user that is a member of a tenant can view the details of `tasks` associated with that tenant.

The `task` details include the following `task` properties:

ID

ID of the `task`.

Operation ID

ID of the operation that created the `task`.

Name

The name of the operation that created the `task`.

Resource

The resource for which the `task` was created.

State

The state of the `task`: Completed if the `task` completed successfully or Error if the `task` completed but with an error.

Description

The description of the operation that created the `task`.

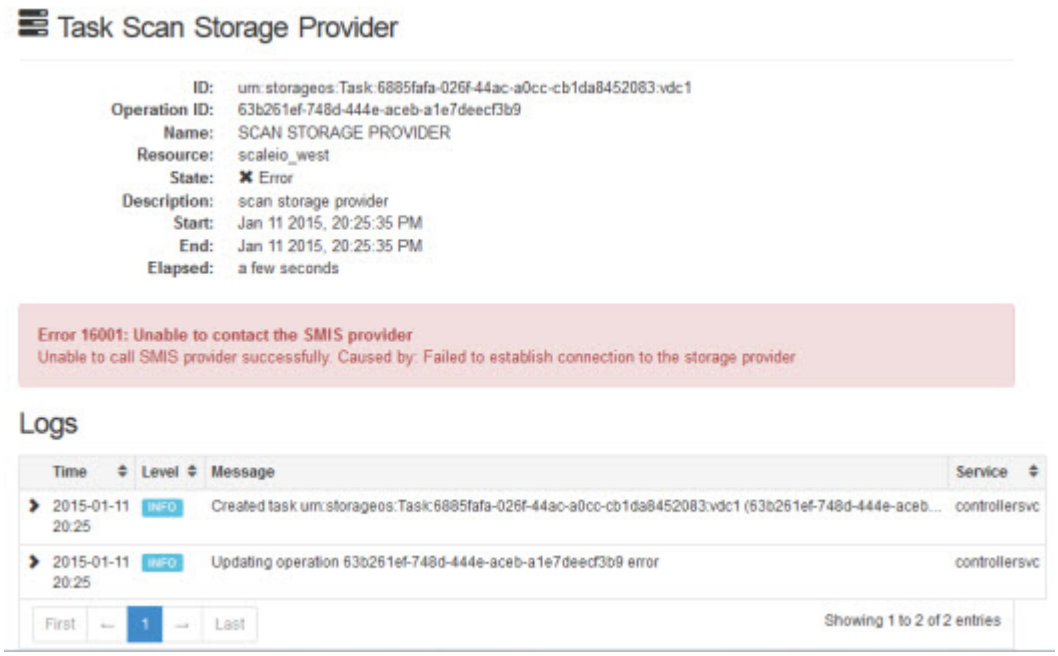
Start, End, and Elasped

The start and end times of the `tasks`, as well as the elapsed time for the `task`.

In addition, if the `task` completed with an error, the error number and message are included.

For `tasks` that are created by ordering a service from the service catalog, there is also a link to the order.

Figure 3 Details of a `task` that completed with an error



The task details also display the workflow steps (if applicable, such as when ordering a service from the service catalog) and the logs associated with each step of the task.

Change task-related configuration settings

Selecting the **Other** tab from **Settings** > **Configuration** allows you to change the task-related configuration settings.

There are two settings that you can change.

Table 13 Task-related configuration settings

Setting	Description
Task Cleaning Interval	Time interval in minutes between task cleaning operations. The default is 60 minutes. The minimum value is 60, anything lower is ignored and the default is used. After you make a change to this property, you must initiate a reboot of the ViPR Controller nodes. **Note** Rebooting the ViPR Controller nodes may disrupt ViPR Controller processes that are currently running.
Task Time To Live	Number of minutes to keep tasks once they have completed. The default is 10080 (7 days). The minimum value is 60 minutes, anything lower is ignored and the default is used.

Delete a task that is permanently in the pending state

Tasks can become permanently pending due to disruption between the ViPR Controller UI and the ViPR Controller nodes.

You can use the ViPR Controller REST API or CLI to remove any pending tasks due to a ViPR Controller node disruption.

First retrieve the task ID that is in the permanent pending state by doing the following:

1. Select **Resources** > **Tasks**. The **Tasks** screen is displayed.
2. Select the pending task to see the details of the task. The ID field displays the ID of the task. See Task details.

A system administrator can use the ViPR Controller REST API to send a POST /vdc/tasks/<task_id>/delete request to remove any tasks that are in a permanent pending state. See the *EMC ViPR Controller REST API Reference* on theViPR Controller Product Documentation Index .

The ViPR Controller CLI can also be used by sending a `viprcli system delete-task` command. See the *ViPR Controller CLI Reference Guide* on the ViPR Controller Product Documentation Index .

CHAPTER 7

Troubleshooting Error Messages

This chapter contains the following topics:

Troubleshooting ViPR Controller error messages

Review this information for common ViPR Controller error messages and their resolutions.

Troubleshooting common error messages

Table 14 Troubleshooting tips for common error messages

Error message	Description	Resolution/Workaround
`UI: Failed command to provision storage resource`	The provisioning operation failed because: • the network connection between ViPR and the storage array was lost • Solutions Enabler is offline	Do the following: • Check your network connections • Restart Solutions Enabler if it is offline.
`API: Error Message/Code = ...`	The provisioning operation failed because: • the network connection between ViPR and the storage array was lost • Solutions Enabler is offline	Do the following: • Check your network connections • Restart Solutions Enabler if it is offline.
`Logs: ConnectException: Connection refused: ... while sending command to the storage system`	The provisioning operation failed because: • the network connection between ViPR and the storage array was lost • Solutions Enabler is offline	Do the following: • Check your network connections • Restart Solutions Enabler if it is offline.
`The target namespace does not exist. (Invalid namespace root/brocade1)`	The SMI-S discovery for an array or switch failed because an array provider was added instead of a switch provider.	Delete the array provider and enter the IP address and port information for the correct switch provider.
`Config change failed could not find disks that satisfy our mirror/raid policy`	Creating a volume failed because the VMAX storage pool does not have a disk with a matching SymWin policy.	Add more disks to the storage pool.

Table 14 Troubleshooting tips for common error messages (continued)

Error message	Description	Resolution/Workaround
`Failed to get array system info (Authorization failed)`	The NetApp discovery failed because the user account does not have administrative privileges.	Add administrative privileges to the users account using the NetApp CLI.
`Storage Array: 'FOO' is not registered. It can not be edited`	Discovery failed because the storage array is not registered and can not be edited.	Register the storage array.
`Dashboard (if accessible) may show network or VIP ERROR (System Health tab -> Diagnostics)`	The system network virtual IP address, or a Controller VM IP address, is incorrect or invalid, resulting in the user being unable to login after deployment and all management and provisioning actions fail.	Redeploy the ViPR virtual appliance, or change the system IP addresses of the virtual appliance using **Edit Settings** in vCenter.
`Invalid Username or Password`	The username or password is incorrect. A username must have a domain suffix and passwords are case sensitive.	Retry your username and password.
`Manager authentication with LDAP server failed. Please contact your administrator if the problem persists`	The authentication provider is registered incorrectly, or the password of the user registering the authentication provider has expired or was changed.	Contact the system administrator to update the authentication provider with the correct manage domain name and valid password.
`[MiscStage:1] ERROR CassandraDaemon.java (line 164) Exception in thread Thread[MiscStage:1,5,main] java.lang.NullPointerException [GossipTasks:1] INFO Gossiper.java (line 768) InetAddress /`	A known issue for ViPR installations utilizing three nodes.	Ignore the error.

Table 14 Troubleshooting tips for common error messages (continued)

Error message	Description	Resolution/Workaround
`xx.xxx.xx.xxx is now dead`		
`svcuser@node1:/etc> ./diagtool sed: can't read /etc/ovf-env.properties: Permission denied`	A permissions error when the svc user executes the diagnostic tool (diagtool).	When executing the diagtool, the svc user should use the sudo command. For example: `sudo /etc/diagtool`
`Certificate error`	Unable to log in using a browser after an upgrade or property reconfiguration because of SSL certificate changes.	Do the following: • Clear your certificates, cookies, cache, and history, and then restart your browser. • If the error is received after restarting your browser, restart the system running the browser.
N/A	An SMI-S Provider can be registered twice.	Do not register SMI-S Providers more than once.
`No Storage Found`	The **Storage Pools** list is empty in a virtual storage pool, or provisioning failed when no storage was found. These errors are caused because the available networks are not assigned to the associated virtual storage array.	Do the following: 1. Ensure all required switches are discovered. 2. Ensure the necessary IP network is created, and the storage ports are assigned to it. 3. Ensure the network is assigned to the corresponding virtual storage array.
N/A	After deleting an SMI-S Provider managed storage array, the storage array is not rediscovered and is marked for permanent exclusion from ViPR.	To use a storage system not managed by ViPR: 1. De-register the storage array. 2. Register the storage array with ViPR.
`2013-08-29 12:32:18,242 [GossipStage:1] INFO Gossiper.java (line 754) InetAddress / a.b.c.d is now UP` `2013-08-29 12:32:55,971 [GossipTasks:1]`	• Multiple ViPR nodes have the same IP address • There is a high load on ViPR and the CPU or memory is almost exhausted • The network is unstable, the connection between nodes is turning off and on	Determine which of the problems is occurring. Depending on the problem, you may need to redeploy ViPR.

Table 14 Troubleshooting tips for common error messages (continued)

Error message	Description	Resolution/Workaround
`INFO Gossiper.java (line 768) InetAddress / a.b.c.d is now dead.`	• There are too many concurrent create and delete operations on the database • The disk space is exhausted or almost exhausted	
`Connection refused or authentication failed`	The Windows host was not added to ViPR after configuring WinRM.	Set the following properties in the WinRM configuration file for local user authentication: • winrm get winrm/config/service • winrm set winrm/config/service/auth @{Basic="true"} For domain authentication with Kerberos, • winrm get winrm/config/service • winrm set winrm/config/service/auth @{Kerberos="true"}
`Run date on each nodes, the time is not the same among nodes`	The ViPR node times are not synchronized. This can be caused by: • The NTPD service is down. • The /etc/ntp.conf file contains an invalid NTP server.	Do the following: 1. Run an NTP diagnostic test. 2. Resolve the problem based on the test results: • `UNCONFIGURED` — Configure the NTP setting in **System** > **Configuration** > **Network**. • `CONFIGURED UNREACHABLE` — Check the NTP settings and the status of the NTP server. • `CONFIGURED DEGRADED` — Check the NTP settings and the status of the NTP server.
`An error occurred while finding a suitable placement to handle the request (code: 1034). no IP networks found`	The host IP address is not set in the virtual storage array network settings.	Do the following: 1. In the virtual storage array settings, click **Edit Network**. 2. Type the file host IP address. 3. Click **OK**.

Table 14 Troubleshooting tips for common error messages (continued)

Error message	Description	Resolution/Workaround
The vSphere HA agent on host 'hostname' failed to quiesce file activity on datastore '/vmfs/volumes/[id]'. To proceed with the operation to unmount or remove a datastore, ensure that the datastore is accessible, the host is reachable and its vSphere HA agent is running.	The vSphere HA agent failed to unmount or remove a datastore. The datastore is not accessible or the vSphere HA agent is not running.	Download vCenter Server 5.1 Update 1a. You can download the latest version from the *VMware vCloud Suite Download Center*.
ViPR virtual appliance is not accessible or status remains at Degraded.	Invalid IPv4 network netmask or network gateway.	Shutdown the ViPR virtual appliance, and update the system IP address and netmask of the virtual appliance using **Edit Settings** in vCenter.
	Invalid IPv6 prefix length or network gateway.	Shutdown the ViPR virtual appliance, and update the system IP address and netmask of the virtual appliance using **Edit Settings** in vCenter.
Service Unavailable (6503) The service is currently unavailable because a connection failed to a core component. Please contact an administrator or try again later.	The ViPR UI was opened before all ViPR services were started.	Wait 5 minutes after ViPR controller deployment before running the UI.
ViPR virtual appliance remains in Syncing state	Credentials for an account with insufficient privileges were used to download the img file during upgrade.	1. Use the ViPR CLI to check the virtual appliance state. Make sure current version is still 1.0.0.7.1065 (V1.0) or whatever the pre-upgrade version should be, and the CLUSTER_STATE is

Table 14 Troubleshooting tips for common error messages (continued)

Error message	Description	Resolution/Workaround
		SYNCING. `# ./viprcli system get-cluster-state` 2. Using remove-image command with force flag (-f), remove the image that failed to download: `#./viprcli system remove-image -f vipr-1.0.0.8.103` 3. At this point the ViPR virtual appliance should return to Stable, and you should be able to upgrade after supplying credentials with correct permissions.
`Error 999 (http: 500): An unexpected error occurred, please check the ViPR logs for more information.`	A user attempts to create a bucket in the ViPR user interface although no datastores are in the services virtual pool, resulting in a failed operation.	Before creating a bucket, ensure the services virtual pool providing the storage for the bucket contains at least one datastore.
`Error 16000: Error occurred running an SMIS command. The job has failed: string ErrorDescription = "Volume Delete failed: C:ERROR_CLASS_SOFTWARE F:ERROR_FAMILY_FAILED R:1000086 L:2 C:ERROR_CLASS_SOFTWARE F:ERROR_FAMILY_FAILED R:1000086 Failed to acquire the requested lock : \"Unable to write-protect selected device \" : 2 : 2550 : \"Unable to`	Unable to delete a volume on a VMAX storage array.	The error message indicates there is a lock on the volume because another user is accessing it. Wait and perform the delete operation again once no other users are accessing the volume.

Table 14 Troubleshooting tips for common error messages (continued)

Error message	Description	Resolution/Workaround
acquire the Symmetrix device lock\" @ [1] com.emc.cmp.osls.se.osl.Device.StorDeviceDelete(): 150 [0] com.emc.cmp.osls.se.array.job.JOB_VolDelete.run(): 136 ";; Rollback error: The job has failed: string ErrorDescription = "Volume Delete failed: C:ERROR_CLASS_SOFTWARE F:ERROR_FAMILY_FAILED R:1000086 L:2 C:ERROR_CLASS_SOFTWARE F:ERROR_FAMILY_FAILED R:1000086 Failed to acquire the requested lock : \"Unable to write-protect selected device \" : 2 : 2550 : \"Unable to acquire the Symmetrix device lock\" @ [1] com.emc.cmp.osls.se.osl.Device.StorDeviceDelete(): 150 [0] com.emc.cmp.osls.se.array.job.JOB_VolDelete.run(): 136 ";		
ERROR Error 40009 (http: 400): "Invalid bucket	The bucket name contains invalid characters.	Rename the bucket using valid characters.

Table 14 Troubleshooting tips for common error messages (continued)

Error message	Description	Resolution/Workaround
name". Invalid bucket Name test this com.emc.vipr.client.exceptions.ServiceErrorException: Error 40009 (http: 400): "Invalid bucket name".		
ERROR HDFS service failed java.io.IOException: ClientApi failed to initialize, status=ERROR_INTERNAL HDFS service failed java.io.IOException: ClientApi failed to initialize, status=ERROR_INTERNAL	After initial deployment of ViPR, errors appear when switching to LOG view.	This error occurs when the HDFS service starts up faster than the services. Ignore the error.
createExportMask failed - maskName: urn:storageos:ExportMask:d101e3a5-146b-4a26-916e-f3bc5112a62c:vdc1 WBEMException: CIM_ERR_FAILED (A general error occurred that is not covered by a more specific error code. (com.emc.cmp.osls.se.osl.Masking.StorEndptGroupCreate():1872 C:ERROR_CLASS_SOFTWARE F:ERROR_FAMILY_FA	A duplicate network was discovered by ViPR and caused ViPR to reuse the same ports to recreate the initiator groups.	Remove the physical assets from the masking view, and then add the physical assets back to the masking view.

Table 14 Troubleshooting tips for common error messages (continued)

Error message	Description	Resolution/Workaround
`ILED R:1000124 L:2 C:ERROR_CLASS_SOFTWARE F:ERROR_FAMILY_FAILED R:1000124 The specified WWN is already in use : "StorEndptGroupCreate failed" : 2 : 3568 : "The specified WWN is already in use"))`		
`Host operation failed: Host <ESX/ESXi host> not reachable in state UNREACHABLE - Ensure host is powered on and responsive. Can be caused by intermittent or temporary connectivity issue thus retry`	During the VCE Vblock System Service, Provision Cluster operation, ViPR: 1. Creates the ESX hosts. 2. Creates the cluster in vCenter. During the `create the cluster in vCenter` operation, ViPR adds the newly created ESX hosts to the vCenter cluster. When ViPR attempts to add the ESX hosts to the vCenter cluster before one or more of the ESX hosts have been started, the `Host not reachable` error occurs because the hosts have not completely rebooted and are not ready to be added to the cluster until they have been started.	To resolve the issue, use the **Update vCenter Cluster** service from the **ViPR Service Catalog** to update the vCenter cluster with the newly created hosts. Optionally, to avoid the error during future operations, increase the ViPR default vCenter host operation timeout value. To increase the timeout value: 1. Get a list of all configuration properties from the ViPR REST API. GET on https://<ViPR Host>:4443/config/properties 2. 2. Change the property for vCenter host operation timeout. PUT to https://<ViPR Host>:4443/config/properties Allowed values, specified in seconds, are: 60, 150, 300, 450, 600, 750, 900, 1800

Table 14 Troubleshooting tips for common error messages (continued)

Error message	Description	Resolution/Workaround

		Note
		Default value is 450 seconds (7.5 minutes). For example:
		`<property_update>`
		`<properties>`
		`<entry>`
		`<key>vcenter_host_operation_timeout</key>`
		`<value>900</value>`
		`</entry>`
		`</properties>`
		`</property_update>`

`Error 12025: Export operation failed due to existence of non FAST volumes in storage group.. While attempting to export a FAST volume, an existing Storage Group PRGDC_2 was found on the array with non-FAST volumes in it. Adding FAST volumes to this Storage Group is not permissible.`	Creating a block volume on a virtual pool with a FAST VP policy, failed.	Create two cascaded storage groups: • FAST VP volumes • non-FAST VP volumes **Note** This solution is an offline operation for VMAX w5876 code, if the storage group to be reconstructed is part of a masking view.
`Error 1013 (http: 400): Bad request body. Cannot change the virtual pool pathsPerInitiator parameter for ExportGroup rdsan04.admin.nbsnet.co.uk ExportMask rdsan04adminnbsnetcouk.`	Moving volumes from one virtual pool to another fails if there is more than one target per initiator.	This operation is not supported.

Troubleshooting Active Directory and LDAP

Table 15 Troubleshooting tips for Active Directory and LDAP

Symptom	Cause	Resolution/Workaround
Access forbidden: Authentication required, and log contains `ERROR CustomAuthenticationManager.java (line 99) Unsupported credentials admin \adc34103`	Invalid format of username	Match the username with the searchfilter used. For example: userName=%u means a username of the format foo@bar.com.
Search failed while trying to find user in ldap tree	User not found because user name does not exist within the searchbase.	Be sure you have specified the searchbase at the correct location in the tree.
	User not found because user name types do not match the filter.	Be sure you are using %u versus %U properly to match complete versus local part of name.
	There is more than one match, based on the filter.	Check the value of the search filter.
Bind problems when adding a new authentication provider	Special characters exist in the managerDN name.	To specify the managerDN value, copy the contents of the user's distinguishedName value from Active Directory Users and Computers, Properties, Attribute Editor. That value will have the proper escape characters.
Authentication issue and log contains: `LDAP: error code 49 - 80090308: LdapErr: DSID-0Cxxxxxx, comment: AcceptSecurityContext error, data xxx, vece`	*xxx* is an Active Directory error code.	Refer to Active Directory documentation for the error code.

Troubleshooting administrator tasks

Table 16 Troubleshooting tips for administrator tasks

Symptom	Resolution/Workaround
No matching storage pools displayed when creating a virtual pool for IP connected file storage.	Ensure a file array has been added to a network in the virtual array.

Table 16 Troubleshooting tips for administrator tasks (continued)

Symptom	Resolution/Workaround
No IP network found to satisfy user request.	If a user is attaching provisioned storage to an IP-connected host, the host IP address or hostname must be added to the IP network.
MultiVolumeConsistency is set to true but no consistency group is provided.	If consistency groups are enabled on a virtual host, a resource is not created unless a user selects a consistency group to add it to.
No volumes are displayed when a user attempts to create a snapshot.	The virtual storage pool must have the maximum number of snapshots set to at least 1.
RAID groups created with unbound RAID levels cannot be used in ViPR because the capacity provider is reporting 0 free capacity.	Do the following: 1. Create a RAID group with unbound RAID levels. 2. Create a small volume on the RAID group.
Unable to login when IPv6 prefix is set to the wrong value.	Update the system settings of the ViPR virtual appliance using **Edit Settings** in vCenter.