

EMC ViPR Controller

Version 2.3

User Interface Virtual Data Center Configuration Guide

302-002-069

REV 02

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

Published July, 2015

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

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

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

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

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

CONTENTS

Figures		5
Chapter 1	Virtual Data Center Configuration Overview	7
Chapter 2	Adding and Configuring Physical Assets in VDC	9
	Adding storage to ViPR Controller	10
	Configuring storage systems added to ViPR Controller.....	11
	Network configuration for storage systems.....	11
	Deregister or delete a storage system from ViPR Controller.....	12
	Define the storage system resource allocation limit.....	12
	Deregister storage pools.....	13
	Set the storage pool utilization limits.....	13
	Deregister storage ports.....	14
	Hitachi Data Systems Host Mode and Host Mode options.....	14
	Configuring multipathing for Third-Party Block (OpenStack) storage systems	15
	Configuration requirements.....	15
	Create a storage port using the ViPR Controller UI.....	15
	Create a storage port using the ViPR Controller CLI.....	16
	Discover storage ports dynamically.....	16
	Data protection configuration for storage systems.....	17
	Add data protection systems to ViPR Controller.....	18
	Add Fabric Managers (SAN switches) to ViPR Controller overview.....	18
	Adding a switch to ViPR Controller.....	18
	Add a Vblock compute system to ViPR Controller.....	19
	Deregister UCS blades.....	20
	Add compute images to ViPR Controller.....	20
	Adding and configuring hosts overview	21
	Add undiscoverable hosts to ViPR Controller.....	21
	Add discoverable hosts to ViPR Controller.....	21
	Host initiator and host port configuration.....	22
	Add a host to a cluster.....	23
	Host network configuration.....	24
	Replace host initiators after a storage volume is exported to a host	25
	Add vCenter to ViPR Controller.....	26
	ESX/ESXi initiator, and port configuration.....	27
	View ESX/ESXi Clusters.....	28
	ViPR Controller network configuration for vCenter.....	28
Chapter 3	Configuring Networks in ViPR Controller	29
	Configuring ViPR Controller networks overview.....	30
	Deregistering fabrics or VSANs from ViPR Controller networks.....	30
	Assigning storage ports and host ports in the ViPR Controller SAN networks.....	31
	Configuring IP, and iSCSI networks.....	31

Chapter 4	Creating and Configuring Virtual Assets in VDC	33
	Creating a virtual array using storage systems.....	34
	Creating a virtual array using storage ports.....	34
	Adding Fibre Channel networks in the virtual array.....	35
	Adding the IP networks in a virtual array.....	35
	Creating block virtual pools.....	36
	Creating file virtual pools.....	41
	Creating a compute virtual pool.....	42
	Set up the VDC for a tenant.....	44
	Set up virtual arrays and virtual pools for a ViPR tenant.....	44

FIGURES

1	Applying virtual array tenant restriction	45
2	Applying virtual pool tenant restriction.....	46

FIGURES

CHAPTER 1

Virtual Data Center Configuration Overview

After EMC ViPR Controller installation, ViPR Controller System Administrators and Tenant Administrators can use the ViPR Controller UI or the ViPR Controller REST API 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 VDC using the ViPR Controller REST API, see the *ViPR Controller REST API Virtual Data Center Configuration Guide*.

Access both documents from the [ViPR Controller Product Documentation Index](#) .

CHAPTER 2

Adding and Configuring Physical Assets in VDC

This chapter contains the following topics:

- [Adding storage to ViPR Controller](#) 10
- [Configuring storage systems added to ViPR Controller](#)..... 11
- [Configuring multipathing for Third-Party Block \(OpenStack\) storage systems](#)..... 15
- [Data protection configuration for storage systems](#)..... 17
- [Add Fabric Managers \(SAN switches\) to ViPR Controller overview](#)..... 18
- [Add a Vblock compute system to ViPR Controller](#)..... 19
- [Add compute images to ViPR Controller](#)..... 20
- [Adding and configuring hosts overview](#) 21
- [Add vCenter to ViPR Controller](#)..... 26

Adding 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

Procedure

1. Log into the ViPR Controller UI with System Administrator privileges.

2. Select **Physical Assets > Storage Systems**

Block storage systems can also be added to ViPR Controller from the **Physical Assets > Storage Providers** page.

3. Click **Add**.

4. Select the storage system or storage provider type.

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.

5. Type the storage system name.

6. Type the host IP address.

- For ScaleIO, type the primary MDM host IP address.
- 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.

7. If adding block storage, enable if SSL will be used.

SSL is disabled for ScaleIO.

8. Leave the default or enter the port.

For ScaleIO, enter the port used to SSH into the primary MDM host.

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.
- For Block Storage Powered by ScaleIO enter the user that can SSH into the MDM host.

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 Block Storage Powered by ScaleIO,

- a. Type the **MDM User** and **MDM Password** with a user that can issue the ScaleIO CLI login.
- b. Type the **Element Manager URL**.

The format must be: `https://<element_manager_FQDN>/resources/dashboard.jnlp?host=<ip_address>&username=<admin_username>`

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 ScaleIO, ViPR Controller automatically creates storage ports, hosts, host initiators, and a network for the ScaleIO. These can not be edited. For additional information on how ViPR Controller uses the ScaleIO components to create the required ViPR Controller objects, see *ViPR Controller Integration of ScaleIO*, which is available from the [ViPR Controller Product Documentation Index](#) .

Configuring storage systems added to ViPR Controller

After a storage system has been 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 Assets**, **Fabric Manager**, and **Networks**.

Fibre Channel

Add the corresponding SAN Switch from the ViPR Controller UI **Physical Assets** , **Fabric Manager** page. For specific steps see: [Add Fabric Managers \(SAN switches\) to ViPR Controller on page 18](#)

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 on page 29](#).

Deregister or delete a storage system from ViPR Controller

Deregister a storage system to keep the storage system in ViPR, while not allowing 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 will remain under ViPR Controller management, but no more of the storage system resources will be used by ViPR Controller.

Procedure

1. From the ViPR Controller UI, select **Physical Assets > Storage Systems**.
2. Select the box in the storage system row.
3. Click **Deregister** to keep the storage system in ViPR Controller, and make it unavailable to use as a ViPR Controller resource or,
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, which define the amount of storage in the storage system that is available for use by ViPR Controller.

Procedure

1. Select **Physical Assets > 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 Controller for 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 Assets > 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 Assets > 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**.

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 Assets > 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 and Host Mode options

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

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

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

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 Assets > 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 Assets** > **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*, 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
wnn_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 Assets > Data Protection** page.

For further information:

- To add RecoverPoint to ViPR Controller see: [Add data protection systems to ViPR Controller on page 18](#).
- About the RecoverPoint configurations supported by ViPR Controller see: *ViPR Controller Integration with RecoverPoint and VPLEX 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, Virtual Assets on page 33](#)
- About ViPR Controller support for SRDF see: *ViPR Controller Integration with VMAX and VNX Storage Systems User and Administration 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 Assets > 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 Assets > 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 Assets > Fabric Manager** page displays the switch and the **Physical Assets > 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 will take the switches directly connected to the storage port being zoned as the control point to add or remove zones.

Add a Vblock compute system to ViPR Controller

ViPR Controller System Administrators can learn the steps to add Vblock compute system (UCS) to the ViPR Controller physical assets.

Before you begin

Procedure

1. Go to the **Physical Assets > 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 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 credentials	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.

4. Click **Save**.

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

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 Assets > 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**.

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 have been registered to ViPR Controller. If ViPR Controller is used to provision ESX clusters, ViPR Controller can also be used to add the cluster to a vCenter datacenter that has been registered to ViPR Controller.

Before you begin

The ViPR Controller compute image server must have been deployed prior to adding the compute images to the ViPR Controller physical assets. For compute image deployment details see the: *ViPR Controller Installation, Upgrade, and Maintenance Guide*, which is available from the [ViPR Controller Product Documentation Index](#).

Procedure

1. Go to the **Physical Assets > 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.

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 Assets > 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 on page 23](#) 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 Assts > 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 on page 22](#).
- Add host initiators to hosts that were manually added to ViPR Controller without automatic discovery. Refer to [Add host initiators on page 23](#).
- Register the host initiators that were manually added to ViPR Controller. Refer to [Register host initiators on page 23](#).

Deregister host initiators

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

Before you begin

Only host initiators, currently not in use in a ViPR export, can be deregistered.

Procedure

1. Open the **Host Initiators** page.

- a. Select **Physical Assets > Hosts**.
- b. Locate the row for the host, and click the **Initiators** button 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

Host initiators must be manually added for hosts that are not automatically discovered by ViPR.

Procedure

1. Open the **Host Initiators** page
 - a. Select **Physical Assets > 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, they must be registered before they are available for use in ViPR service operations.

Registering host initiators

Host initiators manually added to ViPR or host initiators previously unregistered in ViPR, must be registered to be used in a service.

Procedure

1. Open the **Host Initiators** page.
 - a. Select **Physical Assets > Hosts**.
 - b. Locate the row for the host, and click the **Initiators** button 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.

For Windows hosts:

- When a Windows host is added to ViPR Controller with discovery enabled, ViPR Controller identifies 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 can be managed and edited as a ViPR Controller cluster. Changes made to the Windows cluster from ViPR Controller will only be made in the ViPR Controller environment, and will not be 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 Assets > 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.

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 on page 31](#).

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 on page 31](#).

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 iSCSI networks](#).

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, which was added to ViPR Controller as discoverable, you can, add, remove, or replace a host initiator used by ViPR Controller for an export operation directly on the host using an application other than ViPR Controller.

If the host has only one HBA card with a path setting of 121 in ViPR Controller, you must change this setting in the virtual pool to 241 and then perform these steps:

Procedure

1. Add the new HBA in the host.
2. Discover the Fibre Channel network:
 - a. Go to **Physical Assets > Fabric Managers** to select the fabric manager on which the network between the host and the storage is configured.
 - b. Click **Rediscover**.
3. Rediscover the host and verify that the new initiator is in the export group.
4. Remove the HBA card to be replaced.
5. Rediscover the host again.
6. If the host has two HBA cards with a path setting of 241 in ViPR Controller, replace one of the cards directly and then do the following:
 - a. Discover the Fibre Channel network by going to **Physical Assets > Fabric Managers** to select the fabric manager on which the network between the host and the storage is configured.
 - b. Click **Rediscover**.
 - c. Rediscover the host and verify that the new initiator replaced the old initiator in the export group.

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 Assets > 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 on page 23](#)
 3. [Register the host initiator in ViPR Controller. on page 23](#)
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 vCenter to ViPR Controller

Tenant Administrators can 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.

Procedure

1. Select **Physical Assets** › **vCenters**.
2. Click **Add**.
3. Enter a vCenter Server name.
4. Add the host or IP address.
5. Add the port used for communication between the ViPR Controller and the vCenter Server.
6. Enter the credentials for an account that has administrator privileges.
7. 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.

8. Click **Save**.

ESX/ESXi initiator, and port configuration

Once the vCenter has been added to ViPR, configure the ESX/ESXi host initiators, or ports as required.

- Deregister host initiators to make the host initiators unavailable for use in a ViPR service. Refer to [Deregister host initiators on page 22](#).
- For IP connected hosts, [Add the ESX/ESXi ports to the IP Network on page 27](#).

Deregister host initiators

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

Before you begin

Only host initiators, currently not in use in a ViPR export, can be deregistered.

Procedure

1. Open the **Host Initiators** page.
 - a. Select **Physical Assets > Hosts**.
 - b. Locate the row for the host, and click the **Initiators** button 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, the ports must be added 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 that will be used for file system exports to an ESX/ESXi cluster.

Procedure

1. Select **Physical Assets 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:
 - 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 the discovered ports.
4. Enter or select the host ports to use in the IP network.
5. Click **Save**.

View ESX/ESXi Clusters

ESX/ESXi clusters can be viewed **Physical Assets > Clusters** page.

Before you begin

ESX/ESXi clusters are automatically discovered with vCenter. Hosts cannot be added or removed from ESX/ESXi clusters from ViPR.

Procedure

1. Select **Physical Assets > Clusters**.
2. If in a multi-tenancy environment, select the **Tenant**.
3. Locate the cluster that will 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.

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 networks on page 31](#).

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 iSCSI networks](#).

CHAPTER 3

Configuring Networks in ViPR Controller

This chapter contains the following topics:

- [Configuring ViPR Controller networks overview](#) 30

Configuring ViPR Controller networks overview

ViPR Controller System Administrators can create and configure the networks in the ViPR Controller before creating virtual arrays, or the networks can be created and configured while creating or configuring a virtual array.

For information to create and configure networks in the virtual array see: [Adding Fibre Channel networks in the virtual array on page 35](#), or [Adding the IP networks in a virtual array on page 35](#).

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 Assets, 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. on page 30](#)
To exclude the network from being used as a resource in a ViPR Controller service.
- [Assigning storage ports and host ports to the ViPR Controller networks. on page 31](#)
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.

IP networks

You 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.

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 on page 31](#).

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 on page 31](#).

Deregistering fabrics or VSANs from ViPR Controller networks

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

You can deregister but not delete networks from ViPR Controller.

Procedure

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

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 Assets, 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**.

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.

Procedure

1. Go to the **Physical Assets** › **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 the list of added host ports.

To manually add ports, click **Add › Add Ports** to enter the storage ports manually.

6. Click **Save**.

CHAPTER 4

Creating and Configuring Virtual Assets in VDC

This chapter contains the following topics:

- [Creating a virtual array using storage systems](#)..... 34
- [Creating a virtual array using storage ports](#)..... 34
- [Adding Fibre Channel networks in the virtual array](#)..... 35
- [Adding the IP networks in a virtual array](#)..... 35
- [Creating block virtual pools](#)..... 36
- [Creating file virtual pools](#).....41
- [Creating a compute virtual pool](#).....42
- [Set up the VDC for a tenant](#).....44

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 Assets** › **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. on page 35](#)
 - [Add and configure the networks for file storage in a virtual array. on page 35](#)
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 Assets** › **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 the 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, 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.

Before you begin

Procedure

1. Go to **Virtual Assets > 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 *How Storage Pools are Selected for Provisioning* article, which is available on 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 the **Virtual Asset > 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, make sure its 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.

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	<p>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.</p> <hr/> <p>Note</p> <p>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.</p>
Protocols	<p>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.</p>
Drive Type	<p>The drive type supported by the physical storage pools. The value of NONE allows any drive type.</p>
System Type	<p>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.</p>
Thin Volume Preallocation	<p>If you selected thin provisioning, specify the percentage of the physical storage to initially allocate to a volume.</p>
Multi-Volume Consistency	<p>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.</p>
Expandable	<p>When enabled:</p> <ul style="list-style-type: none"> • Volumes are expanded non-disruptively. <hr/> <p>Note</p> <p>This can cause a decrease in performance.</p> <hr/> <ul style="list-style-type: none"> • Native continuous copies are not supported. <p>When disabled, storage is selected based on performance over expandability.</p>

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

Parameter	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.
	<ul style="list-style-type: none"> • 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.

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

Option	Description
None	Uses both VPLEX local and VPLEX distributed volumes that match the other virtual pool settings in the virtual pool.
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: <ul style="list-style-type: none"> • 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

9. 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: <ul style="list-style-type: none"> • None • EMC Recoverpoint <ul style="list-style-type: none"> ▪ 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. <ul style="list-style-type: none"> 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, <ul style="list-style-type: none"> 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.

Option	Description
	<p>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.</p> <hr/> <p>Note</p> <p>The virtual array chosen for the journal volume must provide storage on the same site as the corresponding RecoverPoint copy volume.</p> <hr/> <ul style="list-style-type: none"> ▪ If you selected VPLEX Distributed for High Availability, select RecoverPoint Advanced Settings, and optionally, <ul style="list-style-type: none"> 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 <ul style="list-style-type: none"> ▪ 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 or Asynchronous. ▪ Select Add Copy to add an SRDF copy, specifying the destination virtual array, and optionally a virtual pool. • VPLEX Local • VPLEX Distributed <ul style="list-style-type: none"> ▪ 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.

10.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.

11.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.

12.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

For information on how ViPR Controller performs the selection process for provisioning, see the *How Storage Pools are Selected for Provisioning* article, which is available on 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 the **Virtual Assest** > **File Virtual Pools** page.
2. Click **Add** to add a virtual pool name.
3. Type the name and description for the virtual pool.

Since the virtual pool performs provisioning operations, make sure its 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.

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** to set these options:

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 and NFS. Only the protocols supported by the virtual array networks are listed. Note When configuring a VNX file virtual pool that uses CIFS protocol, there must be at least one CIFS server on any one of the physical data movers.
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.

Option	Description
	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.

7. Expand **Protection** to define the maximum number of local snapshots allowed for resources from this virtual pool.
To use the ViPR Controller Create Snapshot services, specify a value of at least 1.
8. 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.
9. 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.
10. 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 required compute resources from the selected compute virtual pool.

Before you begin

- Once a virtual pool has been used by ViPR Controller, 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.
- For a compute virtual pool, which is made up of UCS blades, to be used by ViPR Controller for provisioning, at least one service profile template must be selected in the compute virtual pool.
- Discuss with your UCS administrator which service profile template should be used by ViPR Controller to provision the Vblock system, and review the 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 Assets > Compute Virtual Pools** page.
2. Click **Add**.
3. Complete the following fields.

Option	Description
Name	Enter the name of the virtual pool.

Option	Description
Description	Optionally, enter a virtual pool description.
System Type	The type of compute system for example, Cisco UCS.
Virtual Arrays	<p>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.</p>
Access Control	Optionally, assign the tenants who will have access to the compute virtual pool.
Qualifiers	<p>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:</p> <ul style="list-style-type: none"> • 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	<p>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.</p> <p>If Manual was selected, chose the compute elements to include in the virtual pool.</p> <p>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.</p> <p>Compute elements that are not available in the Compute Virtual Pools have been used by ViPR Controller for a ViPR Controller operation.</p>

Option	Description
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 the 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 virtual arrays and virtual pools for a ViPR tenant

When setting up a tenant, a System Administrator can configure access to virtual arrays and virtual pools.

Before you begin

- You must have the System Administrator role in ViPR.

Prior to assigning a virtual array or virtual pool to one or more tenants, access the virtual array and virtual pool is available to all tenants. When you assign a virtual array or virtual pool to one or more tenants it will go from being unrestricted to being available only to the selected tenants. Tenants that could see the virtual pool prior to the assignment will no longer be able to do so.

For this reason restricting access to a specific tenant actually means assigning access to all of the tenants that you do want to allow access.

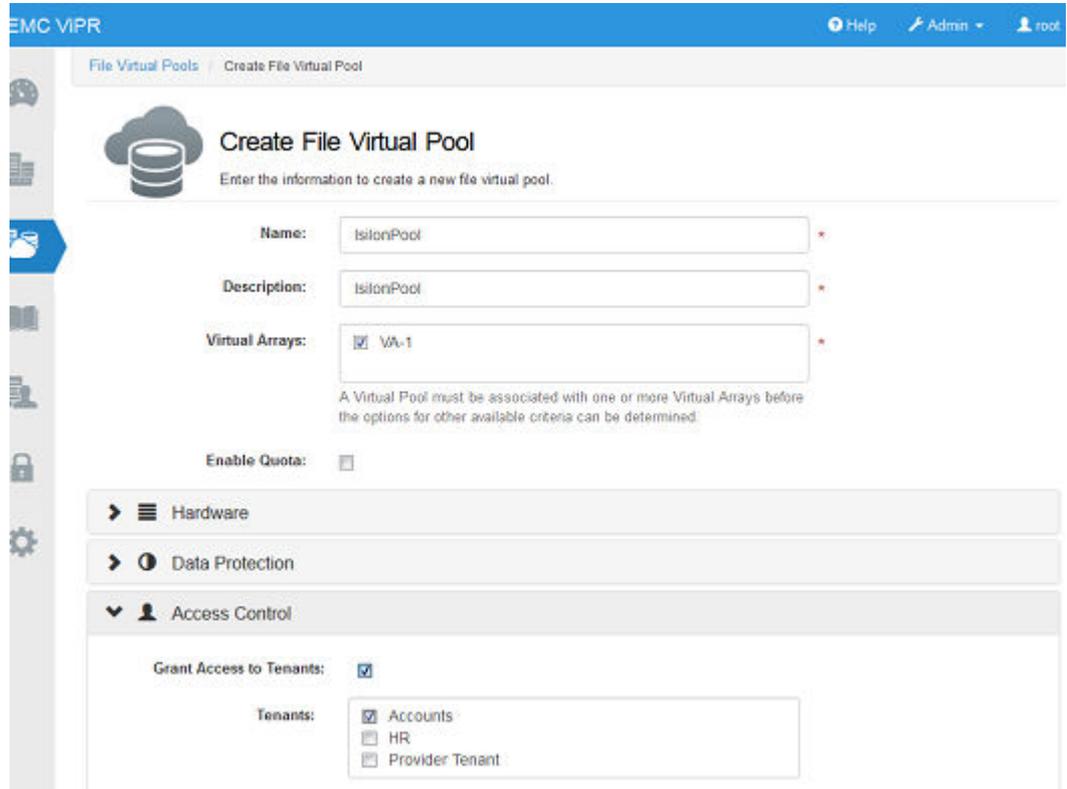
Procedure

1. Virtual array configuration. To select a virtual array and make it available to specific tenants:
 - a. At the ViPR UI, select **Virtual Assets > Virtual Arrays**.
 - b. Select the virtual array that you want to assign/restrict access to.
 - c. Check the Grant Access to Tenants box and choose the tenants that you want the virtual pool to be available to.

The Tenant Access panel on the Edit Virtual Array page is shown below.

- d. **Save** the virtual array.

Figure 1 Applying virtual array tenant restriction



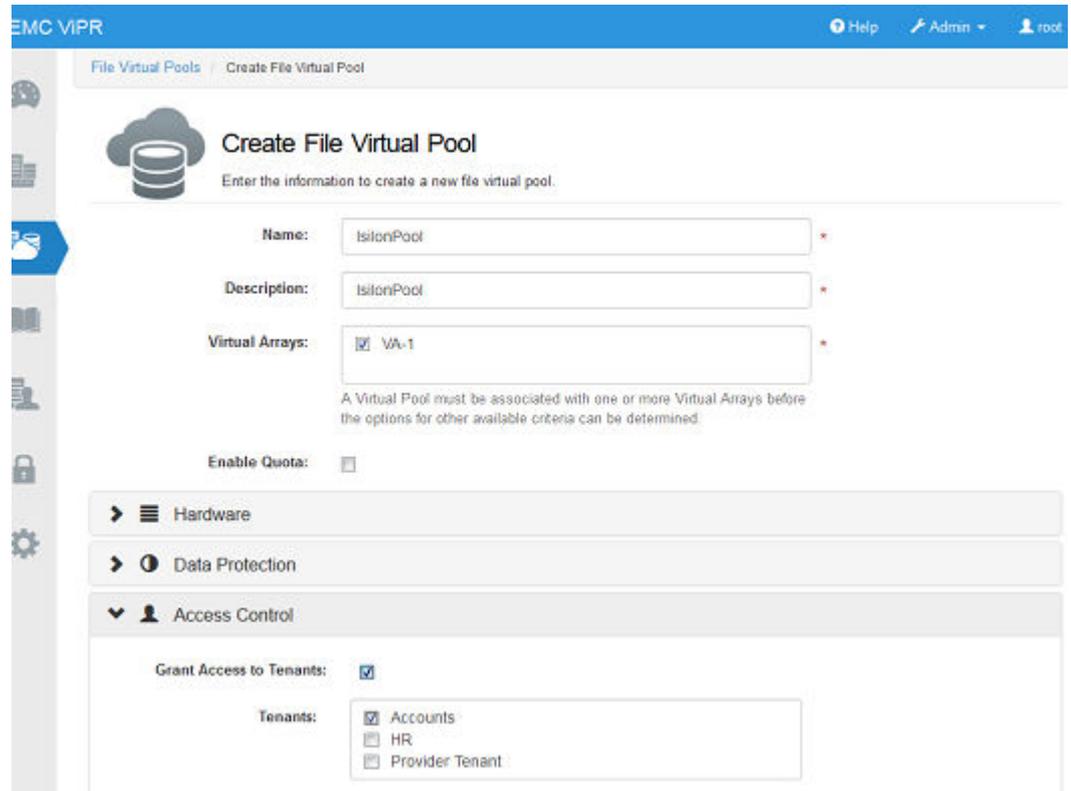
Users belonging to the specified tenants will have access to the virtual array.

2. Virtual pool configuration. To select a virtual pool and make it available to specific tenants:
 - a. At the ViPR UI, select **Virtual Assets > Block Virtual Pools** or **Virtual Assets > File Virtual Pools**.
 - b. Select the virtual pool that you want to assign/restrict access to.
 - c. Expand the Access Control Panel and check the Grant Access to Tenants box. Choose the tenants that you want the virtual array to be available to.

The Tenant Access panel on the Edit/Create File Virtual Pool page is shown below.

- d. **Save** the virtual pool.

Figure 2 Applying virtual pool tenant restriction



Users belonging to the specified tenants will have access to the virtual pool.