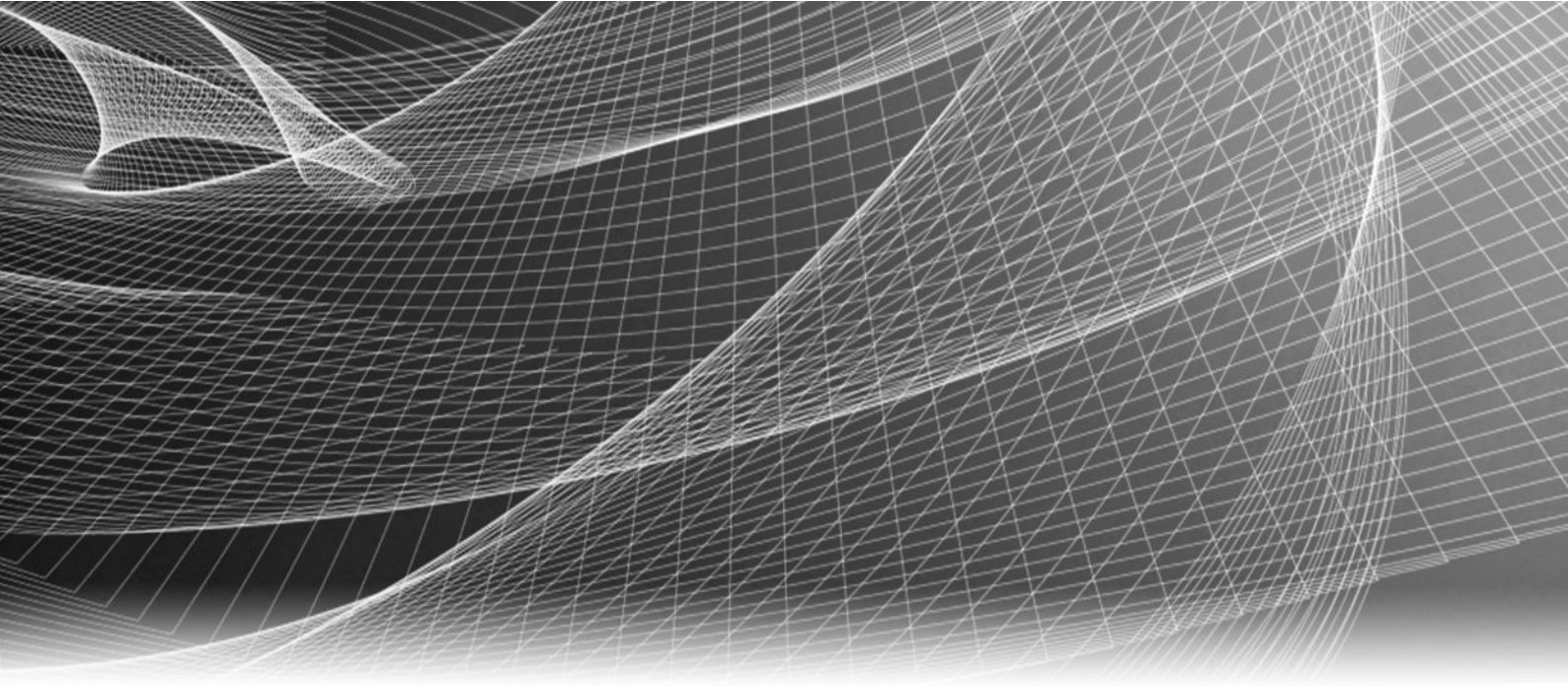


EMC® ViPR™

Version 1.1.0

Administrator Guide

302-000-480

02

EMC²

Published March, 2014

For the most up-to-date regulatory document for your product line, go to EMC Online Support (https://support.emc.com). For documentation on EMC Data Domain products, go to the EMC Data Domain Support Portal (https://my.datadomain.com).

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

CONTENTS

TABLES

FIGURES

CHAPTER 1

Introduction

This chapter contains the following topics:

Introduction to ViPR Administration

The *EMC ViPR Administrator Guide* describes the configuration and management of EMC® ViPR™ from the ViPR Admin and Self-Service UI (the UI), using the CLI, or using the API.

Most of the tasks that a ViPR administrator needs to perform can be accessed from the UI. Where an administration operation requires you to use the CLI or API, because it is not supported from the UI, the required steps using the CLI or API are described in this guide.

You can refer to the following publications for details of using the CLI and API:

- *EMC ViPR CLI Reference*
- *EMC ViPR REST API Reference*

The operations that you can perform depend on the administrator role to which you are assigned. Some roles apply across the ViPR virtual data center (VDC), others are specific to a tenant within the VDC.

You can find more information about roles and about the other main ViPR concepts in the *EMC ViPR Concepts Guide*. The access to the UI provided by each administrator role is described in Role assignment and UI access on page 31.

Admin user and features overview

The Admin view is aimed at ViPR administrators who are responsible for configuring ViPR in preparation for its use by self-service storage provisioning users, or from solutions and plugins which talk to ViPR using its API.

Configuration of ViPR from the UI enables the physical storage infrastructure to be hidden when performing storage provisioning operations, allowing the storage provider to be selected by the level of service it provides, rather than its physical array characteristics.

The ViPR UI exposes the most common storage use cases as services through the service catalog, and the Admin view allows configuration of the ViPR service catalog to control access to the services and to control their behavior. Access to the service catalog for storage provisioning users is from the User view.

Use cases which are not pre-defined in the service catalog can be developed using the ViPR API.

Controls bar

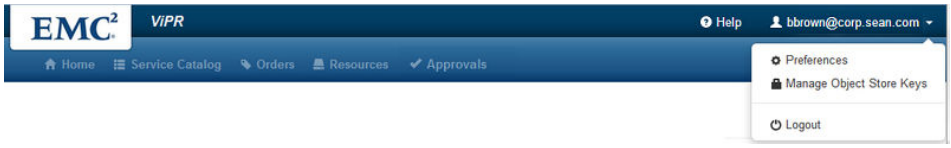
The UI provides a controls bar and a menu bar. The controls bar provides access to the following:

- User menu on page 12
- View selector on page 13
- Notifications area on page 13
- Online help selector on page 13

User menu

The **User** menu is a drop-down located at the top-right of the UI, as shown below. In this figure the logged in user does not have any administrator rights, so a view selector is not displayed.

Figure 1 User menu



The menu provides the following tabs:

Preferences

Provides access to the **User Preferences** panel which allows you to enable email notifications and to specify the email address to which notifications will be sent. Notifications tell you when an order you have submitted has been approved (or rejected) and when the order has been fulfilled.

Manage Object Store Keys

Provides access to the **Manage Object Store Keys** page which enables you to add and delete object store keys that will allow you to access ViPR object storage.

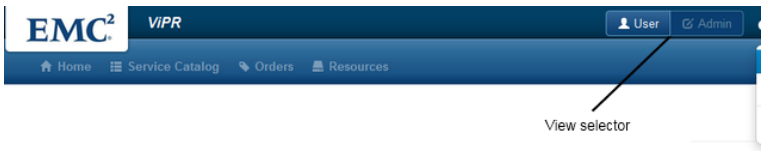
Logout

Enables you to log out from the UI.

View selector

If you are assigned to an administrator role in ViPR, you can switch between the **Admin** and **User** views using the view selector.

Figure 2 View selector

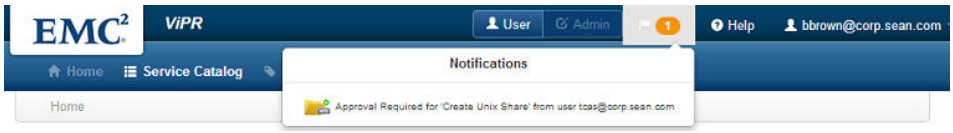


If you are a provisioning user and do not have administrator privileges, you will not see the view selector.

Notifications area

The notifications area is displayed if you are a Tenant Approver and can be expanded to show a list of outstanding approvals, as shown below.

Figure 3 Notifications area



Clicking on an approval notification opens the approvals page to allow the request to be approved. In addition, as a Tenant Approver, approval requests will be notified by email as long as the approval email address has been added by an administrator.

Online help selector

You can display context sensitive online help by clicking the question mark on the status bar. The help displayed will be appropriate to the page that is currently displayed.

Admin menus

The menus within the Admin view enable the configuration of the storage and compute infrastructure, and configuration of the service catalog. The menus are listed in the following table.

Table 1 Admin view menus

Home	Description	More Information
System	Enables a Security Administrator to specify system-wide configuration settings.	Configuration on page 20
	Enables a System Administrator to perform software and licensing upgrades, submit support requests, and view system monitoring information. Enables a System Auditor to view the audit logs.	Managing and monitoring the ViPR instance on page 118
Security	Enables a Security Administrator to configure an authentication provider and to assign roles to users.	Security on page 26
Tenant	Enables a Tenant Administrator to create projects and consistency groups and to configure approval settings.	Projects and consistency groups on page 104
	Provides access to the orders (both immediate and scheduled) that have been created by provisioning users and enables execution windows to be configured for the scheduling of orders.	Orders, order scheduling, and approvals on page 110
Physical Assets	Enables a System Administrator to configure the physical storage infrastructure assets. These comprise: storage systems, SMI-S providers, fabric managers and data protection system.	Physical asset management on page 43
	In addition, enables a Tenant Administrator to perform the configuration of host and vCenter storage consumers to which provisioned storage can be exported.	GUID-89F07F98-F143-44FC-94A1-64CE27612B99
Virtual Assets	Enables a System Administrator to perform the mapping of physical storage infrastructure to virtual storage arrays (referred to as virtual arrays), and for the physical storage pools that meet defined performance and protection criteria to be made available as a virtual storage pools (referred to as virtual pools).	Virtual asset management on page 61
Service Catalog	Provides access to the service catalog to enable a Tenant Administrator to configure it for access by provisioning users, and enables the behavior of individual services to be configured.	GUID-FFF0055B-41B3-4C9D-9A2A-3824A1F6C036
Data Services	Enables a System Administrator to configure ViPR object storage and initialize it by creating a data services virtual pool.	Data Services overview on page 82

The areas that are accessible to an administrator in the Admin view depend on the role assigned (Role assignment and UI access on page 31).

ViPR administration tasks

This guide supports the configuration tasks that ViPR administrators may need to perform through the lifetime ViPR and any administration tasks required to maintain the ViPR virtual application (vApp).

Configuration Tasks

The configuration of ViPR comprises the configuration of the ViPR vApp, the ViPR storage infrastructure, the compute infrastructure, and the service catalog. Many of these tasks need to be performed as part of the initial installation and configuration of ViPR, described in the *EMC VIPR Installation and Configuration Guide*, they will also be performed during the lifetime of ViPR as configuration changes are made. The configuration tasks are listed in the following table.

Table 2 Configuration tasks

Configuration task	Admin user	Description
Create Security Administrator	root	Root user can initialize the system by assigning roles.
Create System Administrator, Tenant Administrator and other roles	Security Administrator	Security Administrator can create roles required to perform vdc and tenant administration.
Configure Authentication Providers	Security Administrator	Configures the security domain so that AD/LDAP users can access ViPR.
Configure Notifications	Security Administrator	Configure SMTP server to enable notifications to be sent.
Add Physical Storage Assets	System Administrator	Add storage systems, SMI-S providers, fabric managers, and data protection systems.
Add Virtual Arrays	System Administrator	Configure array ports and initiators into a virtual storage array (virtual array).
Configure Virtual Pools	System Administrator	Make physical storage pools available as virtual storage pools (virtual pools).
Configure Data Services	System Administrator	Configure ViPR Data Services to provide object and/or HDFS storage capabilities
Ingest Block and File Volumes	System Administrator	Bring existing block volumes and file systems under VIPR management.
Create Tenant Administrator (and Project Administrator) roles	System Administrator	Create a Tenant Administrator who can perform all tenant tasks. Create Project Administrator if required.
Add Host/vCenter Assets	Tenant Administrator	Add any host and vCenter storage consumers to which provisioned storage will be exported.
Configure Windows Hosts	Tenant Administrator	If you have Windows hosts: configure Windows hosts to accept connections from ViPR. Add

Table 2 Configuration tasks (continued)

Configuration task	Admin user	Description
		Windows domains to enable ViPR to talk to any domain-connected Windows hosts.
Create Projects	Tenant Administrator/ Project Administrator	Create projects and assign users/groups to projects.
Create Consistency Groups	Tenant Administrator	Create consistency groups to enable snapshots to be managed.
Configure Service Catalog	Tenant Administrator	Configure the service catalog to show or hide categories from particular groups of users.
Configure Services	Tenant Administrator	Configure user/group access to services and configure the way in which individual services appear to end-users and the way in which they execute.
Configure Execution Windows	Tenant Administrator	Set up time windows in which services can execute.
Configure Approvals	Tenant Administrator	Specify the address to which a request to perform approval will be sent.

vApp Administration Tasks

The following administration tasks for the ViPR vApp are provided:

- Backup and restore of controller nodes on page 142

Accessing the ViPR UI

You can access the ViPR UI from your browser by specifying the address of the ViPR appliance.

Procedure

1. To access the UI, you need to enter the address of the ViPR appliance in your browser's address bar:

   https://*ViPR_virtual_ip*

2. Enter your username and password. It should be in the format **`user@domain.com`**.

   If you are unable to log in, contact your Tenant Administrator.

   All logged in users have access to the User view and you will initially be placed in the user Home page. If you have been assigned to any administrator roles, the Admin view will also be available.

3. You can log out from the Logout item located in the user menu at to right-hand corner of the UI, next to the identity of the logged in user.

Initial login and setup

On first login as the root user, you need to change the ViPR root and system passwords, set the ConnectEMC and email settings, and upload the ViPR license.

Before you begin

- Wait 5 minutes after controller deployment before following the steps in this procedure. This will give the required ViPR services time to start up.
- Be prepared to provide new passwords for the ViPR root and system accounts.
- You need the name of an SMTP server. If TLS/SSL encryption used, the SMTP server must have a valid CA certificate.
- You need access to the ViPR license file.

Procedure

1. Open https://*ViPR_virtual_ip* with a supported browser and log in as root.

   Initial password is ChangeMe.

   The *ViPR_virtual_IP* is the ViPR public virtual IP address, also known as the network.vip (the IPv4 address) or the network.vip6 (IPv6). Either value, or the corresponding FQDN, can be used for the URL.

2. Enter new passwords for the root and system accounts.

   The ViPR root account has all privileges that are needed for initial configuration; it is also the same as the root user on the Controller VMs. The system accounts (sysmonitor, svcuser, and proxyuser) are used internally by ViPR.

3. Select a transport option for ConnectEMC (FTPS (default), SMTP, or none) and enter an email address (user@domain) for the ConnectEMC Service notifications.

   If you select the SMTP transport option (required by the ViPR approval notification feature), you must specify an SMTP server under SMTP settings in the next step. "None" disables ConnectEMC on the ViPR virtual appliance.

4. Specify an SMTP server and port for notification emails, encryption type (TLS/SSL or not), a From address, and authentication type (login, plain, CRAM-MD5, or none).

   Optionally test the settings and supply a valid addressee. The test email will be from the From Address you specified and will have a subject of "Mail Settings Test".

   If TLS/SSL encryption used, the SMTP server must have a valid CA certificate.

5. **Finish.**

   ViPR services restart (this can take several minutes) and the UI opens to the License page.

6. Browse to and select the license file that was downloaded from the EMC license management web site and **Upload License**.

Results

At the end of this procedure you are logged in to the UI as root user, at **Admin** › **System** › **Dashboard**.

CHAPTER 2

Setting ViPR configuration parameters

This chapter contains the following topics:

Configuration

Use **Admin** › **System** › **Configuration** to modify system-wide settings including those related to networks, security, controller, upgrades, and ConnectEMC.

Setting network properties

You can modify the lists of DNS servers, NTP servers, data VM addresses, gateway and netmask settings that were originally set during ViPR deployment.

Before you begin

This operation requires the Security Administrator role in ViPR.

Keep in mind that any changes to these values will initiate a reboot when you click Save.

⚠WARNING

Do not use the vSphere Client to modify Controller vApp properties. The modifications will be saved in vCenter but they will have no effect on the ViPR appliance itself.

Procedure

1. Select **Admin** › **System** › **Configuration** › **Network**.
2. Enter values for the properties.

Attribute	Description
DNS servers	Two or three IP addresses (not FQDNs) for DNS servers, separated by commas. Reboot required.
NTP servers	Two or three IP addresses (not FQDNs) for NTP servers, separated by commas. Reboot required.
Data service IP addresses	List of IP addresses, or the subnet, reserved for the data service VMs. A list of addresses should be comma separated. Reboot required.
IPv4 default gateway	IPv4 IP address of the gateway for the data service VMs. Reboot required.
IPv6 default gateway	IPv6 IP address of the gateway for the data service VMs. Reboot required.
Network mask	The network netmask setting for the data service VMs. Reboot required.
IPv6 prefix length	IPv6 prefix length. Default is 64. Reboot required.

3. **Save**.

Setting security properties

You can change the firewall setting for the controller VMs and edit the authorized public SSH keys for the built-in local accounts root and svcuser.

Before you begin

This operation requires the Security Administrator role in ViPR.

Keep in mind that changes to Enable Firewall or SSL Certificate values will initiate a reboot when you click Save.

Procedure

1. Select **Admin** › **System** › **Configuration** › **Security**.
2. Enter values for the properties.

Attribute	Description
Enable firewall	Enabled by default. Disable the firewall only for troubleshooting, development, testing, and the like. Reboot required.
SSH Key (root)	Authorized public SSH keys for the 'root' account.
SSH Key (svcuser)	Authorized public SSH keys for the 'svcuser' account.

3. **Save**.

Setting controller properties

You can edit controller properties for metering and monitoring and for pool utilization and thin pool subscription.

Before you begin

This operation requires the Security Administrator role in ViPR.

Keep in mind that changes to the metering or monitoring values will initiate a reboot when you click **Save**.

Procedure

1. Select **Admin** › **System** › **Configuration** › **Controller**.
2. Enter values for the properties.

Property	Description
Enable Metering	Indicates whether metering is enabled. Reboot required.
Metering Interval	Number of seconds between metering operations. It is not recommended to change this value unless advised by your EMC customer service representative. Reboot required
Enable Monitoring	Indicates whether system monitoring is enabled. Reboot required.
Pool Utilization	Maximum percentage of storage pool utilization for provisioning operations.
Thin Pool Subscription	Maximum percentage of thin storage pool subscription for provisioning operations.

3. **Save**.

Setting discovery properties

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

Before you begin

This operation requires the Security Administrator role in ViPR.

Keep in mind that changes to any of these values will initiate a reboot when you click Save.

Procedure

1. Select **Admin** › **System** › **Configuration** › **Discovery**.
2. Enter values for the properties.

Attribute	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.
Storage systems	Number of seconds between discovery operations of storage systems. Reboot required.
Network systems	Number of seconds between discovery operations of switches (fabric managers). Reboot required.
Enable auto-scan	Indicates whether auto-scan of SMI-S providers is enabled. Reboot required.
Scan interval	Number of seconds between scan operations of SMI-S providers. Reboot required.

3. **Save**.

Setting ConnectEMC properties

You can edit the properties that ViPR uses to connect with ConnectEMC.

Before you begin

This operation requires the Security Administrator role in ViPR.

Keep in mind that changes to any of these values will initiate a reboot when you click Save.

Procedure

1. Select **Admin** › **System** › **Configuration** › **ConnectEMC**.
2. Enter values for the properties.

Attribute	Description
Encryption	Encrypt ConnectEMC Service data using RSA BSAFE. Reboot required.
Transport	List of acceptable transport options for ConnectEMC. Selecting "None" will disable the ConnectEMC service and no service events will be sent to EMC. Reboot required.
Hostname	ConnectEMC FTPS Hostname. Reboot required.
Notification email	Optional email address (user@domain) for the ConnectEMC Service notifications. Reboot required.

3. **Save**.

Setting email properties

You can change the email properties related to the SMTP server used for approval requests and for accessing ConnectEMC.

Before you begin

This operation requires the Security Administrator role in ViPR.

Keep in mind that changes to any of these values will initiate a reboot when you click Save.

Procedure

1. Select **Admin › System › Configuration › Email**.
2. Enter values for the properties.

Attribute	Description
SMTP server	SMTP server or relay for sending email (For ConnectEMC and approvals). Reboot required.
Port	Port on which the SMTP service on the SMTP server is listening for connections. "0" indicates the default SMTP port is used (25, or 465 if TLS/SSL is enabled). Reboot required.
Encryption	Use TLS/SSL for the SMTP server connections. Reboot required.
Authentication	Authentication type for connecting to the SMTP server. Reboot required.
Username	Username for authenticating with the SMTP server. Reboot required.
Password	Password for authenticating with the SMTP server. Reboot required.
From address	From email address for sending email messages (user@domain). Reboot required.

3. **Save**.

Setting upgrade properties

Sets the properties for accessing the ViPR upgrade repository.

Before you begin

This operation requires the Security Administrator role in ViPR.

Procedure

1. Select **Admin › System › Configuration › Upgrade**.
2. Enter values for the properties.

Attribute	Description
Repository URL	URL to the EMC upgrade repository. One value only. Default value is https://colu.emc.com/soap/rpc.
Proxy	HTTP/HTTPS proxy required to access the EMC upgrade repository. Leave empty if no proxy is required.

Attribute	Description
Username	Username for accessing the EMC upgrade repository.
Password	Password for accessing the EMC upgrade repository.
Check Frequency	Number of hours between checks for new upgrade versions.

3. **Save**.

Setting the VASA base URL

You can edit the ViPR instance URL that the VASA storage provider utilizes. By default the VASA provider utilizes the local ViPR node.

Before you begin

This operation requires the Security Administrator role in ViPR.

Keep in mind that this change will initiate a reboot when you click Save.

Procedure

1. Select **Admin** › **System** › **Configuration** › **Other**.
2. Enter a value for the ViPR instance to be used by the VASA storage provider.
3. **Save**.

CHAPTER 3

Configuring Users and Roles

This chapter contains the following topics:

Security

ViPR uses role-based security to provide administrators with access to appropriate system resources. The ViPR UI enables the Security Administrator to add an authentication provider and to assign users authenticated against that provider to ViPR roles.

Authentication providers

User authentication is done through an authentication provider added to ViPR.

Except for the special built-in administrative users (root, sysmonitor, svcuser, and proxyuser) there are no local users in ViPR. Users who can log in, and who are assigned roles or ACLs, must be found through an authentication provider added to ViPR.

Adding an authentication provider

You need to add at least one authentication provider to ViPR in order to perform operations using accounts other than the built-in administrative accounts.

Before you begin

This operation requires the Security Administrator role in ViPR. (The root user has this role.)

You need access to the authentication provider information listed in Authentication provider settings on page 26. Note especially the requirements for the Manager DN user.

Procedure

1. Select **Admin** › **Security** › **Authentication Providers**
2. **Add**.
3. Enter values for the attributes. Refer to Authentication provider settings on page 26.
4. **Save**.
5. To verify the configuration, add a user from the authentication provider at **Admin** › **Security** › **Role Assignments**, then try to log in as the new user.

Authentication provider settings

You need to provide certain information when adding or editing an authentication provider.

UI name	CLI name (Provider.cfg)	Description and requirements
Name	name	The name of the authentication provider. You can have multiple providers for different domains.
Type	mode	Active Directory or LDAP. In Provider.cfg (CLI), use ad or ldap.
Description	description	Free text description of the authentication provider.

UI name	CLI name (Provider.cfg)	Description and requirements
Domains	domains	Active Directory and LDAP allow administrators to organize objects of a network (such as users, computers, and devices) into a hierarchical collection of containers. Domains are a collection of administratively defined objects that share a common directory database, security policies, and trust relationships with other domains. In this way, each domain is an administrative boundary for objects. A single domain can span multiple physical locations or sites and can contain millions of objects. A typical entry in this field of the authentication provider would look like this: `mycompany.com`
Server URLs	url	ldap or ldaps (secure LDAP) with the domain controller IP address. Default port for ldap is 389 and ldaps is 636. Usage: one or more of ldap://‹Domain controller IP ›:‹port› (if not default port) or ldaps://‹Domain controller IP ›:‹port› (if not default port) If the authentication provider supports a multidomain forest, use the global catalog server IP and always specify the port number. Default is 3268 for ldap, 3269 for ldaps. Usage: ldap(s)://‹Global catalog server IP›:‹port›
Manager DN	managerdn	Indicates the Active Directory Bind user account that ViPR uses to connect to Active Directory or LDAP server. This account is used to search Active Directory when a ViPR administrator specifies a user for role assignment, for example. Requirement: This user must have **Read all inetOrgPerson information** in Active Directory. The InetOrgPerson object class is used in several non-Microsoft, Lightweight Directory Access Protocol (LDAP) and X.500 directory services to represent people in an organization. To set this privilege in Active Directory, open Active Directory Users and Computers, right click on the domain, and select **Delegate Control...** . Click **Next**, then select the user that you are using for managerdn and click **Next**. The required

UI name	CLI name (Provider.cfg)	Description and requirements
		permission is on the next screen "Read all inetOrgPerson information." Example: CN=Manager,CN=Users,DC=mydomaincontroller,DC=com In this example, the Active Directory Bind user is Manager, in the Users tree of the mydomaincontroller.com domain. Usually managerdn is a user who has fewer privileges than Administrator, but has sufficient privileges to query Active Directory for users attributes and group information. **⚠WARNING** **You must update this value in ViPR if the managerdn credentials change in Active Directory.**
Manager Password	passwd_user	The password of the managerdn user. **⚠WARNING** **You must update this value in ViPR if the managerdn credentials change in Active Directory.**
Disabled	disable	Select Disabled if you want to add the server to ViPR but not immediately use it for authentication. (Regardless of whether this property is true, ViPR validates that the provider's name and domain are unique.)
Group Attribute	groupattr	Indicates the Active Directory attribute that is used to identify a group. Used for searching the directory by groups. Example: CN Active Directory only. Does not apply to other authentication providers. **Note** Once this value is set for a provider, it cannot be changed, because of the tenants that are using this provider may already have role assignments and permissions configured using group names in a format using the current attribute.
Group Whitelist	whitelist	Optional. One or more group names as defined by the authentication provider. This setting will filter the group membership information that ViPR retrieves about a user. • When a group or groups are included in the whitelist, it means that ViPR will be aware of a

UI name	CLI name (Provider.cfg)	Description and requirements
		user's membership in the specified group[s] only. Multiple values (one per line in ViPR UI, comma-separated in CLI and API) and wildcards (for example MyGroup*,TopAdminUsers*) are allowed. • Blank value (default) means that ViPR will be aware of any and all groups that a user belongs to. Asterisk (*) is the same as blank. Example: UserA belongs to Group1 and Group2. If the whitelist is blank, ViPR knows that UserA is a member of Group1 and Group2. If the whitelist is "Group1", ViPR knows that UserA is a member of Group1, but does not know that UserA is a member of Group2 (or of any other group). Use care when adding a whitelist value. For example, if mapping a user to a tenant is based on group membership, then ViPR must be aware of the user's membership in the group. To restrict access to a tenant to users of certain group(s) only, one must: • add these group(s) to the tenant user mapping (using the CLI command `viprcli tenant add-group`), so the tenant is configured to accept only users of these group(s). • add these group(s) to the whitelist, so that ViPR is authorized to receive information about them Note that by default, if no groups are added to the tenant user mapping, users from any groups are accepted, regardless of the whitelist configuration. Active Directory only. Does not apply to other authentication providers.
Search Scope	searchscope	One Level (search for users one level under the search base) or Subtree (search the entire subtree under the search base).
Search Base	searchbase	Indicates the Base Distinguished Name that ViPR uses to search for users at login time and when assigning roles or setting ACLs. Example: CN=Users,DC=mydomaincontroller,DC=com

UI name	CLI name (Provider.cfg)	Description and requirements
		This example searches for all users in the Users container. Example: CN=Users,OU=myGroup,DC=mydomaincontroller, DC=com This example searches for all users in the Users container in the myGroup organization unit. Note that the structure of the searchbase value begins with the "leaf" level and goes up to the domain controller level--the reverse of the structure seen in the Active Directory Users and Computers UI.
Search Filter	searchfilter	Indicates the string used to select subsets of users. Example: userPrincipalName=%u **Note** ViPR does not validate this value when you add the authentication provider.
(not applicable)	maxpagesize	Value that controls the maximum number of objects returned in a single search result. This is independent of size of the each returned object. If specified must be greater than 0. Cannot be higher than the max page size configured on the authentication provider.
(not applicable)	validatecertificate	When ldaps protocol is used, SSL validates the certificate from the authentication provider. Default is false. If set to true, the LDAP needs to have a valid CA certificate.

Editing an authentication provider

You can edit an authentication provider's settings.

Before you begin

This operation requires the Security Administrator role in ViPR.

Refer to the authentication provider information listed in Authentication provider attributes on page 26. Note especially the requirements for the Manager DN user.

Use care when entering values. ViPR does not validate your authentication provider entries.

Procedure

1. Select **Admin** › **Security** › **Authentication Providers**
2. Select the authentication provider and **Edit**.
3. Enter values for the attributes. Refer to Authentication provider attributes on page 26.
4. **Save**.

Role assignment and UI access

The administrator role to which a ViPR user is assigned determines what administration operations they can perform. At the Admin view of the UI, the areas of the UI and menu items that are visible to a user are similarly determined by the user's role.

There are two types of ViPR users: end-users and administrators. End-users can be divided into provisioning users and object storage users. Provisioning users create and manage file and block storage, mainly using the services in the service catalog. Object storage users are consumers of ViPR object storage. That is, users who authenticate with ViPR in order to be allowed to create and access ViPR object storage.

There is no explicit role assigned to end-users in ViPR. All users who belong to a domain contributed by an authentication provider, and have been mapped into a tenant, can perform end-user operations and can access the User view at the UI. For end-users, access to certain ViPR functions is restricted using an access control list (ACL).

ViPR administration operations are controlled by a set of administrator roles. Roles can be specific to a tenant or can be applicable to all tenants within a virtual data center. The available roles and their scope is listed in the table below.

Table 3 Scope of ViPR roles

Scope	Role
Tenant	Tenant Administrator, Project Administrator, Tenant Approver
Virtual Data Center	System Administrator, Security Administrator, System Monitor, System Auditor

The Security Administrator is responsible for adding users into ViPR virtual data center roles and can assign users into tenant roles. The Tenant Administrator can assign users to the tenant roles.

After ViPR is deployed, there is a root user (superuser) which includes all role privileges, including Security Administrator privileges. The root user can act as the bootstrap user for the system by assigning one or more users to the Security Administrator role. The Security Administrator can then assign other user roles.

The **Admin** › **Security** › **Role Assignment** page displays the administrator roles that are currently assigned to users and enables roles to be assigned.

The actions available to each role and the Admin view access provided by each role are described in Administrator role permissions on page 31. In addition, access to the User view for administrators and provisioning users is described in User access to UI on page 34.

Administrator role permissions

The actions that can be performed and the areas of the Admin view UI accessible depend on the administrator role assigned to a VIPR user.

The following table lists the roles and their associated permissions.

Table 4 Role permissions

Role	Permission	UI Access
Tenant Administrator	Assigns tenant roles to tenant users.	**Admin › Security › Role Assignments**
	Creates new projects. Has all permissions on projects in the tenant.	**Admin › Tenant › Projects**
	Assigns users to projects using an ACL.	
	Can delegate project ownership to Project Administrator.	
	Can create consistency groups for any project.	**Admin › Tenant › Consistency Groups**
	Can view all recent orders for all users in the tenant.	**Admin › Tenant › Recent Orders**
	Can view all scheduled orders for the tenant and can cancel scheduled orders.	**Admin › Tenant › Scheduled Orders**
	Creates execution windows.	**Admin › Tenant › Execution Windows**
	Specifies approval notification and external approval system settings.	**Admin › Tenant › Approval Settings**
	Adds hosts, clusters, and vCenters to which provisioned storage can be exported.	**Admin › Physical Assets › Hosts/Clusters/vCenters**
Project Administrator	Creates projects and can delegate ownership to another Project Administrator. Has all permissions for own projects.	**Admin › Tenant › Projects**
	Assigns users to projects (that Project Administrator owns) using an ACL.	
	Can create consistency groups for owned projects	**Admin › Tenant › Consistency Groups**
Tenant Approver	Approves orders for the tenant.	No access to Admin view. **User › Approvals**
System Administrator	Adds physical storage resources by adding: storage systems, SMI-S providers, fabrics, and data protection systems.	**Admin › Physical Assets › Storage Systems** **Admin › Physical Assets › SMI-S Providers** **Admin › Physical Assets › Fabric Managers**

Table 4 Role permissions (continued)

Role	Permission	UI Access
		Admin › Physical Assets › Data Protection Systems
	Creates virtual arrays comprising fibre channel and IP networks that connect storage systems and compute environments (hosts and vCenters), and creates virtual pools.	**Admin › Virtual Assets › Virtual Arrays** **Admin › Virtual Assets › Virtual Pools** **Admin › Virtual Assets › Networks**
	Assigns tenants to virtual arrays and virtual pools using an ACL.	
	Sets up ViPR object storage.	**Admin › Data Services**
	Retrieves ViPR status and system health.	**Admin › System › System Health** **Admin › System › Logs**
	Performs system license and software updates.	**Admin › System › License** **Admin › System › Upgrades** **Admin › System › Support Requests**
	Retrieves bulk event and statistical records for the ViPR virtual data center.	**Admin › System › Dashboard** **Admin › System › System Health** **Admin › System › Logs**
Security Administrator	Adds authentication providers.	**Admin › Security › Authentication Providers**
	Sets the configuration parameters for the virtual data center.	**Admin › System › Configuration**
	Assigns users to administrator roles for the virtual data center and for tenants.	**Admin › Security › Role Assignments**
System Monitor	Retrieves bulk event and statistical records for the ViPR virtual data center.	**Admin › System › Dashboard** **Admin › System › System Health**
	Has read-only access to all objects in the ViPR virtual data center.	**Admin › System › Logs**
System Auditor	Retrieves ViPR virtual data center audit log.	**Admin › System › Audit Log**

User access to UI

The User view can be accessed by all users mapped into the tenant.

The following table shows what access end-users and administrators have at the User view.

Table 5 User view access

Role	User view area	Access
Tenant Administrator	Service Catalog	Can always see all categories and services. Access cannot be restricted by ACL. Can create storage in and manage storage belonging to all projects.
	Orders	Can see own orders. Can see all orders in Admin view.
	Resources	Can see resources for all projects.
	Approvals	Cannot access this menu.
Project Administrator	Service Catalog	Can see all categories and services. Access can be restricted by Tenant Administrator using ACL. Can create storage in and manage storage belonging to all owned projects and projects assigned by ACL.
	Orders	Can see own orders.
	Resources	Can see resources for projects that he or she owns.
	Approvals	Cannot access this menu.
Tenant Approver	Service Catalog	Can see all categories and services. Access can be restricted by Tenant Administrator using ACL. Can create storage in and manage storage belonging to all projects to which user is assigned.
	Orders	Can see own orders.
	Resources	Can see resources for projects that he or she owns.
	Approvals	Can access in order to approve orders.
All other roles and end-users (no role)	Service Catalog	Can see all categories and services. Access can be restricted by Tenant Administrator using ACL. Can create storage in and manage storage belonging to all projects to which user is assigned.
	Orders	Can see own orders.
	Resources	Can see resources for projects that he or she has been assigned to.
	Approvals	Cannot access this menu.

Role matrix

A matrix is provided to show the availability of menu items for each role. Where a user has more than one assigned role, the access rights are additive.

Table 6 Role matrix

Menu	Sub-menu	Tenant Roles			VDC Roles				None
		TenAd	ProjAd	TenAp	SysAd	SecAd	SysMo	SysAu	
Admin view									
System	Dashboard				x		x		
	System Health				x		x		
	Logs				x		x		
	Configuration					x			
	Upgrade				x				
	Support Request				x				
	License				x				
	Audit Log							x	
Security	Authentication Provider					x			
	Role Assignments	x				x			
	Local Passwords					x			
Tenant	Project	x	x						
	Consistency Groups	x	x						
	Recent Orders	x			x				
	Scheduled Orders	x			x				
	Execution Windows	x			x				
	Approval Settings	x			x				
Physical Assets	Storage Systems				x				
	SMI-S Providers				x				
	Fabric Managers				x				
	Data Protection Systems				x				
	Hosts	x							
	Clusters	x							
	vCenters	x							
Virtual Assets	Virtual Arrays				x				
	Virtual Pools				x				
	Networks				x				

Table 6 Role matrix (continued)

Menu	Sub-menu	Tenant Roles			VDC Roles				None
		TenAd	ProjAd	TenAp	SysAd	SecAd	SysMo	SysAu	
Service Catalog		x			x				
Data Services	Setup				x				
	Virtual Pools				x				
	Data Stores				x				
	Tenant Configuration				x				
	Base URLs				x				
User view									
Home		x	x		x	x	x	x	x
Service Catalog		x	x		x	x	x	x	x
Orders		x	x		x	x	x	x	x
Resources		x	x		x	x	x	x	x
Approvals				x					

The actions that can be carried out in the User view by Tenant Administrators, Project Administrators, Tenant Approvers, and all other administrator roles and end-users are described in User access to UI on page 34.

Assigning a role to a user or group

The **Admin** › **Security** area provides the ability to assign an administrator role to a user or to a group.

Before you begin

- This operation requires the Security Administrator role to assign virtual data center roles, or the Tenant Administrator role to assign tenant roles.
- An authentication provider must be configured before you can assign roles.

Procedure

1. Select **Admin** › **Security** › **Role Assignment**.
2. Select **Add**.
3. Enter the name of a domain user or group.
4. Select the roles into which you want to assign the user or group.

   The actions available to each role and the availability of UI area for each role are provided in Administrator role permissions on page 31.
5. **Save**.

Access control lists

Access control lists (ACLs) enable ViPR users to be granted access to areas of the UI and to ViPR resources.

Until an ACL is configured, access to an ACL controlled area is available to all users. Once an ACL is configured, access is limited to those users and groups defined in the ACL.

The following table describes the ACLs you can configure.

Table 7 User view ACL permissions

ACL configured on	Permissions
Service Catalog	Determines which categories are visible to a user.
Service	Determines which services are visible to a user.
Projects	Determines which resources are visible to a user and which projects resources can be provisioned for.

The ACL access permissions and their meanings are summarized in the table below.

Table 8 ACL Permissions

Permission	Meaning
OWN	Can perform operations associated with ownership. For example, project ownership enables assignment of users to project ACLs and deletion of projects.
ALL	Can perform all resource operations. On projects, allows all operations on projects and file systems, volumes, snapshots etc that belong to the project.
USE	Can access and use. Can be used to restrict access to virtual arrays and virtual pools for tenants. Assigned to service catalog categories and services users to allow access. If no ACLs are set access remains open.
BACKUP	Can view storage resources and execute protection services.

Assigning permissions using ACLs

Access control lists are provided to enable you to configure access to the service catalog and to projects for provisioning users.

Before you begin

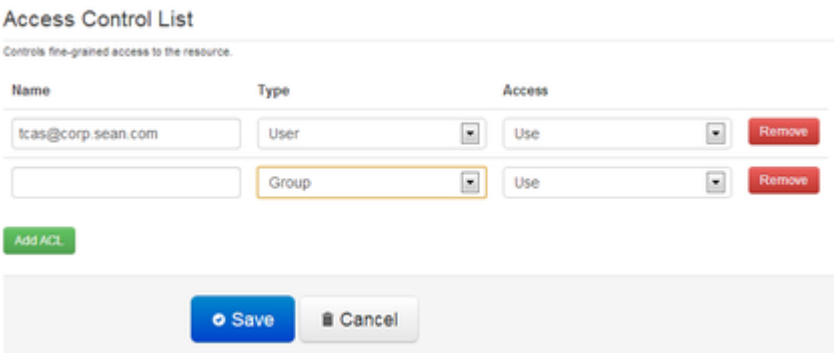
ACLs will only restrict access for users with user rights in the Admin view. A Tenant Administrator has ultimate authority in the tenant and access to the service catalog and projects cannot be restricted using ACLs.

This task is referenced by areas that use ACLs and provides general information on assigning users and groups to ACLs.
The role that you require depends on the area to which you are applying access control.

Procedure

1. Select **Add ACL**.

   An ACL entry record is displayed.



2. From the Type drop-down, select whether you are using this entry to set access permissions for a user or a group.
3. In the Name field, enter the name of the user or group that you are assigning permissions to.

   Both users and groups are added in the format: username@yourco.com, or groupname@yourco.com. If you are using groups they must have been enabled by the Security Administrator by adding them to the Group Whitelist in the authentication provider.
4. In the Access field, use the drop-down list to select the access permissions that you want to assign to the user or group.
5. If you want to add further ACL entries, choose **Add ACL** to add another entry.
6. If you decide you do not need an entry you have made, click the **Remove** button.
7. **Save** the form that your are editing.

Local accounts

ViPR has several local accounts that are used internally or for administration and service.

Table 9 Local accounts

Account	Use	ViPR roles and privileges	Initial password
root	Used for initial setup and for testing, evaluation, and troubleshooting, when most privileged account is needed. Same account as root user on the Controller VMs.	System Administrator, System Monitor, Security Administrator, Tenant Administrator	ChangeMe
svcuser	For read-only support	System Monitor and can access ViPR UI.	ChangeMe
sysmonitor	Used by SolutionPack to collect ViPR data	System Monitor	ChangeMe

Table 9 Local accounts (continued)

Account	Use	ViPR roles and privileges	Initial password
proxyuser	Used internally to run operations on behalf of a user	Proxy User (internal role, not assignable)	ChangeMe

Changing local account passwords

You can change the password of a local account.

Before you begin

This operation requires the Security Administrator role in ViPR.

Procedure

1. Select **Admin** › **Security** › **Local Passwords**
2. Select a local user account.
3. Enter the new password and confirm.
4. **Save**.

CHAPTER 4

Configuring Physical and Virtual Assets

This chapter contains the following topics:

Physical and virtual assets

Configuration of the ViPR virtual data center requires the addition of physical assets and their organization into virtual storage arrays, referred to as virtual arrays, and virtual storage pools, referred to as virtual pools.

When dealing with assets, both physical and virtual, it is important to understand the role of discovery and registration, and their relationship to the virtual pools that you configure as the target for provisioning operations.

Asset discovery

When an asset is added to ViPR, ViPR uses its credentials to connect to it (over IP) and obtain information that will help it to model your storage network. This process is referred to as "discovery."

If the asset is a storage systems, ViPR will collect information about the storage ports and pools that it provides; if the asset is a host or vCenter, ViPR will discover its initiator ports. For a fabric manager, ViPR will retrieve the VSANs or fabrics configured on the switch and use them to discover networks within the data center, where a network comprises a set of end-points (array ports and initiator ports) connected by switch ports.

Hence, the number of networks that you see when discovery is performed depends on the way in which your fabric is configured.

Discovery runs automatically when an asset is added and at a configurable interval (**Admin** › **System** › **Configuration**). It can also be initiated manually to verify the status of an asset. If an asset fails discovery, its status will show as error and an indication of the reason for failure will be displayed. Typically, this will be "Device discovery failed". If ViPR is able to contact the device, but it is not compatible, it will additionally be flagged as incompatible.

If an asset is unavailable it may affect the networks that are available or the end-points associated with those networks. If those networks are contributing to a virtual array, and the storage pools provided by storage systems on the network are contributing to a virtual pool, the ability of a virtual pool to provide a location for a provisioning request may be compromised.

In the case of IP connected storage systems and hosts, ViPR can discover the ports, but it cannot discover the paths between them, so it necessary to create the IP networks manually using the ViPR UI.

Deregistration and registration

You can deregister certain ViPR physical and virtual components so that they can be made temporarily unavailable to the ViPR virtual data center.

ViPR will continue to include the component in its model of the virtual data center and will continue to perform discovery on storage systems and fabric managers. However, any virtual pools that include storage pools contributed by the component will be affected as those storage pools can no longer be a possible location for storage operations that use the virtual pool. Registration is user initiated, if a device fails discovery, it will still be shown as registered unless it is deregistered.

The following assets can be deregistered:

- Storage systems
- Fabric managers

- Networks
- Storage ports
- Storage pools

When the deregistration or failure of a component makes storage pools unavailable, they will not be shown as matching pools when creating a virtual pool, so it will not be possible to select them for inclusion in a "manual" virtual pool.

However, storage pools that are already contained in a "manual" virtual pool, or meet the criteria of an "automatic" virtual pool, will automatically be added back into the virtual pool when they are made available by a re-registration operation or when a rediscovery operation restores an asset.

You can read about virtual pools and the significance of manual and automatic virtual pools in Virtual pools on page 67.

Physical asset management

Physical assets are managed from the **Admin** › **Physical Assets** area. Phyical assets must be added to ViPR to connect ViPR to the data center infrastructure.

ViPR physical assets include:

- Storage systems and SMI-S providers
- Fabric managers
- Data protection systems
- Hosts
- Clusters
- vCenters

Only System Administrators can manage the storage systems, SMI-S providers, Fabric managers, and data protection systems to ViPR. Hosts, clusters, and vCenters can be added by System Administrators, and Tenant Administrators.

Storage system management

Use the **Admin** › **Physical Assets** › **Storage Systems** page to view the list of storage systems, and storage system attributes, and to manage the storage systems, storage pools, and storage ports in the ViPR physical assets.

The tab shows all storage systems added to ViPR, system type, their IP addresses, associated SMI-S providers and data protection sites, and other information.

Adding a storage system

You can add a supported storage system from the Admin view's **Physical Assets** tab.

Before you begin

- This operation requires the System Administrator role in ViPR.

Procedure

1. Select **Admin** › **Physical Assets** › **Storage Systems**.
2. **Add** a storage system.
3. Select the storage system type.
4. To add VMAX or VNX block storage, select **SMI-S Provider for EMC VMAX and VNX Block** as the storage system type and enter the SMI-S provider's host name, IP

address, port used for communication between the ViPR virtual appliance, and credentials for an account that has administrator privileges.

To add file storage (**EMC Isilon**, **EMC VNX File**, **EMC VPLEX**, **NetApp**), enter a name for the storage, the IP address of the host or control station, port (Isilon default is 8080, otherwise 443), and credentials with storage system administrator privileges.

When adding VNX file storage, additionally enter information about the onboard SMI-S provider that resides on the control station. You need to enter the provider host, SSL setting, port (default 5989), and credentials for the onboard SMI-S provider.

5. **Save**.

Editing a storage system

You can change the display name for a storage system in ViPR and modify its resource allocation setting.

Before you begin

This operation requires the System Administrator role in ViPR.

Procedure

1. Select **Admin** › **Physical Assets** › **Storage Systems**.
2. Select a storage system by clicking its name.
3. Optionally change the storage system's name.
4. Optionally change the storage system's resource allocation settings. By default, there is no limit on the amount of a storage system's resources that can be used by ViPR. To set a limit, disable Unlimited Resource Allocation and set a value for Resource Limit. The Resource Limit value is a count of the number of resources (volumes or filesystems, depending on the storage type) allowed to be provisioned on the storage system.

Deleting a storage system

Delete a storage system from ViPR.

Before you begin

- This operation requires the System Administrator role in ViPR.
- Storage systems containing physical storage pools, which have been added to virtual pools, cannot be deleted.
- Storage systems that have been deleted can only be added back into ViPR through the ViPR API.

Procedure

1. Select **Admin** › **Physical Assets** › **Storage Systems**.
2. Select a storage system and click **Delete**.

Rediscovering a storage system

Use the Rediscover action to query the storage system and update the list of storage pools and storage ports.

Before you begin

This operation requires the System Administrator role in ViPR.

Procedure

1. Select **Admin** › **Physical Assets** › **Storage System**.

2. Select an array and **Rediscover**.

Deregistering a storage system

You can deregister a storage system from ViPR. Once deregistered, the storage system will no longer be able to contribute storage pools to a virtual array.

Before you begin

This operation requires the System Administrator role in ViPR.

Procedure

1. Select **Admin** › **Physical Assets** › **Storage Systems**.
2. Select the storage system that you want to deregister.
3. Select **Deregister**.

Registering a storage system

New storage systems or storage systems that have previously been deregistered from ViPR can be registered into ViPR. Once registered, the storage system can contribute its storage pools to any virtual pools it is used in.

Before you begin

This operation requires the System Administrator role in ViPR.

Procedure

1. Select **Admin** › **Physical Assets** › **Storage Systems**.
2. Select the storage system that you want to register.
3. Select **Register**.

Storage pools

Use the **Admin** › **Physical Assets** › **Storage Systems** › **Edit Pools** › **Storage Pools** page to view the list of storage pool attributes for the storage pools discovered with the storage system. The page is also used to register and deregister the storage pools discovered with the storage system.

If you do not want certain pools to be available to a ViPR virtual array, you can deregister the pools.

Best practices for deregistering storage pools

- By default, ViPR registers storage pools when the storage system is added to ViPR. Use the deregister option to make the storage pools unavailable to use as a ViPR resource.
- If a storage pool becomes unavailable on the storage system, the storage pool remains in the list of available ViPR storage pools. The storage pool must be manually deregistered in ViPR to ensure it is not used in a service operation.

Storage pool attributes

Column name	Description
Name	The storage pool name.
Resource Type	Provisioning type: either Thin or Thick.
Drive Types	The supported drive types.

Column name	Description
Free (GB)	Amount of free storage space, in gigabytes, currently available in the storage pool.
Subscribed (GB)	The total amount of usable space that is configured in the pool and presented to attached hosts (GB)
Total (GB)	The size, in gigabytes, of the storage pool.
Registered	If checked, the storage pool is registered for use in ViPR. If empty, the storage pool is discovered in ViPR, but cannot be used as a ViPR resource.

Editing a storage pool

You can change the maximum pool utilization percentage, the maximum thin pool subscription percentage, and the resource limit setting for a storage pool.

Before you begin

This operation requires the System Administrator role in ViPR.
The pool must already exist on the storage system, and the storage system itself must already be added to ViPR.

Procedure

1. Select **Admin** › **Physical Assets** › **Storage Systems**.
2. Select a storage system.
3. **Edit Pools**.

   A pool's default resource limit is derived from the storage system's limit.
4. Optionally change the maximum pool utilization percentage. The default is 75%.
5. Optionally set a maximum thin pool subscription percentage. The default is 300%.
6. Optionally change the pool's resource limit. By default, there is no limit on the amount of a storage pool that can be used by ViPR. To set a limit, set a value for Resource Limit. The Resource Limit value is a count of the number of resources (volumes or file systems, depending on the storage type) allowed to be provisioned using the selected storage pool.

Deregistering a storage pool

By default, ViPR registers storage pools when the storage system is added to ViPR. Use the deregister option to make the storage pools unavailable to use as a ViPR resource.

Before you begin

- This operation requires the System Administrator role in ViPR.
- The pool must already exist on the storage system, and the storage system itself must already be added to ViPR.
- The storage pool must not contain provisioned storage and must not be associated with any virtual arrays.
- If a storage pool becomes unavailable on the storage system, the storage pool remains in the list of available ViPR storage pools. The storage pool must be manually deregistered in ViPR to ensure it is not used in a service operation.

Procedure

1. Select **Admin** › **Physical Assets** › **Storage Systems**.
2. Select a storage system.
3. **Edit Pools**.
4. Select one or more registered storage pools.
5. **Deregister**.

Registering a storage pool

Storage pools are registered automatically when you add a storage system to ViPR. If a storage pool was unregistered for some reason, it can be manually reregistered.

Before you begin

This operation requires the System Administrator role in ViPR.
The pool must already exist on the storage system, and the storage system itself must already be added to ViPR.

Procedure

1. Select **Admin** › **Physical Assets** › **Storage Systems**.
2. Select a storage system.
3. **Edit Pools**.
4. Select a unregistered storage pool.
5. **Register**.

Storage ports

Use the **Admin** › **Physical Assets** › **Storage Systems**, **Storage Ports** page to view the storage ports, and storage port attributes for the selected storage system, and to register and deregister the ViPR storage ports.

The Storage Ports table associated with each storage system shows the discovered ports, the port type (FC or IP), and the port registration status.

Table 10 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 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.

By default ports are automatically registered with ViPR when the storage system is discovered.

Optionally, ports can be deregistered to make them unavailable to be used by ViPR. Deregistered ports can always be registered again at a later date.

To register or deregister a storage port:

1. Go to the **Admin** › **Physical Assets** › **Storage Systems** page.

2. Click **Ports** in the **Edit** column.
3. Select the box in the first column of the port row.
4. Click **Register** to register the port for use in ViPR, or **Deregister** to make the port unavailable for use in ViPR.

Deregistering a storage port

You can deregister a storage port from a storage system. Once deregistered, the port will not be used to when you add a storage system to ViPR.

Before you begin

This operation requires the System Administrator role in ViPR.

Procedure

1. Select **Admin** › **Physical Assets** › **Storage Systems**.
2. Select a storage system.
3. **Edit Ports**.
4. Select one or more ports and **Deregister**.

SMI-S providers

You can use the SMI-S Providers tab (**Admin** › **Physical Assets** › **SMI-S Providers)** to add an SMI-S provider and discover all storage known to it.

Adding an SMI-S provider

You can add an SMI-S provider to ViPR and use it to discover VMAX and VNX block storage.

Before you begin

- This operation requires the System Administrator role in ViPR.

Procedure

1. Select **Admin** › **Physical Assets** › **SMI-S Providers**.
2. **Add** an SMI-S Provider.
3. Enter the SMI-S provider's host name, IPv4 address, port used for communication between the ViPR virtual appliance, and credentials for an account that has array administrator privileges. Enable SSL if used.
4. **Save**.

   Storage discovered through the SMI-S provider is displayed on the **Storage Systems** tab.

Deleting an SMI-S provider

You can delete an SMI-S provider.

Before you begin

This operation requires the System Administrator role in ViPR.
The SMI-S provider must not have any storage systems managed by ViPR.

Procedure

1. Select **Admin** › **Physical Assets** › **SMI-S Providers**.
2. Select an SMI-S provider and **Delete**.

Editing an SMI-S provider

You can edit the settings of an SMI-S provider.

Before you begin

This operation requires the System Administrator role in ViPR.

Procedure

1. Select **Admin** › **Physical Assets** › **SMI-S Providers**.
2. Select the name of an SMI-S provider to edit its information.
3. **Save**.

Rediscovering an SMI-S provider

You can rediscover an SMI-S provider to update the list of storage systems it provides to ViPR.

Before you begin

This operation requires the System Administrator role in ViPR.

Procedure

1. Select **Admin** › **Physical Assets** › **SMI-S Providers**.
2. Select an SMI-S provider and **Rediscover**.

Fabric managers

Use the Fabric Managers tab (**Admin** › **Physical Assets** › **Fabric Managers)** to add a SAN network system to ViPR, the first step in making SAN storage available for provisioning.

When you add a SAN switch, ViPR discovers the topology seen by the switch, and creates a network for each Cisco VSAN or Brocade fabric.

Adding a fabric manager

Add a SAN network switch such as Cisco or Brocade to discover the storage topology.

Before you begin

- This operation requires the System Administrator role in ViPR.
- You need to provide the IPv4 address, port, and administrator credentials for a switch or its SMI-S provider, depending on the switch type.

Procedure

1. Select **Admin** › **Physical Assets** › **Fabric Managers**.
2. **Add** a fabric manager.
3. Select a switch type and enter the switch's name, IPv4 address, the port used for communication between the ViPR virtual appliance and switch, and credentials for an account that has administrator privileges on the switch. For a Brocade switch, you provide the IPv4 address, the port and credentials of the associated SMI-S provider, not of the switch itself.
4. **Save**.

   The fabric manager is automatically registered and all discovered networks associated with the switch are registered.

Deleting a fabric manager

You can delete a fabric manager from ViPR.

Before you begin

This operation requires the System Administrator role in ViPR.

Procedure

1. Select **Admin** › **Physical Assets** › **Fabric Managers**.
2. Select a fabric manager and **Delete**.

Editing a fabric manager

You can edit a fabric manager's settings.

Before you begin

This operation requires the System Administrator role in ViPR.

Procedure

1. Select **Admin** › **Physical Assets** › **Fabric Managers** .
2. Select the name of fabric manager to edit its information.
3. **Save**.

Rediscovering a fabric manager

You can rediscover a fabric manager to update the list of networks it makes available to ViPR.

Before you begin

This operation requires the System Administrator role in ViPR.

Procedure

1. Select **Admin** › **Physical Assets** › **Fabric Managers**.
2. Select a fabric manager and **Rediscover**.

Deregistering a fabric manager

You can deregister a fabric manager to remove it from the virtual data center.

Before you begin

This operation requires the System Administrator role in ViPR.

Procedure

1. Select **Admin** › **Physical Assets** › **Fabric Managers**.
2. Select the fabric manager you want to deregister.
3. Select **Deregister**.

   The registration field in the fabric managers table will display a "x" to indicate the asset is deregistered.

   While deregistered, any networks provided by the fabric manager will be deregistered.

Registering a fabric manager

You can register a fabric manager that has previously been deregistered from the virtual data center. When a fabric manager is registered, all of the networks associated with the fabric manager will be registered.

Before you begin

This operation requires the System Administrator role in ViPR.

Procedure

1. Select **Admin** › **Physical Assets** › **Fabric Managers**.
2. Select the fabric manager you want to register.
3. Select **Register**.

   The registration field in the fabric managers table will display a tick to indicate the asset is registered.

   All networks associated with the fabric manager will show as registered.

Data protection systems

You can use the Data Protection Systems tab (**Admin** › **Physical Assets** › **Data Protection Systems**) to add a protection system such as EMC RecoverPoint to ViPR.

Integrating EMC RecoverPoint in the ViPR virtual appliance

EMC RecoverPoint provides continuous data protection with multiple recovery points to restore applications instantly to a specific point in time. You can set up virtual pools and arrays in ViPR so users can take advantage of RecoverPoint in block storage requests.

When adding physical assets to ViPR, you need to:

- Add the RecoverPoint system as a physical asset (**Admin** › **Physical Assets** › **Data Protection**)
- Add the storage systems that host the source volumes that you want to protect, the target volumes, and the journal volumes for both.
- Add fabric managers that see the storage systems and the RecoverPoint sites.

When creating virtual assets, select RecoverPoint as the data protection type when creating a virtual pool. Add one or two RecoverPoint copies, specifying the destination virtual array, and optionally a virtual pool. The virtual pool specifies the characteristics of the RecoverPoint target and journal volumes. Set the journal size as needed. You can accept the RecoverPoint default (2.5 times protected storage), or you can specify a fixed number, or a multiplier of the protected storage other than the default.

Services that leverage RecoverPoint are in the catalog under Block Protection Services.

Adding a data protection system

You can add a data protection system on the Admin view's **Physical Asset** tab.

Before you begin

- This operation requires the System Administrator role in ViPR.

Procedure

1. Select **Admin** › **Physical Assets** › **Data Protection Systems**.
2. **Add** a data protection system.

3. Enter a name for the data protection system and select a data protection type.

   For RecoverPoint, enter the site management IPv4 address or fully-qualified domain name of the host. The default port to communicate with RecoverPoint is 7225. The credentials must be for an account that has the RecoverPoint admin role to access the RecoverPoint site.

4. **Save**.

Editing a data protection system

You can edit an existing data protection system.

Before you begin

This operation requires the System Administrator role in ViPR.

Procedure

1. Select **Admin** › **Physical Assets** › **Data Protection Systems**.
2. Select the name of an data protection system to edit its information.
3. **Save**.

Deleting a data protection system

You can delete a data protection system from ViPR.

Before you begin

This operation requires the System Administrator role in ViPR.

Procedure

1. Select **Admin** › **Physical Assets** › **Data Protection Systems**.
2. Select a data protection system and **Delete**.

Rediscovering a data protection system

You can rediscover a data protection system to update its information in ViPR.

Before you begin

This operation requires the System Administrator role in ViPR.

Procedure

1. Select **Admin** › **Physical Assets** › **Data Protection Systems**.
2. Select an data protection system and **Rediscover**.

Hosts

Hosts are added to ViPR from the **Admin** › **Physical Assets** › **Hosts Physical Hosts** page.

The list of supported hosts is provided in the *EMC ViPR Data Sheet and Compatibility Matrix* on support.EMC.com.

When provisioning storage for a host, ViPR needs to communicate with the host to validate the host and connect storage to it. For Linux hosts, ViPR will SSH into the host; for Windows hosts, ViPR needs to execute remote PowerShell commands on the host.

When a host is connected to a Fibre Channel (FC) fabric, ViPR uses information from the fabric manager to discover storage systems and host initiator end-points and add them to a network.

When an IP connected host is added, ViPR does not know if it is on the same IP network as the storage system, so the host must be manually added to the IP network that contains the storage system IP ports.

Host and host initiator discovery

Host discovery can include automatically adding and registering the host initiators, or the host initiators can be manually added and registered to ViPR after the hosts are added to the ViPR physical assets.

Host discovery overview

Complete host discovery includes the following steps;

1. A host is added to the ViPR physical assets.
2. The host initiators are added to the ViPR assets.
3. The host initiators are registered for use by ViPR.

Steps 2 and 3 of host discovery can be performed automatically, while adding a host to the physical assets, or manually after a host is added to ViPR.

Automatic discovery of host initiators

By default, ViPR automatically discovers Windows and Linux host. When discovery is enabled, ViPR adds and registers all of the host initiators for that host. When automatically discovered, ViPR will use all the host initiators during service operations.

Manual discovery of host initiators

When a host, other than a Linux or Windows host, is added to ViPR, the host initiators must be manually added and registered in ViPR. Additionally, the automatic discovery option can be disabled for Windows and Linux hosts, so that the host initiators for the hosts can be manually added and registered to ViPR, as well.

The host initiators for undiscovered hosts can be added to the ViPR assets without being registered. Unregistered host initiators will not be used by ViPR for service operations.

Adding a host

Before provisioned storage can be attached to a host, the host must be added to ViPR.

Before you begin

- This operation requires the Tenant Administrator role in ViPR .
- Refer to the *EMC ViPR Data Sheet and Compatibility Matrix* for host version, and compatibility requirements.
- Refer to the *EMC ViPR Installation and Configuration Guide* to ensure the host is configured with the ViPR requirements. Using a host that does not match the ViPR configuration requirements in a ViPR service, could cause the ViPR service operation to fail.
- The host credentials are required to add the host.
    - If using LDAP or Active Directory domain account credentials, the domain user credentials must be in the same domain where the Windows host is located; otherwise the Windows host discovery will fail.
    - If adding a Linux host without root access, the sudo command must have the following privileges to allow ViPR to run the commands it requires on the host.

Table 11 Sudo privileges required by ViPR user

Type	Name
Command	e2fsck, fdisk, multipath, ifconfig, vgdisplay, sh, mkdir, mke2fs, mkfs.ext3, mkfs.ext4, mount, umount, resize2fs, iscsiadm, lsb_release, lvcreate, lvchange, lvremove, lvresize, pvcreate, pvremove, rpm, vgchange, vgremove, vgextend, vgreduce, vgcreate, powermnt
	find, sed, ls, sleep, rm

Procedure

1. Select **Admin** › **Physical Assets** › **Hosts**.
2. **Add** a host.
3. Specify the host **Operating System**.

   If adding a host other than a Linux, or Windows host, the host initiators must be manually managed. Optionally Windows and Linux host initiators can be manually managed by disabling the Discoverable option, otherwise ViPR will discover the Windows or Linux host initiators automatically.
4. Enter a **Name** to identify the host in ViPR.
5. Enter the **Host** fully qualified domain name or IP address.
6. Select the **Protocol**; HTTP or HTTPs
7. Enter the **Port** that ViPR will use to communicate with the host.
   - ViPR uses SSH for Linux hosts.
   - Connection to Windows hosts requires that Windows Remote Management (WinRM) is configured on the host and must listen on the port specified here.
8. Leave **Discoverable** enabled, to allow ViPR to automatically discover the Windows or Linux host initiators, and Windows clusters, or disable the option to manually manage the initiators associated with the host.
9. Enter the host login credentials.
10. Optionally, select the ViPR **Cluster** in which to add the host.
11. Enable **Validation on Save** to enable ViPR to check connectivity to the host before saving the host details.

    If you leave this box checked, and validation fails, the host information is lost.

    Disable the option and click Save to save the host information even if the connection fails. If adding the host fails, edit the host details, and Save again until the host is successfully added to ViPR.
12. **Save**.

After you finish

- Hosts that use ViPR services with the iSCSI protocol must have their iSCSI ports logged into the correct target array ports before they can use the service.
- IP connected hosts must be manually added to the IP network that contains the virtual array IP ports.

Linux host sudo command requirements

When ViPR attaches storage to a Linux host it needs to run commands on the host. To access the host, ViPR uses the credentials entered for the host at the **Admin** › **Physical Assets** › **Hosts** page. These are usually the credentials for the root account. If you do not wish to give ViPR root access to a Linux host, you must ensure that the sudo command has sufficient privileges to allow the user configured for the host to run the commands it requires.

Sudo privileges

The sudoers file configuration for the host user account must have the privileges listed in the table below.

Table 12 Sudo privileges required by ViPR user

Type	Name
Command	e2fsck, fdisk, multipath, ifconfig, vgdisplay, sh, mkdir, mke2fs, mkfs.ext3, mkfs.ext4, mount, umount, resize2fs, iscsiadm, lsb_release, lvcreate, lvchange, lvremove, lvresize, pvcreate, pvremove, rpm, vgchange, vgremove, vgextend, vgreduce, vgcreate, powermnt
	find, sed, ls, sleep, rm

For example, to allow "vipradmin" to run these commands as all users, you could add the following lines to the sudoers file:

```
Cmnd_Alias VIPRMGMT = /sbin/e2fsck, /sbin/fdisk, /sbin/multipath, /
sbin/ifconfig,
/sbin/vgdisplay,/usr/bin/sh, /bin/mkdir, /sbin/mke2fs, /sbin/
mkfs.ext3, /sbin/mkfs.ext4,
/bin/mount, /bin/umount, /sbin/resize2fs, /sbin/iscsiadm, /usr/bin/
lsb_release, /sbin/lvcreate,
/sbin/lvchange, /sbin/lvremove, /sbin/lvresize, /sbin/pvcreate, /sbin/
pvremove, /bin/rpm,
/sbin/vgchange, /sbin/vgremove, /sbin/vgextend,/sbin/vgreduce, /sbin/
vgcreate, /sbin/powermnt,
/bin/find, /bin/sed, /bin/ls, /bin/sleep, /bin/rm

vipradmin ALL=(ALL) VIPRMGMT
```

Adding an IP-connected host to a network

After initial setup, use the **Admin** › **Virtual Assets** › **Virtual Arrays** › **Edit IP Networks** page to add hosts to an IP network.

Before you begin

- This operation requires the System Administrator role in ViPR.

Procedure

1. Select **Admin** › **Virtual Assets** › **Virtual Arrays**.
2. Select the virtual array to which the host will be connected.
3. At the **Edit Virtual Array** page, select **Networks**.
4. In the **Networks** table, select the IP network to which the host will be made available.
5. In the **IP Ports** table, select **Add**.
6. Enter IP ports in the **Add Ports** box and click **Add**.

Editing a host

You can edit an existing host.

Before you begin

This operation requires the System Administrator role in ViPR.

Procedure

1. Select **Admin** › **Physical Assets** › **Hosts**.
2. Click the name of a host, in the **Host** table, **Name** column.
3. Optionally, edit any one of the following host information fields.
4. Enter the **Name** to identify the host in ViPR
5. Enter the **Host** fully qualified domain name or IP address.
6. Select the **Protocol**; HTTP or HTTPs
7. Enter the **Port** that ViPR will use to communicate with the host.
   - ViPR uses SSH for Linux hosts.
   - Connection to Windows hosts requires that Windows Remote Management (WinRM) is configured on the host and must listen on the port specified here.
8. Leave **Discoverable** enabled, to allow ViPR to automatically discover the Windows or Linux host initiators, and Windows clusters, or disable the option to manually manage the initiators associated with the host.
9. Enter the host login credentials.
10. Optionally, select the ViPR **Cluster** in which to add the host.
11. Enable **Validation on Save** to enable ViPR to check connectivity to the host before saving the host details.

    If you leave this box checked, and validation fails, the host information is lost.

    Disable the option and click Save to save the host information even if the connection fails. If adding the host fails, edit the host details, and Save again until the host is successfully added to ViPR.
12. Click **Save** to apply the changes.

Deleting a host

You can delete a host from ViPR.

Before you begin

This operation requires the System Administrator role in ViPR.
The host you want to delete must not have any attached storage.

Procedure

1. Select **Admin** › **Physical Assets** › **Hosts**.
2. Select a host and **Delete**.

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 **Admin** › **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

Registering host initiators makes them available to ViPR to use in services.

Before you begin

The host initiators must have been added to ViPR, or previously unregistered before they can be registered.

Procedure

1. Open the **Host Initiators** page.
   a. Select **Admin** › **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 register.
3. Click **Register**.

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 **Admin** › **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**.

Deleting host initiators

Deleting host initiators, removes the host initiators from the ViPR assets.

Before you begin

- Host initiators must be deregistered before being deleted.
- ESX and ESXi host initiators cannot be deleted.

Procedure

1. Open the **Host Initiators** page.
   a. Select **Admin** › **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 delete.
3. Click **Delete**.

ViPR Clusters

ViPR provides the capability to discover, and create clusters within the ViPR physical assets, and perform service operations using the ViPR clusters or individual hosts.

Cluster discovery

When adding a Windows host to ViPR, if discovery is enabled, ViPR will identify if the Windows host is part of a cluster, and add the cluster to the ViPR assets. Once it is added to ViPR, the cluster can be managed and edited as a ViPR cluster. Changes made to the Windows cluster from ViPR will only be made in the ViPR environment, and will not be applied to the Windows configuration. ViPR 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 physical assets.

ESX and ESXi clusters are also automatically discovered by ViPR when a vCenter is added. Once the ESX or ESXi cluster is added to ViPR, the cluster can be managed and edited as a ViPR cluster. Changes made to the ESX or ESXi cluster from the ViPR **Cluster** page, will only be made in the ViPR environment, and will not be applied to the vCenter configuration.

ViPR cluster operations

Discovered clusters are displayed, and new clusters are created, and managed from the **Admim** › **Physical Assets** › **Clusters** page of the ViPR UI. After a cluster is discovered or

created, hosts are added to the cluster. Hosts can be added to the cluster while creating or editing a host in ViPR, or from the Clusters page. A host can only exist in one cluster. Once a host is part of a ViPR cluster, service operations can be performed exclusively on a single host, or shared across the hosts in a cluster.

- Hosts that are not currently in use in a ViPR 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 will recognize the last assigned cluster as the cluster to which the host belongs.
- Hosts that are in use cannot be removed from the cluster.

Creating a ViPR cluster

Clusters are created from the **Admin** › **Physical Assets** › **Clusters** tab.

Procedure

1. Go to the **Admin** › **Physical Assets** › **Clusters** tab.
2. Click **Add**.
3. Provide the **Name**, and click **Save**.

After you finish

Once the cluster is created hosts can be added at the time the host is created, or by clicking the **Edit** button in the **Clusters** page.

Edit a cluster name

The cluster name is edited from the **Create Cluster** page.

Procedure

1. Go to the **Admin** › **Physical Assets** › **Clusters** tab.
2. Locate the cluster in the cluster list, and click the cluster name.
3. Make the changes to the cluster **Name** in the **Create Cluster** page.
4. Click **Save**.

   The new name appears in the list of clusters on the **Physical Clusters** page.

Delete a cluster

Clusters are deleted from the **Admin** › **Physical Assets** › **Clusters** page.

Before you begin

Clusters that have been configured in a service cannot be deleted from ViPR.

Procedure

1. Go to the **Admin** › **Physical Assets** › **Clusters** tab.
2. Click the checkbox next to the cluster being deleted.
3. Click **Delete**.

Edit hosts in a cluster

Editing hosts in the cluster includes adding, and removing hosts from the cluster.

Before you begin

- Clusters must be created before the hosts can be added to them.
- Hosts can be also be added to the cluster while creating or editing a host in ViPR.

- A host can only exist in one cluster.
- Hosts that are not currently in use in a ViPR 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 will recognize the last assigned cluster as the cluster to which the host belongs.
- Hosts that are in use cannot be removed from the cluster.

Procedure

1. Go to the **Admin** › **Physical Assets** › **Clusters** tab.
2. Locate the cluster that will be edited in the list of clusters.
3. Click **Edit Hosts** in the right column in the same row as the cluster.
4. Check the box to the left of one or more of the hosts.
5. Click **Add** to add the selected hosts to the cluster.

   Click **Remove** to remove the selected hosts from the cluster.

vCenters

You can use the vCenters tab (**Admin** › **Physical Assets** › **vCenters**) to add a vCenter to ViPR which storage can be exported and mounted as a datastore.

Adding a vCenter server

Add a vCenter Server to make provisioned volumes available to ESX hosts. You can add a vCenter from the Admin view's **Physical Asset** tab.

Before you begin

- This operation requires the System Administrator role in ViPR.

Procedure

1. Select **Admin** › **Physical Assets** › **vCenters**.
2. **Add**.
3. Enter the vCenter Server's name, its hostname or IP address, port used for communication between the ViPR virtual appliance and the vCenter server, and credentials for an account that has administrator privileges. Optionally validate the connection on save.

   Use care when identifying the vCenter; the UI does not prevent you from adding the same vCenter twice: once with its hostname, and again with its IP address.
4. Check the status of the **Validate Connection on Save** checkbox.

   If you leave this box checked, ViPR 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.
5. **Save**.

Deleting a vCenter server

You can delete a vCenter server from ViPR.

Before you begin

This operation requires the System Administrator role in ViPR.

Procedure

1. Select **Admin** › **Physical Assets** › **vCenters**.
2. Select a vCenter server and **Delete**.

Editing a vCenter Server

You can edit a vCenter Server's settings.

Before you begin

This operation requires the System Administrator role in ViPR.

Procedure

1. Select **Admin** › **Physical Assets** › **vCenters** .
2. Select the name of a vCenter Server to edit its information.
3. **Save**.

Rediscovering a vCenter server

You can rediscover a vCenter server to update the list of resources it makes available to ViPR.

Before you begin

This operation requires the System Administrator role in ViPR.

Procedure

1. Select **Admin** › **Physical Assets** › **vCenters**.
2. Select a vCenter Server and **Rediscover**.

Virtual asset management

The physical assets that comprise the infrastructure are configured into virtual assets to create the ViPR virtual data center. Virtual assets are configured, and managed through the **Admin** › **Virtual Assets** area.

Virtual assets include:

- Virtual arrays
- Virtual pools
- Networks

Virtual arrays

A virtual array is an abstract or logical array that is created to partition a virtual data center into a group of connected compute, network, and storage resources.

In ViPR, a virtual array is created by giving it a meaningful name and defining whether SAN zoning for the virtual array will be done automatically by ViPR or be manually configured. Once the virtual array is created, it must be populated with at least one network and one virtual pool.

A network consists of the storage ports and the host or initiator ports connected to the SAN switches that were added to ViPR as fabric managers. The assignment of the network to the virtual array, and the subsequent association of the virtual array with a virtual pool, determines the storage that is available when a user requests a provisioning service. Optionally, the devices available to a virtual array can be controlled by manually selecting the storage ports to make available to the virtual array, and the physical storage pools that will supply the storage for the virtual pools associated with the virtual array.

Virtual Arrays

Use the **Admin** › **Virtual Assets** › **Virtual Arrays** page to view, create, edit, and delete virtual arrays, as well as access the pages to define the networks, ports, and pools to include in the virtual array.

The **Virtual Arrays** page lists the virtual arrays with the following virtual array attributes.

Table 13 Virtual Array attributes

Column name	Description
Name	The virtual array name.
San Zoning	Options are: • Automatic ViPR creates the required zones in the SAN fabric when provisioning request is made to this virtual array. This will allow the storage to be visible to the hosts. • Manual When performing a provisioning operation the volumes cannot be visible to the host until the zones have been configured.
Edit	Provides the following buttons: • **Networks** Opens the **Networks** page for the selected virtual array. Use the **Networks** page to define the networks for the selected virtual array. • **Ports** Opens the **Storage Ports** page for the selected virtual array. Use the **Storage Ports** page to define the storage ports that will be used by the selected virtual array. • **Pools** Opens the **Storage Pools** page for the selected virtual array. Use the **Storage Pools** page to define the physical storage pools to associate with the selected virtual array.

Adding a virtual array

You should create one virtual array for each physical site, enterprise SAN, or computing "pod".

Before you begin

- This operation requires the System Administrator role in ViPR.
- At a minimum, a virtual array defines the type of SAN Zoning that will occur when a volume is exported from the array, and must include one or more networks

- Storage systems are brought into the virtual array with the networks.

Procedure

1. Select **Admin** › **Virtual Assets** › **Virtual Arrays**.
2. **Add**.
3. Enter a name for the virtual array.
4. Either:
   - Accept the default SAN zoning setting of **Automatic** to allow ViPR 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.
     - If there is an existing zone for the Host and Array:
       After the ViPR provisioning operation completes, check the Port Group within the Masking View to identify the FA ports that ViPR selected for the provisioning request. Compare the FA ports in the zone to the FA ports in the Port Group. If they match, no further action is required. If they do not match, reconfigure the zone to use the same FA ports. Alternatively, a new zone can be created.
     - If there is no existing zoning for the Host and Array:
       After the ViPR provisioning operation completes, check the Port Group within the Masking View to identify the FA ports that ViPR selected for the provisioning request. Create a zone with the appropriate initiator and target ports.
5. **Save**.

   One or more networks must be added to the virtual array before it can be managed by ViPR.
6. Locate the added virtual array in the table.
7. Click **Networks** in the **Edit** column.
8. Click **Add** to add one or more Fibre Channel SAN, or existing IP networks to the virtual array, or click**Add IP Network** to create a new IP network to add to the virtual array.

After you finish

Optionally, continue to assign storage ports and storage pools to the virtual array.

Editing a virtual array

Use the **Edit Virtual Array** page to change a virtual array name, change the SAN zoning setting, and to add, or edit the networks, storage ports, and storage pools associated with the virtual array.

Before you begin

This operation requires the System Administrator role in ViPR.

Procedure

1. Select **Admin** › **Virtual Assets** › **Virtual Arrays**.
2. Click the virtual array name.
3. Update or change the virtual array **Name**.
4. If no export operations have been performed on the
5. Update or change the type of **SAN Zoning**. Select:
   - **Automatic** to allow ViPR 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.
  - If there is an existing zone for the Host and Array:
    After the ViPR provisioning operation completes, check the Port Group within the Masking View to identify the FA ports that ViPR selected for the provisioning request. Compare the FA ports in the zone to the FA ports in the Port Group. If they match, no further action is required. If they do not match, reconfigure the zone to use the same FA ports. Alternatively, a new zone can be created.
  - If there is no existing zoning for the Host and Array:
    After the ViPR provisioning operation completes, check the Port Group within the Masking View to identify the FA ports that ViPR selected for the provisioning request. Create a zone with the appropriate initiator and target ports.

6. Click **Networks** to view, add, or remove networks associated with the virtual array.
7. Click **Ports** to view, add, or remove the storage ports associated with the virtual array.
8. Click **Pools** to view, add, or remove the physical storage pools associated with the virtual array.
9. Click **Save**.

Deleting a virtual array

Delete a virtual array removes the virtual array from the ViPR virtual assets permanently. Once deleted, the virtual array cannot be restored, and must be recreated to get it back into ViPR.

Before you begin

This operation requires the System Administrator role in ViPR.
The virtual array must have no associated storage pools or networks.

Procedure

1. Select **Admin** › **Physical Assets** › **Virtual Arrays**.
2. Select a virtual array and **Delete**.

Adding a network to a virtual array

Add a discovered Fibre Channel network or an IP network to a virtual array.

Before you begin

This operation requires the System Administrator role in ViPR.

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.

Procedure

1. Select **Admin** › **Virtual Assets** › **Virtual Arrays**.
2. Locate the virtual array to which to add the network.
3. Click **Networks** in the virtual array row.
4. From the Networks page, click:

Option	Description
Add	To choose from the list of available Fibre Channel, or IP networks to add to the virtual array

Option	Description
Add IP Network	To create a new IP network to add to the virtual array. a. From the **Add IP Network** page, enter the name of the network. b. Leave the virtual array name checked, and select any other arrays to which to add the network. c. Click **Save**.

The added networks appear in the list of networks for the virtual array.

Removing a network from a virtual array

Removing the network does not delete the network from ViPR, it removes the network from a virtual array. If the network is assigned to multiple virtual arrays, the network will remain in the other virtual arrays until it is removed.

Procedure

1. Go to the **Admin** › **Virtual Assets** › **Virtual Arrays** page.
2. Locate the virtual array from which the network will be removed.
3. Click **Networks** in the virtual array row.
4. From the Networks page, select the network to remove, and click **Remove**.

Storage Ports

Use the **Admin** › **Virtual Assets** › **Virtual Arrays** › **Storage Ports** page to view the attributes of the storage ports assigned to the virtual array, assign storage ports to the virtual array, or remove the storage ports from the virtual array.

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 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.

Best practices

If planning for File System exports:

- Assign at least one port to the file storage system in the virtual array.
- The same port that is assigned to the virtual array must be assigned to a network.
- If exporting to a host, the host and port must be on the same network.
- Optionally, the network can also be assigned to the virtual array, but it is not required.

Editing the virtual array storage ports

By default storage ports are automatically registered with ViPR when the storage system is discovered. To add or remove a discovered storage port from a virtual array:

1. Go to the **Admin** › **Virtual Assets** › **Virtual Arrays** page.
2. Locate the virtual array to which to add the storage ports.
3. Click **Ports** in the Edit column for the virtual array.
4. Click **Add** to add storage ports to the virtual array, or
   Select a storage port from the list, and click **Remove**, to remove the storage port assignment to the virtual array.

Storage Pools

Use the **Admin** › **Virtual Assets** › **Virtual Arrays** › **Storage Pools** page to manually assign specific physical storage pools to a virtual array, or remove the storage pool assignment from the virtual array.

Storage Pool attributes

When displayed for a specific virtual array, the **Storage Pools** page, lists the storage pools assigned to the virtual array and the following storage pool attributes.

Column name	Description
Name	The storage pool name.
Storage system	The storage systems to which the pool is associated.
Provisioning	Provisioning type either Thin or Thick.
Drive Types	The supported drive types.
Free (GB)	Amount of free storage space, in gigabytes, currently available in the storage pool.
Subscribed (GB)	The total amount of usable space that is configured in the pool and presented to attached hosts (GB)
Total (GB)	The size, in gigabytes, of the storage pool.
Assigned	The virtual arrays, if any, to which the storage pool has been assigned.
Registered	If checked, the storage pool is registered for use in ViPR. If empty, the storage pool is discovered in ViPR, but cannot be used as a ViPR resource. **Note** If a storage pool becomes unavailable on the storage system, the storage pool remains in the list of available ViPR storage pools. The storage pool must be manually deregistered in ViPR to ensure it is not used in a service operation.

Editing the storage pools assigned to a virtual array

To assign storage pools to a virtual array, or remove the storage pool assignment from the virtual array:

1. Go to the **Admin** › **Virtual Assets** › **Virtual Arrays** page.
2. Locate the virtual array from which to add or remove the storage pools.
3. Click **Pools** in the **Edit** column for the virtual array.
4. Click **Add** to add storage ports to the virtual array, or

Select a storage port from the list, and click **Remove**, to remove the storage port assignment to the virtual array.

Virtual pools

Virtual pools are created after virtual arrays have been created in ViPR. Virtual pools must be associated with one or more virtual arrays.

Virtual pools are a collection of storage pools grouped together according to user-defined characteristics.

For example, if your virtual array has a number of storage pools that can provide block storage using SSDs, you can group those physical pools into a single virtual pool. In that case, the performance and protection characteristics of the virtual pool would determine that it provides high performance storage. Hence, when giving a name to the virtual pool, you might choose "gold" or "tier1" to indicate that the storage provides the highest performance.

When a provisioning user requests the creation of a block volume from the "gold" virtual pool, ViPR chooses the physical array/physical storage pool combination on which the volume will be created. The virtual pool can comprise physical pools spanning a number of arrays, so the actual array chosen could be any of them. The provisioning user does not care which physical pool is chosen, only that it provides the level of performance consistent with "gold" storage.

Automatic and manual virtual pools

When creating or editing a virtual pool, the UI helps you choose the physical pools that match the performance and protection criteria that you are looking for by providing a set of criteria and listing the pools that match the criteria. The storage pools table list all of pools that are currently available that match the criteria and is dynamically updated as you make criteria selections.

If you set the pool to be a "manual" pool, you can select the storage pools that will comprise the pool. These storage pools will be fixed unless you edit the virtual pool.

If you select "automatic", the storage pools that comprise the virtual pools will be automatically updated during the virtual pool's lifetime based on the availability of storage pools in the virtual array.

An automatic virtual pool will be updated under the following circumstances:

- During discovery of a storage system.
- When a virtual pool is updated and saved (once a pool has associated assets only protection criteria can be updated).
- When a storage system, storage pool or port is registered or deregistered.
- When the storage ports for a network are updated.
- When the storage pools in a virtual array are updated.
- When a network is assigned to a virtual array.

Virtual Pools

Use the **Admin** › **Virtual Assets** › **Virtual Pools** page to view, create, edit, and delete virtual pools.

The **Virtual Pools** page lists the virtual pools and the following virtual pool attributes.

Table 14 Virtual Pool attributes

Column name	Description
Name	The virtual pool name.
Description	Description of the virtual pool.
Type	Lists types of storage (Block or File) and provisioning (Thin or Thick) criteria defined in the pool.
Pool Assignment	Options are: • Automatic 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. • Manual Storage pools are manually assigned to the virtual pool. These storage pools will be fixed unless manually edited.
Protocols	For • Block storage options are FC and iSCSI. • File storage options are CIFs or NFS.
Pools	Number of storage pools included in the virtual pool.
Resources	The number of times the virtual pool is used in a service.

Creating a virtual pool

Use the **Create Virtual Pools** page to create a virtual pool.

Before you begin

This operation requires the System Administrator role in ViPR.

Procedure

1. Depending on whether you want to create a block or file virtual pool, choose:
   - Creating or editing a block virtual pool on page 68
   - Creating or editing a file virtual pool on page 72

Creating or editing a block virtual pool

Create a virtual pool for block by specifying the criteria that physical storage pools must match.

Before you begin

This operation requires the System Administrator role in ViPR.

Once a virtual pool has been used as the target for ViPR resources, any attempt to modify the pool will fail.

Procedure

1. Select **Admin** › **Virtual Assets** › **Virtual Pools**.
2. Click **Add** or select an existing virtual pool name to edit.

3. Enter a name and a description for the virtual pool.

   The virtual pool will be the target for all provisioning operations, so its name should convey some information about the type of storage that it provides (its performance and protection levels) or how it should be used. For example, "gold", "tier1", or "backup" etc.

4. Select the type of storage that the pool will provide. In this case, block.

   Once a virtual pool has been created, the pool type cannot be changed, it will always be a file or block pool.

5. Select the provisioning type that the pool will support: thick or thin.

6. Select the virtual arrays for which the virtual pool will be created.

7. Select the Block Storage criteria. It is recommended to change the criteria one at a time and then scroll down and check the storage pools table to see which matching pools 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.

Parameter	Description
Protocols	The block protocols supported by the physical storage pools that will comprise the virtual pool. Possible protocols are FC and iSCSI. Only the protocols supported by the virtual array networks are listed.
Minimum Paths	Minimum number of paths from the host to the storage array.
Maximum Paths	The maximum number of paths that can be configured per host.
Paths per Initiator	The number of paths (ports) to allocate to each initiator that is used. ViPR will not allocate more paths than the Maximum Path allows. When the Maximum Path is set too low there may be unused initiators which will not be zoned to ports.
Expandable	When enabled: • Volumes can be expanded non-disruptively. **Note** In some cases this may cause a decrease in performance. • Native continuous copies will not be supported. When disabled, the underlying storage selected for volume creation will consider performance over expandability.
Multi-Volume Consistency	When enabled, resources provisioned from the pool will support the use of consistency groups. If disabled, a resource cannot be assigned to a consistency group when running ViPR block provisioning services.
Drive Type	The drive type that any storage pools in the virtual pool must support. One of: SSD, FC, SAS, SATA.

Parameter	Description
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 other selected criteria. Only the systems supported by the networks configured in the virtual array are selectable.

8. Select the Data Protection/High Availability criteria. It is recommended to change the criteria one at a time and then scroll down and check the storage pools table to see which matching pools 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.

Parameter	Description
Maximum Native Snapshots	Maximum number of local snapshots allowed for resources from this virtual pool. To use the ViPR Create Snapshot services, a value of at least 1 must be specified.
Maximum Native Continuous Copies	Maximum number of native continuous copies allowed for resources from this virtual pool. To use the ViPR Create Continuous Copy services a value of at least 1 must be specified.
Native Continuous Copies Virtual Pool	Enables a different virtual pool to be specified which will be used for native continuous copies. Native continuous copies are not supported for virtual pools with the expandable attribute enabled.
Remote Protection	Enables volumes created in the virtual pool to be protected by a supported protection system. The possible values are: None EMC RecoverPoint (see Setting RecoverPoint data protection criteria for a block virtual pool on page 71) VMAX SRDF (see Setting SRDF data protection criteria for a block virtual pool on page 71 VPLEX Distributed (see Adding VPLEX support for virtual pool recovery on page 72) VPLEX Local (see Adding VPLEX support for virtual pool recovery on page 72)

9. Enable Quota to enter a value for the maximum storage that can be provisioned from the pool.
10. 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.

11. Select **Save**.

Setting RecoverPoint data protection criteria for a block virtual pool

You can set RecoverPoint criteria when you create or edit a block virtual pool.

Before you begin

- This operation requires the System Administrator role in ViPR.
- RecoverPoint data protection is part of the block virtual pool settings, so you need to be creating or editing a block virtual pool to do these steps. Refer to Creating or editing a virtual pool for block storage type.
- You need a virtual array to act as the RecoverPoint target and optionally an existing target virtual pool.
- ViPR sets a default journal size, but if you have specific journal requirements, have them available when creating the virtual pool.

Procedure

1. Select **Admin** › **Virtual Assets** › **Virtual Pools**.
2. Click **Add** or select an existing virtual pool name to edit.
3. Set properties as described in Creating or editing a virtual pool for block storage type.
4. For **Remote Protection/Availability**, select EMC RecoverPoint.
5. Set the source journal size as needed. You can accept the RecoverPoint default (2.5 times protected storage) or select one of the following:
   - A fixed value (in MB, GB or TB)
   - A multiplier of the protected storage
   - Minimum allowable by RecoverPoint (10 GB)
6. Select **Add Copy** to add one or two RecoverPoint copies, specifying the destination virtual array, optionally a virtual pool, and journal size.

   The virtual pool specifies the characteristics of the RecoverPoint target and journal volumes.

   - Set the journal size as needed. You can accept the RecoverPoint default (2.5 times protected storage) or select one of the following:
     - A fixed value
     - A multiplier of the protected storage other than the default
     - Minimum allowable by RecoverPoint (10 GB)

Setting SRDF data protection criteria for a block virtual pool

You can set SRDF criteria when you create or edit a block virtual pool.

Before you begin

- This operation requires the System Administrator role in ViPR.
- SRDF data protection is part of the block virtual pool settings, so you need to be creating or editing a block virtual pool to do these steps. Refer to Creating or editing a virtual pool for block storage type.
- You need a virtual array to act as the SRDF target and optionally an existing target virtual pool.

Procedure

1. Select **Admin** › **Virtual Assets** › **Virtual Pools**.

2. Click **Add** or select an existing virtual pool name to edit.
3. Set properties as described in Creating or editing a virtual pool for block storage type.
4. For **Remote Protection/Availability**, select **VMAX SRDF**.
5. Select a copy mode, either **Synchronous** or **Asynchronous**.
6. Select **Add Copy** to add an SRDF copy, specifying the destination virtual array, and optionally a virtual pool.

Adding VPLEX support for virtual pool recovery
A block virtual pool can be protected by a local or remote VPLEX system.

Before you begin

This operation requires the System Administrator role in ViPR.

Procedure

1. At the **Admin** › **Virtual Assets** › **Virtual Pools** page, locate the **Data Protection** › **Remote Protection** field.
2. In the Remote Protection field, select VPLEX Local or VPLEX Distributed. If you select VPLEX Distributed, you will need to:
   a. Select the ViPR virtual array that will provide the destination for the distributed volume.
   b. Select the ViPR virtual pool that will be used when creating the distributed volume.
3. Select **Save** to save the VPLEX protection settings in the virtual pool.

Creating or editing a file virtual pool

Create a virtual pool for file by specifying the criteria that physical storage pools must match.

Before you begin

This operation requires the System Administrator role in ViPR.

Once a virtual pool has been used as the target for ViPR resources, any attempt to modify the pool will fail.

Procedure

1. Select **Admin** › **Virtual Assets** › **Virtual Pools**.
2. Click **Add** or select an existing virtual pool name to edit.
3. Enter a name and a description for the virtual pool.

   The virtual pool will be the target for all provisioning operations, so its name should convey some information about the type of storage that it provides (its performance and protection levels) or how it should be used. For example, "gold", "tier1", or "backup" etc.
4. Select the type of storage that the pool will provide. In this case: file.

   Once a virtual pool has been created, the pool type cannot be changed, it will always be a file pool.
5. Select the provisioning type that the pool will support: thick or thin.
6. Select the virtual array for which you want to create a virtual pool.
7. Begin the criteria selection by selecting the protocol(s) that the physical storage pools must support to be included in the virtual pool. Possible protocols are CIFS and NFS.

Only the protocols supported by the IP networks that provide file system storage will be listed.

It is recommended that you change the criteria one at a time and then check the storage pools table to see which matching pools are available.

You will see that 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.

8. Select 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 selected protocols.

   Only the systems supported by the IP networks configured in the virtual array are selectable.

9. Now scroll down to the Storage Pool Association area and choose how you want storage pools to be assigned to the virtual pool: Automatic or Manual.

   If you select Automatic (the default) from the Pool Assignment menu, 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 because new storage pools that meet the criteria are added or removed from the system, or their registration or discovery status changes.

   Selecting Manual provides a checkbox against each pool to enable it to be selected. Only pools that you select will be included in the virtual pool.

10. If you want to set a quota for the pool, select Enable Quota and enter a value for the maximum storage that can be provisioned from the pool.

11. Finally, set the maximum number of local snapshots allowed for resources from this virtual pool.

    To use the ViPR Create Snapshot services, a value of at least 1 must be specified.

12. Select **Save**.

Deleting a virtual pool

You can delete a virtual pool if there are no resources using it.

Before you begin

This operation requires the System Administrator role in ViPR.
You must delete all resources being used by the virtual pool.

Procedure

1. Select **Admin** › **Virtual Assets** › **Virtual Pools**.
2. Select a virtual pool and **Delete**.

Networks

ViPR networks provide the connectivity between the components of a ViPR virtual array.

A network maps to physical switch connectivity. A network maps to each VSAN/fabric discovered on a switch and its collection of endpoints. Endpoints include the storage system ports, and host ports (initiator ports on a host ESX server) to which the switch is connected.

When configuring networks for ViPR it is helpful to understand that:

- Fibre Channel networks are automatically discovered, and registered when a Fabric is added to the ViPR physical assets.

- Networks for IP connected storage must be manually created, and added to the virtual array.

Networks

Use the **Admin** › **Virtual Assets** › **Networks** page to view, create, edit, and delete networks.

The **Networks** page lists the networks and the following network attributes.

Table 15 Network attributes

Column name	Description
Name	The network name.
Type	The type of network is either Fibre Channel or IP.
Discovered	If checked, the network was discovered. If empty, the network was created in ViPR. • Fibre Channel networks are automatically discovered, and registered when a Fabric is added to the ViPR physical assets. Fibre Channel networks can be unregistered in ViPR, but not deleted. • IP networks must be manually created and registered with ViPR.
Registered	If checked, the network is registered. If empty, the network was discovered or added to ViPR, but is not registered to be used by ViPR. • Fibre Channel networks are automatically discovered, and registered when a Fabric is added to the ViPR physical assets. Fibre Channel networks can be unregistered in ViPR, but not deleted. • IP networks must be manually created and registered with ViPR. Once registered the IP network can be unregistered, and deleted as long as it is not being used by any other ViPR resource.
Virtual Array	The list of virtual arrays to which the network is assigned. **Note** This column displays when no virtual array is selected.

Adding an IP network

Networks for IP connected storage must be manually created, and added to the virtual array.

Before you begin

- This operation requires the System Administrator role in ViPR.
- There are two ways to access the IP networks page either

Procedure

1. Go to the **Add IP Networks** page:

Option	Description
From the Networks page	a. Go to the **Admin** › **Virtual Assets** › **Networks** page.

Option	Description
	b. Click **Add IP Network**.
From the Virtual Array page	a. Go to the **Admin** › **Virtual Assets** › **Virtual Arrays** page. b. Click **Networks** in the **Edit** column. c. Click **Add IP Network**.

2. Enter the network **Name**.
3. Select the virtual arrays to which the network will be added.
4. Click **Save**.

Edit networks

Editing networks includes making any one of the following changes: changing the network name, changing the virtual array assignment, adding or removing network ports, adding or removing host ports from the network, and adding and removing array ports from the network.

Before you begin

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.

Procedure

1. Go to the **Admin** › **Virtual Assets** › **Networks** page.
2. Click the name of the network to edit.
3. Optionally, make changes to any one of the following settings:
   a. **Name**.
   b. Select additional virtual arrays to which to assign the network.
   c. Unselect the virtual arrays from which to remove the networks.
   d. Click **Add** to add the Fibre Channel ports if editing a Fabric network, or IP ports if editing an IP network.
   e. Click the arrow next to the **Add** button to add **Host Ports** or **Array Ports** to the network.
   f. Select the ports in the list and click **Remove** to remove them from the network.
4. Click Save.

Registering a network

Register newly created IP networks or deregistered Fibre Channel networks in ViPR to make them available to use in a service.

Before you begin

- IP networks must be registered after they are created. Fiber Channel networks are automatically discovered and registered after the Fabric is added to the ViPR physical assests.
- This operation requires the System Administrator role in ViPR.

Procedure

1. Go to the **Admin** › **Virtual Assets** › **Networkds** page.
2. Select the checkbox for the network to register.
3. Click **Register**.

Deregistering a network

Deregistering a network keeps the network in the ViPR virtual assets but it will no longer be available to use in a service. Deregistering a network will deregister any storage system ports and initiator ports provided by the network from a virtual array that it is used in.

Before you begin

This operation requires the System Administrator role in ViPR.

Procedure

1. Go to the **Admin** › **Virtual Assets** › **Networkds** page.
2. Select the checkbox for the network to deregister.
3. Click **Deregister**.

Deleting a network

Deleting the network removes the network from ViPR permanently.

Before you begin

This operation requires the System Administrator role in ViPR.

Procedure

1. Go to the **Admin** › **Virtual Assets** › **Networkds** page.
2. Select the checkbox for the network to delete.
3. Click **Delete**.

CHAPTER 5

Importing Storage Resources into ViPR

This chapter contains the following topics:

Ingesting resources into ViPR

Existing block volumes and file systems can be brought under ViPR management by ingesting them using services provided in the Service Catalog. These services are for use by System Administrators only and are not visible to normal catalog users.

Once under ViPR management, the ingested storage resources can be managed by provisioning users in the same way as if they had been created using ViPR, allowing them to be exported to hosts, expanded, protected using snapshot and copy techniques, etc.

Discover unmanaged volumes

Finds volumes within a virtual pool which are not under ViPR management.

Before you begin

The following prerequisites are applicable:

- This operation requires the System Administrator role in ViPR.
- The virtual array and virtual pool into which you want to ingest the storage pools must exist when the discovery is performed.

  The discovery process finds storage pools on a selected storage system and identifies the virtual array and virtual pool that each array matches with.

Procedure

1. Select **User** › **Service Catalog** › **Block Storage Services** › **Discover Unmanaged Volumes**.
2. Select the physical block storage system on which you want to discover unmanaged volumes. You can select more than one storage system.
3. Select **Order**.

   The orders page is displayed and shows the progress of the request. If the order is successfully fulfilled, you can use the Ingest Unmanaged Volumes to bring them under management by ViPR.

Ingest unmanaged volumes

Imports unmanaged block volumes, which have previously been discovered, into ViPR. The unmanged volumes must be in virtual pools associated with the virtual array from which to ingest.

Before you begin

- This operation requires the System Administrator role in ViPR.
- To be ingested, the unmanged volumes must be in physical pools which are already associated with a ViPR virtual pool.
- The Discover Unmanaged Volumes service must have been run on the array from which the block volumes will be ingested.
- If the virtual array or virtual pool has been modified since the last time the unmanaged volumes were discovered, rerun the discovery prior to running the Ingest unmanaged volumes service, to ensure volumes are assigned to the correct virtual array and virtual pool.
- ViPR will only ingest volumes that are not exported to hosts. Remove the unmanaged exported volumes from the masking view to ingest them into ViPR.

- Ingested volumes will be assigned to a project. You must belong the selected project and have write-permission on the project.

Procedure

1. Select **User › Service Catalog › Block Storage Services › Ingest Unmanaged Volumes**.
2. Select the storage system from which you want to ingest block volumes.
3. Select a virtual array that contains physical array storage pools that you want to import. The storage system might contribute physical storage pools to a number of virtual pools. If you want to ingest from all virtual pools you will need to run the service again for the other virtual pools.

   It is possible that not all of the array physical pools are included in the virtual array or arrays that form part of your virtual data center. For that reason, you don't want to ingest all unmanged block volumes on the array, just those in physical array pools that form part of the virtual array.
4. From the array physical storage pools that form part of the virtual array, select the virtual pool that the unmanged volumes are in.
5. Select the project that you want the unmanaged volumes to be assigned to.
6. Select **Order**.

   The orders page is displayed showing the progress of the request. If the order is successfully fulfilled, you can look at the **User › Resources** page to see the imported volumes.

After you finish

Once the unmanaged volumes have been ingested into ViPR:

1. Export the volumes to either a Windows or Linux host using the following service. **User › Service Catalog › Block Storage Services › Export Volume to Host**.
2. Mount the volumes on a host:
   - For Linux hosts use: **User › Service Catalog › Block Service for Linux › Mount Existing Volume on Linux**.
   - For Windows hosts use: **User › Service Catalog › Block Service for Windows › Mount Existing Volume on Windows**.

Discover unmanaged file systems

Finds file systems which are not under ViPR management.

Before you begin

The following prerequisites are applicable:

- This operation requires the System Administrator role in ViPR.
- The virtual array and virtual pool into which you want to ingest the storage pools must exist when the discovery is performed.

  The discovery process finds storage pools on a selected storage system and identifies the virtual array and virtual pool that each array matches with.
- File systems will only be discovered on file storage system that have been added to ViPR as physical assets.

Procedure

1. Select **User › Service Catalog › File Storage Services › Discover Unmanaged File Systems**

2. Select the physical file storage systems from which you want to discover unmanaged file systems. You can select more than one array.
3. Select **Order**.

   The orders page is displayed and shows the progress of the request. If the order is successfully fulfilled, you can use the Ingest Unmanaged File Systems to bring them under management by ViPR.

Ingest unmanaged file systems

Imports unmanaged file systems, which have previously been discovered, into ViPR.

Before you begin

The following prerequisites are applicable:

- This operation requires the System Administrator role in ViPR.
- To be ingested, the unmanged file systems must be in physical pools which are already associated with a ViPR virtual storage pool.
- The Discover Unmanaged File Systems service must have been run on the virtual array.
- Rerun the Discover Unmanaged File Systems service if:
  - ViPR was upgraded from version 1.0, to ensure that the list of discovered unmanaged file systems is updated.
  - The virtual array or virtual pools have been modified since the last time the Discover Unmanaged File Systems service was run.
- Ingested file systems will be assigned to a project. You must belong to the selected project and have write-permission on the project.

Procedure

1. Select **User › Service Catalog › File Storage Services › Ingest Unmanaged File Systems**
2. Select the storage system from which you want to ingest file systems.
3. Select the virtual array whose virtual pools contain the storage system physical pools that host the file systems you want to import. The storage system might contribute physical storage pools to a number of virtual pools. If you want to ingest from all virtual pools, you will need to run the service again for the other virtual pools.

   It is possible that not all of the storage system physical pools are included in the virtual array that forms part of your virtual data center. For that reason, you don't want to ingest all unmanged file systems on the storage system, just those in physical storage pools that form part of the virtual pools of the virtual array.
4. Select the virtual pool that the unmanaged volumes are in.
5. Select the project that you want the unmanaged file systems to be assigned to.
6. Select **Order**.

   The orders page is displayed showing the progress of the request. If the order is successfully fulfilled, you can look at the **User › Resources** page to see the imported volumes.

CHAPTER 6

Configuring ViPR Data Services

This chapter contains the following topics:

Data Services overview

ViPR currently supports object and HDFS storage backed by ViPR managed file systems. Storage created for use by Data Services can support object services, the HDFS service, or both object and HDFS.

Unlike block and file storage managed by ViPR, data is written to and read from ViPR object and HDFS storage by calling ViPR APIs, and the object data passes through the ViPR system. To support this data path, one or more data services VMs must be added to the ViPR cluster. The Data Services area of the ViPR UI supports most of the initial configuration required to prepare Data Services for use by object and HDFS storage clients.

A core concept of ViPR is the use of virtual pools. In the context of object and HDFS storage, a virtual pool is a pool that comprises one or more data stores, where each data store is backed by a file virtual pool. Hence, when a Data Services client creates a bucket (the object world equivalent of a directory) within a data services virtual pool, the actual file system that provides the bucket could be located on any of the data stores that comprise the virtual pool. A data services virtual pool can be designated for use by object services, by HDFS services, or by both object and HDFS services. When creating a data services virtual pool, you must have the appropriate license installed to support the chosen mode of operation. For example, if you want to use the data services virtual pool for HDFS data only, you must have an HDFS license installed.

The Data Services area of the UI enables the ViPR virtual data center to be configured to support object and HDFS storage, and enables the creation of data services virtual pools for the virtual data center. The data services virtual pools are available to all tenants in a virtual data center. To ensure that objects belonging to a tenant can be differentiated, each tenant can be assigned a namespace. The Data Services area supports setting the namespace for the root tenant, the API or CLI must be used to perform namespace configuration for additional tenants.

The creation of buckets within a data services virtual pool, and the storage of objects within the buckets, is performed by clients that talk to ViPR through its API. ViPR supports Atmos, Amazon S3, and OpenStack Swift APIs, so existing clients that use those protocols can hook into ViPR and begin managing object storage. When an object needs to be modified, the ViPR API enables it to be accessed natively or can supply its location on the underlying file system to allow it to be read and written as a file.

In addition to configuring object and HDFS storage, the Data Services area of the UI also guides an administrator through the addition of data VMs to a ViPR system.

The ViPR Data Services configuration and initialization areas are listed in the table below and can be used in the order presented to perform configuration.

Table 16 Object Data Service configuration and initialization

Configuration	Description
Data Services setup on page 83	Specifies the arrays which can provide the file systems that back the object storage. This is done by specifying an IP network. Provides guidance on the addition of one or more data nodes to the ViPR cluster and enables the download of the controller node configuration file (in ISO form).

Table 16 Object Data Service configuration and initialization (continued)

Configuration	Description
Virtual pool creation on page 87	Enables the creation of data services virtual pools to support Object, HDFS, or Object + HDFS services.
Data store creation on page 88	Enables the creation of data stores and their association with a virtual pool. A data store is backed by ViPR-managed file systems.
Tenant configuration on page 90	Describes the configuration of a tenant. Most importantly this enables a namespace to be assigned to the tenant. In addition, it is possible to specify the default object pool and project that will be used for the tenant. **Note** To perform configuration of tenants other than the primary tenant, it is necessary to perform this configuration stage using the CLI.
Base URL configuration on page 92	Configures the URL that will be used to access data objects in the tenant. This configuration is only required if you need to allow applications that encode the location of an object in a URL, such as Amazon S3, to access ViPR the Object Data Service.

Once you have configured the data services, object storage end-users, who are members of the ViPR security domain for the tenant (are ViPR users), can obtain an object store key at the ViPR UI, from the **User menu** › **Manage Data Store Keys** tab.

Applications that access ViPR object storage can request an object store key using the ViPR API.

Data Services setup

The Data Services setup page is the first page in the sequence of pages designed to guide you through the steps required to set up the Data Services. The pages are arranged so that you can work through them from left to right to complete the setup.

The setup page enables selection of the IP network that connects the file storage systems that you intend to use to support object storage, and provides guidance on deploying and configuring one or more data node VMs to supply the object storage data path.

In addition to the System Administrator role required to access the Data Services area, two further roles are required to complete the setup pages: Security Administrator and Tenant Administrator. The root user account has all of the required roles. Alternatively, the Security Administrator can assign these roles to a specific user who can perform the configuration.

If a network that provides file storage has not been configured, it must be created before it can be selected for used by Data Services. In addition, at least one file virtual pool must be created which will be used to provide the object data stores.

The following topics describe these prerequisite steps:

- Create an IP network that contributes file storage to the virtual array (Adding an IP network on page 74).
- Create a file virtual pool (Creating or editing a file virtual pool on page 72).

The tasks that you need to perform on each page in the data service configuration procedure are described after the overview of the page.

There is one additional step if you are using EMC Isilon. You need to configure your DNS server to delegate resolution of the Isilon SmartConnect name to the SmartConnect service. The SmartConnect service will return the IP address to be used to connect to the Isilon cluster based on the load balancing policy that has been selected.

Choosing an IP network to support Data Services

Select the IP network that provides the file storage systems that underpin Data Services. If an IP network that provides file storage does not exist, create it.

Before you begin

This operation requires the System Administrator role in ViPR.

Procedure

1. Select **Admin** › **Data Services** › **Setup**.
2. In the Network Configuration area, select the network that you want to provide the virtual arrays used by the data services.

   If you have not configured a network, you can do it from the **Admin** › **Virtual Assets** › **Virtual Arrays** page by selecting a virtual array and using **Create IP Network**.
3. Select **Save**.

Configuring the ViPR controller to allow access by data VMs

Before you deploy data VMs, the addresses of the data VMs must be specified in the ViPR controller node configuration to allow each data node to connect to the Controller services.

Before you begin

This operation requires the Security Administrator role in ViPR.

Allocate IPv4 addresses for all data nodes that you intend to add. If you create a subnet for the data VMs, you can use the subnet address. Using a subnet enables you to add data VMs without having to perform this procedure.

The Controller node needs to know which data VMs it will access so that these nodes are allowed to connect through its firewall to access the controller node coordination services.

This configuration must be in place when the data VM first starts. If it is not, the data VMs need to be restarted, one by one, after the data node addresses are added.

Procedure

1. Select **Admin** › **System** › **Configuration**.
2. In the **Network** › **Data Services** area of the Configuration page, enter the IPv4 address of the data node VMs that you are adding in the Data VM IPs field. If you are adding

more than one, enter all addresses in a comma separated list. Alternatively, if you have created a new subnet for the data VMs, enter the subnet address.

3. Select **Save**.

Deploying ViPR data VMs

For Data Services (object and HDFS storage) support, you need to deploy data VMs in addition to the ViPR Controller VMs.

Before you begin

- The ViPR virtual appliance to which you are adding data VMs must already be deployed.
- The IPv4 address or hostname of all data VMs must have been added to the controller node configuration using the procedure in Configuring the ViPR controller to allow access by data VMs on page 84.
- If you are deploying the data node(s) immediately after deploying the ViPR virtual appliance, wait until the ViPR virtual appliance status on the Dashboard tab says "Stable" (about 2 minutes).
- The ESX host to which the data VM is deployed must meet the prerequisites listed below.

Table 17 ViPR data VM prerequisites

Item	Value
Number of CPUs	8
Memory	32 GB
Disk	150 GB
Connectivity	Ensure all data VMs have connectivity to each other.

- You need to be able to access the UI for the deployed ViPR virtual appliance.
- You need an available IPv4 address for each data VM and you need to know the subnet mask and gateway address for the data node.
- You need access to the ViPR data node VM distribution archive file.
- Refer to the *EMC ViPR Data Sheet and Compatibility Matrix* for the CPU, memory, and storage requirements of a data VM.

Procedure

1. Identify a working location that is accessible from the vCenter where you are deploying ViPR and put the files required to install the ViPR data node VM in this location.

   These comprise a dataservice OVF, the ViPR virtual machine disk files (VMDKs), and a configuration file that you download in this procedure. The working location does not need to be on a ViPR VM. You can use laptop storage, for example.

2. Extract the ViPR dataservice OVF file and the VMDK files from the distribution archive, `vipr-*-dataservice.zip`, to the working location.

   The files are `vipr-*-dataservice.ovf`, `vipr-*-disk1.vmdk`, `vipr-*-disk2.vmdk`, `vipr-*-disk4.vmdk`, and `vipr-*-dataservice.mf`.

3. Open a web browser window on https://*ViPR_virtual_ip* to run the ViPR UI.
4. Log in to the UI as a user who has the System Administrator role and the Security Administrator role. The root user has these permissions or the Security Administrator can assign these roles to a user.

   The System Administrator role is required to access the Data Services area of the UI. The Security Administrator role is required due to the need to download a file containing secure configuration information.
5. Select **Admin** › **Data Services** › **Setup**.
6. Under Data Services Configuration, download the Data Services configuration file (`config.iso`).

   If you have a previously downloaded `.iso` file, do not use it if you have made any controller node configuration changes since it was downloaded. Use a newly downloaded `.iso` file.

   During deployment, the ISO image is mounted by vCenter and configuration information required by the data node VM is obtained. This information comprises the addresses and ports of the controller node services that the data node needs to access.
7. Using an OS command, file browser, or the like (not the ViPR UI), copy `config.iso` from the download location to the working location where the OVF file and VMDK files reside.
8. Log in to vCenter using the vSphere client and deploy `vipr-*-dataservice.ovf` for each data VM using the following steps.
   a. From the **File** menu, select **Deploy OVF Template...**.
   b. Browse to and select the dataservice OVF file, located in the working location created earlier.
   c. On the **OVF Template Details** page, review the details about the data node VM.
   d. Accept the End User License Agreement.
   e. Enter a name for the data node VM and select its location.
   f. Select the host or cluster that hosts the VM.

      If you selected a host or cluster before starting the deployment, you are not be offered this selection.
   g. Select a resource pool for the VM.

      If you selected a resource pool before starting the deployment, you are not be offered this selection.

      When selecting the resource pool, do not select the controller vApp.
   h. If more than one datastore is attached to the ESX host, select the datastore for your VM.
   i. Select a disk format: **Thick Provision Lazy Zeroed**, **Thick Provision Eager Zeroed** (recommended for production deployment), or Thin Provision.
   j. On the **Network Mapping** page, map the source network to a destination network as appropriate.
   k. Enter the properties for the VM.

Table 18 ViPR data node VM OVF properties

Property name in vSphere Client	OVF property key name	Description
Data service IP address	network_datanode_ipaddr	One IPv4 address for the data VM.
Data service network netmask	network_datanode_netmask	IPv4 netmask for the data VM.
Data service network gateway IP address	network_datanode_gateway	IPv4 address for the data VM.

l. Review the selections you have made at the **Ready to Complete** page and select **Finish**.

9. Once the deployment has completed successfully, start each data node VM, one at a time, and check to see that the data node VM appears in the ViPR Virtual Appliance area of the UI Dashboard: **Admin** › **System** › **Dashboard**.

ViPR data VM prerequisites

A data VM requires an available IPv4 address and has its own CPU, memory, and storage requirements.

Table 19 ViPR data VM prerequisites

Item	Value
Number of CPUs	8
Memory	32 GB
Disk	150 GB
Connectivity	Ensure all data VMs have connectivity to each other.

Virtual pool creation

Objects are stored in data services virtual pools and each pool must have at least one data store to provide the underlying file system storage.

The ViPR portal provides a Virtual Pools page (**Admin** › **Data Services** › **Virtual Pools**) which enables the creation of a data services virtual pool. The virtual pool created is available to all tenants in ViPR. However, you can set a default virtual pool for the tenant which will be used if the object storage client does not specify a virtual pool.

The **Virtual Pool** page provides a virtual pools table which displays the pools that have been created. The table shows the number of data stores that have been created for the virtual pool and shows the description of the store.

You can refer to the data stores table on **Admin** › **Data Services** › **Data Stores** to see details of the data stores in a particular virtual pool.

Adding a data services virtual pool

Objects are stored in data services virtual pools and each pool must have at least one data store to provide the underlying file system storage.

Before you begin

The following prerequisites apply:

- This operation requires the System Administrator role in ViPR.
- You must know whether the pool will be used for object, HDFS, or both object and HDFS data.

Procedure

1. Select **Admin** › **Data Services** › **Virtual Pools**.
2. Enter a name for the virtual pool.
3. Optional. Enter a description for the virtual pool.

   When the virtual pool has been created, the object description will be displayed on the **Virtual Pools** page.
4. Select the Type of the virtual pool. The type is either: Object (default), HDFS, or Object and HDFS.
5. Select **Save**.

   The virtual pool will be displayed on the **Admin** › **Data Services** › **Virtual Pools** page.

After you finish

A data services virtual pool must have a data store before it can be used. This applies even when you are intending to ingest data into object storage - a process which adds the ingested file system as a data store.

Editing a data services virtual pool

You can edit the name and description of a data services virtual pool.

Before you begin

This operation requires the System Administrator role in ViPR.

Procedure

1. Select **Admin** › **Data Services** › **Virtual Pools**.
2. Click on the name of the data services virtual pool in the Virtual Pools table to open it for editing.
3. Edit the name and description for the virtual pool.
4. Select **Save**.

Data store creation

Each data services virtual pool comprises one or more data stores each of which is backed by a VIPR-managed NFS export file system.

The ViPR portal provides a Data Stores page (**Admin** › **Data Services** › **Data Stores**) which provides the ability to add, edit, and delete data stores. The page displays a data store table which shows the details of each of the data stores: the data services virtual pool it belongs to, the file virtual pool that underpins the data store, its total capacity, the amount of storage unused, and the description of the data store.

If you edit a data store, you will only be given the option of changing the name and description, the file virtual pool used by the data store, or data services virtual pool that it is assigned to, cannot be changed.

Adding a data store

A data services virtual pool must be backed by one or more data stores, each of which is associated with an underlying file system.

Before you begin

This operation requires the System Administrator role in ViPR.

Procedure

1. Select **Admin** › **Data Services** › **Data Stores**.
2. On the **Data Stores** page, select **Add**.
3. Enter a name for the data store.

   The data store name can reflect the underlying file system storage that provides the data store.
4. Optionally, add a description for the data store.
5. Select the virtual array that will provide the data store.

   The file virtual pools that you will be offered will be those associated with the selected array.
6. Select the file virtual pool that will provide the file system that underlies the data store.
7. Enter the size of the data store.
8. Select the data services virtual pool to which this data store belongs.

   When creating object buckets, clients do not know which data stores underpin a data services virtual pool. They choose the virtual pool based on its name.
9. Select **Save**.

Results

The state field in the Data Stores table should display "readytouse".

Editing a data store

You can edit the name and description of an object data store, but you cannot change the file virtual pool that underlies it, or the data services virtual pool with which it is associated.

Before you begin

This operation requires the System Administrator role in ViPR.

Procedure

1. Select **Admin** › **Data Services** › **Data Stores**.
2. Click on the name of the data pool in the Data Stores table to open it for editing.
3. Edit the name and description for the data store.
4. Select **Save**.

Tenant configuration

A tenant must be given a namespace, assigned a default data services virtual pool and, optionally, a default project.

The ViPR portal provides an **Admin** › **Data Services** › **Tenant Configuration** page which provides the following fields:

Tenant Namespace
This is the namespace for the tenant and is used to address object storage for the tenant. Object buckets created within ViPR data services virtual pools are segregated based on the namespace of the tenant. Hence, a bucket called "images", for example, can exist in more than one tenant and the correct one will be accessed by specifying the namespace for the tenant.

Default Virtual Pool
This is the default virtual pool in which to store, and from which to retrieve, objects, if the application accessing ViPR object storage does not provide the ability to choose a virtual pool.

Default Project
This is the project that will be used when creating and retrieving objects in ViPR. If the application accessing ViPR object storage does not provide a project for its user, the request will be authenticated assuming that the user is a member of this default project.

Note

To select a project, the administrator must be assigned to the Tenant Administrator role, or must be assigned project permissions by a Tenant Administrator. This requirement is in addition to the requirement to have the System Administrator role. The root user account has the required roles.

The **Admin** › **Data Services** › **Tenant Configuration** page can only be used to configure the root tenant. Procedures for configuring the root tenant are provided here:

- Configuring the root tenant to use Data Services on page 90

To configure a tenant other than root, refer to:

- Multiple Tenants on page 132

Configuring the root tenant to use Data Services

Enables the configuration of a namespace for the root tenant and configuration of default values for the data services virtual pool and the project to which object storage for this tenant should be assigned.

Before you begin

This operation requires the user to be assigned to more than one role, or to be assigned additional permissions:

- The System Administrator role is required to access the **Admin** › **Data Services** › **Tenant Configuration** area.
- The Tenant Administrator role, or ACL permissions for a project, is required in order to choose the default project.

The root user account has these roles and can be used to perform this task.

Procedure

1. Select **Admin** › **Data Services** › **Tenant Configuration**.
2. Enter the identity of the namespace to use for this tenant.

   The namespace must be unique for each tenant in the same ViPR virtual data center.
3. Select the default virtual pool. If a virtual pool has not been created yet, you can create one by selecting **Create Virtual Pool**.

   When using the Object Data Service, if a client does not specify a virtual pool, the contents of the default virtual pool that is visible to the logged in user will be returned by ViPR.
4. Select the default project that will be used when object requests are made.

   If you are a Tenant Administrator you will be able to select **Create Project** and create a new project. If you are a System Administrator with project permissions, you will be presented with a list of projects that you are assigned to, but you will not be able to create a new one.
5. Select **Save**.

Using the Object Data Service

Once you have configured data services, clients can access object storage using the ViPR API or using an existing object client, such as the S3 browser.

Steps are provided to enable you to demonstrate that the object service is configured, and that you can create buckets and store objects in the buckets using the S3 browser.

Object storage users are required to present an object data store key (also referred to as a secret key) to enable them to authenticate with the object service. Object data store keys can be generated programmatically by a client or can be generated manually from the ViPR UI.

Adding an object data store key

An object data store key can be created in the UI and used to access ViPR object storage.

Before you begin

Object store keys can be created by ViPR users who are domain users and have access to the UI.

Procedure

1. Select **User Menu** › **Manage Data Store Keys**.
2. Select **Add**.

   A new key will be added to the Data Store Keys table. An object user can have a maximum of 2 object data store keys. The key can be copied and used as the secret key when accessing the ViPR object stores using an object client.

Testing the object service using the S3 Browser

You can test your installation by creating an object bucket using the ViPR Amazon S3 API through the S3 Browser.

Before you begin

- You will need to have the S3 Browser installed.
- You will need an object data store key (a secret key) generated from the ViPR UI (refer to Adding an object data store key on page 91).

- You will need to have an authentication provider configured in ViPR so that one or more domain users are available.

Procedure

1. In the S3 Browser, select **Accounts › Add New Account**.
2. At the Add New Account dialog, enter the required details listed below.

Account Setting	Description
Account Name	The name of the account. This can be any name you choose.
Access Key Id	This is the name of the ViPR account. It must be the same account name that you used to generate an object store key. You can use the "root" user or any other available user. For the root user you would simply enter "root", for a normal ViPR user you would enter a name in the format: username@yourco.com.
Secret Access Key	This is the ViPR object store key that must be generated from the UI or by using the ViPR CLI or API. You can copy it from the ViPR UI and paste it into this field.

3. At the Add New Account Dialog, click **Advanced** (in the bottom left-hand corner).
4. Check the Use Amazon S3 Compatible Storage box.
5. Enter the hostname or IP address of the data node and specify the appropriate port for the S3 service. For https the port is 9021, for http it is 9020.

   For example: `mc1234.yourco.com:9021`
6. Select **Close**.
7. Complete the account creation by clicking **Add New Account**.
8. Select **Buckets › Create New Bucket**
9. Enter a name for the bucket and specify a region.
10. Select **Create New Bucket**.

Results

You can now upload files to the bucket.

Base URL configuration

The namespace and bucket that refer to the location of an object can be specified in the x-emc-namespace header of an HTTP request. However, where an applications, such as Amazon S3, encodes the namespace and bucket in the host header, you can use a base URL to resolve the object location.

For example, if you have an existing Amazon S3 application which sends requests to `http://bucket.s3.amazonaws.com`, you can use a proxy setting in the application to route the request to ViPR and ViPR will automatically extract the bucket name from the host header.

When using a URL to locate an object, if the base URL is set to `baseDomain.com`, the host header of the HTTP request can be set in the following formats:

`http://subdomain1.subdomain2.basedomain.com`

or

`http://subdomain1.basedomain.com`

In this case, the bucket name will be extracted from the host header as subdomain1 and the namespace will be extracted as subdomain2. If no namespace is specified, the default for the object storage user's tenant will be assumed.

ViPR is not involved in DNS registration, so you must ensure that the URL specified reaches ViPR. To simplify access to the default object store for the tenant, you could register a DNS entry in the form `*.<namespace>.myco.com`. Hence, if a System Administrator sets the tenant namespace to "viprobject", objects in a bucket called "images" could be addressed as `http://images.viprobject.myco.com/myImage.png`.

Adding a Base URL

This task is only necessary if you use object clients that encode the location of an object, its namespace and bucket, in a URL. In that case you can specify a base URL that will be used, together with the namespace, as the path to objects in a tenant.

Before you begin

This operation requires the System Administrator role in ViPR.

You must ensure that the domain specified in a request that uses a URL to specify an object location resolves to the location of the ViPR appliance.

Procedure

1. Select **Admin** › **Data Services** › **Base URLs**.
2. Select **Add**.

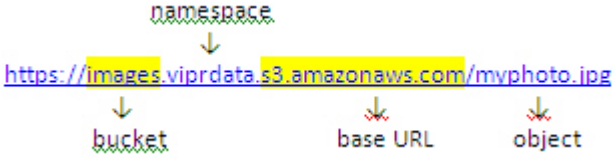
   The **Create Base URL** page is displayed.
3. Enter the name of the base URL. This will provide additional information about the base URL when looking at the base URL table.
4. Enter the base URL.

   If your objects location URLs are in the form: `https://mybucket.mynamespace.acme.com` (that is, `bucket.namespace.baseurl`) or `https://mybucket.acme.com` (that is, `bucket.baseurl`), the base URL would be `acme.com`.

   You can specify which format in the Use Namespace selector.
5. Choose the format in which your object address is encoded in the URL: with a namespace or without a namespace.
6. Select **Save**.

Example of a base URL

As an example of the use of the Base URL, an object named myphoto.jpg in the images bucket with a base URL of s3.amazonaws.com and a tenant namespace of viprdata, would be addressable using the following URL: `https://images.viprdata.s3.amazonaws.com/myphoto.jpg`



Note

The Object Data Service may include a list of base URLs.

CHAPTER 7

Configuring the Service Catalog

This chapter contains the following topics:

Service Catalog for Administrators

Administrators use the Service Catalog to configure the categories in which services are organized, the options that are available from a service, the resource constraints enforced in a service, and user access permissions for using a service.

Modifying the Service Catalog

Administrators can use the Service Catalog to:

- Organize the service catalog into categories and provide access to the categories based on user account or on group membership. For example, if a group of users only need to create Windows network shares, create a category containing just CIFS services and give access to members of a specified group.
- Configure the operation of services. For example, specify what inputs a service requires from a user, whether it requires approval before running, and whether it should run immediately or be scheduled for later.
- Create a new service by copying an existing service or by creating one from scratch. All services are based on the set of installed "base" services.
- Specify custom images for categories and services.
- Restore the default catalog. This restore the catalog to its configuration at installation.

Placing service orders

Orders cannot be placed on the services accessed from the Service Catalog in the Admin view. Orders can only be placed on services accessed from the User view, Service Catalog.

Use the **View Catalog** button to switch to the User view of catalog to place orders on services.

Using the Service Catalog

Use the Service Catalog management buttons to make general changes to the Service Catalog, or use the icons, within the Category images to make changes specific to the category, or service.

Table 20 Service catalog icons

Icon	Description
	Edit icon. Available on services and categories.
	Delete icon. Available on services and categories.
	Duplicate icon. available on services.

Adding a category

You can add a new category to any existing category in the service catalog.

Before you begin

You must be a Tenant Administrator to modify the service catalog.

Procedure

1. Select **Admin** › **Service Catalog**.

   You will initially be placed in the Home category.
2. Select **Add Category**.
3. Enter a title and a description for the category.
4. Select the image that you want to represent the category. The images to represent a category are called "folder" or "folder_<name>".
5. Choose the parent category in which you want your new category to be located.
6. If you want to restrict access to the category, select **Add ACL** and specify the users and groups who can see this category.

   Until you add an entry to the ACL, the category is visible to all users. Once you add an entry to the ACL, the category is only available to the users or group that you have added.

   More information on adding users and groups to an access control list is provided in Assigning permissions using ACLs on page 37.

   There is only one access permission associated with a category, that is "USE", which allows all members of the list to access the category.
7. **Save**.

Editing a category

You can edit a category in the service catalog.

Before you begin

You must be a Tenant Administrator to modify the service catalog.
When you edit a category you can:

- Select the title, the description, and the icon for the category.
- Select the parent of the category. This will place the category in the specified location.
- Specify the users and groups that can see the category. This makes it easy to restrict access to a category.
- Arrange the services within a category by moving them forward or backwards in the displayed order.

Procedure

1. Select **Admin** › **Service Catalog** and select the category that you want to edit.

   If the category is a sub-category of the current, click on the parent catalog to open it and locate the category you want.
2. Click on the Edit icon () of the category. Alternatively, you can click on the category to open it and then select **Edit Current Category**.
3. If you want to change the title and/or description, edit the appropriate fields.
4. If you want to change the image associated with the category, select a new image from the Image field drop-down menu.
5. If you want to change the location of the category within the service catalog, select a parent category from the drop-down menu.

6. In the Services field, use the up and down arrows next to each service to move it towards the start or the end of the catalog.

   A category can contain both services and sub-categories. The sub-categories will always appear first when viewing the category in the portal, however, you can change the displayed order of the services.

7. If you want to restrict access to the category, select **Add ACL** and specify the users and groups who can see this category.

   Until you add an entry to the ACL, the category is visible to all users. Once you add an entry to the ACL, the category is only available to the users or group that you have added.

   More information on adding users and groups to an access control list is provided in Assigning permissions using ACLs on page 37.

   There is only one access permission associated with a category, that is "USE".

8. **Save** the edited category.

Creating a service

Create a new service, or duplicate an existing service and edit the options to create a new service.

Before you begin

Only Tenant Administrators can create a new service.

Procedure

1. Select **Admin** › **Service Catalog**.
2. In the service catalog, either:
   - Select the **Duplicate icon** () for a service.
     Opens a form for a new service and gives it the name: Copy of ‹duplicated service name›.
   - Select **Add Service**.
     Opens a form for a new, unnamed service.
3. Configure the service identity

   The fields that define the service identity are listed below.

Label	Description
Base Service	The built-in, pre-defined service that this catalog service is based on. Each base service requires a set of parameters that must be specified by an end-user. As an administrator, some of the parameters can be pre-selected and locked so that they are hidden form the end-user.
Title	The title of the service as it will be seen in the service catalog.
Description	The description of the service as seen in the service catalog.
Image	The image that will represent the service in the service catalog.
Category	The service catalog category in which the service will be located.

4. Optionally, save the service now, to configure the parameters later. If the service is not saved before leaving the page, the service is lost, and must be created from start again.
5. Select, or deselect any parameters to lock, or unlock.
   - Unlock the values to make them user configurable when placing a service order.
   - Lock the values that will not appear in the service.

   If locking the value:

   a. Select the locked checkbox against the parameter.

   b. Select a value from the drop-down menu, or select one or more checkboxes from a selection list to specify the value (or values) to which the parameter will be locked.
6. Select or specify the service options to add to the service.

   The following service options can be applied:

Label	Description
Maximum Size	Determines the maximum storage size that can be provisioned using this service. (Applicable to create and extend storage services)
Approval Required	Determines whether approval will be requested (and must be granted) before the service will be executed.
Run in Execution Window	Determines whether the service should be run in an execution window.
Execution Window	For a service that runs in an execution window, specifies the execution window in which it will run.

7. To restrict access to the service, select **Add ACL** and specify the users and groups who can see this service.

   Until an entry to the ACL is added, the service is visible to all users. Once an entry is added to the ACL, the service is only available to the added users or groups.

   More information on adding users and groups to an access control list is provided in Assigning permissions using ACLs on page 37.

   There is only one access permission associated with a services, that is "USE", which allows all members of the list to access the service.
8. **Save**.

Configuring a service

Configure the service parameter selections, whether the service will run in an execution window, and whether the service requires approval to run.

Before you begin

Only Tenant Administrator can configure a service.

Procedure

1. Select **Admin** › **Service Catalog** and locate the service that you want to configure within the catalog hierarchy.
2. Click the **Edit icon** ( ) associated with the service.

   The administrator form for the service is opened.

3. Configure the service identity.

   The fields that define the service identity are listed below.

Label	Description
Base Service	The built-in, pre-defined service that this catalog service is based on. Each base service requires a set of parameters that must be specified by an end-user. As an administrator, some of the parameters can be pre-selected and locked so that they are hidden form the end-user.
Title	The title of the service as it will be seen in the service catalog.
Description	The description of the service as seen in the service catalog.
Image	The image that will represent the service in the service catalog.
Category	The service catalog category in which the service will be located.

4. Select, or deselect any parameters to lock, or unlock.
   - Unlock the values to make them user configurable when placing a service order.
   - Lock the values that will not appear in the service.

   If locking the value:

   a. Select the locked checkbox against the parameter.

   b. Select a value from the drop-down menu, or select one or more checkboxes from a selection list to specify the value (or values) to which the parameter will be locked.

5. Select or specify the service options to add to the service.

   The following service options can be applied:

Label	Description
Maximum Size	Determines the maximum storage size that can be provisioned using this service. (Applicable to create and extend storage services)
Approval Required	Determines whether approval will be requested (and must be granted) before the service will be executed.
Run in Execution Window	Determines whether the service should be run in an execution window.
Execution Window	For a service that runs in an execution window, specifies the execution window in which it will run.

6. To restrict access to the service, select **Add ACL** and specify the users and groups who can see this service.

   Until an entry to the ACL is added, the service is visible to all users. Once an entry is added to the ACL, the service is only available to the added users or groups.

   More information on adding users and groups to an access control list is provided in Assigning permissions using ACLs on page 37.

   There is only one access permission associated with a services, that is "USE", which allows all members of the list to access the service.

7. **Save** the service.

Upload category and service images

Custom category and service images can be uploaded for use in the service catalog.

Before you begin

The following prerequisites apply:

- This operation requires the Tenant Administrator role in ViPR .
- The maximum image size is 275x100 pixels. The recommended size is 120x90 pixels.
- Recommended image formats are `.png`, `.jpg/.jpeg` or `.gif`.

Procedure

1. In the **Admin** › **Service Catalog** area of the UI, locate the category or service that you want to change the icon for.
2. Edit the category or catalog.
3. Select the **Upload** control at the right of the Icon field.

   In browsers that do not support receiving data in the background, a new page is created to perform the upload.
4. Select **Choose File** and locate the image file on an accessible file system.

   The Name field will contain the name (minus extension) of the file. You can edit this field to provide a more appropriate name, if required.
5. Select **Upload**.

   In browsers that support asynchronous data transfer, the image that you upload becomes the currently selected image. In browsers that do not support asynchronous data transfer the image will appear in the list of images and you will need to select it if you want it to apply to the current category or service.

Restoring the default service catalog

You can restore the service catalog to its installed configuration.

You must be a Tenant Administrator to restore the service catalog.

Procedure

1. Select **Admin** › **Service Catalog**.
2. Select **Restore Default**.
3. Confirm that you understand that all changes that you have made to the service catalog will be lost.

   The changes that will be lost include configuration changes you have made to the services within the shipped catalog and any new categories or services that you have created.

   The catalog will be restored to its installed configuration.

CHAPTER 8

Working with Projects and Consistency Groups

This chapter contains the following topics:

Projects and consistency groups

ViPR enables resources to be grouped into projects and for related resources to be managed as part of a consistency group.

Projects

Projects enable storage resources (block volumes, file systems and objects) provisioned using ViPR to be grouped logically, and for authorization to perform operations on resources to be based on project membership. All provisioned resources are owned by a project.

For a provisioning user to be able to use a storage provisioning service, the provisioning user must belong to the project that will own the provisioned resource.

At the UI, Tenant Administrators and Project Administrators are responsible for creating projects and using an access control list (ACL) to assign users to projects and assign permissions to them. Projects have the concept of a Project Owner, which conveys certain administrator rights to a user, and enables a Tenant Administrator to delegate administrator rights for a project to a Project Administrator.

The roles associated with a project and the privileges associated with those roles are listed in the table below.

Table 21 Project admin and user permissions

Project User	Privileges
Tenant Administrator	The Tenant Administrator has full administrator and user permissions on all projects in the tenant. The Tenant Administrator has ultimate authority in the tenant and so can create projects that can only be administrated by a Tenant Administrator unless ownership is delegated to a Project Administrator.
Project Administrator	The Project Administrator can create projects and assign users to those projects. However, a Project Administrator can only perform administration operations on projects created by a Tenant Administrator if assigned ownership of the project. The Project Administrator can perform all user operations on projects that they own.
Project Owner	Project Owner is a special role which conveys certain project administration rights, such as granting user access through an ACL, assigning ownership of projects, and deleting projects. However, the UI only allows these administrator functions to be performed by a Project Administrator, where the API allows any project owner to perform these administrator functions. Hence, at the UI, assigning project ownership to a provisioning user will grant all user permissions on the project, but will not allow the user access to the Admin view to perform administration.
Project member with ALL permissions	Project members with ALL permissions can create resources for the project and can run services that operate on the project resources.
Project member with BACKUP permissions	Project members with BACKUP permissions can view project resources, and can perform data protection operations for those resources, but cannot perform storage creation, update, or delete operations.

Projects can have an associated quota which can be used to limit the total amount of provisioned storage that belongs to the project.

The **Admin** › **Tenant** › **Projects** page is accessible to Tenant Administrators and Project Administrators and displays the projects that they can perform administration on. For a Tenant Administrator this is a list of all projects in the tenant. For a Project Administrator this list contains the projects that the Project Administrator has created or has been assigned ownership of.

Creating a project

Go to **Admin** › **Tenant** › **Projects** to create a new project and assign users to the project.

Before you begin

- You must be either a Tenant Administrator or a Project Administrator to be allowed to create projects. You will not see the **Admin** › **Tenant** › **Projects** menu item unless you are in one of these roles.
- Projects created by a Tenant Administrator can only be administrated by a Project Administrator if the Project Administrator is the project owner.
- Projects created by a Project Administrator are visible to, and can be administrated by, a Tenant Administrator.

Procedure

1. Select **Admin** › **Tenant** › **Projects**.
2. Select **Add**.
3. Enter the name of the project.
4. In the **Owner** field, enter the name of the project owner.

   This is the AD/LDAP name of the user. If you do not enter a name, you will be the project owner.

   The project owner should be a Project Administrator. This provides a way of allowing a project created by a Tenant Administrator to be delegated to a Project Administrator.

   If you are a Tenant Administrator, projects that you own cannot be administrated by Project Administrator unless you make them the owner.

   If you assign project ownership to a provisioning user, the user will not be able to perform administration at the UI.

5. You can associate a quota with the project to limit the amount of storage provision for the project.

   a. Check the **Enable Quota** box

   b. In the **Quota** field, enter the maximum amount of storage that you want to allow.

6. To assign project permissions to other users, select **Add ACL**.

   An ACL field is displayed allowing you enter a user or group name and assign a permission.

7. Enter the name of a user or group and set the **Type** field to be consistent.
8. Select the access permission for the user as either ALL or BACKUP.

   ALL permission allows users to provision resources that belong to a project and to run services against resources owned by a project. BACKUP allows a user to view the resources belonging to a project and perform data protection operations.

   More information on adding users and groups to an access control list is provided in Assigning permissions using ACLs on page 37.

9. To add more users or groups, select **Add ACL** again.

   You can remove an ACL entry by clicking **Remove**.

10. When you have added all ACL entries, click **Save**.

Editing a project

You can edit a project in order to rename it, assign users to the project to give them access, or assign a Project Administrator as the project owner.

Before you begin

You must be a Tenant Administrator, or a Project Administrator who owns the project, in order to edit the project.

Procedure

1. Select **Admin** › **Tenant** › **Projects**.
2. Click on the name of the project that you want to edit.
3. If you want to change the name of the project, edit the project name.
4. If you want to assign a project owner, enter their username in the Owner field.

If you are a Tenant Administrator, you can assign ownership to a Project Administrator to allow them to have administrator rights for the project.

If you are a Project Administrator, you can assign ownership to a different Project Administrator. This allows you to delegate ownership of projects that you have created.

5. Add users in the access control list area.

   Select the access permission for the user as either ALL or BACKUP. ALL permission allows users to provision resources that belong to a project and to run services against resources owned by a project. BACKUP allows a user to view the resources belonging to a project and perform data protection operations.

   More information on adding users and groups to an access control list is provided in Assigning permissions using ACLs on page 37.

6. Select **Save**.

Deleting a project

A project that does not own any storage resources or is not referenced by other objects can be deleted.

Before you begin

The following prerequisites are apply:

- A project can only be deleted if it does not own any storage resources.
- You must either be a Tenant Administrator or a Project Administrator to delete a project. A Tenant Administrator can delete any project. A Project Administrator can delete any project that they are the owner of.

Procedure

1. Select **Admin** › **Tenant** › **Projects**.
2. Select the checkbox for the project you want to delete.
3. Select **Delete**.

Consistency groups

Volumes can be assigned to consistency groups to ensure that snapshots of all volumes in the group are taken at the same point in time.

The **Admin** › **Tenant** › **Consistency Groups** page lists the consistency groups that exist and enables consistency groups to be added or deleted.

Consistency groups are associated with projects, so provisioning users will only be allowed to assign volumes to consistency groups that belong to the same project as the volume.

Adding a consistency group

Consistency groups can be created and volumes assigned to them during provisioning operations.

Before you begin

This operation can be performed by a Tenant Administrator for any project or by a Project Administrator for owned projects.

Procedure

1. Select **Admin** › **Tenant** › **Consistency Groups**
2. Select the project that you want to add a consistency group to.

   The consistency group table displays any consistency groups that exist in the project.
3. Select **Add**.
4. Enter a name for the consistency group.
5. Select **Save**.

Deleting a consistency group

You can delete a consistency group that is no longer used.

Before you begin

This operation requires the Tenant Administrator role in ViPR .

if the consistency group has volumes associated with it, it cannot be deleted.

Procedure

1. Select **Admin** › **Tenant** › **Consistency Groups**
2. Select the checkbox for the consistency group to be deleted.
3. Select **Delete**.

CHAPTER 9

Working with Orders, Execution Windows, and Approvals

This chapter contains the following topics:

Orders, order scheduling, and approvals

Orders can be submitted for execution immediately, or can be scheduled to be fulfilled during an execution window. The tenant area also enables approval settings to be specified.

Recent orders

An order is a record of a request to run a service. The Recent Orders page provides a table view of the orders created by users within the tenant.

The Recent Orders table differs from the Orders page in the User view only in that it shows the user who submitted the order.

The order records the details of the request: which service was requested, what parameters were specified in the service request, who requested it, whether the order is scheduled, and the outcome of the order submission.

The order history table tells you the service that was executed and the date and time at which it was executed. The time displayed is UTC and your time offset is shown next to the UTC time.

In addition, the table shows you the status of the order and displays an order ID that provides a unique identity for the order that provisioning users can use when requesting information from you (Tenant Administrator) when there is a problem with the execution of an order.

The icons displayed to indicate the status of an order are provided in the following table.

Table 22 Order status icons

Icon	Meaning
✔	Order was processed successfully.
🕒	Order is scheduled. Open the order to see the execution windows in which it will be executed.
✖	Order failed.
☑	Order is waiting for approval.

Order details

The order details shows the order request information, details of the selected order, and a summary of the execution steps.

Table 23 Order details areas

Order area	Contains
Summary	The top part of the order displays the order identity and status on the left-hand side, and displays the parameters passed to the operation on the right-hand side. You will see all of the

Table 23 Order details areas (continued)

Order area	Contains
	parameters passed to the service, even if they were hidden on the service form. If the order is scheduled to run in an execution window, the status displays `Order Scheduled`. if the order requires approval, the status displays `Pending Approval`.
Affected Resources	Shows the details of the resource that was created as a result of the operation or in which the operation was run.
Order Details	Displays detailed information about the steps taken to process the order.

The following table lists the affected resource types and the information provided with each type.

Table 24 Affected resources

Affected resource	Description
Block Storage	
Block Export	If the operation exports a block volume to a host, this entry displays the details of the host.
Volume	Shows details of the block volume that has been created. If the operation fails and rollback requires the volume to be deleted, displays: "volume has been deleted."
File Storage	
File System	Shows details of the file system created. If the operation fails and rollback requires the file system to be deleted, displays: "file system has been deleted."
CIFS Share	Shows details of the CIFS share. Indicates the mount point that can be used when mapping the drive on a Windows host.
NFS Export	Shows details of the NFS export. Indicates the mount point that can be used when mounting the file system on a Linux host.

The following table describes each of the order detail types.

Table 25 Order details

Category	Content
Logs	Shows the messages written to the log file during execution of the order.
Precheck	Shows the pre-checks carried out before executing the order. The pre-checks ensure that the host to which storage will be attached is available and

Table 25 Order details (continued)

Category	Content
	that there are the required paths between the host HBA and the selected array.
Execution Steps	Lists the execution steps that were carried out in executing the order.
Rollback	If an order fails, the steps carried out to rollback any command executed before failure are listed.

Scheduled orders and execution windows

Orders can be scheduled for execution at a later time or date and at recurring intervals. Scheduled execution takes place in pre-defined execution windows when the system is least loaded or when it as been taken offline for maintenance.

From an administrator perspective, there are three aspects to scheduling that you will use:

- The ability to configure named execution windows.
- The ability to configure a service to execute during a specific execution window.
- The ability to view the orders that are currently scheduled for execution. Scheduled orders can be cancelled if required.

Scheduled Orders Table
The Scheduled Orders Table displays the service that is scheduled, the owner of the order, and the execution window in which it will be executed.

Execution Window Calendar
The execution window calender provides you with a calendar view in which you can create schedule windows, in the same way as you can create events in many other calendar applications.

Creating and configuring an execution window

The **Admin** › **System** › **Execution Windows** page provides you with a calendar view in which you can create schedule windows, in the same way as you can create events in many other calendar applications.

Before you begin

This operation requires the Tenant Administrator role in ViPR .

Procedure

1. Select **Admin** › **Tenant** › **Execution Window**
2. Click on a time-slot in the calendar.

   The **Edit Execution Window** dialog is displayed.
3. Enter a title for the execution window and set its start time and duration. Set and the frequency and interval at which you want the window to occur.

   If the start time of the window has passed, the windows will start on the next possible date. For example, if the windows is daily, the first window will be created the next day; if it is weekly it will be created next week.

Note

If the Execution Window is within the next hour, it is important that your local time and the ViPR server time are in sync. If they are not, it is possible that a time that your portal machine thinks is in the future has actually passed on the server. The timestamps of all activities and logs are server time, so you can check what difference in time you have.

The Hour to Start is displayed in UTC. However, if you select a time on the calendar, the time you select will be local time.

4. **Save**.

After you finish

You can click on an execution window to edit it. If you move the window to another time or day, the orders that are scheduled to execute in that window will execute at the changed time. An attempt to delete a window in which orders are scheduled will fail and you will have to remove the scheduled order.

Scheduling a service to run in an execution window

A service can be configured so that it executes at later time in an execution window.

Before you begin

This operation requires the Tenant Administrator role in ViPR .

Procedure

1. Select **Admin** › **Service Catalog**
2. Locate the service in the service catalog and edit it.
3. Select the Execution Window Required checkbox.
4. Select the execution window in which you want the service to execute or leave it as Use Next Available Execution Window.

   If you need a version of a service that is scheduled for execution in an execution windows, or one that allows the user to choose an execution window, and a version which is executed immediately, you can create two different versions of the service. Access to each version of the service can be controlled in the normal way: by restricting access to the service to a particular group, or by placing the service in a category which is only accessible to certain groups.
5. **Save** the service.

Cancelling a scheduled order

You can cancel a scheduled order from the scheduled orders table.

Before you begin

This operation requires the Tenant Administrator role in ViPR .

Procedure

1. Select **Admin** › **Tenant** › **Scheduled Orders**
2. Select the order, or orders, that you want to cancel by selecting the checkbox to the left of the order in the Scheduled Orders table.
3. Select **Cancel**.

Editing or deleting an execution window

An execution window can be edited or deleted.

This operation requires the Tenant Administrator role in ViPR .

Procedure

1. Select **Admin** › **Tenant** › **Execution Windows**
2. Click on the execution window in the calendar.
3. At the Edit Execution Window, edit the properties or **Delete** to remove the window.
4. Select **Save**.

Approval settings

If services are configured to use approvals, you will need to configure approval settings to notify an approver that a service needs approval and/or to notify an external system of the need for approval.

There are two approval settings:

- Approver Email
- Approval Service URL

Approver Email
You can set an email address to which notification of the need to approve an order will be sent. The recipient of the email must have the Tenant Approver role in ViPR in order to approve the order.

Approval Service URL
The Approval Service URL provides the location of an external service that will perform approval of ViPR orders.

ViPR will perform a HTTP POST and send an ApprovalInfo JSON object payload to the specified URL. The approval service must approve or reject the order by calling the ViPR approvals API and sending an updated ApprovalInfo object indicating the approval status.

You can see the details of the object by looking for "approvalInfo" in the schema for the UI API at https://*ViPR_virtual_ip*/`api/schema.xsd`, or you can look at the API documentation for retrieving an approval request: `/api/approvals/{approvalId}`.

Adding approval settings

Approvals settings can be made at the **Admin** › **Tenant** area.

Before you begin

This operation requires the Tenant Administrator role in ViPR .

Procedure

1. Select **Admin** › **Tenant** › **Approval Settings**
2. If you want approvers to be notified when an order requires approval, enter the email address of an approver for the tenant.
3. If you want to configure ViPR to call an external system that can handle approvals, enter the URL of the system.

4. Select **Save**.

CHAPTER 10

Managing and Monitoring the Virtual Data Center

This chapter contains the following topics:

Managing and monitoring the ViPR instance

The ViPR software installed on the ViPR nodes can be managed and monitored from the **Admin** › **System** area.

Dashboard

The ViPR UI brings together the most important information about your ViPR configuration in one view on the **Admin** › **System** › **Dashboard** page.

The dashboard has the following areas:

ViPR Version
Shows the version of the platform and the UI software components. If you have configured an Update site, the panel displays the identity of the latest available upgrade. If you are a System Administrator, clicking on the platform version number or on the upgrade message takes you to the **Admin** › **System** › **Upgrade** page.

License Status
Shows the status of the Controller license and the Object, HDFS, and Object + HDFS licenses. If you are a System Administrator, clicking on the status links to the license page, **Admin** › **System** › **License**.

Physical Assets
Provides a count each of the physical asset types. For a System Administrator, each label links to its associated UI page.

Virtual Assets
The Virtual Assets panel provides a count of the virtual arrays and virtual pools that have been configured. For a System Administrator, the arrays and pools link to the corresponding virtual asset page.

ViPR Virtual Appliance

Lists the controller and data VMs of the ViPR virtual appliance, shows the overall status of the virtual appliance, provides an indicator of the VM status, and provides a link to the **System Health** page for each VM.

Table 26 ViPR Virtual Appliance status messages

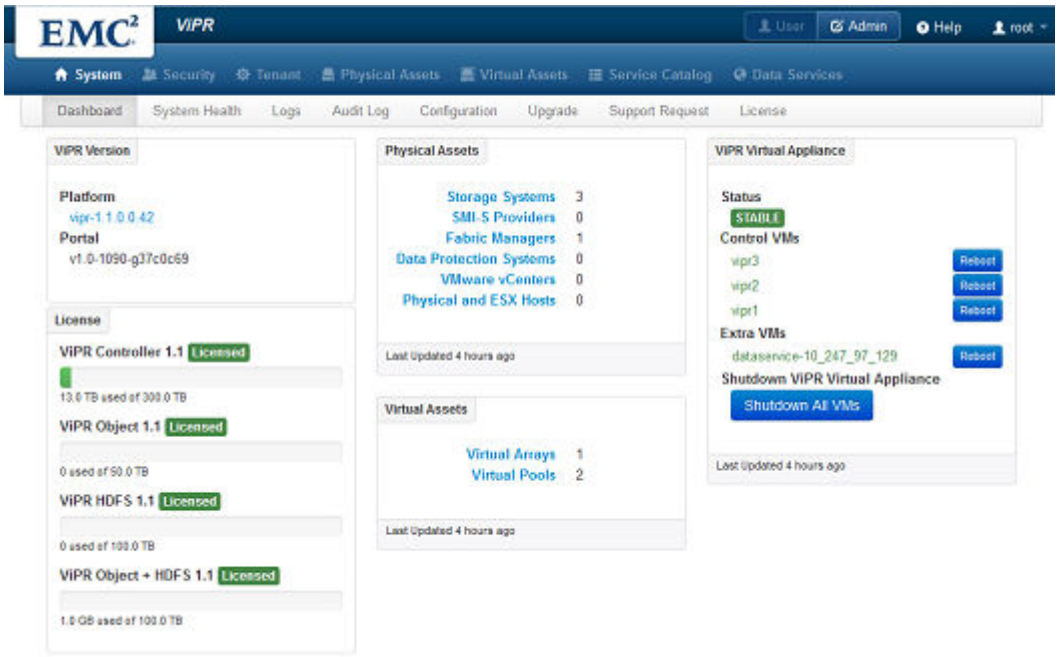
Status	Description
Stable	All of the ViPR virtual appliance VMs are online and available.
Syncing	The VMs of the ViPR virtual appliance are currently running different versions of ViPR, and are being synchronized to the same version.
Upgrading	Changing the ViPR version. This could be for an upgrade or downgrade.
Degraded	At least one of the VMs in the virtual appliance is offline.
Updating	Configuration changes were made to the virtual appliance properties, and the changes are being updated so that all the VMs in the virtual appliance are the same.
Powering Off	ViPR virtual appliance is powering down.
Preparing for database upgrade	Preparing the database for a new version.
Converting database for upgrade	Converting the database to a new version.
Upgrade failed	Database conversion failed. Either go back to a snapshot from previous version, or contact EMC to help resolve the issue.

Table 27 Virtual Machine status indicator

VM link color	Description
Green	Good — The VM is reachable and all the services are running.
Red	Unavailable — when a controller vm is not reachable or the syssvc service is down on the data object vm. Degraded — the virtual machine is reachable, but one or more of the services are not running.
VM not listed	Unavailable — when a data vm is not reachable or the syssvc service is down on the data vm.

An example of the dashboard is shown below.

Figure 4 ViPR dashboard



System health

ViPR presents the overall managed capacity for the ViPR Controller and the ViPR Data Services (object and HDFS). In addition, the display shows health and statistics data for a selected virtual machine (VM) in the ViPR Virtual Appliance.

The **System Health** page is accessed from theViPR UI **Admin** › **System** › **System Health** tab and presents the following information:

- Capacity Reports on page 120
- VM Stats on page 121
- Service Stats on page 121
- Diagnostic Tests on page 122

Capacity Reports

The following capacity reports are provided:

Managed Capacity

Shows the amount of file and block storage used and the free capacity.

The managed capacity will not necessarily match the requested storage capacity. The managed capacity is calculated as the sum of the allocated capacity for all ViPR volumes and file systems. Allocated capacity is the physical capacity of a volume on the storage system and as such will differ from the requested storage because it includes RAID overhead and other storage system specific overheads. For thin volumes, allocated capacity will be different from requested capacity in most of cases, since allocated capacity will show how much space of the requested capacity is really used.

Object Capacity
The Object Capacity is the total storage allocated to data stores for object-only data services virtual pools. You will only have this display if you have an Object license and the Object Capacity will correspond with the amount of storage used against the Object license.

HDFS Capacity
The HDFS Capacity is the total storage allocated to data stores for HDFS-only data services virtual pools. You will only have this display if you have a HDFS license and the HDFS Capacity will correspond with the amount of storage used against the HDFS license.

HDFS + Object Capacity
The HDFS + Object Capacity is the total storage allocated to data stores for HDFS + Object data services virtual pools. You will only have this display if you have a HDFS + Object license and the HDFS + Object Capacity will correspond with the amount of storage used against the HDFS + Object license.

Note

For the Object/HDFS capacity reports, if file systems have been ingested into data services, the allocated capacity that is reported is not guaranteed to be available for use, as only the space taken up by the ingested data is used. No new data is written to ingested file systems.

VM Stats
The VM stats show the memory and storage utilization for the selected VM.

Service Stats
Displays statistics for each of the services running on the currently selected ViPR controller, or VM. The right-hand column enables the logs for the service (on the selected VM) to be displayed.

The services that are monitored on each controller VM are listed in the table below.

Table 28 ViPR Controller Services

Service	Description
apisvc	API service
authsvc	Authorization service
controllersvc	Logic and storage system controller service
coordinatorsvc	Internal cluster controller service
dbsvc	Database service
objcontrolsvc	Object services
portalsvc	Portal service
sasvc	Portal back-end service
syssvc	System services
vasasvc	Storage Provider service

The services that are monitored on each data VM are listed in the table below.

Table 29 ViPR Data Services

Service	Description
syssvc	System services
hdfssvc	HDFS service
datasvc	Data service

Table 30 System Health Service Statistic Status

Service	Description
	Service is up and running.
	Service is down.
R	Service is being restarted.

Diagnostic Tests

Display the results of diagnostic test carried out on the selected VM.

Log Messages and Alerts

ViPR provides the capability to access to the log messages associated with each of the EMC ViPR services and to access to system events (alerts). The log messages and alerts can be filtered to display the log messages or alerts for a specified node for a selected period of time.

Each ViPR service on each node logs messages at an appropriate level (INFO, DEBUG, WARN and ERROR) and the service logs can be viewed when a problem is suspected. However, the log messages may not provide information that can be acted on by a System Administrator, and may need to be referred to EMC.

System alerts are a class of log message generated by the ViPR system management service aimed at System Administrators and reflect issues, such as environment configuration and connectivity, that a System Administrator should be able to resolve.

System Logs Table

The system logs table displays the system events or ViPR service logs in accordance with the current filter settings. The table displays the time of the message, the level, the message text, and the service with which the message is associated.

The table can be filtered to display either system alerts or log messages associated with specific ViPR services (or for all ViPR services) for a specified node, for a specific period of time. The events and log messages can also be filtered to show only those containing a specific text string.

In addition, the logs can be downloaded as a zip so that they can be reviewed offline.

System Logs Summary

The status panel at the top of the system logs table provides a textual summary of the current filter applied to the system logs table.

Filter Control
The **Filter** button provides access to the Filter dialog which enables you to specify: the node for which you want to retrieve the logs, whether you want to retrieve logs or system events, the log level that you want to retrieve, the time span over which logs should be considered, a string that any filtered message must contain.

Download Control
The download button enables the you to download a zip file containing the logs that correspond to the current filter setting. In addition to the logs directory, the zip also contains an info directory, containing the configuration parameters currently applied, and orders directory showing all orders that have been submitted.

Filtering the system logs and system events

You can filter the system logs and system events (also called alerts).

Before you begin

This operation requires the System Administrator role in ViPR.

Procedure

1. At the **Admin** › **System** › **Logs** page select the **Filter** button.
2. Select the Node for which you want to display the log or system alert messages.
3. Select either System Events, All Services or choose a specific service for which you want to see the log messages.
4. At the Level drop-down, select the level above which you want to view log messages. The levels are listed in order (ERROR, WARN, INFO, DEBUG). The level you select and messages logged at all levels above it (that meet the other filter criteria) will be displayed.
5. Select the data and time from which you want the log display to start. You can set the date or time by selecting the appropriate (calendar or clock) control. The clock control uses up and down arrows to change the hours and minutes fields.
6. If yo do not select a To: time, log message up to the current time will be displayed. if you want the message display to be up to an earlier time, click **Enter Specific Time**.
7. If you are only interested in message that contain a specific text string, enter the string in the Message field.
8. Select **Update**. You will be returned to the logs page and the System Logs table will display the filtered log messages or system events.

Collecting system logs for support

You can download a log archive in order to view system configuration, logging, and order information offline.

Before you begin

This operation requires the System Administrator role in ViPR.

A logs archive is automatically sent via ConnectEMC when a support request is submitted (**Admin** › **System** › **Support Request**). However, the ConnectEMC logs are restricted to 16MB. If you want to analyse more than 16MB of log files you should use the download mechanism described here.

Procedure

1. Select **Admin** › **System** › **Logs**.

2. Set up the filters so that the logs/alerts for the time period that you want are captured. See Filtering the system logs and system events on page 123.
3. Select **Download**.

   A logs archive (.zip) file called `logs-<date>-<time>.zip` will be downloaded. The logs archive contains all log, system configuration, and order information.

Upgrade

Use the **Admin** › **System** › **Upgrade** page to:

- View the present ViPR version installed on all VMs, and any newer versions available in the upgrade repository.

  Note

  The upgrade repository is on an EMC server by default, and can be changed from the **Admin** › **System** › **Configuration** › **Upgrade** page.

- Upgrade to a newer version of ViPR.

Table 31 Supported upgrade paths to ViPR 1.1.0 Patch 1

Version	Upgrade path to ViPR 1.1.0 Patch 1
ViPR 1.0.0	Must first upgrade to ViPR 1.0.0 Patch 1, then to ViPR 1.1.0, then to ViPR 1.1.0 Patch 1.
ViPR 1.0.0 Patch 1	Must first upgrade to ViPR 1.1.0, then to ViPR 1.1.0 Patch 1.
ViPR 1.1.0	Upgrade directly to ViPR 1.1.0 Patch 1

Pre-upgrade planning

Some pre-upgrade steps are required and you should prepare for ViPR to be unavailable for a period of time.

Prepare for the ViPR virtual appliance to be unavailable for a total of approximately 25 minutes, starting from the time you take the VMs offline for the snapshots, until the upgraded ViPR virtual appliance state is stable.

- Unmount Linux volumes on page 124.
- Take offline virtual machine snapshots on page 124
- Perform the upgrade on page 125

Unmount Linux volumes before upgrade

Linux volumes that were mounted in v1.0 cannot be expanded, unmounted, or deleted in v1.1. Before upgrade, run the ViPR service Unmount Volume on Linux on mounted Linux volumes.

Take virtual machine snapshots before upgrade

You should take snapshots of all ViPR controller VMs before upgrade.

Before you begin

This procedure is not supported and should not be used if data services VMs are deployed.

This operation requires the System Administrator role in ViPR and root access to the ViPR controller VMs.

In the unlikely event that there is a need to revert to a snapshot, keep in mind that the ViPR database will be at the state it was in when the snapshot was taken.

Procedure

1. Connect using SSH to each ViPR controller VM and shut down with the `halt` command.
2. Use vSphere Client to take a snapshot of each controller VM. Do not snapshot the virtual machine's memory.
3. When the snapshots are complete, power up the ViPR controller vApp.
4. In the ViPR UI, look at the ViPR virtual appliance state in **Admin** › **System** › **Dashboard**.

   When the state is Stable, you can proceed with the upgrade.

Upgrading ViPR software

New versions of software made available from the upgrade repository can be downloaded and installed from the **System** › **Upgrade** page.

Before you begin

- This operation requires the System Administrator role in ViPR.
- Refer to the pre-upgrade steps in the *EMC ViPR Installation and Configuration Guide*.
- To see the available software versions, the upgrade repository must have been configured from the **System** › **Configuration** › **Upgrade** page.
- An upgrade to ViPR 1.1 patch 1 can only be performed from ViPR 1.1 (1.1.0.0.425). If you are running a ViPR version less than 1.1, follow a supported upgrade path to ViPR 1.1 before upgrading to ViPR 1.1 patch 1.
- Verify that the ViPR virtual appliance status is Stable (**Admin** › **System** › **Dashboard**).

Procedure

1. Select **Admin** › **System** › **Upgrade**.
2. Select an available ViPR version and **Download**.

   Note

   The downloaded software is stored on the VM and can be installed at anytime.

3. Click **Install**.

   A rolling upgrade is performed on the ViPR VMs.

   The **System Maintenance** page opens while installation is in progess, and presents the current state of the upgrade process.

   Wait for the system state to be Stable before making provisioning or data requests.

Post-upgrade steps

Depending on which pre-upgrade steps were taken, there may be some required steps after upgrade.

- Mount any Linux volumes that you unmounted before upgrade.
- The list of discovered unmanaged file systems will be out of date after upgrade. Run **File Storage Services** › **Discover Unmanaged File Systems** on all storage systems after upgrade.

- After a successful upgrade, discard the pre-upgrade snapshots. Resume regular ViPR backups.

Reverting to pre-upgrade snapshots

If you need to revert to the VM snapshots made before upgrade, use the vCenter Snapshot Manager.

Before you begin

You need access to the vCenter Server via vSphere Client where the ViPR VMs are located.

You need credentials that allow you to shut down the ViPR VM from the console.

Note that the ViPR database will be at the state it was in when the snapshot was taken.

Procedure

1. From vSphere Client, open the console on each controller VM and shut it down with the `halt` command.
2. From vSphere Client, right-click each ViPR VM and select **Snapshot** › **Snapshot Manager**.
3. For each VM, select the snapshot to which you want to revert and select **Go to** .
4. When the revert operations are complete, power on the controller VMs.

Upgrading ViPR from an internal repository

You can upgrade ViPR from an internal location by downloading a ViPR img file from support.EMC.com and copying it to the ViPR virtual appliance for upgrade.

Before you begin

- This operation requires the System Administrator role in ViPR.
- You need credentials to access support.EMC.com.

Procedure

1. Download the ViPR img file from support.EMC.com and save it locally.
2. Run the following ViPR CLI command:

   ```
   ./viprcli -hostname ViPR_virtual_ip -cf cookie_file system
   upload -imagefile locally_saved_img
   ```

   This command copies the img file to a location on the ViPR virtual appliance where it is found by the upgrade feature.

   Refer to *EMC ViPR CLI Reference* for details of how to install and use the ViPR CLI.
3. In the ViPR UI select **Admin** › **System** › **Upgrade**.
4. Select **Install** next to the version you uploaded with the viprcli command.

Support request

A support request consists of the text comments that you enter at **Admin** › **System** › **Support Request** and the system logs for the range of time that you specify.

Submitting a support request

You can send a support request to ConnectEMC.

Before you begin

This operation requires the System Administrator role in ViPR.
The ConnectEMC and email must already be configured (**Admin** › **Configuration**) .

Procedure

1. Select **Admin** › **Security** › **Support Request**.
2. In the Contact Email field, enter the email address where you can be contacted with a response to your request.
3. Using the problem template, replace the bracketed ([]) text guidelines in order to enter a problem headline/title, a description of the problem and its impact, and the conditions that can be used to reproduce the problem.
4. Select the range of time for which the system logs will be collected to send with this support request.

   The range must be small enough to generate less than 16MB of zipped logs. If greater than 16MB the logs will not be sent successfully.
   Alternatively, you may need to download the logs using **System** › **Logs** › **Download**, and provide the .zip file to the customer service by another method.
5. **Send**.

Licensing

ViPR is licensed for the Controller (file and block), Object, HDFS, and Object + HDFS features in capacity tiers between 1 TB and 5000 TB. You need to obtain a Controller license and upload it to a node before ViPR will function.

The **Admin** › **System** › **Dashboard** page provides a graphical display of the license usage and the **Admin** › **System** › **License** page provides usage and license details. A Controller license is always required, the three Object and HDFS license types are optional and a license display will only be shown if you have the corresponding license.

The license usage display for each license type provides the following information:

Controller
: The Controller license displays the total available capacity that can be managed and displays the amount that is actually being managed ("used"). The amount of storage under management by ViPR corresponds to the sum of the free space on all storage pools provided by the storage arrays that are being managed by ViPR.

Object
: The Object license display shows the amount of file storage that has been allocated to data stores for use by ViPR data services that support the Object storage type.

HDFS
: The HDFS license display shows the amount of file storage that has been allocated to data stores for use by ViPR data services that support the HDFS storage type.

Object+HDFS
: The Object + HDFS license display shows the amount of file storage that has been allocated to data stores for use by ViPR data services that support the Object and HDFS storage type.

Note

For the Object/HDFS license types, the full capacity of any data services ingested file system will be shown as allocated against the license. However, only the space taken up by the ingested data is used, no new data will be written to the file system. Hence, for data services ingested file systems, the amount shown as allocated might not all be useable for object or HDFS data.

Object, HDFS, and Object + HDFS data stores use ViPR managed file systems to provide their underlying storage. Hence, the total controller licensed capacity must always exceed the sum of the capacities of the Object, HDFS, and Object + HDFS licenses, and you will need to ensure that you have enough file system storage to support your object/HDFS requirements.

In addition, even if you have enough file storage capacity for your object/HDFS requirements, it is not reserved for use by object/HDFS services, so non-object/HDFS file system provisioning operations will reduce the file storage available for use by Object/HDFS, and vice-versa.

You can see the amount of storage provisioned from the storage capacity under management on the **Admin** › **System** › **System Health** page (System health on page 120).

Adding a license

After obtaining a license you need to upload it to ViPR.

Before you begin

This operation requires the System Administrator role in ViPR.

You need access to the license file that was downloaded from the EMC license management web site.

Procedure

1. Select **Admin** › **System** › **License**.
2. Browse to and select the license file that was downloaded from the EMC license management web site.
3. **Upload License File**.

Obtaining a license file for ViPR

You can obtain a license file for ViPR from the Managing Licenses page on EMC Support.

Before you begin

You need the License Authorization Code (LAC), which was emailed from EMC.

Procedure

1. Go to **EMC Online Support (http://support.emc.com)** › **Service Center** › **Manage Licenses**.
2. Enter the required information to acquire and save the license file.

Results

Once you have obtained the license file, upload it to ViPR as part of the initial setup steps when logged in toViPR for the first time as root.

Audit log

The ViPR audit log records activities performed by administrative users, such as the addition or modification of physical assets and virtual assets, the creation of virtual assets, the assignment of users to roles, etc.

At the UI, the **Admin** › **System** › **Audit Log** provides an audit log table which displays the time at which the activity occurred, the user that performed the activity, the service type (for example, vdc or tenant), the result of the operation, and a description of the operation.

Displaying the audit log

The audit log can be displayed at the **Admin** › **System** › **Audit Log** page of the ViPR UI and a time period for the log display can be specified.

Before you begin

This operation requires the System Auditor role in ViPR.

Procedure

1. Select **Admin** › **System** › **Audit Log**.

   The audit log table defaults to displaying activities from a specific hour on the current day.
2. To display the audit log for a longer time span, use the calendar control to select the date from which you want to see the logs, and use the hours control to select the hour of day from which you want to display the audit log.
3. Select **Show Log** to display the audit log from the specified time.

CHAPTER 11

Setting up Multiple Tenants

This chapter contains the following topics:

Multiple Tenants

ViPR can be configured with multiple tenants, where each tenant has its own environment for creating and managing storage which cannot be accessed by users from other tenants.

This chapter describes how to create multiple tenants in ViPR. The initial configuration of ViPR is set up for a single-tenant environment. Only the root provider tenant is available by default. If you would like to set up a multi-tenant ViPR environment, you must use either the API or CLI procedure described in this chapter. You cannot create subtenants (called tenants) under the root tenant in the UI.

Physical assets, such as the storage systems and fabrics, added to ViPR are available to the virtual data center and so can be assigned to any tenant. Similarly, virtual array and virtual pools created in ViPR are virtual data center assets and can be assigned to any tenant.

Hence, the configuration of virtual arrays and virtual pools can be performed for the root tenant from the UI and they can then be assigned to any new tenants that you create.

If you are intending to use ViPR Data Services, you should ensure that the configuration for the root tenant has been performed and then perform the tenant-specific configuration described in the procedures provided here.

ViPR role requirements

To perform certain operations, you need to be authenticated as a user with a specific role. The root user for your ViPR vApp has all the role assignments you need to complete the multi-tenant setup.

Configuring multiple tenants with the REST API

This section shows how to configure multiple tenants with the ViPR API.

Before you begin

Complete the deployment and initial configuration steps in the *EMC ViPR Installation and Configuration Guide*.

Procedure

1. Authenticate with ViPR using an account that has Security Administrator and System Administrator roles. The root user has these roles and can be used.

   How you authenticate depends on the HTTP client that you are using. If you are using a browser-based client, you could log in at the ViPR UI and the session cookie created will authenticate the HTTP client connection.

2. Ensure you have an authentication provider configured that will authenticate users in your domain.

   Either:

   - Create an authentication provider at the **Admin** › **Security** › **Authentication Providers** menu of the ViPR UI.
   - Use the `/vdc/admin/authnproviders` API. For example:

     Request

     ```
     POST /vdc/admin/authnproviders
           <authnprovider_create>
             <mode>ad</mode>
             <domains>
                   <domain>yourco.com</domain>
     ```

```
                <domain>domain2.yourco.com</domain>
                <domain>domain3.yourco.com</domain>
            </domains>
            <name>multi-domain forest</name>
            <server_urls>
                <server_url>ldaps://MyLDAPServer.yourco.com:3269</
   server_url>
            </server_urls>
            <server_cert>my_server_certificate</server_cert>

   <manager_dn>CN=manager_bind,OU=Test1,OU=Test,DC=yourco,DC=com</
   manager_dn>
            <manager_password>Password</manager_password>
            <group_attribute>CN</group_attribute>
            <search_base>DC=yourco,DC=com</search_base>
            <search_filter>userPrincipalName=%u</search_filter>
            <search_attribute_key>userPrincipalName</
   search_attribute_key>
            <group_whitelist_values></group_whitelist_values>
            <search_scope>SUBTREE</search_scope>
        </authnprovider_create>
```

3. Get the urn ID of the root provider tenant.

   You must have the Tenant Administrator role to perform this operation.

   Request

   ```
   GET /tenant
   ```

   Response

   ```
   <tenant_info>
       <id>urn:storageos:TenantOrg:e5013f5e-41d7-4cf9-
   b1fd-4fecfad0c18c:</id>
       <name>Provider Tenant</name>
       <link href="/tenants/
   urn:storageos:TenantOrg:e5013f5e-41d7-4cf9-b1fd-4fecfad0c18c:"
             rel="self"/>
     </tenant_info>
   ```

   The urn of the root provider tenant in this example is:

   ```
   urn:storageos:TenantOrg:e5013f5e-41d7-4cf9-b1fd-4fecfad0c18c:
   ```

   Use this urn as the parent when creating a new tenant in the following step.

4. Create a new tenant and map users to it through a domain that is included in the authentication provider.

   Note

   The set of LDAP users assigned to a subtenant is always a subset of the users mapped to the Provider Tenant.

   In this example, the users in the domain `domain2.yourco.com` are mapped into the tenant called `EMC tenant`. You must have the Tenant Administrator role for the parent tenant to perform this operation. The {id} variable is the URN of the provider tenant.

   Request

   ```
   POST /tenants/{id}/subtenants
   <tenant_create>
     <name>EMC_tenant</name>
     <user_mappings>
       <user_mapping>
         <domain>domain2.yourco.com</domain>
       </user_mapping>
     </user_mappings>
   </tenant_create>
   ```

You can control the users mapped into a tenant by specifying attributes. For example, if you only want users assigned to a specific department in AD to be mapped into the tenant, you can set key/value attributes. For example:

```
<user_mapping>
  <domain>domain2.yourco.com</domain>
   <attributes>
     <attribute>
     <key>department</key>
     <value>development</value>
    </attribute>
   <attributes>
  </user_mapping>
```

Alternatively, you can map users into the tenant based on their AD group. The following user mapping maps members of the "lab users" group into the tenant:

```
<user_mapping>
  <domain>domain2.yourco.com</domain>
  <groups>
   <group>lab users</group>
  </groups>
 </user_mapping>
```

You can include more than one ‹user_mapping› to enable users to be mapped from any of the specified mappings.

If you included more than one group in a ‹user_mapping›, the user must belong to all groups. In the example below, users must belong to both "lab users" and "lab administrators" groups to be mapped into the tenant.

```
<user_mapping>
  <domain>domain2.yourco.com</domain>
  <groups>
   <group>lab users</group>
   <group>lab administrators</group>
  </groups>
 </user_mapping>
```

Response

```
<tenant>
    <creation_time>1378919846777</creation_time>
    <id>urn:storageos:TenantOrg:4edc456c-
c7f5-4c54-84b2-29715cc8f504:</id>
    <inactive>false</inactive>
    <link href="/tenants/urn:storageos:TenantOrg:4edc456c-
c7f5-4c54-84b2-29715cc8f504:" rel="self"/>
    <name>EMC tenant</name>
    <tags/>
    <parent_tenant>
      <id>urn:storageos:TenantOrg:e5013f5e-41d7-4cf9-
b1fd-4fecfad0c18c:</id>
      <link href="/tenants/
urn:storageos:TenantOrg:e5013f5e-41d7-4cf9-b1fd-4fecfad0c18c:"
rel="self"/>
    </parent_tenant>
    <user_mappings>
      <user_mapping>
        <attributes/>
        <domain>domain2.yourco.com</domain>
        <groups/>
      </user_mapping>
    </user_mappings>
</tenant>
```

5. If you want to assign access to a virtual array to the newly created tenant you can use the following steps.
   By default, the access control list (ACL) for a virtual array is wide open and all tenants have access. Once you assign a tenant to the ACL for a virtual array, only that tenant will have access unless you assign other tenants to the ACL.

a. Get a list of virtual arrays.

Request

```
GET /vdc/varrays
```

Response

```
  <varrays>
    <varray>
      <id>urn:storageos:VirtualArray:1b86bbe1-c939-49d3-
b0ae-027dc95b1ccc:</id>
      <link href="/vdc/varrays/urn:storageos:VirtualArray:
1b86bbe1-c939-49d3-b0ae-027dc95b1ccc:" rel="self"/>
      <name>VSA</name>
    </varray>
  </varrays>
```

Use one of the virtual array IDs for the next step. This example shows the following ID:

```
<id>urn:storageos:VirtualArray:1b86bbe1-c939-49d3-
b0ae-027dc95b1ccc:</id>
```

b. Assign the new tenant access to a virtual array by adding this tenant to the ACL for the virtual array.

You must be authenticated as a user with the System Administrator or Security Administrator role to perform this operation.

Request

```
PUT /vdc/varrays/urn:storageos:VirtualArray:1b86bbe1-c939-49d3-
b0ae-027dc95b1ccc:/acl
  <acl_assignment_changes>
    <add>
      <privilege>USE</privilege>
      <tenant>urn:storageos:TenantOrg:4edc456c-
c7f5-4c54-84b2-29715cc8f504:</tenant>
    </add>
  </acl_assignment_changes>
```

Response

```
  <acl_assignments>
    <acl_assignment>
      <privilege>USE</privilege>
      <tenant>urn:storageos:TenantOrg:4edc456c-
c7f5-4c54-84b2-29715cc8f504:</tenant>
    </acl_assignment>
  </acl_assignments>
```

6. If you want to a assign access to a virtual pool to the new tenant you can use the following steps.

By default, the access control list (ACL) for a virtual pool is wide open and all tenants have access. Once you assign a tenant to the ACL for a virtual pool, only that tenant will have access unless you assign other tenants to the ACL.

a. Get a list of virtual pools. In the example below, file virtual pools have been listed.

Request

```
GET /file/vpools
```

Response

```
  <vpool_list>
    <virtualpool>
      <id>urn:storageos:VirtualPool:58406f8b-5a0e-41c0-
a91b-5a8c59ac3a02:</id>
```

```
      <link href="/file/vpools/urn:storageos:VirtualPool:
58406f8b-5a0e-41c0-a91b-5a8c59ac3a02:" rel="self"/>
      <name>vsp1</name>
      <vpool_type>file</vpool_type>
    </virtualpool>
  </vpool_list>
```

b. Retrieve the urn of a virtual pool and add the tenant to the ACL for that pool.

You must be authenticated as a user with the System Administrator or Security Administrator role to perform this operation.

Request

```
PUT /file/vpools/urn:storageos:VirtualPool:58406f8b-5a0e-41c0-
a91b-5a8c59ac3a02:/acl
  <acl_assignment_changes>
    <add>
      <privilege>USE</privilege>
      <tenant>urn:storageos:TenantOrg:4edc456c-
c7f5-4c54-84b2-29715cc8f504:</tenant>
    </add>
  </acl_assignment_changes>
```

Response

```
    <acl_assignments>
      <acl_assignment>
        <privilege>USE</privilege>
        <tenant>urn:storageos:TenantOrg:4edc456c-
c7f5-4c54-84b2-29715cc8f504:</tenant>
      </acl_assignment>
    </acl_assignments>
```

7. To perform any tenant-specific administration, you need to have a Tenant Administrator for the tenant. You can create a Tenant Administrator using the `/tenants/{id}/role-assignments` path, as shown below:

Request

```
PUT /tenants/urn:storageos:TenantOrg:4edc456c-
c7f5-4c54-84b2-29715cc8f504:/role-assignments

<role_assignment_change>
<add>
<role>TENANT_ADMIN</role>
<subject_id>fjones@domain2.yourco.com</subject_id>
</add>
</role_assignment_change>
```

8. For users to provision file or block storage, or to access object storage, the user must be assigned to a project. To create projects for the tenant, you can use `/tenants/{id}/projects`. For example:

Request

```
POST /tenants/urn:storageos:TenantOrg:4edc456c-
c7f5-4c54-84b2-29715cc8f504:/projects

<project_create>
   <name>marketing_project</name>
</project_create>
```

Response

```
<tenant_project>
    <id>urn:storageos:Project:
60a3069e-74cc-4e79-9857-1c121ce1635a:</id>
    <link href="/projects/urn:storageos:Project:
60a3069e-74cc-4e79-9857-1c121ce1635a:" rel="self"/>
    <name>marketing_project</name>
</tenant_project>
```

If you have assigned a user to the Tenant Administrator role for the tenant, they will automatically have access to the project.

You can use the `projects/{id}/acl` path to assign permissions to a user for the project. For example:

Request

```
PUT projects/ urn:storageos:Project:
60a3069e-74cc-4e79-9857-1c121ce1635a:/acl
<acl_assignment_changes>
   <add>
      <privilege>USE</privilege>
      <subject_id>bsmith@domain2.yourco.com</subject_id>
   </add>
</acl_assignment_changes>
```

9. If you want to use Data Services, you need to assign a namespace to the tenant and assign a default data services virtual pool. You can also assign a default project. You must be authenticated as a user with the System Administrator role to perform this operation.

   Request

   ```
   POST /object/namespaces/namespace
     <namespace_create>
       <namespace>namespace1</namespace>
       <vdcs>
         <tenant>urn:storageos:TenantOrg:4edc456c-
   c7f5-4c54-84b2-29715cc8f504:</tenant>
       </vdcs>
     </namespace_create>
   ```

   Response

   ```
     <namespace>
       <id>namespace1</id>
       <inactive>false</inactive>
       <link href="/object/namespaces/namespace/namespace1"
   rel="self"/>
       <tags/>
       <vdcs/>
     </namespace>
   ```

Configuring multiple tenants with the CLI

This section describes how to configure multiple tenants with the ViPR CLI. Complete the following procedure for each tenant you want to create.

Before you begin

- This procedure uses the ViPR CLI. Follow the setup instructions in the *EMC ViPR CLI Reference* to setup the command line interface.
- Follow the ViPR initial configuration for the Controller and Data Services in the *EMC ViPR Installation and Configuration Guide*.

Procedure

1. Authenticate using the "root" user.

   ```
   viprcli authenticate -u root -d /tmp
   ```

   ```
   Password: <enter user password>
   ```

2. Ensure you have an authentication provider that will authenticate users in your domain.

   Either:

- Create an authentication provider at the **Admin** › **Security** › **Authentication Providers** menu of the ViPR UI.
- Create an authentication provider using the CLI, as follows:

  a. Create a `provider.cfg` file in local folder. The content of `provider.cfg` should resemble the example below.

```
[Camb AD]
mode:ad
url:ldap://192.0.2.20
certificate:test_cert
passwd_user:Password
managerdn:CN=Administrator,CN=Users,DC=mytown,DC=emc,DC=com
searchbase:CN=Users,DC=mytown,DC=emc,DC=com
searchfilter:sAMAccountName=%U
searchkey:sAMAccountName
groupattr:CN
name:ad configuration
domains:mytown.emc.com
whitelist:*Admins*,*Test*
```

  b. Add AD/LDAP authentication provider. You must be authenticated as a user with the Security Administrator role to do this operation.
  `viprcli authentication add-provider -configfile provider.cfg`

3. Create a new tenant that uses the domain covered by the authentication provider. You need to be a Tenant Administrator for the parent tenant to create a tenant. For example:

   `viprcli tenant create -name marketing -domain mytown.emc.com`

4. You can control the users mapped into a tenant by specifying attributes or specifying AD group. For example, if you only want users assigned to a specific department in AD to be mapped into the tenant, you can set key/value attributes. For example:

   `viprcli tenant add-attribute -name marketing -key department -value marketingdepartment`

   This provides the ability, if required, to map uses from the same domain into different tenants by the appropriate attribute to their AD user.

   To map user from an Active Directory group into the tenant, you can use the `tenant add-group`. For example:

   `viprcli tenant add-group -name marketing -group "lab users" -domain mytown.emc.com`

5. If you want to assign access to a virtual array to the newly-created tenant, you can use the following steps.

   By default, the access control list (ACL) for a virtual array is wide open and all tenants have access. Once you assign a tenant to the ACL for a virtual array, only that tenant will have access unless you assign other tenants to the ACL.

   a. Get a list of virtual arrays.

   `viprcli varray list`

   b. Assign an array to the ACL for the tenant. For example:

   `viprcli allow -name <varray name> -tn marketing`

```
viprcli varray list
  NAME
  Isilon_Virtual_Array
  v_array
```

```
  viprcli varray allow -name Isilon_Virtual_Array -tenant
marketing
```

6. If you want to a assign access to a virtual pool to the newly-created tenant, you can use the following steps.

   By default, the access control list (ACL) for a virtual pool is wide open and all tenants have access. Once you assign a tenant to the ACL for a virtual pool, only that tenant will have access unless you assign other tenants to the ACL.

   a. Get a list of virtual pools, using:

   ```
   # viprcli vpool list -type file

   viprcli vpool list -type file

   Name                    Type    Protocol
   Isilon_Virtual_Pool     file    NFS
   ```

   or:

   ```
   viprcli vpool list -type block
   ```

   b. Give the tenant access to a virtual pool using `vpool allow`, as below:

   ```
   viprcli vpool allow -name Isilon_Virtual_Pool -tn
   marketing
   ```

7. For users to provision file or block storage, or to access object storage, the user must be assigned to a project. To create one or more projects for the tenant, use `project create`. For example:

   ```
   viprcli project create -name marketing_project -tn marketing
   ```

   You can assign users to the project using the update-acl operation and specifying the user and the appropriate privilege (own, use or backup).

   For example, to assign privileges to use a project , you might use:

   ```
   viprcli project update-acl -name marketing_project -tenant
   marketing -privilege use -subjectid bill@mytown.emc.com
   ```

   If you assign a user to the Tenant Administrator role for the tenant, they will automatically have access to all projects in the tenant.

   Note

   The next several steps are specific to Object/HDFS storage.

8. If you want to use Data Services, you need to assign a namespace to the tenant and assign a default data services virtual pool using the steps below. You can also assign a default project.

   a. Get a list of data services virtual pools.

   ```
   viprcli objectvpool list
     OBJECTVPOOL
     Isilon_DS_Virtual_Pool
   ```

   b. Create the namespace and assign a default virtual pool (cos). You can also assign a default project. You must be authenticated as a user with the System Administrator role to do this operation.

   ```
   viprcli namespace create -name namespace1 -cos
   Isilon_DS_Virtual_Pool -project marketing_project
   ```

Creating data store (secret) keys

Each object user requires their user id, from LDAP or Active Directory, and a secret key, also called an object data store key.

To generate a secret key for a user, use one of these three methods:

- Choose **User Menu › Manage Data Store Keys** from the ViPR UI.
- Call the following CLI operation:

  ```
  viprcli secretkeyuser add -uid <username from LDAP or AD>
  ```

- Call this ViPR REST API.

  ```
  POST object/secret-keys

  Request body
    <?xml version="1.0" encoding="UTF-8"?>
      <secret_key_create_param>
      <existing_key_expiry_time_mins>60</
  existing_key_expiry_time_mins>
    </secret_key_create_param>

  Response
    <user_secret_key>
      <secret_key>...</secret_key>
      <key_timestamp>...</key_timestamp>
      <link rel="..." href="..." />
    </user_secret_key>
  ```

CHAPTER 12

ViPR vApp Administration

This chapter contains the following topics:

Backup and restore of controller nodes

ViPR supports the recovery from failure of a minority node in a controller cluster. A ViPR cluster is still available when the majority of controller nodes are functional (2 of 3 nodes in 3-node cluster, or 3 of 5 nodes in 5 node cluster).

In the event of the failure of a ViPR node, the latest backup can be used to restore the node to the ViPR cluster and the restored node will automatically be brought to full functionality by the ViPR database synchronization and coordination services.

You should follow these guidelines for creating and restoring backups:

- VM backups should be taken for all controller nodes. There is no need to back up data nodes.
- VM backups for all controller nodes should be taken after a successful ViPR version upgrade.
- Only failed nodes need to be restored from their backup. There is no need to restore all nodes.

Creating a controller VM backup

Use a virtual machine (VM) backup tool to create a backup of the controller nodes.

Before you begin

The following prerequisites apply:

- Access to a third-party VM backup tool such as VMware vSphere Data Protection (VDP).
- If you are not using VMware VDP for a backup tool, and the tool you are using supports backup of the VM memory, disable the backup support for VM memory.

  Note

  Contact the backup tool vendor of to resolve issues and questions related to the tool.

- Access to the ViPR UI as System Administrator.
- Access to the ESX host with credentials appropriate for performing the backup.
- Access to vCenter with appropriate credentials.

It is recommended to always perform a backup of the ViPR controller VMs after a successful upgrade to a new ViPR version.

There is no requirement for the order of backing up the ViPR VMs in the cluster.

Procedure

1. Validate that the ViPR controller VMs, and daemons running on the controller VMs are running from the ViPR UI **Admin** › **System** › **System Health**.

   Note

   If the VMs or daemons are not running as expected, a restore may not work from the ViPR backup.

2. Use the VM backup tool to backup all the ViPR controller virtual machines in the cluster.

If using VMware VDP, use the vSphere Web Client to select the ViPR vApp controller VMs, and start the backup job. Optionally, use VMware VDP to schedule regular backup jobs on the ViPR vApp.

Restore a ViPR node from a backup

A ViPR node can be restored from a previously taken backup.

Before you begin

The following prerequisites apply:

- No DB (database) repair job can be running on any ViPR nodes when restoring any one of theViPR nodes. If the `AntiEntropyService.java (line 246) [repair #xxxx]..."` appears in `dbsvc.log`, the DB repair job is running.
- Only the failed ViPR node needs to be restored from backup. There is no need to restore all nodes.
- Access to the ESX host with credentials appropriate for performing the restore is required.
- Access to vCenter with appropriate credentials is required.

Procedure

1. Launch the VM restore tool to restore the failed node.

   If using VMware vSphere Data Protection (VDP):

   a. Select the previous backup of the ViPR virtual machine (VM) and restore it to its original location.

   b. After the VM is restored successfully, start the restored VM.
   A ViPR ViPR DB repair job is launched to recover the ViPR DB on the restored VM from the other good virtual machines in the cluster.

2. Perform the following monitoring tasks to determine when the VM restore has been successful.

Note

The VM may reboot once to apply system configuration property changes that may have been made.

Check	Details
Service Status	Check service status at the ViPR UI **Admin** › **System** › **System Health** › **Service Status**
DB Repair	Check `dbsvc.log` to find the message "Ending repair" to indicate db repair job done successfully. Message "repair job failed" indicates db repair job failure.
DB Node Status	Log in to the VM as root and run the following command to verify all db nodes are up and normal: `#/opt/storageos/bin/nodetool status`
Coordinator Status	Log in to the VM as root and run the Zookeeper `stat` command on the newly restored node to verify Zookeeper status. The following is an example of the output, your output might differ slightly:

Check	Details

	`telnet localhost 2181`
	`Trying 127.0.0.1...`
	`Connected to localhost.`
	`Escape character is '^]'.`
	`stat`
	`Zookeeper version: 3.4.5-1392090, built on 09/30/2012 17:52 GMT`
	`Clients:`
	`/10.32.72.188:54191[1](queued=0,recved=761,sent=761)....`
	`Latency min/avg/max: 0/0/120`
	`Received: 20266`
	`Sent: 20267`
	`Connections:18`
	`Outstanding: 0`
	`Zxid: 0x700000784`
	`Mode: leader`
	`Node count: 193`
	`Connection closed by foreign host.`

Syssvc Status Check	Check `syssvc.log` to make sure all system configuration properties are updated and synchronized with Zookeeper. The following messages indicate they are synchronized:
	`2013-09-09 03:02:14,697 [UpgradeManager] INFO UpgradeManager.java`
	`(line 226) Step7: If target version is changed, update`
	`2013-09-09 03:02:14,697 [UpgradeManager] INFO UpgradeManager.java (line 249)`
	`Step8: If target property is changed, update`
	`2013-09-09 03:02:14,697 [UpgradeManager] INFO UpgradeManager.java (line 267) Step9: sleep`