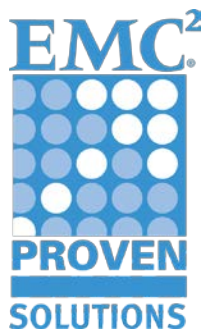Solution Guide

EMC ViPR for On-Demand File Storage with EMC Syncplicity and EMC Isilon or EMC VNX

EMC Solutions

Abstract

This document describes how to deploy EMC® ViPR® software-defined storage in an existing EMC Isilon® or EMC VNX® environment, provision storage, and integrate users into the EMC Syncplicity® file synchronization and sharing solution.

July 2015

EMC ViPR for On-Demand File Storage with EMC Syncplicity and EMC Isilon or EMC VNX
Solution Guide

Part Number H14275

EMC²

Contents

EMC²

Figures

Tables

Chapter 1   Introduction

This chapter presents the following topics:

EMC²

Purpose of this guide

This solution guide describes how to deploy EMC® ViPR® software-defined storage in an existing EMC Isilon® or EMC VNX® environment, provision storage, and seamlessly integrate users into the EMC Syncplicity® Enterprise File Sync and Share (EFSS) solution.

Isilon and VNX are used as examples to provide guidelines for deploying the ViPR storage automation software, ViPR Controller, to an existing storage infrastructure. The ViPR Controller configuration principles can also be applied to other types of storage infrastructure.

Scope

This guide describes the reference architecture for ViPR Controller and the Syncplicity EFSS solution. It also describes the installation and configuration steps to deploy the Syncplicity onsite storage solution on Isilon or VNX storage managed by ViPR.

For additional information regarding Syncplicity onsite storage, such as best practices, test results, and sizing information, refer to the *EMC Syncplicity File Sync and Share Solution Reference Architecture Guide*.

Audience

This document is for system managers and storage administrators who are considering ViPR solutions to simplify managing the heterogeneous storage infrastructure used to deploy Syncplicity.

This guide provides external references where applicable. EMC recommends that personnel implementing this solution be familiar with those documents. See Chapter 7, Reference Documentation, for details.

Business needs

The exponential growth of file and unstructured data and the increasing use of mobile devices present potentially overwhelming problems for enterprise storage and IT organizations. Also, employees now expect to have access to corporate and personal data across all their devices, whether they are working in or outside the office. If enterprise storage and IT organizations do not provide a cross-platform file synchronization and sharing service, employees might put confidential data and intellectual property in jeopardy by using a consumer cloud storage service.

These challenges have created a need for EFSS solutions to share and protect corporate and personal data.

To enable EFSS, IT departments must adopt enterprise-grade solutions, with security protocols to protect corporate data, while giving users mobile access to their content. However, creating a solution is complicated by the variety of hardware and software used by storage arrays. Modern enterprise IT departments need an easy way to

integrate multiple storage infrastructures , and ViPR self-service provisioning is the easy way to deploy new or existing EMC file storage infrastructure.

IT challenges

Implementing an EFSS solution using existing storage hardware presents several IT challenges, including:

- **Storage siloes with inefficient resource use**

  New IT endeavors require allocating and optimizing new storage. Because enterprise data centers tend to be mixed-vendor environments, storage can be allocated from a variety of sources. This piecemeal approach to storage allocation sometimes means that not all storage arrays are fully used. This problem is compounded by application administrators who may not be aware of all available storage resources.

- **Multiple administrator interfaces and utilities**

  Different storage arrays have their own management interface and provisioning and management processes. Mixed-array environments exacerbate the problem, as they provide poor visibility into storage usage, capacity, performance, and health. Storage administrators have become storage managers who spend more time managing arrays than optimizing storage for specific purposes.

- **Shortage of infrastructure skills needed to rapidly deploy storage**

  Because of storage array diversity, storage administrators can spend too much time identifying available storage capacity and manually provisioning storage. This is an inefficient use of valuable staff time and results in IT departments that cannot quickly or cost-effectively deliver storage solutions.

- **Length of time and number of technical resources needed to provision storage for applications**

  Application administrators rely on the storage deployed by storage administrators. The storage deployment process can be time-consuming and can lead to inefficiencies in the deployment of application environments.

ViPR solutions

EMC ViPR is a lightweight, software-only solution that transforms your existing storage environment into a simple, extensible, and open platform that can deliver fully automated storage services to help realize the full potential of the software-defined data center.

ViPR abstracts storage from physical arrays—whether file, block, or object based—into a pool of virtual shared storage resources that enables a flexible storage consumption model across physical arrays and delivers applications and innovative services.

ViPR abstracts the storage control path from the underlying hardware arrays, enabling centralized, software-based access to and management of multivendor storage infrastructures.

EMC²

Chapter 2 ViPR Architecture

This chapter presents the following topics:

Introduction

This chapter provides an overview of EMC ViPR architectural components and concepts used to deploy the Syncplicity EFSS solution, which has been validated and proven by EMC.

ViPR architecture overview

EMC ViPR presents a multivendor storage environment as one virtual array. ViPR uses software adapters to connect to the underlying arrays, similar to how device drivers enable device compatibility on a personal computer. ViPR exposes the APIs so any vendor, partner, or customer can create new adapters to add new arrays. This creates an extensible plug-and-play storage environment that automatically discovers and maps arrays, hosts, and SAN fabrics. Figure 1 shows the solution architecture.
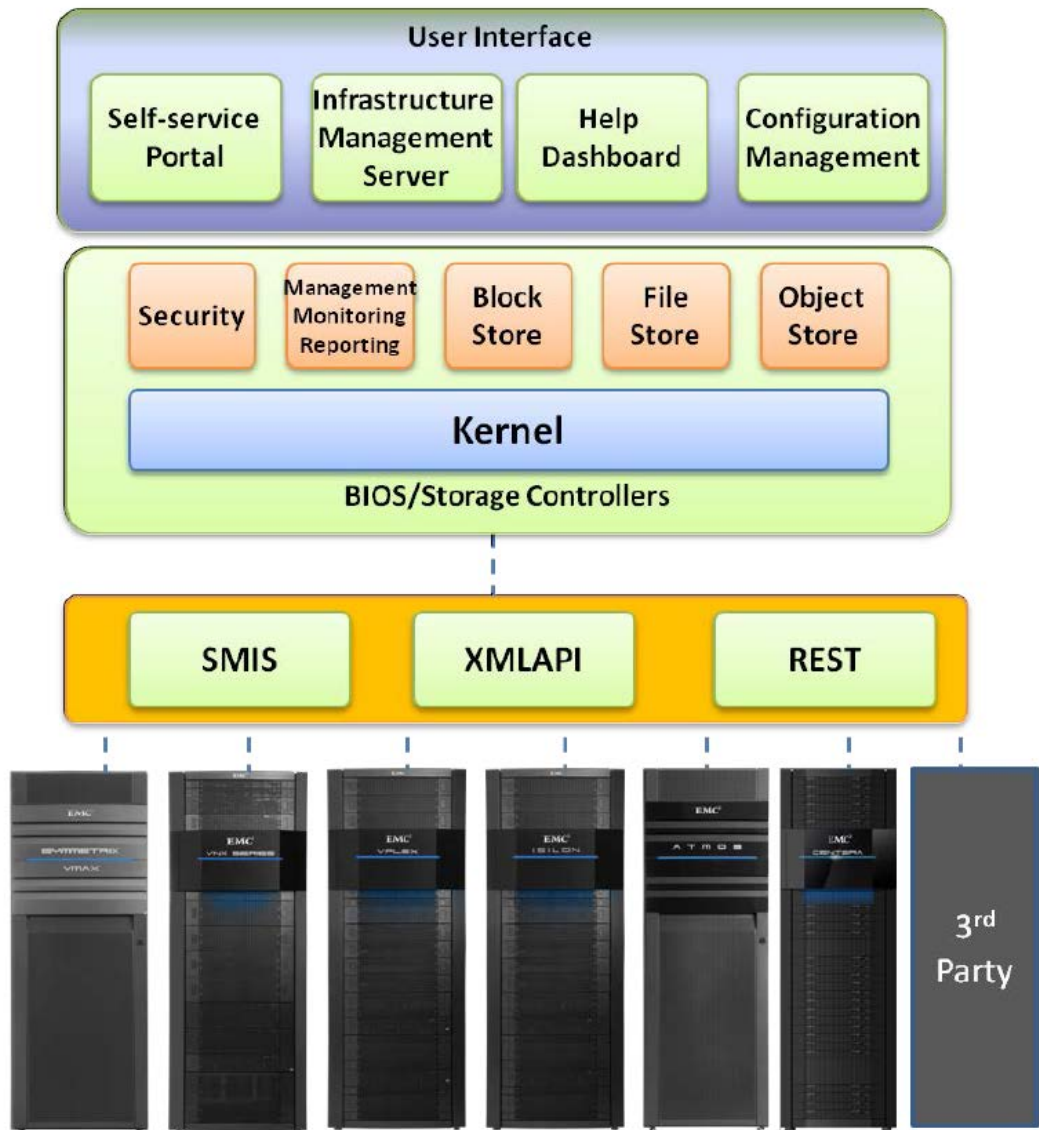

Figure 1.   ViPR architecture

When a storage administrator adds arrays, ViPR discovers the arrays and all their corresponding storage pools and ports. ViPR automatically discovers and maps the Fibre Channel networks when the Fibre Channel switches are added. ViPR can map and virtualize the following EMC and non-EMC arrays:

- EMC Isilon, EMC VMAX®, EMC VNX, and EMC VPLEX®
- Dell, Hitachi Data Systems (HDS), HP, IBM, NetApp, Oracle, and SolidFire
- Certified HP commodity hardware

ViPR hides the complexity of all the underlying storage arrays and exposes their core functionality as services while retaining the unique attributes of the arrays. Storage administrators then create virtual storage pools in ViPR that represent sets of capabilities required by unique application workloads.

For example, a transactional workload would be best served by a virtual storage pool that features the characteristics of high-performance block storage such as EMC VMAX. A cloud application such as Syncplicity is not as performance-sensitive and works well on commodity hardware.

In either case, customers subscribe to a virtual storage pool that meets their workload demands. Users do not know or care about the underlying hardware and software that is providing the service to their application.

With ViPR, rather than provision space on a specific array, storage administrators can expose a unique and customizable combination of hardware and software resources as consumable services.

ViPR with Syncplicity architectural components

A typical enterprise IT infrastructure might contain existing EMC storage arrays such as Isilon and VNX. With ViPR, storage, infrastructure, and application administrators can simplify the management of storage infrastructures used to deploy Syncplicity.

Here is the list of architectural components and the function of each component in this solution:

- **ViPR Controller**

  ViPR Controller is a virtual appliance. Storage and infrastructure administrators deploy ViPR Controllers in their virtual environment. Typically a ViPR Controller is installed as a virtual appliance in vCenter.

- **Active Directory servers**

  We integrated existing Active Directory servers with ViPR Controller. Storage administrators and users from multiple domains or tenant groups are authenticated by authentication providers when they log in to ViPR Controller.

- **Isilon and VNX storage arrays**

  File storage for Syncplicity was provisioned from Isilon X410 and VNX7600™. SAN block storage was provisioned as datastores from VNX7600 for the ESXi hosts.

- **Syncplicity storage connectors**

  Syncplicity storage connectors are application servers in a data center. The Syncplicity storage connectors are virtual appliance servers running CentOS 6.4. ViPR automatically allocates file storage from virtual arrays and exports the file storage to Syncplicity storage connectors.

- **Fibre Channel and IP switches**

  Fibre Channel switches connect SAN arrays while IP switches connect NAS storage. ViPR Controller can scan an existing SAN and IP network and gather switch information such as zoning device connectivity. ViPR can analyze existing networks and intelligently manage switch information to meet application expectations. For example, ViPR can add or modify zoning information and determine which servers are connected to the storage.

- **Users from different departments or companies**

  The users from different departments or companies are referred to as tenants. All tenants are authorized via Active Directory services.

  ViPR can be configured with multiple tenants. Tenants have their own environment for creating and managing storage, which cannot be accessed by users from other tenants. For more information, refer to Understanding ViPR Multi-Tenant Configuration.

  Tenant or project administrators are responsible for creating projects and using an access control list (ACL) to assign users to projects and to assign user permissions. Projects are defined with a schema that enables tenants to use or manage storage resources.

Sample data center diagram

Figure 2 shows a logical diagram of our sample data center. In this sample data center, ViPR Controllers are added as virtual appliances. Each blade server is also an ESXi host. The data center has 12 UCS blade servers, two UCS 6296 interconnects, one VNX7600, and one Isilon X410. It also contains vCenter server appliances, Active Directory servers, DNS servers, DHCP servers, VMware Horizon View servers, and Syncplicity Panorama Connectors running on ESXi hosts.
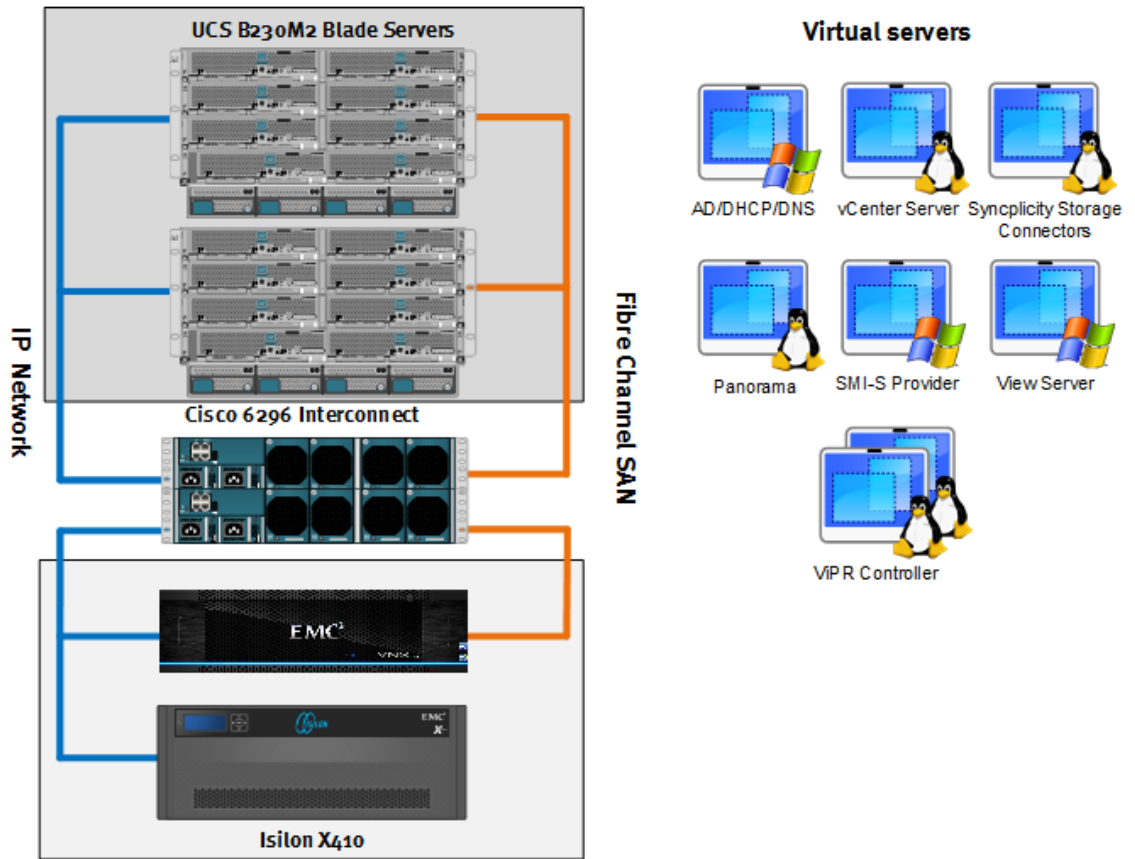
EMC²

Figure 2.   Sample data center diagram

Chapter 3   Before You Begin

This chapter presents the following topics:

EMC²

About ViPR

ViPR is an out-of-band storage management application. It does not sit in the I/O path between servers and data storage arrays. It uses an IP connection to scan, read, and edit information from the components it manages. ViPR Controller must have IP network connectivity to storage devices, Fibre Channel switches, IP switches, SMI-S providers, and servers. ViPR is ready to manage components as soon as IP connectivity is established.

When existing storage arrays are added to ViPR, ViPR Controller collects important information such as the World Wide Port Names (WWPNs) of storage ports and storage pools accessible via SMI-S providers.

ViPR Controller can manage switches when it has both WWPNs from storage ports and the host bus adapter World Wide Name from servers. ViPR Controller zones the switches based on which server is connected to which storage ports.

Predeployment checklist

Set up the components in Table 1 before you begin to implement ViPR.

Table 1.   Environment readiness checklist

	Description	IP address/hostname	Credentials	Comments
1	ViPR Controller	10.244.156.250		
2	ViPR Controller 1	10.244.156.251	Initial login: root/ChangeMe	
3	ViPR Controller 2	10.244.156.252	Initial login: root/ChangeMe	
4	DNS/gateway/NTP	10.244.156.244/ 10.244.156.1		
5	ViPR Controller OVA installation file		Default root login: root/ChangeMe	
6	Your vCenter infrastructure	10.244.156.180	Administration login credential and permission	
7	Your SMI-S provider hostname or IP address and its installation OVA file	10.244.156.242	Initial login: admin/#1Password	SMI-S provider software is SMI-S_Provider*_WINDOWS-x64-SMI.exe.
8	All the IP addresses for your NAS storage	10.244.156.134, 10.244.156.150		10.244.156.150 is a control station IP address for VNX file.
9	Hostnames/IP addresses for FC/IP switches	10.244.156.9, 10.244.156.10, 10.244.156.11	Administration login and password to each of the switches	

	Description	IP address/hostname	Credentials	Comments
10	Hostnames/IP addresses for all the servers being managed	Hostname/IP addresses for all the physical servers being managed		
11	Compute Image Server IP address/hostname	10.244.156.178		
12	Active Directory server	10.244.156.244		Make sure that you have administrator login and permission to this authentication provider.

Checking IP connectivity

After you install ViPR Controller, ensure that each component can communicate with ViPR Controller. Check connectivity as follows:

1. Open an SSH session and log in to servers, switches, the Isilon or VNX, and the control station.

2. Ping your ViPR Controller to make sure the connection is working.

ViPR deployment readiness checklist

Prepare to install and configure the EMC ViPR Controller as follows:

- Identify the Isilon node pools and VNX storage pools in the data center to be used by ViPR. You can put a subset of an array's storage under the control of ViPR.

- Collect array credentials, IP addresses, and ports for the storage you plan to add to ViPR.

  - You will need to provide credentials for an account with administrator privileges on the array when you add VNX and Isilon to ViPR.

  - For VNX, collect credentials for the VNX onboard SMI-S Provider. VNX has an SMI-S Provider that runs on its Control Station.

- Identify a VMware instance on which to deploy ViPR Controller.

- Collect credentials to access the VMware instance. Deploying ViPR Controller requires an account that has privileges to deploy virtual machines on the VMware instance.

- Verify that the VMware instance has sufficient resources for ViPR Controller.

- Identify four IP addresses for a non-production deployment or six IP addresses for a production deployment. The addresses are used by the ViPR Controller virtual machines and for the virtual IP addresses used by REST clients and the UI to access the system. The addresses can be IPv4 or IPv6.

EMC²

- Identify a user authentication provider. ViPR validates users against an authentication server. You need an Active Directory or LDAP server to use accounts other than the built-in user accounts.

- Identify two or three DNS servers. You will have to supply two or three DNS server IP addresses during ViPR initial configuration.

- Identify two or three NTP servers. You will have to supply two or three reliable and synchronized NTP servers during ViPR initial configuration.

- For each ViPR Controller virtual machine, collect an IP address, an IP network mask, an IP network gateway, and, optionally, an IPv6 prefix length and IPv6 default gateway. You will need this information when deploying ViPR Controller.

- Obtain an EMC license. Obtain the license authorization code and use it at the EMC license management web page to obtain a license file. After deployment, upload the license file using the ViPR UI, CLI, or API.

Note: Refer to the *EMC ViPR Support Matrix* for supported storage models and VMware versions.

Chapter 4   ViPR Implementation

This chapter presents the following topics:

EMC²

Introduction

This chapter provides information on how to implement ViPR. Table 2 lists the main stages in the ViPR implementation process.

Table 2.   Implementing ViPR: Process overview

Stage	Description
1	Installing ViPR Controller
2	Configuring users and projects
3	Configuring the ViPR virtual data center

Installing ViPR Controller

Refer to *Install EMC ViPR Controller on VMware as a vApp*. Follow that procedure to install ViPR Controller as a vApp on vSphere Enterprise edition and perform the initial configuration.

Configuring users and projects

This section provides information about configuring users and projects in ViPR, so that authenticated users can log into ViPR with their Active Directory user accounts and use ViPR object data and services associated with their projects.

The tasks, which are described in the following sections, are as follows:

1. Adding users to ViPR via authentication providers
2. Assigning roles to users
3. Creating multiple tenants (optional)
4. Creating projects

Adding users to ViPR via authentication providers

A ViPR user must be discovered and added through an authentication provider like Active Directory before a user can log in and be assigned roles or ACLs.

User authentication is done by adding an authentication provider to ViPR Controller by going to **Security** › **Authentication Providers** in the ViPR UI. Refer to *Add an Authentication Provider to EMC ViPR*.

Assigning roles to users

ViPR has two role levels: virtual data center (VDC) roles and tenant roles. VDC roles are used to set up the ViPR environment, which is shared by all tenants. Tenant roles are used to administer the tenant-specific settings, such as the service catalog and projects, and to assign additional users to tenant roles.

Make sure that you are familiar with the main concepts behind roles that are described in *Understanding Users, Roles, and ACLs*.

ViPR has a local root user who has all roles required to set up the VDC and the root tenant, and is used to bootstrap the system by assigning the required administrator roles. Role administration is as follows:

- The root user assigns a user to the Security Administrator role.
- The Security Administrator:
  - Creates a System Administrator to set up the VDC
  - Creates a Tenant Administrator for the provider tenant to administer tenant level resources
- The Tenant Administrator creates tenant roles for tenants or sub-tenants.

Refer to the procedure in *Assign ViPR Roles*.

Creating multiple tenants (optional)

You can configure ViPR so that each tenant has his or her own environment for creating and managing storage. Other tenants cannot access storage resources assigned to a tenant. You can create a single level of tenants under the provider tenant. Optionally, if an enterprise has multiple departments that need to use ViPR storage resources, you can create multiple tenants for different departments.

Create ViPR Tenants provides the steps for creating a tenant from the ViPR UI as part of ViPR installation. To add multitenant support to an existing ViPR VDC, refer to *Understanding ViPR Multi-Tenant Configuration* to ensure that you understand what a multitenant configuration has to offer. Refer to *Add a New Tenant to an Existing ViPR Virtual Data Center* to perform the configuration steps.

Figure 3 shows an example of how to add tenants to ViPR Controller.

EMC^2

Figure 3.   Adding tenants in ViPR

Creating projects   File resources provisioned with ViPR, and all object data created in the ViPR object store, must be associated with a project. Projects are tenant resources and are created and managed by the Tenant Administrator or delegated to a Project Administrator. To perform ViPR object store configuration, a project must exist for a tenant.

Refer to *Understanding ViPR Projects and Consistency Groups* to understand the role of projects within ViPR and how to work with them. Refer to *Create ViPR Projects* for the steps to create projects in ViPR.

Configuring the ViPR virtual data center

This section describes how to add Isilon and VNX file storage systems to ViPR and then create ViPR virtual assets.

You must have a working ViPR Controller installed in the data center, and it must be ready to manage the SAN and NAS devices. Make sure that ViPR Controller has IP network connectivity to each of the components such as storage devices, Fibre Channel switches, IP switches, SMI-S providers, and servers.

Make sure that remote login is enabled in ViPR by doing the following:

1. Open an SSH session to ViPR Controller.

2. Ping each management IP port for storage devices, switches, servers, and SMI-S providers.

3. When IP connectivity is verified, proceed to Adding Isilon to ViPR or Adding VNX to ViPR, depending on your storage system.

Adding Isilon to ViPR

Add Isilon storage to ViPR as follows:

1. Log in to the ViPR UI with System Administrator privileges.

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

3. Click **Add**.

4. Set the following parameters, , as shown in Figure 4:

   ▪ **Type**: **EMC Isilon**

   ▪ **Name**: *<a storage system name for Isilon>*

   ▪ **IP Address**: *<Isilon Smart Connect IP>*

   ▪ **Port**: 8080

   ▪ **User**: root

   ▪ **Password**: *<password for Isilon root user>*

5. Click **Save**.
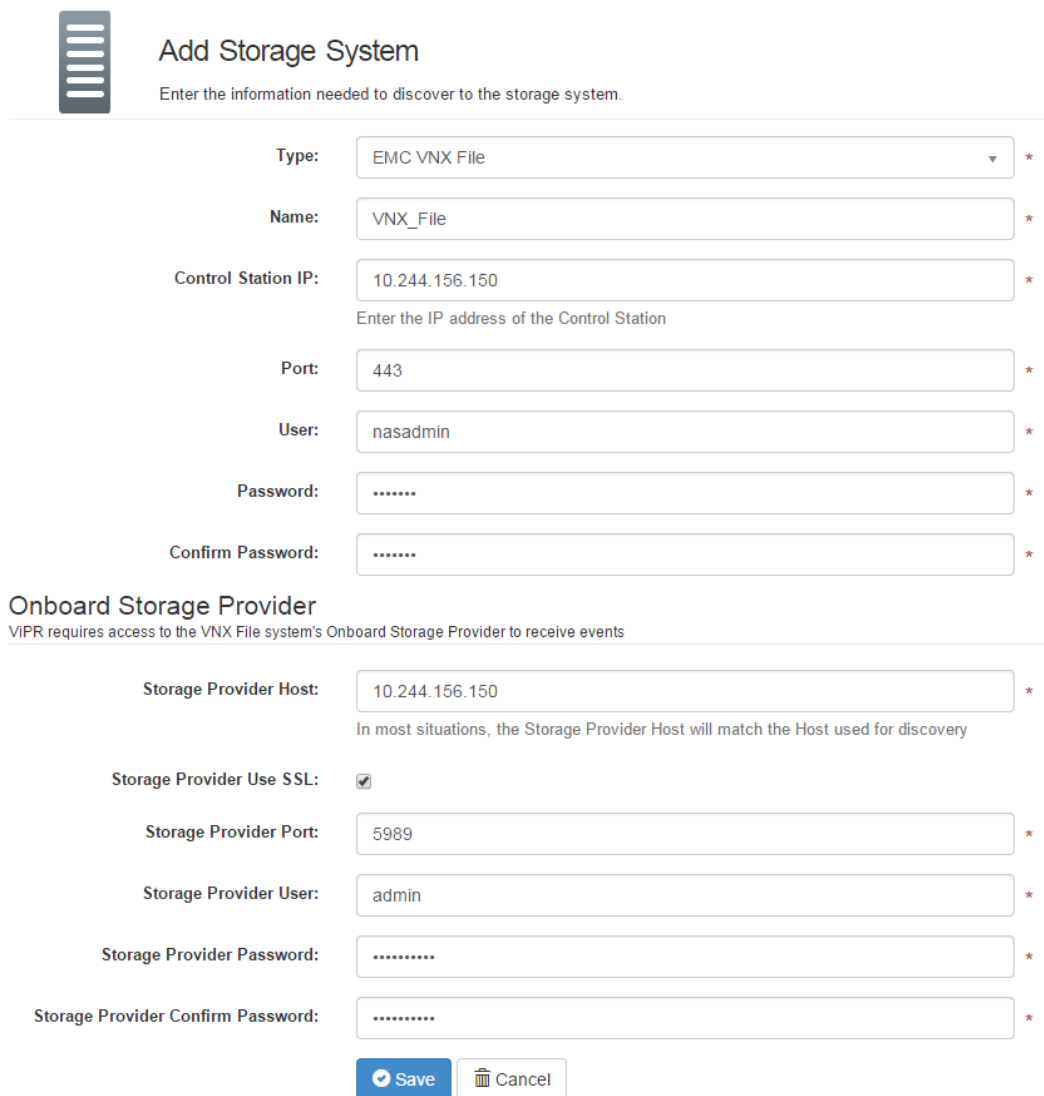
Figure 4.   Adding Isilon to ViPR

EMC²

Chapter 4: ViPR Implementation

Adding VNX to ViPR

Add VNX file storage to ViPR as follows, as shown in Figure 5:

1. Log in to the ViPR UI with System Administrator privileges.

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

3. Click **Add**.

4. Set the following parameters:

   - **Type**: **EMC VNX File**

   - **Name**: *<a storage system name for VNX File>*

   - **Control Station IP**: *<VNX File Control Station IP address>*

   - **Port**: 443

   - **User**: nasadmin

   - **Password**: *<VNX File Password>*

   - **Onboard Storage Provider**

     – **Storage Provider Host**: <Same as Control Station IP>

     – **Storage Provider Use SSL**: Select the check box

     – **Storage Provider Port**: 5989

     – **Storage Provider User**: admin

     – **Storage Provider Password**: #1Password

5. Click **Save**.

Figure 5.   Adding VNX to ViPR

Adding Syncplicity storage connectors as hosts to ViPR

Syncplicity storage connectors are based on CentOS 6.4. Add the connectors to ViPR as Linux hosts as follows:

1. Select **Physical Assets** › **Hosts**.

2. Select the tenant.

3. Click **Add**.

4. Set the following parameters, as shown in Figure 6:

    ▪ **Operating System**: **Linux**

    ▪ **Name**: *<a name for the Syncplicity storage connector>*

    ▪ **Host**: *<the fully qualified domain name or IP address>*

    ▪ **Port**: *<SSH connection port number>*

EMC²

- **Discoverable**: Select the check box

- **Username** and **Password**: `<login credentials for Syncplicity storage connector>`

5. Click **Save**.

Figure 6.   Adding Syncplicity storage connectors as Linux hosts

To provision storage from both Isilon and VNX, you need at least one Syncplicity storage connector for each storage system. You can also deploy the storage connectors in pairs for high availability. For more sizing information, refer to *EMC Syncplicity File Sync and Share Solution Reference Architecture Guide*.

Creating and configuring ViPR virtual arrays

Creating a virtual array

Follow these steps to add storage systems to create a virtual array:

1. Select **Virtual Assets** › **Virtual Arrays**.

2. Click **Add** and type the virtual array name.

3. At **Edit Virtual Array**, select 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 the virtual array.

    - Select **Manual** to configure the zones outside of ViPR.

4. If working in a multitenant environment, click **Grant Access to Tenant**, and select the tenants that will have access to the virtual array.

5. Click **Storage Systems** to add both Isilon and VNX File storage systems to ViPR.

6. Optionally, click **Storage Ports** to add or remove the physical storage ports associated with the virtual array.

7. Optionally, click **Storage Pools** to view the physical storage pools associated with the virtual array.

    You can also add or remove the storage pools from the list of storage pools in the virtual array. This only removes the storage pools from the list. It does not remove the storage pool from the ViPR resources.

8. Click **Save**.

Creating an IP network

ViPR can discover the ports of IP-connected storage systems and hosts, but it cannot discover the paths between them. You must create IP networks and then add the host and storage system ports to the same IP network. The host and storage system are provisioned together.

1. Select **Virtual Assets** › **Virtual Array**.

2. Select the virtual array.

3. Under **Edit Virtual Array**, click **Networks**.

4. Click **Create IP Network**.

5. Leave the selected virtual array, and select any other virtual array to be added to the network.

6. Add host ports for Syncplicity storage connectors to the network:

    ▪ Select **Add** › **Add Host Ports** to select from the list of discovered host ports.

       or

    ▪ Select **Add** › **Add Ports** to enter the host ports manually.

7. Add storage ports for Isilon and VNX File storage systems to the network:

    ▪ Click **Add** › **Add Array Ports** to select from the list of discovered array ports.

       or

    ▪ Click **Add** › **Add Ports** to enter the storage ports manually.

8. Click **Save**.

Creating virtual pools for file storage

This section describes the steps to create virtual pools for file storage from Isilon and VNX file storage systems in ViPR.

Creating an Isilon virtual pool

Follow these steps to create an Isilon virtual pool:

1. Select **Virtual Asset › File Virtual Pools**.

2. Click **Add**.

3. At **Create File Virtual Pool**, set the following parameters, as shown in Figure 7:

   - Type a **Name** and a **Description** for the Isilon File virtual pool.

   - At **Virtual Arrays**, select the virtual array for which the virtual pool will be created.

   - Expand **Hardware** and define the following criteria:

     - **Provisioning Type: Thin**

     - **Protocols: CIFS, NFS**

     - **System Type: EMC Isilon**

   - Expand **Data Protection** to define the maximum number of local snapshots allowed for resources from this virtual pool.

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

   - Expand **Access Control** to restrict access in a multiple tenant environment.

     - Select **Grant Access to Tenants**.

     - Select the **Tenants** that will have access to this virtual pool.

   - Expand **Storage Pools** to view the discovered storage pools.

     - Set **Pool Assignment** to **Manual**.

     - Select the Isilon node pools that will be included in the virtual pool.

4. Click **Save**.

Figure 7.   Creating an Isilon virtual pool for file storage

Creating a VNX virtual pool

Follow these steps to create a VNX virtual pool:

1.   Select **Virtual Asset** › **File Virtual Pools**.

2.   Click **Add**.

3.   At **Create File Virtual Pool,** set the following parameters, as shown in Figure 8:

- Type a **Name** and a **Description** for the VNX virtual pool.

- At **Virtual Arrays,** select a virtual array for which the virtual pool will be created.

- Expand **Hardware** and define the following criteria:

  – **Provisioning Type**: **Thin**

  – **Protocols**: **CIFS, NFS**

  – **System Type**: **EMC VNX File**

- Expand **Data Protection** to define the maximum number of local snapshots allowed for resources from this virtual pool.

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

- Expand **Access Control** to restrict access in a multiple tenant environment.

  – Select **Grant Access to Tenants**.

  – Select the **Tenants** that will have access to the virtual pool.

- Expand **Storage Pools** to view the discovered storage pools.

  – Set **Pool Assignment** to **Manual**.

  – Select the VNX storage pools that will be included in the virtual pool.

4. Click **Save**.

Figure 8.   Creating VNX virtual pool for file storage

Verifying installation

After completing the previous tasks, log in to ViPR Controller and select **System › Dashboard**. This displays an overview of ViPR Controller. You can view the physical components in the dashboard, as shown in Figure 9.
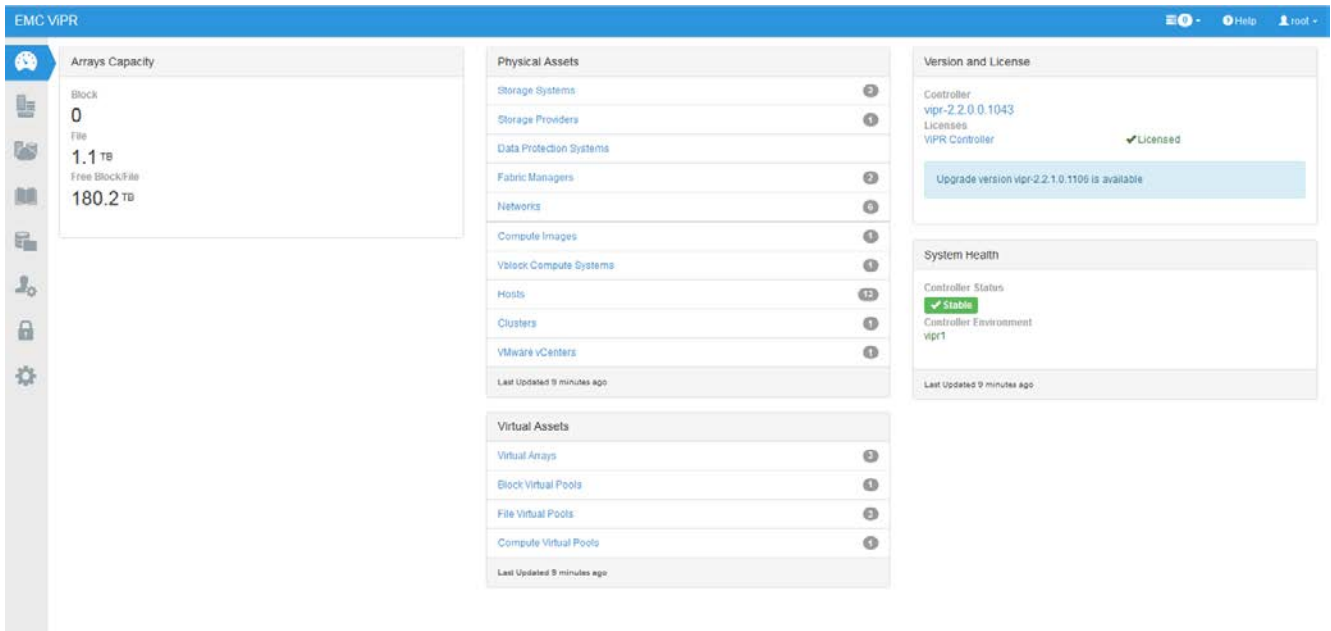
Figure 9.   ViPR management user interface

Chapter 5   Syncplicity Architecture

This chapter presents the following topics:

EMC²

Introduction

This chapter is an overview of the Syncplicity file synchronization and sharing solution architecture. For additional information regarding Syncplicity onsite storage, refer to *EMC Syncplicity File Sync and Share Solution Reference Architecture Guide*.

Syncplicity architecture overview

The Syncplicity architecture includes three main components:

- A cloud-based **orchestration layer** that provides user management, group management, policy enforcement, and metadata operations for sharing files and folders across the enterprise. This is a multitenant, cloud-based service that is common across all Syncplicity customers.

- **Compute nodes** that provide the termination point where client systems access their files. Compute nodes control where files are stored in Syncplicity and provide the interface between the orchestration layer and the on-premises storage systems. A one-to-one or many-to-one relationship exists between compute nodes and the network file system (NFS) or object storage system.

- The **storage layer,** which is the actual NFS or object storage that the compute nodes use to store user and group files. The Isilon and VNX virtual pools in ViPR provide NFS storage.

Figure 10 illustrates these components and how data and files flow between them.

Figure 10.   EMC Syncplicity file synchronization and sharing architecture

Syncplicity architectural components

Client
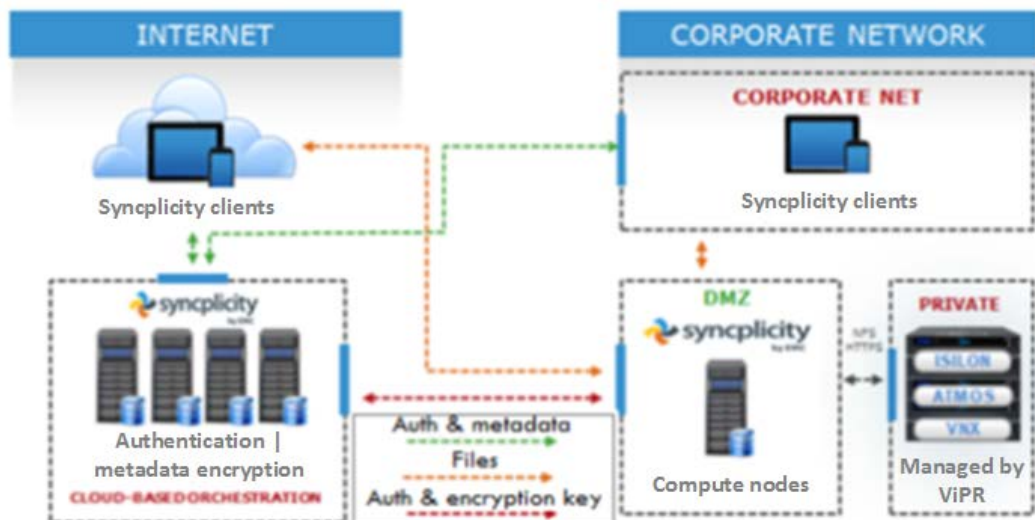The client can be a mobile phone, tablet, or personal computer with the Syncplicity client software installed. It can also be a web browser interface used to access Syncplicity files or, for an IT administrator, to set permissions and policies.

Orchestration
Orchestration includes the following:

- Authentication, unless delegated to Security Assertion Markup Language (SAML)/OpenID single sign-on (SSO)

- Authorization

- Account administration

- Metadata management

- Sharing and collaboration

- Web application

- API, with the exception of file transfer

Orchestration is complex and benefits greatly from being offered as a software-as-a-service (SaaS) application. As a SaaS application, it frees IT from deployment and maintenance problems, delivers a constant stream of enhancements and innovations, and enables seamless enterprise collaboration across the extended enterprise.

Data stored in the orchestration layer is minimal. It includes:

- File name, creation date, size, and SHA-256 hash

- Storage information, including number of chunks, chunk size, encryption key, and data length after encryption or compression or both

- Virtual path relative to the synchronization point root on the compute nodes

- Full path to the location where synchronized folders are mapped on user devices

Information such as file size, SHA-256 hash, and encryption keys are stored in databases separate from all user-specific information.

Compute
The compute function is delivered by compute nodes (also known as storage connectors), which are deployed as virtual machines that control where files (and past file versions) are stored in Syncplicity.

The enterprise storage solution provides the ability to enable or disable encryption at the compute layer, depending on administrative preferences and the security structure. The compute node exposes file transfer APIs, encryption, compression, file transfer resumption, and image thumbnail generation. The compute application is deployed on one or more virtual machines, depending on load and availability requirements. All deployed compute application instances are completely stateless and independent of one another. Instances can be added and removed based on load requirements.

EMC²

By design, clients may reach any instance in the pool with any request, including requests for various segments of the same file being uploaded. Clients initiate file transfers (uploads and downloads) directly with the compute application. File data does not flow through the orchestration component at any time.

Storage

The storage component, StorageVaults, stores file data in a highly available, redundant, and scalable back end designed for instant data access. The files that Syncplicity preserves in the storage layer are stored in an opaque container on the storage array that is optimized for enterprise synchronization and sharing. Files are always stored in an unreadable format.

End users have no direct access to backend storage. Only the compute node communicates with end users and manages the storage reads and writes.

ViPR

ViPR abstracts the storage control path from the underlying hardware arrays, enabling centralized, software-based access to and management of multivendor storage infrastructures.

Chapter 6   Integrating Syncplicity with ViPR

This chapter presents the following topics:

EMC²

Introduction

This chapter describes how to install Syncplicity storage connectors, create NFS exports to Syncplicity with ViPR file services, and configure Syncplicity storage connectors and on-premises storage settings. It also discusses extending storage infrastructure for Syncplicity in ViPR and using ViPR file services to simplify storage functionality.

Table 3 lists the main tasks in the solution implementation process.

Table 3.   Integrating Syncplicity with ViPR: Process overview

Stage	Description
1	Installing Syncplicity storage connectors
2	Creating NFS exports to Syncplicity with ViPR file services
3	Configuring Syncplicity storage connectors
4	Configuring Syncplicity on-premises storage settings
5	Extending storage infrastructure for Syncplicity in ViPR
6	Using ViPR file services to simplify storage functionality

Installing Syncplicity storage connectors

Prerequisites

Refer to the *Prerequisites* on the Syncplicity support website to review the prerequisites for deploying Syncplicity on-premises storage connectors.

To provision storage from both Isilon and VNX, you need at least one Syncplicity storage connector for each storage system. You can also deploy the storage connectors in pairs for high availability. For more sizing information, refer to the *EMC Syncplicity File Sync and Share Solution Reference Architecture Guide*.

Deploying the OVF template

The Syncplicity on-premises storage connector is a virtual machine image in OVA format. The virtual machine image is based on the CentOS 6.4 operating system. It contains the necessary Syncplicity software.

To deploy the OVF template, go to **Task 1: Deploy the OVF Template** in Installing the Storage Connector.

Logging in and changing your password

To log in and change the password, go to **Task 2: Log In and Change Your Password** in Installing the Storage Connector.

Configuring the network connection	To configure the network connection, go to **Task 3: Configure the Network Connection** in <u>Installing the Storage Connector</u>.

Configuring SSL	Each Syncplicity storage connector must have a static IP address assigned to it. To configure SSL, go to **Task 4: Configure SSL** in <u>Installing the Storage Connector</u>.

Creating NFS exports to Syncplicity with ViPR file services

You previously added both Isilon and VNX storage systems as well as Syncplicity storage connectors to ViPR Controller, and created virtual pools for each storage system. You can now use ViPR file services to create file systems from the virtual pools and create NFS exports for Syncplicity storage connectors.

Refer to <u>What are the ViPR File Provisioning and Protection Facilities?</u> for more information on ViPR file services.

Creating NFS exports with ViPR file services

From Isilon virtual pools

Follow these steps to create file systems and NFS exports from an Isilon virtual pool:

1. Log in to the ViPR UI with an Active Directory administrator account.

2. Select **Service Catalog** › **View Catalog** › **File Storage Services**.

3. Select **Create File System and NFS Export**.

4. Set the following parameters, as shown in Figure 11:

    -   **Virtual Array**: *<Virtual array you created>*

    -   **Virtual Pool**: *<Isilon File virtual pool you created>*

    -   **Project**: *<Project you created>*

    -   **Export Name**: *<A name for the NFS export>*

    -   **Size (GB)**: *<File system size, in GB>*

    -   **Export Rules** › **Export Hosts**: *<IP address of the related Syncplicity storage connector>*

        Note: Click **+Add** to add more Syncplicity storage connectors if necessary.

5. Click **Order**.

    Wait for the order to complete.

EMC²

Figure 11. Creating file system and NFS export

From VNX virtual pools

To create another file system and NFS export from a VNX virtual pool, follow the steps under Creating NFS exports with ViPR file services with the following exceptions:

1. Select the VNX virtual pool in **Virtual Pool** list box.

2. In **Export Rules** › **Export Hosts**, enter the IP addresses for other Syncplicity storage connectors deployed to work with VNX file storage.

Mounting the NFS export on the Syncplicity storage connector

Once the NFS export is created in ViPR, you can view the order by selecting **Resources** › **File Systems** to find its mount point, as shown in Figure 12.

Figure 12. NFS export mount point

To mount the Isilon NFS export on the Syncplicity storage connector, go to **Task 5a: Configure Isilon** in *Installing the Storage Connector*.

To mount the VNX File NFS export on the Syncplicity storage connector, go to **Task 5b: Configure Standard NFS v3 Storage** in *Installing the Storage Connector*.

Configuring Syncplicity storage connectors

You must edit the Syncplicity software configuration file on every Syncplicity storage connector to complete the installation. You must also obtain the access key from **Syncplicity administrative console** › **Settings** › **Manage StorageVaults**. Refer to *Configuring the Storage Connector* for detailed procedures.

Configuring Syncplicity on-premises storage settings

At this point, fully functional Syncplicity storage connectors with NFS exports are provisioned via ViPR. The next step is to point the Syncplicity account to the storage connector URL via the Syncplicity StorageVault settings.

To add or edit a StorageVault, go to the My Syncplicity website and log in as an administrator. Select **Admin** › **Settings**, and then click the **Manage StorageVaults** link in the **Enterprise Edition Features** section.

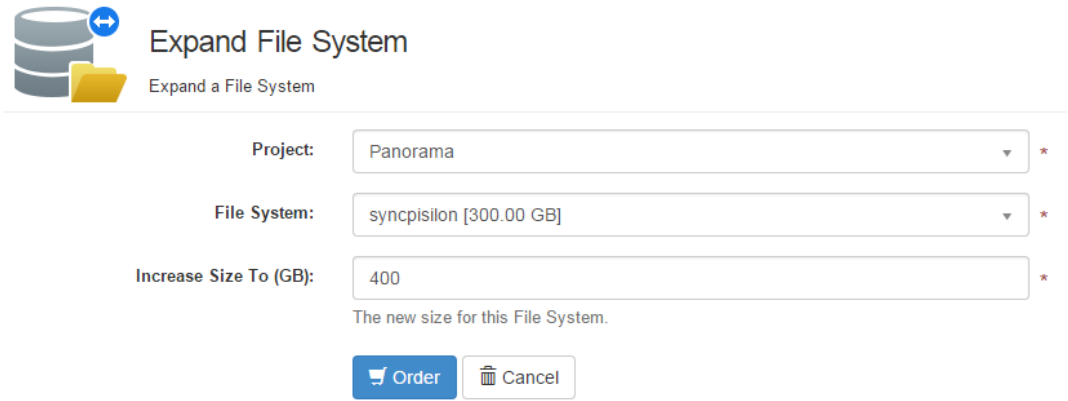Refer to Configuring and managing the on-premise storage settings for more information.

Extending storage infrastructure for Syncplicity in ViPR

When more Syncplicity users are added, the file system and NFS export can become full and must be expanded.

Expanding a file system

Follow these steps to expand an existing file system in ViPR:

1. Log in to the ViPR UI with an Active Directory user account.

2. Select **Service Catalog** › **View Catalog** › **File Storage Services**.

3. Select **Expand File System,** and set the following parameters, as shown in Figure 13:

   - Select the **Project** for Syncplicity and the **File System** to be expanded.

   - In the **Increase Size To (GB)** field, type the new size for the file system.

4. Click **Order**.

EMC²

Expand File System

Expand a File System

Project: Panorama ▾ *

File System: syncpisilon [300.00 GB] ▾ *

Increase Size To (GB): 400 *

The new size for this File System.

🛒 Order   🗑 Cancel

Figure 13.   Expanding a file system

Extending Syncplicity users to a new storage pool

You might have a new batch of application users that need to be added to Syncplicity, but they are on an alternative storage pool because they have different performance, security, or availability requirements. Follow these steps:

1. Follow the steps in Creating a virtual array to create a new physical storage.

2. Follow the steps in Creating virtual pools based on the new physical storage pools from Isilon or VNX.

3. Follow the steps in Installing Syncplicity storage connectors.

4. Follow the steps in Creating NFS exports to Syncplicity with ViPR file services to create a new virtual pool.

5. To associate the new users to the new Syncplicity storage connectors, log in to the Syncplicity administrative console and create new StorageVaults and storage sets.

   Refer to Configuring and managing the on-premise storage settings and Configuring and managing storage sets for instructions.

6. Follow the steps in Configuring Syncplicity storage connectors and Configuring Syncplicity on-premises storage settings to finish the process.

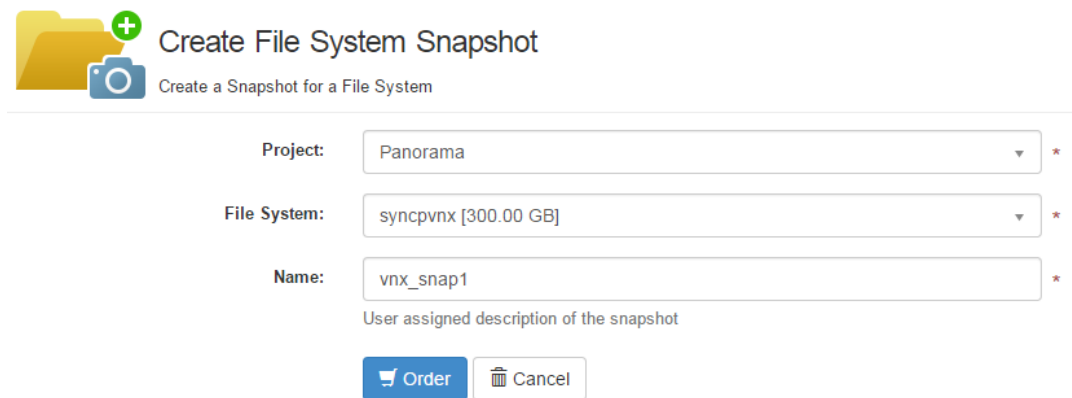# Using ViPR file services to simplify storage functionality

You can also use ViPR file services to simplify storage functions. For example, to protect production data, you typically need to follow various procedures in different storage systems user interfaces or execute complex CLI instructions. With ViPR file protection services, you can easily perform data protection operations such as creating, restoring, and removing file system snapshots.

To create a snapshot of a file system, the virtual pool that the file system is assigned to must be enabled for snapshots. In the UI you can access the virtual pool by selecting **Virtual Assets** › **File Virtual Pools**. You can set the number of snapshots allowed for a virtual pool by selecting **Data Protection** › **Maximum Snapshots**.

Creating a file system snapshot

Follow these steps to create a file system snapshot:

1. Log in to the ViPR UI with an Active Directory user account.

2. Select **Service Catalog** › **View Catalog** › **File Protection Services**.

3. Select **Create File System Snapshot** and set the following parameters, as shown in Figure 14:

    ▪ Select the **Project** for Syncplicity and the **File System** for which you want to create a snapshot.

    ▪ Type a **Name** for the file system snapshot.

4. Click **Order**.

Figure 14.   Creating a file system snapshot

Restoring a file system snapshot

Follow these steps to restore a file system snapshot:

1. Log in to the ViPR UI with an Active Directory user account.

2. Select **Service Catalog** › **View Catalog** › **File Protection Services**.

3. Select **Restore File System Snapshot** and set the following parameters, as shown in Figure 15:

    ▪ Select the **Project** for Syncplicity and the **File System** for which you want to restore a snapshot.

    ▪ Select the **Snapshot** to be restored.

4. Click **Order**.

EMC²

Figure 15.   Restoring a file system snapshot

Removing a file system snapshot

Follow these steps to remove a file system snapshot:

1. Log in to the ViPR UI with an Active Directory user account.

2. Select **Service Catalog** › **View Catalog** › **File Protection Services**.

3. Select **Remove File System Snapshot** and set the following parameters, as shown in Figure 16:

    ▪   Select the **Project** for Syncplicity and the **File System** for which you want to remove a snapshot.

    ▪   Select the **Snapshot** to be removed.

4. Click **Order**.

Figure 16.   Removing a file system snapshot

Refer to What are the ViPR File Provisioning and Protection Facilities? for more information about ViPR file services.

Chapter 7   Reference Documentation

This chapter presents the following topics:

EMC²

ViPR documentation

The following documents, available at EMC.com, provide additional and relevant information:

- *Realizing Software-Defined Storage with EMC ViPR*
- *Understanding ViPR Users, Roles, and ACLs*
- *Understanding ViPR Multi-Tenant Configuration*
- *Understanding Projects and Consistency Groups*
- *Unleash the Value of Data with EMC ViPR Services white paper*
- *ViPR Support Matrix*

Syncplicity documentation

The following documents, available at EMC.com, provide additional and relevant information:

- EMC IT Deploys Syncplicity with Private Cloud Storage
- EMC Syncplicity File Sync and Share Solution Reference Architecture Guide*EMC Syncplicity File Sync and Share Solution with EMC Isilon Scale-Out NAS Implementation Guide*
- *EMC Syncplicity File Sync and Share Solution with EMC VNX Storage Implementation Guide*
- How EMC IT Deployed Syncplicity with On-Premises Storage

The following documents are available on the Syncplicity Support site:

- *Configuring and managing storage sets*
- *Configuring and managing StorageVaults*
- *Configuring and managing the on-premise storage settings*
- *Deploying Syncplicity On-Premise Storage Connector*