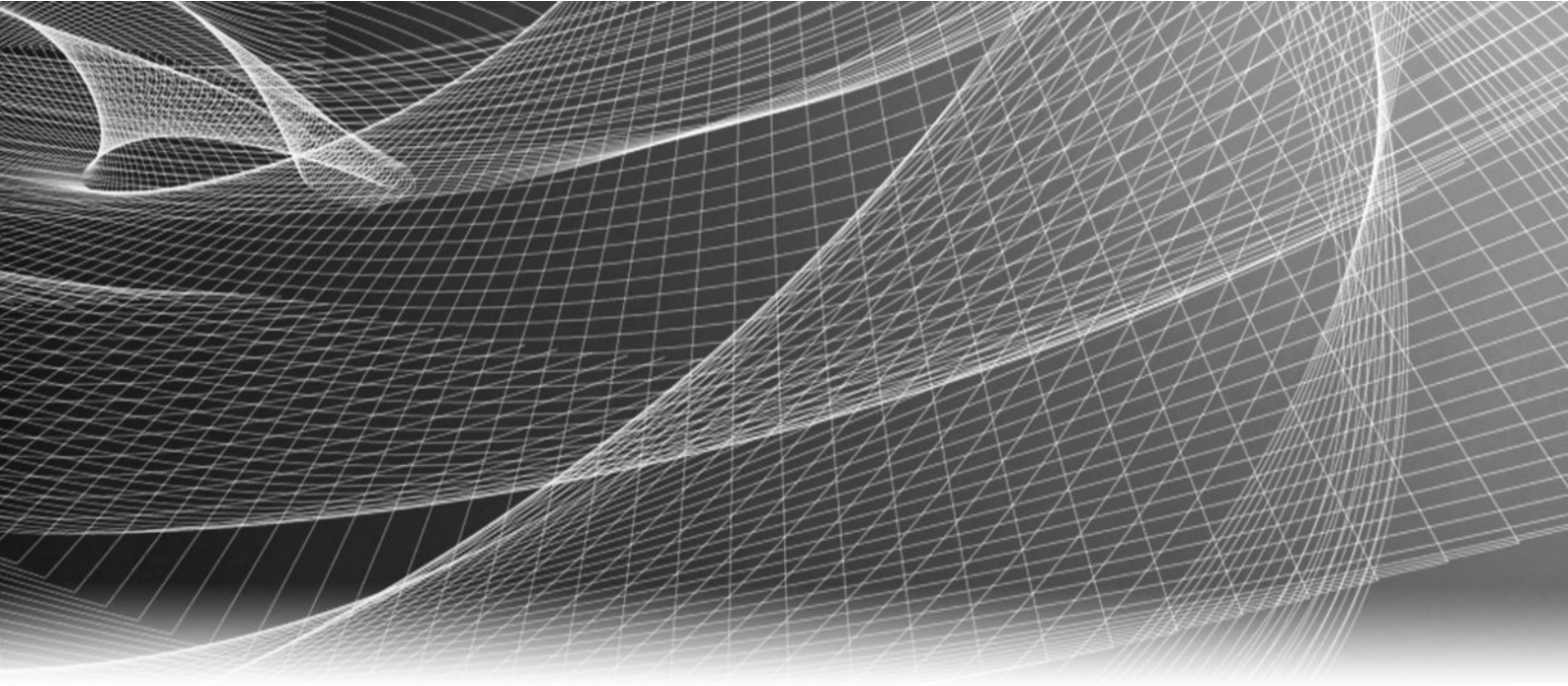

EMC ViPR Controller

Version 2.4

Backup and Disaster Recovery Guide

302-002-414

01

EMC²

Published November, 2015

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

CONTENTS

CHAPTER 1

Backup and restore options for ViPR Controller

Restore of the ViPR Controller instance can be performed for a single ViPR Controller virtual machine (VM), multiple VMs, or when all VMs have failed. How you decide to restore depends on your configuration, and which tool you are using.

Table 1 Options to restore ViPR Controller

Restore options	When to use:	Is ViPR Controller available during recovery?	Supported environment
ViPR Controller Minority node recovery from node failure on page 8	ViPR Controller is still in production (a quorum number of nodes are up and running), and: • 1 VM is permanently lost when ViPR Controller is deployed on 3 VMs. • Up to 2 VMs permanently lost when ViPR Controller is deployed on 5 VMs.	Yes, available	Single, or Multi-VDC, and installed on • VMwre without vApp • Hyper-V Not supported when installed with a vApp.
ViPR Controller native backup and restore service on page 12	• More than half of nodes are permanently lost. • Any number of nodes are permanently lost when installed with a vApp.	Not available	Single, or Multi-VDC, and installed on • VMware wiht vApp • VMware without vApp • Hyper-V
	Backup and restore can also be used to reconfigure the ViPR Controller virtual data center as follows: • Migrate ViPR Controller from a 3 node installation to a 5 node installation, or from a 5 node installation to a 3 node installation. • To relocate the ViPR Controller instance to new location using different IP addresses.	Not available	Single VDC only installed on • VMware with vApp • VMware without vApp • Hyper-V
	• Change the ViPR Controller instance with vApp to a an instance without a vApp.		Single VDC only, installed on VMware

Table 1 Options to restore ViPR Controller (continued)

Restore options	When to use:	Is ViPR Controller available during recovery?	Supported environment
	• Change the ViPR Controller instance without vApp to a an instance with a vApp.		
VMware Site Recovery Manager (SRM) on page 20	In case of a datacenter disaster, VMware SRM for backup and recovery of ViPR Controller allows for quick recovery of a ViPR Controller instance at a recovery site.	Not available	Single VDC only, and installed on • VMware with vApp • VMware without vApp

ViPR Controller post restore

After restoring ViPR Controller, ViPR Controller continues to manage existing available resources.

In case of a disaster including physical resources managed by ViPR Controller

- When there is no array replication under ViPR Controller management, ViPR Controller continues to manage resources which are still available, until remaining are up online.
- When there is array replication under ViPR Controller management (SRDF, RecoverPoint), after restoring ViPR Controller, the storage administrator initiates the necessary failover operations from the “Block Protection Services” in the Service Catalog on the ViPR Controller managed resources to make them available on the recovery sites.

  Note

  Please note that any supported failover operations on ViPR Controller managed array replicated resources should be performed using ViPR Controller , to avoid any subsequent issues with managing these resources using ViPR Controller post failover.

- For ViPR Controller managed SRDF volumes, in the event of a datacenter disaster, if for any reason Failover or Swap of volumes was performed outside of ViPR Controller, perform ViPR Controller rediscovery of underlying storage arrays before performing further action on these resources using ViPR Controller.
- For ViPR Controller managed RecoverPoint protected volumes in the event of a datacenter disaster, If for any reason Failover or Swap of volumes was performed outside of ViPR Controller, return volumes to original state before continuing to manage these resources using ViPR Controller.

CHAPTER 2

Minority Node Recovery

Minority node recovery from node failure

Minority node recovery allows you to recover the ViPR Controller virtual machines (VMs) when the minority number of nodes (1 in a 3 node deployment, or 1, or 2 nodes in a 5 node deployment), while ViPR Controller remains available, and in production.

Before you begin

- Minority node recovery is only supported for ViPR Controller VMware installations without a vApp, or installations on Hyper-V.
- If a virtual machine becomes corrupt, first work with the virtual machine native software to fix the virtual machine. If there is no successful way to fix the virtual machine through the native software, use ViPR Controller minority node recovery to resolve the issue.
- If a ViPR Controller node was down for more than 5 days, you must perform a minority node recovery on the node before it can be added back to the cluster.
- When re-using an IP for the new machine, be sure to powerdown the virtual machine that are currently using the IP.
- Node recovery can be performed through the ViPR Controller UI, REST API, or CLI.
- ViPR Controller Security Administrators can perform a node recovery operation from the ViPR Controller REST API, and CLI.
- You must be assigned to both the ViPR Controller Security Administrator and System Administrator role to initiate a node recovery operation, and to review the recovery status from the ViPR Controller UI.
- System Monitors can see the Node recovery status in the ViPR Controller UI.
- Security Administrators, System Administrators, and System Monitors can see the node recovery status from the ViPR Controller CLI.
- As part of the recovery operation, you will need to redeploy the failed VM. For a VMware installation with no vApp, or a Hyper-V deployment it is recommended that you redeploy the VM from the same system, and path location from which the VM was originally deployed so that the VM settings are available, and can be pre-filled by deployment script during redeployment. When redeploying the failed node, you will need to download the configuration parameters from ViPR Controller, using the ViPR Controller UI, **Recovery** page and pass it as a `–file` parameter to the redeployment script.

Procedure

1. From virtual machine management software, delete the virtual machine (VM) for each failed node.

   In a 3 node environment only 1 node should be deleted, and 2 nodes should remain available, and running.

   In a 5 node environment only up to 2 nodes should be deleted, and at least 3 nodes should remain available, and running.

2. From the ViPR Controller UI, go to the **System** › **Recovery** page, and click **Download Config Parameters**, and save the configProperties file in a location where you will be running the deployment script. The configProperties file contains the network settings of cluster.
3. Run the `vipr-version-deployment.sh`, or `vipr-version-deployment.ps` followed by:

```
-mode redeploy -file configProperties
```

For the installer script to redeploy ViPR Controller use the `configProperties` file you saved in step 3 as the file argument for the vm network settings.

Note

When entering the vmname, you could use a different name to redeploy the virtual machine, but it is recommended to use the same name that was used for the failed vm.

If you omit a required option, the installer will enter interactive mode. When you enter a value or values in interactive mode, do not use quotes. For example the script will prompt you for location of ConfigProperties file and for VMware password. It will also prompt you for VM settings values, if you did not preserve .settings file from the initial deployment. If you do have this file, the script will re-use the values.

Run the following command for each virtual machine you are restoring.

- bash shell:

```
./vipr-2.4.0.0.xxxx-deployment.sh -mode redeploy -file
configProperties
```

- PowerShell:

```
.\vipr-2.4.0.0.xxxx-deployment.ps1 -mode redeploy -file
configProperties
```

For more deployment options see the *ViPR Controller Installation, Upgrade, and Maintenance Guide* which is available from the ViPR Controller Product Documentation Index .

4. Do not power the virtual machine on after deployment.
5. From the ViPR Controller UI, go back to the **System** › **Recovery** page, and click **Start Node Recovery** to initiate the recovery process.
6. Power on the redeployed vm(s) to initiate the discovery process.
7. Continue to monitor the progess of recovery from the **Node Recovery** page.

CHAPTER 3

EMC ViPR Controller Native Backup and Restore Service

EMC ViPR Controller native backup and restore service

The EMC ViPR Controller native backup and restore service is used to create a backup set of the ViPR Controller nodes. The backup set can be scheduled using the ViPR Controller UI, or created through REST API calls, or the viprcli CLI.

The ViPR Controller backup set is a near point-in-time copy of the persistent data (the Cassandra and Zookeeper data files, and the geodb database, which contains data related to multisite ViPR Controller) on all the ViPR Controller nodes. Volatile data such as logs and binaries are not part of the backup set.

The backup set is generated as a set of files on local storage (`/data/backup/`). For protection, it is highly recommended that you configure an external server to automatically upload backups daily. Use the ViPR Controller UI to specify the external server. Alternatively, you can manually copy backup sets to secondary storage using the REST call:

```
GET /backupset/download
```

or with CLI:

```
viprcli system download-backup
```

ViPR Controller internally retains the last 5 backups. Contact EMC Customer Support if you would like to change the retention policy.

Backup and restore must be between the same ViPR Controller version (for example, version 2.4.0.0.1043 must be restored to 2.4.0.0.1043).

Scheduled backup files, are saved to a zip file with the following naming convention:

```
vipr-<version>-<total number of nodes in installation>-
<timestamp>-<total number of nodes>-<number of nodes backed
up>.zip
```

For example

```
vipr-2.4-3.201510100800-3-2.zip
```

Manual backup uses the following naming convention: for example:

```
manualbackupname.<total number of nodes in installation>-
<number of nodes backed up>.zip
```

for example:

```
backupname-3-2.zip
```

Restoring ViPR Controller from a 3 node installation to a 5 node installation, or from a 5 node installation to a 3 node installation, and restoring using different IP addresses is not supported in a GEO Federated environment.

Schedule backups using the ViPR Controller UI

You can use the ViPR Controller UI to schedule a daily backup of the ViPR Controller internal databases, and upload backups to an external storage location.

Before you begin

- This operation can only be performed by ViPR Controller Security Administrators.

- To upload backups to an external server, you need the URL of the server and credentials for an account with read and write privileges on the server. Specifying an external server is optional but is highly recommended.
- Recommended storage allocation for external server storage is 30% of the total disk space allocated for the ViPR Controller VMs.

Procedure

1. Select **Settings** › **General Configuration** › **Backup**.
2. Enter values for the properties.

Option	Description
Enable Scheduler	True turns on the scheduler.
Backup Time	Select the time of day when the backup runs. The backup runs once a day; you cannot change the frequency of the backup. The time of day is the time where the ViPR Controller UI is running.
External Server URL	Specify the URL of an external file server. Supported protocols are ftp and ftps. Example: `ftps://10.233.95.162/my-vipr-backup/` If your FTPS server is configured with Explicit FTPS: • The backup server URL should start with ftp://. • Communication is performed over port 21. If your FTPS server is configured with Implicit FTPS: • The backup server URL should start with ftps://. • In this case port 990 is used. The filename format of the backup file that is uploaded to the external server is: `vipr-<version>-<total number of nodes in installation>-<date and time>-<total number of nodes>-<number of nodes backed up>.zip`. Example: In the following examples: • `vipr-2.3-3-20150707010002-3-3.zip`, 3-3 means all nodes in a 3 node installation have been backed up to the zip file. • `vipr-2.3-5-20150707010002-5-3.zip` 5-3 means that only 3 of the nodes in a 5 node installation have been backed up to the zip file. As long as more than half of all nodes are included in backup (which means they were available when backup was taken) , the backup can be used for successful restore.
User Name	User name for an account with read and write privileges the FTPS server.
Password	Password for the account.

3. **Save**.

After you finish

Backup and upload success and failure messages are logged in the Audit log. Email notification of failure is sent only to the address associated with the ViPR Controller root

user; be sure to add a valid email address at **root** › **Preferences** from the main ViPR UI page.

Summary of REST API for EMC ViPR Controller backup and restore service

This is a summary of the REST API for the EMC ViPR Controller backup and restore service.

You must be assigned a System Administrators role to use the ViPR Controller REST API (or CLI) to use the backup and restore service.

For details see the ViPR Controller REST API Reference .

GET /backupset/
Lists all backups.

POST /backupset/backup/
Creates a new backup. Note the following restrictions on the backupsetname, which might not be covered in *EMC ViPR Controller REST API Reference*:

- The backupsetname maximum length is 200 characters.
- Underscore (_) not supported.
- Otherwise, any character supported in a Linux filename can be used.

DELETE /backupset/backup/
Deletes a backup.

GET /backupset/download?tag=*backupsetname*
Collects the backup set from all nodes and creates a .zip bundle supported by restore utility.

Below is an example using curl to download a backup.

```
curl -ik -X GET -H "X-SDS-AUTH-TOKEN: token_value"
"https://vipr_ip:4443/backupset/download?tag=backupsetname"
> backupsetname.zip
```

The token value is obtained while authenticating with the ViPR Controller REST API . For authentication steps see: *ViPR Controller REST API Virtual Data Center Configuration Guide*, which is available from the ViPR Controller Product Documentation Index .

Summary of viprcli options for native backup

You can create, delete, list, and download a backup using viprcli.

Restore, quota, and purge commands are not currently available through viprcli.

The *EMC ViPR Controller CLI Reference* guide describes how to install and use viprcli.

Create backup

```
viprcli system create-backup -n backupname [-force]
```

`-force` ignores errors and tries to create the backup. Returns success if backup is created, else returns failure and rolls back. Useful in the case of a single node crash.

Delete backup

```
viprcli system delete-backup -n backupname
```

List all backups

```
viprcli system list-backup
```

Download backup

Collects the backup set from all nodes and creates a .zip bundle supported by restore utility.

```
viprcli system download-backup -n backupname -fp filepath
```

Example: `viprcli system download-backup -n 20140728155625 -fp C:\20140728155625.zip`

Back up EMC ViPR Controller internal databases with command line or REST API

You can use POST /backupset/backup/ or the viprcli CLI to back up the ViPR Controller internal databases.

Before you begin

- This task requires the System Administrator (SYSTEM_ADMIN) role in ViPR Controller.
- Services on at least two nodes in a 2+1 deployment, or three nodes in a 3+2 deployment, must have a status of "Good". In the ViPR UI, go to **System** › **Health** › **Services**.
- Not required, but it is better to back up when no database repair is in progress. If the backup is created during database repair, the backup data of each node will not be consistent. A database node repair after restore will take a long time, resulting in a longer overall time to recovery. You can check the progress of the database repair from the ViPR Controller UI, **System** › **Database Housekeeping Status** page.
- It is recommended that the load on the system be light during the time of backup, especially on operations related to volume, fileshare, export, and snapshots.

Procedure

1. On a ViPR Controller node, initiate a backup using one of these methods. Any method creates the backup in /data/backup/ on all ViPR Controller nodes. It is not necessary to run the command on each node:

Method	Command
REST API	`POST /backupset/backup`
viprcli	`viprcli system create-backup -n backupname`

2. Use one of these methods to generate a file containing the backup set, which you can copy to secondary media:

Method	Command
REST API	`GET /backupset/download?tag=backupsetname`
viprcli	`viprcli system download-backup -n backupname -fp filepath`

Restoring from a backup

Use the restore command to restore a backup created by the EMC ViPR Controller backup service.

Before you begin

- Credentials for root user are required. If root ssh is disabled, you will also need credentials for the local ViPR Controller svcuser account.
- The target system must meet these requirements:
  - The target system must be a new deployment of the complete ViPR Controller.
  - When redeploying a single virtual data center environment, you can use different IP addresses, from the originals to restore the instance. You must use the same IP addresses when redeploying in a multi VDC environment.
  - The target system must be at the same ViPR Controller version as the version of the backup set.
  - The size of /data on the target system must be equal to or greater than that of the backed up system.

Procedure

1. If the VDC that you are restoring is part of a geo federated (multisite) configuration, refer to Restoring a virtual data center in a geo federated (multisite) environment on page 28.
2. If you will be restoring to the same IP addresses, shut down the entire old ViPR Controller instance.

   Otherwise continue to the next step.
3. Depending on your deployment type, deploy a new ViPR Controller system using the steps described in the *ViPR Controller Installation, Upgrade, and Maintenance Guide* which is available from the ViPR Controller Product Documentation Index .
4. Power on the virtual machines.

   The dbsvc, geosvc, and controllersvc services must have started at least once.

   Keep in mind that all system properties that you set during Initial Setup will be overwritten by the values in the backup that you restore in an upcoming step.
5. Copy the backup ZIP file from the external server on which you store your backups, to a location on one of the newly deployed ViPR Controller nodes.

   Note that remote login as root might be disabled. It may be necessary to log in initially as svcuser, then switch user to root.
6. Restore the backup by running the following command as the root user:

   `/opt/storageos/bin/restore backup_ZIP_filepath`

   Example: **`/opt/storageos/bin/restore /tmp/vipr-2.4-3-201510100800-3-2.zip`**

   You initiate restore on one node only. Restore on the other nodes happens automatically.
7. Verify that the health of the system, and of all services, is good (in the ViPR Controller UI under **System** › **Health**).

8. Go to the ViPR Controller UI, Dashboard page, and see the Database Consistency Status to see the progress of the database repair. The progress is complete when the status is Successful and progress is 100%. This might require several hours.
9. When you have verified the health of the new system, delete the old ViPR Controller instance. (Do not power on the old instance; if the old and new instances use the same IP addresses, IP conflict issues will result.)

After you finish

If after restoring, the ViPR Controller state remains "Syncing" because the previously downloaded ViPR Controller image files referenced in backup are not available for automatic download through the ViPR Controller upgrade repository, you will need to perform the following steps.

1. View syssvc log, and locate the associated error, for example:

```
Get remote image URL for version (vipr-2.x.x.x.xxx) failed:

com.emc.storageos.systemservices.exceptions.RemoteRepositoryExcepti
on: Failed to read repository null (java.lang.NullPointerException)
```

2. Forcefully remove such image by running the following CLI command for each image that had an issue downloading:

```
/opt/storageos/cli/bin/viprcli system remove-image -v
vipr-2.x.x.x.xxx -force
```

The ViPR Controller cluster should return to STABLE.

Note

The system will be cleaned from all corresponding, previously downloaded images that were there at the time of backup.

Use backup and restore to reconfigure the ViPR Controller instance

The native backup and restore feature can be used: to restore ViPR Controller using different IP addresses from the original system, to change the number of nodes on which ViPR Controller is installed, to change the ViPR Controller instance with vApp to an instance without a vApp instance, or to change the ViPR Controller instance without a vApp to an instance with a vApp.

Before you begin

ViPR Controller can be restored from a 3 node installation to a 5 node installation, or from a 5 node installation to a 3 node installation.

Restoring to migrate ViPR Controller from a 3 node installation to a 5 node installation, or from a 5 node installation to a 3 node installation is not supported in a GEO Federated environment.

Procedure

1. Deploy a new ViPR Controller with the new IP address, or different number of nodes as described in the *ViPR Controller Installation, Upgrade, and Maintenance Guide* which is available from the ViPR Controller Product Documentation Index .
2. Download the ViPR Controller backup files from the FTP site configured in: Schedule backups using the ViPR Controller UI on page 12.

3. Restore the backup on the new ViPR Controller instance as described in Restore backup on page 16.

Note

After restore is complete, other system configuration settings used in original ViPR Controller instance will be in effect and may need to be updated.

After you finish

After restore wait a few minutes, and login to ViPR Controller UI, and make any of the necessary changes described below:

- NTP server, and DNS servers if they should be different based on the new ViPR Controller location.
- ViPR Controller Keystore (in case a CA signed certificate was used in original ViPR Controller.

Note

If self signed certificate was used in original ViPR Controller, then a new self signed certificate will autocratically be generated in the restored ViPR Controller so no action is needed.

- Check all settings under **System** › **General Configuration**, and verify that they are valid for restored ViPR Controller instance.

Considerations when recovering data after restoring a ViPR Controller backup

There are some best practices you should consider when recovering user data that was created or modified after the latest backup.

Details of a data recovery are dependent on the specific configuration. Use these high level steps as a guide when recovering resources that were added, modified, or deleted before a crash, but after the backup that you are restoring:

1. Restore the ViPR Controller backup.
2. Recreate tenants and users.
3. Add the physical assets.
4. Add or modify the virtual assets as required. Be sure to configure virtual arrays and virtual pools exactly as before.
5. For storage resources that support ingestion, ingest them into the ViPR Controller configuration.
   Refer to *ViPR Controller Ingest Services for Existing Environments* , which is available from the ViPR Controller Product Documentation Index .
6. For resources without ingestion support, provision volumes and file systems as necessary.
7. If resources were deleted or modified since the backup, perform those same operations again.

CHAPTER 4

ViPR Controller Recovery with VMware SRM

ViPR Controller recovery with VMware SRM

It is possible to configure VMware SRM to recover the ViPR Controller in the event of datacenter disaster.

How you configure VMware SRM to recover the ViPR Controller on a recovery site depends on how your have installed ViPR Controller. The following sections provide the ViPR Controller-specific steps to configure VMware SRM for ViPR Controller protection. However, you should be sure to use VMware documentation when planning, and deploying your disaster recovery environment.

- Configuring VMware SRM to restore ViPR Controller with vApp on page 20
- Configuring VMware SRM to restore ViPR Controller without vApp on page 23

Configuring VMware SRM to recover ViPR Controller with vApp

The following sections provide the ViPR Controller-specific steps to configure VMware SRM to recover ViPR Controller with a vApp. However, you should be sure to use VMware documentation when planning, and deploying your VMware SRM recovery site.

Before you begin

- This procedure assumes that SRM and a replication of a choice (vSphere Replication or Array-based replication such as RecoverPoint SRA or SRDF SRA), are installed and running in the VMware environment.
- The following example uses vSphere replication. For steps for array-based replication, refer to the VM specific-steps below as an example only, and refer to the array-specific SRA documentation to configure your ViPR Controller protection.
- For vSphere replication ViPR Controller can be installed on any supported datastore. For array-based replication , deploy ViPR Controller on the datastore(s) configured for array-based replication as per SRA requirements.

Procedure

1. Configure ViPR Controller vApp for Recovery as follows:
    a. Configure vSphere replication, or RP SRA, or SRDF SRA, as per VMware requirements.
    b. Configure mappings in SRM: Resource mappings, Folder Mappings, Network Mappings, Placeholder datastores.
    c. Deploy ViPR Controller.
    d. Deploy vApp on recovery site, with IPs for recovered ViPR Controller.

    You can use the same, or new IP addresses.

    e. On recovery site: Delete all VMs from vApp, leave vApp folder intact.
    f. In VMware SRM resource mappings, map the vApp folder of the protected site to the ViPR Controller vApp folder created in the previous step on the recovery site (this way the ViPR Controller VMs will be recovered to the correct vApp folder).
    g. On the protected site: right click on each ViPR Controller node and Configure for vSphere Replication (enable disk1-3 disks for replication in each node).
2. Configure ViPR Controller for VMware SRM failover, in VMware SRM as follows:
    a. Create a protection group which includes all ViPR Controller nodes.

This puts you in the Protection Groups view and the Protection Group Status will show fo reach VM:

```
Device not Found CD/DVD drive 1
```

b. While in Protection Group view, right click on each ViPR Controller node and select "Configure Protection."

c. Click on the CD/DVD drive 1 and "Detach" the CD/DVD device , and then click Save and OK.

The Protection Status will change to OK.

d. Proceed to create the Recovery Plan and select the protection group (created in step 2a), and select the desired Recovery Network for production failover , and "Auto" for Test Network.

The Recovery Network should match network settings you have used when deploying a placeholder vApp on recovery sites in previous steps.

e. Under created Recovery Plan, right click-› Configure each VM and set following options:

Shutdown Action: Shutdown guest OS, and add a reasonable timeout period (5 minutes for example).

Startup Action: "Do not power on."

3. On Recovery site, configure the following options for each VM to match production VMs, and to ensure successful startup when a failover is performed:

a. Using vSphere select Edit Settings and navigate to Options.

b. Under vApp options, select Enable.

c. Under OVF settings, check ON in the ISO image box and VMware Tools box.

d. Under Advanced option, click Properties and create a new property with following values:

- Enter a Label , optionally name it Node ID.
- Leave the Class ID empty.
- Enter "node_id" for the ID. The name "node_id" is required for the id name, and cannot be modified.
- Leave the Instance ID empty.
- Optionally enter a Description of the ViPR Controller node.
- Type: string.
- Enter the Default value, which must be the node id set by ViPR Controller during deployment for example, vipr1, for the first ViPR Controller node, vipr2 for the second ViPR Controller node.
  ViPR Controller values for a 3 node deployment are vipr1, vipr2, vipr3, and for a 5 node deployment are vipr1, vipr2, vipr3, vipr4, and vipr5.
- Uncheck User Configurable.

4. Test your recovery plan, in Test Recovery to verify successful configuration.
5. Upon successful test, perform cleanup.
6. Perform VMware SRM recovery to make ViPR Controller available for production on page 22

Perform VMware SRM recovery to make ViPR Controller with vApp available for production

Warning: this will shut down the currently protected ViPR Controller (if it is still running), so plan accordingly.

Before you begin

If performing VMware SRM recovery on a ViPR Controller instance with a vApp, you must have completed all the steps described in: Configuring VMware SRM to recover ViPR Controller with vApp on page 20.

Procedure

1. Using the **Recovery Plan** defined while configuring VMware SRM to recover the ViPR Controller instance, perform the **Recovery** step in SRM and wait for the recovery plan steps to complete successfully.
2. While ViPR Controller VMs are in powered off state on recovery site, for each VM:
   a. Under **Edit Settings** › **Hardware**, add a CD/DVD drive as a client device.
   b. Using vSphere ensure that the following options are set under **Edit Settings** › **Options**.
      - vApp options are enabled.
      - Under the OVF settings , the ISO image box and VMware Tools box are set to ON
      - Under Advanced option, click Properties and verify the new Node ID property was created with the following values:
        - With the Class ID empty.
        - The name "node_id" is required for the id name, and cannot be modified.
        - With the Instance ID empty.
        - Type: string.
        - The Default value, which must be the node id set by ViPR Controller during deployment for example, vipr1, for the first ViPR Controller node, vipr2 for the second ViPR Controller node.
          ViPR Controller values for a 3 node deployment are vipr1, vipr2, vipr3, and for a 5 node deployment are vipr1, vipr2, vipr3, vipr4, and vipr5.
        - User Configurable must be unchecked.

      Note

      Due to above OVF settings, the .iso image will be mounted to the CD/DVD drive automatically, as expected.

   c. Power on ViPR Controller vApp.

After you finish

After performing SRM recovery, wait a few minutes for VMs to start for ViPR Controller services to initialize. At this point, ViPR Controller should be up and running on recovery site. Login to ViPR Controller UI, and make any of the necessary changes described below:

- NTP server, and DNS servers if they should be different based on the new ViPR Controller location.

- ViPR Controller Keystore (in case a CA signed certificate was used in original ViPR Controller.

Note

If self signed certificate was used in original ViPR Controller, then a new self signed certificate will autocratically be generated in the restored ViPR Controller so no action is needed.

- After successful ViPR Controller recovery, perform Reprotect step in Recovery Plan, to protect current ViPR Controller instance.

Configuring VMware SRM to restore ViPR Controller without vApp

The following sections provide the ViPR Controller-specific steps to configure VMware SRM to restore ViPR Controller without a vApp. However, you should be sure to use VMware documentation when planning, and deploying your VMware SRM recovery site.

Before you begin

- This procedure assumes that SRM and a replication of a choice (vSphere Replication or Array-based replication such as RecoverPoint SRA or SRDF SRA), are installed and running in the VMware environment.
- The following example uses vSphere replication. For steps for array-based replication, refer to the VM specific-steps below as an example only, and refer to the array-specific SRM documentation to configure your ViPR Controller protection.
- For vSphere replication ViPR Controller can be installed on any supported datastore. For array-based replication , deploy ViPR Controller on the datastore(s) configured for array-based replication as per SRA requirements.

Procedure

1. Configure ViPR Controller nodes for recovery.
    a. Configure each ViPR Controller node for replication (include all 4 disks) and wait for initial full sync to complete.
    b. Create all desired Site Mappings: Make sure to map to desired recovery site resources, network, folder, placeholder datastores.
    c. Create a protection group and include all ViPR Controller nodes.
    d. Proceed to create the Recovery Plan. Select Protection Group (created in Step 1c), and select desired Recovery Network for production failover , and "Auto" for Test Network.

       The Recovery Network should match network settings you have used when deploying a placeholder vApp on recovery sites in previous steps.
    e. In the Recovery Plan,

       if ViPR Controller on Recovery Site should have different IP settings from Protected Site configure each VM with following settings:
       - IP Settings: Make sure "Customize IP settings during recovery" is unchecked.
       - Shutdown Action: select"Power Off"
       - Startup Action: select "Do not power on".

Note

After recovery, before ViPR Controller nodes can be successfully powered on with desired IP addresses, you will need to change the IP address of the ViPR Controller node as described in the *ViPR Controller Installation, Upgrade, and Maintenance Guide* which is available from the ViPR Controller Product Documentation Index .

If ViPR on Recovery Site should have same IP settings as on Protected Site:

- IP Settings: Make sure "Customize IP settings during recovery" is unchecked.
- Shutdown Action: select "Power off."
- Startup Action: select "Power on" , make sure "Wait for Vmware tools" is unchecked.

2. Test your recovery plan, in Test Recovery to verify successful configuration.
3. Upon successful test, perform cleanup.
4. Perform VMware SRM recovery to make ViPR Controller without vApp available for production on page 24.

Perform VMware SRM recovery to make ViPR Controller without vApp available for production

Warning: this will shut down the currently protected ViPR Controller (if it is still running), so plan accordingly.

Before you begin

If performing VMware SRM recovery on a ViPR Controller instance without a vApp, you must have completed all the steps described in: Configuring VMware SRM to restore ViPR Controller without vApp on page 23.

Procedure

1. Using the **Recovery Plan** defined while configuring VMware SRM to restore the ViPR Controller instance, perform the **Recovery** step in SRM and wait for the recovery plan steps to complete successfully.
2. Optionally, perform the following post recovery steps after successful recovery, if ViPR Controller should have different IPs on the recovery site.

   Note

   This step is required for every failover, even if the failover is performed to the original site.

   a. Change the IP address of ViPR Controller node on VMware with no vApp using vCenter, which is described in the *ViPR Controller Installation and Configuration Roadmap* which is available from the ViPR Controller Product Documentation Index .

After you finish

After performing SRM recovery, wait a few minutes for VMs to start for ViPR Controller services to initialize. At this point, ViPR Controller should be up and running on recovery site. Login to ViPR Controller UI, and make any of the necessary changes described below:

- NTP server, and DNS servers if they should be different based on the new ViPR Controller location.
- ViPR Controller Keystore (in case a CA signed certificate was used in original ViPR Controller.

Note

If self signed certificate was used in original ViPR Controller, then a new self signed certificate will autocratically be generated in the restored ViPR Controller so no action is needed.

- After successful ViPR Controller recovery, perform Reprotect step in Recovery Plan, to protect current ViPR Controller instance.

APPENDIX A

Restoring a Virtual Data Center in a Geo Federated (Multi-site) Environment

Restoring a virtual data center in a geo federated (multisite) environment

Both ViPR Controller minority node recovery, and native backup and restore can be used to restore your ViPR Controller instance in a geo federated (multisite) environment.

To determine which type of restore is appropriate for your environment see Options for restoring ViPR Controller on page 5.

Minority node recovery for VDC in geo federated environment

In this case simply follow the procedure for minority node recovery as described in Minority node recovery for node failure on page 8.

Pre-requisites for native backup and restore of VDC in a geo federated environment

The following requirements must be met to restore in a geo federated (multisite) envrionment, in addition to the target system requirements described in Restoring from a backup on page 16:

- If there are any version 2.0 or 2.1 VDCs in the federation, contact customer support and refer to KB article 000189026.
- In a geo federated environment, you cannot use the native backup and recovery operations to migrate ViPR Controller from a 3 node installation to a 5 node installation, or from a 5 node installation to a 3 node installation. Also, you cannot use native restore to relocate ViPR Controller instance because you must use the same IP addresses when restoring from a backup.
- Do not use a backup which was created on a single VDC to restore, after the VDC has been added to a multi-VDC configuration, and vice versa.

Native backup and restore when there are three VDCs and one VDC is lost

1. If the VDC that you are restoring is part of a geo federated (multisite) configuration, and one or more VDCs are still running, login to the VDC that is running, and disconnect the VDC that has been lost.
   a. Log in to the ViPR Controller UI for the VDC that is running.
   b. Go to the **Virtual Assets** › **Virtual Data Centers** page.
   c. Select the lost VDC, and click **Disconnect**.

   For further details about disconnecting or reconnecting a VDC see the *ViPR Controller User Interface Tenants, Projects, Security, Users and Multisite Configuration Guide* which is available from the ViPR Controller Product Documentation Index .
2. Restore the ViPR Controller instance using the steps described in Restoring from a backup on page 16.
3. Log into the VDC that was still running in Step 1, and reconnect to the restored VDC.
   a. From the ViPR Controller UI, for the VDC that was not lost, go to the **Virtual Assets** › **Virtual Data Centers** page.
   b. Select the restored VDC, and click **Reconnect**.

For specific steps to disconnect and reconnect VDCs, see the *ViPR Controller User Interface Tenants, Projects, Security, Users and Multisite Configuration Guide*, which is available from the ViPR Controller Product Documentation Index .

Native backup and restore when there are 2 VDCs and both are lost

WARNING: When all VDCs are lost in a geo federated environment, you must restore the original virtual data center first, and then you can continue to restore the virtual data centers that where created after the original virtual data center was created.

Review the prerequisites above before continuing.

1. Download most recent backup files for both VDC1 and VDC2.
2. Shutdown VDC1 and VDC2 (if VMs are still running).
3. Redeploy VDC1 and restore VDC1 using steps described in xref: Restoring from a backup on page 16.
   When VDC1 is successfully restored it will be restored with connectivity to VDC2.
4. From VDC1, disconnect VDC2.
   a. Log in to the ViPR Controller UI for VDC1.
   b. Go to the **Virtual Assets** › **Virtual Data Centers** page.
   c. Select VDC2, and click **Disconnect**.

   For further details about disconnecting or reconnecting a VDC see the *ViPR Controller User Interface Tenants, Projects, Security, Users and Multisite Configuration Guide*which is available from the ViPR Controller Product Documentation Index .
5. Repeat steps 3 and 4 for VDC2.
6. After restore of VDC2 is complete, open the ViPR Controller UI for VDC1 and reconnect VDC2 from VDC1.
   a. From the ViPR Controller UI, for VDC1, go to the **Virtual Assets** › **Virtual Data Centers** page.
   b. Select VDC2, and click **Reconnect**.