Dell EMC ViPR Controller

Version 3.6.2

System Disaster Recovery, Backup, and Restore Guide

302-004-912

DELL EMC

Published June 2018

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

CONTENTS

TABLES

CHAPTER 1

System Disaster Recovery, Backup and Restore Options for ViPR Controller

System Disaster Recovery, backup and 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 for Disaster Recovery, backup and restore of ViPR Controller

Restore options	When to use:	Is ViPR Controller available during recovery?	Supported environment
System Disaster Recovery	Interim or permanent ViPR Controller (or entire Datacenter) Disaster The IT infrastructure managed by ViPR Controller spreads across multiple data centers. Multiple ViPR instances could be deployed in different data centers in order to tolerate center-wide data failures. ViPR System Disaster Recovery uses the Active/Standby model, which means that only one Active ViPR instance serves for provisioning operations while the other ViPR instances are configured as Standby sites. Failover and Switchover operations are supported to cope with disasters **Note** Use either System Disaster Recovery or Backup and Restore for ViPR vApp migration to a new ESX cluster or vCenter. Depending on your configuration, you can either configure a secondary ViPR controller site at the new location and promote it to primary after completion of the synchronization, or you can restore the latest backup of the site to the new location.	Not available	• VMware with vApp • VMware without vApp • Hyper-V Not supported in Muli-site (GEO) environment.

Table 1 Options for Disaster Recovery, backup and restore of ViPR Controller (continued)

Restore options	When to use:	Is ViPR Controller available during recovery?	Supported environment
Node Recovery on page 32	• Recovery on vApp is possible only when all nodes are available (just services corrupted), and doesn't work for whole-node-corrupted scenarios. • 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. • Node recovery can only be performed through the ViPR Controller UI.	Yes, available, but do not run any operations while recovery is ongoing.	VMware No-vApp and Hyper-V environments and for vApp environments with a single site.
ViPR Controller Minority node recovery from node failure	ViPR Controller is still in production (a quorum number of nodes are up and running), and: • One VM is permanently lost when ViPR Controller is deployed on three VMs. • Up to two VMs permanently lost when ViPR Controller is deployed on five VMs. • CLI commands are available to support minority node recovery.	Yes, available	An Active ViPR Controller instance in a System Disaster Recovery environment. Single, or Multi-VDC, and installed on • VMwre without vApp • Hyper-V Not supported for a Standby ViPR Controller instance in a System Disaster Recovery environment. Not supported when installed with a vApp.
ViPR Controller native backup and restore service	If the ViPR controller System Disaster Recovery option is not configured or available, and: • More than half of nodes are permanently lost.	Not available	Single, or Multi-VDC, and installed on • VMware with vApp • VMware without vApp • Hyper-V

Table 1 Options for Disaster Recovery, backup and restore of ViPR Controller (continued)

Restore options	When to use:	Is ViPR Controller available during recovery?	Supported environment
	• Any number of nodes are permanently lost when installed with a vApp. **Note** Use either System Disaster Recovery or Backup and Restore for ViPR vApp migration to a new ESX cluster or vCenter. Depending on your configuration, you can either configure a secondary ViPR controller site at the new location and promote it to primary after completion of the synchronization, or you can restore the latest backup of the site to the new location.		Not supported for a Standby ViPR Controller instance in a System Disaster Recovery environment.
	Backup and restore can also be used to reconfigure the ViPR Controller virtual data center as follows: • Migrate ViPR Controller from a three-node installation to a five-node installation, or from a five-node installation to a three-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 Not supported for a Standby ViPR Controller instance in a System Disaster Recovery environment.
	• Change the ViPR Controller instance with vApp to a an instance without a vApp. • Change the ViPR Controller instance without vApp to a an instance with a vApp.		Single VDC only, installed on VMware Not supported for a Standby ViPR Controller instance in a System Disaster Recovery environment.
VMware Site Recovery Manager (SRM)	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

Table 1 Options for Disaster Recovery, backup and restore of ViPR Controller (continued)

Restore options	When to use:	Is ViPR Controller available during recovery?	Supported environment
Note This method will be deprecated in favor of ViPR System Disaster Recovery in a future release.			• VMware without vApp Not supported for a Standby ViPR Controller instance in a System Disaster Recovery environment.

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

System Disaster Recovery

Use the ViPR Controller System Disaster Recovery solution to help ensure business continuity of applications in case of site disasters.

System Disaster Recovery overview

In enterprise data centers, isolated hardware or software failures occur, as well as massive failures caused by power outages, earthquakes, tornados, and other storms. Preserving the continuous availability of a business application or service in the presence of these failures has become extremely important.

Note

Please contact your EMC Customer Support Representative for assistance in planning of the end-to-end System Disaster Recovery configuration for use cases based on your datacenter physical assets and environment.

A common approach to allowing an enterprise application to "stay alive" involves:

- Transparent fault tolerance within a single data center - basically, "high-availability" (HA) systems with redundant hardware, redundant data storage, and redundant networking and power sources.
- Explicit (and not always transparent) "disaster recovery" (DR) configurations, allowing business applications to "failover" to a separate setup in a different (presumably geographically distant) data center. Typically, these solutions involve a separate copy of the application in the remote location and explicit replication of the application data to the remote setup.

For many enterprises, both HA and DR are must-have requirements for any essential business applications. ViPR Controller allows business applications to remain available in case of a minor, isolated failure (HA), and also in the event of a massive failure (DR), which may involve migration of the application and/or ViPR Controller setup to a different data center.

With its existing Active-Active multi-node cluster and a transparent fail over of its public VIP address, ViPR Controller provides strong HA capabilities. It can reliably tolerate a single node failure in 2+1 deployments, and up to two node failures in 3+2 deployments. Also, it allows the recovery (redeployment) of nodes if the underlying hardware failed permanently or suffered data loss.

The ViPR Controller provisioning model fits well into application HA and DR by automating protected volume provisioning. In addition, it has GEO functionality and an implemented "backup."

Adding, editing, and deleting System Disaster Recovery sites

System Disaster Recovery is accomplished between an Active site and one or more Standby sites. Standby sites can be added, edited (Active sites as well), or deleted from the **System** > **System Disaster Recovery** page.

Note

In order to implement System Disaster Recovery, the ViPR Controller Firewall must be enabled, which it is by default. To verify that the Firewall is enabled, go to the **Security** tab of the **System** > **General Configuration** page.

Note

For System Disaster Recovery configurations, verify that ports 7000 and 7100 are not blocked by a firewall between the datacenters, in order to allow for IPsec communication between the ViPR Controllers at each site. For more information on ViPR Controller port usage, see the EMC ViPR Controller Security Configuration Guide, which is available from the ViPR Controller Product Documentation Index.

Adding a Standby Site

Standby sites can be added from the **System** > **System Disaster Recovery > Add Standby** page.

Before you begin:

- At the present time, the system supports up to two Standby sites.
- A new Standby site to be added must be a freshly-installed and powered-on ViPR Controller.
  - It can be any supported ViPR Controller installation (2+1, 3+2, no vApp or HyperV).
  - Do not perform an initial GUI configuration.
  - Do not specify NTP/DNS, email, etc. settings on the Standby site - they are set only on the Active site and shared by all sites.
  - The correct state of the new Standby site is such that when you log into the GUI, you should see the Add License page.
- Only one Disaster Recovery operation can be done at a time. For example, if an Add Standby operation is still in progress, you cannot add another Standby until the first operation is completed.

To add a Standby site, do the following:

1. Go to the **Add Standby** page.
2. Enter information for the fields as described in the following table.
3. Click **Save** to add a new Standby site. Click **Cancel** to quit the **Add Standby** page.
4. The following table provides details on the information required to add a Standby site.

Table 2 Add Standby

Field Name	Description
Site Name	The name of the Standby site. For example, "US - West".
Description	An optional description for the Standby site. For example, "Original Standby Site".
Site Virtual IP or FQDN	The VIP (or Fully Qualified Domain Name) of the Standby site. For example, `10.247.100.243`
User Name	The default Login User Name for the Standby site (root).
Password	The Login Password for the Standby site. The default ViPR Controller password (ChangeMe) is required in this field, since the Standby site has not yet had an initial GUI configuration. After the Standby site has been added, its password will be changed to the password of the Active site.

Table 2 Add Standby (continued)

Field Name	Description
Confirm Password	Confirm the Login Password.

Editing an Active or Standby Site

Existing Standby or Active sites can be edited from the **System** > **System Disaster Recovery > Edit Site** page.

To edit a Standby or Active site, do the following:

1. From the **System Disaster Recovery** page, select a **Site Name** to open the **Edit Site** page for that site.
2. Enter information for the fields as described in the following table.
3. Click **Save** to edit the information for the site or click **Cancel** to quit the **Edit Site** page.
   After you click **Save**, the Standby site will be reconfigured to establish a System Disaster Recovery relationship with the Active site, followed by an initial data synchronization from Active site to Standby site.
4. The following table provides details on the information required to edit a site.

Table 3 Edit Site

Field Name	Description
Site Name	The name of the Active or Standby site. For example, "US - West".
Description	An optional description for the site. For example, "Original Standby Site".

Deleting a Standby Site

Existing Standby sites can be deleted from the **System** > **System Disaster Recovery** page.

Before you begin:

- All ViPR Controller instances share the same set of security keys. To minimize potential security risks of a deleted Standby site, the Standby site should be powered-off and deleted from disk before starting the delete Standby operation in ViPR.

To delete a Standby site, do the following:

1. From the **System Disaster Recovery** page, click the checkbox to the left of the **Site Name** to select the Standby site. Multiple Standby sites can be deleted at the same time.
2. Click **Delete** to delete the Standby site(s). After a Standby site has been deleted, it cannot be added to System Disaster Recovery again until it is freshly-installed and powered-on.

Note

If the Standby site was up and running and in a good state at deletion time, it will attempt to shut down automatically. If it was in a bad state or not accessible, you should manually power off and delete the Standby site, since it cannot be reused .

Monitoring System Disaster Recovery status and operations

System Disaster Recovery status is displayed on the **Dashboards** > **Overview** page, and Disaster Recovery status and operations are managed from the **System** > **System Disaster Recovery** page.

Note

In order to implement System Disaster Recovery, the ViPR Controller Firewall must be enabled, which it is by default. To verify that the Firewall is enabled, go to the **Security** tab of the **System** > **General Configuration** page.

Dashboards > Overview: System Disaster Recovery

The **Dashboards** > **Overview** page provides summary Status and Network Health information for the Active and Standby Disaster Recovery sites.

Table 4 System Disaster Recovery Status and Health

Column Name	Description
Site Name	The Site Name is specified when the site is initially added.
Status	The current status of the Active and Standby sites. For detailed information on site Status, refer to the next section.
Network Health	The health of the network, as indicated by the Latency in milliseconds. A Latency of <150 ms between ViPR Controller Disaster Recovery sites is supported: • **Good**: <150 ms • **Slow**: >150ms • **Broken**: There is no network connection to the site.

System > System Disaster Recovery

Standby sites can be added, edited, or deleted, and disaster recovery operations managed from the **System** > **System Disaster Recovery** page.

- Click **Add** to add a new Standby site.
- Select a **Site Name** to edit the site information for an Active or Standby site, including **Site Name** and **Description**.
- To delete a Standby site, click the checkbox to the left of the **Site Name** and click **Delete**.

The following table provides details on the information displayed on the **System Disaster Recovery** page and the actions that can be performed during the Disaster Recovery process.

Click anywhere on the site row to display the site status, including **Site UUID**, **Controller Status**, **Site Creation Time**, **Latency**, and **Synchronization Status**.

Table 5 System Disaster Recovery

Column Name	Description
Selection column (checkbox)	Click the checkbox to select the site and display the site status. This also enables you to delete the site.
Site Name	The Site Name is specified when the site is initially added. It can be changed later on by editing the site. For example "US-West".
Description	An optional description of the site. This description can be created when the site is initially added, or later on by editing the site. For example, "Original Standby Site".
Site Virtual IP or FQDN	The VIP (or Fully Qualified Domain Name) of the Active site and the Standby site(s). For example, `10.247.100.243`
Status	The current status of the Active and Standby sites: • **Active** (with green checkmark): The Active site, with data synchronization up-to-date. • **Active** (with yellow exclamation point): The Active site is temporarily unreachable from the Standby site and its current state is not determined. This status would be seen on the Standby site GUI. • **Active Degraded**: The Active site has been replaced by the Standby site during a **Failover** action and synchronization has not been resumed. You can delete the site if it fails permanently, or **Resume** the Active Degraded site as a Standby site after it is back online. • **Standby** (with green checkmark): The Standby site(s), with data synchronization up-to-date. A **Switchover** action may be initiated from the Active site. • **Standby** (with yellow triangle): The Standby site is unreachable, with data synchronization not up-to-date. • **Degrading Standby**: The Standby site is being excluded from data synchronization due to a lost connection for more than15 minutes. • **Standby Degraded**: Data synchronization is not working normally due to a problem at the Standby site or an unreachable network. Check the network and fix the network problem. After that, ViPR will automatically change the site state back to Standby. **Note** ViPR Controller can notify the root user by email if a Standby site becomes unreachable or if synchronization to a Standby site is unexpectedly interrupted (the Standby is placed in **Standby Degraded** mode). This allows you to take appropriate action to resolve the issue in a timely manner. • **Resuming Standby**: Data synchronization to the Standby site is being resumed. This will occur when

Table 5 System Disaster Recovery (continued)

Column Name	Description
	manually resuming a Standby site after upgrading to a new version of ViPR Controller. • **Syncing Standby**: A full data synchronization is in progress between the Active and Standby sites. • **Pausing Standby**: Data synchronization to the Standby site is being paused. This will occur when manually pausing a site prior to upgrading to a new version of ViPR Controller. • **Standby Paused**: The Standby site, with data synchronization from the Active site interrupted or lost, will mark itself as Paused in a short period of time. Or, a site was Paused manually as a prerequisite before Upgrade. A **Failover** action may be initiated from the Standby site. This may also occur when upgrading to a new version of ViPR Controller. • **Removing Standby**: The Standby site is in the process of being removed. After the Standby site is removed from the sites list, it is shut down. • **Standby Error**: A timeout occurred during a disaster recovery operation. When this occurs, you may be able to retry the operation if an option is given in the GUI for that operation. Otherwise, you must delete the site, redeploy it, and re-add it as a new site.
Network Health	The health of the network, as indicated by the Latency in milliseconds. A Latency of <=150 ms between ViPR Controller Disaster Recovery sites is supported: • **Good**: <=150 ms • **Slow**: >150ms • **Broken**: There is no network connection to the site.
Actions	Depending on the Status of the Active and Standby sites, the following actions may be initiated: • **Switchover**: Changes the selected Standby site to the Active site, and the Active site to a Standby site. A **Switchover** is allowed only when the Disaster Recovery status of the selected Standby site is **Standby** and the ViPR Controller status of all sites is "Stable" (refer to the **Dashboards** > **Overview** page. There are warnings when the Active site cannot synchronize to the Standby site. • **Failover**: Changes the Standby site that you are currently logged into to the Active site. Failover is allowed only when the Active site is not reachable or powered off for at least 5 minutes. Synchronization

Table 5 System Disaster Recovery (continued)

Column Name	Description
	Status shows the last data synchronization time with the Active site. There are warnings when the Active site cannot synchronize to the Standby site. **Note** If you want to bring the original Active site back, verify that the Network Health between the new Active site and the original Active site is Good. If that is the case, then the original Active site status will automatically be changed to Active Degraded. Otherwise, a scenario may occur in which there are multiple Active sites. If such a scenario does occur, shut down the original Active site, redeploy the vApp for that site, and add the site back as a Standby site. • **Resume**: Re-establishes data synchronization with the Active site. Resume can also be done on a site which was manually paused (while upgrading ViPR Controller). A manual pause is only used during upgrading, and can only be accessed through the Upgrade page.

Perform a site Failover

If the Active site is in a disaster situation (not available), a site **Failover** changes the Standby site that you are currently logged into to the Active site.

Before you begin

- A **Failover** is allowed only when the Active site is not reachable or powered off for at least 5 minutes.

  Note

  The System Administrator must ensure that the Active site ViPR Controller does not serve any new provisioning operations before initiating Failover.

- The synchronization Status shows the last data synchronization time with the Active site.

  Note

  If there are multiple Standby sites, the System Administrator should check the "last data synchronization time" on each Standby site, and use the Standby site with the most recent time, in order to minimize possible data loss.

- There are warnings when the Active site cannot synchronize to the Standby site.
- For in-progress orders and array discoveries that were in progress during the Active site disaster:
  - In-progress orders will be marked as Failed. They need to be cleaned up and retried after Failover.

- In-progress array discoveries will be marked as Failed. They will be re-initiated based on normal scheduling after Failover.

To perform a site **Failover**, do the following:

Procedure

1. Go to the **System** > **System Disaster Recovery** page for the Standby site.
2. Verify that the network health of the original Active site is broken (not reachable or powered off), before you do a failover on a Standby site.
3. For the Standby site that you want to failover into the Active site, click **Failover** in the **Actions** column.
4. Wait for the failover to complete. Then, redirect all your provisioning requests to the new Active site ViPR Controller.
5. If you want to bring the original Active site back, verify that the Network Health between the new Active site and the original Active site is Good. If that is the case, then the original Active site status will automatically be changed to Active Degraded.
    a. If the original Active site (now Active Degraded) does come back online, it can be resumed from the new Active site, and will automatically become a Standby site of the new Active site.
    b. Resume any other Standby sites (if applicable).
    c. If the Active Degraded site is a total loss and cannot be resumed from the new Active site as a Standby site, delete the site, redeploy the vApp for that site, and add the site back as a Standby site.

Perform a site Switchover

A **Switchover** changes the selected Standby site to the Active site, and the Active site to a Standby site.

Before you begin

Note

A Switchover is a planned action which requires all sites to be available, and is meant for non-disaster situations.

- A **Switchover** is allowed only when the status of the selected Standby site is **Standby** and the ViPR Controller status of all sites is "Stable" (refer to the **Dashboards** > **Overview** page.
- There are warnings when the Active site cannot synchronize to the Standby site.

The are two common use cases for Switchover:

1. A planned outage on the Active site. The System Administrator can switch Active site to another data center to avoid disruptions caused by the outage.
2. Recovery assurance testing. The System Administrator can periodically select a maintenance time window to verify if the Standby site is "good enough" for a real disaster. Such assurance testing can also help in gaining confidence in the System Disaster Recovery solution. To achieve this, the System Administrator can switch the Active site to a Standby site, run a provisioning test, then switch back.

To perform a site **Switchover**, do the following:

Procedure

1. Go to the **System** > **System Disaster Recovery** page for the Active site.
2. For the Standby site that you want to switch over to the Active site, click **Switchover** in the **Actions** column.
3. Wait for the **Switchover** to complete. Then, redirect all your provisioning requests to the new Active site ViPR Controller.

Upgrade ViPR Controller in a System Disaster Recovery environment

Before performing a ViPR Controller software upgrade, you should pause at least one Standby site, to which the system can Failover if the upgrade fails. Standby sites can be paused from the **System** > **Upgrade** > **Software Upgrade** page by clicking **Pause Sites**.

Before you begin

- A manual pause is only used during upgrading, and can only be accessed through the Pause Disaster Recovery Sites page.
- When pausing a site, note the following pre-conditions:
  - The Standby site must be Synced.
  - All sites (Active and Standby) should have a ViPR Controller Status of "STABLE".
  - No other Disaster Recovery operation can be in progress.
  - There should be no DR site in ERROR state.
- When pausing a site, note the following considerations:
  - Pausing a Standby site keeps it in the current version during a software upgrade.
  - Any Standby sites that are not paused will automatically be upgraded along with the Active site.
  - If the upgrade fails on the Active site, all the Standby sites that are not paused in advance may become unstable and must be removed.
  - Any one of the paused Standby sites may be used as a Failover target if the upgrade fails on the Active site, and the issue cannot be resolved by other means:
    - If there was another manually paused Standby site, it can be resumed.
    - All ViPR Controller instances share the same set of security keys. To minimize potential security risks of a deleted Standby site, the Standby site should be powered-off and deleted from disk before starting the delete Standby operation in ViPR.
    - Shut down the old Active site, delete it in Vcenter, and delete it from the ViPR Controller GUI. Redeploy the site and re-add it as a new Standby site to reestablish the Disaster Recovery configuration.
    - If another Standby site was NOT manually paused, shut down the site, delete it from the vCenter, and also delete it from the ViPR Controller UI. Redeploy the site and re-add it as a new Standby site
  - Any one of the paused Standby sites may be Resumed after the upgrade completes successfully. Resuming these sites will result in an automatic

upgrade of the sites being resumed to the same ViPR Controller version as the Active site.

- When resuming a site, note the following pre-conditions:
  - Any other Standby site should have a ViPR Controller Status of "STABLE", or be in a Paused state. If a site is in Active Degraded state, the resume is also allowed.
  - No other Disaster Recovery operation can be in progress.
  - No Disaster Recovery site can be in an ERROR state.

To pause and resume a Standby site, do the following:

Note

The **Pause Sites** option will appear only if there is a new ViPR Controller version available for download from the EMC remote repository, or if a new upgrade image has already be downloaded to ViPR Controller and the system is ready to be upgraded.

Procedure

1. Go to the **System** > **Upgrade** > **Software Upgrade** page, to start the upgrade process. Follow the preliminary steps for the upgrade.
2. Click **Pause Sites** to go to the **Pause Disaster Recovery Sites** page.
3. Click **Pause** to pause one or more Standby sites. The following table provides details on the information required to pause a Standby site.

   After you click **Pause**:

   - The Cluster State reporting for System Disaster Recovery sites view will show "UNKNOWN." This is expected behavior.
   - Changing any system properties (node name, banner, keystore) for the Standby will not be allowed.
4. Click **Install** next to the version you would like to install.
5. After the installation is complete, go to the **System** > **System Disaster Recovery** page to perform a **Resume** action for the Paused Standby site(s). A Standby **Resume** re-establishes data synchronization with the Active site.

Table 6 Pause Disaster Recovery Sites

Column Name	Description
Selection column (checkbox)	Click the checkbox to select the site and display the site status.
Site Name	The Site Name is specified when the site is initially added.
Description	An optional description of the site.
Site Virtual IP or FQDN	The VIP (or Fully Qualified Domain Name) of the Active site and the Standby site(s).
Status	The current status of the Active and Standby sites: • **Active** (with green checkmark): The Active site, with data synchronization up-to-date.

Table 6 Pause Disaster Recovery Sites (continued)

Column Name	Description
	• **Standby** (with green checkmark): The Standby site(s), with data synchronization up-to-date. A **Pause** action may be initiated for the Standby site. • **Pausing Standby**: Data synchronization to the Standby site is being paused. This will occur when manually pausing a site prior to upgrading to a new version of ViPR Controller. • **Standby Paused**: The Standby site, with data synchronization from the Active site interrupted or lost, will mark itself as Paused in a short period of time. Or, a site was Paused manually as a prerequisite before Upgrade. • **Standby Error**: A timeout occurred during a disaster recovery operation. When this occurs, you may be able to retry the operation if an option is given in the GUI for that operation. Otherwise, you must delete the site, redeploy it, and re-add it as a new site. **Note** For a complete list of system states and actions, refer to Monitoring System Disaster Recovery Status and Operations.
Network Health	The health of the network, as indicated by the Latency in milliseconds. A Latency of <=150 ms between ViPR Controller Disaster Recovery sites is supported: • **Good**: <=150 ms • **Slow**: >150ms • **Broken**: There is no network connection to the site.
Actions	Depending on the Status of the Active and Standby sites, the following action may be initiated: • **Pause**: Pauses the Standby site, to which the system can Failover if the upgrade fails. A manual pause is only used during upgrading, and can only be accessed through the Pause Disaster Recovery Sites page. **Note** More than one Standby site may be Paused. But if one site is selected and Pause is initiated, you must wait for the current Pause to complete before proceeding with the next site's Pause.

System Disaster Recovery Email Alerts

ViPR Controller can notify the root user by email if a Standby site becomes unreachable or if synchronization to a Standby site is unexpectedly interrupted (the Standby is placed in **Standby Degraded** mode). This allows you to take appropriate action to resolve the issue in a timely manner.

Configuring ViPR Controller to send out email notifications to root is strongly recommended. You can enable email for the root user and specify a root email address by clicking **root** in the upper-right corner of the ViPR Controller UI, selecting **Preferences**, and then enabling email and specifying a root email address.

System Disaster Recovery provides email alerts for two types of issue:

1. Network issue (the Active site has lost communication with a Standby site)
2. A Standby site has become Degraded, due to a loss of connection with the Active site for ~15 minutes.

Example 1:

From: `"vipr210@vipr.com" <vipr210@vipr.com>`

Date: `Wednesday, February 10, 2016 5:55 PM`

To: `Corporate User <root.user@emc.com>`

Subject: `ATTENTION - standby1-214 network is broken`

Your standby site: standby1-214's network connection to Active site has been broken.

Please note that this could be reported for the following reasons. 1) Network connection between standby site and active site was lost. 2) Standby site is powered off. 3) Network latency is abnormally large and could cause issues with disaster recovery operations.

Thank you, ViPR

Example 2:

From: `"vipr210@vipr.com" <vipr210@vipr.com>`

Date: `Wednesday, February 10, 2016 5:55 PM`

To: `Corporate User <root.user@emc.com>`

Subject: `ATTENTION - standby 10.247.98.73 is degraded`

Your Standby site 10.247.98.73_name has been degraded by Active site at 2016-04-05 10:28:27. This could be caused by following reasons (including but not limited to):1) Network connection between Standby site and Active site was lost.2) Majority of nodes in Standby site instance are down.3) Active or Standby site has experienced an outage or majority of nodes and not all nodes came back online (its controller status is "Degraded").

Please verify network connectivity between Active site and Standby Site(s), and make sure Active and Standby Site's controller status is "STABLE".NOTE: If Active site or Standby site temporarily experienced and outage of majority of nodes, the Standby site can only return to synchronized state with Active when ALL nodes of Active and Standby site(s) are back and their controller status is "STABLE".

Thank you, ViPR

Active site backup

Configure the ViPR Controller Active site for a daily backup.

Configuring your ViPR Controller Active site for a daily backup schedule and uploading backups automatically to an external server is highly recommended, even if ViPR is configured with System Disaster Recovery.

You can configure backups from the **System** > **General Configuration** > **Backup** page. In the event of a Switchover or Failover System Disaster Recovery operation, the backup schedule will automatically continue using the same settings on the new Active site.

System Disaster Recovery Limitations and Best Practices

System Disaster Recovery Limitations

Please note the following System Disaster Recovery Limitations:

- At the present time, the system supports up to two Standby sites.
- IP address change is not supported while a ViPR Controller instance is part of a System Disaster Recovery environment. If IP addresses must be changed, you can:
  - For the Active site, unconfigure System Disaster Recovery by deleting all Standby sites, change the Active site IP address, then redeploy and re-add the Standby sites.
  - Delete a specific Standby site, and redeploy and re-add it with a new IP address.
  - For all Standby sites, delete all Standby sites, change IP addresses in the remaining Active site, then redeploy and re-add the Standby Sites.
- In the System Disaster Recovery environment, the Restore of a backup into a new ViPR Controller instance with different IP addresses or a different number of nodes is not supported. This situation results from the unlikely scenario of a complete loss of the Active site and failure to execute the Failover action at the Standby site. Please contact EMC Support at https://support.emc.com and refer to KB article 000482840 for a workaround.
- System Disaster Recovery and GEO (Multi-Site ViPR Controller) are mutually exclusive and are not supported at the same time. You cannot add System Disaster Recovery in a GEO environment, and cannot add a new VDC to a System Disaster Recovery environment.
- Restore of a backup to the Active site of a system that has System Disaster Recovery sites configured is not supported. Restoring a backup taken in a System Disaster Recovery environment can be done only in a freshly deployed, single VDC, ViPR Controller instance, following the normal Restore procedure. After the Restore, the Standby sites shown in the GUI should be removed , new sites deployed, and the sites re-added to System Disaster Recovery.

Best Practices in Configuring System Disaster Recovery

Following are suggested best practices in configuring ViPR Controller System Disaster Recovery:

Table 7 Best Practices in Configuring System Disaster Recovery

Configuration Item	Recommendation	System Disaster Recovery Notes
Network Infrastructure	The following ports should be enabled for all nodes in remote ViPR Controller nodes: • TCP ports: 443, 2888, 2889, 7000, 7100 • UDP ports: 500, 4500 Ensure that you have quality speed network infrastructure between datacenters. NAT across data centers is not supported. The maximum supported latency between System Disaster Recovery (DR) sites is <= 150ms.	
NTP	• NTP Server settings are shared among Active and all other DR sites in ViPR. • Configure all redundant NTP servers (including the ones for the DR datacenter) in the Active site. Alternatively, NTP server settings can be changed after Failover/Switchover to a DR site. **Note** All NTP servers that are used in ViPR Controller configuration must be synchronized with a reliable time source. • Register redundant NTP servers in the Active site. **Note** You can also change or add NTP settings after Failover on the DR site, if necessary.	
DNS	• DNS Server settings are shared among Active and all other DR sites in ViPR. • Configure all redundant DNS servers (including the ones for the DR datacenter) in the Active Site. Alternatively, DNS server settings can be changed after Failover/Switchover to a DR site. • Register redundant DNS servers in the Active site. **Note** You can also change or add DNS settings after Failover on the DR site, if necessary.	
User Authentication	• Verify that User Authentication works for the Active and Standby site(s), to make sure that there are no firewalls blocking authentication traffic. LDAP users should be able to login to Active and Standby site(s) to avoid any unexpected authentication issues during of Disaster Recovery.	

Table 7 Best Practices in Configuring System Disaster Recovery (continued)

Configuration Item	Recommendation	System Disaster Recovery Notes
Authentication Provider	• Authentication Provider Server settings are shared among Active and all other DR sites in ViPR. • Configure all redundant Authentication Provider URLs (including the ones for the DR datacenter) in the Active Site. Alternatively, Authentication Provider server settings can be changed after Failover/Switchover to a DR site. If the Authentication Provider server configured in the Active site is not available due to a disaster, alternative Authentication Provider server settings can be changed by the root user after a ViPR failover. • For the Authentication Provider server, we recommend using high-availability Authentication Provider, so that if production goes down, ViPR can still connect to the redundant one. Alternatively, register all your redundant Authentication Providers in your Active site. **Note** You can also login to ViPR as root user after Failover and add or change the Authentication Provider details to point to a recovered Authentication Provider, if the URL is different from what you set in the Active site previously.	
SMI-S providers	Follow the usual best practices for the underlying array's DR operations support in ViPR. For example, SRDF : 1 SMI-S for Site1 array, and 1 SMI-S for Site2 array. Both need to be registered in ViPR for SRDF operations to work. If disaster strikes Site 1, you can Failover the DR site's volumes using SMI-S at the DR site. You can also provision new non-replicated volumes (if necessary) using the Site 2 provider. Once Site 1 is back up, you can resume normal operations.	
RecoverPoint	Follow usual ViPR best practices for discovering RecoverPoint. It should be sufficient to register one management IP of the RecoverPoint appliance. ViPR discovers and internally stores the DR site's management IP address, so in the case where the registered one goes down, failover can still be performed, as ViPR will use another site's available IP address that was discovered internally.	
VPLEX	Follow usual the ViPR best practices for discovering VPLEX.	

Table 7 Best Practices in Configuring System Disaster Recovery (continued)

Configuration Item	Recommendation	System Disaster Recovery Notes
Isilon	Isilon file system configurations consist of NFS exports, export rules, NFS ACLs, and quota configurations: • During a Failover operation, the source file system's NFS export, export rules, and NFS ACLs are replicated to the target file system. **Note** Quota directories and snapshots are not replicated during a Failover operation. Sub-directory exports are not replicated if data synchronization has not taken place. During the first Failover, all configurations are replicated to the target file system, but during subsequent Failovers only the changes are replicated. • During a Failback operation, the target file system's NFS export, export rules, NFS ACLs and quota configurations are replicated to the source file system. Only the changes are replicated.	
Arrays with no ViPR managed resource replication	Resources are only managed if datacenter in which they are located is online.	Failover ViPR, then continue to manage the remaining available resources not impacted by the disaster. Physical resources impacted by the disaster can continue to be managed after they are back online, from the DR site. After all datacenters are back online , the Security Administrator can Switchover to the original datacenter.
Arrays with ViPR managed replication technology	Depending on the underlying array/storage type, plan ahead for a potential DR situation and if necessary for business continuity, pre-create any necessary Virtual Pools (with expected Source/Target vpool settings) so that any new provisioning can resume after ViPR failover in a timely manner. Failure to do so in certain situations	Failover ViPR, then perform any supported DR operations on array replicated resources (such as Failover using ViPR

Table 7 Best Practices in Configuring System Disaster Recovery (continued)

Configuration Item	Recommendation	System Disaster Recovery Notes
	may result in a longer time to resume any new provisioning operations. For example, reverse direction Source/Target vpools or completely new pools may need to be created later during DR. These virtual pools may be needed in situations where source volumes need to be created in the DR site, while the Active datacenter is being recovered from disaster) Work with your EMC support specialist if you need any help with proper planning for such situations.	catalog service for SRDF/RP), using ViPR. After all datacenters are back online , the Security Administrator can do a Switchover to the original datacenter.
Setting System Properties	There are some specific system properties that can be set separately for the Active and Standby sites, once they are connected: • Custom Node names • Login banner • Keystore certificate All other system and security settings are shared among all sites.	
Order processing during Failover	For in-progress order and array discoveries that were in progress during an Active site disaster : • In-progress orders will be marked as Failed. They need to be cleaned up and retried after Failover. • In-progress discoveries will be marked as Failed. After Failover, they will be reinitiated, based on normal scheduling. • After Failover, queued orders (concurrent orders for same arrays) will continue. • After Failover, a storage re-discovery and provider re-scan job are initiated immediately. A new order should be initiated after that.	
Backup and Restore	Regular backup is still highly recommended, even after a DR configuration is in place. Backup helps you keep data from days ago, which may be helpful for other disaster recovery cases, such as complete data center failures, man-made disasters, etc. • In DR environments, backup uploads to FTP/FTPS/ CIFS sites will have an appended site ID. • Only the Active site will have backup scheduler running. • After Switchover or Failover is done, the backup schedule continues as it was configured on the original Active site.	

Table 7 Best Practices in Configuring System Disaster Recovery (continued)

Configuration Item	Recommendation	System Disaster Recovery Notes
	• In a DR environment, it is better to Failover to a Standby DR site instead of Restoring. If DR cannot be done, follow with a Restore from backup. • The Restore from backup procedure has extra steps in a DR environment. For details refer to Restoring from a backup in a System Disaster Recovery environment.	
Cluster State in DR Sites	The Cluster State reporting in DR sites view will show "UNKNOWN" if the site is PAUSED. This is expected behavior.	
Properties change in a Standby site	When a Standby site is PAUSED, changing of any properties such as banner, customer names, or keystore is not allowed.	
Standby Mode - services in standby	A Standby site will have eight services "running" as seen via The Health UI page, as opposed to the Active site, which has 11 services running.	
Unexpected shutdown or power outage	In the event of an unexpected shutdown or power outage: • If a Standby site doesn't come back, shut down the ViPR Controller instance and reboot. Redeploy the ViPR Controller instance and re-add it to the Active site as a Standby. • If the Active site doesn't come back, shut down the ViPR Controller instance and reboot. Then do a Failover to a Standby site, redeploy the ViPR Controller instance and add it to the site. Finally do a Switchover.	
Outage of a majority of nodes	If the Active site or a Standby site temporarily experience an outage of a majority of their nodes, the Standby site can return to a synchronized state with the Active site only after ALL nodes of the Active and Standby site(s) are back and their controller status is "STABLE".	
General Guidance	After recovering ViPR controller itself on the Standby site, and bringing physical assets online (if applicable), you can proceed to: • Use ViPR protection catalog service to enable ViPR-managed array replicated resources on the Standby site, if applicable (for example, use ViPR catalog to failover SRDF or RP volumes to the Standby site). • Continue to use ViPR for provisioning on available assets.	

Table 7 Best Practices in Configuring System Disaster Recovery (continued)

Configuration Item	Recommendation	System Disaster Recovery Notes
	Contact your EMC support representative for assistance in planning of the end-to-end DR configuration for use cases based on your datacenter physical assets and environment. Related documents (which is available from the ViPR Controller Product Documentation Index: *EMC ViPR Controller 3.0 Integration with RecoverPoint and VPLEX User and Administration Guide* *EMC ViPR Controller 2.4 Integration with VMAX and VNX Storage Systems Guide*	

CHAPTER 3

Node recovery

Use the Node Recovery page to return the ViPR Controller virtual machine (node) back to normal function.

Node Recovery

Use **System** > **Node Recovery** to recover a ViPR Controller virtual machine (VM), when the minority number of nodes have gone down, while keeping ViPR Controller available and in production.

Recovery steps
Node recovery on a virtual appliance (vApp) is applicable only when the minority node(s) is offline or powered down for greater than five days and cannot rejoin the cluster after the nodes are brought up. At that time, all other services are working well except dbsvc and geodbsvc. You do not need to redeploy the virtual machines.

It is helpful to know the following:

- Recovery is currently available for VMware No-vApp and Hyper-V environments, and for vApp environments with a single site. Recovery on vApp is possible only when all nodes are available (just services corrupted), and doesn't work for whole-node-corrupted scenarios.
- 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.
- Only ViPR Controller Security Administrators can perform a node recovery operation.
- Node recovery can only be performed through the ViPR Controller UI.
- Node recovery may take some time, since a database repair is first required. To check on the status of a database repair, click **Dashboards** > **Database Housekeeping Status**.

Click **Start Node Recovery** to start the node recovery.

Recovery Status
Lists the status of the recovery.

Lists the time recovery started and finished.

Recover virtual machines when minority nodes fail

Minority node recovery allows you to recover the ViPR Controller virtual machines (VMs) when the minority number of nodes fail. (One node in a three-node deployment, or one or two nodes in a five-node deployment.) 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.

Note

In a System Disaster Recovery configuration , minority node recovery is only supported on the Active controller instance. Before performing minority node recovery on the Active site, verify that all other Disaster Recovery sites are STABLE and SYNCED. If there is a fatal issue with a node in a Standby site, the Standby site must be removed, freshly re-deployed, and re-added as a Standby site.

- 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.
- 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** > **Node Recovery** page, and click **Start Node Recovery** to initiate the recovery process.

Note

Node recovery may take some time, since a database repair is first required. To check on the status of a database repair, click **Dashboards** > **Database Housekeeping Status**.

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 4

Native Backup and Restore Service

Use the ViPR Controller native backup and restore service to create a backup set of ViPR Controller nodes.

EMC ViPR Controller native backup and restore service

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.

Managing ViPR Controller backups

By default, a backup of the ViPR Controller instance is created daily. ViPR Controller also allows you to create a point-in-time backup manually, on demand from the ViPR Controller UI, REST API, or CLI.

Note

In a System Disaster Recovery environment, backup can only be run on the Active ViPR controller instance. On Standby ViPR controller instances, the backup and restore service is not supported and disabled.

Automatic vs. manual backup

Automatically generated backups are run at the same time, once or twice a day. The time of day and the number of backups per day are scheduled from the ViPR Controller UI, **System** > **General Configuration** > **Backups** tab. For complete steps see: Schedule backups using the ViPR Controller UI.

Scheduled backups, are saved with the following naming conventions:

```
vipr-<version>-<total number of nodes in installation>-
<timestamp>
```

For example

```
vipr-2.4-3-201510100800
```

For steps to create a point-in-time backup see: Manually creating a ViPR Controller backup.

In addition to creating, and uploading automatic backups at the time defined in the ViPR Controller scheduler, the following will also trigger ViPR Controller backup operations.

When the following occurs, it triggers ViPR Controller to check to see if there are backups on the ViPR Controller that haven't been uploaded to the external site:

- Changes to any one of the ViPR Controller backup schedule options which includes the schedule enabler, backup time, or external server settings.
- Changes to the node status such as: node reboot, cluster reboot, or upgrade.

Additionally, if during unplanned triggering backup schedule, the scheduler detects the previous scheduled backup failed, it will run again.

Storing backups

The backup set is generated as a set of files on local storage (`/data/backup/`).

For automatically generated backups, ViPR Controller internally retains the last five backups. The default max count is 5. You can reconfigure it via the GUI to a value (0-5). When the max count is reached, the oldest backup will be removed from the ViPR Controller local storage, and a new one will be added to the backups.

Manually created backups are stored on the local storage. The default max count is 5. You can reconfigure it via the GUI to a value (0-5). When the max count is reached, you will not be allowed to create another manual backup.

For protection, it is highly recommended that you configure an external server to upload the backups. The external server is assigned from the ViPR Controller UI, **System** > **General Configuration** > **Backups** tab.

When an FTP or CIFS site is configured, the automatic backups are automatically added to a zip file, and uploaded to the FTP/CIFS site at the scheduled time. The zip file added to the FTP/CIFS site uses the following naming convention:

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

For example

```
vipr-2.4-3-201510100800-3-2-<unique site ID>.zip
```

If you manually create a backup, and you want to store it on the FTP/CIFS site, you will need to manually add it from the ViPR Controller UI, **System** > **Data Backup** page.

When manual backups are zipped, and added to the FTP/CIFS site, the file name is:

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

for example:

```
backupname-3-2-<unique site ID>.zip
```

A backup set can only be uploaded to the FTP/CIFS server from the ViPR Controller once. An uploaded backup set can be downloaded and restored from **System** > **Data Backup and Restore** > **Remote Backups** by clicking the **Restore** button after the backup.

Alternatively, you can manually download or copy backup sets to secondary storage using the REST call:

```
GET /backupset/download
```

or with CLI:

```
viprcli system download-backup
```

Note that this download is not from the external server. You can get backups from the external server using the REST call:

```
POST /backupset/pull
```

or with CLI:

```
viprcli system backup-pull
```

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 **System** > **General Configuration** > **Backup**.
2. Enter values for the properties.

Option	Description
Enable Scheduler	True turns on the scheduler.
Backup Time	The time (hh:mm) that the scheduled backup starts, based on the local time zone.
Number of Backups per Day	Choose 1 or 2 backups per day at the scheduled Backup Time. If you select 2, AM or PM will be shown after the Backup Time.
Backup Max Copies (scheduled)	The maximum number of scheduled backup copies (0-5) to save on the ViPR nodes. Once this number is reached, older scheduled backup copies are deleted from the nodes so that newer ones can be saved.
Backup Max Copies (manual)	The maximum number of manually-created backup copies (0-5) to save on the ViPR nodes. Once this number is reached, no additional copies can be created until you manually delete the older manually-created copies from the nodes.
External Server Type	Specify the external server type, FTP (the default) or CIFS. FTPS communications are secure; FTP and CIFS/SMB communications are not secure.
External Server URL	Specify the URL of an external file server. Supported protocols are FTP/FTPS and CIFS/SMB. Example: `ftps://10.233.95.162/my-vipr-backup/` For FTPS servers, 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://.

Option	Description
	• In this case port 990 is used. Due to protocol limitations, it is recommended that an external CIFS server be on the same LAN as the ViPR Controller instance. For CIFS/SMB servers, follow Linux style to set it to `smb://cifs_server`, instead of `\\cifs_server`. 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.
Domain	The Domain field appears only if you specified CIFS for the External Server Type. Specify a domain to login to backup to a CIFS file server.
User Name	User name for an account with read and write privileges to the FTPS or CIFS server.
Password	Password for the account.
Test External Server Settings	Click this button to establish a test connection to the external server specified.

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.

Manually creating and uploading ViPR Controller backups

A ViPR Controller backup can be created, and uploaded from the ViPR Controller UI, REST API, or CLI.

Before you begin

- This operation requires the System Administrator (SYSTEM_ADMIN) role in ViPR Controller.
- The maximum number of manually-created backup copies (0-5) that can be created is specified in the ViPR Controller UI via **System** > **General**

Configuration > **Backup.** Once this number is reached, you are not allowed to create a new backup manually until the old ones are deleted.

- By default, ViPR Controller will not generate a backup set when 1 or more nodes are down or unavailable in a 3 node deployment, or 2 or more nodes are down or unavailable in a 5 node deployment. You can however chose to override the default and force the creation of the backup set. To check the status of your ViPR Controller nodes from the ViPR Controller UI, go to the **Dashboards** > **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, **Dashboards** > **Database Housekeeping Status** page.
- It is recommended that the load on the system be light while creating a backup, especially on operations related to volume, fileshare, export, and snapshots.
- All backups are automatically uploaded to the FTP/CIFS site at the time defined in the ViPR Controller backup scheduler. Alternatively, you can upload manually created backups to the FTP/CIFS site, on demand, from the **Data Backup** page.
- A backup set can only be uploaded to the FTP/CIFS site once from the ViPR Controller UI. Alternatively you can manually download or copy backup sets to secondary storage using the ViPR Controller REST API, or CLI.
- When manual backups are zipped, and added to the FTP/CIFS site, the file name is:
  `manualbackupname-<total number of nodes in installation>-<number of nodes backed up>-<unique site ID>.zip`. For example:

  `backupname-3-2-<unique site ID>.zip`

Procedure

1. On a ViPR Controller node, create and upload a backup using one of these interfaces. These options create the backup in /data/backup/ on all ViPR Controller nodes. It is not necessary to run the command on each node:

Method	Page/Command
UI	Go to the **System** > **Data Backup and Restore** page to create a backup, upload a backup, or restore a backup.
REST API	Use `POST /backupset/backup` to create a backup. Use `POST /backupset/backup/upload` to upload the backup.
viprcli	Use `viprcli system create-backup -n` *`backupname`* to create a backup.

2. If using the ViPR Controller REST API, or CLI, use one of these methods to generate a file containing the backup set:

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

Summary of ViPR Controller UI operations

The following pages can be used to manage the backups from the ViPR Controller UI.

System > **General Configuration** > **Backup page**
To schedule the automatic backups. For details see: Schedule backups using the ViPR Controller UI .

System > **Data Backup and Restore page**
To:

- View the list of both automatically and manually created backups. You can view local backups in the Local Backups tab and Remote Backups (on the FTP/CIFS server, if specified) on the Remote Backups tab.
- Upload manually created backups, on demand, to the FTP/CIFS site configured in ViPR Controller for ViPR Controller backups.

  Note

  All backups are automatically uploaded to the FTP/CIFS site at the time defined in the ViPR Controller backup scheduler.
- Restore a backup from either the Local Backups tab or the Remote Backups tab.

  Note

  If there are many backups listed in the Remote Backups tab, some backup information pages may always be in a "loading" status. You can ignore this and go ahead with clicking **Restore** for the backup.
- Delete backups from the ViPR Controller.

  Note

  This operation does not delete the backup from the FTP/CIFS location.
- Access the **Add Backup** page to create a point-in-time backup of the ViPR Controller nodes.

While working on this page it is helpful to know:

- Only backup sets that were successfully created are listed on the **Data Backup** page. If you attempted to create a backup set that failed it will not be listed on the **Data Backup** page.

System > **Upgrade page**
To create a backup prior to upgrading ViPR Controller.

Summary of ViPR Controller REST API calls for native backup

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.

You can download the *ViPR Controller REST API Reference*, available as a zip file from the ViPR Controller Product Documentation Index.

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.

POST /backupset/backup/upload

Uploads a backup to the FTP/CIFS site configured for backups in the ViPR Controller.

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.

GET /backupset/external

Lists the current backup files in the external server.

POST /backupset/pull

Downloads a backup file from the remote server.

POST /backupset/pull/cancel

Cancels the current download from the external server.

POST /backupset/restore

Restores from the given backup.

GET /backupset/restore/status

Queries the restore status of a backup.

Summary of ViPR Controller CLI 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`

List backup files in external server

```
viprcli system list-external-backup
```

Download backup from external server

```
viprcli system pull-backup -n backupname
```

Cancel download from external server

```
viprcli system pull-backup-cancel
```

Restore the backup

```
viprcli system restore-backup -n backupname -islocal true/false -isgeo true/false
```

Query restore status

```
viprcli system restore-backup-status -n backupname
```

Restoring from a backup

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

Before you begin

Note

To restore from a backup created by the ViPR Controller backup service in a System Disaster Recovery environment, refer to Restoring from a backup in a System Disaster Recovery environment.

- Credentials for root user are required. If root ssh is disabled, you will also need credentials for the local ViPR Controller svcuser account.
- 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).
- 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 (mulitsite) environment.
- 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 or System Disaster Recovery 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.

- If the current ViPR Controller instance is still in a good state with the controller status STABLE, and is the same version as the backup, it can be restored on the current system. Otherwise, you may need to deploy a new ViPR Controller instance, using the same version as the backup, configure FTP/CIFS on that new ViPR Controller, and then go to **System** > **Data Backup and Restore** > **Remote Backups** to select the backup for restore.

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.
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.

   Note

   The next two steps use the ViPR Controller GUI to restore from backup and are recommended. If you prefer to use the older method, those steps are listed in the Note following.
5. Login to the ViPR Controller GUI and go to **System** > **General Configuration** > **Backup** to configure the External Server.
6. Go to the **System** > **Data Backup and Restore** > **Remote Backups** page, select a backup set, and click **Restore** In the **Action** column.
   a. In the **Restore** page that follows, you will see the progress of the download from the external server. When the download is complete, enter the current root password and click OK.
   b. Wait for the restore to complete. In the **Restore** page, you can click Cancel at any time to cancel the download and restore.
   c. You will be returned to the **Remote Backups** page. If the VDC is a part of GEO configuration, check "To restore the vdc1 in an all crashed Geo Environment" to make sure that vdc1 is the first one to restore.

Note

The following two steps use the older method to restore from backup:

- 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.
- 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 **Dashboards** > **Health**).
8. Go to the ViPR Controller UI, Dashboard page, and view 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.

Restoring from a backup in a System Disaster Recovery environment

Use the ViPR Controller GUI to restore a backup created by the EMC ViPR Controller backup service in a System Disaster Recovery environment.

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.
- 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).
- 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 (mulitsite) environment.
- 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 or System Disaster Recovery 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.
- If the current ViPR Controller instance is still in a good state with the controller status STABLE, and is the same version as the backup, it can be restored on the current system. Otherwise, you may need to deploy a new ViPR Controller instance, using the same version as the backup, configure FTP/CIFS on that new ViPR Controller, and then go to **System** > **Data Backup and Restore** > **Remote Backups** to select the backup for restore.

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.
2. **Note**

   Before proceeding, verify that all other options to recover the system have been exhausted. In a ViPR System Disaster Recovery environment, the preferred method is to use a Failover operation in System Disaster Recovery, rather than a restore from backup. Restoring from backup will require the reinstallation of all Disaster Recovery sites along with the Active site. Using Disaster Recovery Failover provides a better solution and minimizes data loss.

   To restore a backup that was taken on a system configured with System Disaster Recovery, proceed with the following steps.
3. Shut down the entire ViPR Controller System Disaster Recovery instance, including the Active site and all Standby sites.

4. 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. You do not need to deploy new Standby sites at this point in the procedure.
5. Power on the newly deployed 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.

Note

The next two steps use the ViPR Controller GUI to restore from backup and are recommended. If you prefer to use the older method, those steps are listed in the Note following.

---

6. Login to the ViPR Controller GUI and go to **System** > **General Configuration** > **Backup** to configure the External Server.
7. Go to the **System** > **Data Backup and Restore** > **Remote Backups** page, select a backup set, and click **Restore** In the **Action** column.
   a. In the **Restore** page that follows, you will see the progress of the download from the external server. When the download is complete, enter the current root password and click OK.
   b. Wait for the restore to complete. In the **Restore** page, you can click Cancel at any time to cancel the download and restore.
   c. You will be returned to the **Remote Backups** page. If the VDC is a part of GEO configuration, check "To restore the vdc1 in an all crashed Geo Environment" to make sure that vdc1 is the first one to restore.

Note

The following two steps use the older method to restore from backup:

- 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.
- 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.

---

8. Verify that the health of the system, and of all services, is good (in the ViPR Controller UI under **Dashboards** > **Health**). Verify that the current ViPR Controller status is reported as STABLE before proceeding to the next step.
9. Go to **System** > **System Disaster Recovery** and delete all Standby sites from the system. You will need to redeploy and re-add them fresh.
10. Go to the ViPR Controller UI, Dashboard page, and view 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.

11. When you have verified the health of the new system, delete all old ViPR Controller instances. (Do not power on the old instances; 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

Note

This procedure is NOT directly supported in a Disaster Recovery environment. To use backup and restore to reconfigure ViPR Controller in a Disaster Recovery environment, you must first remove all Standby sites, perform the reconfiguration, then redeploy and re-add fresh Standby sites.

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/CIFS site configured in: Schedule backups using the ViPR Controller UI.
3. Restore the backup on the new ViPR Controller instance as described in Restore backup.

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 5

Recovery with VMware SRM

It is possible to configure VMware SRM to recover the ViPR Controller in the event of datacenter disaster. First review use of ViPR Controller System Disaster Recovery process to see if appropriate for your deployment instead of VMware SRM.

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, ensure use of VMware documentation when planning, and deploying your disaster recovery environment.

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

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.

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.

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.

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 *EMC ViPR Controller Installation and Configuration Guide*, 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 (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.

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.

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:

- 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** > **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.
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** > **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.
   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** > **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** > **Virtual Data Centers** page.

   b. Select VDC2, and click **Reconnect**.