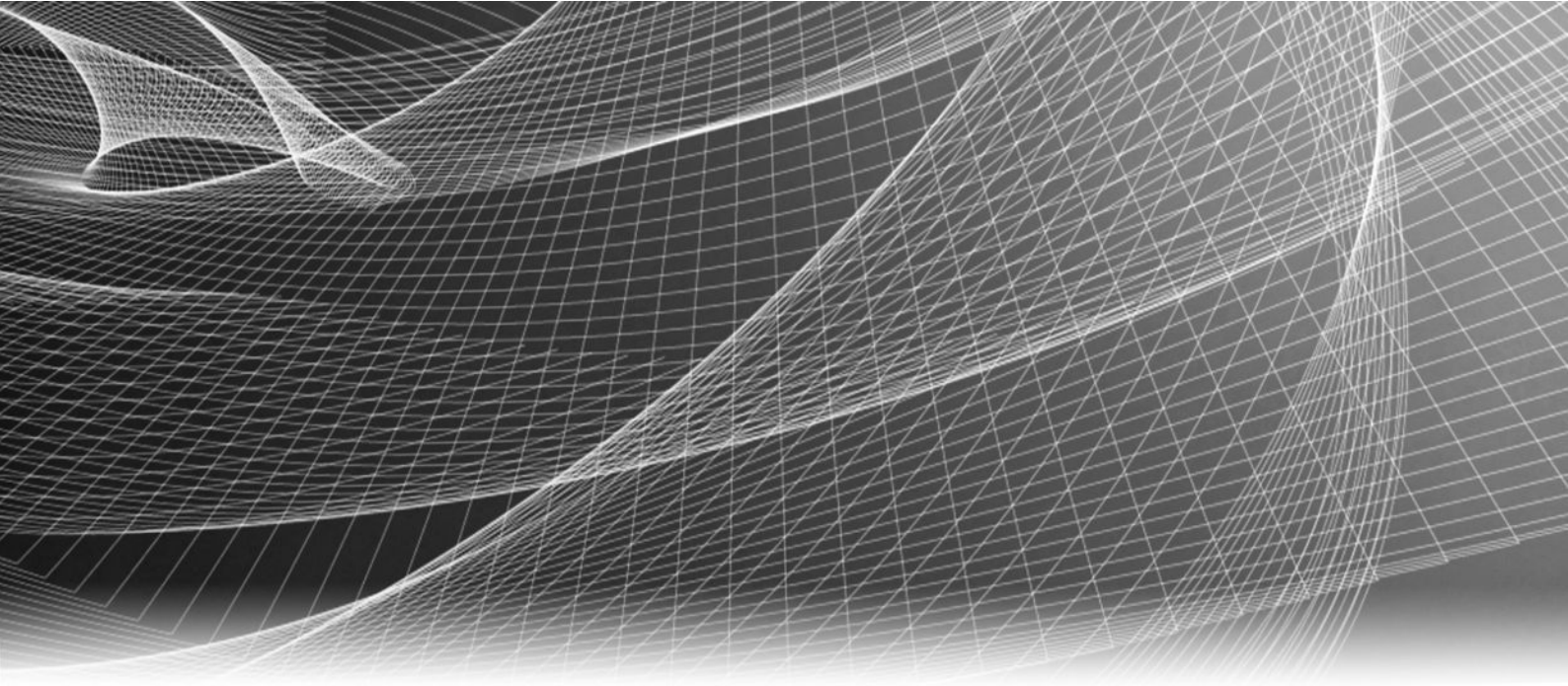

# EMC ViPR Controller

Version 2.3

## Installation, Upgrade, and Maintenance Guide

302-002-067
03

EMC²

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

Published July, 2015

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

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

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

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

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

# CONTENTS

# CHAPTER 1

# ViPR Controller installation and configuration roadmap

Use this roadmap as a starting point for ViPR Controller installation and configuration.

You must perform the following high-level sequence of steps to install and configure ViPR Controller. These steps must be completed for each instance of a ViPR Controller virtual data center. Once ViPR Controller is installed and configured, you can automate block and file storage provisioning tasks within the ViPR Controller virtual data center.

1. Review the ViPR Controller readiness checklist. on page 7
2. Obtain the EMC ViPR Controller license file. on page 10
3. Determine which method you will be using to deploy ViPR Controller, and follow the installation instructions:
   - Install ViPR Controller on VMware as a vApp on page 10
   - Install ViPR Controller on VMware without a vApp on page 14
   - Install ViPR Controller on Hyper-V on page 20
4. Optionally:
   - Install the ViPR Controller CLI.
     For steps to install the ViPR Controller CLI, refer to the *ViPR Controller CLI Reference Guide* which is available from the ViPR Controller Product Documentation Index .
   - Deploy a compute image server on page 25
5. Once you have installed the ViPR Controller, refer to the *ViPR Controller User Interface Tenants, Projects, Security, Users and Multisite Configuration Guide* to:
   - Add users into ViPR Controller via authentication providers.
   - Assign roles to users.
   - Create multiple tenants (optional)
   - Create projects.
6. Prepare to configure the ViPR Controller virtual data center, as described in the *ViPR Controller Virtual Data Center Requirements and Information Guide*.
7. Configure the ViPR Controller virtual data center as described in the *ViPR Controller User Interface Virtual Data Center Configuration Guide*.

# CHAPTER 2

# EMC ViPR Controller deployment readiness checklist

Use this checklist as an overview of the information you will need when you install and configure the EMC ViPR Controller virtual appliance.

For the specific models, and versions supported by the ViPR Controller, ViPR Controller resource requirements see the ViPR Controller Support Matrix.

- Identify an VMware or Hyper-V instance on which to deploy ViPR Controller.
- Make sure all ESXi servers (or all HyperV servers) on which ViPR controller will be installed are synchronized with good NTP servers.
- Collect credentials to access the VMware or Hyper-V instance.
  Deploying ViPR Controller credentials for an account that has privileges to deploy on the VMware or Hyper-V instance.
- Refer to the *ViPR Controller Support Matrix* to understand the ViPR Controller VMware or Hyper-V resource requirements, and verify that the VMware or Hyper-V instance has sufficient resources for ViPR Controller deployment.
- Identify 4 IP addresses for 3 node deployment or 6 IP addresses for 5 node deployment. The addresses are needed for the ViPR Controller VMs and for the virtual IP by which REST clients and the UI access the system. The address can be IPv4 or IPv6.

  **Note**

  that in dual mode, all controllers and VIPs must have both IPv6 and IPv4 addresses.
- A supported browser.
- Download the ViPR Controller deployment files from support.EMC.com and deploy.
- For each ViPR Controller VM, collect: IP address, IP network mask, IP network gateway, and optionally IPv6 prefix length and IPv6 default gateway.
- Two or three DNS servers
- Two or three NTP servers.
- ViPR Controller requires ICMP protocol is enabled for installation and normal usage.
- FTPS server for storing ViPR Controller backups remotely. You need the URL of the FTPS server and credentials for an account with read and write privileges on the FTPS server. Plan for 6 GB per backup initially, then monitor usage and adjust as needed.
- A valid SMTP server and email address.
- An Active Directory or LDAP server and related attributes.
  ViPR Controller validates added users against an authentication server. To use accounts other than the built-in user accounts, you need to specify.

# CHAPTER 3

# Deploying ViPR Controller

The chapter includes the following topics:

# Obtain the EMC ViPR Controller license file

You need to obtain the license file (.lic) from the EMC license management web site for uploading to EMC ViPR Controller.

### Before you begin

In order to obtain the license file you must have the License Authorization Code (LAC), which was emailed from EMC.

### Procedure

1. Go to support.EMC.com
2. Select **Support › Service Center**.
3. Select **Get and Manage Licenses**.
4. Select **ViPR** from the list of products.
5. On the LAC Request page, enter the LAC code and **Activate**.
6. Select the entitlements to activate and **Start Activation Process**.
7. Select **Add a Machine** to specify any meaningful string for grouping licenses.

   The "machine name" does not have to be a machine name at all; enter any string that will help you keep track of your licenses.
8. Enter the quantities for each entitlement to be activated, or select **Activate All**. Click **Next**.

   If you are obtaining licenses for a multisite (geo) configuration, you should distribute the controllers as appropriate in order to obtain individual license files for each virtual data center.
9. Optionally specify an addressee to receive an email summary of the activation transaction.
10. Click **Finish**.
11. Click **Save to File** to save the license file (.lic) to a folder on your computer.

    This is the license file that is needed during initial setup of ViPR after deployment, or when adding a new license later (**Settings › License**).

# Deploying ViPR Controller VMware with a vApp

Follow these steps to install ViPR Controller on VMware as a vApp on vSphere Enterprise edition and perform the initial setup.

### Before you begin

- You need access to the ViPR Controller deployment files. You can get them from the ViPR download page on support.emc.com.

  **vipr-‹version›-controller-2+1.ova**
  Deploys on 3 VMs. One VM can go down without affecting availability of the virtual appliance.

  **vipr-‹version›-controller-3+2.ova**
  Deploys on 5 VMs. Two VMs can go down without affecting availability of the virtual appliance.

  This option is recommended for deployment in production environments.

- You need credentials to log in to vSphere.
- Be prepared to provide new passwords for the ViPR Controller root and system accounts.
- You need IPv4 and/or IPv6 addresses for DNS and NTP servers.
- You need the name of an SMTP server. If TLS/SSL encryption is used, the SMTP server must have a valid CA certificate.
- You need access to the ViPR Controller license file.

### Procedure

1. Download a ViPR Controller OVA file from the ViPR Controller product page to a temporary directory.
2. Start the vSphere Client and log in to the vCenter Server on which you will be deploying the virtual appliance.
3. From the **File** menu, select **Deploy OVF Template**.
4. Browse to and select the ViPR Controller OVA file located in the temporary directory you created earlier.
5. On the **OVF Template Details** page, review the details about the appliance.
6. Accept the End User License Agreement.
7. Specify a name for the appliance.
8. Select the host or cluster on which to run the virtual appliance.
9. If resource pools are configured (not required for ViPR Controller), select one.
10. Select the datastore or datastore cluster for your appliance.
11. Select a disk format:
    - **Thick Provision Lazy Zeroed** (Default)
    - **Thick Provision Eager Zeroed** (Recommended for production deployment)
    - **Thin Provision**
12. On the **Network Mapping** page, map the source network to a destination network as appropriate.

    (If you are running vSphere Web Client, you can disregard the "IP protocol: IPv4" indicator; it is part of the standard screen text. In fact this deployment is used for both IPv4 and IPv6.)

13. Enter values for the properties.

    Note that when entering IP addresses, you must enter values for the IPv4 properties, or IPv6 properties, or both (if dual stack), according to the mode you need to support.

    **Server *n* IPv4 address**

    Key name: **`network_n_ipaddr`**

    One IPv4 address for public network. Each Controller VM requires either a unique, static IPv4 address in the subnet defined by the netmask, or a unique static IPv6 address, or both.

    Note than an address conflict across different ViPR Controller installations can result in ViPR Controller database corruption that would need to be restored from a previous good backup.

**Public virtual IPv4 address**
Key name: **network_vip**

IPv4 address used for UI and REST client access. See also Avoid conflicts in EMC ViPR network virtual IP addresses on page 54.

**Network netmask**
Key name: **network_netmask**

IPv4 netmask for the public network interface.

**IPv4 default gateway**
Key name: **network_gateway**

IPv4 address for the public network gateway.

**Server *n* IPv6 address**
Key name: **network_*n*_ipaddr6**

One IPv6 address for public network. Each Controller VM requires either a unique, static IPv6 address in the subnet defined by the netmask, or a unique static IPv4 address, or both.

Note than an address conflict across different ViPR Controller installations can result in ViPR Controller database corruption that would need to be restored from a previous good backup.

**Public virtual IPv6 address**
Key name: **network_vip6**

IPv6 address used for UI and REST client access. See also Avoid conflicts in EMC ViPR network virtual IP addresses on page 54.

**IPv6 prefix length**
Key name: **network_prefix_length**

IPv6 prefix length. Default is 64.

**IPv6 default gateway**
Key name: **network_gateway6**

IPv6 address for the public network gateway.

14. Power on the VM.

    If you made a mistake specifying IP addresses, netmask, or gateway, the VM may fail to boot up and you will see a message in the console. You can power off the vApp at this point, fix the IP values, and power on vApp again. (Don't rename ViPR VMs; renaming them is not supported.)

15. Wait 7 minutes after powering on the VM before you follow the next steps. This will give the ViPR Controller services time to start up.
16. Open https://*ViPR_virtual_ip* with a supported browser and log in as root.

    Initial password is ChangeMe.

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

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

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

    The passwords must meet these requirements:

    - at least 8 characters
    - at least 1 lowercase
    - at least 1 uppercase
    - at least 1 numeric
    - at least 1 special character
    - no more than 3 consecutive repeating
    - at least change 2 characters (settable)
    - not in last 3 change iterations (settable)

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

19. For DNS servers, enter two or three IPv4 or IPv6 addresses (not FQDNs), separated by commas.
20. For NTP servers, enter two or three IPv4 or IPv6 addresses (not FQDNs), separated by commas.
21. Select a transport option for ConnectEMC (FTPS (default), SMTP, or none) and enter an email address (user@domain) for the ConnectEMC Service notifications.

    If you select the SMTP transport option, you must specify an SMTP server under SMTP settings in the next step. "None" disables ConnectEMC on the ViPR Controller virtual appliance.

    In an IPv6-only environment, use SMTP for the transport protocol. (The ConnectEMC FTPS server is IPv4-only.)

22. (Optional) Specify an SMTP server and port for notification emails (such as ConnectEMC alerts, ViPR Controller approval emails), the encryption type (TLS/SSL or not), a From address, and authentication type (login, plain, CRAM-MD5, or none).

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

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

23. **Finish.**

    At this point ViPR Controller services restart (this can take several minutes).

### After you finish

You can now set up Authentication Providers as described in *ViPR Controller User Interface Tenants, Projects, Security, Users and Multisite Configuration Guide*, and setup your virtual data center as described in *ViPR Controller User Interface Virtual Data Center Configuration Guide*. Both guides are available from the ViPR Controller Product Documentation Index .

# Deploying ViPR Controller on VMware without a vApp

This section describes the prerequisites and the step-by-step procedure to use the installer script to perform initial installation of ViPR Controller nodes on VMware without a vApp, or to redeploy a ViPR Controller after failure.

### Before you begin

- You need access to the ViPR Controller deployment file, vipr-‹version›-controller-vsphere.zip. You can get the file from the ViPR download page on support.emc.com.
- You need credentials for an account with privileges for vSphere deployment.
- You can run the installer on a supported Linux or Windows computer that has IP access to the vCenter Server or to a specific ESXi server. See the *EMC ViPR Controller Support Matrix* for exact OS versions supported.
- The VMware OVF Tool command-line utility (ovftool), version 3.5.0 or 4.0.0, is required on the computer where you are running the installer script. Download OVF Tool from the VMware site. Add OVF Tool to the path environment variable so the installer can find it.
- To run the installer on Windows, PowerShell 4.0 is required.
- Be prepared to provide new passwords for the ViPR Controller root and system accounts.
- You need IPv4 and/or IPv6 addresses for DNS and NTP servers.
- Optionally, you need the name of an SMTP server. If TLS/SSL encryption is used, the SMTP server must have a valid CA certificate.
- You need access to the ViPR Controller license file.
- For details about redeploying ViPR Controller minority nodes see Backup and restore minority node failure on page 39.

### Procedure

1. Log in to a Linux or Windows computer that has IP access to the vCenter Server or to a specific ESXi server.
2. Download vipr-‹version›-controller-vsphere.zip from the ViPR download page on support.emc.com.
3. Unzip the ZIP file.
4. Open a bash command window on Linux, or a PowerShell window on Windows, and change to the directory where you unzipped the installer.
5. To deploy the ViPR Controller, run the vipr-*version*-deployment installer script to deploy ViPR Controller.

   You can run the script in interactive mode, or through the command line. Interactive mode will easily guide you through the installation, and the interactive script encodes the vCenter username and password for you in the event the username or password contains special characters, you will not be required to manually encode them.

   For interactive mode enter:

   - bash shell:

     ```
     .\vipr-2.3.0.0.682-deployment.sh -mode install -interactive
     ```

   - PowerShell

     ```
     .\vipr-2.3.0.0.637-deployment.ps1 -mode install -interactive
     ```

If you choose to deploy the ViPR Controller from the command line, you will need to manually enter the deployment parameters, and encode the vCenter username and password.

The following are examples of deploying ViPR Controller from the command line. See the following table for complete syntax.

- bash shell:

```
./vipr-2.3.0.0.682-deployment.sh -mode install -vip 1.2.3.0 -
ipaddr_1 1.2.3.1 -ipaddr_2 1.2.3.2
-ipaddr_3 1.2.3.3 -gateway 1.1.1.1 -netmask 255.255.255.0 -
nodeid 1 -nodecount 3
-targeturi vi://username:password@vsphere_host_url -ds
datastore_name -net network_name -vmprefix vmprefix-
-vmfolder vm_folder -dm zeroedthick -cpucount 2 -memory 8192 -
poweron
```

- PowerShell:

```
.\vipr-2.3.0.0.637-deployment.ps1 -mode install -vip 1.2.3.0 -
ipaddr_1 1.2.3.1 -ipaddr_2 1.2.3.2 -ipaddr_3
1.2.3.3 -gateway 1.1.1.1 -netmask 255.255.255.0 -nodeid 1 -
nodecount 3
-targeturi vi://username:password@vsphere_host_url -ds
datastore_name -net network_name -vmprefix vmprefix-
-vmfolder vm_folder -dm zeroedthick -cpucount 2 -memory 8192 -
poweron
```

While entering the options:

- 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.
- The argument delimiter for PowerShell is the double quotation (") but for bash it is single quotation (').

| Option | Description |
|---|---|
| **-help** | Optional, to see the list of parameters, and descriptions. |
| **-mode install** | Required for initial install. |
| **-mode redeploy** | Required to redeploy a node for restore. For details see: Backup and restore minority node failure on page 39. |
| **-interactive** | Optional for install, and redeploy.<br>Prompts for user input, one parameter at a time. Do not use delimiters when in interactive mode, that is, no single quotes, no double quotes. |
| **-nodecount** | Required for install.<br>Number of nodes: 3 or 5 or 1 for evaluation installation only. |
| **-vip** | Required for install.<br>Public virtual IPv4 address. |
| **-ipaddrs_n** | Required for install.<br>Where "n" equals the IPv4 address list of each node for example, -ipaddrs_1, -ipaddrs_2... i-ipaddrs_5. |
| **-netmask** | Required for install.<br>Network netmask. |

| Option | Description |
|---|---|
| -gateway | Required for install.<br>IPv4 default gateway. |
| -vip6 | Required for install if using IPv6.<br>Public virtual IPv6 address. |
| -ipaddrs6_n | Required for install.<br>Where "n" equals the IPv6 address list of each node for example, -ipaddrs6_1, -ipaddrs6_2... i-ipaddrs6_5. |
| -gateway6 | Required for install if using IPv6.<br>IPv6 default gateway. |
| -ipv6prefixlength | Optional for install if using IPv6.<br>IPv6 address prefix length. Default is 64. |
| -nodeid | Required for install and redeploy.<br>The -nodeid defines which node in cluster will be deployed (1, 2, 3 in 3 node install, or 1,2,3,4, or 5 in 5 nodes installation. The IP address of the node will be defined by this value (for example if specifying nodeid as 3, the IP address assigned to this node will be the address specified in ipaddrs_3 .<br>For example, when deploying a ViPR Controller 2+1 cluster on multiple ESXi and datastores, you run the installer script 3 times, using different values each time for the options -nodeid, -ds, and -targeturi.<br>The values of IP addresses for the -ipaddrs-n option must be the same each time.<br>node 1:<br>`.\vipr-2.2.1.0.100-deployment.ps1 -mode install -vip 10.20.30.40 -ipaddr_1 10.20.30.41 -ipaddr_2 10.20.30.42 -ipaddr_3 10.20.30.43 -gateway 10.20.35.45 -netmask 10.20.36.46 -vmprefix "Test123-" -dm thin -net mynetworkname -vmfolder "TestConfig/Test1" -poweron -ds "DATA STORE 1" -targeturi "vi://username:password@ESXi_HOST1_url" -nodeid 1`<br>node 2:<br>`.\vipr-2.2.1.0.100-deployment.ps1 -mode install -vip 10.20.30.40 -ipaddr_1 10.20.30.41 -ipaddr_2 10.20.30.42 -ipaddr_3 10.20.30.43 -gateway 10.20.35.45 -netmask 10.20.36.46 -vmprefix "Test123-" -dm thin -net mynetworkname -vmfolder "TestConfig/Test1" -poweron -ds "DATA STORE 1" -targeturi "vi://username:password@ESXi_HOST1_url" -nodeid 2`<br>node 3:<br>`.\vipr-2.2.1.0.100-deployment.ps1 -mode install -vip 10.20.30.40 -ipaddr_1 10.20.30.41 -ipaddr_2 10.20.30.42 -ipaddr_3 10.20.30.43 -gateway 10.20.35.45 -netmask 10.20.36.46 -vmprefix "Test123-" -dm thin -net mynetworkname -vmfolder "TestConfig/Test1" -poweron -ds "DATA STORE 1" -targeturi "vi://username:password@ESXi_HOST1_url" -nodeid 3` |

| Option | Description |
|---|---|
| -net *networkname* | Required for install and redeploy.<br>Set a network assignment. |
| -file | Optional for install, required for redeploy.<br>Valid path and name to the configuration settings file. |
| -vmprefix | Optional for install, and redeploy.<br>Prefix of virtual machine name.<br>You can use either -vmprefix, or -vmname, but not both. |
| -vmname | Optional for install, and redeploy.<br>Name of the virtual machine.<br>You can use either -vmprefix, or -vmname, but not both. |
| -poweron | Optional for install, and redeploy.<br>Use -poweron if using the command line to power on the virtual machine after installation, or don't enter any value to not have the virtual machine power on after installation.<br>For interactive mode, at the command prompt, you will need to enter yes to power on the virtual machine after deployed, or no, do not power on.<br>If redeploying as part of minority node restore, do not power on until after you have started the node recovery as described in Backup and restore minority node failure on page 39. |
| -cpucount | Optional for install, and redeploy.<br>Number of CPUs for each virtual machine. Valid values are 1 - 16.<br>By default , 2 CPUs are used for 3 node installation and 4 CPUs are used for 5 node installation. For details see the ViPR Controller Support Matrix. |
| -memory | Optional for install, and redeploy.<br>Memory size for each virtual machine. Valid values are 4096 - 16384MB.<br>By default , 8192MB is used for a 3 node installation, and 16384 is used for a 5 node installation. To determine right values for specific customer inventory considerations refer to ViPR Controller Support Matrix. |
| -ds | Required for install, and redeploy.<br>Datastore name. |
| -vmfolder *folder* | Optional for install, and redeploy.<br>Target VM folder in VI inventory. |
| -dm {thin \| lazyzeroedthick \| zeroedthick} | Optional for install, and redeploy.<br>Disk format. Use thick for deployment in production environment. Default is zeroedthick. |
| -targeturi *target-uri* | Required for install, and redeploy.<br>This is the Target locator of vSphere. The format is:<br>*vi://vSphere client username:password@esxi_host_url* |

| Option | Description |
|---|---|
| | where the typical format for *esxi_host_uri* is:<br>*esxi_host_uri is datacenter-name/host/host-name/Resources/resource-pool*<br>Entering the username and password in the target URI is optional. If you do not enter the user name and password in the Target URI you will go into interactive mode, and be prompted to enter them during installation. An example for entering the URI without a user name and password is:<br>*My-vcener-or-ESXi.example.com/ViPR-DataCenter/host/ViPR-Cluster-/Resources/ViPR-Pool*<br>If you chose to enter the username and password in the URI, when you use URIs as locators, you must escape special characters using % followed by their ASCII hex value. For example, if *username* requires a backslash (for example, *domain**username*) use %5c instead of \ (that is, use *domain* `%5c`*username*) for example:<br>*vi://user1:password1@vcenter1.emc.com:443/My-vcener-or-ESXi.example.com/host/ViPR-Cluster-/Resources/ViPR-Pool*<br>For details refer to the *VMware OVF Tool User Guide*. |
| **-username** | Optional for install, and redeploy.<br>vSphere client user name.<br>You do not need to escape special characters when entering the username at the interactive mode prompt. |
| **-password** | Optional for install, and redeploy.<br>vSphere client password.<br>You do not need to escape special characters when entering the username at the interactive mode prompt. |

6. If redeploying a failed node, refer to Backup and restore minority node failure on page 39 for the remaining steps.

   If installing ViPR Controller for the first time, repeat steps 1 - 5 for each node you are installing.

   You will need to enter all the information required to install the first node, however, you will not need to enter the information for the additional nodes. A `.settings` file is created during installation of the first node. The settings file is used to enter the configuration information for the remaining nodes.

   Once all nodes are installed continue to step 7.

7. Wait a few minutes after powering on the nodes before you follow the next steps. This will give the ViPR Controller services time to start up.
8. When the installer script indicates successful deployment and the VMs are powered on, open the ViPR Controller UI with a supported browser and log in as root.
   - The initial password is ChangeMe.
   - The *ViPR_virtual_IP* is the ViPR Controller public virtual IP address, which is the vip or vip6 value. You can also use the corresponding FQDN for the URL.

9. Browse to and select the license file that was downloaded from the EMC license management web site, then **Upload License**.
10. Enter new passwords for the root and system accounts.

    The passwords must meet these requirements:

    - at least 8 characters
    - at least 1 lowercase
    - at least 1 uppercase
    - at least 1 numeric
    - at least 1 special character
    - no more than 3 consecutive repeating
    - at least change 2 characters (settable)
    - not in last 3 change iterations (settable)

    The ViPR Controller root account has all privileges that are needed for initial configuration; it is also the same as the root user on the Controller VMs. The system accounts (sysmonitor, svcuser, and proxyuser) are used internally by ViPR Controller.
11. For DNS servers, enter two or three IPv4 or IPv6 addresses (not FQDNs), separated by commas.
12. For NTP servers, enter two or three IPv4 or IPv6 addresses (not FQDNs), separated by commas.
13. Select a transport option for ConnectEMC (FTPS (default), SMTP, or none) and enter an email address (user@domain) for the ConnectEMC Service notifications.

    If you select the SMTP transport option, you must specify an SMTP server under SMTP settings in the next step. "None" disables ConnectEMC on the ViPR Controller virtual appliance.

    In an IPv6-only environment, use SMTP for the transport protocol. (The ConnectEMC FTPS server is IPv4-only.)
14. (Optional) Specify an SMTP server and port for notification emails (such as ConnectEMC alerts, ViPR Controller approval emails), the encryption type (TLS/SSL or not), a From address, and authentication type (login, plain, CRAM-MD5, or none).

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

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

### After you finish

You can now set up Authentication Providers as described in *ViPR Controller User Interface Tenants, Projects, Security, Users and Multisite Configuration Guide*, and setup your virtual data center as described in *ViPR Controller User Interface Virtual Data Center Configuration Guide*. Both guides are available from the ViPR Controller Product Documentation Index .

# Deploying ViPR Controller on Hyper-V

This section describes the prerequisites and the step-by-step procedure for installing the ViPR Controller virtual machine in a Hyper-V environment.

### Before you begin

- You need access to the ViPR Controller deployment file. You can get the file from the ViPR download page on support.emc.com.

  **vipr-<version>-controller-hyperv.zip**
  Deploys 3 or 5 VMs, depending on selection you make during deployment.

- You need credentials to log in to the Service Center Virtual Machine Manager (SCVMM).
- Be prepared to provide new passwords for the ViPR Controller root and system accounts.
- You need IPv4 and/or IPv6 addresses for DNS and NTP servers.
- You need the name of an SMTP server. If TLS/SSL encryption is used, the SMTP server must have a valid CA certificate.
- You need access to the ViPR Controller license file.
- Note the following restrictions on ViPR Controller VMs in a Hyper-V deployment:
  - Hyper-V Integration Services are not supported. Do not install Integration Services on ViPR Controller VMs.
  - Restoring from a Hyper-V virtual machine checkpoint or clone is not supported.
  - Modifications to VM memory, CPU, or data disk size requires powering off whole cluster, prior to changing with SCVMM.

### Procedure

1. Log in to the SCVMM server using the Administrator account, and copy the zip file to the SCVMM server node.
2. Unzip the ZIP file.
3. Open a PowerShell window and change to the unzip directory.
4. To deploy the ViPR Controller, run the vipr-*version*-deployment installer script.

   You can run the script in interactive mode, or through the command line. Interactive mode will easily guide you through the installation, or you can use the command line to enter the parameters on your own.

   For interactive mode enter:

   ```
   .\vipr-release_version_deployment.ps1 -mode install -interactive
   ```

   From the command line, you will need to enter the parameters when deploying. The following is only an example, see the table for complete syntax.

   ```
   .\vipr-release_version_deployment.ps1 -mode install -vip
   10.200.101.100 -ipaddr_1 10.200.101.101
   -ipaddr_2 10.247.101.102 -ipaddr_3 10.247.101.103 -gateway
   10.247.100.1 -netmask 255.255.255.0 -nodeid 1 -nodecount 3
   -net lglw -vswitch vSwitch1 -librarypath \\lglax200\MSSCVMMLibrary
   -vmhostname lglax140.vipr.instance
   ```

```
-vmpath C:\\ClusterStorage\Volume4 -vmprefix viprtest -disktype
dynamic -vlanid 96 -cpucount 2 -memory 8192 -poweron
```

| Option | Description |
|---|---|
| **-help** | Optional, to see the list of parameters, and descriptions. |
| **-mode install** | Required for initial install. |
| **-mode redeploy** | Required to redeploy a node for restore. For details see: Backup and restore minority node failure on page 39. |
| **-interactive** | Optional for install, and redeploy.<br>Prompts for user input, one parameter at a time. Do not use delimiters when in interactive mode, that is, no single quotes, no double quotes. |
| **-nodecount** | Required for install.<br>Number of nodes: 3 or 5 |
| **-vip** | Required for install.<br>Public virtual IPv4 address. |
| **-ipaddrs_n** | Required for install.<br>Where "n" equals the IPv4 address list of each node for example, -ipaddrs_1, -ipaddrs_2... i-ipaddrs_5. |
| **-netmask** | Required for install.<br>Network netmask. |
| **-gateway** | Required for install.<br>IPv4 default gateway. |
| **-vip6** | Required for install if using IPv6.<br>Public virtual IPv6 address. |
| **-ipaddrs6_n** | Required for install.<br>Where "n" equals the IPv6 address list of each node for example, -ipaddrs6_1, -ipaddrs6_2... i-ipaddrs6_5. |
| **-gateway6** | Required for install if using IPv6.<br>IPv6 default gateway. |
| **-ipv6prefixlength** | Optional for install if using IPv6.<br>IPv6 address prefix length.<br>Default is 64. |
| **-nodeid** | Required for install and redeploy.<br>The -nodeid defines which node in cluster will be deployed (1, 2, 3 in 3 node install, or 1,2,3,4, or 5 in 5 nodes installation. The IP address of the node will be defined by this value (for example if specifying nodeid as 3, the IP address assigned to this node will be the address specified in ipaddrs_3 .<br>For example, when deploying a ViPR Controller 2+1 on different hosts of a Hyper-V cluster, you run the installer script 3 times, using different values each time for the options -nodeid, and -vmpath. |

| Option | Description |
|---|---|
| | The order of IP addresses for the -ipaddrs_n option must be the same each time.<br>node 1:<br>`.\vipr-2.3.0.0.669-deployment.ps1 -mode install -vip 1.2.3.0 -ipaddr_1 1.2.3.1 -ipaddr_2 1.2.3.2 -ipaddr_3 1.2.3.3 -gateway 1.1.1.1 -netmask 255.255.255.0 -nodeid 1 -nodecount 3 -net network_name -vswitch virtual_switch_name -librarypath library_path -vmhostname vm_host_name -vmpath vm_path -disktype fixed -vlanid vlan_id -vmnameprefix vmprefix -cpucount 2 -memory 8192 -poweron`<br>node 2:<br>`.\vipr-2.3.0.0.669-deployment.ps1 -mode install -vip 1.2.3.0 -ipaddr_1 1.2.3.1 -ipaddr_2 1.2.3.2 -ipaddr_3 1.2.3.3 -gateway 1.1.1.1 -netmask 255.255.255.0 -nodeid 2 -nodecount 3 -net network_name -vswitch virtual_switch_name -librarypath library_path -vmhostname vm_host_name -vmpath vm_path -disktype fixed -vlanid vlan_id -vmnameprefix vmprefix -cpucount 2 -memory 8192 -poweron`<br>node 3:<br>`.\vipr-2.3.0.0.669-deployment.ps1 -mode install -vip 1.2.3.0 -ipaddr_1 1.2.3.1 -ipaddr_2 1.2.3.2 -ipaddr_3 1.2.3.3 -gateway 1.1.1.1 -netmask 255.255.255.0 -nodeid 3 -nodecount 3 -net network_name -vswitch virtual_switch_name -librarypath library_path -vmhostname vm_host_name -vmpath vm_path -disktype fixed -vlanid vlan_id -vmnameprefix vmprefix -cpucount 2 -memory 8192 -poweron` |
| **-net *networkname*** | Required for install and redeploy.<br>Set a network assignment. |
| **-file** | Optional for install, required for redeploy.<br>Valid path and name to the configuration settings file. |
| **-vmprefix** | Optional for install, and redeploy.<br>Prefix of virtual machine name.<br>You can use either -vmprefix, or -vmname, but not both. |
| **-vmname** | Optional for install, and redeploy.<br>Name of the virtual machine. Enter a different value for each node i.e, vipr1, vipr2, vipr3,<br>You can use either -vmprefix, or -vmname, but not both. |
| **-poweron** | Optional for install, and redeploy.<br>Use -poweron if using the command line to power on the virtual machine after installation, or don't enter any value to not have the virtual machine power on after installation.<br>For interactive mode, at the command prompt, you will need to enter yes to power on the virtual machine after deployed, or no, do not power on. |

| Option | Description |
|---|---|
| | If redeploying as part of minority node restore, do not power on until after you have started the node recovery as described in Backup and restore minority node failure on page 39. |
| **-cpucount** | Optional for install, and redeploy.<br>Number of CPUs for each virtual machine. Valid values are 1 - 16.<br>By default , 2 CPUs are used for 3 node installation and 4 CPUs are used for 5 node installation. For details see the ViPR Controller Support Matrix. |
| **-memory** | Optional for install, and redeploy.<br>Memory size for each virtual machine. Valid values are 4096 - 16384MB.<br>By default , 8192MB is used for a 3 node installation, and 16384 is used for a 5 node installation. To determine right values for specific customer inventory considerations refer to ViPR Controller Support Matrix. |
| **-librarypath** | Required for install, and redeploy.<br>Library path shared in SCVMM. |
| **-vmhostname** | Required for install, and redeploy.<br>Host machine for the VM. |
| **-vmpath** | Required for install, and redeploy.<br>VM Path in host machine Note: user needs to make sure it exists. |
| **-vswitch** | Required for install, and redeploy.<br>Name of the virtual switch. |
| **-disktype** | Optional for install, and redeploy.<br>Type of virtual hard disk: `dynamic` or `fixed`. Use `fixed` for deployment in a production environment. |
| **-vlanid** | Required if VM network is configured with one or more VLANs; otherwise optional.<br>VLAN id. Default is -1. |

5. If redeploying a failed node, refer to Backup and restore minority node failure on page 39 for the remaining steps.

   If installing ViPR Controller for the first time, repeat steps 1 - 4 for each node you are installing.

   You will need to enter all the information required to install the first node, however, you will not need to enter the information for the additional nodes. A `.settings` file is created during installation of the first node. The settings file is used to enter the configuration information for the remaining nodes.

   Once all nodes are installed continue to step 7.

6. Wait a few minutes after powering on the nodes before you follow the next steps. This will give the ViPR Controller services time to start up.
7. Open https://*ViPR_virtual_ip* with a supported browser and log in as root.

   Initial password is ChangeMe.

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

8. Browse to and select the license file that was downloaded from the EMC license management web site, then **Upload License**.
9. Enter new passwords for the root and system accounts.

   The passwords must meet these requirements:

   - at least 8 characters
   - at least 1 lowercase
   - at least 1 uppercase
   - at least 1 numeric
   - at least 1 special character
   - no more than 3 consecutive repeating
   - at least change 2 characters (settable)
   - not in last 3 change iterations (settable)

   The ViPR Controller root account has all privileges that are needed for initial configuration; it is also the same as the root user on the Controller VMs. The system accounts (sysmonitor, svcuser, and proxyuser) are used internally by ViPR Controller.
10. For DNS servers, enter two or three IPv4 or IPv6 addresses (not FQDNs), separated by commas.
11. For NTP servers, enter two or three IPv4 or IPv6 addresses (not FQDNs), separated by commas.
12. Select a transport option for ConnectEMC (FTPS (default), SMTP, or none) and enter an email address (user@domain) for the ConnectEMC Service notifications.

    If you select the SMTP transport option, you must specify an SMTP server under SMTP settings in the next step. "None" disables ConnectEMC on the ViPR Controller virtual appliance.

    In an IPv6-only environment, use SMTP for the transport protocol. (The ConnectEMC FTPS server is IPv4-only.)
13. (Optional) Specify an SMTP server and port for notification emails (such as ConnectEMC alerts, ViPR Controller approval emails), the encryption type (TLS/SSL or not), a From address, and authentication type (login, plain, CRAM-MD5, or none).

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

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

    At this point ViPR Controller services restart. This can take several minutes.

### After you finish

You can now set up Authentication Providers as described in *ViPR Controller User Interface Tenants, Projects, Security, Users and Multisite Configuration Guide*, and setup your virtual data center as described in *ViPR Controller User Interface Virtual Data Center Configuration Guide*. Both guides are available from the ViPR Controller Product Documentation Index .

# Deploy a compute image server

A compute image server is required by ViPR Controller to deploy the compute images when you run a VCE Vblock™ System provisioning service, which performs operating system installation from ViPR Controller.

For information about ViPR Controller support for a Vblock system, see the: *Understanding ViPR Controller Support for VCE Vblock Systems* article which is available from the ViPR Controller Product Documentation Index .

## ViPR Controller network requirements for the compute image server

A network administrator must configure two networks before deploying the compute image server for ViPR Controller.

**Management Network**
The management network is required for communication between ViPR Controller, and the compute image server.

**Private OS Install Network**
The OS Install Network is a private network for operating system (OS) installation. The OS installation Network is used by ViPR Controller during provisioning, for communication between the hosts, and the ViPR Controller compute image server. Once the hosts, and ViPR Controller compute image server are connected over the OS Install Network, the operating system installation is then performed over the OS Install Network. Once installation is complete, the OS Install Network is removed from the hosts.

The Private OS Install Network must be:

- Configured with its own private DHCP server. No other DHCP server can be configured on the OS Install Network.

  **Note**

  The OS Image Server, which is provided with ViPR Controller, contains a dedicated DHCP server.

- Isolated from other networks to avoid conflicts with other VLANs.

## Deploying the compute image server

ViPR Controller provides a compute image server OVF template that you can deploy, or you can create a custom compute image server, which adheres to the ViPR Controller compute image server requirements. Refer to the following for details:

- Deploying the ViPR Controller Compute Image Server OVF file on page 25
- Requirements to create a custom Compute Image Server for ViPR Controller on page 27

### Deploying the ViPR Controller Compute Image Server OVF file

ViPR Controller is provided with a compute image server OVF template that you can deploy as a VM.

**Before you begin**

- You need access to the computer image server deployment file, `OSImageServer.x86_64-2.2.0.0.xx.ovf`, where xx is the compute image

server build version number, from the ViPR Controller download page on support.emc.com.

**Note**

The `OSImageServer.x86_64-2.2.0.0.xx` is supported with ViPR Controller 2.2 and higher.

- You need credentials to log in to vSphere for the vCenter Server where you are deploying the compute image server.
- During deployment you will need to provide:
  - Management Network
  - OS Install Network
  - A fully-qualified hostname for the compute image server
  - IPv4 address for the management network interface
  - IPv4 address for the private OS install network interfaces
  - Netmasks and gateway addresses for both the Management Network
  - One or more DNS server IPv4 addresses
  - Search domain
  - Time zone of the compute image server

**Procedure**

1. Download the compute image server image from the ViPR Controller product page to a temporary directory.
2. Start the vSphere Client and log in to the vCenter Server on which you will be deploying the virtual appliance.
3. From the File menu, select Deploy OVF Template.
4. Browse to and select the ViPR Controller compute image server file located in the temporary directory you created earlier.
5. On the **OVF Template Details** page, review the details about the appliance.
6. Accept the **End User License Agreement**.
7. Specify a name and location for the appliance.
8. Select the host or cluster on which to run the virtual appliance.
9. If resource pools are configured, select one.
10. If more than one datastore is attached to the ESX Server, select the datastore for your appliance.
11. Select a disk format: **Thick Provision Lazy Zeroed**, **Thick Provision Eager Zeroed**, or **Thin Provision**.
12. On the **Network Mapping** page, specify a destination network for the Management Network and for the private OS Install Network.
13. Enter the values for the properties:

| Property | Description |
|---|---|
| **Appliance fully qualified name** | FQDN of the image server host name. |
| **Management Network IP Address** | IPv4 address for the Management Network interface |

| Property | Description |
|---|---|
| **Management Network Netmask** | IPv4 netmask for the Management Network interface |
| **Management Network Gateway** | IPv4 address for the Management Network gateway |
| **Private OS Install Network IP address** | IPv4 address for the OS Install Network interface |
| **DNS Server(s)** | IPv4 addresses for one or more DNS servers |
| **Search Domain(s)** | One or more domains for directing searches. |
| **Time Zone** | Select the time zone where the image server resides. |

14. Power on the VM.

## Requirements to create a custom compute image server

If you choose to create a custom compute image server for the ViPR Controller compute images, the image server must be configured as follows:

- Compute Image Server must run on Linux OS
- Compute Image Server must have 2 vNICs
  - Management Network vNIC
  - OS Install Network vNIC
    OS Install vNIC netmask must be 255.255.255.0 for example:

```
/etc/sysconfig/network/ifcfg-eth1
DEVICE='eth1'
STARTMODE='auto'
BOOTPROTO='static'
IPADDR='12.0.55.10'
NETMASK='255.255.255.0'
```

- Compute Image Server must have DHCP server
  - DHCP server must be listening on the OS Install Network
  - DHCP response must contain "next-server" option with its own OS Install Network IP and "`filename`" option set to "`/pxelinux.0`"
  - Suggested DHCP version: Internet Systems Consortium DHCP Server 4.2 http://www.isc.org/downloads/dhcp/ as demonstrated in the following example. Note the next-server, and filename.

```
/etc/dhcpd.conf
ddns-update-style none;
ignore client-updates;

subnet 12.0.55.0 netmask 255.255.255.0 {
    option subnet-mask      255.255.255.0;
    option time-offset      -18000; # Eastern Standard Time

# --- DHCP pool configuration
    range 12.0.55.1 12.0.55.9;
    range 12.0.55.11 12.0.55.254;
    default-lease-time 3600;
    max-lease-time 7200;

# --- TFTP/PXE configuration
    next-server    12.0.55.10;
```

```
    filename "/pxelinux.0";
}
```

```
/etc/sysconfig/dhcpd
# listen on eth1 only
DHCPD_INTERFACE="eth1"
```

- Compute Image Server must have TFTP server
  - TFTP server must listen on the OS Install Network
  - TFTPBOOT directory must contain `pxelinux.0` binary (version 3.86) https://www.kernel.org/pub/linux/utils/boot/syslinux/3.xx/
  - Suggested TFTP server version: `tftp-hpa` https://www.kernel.org/pub/software/network/tftp/tftp-hpa/
  - TFTP can be configured to run as its own service or as part of `xinetd`. In the following example, TFTP was configured with `xinetd`

```
/etc/xinetd.d/tftp
service tftp
{
        socket_type             = dgram
        protocol                = udp
        wait                    = yes
        user                    = root
        server                  = /usr/sbin/in.tftpd
        server_args             = -s /opt/tftpboot/ -vvvvvvv
        disable                 = no
        per_source              = 11
        cps                     = 100 2
        flags                   = IPv4
}
```

- SSH acces
  - User account must have permissions to write to `TFTPBOOT` directory.
  - User account must have permissions to execute `mount`/`umount` commands
- Python
- Enough disk space to store multiple OS images - at least 50 GB is recommended
- No firewall blocking standard SSH, DHCP, TFTP ports and HTTP on 44491 (or a custom port chosen for HTTP).
- `wget` binary must be installed.

## Configure the compute image server in ViPR Controller

Once the compute image has been installed, you must configure it in ViPR Controller, before you can add the compute images to ViPR Controller.

### Before you begin

- Changes that you make to these properties will initiate a reboot of the ViPR Controller nodes when you click **Save**.

> **Note**
>
> Rebooting the ViPR Controller nodes may disrupt in ViPR Controller processes currently running.

### Procedure

1. Select **Settings** › **General Configuration** › **Compute Image Server**.

2. Enter values for the properties.

| Option | Description |
|---|---|
| **Compute Image Server Address** | FQDN or IP address of the compute image server. |
| **Compute Image Server OS Network IP** | IP address of the OS Install Network interface. The OS Install Network is the second network configured when the compute image server was deployed. |
| **Username** | Leave the default username, Root, or enter a new user name ViPR Controller will use to access the compute image server. |
| **Password** | Password for the compute image server user name. |
| **TFTPBOOT Directory** | Path to TFTPBOOT directory on the compute image server. /opt/tftpboot/ is the location fo the compute image server provided with ViPR Controller. |
| **OS Install Timeout** | Timeout value for OS installation (in seconds). Original value is 3600. |

3. **Save**.

# CHAPTER 4

# Logging in to the ViPR Controller User Interface

This chapter includes the following topics:

# Log in to EMC ViPR Controller

You can log in to the ViPR Controller UI from your browser by specifying the virtual IP address of the ViPR Controller appliance.

### Procedure

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

   https://*ViPR_virtual_ip*

2. Enter your username and password. The username should be in the format **`user@domain`**.
3. Optionally check **Remember me**, which maintains your session for a maximum of 8 hours or 2 hours of idle time (whichever comes first), even if you close the browser. If you don't check this option, your session ends when you close the browser, or log out. Logging out always closes the session.

   Note that this option does not remember user credentials between sessions.

   If you are unable to log in, contact your administrator.
4. You can log out at *username* › **Logout** on the upper-right corner of the UI.

# CHAPTER 5

# Upgrading ViPR Controller

This chapter includes the following topics:

# Pre-upgrade planning

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

- If you have a previous version of ViPR Controller that is running Data Services, you cannot upgrade to ViPR Controller 2.2 or higher. ViPR Controller 2.2 and higher are compatible with Controller-only environments. You must contact EMC Customer Support to upgrade ViPR running Data Services.
- Before upgrading the Controller-only environment, even if Data Services is not deployed, you must verify that there are no extra node ID addresses configured. In the ViPR Controller UI, check **Settings** › **Network**. Remove any values from the **Extra Nodes ID addresses** field.
- To determine if any steps are required before or after installation to ensure your environment is compliant with the latest support matrix, review the ViPR Controller Support Matrix, and the, "Environment and system requirements," in the *Release Notes*, which are available from EMC Online Support.
- In a multisite (geo) configuration, don't start an upgrade under these conditions:
  - if there are add, remove, or update VDC operations in progress on another VDC.
  - if an upgrade is already in progress on another VDC.
  - if any other VDCs in the federation are unreachable, or have been manually disconnected, or if the current VDC has been disconnected.
    In these cases, you should manually disconnect the unreachable VDC, and reconnect any disconnected VDC.
- In the unlikely event that you need to revert to the previous ViPR Controller version, you should make a backup of the ViPR Controller internal databases before upgrading. Refer to EMC ViPR Controller native backup and restore service on page 41.
- Prepare for the ViPR Controller virtual appliance to be unavailable for provisioning operations for approximately 1 minute for every 10,000 file shares, volumes, block mirrors, and block snapshots in the ViPR Controller database. Plan for system management operations to be unavailable for an additional period of 8 minutes (for a 2+1 Controller node deployment) or 12 minutes (for a 3+2 Controller node deployment).
- Verify that all ViPR orders have completed before you start the upgrade.
- If RecoverPoint is used, upgrade RecoverPoint to a version supported by ViPR Controller 2.3, before upgrading ViPR Controller itself. Refer to the EMC ViPR Support Matrix for supported RecoverPoint versions.

# Upgrade procedure

You can download and install new versions of ViPR Controller software from the **Settings** › **Upgrade** page.

### Before you begin

- This operation requires the System Administrator role in ViPR Controller.
- Refer to the pre-upgrade planning steps above.
- If necessary, configure the upgrade repository, including the credentials to access support.emc.com, on the **Settings** › **General Configuration** › **Upgrade** page of the ViPR Controller UI. Default repository is https://colu.emc.com/soap/rpc.

- If your site cannot access the EMC repository, an alternative method of upgrade, for dark sites, is described in Upgrading EMC ViPR Controller from an internal location on page 35.
- Verify that the ViPR controller status is Stable (**System › Dashboard**).

### Procedure

1. Select **Settings › Upgrade**.
2. Select an available ViPR Controller version and **Download**.

   The downloaded software is stored on the VM and can be installed at anytime.
3. In the Software Versions list, click **Install** next to the version that you want to upgrade to.

   A rolling upgrade is performed on the ViPR Controller VMs.

   The **System Maintenance** page opens while installation is in progress, and shows you the current state of the upgrade process.

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

### After you finish

Note the following about ViPR Controller after an upgrade:

- Modified ViPR Controller catalog services are always retained on upgrade, but to obtain new services, and original versions of modified services, go to **Edit Catalog**, and click **Update Catalog**.
- The upgrade process returns the trust store to its default contents. So if you removed certificates from the ViPR Controller trust store before upgrade, they are returned to the trust store upon upgrade. Note that ViPR Controller version 2.3 also adds a default list of certificates.
- After upgrading to version 2.3, any array with meta volumes need to be rediscovered, before you attempt to ingest those meta volumes.
- After upgrading to version 2.3, root login is disabled. To log in to ViPR Controller via the console, connect via SSH as svcuser, then switch user to root (`su - root`).
- After upgrading to version 2.3, rediscover your RecoverPoint Data Protection Systems. This refreshes ViPR Controller's system information and avoids inconsistencies when applying RecoverPoint protection with ViPR Controller 2.3.

# Upgrade ViPR Controller from an internal location

Normally you upgrade EMC ViPR Controller from an EMC-based repository, but you can upgrade from an internal location by first downloading the ViPR Controller. Offline Upgrade img file from support.EMC.com and copying it to the ViPR Controller virtual appliance.

### Before you begin

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

### Procedure

1. Download the ViPR Controller Offline Upgrade img file from support.EMC.com and save it locally on the system where you are running viprcli.

2. Run the following ViPR Controller CLI commands:

```
viprcli authenticate -hostname ViPR_virtual_ip -u root -d /tmp
viprcli -hostname ViPR_virtual_ip -cf cookie_file system upload -
imagefile locally_saved_img
```

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

   For details about using the ViPR Controller CLI see: *ViPR Controller CLI Reference Guide*, which is available from the ViPR Controller Product Documentation Index .

3. In the ViPR Controller UI, select **Settings** › **Upgrade**.
4. Select **Install** next to the version that you uploaded with the viprcli command.

# Upgrade the ViPR Controller CLI

To upgrade the ViPR Controller CLI, you must uninstall the version you are currently running, and install the most recent version.

For steps to uninstall, and install the ViPR Controller CLI see the *ViPR Controller CLI Reference Guide*, which is available from the ViPR Controller Product Documentation Index .

# CHAPTER 6

# ViPR Controller Backup and Restore

This chapter includes the following topics:

# Options for restoring ViPR Controller

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

**Table 1** Options to restore ViPR Controller

| Restore options | When to use: | Is ViPR Controller available during recovery | Supported environment |
|---|---|---|---|
| ViPR Controller Minority node recovery from node failure on page 39 | ViPR Controller is still in production (a quorum number of nodes are up and running), and:<br>• 1 VM is permanently lost when ViPR Controller is deployed on 3 VMs.<br>• Up to 2 VMs permanently lost when ViPR Controller is deployed on 5 VMs. | Yes, available | Single, or Multi-VDC, and installed on<br>• VMwre without vApp<br>• Hyper-V<br>Not supported when installed with a vApp. |
| ViPR Controller native backup and restore service on page 41 | • More than half of nodes are permanently lost.<br>• Any number of nodes are permanently lost when installed with a vApp. | Not available | Single, or Multi-VDC, and installed on<br>• VMware wiht vApp<br>• VMware without vApp<br>• Hyper-V |
| | Other possible use cases for backup and restore when ViPR Controller is configured with a single virtual data center:<br>• Migrate ViPR Controller from a 3 node installation to a 5 node installation, or from a 5 node installation to a 3 node installation.<br>• To relocate the ViPR Controller instance to new location using different IP addresses. | Not available | Single VDC only installed on<br>• VMware with vApp<br>• VMware without vApp<br>• Hyper-V |
| VMware Site Recovery Manager (SRM) on page 49 | 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<br>• VMware with vApp |

**Table 1** Options to restore ViPR Controller (continued)

| Restore options | When to use: | Is ViPR Controller available during recovery | Supported environment |
|---|---|---|---|
| | | | • VMware without vApp |

### ViPR Controller post restore

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

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

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

  **Note**

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

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

# Minority node recovery from node failure

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

### Before you begin

- Minority node recovery is only supported for ViPR Controller VMware installations without a vApp, or installations on Hyper-V.
- If a virtual machine becomes corrupt, first work with the virtual machine native software to fix the virtual machine. If there is no successful way to fix the virtual

machine through the native software, use ViPR Controller minority node recovery to resolve the issue.

- If you will be re-using an IP for the new machine, be sure to powerdown the virtual machine that are currently using the IP.
- Only ViPR Controller Security Administrators can perform a node recovery operation. Node recovery status can bee seen by Security Administrators, System Administrators, and System Monitors.
- Node recovery can be performed through the ViPR Controller UI, API, or 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 failed node, you will need to download the configuration parameters from ViPR Controller UI, **Recovery** page and save it as the parameter `-file` for 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 from where you will be running the deployment script. The configProperties file contains the network settings of cluster.
3. Run the `vipr-`*`version`*`.sh`, or `vipr-`*`version`*`.sh` followed by:

   For VMware

   - `-mode redeploy`
   - `-file configProperties`
     for installer script to redeploy ViPR Controller using 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 to failed vm.

   For example:

   - bash shell:

     ```
     ./vipr-2.3.0.0.xxxx-deployment.sh -mode redeploy -file
     configProperties
     ```

   - PowerShell:

     ```
     .\vipr-2.3.0.0.xxxx-deployment.ps1 -mode redeploy -file
     configProperties
     ```

   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.

For more deployment options for VMware see: Deploying ViPR Controller on VMware without a vApp on page 14.

For Hyper-V Run the following command ViPR Controller for each virtual machine you are restoring.

```
.\vipr-release_version-deployment.ps1 -mode redeploy -file
configProperties
```

For more deployment options for Hyper-V see: Deploying ViPR Controller on Hyper-V on page 20.

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

# EMC ViPR Controller native backup and restore service

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

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

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

```
GET /backupset/download
```

or with CLI:

```
viprcli system download-backup
```

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

Backup and restore must be between the same ViPR Controller version (for example, version 2.3.0.0.1043 must be restored to 2.3.0.0.1043).

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 environment.

## Schedule backups using the ViPR Controller UI

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

### Before you begin

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

### Procedure

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

| Option | Description |
|---|---|
| **Enable Scheduler** | True turns on the scheduler. |
| **Backup Time** | Select the time of day when the backup runs. The backup runs once a day; you cannot change the frequency of the backup. The time of day is the time where the ViPR Controller UI is running. |
| **External Server URL** | Specify the URL of an external file server. Supported protocols are ftp and ftps.<br>Example: `ftps://10.233.95.162/my-vipr-backup/`<br>If your FTPS server is configured with Explicit FTPS:<br>• The backup server URL should start with ftp://.<br>• Communication is performed over port 21.<br>If your FTPS server is configured with Implicit FTPS:<br>• The backup server URL should start with ftps://.<br>• In this case port 990 is used.<br>The filename format of the backup file that is uploaded to the external server is: `vipr-`*`version-nodeCount-datatime-number of nodes in the installation-number of nodes backed up`*`.zip`. Example:<br>In the following examples:<br>• `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.<br>• `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.<br>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. |

| Option | Description |
|---|---|
| **User Name** | User name for an account with read and write privileges the FTPS server. |
| **Password** | Password for the account. |

3. **Save**.

**After you finish**

Backup and upload success and failure messages are logged in the Audit log. Email notification of failure is sent only to the address associated with the ViPR Controller root user; be sure to add a valid email address at **root** › **Preferences** from the main ViPR UI page.

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

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

Details are in *EMC ViPR Controller REST API Reference*.

**GET /backupset/**
Lists all backups.

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

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

**DELETE /backupset/backup/**
Deletes a backup.

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

Below is an example using curl to download a backup.

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

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

## Summary of viprcli options for native backup

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

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

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

**Create backup**

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

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

**Delete backup**

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

**List all backups**

```
viprcli system list-backup
```

**Download backup**

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

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

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

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

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

**Before you begin**

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

**Procedure**

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

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

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

| Method | Command |
|---|---|
| REST API | `GET /backupset/download?tag=backupsetname` |

| Method | Command |
|---|---|
| viprcli | `viprcli system download-backup -n backupname -fp filepath` |

## Restoring from a backup

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

### Before you begin

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

### Procedure

1. If the VDC that you are restoring is part of a geo federated (multisite) configuration, refer to Restoring a virtual data center in a geo federated (multisite) environment on page 47.
2. If you will be restoring to new IP address, 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:
   - Deploying ViPR Controller VMware with a vApp on page 10
   - Deploying ViPR Controller VMware without a vApp on page 14
   - Deploying ViPR Controller on Hyper-V on page 20
4. Power on the virtual machines.

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

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

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

   **`/opt/storageos/bin/restore backup_ZIP_filepath`**

Example: **`/opt/storageos/bin/restore /tmp/vipr-2.3-1-20150114200225.zip`**

You initiate restore on one node only. Restore on the other nodes happens automatically.

Note that remote login as root might be disabled. It may be necessary to log in initially as svcuser, then switch user to root.

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

## Restore to change ViPR Controller IP addresses, or number of nodes

The native backup and restore features can be used to change the IP addresses of ViPR Controller nodes, or to change the number of nodes on which ViPR Controller is installed.

### Before you begin

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

Restoring or migrating 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: Deploying ViPR Controller on page 9.
2. Download the ViPR Controller backup files from the FTP site configured in: Schedule backups using the ViPR Controller UI on page 42.
3. Restore the new ViPR Controller from the original ViPR Controller instance as described in Restore backup on page 45.

**Note**

After restore is complete, ViPR Controller with new IP Addresses, certain system configuration settings from the original ViPR Controller instance, 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.

## 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.

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

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

To determine which type of restore is appropriate for your environment see Options for restoring ViPR Controller on page 38.

**Minority node recovery for VDC in geo federated environment**

In this case simply follow the procedure for minority node recovery as described in Minority node recovery for node failure on page 39.

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

The following requirements must be met to restore in a geo federated (multisite) envrionment, in addition to the target system requirements described in Restoring from a backup on page 45:

- If there are any version 2.0 or 2.1 VDCs in the federation, contact customer support and refer to KB article 000189026.
- In a geo federated environment, you cannot use the native backup and recovery operations to migrate ViPR Controller from a 3 node installation to a 5 node installation, or from a 5 node installation to a 3 node installation. Also, you cannot use native restore to relocate ViPR Controller instance because you must use the same IP addresses when restoring from a backup.

- Do not use a backup which was created on a single VDC to restore, after the VDC has been added to a multi-VDC configuration, and vice versa.

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

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

   For further details about disconnecting or reconnecting a VDC see the *ViPR Controller User Interface Tenants, Projects, Security, Users and Multisite Configuration Guide*which is available from the ViPR Controller Product Documentation Index .
2. Restore the ViPR Controller instance using the steps described in Restoring from a backup on page 45.
3. Log into the VDC that was still running in Step 1, and reconnect to the restored VDC.
   a. From the ViPR Controller UI, for the VDC that was not lost, go to the **Virtual Assets** › **Virtual Data Centers** page.
   b. Select the restored VDC, and click **Reconnect**.
4. Repeat steps 1 - 3 for each VDC that was lost.

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

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

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

Review the prerequisites above before continuing.

1. Download most recent backup files for both VDC1 and VDC2.
2. Shutdown VDC1 and VDC2 (if VMs are still running).
3. Redeploy VDC1 and restore VDC1 using steps described in xref: Restoring from a backup on page 45.
   When VDC1 is successfully restored it will be restored with connectivity to VDC2.
4. From VDC1, disconnect VDC2.
   a. Log in to the ViPR Controller UI for VDC1.
   b. Go to the **Virtual Assets** › **Virtual Data Centers** page.
   c. Select VDC2, and click **Disconnect**.

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

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

# ViPR Controller restore with VMware SRM

It is possible to configure VMware SRM to restore the ViPR Controller in the event of system failure.

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


- Configuring VMware SRM to restore ViPR Controller with vApp on page 49
- Configuring VMware SRM to restore ViPR Controller without vApp on page 51


## Configuring VMware SRM to restore 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.
- When using VMware SRM protection of ViPR Controller deployed on VMWare with a vApp, do not change the ViPR Controller VMs in vSphere from vipr1, vipr2, .. to a different name under any circumstances. This will result in ViPR Controller not functioning after failover to recovery site. ViPR Controller VMs must stay as vipr1, vipr2, vipr3...

### 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. Procced 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: "Power Off."

      Unselect VMware tools checkbox.

3. Test your recovery plan, in Test Recovery to verify successful configuration.
4. Upon successful test, perform cleanup.
5. Perform Recovery to make ViPR Controller available for production.

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

   a. Using the **Recovery Plan** defined in previous steps, perform the **Recovery** step in SRM and wait for the recovery plan steps to complete successfully..

   b. While ViPR Controller VMs are in powered off state on recovery site, for each VM:

      - Under **Edit Settings** › **Hardware**, add a CD/DVD drive as a client device.
      - Using vSphere select **Edit Settings** and navigate to **Options**.
      - Under vApp options, select **Enable**.
      - Under **OVF settings**, check **ON** in the **ISO image** box and **VMware Tools** box.

        **Note**

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

      - Power on ViPR Controller vApp.

### After you finish

After restore 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:

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

## 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 2a), 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, you will need to perform Change the IP address of ViPR Controller node on VMware with no vApp using vCenter on page 56, before ViPR Controller nodes can be successfully powered on with desired IP addresses.

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 a real recovery and optionally, perform the following post recovery steps after successful recovery, if ViPR Controller should have different IPs on the recovery site.

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

   **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 on page 56.

      After changing the IP addresses, the ViPR Controller nodes are up and running.

   If ViPR Controller on Recovery Site should have same IP settings as on Protected Site, ViPR Controller nodes should be up and running, proceed to "Reprotect"

### After you finish

Proceed to Reprotect.

# CHAPTER 7

# Managing IP Addresses of the ViPR Controller Nodes

This chapter includes the following topics:

# Avoid conflicts in EMC ViPR network virtual IP addresses

Restrictions exist on the EMC ViPR virtual IP address when there are multiple ViPR instances in the same subnet.

When more than one ViPR instance exists in the same subnet, use care when allocating the ViPR virtual IP addresses, to prevent a conflict in the load balancer's virtual router ID. The virtual router ID is calculated using the virtual IP address configuration with the following algorithm:

- IPv4 only or dual stack: virtual router ID is the last octet of the IPv4 address.
- IPv6 only: virtual router ID is the decimal equivalent of the last two hex digits in the IPv6 address.

For example, the following addresses in the same subnet would be invalid:

- 172.16.33.98 and 172.16.34.98 (because the last octets are the same, both 98)
- 172.16.33.98 and 2001:db8:170:2842::2462 (because 98 decimal equals 62 hex)

# Change the IP address of EMC ViPR Controller node

You can change the IP addresses of EMC ViPR Controller node and the network virtual IP address.

The method for changing the IP addresses is dependent on the type of installation, and the tool you choose to use:


- Change the IP address of EMC ViPR Controller node deployed as a VMware vApp on page 54
- Change the IP address of ViPR Controller node on VMware without vApp, or Hyper-V using ViPR Controller UI on page 55
- Change the IP address of EMC ViPR Controller node on VMware with no vApp using vCenter on page 56
- Change the IP address of EMC ViPR Controller node on Hyper-V using SCVMM on page 57


## Change the IP address of EMC ViPR Controller node deployed as a VMware vApp

This section describes how to change node IP address or VIP for a ViPR Controller virtual machine on VMware that was deployed as a vApp.

### Before you begin

If ViPR Controller was not deployed as a vApp, do not follow this procedure. Instead, refer to *Change the IP address of EMC ViPR Controller node on VMware deployed with no vApp*.

This operation requires the System Administrator role in ViPR Controller.

You need access to the vCenter Server that hosts the ViPR vApp.

If the ViPR Controller was deployed, do not follow this procedure. Instead, refer to

The ViPR vApp must not be part of a multi-VDC configuration. Check **Virtual Assets** › **Virtual Data Centers**; there should only be one VDC listed.

### Procedure

1. From the ViPR UI, shutdown all VMs (**System** › **Health** › **Shutdown All**).

2. Open a vSphere client on the vCenter Server that hosts the ViPR vApp.
3. Right-click the ViPR vApp whose IP address you want to change and select **Edit Settings**.
4. Expand **EMC ViPR**.
5. Edit the desired IP values and click **OK**.
6. If applicable, change the network adapter to match a change in the subnet:
   a. Select a specific VM.
   b. **Edit Settings**.
   c. Select **Virtual Hardware** › **Network adapter**.
   d. Click **OK**.
7. From the vSphere client, power on the ViPR vApp.

   Note: the ViPR vApp will fail to boot up after an IP address change if the vApp is part of a multi-VDC (geo) configuration. In this case you would need to revert the IP address change.

## Change the IP address of ViPR Controller node on VMware without vApp, or Hyper-V using ViPR Controller UI

Use the ViPR Controller UI to change the IP address of ViPR Controller nodes running on VMware without a vApp, or Hyper-V systems.

### Before you begin

If ViPR Controller was deployed as a vApp, do not follow this procedure. Instead, refer to Change the IP address of EMC ViPR Controller node deployed as a VMware vApp on page 54.

This operation requires the System Administrator role in ViPR Controller.

The ViPR Controller instance must not be part of a multi-VDC configuration. Check **Virtual Assets** › **Virtual Data Centers**; there should only be one VDC listed.

### Procedure

1. From the ViPR Controller UI, go to **Settings** › **Network Configuration.**
2. Leave the defaults, or enter the new IP addresses in the corresponding fields.

   Do not leave any of the IP address fields empty. You must leave the default, or enter the new IP address.
3. If you are changing the subnet, continue to step 4, otherwise, continue to step 5.
4. Enable the **Power off nodes** option.
5. Click **Reconfigure**.

   A message appears telling you that the change was submitted, and your ViPR Controller instance will lose connectivity.

   If you are not changing your subnet, you will be able to log back into ViPR Controller 5 to 15 minutes after the configuration change has been made. Only perform steps 6 and 7 if you are changing your network adapter settings in the VM management console.
6. Go to your VM management console (vSphere for VMware or SCVMM for Hyper-V), and change the network settings for each virtual machine.

7. Power on the VMs from the VM management console.

   You should be able to log back into the ViPR Controller 5 to 15 minutes after powering on the VMs

   If you changed ViPR Controller virtual IP address, remember to login with new virtual IP. ViPR Controller will not redirect you from the old virtual IP to the new virtual IP.

## Change the IP address of ViPR Controller node on VMware with no vApp using vCenter

This section describes how to change a node IP address or VIP from vCenter for a ViPR Controller virtual machine that was deployed on VMware as separate VMs, not as a vApp, in the event that the ViPR Controller UI was unavailable to change the IP addresses.

### Before you begin

If ViPR Controller was deployed as a vApp, do not follow this procedure. Instead, refer to *Change the IP address of EMC ViPR Controller node on VMware deployed as a vApp*.

This operation requires the System Administrator role in ViPR Controller.

You need access to the vCenter Server instance that hosts ViPR Controller.

The ViPR Controller instance must not be part of a multi-VDC configuration. Check **Virtual Assets** › **Virtual Data Centers**; there should only be one VDC listed.

### Procedure

1. From the ViPR UI, shutdown all VMs (**System** › **Health** › **Shutdown All**).
2. Open a vSphere client on the vCenter Server that hosts the ViPR Controller VMs.
3. Right-click the ViPR Controller node whose IP address you want to change and select **Power On**.
4. Right-click the ViPR VM whose IP address you want to change and select **Open Console**.
5. As the node powers on, select the 2nd option in the GRUB boot menu: **Configuration of a single ViPR(vipr-x.x.x.x.x) Controller node**.

   Be aware that you will only have a few seconds to select this option before the virtual machine proceeds with the default boot option.
6. On the Cluster Configuration screen, select the appropriate ViPR node id and click **Next**.
7. On the Network Configuration screen, enter the new IP address in the appropriate field and click **Next**.
8. On the Deployment Confirmation screen, click **Config**.
9. Wait for the "Multicasting" message at the bottom of the console next to the Config button, then power on the next ViPR Controller node.
10. As the node powers on, right-click the node and select **Open Console**.
11. On the next node, select the new VIP.

    Note: if you changed the VIP in a previous step, you will see two similar options. One has the old VIP, the other has the new VIP. Be sure to select the new VIP.
12. Confirm the Network Configuration settings, which are prepopulated.
13. On the Deployment Confirmation screen, click **Config**.
14. Wait for the "Multicasting" message at the bottom of the console next to the Config button, then power on the next ViPR Controller node.

15. Repeat steps 10 through 14 for the remaining nodes.
16. When the "Multicasting" message has appeared for all nodes, select **Reboot** from the console, for each ViPR node.

### After you finish

At this point the IP address change is complete. Note that the virtual machine will fail to boot up after an IP address change if the ViPR Controller is part of a multi-VDC (geo) configuration. In this case you would need to revert the IP address change.

## Change the IP address of ViPR Controller node on Hyper-V using SCVMM

This section describes how to change a node IP address or VIP for a ViPR Controller virtual machine on Hyper-V.

### Before you begin

This operation requires the System Administrator role in ViPR Controller.

You need access to the SCVMM Server instance that hosts ViPR Controller.

The ViPR Controllerr instance must not be part of a multi-VDC configuration. Check **Virtual Assets** › **Virtual Data Centers**; there should only be one VDC listed.

### Procedure

1. From the ViPR UI, shutdown all VMs (**System** › **Health** › **Shutdown All**).
2. Open the SCVMM UI on the SCVMM Server that hosts the ViPR Controller.
3. On the SCVMM UI, right-click the ViPR Controller node whose IP address you want to change and select **Power On**.
4. On the SCVMM UI, as the node powers on, right-click the node and select **Connect or View** › **Connect via Console**.
5. On the console GRUB menu, select the 2nd option, **Configuration of a single node**.

   Be aware that you will only have a few seconds to select this option before the virtual machine proceeds with the default boot option.
6. On the Cluster Configuration screen, select the appropriate ViPR Controller node id and click **Next**.
7. On the Network Configuration screen, enter the new IP address in the appropriate field and click **Next**.
8. On the Deployment Confirmation screen, click **Config**.
9. Wait for the "Multicasting" message at the bottom of the console next to the Config button, then power on the next ViPR Controller node.
10. On the SCVMM UI, as the node powers on, right-click the node and select **Connect or View** › **Connect via Console**.
11. On the next node, select the new VIP for the cluster configuration.

    Note: if you changed the VIP in a previous step, you will see two similar options. One has the old VIP, the other has the new VIP. Be sure to select the new VIP.
12. Confirm the Network Configuration settings, which are prepopulated.
13. On the Deployment Confirmation screen, click **Config**.
14. Wait for the "Multicasting" message at the bottom of the console next to the Config button, then power on the next ViPR Controller node.
15. Repeat steps 10 through 14 for the remaining nodes.

16. When the "Multicasting" message has appeared for all nodes, select **Reboot** from the console, for each ViPR node.

### After you finish

At this point the IP address change is complete. Note that the virtual machine will fail to boot up after an IP address change if theViPR Controller is part of a multi-VDC (geo) configuration. In this case you would need to revert the IP address change.

# CHAPTER 8

# Modifying the ViPR Controller Footprint

This chapter includes the following topics:

# Modify the ViPR Controller footprint on VMware

You can modify the CPU and memory resources used by the ViPR Controller VMs on VMware.

### Before you begin

- This operation requires the System Administrator role in ViPR Controller.
- You need access to the vCenter Server hosting ViPR Controller.

### Procedure

1. Shut down ViPR Controller from the UI at **System** › **Health** › **Shutdown All**.
2. Use the vSphere client to access the editable settings:
   a. Go to **VMs and Templates**
   b. Access the settings for each VM, depending on how ViPR Controller was deployed:

      If ViPR Controller was deployed as a vApp, browse to and select the ViPR Controller vApp, then select the **Virtual Machines** tab to see the individual VMs.

      If ViPR Controller was deployed as separate VMs (that is, no vApp), the individual VMs are visible in the VMs and Templates view.

   c. Right click a VM and select **Edit settings**.
   d. Adjust the **CPU** and **Memory** settings. Refer to the *EMC ViPR Support Matrix* for recommended CPU and memory sizes.

   Use identical settings for CPU and Memory on all ViPR Controller VMs.
3. Power up the ViPR Controller VMs or vApp.

# Modify the ViPR Controller footprint on Hyper-V

You can modify the CPU and memory resources used by ViPR Controller on Hyper-V.

### Before you begin

- This operation requires the System Administrator role in ViPR Controller.
- You need access to the Hyper-V server hosting the ViPR Controller virtual machine.

### Procedure

1. Shut down ViPR Controller from the UI at **System** › **Health** › **Shutdown All**.
2. Use the SCVMM UI to access the editable settings:
   a. Go to **VMs and Services** › **All Hosts**.
   b. Browse to and right-click the ViPR Controller VM for the first node.
   c. Select **Properties**.
   d. Select **Hardware Configuration**.
   e. Adjust the **Processor** and **Memory** settings. Refer to the *EMC ViPR Support Matrix* for recommended processor and memory sizes.
   f. Repeat for each ViPR Controller node.

   Use identical settings for processor and memory on all ViPR Controller nodes.

3. in the SCVMM UI, power up the ViPR Controller VM.

# APPENDIX A

# Other ViPR Controller configuration options

# ViPR Controller email options

ViPR Controller provides functionality to use email to communicate with various ViPR Controller users.

Email notifications can be sent from ViPR Controller to:

- The email configured to receive alert notifications from ViPR Controller. The alert notifications are copies of alerts sent to EMC Support from ConnectEMC. The email to the user from ViPR Controller, further indicates whether the alert sent from ConnectEMC to EMC Support was received by EMC Support successfully, or if it failed to be delivered to EMC Support.
- Tenant Approvers to request approvals from ViPR Controller provisioning users to run a service.
- Users
  - Root users can receive email notifications of failed backup uploads, or notifications of expired passwords.
  - Provisioning users can receive email notifications indicating if the Tenant Approver approved the order the user placed, or not.

**Enabling email notifications**

All email notification require that you enter the following fields either during initial login, or from the **Settings** › **General Configuration** › **Email** tab.

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

Once these settings have been enabled, you can continue to configure ViPR Controller for ConnectEMC, Tenant Approver, and user email notifications.

**To receive email from ConnectEMC**

Configure the ConnectEMC email from the **Settings** › **General Configuration** › **ConnectEMC** tab.

**To send email to Tenant Approvers**

Configure the Tenant Approver email from the **Tenant Settings** › **Approval Settings** page.

**To send email to root users**

You must be logged in as root. Open the root drop-down menu in the right corner of the ViPR Controller UI title bar, and select **Preferences**.

**To send email to provisioning users**

You must be logged in as the provisioning user. Open the user drop-down menu in the right corner of the ViPR Controller UI title bar, and select **Preferences**.