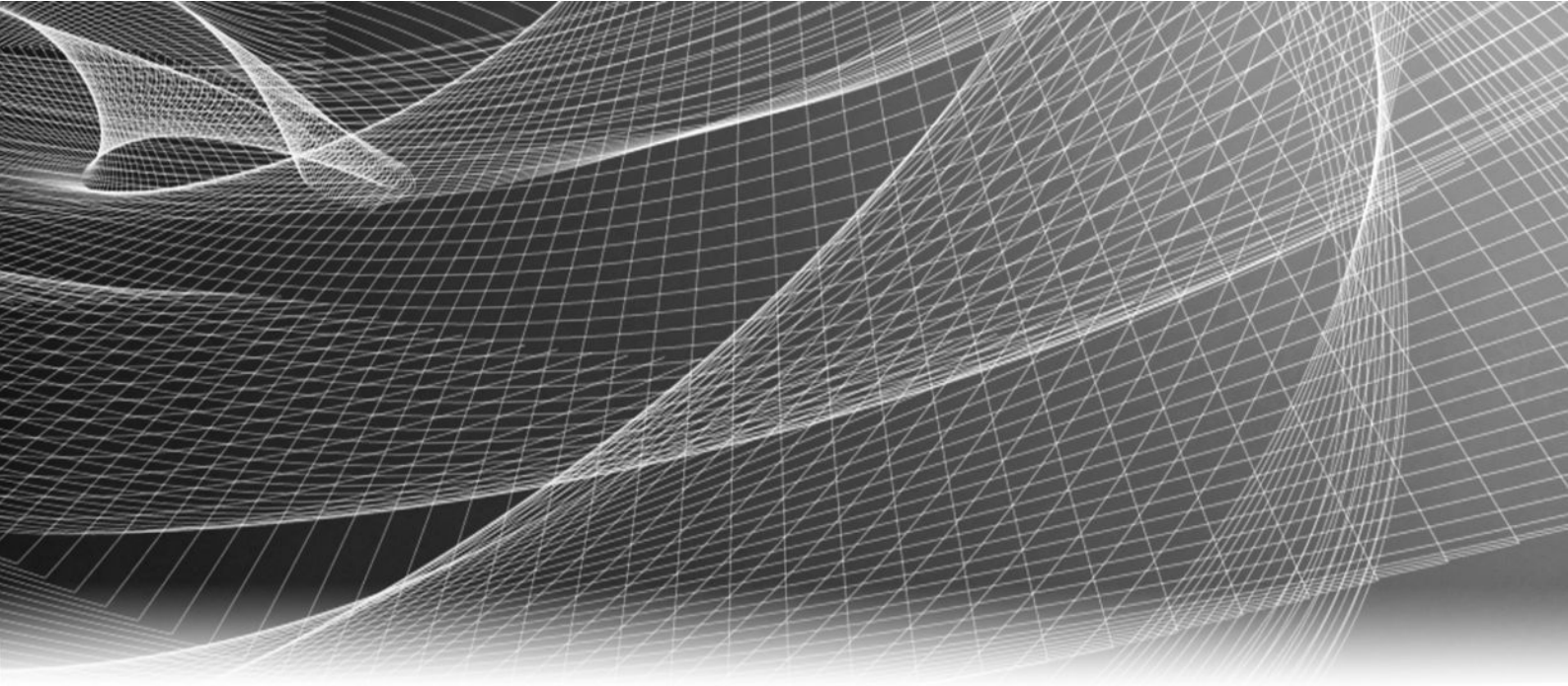

EMC ViPR Controller

Version 3.5

Installation, Upgrade, and Maintenance Guide

302-003-273

01

EMC²

Published October 2016

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.

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 5

Chapter 2 EMC ViPR Controller deployment readiness checklist 7

Chapter 3 Licensing Model 9

Chapter 4 Obtain the EMC ViPR Controller license file 11

Chapter 5 Deploying ViPR Controller 13

Deploying ViPR Controller VMware with a vApp 14
Deploying ViPR Controller on VMware without a vApp 17
Deploying ViPR Controller on Hyper-V 23
Deploy the ViPR Controller CLI 28
Install the ViPR Controller CLI 28
Authenticating with viprcli 32
Uninstall the ViPR Controller CLI 33
Deploy a compute image server 34
ViPR Controller network requirements for the compute image server 34
Deploying the compute image server 34
Add the compute image server in ViPR Controller 37

Chapter 6 ViPR Controller Log in, and User Role Requirements 39

Log in to EMC ViPR Controller 40
ViPR Controller user role requirements 40

Chapter 7 Upgrading ViPR Controller 45

Pre-upgrade planning 46
Configuring ViPR Controller for upgrade from an EMC-based repository 47
Configuring ViPR Controller for an upgrade from an internal location 48
Upgrade ViPR Controller 49
Add the Node ID property in VMware after upgrading the ViPR Controller vApp 50
Changing ScaleIO storage provider type and parameters after upgrading ViPR Controller 51
Upgrade the ViPR Controller CLI 51

Chapter 8 Managing the ViPR Controller Nodes 53

Avoid conflicts in EMC ViPR network virtual IP addresses 54
Change the IP address of EMC ViPR Controller node 54
Change the IP address of EMC ViPR Controller node deployed as a VMware vApp 54

Change the IP address of ViPR Controller node on VMware without vApp, or Hyper-V using ViPR Controller UI 55
Change the IP address of ViPR Controller node on VMware with no vApp using vCenter 56
Change the IP address of ViPR Controller node on Hyper-V using SCVMM 57
Changing the ViPR Controller node names 58
Changing the ViPR Controller node name from the UI 59
Changing the ViPR Controller node name from the CLI 60
Changing the ViPR Controller node name from the API 60
Operating System Configuration Files 61

Chapter 9 Modifying the ViPR Controller Footprint 63

Modify the ViPR Controller footprint on VMware 64
Modify the ViPR Controller footprint on Hyper-V 64

Appendix A Other ViPR Controller configuration options 67

ConnectEMC and ConnectIN 68
ViPR Controller email options 68
System Disaster Recovery Email Alerts 69
Audit Log 73
Forward all real-time log events to a remote Syslog server 73

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 11.
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 14
   - Install ViPR Controller on VMware without a vApp on page 17
   - Install ViPR Controller on Hyper-V on page 23
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 34
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 accurate NTP servers.
- Collect credentials to access the VMware or Hyper-V instance.
  Deploying ViPR Controller requires 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.
- If deploying on VMware, it is recommended to deploy the ViPR Controller on a minimal of a 3 node ESXi DRS cluster, and to set an anti-affinity rule among the ViPR Controller nodes to, "Separate Virtual Machines," on available ESXi nodes. Refer to VMware vSphere documentation for instructions to setup ESX/ESXi DRS anti-affinity rules.
- 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.
- 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
- The DNS servers configured for ViPR Controller deployment must be configured to perform both forward and reverse lookup for all devices that will be managed by ViPR Controller.
- Two or three NTP servers.
- ViPR Controller requires ICMP protocol is enabled for installation and normal usage.
- FTP/FTPS or CIFS/SMB server for storing ViPR Controller backups remotely. You need the URL of the server and credentials for an account with read and write privileges on

the 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

Licensing Model

Starting with ViPR Controller 3.0, a new licensing model was deployed.

Overview

Starting with Release 3.0, ViPR Controller implemented a new licensing model. The new model supports a new-format managed capacity license and a raw, usable, frame-based capacity license. With the raw capacity single license file, each license file can include multiple increments, both array-type and tiered.

The new licensing model is not compatible with the old-format managed capacity license used with older versions of ViPR Controller.

ViPR Controller 3.5 new installation

- For a fresh ViPR 3.5 installation with a new license, you should encounter no problem and may proceed normally.
- If you try to do a fresh ViPR 3.5 installation with an old license, you will receive an error message "Error 1013: License is not valid" and will not be able to proceed with the installation. You must open a Service Request (SR) ticket to obtain a new license file.

ViPR Controller 3.5 upgrade installation

- For an upgrade ViPR 3.5 installation with an old license, ViPR 3.5 will continue to use the old-format license, but the license will say "Legacy" when viewing the **Version and License** section of the **Dashboards** in the ViPR GUI. There is no automatic conversion to the new-format license. To convert to the new-format license, you must open a Service Request (SR) ticket to obtain a new license file. After you upload the new-format license, the GUI display will show "Licensed".

Pre-3.0 versions of ViPR Controller

- Pre 3.0 versions of ViPR controller will accept the new-format license file. However, they will only recognize the last increment in the new file.
- After you upgrade to Version 3.0 or greater, you will need to upload the new-format license again.

CHAPTER 4

Obtain the EMC ViPR Controller license file

EMC ViPR Controller supports a new-format managed capacity license and a raw, usable, frame-based capacity license. You need to obtain the license file (.lic) from the EMC license management web site for uploading to ViPR Controller.

Before you begin

Note

There is a new licensing model for EMC ViPR Controller Version 3.0 and above. For details, refer to the chapter "Licensing Model" in the *EMC ViPR Controller Installation, Upgrade, and Maintenance Guide*, which can be found on the ViPR Controller Product Documentation Index .

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

The license file is needed during initial setup of ViPR Controller, or when adding capacity to your existing ViPR Controller deployment. Initial setup steps are described in the deployment sections of this guide. If you are adding a ViPR Controller license to an existing deployment, follow these steps to obtain a license file.

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, distribute the controllers as appropriate to obtain individual license files for each virtual data center.

   For a System Disaster Recovery environment, you do NOT need extra licenses for Standby sites. The Active site license is shared between the sites.
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.

CHAPTER 5

Deploying ViPR Controller

The chapter includes the following topics:

- Deploying ViPR Controller VMware with a vApp 14
- Deploying ViPR Controller on VMware without a vApp 17
- Deploying ViPR Controller on Hyper-V 23
- Deploy the ViPR Controller CLI 28
- Deploy a compute image server 34

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

- To reserve a specific amount of memory for a VM, go to the Vsphere Client, **VM Properties** › **Resource** › **Memory "Reservation"**. Page 11 of the following VMWare guide has additional information:

  https://www.vmware.com/files/pdf/perf-vsphere-memory_management.pdf

- 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.

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

- To reserve a specific amount of memory for a VM, go to the Vsphere Client, **VM Properties** › **Resource** › **Memory "Reservation"**. Page 11 of the following VMWare guide has additional information:

  https://www.vmware.com/files/pdf/perf-vsphere-memory_management.pdf
- 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 the *EMC ViPR Controller System Disaster Recovery, Backup and Restore Guide*, which is available from the ViPR Controller Product Documentation Index .

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 escape special characters if any are used in 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 the *EMC ViPR Controller System Disaster Recovery, Backup and Restore Guide*, which is available from the ViPR Controller Product Documentation Index .
-interactive	Optional for install, and redeploy. 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. Number of nodes: 3 or 5 or 1 for evaluation installation only.
-vip	Required for install. Public virtual IPv4 address.
-ipaddrs_n	Required for install. Where "n" equals the IPv4 address list of each node for example, -ipaddrs_1, -ipaddrs_2... i-ipaddrs_5.
-netmask	Required for install. Network netmask.
-gateway	Required for install. IPv4 default gateway.
-vip6	Required for install if using IPv6. Public virtual IPv6 address.
-ipaddrs6_n	Required for install. 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. IPv6 default gateway.
-ipv6prefixlength	Optional for install if using IPv6. IPv6 address prefix length. Default is 64.
-nodeid	Required for install and redeploy. 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 . 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. The values of IP addresses for the -ipaddrs-n option must be the same each time.

Option	Description
	node 1: `.\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` node 2: `.\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` node 3: `.\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`
-net ***networkname***	Required for install and redeploy. Set a network assignment.
-file	Optional for install, required for redeploy. Valid path and name to the configuration settings file.
-vmprefix	Optional for install, and redeploy. Prefix of virtual machine name. You can use either -vmprefix, or -vmname, but not both.
-vmname	Optional for install, and redeploy. Name of the virtual machine. You can use either -vmprefix, or -vmname, but not both.
-poweron	Optional for install, and redeploy. 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. 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. If redeploying as part of minority node restore, do not power on until after you have started the node recovery as described in the *EMC ViPR Controller System Disaster Recovery, Backup and Restore Guide*, which is available from the ViPR Controller Product Documentation Index .

Option	Description
-cpucount	Optional for install, and redeploy. Number of CPUs for each virtual machine. Valid values are 2 - 16. 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. Memory size for each virtual machine. Valid values are 4096 - 16384MB. 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. Datastore name.
-vmfolder *folder*	Optional for install, and redeploy. Target VM folder in VI inventory.
-dm {thin | lazyzeroedthick | zeroedthick}	Optional for install, and redeploy. Disk format. Use thick for deployment in production environment. Default is zeroedthick.
-targeturi *target-uri*	Required for install, and redeploy. This is the Target locator of vSphere. The format is: *vi://vSphere client username:password@esxi_host_url* where the typical format for *esxi_host_uri*is: *esxi_host_uri is My-vcener-or-ESXi.example.com/datacenter-name/host/host-name/Resources/resource-pool* 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: *My-vcener-or-ESXi.example.com/ViPR-DataCenter/host/ViPR-Cluster/Resources/ViPR-Pool* 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: *vi://mydomain.com%5cmyuser1:password1@vcenter1.emc.com:443/My-Datacenter/host/ViPR-Cluster/Resources/ViPR-Pool* For details refer to the *VMware OVF Tool User Guide*.
-username	Optional for install, and redeploy. vSphere client user name.

Option	Description
	You do not need to escape special characters when entering the username at the interactive mode prompt.
-password	Optional for install, and redeploy. vSphere client password. You do not need to escape special characters when entering the username at the interactive mode prompt.

6. If redeploying a failed node, for the remaining steps refer to the *EMC ViPR Controller System Disaster Recovery, Backup and Restore Guide*, which is available from the ViPR Controller Product Documentation Index .

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

   You will need to enter the information required to install the first node, however, you will not need to enter all of 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.

   You will only need to change specific parameters for each subsequent node that you want to change, such as "node id", VM name, or target datastore.

   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 the: *EMC ViPR Controller System Disaster Recovery, Backup and Restore Guide*, which is available from the ViPR Controller Product Documentation Index .
-interactive	Optional for install, and redeploy. 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. Number of nodes: 3 or 5
-vip	Required for install. Public virtual IPv4 address.
-ipaddrs_n	Required for install. Where "n" equals the IPv4 address list of each node for example, -ipaddrs_1, -ipaddrs_2... i-ipaddrs_5.
-netmask	Required for install. Network netmask.

Option	Description
-gateway	Required for install. IPv4 default gateway.
-vip6	Required for install if using IPv6. Public virtual IPv6 address.
-ipaddrs6_n	Required for install. 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. IPv6 default gateway.
-ipv6prefixlength	Optional for install if using IPv6. IPv6 address prefix length. Default is 64.
-nodeid	Required for install and redeploy. 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 . 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. The order of IP addresses for the -ipaddrs_n option must be the same each time. node 1: `.\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` node 2: `.\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` node 3: `.\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`

Option	Description
	`-vlanid vlan_id -vmnameprefix vmprefix -cpucount 2 -memory 8192 -poweron`
-net *networkname*	Required for install and redeploy. Set a network assignment.
-file	Optional for install, required for redeploy. Valid path and name to the configuration settings file.
-vmprefix	Optional for install, and redeploy. Prefix of virtual machine name. You can use either -vmprefix, or -vmname, but not both.
-vmname	Optional for install, and redeploy. Name of the virtual machine. Enter a different value for each node i.e, vipr1, vipr2, vipr3, You can use either -vmprefix, or -vmname, but not both.
-poweron	Optional for install, and redeploy. 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. 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. If redeploying as part of minority node restore, do not power on until after you have started the node recovery as described in the *EMC ViPR Controller System Disaster Recovery, Backup and Restore Guide*, which is available from the ViPR Controller Product Documentation Index .
-cpucount	Optional for install, and redeploy. Number of CPUs for each virtual machine. Valid values are 2 - 16. 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. Memory size for each virtual machine. Valid values are 4096 - 16384MB. 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. Library path shared in SCVMM.
-vmhostname	Required for install, and redeploy. Host machine for the VM.
-vmpath	Required for install, and redeploy. VM Path in host machine Note: user needs to make sure it exists.

Option	Description
-vswitch	Required for install, and redeploy. Name of the virtual switch.
-disktype	Optional for install, and redeploy. 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. VLAN id. Default is -1.

5. If redeploying a failed node, for the remaining steps, refer to the *EMC ViPR Controller System Disaster Recovery, Backup and Restore Guide*, which is available from the ViPR Controller Product Documentation Index .

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

   You will need to retype 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 the ViPR Controller CLI

The EMC® ViPR® Command Line Interface (CLI) allows data center personnel to use ViPR Controller to manage storage resources. This section provides information on installing, upgrading, and uninstalling the CLI. For detailed information on the CLI, refer to the *ViPR Controller CLI Reference Guide*, which is available in the ViPR Controller Product Documentation Index .

Install the ViPR Controller CLI

The ViPR Controller CLI (viprcli) is installed, along with all the necessary support files, on each ViPR Controller virtual machine. For best results, install the viprcli on a standalone Linux or Windows machine.

A log file of the installation is created named, `install-log.txt`. The `install-log.txt` file is created in the directory where you install the CLI.

ViPR Controller CLI prerequisites

The ViPR Controller CLI can be installed on the following operating systems.

When installing the CLI, the required Python setuptools, Requests, and Argparse packages are downloaded and installed automatically if your installer has access to DNS server services and the internet. It is advisable to install the ViPR Controller CLI on a physical or virtual machine outside of the ViPR Controller cluster.

After installing the required Python packages, you will need to set up your local host, environment variables, with the path to your Python installation directory. Refer to Python documentation for complete details.

Table 1 Supported operating systems for the ViPR Controller CLI

Operating system	Supported versions	Additional software

Red Hat Enterprise Linux (RHEL)	6.x	• Python setuptools 7.0
		• Python 2.7.9
		  ▪ Python Requests package 2.8.1
		  ▪ Python Argparse package 1.2.1

SUSE Linux Enterprise Server	11 SP2, 11 SP3	• Python setuptools 7.0
		• Python 2.7.9
		  ▪ Python Requests package 2.8.1
		  ▪ Python Argparse package 1.2.1

Microsoft Windows	7, 8	• Python setuptools 7.0
		• Python 2.7.9
		  ▪ Python Requests package 2.8.1
		  ▪ Python Argparse package 1.2.1

Install the ViPR Controller CLI on Linux

You can install the ViPR Controller command line interface executable directly from ViPR Controller appliance onto a supported Linux host.

Before you begin

- You need access to the ViPR Controller appliance host.
- You need root access to the Linux host.
- The installer requires access to DNS server services and the internet. If your installer will not have access to these requirements, you must install the required Python packages manually before running the installer.

Procedure

1. Log in to the Linux server as root.
2. Create a temporary directory to download the CLI installer.

   ```
   mkdir cli/temp
   cd cli/temp
   ```

3. Either point your browser to `https://<FQDN>:4443/cli` or run the `wget` command to retrieve the ViPR Controller CLI installation bundle:

   ```
   wget https://<FQDN>:4443/cli
   ```

Note

For sites with self-signed certificates or where issues are detected, optionally use `http://<ViPR_Controller_VIP>:9998/cli` only when you are inside a trusted network. ‹ViPR_Controller_VIP› is the ViPR Controller public virtual IP address, also known as the network vip. The CLI installation bundle is downloaded to the current directory.

4. Use tar to extract the CLI and its support files from the installation bundle.

   ```
   tar -xvf <cli_install_bundle>
   ```

5. Run the CLI installation program.

   ```
   python setup.py install
   ```

6. Change directory to `/opt/storageos/cli` or to the directory where the CLI is installed.

7. **Note**

   Perform this step only when you have not provided the correct input in step 5.

   Edit the `viprcli.profile` file using the `vi` command and set the *VIPR_HOSTNAME* to the ViPR Controller public virtual IP address and `VIPR_PORT=4443` environment variable and save the file.

```
# vi viprcli.profile
#!/usr/bin/sh


# Installation directory of ViPR Controller CLI
ViPR Controller_CLI_INSTALL_DIR=/opt/storageos/cli

# Add the ViPR Controller install directory to the PATH and
PYTHONPATH env variables
if [ -n $ViPR Controller_CLI_INSTALL_DIR ]
then
        export PATH=$ViPR Controller_CLI_INSTALL_DIR/bin:$PATH
        export PYTHONPATH=$ViPR Controller_CLI_INSTALL_DIR/bin:
$PYTHONPATH
fi

# USER CONFIGURABLE ViPR Controller VARIABLES

# ViPR Controller Host fully qualified domain name
ViPR Controller_HOSTNAME=example.mydomain.com

# ViPR Controller Port Number
ViPR Controller_PORT=4443

:wq
```

8. Run the source command to set the path environment variable for the ViPR Controller executable.

   ```
   source ./viprcli.profile
   ```

9. From the command prompt run the **`viprcli -h`** command.

   If the help for viprcli is displayed, then the installation is successful.

10. Authenticate (log into) the ViPR Controller instance with the viprcli to confirm that your installation was successful.

See Authenticating with viprcli on page 32.

Install the ViPR Controller CLI on Windows

You can download and install the ViPR Controller command line interface executable directly from the ViPR Controller appliance onto a supported Windows host.

Before you begin

- You need access to the ViPR Controller appliance host.
- You need to be logged in to the Windows host as a user with administrator privileges.
- The installer requires access to DNS server services and the internet. If your installer will not have access to these requirements, you must install the required Python packages manually before running the installer.

Procedure

1. Log in to the Windows server as ‹admin user›.
2. Create a temporary directory to download the CLI installer. For example, `c:\cli\temp`
3. Point your browser to `https://<FQDN>:4443/cli`

   Note

   For sites with self-signed certificates or where issues are detected, optionally use `http://<ViPR_Controller_virtual_IP>:9998/cli` only when you are inside a trusted network. ‹ViPR_Controller_virtual_IP› is the ViPR Controller public virtual IP address, also known as the network vip.

   - If your browser prompts you to save the `ViPR-cli.tar.gz` file, save it to the temporary CLI installer directory that you created in step 2. For example, `c:\cli\temp`.
   - If your browser automatically downloads the `ViPR-cli.tar.gz` file, without giving you the opportunity to select a directory, then copy the downloaded `ViPR-cli.tar.gz` file to the temporary CLI installer directory that you created in step 2.

4. Open a command prompt and change to the directory you created in step 2, where you saved or copied the `ViPR-cli.tar.gz` file. This example will use `c:\cli\temp`.
5. Enter the python console by typing `python` at the command prompt:

```
c:\cli\temp>python
Python 2.7.3 (default, Apr 10 2012, 23:24:47) [MSC v.1500 64 bit
(AMD64)] on win
32
Type "help", "copyright", "credits" or "license" for more
information.
>>>
```

6. Using the `tarfile` module, open and extract the files from the `ViPR-cli.tar.gz` file.

```
>>> import tarfile
>>> tfile = tarfile.open("ViPR-cli.tar.gz", 'r:gz')
```

```
>>> tfile.extractall('.')
>>> exit()
```

7. Since you are already in the directory to which the files have been extracted, run the `python setup.py install` command. Follow the installation instructions and provide the required information.

   Note

   You can also enter `y` to select the defaults for the installation directory (`EMC\VIPR\cli`) and the port number (`4443`).

8. (Optional) If incorrect information was provided in the previous step, edit the `viprcli.profile.bat` file and set the following variables.

Variable	Value
SET VIPR_HOSTNAME	The ViPR Controller hostname, set to the fully qualified domain name (FQDN) of the ViPR Controller host, or the virtual IP address of your ViPR Controller configuration.
SET VIPR_PORT	The ViPR Controller port. The default value is 4443.

9. Change directories to the location where the viprcli was installed. The default is: `C:\EMC\ViPR\cli`.
10. Run the `viprcli.profile.bat` command.
11. Authenticate (log into) the ViPR Controller instance with the viprcli to confirm that your installation was successful.

    See Authenticating with viprcli on page 32.

Authenticating with viprcli

You must authenticate a user before any viprcli commands can be successfully executed.

Before you can authenticate, you must have configured your environment variable with the path to the Python installation directory. If you did not do set the environment variable prior to installing the CLI, you must do it now to use the ViPR Controller CLI.

Logging in to the ViPR Controller command line interface is different on `Windows` and `Linux` hosts.

When logging into the ViPR Controller, if you do not enter a host when authenticating, you will automatically log in to the ViPR Controller you provided during installation. If you want to log into a different ViPR instance, you can enter the host name as demonstrated below.

Authenticate on Windows

To log into the default ViPR Controller instance use:

```
C:/>
          viprcli authenticate -u root -d c:\tmp
```

To specify the ViPR Controller instance use:

```
C:/>
          viprcli -hostname <fqdn, or host ip> authenticate  -u root -
d c:\tmp
```

Do not end the directory path with a '\'. For example, `c:\tmp\`

Type the password when prompted.

Authenticate on Linux
To log into the default ViPR Controller instance use:

```
#
          viprcli authenticate -u root -d /tmp
```

To specify the ViPR Controller instance use:

```
#
          viprcli -hostname <fqdn, or host ip> authenticate -u root -
d /tmp
```

Type the password when prompted.

Note

The non-root users must have read, write, and execute permissions to use the CLI installed by root. However, they don't need all these permissions for installing and running the CLI in their home directory.

Uninstall the ViPR Controller CLI

You can uninstall the ViPR Controller command line interface (CLI) executable. The steps to uninstall the ViPR Controller CLI depend on whether you still have the original files that you used to install the CLI.

Before you begin

- You need access to the ViPR Controller appliance host.
- On a Linux host you need root access.
- On a Windows host you need administrator access.
- The uninstaller requires access to DNS server services and the internet. If your uninstaller will not have access to these requirements, you must install the required Python packages manually before running the uninstaller.

Procedure

1. Log in:
   - Linux server as root.
   - Windows server as ‹admin user›.
2. If you do not have the original files that you used to install the ViPR Controller CLI, then follow the steps to extract the CLI and its support files that are appropriate for your platform:
   - Steps 1 through 4 of Install the ViPR Controller CLI on Linux on page 29.
   - Steps 1 through 7 of Install the ViPR Controller CLI on Windows on page 31.
3. In the directory to which you extracted the CLI files, run the CLI uninstall program.

   ```
   python setup.py uninstall
   ```

4. When prompted, provide the directory where the CLI is installed, for example `/opt/storageos/cli`.

Deploy a compute image server

You can deploy a single or multiple compute image servers for each Vblock system you are adding to ViPR Controller.

For information about ViPR Controller support for a Vblock system, see the: *ViPR Controller Virtual Data Center Requirements and Information Guide*, 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 for each compute image server your are deploying 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. Use one fo the following methods each compute image server you are deploying in your environment.

- Deploying the ViPR Controller Compute Image Server OVF file on page 35
- Requirements to create a custom Compute Image Server for ViPR Controller on page 36

Once you have completed deployment of the compute image servers you will need to configure each compute image server with the steps described in

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 compute 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
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.

Add the compute image server in ViPR Controller

Once the compute image server is deployed, you must add and configure the connectivity for the compute image server in the ViPR Controller.

The compute image server can only be added and configured in ViPR Controller using the ViPR Controller REST API, or CLI. To use the ViPR Controller REST API, go to http://www.emc.com/techpubs/api/vipr/v3-5-0-0/index.htm. To use the ViPR Controller CLI see the *ViPR Controller CLI Reference Guide*. Both documents are available from the ViPR Controller Product Documentation Index .

CHAPTER 6

ViPR Controller Log in, and User Role Requirements

This chapter includes the following topics:

- Log in to EMC ViPR Controller 40
- ViPR Controller user role requirements 40

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.

ViPR Controller user role requirements

ViPR Controller roles fall into two groups: roles that exist at the ViPR Controller virtual data center level, and roles that exist at the tenant level.

Note

Access to different areas of the ViPR Controller UI is governed by the actions permitted to the role assigned to the user. The actions authorized when you access ViPR Controller from the UI can differ (be more constrained) from those available when you use the REST API or CLI.

Virtual data center-level roles

VDC roles are used to set up the ViPR Controller environment which is shared by all tenants. The following table lists the authorized actions for each user role at the virtual data center level.

Table 2 VDC roles

VDC Role	Authorized Actions
Security Administrator	• Manages the authentication provider configuration for the ViPR Controller virtual data center to identify and authenticate users. Authentication providers are configured to: ▪ Use Active Directory/Lightweight Directory Access Protocol (AD/LDAP) user accounts/domains to add specified users into ViPR Controller. ▪ Register ViPR Controller as block storage service in Openstack (Keystone).

Table 2 VDC roles (continued)

VDC Role	Authorized Actions
	Note Security Administrator role is required to add Keystone, but Keystone users cannot be added into ViPR Controller. • Creates ViPR Controller User Groups. • Assigns VDC and Tenant roles. • Sets ACL assignments for Projects, and Service Catalog. • Sets ACL assignments for virtual arrays, and virtual pools, from the ViPR Controller API and CLI. • Update vCenter Tenants (ACLs) and Datacenter Tenant from ViPR Controller REST API and CLI (Only System Administrators can perform any of these functions from the ViPR Controller UI). • Creates, modifies, and deletes sub-tenants. • Assigns the tenant quotas, and user mappings. • Manages ViPR Controller virtual data center software and license updates. • Configures the repository from which ViPR Controller upgrade files will be downloaded and installed. • Manages SSL, and trusted certificates. • Can change IPs for ViPR Controller nodes deployed on VMware without a vApp, and Hyper-V. • Schedule backups of ViPR Controller instances. • Reset local user passwords. • Configures ACLs. • Restores access to tenants and projects, if needed. (For example, if the Tenant Administrator locks himself/herself out, the Security Administrator can reset user roles to restore access.) • Can add or change ViPR Controller node names. • Initiate a minority node recovery from the ViPR Controller REST API, and CLI. • View the minority node recovery status from the ViPR Controller CLI. • Make changes to the ViPR Controller, General Configuration, Security settings. • Shuts down, reboots, and restarts ViPR Controller services from the ViPR Controller REST API/CLI. • Manages IPsec actions, such as rotate IPsec key, check IPsec status.
	The Security Administrator must also be assigned a System Administrator role to perform the following operations from the ViPR Controller UI: • Shut down, reboot, and restart ViPR Controller nodes or services. • Set ACL assignments for virtual arrays, and virtual pools. • Initiate a minority node recovery.

Table 2 VDC roles (continued)

VDC Role	Authorized Actions
	In Geo-federated Environment: • Has Security Administrator privileges on authentication providers, which are global resources.
System Administrator	• Performs system upgrades. • Creates system backups • Add ViPR Controller licenses. • Send support requests. • Add, edit, delete, disconnect, and reconnect virtual data centers (VDCs). • Sets up the physical storage infrastructure of the ViPR Controller virtual data center and configures the physical storage into two types of virtual resources: virtual arrays and virtual pools. Authorized actions include: ▪ Adding, modifying, and deleting the following physical storage resources into ViPR Controller such as storage systems, storage ports, and storage pools, data protections systems, fabric managers, networks, compute images, Vblock compute systems, and vCenters. **Note** System Administrators cannot add, delete, or modify hosts or clusters. ▪ Updating vCenter cascade tenancy and vCenter tenants (ACLs) and Datacenter Tenant from the ViPR Controller REST API, UI and CLI. ▪ Associate a vNAS server to one or more projects (Requires both the System and Tenant Administrator roles). ▪ Creating virtual pools. ▪ Creating virtual arrays. ▪ Creating mobility groups. • Manages the ViPR Controller virtual data center resources that tenants do not manage. • Retrieves ViPR Controller virtual data center status and health information. • Retrieves bulk event and statistical records for the ViPR Controller virtual data center. • View the Database Housekeeping Status. • View the minority node recovery status from the ViPR Controller CLI.
	In Geo-federated Environment: • Adds a VDC to create Geo-federated environment • Add, disconnect, reconnect, or delete a VDC • Has System Administrator privileges on global virtual pools, which are global resources. • Sets ACL assignments for virtual arrays, and virtual pools, from the ViPR Controller API

Table 2 VDC roles (continued)

VDC Role	Authorized Actions
System Monitor	• Has read-only access to all resources in the ViPR Controller virtual data center. Has no visibility into security-related resources, such as authentication providers, ACLs, and role assignments. • Retrieves bulk event and statistical records for the ViPR Controller virtual data center. • Retrieves ViPR Controller virtual data center status and health information. • (API only) Can create an alert event, with error logs attached, as an aid to troubleshooting. The alert event is sent to ConnectEMC. • View the Database Housekeeping Status. • View the minority node recovery status from the ViPR Controller UI, and CLI. • List backups from external server. • Check upload status of a backup. • Check restore status.
System Auditor	Has read-only access to the ViPR Controller virtual data center audit logs.

Tenant-level roles

Tenant roles are used to administrate the tenant-specific settings, such as the service catalog and projects, and to assign additional users to tenant roles. The following table lists the authorized actions for each user role at the tenant level.

Table 3 Tenant roles

Tenant-Level Role	Authorized Actions
Tenant Administrator	• Becomes Tenant Administrator of created tenant. • A single-tenant enterprise private cloud environment has only one tenant, the Provider Tenant, and Tenant Administrators have access to all projects. • Modifies the name and description of the tenants. • Add vCenters to ViPR Controller physical assets in their own tenant. • Manages tenant resources, such as Hosts, Clusters vCenters, and Projects. • Configures ACLs for projects and the Service Catalog in their tenant. • Assigns roles to tenant users. (Can assign Tenant Administrator or Project Administrator roles to other users.) • Create Schedule Policies. • Associate a vNAS server to one or more projects (Requires both the System and Tenant Administrator roles). • Manage application services. • Accept or decline actionable events • Edit service order schedules.

Table 3 Tenant roles (continued)

Tenant-Level Role	Authorized Actions
	Note A user or group of users can be configured to have a Tenant Administrator role for Multiple Tenants. This user/group of users must belong to the Provider Tenant. However, they do not have to have the Tenant Administrator role in the provider tenant. This functionality can be used in multi-tenant environments in cases where a group of users needs to perform provisioning operations for multiple tenants and they do not want to use root user for these operations.
	In Geo-federated Environment: • Has Tenant Administrator privileges on tenants, which are global resources.
Tenant Approver	• Approves or rejects Service Catalog orders in their tenant. • Views all approval requests in their tenant.
Project Administrator	• Creates projects in their tenant and obtains an `OWN` ACL on the created project.

CHAPTER 7

Upgrading ViPR Controller

This chapter includes the following topics:

- Pre-upgrade planning 46
- Upgrade ViPR Controller 49
- Add the Node ID property in VMware after upgrading the ViPR Controller vApp 50
- Changing ScaleIO storage provider type and parameters after upgrading ViPR Controller 51
- Upgrade the ViPR Controller CLI 51

Pre-upgrade planning

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

- The minimum base version for upgrade to ViPR Controller 3.5 is version 2.3. If you want to upgrade from version 2.1.x, or earlier or version 2.2, you should first follow the upgrade guide from those releases.
- For supported upgrade paths, and most recent environment and system requirements, see The EMC ViPR Controller Release Notes, which are available from the ViPR Controller Product Documentation Index .
- To ensure your environment is compliant with the latest support matrix, review the ViPR Controller Support Matrix.
- Determine if you will be upgrading from an EMC-based repository, or from an internal location by first downloading the ViPR Controller installation files.
  - If upgrading from an EMC-based repository, configure the ViPR Controller to point to the EMC-based repository as described in: Configuring ViPR Controller for upgrade from an EMC-based repository on page 47.
  - If your site cannot access the EMC repository, and you will be installing from an internal location refer to Configuring ViPR Controller for an upgrade from an internal location on page 48.
- Verify that the ViPR Controller status is **Stable** from the ViPR Controller UI **System** › **Dashboard**.
- 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.
  - Also, make sure that the ports that are used for IPSec in ViPR Controller 3.5 are open (not blocked by a firewall) in the customer environment between the datacenters.
- Before upgrading, make a backup of the ViPR Controller internal databases using a supported backup method so that in the unlikely event of a failure, you will be able to restore to the previous instance. Refer to the version of ViPR Controller backup documentation that matches the version of ViPR Controller you are backing up. For ViPR Controller versions 2.4 and later, backup information is provided in the *EMC ViPR Controller Disaster Recovery, Backup and Restore Guide*. For earlier versions, backup information is provided in the *EMC ViPR Controller Installation, Upgrade, and Maintenance Guide*.
- Prepare for the ViPR Controller virtual appliance to be unavailable for provisioning operations for 6 minutes plus approximately 1 minute for every 10,000 file shares, volumes, block mirrors, and block snapshots in the ViPR Controller database. System Management operations will be unavailable for a period of 8 minutes (for a 2+1 Controller node deployment) or 12 minutes (for a 3+2 Controller node deployment) plus approximately 1 minute for every 10,000 file shares, volumes, block mirrors, and block snapshots in the ViPR Controller database.

- Verify that all ViPR Controller orders have completed before you start the upgrade.
- If RecoverPoint is used, upgrade RecoverPoint to a version supported by ViPR Controller 3.5, before upgrading ViPR Controller itself. Refer to the EMC ViPR Support Matrix for supported RecoverPoint versions.
- If your ViPR Controller is managing EMC ScaleIO storage, upgrade EMC ScaleIO to a version supported by ViPR Controller 3.5, before upgrading ViPR Controller itself. As part of the EMC ScaleIO upgrade, you must install the ScaleIO Gateway. Refer to the EMC ViPR Support Matrix for supported EMC ScaleIO versions.
- Prior to upgrading ViPR Controller to version 3.5, refer to the EMC ViPR Support Matrix for SMI-S versions supported for ViPR Controller 3.5 for VMAX, and VNX for Block storage systems. If upgrading the SMI-S is required:
  - When upgrading an SMI-S provider to meet the ViPR Controller requirements, you must upgrade ViPR Controller first, and then the SMI-S provider.
  - If you are required to upgrade the SMI-S provider from 4.6.2 to 8.x, you must contact EMC Customer Support prior to upgrading ViPR Controller or the SMI-S provider.

  Note

  Use SMI-S provider documentation to upgrade from 8.0.3 to 8.1 or 8.2.
- Verify that XtremIO folder names exactly match the ViPR Controller project names. If there are differences, update the XtremIO folder name to exactly match the ViPR Controller project name.

  Note

  ViPR Controller does not support spaces in project names, therefore, spaces are not supported on XtremIO folder names.

Configuring ViPR Controller for upgrade from an EMC-based repository

If you want to download the latest version of ViPR Controller for an upgrade, ViPR Controller is configured by default to point to the EMC ViPR Controller repository. If you have changed that setting on your system, you must first reconfigure the ViPR Controller to point to the EMC ViPR Controller repository.

Before you begin

- For the ViPR Controller user roles required to perform this operation see ViPR Controller user role requirements on page 40.
- If your site cannot access the EMC repository, an alternative method of upgrade, for dark sites, is described in Configuring ViPR Controller for an upgrade from an internal location on page 48.

Following are the steps to configure the ViPR Controller for upgrade from an EMC-based repository from the ViPR Controller UI.

Procedure

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

Option	Description
Repository URL	URL to the EMC upgrade repository. One value only. Default value is https://colu.emc.com/soap/rpc.
Proxy	HTTP/HTTPS proxy required to access the EMC upgrade repository. Leave empty if no proxy is required.
Username	Username to access EMC Online Support.
Password	Password to access EMC Online Support.
Check Frequency	Number of hours between checks for new upgrade versions.

3. Click **Save**.

After you finish

Use the following command to configure the ViPR Controller for an upgrade from an EMC-based repository using the ViPR Controller CLI:

```
# viprcli system install-image vipr-3.5.0.x.x -hostname
<vipr_ip_address>
```

Note

If you have modified the `viprcli.profile` file appropriately, you do not need to append `-hostname <vipr_ip_address>` to the command.

For complete details refer to the *ViPR Controller CLI Reference Guide* which is available from the ViPR Controller Product Documentation Index .

Configuring ViPR Controller for an upgrade from an internal location

You can upgrade ViPR Controller 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

- Only ViPR Controller System Administrators can perform this operation.
- You need credentials to access EMC Online Support.

Procedure

1. Download the ViPR Controller Offline Upgrade img file from EMC Online Support and save it locally on the system where you are running the viprcli.
2. Authenticate with ViPR Controller CLI:

```
viprcli authenticate -u username -d /tmp -hostname
<vipr_ip_address>
```

Note

If you have modified the `viprcli.profile` file appropriately, you do not need to append `-hostname <vipr_ip_address>` to the command.

For complete details refer to the *ViPR Controller CLI Reference Guide* which is available from the ViPR Controller Product Documentation Index .

Enter the username password.

Upon successful authentication with above command , a cookie file is created in `/tmp` and subsequent viprcli commands can be executed without explicit authentication for each one.

3. Enter the following to upload the image file to a location on the ViPR Controller virtual appliance where it will be found by ViPR Controller to upgrade:

```
viprcli system upload -imagefile locally_saved_img
```

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

4. Proceed to the next section to upgrade to the new version.

Upgrade ViPR Controller

ViPR Controller can be upgraded using the ViPR Controller UI or CLI.

Before you begin

- For the ViPR Controller user roles required to perform this operation see ViPR Controller user role requirements on page 40.
- Review to the Pre-upgrade planning steps on page 46.
- The Security Administrator must have configured ViPR Controller with access to the upgrade files. Refer to one of the following for more information:
  - Configuring ViPR Controller for upgrade from an EMC-based repository on page 47
  - ConfiguringViPR Controller for an upgrade from an internal location on page 48

The following are the steps to upgrade ViPR Controller using the ViPR Controller UI.

Procedure

1. From the ViPR Controller UI, select **Settings** › **Upgrade**.
2. Optionally,
   a. Click **Add Backup** to create a point-in-time backup of your ViPR Controller instance.
   b. Click **Check DB** to validate if your ViPR Controller database is in a consistent state.
3. Select the version and click **Download**.

   The downloaded software is stored on the ViPR Controller VM.
4. Click **Install** next to the version you downloaded in step 3.

   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.
5. If you are upgrading on a ViPR Controller instance that was deployed as a VMware vApp, then continue to add the Node ID property as described in Add the Node ID property in VMware after upgrading the ViPR Controller vApp on page 50.

After you finish

To upgrade ViPR Controller from the ViPR Controller CLI use the following command:

```
# viprcli system update-cluster -v vipr-3.5.x.x.x
```

For complete details refer to the *ViPR Controller CLI Reference Guide* which is available from the ViPR Controller Product Documentation Index .

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**.
- After upgrading to version 2.4 or higher, any array with meta volumes need to be rediscovered, before you attempt to ingest those meta volumes.
- After upgrading to version 2.4 or higher, rediscover your RecoverPoint Data Protection Systems. This refreshes ViPR Controller's system information and avoids inconsistencies when applying RecoverPoint protection with ViPR Controller 2.4 or higher.

Add the Node ID property in VMware after upgrading the ViPR Controller vApp

If you have deployed ViPR Controller on VMware with a vApp, and you are upgrading from ViPR Controller versions 2.3.x or lower, then you will need to add the node_id property in VMware after upgrading to ViPR Controller 2.4 or higher. You do not have to perform this action if this is a new installation, and not an upgrade.

Note

Failure to perform this operation after upgrade from ViPR Controller versions 2.3.x or earlier will cause ViPR Controller operational failures if, at any time, you use vSphere to rename the original ViPR Controller vApp nodes names.

Procedure

1. From the VMware vSphere, power off the ViPR Controller vApp.
2. Right click on the first virtual machine in the ViPR Controller vApp, and choose **Edit Settings**.
3. Go to the **Options** › **vApp Options** › **Advanced** menu.
4. Open the **Properties**, and create a new property with the following settings:
   - Enter a **Label**, optionally name it Node ID.
   - Leave the **Class ID** empty.
   - Enter "node_id" for the **ID**. The name "node_id" is required for the id name, and cannot be modified.
   - Leave the **Instance ID** empty.
   - Optionally enter a **Description** of the ViPR Controller node.
   - Type: string.
   - Enter the **Default value**, which must be the node id set by ViPR Controller during deployment for example, vipr1, for the first ViPR Controller node, vipr2 for the second ViPR Controller node.

ViPR Controller values for a 3 node deployment are vipr1, vipr2, vipr3, and for a 5 node deployment are vipr1, vipr2, vipr3, vipr4, and vipr5.

- Check **User Configurable**.

5. Repeat steps 2 through 4 for each virtual machine deployed with the ViPR Controller vApp.
6. Power on the ViPR Controller vApp.

Changing ScaleIO storage provider type and parameters after upgrading ViPR Controller

If you discovered ScaleIO storage in a previous ViPR Controller release, you must update the storage provider associated with the ScaleIO storage and rediscover the associated storage systems. You do not have to perform this action if this is a new installation, and not an upgrade.

Before you begin

- EMC ScaleIO has been upgraded to a release supported by ViPR Controller 2.4.
- The ScaleIO Gateway has been installed.

These steps use the ViPR Controller UI. But you can also use the ViPR Controller UI REST API or CLI to update the storage provider parameters and rediscover the associated storage systems.

Procedure

1. Navigate to **Pysical Assets** › **Storage Providers**.
2. Select the ScaleIO storage provider.

   The **Edit Storage Provider** screen appears.
3. Change **Type** to `ScaleIO Gateway`.
4. Change **Host** to the FQDN or IP Address of the ScaleIO Gateway host.
5. Change **Port** to the port used to communicate with the ScaleIO REST API service .
   - With SSL enabled, the default is `443`.
   - With SSL disabled, the default is `80`.
6. Select **Save**.
7. Navigate to **Pysical Assets** › **Storage Systems**.
8. For each of the storage systems associated with the updated ScaleIO storage provider:
   a. Select the ScaleIO storage system.
   b. Click **Rediscover**.

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 Deploy the ViPR Controller CLI on page 28.

CHAPTER 8

Managing the ViPR Controller Nodes

This chapter includes the following topics:

- Avoid conflicts in EMC ViPR network virtual IP addresses 54
- Change the IP address of EMC ViPR Controller node 54
- Changing the ViPR Controller node names 58
- Operating System Configuration Files 61

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 without a vApp, do not follow this procedure.

The ViPR Controller vApp must not be part of a multi-VDC or System Disaster Recovery configuration:

- To check for a multi-VDC environment, go to **Virtual** › **Virtual Data Centers**; there should only be one VDC listed.
- To check for a System Disaster Recovery environment, go to **System** › **System Disaster Recovery**; there should only be an Active site listed, and no Standby sites.

Procedure

1. From the ViPR Controller UI, shutdown all VMs (**System** › **Health** › **Shutdown All**).
2. Open a vSphere client on the vCenter Server that hosts the ViPR Controller vApp.
3. Right-click the ViPR vApp whose IP address you want to change and select **Edit Settings**.
4. Click **Properties** and 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 Controller 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 Security Administrator role in ViPR Controller.

The ViPR Controller instance must not be part of a multi-VDC or System Disaster Recovery configuration:

- To check for a multi-VDC environment, go to **Virtual** › **Virtual Data Centers**; there should only be one VDC listed.
- To check for a System Disaster Recovery environment, go to **System** › **System Disaster Recovery**; there should only be an Active site listed, and no Standby sites.

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 the EMC ViPR Controller node on VMware deployed as vApp on page 57.

For the ViPR Controller user roles required to perform this operation see ViPR Controller user role requirements on page 40.

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

The ViPR Controller instance must not be part of a multi-VDC or System Disaster Recovery configuration:

- To check for a multi-VDC environment, go to **Virtual** › **Virtual Data Centers**; there should only be one VDC listed.
- To check for a System Disaster Recovery environment, go to **System** › **System Disaster Recovery**; there should only be an Active site listed, and no Standby sites.

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 addresses for all nodes that need to change in the appropriate fields and click **Next.**

You will only need to type new IP addresses in one node, and then accept new configuration on subsequent nodes in steps 12-13.

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 using SCVMM in the event that the ViPR Controller UI was unavailable to change the IP addresses..

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 Controller instance must not be part of a multi-VDC or System Disaster Recovery configuration:

- To check for a multi-VDC environment, go to **Virtual › Virtual Data Centers**; there should only be one VDC listed.
- To check for a System Disaster Recovery environment, go to **System › System Disaster Recovery**; there should only be an Active site listed, and no Standby sites.

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 addresses for all nodes that need to change in the appropriate fields and click **Next.**

   You will only need to type new IP addresses in one node, and then accept new configuration on subsequent nodes in steps 12-13.
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.

Changing the ViPR Controller node names

After installing ViPR Controller on VMware with a vApp, VMware without a vApp, or on Hyper-V, you can provide custom names to the ViPR Controller nodes using the ViPR Controller UI, REST API, or CLI. The custom node names allow you to easily identify the nodes in the ViPR Controller UI, REST API, and ViPR Controller logs. The custom node names can also be used to SSH between the ViPR Controller nodes.

By default ViPR Controller is installed with the following node IDs, which are also the default node names:

Number of Nodes	Node ID and default Node Names
3 nodes	vipr1, vipr2, vipr3
5 nodes	vipr1, vipr2, vipr3, vipr4, vipr5

During initial deployment, the default names are assigned to the nodes in ViPR Controller, vSphere for VMware installations, and SCVMM for Hyper-V installations.

Note

Node ids cannot be changed. Only the node names can be changed.

Before you begin

- For the ViPR Controller user roles required to perform this operation see ViPR Controller user role requirements on page 40.
- Host names in the DNS entries do not need to match the ViPR Controller VM names, or "Custom Node Names" defined in ViPR Controller.
- When the ViPR Controller node names are changed from the ViPR Controller, the node names are not changed in vSphere, or SCVMM. If you want the ViPR Controller node names to be the same in ViPR Controller and vSphere, or Hyper-V, you will need to go into vSphere for VMware installations, or SCVMM for Hyper-V installations, and manually change the node name to match the name you provided in ViPR Controller.

  Note

  Alternatively, if you change the ViPR Controller node names in vSphere or SCVMM, they are not changed in the ViPR Controller. If you want the node names to mach, you will need to manually change the node names in ViPR Controller to match the changes made in vSphere or SCVMM.

- Use the following naming conventions for the node name:
  - Use only characters 0-9, a-z, and '-'
  - Maximum number of characters is 253
  - If using FQDN for the node name:
    - No labels can be empty
    - Each label can have a maximum of 63 chars
  - Each custom node name must be unique
  - If you will be using custom short names, each custom short name must be unique The short node name can be used for API query parameters and SSH between nodes. The short node name is the name that comes before the first period of the fully node name for example the short name for myhost.test.companyname.com is “myhost.”
  - Do not use the node id for another node in the custom node name for example, do not use vipr1.test.companyname.com for the vipr2 node name.
- Whether you change the node name or not, if you have deployed ViPR Controller on VMware with a vApp, and you are upgrading from ViPR Controller versions 2.3.x or lower, then you will need to add the node_id property in VMware after upgrading to ViPR Controller 2.4 or higher, as described in Add the Node ID property in VMware after upgrading the ViPR Controller vApp on page 50. You do not have to perform this action if this is a new installation and not an upgrade

Changing the ViPR Controller node name from the UI

To change the ViPR Controller node name from the UI:

Procedure

1. From the ViPR Controller UI, go to the **Settings** › **General Configuraiton** › **Custom Node Names** tab.
2. Enter a name for each of the nodes.

3. Choose **True** to enable ViPR Controller to use the short node name.
4. Click **Save**.

   The ViPR Controller instance will automatically restart to apply the changes.

Changing the ViPR Controller node name from the CLI

ViPR Controller node names can be changed from the ViPR Controller CLI as follows.

1. Create a file with list of properties for the new ViPR Controller names, and optionally short name property to enable the use of the short node name. The following example is for a 5 node deployment.

   ```
   # cat nodenames-file.txt

   node_1_name=mynode1.domain.com
   node_2_name=mynode2.domain.com
   node_3_name=mynode3.domain.com
   node_4_name=mynode4.domain.com
   node_5_name=mynode5.domain.com
   use_short_node_name=true
   ```

   Where the node_n_name, sets the node name for the associated ViPR Controller Node ID for example:

   - The value for node_1_name will replace the node name for vipr1
   - The value for node_2_name will replace the node name for vipr2
   - The value for node_3_name will replace the node name for vipr3
   - The value for node_4_name will replace the node name for vipr4
   - The value for node_5_name will replace the node name for vipr5

   You can change the node names for as many number of nodes that are deployed either 3 node, or 5 node deployment.
2. Run the CLI command to update properties, and pass the file as an argument:

   ```
   ./viprcli system set-properties -pf /<path>/nodenames-file.txt
   ```

Changing the ViPR Controller node name from the API

ViPR Controller node names can be changed from the ViPR Controller REST API using:

```
PUT https://ViPR_Controller_VIP:4443/config/properties/
<property_update>
  <properties>
    <entry>
      <key>node_1_name</key>
      <value>mynode1.domain.com</value>
    </entry>
    <entry>
      <key>node_2_name</key>
      <value>mynode2.domain.com</value>
    </entry>
    <entry>
      <key>node_3_name</key>
      <value>mynode3.domain.com</value>
    </entry>
            <entry>
      <key>node_4_name</key>
      <value>mynode4.domain.com</value>
    </entry>
            <entry>
```

```
      <key>node_5_name</key>
      <value>mynode5.domain.com</value>
    </entry>
    <entry>
      <key> use_short_node_name </key>
      <value>true</value>
    </entry>
  </properties>
</property_update>
```

Where the node name key, sets the node name for the associated ViPR Controller Node ID for example:

- The value for node_1_name will replace the node name for vipr1
- The value for node_2_name will replace the node name for vipr2
- The value for node_3_name will replace the node name for vipr3
- The value for node_4_name will replace the node name for vipr4
- The value for node_5_name will replace the node name for vipr5

You can change the node names for as many number of nodes that are deployed either 3 node, or 5 node deployment.

For more details about using the ViPR Controller REST API, see the ViPR Controller REST API Reference .

Operating System Configuration Files

If you make manual changes to Operating System configuration files, the changes will be lost after a system reboot.

CHAPTER 9

Modifying the ViPR Controller Footprint

This chapter includes the following topics:

- Modify the ViPR Controller footprint on VMware 64
- Modify the ViPR Controller footprint on Hyper-V 64

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

- ConnectEMC and ConnectIN 68
- ViPR Controller email options 68
- System Disaster Recovery Email Alerts 69
- Add a ViPR Controller license 70
- Submitting a support request 71
- View and download ViPR Controller System logs and alerts 71
- Audit Log 73
- Forward all real-time log events to a remote Syslog server 73

ConnectEMC and ConnectIN

ConnectEMC is used to send data to EMC Support. ConnectIN is used by EMC Support to interact with your ViPR Controller instance.

ConnectEMC provides a means for ViPR Controller to send data to EMC support. You can 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. "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.)

The following table provides details on the event notifications sent out by ConnectEMC.

Event	Code	Frequency	Attachments
Heartbeat	101	Once every 30 days	Two attachments: • XML attachment with ConnectEMC needed data • Properties
Registration	100	When license is added or updated	Two attachments: • XML attachment with ConnectEMC needed data • Properties
Support request	999	On demand	Four attachments: • XML attachment with ConnectEMC configuration data • Properties • System events • Logs

ConnectIN is used by EMC Support to interact with ViPR Controller. ConnectIN uses the ESRS protocol for communications. ConnectIN functionality is generic and does not require configuration in ViPR Controller. After you register ViPR Controller, EMC engineers will be able to establish an ESRS tunnel to your ViPR Controller instance and start an SSH or UI session.

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**.

System Disaster Recovery Email Alerts

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

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

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

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

Example 1:

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

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

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

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

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

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

Thank you, ViPR

Example 2:

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

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

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

Subject: `ATTENTION - standby 10.247.98.73 is degraded`

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

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

Thank you, ViPR

Add a ViPR Controller license

Use the following steps to add a ViPR Controller license file.

Before you begin

For the ViPR Controller user roles required to perform this operation see ViPR Controller user role requirements on page 40.

Procedure

1. Obtain the ViPR Controller license file, and download it to a directory on your local host, as described in Obtain the EMC ViPR Controller license file on page 11.
2. Login to the ViPR Controller UI.
3. Select **Settings** › **License**.

4. In the **License File** field, click **Browse** and select the license file that was saved to your local host.
5. Click **Upload License File**.

Submitting a support request

You can send a support request to ConnectEMC. A support request consists of the text comments that you enter in the ViPR Controller UI **System** › **Support Request** page, and the system logs for the range of time that you specify.

Before you begin

- In a System Disaster Recovery environment, a support request can be submitted only for the currently Active site. To determine the currently Active site, go to **System** › **System Disaster Recovery**; the Active site is listed, along with any Standby site(s).
- For the ViPR Controller user roles required to perform this operation see ViPR Controller user role requirements on page 40.
- The ConnectEMC and email must already be configured (**General Configuration** › **ConnectEMC**) .
- A logs archive is automatically sent via ConnectEMC when a support request is submitted. However, the ConnectEMC logs are restricted to 16MB. If you want to analyze more than 16MB of log files you should use the download mechanism described in View and download ViPR Controller System logs and alerts on page 71.

Procedure

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

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

5. **Send**.

View and download ViPR Controller System logs and alerts

You can access log messages associated with each of the EMC ViPR Controller services and access to system events (alerts) through the **System** › **Logs** page.

Note

System logs and alerts are site-specific. In a System Disaster Recovery environment, logs can be viewed and collected separately on the Active site and the Standby site(s) .

Each ViPR Controller service on each virtual machine logs messages at an appropriate level (INFO, DEBUG, WARN and ERROR) and the service logs can be viewed when a

problem is suspected. However, the log messages may not provide information that can be acted on by a System Administrator, and may need to be referred to EMC.

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

Download ViPR Controller System logs

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

1. From the ViPR Controller UI go to the **System** › **Logs** page.
2. Click **Download** and specify the content that will be packaged in the zip file containing the logs.

A logs archive (.zip) file called `logs-<date>-<time>.zip` will be downloaded. The logs archive contains all log, system configuration, and order information. You can identify the service log file for a specific node in the zip file, by the log file name. The .log files are named as follows: `servicename_nodeid_nodename.log` for example:

- `apisvc.vipr1.mynodename.log` is a log file of the API service operations run on the first node of a ViPR Controller. mynodename.log is the custom node name provided by the user.

If a custom node name was not provided, then the node id will also be in the place of the node name for example:

- `apisvc.vipr1.vipr1.log`.

System Logs Table

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

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

In addition, the logs can be downloaded as a zip so that they can be reviewed offline, or shared with EMC Support.

System Logs Summary

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

Filter Control

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

Audit Log

The **System › Audit Log** page displays the recorded activities performed by administrative users for a defined period of time.

The Audit Log table displays the Time at which the activity occurred, the Service Type (for example, vdc or tenant), the User who performed the activity, the Result of the operation, and a Description of the operation.

Filtering the Audit Log Display

1. Select **System › Audit Log**. The Audit Log table defaults to displaying activities from the current hour on the current day and with a Result Status of ALL STATUS (both SUCCESS and FAILURE) .
2. To filter the Audit Log table, click **Filter**.
3. In the **Filter System Logs** dialog box, you can specify the following filters:
   - **Result Status**: Specify ALL STATUS (the default), SUCCESS, or FAILURE.
   - **Start Time**: To display the audit log for a longer time span, use the calendar control to select the **Date** from which you want to see the logs, and use the **Hour** control to select the hour of day from which you want to display the audit log.
   - **Service Type**: Specify a Service Type (for example, vdc or tenant).
   - **User**: Specify the user who performed the activity.
   - **Keyword**: Specify a keyword term to filter the Audit Log even further.
4. Select **Update** to display the filtered Audit Log.

Downloading Audit Logs

1. Select **System › Audit Log**. The Audit Log table defaults to displaying activities from the current hour on the current day and with a Result Status of ALL STATUS (both SUCCESS and FAILURE) .
2. To download audit logs, click **Download**.
3. In the **Download System Logs** dialog box, you can specify the following filters:
   - **Result Status**: Specify ALL STATUS (the default), SUCCESS, or FAILURE.
   - **Start Time**: Use the calendar control to select the **Date** from which you want to see the logs, and use the **Hour** control to select the hour of day from which you want to display the audit log.
   - **End Time**: Use the calendar control to select the **Date** to which you want to see the logs, and use the **Hour** control to select the hour of day to which you want to display the audit log. Check **Current Time** to use the current time of day.
   - **Service Type**: Specify a Service Type (for example, vdc or tenant).
   - **User**: Specify the user who performed the activity.
   - **Keyword**: Specify a keyword term to filter the downloaded system logs even further.
4. Select **Download** to download the system logs to your system as a zip file.

Forward all real-time log events to a remote Syslog server

This feature allows the forwarding and consolidation of all real-time log events to one or more common, configured, remote Syslog server(s), and will help the user to analyze the

log events. All logs from all ViPR services except Nginx (for example, syssvc, apisvc, dbsvc, etc.) are forwarded in real time to the remote Syslog server after successful configuration. Audit logs are also forwarded.

Before you begin

Procedure

1. **Configure Syslog Server to accept messages from remote hosts:**

   Note

   Follow the steps for your protocol.

   Configure Syslog server to accept messages via TLS protocol:

1. On the remote Syslog server, create certificates in the `/data` folder. The output will be `server.crt` and `server.key`.
   a. `openssl genrsa -des3 -out server.key 1024`

      Enter a passphrase.

   b. `openssl req -new -key server.key -out server.csr`

      Provide the passphrase from step 1-a. Provide information for the prompts.

   c. `cp server.key server.key.org`

   d. `openssl rsa -in server.key.org -out server.key`

      Provide the passphrase from step 1-a.

   e. `openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt`

      The certificate will expire in 365 days.
2. On the ViPR Controller server, download the certificate chain.
   a. Select **Virtual › Virtual Data Centers**.
   b. Click **Download Certificate Chain**.
   c. Copy the certificate to the remote Syslog server `/data` folder. For example, `/data/2021.crt`.
3. On the remote Syslog server, verify that the `rsyslog gtls` module is installed:

   ```
   # rpm -qa |grep gtls
   ```

   If it does not exist, install it. For example, in SUSE Linux:

   ```
   # zypper install rsyslog-module-gtls
   ```
4. On the remote Syslog server, edit (or create) the file `/etc/rsyslog.d/remote.conf` to include the following lines:

   ```
   $DefaultNetstreamDriverCAFile /data/2021.crt #This is the certificate downloaded from the ViPR Controller server

   $DefaultNetstreamDriverCertFile /data/server.crt #This is generated in step 1

   $DefaultNetstreamDriverKeyFile /data/server.key #This is generated in step 1
   ```
5. On the remote Syslog server, edit the `/etc/rsyslog.conf` file to add these lines:

   ```
   $ModLoad imtcp
   ```

```
$InputTCPServerStreamDriverMode 1

$InputTCPServerStreamDriverAuthMode x509/certvalid

$InputTCPServerRun 10514 #This is the port number you input
in the configuration page for the rsyslog server
```

Configure Syslog server to accept messages via UDP protocol:

6. On the remote Syslog server, edit the `/etc/rsyslog.conf` file to add these lines:

```
$ModLoad imudp # Module to support UDP remote messages
inbound

$UDPServerAddress * # Listen to any/all inbound IP addresses
(note that the * is default, specifying to make config
clear)

$UDPServerRun 514 # Listen on port 514
```

Configure Syslog server to accept messages via TCP protocol:

7. On the remote Syslog server, edit the `/etc/rsyslog.conf` file to add these lines:

```
$ModLoad imtcp

$InputTCPServerRun 514
```

2. **Configure the format/template for formatting and saving logs:**

Note

The following steps are the same for all protocols.

8. Configure the format/template for how and where the logs are saved, by editing `/etc/rsyslog.conf`. Following are two examples:

   a. **Example 1: Configure a central location to save the logs** (`/var/log/syslog/TemplateLogs`):

```
$template MyTemplate, "[ViPR] - <%pri%> - %timestamp% -
%FROMHOST% - %HOSTNAME% -## %PROGRAMNAME% ##- %syslogtag%
-MM- %msg%\n"

local2.* -/var/log/syslog/TemplateLogs;MyTemplate
```

   b. **Example 2: Configure locations to save the logs by service** (with log location as `/var/log/syslog/AuditLog.log` and `/var/log/syslog/syssvcLog.log`):

```
if ($msg contains ' AuditLog ') then -/var/log/syslog/
AuditLog.log

if ($msg contains ' syssvc ') then -/var/log/syslog/
syssvcLog.log
```

9. Restart the remote Syslog server.

```
# service rsyslog restart
```

3. **Setup ViPR Controller for Syslog forwarding:**
10. Select **System › General Configuration › Syslog Forwarder**.
11. Enter values for the properties.

Option	Description
Syslog Settings	

Option	Description
Enable Remote Syslog	Select True to specify and enable a remote Syslog server.
Remote Server Settings	
Syslog Transport Protocol	Specify the Syslog transport protocol. Select UDP, TCP, or "TCP with encryption" (TLS). For a UDP or TCP connection, you will specify a Syslog Server IP or FQDN, and a Port. For a TLS connection, you will specify a Syslog Server IP or FQDN, a Port, a Security Certificate, and ViPR Controller Security Certificate.
Remote Syslog Servers & Ports	
Server	The IP address of the remote Syslog server. You can obtain this from the Syslog server Administrator.
Port	The port number for the server. The ports on which syslog services typically accept connections are 514/10514.
Certificate	This field appears only if you selected "TCP with encryption" (TLS) as the Syslog Transport Protocol. This field contains the certificate file from the remote Syslog server. Paste the entire content of `server.crt` (including --Start and --End strings), generated in step 1, if TLS is enabled.
Add	Click this button to additional remote Syslog servers.

12. Click the **Test** button to validate the Syslog server input before saving.
13. Click **Save**.
4. **Confirm that the remote Syslog server setup:**
14. Confirm that the remote Syslog server is saving the ViPR Controller logs as expected.
    a. Login to the remote Syslog server.
    b. Verify that the Syslog server is running and listening on the configured port and protocol. In the example below, it is UDP on port 514:

    ```
    # netstat -uanp|grep rsyslog
    udp 0 0 0.0.0.0:514 0.0.0.0:* 21451/rsyslogd
    udp 0 0 :::514 :::* 21451/rsyslogd
    ```

    c. Determine the location of the logs specified in the template section of `/etc/rsyslog.conf`. In the example below it is `/var/log/syslog/TemplateLogs`.

    ```
    $template MyTemplate, "[ViPR] - <%pri%> - %timestamp% - %FROMHOST% - %HOSTNAME% -## %PROGRAMNAME% ##- %syslogtag% -MM- %msg%\n"
    local2.* -/var/log/syslog/TemplateLogs;MyTemplate
    ```

    d. Go to the directory defined in `/etc/rsylsog.conf` and confirm that logs are written to that directory. Note that the format of the saved files will be depend on templates defined by the Syslog server System Administrator.

Example 1:

```
# tail -f /var/log/syslog/TemplateLogs

…

[ViPR] - <150> - Aug 19 09:28:33 - lglw2022.lss.emc.com -
vipr2 -## ...lable_versions><available_ver
##- ...lable_versions><available_ver -MM-
on><new_version>vipr-3.5.0...

[ViPR] - <150> - Aug 19 09:28:33 - lglw2023.lss.emc.com -
vipr3 -## vipr ##- vipr -MM- vipr3 syssvc 2016-08-19
09:28:33 INFO DrUtil:531 - get local coordinator mode from
vipr3:2181

[ViPR] - <150> - Aug 19 09:28:33 - lglw2023.lss.emc.com -
vipr3 -## vipr ##- vipr -MM- vipr3 syssvc 2016-08-19
09:28:33 INFO DrUtil:543 - Get current zookeeper mode leader

…
```

Example 2:

```
# tail -f /var/log/syslog/AuditLog.log

…

2016-08-19T07:56:56+00:00 vipr2 vipr vipr2 AuditLog
2016-08-19 07:56:56 INFO AuditLog:114 - audit log is config
null SUCCESS "Update system property
(config_version=1471593416583,network_syslog_remote_servers_
ports=10.247.102.30:514) succeed."

2016-08-19T07:58:04+00:00 vipr2 vipr vipr2 AuditLog
2016-08-19 07:58:04 INFO AuditLog:114 - audit log is config
null SUCCESS "Update system property
(config_version=1471593484027,network_syslog_remote_servers_
ports=lglw2030.lss.emc.com:
514,system_syslog_transport_protocol=TCP) succeed."

…

#tail -f /var/log/syslog/syssvcLog.log

…

2016-08-19T09:37:39+00:00 vipr4 vipr vipr4 syssvc 2016-08-19
09:37:39 INFO DrUtil:543 - Get current zookeeper mode
follower

2016-08-19T09:37:39+00:00 vipr4 vipr vipr4 syssvc 2016-08-19
09:37:39 INFO DrDbHealthMonitor:55 - Current node is not ZK
leader. Do nothing
```