EMC ViPR Controller

Version 3.6

Security Configuration Guide

302-003-709

REV 01

Published May 2017

Dell 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.“ DELL 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 DELL SOFTWARE DESCRIBED IN THIS PUBLICATION REQUIRES AN APPLICABLE SOFTWARE LICENSE.

Published in the USA.

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

Revision history

Table 1 Revision history

Revision Date	Description of change
May 2017	ViPR Controller 3.6 GA Release

CONTENTS

TABLES

CHAPTER 1

Overview

Overview

This guide provides an overview of security configuration settings available in the product, secure deployment and usage settings, secure maintenance and physical security controls needed to ensure secure operation of the product.

Note

Throughout this document, virtual storage pools are also referred to as virtual pools and virtual storage arrays are also referred to as virtual arrays.

This guide is divided into the following sections:

- Security configuration settings describes settings available in the product to ensure a secure operation of the product.
- Secure deployment and usage settings describes instructions on how to deploy the product securely and how to use the product securely.
- Secure maintenance describes how to perform secure maintenance of the product.
- Physical security controls describes controls needed to protect the product components against unauthorized physical access and physical tampering.

Log in to EMC ViPR Controller

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

Procedure

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

   https://*ViPR_virtual_ip*

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

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

   If you are unable to log in, contact your administrator.

4. You can log out at ***username*** > **Logout** on the upper-right corner of the UI.

CHAPTER 2

Security Configuration Settings

Introduction

This section provides an overview of the settings available in the product to ensure secure operation of the product.

Security settings are split into the following categories:

- Access control settings describes settings available to limit access by end-user or by external product components
- Log settings describes settings related to the logging of events
- Communication security settings describes settings related to security for the product network communications
- Data security settings describes settings available to ensure protection of the data handled by the product
- Secure serviceability settings describes settings available to ensure control of service operations performed on the products by EMC or its service partners
- Security alert system settings describes settings related to sending security alerts and notifications for the security-related events
- Other security considerations describes security settings that may not fall in one of the previous sections

Access control settings

Access control settings enable the protection of resources against unauthorized access.

User authentication

User authentication settings control the process of verifying an identity claimed by a user for accessing the product.

Default accounts

Table 2 Default user accounts and passwords

User account	Password	Description
root	ChangeMe	Default root user
svcuser	ChangeMe	Default SVC user
sysmonitor	ChangeMe	Default System Monitor user. Internal ViPR Controller user only.
proxyuser	ChangeMe	Default Proxy user. Internal ViPR user only.
bin	N/A	Bin
daemon	N/A	Daemon
haldaemon	N/A	HAL daemon
man	N/A	Man page daemon

Table 2 Default user accounts and passwords (continued)

User account	Password	Description
messagebus	N/A	Message bus daemon
nobody	N/A	Nobody user
ntp	N/A	Network Time Protocol daemon
polkituser	N/A	Polkit user group
sshd	N/A	SSHD daemon
storageos	N/A	EMC ViPR Controller user

Authentication configuration

Table 3 Supported external authentication methods

Authentication method	Description
LDAP	As a best practice, the Active Directory filter should be configured so only a system administrator can login.
Active Directory	

Unlocking the svcuser user account

If you login using SSH to a ViPR Controller node using the svcuser account, and your login fails three times, the fourth time you will be locked out.

To unlock the locked svcuser account:

1. Login as root over SSH to the appliance.
2. Run the `pam_tally2 --user=svcuser --reset` command.

Configuring an authentication provider

To ensure that a user or group is uniquely identifiable, when configuring a single authentication provider that spans multiple domains it is advisable to use an attribute which uniquely identifies the group.

For example, the common name can be used if the name attribute is unique for all items within the group.

Setting automated processing account passwords to expire

Local user passwords should be set to expire every year or less.

Changing local account passwords

You can change the password of a local account.

Before you begin

This operation requires the Security Administrator role in ViPR Controller.

The new password must conform to the site-specific local password policy (**System** > **General Configuration** > **Password**), in addition to the ViPR Controller password validation rules:

- at least 8 characters (settable at **System** > **General Configuration** > **Password**)
- 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)
- Cannot be changed more than once in every 60 minutes

Procedure

1. Select **Security** > **Local Passwords**
2. Select a local user account.
3. Enter the new password and confirm.
4. **Save**.

   Alternate method for changing local password:

   When logged in as a local user, you can change password from the top level of the ViPR UI at ***username*** > **Change Password**.

Setting ViPR Controller local user password policy

You can enforce a strong password policy for ViPR Controller local users.

Before you begin

This operation requires the Security Administrator role in ViPR Controller.

The password policy settings only apply to the ViPR Controller local users, which are root, svcuser, proxyuser, and sysmonitor.

If you make no changes to these settings, the default ViPR Controller password validation rules apply:

- at least 8 characters (settable)
- 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
- not in last 3 change iterations

Procedure

1. Select **System** > **General Configuration** > **Password**.
2. Enter values for the properties.

Property	Description
Change interval	The amount of time (in minutes) that a password must be in use before it can be changed. The value 0 allows changes immediately.
Minimum length	The minimum number of characters that a local user password can contain. The value 0 means password length validation will be skipped.
Lowercase Character Number	Minimum number of lowercase alphabetic characters that a local user password must contain. Valid values are 1, 2, 3, 4, or 5.
Uppercase Character Number	Minimum number of uppercase alphabetic characters that a local user password must contain. Valid values are 1, 2, 3, 4, or 5.
Numeric Character Number	Minimum number of numeric characters that a local user password must contain. Valid values are 1, 2, 3, 4, or 5.
Special Character Number	Minimum number of special characters that a local user password must contain. Valid values are 1, 2, 3, 4, or 5.
Repeating Character Number	Maximum number of consecutive repeating characters that a local user password can contain. (0 means disable repeating characters check.)
Characters Need Be Changed	The minimum number of characters that need be changed in a password. (0 means no characters need to be changed.)
History rule	The number of unique passwords that must be associated with a local user before an old password can be reused.
Expire time	The number of days that a password can be in use before ViPR Controller requires a password change. Default is 0, which means password expiry is disabled. When enabling Expire Time, set a value larger than 14, to account for the grace period. Be sure to configure root and svcuser email (under **username** > **Preferences**) before enabling Expire Time, so that password expiration warning emails are received.

3. **Save**.

SUID and SGID files

ViPR Controller contains files that set a user ID (SUID) or set a group ID (SGID) upon execution.

Table 4 Owners, groups, and permissions for SUID and SGID files

File and Location	Owner	Group	Permission	Description
/sbin/unix2_chkpwd	root	shadow	4755	Used by PAM to check the password for the current user.

Table 4 Owners, groups, and permissions for SUID and SGID files (continued)

File and Location	Owner	Group	Permission	Description
				Must have access to files owned by root. Cannot be run as root.
/sbin/unix_chkpwd	root	shadow	4755	Used by PAM to check the password for the current user. Must have access to files owned by root. Cannot be run as root.
/data/connectemc/logs	storageos	users	2770	Required for ConnectEMC logs.
/usr/bin/atop	root	root	4711	Used for monitoring system and troubleshooting.
/usr/bin/chage	root	shadow	4755	Used to change expiry.
/usr/bin/expiry	root	shadow	4755	Used to check if a user password has expired. Requires root privileges.
/usr/bin/chsh	root	shadow	4755	Used to change the shell of a user.
/usr/bin/crontab	root	trusted	4750	Static.
/usr/bin/gpasswd	root	shadow	4755	Used to change a group password.
/usr/bin/mount	root	root	4755	Used to mount a file system.
/usr/bin/mount.nfs	root	root	4755	Used to mount an NFS file system.
/usr/bin/newgrp	root	root	4755	Used to change a group.
/usr/bin/passwd	root	shadow	4755	Used to change a user password.
/usr/bin/passwd.orig	root	shadow	4755	Used to change a user password.
/usr/bin/pkexec	root	root	4755	Used to execute a command as another user.
/usr/bin/su	root	root	4755	Used to switch to the super user (root privileges) or to a specified user.
/usr/bin/sudo	root	root	4755	Used by storageos and svcuser accounts to run commands with elevated privileges.
/usr/bin/umount	root	root	4755	Used to unmount a file system.
/usr/bin/wall	root	tty	2755	Used to send a system-wide message.

Table 4 Owners, groups, and permissions for SUID and SGID files (continued)

File and Location	Owner	Group	Permission	Description
/usr/bin/write	root	tty	2755	Used to send a message to another user.
/usr/lib/polkit-1/polkit-agent-helper-1	root	root	4755	Used to help the policy that allows unprivileged processes to speak to privileged processes.
/usr/lib/utempter/utempter	root	utmp	2755	Used to allow non-privileged applications, such as terminal emulators, to modify the utmp database without having to be setuid root.
/usr/lib64/pt_chown	root	root	4755	Required for Linux system operation.
/usr/sbin/sendmail	root	mail	2555	Runs as storageos and requires send mail privileges.
/run/log/journal	root	systemd-journal	2755	Required for Linux system operation.
/run/log/journal/*<4e03692dd68a8cce4a33b2bd555175f2>*	root	systemd-journal	2755	Required for Linux system operation.

Administrator Groups in Geo Scale Deployments

It is advised to have more than one Security Administrator user or group located in distinct domains in a geo-distributed environment.

If a domain in a geo-distributed environment becomes unavailable, and all Security Administrator users or groups are located on that domain, then access to all Security Administrator users or groups are not accessible.

User authorization

User authorization settings control rights or permissions that are granted to a user to access a resource managed by the product.

VDC Role Assignments

The role to which a user is assigned determines what menu items they can access at the UI and which administration operations they can perform.

For more information about VDC roles, see the *ViPR Controller User Interface Tenants, Projects, Security, Users and Multisite Configuration Guide* which is available from the ViPR Controller Product Documentation Index.

Roles can apply to the virtual data center (VDC) or can be specific to a tenant. The available roles and their scope are listed in this table.

Table 5 Scope of ViPR Controller roles

Scope	Role
Virtual Data Center	System Administrator, Security Administrator, System Monitor, System Auditor
Tenant	Tenant Administrator, Project Administrator, Tenant Approver

The root user (superuser) includes all VDC roles and the Tenant Administrator role for the provider tenant. The root user can act as the bootstrap user for the system by assigning one or more users to the Security Administrator role. The Security Administrator can then assign other user roles.

The **Security** > **VDC Role Assignments** page, provides a Role Assignments table which lists the users and groups to which roles have been assigned.

Table 6 VDC role assignments

Field	Description
Name	The name of the user or group.
Type	The type of assignment: user or group.
VDC Roles	Lists the VDC roles to which a user or group is assigned. You will only see this if you are a Security Administrator. Tenant Administrators can only see tenant roles.

Tenant roles can be set by a Security Administrator from the **Tenants** > **Tenants** page.

Administrator role permissions

The actions that can be performed and the Administrator areas of the UI accessible depend on the administrator role assigned to a ViPR Controller user.

The following table lists the roles and their associated permissions.

Table 7 Role permissions

Role	Permission	UI Access
Tenant Administrator	Assigns tenant roles to tenant users in the given tenant.	**Tenants** > **Tenants** > **Role Assignments**
	View, and modify the name and description of the given tenant.	**Tenants** > **Tenants**
	Adds hosts, clusters, and vCenters to which provisioned storage can be exported.	**Physical** > **Hosts/Clusters/vCenters**
	Configures the Service Catalog for their Tenant.	**Catalog** > **Edit Catalog**
	Creates new projects. Has all permissions on projects in the tenant.	**Tenants** > **Projects**
	Give access to users to projects using an ACL.	
	Can create consistency groups for any project.	**Tenants** > **Consistency Groups**

Table 7 Role permissions (continued)

Role	**Permission**	**UI Access**
	Can view all recent orders for all users in the tenant.	**Catalog** > **All Orders**
	Can view all scheduled orders for the tenant and can cancel scheduled orders.	**Catalog** > **Scheduled Orders**
	Creates execution windows.	**Tenants** > **Execution Windows**
	Specifies approval notification and external approval system settings.	**Tenants** > **Approval Settings**
Project Administrator	Creates projects and can delegate ownership of own projects to other users in the same tenant. Has all permissions for own projects.	**Tenants** > **Projects**
	Give access to users to projects (that Project Administrator owns) using an ACL.	
	Can create consistency groups for owned projects	**Tenants** > **Consistency Groups**
Tenant Approver	Approves orders for the tenant.	No access to Admin view. **Catalog** > **Approvals**
System Administrator	Adds physical storage resources by adding: storage systems, SMI-S providers, fabrics, data protection systems, Vblock compute systems, and networks.	**Physical** > **Storage Systems** **Physical** > **Storage Providers** **Physical** > **Data Protection Systems** **Physical** > **Fabric Managers** **Physical** > **Networks** **Physical** > **Vblock Compute Systems**
	Creates virtual arrays comprising fibre channel and IP networks that connect storage systems and compute environments (hosts and vCenters), and creates virtual pools.	**Virtual** > **Virtual Arrays** **Virtual** > **Block Virtual Pools** **Virtual** > **File Virtual Pools**
	Assigns tenants to virtual arrays and virtual pools using an ACL.	
	Retrieves ViPR Controller status and system health.	**Dashboards** > **Overview** **Dashboards** > **Health** **System** > **Logs**
	Performs system license and software updates.	**System** > **License** **System** > **Upgrade** **System** > **Support Request**
	Retrieves bulk event and statistical records for the ViPR Controller virtual data center.	**Dashboards** > **Overview** **System** > **Logs**
	Views system tasks as well as tenant tasks	**Resources** > **Tasks**

Table 7 Role permissions (continued)

Role	Permission	UI Access
Security Administrator	Create new tenants (sub-tenants), modify tenant user-mappings, and change the quota set for a tenant.	**Tenants** > **Tenants**
	Adds authentication providers.	**Security** > **Authentication Providers**
	Sets the configuration parameters for the virtual data center.	**System** > **General Configuration**
	Creates User Groups	**Security** > **User Groups**
	Assigns users to administrator roles for the virtual data center and for tenants.	\\lglor056\c$\Program Files (x86)\Apache Software Foundation\Apache2.2\htdocs\viprdocs
	Adds trusted certificates and updates keystore.	**Security** > **Trusted Certificates** **Security** > **Keystore**
	Can join sites to created a federated configuration.	**Virtual** > **Virtual Data Centers**
	Assigns tenants to virtual arrays and virtual pools using an ACL.	**Virtual** > **File Virtual Pools**
	Monitors IPsec Status and rotates IPsec Key	**Security** > **IPsec**
	Manages security User Groups	**Security** > **User Groups**
	Manages System Disaster Recovery sites	**System** > **System Disaster Recovery**
System Monitor	Retrieves bulk event and statistical records for the ViPR Controller virtual data center.	**Dashboards** > **Overview**
	Has read-only access to all objects in the ViPR Controller virtual data center.	
System Auditor	Retrieves ViPR Controller virtual data center audit log.	**System** > **Audit Log**

Role matrix

A role matrix shows the availability of menu items for each role. Where a user has more than one assigned role, the access rights are additive.

Table 8 Role matrix

Menu	Sub-menu	Tenant Roles			VDC Roles				None
		TenAd	**ProjAd**	**TenAp**	**SysAd**	**SecAd**	**SysMo**	**SysAu**	
Dashboards	Overview				×		×		
	Health				×		×		
	Database Housekeeping Status				×		×		
Physical	Storage Systems				×				

Table 8 Role matrix (continued)

Menu	Sub-menu	Tenant Roles			VDC Roles				None
		TenAd	ProjAd	TenAp	SysAd	SecAd	SysMo	SysAu	
	Storage Providers				×				
	Data Protection Systems				×				
	Fabric Managers				×				
	Networks				×				
	Compute Images				×				
	Vblock Compute Systems				×				
	Hosts	×							
	Clusters	×							
	vCenters	×							
	Controller Config				×				
Virtual	Virtual Arrays				×				
	Block Virtual Pools				×				
	File Virtual Pools				×				
	Object Virtual Pools				×				
	Compute Virtual Pools				×				
	Mobility Groups				×				
	Virtual Data Centers				×	×			
Catalog	Recently Used	×	×	×	×	×	×	×	×
	View Catalog	×	×	×	×	×	×	×	×
	Edit Catalog	×	×						
	My Orders	×	×	×	×	×	×	×	×
	All Orders	×	×						
	Scheduled Orders	×	×						
	Approvals			×					
Resources	Applications	×	×	×	×	×	×	×	×
	Volumes	×	×	×	×	×	×	×	×
	Block Snapshots	×	×	×	×	×	×	×	×
	Snap Sessions	×	×	×	×	×	×	×	×
	Export Groups	×	×	×	×	×	×	×	×
	File Systems	×	×	×	×	×	×	×	×
	File Snapshots	×	×	×	×	×	×	×	×
	vNAS Servers	×	×	×	×	×	×	×	×

Table 8 Role matrix (continued)

Menu	Sub-menu	Tenant Roles			VDC Roles				None
		TenAd	ProjAd	TenAp	SysAd	SecAd	SysMo	SysAu	
	Buckets	×	×	×	×	×	×	×	×
	Tasks	×	×	×	×	×	×	×	×
Tenants	Tenants	×							
	Projects	×	×			×			
	Schedule Policies	×	×						
	Consistency Groups	×	×						
	Execution Windows	×							
	Approval Settings	×			×				
Security	VDC Role Assignments	×				×			
	Authentication Providers					×			
	User Groups					×			
	Local Passwords					×			
	Keystore					×			
	Trusted Certificates					×			
	IPsec					×			
System	General Configuration					×			
	Data Backup and Restore					×			
	System Disaster Recovery					×			
	Upgrade				×				
	License				×				
	Support Request				×				
	Logs				×		×		
	Audit Log							×	

Assigning a VDC role

The **Security VDC Role Assignments** area provides the ability to assign a VDC administrator role to a user or to a group, or to a ViPR Controller user group.

Before you begin

- This operation requires the Security Administrator role to assign virtual data center roles.
- An authentication provider must be configured before you can assign roles.
- For the ViPR Controller user roles required to perform this operation see the *ViPR Controller Virtual Data Center Requirements and Information Guide*, which is available from the ViPR Controller Product Documentation Index.

A Tenant Administrator can assign tenant roles by going to the **Tenant** > **Tenants** page and selecting **Role Assignments**.

Procedure

1. Select **Security** > **VDC Role Assignments**.
2. Select **Add**.
3. Select Group or User.
4. Enter the name of a domain user or group.

   The group that you specify can be either AD, or LDAP groups, that were provided by the configured Authentication Providers or be a ViPR Controller User Group for a domain provided by the configured Authentication Providers.

5. Select the roles into which you want to assign the user or group.
6. **Save**.

Assign project and service catalog permissions using ACLs

Access control lists are provided to enable you to configure access to the service catalog and to projects for provisioning users. ACLs do not restrict access to a Tenant Administrator. A Tenant Administrator has ultimate authority in the tenant and access to the service catalog and projects cannot be restricted using ACLs.

This task is referenced by areas that use ACLs and provides general information on assigning users and groups to ACLs.
The role that you require depends on the area to which you are applying access control.

Procedure

1. Select **Add ACL**.
2. From the Type drop-down, select whether you are using this entry to set access permissions for a user or a group.
3. In the Name field, enter the name of the user or group that you are assigning permissions to.

   Both users and groups are added in the format: username@yourco.com, or groupname@yourco.com. Users and groups must have been made available to the current tenant (mapped).

   When adding a ViPR Controller User Group, you only need to enter the name of the user group. It is not required to enter any of the domain components for User Groups.

4. In the Access field, use the drop-down list to select the access permissions that you want to assign to the user or group.
5. If you want to add further ACL entries, choose **Add ACL** to add another entry.
6. If you decide you do not need an entry you have made, click the **Remove** button.
7. **Save** the form that your are editing.

Log settings

A log is a chronological record of system activities that is sufficient to enable the reconstruction and examination of the sequence of environments and activities surrounding or leading to an operation, procedure, or event in a security-relevant transaction from inception to final results.

Log description

Table 9 Log file locations and contents

Location	Description of log file
/opt/storageos/logs/apisvc.log	API service log
/opt/storageos/logs/audit/audit.log	Audit log
/opt/storageos/logs/authsvc.log	Authentication service log
/opt/storageos/logs/bkutils.log	Backup/Restore log
/opt/storageos/logs/geodbsvc.log	GEO database service log
/opt/storageos/logs/geosvc.log	GEO service log
/opt/storageos/logs/connectemc.log	ConnectEMC log
/opt/storageos/logs/controllersvc.log	Controller service log
/opt/storageos/logs/coordinatorsvc.log	Coordinator service log
/opt/storageos/logs/dbsvc.log	Database service log
/opt/storageos/logs/dbutils.log	Database utilities log
/opt/storageos/logs/genconfig.log	General configuration log
/opt/storageos/logs/nginx.log	NGINX log
/opt/storageos/logs/nginx_access.log	NGINX access log
/opt/storageos/logs/nginx_error.log	NGINX error log
/opt/storageos/logs/portalsvc.log	User Interface service log
/opt/storageos/logs/sasvc.log	SA service log
/opt/storageos/logs/syssvc.log	System service log
/opt/storageos/logs/vasasvc.log	VASA service log

Log management and retrieval

Retrieving log files

You can access the EMC ViPR Controller log files from the user interface.

Procedure

1. Open the ViPR Controller user interface.
2. Click **System** > **Logs**.
3. Click **Download**.

Retrieving Order log files

You can retrieve Order log file information using the ViPR Controller API.

To retrieve order information, use the following API commands:

Table 10 API commands to retrieve Order information

Command	Description
GET /api/orders	List orders
GET /api/orders/all	List orders
POST /api/orders/bulk	List orders
GET /api/orders/bulk	Bulk ID parameter with order IDs suitable for passing to the POST /api/orders/bulk call
GET /api/orders/{orderId}	Shows orders
PUT /api/orders/{orderId}/tags	Updates Order Tags
GET /api/orders/{orderId}/tags	Shows Order Tags
GET /api/orders/{orderId}/execution	Shows execution information for an order

Communication security settings

Communication security settings enable the establishment of secure communication channels between the product components as well as between product components and external systems or components.

Port usage

ViPR Controller ports

Correct operation of ViPR Controller and its services requires certain ports to be open in the firewall. When installed, these ports are automatically configured.

ViPR Controller Authentication Provider Ports
These ports are the default listening (incoming) ports in the external AD or LDAP through which ViPR Controller tries to establish the connection. When the AD or LDAP is not listening through these default ports, the server_url (ldap(s)://<ip:port>) in the ViPR Controller authorization provider configuration can be modified to specify ports other than the defaults.

Table 11 ViPR Controller Authentication Provider Ports

Port	Protocol	Direction	Description
88	TCP and UDP	Outbound	Domain Controller to which ViPR Controller connects during Windows host discovery for Kerberos authentication
389	TCP	Outbound	For non-secure communication with external authentication providers like AD or LDAP

Table 11 ViPR Controller Authentication Provider Ports (continued)

Port	Protocol	Direction	Description
636	TCP	Outbound	For secure communication (SSL) with external authentication providers like AD or LDAP
35357	TCP	Outbound	Keystone (OpenStack Authentication Provider)

ViPR Controller VM ports

ViPR Controller VM ports are deployed with the firewall enabled by default, with these ports open:

Note

Ports exposed to outside ViPR nodes are: 7, 22, 25, 123, 162, 443, 500, 990, 4443, 4500, 7012, 7100, 8776, 9083, and 9998. All other ports are ViPR inter-nodes connections.

Table 12 ViPR Controller VM ports

Port	Protocol	Direction	Description
7	UDP	Inbound	echo protocol
22	TCP	Inbound	SSH port
25	TCP	Outbound	SMTP port
123	UDP	Bi-directional	NTP
162	UDP	Outbound	SNMP
443	TCP	Bi-directional	Standard HTTPS port to be redirected to 4443
500	UDP	Bi-directional	IPsec
990	FTPS	Outbound	ConnectEMC - Outbound Only
2181 and 2889	TCP	Bi-directional	Coordinator service
2888	TCP	Bi-directional	Zookeeper peers connect to each other
1098	TCP		Internal communication port. Open manually only for JMX in development
1443	TCP		Nginx uses for accessing the REST apis
6080	TCP		REST interface for S3 API
4443	TCP	Bi-directional	Reverse Proxy/Load balancer for ViPR REST APIs ; GUI port
4500	UDP	Bi-directional	IPsec
5000	UDP	Inbound	CIM adapter for internal nodes
6443	TCP	Inbound	ViPR Controller user interface
7000	TCP	Bi-directional	DB service
7001	TCP	Bi-directional	DB SSL

Table 12 ViPR Controller VM ports (continued)

Port	Protocol	Direction	Description
7012	TCP	Inbound	CIM adapter
7100	TCP	Bi-directional	GEO (across VDCs) database connections; protected by IPsec
7199	TCP	Bi-directional	DB service
7200	TCP	Bi-directional	DB service
7299	TCP	Bi-directional	JMX server and register ports
7300	TCP	Bi-directional	JMX server and register ports
7399	TCP	Bi-directional	Coordinator service
7400	TCP	Bi-directional	Coordinator service
7443	TCP	Inbound	Authentication service
8080	TCP	Inbound	API service
8443	TCP	Inbound	API service
8444	TCP	Outbound	SA service
8543	TCP	Bi-directional	Nginx
8776	TCP	Bi-directional	Cinder-compatible REST API
9083	TCP	Inbound	VASA service
9093	TCP	Inbound	VASA service
9160	TCP	Bi-directional	DB service
9260	TCP	Bi-directional	Geo DB service
9993	TCP	Bi-directional	sys service
9998	TCP	Bi-directional	syssvc CLI download (unauthenticated)
10099	TCP	Bi-directional	Controller service
10099	TCP		Controller service
10100	TCP		Open manually only for JMX in development on extranode
10101	TCP		Open manually only for JMX in development on extranode
40201	TCP	Bi-directional	Controller service

Firewall ports required to be open for implementing ViPR Controller Disaster Recovery

ViPR Controller uses these ports in support of disaster recovery.

Certain ports are required to be opened in bi-directional fashion for ViPR Controller to be deployed in the presence of firewalls. (For example, when replicating data to another physical location.)

- All active or standby nodes should have unique IP addresses and be reachable by others. This requirement supports "hot" standby required by Cassandra/ Zookeeper replication.
- Ensure that you have quality speed network infrastructure between datacenters. The maximum supported latency between Disaster Recovery (DR) sites is less than or equal to 150ms. This supports the synchronous replication of Cassandra/ Zookeeper and storage management to remote sites.
- NAT across data centers is not supported. No ViPR Controller nodes can be behind NAT proxy. This is a requirement for Cassandra/Zookeeper replication.
- Ports 2888(ZK), 2889(ZK), 7100(dbsvc), 7000(geodbsvc), 500(ipsec), 4500(ipsec) should be allowed for all nodes in remote data center on firewall for ViPR Controller data replication. Allow port 443 (HTTPS) access on the cross-datacenter firewall to issue inter-site control commands.

Ensure that you have quality speed network infrastructure between datacenters. NAT across data centers is not supported. The maximum supported latency between System Disaster Recovery (DR) sites is <= 150ms.

Table 13 ViPR Controller ports required to be open between disaster recovery sites

Port	Protocol	Direction	Description
443	TCP	Bi-directional	Standard HTTPS port to be redirected to 4443
500	UDP	Bi-directional	IPsec
2888	TCP	Bi-directional	Zookeeper (Zookeeper peers connect to each other)
2889	TCP	Bi-directional	Co-ordinator service
4500	UDP	Bi-directional	IPsec
7000	TCP	Bi-directional	DB Service
7100	TCP	Bi-directional	Outbound Virtual data center to virtual data center communication port used for GEO and System Disaster Recovery sites communication. **Note** This port must be open for inbound and outbound traffic.

Storage-related ports

ViPR Controller uses these storage ports.

Table 14 ViPR Controller storage-related ports

Port	Protocol	Direction	Description
22	TCP	Outbound	ScaleIO, non-SSL
22	TCP	Outbound	Cinder; third-party block discovery
22	TCP	Outbound	Cisco switches
443	TCP	Outbound	ScaleIO, SSL
443	TCP	Outbound	VNX File

Table 14 ViPR Controller storage-related ports (continued)

Port	Protocol	Direction	Description
443	TCP	Outbound	VPLEX
443	TCP	Outbound	XtremIO
443	TCP	Outbound	NetApp
443	TCP	Outbound	EMC Unity
2001	TCP	Outbound	Hitachi
3033	TCP	Outbound	The ViPR Controller Dell SC driver uses the REST API available with Dell Storage Manager 2015 R3 or above. All API communication uses HTTPS over port 3033.
5000	TCP	Outbound	Keystone; third-party block authentication
5988	TCP	Bi-directional	VNX File
5988	TCP	Bi-directional	VNX Block, non-SSL
5988	TCP	Bi-directional	VMAX, non-SSL
5989	TCP	Bi-directional	VNX File
5989	TCP	Outbound	SMI-S for XIV, SSL
5989	TCP	Bi-directional	VNX Block, SSL
5989	TCP	Bi-directional	VMAX, SSL
7100	TCP	Outbound	Virtual data center to virtual data center communication port used for GEO and System Disaster Recovery sites communication **Note** This port must be open for inbound and outbound traffic.
7225	TCP	Outbound	RecoverPoint
8080	TCP	Outbound	Isilon
8443	TCP	Outbound	Hyper-Scale Manager for XIV, REST API
9998	TCP	Outbound	CLI download (unauthenticated)

Host access ports

ViPR Controller accesses hosts over the following ports.

Table 15 ViPR Controller host access ports

Port	Protocol	Direction	Description
22	TCP	Bi-directional	Linux, AIX, AIX VIO, HP-UX, SSH port
22	TCP	Bi-directional	AIX
22	TCP	Bi-directional	AIX VIO

Table 15 ViPR Controller host access ports (continued)

Port	Protocol	Direction	Description
22	TCP	Bi-directional	HP-UX
443	TCP	Bi-directional	vCenter HTTP port
5985	TCP	Bi-directional	Windows WinRM HTTP port
5986	TCP	Bi-directional	Windows WinRM HTTPS port

Fabric provider ports

ViPR Controller accesses fabric providers over the following ports.

Table 16 ViPR Controller fabric provider ports

Port	Protocol	Direction	Description
22	TCP	Bi-directional	Cisco MDS
5988	TCP	Bi-directional	Brocade SMI-S provider, for discovering Brocade switches (non-SSL)
5989	TCP	Bi-directional	Brocade SMI-S provider, for discovering Brocade switches (SSL)

Compute Image server ports

ViPR Controller accesses compute image servers over the following ports.

Table 17 ViPR Controller compute image server ports

Port	Protocol	Direction	Description
22	TCP	Outbound	SSH

Network encryption

IPsec

Internet Protocol Security (IPsec) is a protocol suite for secure Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPsec enables secure communication between nodes in a ViPR cluster and between ViPR clusters, and uses an IPsec Key to secure the communication. IPsec is managed from the **Security** > **IPsec** page.

The **IPsec** page provides current information on **IPsec Status** and **IPsec Configuration**. The page is refreshed once per minute.

- **IPsec Status**: This area provides an indication of the IPsec stability. Possible values are:
    - **Stable**: IPsec connections between the nodes are good.
    - **Disabled**: The IPsec feature is turned off.

  - **Degraded**: Some IPsec connections are broken. In most situations, ViPR Controller should be able to resolve the issue, and user action will not be required.

  Information is also provided on the time interval since the last update.

- **IPsec Configuration**: This area provides the date and time on which the current IPsec Key was generated. Click **Rotate IPsec Key** to generate a new key. The IPsec communication between the nodes in the cluster will be stopped for a minute or so while restarting the IPsec service.

Configuring SSH keys

You can configure SSH keys from the user interface.

Procedure

1. Open the ViPR user interface.
2. Click **System** > **General Configuration** > **Security**.

SHA-256 support

A `strong_ciphers` configurable parameter has been added to ViPR Controller to support use of SHA-256.

Use either `viprcli` or API commands to set the parameter. You will need to create a property values file with a comma-separated list of the encryption algorithms you want ViPR Controller to support. For example,

```
TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA
```

In this `viprcli` example, the file, `propvalue`, holds the list of new values to be set:

```
./viprcli system set-properties -propertyname strong_ciphers
-propertyvaluefile propvalue
```

Note

Both AES-128 and SHA-256 encryption algorithms are supported by default.

Data security settings

Data security settings enable definition of controls to prevent data permanently stored by the product to be disclosed in an unauthorized manner.

ViPR Geo-Replication service

When securing a ViPR instance that utilizes the Geo-Replication service, it is advisable to configure the following:

- Ensure all traffic is encrypted across your data centers.
- Ensure all data leaving your data center from ViPR services is encrypted.
- Enable IP address whitelisting to ensure only authorized IP addresses are allowed to access the ViPR Geo-Replication service.

Security alert system settings

Setting email properties

You can change the email properties related to the SMTP server used for approval requests and for accessing ConnectEMC.

Before you begin

This operation requires the Security Administrator role in ViPR Controller.

Procedure

1. Select **System** > **General Configuration** > **Email**.
2. Enter values for the properties.

Option	Description
SMTP server	SMTP server or relay for sending email (For ConnectEMC and approvals).
SMTP 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 to the SMTP server.
Username	Username for authenticating with the SMTP server.
Password	Password for authenticating with the SMTP server.
From address	From email address for sending email messages (user@domain).

3. Click **Test Email Settings** to test the email settings.
4. Click **Save**.

Approvals

Tenant approvers can access the **Approvals** page from the **Catalog** > **Approvals** menu. Only Tenant Approvers can see the Approvals menu.

Approval table
The **Approvals** page shows all approvals that have been submitted, the user who submitted the order, the status of the order's approval request, the time it was submitted and, if it has been approved, who approved it.

Approving or rejecting orders

Note

Tenant Administrators can configure the approvals feature to send a notification email when an order is waiting for approval.

1. From the **Catalog** > **Approvals** page, click the service name in the table to open the approval panel.
2. Optionally, enter a reason for approving or rejecting the order.
3. Click **Approve** or **Reject**.

   Note

   If you created the order, the **Approve** button is not available. It is a security issue to permit the same user to create an order and then approve it. You can only reject your own orders.

Other security considerations

Native backup and restore service

ViPR Controller has a native backup and restore service that creates a backup set of the ViPR controller nodes database. The backup set can be created through REST API calls, on demand using viprcli or the ViPR Controller UI, or scheduled using the ViPR Controller UI.

To use the ViPR Controller native backup and restore service, see the *ViPR Controller Installation, Upgrade, and Maintenance Guide* on the ViPR Controller Product Documentation Index.

Licensing

The EMC ViPR Controller licensing model supports a managed capacity license and a raw, usable, frame-based capacity license.

Note

Starting with Release 3.0, ViPR Controller has 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.

For details on licensing considerations for new installations and upgrade installations, refer to the *ViPR Controller Installation, Upgrade, and Maintenance Guide*, which is available from the ViPR Controller Product Documentation Index.

At a minimum you need to obtain at least a ViPR Controller license and upload it to the ViPR virtual appliance.

The **Dashboards** > **Overview** page shows the installed licenses and the **System** > **License** page provides additional details.

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 **Service Center**.
3. Select **Product Registration & Licenses** > **Manage Licenses and Usage Intelligence**.
4. Select **ViPR Controller** 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.