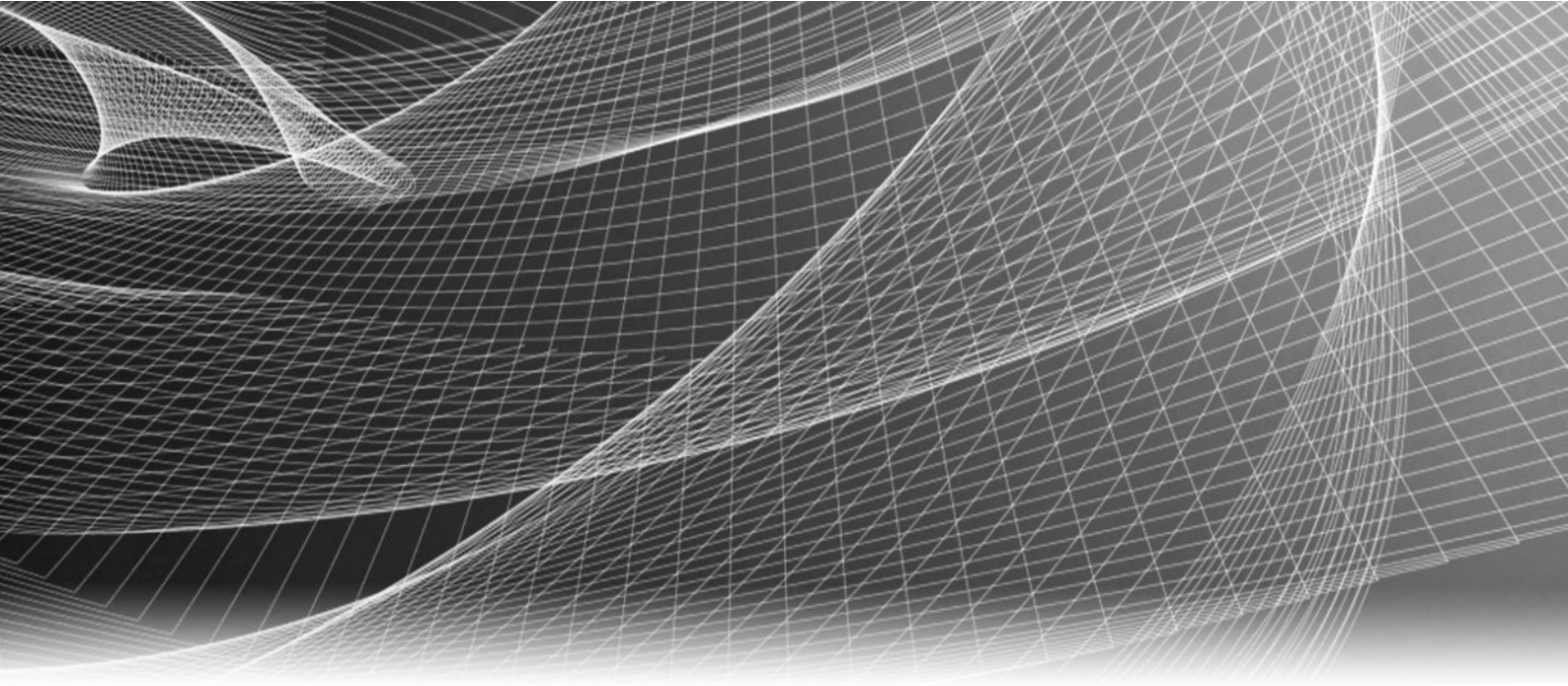


EMC ViPR Controller

Version 3.0

User Interface Tenants, Projects, Security, Users, and Multisite Configuration Guide

302-002-707

01

EMC²

Published May, 2016

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

CONTENTS

Chapter 1 **Setting up Tenants, Projects, Consistency Groups, and Schedule Policies** 5

Creating a tenant in the ViPR Controller UI 6
Adding a new tenant to an existing ViPR Controller virtual data center 7
Assign the Tenant Administrator role for the provider tenant or a sub-tenant 7
Set up VDC for a tenant 8
Set up the tenant for end users 9
Map users into a tenant from the ViPR Controller UI 10
Creating or editing projects 10
Create or edit schedule policy 12

Chapter 2 **Setting up security for the ViPR Controller** 13

ViPR Controller user role requirements 14
Assigning ViPR Controller roles 17
Assigning a user or group to a VDC role 18
Assigning a user, group, or user group to a tenant role 18
Adding an authentication provider 19
Authentication provider settings 20
Considerations when adding Active Directory authentication providers 26
Creating or editing User Groups 28
Local Account Passwords 29
Updating EMC ViPR Controller Keystore 32
Create and import a CA-signed certificate into ViPR Controller 32
Validating connection to LDAPS server in EMC ViPR Controller 33

Chapter 3 **Managing ViPR Controller virtual data centers in different geographical locations** 35

Overview of a ViPR Controller multisite (GEO-federated) configuration 36
Planning the deployment of a multisite ViPR Controller 36
Linking multiple ViPR Controller virtual data centers in a multisite configuration 37
Disconnecting and reconnecting aViPR Controller VDC in a geo federation 39
Disconnecting a virtual data center 39
Reconnecting a virtual data center 40
Deleting a virtual data center 40
Upgrading a ViPR Controller VDC in a GEO (multi-site) federation 41

CHAPTER 1

Setting up Tenants, Projects, Consistency Groups, and Schedule Policies

This chapter includes the following topics:

- Creating a tenant in the ViPR Controller UI 6
- Adding a new tenant to an existing ViPR Controller virtual data center 7
- Map users into a tenant from the ViPR Controller UI 10
- Creating or editing projects 10
- Create or edit schedule policy 12

Creating a tenant in the ViPR Controller UI

You can configure ViPR Controller with multiple tenants where each tenant has its own environment for creating and managing storage. Storage resources assigned to a tenant cannot be accessed by users from other tenants. You can create a single level of tenants under the provider tenant. The ViPR Controller UI enables you to create new tenants and map users into the tenant.

Before you begin

- For the ViPR Controller user roles required to perform this operation see ViPR Controller user role requirements on page 14.
- For steps to configure multiple tenants, refer to Adding ViPR Controller Tenant to Existing VDC on page 7.
- An authentication provider must have been registered with ViPR Controller and must be part of the domain from which you want to map users.
- Your AD, or LDAP administrator must have set up AD or LDAP groups and/or attribute mappings in accordance with your tenant plan.
- If you want to map a ViPR Controller User Group to the tenant, you must configure the User Group first.
- If you are configuring a tenant with a namespace for Elastic Cloud Storage, be sure to review the configuration requirements in the *ViPR Controller Virtual Data Center Requirements and Information Guide*, which is available from the ViPR Controller Product Documentation Index .

Procedure

1. At the ViPR Controller UI, select **Tenant** › **Tenants**.
2. You can add a tenant by choosing **Add**, or to edit an existing tenant, click on the tenant name.
3. Type a name and a description for the tenant.
4. If you will be using ViPR Controller to discover Elastic Cloud Storage (ECS), and create buckets, enable **Object Namespace**.
5. If you will be using ViPR Controller to discover ECS, and create buckets, select the **Namespace** which was discovered with the ECS.
6. Optionally, specify a quota for the tenant. This is the total storage that users in the tenant can create.
7. Select the domain to which the tenant users belong.

   You can use the same domain to provide users for more than one tenant. To do so, you must configure the user mappings to identify the specific set of users that will belong to the tenant and to ensure that a user is mapped into only a single tenant.
8. Specify any groups that you want to use to map users into the tenant.

   The group or groups that you specify can be either AD, or LDAP groups, that were added as Authentication Providers, or be a ViPR Controller User Group.

   A group associated with a domain can be used by more than one tenant, and the selection of users from the domain group can be based on attributes associated with the user.
9. To use attributes to map users into the tenant, click the **Add Attribute** button and enter the name of the attribute and the value or values for the attribute.

For users to be mapped into the domain, the attribute value set for the user must match the attribute value specified in ViPR Controller.

10. To specify the way users will be mapped from the selected domain, select **Add User Mapping Rule**.

    A user mapping rule is added to the tenant. You can add more than one user mapping to achieve finer grained control over the selection of users for the tenant.

11. Click **Save**.

After you finish

Any sub-tenant that you created requires a Tenant Administrator to perform day-to-day administration of the tenant: configuration of the service catalog, creation of projects, assignment of users to tenant roles. Sub-tenants cannot be managed by the tenant administrator of the provider tenant. Ideally, tenants can be managed by the creator of the tenant (since they are, by default, the Tenant Administrator), or a user that belongs to the group can be assigned the role of Tenant Administrator.

Adding a new tenant to an existing ViPR Controller virtual data center

This topic outlines the steps required to configure a new tenant, which is a sub-tenant under the provider tenant.

Before you begin

- You should plan how you want to map users into tenants.
- To create a new tenant you will need the Security Administrator.
- To perform virtual array or virtual pool tenant assignment, you will need the System Administrator role.

Procedure

1. Create a new tenant and map users into the tenant.

   See: Creating a tenant at the ViPR Controller UI on page 6.

2. Assign a Tenant Administrator role for the tenant.

   See: Assign the Tenant Administrator role for the provider tenant or a sub-tenant on page 7

3. Perform any virtual array and/or virtual pool assignment for the tenant.

   You will need the System Administrator role and the Tenant Administrator role to perform this assignment.

   See: Set up VDC for a tenant on page 8

4. The Tenant Administrator, prepares the tenant for end-users by assigning users to projects and customizing the service catalog.

   See: Set up the tenant for end users on page 9

Assign the Tenant Administrator role for the provider tenant or a sub-tenant

Initially, the Security Administrator for the VDC is the only user that can configure the provider tenant. Configuring the provider tenant, includes assigning a Tenant Administrator to the provider tenant. Once a Tenant Administrator is assigned to the provider tenant, the Tenant Administrator for the provider tenant can do all of the tenant

level operations including assigning tenant roles to the other provider tenant users and access the virtual data center resources configured for the provider tenant. The Tenant Administrator of the provider tenant does not have access to the sub-tenants.

Before you begin

- You must have the Security Administrator role or the Tenant Administrator role for the tenant to which you want to assign the Tenant Administrator role.
- You will need the username or group to which you want to assign the Tenant Administrator role. The user or group must be a member of the tenant for which you want the user or group to be the administrator.

Procedure

1. Select **Tenant Settings** › **Tenants**.
2. For the tenant for which you want to perform the assignment, select the **Role Assignments** button, located in the Edit column of the Tenants table.
3. At the Tenant drop-down, select the tenant for which you want to assign a Tenant Administrator role.
4. Click **Add**.
5. Select whether the role is being assigned to a User or Group.
6. Enter the name of the user or group.
7. Select the Tenant Administrator role.
8. Click **Save**.

Results

The user or group will appear in the Role Assignments table as Tenant Administrator for the tenant to which he has been assigned. If an error occurs check that the user is a member of the tenant to which you are assigning the role.

Set up VDC for a tenant

You can add access control to virtual arrays and virtual pools to make them available to specific tenants.

A virtual array comprises array endpoints and host endpoints interconnected by a SAN fabric or an IP network. The virtual array can comprise both fibre channel and IP networks. In this way different array ports can be configured into different virtual arrays, allowing a physical array to contribute to more than one virtual array.

This partitioning of physical arrays into virtual arrays, coupled with the ability to assign access to specific tenants, provides control over the storage provisioning environment made available to a tenant.

Even finer grained control can be obtained by assigning specific virtual pools to tenants. For storage provisioning purposes, the physical storage pools of a virtual array are offered as virtual pools based on their performance and protection characteristics. Restricting access to a virtual pool to specific tenants could mean that if a virtual pool is configured to use a particular array type, restricting access to the virtual pool can prevent a particular tenants from accessing the array. Similarly, you could restrict access to a pool that provides a particular performance characteristic, such as SSD.

Set up tenant access to virtual arrays and virtual pools

When configuring a tenant, you define which virtual arrays and virtual pools a tenant can access using an access control list. This lists controls which tenants are authorized to

access VDC-level resources and which users or groups are authorized to access tenant-level resources.

Before you begin

- You must be a System Administrator in ViPR Controller.

Procedure

1. To make a virtual array available to specific tenants:
   a. Navigate to **Virtual Assets** › **Virtual Arrays**.
   b. Select the virtual array to assign tenant access.

      The **Edit Virtual Array** page appears.
   c. Expand **Access Control**.
   d. Click the **Grant Access to Tenants** box and select the tenants to access this virtual array.
   e. Click **Save**.

      Users belonging to the selected tenants can access the virtual array.
2. To make a virtual pool available to specific tenants:
   a. Navigate to **Virtual Assets** › **Block Virtual Pools** or **Virtual Assets** › **File Virtual Pools**.
   b. Select the virtual pool to assign tenant access.

      The **Edit Virtual Pool** page appears.
   c. Expand **Access Control**.
   d. Click the **Grant Access to Tenants** box and select the tenants to access this virtual pool.
   e. Click **Save**.

      Users belonging to the selected tenants can access the virtual pool.

Set up the tenant for end users

Once a tenant has been created and configured, there are a number of Tenant Administrator tasks that can be performed.

The following administration tasks can be performed in preparation for using the tenant for block and file provisioning operations.

- Projects can be created and tenant users given access to the project.
- The service catalog can be configured by arranging services in categories. Tenant users can be assigned access to the categories or individual services.
- Hosts, clusters, and vCenters for the tenant can be added.
- Consistency groups can be created.
- Execution windows can be created.

Map users into a tenant from the ViPR Controller UI

The ViPR Controller UI provides the ability to map users into a tenant based on the AD/LDAP domain, groups and attributes associated with users. (Keystone cannot be used to map users into a tenant.)

Before you begin

- Only Security Administrators can map users into a tenant.
- An authentication provider must have been registered with ViPR Controller and must be for the domain from which you want to map users. For steps see: Adding an authentication provider on page 19.
- You must have administrator access to your AD in order to configure groups and attribute mappings.
- You must create the groups or users in AD, or LDAP prior to mapping the users from the ViPR Controller UI.
- If you will be using ViPR Controller User Groups, you must create the User Group prior to mapping the users from the ViPR Controller UI.
- If you are using attribute mapping, each user must have the appropriate attribute value set in AD or LDAP.

An authentication provider links to an Active Directory (AD) or Lightweight Directory Access Protocol (LDAP) domain and provides access to a set of users from the domain. User mapping provides an additional level of control over the selection of users from the available domains. The use of user mappings is particularly useful where you have multiple domains or where you want to divide users available from a domain between multiple ViPR Controller tenants.

For more information, review Adding an authentication provider on page 19.

Procedure

1. At the ViPR Controller UI, select **Tenant Settings** › **Tenants**.
2. In the Tenants table, click on the name of the tenant to open it for editing.
3. If a domain hasn't been selected select one from the domain drop-down.
4. Specify any groups that you want to use to map users into the tenant.
5. If you want to use attributes to map users into the tenant, click the **Add Attribute** button and enter the name of the attribute and the value or values for the attribute.

   For users to be mapped into the domain, the attribute value set for the user must match the attribute value specified in ViPR Controller.
6. **Save** the tenant settings.

Creating or editing projects

All file and block resources provisioned by using ViPR Controller must be associated with a project. Projects are tenant resources and are created and managed by the Tenant Administrator of the tenant (or delegated to a Project Administrator).

Before you begin

- You must be either a Tenant Administrator or a Project Administrator to be allowed to create projects.

- Projects created by a Tenant Administrator can only be administrated by a Project Administrator if the Project Administrator is the project owner.
- Projects created by a Project Administrator are visible to, and can be administrated by, a Tenant Administrator.

Procedure

1. Select **Tenants** › **Projects**.
2. Click **Add**, to create a new project, or click the project name to edit the project.
3. Enter the name of the project.
4. In the **Owner** field, enter the name of the project owner.

   Note

   This option is available only while editing a project, and is not present while creating a new project.

   This is the AD/LDAP name of the user. If you do not enter a name, you will be the project owner.

   The project owner should be a Project Administrator. This provides a way of allowing a project created by a Tenant Administrator to be delegated to a Project Administrator.

   If you are a Tenant Administrator, projects that you own cannot be administrated by Project Administrator unless you make them the owner.

   If you assign project ownership to a provisioning user, the user will not be able to perform administration at the UI.

5. You can associate a quota with the project to limit the amount of storage provision for the project.
   a. Check the **Enable Quota** box
   b. In the **Quota** field, enter the maximum amount of storage that you want to allow.
6. To assign project permissions to other users, select **Add ACL**.

   An ACL field is displayed allowing you enter a user or group name and assign a permission.
7. Enter the name of a user or group and set the **Type** field to be consistent.
8. Select the access permission for the user as either ALL or BACKUP.

   ALL permission allows users to provision resources that belong to a project and to run services against resources owned by a project. BACKUP allows a user to view the resources belonging to a project and perform data protection operations.

   For more information see Adding an authentication provider on page 19.
9. To add more users or groups, select **Add ACL** again.

   You can remove an ACL entry by clicking **Remove**.
10. When you have added all ACL entries, click **Save**.

Create or edit schedule policy

Tenant Administrators can use the **Tenants › Schedule Policies › Create or Edit Schedule Policy** page to create or edit a schedule policy.

Procedure

1. Go to the **Tenants › Schedule Policies** page.
2. If you are creating a new policy, click **Add**.

   If you are editing an existing policy, click the policy name.

   Note

   You can only edit a schedule policy when it is not assigned to any storage resources.

3. Enter the following information:

Option	Description
Type	Select the type of Schedule Policy. **Note** File Snapshot is currently the only available option. The File Snapshot Schedule policy defines: • Regularly scheduled intervals when ViPR Controller will create snapshots of an Isilon file system. • The retention period for how long the snapshot will be retained before it is deleted.
Name	Enter a schedule policy name.
Schedule Time	The time of day the first file system snapshot will be taken. If ViPR Controller and the Isilon storage system are running in two different time zones, the schedule time is set for the time zone in which ViPR Controller is running.
Generate Snapshot every	The number of times the snapshot will be taken during a given frequency.
Frequency	Defines how often the snapshot will be taken: daily, weekly, or monthly. It further allows you to define which day or week of the month the snapshots will be taken.
Snapshot Expiration	The retention period for how long the snapshot will be retained before it is deleted.

CHAPTER 2

Setting up security for the ViPR Controller

This chapter includes the following topics:

- ViPR Controller user role requirements 14
- Assigning ViPR Controller roles 17
- Adding an authentication provider 19
- Creating or editing User Groups 28
- Local Account Passwords 29
- Updating EMC ViPR Controller Keystore 32
- Validating connection to LDAPS server in EMC ViPR Controller 33

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 1 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). **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.

Table 1 VDC roles (continued)

VDC Role	Authorized Actions
	• 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.
	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. • 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).

Table 1 VDC roles (continued)

VDC Role	Authorized Actions
	▪ 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
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 2 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.
	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.

Assigning ViPR Controller roles

ViPR Controller has a local "root" user who has all roles required to set up the VDC and the root tenant and can be used to bootstrap the system by assigning the required administrator roles.

In general, the role administration proceeds as follows:

- The "root" user assigns a user to the Security Administrator role.
- Security Administrator:
  - Creates a System Administrator to set up the VDC
  - Creates a Tenant Administrator for the provider tenant to administrate tenant level resources.
- Tenant Administrator assigns roles to tenant users.

For user role details see ViPR Controller user role requirements on page 14.

Assigning a user or group to a VDC role

The ViPR Controller Security Administrator can assign both VDC roles and tenant roles.

Before you begin

- An authentication provider must have been added to ViPR Controller.
- The user or group to be assigned to a role must belong to the provider tenant.
- To assign a VDC role, you must have the Security Administrator role in ViPR Controller.

Procedure

1. Select **Security** › **VDC Role Assignments**
2. Click **Add**.
3. At the **Create VDC Role Assignment** page, select **Group** or **User**.
4. Either enter the name of the user, group, or the ViPR Controller User Group to which you want to assign a role.

   AD or LDAP user names and group names are in the form: user@mydomain.com and group@mydomain.com.

   If an alternate UPN suffix is configured in Active Directory and the authentication provider for the user's domain (for example, `mydo` for `mydomain.com`), enter the user name as user@mydo.

   For ViPR Controller User Groups just enter the name.

   Any group from an authentication provider can be assigned to a role. However, the group can comprise users who are mapped into different tenants and, as only members of the provider tenant can be assigned to a VDC role, only members of this group who are also part of the provider tenant will be able to access the role when they log in.
5. Select the VDC role(s) that you want to assign.
6. Click **Save**.

Assigning a user, group, or user group to a tenant role

A user with the Security Administrator role, or Tenant Administrator role for a tenant, can assign roles to users, groups, or ViPR Controller User Groups who belong to the tenant.

Before you begin

- An authentication provider must have been added to ViPR Controller.
- You will need the user name or group name to which you want to assign the Tenant Administrator role.
- In general, the user to be assigned to a role should belong to the tenant for which you want to assign the role. However, It is possible to assign a member of the provider tenant as the Tenant Administrator for the sub-tenant.
- You must have Tenant Administrator role for the tenant that you are logged in to, or you must have the Security Administrator role for the VDC.

Procedure

1. Select **Tenants** › **Tenants**.
2. For the tenant for which you want to perform the assignment, click the **Role Assignments** button, located in the Edit column of the Tenants table.

3. Click **Add**.
4. Select whether the role is being assigned to a User or Group.
5. Enter the name of the user, group, or ViPR Controller User Group.

   User names and group names are in the form: user@mydomain.com and group@mydomain.com.

   If providing a ViPR Controller User Group, only the User Group name is required. You do not need to enter any domain components.

   Any group from an authentication provider can be assigned to a role. However, the members of the group can be mapped into different ViPR Controller tenants and only members of the tenant in which the role assignment has been made (and the provider tenant, in the case of the Tenant Administrator role) will be granted the role when the user logs in.

   If an alternate UPN suffix is configured in Active Directory and the authentication provider for the user's domain (for example, `mydo` for `mydomain.com`), enter the user name as user@mydo.
6. Select the tenant roles that you want to assign.
7. Click **Save**.

Adding an authentication provider

Authentication providers are added to ViPR Controller so that the user can be assigned roles or ACLs, and for registering ViPR Controller as a block storage service in Openstack (Keystone).

Before you begin

This operation requires the Security Administrator role in ViPR Controller. (The root user has this role.)

You need access to the authentication provider information listed in Authentication Provider Settings on page 20. Note especially the requirements for the Manager DN user.

The only local users in ViPR Controller are the special built-in administrative users (root, sysmonitor, svcuser, and proxyuser),

User authentication is done through an authentication provider added to ViPR Controller at **Security** › **Authentication Providers** in the ViPR Controller UI.

Procedure

1. Select **Security** › **Authentication Providers**.
2. Click **Add**.
3. Enter values for the attributes. Refer to Authentication Provider Settings on page 20.
4. Click **Save**.
5. To verify the LDAP or AD configuration, add a user or group from the authentication provider at **Security** › **VDC Role Assignments**, then try to log in as the new user or as a member of the new group.

   This step is not required for Keystone configuration.
6. Select **Tenants** › **Tenants** › **Provider Tenant** and add the required domain group to the Authentication User Mapping of the Provider Tenant. This is required in order to prevent all domain users from being able to log in to ViPR using the Provider Tenant.

This step is not required for Keystone configuration.

Authentication provider settings

You need to provide certain information when adding or editing an authentication provider.

Table 3 Authentication provider settings

UI name	CLI name (Provider.cfg)	Description and requirements
Name	name	The name of the authentication provider. You can have multiple providers for different domains. **Note** For Keystone, only one Keystone provider can be added for each ViPR Controller deployment.
Type	mode	The following types of authentication providers: • Active Directory • LDAP • Keystone — to register ViPR Controller as block storage service in Openstack (Keystone). For details see: CoprHD User Guide: Storage Orchestration for Openstack. If adding Active Directory or LDAP, use ad or ldap in Provider.cfg (CLI).
Description	description	Free text description of the authentication provider.
Domains	domains	Active Directory and LDAP allow administrators to organize objects of a network (such as users, computers, and devices) into a hierarchical collection of containers. ViPR Controller 3.0 and higher supports Keystone version 2. The domain name provided in ViPR Controller for Keystone is a dummy name. Domains are a collection of administratively defined objects that share a common directory database, security policies, and trust relationships with other domains. In this way, each domain is an administrative boundary for objects. A single domain can span multiple physical locations or sites and can contain millions of objects. A typical entry in this field of the authentication provider would look like this: `mycompany.com` If an alternate UPN suffix is configured in the Active Directory, the Domains list should also contain the

Table 3 Authentication provider settings (continued)

UI name	CLI name (Provider.cfg)	Description and requirements
		alternate UPN configured for the domain. For example, if `myco` is added as an alternate UPN suffix for `mycompany.com`, then the Domains list should contain both `myco` and `mycompany.com`.
Server URLs	url	ldap or ldaps (secure LDAP) with the domain controller IP address. Default port for ldap is 389 and ldaps is 636. • Usage: one or more of • ldap://‹Domain controller IP ›:‹port› (if not default port) or ldaps://‹Domain controller IP ›:‹port› (if not default port) • If the authentication provider supports a multidomain forest, use the global catalog server IP and always specify the port number. Default is 3268 for ldap, 3269 for ldaps. • Usage: ldap(s)://‹Global catalog server IP›:‹port› Keystone usage: http://‹IP Address›:‹port›/‹keystone version›. Both http and https are supported. For example, enter: http://[keystone host IP Address]:35357/v2 or https://[keystone host IP Address]:35357/v2
Manager DN	managerdn	Indicates the Active Directory Bind user account that ViPR Controller uses to connect to Active Directory or LDAP server. This account is used to search Active Directory when a ViPR Controller administrator specifies a user for role assignment, for example. For Keystone, this is the user with administrator role on Keystone and the OpenStack tenant to which the user belongs. For example: "username=admin,tenantname=admin" Requirement: This user must have **Read all inetOrgPerson information** in Active Directory. The InetOrgPerson object class is used in several non-Microsoft, Lightweight Directory Access Protocol (LDAP) and X.500 directory services to represent people in an organization. To set this privilege in Active Directory, open Active Directory Users and Computers, right click on the domain, and select **Delegate Control...** . Click **Next**, then select the user that you are using for

Table 3 Authentication provider settings (continued)

UI name	CLI name (Provider.cfg)	Description and requirements
		managerdn and click **Next**. The required permission is on the next screen "Read all inetOrgPerson information." Example: CN=Manager,CN=Users,DC=mydomaincontroller,DC=com In this example, the Active Directory Bind user is Manager, in the Users tree of the mydomaincontroller.com domain. Usually managerdn is a user who has fewer privileges than Administrator, but has sufficient privileges to query Active Directory for users attributes and group information. **⚠WARNING** **You must update this value in ViPR Controller if the managerdn credentials change in Active Directory.**
Manager Password	passwd_user	The password of the managerdn user. **⚠WARNING** **You must update this value in ViPR Controller if the managerdn credentials change in Active Directory.**
Disabled	disable	Select Disabled if you want to add the server to ViPR Controller but not immediately use it for authentication. (Regardless of whether this property is true, ViPR Controller validates that the provider's name and domain are unique.) **Note** Disable does not work for Keystone.
Automatic Registration and Tenant Mapping:	autoreg-coprhd-import-osprojects	For OpenStack (Keystone) orchestration only: • Import all tenants which are present in OpenStack into ViPR Controller. • Import all projects which are present in OpenStack into ViPR Controller. • Tag ViPR Controller tenants and projects with appropriate tenant and project IDs to create a logical mapping.
Group Attribute	groupattr	Indicates the Active Directory, or LDAP attribute that is used to identify a group. Used for searching the directory by groups. Example: CN

Table 3 Authentication provider settings (continued)

UI name	CLI name (Provider.cfg)	Description and requirements
		Example for Keystone: tenant_id **Note** Once this value is set for a provider, it cannot be changed, because of the tenants that are using this provider may already have role assignments and permissions configured using group names in a format using the current attribute.
Group Whitelist	whitelist	Optional. One or more group names as defined by the authentication provider. This setting will filter the group membership information that ViPR Controller retrieves about a user. • When a group or groups are included in the whitelist, it means that ViPR Controller will be aware of a user's membership in the specified group[s] only. Multiple values (one per line in ViPR Controller UI, comma-separated in CLI and API) and wildcards (for example MyGroup*,TopAdminUsers*) are allowed. • Blank value (default) means that ViPR Controller will be aware of any and all groups that a user belongs to. Asterisk (*) is the same as blank. Example: UserA belongs to Group1 and Group2. If the whitelist is blank, ViPR Controller knows that UserA is a member of Group1 and Group2. If the whitelist is "Group1", ViPR Controller knows that UserA is a member of Group1, but does not know that UserA is a member of Group2 (or of any other group). Use care when adding a whitelist value. For example, if mapping a user to a tenant is based on group membership, then ViPR Controller must be aware of the user's membership in the group. To restrict access to a tenant to users of certain group(s) only, one must: • add these group(s) to the tenant user mapping (using the CLI command `viprcli tenant add-group`), so the tenant is configured to accept only users of these group(s).

Table 3 Authentication provider settings (continued)

UI name	CLI name (Provider.cfg)	Description and requirements
		• add these group(s) to the whitelist, so that ViPR is authorized to receive information about them Note that by default, if no groups are added to the tenant user mapping, users from any groups are accepted, regardless of the whitelist configuration.
Group Object Class	groupobjectclasses	Required for LDAP All the object classes that represents the group in the LDAP schema When using the ViPR Controller UI, by default ViPR Controller will search the following group object classes, groupOfNames, groupOfUniqueNames, posixGroup, organizationalRole. However, you can remove the classes you know are not being used, or add custom classes that are being used in your LDAP schema. The default values are not provided in the ViPR Controller API, or CLI. You will need to enter the values manually if using the API or CLI. Provider.cfg is used for the creating the authentication provider. groupobjectclasses is the field to use in that Provider.cfg. UpdateProvider.cfg is used for editing the authentication provider the add-groupobjectclasses, remove-groupobjectclasses are the fields to use for editing.
Group Member Attributes	groupmemberattributes	Required for LDAP All the attributes of group object that represents members in the LDAP schema. When using the ViPR Controller UI, by default ViPR Controller will search for the following attributes within your LDAP group object classes, member, uniqueMember, memberUid, roleOccupant. However, you can remove the attributes you know are not being used, or add custom attributes that are being used in your LDAP schema. The default values are not provided in the ViPR Controller API, or CLI. You will need to enter the values manually if using the API or CLI. Provider.cfg is used for the creating the authentication provider. groupmemberattributes is the field to use in that Provider.cfg. When updating the UpdateProvider.cfg is used for editing the authentication provider. add-

Table 3 Authentication provider settings (continued)

UI name	CLI name (Provider.cfg)	Description and requirements
		groupmemberattributes, remove-groupmemberattributes are the fields to enter when editing.
Search Scope	searchscope	One Level (search for users one level under the search base) or Subtree (search the entire subtree under the search base).
Search Base	searchbase	Indicates the Base Distinguished Name that ViPR Controller uses to search for users at login time and when assigning roles or setting ACLs. Example: CN=Users,DC=mydomaincontroller,DC=com This example searches for all users in the Users container. Example: CN=Users,OU=myGroup,DC=mydomaincontroller, DC=com This example searches for all users in the Users container in the myGroup organization unit. Note that the structure of the searchbase value begins with the "leaf" level and goes up to the domain controller level--the reverse of the structure seen in the Active Directory Users and Computers UI.
Search Filter	searchfilter	Indicates the string used to select subsets of users. Example: userPrincipalName=%u **Note** ViPR Controller does not validate this value when you add the authentication provider. If an alternate UPN suffix is configured in the Active Directory, the Search Filter value must be of the format sAMAccountName=%U where %U is the username, and does not contain the domain name.
(This setting not available in the UI.)	maxpagesize	Value that controls the maximum number of objects returned in a single search result. This is independent of size of the each returned object. If specified must be greater than 0. Cannot be higher than the max page size configured on the authentication provider.

Considerations when adding Active Directory authentication providers

When you configure ViPR Controller to work with Active Directory, you must decide whether to manage several domains in a single authentication provider, or to add separate authentication providers for each domain.

The decision to add a single authentication provider, or multiple, depends on the number of domains in the environment, and the location on the tree from which the manager user is able to search. Authentication providers have a single search_base from which searches are conducted. They have a single manager account who must have read access at the search_base level and below.

Use the one-authentication-provider-for-multiple-domains if you are managing an Active Directory forest and these conditions are present: the manager account has privileges to search high enough in the tree to access all user entries, and the search will be conducted throughout the whole forest from a single search base, and not just the domains listed in the provider. Otherwise, configure an authentication provider for each domain.

Note that even if you are dealing with a forest and you have the correct privileges, you might not want to manage all the domains with a single authentication provider. You would still use one authentication provider per domain when you need granularity and tight control on each domain, especially to set the search base starting point for the search. Since there is only one search base per configuration, it needs to include everything that is scoped in the configuration in order for the search to work.

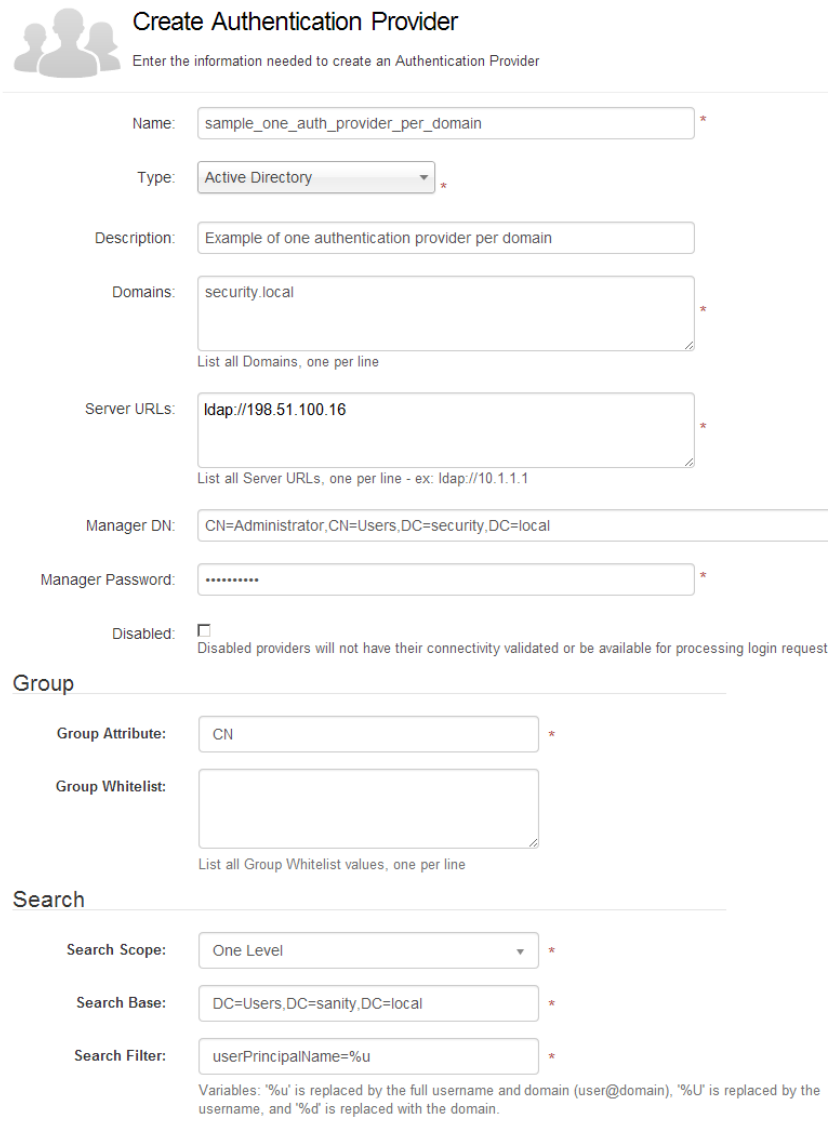
The search base needs to be high enough in the directory structure of the forest for the search to correctly find all the users in the targeted domains.

- If the forest in the configuration contains ten domains but you target only three, do not use a single provider configuration, because the search will unnecessarily span the whole forest, and this may adversely affect performance. In this case, use three individual configurations.
- If the forest in the configuration contains ten domains and you want to target ten domains, a global configuration is a good choice, because there is less overhead to set up.

Example of one Active Directory authentication provider per domain

In environments where the whole ViPR Controller virtual data center integrates with a single domain, or with several individually-managed domains, use one domain per authentication provider.

The following example creates an authentication provider for security.local.

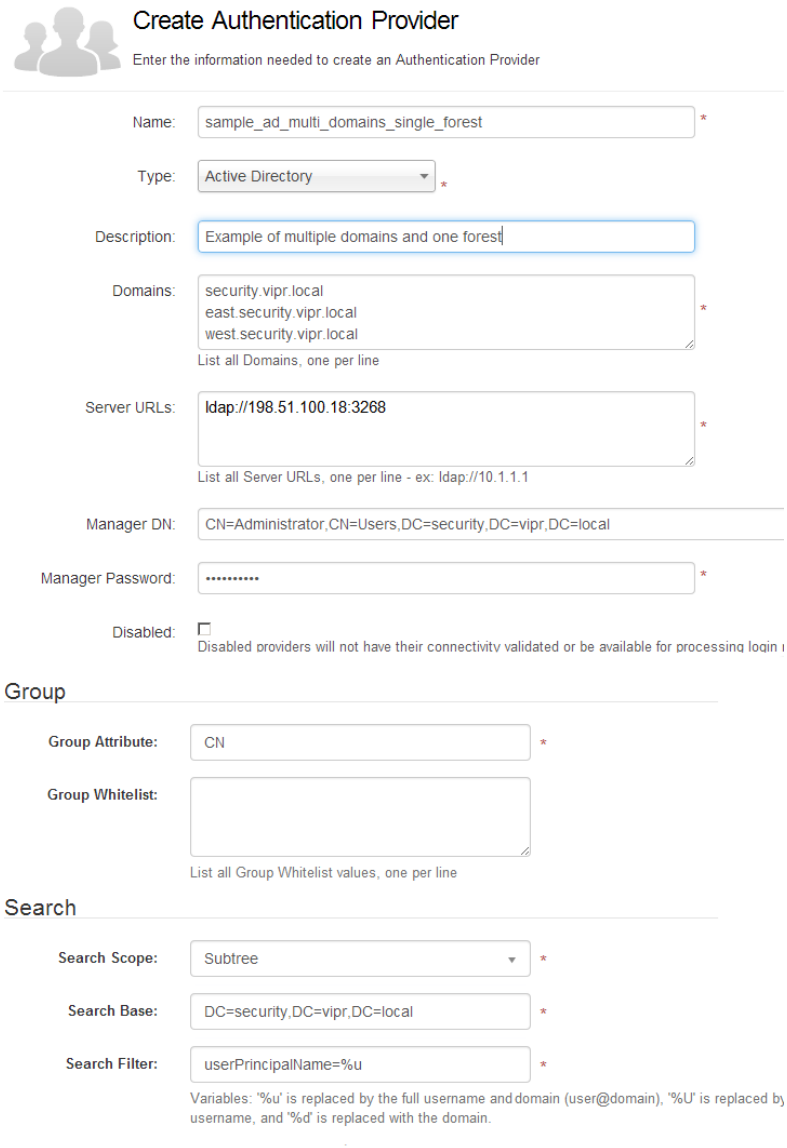


Example of one authentication provider managing multiple domains in a single forest

In this example, the environment includes a forest with one top domain and two subdomains. A single authentication provider manages all the domains.

In this example:

- The port for the Global Catalog (central repository of domain information for the forest) in the server URL is 3268.
- The domains to be managed are the top domain, security.vipr.local, and the subdomains east.security.vipr.local, and west.security.vipr.local.
- The manager user on the Global Catalog has read access on the search base.
- The search base is high enough in the hierarchy that it encompasses the subpaths to include east and west subdomains. In this case, the common path between users.security.vipr.local, users.east.security.vipr.local, and users.west.security.vipr.local is security.vipr.local.
- The search scope parameter is set to Subtree.



Creating or editing User Groups

User groups are used to group a set Active Directory (AD) or LDAP user attributes into a named entity that can be used as a group in tenant user mappings, role, and ACL assignments. This is not applicable for Keystone.

Before you begin

- ViPR Controller Security Administrators can create, list, view, edit and delete User Groups from ViPR Controller UI, CLI and REST API.
- ViPR Controller Tenant Administrators can list and view the existing User Groups from ViPR Controller UI, CLI and REST API.
- ViPR Controller Project Owner can list, and view the existing User Groups from ViPR Controller CLI and REST API.
- In geo-federated environment, user groups are only enabled once all VDCs are upgraded to 2.3.

Procedure

1. Go to the **Security** › **User Groups** page.
2. If editing an existing user group, click the group in the list, if creating a new group, click **Add**.
3. Complete the following options:

Option	Description
Name	Name of the User Group. User Group name must be unique for each group. Two User Groups with same name is not allowed. Do not use the @ character in the User Group name.
Domain	Domain in which the user group resides. Each User Group is associated with a Domain. Changing the domain of a User Group that is actively used by tenant user mapping or any ROLE or ACL assignments is not allowed. A user can only be included in one user group. Any attempt to add a domain with potentially overlapping users, will not be accepted by ViPR Controller.
Attribute	User Group attributes. Attribute keys in a User Group are unique. Adding two attributes with same key and same or different values will be combined into one attribute with all the values.

4. Click **Save** to save the User Group.

After you finish

Once the user group has been created it can used to assign the group of users in the user group, to tenant user mappings, roles, and ACL assignments.

Local Account Passwords

ViPR Controller has several local accounts that are used internally or for administration and service. You can change these passwords from the ViPR Controller user interface, **Security**, **Local Passwords** page.

Table 4 Local accounts

Account	Use	ViPR Controller roles and privileges	Initial password
root	Used for initial setup and for testing, evaluation, and troubleshooting, when most privileged account is needed. Same account as root user on the Controller VMs.	System Administrator, System Monitor, Security Administrator, System Auditor, Tenant Administrator	ChangeMe

Table 4 Local accounts (continued)

Account	Use	ViPR Controller roles and privileges	Initial password
svcuser	For read-only support	System Monitor and can access ViPR Controller UI, and has ssh access to the ViPR Controller VMs.	ChangeMe
sysmonitor	Used by SolutionPack to collect ViPR Controller data	System Monitor	ChangeMe
proxyuser	Used internally to run operations on behalf of a user	Proxy User (internal role, not assignable)	Not applicable

Local account password policy

The password policies can be defined and enforced by Security Administrators from the **General Configuration** page, **Password** tab. For details see: Setting ViPR Controller local user password policy. on page 30

Changing the local account passwords

This operation requires the Security Administrator role in ViPR Controller.

The new password must conform to the site-specific local password policy defined by the Security Administrator, by default ViPR Controller sets the following password validation rules:

- 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
- not in last 3 change iterations

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

An alternative way to change the local passwords is, when logged in as a local user, you can change password from the top level of the ViPR Controller 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.

Property	Description
	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**.

Updating EMC ViPR Controller Keystore

EMC ViPR Controller generates a self-signed certificate on startup, but you can generate a new self-signed certificate at **Security** › **Keystore**. If you want ViPR Controller to use a CA-signed certificate, you can upload it here.

Any change to these properties causes ViPR Controller to reboot.

Generate self-signed certificate
Check this option to instruct ViPR Controller to generate a new self-signed certificate.

Private key and Certificate chain
If you have a certificate authority (CA-) signed certificate to upload, or you generated a self-signed certificate externally, upload the private key and certificate chain here. Both uploads are required.

Note that when obtaining a CA-signed certificate, you must provide all IP addresses and FQDNs of the ViPR Controller nodes, and of the VIP for the ViPR Controller instance.

Note the following requirements for the private key:

- Must be an RSA Private Key.
- The key length must be at least 2048 bits.

Create and import a CA-signed certificate into ViPR Controller

You can create a certificate signed by a certificate authority (CA) and import it into ViPR Controller. The following process includes the steps from Certificate Signing Request (CSR) to final private key and CA signed certificate (.crt) ViPR Controller import.

Before you begin

- A certificate should not have a password. Remove any password if necessary. The example procedure below includes a step to remove a password from a certificate.
- The examples in this procedure use Windows IIS 7 as the CSR generator.

Procedure

1. Generate a CSR using Windows IIS 7 or other CSR application. The CSR should be associated with and created using the FQDN of the ViPR virtual IP address (also known as the VIP or the public virtual IP address). The CSR is a text file that begins ---BEGIN CERTIFICATE REQUEST-- and ends with --END CERTIFICATE REQUEST--.
2. Send the CSR generated by step 1 to a certificate authority (CA) such as RSA, VeriSign, etc.

   Follow the CA's directions for completing the certificate request. The CA will send back a group of CA-signed crt files.
3. Complete the certificate signing request, using the CSR application that you used in step 1.

You may need to complete this step on the host where the CSR originated.

4. Once complete, export the private key from the CSR-generating tool. A password may be required; if so, it will be removed in a subsequent step.

   If generated by IIS 7, the private key will be a pfx file in PKCS #12 format. Check the format if you are using a different CSR generator.

5. Convert the private key to PEM format without certs:

   ```
   openssl pkcs12 -in iis_pfx_pkey -nocerts -nodes -out
   new_pem_format_pkey_nocerts
   ```

6. Check the new pkey file:

   ```
   openssl rsa -in new_pem_format_pkey_nocerts -check
   ```

   Output from the above command should begin with one of the following: `BEGIN RSA PRIVATE KEY` or `BEGIN PRIVATE KEY`.

7. Remove the password from the PEM-formatted private key file created above:

   ```
   openssl rsa -in pem_format_pkey_file -out
   new_pem_without_pw_pkey
   ```

8. Check the new pkey file:

   ```
   openssl rsa -in new_pem_format_pkey_nocerts -check
   ```

9. Use the ViPR Controller UI to upload the converted private key and hostname crt file to the ViPR Controller keystore at **Security** › **Keystore**.

   This step requires the Security Administrator role in ViPR.

   ViPR Controller nodes will execute a rolling reboot after this step.

   At the next ViPR Controller UI login, the web browser will show the trusted certificate lock icon. If not, clear the browser cache, then close the browser and launch a new browser session.

Validating connection to LDAPS server in EMC ViPR Controller

By default ViPR Controller accepts all security certificates from all resources, but if you want to verify the pre-loaded certificates, or certificates that you upload to ViPR Controller, set **Accept All Certificates** to False.

Use **Security** › **Trusted Certificates** to change the default behavior and add and remove certificates.

Upload either a self-signed certificate, or if the LDAPS server has a certificate signed by a certificate authority (CA), upload the certificate for the CA. The certificate must be PEM-encoded.

Uploading a certificate requires the Security Administrator role.

CHAPTER 3

Managing ViPR Controller virtual data centers in different geographical locations

This chapter includes the following topics:

- Overview of a ViPR Controller multisite (GEO-federated) configuration 36
- Disconnecting and reconnecting aViPR Controller VDC in a geo federation 39
- Upgrading a ViPR Controller VDC in a GEO (multi-site) federation 41

Overview of a ViPR Controller multisite (GEO-federated) configuration

In a ViPR Controller multisite configuration, each VDC is configured on different ViPR Controller instances, and then each ViPR Controller instance is linked together, which allows you to control multiple ViPR Controller virtual data centers (VDC) in different locations.

Note

A GEO multisite environment is not compatible with a System Disaster Recovery environment, and vice versa. These two environments are mutually exclusive, and are not supported at the same time.

The multisite capabilities of ViPR Controller provide:

- Security configuration propagated across ViPR Controller instances
- Single sign-on access across ViPR Controller instances
- Tenants and projects are defined once and are accessible across ViPR Controller instances
- Consolidated monitoring of resources across ViPR Controller instances through ViPR Controller SolutionPack

However, the multisite capabilities do not provide:

- Provisioning (or any user service) initiated from one ViPR Controller instance, to be executed in another ViPR Controller instance.
- ViPR Controller failover from one site to another.

Planning the deployment of a multisite ViPR Controller

Deploying a multisite ViPR Controller configuration consists of installing a ViPR Controller instance for each virtual data center (VDC), and then linking each instance together. Review the following information before linking ViPR Controller instances together.

- Minimum of 2 VDCs is required. Maximum is 8.
- Verify that each VDC in the multisite configuration meets the requirements of a single-site ViPR Controller VM, in addition to the several requirements specific to multisite. Refer to the ViPR Controller Support Matrix.
  Node counts do not need to match; you can link a 3+2 configuration to a 2+1, for example.
- Each VDC must be licensed.
- Port 7100 (used for inter-VDC communication by Cassandra database) must be open at each site.

Linking different versions of ViPR Controller VDCs in a multisite environment

It is important to understand how ViPR Controller supports linking different versions of VDCs:

- Linking VDCs with different service packs and patches is allowed.
- Linking VDCs with different hotfixes on same release is allowed.
- ViPR Controller will tolerate linking up to two different versions of ViPR Controller VDC. However, when linking two VDCs at different versions:

  - You can only link a newer version of a ViPR Controller VDC to an earlier version.
  - You cannot link an earlier version of ViPR Controller VDC to a more recent version.
  - You cannot link ViPR Controller 3.0 VDC to any older version due to new IPSec communication in 3.0.
- Linking considerations for ViPR Controller 3.0:
  - You can upgrade from an older ViPR Controller version to 3.0. If you are upgrading a multi-VDC setup, the procedure is to upgrade each VDC to 3.0, and after upgrading the last VDC to 3.0, ViPR Controller will reboot all VDCs to enable IPsec on all of them. While the upgrade is in progress, there is a time where the federation will have older version VDCs and a ViPR Controller 3.0 VDC running simultaneously. This is allowed. IPsec will not be enabled in the entire federation until the last VDC is upgraded to 3.0.
  - While upgrading multiple VDCs, you cannot have more then two different ViPR versions running in the federation (such as 2.3, 2.4 and 3.0). The maximum allowed is two different versions. It is recommended that you bring all your VDCs up to version 3.0 as soon as possible, so that all VDCs will be IPsec-enabled.

Linking multiple ViPR Controller virtual data centers in a multisite configuration

Each VDC in the multisite configuration requires IP connectivity to the other VDCs. The procedure below describes how to link up multiple ViPR Controller virtual data centers in a geo-configuration. You can link up to 8 VDCs.

Before you begin

- You need a non-local account on the initial VDC (that is, an account from the authentication provider) that has the Security Administrator role. The root user cannot be used for the main step of linking to another VDC.
- You need to know the network virtual IP address (or its FQDN) for each ViPR Controller VDC that you are adding.
- The VDC that you link to (VDC2, VDC3, etc.) must have no data, namely:
  - No physical assets
  - No virtual assets

Procedure

1. Deploy ViPR Controller, and each ViPR Controller virtual data center as an individual VDC. For deployment steps refer to the *ViPR Controller Installation, Upgrade, and Maintenance Guide*, which is available from the ViPR Controller Product Documentation Index .

   Be sure you add an authentication provider to the initial VDC (VDC1) because some of these steps cannot be done by root.

   Note

   In a multisite configuration, changing the IP addresses of ViPR Controller nodes is not supported.

2. Log in to VDC1 as a user with the Security Administrator role (not root user).
3. Log in to VDC2 as root and select **Virtual Assets** › **Virtual Data Centers** › **Download Certificate Chain**. This operation downloads a file that you will upload to VDC1 in a subsequent step.

4. Remain on VDC2, and copy VDC2's secret key from **Virtual Assets** › **Virtual Data Centers** › **Secret Key**.

   In the next step you will paste the secret key when adding VDC2 to VDC1.

5. Now go back to VDC1 as a user with the Security Administrator role (not root), and add VDC2: **Virtual Assets** › **Virtual Data Centers** › **Add**.

   a. Assign a name and enter a description.

   b. Enter the public virtual IP address of the VDC you are adding.

      Note the following limitations:

      - Adding an IPv4 system to an IPv4 system, and vice versa: Supported.
      - Adding an IPv6 system to an IPv6 system, and vice versa: Supported.
      - Adding an IPv4 system to an IPv6 system, and vice versa: Not supported.
      - Adding an IPv6 system to a dual stack system, and vice versa: Not supported.
      - Adding an IPv4 system to a dual stack, and vice versa: Supported. Both systems are treated as IPv6 systems for inter-VDC connections; normal dual-stack is used for API calls, UI access.
      - Adding a dual stack to a dual stack system: Supported. Both systems are treated as IPv4 systems.

   c. Paste the secret key from the VDC that you copied earlier.

   d. Browse to and add the certificate chain file from VDC2 that you downloaded earlier.

   e. Log off VDC2 and close the browser window or browser tab for VDC2.

   f. On the ViPR Controller UI for VDC1, click **Save**.

   At this point, a rolling reboot of VDCs in the configuration is initiated. After several minutes:

   - VDC status is Connected.
   - The authentication provider that was added to VDC1 is visible to VDC2 and users on VDC2 can authenticate through the authentication provider that was added to VDC1. Authentication providers that you add later are also visible to all linked VDCs.
   - Tenant roles from VDC1 automatically carry over to users on VDC2.
   - Virtual data center roles (Security Administrator and the System * roles) must be separately assigned to users on VDC2; they do not carry over automatically.
   - Tenants and projects created on one VDC are accessible from the other VDC.
   - Tenant user mappings and project ACLs are common across the linked VDCs.
   - The root user no longer has any tenant roles, nor project ACLs, and in the **Security** menu, the root user can only access the **VDC Role Assignments**.
   - Only domain users with Security Administrative privileges can perform ViPR Controller Tenant, Project, or Security operations in a new VDC. The domain users must each be assigned the Security Administrator role in each VDC.

6. At this point, assets can be added to VDC2 as described in *ViPR Controller User Interface Virtual Data Center Configuration Guide*, which is available from the ViPR Controller Product Documentation Index .

7. To add additional VDCs, repeat the above steps.

8. Each new VDC only needs to be added once, to the original VDC. Once added information about the new site(s) will be automatically propagated.

After you finish

Note that backups of a standalone VDC made with the ViPR bkutils backup utility cannot be used to restore the VDC after the VDC has become part of a multisite configuration. For this reason, you should consider backing up the VDCs immediately after linking them.

Disconnecting and reconnecting aViPR Controller VDC in a geo federation

If a virtual data center in a geo federation becomes inaccessible, then all write operations to geo-replicated resources will fail. In this case you should disconnect the inaccessible VDC, so that writes can continue to geo-replicated resources via the other VDCs in the federation.

After disconnecting the VDC to perform the necessary repairs, you can then return it to the federation with the Reconnect operation.

If you decide that a VDC should not be part of the federation, use the Delete operation, which permanently removes the VDC from the geo database, and the VDC cannot be added back. After deletion the VDC continues to function as an isolated VDC.

Disconnecting a virtual data center

Disconnect the inaccessible VDC so that writes can continue to the other VDCs in the federation.

- This operation requires the System Administrator role in ViPR Controller.
- All VDCs in the federation must be at ViPR Controller version 2.1 or higher.
- The target VDC must be inaccessible by all living VDCs in the federation.
- You cannot run the disconnect operation on the local VDC.
- In the case of a planned outage, before issuing the Disconnect operation, either shut down and power off the VDC, or close the socket port 4443.
- All VDCs in the federation must be in the Stable state.

The viprcli command for disconnecting a VDC is `viprcli vdc disconnect -name` *`vdc_name`*

The REST API method is `POST /vdc/{id}/disconnect`.

To disconnect using the ViPR Controller UI:

1. Log in to an accessible VDC in the federation as a user with the System Administrator role (not root user).
2. Go to **Virtual Assets** › **Virtual Data Centers**
3. Select the disconnected VDC and click **Disconnect.**

Note

The ViPR Controller UI that is running on the disconnected VDC will show its status as Connected, even after it was disconnected. You can see the actual status by viewing the disconnected VDC's status from a ViPR Controller UI running on a different VDC in the federation.

Reconnecting a virtual data center

You can reconnect a disconnected virtual data center to return it to the geo federation.

- This operation requires the System Administrator role in ViPR Controller.
- All VDCs in the federation must be at ViPR Controller version 2.1 or higher.
- The target VDC must be reachable from all living VDCs in the federation.
- You cannot run the Reconnect operation on the target VDC.
- After the reconnect operation, allow several minutes, in general, for data to be propagated to the target VDC.
- All VDCs in the federation must be in the Stable state.

The viprcli command for reconnecting a VDC is `viprcli vdc reconnect -name vdc_name`

The REST API method is `POST /vdc/{id}/reconnect`.

To reconnect using the ViPR Controller UI:

1. Log in to an accessible VDC in the federation as a user with the System Administrator role (not root user).
2. Go to **Virtual Assets** › **Virtual Data Centers**
3. Select the disconnected VDC and click **Reconnect.**

Deleting a virtual data center

You can delete a virtual data center from a geo federation. This operation will remove it entirely from the ViPR Controller internal database. Once you delete a virtual data center from a geo federation, it cannot be added back. If you want to remove a VDC from a federation temporarily, you should disconnect it instead of deleting it.

After you delete a virtual data center from the geo federation, each VDC works independently; tenants and projects are no longer shared, and single sign-on through a shared authentication provider is no longer available.

- This operation requires the System Administrator role in ViPR Controller.
- All VDCs in the federation must be at ViPR Controller version 2.0 or higher.
- The target VDC must be reachable.
- All VDCs in the federation must be in the Stable state.
- You cannot run the Delete operation on the local VDC.

The viprcli command for deleting a VDC is `viprcli vdc delete -name vdc_name`

The REST API method is `POST /vdc/{id}/delete`.

To delete using the ViPR UI:

1. Log in to an accessible VDC in the federation as a user with the Security Administrator role (not root user).
2. Go to **Virtual Assets** › **Virtual Data Centers**
3. Select the VDC and click **Delete**.

Upgrading a ViPR Controller VDC in a GEO (multi-site) federation

Best Practices for upgrading a ViPR Controller VDC in a GEO (multi-site) federation

General Recommendations

- Upgrade one VDC at a time, then move on to next VDC.
- ViPR Controller can continue to operate while running two different versions across sites, but it is best practice to finish upgrading the remaining VDCs as soon as possible, to take advantage of any new feature that may require that all VDCs are on same target version.

Upgrading to ViPR Controller 3.0

- Upgrade one VDC at a time, then move on to next VDC.
- The new IPSec communication, which is new and the default in 3.0, will not be enabled until the last VDC in the federation is upgraded to 3.0. After the last VDC is upgraded, IPsec communication will be enabled automatically, at which time all VDCs will reboot simultaneously. Therefore, make sure you plan in advance for a brief outage of all VDCs in the environment.