zadara

zStorage VPSA Object Storage

Release 20.01

Zadara

Jan 18, 2022

CONTENTS

CHAPTER

ONE

PREFACE

This documentation presents information specific to Zadara Storage Object Storage product.

1.1 Intended Audience

This document is intended for end users and storage administrators subscribers of Zadara's Enterprise Storage-as-a-Service product VPSA Object Storage, in both public and private clouds.

1.2 Document History

Date	Revision	Description
Jul 2016	A	Initial revision for 16.05 Release
Nov 2016	B	Few updates: Object size, Isolated Environment, Custom Domain
May 2017	C	Updates for Release 16.05-SP2 New HTML Format
Nov 2017	D	Updates for Release 17.11
Jul 2018	E	Updates for Release 18.07
Aug 2019	F	Updates for Release 19.08
Mar 2020	G	Updates for Release 20.01

CHAPTER

TWO

INTRODUCTION

What is Object Storage?

Object Storage is an alternative way to store, organize and access units of data. It provides a reasonable balance between performance and functionality versus simplicity and scalability. Object Storage enables a minimal set of features: store, retrieve, copy, and delete objects. These basic operations are done via REST APIs that allow programmers to work with the objects. The HTTP interface to Object Storage systems allows fast and easy access to the data for users from anywhere in the world.

Object Storage vs. Block and File Storage

Object Storage is much more scalable than file storage because it is vastly simpler. Objects are not organized in hierarchical folders, but in a flat organization of containers or buckets. Each object is assigned a unique ID or key. Their keys, regardless of where the objects are stored, retrieve objects. Access is via APIs at the application level, rather than via OS at the file system level. As a result, Object Storage requires less metadata, and less management overhead than file systems. This means Object Storage can be scaled out with almost no limits. Object Storage is easier to use than block storage and overcomes the limitation of fixed size LUNs. It also removes file system limitations such as the folder size or path name length. Unlike block or file, Object Storage does not use RAID for data protection. It simply keeps a number of copies of each object.

VPSA Object Storage is Zadara's object storage service. It is provided on Zadara clouds, side by side with the VPSA that provides block and file storage services.

2.1 VPSA Object Storage Components

2.1.1 Provisioning Portal

The Zadara Provisioning Portal is your gateway to the Zadara Storage ecosystem through which you can create, view, and modify your VPSA configurations on multiple Clouds that Zadara Storage offers.

2.1.2 Virtual Controller

A Virtual Controller (VC) is a Virtual Machine with dedicated CPUs & RAM, which runs the VPSA Object Storage IO stack and control stack. The number of VC's in a configuration is determined by the number of drives assigned, starting with a minimal configuration of 2 VCs, and can grow to hundreds. Each VC supports up to 12 drives. VCs are automatically provisioned as needed.

There are 2 services running in each VC: Proxy Layer and Storage Layer. The Proxy Layer is the interface to the users or the application using the data objects. The storage Layer is responsible for storing the objects on the drives, and updating the metadata in the databases.

The VCs also provide a web management interface and REST API endpoints for management and control, as well as authentication and load balancing services.

2.1.3 Dedicated Drives

The Zadara Storage Cloud Orchestrator assigns dedicated drives for each each VPSA. The drives are provisioned from different Storage Nodes (SNs) for maximum redundancy and performance. Each drive is exposed as a separate iSCSI target from the SN and is LUN masked only to the VPSA's VCs. Your QoS is guaranteed, because neighbors, with provisioned drives adjacent to yours, cannot access your drives, impact your performance, or compromise your privacy and security.

2.2 VPSA Object Storage Profiles

Zadara have predefined three Object Storage Profiles, a profile should be chosen according to the required usable capacity and the required Data Protection Policy.

In the table below you will find the main differences between the Object Storage profiles.

Table 1: **Object Storage Profiles**

	Standard	Premium	Premium Plus
Max Usable Capacity (TiB)	1,024	4,096	61,440
Min Drives per Object Storage	4	24	48
Load Balancer	Internal	Internal	Elastic LB (ZELB)

Table 2: **Object Storage Data Protection Policies**

	Standard	Premium	Premium Plus
Erasure Coding Support	×	✓	✓
2 Way Mirror	✓	✓	✓
3 Way Mirror	✓	✓	✓
Erasure Coding 4+2	×	✓	✓
Erasure Coding 6+3	×	✓	✓
Erasure Coding 6+2	×	✓	✓
Erasure Coding 9+3	×	✓	✓
MZ Erasure Coding 4+2	×	✓	✓
MZ Erasure Coding 9+3	×	✓	✓

✔ **Note:** The availability of Data Protection policies may differ in different Zadara deployment, as it is dependent on the amount of nodes the cloud is structured from.

Table 3: Minimal drives required for Data Policy creation

	Standard	Premium	Premium Plus
2 Way Mirror	4	24	48
3 Way Mirror Protection	6	36	72
Erasure Coding 4+2	×	36	72
Erasure Coding 6+3	×	36	72
Erasure Coding 6+2	×	48	96
Erasure Coding 9+3	×	48	96
Multizone Erasure Coding 4+2	×	72	144
Multizone Erasure Coding 9+3	×	96	192

Table 4: Minimal drives required for Data Policy Expansion

	Standard	Premium	Premium Plus
2 Way Mirror	2	2	24
3 Way Mirror Protection	3	3	36
Erasure Coding 4+2	×	6	36
Erasure Coding 6+3	×	9	36
Erasure Coding 6+2	×	8	48
Erasure Coding 9+3	×	12	48
Multizone Erasure Coding 4+2	×	12	72
Multizone Erasure Coding 9+3	×	24	96

Standard Object Storage profile For general purpose workloads and low capacity (up to 1PB of usable capacity at creation time).

Premium Object Storage For intermediate deployments and workload (up to 4PB of usable capacity at creation time) and extended data policy protection (including Erasure Coding). Zadara have created a dedicated profile in order to allow a structured deployment with additional allocated resources. The Premium Object Storage is structured from:

1. Dedicated Controllers - a pair of Virtual Controller that manages the Object Storage Ring, it will not perform any Proxy or Storage operations.
2. Proxy+Storage Virtual Controllers with extended resources to manage high volume of client connections and Object Storage operations.

Premium Plus Object Storage For high scale deployments, up to 60 PB of usable capacity at creation time, Along with extended Data Protection offering the Premium Plus Object Storage is structured from:

1. Dedicated Controllers - a pair of Virtual Controller that manages the Object Storage Ring, it will not perform any Proxy or Storage operations.
2. Zadara Elastic Load Balancer (ZELB) - will be created by default.
3. Proxy+Storage Virtual Controllers with extended resources to manage high volume of client connections and Object Storage operations.

✔ **Note:** Currently, Changing the VPSA Object Storage profile post creation is not supported.

2.3 VPSA Object Storage Administration

2.3.1 VPSA Object Storage Hierarchy

The Object Storage system organizes data in a hierarchy, as follows:

- **Account** (also referred to as Tenant). Represents the top-level of the hierarchy. Usually created by the service provider. The account admin owns all resources in that account. The account defines a namespace for containers. Containers in two different accounts, might have the same name. Accounts are also used to control users access to objects and containers.
- **Container** (Also referred to as Bucket). Defines a namespace for objects. Objects in two different containers, may have the same name. Any number of containers can be created within an account. In addition to containing objects, you can also use the container to control access to objects, and you can set a storage policy that each container uses.
- **Object**. Stores data content, such as documents, images, and so on.

2.3.2 VPSA Object Storage Users and Roles

There are four types of Roles assigned to VPSA Object Storage Users:

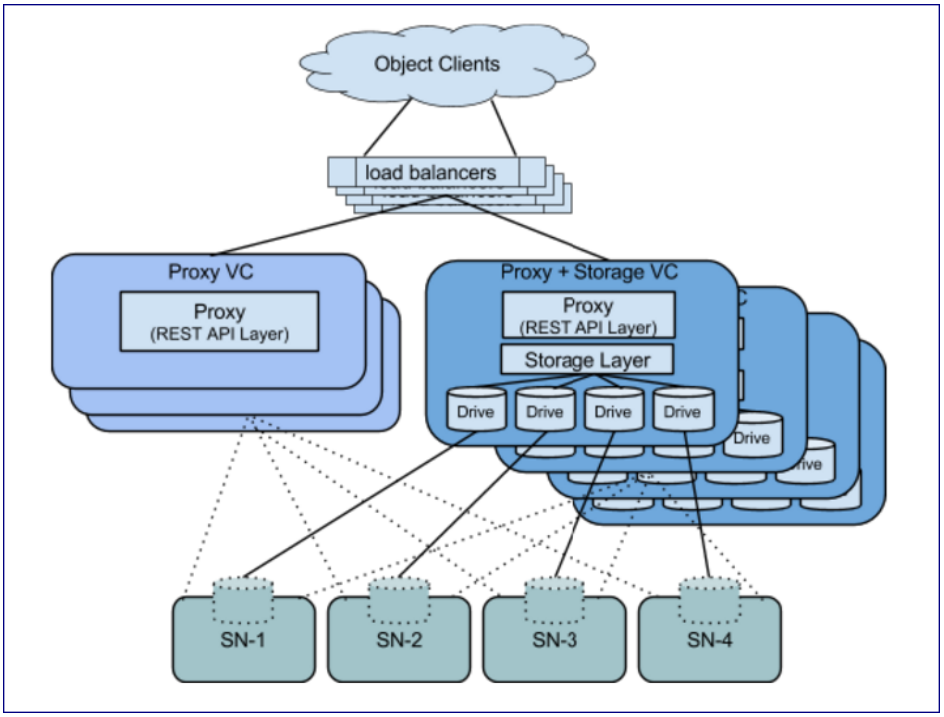
- **VPSA Object Storage Admin** responsible for the administration of the VPSA Object Storage. The user (registered in Zadara Provisioning Portal) that orders the VPSA Object Storage becomes its Administrator. By default, the VPSA Object Storage is created with one account (VPSA Object Storage administrator account) and the VPSA Object Storage Administrator is a member of this account. VPSA Object Storage Administrators can add other users with the same role. VPSA Object Storage Administrator is a super-user with privileges to create accounts and users of any role. Users with VPSA Object Storage Administrator role can define policies, add/ remove drives and assign drives to policies. Users with VPSA Object Storage Administrator role can perform containers and objects operations across accounts. VPSA Object Storage administrator is also responsible for the VPSA Object Storage settings (like IP addresses, SSL certification, etc.), and has access to the metering and usage information.
- **VPSA Object Storage Admin - Read Only** a dedicated Read-Only account for cross-accounts monitoring and reporting purposes. The Read-Only role is available for the zios_admin account only. A Read-Only user will have access to the VPSA Object Storage RestAPI, however it will not have data access. The user role is designated for monitoring and reporting purposes, such as:
  - Performance monitoring
  - Capacity monitoring
  - Usage reports & billing automation
- **Account Admin** can create an account (using the Self Account Creation Wizard) and can manage their own accounts. They can perform any user management and containers/objects operations.
- **Member** can do object storage operations according to the permission given by the account administrator, within the limits of that account. These operations include create/delete/list containers and create/delete/list objects.

User authentication is done against an internal VPSA Object Storage Users database.

2.4 VPSA Object Storage Architecture

VPSA Object Storage architecture is a scale out cluster of Virtual Controllers that together provides the service. The number Of VC's is automatically determined as needed to serve the capacity and performance of the system.

2.4.1 VPSA Object Storage Structure



This figure shows high level logical view of VPSA Object Storage. It is a Virtual Object Store cluster, with two distinct layers:

- "Storage Layer" that manages individual disks
- "Proxy - REST API Layer" that provides REST API front-end of the Object Storage.

The typical VC runs both functions and is referred to as "Proxy+Storage" VC. It is possible to add VCs with the Proxy layer only. There are referred to as "Proxy" VC.

Each VPSA Object Storage is typically composed of several Proxy+Storage VCs and optionally one or more Proxy VCs with each VC having dedicated CPU/RAM/networking. Proxy+Storage VC's consume raw Physical drives (like SAS/SATA/SSD) exposed from Storage Nodes (SNs). Proxy+Storage and Proxy VCs run Object Storage Stack that provide Amazon S3 and Swift REST API interface.

Capacity & Performance can independently scaled up/down by adding/removing disks and proxy-VCs respectively. VPSA Object Storage typically has a set of load-balancers to distribute REST API traffic across the Proxy REST API Layers. Each VPSA Object Storage natively being multi-tenant allows creation of multiple accounts within it, with each account having multiple users who can work with the object interface (GET/PUT objects).

A single Zadara Storage Cloud can host several virtual object stores and this makes it truly disruptive and unique, as each VPSA Object Storage has entirely provisioned resources of CPU/RAM/networking/disks & runs the object stack in isolated Virtual Machines (i.e. there is no sharing of resources anywhere across VPSA's) thereby providing complete performance and fault isolation.

2.4.2 Virtual Controller

VPSA Object Storage Virtual Controller (VC) provides multi-tenant, protected object storage.

Virtual Controller Responsibilities:

- Query Cloud Controller and Storage Nodes for resource assignments and changes.
- Provide data protection for objects - 2-way protection, 3-way protection & Erasure Coding protection with objects distributed across multiple SN's disks
- Provide Authentication/Authorization framework with which individual accounts/users can be managed and these account/users being able to work with objects within their account
- Provide Amazon S3 and Swift API's on object front-end with support for internal & external HTTPS termination
- Provides capability to scale up/down capacity with addition/removal of drives with corresponding automatic addition/removal of proxy+storage VCs
- Provide capability to scale REST API performance with addition/removal of proxy-VCs
- Automatically reconfigure/redistribute object data across available disks on addition/removal of disks, failure/recovery
- Provide management GUI and REST API to manipulate the system entities and also to work with the object store
- Provide metering visibility in object request flows, capacity trend utilization
- Billing based on capacity/throughput usage for each of the tenants
- Provide internal load balancing service
- Provide HA architecture for VC failure resiliency

2.4.3 The Ring

A ring represents a mapping between the names of entities stored on disk and their physical location. There are separate rings for accounts, containers, and one object ring per storage policy. When any components need to perform any operation on an object, container, or account, they need to interact with the appropriate ring to determine its location in the cluster.

The objects rings are stores in each Policy. The accounts and containers rings are stored in dedicated Policy named Metadata Policy.

One of the Virtual controllers (called Ring Master), runs the Rings, in addition to its other responsibilities. In case of failure of the Ring Master, another VC (called Ring Slave) will take its place.

2.4.4 VPSA Object Storage Fault Domains

In order to ensure the Object Storage survival in case a complete storage node is lost, the data is distributed between Fault Domains. "Object Storage Fault Domains" are manually populated for the cloud Storage Nodes by the cloud admin.

Object Storage VCs are created in "VC-Sets" according to the desired policy protection type (2-way/3-way/Erasure Coding protection). Each VC in a Set is created in a different Fault Domain.

Drives are added to the the Object Storage in sets as well. And allocated only to VCs within the same Fault Domain.

CHAPTER

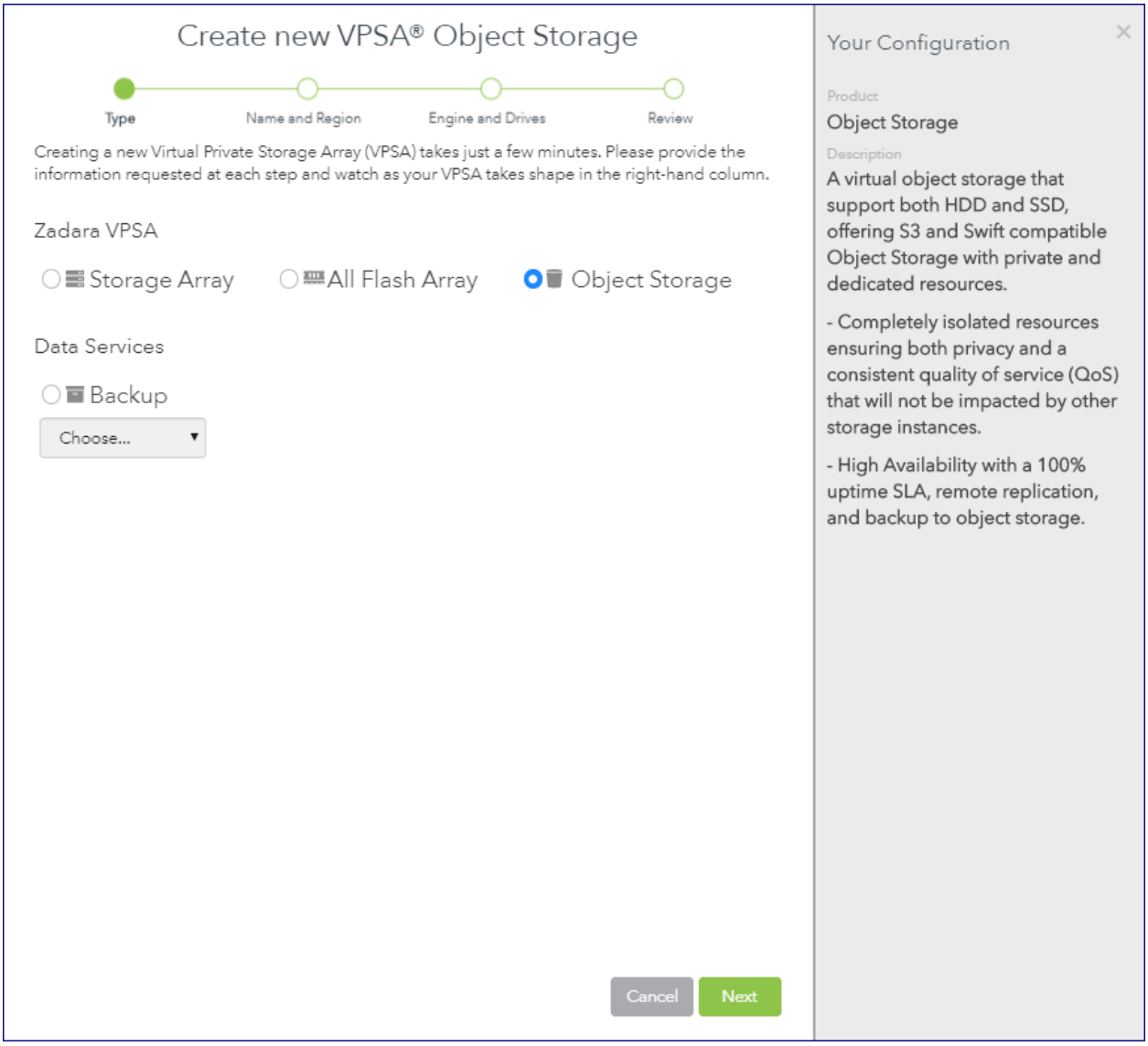
THREE

GETTING STARTED

This chapter contains step-by-step instructions to both create a VPSA Object Storage and then to configure its storage properties

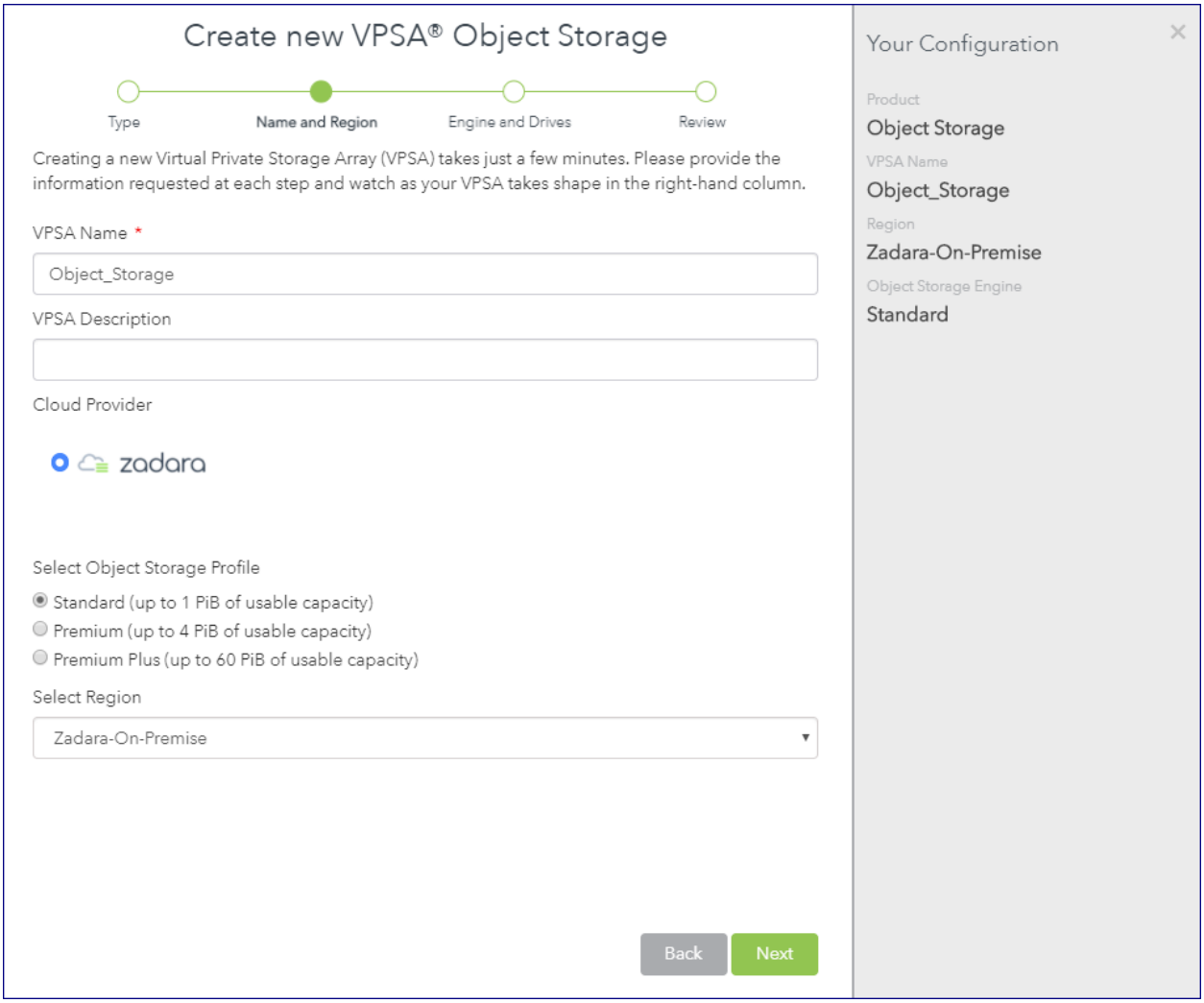
3.1 Registering a Zadara Account & Creating a VPSA Object Storage

- Go to https://manage.zadarastorage.com/register/ and complete the registration form to create a new Zadara Account.
- Go to your **Zadara Provisioning Portal** at https://manage.zadarastorage.com, or at your private cloud, using your username/email & password, and press Create Zadara Storage VPSA
- In the creation wizard select Storage Array, Flash Optimized or Object Storage. VPSA Storage Array and Flash Optimized creation are described in the VPSA Storage Array User Guide.



✔ **Note:** This example uses the Zadara Storage provisioning portal https://manage.zadarstorage.com . In case you have your own Zadara Cloud deployment, replace the example URL with your own URL or IP address of your Provisioning Portal.

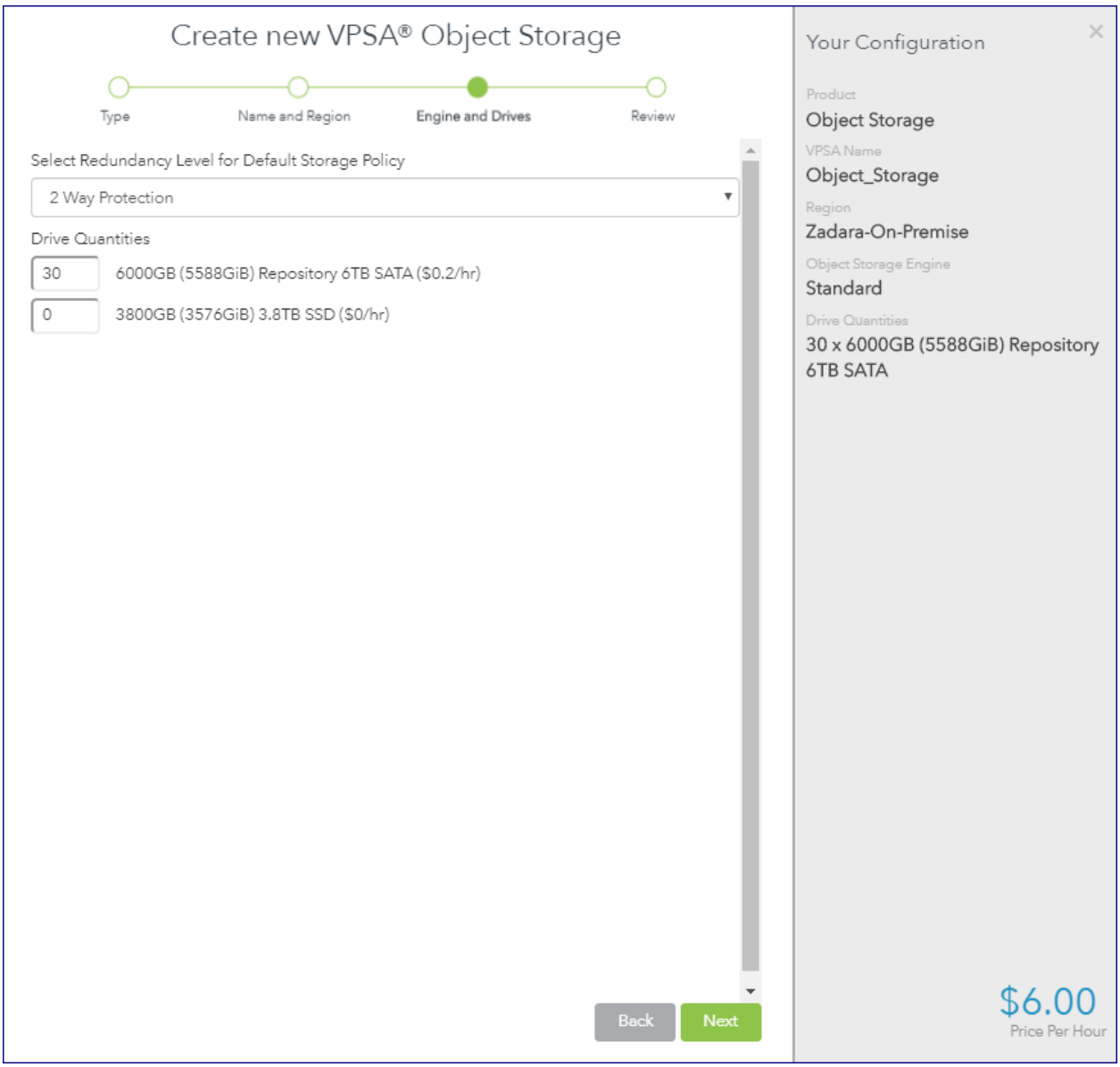
- If VPSA Object Storage was selected The following screen will be displayed:



Enter the following mandatory fields:

- **VPSA Name** Give the Object Store a name. This is how it will appear in the Cloud Console and in the GUI. If you are planning on having multiple VPSA Object Storage configurations, you might want to give it as detailed a name as possible.
- **VPSA Description** free text description.
- **Cloud Provider** Select the Cloud or Co-lo where your compute instances are hosted.
- **Object Storage Profile** Standard/Premium/Premium Plus For addition information about the VPSA Object Storage profiles, see VPSA Object Storage Profiles
- **Select a Region** Select the Cloud Provider region where you want the system to reside. For best performance the servers using the object storage should be in the same region in order to establish connectivity, however this is not a must. Available Regions depend on which Cloud Provider you select.
- **High Availability Protection Zone** In cloud locations that provide protection zones, select in which zone the new VPSA Object Storage will be built. Zones depend on which Cloud Provider and region you select. Selecting the "Multizone HA" option, will provision the VPSA Object Storage across the two availability zones.

Press Next



- **Redundancy Level supported**

  Single zone VPSA Object Storage

  1. 2-Way Protection
  2. Erasure-Coding 2+1 or 4+2 (using 3 Fault Domains), 6+2 or 9+3 (using 4 Fault Domains)

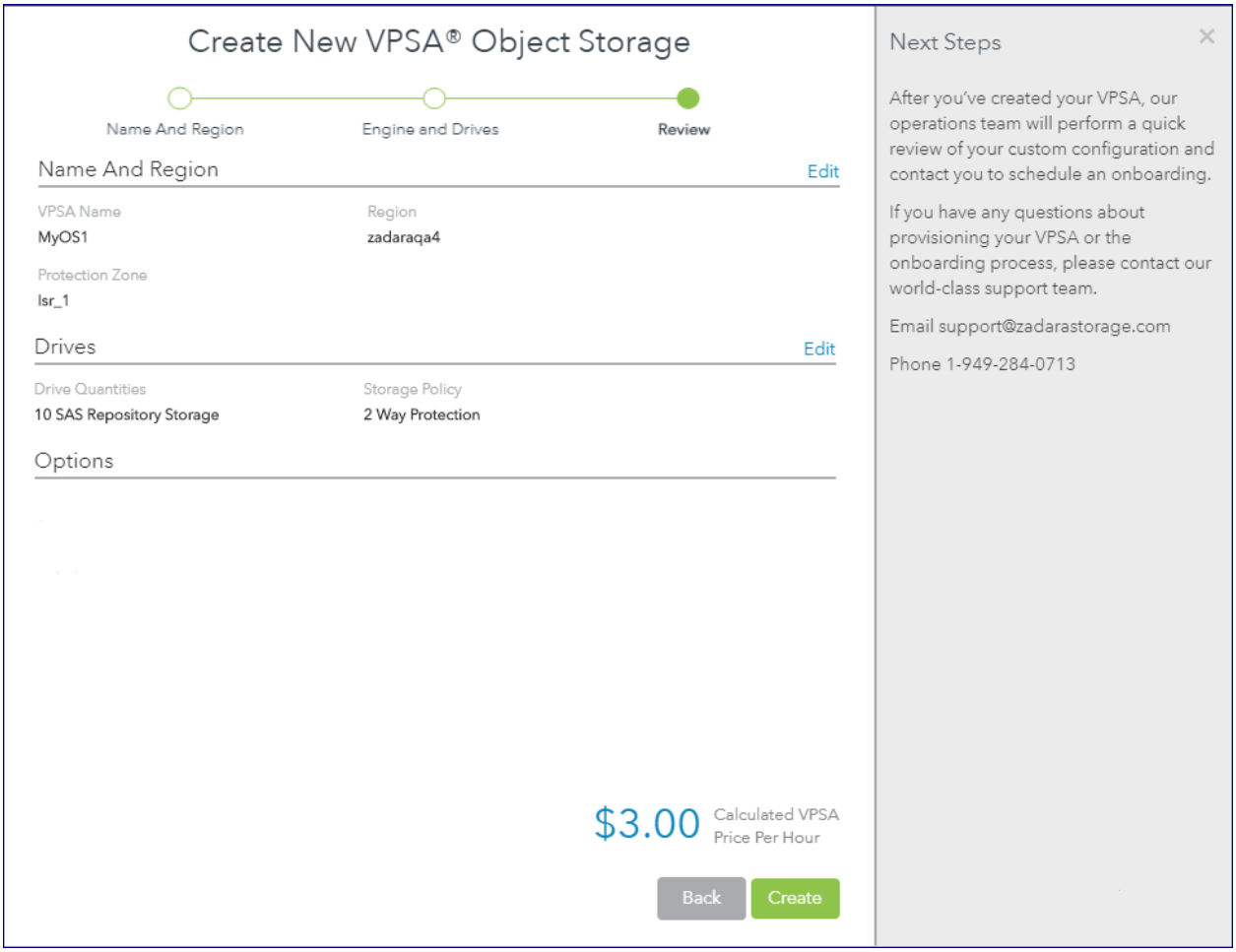
  Multizone HA VPSA Object Storage - all the above policies support MZ deployment, please refer to VPSA Object Storage Profiles for additional information and requirements for Object Storage Data policies.

  With 2-way it keeps 2 copies of each object. Erasure coding protection is done in 2+1 and 4+2 configuration that requires 50% extra capacity for redundancy. 6+2 or 9+3 configuration requires 33% extra capacity for redundancy.

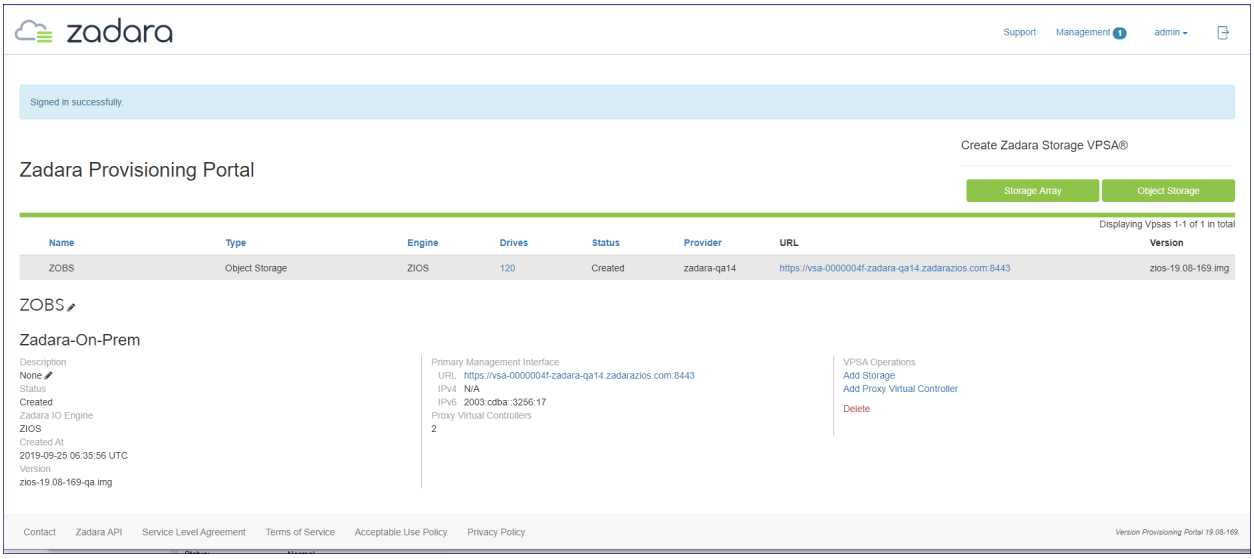
- **Drive Quantities** Select the type and number of Drives that you would like to allocated to your VPSA Object Storage.
  - The Zadara Cloud orchestrator allocates dedicated drives.
  - Drives are allocated from as many different Storage Nodes as possible to provide max redundancy and availability.

- The number of drives that can be selected depends on the protection level required.
  - For 2 way protection, 4 - 24 drives can be added to the system in one operation.
  - For erasure coding, 3 - 48 drives can be added to the system in one operation.
- For 2-way protection an even number of drive must be selected.
- For Erasure Coding protection the number of drives must be divisible by the EC redundancy policy (e.g for 4+2 protection, the number of drives must be divisible by 6).

Press Next



- Once you have completed selecting the above VPSA characteristics, review the displayed summary. You can click Edit to modify your previous selections. Press the Create button to confirm the VPSA creation request. The requested VPSA Object Storage will appear in the "Awaiting Approval" list.
- Completing the VPSA Object Storage creation requires the approval of a Zadara Storage Cloud admin. Once approved, the new system only takes a few minutes to launch. During that time the VPSA Object Storage status will be changes to "Launching".
- Once ready, you'll receive an email with a temporary password to the registered email address.
- The VPSA Object Storage web management interface is accessible using the "Management Address":



- Use your registered username or email address, and the temporary password, to enter the management interface. You will be immediately prompted to set a new password for your VPSA Object Storage Admin account. It is recommended to enable MFA (Multi-Factor Authentication) in order to add an additional layer of security to your account.

Congratulations! You have a new VPSA Object Storage provisioned and ready.

The newly created VPSA Object Storage already has a single account named “zios_admin”, and you are the only user defined “admin” with the role of “VPSA Object Storage Admin”. You can now manage your VPSA Object Storage - create containers and start uploading and serve objects, or create additional accounts and users for others to use.

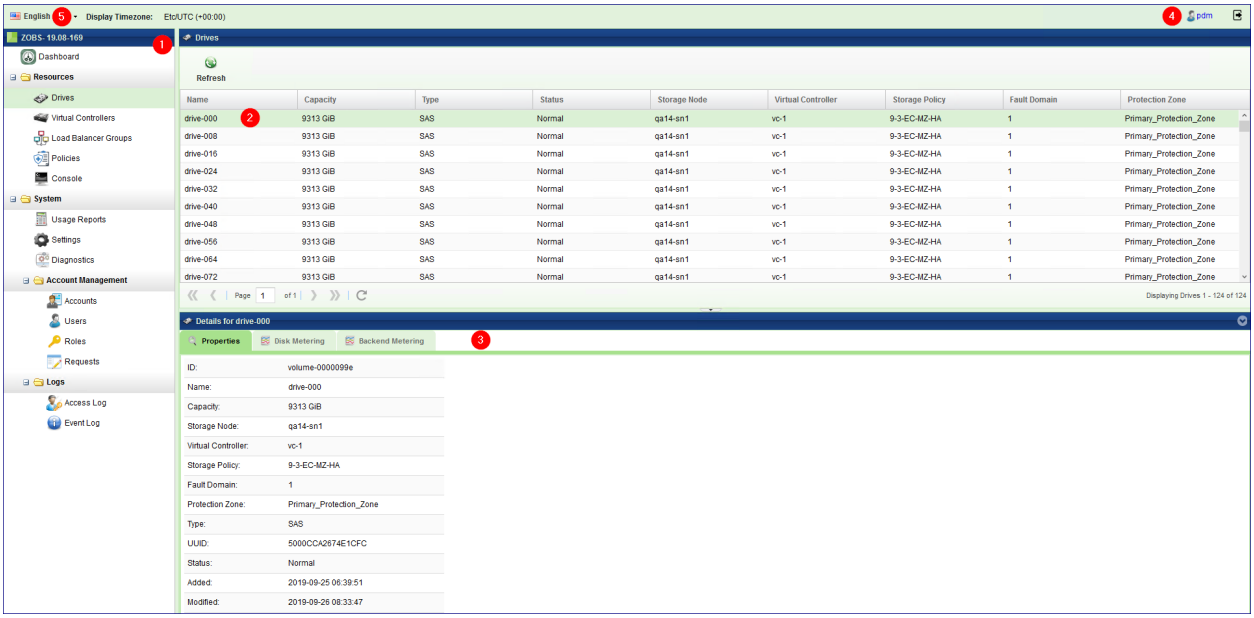
The following sections describe in detail the various capabilities and services of your VPSA Object Storage.

3.2 Understanding the VPSA Object Storage User Interface

The web management interface changes according to the context of the user that logs in. The User’s Role determines the actions, available for each specific user.

This is the web management interface as seen by the **VPSA Object Storage admin** account users. It includes:

- Dashboard
- Resources Management (Drives, Policies, Reports, VPSA Object Storage Console)
- System Settings
- Accounts Management (Accounts, Users, Roles, Requests)
- Logs (Access Log, Event Log)

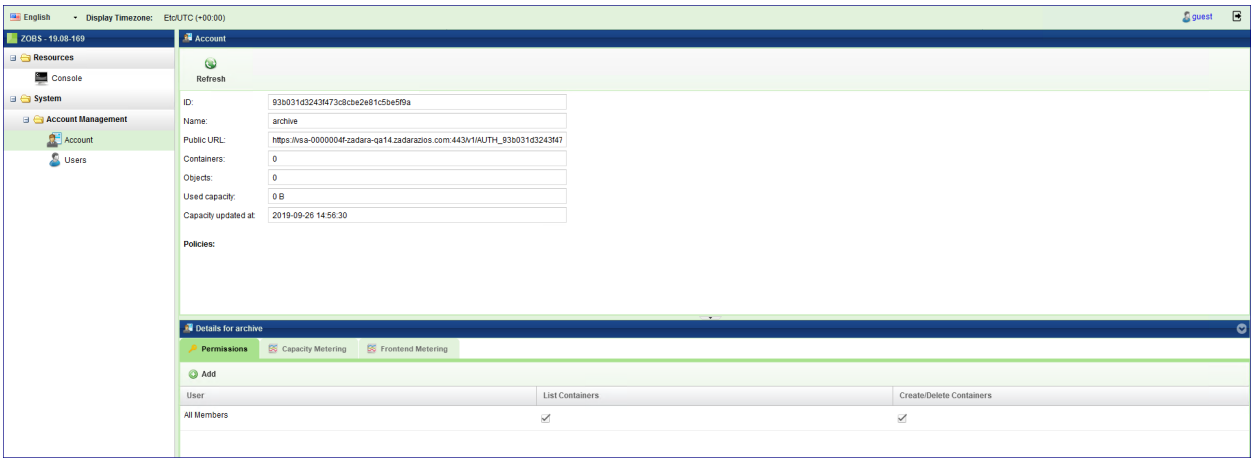


The VPSA Object Storage web management interface provides full management capabilities and control of your VPSA Object Storage, for VPSA Object Storage Admins. It provides full management and control of the Account level to the Account admins. It contains the following main components (as numbered in the above screenshot):

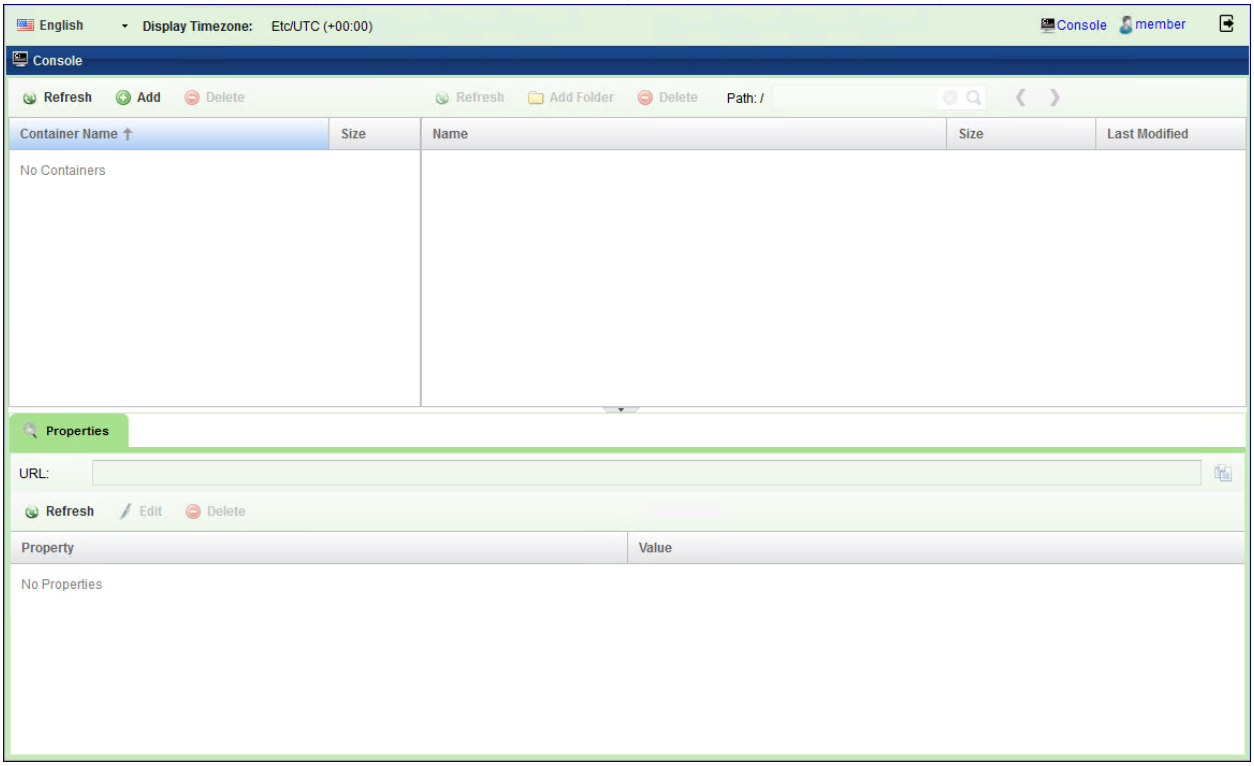
1. **Main Navigation Left Panel** – Traverse through the various entities. The selected entity is highlighted.
2. **The Center Pane** – Displays a list of objects from the selected entity type (e.g. drives in the above screenshot example), and for each object it displays its main properties.
3. **The South Pane** – Displays detailed information regarding the selected object. All objects have at least 2 tabs:
    - **Properties** – Detailed properties of the object selected.
    - **Metering** – Typically IO workload metering info.
    - **Related Objects – Lists of other objects related to the** selected object.
4. **Logged-in user** – Displayed at the upper right corner. Clicking this link opens the user's information screen as described under the User Information (Managing Users section).
5. **Selected Language** – Displayed at the top right corner. You can use this drop down to change the displayed language. Available display languages are: - English - Japanese - Korean - Deutsche - Portuguese

This is the web management interface as seen by an **Account Admin**. It includes:

- Users Management
- VPSA Object Storage Console



Account Member logged in user will have the VPSA Object Storage Console view only.



CHAPTER

FOUR

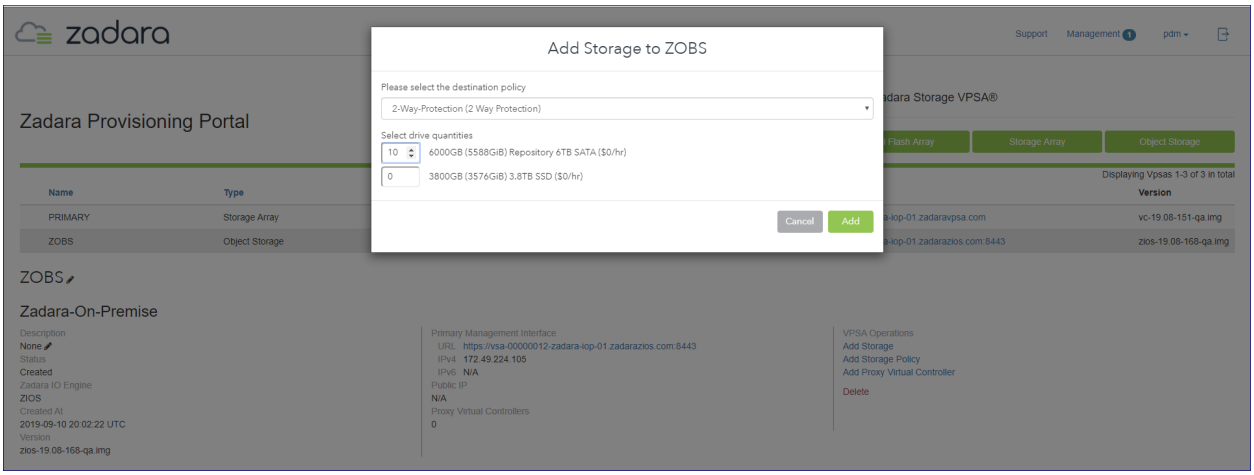
PROVISIONING YOUR OBJECT STORAGE

You create, delete, and manage the resources composing your VPSA Object Storage via Zadara's **Provisioning Portal**.

This section describes the available operations in the Provisioning Portal (https://manage.zadarastorage.com).

4.1 Adding Drives to an Existing Storage Policy (VPSA Object Storage Admin)

To add Drives to your VPSA Object Storage, go to the Zadara Provisioning Portal, select the VPSA Object Storage, and then press the Add Storage link.

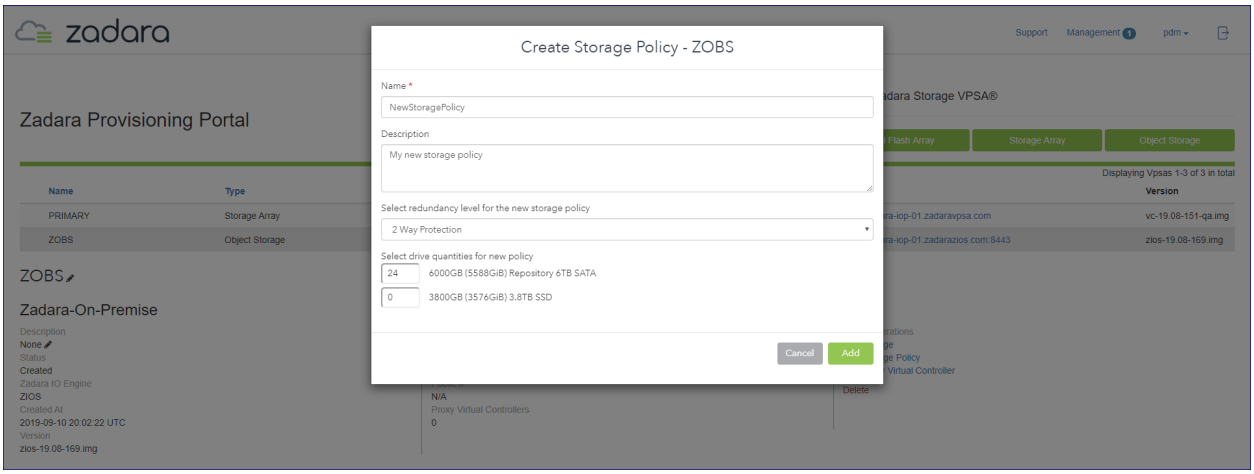


- Select the Storage Policy for which you add the drives
- Select the number of Drives of the relevant type you wish to add to your VPSA Object Storage, and press Add. The number of drives added to the "Storage Policy" should match its characteristics, as described in the Getting Started section of this guide.
- This operation requires the approval of a Zadara Storage Cloud Admin. Once approved, you'll see the number of Drives in the Provisioning portal updated according to the request. The new drives will be automatically assigned to the selected Storage policy.

Note: Drives can't be added more frequently than every 8 hours to let the Storage Policy to re-balance.

4.2 Adding Storage Policy (VPSA Object Storage Admin)

To add Storage policy to your VPSA Object Storage, go to the Zadara Provisioning Portal, select the VPSA Object Storage, and then press the Add Storage Policy link.



- Give the new Policy a name and description.

> **Note:** Objects names can be up to 128 chars long and can contain letters and digits, dashes "-" and underscores "_"

- Select the protection level for this Storage Policy.
- Select the number of Drives of the relevant type you wish to assign to this Storage Policy, and press Add. The number of drives added to the "Storage Policy" should match its characteristics, as described in the Getting Started section of this guide.
- This operation requires the approval of a Zadara Storage Cloud Admin. Once approved, you'll see the new Policy created in the VPSA Object Storage web management interface.

4.3 Assigning Public IPs (VPSA Object Storage Admin)

For security and privacy reasons, by default you cannot access the VPSA Object Storage from the public Internet. The Front-End IP address, used for management (via GUI and REST API) and for data IO workload (S3/Swift API), is allocated on the Zadara Storage Cloud "Front-End" network 10/40 GbE which is routable only from the Cloud Servers network. As this is an internal IP address, servers outside of your cloud network will not be able to reach this IP address. This means you cannot access your VPSA Object Storage from the Internet or any network with no routing to the Front-End network.

To assign a Public IP address to your VPSA Object Storage, for Internet inbound connectivity, open the Provisioning Portal, select the VPSA Object Storage, and click the Assign Public IP link. This operation requires Zadara Storage Cloud Admin approval. Once approved, the IP address will be added to the VPSA Object Storage characteristics. And In the VPSA Object Storage web management interface, under Settings > General > Public IP. To remove it, simply click the Remove Public IP link in the Zadara Provisioning Portal.

4.4 VPSA Object Storage In an Isolated Environment

VPSA Object Storage can be created in an isolated environment where no Internet access is available.

VPSA Object Storage includes SSL object web server in addition to the web management interface SSL server, therefore it is created with a default SSL certificate issued to zadarazios.com domain name.

In an isolated environment, there is no automatic DNS registration of the zadarazios.com domain name in DNSimple, hence the certificate will not match the FQDN of the VPSA Object Storage. In this case, you may encounter with the following behavior:

- Object operations, including backup from VPSA Storage Array to VPSA Object Storage, may fail (as the VPSA Object Storage certificate cannot be verified).
- VPSA Object Storage Console will not be available.
- Accounts will be created without permissions

There are two approaches to adjust the VPSA Object Storage within an isolated environment:

- Option 1 - Domain name for the FE interface **(Recommended)**

  1.a Use the default zadarazios.com domain name

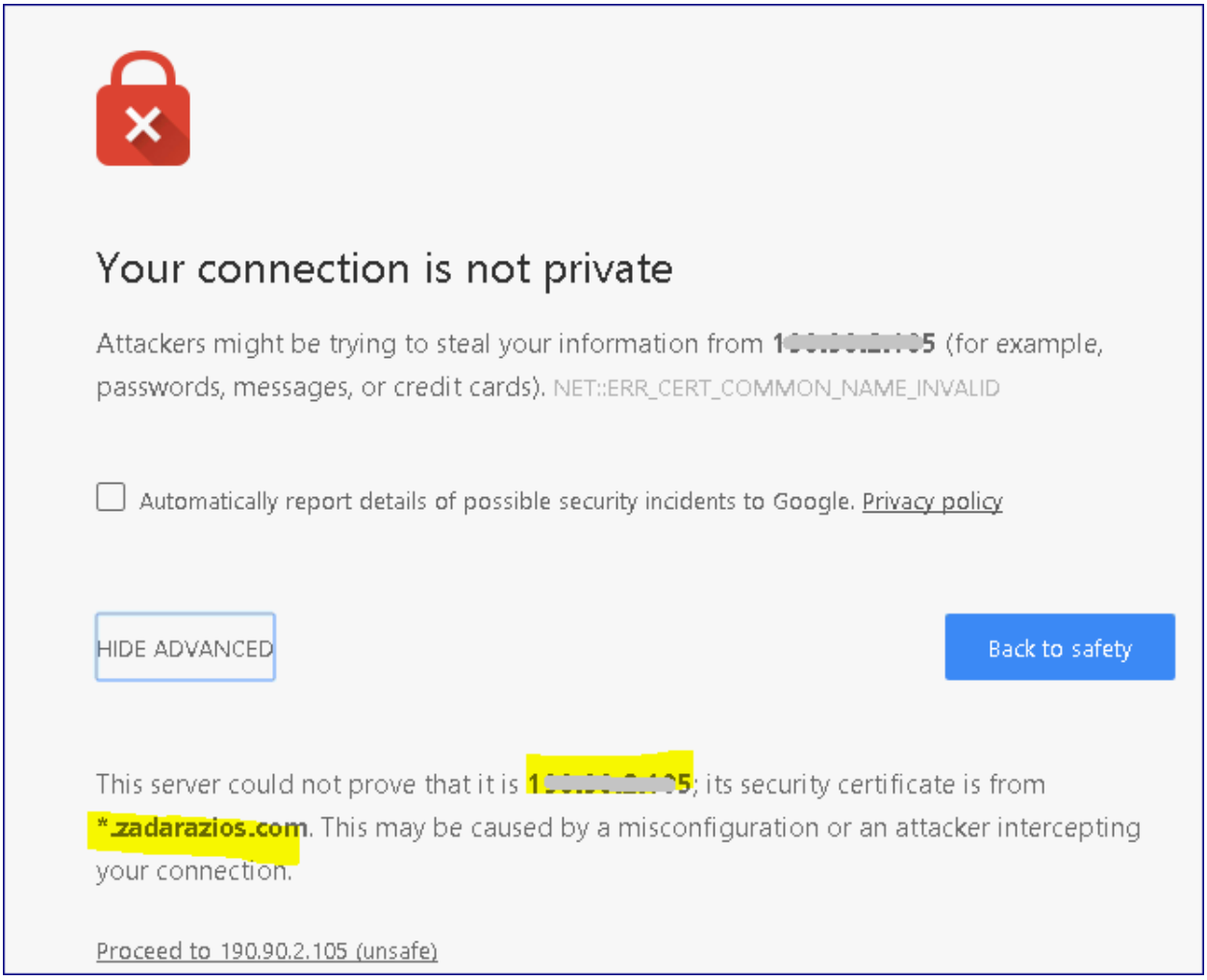
  1.b Use a custom domain name

- Option 2 - IP address for the FE interface

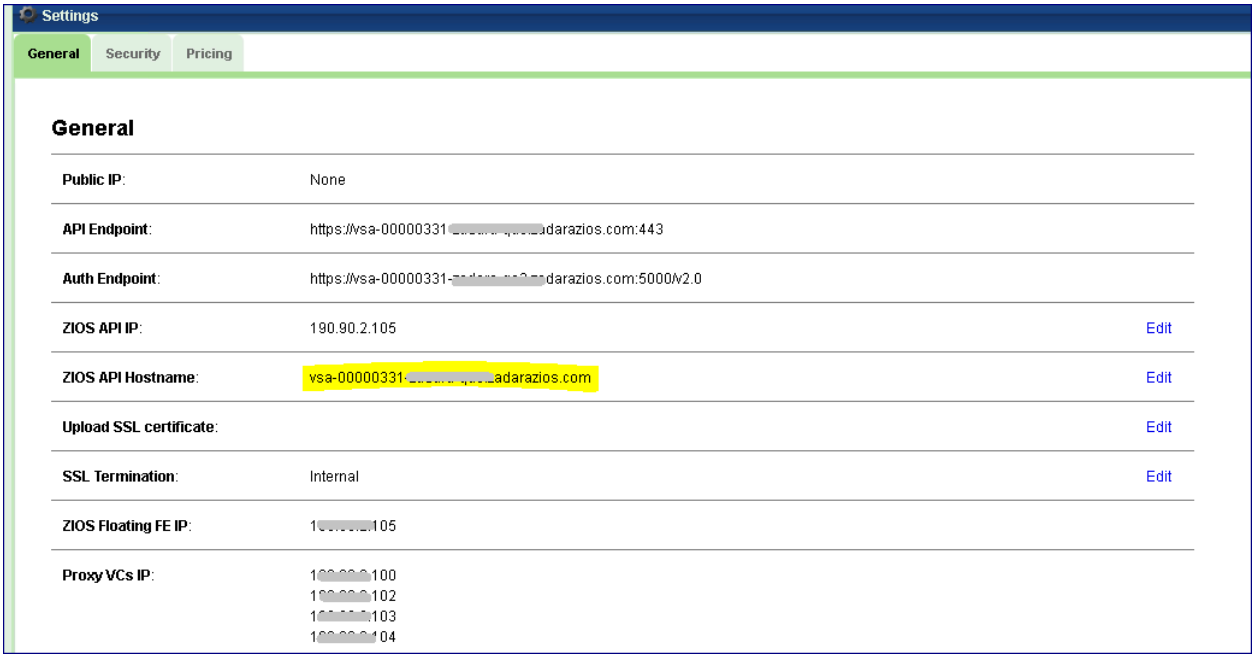
4.4.1 Option 1.a: Default VPSA Object Storage Domain Name

Once VPSA Object Storage is created, proceed as following:

- Browse to the Management Interface IP address (as displayed in the provisioning portal), and approve the “insecure” certificate which does not match the URL IP:



- Login to the web management interface with initial credentials and follow the prompt to replace the initial password.
- Go to Settings page and copy the VPSA Object Storage API Hostname, which is the default domain name.

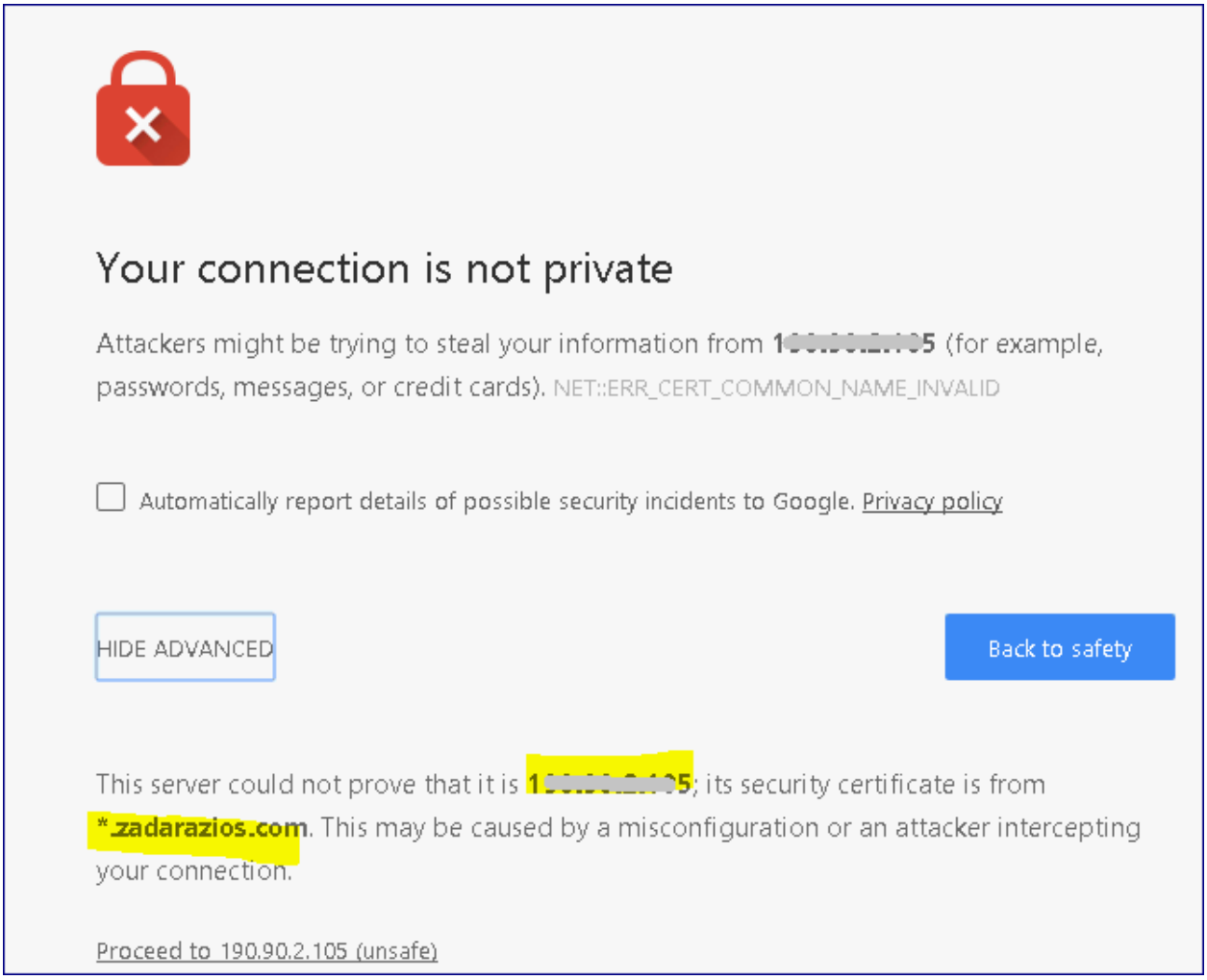


- Manually register the default domain name with VPSA Object Storage FE IP in your internal DNS server.
- Now, GUI connection and object operations should be done against the VPSA Object Storage default domain name which matches the name in the SSL certificate the VPSA is holding.

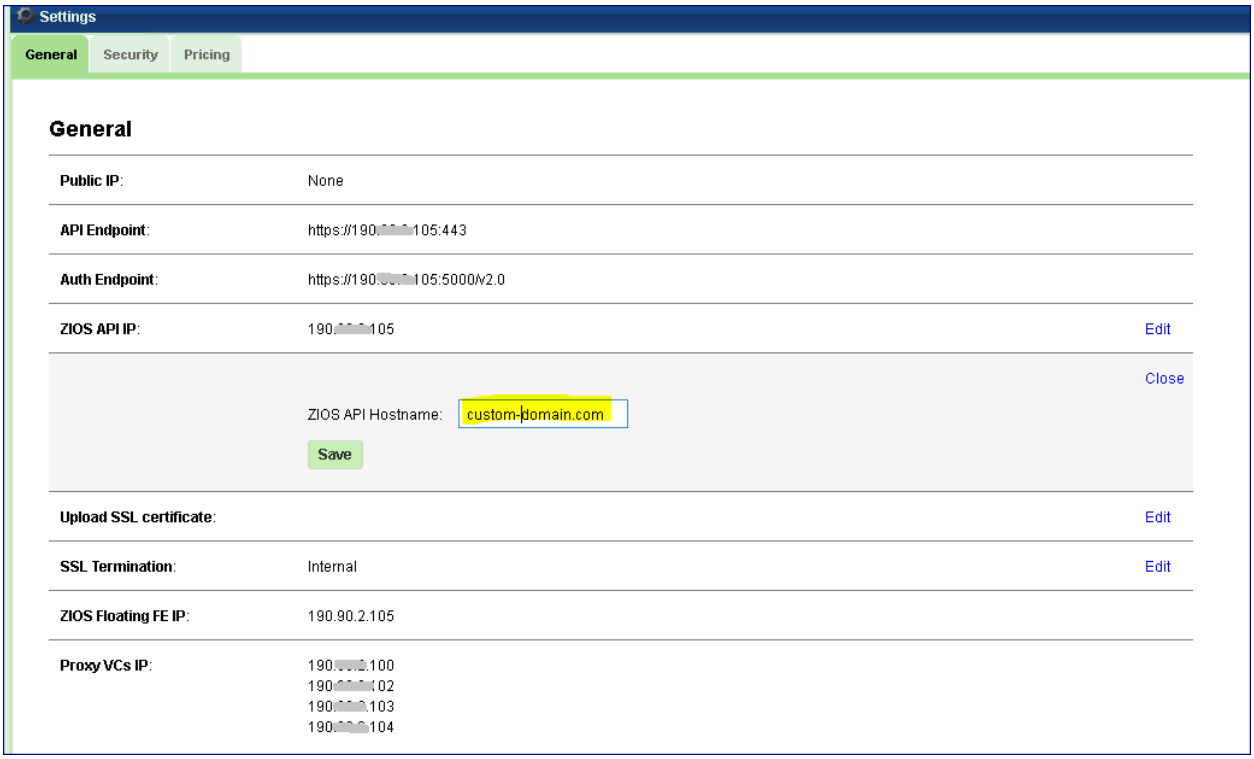
4.4.2 Option 1.b: Custom VPSA Object Storage Domain Name

Once VPSA Object Storage is created, proceed as following:

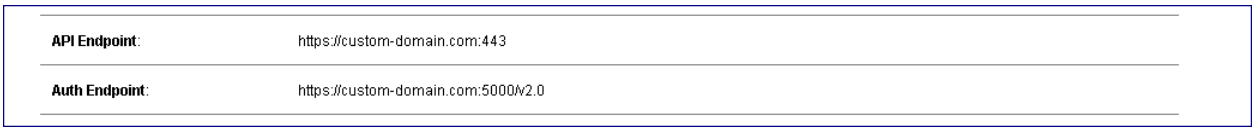
- Browse to VPSA Object Storage GUI IP (as appears in the provisioning portal), and approve the “insecure” certificate which is not matching the URL IP:



- Login to the GUI with initial credentials and change password
- Go to Settings page and edit the VPSA Object Storage API Hostname, remove the default domain name and set a custom domain name as required:



- The GUI will be reloaded and you will need to re-login, once logged in you will see in the Settings page that the API and Auth Endpoints were changed to the custom domain name instead of the default one:

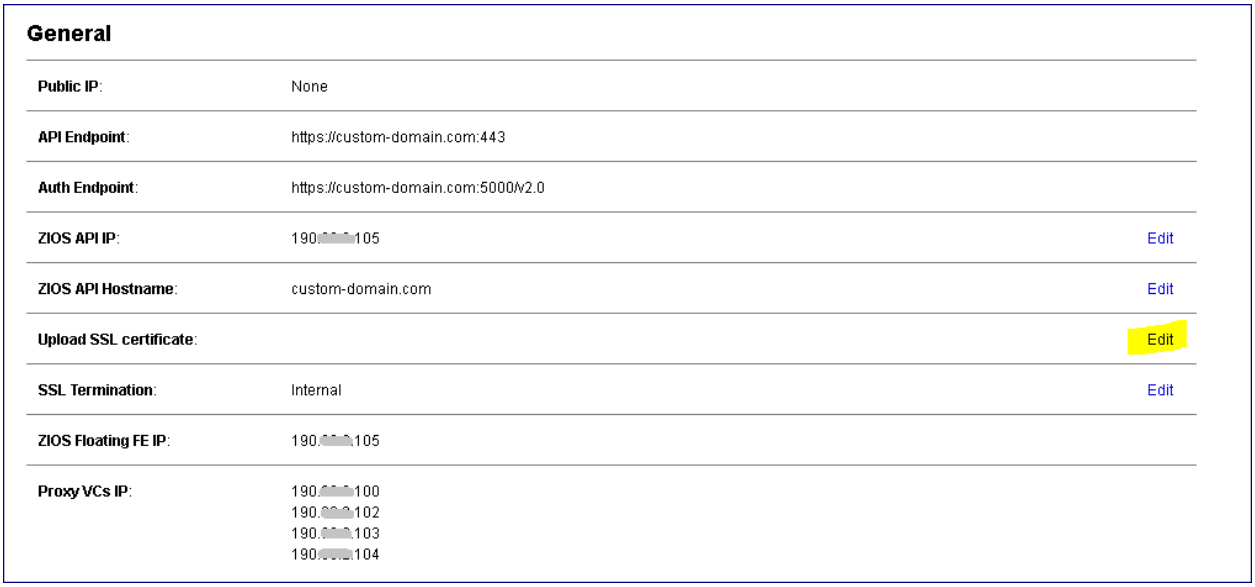


✔ **Note:** Starting that point, all mails sent to users by VPSA Object Storage will include URL with the custom domain name.

At this point VPSA Object Storage is still using “insecure” SSL certificate which was issued to zadarazios domain name. Although objects operations will now be possible, objects clients such as Cloudberry / S3browser will warn about an insecure connection to VPSA Object Storage. VPSA Storage Array backup to Object Storage will fail as it cannot handle insecure connections.

In order to complete the procedure and work in “secure” mode, you will need to:

- Manually register the custom domain name with the VPSA Object Storage FE IP in your internal DNS server.
- Generate SSL certificate issued to the custom domain name.
- Upload it to the VPSA Object Storage as a PEM file. Use the Settings page to upload the certificate:

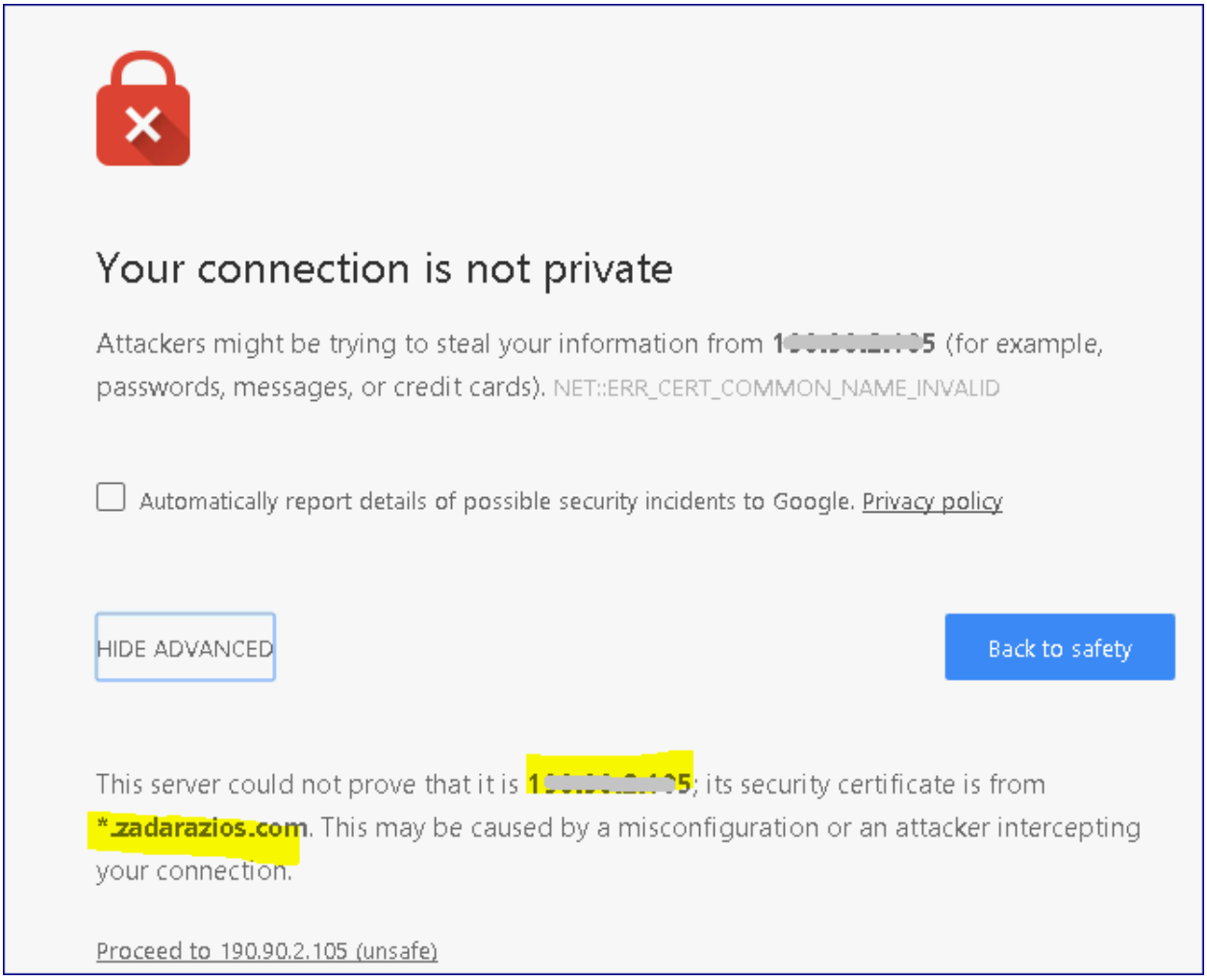


Once the new PEM is uploaded, the web management interface will reload. Now, GUI connection and object operations should be done against VPSA Object Storage custom domain name which is matching the name in the SSL certificate VPSA Object Storage is holding.

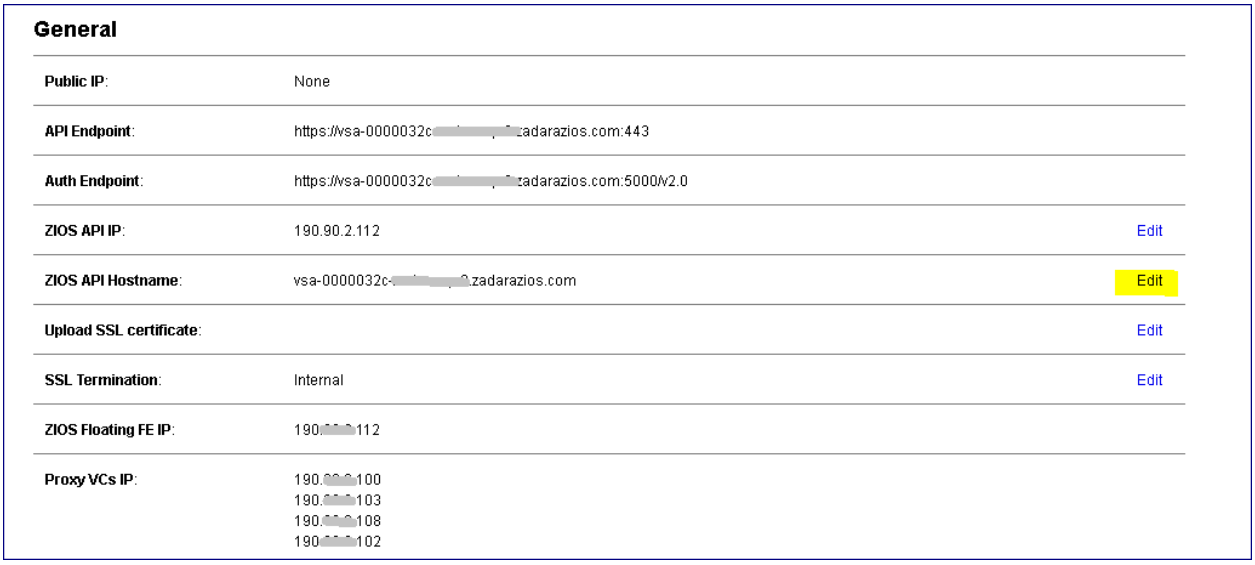
4.4.3 Option 2: IP Address

Once VPSA Object Storage is created, proceed as following:

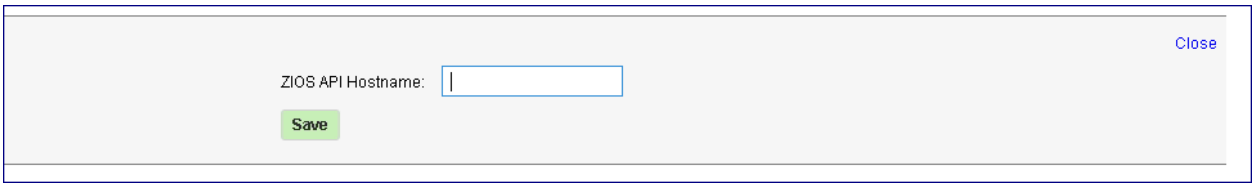
- Browse to GUI IP (as appears in the provisioning portal), and approve the “insecure” certificate which is not matching the URL IP:



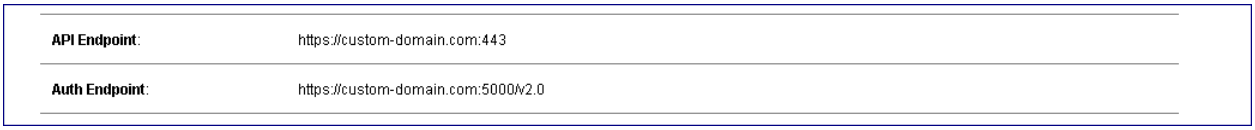
- Login to VPSA Object Storage GUI with initial credentials and change password
- Go to Settings page and edit the VPSA Object Storage API Hostname



- Clear the value and save



- The GUI will be reloaded and you will need to re-login, once logged in you will see the API and Auth Endpoints were changed to include IP instead of domain name:

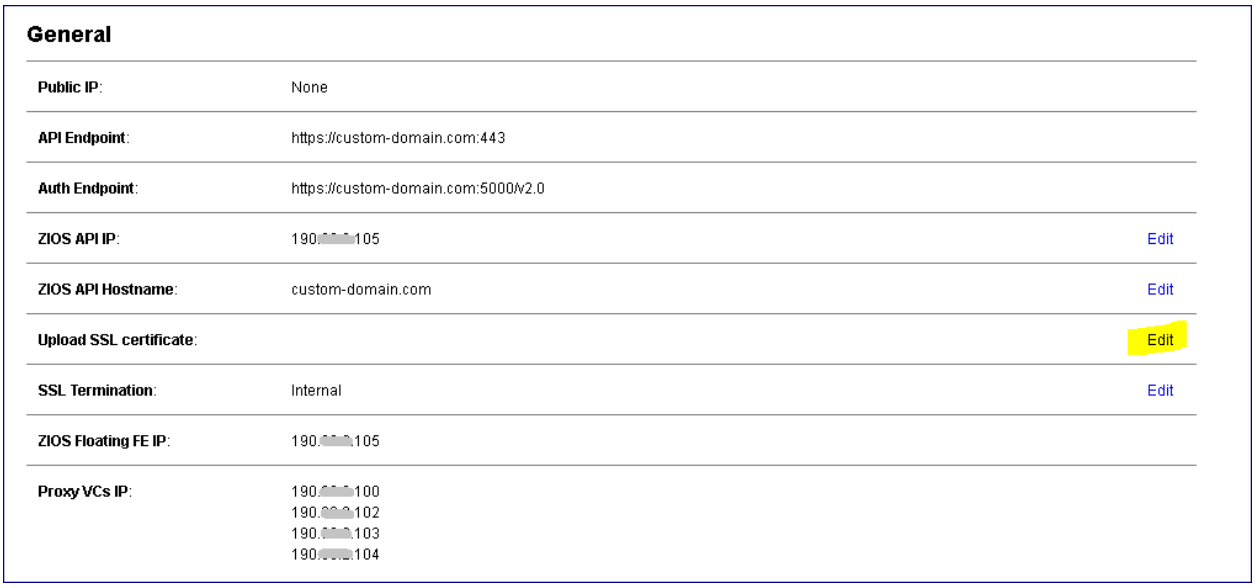


Note: Starting that point, all mails sent to users by the VPSA Object Storage will include the IP-based URL instead of the domain name.

At this point the web server is still using the “insecure” SSL certificate which was issued to zadarazios.com domain name. Although objects operations will now be possible to VPSA Object Storage, objects clients such as Cloudberry \ S3browser will warn about an insecure connection to the VPSA Object Storage. VPSA Storage Array backup to VPSA Object Storage will fail as it cannot handle insecure connections.

In order to work in “secure” mode, you will need to:

- Generate SSL certificate issued to the VPSA Object Storage FE IP (it can be self-signed certificate).
- Upload it to the VPSA Object Storage as a PEM file . Use the Settings page to upload the certificate:



Once the PEM is uploaded, GUI will reload. Now, GUI connection and object operations should be done against VPSA Object Storage FE IP which is matching the name in the SSL certificate VPSA Object Storage is holding.

4.5 Setting Custom Domain for VPSA Object Storage

VPSA Object Storage is created by default with zadarazios.com domain and registered with this domain name in DNSimple DNS service.

VPSA Object Storage includes SSL object server in addition to the GUI SSL server, therefore it is created with a default SSL certificate issued to zadarazios.com .

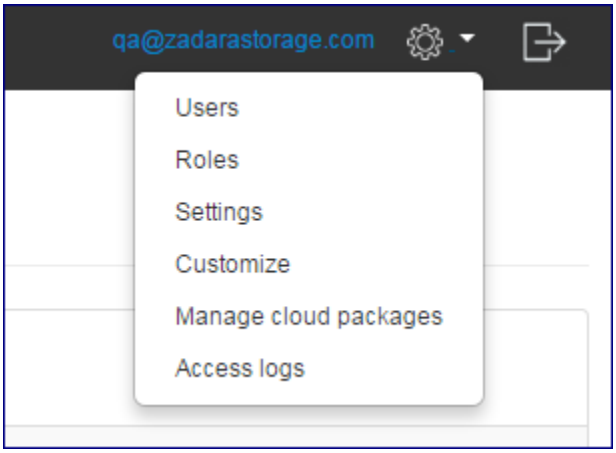
VPSA Object Storage domain name and certificate are not only used for management but also for Authentication and Object Operations.

Follow the procedure below to set a custom domain instead of the default:

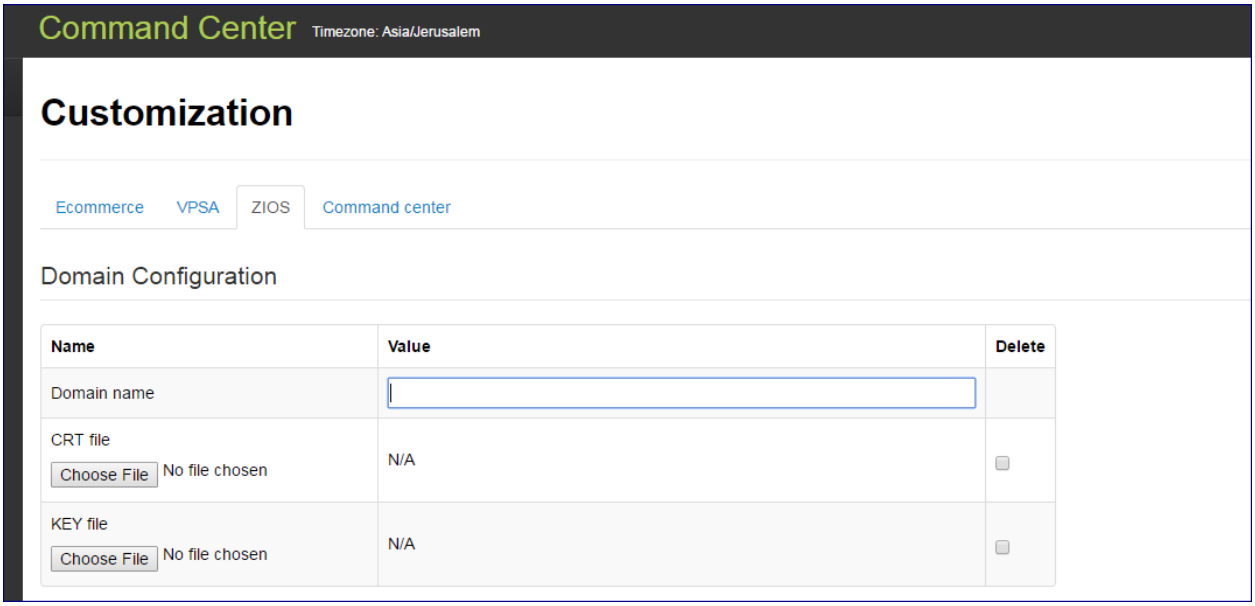
4.5.1 Global custom domain for all Object Storage VPSA's in the cloud

Similar to VPSA Storage Array, it is possible to customize the cloud via Command Center in order to make sure every VPSA Object Storage which is created on the cloud will own a custom domain name and a matching SSL certificate.

- Login to Command Center and open customization page:



- Under the General tab set a custom domain name, and upload a matching SSL certificate:

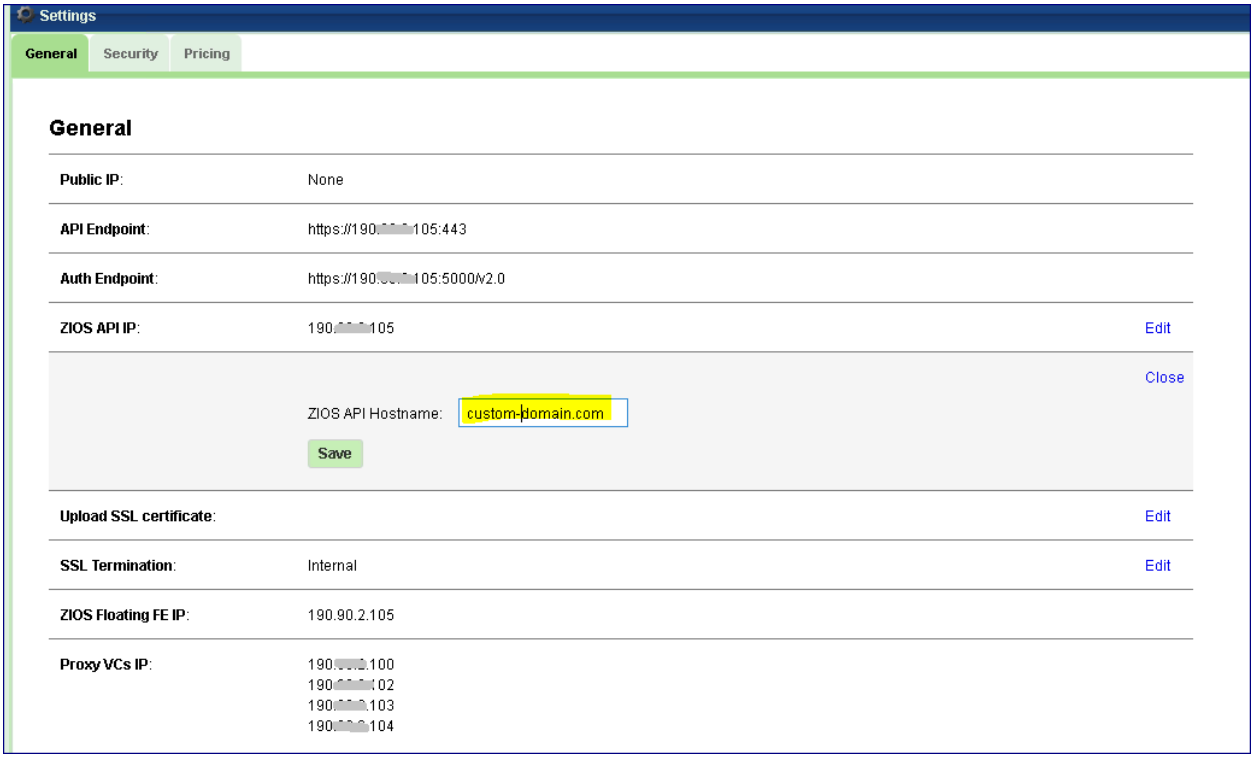


- From that point on, every VPSA Object Storage to be created in this cloud will have the custom domain name and matching certificate
- Manually register the custom domain of each VPSA in a public DNS server.

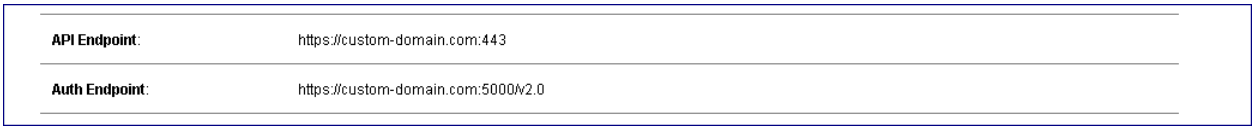
4.5.2 Explicit custom domain per VPSA Object Storage

Once VPSA Object Storage is created proceed as following:

- Browse to the management URL (zadarazios domain name) as appears in the provisioning portal
- Login to the GUI with initial credentials and change password
- Go to the Settings page and edit the VPSA Object Storage API Hostname, remove the default domain name and set a custom domain name as required:



- The GUI will be reloaded and you will need to re-login, once logged in you will see in the Settings page that the API and Auth Endpoints were changed to the custom domain name instead of the default one:



Note: Starting that point, all mails sent to users will include URL with the custom domain name.

At this point VPSA Object Storage is still using the default SSL certificate which was issued to zadarazios domain name. Although objects operations will now be possible, objects clients such as Cloudberry / S3browser will complain about an insecure connection to VPSA Object Storage as the certificate is not matching the custom domain name. In addition VPSA backup to VPSA Object Storage will fail as it cannot handle insecure connections.

In order to work in “secure” mode, you will need to:

- Manually register the custom domain name with VPSA Object Storage FE IP in any public DNS server. If a Public IP is required, assign a public IP to the VPSA Object Storage and register the custom domain name with the public IP in the DNS.
- Generate SSL certificate issued to the custom domain name
- Upload it to the VPSA Object Storage as a PEM file . Use the Settings page to upload the certificate:

Once PEM is uploaded, GUI will reload. Now, GUI connection and object operations should be done against VPSA Object Storage custom domain name which is matching the name in the SSL certificate VPSA Object Storage is holding.

✔ **Note:** The management URL will still appear in the provisioning portal with the default zadarazios domain name, however management, authentication and objects operations will be done against the custom domain as seen in VPSA Object Storage settings page and which will also appear in mails.

4.6 Adding Proxy Virtual Controllers (VPSA Object Storage Admin)

The public VPSA Object Storage REST API is exposed through the Proxy. For each request, it will look up the location of the account, container, or object and route the request accordingly. Failures are also handled in the Proxy. For example, if an object server is unavailable for an object PUT request, it will find an alternate route there instead.

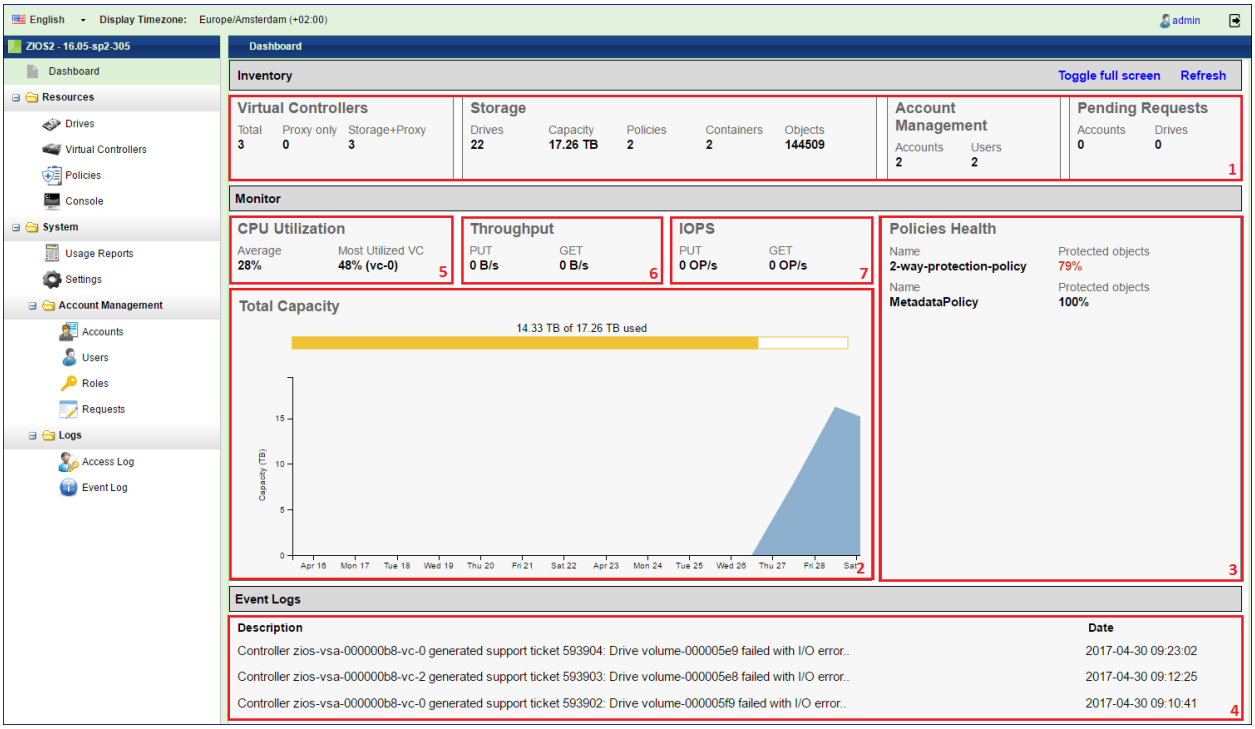
In VPSA Object Storage every VC automatically assigned to the system has both Storage and Proxy roles. However, in order to improve performance, you have the option to add additional Proxy only VC’s.

To assign additional Proxy VC’s, go to the Zadara Provisioning Portal, select the VPSA Object Storage system, and press the Add Proxy Virtual Controllers button. This operation requires the approval of a Zadara Storage Cloud Admin.

CHAPTER

FIVE

UNDERSTANDING THE VPSA OBJECT STORAGE DASHBOARD



The VPSA Object Storage Dashboard allows administrators to get the overall health of the system at a glance.

1. **Inventory** – Lists the number of entities of each type currently defined in the VPSA Object Storage.
2. **Capacity Usage** – This chart shows the accumulated used capacity of all storage Policies over time. The bar shows the current used/free capacity.
3. **Policies Health** – Lists all storage policies with their health index as calculated by the system.
4. **Events** – Shows the top priority latest events that the admin must be aware of.
5. **CPU Usage** – Shows the average load on all Virtual Controller and the load on the most utilized Virtual Controller.
6. **Throughput** – Shows the current aggregated throughput of all objects Put/Get operations at the proxy level.
7. **IOPS** - Shows the current aggregated number of all objects Put/Get operations at the proxy level.

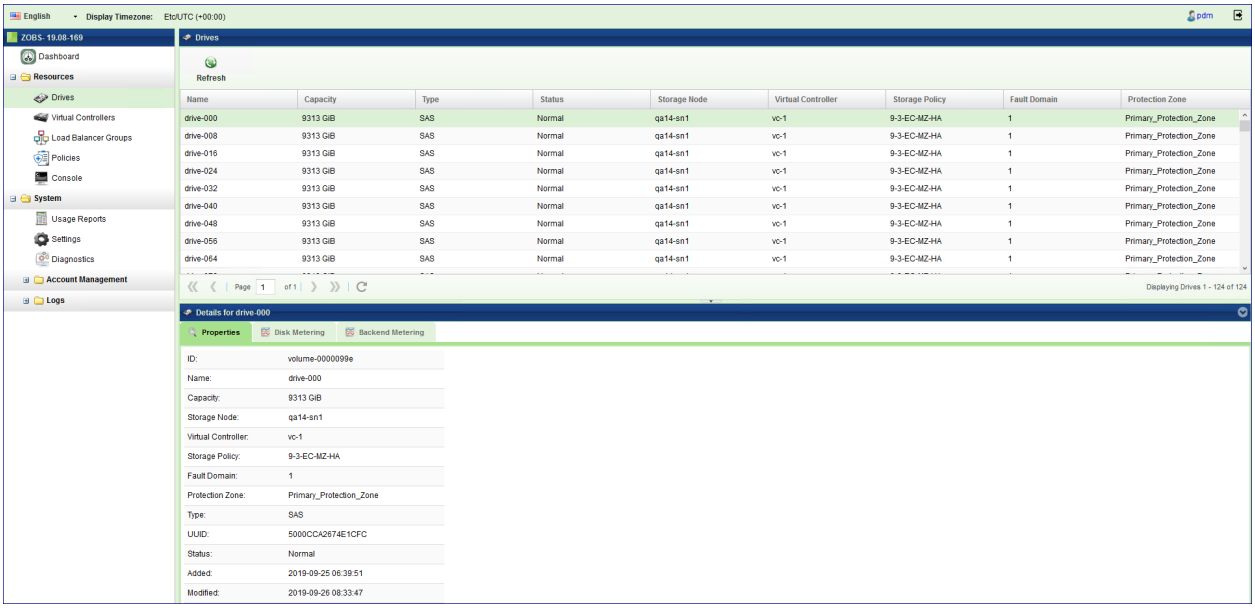
CHAPTER

SIX

VPSA OBJECT STORAGE ADMINISTRATION

6.1 Monitoring Drives

To monitor drives in your Object Storage system open the GUI > Resources > Drives



6.1.1 Viewing Drives Properties (VPSA Object Storage Admin)

The Drives details (properties and metering), are shown in the South Panel tabs:

Properties

Each Drive includes the following properties:

Property	Description
ID	An internally assigned unique ID
Name	Automatically assigned name.
Capacity	The Drive capacity in GiB
Storage Node	The Storage Node that contains the selected Drive
Virtual Controller	The virtual controller that owns the selected drives and performs IO operations on it
Storage Policy	The Storage Policy where the selected Drive belongs
Fault Domain	The Zadara cloud Fault Domain this Drive resides belongs to
Protection Zone	The Zadara cloud protection zone this drive is physically located at
Type	Drive type: SATA, SAS, SSD
UUID	The unique identifier of the drive
Status	• Normal – All drives are in sync • Failed – The drive does not function • Absent – The drive does not exist
Added	Date & time when the drive was added
Modified	Date & time when the drive was last modified

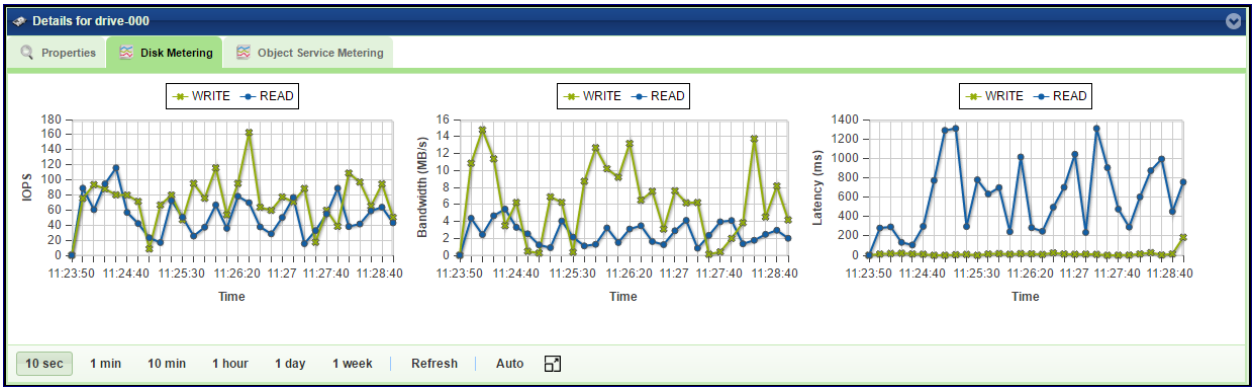
Disk Metering

The Metering Charts provide live metering of the IO workload associated with the selected Drive.

The charts display the metering data as it was captured in the past 20 intervals. An interval length can be one of the following: 10 second, 1 minute, 10 minutes, 1 hour, 1 day, 1 week. The Auto button lets you see continuously-update live metering info.

The following charts are displayed:

Chart	Description
IOPs	The number of read and write commands issued to the selected Drive per second
Bandwidth (MB/s)	Total throughput (in MB) of read and write commands issued to the selected Drive per second
Latency (ms)	Average response time of all read and write commands issued to the selected Drive per selected interval



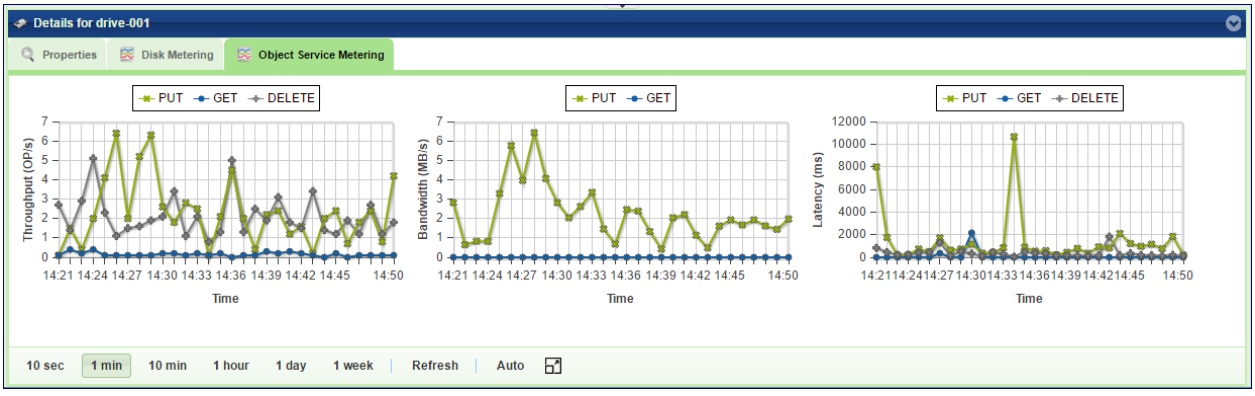
Backend Metering

The Metering Charts provide live metering of the IO workload on the selected Drive.

The charts display the metering data as it was captured in the past 20 intervals. An interval length can be one of the following: 10 second, 1 minute, 10 minutes, or 1 hour, 1 day, 1 week. The Auto button lets you see continuously-updating live metering info.

The following charts are displayed:

Chart	Description
Throughput (OP/s)	The number of operations (PUT/GET/DELETE) that were sent to the selected Drive per second
Bandwidth (MB/s)	Total throughput (in MB) of read and write commands that were sent to the selected Drive per second
Latency (ms)	Average response time of all operations (PUT/GET/DELETE) that were sent to the selected Drive per selected interval



6.2 Monitoring Virtual Controllers

Virtual Controllers are Virtual Machines (VM) on the Zadara cloud that serves client operations on the Object Storage. For a full list of the VC responsibilities refer to Virtual Controller. Virtual Controllers are automatically created and added/removed to the Object Storage configuration, depending on the number of the allocated drives. There are minimum of two VCs in each VPSA Object Storage deployment: vc-0, vc-1. These VCs have role of Proxy+Storage. To improve performance you can add Proxy only VCs from the Zadara Provisioning Portal as described at Adding Proxy Virtual Controllers (VPSA Object Storage Admin).

6.2.1 Viewing VCs Properties (VPSA Object Storage Admin)

Properties

Each Virtual Controller has the following properties:

Property	Description
ID	An internally assigned unique ID
Storage Role	Proxy+Storage / Proxy-Only
Management Role	• Ring Master – Runs the Object Storage Rings • Ring Slave – Standby to run the Object Storage Rings • VC – Regular VPSA Object Storage VC
Status	• Created – VC is running normally • Failed – VC is not running • Passivating – VC is shutting down • Deleting – in the process of being removed from the cluster
Storage Node	The Storage Node hosting selected VC
Fault Domain	The Zadara cloud Fault Domain this VC resides belongs to
Protection Zone	The Zadara cloud protection zone this VC is allocated to
Frontend IP	The IPv4 or IPv6 address allocated to the VC
Backend IP	The VC IP address on the backend network that connects to the Drives
Load Balancer Group	(Optional) In case an ELB is enabled, represent the LB Group of the VC
Added	Date & time when the VC was added
Modified	Date & time when the VC was last modified

Drives

List the drives assigned to the selected Storage Policy.

System Usage

This chart shows the CPU utilization of the selected VC.

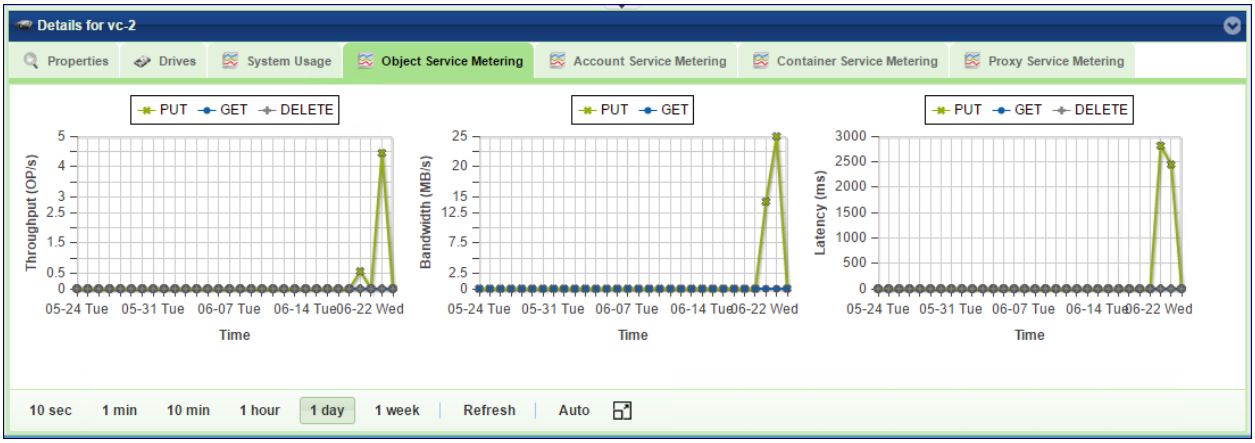
Backend Metering

The Metering Charts provide live metering of the IO workload at the backend of the selected VC.

The charts display the metering data as it was captured in the past 20 intervals. An interval length can be one of the following: 10 second, 1 minute, 10 minutes, or 1 hour, 1 day, 1 week. The Auto button lets you see continuously-updating live metering info.

The following charts are displayed:

Chart	Description
Throughput (OP/s)	The number of operations (PUT/GET/DELETE) issued to objects and handled by the selected VC per second
Bandwidth (MB/s)	Total throughput (in MB) of read and write commands issued by the selected VC per second
Latency (ms)	Average response time of all operations (PUT/GET/DELETE) issued to objects and handled by the selected VC per selected interval



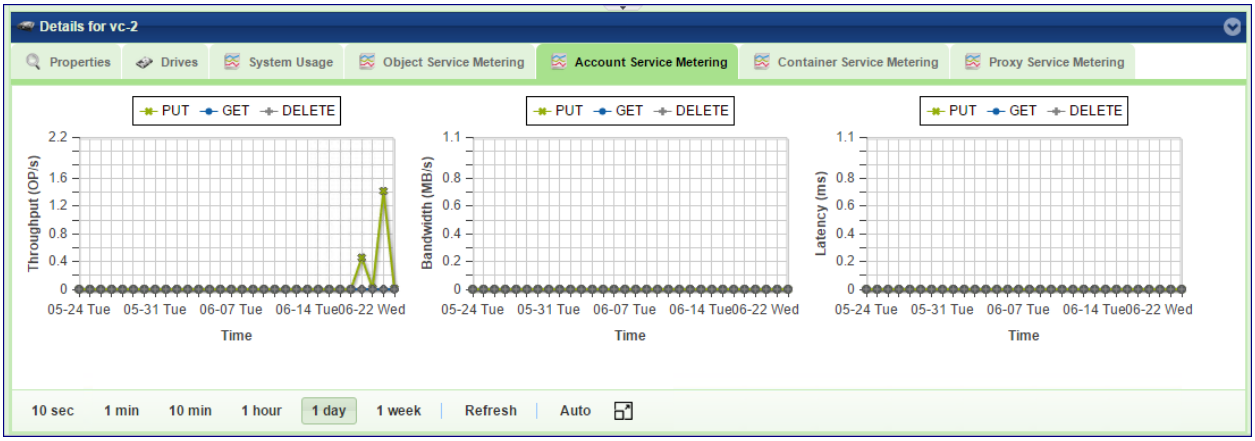
Account Service Metering

The Metering Charts provide live metering of the IO workload on the accounts database at the backend of the selected VC.

The charts display the metering data as it was captured in the past 20 intervals. An interval length can be one of the following: 10 second, 1 minute, 10 minutes, or 1 hour, 1 day, 1 week. The Auto button lets you see continuously-updating live metering info.

The following charts are displayed:

Chart	Description
Throughput (OP/s)	The number of operations (PUT/GET/DELETE) issued to the accounts database and handled by the selected VC per second
Bandwidth (MB/s)	Total throughput (in MB) of read and write commands issued by the selected VC to the accounts DB per second
Latency (ms)	Average response time of all operations (PUT/GET/DELETE) issued to the accounts database and handled by the selected VC per selected interval



Container Service Metering

The Metering Charts provide live metering of the IO workload on the containers database at the backend of the selected VC .

The charts display the metering data as it was captured in the past 20 intervals. An interval length can be one of the following: 10 second, 1 minute, 10 minutes, or 1 hour, 1 day, 1 week. The Auto button lets you see continuously-updating live metering info.

The following charts are displayed:

Chart	Description
Throughput (OP/s)	The number of operations (PUT/GET/DELETE) issued to containers and handled by the selected VC per second
Bandwidth (MB/s)	Total throughput (in MB) of operations (PUT/GET/DELETE) issued by the selected VC to containers per second
Latency (ms)	Average response time of all operations (PUT/GET/DELETE) issued to containers and handled by the selected VC per selected interval

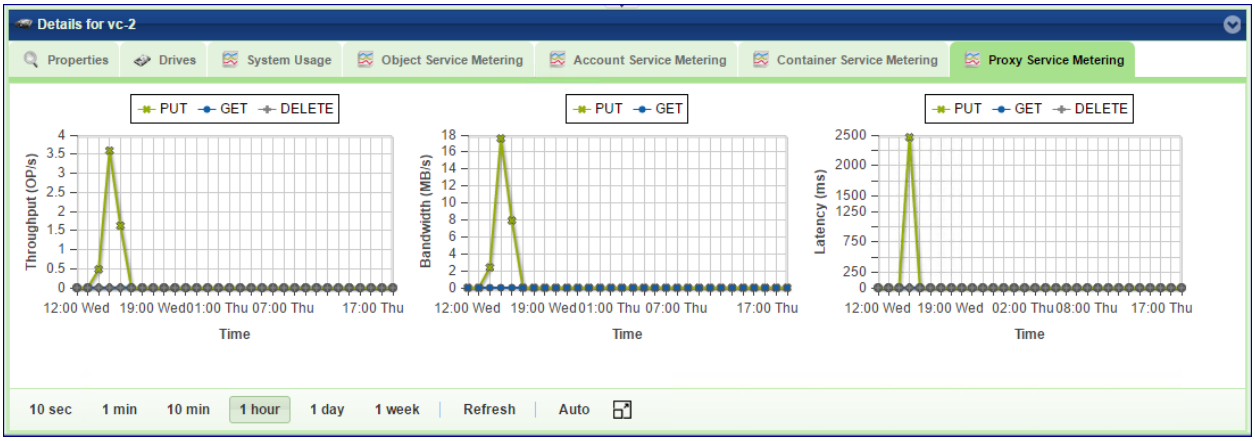
Frontend Metering

The Metering Charts provide live metering of the IO workload at the frontend of the selected VC.

The charts display the metering data as it was captured in the past 20 intervals. An interval length can be one of the following: 10 second, 1 minute, 10 minutes, or 1 hour, 1 day, 1 week. The Auto button lets you see continuously-updating live metering info.

The following charts are displayed:

Chart	Description
Throughput (OP/s)	The number of operations (PUT/GET/DELETE) issued to objects and handled by the proxy of the selected VC per second
Bandwidth (MB/s)	Total throughput (in MB) of read and write commands issued to proxy of the selected VC per second
Latency (ms)	Average response time of all operations (PUT/GET/DELETE) issued to objects and handled by proxy of the selected VC per selected interval



6.3 Load Balancer Groups (Optional)

Zadara Elastic Load Balancer can be enabled for the VPSA Object Storage in order to provide improved performance and load allocation across the VPSA Object Storage VCs. Once enabled, a dedicated VC will be added to the VPSA Object Storage as the Load Balancer Master. The Load Balancer Master VC will aggregate a bulk of up to 12 VCs from the same protection zone under the same VRID index.

From this view, a VPSA Object Storage administrator can review the utilization and distribution of each Load Balancer Group.

Property	Description
ID	An internally assigned unique ID
VRID	The VRRP VRID assigned to the Elastic Load Balancer Group
VC Master	The Load Balancer Group Active (Master) VC
IPv4/IPv6	The Load Balancer Group Active (Master) VC IP address
Protection Zone	The Zadara cloud protection zone
Added	Date & time when the LBG was created
Modified	Date & time when the LBG was last modified

6.4 Managing Storage Policies

Storage Policies provide a way for object storage providers to differentiate service levels, features and behaviors of a Object Storage deployment.

Policies can be think of as a group of drives, with a redundancy level policy assigned to it.

Before placing object data into the VPSA Object Storage, users create a container which holds the listing of all objects stored under the container's namespace. Users can select the Storage Policy that will be used when storing data objects under a container's namespace when they create the container. All objects stored in a container will be placed according the configuration of the Storage Policy which was set when the container was created. If no policy was specified at the container creation time, the default policy is used.

To ensure availability of the VPSA object Storage data, the drives assigned to a Storage Policy are evenly distributed between Object Storage Fault Domains. The cloud administrator defines the Fault Domain of each Storage Node. The system makes sure to allocated drives across zones based on the Storage Policy type

Storage Policies allow some level of segmenting in terms of quality of service, within a single system for various purposes. Storage Policies allow objects to be stored based on the following criteria:

- Quality of Service: By using different disk drives for different policies, tiers of storage performance can be created. For example, an SSD-only policy can be created used to implement a low-latency/high performance tier.
- Number of Replicas: offer different protection levels in the same VPSA Object Storage cluster
  - 2x replication offers protection for one FD failure, at the cost of 50% storage utilization.
  - 3x replication offers protection for 2 FDs failures, at the cost of 33.33% storage utilization.
  - Erasure Coding (4+2, 6+3) offers protection for 1 FD failures, at the cost of 67% storage utilization.
  - Erasure Coding (6+2, 9+3) offers protection for 1 FD failures, at the cost of 75% storage utilization.
  - Erasure Coding (4+2 - Multizone-HA) offers protection for 1 FD failures, on each zone or a complete protection zone failure at the cost of 67% storage utilization per protection zone.
  - Erasure Coding (9+3 - Multizone-HA) offers protection for 1 FD failures, on each zone or a complete protection zone failure at the cost of 75% storage utilization per protection zone.

  The following Storage Policies are supported:

Table 1: Object Storage Data Protection Policies

Policy Type	Redundancy	Minimal Configuration
2 Way	x 2	2 VCs on 2 SNs, each in a different Fault Domain
3 Way	x 3	3 VCs on 3 SNs, each in a different Fault Domain
Erasure Coding 4+2	x 1.5	3 VCs on 3 SNs, each in a different Fault Domain
Erasure Coding 6+3	x 1.5	3 VCs on 3 SNs, each in a different Fault Domain
Erasure Coding 6+2	x 1.33	4 VCs on 4 SNs, each in a different Fault Domain
Erasure Coding 9+3	x 1.33	4 VCs on 4 SNs, each in a different Fault Domain
Erasure Coding 4+2 (Multizone-HA)	x 1.5	3 VCs on 3 SNs, each in a different Fault Domain (in each region)
Erasure Coding 9+3 (Multizone-HA)	x 1.33	4 VCs on 4 SNs, each in a different Fault Domain (in each region)

Each drive in the system is assigned to one Storage Policy.

VPSA Object Storage is created with a default data Storage Policy for objects and another system Storage Policy for metadata. The VPSA Object Storage administrator (zios_admin) can later on create additional storage policies, expand existing policies and set a specific policy as the Default Policy.

For Multizone HA VPSA Object Storage, the protection policy is created symmetrically on both zones, in each availability zone, the same protection policy will be created in order to sustain a complete availability zone failure.

Policies are assigned when a container is created. Once a container has been assigned for a policy, it cannot be changed (unless it is deleted/recreated).

6.4.1 Creating Policy (VPSA Object Storage Admin)

When a VPSA Object Storage system is created, 2 policies are created by default:

- MetadataPolicy: Used to store the Accounts and Containers metadata, usually contains 2 SSD drives, with 2-way replication
- 2/3-way/EC-protection-policy: Used to store the users' objects, usually contain all the drives that were assigned to the Object Storage at creation time, with 3-way or 2-way replication or EC protection, according to the initial selection on the provisioning portal.

Storage Policies can be added form the provisioning Portal by the VPSA Object Storage admin. To create additional Policies, Go to the Provisioning Portal, select the VPSA Object Storage of the new Storage Policy, and then click the Add Storage Policy button in the right panel. Follow the instruction here: Adding Storage Policy (VPSA Object Storage Admin)

6.4.2 Viewing Policies Properties (VPSA Object Storage Admin)

You can view the following properties and metering information in the Policies Details South Panel tabs:

Properties

Each Policy includes the following properties:

Property	Description
ID	An internally assigned unique ID
Name	The name of Policy
Type	Object or Account/Container
State	Not Configured / Configuring / Initialized
Description	A user defined policy description
GB per Month Price	Price of used capacity for charge back purposes
Health Status	Normal / Degraded / Critical
Health Percentage	Indicates the percentage of the stored data that is accessible.
Rebalance Status	Normal / Rebalancing / Failed
Rebalance Prec.	Indicates the progress of the rebalance process
Cross-Region Rep-mode	Synchronous (for VPSA Multizone HA)
Capacity	Total usable capacity of the Storage Policy
Used Capacity	Amount of written data in the Storage Policy
Containers	Total amount of containers created within the policy
Objects	Total amount of objects created within the policy
Default	Yes/No
Redundancy Level	2-way/3-way/EC
Ring Version	Ring Database version
Rebalanced	The date and time when the Policy was last rebalanced. (Rebalance usually happens when the HW configuration changes, Adding/removing drives, failed components, etc.)
Added	The date and time when the Policy was added
Modified	The date and time when the Policy was last modified

Drives

List the drives assigned with the selected Storage Policy.

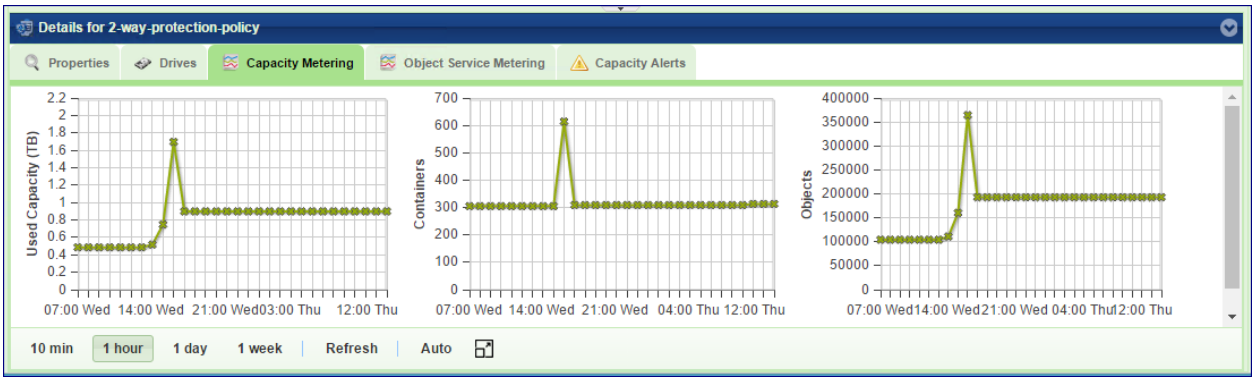
Capacity Metering

The Metering Charts provide live metering of the capacity usage associated with the selected Policy.

The charts display the metering data as it was captured in the past 20 intervals. An interval length can be one of the following: 10 minutes, or 1 hour, 1 day, 1 week. The Auto button lets you see continuously-updating live metering info.

The following charts are displayed:

Chart	Description
Used Capacity	Total storage capacity consumed in the selected Policy
Containers	Total numbers of containers that store their objects in the selected policy
Objects	Total numbers of objects stored in the selected policy



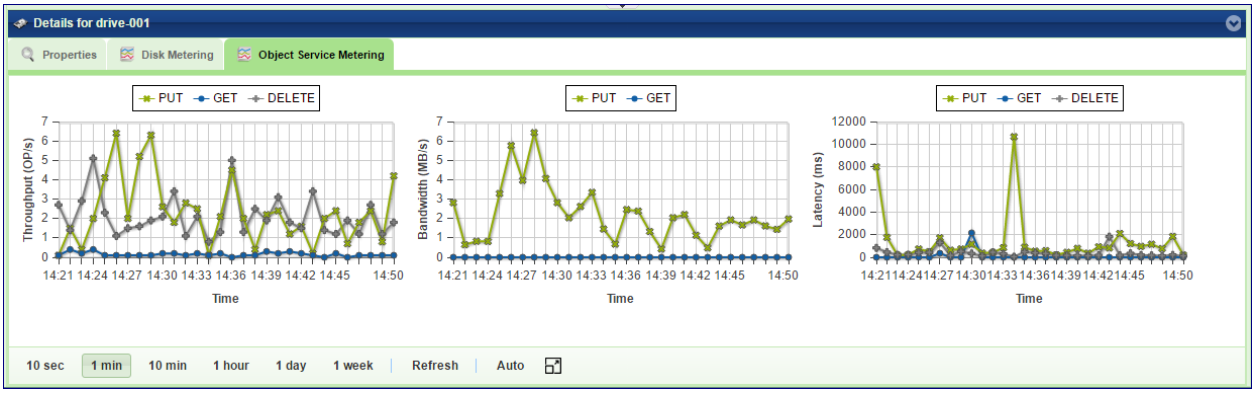
Backend Metering

The Metering Charts provide live metering of the IO workload associated with the selected Policy.

The charts display the metering data as it was captured in the past 20 intervals. An interval length can be one of the following: 10 second, 1 minute, 10 minutes, or 1 hour, 1 day, 1 week. The Auto button lets you see continuously-updating live metering info.

The following charts are displayed:

Chart	Description
Throughput (OP/s)	The number of operations (PUT/GET/DELETE) issued to the Drives of the selected Policy per second
Bandwidth (MB/s)	Total throughput (in MB) of read and write commands issued to the Drives of selected Policy per second
Av. Drive Latency	Average response time of all operations (PUT/GET/DELETE) issued to objects in the selected Policy per selected interval



Frontend Metering

The Metering Charts provide live metering of the IO workload associated with the traffic coming to the selected Policy.

The charts display the metering data as it was captured in the past 20 intervals. An interval length can be one of the following: 10 second, 1 minute, 10 minutes, or 1 hour, 1 day, 1 week. The Auto button lets you see continuously-updating live metering info.

The following charts are displayed:

Chart	Description
Throughput (OP/s)	The number of operations (PUT/GET/DELETE) issued to objects in the selected Policy per second
Bandwidth (MB\s)	Total throughput (in MB) of read and write commands issued to the selected Policy per second
Avg. Latency (ms)	Average response time of all operations (PUT/GET/DELETE) issued to objects in the selected Policy per selected interval

Capacity Alerts

Alert Threshold – Send Alert when it is estimated that the Policy will be at full capacity within the given time period (in minutes)

Alert Interval - Calculate the above threshold based on the capacity usage growth in the previous given time period (in minutes)

6.4.3 Set default Policy (VPSA Object Storage Admin)

The default Policy is the Policy used by default for newly created containers, if no other policy is explicitly specified. To change the default Policy, select the Policy you want to make the default and click "Set as Default".

✔ **Note:** As long as there is only one Policy for user data (this is the situation when a new VPSA Object Storage system is created), that only Policy is the default, and there no way to change it.

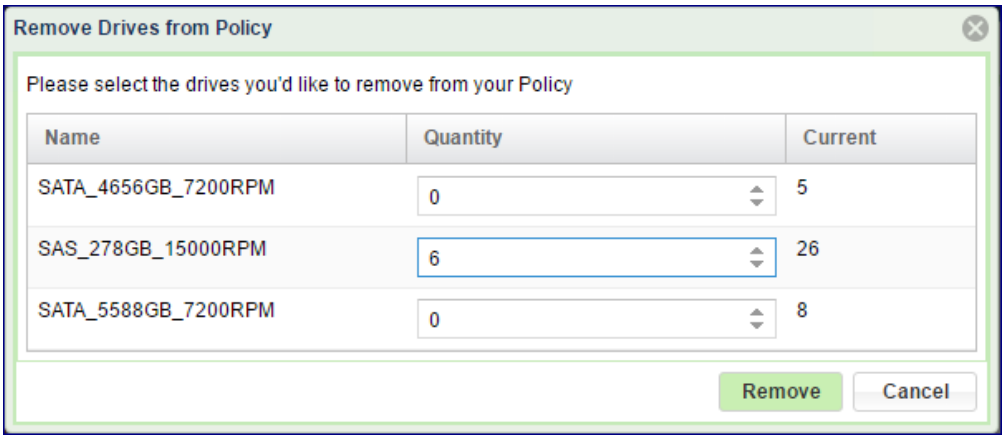
6.4.4 Adding Drives to Policy (VPSA Object Storage Admin)

Drives are added to an Object Storage policy via the Provisioning Portal. To add drives into a policy, go to the Provisioning Portal, select the VPSA Object Storage of interest and click Add Storage. Follow the instruction here: Adding Drives to an Existing Storage Policy (VPSA Object Storage Admin).

✔ **Note:** Drive-related operations in a storage policy will require rebalance that might take several hours until completion.

6.4.5 Removing Drives from Policy (VPSA Object Storage Admin)

If the there is a need to reduce the total available capacity of a given policy, or to remove some failed drives that were detached from the policy, you may remove drives from the policy and return them to the cloud for a different use. To remove drives from a Policy go to GUI > Policies, select the policy of interest, and click Remove Drives.



The dialog that will open will list all the drives types and quantities that currently belong to the policy. Set the number of drives you want to remove from each type, and click Remove.

✔ **Note:** Drive-related operations in a storage policy will require rebalance that might take several hours until completion.

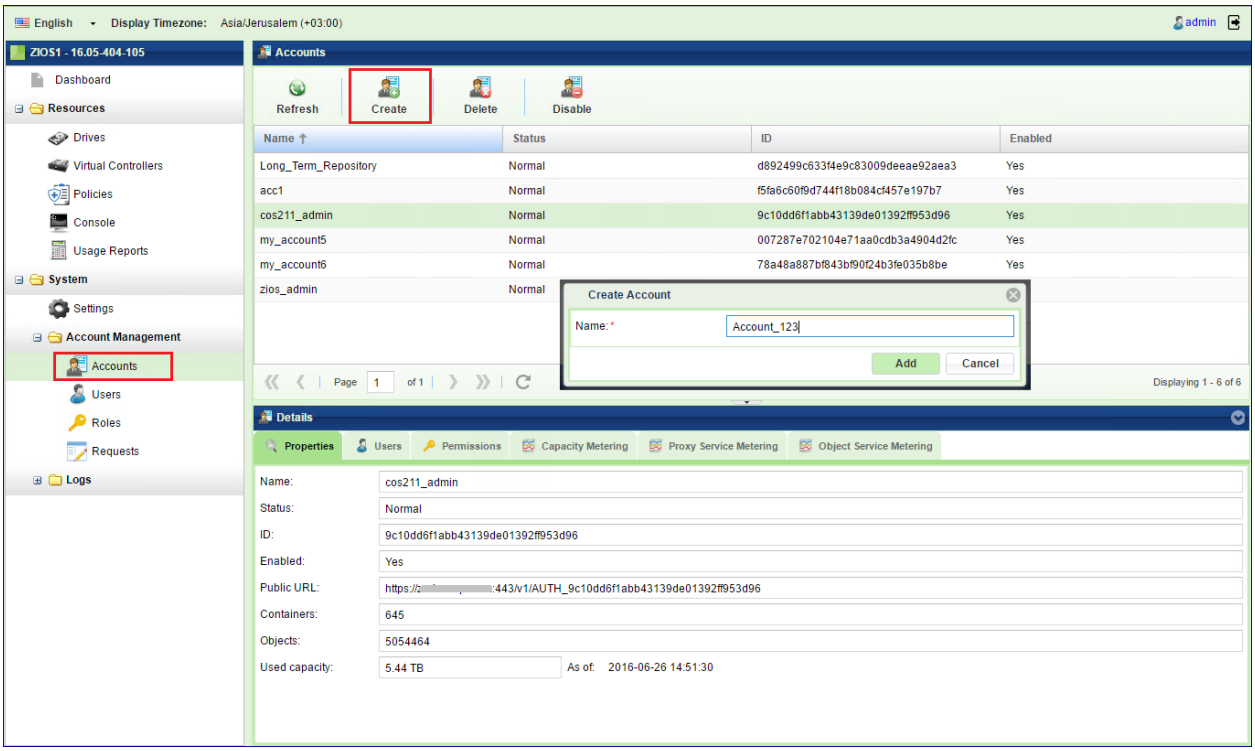
6.5 Managing Accounts

Object Storage Account is a collection of Containers. Typically an account is associated with a tenant. Access rights can be granted for users per account.

6.5.1 Creating account (VPSA Object Storage Admin)

When the system is first built, a default account is created called zios_admin account. At that point only the VPSA Object Storage admin has access to this account. In order to provision object storage to customers, the VPSA Object Storage administrator needs to create Accounts.

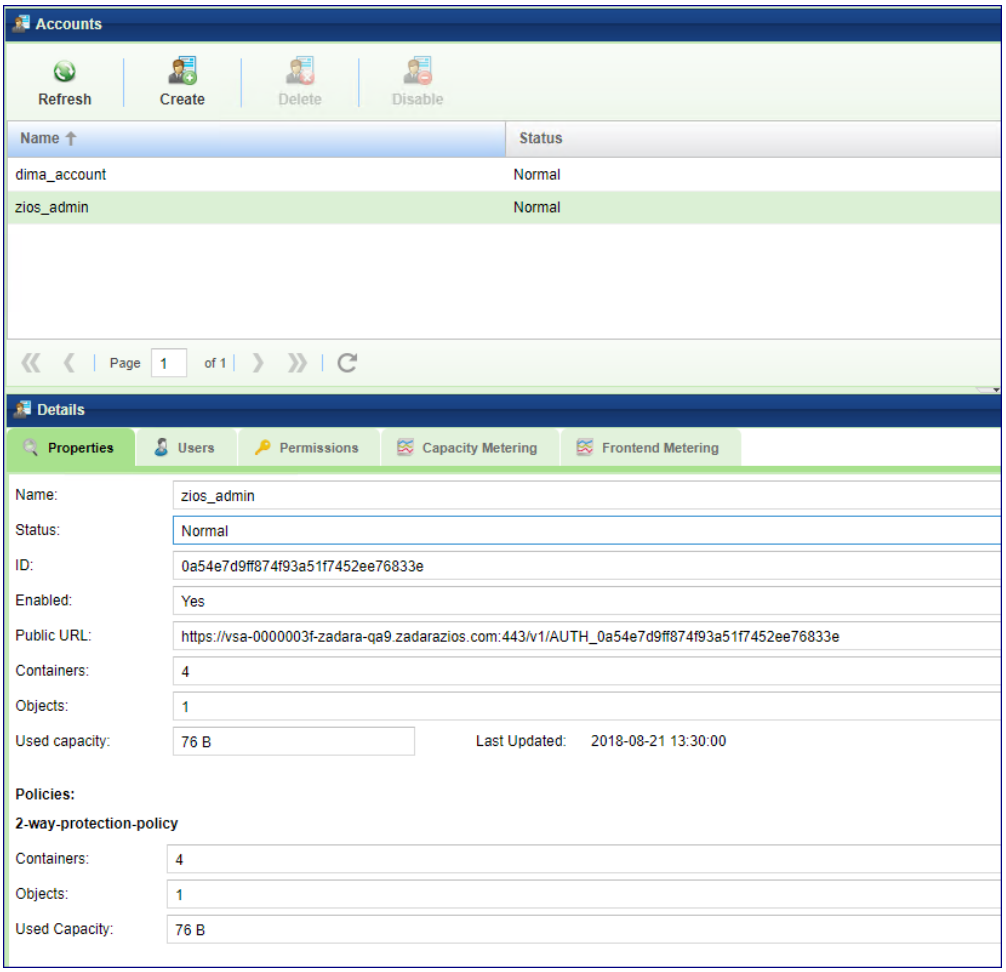
To create additional Accounts, first select the Accounts entity in the Main Navigation Panel (Left Panel) under Account Management, and then click the Create button in the Center Panel.



In the dialog that opens give a name to the new account. And click Add. The new account will be added.

6.5.2 Viewing Accounts Properties (VPSA Object Storage and Account Admin)

You can view the following properties and metering information in the Accounts Details South Panel tabs:



Properties

Each Account includes the following properties:

Property	Description
Name	The name of the Account
Status	Normal / Deleting / Deleted, awaiting cleanup
ID	An internally assigned unique ID
Enabled	Yes/No
Public URL	The URL that identifies this account. To be used by the REST API
Containers	Number of containers in the selected Account
Objects	Number of objects stored in the selected Account
Used Capacity	Amount of written data in the Account
Policies	Show statistics per each policy used by this account Details include: • Containers: Number of containers this account keeps in this policy • Objects: Number of objects this account keeps in this policy • Used Capacity: Capacity consumed by this account keeps in this policy

Users

Lists the users of the selected account.

Permissions

For account permissions see here Setting Account Permissions (Account Admin)

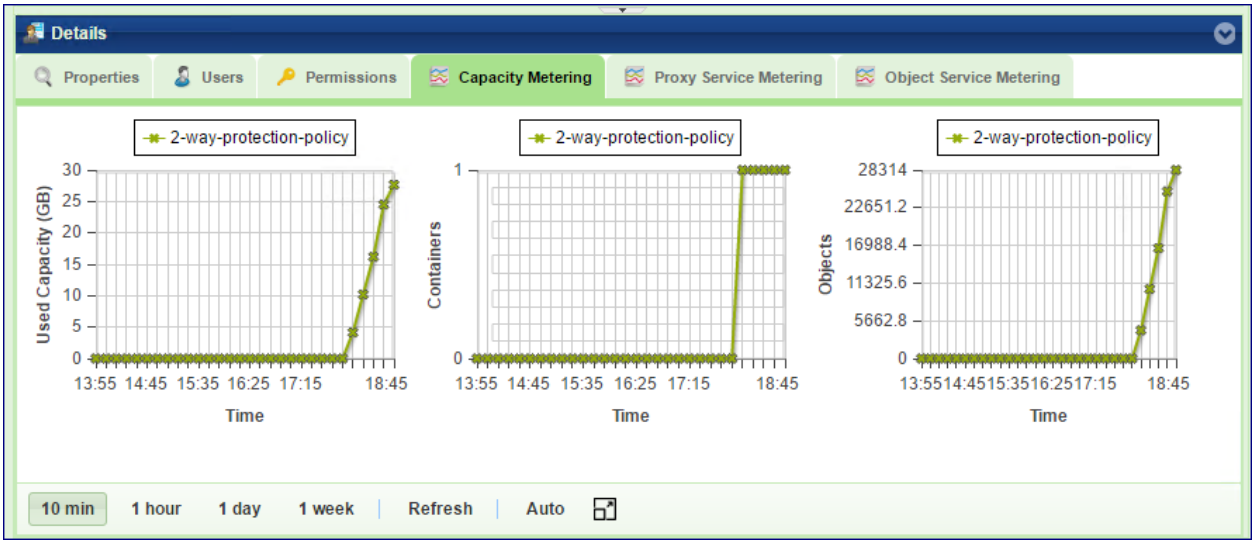
Capacity Metering

The Metering Charts provide live metering of the capacity usage associated with the selected Account.

The charts display the metering data as it was captured in the past 20 intervals. An interval length can be one of the following: 10 minutes, or 1 hour, 1 day, 1 week. The Auto button lets you see continuously-updating live metering info.

The following charts are displayed:

Chart	Description
Used Capacity	Total storage capacity consumed in the selected Account
Containers	Total numbers of containers belonging to the selected Account, by Storage Policy
Objects	Total numbers of objects belonging to the selected Account, by Storage Policy



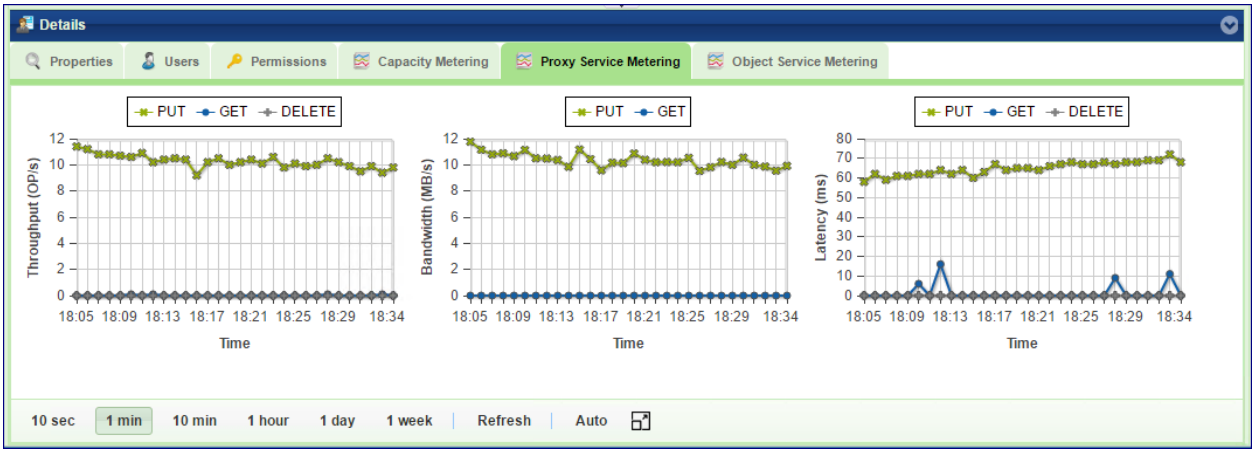
Frontend Metering

The Metering Charts provide live metering of the IO workload at the Object Storage frontend that belong to the selected Account.

The charts display the metering data as it was captured in the past 20 intervals. An interval length can be one of the following: 10 second, 1 minute, 10 minutes, or 1 hour, 1 day, 1 week. The Auto button lets you see continuously-updating live metering info.

The following charts are displayed:

Chart	Description
Throughput (OP/s)	The number of operations (PUT/GET/DELETE) issued to objects that belong to the selected Account.
Bandwidth (MB/s)	Total throughput (in MB) of read and write commands issued to proxy for the selected account.
Latency (ms)	Average response time of all operations (PUT/GET/DELETE) issued to objects of the selected Account per selected interval.



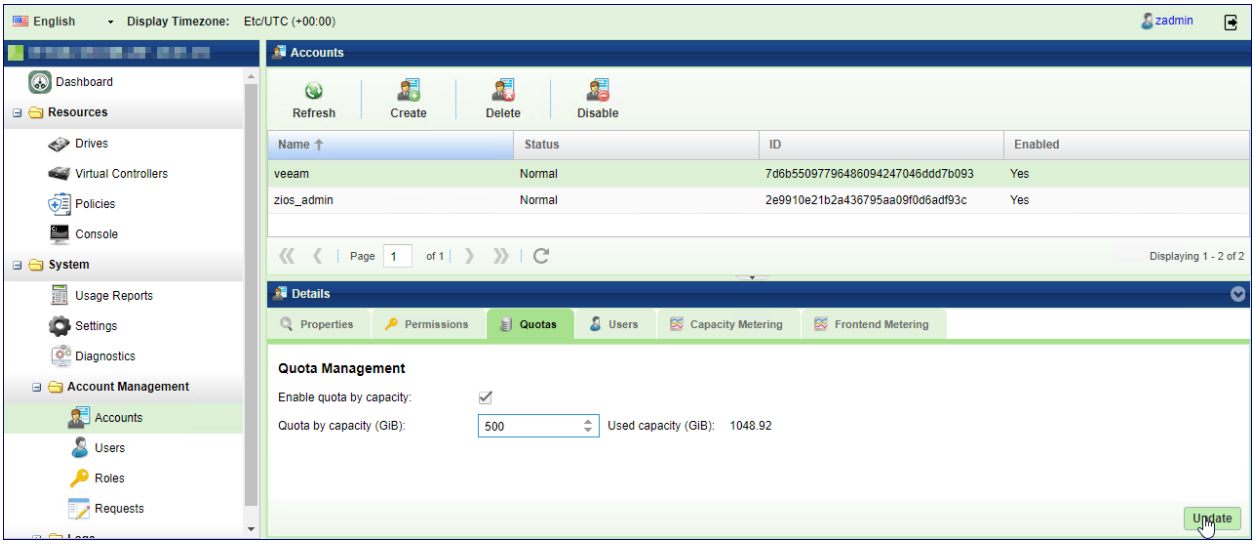
6.5.3 Account Quota Management (Object Storage Administrator or Account Admin)

If needed, a VPSA Object Storage administrator (zios_admin) or Account administrator can set an account level/container level quota.

Note: Once enabled, It will take up to 10 minutes for the quota management to be activated.

Enable Account - Quota Management

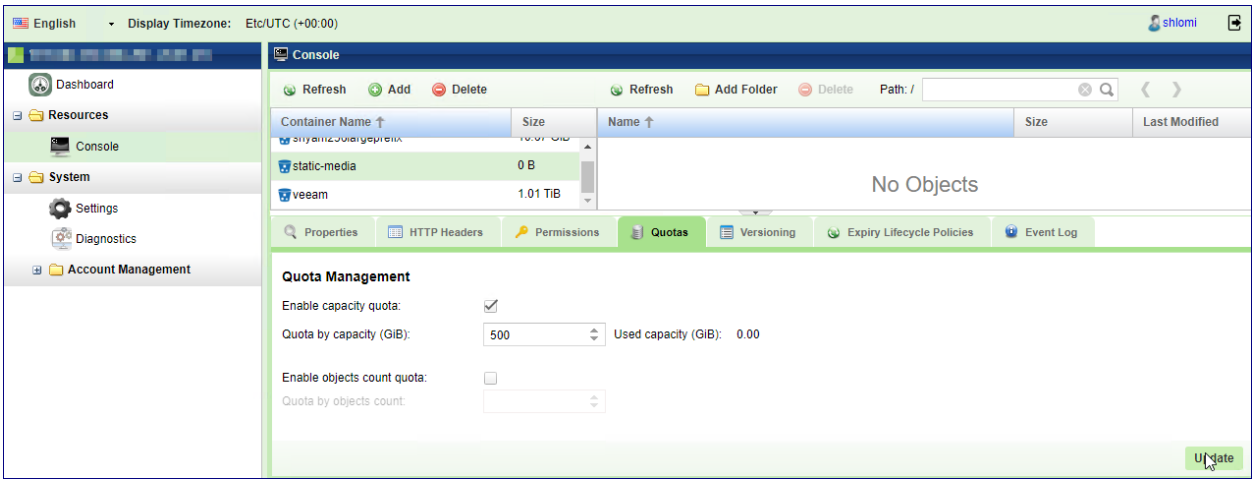
In the VPSA Object Storage management interface navigate to the Account view: Account Management > Accounts, select an Object Storage Account. In the view south pane open the Quotas tab and check the Enable quota by capacity checkbox.



Note: Account level quota can be enabled by the VPSA Object Storage administrator (zios_admin)

Enable Container Quota Management

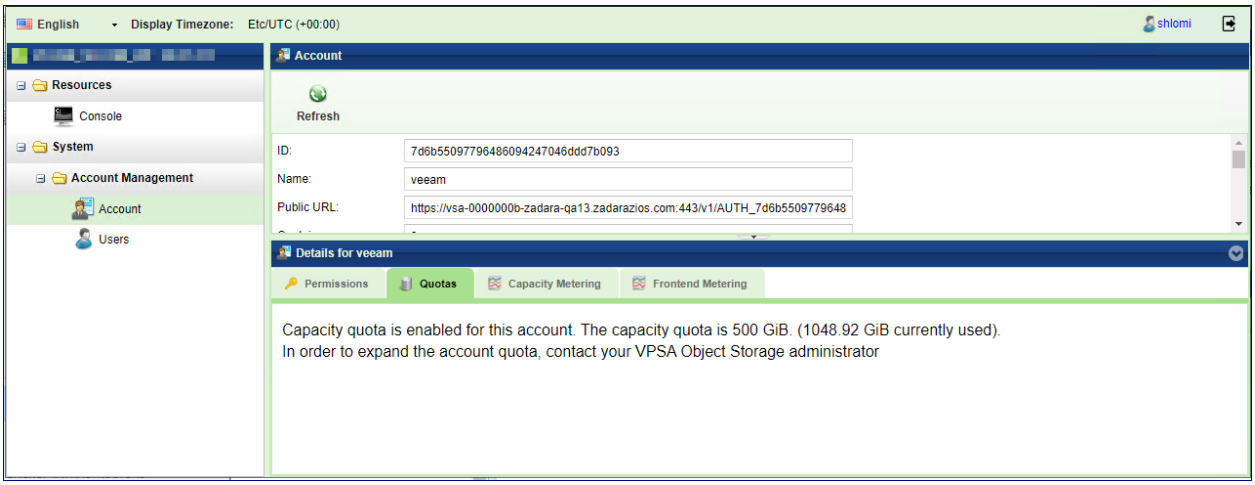
In the VPSA Object Storage management interface navigate to the Console view. Select a container, in the view south pane open the Quotas tab and check the Enable capacity quota, and/or the Enable objects count quota.



View quota consumption

Account quota

Once quota management was enabled for a given account, the account administrator will have a clear visibility for the current consumption. In the VPSA Object Storage management interface navigate to the Account view, Account Management > Accounts. In the view south pane open the Quotas.

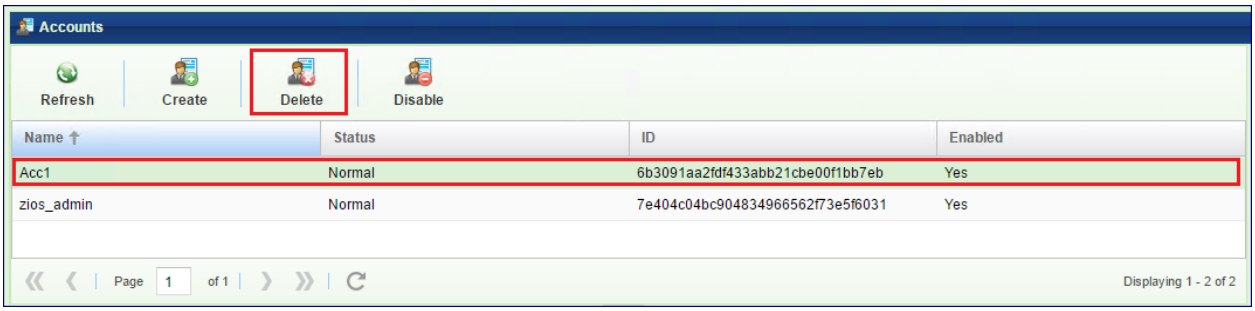


Container quota

Once quota management was enabled for a given container, the account member will have a clear visibility for the current consumption. In the VPSA Object Storage management interface navigate to the Console view, select a container and in the view south pane open the :guilabel:'Quotas'.

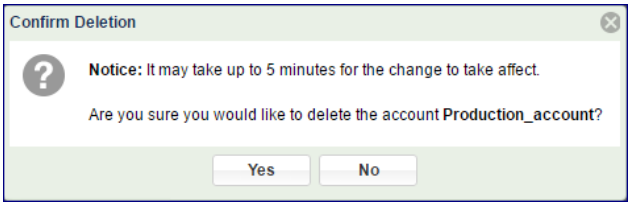
6.5.4 Deleting account (VPSA Object Storage Admin)

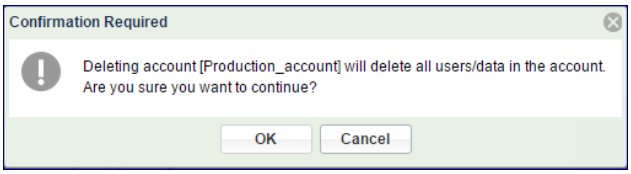
To Delete an Account, first select the Accounts entity in the Main Navigation Panel (Left Panel) under Account Management, select the Account to be deleted, and then click the Delete button in the Center Panel.



Deleting an account is an irreversible operation, and requires double confirmation

Note: After an account is deleted, all account user data is removed however account billing information still exist in the system for usage report generation. The VPSA Object Storage Admin need to click the "Cleanup" button in the Center Panel in order to completely remove it from the system.





6.5.5 Disabling an account (VPSA Object Storage Admin)

When an account is disabled by the VPSA Object Storage Administrator, no one can access that account, not for read nor for write operations. However, VPSA Object Storage keeps all the account definitions (Users, access rights, etc.), and all the containers and objects.

To Disable an Account, first select the Accounts entity in the Main Navigation Panel (Left Panel) under Account Management, select the Account to be disabled, and then click the Disable button in the Center Panel.

Note: Disable/Enable button toggles as the account state changes.

6.5.6 Self Service Account Creation (Account Admin)

VPSA Object Storage Administrator have an alternative procedure for creating new accounts. Instead of creating the Account (as described here Creating account (VPSA Object Storage Admin)) and creating Account admin, the VPSA Object Storage admin can let users to create their own Accounts. The procedure is as follows:

a. VPSA Object Storage admin gives the GUI URL to the person that will create the Account (Account admin)

b. The account admin uses the GUI to create a request for new account

c. VPSA Object Storage admin approves the request

d. A new Account is being built, and a new admin user is defined in it.

Below is a detailed description of this procedure.

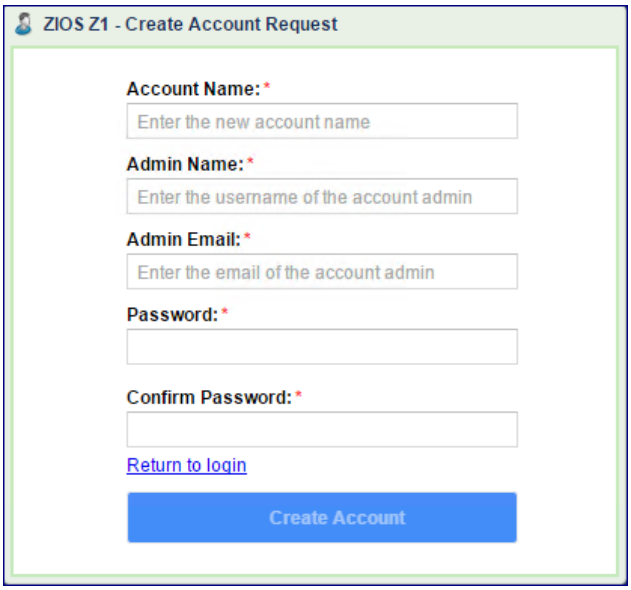
Use the GUI URL and get to the login screen:

Since you don't have login credentials, and you want to create a new account, click the Create new account link. In the new account dialog enter the following fields:

- Name for the new Account
- Your username as the Account admin
- Your email address
- Select a password

Note: While account name and the username for a given user are unique across the VPSA Object Storage, the same email address can be used for multiple users. This is useful in cases the same entity needs visibility to more than a single account.

And click Create Account. This will create an Account creation request that will go to the VPSA Object Storage Admin for approval. You will automatically become the Account admin of your new account.



You will receive the following email, as confirmation for the request:

Important: **Subject** : Your new account creation request (Production_Account - requested 2016-06-27 10:27:12)

Your new account creation request has been sent.

Please notice that the Account will not be active until the creation request is approved. A mail notification will be sent to you upon approval.

User: Prod_Account_Admin

Email: myname@zadarastorage.com

Account: Production_Account

The VPSA Object Storage admin will receive an email informing him about the pending request:

Important: **Subject** : New Account creation request (Production_Account - requested 2016-06-27 10:27:11)

A new account creation request created on cloud zadara-qa3

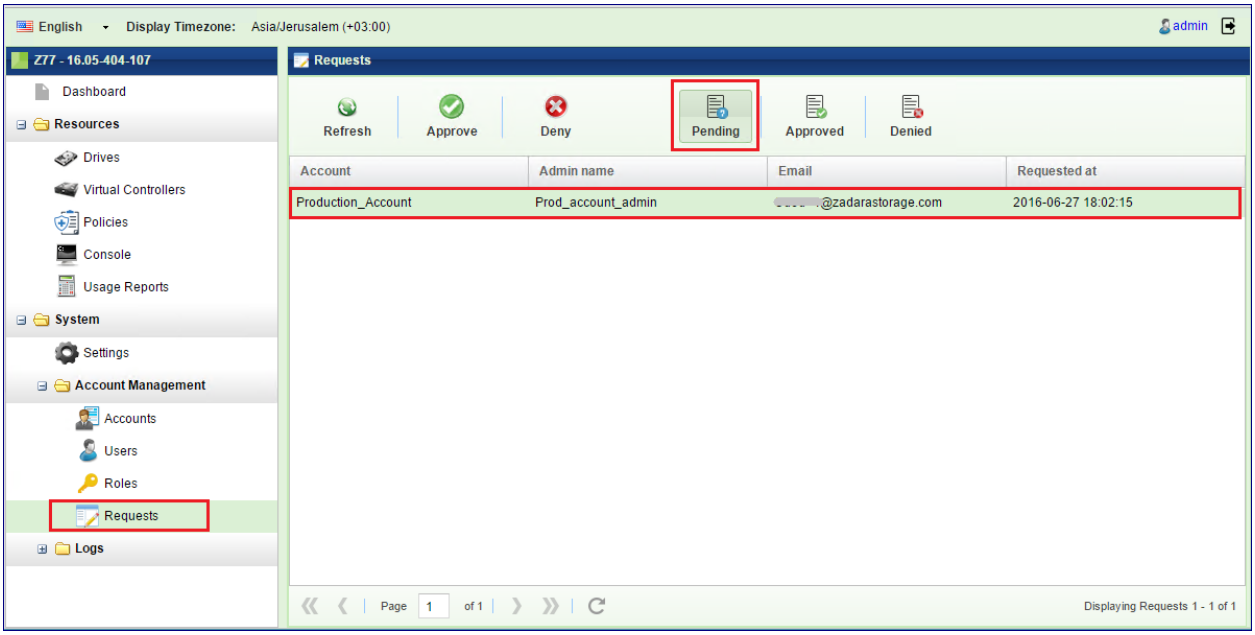
You can approve/deny requests on your VPSA Object Storage Z1 at https://vsa-00000144-zadaraqa3.zadarazios.com:8443.

Details:

User: Prod_Account_Admin

Email: myname@zadarastorage.com

The VPSA Object Storage Admin should open the GUI, select Users entity in the Main Navigation Panel (Left Panel) under Account Management, select the pending Account request, and either Approve or Deny it.



Upon approval the new account will be created, the account admin will be defined with the given credentials. You will receive an email notification about the new account:

Important: **Subject** : Your new account creation request has been approved

Your Account Creation request was approved, and you were added to Z77 VPSA Object Storage as Admin user under Production_Account account.

Your role allows you to manage objects and users under your account.

To start working with your VPSA Object Storage use the following information:

VPSA Object Storage Account Management & Console URL: https://vsa-00000152-zadara-qa3.zadarazios.com:8443

VPSA Object Storage API Endpoint URL: https://vsa-00000152-zadara-qa3.zadarazios.com:443

Account: Production_Account

Username: Prod_account_admin

The Account is ready. You can now login to the GUI, add members to the Account, create containers and start store objects.

6.6 Managing Users

6.6.1 Understanding users roles

The VPSA Object Storage support the following roles:

- **VPSA Object Storage Administrator(zios_admin):** Responsible for the administration of the VPSA Object Storage. This is the user that created the VPSA Object Storage in the Zadara Provisioning Portal.
- **VPSA Object Storage Admin - Read Only** a dedicated Read-Only account for cross-accounts monitoring and reporting purposes. **The Read-Only role is available for the zios_admin account only**. A Read-Only user will

have access to the VPSA Object Storage RestAPI, however it will not have data access. The user role is designated for monitoring and reporting purposes, such as:

  - Performance monitoring
  - Capacity monitoring
  - Usage reports & billing automation

- **Account Administrators** : Responsible for the administration of their account
- **Account Member** can do object storage operations according to the given permissions within the limits of that account.

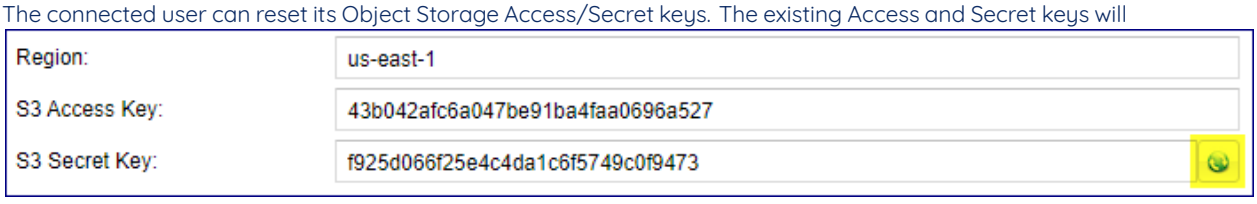
6.6.2 User Information

Information about the user currently logged in to the GUI is displayed by clicking the user name on the GUI upper right corner.

The following User's properties are displayed:

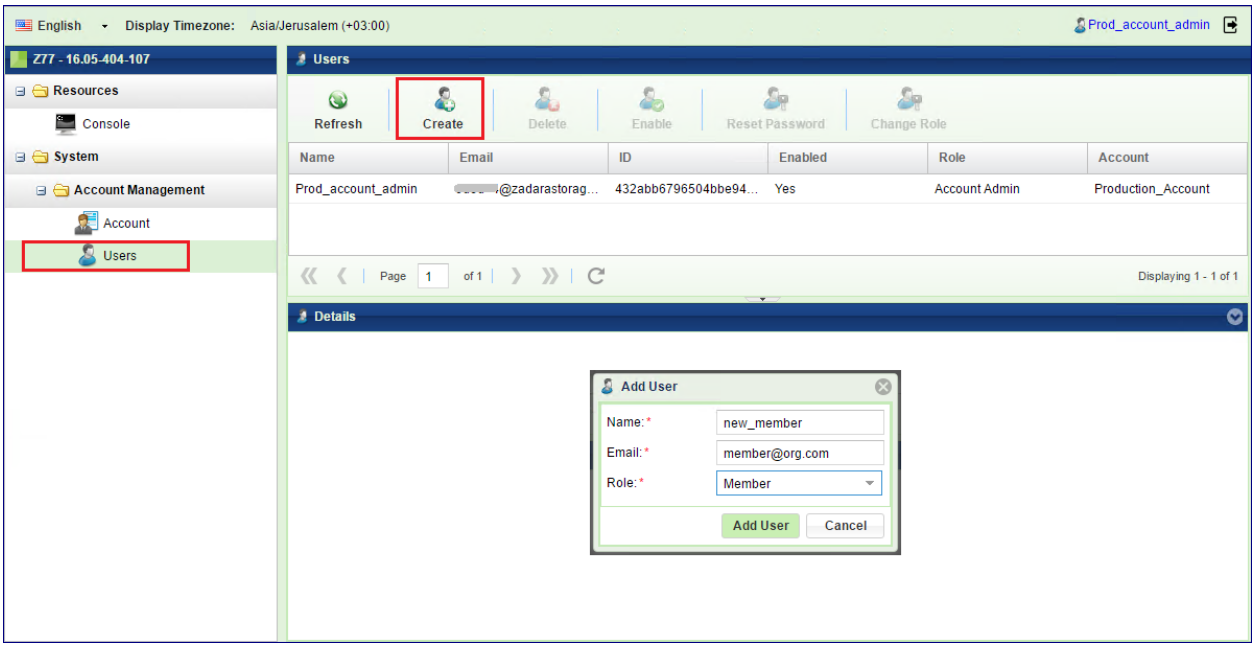
Property	Description
Username	The login ID of the User
Email	User's email address
Account	The account where the user belongs
Public URL	The URL that identifies this user's account. To be used by the REST API
User ID	An internally assigned unique ID
Account ID	An internally assigned unique ID
Dual Factor Auth.	Indication if this user has dual factor authentication activated
Object Storage API Token	Token to be used for authentication by the REST API The token expires in 24 hours. Good practice is for every script to start with getting a new token. See API guide http://zios-api.zadarastorage.com
Public IP	Public IP of the VPSA Object Storage (see: Assigning Public IPs (VPSA Object Storage Admin))
API Endpoint	The effective address for REST API for all IO requests
Auth Endpoint	The effective address for REST API for all authentication requests
S3 Access Key	To be used by client using the S3 interface
S3 Secret Key	To be used by client using the S3 interface

Note: The connected user can reset its Object Storage Access/Secret keys. The existing Access and Secret keys will be revoked.



6.6.3 Creating user (VPSA Object Storage Admin, Account Admin)

To create a User, first select the Users entity in the Main Navigation Panel (Left Panel) under Account Management, and then click the Create button in the Center Panel.



In the dialog that opens, give the user a name, select the role, enter an email address, and select the User's Account. Click Create.

✔ **Note:** Everything an Account admin does, is within the context of that Account. So, when an Account admin creates users, there is no need to select an Account.

✔ **Note:** Users with VPSA Object Storage Admin role can only be created in the zios_admin account.

The new user will receive an email with links to access the GUI for their account, and the first-time password. The new user must change the temporary password at first login

---

Important: You were just added to Z1 as #Member user under Test_Account account. Your role allows you to manage objects in your account according to your permissions.

To start working with your Object Storage use the following information:

Console URL: https://vsa-00000144-zadara-qa3.zadarazios.com:8443

API Endpoint URL: https://vsa-00000144-zadara-qa3.zadarazios.com:443

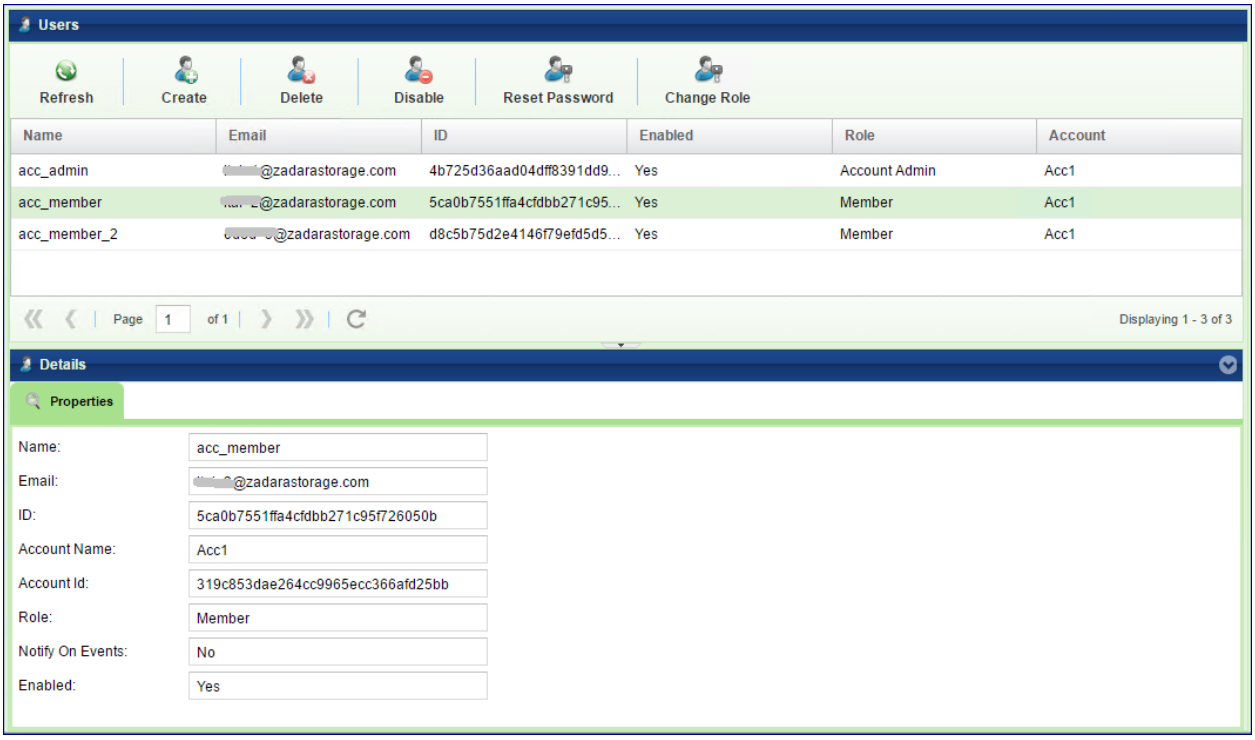
Account: Test_Account

Username: Test_Account_Member

Temporary Password Code: 9oya82BXV53Z2_qwJGq3

Please use the Temporary Password Code when logging into your Object Storage user interface for the first time to create a new password.

6.6.4 Viewing Users Properties (VPSA Object Storage Admin, Account Admin)

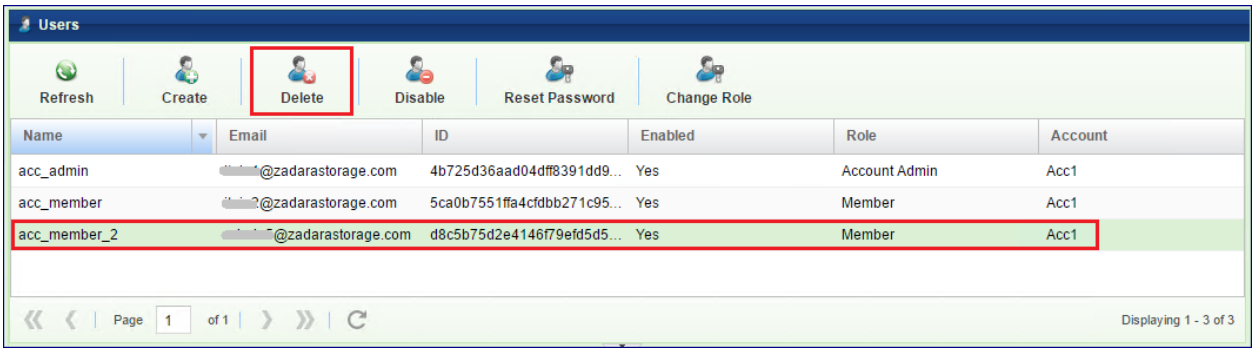


The following User's properties are displayed:

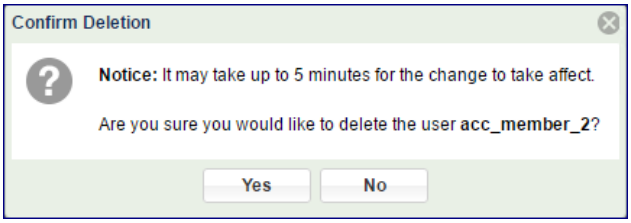
Property	Description
Name	The login ID of the User
Email	User's email address
ID	An internally assigned unique ID
Account Name	The account where the user belongs
Account ID	An internally assigned unique ID
Role	VPSA Object Storage Admin, Account Admin, Member
Notify on Events	Specify is this user want to get email notifications for events
Dual Factor Auth.	Indication if this user has dual factor authentication activated
Enabled	User is active or not. Disabled user can't login and can't perform any operation

6.6.5 Deleting users (VPSA Object Storage, Account Admin)

To Delete a User, first select the Users entity in the Main Navigation Panel (Left Panel) under Account Management, select the User to be deleted, and then click the Delete button in the Center Panel.



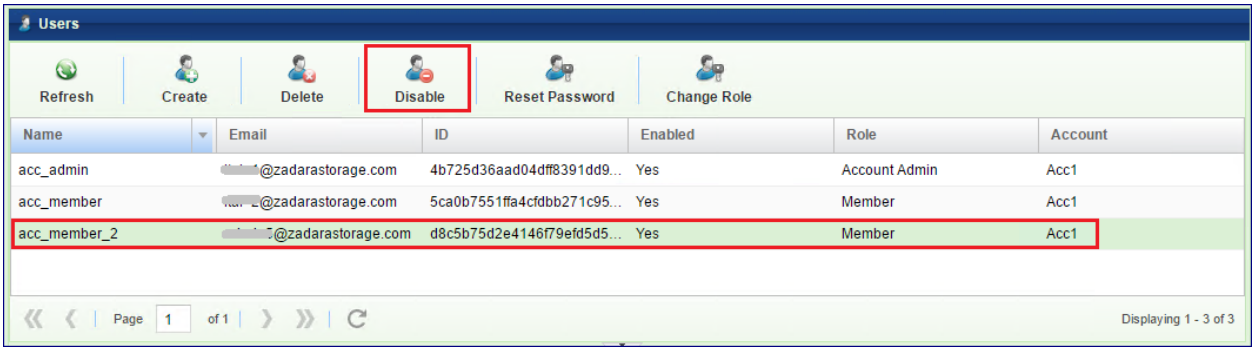
The system will ask for confirmation. By clicking Yes the deletion process will begin, and might take few minutes.



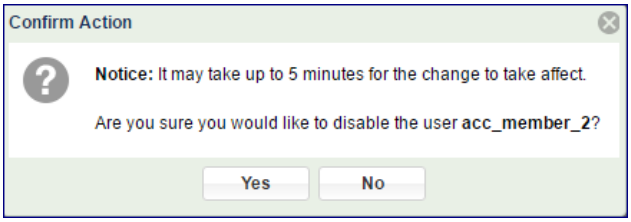
6.6.6 Disabling users (VPSA Object Storage Admin, Account Admin)

A disabled user cannot login to the GUI or perform any operation via the REST API. However the system remembers the User with all the properties and permissions. Once users are enabled, they can resume operations as before.

To Disable a User, first select the Users entity in the Main Navigation Panel (Left Panel) under Account Management, select the User to be deleted, and then click the Disable button in the Center Panel.



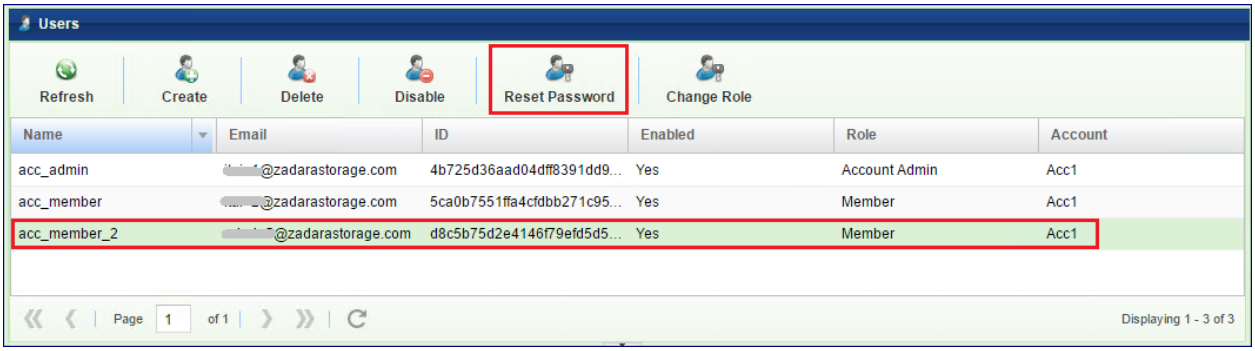
The system will ask for confirmation. By clicking Yes the disabling process will begin, and might take few minutes.

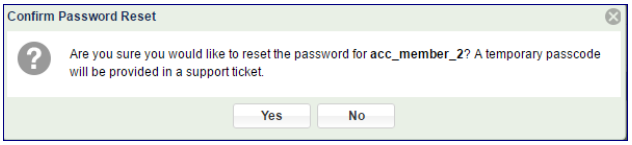


6.6.7 Reset password (VPSA Object Storage Admin, Account Admin)

VPSA Object Storage admin and Account admins can reset Users' passwords. When resetting a password, the User will receive an email with a temporary password that they will have to change at the next login.

To reset someone's password, first select the Users entity in the Main Navigation Panel (Left Panel) under Account Management, select the User for whom you will reset the password, and then click the Reset Password button in the Center Panel.





The system will ask for confirmation. By clicking Yes the user will be assigned a

temporary password that will be sent by email:

Important: **Subject** :Forgot Z888 Password - acc_member_2 - requested at: 2016-06-28 12:10:49 +0300

You requested to reset the password on your VPSA Object Storage Z888. If you made this request follow the instructions below:

Your temporary passcode is: t5CpKs_M-oMNwqX6jiJ4

In order to reset your password, you must login to the VPSA Object Storage at https://vsa-00000154-zadaraqa3.zadarazios.com:8443 using your username and the supplied password code as your

password.Account: Production_Account

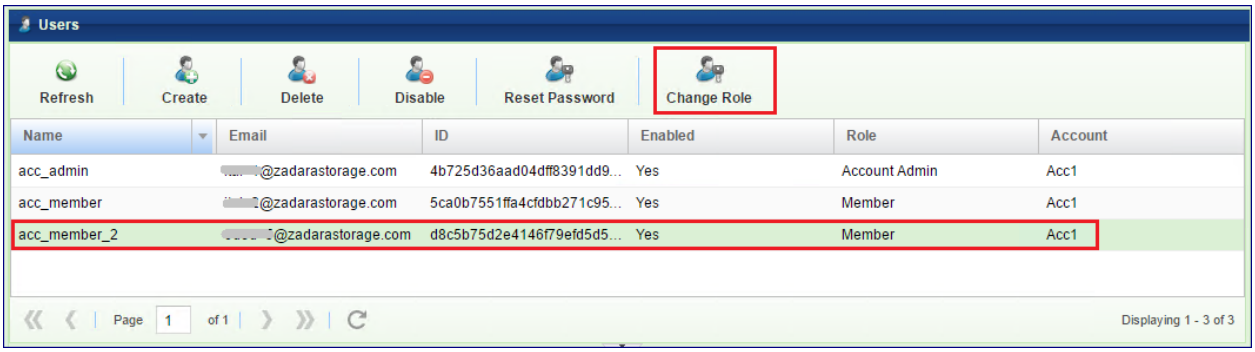
Username: Prod_account_adminAccount: Production_Account

✔ **Note:** Users who have forgotten their password do not need to refer to the admin to reset their password. They can click the **Forgot Password** link on the login screen.

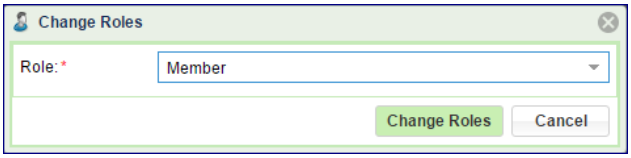
6.6.8 Change Role (VPSA Object Storage Admin, Account Admin)

Account member can be promoted to become an Account Admin, and vice versa. Users under the system account zios_admin can be promoted to VPSA Object Storage Admins only by VPSA Object Storage Admin.

To change someone's role, first select the Users entity in the Main Navigation Panel (Left Panel) under Account Management, select the User for whom you want to promote, and then click the Change Role button in the Center Panel.



In the dialog that open select the new role and click Change Roles

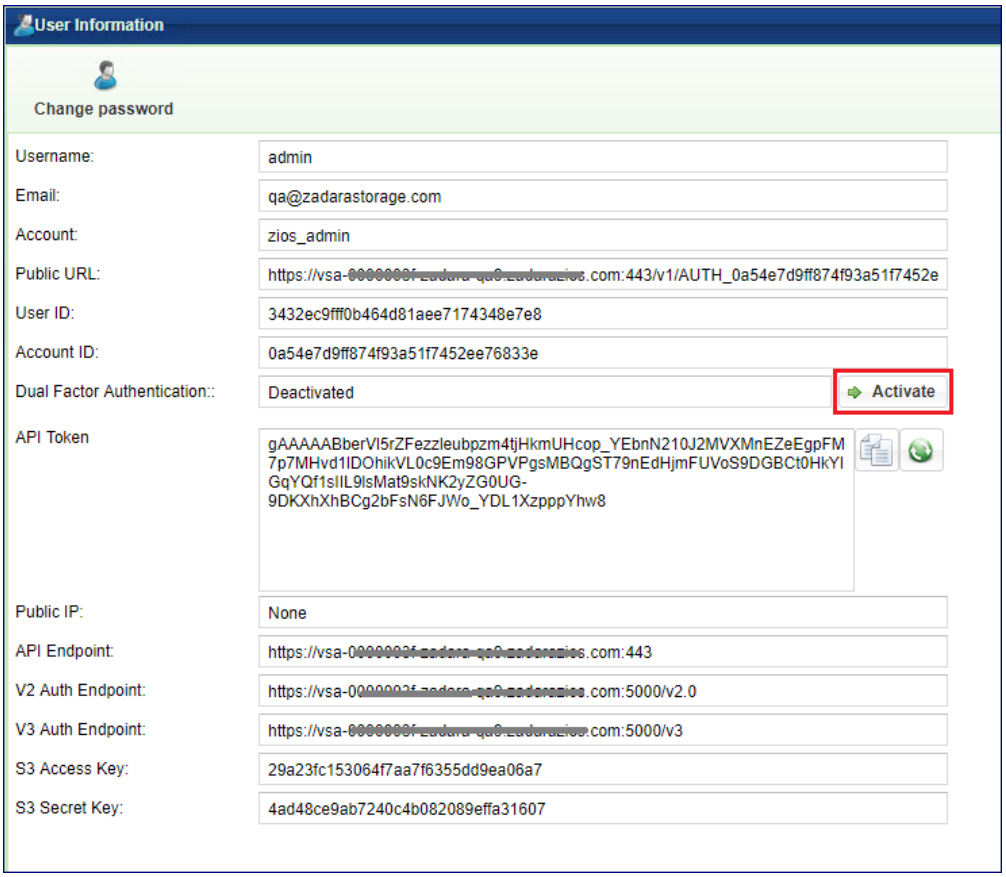


6.7 Dual Factor Authentication

The VPSA Object Storage supports Dual Factor Authentication (DFA) using Authenticator mobile application. It is a common practice to protect access in case of compromised password, as a password is not enough in order to login. Each user can turn Dual Factor Authentication on/off for themself. The VPSA Object Storage admin can force Dual Factor Authentication on all users.

6.7.1 Enabling Dual Factor Authentication

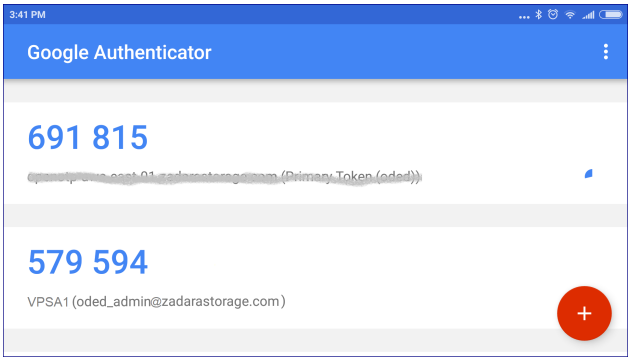
To enable DFA open the current User Properties by clicking the user name on the upper right corner of VPSA GUI screen.



Click Activate or Deactivate. Close the properties dialog, and logout.

The first time you login again, the following screen will pop up.

Install Authenticator mobile app. (e.g. Google Authenticator) from Google Play or Apple AppStore, and scan the QR code. Enter the code you get on the Authenticator. You are now set.

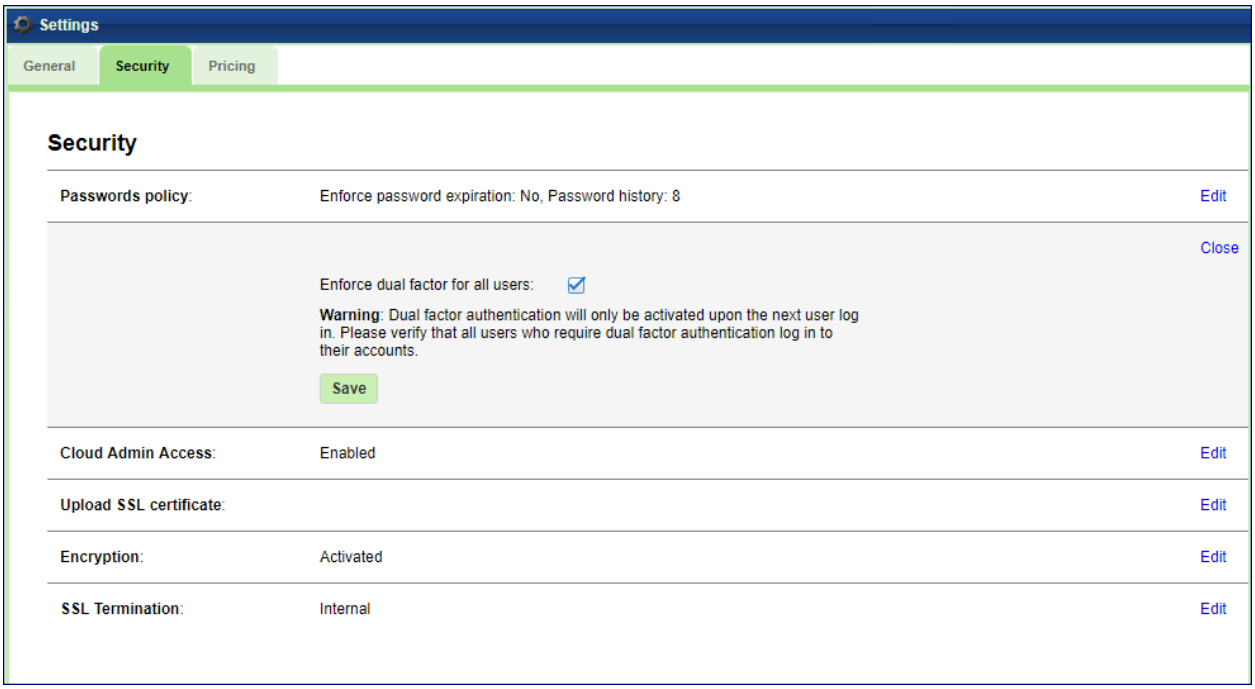


Every login, from now on will require the temporary code from the Authenticator app.

Important: The mobile device that runs the Authenticator app is needed for login. In case the device was lost or replaced, the user must ask the VPSA admin to reset their DFA settings. VPSA admin must contact Zadara support for reset the DFA.

6.7.2 Enforcing Dual Factor Authentication

VPSA administrator can force DFA for all users. In setting/Security click Edit on the Dual Factor Authentication, check the checkbox and Save. This setting change doe not have immediate effect. Next time each user will login, she will be required to set her mobile device Authenticator app as described above.



Note: When DFA enforcement is removed, the users with DFA configured are still required to use the temporary

code when logging in. However each user can change her settings in the user properties as described above.

6.8 Managing Access Control (Permissions)

6.8.1 Understanding Permissions

VPSA Object Storage provides 2 levels of permissions: Account and Container.

Both permissions types are enforced on account Members only, account Admins will always have all permissions.

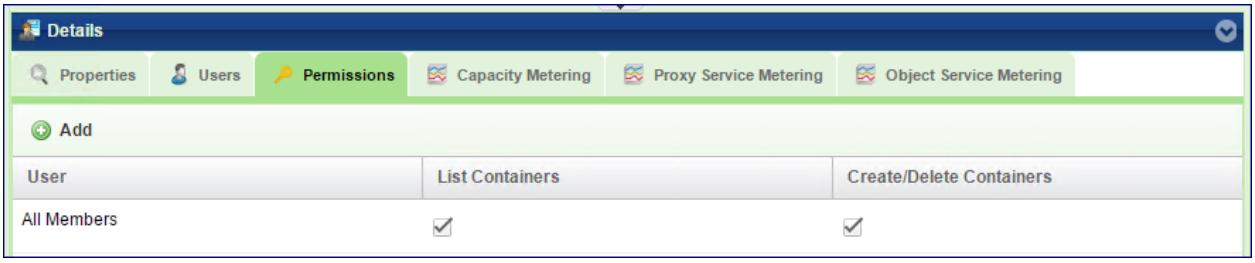
Account-level permissions enforce Read (listing) and Write (creating/deleting) option for **containers** under an account.

Container-level permissions enforce Read (list/download) and Write (upload/delete) options for **objects** under container.

Default Permissions:

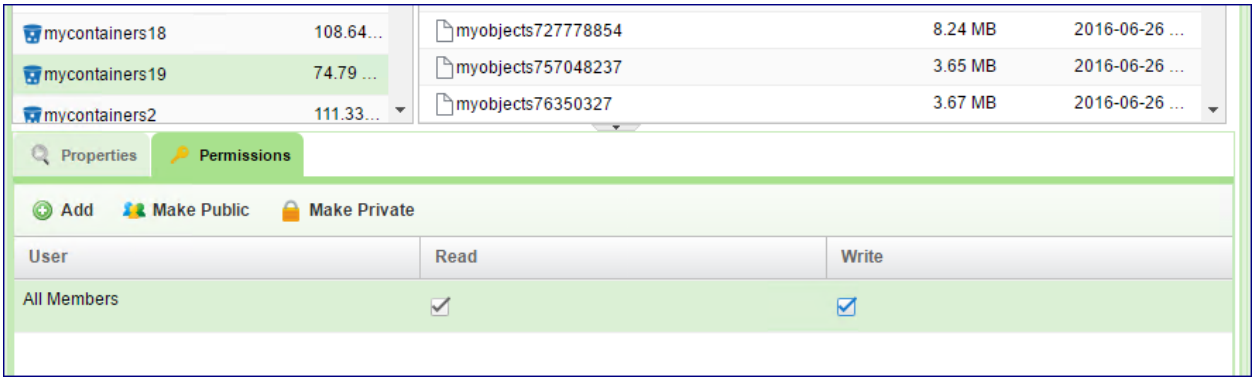
An account is created with default Account-level permissions that allow all account members to list/create/delete containers in the account.

The Account-level permissions can be set after account is created, by Account admin or VPSA Object Storage admin.



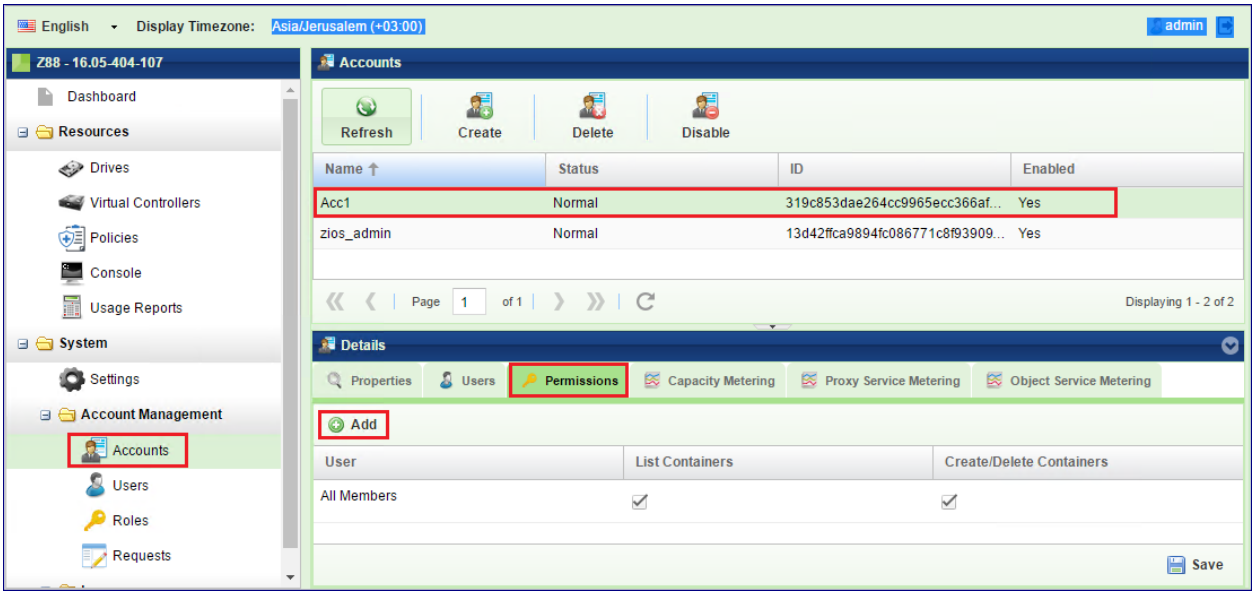
- Container is created with default Container-level permissions that allow all account members to list/get/put/delete objects in the container.

The Container-level permissions can be set after container is created, by account admin or VPSA Object Storage admin.



6.8.2 Setting Account Permissions (Account Admin)

Account-level permissions are set in Account south panel of the GUI by the account admin.

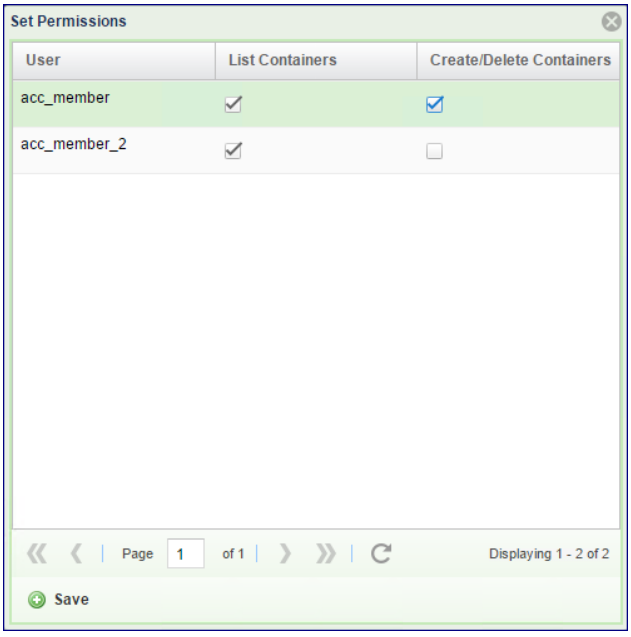


It can be set globally (apply on ALL account members), or explicitly per member or members list.

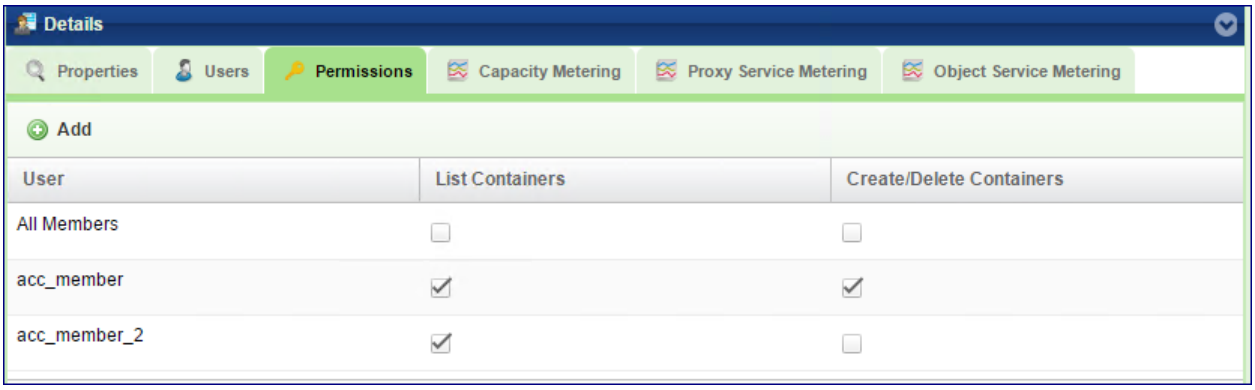
When setting permission per member or members list, the global setting is removed.

To set an explicit permission per user:

- Click on Add button in the permission tab
- Set the required permissions per user
- Click the Save button



The global permissions were removed when the member was added:

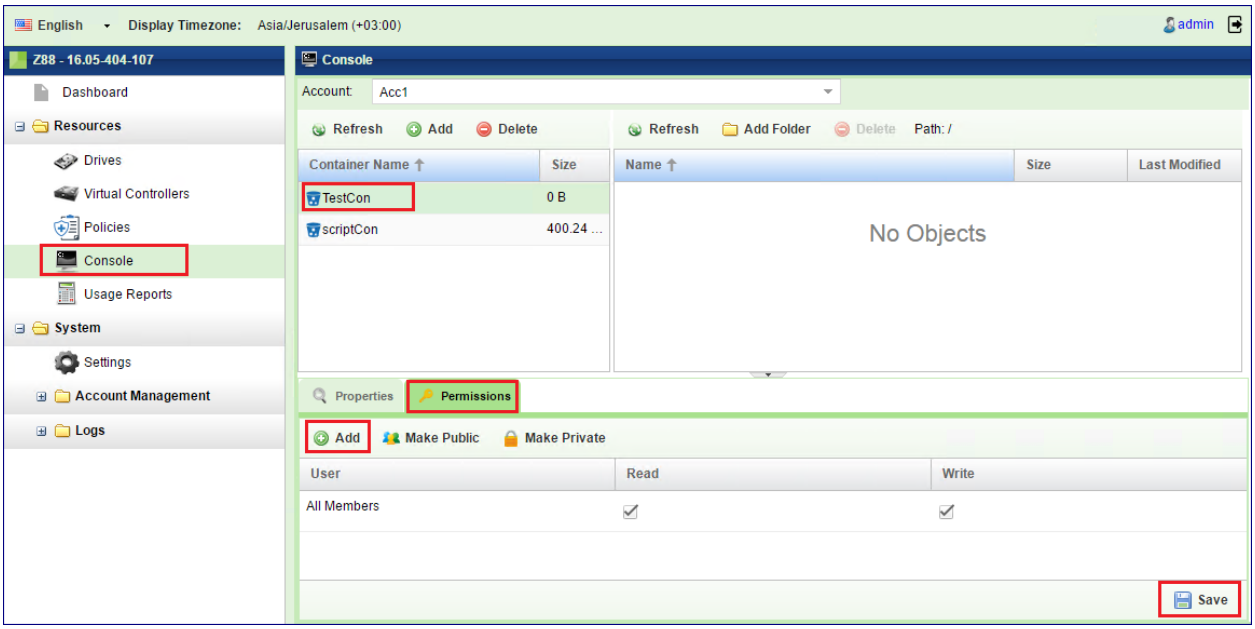


When setting the global permissions back, the member permissions will be removed.

Use the Save button in the down right corner to set permissions in the south tab.

6.8.3 Setting Container Permissions (Account Admin)

Container-level permissions are set in Container south panel in VPSA Object Storage Console by the account admin.



It can be set globally (apply on ALL account members), or explicitly per member or members list.

When setting permission per member or members list, the global setting is removed.

Note: By making a container public (Make Public/Private button) any user can list this container's objects (using "referral" API) even without permissions for this container.*

To set an explicit permission per user:

- Select the Container of interest
- Click on Add button in the permission tab
- Set the required permissions per member

- Click the Save button

The global permissions were removed when the member was added:

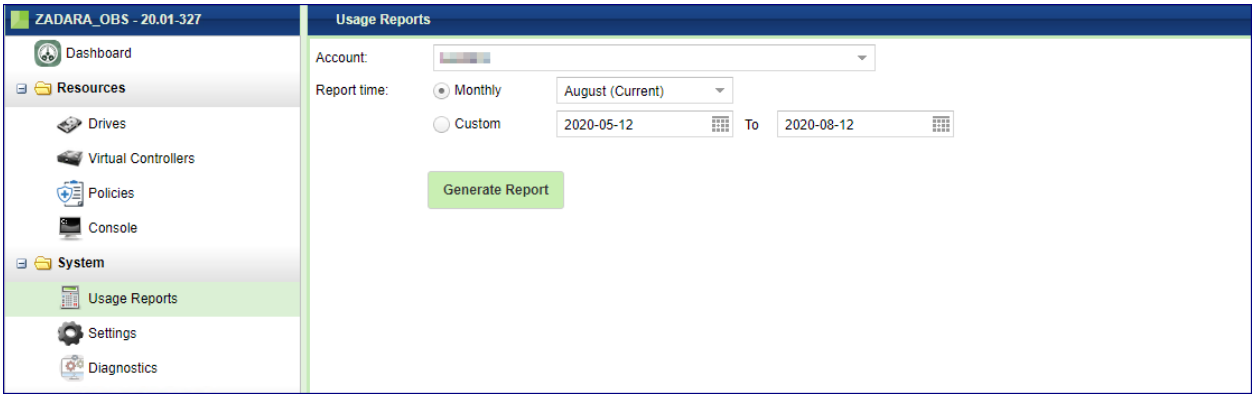
When setting the global permissions back, the member permissions will be removed.

Use the Save button in the down right corner to set permissions in the south tab.

6.9 Generating Usage Reports (VPSA Object Storage Admin)

a VPSA Object Storage administrator (zios_admin) can create a report with all billing metering information, and export the data into any billing system used. This report uses the pricing information that you have set as described in the Pricing settings options and in the Creating Policy (VPSA Object Storage Admin) wizard.

To create a Usage Report, first select the Usage Reports view in the lef navigation menu (left navigation menu) under System. In the main form select the Account you want to create the report for. (You can also select All to create a report for all accounts). Select the period of time for the report (typically monthly, however custom time range can be selected as well), and click Generate Report.



A high level summary of the report will be displayed, the report can be exported to JSON or CSV format with finer granularity.

6.9.1 Usage Reports - Exporting a Summary Report

The exported “Summary Report” include a high-level report, with the same granularity as presented in the management GUI.

For the CSV option, the exported report archive include two CSV files:

1. Report header - the general information for the Object Storage and the account such as:
    - VPSA Object Storage ID
    - VPSA Object Storage name and URL
    - VPSA Object Storage Version
    - Pricing information
    - Reporting interval
2. Usage Summary - the actual usage report information:
    - Billing units
    - Billing sub-category (incoming_bytes, outgoing_bytes and used capacity)

- Container & Object count
- Account information

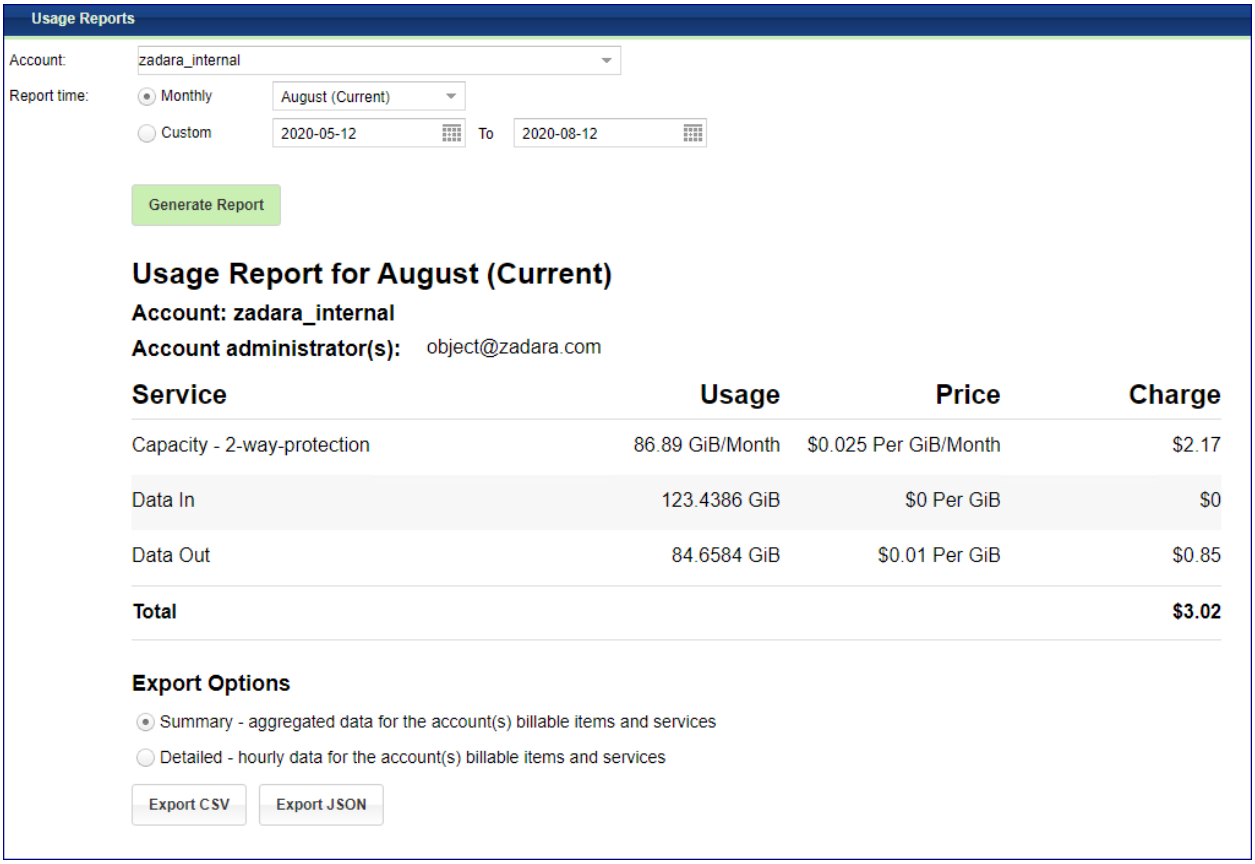
The JSON option will include all of the above information in a single JSON object.

6.9.2 Usage Reports - Exporting a Detailed Report

The exported “Detailed Report” include a finer resolution report, that can assist the VPSA Object Storage administrator to break down the usage report to its building block during the requested time frame.

For the CSV option, the exported report archive include two CSV files:

1. Report header - the general information for the Object Storage and the account such as:
    - VPSA Object Storage ID
    - VPSA Object Storage name and URL
    - VPSA Object Storage Version
    - Pricing information
    - Reporting interval
2. Usage - the actual usage report information, with an hour by hour service breakdown:
    - Billing units
    - Billing sub-category (incoming_bytes, outgoing_bytes and used capacity)
    - Container & Object count
    - Account information



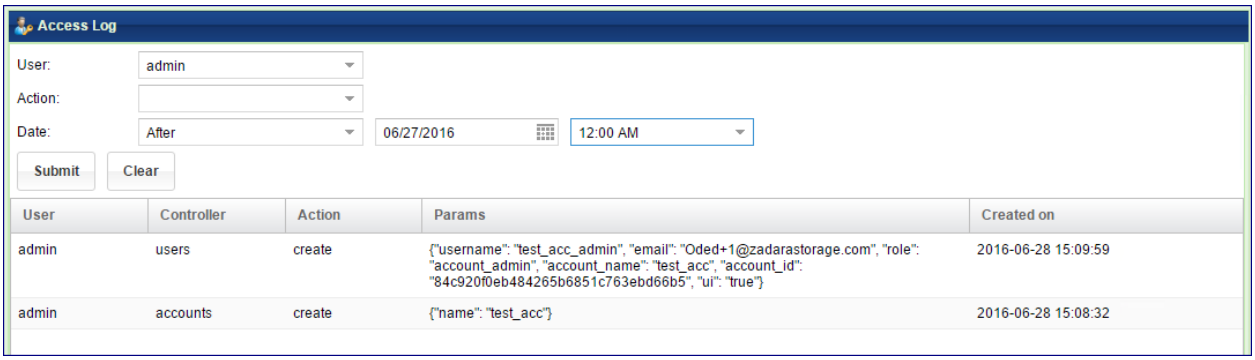
6.10 Object Storage Logs

6.10.1 Access Log (VPSA Object Storage Admin)

Access log lists all operations done by Any user, either using the GUI or the REST API. Each operation is list with all given parameters.

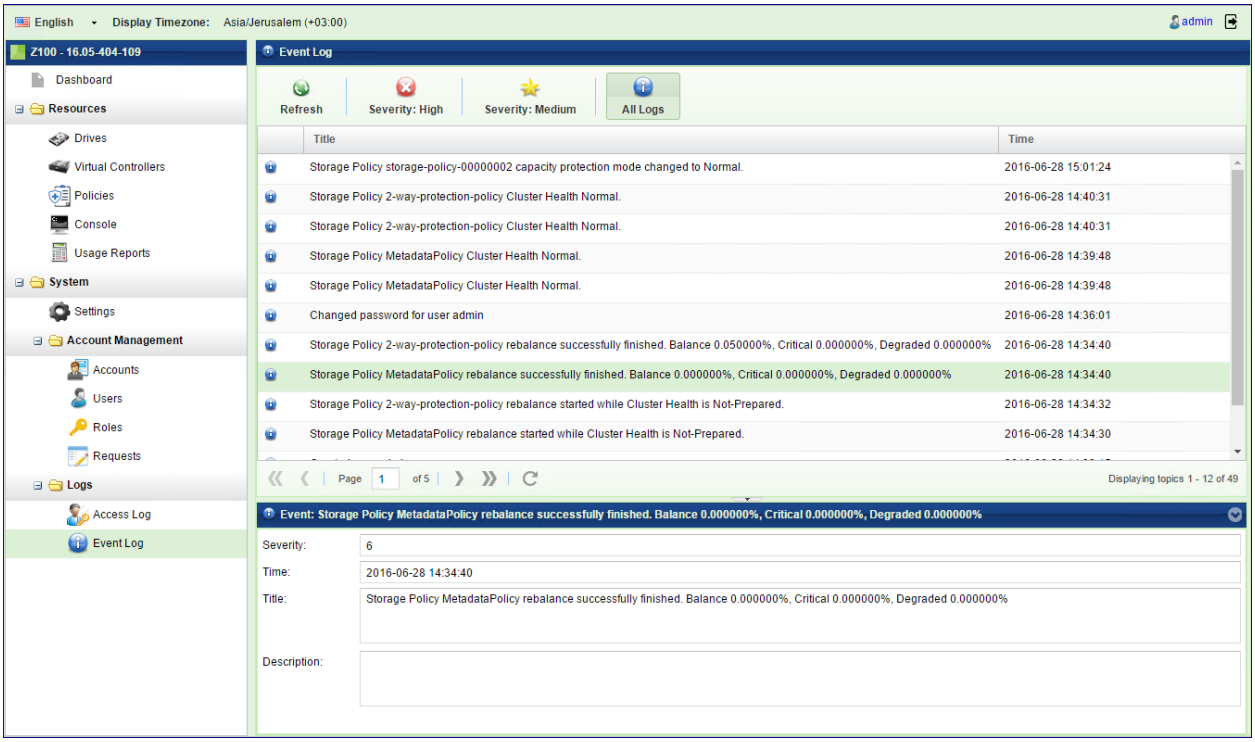
The list can be filtered by:

- User who took the action
- Action type (e.g. create account)
- Date and time



6.10.2 Events Log (VPSA Object Storage Admin)

The events log lists all the events reported by the system. The list can be filtered by severity.



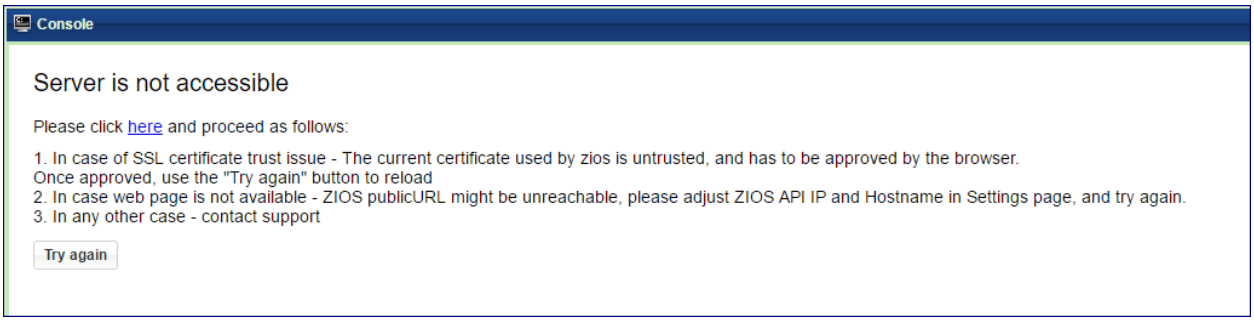
CHAPTER

SEVEN

VPSA OBJECT STORAGE CONSOLE

VPSA Object Storage Console is a tool that gives users visibility into their Object Storage accounts for administration purposes. It is not a tool for read/write operations from/to the object storage. You can create/delete containers, view containers and list their content. You can also create and delete folders to better organized the objects, and set permissions.

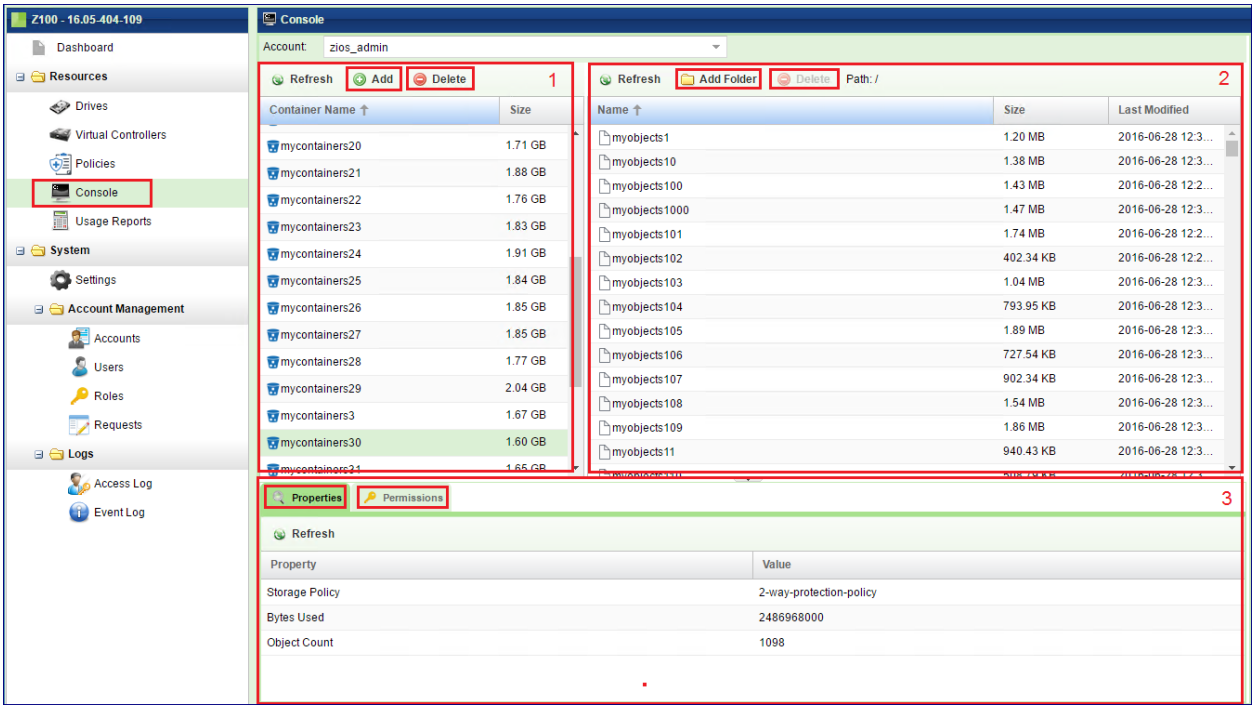
When opening the Console for the first time after changing the default settings, you might get the following error message, as a result of wrong network configuration, or lack of SSL certification trust. Follow the instruction to fix the situation.



7.1 The VPSA Object Storage Console Window

The Console Window is built of the following:

1. Containers pane
2. Objects pane
3. Details south pane, where both properties and permissions can be found.



Note: The Accounts selector above the Containers pane is visible for the VPSA Object Storage Admin only. If you are an account admin/member your account context is well known, and there is no need to select it.

7.2 Encrypted Containers

Encryption management of Data-at-Rest (data on the Disk Drives) is applied by the Object Storage on a per-Container basis. Encrypted and unencrypted Containers can coexist in the same account.

A VPSA Object Storage generates a random 256-bit unique Encryption Key per encrypted Container and uses the Advanced Encryption Standard (AES) to encrypt and decrypt the objects data.

The Encryption Keys are stored on disk as ciphertext, using AES with a 256-bit Master Encryption Key, which is generated from a user-supplied **Master Encryption Password.**

The User owns the Master Encryption Password. It is never stored on any persistent media. Instead, only its SHA3 hash-sum is saved on disk for password validation.

Caution: Since the system does not keep the Master Encryption Password, you are **fully responsible to retain and protect the Master Encryption Password**.

During VPSA Object Storage operation, the Master Encryption Password itself is held in kernel memory of the VPSA. Core-dumping any User Mode process within the VPSA will not reveal the Master Encryption Key.

This method ensures that encrypted Data-at-Rest cannot be accessed without explicitly knowing the user-supplied Master Encryption Password, thus providing you full protection if you opt for Data-at-Rest Volume encryption.

The encryption attribute of a Container cannot be changed! If you'd like to encrypt the objects of a non-encrypted Container, or vice versa, you will need to create a new Container and copy the data.

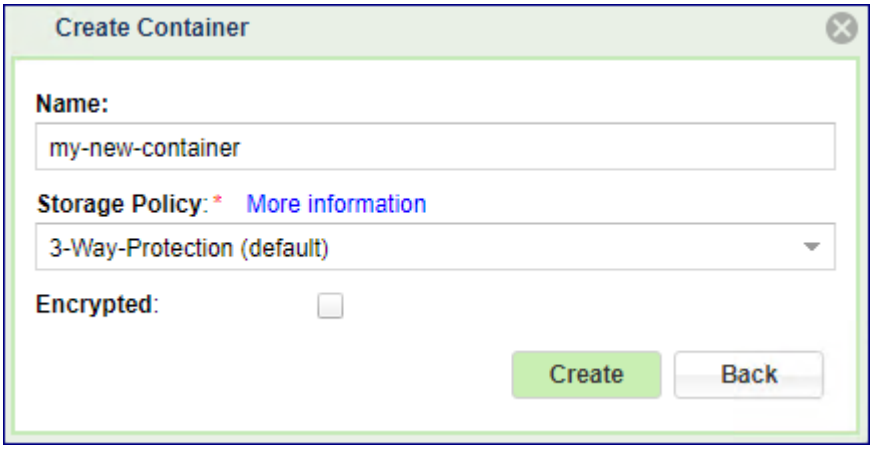
7.2.1 Setting Encryption Password (VPSA Object Storage Admin)

To create a Master Encryption Password, go to the Settings page, Security tab and press the Edit in the Encryption section. Read the instructions and warning. Type your Password and Save.

Store your Master Encryption Password in a secure place

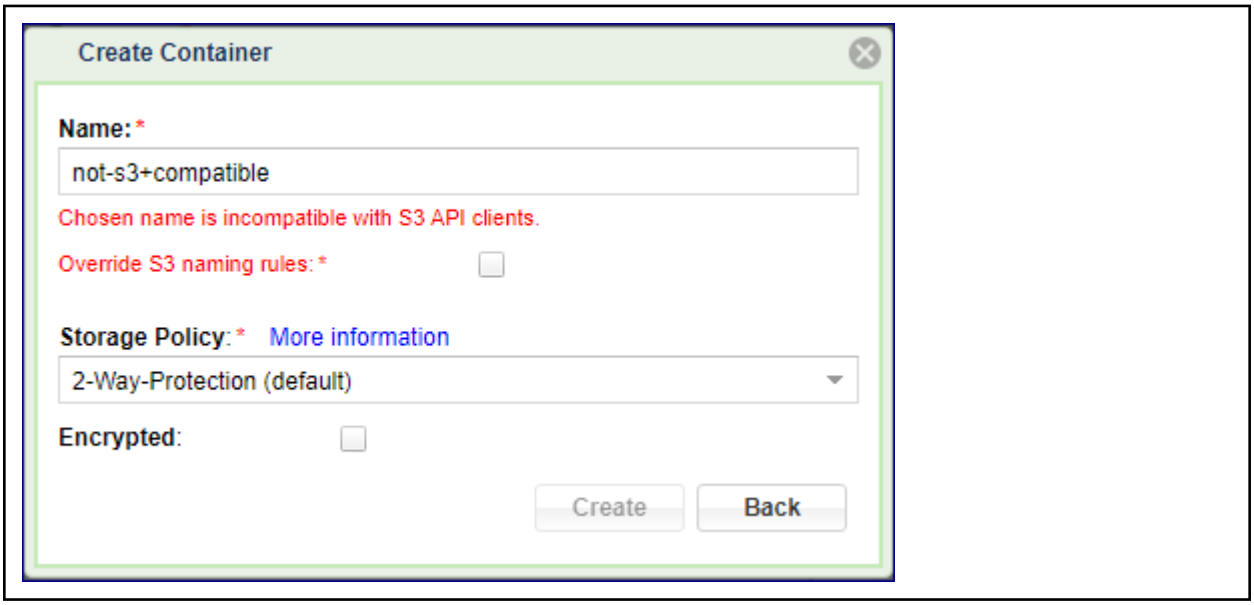
7.3 Create Container

To create a new Container in the account open the Console, go to the Containers pane, and click Add.



The system will prompt you for the Container's name, and will let you select the storage Policy that will contain the newly created Container.

Warning: The VPSA Object Storage is both S3 and Swift API protocol compatible. S3 containers are expected to contain only lowercase letters, numbers, periods and dashed. The Swift API is less restrictive, container name can start with any character and contain any pattern. The container name cannot contain a slash (/) character because this character delimits the container and object name. The creation wizard will verify the proposed container name, a warning message will be displayed in case a non-s3 compatible name was chosen. This restriction can be overridden by checking the Override S3 naming rules checkbox.



The Policy that you have defined as "default" here Set default Policy (VPSA Object Storage Admin) will be automatically selected. Clicking on More information will display details about the selected policy including rates.

If you want this Container to be encrypted check the Encrypted checkbox.

Click Create.

The new container will show up in the Containers pane. See here Setting Container Permissions (Account Admin) regarding assigning permissions for the new Container.

7.4 Object Versioning

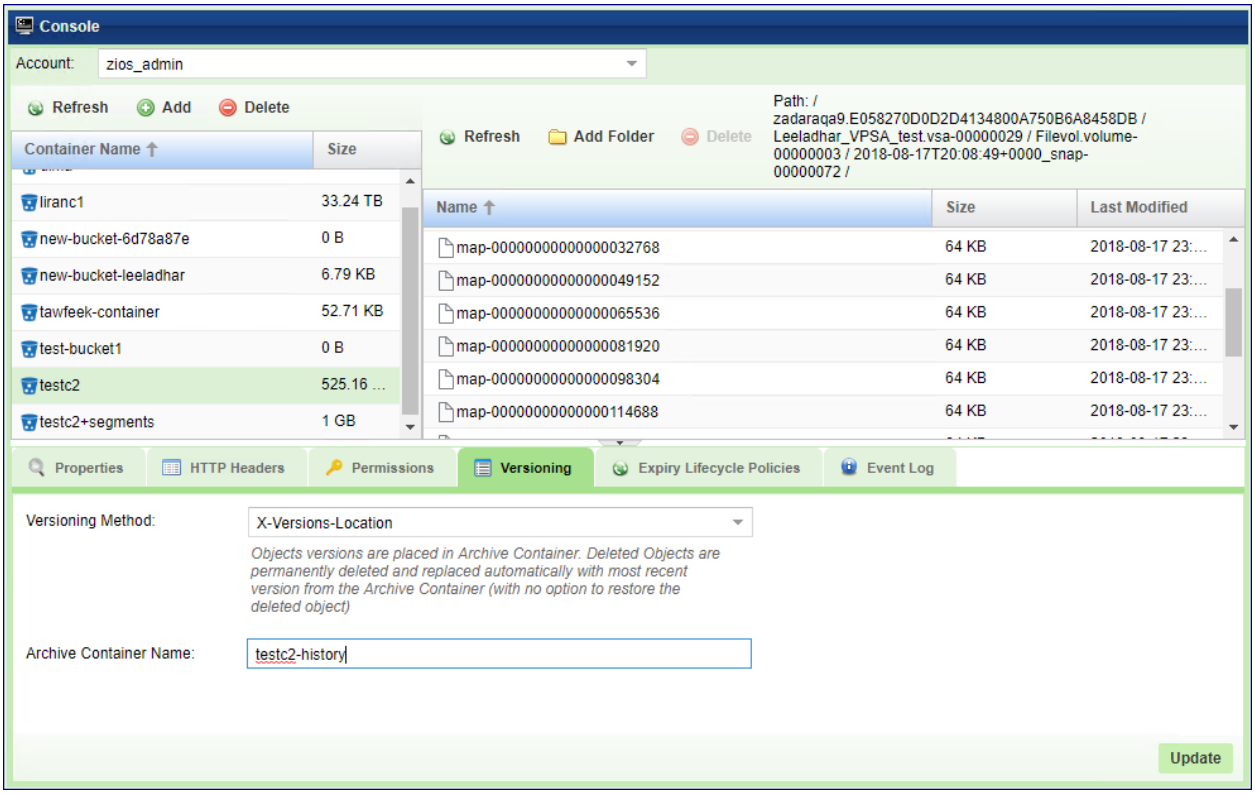
Object versioning is implemented by setting a flag on the container to tell the object storage to version all objects in the container. The value of the flag is the container where the versions are stored (commonly referred to as the "archive container").

There are 2 types of versioning supported by the Object Storage: X-History-Location and X-Versions-Location. They differ by behavior when an Object is deleted.

Once the versioning flag is set to **X-History-Location** on a container, on DELETE operation the deleted Objects are moved to the Archive Container with a Deleted Marker for future restore.

Once the versioning flag is set to **X-Versions-Location** on a container, DELETE operation only removes the current version of the object. If any previous versions exist in the archive container, the most recent one is copied over the current version, and the copy in the archive container is deleted. As a result, if you have 5 total versions of the object, you must delete the object 5 times for that object to be removed.

To set the versioning flag on a Container open the Console, go to the Containers pane, select the container of interest, go to the south pane, and select the HTTP Headers tab and click Add.

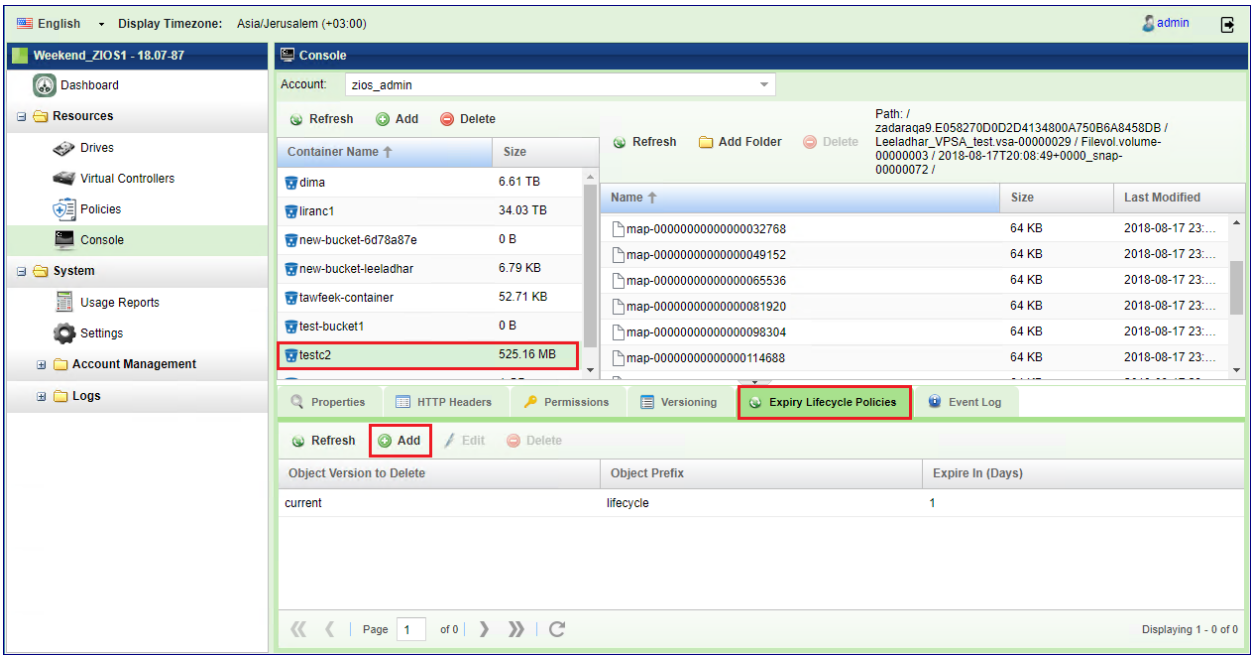


- In the Versioning Method filed select: “X-Versions-Location” or “X-History-Location”
- In the Archive Container Name field put the name of the container where you want to keep the previous versions.
- Click Update

7.5 Setting Objects Lifecycle Policy

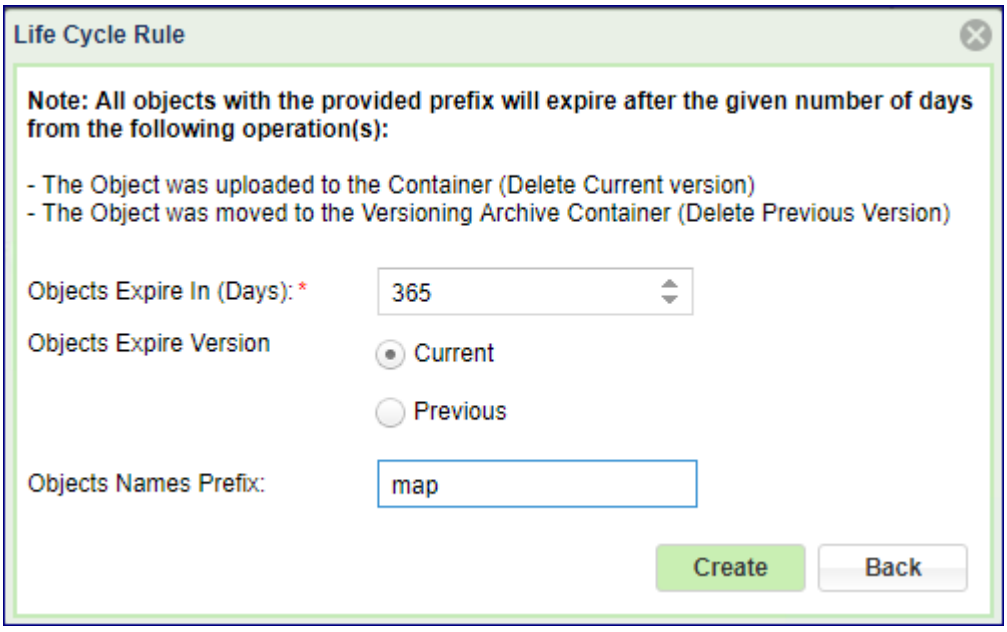
Zadara Object Storage supports retention period for objects. The period is set at the object creation time, and it will be automatically removed when expired. It is possible to set number of such policies per Container, for different types of objects.

To create a new expiration policy in the account open the Console, go to the Containers pane and select the Container of interest. On the right lower hand pane click the Expiry Lifecycle Policies tab and click Add.



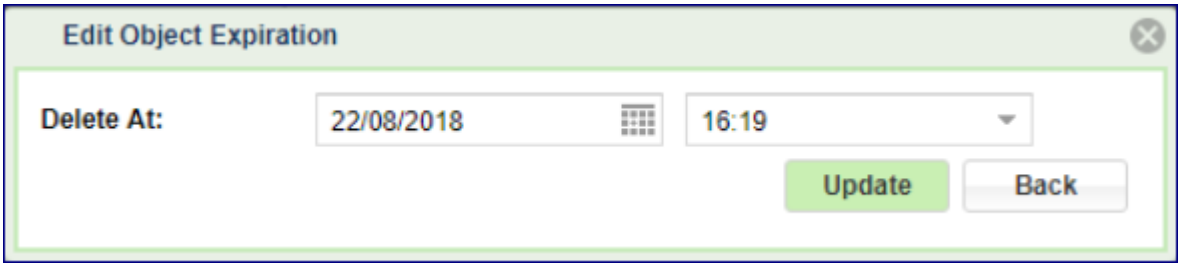
In the dialog that opens set the retention period in days, and you can add an object name prefix. If prefix is given only Objects with such names will be removed by this policy. If the field is left empty, all Objects are affected. If versioning is not enabled for this Container (See Object Versioning) the Lifecycle policy always affects the current version of the object. If versioning is enabled, you can set policies for both the current version of the object (in the current Container) and for the previous version (in the archive Container). For example, you can set policies that an object expires after 90 days, and every time the object is updated, the previous version is kept for week.

Click Create.



From now on every object that will be placed in this container will get an expiration date according to the defined policy.

You can modify the expiration date/time of an object by selecting the relevant object and clicking Edit in the Properties pane.



Lifecycle Policies can be modified by selecting the relevant policy and pressing Edit.

Lifecycle Policies can be removed by selecting the relevant policy and pressing Delete.

Note: Removing the life cycle rule, does not affect objects that were created while this rule was effective. To prevent deletion of these objects at the expiration date, you must explicitly remove the delete_at header of these objects.

7.6 Delete Containers

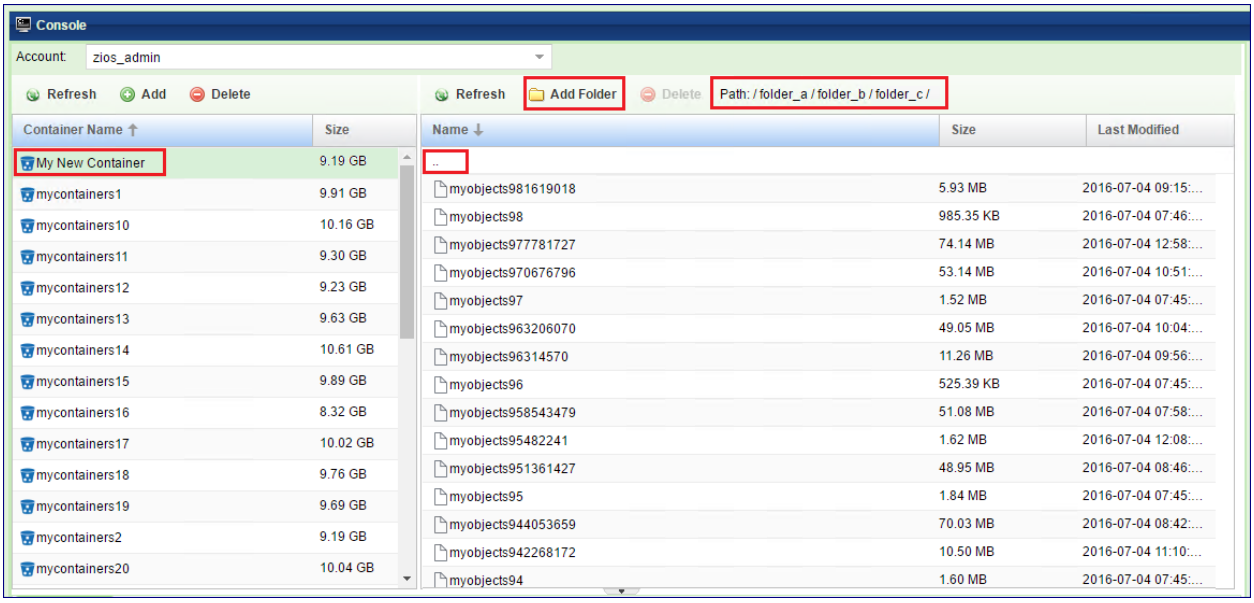
To remove a Container open the Console, go to the Containers pane, select the container to be deleted and click Delete. The system will prompt you for deletion confirmation. After confirming the container **with all its content** will be deleted.

7.7 Adding folders

By definition, containers are flat, and there is no hierarchy structure, for storing the objects. However, since many users are used to the folders tree concept of file systems, VPSA Object Storage Console gives you an option to simulate hierarchical structure within the Object Storage Containers.

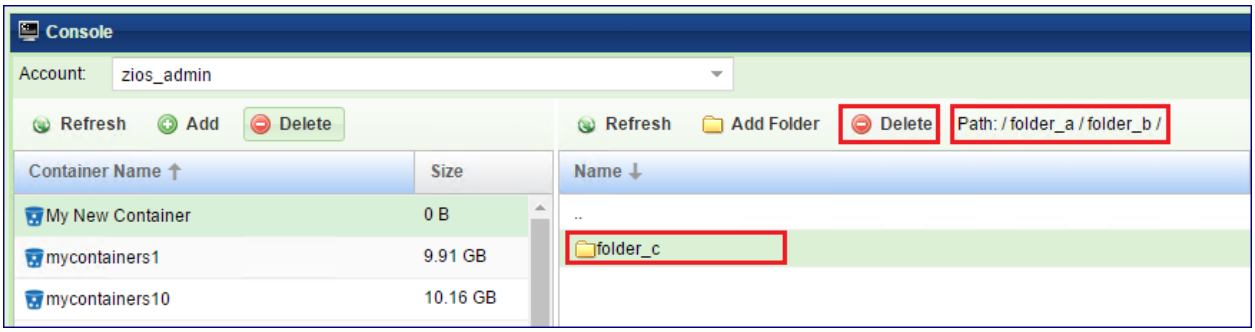
To create a folder open the Console, select a Container in the Containers pane, Navigate to the hierarchy level where you want to create the new Folder, and click Add Folder. Give it a name and click Submit.

Navigation within the Container's Folders tree is done in a way similar to the common user experience of file systems explorer. By double clicking a folder you enter it and see its content (Objects and sub Folders). By double clicking the .. at the top of the Objects pane, you navigate one level up to the parent Folder. The Path indicator above the Objects pane always show you current position in the tree.



7.8 Removing folders

To remove a folder, Navigate to its parent folder, select the folder to be removed and click Delete.



After confirmation the Folder with all its content will be deleted

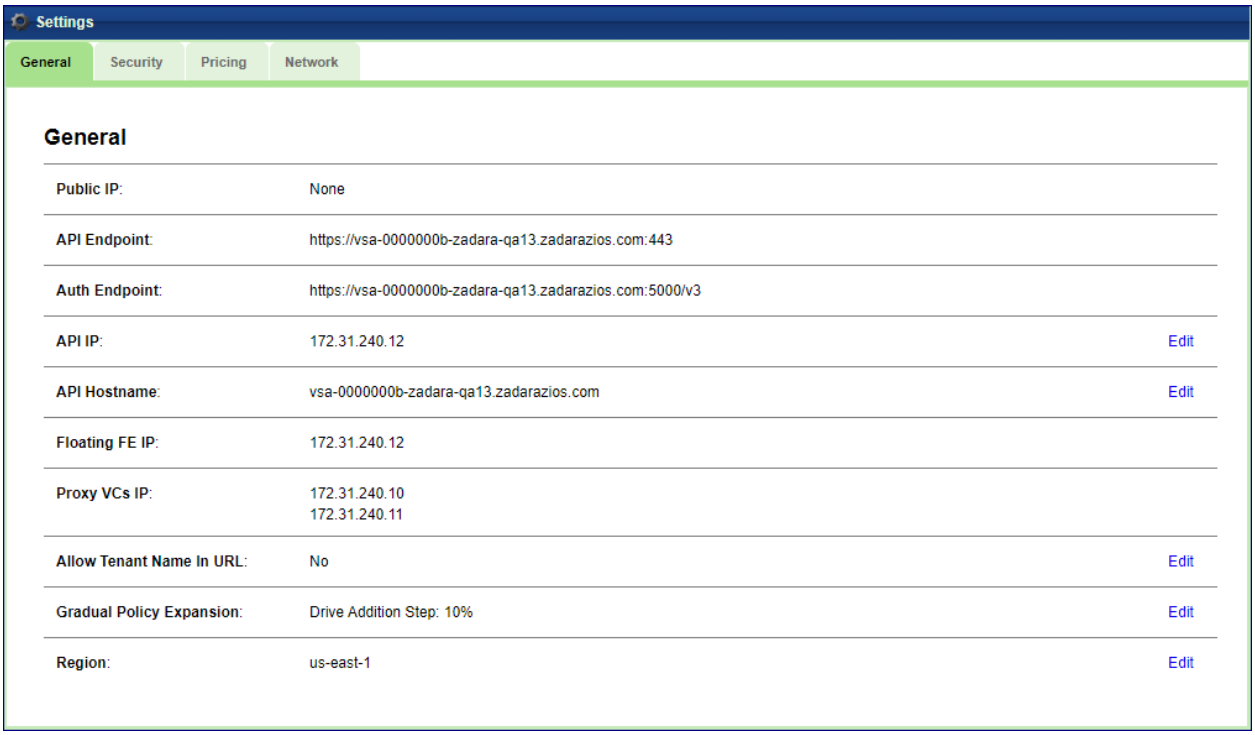
CHAPTER

EIGHT

VPSA OBJECT STORAGE SETTINGS

8.1 General settings

VPSA Object Storage settings is a list of configuration settings. Some are displayed for information purposes only, other can be modified. To change a setting parameter click the edit link next to it.



Public IP: (read only)

An IP address that allows access to the VPSA Object Storage system from the Internet. Assigning Public IP is done via the Zadara Provisioning Portal, as described here Assigning Public IPs (VPSA Object Storage Admin). In order to access the Object Storage over the Public IP, make sure to set the VPSA Object Storage API IP to the assigned Public IP or to set the VPSA Object Storage API Hostname to its registered domain.

API Endpoint: (read only)

The effective address for VPSA Object Storage REST API for all IO requests. It depends on the setting of the VPSA Object Storage API IP and VPSA Object Storage API Hostname, below.

Auth Endpoint: (read only)

The effective address for VPSA Object Storage REST API for all authentication requests. This field depends on the setting of the VPSA Object Storage API IP and VPSA Object Storage API Hostname, below. Starting from version 19.08 the deafult suppoted authenction for Openstack Swift client is Keystone v3 authenction. The support for Keystone v2 was deprecated.

API Hostname:

VPSA Object Storage FQDN.

Note: For the VPSA Object Storage API Hostname either static IP, or FQDN must be given.

Floating FE IP: (read only)

The floating frontend IP address used by the Object Storage.

Proxy VC IP: (read only)

The Object Storage VC's IP frontend addresses.

Load Balancer Group IP: (read only) List the LBG IP addresses (in case the Elastic Load Balancer is enabled)

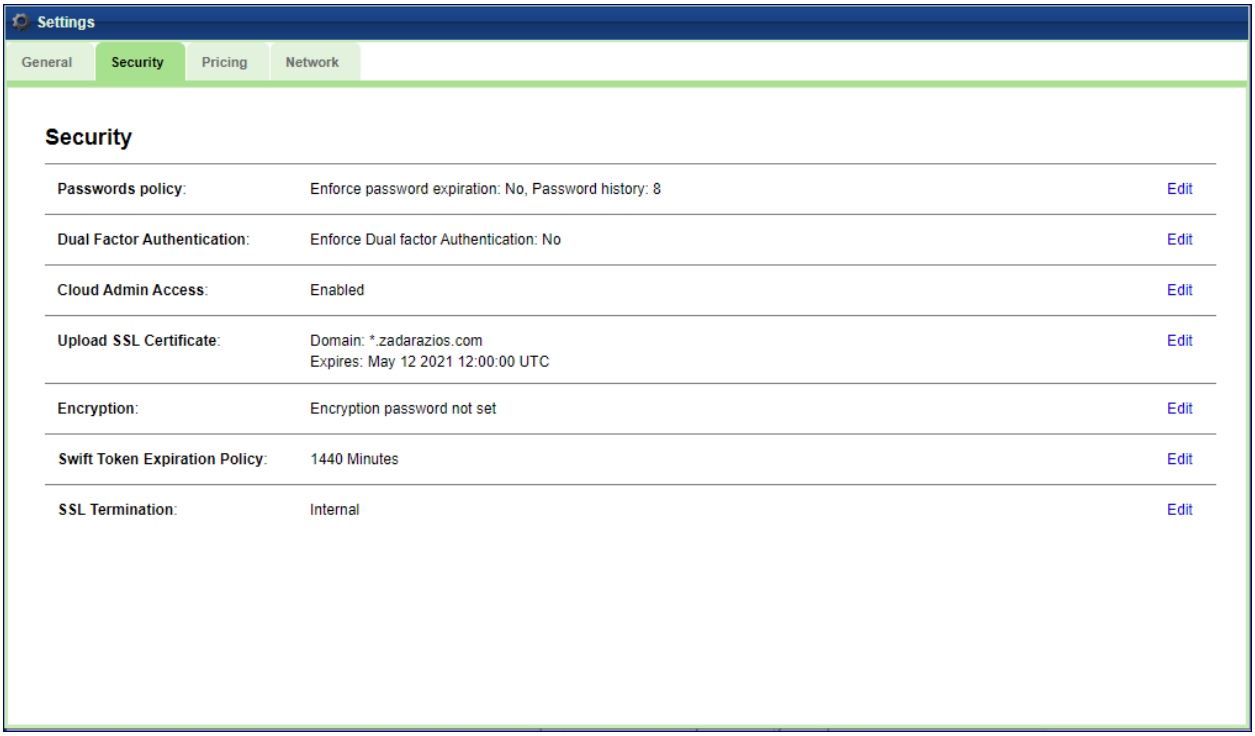
Allow Tenant Name In URL: Allow specifying the tenant name in the URL passed in the API instead of its ID. (Default: No)

Gradual Policy Expansion: The "Drive Addition Step" will enforce gradual disk addition to a given policy, expanding a data policy gradually will reduce the impact of the Data Policy performance throughout the expansion process. The Object Storage administrator may adjust the drive additon step to expedite the expansion process. (Default: 10%)

Region:

For AWS v4 signature, "region" (also called bucket_location) must be specified for the signature to work. Default is US. Some S3 compatiable object storage clients expect to have us-east-1 as the default region, in such case the Object Storage administrator is required to adjust the Object Storage region accordingly.

8.2 Security settings



Password Policy:

VPSA Admin can control the VPSA Password expiration policy and password history policy.

Dual Factor Authentication: Enforce Dual Factor Authentication for all users.

Cloud Admin Access:

This sets the cloud admin's VPSA GUI access (via the Command Center), to Enabled/Disabled status.

Upload SSL Certificate: (Optional)

VPSA Object Storage REST API works over HTTPS with SSL certificate. VPSA Object Storage defaults to its built in SSL certificate (issued for zadarazios.com domain). In case the Object Storage administrator may want to use its own certificate, upload it in this section. The supported certificate format is "PEM". SSL "PEM" certificate format, as defined in RFCs 1421 through 1424, is a concatenated certificate container files. It is expected that the Object Storage administrator will append the private-key to the certificate prior uploading it.

The resulting PEM should like like this:

```
-----BEGIN RSA PRIVATE KEY-----
(Your Private Key: your_domain_name.key)
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
(Your Primary SSL certificate: your_domain_name.crt)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your Intermediate certificate: Intermediate.crt)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your Root certificate: RootCertificate.crt)
-----END CERTIFICATE-----
```

✔ **Note:** Make sure the certificate used is issued for the Hostname or IP specified in VPSA Object Storage endpoints listed above

Encryption:

This sets the encryption password for the Object Storage data-at-rest encryption.

For more information on encrypted containers see Encrypted Containers .

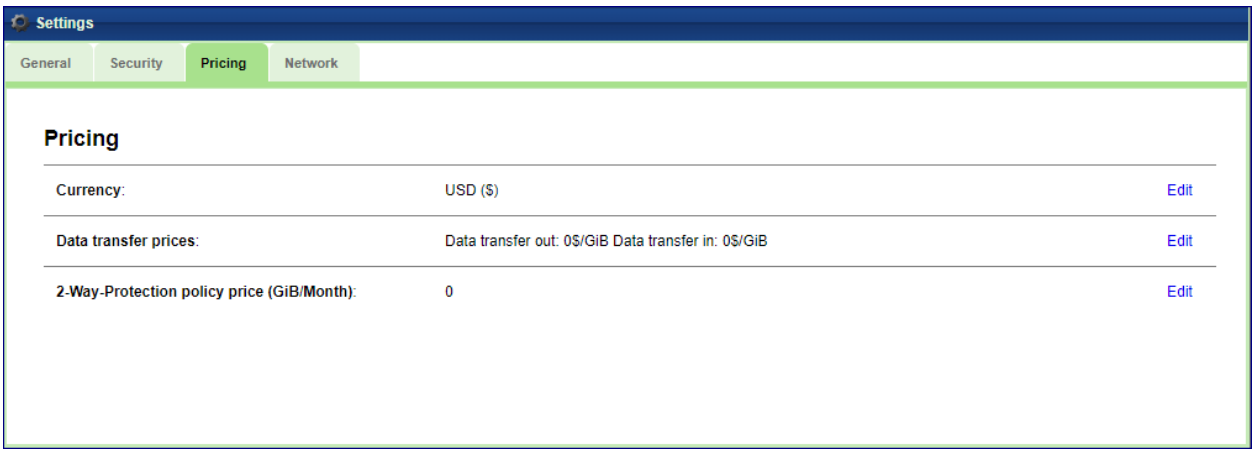
Swift Token Expiration

Swift token expiration can be set manually, default is one day (14,440 minutes).

SSL Termination:

Internal (default)/external. By default the HTTPS traffic enters the Object Storage proxy server and encryption/decryption is done internally. Users In case of an external load balancer, it is recommended to offload the SSL termination to the external load balancer, should select "external". In this case the VPSA Object Storage expects HTTP traffic (not encrypted).

8.3 Pricing settings



Currency:

Select the currency used for billing purposes. Supported currencies are:

1. USD - USA Dollar
2. GBP - Great Britain Pound
3. EUR - Euro
4. AUD - Australia Dollar
5. KRW - South Korea Won
6. JPY - Japan Yen
7. CNY - China Yuan

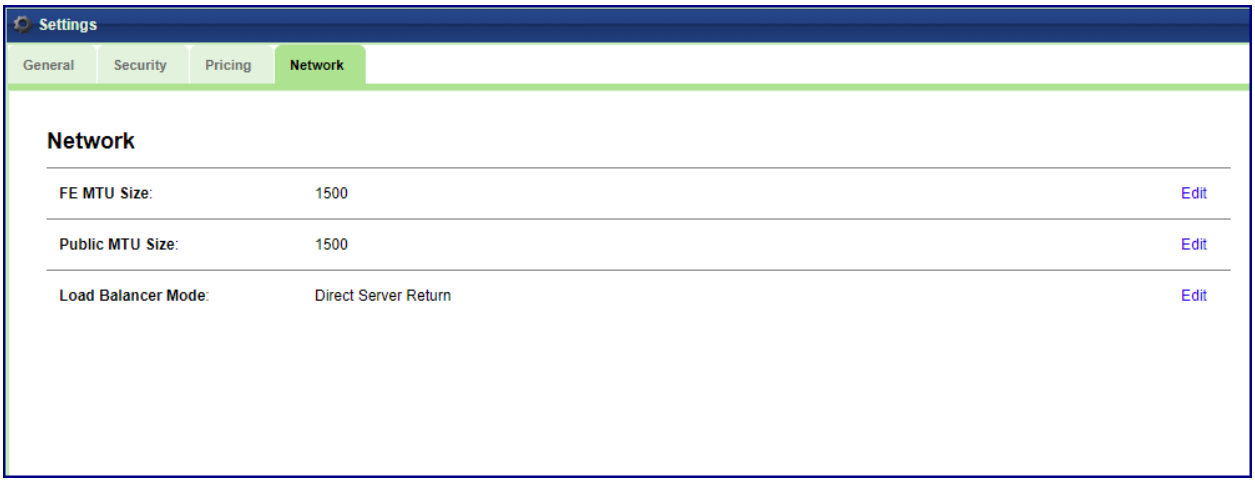
Data Transfer Pricing:

If you want to charge your internal/external customers for the traffic going into and from VPSA Object Storage, you can specify your currency and pricing in the Setting>Pricing tab.

Storage Capacity Pricing:

Pricing for stored capacity depends on the storage Policy used. Therefore the capacity price is set per Policy as the price per GB per month. In case multiple Data Policies exist, a different pricing can be configured for each Data Policy.

8.4 Network settings



FE MTU Size: Modify the MTU size for the Frontend interface (1500 - Default, 2048, 4096, 9000)

Public MTU Size: Modify the MTU size for the Public interface (1500 - Default, 2048, 4096, 9000)

Load Balancer Mode: Toggle the internal load balancer & Zadara Elastic Load Balancer mode of operation:

- **Direct Server Return (default)** - Recommended for scale. Packets from the Object Storage Virtual Controller bypass the load balancer, maximizing the egress throuphput.
- **NAT** - The load balancer will be used as a gateway for all traffic from /to the object storage virtual controller.

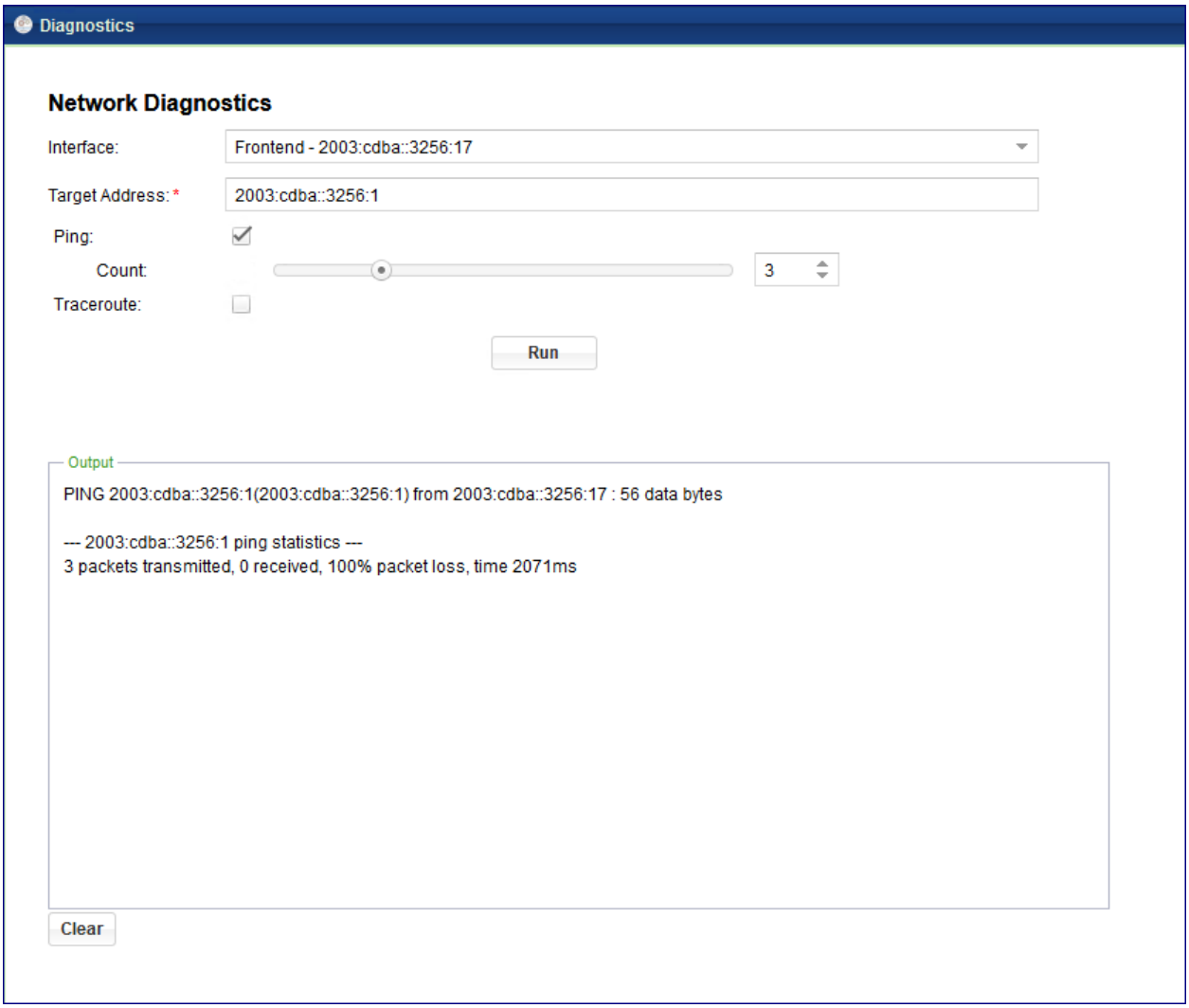
> **Warning:** Changing the Load Balancer mode of operation can be distruptive for existing clients workload.

CHAPTER

NINE

VPSA OBJECT STORAGE NETWORK DIAGNOSTICS

This view allow the VPSA Object Storage Admin to perform connectivity checks from within the VPSA Object Storage itself throughout his servers/networking devices.



Interface: Select the source interface of the VPSA Object Storage (Frontend, Public IP)

Target Address: IPv4 (or IPv6) of the target network device/server.

Ping: Checkbox - perform a ping test (count - number of echo requests to send).

Traceroute:: Checkbox - Perform a traceroute scan to the target host.

CHAPTER

TEN

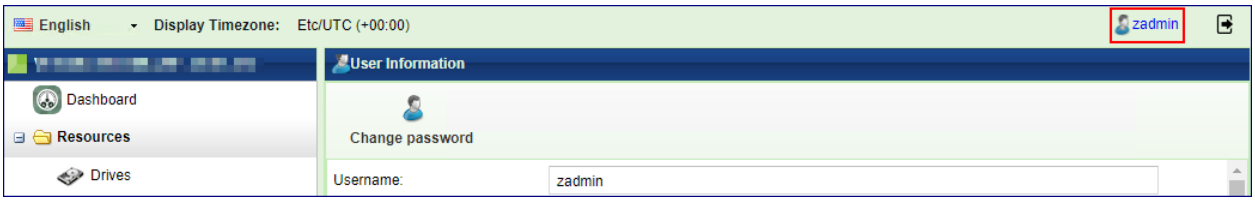
OBJECT STORAGE CLIENTS - CONFIGURATION

Standard client tools can be used to browse objects in VPSA Object Storage. This Appendix will help configuring Object Storage Client Tools to work against VPSA Object Storage. In order to access the VPSA Object Storage the client tool must be configured with the user's authentication credentials.

The VPSA Object Storage support two API interfaces:

1. Openstack Swift API
2. AWS S3 API

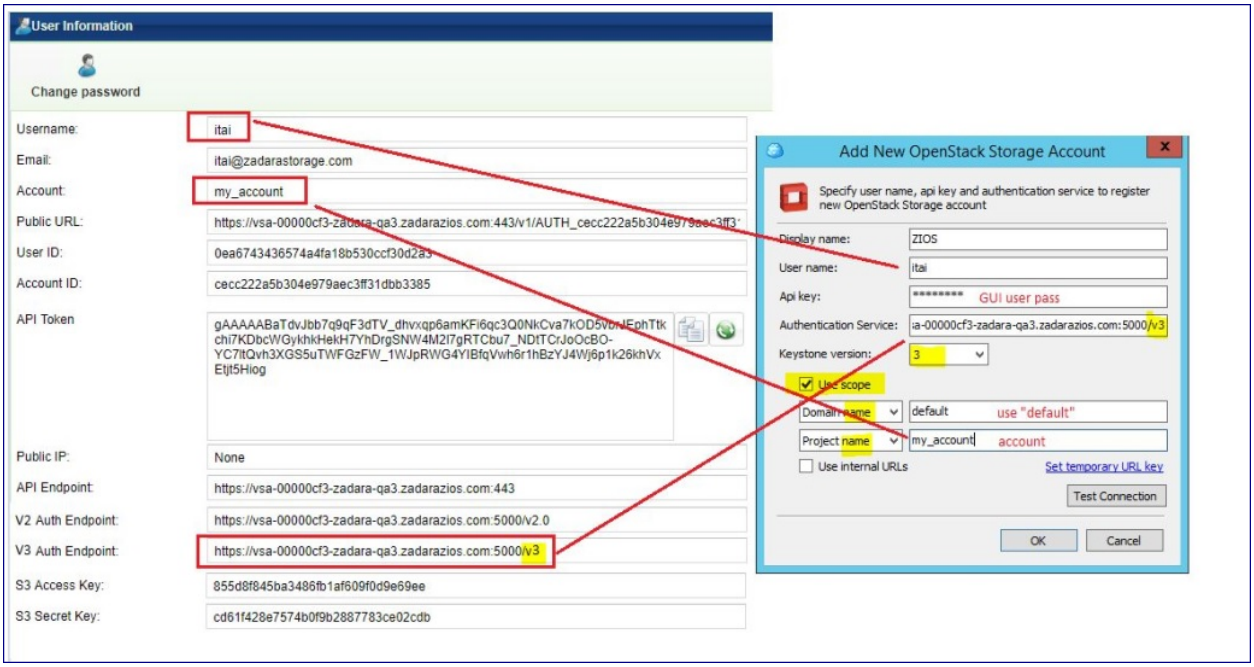
The Needed parameters can be found in the Object Storage User Information page. Information about the user currently logged in to the Object Storage GUI is displayed by clicking the user name on the GUI upper right corner.



10.1 Openstack Swift Interface

10.1.1 Cloudberry Explorer for OpenStack (v3 authentication)

Use the logged-in User Information properties to set the authentication fields of Cloudberry Explorer



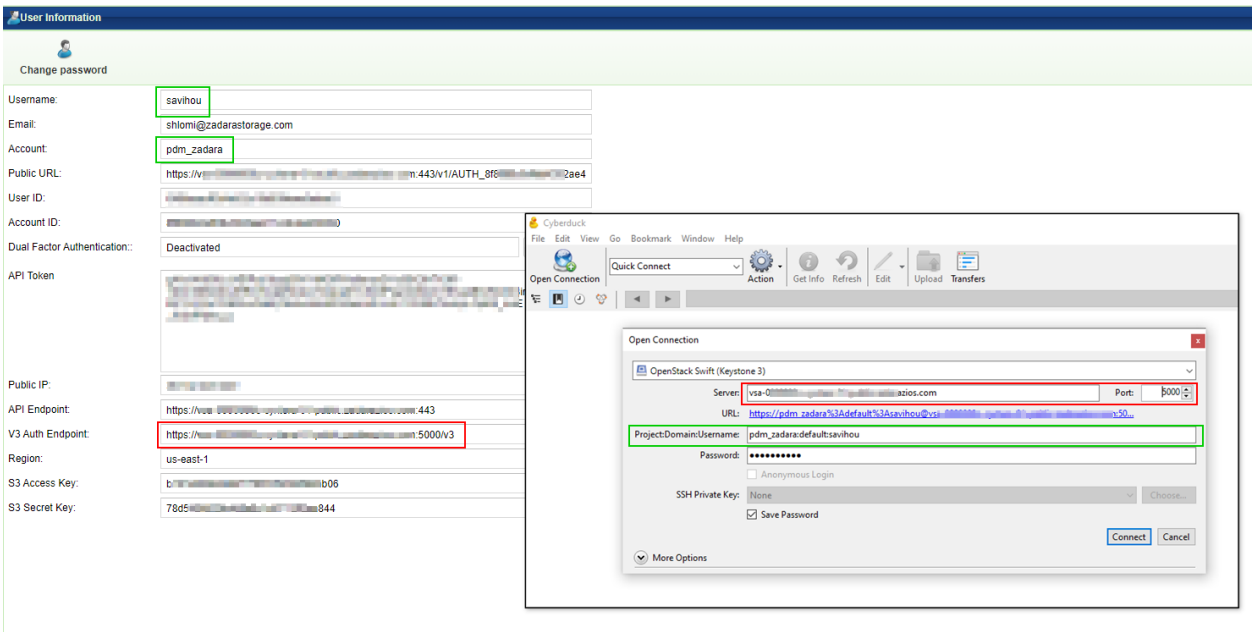
10.1.2 CyberDuck

Cyberduck version: 7.7.1 (33788)

Cyberduck client support “Openstack Swift (Keystone 3)” API interface.

Use the logged-in User Information properties to set the authentication field of CyberDuck client.

1. Server - the VPSA Object Storage v3 Auth Endpoint.
2. Port - 5000
3. Project:Domain:Username - <VPSA Object Storage Account>:default:<VPSA Object Storage Username>



10.1.3 cURL (swift API)

cURL can be used for Object Storage operations. The connectiviy information is available in the User Information view.

In this example, we will use the API Token and Account URL in order to create a new container:

```
$ curl -H "x-auth-token: <user_token>" -X PUT <account_url>/test-bucket1/
$ URL=https://vsa-00000001-mycloud-01.zadarazios.com:443/v1/AUTH_123456789
$ TOKEN=<MYAPI TOKEN>
$ curl -H "x-auth-token: $TOKEN" -X PUT $URL/test-bucket1/
```

Important: By default, the API token is valid for 24 hours. the preferred option to identify/renew the API token via an API call is to use a Swift command and not the VPSA Object Storage command indicated in the Zadara Storage VPSA Object Storage REST API User Guide here: http://zios-api.zadarastorage.com .

The following example describes how to get the token programmatically using the Swift API:

```
$ curl -i -H "Content-Type: application/json" \
-d '{ "auth": \
{ "identity": { "methods": ["password"], "password": \
{ "user": {"name": "<USERNAME>", "domain": { "id": "default" }, \
"password": "<USER PASSWORD>" }} }, "scope": { "project": \
{ "name": "<ACCOUNT_NAME>", "domain": { "id": "default" } } } } }' \
"https://vsa-00000001-mycloud-01.zadarazios.com:5000/v3/auth/tokens" ;
```

and use the returned token for the subsequent API calls.

```
HTTP/1.1 201 Created
Date: Thu, 19 Nov 2020 16:05:28 GMT
Server: Apache/2.4.29 (Ubuntu)
Content-Length: 1114
X-Subject-Token: gAAAAABftpfIAiuo2tRZZP8VVtomU1knVG7xNUONV4b2u....
```

Additional examples of using the Openstack Swift API can be found at the Openstack Swift API documentation

10.2 AWS S3 Compatible clients

10.2.1 Supported S3 APIs

The VPSA Object Storage is utilizing Openstack Swift's S3 Middleware. As S3 is an AWS product, It includes some features that are AWS oriented and are outside of the scope of Zadara's Object Storage offering.

The list of supported S3 operations can be found in the S3/Swift REST API Comparison Matrix.

Zadara have added a specific support for:

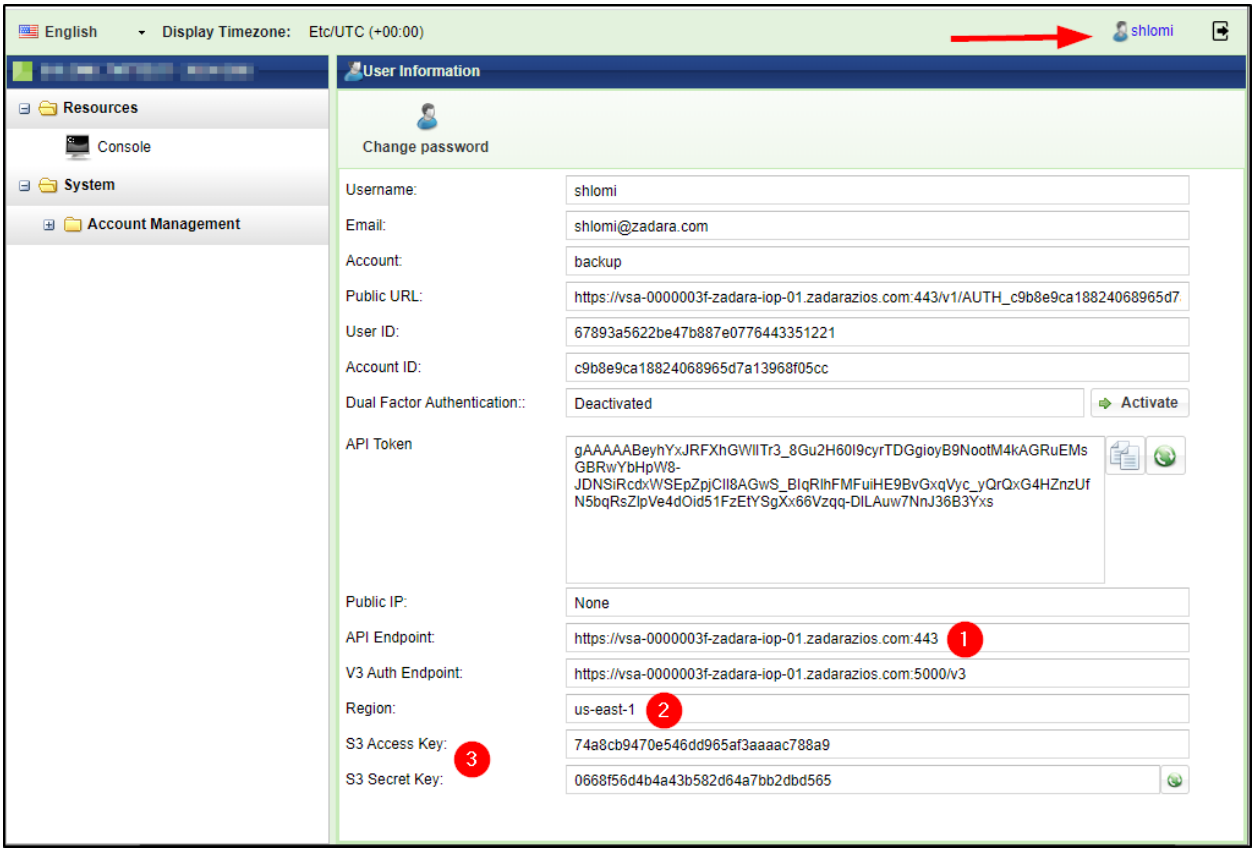
- Versioning.
- Object Retention Support.

10.2.2 Authentication information

For Object Storage connectivity, it is required to gather the following information from the VPSA Object Storage management UI:

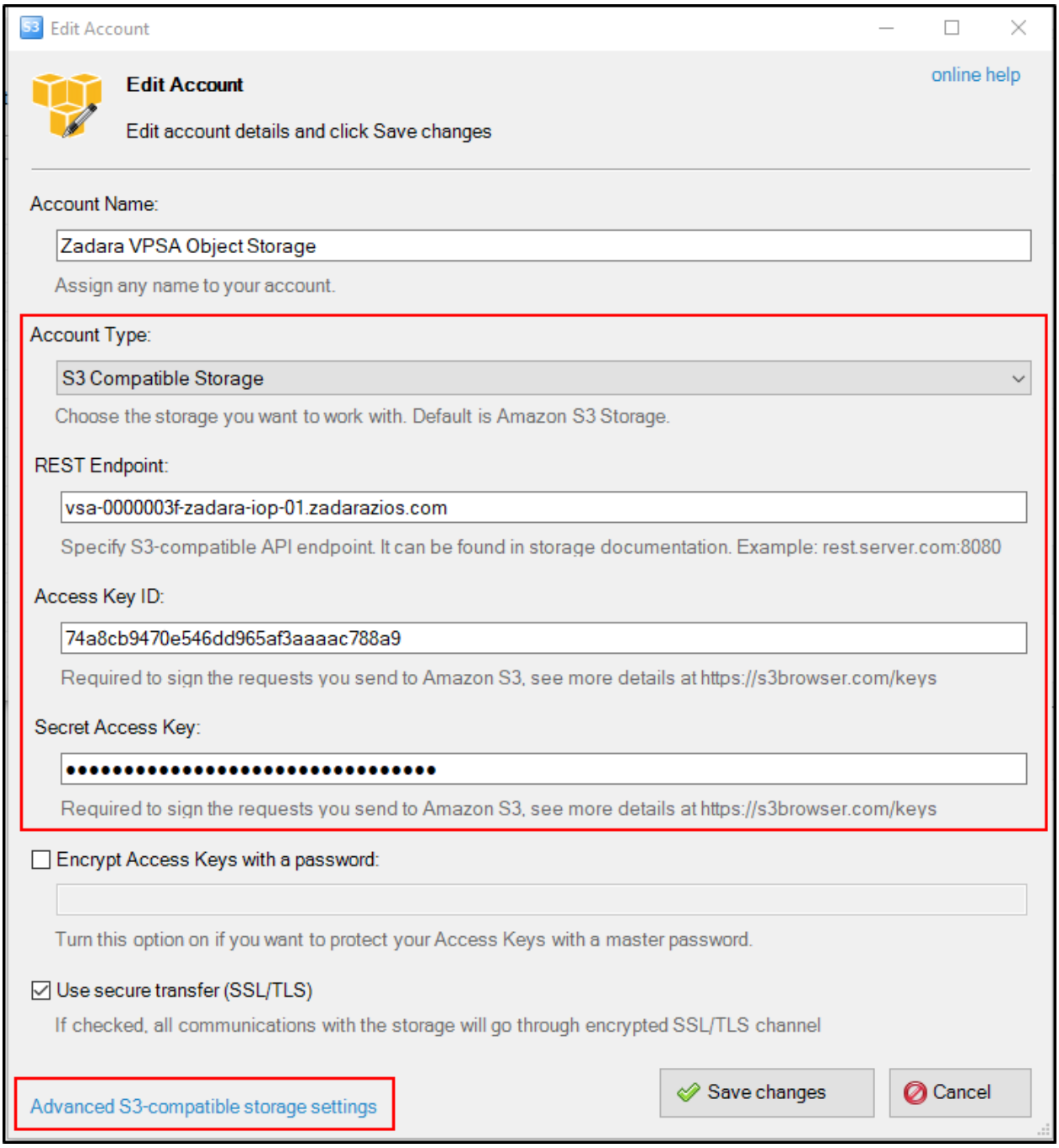
1. VPSA Object Storage Endpoint
2. VPSA Object Storage region.
3. S3 API Access Key/Secret Key

In the VPSA Object Storage GUI, navigate to the User Information section (top right corner, by clicking the logged in username).



10.2.3 S3 Browser

S3 Browser can be used to administrate and perform object operations against Zadara's VPSA Object Storage. The account information in S3 Browser should be configured according to the following example (S3 Compatible Storage):



Once the Endpoint and authentication details are configured properly, click on the Advanced S3-compatible storage settings

In the advanced settings select the following:

1. Signature version - Signature V4
2. Addressing model - Path style

3. Override storage regions - specify the VPSA Object Storage region name; the format is `Region Name=<region name>`.

Close and save the account information.

Note: S3 Browser client is hard-coded to use `us-east-1` as the default region, In order to use Object Storage v4 signatures, ensure the same region value is configured in your VPSA Object Storage or override the default S3Browser region name in the Advanced Settings options.

10.2.4 S3cmd

The credentials can be retrieved from the VPSA Object Storage logged in "User Information" properties.

/etc/.s3cfg

```
[default]
access_key = <S3 Access Key>
secret_key = <S3 Secret Key>
host_base = vsa-00000001-cloud-01.zadarazios.com
host_bucket = vsa-00000001-cloud-01.zadarazios.com
use_https = True
```

Note:

- `access_key` is the user S3 Access Key
- `secret_key` is the user S3 Secret Key
- `host_base` is the HTTPS path to the VPSA Object Storage being accessed

10.2.5 AWS Command Line Interface

Update the default/create new profile for the VPSA Object Storage within aws configuration file.

~/.aws/config

```
[profile zadara]
s3 =
    signature_version = s3v4
```

Note: It is possible to use both AWS v4/v2 signatures with S3-compatible storage such as Zadara VPSA Object Storage.

~/.aws/credentials

```
[zadara]
aws_access_key_id = <S3 Access Key>
aws_secret_access_key = <S3 Secret Key>
```

The credentials can be retrieved from the VPSA Object Storage logged in "User Information" properties.

Example of usage:

```
$ aws s3 --profile=zadara --endpoint-url=https://vsa-00000001-cloud-01.zadarazios.com --region=US ls s3://
↪zadara-test

2018-04-01 19:00 mytestfile1
2018-04-01 19:10 mytestfile2
2018-04-01 19:20 mytestfile3
```

Note:

- `profile` is the name of the credentials and config profile specified above (in this case, "zadara")
- `endpoint-url` is the HTTPS path to the VPSA Object Storage being accessed
- `region` should match the Region defined in the VPSA Object Storage settings page

10.2.6 boto3 python library

Update the default/create new profile for the VPSA Object Storage within aws configuration file.

~/.aws/config

```
[profile zadara]
s3 =
    signature_version = s3v4
```

Note: It is possible to use both AWS v4/v2 signatures with S3-compatible storage such as Zadara VPSA Object Storage.

~/.aws/credentials

```
[zadara]
aws_access_key_id = <S3 Access Key>
aws_secret_access_key = <S3 Secret Key>
```

The credentials can be retrieved from the VPSA Object Storage logged in "User Information" properties.

In your python code:

```
#!/usr/bin/env python

import boto3

session = boto3.session.Session(profile_name='zadara')

s3_client = session.client(
    service_name='s3',
    region_name='US',
    endpoint_url='https://vsa-00000001-cloud-01.zadarazios.com',
)

print('Buckets')
print(s3_client.list_buckets())

print('')
```

(continues on next page)

(continued from previous page)

```
print('Objects')
print(s3_client.list_objects(Bucket='test'))
```

Note:

- `profile_name` is the name of the credentials and config profile specified above (in this case, "zadara")
- `endpoint_url` is the HTTPS path to the VPSA Object Storage being accessed
- `region` should match the Region defined in the VPSA Object Storage settings page

10.2.7 AWS S3 Java SDK (aws-java-sdk)

AWS Provides a comprehensive S3 Java SDK that can be used with Zadara's VPSA Object Storage. Getting started guide is available in Zadara's Support Knowledge Base article - How to use AWS S3 Java SDK with VPSA Object Storage.

10.2.8 AWS S3 PHP SDK (aws-sdk-php)

AWS Provides a comprehensive S3 PHP SDK that can be used with Zadara's VPSA Object Storage. Getting started guide is available in Zadara's Support Knowledge Base article - How to use AWS S3 PHP SDK with VPSA Object Storage.

10.2.9 AWS S3 JavaScript SDK (aws-sdk)

AWS Provides a comprehensive S3 JavaScript SDK that can be used with Zadara's VPSA Object Storage. Getting started guide is available in Zadara's Support Knowledge Base article - How to use AWS S3 JavaScript SDK with VPSA Object Storage.

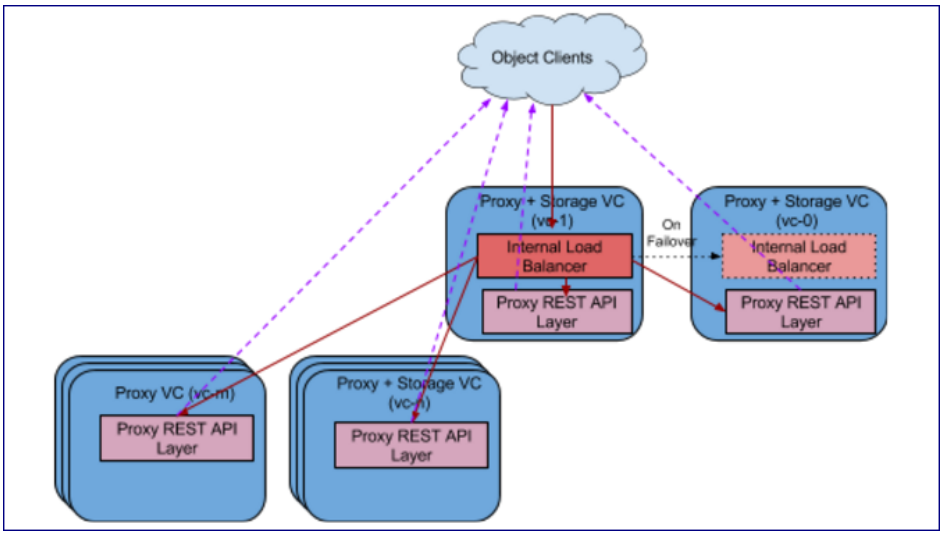
CHAPTER

ELEVEN

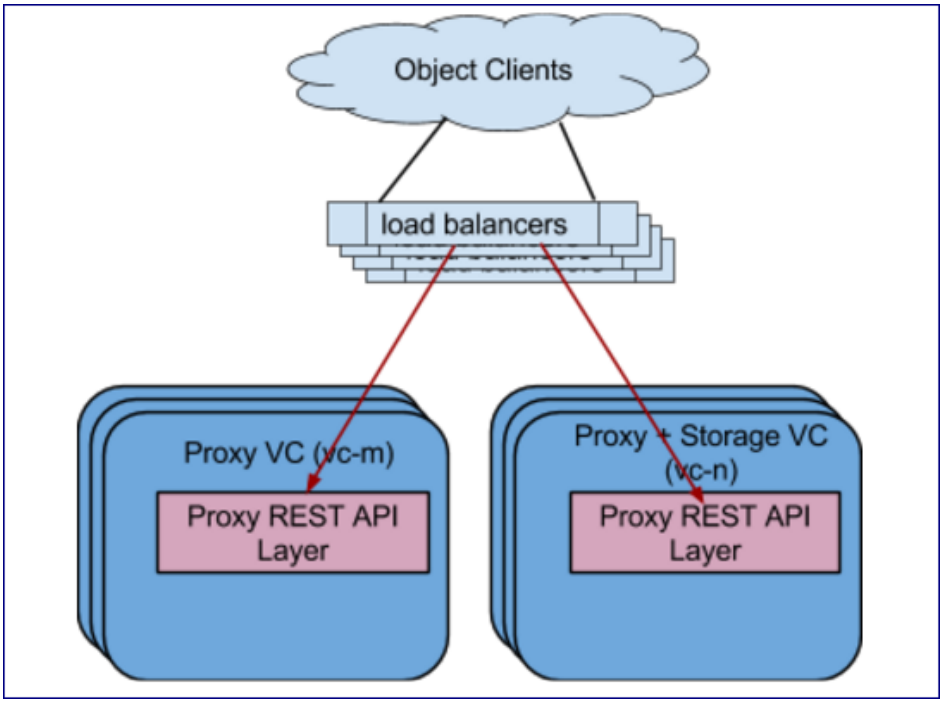
APPENDIX A: SETTING EXTERNAL LOAD-BALANCER

VPSA Object Storage is created by default with internal load balancer to distribute object operations between proxy virtual controllers (VC's). When VPSA Object Storage cluster scales out and connections load is increasing, switching to an external load balancer might be required.

VPSA Object Storage provides a very smooth and easy way to switch between internal and external load balancer setups.



Internal Load Balancer runs in one of the VC's



External Load Balancer(s) runs outside of the VPSA Object Storage VC's

Below are instructions for setting up an external load balancer to terminate SSL connections and distribute the load over all VC's.

There are many load balancer solutions in the market, setting them all up is quite similar procedure. This appendix gives an example of HAproxy, an open-source TCP/HTTP load-balancing proxy server that can be found in www.haproxy.org

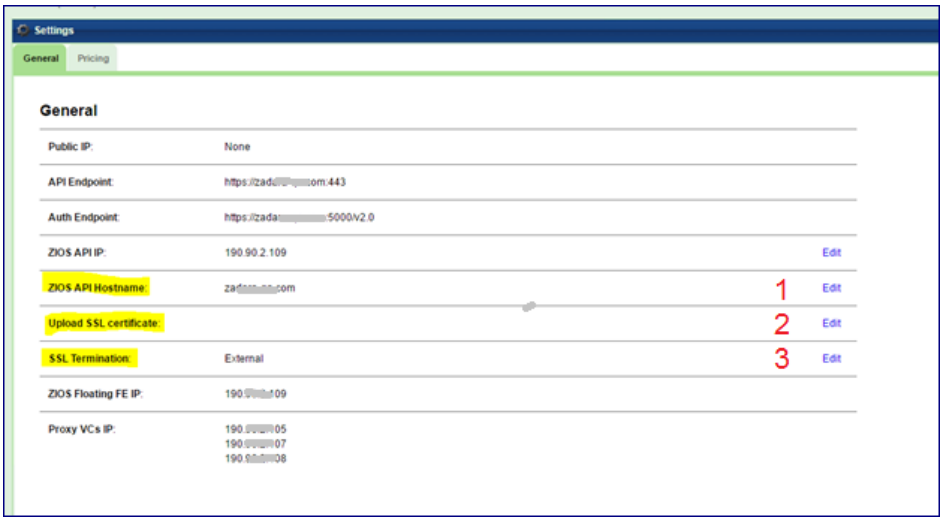
The recommended configuration below will allow the following:

- SSL Termination is done on the external load balancer for both object operation API's and GUI connections. Authentication connections are always terminated in Object Storage.
- Custom SSL certificate (PEM) located on the load balancer is used for SSL connections
- Object operation connections are redirected to VPSA Object Storage proxy VC's
- Object operation connections are distributed between VC's unevenly (proxy-only VCs to take more load than storage VC's, and HA VCs to take the lowest load)
- Redirected object operation connections will include the original client IP in a special header added by the load balancer (for logging in VPSA Object Storage proxy)
- HTTP-based health check is performed by the load balancer to probe all VPSA Object Storage proxy VC's
- Authentication connections are redirected to ZObject Storage floating IP (SSL pass-through terminated on VPSA Object Storage, Custom SSL certificate must be uploaded to VPSA Object Storage as well).
- GUI connections are redirected to VPSA Object Storage floating IP
- Graphical statistics interface is enabled on the load balancer

Apply the following configuration to your VPSA Object Storage Settings:

1. Set the internet-facing domain-name/IP of the external LoadBalancer as VPSA Object Storage API Hostname / IP (zadara-qa.com which resolves to the external LB IP 180.80.2.217, is set in this example as VPSA Object Storage API Hostname)

2. Upload your custom SSL certificate (will be used for authentication connections). The certificate should match the custom domain name.
3. Set SSL Termination to “External”



HAProxy Installation and configuration instructions:

- Install HAProxy:

```
sudo add-apt-repository -y ppa:vbernat/haproxy-1.5

sudo apt-get update

sudo apt-get install -y haproxy
```

- **Upload your custom SSL certificate to HAProxy server. In this example** the certificate PEM file is placed under /etc/ssl/private/zadara_custom.pem
- Edit /etc/haproxy/haproxy.cfg to include the following:

```
| global
|    maxconn 2048
|    log /dev/log    local0
|    log /dev/log    local1 notice
|    chroot /var/lib/haproxy
|    stats socket /run/haproxy/admin.sock mode 660 level admin
|    stats timeout 30s
|    user haproxy
|    group haproxy
|    daemon
|    tune.ssl.default-dh-param 2048
|    # Default SSL material locations
|    ca-base /etc/ssl/certs
|    crt-base /etc/ssl/private
|    # Default ciphers to use on SSL-enabled listening sockets.
|    # For more information, see ciphers(1SSL). This list is from:
|    #  https://hynek.me/articles/hardening-your-web-servers-ssl-ciphers/ssl-default-bind-ciphers
|    ECDH+AESGCM:DH+AESGCM:ECDH+AES256:DH+AES256:ECDH+AES128:DH+AES:ECDH+3DES:DH+3DES:RSA+AESGCM:RSA+AES:
↪RSA+3DES:!aNULL:!MD5:!DSS
|    ssl-default-bind-options no-sslv3
|
```

(continues on next page)

(continued from previous page)

```
| defaults
|    log     global
|    mode    http
|    option  httplog
|    option  dontlognull
|    timeout connect 5000
|    timeout client  50000
|    timeout server  50000
|    errorfile 400 /etc/haproxy/errors/400.http
|    errorfile 403 /etc/haproxy/errors/403.http
|    errorfile 408 /etc/haproxy/errors/408.http
|    errorfile 500 /etc/haproxy/errors/500.http
|    errorfile 502 /etc/haproxy/errors/502.http
|    errorfile 503 /etc/haproxy/errors/503.http
|    errorfile 504 /etc/haproxy/errors/504.http
|    frontend fe-object-operations
|    bind 180.80.2.217:443 ssl crt /etc/ssl/private/zadara\_custom.pem
|    mode http
|    default\_backend be-zios-object-operations
|
| frontend fe-auth
|    bind 180.80.2.217:5000
|    option tcplog
|    mode tcp
|    default\_backend be-floating-zios-auth
|
| frontend fe-gui
|    bind 180.80.2.217:8443 ssl crt /etc/ssl/private/zadara\_custom.pem
|    mode http
|    default\_backend be-floating-zios-gui
|
| backend be-zios-object-operations
|    mode http
|    balance roundrobin
|    option forwardfor
|    option  httpclose
|    option  httpchk HEAD /healthcheck HTTP/1.0
|    server ziosStorageProxy0 190.90.2.102:8080 weight 10 check
|    server ziosStorageProxy1 190.90.2.104:8080 weight 10 check
|    server ziosStorageProxy2 190.90.2.114:8080 weight 50 check
|    server ziosProxyOnly3 190.90.2.106:8080 weight 100 check
|    server ziosProxyOnly4 190.90.2.109:8080 weight 100 check
|
| backend be-floating-zios-auth
|    mode tcp
|    server ziosFloating 190.90.2.118:5000
|
| backend be-floating-zios-gui
|    mode http
|    server ziosFloating 190.90.2.118:80
|
| listen stats \*:1936
|    stats enable
|    stats uri /
|    stats auth zadara:zadara
```

- Enable HAProxy logging (Optional)

a. Edit rsyslog conf:

```
| sudo vi /etc/rsyslog.conf
| # provides UDP syslog reception
| $ModLoad imudp
| $UDPServerRun 514
| # provides TCP syslog reception
| $ModLoad imtcp
| $InputTCPServerRun 514
```

b. Restart the service:

```
sudo service rsyslog restart
```

- Restart HAProxy service:

```
sudo service haproxy restart
```

- Monitor statistics by browsing to http://**<HAProxy server IP>**:1936/ Credentials: zadara/zadara

CHAPTER

TWELVE

APPENDIX B: LARGE OBJECT SUPPORT

12.1 Overview

VPSA Object Storage has a 5GB limit on the size of a single uploaded object. However, the download size of a single object is virtually unlimited with the concept of segmentation. Segments of the larger object are uploaded and a special manifest file is created that, when downloaded, sends all the segments concatenated as a single object. This also offers much greater upload speed with the possibility of parallel uploads of the segments.

12.2 Dynamic Large Objects

VPSA Object Storage is providing Dynamic Large Object (DLO) support via a dedicated middleware.

It is possible to upload file at any size as long as it is segmented into segments smaller than 5GB.

It's the responsibility of the object operation client tool to break a file into segments, different tools can use different size of segments

12.2.1 S3 Interface

Most S3 clients tools support large objects handling. and operation is transparent to the user.

12.2.2 Swift Interface

Using the Swift Tool included with the python-swiftclient library, you can use the -S option to specify the segment size to use when splitting a large file. For example:

```
swift upload test\_container -S 1073741824 large\_file
```

This would split the large_file into 1G segments and begin uploading those segments in parallel. Once all the segments have been uploaded, swift will then create the manifest file so the segments can be downloaded as one.

So now, the following swift command would download the entire large object:

```
swift download test\_container large\_file
```

swift command uses a strict convention for its segmented object support. In the above example it will upload all the segments into a second container named test_container_segments.

CHAPTER

THIRTEEN

APPENDIX C: OBJECT STORAGE IMMUTABILITY (S3 OBJECT LOCK)

13.1 Overview

Zadara Object Storage Immutability ensures data integrity by stopping stored objects from being deleted or overwritten during a specific retention timeframe. With Object Storage Immutability (Object Lock) enabled on a container, it is impossible to modify or shorten the retention period for an existing object. Immutability ensures object version integrity and availability throughout the defined retention period.

This feature can be leveraged directly from the S3 Compatible backup software (i.e. Veeam v10) to ensure the integrity and availability of the backup as required. A configuration guide for SOBR(Scale-Out Backup Repository) that leverages Veeam's Immutability feature can be found in Zadara's Knowledge-Base portal.

13.2 S3 Object Lock

The VPSA Object Storage is utilizing the S3 Object Lock feature (Compliant Mode) in order to set a retention period to a given object and mark it as an immutable object. Deleting this object will be blocked until the retention period has expired. Object Lock should be enabled during the creation time of a new container directly from the management interface or by using AWS S3 Tools (CLI/SDK). Please note that Object-Lock cannot be enabled for existing containers.

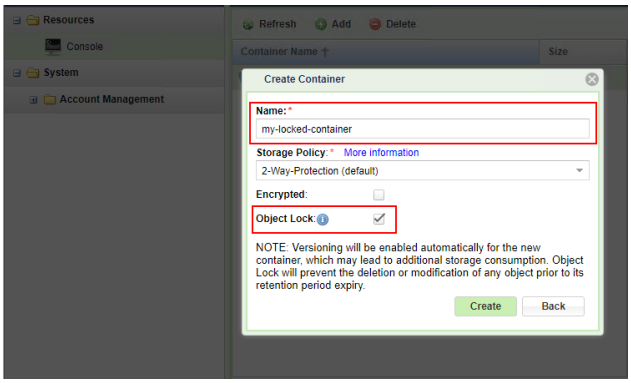
Note:

- All object management related operations for a container with S3 Object Lock enabled will be blocked from the VPSA Object Storage management interface.
- Starting from version 20.01-367, it is possible to set quotas and adjust containers permissions from the VPSA Object Storage management interface.

13.2.1 Enable Object Lock from the Management Interface

Object Lock can be enabled for a new container during its creation. In order to create a new container with Object Lock:

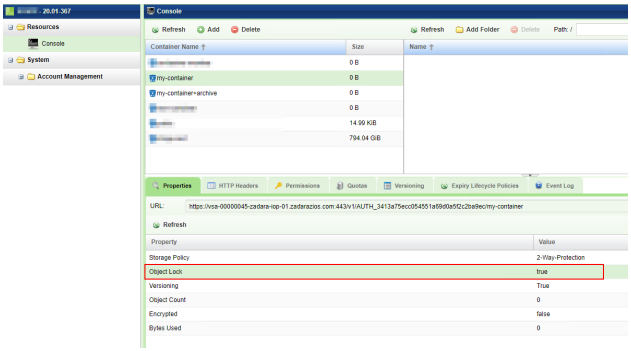
1. Login to the management interface.
2. Navigate to the Object Storage Console section.
3. In the upper options menu, click on the Add button.
4. Provide a new container name.
5. Check the "Object Lock" option.
6. Create the new container by clicking the Create button.



Upon creation the Versioning feature will be enabled automatically for the new container.

Note: Versioning will be enabled automatically for the new container, which may lead to additional storage consumption. Object Lock will prevent the deletion or modification of any object prior to its retention period expiry.

A container with Object Lock enabled can be identified from the container properties. Object Lock property would be set to `true`.



13.2.2 Enable Object Lock using the AWS S3 CLI

In the following examples, we will enable Object Lock using AWS Tools for Power-Shell.

Currently, Object Lock can be enabled and reviewed only from the VPSA Object Storage S3 API interface.

Note: The below examples are utilizing Power-Shell syntax. A matching API calls will achieve the same functionality using the language of your choice.

13.2.3 Enabling Object Lock

Object lock should be enabled on the container level, during creation time, Object versioning will be enabled automatically.

Make sure the Object Storage credentials were set.

Define the VPSA Object Storage as an endpoint:

```
$ENDPOINT="https://vsa-0000000b-zadara-qa13.zadarazios.com"
```

Container Creation

```
$BUCKET="immutable-container"
aws s3api --endpoint-url=$ENDPOINT create-bucket --bucket $BUCKET --object-lock-enabled-for-bucket
```

The expect result should be:

```
{
    "Location": "/immutable-container"
}
```

Confirm Object Lock was enabled for the newly created container

```
aws s3api --endpoint-url=$ENDPOINT get-object-lock-configuration --bucket $BUCKET
```

The expected result should be:

```
{
    "ObjectLockConfiguration": {
        "ObjectLockEnabled": "Enabled"
    }
}
```

Upload an new object

```
$OBJECT="new-object-with-lock.log"
aws s3api --endpoint-url=$ENDPOINT put-object --bucket $BUCKET --key $OBJECT --body $OBJECT

#Response

{
   "ETag": "\"c6125a47483a2823d993da3d31ba6a50\"",
   "VersionId": "MzMxNjlmNzItOWQ3Ni00MWI0LTllOGYtZDQyN2RkMjRlN2Jk"
}
```

Set Object retention

```
aws s3api --endpoint-url=$ENDPOINT put-object-retention --bucket $BUCKET --key $OBJECT --retention
↪Mode=COMPLIANCE,RetainUntilDate=2020-04-01
```

Retrieve object lock configuration:

```
aws s3api --endpoint-url=$ENDPOINT get-object-retention --bucket $BUCKET --key $OBJECT
{
   "Retention": {
      "Mode": "COMPLIANCE",
      "RetainUntilDate": "2020-04-01T00:00:00"
   }
}
```

In this example, the object will remain locked until April 1st, 2020.

List the object versions and attempt to delete a specific version

```
aws s3api --endpoint-url=$ENDPOINT list-object-versions --bucket $BUCKET  --prefix $OBJECT
{
   "Versions": [
      {
            "ETag": "%22c6125a47483a2823d993da3d31ba6a50%22",
            "Size": 14871255,
            "StorageClass": "STANDARD",
            "Key": "new-object-with-lock.log",
            "VersionId": "MzMxNjlmNzItOWQ3Ni00MWI0LTllOGYtZDQyN2RkMjRlN2Jk",
            "IsLatest": true,
            "LastModified": "2020-03-08T16:54:30.225Z",
            "Owner": {
               "DisplayName": "veeam:client",
               "ID": "veeam:client"
            }
      }
   ]
}
```

Select the object version and attempt to delete the object

```
aws s3api --endpoint-url=$ENDPOINT delete-object --bucket=$BUCKET --key=$OBJECT --version-id=$VERSION

An error occurred (AccessDenied) when calling the DeleteObject operation: Access Denied.
```