zadara

Command Center Administrator Guide

Release 23.09-SP3

Zadara

Apr 15, 2025

GETTING STARTED

Dashboard Command Center Dashboard

- VPSAs Manage your VPSAs
- Object Storages Manage your Object Storage VPSAs
- Access Control Manage your Users and Roles

CHAPTER

ONE

INTRODUCTION

1.1 Audience

This document is intended for Zadara Private Cloud administrators and assumes access permissions for the Cloud management applications.

1.2 Zadara Storage Command Center

1.2.1 Overview

Zadara Storage Cloud was architectured from the ground up to build the first “Enterprise-Storage-as-a-Service Data Storage System for the Cloud” with the following key targets:

- Enterprise quality, resilient, highly available, consistent performance storage for the most demanding data center application workloads
- Consumed as a Service - flexible, dynamic and billable
- Scale out - grow to hundreds of Storage Nodes, thousands of drives and multi-Petabyte Storage
- True Multi-tenancy - End-user controlled privacy and security. Separate workloads, resource allocation, and management per tenant, such that each tenant truly experiences “no noisy neighbors” secure storage.
- Universal Storage - Supports all data services on one common infrastructure: Block, File, Object

Zadara Command Center is a centralized point of management and monitoring for the Zadara Storage Cloud. Command Center enables Administrators to:

- Extract detailed information regarding cloud elements such as : VPSA instances , Storage Nodes , disk drives and software images
- Define global cloud level polices that impact all underlying tenants
- Monitor cloud resources utilization and health from a single pane of glass
- Maintain cloud infrastructure and control software images available for tenants
- Perform management and maintenance operations on Virtual Private Storage Array instances defined on the cloud
- Manage cloud expansions - adding storage nodes and disk drives
- Manage cloud roles and users
- Manage cloud level license-keys
- View a detailed central log of all cloud elements

1.2.2 Terminology

Item	Description
SN	Storage Node. Commodity server with a large number of CPU cores (typically 16 or more) and large RAM (typically 64GB or more), connected to a 40GbE/100GbE data network with Intel/NVIDIA SRIOV NICs and 1Gb management network
VPSA	Virtual Private Storage Array. A redundant and Highly Available Software Defined Storage (SDS) that has all resources (CPU, memory, network, disks) provisioned entirely for itself, thereby providing consistent QoS storage
Object Storage	Redundant, Durable, Private and Highly Available virtual object store cluster that has provisioned resources (CPU, memory, network, disks)
VC	Virtual Controller. A Virtual Machine running Zadara Storage IO stack. Two VC's are paired together in High-Availability configuration to form a VPSA.
Provisioning Portal (eCommerce)	The web application portal for the end-users to create VPSA's/ Object Storage and provisioning their resources (Drives, IO Engines, Flash Cache etc). Pricing and Billing are also managed via the Provisioning Portal.
Cloud Controller (CC)	Set of software components that manages the storage cloud (like allocating resources for VPSA/Object Storage with intelligent scheduler, monitoring, and provisioning networking/storage for VPSA/Object Storage etc.)
Command Center	The Web Application for the Cloud Administrator to monitor and maintain the Zadara Cloud (inventory management, maintenance operations etc.)
CCVM	A system Virtual Machine within the Zadara Cloud which runs the Command Center and the Provisioning Portal
FE Network/Data Network	Front-End network. 40GbE/100GbE network through which Application Servers can connect to Zadara VPSA Storage for IO and Control
BE Network	Back-End network. 40GbE/100GbE network through which SNs and VPSA interconnect for data IOs
Management Network	Internal 1Gb network for management operations of VPSA, VPSA Object Storage & SN
SRIOV	Single Root IO Virtualization. A networking standard by which a physical adapter is logically provisioned for different VMs, bypassing the Hypervisor
Application Server	A server or a Virtual Machine in the Compute Cloud which consumes VPSA iSCSI Block Volume or NAS shares
Tenant	Each end-user that accesses Zadara Storage Cloud. **Note**: Each end-user can have multiple users or logins belonging to the same tenant
QoS	Quality of Service. Performance and reliability characteristics of a service

CHAPTER

TWO

ARCHITECTURE

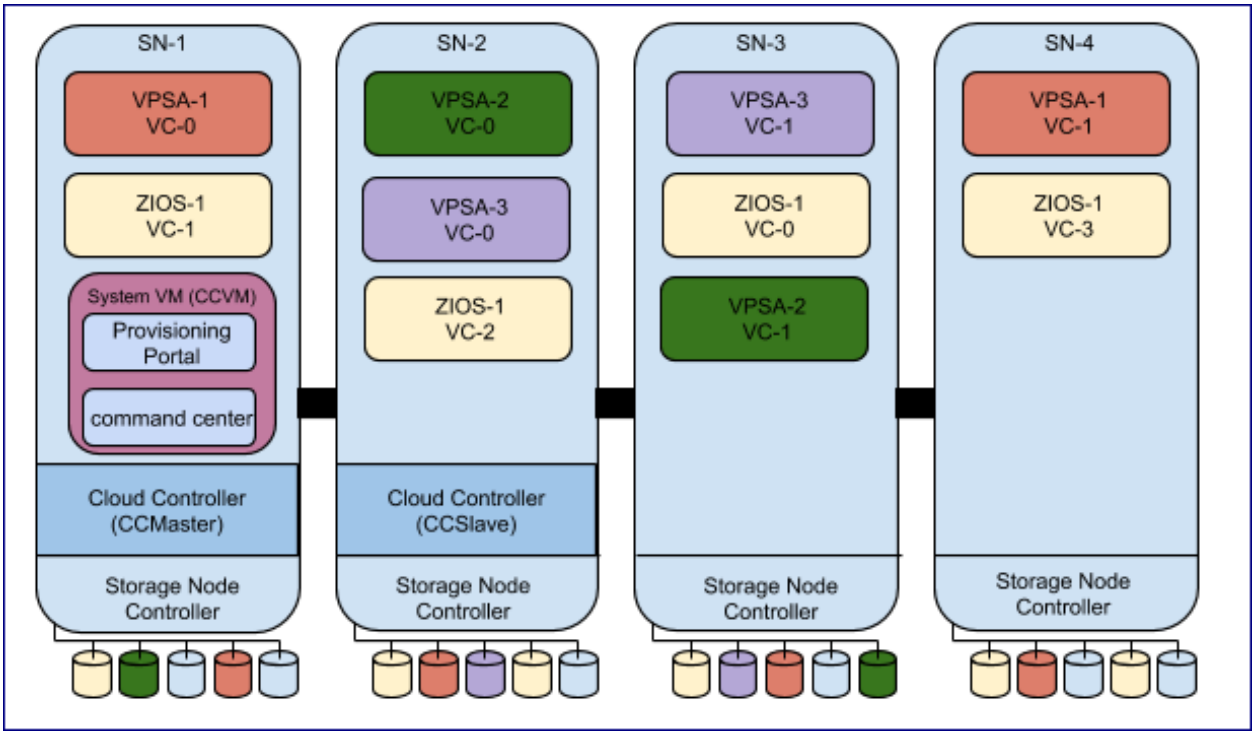
The Zadara cloud contains two storage nodes which are assigned the roles of Cloud Controller Master (CCMaster) and Cloud Controller Slave (CCSlave). The CCMaster and CCSlave Storage Nodes (SN) are responsible for Cloud management and monitoring in addition to virtual storage controller hosting, like any other Cloud storage node. The CCMaster storage node actively hosts all cloud management function including a dedicated Cloud Controller Virtual Machine (CCVM). In case of any failure in the Cloud Controller Master, a failover of all cloud management resources to the Cloud Controller Slave is performed.

Zadara cloud can be centrally managed by 2 software components:

- Provisioning portal
- Command center

By default, both Provisioning portal and Command Center reside within the Cloud Controller Virtual Machine.

Zadara's Provisioning portal can also be deployed in a centralized location, detached from a single Cloud CCVM. This topology should be deployed when there is a need to manage multiple clouds in multiple regions in a single portal.



Important: Zadara's web applications allow only TLS 1.2 and higher, which is the recommended TLS level by industry

standards. The TLS (Transport Layer Security) protocol secures transmission of data over the internet using standard encryption technology.

CHAPTER

THREE

COMMAND CENTER DASHBOARD

3.1 Accessing Command Center

To access Command Center, open you web browser and navigate to http://<Zadara cloud management URL>:8888

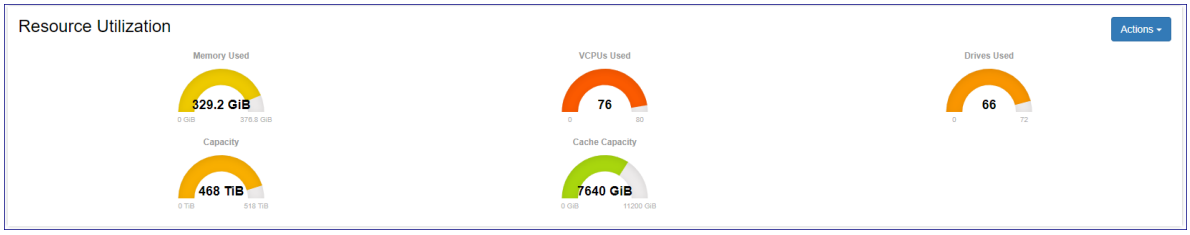
For the first login, the cloud administrator user credentials will be provided by Zadara Operations team after cloud installation. Additional user-IDs can be created by the cloud administrator, and will receive temporary credentials for initial login via their provided e-mail address.

3.2 Command Center Dashboard Overview

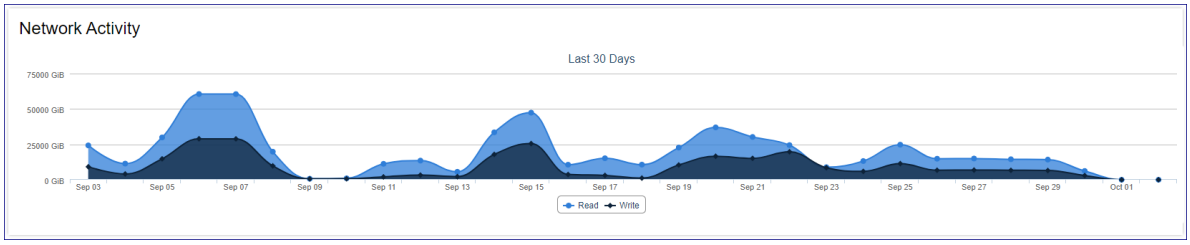
Command Center's main dashboard was designed to provide Zadara cloud administrators with a centralized viewpoint on their cloud utilization, and to perform cloud level operations.

The dashboard has four main panels, each monitoring a different key aspect of the cloud infrastructure:

- The **Resource Utilization** panel provides a birds-eye view on the core cloud resources utilization, such as VCPUs, memory, disks etc.

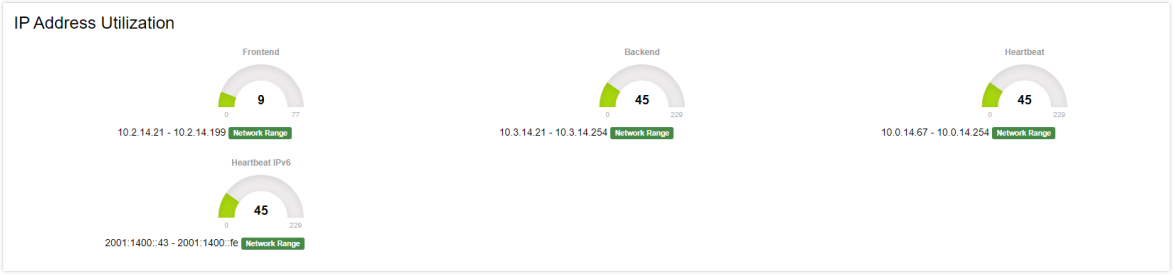


- The **Network Activity** panel provides monitoring data for real-time network throughput and utilization.



- The **Drive Utilization** panel provides a breakdown of drives by their model and utilization per drive.

- The **IP Address Utilization** panel displays the defined IP ranges for frontend, backend and heartbeat networks, the allocation and the level of utilization for each range.



✔ **Note:** These networks are predefined with fixed ranges of IP addresses and cannot overlap with the VPSA and Object Storage Virtual Networks.

- The **Default Cloud Certificates** panel lists the certificates per domain, the certificate's start and expiration dates, and certificate issuer.

3.3 Performing Cloud Level Operations

3.3.1 Creating a CCVM Zsnap

A CCVM Zsnap is a collection of logs and system meta-data information used for troubleshooting and analysis of the component's health.

To manually create a Zsnap of the Cloud Controller Virtual Machine:

1. Navigate to Command Center's dashboard.
2. On the **Resource Utilization** panel, click **Actions**.
3. From the dropdown menu, select **Create CCVM Zsnap**.
4. In the popup dialog, provide a prefix for the Zsnap and click **Create Zsnap** to confirm creation of the Zsnap.

✔ **Note:** Zadara manages collection of Zsnaps and recovery from Zsnaps when relevant.

There is no need for customers to take Zsnaps, but can do so if requested by Zadara Support.

Customers cannot perform any restore operations.

3.3.2 Performing cloud version upgrades

Command Center allows cloud administrators to orchestrate a complete cloud upgrade workflow, including :

- Storage Nodes software
- Storage Node utilities
- VPSA instances running on the cloud
- VPSA Object Storage instances running on the cloud
- Cloud Controller Virtual Machine (CCVM)

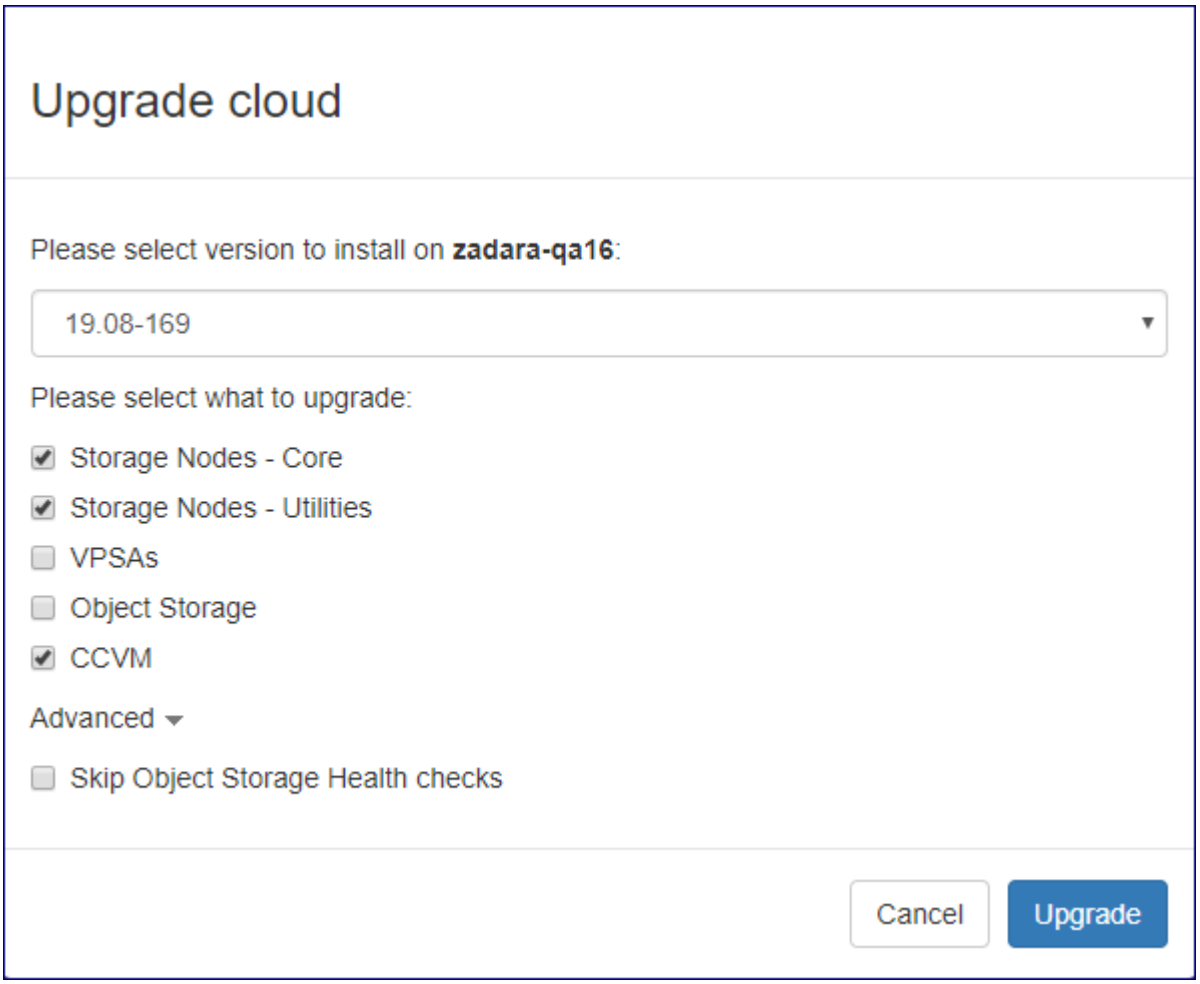
All the elements listed above, or any subset, can be upgraded in a single workflow.

To perform a cloud version upgrade, navigate to Command Center's dashboard, click on the **Actions** button and select **Upgrade** from the dropdown menu.

In the **Upgrade cloud** dialog:

1. From the dropdown listing available versions, select the **Version** to install.
2. Mark the checkboxes of the elements you would like to upgrade.

   When upgrading VPSA Object Storage, you can configure that the upgrade process will not perform Object Storage Health Checks, by clicking on **Advanced** and checking **Skip Object Storage Health checks**.

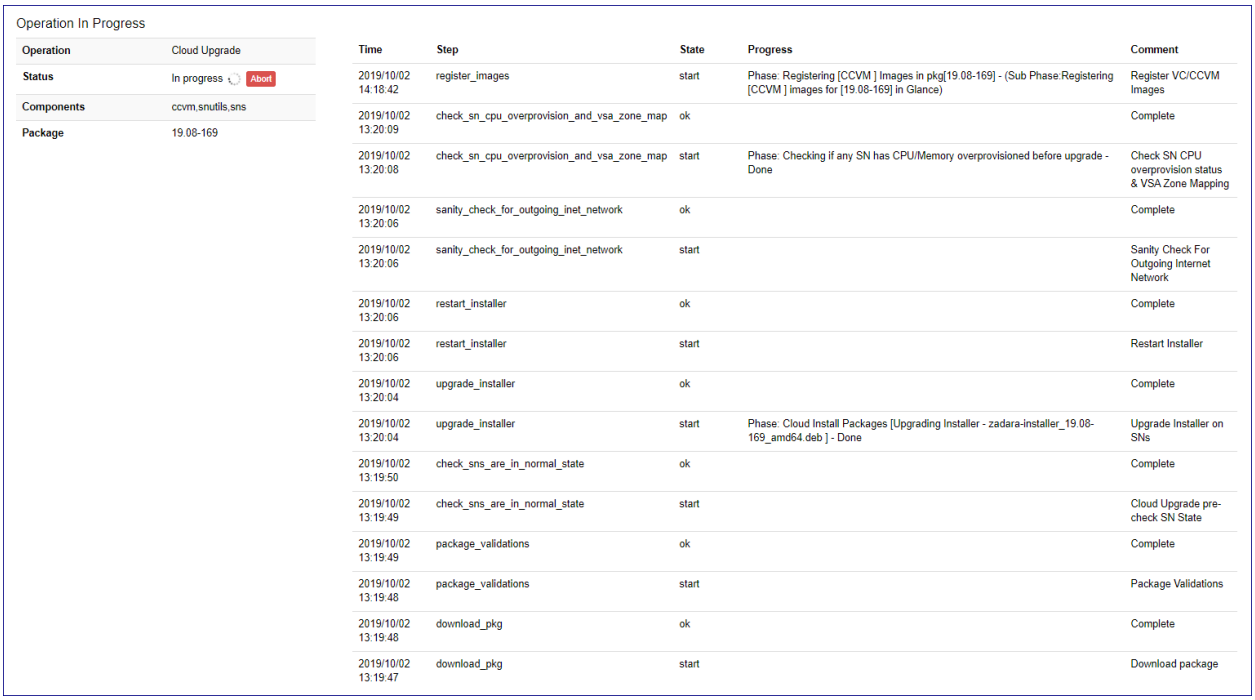


✔ **Note:** The recommended procedure for the cloud upgrade is:

1. Perform SN (software + Utilities) and CCVM upgrade in a single workflow.
2. After successful completion of the first upgrade workflow, perform the VPSA or Object Storage instances upgrade.

Click the **Upgrade** button to confirm the upgrade process.

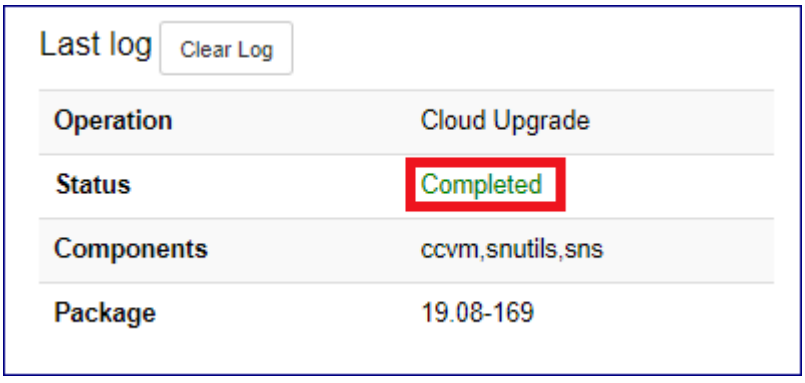
During the cloud upgrade process, the Command Center Dashboard displays the upgrade workflow and status for all stages.



✔ **Note:** During the SN software upgrade, CCMaster failover is performed. This is applicable only for node that is the active CCMaster.

During CCMaster failover and CCVM version upgrade, the Command Center web application is temporarily unavailable. This does not impact the VPSA and Object Storage services.

When the upgrade workflow is finished, the Command Center dashboard displays the **Completed** status, the upgraded components and the package version.



3.3.3 Shutdown

> **Caution:** When shutting down a cloud, all of its storage services are stopped and all Storage Nodes will be powered off.
>
> VPSAs and all other cloud management operations are disabled.

To shut down the cloud:

1. Navigate to Command Center's dashboard.
2. On the **Resource Utilization** panel, click **Actions**.
3. From the dropdown menu, select **Shutdown**.
4. In the popup dialog, enter your password and click **Shutdown** to confirm shutting down the cloud, and stopping all of its storage services.

3.3.4 Restarting a cloud after Shutdown

To restart a cloud after Shutdown:

1. Turn on the servers. This can take a number of minutes.
2. Follow the servers' progress in Storage Node section of Command Center.

3.3.5 Install and Configure Cube

Note: This functionality is deprecated and should not be used. It will be reoved from Command Center in future.

CHAPTER

FOUR

USING COMMENTS IN COMMAND CENTER

4.1 Understanding Command Center Comments

Command Center allows cloud administrators to attach comments to most of the cloud managed entities. Comments can be used to document any issue or business process conducted in the cloud, for example, communicate resource (storage nodes or parts of it, disk drives etc.) dedication to a specific project/tenant.

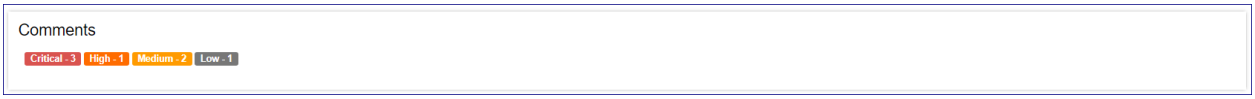
Command Center comments can be assigned to the following Zadara cloud entities:

- Storage nodes
- VPSA and Object Storage
- Cloud users
- Disk drive series/Individual disk drives

Comments are assigned a severity level. Supported severity levels:

- Low
- Medium
- High
- Critical

An indication of all cloud comments according to their severity is displayed on Command Center's main dashboard.



All comments created in Command Center can be displayed by clicking on the comment section on Command Center's main dashboard.

Note:

Command Center comments support standard GitHub Markdown.

Comments for zadara-iop-01

Type	Name	Content	severity	created_by	created_at	
Vpsa	PRIMARY	this comment has a `code block` in it.	Critical	pdm@zadarastorage.com	2019-10-10 11:59:31 UTC	
Node	zdr-iop-sn-01	this comments contains several items: • this is the first item • this is the second item	Critical	pdm@zadarastorage.com	2019-10-10 11:56:47 UTC	
Vpsa	PRIMARY	test markdown **comment** with **highlight**	Critical	pdm@zadarastorage.com	2019-10-10 10:57:32 UTC	
Zios	ZOBS	test comment with `markdown`	High	pdm@zadarastorage.com	2019-10-10 10:37:01 UTC	
Drive Type	SSD CACHE DRIVES	this comment has a logo embedded in it 	Medium	pdm@zadarastorage.com	2019-10-10 11:38:13 UTC	
Drive Type	SAS 5588GB 7200RPM	markdown H2 title this is an embedded hyper link to Serial Attached SCSI wikipedia definition	Medium	pdm@zadarastorage.com	2019-10-10 11:12:27 UTC	
Zios	ZOBS	*this is another test comment with markdown*	Low	pdm@zadarastorage.com	2019-10-10 11:08:46 UTC	

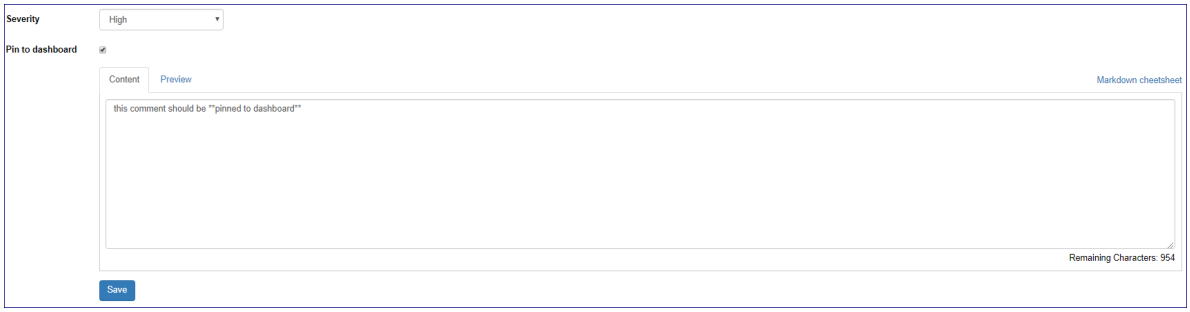
Displaying 7 Comments

4.2 Working With Comments

4.2.1 Adding a New Comment

To add a new comment to a supported command center entity:

1. Navigate to the element's dashboard.
2. On the **Comments** tab, click **New Comment**.
3. In the **New Comment** screen:



1. From the dropdown, assign a **Severity** level to your comment.
2. If you want this comment's text to be displayed on the element's dashboard, mark the **Pin to dashboard** checkbox.
3. Enter the comment's **Content**.

✔ **Note:** You can use GitHub Markdown to add formatting elements to the comment's content.

- Click **Markdown cheatsheet** for examples.
- Click **Preview** to view the formatted content.

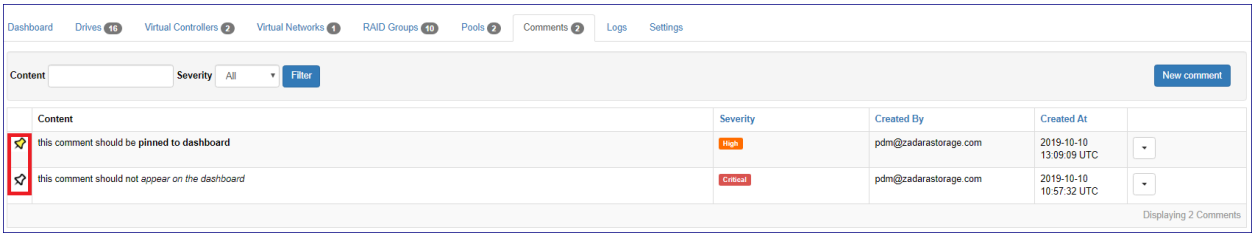
  The content is read-only in the **Preview** tab.

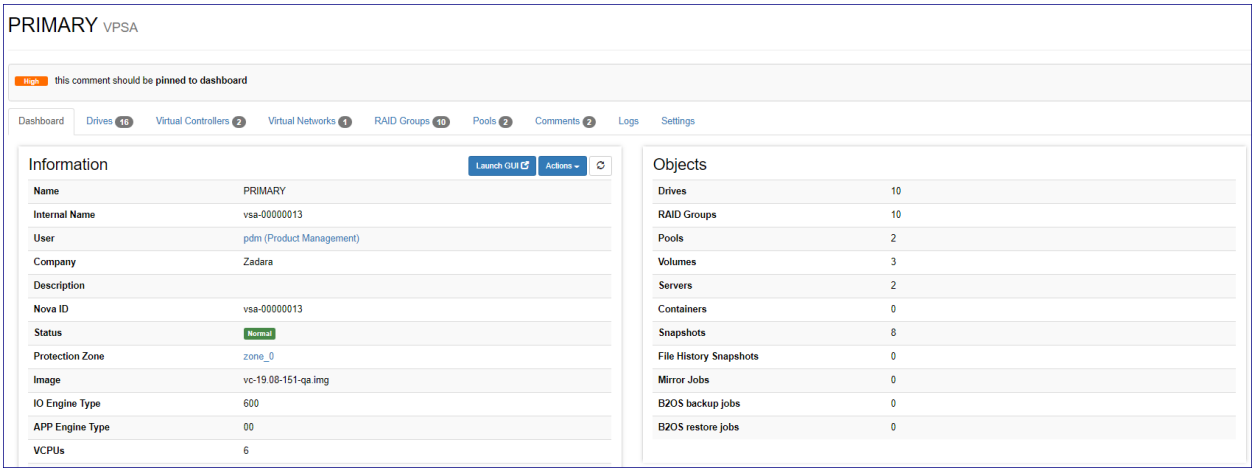
The maximum length of the raw **Content** is 1000 characters including formatting elements.

---

4. Click **Save** to create the new comment.

✔ **Note:** By clicking a comment's pin icon toggle on the element's **Comments** tab, each comment can be pinned to be displayed, or unpinned to be hidden, in the element's dashboard.





4.2.2 Searching and Filtering Comments

To find a specific comment or group of comments for an element that matches specific search criteria:

1. Navigate to the element's dashboard.
2. On the **Comments** tab, in the **Filter** panel above the comments grid, enter a string (case-insensitive) that matches part of the **Contents**, or select the **Severity** level, or a combination of both.
3. Click **Filter** to display matches in the comments grid.

4.2.3 Editing a Comment

To edit an existing comment's content, to pin or unpin it, or to change its severity level:

1. Navigate to the element's dashboard.
2. On the **Comments** tab, locate the comment in the comments grid.
3. From the dropdown to the right of the comment, select **Edit**.
4. In the comment's editing screen, you can:
    1. Assign a different **Severity** level to the comment.
    2. Mark the **Pin to dashboard** checkbox to display this comment's text on the element's dashboard, or leave the checkbox unmarked to hide it.
    3. Update the comment's **Content**.

    ✔ **Note:** You can use GitHub Markdown to add formatting elements to the comment's content.

    - Click **Markdown cheatsheet** for examples.
    - Click **Preview** to view the formatted content.

      The content is read-only in the **Preview** tab.

    The maximum length of the raw **Content** is 1000 characters including formatting elements.

    ---

5. Click **Save** to update the comment.

4.2.4 Deleting a Comment

To delete a comment:

1. Navigate to the element's dashboard.
2. On the **Comments** tab, locate the comment in the comments grid.
3. From the dropdown to the right of the comment, select **Delete**.

> ⚠ **Caution:** On clicking **Delete**, the comment is deleted immediately.
>
> There is no warning or confirmation prompt.

CHAPTER

FIVE

STORAGE NODES

One of Command Center's key roles is to enable cloud infrastructure management, in which Storage Nodes (SN) are a core component. Command Center provides comprehensive management and monitoring capabilities for the cloud's Storage Nodes, including all aspects of:

- Ongoing maintenance
- Upgrade management
- Hardware addition and retirement
- Health checks
- Performance monitoring

5.1 Understanding The Storage Node Dashboard

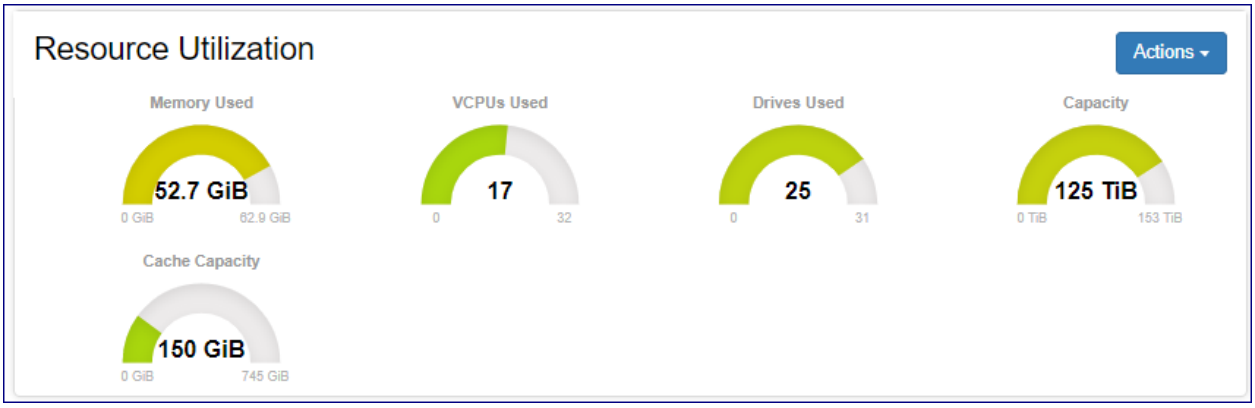
The Storage Node dashboard presents information regarding its configuration, status and resource utilization.

Navigate to the dashboard by clicking **Storage Nodes** in Command Center's left menu panel, and then select a specific Storage Node from the cloud inventory.

The Storage Node dashboard contains multiple panels, each providing information on a specific aspect of the SN configuration and status:

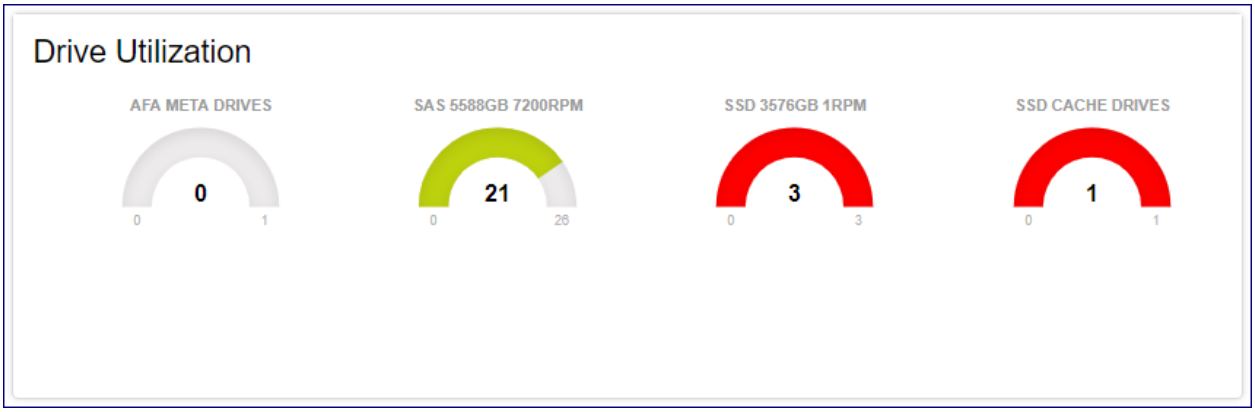
5.1.1 Resource Utilization

Provides a current reflection of SN hardware resources and their level of utilization.



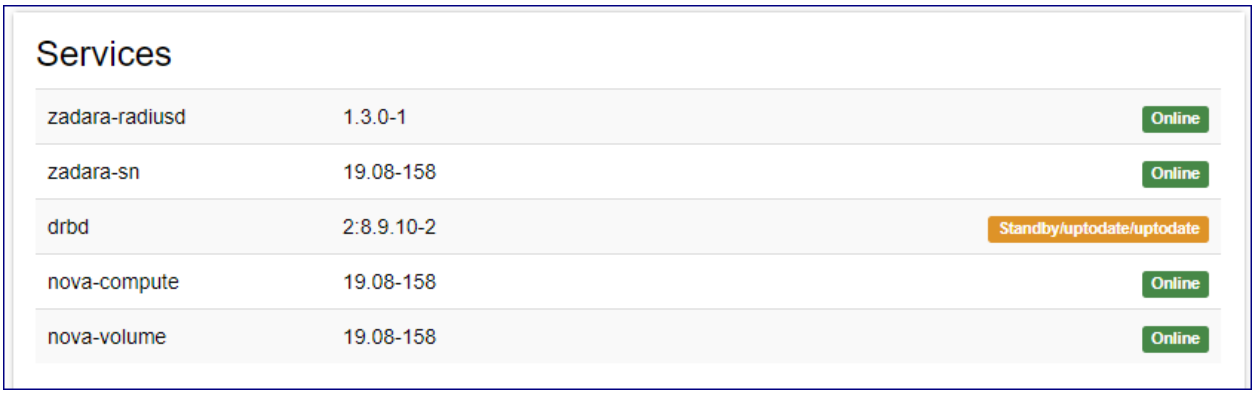
5.1.2 Drive Utilization

Provides a breakdown of the SN drive inventory by type and role, and displays the level of utilization per drive group.

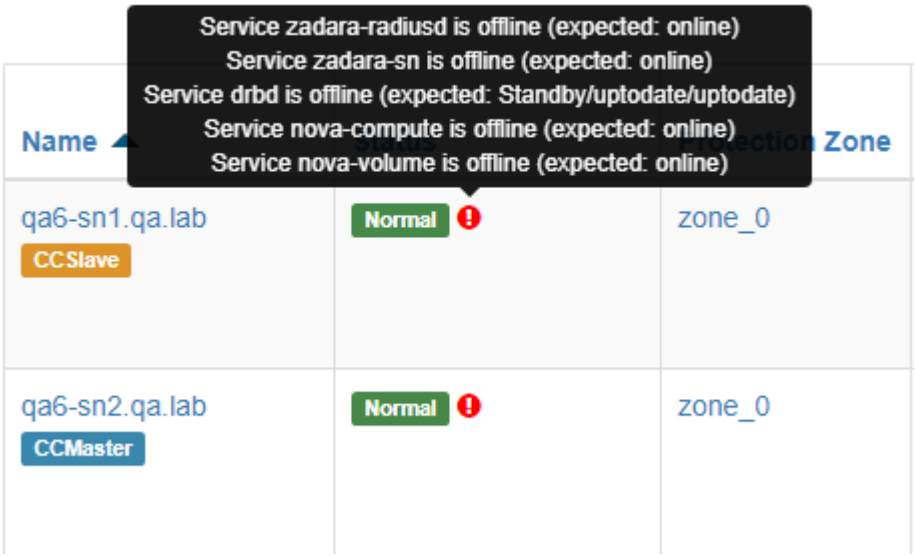


5.1.3 Services

Displays the list of services running on the SN and their current status.

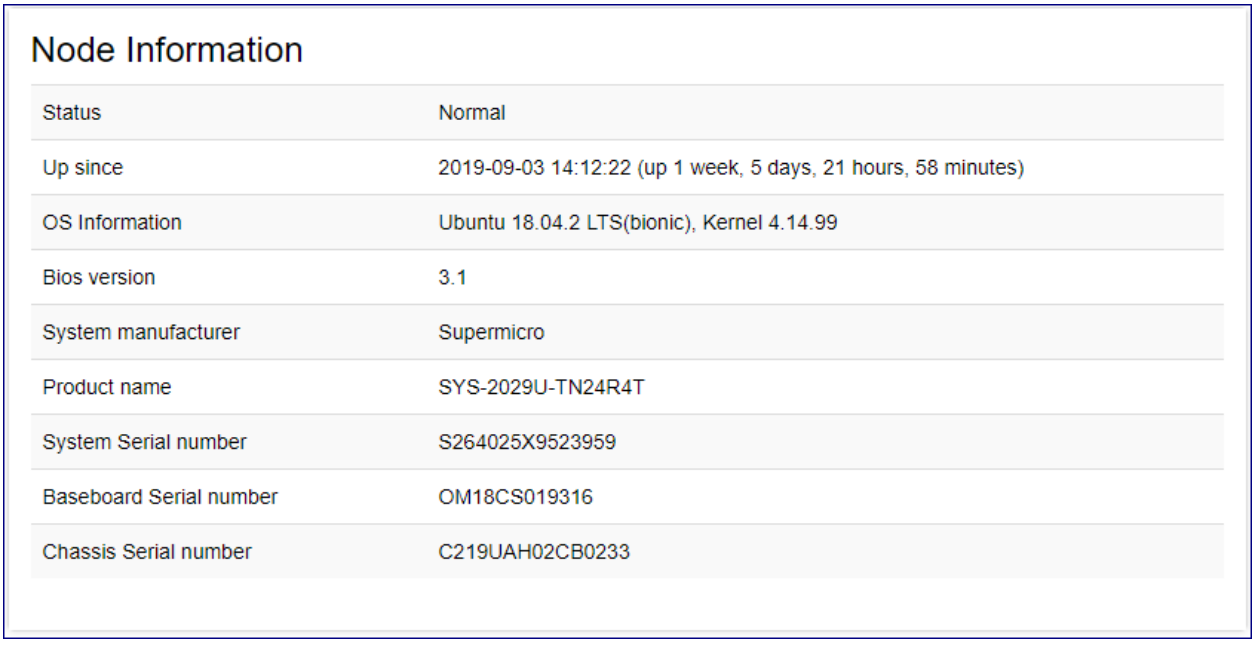


In the event that the Status is not **Normal** for any services on the Storage Node, the affected services are also indicated by a tooltip on the cloud's Storage Nodes grid.



5.1.4 Node Information

Displays SN hardware, configuration and status information such as: SW version, uptime and serial number.

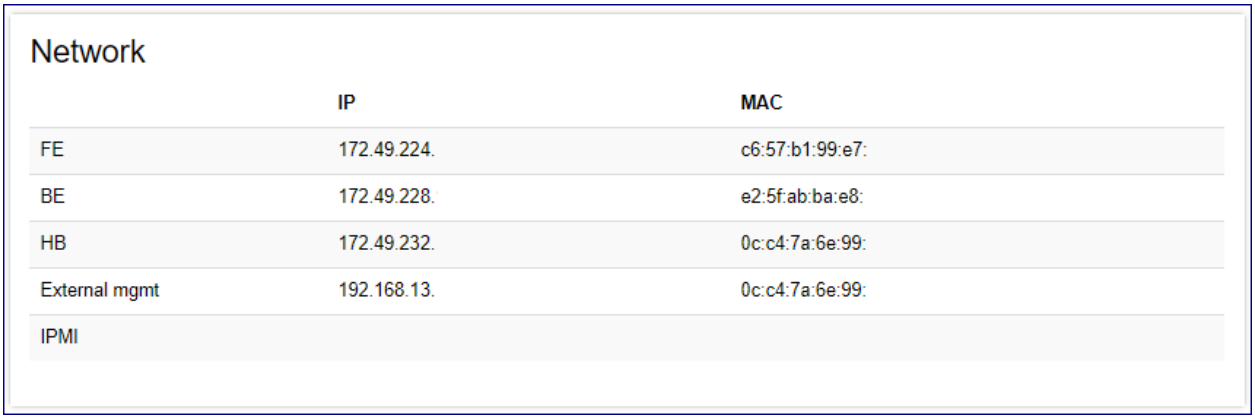


Node Information

Status	Normal
Up since	2019-09-03 14:12:22 (up 1 week, 5 days, 21 hours, 58 minutes)
OS Information	Ubuntu 18.04.2 LTS(bionic), Kernel 4.14.99
Bios version	3.1
System manufacturer	Supermicro
Product name	SYS-2029U-TN24R4T
System Serial number	S264025X9523959
Baseboard Serial number	OM18CS019316
Chassis Serial number	C219UAH02CB0233

5.1.5 Network

Displays SN networks and configured IP addresses.

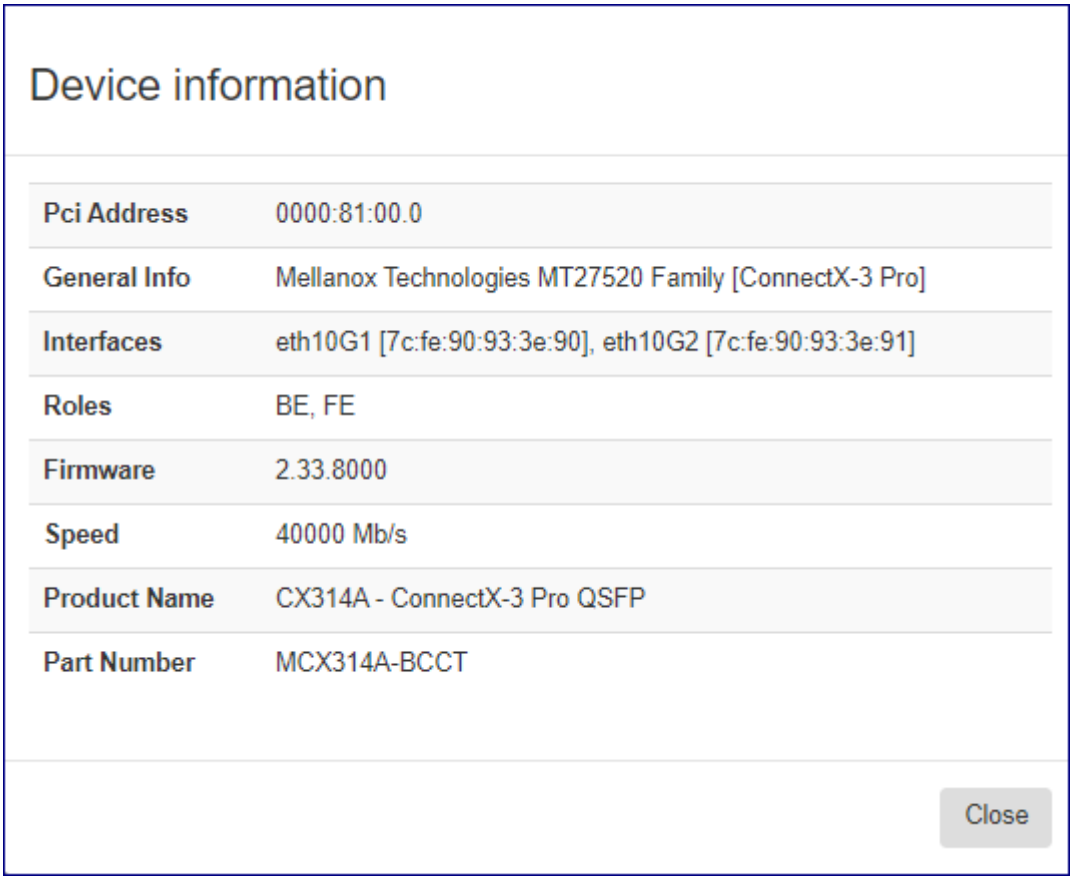


5.1.6 Resource Scheduling

Displays information regarding the availability of the SN's resources such as VCPUs and disk drives, that can be allocated for newly provisioned VPSA/VPSA Object Storage entities by the cloud's orchestration framework.

5.1.7 NIC Information

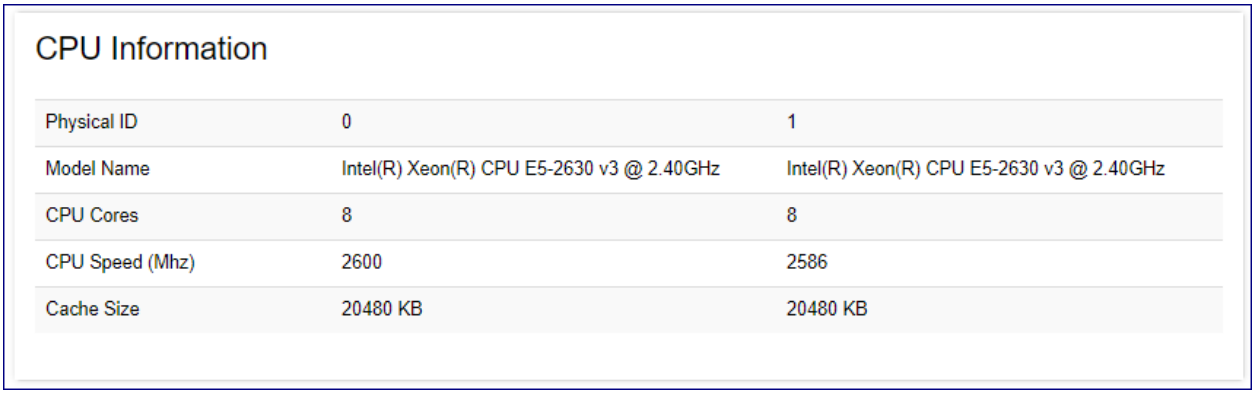
Displays hardware and configuration information on the SN data path network card.



✔ **Note:** Mellanox ConnectX-5 dual port NICs are presented as 2 sperate network adapters, due to having 2 different PCI addresses.

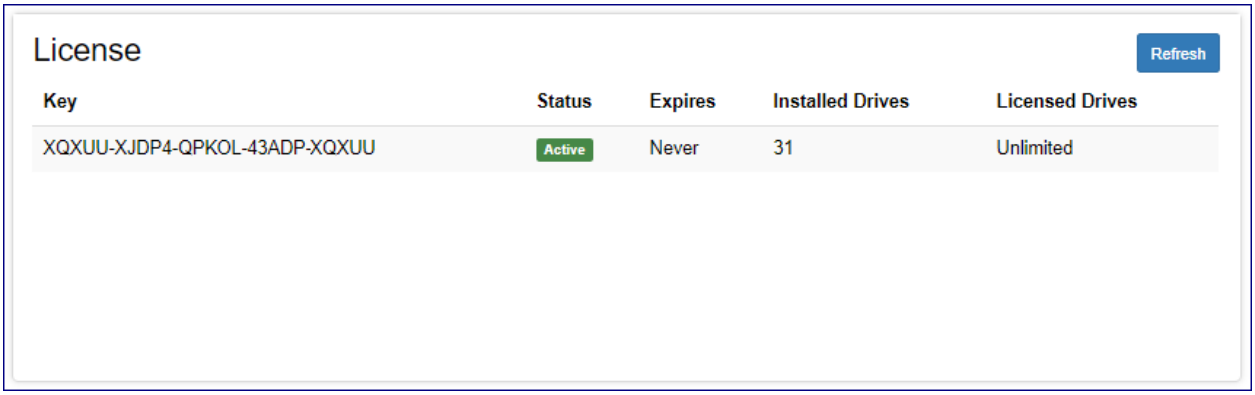
5.1.8 CPU Information

Displays information on the SNs processors.



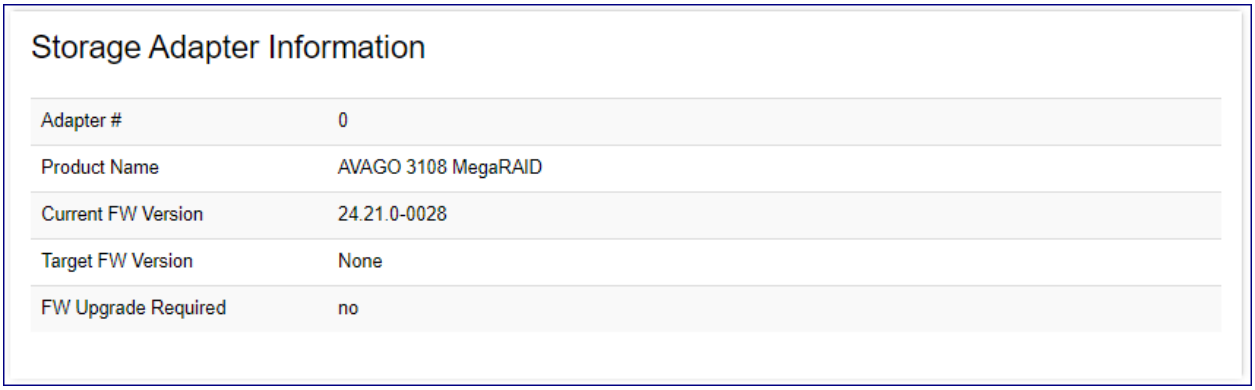
5.1.9 License

Displays SN licensing information.



5.1.10 Storage Adapter Information

Displays information on the SN internal RAID adapter.

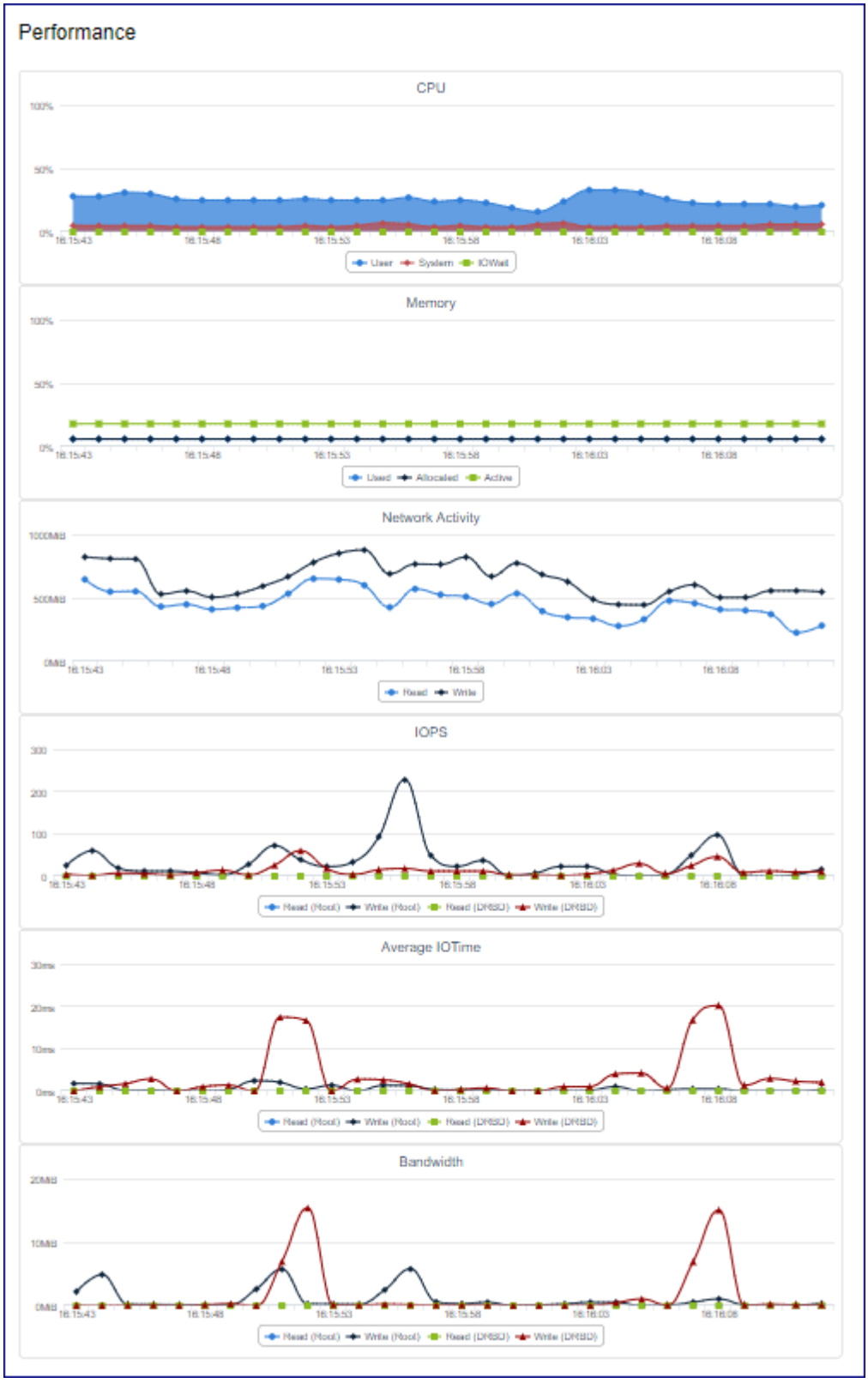


5.2 Monitoring Storage Node Performance

Command Center provides a real-time monitoring framework for Storage Node performance. Monitoring is available in the selected SN's **Performance** tab.

Performance statistics displayed per Storage Nodes include :

- Storage Node CPU utilization
- Storage Node memory consumption
- Network bandwidth distribution (read/write)
- Average IO service time per IO type
- IO throughput distribution



The monitoring interval can be changed. Supported monitoring intervals:

- 1 seconds

- 10 seconds
- 1 minute
- 1 hour
- 1 day

Click the **Auto-Refresh** toggle to activate or disable the automatic display of updated monitoring data on reaching the monitoring interval.

5.3 Performing Storage Node Operations

5.3.1 Changing Storage Node Resource Scheduling Configuration

A Storage Node contains compute and storage resources(CPU, RAM and disks) that are allocated for virtual controllers of VPSA and VPSA Object Storage entities. Allocation of SN resources for the creation of virtual controllers, and allocation of disks from SN to virtual controllers can be enabled or disabled using Command Center.

To modify a Storage Node resource allocation policy go to the **Resources Scheduling** panel in the SN dashboard.

- Click on **Enable** or **Disable** for **Drive Scheduling**, to enable or disable allocation of disks from this SN to virtual controllers.
- Click on **Enable** or **Disable** for **VC Scheduling**, to enable or disable creation of avirtual controller on this SN.

Changes in the SN scheduling policy are immediately applied.

5.3.2 Creating Storage Node Zsnap

To trigger manual creation of a Zsnap for a Storage Node:

1. Navigate to the Storage Node's dashboard.
2. On the **Resource Utilization** panel, click **Actions**.
3. From the dropdown, select **Create Zsnap**.
4. In the popup dialog, provide a prefix for the Zsnap and click **Create Zsnap** to confirm creation of the Zsnap.

✔ **Note:** Zadara manages collection of Zsnaps and recovery from Zsnaps when relevant.

There is no need for customers to take Zsnaps, but can do so if requested by Zadara Support.

5.3.3 Install and import new drives in a Storage Node

Cloud storage capacity expansion is performed by installing drives in the Storage Node, and then importing the newly installed drives into the SN.

The import operation encapsulates hardware discovery and SN/cloud inventory update.

To import newly installed physical drives into a Storage Node:

1. Navigate to the Storage Node's dashboard.
2. On the **Resource Utilization** panel, click **Actions**.
3. From the dropdown, select **Import Drives**.

4. In the popup dialog, click **Confirm** to confirm the import drives operation.

A resource scan will be performed and any newly installed disks will be imported.

The output from the import operation will be presented in a new popup window.

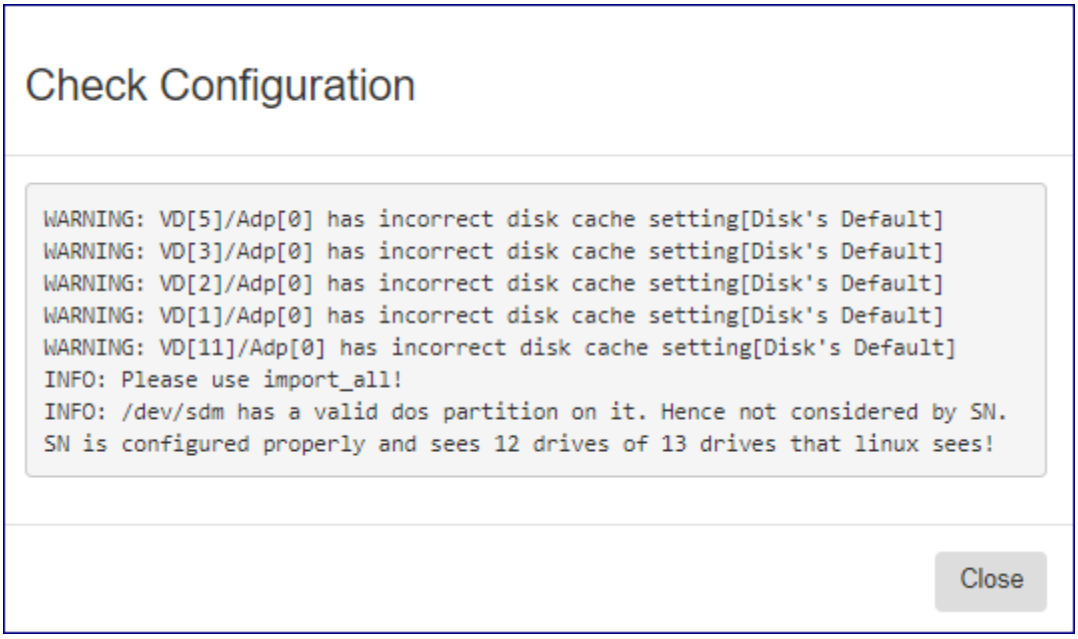
5.3.4 Perform Storage Node drive configuration check

Command Center can trigger a Storage Node drive configuration check, in which the SN drive configuration is validated against the OS drive configuration.

To perform a drive configuration check:

1. Navigate to the Storage Node's dashboard.
2. On the **Resource Utilization** panel, click **Actions**.
3. From the dropdown, select **Check Configuration**.
4. In the popup dialog, click **Confirm** to confirm the drive configuration check operation.

The configuration check will be immediately performed and its output displayed on a new popup dialog.



5.3.5 Upgrading Storage Node Version

A Storage Node Version upgrade can be performed as part of a complete cloud upgrade workflow from Command Center's main dashboard or from the Storage Node dashboard. The upgrade from the SN dashboard is useful when the cloud upgrade process is performed gradually as a multiple milestone process.

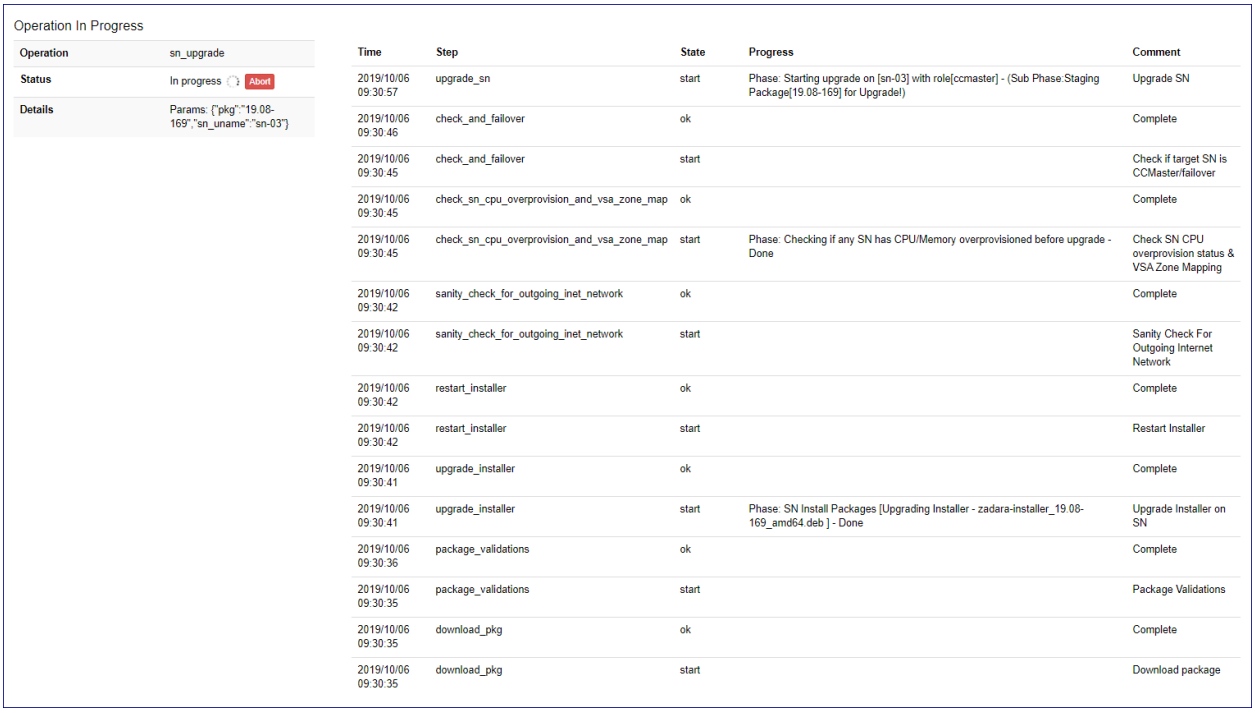
To upgrade a Storage Node from the SN dashboard:

1. Navigate to the Storage Node's dashboard.
2. On the **Resource Utilization** panel, click **Actions**.
3. From the dropdown, select **Upgrade Version**.
4. In the **Upgrade Storage Node** dialog:
    1. From the dropdown listing available versions, select the **Version** to install.

    > ✔ **Note:** Versions marked with an asterisk are available, but not downloaded to the cloud.
    >
    > Upgrading to an asterisked version requires a package download and registration beforehand.

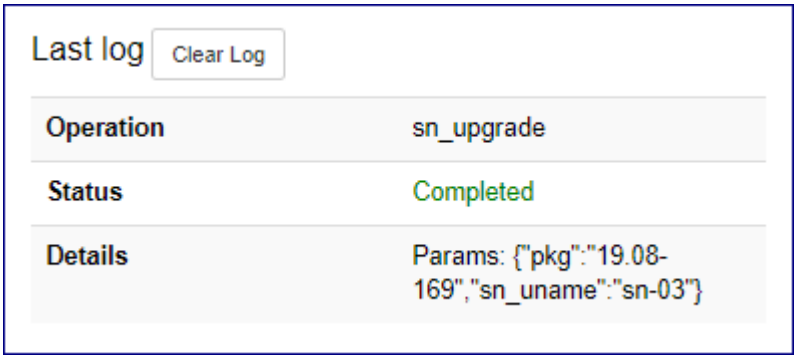
    2. Click **Upgrade** to confirm the Storage Node Version upgrade.

During the SN Version upgrade process, the status is displayed on Command Center's main dashboard.



The upgraded Storage Node's **Services** panel will present all services as **Offline**.

When the workflow is finished, the Command Center dashboard displays the **Completed** status for the Storage Node Version upgrade.



5.3.6 Upgradinging Storage Node Utilities Version

Storage Node utilities can be upgraded in a dedicated process via Command Center's SN dashboard.

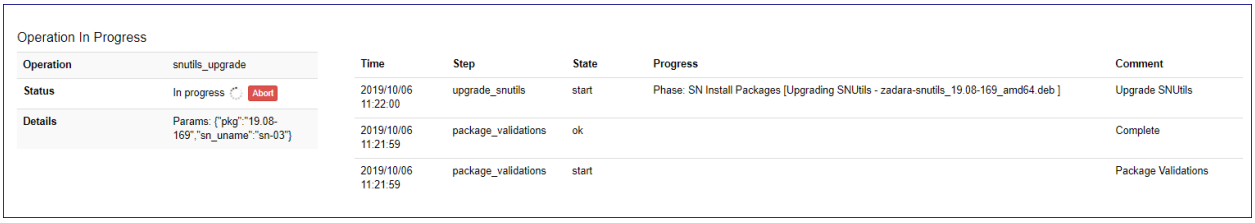
To upgrade Storage Node utilities from the SN dashboard:

1. Navigate to the Storage Node's dashboard.
2. On the **Resource Utilization** panel, click **Actions**.
3. From the dropdown, select **Upgrade Utilities**.
4. In the **Upgrade Storage Node Utilities** dialog:
    1. From the dropdown listing available versions, select the **Version** to install.

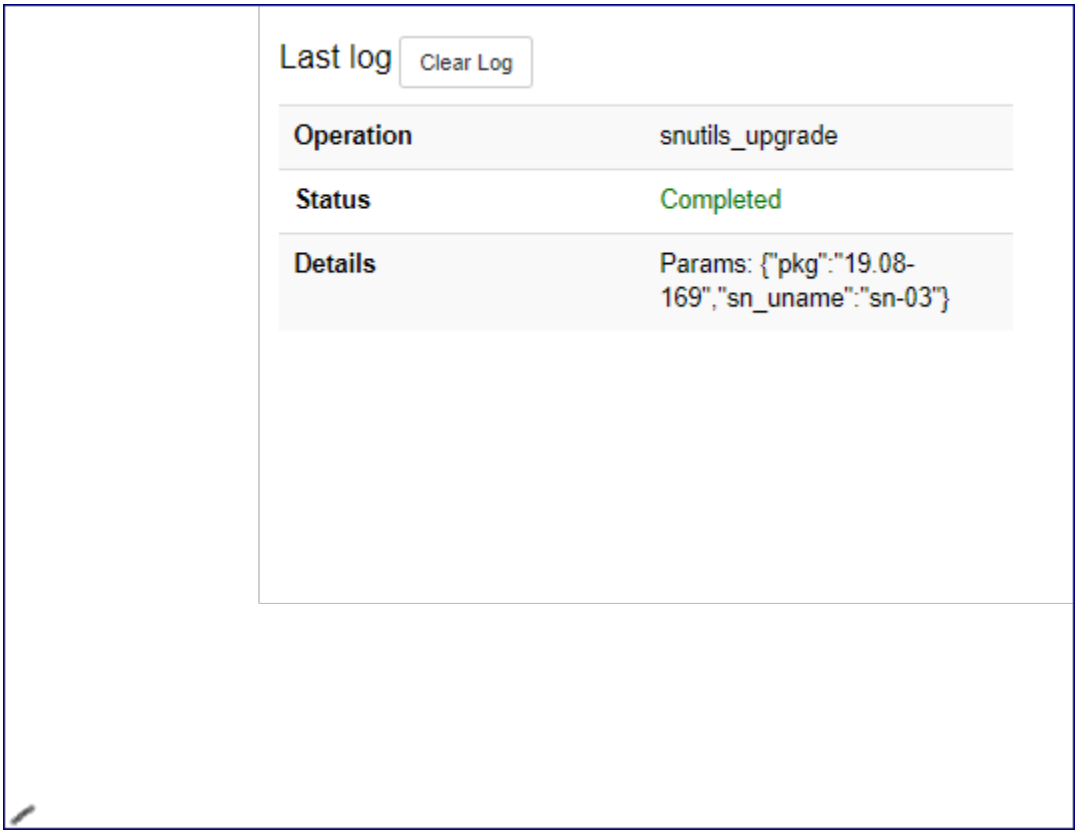
    > **Note:** Versions marked with an asterisk are available, but not downloaded to the cloud.
    >
    > Upgrading to an asterisked version requires a package download and registration beforehand.

    2. Click **Upgrade** to confirm the Storage Node Utilities upgrade.

During the SN Utilities upgrade process, the status is displayed on Command Center's main dashboard.



When the workflow is finished, the Command Center dashboard displays the **Completed** status for the Storage Node Utilities upgrade.

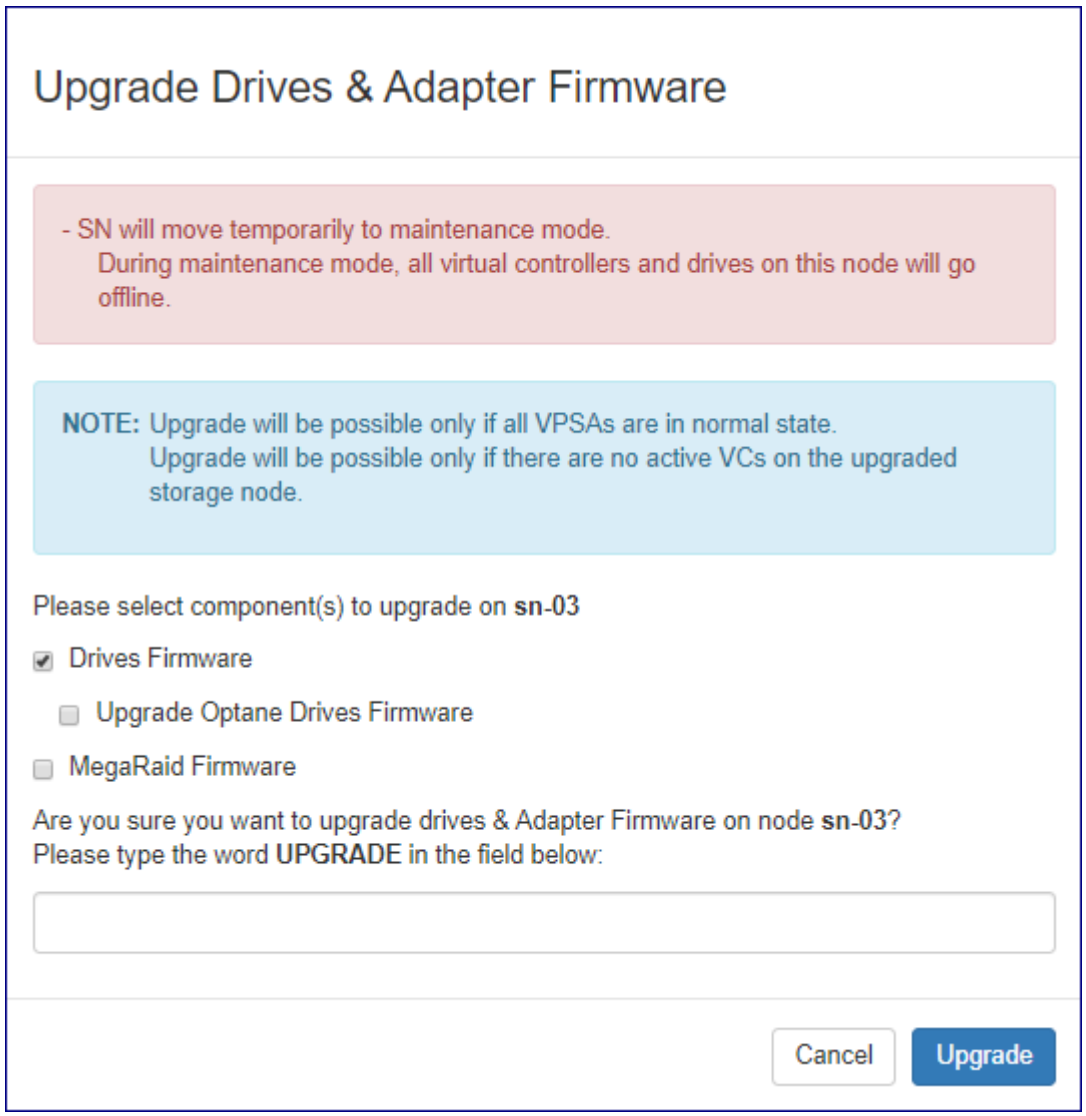


5.3.7 Upgrading Storage Node Disk Drives/RAID Controller Firmware

Command Center can be used to trigger an update of a Storage Node disk drive firmware or RAID controller firmware. Disk drive/RAID controller firmware are bundles with a specific SN software distribution and are updated according to each SW version's supported levels.

To update Drive/RAID controller firmware for a Storage Node:

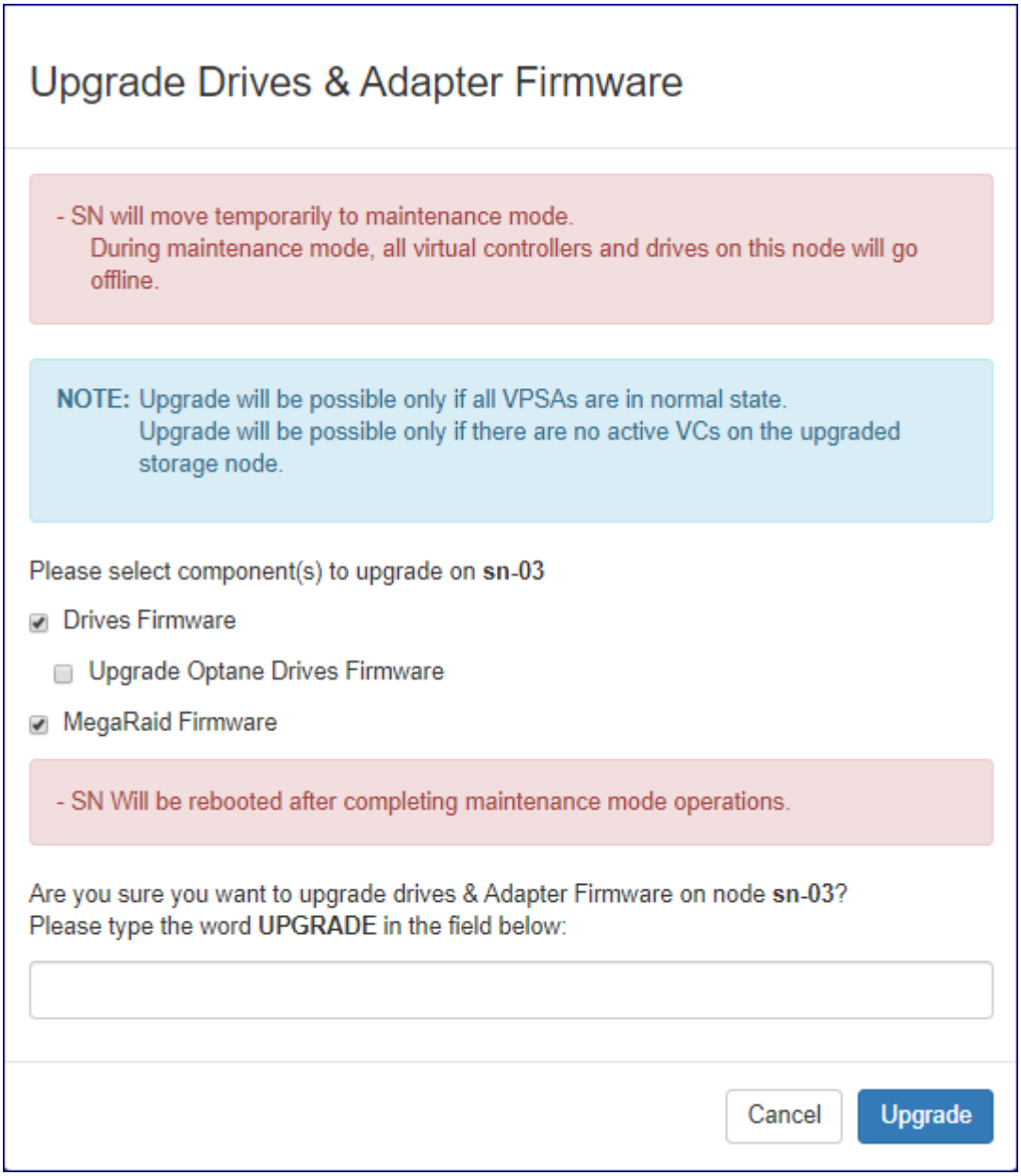
1. Navigate to the Storage Node's dashboard.
2. On the **Resource Utilization** panel, click **Actions**.
3. From the dropdown, select **Upgrade Drives & Adapter Firmware**.
4. In the **Upgrade Drives & Adapter Firmware** dialog:
    1. Select the elements for which you would like to perform the FW upgrade:



- Disk Drives
- Intel Optane Drives
- RAID controller

Note:

- In the event of a FW upgrade for Disk Drives or Intel Optane Drive, all disk drives and virtual controllers running on the SN will be taken offline.
- In the event of a FW upgrade for RAID controller, the SN will reboot after the FW is installed.



2. In the text box, enter the word "**UPGRADE**" and click **Upgrade** to confirm the Storage Node firmware upgrade.

During the SN firmware upgrade process, the status is displayed on Command Center's main dashboard.

When the workflow is finished, the Command Center dashboard displays the **Completed** status for the Storage Node firmware upgrade.

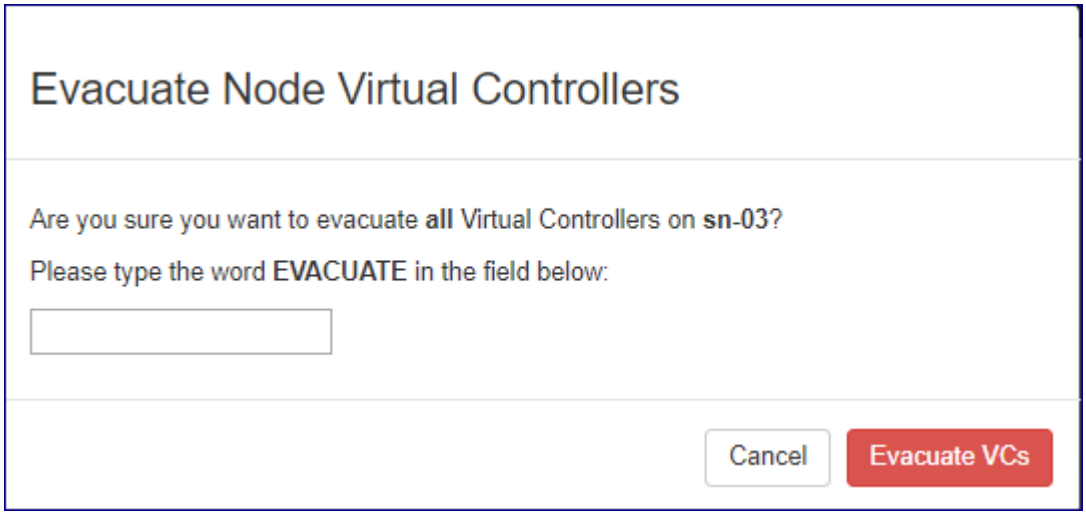
5.3.8 Evacuating all Virtual Controllers from a Storage Node

To immediately free all Storage Node compute resources, you can use Command Center to evacuate all virtual controllers running on it. Evacuation of virtual controllers is useful for preparation of activities such as hardware maintenance or refresh.

To evacuate all virtual controllers from a Storage Node:

1. Navigate to the Storage Node's dashboard.
2. On the **Resource Utilization** panel, click **Actions**.
3. From the dropdown, select **Evacuate Virtual Controllers**.
4. In the **Evacuate Node Virtual Controllers** dialog:

   In the text box, enter the word "**EVACUATE**" and click **Evacuate VCs** to confirm the Storage Node Virtual Controllers evacuation.



✔ **Note:** VC Evacuation is possible only if there is available compute capacity in other storage nodes within the cloud, which is sufficient for receiving the evacuated VCs (maintaining dual controller HA for VPSA and Object Storage fault domain demands).

5.3.9 Evacuating all drives from a Storage Node

In the event of decommisioning a Service Node, its drives should be evacuated. The result is the Service Node's drive data is tranferred from the Service Node's drives to new locations on a replacement Storage Node.

To evacuate all drives from a Storage Node:

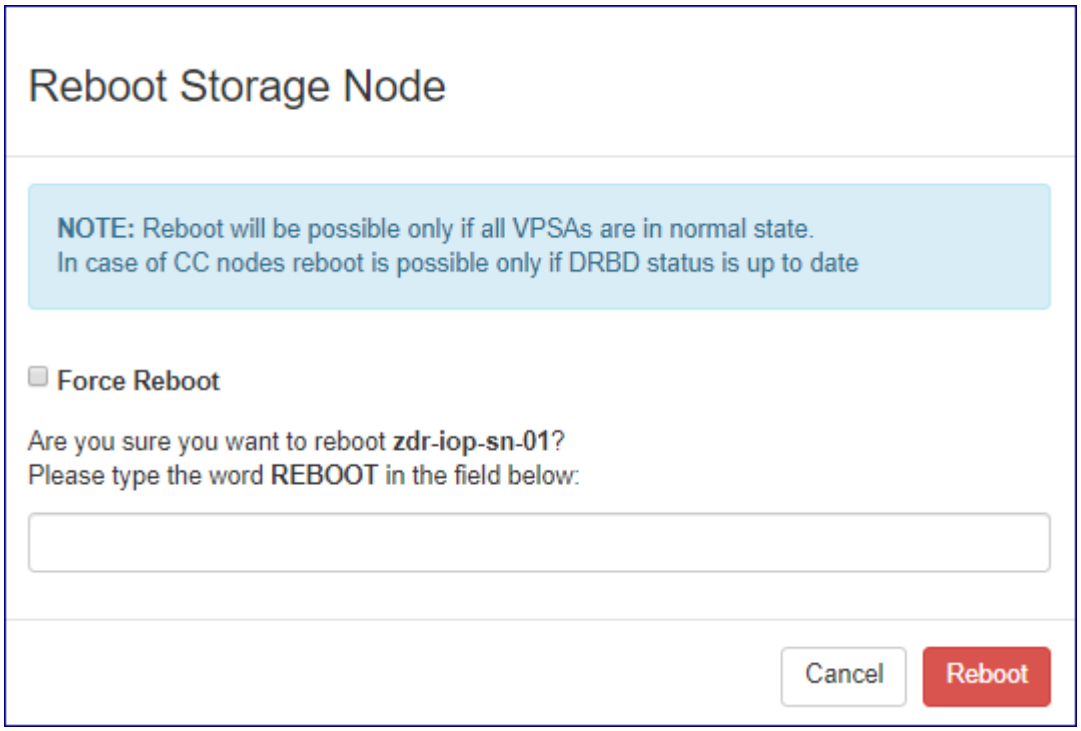
1. Navigate to the Storage Node's dashboard.
2. On the **Resource Utilization** panel, click **Actions**.
3. From the dropdown, select **Evacuate Drives**.
4. In the **Evacuate Node Drives** dialog:

   In the text box, enter the word "**EVACUATE**" and click **Evacuate Drives** to confirm the Storage Node drives evacuation.

5.3.10 Reboot a Storage Node

To reboot a Storage Node:

1. Navigate to the Storage Node's dashboard.
2. On the **Resource Utilization** panel, click **Actions**.
3. From the dropdown, select **Reboot**.
4. In the **Reboot Storage Node** dialog:



✔ **Note:** Restrictions:

- Storage Node reboot can be performed only if all underlying VPSA/VPSA Object Storage instances statuses are **Normal**.
- A reboot of the CCmaster/CCslave is performed only if the DRBD service is up to date.

The restrictions noted above can be overridden by marking the **Force Reboot** checkbox.

When using the **Force reboot** option, the cloud administrator is responsible for verifying and validating the VPSA/DRBD status before rebooting.

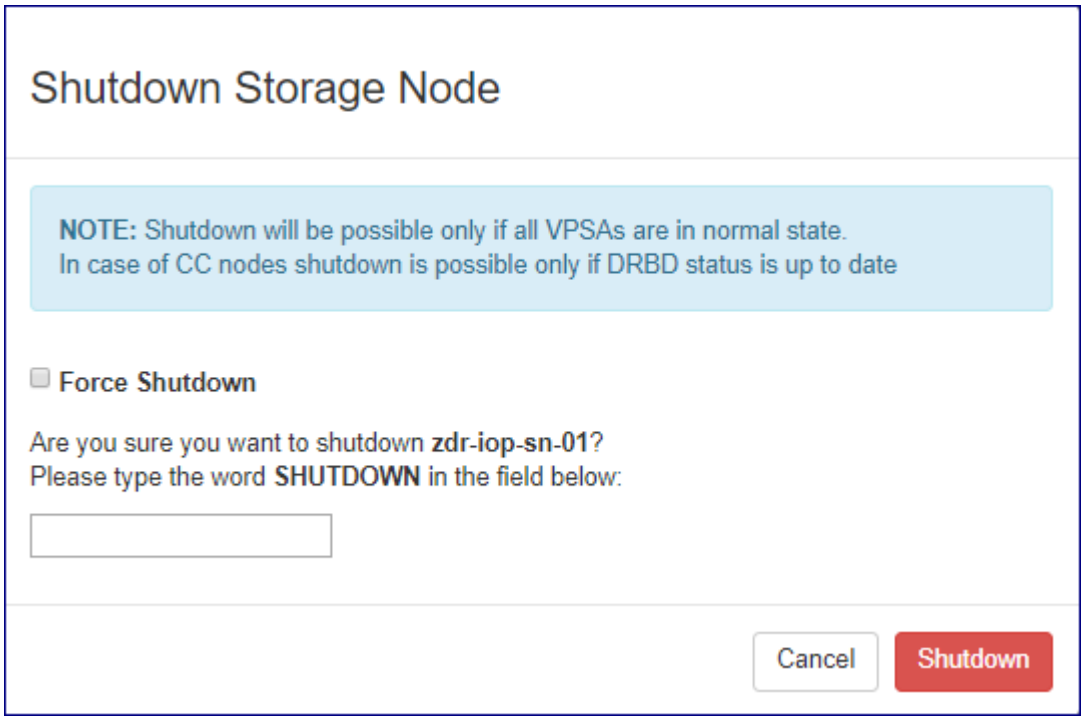
1. To override the restrictions, and force the reboot, mark the **Force Reboot** checkbox.
2. In the text box, enter the word "**REBOOT**" and click **Reboot** to confirm the Storage Node reboot.

5.3.11 Shutdown a Storage Node

To shut down a Storage Node:

a Storage Node:

1. Navigate to the Storage Node's dashboard.
2. On the **Resource Utilization** panel, click **Actions**.
3. From the dropdown, select **Shutdown**.
4. In the **Shutdown Storage Node** dialog:



Note: Restrictions:

- Storage Node shutdown can be performed only if all underlying VPSA/VPSA Object Storage instances statuses are **Normal**.
- A shutdown of the CCmaster/CCslave is performed only if the DRBD service is up to date.

The restrictions noted above can be overridden by marking the **Force Shutdown** checkbox.

When using the **Force Shutdown** option, the cloud administrator is responsible for verifying and validating the VPSA/DRBD status before shutting down the SN.

1. To override the restrictions and force the shutdown, mark the **Force Shutdown** checkbox.
2. In the text box, enter the word "**SHUTDOWN**" and click **Shutdown** to confirm the Storage Node shutdown.

CHAPTER

SIX

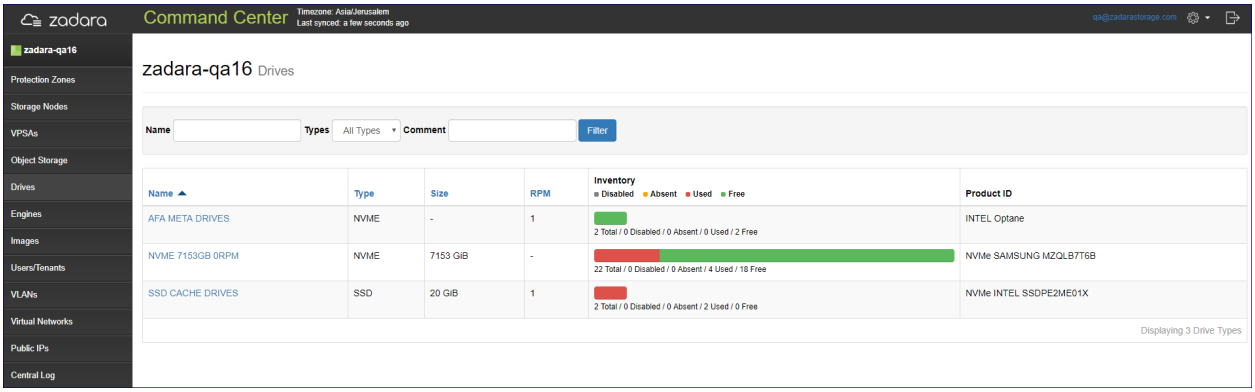
PHYSICAL DRIVES

Command Center provides extensive cloud physical drive management functionality. Using Command Center, a Zadara Cloud administrator can easily perform activities such as :

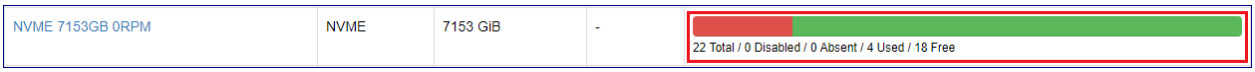
- Drive inventory management
- Drive validation and failure management
- Assignment of Drives to specific Quality of Service groups

6.1 Viewing Physical Drive Inventory

Command Center displays the overall Drive inventory in the **Drives** view.



The Drive inventory is primarily grouped by Drive model, and displays detailed utilization per group.



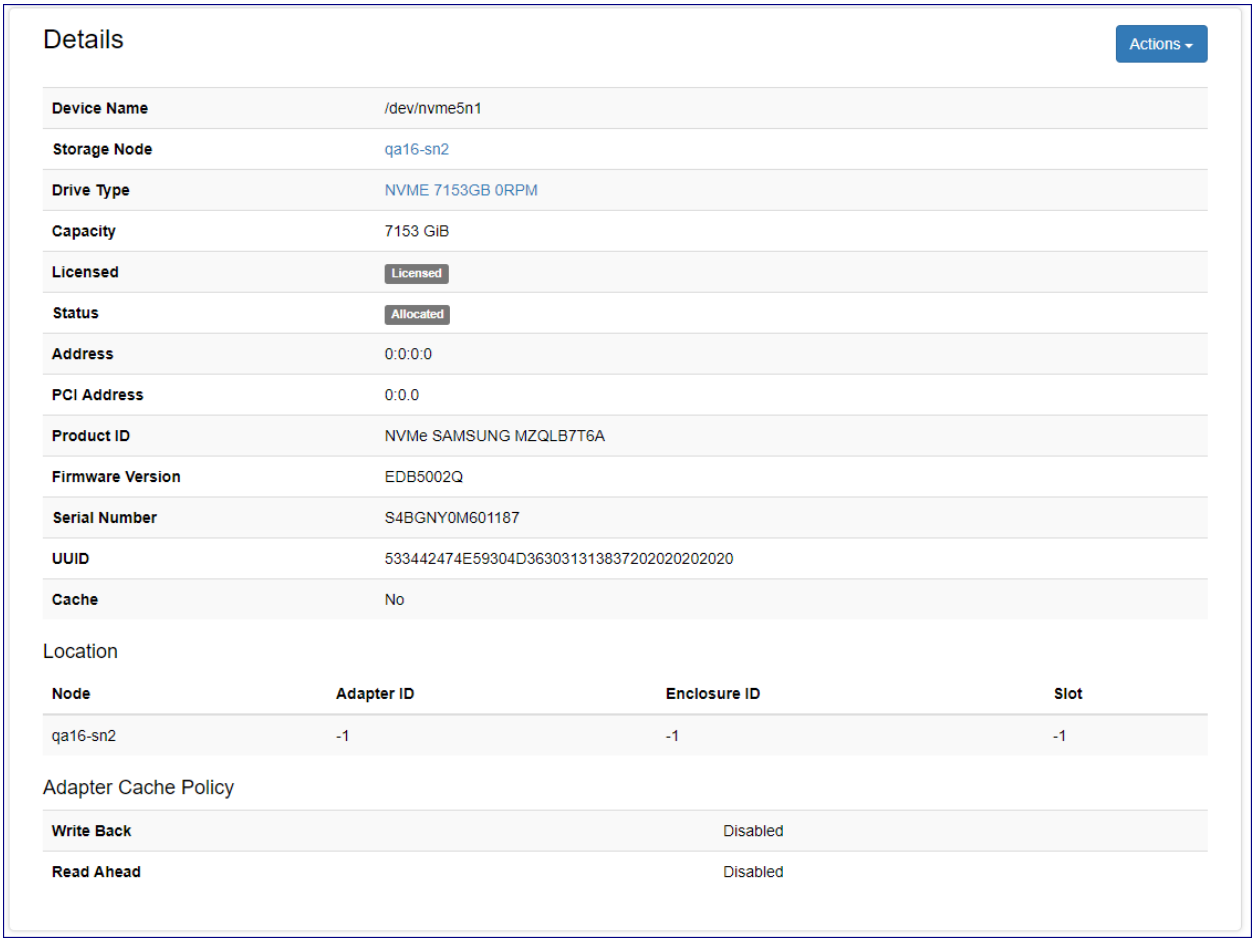
Status	Description
Total	Number of Drives from the specific model available in this cloud
Disabled	Drives that the cloud admin set as disabled
Absent	Drives that are physically unavailable (taken out of their bay)
Used	Drives that are actively assigned to a VPSA instance
Free	Drives that are not assigned to any VPSA instance

✔ **Note:** Drives that are assigned to a specific VPSA, deployed on a specific Protection Zone or installed on a specific Storage Node can also be viewed from the corresponding VPSA, Protection Zone and Storage Node.

6.2 Viewing Drive Properties

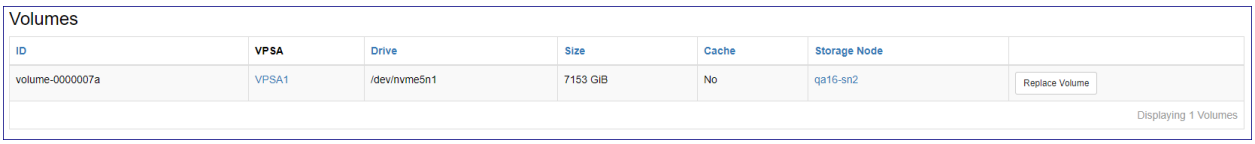
In the Command Center's **Drives** view, select the Drive Group to which the required Drive belongs. After the list of group members appears, select the required Drive.

6.2.1 Drive Properties



Property	Description
Device Name	Device file identifier for the Drive
Drive Type	Drive model
Capacity	Physical capacity (GiB) of the Drive **Note:** SSD Cache Drives also present the capacity of allocated partitions
License	Indicates whether the Drive is licensed on the cloud level
Status	Indicates the current status of the Drive. Possible values: • **Available**: The drive is ready for use and can be allocated • **Disabled**: An unassigned available drive has been removed from availability • **Allocated**: The drive is assigned to a VPSA • **Allocated (Disabled)**: The drive is assigned to a VPSA, but disabled • **Normal**: The drive is functioning correctly • **Failed**: The drive is not responding • **Replaced**: The drive data has been moved to another drive
Address	Storage Node SCSI address for the specified Drive
PCI Address	Storage Node PCI address for the specified Drive
Address	Storage Node SCSI address for the specified Drive
PCI Address	Storage Node PCI address for the specified Drive
Product ID	Product ID for the Drive
Firmware Version	Firmware Version of the Drive
Serial Number	Serial Number of the Drive
UUID	Linux UUID for the Storage Node Device
Cache	Whether the Drive is being used as SSD Cache
Location	Storage Node and MegaRaid location identifier for the Drive (Adapter ID/Enclosure ID/Slot)
Adapter Cache Policy	MegaRaid Adapter Cache Policy: • **Write Back**: Adapter write buffering • **Read Ahead**: Adapter read prefetching

6.2.2 Volume Properties

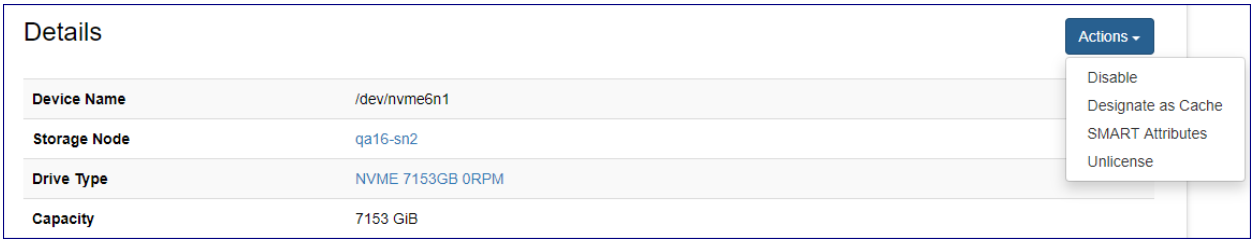


property	Description
ID	Volume Identifier
VPSA	VPSA/Object Storage to which this volume is allocated
Drive	Device file name for the Storage Node Physical Drive
Size	Volume Capacity
Cache	Whether this volume is used as a GEN2 SSD Cache device
Storage Node	Storage Node in which this volume is defined
Replace Volume	Toggle Drive replacement for this volume

6.3 Performing Operations On Physical Drives

To view all operations that can be performed on a specific Drive:

1. From the **Drives** view, select the appropriate Drive Group and go to the **Drives** tab.
2. Click the required Physical Drive.
3. In the Drive's **Details** panel on its **Dashboard** tab, click **Actions** to display the dropdown listing the possible operations for the Drive.



6.3.1 Disabling a Drive

1. From the Drive's **Actions** dropdown, select **Disable**.
2. In the **Disable Drive** dialog, click **Disable** to confirm disabling the Drive.

   After the operation is complete, the Drive's Status change to **Disabled**.

6.3.2 Enabling a Drive

1. Select a disabled Physical Drive.
2. In the **Enable Drive** dialog, click **Enable** to confirm enabling the Drive.

   After the operation is complete, the Drive's Status change to **Enabled**.

6.3.3 Managing Drive LED

A Physical Drive LED can be turned on or off in Command Center.

To manage a Physical Drive LED:

1. From the Drive's **Actions** dropdown, select **LED On** or **LED Off**.
2. In the **Enable Drive LED** or **Disable Drive LED** dialog, click **Confirm** to confirm enabling or disabling the Drive LED.

6.3.4 Viewing Drive SMART Attributes

✔ **Note:** Self-Monitoring, Analysis and Reporting Technology (SMART) attributes are parameters that provide information about the health and status of a disk drive. These attributes are monitored by the disk drive itself.

SMART attributes can differ betwwen disk brands and models.

To view a Drive's SMART attributes:

1. From the **Drives** view, select the appropriate Drive Group and go to its **Drives** tab.
2. Click the required Physical Drive.
3. In the Drive's **Dashboard** tab, in the **Details** panel, click **Actions** and from the dropdown select **SMART Attributes**.

   The **SMART Attributes** dialog displays the Drive's SMART attributes.

6.3.5 Designating SSD Drive as Cache

SSD Drives installed in the cloud can be designated as Cache Drives for use in hybrid VPSA configurations.

✔ **Note:** The available capacity of an SSD Drive designated as Cache cannot be allocated as user data to VPSA images.

1. From the Drive's **Actions** dropdown, select **Designate as Cache**.
2. The **Confirm Drive Change** dialog displays warning information that the Drive will no longer be available for user storage.

   Click **Confirm** to confirm designating the Drive as Cache.

   After the operation is complete, the Drive Type will change to **SSD CACHE DRIVES**.

6.3.6 Undesignating SSD Drive as Cache

An SSD Drive that is designated as a Cache Drive can be undesignated, to serve as regular drive for user storage.

1. From the Drive's **Actions** dropdown, select **Undesignate as Cache**.
2. In the **Confirm Drive Change** dialog click **Confirm** to confirm undesignating the Drive as Cache.

   After the operation is complete, the Drive Type will change to its native SSD Drive Type.

6.3.7 Removing Drives

The cloud administrator can initiate an orderly removal of Physical Drives from the cloud via Command Center.

To start the removal process, select **Offline and Remove** from the Drive's **Actions** dropdown.

6.3.8 Unlicensing a Drive

✔ **Note:** Drives that are in use and have the **Allocated** status cannot be unlicensed.

Only licensed Drives that have the **Available** status can be unlicensed.

1. From the Drive's **Actions** dropdown, select **Unlicense**.
2. In the **Unlicense Drive** dialog, click **Confirm** to confirm unlicensing the Drive.

   After the operation is complete, the Drive Type will change to **Unlicensed**.

6.4 Monitoring Drive Performance

To view performance statistics for a specific Drive:

1. From the **Drives** view, select the appropriate Drive Group and go to the **Drives** tab.
2. Click the required Physical Drive.
3. Go to the **Performance** tab that displays the Drive's performance statistics:
    - Average IO rate displayed as read vs. write IOs
    - Average IO time displayed as read vs. write IOs
    - Average Bandwidth displayed as read vs. write activity

The monitoring interval can be changed. Supported monitoring intervals:

- 1 seconds
- 10 seconds
- 1 minute
- 1 hour
- 1 day

Click the **Auto-Refresh** toggle to activate or disable the automatic display of updated monitoring data on reaching the monitoring interval.

CHAPTER

SEVEN

VPSA (VIRTUAL PRIVATE STORAGE ARRAYS)

Using Command Center, cloud administrators can manage and monitor Virtual Private Storage Array instances running in the cloud. Command Center's VPSA management feature set provides administrators with a single pane of glass, in which administrators receive a holistic image of the underlying instance's status and operations, and allows for enforcements of policies, lifecycle management and supervised resource distribution.

Important: Administrators are recommended not to change any configurations, unless directed to do so by Zadara Support.

7.1 Viewing Virtual Private Storage Array Properties

To view a specific VPSA:

1. Click **VPSAs** in Command Center's left menu panel.
2. In the VPSAs grid, click the VPSA instance.

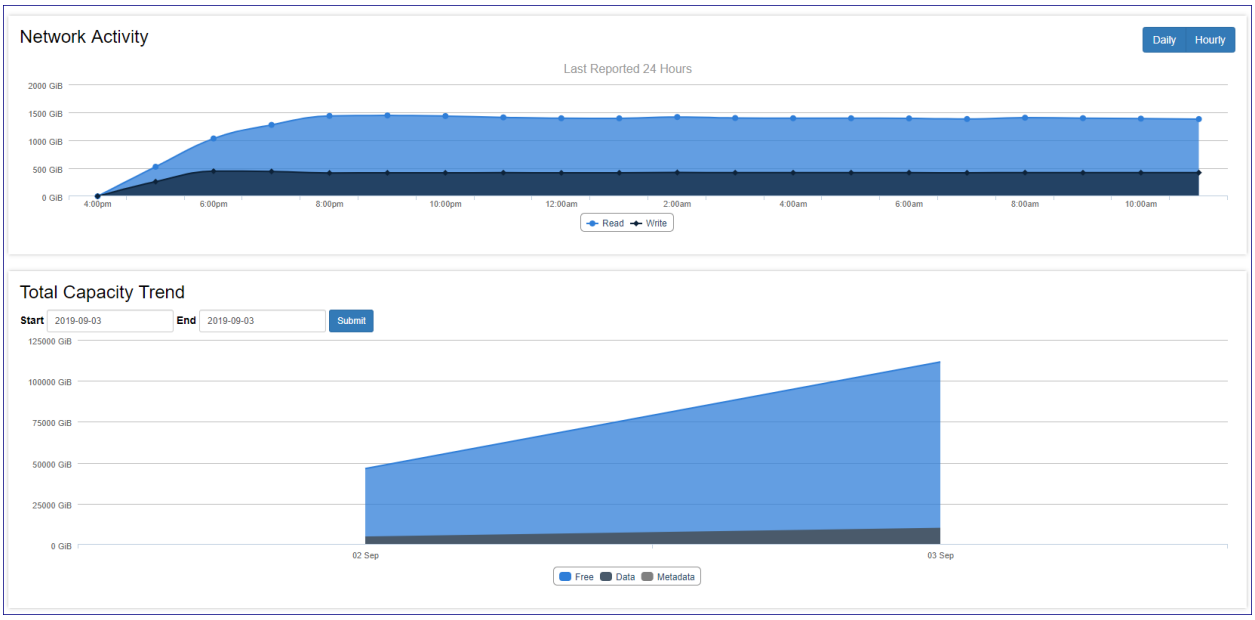
7.1.1 VPSA Instance Dashboard

The VPSA instance's main **Dashboard** tab's **Information** panel provides information regarding the VPSA's configuration, current health status and network topology.

Property	Description
Name	VPSA instance's display name
Internal Name	VPSA instance's internal name
User	User who created the instance
Company	Company of the user who created the instance
Description	Description given when the instance was provisioned
Nova ID	VPSA instance's Nova ID
Status	Current status of the instance
Protection Zone	Instance Protection Zone configuration
Image	Instance deployment image
IO Engine Type	VPSA IO Engine Flavor
App Engine Type	VPSA APP Engine Flavor
VCPUs	Instance VCPU count
RAM	Instance configured RAM capacity
Base Cache	Instance Base Cache capacity
Extended Cache	Instance Extended SSD cache configured capacity
Setup Volume Capacity	Instance setup volume capacity
IP Address	Instance floating frontend IP address
Public IP	Instance public IP address
Mgmt. Address	Instance hostname for management access
UUID	Instance UUID
SNMPv3 Engine ID	Instance SNMPv3 Engine ID
Created	Instance creation timestamp
Updated	Instance last update timestamp

The VPSA instance's main **Dashboard** tab provides monitoring charts with adjustable time period views:

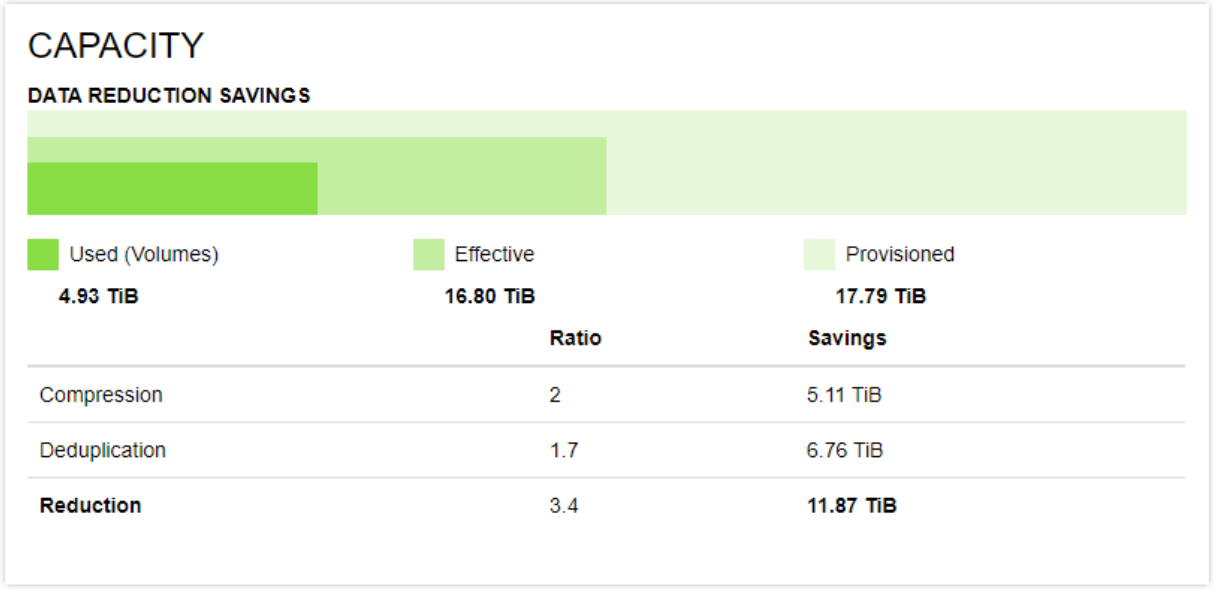
- **Network Activity** chart
- **Total Capacity Trend** chart displaying capacity utilization



VPSA Flash Array: The main **Dashboard** tab also displays the **Capacity Data Reduction Savings** panel:

- A chart comparing used capacity, provisioned and effective capacity.

- Information about savings from inline data deduplication and inline data compression, and the VPSA overall data reduction ratio.



The VPSA resource tabs provide information regarding underlying resources attached to the VPSA:

- Physical Drives
- Virtual Controllers
- RAID Groups
- Pools

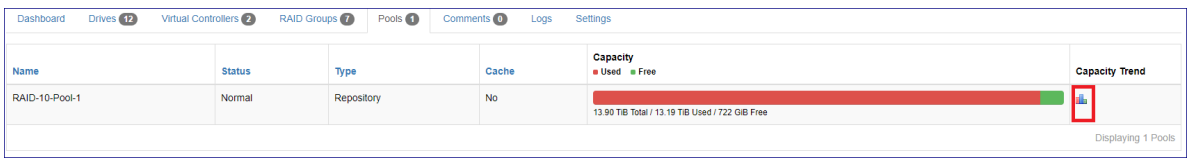
✔ **Note:** The **RAID Group** tab also displays information on internal groups such as **Metering** and **Journal**, which are not visible or accessible to VPSA users.

7.1.2 VPSA Pools tab

The VPSA **Pools** tab displays consumption in **Pool Capacity Trend** charts. These charts provide cloud administration with an overview of the Pool's capacity change over time, and the effect of data reduction mechanisms such as deduplication and compression on VPSA Flash Array Pools.

To view the capacity trend for a specific Pool:

1. Navigate to the VPSA's **Pools** tab.
2. In the Pools grid, click the charts icon in the Pool's **Capacity Trend** column.



Pool Capacity Trends charts display capcity trends over a period of time, defaulting to the past month.

To change the trend display period, enter the **Start** and **End** dates, and click **Submit**.

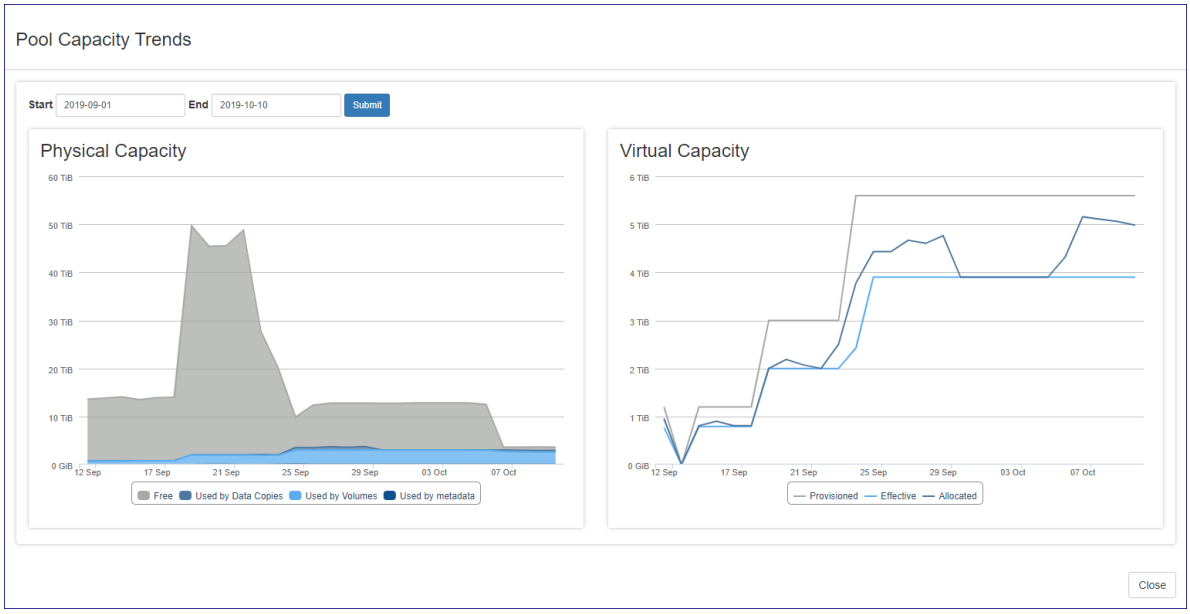
Pool Capacity Trends chart styles

The **Pool Capacity Trends** chart styles depend on the type of VPSA:

- VPSA Storage Array:

  A single chart displays the overall **Free**, **Data** and **Metadata** Pool Capacity Trends over time.

- VPSA Flash Array: Two charts display the Pool's Capacity Trends:
  - **Physical Capacity**: Overall Pool Capacity trends over time:
    - Free
    - Used by Data Copies
    - Used by volumes
    - Used by metadata
  - **Virtual Capacity**: Comparison of Provisioned Capacity, Virtual Capacity and Effective Capacity trends over time.

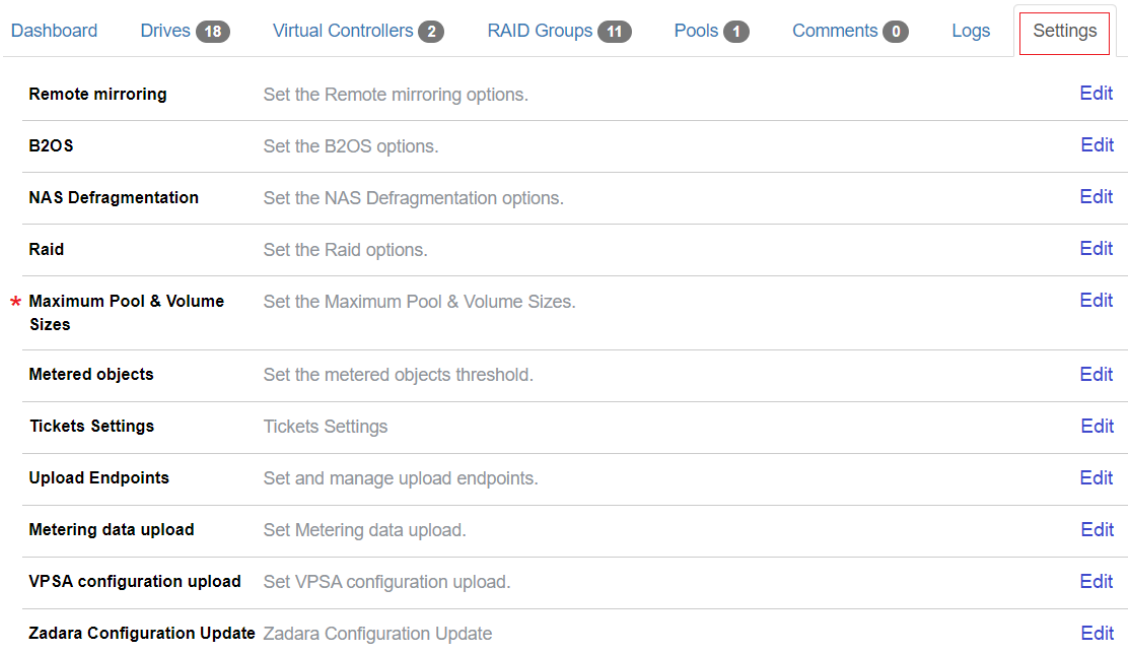


7.2 Configuring Virtual Private Storage Array Settings

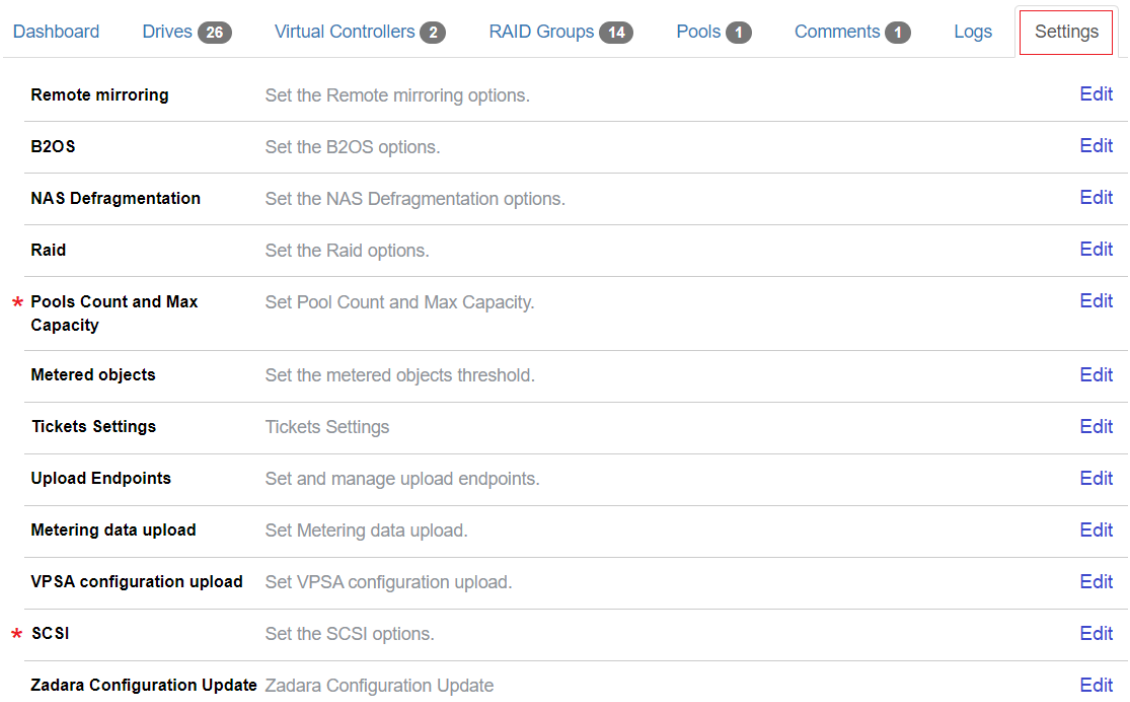
✔ **Note:** Most of the VPSA settings for VPSA Storage Array and VPSA Flash Array are identical. Differences are highlighted.

To view or alter VPSA settings:

1. Click the VPSA's **Settings** tab.
2. Click **Edit** on a specific setting to view or update its details.
   - VPSA Storage Array **Settings**:



   - VPSA Flash Array **Settings**:



7.2.1 Remote mirroring properties

Parameter	Description
Dst total quota pc	Allowance for amount of unapplied data for all VPSA mirror jobs 0 - No quota enforcement
Connections count	Number of TCP sessions established between two VPSAs performing mirroring

7.2.2 Backup to Object Storage (B2OS)

Parameter	Description
Src buffers count	Amount of source buffers allocated for B2OS activities
Dst buffers count	Amount of destination buffers allocated for B2OS activities

7.2.3 NAS Defragmentation

Parameter	Description
Minimum extents count	Number of extents a file needs to have to be considered for defragmentation
Minimum file alignment percent VPSA Flash Array	Defrag files of size greater than “Minimum file size in KiB” AND have less than “Minimum file alignment percent” of extents that are not aligned to pool LSA chunk size.
Minimum file size in kib VPSA Flash Array	Defrag files of size greater than “Minimum file size in KiB” AND have less than “Minimum file alignment percent” of extents that are not aligned to pool LSA chunk size.

✔ **Note:** Scope: VPSA Flash Array

For a file defragmention to occur, both of the following conditions must apply:

- The file's size is greater than the **Minimum file size in KiB**
- The file has fewer extents than the **Minimum file alignment percent** that are not aligned to the Pool's LSA chunk size

7.2.4 RAID

Parameter	Description
Allow mixed types	Enable allowing a mix of HDD types in the sameRAID Group or Pool

7.2.5 Maximum Pool & Volume Sizes

Scope: VPSA Storage Array

Parameter	Description
Pool transactional max size	Maximum capacity (TiB) of a transactional pool
Pool repository max size	Maximum capacity (TiB) of a repository pool
Pool archival max size	Maximum capacity (TiB) of an archival pool
Pool depot max size	Maximum capacity (TiB) of a depot pool

7.2.6 Pools Count and Max Capacity

Scope VPSA Flash Array

Parameter	Description
Pool iops optimized allocation limit capacity in tib	Pool IOPs optimized allocation limit capacity in TiB
Pool balanced allocation limit capacity in tib	Pool balanced max mapped capacity in TiB
Pool throughput optimized allocation limit capacity in tib	Pool throughput optimized max mapped capacity in TiB
Maximum number of pools	Max Number of Pools allowed for this VPSA

7.2.7 Metered objects

Parameter	Description
Check interval	Interval in seconds for validation of metered objects threshold alerts
Report interval	Interval in seconds for rate limiting all metered objects thresholds alerts
Read cache late IO threshold	Amount of read hit IO operations with late time exception required to trigger an alert
Read cache late IO threshold time(ms)	Read hit IO operation service time value that is considered as late IO
Write cache late IO threshold	Amount of write hit IO operations with late time exception required to trigger an alert
Write cache late IO threshold time (ms)	Write hit IO operation service time value that is considered as late IO
Enable metering upload agent	Enable upload of metering data to an external cloud repository

7.2.8 Ticket Settings

See Managing Cloud Settings > Management Settings in this manual for details regarding the ticket settings section.

7.2.9 Upload Endpoints

The cloud administrator can configure alternative endpoints for uploading cloud Zsnaps, MAG and configuration information.

Expanding the Upload Enpoints section displays details of the cloud's configured endpoints.

Upload endpoints can be of the following types:

- AWS S3 endpoint

Parameter	Description
Endpoint name	The endpoint's name
Method	AWS S3
Access Key	Endpoint access key
Secret Key	Endpoint secret key
Region	AWS region

- Object Storage endpoint

Parameter	Description
Endpoint name	The endpoint's name
Method	ZIOS S3
Access Key	Endpoint access key
Secret Key	Endpoint secret key
Endpoint	Object Storage FQDN

- FTP target

Parameter	Description
Endpoint name	The endpoint's name
Method	FTP
Server	FTP server
User	Username
Password	Password
Use Proxy	Whether to use a proxy for the connection

Creating a new endpoint

To create a new endpoint:

1. Expand the **Upload Endpoints** section.
2. At the top right of this section, click **New**.
3. In the **Create Upload Endpoint** dialog, select the endpoint **Method** from the dropdown list, and enter the other parameters relevant to its **Method**.
4. Click **Save**.

Editing an endpoint

To edit an endpoint:

1. Expand the **Upload Endpoints** section.
2. Locate the endpoint to edit. In its **Actions** column, click **Edit**.

> ✔ **Note:** Some system-supplied endpoints are not editable.

3. In the **Edit Upload Endpoint** dialog, update the relevant parameters.

> ✔ **Note:** The endpoint's **Name** and **Method** can not be changed.

4. Click **Save**.

Deleting an endpoint

To delete an endpoint:

1. Expand the **Upload Endpoints** section.
2. Locate the endpoint to delete. In its **Actions** column, click **Delete**.

> ✔ **Note:** Some system-supplied endpoints can not be deleted.

3. In the **Delete Upload Endpoint** dialog, confirm the deletion.

7.2.10 Metering data upload

The cloud administrator can configure the target endpoints to which metering data can be uploaded. Up to three AWS S3 endpoints can be configured for metering data uploads.

Adding an additional endpoint

To add an additional upload endpoint:

1. Expand the **Metering data upload** section.
2. Click **Add Another**.
3. Select the **Endpoint** from the dropdown and enter the **Bucket**.

Parameter	Description
Endpoint	Endpoint for metering data upload
Bucket	Bucket for metering data upload

4. Click **Update**.

Removing an additional endpoint

To remove an additional endpoint:

1. Expand the **Metering data upload** section.
2. Locate the additional endpoint to remove and click **Discard Endpoint**.
3. Click **Update**.

7.2.11 VPSA configuration upload

The cloud administrator can configure the target endpoints to which metadata from this cloud for Zadara management and analysis can be uploaded. Up to three AWS S3 endpoints can be configured for these uploads.

Adding an additional endpoint

To add an additional upload endpoint:

1. Expand the **VPSA configuration upload** section.
2. Click **Add Another**.
3. Select the **Endpoint** from the dropdown and enter the **Bucket**.

Parameter	Description
Endpoint	Endpoint for metering data upload
Bucket	Bucket for metering data upload

4. Click **Update**.

Removing an additional endpoint

To remove an additional endpoint:

1. Expand the **VPSA configuration upload** section.
2. Locate the additional endpoint to remove and click **Discard Endpoint**.
3. Click **Update**.

7.2.12 SCSI

Scope: VPSA Flash Array

- VPSA Block Volume XCopy Concurrency

7.2.13 Zadara Configuration Update

Administrators can define Zadara Configuration Keys.

Creating Zadara Configuration Keys

To create a new Configuration Key:

1. Click **New**.
2. In the Create Zadara Configuration Key dialog:
    1. Select **Key Type** from the dropdown. Possible options:
        - **String**
        - **Integer**
        - **Float**
        - **Boolean**
    2. Enter the **Keyname** and **Key Value** pair.
    3. Click **Save**.

Editing and Deleting Zadara Configuration Keys

To **Edit** or **Delete** an entry, click on the appropriate button in the **Actions** column.

7.3 Performing Virtual Private Storage Array Operations

7.3.1 Changing VPSA engine configuration

Command Center can be used to modify a VPSA engine type to a bigger or smaller engine, or to update the configuration of a VPSA ZCS engine.

To change a VPSA's engine configuration:

1. Navigate to the VPSA's dashboard.
2. On the VPSA's **Information** panel, click **Actions**.
3. From the dropdown, select **Change Engine Type(s)**.
4. In the **Change Engine Type(s)** dialog:
    1. Select an **IO Engine type** from the dropdown.
    2. Select a **ZCS App Engine type** from the dropdown.
    3. **Advanced** options:

Option	Description
Advanced Scheduling	After the Standby Virtual Controller changes to the new engine, the change engine process is paused. The VPSA will failover to the Standby Virtual Controller and proceed with active Virtual Control engine change according to the selected option: • **Immediate** Failover will take place immediately after the Standby Virtual Controller engine is changed (default) • **Manual** Failover will be done on demand, upon Resume action initiation • **Scheduled** Failover will be done at the requested time, configurable from 30 minutes from the current time and up to 7 days
Version Upgrade	Performs a VPSA version upgrade to a selected version, alongside the engine model change process

4. Click **Confirm** to confirm the **Change Engine Type(s)** operation.

   The VPSA Status changes to **Change Engine** for the duration of the process, and then to **Normal** when complete.

7.3.2 Adding physical drives

Note:

- New drives added to a VPSA are not automatically associated with a RAID group or data pool. The VPSA administrator is required to configure drive association.
- zStorage enforces the limits of maximum permitted drives per VPSA engine model, and they cannot be exceeded.

To add physical drives to a VPSA:

1. Navigate to the VPSA's dashboard.
2. On the VPSA's **Information** panel, click **Actions**.
3. From the dropdown, select **Add Drives**.
4. In the **Add Drives** dialog:
   1. VPSA Flash Array

      Select the **Storage Class** of the Drives to add:

      - SSD Storage Class
      - HDD Storage Class

      The selected **Storage Class** determines the possible Drive Types for the next selection step.

2. VPSA Storage Array and VPSA Flash Array

   From the dropdowns, select:

   1. **Number** of Drives to add
   2. **Drive Type**
   3. Click **Confirm** to confirm the **Add Drives** operation.

7.3.3 Change VPSA Cache configuration

Scope: VPSA Storage Array

The Flash Cache configuration specifies the amount of Flash Cache capacity on top of the specific model baseline. By default it is 0 GiB.

Cloud administrators can use Command Center to raise or lower the Flash Cache configuration of a VPSA.

✔ **Note:** VPSA model 200 does not support extended Flash Cache.

To change the Cache configuration for a specific VPSA:

1. Navigate to the VPSA's dashboard.
2. On the VPSA's **Information** panel, click **Actions**.
3. From the dropdown, select **Change Cache**.
4. In the **Change Cache** dialog:
   1. From the dropdown, select the amount of Cache in GiB.
   2. Click **Submit** to confirm the **Change Cache** operation.

7.3.4 Upgrading a VPSA

Command Center allows administrators to perform a version upgrade on the VPSA instances running in the cloud.

To upgrade a VPSA's version:

1. Navigate to the VPSA's dashboard.
2. On the VPSA's **Information** panel, click **Actions**.
3. From the dropdown, select **Upgrade**.
4. In the **Upgrade VPSA** dialog:
   1. From the dropdown, select the VPSA image version for the upgrade.
   2. **Advanced** options:

Option	Description
Advanced Scheduling	After the Standby Virtual Controller changes to the new engine, the upgrade is paused. The VPSA will failover to the Standby Virtual Controller and proceed with active Virtual Control upgrade according to the selected option: • **Immediate** Failover will take place immediately after the Standby Virtual Controller engine is upgraded • **Manual** Failover will be done on demand, upon Resume action initiation • **Scheduled** Failover will be done at the requested time, configurable from 30 minutes from the current time and up to 7 days
Version Validation	By default, the upgrade process includes version validation. Mark the checkbox to skip the validation.

3. Click **Upgrade**.
4. In the **Confirm Upgrade** dialog, click **Upgrade** to confirm the **Upgrade VPSA version** operation.

   The VPSA Status changes to **Upgrading version** for the duration of the process, and then to **Normal** when complete.

✔ **Note:**

- A scheduled VPSA upgrade operation performs an immediate upgrade of the passive Virtual Controller.
- From cloud version 20.12, an upgrade to a VPSA version that is more than 2 major releases after the current version will be blocked by Command Center.
- From cloud version 20.12, VPSA version downgrades are blocked by Command Center.

7.3.5 Cancelling a Scheduled VPSA upgrade

From version 20.12 and later, it is possible to cancel a scheduled VPSA upgrade in Command Center:

To cancel a scheduled upgrade:

1. Navigate to the VPSA's dashboard.
2. On the VPSA's **Information** panel, click **Actions**.
3. From the dropdown, select **Cancel Scheduled upgrade**.
4. In the **Cancel Scheduled upgrade** dialog, click **Cancel Upgrade** to confirm cancellation of the scheduled VPSA upgrade.

✔ **Note:** A scheduled upgrade operation performs an immediate upgrade of the passive Virtual Controller.

Cancelling a scheduled upgrade reverts the passive Virtual Controller back to the base version.

7.3.6 Assigning or Unassigning a Public IP address to a VPSA

In specific cases where a VPSA must be available for management access from outside of its cloud-allocated VLAN, a public IP address can be assigned to it.

See Public IP Addresses for information about configuration of cloud-level public IP ranges.

Assigning a Public IP address to a VPSA

To assign a public IP address:

1. Navigate to the VPSA's dashboard.
2. On the VPSA's **Information** panel, click **Actions**.
3. From the dropdown, select **Assign Public IP**.
4. In the **Assign Public IP** dialog:
    1. Select one of the options:
        - **Automatic IP address assignment**
        - **Manual IP address assignment**

          Select an IP from the dropdown that displays for the manual IP assignment option.
    2. Click **Assign** to confirm the **Assign Public IP** operation.

Unassigning a Public IP address

To unassign a Public IP address:

1. Navigate to the VPSA's dashboard.
2. On the VPSA's **Information** panel, click **Actions**.
3. From the dropdown, select **Unassign Public IP**.
4. In the **Unassign Public IP** dialog, click **Confirm** to confirm the **Unassign Public IP** operation.

7.3.7 Adding or removing a VPSA's Virtual Network

An existing VSPA is created with one Primary Virtual Network, and can be assigned additional Virtual Networks.

VPSAs connected to multiple networks can be used to enable use cases requiring partitioning or isolation per volume.

✔ **Note:**

- A VPSA is limited to a maximum of 64 Virtual Networks, depending on the IO engine.
- The VPSA REST API and UI are accessible through any Virtual Networks.
- Only the Primary Virtual Network's IP is registered in DNSimple.
- A VPSA can't have two Virtual Networks with the same VLAN.
- The Primary Virtual Network is the only routable network.

  Other Virtual Networks are not routable.
- Active Directory can be joined only through the Primary Virtual Network.

- Backup (B2OS), Mirror, Remote Clone through the FE network are possible only via the Primary Virtual Network.
- ZCS container services exposed through the FE network can be done only on the Primary Virtual Network.
- iSER host connectivity is available only on the Primary Virtual Network.

See Performing Cloud Networking Management for viewing, creating and deleting the cloud's Virtual Networks.

Adding a Virtual Network to a VPSA

Warning: The addition of a Virtual Network will restart SMB services, causing existing mapped shares to be temporarily unavailable.

To assign a Virtual Network to a VPSA:

1. Verify that an appropriate Virtual Network is already defined in the cloud, excluding the Virtual Network already in use by the VPSA.
2. Navigate to the VPSA's dashboard.
3. On the VPSA's **Information** panel, click **Actions**.
4. From the dropdown, select **Add Virtual Network**.
5. In the **Add Virtual Network** dialog:
    1. Select the Virtual Network to assign to the VPSA.
    2. Click **Add** to confirm adding the Virtual Network to the VPSA.

       On completion, the newly added Virtual Network displays in the VPSA's **Virtual Network** tab.

Releasing a Virtual Network from a VPSA

Note: The VPSA's Primary Virtual Network cannot be released.

Warning: Releasing a Virtual Network restarts SMB services, causing existing mapped shares to be temporarily unavailable.

The exact reaction to such disconnections is dependent on the underlying application that is using the files shares.

To release a Virtual Network from a VPSA:

1. Navigate to the VPSA's dashboard.
2. On the VPSA's **Information** panel, click **Actions**.
3. From the dropdown, select **Release Virtual Network**.
4. In the **Release Virtual Network** dialog:
    1. Select the Virtual Network to release from the VPSA.

2. Click **Release**.

   The **Confirm Release Virtual Network** dialog opens, displaying a warning that the VPSA will no longer be accessible via the selected Virtual Network.

   Click **Release** to reconfirm releasing the Virtual Network from the VPSA.

   On completion, the released Virtual Network no longer appears in the VPSA's **Virtual Network** tab.

7.3.8 Performing a managed Virtual Controller failover

Command Center can be used to trigger a managed VPSA failover to its standby Virtual Controller. A managed failover can be used by cloud administrator to evacuate all active Virtual Controllers from a specific Storage node before infrastructure operations or hardware replacement.

> **Warning:** A Virtual Controller failover restarts SMB services, causing existing mapped shares to be temporarily unavailable. The exact reaction to such disconnections is dependent on the underlying application that is using the files shares.

To perform A Virtual Controller failover:

1. Navigate to the VPSA's dashboard.
2. On the VPSA's **Information** panel, click **Actions**.
3. From the dropdown, select **Failover**.
4. In the **Failover** dialog:
   1. **Advanced** options:

Option	Description
Advanced Scheduling	• **Immediate** Failover will take place immediately • **Scheduled** Failover will be done at the requested time, configurable from 30 minutes from the current time and up to 7 days

   2. Click **Failover** to confirm the **Failover** operation.

The failover Status and progress can be monitored in the VPSA log tab.

7.3.9 Moving a Virtual Controller

In cases where the cloud's Storage Node inventory and capacity are sufficient, Virtual Controllers can be moved from the SN the currently reside in to another. Both Primary and secondary Virtual Controllers can be moved. Moving the Primary Virtual Controller will trigger a failover operation prior to its relocation.

To move a Virtual Controller:

1. Navigate to the VPSA's dashboard.
2. On the VPSA's **Information** panel, click **Actions**.

3. From the dropdown, select **Move Virtual Controller**.
4. In the **Move Virtual Controller** dialog:
    1. Click the **Virtual Controller** to move.
    2. From the **Available Nodes** dropdown, select the destination Storage Node.

       The **Selected Storage nodes** column displays the selected Storage Nodes.
    3. Optionally, to select multiple destination Storage Nodes, select additional destination Storage Nodes rom the **Available Nodes** dropdown.

       The **Selected Storage nodes** column displays the selected Storage Nodes in the sequence they were selected.

       To change the order, drag the individual Storage Nodes up or down.

       ✔ **Note:** The destination Storage Nodes are scanned for sufficient resources according to their listed order. The Virtual Controller will be moved to the first destination Storage Node with sufficient resources.
    4. Click **Move** to confirm the **Move Virtual Controller** operation.

✔ **Note:** Virtual Controllers that belong to a VPSA instance older than version 20.01 cannot be spawned on Storage Nodes with ConnectX-5 NICs.

7.3.10 Hibernate a VPSA

VPSA hibernation takes the instance offline and releases its consumed resources (vCPU, RAM) on the Storage Nodes level. Hibernation of a VPSA also reduces its associated service cost, in that only drives are billed for VPSAs in a hibernated state. Hibernating a VPSA deletes its Virtual Controllers (the VPSA) while maintaining the data drives and all the necessary metadata to resume its operation at a later stage. Resuming a hibernated VPSA takes only a few minutes.

To hibernate a VPSA:

1. Navigate to the VPSA's dashboard.
2. On the VPSA's **Information** panel, click **Actions**.
3. From the dropdown, select **Hibernate**.
4. In the **Hibernate** dialog:
    1. In the text box, enter the word "**HIBERNATE**".
    2. Click **Hibernate** to confirm hibernating the VPSA.

       The VPSA Status changes to **Hibernated** when complete.

7.3.11 Creating VPSA Zsnap

A VPSA Zsnap is a snapshot of the VPSA at a point in time.

By taking periodic Zsnaps and identifying each Zsnap with a prefix, at a later date or time you can restore the VPSA back to its state as at the latest or a specific earlier Zsnap.

To trigger the manual creation of a Zsnap of the VPSA:

1. Navigate to the VPSA's dashboard.
2. On the VPSA's **Information** panel, click **Actions**.
3. From the dropdown menu, select **Create Zsnap**.
4. In the **Create Zsnap** dialog:
    1. Enter a prefix for the Zsnap.
    2. **Advanced** options:

Option	Description
Advanced Scheduling	• **Immediate** Zsnap creation will take place immediately • **Scheduled** Zsnap creation will be done at the requested time, configurable from 30 minutes from the current time and up to 7 days

    3. Click **Create Zsnap** to confirm creation of the Zsnap.

✔ **Note:** Zadara manages collection of Zsnaps and recovery from Zsnaps when relevant.

There is no need for customers to take Zsnaps, but can do so if requested by Zadara Support.

7.3.12 Purging or restoring a deleted VPSA

Any VPSA instance that has been deleted from the cloud will remain in the cloud's recycle bin for the period specified in it's settings. See **Recycle Bin** in VPSA Settings.

Cloud administrators can manually purge a deleted VPSA prior to the Recycle Bin retention period expiration, to free allocated cloud resources such as Physical Drives. Administrators can also restore an VPSA from the Recycle Bin and get it up and running on the same data set it contained when it was deleted.

7.3.13 Purging a deleted VPSA

To purge a VPSA from the cloud's Recycle Bin:

1. Navigate to the VPSA's dashboard.
2. On the VPSA's **Information** panel, make sure that the VPSA's Status is **Recycle Bin**.
3. On the VPSA's **Information** panel, click **Actions**.
4. From the dropdown menu, select **Purge**.

5. In the **Purge** dialog:
    1. In the text box, enter the VPSA ID.
    2. Click **Purge** to confirm purging the VPSA from the Recycle Bin.

7.3.14 Restoring a deleted VPSA

To restore a VPSA from the cloud's Recycle Bin:

1. Navigate to the VPSA's dashboard.
2. On the VPSA's **Information** panel, make sure that the VPSA's Status is **Recycle Bin**.
3. On the VPSA's **Information** panel, click **Actions**.
4. From the dropdown menu, select **Restore**.
5. In the **Restore** dialog, click **Restore** to confirm restoring the VPSA from the Recycle Bin.

    The VPSA Status changes to **Launching**. When the process completes and the VPSA is fully restored, the VPSA Status changes to **Normal**.

CHAPTER

EIGHT

OBJECT STORAGE

Command Center provides cloud administrators with centralized management capabilities for Zadara Cloud Object Storage environment. Cloud administrators can use Command Center for:

- Management operations on Object Storage instances
- Configuring Object Storage Availability Zones resource allocation
- Monitoring Object Storage capacity consumption trends

8.1 Viewing Object Storage Properties

To view a specific Object Storage:

1. Click **Object Storage** in Command Center's left menu panel.
2. In the **Instances** tab, click the Object Storage instance in the Object Storages grid.

8.1.1 Object Storage Instance Dashboard

The Object Storage instance's main **Dashboard** tab's **Information** panel provides information regarding the Object Storage's configuration, current health status and network topology.

Property	Description
Name	Object Storage instance's display name
Internal Name	Object Storage instance's internal name
User	User who created the instance
Company	Company of the user who created the instance
Description	Description given when the instance was provisioned
Nova ID	Object Storage instance's Nova ID
Status	Current status of the instance
Protection Zone	Instance Protection Zone configuration
IO Engine type	VC type for the Object Storage • **NGOS** type: – NextGen Object Storage • **ZIOS** types: Scope: VPSA Object Storage – Mini – Standard – Premium – Premium Plus
VCPUs	VCPUs per VC type (Proxy+Storage/Proxy) for this instance
RAM	RAM per VC type (Proxy+Storage/Proxy) for this instance
SSL Termination	Indicates whether SSL termination is internal or external
Storage VCs	Instance Storage VC count
Proxy VCs	Instance Proxy VC count
IP Address	Instance floating frontend IP address
Public IP	Instance public IP address
Mgmt. Address	Instance hostname for management access
Load Balancer	Instance Load Balancer type: Basic (Internal Load Balancer)
Image	Instance deployment image
UUID	Instance UUID
SNMPv3 Engine ID	Instance SNMPv3 Engine ID
Created	Instance creation timestamp
Updated	Instance last update timestamp

8.2 Managing Object Storage Availability Zones

Object Storage Availability Zones are required to support the various protection policies used in the cloud. By default there are four Availability Zones defined in each cloud to which Storage Nodes can be allocated.

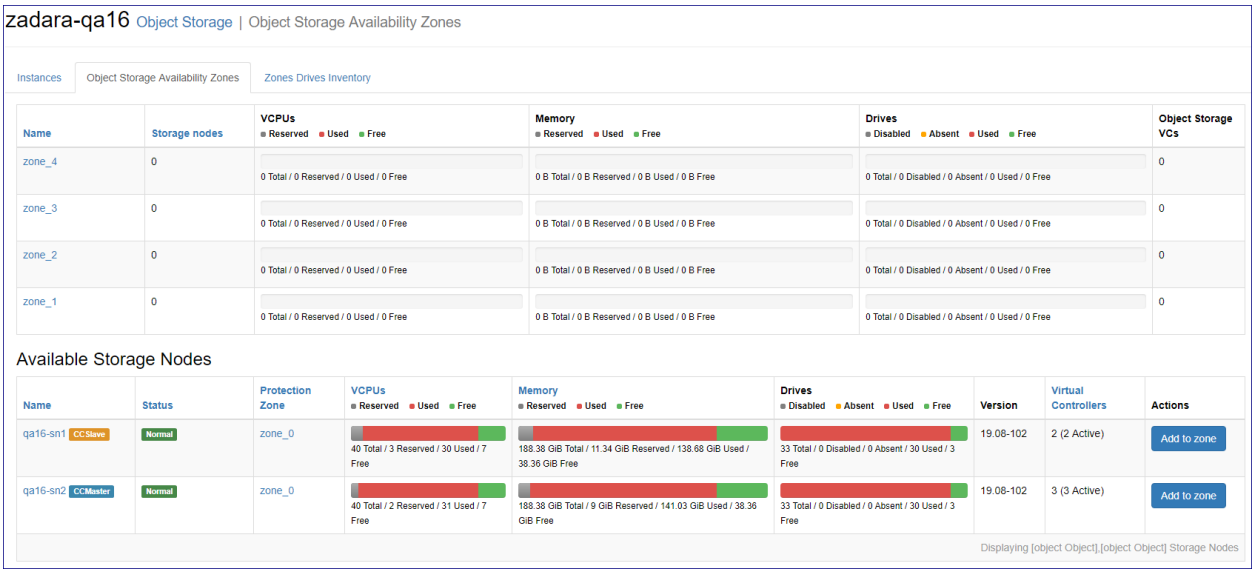
The cloud administrator's ability to define specific Object Storage protection policies is dependent on the Storage Node to Availability Zones allocation scheme.

Protection Policy	Number of Fault Domains (FD)
2-way mirroring	2
4+2 erasure coding	3

8.2.1 Assigning and removing Storage Nodes to Object Storage Availability Zones

To view the current Object Storage Availability Zones configuration:

select the Object Storage tab and then on the following screen select the Object Storage Availability Zones tab. The Object Storage Availability Zones tab presents the current resource allocation scheme and amount of resources (VCPUs , Memory and Drives) is Allocated , Utilized or free in each availability Zone. On the lower part of the screen a list of available Storage Nodes and their resources inventory is displayed.

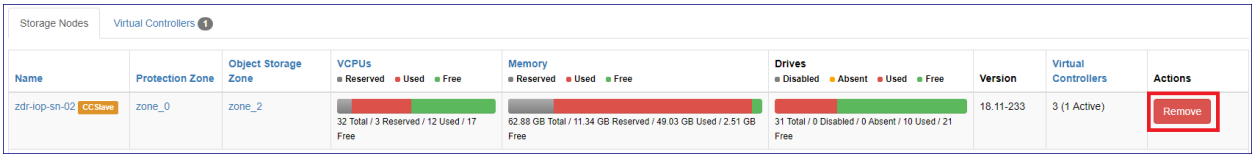


To allocate a Storage Node to an Availability Zone:

- Select a Storage Node and click the appropriate `Add to zone` button on the right side of the screen
- On the popup dialog that appears select the required Availability Zone and click `add`
- The Availability Zone configuration will update to reflect the required changes.

To remove a Storage Node from an Availability Zone:

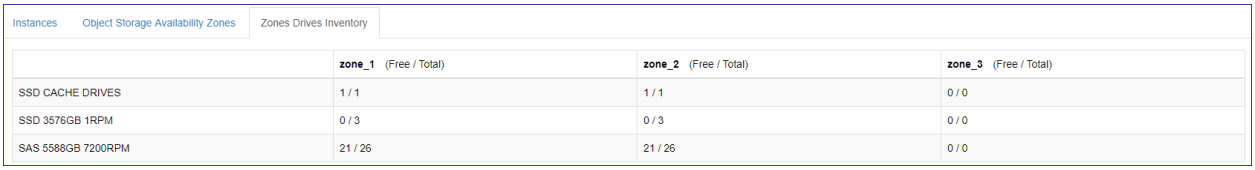
- Click on required Availability Zone
- On the Storage Nodes tab locate the node you wish to remove and click the `Remove` button



- On the following popup dialog confirm the removal request
- The Availability Zone configuration will update to reflect the required changes.

8.2.2 Viewing Object Storage Availability Zones drive inventory

To view drive inventory click on the Zones Drives inventory tab, Inventory will be presented grouped by drive types.



8.3 Managing Object Storage Instances

Object Storage instance management options are available from the **Actions** dropdown menu in the **Information** panel on the Object Storage's **Dashboard** tab:

- Adding Drives to an Object Storage
- Adding a Proxy Virtual Controller
- Changing a VPSA Object Storage engine type VPSA Object Storage
- Upgrading an Object Storage
- Maintenance mode
- Assigning or Unassigning a Public IP address to an Object Storage
- Creating an Object Storage Zsnap
- Adding or releasing an Object Storage's Virtual Network
- Enable Elastic Load Balancer for a VPSA Object Storage VPSA Object Storage

8.3.1 Adding Drives to an Object Storage

To add drives to an Object Storage:

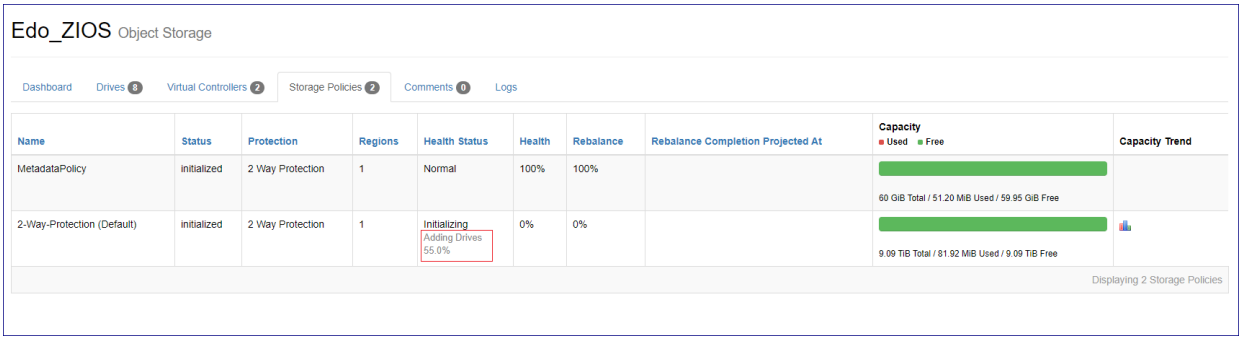
1. Click **Object Storage** in Command Center's left menu panel.
2. In the **Instances** tab, click the Object Storage instance in the Object Storages grid.
3. In the Object Storage's **Dashboard** tab, on the Object Storage's **Information** panel, click **Actions**.
4. From the dropdown, select **Add Drives**.
5. In the **Add Drives** dialog, select the relevant values from each parameter's dropdown:
    1. **Policy Name**
    2. **Drive Type**
    3. **Quantity**
6. Click **Add Drives** to confirm the operation.

✔ **Note:**

- When adding drives to an Object Storage, Virtual Controllers can also be added automatically, depending on the drive to VC ratio

- Virtual Controllers that belong to an Object Storage instance older than version 20.01 cannot be spawned on Storage Nodes with ConnectX-5 NICs.
- To avoid any performance impact, the drive addition process is performed gradually. VPSA Object Storage

The drive addition progress can be monitored in the **Health Status** column of the Object Storage's **Storage Policies** tab in Command Center.



8.3.2 Adding a Proxy Virtual Controller

To add a Proxy Virtual Controller to an Object Storage:

1. Click **Object Storage** in Command Center's left menu panel.
2. In the **Instances** tab, click the Object Storage instance in the Object Storages grid.
3. In the Object Storage's **Dashboard** tab, on the Object Storage's **Information** panel, click **Actions**.
4. From the dropdown, select **Add Proxy VCs**.
5. In the **Add Proxy Virtual Controller** dialog, click **Add Proxy Virtual Controller** to confirm the operation.

   On completion, the **Proxy VCs** count on the Object Storage's **Information** panel is incremented.

8.3.3 Changing a VPSA Object Storage engine type

Scope: VPSA Object Storage

When creating a VPSA Object Storage with 4 disk drives or less, the VPSA Object Storage's engine type is set to **Mini**. The **Mini** engine type is a lesser footprint engine compared to the full **Standard** VPSA Object Storage virtual controller, designed to support up to 12 disk drives.

VPSA Object Storage **Mini** virtual controllers can be manually converted to the full **Standard** footprint in Command Center.

✔ **Note:** When more than 4 disk drives are provisioned to a VPSA Object Storage engine, it will be automatically be upgraded.

To change a VPSA Object Storage's engine type:

1. Click **Object Storage** in Command Center's left menu panel.
2. In the **Instances** tab, click the Object Storage instance in the Object Storages grid.
3. In the Object Storage's **Dashboard** tab, on the Object Storage's **Information** panel, click **Actions**.
4. From the dropdown, select **Change Engine Type**.

5. In the **Change Engine** dialog, click **Change engine** to confirm the **Change Engine Type** operation.

   On completion, on the VPSA Object Storage's **Information** panel, the **IO Engine Type** changes to **Standard**.

8.3.4 Upgrading an Object Storage

Command Center allows administrators to perform a version upgrade on the Object Storage instances running in the cloud.

To upgrade an Object Storage's version:

1. Click **Object Storage** in Command Center's left menu panel.
2. In the **Instances** tab, click the Object Storage instance in the Object Storages grid.
3. In the Object Storage's **Dashboard** tab, on the Object Storage's **Information** panel, click **Actions**.
4. From the dropdown, select **Upgrade**.
5. In the **Upgrade Object Storage** dialog:
   1. From the dropdown, select the Object Storage image version for the upgrade.
   2. **Advanced** options:

      Version Validation: By default, the upgrade process includes version validation. To skip the validation, mark the checkbox.
   3. Click **Upgrade**.
   4. In the **Confirm Upgrade** dialog, click **Upgrade** to confirm the **Upgrade Object Storage version** operation.

      The Object Storage's Status changes to **Upgrading version** for the duration of the process, and then to **Normal** when complete.

✔ **Note:** From cloud version 20.12:

- An Object Storage upgrade to a version which is more then 2 major releases higher than the current version will be blocked by Command Center.
- An Object Storage version downgrade will be blocked by Command Center.

8.3.5 Maintenance mode

Maintenance mode is useful for protecting an Object Storage against any data integrity issue when a planned cloud physical maintenance is scheduled.

While in maintenance mode, all Object Storage services are stopped and the Object Storage's management console is not accessible. The instance is offline and its consumed resources (vCPU, RAM) are freed at the Storage Node level.

Maintenance mode involves the process of deleting an Object Storage's Virtual Controllers, while maintaining the data drives and all the necessary metadata to resume its operation at a later stage.

Taking an Object Storage out of maintenance mode and resuming its operation takes only a few minutes.

To transit an Object Storage to maintenance mode:

1. Click **Object Storage** in Command Center's left menu panel.
2. In the **Instances** tab, click the Object Storage instance in the Object Storages grid.
3. In the Object Storage's **Dashboard** tab, on the Object Storage's **Information** panel, click **Actions**.

4. From the dropdown, select **Maintenance Mode**.
5. In the **Enter Maintenance Mode** dialog:
    1. In the text box, enter the Object Storage ID.
    2. Click **Maintenance** to confirm the **Enter Maintenance Mode** operation.

8.3.6 Assigning or Unassigning a Public IP address to an Object Storage

In specific cases where an Object Storage requires public internet connectivity, a public IP address can be assigned to it.

See Public IP Addresses for information about configuration of cloud-level public IP ranges.

Assigning a Public IP address

To assign a Public IP address:

1. Click **Object Storage** in Command Center's left menu panel.
2. In the **Instances** tab, click the Object Storage instance in the Object Storages grid.
3. In the Object Storage's **Dashboard** tab, on the Object Storage's **Information** panel, click **Actions**.
4. From the dropdown, select **Assign Public IP**.
5. In the **Assign Public IP** dialog:
    1. Select one of the options:
        - **Automatic IP address assignment**
        - **Manual IP address assignment**

          Select an IP from the dropdown that displays for the manual IP assignment option.

    ✔ **Note:**

    - Manual public IP assignment is only available for VPSA Object Storage instances from version 20.01 and later
    - Public IP is not supported for Object Storage instances with IPV6 frontend addresses

    ---

    2. Click **Assign** to confirm the **Assign Public IP** operation.

Unassigning a Public IP address

To unassign a Public IP address:

1. Click **Object Storage** in Command Center's left menu panel.
2. In the **Instances** tab, click the Object Storage instance in the Object Storages grid.
3. In the Object Storage's **Dashboard** tab, on the Object Storage's **Information** panel, click **Actions**.
4. From the dropdown, select **Unassign Public IP**.
5. In the **Unassign Public IP** dialog, click **Confirm** to confirm the **Unassign Public IP** operation.

8.3.7 Creating an Object Storage Zsnap

An Object Storage Zsnap is a snapshot of the Object Storage at a point in time.

An Object Storage Zsnap is a collection of logs and system meta-data information used for troubleshooting and analysis of the component's health.

To trigger the manual creation of a Zsnap of the Object Storage:

1. Click **Object Storage** in Command Center's left menu panel.
2. In the **Instances** tab, click the Object Storage instance in the Object Storages grid.
3. In the Object Storage's **Dashboard** tab, on the Object Storage's **Information** panel, click **Actions**.
4. From the dropdown menu, select **Create Zsnap**.
5. In the **Create Zsnap** dialog:
    1. Enter a prefix for the Zsnap.
    2. To include the Object Storage's metering data in the Zsnap, mark the **Collect Metered Data** checkbox.
    3. Click **Create Zsnap** to confirm creation of the Zsnap.

✔ **Note:** Zadara manages collection of Zsnaps and recovery from Zsnaps when relevant.

There is no need for customers to take Zsnaps, but can do so if requested by Zadara Support.

Customers cannot perform any restore operations.

8.3.8 Adding or releasing an Object Storage's Virtual Network

Object Storages connected to multiple networks can be used to enable use cases where multiple networks require connectivity to the same Object Storage.

✔ **Note:**

- An Object Storage is limited to a maximum of 10 Virtual Networks.
- The Object Storage REST API and UI are accessible through any Virtual Networks.
- An Object Storage can't have two Virtual Networks with the same VLAN.

See Performing Cloud Networking Management for viewing, creating and deleting the cloud's Virtual Networks.

Adding a Virtual Network to an Object Storage

To assign a Virtual Network to an Object Storage:

1. Verify that an appropriate Virtual Network is already defined in the cloud, excluding the Virtual Network already in use by the Object Storage.
2. Click **Object Storage** in Command Center's left menu panel.
3. In the **Instances** tab, click the Object Storage instance in the Object Storages grid.
4. In the Object Storage's **Dashboard** tab, on the Object Storage's **Information** panel, click **Actions**.
5. From the dropdown, select **Add Virtual Network**.

6. In the **Add Virtual Network** dialog:
    1. Select the Virtual Network to assign to the Object Storage.
    2. Click **Add** to confirm adding the Virtual Network to the Object Storage.

       On completion, the newly added Virtual Network displays in the Object Storage's **Virtual Network** tab.

Releasing a Virtual Network from an Object Storage

To release a Virtual Network from an Object Storage:

1. Click **Object Storage** in Command Center's left menu panel.
2. In the **Instances** tab, click the Object Storage instance in the Object Storages grid.
3. In the Object Storage's **Dashboard** tab, on the Object Storage's **Information** panel, click **Actions**.
4. From the dropdown, select **Release Virtual Network**.
5. In the **Release Virtual Network** dialog:
    1. Select the Virtual Network to release from the Object Storage.
    2. Click **Release**.

       The **Confirm Release Virtual Network** dialog opens, displaying a warning that the Object Storage will no longer be accessible via the selected Virtual Network.

       Click **Release** to reconfirm releasing the Virtual Network from the Object Storage.

       On completion, the released Virtual Network no longer appears in the Object Storage's **Virtual Network** tab.

8.3.9 Enable Elastic Load Balancer for a VPSA Object Storage

Scope: VPSA Object Storage

To enable an Elastic Load Balancer for a VPSA Object Storage:

1. Click **Object Storage** in Command Center's left menu panel.
2. In the **Instances** tab, click the VPSA Object Storage instance in the Object Storages grid.
3. In the VPSA Object Storage's **Dashboard** tab, on the VPSA Object Storage's **Information** panel, click **Actions**.
4. From the dropdown, select **Enable Elastic Load Balancer**.
5. In the **Enable Elastic Load Balancer** dialog, click **Confirm** to confirm the **Enable Elastic Load Balancer** operation.

   On completion, on the VPSA Object Storage's **Information** panel, the **Load Balancer** changes to **Elastic**.

CHAPTER

NINE

ENGINES

Command Center allows cloud administrators to view all storage instance specifications available for deployment on the cloud.

To view VPSA engine properties:

1. Click **Engines** in Command Center's left menu panel.
2. Click the tabs to view properties per engine type:
    - VPSA IO engines properties
    - VPSA App engines properties
    - VPSA Composite engines properties

9.1 VPSA IO engines properties

The **IO** tab displays the following properties per IO engine:

Property	Description
Name	IO Engine Name
Internal Type	Internal type used by Nova for this engine
Memory	**Single virtual controller** RAM requirement for this IO engine
VCPU	**Single virtual controller** VCPUs requirement for this IO engine
VPSAs / Object Storage	Count of VPSAs with this engine type, in this cloud

9.2 VPSA App engines properties

The **App** tab displays the following properties per App engine:

Property	Description
Name	APP Engine Name
Internal Type	Internal type used by Nova for this engine
Memory	RAM requirement for this APP engine
VCPU	VCPUs requirement for this APP engine
VPSAs / Object Storage	Count of VPSAs with this engine type, in this cloud

9.3 VPSA Composite engines properties

The **Composite** tab displays the following properties per Composite engine:

Property	Description
Category	Composite engine type
Controller Instance Type	Link to the image used for composite controller instances. Click the sub-instance image link to display its properties: • **Name**: Composite sub-instance engine name • **Internal Type**: Internal type used by Nova for this engine • **Memory**: RAM requirement for this sub-instance engine • **VCPU**: VCPUs requirement for this sub-instance engine
Data Policy Partition Power	Swift partition power used for data policies for this composite engine type
Dedicated Controller Vcs	Count of dedicated controller VCs deployed for this composite engine type
Enable ZELB On Object Storage Creation	Whether Zadara Extend load balancing is enabled on VPSA creation
Enforce Drive Add With VC Set	Whether disk drives are automatically added when the VPSA is expanded by an additional VC set
Max Capacity In TiB	Maximum storage capacity supported by this composite engine type
Max Drives Per Proxy Storage VC	Maximum disk drives that can be added to a proxy storage virtual controller
Metadata Partition Size In GiB	Size in gigabytes of each Metadata partition
Metadata Partitions Per Proxystorage VC	Metadata partitions allocated for each proxy storage virtual controller
Metadata Policy Partition Power	Swift partition power used for metadata policies for this composite engine type
Minimum VC Sets for Object Storage Creation	Minimum footprint in terms of virtual controller sets for this composite engine type
Name	Composite engine instance type name
Proxy Instance Type	Link to the image used for composite proxy instances Click the sub-instance image link to display its properties: • **Name**: Composite sub-instance engine name • **Internal Type**: Internal type used by Nova for this engine • **Memory**: RAM requirement for this sub-instance engine • **VCPU**: VCPUs requirement for this sub-instance engine
Proxy Storage Instance Type	Link to the image used for composite storage proxy instances Click the sub-instance image link to display its properties: • **Name**: Composite sub-instance engine name • **Internal Type**: Internal type used by Nova for this engine • **Memory**: RAM requirement for this sub-instance engine • **VCPU**: VCPUs requirement for this sub-instance engine
Setup Partition Size In GiB	Allocation size in gigabytes for the composite instance setup partition

CHAPTER

TEN

IMAGES

Using Command Center, administrators manage virtual machine images for:

- VPSA
- VPSA Object storage
- CCVM

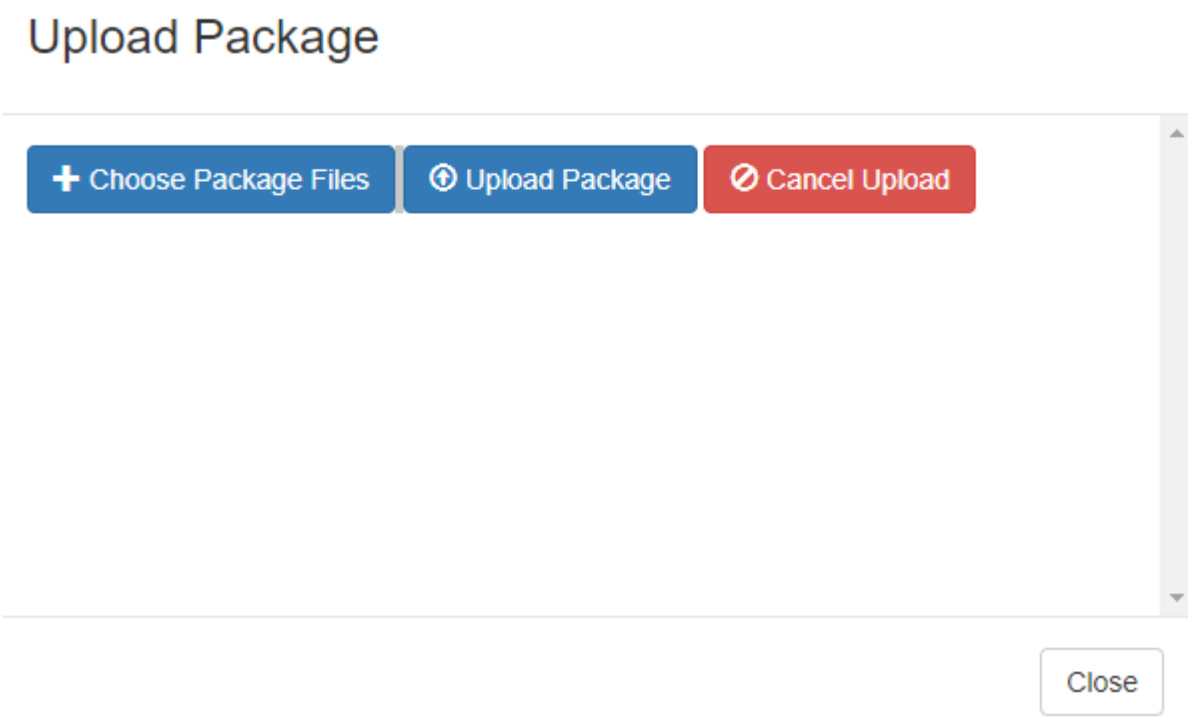
Cloud administrators can pull specific images from a repository and specify a set of images as default. Default images will be the ones deployed when a new VPSA instance is created.

10.1 Pulling Package And Registering Images

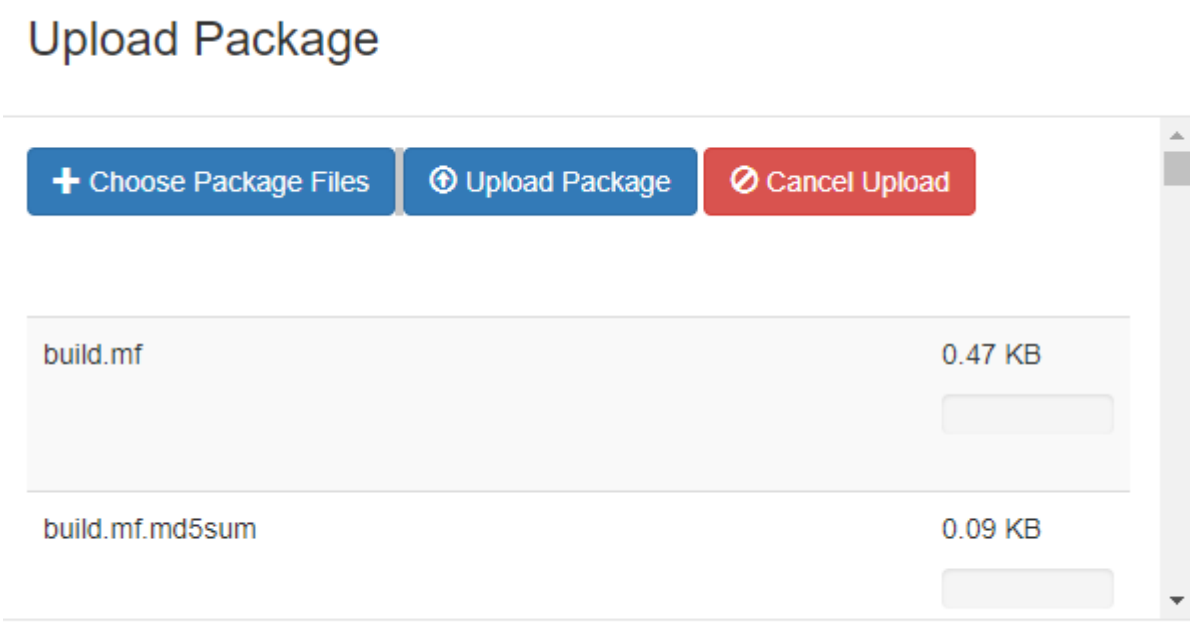
To make new virtual machine images available for cloud users, image packages must be pulled from Zadara repository and the images registered. To pull image packages from the Zadara repository click on the gear icon on the top right of the screen and select `manage cloud packages` from the drop down menu. Make sure that your repository location is set to default(as shown below) or to a valid location accssible via the S3 protocol and containing the relevant image packages. A list of available image packages should appear. You can regenerate the list of packages available in the repository by clicking the refresh icon next to the screen title.

✔ **Note:** Zadara storage public image repository is: s3://zadarastorage-install/ and it is set as the default Command Center repository.

Packages can also be uploaded from local storage, if a package repository is not available or reachable from the cloud. To upload a package from local storage click on the `Upload Package` button. On the popup window that will appear, click on `Choose Package File` and use the file-grid to navigate into a folder containing cloud package files and select all of them.



A list of the selected files will be populated in the popup window. To begin uploading the package click on `Upload Package`.



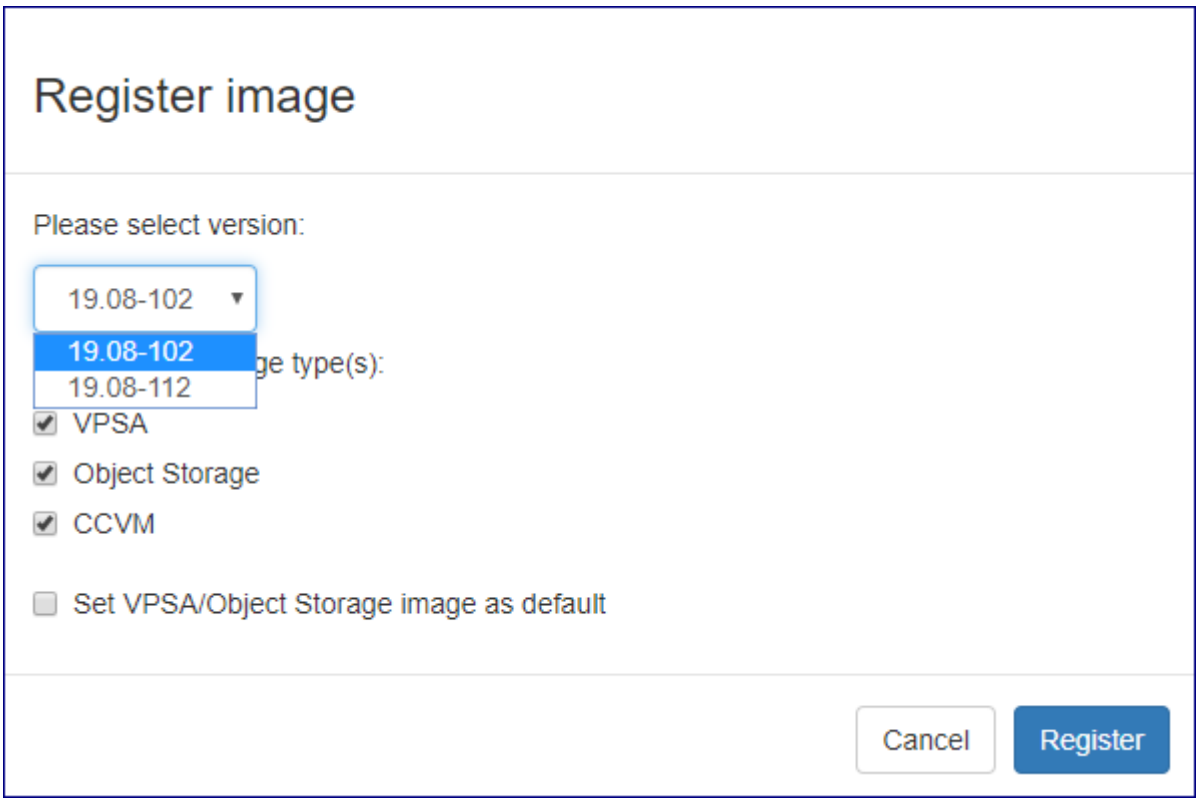
The upload progress is tracked on a file level progress bar. When the file upload and registration process are finished, the package will be added to the available packages grid.

To download a specific package, locate it on the package list. Make sure its status is Available for download and click the `Download` button.

Downloaded packages can be erased from local storage once they are no longer required. To erase a package click on the `erase` button for the image and confirm the package deletion in the popup window that will appear.

To register mages from the downloaded package go to the Command Center Images tab and click on the `Register image from local repository` button. In the popup dialog that will appear, wait for the package version list to load and select the specific version from which you would like to register the images. Select the Images you would like to register (VPSA, Object storage or CCVM) and weather you would like to set them as the default image for new VPSA deployments and click the `Register` button to confirm the operation.

✔ **Note:** You can set a specific image as default at any time by clicking the downward arrow button for the specific image and select Set default from the drop down menu.



A registered image can be later deleted by clicking the downward arrow button for the specific image and select Delete from the drop down menu.

CHAPTER

ELEVEN

MANAGING CLOUD NETWORKING

11.1 Background

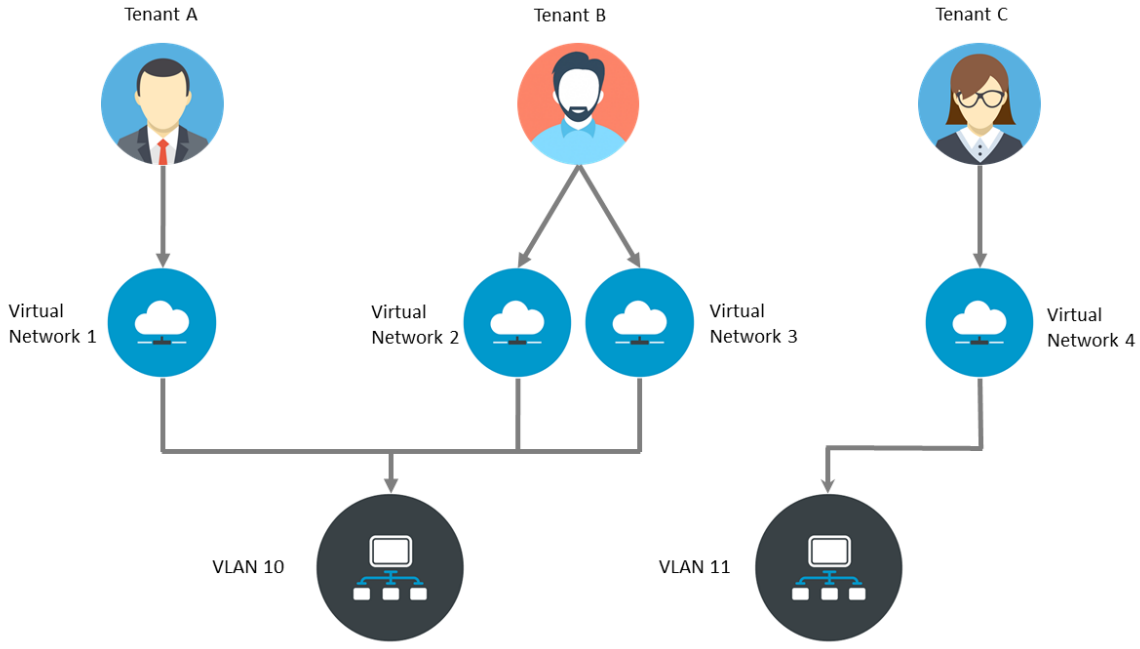
The Zadara cloud is a flexible storage cloud supporting multiple topologies, a vast range of use cases and cloud hosted environments. Due to the Zadara cloud flexibility it requires a flexible and dynamic virtual networking infrastructure that can be tailored to meet any customer demand and configuration while also enabling Zadara's managed services architecture.

The Zadara cloud networking architecture enables allocation of virtual networks to Cloud tenants (which are a representation of a cloud user and a referring provider) and interconnecting between virtual networks and networks external to the Zadara cloud using technologies such as IP routing and 802.1q VLAN tagging.

There are 2 distinct virtual networking elements managed within the Zadara Cloud:

- Virtual Local area networks(VLANs): Supported VLAN ID range per for the Zadara cloud is specified at installation. Specific VLAN IDs can be allocated to one or more cloud tenants.
- Virtual networks : Defines a set of available IP addresses within a specific network segment. Virtual networks are allocated for a specific cloud tenant and within a specific VLAN.

The below diagram depicts the relationship between cloud tenants, virtual networks and VLANs:

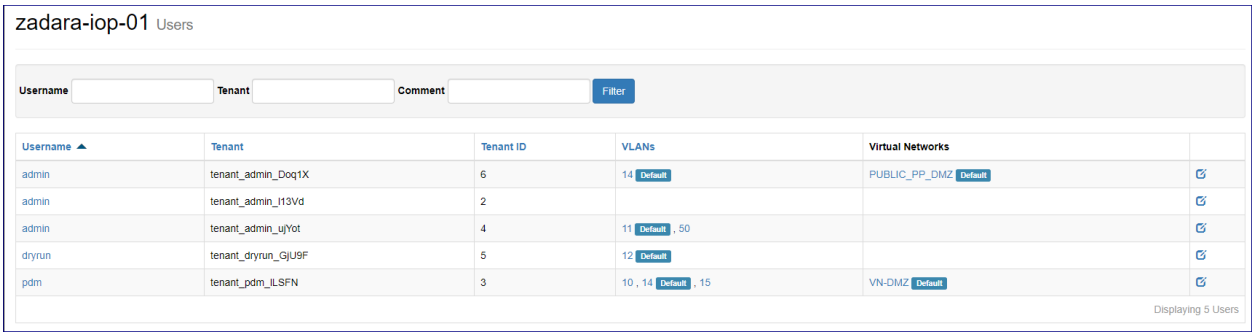


Command center provides a single point of management in which cloud administrator can define virtual networking configuration allocate networking resources to tenants.

11.2 Performing Cloud Networking Management

Viewing tenant configuration

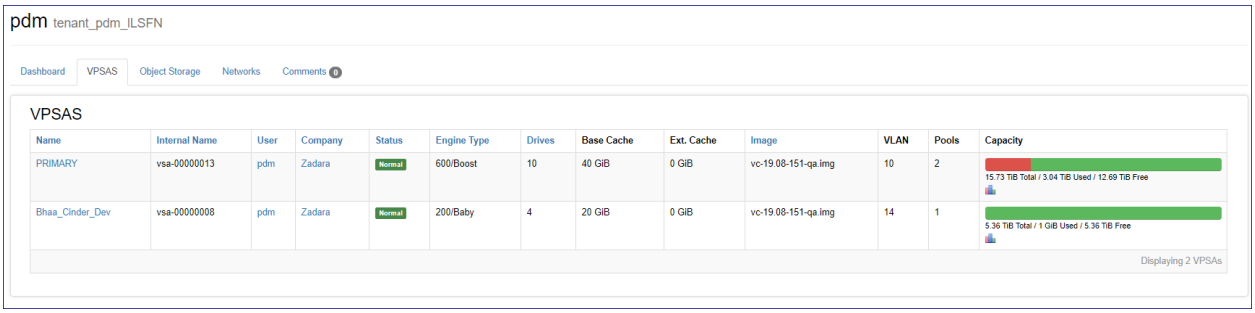
To view configuration for a specific Tenants from Command center click on Users/Tenants on the right menu pane.



The tenants dialog provides basic configuration details for all tenants defined in the cloud. The main tenant table display the following details:

- Cloud user name
- Cloud tenant name
- Tenant id
- VLANs which have allocation per each tenant
- Virtual networks defined in each tenant

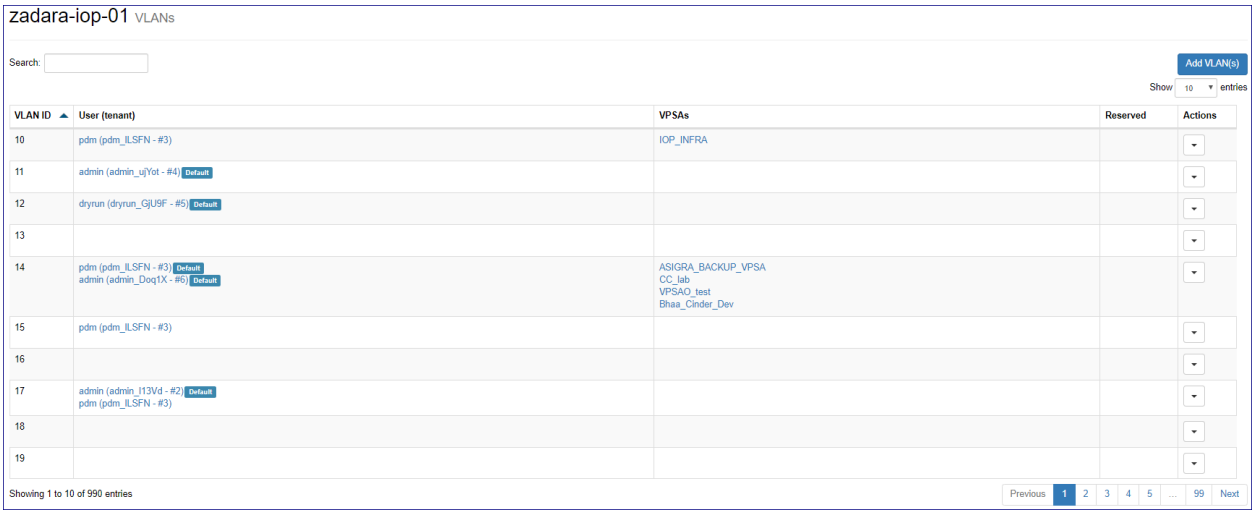
Clicking on a specific tenant record displays a drilled down view of the tenants configuration and allocated assets such as VPSA/VPSA Object storage instances and allocated virtual network details.



11.3 VLANs

Viewing VLAN configuration

To view VLAN configuration from Command center click on VLANs from the right menu pane.



The VLAN configuration screen displays a list of ALL VLAN IDs specified as the cloud available VLAN range while per VLANS that have been assigned to a specific tenant Tenant and allocated VPSA/VPSA Object storage information is also displayed.

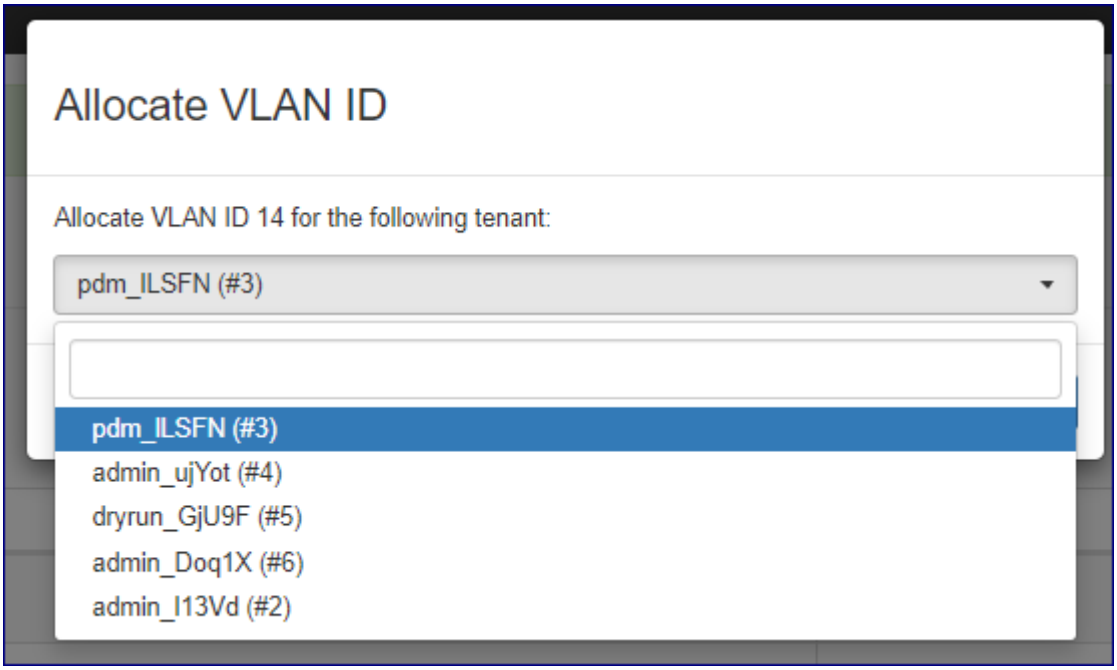
Expanding cloud addressable VLAN range

To add additional VLANS to the addressable range specified in the initial cloud configuration navigate the VLAN properties screen and click on the `Add VLAN(S)` button.

Specify an additional VLAN range that is not overlapping the currently defined range and click the `Add VLAN(S)` button the confirm expansion.

Assigning and unsinging VLANS

To assign a VLAN to a cloud tenant navigate the VLAN properties screen, locate the required VLAN id, click on its corresponding downward arrow button on the left side button and select Allocate.

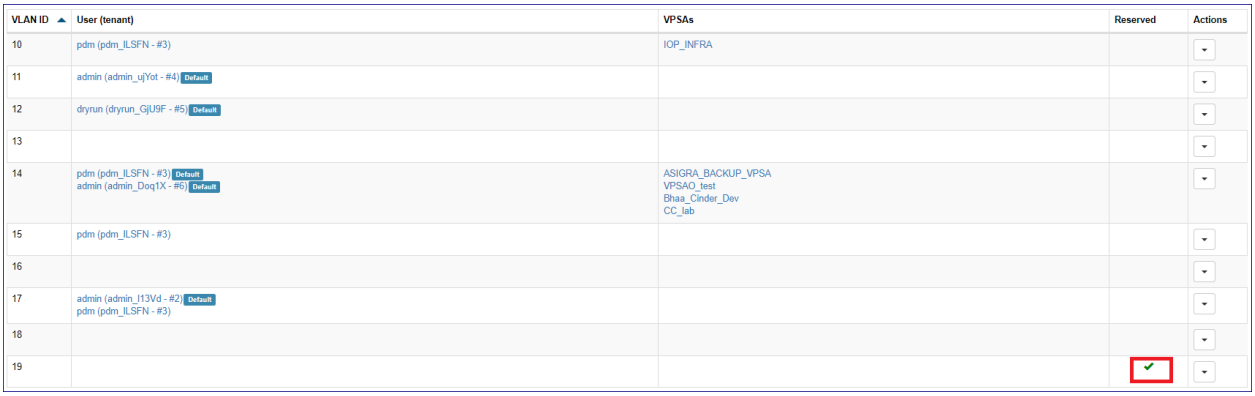


On the popup dialog that will appear select the tenant to which you would list to allocate this VLAN and click on the `Allocate` button to confirm.

To remove a VLAN from a cloud tenant navigate the VLAN properties screen, locate the required VLAN ID, click on its corresponding downward arrow button on the left side button and select Deallocate. On the popup dialog that will appear select the tenant to which you would list to allocate this VLAN and click on the `Deallocate` button to confirm.

Reserving VLANS

VLAN IDs can be reserved by command center to protect them from being allocated to tenants, reserved VLANs can be identified by a green check sign on the VLAN properties screen.



To reserve a VLAN ID navigate the VLAN properties screen, locate the required VLAN id, click on its corresponding downward arrow button on the left side button and select Reserve.

To release a VLAN ID from reservation navigate the VLAN properties screen, locate the required VLAN id, click on its corresponding downward arrow button on the left side button and select Unreserve.

Setting a VLAN as default

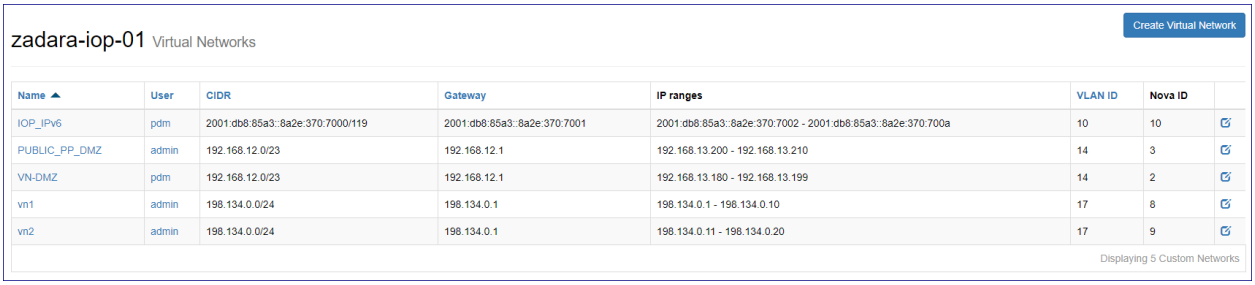
Per each tenant one VLAN can be set as its default VLAN, default VLAN is the one that will be allocated for newly created VPSA\VPSA Object storage instances. To set a VLAN as default navigate the VLAN properties screen, locate the required VLAN id, click on its corresponding downward arrow button on the left side button and select Set As default. On the popup

dialog that will appear select the tenant for which this VLAN will be set as default and click on the `Set as default` button to confirm the operation.

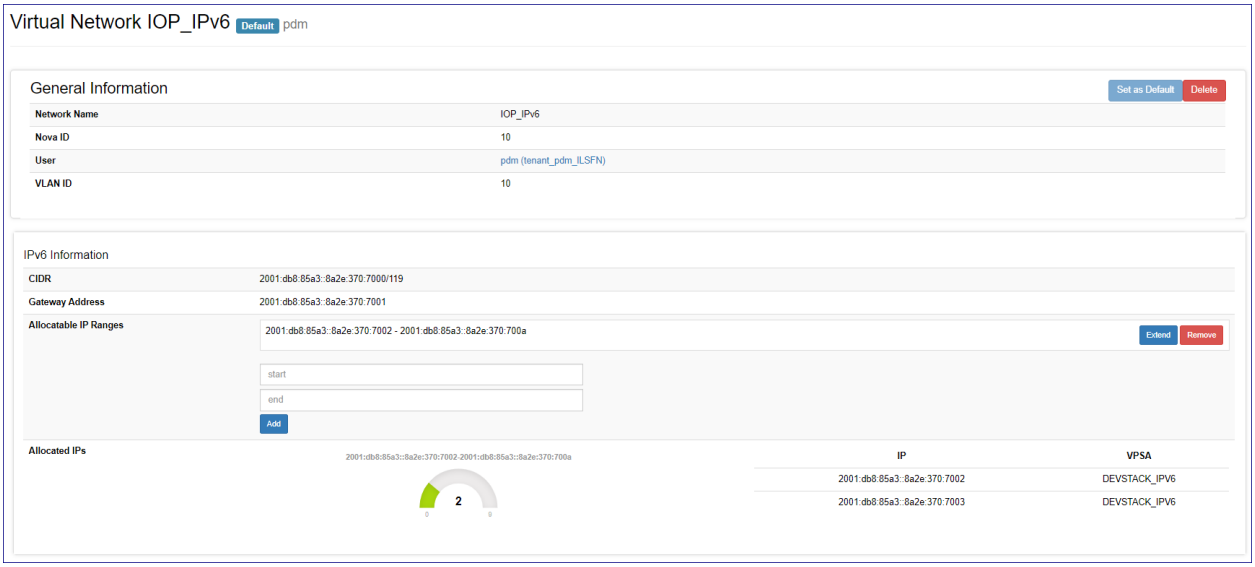
11.4 Virtual Networks

Viewing virtual networks configuration

To view the configuration of one or more virtual networks from Command center click on Virtual Networks on the right menu pane.



To drill down into a specific virtual network configuration click on its name.

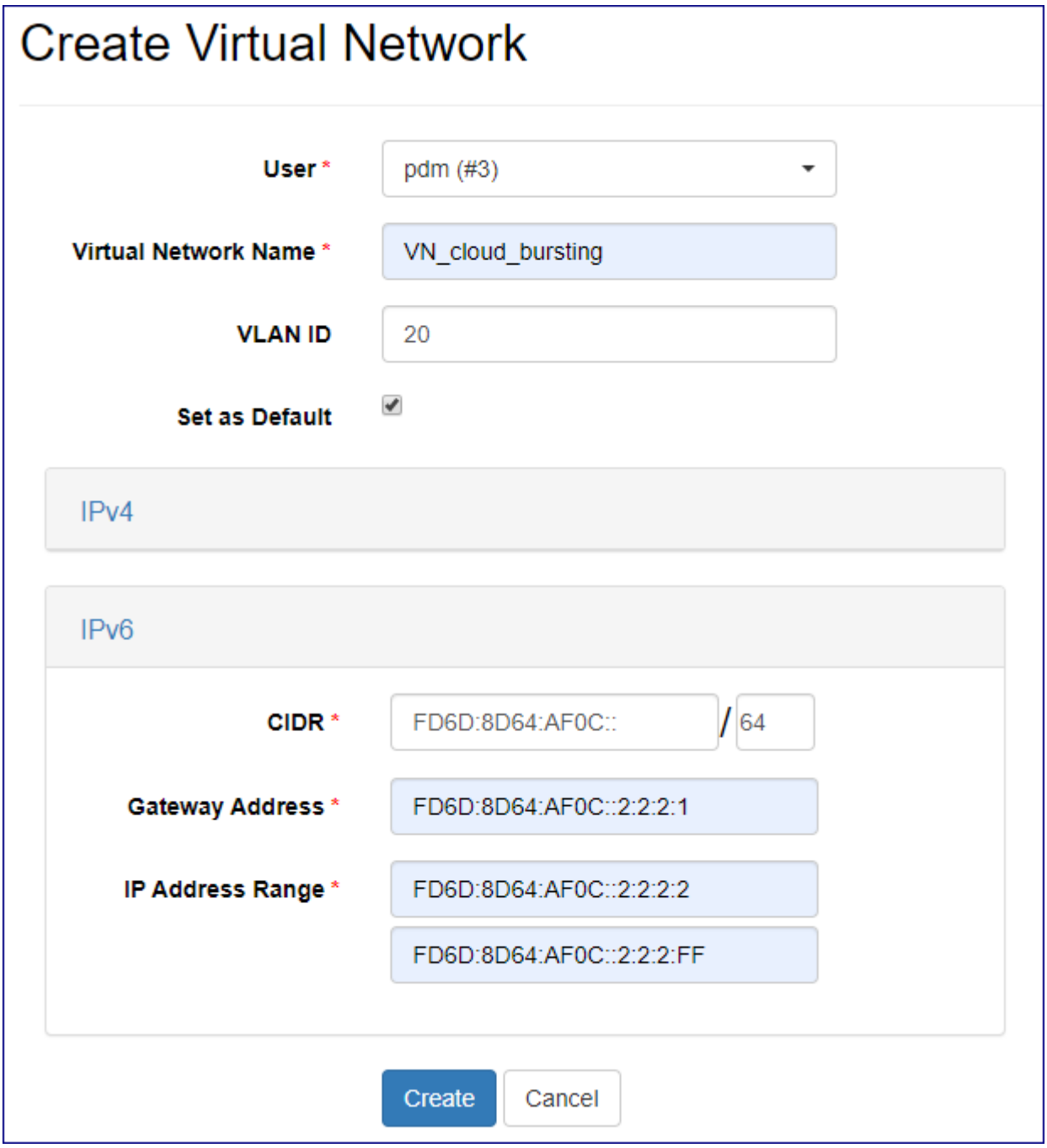


The virtual network configuration screens displays information on the network configuration such as:

- User and tenant to which this network is allocated
- Virtual Network internet protocol(IP) version (IPv4/IPv6)
- CIDR
- Default gateway
- Virtual network IP address range
- IP address allocation for VPSA and VPSA object storage entities

Creating a virtual network

To create a new virtual network from Command center click on Virtual Networks on the right menu pane and then click on the `Create Virtual Network` button.



On the virtual network creation dialog specify:

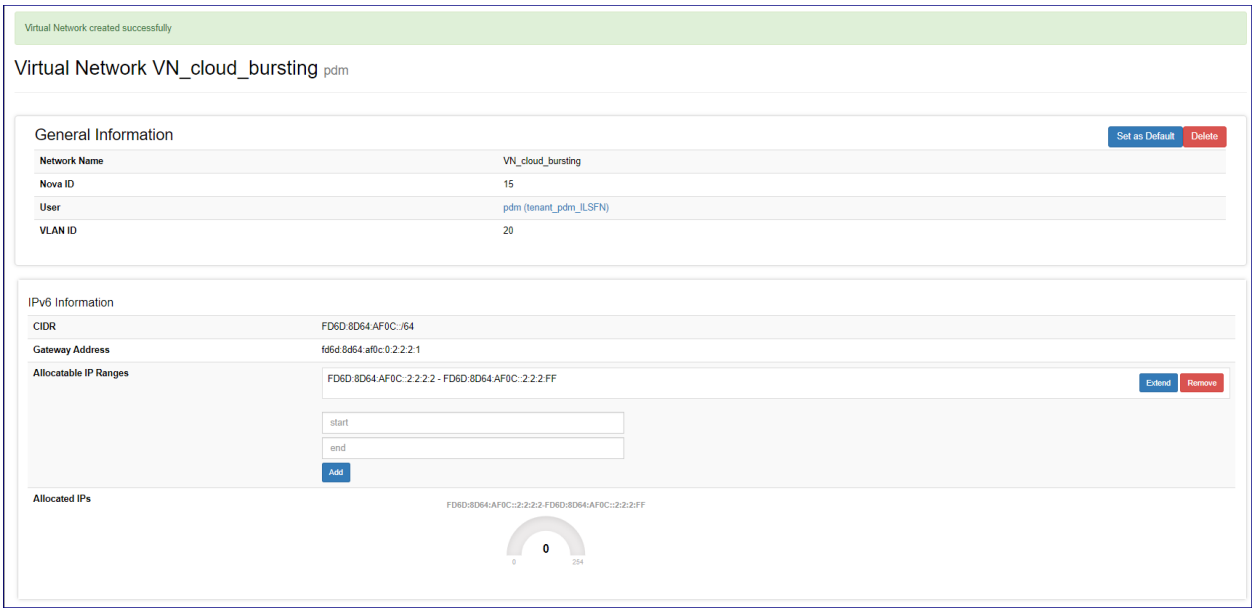
- The owning user name and tenant id (tenant id can be verified in the Users/Tenants screen).
- The new virtual network name
- Internet protocol(IP) version (define IPv4 or IPv6 Virtual Network)
- Network CIDR
- Default gateway
- IP address range allocated for this virtual network

- VLAN ID in which this virtual network will be allocated (if VLAN ID is left blank it will be automatically selected)
- Weather you would like to set this virtual network as the default network for this Tenant (each VPSA\VPSA object storage created by this tenant will attempt to allocate a front-end IP address from this virtual network).

Note:

When creating virtual networks on a multi-zone cloud you will be able to specificy a gateway address for each protection zone

Click on the `Create` button to confirm the virtual network creation



Note:

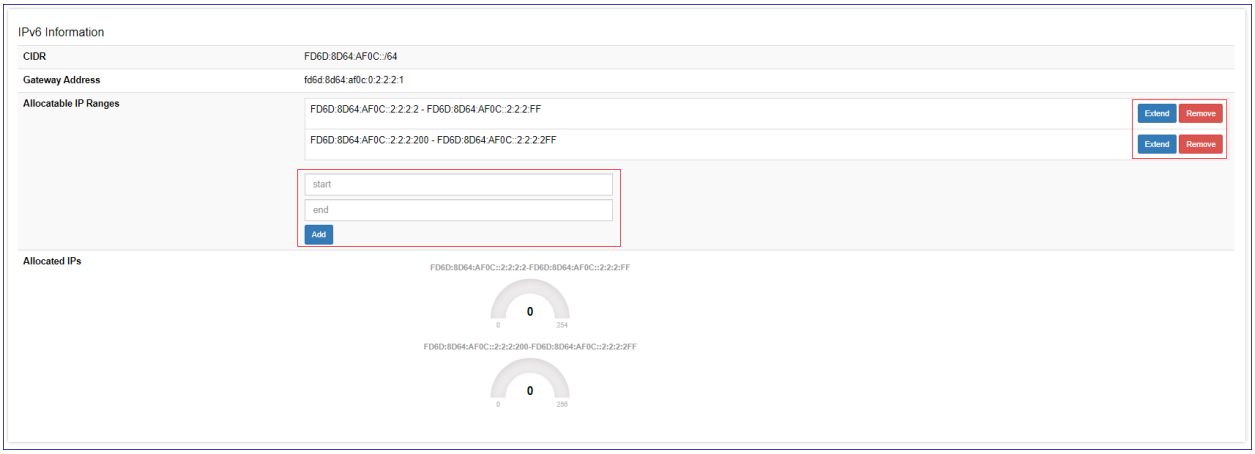
Multiple virtual networks can be defined in the same VLAN

Expanding/Shrinking a virtual network IP range

A virtual network IP range can be expanded in 2 ways:

- Addition of another IP range within the specified subnet.
- Expansion of an existing IP range with contiguous IP addresses.

To add a new IP address range : to go to the specific virtual network configuration screen, specify the new IP range in the Allocatable IP Ranges section and click on the `Add` button.



To extend an existing IP address range : click on the `Extend` button in the Allocatable IP Ranges section, specify the new upper limit for the virtual network IP range and click the `Extend` button.

To remove an existing IP address range from a virtual network : click on the `Remove` button in the Allocatable IP Ranges section, on the popup dialog that will appear click the `Confirm` button for removal confirmation.

Setting a virtual network as default

Per each tenant one Virtual network can be set as its default virtual network, default network is the one from which IP addresses will be allocated for newly created VPSA\VPSA Object storage instances. To set a virtual network as the default network to go to the specific virtual network configuration screen and click the `Set As default` button. the setting will be immediately applied and reflected in the virtual network\tenant configuration.

Deleting a virtual network

To delete a virtual network it must be unutilized(without any IP address allocations to VPSA/VPSA object storage instances). To perform deletion to go to the specific virtual network configuration screen and click the `Delete` button. On the popup dialog that will appear confirm deletion by clicking on the `Delete` button.

CHAPTER

TWELVE

PUBLIC IP ADDRESSES

By default, access to VPSA instances from the public Internet is not available, for security and privacy reasons.

The VPSA Front-End IP address is used for VPSA management via the UI and REST API. It is also used for data IO workload, where host connectivity is via iSCSI, NFS, and SMB protocols. The VPSA Front-End IP address is allocated on the Zadara Storage Cloud Front-End network. Only servers in the Cloud Servers network can reach this IP address. Servers outside this network cannot access it.

To enable access to VPSA instances from outside the cloud network, Public IP addresses are allocated in the Cloud management interface, and can be assigned to VPSA instances.

A typical use case requiring Public IP addresses is VPSA Asynchronous Remote Mirroring. This involves two VPSAs in different regions, or between on-premise and public cloud deployments, or even between different Cloud Providers for Disaster Recovery (DR). In these cases, communication between the VPSAs takes place via an authenticated and encrypted channel over the public Internet , thus requiring Public IPs.

Cloud admins can use Command Center to view, define, edit and delete public IP addresses, and to assign them to VPSA instances.

12.1 Adding Public IP Addresses

To define new Public IP Addresses:

1. Click **Public IPs** in Command Center's left menu panel.

   The Public IPs grid displays.

2. Click **New Public IP(s)** at the top right.

   The **New Public IP(s)** dialog opens.

   1. To configure the new IP range, enter the properties' values:

Property	Description
Label	Descriptor for the Public IPs
VLAN ID	A new or existing VLAN for this Public IP range that is different from the cloud tenant's VLANs
Gateway	Public IP network Gateway
Netmask	Public IP network subnet mask
Public IP Range	Range of external public IP addresses to be defined
IP Range	For NAT, enter the Corresponding internal IP range. Otherwise, enter the external range

   2. Click **Submit** to confirm the operation.

✔ **Note:** To assign Public IPs to VPSAs and Object Storages, see:

- Assigning or Unassigning a Public IP address to a VPSA
- Assigning or Unassigning a Public IP address to an Object Storage

12.2 Editing Public IP Addresses

To edit the configuration of a Public IP:

1. Click **Public IPs** in Command Center's left menu panel.

   The Public IPs grid displays.

2. Click the edit icon on the right of the IP to be edited.

   The **Edit Public IP** dialog opens.

   1. Update the relevant properties' values.
   2. Click **Submit** to confirm the operation.

12.3 Deleting Public IP Addresses

To delete the configuration of a Public IP:

1. Click **Public IPs** in Command Center's left menu panel.

   The Public IPs grid displays.

2. Click the edit icon on the right of the IP to be edited.

   The **Edit Public IP** dialog opens.

   1. At the top right, click **Delete**.
   2. Confirm the deletion operation.

CHAPTER

THIRTEEN

OUTNET

Outnet is an optional dedicated cloud-level network, that enables outbound connectivity to external networks. Outnet allows storage resources to interact with remote services, such as cloud storage, without requiring direct exposure to the public internet.

Unlike public networking setups that support both inbound and outbound traffic, Outnet is designed for outbound communication only. External sources can't use a VPSA or Object Storage's Outnet address to access them directly.

Outnet's underpinning principles and benefits:

- **Network Address Translation (NAT)**

  VPSA resources use a private internal IP range. When connecting to external endpoints, Outnet performs Network Address Translation (NAT), translating internal VPSA IPs to a routable external address.

- **Routing and firewall rules**

  Outnet ensures that only approved outbound connections are allowed.

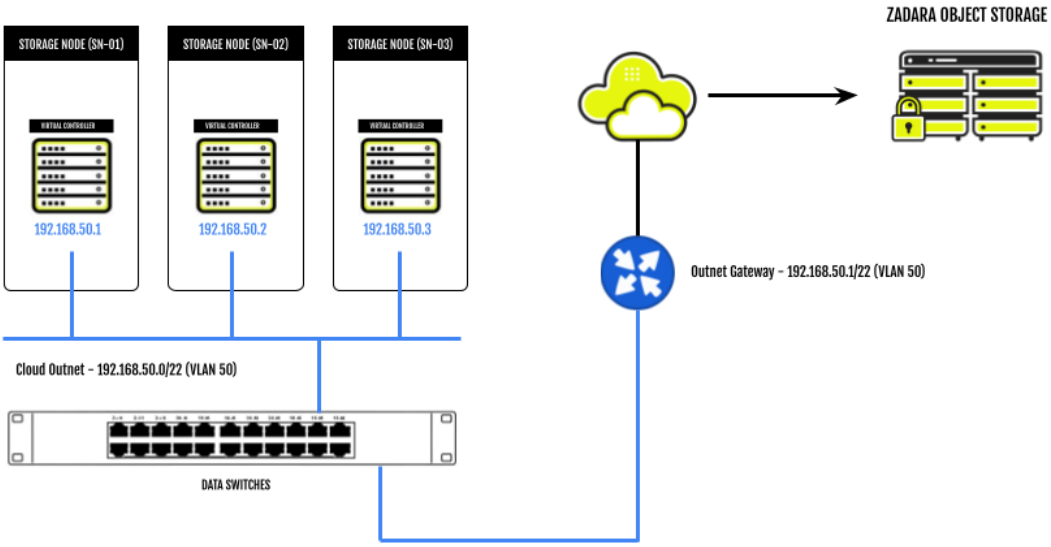
- **Security and access control**

  Outnet restricts traffic to prevent unauthorized access.

13.1 Data flow through Outnet

The most common use case for Outnet is to enable the B2OS VPSA service to back up to Object Storage in a different location, whether public or private.

The diagram below shows the data flow in an example configuration, where the VPSA is located at a local site and the Object Storage is located at a public site.



1. A VPSA service initiates an outbound request to an external IP, for example, Backup to Object Storage (B2OS).
2. The request is routed through the Outnet gateway, where NAT translates the private IP to an external one.
3. The request reaches the external service.
4. The external service sends a response back, which is allowed only if it is part of an active session initiated by the VPSA.
5. The response is NAT-translated back to the VPSA's private IP, ensuring data returns to the correct source.

13.2 Outnet Implementation

Outnet is a cloud-level network, and its implementation requires the involvement of Zadara Support.

After Outnet is configured for a cloud, all VPSAs and Object Storages hosted in the cloud will be allocated an Outnet network IP. Outnet doesn't affect the normal operation of the VPSA or Object Storage.

13.2.1 Prerequisites

To enable an Outnet configuration, customers must provide the following details:

- RFC1918 Network Subnet - It is possible to allocate a subset of IPs from a given subnet. Each VC will be allocated an IP from this pool. We recommend aligning to the FE/BE network subnet size (default /22).
- A unique VLAN (in the range of 10-4090), that will be defined on Zadara's data switches
- A gateway IP in the same network subnet range provided above

Although Outnet is designed as an internet-facing network, you can also use it to create a backup network between sites that don't have internet connectivity.

13.3 Viewing the Outnet configuration

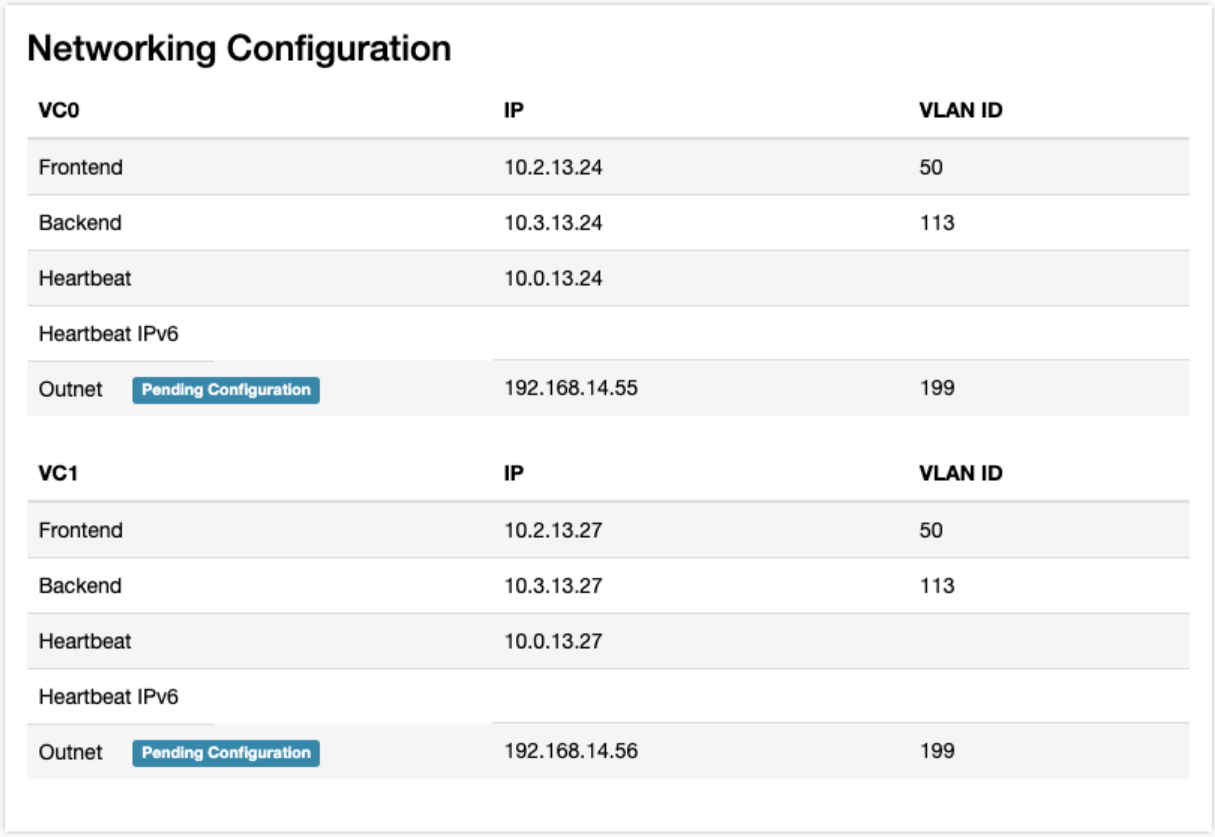
To view the Outnet IP allocated for a VPSA or Object Storage:

1. In the navigation tree, select **VPSAs** or **Object Storage**, according to the storage type of the service whose Outnet parameters you want to view.
2. In the **VPSAs** page, or **Object Storage** page's **Instances** tab, select the VPSA or Object Storage to view.
3. In the **Dashboard** tab, scroll down to the **Networking Configuration** tile.

   If Outnet is configured, each Virtual Controller has an **Outnet** entry displaying its **IP** and **VLAN ID**.

✔ **Note:** If Outnet is configured after VPSAs or Object Storage instances are created:

- The `Pending Configuration` badge appears on the Outnet entry of each VC, in the Networking Configuration tile of the affected VPSAs and Object Storages.
- The next time the VPSA or Object Storage is upgraded, the individual VCs will acquire their Outnet address.



Networking Configuration

VC0	IP	VLAN ID
Frontend	10.2.13.24	50
Backend	10.3.13.24	113
Heartbeat	10.0.13.24	
Heartbeat IPv6		
Outnet Pending Configuration	192.168.14.55	199

VC1	IP	VLAN ID
Frontend	10.2.13.27	50
Backend	10.3.13.27	113
Heartbeat	10.0.13.27	
Heartbeat IPv6		
Outnet Pending Configuration	192.168.14.56	199

CHAPTER

FOURTEEN

CLOUD SETTINGS

Cloud administrators can use Command Center to configure global cloud settings.

14.1 Viewing and Editing Cloud Settings

1. At the top right of the Command Center window, click the gear icon.
2. In the dropdown menu that displays, select **Settings**.

   The **Management Settings** default view displays the **General** settings.list.

   Command Center cloud settings are grouped into the following categories, accessible from the left menu:

Category	Description
General	General Cloud level setting
Security	Cloud level security settings
Network	Cloud networking parameters
VPSA	Settings effecting VPSA instances defined on the cloud
Object Storage	Settings effecting VPSA Object Storage instances defined on the cloud
Management	Management protocols settings

   - To select a different category of settings, click the category name on the left.

     The selected category's parameter list displays.
   - To view or edit sparameter, click **Edit** on the right of a selected parameter.

     The parameter section expands, displaying parameter values.

     Optionally, in the expanded view, edit the values as required and click **Update** to save the changes.

14.2 General Cloud Settings

Parameter	Description
Cloud Name	Set the Cloud Name.
Domain Name	Set the Command Center Domain Name in the URL sent by email to users.
Internet Access	Set internet accessibilty of the cloud.
Support ticket method	Set the method the cloud will use to send support tickets.
Support Tickets Notifications	Set the email recipients to notify of support tickets.
Emails sending method	Set the method the cloud will use to send emails.
Upload Endpoints	Set and manage upload endpoints.
ZSnap upload	Set ZSnap upload.
Metering data upload	Set Metering data upload.
VPSA Usage Reports upload	Set VPSA Usage Reports upload.
Cloud configuration upload	Set Cloud configuration upload.
Cache/AFA-Meta drives settings	Set Cache/AFA-Meta drives settings.
Mount Capacity Alert Threshold (GiB)	Set Mount Capacity Alert Threshold (GiB).
Ticket threshold	Set the ticket sending threshold.
CCVM Engine size	Set CCVM default Engine size.
Automatic Drive Replacement	Automatic Drive Replacement.
Package Upload Size Limit	Set the maximum package upload size (GiB).
Physical Inventory Report	Physical Inventory Report.
Zadara Configuration Update	Zadara Configuration Update.

14.2.1 Cloud Name

Allows renaming the cloud

✔ **Note:** The cloud can be renamed only if the cloud does not contain any VPSA or Object Storage entities.

14.2.2 Domain Name

Specify the domain name to be used as the sender address in emails sent from the cloud to users.

14.2.3 Internet Access

This setting toggles between an online and offline cloud.

An offline cloud is a cloud without Internet access for management. Users managing offline clouds must provide local SMTP, FTP, and NTP services, and adjust support ticket and Zsnap configurations accordingly. In offline clouds, license management is handled manually, as a remote licensing server is not available.

✔ **Note:** MAG files can be created and uploaded only in clouds that have Internet access.

14.2.4 Support ticket method

Specify parameters according to the method selected for sending support tickets.

- **Zendesk**

Parameter	Description
Zendesk URL	URL for the Zendesk Application
Zendesk user	User id used for Zendesk login
ZenDesk Password	Zendesk users password

- **SMTP**

Parameter	Description
Server	SMTP server address
Login	SMTP server login required?
Login User	SMTP User id
AUTH method	SMTP Authentication method to be used (PLAIN or LOGIN supported)
Password	Password for SMTP user
Port	TCP port number for SMTP service
Port SSL	TCP port number for SMTP service is SSL is used
Secure	Force secure SMTP(via TLS)
From user	Email sender address
To User	Email recipient address

14.2.5 Support Tickets Notifications

Specify comma-separated lists of email recipients to notify about support tickets:

- User-facing Support Tickets
- All Support Tickets

14.2.6 Emails sending method

Enables the cloud admin to set up a custom email account for sending customer emails.

The cloud admin can also specify the **Support email** address, that will be included in the email body as the support contact.

✔ **Note:** If the **Emails sending method** is not defined:

- If the cloud has Internet connectivity, customer emails will be sent from the Zadara's AWS SES email account.
- If the cloud lacks Internet connectivity, customer emails will be sent from the SMTP account specified in the Support ticket method section.

Parameter	Description
Server	SMTP server address
Login	SMTP server login required?
Login User	SMTP User id
AUTH method	SMTP Authentication method to be used (PLAIN or LOGIN supported)
Password	Password for SMTP user
Port	TCP port number for SMTP service
Port SSL	TCP port number for SMTP service is SSL is used
Secure	Force secure SMTP(via TLS)
From user	Email sender address
To User	Email recipient address

14.2.7 Upload Endpoints

The cloud administrator can configure alternate endpoints for uploading cloud Zsnaps, MAG and configuration information.

Expanding the Upload Enpoints section displays details of the cloud's configured endpoints.

Upload endpoints can be of the following types:

- AWS S3 endpoint

Parameter	Description
Endpoint name	The endpoint's name
Method	AWS S3
Access Key	Endpoint access key
Secret Key	Endpoint secret key
Region	AWS region

- Object Storage endpoint

Parameter	Description
Endpoint name	The endpoint's name
Method	ZIOS S3
Access Key	Endpoint access key
Secret Key	Endpoint secret key
Endpoint	Object Storage FQDN

- FTP target

Parameter	Description
Endpoint name	The endpoint's name
Method	FTP
Server	FTP server
User	Username
Password	Password
Use Proxy	Whether to use a proxy for the connection

Creating a new endpoint

To create a new endpoint:

1. Expand the **Upload Endpoints** section.
2. At the top right of this section, click **New**.
3. In the **Create Upload Endpoint** dialog, select the endpoint **Method** from the dropdown list, and enter the other parameters relevant to its **Method**.
4. Click **Save**.

Editing an endpoint

To edit an endpoint:

1. Expand the **Upload Endpoints** section.
2. Locate the endpoint to edit. In its **Actions** column, click **Edit**.

   ✔ **Note:** Some system-supplied endpoints are not editable.

3. In the **Edit Upload Endpoint** dialog, update the relevant parameters.

   ✔ **Note:** The endpoint's **Name** and **Method** can not be changed.

4. Click **Save**.

Deleting an endpoint

To delete an endpoint:

1. Expand the **Upload Endpoints** section.
2. Locate the endpoint to delete. In its **Actions** column, click **Delete**.

   ✔ **Note:** Some system-supplied endpoints can not be deleted.

3. In the **Delete Upload Endpoint** dialog, confirm the deletion.

14.2.8 ZSnap upload

Configurations for the target used for the cloud's ZSnaps upload.

✔ **Note:** Only one upload endpoint can be specified for ZSnap uploads.

- **Settings for ZSnap upload to an AWS S3 or Object Storage endpoint**

Parameter	Description
Bucket	bucket for ZSnap upload

- **Settings for ZSnap upload to an FTP endpoint**

Parameter	Description
Max-allowed-mb	Maximum ZSnap capacity threshold when using CCmaster FTP server
Max-retain-mb	Minimum ZSnap capacity retained when using CCmaster FTP server

14.2.9 Metering data upload

The cloud administrator can configure the target endpoints to which metering data can be uploaded. Up to three AWS S3 endpoints can be configured for metering data uploads.

Adding an additional endpoint

To add an additional upload endpoint:

1. Expand the **ZSnap Upload** section.
2. Click **Add Another**.
3. Select the **Endpoint** from the dropdown and enter the **Bucket**.

Parameter	Description
Endpoint	Endpoint for metering data upload
Bucket	Bucket for metering data upload

4. Click **Update**.

Removing an additional endpoint

To remove an additional endpoint:

1. Expand the **ZSnap Upload** section.
2. Locate the additional endpoint to remove and click **Discard Endpoint**.
3. Click **Update**.

14.2.10 VPSA Usage Reports upload

The cloud administrator can configure the target endpoints to which VPSA Usage Reports data can be uploaded. Up to three AWS S3 endpoints can be configured for VPSA Usage Reports data uploads.

Adding an additional endpoint

To add an additional upload endpoint:

1. Expand the **VPSA Usage Reports Upload** section.
2. Click **Add Another**.

3. Select the **Endpoint** from the dropdown and enter the **Bucket**.

Parameter	Description
Endpoint	Endpoint for VPSA Usage Reports data upload
Bucket	Bucket for VPSA Usage Reports data upload

4. Click **Update**.

Removing an additional endpoint

To remove an additional endpoint:

1. Expand the **VPSA Usage Reports Upload** section.
2. Locate the additional endpoint to remove and click **Discard Endpoint**.
3. Click **Update**.

14.2.11 Cloud configuration upload

The cloud administrator can configure the target endpoints to which VPSA Usage Reports data can be uploaded. Up to three AWS S3 endpoints can be configured for VPSA Usage Reports data uploads.

Adding an additional endpoint

To add an additional upload endpoint:

1. Expand the **Cloud configuration upload** section.
2. Click **Add Another**.
3. **Select the Endpoint from the dropdown, and enter the Bucket and Upload period**.

Parameter	Description
Endpoint	Endpoint for cloud configuration data upload
Bucket	Bucket for configuration data upload
Upload period (seconds)	Sets the configuration data upload interval

4. Click **Update**.

Removing an additional endpoint

To remove an additional endpoint:

1. Expand the **Cloud configuration upload** section.
2. Locate the additional endpoint to remove and click **Discard Endpoint**.
3. Click **Update**.

14.2.12 Cache/AFA-Meta drives settings

Cloud administrators can configure the behavior of the cloud when provisioning VPSA All Flash (AFA), and whether to allow the use of cloud solid state drives as AFA cache instead of Optane drives.

✔ **Note:** VPSA All Flash architecture was designed to utilize Optane drives to optimize overall system performance. The use of solid state drives as AFA cache should be limited for testing purposes only, and coordinated with Zadara support.

Parameter	Description
Allow temporarily setting SSDs as AFA-Meta Drive	Enables setting SSDs as AFA cache
SSD Cache Max usable capacity	Sets the maximum capacity that will be used for an SSD drive designated as AFA cache

To save changes, click **Update**.

14.2.13 Mount Capacity Alert Threshold (GiB)

Mount Capacity Threshold

Administrators can configure the cloud's `/mnt/Nova` folder's capacity threshold.

An alert will be issued if this capacity threshold is exceeded.

Parameter	Description
Mount Capacity Alert Threshold (GiB)	Capacity threshold in GiB

To save changes, click **Update**.

14.2.14 Ticket threshold

Administrators can configure timed thresholds for specific events to be considered for support ticket generation:

Parameter	Description
Failed drive ticket time	Allowed failure time before user ticket generation
Failed drive support ticket time	Allowed failure time before support ticket generation
Failed heartbeat ticket time	Allowed failure time before user ticket generation

To save changes, click **Update**.

14.2.15 CCVM Engine size

CCVM Engine size

Administrators can select a configuration determining the CCVM's CPU and memory .

Engine size	Number of CPUs	Ram(Gib)
Small	1	2
Medium	2	4
Large	4	8

To save changes, click **Update**.

Caution: On saving changes, the CCVM is restarted. The restart process could take few minutes.

14.2.16 Automatic Drive Replacement

Administrators can configure the cloud's automatic drive replacement feature.

When Automatic Drive Replacement is enabled, replacement is triggered for any reported failed drive in any cloud-resident VPSA.

The drive replacement begins after a user-defined monitoring interval.

Failed drives are replaced with spares of the same or similar model and capacity, provided that such spares are available in the cloud.

Parameter	Description
Enable Automatic Drive Replacement	Toggle to enable auto-replace
Failed drive support ticket time	The time (in minutes) after which replacement will be triggered for a drive presumed to be failed

Note: The recommended value for Automatic Drive Replacement timeout is 30 minutes.

Automatic Drive Replacement does not take place for drives that are part of a RAID group that has an assigned dedicated hot spare.

Automatic Drive Replacement does not take place when more then four drives fail at the same time.

To save changes, click **Update**.

14.2.17 Package Upload Size Limit

Admins can configure the maximum package upload size in GiB.

Parameter	Description
Max upload size	Maximum Package File Size (GiB) Default: 25 GiB

14.2.18 Physical Inventory Report

Administrators can determine the Upload Method of the Physical Inventory Report, and whether to enable or disable it.

Parameter	Description
Enabled	Enable/disable toggle
Upload Method	Physical Inventory Report's upload method. Possible options: • **S3** (default) • **SMTP**

14.2.19 Zadara Configuration Update

Administrators can define Zadara Configuration Keys.

Creating Zadara Configuration Keys

To create a new Configuration Key:

1. Click **New**.
2. In the Create Zadara Configuration Key dialog:
    1. Select **Key Type** from the dropdown. Possible options:
        - **String**
        - **Integer**
        - **Float**
        - **Boolean**
    2. Enter the **Keyname** and **Key Value** pair.
    3. Click **Save**.

Editing and Deleting Zadara Configuration Keys

To **Edit** or **Delete** an entry, click on the appropriate button in the **Actions** column.

14.3 Security Settings

Parameter	Description
Password expiration	Set when passwords expire and set how many old passwords the system will forbid to reuse.
VPSA API Passthrough	Allow VPSA APIs to Pass-Through Command Center server.
Custom Certificate for Command Center & Provisioning Portal	Set a custom certificate for Command Center & Provisioning Portal web applications.
Trusted CAs	Update trusted CA list for VPSA/Object Storage/CCVM with uploaded certificates.
Dual Factor	Turn on dual factor for all LOCAL Command Center users.
Cloud Control IP Whitelist	Turn on and manage Command Center and Provisioning Portal Access Control.
Cloud Remote Access	Manage access to the cloud.

14.3.1 Password expiration

Administrators can determine the user passwords expiration and replacement policy.

Parameter	Description
Enforce Password Expiration	ON - User Password expires and replacement is required after the specified period
Password Expire After	Number of days a current password is valid
Password history	Number of password replacement cycles in which a password cannot be repeated

To save changes, click **Update**.

14.3.2 VPSA API Passthrough

VPSA instances running in the cloud can be managed using Command Center as an API endpoint.

This option should be used when an application requires management access to VPSAs from a dedicated network outside of the Zadara cloud.

Parameter	Description
Allow VPSA API Passthrough	ON - Allow VPSA APIs to pass through the Command Center server

To save changes, click **Update**.

14.3.3 Custom Certificate for Command Center & Provisioning Portal

The default certificate used in Command Center and Provisioning Portal can be replaced by a user provided certificate.

Users are required to upload their `.crt` and `.key` files to perform the certificate replacement.

✔ **Note:** The provided user certificate must be compatible with NGINX HTTP server.

14.3.4 Trusted CAs

Enables the addition of certificate authorities to the VPSA and Command Center Trusted CA lists by uploading certificates signed by them, bundled in a `.zip` file.

14.3.5 Dual Factor

Enables activation or cancellation of dual factor authentication for all local Command Center users.

Activation of dual factor authentication will sign out local users who are not yet using this feature.

14.3.6 Cloud Control IP Whitelist

Enables activation or cancellation of access control for the Command Center and Provisioning Portal applications, granting access only to specified IP addresses.

By default, IP address whitelisting is disabled.

- **Granting access to the the Command Center and Provisioning Portal**:

  To allow access to the the Command Center and Provisioning Portal, add the relevant accessing IP addresses to the Cloud Control IP Whitelist:

  1. Mark the **Enable Cloud Control IP Whitelisting** checkbox.

     ✔ **Note:** An alert advises that access to all interfaces will be blocked for all IPs not specifically listed in the Whitelist.

     Saving the IP Whitelisting feature as active is only possible when there is at least one configured whitelisted IP address.

  2. Click **Add New** and in the whitelist table enter:
     - **IP/CIDR**: The IP address or CIDR to be whitelisted and permitted access.
     - **Application Access**: Select from the dropdown, whether access should be granted to the Provisioning Portal, the Command Center, or both.
     - **Comment**: Enter free text details, a note or comment about this entry.

     Repeat this procedure for all IP addresses or CIDRs that should be whitelisted.
  3. Click **Save**.

- **Updating access to the the Command Center and Provisioning Portal**:

  Entries in the whitelist table can be updated by clicking the IP/CIDR's **Edit** Action, and then editing the relevant fields and clicking **Save**.

- **Denying access to the the Command Center and Provisioning Portal**:

  An IP/CIDR entry can be removed from the whitelist by clicking the IP/CIDR's **Discard** Action, and then **Save**.

✔ **Note: Exceptions and Restrictions**:

- The IP Whitelist is limited to a maximum of 256 rows of IP addresses and CIDRs (the allowed entries limit was increased in version 23.09-SP1)
- By default, specific fixed Zadara operations IP addresses are whitelisted in all zStorage clouds. These IP addresses are managed internally and are not visible in the Command Center UI or via the API.
- Although IPv6 addresses can be used, they are not officially supported. In cases where an IPv6 address is used, logs display an IPv4 conversion of the address.
- The IP Whitelisting feature relies on source IP visibility. For administrators accessing the Cloud management applications over public networks, whitelisting a private IP address space will not achieve the required behavior. Simarly, IP Whitelisting is not supported for source IP addresses that are masked. If a source IP is hidden, IP Whitelisting might not work as expected.

14.3.7 Cloud Remote Access

Manages access to the cloud infrastructure management interfaces for remote support and administration.

14.4 Network Settings

Parameter	Description
MTU Size	Set and review the cloud networks' MTU size.
Protection Zones backend connectivity	backend connectivity settings in Protection Zones change the protocol used for inter-zone connectivity.

14.4.1 MTU Size

Maximum Transmission Unit (MTU) is the largest size, in bytes, of a single packet that can be sent over a network interface without fragmentation.

Admins can adjust their cloud networks' MTU size.

Important: Best Practice

While the FE and Public networks may use different MTU values from each other, all components within each network must use the same MTU setting.

- For the **FE Network**, configure an identical MTU across all its connected zStorage components — VPSAs, Object Storages, Storage Nodes, and any associated customer-side hosts or switches.
- For the **Public Network**, also ensure a consistent MTU across all of its connected components.

Inconsistent MTU settings across zStorage components for a network can cause packet fragmentation, increased latency, or dropped connections, which could impact performance and data availability.

Parameter	Description
FE MTU size	MTU size for the VPSA network (Front-End). Select 1500 (Default), 2048, 4096, 9000 from the dropdown, or overwrite the displayed value with a custom MTU size in the range of 1420 - 9000.
Public MTU size	MTU size for the public network. Select 1500 (Default), 2048, 4096, 9000 from the dropdown.

14.4.2 Protection Zones backend connectivity

In multizone clouds, administrators can configure use of the iSCSI protocol instead of the iSER protocol.

The backend connectivity settings in Protection Zones change the protocol used for inter-zone connectivity **only**. In-zone requests will continue using iSER. Switching to iSCSI for inter-zone connectivity should be done only when iSER connectivity between zones is not possible, for example, due to the network configuration.

To configure iSCSI Inter-Zone Backend connectivity

1. Ensure that no multizone VPSA or Object Storage is already configured in the cloud.
2. Set the **Remote Region Backend Protocol** to **iSCSI**.
3. Click **Update** to apply the changes.

When the **Remote Region Backend Protocol** is set to **iSCSI**, a warning message appears in Command Center's Protection Zone tab.

> **Warning:** Changing the inter-region connectivity protocol to iSCSI might affect the performance of VPSA or Object Storage.

14.5 VPSA Settings

Parameter	Description
Domain Name	Set the VPSA Domain name.
Recycle bin	Set the duration in which a VPSA will stay in recycle bin before purging.
Certificate	Set the certificate used in VPSA web application.

14.5.1 Domain Name

Administrators can configure and modify the domain name used for VPSA entities in the cloud.

14.5.2 Recycle bin

Administrators can specify the number of days that deleted VPSA entities stay in the recycle bin before being permanently purged from the system, making them unrecoverable.

14.5.3 Certificate

Administrators can substitute the default certificate used in the VPSA web management application by providing a custom certificate.

To replace the certificate, upload the certificate's `.crt` and `.key` files.

✔ **Note:** The user-provided certificate must be compatible with the NGINX HTTP server.

The default certificate is automatically updated and propagated to existing VPSAs.

To propagate the new certificate to all running VPSAs in the cloud, select the **Update new certificate on all running VPSAs in the cloud** checkbox, that displays after uploading the new certificate and key files.

14.6 Object Storage Settings

Parameter	Description
Certificate	Set the default certificate that will be used for newly created VPSA Object Storage web application. Existing VPSA Object Storage certificate can be updated from the VPSA Object Storage itself.

14.6.1 Certificate

Administrators can substitute the default certificate used in the Object Storage web management application by providing a custom certificate.

To replace the certificate, upload the certificate's `.crt` and `.key` files.

✔ **Note:** The user-provided certificate must be compatible with the NGINX HTTP server.

Existing Object Storage certificates can be updated directly in the Object Storage.

14.7 Management Settings

Parameter	Description
SNMP	SNMP
Tickets Settings	Tickets Settings
Log Level	Log Level

14.7.1 SNMP

The Zadara cloud ecosystem enables infrastructure monitoring for Cloud, VPSA, and Object Storage administrators through SNMP traps. These SNMP traps are designed to notify administrators of infrastructure events and are generated in parallel to Zendesk tickets.

SNMP traps can be sent from:

- VPSA
- Object Storage
- Cloud Storage Nodes
- CCVM

The Zadara cloud SNMP MIB can be downloaded publicly from the following link:
https://zadarastorage-software.s3.amazonaws.com/snmp-mib/20.01/ZADARA-MIB.txt

✔ **Note:**

- The Zadara cloud currently supports a single trap recipient.
- SNMP is supported for VPSA and Object Storage entities, from version 20.01 and later.
- SNMP traps at the Storage Node level are not supported for nodes operating with the Trusty kernel.

General SNMP Settings

Parameter	Description
Enable SNMP	If enabled, SNMP Traps will be sent from all the cloud monitored elements according to the specified configuration
Minimum ticket priority	The minimum priority for a Zendesk ticket that will trigger an SNMP trap to be sent
Trap recipient	The IP address of the receiver of trap notifications.
Protocol Version	The SNMP version to use. The supported versions are SNMPv2 and SNMPv3.

✔ **Note:** SNMP traps are not bound to any specific network. The network interface from which SNMP traps are sent is determined based on the routing configuration of the managed entity.

SNMPV2 setting

Parameter	Description
Community	SNMPv2 community string that the SNMP agent uses when sending trap messages to the SNMP client

SNMPV3 setting

Parameter	Description
Username	SNMPV3 username for sending traps
Minimum ticket priority	Minimum priority set for a Zendesk ticket from which an SNMP trap will also be sent
Auth Protocol	SNMPv3 Authentication protocol to use. Supported protocols are: none, MD5, SHA-1, SHA-2-224, SHA-2-256, SHA-2-384 and SHA-2-512.
Auth key	SNMPv3 authentication password (valid of Auth protocol is set to any value but none). Minimum Auth key lengths is 8 characters.
Privacy Protocol	SNMPv3 privacy(encryption) protocol to use. Supported protocols are: none, AES128 , AES192, AES256 and DES
Priv key	SNMPv3 privacy(encryption) key (valid of privacy protocol is set to any value but none) Minimum. Priv key lengths is 8 characters.

Parameter	Description
Username	The SNMPv3 username used for sending traps.
Minimum ticket priority	The minimum priority for a Zendesk ticket that will trigger an SNMP trap to be sent.
Auth Protocol	The SNMPv3 authentication protocol to use. Supported protocols: • none • MD5 • SHA-1 • SHA-2-224 • SHA-2-256 • SHA-2-384 • SHA-2-512
Auth key	The SNMPv3 authentication password. This is required if the authentication protocol is set to any value other than **none**. The minimum length for the Auth key is 8 characters.
Privacy Protocol	The SNMPv3 privacy (encryption) protocol to use. Supported protocols : • none • AES128 • AES192 • AES256 • DES
Priv key	The SNMPv3 privacy (encryption) key. This is required if the privacy protocol is set to any value other than **none**. The minimum length for the Priv key is 8 characters.

Note: Supported security levels for SNMPv3:

- **NoAuthNoPriv**:

  No cryptographic authentication
  No encryption of the SNMP messages payload

- **AuthNoPriv**:

  Cryptographic authentication
  No encryption of the SNMP messages payload

- **AuthPriv**:

  Cryptographic authentication
  SNMP packet is encrypted

Testing SNMP Settings

Cloud administrators can test and verify their SNMP settings before applying them, by sending a test trap.

To send a test trap, click the **Test** button on the SNMP settings dialog.

The system generates and transmits the test traps based on the specified settings.

Working with SNMPv3 Engine IDs

Sending and receiving SNMPv3 Traps involves using the SNMP Engine ID managed element identifier.

Configure the engine ID of each managed element in the SNMP trap recipient so that it can receive traps from that entity.

Zadara Cloud assigns a unique engine ID for:

- The Zadara Cloud infrastructure, including all Storage Nodes and the Cloud Controller VM
- Each VPSA and Object Storage entity

You can find the Engine ID for the Zadara Cloud infrastructure at the lowers right corner of the screen.

The Engine ID for a VPSA or Object Storage entity is specified in the entity's Property tab.

Note: The SNMPv3 Engine ID is not displayed in versions earlier than 20.01.

14.7.2 Ticket Settings

The cloud administrator can override the default attributes of the cloud infrastructure support tickets, in the Ticket Settings section.

Overriding global ticket attributes for an individual VPSA or Object Storage can be specified in VPSA or Object Storage's Settings tab.

Parameter	Description
Message ID	The Message ID of the ticket to be configured
Suppression expiration date (UTC)	Sets a ticket as suppressed until a given timestamp. Suppressed tickets are not sent to Zendesk from this particular cloud.
Zsnap	Allows the user to configure whether a Zsnap is created when this ticket is produced, and the type of Zsnap to create (full/light)
Send To Users	Indicates whether tickets for the specific message id are sent to cloud users that have enabled notifications.
Rate limit (seconds)	The interval from the time a specific ticket is produced to the time that another ticket for the same monitored element and with the same Message ID can be produced again.
Comment	User comment explaining the reason for this attributes change

After creation of a custom ticket rule, the initial dialog of the Ticket Settings section is modified to display the rules currently applied on this cloud.

Existing rules can also be edited or deleted by clicking on the appropriate button in the **Actions** column.

✔ **Note:** The cloud level ticket rules display does not provide any visibility of rules defined for an individual VPSA or Object Storage, and vice versa.

14.7.3 Log Level

Administrators can specify the level of detail in the Command Center's web application internal logs:

- **Info**: (default)
- **Debug**: logs with more detail for analysis purposes

⚠ **Caution:** Activate the Debug level only after consultation with Zadara Support.

CHAPTER

FIFTEEN

UI CUSTOMIZATION

Command Center allows cloud administrators to personalize their underlying VPSA and Object Storage user interface look and feel, by modifying the VPSA login header image and the favicon that appear on the browser tab and the UI left menu panel.

15.1 Prerequisites

In advance of the UI customization, prepare and resize custom images:

15.1.1 VPSA and Object Storage UI Customization

- Login header image
  - Format: **jpg**
  - Height: 115px
  - Width: 400px
- Favicon image
  - Format: **png**
  - Height: 16px
  - Width: 16px

15.1.2 Command Center UI Customization

- Header image
  - Format: **png**
  - Height: 135px
  - Width: 516px

15.2 Customizing the Command Center UI

1. At the top right of the Command Center window, click the gear icon.
2. In the dropdown menu that displays, select **UI Customizations**.
3. In the **Customization** view, click the tab of the UI entity to customize:
   - **VPSA**
   - **Object Storage**
   - **Command Center**

   Customization controls, custom images and their attributes are displayed in the selected tab's **Images** view:

Column	Description
Name	The custom image's filename. The **Choose File** button to upload a custom image, when there is no current custom image.
Custom	The custom image display. The **N/A** indicator, when there is no current custom image.
Notes	The format and dimension requirements for the image type.
Delete	The control checkbox for removing a custom image.

4. For each image to customize, in the image's **Name** column click **Choose File**.

   In the file explorer dialog that opens, browse, select and upload the new image file.
5. Click **Update** to confirm uploading the selected images.
   - The custom images display in the **Custom** column.
   - The modified images display in their respective headers.

   ✔ **Note:** The modified header image and favicon will be applied to newly created VPSA and Object Storage instances, or to instances that have been hibernated and then restored.

15.3 Removing Customized Command Center UI elements

To undo customization and revert to the default header image and favicon:

1. At the top right of the Command Center window, click the gear icon.
2. In the dropdown menu that displays, select **UI Customizations**.
3. In the **Customization** view, click the tab of the UI entity to customize:
   - **VPSA**
   - **Object Storage**
   - **Command Center**
4. For each custom image that should be reverted to the default, in the image's **Delete** column mark the **Delete** checkbox.
5. Click **Update** to confirm removing the selected images and reverting to the default.

CHAPTER

SIXTEEN

CLOUD SOFTWARE MANAGEMENT

Using Command Center, administrators manage virtual machine images for:

- VPSA
- VPSA Object storage
- CCVM

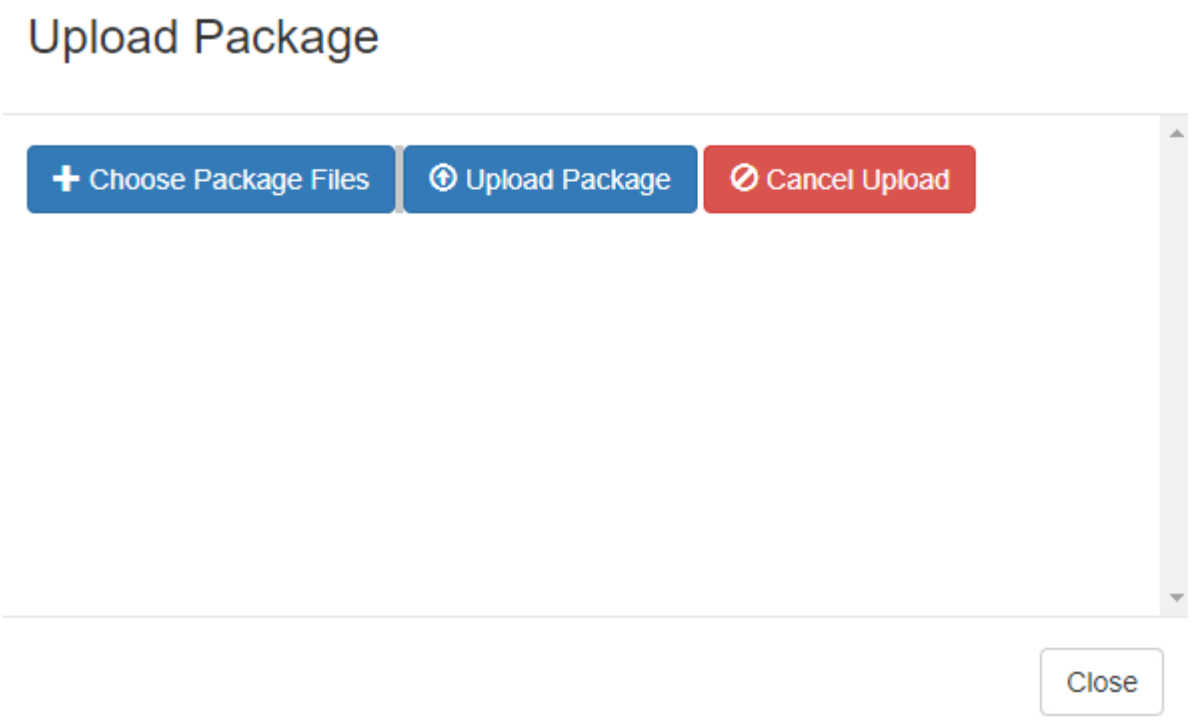
Cloud administrators can pull specific images from a repository and specify a set of images as default. Default images will be the ones deployed when a new VPSA instance is created.

16.1 Pulling Package And Registering Images

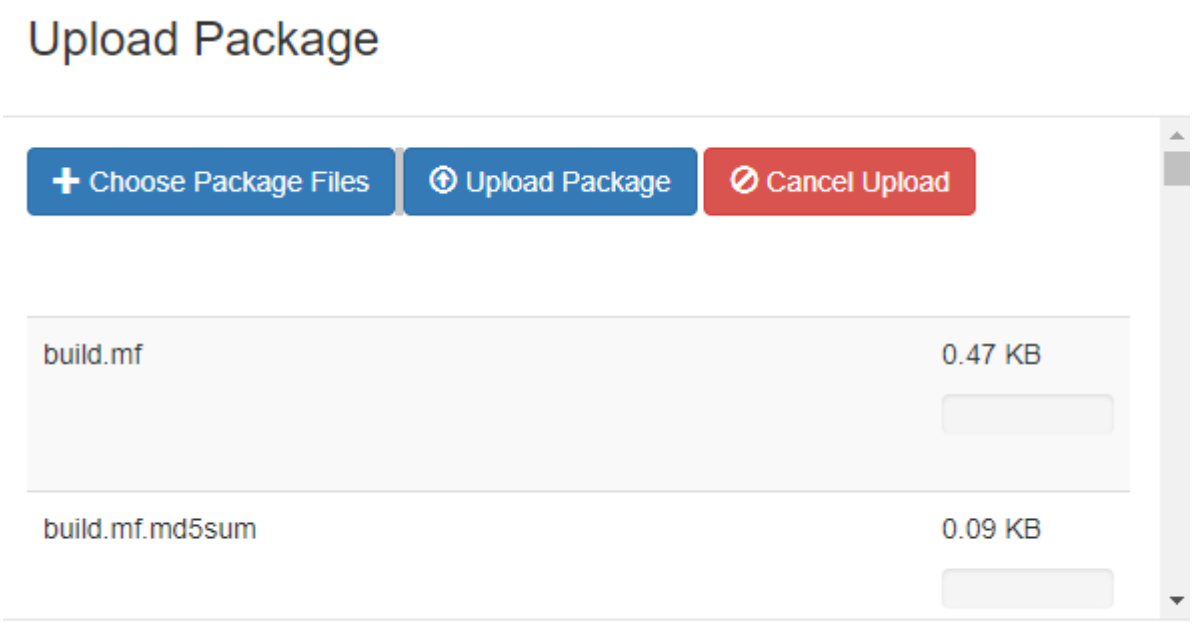
To make new virtual machine images available for cloud users, image packages must be pulled from Zadara repository and the images registered. To pull image packages from the Zadara repository click on the gear icon on the top right of the screen and select `manage cloud packages` from the drop down menu. Make sure that your repository location is set to default(as shown below) or to a valid location accssible via the S3 protocol and containing the relevant image packages. A list of available image packages should appear. You can regenerate the list of packages available in the repository by clicking the refresh icon next to the screen title.

✔ **Note:** Zadara storage public image repository is: s3://zadarastorage-install/ and it is set as the default Command Center repository.

Packages can also be uploaded from local storage, if a package repository is not available or reachable from the cloud. To upload a package from local storage click on the `Upload Package` button. On the popup window that will appear, click on `Choose Package File` and use the file-grid to navigate into a folder containing cloud package files and select all of them.



A list of the selected files will be populated in the popup window. To begin uploading the package click on `Upload Package`.



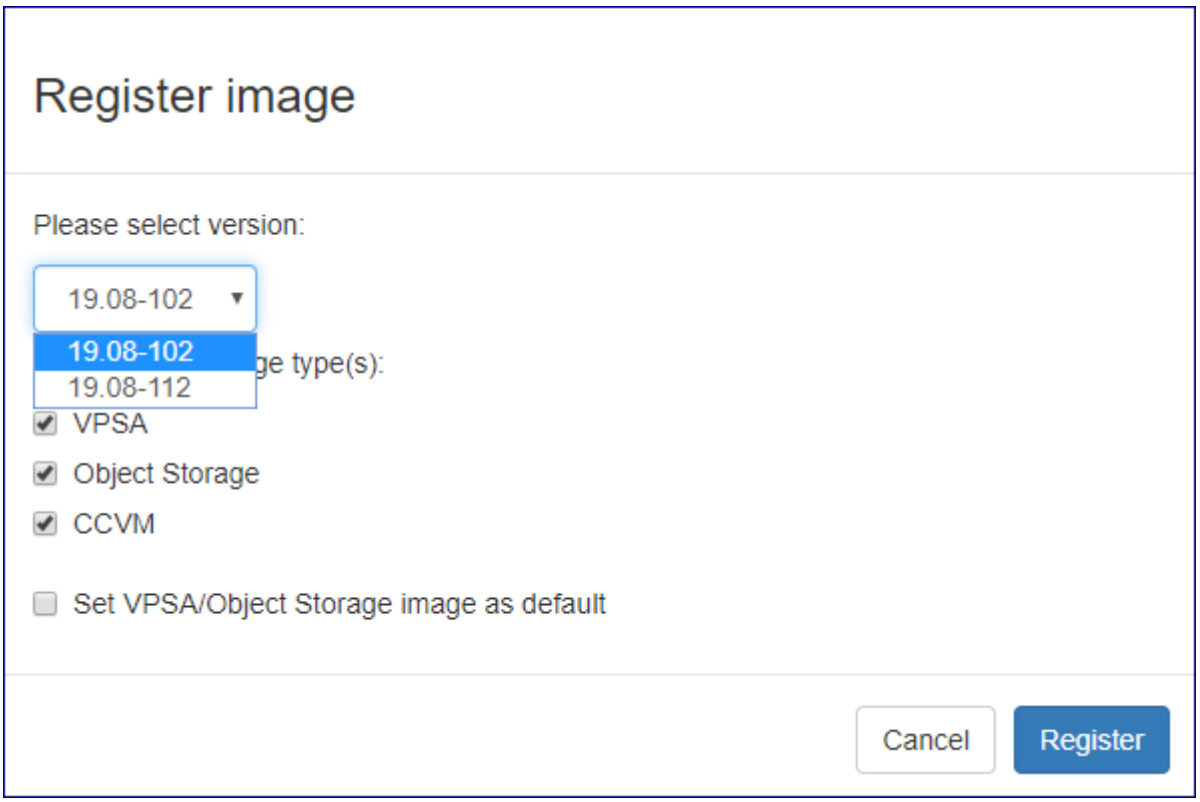
The upload progress is tracked on a file level progress bar. When the file upload and registration process are finished, the package will be added to the available packages grid.

To download a specific package, locate it on the package list. Make sure its status is Available for download and click the `Download` button.

Downloaded packages can be erased from local storage once they are no longer required. To erase a package click on the `erase` button for the image and confirm the package deletion in the popup window that will appear.

To register mages from the downloaded package go to the Command Center Images tab and click on the `Register image from local repository` button. In the popup dialog that will appear, wait for the package version list to load and select the specific version from which you would like to register the images. Select the Images you would like to register (VPSA, Object storage or CCVM) and weather you would like to set them as the default image for new VPSA deployments and click the `Register` button to confirm the operation.

✔ **Note:** You can set a specific image as default at any time by clicking the downward arrow button for the specific image and select Set default from the drop down menu.



A registered image can be later deleted by clicking the downward arrow button for the specific image and select Delete from the drop down menu.

CHAPTER

SEVENTEEN

USERS

Command Center provides role-based user management functionality. Granular per-activity user roles can be defined and assigned to Command Center user accounts.

To create and configure Command Center roles, see Roles.

17.1 Viewing Users

1. At the top right of the Command Center window, click the cog wheel icon.
2. In the dropdown menu that displays, select **Users**.

   The **Users** view displays the **Users** grid:

Column	Description
User	The user's username.
Roles	Link to the user's associated role.
Domain	Indicates whether the user is local or imported from an external directory: • **local**: User created in Command Center • **<domain name>**: The domain name of the external directory from which the user was imported.
Admin	Indicator whether the user is an admin user.
Enabled	Indicator whether the user is enabled or disabled.
Dual Factor	Indicator whether dual factor authentication sign-on is required for the user.
Actions	Dropdown menu of configuration actions for a user's settings: • **Edit** • **Enable/Disable** • **Delete**

17.2 Creating a local user

To create a new local Command Center user:

1. At the top right of the Command Center window, click the cog wheel icon.
2. In the dropdown menu that displays, select **Users**.
3. In the Users screen, click **Create new user**.
4. In the **Create User** dialog, configure the new user:
   - **Email**:

     The user's email address. This is also the user's Command Center user ID and sign-on name.
   - **First name**:

     The user's first name.
   - **Last name**:

     The user's last name.
   - **Admin**:

     Mark the checkbox if the user is an admin user with admin privileges.
   - **Roles**:

     Mark the checkbox for each role with which the user should be associated.

     ✔ **Note:** This setting is not relevant for users marked as **Admin**, as they have full system-wide access privileges.
5. Click **Create** to confirm creation of the user with the configured settings.

   The new user is emailed Command Center sign-on details and a temporary password for the first sign-on.

   ✔ **Note:** On first sign-on, the user is required to change the password.

17.3 Editing a local user

To edit a local Command Center user:

1. At the top right of the Command Center window, click the cog wheel icon.
2. In the dropdown menu that displays, select **Users**.
3. In the Users screen, locate the user to edit, open the user's **Actions** dropdown menu and select **Edit**.
4. In the user's **Settings** screen, edit the user configuration:
   - **Basic Details**
     - **Email**:

       The user's email address. This is also the user's Command Center user ID and sign-on name.

- **First name**:

  The user's first name.

- **Last name**:

  The user's last name.

- **Admin**:

  Mark the checkbox if the user is an admin user with admin privileges, or unmark it to remove admin privileges.

  ✔ **Note:**

  * If a user is changed to an admin user, the **Roles** associations are removed for this user, as admin users have full system-wide access privileges.
  * If the user was an admin user and the checkbox is changed to unmarked to remove admin privileges, the user should be assigned relevant **Roles** separately, after the Basic Details are updated.

To apply these changes, click **Update** at the end of the **Basic Details** section.

- **Reset Password**

  To reset the user's password click **Reset**.

  A **Confirm Password Reset** dialog opens, notifying that resetting the user's password will also regenerate the user's API Key for REST API requests.

  To confirm resetting the user's password, click **Confirm**.

  The user is emailed a temporary password for the next sign-on, that must be changed after sign-on.

- **Disable/Enable**

  To enable or disable the user, click the **Enable** or **Disable** toggle.

  The user's updated enabled or disabled state displays.

- **Roles**:

  Mark the checkbox for each role with which the user should be associated.

  To confirm the updated role assignments, click click **Update** at the end of the **Roles** section.

  ✔ **Note:** This setting is not relevant for users marked as **Admin**, as they have full system-wide access privileges.

17.4 Enabling or Disabling a local user

All user attributes remain intact when a user is disabled, except for the ability to access Command Center.

When enabling or disabling an imported user, only the local Command Center user's ability to access the system changes, and the external Active Directory user is not impacted.

There are two ways to enable or disable a local user:

- **Enable or Disable a user by using the Actions menu**:

  1. At the top right of the Command Center window, click the cog wheel icon.

2. In the dropdown menu that displays, select **Users**.
3. In the Users screen, locate the user to enable or disable, open the user's **Actions** dropdown menu and select the **Enable** or **Disable** toggle, depending on the user's current state.

   The user's **Enabled** column indicator displays the updated state.

- **Enable or Disable a user in the Edit screen**:
  1. At the top right of the Command Center window, click the cog wheel icon.
  2. In the dropdown menu that displays, select **Users**.
  3. In the Users screen, locate the user to enable or disable, open the user's **Actions** dropdown menu and select **Edit**.
  4. In the user's **Settings** screen, in the **Disable/Enable** section, click the **Enable** or **Disable** toggle.

     The user's updated enabled or disabled state displays.

17.5 Deleting a local user

Deleting a local user removes the user and its attributes from Command Center.

When deleting an imported user, only the local Command Center user's is removed, and the external Active Directory user is not impacted.

1. At the top right of the Command Center window, click the cog wheel icon.
2. In the dropdown menu that displays, select **Users**.
3. In the Users screen, locate the user to delete, open the user's **Actions** dropdown menu and select **Delete**.
4. In the deletion confirmation dialog that displays, click **Confirm** to proceed with the deletion.

   The user's entry is removed from the grid on the Users screen.

17.6 Importing users from an external directory

To import users from an external directory service, a connection to the service must be defined.

17.6.1 Viewing directory service connections

1. At the top right of the Command Center window, click the gear icon.
2. In the dropdown menu that displays, select **Remote Authentication**.

   The Remote Authentication screen displays the directory service connections.

Parameter	Description
Type	Directory type (currently AD LDAP is supported)
Domain	FQDN for the Domain
Alias	Short name for the domain
Port	LDAP service port
Base DN	DN for user search (format: CN=x,DN=y)
DNS	IP of the Domain DNS server
SSL	Whether to use SSL encrypted communication to the DC

17.6.2 Defining a directory service connection

1. At the top right of the Command Center window, click the gear icon.
2. In the dropdown menu that displays, select **Remote Authentication**.
3. In the Remote Authentication screen, click **Add Authentication Server**.
4. Configure the new directory service connection:

Parameter	Description
Type	Directory type (currently AD LDAP is supported)
Domain	FQDN for the Domain
Alias	Short name for the domain
Port	LDAP service port
Base DN	DN for user search (format: CN=x,DN=y)
DNS IP #1	IP of the Domain DNS server
DNS IP #2	Alternate DNS IP
SSL	Whether to use SSL encrypted communication to the DC

5. Click **Save**.

Important: Command Center uses the LDAP or LDAPS protocol to integrate with Microsoft Active Directory.

- LDAP connectivity occurs via port 389/TCP.
- LDAPS connectivity occurs via port 636/TCP.

17.6.3 Importing domain users

1. At the top right of the Command Center window, click the cog wheel icon.
2. In the dropdown menu that displays, select **Users**.
3. In the Users screen, click **Import directory users**.
4. In the Import Directory Users dialog, enter the domain and its sign-on credentials:
   - **Domain**: Select the domain from the dropdown list.
   - **Directory username**
   - **Directory password**

   Click **Step 2: Select users**.
5. In the dialog listing the domain's users, select the users that will be granted Command Center access.

   In the same way as during creation of a local user, each imported user can be assigned roles that define their specific privileges.
6. To confirm importing the selected domain users, click **Import Users**.

   The imported users are added to the Command Center users list.

   The Users screen's Domain column indicates the type of user:
   - **local**: User created in Command Center
   - **<domain name>**: The domain name of the external directory from which the user was imported.

CHAPTER

EIGHTEEN

ROLES

Command Center provides role-based user management functionality. Granular per-activity user roles can be defined and assigned to Command Center user accounts.

To create and configure Command Center users, see Users.

18.1 Managing Roles

The system includes the preconfigured, non-modifiable **Read Only** role. **Read Only** role holders have viewing access of all managed resources:

Additional roles can be created as needed.

18.1.1 Viewing roles

1. At the top right of the Command Center window, click the cog wheel icon.
2. In the dropdown menu that displays, select **Roles**.

   The **Roles** view displays the **Roles** grid:

Column	Description
Name	The role's name.
Permissions	A list of the managed resources, each resource followed by access permissions for this role.

   Some managed resources only have permission to allow view access. The others have configurable resource-specific permissions, in addition to the viewing permission:

Managed Resource	Permissions
Access Logs	• View
Protection Zones	• View • Rename
App Engine types	• View
Central logs	• View • Manage RSYSLOG
Cloud users	• View • Manage Vlan ID
Clouds	• View • Zsnap • Upgrade • Shutdown
Comments	• View • Manage
Composite Engine types	• View
Virtual Networks	• View • Manage
Data services	• View • Manage
Drive types	• View
Drives	• View • Replace • Manage led • Enable • Disable • Designate as Cache/AFA-Meta • Undesignate a Cache/AFA-Meta • SMART test • License • Unlicense • Purge
IO Engine types	• View
Images	• View • Set default • Register • Delete
Licensing	

18.1.2 Defining a new custom role

To define a new custom role:

1. At the top right of the Command Center window, click the cog wheel icon.
2. In the dropdown menu that displays, select **Roles**.
3. In the Roles screen, click **Create new role**.
4. In the **Create Role** dialog, configure the new role:
    - **Name**: Enter a name for the role.
    - **Permissions**:
        - **Global Permission Controls**

          This set of controls apply permission configurations across all managed resources.
            - **Select All**:
                - Mark the checkbox to grant all permissions of all resources.
                - Unmarking this checkbox removes all permissions of all resources, including those that were applied individually or via a specific resource's **Select All** control.
            - **Expand All**: Display the permissions for all managed resources.
            - **Hide All**: Display the list of managed resources only.
            - **Import Role**: To populate specific permissions based on an existing role's configuration, select the role from the dropdown list.

              Multiple roles can be imported to build up a combined permissions set.
        - **Managed Resource Permission Controls**

          Each managed resource has its own set of controls:
            - **Expand/Contract** arrow toggle displays all of the selected resource's permission settings, or hides them.
            - **Select All** checkbox appears only for resources that have other permissions in addition to the **View** permission setting.
                - Mark the checkbox to grant all permissions of the resource.
                - Unmarking this checkbox removes all permissions of the resource, including those that were applied individually.

              ✔ **Note:** Granting or revoking all permissions is applied, irrespective of whether the resource's permissions are displayed or hidden by the **Expand/Contract** control.

            - One or more resource-specific permission checkboxes:

              Mark the checkbox of each permission that you want to grant to users who are assigned this role.
5. Click **Create** to confirm creation of the role with the configured settings.

18.1.3 Editing a custom role

To edit a custom role:

1. At the top right of the Command Center window, click the cog wheel icon.
2. In the dropdown menu that displays, select **Roles**.
3. In the Roles screen, locate the role to edit and click its **Name**.
4. In the **Edit Role** dialog, all attributes are configurable, as described in the Defining a new custom role section.
5. Click **Update** to confirm applying the changed settings to the role.

18.1.4 Deleting a custom role

To edit a custom role:

1. At the top right of the Command Center window, click the cog wheel icon.
2. In the dropdown menu that displays, select **Roles**.
3. In the Roles screen, locate the role and click the down-arrow on its right. In the dropdown menu, select **Destroy**.
4. In the **Destroy Role** dialog, click **Confirm** to delete the role.

   On completion, the role will disappear from the list in the Roles screen.

> **Caution:** Deleting a role removes its association with any users assigned to it. Creating a new role with the same name afterward will not reassign it to the users who previously held that role.
>
> The role deletion process occurs even if there are users whose sole role assignment is the one being deleted. As a result, these users are left without a role and lose access privileges altogether, until they are assigned a new role.

CHAPTER

NINETEEN

REMOTE AUTHENTICATION

Command Center supports configuring connections to external user directory services.

After defining a connection to an external directory service, users in that directory service can be imported into Command Center and assigned relevant roles governing their access privileges. See Importing users from an external directory and Roles.

19.1 Viewing directory service connections

1. At the top right of the Command Center window, click the gear icon.
2. In the dropdown menu that displays, select **Remote Authentication**.

   The Remote Authentication screen displays the directory service connections.

Parameter	Description
Type	Directory type (currently AD LDAP is supported)
Domain	FQDN for the Domain
Alias	Short name for the domain
Port	LDAP service port
Base DN	DN for user search (format: CN=x,DN=y)
DNS	IP of the Domain DNS server
SSL	Whether to use SSL encrypted communication to the DC

19.2 Defining a directory service connection

1. At the top right of the Command Center window, click the gear icon.
2. In the dropdown menu that displays, select **Remote Authentication**.
3. In the Remote Authentication screen, click **Add Authentication Server**.
4. Configure the new directory service connection:

Parameter	Description
Type	Directory type (currently AD LDAP is supported)
Domain	FQDN for the Domain
Alias	Short name for the domain
Port	LDAP service port
Base DN	DN for user search (format: CN=x,DN=y)
DNS IP #1	IP of the Domain DNS server
DNS IP #2	Alternate DNS IP
SSL	Whether to use SSL encrypted communication to the DC

5. Click **Save**.

Important: Command Center uses the LDAP or LDAPS protocol to integrate with Microsoft Active Directory.

- LDAP connectivity occurs via port 389/TCP.
- LDAPS connectivity occurs via port 636/TCP.

CHAPTER

TWENTY

CENTRAL LOG

Command Center maintains a centralized cloud-level event log, which can be used for detailed infrastructure monitoring and troubleshooting.

Logged events can be viewed and searched from Command Center's **Central Log** option on the left navigation tree.

Events can also be exported to an external syslog daemon for 3rd party application-based event monitoring.

20.1 Searching and filtering logs

Cloud logs can be searched and specific events extracted, using the Command Center filtering functionality.

To view and search for specific content in log messages:

1. Click **Central Log** on the left navigation tree.
2. In the **Central Log** view, click in **Add Filter** to display its dropdown, and select and configure one or more filters to narrow down the log events search:
   - **Message**:
     - **Contains**: A case-insensitive string that matches searched log entries.
     - **Doesn't Contain**: Exclude log entries that match this case-insensitive string.
   - **Created**:

     From the dropdown select the log entry's creation date's relational operator:
     - **>=**: On or after date and time (inclusive). Select the date and edit the time. The search will return matching log entries created on or after the entered date and time.
     - **<**: Before date and time (exclusive). Select the date and edit the time. The search will return matching log entries created before the entered date and time.
     - **Between**: A period specified by a starting date and time, and an ending date and time. Select the start and end dates, and edit the time for each. The search will return matching log entries created on or after the starting date and time, and before the ending date and time.
   - **Min Severity**:

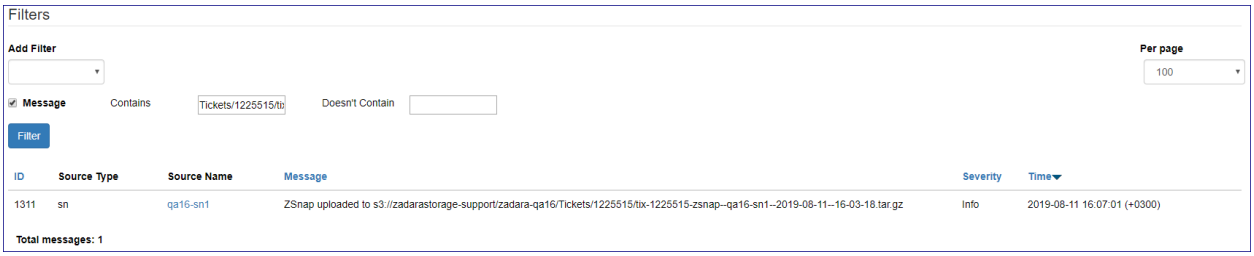
     The search will return all log entries that match the selected severity level, or have a higher severity level.

     Severity levels, listed from high to low:
     - **Emergency** - highest severity level
     - **Alert**
     - **Critical**

  - **Warning**
  - **Error**
  - **Notice**
  - **Info**
  - **Debug** - lowest severity level
- **Source type**: The component type for which the log event was generated:
  - **sn**: Storage Node
  - **vpsa**: VPSA
  - **zios**: Object Storage VPSA
  - **ccvm**: Command Center
- **Source name**: The name of the component for which the log event was generated:

  Enter only one of:
  - **Is**: The search returns only the log events for the specified component.
  - **Is not**: The search excludes the log events for the specified component, and returns all others.

3. Click **Filter**.



Note: Filter statements have a logical “and” relationship between them.

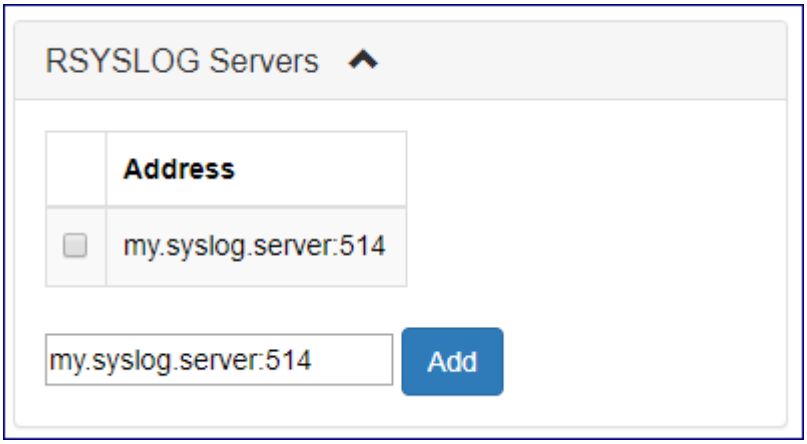
All filters are optional.

20.2 Forwarding events to a syslog daemon

To forward cloud events to an external syslog daemon:

1. Click **Central Log** on the left navigation tree.
2. Narrow down the log events to export, by Searching and filtering logs.
3. Click the **RSYSLOG Servers** caption.

   In the text box, enter the syslog server’s IP address and the syslog daemon port number, separated by a colon: `<url>:<port>`.
4. Click **Add**.



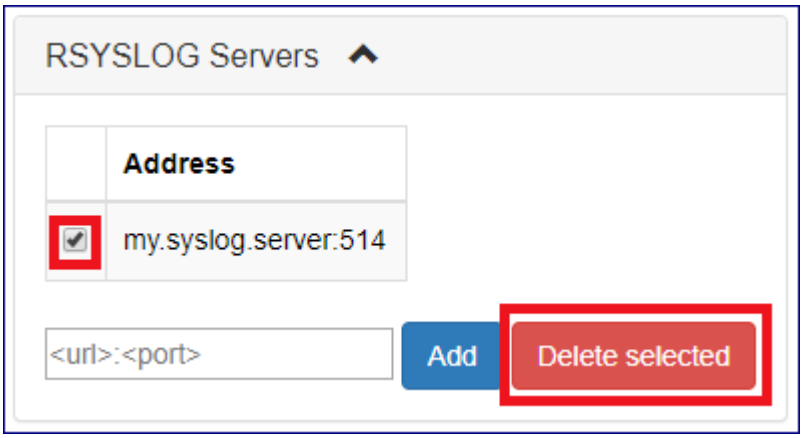
20.2.1 Stop forwarding events to a syslog daemon

To stop forwarding cloud events to a defined syslog daemon:

On the Central Log tab select click on the **RSYSLOG Servers** caption. Select the checkbox for the specific syslog daemon server you would like to remove and click the `Delete selected` button.

1. Click **Central Log** on the left navigation tree.
2. Click the **RSYSLOG Servers** caption.

   Mark the checkbox of the syslog daemon server to remove.
3. Click **Delete selected**.



CHAPTER

TWENTYONE

ACCESS LOGS

Command Center maintains centralized cloud-level Access Logs. In addition to basic information such as the accessing user and the date and time, the system also logs access details including the accessed components, actions, access type (web or API), and originating IP address.

Access Logs can be viewed and searched from the Command Center's cog wheel menu at the top right of the screen.

✔ **Note:** Unlike Command Center's Central Log, Access Logs **cannot** be exported to an external syslog daemon.

21.1 Managing Command Center Access Logs

Cloud logs can be searched and specific events extracted, using the Command Center filtering functionality.

To view and search for specific content in Access Logs:

1. At the top right of the screen, click the cog wheel.

   From the dropdown menu, select **Access Logs**.

2. In the **Access Logs** view, click in **Add Filter** to display its dropdown, and select and configure one or more filters to narrow down the Access Logs events search:

   - **Controller**: The accessed component.

     To narrow down the search to a specific controller, from the dropdown, select one of:

     - **sessions**
     - **clouds**
     - **vlans**
     - **nodes**
     - **vpsas**
     - **zioses**
     - **drive_types**
     - **images**
     - **custom_networks**
     - **drives**
     - **vfloating_ips**

  - admins
  - license_keys

- **Action**: The action peformed or attempted by Command Center on the controller.

  Note: Each controller has a set of possible actions, and each action is associated with only one controller.

  - If a controller is specified for the search, from the dropdown, optionally select one of the actions of that controller to narrow the search.
  - If a controller is not specified for the search, selecting an action from the dropdown effectively narrows the search to logged events of the action and its implied controller.

- **Access Type**: The access method.

  To narrow down the search to a Access Type, from the dropdown, select one of:

  - **Web**: Access requests originating from a web browser.
  - **API**: Access requests originating from an application API.

- **IP Address**: The IP address from which the access request originated.

  To narrow down the search to a specific IP address, enter the IP address in the text box.

  Note: Only a single IP address can be entered as a filter. Wildcards and CIDRs are not valid entries.

- **User**: The username of the user who triggered the access request.

  To narrow down the search to a specific user, from the dropdown, select the user.

- **Created**:

  From the dropdown select the log entry's creation date's relational operator:

  - **>=**: On or after date and time (inclusive). Select the date and edit the time. The search will return matching log entries created on or after the entered date and time.
  - **<**: Before date and time (exclusive). Select the date and edit the time. The search will return matching log entries created before the entered date and time.
  - **Between**: A period specified by a starting date and time, and an ending date and time. Select the start and end dates, and edit the time for each. The search will return matching log entries created on or after the starting date and time, and before the ending date and time.

3. Click **Filter**.

The **Params** column displays a JSON string specifying the performed or attempted event's parameters and their values.


Filters
Add Filter
Per page
100
Action
Is
change_engine_type
Created
>=
2019-08-06 00:00
Filter
Clear
User
Controller
Action
Source
Ip
Params
Created at
qa@zadarastorage.com
vpsas
change_engine_type
Web
127.0.0.1
{"app_engine_type": "None", "when": "", "cloud_id": "zadaraqa16", "id": "vsa-00000004", "engine_type_from": {"name": "1600", "type": "vsa.V2.1600.vf", "ram": "34816", "vcpus": "8"}, "engine_type_to": {"name": "2400", "type": "vsa.V2.2400.vf", "ram": "51200", "vcpus": "12"}, "name": "VPSA_NVMe_Performance", "internal_name": "vsa-00000004"}
2019-08-15 21:32:16
qa@zadarastorage.com
vpsas
change_engine_type
Web
127.0.0.1
{"app_engine_type": "xlarge", "when": "", "cloud_id": "zadaraqa16", "id": "vsa-00000002", "engine_type_from": {"name": "F3600", "type": "vsa.V3.large.vf", "ram": "90112", "vcpus": "18"}, "engine_type_to": {"name": "F4800", "type": "vsa.V3.xlarge.vf", "ram": "120832", "vcpus": "24"}, "name": "Liran_Weekend", "internal_name": "vsa-00000002"}
2019-08-08 11:29:00
qa@zadarastorage.com
vpsas
change_engine_type
Web
127.0.0.1
{"app_engine_type": "xlarge", "when": "", "cloud_id": "zadaraqa16", "id": "vsa-00000002", "engine_type_from": {"name": "F4800", "type": "vsa.V3.xlarge.vf", "ram": "120832", "vcpus": "24"}, "engine_type_to": {"name": "F3600", "type": "vsa.V3.large.vf", "ram": "90112", "vcpus": "18"}, "name": "Liran_Weekend", "internal_name": "vsa-00000002"}
2019-08-06 20:28:45
Total logs: 3