

zadara

Command Center Administrator Guide

Release 23.09-SP1

Zadara

Jun 06, 2024

CONTENTS

| | | |
|----|--|-----|
| 1 | Introduction | 1 |
| 2 | Architecture | 3 |
| 3 | Understanding Command Center Main Dashboard | 5 |
| 4 | Managing Storage Nodes | 9 |
| 5 | Managing VPSAs | 25 |
| 6 | Managing Object Storage VPSAs | 47 |
| 7 | Managing Physical Drives | 57 |
| 8 | Viewing Engine Properties | 63 |
| 9 | Managing Cloud Networking | 67 |
| 10 | Creating Public IP Addresses | 75 |
| 11 | Managing Data Services | 77 |
| 12 | Performing Image Management | 83 |
| 13 | Customizing VPSA And Object Storage User Interface | 87 |
| 14 | Managing Command Center Users And Roles | 89 |
| 15 | Managing Cloud Settings | 99 |
| 16 | Managing Cloud Logs | 117 |
| 17 | Using Comments In Command Center | 121 |

INTRODUCTION

1.1 Intended Audience

This document is intended for Storage Administrators of the Zadara Storage Cloud who are responsible for managing the cloud and providing Enterprise Storage-as-a-Service via the Zadara Storage VPSA service.

1.2 Zadara Storage Command Center

1.2.1 Overview

Zadara Storage Cloud was architected 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 policies 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 nodesdisk drives)
- Perform cloud user management
- Perform cloud level license key management
- View a detailed Central-Log of all cloud elements

1.2.2 Terminology

| Item | Description |
|---------------------------------|--|
| SN | Storage Node. Commodity server with large number of CPU cores (typically 16 or more) and large RAM (typically 64GB or more), connected to 10Gb/40Gb data network with Intel/Mellanox SRIOV NICs & 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 |
| VPSA Object Storage | Zadara Intelligent Object Store. Redundant, Durable, Highly Available virtual object store cluster that has resources (CPU, memory, network, disks) provisioned |
| 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/VPSA 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/VPSA Object Storage with intelligent scheduler, monitoring, and provisioning networking/storage for VPSA/VPSA Object Storage etc.) |
| Command Center | 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. 10Gb/40Gb network through which Application Servers can connect to Zadara VPSA Storage for IO and Control |
| BE Network | Back-End network. 10Gb/40Gb 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 could have multiple users/logins, but they all could belong to same tenant |
| QoS | Quality of Service - Defines Performance/Reliability characteristics of a service |

ARCHITECTURE

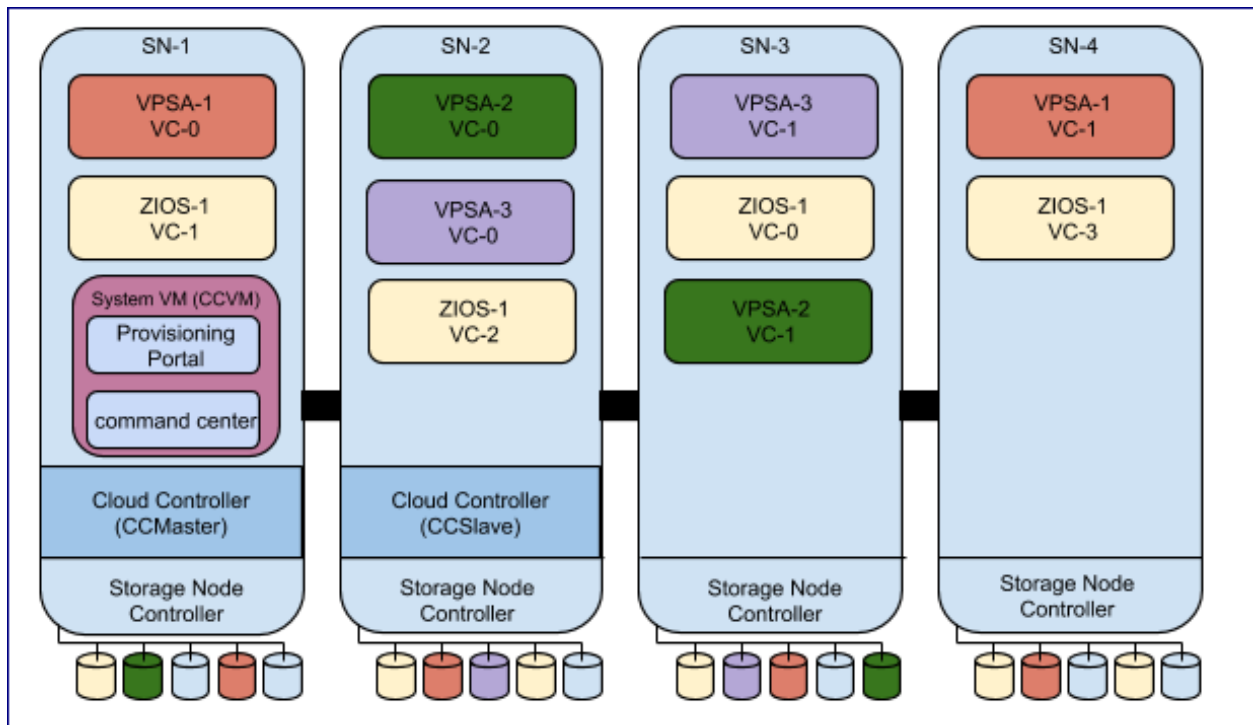
2.1 Cloud Management Software Deployment

The Zadara cloud contains two storage nodes which are assigned to the roles of Cloud controller master(or ccmaster) and Cloud controller slave(or ccslave). CCmaster/CCslave Storage nodes 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(or ccvm). In case of any failure in the cloud controller master node a fail over 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 .



Provisioning portal can also be deployed on any cloud application platform such as Heroku. This topology should be deployed when there is a need to manage multiple clouds in multiple regions in a single portal.

✓ **Note:**

- The cloud controller virtual machine supports both IPv4 and IPv6 for its frontend address.

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.

UNDERSTANDING COMMAND CENTER MAIN DASHBOARD

3.1 Accessing Command Center

To Access command center open you web browser and navigate to the following URL: <http://your-ccvm-hostname:8888>

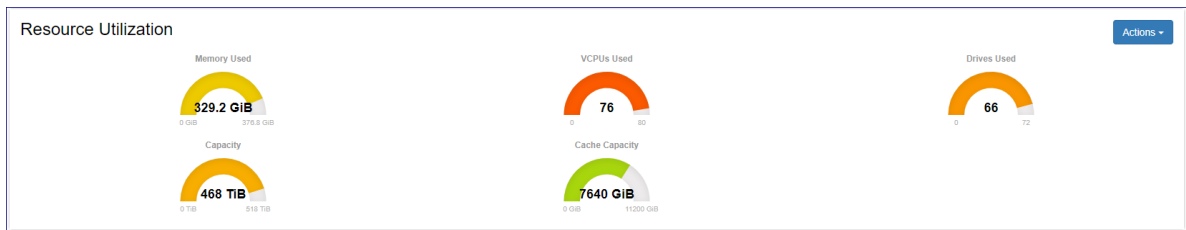
In case of first login the cloud administrator user credentials will be provided by Zadara operation after cloud installation. Additional user-ids can be created by the cloud administrator and will receive temporary credentials for initial login via their provided e-mail address.

3.2 Command Center Dashboard Overview

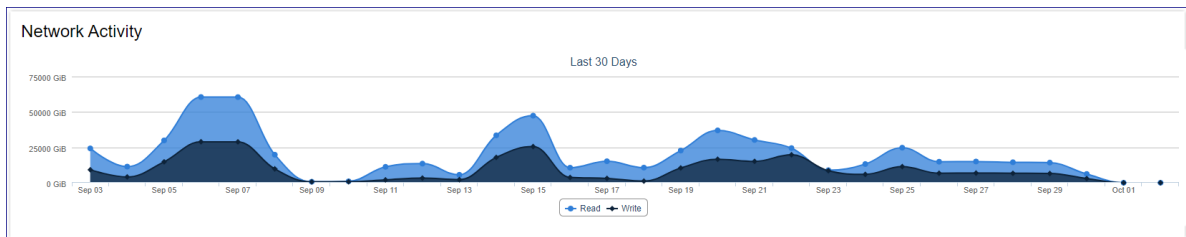
Command centers main dashboard was designed to provide Zadara cloud administrators with a centralized viewpoint on their cloud utilization and to perform cloud level operations.

The dashboard is built out of 4 main panels - each monitoring a different key aspect of the cloud infrastructure:

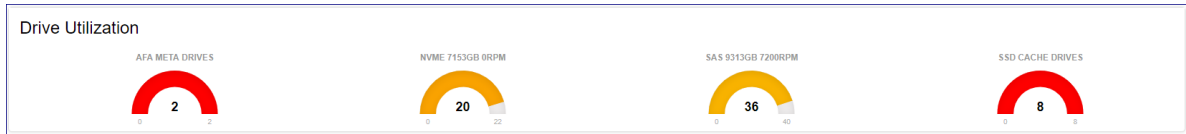
- The resource utilization panel provides a birds eye view on the core cloud resources utilization such as : vcpus, memory, disks etc.



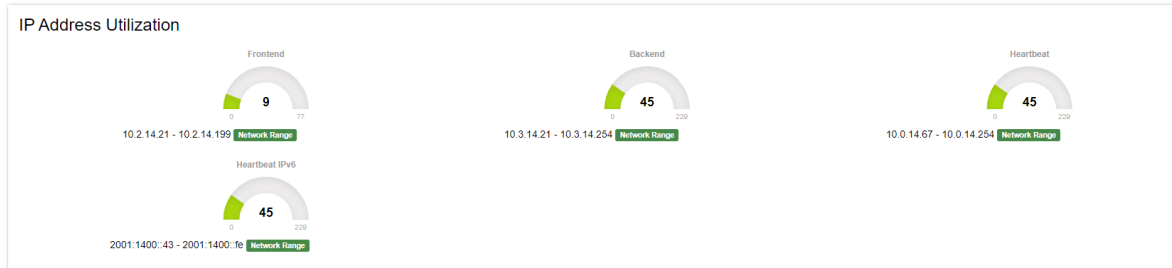
- The Network Activity panel provides monitoring data for real time network throughput and utilization.



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



- The IP address Utilization panel displays the defined IP ranges for frontend, Backend and heartbeat networks and the level of allocation per each.



✓ **Note:** These networks are predefined with fixed ranges of IP addresses and cannot be overlapped with VPSA virtual networks.

3.3 Performing Cloud Level Operations

Creating a CCVM Zsnap

To create a zSnap of the cloud controller virtual machine navigate to command centers dashboard, click on the **Actions** button and select create CCVM zSnap from the drop down menu. On the popup dialog that will appear provide a prefix for the zSnap and click on the **Create zSnap** button to confirm creation.

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 elements listed above or any subset of them can be upgraded in a single workflow.

To perform cloud version upgrade navigate to command centers dashboard, click on the **Actions** button and select Upgrade from the drop down menu. On the cloud upgrade dialog that will appear check 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**.

Upgrade cloud

Please select version to install on **zadara-qa16**:

19.08-169 ▼

Please select what to upgrade:

- Storage Nodes - Core
- Storage Nodes - Utilities
- VPSAs
- Object Storage
- CCVM

Advanced ▼

- Skip Object Storage Health checks


Cancel Upgrade

✓ **Note:**

The recommended procedure for cloud upgrade is to perform SN (software + Utilities) and CCVM upgrade in a single workflow and perform VPSA/VPSA Object storage instances upgrade after successful completion of the first workflow.

To confirm the upgrade process click on the **Upgrade** button.

During cloud upgrade processing the Command Center Dashboard will present the upgrade workflow and status per all stages.

| Operation In Progress | | Time | Step | State | Progress | Comment |
|-----------------------|---|------------------------|---|-------|--|--|
| Operation | Cloud Upgrade | | | | | |
| Status | In progress  Abort | 2019/10/02 14:18:42 | register_images | start | Phase: Registering [CCVM] Images in pkg[19.08-169] - (Sub Phase Registering [CCVM] Images for [19.08-169] in Glance) | Register VC/CCVM Images |
| Components | ccvm,snutils,sns | | | | | |
| Package | 19.08-169 | | | | | |
| | | 2019/10/02 13:20:09 | check_sn_cpu_overprovision_and_vsa_zone_map | ok | | Complete |
| | | 2019/10/02 13:20:08 | check_sn_cpu_overprovision_and_vsa_zone_map | start | Phase: Checking if any SN has CPU/Memory overprovisioned before upgrade - Done | Check SN CPU overprovision status & VSA Zone Mapping |
| | | 2019/10/02 13:20:06 | sanity_check_for_outgoing_inet_network | ok | | Complete |
| | | 2019/10/02 13:20:06 | sanity_check_for_outgoing_inet_network | start | | Sanity Check For Outgoing Internet Network |
| | | 2019/10/02 13:20:06 | restart_installer | ok | | Complete |
| | | 2019/10/02 13:20:06 | restart_installer | start | | Restart Installer |
| | | 2019/10/02 13:20:04 | upgrade_installer | ok | | Complete |
| | | 2019/10/02 13:20:04 | upgrade_installer | start | Phase: Cloud Install Packages [Upgrading Installer - zadara-installer_19.08-169_amd64.deb] - Done | Upgrade Installer on SNS |
| | | 2019/10/02 13:19:50 | check_sns_are_in_normal_state | ok | | Complete |
| | | 2019/10/02 13:19:49 | check_sns_are_in_normal_state | start | | Cloud Upgrade pre-check SN State |
| | | 2019/10/02 13:19:49 | package_validations | ok | | Complete |
| | | 2019/10/02 13:19:48 | package_validations | start | | Package Validations |
| | | 2019/10/02 13:19:48 | download_pkg | ok | | Complete |
| | | 2019/10/02 13:19:47 | download_pkg | start | | Download package |

✔ **Note:**

During SN software upgrade ccmaster failover will be performed. At this period CCVM will reboot and Command center will not be available until reboot is finished - same for CCVM version upgrade.

When upgrade workflow is finished completion will be indicated on the command center dashboard.

Last log Clear Log

| | |
|-------------------|------------------|
| Operation | Cloud Upgrade |
| Status | Completed |
| Components | ccvm,snutils,sns |
| Package | 19.08-169 |

MANAGING STORAGE NODES

One of Command center's key roles is to enable Cloud infrastructure management in which storage nodes are a core component. Command center provides comprehensive management and monitoring capabilities for the cloud's storage nodes including all aspects of:

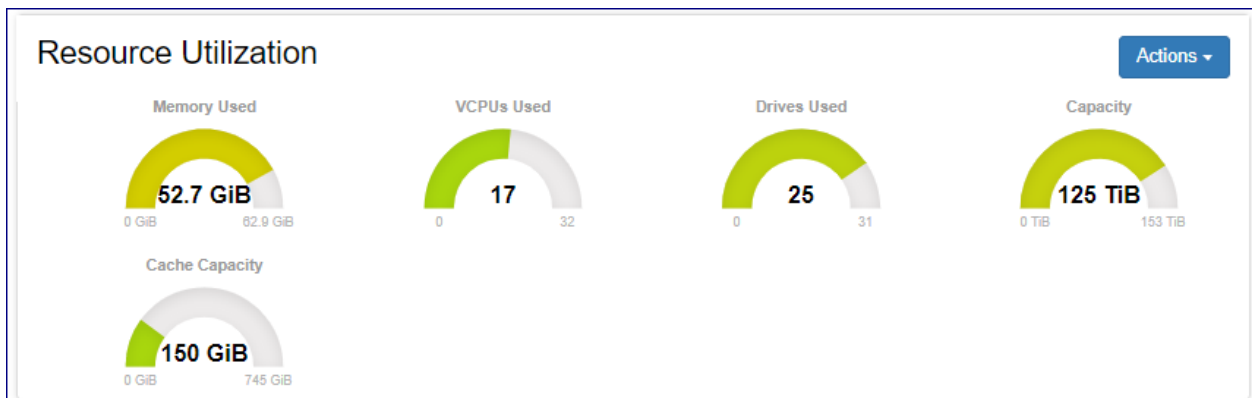
- Ongoing maintenance
- Upgrade managing
- Hardware addition and retirement
- Health checks
- Performance monitoring

4.1 Understanding The Storage Node Dashboard

The storage node dashboard presents information regarding its configuration, status and resource utilization. The dashboard can be reached by clicking on Storage Nodes from Command center left menu panel and then selecting a specific storage node from the cloud inventory and clicking on it. The storage node dashboard contains multiple panels each providing information on a specific aspect of the SN configuration and status:

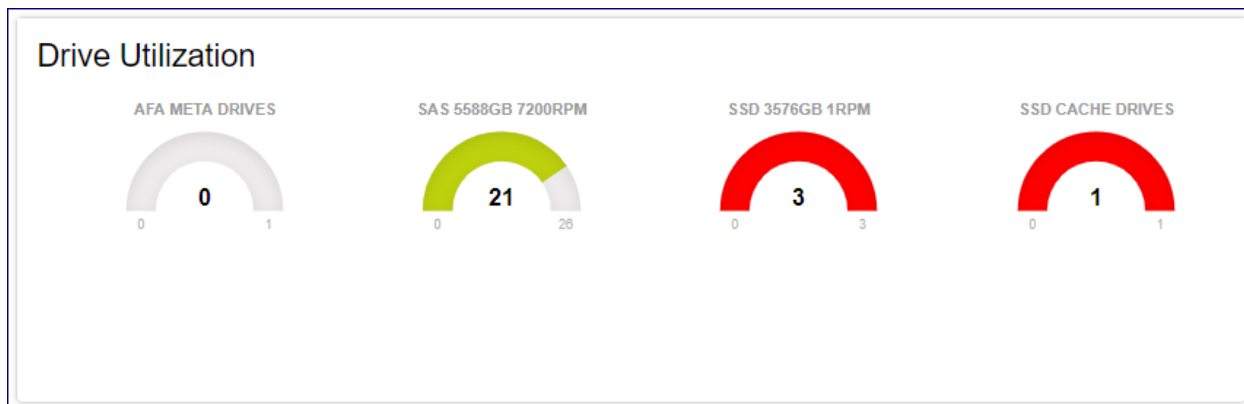
Resource Utilization

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



Drive Utilization

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



services

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

| Services | | |
|----------------|------------|---------------------------|
| zadara-radiusd | 1.3.0-1 | Online |
| zadara-sn | 19.08-158 | Online |
| drbd | 2:8.9.10-2 | Standby/uptodate/uptodate |
| nova-compute | 19.08-158 | Online |
| nova-volume | 19.08-158 | Online |

In case that some services on the storage node are not in normal status those specific services will also be indicated by a tooltip on the cloud storage nodes grid.

| Name | Status | Protection Zone |
|----------------------------|--------|-----------------|
| qa6-sn1.qa.lab CCSlave | Normal | zone_0 |
| qa6-sn2.qa.lab CCMaster | Normal | zone_0 |

Service zadara-radiusd is offline (expected: online)
 Service zadara-sn is offline (expected: online)
 Service drbd is offline (expected: Standby/uptodate/uptodate)
 Service nova-compute is offline (expected: online)
 Service nova-volume is offline (expected: online)

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 |

Network

Displays SN networks and configured IP addresses.

Network

| | IP | MAC |
|---------------|-------------|-----------------|
| FE | 172.49.224. | c6:57:b1:99:e7: |
| BE | 172.49.228. | e2:5f:ab:ba:e8: |
| HB | 172.49.232. | 0c:c4:7a:6e:99: |
| External mgmt | 192.168.13. | 0c:c4:7a:6e:99: |
| IPMI | | |

Resource Scheduling

Display information regarding the availability of the Sn resources(VCPUs and disk drives) To be allocated for newly provisioned VPSA/VPSA Object Storage entities by the clouds orchestration framework.

Resource Scheduling

| | | |
|------------------|----------|-------------------------|
| Drive Scheduling | Disabled | Enable |
| VC Scheduling | Enabled | Disable |

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

Device information

| | |
|---------------------|--|
| Pci Address | 0000:81:00.0 |
| General Info | Mellanox Technologies MT27520 Family [ConnectX-3 Pro] |
| Interfaces | eth10G1 [7c:fe:90:93:3e:90], eth10G2 [7c:fe:90:93:3e:91] |
| Roles | BE, FE |
| Firmware | 2.33.8000 |
| Speed | 40000 Mb/s |
| Product Name | CX314A - ConnectX-3 Pro QSFP |
| Part Number | MCX314A-BCCT |

[Close](#)

✓ Note:

Mellanox ConnectX-5 dual port NICs will be presented as 2 sperate network adapters due to having 2 different PCI addresses.

CPU information

Displays information on the SNs processors.

CPU Information

| | 0 | 1 |
|------------------------|---|---|
| Physical ID | 0 | 1 |
| Model Name | Intel(R) Xeon(R) CPU E5-2630 v3 @ 2.40GHz | Intel(R) Xeon(R) CPU E5-2630 v3 @ 2.40GHz |
| CPU Cores | 8 | 8 |
| CPU Speed (Mhz) | 2600 | 2586 |
| Cache Size | 20480 KB | 20480 KB |

License information

Displays SN licensing information.

| License Refresh | | | | |
|--|--------|---------|------------------|-----------------|
| Key | Status | Expires | Installed Drives | Licensed Drives |
| XQXUU-XJDP4-QPKOL-43ADP-XQXUU | Active | Never | 31 | Unlimited |

Storage Adapter

Displays information on the SN internal RAID adapter.

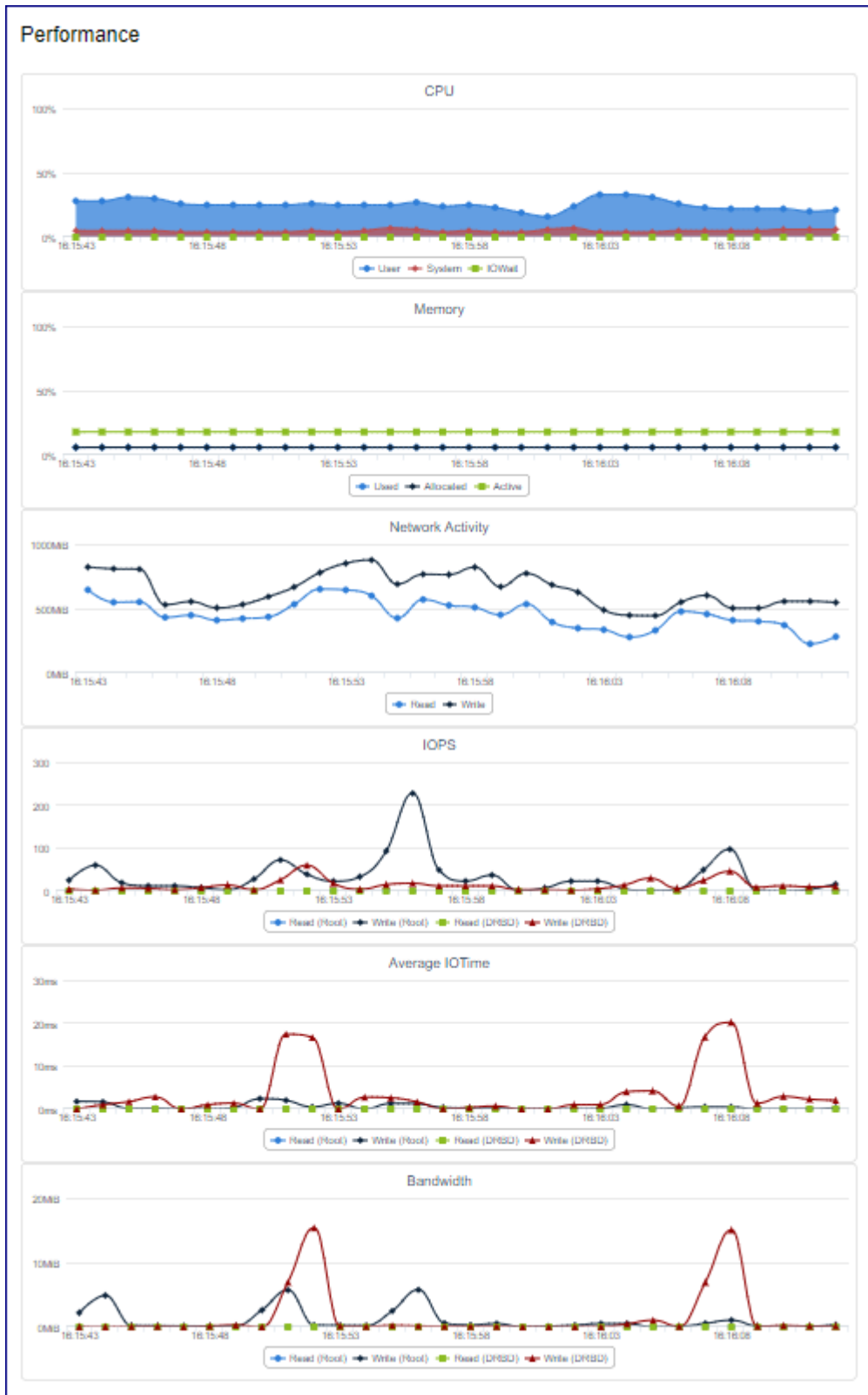
| Storage Adapter Information | |
|-----------------------------|---------------------|
| Adapter # | 0 |
| Product Name | AVAGO 3108 MegaRAID |
| Current FW Version | 24.21.0-0028 |
| Target FW Version | None |
| FW Upgrade Required | no |

4.2 Monitoring Storage Node Performance

Command center provides a real time monitoring framework for storage node performance. Monitoring is available from the Performance in tab in the specific VPSA.

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



Monitoring interval can be changed supported intervals are : 1sec, 10sec, 1min, 1hr and 1day. Interactively refreshed charts can be triggered by pushing the Auto refresh button.

4.3 Performing Storage Node Operations

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

Any changes made in the SN scheduling policy are immediately applied.

Creating storage node Zsnap

To Trigger Manual creation of Zsnap for a storage node go to its dashboard, click the **Actions** button and select Create Zsnap from the drop down menu. On the popup dialog that will appear provide the prefix for the Zsnap and confirm creation by clicking on the **Create Zsnap** button.

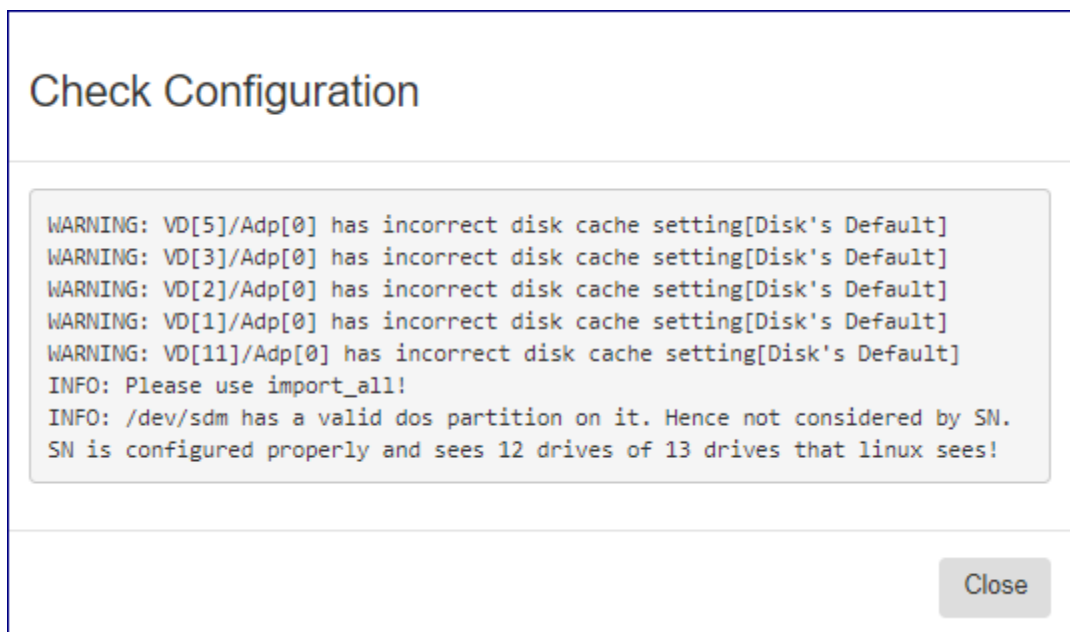
Install and import new drives in a storage node

Cloud storage capacity expansion is performed by installing drives into the storage node importing the newly installed drives into the SN. The import operation encapsulates hardware discovery and SN\cloud inventory update. To perform import of newly installed physical drives select the SN to which drives were installed, click on the **Actions** button and select Import Drives. On the popup dialog that will appear confirm the import operation by clicking on the **Confirm** button. 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.



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 select the SN to which drives were installed click on the **Actions** button and select **Check Configuration**. On the popup dialog that will appear confirm the import operation by clicking on the **Confirm** button. The configuration check will be immediately performed and its output displayed on a new popup dialog.



Performing storage node version upgrade

Storage node Version upgrade can be performed as part of a complete cloud upgrade workflow from Command centers main dashboard or from the Storage Node dashboard. Upgrade done 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 navigate to the appropriate SN, click on the **Actions** button and select Upgrade Version. On the popup dialog that will appear select the software version you would like to upgrade your SN to and click on **Upgrade** to confirm the process.

✓ Note:

Versions marked by asterisk are available but not downloaded to the cloud. Upgrade to those version requires package download and registration beforehand.

During the SN upgrade process status will be displayed on Command center main dashboard, The upgraded Storage node services panel will present all services as offline.

| Operation In Progress | | | | | | |
|-----------------------|--|---------------------|---|-------|---|--|
| Operation | sn_upgrade | Time | Step | State | Progress | Comment |
| Status | In progress Abort | 2019/10/06 09:30:57 | upgrade_sn | start | Phase: Starting upgrade on [sn-03] with role[ccmaster] - (Sub Phase: Staging Package[19.08-169] for Upgrade!) | Upgrade SN |
| Details | Params: {"pkg":"19.08-169","sn_uname":"sn-03"} | 2019/10/06 09:30:46 | check_and_failover | ok | | Complete |
| | | 2019/10/06 09:30:45 | check_and_failover | start | | Check if target SN is CCMaster/failover |
| | | 2019/10/06 09:30:45 | check_sn_cpu_overprovision_and_vsa_zone_map | ok | | Complete |
| | | 2019/10/06 09:30:45 | check_sn_cpu_overprovision_and_vsa_zone_map | start | Phase: Checking if any SN has CPU/Memory overprovisioned before upgrade - Done | Check SN CPU overprovision status & VSA Zone Mapping |
| | | 2019/10/06 09:30:42 | sanity_check_for_outgoing_inet_network | ok | | Complete |
| | | 2019/10/06 09:30:42 | sanity_check_for_outgoing_inet_network | start | | Sanity Check For Outgoing Internet Network |
| | | 2019/10/06 09:30:42 | restart_installer | ok | | Complete |
| | | 2019/10/06 09:30:42 | restart_installer | start | | Restart Installer |
| | | 2019/10/06 09:30:41 | upgrade_installer | ok | | Complete |
| | | 2019/10/06 09:30:41 | upgrade_installer | start | Phase: SN Install Packages [Upgrading Installer - zadara-installer_19.08-169_amd64.deb] - Done | Upgrade Installer on SN |
| | | 2019/10/06 09:30:36 | package_validations | ok | | Complete |
| | | 2019/10/06 09:30:35 | package_validations | start | | Package Validations |
| | | 2019/10/06 09:30:35 | download_pkg | ok | | Complete |
| | | 2019/10/06 09:30:35 | download_pkg | start | | Download package |

| Services | | |
|----------------|---------------|----------------------|
| zadara-radiusd | 1.3.0-1 | Offline |
| zadara-sn | 19.08-169 | Offline |
| drbd | 2:8.9.2~rc1-3 | Offline |
| nova-compute | 19.08-169 | Offline |
| nova-volume | 19.08-169 | Offline |

When the Storage node upgrade is finished completion will be indicated on the Command center dashboard.

| Last log Clear Log | |
|---------------------------------|--|
| Operation | sn_upgrade |
| Status | Completed |
| Details | Params: {"pkg":"19.08-169","sn_uname":"sn-03"} |

Performing storage node utilities version upgrade Storage Node utilities can be upgraded in a dedicated process via Command centers SN dashboard. To upgrade Storage node utilities navigate to the appropriate SN, click on the **Actions** button and select Upgrade Utilities. On the popup dialog that will appear select the utilities version you would like to upgrade your SN to and click on **Upgrade** to confirm the process.

Note:

Versions marked by asterisk are available but not downloaded to the cloud. Upgrade to those version requires package download and registration beforehand.

During the Utilities upgrade process status will be displayed on Command center main dashboard.

| Operation In Progress | | | | | | |
|-----------------------|---|------------------------|---------------------|-------|--|---------------------|
| Operation | snutils_upgrade | Time | Step | State | Progress | Comment |
| Status | In progress Abort | 2019/10/06 11:22:00 | upgrade_snutils | start | Phase: SN Install Packages [Upgrading SNUtils - zadara-snutils_19.08-169_amd64.deb] | Upgrade SNUtils |
| Details | Params: {"pkg":"19.08-169","sn_uname":"sn-03"} | 2019/10/06 11:21:59 | package_validations | ok | | Complete |
| | | 2019/10/06 11:21:59 | package_validations | start | | Package Validations |

When the Storage node utilities upgrade is finished completion will be indicated on the Command center dashboard.

Last log
Clear Log

| | |
|------------------|--|
| Operation | snutils_upgrade |
| Status | Completed |
| Details | Params: {"pkg":"19.08-169","sn_uname":"sn-03"} |

Performing upgrade of 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 supported levels.

To update Drive\RAID controller firmware for a Storage node navigate to the required node dashboard, click on the **Actions** button and select Upgrade Drives & Adapter Firmware. On the popup dialog that will appear select the elements you would like to perform FW upgrade for, available options are : Disk drives, Intel Optane drives and RAID controller. In case of Disk drives or Intel Optane drives FW upgrade : all disk drives and virtual controllers running on the SN will be taken offline.

Upgrade Drives & Adapter Firmware

- SN will move temporarily to maintenance mode.
During maintenance mode, all virtual controllers and drives on this node will go offline.

NOTE: Upgrade will be possible only if all VPSAs are in normal state.
Upgrade will be possible only if there are no active VCs on the upgraded storage node.

Please select component(s) to upgrade on **sn-03**

- Drives Firmware
 - Upgrade Optane Drives Firmware
- MegaRaid Firmware

Are you sure you want to upgrade drives & Adapter Firmware on node **sn-03**?
Please type the word **UPGRADE** in the field below:

In case of RAID controller FW upgrade the SN will reboot after FW is installed.

Upgrade Drives & Adapter Firmware

- SN will move temporarily to maintenance mode.
During maintenance mode, all virtual controllers and drives on this node will go offline.

NOTE: Upgrade will be possible only if all VPSAs are in normal state.
Upgrade will be possible only if there are no active VCs on the upgraded storage node.

Please select component(s) to upgrade on **sn-03**

Drives Firmware

Upgrade Optane Drives Firmware

MegaRaid Firmware

- SN Will be rebooted after completing maintenance mode operations.

Are you sure you want to upgrade drives & Adapter Firmware on node **sn-03**?
Please type the word **UPGRADE** in the field below:

Cancel
Upgrade

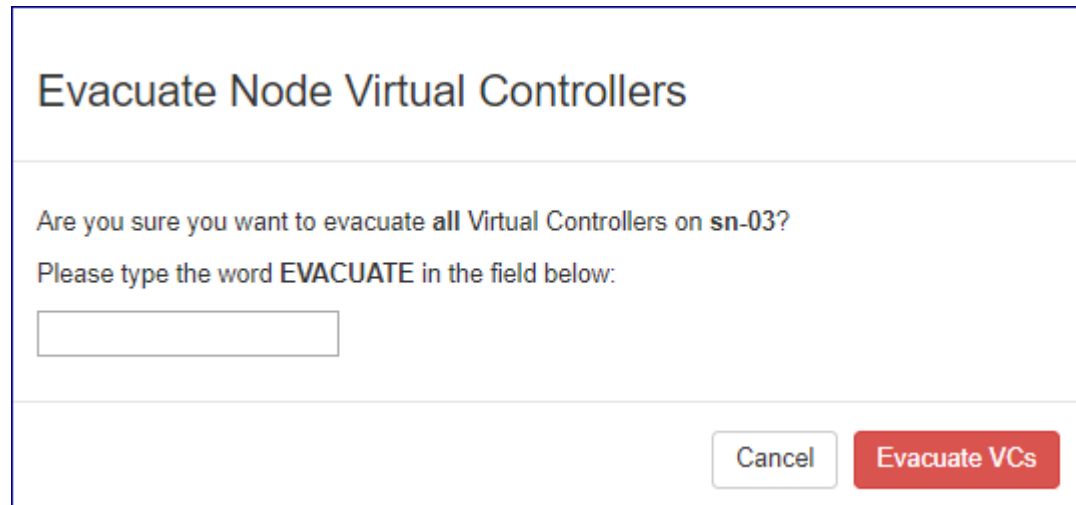
To confirm upgrade type “UPGRADE” in the text box as required and click on the **Upgrade** button.

The firmware upgrade process status will be displayed on Command center main dashboard. Completion will be also indicated on the Command Centers main dashboard.

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 in preparation for performing activities such as hardware maintenance or refresh.

To evacuate all virtual controllers from a storage note navigate to its dashboard, click on the **Actions** button and select **Evacuate Virtual Controllers**.



Evacuate Node Virtual Controllers

Are you sure you want to evacuate **all** Virtual Controllers on **sn-03**?

Please type the word **EVACUATE** in the field below:

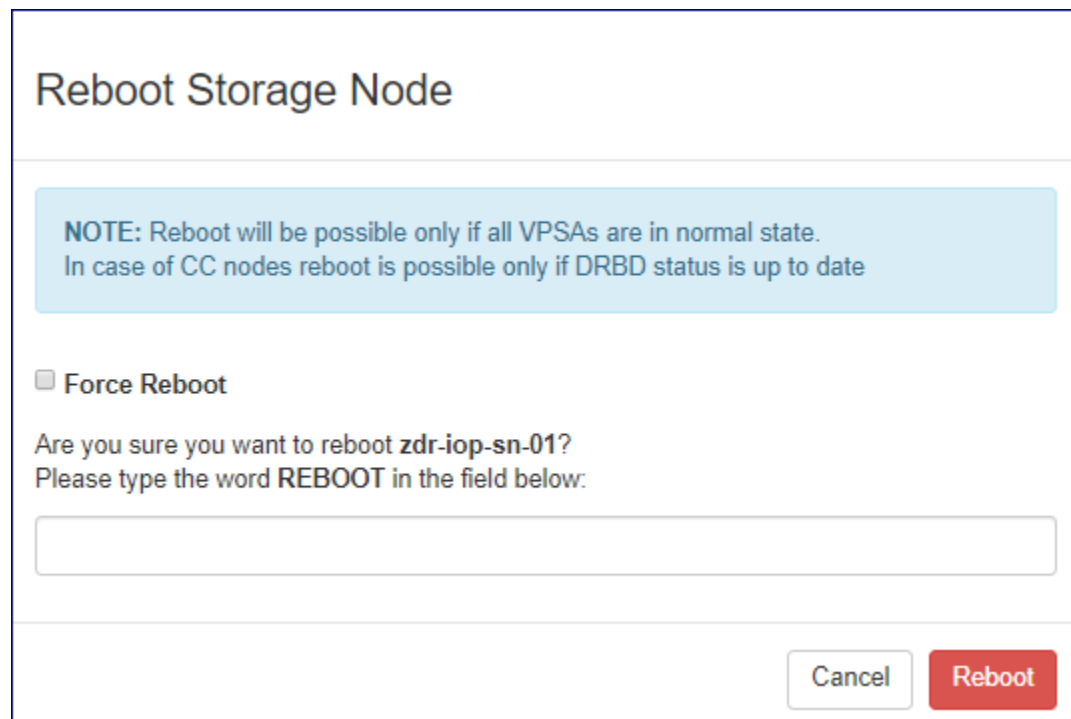
On the popup dialog that will appear type “EVACUATE” and click on **Evacuate VCs** to confirm the operation.

✓ **Note:**

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

Reboot a storage node

To reboot a Storage node navigate to its dashboard **Actions** button and select **Reboot**.



Reboot Storage Node

NOTE: Reboot will be possible only if all VPSAs are in normal state.
In case of CC nodes reboot is possible only if DRBD status is up to date

Force Reboot

Are you sure you want to reboot **zdr-iop-sn-01**?

Please type the word **REBOOT** in the field below:

On the popup dialog that will appear confirm the reboot operation by typing **reboot** on the textbox as requested and clicking on the **Reboot** button.

✓ Note:

Storage Node reboot will be performed only if all underlying VPS/ VPSA Object storage instances status is Normal.

A reboot of CCmaster\CCslave will be performed only if the DRBD service is up to date.

The restrictions noted above can be overridden by checking the Force reboot option. When using Force reboot option the cloud administrator is considered responsible of verifying and validating the VPSA/DRBD status before rebooting.

Shutdown a storage Node To shut down a Storage node navigate to its dashboard **Actions** button and select Shutdown.

Shutdown Storage Node

NOTE: Shutdown will be possible only if all VPSAs are in normal state.
In case of CC nodes shutdown is possible only if DRBD status is up to date

Force Shutdown

Are you sure you want to shutdown **zdr-iop-sn-01**?
Please type the word **SHUTDOWN** in the field below:

On the popup dialog that will appear confirm the reboot operation by typing reboot on the text box as requested and clicking on the Shutdown button.

✓ Note:

Storage Node shutdown will be performed only if all underlying VPS/ VPSA Object storage instances status is Normal.

A shutdown of CCmaster\CCslave will be performed only if the DRBD service is up to date.

The restrictions noted above can be overridden by checking the Force Shutdown option. When using the Force Shutdown




option the cloud administrator is considered responsible of verifying and validating the VPSA/DRBD status before shutting down the SN.

MANAGING VPSAS

Virtual private storage array instances running in the cloud can be centrally managed and monitored by cloud admins from Command center. Command center VPSA management feature set provides administrators with a single pain of glass in which the receive a holistic image of the underlying instances status and operations and allows for enforcements of policies, lifecycle management and supervised resource distribution.

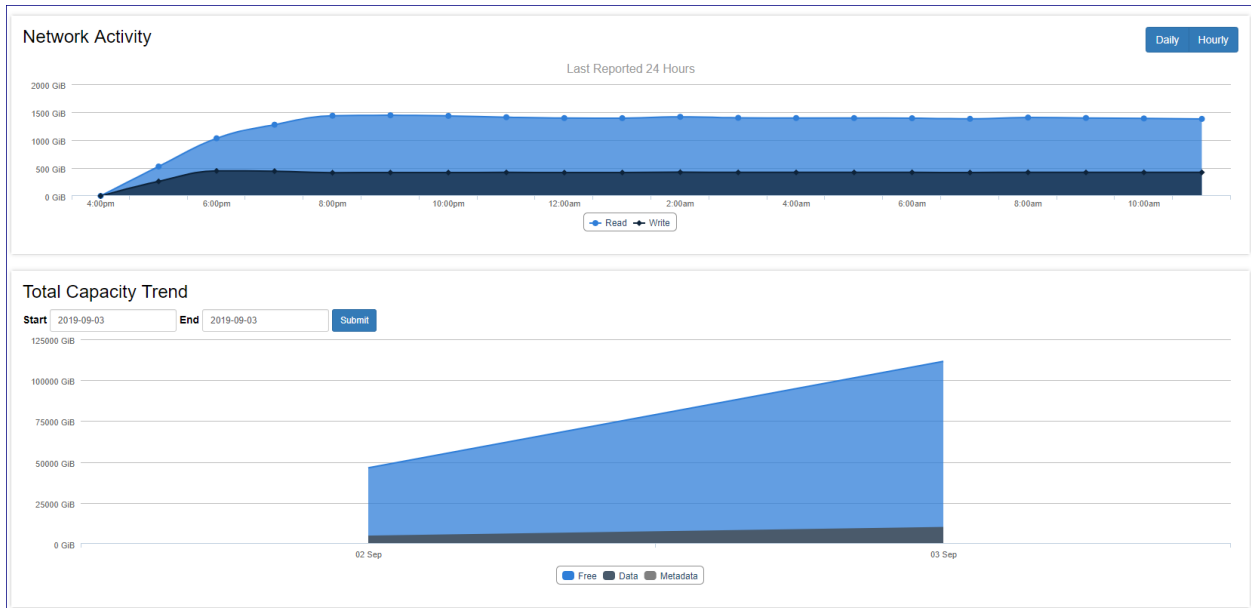
5.1 Viewing Virtual Private Storage Array Properties

Specific VPSAs can be reached by clicking on the VPSAs label on Command centers left menu panel and selecting the appropriate Instance from the displayed list. The VPSA main dashboard tab provides information regarding its configuration, current health status and network topology.

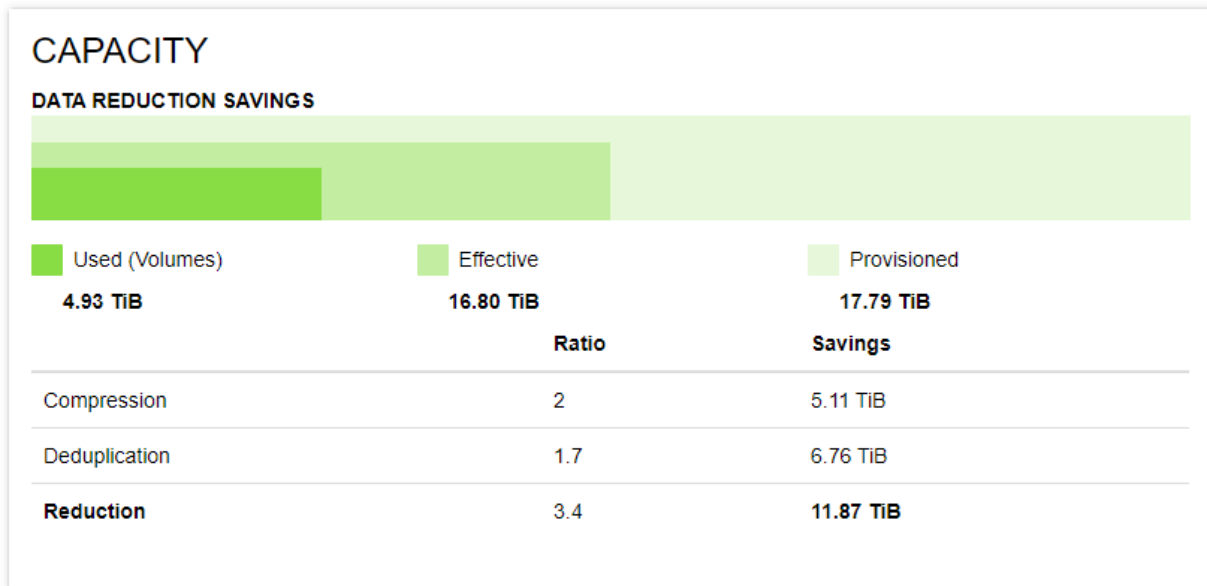
| Information | | Launch GUI  | Actions  |  |
|-----------------------|--|--|---|---|
| Name | DEVSTACK_IPV6 | | | |
| Internal Name | vsa-00000029 | | | |
| User | pdm (Product Management) | | | |
| Company | Zadara | | | |
| Description | | | | |
| Nova ID | vsa-00000029 | | | |
| Status | Normal | | | |
| Protection Zone | Primary | | | |
| Image | vc-20.01-127-qa.img | | | |
| IO Engine Type | 200 | | | |
| APP Engine Type | 00 | | | |
| VCPUs | 2 | | | |
| RAM | 6144 MB | | | |
| Base Cache | 20 GiB | | | |
| Extended Cache | 0 GiB | | | |
| Setup Volume Capacity | 10 GiB | | | |
| IP Address | 2001:db8:85a3::8a2e:370:7002 | | | |
| Public IP | None | | | |
| Mgmt. Address | vsa-00000029-zadara-iop-01.zadaravpsa.com | | | |
| UUID | 2990c33e-9cd6-4222-bbc2-cdd3f137e734 | | | |
| SNMPv3 Engine ID | 8000aa8c052990c33e9cd64222bbc2cdd3f137e734 | | | |
| Created | January 20, 2020 10:28 AM (17 days ago) | | | |
| Updated | a few seconds ago | | | |

| Property | Description |
|-----------------------|--|
| Name | Instance display name |
| Internal Name | internal instance name |
| Company | Creating user company |
| Description | Description given while instance was provisioned |
| Nova ID | Nova ID for this instance |
| Status | Current Instance status |
| 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 EngineID |
| Created | Creation timestamp |
| Updated | Last update timestamp |

The main dashboard also contains monitoring charts regarding the VPSA capacity utilization and Network activity.



For VPSA Flash array the main dashboard also contains a data reduction savings chart presenting used capacity vs. provisioned and effective capacity. The Flash Array Data reduction tile also includes information about savings from inline data deduplication and inline data compression and the VPSA overall data reduction ratio.




The VPSA resource tabs provides 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.

The VPSA Pools tab contains pool capacity consumption trend charts that provides cloud administration with an overview of the pools capacity change over time and the effect of data reduction mechanisms such as deduplication and compression on all flash VPSA pools. To present the capacity trend for a specific pool navigate to the VPSA pools tab, select the required pool and click on the relevant chart icon on the capacity trend column.

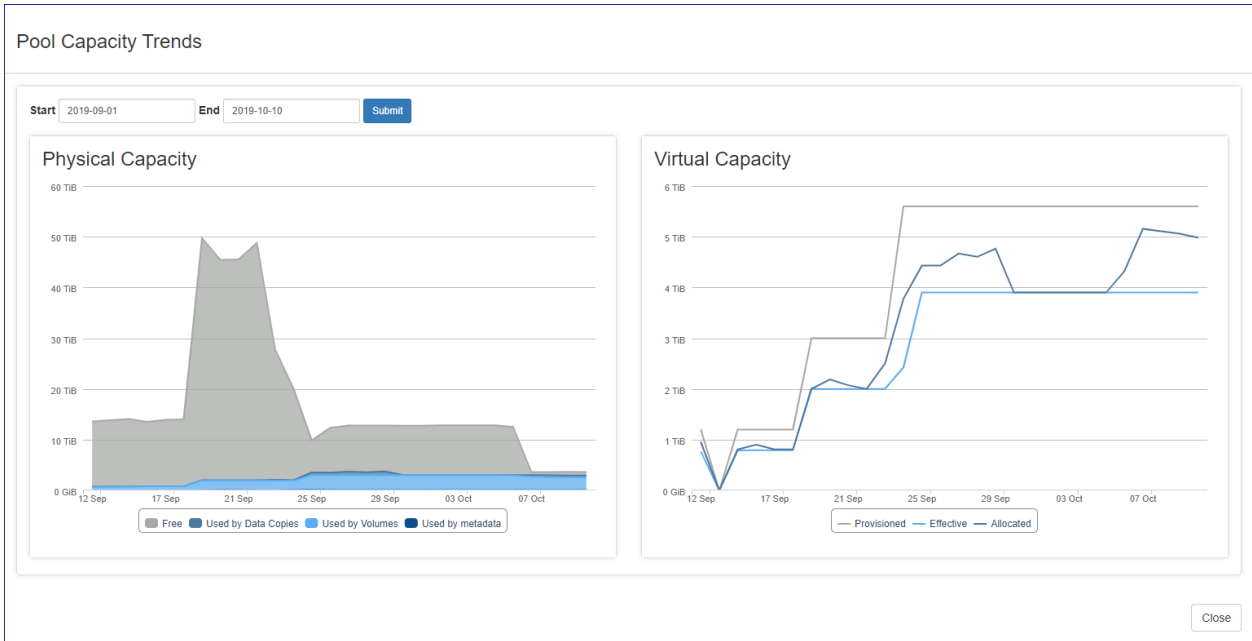
| Name | Status | Type | Cache | Capacity | Capacity Trend |
|----------------|--------|------------|-------|---|---|
| RAID-10-Pool-1 | Normal | Repository | No | 13.90 TiB Total / 13.19 TiB Used / 722 GiB Free |  |

Displaying 1 Pools

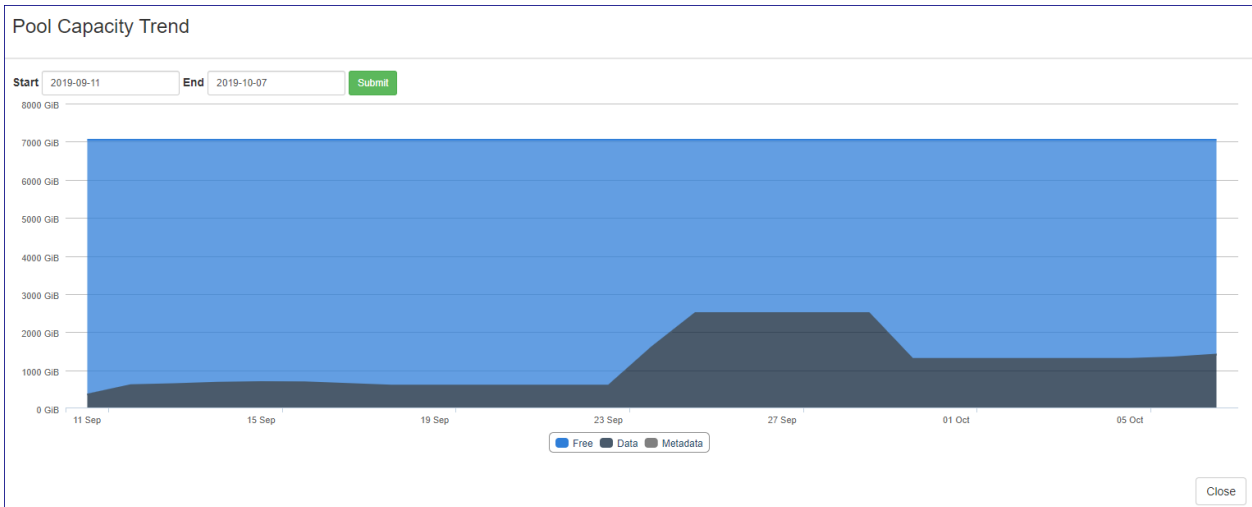
The pool capacity charts display differs between a hybrid VPSA and a Flash VPSA:

An all flash VPSA pool capacity trend display contains 2 charts:

- Overall pool capacity trend over time
- Provisioned capacity vs. virtual capacity and effective capacity over time



A hybrid VPSA pool capacity trend contains only the Overall pool capacity trend over time chart.



5.2 Configuring Virtual Private Storage Array Settings

To view or alter VPSA settings click on the Settings tab on the VPSA dashboard.

| | |
|--|--------------------------------------|
| Remote mirroring | Set the Remote mirroring options. |
| B2OS | Set the B2OS options. |
| NAS Defragmentation | Set the NAS Defragmentation options. |
| Raid | Set the Raid options. |
| Maximum Pool & Volume Sizes | Set the Maximum Pool & Volume Sizes. |
| Metered objects | Set the metered objects threshold. |

5.2.1 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 VPAs performing mirroring |

5.2.2 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 |

5.2.3 NAS defragmentation

| Parameter | Description |
|-----------------------|---|
| Minimum extents count | Amount of extents a file needs to have to be considered for defragmentation |

5.2.4 RAID

| Parameter | Description |
|-------------------|---|
| Allow mixed types | Is HDD type mixture in RAID group/pool allowed? |

5.2.5 Maximum Pool & Volume Sizes

| Parameter | Description |
|-----------------------------|--|
| Pool transactional max size | Maximum capacity(TB) of a transactional pool |
| Pool repository max size | Maximum capacity(TB) of a repository pool |
| Pool archival max size | Maximum capacity(TB) of a archival pool |
| Pool depot max size | Maximum capacity(TB) of a depot pool |

5.2.6 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 |

5.2.7 Ticket Settings

See [Managing Cloud Settings > Management Settings](#) in this manual for details regarding the ticket settings section.

5.3 Performing Virtual Private Storage Array Operations

5.3.1 Changing VPSA engine configuration

Command center can be used to modify a VPSA engine type (to a bigger or smaller engine) and to add or change configuration of a VPSA ZCS engine.

To change engine configuration click on the **actions** button from the VPSA dashboard and select **Change Engine Type(s)** from the dropdown.

In the popup window that will appear select the type of VPSA engine you would like to shift to and/or the type of ZCS engine.

Change Engine Type(s)

Please select an IO Engine type:

200 (Current) ▾

200 (Current)

400

600

800

1000

1200

1600

2400

3600

App Engine type:

Cancel
Change Engine Type(s)

You can also configure advanced option for the model change process by clicking on Advanced options

[Advanced options](#)

Advanced Scheduling

*By selecting Advanced scheduling, after standby Virtual Controller is changed to the new engine, the change engine process will be paused.
VPSA will failover to standby Virtual Controller and proceed with active Virtual Control engine change according to the selected option:*

- Immediate** Failover will take place immediately after Standby Virtual Controller engine is changed.
- Manual** Failover will be done on demand, upon Resume action initiation
- Scheduled** Failover will be done at the requested time (starting 30 minutes from now and up to 7 days).

Version Upgrade

Upgrade version with engine change

vc-19.08-102.img ▾

vc-19.08-102.img

vc-19.08-108-qa.img

Cancel
Change Engine Type(s)

| op-tion | Description |
|----------------------------------|---|
| Ad- vanced schedul- ing | Configure when does the engine change process performs required virtual controller failover: Immediate Failover will take place immediately after 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 (starting 30 minutes from now and up to 7 days). |
| Ver- sion up- grade | Perform VPSA version upgrade alongside the engine model change process |

Click on the **Change Engine Type(s)** button to proceed and approve the operation in the popup windows that will appear. The engine reconfiguration process will commence and your VPSA status will be modified to change engine and will be remodified to Normal as the process concludes.

5.3.2 Adding physical drives

To add physical drives to a VPSA click the **Actions** button then select Add drives from the dropdown. On the popup dialog that will appear select the number of drives to be added and the drive type. Click on the **Add drives** button, the request will be submitted.

✓ **Note:**

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

5.3.3 Change VPSA cache configuration

Cloud Administrators can use Command center to change the Flash cache configuration of a VPSA and add/remove Flash cache capacity on top of the specific model baseline.

✓ **Note:**

VPSA model 200 does not support extended flash cache.

To change cache configuration for a specific VPSA click the **Actions** button then select Change Cache from the dropdown. On the popup dialog that will appear select the new cache configuration you would like to apply for the VPSA and click on the **Submit** button to confirm.

Change Cache

Please select the desired amount of cache for this VPSA (currently **0GiB**).

200 GiB ▾
200 GiB
400 GiB

Cancel Submit

5.3.4 Upgrading a VPSA

Command center allows administrators to perform version upgrade on the VPSA instances running in the cloud. To perform version upgrade click on the **Actions** button then select Upgrade from the dropdown.

On the popup dialog that will appear select the specific image level to which you would like to upgrade to. Advanced options for upgrade can also be selected these options include the ability to schedule the VPSA upgrade and perform an manual VPSA upgrade (failover performed manually by admin). You can also request that version checking will be skipped in the upgrade process. to finalize selection click on the **Upgrade** button .

Upgrade VPSA

Please select an image to upgrade

vc-20.12-sp1-115-qa.img

[Advanced options](#)

Advanced scheduling

By selecting Advanced scheduling, after standby Virtual Controller is upgraded to the new version, the upgrade will be paused.

VPSA will failover to standby Virtual Controller and proceed with active Virtual Control upgrade according to the selected option:

Immediate Failover will take place immediately after Standby Virtual Controller is upgraded.

Manual Failover will be done on demand, upon Resume action initiation

Scheduled Failover will be done at the requested time (starting 30 minutes from now and up to 7 days).

Version validation

Skip version validation

Another Pop up dialog will appear requesting confirmation for upgrading to the selected version click on the **Upgrade** button to confirm the process.

Confirm Upgrade

You are about to upgrade VPSA **CC_lab** from **vc-19.08-111-qa.img** to **vc-19.08-102.img**. Continue?

Cancel
Upgrade

The request will be submitted and the VPSA status property will change to Upgrading version while the process is running.

Information Launch GUI Actions ↻

| | |
|------------------------|--|
| Name | CC_lab |
| Internal Name | vsa-0000000d |
| User | pdm (Product Management) |
| Company | Zadara |
| Description | |
| Nova ID | vsa-0000000d |
| Status | Upgrading version |
| Protection Zone | zone_0 |
| Image | vc-19.08-102.img |
| IO Engine Type | 200 |
| APP Engine Type | 00 |

When the VPSA version upgrade process is completed the status property will be changed back to Normal.

✓ Note:

A scheduled VPSA upgrade operation performs an immediate upgrade of the passive virtual controller.

5.3.5 Canceling a Scheduled VPSA upgrade

For VPSAs in version 20.12 and above who was set up for a scheduled upgrade operation this scheduled upgrade can be canceled from Command Center.

To cancel a scheduled upgrade click on the **Actions** button then select Cancel Scheduled upgrade from the dropdown. on the popup window that will appear confirm upgrade cancellation and the scheduled upgrade will be canceled.

✓ **Note:** As a scheduled upgrade operation performs an immediate upgrade of the passive virtual controller, canceling a scheduled upgrade will revert the passive virtual controller back to the base version.

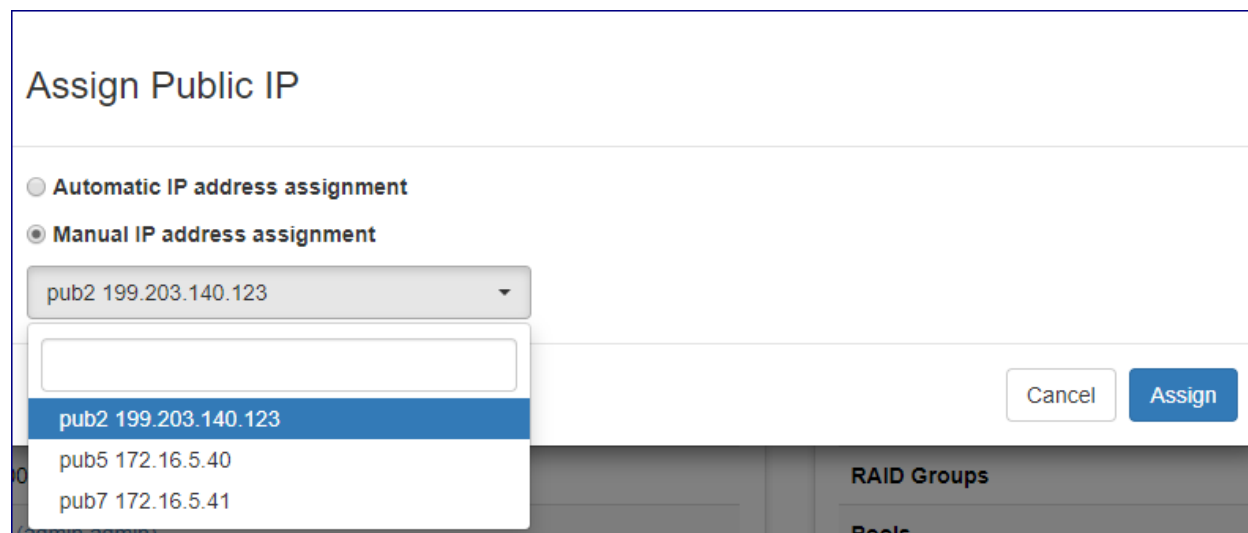
5.3.6 Assigning a Public IP address to a VPSA

In specific cases where a VPSA needs to be available for management access from outside of his Cloud allocated VLAN, a public IP address can be assigned to it. On information regarding the definition of Cloud level public IP ranges please refer to Creating Public IP addresses in this manual.

To assign a public IP address go to the appropriate object storage instance and click the **Actions** button and select assign public IP from the dropdown.

✓ **Note:**

- 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.
-



Public IP addresses can be automatically assigned from a cloud level pool or manually selected. To automatically assign a public IP address: On the popup dialog that will appear make sure Automatic IP address assignment is selected and confirm the operation by clicking on the **Confirm** button. To manually select a specific public IP address: On the popup dialog that will appear select Manual IP address assignment, select the required public IP and confirm the operation by clicking on the **Confirm** button.

✓ **Note:**

- Manual public IP assignment is only available for VPSAs in version 20.01 and later.
- Public IP is not supported for VPSA object storage instances with IPV6 frontend addresses.

5.3.7 Adding or removing a VPSA’s virtual network

An existing VPSA is created with one primary virtual network and can be assigned with additional virtual networks. VPSAs connected to multiple networks can be utilized to Enable use cases requiring per volume partitioning/isolation.

To assign a virtual network to a VPSA first make sure that an appropriate virtual network is defined in the cloud (except the one already used by the VPSA). Click the **Actions** button and select Add Virtual Network from the dropdown.

Add Virtual Network

Warning

- SMB File services will be restarted once Virtual Network Interface is added to the VPSA.

| | Name | CIDR | VLAN ID |
|-----------------------|---------|----------------|---------|
| <input type="radio"/> | cc_test | 191.129.0.0/24 | 15 |

Cancel
Add

On the popup dialog that will appear select the appropriate virtual network and confirm the operation by clicking on the Add button.

Warning:

Addition of a virtual network will restart SMB services causing existing mapped shares to be temporarily unavailable.

When the add operation completes the newly added virtual network should be displayed in the VPSA virtual networks tab.

Dashboard Drives 3 Virtual Controllers 2 Virtual Networks 1 RAID Groups 5 Pools 1 Comments 0 Logs Settings

Networking Configuration

| VCO | IP | VLAN ID |
|-----------|----------------|---------|
| Frontend | 192.168.13.180 | 14 |
| Backend | 172.49.228.101 | 3 |
| Heartbeat | 172.49.232.101 | |
| Outnet | | |

| VC1 | IP | VLAN ID |
|-----------|----------------|---------|
| Frontend | 192.168.13.181 | 14 |
| Backend | 172.49.228.102 | 3 |
| Heartbeat | 172.49.232.102 | |
| Outnet | | |

Virtual Networks

| Name | IP | VLAN ID |
|---------|-------------|---------|
| cc_test | 191.129.0.2 | 15 |

✓ **Note:**

- Number of virtual networks per VPSA is limited to 5.
- VPSA REST API/GUI is accessible through any virtual networks.
- Only Primary virtual networks IP is registered in DNSimple
- VPSA can't have two virtual networks with the same VLAN.
- Only "Primary Virtual Network" is a routable network. Remaining virtual networks are not routable.
- Active Directory can be joined only through "primary virtual network".
- Backup (B2OS), Mirror, Remote Clone through FE network are only allowed via the "primary virtual network".
- ZCS container services exposed through FE network can be done only on "primary virtual network".
- "ISER" host connectivity is available only on the "Primary Virtual Network".

To release a virtual network from a VPSA click the **Actions** button and select Release Virtual Network from the dropdown.

Release Virtual Network

Warning

- SMB File services will be restarted once Virtual Network Interface is removed from the VPSA.
- Once the removal request will be submitted, the VPSA will not be accessible from: 191.129.0.2

| | Name | IP | VLAN ID |
|----------------------------------|---------|-------------|---------|
| <input checked="" type="radio"/> | cc_test | 191.129.0.2 | 15 |

On the popup dialog that will appear select the appropriate virtual network and confirm the operation by clicking on the **Release** button.

✓ Note:

Release of a virtual network will restart 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.

Reconfirm the release operation on the popup dialog that will appear by clicking the red **Release** button.

Confirm Virtual Network Release

You are about to release 191.129.0.2 from VPSA **CC_lab**.

Once the network interface will be released from the VPSA, the VPSA will no longer be accessible via 191.129.0.2

Continue?

5.3.8 Dedicating VPSA to a zCompute cloud

A VPSA can be connected to a zCompute cloud to be utilized as a backend to a Storage Pool (used for creation of EBS compatible block volumes for zCompute VMs). A VPSA connected to zCompute cloud is used solely for this compute cloud and therefore “dedicated” to it.


To dedicate a VPSA to a zCompute Cloud, click the **actions** and select **Dedicate VPSA to Compute** from the dropdown.

Dedicate VPSA to Compute

VPSA Admin Username

VPSA Admin Password

Enable Encryption 

Snapshot Policy 

Set As Default Storage Pool

On the popup dialog that will appear provide the following :

- An admin username for this VPSA to be used by zCompute for VPSA API
- The admin user password

You can also toggle :

- Volume encryption for the compute cloud block volumes provisioned from this VPSA
- The use of VPSA default snapshot policies for the compute cloud block volumes
- Whether this VPSA will be attached to the zCompute cloud default storage pool.

After providing all required information click on **submit** to confirm dedication of this VPSA .

The operation will commence. If it concludes successfully the VPSA will be marked with a **Compute Dedicated** label.

5.3.9 Releasing a VPSA from zCompute cloud dedication

A VPSA dedicated to zCompute cloud can be released from its dedication.

To release a VPSA from compute cloud dedication click the **actions** and select Release VPSA from Compute from the dropdown.

On the popup dialog that will appear confirm release by clicking on the **submit** button.

5.3.10 Performing managed virtual controller failover

Command center can be used to trigger a managed VPSA failover to its standby virtual controller. 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:

Virtual controller failover restart 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 virtual controller failover click the **Actions** button and select Failover from the dropdown. Failover can be performed immediately or be scheduled to a specific date and time.

Failover

You are about to failover VPSA **CC_lab**. Continue?

[Advanced options](#)

VPSA will failover to standby Virtual Controller according to the selected option:

Immediate Failover will take place immediately.

Scheduled Failover will be done at the requested time (starting 30 minutes from now and up to 7 days).

Select Date and Time (Etc/UTC)

2019-09-15 13:00

| Sun | Mon | Tue | Wed | Thu | Fri | Sat |
|-----|-----|-----|-----|-----|-----|-----|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 8 | 9 | 10 | 11 | 12 | 13 | 14 |
| 15 | 16 | 17 | 18 | 19 | 20 | 21 |
| 22 | 23 | 24 | 25 | 26 | 27 | 28 |
| 29 | 30 | 1 | 2 | 3 | 4 | 5 |

September 2019

13:00

14:00

15:00

16:00

17:00

18:00

To perform immediate Failover: on the popup dialog that will appear confirm the action by clicking on the **Failover** button or click on the advanced settings link and make sure that failover is set to immediate and then click on the **Failover** button.

To schedule failover to a specific point in time: on the popup dialog that will appear click on the advanced settings and select Scheduled, select the date and time in which failover should be performed and then click on the **Failover** button.

The failover process will be initiated, Failover status and progress can be monitored from the VPSA log tab.

5.3.11 Moving a virtual controller

In cases where the cloud Storage Node inventory & 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 failover click the **Acti**ons button and select Move Virtual controller from the dropdown.

Move Virtual Controller

Please select the virtual controller to move:

VC-0 (Active) (on qa4-sn5)

VC-1 (Standby) (on qa4-sn3)

Moving active VC will cause a failover

Select one or more destination storage node(s):

When selecting multiple destination storage nodes, the VC will be moved to the first storage node with sufficient resources, according to the selected order

| Available Nodes | Selected Storage nodes <i>(Drag to order)</i> | | | | | | |
|---|---|---------|---|---------|---|---------|---|
| <div style="border: 1px solid gray; padding: 2px; margin-bottom: 2px;">Select storage node ▼</div> <div style="border: 1px solid gray; padding: 2px; background-color: #007bff; color: white; margin-bottom: 2px;">Select storage node</div> <div style="border: 1px solid gray; padding: 2px;">qa4-sn6</div> | <table style="width: 100%; border-collapse: collapse;"> <tr><td style="padding: 2px 10px;">qa4-sn1</td><td style="text-align: right; padding: 2px 10px;">X</td></tr> <tr><td style="padding: 2px 10px;">qa4-sn4</td><td style="text-align: right; padding: 2px 10px;">X</td></tr> <tr><td style="padding: 2px 10px;">qa4-sn2</td><td style="text-align: right; padding: 2px 10px;">X</td></tr> </table> | qa4-sn1 | X | qa4-sn4 | X | qa4-sn2 | X |
| qa4-sn1 | X | | | | | | |
| qa4-sn4 | X | | | | | | |
| qa4-sn2 | X | | | | | | |

Cancel

Move

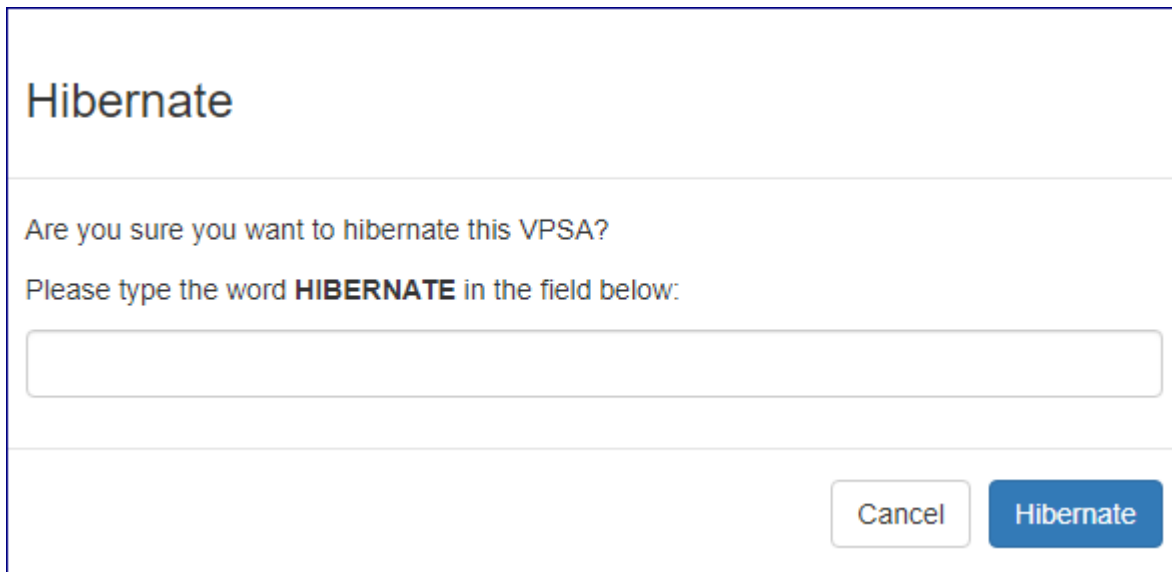
Select the virtual controller you want to relocate and select one or more storage nodes as the destination, in case multiple storage node a slected relocation will be performed to the first SN that has sufficient resource capacity. to confirm relocation click on the **Move** button.

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

5.3.12 Hibernate a VPSA

VPSA Hibernation will take the instance offline and free its consumed resources (vCPU , RAM) on the Storage Nodes level. Hibernation of a VPSA will also reduce its associated service cost. For VPSA in a hibernated state only drives are billed. Hibernating a VPSA involves the process of deleting 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 only takes a few minutes.

To hibernate a VPSA click the **Actions** button and select Hibernate from the dropdown. On the popup dialog that will appear Type HIBERNATE on the textbox item as required and confirm the operation by clicking on the **Hibernate** button.



Hibernate

Are you sure you want to hibernate this VPSA?

Please type the word **HIBERNATE** in the field below:

Cancel **Hibernate**

The request will be submitted for processing, upon successful completion the VPSA status will change to Hibernated.

5.3.13 Creating VPSA Zsnap

To Trigger Manual creation of Zsnap for a VPSA go to its dashboard, click the **Actions** button and select Create Zsnap from the dropdown.

Create Zsnap

You are about to create a zsnap for VPSA **DEVSTACK_IPV6**. Continue?

Zsnap Prefix

Advanced options

VPSA will create the zsnap according to the selected option:

Immediate Zsnap will take place immediately.

Scheduled Zsnap will be done at the requested time (starting 30 minutes from now and up to 7 days).

Select Date and Time (Etc/UTC)

VPSA Zsnaps can be created immediately or scheduled. To create Zsnap immediately: On the popup dialog that will appear provide the prefix for the Zsnap and confirm creation by clicking on the **Create Zsnap** button. To schedule a Zsnap creation: On the popup dialog that will appear provide the prefix for the Zsnap and click on Advanced option. select Scheduled Zsnap and provide creation date and time. to confirm scheduling the Zsnap click on the **Create Zsnap** button.

5.3.14 Purging or restoring a deleted VPSA

Any VPSA instance that has been deleted from the cloud will remain in the clouds recycle bin for a period specified in it's settings (see Managing Cloud Settings). Cloud administrator can manually purge a deleted VPSA prior to the recycle bin retention period expiration to free cloud resources allocated by it (Physical drives). Administrator can also restore the VPSA from the recycle bin and get it up and running on the same data set it contained as it was deleted.

To purge a VPSA from the clouds recycle bin make sure the status of the VPSA is Recycle bin , click the **Actions** button then select Purge from the dropdown. Type the VPSA ID specified in the popup dialog that will appear and click on the **Purge** button to confirm the operation.

To restore a VPSA from the clouds recycle bin make sure the status of the VPSA is recycle bin , click the **Actions** button then select Restore from the dropdown. On the popup dialog that will appear click on the **Restore** button to confirm the operation. The restoration will start and the VPSA status will be modified to Lunning and reverted back to Normal as the restoration concludes.

MANAGING OBJECT STORAGE VPSAS

Command center provides cloud administrators with centralized management capabilities for Zadara Cloud Object storage environment. Using command Center Cloud administrators can:

- Perform various management operations on VPSA object storage instances
- Configure Object storage availability zones resource allocation
- Monitor Object storage capacity consumption trends

6.1 Viewing Object Storage Properties

Object Storage properties/status can be viewed in the Object Storage Dashboard tab.

| Information | | Launch CLI | Actions |
|-------------------|--|------------|---------|
| Name | Leeladhar_TV1 | | |
| Internal Name | vsa-00000037 | | |
| User | idattatrey | | |
| Company | Zadara | | |
| Description | | | |
| Nova ID | vsa-00000037 | | |
| Status | Normal | | |
| Protection Zone | Multiple | | |
| IO Engine Type | Standard | | |
| VCPUs | Proxy+Storage: 96 Proxy Only: 12 | | |
| RAM | Proxy+Storage: 288 GiB Proxy Only: 36 GiB | | |
| SSL Termination | Internal | | |
| Proxy+Storage VCs | 16 | | |
| Proxy Only VCs | 2 | | |
| IP Address | 2003.cdb-a-3256-10 | | |
| Public IP | None | | |
| Mgmt. Address | vsa-00000037.zadara-qa14.zadaracloud.com | | |
| Load Balancer | Elastic Load Balancer | | |
| Image | zios-20.01-199-qa.img | | |
| UUID | f332e0c6-407-4a41-9c58-157893c6aa42 | | |
| SNMPv3 Engine ID | 8000aa8c09f332e0c64074a419c58157893c6aa42 | | |
| Created | February 05, 2020 10:30 AM (a day ago) | | |
| Updated | a few seconds ago | | |

| Property | Description |
|---------------------|--|
| Name | Instance display name |
| Internal Name | internal instance name |
| Company | Creating user company |
| Description | Description given while instance was provisioned |
| Nova ID | Nova ID for this instance |
| Status | Current Instance status |
| Protection Zone | Instance protection zone configuration |
| IO Engine type | VC type for this Object storage Mini/Standard/Premium |
| VCPUs | VCPUs per VC type (Proxy+Storage/Proxy) for this instance |
| RAM | RAM per VC type (Proxy+Storage/Proxy) for this instance |
| SSL Termination | Where does SSL termination Occur (internal/External) |
| Proxy + Storage VCs | Instance Proxy + Storage VC count |
| Proxy Only VCs | Instance Proxy only 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\Elastic Load Balancer) |
| Image | Instance deployment image |
| UUID | Instance UUID |
| SNMPv3 Engine ID | Instance SNMPv3 EngineID |
| Created | Creation timestamp |
| Updated | Last update timestamp |

6.2 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 4 Availability zones defined in each cloud to which different storage nodes can be allocated.

Cloud administrators ability to define specific object storage protection policies is dependent on the SN to availability zone allocation scheme.

| Protection Policy | Number of availability zones with SN allocated required |
|--------------------|---|
| 2-way mirroring | 2 |
| 3-way mirroring | 3 |
| 6+3 erasure coding | 3 |
| 8+4 erasure coding | 3 |
| 9+3 erasure coding | 4 |

6.2.1 Assigning and removing Storage nodes to Object storage availability zones

To view 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.

zadara-qa16 Object Storage | Object Storage Availability Zones

Instances Object Storage Availability Zones Zones Drives Inventory

| Name | Storage nodes | VCPUs Reserved Used Free | Memory Reserved Used Free | Drives Disabled Absent Used Free | Object Storage VCs |
|--------|---------------|--|--|---|--------------------|
| zone_4 | 0 | 0 Total / 0 Reserved / 0 Used / 0 Free | 0 B Total / 0 B Reserved / 0 B Used / 0 B Free | 0 Total / 0 Disabled / 0 Absent / 0 Used / 0 Free | 0 |
| zone_3 | 0 | 0 Total / 0 Reserved / 0 Used / 0 Free | 0 B Total / 0 B Reserved / 0 B Used / 0 B Free | 0 Total / 0 Disabled / 0 Absent / 0 Used / 0 Free | 0 |
| zone_2 | 0 | 0 Total / 0 Reserved / 0 Used / 0 Free | 0 B Total / 0 B Reserved / 0 B Used / 0 B Free | 0 Total / 0 Disabled / 0 Absent / 0 Used / 0 Free | 0 |
| zone_1 | 0 | 0 Total / 0 Reserved / 0 Used / 0 Free | 0 B Total / 0 B Reserved / 0 B Used / 0 B Free | 0 Total / 0 Disabled / 0 Absent / 0 Used / 0 Free | 0 |

Available Storage Nodes

| Name | Status | Protection Zone | VCPUs Reserved Used Free | Memory Reserved Used Free | Drives Disabled Absent Used Free | Version | Virtual Controllers | Actions |
|--------------------|--------|-----------------|--|--|---|-----------|---------------------|-------------|
| qa16-sn1 CC Slave | Normal | zone_0 | 40 Total / 3 Reserved / 30 Used / 7 Free | 188.38 GiB Total / 11.34 GiB Reserved / 138.68 GiB Used / 38.36 GiB Free | 33 Total / 0 Disabled / 0 Absent / 30 Used / 3 Free | 19.08-102 | 2 (2 Active) | Add to zone |
| qa16-sn2 CC Master | Normal | zone_0 | 40 Total / 2 Reserved / 31 Used / 7 Free | 188.38 GiB Total / 9 GiB Reserved / 141.03 GiB Used / 38.36 GiB Free | 33 Total / 0 Disabled / 0 Absent / 30 Used / 3 Free | 19.08-102 | 3 (3 Active) | Add to zone |

Displaying [object Object],[object Object] Storage Nodes

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

Storage Nodes Virtual Controllers 1

| Name | Protection Zone | Object Storage Zone | VCPUs Reserved Used Free | Memory Reserved Used Free | Drives Disabled Absent Used Free | Version | Virtual Controllers | Actions |
|------------------------|-----------------|---------------------|---|---|--|-----------|---------------------|---------|
| zdr-lcp-sn-02 CC Slave | zone_0 | zone_2 | 32 Total / 3 Reserved / 12 Used / 17 Free | 62.88 GB Total / 11.34 GB Reserved / 49.03 GB Used / 2.51 GB Free | 31 Total / 0 Disabled / 0 Absent / 10 Used / 21 Free | 18.11-233 | 3 (1 Active) | Remove |

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

6.2.2 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.

Instances Object Storage Availability Zones Zones Drives Inventory

| | zone_1 (Free / Total) | zone_2 (Free / Total) | zone_3 (Free / Total) |
|--------------------|-----------------------|-----------------------|-----------------------|
| SSD CACHE DRIVES | 1 / 1 | 1 / 1 | 0 / 0 |
| SSD 3576GB 1RPM | 0 / 3 | 0 / 3 | 0 / 0 |
| SAS 5588GB 7200RPM | 21 / 26 | 21 / 26 | 0 / 0 |

6.3 Managing VPSA Object Storage Instances

6.3.1 Adding drives to VPSA object Storage

From the Instances tab on the Object Storage screen select the appropriate VPSA Object storage instance. From the specific Instance dashboard click the **Actions** button then select Add drives from the drop down menu. On the popup dialog that will appear select the required protection policy, number of drives to be added and the drive type. Click on the **Add drives** button, the request will be submitted.

✓ Note:

- When Adding drives to VPSA Object storage virtual controllers can also be added automatically depending on the drive to VC ratio
- In case that the VPSA Object Storage instance version is older then 20.01 - virtual controllers cannot be spawn on Storage Nodes with ConnectX-5 NICs

To avoid any performance impact - drive addition process is performed gradually, configuration of drive addition increments can be performed from the settings dialog in the VPSA object storage GUI. Drive addition progress can be monitored from the VPSA Object Storage Storage Policies tab in command center.

| Name | Status | Protection | Regions | HEALTH STATUS | HEALTH | Resilience | Resilience Configuration / Protected at | CAPACITY | Capacity Used |
|----------------------------|---------|------------------|---------|---------------|--------|------------|---|------------------------|-----------------|
| StandardPolicy | enabled | 2-Way Protection | 1 | HEALTHY | 100% | 100% | | 100% (100 GB / 100 GB) | 100 GB / 100 GB |
| 2-Way Protection (Default) | enabled | 2-Way Protection | 1 | WARNING | 0% | 0% | | 0% (0 GB / 100 GB) | 0 GB / 100 GB |

6.3.2 Creating a storage policy

From the Instances tab on the Object Storage screen select the appropriate VPSA Object storage instance. From the specific Instance dashboard click the **Actions** button then select Create Storage policy from the drop down menu.

On the popup dialog that will appear select name your new storage policy and select an appropriate protection policy from the list of the cloud supported policies. Select the number of drives you wish to assign to your new policy and the drive type to use. click on the **create storage policy** button , the request will be submitted for processing.

Create Storage Policy

Please select the drive type and quantity you would like to add.

Policy name

Must contain only lowercase letters, numbers and hypens

Description

Redundancy Level

2 Way Protection ▼

2 ▼ SAS 5588GB 7200RPM ▼

Cancel Create Storage Policy

6.3.3 Adding a proxy virtual controller

From the Instances tab on the **Object Storage** screen select the appropriate VPSA Object storage instance. From the specific Instance dashboard click the **Actions** button then select Add Proxy VC from the drop down menu.

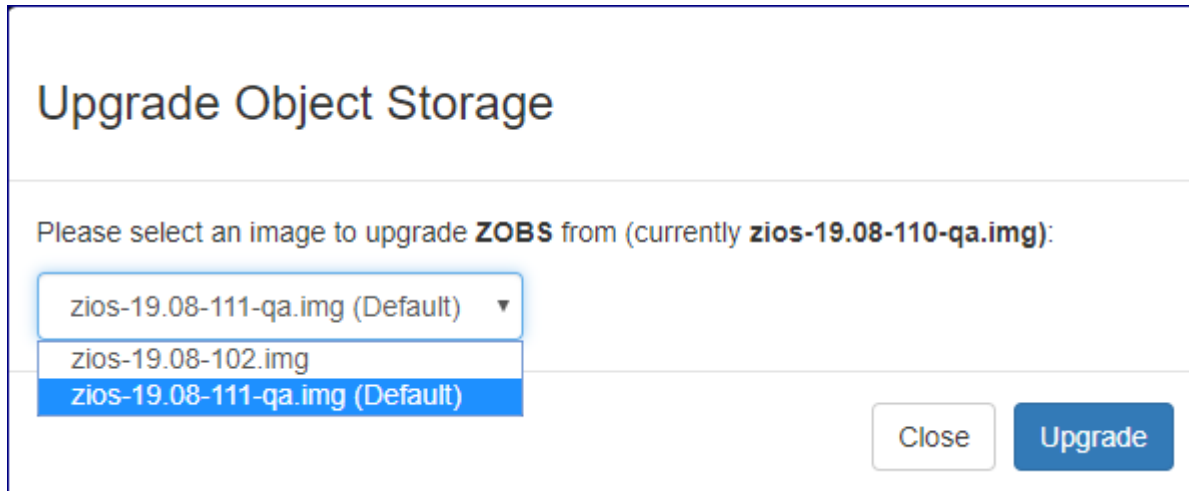
On the popup dialog that will appear confirm the operation by clicking on the **Add Proxy Virtual Controller** button. The request will be submitted for processing, after completion the proxy only VCs property on the specific VPSA Object storage dashboard will be incremented.

| | |
|--------------------------|---|
| Proxy+Storage VCs | 2 |
| Proxy Only VCs | 1 |

6.3.4 Upgrading VPSA Object storage

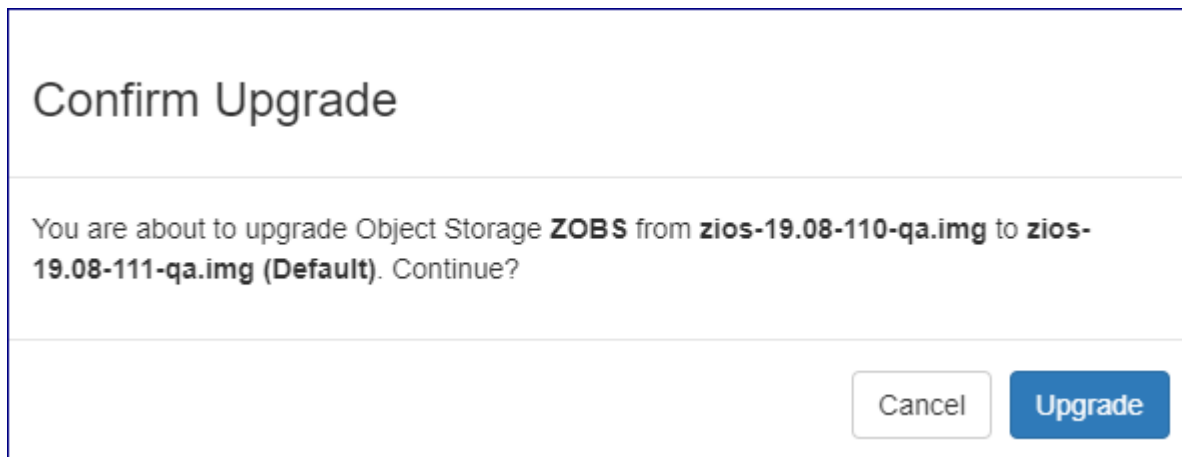
Command center allows administrators to perform version upgrade on the VPSA Object storage instances running in the cloud. to perform version upgrade select the appropriate VPSA Object storage instance from the Instances tab on the Object Storage screen. From the specific Instance dashboard click the **Act ions** button then select Upgrade from the drop down menu.

On the popup dialog that will appear select the specific image level to which h you would like to upgrade and click on the **Upgrade** button to confirm.



The screenshot shows a dialog box titled "Upgrade Object Storage". Below the title, it says "Please select an image to upgrade **ZOBS** from (currently **zios-19.08-110-qa.img**):". There is a dropdown menu with three options: "zios-19.08-111-qa.img (Default)", "zios-19.08-102.img", and "zios-19.08-111-qa.img (Default)". The second option is highlighted. At the bottom right, there are two buttons: "Close" and "Upgrade".

Another Pop up dialog will appear requesting confirmation for upgrading to the selected version click on the **Upgrade** button to confirm the process.



The screenshot shows a dialog box titled "Confirm Upgrade". Below the title, it says "You are about to upgrade Object Storage **ZOBS** from **zios-19.08-110-qa.img** to **zios-19.08-111-qa.img (Default)**. Continue?". At the bottom right, there are two buttons: "Cancel" and "Upgrade".

The request will be submitted and the VPSA Object storage status property will change to Upgrading version while the process is running.

| Information | |
|------------------------|-------------------|
| Name | ZOBS |
| User | pdm |
| Internal Name | vsa-00000006 |
| Description | |
| Nova ID | vsa-00000006 |
| Status | Upgrading version |
| Protection Zone | zone_0 |

When the VPSA version upgrade process is completed the status property will be changed back to normal and the image property will be updated to reflect the new VPSA version.

| | |
|--------------------------|---|
| Status | Normal |
| Protection Zone | zone_0 |
| IO Engine Type | ZIOS_MINI |
| VCPUs | 6 |
| RAM | 18432 MB |
| SSL Termination | Internal |
| Proxy+Storage VCs | 2 |
| Proxy Only VCs | 0 |
| IP Address | 192.168.13.182 |
| Public IP | None |
| Mgmt. Address | vsa-00000006-zadara-iop-01.zadarazios.com |
| Image | zios-19.08-111-qa.img |

✓ Note:

- From cloud version 20.12 VPSA Object Storage upgrade to a version which more than 2 major release higher than the current version will be blocked by Command Center
- From cloud version 20.12 VPSA Object Storage version downgrade will be blocked by Command Center

6.3.5 Changing VPSA Object Storage engine type

When creating a VPSA Object storage with 4 disk drives or less the VPSAs engine type will be set to MINI which is a lower footprint engine compared to the fully blown VPSA for object storage virtual controller (designed to support up to 12 disk drives). VPSA for Object Storage MINI virtual controllers can be manually converted to the fully blown footprint by Command Center.

| Information | |
|-----------------------|---|
| Name | ZIOS_for_CC_manual |
| User | admin |
| Internal Name | vsa-00000008 |
| Description | for testing C.C With ZIOS functionality |
| Nova ID | vsa-00000008 |
| Status | Normal |
| IO Engine Type | ZIOS_MINI |

✓ **Note:** VPSA Object Storage engine will be automatically upgraded when more than 4 disk drives overall are provisioned to it

To change engine type go to the appropriate object storage instance and click the **Actions** button and select Change Engine Type from the drop down menu. On the popup dialog that will appear confirm the operation by clicking on the **Change engine** button. The request will be submitted for processing. After completion the IO Engine Type property on the specific VPSA Object storage dashboard will be changed to Standard.

6.3.6 Hibernate VPSA Object storage instance

VPSA Hibernation will take the instance offline and free its consumed resources (vCPU , RAM) on the Storage Nodes level. Hibernation of a VPSA will also reduce its associated service cost. For VPSA in a hibernated state only drives are billed. Hibernating a VPSA involves the process of deleting 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 only takes a few minutes.

From the Instances tab on the Object Storage screen select the appropriate VPSA Object storage instance. From the specific Instance dashboard click the **Actions** button then select Hibernate from the drop down menu. On the popup

dialog that will appear confirm the operation by clicking on the **Hibernate** button. The request will be submitted for processing, upon successful completion the VPSA Object storage status will change to Hibernated.

6.3.7 Assigning a Public IP address to VPSA object Storage

In specific cases where a VPSA object storage instance needs to be available for management access from outside of his Cloud allocated VLAN, a public IP address can be assigned to it. On information regarding the definition of Cloud level public IP ranges please refer to Creating Public IP addresses in this manual.

To assign a public IP address go to the appropriate object storage instance and click the **Actions** button and select assign public IP from the drop down menu.

Public IP addresses can be automatically assigned from a cloud level pool or manually selected. To automatically assign a public IP address: On the popup dialog that will appear make sure Automatic IP address assignment is selected and confirm the operation by clicking on the **Confirm** button. To manually select a specific public IP address: On the popup dialog that will appear select Manual IP address assignment, select the required public IP and confirm the operation by clicking on the **Confirm** button.

✓ Note:

- Manual public IP assignment is only available for VPSA object storage instances in version 20.01 and above
- Public IP is not supported for VPSA object storage instances with IPV6 frontend address

6.3.8 Creating VPSA Object Storage Zsnap

To Trigger Manual creation of Zsnap for the VPSA Object storage go the its dashboard, click the **Actions** button and select Create Zsnap from the drop down menu. On the popup dialog that will appear provide the prefix for the Zsnap and confirm weather you would like to include the VPSA Object storage metering data. Confirm the Zsnap creation by clicking on the **Create Zsnap** button.

Create Zsnap

You are about to create a zsnap for Object Storage **ZOBS**. Continue?

Zsnap Prefix

Collect Metered Data

Cancel

Create Zsnap

MANAGING PHYSICAL DRIVES

Command center provides extensive cloud physical drive management functionality.

Using Command Center Zadara Cloud administrator can easily perform activities such as :

- Drive inventory management
- Drive validation and failure management
- Assignment of drives to specific roles

7.1 Viewing Physical Drive Inventory

Command center displays overall drive inventory under the **Drives** tab.

| Name | Type | Size | RPM | Inventory | Product ID |
|------------------|------|----------|-----|---|-------------------------|
| AFA META DRIVES | NVME | - | 1 | 2 Total / 0 Disabled / 0 Absent / 0 Used / 2 Free | INTEL Optane |
| NVME 7153GB 0RPM | NVME | 7153 GiB | - | 22 Total / 0 Disabled / 0 Absent / 4 Used / 18 Free | NVMe SAMSUNG IMZQLB7T6B |
| SSD CACHE DRIVES | SSD | 20 GiB | 1 | 2 Total / 0 Disabled / 0 Absent / 2 Used / 0 Free | NVMe INTEL SSDPE2ME01X |

Drive inventory is primarily divided by drive model and displays detailed utilization per each group.

| | | | | |
|------------------|------|----------|---|---|
| NVME 7153GB 0RPM | NVME | 7153 GiB | - | 22 Total / 0 Disabled / 0 Absent / 4 Used / 18 Free |
|------------------|------|----------|---|---|

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

✓ **Note:**

Drive inventory assigned to a specific VPSA, deployed on a specific protection zone or installed on a specific Storage node can be also viewed from the corresponding VPSA/SN/Protection Zone

7.2 Viewing Drive Properties

From the Command center drives tab select the drive group to which the required drive belong a after list of group members appear select the required drive.

Drive Properties

Details
Actions ▾

| | |
|------------------|--|
| Device Name | /dev/nvme5n1 |
| Storage Node | qa16-sn2 |
| Drive Type | NVME 7153GB 0RPM |
| Capacity | 7153 GiB |
| Licensed | Licensed |
| Status | Allocated |
| Address | 0:0:0:0 |
| PCI Address | 0:0:0 |
| Product ID | NVMe SAMSUNG MZQLB7T6A |
| Firmware Version | EDB5002Q |
| Serial Number | S4BGNY0M601187 |
| UUID | 533442474E59304D363031313837202020202020 |
| Cache | No |

Location

| Node | Adapter ID | Enclosure ID | Slot |
|----------|------------|--------------|------|
| qa16-sn2 | -1 | -1 | -1 |

Adapter Cache Policy

| | |
|------------|----------|
| Write Back | Disabled |
| Read Ahead | Disabled |

| property | Description |
|----------------------|---|
| Device name | Device file identifier for this drive |
| Drive Type | Drive model |
| Capacity | Physical capacity(Gib) of the drive. Note: SSD cache drives will also present capacity of allocated partitions |
| License | Indicates whether this drive is licensed on the cloud level |
| Status | Indicates the current status of the drive(Ex: allocated) |
| Address | SN SCSI address for the specified Drive |
| PCI Address | SN PCI address for the specified Drive |
| Address | SN SCSI address for the specified Drive |
| PCI Address | SN PCI address for the specified Drive |
| Product ID | Product Id for the specific drive |
| Firmware version | Specified Drive Firmware Version |
| Serial Number | Serial Number of this drive |
| UUID | Linux UUID for the SN Device |
| Cache | weather this drive is being used as SSD cache |
| Location | SN and MegaRaid location identifier for this drive (Adapter IDEnclosure IDSlot) |
| Adapter cache policy | MegaRaid Adapter cache policy(Writeback - adapter write buffering Readahead - adapter read prefetching) |

Volume Properties

| ID | VPSA | Drive | Size | Cache | Storage Node | |
|-----------------|-------|--------------|----------|-------|--------------|----------------|
| volume-0000007a | VPSA1 | /dev/nvme5n1 | 7153 GiB | No | qa16-sn2 | Replace Volume |

Displaying 1 Volumes

| property | Description |
|----------------|---|
| ID | Volume Identifier |
| VPSA | VPSA/Object Storage to which this volume is allocated |
| Drive | Device file name for the SN physical drive |
| Size | Volume Capacity |
| cache | Weather this volume is used as GEN2 SSD cache device |
| Storage Node | SN in which this volume is defined |
| Replace Volume | Toggle drive replacement for this volume |

7.3 Performing Operations On Physical Drives

To view all operations that can be performed on a specific drive: From the **Drives** tab select the appropriate drive group and go to the drives tab. Select the required physical drive and click on the **Actions** button.

Details

| | |
|---------------------|------------------|
| Device Name | /dev/nvme6n1 |
| Storage Node | qa16-sn2 |
| Drive Type | NVME 7153GB 0RPM |
| Capacity | 7153 GiB |

Actions ▾

- Disable
- Designate as Cache
- SMART Attributes
- Unlicense

Disabling a drive

From the actions drop down menu select **Disable** a pop up confirmation window will appear in which select **Disable**. After operation the will complete the drive status will be changed to **Disabled**.

Enabling a drive

Select a disabled physical drive. From the actions drop down menu select **Enable** and confirm the operation in the pop up dialog that will appear. After the operation will complete the drive status will be changed to **Enabled**.

Managing drive LED

A Physical drive LED can be turned on\off from Command center. To manage a physical drive LED select **LED On** or **LED Off** from the actions drop down menu and confirm the operation in the pop up dialog.

Viewing drive SMART attributes

From the actions drop down menu select **SMART Attributes**. A pop up windows will appear displaying **SMART Attributes** for the specific drive.

Designating SSD drive as Cache

SSD drives installed within the cloud can be designated as cache drives that will be used in hybrid VPSA configurations.

Note:

Available capacity from an SSD drive designated as cache cannot be allocated as user data to VPSA images.

From the actions drop down menu select **Designate as cache**. A pop up windows will appear displaying warning information and requesting action confirmation. After confirmation drive type will be changed to **SSD CACHE DRIVES**.

Removing drives

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 actions drop down menu.

Unlicensing a drive

From the actions drop down menu select **Unlicense**. A pop up windows will appear displaying warning information and requesting action confirmation. After confirmation drive type will be changed to **Unlicensed**.

7.4 Monitoring Drive Performance

To view performance statistics for a specific drive: From the **Drives** tab select the appropriate drive group and go to the **drives** tab. Select the required physical drive and go to the **Performance** tab. Performance statistics displayed per physical drive include :

- Average IO rate divided in to read vs. write IOs
- Average IO time divided in to read vs. write IOs
- Average Bandwidth divided in to read vs. write activity



Monitoring interval can be changed supported intervals are : 1sec ,10sec, 1min, 1hr and 1day. Interactively refreshed charts can be triggered by pushing the Auto refresh button.

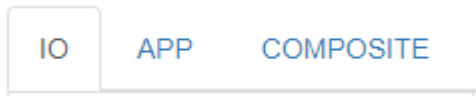
VIEWING ENGINE PROPERTIES

Command Center allows cloud administrator to view all Virtual Private Storage Array engine types available for deployment on the cloud. To view VPSA engine properties navigate to Command Center Engines section from the left menu pane.

The VPSA engine types presented in this section are:

- VPSA IO engines
- VPSA app engines
- VPSA composite engines

Toggleing between the engine types is done via the tabs section in the top part of the dialog”



8.1 VPSA IO engines properties

For VPSA IO engines the following properties are presented:

| <input type="radio"/> IO <input type="radio"/> APP <input type="radio"/> COMPOSITE | | | | |
|--|---------------------|-----------|-------|------------------------|
| Name ▲ | Internal Type | Memory | VCPUs | VPSAs / Object Storage |
| 1000 | vsa.V2.large.vf | 18432 MiB | 5 | 1 |
| 1000m | vsa.V2.large.mz.vf | 18432 MiB | 5 | 0 |
| 1200 | vsa.V2.xlarge.vf | 26624 MiB | 6 | 0 |
| 1200m | vsa.V2.xlarge.mz.vf | 26624 MiB | 6 | 0 |
| 1600 | vsa.V2.1600.vf | 34816 MiB | 8 | 0 |

| 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 in this cloud with this engine type |

8.2 VPSA APP engines properties

For VPSA APP engines the following properties are presented:

| IO APP COMPOSITE | | | | |
|------------------|---------------|----------|-------|-------|
| Name | Internal Type | Memory ▲ | VCPUs | VPSAs |
| 00 | None | 0 MiB | 0 | 8 |
| 01 | tiny | 256 MiB | 1 | 0 |
| 02 | small | 512 MiB | 1 | 0 |
| 04 | medium | 1024 MiB | 2 | 0 |
| 06 | large | 2048 MiB | 3 | 0 |
| 08 | xlarge | 4096 MiB | 4 | 0 |

Displaying 6 App Engine Types

| 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 in this cloud with this APP engine type allocated to them |

8.3 VPSA composite engines properties

For VPSA composite engines the following properties are presented:

| IO APP COMPOSITE | | | |
|---|------------------------------|------------------------------|----------|
| Property ▲ | PREMIUM_PLUS | PREMIUM | STANDARD |
| Category | zios | zios | zios |
| Controller Instance Type | zios_premium_ctrler.vf | zios_premium_ctrler.vf | zios.vf |
| Data Policy Partition Power | 18 | 15 | 14 |
| Dedicated Controller Vcs | 1 | 1 | |
| Enable Zelf On Zios Creation | 1 | | |
| Enforce Drive Add With VC Set | 1 | 0 | |
| Max Capacity in TB | 61440 | 4096 | 1024 |
| Max Drives Per Proxy Storage VC | 12 | 12 | 12 |
| Metadata Partition Size in GB | 200 | 200 | 120 |
| Metadata Partitions Per Proxystorage VC | 1 | 1 | |
| Metadata Policy Partition Power | 14 | 12 | 12 |
| Minimum VC Sets During Zios Creation | 2 | 1 | |
| Name | premium_plus | premium | standard |
| Proxy Instance Type | zios_premium_proxy.vf | zios_premium_proxy.vf | zios.vf |
| Proxy Storage Instance Type | zios_premium_proxystorage.vf | zios_premium_proxystorage.vf | zios.vf |
| Setup Partition Size in GB | 60 | 60 | 10 |

Displaying 3 Composite Instance Types

| property | Description |
|---|--|
| Type | Composite engine type |
| Controller Instance Type | link to image used for composite controller instances |
| 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 Zadarra Extend load balancing will be enabled on VPSA creation |
| Enforce Drive Add With VC Set | Whether disk drives are automatically added when the VPSA is expanded by additional vc set |
| Max Capacity In TB | 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 GB | 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 image used for composite proxy instances |
| Proxy Storage Instance Type | Link to image used for composite storage proxy instances |
| Setup Partition Size In GB | Allocation size in gigabytes for the composite instance setup partition |

✔ **Note:**

A composite engine instance sub-instances properties can be displayed by clicking on the sub-instance image link.

| Engine Details | |
|----------------------|-----------------------|
| Name | ZIOS_PREMIUM_PROXY |
| Internal Type | zios_premium_proxy.vf |
| Memory | 16384 MIB |
| VCPUs | 4 |

MANAGING CLOUD NETWORKING

9.1 Background

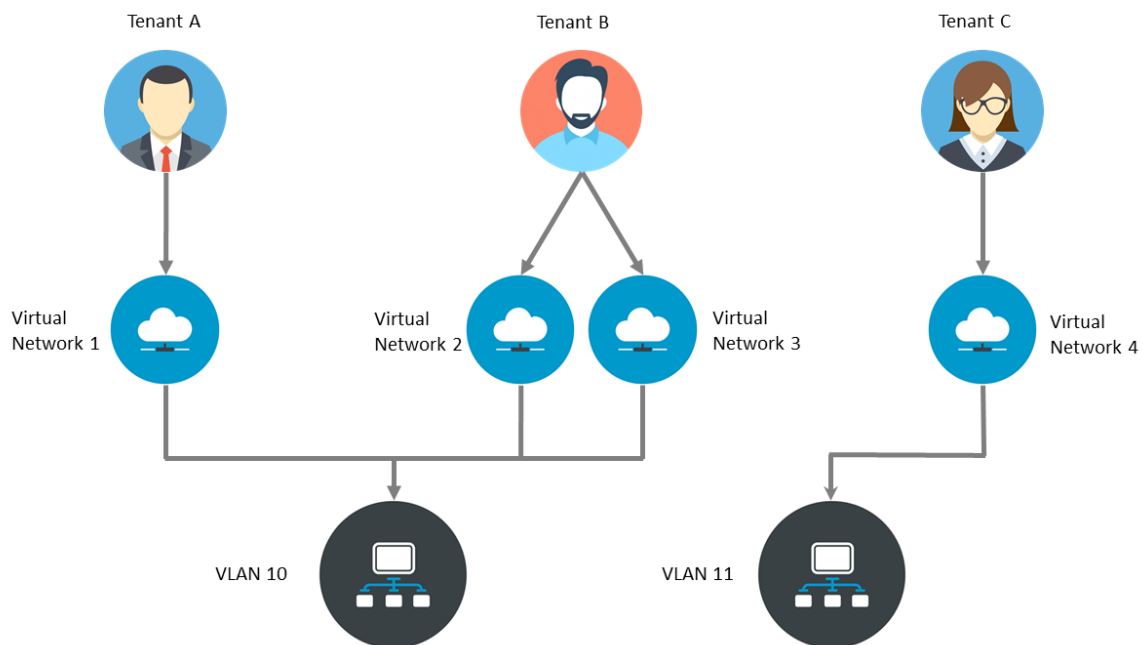
The Zadara cloud is a flexible storage cloud supporting multiple topologies, a vast range of use cases and cloud hosted environments. Due to the Zadara cloud flexibility it requires a flexible and dynamic virtual networking infrastructure that can be tailored to meet any customer demand and configuration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

9.2 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.

zadara-iop-01 Users

Username Tenant Comment Filter

| Username | Tenant | Tenant ID | VLANs | Virtual Networks |
|----------|---------------------|-----------|----------------------------------|------------------------------------|
| admin | tenant_admin_Doq1X | 6 | 14 Default | PUBLIC_PP_DMZ Default |
| admin | tenant_admin_t13Vd | 2 | | |
| admin | tenant_admin_ujYot | 4 | 11 Default , 50 | |
| dryrun | tenant_dryrun_GjU9F | 5 | 12 Default | |
| pdm | tenant_pdm_ILSFN | 3 | 10, 14 Default , 15 | VN-DMZ Default |

Displaying 5 Users

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
- VLNAS which have allocation per each tenant
- Virtual networks defined in each tenant

✓ Note:

Tenant names and ids are unique per cloud but a user can have multiple tenants due to the fact a user can create tenant entries from both the local provisioning portal and a public provisioning Portal running in a PaaS environment(Heroku)

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.

pdm tenant_pdm_ILSFN

Dashboard **VPSAS** Object Storage Networks Comments

| Name | Internal Name | User | Company | Status | Engine Type | Drives | Base Cache | Ext. Cache | Image | VLAN | Pools | Capacity |
|-----------------|---------------|------|---------|--------|-------------|--------|------------|------------|---------------------|------|-------|--|
| PRIMARY | vsa-00000013 | pdm | Zadara | Normal | 600/Boost | 10 | 40 GiB | 0 GiB | vc-19-08-151-qa.img | 10 | 2 | 15.73 TiB Total / 3.04 TiB Used / 12.69 TiB Free |
| Bhaa_Cinder_Dev | vsa-00000008 | pdm | Zadara | Normal | 200/Baby | 4 | 20 GiB | 0 GiB | vc-19-08-151-qa.img | 14 | 1 | 5.36 TiB Total / 1 GiB Used / 5.36 TiB Free |

Displaying 2 VPSAs

Viewing VLAN configuration

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

zadara-iop-01 VLANs

Search:

[Add VLAN\(s\)](#)

Show 10 entries

| VLAN ID | User (tenant) | VPSAs | Reserved | Actions |
|---------|--|---|----------|---------|
| 10 | pdm (pdm_ILSFN - #3) | IOP_INFRA | | ▼ |
| 11 | admin (admin_ujYot - #4) Default | | | ▼ |
| 12 | dryrun (dryrun_CJUSF - #5) Default | | | ▼ |
| 13 | | | | ▼ |
| 14 | pdm (pdm_ILSFN - #3) Default admin (admin_Doq1X - #6) Default | ASIGRA_BACKUP_VPSA CC_lab VPSAO_test Bhaa_Cinder_Dev | | ▼ |
| 15 | pdm (pdm_ILSFN - #3) | | | ▼ |
| 16 | | | | ▼ |
| 17 | admin (admin_113Vd - #2) Default pdm (pdm_ILSFN - #3) | | | ▼ |
| 18 | | | | ▼ |
| 19 | | | | ▼ |

Showing 1 to 10 of 990 entries

Previous 1 2 3 4 5 ... 99 Next

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.

Add VLAN(s)

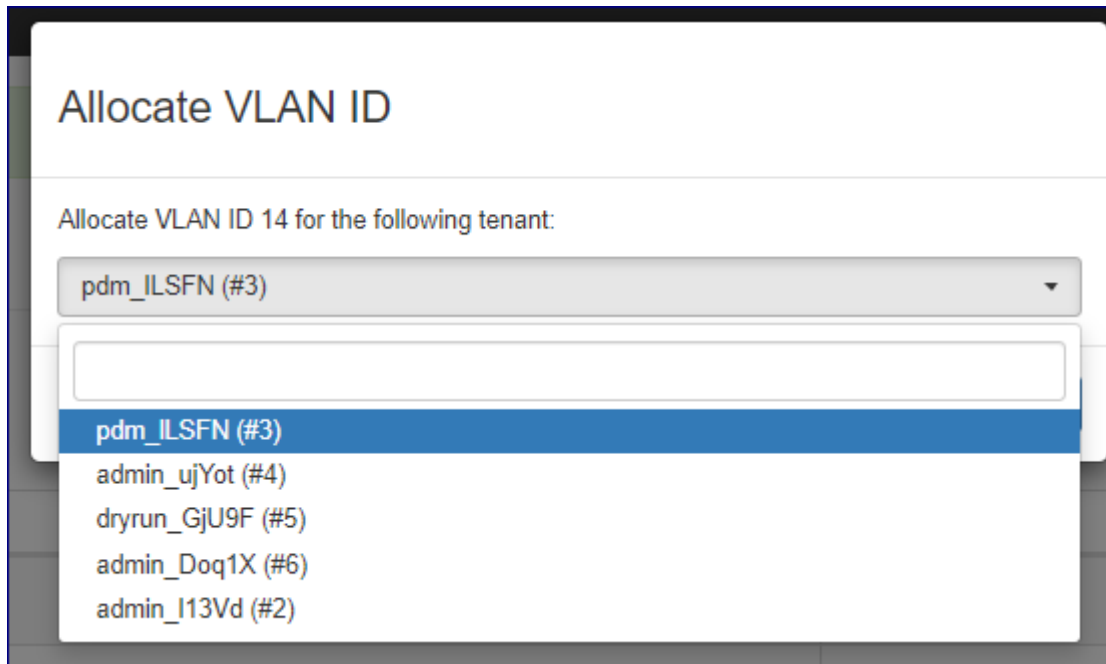
VLAN id(s)

Cancel
Add VLAN(s)

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 unassigning 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.

| VLAN ID | User (tenant) | VPSAs | Reserved | Actions |
|---------|--|---|-------------------------------------|---------|
| 10 | pdm (pdm_ILSFN - #3) | IOP_INFRA | | ▼ |
| 11 | admin (admin_ujYot - #4) <small>Default</small> | | | ▼ |
| 12 | dryrun (dryrun_GjU9F - #5) <small>Default</small> | | | ▼ |
| 13 | | | | ▼ |
| 14 | pdm (pdm_ILSFN - #3) <small>Default</small> admin (admin_Doq1X - #6) <small>Default</small> | ASIGRA_BACKUP_VPSA VPSAO_test Bhaa_Cinder_Dev CC_lab | | ▼ |
| 15 | pdm (pdm_ILSFN - #3) | | | ▼ |
| 16 | | | | ▼ |
| 17 | admin (admin_I13Vd - #2) <small>Default</small> pdm (pdm_ILSFN - #3) | | | ▼ |
| 18 | | | | ▼ |
| 19 | | | <input checked="" type="checkbox"/> | ▼ |

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.

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.

zadara-iop-01 Virtual Networks Create Virtual Network

| Name ▲ | User | CIDR | Gateway | IP ranges | VLAN ID | Nova ID | |
|---------------|-------|----------------------------------|------------------------------|---|---------|---------|--|
| IOP_IPv6 | pdm | 2001:db8:85a3::8a2e:370:7000/119 | 2001:db8:85a3::8a2e:370:7001 | 2001:db8:85a3::8a2e:370:7002 - 2001:db8:85a3::8a2e:370:700a | 10 | 10 | |
| PUBLIC_PP_DMZ | admin | 192.168.12.0/23 | 192.168.12.1 | 192.168.13.200 - 192.168.13.210 | 14 | 3 | |
| VN-DMZ | pdm | 192.168.12.0/23 | 192.168.12.1 | 192.168.13.180 - 192.168.13.199 | 14 | 2 | |
| vn1 | admin | 198.134.0.0/24 | 198.134.0.1 | 198.134.0.1 - 198.134.0.10 | 17 | 8 | |
| vn2 | admin | 198.134.0.0/24 | 198.134.0.1 | 198.134.0.11 - 198.134.0.20 | 17 | 9 | |

Displaying 5 Custom Networks

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

Virtual Network IOP_IPv6 Default pdm

General Information Set as Default Delete

| | |
|--------------|------------------------|
| Network Name | IOP_IPv6 |
| Nova ID | 10 |
| User | pdm (tenant_pdm_ILSFN) |
| VLAN ID | 10 |

IPv6 Information

| | |
|-----------------------|--|
| CIDR | 2001:db8:85a3::8a2e:370:7000/119 |
| Gateway Address | 2001:db8:85a3::8a2e:370:7001 |
| Allocatable IP Ranges | 2001:db8:85a3::8a2e:370:7002 - 2001:db8:85a3::8a2e:370:700a Extend Remove |

start
 end
 Add Add

Allocated IPs

2 / 10

| IP | VPSA |
|------------------------------|---------------|
| 2001:db8:85a3::8a2e:370:7002 | DEVSTACK_IPV6 |
| 2001:db8:85a3::8a2e:370:7003 | DEVSTACK_IPV6 |

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.

Create Virtual Network

| | |
|---|---|
| User * | <input type="text" value="pdm (#3)"/> |
| Virtual Network Name * | <input type="text" value="VN_cloud_bursting"/> |
| VLAN ID | <input type="text" value="20"/> |
| Set as Default | <input checked="" type="checkbox"/> |
| IPv4 | |
| IPv6 | |
| CIDR * | <input type="text" value="FD6D:8D64:AF0C::"/> / <input type="text" value="64"/> |
| Gateway Address * | <input type="text" value="FD6D:8D64:AF0C::2:2:2:1"/> |
| IP Address Range * | <input type="text" value="FD6D:8D64:AF0C::2:2:2:2"/> <input type="text" value="FD6D:8D64:AF0C::2:2:2:FF"/> |
| <input type="button" value="Create"/> <input type="button" value="Cancel"/> | |

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)
- Whether 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 specify a gateway address for each protection zone

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

Virtual Network created successfully

Virtual Network VN_cloud_bursting pdm

General Information [Set as Default](#) [Delete](#)


| | |
|--------------|------------------------|
| Network Name | VN_cloud_bursting |
| Nova ID | 15 |
| User | pdm (tenant_pdm_ILSFN) |
| VLAN ID | 20 |

IPv6 Information

| | |
|-----------------------|---|
| CIDR | FD6D:8D64:AF0C::/64 |
| Gateway Address | fd6d:8d64:af0c:0:2:2:2:1 |
| Allocatable IP Ranges | FD6D:8D64:AF0C::2:2:2:2 - FD6D:8D64:AF0C::2:2:2:FF Extend Remove |
| | <input type="text" value="start"/> <input type="text" value="end"/> <input type="button" value="Add"/> |

Allocated IPs

FD6D:8D64:AF0C::2:2:2:2 - FD6D:8D64:AF0C::2:2:2:FF



0 / 254

✔ **Note:**

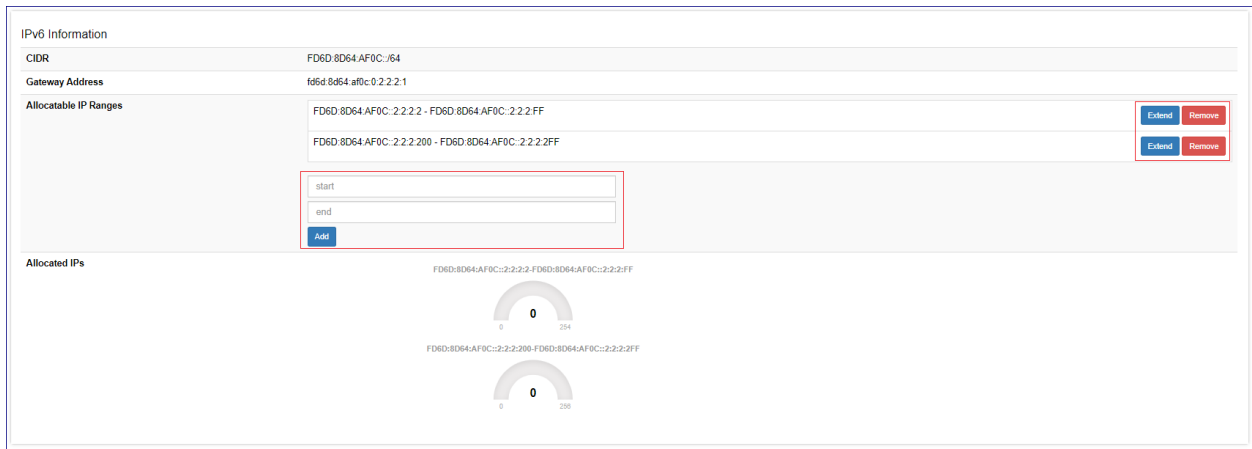
Multiple virtual networks can be defined in the same VLAN

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.

CREATING PUBLIC IP ADDRESSES

By default you access to VPSA instances from the public Internet is not available for security and privacy reasons. The VPSA Front-End IP address which is used for VPSA management (via GUI and REST API) and for data IO workload (host connectivity via iSCSI/NFS/SMB protocols), is allocated on the Zadara Storage Cloud “Front-End” network which is routable only from the Cloud Servers network. Servers outside of the Cloud Servers network cannot reach this IP address.

Public IP addresses are allocated on the Cloud management interface and can be assigned to VPSA instances to enable management access to it from outside of the cloud network.

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

Cloud admins can use command center to define public IP addresses and assign them to VPSA instances. To define a public address range: go to the Public IPs tab and Click on the **New Public IP** button.

On the New Public IP(s) screen provide all the required details to configure the public IP range:

New Public IP(s)

| | |
|--------------------------|--|
| Label * | <input type="text" value="ACME_public_IPs"/> |
| VLAN ID * | <input type="text" value="12"/> |
| Gateway * | <input type="text" value="199.179.0.1"/> |
| Netmask * | <input type="text" value="255.255.255.0"/> |
| Public IP Range * | <input type="text" value="199.179.0.2-199.179.0.5"/> |
| IP Range * | <input type="text" value="129.0.0.2-129.0.0.5"/> |

| property | Description |
|-----------------|---|
| Label | Descriptor for the public IPs |
| VLAN ID | a new\existing VLAN for this Public IP range (different from the cloud tenants 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 | In case NAT is being used : Corresponding internal IP range otherwise : identical to the external range |

To confirm click on the **Submit**, The public IP addresses range will be defined and ready for VPSA allocation.

Public IP(s) created successfully.

zadara-iop-01 Public IPs New Public IP(s)

| VPSA/ZIOS | Label | Public Address | Address | Network Label | VLAN ID | Gateway | Netmask | |
|-----------|-----------------|----------------|--------------|------------------|---------|-------------|---------------|--|
| N/A | test_public_IP | 197.179.0.10 | 197.179.0.10 | FE_MGMT_FEBOND_2 | 11 | 197.179.0.1 | 255.255.255 | |
| N/A | ACME_public_IPs | 199.179.0.2 | 129.0.0.2 | FE_MGMT_FEBOND_2 | 12 | 199.179.0.1 | 255.255.255.0 | |
| N/A | ACME_public_IPs | 199.179.0.3 | 129.0.0.3 | FE_MGMT_FEBOND_2 | 12 | 199.179.0.1 | 255.255.255.0 | |
| N/A | ACME_public_IPs | 199.179.0.4 | 129.0.0.4 | FE_MGMT_FEBOND_2 | 12 | 199.179.0.1 | 255.255.255.0 | |
| N/A | ACME_public_IPs | 199.179.0.5 | 129.0.0.5 | FE_MGMT_FEBOND_2 | 12 | 199.179.0.1 | 255.255.255.0 | |

MANAGING DATA SERVICES

Zadara Cloud administrator can use Command Center to manage and monitor data services deployed on Zadara cloud.

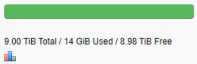
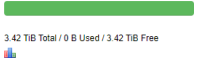
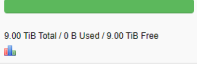
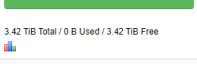
Command center displays the status of data services environments (VPSAs and data services virtual machines) and allows the configuration of data services properties.

11.1 Monitoring Data Services Environments

Command center Displays data services VPSA as part of the cloud VPSA inventory, A DVM label containing data service identification is attached to the VPSAs allowing for its identification as a data services environment.

zadara-qa12 VPSAs

Name User: All Users Comment

| Name | Internal Name | User | Company | Status | Protection Zone | Engine Type | Drives | Base Cache | Ext. Cache | Image | VLAN | Pools | Capacity |
|---|---------------|-------|---------|--------|-----------------|-------------|--------|------------|------------|---------------------|------|-------|---|
| Asigra_VPSA1 DVM - Asigra Backup | vsa-00000003 | admin | zadara | Normal | zone_0 | 600/Boost | 2 | 40 GiB | 0 GiB | vc-20.01-186-qa.img | 50 | 1 |  9.00 TiB Total / 14 GiB Used / 8.98 TiB Free |
| Dima_VPSA1 | vsa-00000004 | admin | zadara | Normal | zone_0 | 600/Boost | 2 | 40 GiB | 0 GiB | vc-20.01-187-qa.img | 50 | 1 |  3.42 TiB Total / 0 B Used / 3.42 TiB Free |
| Dima_VPSA2 | vsa-00000005 | admin | zadara | Normal | zone_0 | 200/Baby | 2 | 20 GiB | 0 GiB | vc-20.01-187-qa.img | 50 | 1 |  9.00 TiB Total / 0 B Used / 9.00 TiB Free |
| Dima_VPSA3 | vsa-00000006 | dima | Zadara | Normal | zone_0 | 200/Baby | 2 | 20 GiB | 0 GiB | vc-20.01-187-qa.img | 50 | 1 |  3.42 TiB Total / 0 B Used / 3.42 TiB Free |

Displaying 4 VPSAs

The Data Services VPSA properties contains specific items that present information on the data service configuration and status:

Information [Launch GUI](#) [Actions](#)

| | |
|------------------------------|--|
| Name | Asigra_VPSA1 |
| Internal Name | vsa-00000003 |
| User | admin (admin admin) |
| Company | zadara |
| Description | |
| Nova ID | vsa-00000003 |
| Status | Normal |
| DVM Status | Normal |
| Protection Zone | zone_0 |
| Image | vc-20.01-186-qa.img |
| IO Engine Type | 600 |
| APP Engine Type | 00 |
| Data Service Type | dvm.200.vf |
| Data Service Version | asigra-20.01-47-qa.img |
| VCPUs | 9 |
| RAM | 30720 MB |
| Base Cache | 40 GiB |
| Extended Cache | 0 GiB |
| Setup Volume Capacity | 10 GiB |
| IP Address | 10.2.12.22/24 |
| DVM Public IP | 172.16.5.30/16 |
| Mgmt. Address | vsa-00000003-zadara-qa12.zadaravpsa.com |
| UUID | 46a76338-9246-4f98-be01-70cabea47d4d |
| SNMPv3 Engine ID | 8000aa8c0546a7633892464f98be0170cabea47d4d |
| Created | January 28, 2020 01:54 PM (2 days ago) |
| Updated | a few seconds ago |

| property | description |
|----------------------|--|
| DVM Status | Status of the DVM Virtual Controller |
| Data Service type | Data service image type |
| Data Service version | Data service image version |
| DVM Public IP | The Public IP address attached to the data services VM |

The Data Services VPSA Networking Configuration also includes the networking configuration of the Data Services Virtual Controller.

Networking Configuration


| VC0 | IP | VLAN ID |
|-----------|------------|---------|
| Frontend | 10.2.12.22 | 50 |
| Backend | 10.3.12.22 | 110 |
| Heartbeat | 10.0.12.22 | |
| Outnet | | |

| VC1 | IP | VLAN ID |
|-----------|------------|---------|
| Frontend | 10.2.12.23 | 50 |
| Backend | 10.3.12.23 | 110 |
| Heartbeat | 10.0.12.23 | |
| Outnet | | |

| VC2 DVM - Asigra backup | IP | VLAN ID |
|---|------------|---------|
| Frontend | 10.2.12.27 | 50 |

11.2 Configuring-Data-Services

Data services can be configured via Command centers Data Services tab.

| Data Services | | | |
|---------------|--------------|---------|---|
| Name | Display Name | Enabled | Actions |
| Asigra | asigra | ✓ |  |

To configure a specific data service click on the Actions icon in the rightmost column that correspond to the requested data service.

configuring Asigra backup data service

Data Services

Name *
Asigra

Display Name *
Asigra Backup

Enabled *

Config *

```

{
  "name": "asigra",
  "storage": { 1 item },
  "category": "Backup",
  "mgmt_url": {
    "port": 9595,
    "suffix": "/amc/",
    "protocol": "https"
  },
  "description": "A comprehensive Backup-as-a-Service solution consist of Asigra's cloud data protection virtual appliance integrated with Zadara's award winning VPSA Storage Array",
  "display_name": "Asigra Backup",
  "data_vm_image": "asigra-20.01-47-qa.img",
  "data_vm_flavors": {
    "basic": { 4 items }
  },
  "data_vm_networking": { 2 items },
  "license_server_url": "zadara.asigra.com",
  "license_server_url_alt": "zadara2.asigra.com"
}

```

From the Asigra data service configuration screens users can:

- Modify the data service display name
- Enable or disable the Asigra backup data service for the Cloud
- Configure data service specific settings using the configuration dialog

```

{
  "name": "asigra",
  "storage": { 1 item },
  "category": "Backup",
  "mgmt_url": {
    "port": 9595,
    "suffix": "/amc/",
    "protocol": "To modify a property just edit it's value"
  },
  "description": "A comprehensive Backup-as-a-Service solution consist of Asigra's cloud data protection virtual appliance integrated with Zadara's award winning VPSA Storage Array",
  "display_name": "Asigra Backup",
  "data_vm_image": "asigra-20.01-47-qa.img",
  "data_vm_flavors": { 1 item },
  "data_vm_networking": { 2 items },
  "license_server_url": "zadara.asigra.com",
  "license_server_url_alt": "zadara2.asigra.com"
}

```

the Asigra data service configuration dialog allows you to set the following:

Data VM storage configuration

| property | description |
|----------|---------------------------------|
| Block | SAN(Block) Disks size and count |
| File | Filesystems(NAS) size and count |

Provisioning Portal(Ecommerce) general attributes

| property | description |
|---------------|---|
| category | Provisioning Portal data service category |
| description | Data Service Description (displayed when user selects on the data service in provisioning portal) |
| display_name | Data service display name in provisioning portal |
| data_vm_image | image file used when provisioning a data VM for this service |

Provisioning Portal(Ecommerce) data service flavors attributes

| property | description |
|--------------|-------------------------------------|
| flavor | Data VM flavor internal type |
| vm_count | Data VM count for this data service |
| vpsa_flavor | Bundled VPSA internal type |
| display_name | Flavor display name |

Data VM networking attributes

| property | description |
|-------------------------|---|
| fe_allowed_ports | Ports that are allowed on the data VM front end network |
| public_ip_allowed_ports | Ports that are allowed on the data VM public network |

Data VM licensing attributes

| property | description |
|------------------------|--------------------------------|
| license_server_url | Primary licensing server URL |
| license_server_url_alt | Alternate licensing server URL |

PERFORMING IMAGE MANAGEMENT


Using Command Center administrators manage virtual machine images for:

- VPSA
- VPSA Object storage
- CCVM

Cloud administrator can pull specific images from a repository and set a set of images a default, Default images will be the ones deployed when a new VPSA instance is crated.

12.1 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 register. To pull image packages from the Zadara repository click on the  icon on the top right part of the screen and select **manage cloud packages** from the drop down menu. Make sure that you 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://zadara-storage-install/` and it is set as the default Command center repository.

zadara-qa16 Packages 

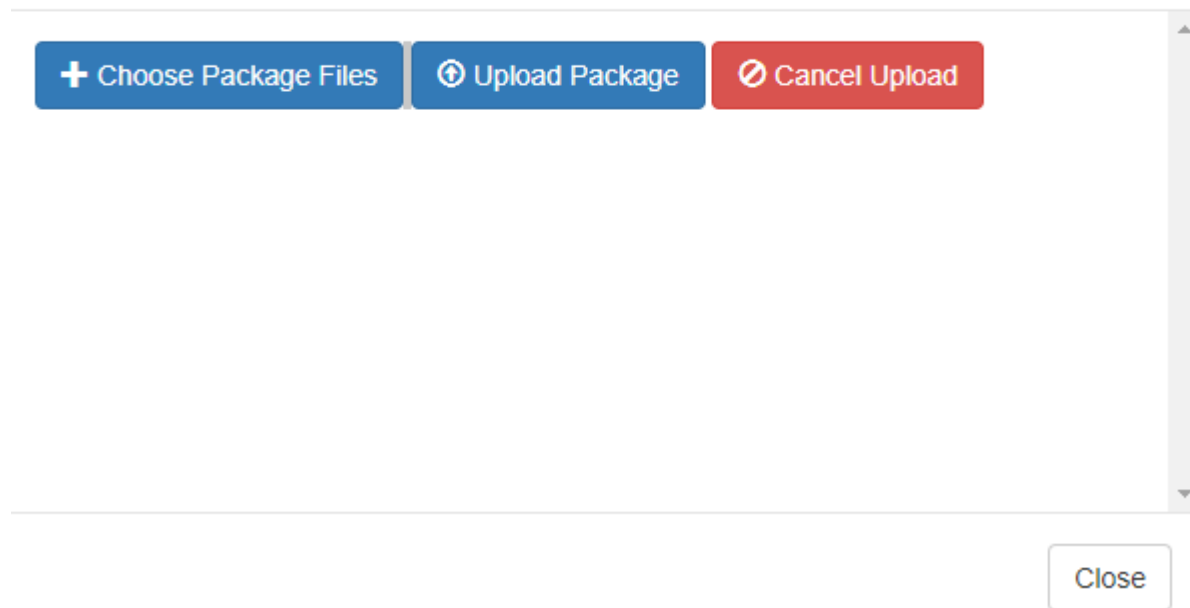
Default
 Custom
 S3:// source

Settings version: 20.12-230

| Name | Status | Actions |
|-----------|----------------------------------|---|
| 20.12-259 | Downloaded (not in s3) | <input type="button" value="Erase"/> |
| 20.12-265 | Downloaded (not in s3) | <input type="button" value="Erase"/> |
| 20.12-245 | Partially downloaded (not in s3) | <input type="button" value="Erase"/> |
| 20.01-383 | Available for download | <input type="button" value="Download"/> |
| 20.01-386 | Available for download | <input type="button" value="Download"/> |
| 19.08-214 | Available for download | <input type="button" value="Download"/> |
| 20.12-238 | Downloaded (no zios) (not in s3) | <input type="button" value="Erase"/> |

Packages can also be uploaded from local storage in case 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 windows 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.

Upload Package



A list of the selected files will be populated to the popup window, to begin uploading the package click on **Upload Package**.

Upload Package

| File Name | Size | Progress |
|-----------------|---------|----------------------|
| build.mf | 0.47 KB | <input type="text"/> |
| build.mf.md5sum | 0.09 KB | <input type="text"/> |

Upload progress is tracked on a file level progress bar. When 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. On 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.

Register image

Please select version:

19.08-102 ▼

19.08-102
19.08-112

Image type(s):

- VPSA
- Object Storage
- CCVM
- Set VPSA/Object Storage image as default

Cancel Register

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.


CUSTOMIZING VPSA AND OBJECT STORAGE USER INTERFACE

Command center allows cloud administrators to personalize their underlying VPSA/VPSA object storage User interface look and feel by modifying the VPSA login header image and the favicon which appears on the browser tab and the UI left menu panel.

To customize the underlying VPSA/VPSA object storage UI images for the login header and the favicon should be prepared in advance according to the following demands:

- Login header image must be in jpeg format and in the following dimensions : height 115px and width 400px
- Favicon image must be in png format and in the following dimensions : height 16px and width 16px.





To perform customization click on the  icon on the upper right corner of the screen and select **UI customization** from the drop down menu. Click on the tab for the specific entity you would like to personalize (VPSA/VPSA Object Storage) and use the **Choose File** buttons to upload the images you prepared and confirm by clicking on the **Update** button.

After upload has been successfully performed you should see your modified header and favicon presented.

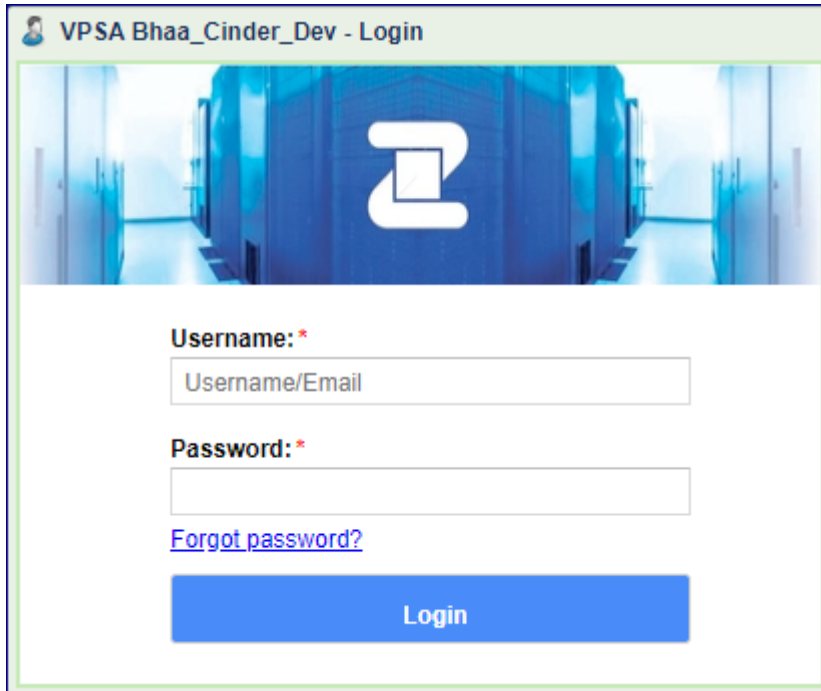
Customization

VPSA [Object Storage](#)

Images

| Name | Custom | Notes | Delete |
|---|---|--|--------------------------|
| Favicon <input type="button" value="Choose File"/> No file chosen |  | Must be png format with the dimensions 16x16. | <input type="checkbox"/> |
| Header Image (Logo) <input type="button" value="Choose File"/> No file chosen |  | Must be a jpg with a height of 115px and width of 400px. | <input type="checkbox"/> |

VPSA Login with modified header:




VPSA menu header with modified favicon:



✓ **Note:**

The modified header image and favicon will be applied to newly created VPSA/VPSA Object storage instances or for instances that has been hibernated and then restored.




To undo personalization and revert to the default header image and favicon click on the  icon on the upper right corner of the screen and select **UI customization** from the drop down menu. Click on the tab for the specific entity you would like to personalize (VPSA/VPSA Object Storage) check the boxes on the Delete column for the images you want reverted and click on the **Update** button to confirm.

MANAGING COMMAND CENTER USERS AND ROLES

Command center provides role based user management functionality.

Granular per-activity user roles can be defined and assigned to command center user accounts.

Users and roles settings can be reached by clicking the  icon on the upper right corner of the screen and selecting the **users\roles** options on the drop down menu.

14.1 Managing Roles

By default a view only non modifiable role with access to all managed resources exists in the system. Additional Roles can be defined as required.

Roles

| Name | Permissions |
|--------------|---|
| Read Only | Access Logs : View Protection Zones : View App Engine types : View Central logs : View Cloud users : View Clouds : View Custom networking : View Drive types : View Drives : View IO Engine types : View Images : View Licensing : View Remote Authentications : View Storage nodes : View Public IPs : View VLANs : View Vpsas : View |
| limited_view | Access Logs : View Protection Zones : View App Engine types : View Central logs : View |

Create new role

Defining a new custom role

To define a new custom Role: click on the **Create new role** button and define the exact permission you would like to assign to the new role. Name the new role and click **create** to confirm creation. The newly created role with the specified permissions can be viewed from the roles screen.

✔ **Note:**

The 'select all' or 'import role' options can be used to simplify and shorten role creation process.

Editing a custom role

To edit a custom role click on the downward arrow icon on right side of the screen and select the Edit option from the drop down menu. The edit role screen will load, Modify the custom role as required and click on the update button to apply modifications.



Deleting a custom role

To edit a custom role click on the downward arrow icon on right side of the screen and select the Destroy option from the drop down menu. A confirmation message will appear, Click on **confirm** to delete the custom role.

14.2 Managing Command Center Users

Defining a new local user



In the users management screen click on the **create new user** button

Provide the users email address (that will serve as his Command center user id), First and last name tick the admin checkbox if this user requires full administrative privileges or select a specific role to assign for the user and click on the **Create** button. A confirmation message will be displayed specifying that the newly created user will be emailed with a temporary password for his first login.

On the first login to Command center the newly created user will be prompted to replace his temporary password.

Disabling a local user

From the users management screen locate the user you would like to disable and click on the downward arrow button on the right side of the screen.

| Users | | | | | | |
|--|-----------|--------|-------|---------|-------------|---|
| User | Roles | Domain | Admin | Enabled | Dual Factor | Actions |
| <input type="checkbox"/> team@zadarastorage.com | | local | Yes | Yes | No |  |
| <input type="checkbox"/> firemansam@pontypandy.com | Read Only | local | No | Yes | No |  |

On the drop down menu select Disable, A confirmation message will appear on the upper part of the screen and the users enabled property will be set to No.

Deleting a local user

From the users management screen locate the user you would like to disable and click on the downward arrow button on the right side of the screen.


On the drop down menu select Delete, A popup windows requesting confirmation will appear, review that the user id about to be deleted is correct and click on **confirm** to perform deletion.

Importing users from an external directory

Defining connection to a directory server

To import users from an external directory service a connection to the service has to be defined. From Command center



main dashboard click the  icon on the upper right corner of the screen and select Remote Authentication from the drop down menu. Click on the **Add Authentication Server** button and provide the required details for the external directory connection.

Add Authentication Server

Type

Active Directory as LDAP server ▼

Domain ⓘ**Domain Alias** ⓘ**Port**

389

Base DN ⓘ**DNS IP#1 (optional)** ⓘ**DNS IP#2 (optional)** ⓘ

SSL

Enabling this option requires uploading server certificate (*.crt) file

Save

| 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 |

After filling all required information click on the **Save** button to define the external directory.

Important: Command Center uses LDAP or LDAPS protocol to integrate with Microsoft Active Directory. LDAP connectivity is done over port 389/TCP or 636/TCP in case of LDAPS.

Importing domain users

From the users screen click on the **import directory users** button. Select the domain name for the directory server you defined and type the logon credentials for domain connectivity. A pop up screen containing a list of domain users will appear, Select the ones you would like to allow command center logon for.

Import Directory Users

Please select the users you would like to import

Users

Nothing selected

- AWSAdminD-9267102432
- ashley.j.williams
- madison.bumgarner
- Administrator
- shohei.ohtani
- buster.posey
- barry.bonds
- mike.trout
- tim.salmon
- krbtgt
- Guest

Same as with creating a local user; each imported user can be assigned with a role that will determine its specific privileges.

Import Directory Users

Please select the users you would like to import

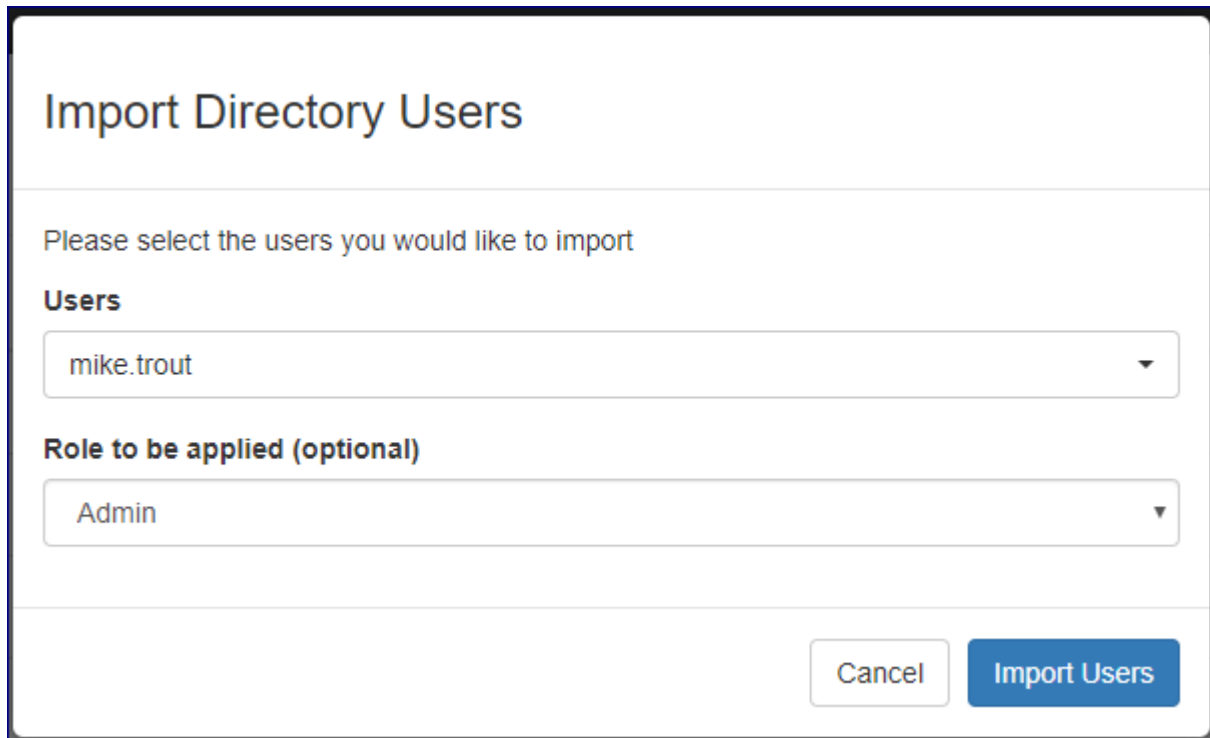
Users

mike.trout ▼



Role to be applied (optional)

Admin ▼

Cancel Import Users









After confirming creation the imported users will appear on the command center users list, Imported can be differentiated from local users via the domain property displayed on the users management screen.

Command Center Timezone: Etc/UTC CONTOSO\amacgyver  

Users successfully imported

Users

| User | Roles | Domain | Admin | Enabled | Dual Factor | Actions |
|--|-------|----------|-------|---------|-------------|---|
| <input type="checkbox"/> djohnson@contoso.com | | local | Yes | Yes | No |  |
| <input type="checkbox"/> amacgyver@contoso.com | | local | Yes | Yes | No |  |
| <input type="checkbox"/> hsimpson@contoso.com | | local | Yes | Yes | No |  |
| <input type="checkbox"/> sjobs@contoso.com | | local | Yes | Yes | No |  |
| <input type="checkbox"/> ltorvalds@contoso.com | | local | Yes | Yes | No |  |
| <input type="checkbox"/> mike.trout | | MYDOMAIN | Yes | Yes | No |  |

[Create new user](#) [Import directory users](#)

Version zadara-command-center 18.11-234

MANAGING CLOUD SETTINGS

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



Cloud settings can be reached by clicking the  icon on the upper right corner of the screen and selecting the **Settings** option on the drop down menu.

Cloud setting managed by command center are divided into 5 categories:

| 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 |

15.1 General Cloud Settings

General Settings

| | |
|---|---|
| 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 accessibility 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. |
| 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 (GB). |

Cloud Name Allows to change the Cloud name

✓ Note:

Cloud name can be set only if the cloud does not contain any VPSA/VPSA Object Storage entities

Domain Name

Sets the domain name that will be used for sender address in emails sent from the cloud.

Internet Access Toggles between Online and Offline Cloud. An Offline cloud is defined as a Cloud that has no internet

access for management. Users of offline clouds are required to provide local SMTP , FTP and NTP services and to configure support ticket and Zsnap methods accordingly. In offline clouds license management is also performed manually as there is availability of a remote licensing server.

✔ **Note:**

MAG files will be created and upload only in clouds with internet access

Support ticket method Toggles support tickets sending on/off and to select the ticket transmission method. Valid options for support ticket transmissions are Zendesk or SMTP

Settings for Zendsesk ticket transmission:

Support ticket method

Method default - zendesk

Uri* default: https://zadarastorage.zendesk.com **Use default**

Username default: auto@zadarastorage.com **Use default**

Password **Use default**

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

Settings for SMTP ticket transmission:

Support ticket method

Method SMTP

NOTE: SMTP setting will be ignored in case internet access is enabled

Server* default: 172.16.7.81 **Use default**
Please fill out this field.

Login

Login user

AUTH method PLAIN default: PLAIN **Use default**

Password

Port 25 default: 25 **Use default**

Port ssl 465 default: 465 **Use default**

Secure

Source email address default: auto@zadarastorage.com **Use default**

Destination email address default: qa@zadarastorage.com **Use default**

Update **Cancel**

| 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 |

Emails sending method

Allows the cloud admin to configure a personalized email account from which customer emails will be issued. The cloud admin can also define the support email address which will be referenced in the emails body as the support contact email.

✔ Note:

In case emails sending method is not defined and the cloud has internet connectivity customer emails will be issued from Zadara’s AWS SES email account.

In case emails sending method is not defined and the cloud does not have internet connectivity customer emails will be issued from the SMTP account defined in the Support ticket method section.

Settings for personalized SMTP account

Emails sending method

Support email ⓘ support@zadarastorage.com default: support@zadarastorage.com Use default

Method

Server* ⓘ Please fill out this field.

Login ⓘ

Login user ⓘ

AUTH method default: PLAIN Use default

Password ⓘ

Port ⓘ default: 25 Use default

Port ssl ⓘ default: 465 Use default

Secure ⓘ

From user ⓘ default: auto@zadarastorage.com Use default

| 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 |

Upload endpoints settings

Allows the cloud administrator to configure alternate endpoints for upload of cloud Zsnaps, Mag and configuration information

Upload endpoints can be of the following types:

- AWS S3 endpoint
- VPSA Object Storage endpoint
- FTP target

Upon entry this section will display details on the clouds configured endpoints.

Upload Endpoints [New](#)

Available AWS S3 Endpoints

| Name | Method | Access Key | Region | Actions |
|-----------------------------|--------|-----------------------|-----------|---|
| zadarastorage_metering_test | AWS S3 | AKIAYNVAWXSNS5SGSI7YT | us-east-1 | Edit Delete |
| default_config_ep | AWS S3 | AKIAIRPPLTX5X6FMD62A | us-east-1 | |
| default_mag_ep | AWS S3 | AKIAJW52QPHI22XFBNSA | us-east-1 | |
| default_zsnap_ep | AWS S3 | AKIAIRPPLTX5X6FMD62A | us-east-1 | |

Displaying 4 Endpoints

Available ZIOS S3 Endpoints

| Name | Method | Access Key | Endpoint | Region | Actions |
|--------------|---------|----------------------------------|---|-----------|---|
| zCenter_Zios | ZIOS S3 | 7fba5c98d3ab43e8bde90f836d76ebce | https://vsa-00000283-public-zadara-qa9.zadaraeios.com | us-east-1 | Edit Delete |

Displaying 1 Endpoints

The Cloud administrator can configure additional upload endpoints by clicking on the **New** button on the top left corner of this section.

Upload Endpoints Create Upload Endpoint

Endpoint Name

Method

Access Key

Secret Key

Region

[Save](#) [Cancel](#)

Upload endpoint configuration requires the following input:

| Parameter | Description |
|---------------|--|
| Endpoint name | A name for this upload endpoint |
| Method | Endpoint type(AWS S3/VPSA Object Storage/FTP) |
| Access Key | in case of AWS S3/VPSA Object Storage a valid access key for this endpoint |
| Secret Key | in case of AWS S3/VPSA Object Storage a valid secret key for this endpoint |
| Server | in case of FTP the FTP server address |
| User | in case of FTP the FTP FTP user |
| Password | in case of FTP the FTP FTP password |
| Use Proxy | in case of FTP wether to use a proxy for FTP connection |

To configure the new upload endpoint provide all required details and click on **Save**, your endpoint will be created. User configured endpoints can also be updated or deleted.

ZSNAP upload settings

Sets upload target used for the cloud zSnaps upload.

✓ Note:

Only one upload endpoint can be specified for zSnap upload.

Settings for zSnap upload to an AWS S3/VPSA Object Storage endpoint:

ZSnap upload

Endpoint: * zsnap_ep

Upload method: ZIOS S3

Bucket:

zadara-support

| Parameter | Description |
|-----------|-------------------------|
| Bucket | bucket for ZSANP upload |

Settings for zSnap upload to an FTP endpoint

ZSnap upload

Endpoint: * dummyftp

Upload method: FTP

Max Allowed MB (min:1 max:200000)

Max Retain MB (min:1 max:150000) *

| Parameter | Description |
|----------------|--|
| Max-allowed-mb | When using CCmaster FTP server. maximum ZSNAP capacity threshold |
| Max-retain-mb | When using CCmaster FTP server. minimum ZSNAP capacity retained |

Settings for metering data upload

Sets the target endpoints to which metering data can be uploaded. Up to 3 AWS S3 endpoints can be configured for metering data upload. To add additional upload endpoints click on the **Add Another** button. Additional endpoints can also be removed by clicking on the **Discard** button.

Metering data upload

Endpoint: * default_mag_ep

Upload method: AWS S3

Bucket: zadarastorage-metering-test

Endpoint: default_zreport_ep Discard Endpoint

Upload method: AWS S3

Bucket:

test

Update Cancel Add Another

| Parameter | Description |
|-----------|---------------------------------|
| Bucket | bucket for metering data upload |

Settings for configuration data upload

Sets the target endpoints to which configuration data can be uploaded. Up to 3 AWS S3 endpoints can be configured for metering data upload. To add additional upload endpoints click on the **Add Another** button. Additional endpoints can also be removed by clicking on the **Discard** button.

Cloud configuration upload

Endpoint: * default_config_ep

Upload method: AWS S3

Bucket: zadarastorage-config-uploads

Endpoint: default_zreport_ep Discard Endpoint

Upload method: AWS S3

Bucket:

test

Upload period (seconds)* ⓘ min: 60
default: 3600 Use default

Update Cancel Add Another

| Parameter | Description |
|-------------------------|---|
| Bucket | bucket for configuration data upload |
| Upload period (seconds) | Sets the configuration data upload interval |

Cache/AFA-Meta drives settings

Configures the behavior of the cloud when provisioning VPSA all flash 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 |

Mount Capacity Threshold

Sets the Clouds /mnt/Nova folder capacity threshold. an alert will be issued in case this capacity threshold is exceeded.

| Parameter | Description |
|--------------------------------------|--------------------------|
| Mount Capacity Alert Threshold (GiB) | Capacity treshold in GiB |

Ticket threshold

Sets 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 |

CCVM Engine size

Sets the CCVM configuration in terms of CPU and memory.

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

Automatic drive replacement

Configuration for the cloud automatic drive replacement feature. When Automatic drive replacement is enabled replacement will be triggered for a failed drive reported in any cloud resident VPSA. The Drive replacement will be performed after a user provided monitoring interval. Failed drives will be replace by drives from similar model an similar capacity (given that spares from this drive types exist in the cloud).

Automatic Drive Replacement

Enable Automatic Drive Replacement 📘

Automatic Drive Replacement Timeout 📘 *min:5 max:600*

| Parameter | Description |
|------------------------------------|---|
| Enable Automatic Drive Replacement | Is auto replace enabled |
| 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 will not occur for drives which are members in a RAID group with dedicated hot spare drive defined. Automatic drive replacement will not occur when more than 4 drives fail at the same time.

15.2 Security Settings

| | | |
|-----------------|--|--|
| General | Security Settings | |
| Security | Password expiration | Set when passwords expires and set how many old passwords the system will forbid to reuse. |
| Network | VPSA API Passthrough | Allow VPSA APIs to Pass-Through Command Center server. |
| VPSA | Default zadarastorage.com Certificate | Set the certificate used for zadarastorage.com. |
| Object Storage | 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 |

Password expiration

Settings to determine the managed entities password 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 certain password is valid |
| Password history | Number password replacement cycles in which a password cannot be repeated |

VPSA API Passthrough

Allows VPSA instances running in the cloud to 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.

Custom Certificate for Command Center & Provisioning Portal

Allows replacement of the default certificate used in Command Center and Provisioning Portal 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.

Trusted CAs

Allows for adding certificate authorities to the VPSACommand Center Trusted CA lists by uploading Certificates signed by them bundled in a .zip file.

Dual Factor

Turns on dual factor authentication for all local command center users.

Cloud Control IP Whitelist

Turns on and manages 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. Similarly, 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.

Cloud Remote Access

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

15.3 Network Settings

| | | | |
|----------------|--|--|----------------------|
| General | Network Settings | | |
| Security | MTU Size | MTU Size. | Edit |
| Network | Protection Zones Backend Connectivity | Protection Zones Backend Connectivity. | Edit |
| VPSA | | | |
| Object Storage | | | |
| Management | | | |

MTU Size

Allows user to increase their Cloud Networks MTU.

| Parameter | Description |
|-----------------|---|
| FE MTU size | MTU size for the VPSA network (Front-End) |
| Public MTU size | MTU size for the public network |

✓ Note:

FE MTU setting effect all custom networks defined in the cloud.

Protection Zones backend connectivity

Allows to configure the use of the iSCSI protocol instead of the iSER protocol in multizone clouds. Protection Zones backend connectivity settings modifies the backend protocol used for inter-zone connectivity **only** (in-zone requests will still use iSER). Inter-Zone Backend connectivity should be switched to iSCSI only in cases where iSER connectivity cannot be established between zones (for example due to the network setup).

Protection Zones Backend Connectivity Set the protocol to be used for remote region backend connectivity. This setting should be modified only in case iSER connectivity cannot be established between Protection Zones.

Remote region backend protocol: iSCSI default: iSER Use default

Verify that no Multizone VPSAs running in this cloud before switching the remote region backend connectivity type.

Update Cancel

To configure iSCSI Inter-Zone Backend connectivity first make sure that no multizone VPSA\Object storage is already configured in the cloud . Set Remote region backend protocol to iSCSI and click on the **Update** button to apply settings.

When Remote region backend protocol is set to iSCSI a warning message will be displayed on Command center Protection Zone tab.

zadara-qa14 Protection Zones

⚠ WARNING - iSCSI protocol is being used for remote region backend connectivity

| Name | Internal Name | Internal | Storage Nodes | Object Storage Fault Domains | VPSAs/Object Storage |
|--------|---------------|----------|---------------|------------------------------|----------------------|
| zone_0 | zone_0 | 1 | 4 | 4 | 3 |
| zone_1 | zone_1 | 2 | 4 | 4 | 3 |



Warning:

switching inter-region connectivity protocol to iSCSI might impact VPSA/Object storage performance

15.4 VPSA Settings

General

Security

Network

VPSA

Object Storage

VPSA Settings

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.

Domain name

Sets the domain name to be used for VPSA entities defined on the cloud.

Recycle bin

Sets the period (in days) in which deleted VPSA entities remain in the recycle bin before being purged from the system therefore becoming unrecoverable.

Certificate

Allows replacement of the default certificate used in VPSA web management application 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.

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

The new certificate can be propagated to all existing VPSAs by marking the **Update new certificate on all running VPSAs in the cloud** checkbox, that displays after uploading the new certificate and key files.

15.5 Object Storage Settings

| | | |
|-----------------------|--------------------------------|---|
| General | Object Storage Settings | |
| Security | 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. |
| Network | | |
| VPSA | | |
| Object Storage | | |

Certificate

Allows replacement of the default certificate used for newly VPSA Object storage web management application 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.
To replace certificates used in existing VPSA Object storage instances use the VPSA GUI.

15.6 Management Settings

| | | |
|-------------------|----------------------------|------------------|
| General | Management Settings | |
| Security | SNMP | SNMP |
| Network | | |
| VPSA | Tickets Settings | Tickets Settings |
| Object Storage | | |
| Management | | |

SNMP

The Zadara cloud ecosystem supports Cloud/VPSA/Object Storage administrator level infrastructure monitoring via SNMP Traps. Zadara Cloud SNMP traps are architecture to alert administrator on infrastructure events and are produced in parallel to Zendesk tickets.

SNMP traps can be sent from:

- VPSA
- VPSA Object Storage
- Cloud Storage Nodes
- CCVM

The Zadara cloud SNMP MIB is publicly available for downloading at the following link: <https://zadara-storage-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/VPSA Object Storage entities in version 20.01 and above
- Storage Node level SNMP traps are not supported for nodes running with trusty kernel

General SNMP Setting

SNMP

Enable snmp

Minimum ticket priority ⓘ default: normal Use default

Trap recipient*

Protocol Version

| Parameter | Description |
|-------------------------|---|
| Enable SNMP | If checked - SNMP Traps will be sent from all the cloud monitored elements according to the specified configuration |
| Minimum ticket priority | Minimum priority set for a Zendesk ticket from which an SNMP trap will also be sent |
| Protocol Version | SNMP version to be used (supported versions are SNMPv2 and SNMPv3) |

✓ Note:

SNMP Traps are not bound to any specific network. The network interface from which SNMP traps will be sent will be determined according to the managed entity routing configuration

Settings for SNMPV2

SNMP

Enable snmp

Minimum ticket priority default: normal Use default

Trap recipient*

Protocol Version

Community default: public Use default

| Parameter | Description |
|-----------|----------------------------------|
| Community | SNMPv2 trap community to be used |

Settings for SNMPV3

SNMP

Enable snmp

Minimum ticket priority default: normal Use default

Trap recipient*

Protocol Version

Username*

Auth protocol

Auth key

Privacy protocol

Priv key

| 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. |

✓ Note:

SNMPv3 supported modes of operations are : NoAuthNoPriv, AuthNoPriv, AuthPriv

Testing SNMP Settings Cloud Administrator can test and validate their SNMP settings prior to applying then by sending a test trap. Test traps are produced by clicking on the **Test** button on the SNMP settings dialog, Test traps are produced and transmitted according to the specified settings.

Working with SNMPv3 Engine IDs Sending and receiving SNMPv3 Traps requires the usage of a managed element identifier known as SNMP Engine ID. Each managed element engine ID should be configured in the SNMP trap recipient to allow receipt of traps from this entity. The Zadara cloud defines a different engine ID for :

- The Zadara Cloud infrastructure(All Storage Node and the Cloud Controller VM)
- Each VPSA/VPSA Object Storage entity

The Engine ID for the Zadara Cloud infrastructure is specified on the bottom right corner of the screen.

```

UUID 1b9346c6-7a5d-4363-a895-356711c7734a
SNMPv3 Engine ID 8000aa8c051b9346c67a5d4363a895356711c7734a
Version zadara-command-center 20.01-167

```

The Engine ID for a VPSA/VPSA object Storage entity is specified in the entities property tab.

| | |
|-------------------------|--|
| Public IP | None |
| Mgmt. Address | vsa-00000029-zadara-iop-01.zadaravpsa.com |
| UUID | 2990c33e-9cd6-4222-bbc2-cdd3f137e734 |
| SNMPv3 Engine ID | 8000aa8c052990c33e9cd64222bbc2cdd3f137e734 |
| Created | January 20, 2020 10:28 AM (6 hours ago) |
| Updated | a few seconds ago |

✓ Note:

for VPSA/VPSA Object storage entities with versions lower than 20.01 - SNMPv3 Engine ID will not be displayed.

Ticket Settings

The Ticket Settings Section allows the cloud administrator to override the default attributes of the cloud infrastructure support tickets.

Ticket attributes can be configured in 2 different scopes:

- Cloud level scope - performed from Command Center Settings management section
- VPSA/VPSA Object Storage scope - performed from the virtual array settings tab

✓ Note:

In case of conflict between global and VPSA/VPSA Object Storage ticket settings VPSA/VPSA Object storage setting are applied for tickets produced by the virtual array.

Tickets Settings

Message id *
 TICKET_ ANTIVIRUS_ENGINE_ENABLED

Suppression expiration date (UTC)

Priority
 Default

Zsnap
 Default

Send To Users
 Default

Rate limit (seconds)

Comment *

Save

| Parameter | Description |
|-------------------------------|--|
| Message ID | The Message Id of the ticket to be configured |
| Suppression expiry date (UTC) | Sets a ticket as suppressed until a given timestamp. Suppressed will not be sent into zendesk from this particular cloud |
| Zsnap | allows the user to configure weather a Zsnap will be created when this ticket is produced and what type of Zsnap will be created (full/light) |
| Send To Users | indicates weather tickets for the specific message id will be sent to cloud users that have enabled notifications. |
| rate limit(seconds) | The interval from the time a specific ticket is produced to the time in which another ticket with the same message id and concerning the monitored element can be produced again |
| comment | User Filled Comment explaining the reason for this attributes change |

After creation of a custom ticket rule the initial dialog of the ticket settings section will be modified to display the rules currently applied on this cloud.

Tickets Settings New

| Message | Suppression expiry date (UTC) | Priority | Zsnap | Send To Users | Rate limit (seconds) | Comment | Last Modified By | Actions |
|------------------------|-------------------------------|----------|---------|---------------|----------------------|---|----------------------|-------------|
| TICKET_FC_LINK_FAILURE | | Default | Default | No | | Refrain from sending to cloud users due to customer request | qa@zadarastorage.com | Edit Delete |
| TICKET_TEST | 2021-01-30Z18:00 | Default | Default | No | | Testing suppression | qa@zadarastorage.com | Edit Delete |

Displaying 2 Tickets

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 in a single VPSA or VPSA Object Storage Scope and vice versa.

MANAGING CLOUD LOGS

Command Center maintains a centralized cloud level event log which can be utilized for detailed infrastructure monitoring and troubleshooting. Log event can be viewed and searched from the Command Center Central Log tab. Events may also be shipped to an external syslog daemon for 3rd party application based event monitoring.

16.1 Searching And Filtering Logs

Cloud log can be searched and specific events extracted using the Command Center filtering functionality. To search for specific content in log messages:

On the Central Log tab select **Message** in the **Add Filter** list box. Type a search string in **Contains** or an exclude string in **Doesn't Contain** and Click on the **Filter** button

| ID | Source Type | Source Name | Message | Severity | Time |
|------|-------------|-------------|---|----------|-----------------------------|
| 1311 | sn | qa16-sn1 | ZSnap uploaded to s3://zadara-storage-support/zadara-qa16/Tickets/1225515/tix-1225515-zsnap-qa16-sn1--2019-08-11--16-03-18.tar.gz | info | 2019-08-11 16:07:01 (+0300) |

Total messages: 1

Additional filters can be applied by selecting more statements in the **Add Filter** list box.

Users can filter log messages by:

| Statement | Description |
|--------------|---|
| Message | Search\exclude string |
| Created | Event creation date range |
| Min Severity | Minimum severity level |
| Source Type | Element in which event occurred (Storage Node, VPSA, etc.) |
| Source Name | Selection\exclusion of a specific element |

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

16.2 Forwarding Events To A Syslog Daemon

To forward cloud events events to an external syslog daemon:

On the Central Log tab select click on the **RSYSLOG Servers** caption. In the text box below type your syslog server IP address and the syslog daemon port number separated by “:” . Click on the **Add** button to apply changes.

The screenshot shows the 'RSYSLOG Servers' configuration page. At the top, there is a header 'RSYSLOG Servers' with an upward-pointing arrow. Below this is a table with a single row. The table has two columns: the first column contains a checkbox, and the second column contains the text 'my.syslog.server:514'. Below the table, there is a text input field containing 'my.syslog.server:514' and a blue 'Add' button.

To stop forwarding cloud events 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.

The screenshot shows the 'RSYSLOG Servers' configuration page. The table from the previous screenshot is shown, but the checkbox next to 'my.syslog.server:514' is now checked and highlighted with a red square. Below the table, there is a text input field containing '<url>:<port>', a blue 'Add' button, and a red 'Delete selected' button, which is also highlighted with a red square.

16.3 Managing Command Center Access Log



To view command center access log click on the  icon on the top right side of the screen and select Access logs from the drop down menu.

Access log messages can be filtered in a similar way as with cloud central logs.

Available filter statements are :

| Statement | Description |
|-------------|--|
| Action | Command center Action performed or attempted |
| Access Type | Web or API access |
| IP Address | Originating IP address |
| User | Originating User ID |
| Created | Log record creation date |

Filters

Add Filter

Action is

Created

Filter Clear

Per page

100

| 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"] | 2019-08-06 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

USING COMMENTS IN COMMAND CENTER

17.1 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/VPSA object storage
- Cloud users
- Disk drive series/Individual disk drives

Comments as assigned with a severity level, supported levels are : low , medium ,high and critical. An indication of all cloud comments according to their severity is displayed on Command centers main dashboard.



All comments created in command center can be displayed by clicking on the comment section on command centers 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>code block</code> in it. | Critical | pdm@zadarastorage.com | 2019-10-10 11:59:31 UTC | ▼ |
| Node | zdr-iop-sn-01 | this comments contains several items: <ul style="list-style-type: none"> 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 <code>markdown</code> | 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 | <i>this is another test comment with markdown</i> | Low | pdm@zadarastorage.com | 2019-10-10 11:08:46 UTC | ▼ |

Displaying 7 Comments

17.2 Working With Comments

To add a new comment to a supported command center entity navigate to its dashboard and click on the comments tab and then on the **New Comment** button. Assign a severity to your comment ,add the required content and tick the Pin to dashboard box if you want this specific comment text to be displayed on the elements dashboard. Click on the **Save** button to create the new comment.

Severity High

Pin to dashboard

Content Preview Markdown cheatsheet

this comment should be "pinned to dashboard"

Remaining Characters: 954

Save

✓ Note:

Comments can be pinned\unpinned from the elements dashboard by clicking on the comments pin icon on the elements Comments tab

Dashboard Drives 16 Virtual Controllers 2 Virtual Networks 1 RAID Groups 10 Pools 2 Comments 2 Logs Settings

Content Severity All Filter New comment

| Content | Severity | Created By | Created At |
|---|----------|-----------------------|-------------------------|
| <input checked="" type="checkbox"/> this comment should be pinned to dashboard | High | pdm@zadarastorage.com | 2019-10-10 13:09:09 UTC |
| <input checked="" type="checkbox"/> this comment should not appear on the dashboard | Critical | pdm@zadarastorage.com | 2019-10-10 10:57:32 UTC |

Displaying 2 Comments

PRIMARY VPSA

High this comment should be pinned to dashboard

Dashboard Drives 16 Virtual Controllers 2 Virtual Networks 1 RAID Groups 10 Pools 2 Comments 2 Logs Settings

Information Launch GUI Actions

| | |
|-----------------|--------------------------|
| Name | PRIMARY |
| Internal Name | vsa-00000013 |
| User | pdm (Product Management) |
| Company | Zadara |
| Description | |
| Nova ID | vsa-00000013 |
| Status | Normal |
| Protection Zone | zone_0 |
| Image | vc-19.08-151-qa.img |
| IO Engine Type | 600 |
| APP Engine Type | 00 |
| VCPUs | 6 |

Objects

| | |
|------------------------|----|
| Drives | 10 |
| RAID Groups | 10 |
| Pools | 2 |
| Volumes | 3 |
| Servers | 2 |
| Containers | 0 |
| Snapshots | 8 |
| File History Snapshots | 0 |
| Mirror Jobs | 0 |
| BZOS backup jobs | 0 |
| BZOS restore jobs | 0 |