Intel® Accelerated Storage Manager

Release 2.0

Linux Administration Guide

December 2018
Revision 2.1

Intel Confidential

Contents

Revision History

Revision Number	Description	Revision Date
0.1	Initial version	June 2016
1.0	Full Release	March 2017
1.1	Update to 1.1 release	April 2017
1.2	Update to 1.2 release	June 2017
1.3	Update to 1.3 release	September 2017
1.4	Update to 1.4 release	February 2018
2.0	Update to 2.0 release	May 2018
2.1	Release with VROC6.0	December 2018

1 Introduction

1.1 Purpose and Scope of this Document

This document offers the guidance to learn, install and use Intel® Accelerated Storage Manager.

This guide assumes a basic knowledge of storage, application, services management and Linux Distributions.

1.2 Acronyms and Definitions

The following terms are used throughout this document to describe varying aspects:

Term	Definition
HTTP/HTTPS	Hyper Text Transport Protocol, application protocol that is a base standard used in WWW.
Certificate Authority	Trusted entity used to sign digital certificates.
HTTPS Certificate	Digital certificate used in data encryption.
REST	Representational State Transfer, a software architecture approach for building scalable web services.
JSON	JavaScript Object Notation, a human readable format used to transmit data.
URI	Unified Resource Identification standard, a string and number standard used to uniquely identifying resource in i.e. network.
OAuth 2.0	Three-legged token based authentication protocol used commonly in REST APIs.
OAuth 2.0 Grant	Method of authentication used by OAuth 2.0.
OAuth 2.0 Scope	Name of the part of protected resource.
Static Content	Web application or HTML/JavaScript/CSS pages that can be hosted from web server.

SSD	Solid-State Drive. A device used for data storage that uses non-volatile memory chips instead of a rotation disk.
S.M.A.R.T	Self-Monitoring, Analysis and Reporting Technology, monitoring system included in HDD/SSD disks that reports various drive information.
RAID	Redundant Array of Independent Disks.
VROC	Intel® Virtual RAID on CPU.

2 Product overview

2.1 Intel® Accelerated Storage Manager

The Intel Accelerated Storage Manager project aims to provide REST API capabilities for various, supported Intel storage products.

Intel ASM is complete RESTful solution providing, among others, features like REST API for system and devices information, RAID information through VROC plugin, authentication and authorization using OAuth 2.0, web page and application serving through built-in web server.

2.2 System Requirements

Distribution	Versions
Red Hat Enterprise Linux	7.4+
SUSE Linux Enterprise Linux	12 SP3+

3 Quick installation guide

This part of guide is focused to show how correctly configure IASM to work on localhost (on the same machine) and login as root. More detailed steps are in next sections.

1. Install all three rpm packages.
2. Open /etc/iasm/iasm.conf with vim, emacs, gedit or any suitable tool to edit plain text file. Use 'sudo' if not logged as root.
3. Find "web_server" and set it to "true".
   Find "web_content" and set it to "/usr/share/iasm/www".

   Find "host" and set it to "127.0.0.1".
4. Go to the very bottom of the file. For each [scope], remove '#' next to "users" and add "root" (without quotation marks) after '='.
5. Save the file.
6. Open /usr/share/iasm/www/config.json.
7. Add "http://127.0.0.1:80" (**with quotation marks!**) between '[]' for RESOURCE_SERVER_ARRAY.
8. Save the file.
9. Open terminal and put these commands:
   ```
   systemctl enable iasmd
   systemctl restart iasmd
   ```
10. Use "systemctl status iasmd" to check if IASM is alive. If not, there's a syntax error in the config file.
11. Open browser and just type in url field: 127.0.0.1
    Browser should open page named: 127.0.0.1/#/login
12. Login as root using Linux password. Leave "domain" empty.

4 Theory of operation

4.1 Service operation modes

Depending on configuration, Intel ASM can work in several operating modes.

One instance of Service can operate in one or many modes at a time.

Following sections describe available modes in detail.

4.1.1 Authentication server

This is a mandatory mode to be used with Intel ASM. Depending on configuration at least one authentication server needs to be present in the network in order to provide user authentication and authorization.

Intel ASM Service, configured to act as such server, provides OAuth 2.0 interface for client applications. To perform authentication, service can be configured to use OS user database or domain database.

Each application, before using REST API, needs to authenticate itself to this server to obtain special access token, used later in client – server communication.

For details about using authentication mechanism refer to Intel ASM Security API specification.

4.1.2 Resource server

Resource server is a basic mode of Intel ASM. It provides REST API capabilities listed below:

- **System information**: basic information about platform and system where server is running, such as name and version of the running operating system, CPU and Memory usage as well as performance information.
- **SSD Information**: set of information about connected SSD devices and partial information about HDD devices, like device identity and S.M.A.R.T.
- **VROC management:** provides management capabilities for Intel® Virtual RAID on CPU.

For more details about REST APIs, refer to Intel ASM REST specifications (section 7).

4.1.3 Application Server

One of the features of Intel Accelerated Storage Manager is to serve static content (HTML pages or HTML/JavaScript applications).

After configuring Intel ASM, such application will be available on given IP address and port.

However, Intel ASM is not responsible for application functioning except the Intel ASM Management Console provided with this release.

4.2 Standalone configuration

Depending on user choice, Intel Accelerated Storage Manager can be configured to run on one server machine – in standalone configuration.

In such configuration, service runs in all operation modes at a time. It provides authentication interface, application server and resource server capabilities on a single machine, under one configured IP address and port (see Figure 1).

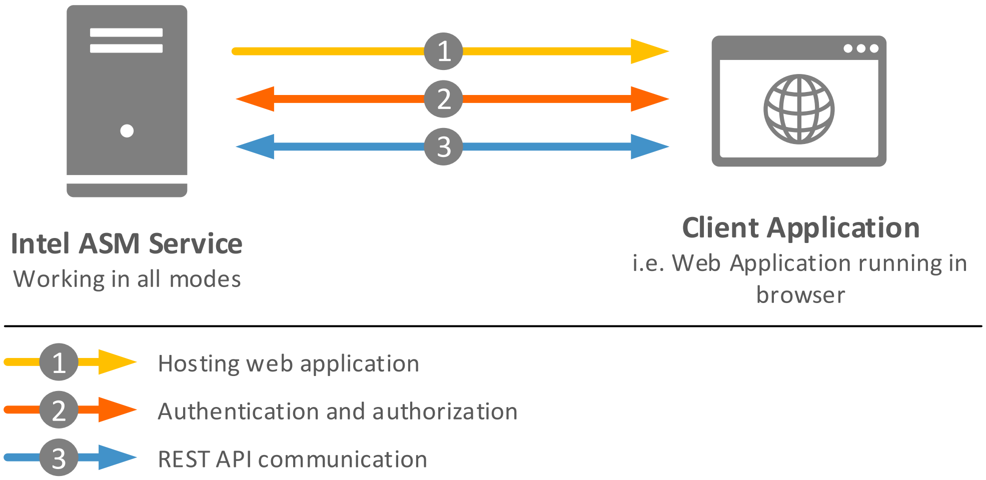

1
2
3
Intel ASM Service
Working in all modes
Client Application
i.e. Web Application running in browser
1 Hosting web application
2 Authentication and authorization
3 REST API communication

Figure 1 Intel ASM Standalone Configuration

4.3 Distributed configuration

If usage of multiple server machines is planned, Intel ASM shall be configured in distributed configuration. This configuration allows to use one authentication end-point and one application server to manage resource servers (see Figure 2).

Web application i.e. Intel ASM Management Console can be hosted from one dedicated machine. To perform authentication, client application running in web browser will then use one, known authentication server, instead of authenticating with each resource server separately.

After successful sign in, client application can communicate with selected resource server using REST API.

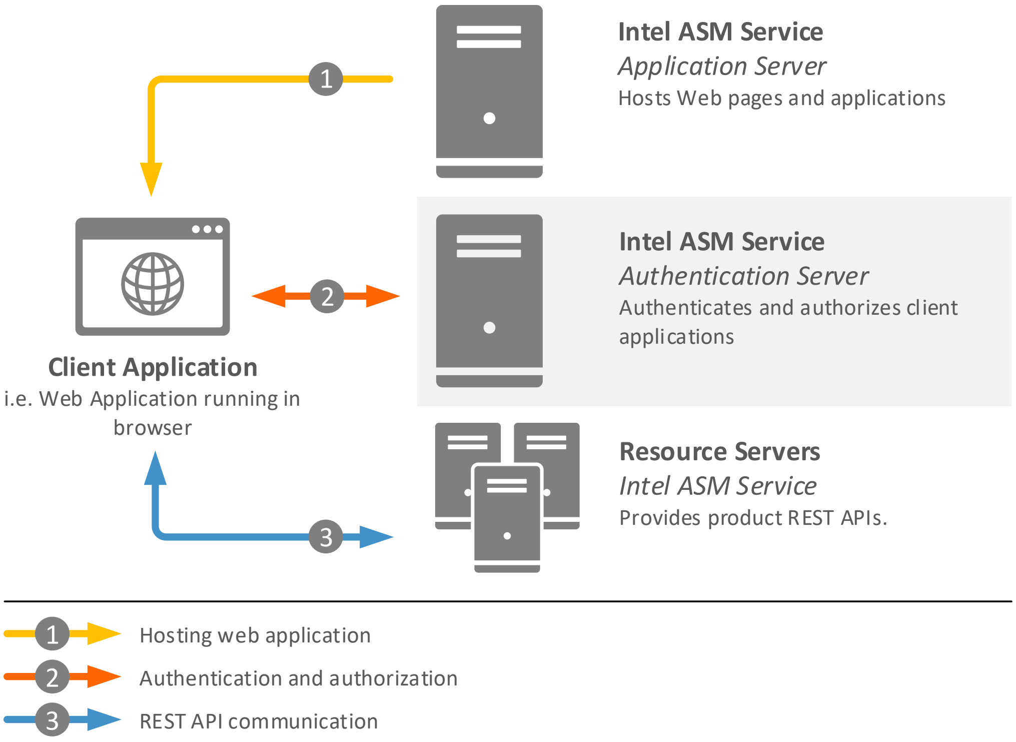

1
Intel ASM Service
Application Server
Hosts Web pages and applications
2
Intel ASM Service
Authentication Server
Authenticates and authorizes client applications
Client Application
i.e. Web Application running in browser
3
Resource Servers
Intel ASM Service
Provides product REST APIs.
1 Hosting web application
2 Authentication and authorization
3 REST API communication

Figure 2 Intel ASM Distributed Configuration

5 Getting started

5.1 Package Contents

For all supported systems, Intel Accelerated Storage Manager is released as installation packages.

For Linux SLES and RHEL distributions, all binaries and documentation are provided as native RED HAT PACKAGE MANAGER files (rpm):

- iasm-2.0.0-X.x86_64.rpm
- iasm-vroc-2.0.0-X.x86_64.rpm
- iasm-management-console-2.0.0-X.noarch.rpm

Intel Accelerated Storage Manager package contains:

- HTTP Service core binaries and configuration file.
- VROC Plugin to manage the product.
- System Plugin providing information about basic platform configuration.
- SSD Plugin providing device specific information.
- Web management console, a WEB GUI application to manage products through REST API.

5.2 System preparation

If usage of HTTPS is planned (which is strongly recommended for security reasons), Network or System Administrators or any authorized entity should create, sign and configure proper HTTPS certificates. For details of this configuration see section 6.1.

Note: It is recommended to install and configure Intel ASM only in local trusted network. Intel is not responsible for any damage caused by enabling remote access from public networks/Internet.

5.3 Installing Intel® ASM

On supported Linux distribution Intel Accelerated Storage Manager can be installed:

- *.rpm - through rpm package manager tool or through distribution specific package manager engine, *yum* for RHEL and *zypper* on SLES.

For more details about REST APIs, refer to section 6.5 - 6.6.

5.3.1 RPM Package Manager

Following example demonstrates installation of all components with rpm command (using '*' wildcard to select all rpm packages). To perform this action, administrator need to prior navigate to directory where Intel ASM packages are located:

```
$ sudo rpm –Uvh iasm*
Preparing...                           ################################# [100%]
Updating / installing...
   1:iasm-2.0.0-24                     ################################# [ 33%]
   2:iasm-vroc-2.0.0-24                ################################# [ 67%]
   3:iasm-management-console-2.0.0-24  ################################# [100%]
```

To verify if all packages were installed using *rpm*, run:

```
$ rpm -qa | grep iasm
iasm-2.0.0-24.x86_64
iasm-management-console-2.0.0-24.x86_64
iasm-vroc-2.0.0-24.x86_64
```

5.3.2 YUM Package Manager Engine

Example installation command using *yum* on RHEL distribution:

```
$ sudo yum install iasm*
```

To verify if all packages were installed, run:

```
$ yum list installed "iasm*"
Loaded plugins: product-id, search-disabled-repos, subscription-manager
Installed Packages
iasm.x86_64                     2.0.0-24  installed
iasm-management-console.x86_64  2.0.0-24  installed
iasm-vroc.x86_64                2.0.0-24  installed
```

5.3.3 ZYPPER Package Manager Engine

Example installation command using *zypper* on SLES distribution:

```
$ sudo zypper in iasm*
```

To verify if all packages were installed, run:

```
$ zypper se -i "iasm*"
Loading repository data...
Reading installed packages...

S | Name                    | Summary                                    | Type
--+-------------------------+--------------------------------------------+--------
i | iasm                    | Intel(R) Accelerated Storage Manager       | package
i | iasm-management-console | Intel(R) Accelerated Storage Manager - M-> | package
i | iasm-vroc               | Intel(R) Accelerated Storage Manager - R-> | package
```

5.4 Uninstalling Intel® ASM

Depending on preferences, administrator can use rpm command or distribution specific tools.

Example commands using *rpm* command:

```
$ sudo rpm -e iasm-management-console
$ sudo rpm -e iasm-vroc
$ sudo rpm -e iasm
```

Example command using *yum* on RHEL distribution:

```
$ sudo yum remove "iasm*"
```

Example command using *zypper* on SLES distribution.

```
$ sudo zypper remove "iasm*"
```

6 Configuring Intel® ASM

6.1 HTTPS recommended configuration

From security reason, it is highly recommended to use HTTPS communication. Unencrypted communication can lead to security vulnerability and cause, among others, leak of sensitive data.

Intel Accelerated Storage Manager can use valid and signed digital certificates to communicate over HTTPS.

To use HTTPS users need to be able to generate and sign such certificates. Certificate generation can be done on any machine with proper tools, however signing requires specific network and services configuration.

To sign certificate in local network at least one trusted Certificate Authority (CA) needs to be available and CAs root certificate needs to be propagated to all client machines.

Configuration of such environment is beyond the scope of this guide.

6.1.1 HTTPS configuration policies

6.1.1.1 Private Key Strength

Keys should be strong and remain strong for the planned lifetime. For use in Intel Accelerated Storage Manager Service, at least **2048** bit private key is recommended.

6.1.1.2 Private Key and Certificate Protection

Keys are very important and sensitive assets. They need to be stored in a secure location, under an access control, like file system with Access Control List on a trusted computer.

Always limit access only to minimum number of users.

If the key is compromised, it is always necessary to create a new key and revoke existing certificates.

It is highly recommended to renew certificates at least once in a year, with new private key.

6.1.1.3 Certification Authority (CA)

All used certificates should be signed by trusted Certification Authority. It is not recommended to use self-signed certificates.

Certification Authority shall be reliable, known and trusted, however it is up to network Administrators or other authorized entity to choose CA, since it is specific and dependent on current network infrastructure.

6.1.1.4 Certificate Chain of Trust

Always provide all intermediate certificates to ensure that path validation is done correctly on client side.

6.1.2 HTTPS configuration

Following sections describes sample generation of key and certificate signing request. All below examples use *OpenSSL* toolkit and assume that *OpenSSL* is already installed on configured machine.

6.1.2.1 Generating Private Key

Before generating signed request, private key needs to be created. Following example generates 2048 bit RSA key.

```
$ openssl genrsa -out ~/private.key 2048
Generating RSA private key, 2048 bit long modulus
.....................+++
.................................+++
e is 65537 (0x10001)
```

6.1.2.2 Generating Certificate Signing Request (CSR)

Command below generates CSR with use of private key. In this process, user will need to enter additional information. Using sha256 here is highly recommended.

```
$ openssl req -new -sha256 -key ~/private.key -out request.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:PL
State or Province Name (full name) [Some-State]:Pomerianian
Locality Name (eg, city) []:Gdansk
Organization Name (eg, company) [Internet Widgits Pty Ltd]:My Corporation
Organizational Unit Name (eg, section) []:MyUnit
Common Name (e.g. server FQDN or YOUR name) []:restapi.mycorp.com
Email Address []:johndoe@mycorp.org

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Following command can be used to validate created CSR:

```
$ openssl req -noout -text -in ~/request.csr
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=PL, ST=Pomerianian, L=Gdansk, O=My Corporation,
OU=MyUnit, CN= restapi.mycorp.com /emailAddress= johndoe@mycorp.org
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:d6:c9 ...
                Exponent: 65537 (0x10001)
        Attributes:
            a0:00
    Signature Algorithm: sha256WithRSAEncryption
         69:bc:2e ...
```

6.1.2.3 Submitting CSR

Generated CSR should be now submitted to CA in order to be signed. Certificate Authority, if CSR will be issued successfully, will return signed certificate.

Form and process of submission and signing depends on CA policies.

Since configuration of Certificate Authority and issuing process is different depending on used technology and infrastructure setup, signing process will not be described in this document.

6.1.2.4 Using Signed certificate in HTTP Service

Intel Accelerated storage manager uses private key and certificate stored in one file. Use following command to create such file (assuming that signed certificate returned by CA is named "signed.pem"):

```
(openssl x509 -in signed.pem; cat private.key) > iasm.pem
```

In order to use signed certificate, Administrator need to set following options in configuration file and restart Intel ASM service:

```
…
port = 443
https = true
certificate = /path-to-certificate-directory/iasm.pem
…
```

6.2 Command line configuration

Preferred configuration method of Intel Accelerated Storage Manager is to run service executable with proper command line options. This method will not only write provided options to file, but it will also validate configuration file correctness.

To print all available commands with parameters run service executable with "help" command.

6.2.1 Command line options

6.2.1.1 "serve" command

Usage:

```
iasm serve [-I][--host] [-P][--port] [-H][--https]
[-C][--certificate] [-X][--http-threads] [-Y][--plug-threads]
[-Z][--plug-timeout] [-V][--oa-auth-provider] [-D][--web-content]  [-S][--
web-server] [-A][--oa-server] [-O][--oa-server-host]
[-T][--oa-server-port] [-B][--oa-token-expiration-time]
[-E] [--oa-code-expiration-time] [-R][--oa-refresh-expiration-time]  [-
G][--oa-grants]
```

Options:

Config parameter	Option	Short option	description

host	--host	-I	HTTP Server IP address (127.0.0.1 for local offline configuration)
port	--port	-P	HTTP Server port
https	--https	-H	Set https on or off. (true/false)
certificate	--certificate	-C	Path to certificate, if https is on. Set "none" or "non" if no path was specified.
http_threads	--http-threads	-X	Set number of threads handling requests in HTTP server
plugins_threads	--plug-threads	-Y	Set number of threads handling request's code execution in plugins
plugins_timeout	--plug-timeout	-Z	Set timeout on request's code execution in plugin
oa_auth_provider	--oa-auth-provider	-V	Set authentication provider. (local/domain)
web_content	--web-content	-D	Path to directory with webpage files. Set "none" or "non" if no path was specified.
web_server	--web-server	-S	Enables webpage serving. (true/false)
oa_server	--oa-server	-A	Enable authorization on remote server. (true/false)
oa_server_host	--oa-server-host	-O	Authorization server IP address
oa_server_port	--oa-server-port	-T	Authorization server port
oa_token_expiration_time	--oa-token-expiration-time	-B	Set access token expiration time. (in seconds)
oa_code_expiration_time	--oa-code-expiration	-E	Set access code expiration time. (in seconds)
oa_refresh_expiration_time	--oa-refresh-expiration	-R	Set refresh token expiration time. (in seconds)
oa_grants	--oa-grants	-G	Set grants supported by authorization server. (code,implicit,password)

6.2.1.2 Client applications management

6.2.1.2.1 New client registration

Usage:

```
iasm register_client [-C][--client_id] [-S][--scopes] [-G][--grants]
```

Options:

Config parameter	Option	Short option	description
client_id	--client_id	-C	ID of client to be added
scopes	--scopes	-S	Scopes to which client will have an access separated by comma. Scope format: ip@scope. No ip defines scope for all resource servers
Grants	--grants	-G	Grants allowed to use by new client separated by comma (implicit,code)

6.2.1.2.2 Unregistering client application

Usage:

```
iasm remove_client [-C][--client_id]
```

Options:

Config parameter	Option	Short option	description
client_id	--client_id	-C	ID of client to remove

6.2.1.2.3 Updating client information

If key is left empty, its value will be erased.

Usage:

```
iasm update_client [-C][--client_id] [-S][--scopes] [-G][--grants]
```

Options:

Config parameter	Option	Short option	description
client_id	--client_id	-C	ID of client to be added
scopes	--scopes	-S	Scopes to which client will have an access separated by comma. Scope format: ip@scope. No ip defines scope for all resource servers
grants	--grants	-G	Grants allowed to use by new client separated by comma (implicit,code)

6.2.1.3 Scopes management

6.2.1.3.1 Adding new scope

Usage:

```
iasm add_scope [-N][--name] [-U][--users] [-G][--groups]
```

Options:

Config parameter	Option	Short option	description
name	--name	-N	Name of scope to be added with ip address of resource server. Format: ip@scope. No ip defines scope for all resource servers.
users	--users	-U	Users having access to scope separated by comma
groups	--groups	-G	Groups having access to scope separated by comma

6.2.1.3.2 Removing scope

Usage:

```
iasm remove_scope [-N][--name]
```

Options:

Config parameter	Option	Short option	description
name	--name	-N	Name of scope to be added with ip address of resource server. Format: ip@scope. No ip defines scope for all resource servers.

6.2.1.3.3 Updating scope information

Usage:

```
iasm update_scope [-N][--name] [-U][--users] [-G][--groups]
```

Options:

Config parameter	Option	Short option	description
name	--name	-N	Name of scope to be added with ip address of resource server. Format: ip@scope. No ip defines scope for all resource servers.
users	--users	-U	Users having access to scope separated by comma
groups	--groups	-G	Groups having access to scope separated by comma

6.2.1.4 List command

Lists queried parameters.

Usage:

```
iasm list [-C][--clients] [-S][--scopes] [-U][--users] [-G][--groups]
```

Options:

Config parameter	Option	Short option	description
clients	--clients	-C	List clients
scopes	--scopes	-S	List scopes
users	--users	-U	List users
groups	--groups	-G	List groups

6.3 Configuration file structure

Intel Accelerated Storage Manager uses *iasm.conf* file to store and read configuration. This file is placed in */etc/iasm/* directory on Linux.

After each file modification, service restart is required.

Default *iasm.conf* file presented below:

```
[config]
host = localhost
port = 80
http_threads = 16
plugins_threads = 8
plugins_timeout = 300
https = false
certificate = non
web_server = false
web_content = non
oa_auth_provider = local
oa_server = false
oa_server_host = localhost
oa_server_port = 80
oa_grants = implicit,code
oa_token_expiration_time = 3600
oa_code_expiration_time = 30
oa_refresh_expiration_time = 7200

[client]
client_id = "Intel Accelerated Storage Manager"
scopes = info,vroc,ssd
grants = implicit,code

[scope]
name = info
```

```
[scope]
name = vroc

[scope]
name = ssd
```

6.4 Managing the service

To start/stop or check the status of Intel Accelerated Storage Manager service on Linux distribution user with administrative privileges should use the *systemd system and services manager* control tool: '*systemctl*':

Starting the service and checking its' status:

```
$ sudo systemctl start iasmd.service

$ systemctl status iasmd.service
● iasmd.service - The Intel Accelerated Storage Service
   Loaded: loaded (/usr/lib/systemd/system/iasmd.service; disabled; vendor preset:
disabled)
   Active: active (running) since Sat 2016-07-09 02:30:58 EDT; 1 weeks 3 days ago
  Process: 3132 ExecStart=/usr/bin/iasm daemon (code=exited, status=0/SUCCESS)
 Main PID: 3133 (iasm)
   CGroup: /system.slice/iasmd.service
           └─3133 /usr/bin/iasm daemon

Jul 09 02:30:58 srv systemd[1]: Starting The Intel Accelerated Storage Service...
Jul 09 02:30:58 srv systemd[1]: Started The Intel Accelerated Storage Service.
Jul 09 02:30:58 srv iasm[3133]: Intel Accelerated Storage Manager: Service Started
(localhost:80)
```

Stopping the service and checking its' status:

```
$ sudo systemctl stop iasmd.service

$ systemctl status iasmd.service
● iasmd.service - The Intel Accelerated Storage Service
   Loaded: loaded (/usr/lib/systemd/system/iasmd.service; disabled; vendor preset:
disabled)
   Active: inactive (dead)

Jul 09 02:30:58 srv systemd[1]: Starting The Intel Accelerated Storage Service...
Jul 09 02:30:58 srv systemd[1]: Started The Intel Accelerated Storage Service.
Jul 09 02:30:58 srv iasm[3133]: Intel Accelerated Storage Manager: Service Started
(localhost:80)
Jul 19 03:51:18 srv systemd[1]: Stopping The Intel Accelerated Storage Service...
Jul 19 03:51:18 srv systemd[1]: Stopped The Intel Accelerated Storage Service.
```

By default Intel Accelerated Storage Manager does not start with system boot, this however, can be configured using the '*systemctl*' tool.

Enabling service auto-start:

```
$ sudo systemctl enable iasmd.service
Created symlink from /etc/systemd/system/multi-user.target.wants/iasmd.service to
/usr/lib/systemd/system/iasmd.service.

$ systemctl status iasmd.service
● iasmd.service - The Intel Accelerated Storage Service
   Loaded: loaded (/usr/lib/systemd/system/iasmd.service; enabled; vendor preset:
disabled)
   Active: active (running) since Tue 2016-07-19 04:00:34 EDT; 1s ago
  Process: 11758 ExecStart=/usr/bin/iasm daemon (code=exited, status=0/SUCCESS)
 Main PID: 11759 (iasm)
   CGroup: /system.slice/iasmd.service
           └─11759 /usr/bin/iasm daemon

Jul 19 04:00:34 srv systemd[1]: Starting The Intel Accelerated Storage Service...
Jul 19 04:00:34 srv systemd[1]: Started The Intel Accelerated Storage Service.
Jul 19 04:00:34 srv iasm[11759]: Intel Accelerated Storage Manager: Service
Started (localhost:80)
```

6.5 Standalone configuration example

This section contains an example standalone configuration of Intel Accelerated Storage Manager. All application components will be installed and configured on one server machine.

Installation of Intel ASM for remote management requires system with configured network interface.

For details of Linux network configuration please refer to distribution specific documentation i.e. “RHEL Network Guide” or “Configuring a Network Connection with YaST”.

6.5.1 Assumptions

- **All used IP addresses are examples only (except 127.0.0.1).**
- Platform used **must** support VROC 6.0.
- Server machine contains a Red Hat Linux Enterprise distribution already installed.
- Machine IP address is 10.100.100.10 (To configure service locally, on machine without network access, 127.0.0.1 loopback address should be used).
- Intel ASM Server will be configured to use machine IP address and 8080 port.
- User that will perform all configuration steps (admin) has superuser (sudo) privileges.

6.5.2 Installation

Extracting the release package files.

Copy the Intel Accelerated Storage Manager release package (iasm-2.0.0.X.zip) to your home directory ("/home/admin" in this example).

Run following commands to unpack rpm files:

```
[admin@10.100.100.10 ~]$ unzip iasm-2.0.0.24.zip -d ~/iasm-2.0.0.24
Archive:  iasm-2.0.0.24.zip
  inflating: /home/admin/iasm-2.0.0.24/iasm-2.0.0-24.x86_64.rpm
  inflating: /home/admin/iasm-2.0.0.24/iasm-management-console-2.0.0-24.noarch.rpm
  inflating: /home/admin/iasm-2.0.0.24/iasm-vroc-2.0.0-24.x86_64.rpm

[admin@10.100.100.10 ~]$ cd iasm-2.0.0.24/
```

Installing components.

Using "*yum*", install all rpm packages previously extracted to "iasm-2.0.0.24" directory and verify installation status:

```
[admin@10.100.100.10 iasm-2.0.0.24]$ sudo yum install *.rpm
...
[admin@10.100.100.10 iasm-2.0.0.24]$ yum list installed "iasm*"
Loaded plugins: product-id, search-disabled-repos, subscription-manager
Installed Packages
iasm.x86_64                     2.0.0-24  installed
iasm-management-console.x86_64  2.0.0-24  installed
iasm-vroc.x86_64                2.0.0-24  installed
```

6.5.3 Configuration

Configuring Intel ASM Service

All configuration presented below can be done by manually editing "/etc/iasm/iasm.conf" file. This file contains also commented entries for all available application scopes.

Configure HTTP service to listen on 10.100.100.10 address, under 8080 port, enable WWW server capability and provide valid path to Intel ASM GUI:

```
[admin@10.100.100.10 ~]$ sudo iasm config -I 10.100.100.10 -P 8080
[admin@10.100.100.10 ~]$ sudo iasm config -S true -D /usr/share/iasm/www/
```

For the localhost configuration:

```
[admin@10.100.100.10 ~]$ sudo iasm config -I 127.0.0.1 -P 8080
[admin@10.100.100.10 ~]$ sudo iasm config -S true -D /usr/share/iasm/www/
```

Update required scopes to grant access to "*admin*" user:

```
[admin@10.100.100.10 ~]$ sudo iasm update_scope -N vroc -U admin
[admin@10.100.100.10 ~]$ sudo iasm update_scope -N info -U admin
[admin@10.100.100.10 ~]$ sudo iasm update_scope -N ssd -U admin
```

By default Linux firewall will block all connection on port 8080, to open this port for public zone run following commands:

```
[admin@10.100.100.10 ~]$ sudo firewall-cmd --permanent --zone=public --add-
port=8080/tcp
[admin@10.100.100.10 ~]$ sudo firewall-cmd --reload
```

Note: This is just an example firewall configuration. This is up to administrator choice which port will be used and opened on which zone. On production server, firewall configuration should follow the company network security policies.

Configuring Intel ASM Management Console

Open GUI configuration file for editing i.e. using vi:

```
[admin@10.100.100.10 ~]$ sudo vi /usr/share/iasm/www/config.json
```

Edit file by adding resource server URI, in this example, for standalone configuration this should point to current server IP and port.

After modifications GUI configuration file should look like this:

```
{
    "AUTHORIZATION_URL": "",
    "RESOURCE_SERVER_ARRAY": ["http://10.100.100.10:8080"],
    "API_VERSION": "v1",
    "PLUGINS_PATH": "source/plugins/",
    "APPLICATION_IDENTIFIER": "Intel Accelerated Storage Manager"
}
```

For the localhost configuration:

```
{
    "AUTHORIZATION_URL": "",
    "RESOURCE_SERVER_ARRAY": ["http://127.0.0.1:8080"],
    "API_VERSION": "v1",
    "PLUGINS_PATH": "source/plugins/",
    "APPLICATION_IDENTIFIER": "Intel Accelerated Storage Manager"
}
```

Starting and testing configuration

Start Intel ASM service:

```
[admin@10.100.100.10 ~]$ sudo systemctl start iasmd
```

Test installation by navigating to "http://10.100.100.10:8080" URI in web browser.

As a username and password, use previously configured user with his corresponding system password (admin).

6.6 Distributed configuration example

As described in 4.3 Intel Accelerated Storage manager can be configured to work on multiple servers with one or many authentication end points and one or many application servers.

Installation of Intel ASM for remote management requires system with configured network interface.

For details of Linux network configuration please refer to distribution specific documentation i.e. “RHEL Network Guide” or “Configuring a Network Connection with YaST”.

6.6.1 Assumptions

Example configuration assumes that (Figure 3):

- **All used IP addresses are examples only (except 127.0.0.1).**
- Network configuration contains at least one domain controller against which all Intel ASM Clients will be authenticated (domain example.com),
- There are two users configured on Domain Controller that will be authorized for Intel ASM services with logins: "*jeff*" and "*esmond*".
- All resource servers will be authenticated against one Intel ASM authentication service – this target machine is joined to domain "*example.com*",
- One Intel ASM service will work in application server mode, where Intel ASM management console will be hosted,
- There are two Intel ASM services working in resource server mode.

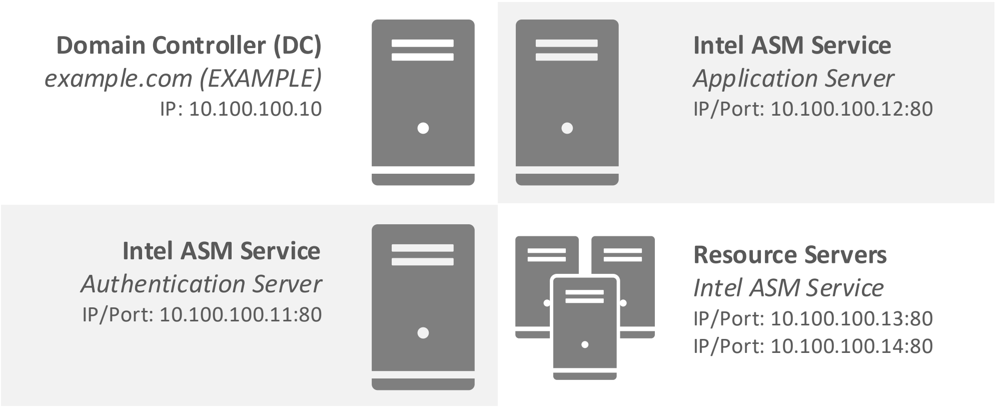


Figure 3 Example of distributed configuration

6.6.1 Authentication Server Configuration

Installing components.

Log-in to dedicated server (10.100.100.11 in this example) and extract "iasm-x.x-xxx.x86_64.rpm" file from Intel ASM release package.

Install this package using "*yum*" and verify installation status:

```
[admin@10.100.100.11 iasm-2.0.0.24]$ sudo yum install iasm-2.0.0-24.x86_64.rpm
[admin@10.100.100.11 iasm-2.0.0.24]$ yum list installed "iasm*"
Loaded plugins: product-id, search-disabled-repos, subscription-manager
Installed Packages
iasm.x86_64                     2.0.0-24   installed
```

Configuring Authentication service

For configuration, use following commands or manually edit "*/etc/iasm/iasm.conf*" file.

Configure HTTP service to listen on 10.100.100.11 address, under 80 port:

```
[admin@10.100.100.11 ~]$ sudo iasm config -I 10.100.100.11 -P 80
```

Configure Intel ASM to use domain authentication:

```
[admin@10.100.100.11 ~]$ sudo iasm config -V domain
```

Update required scopes to grant user access:

```
[admin@10.100.100.11 ~]$ sudo iasm update_scope -N vroc -U jeff@example.com
[admin@10.100.100.11 ~]$ sudo iasm update_scope -N vroc -U esmond@example.com
[admin@10.100.100.11 ~]$ sudo iasm update_scope -N info -U jeff@example.com
[admin@10.100.100.11 ~]$ sudo iasm update_scope -N info -U esmond@example.com
[admin@10.100.100.11 ~]$ sudo iasm update_scope -N ssd -U jeff@example.com
[admin@10.100.100.11 ~]$ sudo iasm update_scope -N ssd -U esmond@example.com
```

Starting Authorization Service

Start Intel ASM service with following command:

```
[admin@10.100.100.11 ~]$ sudo systemctl start iasmd
```

6.6.2 Application Server Configuration

Installing components.

Log-in to dedicated server (10.100.100.12 in this example) and extract "iasm-2.0.0-X.x86_64.rpm" and "iasm-management-console-2.0.0-X.noarch.rpm" files from Intel ASM release package.

Install packages using "*yum*" and verify installation status:

```
[admin@10.100.100.12 iasm-2.0.0.24]$ sudo yum install iasm*
...
[admin@10.100.100.12 iasm-2.0.0.24]$ yum list installed "iasm*"
Loaded plugins: product-id, search-disabled-repos, subscription-manager
Installed Packages
iasm.x86_64                     2.0.0-24  installed
iasm-management-console.x86_64  2.0.0-24  installed
```

Configuring HTTP service

For configuration, use following commands or manually edit "*/etc/iasm/iasm.conf*" file.

Configure HTTP service to listen on 10.100.100.12 address, under 80 port, enable WWW server capability and provide valid path to Intel ASM GUI:

```
[admin@10.100.100.12 ~]$ sudo iasm config -I 10.100.100.12 -P 80
[admin@10.100.100.12 ~]$ sudo iasm config -S true -D /usr/share/iasm/www/
```

Configuring Intel ASM Management Console

Open GUI configuration file for editing i.e. using vi:

```
[admin@10.100.100.12 ~]$ sudo vi /usr/share/iasm/www/config.json
```

Edit file by adding previously configured authorization server URI (10.100.100.11) and by adding resource server URIs, in this example 10.100.100.13 and 10.100.100.14.

After modifications, GUI configuration file should look like this:

```
{
    "AUTHORIZATION_URL": ""http://10.100.100.11:80",
    "RESOURCE_SERVER_ARRAY": ["http://10.100.100.13:80", "http://10.100.100.14:80"],
    "API_VERSION": "v1",
    "PLUGINS_PATH": "source/plugins/",
    "APPLICATION_IDENTIFIER": "Intel Accelerated Storage Manager"
}
```

Starting Application Service

Start Intel ASM service with following command:

```
[admin@10.100.100.12 ~]$ sudo systemctl start iasmd
```

6.6.3 Resource Servers Configuration

Perform those steps for each resource server machine.

Installing components.

Log-in to dedicated server (10.100.100.13 in this example) and extract "iasm-2.0.0-X.x86_64.rpm" and "iasm-vroc-2.0.0-X.x86_64.rpm" files from Intel ASM release package.

Install packages using "*yum*" and verify installation status:

```
[admin@10.100.100.13 iasm-2.0.0.24]$ sudo yum install iasm*
...
[admin@10.100.100.13 iasm-2.0.0.24]$ yum list installed "iasm*"
Loaded plugins: product-id, search-disabled-repos, subscription-manager
Installed Packages
iasm.x86_64                     2.0.0-24  installed
iasm-vroc.x86_64                2.0.0-24  installed
```

Configuring HTTP service

For configuration, use following commands or manually edit "*/etc/iasm/iasm.conf*" file.

Configure HTTP service to listen on 10.100.100.13 address, under 80 port:

```
[admin@10.100.100.13 ~]$ sudo iasm config -I 10.100.100.13 -P 80
```

Configure Intel ASM to use previously configured authentication server (10.100.100.11:80):

```
[admin@10.100.100.13 ~]$ sudo iasm config -A true -O 10.100.100.11 -T 80
```

Starting Resource Service

Start Intel ASM service with following command:

```
[admin@10.100.100.13 ~]$ sudo systemctl start iasmd
```

Repeat these steps for 10.100.100.14 machine.

6.6.4 Testing Configuration

To test configuration, navigate in your web browser to application server (http://10.102.108.12), select one of resource servers from drop down list and click "Sign In" button.

Browser should navigate you to login page located on 10.100.100.11 machine.

Enter user credentials with domain name i.e.

- Username: jeff,
- Password: [jeff's password],

- Domain: example.lab,

Then click "Sign In".

After successful logging in, browser should redirect user back to 10.100.100.12 displaying Intel ASM Management Consoles Dashboard for selected resource server.

6.7 VROC 6.0 Managed Hotplug Locate

To enable correct behavior of Managed Hotplug to trigger LED Locate on removed disk, remember to configure ledmon to only control RAID devices (in */etc/ledmon.conf*):

```
RAID_MEMBERS_ONLY=1
```

Without this change, all Managed Hotplug operations will trigger LED Failed instead of Locate.

7 REST API

Intel Accelerated Storage Manager released with VROC 6.0 provides REST API for four different scopes:

- Security requests – set of functions providing OAuth 2.0 authentication capability.
- System Information – general set of information about platform where service is installed.
- SSD API – set of information about connected and supported storage devices.
- VROC API – set of management and informational functions for VROC 6.0 product.

Detailed information about requests and responses format are available in referenced documents:

- Intel ASM Security API.pdf
- Intel ASM System API.pdf
- Intel ASM SSD API.pdf
- Intel ASM VROC Plugin API.pdf

8 Intel VROC 6.0 Web GUI

8.1 Getting Started

8.1.1 Configuration

Web GUI settings are configured in config.json file. The file is located in the www directory.

After file modification service restart is required.

Web GUI configurables:

- Authorization URL – address of Oauth2.0 authorization server used by GUI to authenticate a user.
- API version – REST API version
- Application identifier – GUI ID used for application identification to authorization server (“client_id” from the iasm.conf file)
- Resource servers array – List of resource servers (servers’ URLs with RESTful Service)

  Resource server is an operating ASM service that exposes REST API through HTTP or HTTPS that allows Web GUI to fetch necessary data.

  Multiple Resource server URLs may be defined allowing user to quickly navigate through and manage different machines.

Example of *config.json* file presented below.

```
{
  "AUTHORIZATION_URL": "http://10.100.100.100:8080",
  "API_VERSION": "v1",
  "APPLICATION_IDENTIFIER": "Intel Accelerated Storage Manager",
  "PLUGINS_PATH": "source/plugins/",
  "RESOURCE_SERVER_ARRAY": [
    "http://10.100.100.100:8080",
    "http://10.100.100.101:8080"
  ]
}
```

8.1.2 Supported Browsers

- Google Chrome (version 50.0.2661+)
- Mozilla Firefox (version 42.0+)

- Internet Explorer 11+

8.1.3 Web Page Responsiveness

Web Page is responsive; therefore, it can be accessed by devices of all sizes from mobile phones through large monitors with comparable level of user experience.

Due to performance considerations, some functionalities are unavailable on mobile devices. These include dashboard edition, memory, and CPU performance monitoring.

8.1.4 Cookies

Application's session data is stored in cookies.

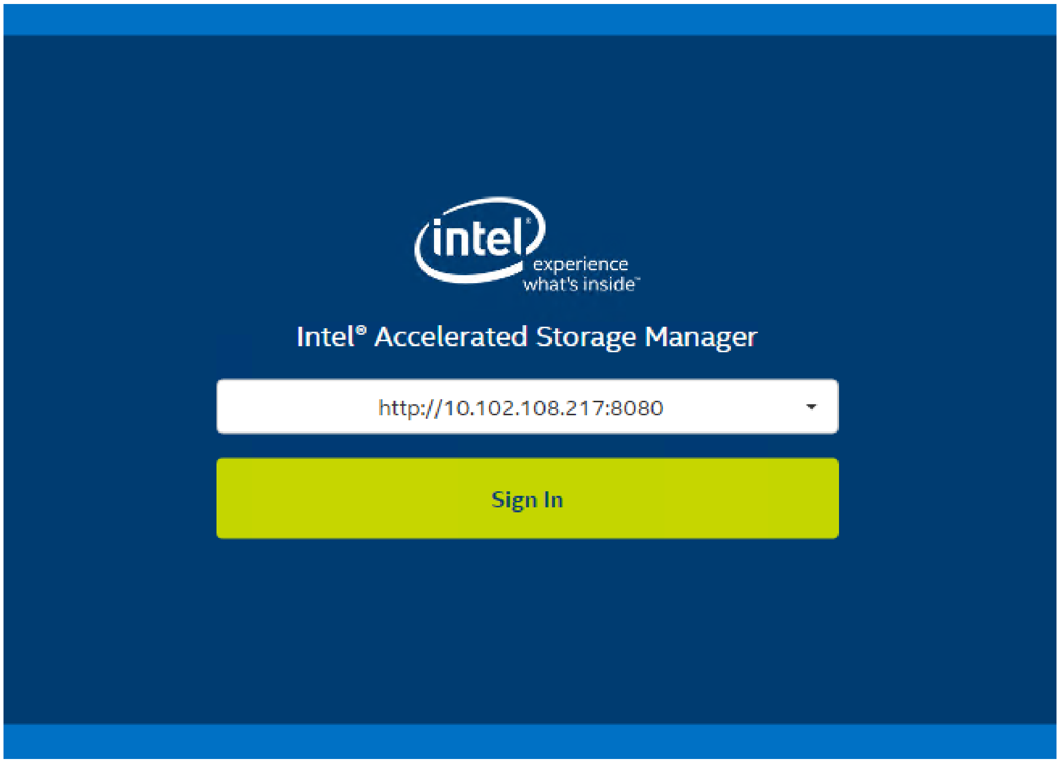
Browser's cookies are required for Web Page to work.
Disallowing cookies or removing them manually will log off a user.

8.2 Login Page

User requests access to the resource server by selecting it from dropdown menu.

List of available resource servers is configured in config.json file.

There has to be at least one resource server defined to gain access to the application. Authorization server cannot be selected from login page. It has to be configured in config.json file. If "AUTHORIZATION_URL" configurable is left blank, resource server is assumed to act as authorization server as well.

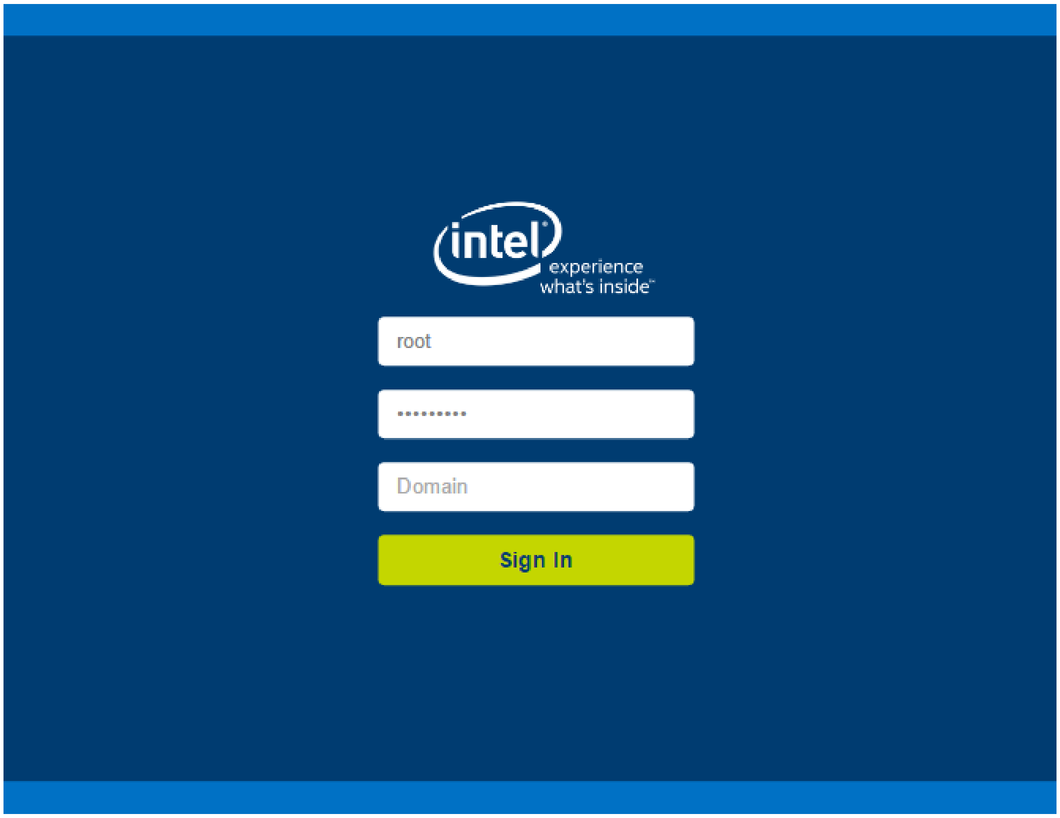


experience what's inside
Intel® Accelerated Storage Manager
http://10.102.108.217:8080
Sign In

“Sign In” button redirects user to the login form served by the authentication server.

User shall authenticate himself with system or domain credentials depending on Intel ASM configuration.

“Domain” field is mandatory when user authenticates against Active Directory Domain Services, otherwise field should remain empty.

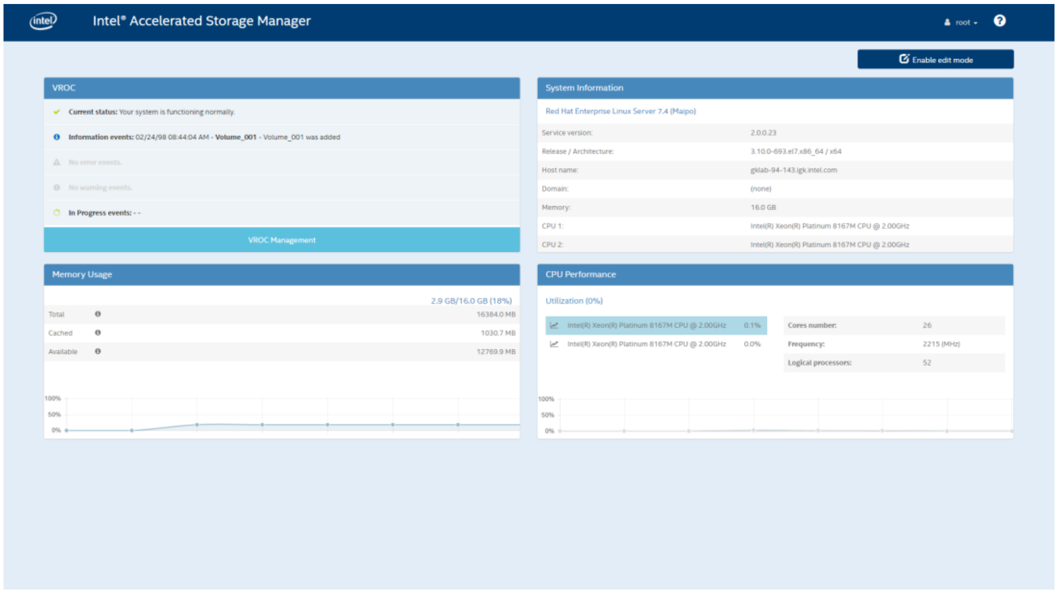


root

••••••••••

Once submitted credentials are confirmed, the user is redirected back to the application, where application dashboard is displayed.

8.3 Dashboard



Current status: Your system is functioning normally.

Information events: 02/24/98 08:44:04 AM - **Volume_001** - Volume_001 was added

No error events.

No warning events.

In Progress events: - -

2.9 GB/16.0 GB (18%)

Total	16384.0 MB
Cached	1030.7 MB
Available	12769.9 MB

Red Hat Enterprise Linux Server 7.4 (Maipo)

Service version:	2.0.0.23
Release / Architecture:	3.10.0-693.el7.x86_64 / x64
Host name:	gklab-94-143.igk.intel.com
Domain:	(none)
Memory:	16.0 GB
CPU 1:	Intel(R) Xeon(R) Platinum 8167M CPU @ 2.00GHz
CPU 2:	Intel(R) Xeon(R) Platinum 8167M CPU @ 2.00GHz

Utilization (0%)

Intel(R) Xeon(R) Platinum 8167M CPU @ 2.00GHz	0.1%
Intel(R) Xeon(R) Platinum 8167M CPU @ 2.00GHz	0.0%

Cores number:	26
Frequency:	2215 (MHz)
Logical processors:	52

This is main page of the web application. User may always navigate back to dashboard by clicking on INTEL logo in upper left corner or by selecting “Home” option in dropdown menu in upper right corner.

Dashboard is editable; therefore, user may configure widgets’ order and composition on the screen. To edit dashboard click “Enable edit mode” button and confirm changes once done. Dashboard settings are stored in browser’s Local Storage; hence, are not lost upon browser closure.

8.3.1 System Widget

System Widget presents basic information about the system, on which resource server is located.

8.3.2 Memory Widget

Memory Widget presents memory data such as Total, Cached, and Available memory. Real-time memory usage is presented on the graph.

8.3.3 CPU Performance Widget

CPU Performance Widget presents basic processor information.

Real-time CPU usage is presented on the graph. Each processor usage is shown as a separate plot.

8.3.4 VROC Management Widget

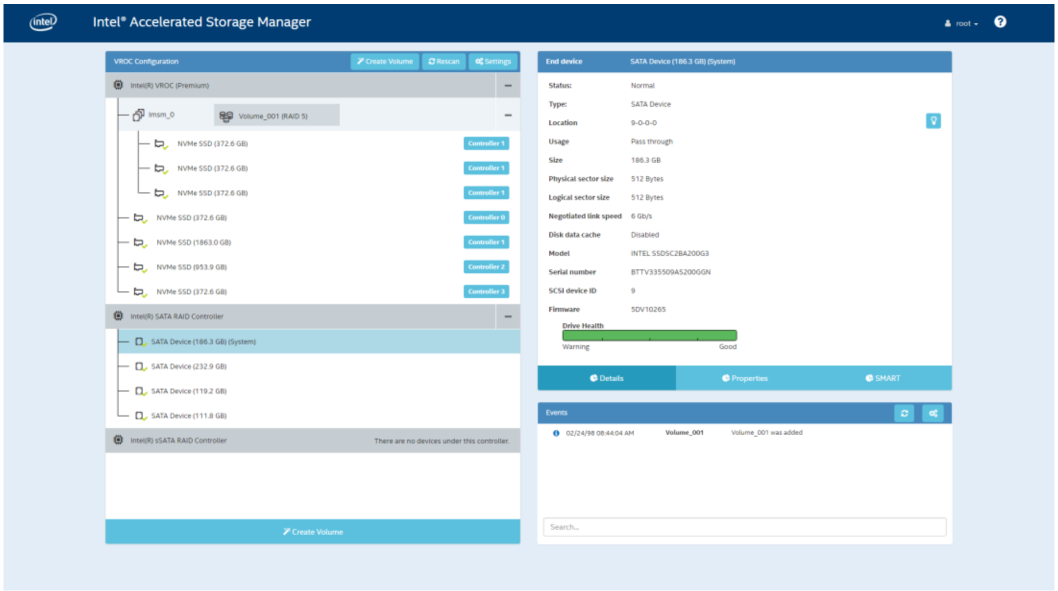
VROC Management Widget indicates whether VROC is functioning normally.

Additionally, all VROC events are displayed on this widget.

8.4 VROC Management

VROC Management is divided into three sections.

- Tree View
- Element Details View
- Events Log



End device SATA Device (186.3 GB) (System)

Status:	Normal
Type:	SATA Device
Location	9-0-0-0
Usage	Pass through
Size	186.3 GB
Physical sector size	512 Bytes
Logical sector size	512 Bytes
Negotiated link speed	6 Gb/s
Disk data cache	Disabled
Model	INTEL SSDSC2BA200G3
Serial number	BTTV335509A5200GGN
SCSI device ID	9
Firmware	5DV10265

02/24/98 08:44:04 AM **Volume_001** Volume_001 was added

8.4.1 Tree View

Tree View presents Controllers, Arrays, Volumes, and EndDevices. This guide will refer to them as components.

Controllers and Arrays can be collapsed to simplify the view if needed.

Aforementioned components are selectable. Selecting a component displays its details on the right side of the page in Details View.

8.4.2 Details View

This view contains detailed component information along with action buttons associated with them.

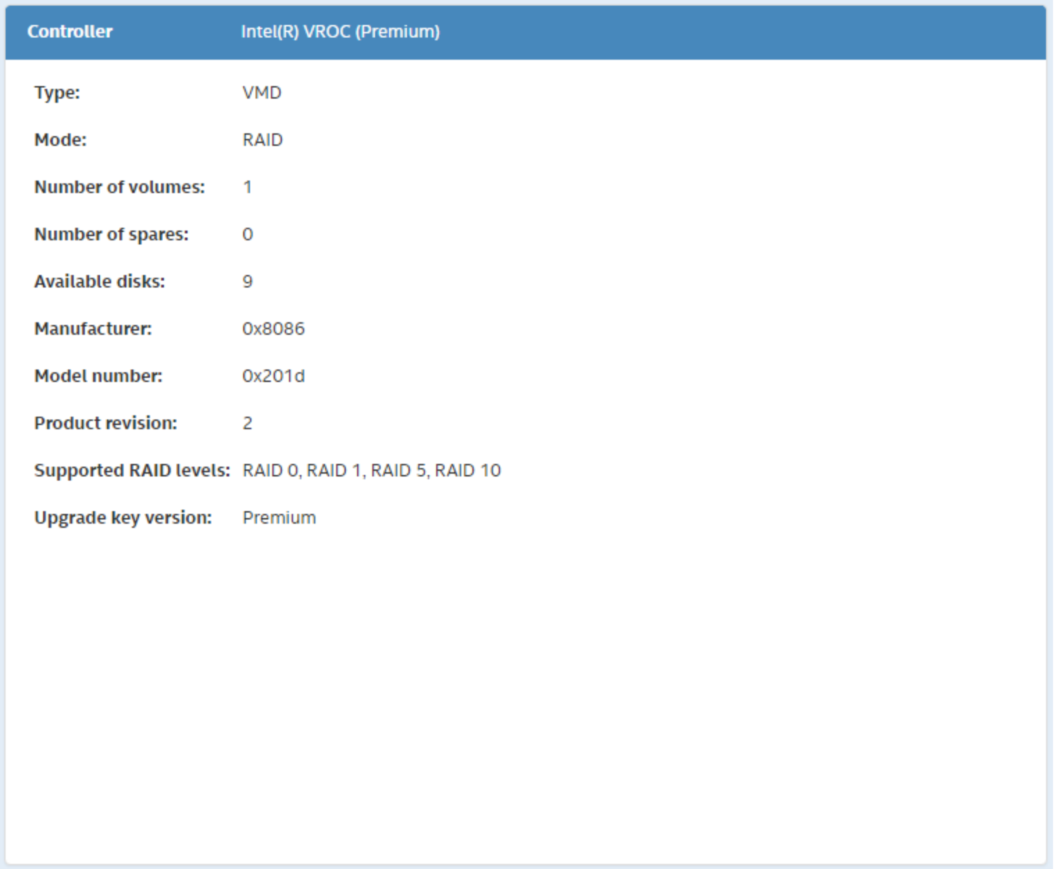
Displayed data and action buttons vary with every component.

Action buttons are displayed only when given action may be performed. Buttons are located next to the field they have impact on. Example: “Rename” button stands next to “Volume Name” field.

Complete list of action can be found below.

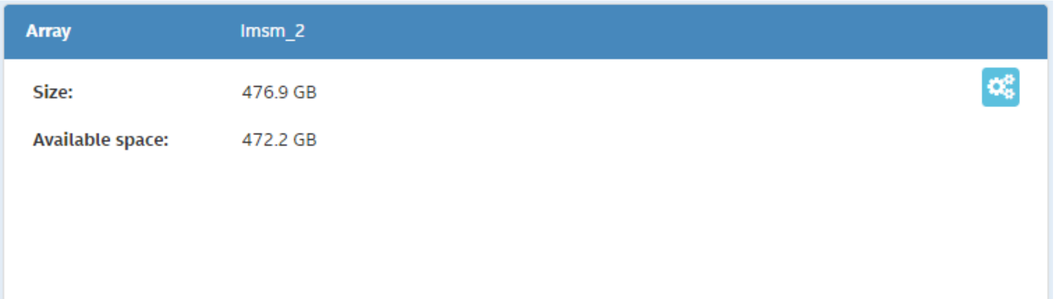
Help module describes these actions in more details.

8.4.2.1 Controller Details



Controller	Intel(R) VROC (Premium)
Type:	VMD
Mode:	RAID
Number of volumes:	1
Number of spares:	0
Available disks:	9
Manufacturer:	0x8086
Model number:	0x201d
Product revision:	2
Supported RAID levels:	RAID 0, RAID 1, RAID 5, RAID 10
Upgrade key version:	Premium

8.4.2.2 Array Details

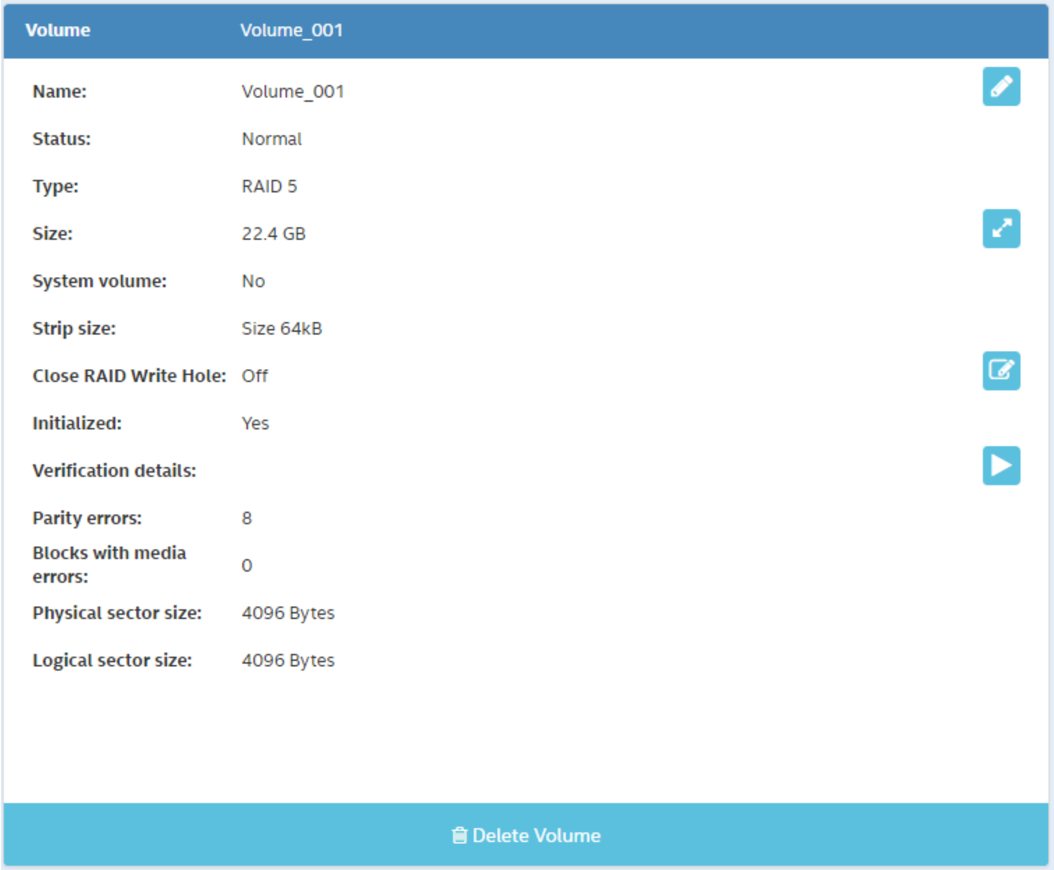


Array	Imsm_2
Size:	476.9 GB
Available space:	472.2 GB

Array actions:

- Add disk to Array

8.4.2.3 Volume Details



Volume Volume_001

Name: Volume_001

Status: Normal

Type: RAID 5

Size: 22.4 GB

System volume: No

Strip size: Size 64kB

Close RAID Write Hole: Off

Initialized: Yes

Verification details:

Parity errors: 8

Blocks with media errors: 0

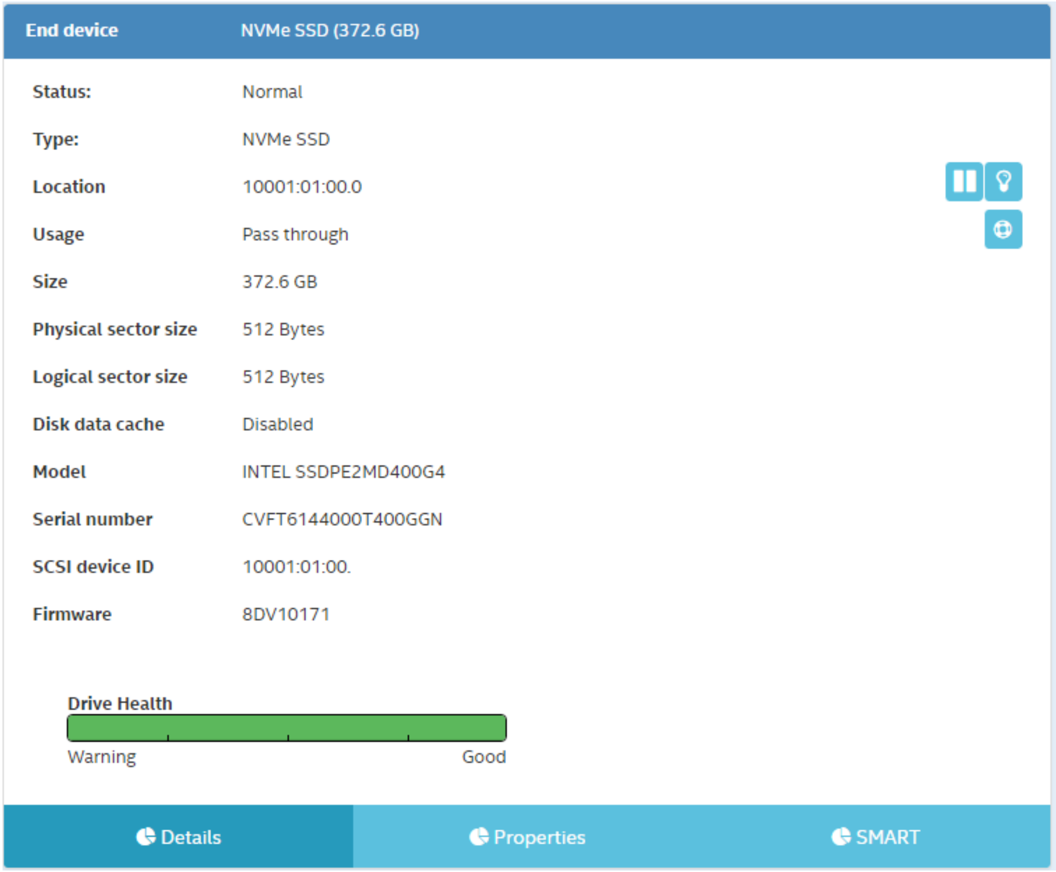
Physical sector size: 4096 Bytes

Logical sector size: 4096 Bytes

Volume actions:

- Rename Volume
- Rebuild Volume
- Mark Volume as Normal (Clear Volume Metadata)
- Change Volume Type (Raid Level migration)
- Change Volume Size
- Change Close RAID Write Hole (RWH) policy
- Verify/Verify and Fix
- Delete Volume

8.4.2.4 EndDevice Details



End device	NVMe SSD (372.6 GB)
Status:	Normal
Type:	NVMe SSD
Location	10001:01:00.0
Usage	Pass through
Size	372.6 GB
Physical sector size	512 Bytes
Logical sector size	512 Bytes
Disk data cache	Disabled
Model	INTEL SSDPE2MD400G4
Serial number	CVFT6144000T400GGN
SCSI device ID	10001:01:00.
Firmware	8DV10171

EndDevice actions:

- Mark disk as Normal
- Clear Metadata
- Activate LED/toggle LED
- Mark as Spare

There are two more tabs that are enabled only if SSD Plugin is installed.

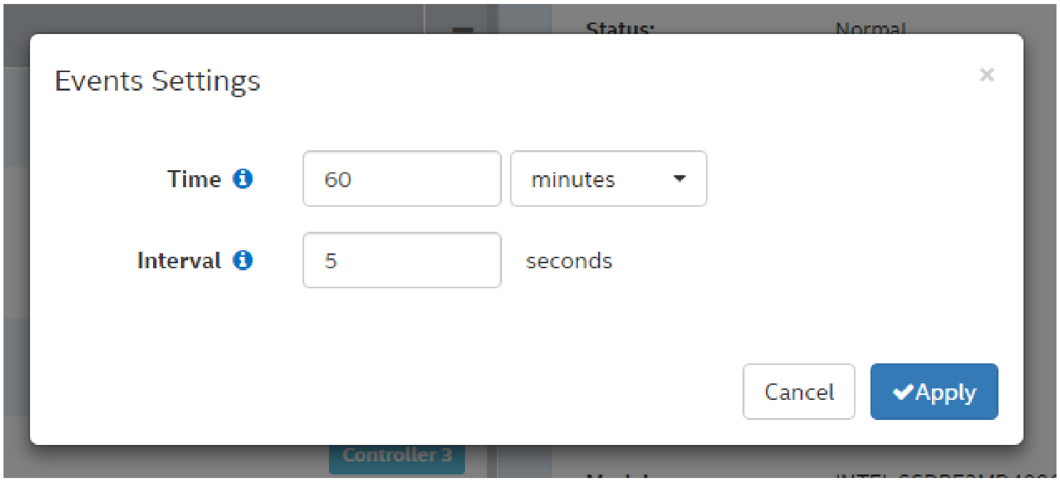
- Properties – collection of drive properties and health data.
- S.M.A.R.T. – collection of S.M.A.R.T. data

8.4.3 Events Log

Events log is a list of predefined events that ASM Service has reported.

Events log displays all events including those not triggered by the webpage user.

User may configure how frequently wants to update events log and what time depth should be.

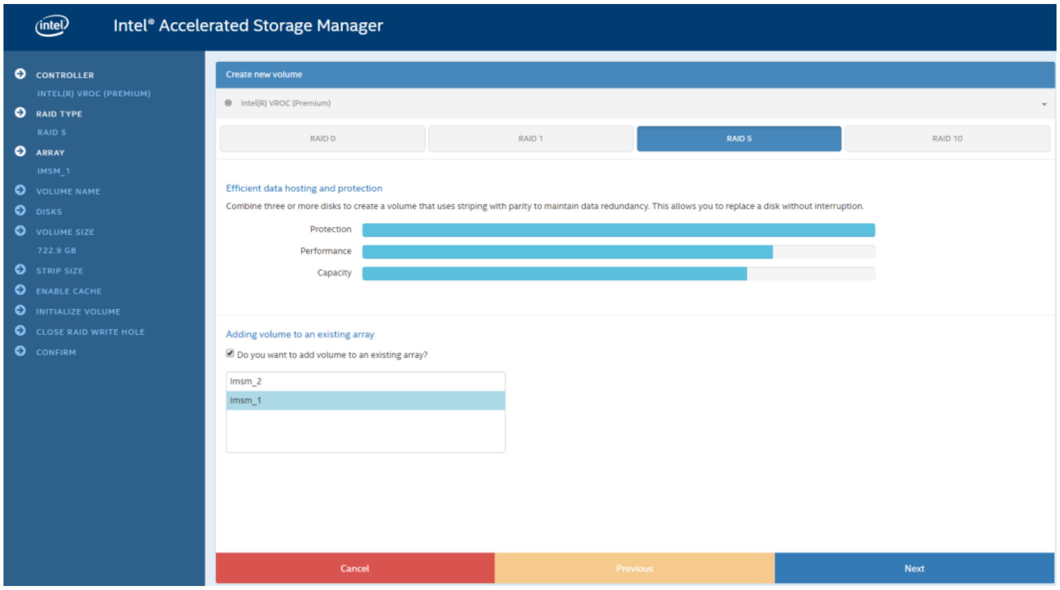


Events Settings

Time 60 minutes

Interval 5 seconds

8.4.4 Create New Volume Wizard



Intel® Accelerated Storage Manager

CONTROLLER
INTEL(R) VROC (PREMIUM)
RAID TYPE
RAID 5
ARRAY
IMSM_1
VOLUME NAME
DISKS
VOLUME SIZE
722.9 GB
STRIP SIZE
ENABLE CACHE
INITIALIZE VOLUME
CLOSE RAID WRITE HOLE
CONFIRM

Create new volume

Intel(R) VROC (Premium)

Efficient data hosting and protection

Combine three or more disks to create a volume that uses striping with parity to maintain data redundancy. This allows you to replace a disk without interruption.

Adding volume to an existing array

☑ Do you want to add volume to an existing array?

Imsm_2
Imsm_1

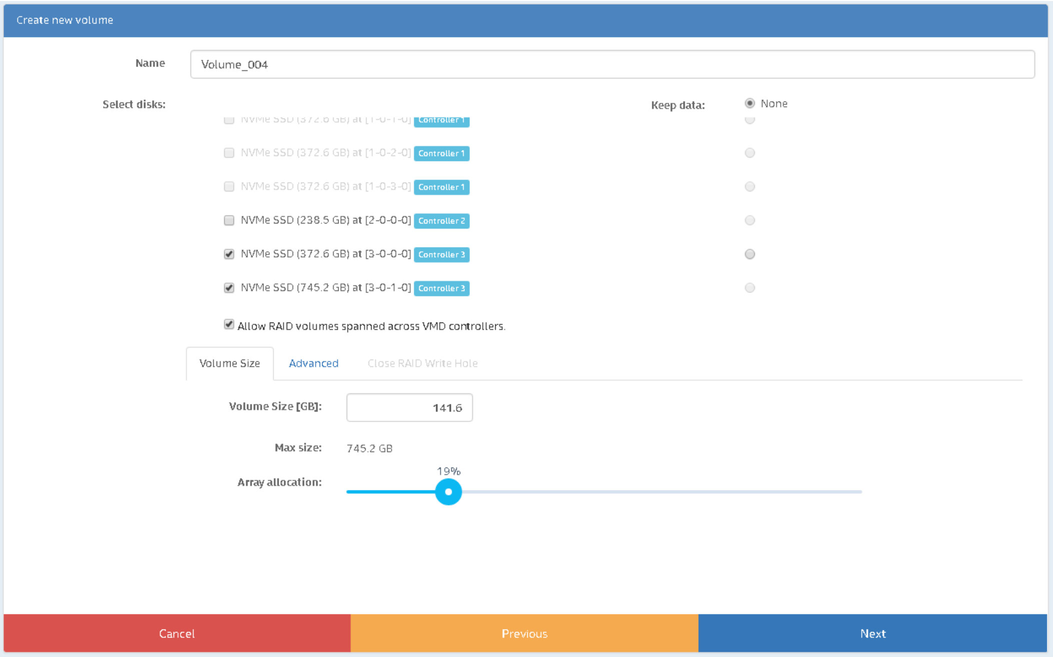
Process of creating new volume consists of several steps.

Each step's possible selection may be dependent on made selections in previous steps; therefore, it is highly recommended to work the process page by page, from top to bottom.

Steps:

- Select Controller
  - Select controller, on which new Volume shall be created. Controller has to be in RAID mode.
- Select RAID Level:
  - Select RAID Level for new volume. There are four RAID levels available: RAID0, RAID1, RAID5, and RAID10. RAID description can be found below RAID selection.

    Note: Key version determines which RAID levels can be created on a platform. These are as follows:
    - VROC (in pass-thru mode): RAID0
    - VROC STANDARD: RAID0, RAID1, RAID10
    - VROC PREMIUM: RAID0, RAID1, RAID5, RAID10
- Add volume to already existing array or create volume in a new array
  - Volume is created in a container called array. There is a possibility of creating up to two volumes in single array (Matrix RAID configuration). User may choose to create a volume in a new array or to add it to an already existing array. If user choose to add a new volume to an already existing array, most following options are blocked and cannot be altered.



Name: Volume_004

Select disks:

- ☐ NVMe SSD (372.6 GB) at [1-0-1-0] Controller 1
- ☐ NVMe SSD (372.6 GB) at [1-0-2-0] Controller 1
- ☐ NVMe SSD (372.6 GB) at [1-0-3-0] Controller 1
- ☐ NVMe SSD (238.5 GB) at [2-0-0-0] Controller 2
- ☑ NVMe SSD (372.6 GB) at [3-0-0-0] Controller 3
- ☑ NVMe SSD (745.2 GB) at [3-0-1-0] Controller 3

Keep data: ● None

☑ Allow RAID volumes spanned across VMD controllers.

Volume Size [GB]: 141.6

Max size: 745.2 GB

Array allocation: 19%

- Name new Volume
    - User may choose a name for the volume. Default name will be given, if user chooses not to do so.
- Select Disks to be included in a new volume
    - RAID0 – select at least two disks
    - RAID1 – select exactly two disks
    - RAID5 – select at least three disks
    - RAID10 – select exactly four disks

Note: While creating volume on VMD Controller, it is possible to create volume from disks located in different VMD Domains. User has to explicitly confirm that he wants to create such volume by checking “Allow VMD Spanning” checkbox.

Wizard blocks user from proceeding until disks are selected.

- Decide Volume Size
    - User may set volume’s size. This can be done either by slider or by manual input.
- Select Strip Size
    - Select volume Strip Size. Recommended Strip Size is set by default.

- Initialize Volume
    - This action will be done automatically once volume is created
- Select Close RAID Write Hole policy
    - Available RAID Write Hole policies are OFF, DISTRIBUTED